

# CamTrace

**videosurveillance**

## Quick Setup guide

**For CT-Server : V9.16.x**

**Document version : v1.3**

**Creation date of the document : 10/08/2022**

**Last modification date of the document : 22/02/2024**

For further information :

**[www.camtrace.com](http://www.camtrace.com)**

# Table des matières

<b>1</b>	<b>Lexicon.....</b>	<b>3</b>
<b>2</b>	<b>Start-up and access to the administration panel.....</b>	<b>4</b>
<b>2.1</b>	<b>Power up and shut down.....</b>	<b>4</b>
2.1.1	Power up.....	4
2.1.2	Shut down.....	5
<b>2.2</b>	<b>Power up and shut down without monitor.....</b>	<b>5</b>
<b>2.3</b>	<b>Administration panel access from the CT-Server machine, or from a remote machine.....</b>	<b>6</b>
2.3.1	Using the administration panel locally.....	6
2.3.2	Using the administration panel from a remote machine.....	8
<b>3</b>	<b>Adding the license key.....</b>	<b>9</b>
<b>4</b>	<b>System configuration.....</b>	<b>10</b>
<b>4.1</b>	<b>Storage space management.....</b>	<b>10</b>
<b>4.2</b>	<b>Network settings.....</b>	<b>13</b>
4.2.1	General information and recommendations.....	13
4.2.2	Information to be collected to connect to an existing network.....	14
4.2.3	IP address assignment.....	14
4.2.4	Network identity, gateway, DNS servers.....	15
<b>4.3</b>	<b>Server time.....</b>	<b>16</b>
<b>5</b>	<b>Cameras configuration.....</b>	<b>17</b>
<b>5.1</b>	<b>List of actions to be performed on each camera.....</b>	<b>17</b>
<b>6</b>	<b>Camera detection.....</b>	<b>18</b>
<b>6.1</b>	<b>ONVIF detection.....</b>	<b>18</b>
<b>7</b>	<b>Regular recording and alarm recording.....</b>	<b>20</b>
<b>7.1</b>	<b>Add recordings on a camera.....</b>	<b>20</b>
7.1.1	'Records' section.....	21
7.1.1.1	Regular recording.....	21
7.1.1.2	Alarm recording.....	21
7.1.2	Motion detection performed by the CT-Server.....	22
<b>8</b>	<b>Saving the configuration.....</b>	<b>25</b>

# 1 Lexicon

**Administration panel** : The entire administration of the CT-Server is done using a web-based interface accessible from the Firefox browser installed on the CT-Server, or from any other machine on the network via the browser of your choice (preferably: Firefox, Edge, Chrome).

**CT-Client** : Fat client software that runs on Windows/MAC/Linux. It is used by the operator or security officer (to connect to the CT-Server).

**CT-Mobile** : Mobile app that runs on iOS or Android. It is used by the operator or security officer (to connect to the CT-Server).

**CT-Server** : CamTrace server.

**Data disk** : Disk used for data (recordings of cameras). It is often a hard disk (with or without RAID).

**Mosaic** : View consisting of several cameras. This view is visible from the CT-Client or CT-Mobile.

**System disk** : Disk used for the OS. We recommend using SSD.

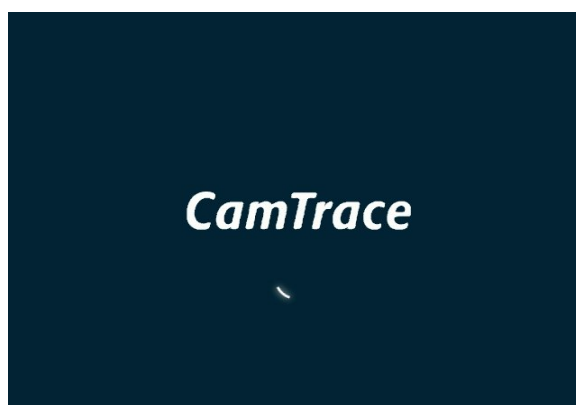
## 2 Start-up and access to the administration panel

### 2.1 POWER UP AND SHUT DOWN

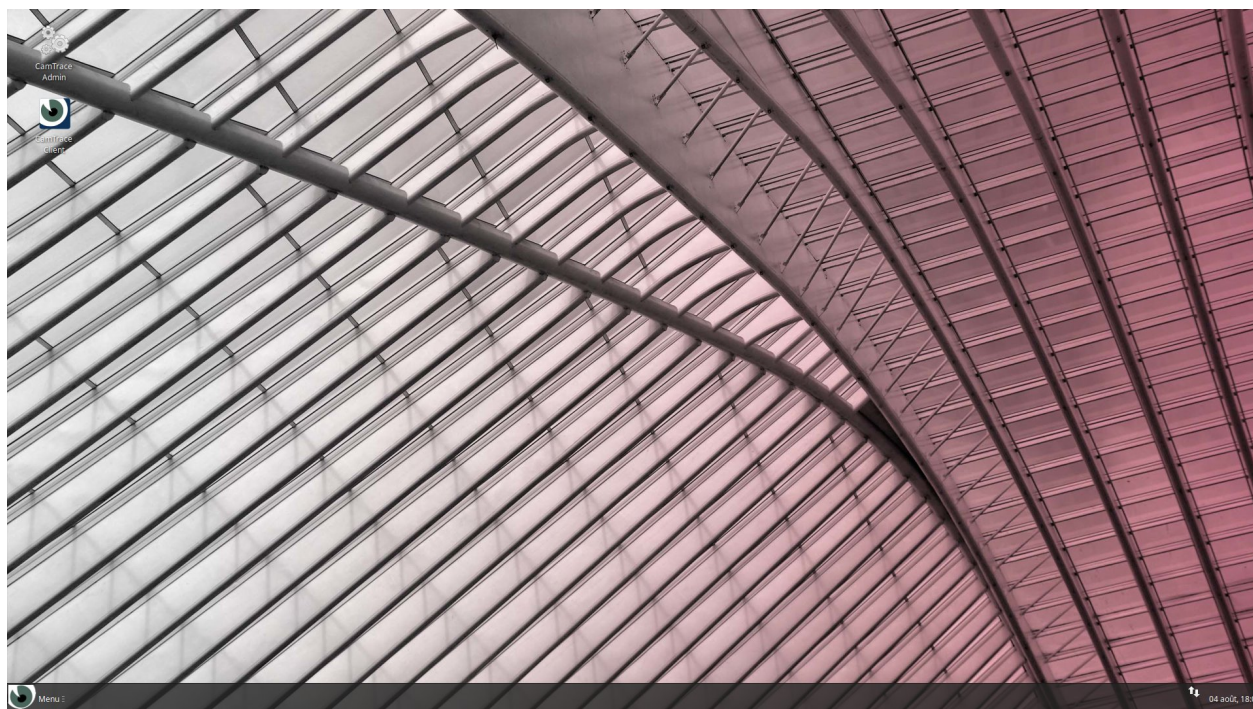
A CT-Server is usually delivered without a monitor. Make sure you have a monitor, keyboard and mouse. During operation, it is advisable to add an inverter on the CT-Server's power supply, to avoid unwanted interruptions. Once powered, you can start the server.

