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 - 2024 Motorola Solutions, Inc. All rights reserved.

PDF-CCT-C

Revision: 10 - EN

20240925

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
- Secondary Media Profile Settings 8

Setting Tabs 10

Assigning IP Addresses 13
- Assigning Static IP Addresses 13

Setting the NTP Server 14

Configuring Multicast Networking 15

Managing Certificates 16
- Downloading a Certificate Signing Request 16
- Uploading Signed Certificates 17
- Applying Certificates 17
- Deleting Certificates 18
- Setting the Encryption Mode 18

Network Security 20
- Disabling HTTP Connections in the Camera Configuration Tool 20
- Disabling HTTP Connections for a Camera 20
- Changing the HTTP or HTTPS Port 20

Changing Camera Mode 22

Configuring Analytics 23

Analytics Setting Description 23

Setting Up Classified Object Motion Detection 25

Configuring Analytic Events 26

Setting Up a Radiometric Analytics Event 27

Advanced Thermal Event Settings 29

Temperature Threshold Advanced Settings 30

Temperature Change Advanced Settings 30

Configure a Radiometric Detection Area 31

Analytic Event Descriptions 31

Configuring Crowd Detection 32

Updating Firmware 34

Downloading Firmware 34

Applying Firmware 34

Critical Firmware Updates 34

Exporting and Importing Settings 36

Exporting Settings 36

Editing the Export File 36

Importing Settings 37

Configuration Templates 38

Use Configuration Templates to Bulk Apply Settings 39

Export a Configuration Template 39

Remove Settings from a Configuration Template (Optional) 39

Example 1 39

Example 2 40

Import and Apply a Configuration Template 40

Using the CCT Command Line 42

Starting the CCT Command Line 42

Command Line Parameters 43

Tips for Using the Command Line 45

Device Logs 47

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**.

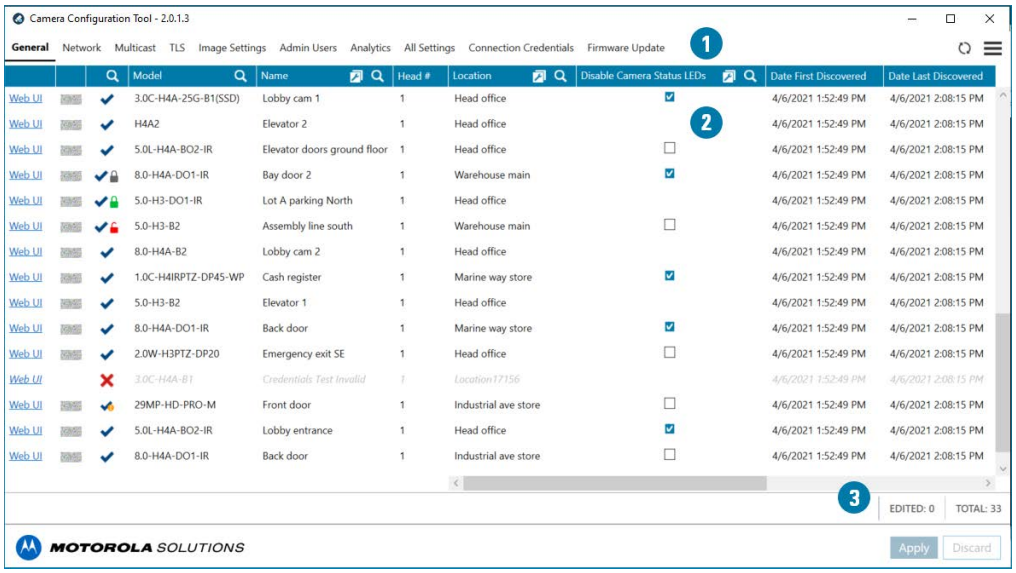
    You are logged into the discovered cameras using the selected credentials.

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 10.
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.

   > **Note:** If you have made any setting changes that are unsaved, you will not be able to change tabs. Discard your settings if you want to be able to 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**.

   > **Note:** Pelco cameras do not support an empty password field. A password must be set for Pelco camera admin accounts.

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**.

> **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 10.

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**.

