



Camera Configuration Tool 3.0.0

User Guide

© 2026, Motorola Solutions Inc. All rights reserved. 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. Unless stated explicitly and in writing, no license is granted with respect to any copyright, industrial design, trademark, patent or other intellectual property rights of Motorola Solutions Inc or its licensors.

This document has been compiled and published using product descriptions and specifications available at the time of publication. The contents of this document and the specifications of the products discussed herein are subject to change without notice. Motorola Solutions Inc reserves the right to make any such changes without notice. Neither Motorola Solutions Inc nor any of its affiliated companies: (1) guarantees the completeness or accuracy of the information contained in this document; or (2) is responsible for your use of, or reliance on, the information. Motorola Solutions Inc shall not be responsible for any losses or damages (including consequential damages) caused by reliance on the information presented herein.

Motorola Solutions Inc
motorolasolutions.com

PDF-CCT-GUIDE
Revision: 1 – EN
20261001

Contents

Camera Configuration Tool (CCT) User Guide	6
Initial Setup	7
Requirements	7
Downloading and Installing CCT	7
Logging in for the First Time	8
Navigating CCT	9
Devices	10
Finding Devices	10
Discovering Devices	10
Adding Devices by IP	10
Cloud Claiming	11
Filtering and Sorting Devices	12
Showing or Hiding Columns	12
Viewing Devices in Grid View	13
Accessing Grid View	13
Grid View Features	14
Switching Back to List View	14
Removing Devices	14
Removing Individual Devices	14
Removing Multiple Devices	14
What Happens When You Remove a Device	15
Re-adding Removed Devices	15
Moving Devices to Another Project	15
Monitoring Task Status	15
Accessing Task Status	15
Task Status Panel	16
Understanding Task Statuses	16
Task Details	16
Managing Active Tasks	16
Common Task Types	16
Configuration	18
General Settings	18
Editing the Device's Name and Location	18
Changing Device Mode	18
Setting the Device's Timezone	19
Network Settings	20

Turning off DHCP	20
Changing the IP Address, Subnet Mask and Default Gateway	20
Changing the Device's Hostname	20
Changing the NTP Server Mode and Information	20
Turning Off Automatic DNS Assignment from DHCP	21
Configuring Control Ports: HTTP, HTTP Port and HTTPS	21
Image Settings	22
Configuring Image Quality	22
Setting Day/Night Mode	23
Turning on Backlight Compensation	23
Turning on Digital Defog	23
Configuring Color Mode	24
Configuring White Balance	24
PTZ Settings	25
Setting Pan, Tilt and Speed Limits	25
Turning on Digital Zoom	25
User Management	26
Managing Users	28
Security Groups	28
Analytics	29
Updating Connection Credentials	29
Updating Credentials for Multiple Devices	29
Credential Update Process	30
Updating Credentials for Offline Devices	30
Handling Credential Update Failures	30
Templates	31
Template Best Practices	31
Exporting Device Templates	31
Importing Device Templates	32
Applying Templates to Selected Devices	32
Firmware Management	33
Best Practices for Firmware Updates	33
Important Notices	33
Troubleshooting Update Failures	33
Certificates	34
Viewing Device Certificates	34
Uploading Certificates to a Device	34
Generating CSR Certificates	34

Uploading Certificates to CCT	35
Projects	36
Accessing Projects	36
Creating and Managing Projects	36
Creating a New Project	36
Selecting an Existing Project	37
Multi-Project Login Workflow	37
Project Settings	37
Editing the Project Name	37
Changing the Password	37
Deleting Projects	38
Selecting a Different Project	38
Generating Project Reports	39
Generating a Report	39
Report Layout	39
Settings	41
System Settings	41
Allowing Self-Signed Certificates	41
Allowing Fallback to HTTP	41
Creating a Firewall Rule for Device Discovery	41
Sharing Anonymous Data	41
Client Settings	42
Accessing Client Settings	42
General Settings	42
Language	42
Theme	42
Display and Performance	42
Grid View Options	42
Advanced Options	42
Diagnostics	42
Applying Settings	43
Settings Storage	43
More Information & Support	44

Camera Configuration Tool (CCT) User Guide

CCT 3.0.0

The Camera Configuration Tool (CCT) is important for device setup and management. You can use CCT for new device installations or to change settings on existing devices. CCT is the only tool that lets you manage many devices at once.

CCT provides one place to find, claim, and set up devices on the network. This tool saves time by managing devices in a large group. You can change one device's settings using its web interface or the Avigilon Unity Video client. CCT lets you change settings for many devices at the same time.

You can configure the following settings using CCT 3.0.0:

- **Initial Setup:** Create your account, set up projects, and discover devices on your network. Configure login credentials and organize devices by location or deployment.
- **Add and Manage Devices:** Discover devices automatically or add them manually by IP address. Remove devices, move them between projects, and monitor connection status in real-time.
- **Firmware Management:** Upload and apply new software (firmware) to groups of devices. Monitor update progress and verify firmware versions across your deployment.
- **Configure Devices:** Apply settings to individual devices or groups including network configuration, image settings, video profiles, analytics, PTZ, user management, and certificates.
- **Templates:** Save device configurations as templates and apply them to multiple devices. Export and import templates to standardize settings across deployments.
- **Certificates:** Install and manage security certificates for HTTPS connections. Upload certificates to devices, view certificate status, and configure certificate validation policies for secure communication.
- **Manage Projects:** Switch between the various projects you have access to. Create new projects, modify project settings, and generate comprehensive project reports.
- **Edit System Settings:** Modify CCT system settings. Customize the interface theme, language, and security preferences.

For more resources, visit support.avigilon.com or support.pelco.com, e.g., official software and firmware downloads.

Initial Setup

The following topics cover the initial set up of CCT3. Ensure you review [Requirements below](#) first.

Requirements

Before installing CCT 3.0.0, ensure your computer meets the following requirements:

Component	Minimum Requirement
Operating System	Windows 10 version 1607 (build 14393)
Processor	Intel Core i5 or equivalent
RAM	8 GB
Hard Drive Space	500 MB available space
Network	Ethernet connection required
Display	1920x1080 resolution or higher recommended

Downloading and Installing CCT

To begin using CCT 3.0.0, you must first install it on your computer. The computer running CCT must be on the same network as the devices you want to set up. This is so CCT can find and set up the devices.

Before you start, make sure your computer meets the hardware and system needs for CCT. You must also have a valid login for the Avigilon or Pelco Partner Portal.

1. Go to the Avigilon or Pelco Software Downloads website: avigilon.com/software-downloads or pelco.com/updates. You must log in to the Avigilon or Pelco Partner Portal before you can access the software files.
2. Find the Camera Configuration Tool.
3. Click the **Download** link for the newest version. The installer file will download.
4. Find the installer file in your downloads folder and double-click it.
5. Follow the steps in the Installation Wizard. Agree to the license.
6. Click **Install**.
7. Click **Finish** when done.

CCT is now installed.

Logging in for the First Time

You will need to log into CCT3 when you launch the program.

