



RDCAM Software Encryption Function Manual

Notice: The actual mode of operation and feature setting are inconsistent with this manual which caused by the software upgrade. Please refer to software.

Click [File] -> [Password Setting].



If the system is unencrypted, "Unlock entry" button will be in prohibited use state. Input the vendor password at "Vendor right", and then click "Enter" button to enter the password management interface.



If the system is unencrypted, the "Unlock mainboard" button is in prohibited use state.

1. : Vendor password settings

The RDCAM software can distinguish the ordinary user from facility manufacturer according to the "Vendor Password ". Therefore, when you know the factory password is considered to the equipment manufacturer and with full permission of RDCAM software, which might contains some parts manufacturers do not want the end-user to modify (such as setting the period of encryption, manufacturers can directly unlock the encryption).

Manufacturers need to modify the default vendor password on the mainboard to the

exclusive manufacturer password.

Note: RDCAM software defaults vendor password is RD8888.

Click "Vendor Password "to enter the interface of updating factory password settings.

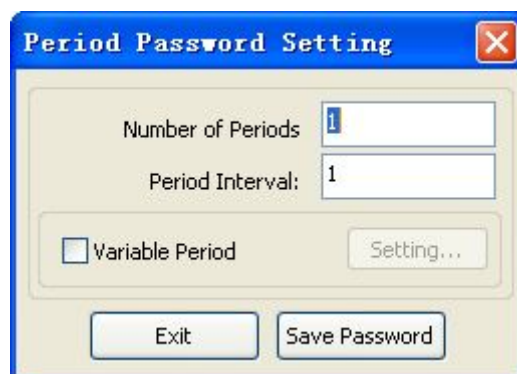


A dialog box titled "Vendor Password Set..." with a close button (X) in the top right corner. Inside the dialog, there is a note that says "Note: Password be". Below the note, there are three text input fields labeled "Old Password:", "New Password:", and "Confirm Password:". To the right of the "Confirm Password:" field is a "Modify" button. At the bottom center of the dialog is a "Quit" button.

Enter the old password, the new password and re-enter the new password at the "Confirm Password", then click the "Modify" button to complete the vendor password settings.

2. Period password settings

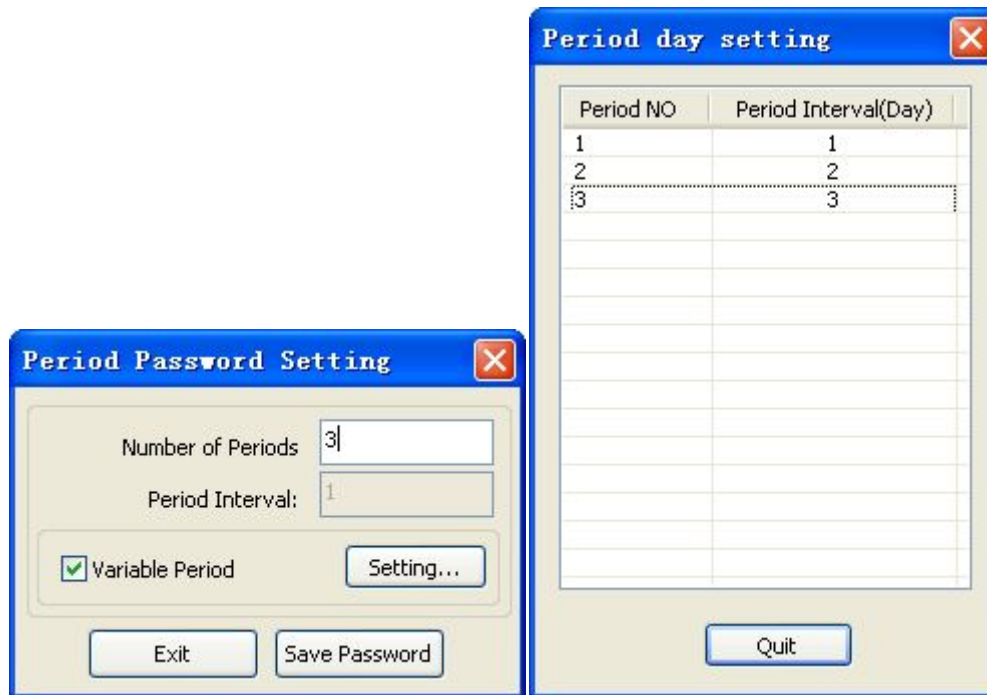
Click "Period password" button to enter the interface of "period password setting".



A dialog box titled "Period Password Setting" with a close button (X) in the top right corner. Inside the dialog, there are two text input fields: "Number of Periods" with the value "1" and "Period Interval:" with the value "1". Below these fields is a checkbox labeled "Variable Period" which is currently unchecked. To the right of the checkbox is a "Setting..." button. At the bottom of the dialog are two buttons: "Exit" and "Save Password".

