Oncam C-Series
Camera Configuration Tool User Manual

Contents

1. Legal and Warnings

⚠️ Please Read before Installation

Read through the guide carefully before installing the product. Keep this guide for future reference. If you need further support during installation, please visit:

https://www.oncamgrandeye.com/

1.1 Legal Considerations

The use of video surveillance may be regulated by local laws that vary from country to country. Please check the laws in your local region before using this product for surveillance purposes.

1.1.1 Intellectual Property Rights

Oncam has intellectual property rights relating to the technology embodied in the product described in this document. These intellectual property rights may include one or more of the Oncam patents or pending patent applications in the US and other countries. This product contains licensed third-party software.

1.1.2 Liability Notice

Every care has been taken in the preparation of this and the accompanying installation documentation.

©Oncam Global Group AG, 2013 - 2020. All rights reserved. No part of this manual may be reproduced except for your express personal use. Oncam and their affiliate's further reserve the right to alter, amend or revise this document and any product specifications without any obligation to provide notice of such changes. Oncam and its affiliates make no guarantee, representation, or warranty, either expressed or implied, regarding the accuracy of the information contained in this manual. Furthermore, Oncam and its affiliates assume no responsibility or any potential liability for any errors that may appear in this manual.

For product and service liabilities please refer to our standard terms and conditions. https://www.oncamgrandeye.com/terms-and-conditions/

1.1.3 Trademarks and Third-Party Trademarks

"ONCAM" and the "ONCAM logo" are trademarks, and in some cases registered or protected trademarks, of Oncam Global Limited and/or Oncam Global, Inc., including under registration in the UK, India and in the U.S. Patent and Trademark Office.
The names of other companies, organizations, products or services mentioned in this manual are the trademarks of their respective owners.

1.1.4 Copyright

© Copyright 2020 ONVU Technologies AG. All rights reserved. Oncam is a trading name of ONVU Technologies AG.

1.1.5 Contact Information

For our contact details please go to: https://www.oncamgrandeye.com/contact-us/

1.1.6   Support

If you require any technical assistance, please contact your Oncam reseller. If your questions cannot be answered immediately, your reseller will forward your queries through the appropriate channels to ensure a rapid response. If you are connected to the Internet, you can go to:
https://support.oncamgrandeye.com/

Here you can:
- Download user documentation and software updates.
- Find answers to resolved problems in the FAQ database, search by product, category, or phrase.

To contact us via email, please use support@oncamgrandeye.com.

Include the following in your email:
- A detailed description of the problem
- Camera model numbers
- Relevant configuration information

1.1.7   End User License Agreement (EULA)

By copying, installing or using all or any portion of the software you accept all the terms and conditions of the End User License Agreement (EULA). You will be asked to accept this as part of the installation process. For the full EULA related to the C-Series Camera Configuration Tool, please go to: https://www.oncamgrandeye.com/wp-content/uploads/Oncam-C-Series-Camera-Configuration-Tool-EULA.pdf

2. Introduction

The Oncam C-12 Series of cameras are the most powerful compact cameras from Oncam, the first derived from the new C-Series platform. These 12MP cameras stream 55 fps at full resolution, significantly outperforming other 360-degree cameras in the market today.

The benefits of a high performance, powerful camera can only be achieved when users are equipped with the right tools to harness them and this is where the C-Series really comes into its own. Thanks to a wide range of onboard technologies developed by the Oncam team, combined with an intuitive user interface and seamless ONVIF implementation, users have the freedom to configure and tailor the camera to best serve their installation environment.

This document describes how to use the Camera Configuration Tool with its sleek user interface to manage of the C-Series camera range. It will enable you to discover, update and control single or multiple cameras simultaneously with ease, saving time and resource.

3. Application Installation

3.1 Installation steps

3.1.1 Download application

Download the C-Series Camera Configuration Tool (CCT) from:
https://www.oncamgrandeye.com/resources/c-series-camera-config-tool/

> Please ensure you meet the minimum system requirements and have the latest Microsoft Edge Browser (85 or above) installed.

Minimum system requirements:

Operating System: Windows 10 64bit
Processor: Intel Celeron or greater; GHz processor or faster
Memory: 4 GB RAM or greater
Disk space: 2 GB or more free hard drive space
Web Browser: Minimum Microsoft Edge 85

Unzip the file OCCT_4.x.xxxx.zip to your preferred folder location

Open and read the Instruction.md file

3.1.2 Pre-Installation environment

3.1.2.1 Step 1

The Oncam C-Series CCT requires the correct pre-installation environment prior to installation of the App.

After unzipping the installation package (OCCT_4.x.xxxx.zip), Double click Setup > Step 1 – Pre- Installation environment and install the file: **windowsdesktop-runtime-3.1.8-win-x64.**
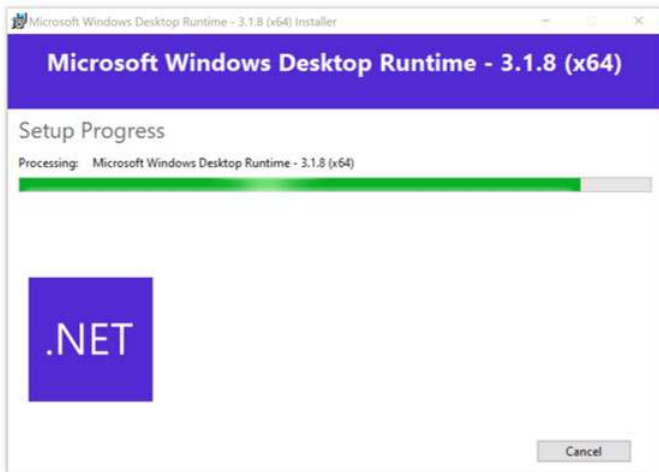
Follow the on-screen instructions to install this environment, as shown below.
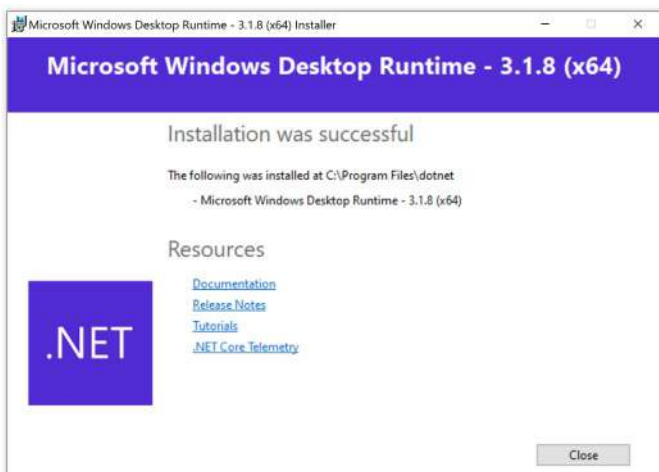
Select **Install**
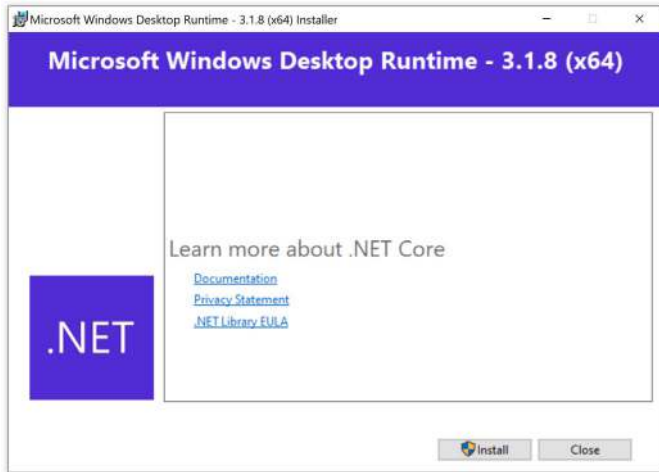
Pop-up will be shown - Accept and allow system changes to continue.

Windows Desktop Runtime will then install.

Successful Installation will be confirmed.

3.1.3 CCT Application Installation

3.1.3.1   Step 2

Return to unzipped installation package (OCCT_4.x.xxxx), Double click Setup > Step 2 > Oncam Camera Configuration Tool Application and install the file: **OncamCCT.msi**

A pop-up will be shown informing you that the Windows Installer certificate is not integrated into the installer, this installation warning will need to be accepted to proceed.

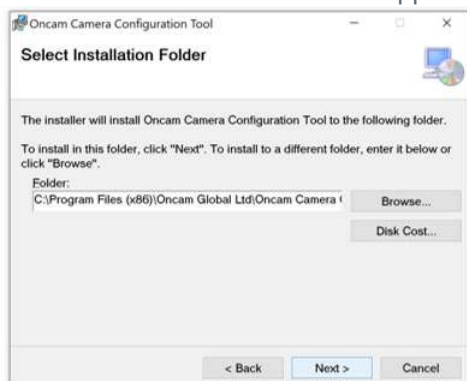Follow the on-screen instructions to install the application, as shown below.

Set Up Wizard will be shown, click **Next**
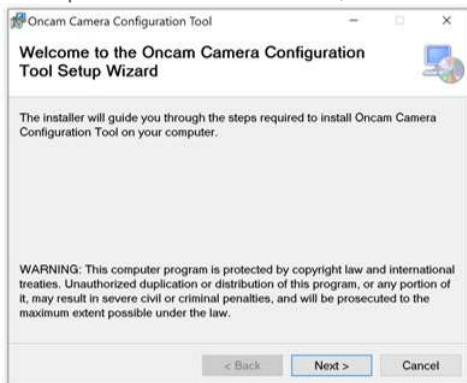
Carefully read and review the License Agreement. If you accept the terms, select: **I Agree** then click **Next**
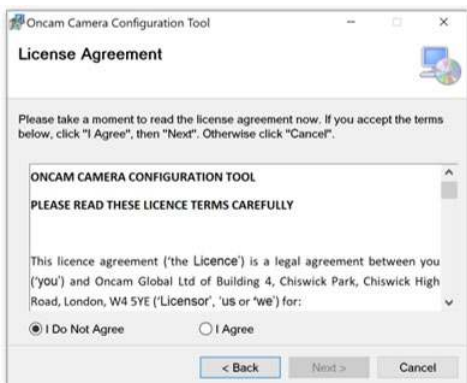
Select the folder location for the application or accept the default, then click **Next**

Review the dependencies required for the application.

NetCore 3.18 will already have been installed as part of Step 1.

