EN-PCC-5.1-TT-20190305

Kofax Unified Client for Ricoh PCC 5.1 - Tips & Troubleshooting

Version 1.1

KOFAX

Contents

Kofax Unified Client for Ricoh PCC 5.1 - Tips & Troubleshooting Guide....3
General Troubleshooting....3
Troubleshooting....3
Enabling Home Key Settings....7
Disabling Print from USB....8
Configuring Common Access Card Authentication Solution....9
Configuring SP Mode Settings....10
SP Modes - Configuration profiles....14
Changing the TLS Settings....17
Enforcing Account Limits for Copy Job....19
Paper Type Setup....21
DCE Pinning....21
DRS Authorization Key....22
System Configuration Settings....23
Finalize the Uninstallation....24
Restarting the Device....24
Device Logs....25
Supporting a Mixed Fleet Environment....25
Additional Device Registration Service Documentation....25
Enabling the PC Keyboard....25
Tips - More information on Equitrac....28
Equitrac documentation....28

Kofax Unified Client for Ricoh PCC 5.1 - Tips & Troubleshooting Guide

General Troubleshooting

Troubleshooting

Issue	Cause	Solution
Home key on an MFP was not enabled by **Assign as home key application** Device setting.	• Device configuration may not be implemented yet for a particular MFP. • Install and Reboot action was performed previously.	You can enable the Home key manually on an MFP using the following procedure: • Enabling Home Key Settings on page 7
Need to manually configure SP Modes on a device.	SP Modes are normally configured by running on a device.	You can manually configure SP Modes on a device using the following procedure: • Configuring SP Mode Settings on page 10 Tip: Also check if Baseline installation is an option and if it is inadvertently left as **False**.
When accessing workflows, the user cannot perform scan and `You do not have the privileges to use this function` message appears.	SP Modes are set incorrectly.	You can manually configure SP Modes on a device using the following procedure: • Configuring SP Mode Settings on page 10 You must set **Admin. Authentication** to **Off**.
Installation fails.	SP Mode 5113-2 is set incorrectly.	The SP Mode 5113-2 (External Optional Counter Type) must be left to the default value: 0.

Issue	Cause	Solution
Not able to log in when switching from Equitrac only (Auth On) to AutoStore only (baseline set to false).	There is no indication from DRS that the Service Provider (SP) modes are set wrong.	You must check SP modes when baseline is set to OFF.
Need to disable Print from USB on the MFP.	Print from USB is not tracked and no quotas or limits are applied.	You can manually disable print from USB/memory stick using the following procedure: • Disabling Print from USB on page 8
Need to replace the DRS.	The DRS crashes and cannot be used any longer or similar.	The customers are advised to back up their DRS database after they have completed the configuration. Restoring the database will restore the saved Authorization key for each device. If this is not available, the customer must run the **Uninstall** command first to fully remove the Ricoh client from the device and then they will be able to set the configuration again as the client will accept the new Authorization key after a new install.
Need to replace the DCE.	The DCE crashes and cannot be used any longer or similar.	If the customers have to point to a new DCE, they must go to DRS and update the list of DCEs. Pinning will be re-established with all DCEs in the new list when the new list of DCEs are sent down from DRS by using the **Configure and Reboot** action. The client will ensure that the same DRS is used which was initially used to set the initial list of DCEs by checking the Authorization key which will be provided by DRS in the request to change the DCEs.

Issue	Cause	Solution
• DRS fails to execute the **Full Install** action. Device is not reachable and requires a manual reboot to execute **Full Install**. • The message `Device not reachable` is received.	• The TLS settings are changed on the device. • The IP address or the host name is not valid or the device is currently not visible on the network.	TLS versions must match service on the Controller and service on JavaVM. Complete the following procedure: **1.** Change the TLS settings on JavaVM or change the TLS settings on the Controller. **2.** Reboot the device. For detailed instructions, see Changing the TLS Settings on page 17.
When running Client Installer, `Please wait... Ricoh Persistence Provider` message is pending (unknown error).	The optional HDD from the device is missing.	The optional HDD is required to be installed on SFP and various MFP devices (for example, SP C842DN and MP C306) in order to be supported.
The **Login** button is not visible at the top right corner of the screen and the **Welcome** or **Login** screen is showing. The user is unable to login.	Pressing the **Stop** button at **Welcome** screen takes user interface into restricted mode.	Complete the following procedure: **1.** Dismiss the **Welcome** screen by clicking the hamburger menu and selecting **Administration** from the drop-down list. **2.** Click the **Continue Printing** button to exit access restricted mode. The **Login** button is now visible at the top right corner of the Ricoh panel and the user is able to login.

Issue	Cause	Solution
The user receives an error when running **Full Install**, **Quick Install** with either Asset or Workflow Customization enabled or when trying to deploy the customization package or perform an **Asset Sync**. The user receives the error `Failed to install the customization package`. The user receives a similar error for **Asset Sync**.	This issue may occur due to an incorrect **DRS Service URI** setting which does not respect the TLS configuration of DRS.	If DRS is configured with TLS enabled, then the URI needs to start with HTTPS. Otherwise, it should start with HTTP.
An error message occurs when selecting **Refresh Status**.	Occurs due to a missing application package.	Ensure that complete application package is uploaded.
After performing uninstallation, the device authentication settings were not reset completely in DRS.	Administrator authentication is set to ON.	Administrator authentication must be manually set to OFF in order to set back default device settings prior to client installation.

Property files generated during action with Equitrac as print manager

Equitrac-Home=True and Scan=True

Install and Reboot

- `deviceconfig_tracking_off.properties`
- `default_deviceconfig.properties`
- `deviceconfig_to_auth_on_preinstall.properties`

Configure and Reboot

- `deviceconfig_auth_on.properties`
- `deviceconfig_home_key_on.properties`

Uninstall

- `deviceconfig_tracking_off.properties`
- `default_deviceconfig.properties`

Equitrac -Home=False and Scan=False

Install and Reboot

- `deviceconfig_tracking_off.properties`
- `default_deviceconfig.properties`
- `deviceconfig_to_auth_on_preinstall.properties`

Configure and Reboot

- `deviceconfig_auth_on.properties`

Uninstall

- `deviceconfig_tracking_off.properties`

Equitrac -Home=False and Scan=False

- `default_deviceconfig.properties`

Enabling Home Key Settings

Use this procedure to manually enable the Home key when the **Assign as home key application** option in the Device settings fails to enable the Home key on an MFP.

The home key is disabled by default. This procedure describes how to enable this feature.

Important: This procedure requires working in Service Mode, which is typically performed by a Ricoh technician.

1. On the SOP device, open the **Printer** application.
2. Enter SOP Service Mode mode to complete the succeeding steps.

   If the SOP Service Mode screen does not appear, the foreground app may be covering the SOP Service Mode screen. Try closing the foreground app by pressing the **Return** or **Home** button.
3. Press **SYSTEM**.

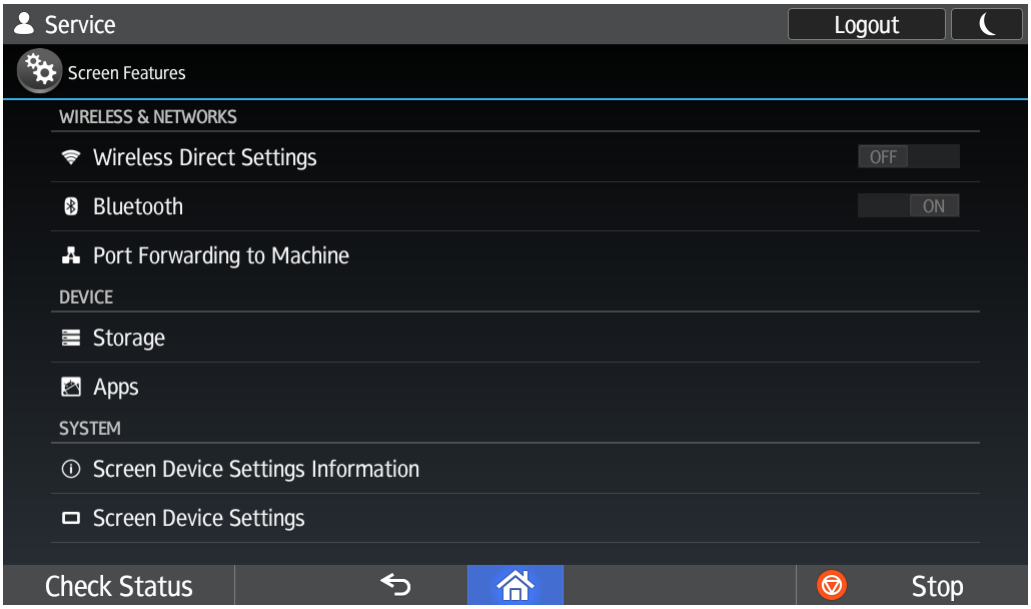
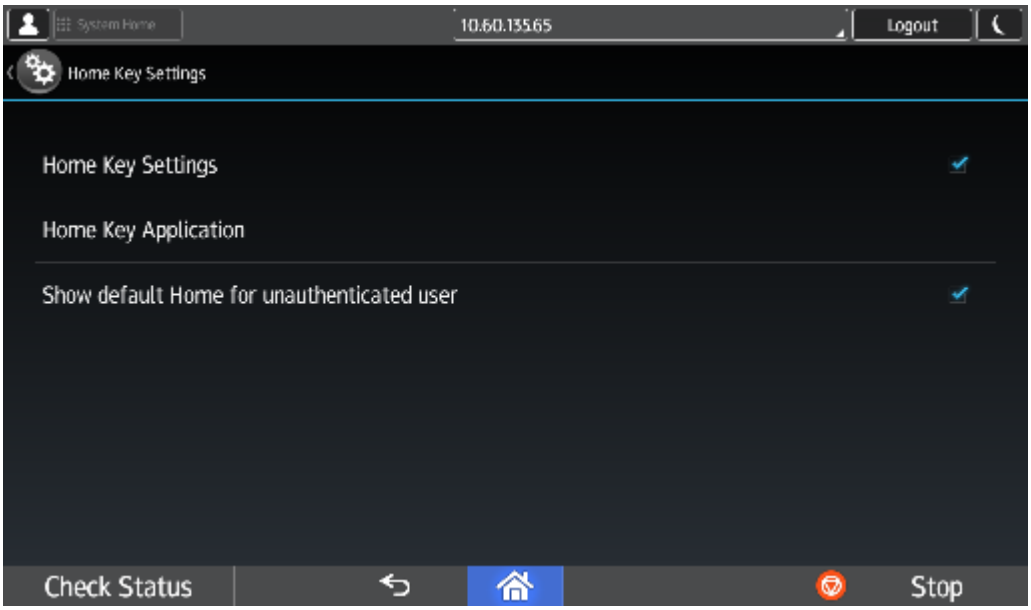