1. Start CCT3.0.
2. Share anonymous diagnostic data:
 - a. Click **Allow** to share anonymous diagnostic data. This helps identify performance bottlenecks and optimize application stability. Data collection is strictly limited to functional metadata and excludes Personally Identifiable Information (PII). You can change your preferences later.
3. Set a password:
 - a. Enter a password to set a password.
 - b. Reenter the password to confirm.
 - c. Click **Proceed**.
4. Save the recovery key:
 - a. Click the Copy icon to copy the recovery key and save it in a safe place. You will need to enter the recovery key if you forget your password.
 - b. Click **Continue**.
5. Create new project:
 - a. Enter a name for the project.
 - b. Click **Create**.
6. Select project:
 - a. Click the project from the list to select it or click **Create project** to create a new one.
 - b. Click **Open**.

You are now logged into CCT3.

Navigating CCT

After you log into CCT, you will be directed to the main page. In the image below, you can become oriented with the main components in CCT3.

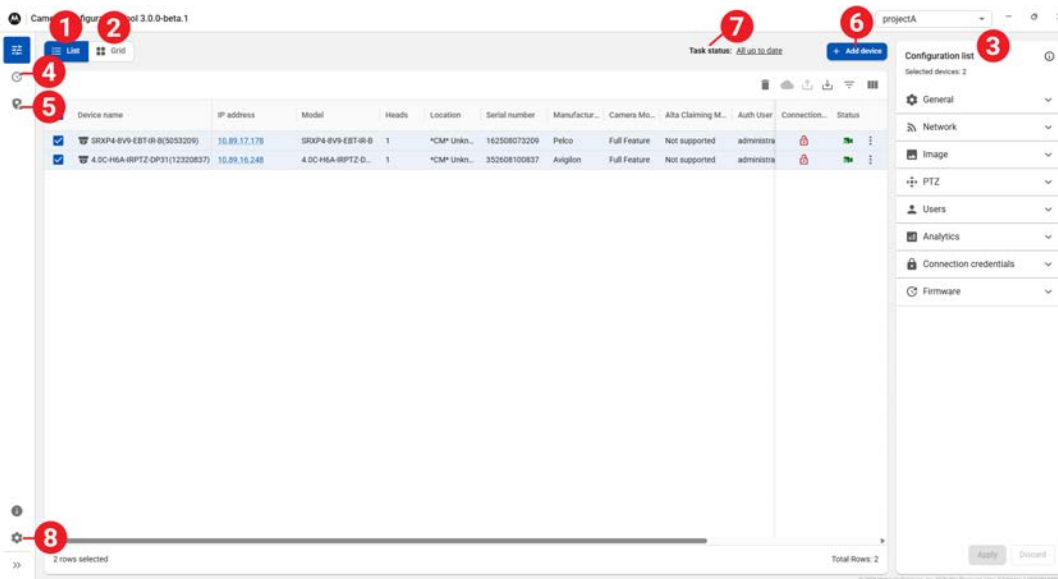


Figure 1: The CCT 3.0 interface.

1. **List:** The list shows which devices and devices are connected to CCT.
2. **Grid:** The grid view shows a snapshot of the live view. Snapshots are refreshed periodically. The snapshot is not meant to be a live stream; it just shows where the device is pointed for reference.
3. **Configuration list:** The configuration area for editing device settings. You must select at least one device to open the Configuration list.
4. **Firmware:** Manage device and device firmware. The Firmware page also allows you to filter the device list and upgrade select groups of devices and devices at once.
5. **Certificates:** Add and manage security certificates.
6. **Add device:** Adds devices and devices by the IP address. You will need the login credentials.
7. **Task status:** Lists the device and device configuration updates, e.g., firmware updates.
8. **Client settings:** Change the UI language or theme.

Devices

The following topics cover how to manage devices in CCT.

Finding Devices

You can discover devices or manually add them to the tool for configuration.



TIP

New devices may not be displayed if the Devices list is filtered.

Discovering Devices

CCT will discover devices on the network automatically. Follow these steps to add the devices:

1. In the top-right corner, select **Add Devices**.
CCT will begin scanning the network. Discovered devices will start appearing in the list.
2. Use the checkboxes to select which devices you want to add.
3. Click **Next**.
4. Enter the User Name and Password for the devices.
5. Click **Add**.

The devices should be added to the Devices List on the main page.

Adding Devices by IP

You can add devices manually if CCT does not discover them automatically.

1. In the top-right corner, select **Add Devices** then click **Add Devices by IP** in the pop-up window.
2. To find one device, enter the IP address of the device in the **Start IP Address** field. Leave the **End IP Address (Optional)** field empty.
3. To find multiple devices, 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. Click **Next**.
5. Enter the User Name and Password for the devices.
6. Update the HTTP Port # and HTTPS Port # if needed.
7. Click **Add**.

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 devices may not be displayed if the Device list is filtered.

Cloud Claiming

Cloud claiming changes the existing on-prem devices to cloud-connected devices. You can enable cloud claiming mode to be able to claim cloud-capable devices in Alta cloud.

1. Click the **Cloud** icon at the upper-right corner of the device list.
2. Alternatively, you can click the  icon next to the device and select **Convert to cloud claiming mode**. Cloud claiming will export keys required for claiming.

**IMPORTANT**

Keys will be exported automatically once the selected device(s) are ready to be claimed. Store them securely, as they are required for claiming the device(s) in the cloud.

3. Click **Apply**.
4. CCT will enable cloud claiming mode on cloud-capable devices.
5. Claim the devices in Alta cloud using the saved CSV file.

CCT will begin claiming the cloud-connected devices on the network.

**NOTE**

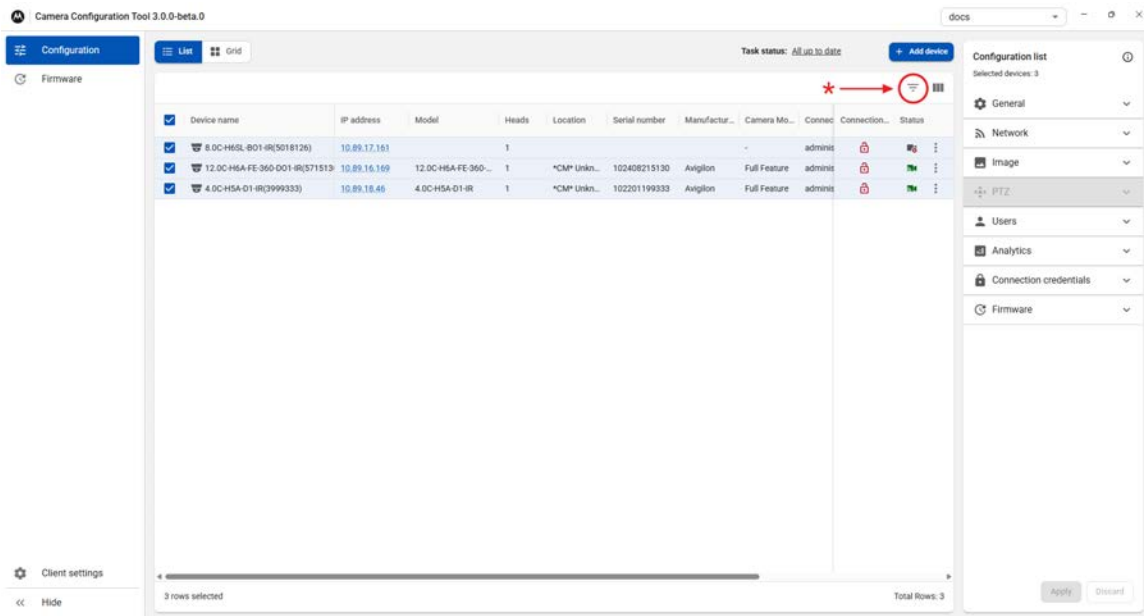
CCT does not support cloud device configuration.

