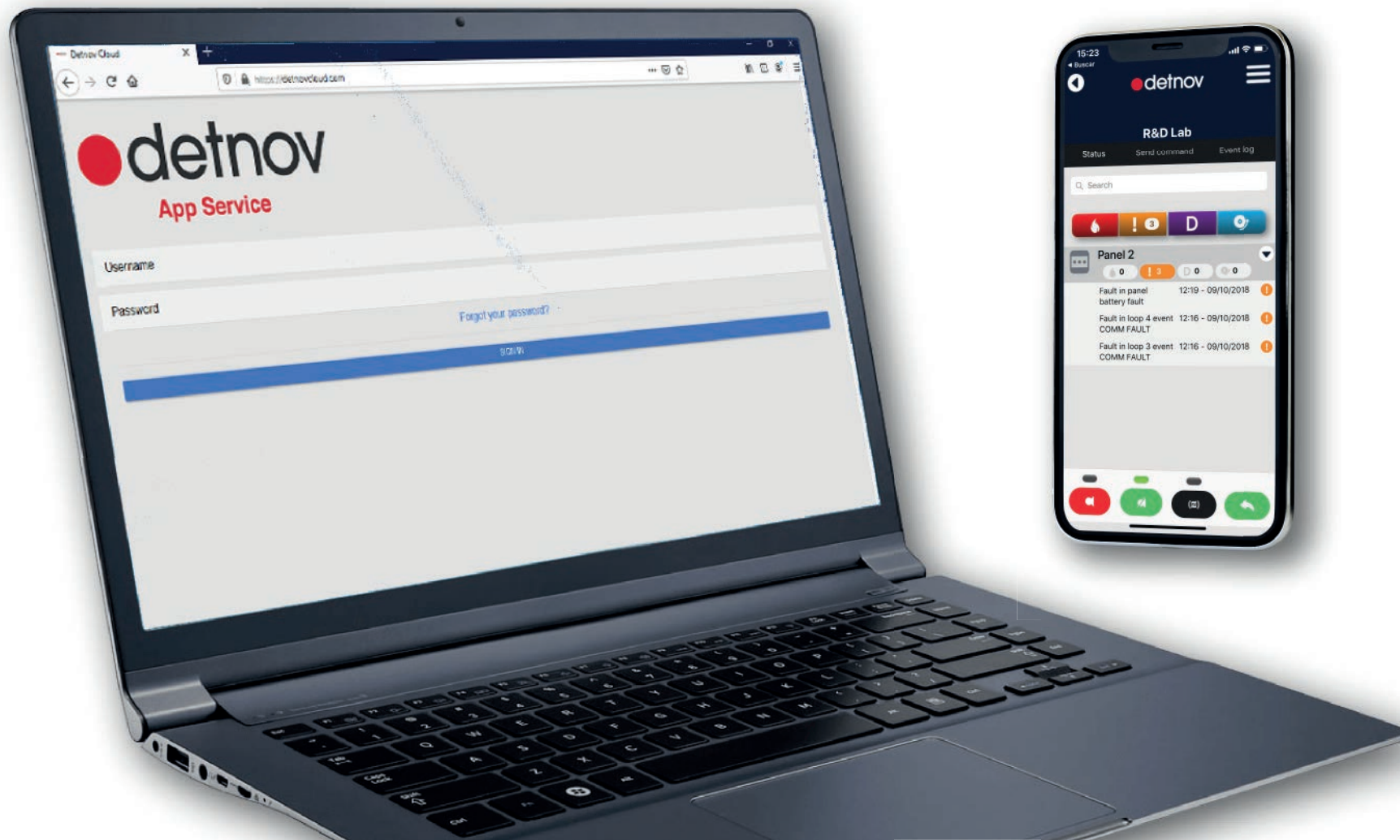


DETNOV CLOUD USER AND CONFIGURATION MANUAL



ENG





CONTENTS

1.	INTRODUCTION	6
2.	USERS	6
2.1.	Administrator users	6
2.2.	Users	6
3.	WEB	7
3.1.	Web administration.....	7
3.1.1.	Top bar	7
3.1.2.	MY FACILITIES	8
3.1.3.	View facility details and import event log.....	8
3.1.4.	Edit facility details.....	9
3.1.5.	Users	9
3.1.6.	View user details	10
3.1.7.	Edit user details.....	10
3.1.8.	Define facilities	11
3.1.9.	Add users	11
4.	APP	12
4.1.	Main screen.....	13
4.2.	Main menu.....	13
4.2.1.	Synchronise.....	14
4.2.2.	Configuration	14
4.2.3.	Connect facility	14
4.2.4.	Change password	15
4.3.	Facility list.....	15
4.4.	Remote control of the facility	16
4.5.	Send command	17
4.6.	Event log	18

Revision control

Revision	Comment	Date
a	First edition	17/09/2020
b	COVer an web changes	12/11/2020

PRIVACY POLICY

Detnov Security S.L. created the Detnov app as a free application. This SERVICE is provided by Detnov Security S.L. free of charge and is intended for use as is.

This page is used to inform visitors of our policies regarding the collection, use and disclosure of personal information for anyone who decides to use our Service.

If you choose to use our Service, you agree to the collection and use of information in relation to this policy. The personal information that we collect is used to provide and improve the service. We will not use or share your information with anyone, except as described in this Privacy Policy.

The terms used in the Privacy Policy have the same meanings as in our website, <https://www.detnov.com/politica-de-privacidad/>, unless otherwise defined in this Privacy Policy.

Information collection and use

For a better experience, whilst using our Service, we may ask you to provide certain personally identifiable information, including the device ID, name of the user, surname and email address. We will retain the information that we request and will use it as described in this Privacy Policy.

The app uses third-party services that may collect information used to identify you.

Link to the privacy policy of third-party service providers used by the Google Play Services app. The manufacturer or distributors of this range of fire alarm panels cannot accept any responsibility for any misinterpretation of an instruction or guidance note or for full system compliance.

The manufacturer's policy is improved on an on-going basis and we reserve the right to make changes to the product specifications at our discretion and without prior notice.

Incorrect assembly, improper installation, poor configuration of the unit or the state of the detection wiring are not the responsibility of the control panel manufacturer.

Log data

Please note that whenever you use our Service, in case of an error in the app, we collect data and information (via third-party products) on your phone called Log Data. This Log Data may include information such as your device's Internet Protocol (IP) address, device name, operating system version, the app's configuration when using our Service, the date and time of use of the Service and other statistics.

Cookies

Cookies are small data files that are commonly used as anonymous unique identifiers. They are sent to your browser from the websites you visit and are stored in the internal memory of your device.

This Service does not use cookies explicitly. However, the app may use third-party code and libraries that use cookies to collect information and improve their services. You have the option of accepting or rejecting these cookies and knowing when a cookie is sent to your device. If you decide to reject our cookies, you may not be able to use certain parts of this Service.

Service providers

We may employ third-party companies and individuals due to the following reasons:

- To facilitate our Service;
- To provide the Service on our behalf;
- To perform services related to the Service; or
- To help us analyse how our Service is used.

We want to inform users of this Service that these third parties have access to their personal information. The reason is to perform the tasks assigned to them on our behalf. However, they are obligated not to disclose or use the information for any other purpose.

Security

We value your trust in providing us with your personal information, thus we strive to use commercially acceptable means of protecting it. However, please remember that no method of transmission over the Internet or method of electronic storage is 100% safe and reliable, and we cannot guarantee its absolute security.

Links to other sites

This service may contain links to other sites. If you click on a third-party link, you will be directed to that site. Please note that these external sites are not operated by us. Therefore, we strongly recommend that you review the Privacy Policy of these websites. We have no control over and assume no responsibility for the content, privacy policies or practices of third-party sites or services.

Children's privacy

These Services are not aimed at those below the age of 13. We do not knowingly collect personally identifiable information from children under 13. If we discover that a child under 13 has provided us with personal information, we will immediately delete it from our servers. If you are a parent or guardian and you are aware that your child has provided us with personal information, please contact us so that we can take the necessary actions.

Changes to this Privacy Policy

We may update our Privacy Policy from time to time. You are therefore advised to check this page periodically for any changes. We will notify you of any changes by publishing the new Privacy Policy on this page. These changes are effective immediately after posting on this page.

1. INTRODUCTION

Detnov Cloud is the cloud-based remote connectivity solution that maintainers have been waiting for. This solution will let you offer new services to your customers via an app that is installed on mobile telephones, tablets or computers. It gives you real-time access to information on all of your facilities, with remote monitoring and control, if you have the relevant permissions, remote activation and deactivation of zones or devices.

The TCP/IP communication card, with reference TED-151-CL, is installed in Detnov's range of conventional control panels and addressable control panels, allowing the control panels to be connected to the Internet via the Ethernet port on the card's board.

The cloud is arranged in closed and encrypted groups so that the users of one group only have access to the facilities that belong to that group. Thus, the confidentiality of the facilities and the security of use for each one is guaranteed.

This manual details the necessary aspects for managing and operating Detnov Cloud, in terms of both its web interface and the mobile app.

In order to access the cloud services, you must contact your distributor and ask to be registered in the cloud.

2. USERS

Each person that uses the Detnov Cloud services must be registered as a user in the system. There are two user levels:

- Administrator users
- Users

The system is designed so that each group has a maximum of **10 users**. Should you require more, please contact your distributor.

2.1. ADMINISTRATOR USERS

An administrator user will be the first in the group. To obtain this user, you must ask your distributor to register you in the service. Once you receive the login credentials, you can start to use Detnov Cloud.

Only those who are responsible for your group can register or deregister other administrators or users, deactivate users temporarily, allow or restrict the access of each user to the facilities and define their permissions.

In addition, just like users, they can use the system to control and monitor the facilities and register new facilities in their group.

2.2. USERS

In order to access both web pages, the login credentials of a system user provided by your distributor if you are the first user, or by your system administrator if you are not the first user, are necessary.

The functions described in the following sections of the manual are available for system administrator users. If you access the system as a user, some of the functions shown below will not appear.

3. WEB

The service includes the web page:

- **www.mydetnov.com**

This page lets you manage all of the facilities you have access to, as well as the users of your group.

In order to access both web pages, the login credentials of a system user provided by your distributor if you are the first user, or by your system administrator if you are not the first user, are necessary.

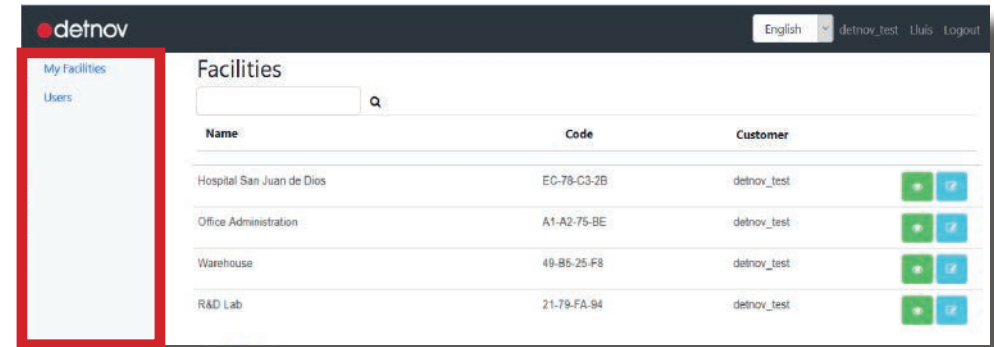
The functions described in the following sections of the manual are available for system administrator users. If you access the system as a user, some of the functions shown below will not appear.

3.1. WEB ADMINISTRATION

To manage your accounts or link facilities, go to the manager at **www.mydetnov.com**.

This is the page that lets you manage the group you belong to. The frame on the left shows two configuration options.

- My facilities
- Users



3.1.1. Top bar

The following fields appear in the top bar:

- **Group name:** company “detnov-test”
- **Language:** option to select the language
- **Username:** name of the user
- **Logout:** option to leave the page



3.1.2. MY FACILITIES

On the facilities page, all of the facilities you have access to are shown. The following fields are specified for each one:

- **Name:** the description of the facility
- **Code:** the single identifier for each card that connects the facilities to Detnov Cloud
- **Customer:** the group each facility belongs to. The name of your company must always be shown for all.

