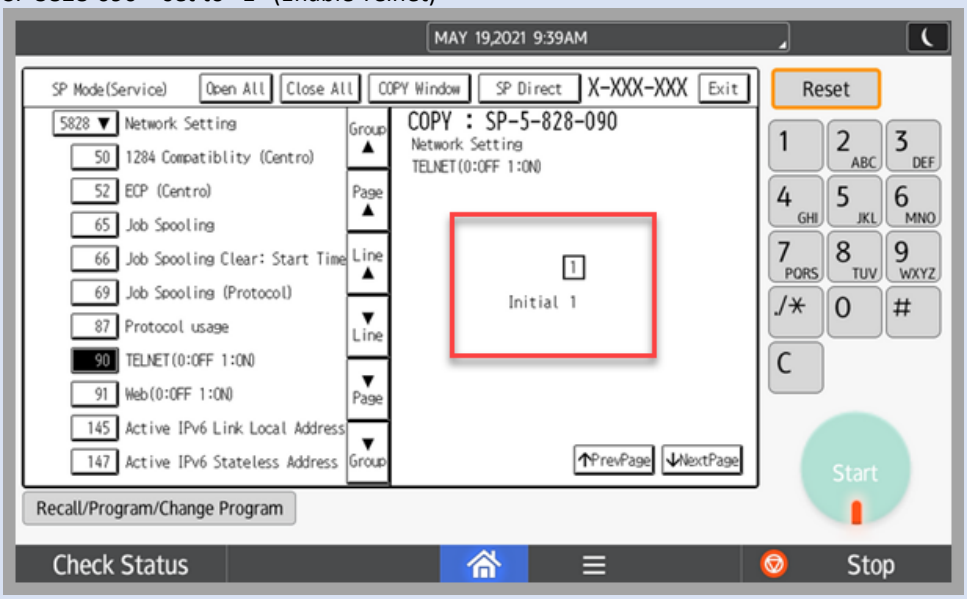
Hardware configuration tasks for new devices

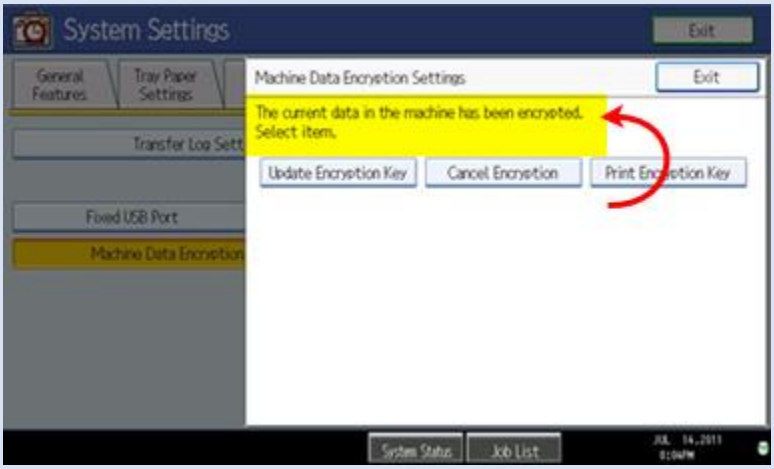
The following hardware configuration settings must be made/confirmed by an installation engineer/technician on all devices with Streamline NX being installed at any of the worldwide Parker Hannifin facilities.

Note: These instructions apply to all new device installations globally but there are some exceptions for Parker sites in Japan region. Please take a note of those exceptions highlighted in YELLOW cells below.