Filtering and Sorting Devices

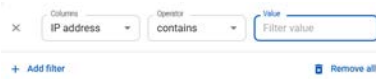
Depending on the size of your site, you may need to edit over 100 devices. To help you focus on the devices that need your attention, you can filter or sort the listed devices.

Follow these steps to filter and sort the Devices List:

1. On the main page, select the **Filter** icon in the top-right corner.



2. Use the **Columns** drop-down menu to select an attribute to filter by.



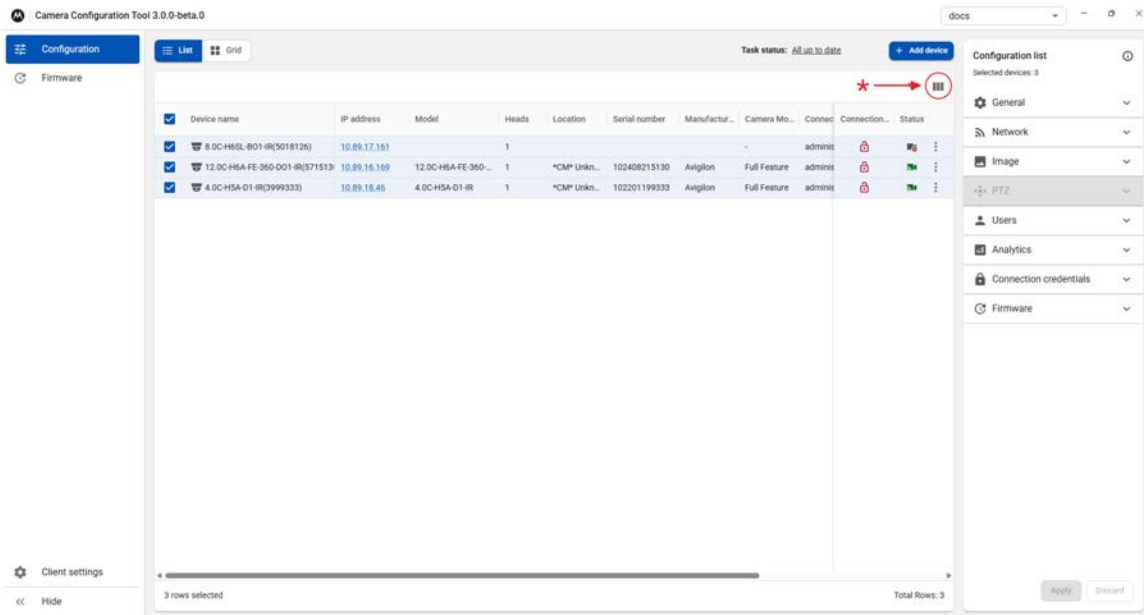
3. Use the **Operator** drop-down menu to determine how the list is filtered.
4. Use the **Value** field to refine the list using text.
5. Use the **Add filter** button to add filters to your search.
6. The list will only show devices that match your text.
7. Click the top checkbox to select all devices now shown.

You can now use the Configuration list on the right side to set up the group.

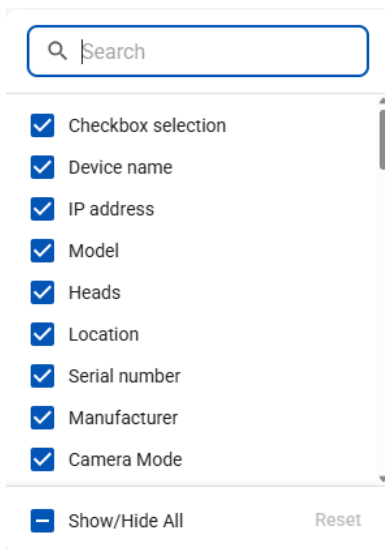
Showing or Hiding Columns

If you want to show or hide columns in the Devices List, use the column option in the top-right corner.

1. On the main page, select the **Column** icon in the top-right corner.



2. Use the check-boxes to select or deselect columns.



3. Click **Reset** to reset to the default options.

The *Devices List* will update automatically.

Viewing Devices in Grid View

Grid View provides a quick way to preview live video from multiple devices simultaneously. This view is useful for verifying device positioning, checking video quality, and ensuring devices are online.

Accessing Grid View

1. From the main device list, click the **Grid View** icon in the view options.
2. Alternatively, click **View > Grid View** from the menu.

The interface switches from the device list table to a grid layout showing device thumbnails.

Grid View Features

In Grid View, each device displays:

- **Snapshot** - Low-resolution reference image for quick viewing
- **Device name** - Device name and location
- **Status indicators** - Connection status and login state

Switching Back to List View

To return to the detailed device list:

- Click the **List View** icon in the view options
- Or select **View > List View** from the menu



TIP

Grid View is particularly useful after adding new devices to quickly verify they are all online and properly positioned.



NOTE

Video previews in Grid View use a low-resolution stream to minimize network bandwidth.

Removing Devices

You can remove devices from CCT when they are no longer needed in the project. Removing a device disconnects it from CCT but does not affect the physical device itself.



NOTE

Removing a device from CCT does not delete or reset the device. The device remains configured and can be added to the same project or a different project later.

Removing Individual Devices

1. Select the device you want to remove from the device list.
2. Click the  icon and select **Remove**.
3. A confirmation dialog appears showing:
 - The device name and model
 - A warning that the device will be removed from this project
4. Click **Remove** to confirm, or **Cancel** to keep the device.

Removing Multiple Devices

To remove several devices at once:

1. Select multiple devices using checkboxes in the device list.
2. Click the  icon and select **Remove**.
3. The confirmation dialog lists all selected devices.
4. Review the list and click **Remove** to confirm.

The devices disappear from the device list immediately.

What Happens When You Remove a Device

When a device is removed from CCT:

- The device is disconnected from the project
- CCT stops monitoring the device
- The device no longer appears in the device list
- Configuration changes can no longer be applied through this project

Re-adding Removed Devices

To add a previously removed device back to the project:

- Use **Add Devices** to discover the device again
- Or add it manually by IP address
- The device retains its previous configuration



TIP

Before removing devices during a reorganization, consider using the "Move to another project" feature instead to preserve device organization.

Moving Devices to Another Project

You can move devices to another project using the options on the devices list.

