



## Aloha POS v6.4 and v6.5 Receive PA DSS Validation!

Payment application software vendors must adhere to the Payment Application Data Security Standards (PA DSS) to ensure they are developing products that are secure and protect cardholder data. Independent security consultants have recently audited Aloha POS v6.4 and v6.5 and Radiant Systems is pleased to announce these versions have been validated as conforming to the PA DSS requirements.

Aloha POS v6.4	Received Report on Validation in February, 2009	Validated against PA DSS v1.1
Aloha POS v6.5	Received Report on Validation in June, 2009.	Validated against PA DSS v1.2

We expect these versions to appear on the list of validated payment applications published by the Payment Card Industry Security Standards Council (PCI SSC) in late June or early July.

As a reminder, previously validated versions of the Aloha POS expire on the following dates:

POS version number:	Validated against PABP/PA DSS version:	Deployment notes:	Current validation expires on:
Aloha v5.3.15	Pre-PABP v1.3	Not recommended for new deployments.	December 2, 2009
Aloha v6.1	PABP v1.3	Acceptable for new deployments.	June 2, 2010
Aloha v6.2	PABP v1.4	Acceptable for new deployments.	December 2, 2010

We strongly encourage you to adopt the most recent market ready Aloha releases as they become available.

Access the following Web site to view the list of validated payment applications and their expiration dates, as published by the PCI Security Standards Council:

[https://www.pcisecuritystandards.org/security\\_standards/vpa/](https://www.pcisecuritystandards.org/security_standards/vpa/)



## New Security Features in Aloha POS and Aloha EDC

Radiant Systems is committed to continuously enhancing our products to increase security and protect cardholders and merchants. With each new release, we include features to proactively meet or exceed the Payment Card Industry Data Security Standards (PCI DSS). In keeping with that commitment, we implemented the following features in Aloha POS and Aloha EDC v6.5:

- To be consistent with PCI DSS password requirements, we are introducing complex passwords for logging in to Aloha Manager and Aloha EDC. The first time you log in, you must change your password to comply with the new requirements.

Complex passwords....

- Must be between 7 and 25 characters in length.
- Must not contain the employee name, nickname, or the employee number.
- Must contain at least one alpha and at least one numeric character, in any desired order.
- Must not be identical to a password used in the most recent X number of times, as specified by the system administrator.

With the introduction of complex passwords in Aloha Back-of-House applications, you will be able to specify:

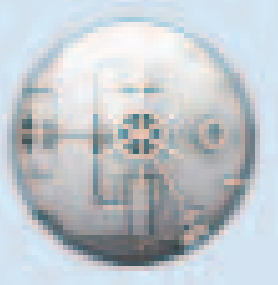
- The number of unsuccessful attempts you want to allow a legitimate user before locking them out.
- The number of days after which an employee must create a new password.
- The number of recent passwords you want to prevent employees from reusing, when they create a new password.
- In an effort to help combat possible security issues, we disabled the keyboard wedge service on POS images available from Radiant Systems. Radiant terminals now provide a more secure way of communicating with the magnetic stripe reader (MSR) through the Radiant MSR interface. **Note:** This feature is not available on the P1210.
- We now incorporate the “secure delete” functionality when automatically deleting files containing sensitive cardholder data, such as the Trans.log, Mirror.log, and spooling files. While the normal command for deleting a file removes the ability for the operating system to find the file, securely deleting a file removes it from the hard drive completely, thus removing the risk of sensitive data being captured via the use of malicious software.