The period password function can be used for use management, such as installment, product on trial, the distributor payment and so on. It can be at most used for 20 encrypted phases. Generally, the limit days of single-use are less than 200 days. When expiration, the controller will lock the machine automatically, user cannot use the machine for processing normally.

The single encryption days can be set the same days or set the days respectively.



Set up the encrypted information, click "Save Password" button, select the save path of the password file and save it.



Main board encrypted successfully, the software will remind that password is set up successfully.



Open the password file that you will see each phase of encryption.

1: represents on which phase, the following password represents the password on this phase. The figures behind the password are the encryption days.

The following information is the second and the third encrypted information.

The last password is to cancel password.

The Cancel password is a total control password. Such as installment, assume that the user in three phases payment, but the user pay in full, so to use to the cancel password to cancel all encryption.

Manufacturers need to take good care of password file.

3. Decryption

User can decrypt the password at any time when main board is encrypted. In multi-encryption phases, if you decrypt the current phase, it will automatically entry into the next phase encryption process from the current. In other words, the current decryption time is the beginning time of the next phase.

Click [File] -> [Password setting].



Click the "Unlock entry", pop up the dialog box and input the password of the current period, and click "Verification" button.

"Password (NO.1)" asked to enter the first phase password.

User can enter the first phase password to remove it, and also can directly input the cancel password to cancel all encryptions.



If the operator is a manufacturer, the manufacturer can input the vendor password in "Password Management" dialog box, and click the "Unlock mainboard" to cancel all encryptions.



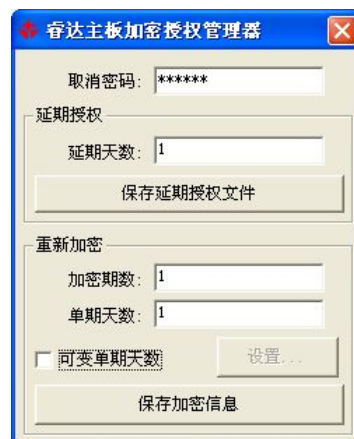
4. Extension

In some special cases, it may be need an extension. Such as the machine encryption has expired, but due to some special reasons to request an extension payment. Manufacturers can make an extension file to set up the extension days as the negotiated.

The extension files can be created by small software "RuiDa Mainboard Encryption Authorization Manager". There is no requirement to connect mainboard when the software is working which can do on any computer. For the manufacturers' safety consideration, recommended that the person who is especially responsible for the management when use this software.

Whether it is an extension or re-encryption, both need to input the cancel password. The Cancel Password is the last password of the saved password file.

The Cancel Password is created randomly, so you can think that the cancel password is one-to-one correspondence to the mainboard.



Input "Cancel password" and "Extended Days", then click "save the authorized extension documents" to save the extension file. The manufacturer can send it to the user when created and loaded by the user.

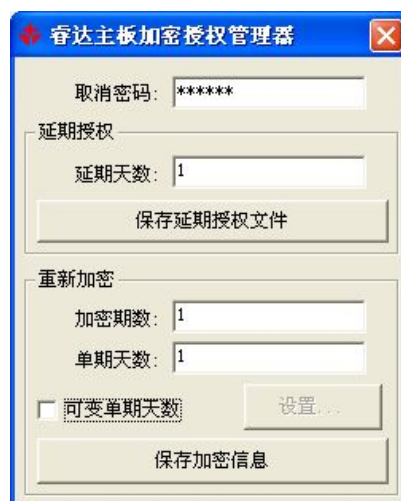


The extended operation is limit. Each encryption can be extended 5 times.

The extension files just can be used for one time. If user needs a further extension, the extension file must be recreated.

5. Re-encryption

In practical applications which needs re-encryption, such as uncertain payment in advance or payments changed. The manufacturer does not need to re-encrypt on site, only need to create the authorization documents and then the user to load it.



Re-encryption process is exactly the same as the encryption process, but only need to input the cancel password and no need to connect the control card.

Set "encryption phases" and "Single phase days", and click "Save encrypted information" button, then save the password file and the re-encrypted authorized files.

Notice: When confirmed the user loaded re-encrypted authorized files, the original

password file is invalid. Please keep the new password file and delete the original password file to avoid confusion.

6. Presentment for payment

RDCAM software supports displaying the payment presentment.

If the customer's equipment encryption will be expired, the software will display the user the remaining time and remind customer to pay on time when clicked "marking".

Presentment rules are as follows:

The remaining time is more than 4 days, no reminding.

The remaining time is more than one day but less than 4 days. The software will remind one time when continuously use.

The remaining time is less than 24 hours. The software will remind one time once press "marking" button and display the remaining time with hours.

Manufacturers can define the presentment payment content by themselves. A file called "tips" with RDCAM software's installer; manufacturers can open and edit it through Notepad. If the "tips" file uninstalled with RDCAM software, the default message is as follows:

Dear users:

Thank you for using our laser marking machine.

An installment may be close to expire, please pay in a timely manner.

We are very grateful for your support of our work!