Quick guide how to set up a Ricoh print device

Due to the implementation of EU´s Radio Equipment Directive **(RED)**, there have been several changes to the pre-configuration of some of the Ricoh printers and multi-functional products.

- Preprogrammed passwords from the factory are **not** allowed
- All protocols considered unsafe/unencrypted are turned **off**
- Device hard drive is encrypted.

Ricoh offers a pre-configuration service for customers who have entered into a special agreement. This allows the device to be delivered with customized settings aligned with the customer's IT environment and security policies.

Password setting

The first time you power on the device, you are forced to set an administrator password and a supervisor password.

Administrator 1 (Main Administrator)

- Permissions: Has access to all system functionalities and settings.
- Password setting: Set during the initial setup procedure.
- Restrictions: Cannot change the password of other administrators or the supervisor password.

Supervisor

- Access Rights:
  - Only users who can change or reset the password of Administrator(s).
  - Does not have access to the full functionality of the system itself.
- Password setting: Set during initial setup. Make sure this is stored securely.
- Forgot Password / Reset Process
  - If an administrator forgets the password, only the supervisor account can reset this password.
  - There is no automatic recovery option via email or security questions.

⚠ Important Note

Ricoh is not responsible for the management, loss or recovery of administrator or supervisor passwords. It is the responsibility of the customer/user to store these passwords securely and to treat them confidentially. If the supervisor password is lost, recovery can only take place through a full reinstallation of the device.

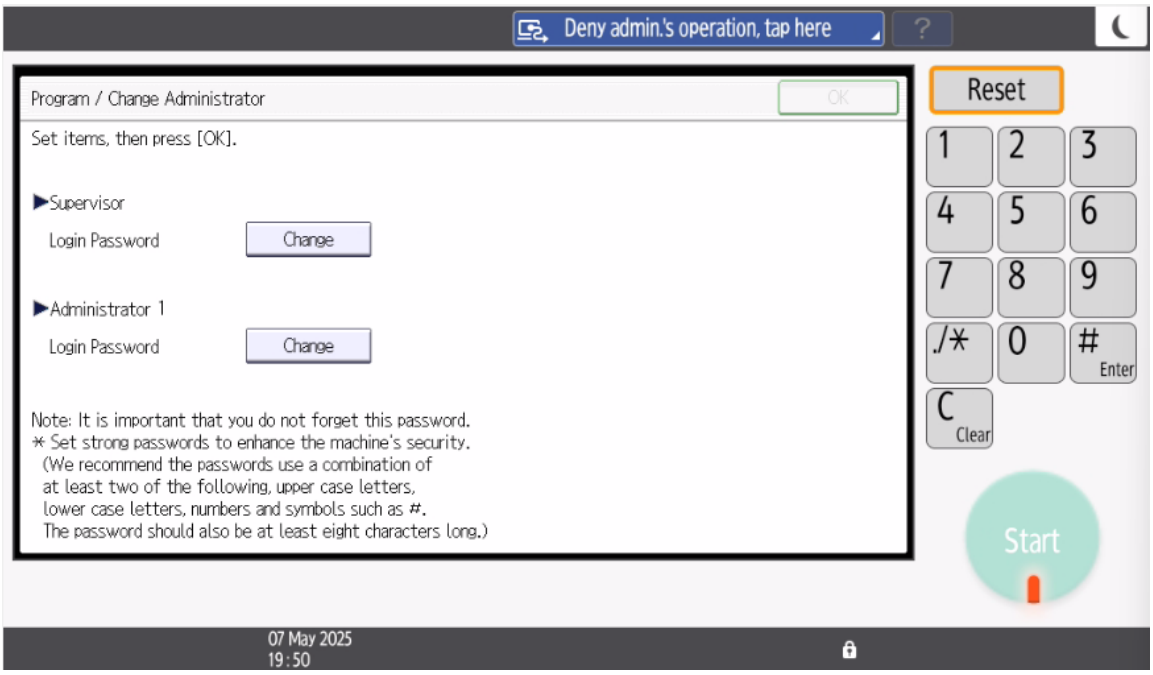
Initial Power ON

When you turn on the device for the first time, you will see this:

There are 2 different options, depending on the model, option 1 or 2 is used.