## New Security Features in Aloha POS and Aloha EDC (cont'd)

- Using Radiant Payment Services, you can take advantage of Aloha Payment Guard™, a new point-of-sale feature designed to process all credit card data within a tightly secured environment. Rather than store the sensitive cardholder data in an encrypted format, which meets current data security standards, Aloha Payment Guard takes it further and replaces the sensitive cardholder data with a unique identifier, also referred to as a “token,” immediately after authorizing the transaction and sending it back to the site. Using Aloha Payment Guard, the sensitive data is not stored at the site, thus making it impossible for data thieves to obtain the sensitive data from the site. There are some exceptions to when cardholder data is replaced with a token. Refer to the “Introducing Aloha Payment Guard™ for Protecting Cardholder Data” article for more information.
- EDC now logs off the current user after a specified length of time elapses with no activity by the user. The login screen reappears, forcing the user to log back in to the application. EDC uses the existing screen timeout value specified in Aloha Manager for the back office security level to which the currently logged in user is assigned. **Note:** The maximum length of time a user can be logged in to EDC without activity is 15 minutes, regardless of the time set in Aloha Manager.
- A new EDC Audit Transaction Report is now available on the EDC Reports menu. This report includes the following information for each transaction: Date and time the transaction occurred, the terminal ID from which the transaction was generated, the employee number, the check number, the transaction type, the type of credit card, the card number (masked), the expiration date, and the transaction amount.
- We now insert a message in Debout.txt each time an employee views Debout.EDC from within Aloha Manager. The message includes the date, time, employee number, and path to the logging file that was viewed by the employee.

It is our sincere aim to increase your knowledge and awareness of security related issues. We strongly encourage you to adopt the most recent market ready Aloha release, to stay current with security-related enhancements.



## Introducing Aloha Payment Guard™ for Protecting Cardholder Data

Radiant Systems introduces Aloha Payment Guard™, available when using Radiant Payment Services and Aloha POS and EDC v6.5 and later.

With Aloha Payment Guard, you gain:

- Increased Trust
  - Rest assured that all card data from every credit transaction is processed within a tightly secured environment.
- Ease of Working with One Provider
  - Work with one supplier providing a highly secure and highly integrated payment system. Aloha Payment Guard is a carefully designed point-of-sale feature, not a bolt-on to your technology solution.
- Increased Speed-of-Service
  - Maximize profits with increased speed-of-service. The tight integration that Aloha Payment Guard provides reduces processing time and lets sales happen faster.

Current data security standards require that sensitive cardholder data be stored in an encrypted format. Aloha Payment Guard takes data security a step further and replaces the sensitive cardholder data with a unique identifier, also referred to as a “token,” immediately after authorizing the transaction and sending it back to the site.

### EDC transaction process using Radiant Payment Services:

1. The site enters the credit or debit card into the Aloha POS system.
2. The primary account number is encrypted in the log file (Trans.log).
3. The transaction is sent to an Aloha Payment Guard certified processor for authorization.\*
4. Upon authorization, the processor replaces the primary account number in the transaction file with a token.
5. The site receives the authorization from the processor.
6. The primary account number is removed from the log file (Trans.log).
7. At settlement, the transaction is sent to the processor using the token, not the primary account number.
8. The processor approves the settlement with the primary account number not present in the settlement file.

\*Currently, Aloha Payment Guard is being offered with Radiant Payment Services, which provides enhanced security, high impact solutions, and unmatched service to the merchant processing experience.



## Introducing Aloha Payment Guard™ for Protecting Cardholder Data (cont'd)

### Exceptions to When Processor Replaces Cardholder Data with a Token

A token is issued by the processor for each transaction. The POS supports some transaction types that are not submitted to the processor immediately and these transactions will not contain a token. The transaction types are:

Refund	Performed locally and is not sent to processor until settlement. Authorization is not received from the processor; therefore, the transaction will not contain a token.
Force	Performed locally, sometimes with voice approval, and is not sent to the processor until settlement. Authorization is not received from the processor; therefore, the transaction will not contain a token.
Decline	Can occur without connecting to the processor. Whether the system connects to the processor or not, the processor does not support generating a token. The transaction will not contain a token.
Spooling	While in spooling mode, all transactions occur locally on the POS system and do not connect to the processor. All transactions generated while in spooling mode will not contain a token.

Note: The sensitive card data for these transaction types is always stored in an encrypted format. Your ability to view the full account number in the Audit Report is based on your back office security level.