Item	Description
A. Device Firmware and Java* check (* Java if present and applicable)	1. Confirm that new device/s being deployed at this site are all updated with latest firmware components as well as Java VM (if applicable) **2. **If not, update the device/s with necessary firmware updates and Java VM updates****
B. Machine Administrator Password	1. Leave the Administrator ID and password at factory default values. Reset to factory default if it is different than what is written here. a. Administrator 1 ID = ***admin*** | password = <***blank***> 2. Leave the Supervisor ID and password at factory default values. Reset to factory default if it is different than what is written here. a. Administrator 1 ID = ***supervisor*** | password = <***blank***>
C. DO NOT setup embedded @Remote service (Except devices in Japan)	Confirm that embedded @Remote service IS NOT setup except for devices installed in Japan 1. SP 5816-201 is set to "0" 2. SP 5816-209 > Execute – Install Clear 3. SP 5870-003 > Execute – Common Key Info Initialize 4. SP 5870-004 > Execute – Common Key Info Writing (2048 bit) if available and **a. Reboot the device > This is a mandatory step** 5. SP 5870-001 > Execute – Common Key Info Writing (512 bit) only if 5870-004 is not available and **a. Reboot the device > This is a mandatory step**
D. For Japan devices only Enable embedded @Remote service	1. Enable and setup embedded @Remote service on each device. 2. Request a registration number form @Remote Center system 3. Register the device with @Remote Center system using account named "Parker Hannifin_Japan"
E. Low toner alerts and threshold settings in Service mode	1. SP 5507-80# > Set to 1-- At Less Than Thresh # 2. SP 5507-81# > Toner call threshold set to 20% # 3. SP 5507-82# > Toner call threshold set to 20% #
F. Waste toner settings	1. SP 5507-003 > (Supply/CC Alarm: Toner Supply Alarm) set to 1 (enable) 2. SP 5507-006 > (Supply/CC Alarm: Waste Toner Bottle) set to 1 (enable) 3. SP 5515-010 > (SC/Alarm Setting: Supply Automatic Ordering Call) set to 1 (enable)
G. Enable Remote Operation Panel feature * This may not apply to Single Function printers	"Remote Operation Panel" function is disabled by default. Follow the process below to enable it. For IM C300/C400, IM C4500/C6000, IM 4000/5000 devices only 1. Enable machine administrator authentication and login as administrator

Item	Description
	2. Press the "Settings" icon on the HOME screen 3. Press "Basic Settings for Extended Devices" 4. Press "Remote Panel Operation" 5. Enable “Remote Operation/Monitoring Functions” For MP 4055/5055, MP 305 and IM 350 devices only 1. You WILL have to Login into Screen Service mode. Open a keypad by accessing the Document Server. 2. Enter Reset 8 0 6 1 8 2 # # C – This will allow you to activate a hidden screen from Service Mode which will ultimately allow you activate RPO. 3. Select Screen Device Settings, then select Application Settings, then select Remote Panel Operation (this screen is a couple of pages down in the scroll so be sure to select Remote Panel Operation) then select Remote Operation/Monitoring Function and switch to ON. 4. Logout of Services mode and go back to the home screen. 5. From the home screen select Settings, then select Machine Feature Settings. This will allow you to access Administrator Tools where you will have to turn on Administrator Authentication Management which will activate another hidden that will allow you turn on RPO. This probably seems a little redundant, but these steps are required to fully activate RPO. 6. Select System Settings, then select Administrator Tools and select Next to scroll to page 2 of 6 and select Administrator Authentication Management. 7. Select Machine Management and switch to ON. Select OK and then select Exit, then select Login which will ultimately allow you to activate RPO. 8. Enter admin as User Name and select OK. Leave Password blank and select OK 9. This will bring you back to the screen below where you will want to select the blue house Home Screen at the bottom. From there select Settings. 10. Select Basic Settings for Extended Devices at the bottom of the screen, then select Remote Panel Operation on the next screen. 11. Switch Remote Operation/Monitoring Functions to ON. Again, this seems redundant but is necessary as the first time was to activate from Service mode which allows the page to be visible on the device. This activation allows the administrator to activate RPO for use. a. A word of caution here…the screen can lag and you may select an option a couple of times before the SOP reacts. I accidentally turned RPO off at this point and had to go back to the device to turn it back on as I locked myself out from the laptop. (You’re welcome!) b. Also take note here of the IP address of the device as you will need that to access Web Image Monitor (WIM). Select the blue house Home button at the bottom of the screen. At this point you no longer have to have user’s login to access the device so we will turn off Machine Management in Administrator Authentication Management. 12. Select Settings, then select Machine Feature Settings. 13. Select System Settings, then select Administrator Tools, then select Next to scroll to page 2 of 6 and select Administrator Authentication Management. 14. Select Machine Management and switch to OFF. Select OK and then select Exit. The device will ask if you are sure as it will log you out of admin. Select OK…ALL DONE!!! At this point you should have activated Remote Panel Operation (RPO) and you should be able to enter the IP address of the device into the browser on an IFPD or your laptop if you

