

ANNEX 4

DATA PROTECTION MODULE

- Introduction
- User Manual



INTRODUCTION

In order to facilitate compliance with General Data Protection Regulation (EU) 2016/679 and its implementing law, the IBV has implemented the *Data Protection Module* in Ergo/IBV, where an administrator can control the users who will use the application.

This access control system can be configured by the administrator in the most appropriate manner.

It allows to implement in Ergo/IBV an authentication mechanism with username and password, which identifies in an unequivocal and personalized way the user who is accessing the application.

The system keeps a record of the accesses to the application and the patient's data.

The period of validity of the passwords can be set, after which they expire and users are urged to change.

The use of the applications generates files of information about patients. The applications help users comply with the law by controlling user access. Managing patient's saved files is the responsibility of the customer, who must take the applicable technical precautions according to that law.

USER MANUAL

This user manual is designed for systems administrator or equivalent technical staff. The protection data module works by default with the database ModuloPD.mdb, which is in the application's directory and which can be renamed and located wherever you want from the configuration file 'ModuloPD.ini', which is in the Config folder of the installation directory.

In order to enter the Data Protection Module, execute the file ModuloPD.exe, which is located in the application directory; a dialog box will immediately open (*Fig. 1*), where you must enter the administrator's username and password. Initially, you can enter with:

Username: ***administrador***

Password: ***admin***

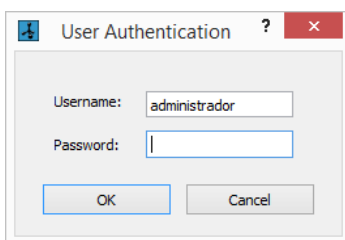


Fig. 1. Administrator's identification

After correctly authenticating, the application main window (Fig. 2) will appear. You must set a new administrator password (see section "Password change" in this chapter).

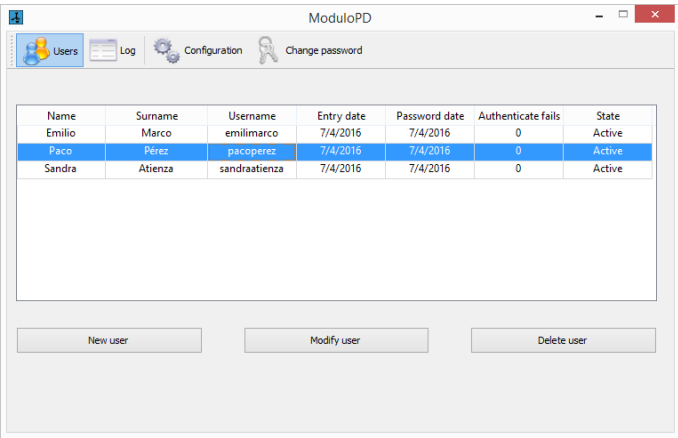


Fig. 2. Main window

At the top of the main window there is a tool bar with the following options:



Users. This option accesses the application user management.



Log. This function visualizes the users log activity.



Configuration. This feature configures the data protection.



Change password. This allows you to change the administrator's password.

How to activate the access control

In order to activate application's access control system, follow these steps:

1. Click the **Configuration** button in the window that will appear when you activate the box '*Enable the application control access*' and click *Ok*.
2. Click the **Users** button, and create all the users that will Access the application with the *New User* button.

From this moment on, only the users that have been created can run the Ergo/IBV application; they will have to use their username and password. In addition, everything they read and write will be recorded in an activity log.

Users Management

The button *Users* opens a table with all the module users (*Fig. 2*) which shows each user's name, surname, user, registration date, password date, authentication failures and status.

There are three buttons at the bottom of the window:

New User. This button allows you to create a new user; it opens a new window to enter the user's information (*Fig. 3*):

Name and surname

User: It must be at least 8 alphanumeric characters long.

Password: It must be at least 6 characters long, 2 of which must be numerical.

Registration Date: It will be the current date by default.