Using Aloha Payment Guard, you greatly reduce the risk of a data compromise as a result of a security breach. It is impossible for data thieves to obtain sensitive card data from the site because the data is not there!



## Best Practices for Complying with PCI Data Retention Requirements

As a merchant or credit and debit card service provider, you must adhere to the following requirements laid out by the Payment Card Industry Security Standards Council (PCI SSC) with regard to data retention:

- *You cannot* store sensitive authentication data post-authorization. Authentication data includes:
  - Magnetic stripe data
  - Card validation code or value
  - PIN block data
- *You can* store cardholder data post-authorization, but only if it is done in a secure manner, and only if you securely delete it after the retention period required for meeting the business need. Cardholder data includes:
  - Account number
  - Cardholder name
  - Service code
  - Expiration date

The Aloha POS currently supports the onsite requirements by:

- Using secure deletion technology to delete sensitive authentication data automatically when authorizing a transaction and files containing cardholder data that are automatically deleted by the system, such as spooling files, Trans.logs, and Mirror.logs. **Note:** It is up to you to clearly define a data retention policy for each site, and to obtain third-party secure deletion technology. When the defined retention period is over, securely delete files that are not automatically deleted by the system, such as .stl files and Trans.logs that reside on the FOH terminals, based on your data retention policies.
- Using strong encryption algorithms when storing cardholder data.
- Replacing the card number with a unique identifier, or “token,” after authorization, when using Aloha Payment Guard™.
- Purging cardholder data from historical files using the DelTrack utility. The DelTrack utility can be configured to run automatically using the Winhook batch file post-End-of-Day.



## **Best Practices for Complying with PCI Data Retention Requirements (cont'd)**

It is your responsibility to implement policies and procedures to support the offsite requirements. Some best practices you should follow include:

- Ensure only trusted personnel can access sensitive information for troubleshooting purposes.
- Collect this type of information only when it is necessary to solve a specific problem.
- Gather only information that is required to troubleshoot the current issue.
- Use only a secure transfer mechanism when transferring data. We recommend using Aloha Command Center.
- Store the files in specific, known, highly secure areas.
- Use secure delete technology to remove cardholder data from your computer after you troubleshoot an issue.
- Clearly define a data retention policy for each site, and when the defined retention period is over, securely delete the files.

It is of utmost importance that you implement the above best practices to not only ensure you are compliant with the PCI standards, but to also ensure you are doing as much as possible to keep your customer cardholder data safe and out of the hands of data thieves.



## Aloha Command Center Alerts Assist with Security Risks

Aloha Command Center provides alerts to assist you in your efforts to comply with the Fair and Accurate Credit Transactions Act (FACTA) and the Payment Card Industry Data Security Standards. Four new security-related alerts were released with Command Center v3.0, making a total of seven security-related alerts.

### Security risk: Unmasked credit card numbers or expiration dates

FACTA provides that “no person that accepts credit or debit cards for the transaction of business shall print more than the last five digits of the card number or the expiration date upon any receipt provided to the cardholder at the point of sale or transaction.” To be compliant, access Maintenance > Store Settings > Credit Card group > Voucher Printing tab in Aloha Manager, and change your options to reflect the following values:

**Credit Card Number Mask:** Only show last 4 digits (Aloha.ini value equals 2)  
**Suppress Expiration dates:** Selected (Aloha.ini value equals TRUE)

### Credit/Debit card expiration dates are printing on guest check



FACTA requirements state the credit card expiration date cannot appear on any receipt provided to the cardholder. The prior alert notifies you when you are printing the expiration date on the credit card voucher. This alert notifies you when you are printing the credit card expiration date on the guest check. To be compliant, access Maintenance > Payments > Tenders > Type tab in Aloha Manager, and change your options to reflect the following values for each credit card tender:

**Credit Card:** Selected  
**Print Expiration:** Cleared

Command Center continuously monitors these options and displays this alert when a credit card tender is configured to print the expiration date. You can elect to auto-fix this security risk.