#### 2.1.1 Power up

On start-up, 'CamTrace' is displayed on the screen:

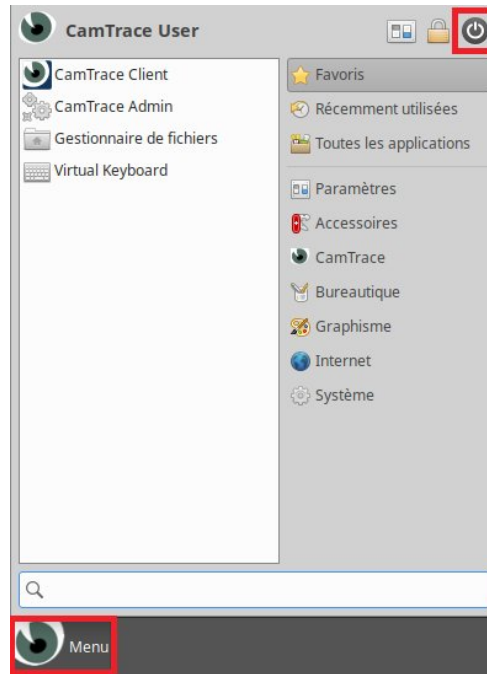


The screen then displays the CamTrace OS desktop:



## 2.1.2 Shut down

To turn off the system, click on Menu (see below) then on the logout button and choose 'Turn off':



A CT-Server is designed to operate 24 hours a day. It should never be switched off by removing the power cable.

## 2.2 POWER UP AND SHUT DOWN WITHOUT MONITOR

If you do not have a monitor connected to the CT-Server: press the 'Start/Stop' button on your server. At the end of the start-up procedure, a series of beeps informs you that the server has finished starting and your server is accessible via your local network. To stop the server, briefly press the 'On/Off' button and wait for the server to shut down.

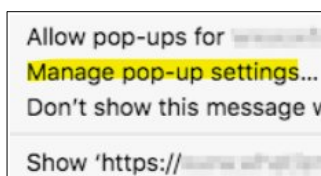
## 2.3 ADMINISTRATION PANEL ACCESS FROM THE CT-SERVER MACHINE, OR FROM A REMOTE MACHINE

There are two choices for configuring the CT-Server. You can do it locally on the CT-Server machine (read Using the administration panel locally chapter), or you can configure from a remote machine -the remote machine must be on the same network (read Using the administration panel from a remote machine).

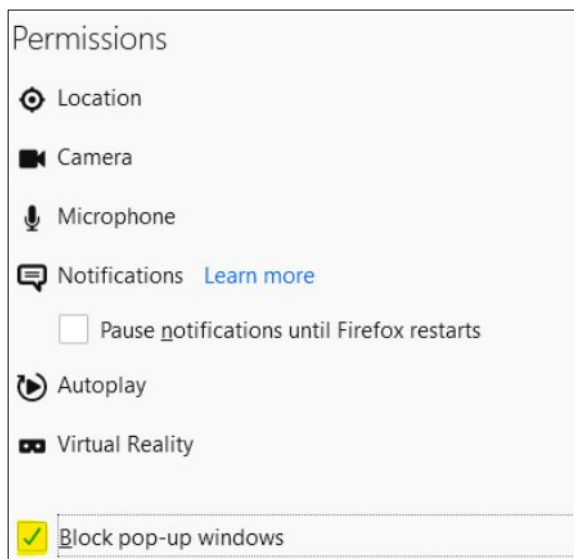
### 2.3.1 Using the administration panel locally

To configure the CT-Server, you must use the server administration panel. Click on the 'CamTrace Admin' shortcut on the OS desktop.

A web browser (Firefox) will be launched. You must allow popups by choosing 'Preferences' and then 'Manage popup settings':



Disable it by **unchecking** the 'Block pop-up windows' field (see below) :



When the popups have been authorised, the administration panel is displayed:



The image shows the CamTrace administration panel login interface. At the top left is the CamTrace logo, which consists of a stylized camera lens icon and the text 'CamTrace' in a bold, white, sans-serif font. Below the logo are three input fields: 'Nom d'utilisateur :', 'Mot de passe :', and 'Langue : Français'. The 'Langue' field is a dropdown menu with a small downward arrow. At the bottom of the form are three buttons: 'Entrer', 'Annuler', and 'Fermer'.

Username : **admin**

Password : **camtrace**

Choose your language before clicking on '**Entrer**' / '**Enter**'.

To log out, use the logout button:



### 2.3.2 Using the administration panel from a remote machine

It is also possible to configure the CT-Server if you do not have a monitor connected to the CT-Server. The primary network interface has the default address 192.168.0.100/24.

*Note: If the CT-Server has a second interface, it has the address 192.168.1.100/24.*

You can connect to the CT-Server and configure it using a web browser. To avoid incompatibilities, it is recommended to use Firefox, Edge or Chrome in Private mode, from another remote machine (PC, laptop...).