1. Select the devices you want to move.
2. Click the  icon and select **Move to Another Project**.
3. Select the project and click **Confirm** in the pop-up window.

The devices will move projects.

Monitoring Task Status

The Task Status panel displays real-time information about background operations in CCT. This helps you track the progress of configuration changes, firmware updates, and other bulk operations.

Accessing Task Status

The Task Status indicator appears in the top-right area of the main interface:

- **All up to date** - No active tasks are running
- **In progress** - One or more tasks are currently running
- **Completed** - Recent tasks have finished
- **Failed** - One or more tasks encountered errors

Click the Task Status indicator to open the detailed task panel.

Task Status Panel

The Task Status panel shows:

- **Task name** - Description of the operation (e.g., "Firmware update", "Apply template", "Change credentials")
- **Affected devices** - Number of devices involved in the task
- **Progress indicator** - Visual progress bar and percentage
- **Status** - Current state (Queued, In Progress, Completed, Failed)
- **Start time** - When the task began
- **Completion time** - When the task finished (if applicable)

Understanding Task Statuses

Tasks progress through several states:

- **Queued** - Task is waiting to begin
- **In Progress** - Task is currently executing
- **Completed Successfully** - All operations finished without errors
- **Completed with Warnings** - Task finished but some devices had issues
- **Failed** - Task could not complete

Task Details

Click on a task to view detailed information:

- **Per-device status** - Shows which devices succeeded and which failed
- **Error messages** - Specific errors for failed operations
- **Retry options** - Ability to retry failed operations

Managing Active Tasks

While tasks are running, you can:

- **Cancel tasks** - Stop a running task before completion (Click **Cancel** next to the task)

Common Task Types

The Task Status panel tracks these operations:

- **Adding devices** - Device discovery and login
- **Firmware updates** - Uploading and installing firmware
- **Configuration changes** - Applying settings to multiple devices
- **Template application** - Deploying device templates
- **Credential updates** - Changing usernames and passwords
- **Certificate installation** - Uploading and installing certificates

**TIP**

For long-running operations like firmware updates, you can continue working in CCT while monitoring progress in the Task Status panel.

**IMPORTANT**

Do not close CCT while tasks are in progress. This may interrupt operations and leave devices in an inconsistent state.

Configuration

The Configuration panel provides access to all device settings. Select one or more devices from the Device List, then use the configuration tabs to modify settings.

General Settings

Under *General* Settings, you can configure device information and change the device mode.

Editing the Device's Name and Location

Changing the device's name and location helps identify the source when multiple devices create events.



TIP

Use consistent naming conventions (e.g., "Building A - Entrance - Device 1") to make device management easier.

1. Click the  icon to access Settings.
2. Edit the device name in the **Name** field.
3. Edit the location in the **Location** field.
4. Click **Apply** to save.

The device information will change to reflect the new name and location.

Changing Device Mode

Under *General* settings, you can change the device mode to prioritize different features on a per device basis. For example, if you want to increase the framerate on a device you can set it to High Framerate mode. However, this turns off certain features. You can only change the device mode on devices with higher bandwidth usage. You will not see this feature if the device model does not support it.

1. Click the  icon to access Settings.
2. Click the **Mode** drop-down list and select from the available device modes:
 - a. **Full feature:** Offers the full functionality of the device. Full feature is the default device mode.
 - b. **High Frame Rate:** Uses the maximum image rate possible but may disable some features on the device.
 - c. **No Video Analytics:** Turns off video analytics. This option is for deployments where device-based video analytics would interfere with other analytics integrations.
 - d. **Dynamic Privacy Masks:** Enables dynamic privacy masks. Dynamic Privacy Masks can detect when the object, e.g., a person or vehicle, is moving and adjust so that the object remains masked. This mode is not available on all models.
3. Click **Apply** to save.

The device will reboot after you change the device mode.

CCT will wait until device reboot is finished and then will treat command as done.

Setting the Device's Timezone

1. Select your region from the **Timezone** drop-down list.
2. Ensure the **Daylight Savings** checkbox remains checked to compensate for the time change related to daylight savings.
3. Click **Apply** to save.

The device will keep time based on the new settings.

Network Settings

On the *Network* tab, administrators can configure a number of network and security settings to improve network performance and bolster security. Most of the device's network settings can be configured for many devices at once using the Camera Configuration Tool (CCT). However, certain settings can only be configured in the device's web interface. HTTPS port, RTSP port, and NTP Server settings can only be set in the device web interface.

Turning off DHCP

Administrators can turn on or off DHCP. DHCP is enabled by default.

1. Use the **DHCP** drop-down menu to turn off DHCP if required.
2. Click **Apply** to save.

DHCP will turn off.

Changing the IP Address, Subnet Mask and Default Gateway

Administrators can change the device's IP address, subnet mask and/or default gateway.



IMPORTANT

Ensure the IP address is not already in use on your network.



NOTE

You must turn off DHCP before you can change these settings.

1. Edit the **IP address** field if you need to give the device a different IP address.
2. Edit the **Subnet mask** field to move the device to a different subnet.
3. Edit the **Default gateway** field to ensure proper network communication between the subnets.
4. Click **Apply** to save.

Changing the Device's Hostname

Administrators can change the device's Hostname by editing the text in the Hostname field.

1. Edit the text in the **Hostname** field.
2. Click **Apply** to save.

The Hostname will update.

Changing the NTP Server Mode and Information

You can change the NTP server mode to manual to reassign NTP servers. The NTP Server mode is set to DHCP by default. We recommend leaving DHCP enabled to ensure clock synchronization across the network. If the clocks are not properly synchronized, the devices and devices will not work. For example, twice a year the clocks change in certain regions due to daylight savings time.

1. Use the NTP server mode field if you need to change the NTP server mode to manual.
2. Edit the NTP server address to reassign servers.
3. Click **Apply** to save.

The system will now adhere to the new NTP server for time.

Turning Off Automatic DNS Assignment from DHCP

You can turn off automatic DNS assignment from DHCP to force the device to use the manually specified DNS server you assign.

1. Use the **DNS from DHCP** drop-down menu to turn off automatic DNS assignment from DHCP if required.
2. Click **Apply** to save.

Configuring Control Ports: HTTP, HTTP Port and HTTPS

Administrators can configure the Control Port settings to assign certain connection types to certain ports.

1. Use the **HTTP** drop-down menu to turn off HTTP if required.
2. Ensure HTTP is turned on to edit HTTP and HTTPS port information. These are the default ports:
 - a. HTTP port: 80
 - b. HTTPS port: 443
3. Click **Apply** to save.

The device will use the new control port settings.

If you need to edit the HTTPS port, RTSP port, or NTP Server settings, you must use the device web interface.

Image Settings

Under *Image* settings, you can configure the device streaming settings to optimize video quality in light of network constraints. The device will automatically adjust compression quality in order to abide by the bandwidth cap specified.

Devices can have primary, secondary, tertiary and quaternary streams. Not all device models have quaternary streams. Refer to the for the device's specifications.