Webview2 Runtime will automatically be installed with the application if not already present on your system. Click **Next** to acknowledge.
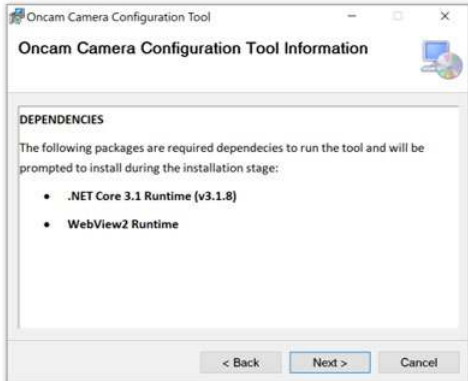
Once ready to run the installation click **Next**
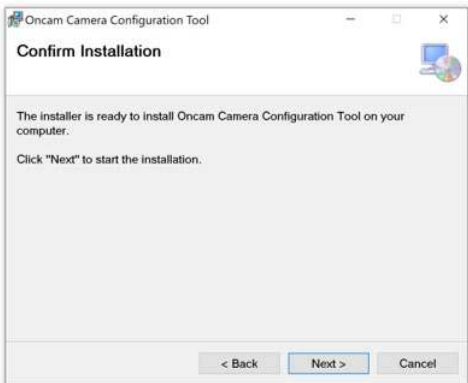
Application will install
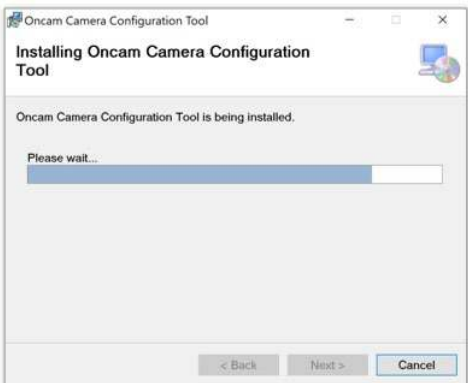
Screen below will be shown when installation is complete, select **Close**
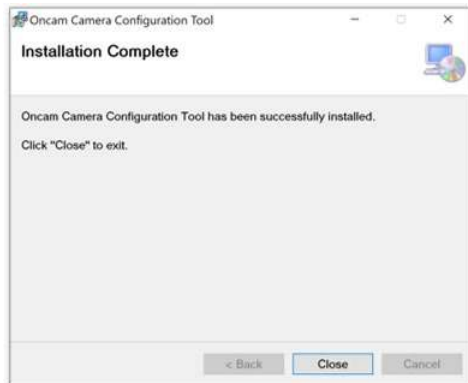
Open start menu and Oncam Camera Configuration Tool will be shown at the top of this menu as recently added. Select it to open the application. A short cut to this application will be accessible from your desktop.
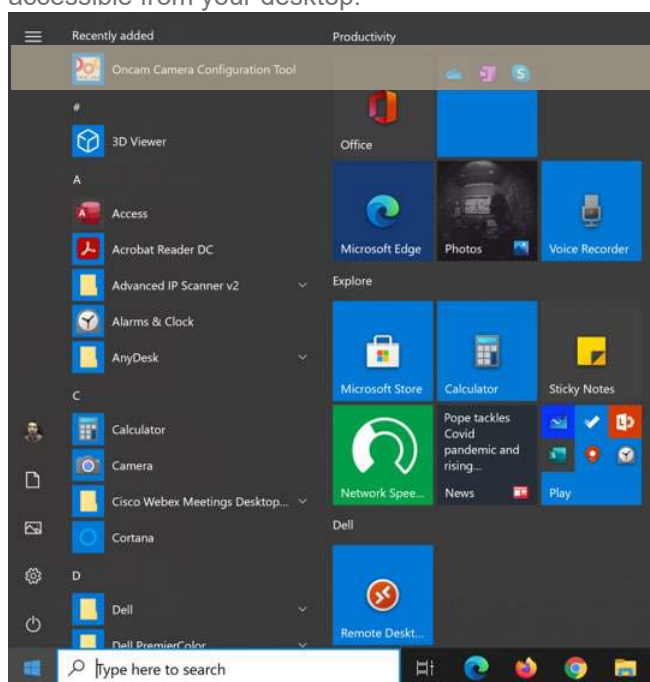
3.1.4 HTTPS support

HTTPS is recommended as the securest way to access the camera as it encrypts traffic between the client and the camera, to ensure communication remains secure end to end. When using HTTPS to access the camera the Oncam Root Certificate will need to be installed to your client workstation to enable discovery and connection via the Oncam CCT.

> Once installed, this Root CA will allow you to connect securely to all C-Series cameras.

To Install this, return to unzipped installation package (OCCT_4.x.xxxx), Double click Setup > HTTPS Support and install the file: **OncamRootCA.crt**

A pop-up will be shown informing you that the Windows Installer certificate is not integrated into the installer, this installation warning will need to be accepted to proceed.

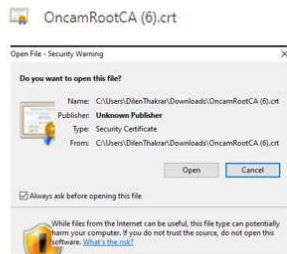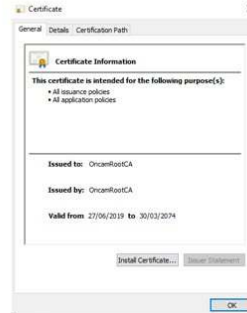Follow the on-screen instructions to install the application, as shown below.

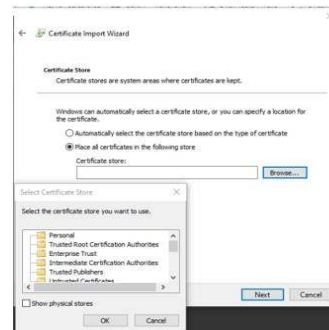|			
1	Double click on the downloaded.crt file. Accept the security warning by selecting **Open**	**2**	A popup window is displayed with the Certificate Information, select **Install certificate…**, another Pop up window will be shown.
3	Certificate Import wizard will be displayed, select **Current User** and click **Next**	**4**	From the Certificate store presented, select **Place all certificates in the following store** and click **browse**
5	Select **Trusted Root Certificate Authorities**, click **OK** and then **Next**	**6**	Check and confirm your settings. Select **Finish.** Click **Yes** if a security warning message is displayed. A confirmation of the successfully imported certificate will be displayed
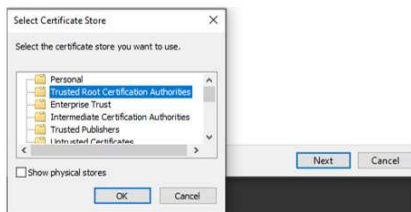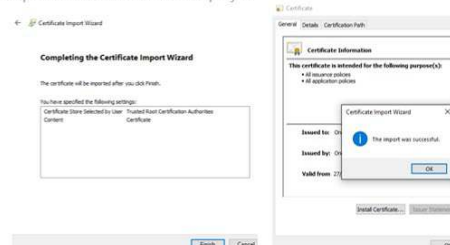
You can now connect to the camera over HTTPS without encountering a security warning.

HTTPS enables RTP, WebRTC video and all data to be encrypted.

> HTTP is enabled by default as it is required by some discovery tools. For secure access it is recommended to turn off HTTP and communicate with the camera over HTTPS only.

To turn off HTTP via the Camera Web Interface go to **Device > Security > Client Connectivity > Connection.**

4. Camera Discovery

4.1 Discovery Tools

To access the camera for the first time, you will need to discover the IP address of the camera.

This can be discovered using your ONVIF compatible VMS (for a list of supported VMS partners please go to https://www.oncamgrandeye.com), the Oncam C-series Camera Configuration Tool (download from https://www.oncamgrandeye.com/resources/c-series-camera-config-tool/) or an IP Address scanning tool.

4.2 IP Address Allocation

4.2.1 IP Address

The IP Address can be assigned to the camera in three different ways as described in the sections below. When the camera is configured with DHCP it responds using the DHCP provided address; if configured with a Static IP address, it responds with the static address, and it responds with its Link Local address if DHCP is not reachable or the Static IP address is in a different subnet to the discovering device.

4.2.1.1 DHCP

The factory default configuration of the camera is DHCP.

If a DHCP server is present, the camera will be allocated an IP Address, a Gateway address and DNS addresses, if these are available for discovery and connected to the camera.

> When on DHCP, the camera also self-allocates a Link Local address - see Link Local.

4.2.1.2 Link Local

When a DHCP server is not found and the camera does not yet have a static IP address, after a period (up to 60 seconds) the camera will self-allocate a random Link Local address. This address can be used to communicate with the camera over HTTP / HTTPS and RTSP. The Link Local address is also used by the camera to respond if the Static IP address configured does not match the current network. If this is the case, the camera responds over Link Local.

To communicate with a camera on a Link Local address, the PC must also have a Link Local address allocated. This can be done manually if needed in all PC operating systems.

> The Link Local address is always accessible over HTTP / HTTPS and RTSP, and a previously assigned address is reused on the camera where possible. However, during boot up if the previous Link Local address is detected to be in use by another device, the camera will select the next available random Link Local address.

4.2.1.3 Static IP

The camera can be configured with a manual Static IP Address. This will also require the Gateway to be set to allow communication with the outside network, and DNS addresses to resolve DNS names if required. On first time setup, the camera will need to be discovered using DHCP or Link Local as described above. The Primary Administrator will need to create login credentials, log-into the camera and set up the Static IP Address. This can be configured in the

Camera Web Interface; **Network > Network Configuration** or using the Camera Configuration Tool please see section 8 Assign IP Addresses.

> If the camera is configured with a Static IP Address on a different subnet than the local network, either use the camera's Link Local address, which will be provided in discovery, or simply force a Physical Reset to Factory Defaults (*See Oncam C-12 Installation & User Manual - Section 11) Reset to Factory Defaults*

4.3 Camera Configuration Tool – Discovery

4.3.1 Discovery

Open the Camera Configuration Tool on a PC that is on the same network as the cameras. As soon as the App is initiated it will discover the Oncam C-Series cameras on your network and display key information including the Friendly name, Model number, MAC Address and most importantly the IP Address of the camera. To update the list, select **Refresh Discovery** in the top right-hand corner.

5. Set Primary Administrator Username and Password

5.1 Connecting to the Camera – First Time Access

Once you have discovered the IP Address of the camera, you will need to set the Primary Administrator Username and Password before you can access the camera. This can be done via the Camera Web Interface (See Oncam C-12 Installation and User Manual section 4.2.1.1). and the Camera Configuration Tool.

