

# IMTLazarus

## Operation Guide for supervisors of Windows devices within IMTLazarus

Throughout this document it will be described all functionalities that supervisors of devices using Windows Operating system.

A browser will be necessary to accede to **IMTLazarus** management dashboard.

Access will be possible throughout any device with an internet connection-

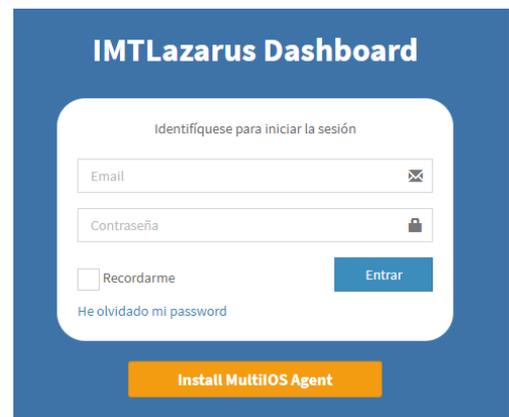
Open the browser. At URL bar we type the URL provided by the school, in order to accede **IMTLazarus** platform; this URL will always follow this standard:

<https://IDSERVIDOR.imtlazarus.com/lazarus>

A username and password will be required; they will be provided by the school.

Username > Email address

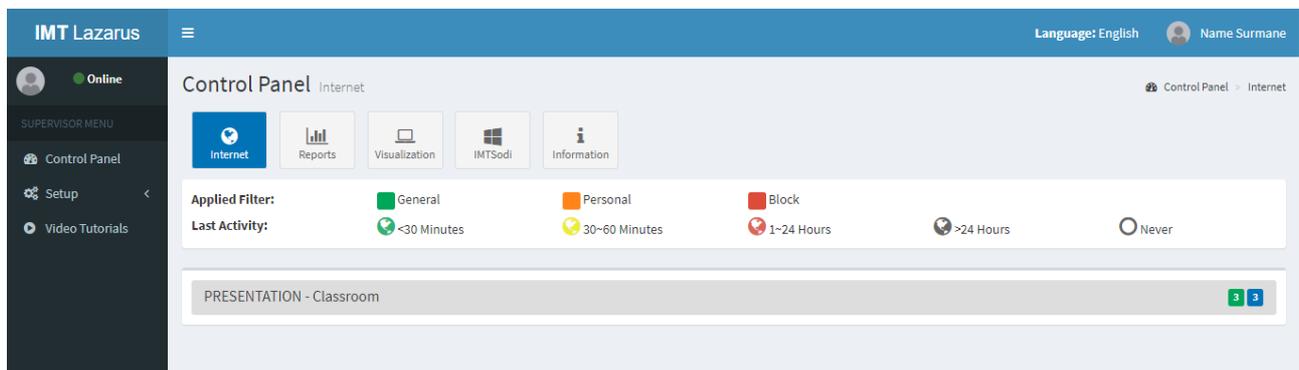
Password > 6 digits generated at random.



Access details are personal and non-transferable given that they provide full access to personal data from the devices of students / children managed by **IMTLazarus**.

Access to **IMTLazarus** platform is aimed only for teachers and parents, in no case for students' access.

Once validated the following screen will be displayed (it may varies and include modifications according to different users' privileges.)



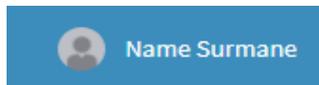
First thing we could modify / personalize is the interface language by clicking at top on the following button.



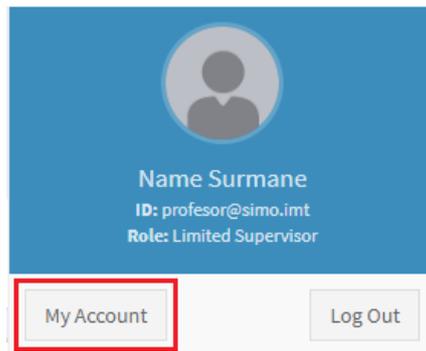
List of languages available so far within the system, are:

- Spanish
- Basque
- Catalan
- French
- English
- Italian
- Portuguese

Once the language is saved we could then modify any personal detail by clicking on the top button, as shown below:



And then click on "My Account" button:



Then, in the next screen, details such as first and last names, and password (recommendable to change it after first access by one that sounds more familiar to remember), maybe be modified.

<b>First Name:</b> <input type="text" value="Name"/>	<b>Password:</b> <input type="password" value="password"/>
<b>Last Name:</b> <input type="text" value="Surmane"/>	<b>Repeat Password:</b> <input type="password" value="password"/>

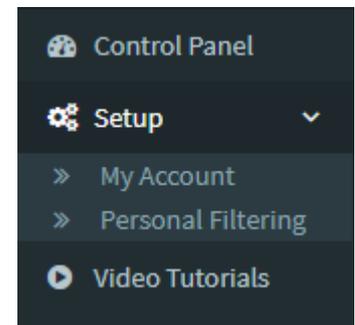
Green button will be clicked to apply and save any changes in this screen.



Once the name and personal data is modified we could then start to manage the devices through **IMTLazarus**.