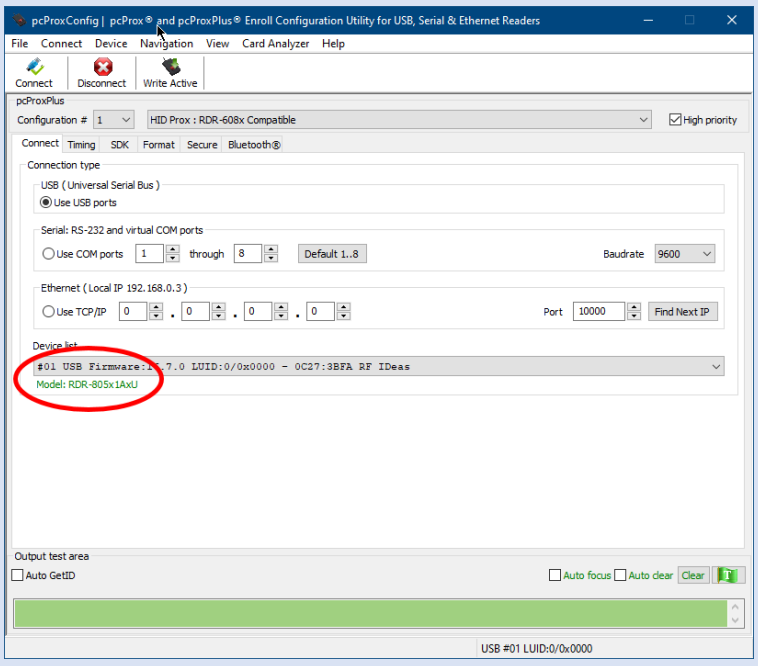
Item	Description
	are on the Ricoh network or on VPN. It may take a couple of times to get it to pick up the device so give it a couple of shots before throwing anything.
H. Disable AirPrint	Disable AIRPRINT option using the User Tools/System settings OR Printer Service Menu > SP 1-001-012 > Bit Switch C > Bit 6 = “1” (Default is “0”)
I. Enable TELNET	SP 5828-090 > set to “1” (Enable Telnet) 
J. Confirm/Enable SNMP settings	SNMP v1/v2 for IPv4 networks must be Set to “Active”
K. HDD Encryption ** This applies to all devices with HDD installed, including Single Function printers	Enable and complete HDD Encryption 1. Enable HDD Encryption using SP 5-878-002 a. Newer models may have this enabled already b. Required step for machine models with HDD Encryption on SD card 2. Login as machine administrator at device panel 3. Go to User Tools > System Settings > Administrator Tools > Select Machine Data Encryption Settings > Select Encrypt > Select “Format all data” 4. Print “Machine Data Encryption Key” page and hand it over to site IT contact for safe keeping a. This printed page with encryption key can be safely shredded for security. It can be reprinted any time by a machine administrator 5. Restart the machine when prompted to start machine encryption process 6. Confirm all data on machine is encrypted when the process is done a. This may take a few hours. If leaving the machine, put a sign on the machine “Work in progress > DO NOT power off this machine” b. When complete, restart the machine as prompted c. Confirm HDD Encryption is now working > see the picture below