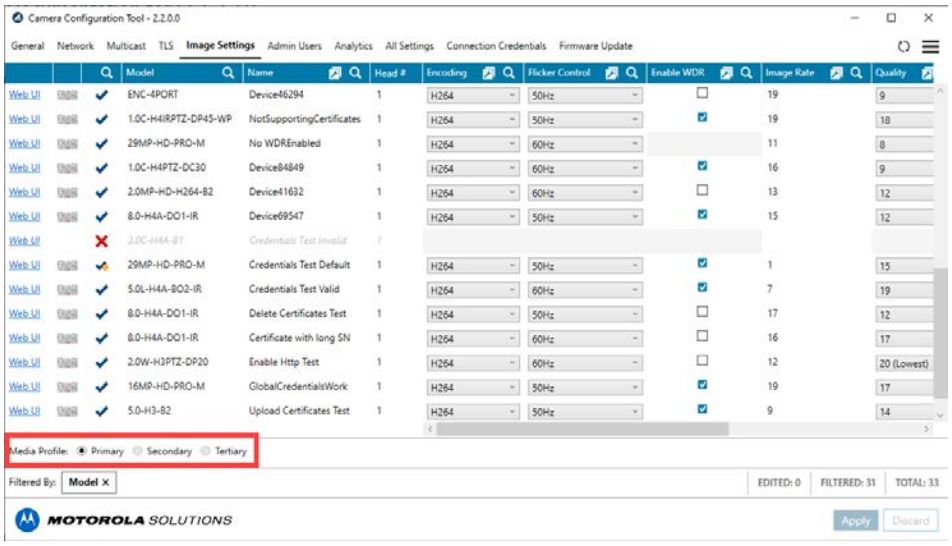
Secondary Media Profile Settings

Many cameras have the capability of transmitting additional video streams, or media profiles, in addition to its primary stream. For example, a secondary stream can be used as a lower resolution stream for monitoring on client or mobile networks with reduced bandwidth capacity. Some cameras only have a primary and secondary profile, some cameras also have a tertiary profile, and other cameras have many additional profiles. The Primary, Secondary, and Tertiary media profiles can be configured using the Camera Configuration Tool.

The Camera Configuration Tool allows you to configure Multicast and Image Settings for your Primary, Secondary, and Tertiary streams for applicable cameras. For more information, see *Setting Tabs* on page 10.

When you navigate to the Multicast or Image Settings tabs, the **Primary** media profile will be selected by default.

1. On the **Multicast** or **Image Settings** tabs, at the bottom-left corner of the window, select the **Secondary** or **Tertiary** to change the page to the settings for that media profile.



2. Make any setting changes needed to the cameras in the selected media profile.
3. At the bottom-right corner of the window, click **Apply** to apply the settings to the media profile selected in step 1.

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 • Enable PTZ: enables and disables PTZ controls in the VMS. This may be useful for non-PTZ cameras which use PTZ commands for zoom control, as an example, and therefore PTZ controls are not required. • PTZ Name: lists any PTZ commands that the camera may use • Enable Metadata: enables and disables metadata stream transmission on all camera media profiles • Export Configuration Template

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 #
Multicast	• Video Multicast IP • Video Multicast Port # • Video Multicast TTL • Audio Multicast IP • Audio Multicast Port # • Audio Multicast TTL • Metadata Multicast IP • Metadata Multicast Port # • Metadata Multicast TTL
TLS	• Download CSR • TLS Certificate Subject • TLS Certificate Issuer • Expiry Date • Certificate Type • Signature Algorithm • Manage Certificates • Certificates • Encryption Mode

Tab	Settings
Image Settings	• Encoding • Flicker Control • Image Stabilization: enables and disables Image Stabilization which will disable other features. Refer to the camera's user guide for more information. • 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
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 • Crowd Detection • Enable ONVIF Analytics Metadata
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 page 1.

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.

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**.

Configuring Multicast Networking

For large networks where several concurrent users may be viewing video from cameras at the same time, it is recommended to use multicast networking to increase the performance over a unicast system. With multicast, high megapixel video can be streamed to a range of designated users on a network with clearer video and faster video delivery than a unicast system. Video, audio and metadata multicast settings can be configured individually for additional flexibility for your network.

Multicast settings can be configured for each of your camera's stream profiles. By default, the Primary stream is selected when you navigate to the Multicast tab. For more information on applying settings on additional stream profiles, see *Secondary Media Profile Settings* on page 8.

To disable a multicast, set its IP to 0.0.0.0 and its port number to 0.

1. Select the **Multicast** tab.
2. For video multicast, configure the following settings:

   Important: For cameras with multiple profiles, each profile's multicast IP and Port settings must be unique. For cameras with multiple heads, each head, and each head's profile's multicast IP and Port settings must be unique.

   - **Video Multicast IP**: Enter the IP address for your video multicast transmission.
   - **Video Multicast Port #**: Enter the port number for your video multicast transmission. Ports must be even numbered.
   - **Video Multicast TTL**: Enter the Time to Leave (TTL) setting for your multicast transmission, from 1 to 255.