Figure 1: SOP device System Service settings

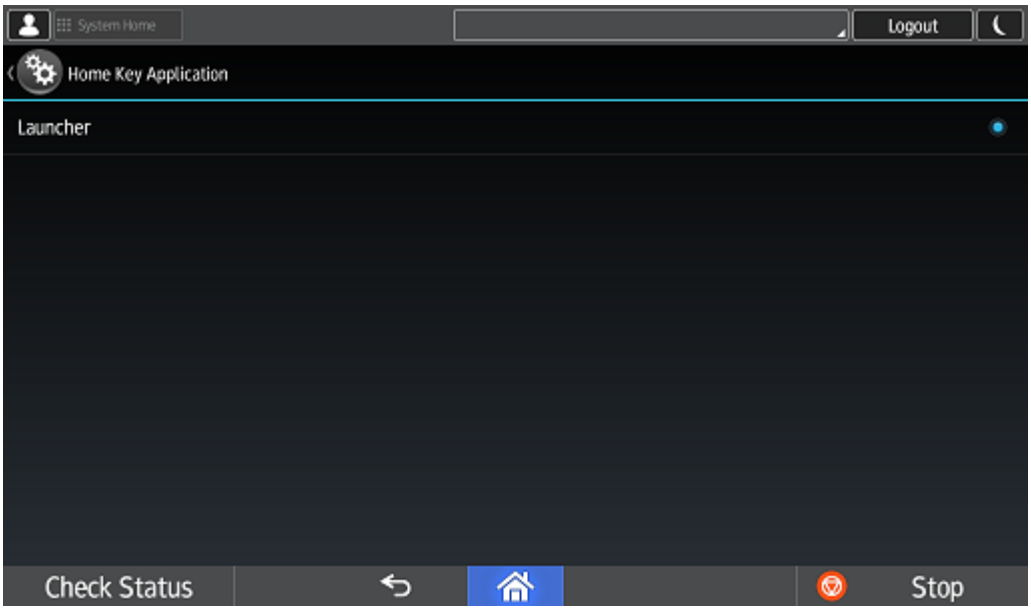
4. Press **Screen Device Settings**.
5. Press **Home Key Settings**.

   This displays the **Home Key** settings screen.



6. Press **Home Key Application**.
7. On the **Home Key Application** screen, select the application that starts when a user presses the **Home** key.

   By default, this screen lists the Launcher, which is the Ricoh **Home** key application.



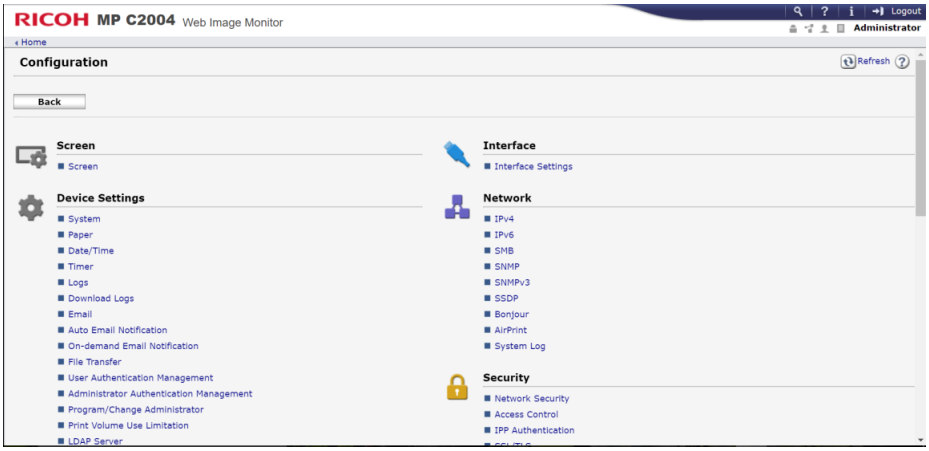
8. Log out of Service Mode.
9. Reboot the device.

Disabling Print from USB

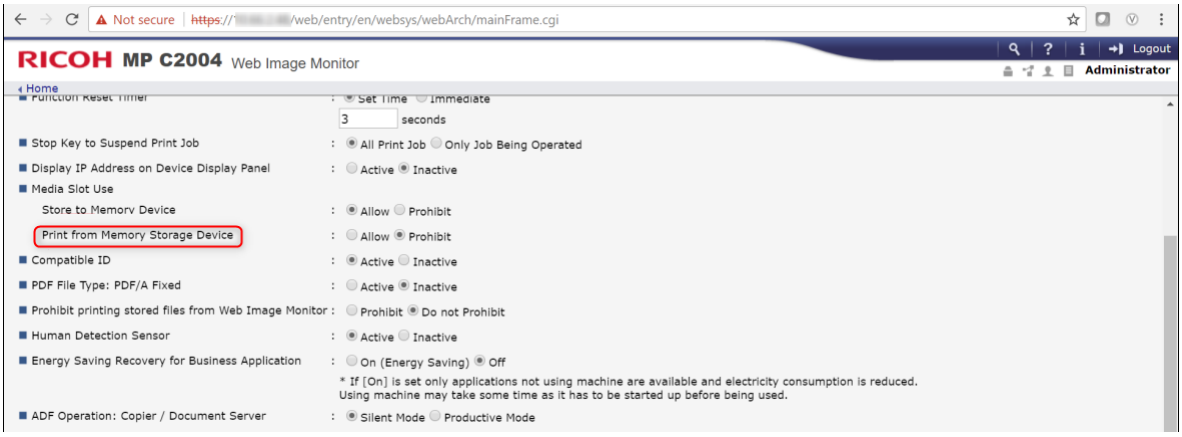
Use this procedure to manually disable print from USB/memory stick on Ricoh devices.

Print from Memory Storage Device is enabled by default. This procedure describes how to disable this feature.

1. Login to the Web Image Monitor application (which allows users to remotely monitor and change the network configuration via web browsers as long as the target MFP is networked and has an IP address) by entering the IP address of MFP on your browser.



2. Go to **Device Management** > **Configuration** > **Device Settings** > **System**.
3. Go to **Media Slot Use** > **Print from Memory Storage Device** and select **Prohibit**.



4. Select **Prohibit** for disabling print from storage devices (USB or SD card).
5. Click **OK**.

Configuring Common Access Card Authentication Solution

Ricoh PCC 5.1 supports Ricoh Common Access Card (CAC) version 4.0.5 that has authentication capabilities and prevents unauthorized access to MFPs with Equitrac installed.

A US Department of Defense (DOD) CAC authentication solution provides US federal government customers with the ability to use their exiting ID cards with the solution, increasing user satisfaction, security and productivity.

The CAC authentication solution provides the following benefits:

- Easy to use turn-key solution
- Holders of a valid CAC can perform copy, scan, fax, and/or document server functions
- Card is inserted into CAC reader connected to MFP and PIN is entered
- Upon successful authentication the multifunction device is unlocked for use

For US Government accounts the embedded client can use CAC cards for user authentication when configured with Equitrac. In this instance, Equitrac will operate when **Authentication** is set to **False** in the DRS application profile.

Note: The **Authentication** setting is only visible if a Print Manager is selected.

To use CAC authentication when Equitrac 5.6 or later is configured as the authentication provider:

1. Install CAC.
2. Register and configure Ricoh MFP devices using CAC authentication.
3. Swipe your card and enter your CAC PIN code to log in.

Note: The following Equitrac features are not supported with CAC login: Function Access Control (monochrome and color copy, scan and fax permissions and copy stop enforcement), Release All at login, Release First at login, Billing Codes at login, and Copy Rules (limit access).

Note: CAC does not support Equitrac multi-DCE environment.

Setting Alternate Primary PIN as UPN

Equitrac offers an optional alternate primary PIN that the user can enter instead of the primary PIN. Alternate primary PIN can be used for an additional level of security as it serves as another primary PIN for the user.

