Add: 8255 E Raintree Dr
Scottsdale, AZ 85260
Phone: 480-425-2222
Email: info@rpower.com

PA-DSS 3.2 Validation & PCI Implementation Documentation

For RPOWER POS Version 19110001
Last Updated: March 25th, 2019

Since 1995, RPOWER has always been protective of cardholder data. It has never stored credit card PANs, expiration dates, and track data unencrypted. It has always formatted its receipts to be secure according to the strictest requirements of the time.

RPOWER Restaurant POS Version releases 2008, 2009 and 2010 adhere to the PA-DSS 1.2 guidelines. RPOWER POS Version 2014 adheres to PA-DSS 2.1 Guidelines. RPOWER Restaurant POS release 2017 and higher, adhere to the PCI Security Council PA-DSS 3.2 guidelines and beyond. Furthermore, we can identify the following specific statements about credit card security and cardholder information with regards to RPOWER Restaurant POS.

PA-DSS 3.2 Implementation Guide for RPOWER System Networks

In addition to the security measure implemented by RPOWER in Version 2017, the following guidelines are PCI recommendations to further secure all data at each location.

Additional information on each of the following topics can be found in the **PCI Data Security Standard** documentation located on their website at:

https://www.pcisecuritystandards.org/

Remove Potentially Sensitive Historical Information

RPOWER securely deletes all previous existing historical sensitive data in its database, however previous "Daily Zip"(*.zip) and log files (*.txt) created by Versions previous to RPOWER 2008 must be deleted to remove all potentially sensitive information to maintain PCI compliancy. A known secure removal of these files is absolutely necessary to meet PCI DSS compliance.

Potentially sensitive historical files (*.zip and *.txt) are typically located in the following directories on the RPOWER File Server and Alternate Server Systems:

Daily Zips:	C:\SYS\ARCHIVE
System Logs:	C:\SYS\RPOWER\WINRUN\Logs
Keystroke Logs:	C:\SYS\RPOWER\WINRUN\Logs\Keys

RPOWER recommends the use of SDelete for the removal of these files. SDelete is available for download at:

http://technet.microsoft.com/en-us/sysinternals/bb897443

Once downloaded, place the SDelete.exe file in the C:\Windows\System32 directory of the local workstation. Using a command prompt you may delete the desired files with the syntax:

Sdelete –p 7 –q C:\SYS\ARCHIVE**.zip

Sdelete –p 7 –q C:\SYS\RPOWER\WINRUN\Logs*.txt

Sdelete –p 7 –q C:\SYS\RPOWER\WINRUN\Logs\Keys*.txt

RPOWER advises that the above steps be taken to delete any historical cardholder data when no longer required for legal, regulatory, or business purposes.

Any cardholder data no longer needed (as defined by the customer) must be securely deleted.

Procedures For Prevention of Cardholder Data in System Backup/Restore Points

Run regedit.exe as administrator.

Navigate to:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup

Add a new multi-string value named "RPOWER". Edit the value to include the base RPOWER install directory on the hard drive (typically c:\sys, do not use the mapped or subst'ed drives. Append *.* /s to apply it to all files in all subfolders. For example:

c:\sys*.* /s

When done there, navigate to:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot

Add the same key there.

Make sure to do this on the file server and on any machine that is setup as a backup workstation.

Procedures For the Retrieval of Logs, Databases, and Keystores

All folders are relative to the RPOWER drive (typically R: which is substituted or shared from the file server's C:\SYS).

1. The working database can be retrieved by copying the dbf files from "\RPOWER\DATA\".
2. Archives of previous days' backups are found as zip files in "\ARCHIVE\" under folders named using the following format: ymmMON. For example, 608AUG is August of 2016. This folder may also hold the current training database and any Pre-Update backups (under "TRAINING" and "Previous Updates" respectively).
3. RPOWER logs are located in "\RPOWER\WINRUN\LOGS\". This entire directory should be taken in the case of a full recovery..
4. Keystores can retrieved by backing up the "\RPOWER\WINRUN\INI\" folder. This folder should be taken in entirety as well.
5. Windows event logs can be backed up in the following manner:
    a. From "Start", go to "Run", and enter and launch "eventvwr.msc".
    b. On each section listed under "Windows Logs" (for example "Application" or "System"):
        i. Select that section by clicking on it.
        ii. Select "Action" and select "Save All Events As…"
        iii. Name the file appropriately.
        iv. Chose "Display information for these languages" and select your language. Hit "OK".

Access and Storage of Sensitive Card Holder Data

For existing RPOWER customers upgrading to PCI-DSS 3.2 validated software, RPOWER Version 2014 or newer:

RPOWER does not allow for open recovery of encrypted cardholder data regardless of user privilege levels in RPOWER under any circumstances. Request for cardholder PAN information can be made to RPOWER Holdings LLC. through your local RPOWER dealer. All requests must be accompanied by: the reason for submittal along with requesting individual full name and contact information. The request will be processed within 24 hours of notification in most cases.

Cardholder PAN data once provided to the site must:

- Be stored only in specific, known locations with limited access.
- Be limited to the amount needed to solve a specific problem.
- Be securely deleted immediately after use using SDelete.