There are also two buttons for each facility for viewing and editing at the end of each line:

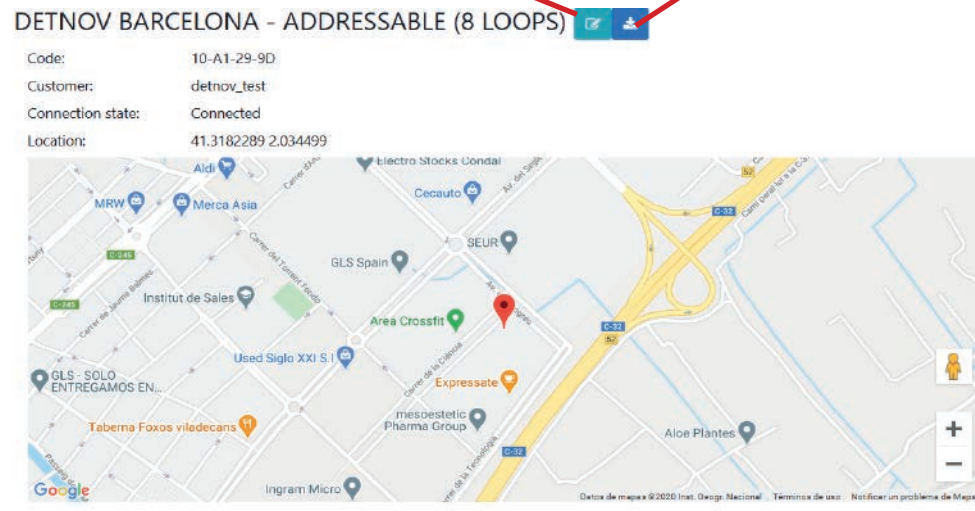
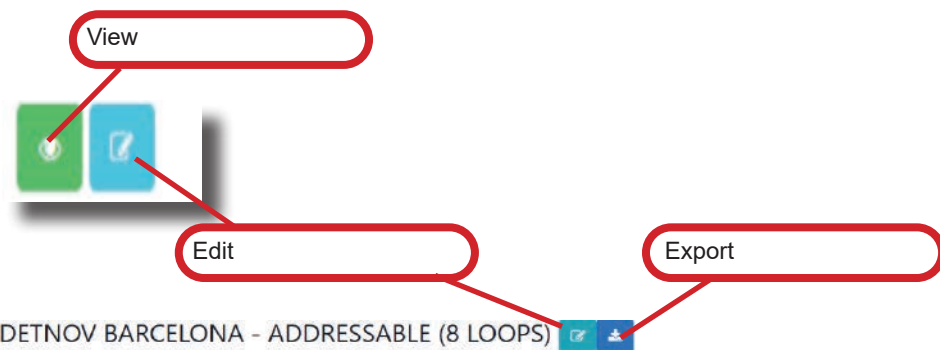
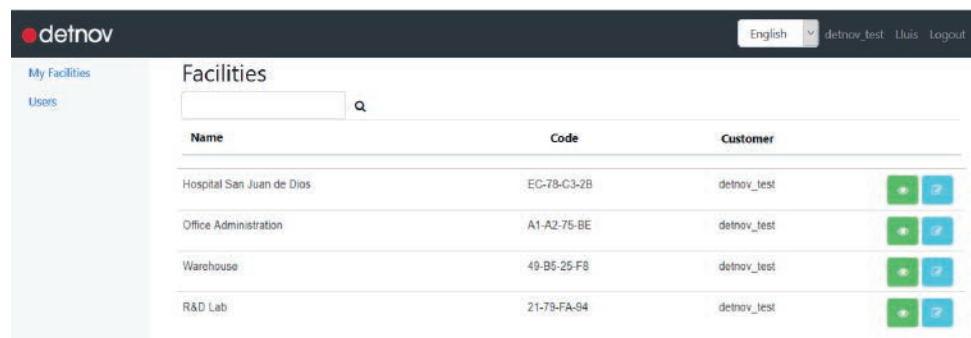
- **View:** it lets you view the details of the facility
- **Edit:** it lets you modify the details of the facility

3.1.3. View details

The following details are shown for each facility:

- **Name:** "Office Administration"
- **Code:** "A1-A2-75-BE", unique identifier of the card
- **Customer:** "detnov_test", the group it belongs to
- **Connection state:** it may show Connected or Disconnected, depending on whether the server is connected to the facility's card or not
- **Location:** it shows the GPS coordinates and the map of the location defined for the facility

There are two buttons next to the facility's name, the first for editing the facility's details and the second for exporting the facility's event log.



3.1.4. Edit facility details

This screen lets you define and edit the following fields:

- Facility name
- Facility location

To apply the changes, you must save them via the **Save** button at the bottom of the screen.

By pressing the Export icon, you will access a pop-up screen that lets you select the type of events to export.

Select the events and the period for which you want to download the events.

Press **Download** to begin the export process.

Press **Cancel** to discard the operation.

3.1.5. Users

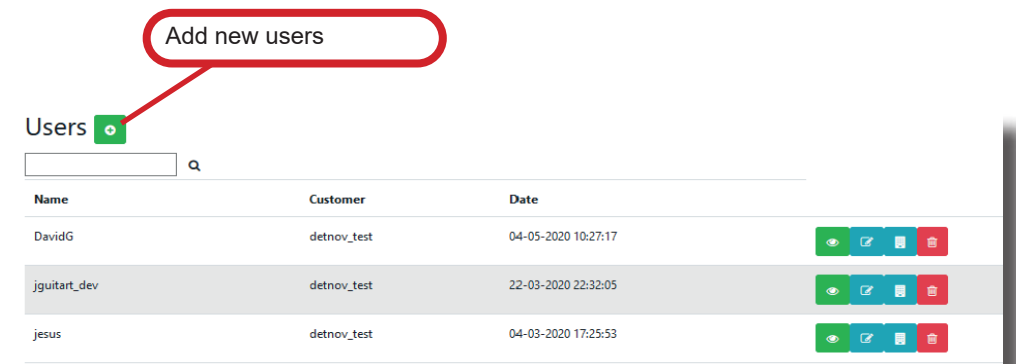
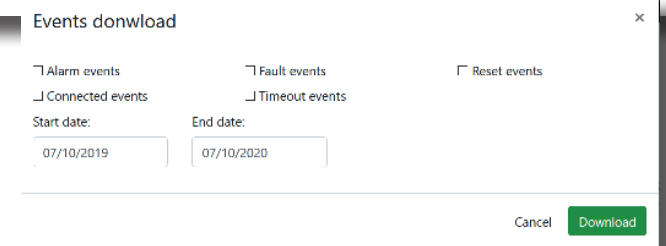
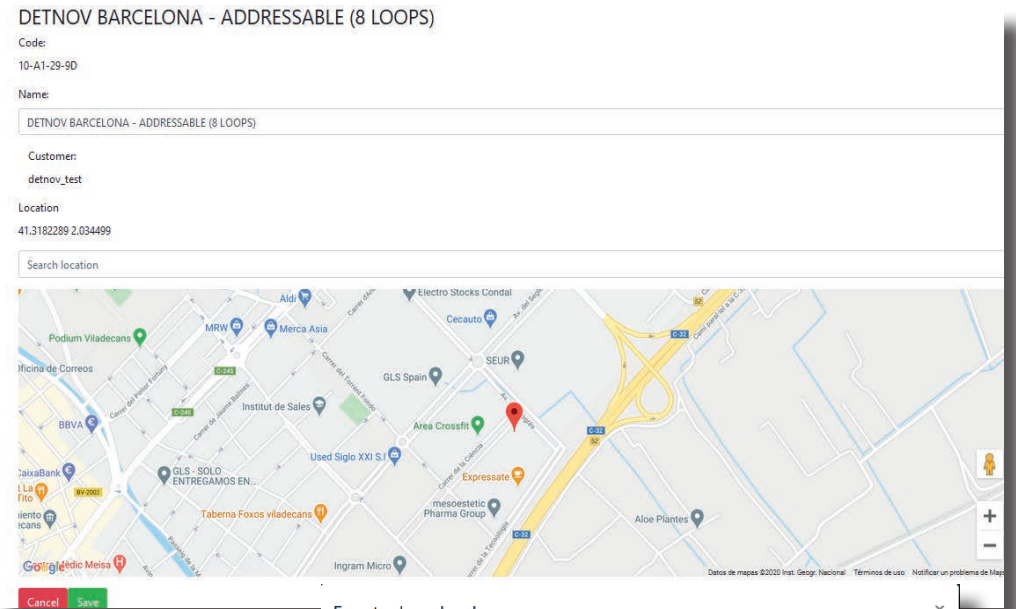
This screen lets you view all users of the group and for each one, the following fields:

- **Name:** user identifier
- **Customer:** the group to which they belong. The name of your company must always be shown for all.
- **Date:** the date of registration in the system

There are also four buttons for each user at the end of each line. From left to right:

- **View:** it lets you view the user's details
- **Edit:** it lets you edit the user's details
- **Define facilities:** it lets you view and define the facilities of the group to which the user has access
- **Delete:** it deletes the user from the system

At the top, next to **Users**, is the button for adding new users to the group.



3.1.6. View user details

The following details are shown for each user:

- **Username:** name of the user
- **Email:** it identifies each user and must be unique for each user
- **Client:** the group to which they belong
- **Role:** user type, which may be USER (basic user) or CLIENT_ADMIN (administrator user)
- **Can send commands:** Yes or No, whether you can operate the facility remotely or not. If not, then you will only be able to monitor it.
- **Enabled:** Yes or No; if not enabled, the user will not be able to access the system

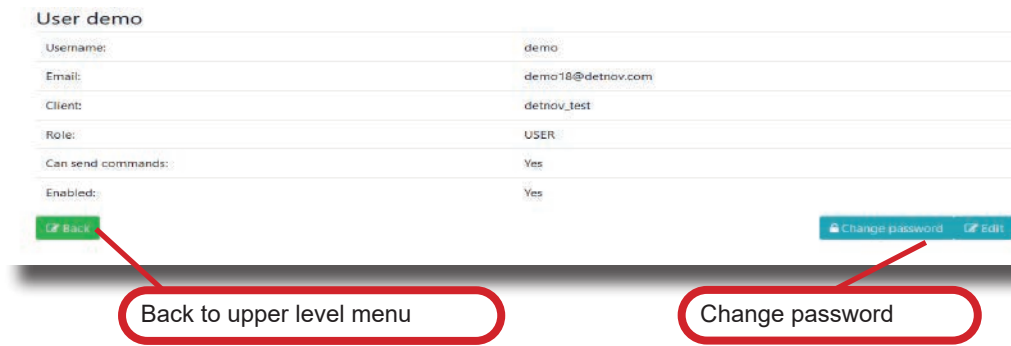
The button for changing the user password is at the bottom right. To change the password, it is not necessary to know the current user password. So any group administrator can change the password of other group users.

3.1.7. Edit user details

The following fields can be edited for each user:

- **Username:** name of the user
- **Email:** email that identifies the user, it must be unique for each user
- **Role:** USER or CLIENT_ADMIN, if the user is a basic user or an administrator user
- **Time zone:** the time zone for each user must be defined according to the closest city from those available so that the system takes local summer/winter time changes into account
- **Can send commands:** it enables remote operation for this user of the facilities they have access to
- **Enabled:** it enables or disables this user. It does not delete the user from the system, it just disables them until the next activation.

To apply the changes, you must save them via the **Save** button at the bottom of the screen.



3.1.8. Define facilities

This screen lets you indicate the facilities a user can access and the ones they cannot. To do so, use the checkbox at the end of each line. If you mark the checkbox, you will enable access, if you unmark it, you will disable access.

To apply the changes, you must save them via the **Save** button at the bottom of the screen.

The screenshot shows a window titled "User facilities" with a "Facility Filter" input field. Below it is a table with four rows, each representing a facility and its access status:

Facility Name	Facility ID	Access Status
hospital veteranos	(0AABA479)	<input type="checkbox"/>
Hospital San Juan de Dios	(EC-78-C3-2B)	<input checked="" type="checkbox"/>
Centro geriatrico	(7B-0B-77-C3)	<input type="checkbox"/>
Office Administration	(A1-A2-76-8E)	<input checked="" type="checkbox"/>

3.1.9. Add users

To add a new user to the system, the following fields must be added:

- **Username:** name of the user
- **Email:** it identifies each user and must be unique for each user
- **Password:** password for the new user
- **Confirm password:** repeat the user password
- **Role:** user type, which may be USER (basic user) or CLIENT_ADMIN (administrator user)
- **Can send commands:** Yes or No, whether you can operate the facility remotely or not. If not, then you will only be able to monitor it.
- **Enabled:** Yes or No; if not enabled, the user will not be able to access the system

Finally, save the new user using the **“Save”** button.

