
FUSS - User Manual

Release 12.0

FUSS Lab

Jul 14, 2023

1 The desktop	3
1. 1Description	3
1.2The bottom panel	3
1.3The application window	4
2 Main operations on the desktop	5
2. 1 Opening a terminal	5
2. 2Adding a program to the main program panel	5
2. 3Adding plugins to the bottom panel	6
2. 4Adding workspace selector	6
3 View hidden files	9
3. 1Premise	9
3. 2View hidden files	9
4 Language settings	11
4. 1Changing interface language	11
4. 2Layout of the keyboard	13
5 Bluetooth Devices	17
5. 1Permissions to use bluetooth devices	17
5. 2Configuring amplified speakers or Bluetooth headsets	17
5. 3Connecting to the configured device	22
6 Resize many images in one operation	25
6. 1Premise	25
6. 2Modify the file manager (File manager)	25
6. 3Resize multiple images	26
7 The management of login credentials	29
7.1General Objectives	29
7. 2Responsibility of users	29
7.3Technical requirements for password creation and management	30
7. 4Changing password before expiration	30
7. 5Changing password after expiration	32
8 Problems and solutions	37
8.1Browser access problem	37
8.2Panel display problem on the desktop	37
9 Veyon - User Manual	39
9. 1Introduction	39

9.1.	1 Program startup and access	39
	9.1.2 User interface	41
	9.1.3 State bar	42
	9.1.4 Toolbar	42
	9.1.5 Computer selection panel	42
	9.1.6 Screen panel	43
9.	2 Functionality of the program	45
9.2.	1 Use of functions on individual computers	45
	9.2. 2 Mode of monitoring	46
	9.2.3 Demonstration mode	46
	9.2.4 Blocking screens	47
	9.2.5 Remote access	48
9.2.	6 Restarting and shutting down computers	49
	9.2. 7 Log in user	50
	9.2. 8 Log off users	50
	9.2. 9 Send a text message	51
	9.2.10 Open a program	52
	9.2.11 Linking to a website	53
	9.2.12 File transfer	54
	9.2.13 Screenshots	56
10	Cryptomator - User Manual	57
	10.1 Foreword	57
	10.2 Starting and accessing the program	58
	10.3 Adding safes	60
	10.3.1 Create a new safe	60
	10.3.2 Opening an existing safe	62
	10.4 Access to Safes	62
	10.4.1 Unlocking a safe	62
	10.4.2 Working with the unlocked safe	63
	10.4.3 Locking a safe	63
	10.5 Changing the password	63
	10.6 Recovery key	64
	10.6.1 Show the recovery key	64
	10.6.2 Reset password with reset key	65
	10.7 Removing safes	66
11	Contribute	67
12	Support	69
13	Licenses	71
	Index	73

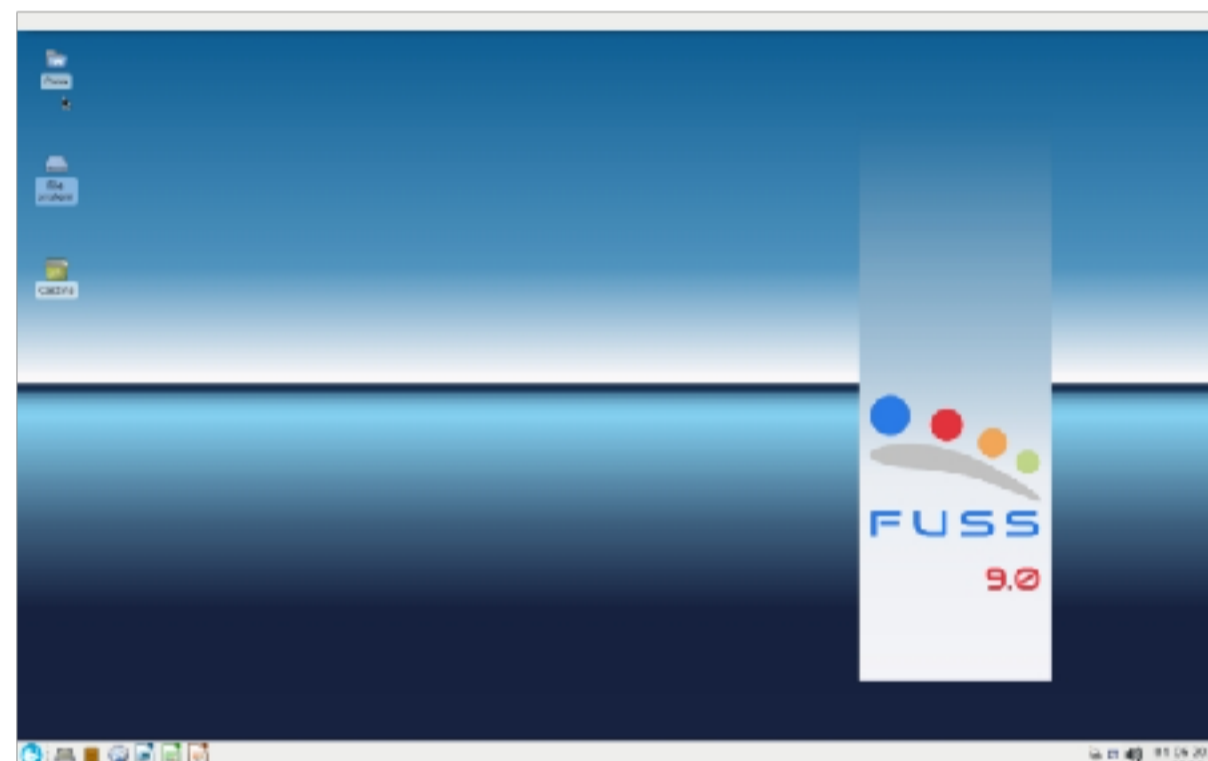
This manual guides the user in using the live/desktop/client version of the **FUSS** GNU/Linux distribution in the current Debian 12 "bookworm" based version 12.



CHAPTER 1

The desktop

At first, the desktop presented to the user is as follows:



1.1 Description

The desktop displays three folders:

- Home, which is the user's home
- File system, which allows navigation and display of PC folders and shared folders
- Recycle bin, for deleting files

1.2 The bottom panel

At the bottom is a panel.

On the left you see what is in the following picture, which we can call the main applications panel:



On the lower right is this panel:

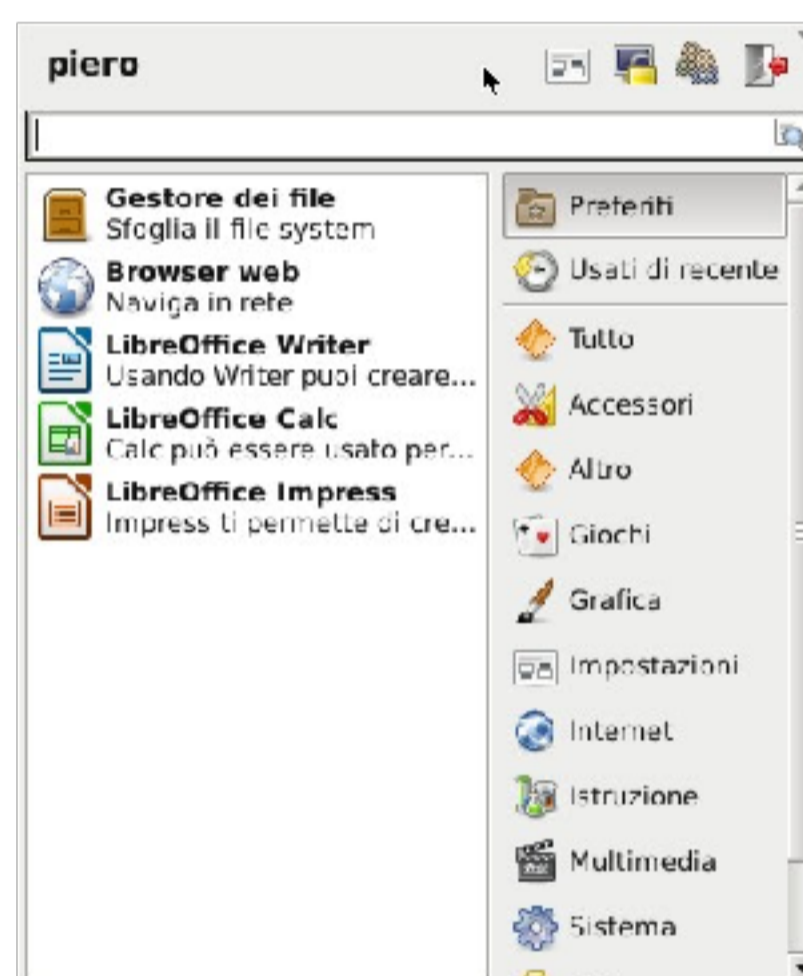
The following icons are found, from right to left:

- date and time
- audio manager: in the image state the audio is muted. To activate it click on the icon with right mouse button and uncheck Mute. Then left-click on the icon, the volume bar appears and drag to adjust the volume itself
- The language selector applied to the keyboard: by clicking you can select between Italian, English and German
- the connection manager



1.3 The application window

Clicking on the all applications icon opens the following window:



The application window is structured like this:

- there is a panel at the top that reads right to left: left to right:
 - the name of the user
 - An icon to manage all settings
 - an icon to lock the screen
 - switching between users
 - the exit from the system
- a search and launch bar for programs
- Two columns of which:
 - The one on the left shows the programs only initially present in the main program panel
 - The one on the right shows all program categories, so it is easy to search for them

Main desktop operations

2.1 Opening a terminal

Right-click in an empty spot on the Desktop: the following context menu opens. Click on *Open a terminal here*.



2.2 Adding of a program to panel of main programs

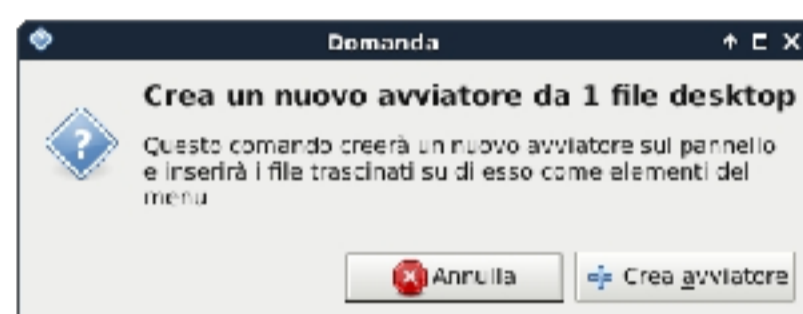
- Open the Applications window
- Select the program from the category menu on the right
- While holding down the CTRL key, drag the program icon on the bottom panel to an empty space. If you are not mistaken, the following window appears:



- Click on the *Create launcher* button : the icon should appear next to those of your favorite programs

2.3 Adding plugins to the bottom panel

Right-click in an empty spot on the bottom panel. The following context menu opens



- Click on Panel item and a submenu opens.
- Click on Add new items: the following window opens:
- Search for the plugin or select it - it will be added to the plugin panel on the right below

2.4 Added workspace selector

- Follow the instructions to add a plugin to the bottom panel
- Select the *Workspace Selector* plugin. The

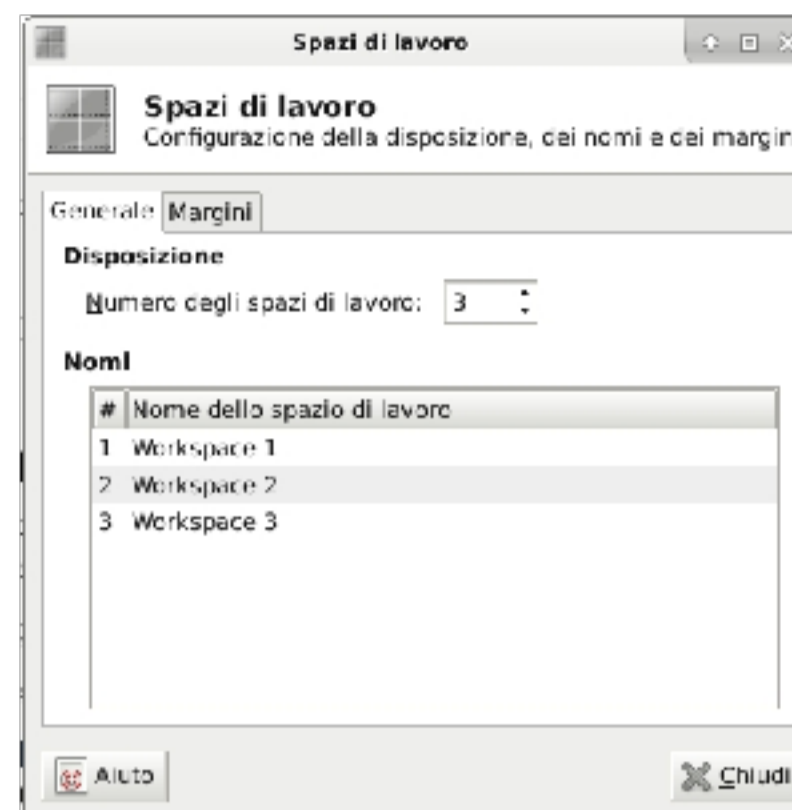
following window opens:



- Right-click on the new item created in the panel. From the context menu that opens, select *Workspace Setup* , as shown in the image below:



- Change the number of spaces you want to use as in the image below:



Having done this, click on the *Close* button

In conclusion, if for example you have chosen three workspaces, in the bottom panel you will find the elements as in the image below:



You can hover over one of them with a mouse click to switch from one workspace to another.

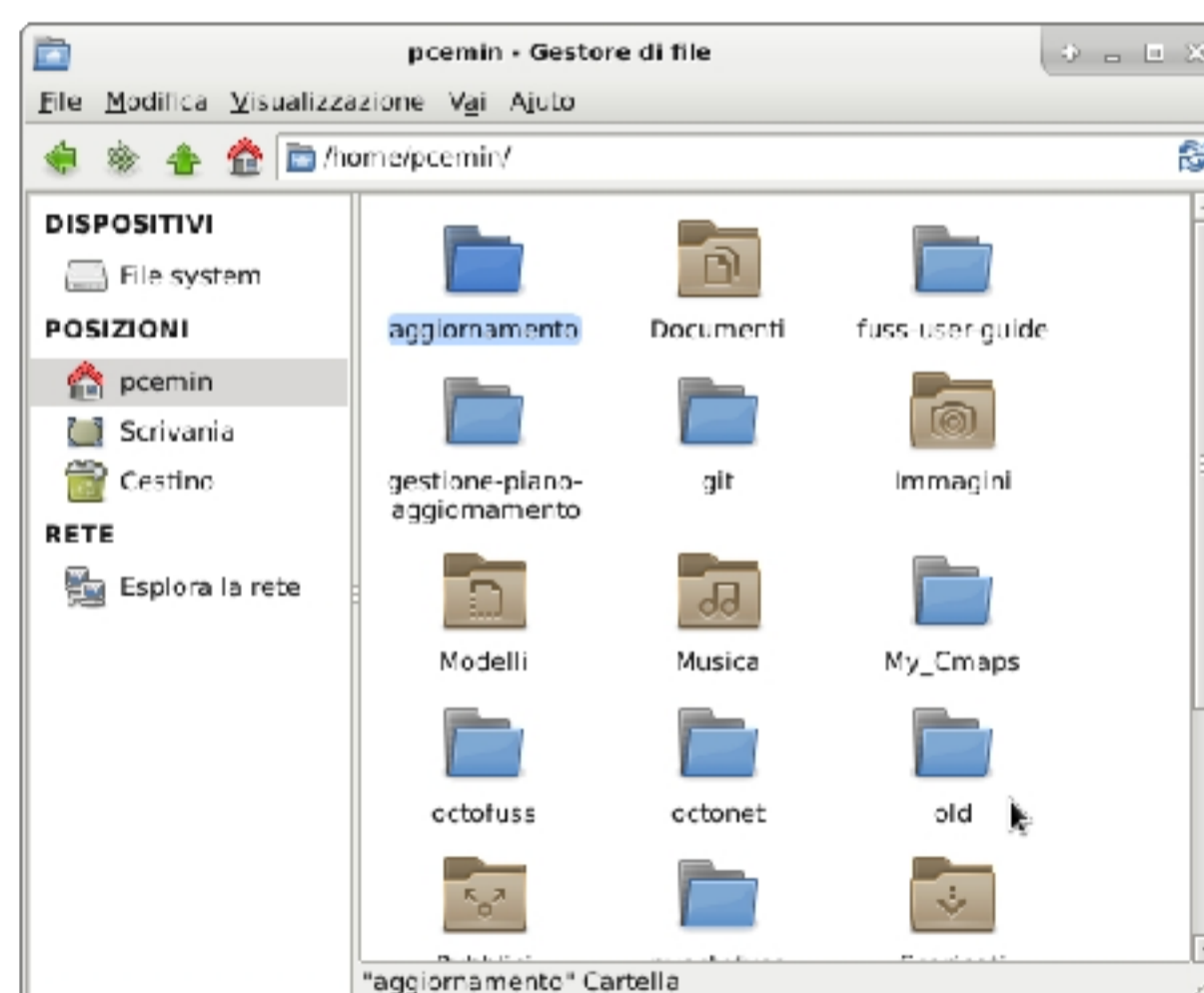
View hidden files

3.1 Foreword

Hidden files have the characteristic that their names begin with a period (.). All user-specific configuration files are stored in hidden files, usually divided by folders. They are all located in the user's home folder.

3.2 View hidden files

- Enter your home (from Desktop double click on Home)
- The following window opens:



- In the top menu bar, select View. Put a flag (or click) on the *Show hidden files* item.

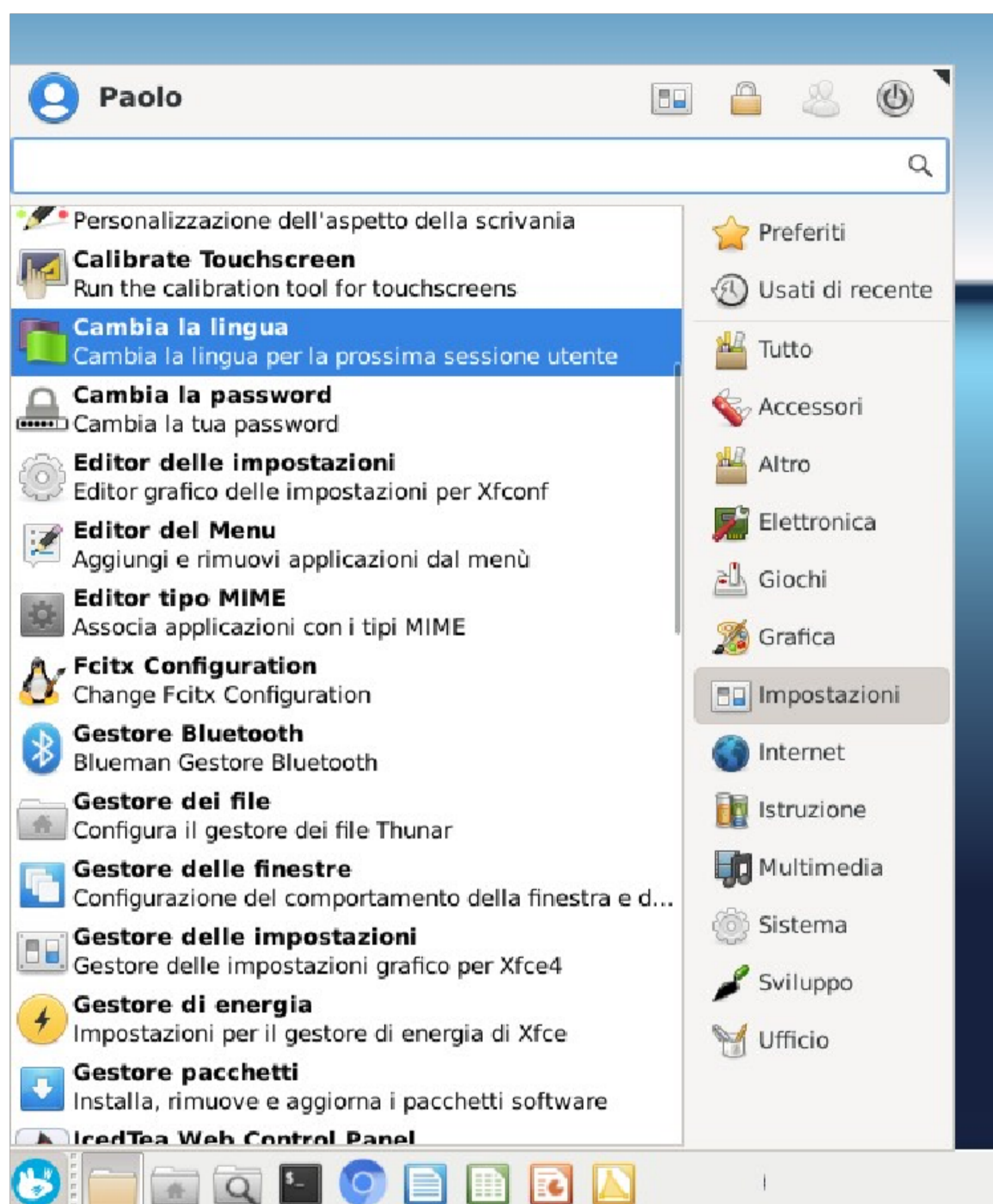


- Now the folder will show many more files and subfolders that were not visible before

Language settings

4.1 Changing interface language

After authenticating yourself, you can change the system language by choosing from those available. You must start from the menu the *Set language for Next Session* program found in the *Settings* category.



A simple settings window will open: simply select the desired language and then press the *Set locale* button.



Finally, it is necessary to exit the interface and re-enter to make the changes effective and to be able to work with the desired language.

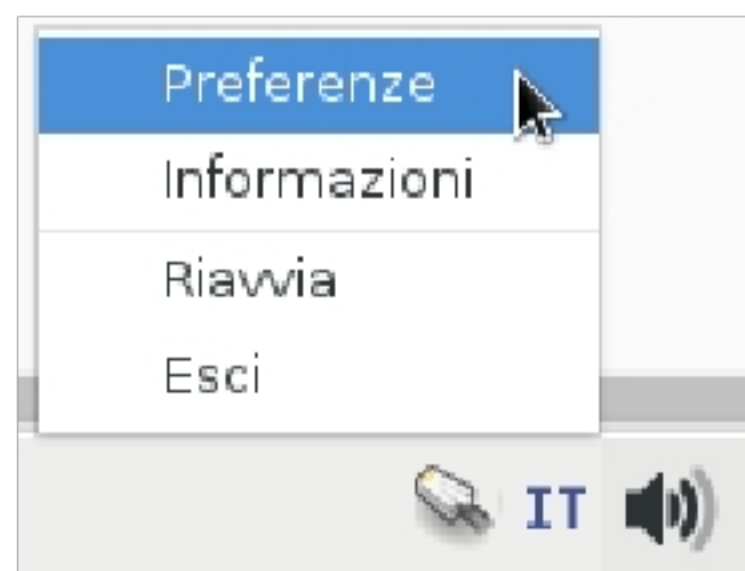


4.2 Keyboard layout

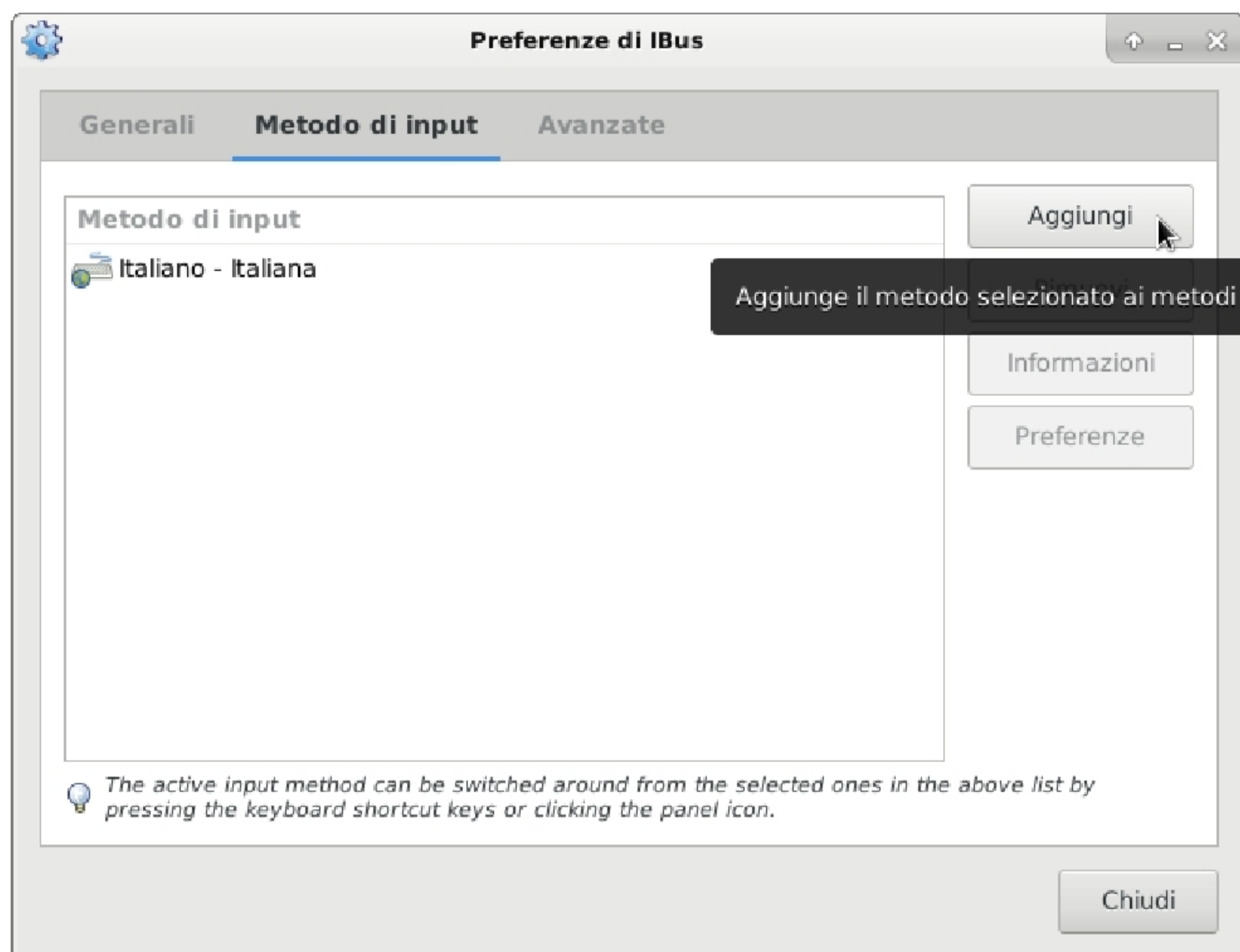
The default keyboard in FUSS is Italian, and the *IT* indicator is in the notification area in the lower right panel.



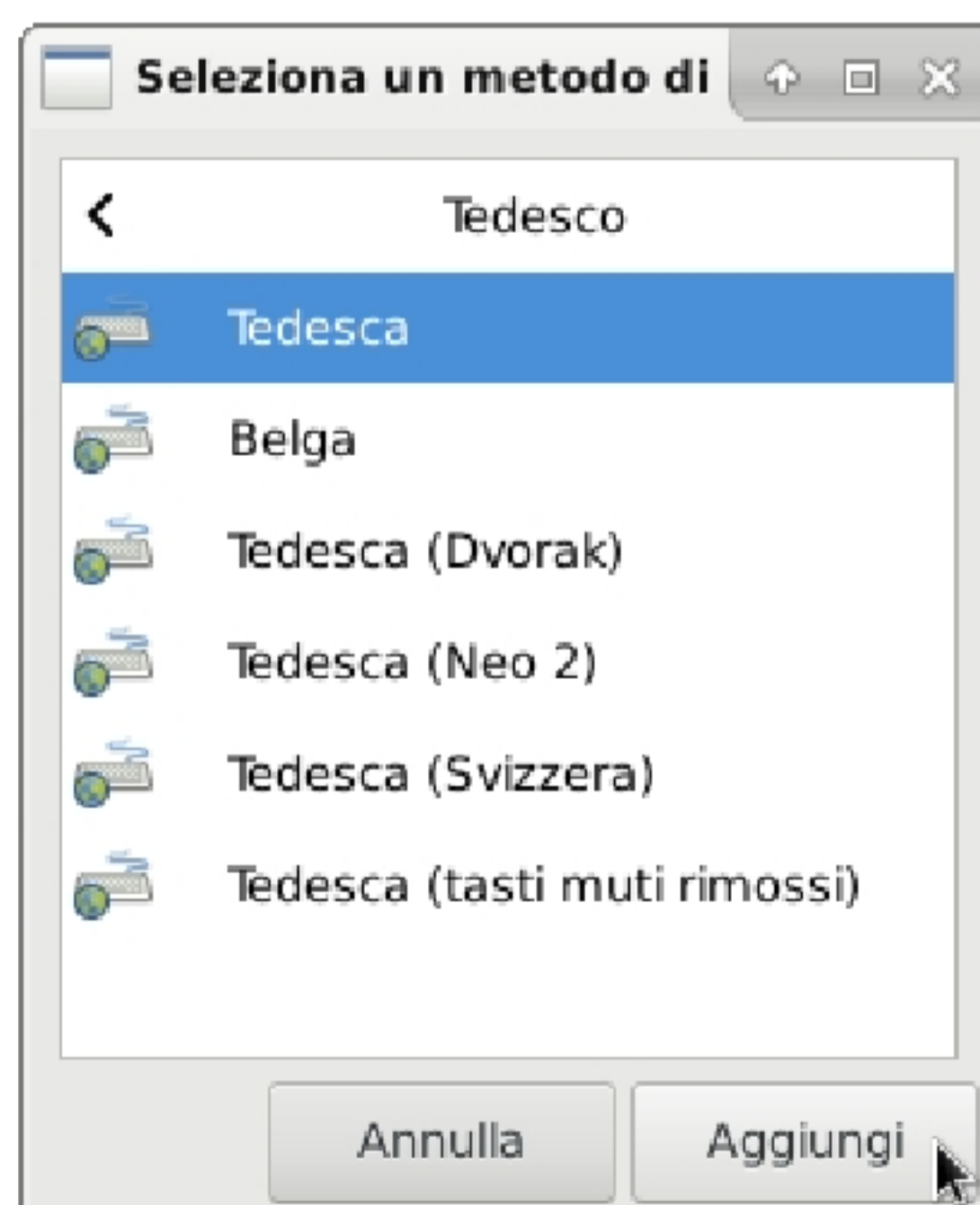
You can add more keyboards by right-clicking and selecting *Preferences*.