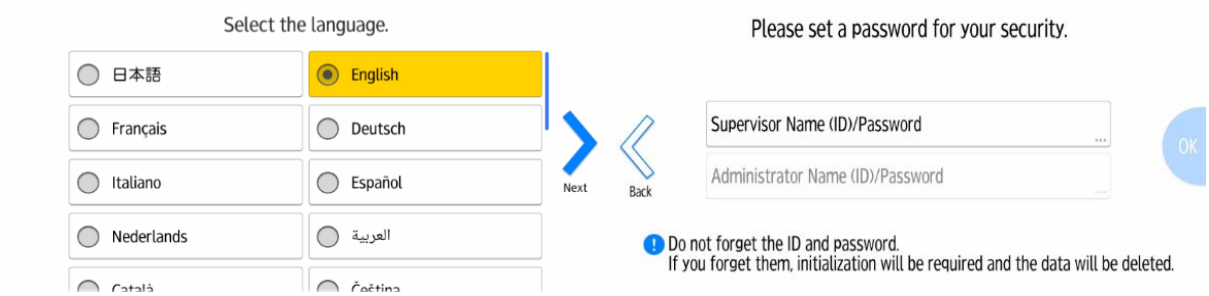
Option 1:

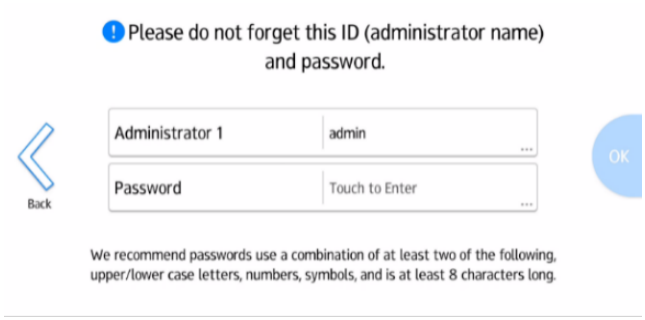
This screen cannot be closed without both passwords being programmed.



Option 2:

Select the language:

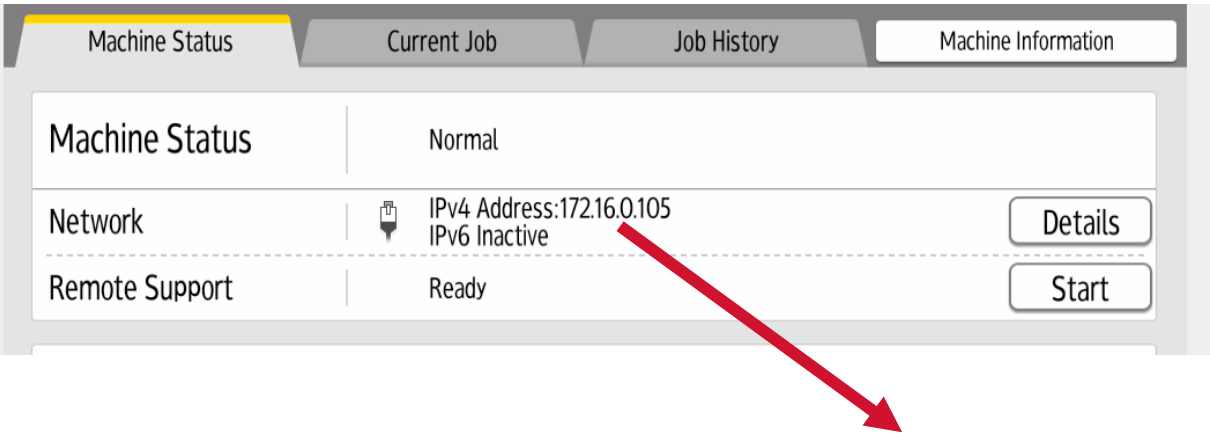



Please do not forget this ID (administrator name) and password.
Administrator 1
admin
Password
Touch to Enter
OK
Back
We recommend passwords use a combination of at least two of the following, upper/lower case letters, numbers, symbols, and is at least 8 characters long.