Follow these steps to configure a device stream:

1. Find the stream under *Media profiles*, and click the icon.
2. Choose the streaming format for video compression in the **Compression Standard** list. If you use Onboard Storage, you must select H.264.
3. Select an option from the **Encoding** list:
 - a. H.264 is needed for onboard storage.
 - b. H.265 offers higher compression than H.264.
 - c. JPEG has the best image quality but the largest file size.
4. Select the **Image Resolution** from the list.
5. Select the **Frame rate** from the list. Choose a value between 1 and 30 frames per second. This sets how many images stream per second. The default rate is 30.
6. Select the desired **Image Quality** from the list. A quality setting of 1 gives the highest quality video but uses the most bandwidth.
7. Enter the maximum bandwidth the device can use in the **Max Bitrate** field.
8. Enter the number of frames between each keyframe in the **Keyframe Interval** field. You can enter a number between 2 and 64.
9. Click **OK**.

This applies the image settings to the stream.

Configuring Image Quality

Follow these steps to improve image quality:

1. Use the **Flicker Control** option if the image flickers. Fluorescent lights often cause flickering. Set the control to the same frequency as the lights to reduce the effect. Europe is often 50Hz, and North America is often 60Hz.
2. Use **Image stabilization** if the device is mounted on a shaking surface. This feature can make the footage better by making up for motion.
3. Use the **WDR** option if bright light and dark shadows are both visible. This lets the device adjust the video image.
4. Click **Apply** to save.

This applies the image settings to the device.

Setting Day/Night Mode

Follow these steps to set the day/night mode:

1. Select a mode from the **Day/night mode** drop-down menu.
 - a. **Automatic:** When the light level is above the day/night threshold, the video image will be in color. When the light level goes below the day/night threshold, the device will automatically open the IR cut filter and switch to monochrome mode. For device with no IRCF, the device will just switch to monochrome. If IR illuminators are enabled, they also turn on.
When the Day / Night mode setting is set to Automatic you can use the slider to set the Day/Night Threshold. Move the slider to set the light level when the device switches between day mode and night mode. The slider value is in Exposure Values (EV). In day mode, the last known light level is displayed under the image panel and is also shown as a blue bar on the Day/Night Threshold slider.
 - b. **Color:** The video image will always be in color.
 - c. **Monochrome:** The video image will always be monochrome.
 - d. **External:** The device will open the IR cut filter and switch to monochrome mode based on the digital input circuit state. For device with no IRCF, the device will just switch to monochrome.
2. Set the day/night threshold in the **Day/night threshold** field. This setting increases or decreases the minimum threshold required for the device to change modes. Alternatively, you can enter a value (-8 and 8) in the EV field.
 - a. Moving the slider to the right decreases the threshold required for the device to switch to daytime settings.
 - b. Moving the slider to the left decreases the threshold required for the device to switch to night time settings.
3. Click **Apply** to save.

This applies the day/night mode to the device.

Turning on Backlight Compensation

Backlight Compensation helps brighten dark areas when there is strong background lighting, for example, a large window in the background. You can enable Backlight Compensation to brighten the dark areas and achieve a well exposed image.

- Toggle the **Backlight Compensation Mode** button to the ON position. Click **Apply** to save.

The device will start using backlight compensation.

Turning on Digital Defog

If the device is installed in a foggy environment, you can use Digital Defog increase the video contrast to help make objects more visible in the scene.

1. Select **On** from the **Digital Defog** drop-down menu.
2. Select a setting from the **Digital Defog** level drop-down menu.
3. Click **Apply** to save.

The device will apply Digital Defog to help clarify foggy images.

Configuring Color Mode

1. Select a mode from the **Color mode** drop-down menu.
2. Enter a value in the **Saturation** field to set the Saturation level. Increasing saturation will enhance the color intensity. Lowering the saturation will reduce the intensity.
3. Enter a value in the **Sharpness** field to set the Sharpness level. Increasing sharpness will help clarify fine details. Adjusting the sharpness will make the image blurry initially. Refocus the device after adjusting the sharpness.
4. Enter a value in the **Brightness** field to set the Brightness level. Increasing brightness can make dark scenes easier to see. If increasing brightness makes the dark areas harder to see, due to a strong back light for example, you can use Backlight Compensation Mode instead.
5. Enter a value in the **Contrast** field to set the Contrast level. Increasing contrast can emphasize certain aspects of the image. Lowering the contrast can make the image softer. The right level of contrast depends on the subjects you want to see clearly as well as the setting.
6. Click **Apply** to save.

Configuring White Balance

Assign a White Balance mode to compensate for discoloration in the image. For example, florescent lights can cast a green hue on the scene. White Balance corrects this effect and makes objects in the field of view appear as they normally would.

1. Select a mode from the **White balance** drop-down menu:
 - a. Automatic: Allows the device to automatically control the red, green and blue color channels to neutralize the color cast and achieve a more accurate white.
 - b. Manual: Allows you to manually set the Red and Blue levels.
2. Enter a value in the **Red adjust** field to set the Redness level.
3. Enter a value in the **Blue adjust** field to set the Blueness level.
4. Click **Apply** to save.

PTZ Settings

Under *PTZ*, users can configure the pan, tilt and zoom limits and turn on or off digital zoom.

Setting Pan, Tilt and Speed Limits

Setting PTZ limits is a critical step in configuring a surveillance system to protect both the equipment and the privacy of the surrounding area. For example, if the device is mounted near an obstacle, setting limits ensures the device doesn't attempt to pan into it, thus protecting the equipment.

1. To set a pan limit, enter the coordinates in the **From** and **To** fields (0° - 360°). This limits the device's horizontal movement.
2. To set a tilt limit, enter the coordinates in the **From** and **To** fields (-180° - 180°). This limits the device's vertical movement.
3. To set a speed limit, enter the degrees per second for the **Preset speed limit** and **Pan/Tilt speed limit** fields (°/s). This limits the device's vertical movement.
4. Click **Apply** to save.

Turning on Digital Zoom

Digital zoom is a software process that magnifies a subject by cropping the center of the image and enlarging it to fill the frame.

- Select Enabled from the **Digital Zoom** drop-down menu and click **Apply** to save.



NOTE

Digital Zoom can diminish image clarity and sharpness. Use digital zoom in scenes where this will not be an issue.

User Management

On the *Users* tab, administrators can add new users and manage user accounts.

Follow these steps to add a new user:

1. You can add new users on the **Users** tab.
2. Go to the Users tab in the **Configuration** list.
3. Click the **Add user** button.
4. Enter a Username.
5. Enter a Password.



TIP

The password must have uppercase letters, lowercase letters, numbers, and symbols.

6. Select a Security Group. See the [Security Groups on page 28](#) table for permission levels.
7. Select the Use PTZ controls option to let the user move PTZ devices.
8. To add this user to other devices:
 - a. Make sure you selected the right devices in the List.
 - b. In the **Add user** window, click the additional devices option (e.g., 3/3 devices).

Add user

Username

Password

Role

☐ PTZ Control

 3/3 devices

- c. The Manage user on devices window will open. Check the list of devices. You can uncheck a box to remove the new account from a device.