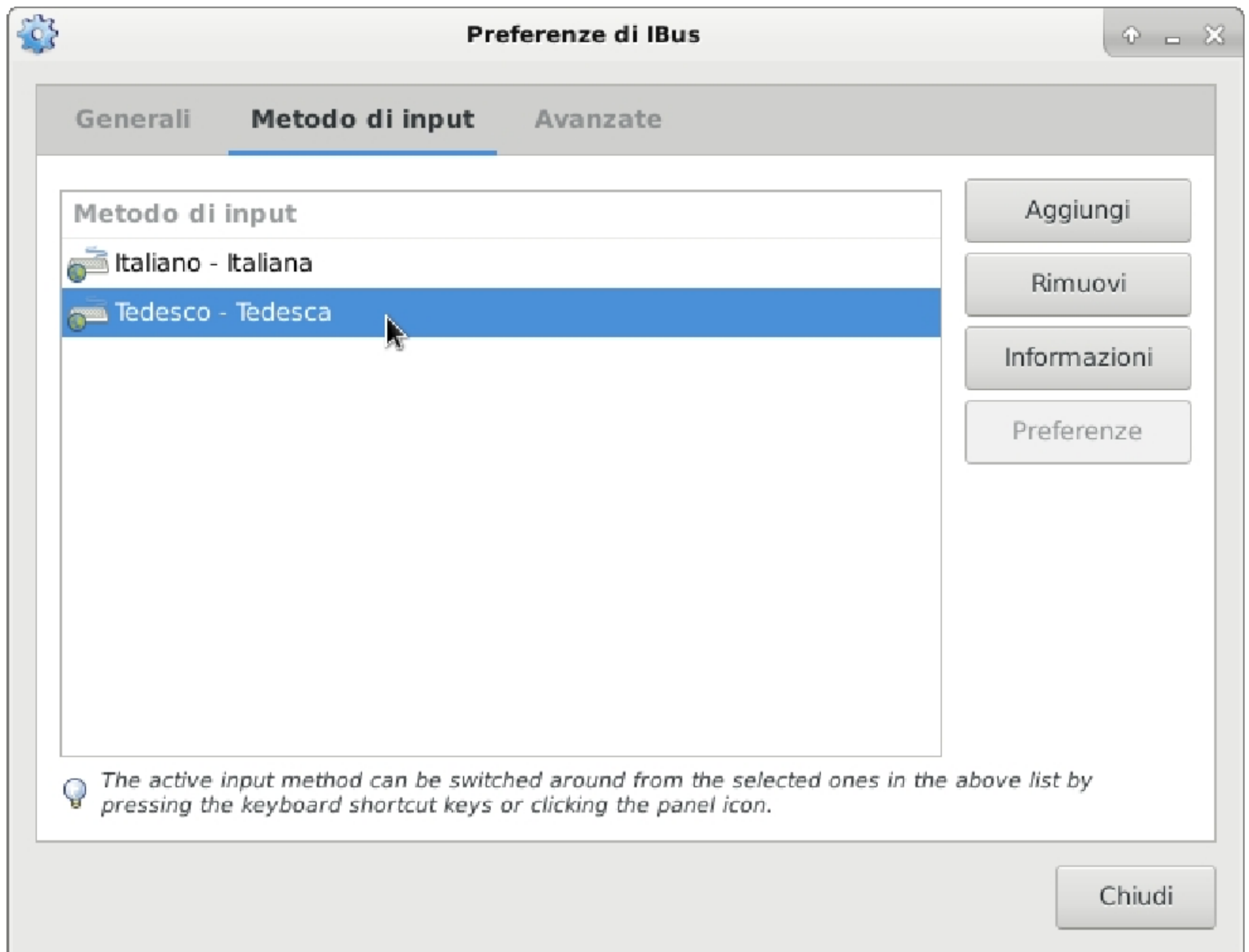


This opens the Preferences window in which the *Input Method* tab should be chosen.



With the *Add* button you can select other virtual keyboards besides the preset one. In the example we add the German keyboard that will be inserted below the Italian one.





Similarly with the *Remove* you can remove a selected keyboard.

In the notification area, by left-clicking on the keyboard indicator, you can now select the German keyboard.



After selection, the indicator will show *DE*.



Bluetooth Devices

This section discusses the configuration and use of external bluetooth peripherals (e.g., amplified speakers, bluetooth headsets, etc.) with FUSS PCs equipped with a bluetooth device.

5.1 Permissions to use bluetooth devices

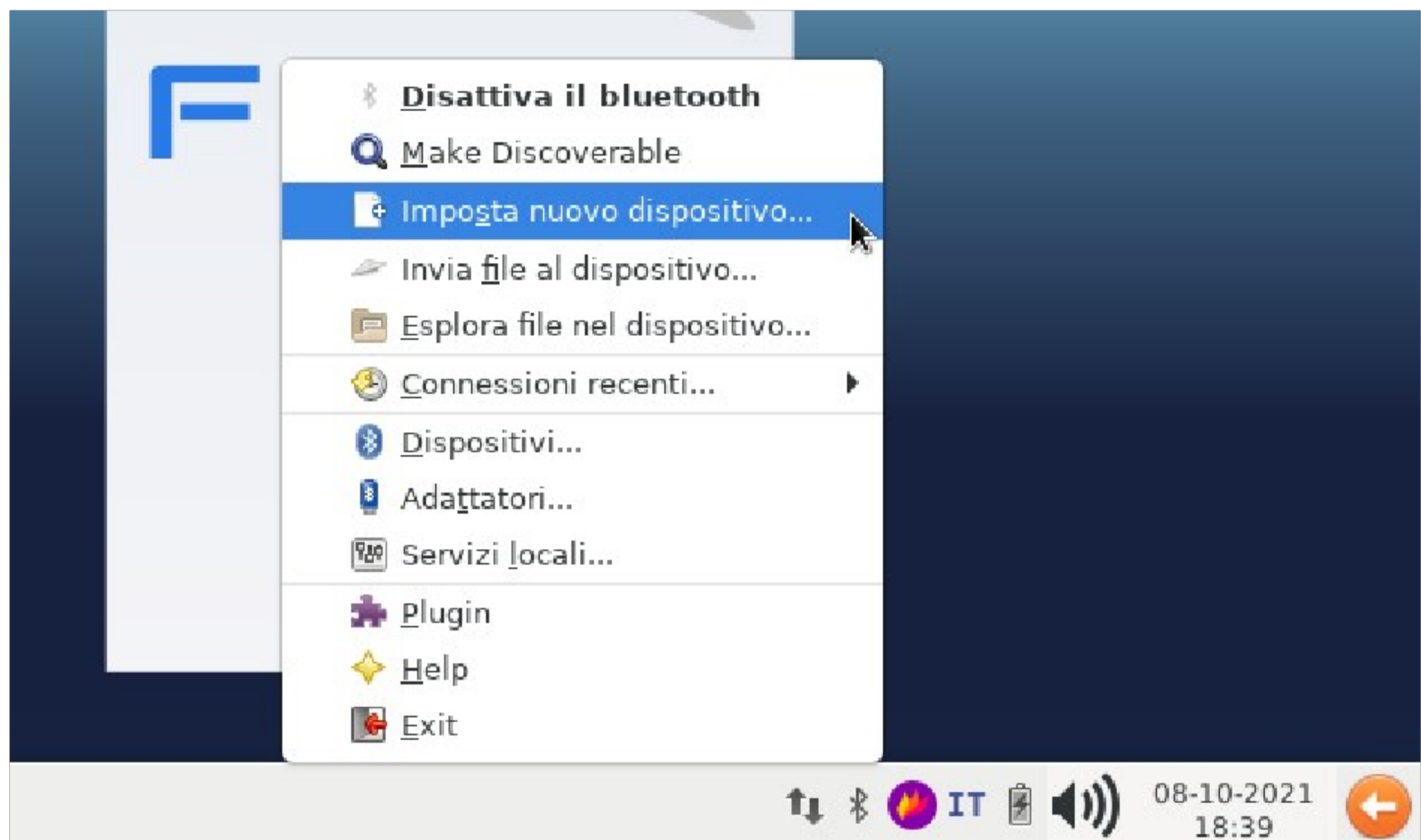
The prerequisite for a user to use a bluetooth device is that he or she has the two permissions `bluetooth` and `netdev` and the `blueman` package is installed on the machine. If you are not an administrator on the machine, contact the system administrator to associate the intended users with the two aforementioned groups (server side if the PC is a client within the school network) and to have the package installed.

5.2 Configuration of amplified speakers or bluetooth headsets

If the listed prerequisites are met, after login in the notification area in the lower right corner you will find the icon of the `blueman-applet`



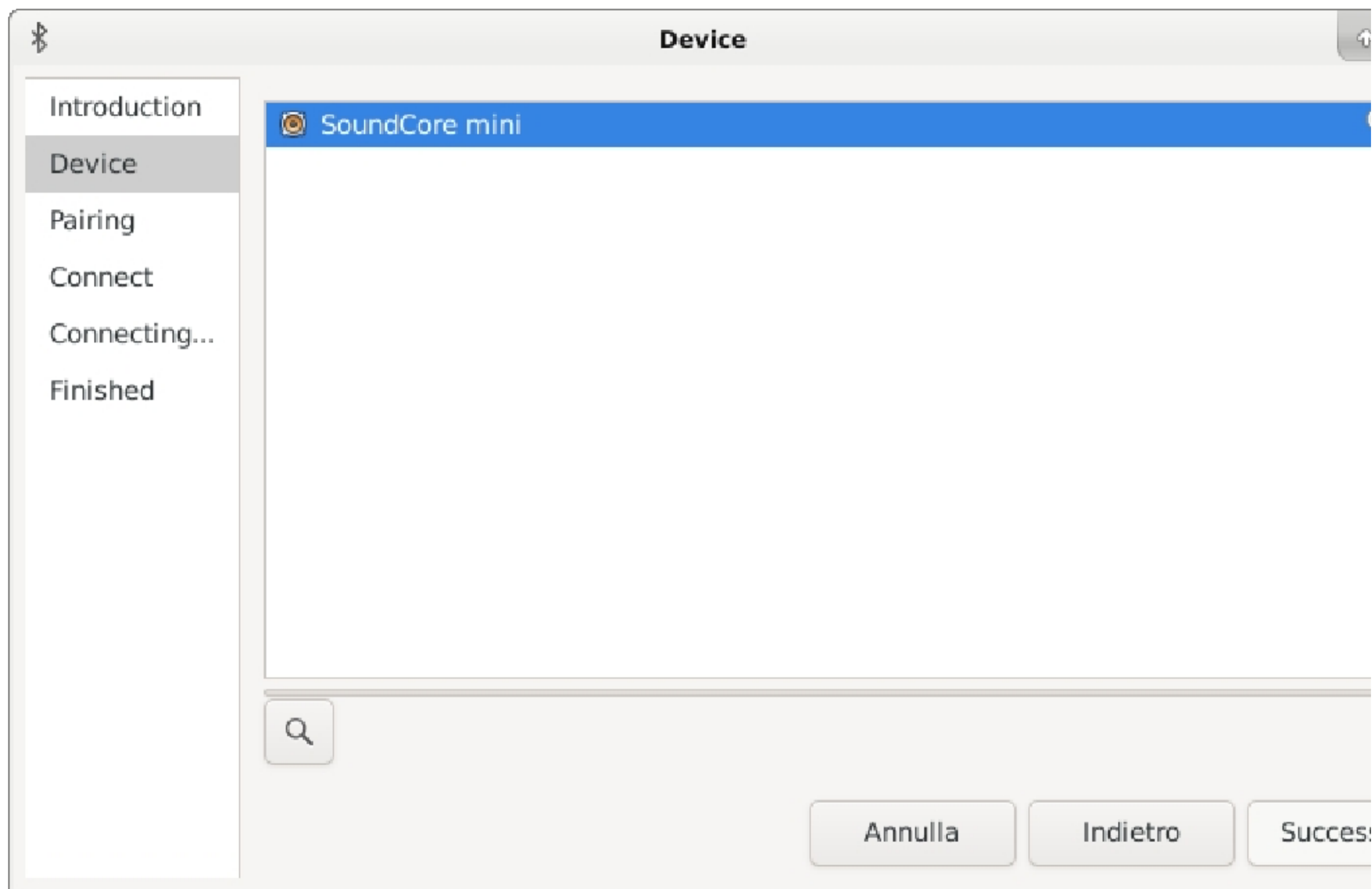
Verify that the device is turned on and ready to connect. Click on the `blueman-applet` icon. A menu opens. Choose the item *Set up new device . . .*



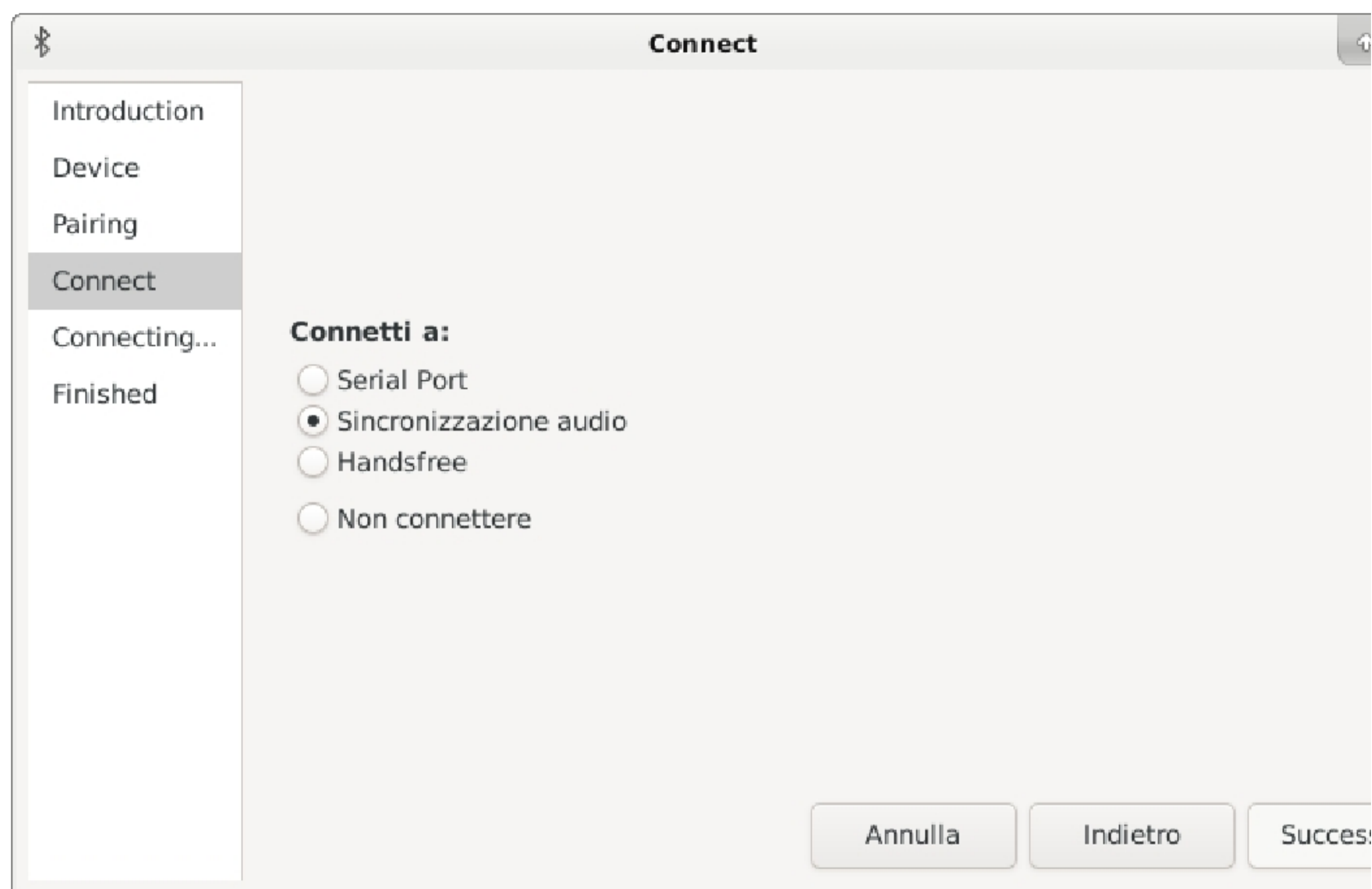
The bluetooth device installation wizard will start; click *Next*;



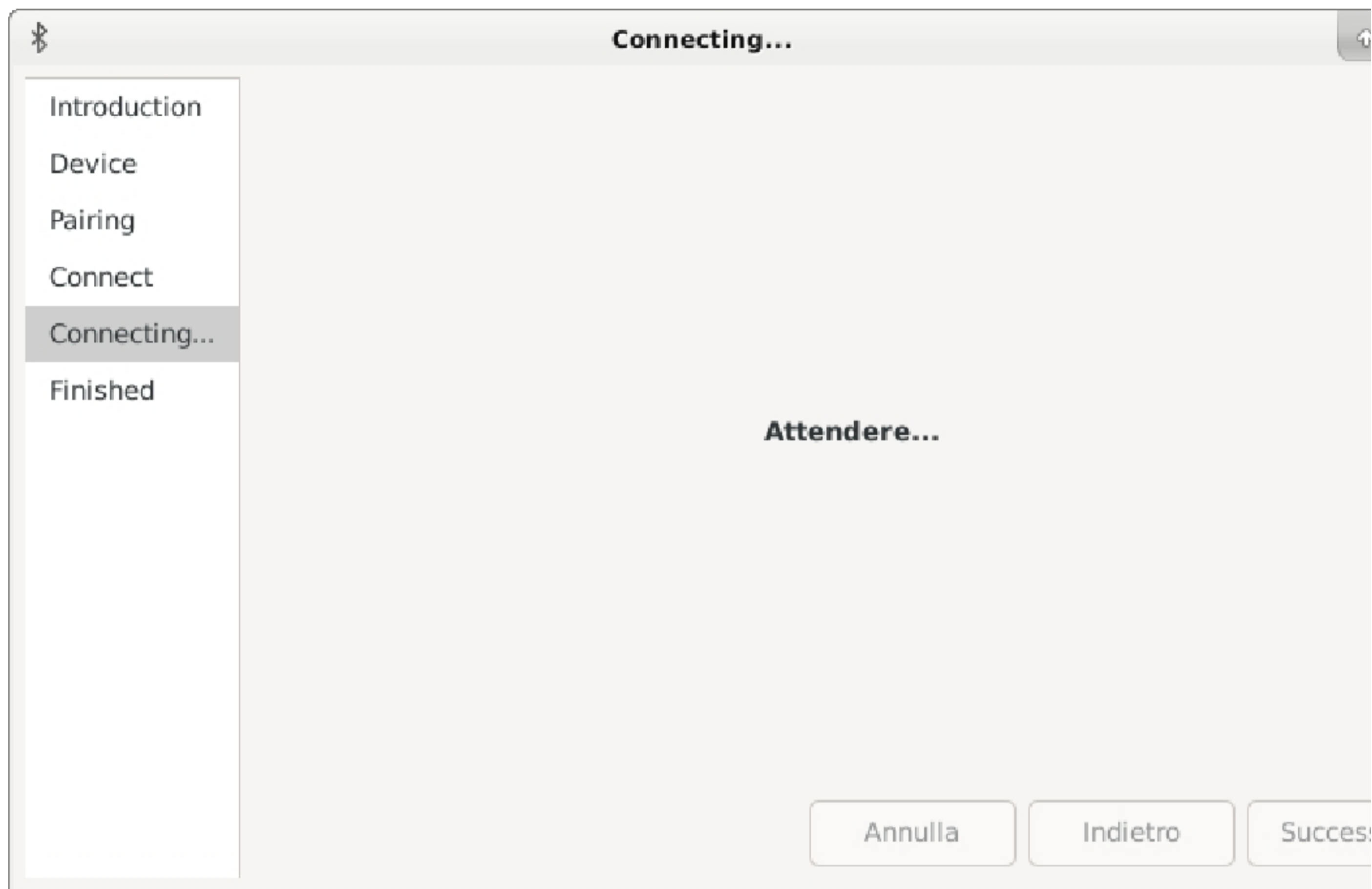
The available devices will be listed; select the one you want to connect to by pressing *Next*.



In the *Connect* menu, choose *Audio Synchronization* mode followed by *Next*



A pairing attempt will be made to the device.

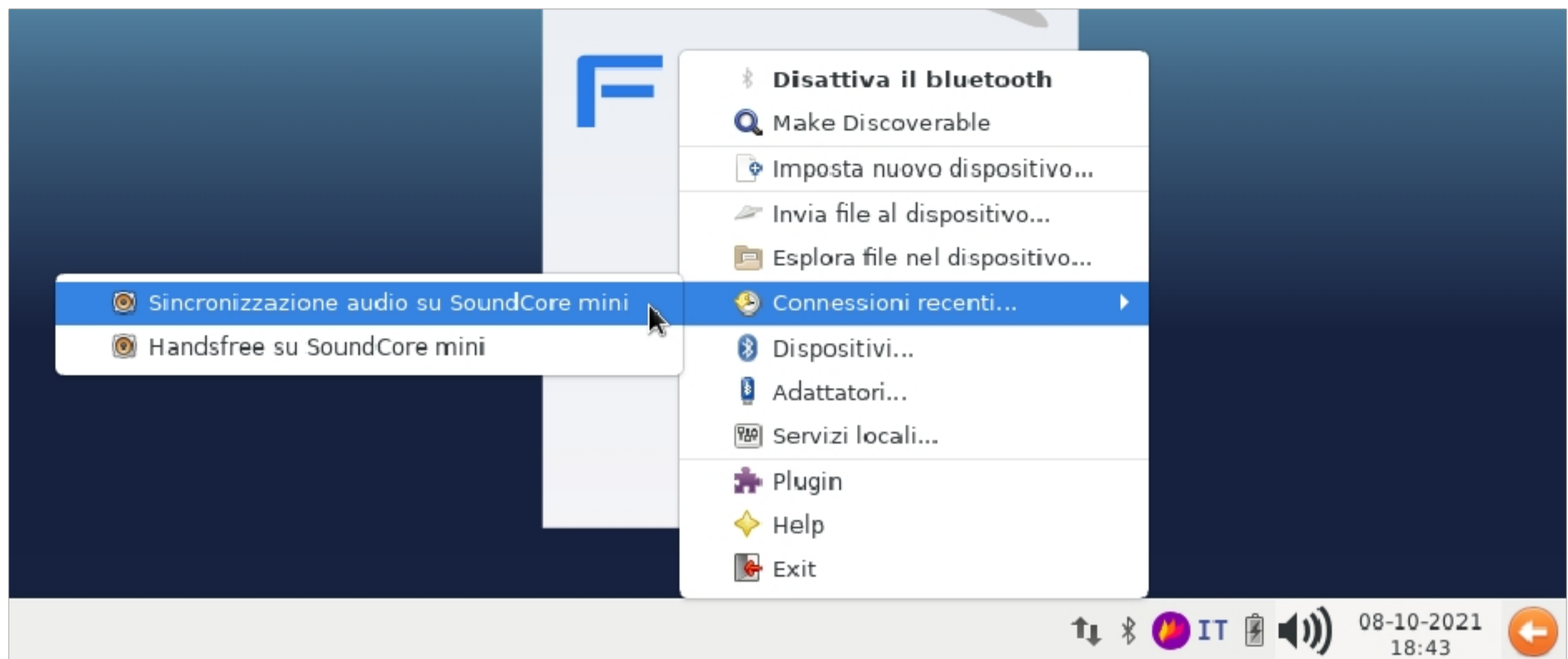


If the association ends positively, the configuration is finished and you can press the *Close* button.

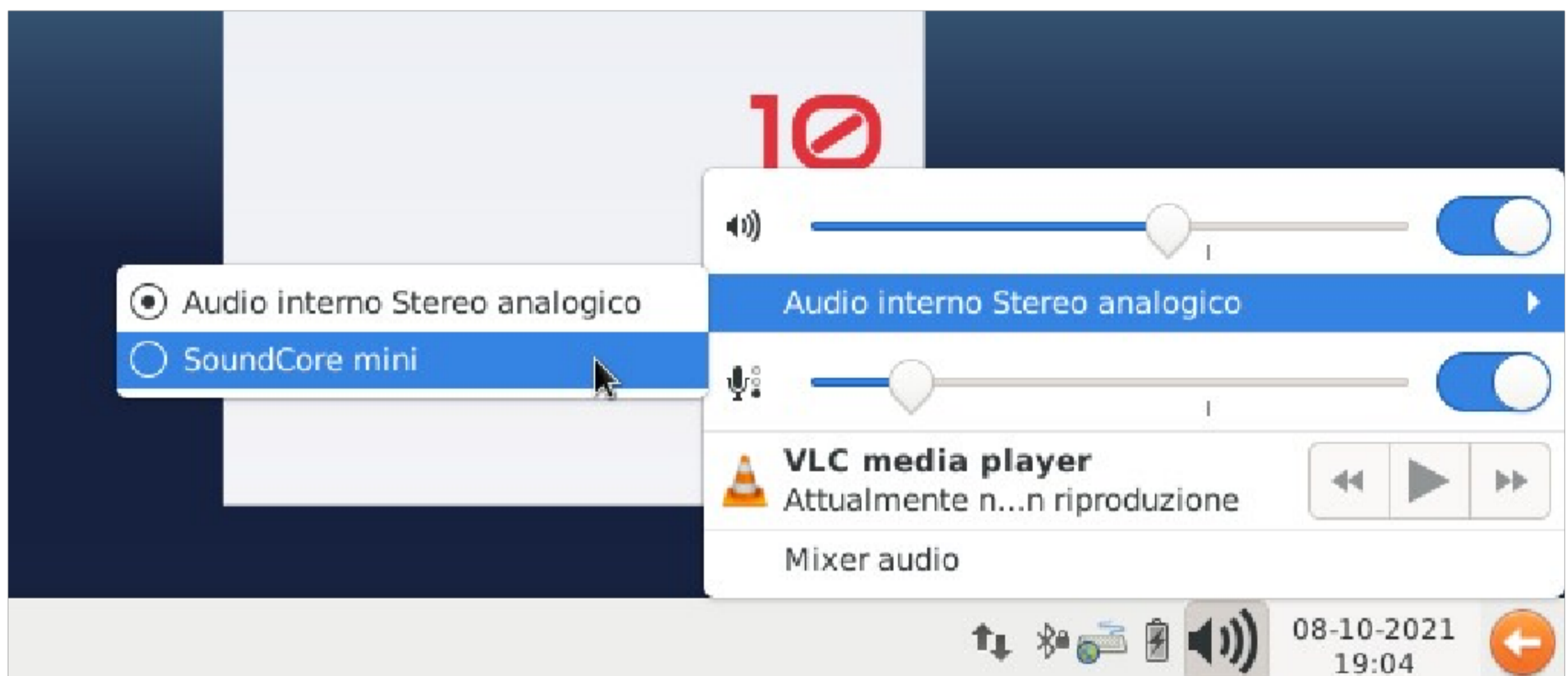


5.3 Connection to the configured device

Whenever you want to connect to the device, simply select the *Recent Connections* item in the `blueman-applet` menu... choosing the device and waiting for the confirmation of successful connection.



In the audio mixer at the bottom right, it will only remain to choose the bluetooth device for audio output (and if necessary, in the case of bluetooth headsets, also for the microphone).