New User

The screenshot shows a "New User" form with the following fields and options:

- Username:** Input field with placeholder "Username"
- Email:** Input field with placeholder "e-mail"
- Password:** Input field with masked characters "••••••"
- Confirm password:** Input field with placeholder "Confirm password"
- Role:** Input field
- Timezone:** Input field with value "Europe/Berlin"
- Can send commands
- Enabled
- Buttons:** "Cancel" (red) and "Save" (green)

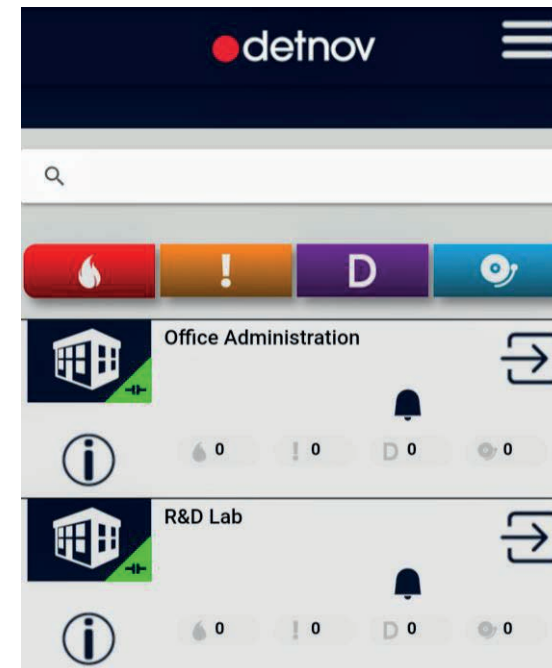
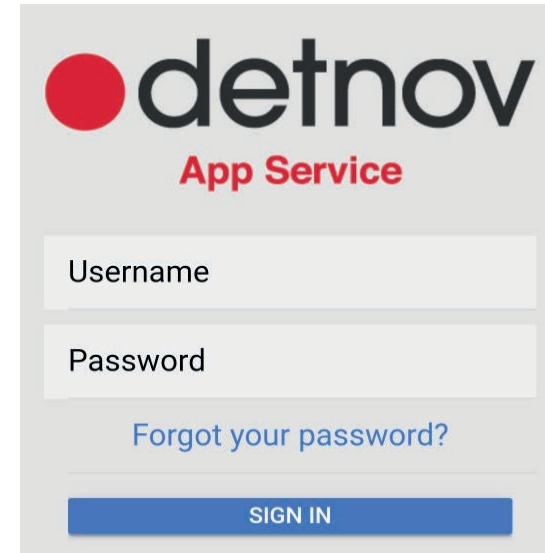
4. App

The Detnov APP can be downloaded free of charge from the Android Play Store and the iOS App Store. Once downloaded, it is important to set the permissions on your mobile device so that the app updates automatically, or it must be kept updated manually. Otherwise, incompatibilities may occur.

The app generates notifications automatically when it receives warnings from the Cloud server. It is recommended not to block the app's notifications in the operating system of your mobile device.

The app requires a user that is registered in the system to log in with their login credentials. Once logged in, a list of all the facilities available for that user appears.

If you need to reset the password, use the **“Forgot your password?”** option.



4.1. Main screen

The main screen consists of the following sections:

- **Main menu:** it contains the basic configuration options and the functions for connecting new facilities to the system.
- **Search bar:** it lets you search for a facility by name from all those currently shown in the list.
- **Event filters:** filters using 4 buttons to view control panels from the list that have events of the selected type.
 - o Fire events
 - o Fault events
 - o Disabled zone or point events
 - o Technical or information events

Facility list: it shows all the facilities to which the logged user has access. The active events of each type are shown for each one.

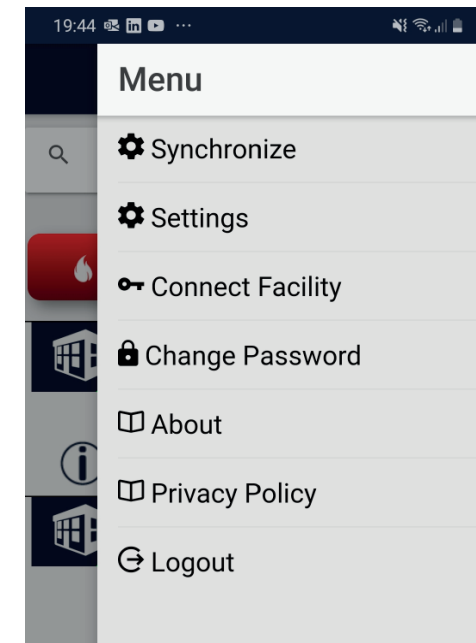


4.2. Main menu

By pressing the main menu button, the menu bar is displayed, as shown in the image below.

The options that appear are as follows:

- Synchronise
- Configuration
- Connect facility
- Change password
- Log out



4.2.1. Synchronise

It forces the synchronisation of the app with all of the facilities at that time. In any case, automatic synchronisation occurs every **2 minutes** if there is no event in the facility or instantaneously if the facility has new events to transmit.

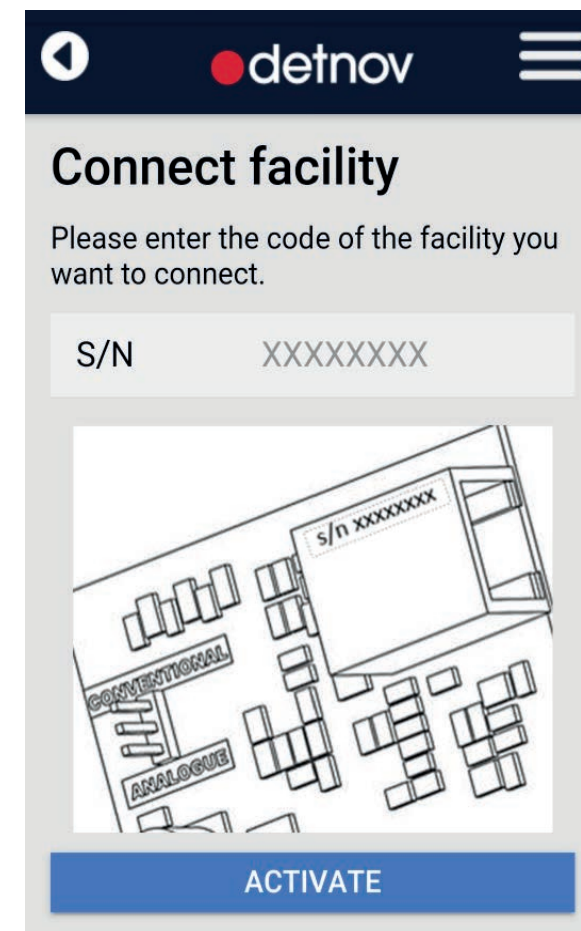
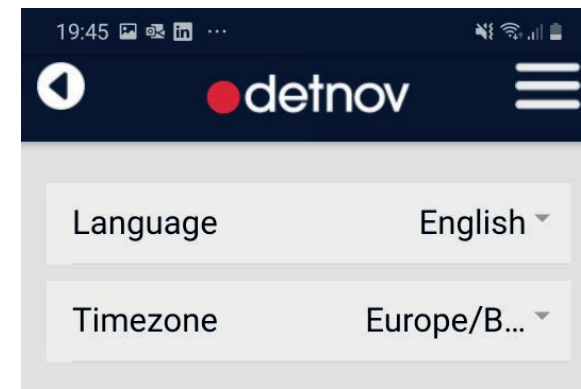
4.2.2. Configuration

It lets you choose between the different languages available for the app and set the correct time zone for the user.

4.2.3. - Connect facility

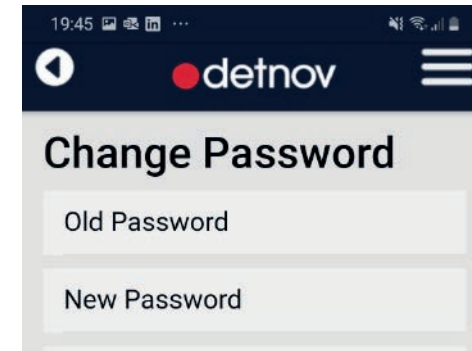
It lets you register new facilities in the system. The registration process is based on the serial number indicated on each cloud card. Enter it in the app and press "**ACTIVATE**".

From the moment a facility is activated, it forms part of the group to which the user who activated it belongs. This makes subsequent activation by another user impossible. To activate a facility, the card must be correctly connected to the control panel and the Internet via the card's RJ-45 connector.



4.2.4. Change password

It lets a user change their password for accessing the system, as shown in the image below.



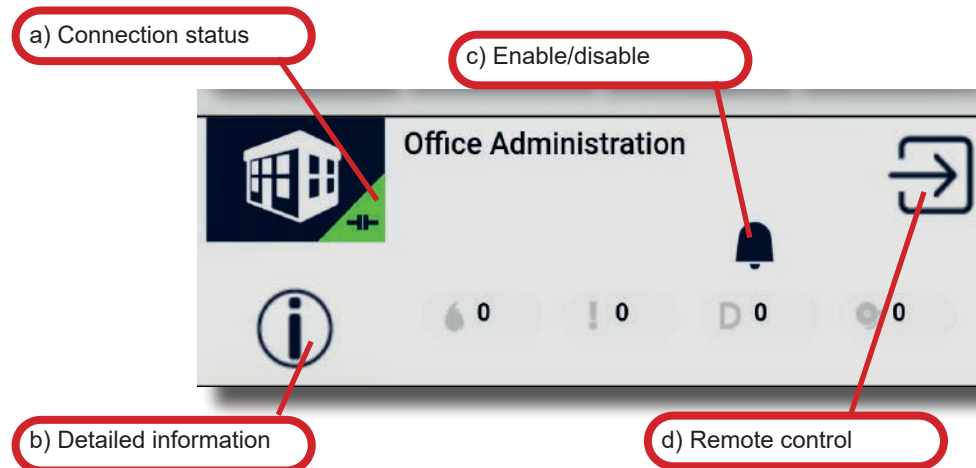
4.3. Facility list

For each facility, the facility list shows the following information:

a) Connection status: if the icon is green, it indicates that there is a connection between the control panel and the server. If the icon is grey, it indicates that there is no connection between the control panel and the server.

b) Detailed information button: by pressing it, a new information window appears for the facility, like the following one:

- o **Serial number:** single identification number of the cloud card
- o **Last connection:** time and date of the facility's last data transmission
- o **Panel type:** type of control panel installed
- o **Panel version:** version of the control panel program
- o **Cloud version:** version of the cloud card program
- o **Description:** brief description in the event of having defined it



WORK POINT 3

Serial number:84-12-5C-AB

Last connection:
17/09/2020 19:46

Panel Type: CAD150-4

Panel Version: 3.6

Cloud type:TRED250

Cloud version: 2.0.8

Description:

c) Button to enable or disable notifications

Enables or disables the generation of notifications from the app for that specific facility. If the button is a black bell, as shown in the previous image, notifications will be generated. Otherwise, if you press the button and the bell turns grey, the app will not generate notifications.

d) Button for accessing the remote control of the facility

4.4. Remote control of the facility

This screen consists of three tabs:

- Status
- Send command
- Event log

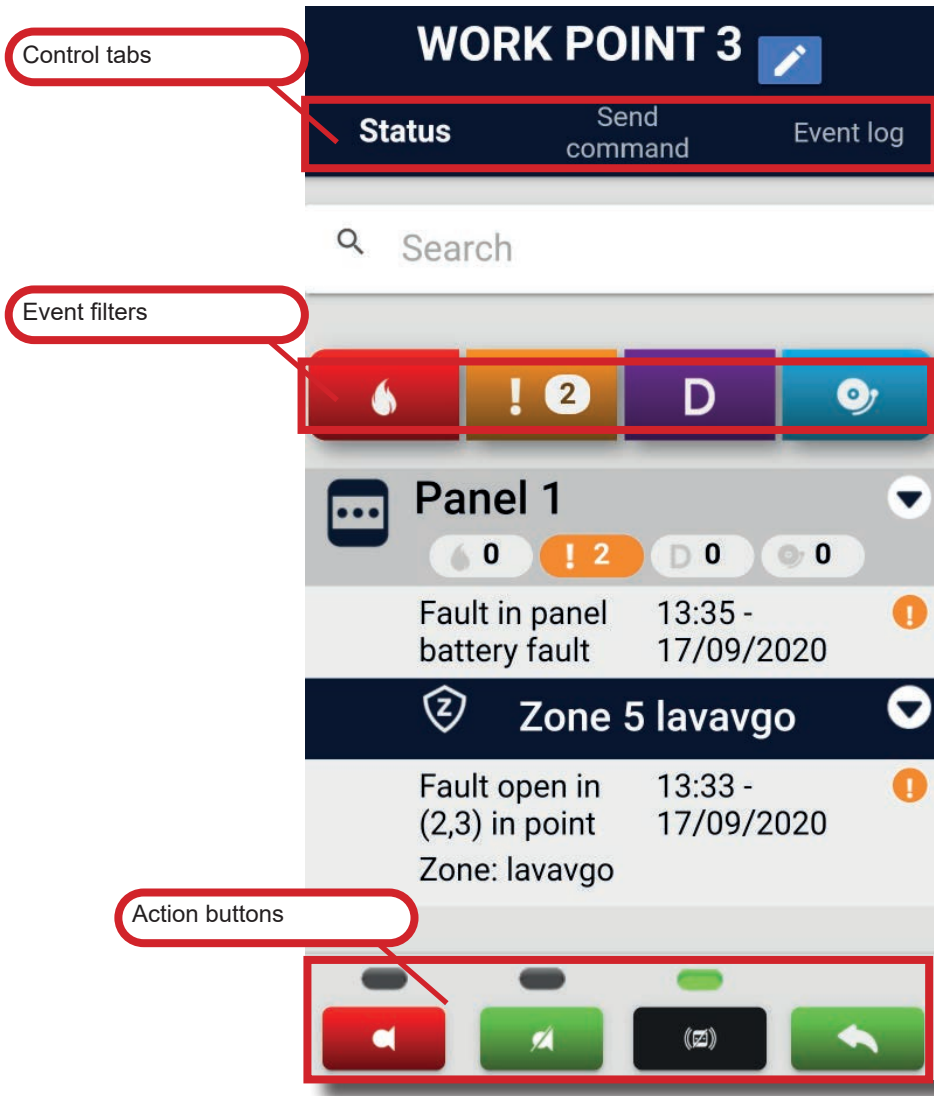
Status

This tab reflects the current status of the facility, showing the total number of fire, fault and disablement events, as well as technical events that are present. It also shows the events as the control panel shows them in the facility.

Apply the filters to view only those of the type you want to check.

The four action buttons on the control panel are at the bottom of the screen.

From left to right: activate sounders, mute sounders, mute control panel and reset control panel. The first three have a LED to indicate their status.

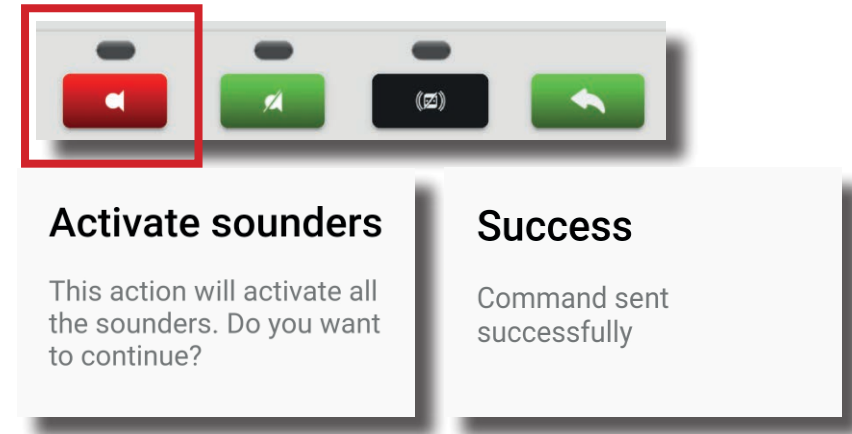


When you press the activate sounders button, a confirmation message will appear to prevent accidental activation.

Press YES to confirm

Press NO to discard

After sending any command from the app, a message should appear on the screen to notify that the command has been delivered to the cloud server.



4.5. Send command

From this tab, points and zones can be enabled and disabled.

Complete the following steps:

1) Select whether you want to enable/disable a zone or point by moving the selector to the left or right.

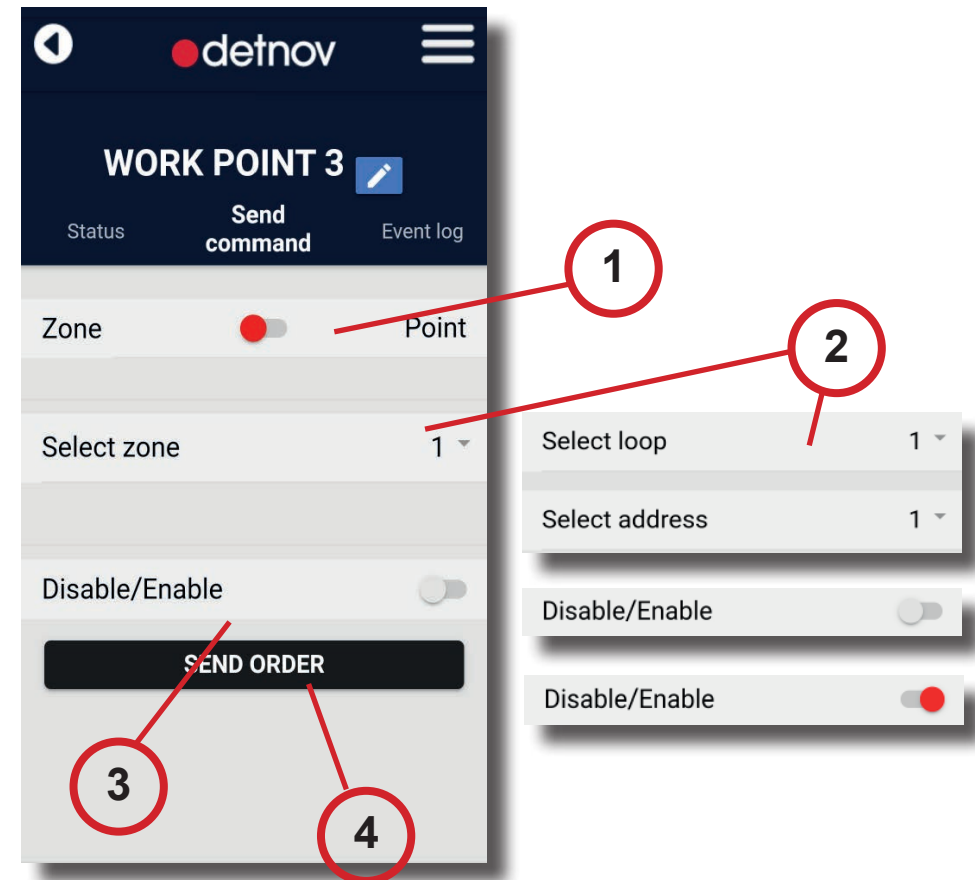
The “**point**” option will only be available if it is an addressable control panel.

2) The options in this field will change according to the options chosen in step 1.

Select the number of the zone or point to enable/disable.

3) Choose whether you want to enable or disable the entity selected in step 2.

4) Press the “**Send order**” button.



4.6. Event log

This tab lets you check the event log of the control panel.

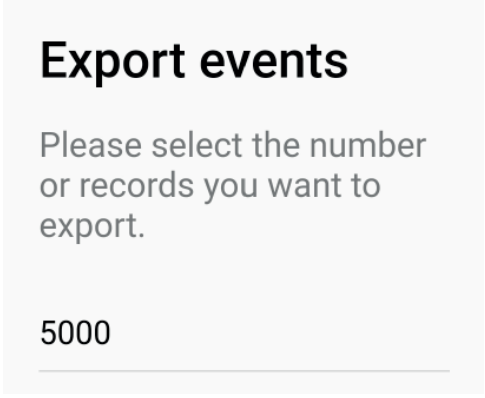
The events are arranged in chronological order, with the most recent at the top, and you can browse them all by scrolling down the screen.

It also lets you export the event log of the control panel to the mobile device via the "export" button.

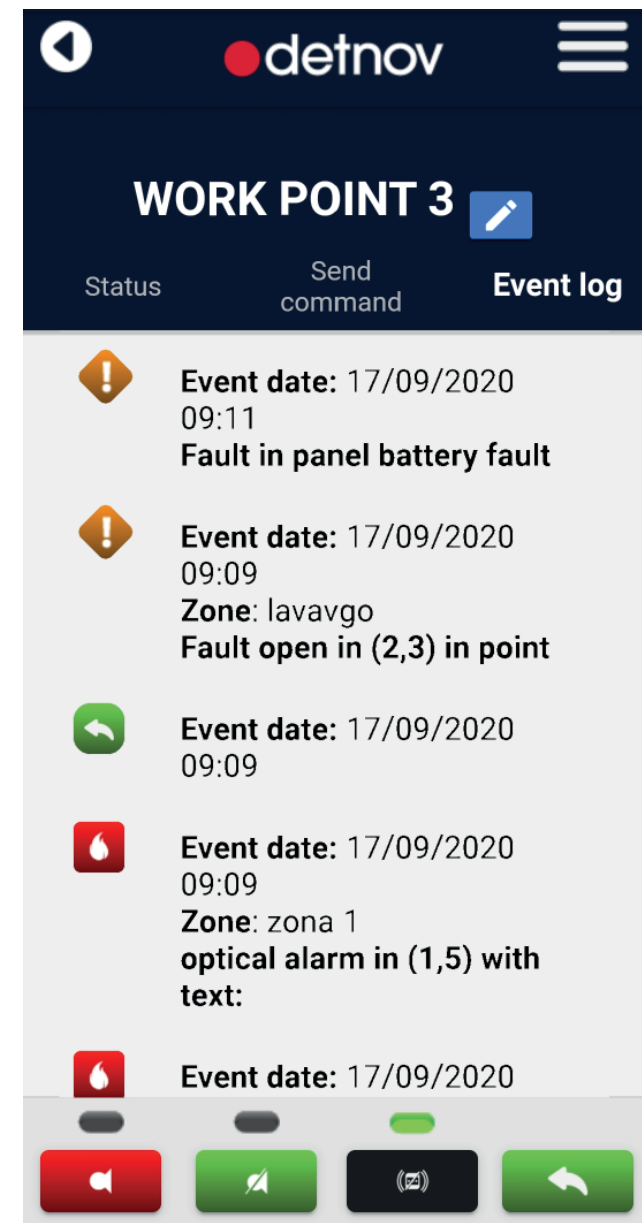
When you select this option, the app will ask you to indicate the number of logs that you want to export.

The app will generate a *.csv file that can be read easily with a spreadsheet program.

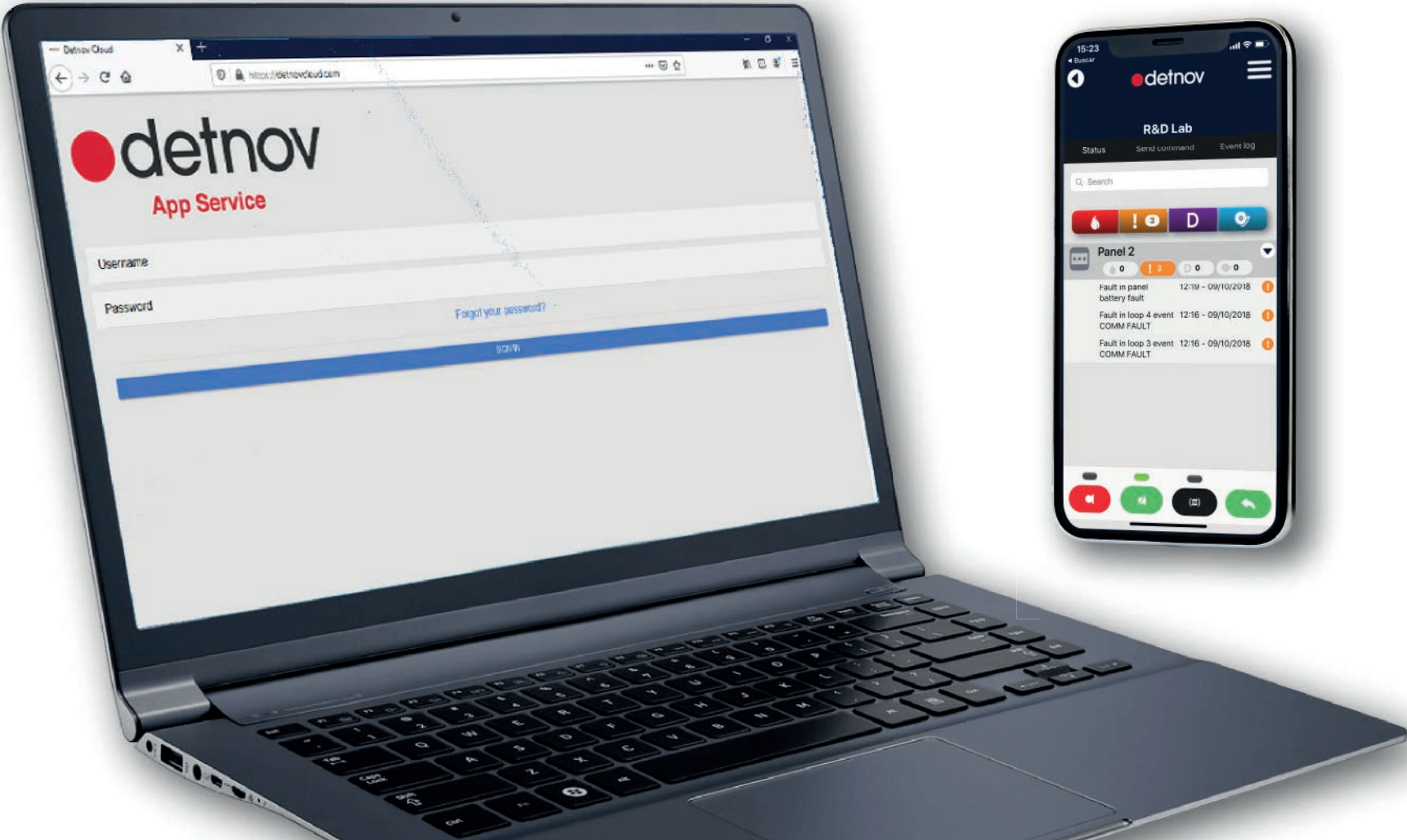
Send the log from your mobile device using the standard tools provided by your device.