Start the CT-Server until you hear the beeps. Set your PC to an address on the 192.168.0.0/24 network (for example 192.168.0.2). Connect the PC (using a crossover cable or switch) to one of the network interfaces. Issue a 'ping 192.168.0.100' command to the server. If it does not respond, change the network connector on the server and ping it again until you find the server's primary interface.

When your client PC is connected to the same network as your CT-Server, go to 'http://192.168.0.100' using your web browser.

An authentication popup is displayed (you have to allow popups on your web browser):

The image shows a web browser authentication popup for CamTrace. At the top left is the CamTrace logo, which consists of a stylized camera lens icon and the text 'CamTrace' in a bold, white, sans-serif font on a dark blue background. Below the logo, there are three input fields: 'Nom d'utilisateur :', 'Mot de passe :', and 'Langue :'. The 'Langue' field is a dropdown menu currently set to 'Français'. At the bottom of the form are three buttons: 'Entrer', 'Annuler', and 'Fermer'.

Username : **admin**  
Password : **camtrace**

Choose your language before clicking on '**Entrer**' / '**Enter**'.

To log out, use the logout button:





### 3 Adding the license key

On the administration panel, select 'Help' then 'About'.

If it says 'DEMO' on the 'License Status' line, you need to add the license key to the CT-Server.

From the administration panel, select 'Help' then 'Update'. Go to the 'Update your licence key' section.

Check 'Send license key file' (**do not check** the 'Reset system administration password' option) and then click 'Choose file'.

Select the license key. The license key is a file named :

'**SERIAL**\_DATEOFGENERATION.key'.

For example :

**1117\_2022-08-11-16-01-20**.key

**If the licence key has been added correctly**, a popup will indicate 'The licence key has been updated successfully'.

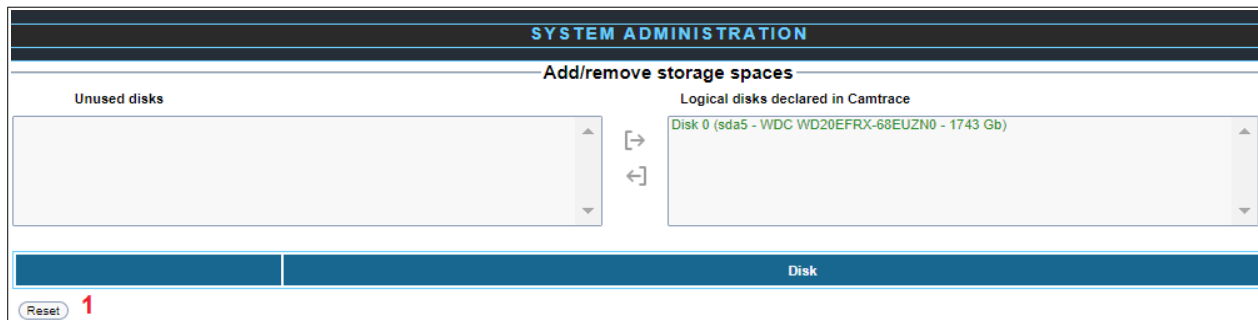
*Note: If you are working on CT-Server locally, you can transfer the licence key to the CT-Server using a USB key.*

## 4 System configuration

### 4.1 STORAGE SPACE MANAGEMENT

On the administration panel, select 'Manage' then 'System' and refer to the 'Add/remove storage spaces' section.

If your machine has several disks, you must declare which disks can be used by the CT-Server.



On the left column (named 'Unused disks') are listed the unused disks that you can declare.

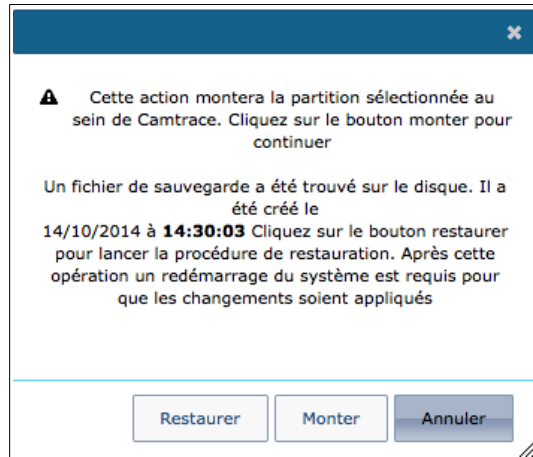
If you need to reset (format) a disk, you can do this via the bottom section (see [1] above): select the disk(s) to be formatted and then click 'Reset'. All data on the selected disk(s) will be erased. **If you have a doubt, it is best to reset the disk to make sure it is empty before use.**

Select the disk you want to mount (from the 'Unused disks' section) and then click on the mount button [→].

A confirmation popup appears. There are two possible scenarios :

- A backup configuration file has been found :

When mounting a disk, it may contain a backup of a previous CamTrace installation (after a reinstallation on the System disk for example). If this is the case, a message proposes to restore this backup.

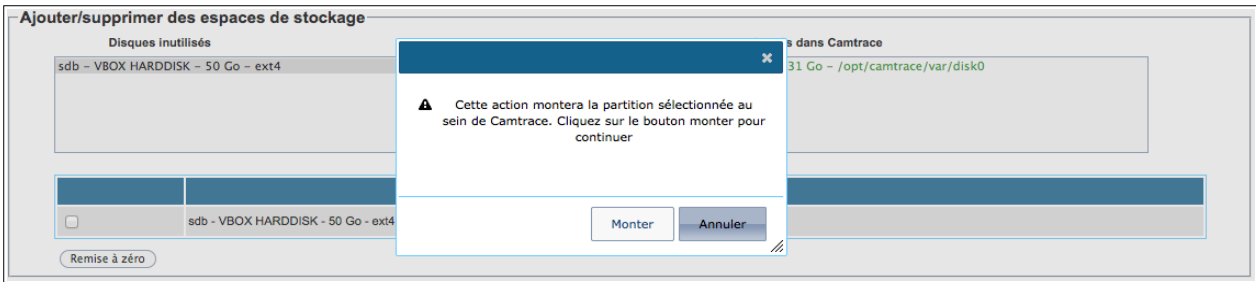


If you wish to restore the configuration from the previous CamTrace installation, click 'Restore'. Otherwise, ignore this backup by choosing 'Mount'.