     Note: The TTL setting can be used to keep multicast traffic within a certain well-defined part of the network. Every time a router receives a multicast packet, it will decrement the TTL value by 1, and when a router receives a packet with a TTL value of 1, it will drop the packet and not transmit it any further. Therefore, lower multicast TTL settings will confine the multicast traffic to a smaller part of your network. You will need to enforce these limits with your routers.
3. Configure the audio and metadata multicast IP, port and TTL settings, as required.
4. At the bottom-right corner of the window, click **Apply**.

The new multicast settings are implemented on the cameras. The cameras will not start transmitting in multicast until the first client connects to the camera.

Managing Certificates

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

Tip: You can also use the command line to manage certificates and make batch changes to certificates. For more information, see *Command Line Parameters* on page 43.

Note:
Upgrading the camera's firmware does not change the active certificate for the camera.

Performing a factory reset on the camera will clear the custom certificate and switch to the camera's default certificate.

Downloading a Certificate Signing Request

Download a Certificate Signing Request (CSR) for each camera, or multiple cameras. 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 for the camera(s).
3. Click **Apply**.
4. Enter a **Common Name** for the CSRs. Maximum 64 characters, including the Prefix, Suffix, and Source of unique data. A preview is displayed as you enter a value. The Common Name cannot be empty, so you must enter a value for at least one of the Prefix, Suffix, and Source of unique data fields, or any combination of those fields.
    - **Prefix**: Enter a prefix for the Common Name.
    - **Source of unique data**: Select one camera identifier to append to the common name. This is a useful identifier when downloading CSRs for multiple cameras. Options are: None, Counter, Name of the camera, Location of the camera, Hostname of the camera, IP address of the camera, MAC address of the camera, Serial number of the camera, Common Name of the current certificate, or Autogenerated hex number.
    - **Suffix**: Enter a suffix for the Common Name.
5. Enter a **Subject Alternative Name** for the CSRs. A preview is displayed as you enter a value.

- To enter a user specified Subject Alternative Name, select **User input** as the **Source of data** and enter the name in **Value of Subject Alternative Name** field.
- To enter a camera identifier as the Subject Alternative Name, select one of the following options from the **Source of data** drop-down list: A copy of the Common Name, Hostname of the camera, IP address of the camera, or First Subject Alternative Name of the current certificate.

6. 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.

   > **Note:** The **Country** field is not optional for Pelco cameras and must be filled in.

7. 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 the certificates to upload into the Camera Configuration Tool.

> **Note:**
> - Signed certificate files that you add to the zip file must have specific file extensions such as *.crt*, *.cer*, or *.pem*.
> - To see which cameras have trusted certificates in the Camera Configuration Tool, you will also need to add the CA certificate file to the same zip file as the signed certificate(s).

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 a camera connected with the Camera Configuration Tool.

Note:

- You cannot delete a certificate that is Currently Active. Apply a different certificate, and then delete the unused certificate.
- You cannot delete the factory default self-signed certificate.
- You cannot delete a certificate when you are editing other settings in the Camera Configuration Tool. Apply or Discard your changes before deleting a 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.

Setting the Encryption Mode

For greater network communication security, you can enable compliance with the Federal Information Processing Standard (FIPS) 140-2 Level 1 or Level 3 Security Requirements for Cryptographic Modules for server and camera communication.

Note:

- FIPS 140-2 Level 1 requires the purchase of a FIPS camera license.
- FIPS 140-2 Level 3 requires the purchase of a CRYPTR micro card. The CRYPTR card must be inserted into the camera's SD card slot before it can be enabled.

1. Select the **TLS** tab.
2. In the **Encryption Mode** column, use the drop-down list for each camera to select the type of encryption to use:
   - **OpenSSL** is the default option for encryption.
   - **FIPS 140-2 Level 1** enables FIPS 140-2 level 1 encryption.
   - **NXP TPM** enables the onboard trusted platform module (TPM) to securely store your encryption keys. Only cameras that come with the onboard NXP TPM will display this option.
   - **CRYPTR FIPS 140-2 Level 3** enables the installed CRYPTR card to securely store your encryption keys.

     Important: Switching the setting to CRYPTR FIPS 140-2 Level 3 or NXP TPM will cause the camera to generate a new key and self-signed certificate. Some certificate and key management may be required when you enable this setting. If your previous keys were signed by a certificate authority (CA), the newly generated keys will also need to be signed by the CA to keep the connection to your camera secure.
     For more information, see *Downloading a Certificate Signing Request* on page 16 and *Uploading Signed Certificates* on page 17.
3. At the bottom-right corner of the window, click **Apply**.

   Important: Changing this setting on your camera will require your camera to reboot and you will lose the video stream for that time. Avigilon recommends that you apply this setting during non-critical operating times. Applying this setting on a single camera can take from 1 to 5 minutes.

The new encryption mode settings are implemented on the cameras.