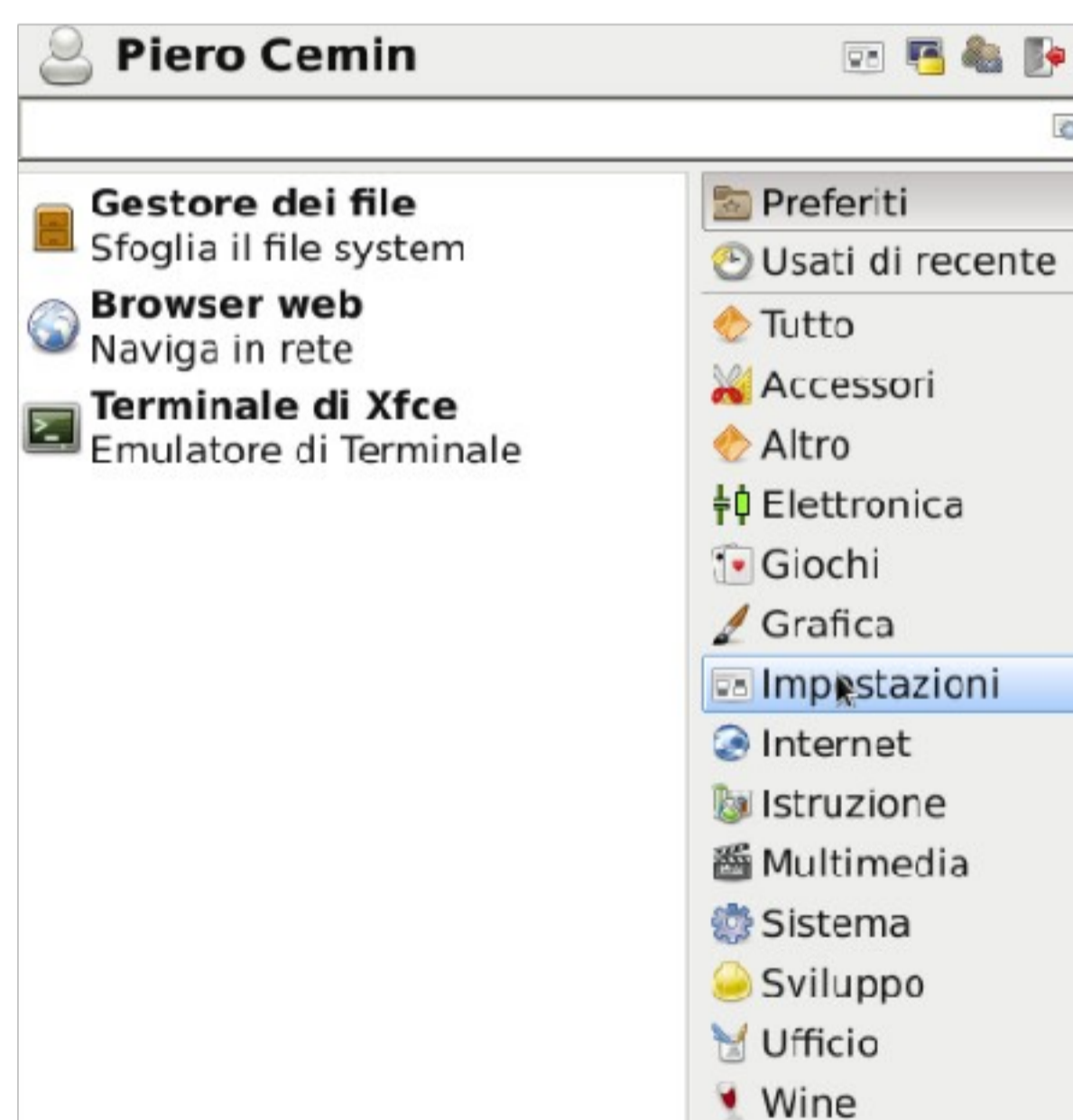
Resize many images in one operation

6.1 Foreword

The file manager used by default (Thunar) does not allow multiple images to be resized in one operation. If there is a need to do this operation, the fastest solution is to change the file manager used by the system. There is another file manager installed in the distribution, whose name is Nautilus, which instead allows this operation to be done easily. The choice to modify the file manager is up to the user. In this chapter we explain how to do this.

6.2 Change the file manager (File manager)

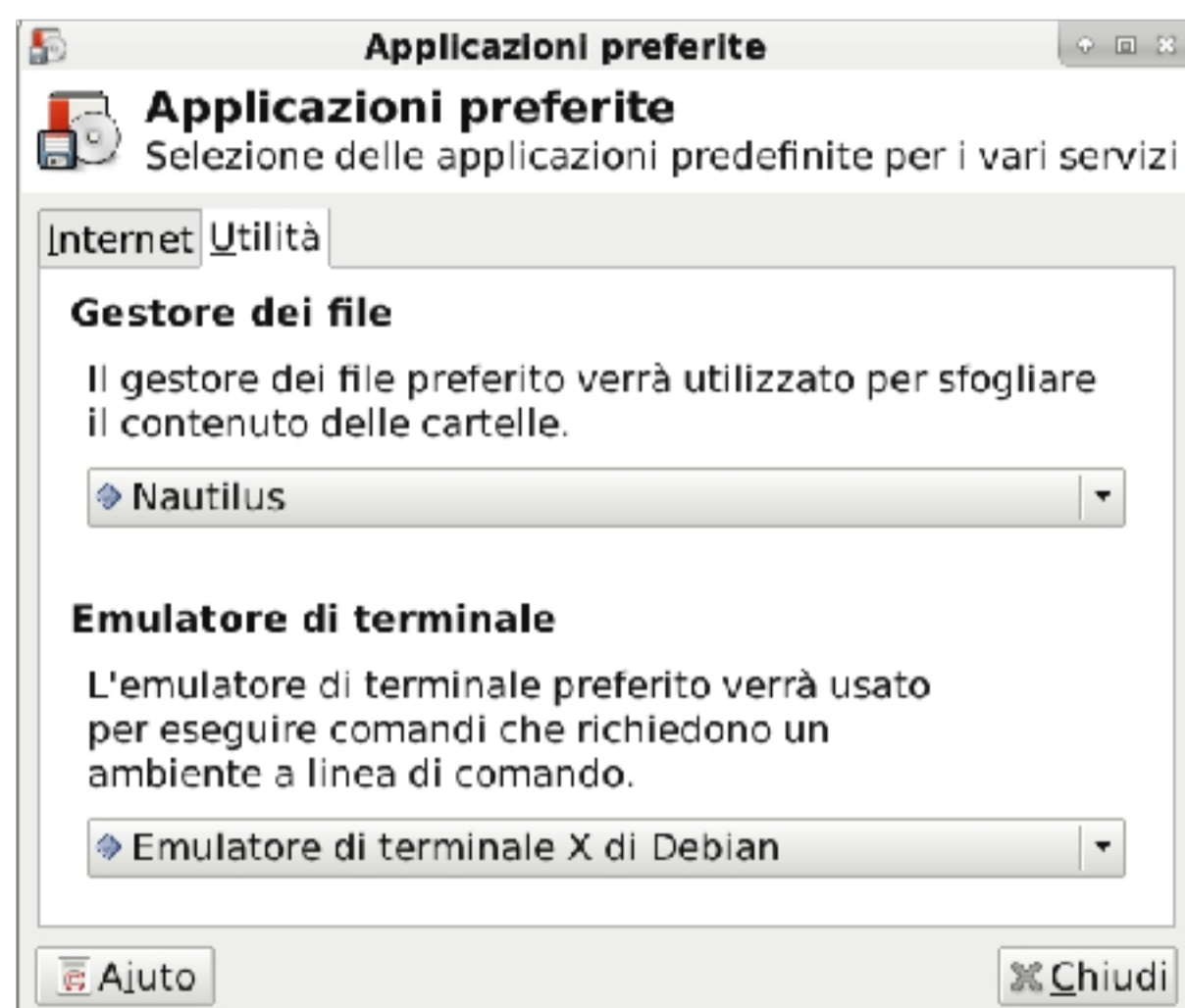
- Click on the Applications icon (Whisker Menu, usually in the lower left corner)
- Opening the Applications menu, select in the list on the right Settings, (as in the figure below):



- In the list that opens on the left, select **Favorite Applications**, as in the image below:



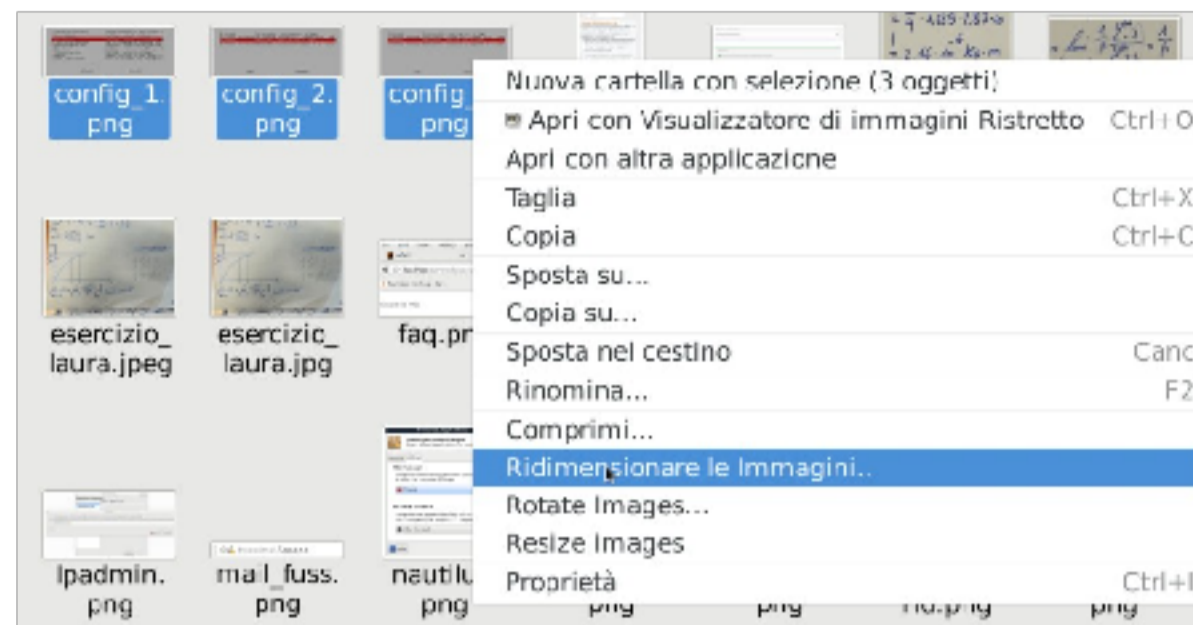
- A new window opens as in the image below, in which you can configure various options. The one we are interested in is found by selecting the **Utilities** tab (at the top of the tab) :



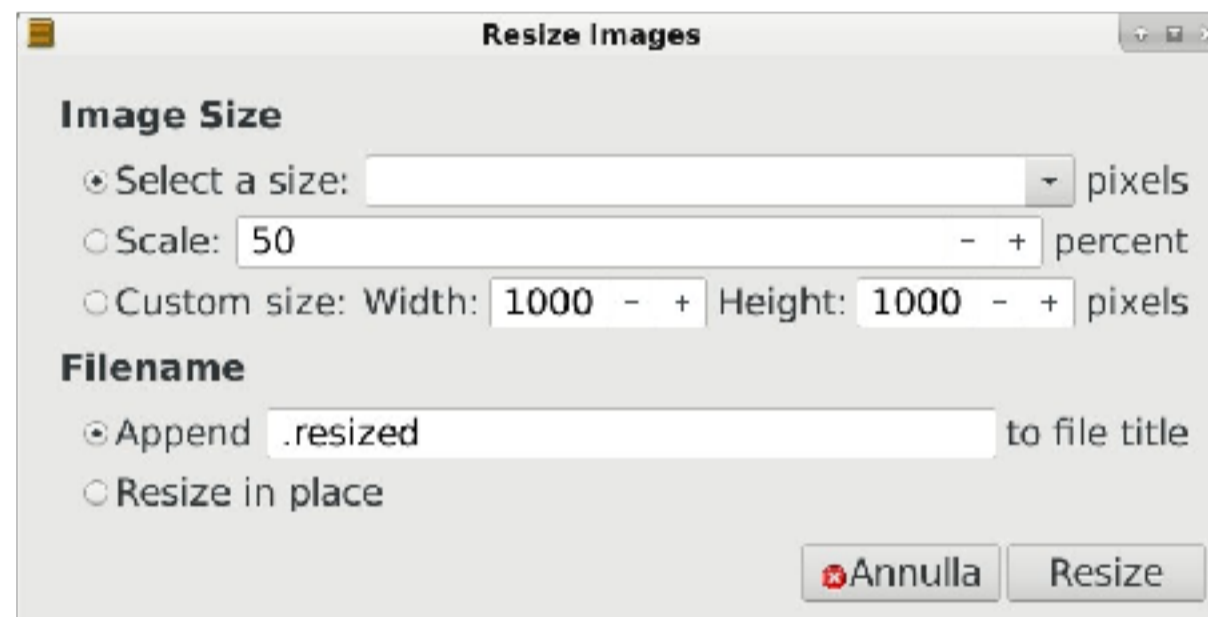
- At this point, by clicking on the **File Manager** drop-down menu, you can select Nautilus instead of the default Thunar.
- By closing any open instances of the File Manager and reopening it, you can perform the immediate operation of resizing multiple images

6.3 Resize multiple images

- Access with the **File Festore** to the folder where there are the images to be edited
- Select all the images you want to resize and **right-click** inside one of the selected ones: a context menu opens as in the figure below:



- Click on `Resize images`: a window opens that contains the operations for resizing:



- Select `Scale` and enter the percentage value by which you want to reduce the image
- Type (or select the present ".resized" one) an extension that is appended to the filenames: you can alternatively select the option `Resize in place`, but this way you lose the original images.
- Clicking on the `Resize` button performs the operation.

The management of login credentials

7.1 General objectives

The protection of access credentials is one of the fundamental principles of information security, particularly the creation and management of passwords, which are the main countermeasure to unauthorized access.

Given the provisions of the current code on the protection of personal data Legislative Decree 196/03 - and, successively, taken up by the new European regulation in force since 24/05/2018, on the protection of natural persons with regard to the processing of personal data - GDPR EU 2016/679, it is necessary to define adequate and appropriate protection measures for the processing and protection of users' personal data.

Access to processors installed with the FUSS operating system provide for a credential-based authentication (and authorization) system as an access tool for users. It consists of a code for user identification ("username" or "password"), associated with a confidential keyword ("password") known only to the user. The two elements, joined together, constitute the access credential ("account" or "user") as defined by current legislation on personal data.

7.2 Responsibility of users

Users agree to comply with the following criteria for creating, storing, and managing access credentials.

Users, once in possession of credentials, must change their passwords when they first log in, respecting the criteria described below, avoiding combinations that are easy to identify. They must choose unique passwords that make sense only to the user who chooses them, avoiding using the same password for other users.

The password is strictly personal and should not be communicated and/or shared with any other person inside or outside the school.

Users should be careful about providing their login credentials, responding to suspicious e - mails and/or clicking on links while browsing the web (or in the email) in order to counter possible computer fraud (such as phishing, spear phishing, identity theft, etc.).

Each user is responsible for all actions and functions performed by his/her account. If there is reasonable certainty that the credentials assigned have been used by a third party, the user should change the password immediately. For the secure storage of login credentials, it is advisable to use a management software

of passwords (e.g., KeePass, LastPass, etc.) by avoiding storing them on sheets of paper, paper documents and files kept within the workstation.

In case the user is locked as a result of password expiration, it is possible to change the password using the procedure described below. In case the password has been forgotten, you should contact the technical support service or the system administrator.

7.3 Technical requirements for password creation and management

As a general rule, the password should be reasonably complex and difficult to identify and/or derive. Within the technical limits allowed by the systems, the password:

1. must be no less than 8 characters in length;
2. must be mandatorily changed when first used and at least every 3 (three) months thereafter;
3. must contain, where possible, at least 3 characters including numbers, upper and lower case alphabetic characters, and special characters (e.g., C@p13nZa);
4. must differ from the previous password by at least three characters;
5. must not present a sequence of identical characters or repeated groups of characters;
6. must not contain references that can be easily traced back to the user or to known areas;
7. must not be based on names of people, dates of birth, animals, objects or words that can be taken from the dictionary (including foreign ones) or that refer to personal information;

Where technically possible, the requirements in (1) to (5) are imposed by automatic mechanisms of the system.

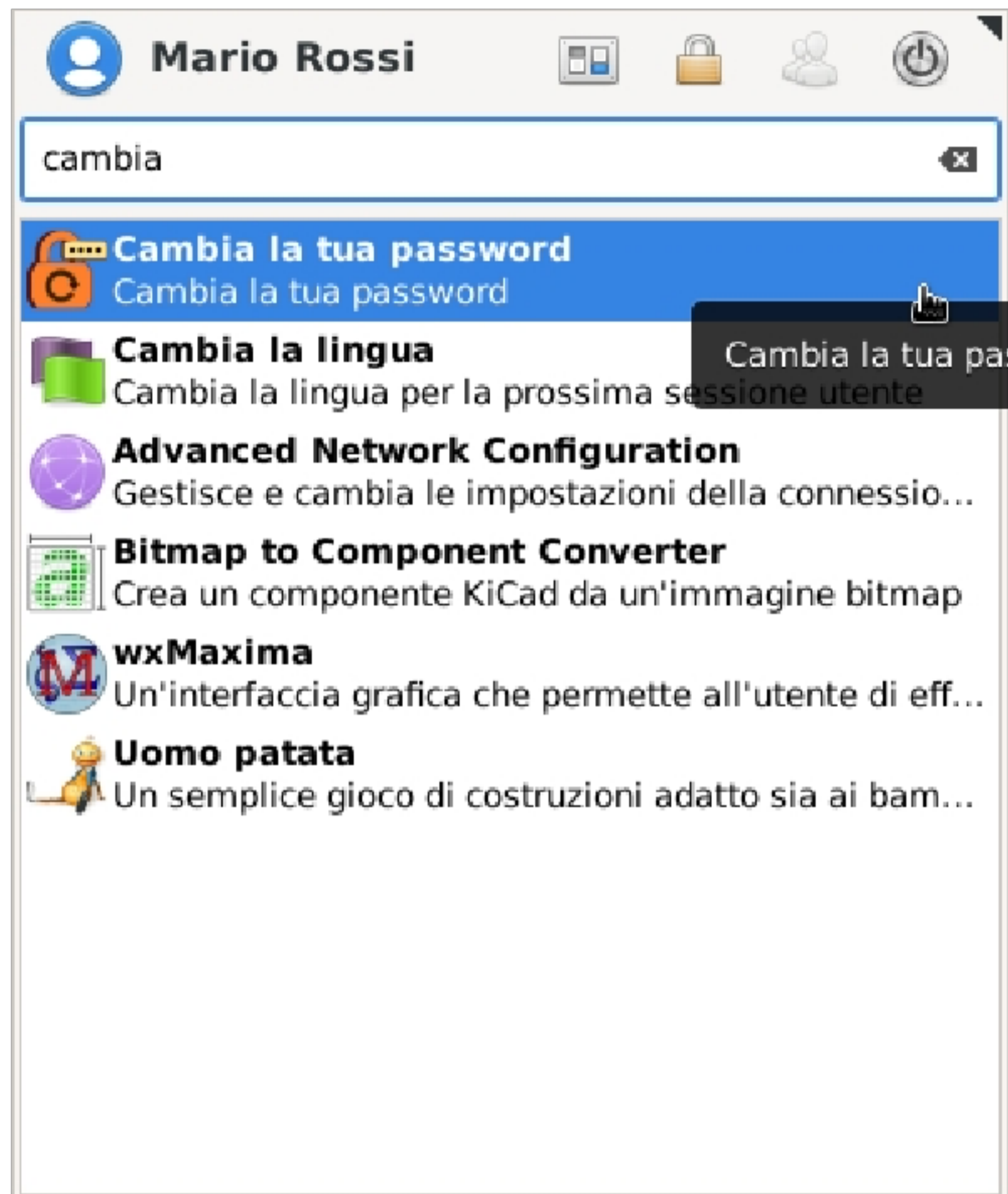
For justified needs for urgent access to information, if the credential holder is prevented from accessing the information, the password may be cancelled and replaced by the system administrators with a new password. In this case, the new password must be given by the system administrator to the user, who must change it at the first access.

7.4 Change password before expiration

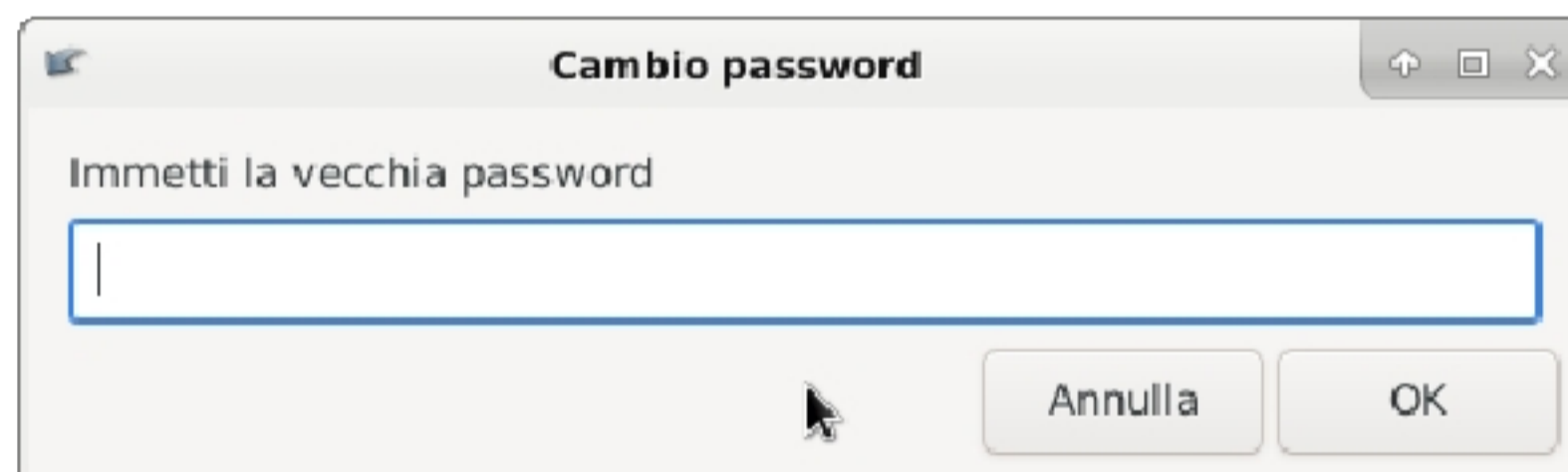
A control system was recently added that alerts the user about 10 days before the password expires (for the *faculty* group it is 90 days) . At this point the user is guided by intuitive messages to change it. If you do not proceed with the password change, the message will be repeated at each login until the natural expiration (which we do not recommend waiting for anyway).

Passwords can be changed at any time as follows:

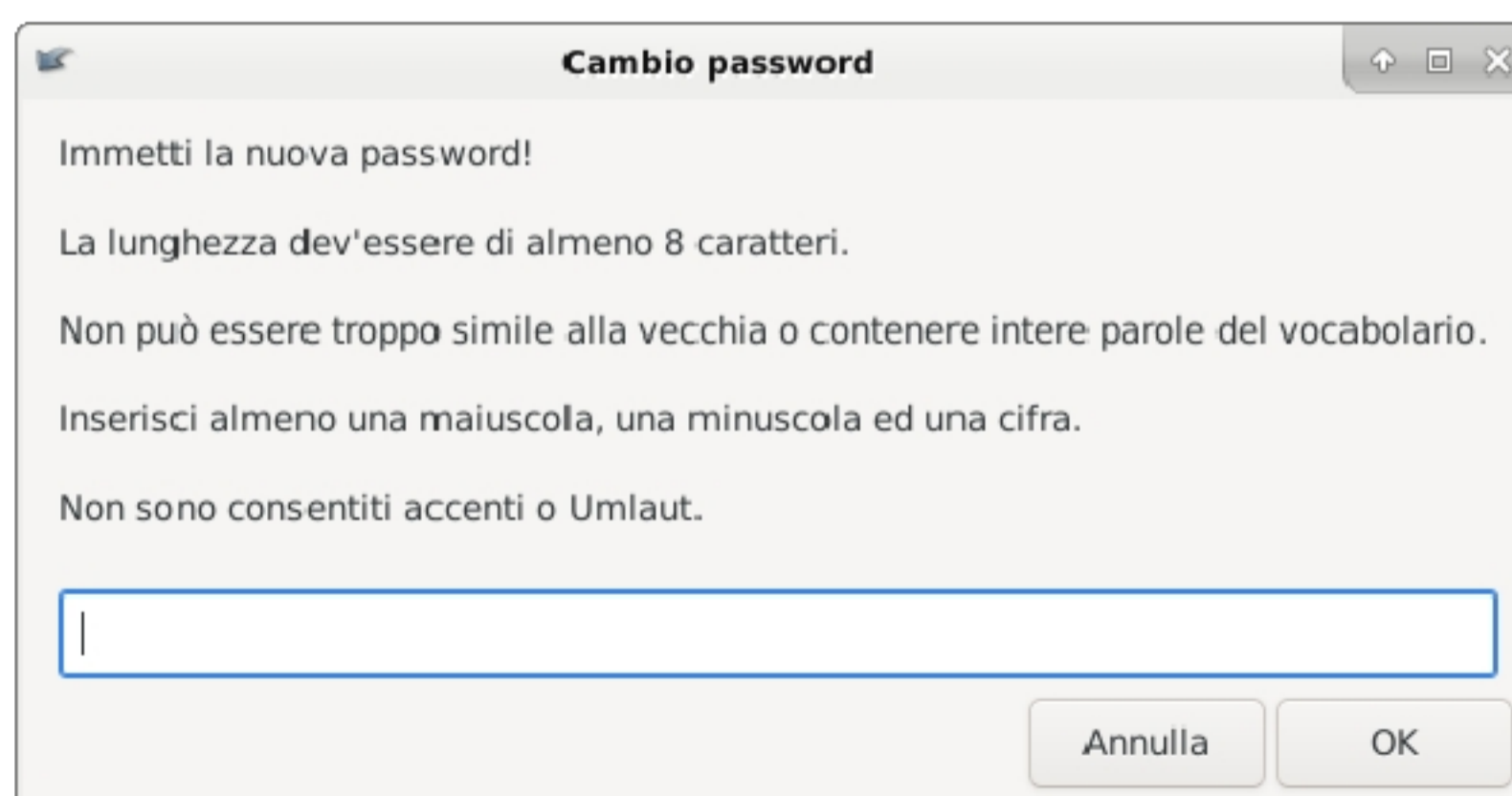
1. Open from the bottom left menu the **Change Your Password** program (just type "change" in the search field).