Collection of Sensitive Authentication Data is never allowed by the end user for any means. In any attempts to do so all files, records, and storage of such transactions must be deleted securely using SDelete. All instances of Card Holder Data stored by RPOWER can be found in:

C:\SYS\RPOWER\DATA\ICT.DBF.

In specific circumstances during support, testing, and troubleshooting of system components where sensitive data is collected or accumulated the user must ensure:

- Collect sensitive data only when needed to solve a specific problem
- Collect as little of these data as necessary to solve the specific problem
- Store these data only in specific, known locations with limited access
- Encrypt these data when stored
- Be securely deleted immediately after use using SDelete.

Instances of Card Holder Data

RPOWER never prints or displays a full credit card PAN number to anyone under any circumstances, regardless of their access permissions in RPOWER.

RPOWER does print and/or display the first six and last four of card holder data in the below listed instances within the RPOWER POS Application:

- On a Customer Copy of the Authorization Receipt (Last 4 only)
- On the Merchant Copt of the Authorization Receipt (First 6 and Last 4)

- In the Payment Window for a specific check within RPOWER POS
- On RPOWER Close Day Reports under the Credit Card Detail Section: RPOWER displays the (First 6 and Last 4) of each credit card transaction processed throughout the business date. – Copies of these reports are located in ..SYS\RPOWER\Winrun\Reports
- In Paid Check Review Window for a specified Check with a credit card payment attached (First 6 and Last 4) within RPOWER POS
- In RPOWER System Logs (First 6 and Last 4) – Located in ..SYS\RPOWER\Winrun\Logs
- In any database file instance of ICT.DBF, ICH.DBF, and ICSICT.DBF in plaintext (First 6 and Last 4) – Located in: C:\SYS\RPOWER\data\ or Database Backup locations C:\SYS\RPOWER\BACKUP or C:\SYS\ARCHIVE\

Customer Options Regarding Card Holder Data

RPOWER never prints, displays or outputs the full credit card PAN number to anyone under any circumstances, regardless of their access permissions in RPOWER. Below are the only configurable options for RPOWER Customers regarding Card Holder Data:

Obscured Card Lookup

RPOWER does store fully encrypted PAN data for retrieval using obscured card number entry, which means entering the first six and last four digits of a card number, with X's in between. All Track 2 and AVS data is deleted after the initial card authorization is processed. CVC data is never stored.

After settlement, you may still use obscured card number entry (defined below) to retrieve credit card PANs and expiration dates (as if manually keyed) for up to 10 days (two full weekends prior to any given Monday). The default retention period is 10 business days and can only be configured by modifying the RPOWER.ini file setting ICTDAYS. Please contact RPOWER or your reseller to adjust this setting.

RPOWER securely deletes all cardholder information beyond the ICTDAYS parameter setting: Post batch settlement on the final ICTDAYS day, RPOWER writes random bytes to the records to be deleted then flushes the file to disk, the process is repeated five times and finalizes with deleting the targeted records.

You can turn off the ability for obscured card lookup by setting ICTDAYS=-1

Obscured card number entry means that if original the credit card number is, for example, 4003 0101 2345 6780, then:

- 400301xxxxxx6780 will print on merchant copies and reports.
- xxxxxxxxxxxx6780 will print on customer copies, and, optionally, merchant copies.
- With manager approval, you now can enter it (with the Enter CC# button) as 400301XXXXXX6780. If this card was used within the last ICTDAYS days, RPOWER will find it and prompt for confirmation of use.

Obscured card number entry covers only the ability for RPOWER users to retrieve cardholder PAN data at the location for subsequent recovery and error correction, using the restaurant's own 128-bit AES encryption keys through RPOWER software only.

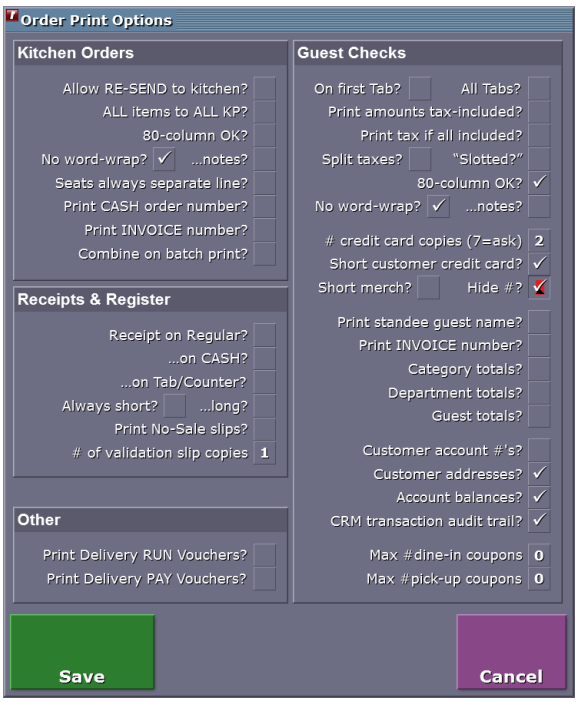
It is important to note that RPOWER still keeps daily Zips going back up to 1200 days (by default). Credit card information in these files (and the 200-day 911\DATA backup archive) is protected by 2,048-bit RSA public key encryption and recoverable only by RPOWER Holdings LLC.