Status: This reflects the status of the user account, the value set as default is New; it can show three values:

New: This status will be showed for as long as the user does not change the password. After you authenticate, you will be given access, but you will also be informed about your status and asked to change your password.

Active: this status means that the user is enabled to use the application. You will be given access after correctly authenticating.

Blocked: in this status, the user is denied access to the application. It can be assigned by the administrator or

automatically when the user exceeds the number of failed authentication retries.

Authenticate Fails: this indicates the number of failed consecutive authentication attempts, which is initially zero. The system will count the failed attempts and restore the value to zero when a positive authentication occurs.

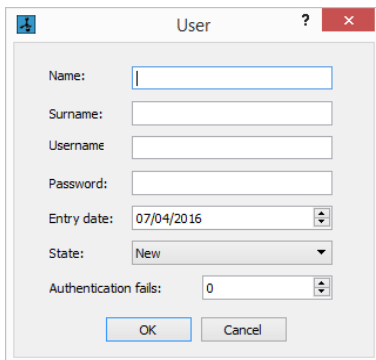
A screenshot of a Windows-style dialog box titled "User". The dialog box has a standard title bar with a question mark icon, a red close button, and a maximize button. Inside the dialog, there are several input fields: "Name:" with a text box containing a cursor; "Surname:" with an empty text box; "Username:" with an empty text box; "Password:" with an empty text box; "Entry date:" with a date picker showing "07/04/2016"; "State:" with a dropdown menu showing "New"; and "Authentication fails:" with a spinner box showing "0". At the bottom of the dialog are two buttons: "OK" and "Cancel".

Fig. 3. User's file

Modify User. This allows you to modify the information of the user you select from the list. A user's file will open with the editable data.

Delete User. This allows you to delete the selected user. You will be asked to confirm the action first.

Activity Log

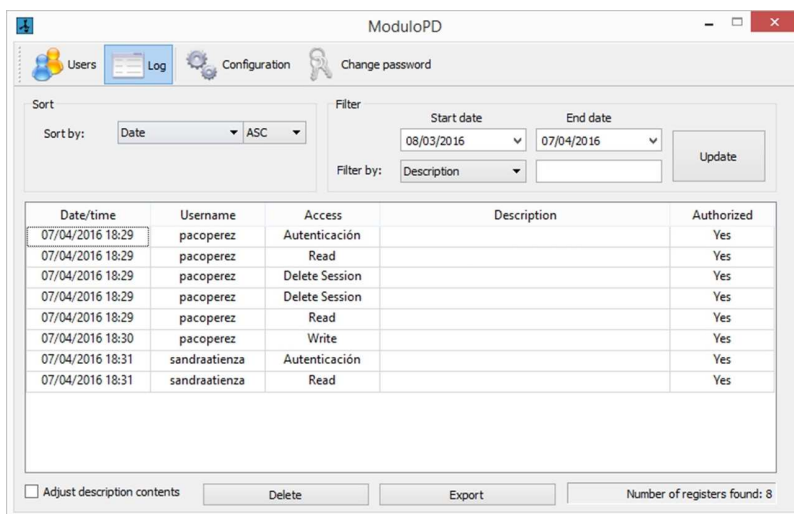
As pointed out above, if the *Application Access Control* is enabled, the IBV application will record the activities performed by the user (see section *Configura* in this chapter).

To do this, Ergo/IBV records in a database file the accesses to the application and the reading and writing actions on workers' data.

When a user attempts to authenticate, Ergo/IBV creates a log indicating an access authentication, the user who performs it, the date and time it takes place, and whether the access was authorized or denied.

When the user opens or saves jobs, Ergo/IBV generates a data access log indicating: the user, the date and time when the access is performed, the file accessed, type of access (read, write, delete, creation, import or export) and whether it has been authorized or denied.

If you press the **Log** button on the toolbar, a table with all the activity logs generated by the use of the application will be displayed (*Fig. 4*).