Open Equitrac System Manager and go to **Configuration** → **Users** and click on a user. In **Properties of…** dialog box, set the Alternate primary PIN as **UPN** from CAC server.

Configuring and Using DRS for a CAC Device

Selection on the Ricoh SOP device – DRS Web client

1. Open the http://<DRSIP>:9000/device.
2. When selecting an **Auth Off** application in device, a **Baseline Installation** option is shown..
3. Make sure you select the **Baseline Installation** as **false**.

DRS action steps

1. Select the device which has CAC on it.
2. Run action “Full Install”.

Note: You must set Home key to **System Home** and not **Embedded for Ricoh SOP** in CAC environment.

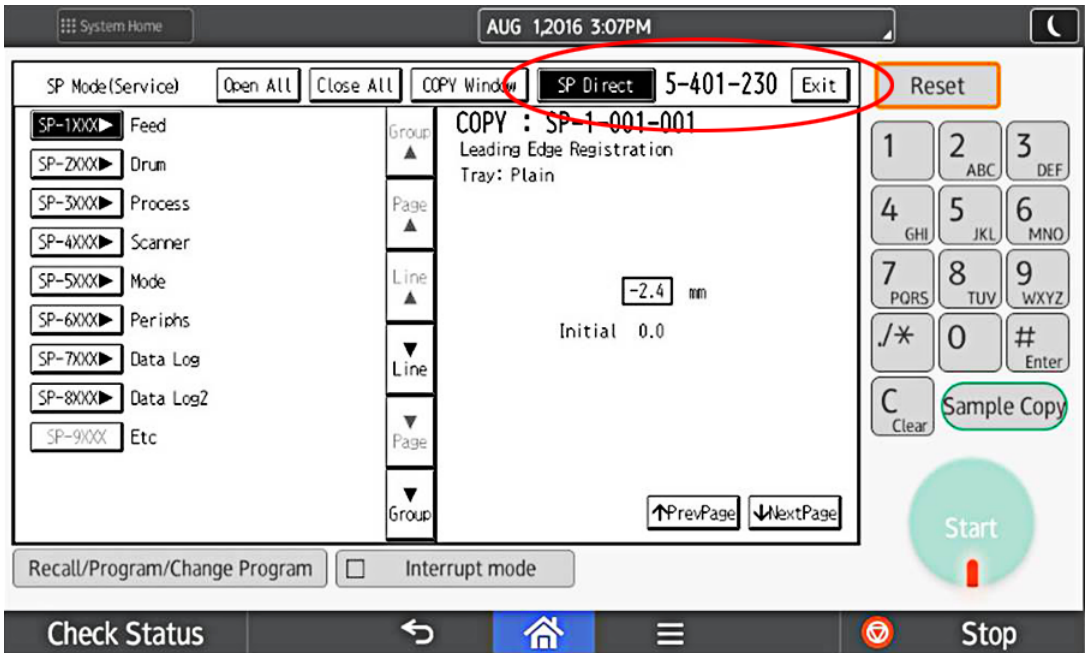
Configuring SP Mode Settings

This procedure describes how to configure Service Provider (SP) modes. The SP Mode settings are normally configured by the **Configure and Reboot Action** Action. You can use this procedure to configure settings manually when a device does not allow Device Registration Service to configure SP Mode settings through the Action.

Important: This procedure requires working in Service Mode, which is typically performed by a Ricoh technician.

1. On the **Home** screen, go to **Printer** (scroll screen) and press the **Printer** icon.
2. Enter SOP Service Mode mode (press **Reset**, then **806182** and then press and hold **C**) to complete the succeeding steps.

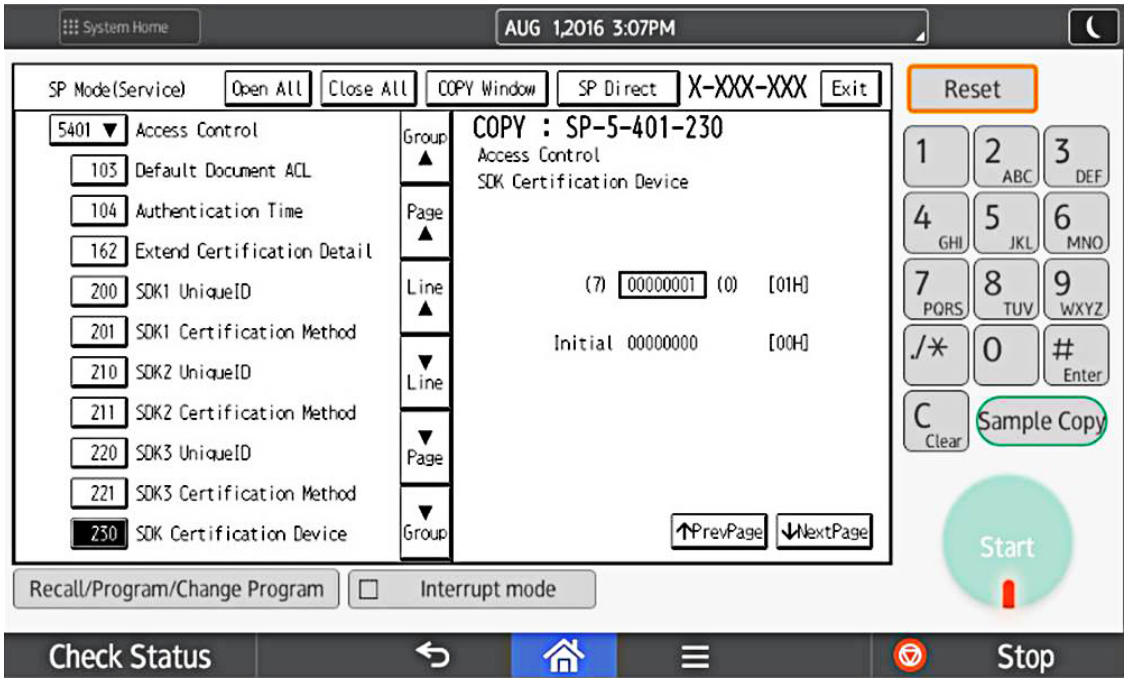
3. Press **System SP** to enter SP Mode (press **0** to change bit from **0** to **1**, then **#** to save).
4. Press **SP Direct**.



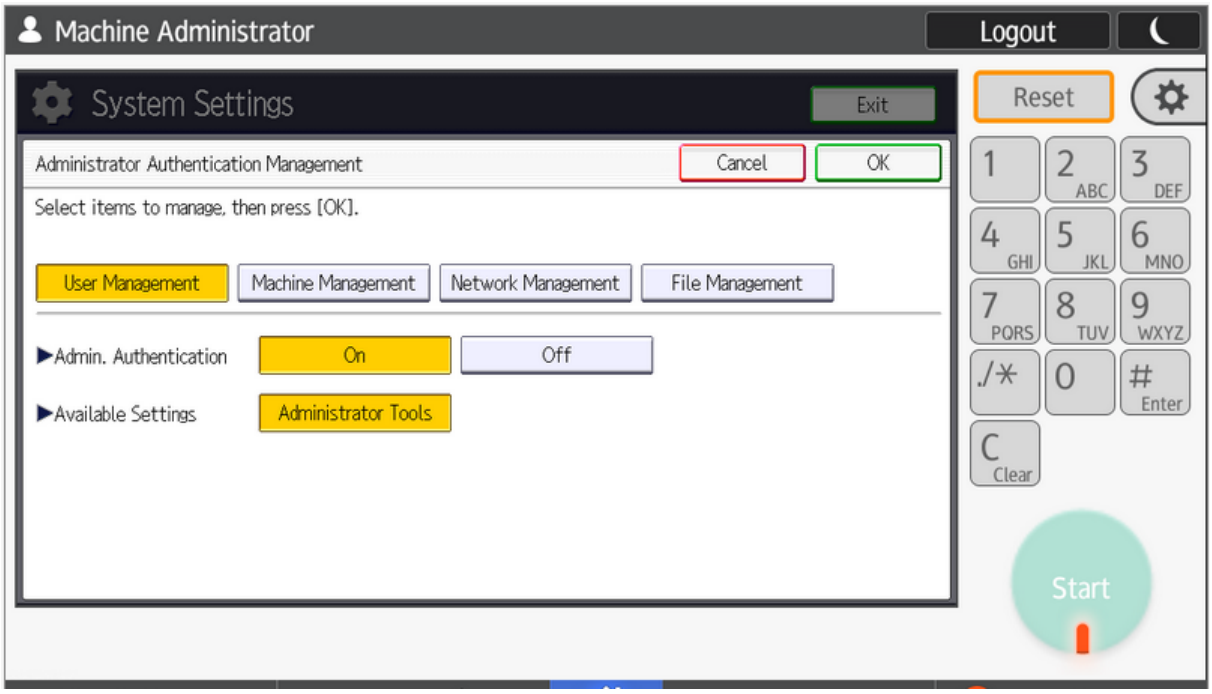
5. In **SP Direct** type `5401230` on keypad, then type `#`.
6. Set the **LSB** to **1** by pressing zero **0** (**Note**: Value of the bit at index 0 is changed when pressing **0**) on keypad in CAC configuration.
   The last digit should now be **1**.