Receipt Masking to Display Last 4 Only

RPOWER by default prints the First 6 and Last 4 of Card Holder PAN on the Merchant Copy of Authorization Receipts and only the Last 4 of the PAN on the Customer Copy of Authorization Receipts.

This setting can be changed to enforce RPOWER to print the Last 4 of Card Holder PAN on both the Merchant Copy and the Customer Copy. With the proper credentials, in RPOWER POS:

Enter Manager Functions, select System Setup, select Order Print Options, Place a Check Mark in “Hide #?”, select Save.



RPOWER Cryptography and Key Storage

All site encryption keys are managed and encrypted before being stored within the RPOWER POS application. RPOWER POS users have no knowledge nor access to key storage and are not expected nor obliged to maintain key storage in any way. RPOWER limits the locations where all key data is stored to the fewest locations necessary and strongly advises all merchants to limit Operating System administrative accounts to the minimum necessary.

"Current day" individual card information is encrypted with 128-bit AES encryption using a site-specific key. All encryption keys associated with the RPOWER data encryption process are managed and maintained solely by the locally installed RPOWER application. Individual site keys are generated using a combination of entropy collection and cryptographic random number generation. This encryption is only present for the day until batch processing where the data is encrypted by the public RSA key. This key is generated using the Microsoft CryptoAPI, is unique as it is generated daily without any user action, and stored in code. There is no means for any user to access these keys. The data is encrypted within the ICT database.

PAN and expiration dates are re-encrypted each day as part of the Close Day process using a 2,048-bit RSA public key from RPOWER Holdings LLC for potential problem resolution and batch reconstruction when necessary. This key pair is generated using the Microsoft CryptoAPI, is unique as it is generated daily without any user action, and stored in code. There is no means for any user to access these keys. The data is encrypted within the ICT database.

RSA estimates these key strengths to be valid until at least 2030. See http://en.wikipedia.org/wiki/Key_size for an overview.

All historical cryptographic material related to sensitive data encryption is automatically destroyed and replaced with new encryption keys during any licensing update. This typically occurs once per month and is mandatory when updating software or making changes to a site's software license. This process is completely managed within the RPOWER application itself and requires no human intervention for completion.

At any time, a site manager with proper credentials may enforce a software license update, and subsequently a crypto-key update, by:

Enter Manager Functions, select System Maintenance, select Enter Site Code, select OK. RPOWER will retrieve a new software license and crypto-key from RPOWER POS Servers through a secure connection.

It is important to note that historical data is encrypted based on a public key. The local RPOWER system does not have the ability/ nor the encryption keys necessary to decipher historically encrypted data. Any requests pertaining to historically encrypted information is managed solely by RPOWER Corporate.

Historical Cryptographic Material

For existing RPOWER customers upgrading to PCI-DSS 3.2 validated software, since RPOWER Version 2008 and newer:

RPOWER deletes all previous existing cryptographic data from its database and no longer provides a means of recovering cardholder data from the local RPOWER installation regardless of local user access levels upon completion of an RPOWER Software Update.

User Passwords and Logins

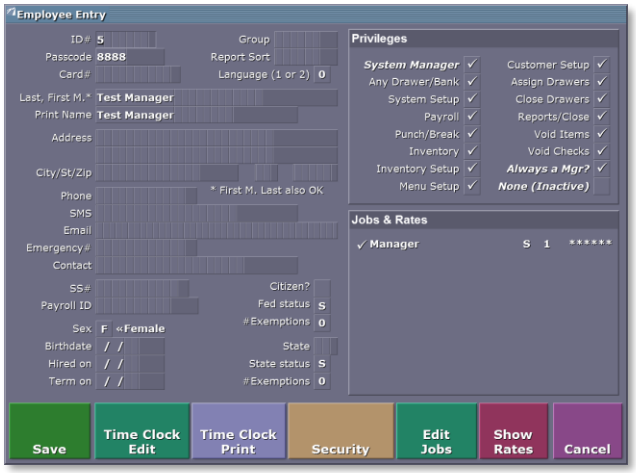
RPOWER POS ships with a single pre-configured default user account for user setup. Upon installation of the application, it is required that new administrative users are created.

There are no users within the RPOWER payment application that allow for access to unencrypted card holder data, nor ability to change any configuration options that would impact the access or security of cardholder data.

