

Welcome to Radiant System's Compliance newsletter! The goal of this newsletter is to inform and educate Radiant partners on Compliance related topics. We realize that the task of understanding and staying informed of compliance issues is challenging. We thought a newsletter would be an effective way to provide information bi-monthly, in a simple format geared to any audience. Please feel free to share your comments and questions by emailing ProdMgmt@RadiantSystems.com.



Disabling Alt+X Access to Aloha and EDC in All Versions

In a previous edition of the Compliance newsletter, we announced that the Alt+X method of accessing Aloha QuickService, TableService, and EDC is no longer available, beginning with version 6.3. You can also disable this method of access for all prior versions of these products, and should do so as soon as possible, for PCI DSS compliance. RKS ID 6298 discusses the procedure for disabling this method of access for all versions of Aloha prior to v6.3. Please contact your Radiant representative if you cannot access the Radiant Knowledge System to obtain this document.

Two-Factor Authentication Is Coming to a Site Near You

Data and identity thieves are becoming much more sophisticated in their ability to access systems previously regarded as secure. User name and password are no longer sufficient to prevent unauthorized access to data systems containing cardholder information. To meet these new challenges, stronger techniques are necessary to secure your Aloha network and attached computers. Two-factor authentication is a required method of securing remote access to systems containing cardholder data.



What is two-factor authentication?

Two-factor authentication is the use of two separate methods of verifying the authenticity of an access request. Examples of this type of authentication include providing a user name and a password (the first factor), followed by a touch on a biometric scanner, or having to provide a specific code, typically generated just for a specific session (the second factor). Two-factor authentication involves using two of the following three categories of information:

- *Something you know.* Information in this category includes a user name and password combination, a PIN, or personal information such as a school, family member names, or other information input criteria. This type of information is easily stolen, so it is insufficient for access control, by itself.

- *Something you have.* This can be a mobile phone, a payment card, a 'smart' card, or a hardware security token, such as a USB dongle. Session-specific codes generated by a third party, or 'token' generators are also effective in this area.
- *Something you are.* This type of information is typically a biometric, like a fingerprint or a retinal scan.

The limitations of authenticating across a network or the Internet tend to relate to things we know, or things we have, due to the difficulty of collecting biometric data in this environment.

Why do I need to use two-factor authentication?

All POS systems are potential targets for hackers, and the Aloha system is no exception, due to the possible availability of credit card information they can use for illegal purposes. If you support your sites remotely, the vulnerability to external attack is significantly higher. Two-factor authentication considerably decreases the likelihood that anyone else but you has access to your sites.

Two-factor authentication is already a Payment Card Industry Data Security Standard (PCI DSS) requirement, see section 8.3. You can use the following link to download the entire PCI Security Standards in PDF format.

https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf

continued on page 2

How can I implement two-factor authentication?

Two-factor authentication is a 'hot topic,' as you might imagine. Numerous third-party companies are offering solutions at widely varying costs and degrees of effectiveness. Although a practical 'answer' to this question is still emerging, Radiant Systems has recommendations that will help you to prepare your sites, networks, and operating procedures for two-part authentication:

- Use a unique user ID and password for every employee in your local or 'home' network. You must never use shared user names and passwords.
- Use a unique user ID and password for each site, when you log in remotely. Do not use the same user name and password across every site in your organization. Every site must have a unique set of credentials. Using the same user name and password for more than one site is an automatic failure to comply with PCI DSS standards for you and for your customer site
- Establish policies and configurations that cause all passwords to expire after a specific time frame. These policies must apply to all passwords used to access computers, third-party programs, and the Aloha system. We recommend you use an expiration interval of 45 to 90 days.
- Create new passwords to replace old passwords as they expire.
- Make sure all passwords are 'strong,' consisting of at least seven characters that include upper and lower case letters, numbers, and symbols, and that are not strings found in dictionaries. An example of a 'strong' password could be something like AgBr45&7*.
- Ensure that sites are not leaving pcAnywhere®, or other remote administration tools, 'listening,' or active and logged in when not needed. Give site personnel specific instructions to close these applications completely when they are not in active use. Whenever possible, configure the application to close after each session, and to not start automatically at any time.
- Make sure any sites using dial-up connections disconnect after every on-line session.

