CAM-Pro Security

Radonix

Headquarters

Iran
Radnik Automation Company

Unit 2, Tatis Building, No. 4, Suhend Alley, Laleh Square, 7th East Boustan, Laleh Boulevard, Marzdaran Boulevard, Tehran
Telephone: +98-21-46112012-4 | Postal Code: 1461844843 | SMS gateway number: +98-9351983070

Türkiye
Armeh Mühendislik Sanayı Ve Ticaret Limited Şirketi

HUZUR MAH. AZERBAYCAN CAD. SKYLAND B NO: 4 B Sarıyer / İstanbul
Telefon: +90 553 920 5500

Introduction

The Radonix controller incorporates this advanced security feature, which allows manufacturers to define specific time periods during which the CNC machine can be operated.(time-based lock)
Or setting Password ensures that unauthorized users cannot access or manipulate the machine without the permission of the manufacturer. The Radonix controller offers a robust and reliable security solution for CNC manufacturers.

A maximum of 24 timer locks can be defined on the controller, and each password must be 8 letters or English numbers in length and can include a mix of uppercase and lowercase letters. The dates for the timer locks can be based on the month of the year, and the structure must match the structure specified by the software when the timer locks are defined.

1- Time-Based Locks

To set up time-based locks on the CNC controller, you need to establish a connection between the controller and the computer, ensuring they can communicate with each other. The controller must be online, and the activation code for the controller must be entered and validated. If all conditions are met, the Update button in the Internal Clock section will become active, allowing you to update the time and date on the controller. This process is illustrated in Figure (1).
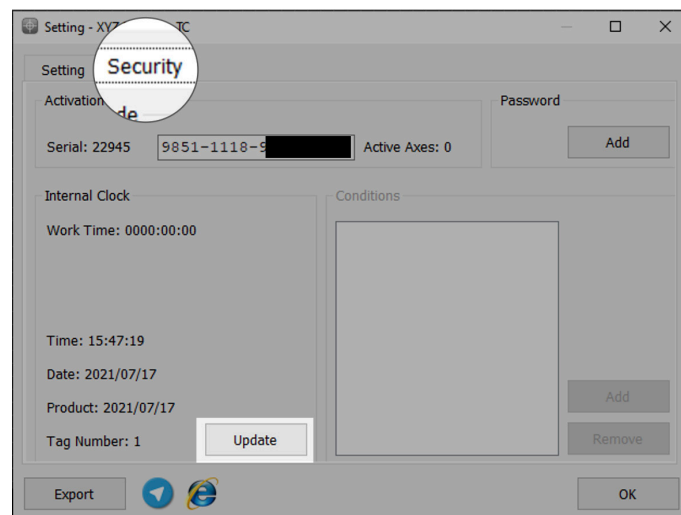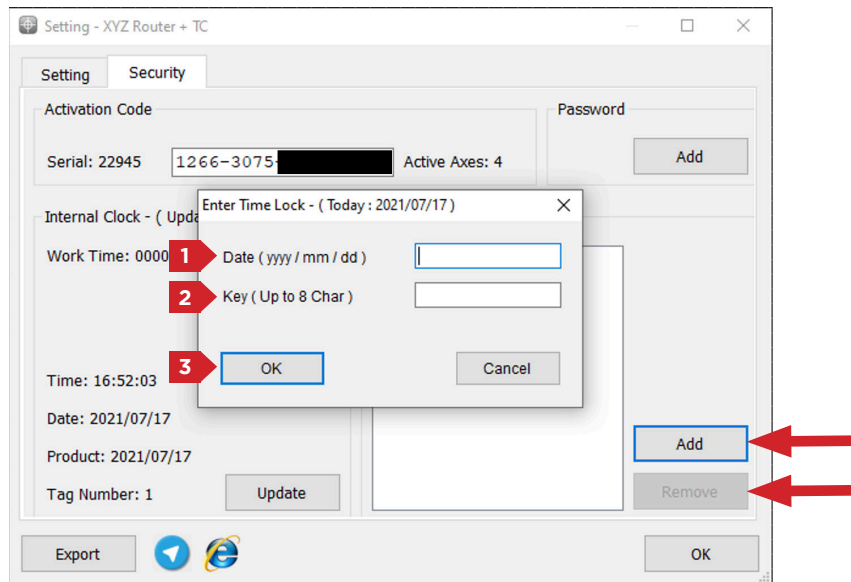

Figure(1)

> • If the controller is updated with an incorrect time, it may cause the time-based locks to malfunction. Therefore, double-check the computer's time and date before updating the controller's internal clock.
> • If a lock is already set on the controller, the Update button will not be activated. To update the internal clock, all previously defined time-based locks must be removed first.

Defining Time-Based Locks

In the Conditions section, there are two buttons: "Add" and "Remove," used for defining and removing locks, respectively. The manufacturer can define up to 24 locks or remove them as needed. Pressing the "Add" button opens a lock definition window, allowing the user to set up the lock. The lock must be defined in a specific structure, with the start date entered first, followed by the desired password, which can have a length of up to 8 characters. To remove a lock, the password is required; if the password is unknown or forgotten, the lock cannot be deleted. Refer to Figure 2 for details.