Note: If the CRYPTR micro card is ejected or becomes unusable while it is inserted in the camera and enabled, the camera will restart in FIPS 140-2 Level 1 mode. If the card is re-inserted into the camera, CRYPTR FIPS 140-2 Level 3 will need to be re-selected as the Encryption Mode to continue using the CryptR micro card to store your keys.

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**.

Changing Camera Mode

On the Image Settings page, use the Camera Mode option to change camera mode. To configure the same setting for multiple cameras, click .

1. Select one of the following modes from the drop-down list:
    - Full Feature — this is the standard operating mode. Offers the full functionality of the camera.
    - High Frame Rate — this mode will use the maximum image rate possible but will disable certain features. Refer to the camera's user guide for more information.
    - Dynamic Privacy Masks — this mode will enable you to create dynamic privacy masks but will disable certain features. Refer to the camera's user guide for more information.
    - No Video Analytics — this mode will disable video analytics.
2. Click **Apply**.

Note: Changing camera mode can take several minutes during which time the camera will reboot.

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 Close-up** — only detects people and is optimized to detect people that come near to the camera and may be only partially in the frame. This mode will disable the Object crosses beam and Direction violated analytic events for this camera. The Indoor Close-up mode is currently only available on modular cameras. • **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.
Enable Tamper	Select the checkbox to enable tamper detection. Tampering is a sudden change in the camera field of view, usually caused by someone unexpectedly moving the camera. Enabling this setting will cause the camera to trigger alarms in the event of possible human interference.
Tamper Sensitivity	Enter a value between 1-10 to select how sensitive a camera is to tampering events. 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.

Column	Description
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.
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. Object types include the following vehicle subclasses: bicycle, car, motorcycle, bus, large truck, pickup truck, and van. • **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.
Enable ONVIF Analytics Metadata	When enabled, the camera will send ONVIF Profile M compliant analytics metadata to the VMS. **Note:** CCT supports display of bounding boxes and confidence levels around objects when Profile M is enabled.

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.
      a. Click the check-boxes next to the vehicle subtypes to deselect them.
   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 **Add Event**.
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 page 31.
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 **Edit**.
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 **Delete**.

Setting Up a Radiometric Analytics Event

Use the Thermal analytic event settings to configure Temperature Threshold or Temperature Change events with a supported thermal radiometric camera.

These types of events are only supported by thermal cameras with radiometric capabilities.

1. Select the **Analytics** tab.
2. In the Analytic Events column, click **Configure**.
3. Click **Add Event**.
4. Enter a name for the event in the **Name:** field. Confirm that the **Enabled** checkbox is checked.
5. Select the **Thermal** tab to configure thermal event settings.
6. If necessary, you can adjust the **Emissivity** setting for the thermal camera.

   > **Tip:** The emissivity of a material or surface is its effectiveness in emitting thermal energy. Changing this setting will apply an offset based on different material's efficiency in radiating heat energy. You may want to adjust this setting if your thermal camera is viewing a large object or surface that has a different emissivity than the default value. Check the tooltip beside this setting for some recommended Emissivity settings for different common materials. This is a global setting and will apply to the thermal camera as a whole.

7. In the **Activity:** area, select the type of temperature event to configure.
   - **Temperature Threshold**: Select a temperature threshold activity when you want an event to be triggered when the camera detects a temperature in the defined measurement area that reaches or passes a defined temperature threshold. Configure the following temperature threshold settings:
     a. In the **Temperature** area, select if the set temperature threshold will trigger when the measured temperature goes above, below, or matches the set temperature.
     b. Set the temperature that will trigger the temperature threshold event. Use the drop-down menu to set it as either a Celsius or Fahrenheit temperature.
     c. Set the minimum time that the temperature threshold triggering condition needs to persist before generating an alarm in the **Minimum duration:** field. The duration can be set from 1-1800 seconds.
   - **Temperature Change**: Select a temperature change activity when you want an event to be triggered when the camera detects that a temperature in the defined measurement area has changed by a defined amount. Configure the following temperature change settings:
     a. In the **Temperature** area, select if the event should detect an increased or decreased type of temperature change by selecting either the **Increases by** or **Decreases by** option.
     b. Set the amount that the temperature must change to trigger the event. Use the drop-down menu to set it as either a Celsius or Fahrenheit temperature.
     c. Set the time within which the temperature change needs to occur in order to trigger the event in the **Duration** field.
     d. Enable the **Starting Value** field if you want to set a starting temperature for the temperature change event. Temperature change events will not be triggered if the temperature change event conditions are met above or below this defined threshold. Enter the starting temperature value in the **Starting Value** field.

> **Tip:** For example, if you have a Starting Temperature: of **20°C** and are configuring a *Decreases by* temperature change event set at **15°C**, the temperature must decrease to 5°C to trigger the event. Any other decreases by 15°C, such as from 25°C to 10°C will not trigger the event.