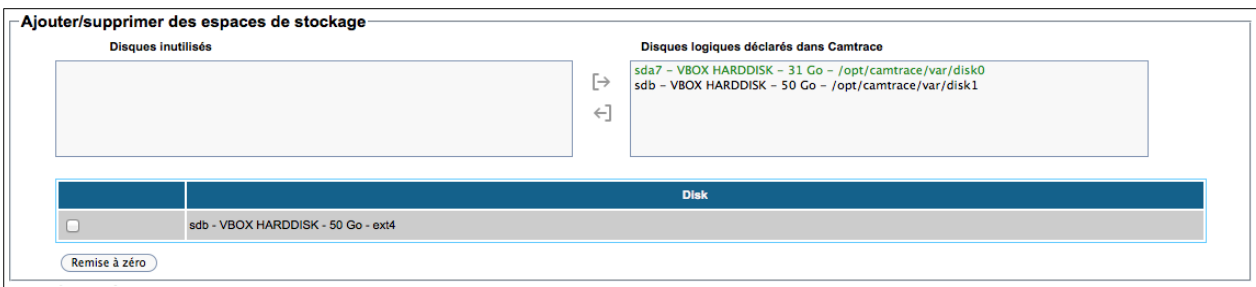
If you choose to 'Mount', **you will not be able to 'Restore' afterwards.**

*Note: If you clicked on 'Mount' when you wanted to retrieve the configuration because there are records on the Data disk, you can go to the 'Manage' interface and then 'Disk usage' and launch the 'Check' process on all cameras. After the 'Check' process is finished, you should be able to retrieve all your cameras recordings.*

- No backup file has been found :



Confirm by clicking on 'Mount'. Your disk is now usable as storage space in the administration panel.



Note : Using the ←] button will unmount a storage space.

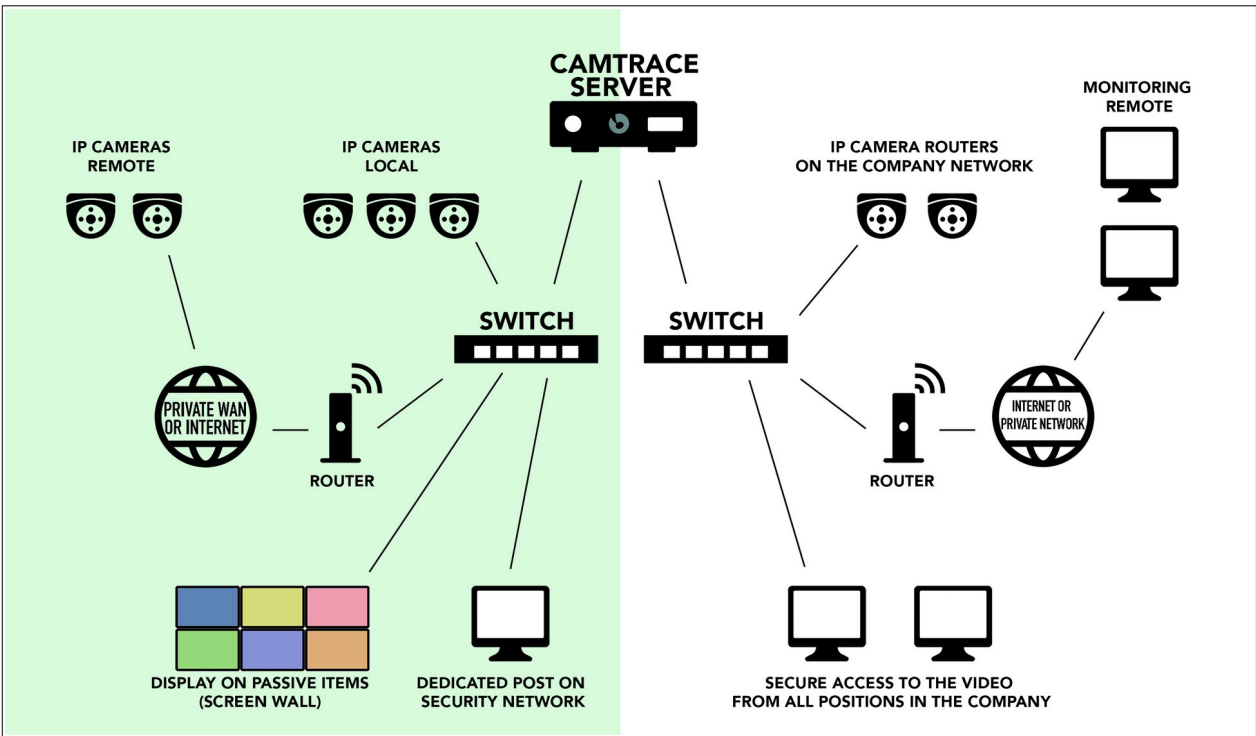
## 4.2 NETWORK SETTINGS

### 4.2.1 General information and recommendations

A CT-Server has one or more network cards (usually two network cards).

Although it is possible to mix cameras and visualisation stations on all networks, it is recommended to specialise the networks.

For example, it is recommended to group cameras on one or more security networks and to use another network interface to connect to the corporate/organisational network. It is also possible to use another interface to connect to a display network (guard station and display PC).



This separation of networks optimises the performance and security of your video installation. When multiple CT-Servers are used, it is recommended that the cameras attached to each CT-Server are isolated on separate networks. For smaller installations, it is possible to use only one network card.