Figure(2)

- When the lock date arrives or has passed, the device will stop until the correct password is entered. The user will receive a "Condition Key" warning and be prompted to input the password for that lock. If the correct password is entered, the device resumes normal operation. However, if the user does not have or has forgotten the password, the device cannot be operated.
- If the lock date arrives during a project's execution, the lock warning will not appear immediately. Instead, the warning will appear the next time a command is executed by the user.
- The time-based lock affects only the program execution command, while other commands such as manual commands, input, and output remain active. Pay careful attention to the password's capitalization when defining the locks and securely store the passwords. Incorrect or forgotten passwords cannot be deleted. The only possible solution in such cases is to erase the controller's memory, a service provided by its manufacturer.
- Time-based locks serve as a security measure to ensure the financial settlement of the manufactured device. Intentionally tampering with the controller's clock function can result in the controller's disabling.
- Follow the manufacturer's guidelines and refrain from making unauthorized changes to the controller's clock settings.
- Store the passwords in a safe place, as forgetting the passwords may prevent the locks from being deleted. The list of entered locks can only be viewed with the controller clock's activation code, provided by the manufacturer.
- Device manufacturers ensure that buyers can remove the time-based locks without the coordination of the controller manufacturer. This is achieved by recording the original purchaser of the controller in the controller manufacturer's company documents. The controller manufacturer will not update, clear memory, or reprogram the controller without the coordination of the original purchaser, as recorded in their company documents. This ensures that buyers have the necessary information and access to remove the time-based locks if needed.
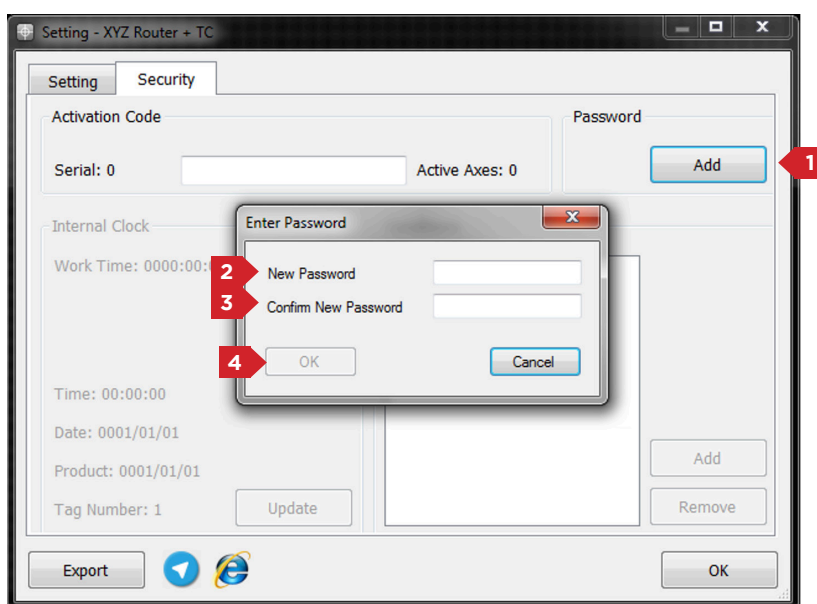
2- Password

To preserve the basic settings of the device and prevent unwanted changes by non-experts, you can define an 8-character password including numbers, letters, and symbols with case sensitivity on the interface. This password restricts the ability to change settings related to the device's essential variables and only allows changes to general settings without it.

The password is transferred by the backup settings version, so if a backup settings version is installed on another computer, changing the settings requires knowing that password.

- To define a password, first use the Add button in the Password section of the Security tab in the Settings window. Then, enter your desired password twice (step two) and finally click the OK button.
- To define, change, or delete a password, use the "Change" button in the "Security" tab of the "Setting" window in the "Password" section (Figure 3). To change or delete the password, it is necessary to know the previous password. To delete the password, after entering the previous password, leave the new password field empty and confirm the password. Keep in mind that space or empty space is also considered a character.

The settings password is not registered on the hardware; therefore, it does not have the security of time-based locks.

Figure(3) - Adding password
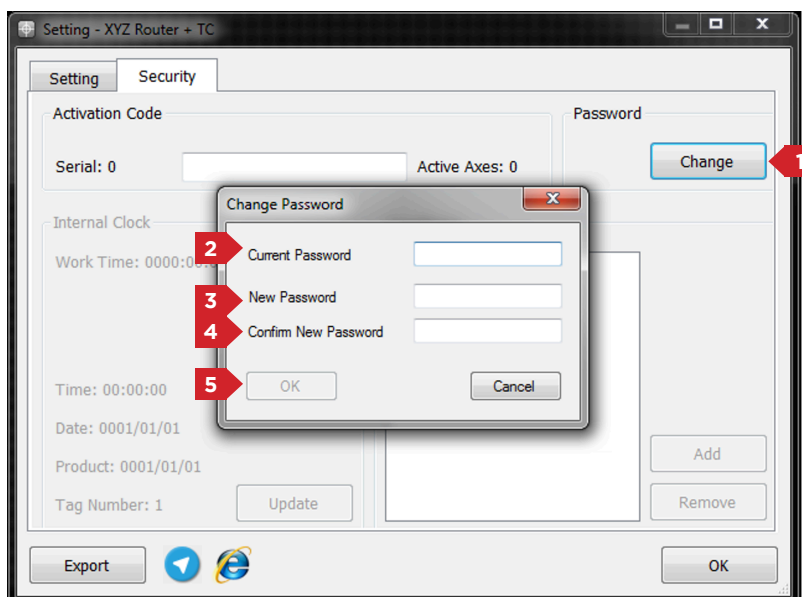
Figure(4) - Change or delete password

Work time

The controller's operation time is displayed by the Work option in the Security tab of the Settings window when the controller and interface are connected.
The controller being powered on or online is not a condition for registering the operation time.
This time only includes instances when a program is being executed.