Important Notification

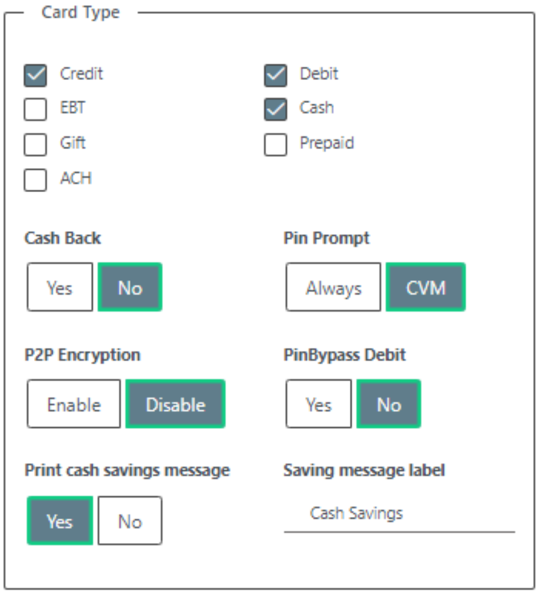
Dejavoo
Payment Software Solutions

IPOSPAYS P2PE Notification Advisory

Dear Valued IPOSpays Customer,

We are committed to uphold the utmost security standards for our services. Accordingly, we have implemented multiple levels of security on servers and on terminals. During our routine security monitoring, we discovered that some Dejavoo Gateway powered terminals were Point to Point Encryption disabled and/or not activated for the service ("P2P Encryption" and "P2P Key") due to incorrect configuration in the TPN parameters, such as:

- Edit Parameters Module -> Transaction Tab -> Card Type -> P2P Encryption -> **Disabled**



Card Type

☑ Credit ☑ Debit
□ EBT ☑ Cash
□ Gift □ Prepaid
□ ACH

Cash Back: Yes [✓ No]

Pin Prompt: Always [✓ CVM]

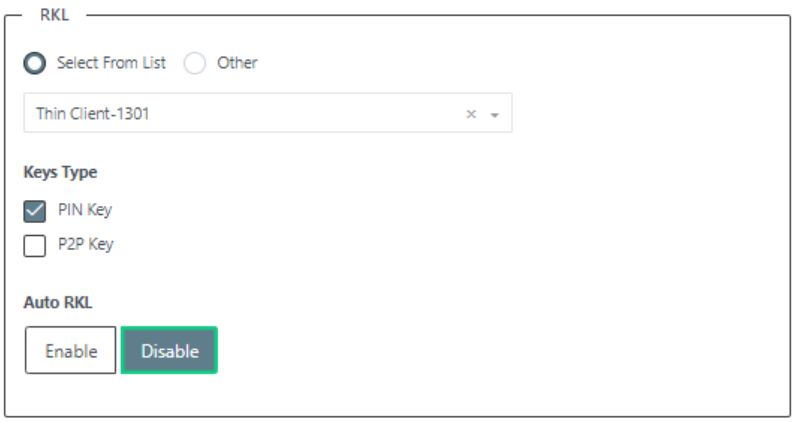
P2P Encryption: Enable [✓ Disable]

PinBypass Debit: Yes [✓ No]

Print cash savings message: [✓ Yes] No

Saving message label: Cash Savings

- Edit Parameters Module -> Miscellaneous Tab -> RKL ->
  1. Incorrect **Device Group name**
  2. **P2P Key** Disabled
  3. **Auto RKL** Disabled



RKL

● Select From List ○ Other

Thin Client-1301

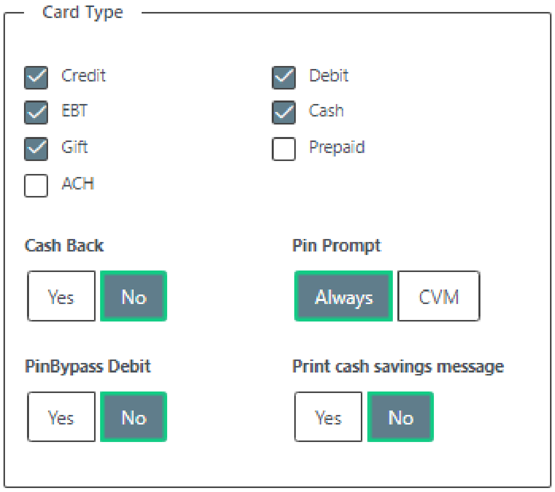
Keys Type

☑ PIN Key
□ P2P Key

Auto RKL: Enable [✓ Disable]

We have promptly addressed this matter by taking corrective measures to rectify the configuration errors on your behalf, on the affected devices:

- We changed the P2P Encryption configuration to be a back-end parameter enabled by default, limiting possibilities of incorrect set up on the TPN parameters