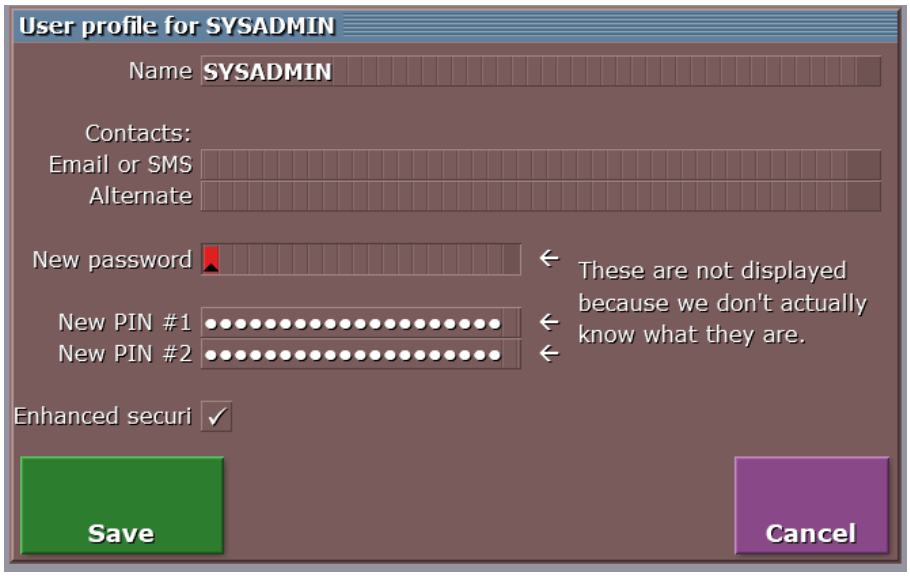
RPOWER POS User Security

RPOWER by default prohibits access to the local Windows desktop environment to any non-elevated users. These users are defined as a PCI User in RPOWER Employee Setup.

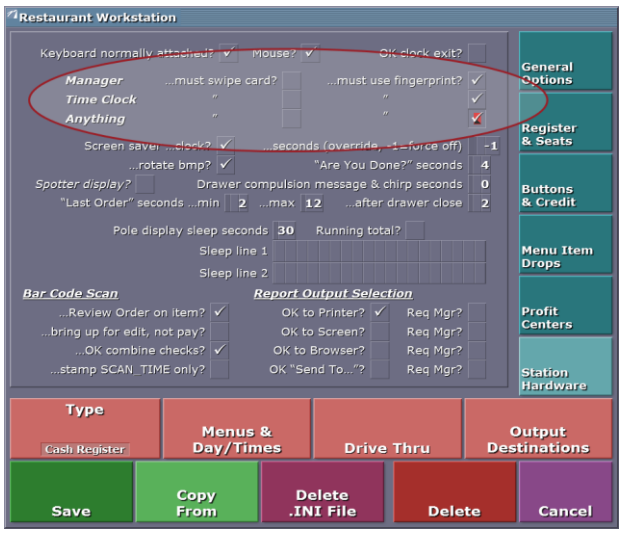
To configure a PCI user in RPOWER edit the appropriate employee profile and select the "Security" Button:



Under the Security button; edit the user security fields. RPOWER will use the Email or SMS and Emergency fields for password recovery. Password recovery is only permitted with successful confirmation of matching PIN#1 and PIN#2 set for this user profile.



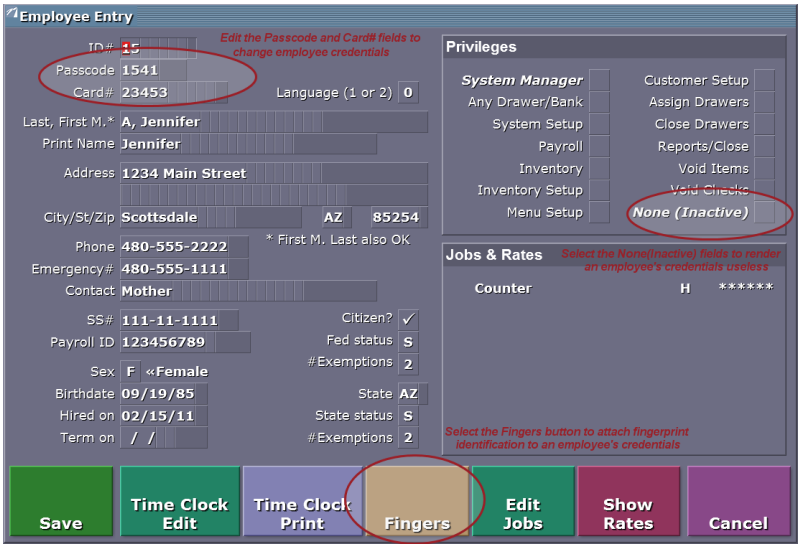
Your RPOWER system may be configured to accept employee biometrics to grant user access. To configure RPOWER to require fingerprint access:



In Workstation Setup (shown above) – Select the …must use fingerprint dialogue boxes to require employee access for your RPOWER system.

Alternatively, your RPOWER system may be configured to accept employee 4-6 digit passcodes or individually assigned magnetic swipe cards to grant user access. Adhere to the following rules when assigning employee passcodes.

- Do not allow employees to share user IDs.
- Change employee passcodes every 90 days.
- Immediately edit terminated employee files to an "inactive" status to revoke all RPOWER application privileges.



RPOWER Employee Entry window provides configuration access for employee id, passcodes, and magnetic card & fingerprint association.

Minimum Session Security for Windows Network Authentication

RPOWER used in a multi-terminal setting requires the use of stronger authentication mechanisms for Windows shares.

This can be set by running gpedit.msc (or searching for "group policy editor" and running it there) and navigating to Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security options.

Then, on the right, scroll down in the list to the section that starts with "Network Security: ".

On both "Minimum session security for NTLM SSP based (including RPC) clients" and "Minimum session security for NTLM SSP based (including RPC) servers", check "Require NTLMv2 session security" and uncheck "Require 128-bit encryption".

Windows User Accounts

While RPOWER POS operates in a Non-Administrative Windows User-mode, it does require the initial installation to be performed by an Administrative User.