5.2 Camera Configuration Tool – Set Password

5.2.1 Single or multiple Cameras

The Camera Configuration Tool can be used to create the Primary Administrator username and password for first time use of the camera. Using this powerful tool, the same login details can be created for multiple cameras at the same time, saving valuable time and resource during installation.

### 5.2.1.1 Setting username and password

After the C-Series cameras have been discovered, any cameras that require login credentials to be created will display **Set Password** under the **ACTIONS** column. Click the check box next to each camera you want to create credentials for and select the **Set Username & Password** button. For enhanced security, default username and passwords are not supported. Users will be required to set a secure password, which will need to meet the minimum requirement below. Please follow these steps to set up your login credentials.
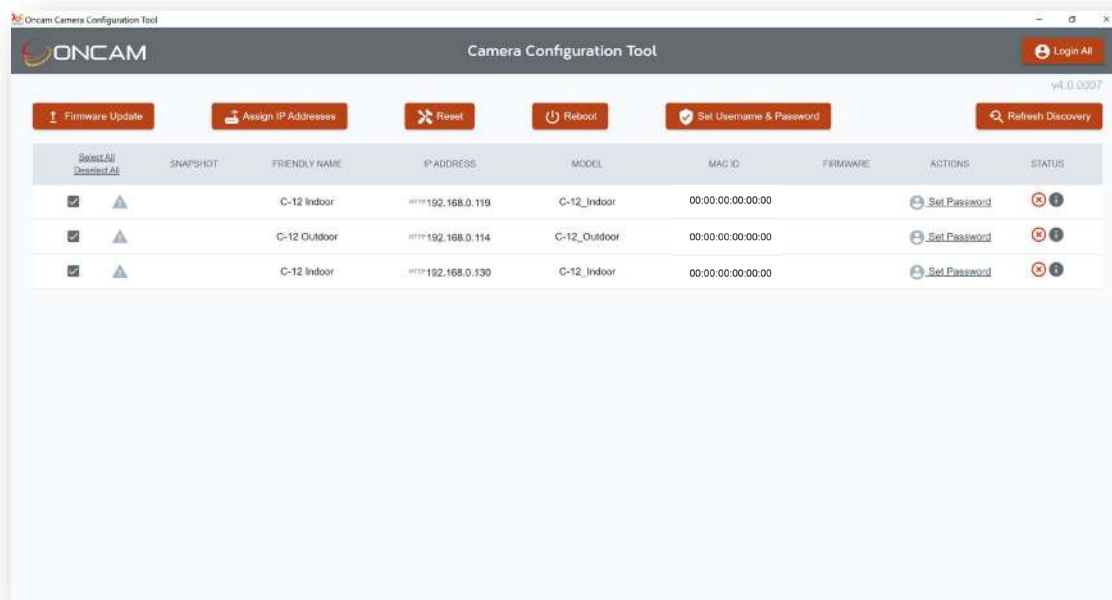
5.2.1.1.1 Username

Set an easily identifiable and memorable username for the Primary Administrator. The name must be a between 4-12 characters in length. The username can consist of uppercase letters (A-Z), lowercase letters (a-z) and numbers (0-9). Special characters are not supported.

> Once created the username cannot be updated.
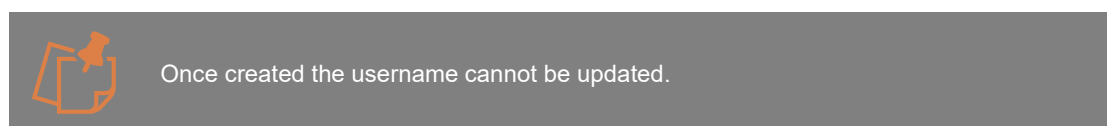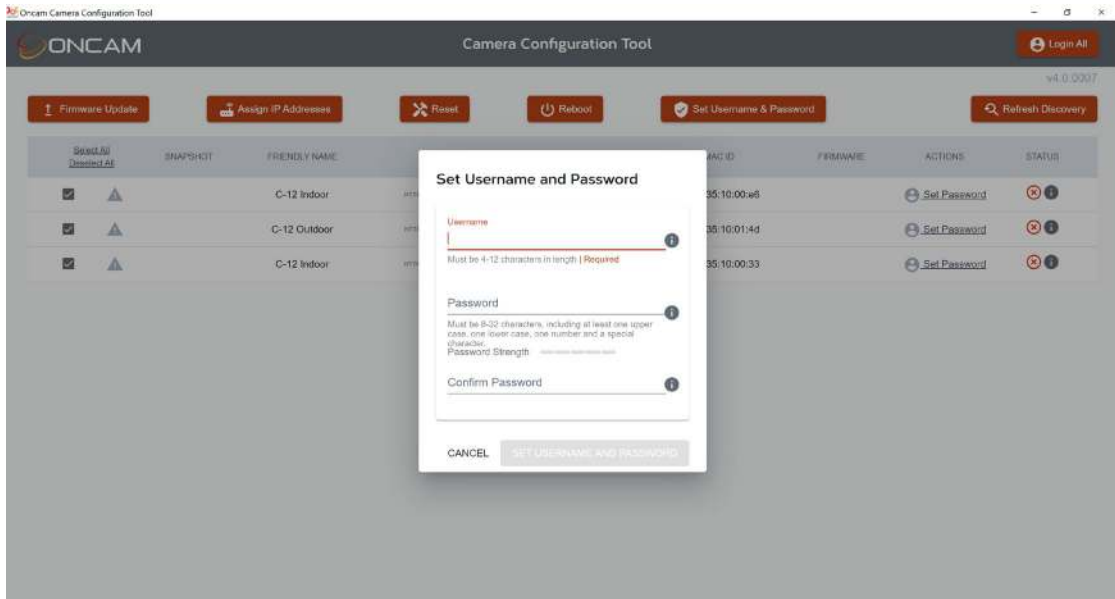
5.2.1.1.2 Password

It is important to always set and use a secure password to access the camera, therefore the camera enforces strong password criteria for all user accounts as specified below:

- Minimum of 8 characters and a maximum of 32.
- The password requires at least one uppercase letter (A-Z), one lowercase letter (a-z), one number (0-9) and one special character. The following special characters are supported (~!@#$%^&*_-+=`|(){}[]:;',.?/).

5.2.1.1.3 Strength Indicator

For guidance, the strength of the password combination is displayed below the password. Use the combination of upper and lower case alphabetic, numeric, and special characters until the password strength is strong enough.

5.2.1.1.4 Confirm Password

Please retype your password to confirm it has been correctly entered, if the passwords do not match a notification will appear.

5.2.1.1.5 Set Password Confirmation

Click **Set Username and Password**, the credentials will be saved, and you will be taken back to the main Camera Configuration Tool discovery page.
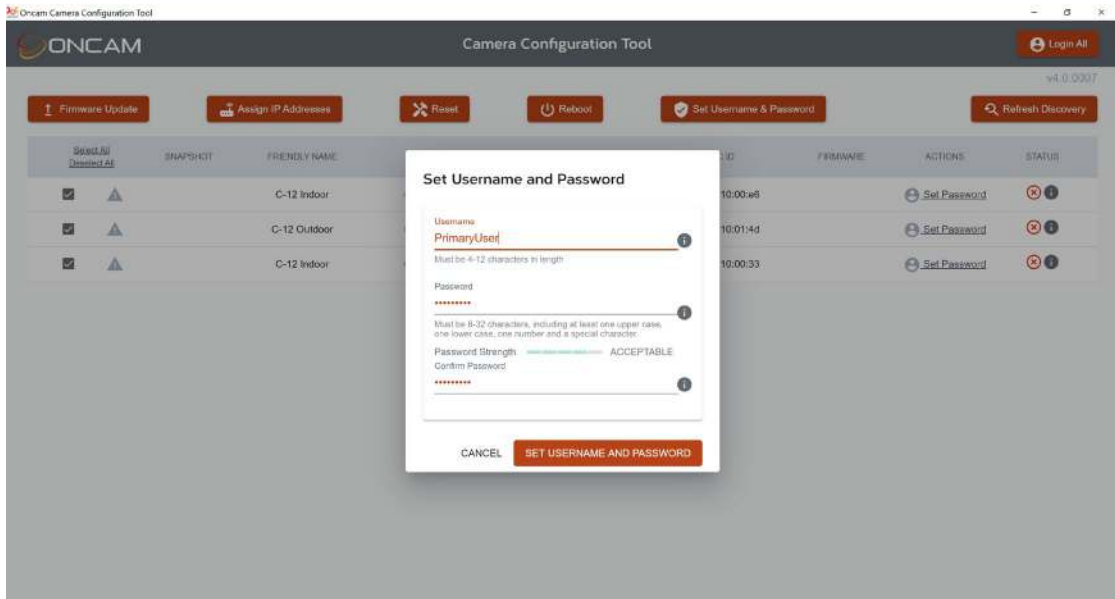
The **Logout** option will now be displayed under the ACTIONS column for the selected cameras

.
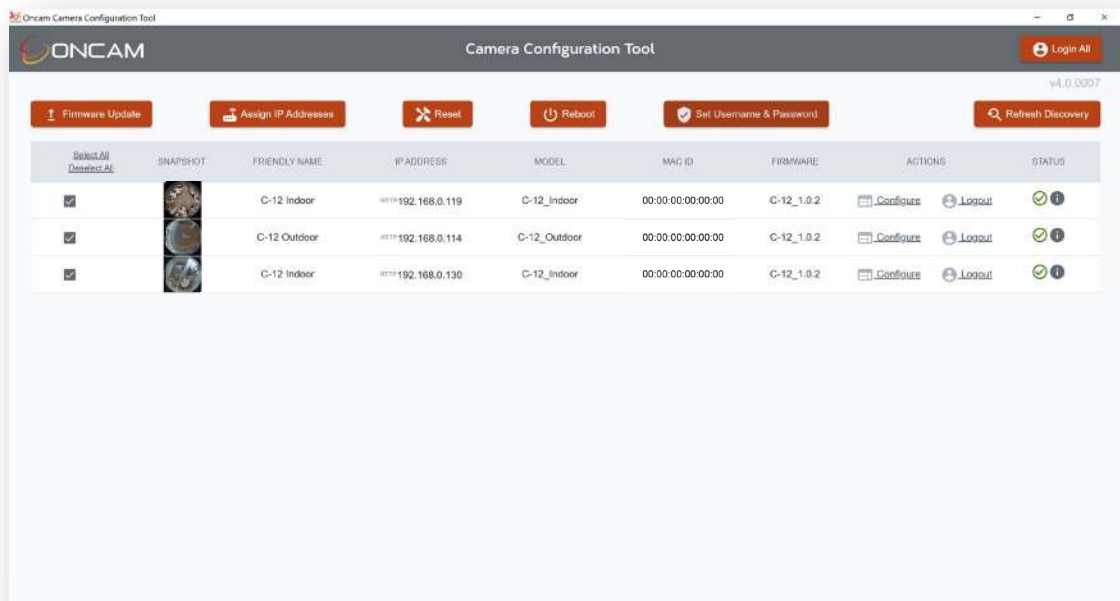
Set Username & Password can only be set from the CCT as part of first-time camera access. If you wish to update user credentials, select the configure option under the ACTIONS column for the camera and update the password in the user section of the web interface. Usernames cannot be updated.