Manage user on devices



Device name	Model	☒ User: ⓘ
8.0C-H6SL-B01-1R(5018080)	8.0C-H6SL-B01-1R	☒
din00	4.0C-H6A-PTZ-DP30-B	☒
8.0C-H6A-FE-360-D01-1R(14113806)	8.0C-H6A-FE-360-D01-1R	☒

Selected:3

Apply Cancel

d. Click **Apply** to save.

e. Click **OK**.

9. Click **Apply** to save.

The user will now show in the *Users* list.

Users ^

User list

administrator (Administrator)

3/3 devices

* user (User)

3/3 devices

+ Add user

Managing Users

You can edit and delete user accounts on the *Users* page.

- To edit the account username, click the  icon, edit the settings and click **Apply** to save.
- To delete an account, click the  icon, click **Delete** in the confirmation dialog and click **Apply** to save.

Security Groups

Settings	Users	Operators	Administrators
Live Preview	Yes	Yes	Yes
PTZ Controls	Yes ¹	Yes	Yes
General Settings	No	No	Yes
Network Settings	No	No	Yes
Image and Display	No	Yes	Yes
Compression and Image Rate	No	Yes	Yes
Motion Detection	No	Yes	Yes
Tamper Detection	No	Yes	Yes
Analytics	No	Yes	Yes
Device Automation	No	No	Yes
Privacy Zones	No	Yes	Yes
Digital Inputs and Outputs	No	Yes	Yes
Audio Settings	No	Yes	Yes
Storage	No	Yes ²	Yes
Licensing	No	No	Yes
Users	No	No	Yes
System	No	No	Yes
Device Logs	No	No	Yes

¹ Users can use the PTZ controls if the administrator gives them permission by selecting the Use PTZ Controls check box under *User Settings*.

² Operators can configure onboard storage settings but cannot delete video recordings or format the SD card.

Analytics

Under Analytics, users can enable and configure analytic features on devices.

1. To change the analytics scene mode, select an option from the drop-down menu:
 - a. Large Indoor Area: use this mode for indoor areas.
 - b. Outdoors: use this mode for outdoor areas.
2. Use the options under **Self-Learning** to turn on or off self-learning analytics.
3. Use the options under **Self-Learning Updates** to either activate or suspend self-learning updates.
4. Click **Reset Self-Learning** to re-initiate self-learning analytics on the device.
5. Enter a value (0 - 100) to set the **Motion Detection Sensitivity**. The default is 50.
6. Enter a value (0 - 100) to set the **Motion Detection Threshold**. The default is 20.
7. Use the options under **Tamper Detection** to turn on or off the tamper detection analytic.
8. Enter a value (1 - 10) to set the **Tamper Sensitivity**. The default is 5.
9. Enter a value (2 - 30) to set the **Tamper Duration**. The default is 20.
10. Click **Apply** to save.

The changes will be applied.

Updating Connection Credentials

When device login credentials change, you can update them in CCT to maintain connectivity. This is particularly useful after security audits, policy changes, or when replacing factory default credentials.

Update credentials when:

- Devices are using factory default credentials that need to be secured
- Password policies require periodic credential rotation
- A security incident requires credential changes
- Credentials have been compromised
- Standardizing credentials across multiple devices

Updating Credentials for Multiple Devices

You can use the connection credentials section of configuration panel to change the credentials used to connect:

1. Select the devices that need credential updates from the device list.
2. Right-click and select **Change Credentials**, or click the action menu and choose **Change Credentials**.
3. The Connection Credentials dialog appears showing:
 - List of selected devices
 - Current connection status
 - Current username (if known)
4. Enter the **New Username** (if changing the username).

5. Enter the **New Password**.
6. Re-enter the password in the **Confirm Password** field.
7. Click **Apply**.

Credential Update Process

After clicking Apply, CCT performs these steps for each device:

1. **Verification** - Tests the new credentials to ensure they work
2. **Update** - Changes the credentials on the device
3. **Reconnection** - Logs in with the new credentials
4. **Status update** - Updates the device status in CCT

Monitor progress in the Task Status panel. Devices will briefly show "Login Pending" status during the credential update.

Updating Credentials for Offline Devices

For devices that are currently offline or showing "Login Failed":

1. Select the offline devices.
2. Choose **Change Credentials**.
3. Enter the correct credentials.
4. Click **Apply**.

CCT stores the new credentials and attempts to reconnect. If credentials are correct, devices will change to "Logged in" status.

Handling Credential Update Failures

If credential updates fail on some devices:

- **Authentication Failed** - The current credentials are incorrect. Verify you're using the right credentials before attempting the update.
- **Password Policy Violation** - The new password doesn't meet the device's password requirements (length, complexity, etc.).
- **Connection Error** - Device is unreachable. Verify network connectivity.
- **Permission Denied** - The current account doesn't have permission to change credentials.

Check the Task Status panel for specific error messages and resolve issues before retrying.

Templates

Device templates allow you to save and reuse device configurations across multiple devices. This feature streamlines deployment by applying consistent settings to groups of devices.

Templates are particularly useful for:

- Deploying multiple devices with identical configurations
- Standardizing settings across different projects
- Backing up and restoring device configurations
- Quickly configuring replacement devices

Template Best Practices

- **Name templates descriptively** - Include the device model and purpose (e.g., "12MP-FE-DC1-Parking.json")
- **Create model-specific templates** - Different device models have different capabilities
- **Exclude network settings** - Unless deploying to an isolated network, avoid including IP addresses in templates
- **Test templates** - Apply templates to a test device before mass deployment
- **Version control** - Include dates in template filenames to track configuration versions



IMPORTANT

When applying templates, devices will briefly disconnect as settings are updated. Plan template deployment during maintenance windows.

Exporting Device Templates

Export templates to save device configurations for reuse:

1. Select a device from the device list.
2. Click **Templates** in the top menu.
3. Click **Export device template**.
4. Choose which configuration categories to include:
 - General settings
 - Network configuration
 - Image settings
 - Video profiles
 - Analytics
 - User management
 - Certificates

- PTZ settings
5. Click **Export**.
 6. Choose a location and filename for the template file.



NOTE

Templates are exported in .cct3x format. The template file does not include passwords or sensitive credentials.

Importing Device Templates

Apply saved templates to new or existing devices:

1. Select the target devices from the device list.
2. Click **Templates** in the top menu.
3. Click **Import device template**.
4. Browse to and select the template file.
5. Review the configuration tree showing all settings that will be applied.
6. Deselect any settings you don't want to apply.
7. Click **Apply**.

CCT applies the template settings to all selected devices and displays the progress in the task status area.

Applying Templates to Selected Devices

You can selectively apply template configurations:

1. Select the devices from the device list.
2. Import the device template.
3. In the template preview dialog, expand the configuration tree.
4. Use checkboxes to select specific settings:
 - Check parent categories to apply all settings within that category
 - Expand categories and check individual settings for granular control
 - Uncheck settings that should remain unchanged
5. Click **Apply** to apply only the selected settings.