RPOWER recommends the use of complex passwords for your windows environment, networking components, and other non-RPOWER applications. A complex password is more resistant to an external attack and almost impossible to guess. These passwords are made up from a series of upper case letters, lower case letters, numbers, and special characters. Example: A7&nj36*Y

RPOWER recommends the following system wide settings for local password security:

1. From "Start", open "Control Panel", change the view to "Large" or "Small" if needed and run "Administrative Tools".
2. On "Local Security Policy", right click and "Run as Administrator".
3. Under "Account Policy", then "Password Policy", set the following settings:
    a. Enforce password history: 24 passwords remembered.
    b. Maximum password age: 90 days
    c. Minimum password age: 3 days
    d. Minimum password length: 9

e. Password must meet complexity requirements: Enabled

f. Store passwords using reversible encryption: Disabled

Creating user accounts:

1. From "Start", open up"Control Panel".
2. Select "User Accounts",
    a. Select "Manage user accounts".
    b. Select "Add…."
3. Fill in the box with the new user name and assign the appropriate permission level. Auto logon, if enabled, should only be selected for a standard (non-administrative) users.
4. Click "Create Account".

Finally, make sure users are not exempt from password change:

1. From "Start", select "Run", and launch "lusrmgr.msc".
2. Under "Local Users and Groups (Local)" select the "Users" folder.
3. For each user, double click their name and uncheck "Password never expires" and then hit "OK".

Installing RPOWER with a Non-Administrative User

RPOWER requires administrative privileges for one time registry and startup changes during the initial installation of RPOWER POS on each workstation:

On the RPOWER System Data Server:

Log in as a Non-Administrative User:

- Run the provided RPOWER installer. Install to the C:\SYS directory.
- Open an administrative command prompt and enter the Administrative Password.
- From the administrative command prompt, run "C:\SYS\RPOWER\WINRUN_Make_File_Server.wsf"

- Set C:\SYS as the root of the RPOWER directory and R: as the RPOWER drive letter.
- Still in the administrative command prompt, substitute the R: drive (type the command "subst r: c:\sys").
- Run r:_RPOWER.wsf
- Exit the command prompt and restart.
- Future forward, RPOWER will launch automatically with the Start of Windows.

On any additional RPOWER stations:

If additional stations will be used as part of the RPOWER system, share the C:\SYS folder from the RPOWER Data Server, enable with read/write access given to the Non-Administrative user(s) from each additional RPOWER station. *Note: Under "Specific People" these users should show as "Owner".*

Log in as a Non-Administrative User:

- Open an administrative command prompt and enter the Administrative Password.
- In the administrative command prompt, map the R: drive to the folder shared on the file server (for example: "net use r: \\filesvr\SYS").
- Enter in the credentials of the Non-Administrative user on the file server.
- Run r:_RPOWER.wsf
- Run net use /d r:
- Exit the command prompt and restart.
- Future forward, RPOWER will launch automatically with the Start of Windows.

Auto Login

It will typically be desired for the POS machines to boot directly to RPOWER. In order to do this with a password protected user account, auto login will need to be setup. If punching in a password at boot time is not an issue or is desired, this step can be skipped.

- Press Win+R to bring up the Run dialog. Enter in and run "control userpasswords2".
- On the "User Accounts" screen that pops up, highlight the POS system user so it's blue and uncheck "Users must enter a user name and password to use this computer".
- When you hit ok, it will ask you to confirm the password for that user. Do so and hit ok again.
- Now reboot. When the system comes back up this user will be logged in automatically.

RPOWER System and Keystroke Logging

RPOWER by default, upon installation, logs all system activity via keystroke logging and application logging. This includes the follow system activity:

- All actions by users with administrative privileges as assigned in the application.
- Access to audit trails managed by or within the application
- Invalid logical access attempts
- Use of, and changes to the application's identification and authentication mechanisms (for example users account creation, user privilege escalation, etc.), and all changes, additions, deletions to application accounts with root or administrative privileges
- Initialization, stopping or pausing of the application audit logs
- Identity or name of affected data, system component, or resource
- Creation and deletion of system-level objects within or by the application

Additionally, RPOWER collects and logs:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event

All logs related to credit card swipes and manual entries are obscured in a non-recoverable manner. RPOWER does not offer functionally to disable its logging capabilities. Credit Card activity logs are located in C:\SYS\RPOWER\Winrun\Logs\CC

RPOWER system logs are stored in C:\SYS\RPOWER\Winrun\Logs and track system operations, errors, and high-level user activity. This includes each attempt to access the Manager Functions area of RPOWER.

RPOWER workstation logs record ALL user activity within the RPOWER application via means of a keystroke log. Whereas the entire activity of a given RPOWER workstation can be rebuilt step-for-step as the original actions were performed. These files are stored in C:\SYS\RPOWER\Winrun\Logs\Keys.