6. Accessing the Camera

Using the login credentials created, the camera is now ready to be configured using your compatible VMS, the Camera Web Interface or the C-Series Camera Configuration tool.

6.1 Login

Unless you have just set the username and password for the camera, following discovery you will need to login to the cameras you would like to access. The X symbol in the **STATUS** column indicates that login is required as also described under the **ACTIONS** column.
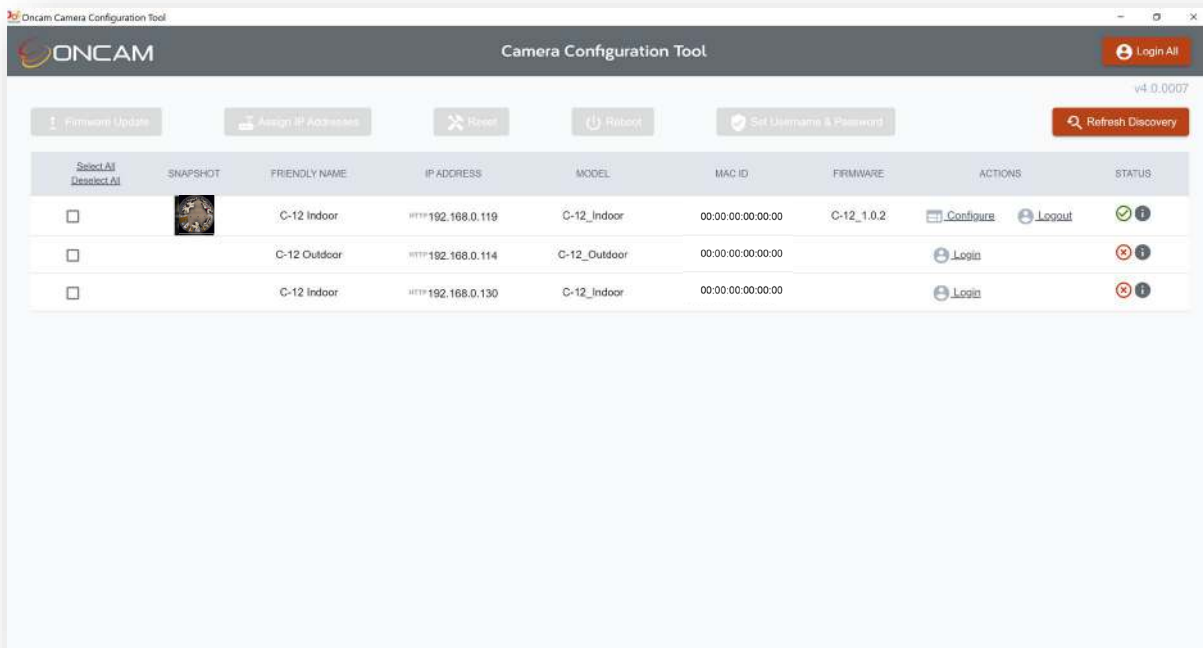
6.1.1 Single camera Login

To login to an individual camera select Login in the **ACTIONS** column and enter the username and password for that camera.
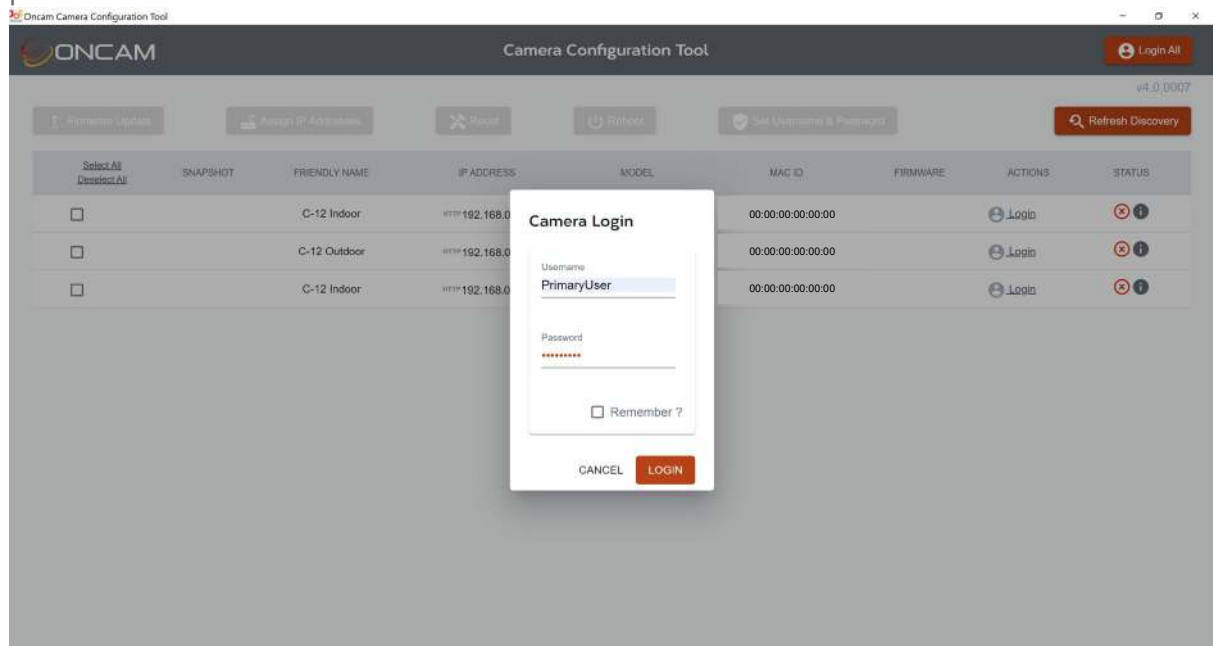
You will be taken back to the dashboard screen and the camera will show as logged in.

If you press the **Refresh Discovery** button, or close and reopen the Camera Configuration Tool, you will need to re-enter the username and password in order to connect to each camera

6.1.2 Multiple Camera Login

If you have multiple cameras with the same Login credentials, you can use the **Login All** button located on the top right hand corner of the CCT dashboard.
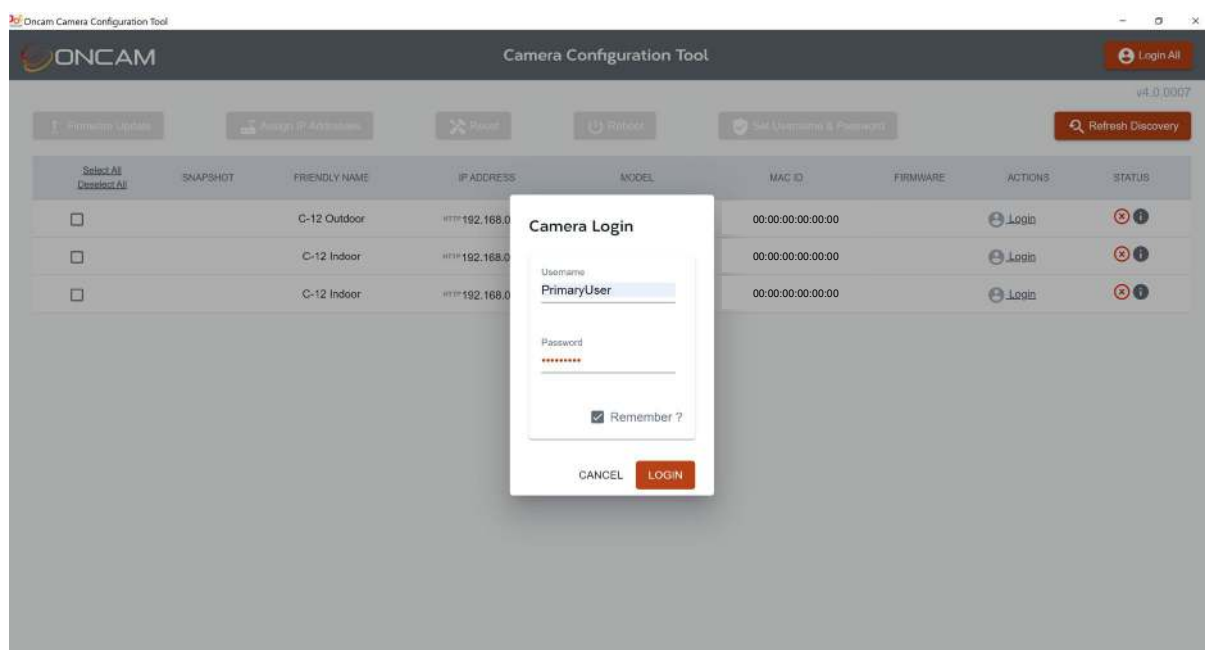
By selecting the **Remember** button the camera will be logged into automatically even if you refresh or close and open the CCT application. If at any point you want to stop this automatic login you can select the Bin icon next to **Remember.** This will be displayed the next time you select this button, this will remove the automatic login feature.

All cameras with the same credentials are logged into.

7. Camera Configuration

7.1 Dashboard – Camera Web Interface

Once you have created your Primary Administrator username and password, you can use these credentials to set up and configure the camera in one of the following ways:

1. ONVIF commands using your compatible VMS
2. The Camera Web Interface
3. The Camera Configuration Tool (opens Camera Web Interface within the tool)

To access the Camera Web Interface, type the IP address of the camera into a compatible web browser (supported browsers with minimum versions are: Chrome 84, Firefox 79, Edge 84 or Safari 13.1) and enter your username and password.