8. In the **Measurement Mode:** area, select how you want to measure the temperature in the image.
   - **Spot Detection**: Select spot detection to detect temperature changes in a specific spot or pixel in the video frame. Click and drag the green cross marker so that it is selecting the part of the video image where you want to detect temperature changes. The selected spot should not be set at the edge of the field of view. Temperature measurements at the edge of the field of view may not be as accurate.
   - **Box Detection**: Select box detection to detect the temperature changes in a region of interest (ROI).
     a. Define the ROI where temperature changes will be detected. Thermal event ROIs should not be created at the edge of the field of view. Temperature measurements at the edge of the field of view may not be as accurate.
        - Click and drag the yellow points on the corner to reshape the green overlay.
        - Click and drag to move the green overlay.
        - Click to restore the default green overlay.
     b. In addition to setting the ROI, you can select how the temperature will be measured inside the ROI and tigger the event from the following options:
        - **Average temperature in ROI**: The camera calculates the average temperature inside the ROI and compares it to the event settings.
        - **Maximum temperature in ROI**: The camera takes the highest measured temperature inside the ROI and compares it to the event settings.
        - **Minimum temperature in ROI**: The camera takes the lowest measured temperature inside the ROI and compares it to the event settings.
9. Set the **Timeout:** value. This is 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.
10. If necessary, click the **Advanced Settings** button to configure the advanced settings for this event. Most standard thermal events can be configured using the default advanced settings, but they can be adjusted if necessary. For more information, see *Advanced Thermal Event Settings* below.
11. Click **OK** to save your settings.

Advanced Thermal Event Settings

The following advanced thermal event settings can be configured on the Advanced Settings page. These settings will be different depending on the type of thermal event you are configuring.

Temperature Threshold Advanced Settings

- **Sensitivity:** Define the sensitivity of the temperature threshold detection. Sensitivity correlates with the confidence of the rule condition being met. 1 requires the highest confidence and has higher chances of false negative events. 10 requires the lowest confidence and has higher chances of false positive events.
- **Significant temperature change:** Set if a new event will be triggered on top of an already triggered event condition if the temperature changes by the specified percentage. Enter a value between 0.0 (0%) and 1.0 (100%). Set 0 if you don't want any new events to be triggered.
- **Absolute significant temperature change:** Set if a new event will be triggered on top of an already triggered event condition if the temperature changes by the specified value. Enter a value between 1°C and 50°C. Set 0 if you don't want any new events to be triggered.
- **Significant pixel count change:** Set if a new event will be triggered on top of an already triggered event condition if the number of pixels meeting the event condition change by the specified percentage. Enter a value between 0.0 (0%) and 1.0 (100%). Set 0 if you don't want any new events to be triggered.
- **Absolute significant pixel change:** Set if a new event will be triggered on top of an already triggered event condition if the number of pixels meeting the event condition change by the specified value. Enter a value between 1 and 200 pixels. Set 0 if you don't want any new events to be triggered.
- **Maximum time to ignore:** Set the amount of time that the event condition must not persist before the triggered event is terminated. Enter a value between 0 and 1800 seconds. This value must be shorter than the Timeout: value.
- **Minimum throttle update:** Set the minimum time that must elapse since the last trigger before a new event can be triggered. Enter a value between 0 and 10 minutes. Enter 0 to not throttle any new events being triggered.
- **Hysteresis:** Define the offset temperature above/below the set temperature threshold that needs to be crossed in order to terminate the event. Enter a value between 1°C and 50°C.
- **Match Range:** Set a ± range value that will be added to the set temperature for matching-type temperature events. This expands the temperature range for matching events. For example, if you set the temperature as 5°C and have a Match Range of 3°C, the event can be triggered anywhere within the range of 2°C to 8°C. Enter a value between 1°C and 50°C.

Temperature Change Advanced Settings

- **Sensitivity:** Define the sensitivity of the temperature change detection. Sensitivity correlates with the confidence of the rule condition being met. 1 requires the highest confidence and has higher chances of false negative events. 10 requires the lowest confidence and has higher chances of false positive events.
- **Maximum time to ignore:** Set the amount of time that the event condition must not persist before the triggered event is terminated. Enter a value between 0 and 1800 seconds. This value must be shorter than the Timeout: value.
- **Minimum throttle update:** Set the minimum time that must elapse since the last trigger before a new event can be triggered. Enter a value between 0 and 10 minutes. Enter 0 to not throttle any new

events being triggered.

- **Hysteresis:** Define the offset temperature above/below the set temperature threshold that needs to be crossed in order to terminate the event. Enter a value between 1°C and 50°C.