1	Date	Facility	Type	Text	User	Source
2	17/09/2020 9:02	84-12-5C-AB	fault	Fault in panel battery fault		Panel: 1
3	17/09/2020 9:02	84-12-5C-AB	fault	Fault open in (2,3) in point		Panel: 1 Zone: 5 lavavgo Loop: 2 Address: 3
4	17/09/2020 9:02	84-12-5C-AB	reset			
5	07/09/2020 9:00	84-12-5C-AB	timeout	Timeout		
6	07/09/2020 5:50	84-12-5C-AB	fault	Fault in panel battery fault		Panel: 1
7	07/09/2020 5:50	84-12-5C-AB	reset			
8	07/09/2020 0:35	84-12-5C-AB	timeout	Timeout		
9	02/09/2020 12:08	84-12-5C-AB	fault	Fault in panel charger fault		Panel: 1
10	02/09/2020 10:13	84-12-5C-AB	reset			
11	02/09/2020 10:13	84-12-5C-AB	fault	Fault in panel battery fault		Panel: 1
12	02/09/2020 10:12	84-12-5C-AB	reset			
13	02/09/2020 9:51	84-12-5C-AB	timeout	Timeout		
14	31/08/2020 16:08	84-12-5C-AB	fault	Fault in panel charger fault		Panel: 1
15	31/08/2020 11:10	84-12-5C-AB	fault	Fault in loop 4 event COMM FAULT		Panel: 1
16	31/08/2020 11:10	84-12-5C-AB	fault	Fault in loop 3 event COMM FAULT		Panel: 1
17	31/08/2020 11:10	84-12-5C-AB	fault	Fault in loop 2 event COMM FAULT		Panel: 1
18	31/08/2020 11:10	84-12-5C-AB	fault	Fault in loop 1 event COMM FAULT		Panel: 1
19	31/08/2020 11:09	84-12-5C-AB	reset			



DETN OV CLOUD MANUAL DE USUARIO Y CONFIGURACION





1.	INTRODUCCION	6
2.	USUARIOS	6
2.1.	Usuarisos administradores.....	6
2.2.	Usuarios	6
3.	WEB	7
3.1.	Web administración.....	7
3.1.1.	Barra superior.....	7
3.1.2.	MIS INSTALACIONES	8
3.1.3.	Ver, detalle de instalación e importar registro de eventos.....	8
3.1.4.	Editar detalles de la instalación.....	9
3.1.5.	Usuarios	9
3.1.6.	Ver detalles de usuario.....	10
3.1.7.	Editar detalles de usuario.....	10
3.1.8.	Definir instalaciones	11
3.1.9.	Añadir Usuarios.....	11
4.	APLICACION	12
4.1.	Pantalla principal.....	13
4.2.	Menú principal.....	13
4.2.1.	Sincronizar	14
4.2.2.	Configuración	14
4.2.3.	Conectar instalación.....	14
4.2.4.	Cambiar contraseña.....	15
4.3.	Lista de instalaciones.....	15
4.4.	Control remoto de la instalación.....	16
4.5.	Enviar orden.....	17
4.6.	Registro de eventos	18

Control de revisiones

Revisión	Comentario	Fecha
a	Primera edición	17/09/2020
b	Correcciones gráficas y gestión web	17/11/2020

POLITICA DE PRIVACIDAD

Detnov Security S.L creó la aplicación Detnov App como una aplicación gratuita. Este SERVICIO es provisto por Detnov Security S.L sin costo y está diseñado para ser utilizado tal como es.

Esta página se utiliza para informar a los visitantes sobre nuestras políticas con la recopilación, el uso y la divulgación de información personal si alguien decide utilizar nuestro Servicio.

Si elige utilizar nuestro Servicio, entonces acepta la recopilación y el uso de la información en relación con esta política. La información personal que recopilamos se utiliza para proporcionar y mejorar el servicio. No usaremos ni compartiremos su información con nadie, excepto como se describe en esta Política de privacidad.

Los términos utilizados en esta política de privacidad tienen los mismos significados que en nuestra página web en la dirección <https://www.detnov.com/politica-de-privacidad/> y a menos que se defina explícitamente lo contrario en esta política de privacidad.

Recopilación y uso de información

Para una mejor experiencia, mientras usamos nuestro Servicio, es posible que le solicitemos que nos brinde cierta información de identificación personal, que incluye, entre otros, la identificación del dispositivo, el nombre de usuario, el apellido y el correo electrónico. Nosotros retendremos la información que solicitamos y la utilizaremos como se describe en esta política de privacidad.

La aplicación utiliza servicios de terceros que pueden recopilar información utilizada para identificarlo.

Enlace a la política de privacidad de los proveedores de servicios de terceros utilizados por la aplicación Servicios de Google Play El fabricante o los distribuidores de esta gama de paneles contra incendios no pueden aceptar ninguna responsabilidad por cualquier Interpretación errónea de una nota de instrucción u orientación o por el cumplimiento del sistema por entero.

La política del fabricante es de mejora continua y nos reservamos el derecho de realizar cambios en las especificaciones del producto a nuestra discreción y sin previo aviso.

Un montaje deficiente, una instalación inapropiada o una mala configuración del equipo, el estado del cableado de detección no son responsabilidad del fabricante de la central.

Dato de registro

Queremos informarle que siempre que utilice nuestro Servicio, en caso de un error en la aplicación, recopilamos datos e información (a través de productos de terceros) en su teléfono llamado Datos de registro. Estos datos de registro pueden incluir información como la dirección del Protocolo de Internet ("IP") de su dispositivo, el nombre del dispositivo, la versión del sistema operativo, la configuración de la aplicación cuando utiliza nuestro Servicio, la fecha y hora de uso del Servicio y otras estadísticas.

Cookies

Las cookies son archivos con una pequeña cantidad de datos que se utilizan comúnmente como identificadores únicos anónimos. Estos se envían a su navegador desde los sitios web que visita y se almacenan en la memoria interna de su dispositivo.

Este Servicio no utiliza estas “cookies” explícitamente. Sin embargo, la aplicación puede usar códigos de terceros y bibliotecas que usan “cookies” para recopilar información y mejorar sus servicios. Tiene la opción de aceptar o rechazar estas cookies y saber cuándo se envía una cookie a su dispositivo. Si decide rechazar nuestras cookies, es posible que no pueda utilizar algunas partes de este Servicio.

Proveedores de servicio

Es posible que contratemos a empresas y personas de terceros debido a los siguientes motivos:

Para facilitar nuestro Servicio;

Para proporcionar el Servicio en nuestro nombre;

Para realizar servicios relacionados con el servicio; o

Para ayudarnos a analizar cómo se utiliza nuestro servicio.

queremos informar a los usuarios de este Servicio que estos terceros tienen acceso a su Información personal. El motivo es realizar las tareas asignadas a ellos en nuestro nombre. Sin embargo, están obligados a no divulgar o utilizar la información para ningún otro propósito.

Seguridad

Valoramos su confianza al proporcionarnos su información personal, por lo que nos esforzamos por utilizar medios comercialmente aceptables para protegerla. Pero recuerde que ningún método de transmisión a través de Internet o de almacenamiento electrónico es 100% seguro y confiable, y no podemos garantizar su absoluta seguridad.

Enlaces a otros sitios

Este servicio puede contener enlaces a otros sitios. Si hace clic en un enlace de terceros, se le dirigirá a ese sitio. Tenga en cuenta que estos sitios externos no son operados por nosotros. Por lo tanto, le recomendamos encarecidamente que revise la Política de privacidad de estos sitios web. no tenemos control ni asumimos responsabilidad alguna por el contenido, las políticas de privacidad o las prácticas de los sitios o servicios de terceros.

Privacidad de los niños

Estos Servicios no se dirigen a personas menores de 13 años. No recopilamos, a sabiendas, información de identificación personal de niños menores de 13 años. En el caso de que descubramos que un niño menor de 13 años nos ha proporcionado información personal, lo eliminamos de inmediato de nuestros servidores. Si usted es un padre o tutor y sabe que su hijo nos ha proporcionado información personal, comuníquese con nosotros para que podamos realizar las acciones necesarias.

Cambios a esta política de privacidad

Podemos actualizar nuestra Política de Privacidad de vez en cuando. Por lo tanto, se recomienda revisar esta página periódicamente para ver si hay cambios. Le notificaremos cualquier cambio mediante la publicación de la nueva Política de privacidad en esta página. Estos cambios entrarán en vigor inmediatamente después de su publicación en esta página.

1. INTRODUCCION

Detnov Cloud es la solución de conectividad remota asentada en la nube que los mantenedores estaban esperando. Dicha solución les permitirá ofrecer nuevos servicios, a sus clientes, a través de una aplicación que se instala en los teléfonos móviles, tabletas u ordenadores. Permite conocer, en tiempo real, la información de todo el parque de sus instalaciones, con monitorización y control remoto, si se disponen de los permisos pertinentes, activación y desactivación de zonas o dispositivos remotamente.

La tarjeta de comunicación TCP/IP, con referencia TED-151-CL, se instala en el interior de la gama de centrales convencionales y centrales analógicas Detnov, lo cual nos permite la conexión a Internet de las centrales a través del puerto Ethernet que viene en la placa de la tarjeta.

La nube se estructura en grupos cerrados y cifrados de tal modo que, los usuarios de un grupo solo tienen acceso a las instalaciones que pertenezcan a ese grupo. Así, se garantiza la confidencialidad de las instalaciones y la seguridad de uso para cada una de ellas.

Este manual detalla los aspectos necesarios para gestionar y manipular la detnov Cloud tanto en su interfaz web como en la aplicación para móvil.

Para poder acceder a los servicios de la cloud, es indispensable que se ponga en contacto con su distribuidor y le solicite el alta en la nube.

2. USUARIOS

Cada persona que use los servicios de la detnov cloud debe tener su usuario en el sistema. Existen dos niveles de usuarios:

- Usuarios administradores
- Usuarios

El sistema esta dimensionado para que cada grupo tenga un máximo de **10 usuarios**, pónganse en contacto con su distribuidor en caso de requerir más.

2.1. USUARIOS ADMINISTRADORES

Un usuario administrador será el primero del grupo, para obtenerlo debe solicitar el alta en el servicio a su distribuidor. En el momento en el que reciba las credenciales podrá empezar a utilizar la detnov cloud.

Únicamente los responsables de su grupo, pueden dar de alta o baja otros administradores o usuarios, desactivar temporalmente usuarios, permitir o restringir el acceso de cada usuario a las instalaciones y definir los permisos de los mismos.

Además, igual que los usuarios, pueden utilizar el sistema para controlar y monitorizar las instalaciones y dar de alta nuevas instalaciones en su grupo.

2.2. USUARIOS

Para acceder a ambas páginas web son necesarias las credenciales de un usuario del sistema facilitadas por su distribuidor en caso de ser el primer usuario, o por el administrador de su sistema en caso de no ser el primero.

Las funcionalidades descritas en los siguientes apartados del manual son las que están disponibles para los usuarios administradores del sistema. En caso de acceder al sistema como usuario no aparecerán algunas de las funcionalidades mostradas a continuación.