## 7.2 Dashboard – Camera Configuration Tool

The Camera Web Interface can also be accessed via the Camera Configuration Tool. Once you have logged into your camera click **Configure** under **ACTIONS** column next to the camera and this will open up the Camera Web Interface from within the configuration tool.

You will need to reauthenticate to access the Camera Web Interface:
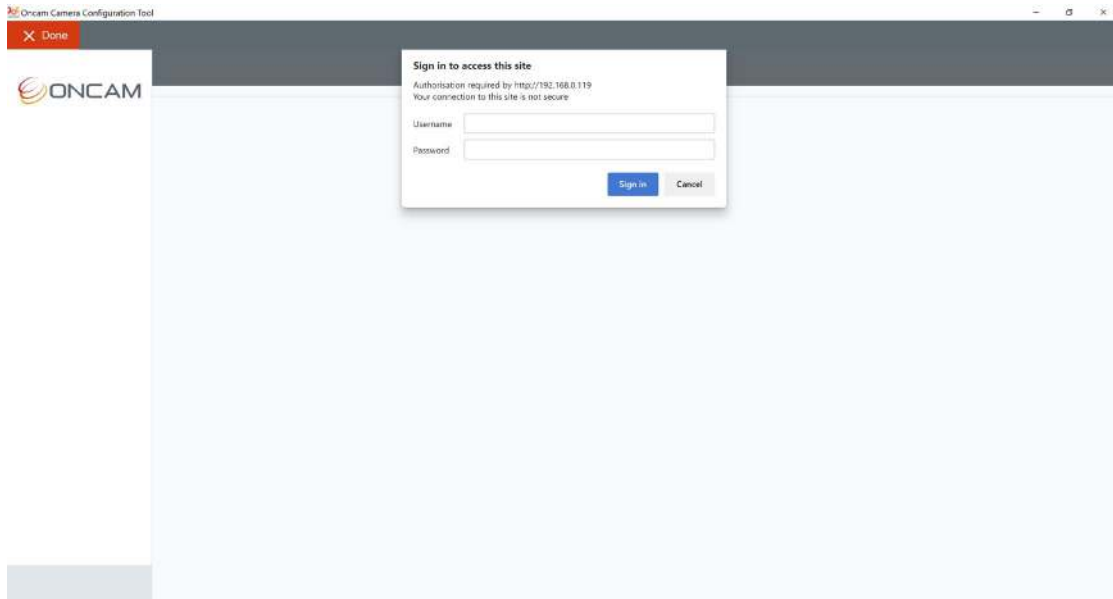
You will be presented with the main camera dashboard. From this page you can access all camera configuration settings, test the live stream, and set up the camera based on your requirements.

> Only Administrator level users will have access to camera settings, users with operator and user level privileges will only be able to view the dashboard page and the live stream.
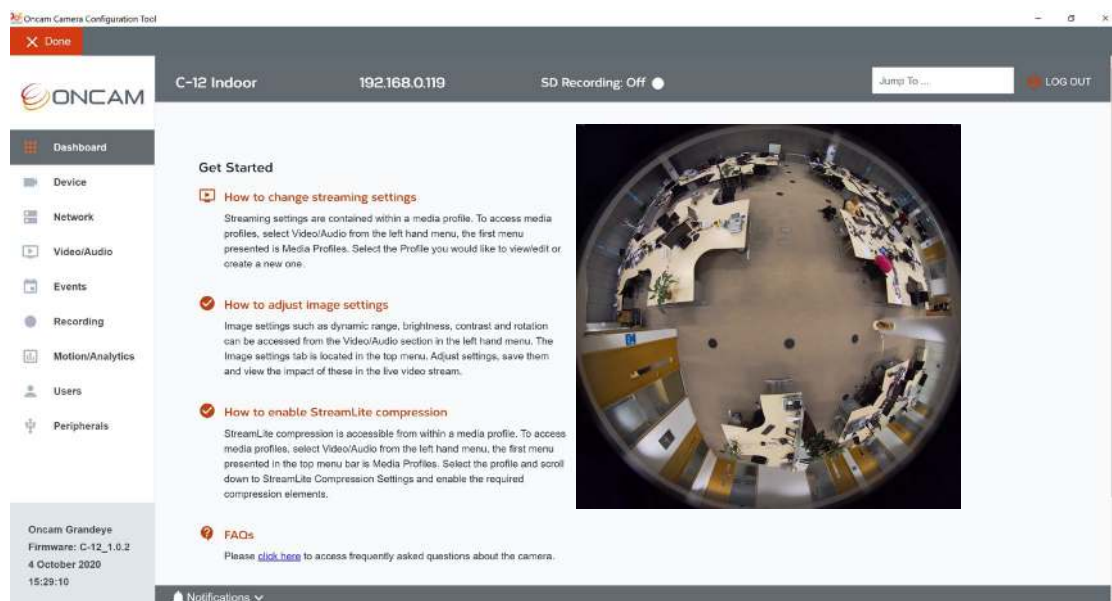
For full details and guidance on how to configure your camera (See Oncam C-12 Installation and User Manual section 5).

Please remember to save your changes as you progress through the configuration sections.

Once all changes have been made, select **Done** in the top left-hand corner to return to the CCT dashboard.

8. Assign IP Addresses

The camera can be configured with a manual Static IP Address. This will also require the Gateway to be set to allow communication with the outside network, and DNS addresses to resolve DNS names if required. On first time setup, the camera will need to be discovered using DHCP or Link Local (see section 4.2.1.)

The Static IP Address can then be set as follows to one or multiple cameras using the CCT.

Login to the cameras that require a Static IP Address assigned.

Select the cameras that require a Static IP addresses using the check box (single or multiple cameras can be selected) next to each camera, the **Assign IP Addresses** button on the top menu bar will be lit up red.

Select the **Assign IP Addresses** button.

A pop-up will be shown displaying the selected cameras.
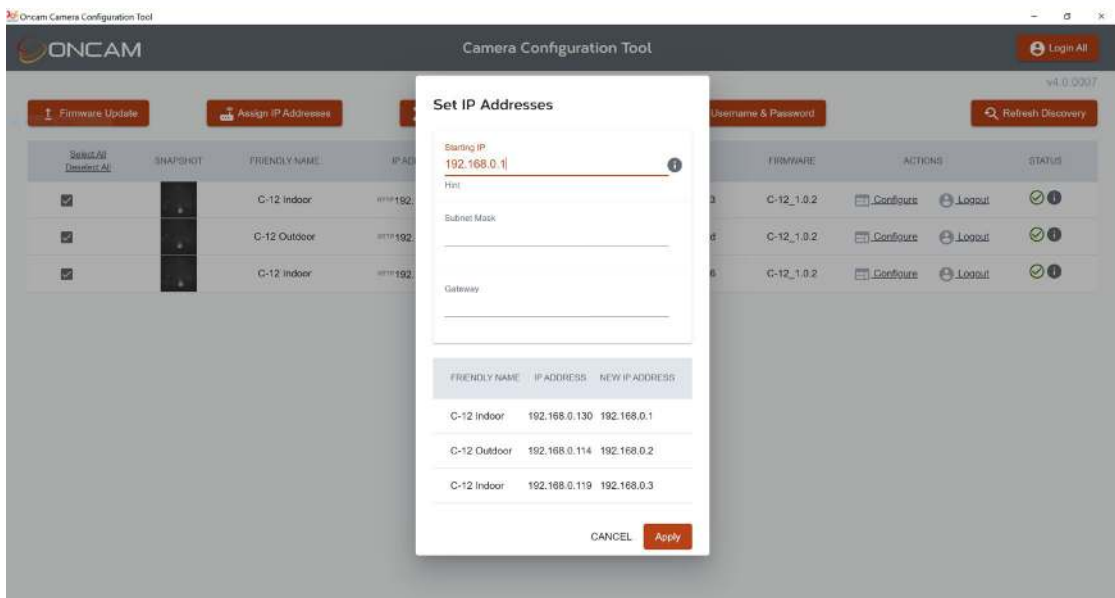
Enter the starting static IP address – ensure the selected Addresses are not already in use by other devices on the network.

Enter the subnet mask

Enter the Gateway address

Select **Apply**

Sequential Static IP Address will then be applied to each selected camera in order listed.

The pop-up will close and return to the CCT dashboard, the discovery will be automatically refreshed and the cameras will display the allocated Static IP addresses in the discovery list.

20

9. Firmware update

9.1 Check Camera Firmware Version

To take advantage of the camera's latest product and security features it is important to ensure you have the latest firmware installed.

The camera UI displays the currently installed firmware version on the bottom left of every page, as well as on the Device Information and Firmware tabs of the Device page.

The Camera Configuration Tool displays the firmware version for each camera in the Firmware column.

Visit https://www.oncamgrandeye.com to check the latest firmware available for the camera.

If a newer version of the firmware is available, check that your NVR/VMS version supports this latest firmware and download the file. The firmware can be updated in two ways:

1. The Camera Web Interface (single camera)
2. The Camera Configuration Tool (single or multiple cameras)

9.2 Camera Configuration Tool – Firmware Update
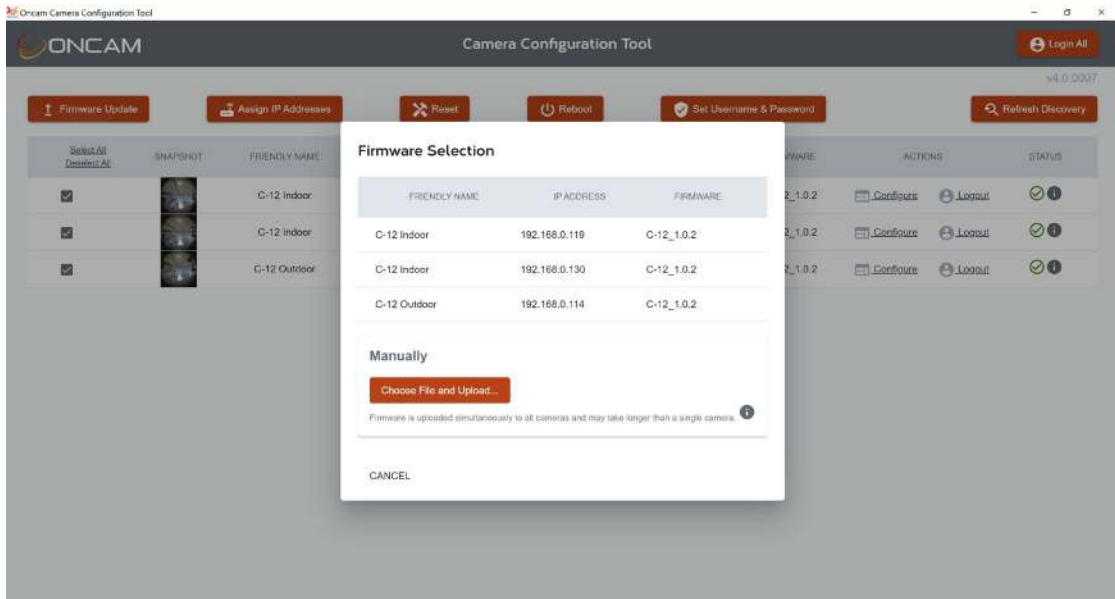
9.2.1 Firmware update process

Login to the cameras that require updating.