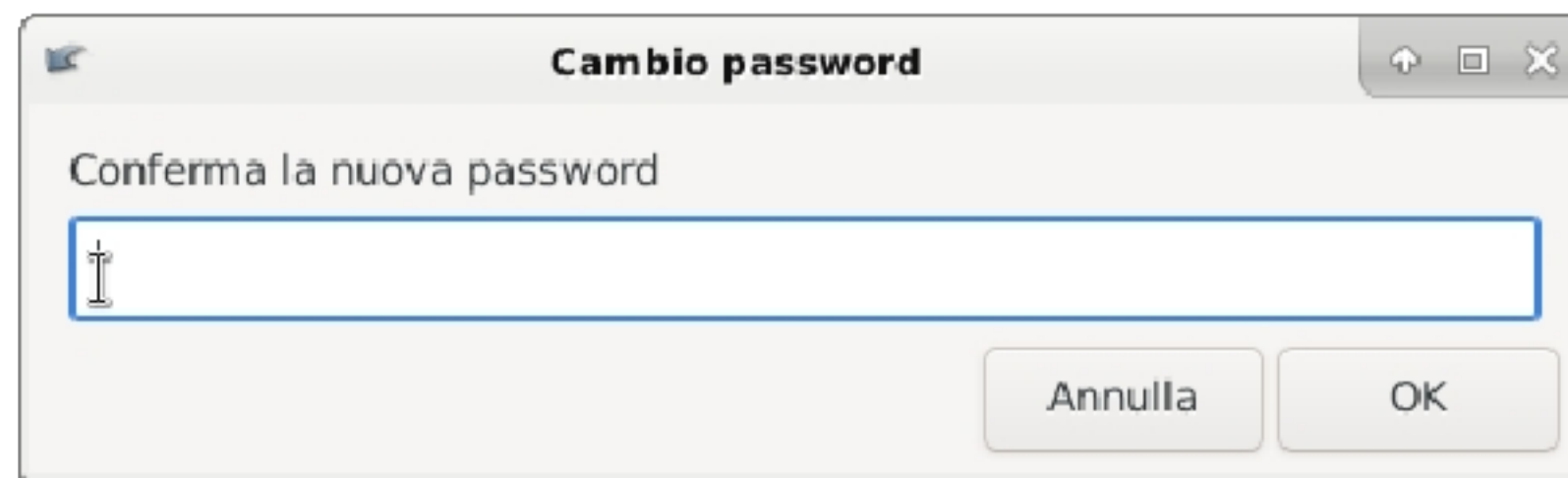


2. A window appears asking for the current password. Enter it and click *OK*.



3. Then enter the new password twice and click *OK*.

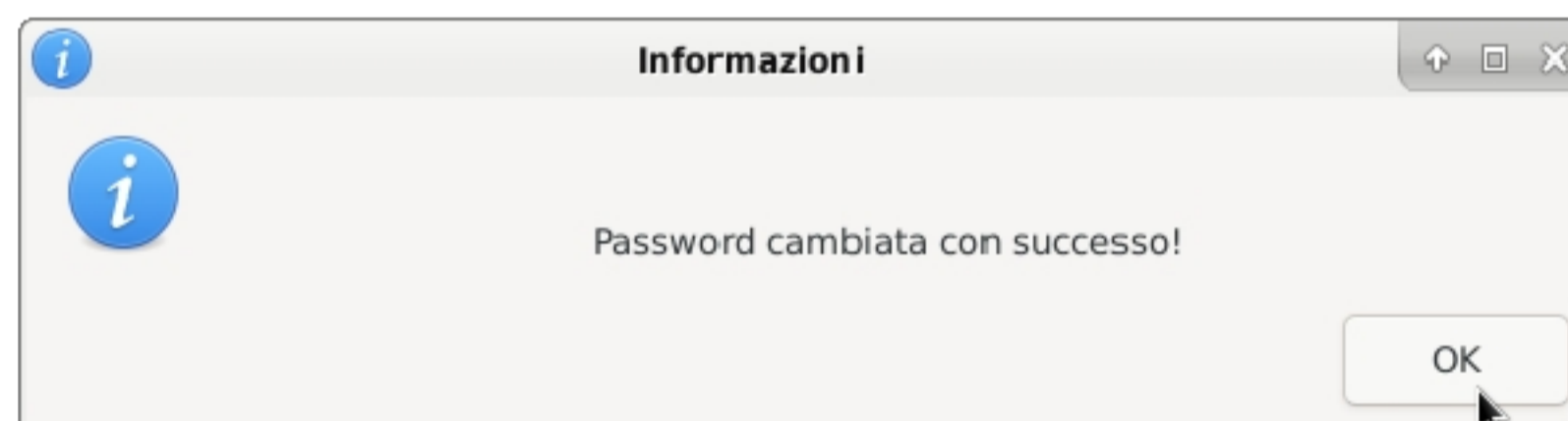




4. In case the password change was unsuccessful, a window appears warning of the error and a suggestion to try again:

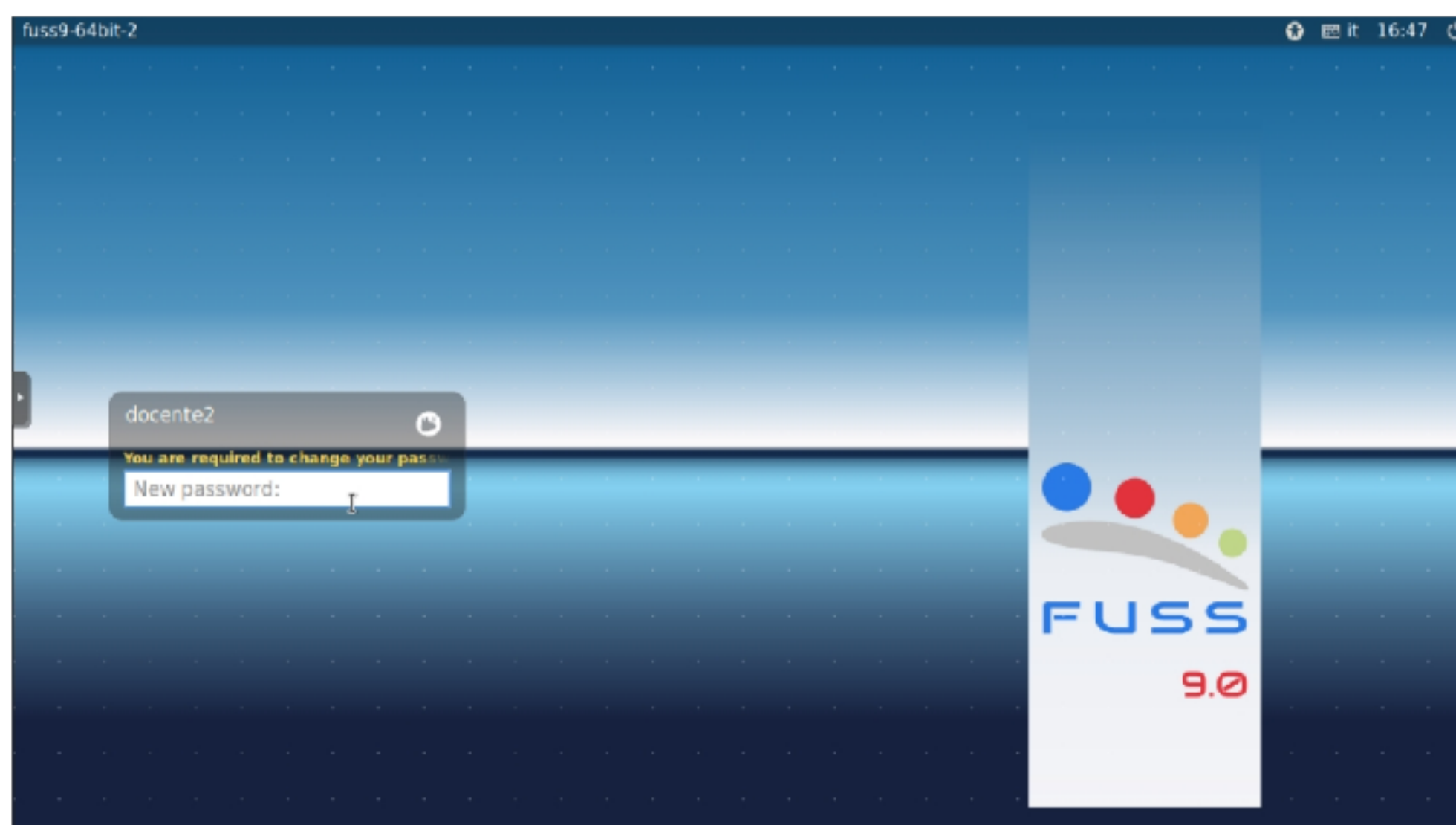


5. In case the password change was successful the message will appear:



7.5 Password change after expiration

If one's password has expired without being able to update it from the user session with the appropriate application, after authenticating oneself the system will respond with the message *"You are required to change your password immediately (password aged)"* which means *"You are required to change your password immediately (password expired)."*



The system will prompt you to enter your new password, which must follow the rules described in the requirements outlined above. If the password is too simple, the system will display a message prompting you to enter a stronger password. Below are two examples.

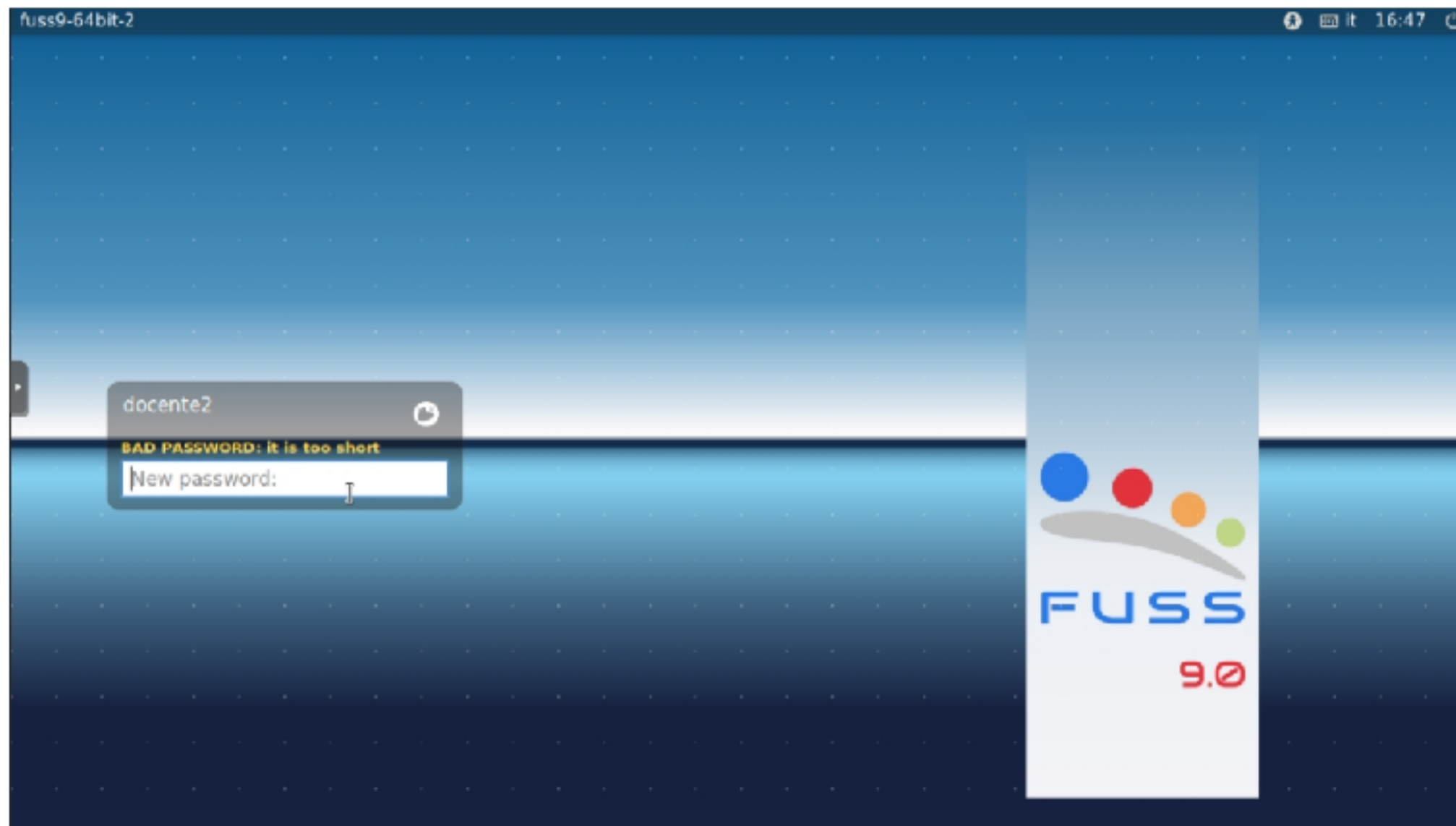


Fig. 1: Password too short

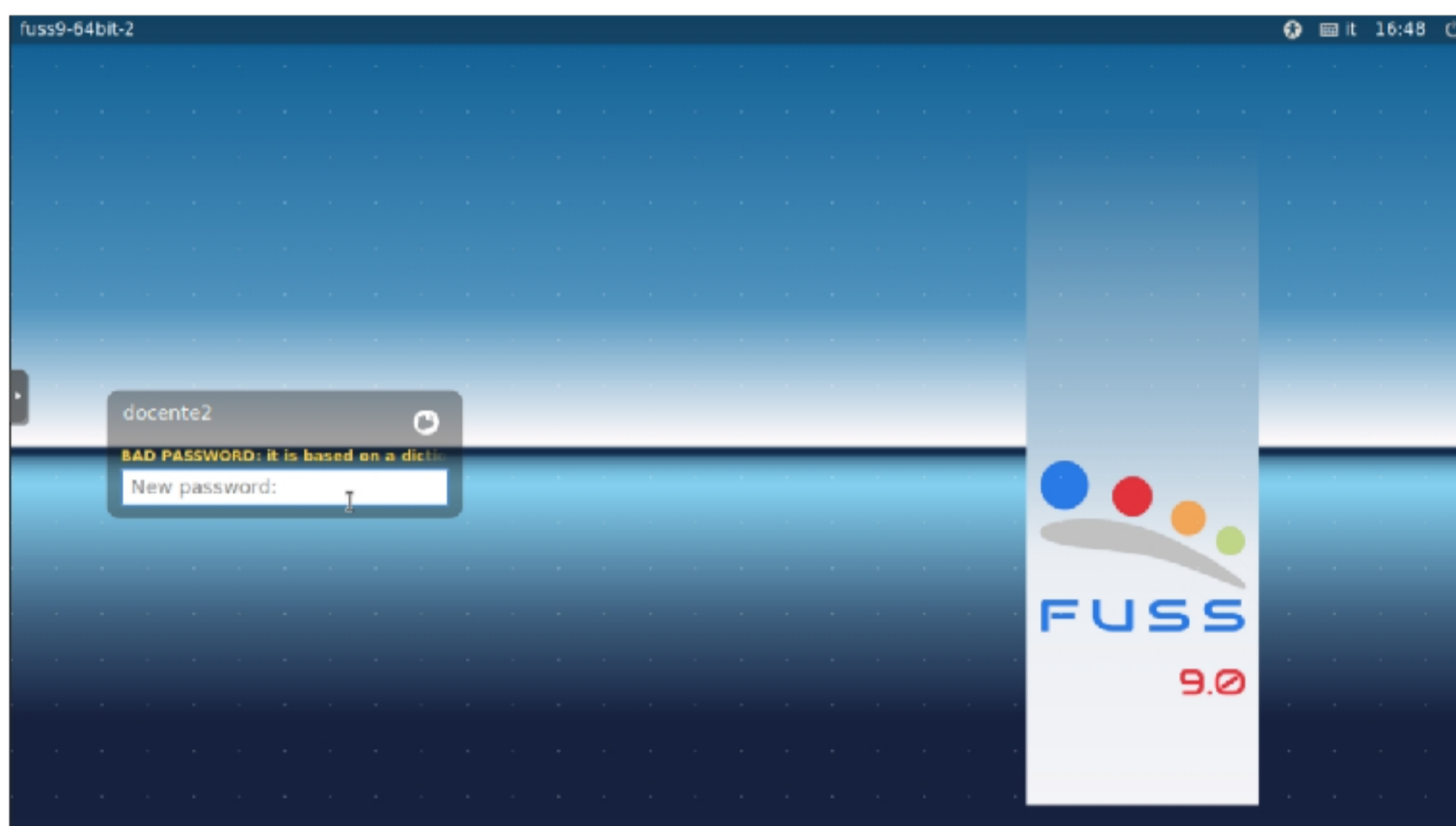
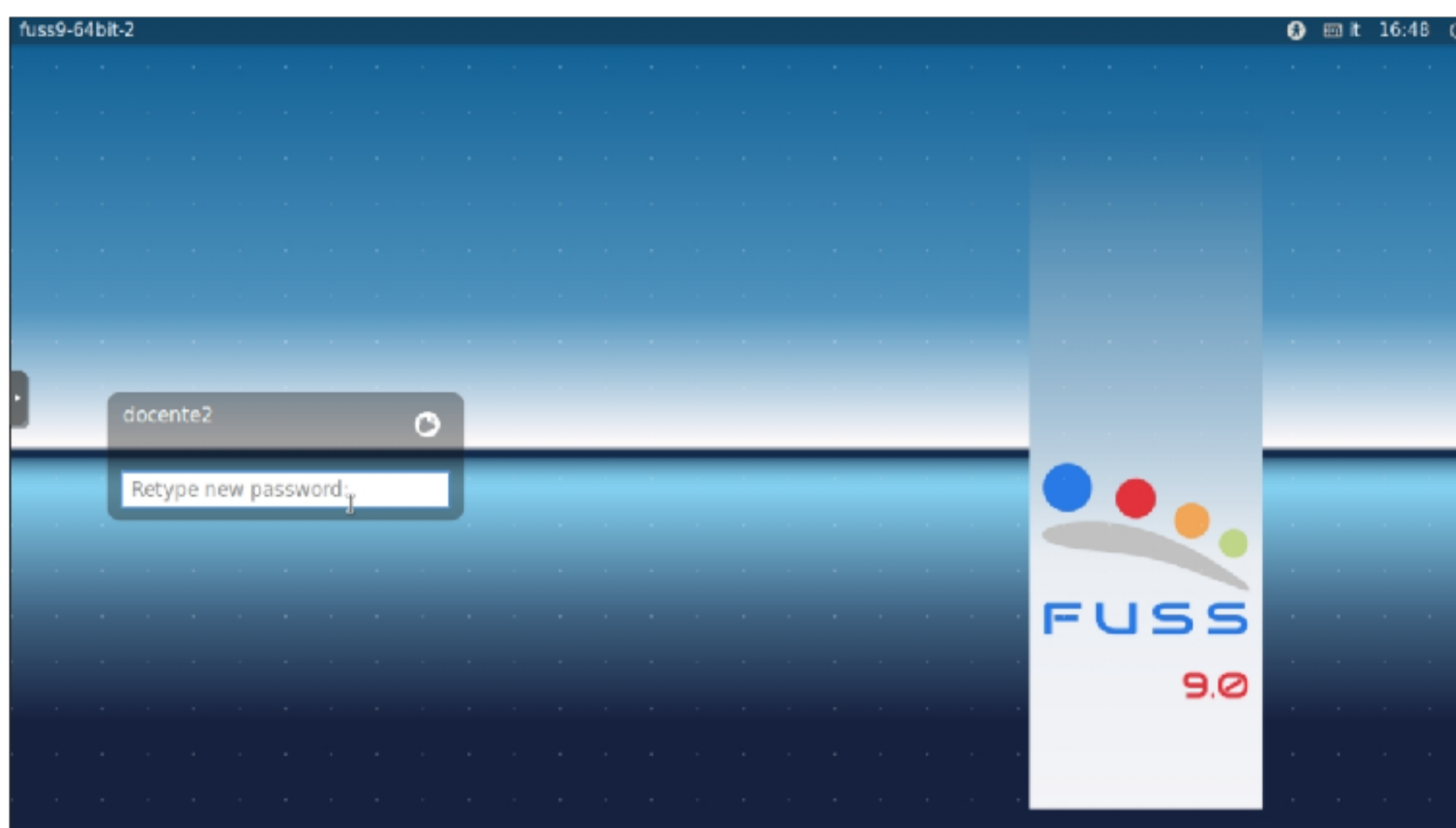


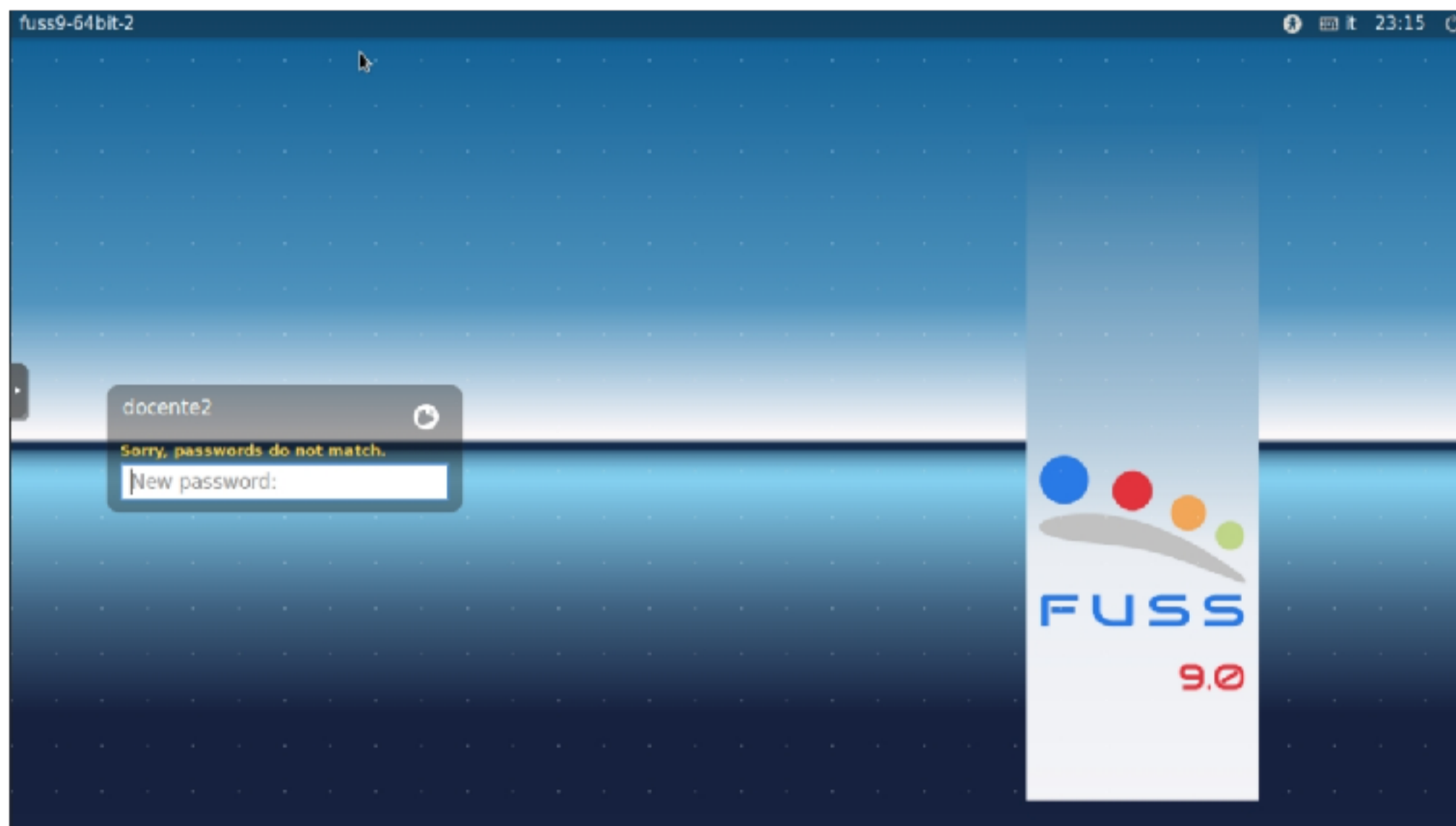
Fig. 2: Common password based on a dictionary term.

The system offers only three attempts to enter the new password; after the third attempt you will have to start over by entering your username and old password again.

Instead, if the new password matches the requirements, you will be prompted to retype it with the message "*Retype new password.*"



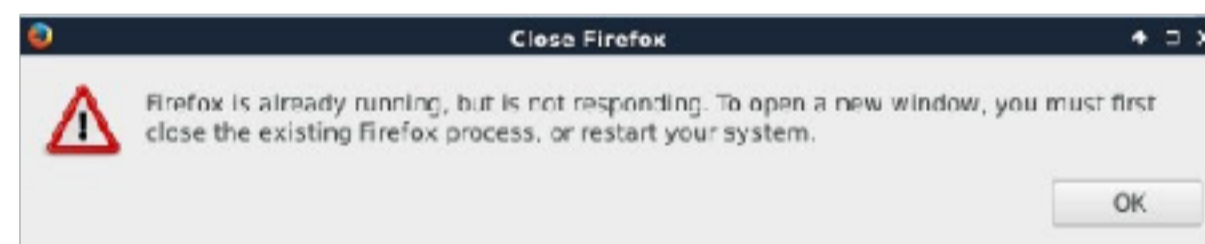
After typing it twice correctly, it will be possible to access the system. Otherwise, the user will be notified that the passwords entered do not match: *"Sorry, passwords do not match."*



Password changes for faculty are required when they first log in to the system and periodically every 90 days.

8.1 Browser access problem

The following window appears:



The problem is due to the fact that when you launch firefox, it creates a file (.parentlock) that does not allow access from another PC on the network with the same user . This may be due to a previous incorrect closing of the browser or momentary problems with the PC on which you previously worked.

- View hidden files
- Double click on the .mozilla folder , then on the firefox folder
- Inside the firefox folder is a folder named random.default, where random is a random sequence of characters
- Double click on this folder, then look for the .parentlock file and delete it.

8.2 Panel display problem on desktop

If you do not see the desktop correctly in all its parts, you can do this operation, which returns the desktop to the original situation

- open a terminal (see entry)
- type:

`rm -fr .cache/sessions/ .config/xfce4/` or:

- View hidden files
- Double click on the .cache folder , then delete the sessions folder

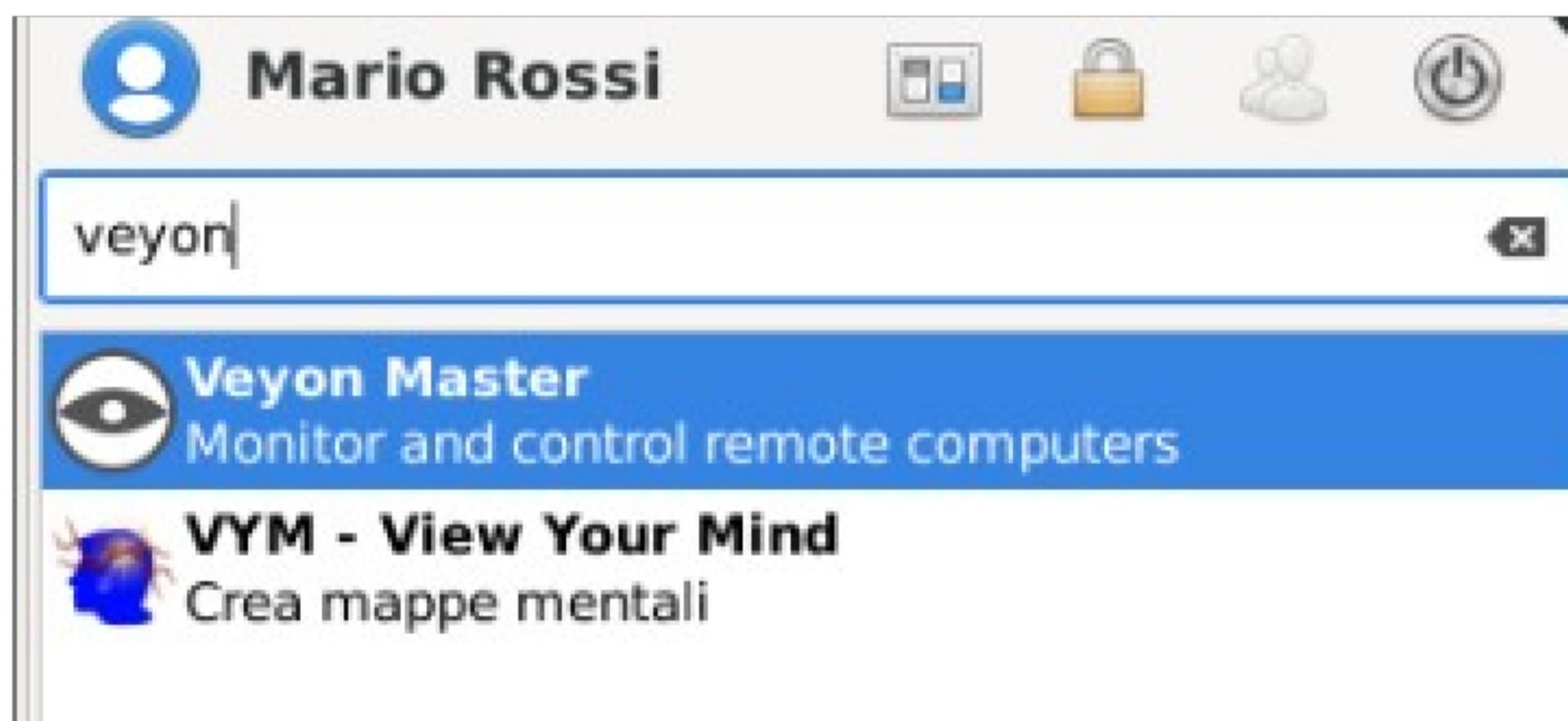
- Double click on the .config folder , then delete the xfce4 folder

9.1 Introduction

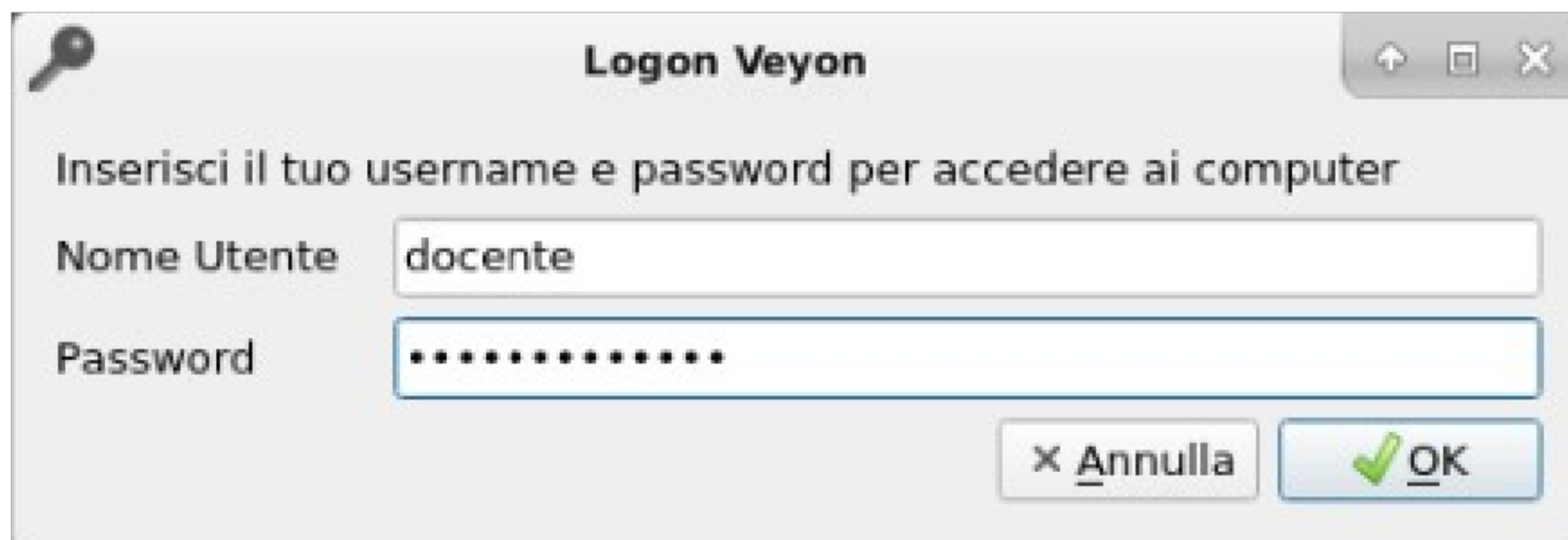
Veyon is an application that allows you to monitor and control a group of computers (e.g., classrooms) on a central computer (e.g., a teacher's computer) and use various features and modes.