### Full credit card numbers are being printed in EDC reports



PCI data security standards require that you protect all stored cardholder data. To prevent unauthorized access to cardholder data, credit and debit card numbers are not available in the EDC reports (EDC > Reports > Review Transactions), by default.

Command Center monitors whether the full card number is available in these reports, and displays an alert anytime it is true. You can elect to auto-fix this security risk.



## Aloha Command Center Alerts Assist with Security Risks (cont'd)

### Unsettled Credit Card Batch (Processor: ProcessorName Oldest TXN: HHMMSS)

When you settle a credit card batch, the .txn files are collected into a .zip file and sent to the processor for settling. Usually, this occurs nightly, but can occur on a less frequent basis, such as every two to three days. This alert is designed not only to let you know when your recent credit card batches have not been processed, but also to make you aware of a possible security risk. For example, it is very common to make backups of .txn files when troubleshooting a credit card issue, and then forget to delete these files when you are done. If these files were created with an older, non-compliant version of the POS, they could possibly contain sensitive card information (have full credit card numbers stored in them). Older .txn files from non-compliant versions of the software are a known security risk. It is valuable for you to know these files exist and to clean them up. If you do not, you may not pass an audit, or worse, if your system is breached and these non-compliant files are found by a forensic auditor, the liability now falls back on the restaurant.

Command Center uses the number of hours specified in Show Last Settlement Alert if More Than \_\_\_\_ Hours Ago in Maintenance > Store Settings > Credit Card group > EDC Setup tab in Aloha Manager to determine the hours allowed between settling your credit card batches. Once a .txn file is older than the value entered here, an alert is sent. The default value for this option is 24 hours. In the case where you process batches every two or three days, you may want to change this value to 96 hours to reduce the number of alerts you receive. Changing the value to 96 will still bring older, non-secure files to your attention, allowing you the opportunity to remove the security risk.

There is no auto-correct available for this alert. We recommend using File Manager to locate the files and securely delete them from the site.

### Security risk: Alt-X password available

To comply with the PCI data security standards, you must not use vendor-supplied defaults for system passwords and you must assign a unique ID to each user with access to the system. To comply with these requirements, we disabled the Alt+X method of accessing Aloha Manager for Quick Service and Table Service, and Aloha EDC. This change is effective for versions 6.3 and later.

Command Center verifies Alt+X is disabled, and if it is not, displays this alert. You can elect to auto-fix this security risk.

When you use Command Center to log in to Aloha Manager at a site, for Aloha POS v6.3 and later, the log file includes the specific name of the user who is logged in to Command Center. The Audit Report found in Command Center includes the specific name of the user who is logged in, regardless of the POS software version installed at the site the user is accessing. This ensures that all actions taken on critical data can be traced to known and authorized users, and the

## Aloha Command Center Alerts Assist with Security Risks (cont'd)

### Remote Desktop is enabled.

Enabling Remote Desktop on Aloha BOH servers, POS terminals, and routers may provide unauthorized users access to the POS system and sensitive cardholder data. Radiant Systems strongly recommends you disable Remote Desktop and use Command Center as your single means of remote access for Aloha POS systems, to ensure the highest level of site security.

Command Center checks the appropriate registry key value and displays this alert if Remote Desktop is enabled. You can elect to auto-fix this security risk.

### VNC may not be secure

VNC (Virtual Network Computing) is a remote access application that allows you to see and interact with desktop applications across any network. PCI data security standards require that you build and maintain a secure network, including ensuring secure remote application access. To meet PCI requirements, you should configure VNC so that it does not accept any inbound connections.

Command Center checks the appropriate registry key value and displays this alert if VNC is accepting inbound connections. You can elect to auto-fix this security risk.

Radiant Systems is dedicated to reducing your security risks and assisting you in your efforts to comply with PCI data security standards. By providing you with new innovative products, such as Command Center, maintaining a secure system is much easier to accomplish!