On the left side it will be shown the different options we could work with:

- **Control Panel**  
In this section we will have all configurations regarding the control and supervision of the devices.
- **Setup:** In which there are 2 options available:
  - My account (as abovementioned).
  - Personal filtering: to set personalized filters for browsing.
- **Video Tutorials:** in which videos with de diverse functionalities of the system will be displayed.



Let's begin with the actions

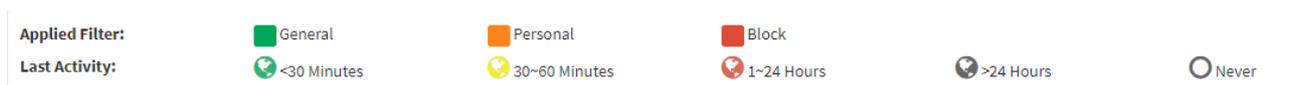
## Control panel

### Internet

Within this section internet access will be setup:



First thing that will be displayed it is a legend of the filtering groups and the conection status.



Applied Filter:

- Green (General); this filter is defined by the school and will restrict access to not schooling websites. *This is like a "free browsing"*.
- Orange (Personalized); this filter may be decided either by teachers or families in order to create a personalized setup.
- Red (Blocking); this filter will block total internet connection, except for some specific websites predefined by the school. *This is like a "NO browsing"*.

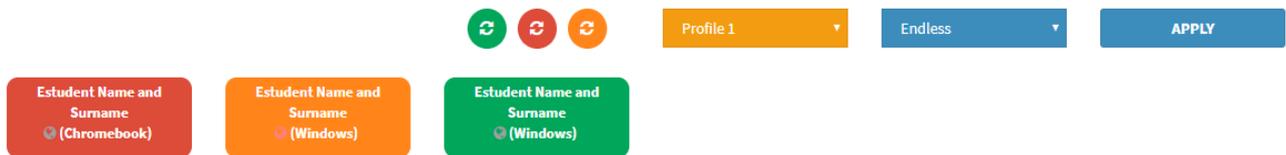
Latest Activity:

- Green: the device has had connectivity during the last 30 minutes.
- Yellow: the device has not been connected for the last 30 – 60 minutes.
- Red: the device has not been connected for the last 1 to 24 hours.
- Grey: the device has not been connected during the last 24 hours.
- Empty: the device has not been connected ever.

Below the legend it will be displayed as much groups / classrooms as we are managing, being several in the case of teachers, and just one (or more if they have more than one child) in the case of families.

The figures displayed on the right side of the group bar, refer to the amount of devices managed under the said group, specifying by the above explained color code, the amount of devices under each one of the filters applied.

Clicking on the group bar will deploy the checkbox of each device.



There are 2 ways to switch between filters, either by clicking on each one of the checkboxes or by clicking on the colored little balls displayed on top of them.

By clicking on the colored little balls will make all devices to turn their status at once, while clicking one by one on each device checkbox, the status will change individually.

We will also be able to define for how long the setup will be applied on each device, so the time can be defined with the deployable menu.



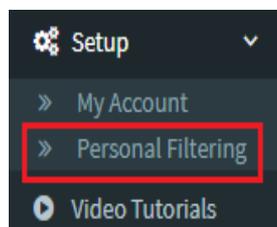
If a temporary order is setup, when countdown is over, the devices will return to the status prior the order went through.

Last, do not forget to click "Apply" any order to actually perform it.



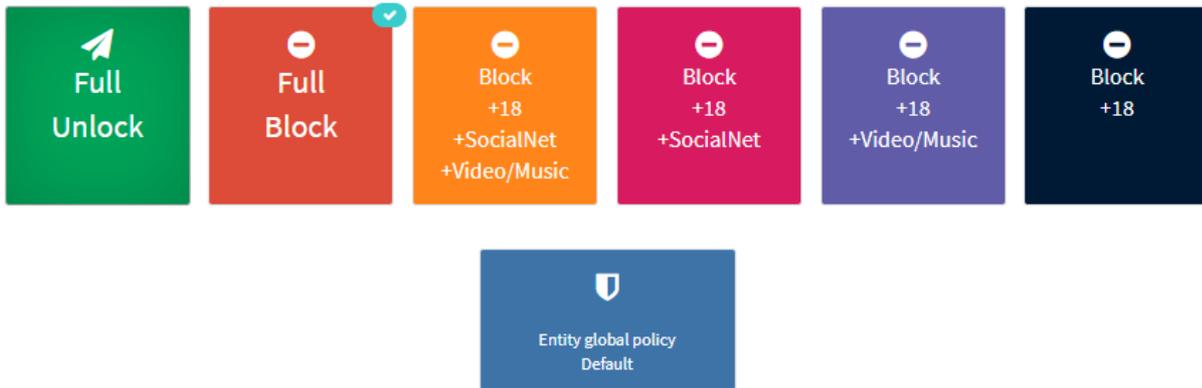
As it has been explained before, Green status (full browsing) and Red status (no browsing) are not modifiable; Orange status, instead it is modifiable to adapt it to our needs.

To do so, on the left side menu we will click on the dropdown menu of "Settings" and "Personal Filtering"



By doing it we will accede to the next page where we would be able to personalize our own filtering features.

First to be displayed will be the groups of predefined filters at our disposal.