Date/time	Username	Access	Description	Authorized
07/04/2016 18:29	pacoperez	Autenticación		Yes
07/04/2016 18:29	pacoperez	Read		Yes
07/04/2016 18:29	pacoperez	Delete Session		Yes
07/04/2016 18:29	pacoperez	Delete Session		Yes
07/04/2016 18:29	pacoperez	Read		Yes
07/04/2016 18:30	pacoperez	Write		Yes
07/04/2016 18:31	sandraatienza	Autenticación		Yes
07/04/2016 18:31	sandraatienza	Read		Yes

Fig. 4. Activity log

That table allows you to perform the following actions on the activity logs:

Sort. Select the sorting field (user, date, action, etc.) in the first drop-down menu, and the ascending or descending order (ASC o DESC) in the second dropdown.

Filter. When you change the filter options, you must click the *Update* button in order to update the log list. The logs can be filtered as follows:

By date: logs between the *Start date* and the *End date*.

By other field: in the drop-down menu, select '*Filter by*' the field by which you want to filter:

If you select *User*, *Access* or *Authorized*, the possible values for that field will load in a second dropdown, so that you will only have to select the desired filter value.

If you select *description*, you can enter free text and the actions containing such text will be filtered.

Delete. This option deletes the listed logs, that is, those that meet the filter criteria.

For example, if you want to delete all the unauthorized logs of a given period, select the start and end date of the desired period, and select the *Authorized* field in the filter dropdown, and the *Number* option in the second dropdown. When you click the *Update* button, the logs that meet those criteria will be shown so that you can delete them.

When you click the delete button, a confirmation message is displayed; if the answer is positive, a message will advise the administrator to export the logs to a file before deleting them.

Export. This allows you to export the listed logs, that is, those that meet the filtering criteria, to a file with structured CSV format.

Configuration

In order to configure the data protection module, click the *Configuration* button on the main screen, which will show a window for configuring the parameters of this access control (*Fig. 5*).

The check box enables or disables the activity of the data protection module. If you enable the control, the IBV application will ask for authentication when it starts to run, and will also record the activity of the users. If you disable the control, the application will perform neither of these things. After installing the IBV application, this control is disabled until the administrator enables it.

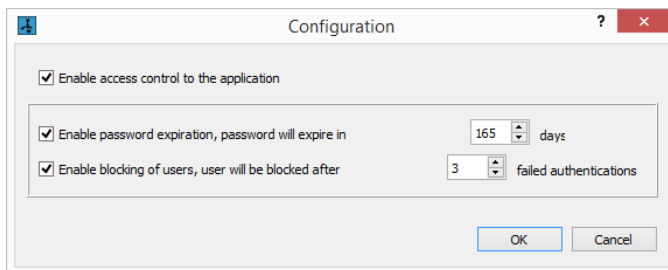


Fig. 5. Configuration window

The check box *Enable password expiration*, enables or disables the function that makes passwords automatically expire after a set period of time. If enabled, you can establish the number of days during which a password is valid. When a password expires, the user can access the application, but it will remind you to change the password.

The check box *Enable blocking of users*, enables or disables the function that automatically changes users to the blocked status if they reach the maximum number of failed authentications. If enabled, it is possible to set the maximum number of attempts allowed. When users are blocked, they can no longer access the application until the administrator unblocks them.

Password change

If you press the Change Password button, you can change the administrator password; to do this, enter the current password followed by the new one and its confirmation (*Fig. 6*).

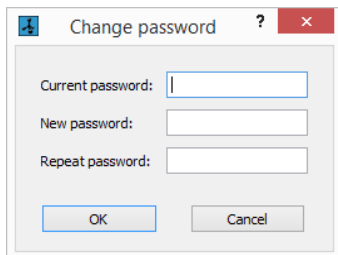
A screenshot of a 'Change password' dialog box. The dialog has a title bar with a blue icon, the text 'Change password', a question mark, and a red close button. Inside the dialog, there are three text input fields labeled 'Current password:', 'New password:', and 'Repeat password:'. Below the fields are two buttons: 'OK' and 'Cancel'.

Fig. 6. Password change