Firmware Management

Under *Firmware*, administrators can upgrade the device's firmware by downloading the .BIN file and uploading it to CCT. Administrators can also check the current firmware version on the *Firmware* tab.

Best Practices for Firmware Updates

- **Test first** - Update one or two devices before deploying to all devices
- **Schedule during maintenance windows** - Devices will be offline during updates
- **Ensure stable network** - Use wired connections when possible
- **Verify power** - Confirm devices have stable power, preferably UPS-backed
- **Batch updates** - For large deployments, update in smaller groups
- **Monitor progress** - Watch the Task Status panel throughout the process

Important Notices

- Do not power off devices during firmware upgrade.
- Devices will reboot after firmware installation.
- Upgrade may take 5-15 minutes per device.
- Back up device configuration before upgrading.

Troubleshooting Update Failures

If firmware updates fail on some devices:

1. Check the Task Status panel for error details.
2. Common causes include:
 - Network disconnection during upload
 - Insufficient device storage
 - Incompatible firmware file
 - Device power loss during update
3. Resolve the issue and click **Retry** in the Task Status panel for failed devices.



IMPORTANT

If a device becomes unresponsive after a failed firmware update, power cycle the device. Most devices have a recovery mode that activates after failed updates.

Certificates

On the *Certificates* page, you can view the number of active certificates, the certificates expiring soon and the expired certificates.



NOTE

Some devices do not support certificate management by ONVIF.

Certificate Status Indicators

	Device is connected using a trusted certificate
	Device is using an untrusted certificate
	Device is connected over HTTP
	Device is using an invalid certificate

Viewing Device Certificates

Follow these steps to view the certificates on a device:

1. Locate the device in the list.
2. Click the  icon and select **View Certificates**.

You can now view the certificates on the device.

Uploading Certificates to a Device

Follow these steps to upload the certificate to a device:

1. Locate the device in the list.
2. Click the  icon and select **Upload Certificates**.

The certificate will be applied to the device.

Generating CSR Certificates

Follow these steps to generate a CSR certificate:

1. Click the **Generate CSR Certificates** button above the devices list.
2. Enter the Certificate Subject data to create CSR:
 - a. Common Name
 - b. Prefix
 - c. Source of unique data
 - d. none
 - e. Suffix
 - f. Subject Alternative Name
 - g. Source of data
 - h. none
 - i. Organizational Unit
 - j. Organization
 - k. Locality
 - l. State or Province
 - m. Country
3. Click **Download**.

The certificate will be generated.

Uploading Certificates to CCT

Follow these steps to upload a certificate:

1. Click the **Upload Certificates** button above the devices list.
2. Navigate to the file on your computer.
3. Click the **Upload** button.

The certificate will be uploaded.

Projects

Projects allow you to organize devices by location, client, or any other logical grouping. Each project maintains its own device list and settings.

- Separate device management for different sites
- Different user permissions per project
- Isolated configuration changes
- Better organization for large deployments

Accessing Projects

You can access projects from the drop-down list on the top-ribbon.

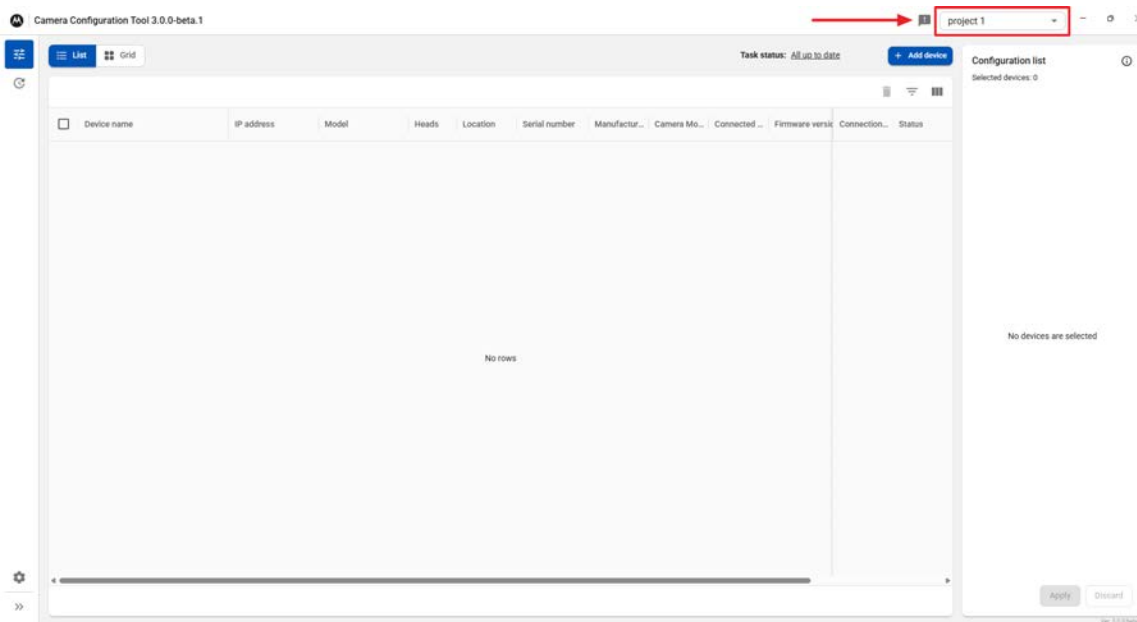


Figure 2: Projects are listed in a drop-down menu.

Creating and Managing Projects

Projects help you organize and manage devices by location, client, or deployment. You can create new projects, switch between existing projects, and manage project settings.

Creating a New Project

When you first launch CCT or need to create a new project:

1. Click the project dropdown in the top-ribbon.
2. Click **Create project**.
3. Enter a name for the project.
4. Click **Create**.

The new project opens automatically and you can begin adding devices.

Selecting an Existing Project

To switch between projects:

1. Click the project dropdown in the top-ribbon.
2. Select the project you want to open from the list.
3. Click **Open**.

CCT loads the device list and settings for the selected project.

Multi-Project Login Workflow

When you have multiple projects, CCT streamlines your workflow:

1. Launch CCT and enter your password.
2. The project selection screen displays all available projects.
3. Select a project from the list or create a new one.
4. Click **Open** to access the project.

You can switch projects at any time using the project dropdown in the main interface.

Project Settings

On the top ribbon of the application, users can access project settings.

Editing the Project Name

Follow these steps to edit the project name:

1. Click the **Project** drop-down menu from the top-ribbon and click **Project Settings**.
2. Edit the text in the **Project Name** field if you want to edit the name.
3. Click **Apply** to save.

The project name will change.

Changing the Password

You can change your CCT password from project settings:

1. Click the **Project** drop-down menu from the top-ribbon and click **Project Settings**.
2. In the Password section, enter your current password.
3. Enter and confirm your new password.
4. Click **Apply** to save.

Deleting Projects

When you no longer need a project, you can remove it from the system.



IMPORTANT

Deleting a project removes all device associations and project-specific settings. This action cannot be undone. The devices themselves are not affected and can be added to other projects.