3. WEB

El servicio incluye la páginas web:

- **www.mydetnov.com**

Esta página permite la administración de todas las instalaciones a las que se tiene acceso, así como la gestión de los usuarios de su grupo

Para acceder a ambas páginas web son necesarias las credenciales de un usuario del sistema facilitadas por su distribuidor en caso de ser el primer usuario, o por el administrador de su sistema en caso de no ser el primero.

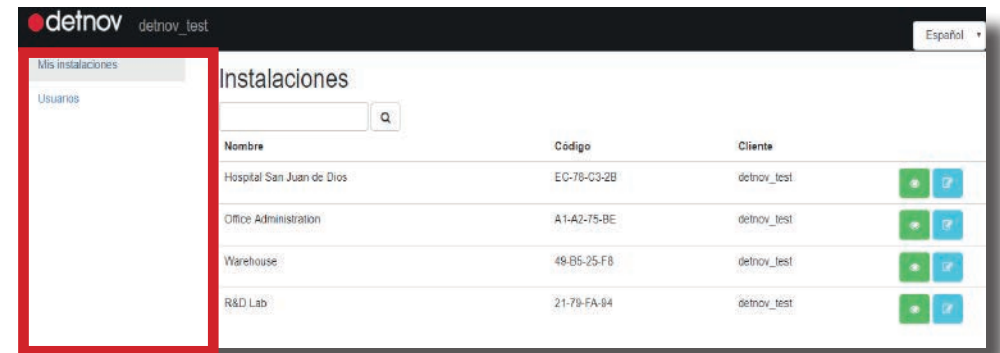
Las funcionalidades descritas en los siguientes apartados del manual son las que están disponibles para los usuarios administradores del sistema. En caso de acceder al sistema como usuario no aparecerán algunas de las funcionalidades mostradas a continuación.

3.1. WEB ADMINISTRACIÓN

Para gestionar sus cuentas o vincular instalaciones acceda al gestor en **www.mydetnov.com**.

Esta es la página desde la que se puede administrar el grupo al que pertenece. El marco izquierdo presenta dos opciones de configuración.

- Mis instalaciones
- Usuarios



3.1.1. Barra superior

En la barra superior aparecen los siguientes campos:

- **Nombre del grupo:** empresa “detnov-test”
- **Idioma:** opción para seleccionar el idioma
- **Nombre del usuario:** “Usuario”
- **Logout:** opción para salir de la página



3.1.2. MIS INSTALACIONES

En la página de instalaciones se muestran todas las instalaciones a las que tiene acceso el usuario. Para cada una de ellas se especifican los siguientes campos:

- **Nombre:** el descriptivo de la instalación
- **Código:** Identificativo único para cada una de las tarjetas que conectan las instalaciones con la detnov cloud
- **Cliente:** Grupo al que pertenece cada instalación. Siempre debe mostrar el nombre de su empresa para todas.

Además, para cada instalación hay dos botones de ver y editar al final de cada línea:

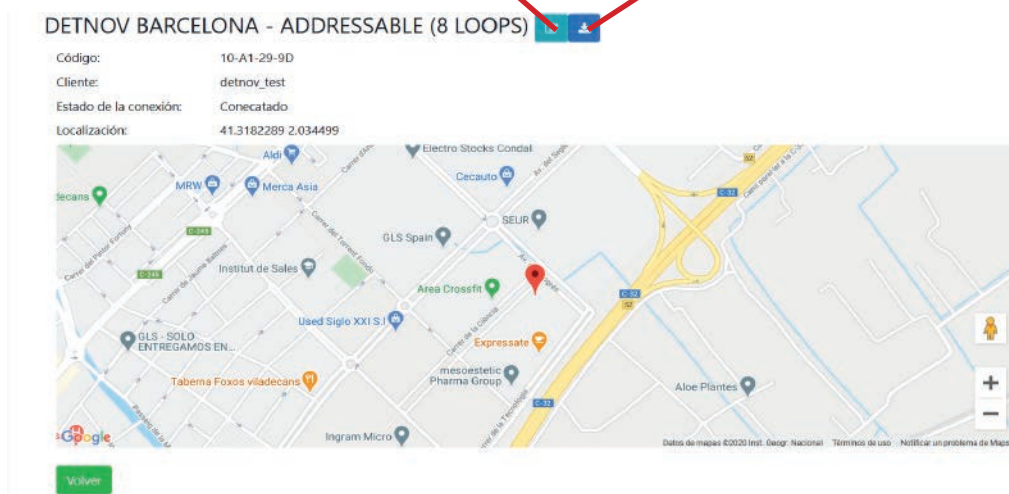
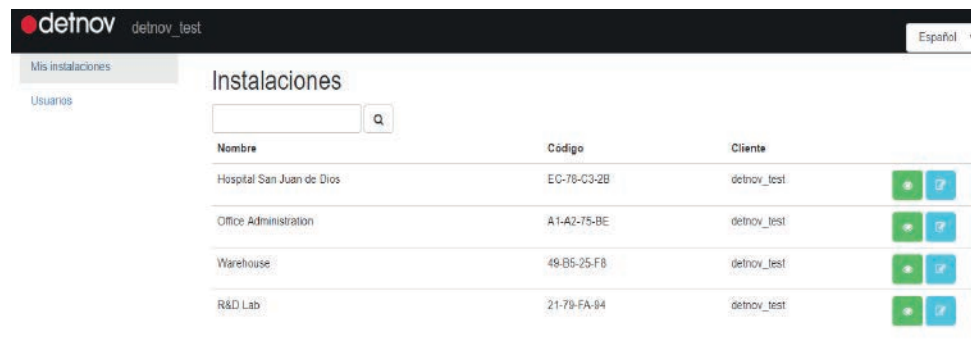
- **Ver:** Permite ver los detalles de la instalación
- **Editar:** Permite hacer modificaciones en los detalles de la instalación

3.1.3. Ver detalles.

Para cada instalación se muestran los siguientes detalles:

- **Nombre:** "Office Administration"
- **Código:** "A1-A2-75-BE", identificador único de la tarjeta
- **Cliente:** "detnov_test", grupo al que pertenece
- **Estado de la conexión:** Puede mostrar Conectado o Desconectado dependiendo de si el servidor tiene conexión con la tarjeta de la instalación.
- **Localización:** muestra las coordenadas GPS y el plano de la ubicación definida para la instalación

Junto al nombre de la instalación aparecen dos botones, el primero para editar los detalles de la instalación y el segundo para exportar el registro de eventos de la instalación.



3.1.4. Editar detalles de la instalación.

Esta pantalla permite definir y editar los campos:

- Nombre de la instalación
- Localización de la instalación

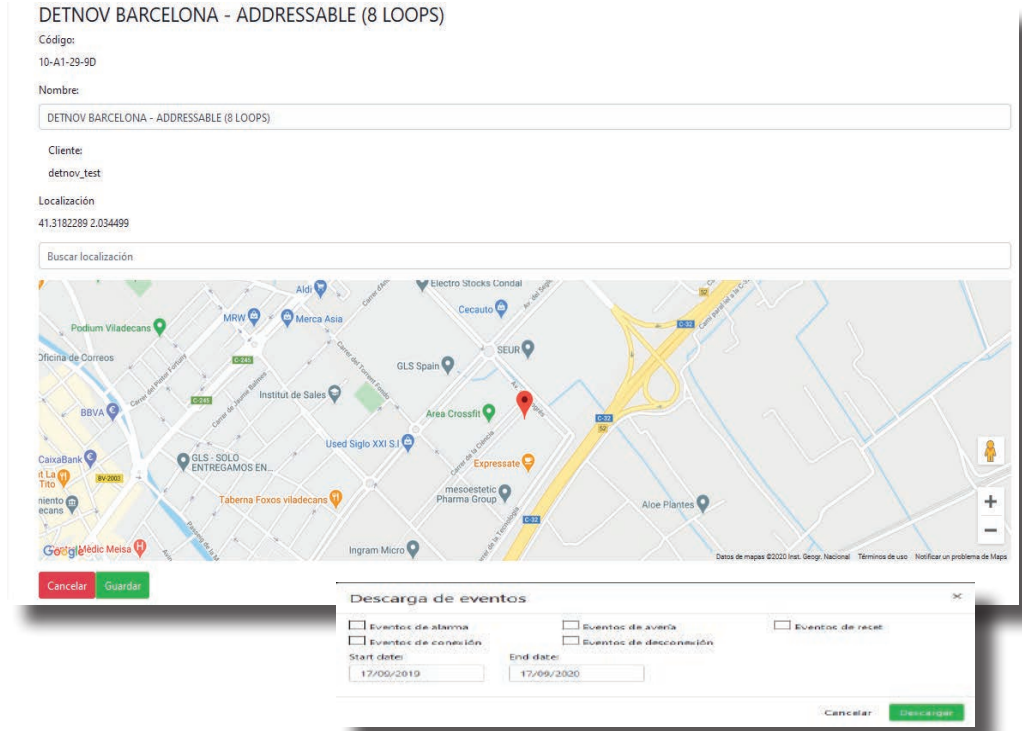
Para aplicar los cambios es necesario guardar mediante el botón **Guardar** ubicado al pie de la página.

Al pulsar el icono Exportar, tendrá acceso a una pantalla emergente que le permitirá seleccionar el tipo de eventos a exportar

Seleccion los eventos y el periodo del cual desea descargar los eventos

Pulse **Descargar** para iniciar el proceso de exportación

Pulse **Cancelar** para descartar la operación



3.1.5. Usuarios

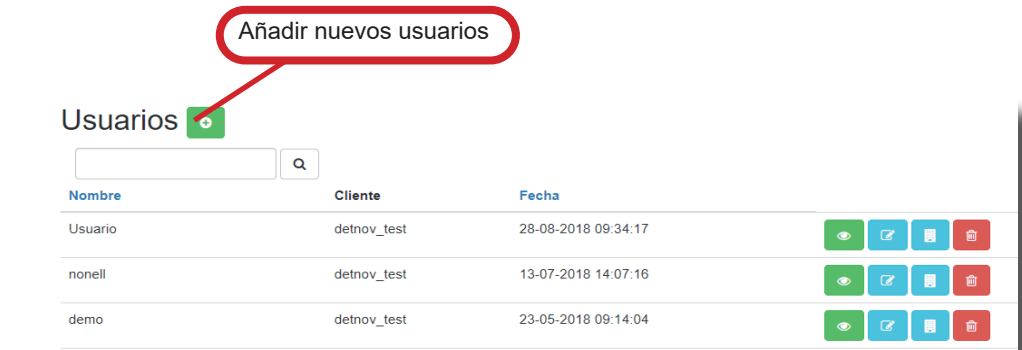
Desde esta pantalla se pueden ver todos los usuarios del grupo y para cada uno de ellos los siguientes campos:

- **Nombre:** identificador del usuario
- **Cliente:** grupo al que pertenecen. Siempre debe mostrar el nombre de su empresa para todos
- **Fecha:** fecha de alta en el sistema

Además, para cada usuario hay cuatro botones al final de cada línea. De izquierda a derecha:

- **Ver:** permite ver los detalles del usuario.
- **Editar:** permite editar los detalles del usuario
- **Definir instalaciones:** permite ver y definir las instalaciones del grupo a las que el usuario tiene acceso.
- **Eliminar:** borra el usuario del sistema.

En la parte superior, junto a **“Usuarios”**, aparece el botón para añadir nuevos usuarios al grupo.

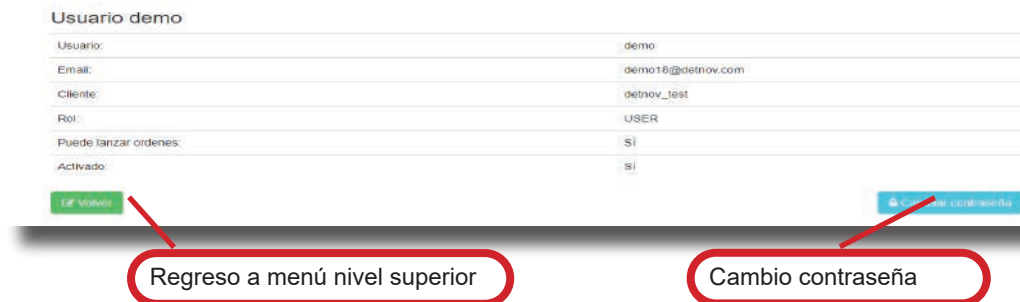


3.1.6. Ver detalles de usuario.

Para cada usuario se muestran los detalles siguientes:

- **Usuario:** nombre del usuario
- **Email:** identificativo de cada usuario, debe ser único para cada usuario
- **Cliente:** grupo al que pertenece
- **Rol:** tipo de usuario, puede ser USER (usuario básico) o CLIENT_ADMIN (usuario administrador)
- **Puede lanzar ordenes:** Si o No, si puede manipular la instalación remotamente o no. En caso de que no, solo podrá monitorizarla.
- **Activado:** Si o No, si no está activado el usuario no podrá acceder al sistema.