## Visa Data Security Alert Targets Vulnerabilities in Hospitality Industry

In May, 2009, Visa Business News released a data security alert in which they targeted best practices for the Hospitality industry with regard to protecting cardholder data. The following is a summary of the best practices recommended by Visa:

- Secure your remote access connectivity.
- Implement a secure network configuration including egress and ingress filtering to only allow the ports/services necessary to conduct business.
- Utilize host-based Intrusion Detection Systems (IDS).
- Monitor firewalls for suspicious traffic (particularly outbound traffic to unknown addresses).
- Implement file integrity monitoring.
- Secure systems so that unauthorized software cannot be installed.
- Ensure that all antivirus and antispyware software programs are up-to-date.
- Routinely examine systems and networks for newly-added hardware devices, unknown files, and software.
- Periodically reboot your POS systems to clear volatile memory.\*
- If you detect a suspected or confirmed security breach, notify your acquiring bank immediately.

Each of these best practices directly correlates to one or more of the data security standards mandated by the Payment Card Industry Security Standards Council (PCI SSC). When you configure an Aloha POS system to comply with the best practices outlined in the Aloha POS v6.5 Data Security Handbook, you can feel confident you are putting practices into place that protect you from these targeted vulnerabilities.

\*This is the only vulnerability targeted by Visa that does not directly correlate to a PCI data security standard; however, rebooting your system to clear the volatile memory is always a good practice.

For a full discussion on configuring an Aloha POS system to comply with the PCI DSS requirements, refer to the Aloha POS v6.5 Data Security Handbook.

### Bibliography:

Visa Business News (May 20, 2009) "Data Security Alert – Targeted Hospitality Sector Vulnerabilities" retrieved 06/08/2009 from <http://broadcast01p.visabroadcasts.com/doc/20090519162059/e552fb1cf11de33021b405de32acc0b4>

Acceptance of a given payment application by the PCI Security Standards Council, LLC (PCI SSC) only applies to the specific version of that payment application that was reviewed by a PA-QSA and subsequently accepted by PCI SSC (the “Accepted Version”). If any aspect of a payment application or version thereof is different from that which was reviewed by the PA-QSA and accepted by PCI SSC – even if the different payment application or version (the “Alternate Version”) conforms to the basic product description of the Accepted Version – then the Alternate Version should not be considered accepted by PCI SSC, nor promoted as accepted by PCI SSC.

No vendor or other third party may refer to a payment application as “PCI Approved” or “PCI SSC Approved”, and no vendor or other third party may otherwise state or imply that PCI SSC has, in whole or part, accepted or approved any aspect of a vendor or its services or payment applications, except to the extent and subject to the terms and restrictions expressly set forth in a written agreement with PCI SSC, or in a PA-DSS letter of acceptance provided by PCI SSC. All other references to PCI SSC’s approval or acceptance of a payment application or version thereof are strictly and actively prohibited by PCI SSC.

When granted, PCI SSC acceptance is provided to ensure certain security and operational characteristics important to the achievement of PCI SSC’s goals, but such acceptance does not under any circumstances include or imply any endorsement or warranty regarding the payment application vendor or the functionality, quality, or performance of the payment application or any other product or service. PCI SSC does not warrant any products or services provided by third parties. PCI SSC acceptance does not, under any circumstances, include or imply any product warranties from PCI SSC, including, without limitation, any implied warranties of merchantability, fitness for purpose or noninfringement, all of which are expressly disclaimed by PCI SSC. All rights and remedies regarding products and services that have received acceptance from PCI SSC, shall be provided by the party providing such products or services, and not by PCI SSC or any payment brands.

The Compliance Newsletter is published on a quarterly basis. Channel partners can download a copy of each newsletter from the Reseller Portal. Corporate clients can download a copy of each newsletter from the Corporate User Portal. Also refer to the Aloha POS Data Security Handbook, in these same locations, for detailed information regarding configuring an Aloha system to meet PCI requirements.

While the content in this newsletter has been obtained from sources believed to be reliable, no warranty is provided concerning such content and it does not constitute legal advice. Legal advice concerning specific situations should be obtained by your legal counsel.