Select the cameras that require updating using the check box (single or multiple cameras can be selected) next to each camera, the Firmware Update button on the top menu bar will be lit up red.
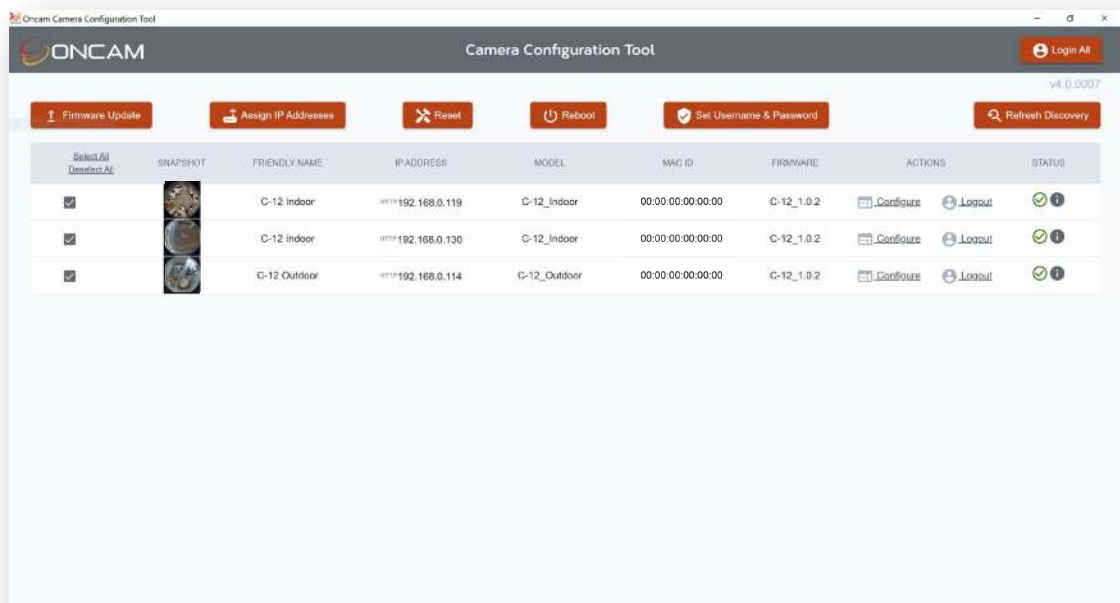
Select the **Firmware Update** button.

A pop-up will be shown confirming the list of cameras to be updated, including their current firmware version.
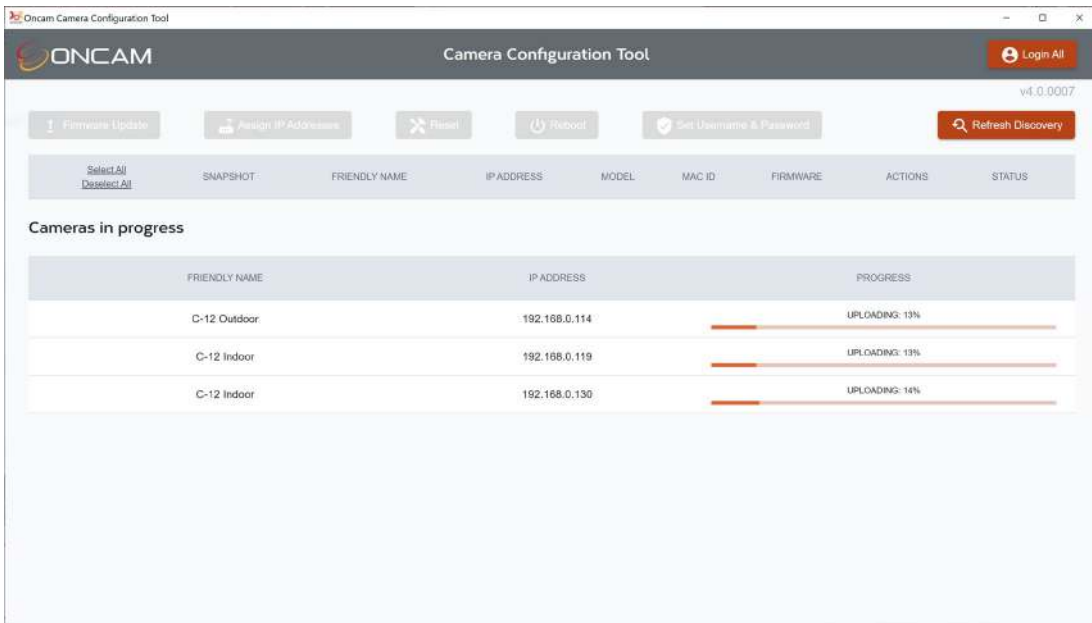

Select the **Choose File and Upload** button.

Navigate to the location where the new firmware file is saved. Select the file and click open to begin the update process.

The pop up will close, and you will return to the CCT dashboard. The camera will be displayed in **Cameras in progress** section of the dashboard.
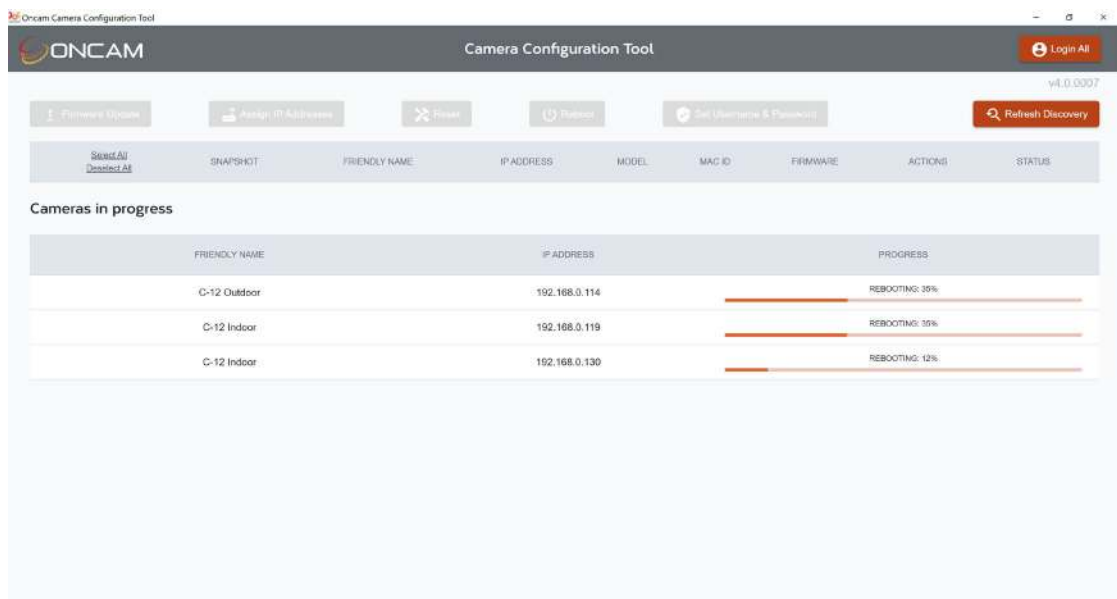The new firmware will be validated and uploaded to each camera.