En la parte inferior derecha está el botón para cambiar la contraseña del usuario. Para cambiar la contraseña no es necesario conocer la contraseña actual del usuario. Así, cualquier administrador del grupo puede cambiar la clave de los otros usuarios del grupo.



3.1.7. Editar detalles de usuario

Para cada usuario se pueden editar los siguientes campos:

- **Usuario:** Nombre del usuario
- **Email:** email identificativo del usuario, debe ser único para cada usuario.
- **Rol:** USER o CLIENT_ADMIN, si el usuario es usuario básico o usuario administrador
- **Zona horaria:** Zona horaria para cada usuario, debe definirse a la ciudad más cercana entre las disponibles para que el sistema tenga en cuenta los cambios de horario verano/invierno locales.
- **Puede lanzar ordenes:** habilitar la operación remota para este usuario de las instalaciones a las que tenga acceso.
- **Activado:** habilitar o deshabilitar a este usuario. No elimina al usuario del sistema, solo lo desactiva hasta la próxima activación.

Para aplicar los cambios es necesario **Guardar** mediante el botón ubicado al pie de la página.



3.1.8. Definir instalaciones

Esta pantalla le permite indicar a que instalaciones puede tener acceso un usuario y a cuáles no. Para ello es necesario utilizar el cuadro de selección al final de cada línea. En caso de marcar la casilla de selección, se habilitará el acceso, en caso de desmarcarla se deshabilitará el acceso.

Para aplicar los cambios es necesario **Guardar** mediante el botón ubicado al pie de la página.

User facilities

Facility Filter

hospital veteranos	(0AABA479)	<input type="checkbox"/>
Hospital San Juan de Dios	(EC-78-C3-2B)	<input checked="" type="checkbox"/>
Centro geriatrico	(7B-0B-77-C3)	<input type="checkbox"/>
Office Administration	(A1-A2-76-BE)	<input checked="" type="checkbox"/>

3.1.9. Añadir Usuarios

Para añadir un nuevo usuario al sistema se deben añadir los campos siguientes:

- **Usuario:** nombre del usuario
- **Email:** identificativo de cada usuario, debe ser único para cada usuario
- **Contraseña:** clave para el nuevo usuario
- **Confirmar contraseña:** repetir clave usuario
- **Rol:** tipo de usuario, puede ser USER (usuario básico) o CLIENT_ADMIN (usuario administrador)
- **Puede lanzar ordenes:** Si o No, si puede manipular la instalación remotamente o no. En caso de que no, solo podrá monitorizarla.
- **Activado:** Si o No. Si no está activado el usuario no podrá acceder al sistema

Finalmente, se debe guardar el nuevo usuario mediante el botón **“Guardar”**.

Nuevo usuario

Usuario:

Email:

Contraseña:

Confirmar contraseña:

Rol:

Timezone:

Puede lanzar ordenes

Activado

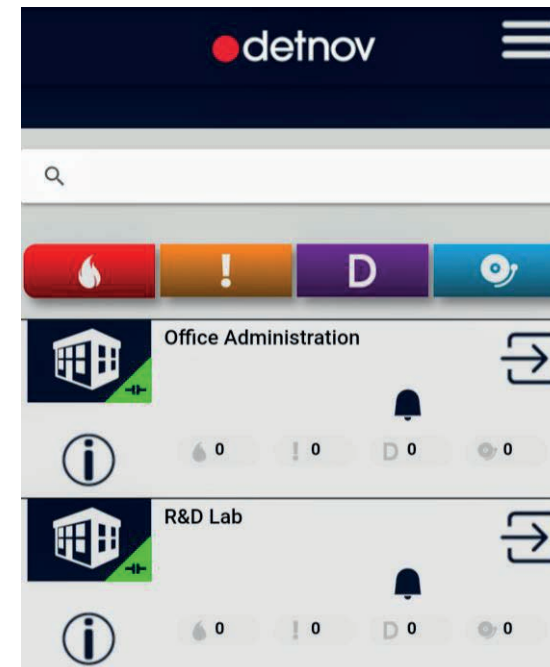
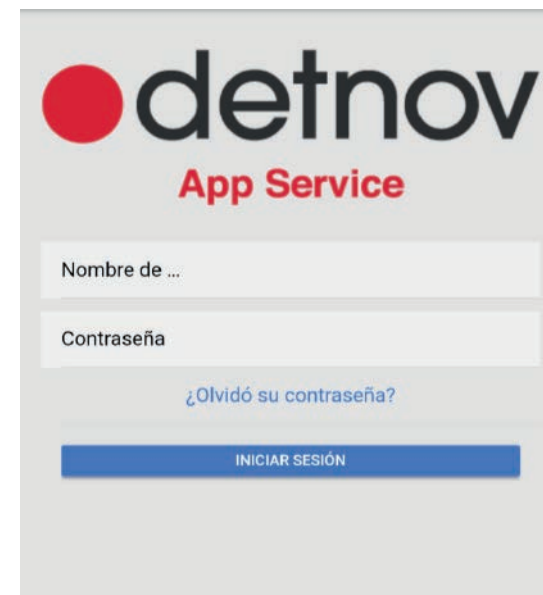
4. Aplicación

La aplicación Detnov APP está disponible para su descarga gratuita tanto en el play Store de Android como en la app Store de iOS. Es importante que una vez descargada se establezcan los permisos en su dispositivo móvil para que la aplicación se actualice automáticamente, o mantenerla actualizada manualmente. De lo contrario, puede haber incompatibilidades.

La aplicación genera notificaciones automáticamente al recibir avisos desde el servidor de la Cloud. Se recomienda no bloquear las notificaciones de la aplicación en el sistema operativo del dispositivo móvil.

La aplicación requiere que un usuario dado de alta en el sistema inicie sesión con sus credenciales. Una vez iniciada la sesión se muestra una lista con todas las instalaciones disponibles para ese usuario.

En caso de necesitar restablecer la contraseña se debe usar la opción “¿Olvidó su contraseña?”



4.1. Pantalla principal

La pantalla principal consta de las siguientes partes:

- **Menú principal:** contiene las opciones básicas de configuración y la funcionalidad para conectar nuevas instalaciones al sistema.
- **Barra de búsqueda:** Permite buscar por el nombre una instalación entre todas las que haya en la lista en ese momento.
- **Filtros por eventos:** Filtros mediante 4 botones para ver aquellas centrales de la lista que tengan presentes eventos del tipo seleccionado.
 - o Eventos de fuego
 - o Eventos de avería
 - o Eventos de puntos o zonas deshabilitados
 - o Eventos técnicos o de tipo información

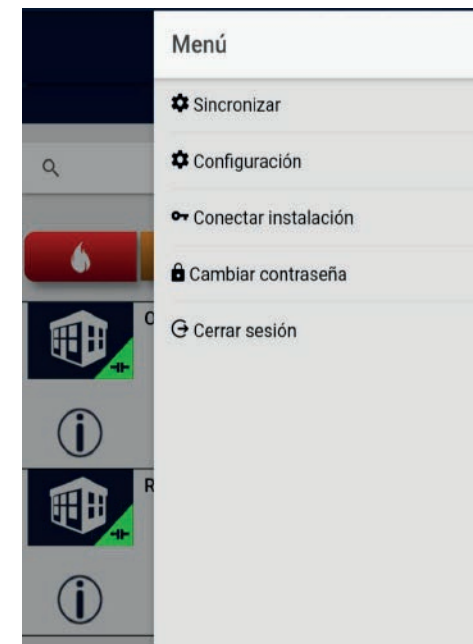
Lista de instalaciones: muestra todas las instalaciones a las que el usuario conectado tiene acceso. Para cada una de ellas muestra los eventos activos de cada tipo.

4.2. Menú principal

Al pulsar sobre el botón del menú principal se despliega la barra de menú, tal y como muestra la imagen a continuación.

Las opciones que aparecen son las siguientes:

- Sincronizar
- Configuración
- Conectar Instalación
- Cambiar contraseña
- Cerrar sesión



4.2.1. Sincronizar

Fuerza la sincronización de la aplicación con todas las instalaciones en ese instante. De todos modos, la sincronización automática se produce cada **2 minutos** si no existe ningún evento en la instalación o instantáneamente si la instalación tiene nuevos eventos que transmitir.

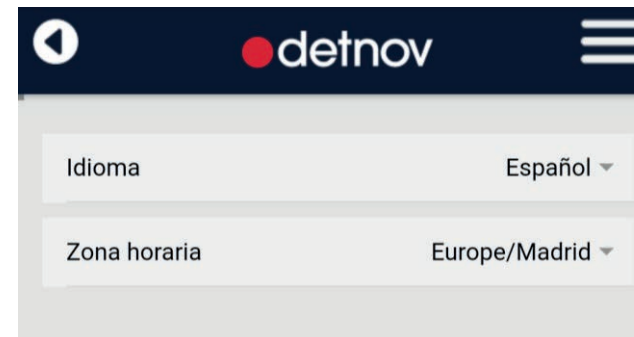
4.2.2. Configuración

Permite escoger entre los diferentes idiomas disponibles para la aplicación y establecer la zona horaria correcta para el usuario.

4.2.3. - Conectar instalación

Permite dar de alta nuevas instalaciones en el sistema. El proceso de alta se basa en el número de serie indicado en cada una de las tarjetas cloud, debe ser introducido en la aplicación y pulsar **“ACTIVATE”**.

A partir del momento en que se activa una instalación, ésta forma parte del grupo al que pertenece el usuario que la ha activado. De este modo se imposibilita una activación posterior por parte de otro usuario. Para activar una instalación es imprescindible que la tarjeta esté debidamente conectada a la central y a internet mediante el conector RJ-45 de la tarjeta.



4.2.4. Cambiar contraseña

Permite a un usuario cambiar su contraseña de acceso al sistema, tal y como muestra la imagen a continuación.

4.3. Lista de instalaciones

La lista de instalaciones muestra para cada una de las instalaciones la siguiente información:

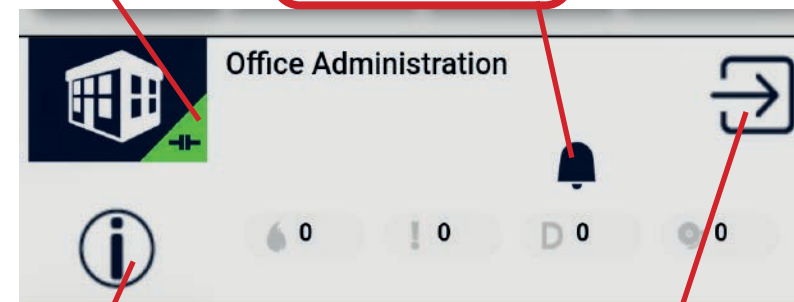
a) Estado de la conexión: Si el icono está de color verde indica que hay conexión entre la central y el servidor. Si el icono se muestra en color gris, indicará que no existe conexión entre la central y el servidor

b) Botón de información detallada: Al pulsarlo se muestra una nueva ventana de información de la instalación como la siguiente:

- o **Número de serie:** número identificativo único de la tarjeta cloud
- o **Última conexión:** momento de la última transmisión de datos de la instalación
- o **Tipo de panel:** tipo de central instalada
- o **Versión de panel:** versión de programa que tiene la central
- o **Versión de cloud:** versión de programa que tiene la tarjeta cloud
- o **Descripción:** breve descripción en caso de haberla definido.

a) Estado de conexión

c) Activar/Desactivar



b) Información detalle

d) Control remoto

Office Administration

Número de serie:A1-A2-75-BE
Última conexión: 28/08/2018
 12:26
Tipo de panel: CAD150
Versión de panel: 2.83
Versión de cloud: 0.1.9
Descripción:

OK

c) Botón para activar o desactivar notificaciones

Activa o desactiva la generación de notificaciones de la aplicación para esa instalación en concreto. Si el botón es una campana de color negro, tal y como muestra la imagen anterior, se generarán notificaciones. De lo contrario, si se pulsa el botón y la campana toma un color gris, la aplicación no generará notificaciones.

d) Botón para acceder al control remoto de la instalación.