Follow these steps to delete a project:

1. Click the **Project** drop-down menu from the top-ribbon and click **Project Settings**.
2. Scroll down and click **Delete Project**.
3. A confirmation dialog appears warning that:
 - This action cannot be undone
 - All project data will be permanently deleted
 - You will be returned to the project selection screen
4. Click **Delete** to confirm, or **Cancel** to keep the project.

After deletion, you are returned to the project selection screen where you can open a different project or create a new one.

Selecting a Different Project

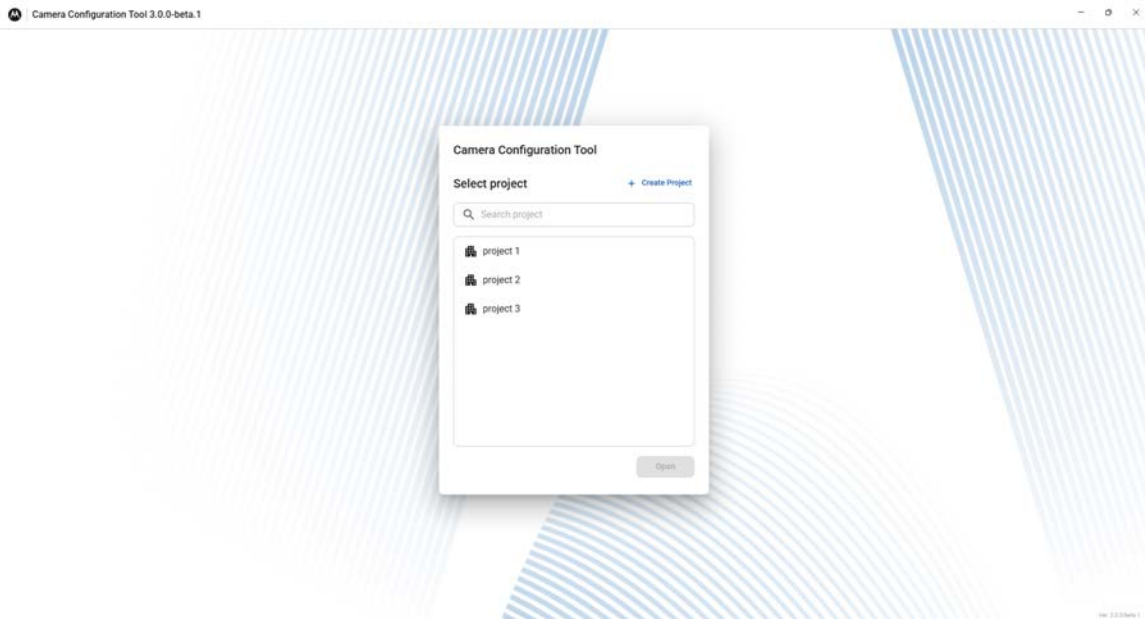
On the top ribbon of the application, users can access a drop-down list to select a different project.

1. Click the **Project** drop-down menu from the top-ribbon and click **Select Project**.
2. Choose the project from the list in the **Select Project** window.



TIP

Use the search bar to find the project faster.



3. Click **Open**.

The project will open.

Generating Project Reports

CCT can generate comprehensive reports that document all devices and their configurations within a project. These reports are useful for documentation, audits, and project handoffs.

Project reports include:

- Project name and device count
- Complete device list with model information
- Network configuration (IP addresses, ports, protocols)
- Device locations and names
- Firmware versions
- Device settings organized by category
- Video profile configurations
- Analytics settings
- User management and security settings

Generating a Report

1. Open the project you want to document.
2. Use the **Project** drop-down to select **Export PDF Report**.
3. Choose a location to save the report file.

Report Layout

The report presents information in a structured format:

- **Cover page** - Project name and summary statistics
- **Device overview** - List of all devices with key parameters
- **Configuration details** - Detailed settings organized by device and category
- **Visual references** - Device snapshots and location diagrams (when available)



TIP

Save reports after completing major configuration changes to maintain a documentation history.

Settings

System Settings

On the *General* tab, users can set the system language, theme and configure CCT network settings.

Allowing Self-Signed Certificates

- Toggle the **Always Trust Self-Signed Certificates** button to allow access based on the presence self-signed certificates.



IMPORTANT

User will not be prompted with a warning dialog when connecting to devices with self-signed certificates. Enabling this option may pose security risks. Only enable if you trust the devices in your network and understand the implications.

Allowing Fallback to HTTP

- Toggle the **Allow Fallback to HTTP** button to allow fallback to HTTP in the absence of HTTPS.

When enabled, HTTPS connection is tried first and HTTP is used as a fallback if HTTPS fails. When disabled, only HTTPS connections are attempted.



NOTE

Some devices do not connect by HTTPS out of the box; like Sarix Value 2.

Creating a Firewall Rule for Device Discovery

- Users can create a Windows Firewall exception so the application can receive all device auto-discovery traffic.

Sharing Anonymous Data

Under Telemetry, users can choose to share anonymous data to improve the application.

- Toggle the **Share anonymous data** button to enable data sharing.



IMPORTANT

Share anonymous diagnostic data to help identify performance bottlenecks and optimize application stability. Data collection is strictly limited to functional metadata and excludes Personally Identifiable Information (PII).

Client Settings

Client Settings allow you to customize the CCT interface and behavior to match your preferences and working environment.

Accessing Client Settings

To open Client Settings:

1. Click the settings icon (gear) in the left sidebar.
2. Select **Client Settings** from the settings menu.

General Settings

The General section includes basic application preferences:

Language

Select the display language for CCT:

- Click the **Language** dropdown
- Select your preferred language
- CCT restarts to apply the language change

Theme

Choose between light and dark interface themes:

- **Light theme** - Bright interface with light backgrounds
- **Dark theme** - Dark interface optimized for low-light environments

Click the theme preview to switch between themes. The change applies immediately.

Display and Performance

Grid View Options

Configure how devices appear in Grid View:

- **Show device names** - Display device names under thumbnails
- **Show device information** - Display model and status information
- **Thumbnail quality** - Adjust preview image quality (higher quality uses more bandwidth)

Advanced Options

Diagnostics

Share anonymous usage data to help improve CCT:

- **Enable anonymous telemetry** - Send usage statistics and performance data

All diagnostic data is anonymous and does not include personally identifiable information, device footage, or network credentials.

Applying Settings

After making changes:

1. Click **Apply** at the bottom of the settings panel.
2. Some changes take effect immediately (theme, display options).
3. Other changes may require restarting CCT (language, region).

Click **Reset to defaults** to restore all settings to factory defaults.

Settings Storage

Client settings are stored locally on your computer and persist across sessions. Settings are user-specific and do not affect other users on the same system.



NOTE

Theme preference is particularly useful in control rooms or when monitoring devices in low-light environments.

More Information & Support

For additional product documentation and software and firmware upgrades, visit support.avigilon.com or support.pelco.com.

Technical Support

Contact Avigilon or Pelco Technical Support at support.avigilon.com/s/contactsupport or support.pelco.com/s/contactsupport.