Note: As for MFP and MPC306/MPC406 devices: SP-5420 must be set to 1 for CAC (in order for copy to work) and 0 for none-CAC installation (in order for copy to track).

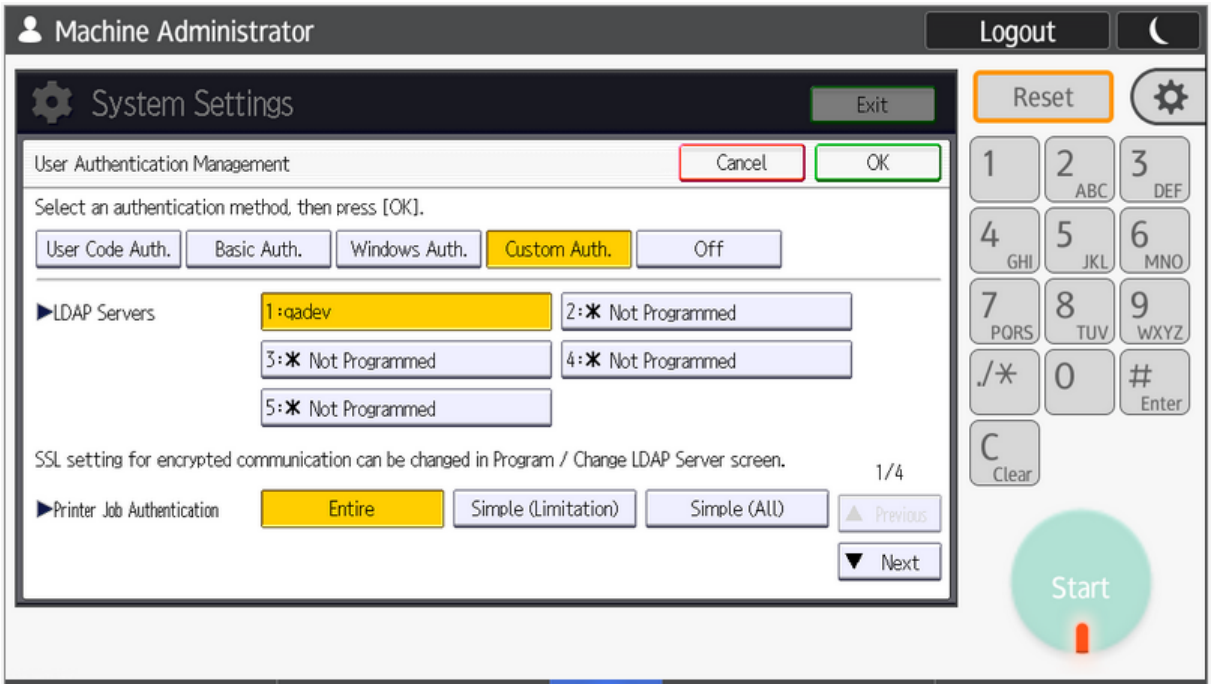
7. Type `#` to save your changes.



8. Navigate to **User Tools** > **Machine Features** > **System Settings** > **Administrator Tools** > **Administrator Authentication Management**, and on the **User Management** tab, set **Admin. Authentication** to **On**.



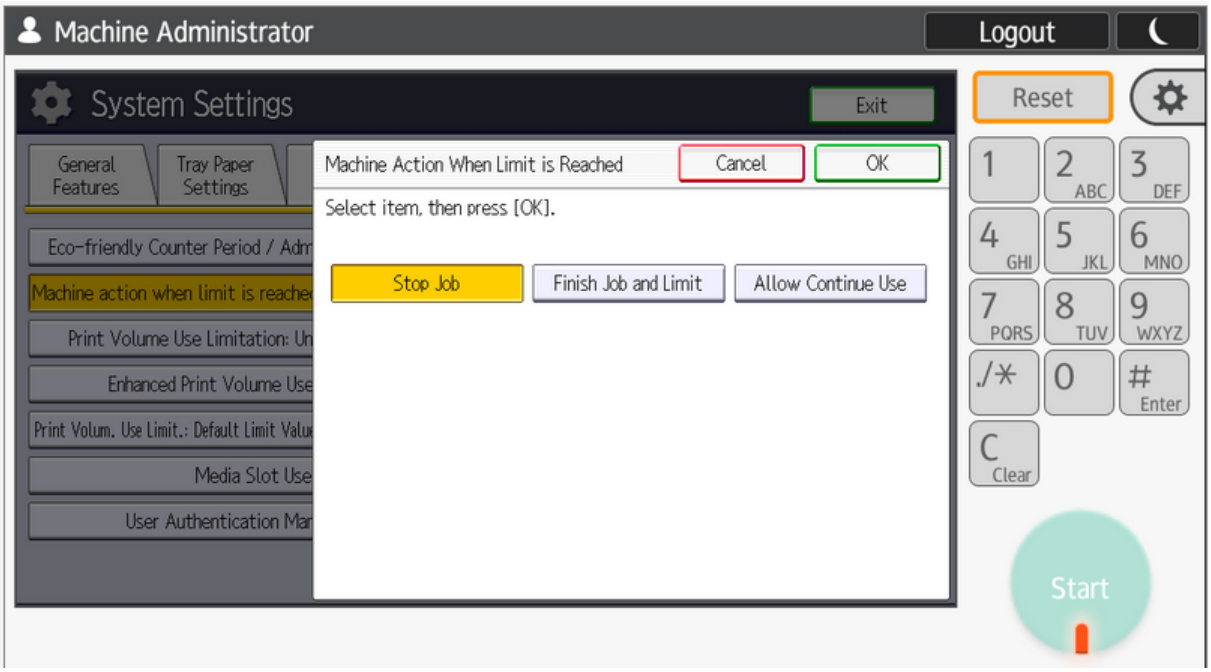
9. Navigate to **User Tools** > **Machine Features** > **System Settings** > **Administrator Tools** > **User Authentication Management Setting**, and on the **Custom Auth.** tab, enable LDAP authentication.



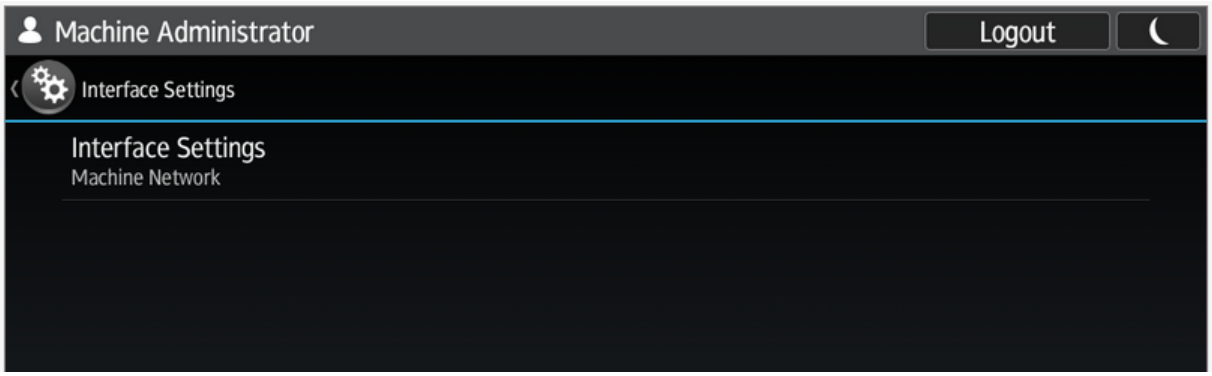
The label **LDAP authentication** in step 8 will be changed to **Custom authentication** after the machine is rebooted.

10. Configure the LDAP server, as described in the *Equitrac Express Administration Guide*.
11. Enable **Machine action when limit is reached** in **System Settings** (Administration tools).

Set this to **Stop Job** or **Finish Job and Limit**.

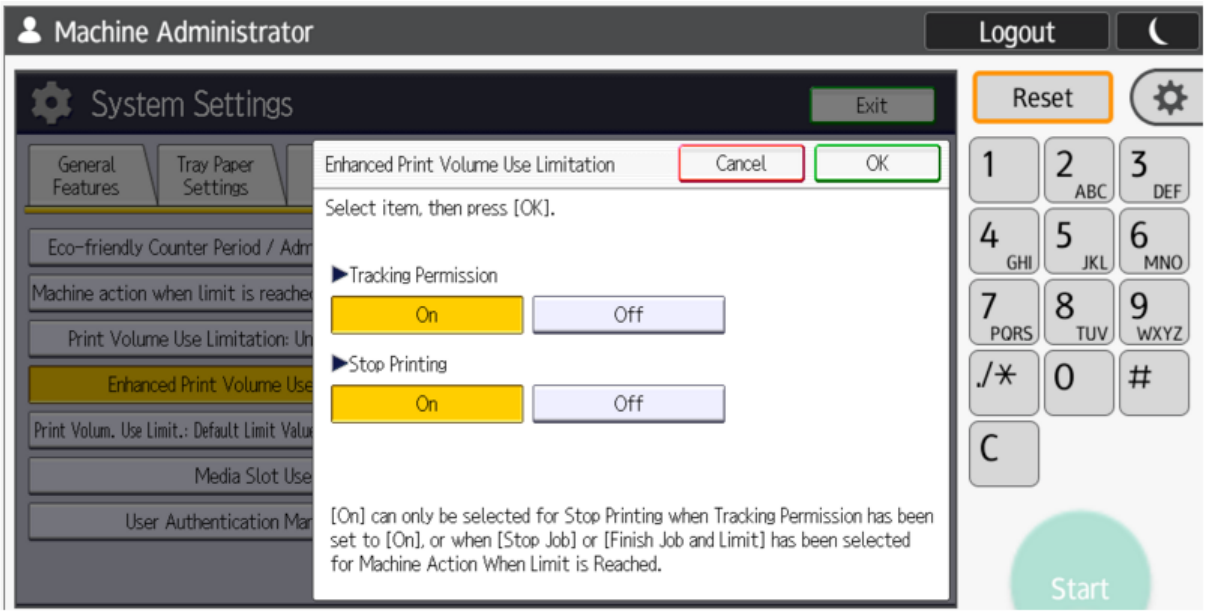


12. Enable the network by setting **User tools** > **Login** > **Exit** > **Screen Features** > **Interface Settings** > **Set to Machine Network**.