4.4. Control remoto de la instalación

Esta pantalla consta de tres pestañas:

- Estado
- Enviar orden
- Registro de eventos

Estado

Esta pestaña refleja el estado actual de la instalación, muestra el número total de eventos de fuego, averías, deshabilitaciones y eventos técnicos presentes en ella. Además, muestra los eventos tal y como los muestra la central en la instalación.

Aplique los filtros para ver solo los del tipo que desee revisar.

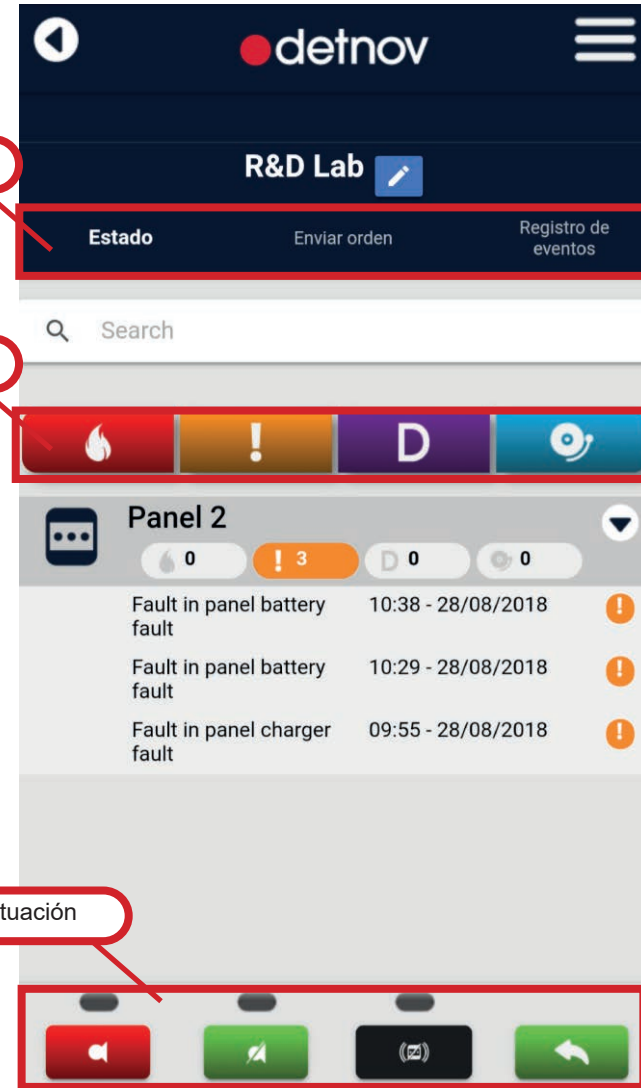
En la parte inferior de la pantalla, están los cuatro botones de actuación sobre la central.

De izquierda a derecha: activar sirenas, silenciar sirenas, silenciar central y rearmar central. Los tres primeros tienen un led sobre ellos para indicar su estado.

Pestañas de control

Filtros de eventos

Botones de actuación

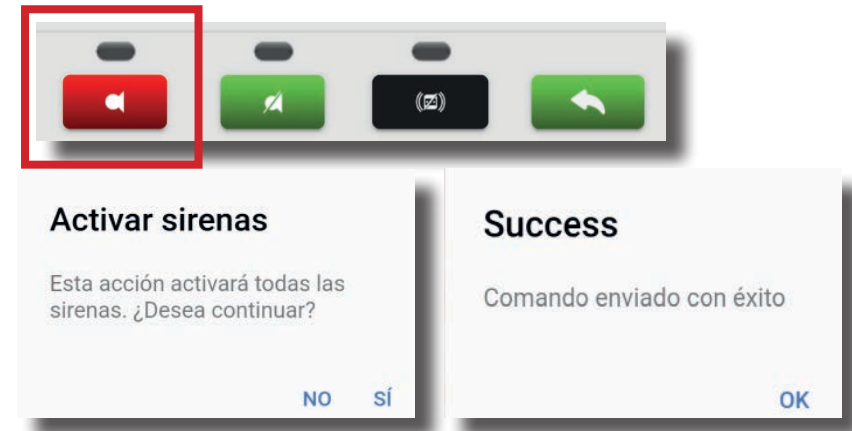


Al pulsar el botón activar sirenas se mostrará un mensaje de confirmación para evitar activaciones accidentales.

Pulse SI para confirmar

Pulse NO para descartar

Tras enviar cualquier comando desde la aplicación debe aparecer en pantalla un mensaje notificando que el comando ha sido entregado al servidor de la nube.



4.5. Enviar orden

Desde esta pestaña se pueden habilitar y deshabilitar puntos y zonas.

Los pasos a seguir son los siguientes:

1) Seleccionar si se desea habilitar/deshabilitar una zona o un punto desplazando el selector a izquierda o derecha.

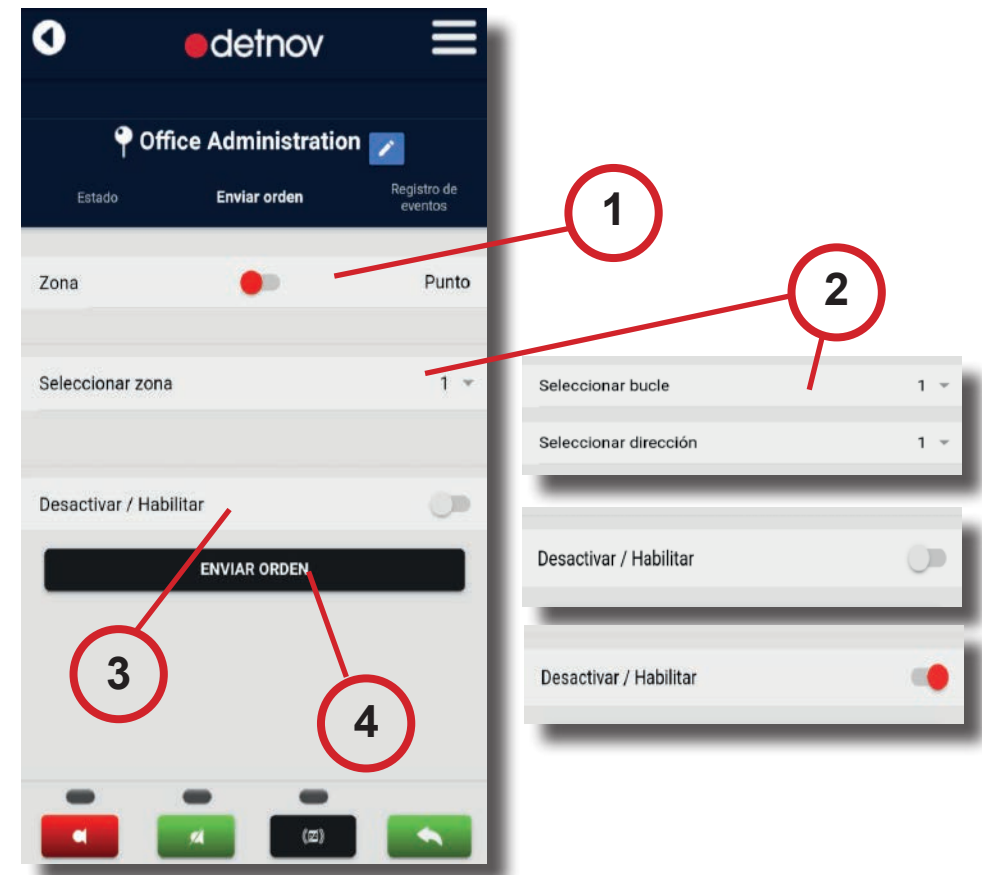
La opción **"punto"** solo estará disponible si se trata de una central analógica

2) Las opciones en este campo cambiarán según sea la opción escogida en el paso 1.

Seleccione el número de la zona a habilitar/deshabilitar o el del punto

3) Seleccione si se desea habilitar o deshabilitar la entidad seleccionada en el paso 2.

4) Pulse el botón **"Enviar orden"**



4.6. Registro de eventos

Desde esta pestaña se puede consultar el registro de eventos de la central.

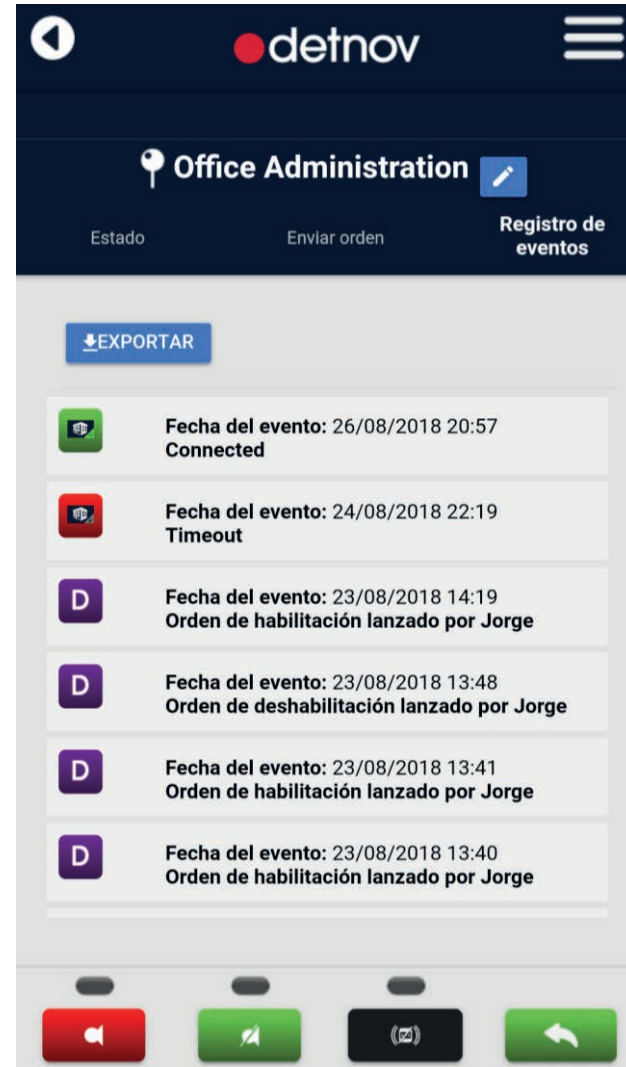
Los eventos están ordenados cronológicamente, los más recientes arriba, y se puede navegar por todos ellos moviéndose por la pantalla hacia abajo.

Además, permite exportar el registro de eventos de la central al dispositivo móvil mediante el botón “exportar”.

Al seleccionar esta opción, la aplicación pedirá que se indique el número de registros que se quiere exportar.

La aplicación generará un archivo *.csv que puede ser fácilmente leído con un programa de hoja de cálculo.

Envíe el registro desde su terminal móvil empleando las herramientas estandar que le ofrece e propio terminal



1	Date	Facility	Type	Text	User	Source
2	17/09/2020 9:02	84-12-SC-AB	fault	Fault in panel battery fault		Panel: 1
3	17/09/2020 9:02	84-12-SC-AB	fault	Fault opens in (2,3) in point		Panel: 1 Zone: 5 Lavago Loop: 2 Address: 3
4	17/09/2020 9:02	84-12-SC-AB	reset			
5	07/09/2020 09:00	84-12-SC-AB	timeout	Timeout		Panel: 1
6	07/09/2020 5:50	84-12-SC-AB	fault	Fault in panel battery fault		Panel: 1
7	07/09/2020 5:50	84-12-SC-AB	reset			
8	07/09/2020 0:35	84-12-SC-AB	timeout	Timeout		
9	02/09/2020 12:08	84-12-SC-AB	fault	Fault in panel charger fault		Panel: 1
10	02/09/2020 10:13	84-12-SC-AB	reset			
11	02/09/2020 10:13	84-12-SC-AB	fault	Fault in panel battery fault		Panel: 1
12	02/09/2020 10:12	84-12-SC-AB	reset			
13	02/09/2020 9:51	84-12-SC-AB	timeout	Timeout		
14	31/08/2020 16:08	84-12-SC-AB	fault	Fault in panel charger fault		Panel: 1
15	31/08/2020 11:10	84-12-SC-AB	fault	Fault in loop 4 event COMM FAULT		Panel: 1
16	31/08/2020 11:10	84-12-SC-AB	fault	Fault in loop 3 event COMM FAULT		Panel: 1
17	31/08/2020 11:10	84-12-SC-AB	fault	Fault in loop 2 event COMM FAULT		Panel: 1
18	31/08/2020 11:10	84-12-SC-AB	fault	Fault in loop 1 event COMM FAULT		Panel: 1
19	31/08/2020 11:09	84-12-SC-AB	reset			