Network settings

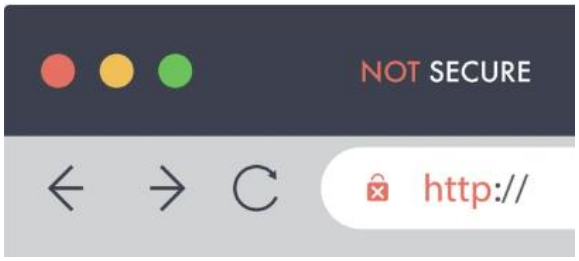
To use the device for printing like previous, some protocols have to be activated. The easiest way to do this is to configure this on the device web page.

Find the IPv4 address of the device:

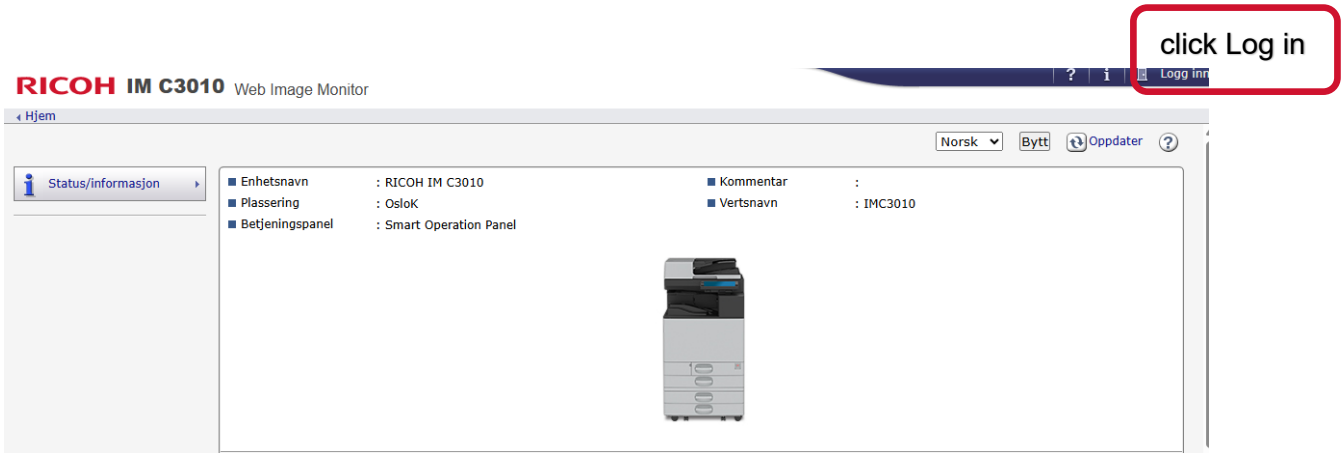


Open a web browser and type in the IPv4 address using https://172.16.0.105

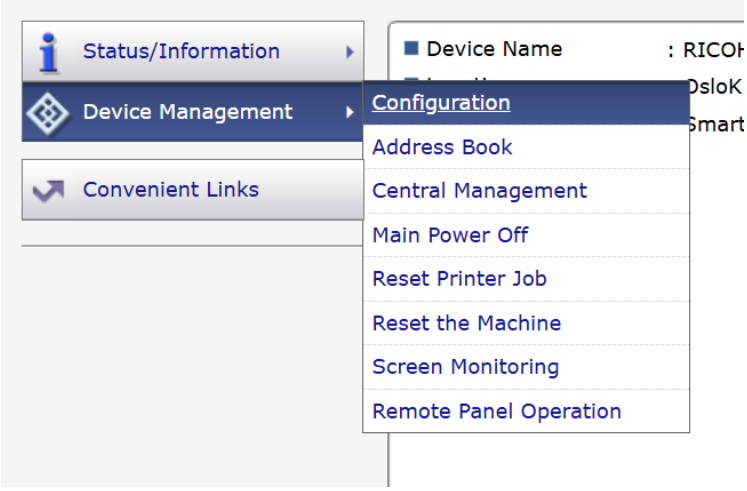
You might get a message in the browser about unsecure connection, but here you can click advanced and continue. This is due to the fact that the device has a self-signed certificate.