Note: The authentication logic customization feature becomes valid when the following condition is satisfied.

13. Turn on **Tracking Permission**.



SP Modes - Configuration profiles

Purpose

The following is a list of the specific SP modes that DRS uses with Ricoh devices.

The factory default values of SP modes are listed here under the following entries:

- **“tracking off”** profile, before removing packages
- **“default”** profile, after removing packages.

These are the settings that will be set by DRS after a full uninstallation and configuration sequence.

Note: In case you want to preserve your configuration from prior DRS running actions, run the **Get Config** action which saves the values for all SP modes to a file which could be used later to compare two configurations.

Note: As for the effect on other third-party applications residing on the Ricoh device, if any of these applications depend on a setting which value must be different than what is listed under the **default** profile here, then they would be affected.

Setting		Authentication ON	Authentication OFF		SP mode definition and values
			Baseline ON	Baseline OFF	
Preparation before installing service and application packages					
"tracking off" profile, before removing packages	trackingPermission	0	0	Skip	TRACK_PERMISSION: 0 = disable tracking event; 1 = enable tracking event
	stopPrintSetting	0	0	Skip	STOP_PRINT_SETTING: 0 = do not stop; 1 = stop
"default" profile, after removing packages	setspmode.5401.230	0	0	Skip	ACCESS_CONTROL__SDK_CERTIFICATION_DEVICE

setspmode.5490.1	0	0	Skip	MF_KEYCARD_JOB_ PERMIT_SETTING: 0=authenticated by printer (default); 1=ask authentication Skip on SFP device
userAuthPrinter	0	0	Skip	USER_AUTHENTICATION __PRINTER: 0=On; 1=Off SFP device only
adminAuth	1	1	Skip	ADMINISTRATOR _AUTHENTICATION _MANAGEMENT __USER_ ADMINISTRATOR _AUTHENTICATION _SETTING
userAuth	0	0	Skip	USER_AUTHENTICATION _MANAGEMENT
printerJobAuthLevel	0	0	Skip	PRINTER_JOB_ AUTHENTICATION_LEVEL: 0=Entire (default); 1=Simple (ALL); 2=Simple (Limitation)
trackingPermission	0	0	Skip	TRACK_PERMISSION: 0 = disable tracking event; 1 = enable tracking event :
stopPrintSetting	0	0	Skip	STOP_PRINT_SETTING: 0 = do not stop; 1 = stop
actionWhenLimitReached	0	0	Skip	MACHINE_ACTION_WHEN _LIMIT_REACHED: 1 = "Finish Job and Limit"; 2 = "Stop Job"
adminAuthKey.user.tools	TRUE	TRUE	Skip	ricoh.rxop.rxconf.Configurator: ADMIN_AUTH_KEY_USER. TOOLS
adminAuthKey.machine	TRUE	TRUE	Skip	ricoh.rxop.rxconf.Configurator: ADMIN_AUTH_KEY_ MACHINE
adminAuthKey.machine.tools	TRUE	TRUE	Skip	ricoh.rxop.rxconf.Configurator: ADMIN_AUTH_KEY_ MACHINE.TOOLS
defaultUserPermission	-1,-1	-1,-1	Skip	DEFAULT_USER_PERMISSION: "0000" (0,0) "NO_PERMISSION", "001f" (0,31) "COPY_ALL", "ffff" (-1,-1) "ALL_PERMISSIONS", "4060" (64,96) "PRINTER_ALL"

Preparation before installing service and application packages

"pre-install" profile, before installing packages	setspmode.5401.230	-127 bit 0=1: Enable bit 7=1: Timer starts at the end of job	0 bit 0=0 : Disable bit 7=0 : Ricoh default behavior	Skip	ACCESS_CONTROL__SDK_ CERTIFICATION_DEVICE bit 0=0 : Disable (Ricoh's device embedded authentication is used) bit 0=1 : Enable (Partner's custom authentication is used) bit 7=0 : Ricoh default behavior (timer starts at the last panel operation) bit 7=1 : New behavior (timer starts at the end of job)
	setspmode.5490.1	1	0	Skip	MF_KEYCARD_JOB_ PERMIT_SETTING: 0=authenticated by printer (default); 1=ask authentication Skip on SFP device
	userAuthPrinter	1	1	Skip	USER_AUTHENTICATION __PRINTER: 0=On; 1=Off SFP device only
	adminAuth	1	1	Skip	ADMINISTRATOR_ AUTHENTICATION_ MANAGEMENT __USER_ADMINISTRATOR _AUTHENTICATION _SETTING
	userAuth	4	0	Skip	USER_AUTHENTICATION _MANAGEMENT
	trackingPermission	0	0	Skip	TRACK_PERMISSION: 0 = disable tracking event; 1 = enable tracking event
	stopPrintSetting	0	0	Skip	STOP_PRINT_SETTING: 0 = do not stop; 1 = stop
	actionWhenLimitReached	2	0	Skip	MACHINE_ACTION _WHEN_LIMIT_REACHED: 1 = "Finish Job and Limit"; 2 = "Stop Job"
	printerJobAuthLevel	0	0	Skip	PRINTER_JOB _AUTHENTICATION_LEVEL: 0=Entire (default); 1=Simple (ALL); 2=Simple (Limitation)
	defaultUserPermission	64,96	-1,-1	Skip	DEFAULT_USER_PERMISSION: "0000" (0,0) "NO_PERMISSION", "001f" (0,31) "COPY_ALL", "ffff" (-1,-1) "ALL_PERMISSIONS", "4060" (64,96) "PRINTER_ALL"
During configuration, after sending wiring and associated server settings to configuration servlet					

"post-install" profiles, after packages are installed and verified	trackingPermission	1	Skip	Skip	TRACK_PERMISSION: 0 = disable tracking event; 1 = enable tracking event
	stopPrintSetting	1	Skip	Skip	STOP_PRINT _SETTING: 0 = do not stop; 1 = stop

	homeKeyFuncId	Intent link to NEUF app (only if “Assign as home key application” is enabled)	Skip	Skip	#Intent;componen
					t=com.kofax

Changing the TLS Settings

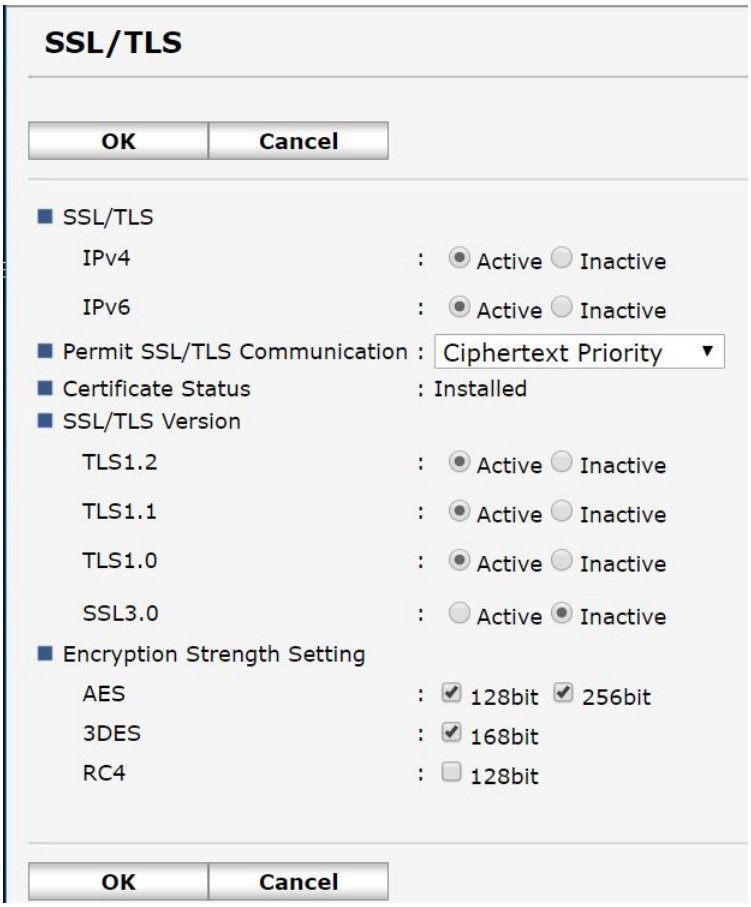
Changing the TLS settings can be performed on JavaVM and on the Controller using the Web Image Monitor.