9.1.1 Starting and accessing the program

Users not belonging to the veyon-master group will be blocked with an error message. For users belonging to the `veyon-master` group, the program is started via the Start menu:

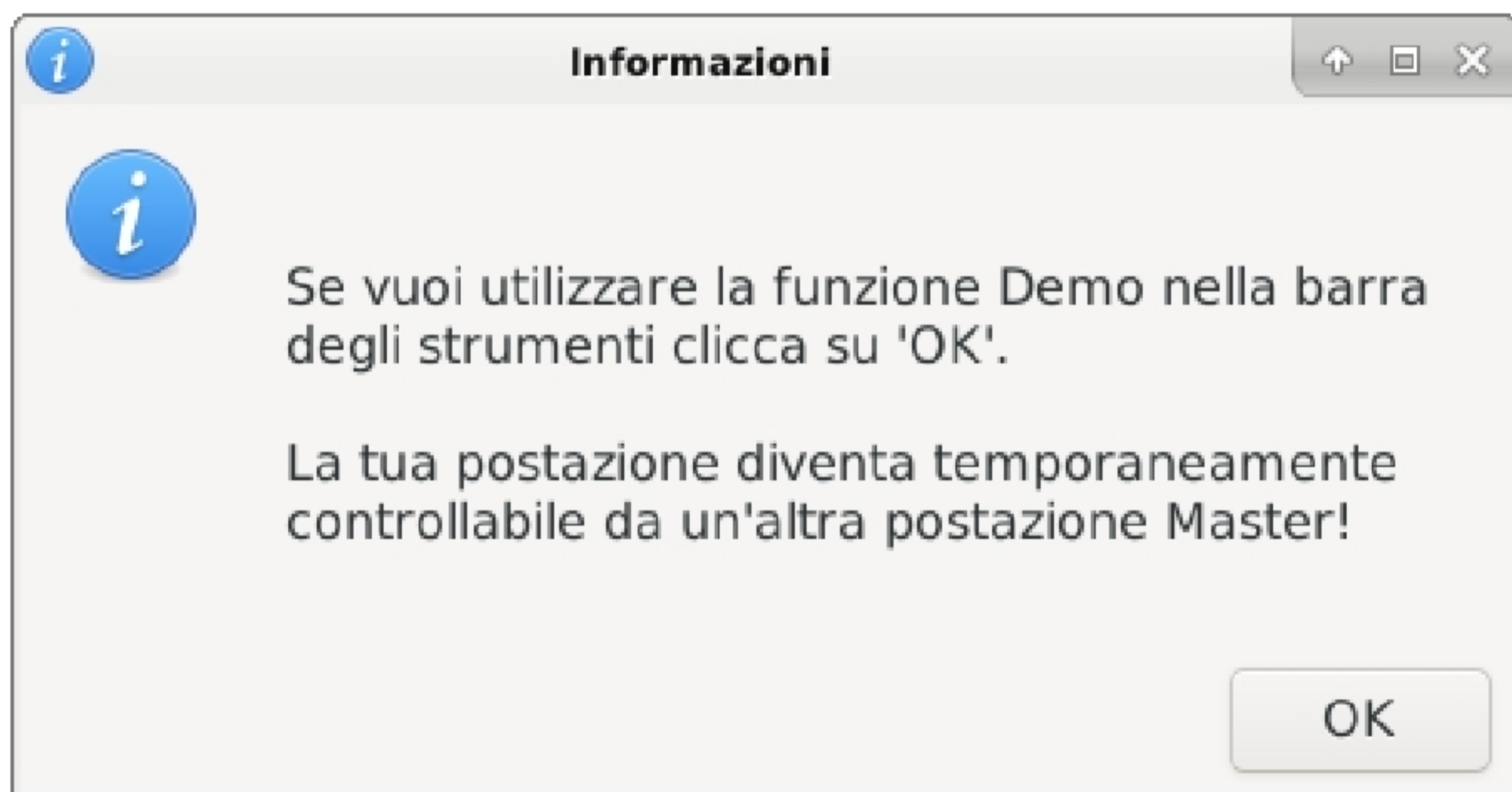


A user name and password will be required to log in:

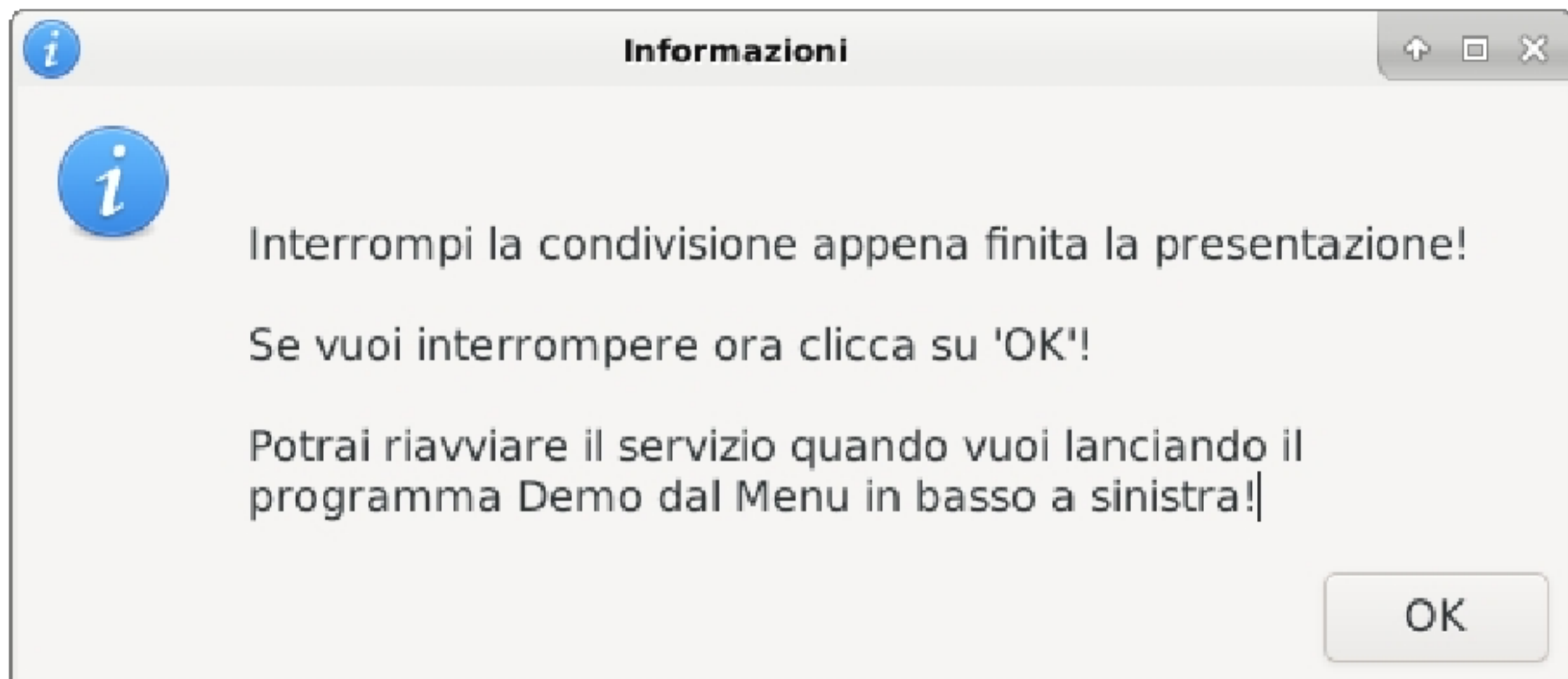


Enter user name and password. If the data entered are correct you can log in and the program will be started. Otherwise, access will be denied with an error message. In that case you can try to log in again by entering the correct data.

When the program starts, an information window appears asking if you want to use the Demo Function; in order to present your screen, you must click OK or even simply close it.

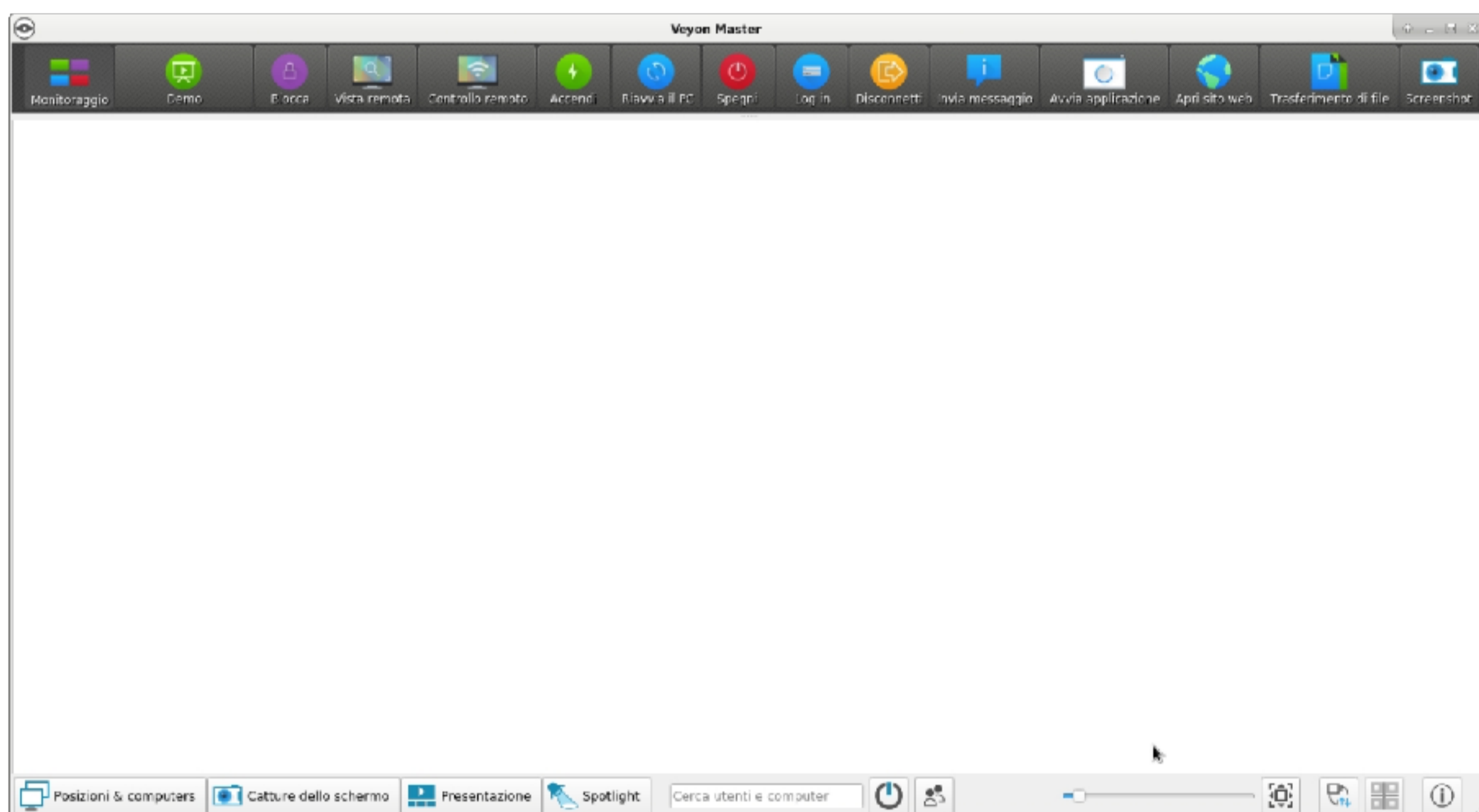


If you do not need it immediately, it is recommended to leave the window in the background. The moment you activate this function you temporarily become "controllable" from another location (you will be able to notice a kind of eye on the panel in the lower right corner). To stop the service simply click OK in the window:



9.1.2 User interface

After starting the program you will see the user interface with the toolbar (top panel), the monitor view (middle part) and the status bar with various controls (bottom panel)



The toolbar contains numerous buttons for activating various functions. A detailed description of each function can be found in the chapter *Program Features*.

The appearance and behavior of the toolbar can be customized as described in the section *Toolbar*.

In the monitor view, the computers are displayed in a tile view. Depending on the system configuration and previous program startup, you can already view the computers in the current location here.

The computer selection panel allows you to show or hide individual computers or entire locations.

The items in the status bar are used to control the program interface and are described in detail in the following section.

9.1.3 Status bar

Using the *Locations & computers* and *Screenshots* buttons , you can open and close the *Computer Selection* panel and the panel: *Screenshots* .

The search bar allows you to filter the displayed computers using computer names or user names as search terms.

The (*Show only computers on*) button hides all computers that are turned off, disconnected, or unreachable for some other reason.

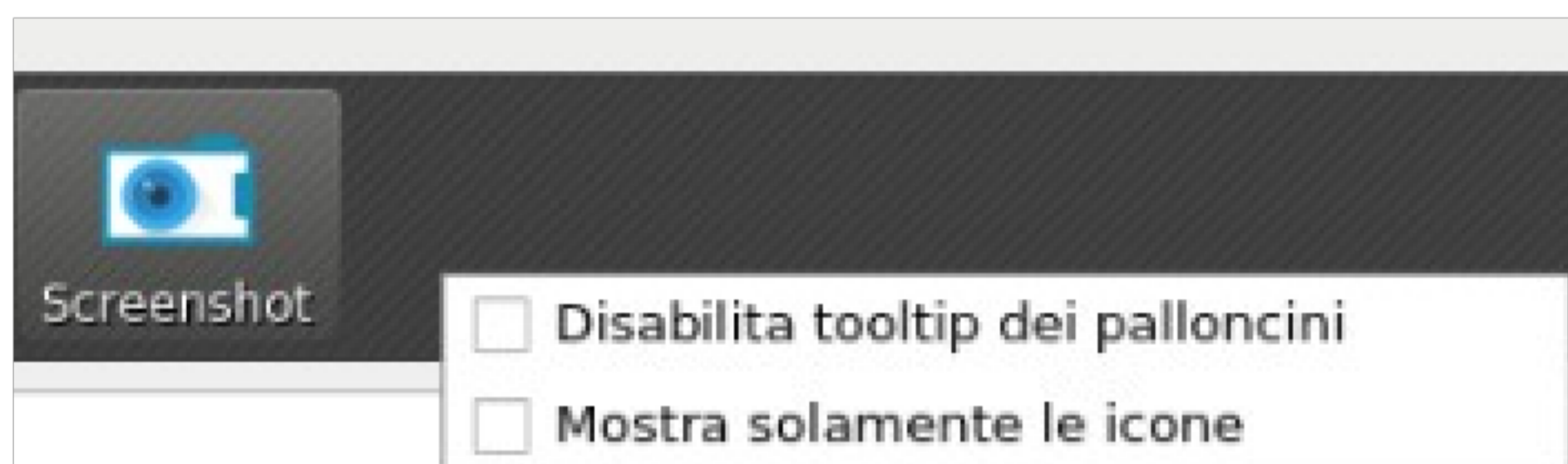
Use the slider to control the size of the displayed computer screens. By holding down then Ctrl key, the size can also be changed using the mouse wheel. The size is automatically adjusted by clicking the button (*Use the slider to control the size of the displayed computer screens. By holding down then Ctrl key, the dimension can also be changed using the mouse wheel. The size is automatically adjusted by clicking the button*) on the right.

It is also possible to use a custom computer arrangement, e.g., representing the current disposition of computers in classrooms. After clicking the (*Use Custom Computer Arrangement*) button, each computer individually or a selection of computers can be moved with the left mouse button pressed down and arranged as desired. To align all computers in the custom arrangement, click the button| (*Align computers to grid*) . If you want to use the standard ordered arrangement again, simply disable the button .

The (*About*) button opens a dialog box with information about Veyon such as version, manufacturer, and license conditions.

9.1.4 Toolbar

You can customize the appearance and behavior of the toolbar. A right click on a free section or button opens a shortcut menu with several items:



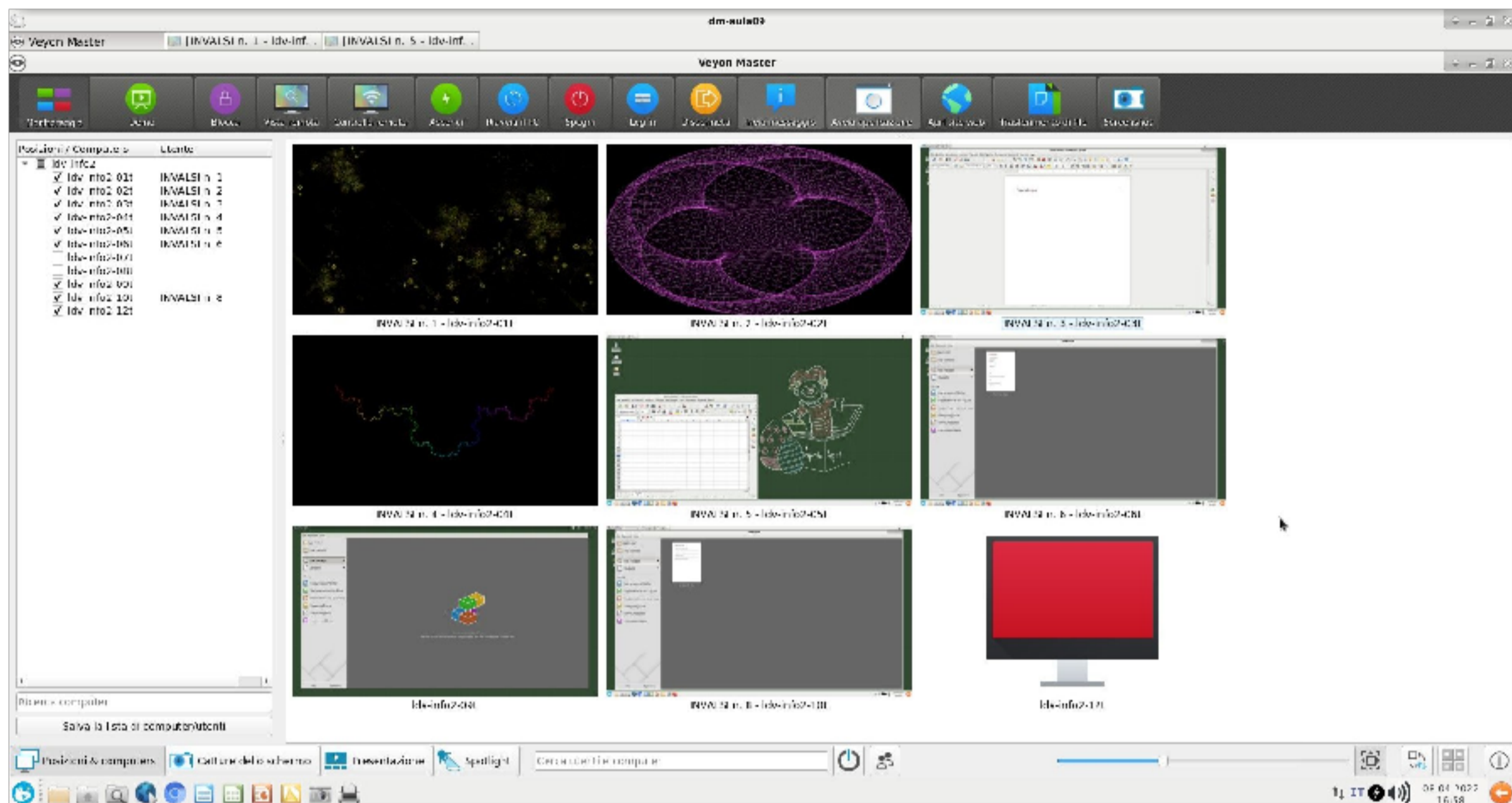
If you click the *Disable balloon command descriptions* item, command descriptions will no longer be displayed whenever you hover over the buttons. You can open the context menu at any time and deselect the item again.

The *Show only icons* option provides a compact view of the toolbar buttons by hiding the labels and displaying only the icons. On smaller screens this option may be necessary to display all buttons.

9.1.5 Computer selection panel

The *Locations & Computers* button in the status bar opens the computer selection panel. This panel displays all available computer locations in a tree structure. You can expand individual location entries by clicking on the corresponding symbol in front of them.

You can activate for monitoring individual computers or entire classrooms . All monitored computers will then be displayed in the monitoring view.



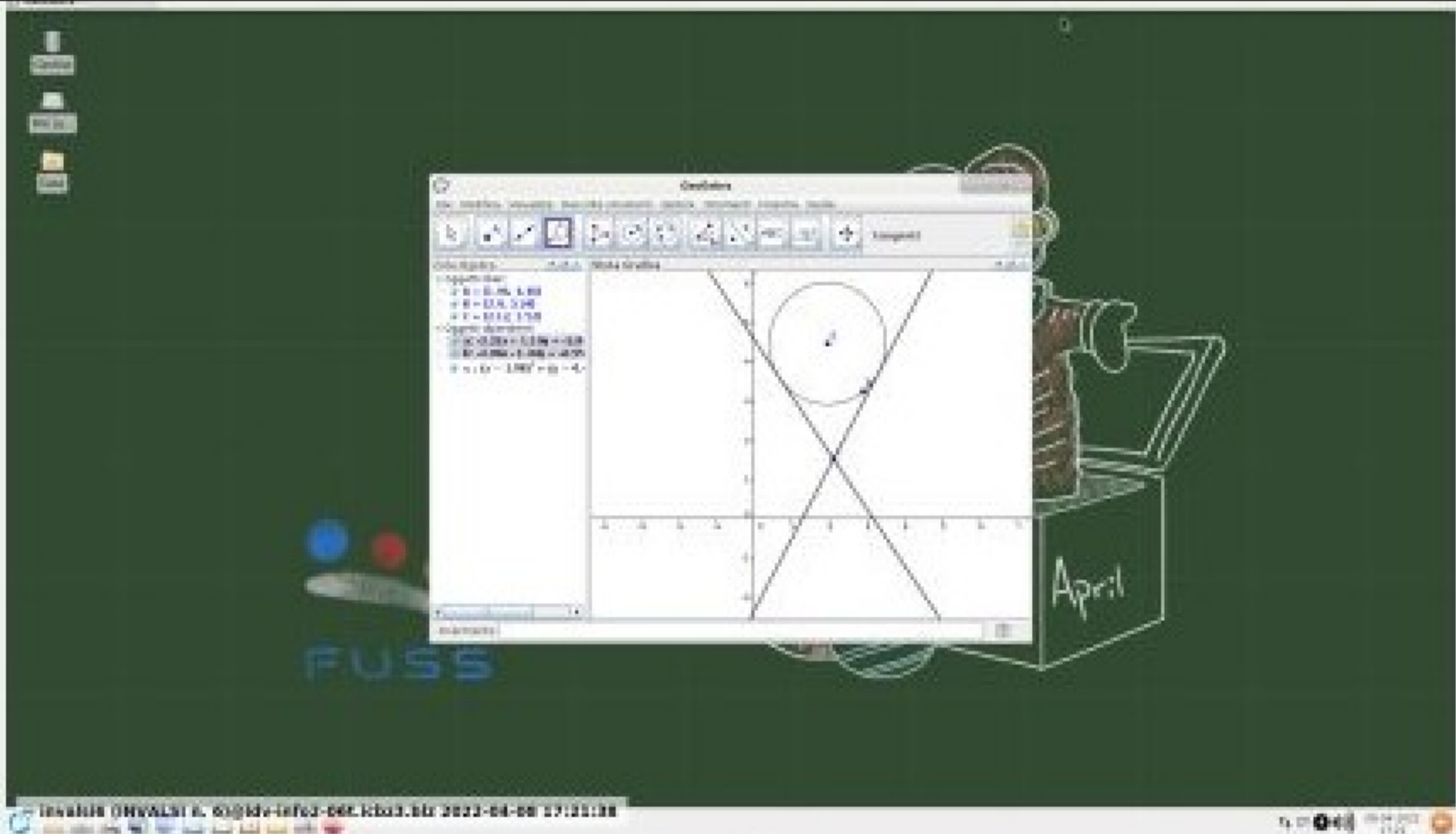
With the *Save Computer/User List* button, the list of computers and registered users can be saved in a CSV file. Typical use cases for this are subsequent IT-based attendance checks or exams.

9.1.6 Screens panel

Using the screenshot management panel, you can view and delete all acquired screenshots. Information on how to capture screenshots is provided in *Program Features*, chapter under *Screenshots*.

invalsi1_ldv-info2-01t.icbz3.blz_2022-04-08_17-21-38.png
invalsi2_ldv-info2-02t.icbz3.blz_2022-04-08_17-21-38.png
invalsi3_ldv-info2-03t.icbz3.blz_2022-04-08_17-21-38.png
invalsi4_ldv-info2-04t.icbz3.blz_2022-04-08_17-21-38.png
invalsi5_ldv-info2-05t.icbz3.blz_2022-04-08_17-21-38.png
invalsi6_ldv-info2-06t.icbz3.blz_2022-04-08_17-21-38.png
invalsi8_ldv-info2-10t.icbz3.blz_2022-04-08_17-21-38.png
sconosciuto_ldv-info2-09t.icbz3.blz_2022-04-08_17-21-38.png
sconosciuto_ldv-info2-12t.icbz3.blz_2022-04-08_17-21-38.png

Puoi effettuare screenshot cliccando l'elemento "Screenshot" nel r



Utente: invalsi6 (INVALSI n. 6)

Data: 08/04/22

Ora: 17:21:38

Computer ldv-info2-06t.icbz3.blz

Now you can select individual screenshots from the list. The details of the screenshot, such as the capture date, user name, and computer, are then displayed in the table below. The *Show* button or a double-click in the list shows the selected screenshot in full screen. If you no longer need the screenshot, you can permanently delete it using the *Delete* button . Note that this process cannot be undone and the files will not be moved to the recycle bin.

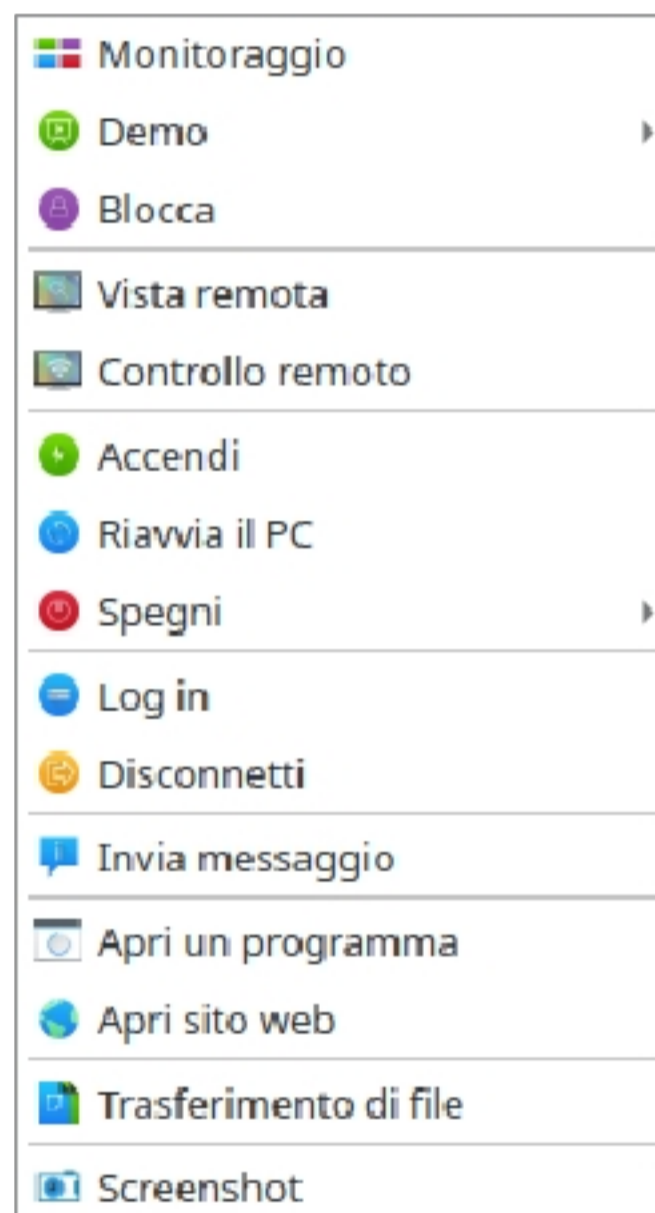
9.2 Functionality of the program

Veyon offers a variety of features that allow you to control and access computers. All available features can be accessed through buttons in the toolbar and the shortcut menu on individual computers.