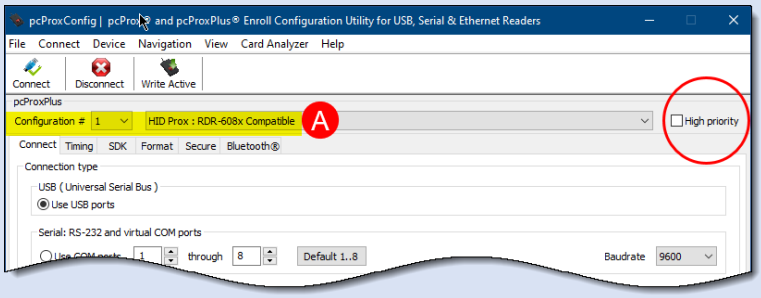
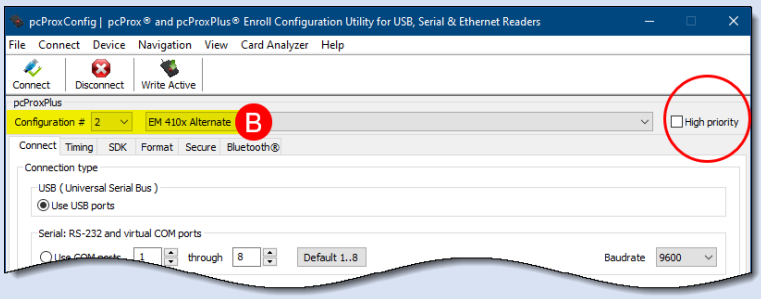
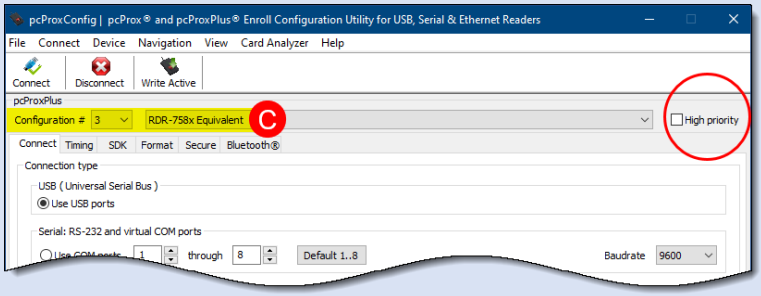
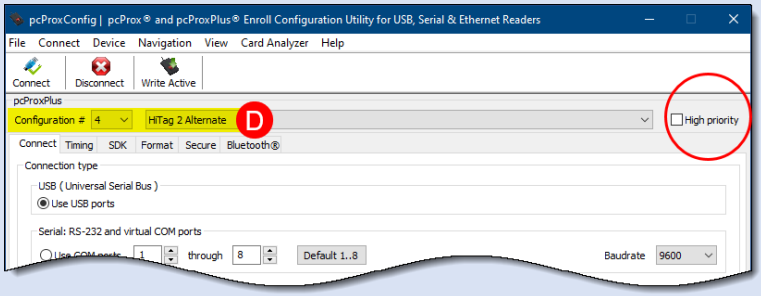
Item	Description
	
L. Install the card reader * This does not apply to Single Function printers	For IM C300/C400F, IM C4500/C6000, IM 350F, IM 4000/5000 devices only 1. Install the reader using short 6” mini-USB cable on the mini-USB port on the right side of the display panel. 2. Use Card reader mounting kit Type M37 where applicable OR affix the reader on a flat surface on Right side of the MFP using provided Velcro strips (see pictures below)   