Further detailed logging for generic types of activity for the intent of troubleshooting and support can be enabled by adding anyone of the following line items to the C:\SYS\RPOWER\WINRUN\INI\RPOWER.INI file and restarting the RPOWER POS application:

K3LogDB_DEV=0x03; logs all device communication activity

K3loghttp=1 ; logs all http traffic

K3logsmtp=1 ; logs all email services

The resultant logging detail will be added to the standard RPOWER System logs or in some cases a unique log file with be created in C:\SYS\RPOWER\Winrun\Logs

RPOWER POS Versioning Methodology

RPOWER POS is released with a Master Version moniker (eg. RPOWER 2019) with a specific build version (eg. 191XXXXX.), where:

The **Master Version** is the first two digits of the version number. This number increments annually to match the last 2 digits of the release year. This part of the version is not a part of the versioning hierarchy. The **Master Version** increments independently from the **PA-DSS Validation Number**.

The RPOWER **PA-DSS Validation Number** increments with any developmental changes that impact the security, transmission, handling, storage, or interaction with middleware pertaining to cardholder data.

- The first two digits reference the **Master Version** (19)

  Eg. **19**131210

- The third digit references the **PA-DSS Validation Version**(1) within the Master Version.

  Eg. 19**1**31210

The remaining five digits of the RPOWER POS application represent changes to the software application that do impact the security, transmission, handling, storage, or interaction with middleware pertaining to cardholder data.

- The fourth digit references **Non-PA-DSS Security Version** (3) within the Master Version.

  Eg. 191**3**1210
- The fifth and sixth digits references the **RPOWER Database Version** (12),

  Eg. 1913**12**10
- The final two digits (seven, eight) reference the RPOWER **Functionality Version** for non-security/PA-DSS impacting items (10).

  Eg. 191312**10**

The **Non-PA-DSS Security Version** increments with any developmental changes that impact the security components of RPOWER *not* related to the transmission, handling, storage, or interaction with middleware pertaining to cardholder data.

The **Database Version** increments with any changes or additions to the local RPOWER Database structure.

The **Functionality Version** increments with minor updates that do not affect database, PA-DSS, Payment Engine, or Security changes.

Wireless Networking Environments

RPOWER does not come bundled with wireless connectivity.

RPOWER uses the utmost security protocols when transmitting data between its POS terminals, wired or wireless.

The use of network firewalls must be in place to fully segregate any public wireless networks from an RPOWER network in which card holder data is stored, no exceptions.

If implementing a private wireless network for use with handheld and/or remote devices on the RPOWER network, the network must be configured according to

industry best practices (e.g., IEEE 802.11i) regarding strong encryption for authentication and transmission.

The following recommendations should be considered in order to preserve the utmost system security within a wireless RPOWER network:

- Install, use, and maintain a personal firewall on all components using a wireless networking connection.
- Do not use provided defaults in any manner for passwords or users, change all passwords upon termination of anyone with knowledge .
- Do not use the default SSID or broadcast the wireless SSID.
- Do not allow remote management of your wireless networks.
- Restrict access to wireless access points by MAC address only.
- Static assign IP address for all wireless system components. Do not enable DHCP service for access points.
- Physical access to networking components such as wireless access points, gateways and unused handheld systems is restricted from non-essential personnel.
- A minimum WPA2 encryption must be used.
- Change passwords and encryption keys when knowledgeable personnel leave the company.

An unsecure wireless network is a gross security violation and leaves your network extremely vulnerable to outside threats.

Turn on SMB Signing

SMB Signing prevents "man-in-the-middle" attacks and should be turned on everywhere RPOWER is used.

On the file server, perform the following steps

1. Run Registry Editor (Regedt32.exe).
2. From the HKEY_LOCAL_MACHINE subtree, go to the following key:

   System\CurrentControlSet\Services\LanManServer\Parameters
3. Click Add Value on the Edit menu.
4. Add the following two values:

```
Value Name: EnableSecuritySignature
Data Type: REG_DWORD
Data: 0 (disable), 1 (enable)

   NOTE: The default is 0 (disable)

Name: RequireSecuritySignature
Type: REG_DWORD
Value: 0 (disable), 1 (enable)

   NOTE: The default is 0 (disable)
```

5. Click OK and then quit Registry Editor.
6. Shut down and restart.

On all workstations, perform the following steps:

1. Run Registry Editor (Regedt32.exe).
2. From the HKEY_LOCAL_MACHINE subtree, go to the following key:

   \System\CurrentControlSet\Services\Rdr\Parameters
3. Click Add Value on the Edit menu.
4. Add the following two values:

```
Value Name: EnableSecuritySignature
Data Type: REG_DWORD
Data: 0 (disable), 1 (enable)

   NOTE: The default is 1 (enable)

Name: RequireSecuritySignature
Type: REG_DWORD
Value: 0 (disable), 1 (enable)

   NOTE: The default is 0 (disable)
```

5. Click OK and then quit Registry Editor.
6. Shut down and restart.

Turn off Autoplay

USB (and other removeable media) can be used to run unauthorized programs. We advise you turn it off. You can do so by following this procedure:

1. Click Start, type Gpedit.msc in the Start Search box, and then press ENTER.
2. Under Computer Configuration, expand Administrative Templates, expand Windows Components, and then click Autoplay Policies.
3. In the Details pane, double-click Turn off Autoplay.
4. Click Enabled, and then select All drives in the Turn off Autoplay box to disable Autorun on all drives.
5. Restart the computer.