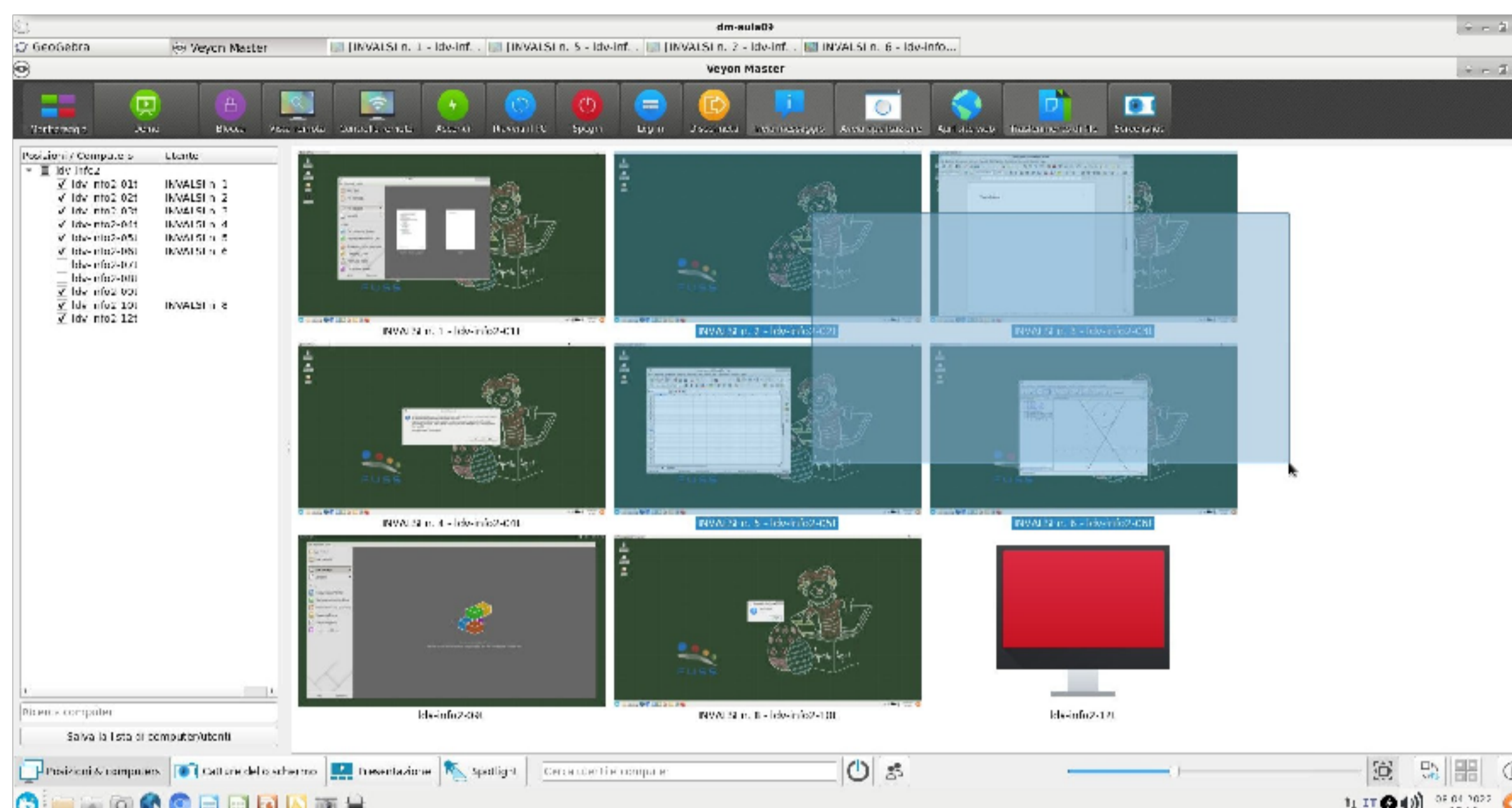
If you move your mouse over individual toolbar buttons, a tooltip with short help text is displayed, unless you have disabled tooltips. Pressing a button activates the desired function on all displayed computers.

9.2.1 Using functions on individual computers

If you want to activate only one function on a single computer, right-click on the computer in the monitor view and select the desired function from the shortcut menu. Items in the context menu are displayed dynamically according to the active functions.



You can also select multiple computers in the monitor view by drawing a selection rectangle with the mouse that includes all the desired computers:



Alternatively, you can press the **Ctrl** key and add computers individually to the selection by mouse click.

9.2.2 Monitoring mode

By default, Veyon is running in monitoring mode. In this mode you have a panoramic view of all computers and see their screen contents in thumbnails. The screen contents are updated almost in real time, so you can monitor all activity at the selected locations.

As long as there is no connection to a computer, a computer icon is displayed instead of the contents of the screen. After the program starts, the icon is initially colored gray. As soon as the program detects that the computer is unreachable or access is denied, the color turns red.

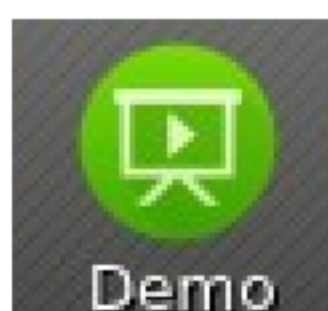
Some of the features described in the following sections change remote computers to a different mode. You can exit the respective mode by activating the monitoring mode again.



9.2.3 Demonstration mode

You can use the demonstration mode (demo mode) to start a presentation. In this mode, your or a student's screen content is broadcast to all computers and displayed in real time. You can choose between a full screen and a demo window.

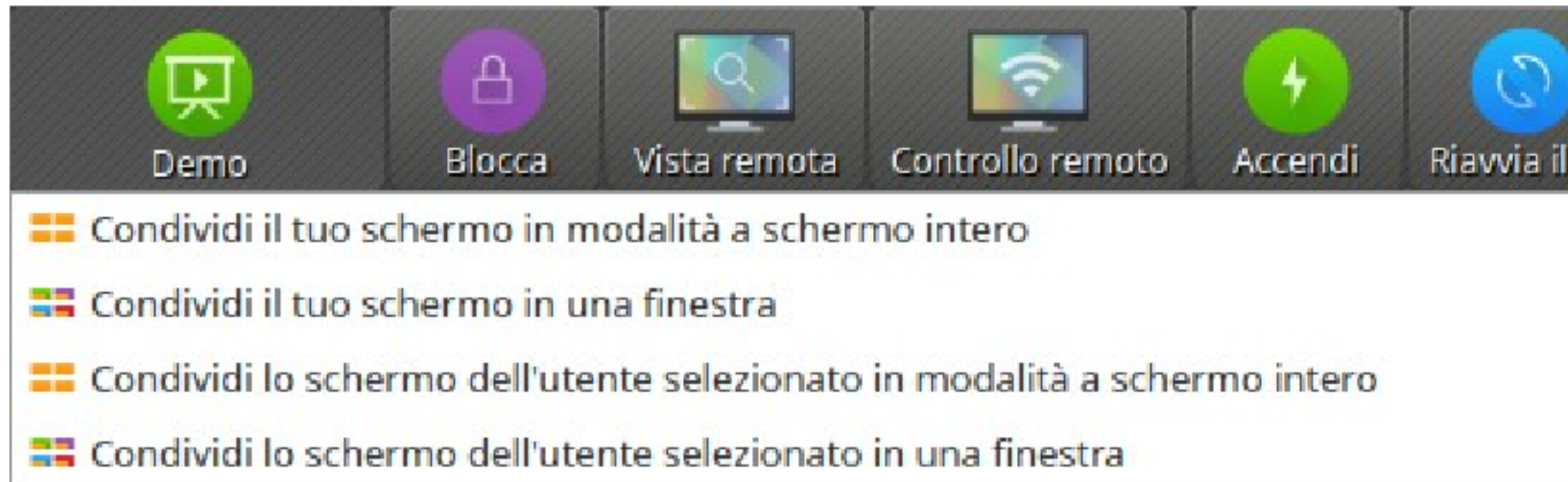
To start a presentation from your monitor, you must first start a service. You can do this by using the appropriate Start *Demo Service* window, or, if it has already been closed, by starting the Demo program in the Start Menu at the lower left.



During a full-screen demo, the screen content will be displayed full screen on the remote computers. Logged-in users cannot use their computers for other activities in this mode because all input devices are locked. In this way you will get the full attention of your students.

In contrast, a demo window allows users to alternate between the demo window and their own applications. For example, course participants can arrange the windows side by side and try the demonstrated steps in parallel. Input devices are therefore not blocked in this mode.

To start a demonstration, you must open the demo menu by pressing *Demo*:



Now click on the desired item in the menu. If you want to share a student's screen, be sure to select it first so that the program knows which screen to broadcast.

In case your computer has multiple screens, you can choose to broadcast only one of the screens. To do so, click on the corresponding screen item in the demo menu before sharing the screen.

If you want to exit demonstration mode again, simply press the button or click the *Monitoring* button to return to global monitoring mode. The shortcut menu can also be used to stop demo mode on individual computers.

9.2.4 Blocking screens

Another way to get students' attention is to use the screen lock function. As during a full-screen demonstration, all input devices on the students' computers are locked. The computers can therefore no longer be used by students. In addition, a lock symbol is displayed to avoid distractions caused by open applications.

Press the *Lock* button to lock all displayed computers:



If you want to unlock the screens, simply press the button again or click the button *Monitoring* to return to global monitoring mode.

If only individual computers are to be locked, they can be selected as described in *Using functions on individual computers* and select the screen lock function in the shortcut menu. The screen lock can then be turned off by selecting *unlock* or returning to *Monitor* mode. Screen lock can also be initially activated globally and then deactivated for individual computers via the shortcut menu.

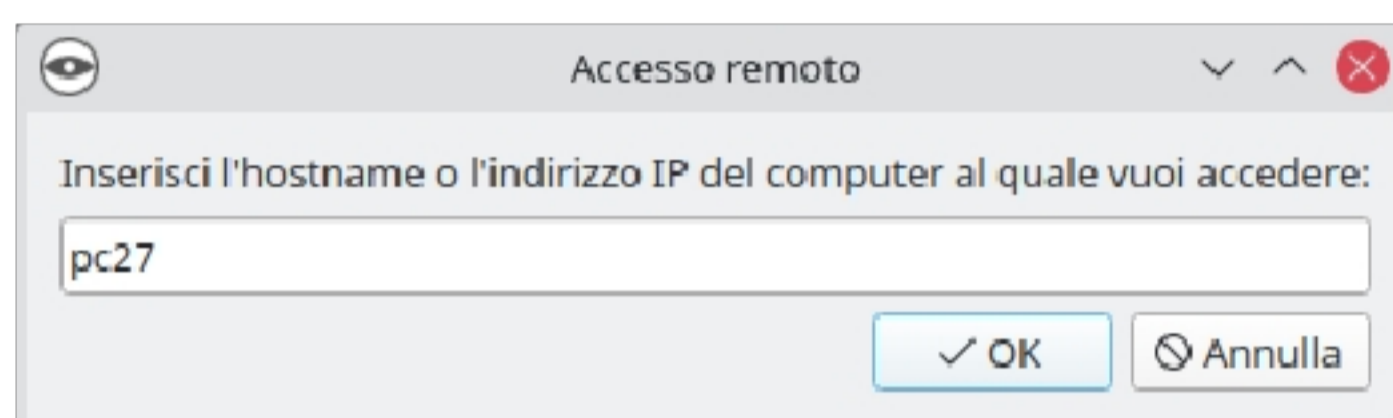
Note: Due to security restrictions of most operating systems, the lock screen cannot be displayed if no user is logged in. Input devices are still locked, so they cannot be accessed by the user.

9.2.5 Remote access

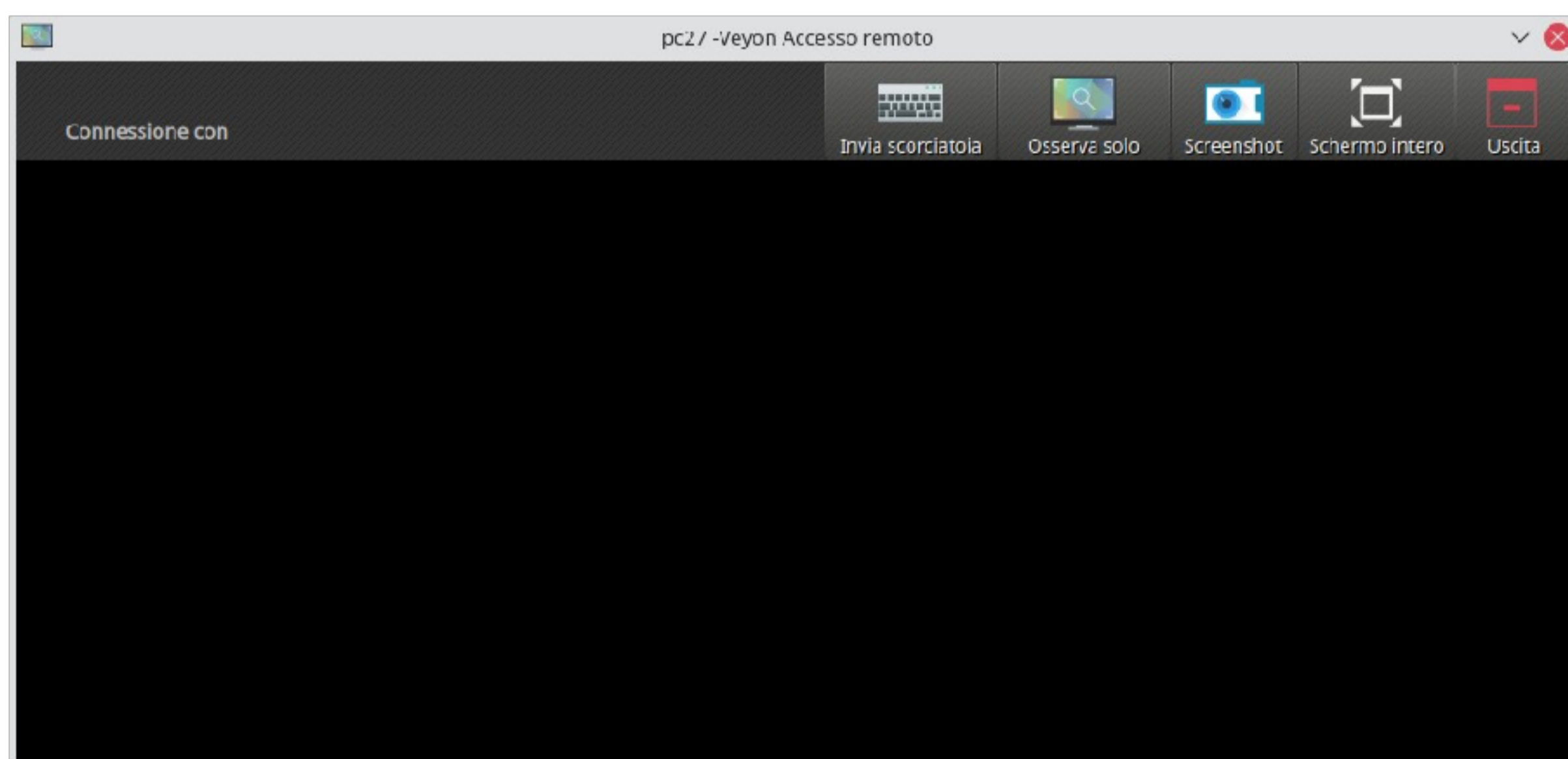
The *Remote Access* function group consists of two very similar functions *Remote View* and *Remote Control*. In both access modes, the screen of a remote computer is displayed full screen in a separate window. In contrast to the monitoring mode in the main window, you can look at activities on a computer in detail or take action yourself. In both access modes, the screen of a remote computer is displayed full screen in a separate window. In contrast to the monitoring mode in the main window, you can watch activities on a computer in detail or take action yourself.



After this button is pressed, a dialog box is opened requesting access to the computer's host name:



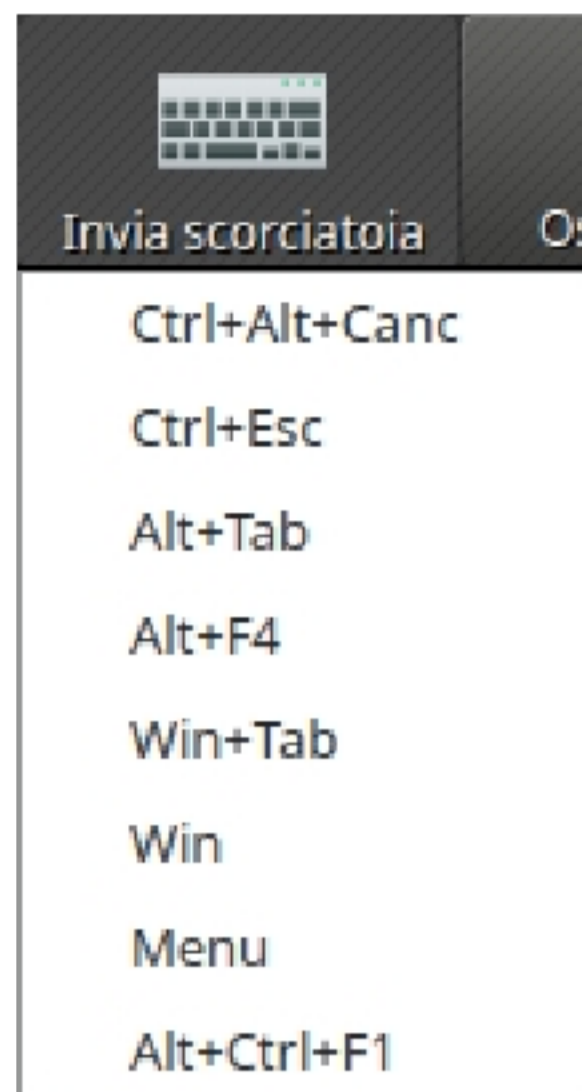
Then a new window opens with the remote access view:



The remote screen is then displayed in seconds and updated in real time. At the top of the window you will see a toolbar with buttons similar to the main application. The toolbar automatically disappears a few seconds after the connection is established. You can show it again at any time by moving the mouse pointer to the top of the screen.

You can also change the access mode at any time during a running remote access session. All you have to do is click on the *Remote Control* or *Observe Only* button. The button does not show the current access mode, but the access mode that is changed when it is pressed.

As soon as you enter *Remote Control* mode, keystrokes, mouse movements and clicks are transmitted to the remote computer so you can use it as usual. However, depending on the operating system, some special keys or keyboard shortcuts such as `Ctrl+Alt+Del` cannot be used directly. If you want to use these shortcuts, you can use the *Send Shortcut* button. Clicking this button opens a menu where you can select the desired shortcut:



If the menu was opened accidentally, it can also be closed again without triggering an action by clicking the button again or pressing the `Esc` key.

If you want to switch to full screen mode, you can use the *Full Screen* button . In full screen mode, the label of the button changes to *Window*. You can easily switch back to window mode by clicking on it again.

The *Screenshot* function captures the content of the current screen and saves it to a file that can be viewed later. More information about screenshots can be found in the Screenshot and *Screenshot Panel* sections.

With the *Exit* button, the remote access window is closed.

9.2.6 Restarting and shutting down computers

The *Turn On* function is currently not functional in FUSS networks, although it is present in the toolbar.

Using the functions *Restart PC* and *Shut Down* , you can restart or shut down remotely controlled computers. The corresponding buttons are available in the toolbar:



Click the appropriate button to reboot or shut down all displayed computers. If you want to use a function only for individual computers, you can select the respective computers and select the desired item in the shortcut menu (right-click).

Veyon 4.2 and later versions offer additional shutdown options. These options can be selected from a menu that opens by clicking the *Shut Down* button :



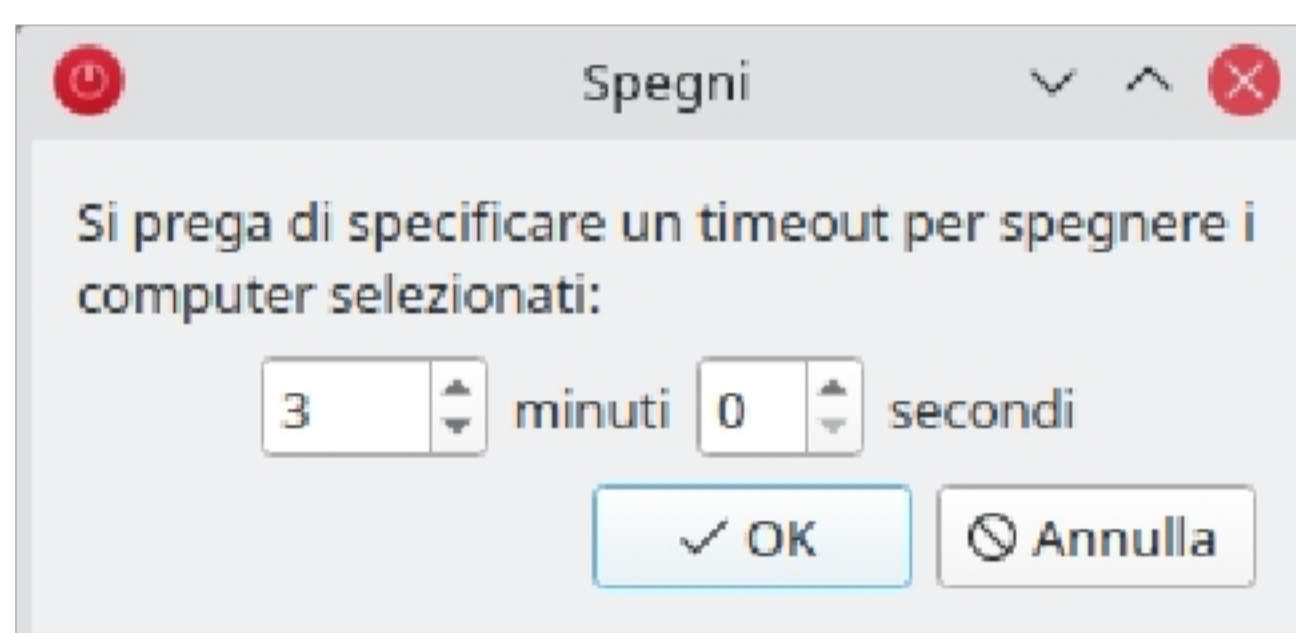
The following actions are available:

Shut down now Computers will shut down immediately without any further confirmation dialogs.

Install updates and shutdown If supported by the operating system, all disposable system updates will be installed during the shutdown process. If no updates are available, the respective computer will be shut down immediately.

Turn off after user confirmation With this option, each connected user will be asked whether to turn off the respective computer. If no user is connected to a particular computer, it will be turned off immediately.

Shut down after timeout With this option, each connected user will be asked whether to shut down the respective computer. If no user is connected to a particular computer, it will be shut down immediately.

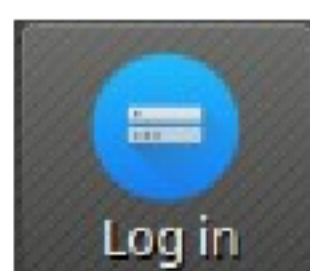


After accepting the dialog box, a countdown window appears on all computers telling users to save their work and close all applications.

Caution: Note that, depending on the program configuration, computers will be restarted or shut down without additional confirmation dialogs. Therefore, always make sure that users who have logged in have saved all open documents, etc. And, if possible, have closed all programs. This prevents unwanted loss of data.

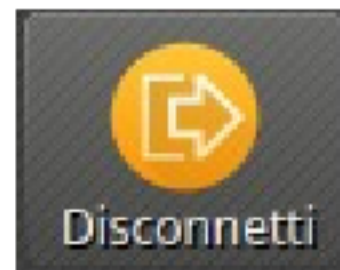
9.2.7 User log in

The function: *log in* for security reasons is not currently available in school networks.



9.2.8 Log off users

The *Disconnect* function complements the possibilities described in the previous section for controlling the basic states of the computer. A corresponding button in the toolbar is available for this purpose:



Activate this button to disconnect all users from all controlled computers. If you want to use this function only for individual computers, you can select the respective computers and select the desired item in the shortcut menu (right click).

Tip: After accepting the dialog box, a countdown window closes on all computers, telling users to save their work and close all applications.

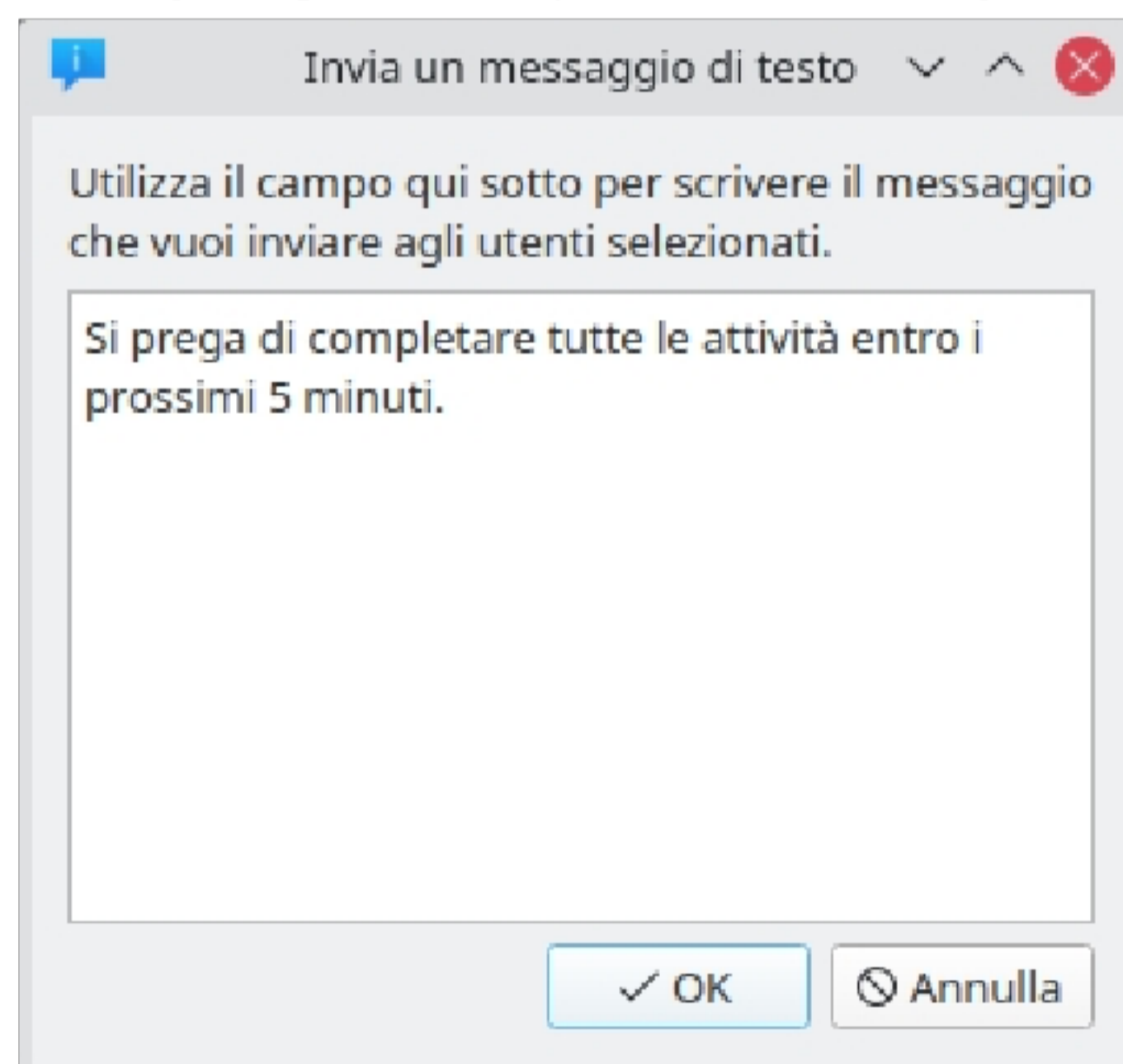
Caution: Note that logged-in users, depending on the program configuration, are logged out without further confirmation dialogs. Therefore, always make sure that the logged-in users have saved all open documents, etc. And, if possible, have closed all programs. This prevents unwanted loss of data.