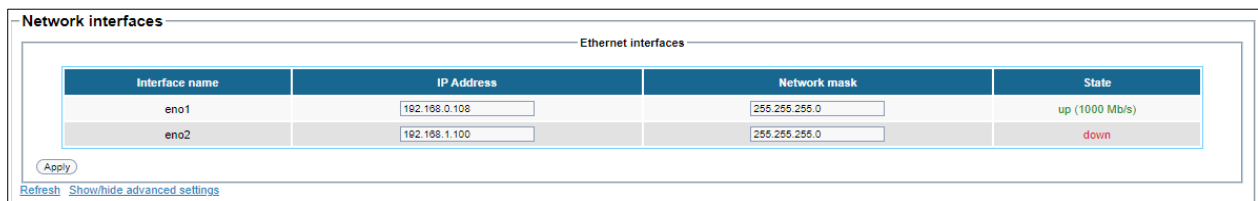
Preferably use a Gigabit link between the CT-Server and the switches: if the network has more than ten cameras, Gigabit becomes necessary.

## 4.2.2 Information to be collected to connect to an existing network

- IP address for your CT-Server on the company network.
- Network mask.
- Network name for the CT-Server. The 'network name' is the name you will give to the CT-Server on the local network. If the company has a DNS, it is recommended that this name is consistent with the name given to the CT-Server in that DNS.
- IP address of an internal or external DNS.
- IP address of the default gateway.

## 4.2.3 IP address assignment

On the administration panel, select 'Manage' then 'System' and refer to the 'Network interfaces' section.



The screenshot shows a web interface for configuring network interfaces. The main heading is "Network interfaces" and the sub-heading is "Ethernet interfaces". Below this is a table with four columns: "Interface name", "IP Address", "Network mask", and "State".

Interface name	IP Address	Network mask	State
eno1	<input type="text" value="192.168.0.108"/>	<input type="text" value="255.255.255.0"/>	up (1000 Mb/s)
eno2	<input type="text" value="192.168.1.100"/>	<input type="text" value="255.255.255.0"/>	down

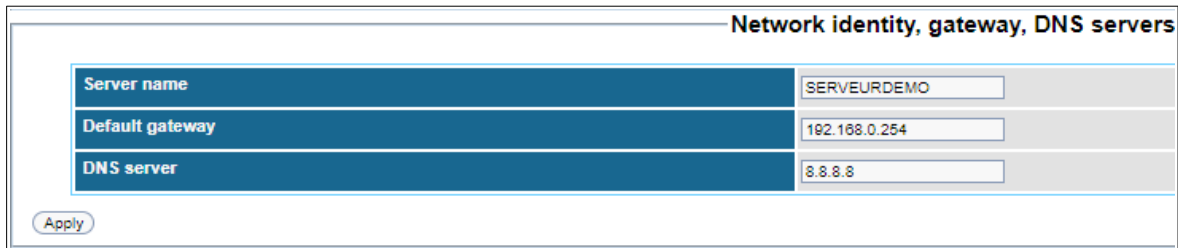
Below the table, there is an "Apply" button and a "Refresh" button. A link "Show/hide advanced settings" is also present.

Edit the 'IP Address' and 'Network Mask' fields according to your local network configuration. You must allocate addresses belonging to different networks on its different interfaces, **otherwise serious malfunctions may occur**.

**Warning:** if you are configuring the CT-Server from a remote machine (see Using the administration panel from a remote machine): you will lose the network connection to your CT-Server when you click on 'Apply', and you will have to connect your machine on the new network.

#### 4.2.4 Network identity, gateway, DNS servers

On the administration panel, select 'Manage' then 'System' and refer to the 'Network identity, gateway, DNS servers' section.



Network identity, gateway, DNS servers	
Server name	SERVEURDEMO
Default gateway	192.168.0.254
DNS server	8.8.8.8

Apply

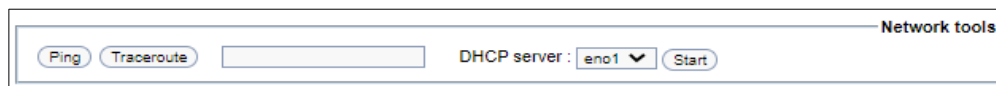
In the 'DNS server' field, you can either :

- Leave the field empty,
- Enter the IP address of the internal DNS if it exists,
- Enter the IP address of the company's Internet Service Provider's DNS,
- Enter the IP address of a public DNS server, for example: '8.8.8.8'.

**Warning:** If the address range of the name server (DNS) is different from those used on the CT-Server networks, the gateway must be filled in.

If you are not sure of the DNS address, leave the field empty. A wrong value would **cause strong slowdowns**.

To test the configuration, you can use the network tools available in the 'Network Tools' section.



Ping Traceroute  DHCP server : eno1 Start

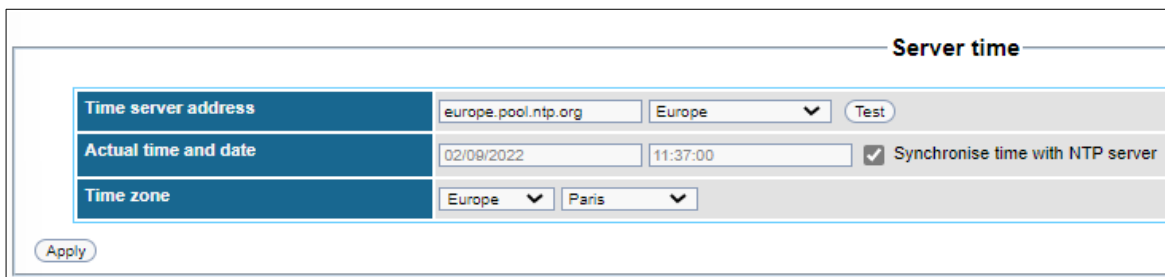
### 4.3 SERVER TIME

On the administration panel, select 'Manage' then 'System' and refer to the 'Server time' section.

You must set the time and time zone of your server. CamTrace automatically handles winter and summer time. You simply enter the current local time.

However, it is recommended that you fill in the 'Time Server Address' field, in order to declare an NTP server that will be used for server synchronisation.