Configure a Radiometric Detection Area

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 page 26.

> **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.
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.

Activity:	Description
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.
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.
Auto-track objects in area	The event is triggered when the selected object type moves into the region of interest causing the camera to automatically reposition to track the object. Returning to preset position once object is lost.

Configuring Crowd Detection

Use the Crowd Detection rules to configure crowd detection. This allows you to define when the system detects a crowd in the scene.

1. Select the **Analytics** tab.
2. In the Crowd Detection column, click **Configure**.
3. Select the Crowd Detection rule you want to edit:
    - Unusual crowd growth — This event is triggered when a crowd size grows unexpectedly.
    - Crowd size — This event is triggered when the number of people is exceeded over a configurable duration.
    - Unusual crowd size — This event is triggered when an unusual crowd size is detected.

4. Define the **Inclusion Area** where crowds are detected.
    - 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 restart the stream if a stream error occurs.
    - Click to reset to the default inclusion area.
5. In the Settings panel, select the **Enabled** checkbox to enable the Crowd Detection rule.
6. Define the requirements necessary for the Crowd Detection rule to trigger an event.
    a. Number of people — the minimum number of people required to be detected in the defined zone to trigger an event.
    b. Threshold Time — the amount of time that the defined number of people will need to remain in the defined zone before it will trigger an event.
    c. Timeout — the amount of time beyond which the event is terminated.
    d. Sensitivity — sensitivity correlates with confidence of the rule condition being met. 1 requires highest confidence (higher chances of false negatives) and 10 requires lowest confidence (higher changes of false positives). At current sensitivity level, objects with confidence level 50% and above will trigger events.
7. Click **Apply** to save your settings without closing the Crowd Detection window.
8. Click **OK** to save your settings and exit the Crowd Detection window.

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.

Critical Firmware Updates

Important: Sometimes a critical firmware update is required to keep the camera running. We

recommend that you apply these critical updates as soon as possible. These updates can take longer than usual and should be done at a convenient time for your facility to have missing video from that camera.

If the Camera Configuration Tool detects a critical update needs to be performed, a message about the update will appear at the bottom of the screen.

Note: If you have made any settings changes, make sure to Apply them before starting the critical update process. Unsaved changes will be discarded during the update.

1. Click the **Update cameras** button on the message to generate a list of all the cameras that require the update and have the required update selected.
2. Click **Apply** to perform the update.
3. A message appears to warn that the updates will take longer than usual. Click **OK** to proceed.

Alternatively you can go to the Firmware Update tab to perform the update. For more information, see *Applying Firmware* on the previous page.

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.

> **Tip:** You can also use the command line to import or export settings for devices connected to the Camera Configuration Tool. For more information, see *Command Line Parameters* on page 43.

Exporting Settings

You can export camera settings to edit and re-import to apply the settings to the camera list. 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. Select the option to export the file either with or without analytic settings:
   - **Export with analytics**: Exporting the camera settings with analytics will require two or more rows of settings per camera in the exported .csv file.
   - **Export without analytics**: Exporting the camera settings without analytics will limit each camera to one row in the .csv file.
4. 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.

Configuration Templates

Configuration templates are files that capture a set of predefined settings from one camera. These templates can be used to replicate the same settings across multiple cameras, simplifying the configuration process. Settings that are not listed in the configuration template will need to be applied through alternative methods.

Configuration Templates support the following settings:

- SmartCompression Enable
- SmartCompression Min Image Rage
- SmartCompression Idle Keyframe Interval
- SmartCompression Bandwidth Reduction
- SmartCompression Background Quality
- SmartCompression Post Motion Delay
- SmartCompression Quality
- SmartCompression Max Bitrate
- SmartCompression Enable Idle Scene Mode
- DST/Timezone
- Day/Night Mode / Threshold
- Backlight Compensation Enabled
- Backlight Compensation Level
- Digital Defog Enable
- Digital Defog Level
- Color Mode
- Saturation
- Sharpness
- Brightness
- Contrast
- WhiteBalance mode
- WB-Red
- WB-Blue
- IPV6 enable
- WS-discovery Enable/disable
- Preset Speed Limit
- Pan/Tilt Speed Limit
- Digital Zoom Enabled

Use Configuration Templates to Bulk Apply Settings

You can export a configuration template that lists the camera settings as they were configured in the camera. Then, you can import the configuration template and apply it to multiple cameras at once.

Export a Configuration Template

Note: Make sure you configure the camera's settings in the Web UI to the desired values before exporting the configuration template.

1. Navigate to the *General* page.
2. Click **Export** in the *Export Configuration Template* column.
3. Save the .json file to your local machine.
4. Review the *Configuration Status* information in the pop-up window. Any errors will be listed in the *Error summary* section.
5. Click **OK**.
6. You can open the configuration template as a .json file in any text editor to review the configured settings.