The Web Image Monitor allows users to remotely monitor and change the network configuration via web browsers as long as the target MFP is networked and has an IP address. Follow these steps to open the Web Image Monitor:

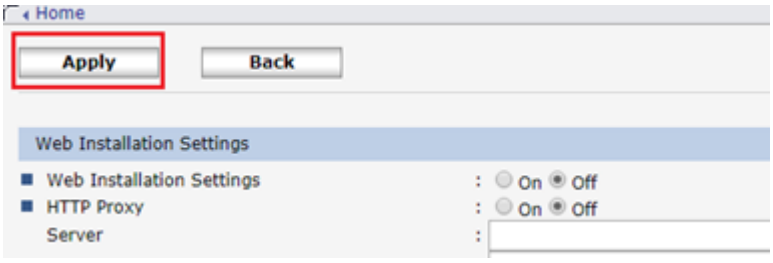
1. Open a web browser and enter http://<MFP IP Address> in the **Address** field. The device web page opens.
2. Click **Login** and enter your administrator User Name and Password.

Changing the TLS settings on JavaVM

1. Open the Web Image Monitor and log in.
2. Go to **Device Management** > **Configuration** > **Extended Feature Settings** > **Administrator Tools** and change the settings.

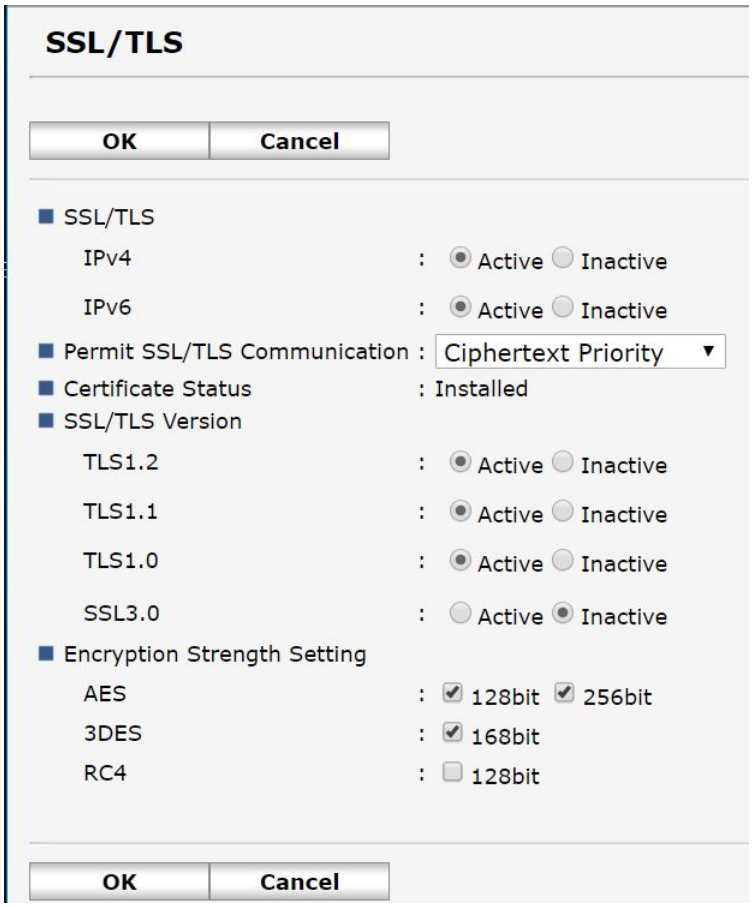


3. Click **Apply**



Changing the TLS settings on the Controller

1. Open the Web Image Monitor.
2. Go to **Device Management** > **Configuration** > **SSL/TLS** and change the settings.



3. Click **OK**.

Enforcing Account Limits for Copy Job

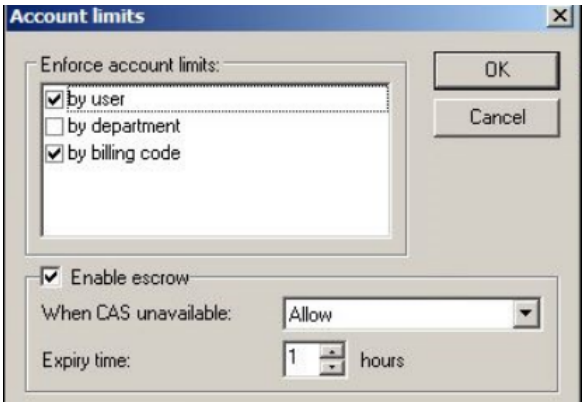
Use this procedure to perform a copy job when billing code balance is **negative** and **Enforce account limits** is set for billing code.

Before you start: Account limits for copy job use the user's limit (not billing code account limit) when entering a billing code at login. The only time billing code account is considered for copy-stop is when:

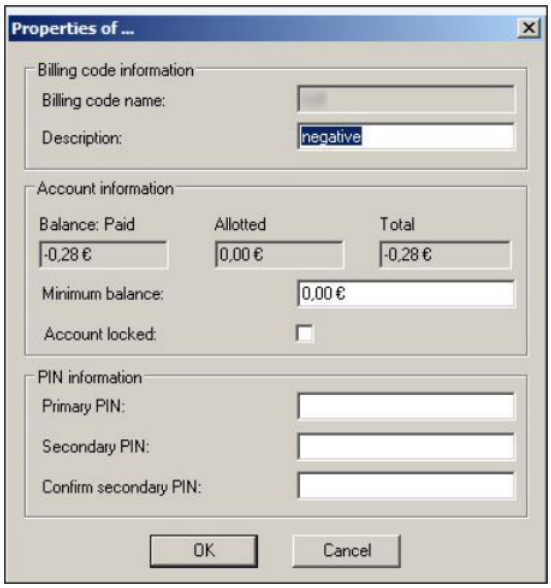
1. User has a default billing code populated in System Manager
2. User logs onto device using billing code account (logs on as a billing code).

Follow these steps:

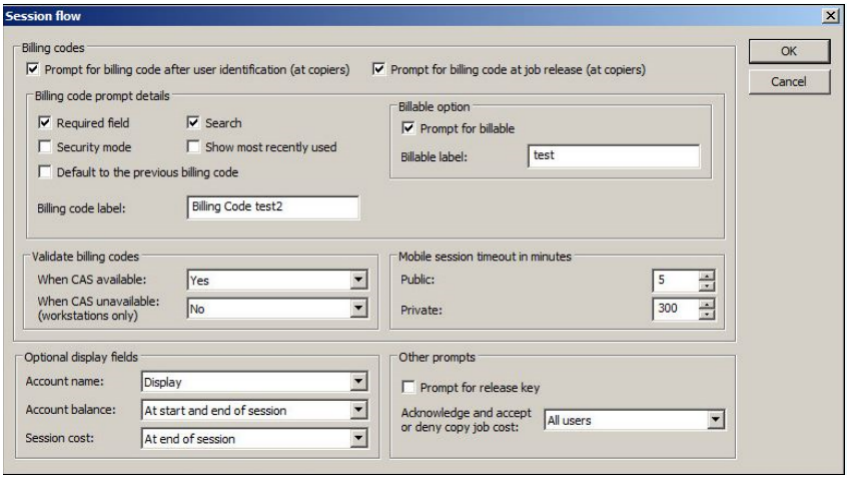
1. Set enforce limits (by user, by department or by billing code) under **Account limits**.



2. Create billing codes and make sure a user has a positive fund balance.
3. Create a billing code with null or negative funds.



4. Ensure Billing Codes are enabled in Session Flow.



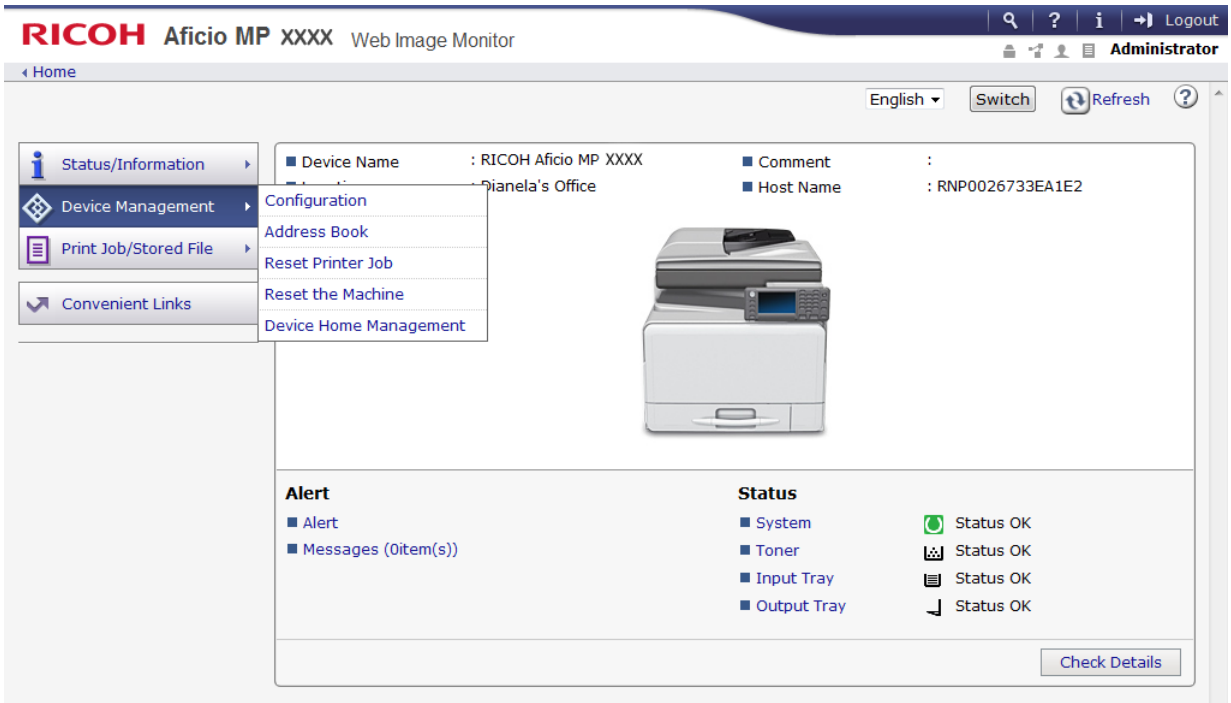
5. Login into Ricoh PCC 5.1 with a user account that has funds and select the billing code "null".
6. Perform a copy job .