9.2.9 Send a text message

Another option for user interaction is to send a text message to individual or all course participants. The text message is displayed on computers in the form of a message window. The *Send Message* button is available for this purpose:



After pressing the button, a dialog box opens in which you can enter the message to be displayed:



Click *OK* to send the entered message.

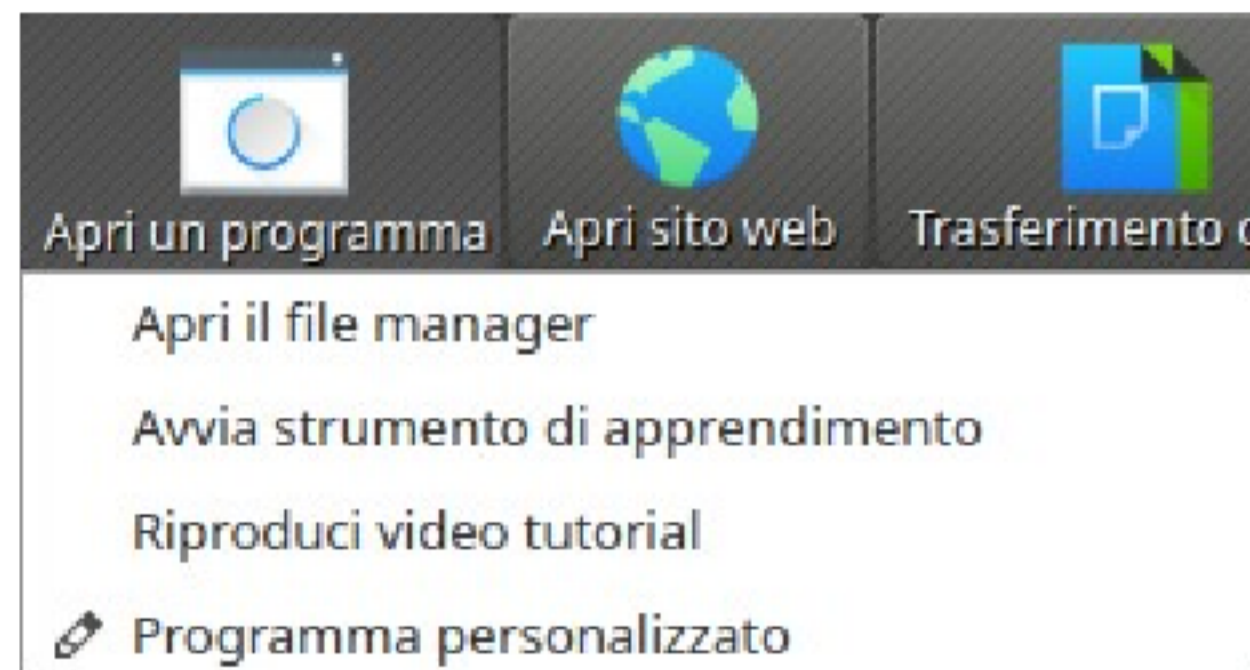
If you want to use this function only for individual computers, you can select the respective computers and select the desired item in the shortcut menu.

9.2.10 Open a program

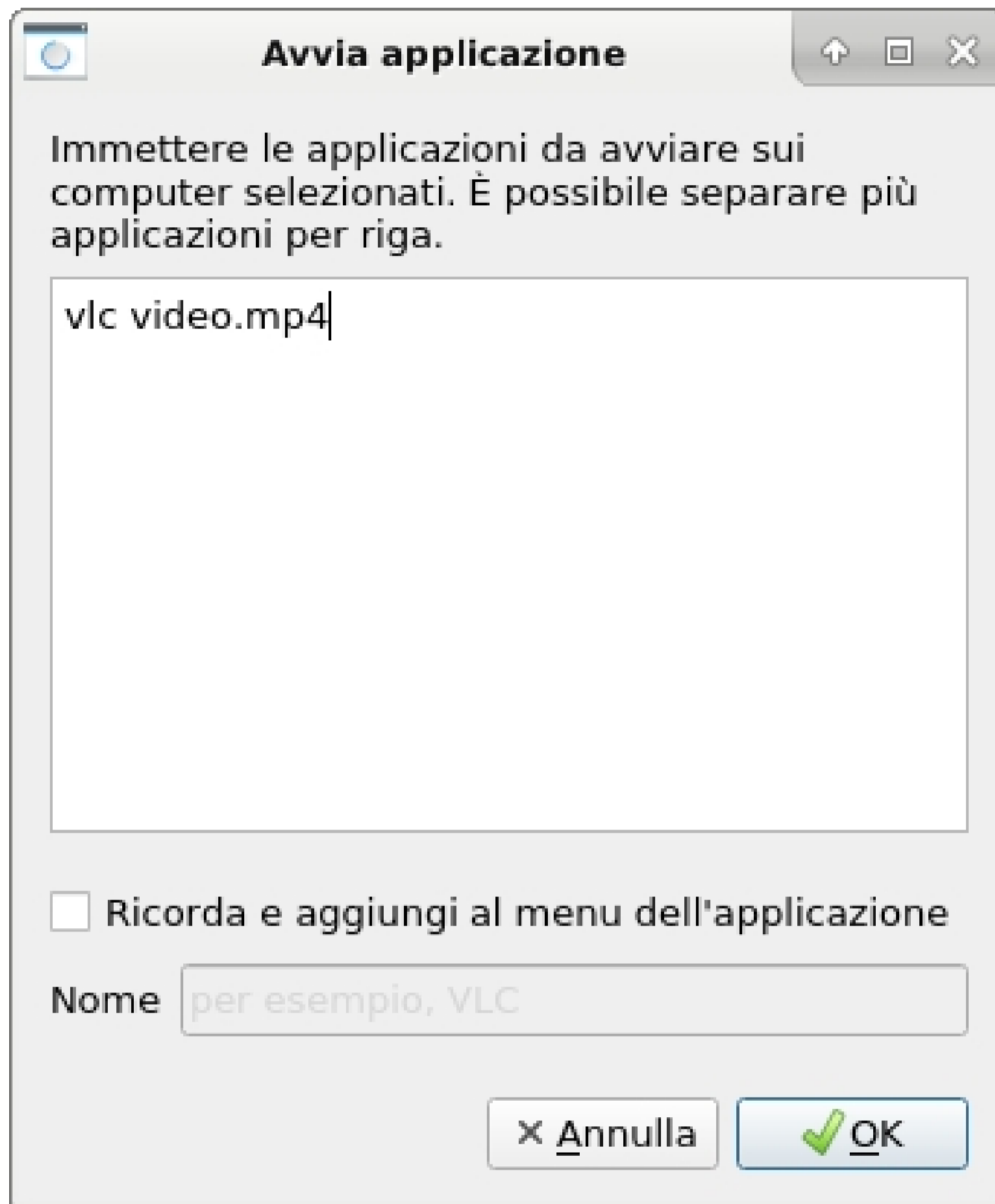
If a specific program needs to be started on all computers, you can use the *Run Program* feature in the toolbar. For this purpose, click on the button shown:



Depending on whether custom programs were added earlier or whether the programs were predefined by the administrator, a pop-up menu or a dialog box will open. In the former case, all available programs are listed in the menu:



Click on the desired item to run the respective program on all computers. Alternatively, click on the last *Custom Program* item to run an unlisted program. This will open a new dialog box. In this dialog box you can enter the name of the program to be run:



Confirm this dialog box with *OK* to run the program.

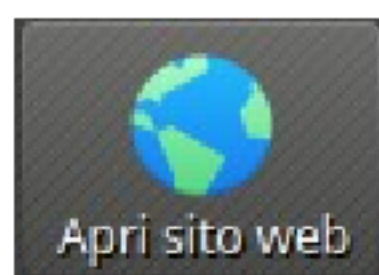
Note: To remove a previously added custom program, move the mouse over the corresponding item and press the *Del* key.

Tip: You can pass an argument to most programs with the name of a file you want to open automatically. For example, if you want to play a video on all computers, add the path to the video file separated by a space, e.g., `vlc Writing\Esempio.mp4`.

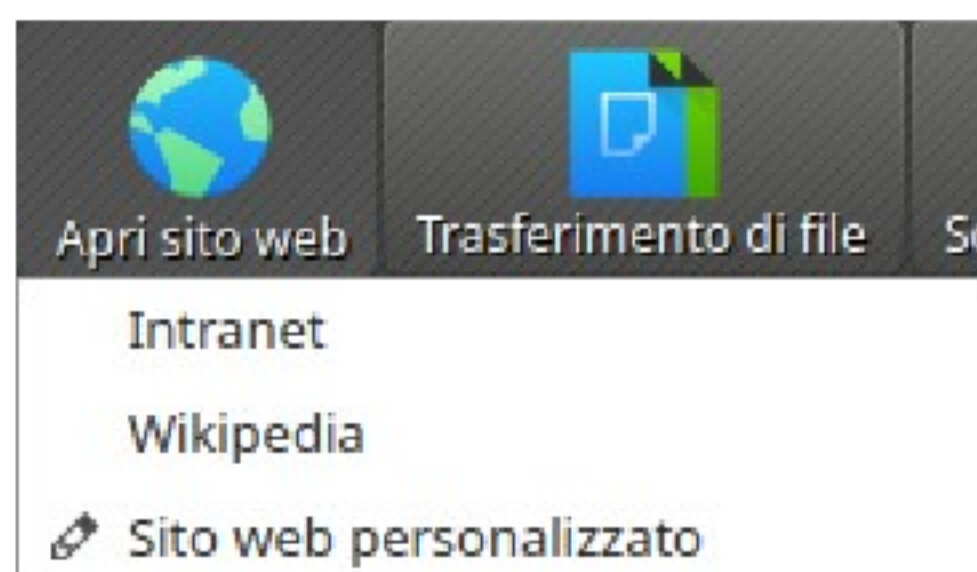
Warning: In the event that the program path or file name contains spaces (something generally to be avoided with Linux), it is not currently possible to run it or open the file.

9.2.11 Linking to a website

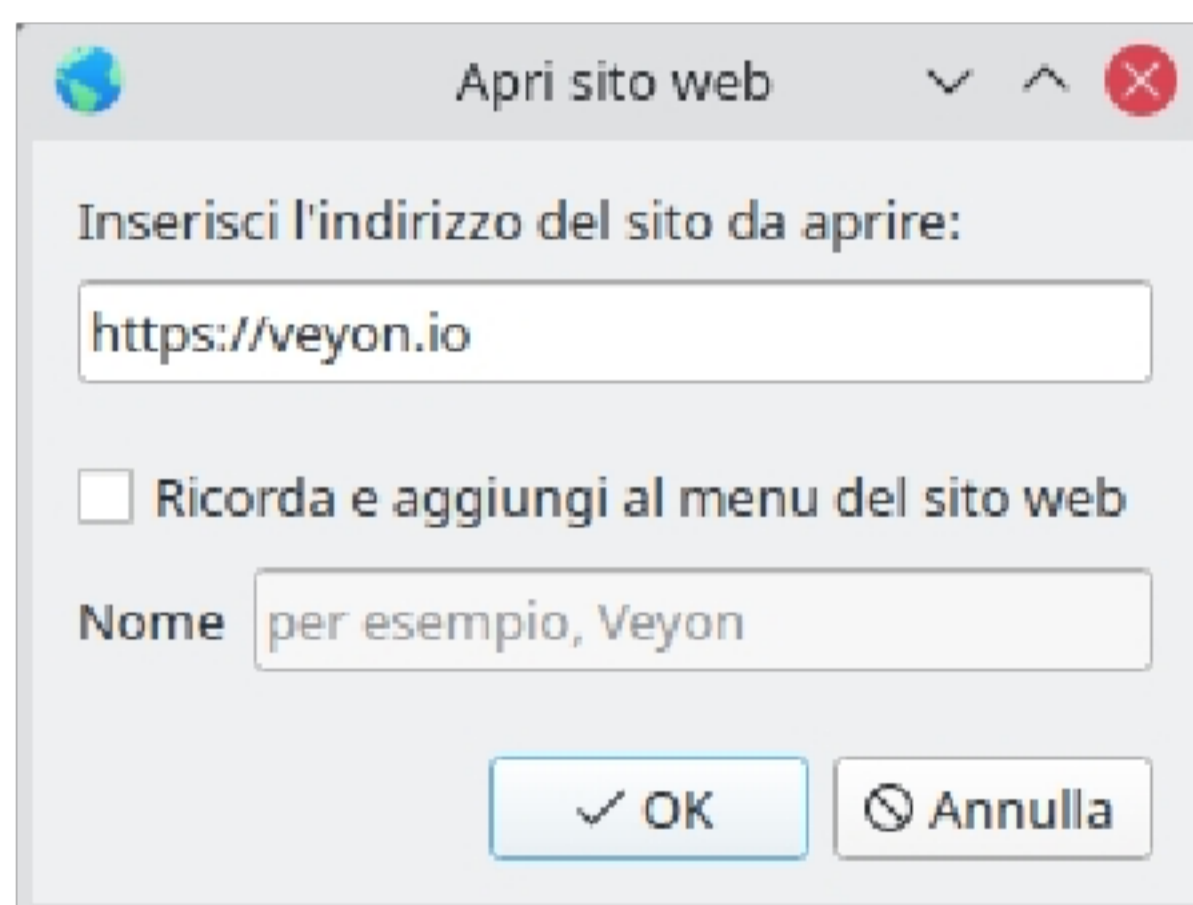
If you want all students to open a specific Web site, you can automatically open that Web site on all computers. Use the *Open Web Site* button to do this:



Depending on whether custom Web sites have been added previously or whether Web sites have been predefined by the administrator, a pop-up menu or a dialog box is displayed. In the former case, all available Web sites are listed in the menu:



Click the desired item to open the respective Web site on all computers. Alternatively, click on the last *Custom Web Site* item to open an unlisted Web site. This will open a new dialog box. In this dialog box you can enter the address of the Web site to be opened:

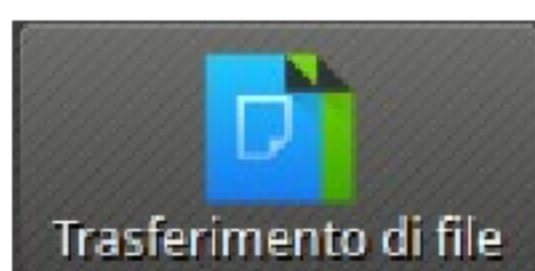


Confirm this dialog box with *OK* to open the Web site.

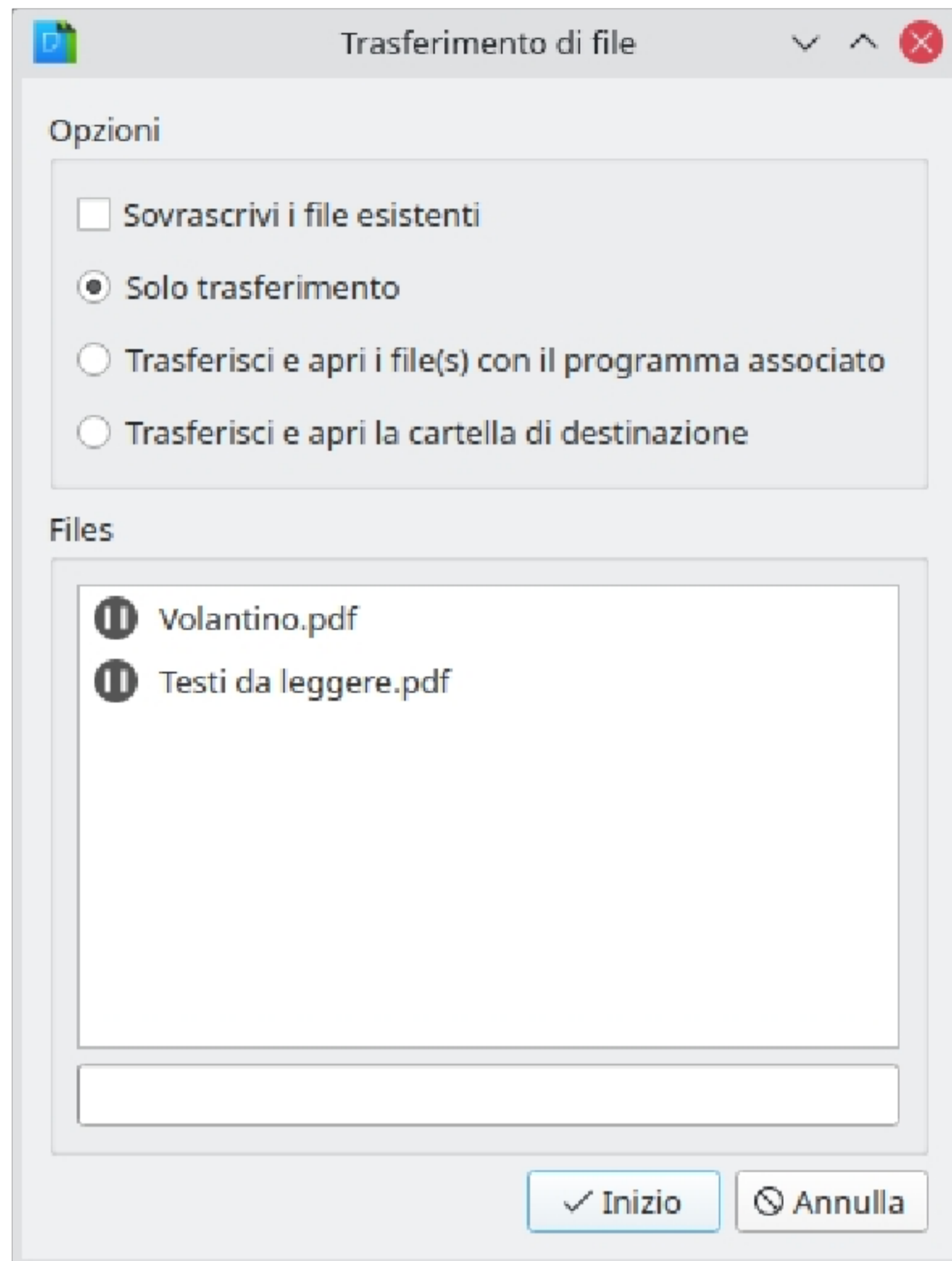
Note: To remove a previously added custom Web site, move the mouse over the corresponding item and press the *Del* key .

9.2.12 File Transfer

Using the file transfer function you can easily transfer files to all students and, successively, open the transferred files. First click on the *File Transfer* button to open a dialog box that allows you to select the files to be transferred:



After selecting the desired files, the file transfer dialog box opens:



In this dialog box you can choose additional options before starting the file transfer. By default, only files will be transferred to the user's home or profile directory without overwriting existing files.

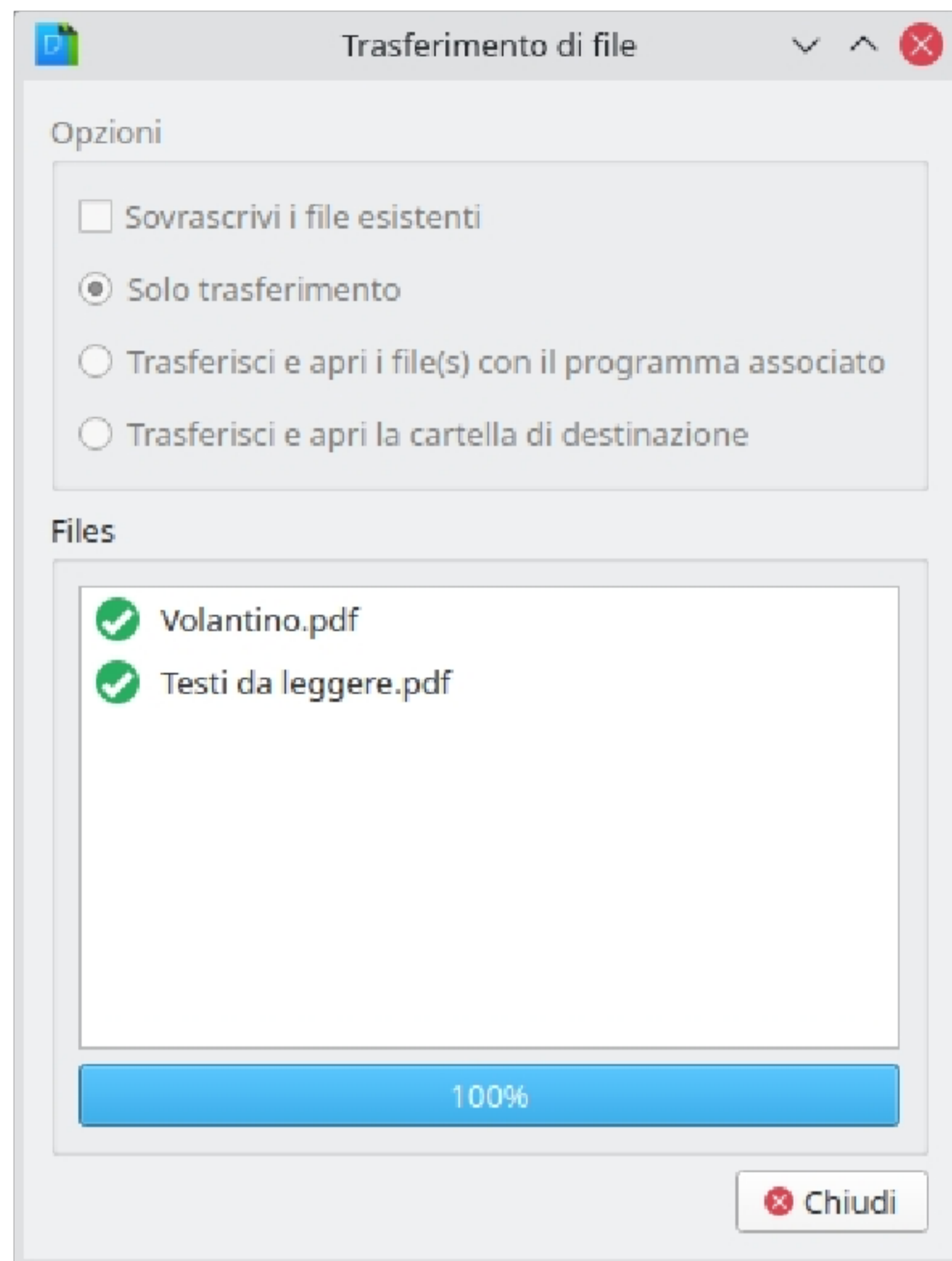
Overwrite existing files In this dialog box you can select additional options before starting the file transfer. By default, only files will be transferred to the user's home or profile directory without overwriting existing files.

Transfer only In this mode, only files are transferred without performing any further actions. Use this mode to silently distribute teaching materials in advance without disturbing students.

Transfer and open file(s) with associated program In this mode, transferred files will be opened with the corresponding program associated with the respective file type. For example, text documents will be opened with the installed word processing program. Use this mode to have students work immediately with the materials provided.

Transfer and open the destination folder If you intend to transfer several files at once, opening them all automatically is not a good choice in most cases. Instead, the destination folder can be opened in a file management window where students can view the transferred files and open the desired ones themselves.

After choosing the desired options click the *Start* button to start the file transfer. Depending on the size of the files and the number of computers, this may take some time. A progress bar with the total progress is displayed at the bottom of the dialog box. After the transfers are completed, you can click the *Close* button to finish:



9.2.13 Screenshot

Veyon allows you to save the current screen contents of individual or all computers in screenshot files. Clicking the *Screenshot* button activates the function for all displayed computers:



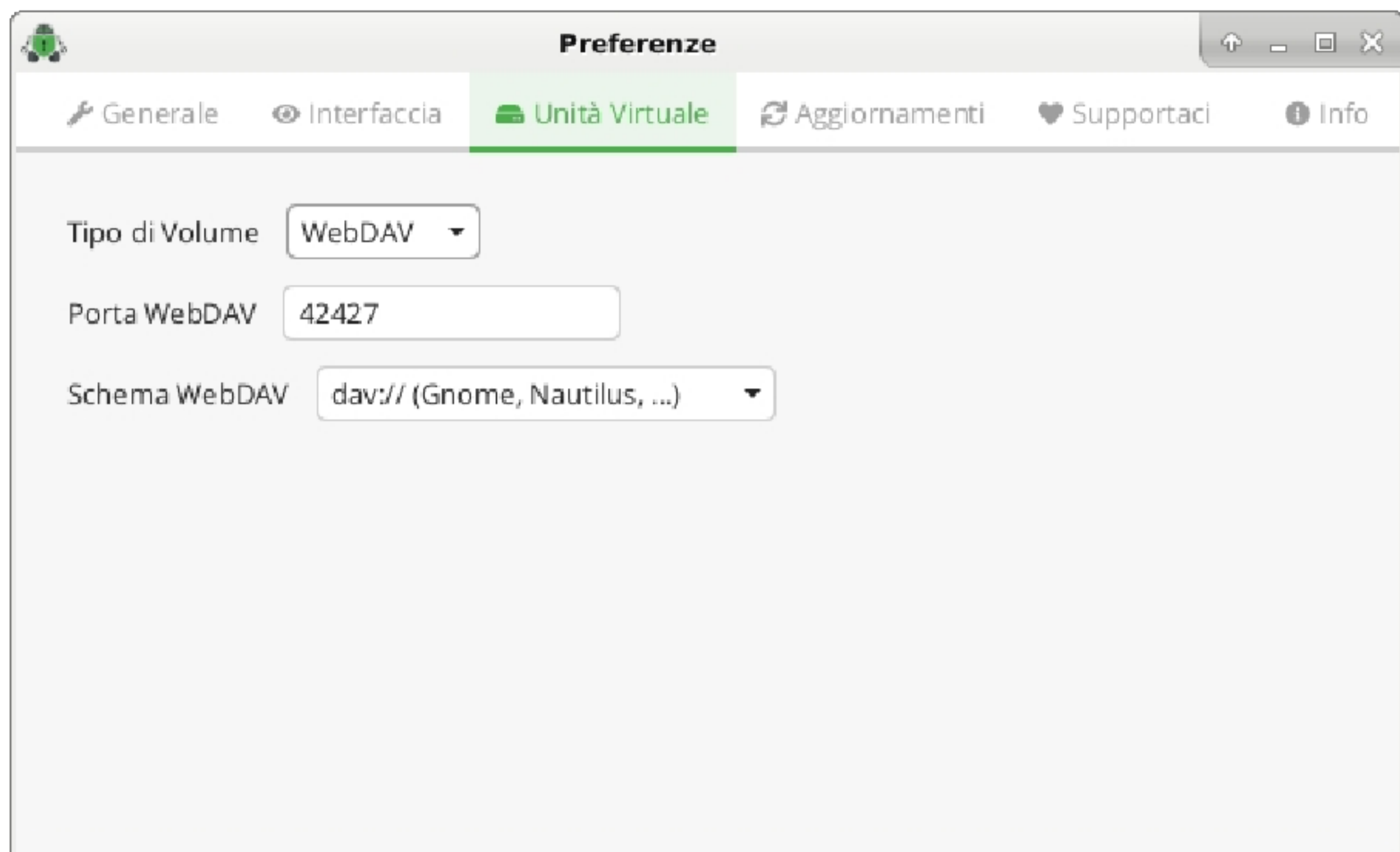
If you want to use this function only for individual computers, you can select the respective computers and select the *Screenshot* item from the context menu.

You will then receive an informational message about how many screenshots have been captured. You can now view the *screenshots* in the *Screen Capture* panel and delete them if they are not needed.

10.1 Foreword

Cryptomator is an application that allows you to encrypt your data quickly and easily, so you can securely upload it to an external device such as a USB stick or to your favorite cloud service. With Cryptomator you can create encrypted "safes". Each safe is password protected and can hold as many files and folders as you wish. For insights and details refer to the official site: <https://docs.cryptomator.org/en/latest/>. After a safe has been unlocked, it must be integrated into the system to be accessible to the user. Cryptomator uses three different technologies (called adapters) for this integration. To work properly on `Fuss 10` you must choose the `WebDAV` option (on `Fuss 11` you can also choose `FUSE`).

- 1) Click on the `Preferences` wheel in the initial window.
- 2) Click on `Virtual Drive`
- 3) Choose `WebDAV`; port and scheme are assigned by default.