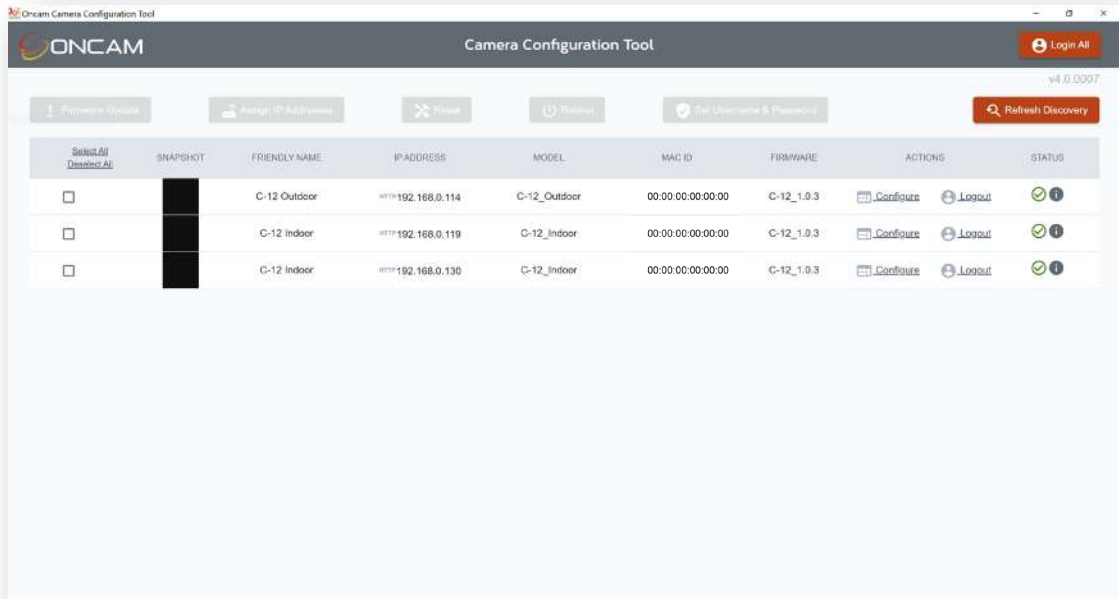During each stage progress bars will be displayed for each camera.
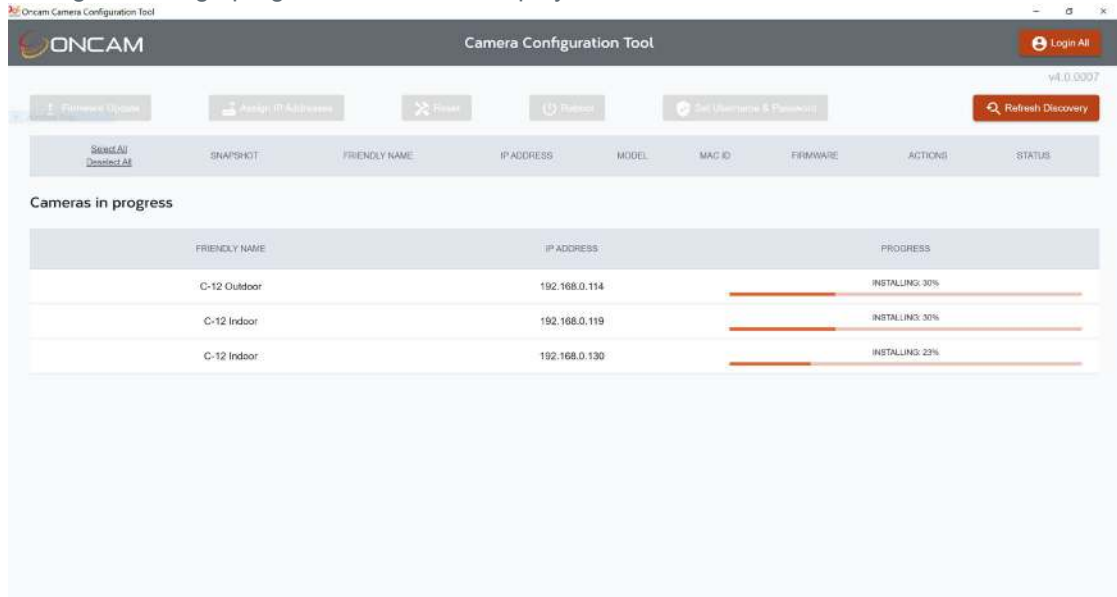
Once a Firmware Update process has started on one or more cameras, another Firmware Update process cannot be initiated from the CCT until the first process has finished.
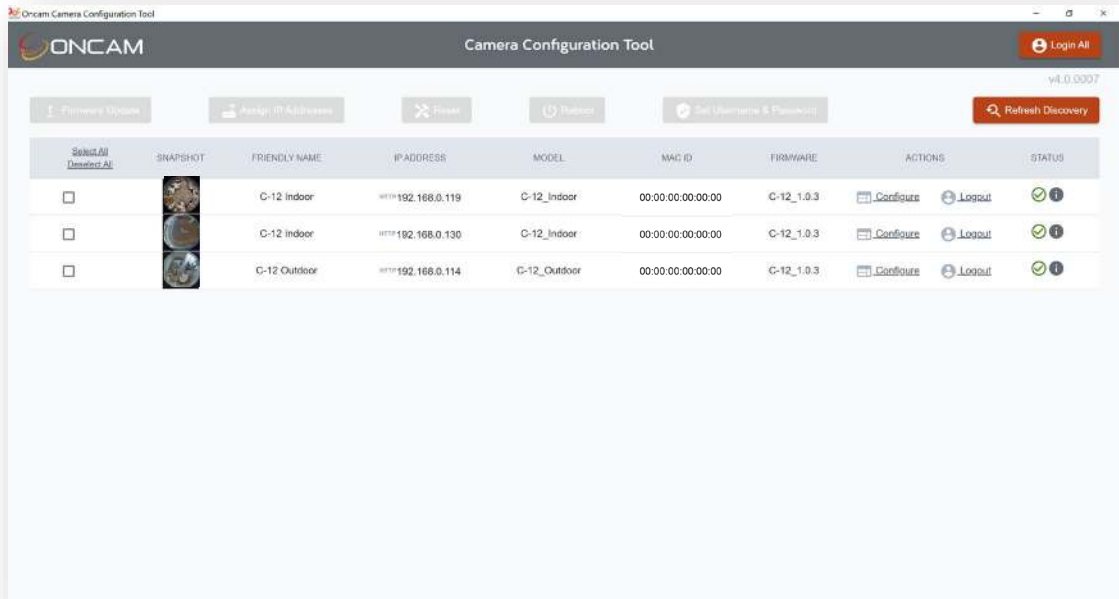
Once complete each camera will be rebooted.

Once rebooted the cameras will be displayed in the discovered list.

The snapshot image may display as blank or black as above (known issue), to see the latest snapshot click the discovery button.

The upgrade time for each camera will vary based on network speed and traffic.
To confirm the new firmware version has been applied, check the firmware version number displayed in the discovery table under **Firmware**.

All camera settings will be retained after the firmware update process.

10. Reboot

From time to time the camera may need to be restarted (for instance when a significant configuration change is made or when there are changes to external systems affecting the camera).

The camera can be rebooted in two ways:

1. Via Software Tools – Camera Web interface (See Oncam C-12 Installation and User Manual section 5.8.3.2) and Camera Configuration Tool (See below)

2. Via physical button press (See Oncam C-12 Installation and User Manual section 5.8.3.2)

10.1 Camera Configuration Tool – Reboot

Login to the cameras that require rebooting.

Select the cameras that require rebooting using the check box (single or multiple cameras can be selected) next to each camera, the **Reboot** button on the top menu bar will be lit up red
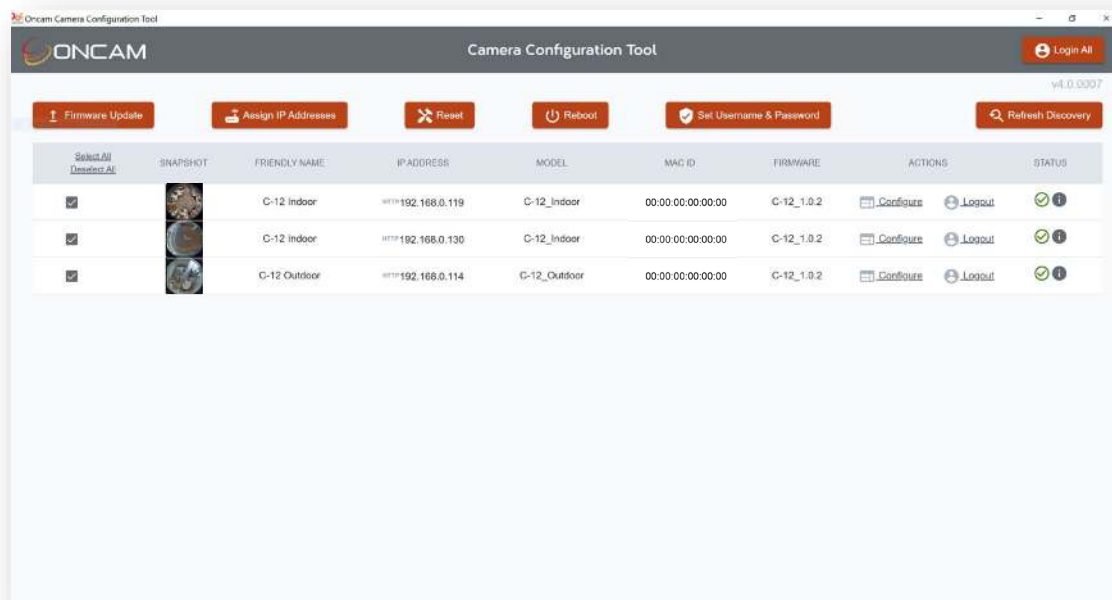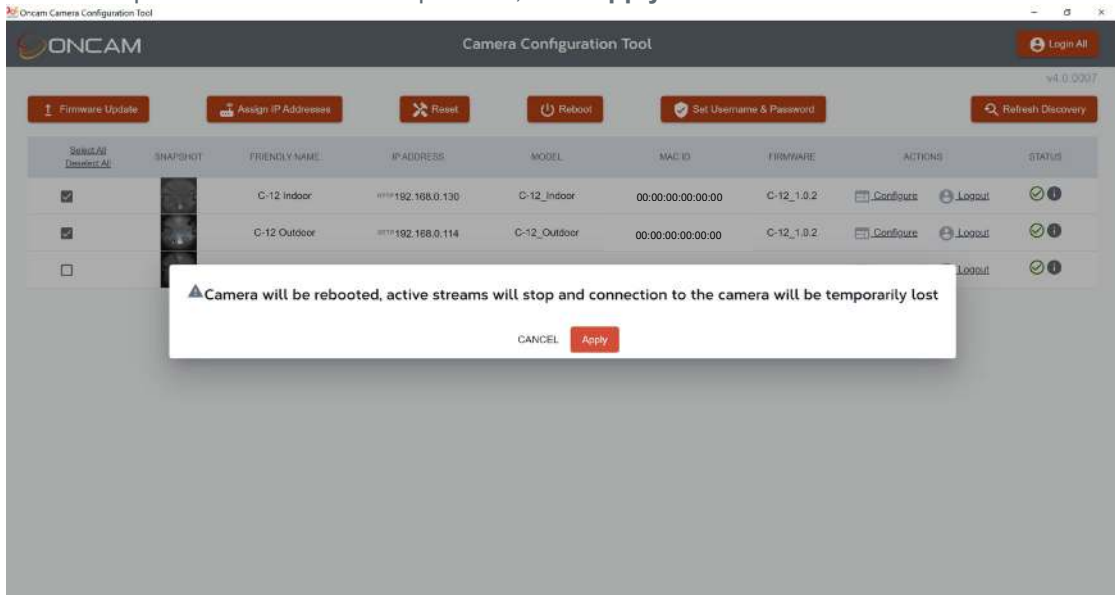

Select the **Reboot** button.