- Green (full freedom). This filter will allow us to accede any website with no restriction at all. (*do not confuse with the Green status explained above*).
- Red (full blocking). This filter will block all device's connections and will not allow internet access at all. (*do not confuse with the Red status explained above*).
- Orange (+18, +Social Media, +Video/Music). This filter will block access to adult content websites, to social media and to music / video websites and / or platforms.
- Violet (+18, +Video/Music). This filter will block access to adult content websites and to music / video websites and / or platforms.
- Pink (+18, +Social Media). This filter will block access to adult content websites and to social media.
- Black (+18). This filter will block access to adult's content websites.
- Blue (Global policy). This filter will have the features set by the school and on top will be shown with a blue tic.

Under the Groups we will have the option to set both White and Black Lists.

The domains or websites introduced in the "White List" section will be free, regardless of the filter chosen. As shown in the example below, "facebook.com" will be free to accede, even if the red filter (full blocking) was selected.

---

**Allowed Domains ("white list")**

**Domain**

Search:

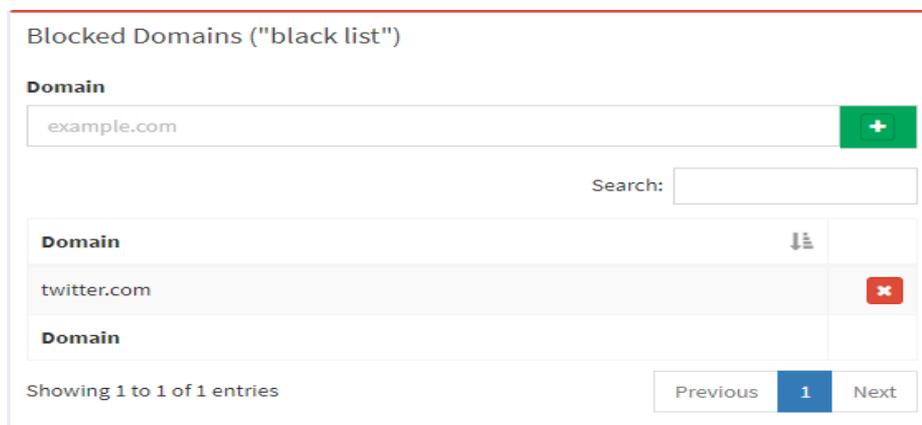
Domain	
facebook.com	
Domain	

Showing 1 to 1 of 1 entries

Previous **1** Next

---

The domains or websites introduced in the “Black List” section will be blocked, regardless of the filter chosen. As shown in the example below, “twitter.com” will be blocked to accede, even if the green filter (full browsing) was selected.



Once the filters is selected and the White and black lists are defined, we will be able to load this setup as explained in the “internet” section above, setting the devices with the orange color code.

## Reports

In this section we will view the browsing reports performed by the devices.



First thing we will see is a legend with the temporary info of the latest report received.

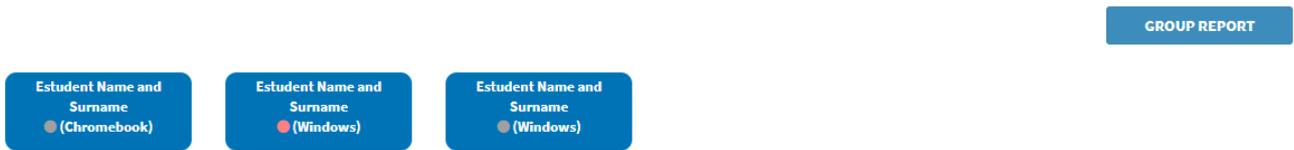


Latest browsing performed

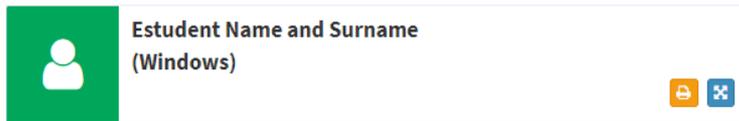
- Green (<30 m). Green color will mean that it's been less than 30 minutes since the system gathered any info on the device.
- Orange (30-60 m). Orange color will mean that it's been between 30 and 60 minutes since the system gathered any info on the device.
- Red (1-24 H). Red color will mean that it's been between 1 and 24 hours since the system gathered any info on the device.
- Pink (>24 H). Pink color will mean that it's been more than 24 hours since the system gathered any info on the device.

Clicking on the group it will be deployed the checkboxes showing the devices.

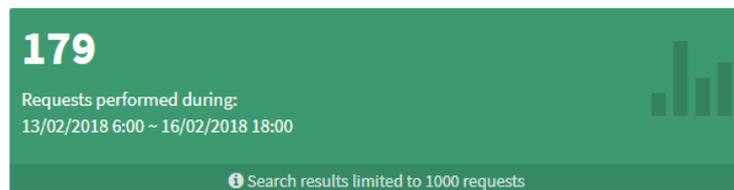
To view the reports there are 2 options, either by clicking on a single device (single report), or clicking on the button "Group Report" on the top right side.



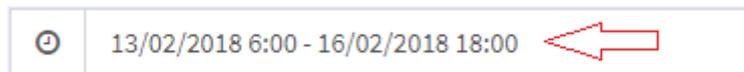
First thing we will see it's the username or the name of the group of which we are viewing the report.



At its right side we will see the number of demands made from a specified date and time until the report time.



Down below the report, there is a watch icon with two dates. Clicking on the dates we could define the period over which we want to view the report.