RPOWER Environment Services & Components

RPOWER POS Related Services and Components

Required Proprietary Software

RPOWER POS Version 191XXXXX- RPOWER POS PA-DSS Validated software application

Required Ancillary Software

Windows Operating System Versions:POS Ready 7, Windows 7 Pro, Windows 10 Pro, Windows 10 IoT Enterprise

Protocols & Services used by RPOWER POS

Core Protocol	Application Protocol	Public	Private	Port	Local System	Client Target	RPOWER Use
ICMP ECHO	(Tracert)	Yes	No	None	None	8.8.8.8	Windows tracert.exe executed periodically to locate site's ISP gateway.
ICMP ECHO	(Ping)	Yes	No	None	None	Site's ISP gateway	Ping nearby public IP address to determine if Internet is online.
UDP	DNS	Yes	Possible	53	None	Various	DNS name resolutions;

							details depend on site configuration.
Outbound TCP	HTTP POST XyzzyTalk STAMPCNX (HQDingee) XML	Yes	No	32111	None	rpower.dyndns.org	Time server connects to RPOWER every 30 minutes. Also SITE IP address lookup.
In and Out TCP	None	No	Yes	9101 e.g.	Workstations	Station or device IP	TCP printers; stations pretending to be TCP printers; devices such as video recording systems.
In and Out UDP	KSAUDP	No	Yes	26264	Workstations	Station IP	Station-to-station communication.
In and Out TCP	XMCP XyzzyTalk LSCNX XML	No	Yes	26262	File server	File server IP	Lock Server resource locking system.
Outbound TCP	Daytime per RFC 867	Yes	No	13	None	One from a list of NIST servers	Setting system time on 'time server.'
Outbound TCP	None	Yes	No	80 or 443	None	Various	Check to see if IP address is 'online.' Connection only -- no data transmitted.
Outbound TCP	SMTP	Yes	No	587 typical	None	smtp.rpower.com typical	Sending report and support emails to subscribers listed in email.ini.
Outbound TCP	HTTP GET from FireFox browser	Yes	No	80 typical	None	rpowerpos.com/maps	Delivery zone mapping display and directions.
Outbound TCP	HTTP POST	Yes	No	80 typical	None	rpowerpos.com/addressZone	Delivery address data retrieval.
In and Out TCP	HTTP POST XyzzyTalk CUSCNX XML	Yes	Yes	32112 typical	File server	Site IP	RPOWER Multi-Store Gift and Loyalty.
Inbound TCP	HTTP POST XyzzyTalk POSCNX XML	Yes	No	32112 typical	File server	None	RPOWER Online Ordering.
Outbound TCP	HTTP POST XyzzTalk RFX XML for QBCNX	Yes	No	32150 or 32113 typical	None	rpower.dyndns.org or corp. office	RPOWER File Exchange for QuickBooks.
Outbound TCP	HTTP POST XyzzTalk RFX XML for DATACNX	Yes	No	32150 or 32113 typical	None	rpower.dyndns.org or corp. office	RPOWER File Exchange for SQL Reporting Database.
Outbound TCP	HTTP POST XyzzTalk RFX XML for (Other API)	Yes	No	32150 or 32113 typical	None	rpower.dyndns.org or corp. office	RPOWER File Exchange for backups; menu file imports; etc.

Outbound TCP	HTTP POST	Yes	No	80 (!)	None	Various (!)	Online Certificate Status Protocol (OCSP) performed by Internet Explorer (WinInet.dll) et al.
Outbound TLS	HTTPS POST via WinInet API HttpSendRequest()	Yes	No	443	None	Various non-credit-card gateways	TLSv1.1 or higher; Gift & loyalty plus other non-payment-related services. Will allow for certificate errors.
Outbound TLS	HTTPS POST via WinInet API HttpSendRequest()	Yes	No	443	None	Various credit card gateways	TLSv1.1 or higher; Services with credit card data. Rejects invalid and expired certificates; unknown certificate authorities; revoked certificates.

Optional Additional Software

Datacap (dsiEMVUS, dsiClient, and NetEPay): Local Credit Card Processing Gateway for use with various acquirers - Version 5.06.XX and 5.07.XX

Required Hardware

POS Workstation - running Windows OS versions Win 7 pro, POSReady 7, Win 10 Pro, or Win 10 IoT Enterprise.
Magnetic Stripe Reader - Attached to POS Workstation for collecting credit card data
EMV Reader - Attached to POS Workstation for collecting EMV Chip credit card data

System Libraries

Iphlpapi.lib	IP Helper Functions
version.lib	System version information
Mpr.lib	Windows Multiple Provider Router
PowrProf.lib	Power Profile Helper
Wininet.lib	Internet Extensions for Win32
Ws2_32.lib	Windows Socket 2.0 32-Bit
Winmm.lib	Media Control Interface API
Crypt32.lib	Windows Cryptography API
kernel32.lib	Windows NT Base API
user32.lib	Multi-User Windows API
gdi32.lib	Windows Graphics Device Interface
winspool.lib	Windows Printer API
comdlg32.lib	Common Dialogs
advapi32.lib	Advanced Windows 32 Base API
shell32.lib	Windows Shell Common
ole32.lib	Object Linking and Embedding
oleaut32.lib	OLE Automation
uuid.lib	COM Interface Identifiers

Internet Accessible Systems

Sites utilizing a high-speed Internet connection should implement the following to further secure their network:

- Install and maintain a network firewall.
- RPOWER networks storing card holder data may not be used for direct incoming Internet connections.
- Do not use the RPOWER system or terminals on the network for general Internet activity.