Log in with the administrator and password details you have set on the initial set-up



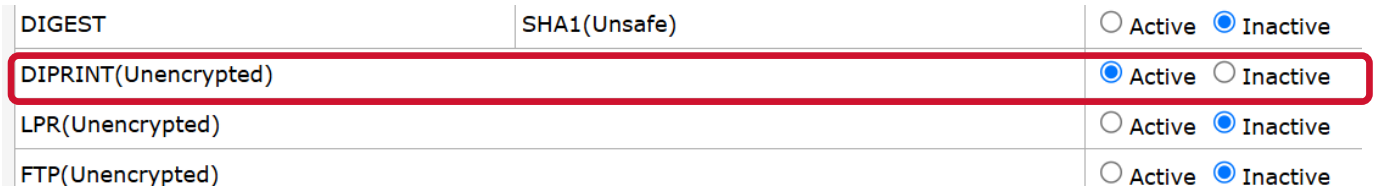
Device management - Configuration



Network security

⚠ Important Note
The following is what Ricoh suggest for network settings.
The setting may not comply with your network security, but they can be used in most cases.

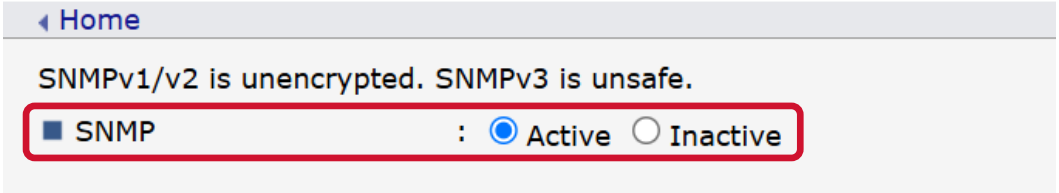
Set DIPRINT to active:

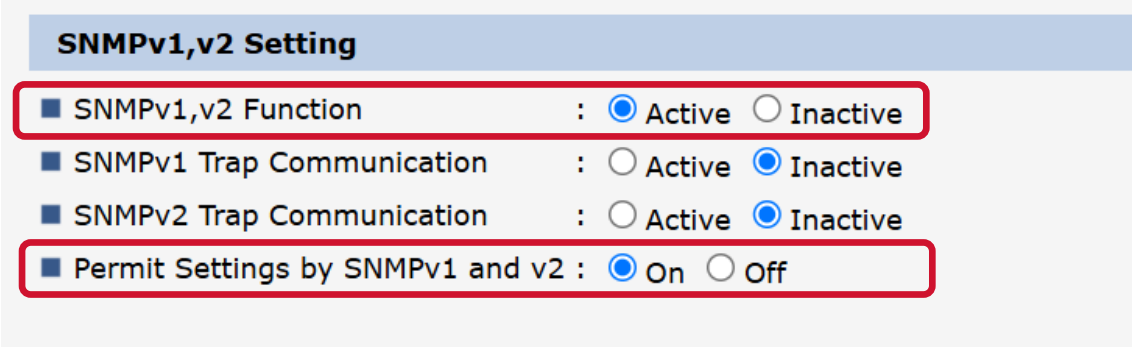


Setting DIPRINT protocol on for regular windows printing. Please note, DIPRINT protocol is **not** encrypted.

Enable SNMP

To get status in your windows print queue and status in your Ricoh universal printer driver, you need to turn SNMP V1 and 2 on.





SNMP V1, V2 is **not** encrypted communication. If this is required you need to set up SNMP V3 with the proper user account, password and encryption algorithms

With these settings you should be able to use your device as normal.

Encryption key

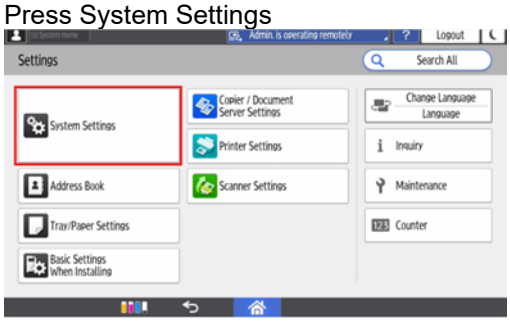
EU RED directive states that Hard drives must be encrypted from factory.
It is customer responsibility to store the encryption key, and the key must be delivered to Ricoh engineer on request if needed to do repairs.