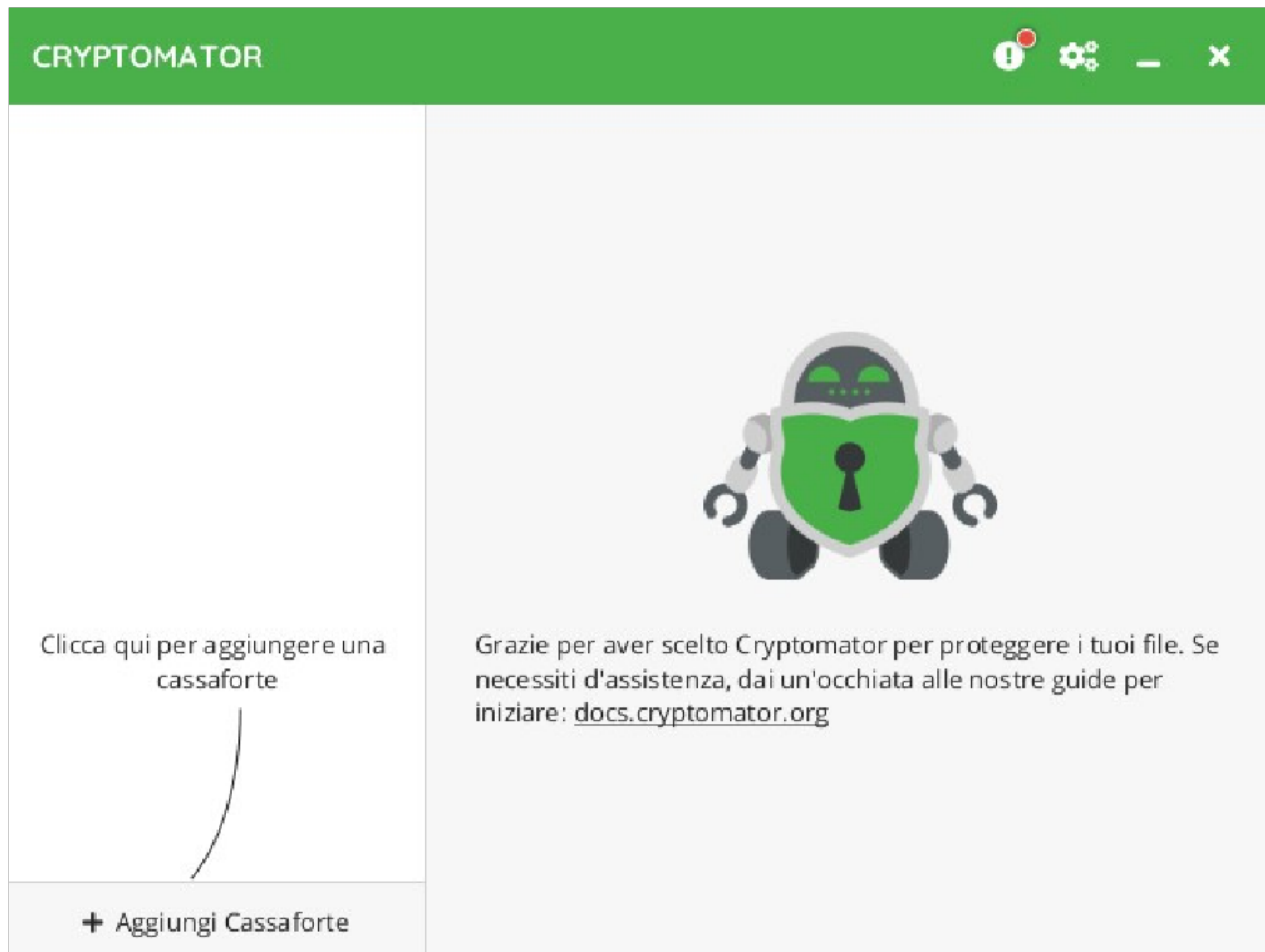


10.2 Starting and accessing the program

The program can be started from the start menu in the lower left corner.

When you first access Cryptomator, you obviously do not yet have a safe. start the application, the following screen will appear:

If you



By clicking on the **Add Safe** button in the lower left corner of the window, you can create a new safe.

10.3 Addition of safes



If you want to add a new safe, you have essentially two options:

1. If you want to create a safe yourself, choose `Create New Safe`
2. If you already have a safe, for example because someone has shared it with you through a cloud storage service, you can instead choose `Open Existing Safe`.

10.3.1 Create a new safe

If you have chosen to create a new safe, the wizard will walk you through the creation process:

- choose a name
- choose a storage location (local, on an external device such as a USB stick, or in the cloud)

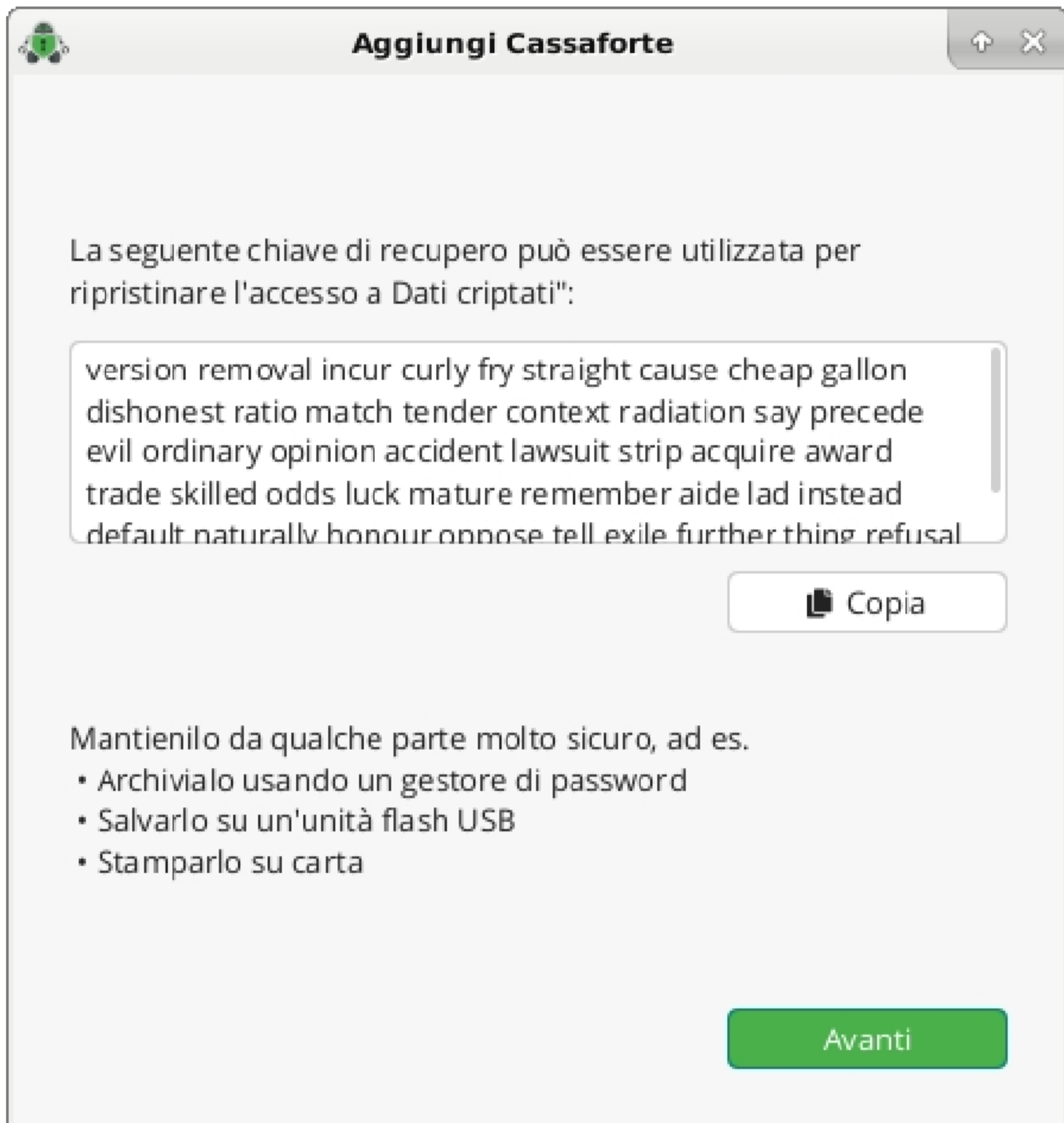
- choose a password (not to be forgotten, for safety you may decide to save a recovery key)

Warning: No one but yourself knows this password, and no one can "reset" your password for you.

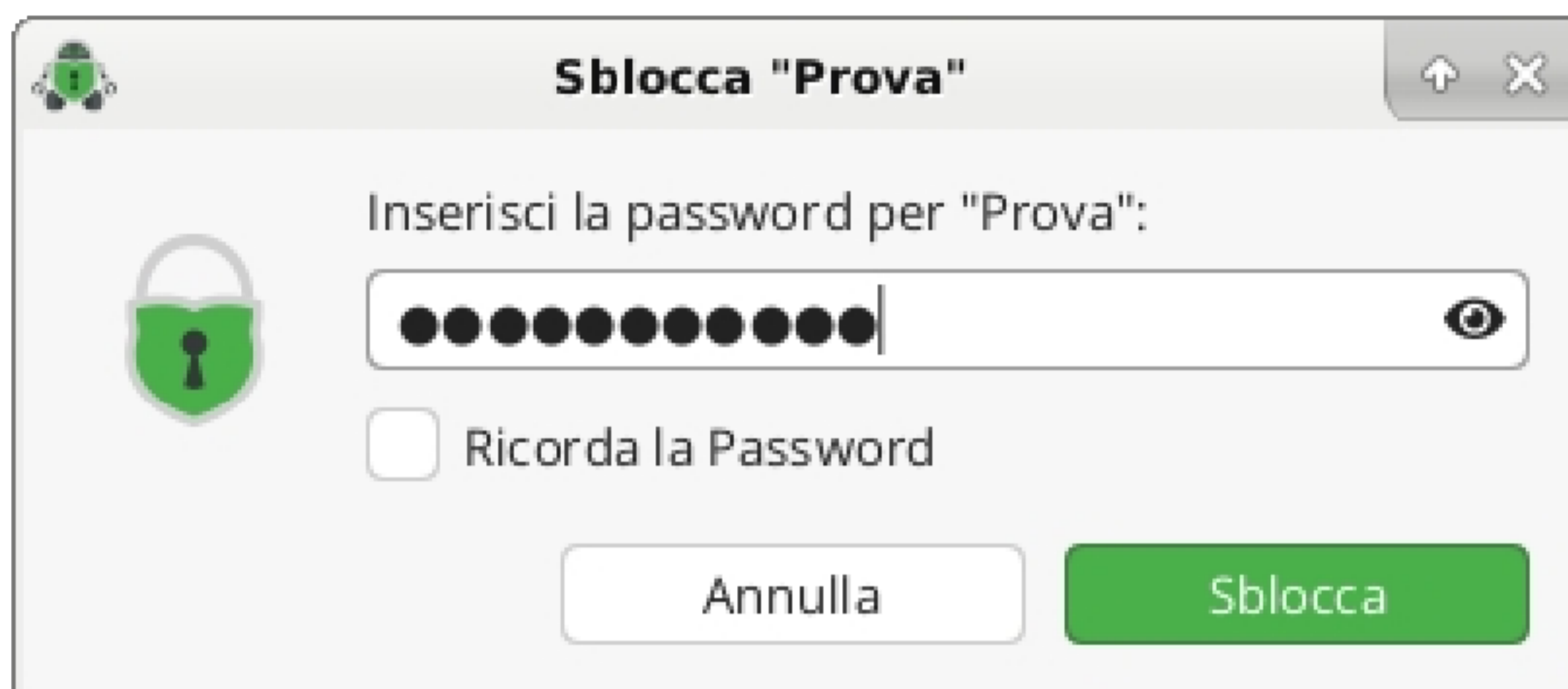
Note: If you plan to share this safe with another person, you will both need to know the password. In this case, choose a different password than the one you tend to use only for yourself. To share the password, use an encrypted message or any other secure means of communication. Since you cannot reset your password in case you forget it, we recommend that you create an additional reset key .

- Show recovery key (optional step)

If you chose to create a recovery key in the previous step, it will now be displayed. Be sure not to lose it and store it carefully.



That's it. You have successfully created a new safe. Now you can unlock it using your password and start adding confidential files.



10.3.2 Opening an existing safe

If you chose to open an existing safe, all you have to do is locate the file `masterkey.cryptomator` of the safe you wish to open.

Note: If you have created the repository on another device and cannot find it or its master key file, make sure the directory containing the repository is properly synchronized and fully accessible on your device.

10.4 Access to Safes

After adding a safe to Cryptomator, you will probably want to unlock it so you can start adding files.

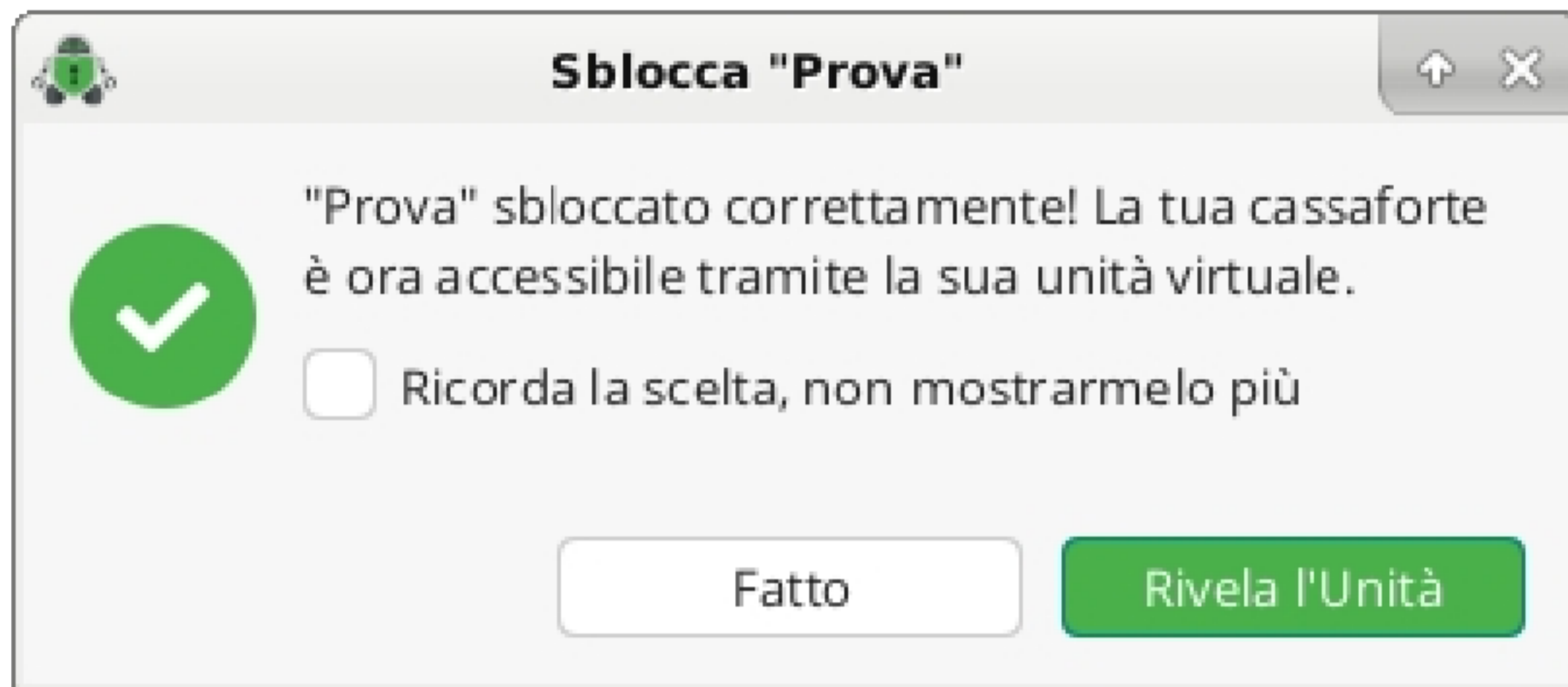
10.4.1 Unlocking a safe

To unlock the selected safe, click the `Unlock` button in the center of the Cryptomator window. You will then be prompted for the password:

Note: Selecting the "Save Password" checkbox will store the password in your operating system's keychain.

Warning: Store your password only on trusted devices. Anyone with access to this computer will be able to access your safe if the password is stored in the system key fob.

A confirmation is displayed if the password is correct. You can simply close this window by clicking `Done` or by clicking `Reveal Drive` to show the unlocked safe in your file manager.



10.4.2 Working with the safe unlocked

After unlocking, the contents of your safe will be available as a virtual drive on your PC. This means that you can interact with your safe files in the same way as any other hard drive or USB stick. If you cannot find the unlocked safe in your system's file manager (File Manager, Windows Explorer, . . .), you can always click `Reveal Drive` in the Cryptomator window.

10.4.3 Locking a safe

To lock your vault again, simply click `Lock` and your data will be protected and encrypted again.

10.5 Changing the password

You can change the password of an existing safe. The only thing you need is to remember the current one.

Note: When you change the password, the keys encrypted the first time will remain the same. The actual files will not be re-encrypted. If you wish to encrypt the files in your safe with a new stronger password, you must create a new safe and drag and drop the data from the old to the new.

To do this, click the `Change Password` button on the `Password` tab of the `Safe Options`. Three text entry fields are displayed in the opened window:

1. In the first you need to enter the current password.
2. The second takes the new password and, as mentioned above, we suggest following the rules of creating good passwords.
3. In the third, it is necessary to enter the new password again for confirmation.



Modifica la Password

Inserisci la password corrente per "Dati criptati"

Inserisci una nuova password

Usa almeno 8 caratteri

Conferma la nuova password

☐ Capisco che non potrò accedere ai miei dati se dimentico la mia password

Annulla Modifica

To proceed you must confirm what you are doing by checking the check box. To finish and actually change the password, click the `Edit` button.

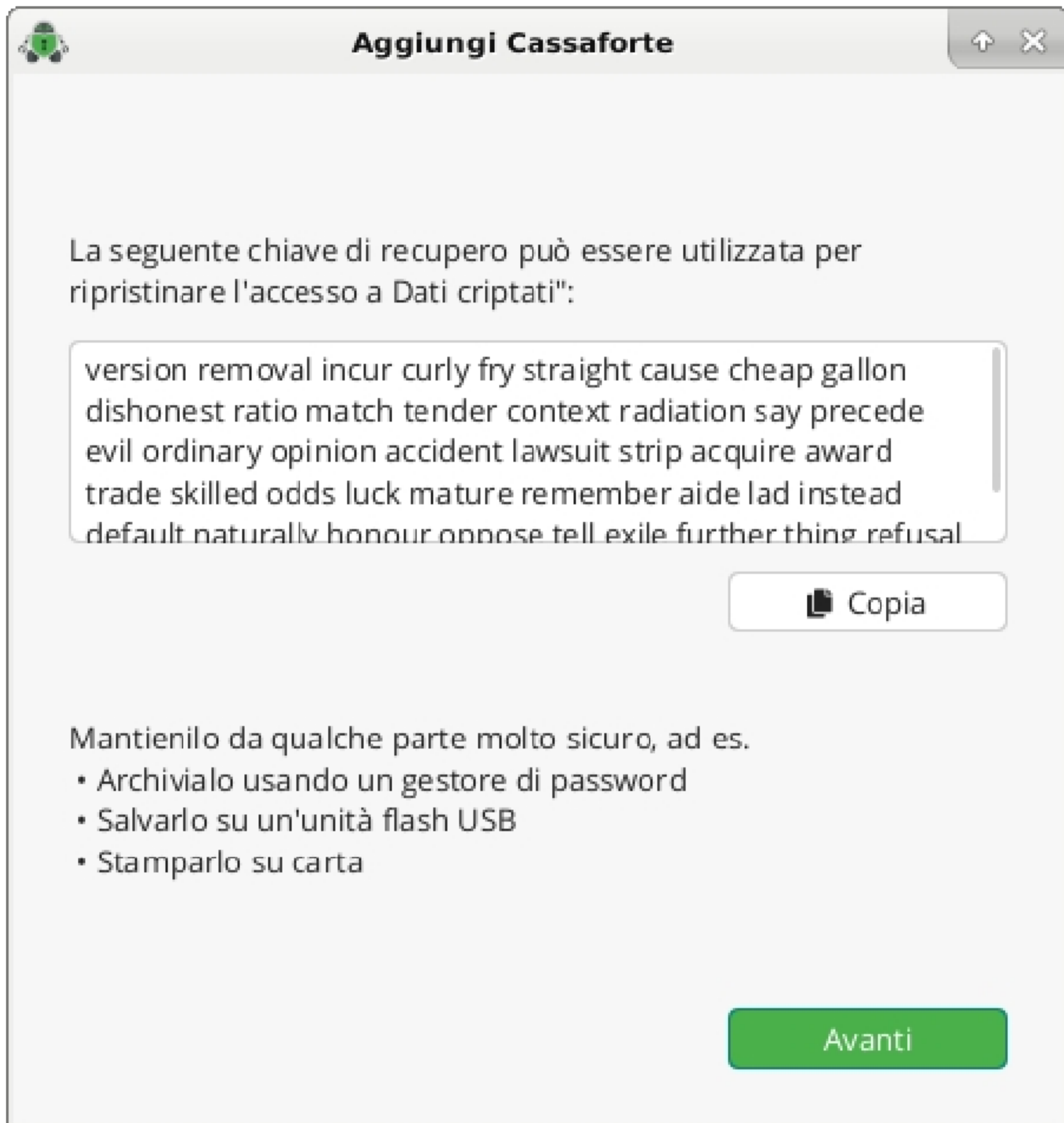
Note: Only if the second and third text entry fields match and the check box is selected, the `Edit` button is enabled.

10.6 Reset key

10.6.1 Show the recovery key

It is not a problem if you lost the display of the recovery key during the creation of the safe. You can still derive it and display it later. To increase security, Cryptomator does not store it on the hard drive and always obtains it "on the fly." .. attention:: Keep in mind that because of the reset key's ability to reset the current password, it is highly confidential. Make sure that only trusted people have access to it and keep it in a safe place.

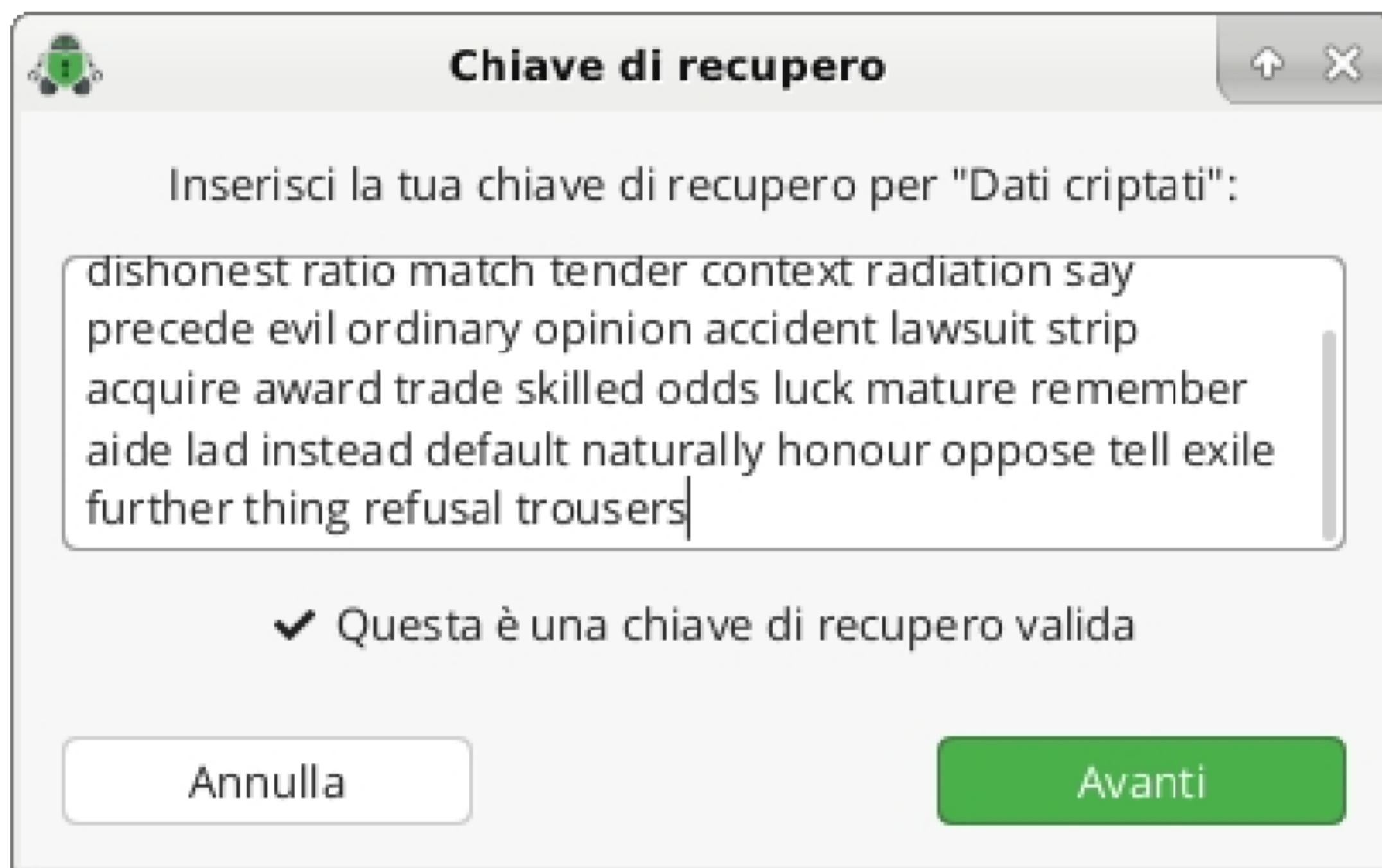
To do this, click `View Recovery Key` on the `Password` tab of `Safe Options` and enter your password. A new window will open. It shows a sequence of words within a text field. This sequence is the safe's recovery key.



You can copy it to the clipboard or print it on paper. If you are finished, close the window with the `Done` button.

10.6.2 Resetting the password with the reset key

If you have forgotten the password for a safe, but have saved the recovery key in an external location, you can create a new password and access the safe again. Switch to `Password` on the tab in the `Safe Options` and click the `Recover Password` button. A new window will open asking you to enter the recovery key in the text box shown. Enter it there by copying it from a file or typing.



Note: If you have printed your recovery key on paper or stored it somewhere where you can't copy it, Cryptomator offers an auto-complete function for entry. Type in a letter and see if the word shown matches your key part. If it does, you can press the Tab key or the right arrow key to autocomplete the word. If not, enter more letters and the suggestion will change accordingly.

If the recovery key is valid, Cryptomator signals this with a small message and activates the `Next` button.

In the last step you must assign a new password to your safe. This is the same procedure followed when creating the safe, except that no new reset key is generated. It is recommended that you follow the tips on creating a good password.

Finish the dialog box by entering the same password again and clicking the `Done` button. You can now unlock the safe with the new password.

Note: Since the recovery key remains the same, do not discard it and store it in a safe place.

10.7 Removing safes

You can remove a safe from the list by right-clicking on the list item. This is only possible while the safe is locked.

Note: Removing a safe from this directory does not delete it from the filesystem. To irrevocably delete the safe, you can simply delete the safe's directory (which contains your `masterkey.cryptomator` and the `d` folder) using your regular `File manager`.

CHAPTER 11

Contribute

Anyone can help improve this documentation that is written in [reStructuredText](#).

CHAPTER 12

Support

If you need help, email info@fuss.bz.it

CHAPTER 13

Licenses

code GPLv3

documentation CC BY-SA

- [genindex](#)

A

Addition of safes, 60
Starting from menu, 39, 58

B

Browser, 53

C

Commands, 52
Computer overview, 46
Computer select panel, 42

D

Demo mode, 46
Demonstration, 46
Demonstration mode, 46
Destination folder, 54
Distribute files, 54

E

End of lesson, 50
Execute program, 52

F

File transfer, 54
Files, 54
Fullscreen demo, 46

L

Lock computers, 47
Lock input devices,
47 Lock screen, 47
Log in, 50
Log off, 50
Log off users, 50
Log on, 50
Log out, 50
Login, 39, 50
Logon, 50

M

Message, 51
Message window, 51

Monitor view, 41
Monitoring, 46
Monitoring mode, 46

O

Observation, 46
Open browser, 53
Open document, 52
Open files, 54
Open website, 53

P

Password, 39
Power down, 49
Power on, 49
Presentation, 46

R

Reboot, 49
Remote access, 48
Remote control, 48
Remote view, 48
Restart, 49
Run program, 52

S

Screen broadcast, 46
Screen lock, 47
Screenshots, 56
Screenshots panel, 43
Send files, 54
Shutdown, 49
Snapshot, 56
Start program, 52
Status bar, 41
Switch on, 49

T

Text message, 51
Toolbar, 41
Transfer files, 54
Turn off, 49
Turn on, 49

U

URL, [53](#)

User interface, [41](#)

User log out, [50](#)

Username, [39](#)

W

Wake-on-LAN, [49](#)

Web address, [53](#)

Website, [53](#)

Window demo, [46](#)

WoL, [49](#)