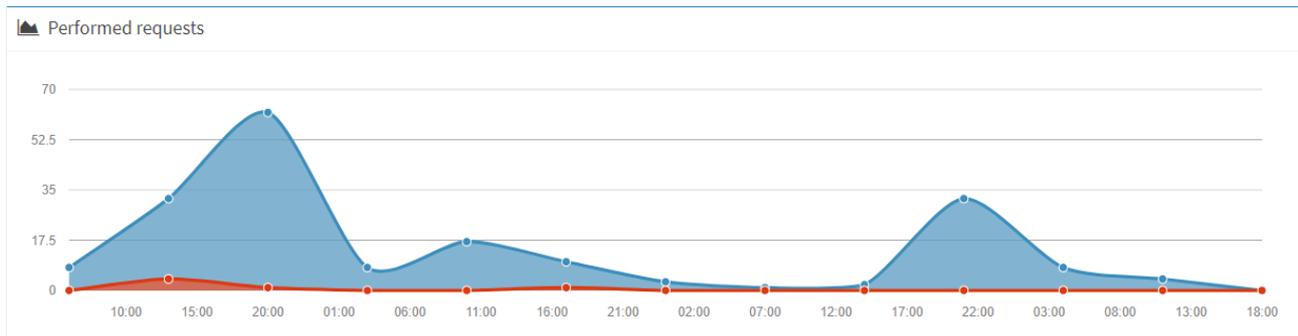


Clicking on the dates a dropdown menu will allow us to settle the starting date and time and the finishing date and time for which we want to present the report.

The screenshot shows two calendar views for February 2018. The left calendar has the 13th selected, and the right calendar has the 16th selected. Below the calendars are two time selection boxes: "6 : 00" and "18 : 00". At the bottom, there are "FROM" and "TO" labels, input fields with "13/02/2018 6" and "16/02/2018 1", and "Apply" and "Cancel" buttons.

In detail, on the left side calendar we will define the report starting day and down below the time, whilst on the right side calendar we will define the finishing date and the time.

Right below the calendar we will see an operation graph with 2 colors (blue & red).



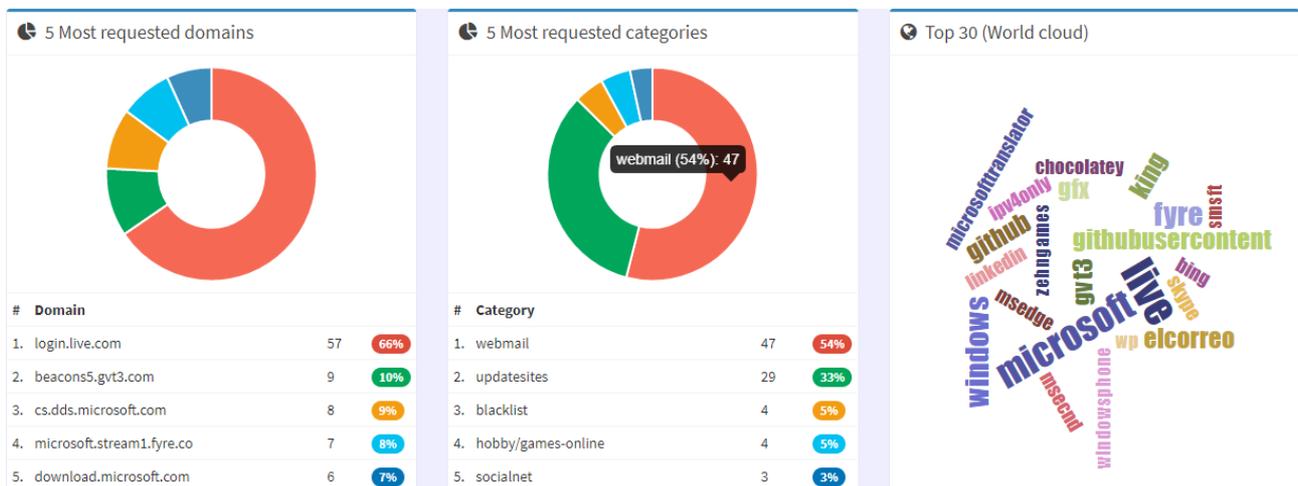
- Blue: Pages to which access has been attempted.
- Red: Pages blocked by **IMTLazarus**.

Difference between Blue & Red will be the pages to which the device has acceded.

Place the mouse on each of the dots shown in the graphs, to view the amount of pages browsed and of pages blocked for the track divided.