GUIDE to print the key
User Name: admin
Press Login Password: [The one set at Initial Power On]

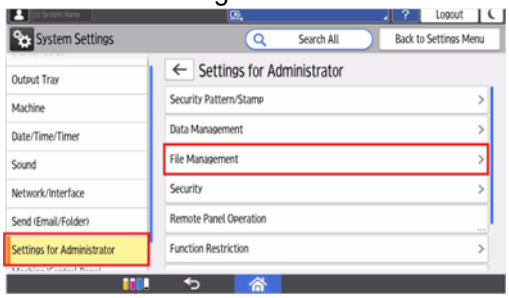
Press Arrow Press Settings

Press Settings for Administartor

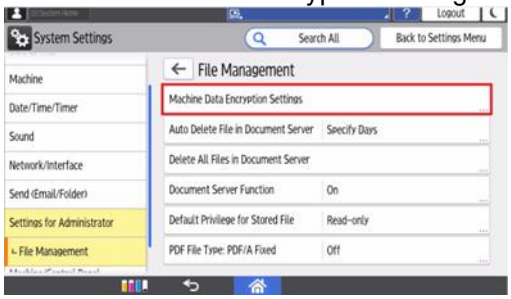
Press System Settings



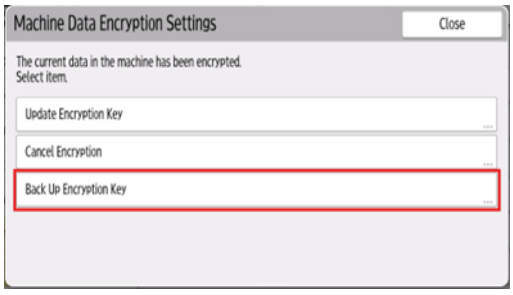
Press File Management



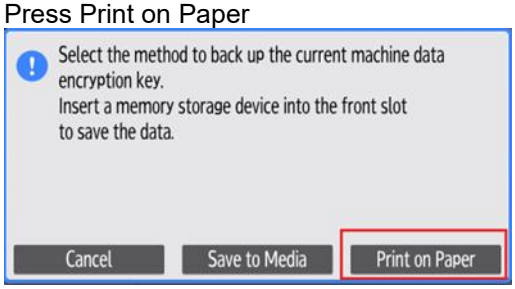
Press Machine Data Encryption Settings



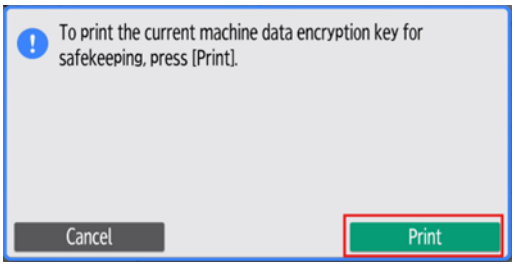
Press Back Up Encryption Key



Press Print on Paper

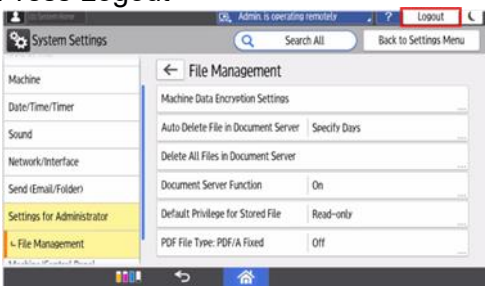


Press Print

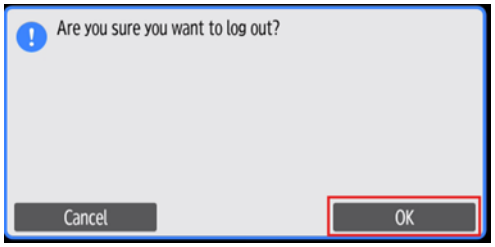


Press Close

Press Logout



Press OK



Keep the printed Encryption Key.

RICOH RED devices will from factory have the following protocols disabled.

For the device to function in your environment, they be subject to change.

FTP, LPR, RSH/RCP, TELNET ,DIPRINT, HTTP, IPP, WINS, Bonjour, NetBIOS over TCP/IPv4, SSDP, IPDS, RHPP, WSD(Device), WSD(Printer), WSD(Scanner), LLMNR, SNMP, SNMPv3, SMB, UPnP Setting, Firmware Update

These unsafe Encryption algorithms have been disabled by default.