Card Type

☑ Credit ☑ Debit
☑ EBT ☑ Cash
☑ Gift □ Prepaid
□ ACH

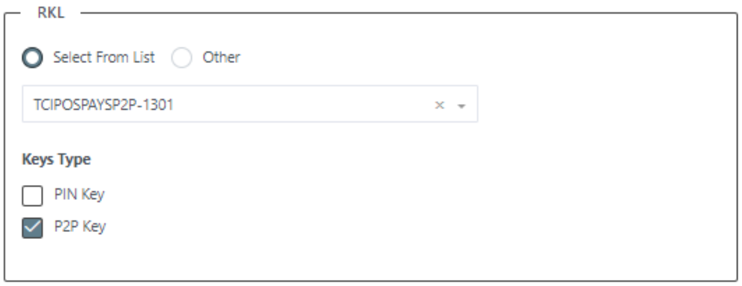
Cash Back: Yes [✓ No]

Pin Prompt: [✓ Always] CVM

PinBypass Debit: Yes [✓ No]

Print cash savings message: Yes [✓ No]

- We enabled all Gateway powered serial numbers, including devices ever shipped and downloaded, to have access to the P2P Encryption on the RKL Server.
- To correct terminals that are already deployed in the field, we are identifying and correcting the parameters to ensure these devices will download the proper settings and P2P Encryption Key.
- Terminals that are already deployed, based on our corrections, will automatically pull a parameter update that will trigger the device to initiate the Remote Key Load (RKL) , procedure which is the final correction to the issue.
- We have defaulted our portal for new TPNs created to have the correct configuration for P2P Encryption only devices. The following changes were applied: we have added our P2P Encryption Group Name to the list and made it the default selection, we also enabled the P2P Key, disabled the Pin Key selection and lastly, **we configured Auto RKL to be a back-end parameter defaulted to "Enable"** to ensure all the devices will complete the RKL process upon download (see image below for reference).



RKL

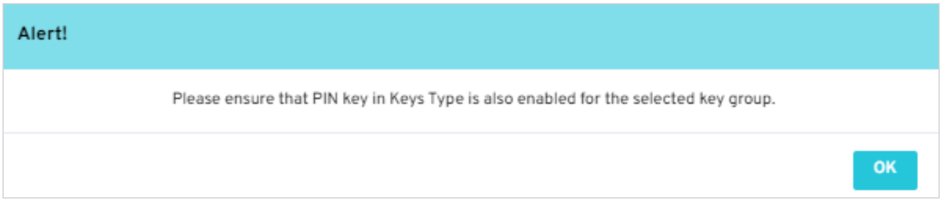
● Select From List ○ Other

TCIPOSPAYSP2P-1301

Keys Type

□ PIN Key
☑ P2P Key

- We have implemented a pop up warning message that will trigger when the defaulted Group Name is altered to ensure that terminals that require a Pin Debit Key injection will be properly configured, see image below for reference:



Alert!

Please ensure that PIN key in Keys Type is also enabled for the selected key group.

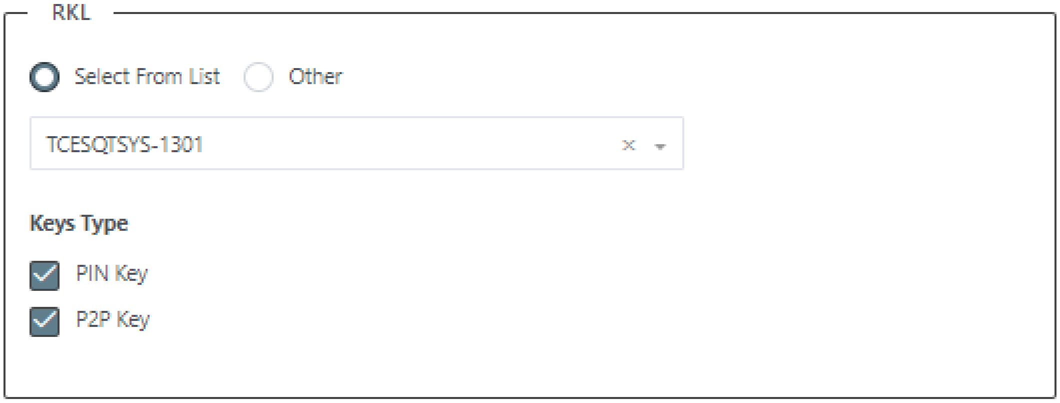
In the scenario that the device does not require a Pin Debit Encryption or if the Key Injection is being handled locally, and the selected Device Group Name does not contain the initials TC, the current default settings should not be changed or modified.

Adding Pin Debit Encryption Keys:

In the scenario that the device requires a Pin Debit encryption, the TPN parameters should be configured as shown below (in the example below, Device Group Name TCESQTSYS-1301 is used for reference purposes only).

Edit Parameters Module -> Miscellaneous Tab -> RKL:

- Select desired **Device Group Name** from the list or add it from the “Other” section
- **Enable** Pin Key Checkbox
- **Enable** P2P Key Checkbox



RKL

● Select From List ○ Other

TCESQTSYS-1301

Keys Type

☑ PIN Key

☑ P2P Key

We wish to reassure you that, to date, no security incidents or concerns related to this matter have been reported. Consequently, the only action required on your end is to train your boarding and data entry personnel and ensure they are adhering to the instructions outlined in this document.

We thank you for your continued trust in our services. Should you have any questions or require further assistance, please do not hesitate to contact our customer support team.