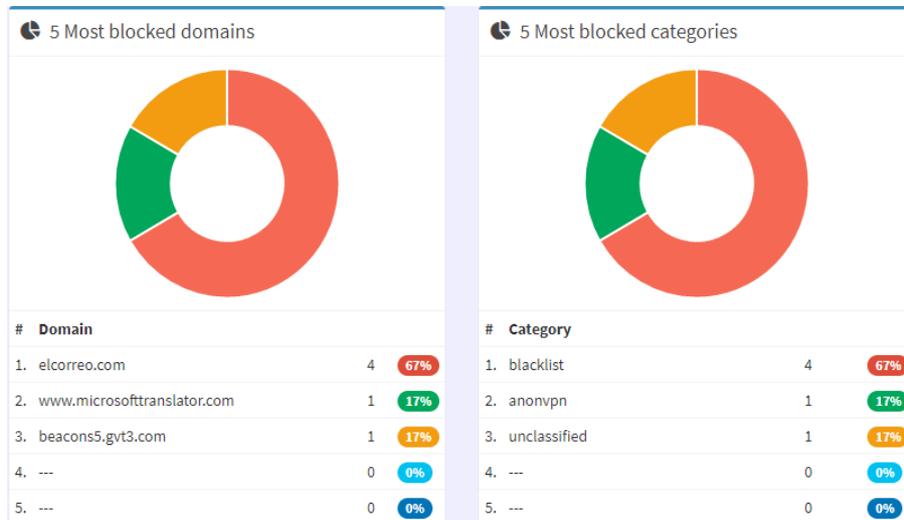


Hereafter, the 3 checkboxes will show us which are the websites / domains more visited, the categories more registered (pages are registered in the server by groups of categories), and top 30 *word cloud*, a visual summary of the most visited 30 dom.



Placing the mouse on the graphs we will identify which domain or category is represented within each section.

Then, we will see two checkboxes that will show which are the websites/ domains, most visited, as well as the blocking categories most registered (pages will be registered in the server by groups of categories).



Placing the mouse on the graphics we will identify which domain or category is represented in each section-

Finally we could see a detailed report of the whole browsing.

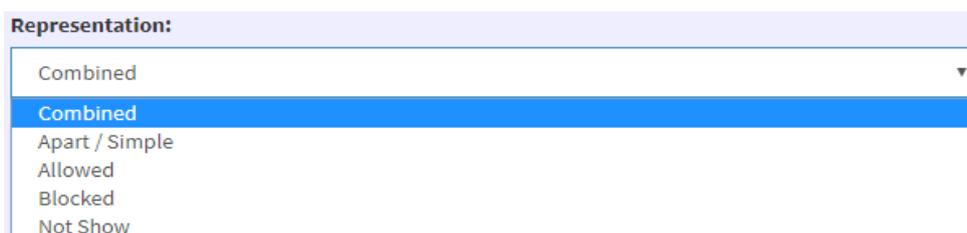
Performed requests (Max. 1000)

Show  entries Search:

Date	Url	User	IP	Category	
2018-02-13 14:18:42	<a href="#">mem.gfx.ms</a>	Estudent Name and	172.18.7.70	unclassified	✓
2018-02-13 14:18:42	<a href="#">az725175.vo.msecnd.net</a>	Estudent Name and	172.18.7.70	unclassified	✓
2018-02-13 14:18:33	<a href="#">www.zehngames.com</a>	Estudent Name and	172.18.7.70	unclassified	✓
2018-02-13 13:44:37	<a href="#">cs.dds.microsoft.com</a>	Estudent Name and	172.18.7.70	updatesites	✓
2018-02-13 13:26:12	<a href="#">storagetos.datamart.windows.com</a>	Estudent Name and	172.18.7.70	unclassified	✓

- Date: Date and time when a website was attempted to enter or entered.
- Url: page or domain entered or attempted to enter.
- User: user that attempted to enter the page or domain.
- IP: Virtual IP connection with **IMTLazarus**.
- Category: Category to which it belongs the page depending on the contents.
- Access / Blocking: A green tick mark shows an "allowed" page while a red forbidden shows a blocked page.

Reports can be displayed in many ways, for it we have to deploy the dropdown menu of "Representation" and select the most convenient one.



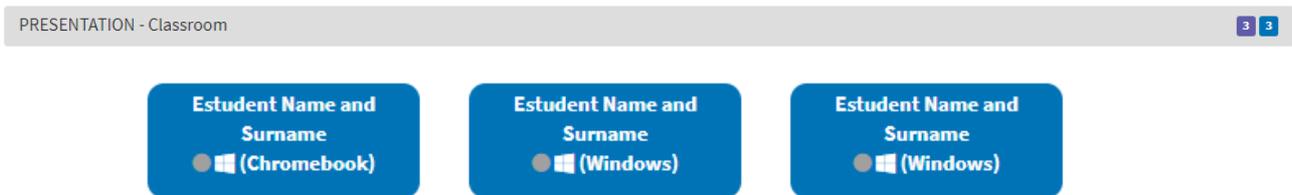
- Combined: It shows the whole information, pages allowed and blocked.
- Apart: It shows the information of the pages allowed and blocked, separately.
- Allowed: It only shows the allowed pages.
- Blocked: It only shows the blocked pages.
- Not Displaying: It does not show any final report.

## Displaying

In this section we will see the devices' screens.



Clicking on the group bar the checkboxes representing each device will dropdown.



To see remotely the screen of any of the devices we just need to click on any of the checkboxes.

Doing so a new tab will open and once all checks are done we will be able to see the device screen in real time.



System only allows to display one device at a time.

In case a device is already been displayed by another supervisor, it could not be displayed until the first supervisor's connection is over.