To add a time server, enter for example '**europe.pool.ntp.org**' (or '**pool.ntp.org**' if the CT-Server is not located in Europe) :



The screenshot shows the 'Server time' configuration panel. It contains the following fields and controls:

- Time server address:** A text input field containing 'europe.pool.ntp.org', a dropdown menu set to 'Europe', and a 'Test' button.
- Actual time and date:** Two text input fields for date and time, containing '02/09/2022' and '11:37:00' respectively, followed by a checked checkbox labeled 'Synchronise time with NTP server'.
- Time zone:** Two dropdown menus, the first set to 'Europe' and the second set to 'Paris'.
- An 'Apply' button is located at the bottom left of the panel.

and click on '**Test**' to check that the server is responding. If OK, a '**Server has responded**' message is displayed. Check 'Synchronise with time server' and click 'Apply'.



## 5 Cameras configuration

It is imperative to perform the operations described below **BEFORE** declaring the cameras on the CT-Server.

### 5.1 LIST OF ACTIONS TO BE PERFORMED ON EACH CAMERA

> **Give the camera a fixed IP address.**

Make sure that DHCP is not activated. Enter the network gateway of the camera.

> **Activate the camera's ONVIF profile.**

It is recommended to choose an identical user/password combination for logging in to the camera's administration interface and for the ONVIF profile.

> **Set the camera's time.**

You can set the time manually or (preferably) by specifying an NTP server. The CT-Server can be used as an NTP server.

> **Activate at least two video streams in the camera :**

Set the first stream as a **high quality stream**. E.g. : **1920\*1080** with **12 frames per second (FPS)**.

Set the second stream as a **standard (medium) quality stream**. E.g. : **640\*480** with **12 frames per second (FPS)**. This stream is useful for displaying many cameras in a mosaic.

If your camera allows you to create a third stream : set the third stream as a **low quality stream**. E.g. : **320\*240** with **12 frames per second (FPS)**. This stream is useful for displaying many cameras in a mosaic.

## 6 Camera detection

On the administration panel, select 'Manage' then 'System' and refer to the 'Add camera' section.

**You should not detect/connect** cameras to the CT-Server if the cameras have not been configured correctly beforehand, see Cameras configuration.

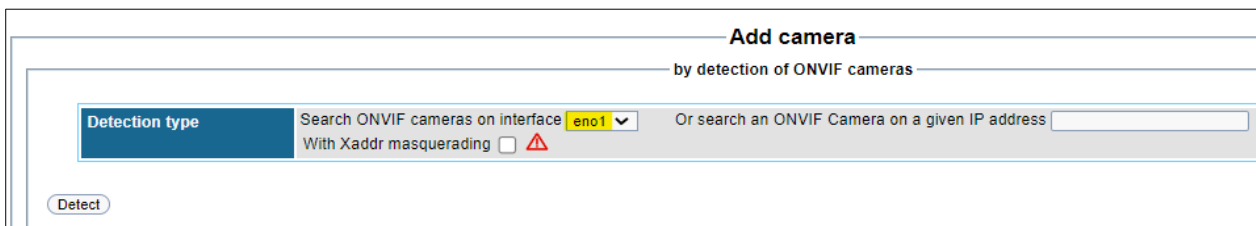
If ONVIF detection works for your camera, **it is recommended to add your cameras using ONVIF.**

**It is not recommended to add the camera manually** from the 'Manage' page then 'Cameras' then 'Add a new camera'.

### 6.1 ONVIF DETECTION

Refer to the 'by detection of ONVIF cameras' section.

Make sure that the camera detection is done on the appropriate network interface (see yellow field, in the picture below):



The screenshot shows a web interface titled "Add camera" with a sub-section "by detection of ONVIF cameras". It features a "Detection type" dropdown menu, a search field for "Search ONVIF cameras on interface" with a dropdown menu showing "eno1" (highlighted in yellow), and a search field for "Or search an ONVIF Camera on a given IP address". There is also a checkbox for "With Xaddr masquerading" and a warning icon. A "Detect" button is located at the bottom left.

**You should not detect/connect** cameras to the CT-Server if the cameras have not been configured correctly beforehand, see Cameras configuration.

If cameras have been detected, they are displayed in the '**Newly detected cameras**' section:

Newly detected cameras									
	Disk	Name	View code	More information	IP Address	Port	PTZ	Username	Password
<input type="checkbox"/>	0						if avail.		
<input type="checkbox"/>	0	CT_camera_21	21		192.168.0.21	80	if avail.		
<input type="checkbox"/>	0	CT_camera_29	29		192.168.0.29	80	if avail.		
<input type="checkbox"/>	0	Embedded_Net_DVR_30	30		192.168.0.30	80	if avail.		
<input type="checkbox"/>	0	HIKVISION_DS_2CD6D54G	31		192.168.0.31	80	if avail.		
<input type="checkbox"/>	0	AXIS_P1435_LE_35	35		192.168.0.35	80	if avail.		
<input type="checkbox"/>	0	HIKVISION_DS_2CD2123G:	68		192.168.0.68	80	if avail.		

Your license allows to handle 15 cameras. There is actually 21 declared camera(s). Only checked cameras will be added into database

Add

Check the cameras to be added, then enter the user and password for each camera and click 'Add'.