A pop-up will be shown displaying the list of cameras to be rebooted based on your selection, click **Apply**.
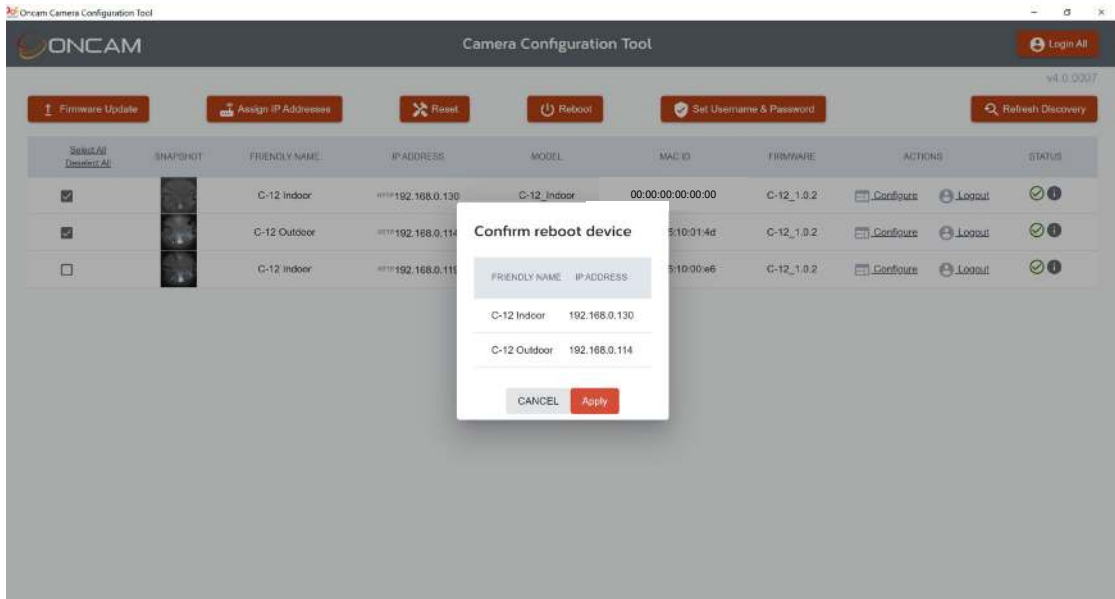
A warning will be shown to advise that all active streams will be stopped and restarted due to the reboot process. If would like to proceed, click **Apply.**

The pop-up will close, and you will return to the CCT dashboard. The cameras will be listed in the **Cameras in progress** section of the dashboard. Individual progress bars will be displayed on screen while the cameras are rebooted.
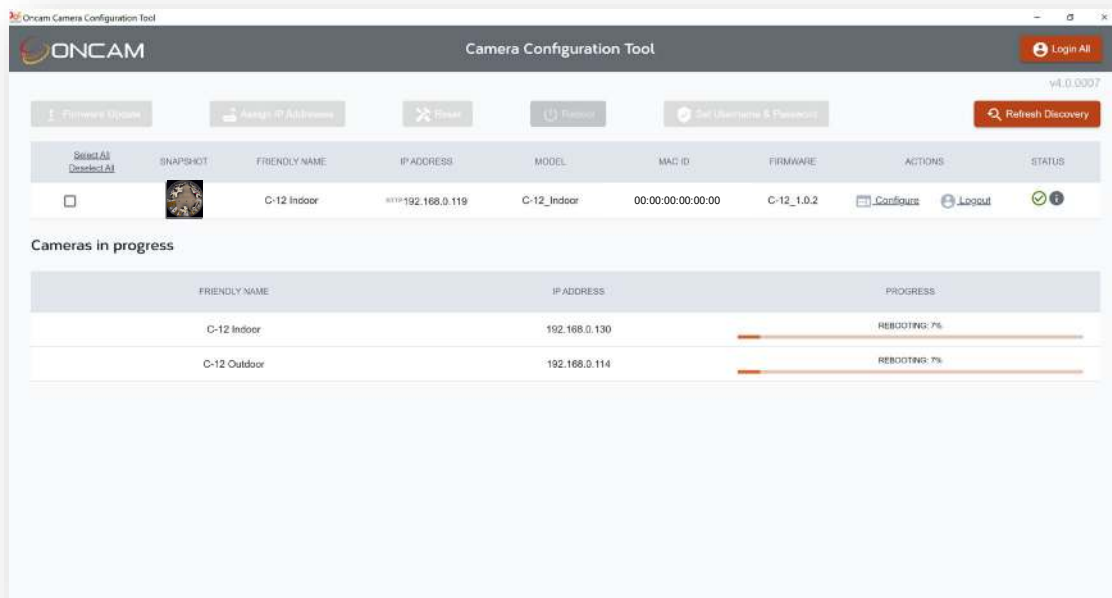
Once rebooted the cameras will be displayed in the discovered list.

11. Reset to Factory Defaults

The camera may require a reset to factory defaults if unknown configuration changes have been made and you want to start from a default state.

> This option will overwrite existing settings therefore careful consideration is required before applying it.

Three levels of reset to factory defaults are supported:
1. All Settings.
2. All settings except the IP Settings - Essential IP settings are retained- IP Address, subnet mask, Gateway, DNS, NTP, HTTP and HTTPS ports.
3. User accounts only - all other settings will remain.

The camera can be reset to factory defaults in two ways:

1. Via Software Tools – Camera Web interface (See Oncam C-12 Installation and User Manual section 5.8.3.3) and Camera Configuration Tool (See below)

2. Via Physical Button Press (See Oncam C-12 Installation and User Manual section 5.8.3.3)

11.1 Camera Configuration Tool – Reset

Login to the cameras that require a reset.

Select the cameras that require resetting using the check box (single or multiple cameras can be selected) next to each camera, the **Reset** button on the top menu bar will be lit up red.

Select the **Reset** button.

A pop-up will be shown displaying the list of cameras to be reset based on your selection.
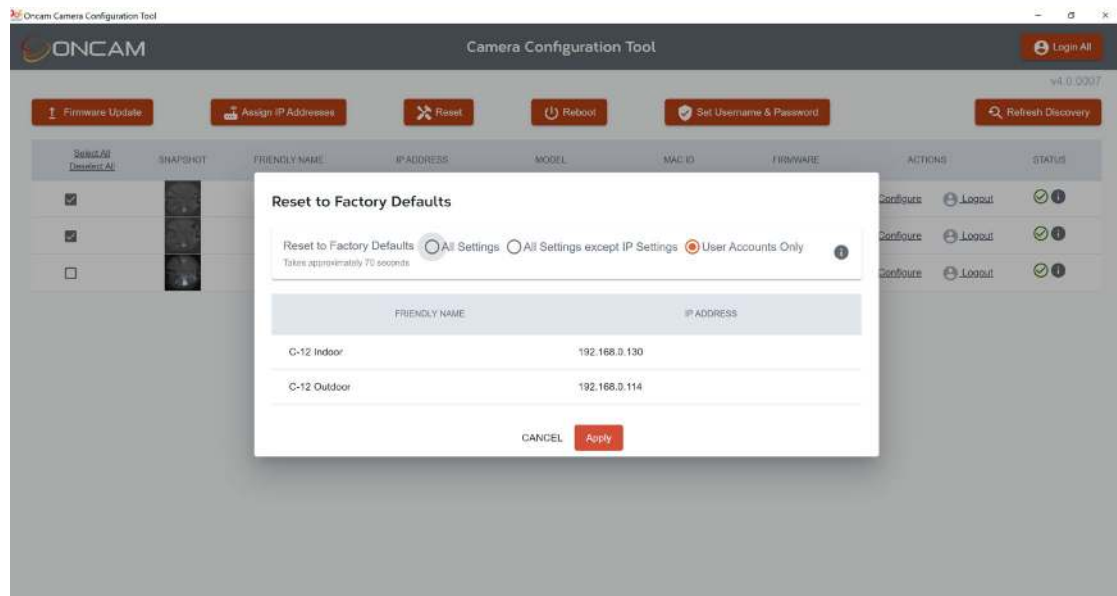
Select the preferred reset option and **Apply.**

A warning will be shown to advise that all active streams will be stopped due to reset process. If would like to proceed, click **Apply.**

> ⚠️ Camera: This option will overwrite current cameras settings.
>
> MicroSD Card: if the camera is Reset to Factory Defaults and has a microSD card, recorded files and recording configuration data will not be deleted from the microSD card. The recording configurations will be copied to the camera once the camera restarts, however the recording configurations will be changed to an inactive state and will need to be activated to restart local recording on the microSD card. The previous recorded data is still searchable and can be downloaded. To delete it, the recording configuration needs to be deleted. In the Camera Web Interface, go to Recording > Recording Configuration and select Delete button next to the recording configuration in the summary table.
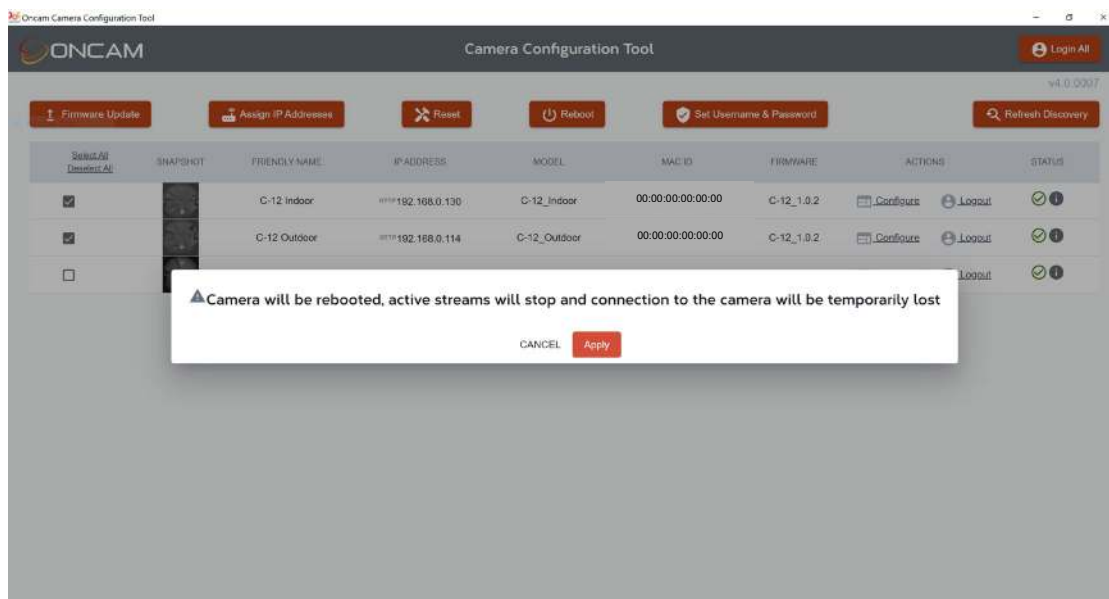
The pop up will close, and you will return to the CCT dashboard. The cameras will be listed in the **Cameras in progress** section of the dashboard. Individual progress bars will be displayed on screen while the reset takes effect.

Once the reset process is complete, the cameras will be displayed in the discovered list.
As the cameras have been Reset to Factory defaults, the primary administrator username and
password will need to be set for the selected cameras, therefore **Set Password** will be shown
in the **ACTIONS** column for the reset cameras.