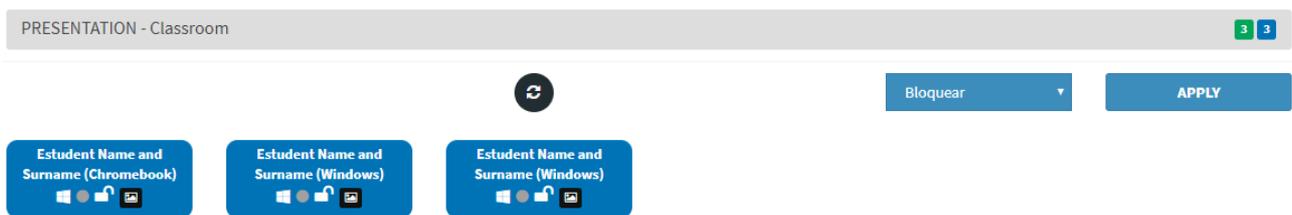
## IMTSodi

In this section we could perform additional actions of system on the devices.



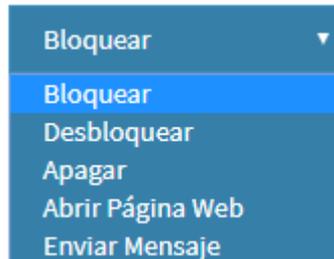
Within this section, actions of system on the devices could be performed; actions such as blocking or unlocking the device, turn the device off, open websites or send a message.

Clicking on the group bar the checkboxes representing each device will dropdown.



To perform the actions of the system there are 2 options: clicking on every one of the checkboxes for individual actions, or clicking on the top small black ball for global actions.

Once we have marked the devices to which we want to send an order or action, -those devices will change to a lighter blue-, then we will click on the dropdown menu on top and will choose the action to be performed to all of them.



The actions we could perform will be the following:

- Blocking: It uploads a blocking screen into the device.
- Unlocking: It releases the blocking action.
- Turn Off: It turns off the device.
- Open a website: It opens a website through one of the devices' browser. When selecting this option it will appear a text bar to type in the website we want to send. We could send a website to all devices at once.

<http://wikipedia.org>

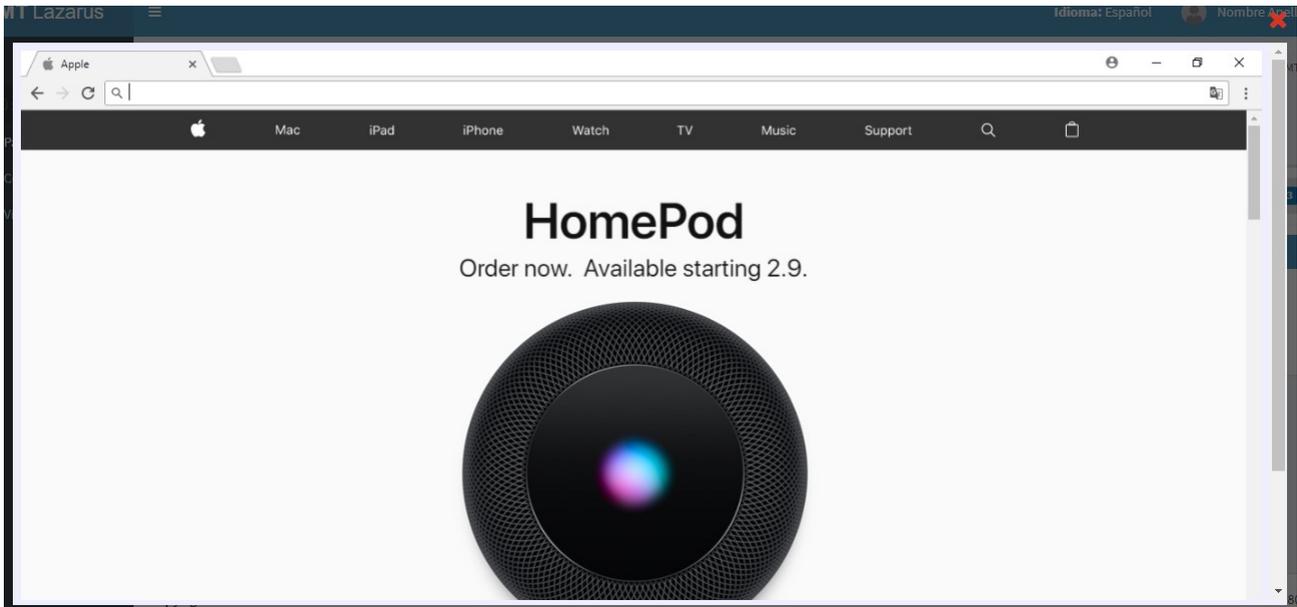
- Send a message: It sends a message to the device. When selecting this option it will appear a text bar to type in the message we want to send. We could send a message to all devices at once.

We are going to have dinner

Finally we could receive a screenshot of what is being done with the device.

To do so we just need to click on this button  by the checkbox representing the device to which the mentioned action is aimed.

In so doing a new screen will open and display the screenshot of the tracked device. It will display a static image not a live video.



## Information

Within this section we will be able to see information of the devices.

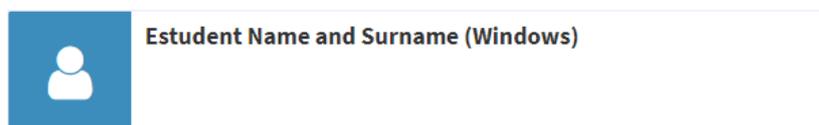


Within this section we can see the info related to the operating system, storage, RAM memory, etc.