Remove Settings from a Configuration Template (Optional)

You can remove a section of text that you do not want applied to other cameras during the update. The settings listed in the configuration template will overwrite the configured settings on the cameras being updated. Removing the settings does not remove the settings on the cameras; it prevents them from being overwritten during the update.

Important: We do not recommend using the configuration template to edit individual settings. Instead, use the configuration template to delete sections of text that you do not want bulk applied to other cameras.

Follow these steps to remove settings from the configuration template:

1. Open the configuration template .json file in a text editor.
2. Review and omit the settings you do want affected by the update.
3. Save the updated file.

Example 1

You can remove a group of settings by deleting them from the configuration template. For example, you can remove the Color Mode settings by deleting the following section of text:

```
"ColorMode": {
      "Preset": "Avigilon",
      "Brightness": 50,
      "Saturation": 40,
      "Contrast": 50,
      "Sharpness": 50
}
```

Example 2

Alternatively, you may need to delete a section of text to remove a single setting. For example, you can remove the *Network* section by deleting the following section of text:

```
"Network": [
   {
      "Identifier": {
      "Name": "eth0"
      },
      "IPv6": {
      "Enabled": false
      }
   }
]
```

Import and Apply a Configuration Template

You can import the configuration template as a .json file and apply it to other cameras. A configuration template can only be applied to cameras of the same model at this time.

Note: Make sure you open the configuration template and review the settings in the .json file before bulk applying it to cameras. The settings listed in the configuration template will overwrite the configured settings on the cameras being updated. See *Remove Settings from a Configuration Template (Optional)* on the previous page for more information.

1. Filter the list of cameras to show only the cameras you want to apply the configuration template to. See *Filtering and Sorting Cameras* on page 6 for instructions.
2. Click the ☰ icon in CCT.
3. Click **Import Configuration Template**.
4. Locate the .json file and select it.
5. Review the *Import Device Settings* information:
   - Selected File: the name and location of the .json file that was uploaded from your local machine.
   - Applicable Model: the camera model that the configuration template can be applied to.
   - Number of applicable devices: lists the device name, model number and IP address of the device that will be updated.
6. Click **Continue** and then click **Apply**.

7. Review the *Import Configuration Template* information:
    - Successfully applied devices: lists the device name, model number and IP address of the device that were successfully updated.
    - Failed devices: lists the device name, model number and IP address of the device that were not successfully updated
8. Click the **OK** button in the Report area to generate a report.
9. Review the *Configuration Status* information to see which settings were successfully applied. The ❌ icon indicates an error.
10. Select the triangle icons to show additional settings. You must select the setting to see the *Error Summary* details.
11. Click **OK**.
12. Click **Download successful IPs** to save a list of the cameras IP addresses that were updated. The list is saved as a .txt file.
13. Click **Download failed IPs list** to save a list of the camera IP addresses that could not be updated. The list is saved as a .txt file.
14. Click **Close**.

Using the CCT Command Line

Using the CCT command line makes it possible to perform actions through the command line, and to make batch changes for sites that have a large number of cameras. These batch jobs can import or export settings, or to manage the certificates on your cameras.

Note: It is recommended to only use the command line to perform these functions if you are already familiar with using the command line.

Starting the CCT Command Line

Before you can make batch changes with the command line, you will need to launch it and navigate to the correct file.

1. Open the command line on your computer. Type `CMD` in the search bar at the bottom of your screen and launch the command prompt app.
2. Navigate to your Camera Configuration Tool folder. To go to the default location, type `c:\Program Files (x86)\Motorola Solutions\Camera Configuration Tool` and press **Enter**.
3. Once you are in the correct folder, type `CCT-Batch.exe` and press **Enter**.

   The CCT Batch Job help information will display. This help information will summarize all of the commands and actions that you are able to do as well as some examples on how to enter the commands. The exit codes are also provided so you can get feedback on whether an action was successful.

   Tip: Be sure to use the examples in the CCT Batch Job help information as a guideline for entering your commands.

Command Line Parameters

The following parameters are provided here as reference, and are also listed in the CCT Batch Job help information.

Command	Function	Description

-a
`--addIP <IP Address>`
`--addIP <start IP>-<end IP>`
	Identify a camera by IP address, or by range of IP addresses, to direct the following commands to.	Use this command to identify and connect with a single camera by IP address or a number of cameras by using a range of IP addresses. For example:
		`-a 192.168.1.1-192.168.1.120`
		Spaces are not permitted in the IP range portion. The identified cameras will be the cameras that the following import, export or certificate commands will be sent to.
		This is used with the **-u**, **-p**, **-t**, and **-s** commands to enter the camera information needed to connect to the camera(s).