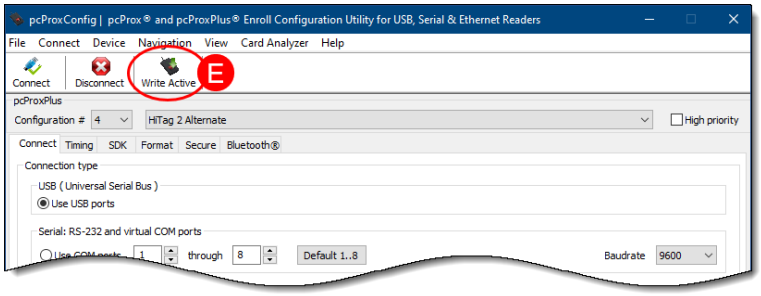
Item	Description
	For MP 4055/5055, MP 305 devices only 1. Install the reader using 6’ long normal USB cable and plug it in the USB port on the rear panel of the device. 2. Use Card reader mounting kit Type M37 where applicable OR affix the reader on a flat surface on Right side of the MFP using provided Velcro strips (see pictures below)   **Note:** Save all cables that came with Reader with the machine or hand it over to customer contact for safe keeping. Customer or field technician may need these cables in the future.
M. Program the card reader	RFIdeas RDR-805R1AKU reader shipped with the MFP unit should already be programmed for Parker Hannifin use. If it is determined that the reader is not programmed OR cannot read customer badges, it MUST be re-programmed using directions provided on next page. **Note:** 1. Some Parker sites have unique badge types in use and may require site specific reader program. In such cases, a. Please contact the site IT admin first before using the configuration file provided here and get the site-specific reader configuration file b. Card reader re-programming process remains the same. 2. This is for MFPs only. 3. It does not apply to Single Function printers
N. On Board USB * ONLY applies to Single Function Printers	1. SP-5985-002 Set to “0” Disable

Program RFIdeas RDR-805R1AKU Card Reader

Use the following process to program the USB card readers on all Secure Print/Scan enabled (Streamline NX) MFP devices for Parker Hannifin Global Deployment project. The instructions are for Ricoh CC use as well as Ricoh field service technicians or customer site IT admins, when applicable and/or required.

Process details	Guidance
1. Find a file named "Parker_Badges_12082020.hwg+" along with this instructions and save it on your PC	Press CTRL + Click on the "Click here" picture below to download the card reader configuration file named > "Parker_Badges_12082020.hwg+" CLICK HERE
2. Download and install PC Prox Config tool → on a Windows PC	https://www.rfideas.com/sites/default/files/2020-07/pcProxConfig-5.3.3_0.zip
3. Disconnect the PCProx Plus card reader from MFP. • *Note the MFP port where it is/was connected. You will use the same port to reconnect it to MFP later in this process* • *For Ricoh CC > this step may not be necessary* 4. Plug in the card reader to an available USB port on your laptop • *You do not need to power off the MFP* • *MFP Users may continue using it with manual login or pin code login methods, until the reader is programmed and connected again* 5. Launch pcProxConfig.exe 6. The RED LED light on the card reader will turn ON 7. Click on Connect 8. At this point you will see the screen on right and Under Device List section, now should read Model: RDR-805x1AxU	

Process details	Guidance
9. Click on File > Select Open hwg/hwg+ file 10. Locate and select file "Parker_Badges_12082020.hwg+" (from step 1) 11. Click Open 12. IMPORTANT > Wait for the screen to refresh and confirm the changes as detailed below.	
13. Note the settings values changed and confirm • Configuration #1 should read "HD Prox : RDR-608x Compatible" (A as shown in picture) and High priority checkbox is Unchecked • Configuration #2 should read "EM 410x Alternate" (B as shown in picture) and High priority checkbox is Unchecked • Configuration #3 should read "RDR-758x Equivalent" (C as shown in picture) and High priority checkbox is Unchecked • Configuration #4 should read "HiTag 2 Alternate" (D as shown in picture) and High priority checkbox is Unchecked	   

Process details	Guidance
14. Click on “Write Settings” icon (E as shown in picture) • Red LED on Card Reader will blink for a few times • A message at the bottom of the screen will say “Writing to device” for a few seconds and then “Writing to device … Done” 15. Desired settings are now saved on the card reader	
16. At this point, disconnect the Card Reader from laptop 17. Reconnect to the USB port on MFP panel again and secure to MFP using the Velcro strip • *You may have to use short cable with mini-USB connector* • *There is no need to restart the MFP* 18. Before leaving, test a card (badge) with the help of customer site contact • When you swipe access badge or a key fob, the MFP will prompt to register the badge/fob • Login manually with user’s network ID and password to register the badge/fob 19. All new users will have to register their badge/fob once this card reader is reprogrammed	