*Note :* To enter the same user/password on several cameras, it is necessary to check multiple cameras :

Newly detected cameras									
	Disk	Name	View code	More information	IP Address	Port	PTZ	Username	Password
<input checked="" type="checkbox"/>	0	CT_camera_21	21		192.168.0.21	80	if avail.	admin	test
<input checked="" type="checkbox"/>	0	CT_camera_29	29		192.168.0.29	80	if avail.	admin	test
<input checked="" type="checkbox"/>	0	Embedded_Net_DVR_30	30		192.168.0.30	80	if avail.	admin	test

If any information is incorrect, the 'User' and 'Password' fields appear in red: it is imperative to correct the user/password, or to uncheck the invalid lines (see [1] below):

Nouvelles caméras détectées									
	Disque	Nom	Code vue	Plus d'informations	Adresse IP	PTZ	Utilisateur	Mot de passe	
<input checked="" type="checkbox"/>	0					si dispo.	admin	test	
<input type="checkbox"/>	0	CCTN2EW01F_29	29		192.168.0.29	si dispo.	admin	test	
<input type="checkbox"/>	0	AXISM3007_34	34		192.168.0.34	si dispo.	admin	test	
<input type="checkbox"/>	0	AXISP1435_LE_35	35		192.168.0.35	si dispo.	admin	test	
<input type="checkbox"/>	0	AXISQ6115_E_36	36		192.168.0.36	si dispo.	admin	test	
<input checked="" type="checkbox"/>	0	DINTON_4000_HD_39	39		192.168.0.39	si dispo.	admin	test	

If your camera(s) was/were added properly, the message '**X camera(s) added into database**' appears:

Newly detected cameras									
	Disk	Name	View code	More information	IP Address	Port	PTZ	Username	Password
<input type="checkbox"/>	0						if avail.		
<input type="checkbox"/>	0	CT_camera_29	29		192.168.0.29	80	if avail.		
<input type="checkbox"/>	0	AXIS_P1435_LE_35	35		192.168.0.35	80	if avail.		
<input type="checkbox"/>	0	HIKVISION_DS_2CD2123G:	68		192.168.0.68	80	if avail.		

Your license allows to handle 15 cameras. There is actually 22 declared camera(s). Only checked cameras will be added into database

Add

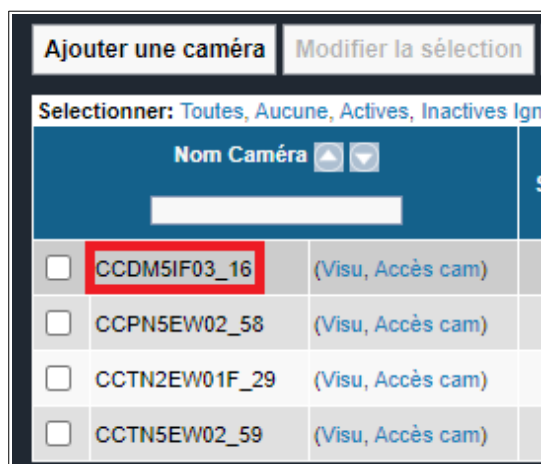
1 camera(s) added into database

If the above message does not appear, **no camera has been added** to the CT-Server.

## 7 Regular recording and alarm recording

### 7.1 ADD RECORDINGS ON A CAMERA

On the administration panel, select 'Manage' then 'Cameras'. Then, click on a camera's name to configure it :



The screenshot shows a web interface for managing cameras. At the top, there are two buttons: 'Ajouter une caméra' and 'Modifier la sélection'. Below these, there is a filter section with the text 'Selectionner: Toutes, Aucune, Actives, Inactives Ign' and a search box labeled 'Nom Caméra' with up and down arrow icons. Below the search box is a table with four rows of camera information. Each row has a checkbox, a camera name, and a link '(Visu, Accès cam)'. The first row, 'CCDM5IF03\_16', is highlighted with a red box.

Ajouter une caméra		Modifier la sélection	
Selectionner: Toutes, Aucune, Actives, Inactives Ign			
Nom Caméra ▲ ▼			
<input type="text"/>			
<input type="checkbox"/>	CCDM5IF03_16	(Visu, Accès cam)	
<input type="checkbox"/>	CCPN5EW02_58	(Visu, Accès cam)	
<input type="checkbox"/>	CCTN2EW01F_29	(Visu, Accès cam)	
<input type="checkbox"/>	CCTN5EW02_59	(Visu, Accès cam)	

### 7.1.1 'Records' section

In the 'Records' section, we will set up a common scenario: regular permanent 24/7 recording (on a medium quality stream). And, if motion is detected, then it will trigger an alarm recording (in high quality).

#### 7.1.1.1 Regular recording

In the screenshot below: regular recording is done on the standard quality stream (see [1] below) and is permanent 24/7 (see [2]). If you do not want to record 24/7 and want to record on a specific schedule (e.g. only during working hours), you can change the calendar (see [2]).

#### 7.1.1.2 Alarm recording

In the screenshot below: alarm recording is done on the high quality stream (see [3] below) and is permanent 24/7 (see [4]). If you do not want alarms to be triggered anytime, you can change the calendar (see [4]).

- Records	
Days before purge:	<input type="text" value="30"/> days
Regular recording	
Record stream	<input type="text" value="Standard Quality"/> ▾ <span style="float: right;">1</span>
Stop forcing at most after:	<input type="text"/> seconds
Regular recording:	<input type="text" value="Always"/> ▾ <span style="float: right;">2</span>
Frequency of regular recording (MJPEG only if >1 im/s):	<input type="text" value="3"/> images per <input type="text" value="second"/> ▾
Record on alarm	
Record stream	<input type="text" value="High Quality"/> ▾ <span style="float: right;">3</span>
Record on alarm:	<input type="text" value="Always"/> ▾ <span style="float: right;">4</span>
Pre alarm length:	<input type="text" value="5"/> seconds
Frequency of alarm recording (MJPEG only if >1 im/s):	<input type="text" value="6"/> images per <input type="text" value="second"/> ▾
Storage space (cannot be changed if camera has recordings)	<input type="text" value="Disk 1"/> ▾ <span style="float: right;">5</span>

**IMPORTANT** : Choose the correct disk as storage space (see [5] above).

Do not save your cameras on the System disk if you have the opportunity not to do so, for example if you have several disks : one System disk, and one or several Data disk(s).

Of course, if you only have one disk on your machine, you are forced to choose the System disk because you do not have other available disks.

We continue our common scenario with the addition of a **trigger** (in our example, it will be a motion detection) for the alarm recording.  
Because, currently, no trigger is set up so **there will not be any alarms recordings** so far.

### 7.1.2 Motion detection performed by the CT-Server

It is recommended to use a low-quality (or medium-quality) stream for motion detection to consume less CT-Server resources.