Clicking on the group bar we will deploy the checkboxes representing each device.



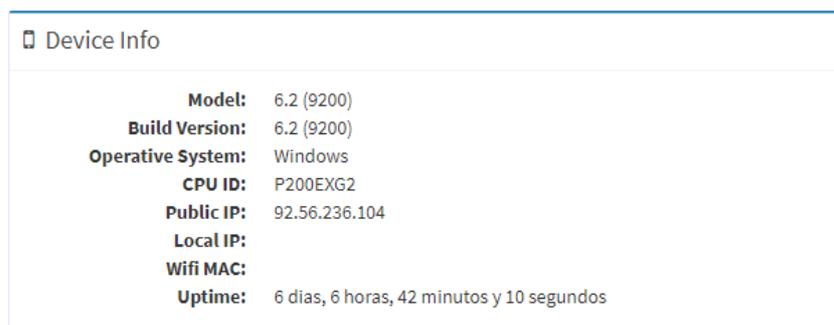
To visualize the info of a specific device we will have to click on one of the checkboxes. First to appear will be the username of the device (student / child).



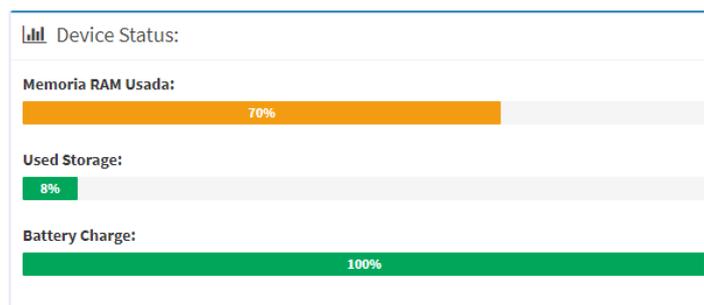
Next to be displayed will be info related to the MDM (in case there is any) to which the device is registered.



Bottom-left checkbox will display info related to the HW and SW of the device.



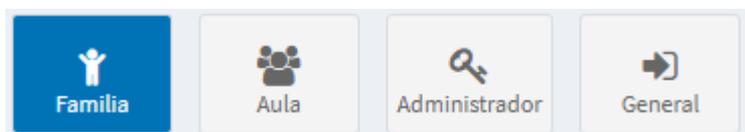
Finally in the bottom-right checkbox we will see the info related to the storage and RAM memory of the device.



This subsection is the last one of the section "Control Panel".

## Video Tutorials

Within this section we can see a set of videos of how it functions and additional info of **IMTLazarus**.



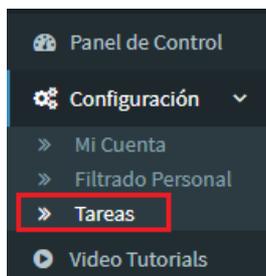
We will have different videos depending on the type of videos:

- Families: Orientation videos explaining to the families the use of the platform / device.
- Classroom: Orientation videos explaining to teachers staff the use of the platform / device.
- Administrator: Orientation videos explaining to administrators the use of the platform / device.
- General: Videos not aimed for a specific collective, containing information about the platform / device, speeches, interviews, etc.

## Functioning Guide for supervisors; personal tasks IMTLazarus

Throughout this Guide it will be explained the setting of the personal tasks for families and teachers.

Once validated by the system, we will access to the section “Settings >Tasks” as shown in the image below.



In the next screen we will click on the Green button to “Create new”.

Tareas + Crear Nueva

Show  entries Search:

Nombre	Tarea	Ámbito	Hora	Días	Último Check
No data available in table					
Nombre	Tarea	Ámbito	Hora	Días	Último Check

Showing 0 to 0 of 0 entries Previous Next

We will then fill in the following data:

Datos de la Tarea

**Nombre:**

**Tarea:**

**Ámbito: (\*)**

**Hora:**

**Días:**

Lunes  Sábado  
 Martes  Domingo  
 Miércoles  
 Jueves  
 Viernes

**Descripción:**

Tarea Activa

Being:

Name > It will be the name with which we will identify the task (e.g. "no internet", "night blocking", etc.)

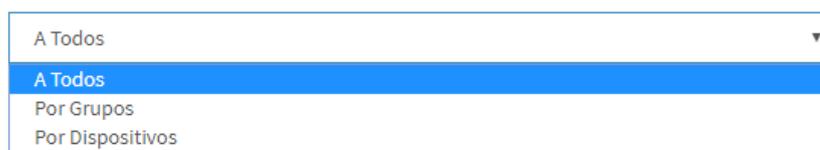
Task > we will choose among the allowed tasks, depending on the operating system and the available options:

- Enable Camera: It allows the use of the camera within the device
- Disable Camera: It restricts the use of the camera within the device
- Activate Browsing: It allows the device to connect to internet (green status at internet control on the console)
- Deactivate Browsing: It restricts the device to connect to internet (red status at internet control on the console)
- Windows Lock ON: It blocks the device' screen (only for Windows)
- Windows Lock OFF: It unblocks the device' screen (only for Windows)
- App Whitelist OFF: It de-links any control profile from personalized applications of the device