7. Expected result: The copy job will stop after the billing code funds have been exhausted and the copy stop dialog box will show "Exceeded the number of sheets that can be used. Copying will be stopped" message. Use an **Exit** button.

Paper Type Setup

If you notice that your tracking and pricing for copies is different than expected, please ensure you have the paper type set to **Tray 1** and **Plain Paper**. Follow these steps:

1. Open a web browser and enter `http://<MFP IP Address>` in the Address field. The device web page opens.
2. Click **Login** and enter your administrator User Name and Password. The Web Image Monitor page opens.



Note: The Web Image Monitor page may differ in appearance and location of functions by device. The basic functionality remains the same.

3. Navigate to **Device Management** > **Configuration**. The Configuration options display.
4. Under **Device Settings**, click **Paper**. The Paper options display.
5. Under **Tray 1**, from the **Paper Weight** drop-down list, select any of the **Plain Paper** options.
6. If you are using the Bypass Tray, ensure it is also using this setting.
7. Click **OK**.

DCE Pinning

Purpose

DCE pinning services are used to reduce a man-in-the-middle attack (MITM) and provide additional security by pinning your client to a specific DCE that belongs to your configuration for the duration of that configuration.

Details

This additional security is achieved through certificate pinning where you are bound to the DCE using the certificate that the DCE provides upon connection and use it to validate the trust of subsequent communications with that server.

Note: You are not allowed to change the DCE endpoints until you reconfigure the client application again (until then, you are bound to the DCE you have configured initially).

Possible failures

You may receive connection failures if the following possibilities occur:

- Failure to create JavaKeystore (JKS) for any reason (example: HDD issues)
- Failure to write to the JKS for any reason (example: corrupt file, HDD issues)
- Invalid certificate is provided by the DCE (MITM server, DCE has changed its certificate sometime after).

Recovery

Validate if the DCE you are unable to connect to has the same certificate (since your initial client application configuration) in order to eliminate a possible MITM attack.

To recover from connection issues related to DCE pinning that are not related to hardware failures (HDD):

- Perform a **Configure and reboot** action for a new configuration using the DRS, or
- Perform a **Full Install** action.

Note: New configuration means that either a DCE endpoint has changed (IP, FQDN) or DCE endpoints have been added or removed from the list.

Reset

To reset DCE pinning, only **Uninstall** and **Full Install** actions must be used.

DRS Authorization Key

This security feature has been added to DRS where additional security between the DRS application and the device is enabled using an authorization key. This additional security check will confirm that only the initial DRS instance that was used to deploy or configure the device can be used to update the configuration of the embedded client on the device.

The DRS Authorization Key is pinned to a device or group of devices when a **Full Install** is performed, the DRS Authorization Key is pinned to the device the first time the device is configured within the DRS application and is kept on the device and this authorization key cannot be changed. If any DRS configuration actions, such as Sync Assets, Sync Workflow Buttons or Configure and Reboot do not contain the pinned authorization key, the request will fail and failure message will be displayed in DRS.

The DRS Authorization Key is stored in the DRS database and it is uniquely generated every time a device is added into the same used DRS application. If the same device is added to another DRS instance, then the DRS Authorization Key will be different.

Note: If TLS is not enabled on the device, the DRS Authorization Key pinning will not be engaged. Once the device is pinned to a given DRS instance, only that DRS instance can perform the following actions of the install and configuration options: **Sync Assets**, **Sync Workflow Buttons** and **Configure and Reboot**.

Note: If you go from TLS enabled to TLS disabled, the Authorization Key Pinning must be reset.

Note: If want to move the control from one DRS to another DRS, the second DRS must run **Full Install**.

Note: In order to reset Authorization Key pinning, DRS must run **Full Install** or **Uninstall**.

System Configuration Settings

CAUTION: When installing Equitrac, you **must** use the settings listed under **Auth On**. Auth Off settings handle other configurations of Ricoh PCC 5.1.

Configuration Path	Auth On	Notes
Service > Screen Features > Screen Device Settings > Home key settings > Home key application	Either	
Service > Screen Features > Screen Device Settings > Screen device always-connection Setting	Active	Needed for card reader auto-wakeup
User Tools > Machine Features > System Settings > Administrator Tools > Administrator Authentication Management > Admin. Authentication	On	
User Tools > Machine Features > System Settings > Administrator Tools > Administrator Authentication Management >Available Settings	Administrator Tools	
User Tools > Machine Features > System Settings > Administrator Tools > Enhanced Print Volume Use Limitation > Stop Printing	On	
User Tools > Machine Features > System Settings > Administrator Tools > Enhanced Print Volume Use Limitation > Tracking Permission	On	
User Tools > Machine Features > System Settings > Administrator Tools > Machine action when limit is reached	Stop Job	
User Tools > Machine Features > System Settings	None	

Configuration Path	Auth On	Notes
> Administrator Tools > User Authentication Management > Custom Auth > Available Functions Copier		
User Tools > Machine Features > System Settings > Administrator Tools > User Authentication Management > Custom Auth > LDAP Servers	Not Programmed	
User Tools > Machine Features > System Settings > Administrator Tools > User Authentication Management > Custom Auth > Other Functions	None	
User Tools > Machine Features > System Settings > Administrator Tools > User Authentication Management > Custom Auth > Printer Job authentication	Entire	
User Tools > Machine Features > System Settings > Administrator Tools > User Authentication Management > OFF	N/A	
User Tools > Screen Features > Interface Settings	Machine Network	

Finalize the Uninstallation

If, after the uninstallation is complete, the Launcher icon remains on the Ricoh Smart Operation Panel Home screen, do this to remove it:

1. Login to the device with administrator credentials.
2. Ensure that you are on the Ricoh Smart Operation Panel Home screen, where the Launcher icon appears.
3. Press down and hold the Launcher icon. After a few seconds, a small trash can icon displays on the screen.
4. Still pressing down on the icon, drag it into the trash can.

Restarting the Device

A restart of the device is recommended after installing or uninstalling new software. Follow these steps:

1. Locate the physical on/off switch of the device, then press until the device screen displays a dialog indicating the device is shutting down.

   You can then release the button. The shutdown process may take as long as 7 minutes.

Note: Once the screen shuts down, the device's blue LED indicator light continues to flash. The device is not fully shut down until this light stops flashing.

2. Once the device is fully shut down, press the on/off button again. The screen indicates the startup is in progress.

Depending upon the device's setup, the main display will either show the Ricoh PCC 5.1 login screen, or if the embedded solution is not installed, the standard Ricoh Smart Operation Panel Home screen with option icons.

Device Logs

Device Registration Service configures the client to generate additional logs on the device which can be downloaded by support and submitted for troubleshooting. Contact your support provider to collect logs.

Enable logging in device

Device logs can be enabled by using Device Registration Service web console.

Open Device Registration Service Web console, go to **Devices** and select device. In the **Details** section click on edit icon and set **Enable Debug Log** to **True**.

Disable logging in device

Device logs can be disabled on the device by using Device Registration Service web console.

Open Device Registration Service Web console, go to **Devices** and select device. In the **Details** section click on edit icon and set **Enable Debug Log** to **False**.

Supporting a Mixed Fleet Environment

If you have an existing fleet of PCC 4 devices and are adding PCC 5.1 to your environment, refer to the *PCC 4 Setup Guide* for all PCC 4 devices.

Additional Device Registration Service Documentation

Device Registration Service documentation

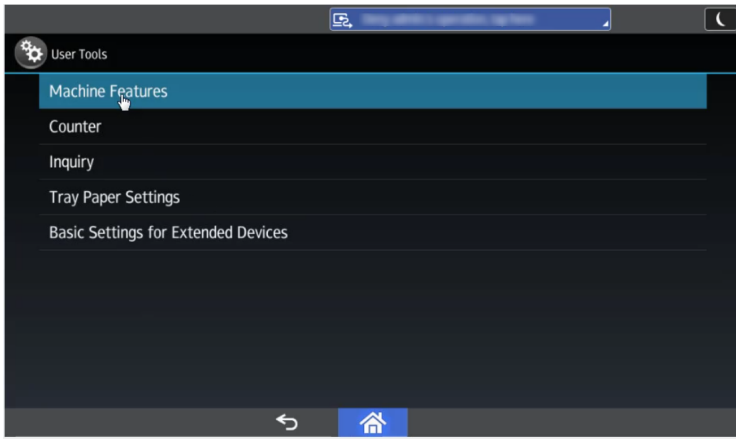
For more information on how to perform an initial installation, configuration or upgrade of Device Registration Service, see *Device Registration Service Installation Guide* provided with your product software.