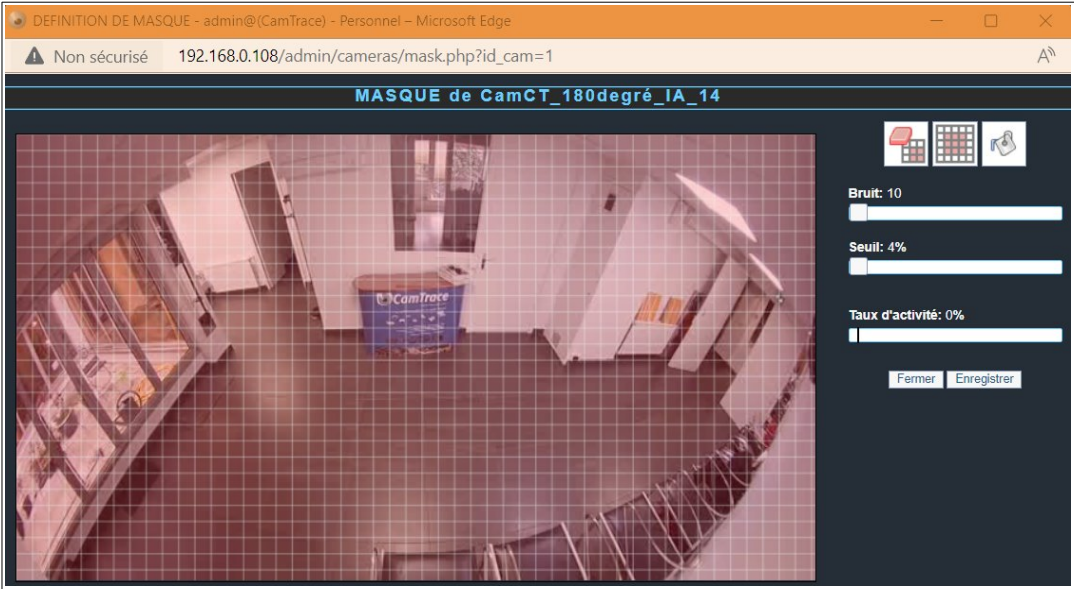
In the 'Motion detection' section, click on **'Define mask'** :

- Motion detection	
Motion detection:	Always <input type="button" value="Define mask"/>
Movement detection stream	Standard Quality <input type="button" value="Define mask"/>
Check for movement every	<input type="text" value="500"/> mS
Detection noise level (0 to 255)	<input type="text" value="10"/>
Detection threshold (in %)	<input type="text" value="4"/>

It is preferable that the **'Motion detection stream'** is the same stream as the one chosen as **the regular recording** (see Regular recording).

A 'DEFINE MASK' pop-up appears after clicking on 'Define Mask'.  
If the video stream does not appear on the 'SET MASK' pop-up, log back into the administration panel using your browser's **private mode**.

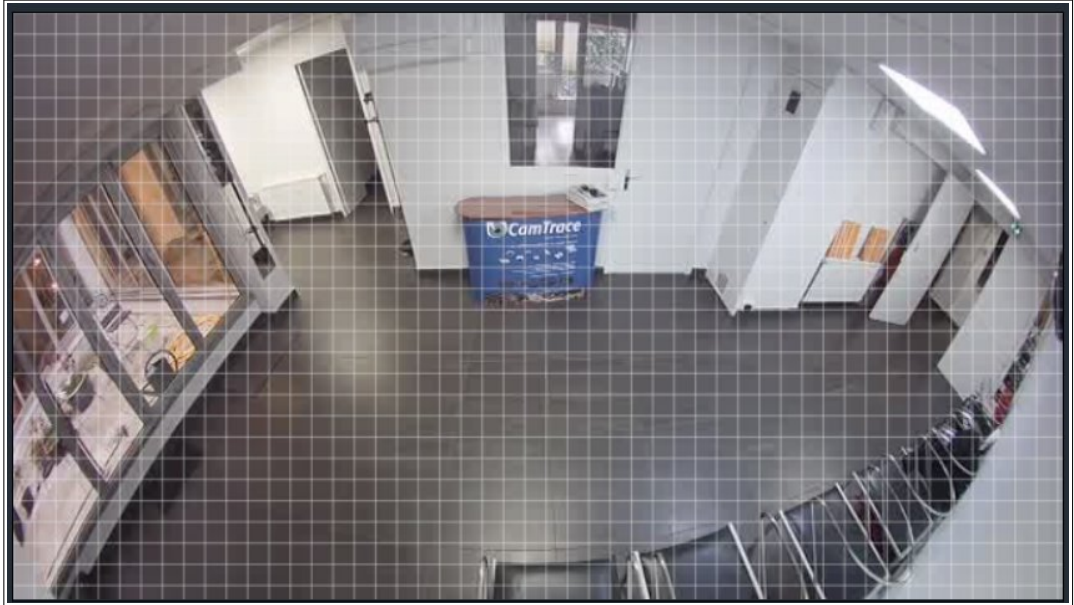
By default, the motion detection area (in red below) covers the entire view of the camera:



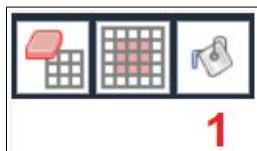
Click on the delete button :



to remove the detection field from the entire view:



Check that you are in **Paint mode** (see [1] below):



and not in **Erase mode** (see [1] below) :



Then draw the area(s) of motion detection. These areas appear in red in the video stream. If there is movement in the detection area, this will cause an alarm and trigger an alarm recording (see Alarm recording) :



Then click on 'Save'.



## 8 Saving the configuration

Once you have completed your CT-Server setup, it is strongly recommended that you **export the configuration**. On the administration panel, select 'Manage' then 'Configuration' and click on 'Save this configuration'.

It is recommended to make backups of the configuration when you make changes to the CT-Server (e.g. adding new cameras or modifying existing cameras). Save this configuration file on an independent device, it is better not to store this file on the CT-Server itself.

For further information :

**[www.camtrace.com](http://www.camtrace.com)**