-u `--user <user name>`	Enter the user name of the camera(s) you are sending a command to.	Use this command with the **-a** command to enter the camera's user name.
-p `--password <password>`	Enter the password for the camera(s) you are sending a command to.	Use this command with the **-a** command to enter the camera's password.
-t `--httpPort <port number>`	Enter the HTTP port number needed to connect to the camera(s).	Use this command with the **-a** command to specify the HTTP port to use to connect to the camera(s). This parameter is optional. If skipped, CCT Batch will use the default port 80.
-s `--httpsPort <port number>`	Enter the HTTPS port number needed to connect to the camera(s).	Use this command with the **-a** command to specify the HTTPS port to use to connect to the camera(s). This parameter is optional. If skipped, CCT Batch will use the default port 443.

Command	Function	Description
-f `--forceActionExecute`	Forces the entered command to execute regardless of issues.	Use this command with any of the other commands to force the command to execute. This will force commands to be executed on any devices that can establish a connection, and any devices that are offline, in a pending state or unreachable will be skipped. **Tip:** If you are sending a command without the force option and one of the cameras can't be reached, the command will be aborted.
-e `--export "<file.csv>"`	Exports settings from the selected camera(s) as a .csv file.	Apply this command export the settings of all the cameras connected through the **-a** command into a .csv file. Enter the name and location of the .csv file after the command.
-i `--import "<file.csv>"`	Import settings to the selected camera(s) from a .csv file.	Apply this command to import settings in a .csv file to all of the cameras connected through the **-a** command. Enter the name and location of the .csv file after the command.
-d `--downloadCsr "<subject and SAN>" "<file.zip or file.csr>"`	Download a certificate signing request (CSR) for the selected camera(s).	Use this command to download a CSR in PEM format to a .zip or .csr file type for the camera(s) connected through the **-a** command. After the **-d** command, add the CSR subject and SAN (subject alternative name) to use, and the file name and type to download the CSR as. **Tip:** More information about the **-d** command and its parameters, including all options and examples, can be found by entering `CCT-Batch.exe --csrHelp`.

Command	Function	Description
-c `--uploadCrt "<file.zip or file.crt>"`	Upload a certificate and make it the active certificate on the selected camera(s). This can be used in conjunction with the remove command to remove unwanted certificates.	Use this command to upload a signed certificate, in a .zip or .csr file type, and make this certificate the active certificate on the camera(s) connected through the **-a** command. After the **-c** command, enter the path and name of the certificate to be uploaded. **Tip:** You can also remove the *old* certificate you are replacing, or *all* of the unused certificates as part of the upload command by adding **-r OLD**, or **-r ALL** after the upload command.

-r
`--removeCrt <certificate ID>`
`--removeCrt <certificate ID>;<certificate ID>`
	Remove specific certificates from your selected camera(s).	Use this command to remove unwanted certificates from the camera(s) connected through the **-a** command. After the **-r** command, enter the certificate ID of the certificate to remove. If removing multiple certificates, put a semicolon in between the multiple certificate IDs. Certificate IDs are not connected with the certificate subject or serial number. Retrieve certificate IDs by using the **-l** command.
		Tip: If used in conjunction with the upload command, **-c**, you can remove the *old* certificate that is being replaced, or *all* of the unused certificates at the same time as uploading the certificate by adding **-r OLD**, or **-r ALL** after the upload command.

-l `--listCrt`	List the certificates and certificate information for the selected camera(s).	Use this command to list the certificates of the camera(s) connected through the **-a** command. This will generate a list of the certificate ID, expiration date and certificate common name of all the certificates for those cameras. The active certificate will be prefixed by an exclamation mark and highlighted in green, expired certificates are highlighted in red, and self-signed or untrusted certificates are grey.

Tips for Using the Command Line

Keep the following tips in mind when using the command line to execute CCT Batch commands:

- An exit code of **0** means that the command ran successfully. All of the other exit codes are listed in the CCT Batch help information.

  > **Tip:** You can retrieve the exit code from the system of the last batch job that was completed:
  > — CMD.exe: Enter variable **%errorlevel%**. For example: `echo %errorlevel%`.
  > — PowerShell: Enter variable $LastExitCode. For example: `echo $LastExitCode`.

- It can take a few minutes for the CCT Batch to search for cameras after entering a command.
- If one of the cameras you are connecting to is not in a state that it can be logged into, this will stop the batch job process unless the **-f** force command is used.
- If the password is empty, use double-quotes instead (**""**). If you are using PowerShell, you cannot use an empty password.
- If there is a space in the password, put double-quotes on each side of the space (**" "**). This will not work in PowerShell.

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.