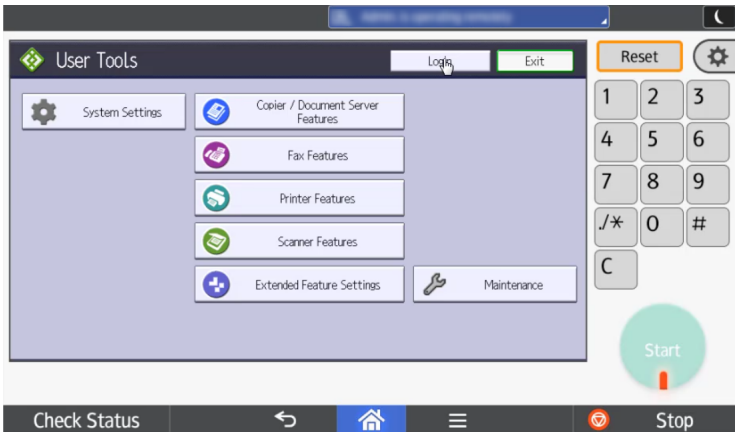
For more information on how to use Device Registration Service with Ricoh PCC 5.1, see *Device Registration Service Help* provided with your product software.

Enabling the PC Keyboard

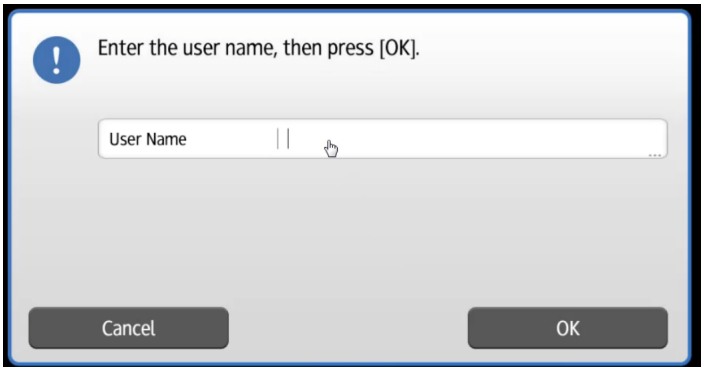
The following is configuration of the PC keyboard on Ricoh devices so that alphanumeric keys can be used instead of default keyboard. Follow these steps:

1. Navigate to **User Tools** > **Machine Features** > **Login**.

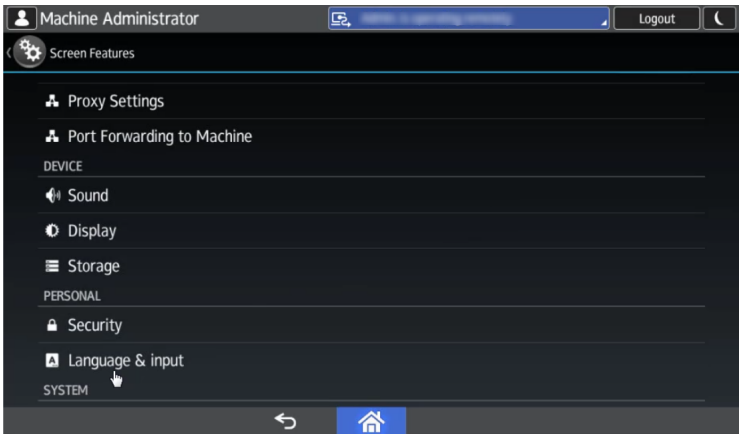




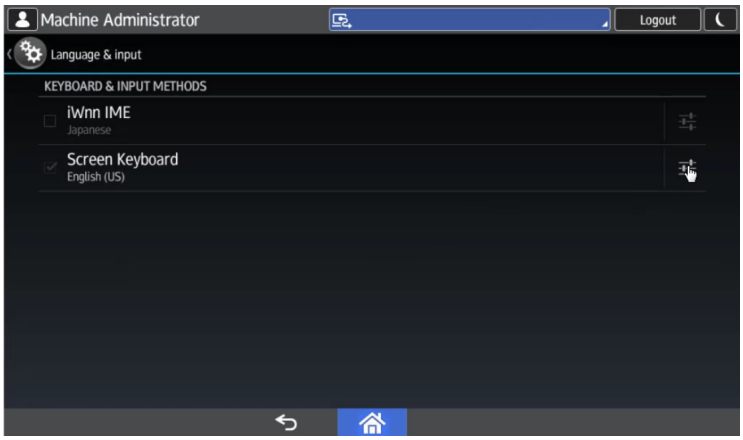
2. Click **Login** again and enter the user name (default is 'admin' with blank password). Click **OK**.



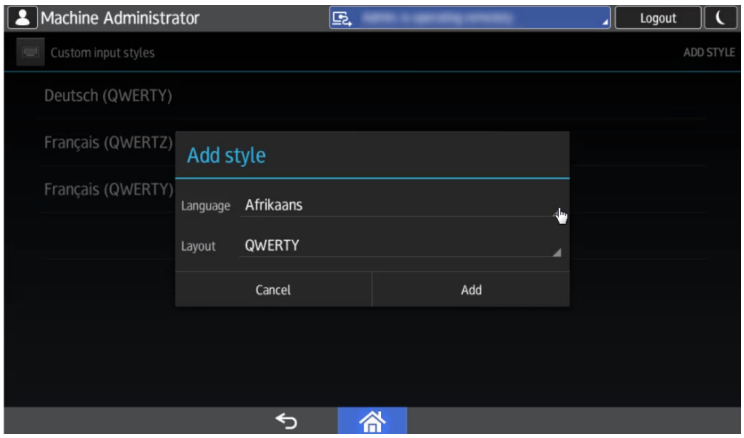
3. Once logged in, a splash screen appears. Go to hamburger menu and click **Administration**.
4. Click **Exit** in the User Tools page. A **Screen Feature** screen appears.
5. Scroll down to **Personal** > **Language & input**.



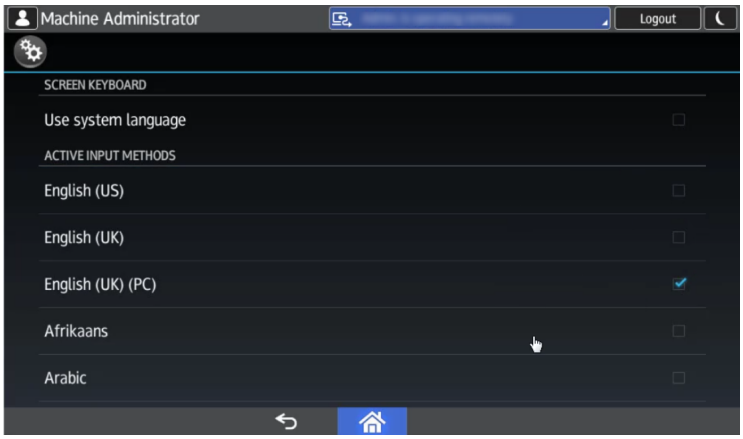
6. In **Language & input** under **Keyboards & input methods**, click **Default** > **Set up input methods** > **Screen Keyboard** (Advanced settings icon).



7. In **Advanced settings** under **Other options** click **Advanced settings** > **Custom input styles**.
8. In **Custom input styles** click **Add style**. In the popup window, select **Language** and **Layout** of your choice.

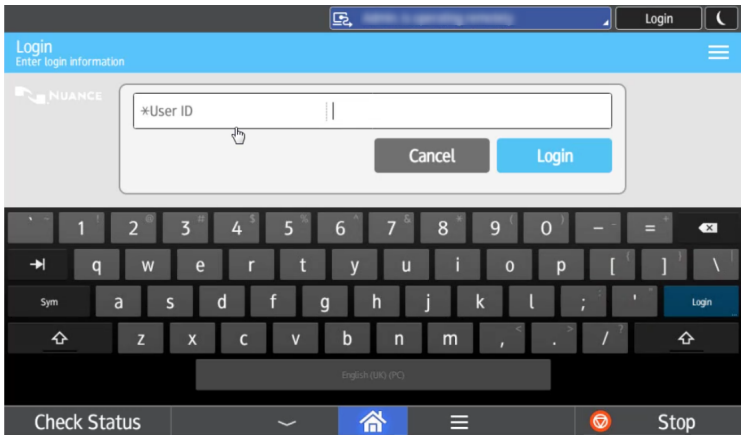


9. In **Layout** (default is QUERTY), choose **PC** and click **Add** > **Enable**.
10. In **Screen keyboard**, turn off the original keyboard settings and **Use system language** entry.
11. Under **Active input methods**, click **(your language) (PC)**. Click the back button.



12. Under **Custom input styles** chose your language. Click the back button until the main menu appears.
13. Click **Logout** button.

The login screen will now appear with the PC keyboard displayed.



Tips - More information on Equitrac

Equitrac documentation

You may need to refer to one of the following documents when performing server-side configuration tasks.

For more information on Equitrac, see the following documents provided with your product software:

- *Equitrac Office or Express Administration Guide*
- *Equitrac Office or Express Installation Guide*