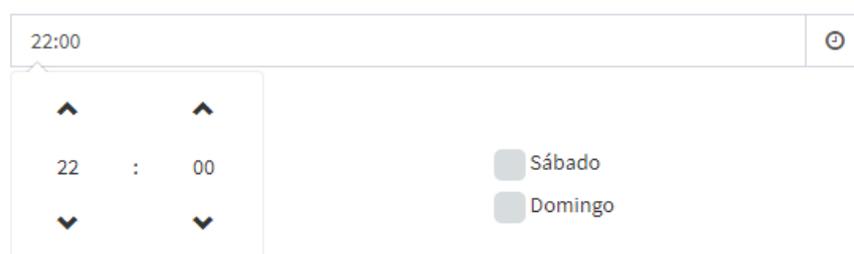


Once we have defined the action that our task will perform (just one action per task), we will set the application range; to do so, we will choose one of the following 3 options within the drop-down menu:

- To all: it will be applied to all devices managed, in case of the teachers to all the devices in his or her classes, and in case of the families to all children devices' that pass through IMT-Lazarus.
- By groups: It will be applied only to the groups selected after having defined entirely the task (usage option for teachers).
- By device: it will be applied to all and every devices selected after having defined entirely the task (usage option for families).



Next we will define the implementation timing of the task; take into account that the task will be implemented from the selected timing on, i.e. in case a device is out when the task is implemented, the task will be upload when the device is turned on.



Along with the selected timing we will choose the days for which it will apply; to do so, we will just click in the correspondent checking boxes. (i.e. the task shown below will just apply from Mon thru Fri).

**Días:**

- Lunes
- Martes
- Miércoles
- Jueves
- Viernes
- Sábado
- Domingo

Next step will be to define a description for the scheduled task (optional step, given that the name can identify as well the taks goal).

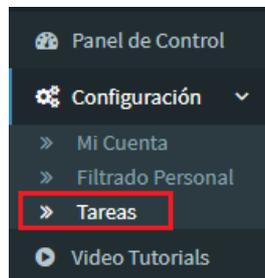
**Descripción:**

Tarea para quitar Internet a las 23:00 de lunes a viernes

Last, we will have to activate the task, to do so we will click the checkbox that shows the action. In case of creating a task but not clicking the box, the task will not be performed.



Once finished the task setting we will go back to the task management page “Settings > Tasks” in order to visualize or modify its actions.



In this page we will be able to visualize all historical tasks that we have generated, modify or delete them, according to our needs or likes.

Tareas [+ Crear Nueva](#)

Show  entries Search:

Nombre	Tarea	Ámbito	Hora	Días	Último Check	
Bloqueo internet	Deshabilitar Navegación	Por Dispositivos	23:00	L,M,X,J,V	<input type="radio"/> Pendiente	
Bloquear cámara	Habilitar Cámara	A Todos	16:00	L,M,X,J,V,S,D	26-02-2018 17:24:01	
Bloquear el ordenador	Windows Lock ON	Por Grupos	22:00	L,M,X,J	<input type="radio"/> Pendiente	
Nombre	Tarea	Ámbito	Hora	Días	Último Check	

Showing 1 to 3 of 3 entries Previous **1** Next

In that section, we will find the following Information:

- Name: the name assigned to that task.
- Task: the action the task will perform.
- Range: showing the devices or group of devices for which the task will be assigned (To all, By groups, By device).
- Hour: implementation hour of the task.
- Days: days of the week in which the task will be implemented.
- Last check: it will identify the last time the task was performed.

## ICONS

-  Clicking on this icon we will be able to modify or finalize the definition of any task.
-  It will identify if a task is active or not. In case the icon is on (orange), it means the task is active; in case the icon is off (grey), it means the task is deactivated and thus will not be performed. By clicking on this icon we can activate or deactivate the tasks.
-  Forced task, by clicking on this icon the task will be launched automatically. This action only will be performed when fitting the task timing, i.e. a scheduled task from Mon thru Fri at 22:00 cannot be forced before 22:00 hours during weekdays nor during weekends.
-  Task delete button, by clicking on this button the selected task will be deleted.

## Scheduled tasks for groups and / or devices

When generating a task we can choose to apply it to a certain series of groups or devices; to select them we will just click on the button to modify task.

At the new screen bottom we will have the groups or devices to which we can select to check for its application.

**Dispositivos disponibles:**

Q search	□	+
Apellidos del alumno 1, Nombre (Chromebook)		+
Apellidos del alumno 2, Nombre (Chromebook)		+
Apellidos del alumno 3, Nombre (Chromebook)		+

**Grupos disponibles:**

Q search	□	+
Aula		+

We will just check on the “+” next to each one of them and they will move to the right side box.

**Aplicar la tarea "Bloqueo internet " a:**

Q search	□	-
-	Apellidos del alumno 1, Nombre (Chromebook)	
-	Apellidos del alumno 2, Nombre (Chromebook)	
-	Apellidos del alumno 3, Nombre (Chromebook)	

**Aplicar la tarea "Bloquear el ordenador" a:**

Q search	□	-
-	Aula	

To de-link a group or a single device from a task, just click on the “-“ button beside them.

Finally, to save it we will click on the “Apply Changes” button

A green rectangular button with the text "APLICAR CAMBIOS" in white uppercase letters and a white checkmark icon to the right of the text.

Tasks that are assigned “To all” do not require group setting or single device setting, given that setting will be applied to all assigned devices.