- RPOWER does not facilitate the sending of cardholder data via any end-user messaging technology. It is strongly recommended to not send cardholder information over the Internet via Email, Instant Messaging, or other means unless absolutely necessary. When doing so, use the utmost security precautions to protect the card holder data.

Remote Software Access

The RPOWER POS application does not facilitate the use of a remote access tool.

To meet PCI DSS compliance, all remote access (including RPOWER direct and/or RPOWER Reseller Support) requires the use of a two-factor authentication.

RPOWER by default does not prohibit the use of any two-factor authentication Remote Support Utilities. Further details regarding the proper use of two-factor authentication can be found on the PCI Security Council web site, specifically see PA-DSS Requirement 3.1.4

Remote support utilities installed by the Merchant should never be configured in an "Always On" mode. Any remote support utilities should only be enabled at time of request and immediately disabled upon completion of the remote session.

Any Remote Support Utilities utilized by an RPOWER Reseller/ Merchant or Support Personnel should be:

- Change default settings in the remote-access software (for example, change default passwords and use unique passwords for each customer).
- Allow connections only from specific (known)IP/MAC addresses.
- Use strong authentication and complex passwords for logins (See PA-DSS Requirements 3.1.1through 3.1.11).
- Enable encrypted data transmission according to PA-DSS Requirement 12.1.
- Enable account lockout after a certain number of failed login attempts. (See PA-DSS Requirement 3.1.8.)
- Enable the logging function.
- Restrict access to customer environments to authorized integrator/reseller personnel.

Public Transmission of Secure Data Over The Internet

RPOWER uses the security protocols used within the current Windows OS WinHTTP communications API for transmission of secure data over the Internet and through the use of NetePay/Datacap Software if that is selected.

The security standards of HTTPS post are dictated by the end point provider in compliance with their current PA-DSS standards. Additionally, RPOWER does not facilitate the transmission of secure data for any other purposes.

RPOWER,by default, implements the use of the highest level security protocols available in the supported versions of Windows OS listed. Currently, RPOWER enforces the use TLS 1.1 or 1.2 security protocols.

RPOWER Required Dependent Applications

This Implementation Guide relates to RPOWER POS Version 191XXXXXX RPOWER will review and update this guide annually to adhere to future PCI and PA-DSS guidelines. Contact your local RPOWER dealership for an updated copy of our procedures at least once annually.

For Additional information regarding PCI-DSS 3.1 Validation for RPOWER POS, or additional information on updating your site to comply with PCI regulations please contact your local RPOWER dealership.

RPOWER systems with integrated credit card processing require the following operating systems with the most current service packs and security updates available:

Windows 7, POS Ready 7, Windows 10 with Internet Explorer 10.0 or newer.

Specifically, RPOWER utilizes WinInet/WinHTTP to perform HTTPS post to a given processing provider gateway. Each and every workstation on an RPOWER system establishes its own direct connection to the provider gateway.

Additionally, pending the merchant processing platform used by your location, RPOWER may require the use of the PA-DSS validated credit card processing middleware: Datacap's NetePay Version 5.6.1 or newer.

RPOWER requires port 443 open for secure http transmission.

RPOWER Remote Software Updates

Your local RPOWER system, with proper, secure RPOWER user credentials, has the ability to send a request to RPOWER secure servers over HTTPS for the sole purpose of downloading the latest RPOWER software, once downloaded RPOWER will prompt for permission to execute and install the software update locally.

Prior to any update taking place RPOWER performs a complete system backup on the local network such that a system update reversal may be performed if needed.

RPOWER will not and cannot perform remote software updates without an initiation and request from each site internally prior to execution.

RPOWER POS Policies for Patch and Update Delivery

RPOWER is typically capable of addressing a known problem/vulnerability within 48 hours of notice. Pending the vulnerability RPOWER POS is generally capable of releasing a software update/patch available for implementation within thirty days.

Timely development and deployment of patches to customers

RPOWER POS always maintains a publicly available release of the application in its Version Control System (SVN). This enables the RPOWER POS development team to make swift changes to the application when required within the constraints of the RPOWER Code Review Policy.

RPOWER POS application updates are made available in accordance with the below policies.

Delivery in a secure manner with a known chain-of-trust

RPOWER POS provides its installer package digitally via its own secure servers protected by an Extended Validation SSL Certificate.

RPOWER POS signs all of its executables with a code-signing certificate registered to " RPOWER Point-of-Sale". The current certificate utilizes SHA256 and is valid until 10/5/2019.

All RPOWER POS resellers must utilize individualized, custom credentials to access the website for download.

Integrity testing on target systems prior to installation

RPOWER POS is a digitally signed and certificated application by GoDaddy Secure Certificate Authority – G2. until 10/5/2019.

Automatic Updates

RPOWER POS is capable of updating itself as initiated by the merchant, authorized reseller, or RPOWER corporate personnel. These processes occur in the same manner stated above and maintain the integrity of the deliverable utilizing the same controls.

RPOWER POS Policies for the Availability of the Implementation Guide

Updated copies of this guide are available at https://rpowerpos.com/pos-pa-dss or via email request to info@rpower.com.