What do I do if a security breach occurs?

You should immediately involve law enforcement after any security breach, as early as possible. They can make use of any trace data still available to locate and identify the responsible party. Time is absolutely of the essence. You should notify all processors and payment card companies you use, and tell them of the breach. Get as many people involved as possible, and as early as possible, to identify and catch the perpetrators. You should also attempt to protect and notify affected cardholders, to limit financial losses for all parties involved. Early notification will give these individuals the opportunity to begin monitoring their accounts for fraudulent activity or request new card numbers, at their discretion.



Don't Let "Data Thieves" Catch You Unprepared!

Here are some statistics you might find interesting, as released by Visa® USA, to explain the percentage of sites that are PCI compliant:

| Type of Merchants Reporting (definitions) | Percent Compliance by Self-Report |
|---|-----------------------------------|
| Level 1 (more than 6 million transactions per year) Level 2 (1 million to 6 million transactions per year) | 96% |
| Level 3 (20,000 to 1 million transactions per year) | 52% |
| Level 4 (fewer than 20,000 transactions per year) | Not Released |

As larger retailers tighten their security programs, 'data thieves' are moving on to the remaining soft targets, level 3 and level 4 merchants, in the area of payment card fraud. To provide your sites with the newest data security features available, we encourage you to implement the best practices as they are laid out in the Aloha CISP Best Practices Guide.



New Data Security Features in Aloha, Version 6.3

Aloha POS v6.3 incorporates several new security features, to help you strengthen the data integrity of your sites, or those of your customers. Some of these enhancements are in direct response to requirements of the Payment Card Industry Data Security Standards (PCI DSS), while others are in response to customer requests.

More detailed information about these new features is available in the Aloha CISP Best Practices Guide, including configuration steps, where required. Prior to upgrading to Aloha v6.3, we recommend you obtain the corresponding version of this document, and use it to prepare for the upgrade. Proper preparation can save you considerable time, and make it easier for you to comply with PCI DSS.

In summary, the new security enhancements in Aloha v6.3 are as follows:

- The Audit report in QuickService® and TableService® will, by default, mask credit card and expiration date information. You must specifically grant users the ability to view this information by adding the option to their Back Office Security Level, by selecting Maintenance > Labor > Back Office Security Levels in Aloha Manager. The new option is located in Reprints > Audits > Display Credit/Debit Card Numbers, in the Functions column. Select the security level ID to which you want to give permission for this function, and then select 'Run' and 'Save' for the specified line item. After the next data refresh, employees with this security level assigned to them can view credit or debit card numbers and expiration dates in the Audit report. All other employees with access to the Audit report see these numbers in masked format.
- As reported in the previous issue of this newsletter, the 'Alt+X' method of accessing Aloha Manager and Aloha EDC is no longer available in Aloha v6.3 unless you are using a 'super key.'
- The configuration of EDC, as it relates to security, is of vital importance. If misconfigured, EDC may not work properly, but it is also possible to expose EDC to unnecessary risk. For this reason, the existing EDC logging function is now enhanced, to clearly record detailed usage information in a more human-readable format. EDC now records all program activities, including log-in, date, time, terminal number (if applicable), program actions, and log-out. It is not possible to modify or disable this logging function. EDCSvr captures this information, and stores it in the EDC debut file on the EDC server.

- We have removed the option 'Disable masking in grind files' in Maintenance > Payments > Tenders > Type tab, from the Aloha system altogether. You must clear this option for all tenders, prior to upgrading to Aloha v6.3.
- Aloha v6.3 includes a new option, in Maintenance > Store Settings > Credit Card group > Voucher Printing 2 tab, to prevent the cardholder name from printing on credit card vouchers. When you select this option, Aloha replaces 'Magnetic card present: «Cardholder Name»' with 'Magnetic card present: Yes.' Although U.S. Federal law and PCI DSS do not currently require you to suppress the cardholder name, customers have requested this capability.

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.



FOR MORE INFORMATION, PLEASE VISIT US AT
WWW.RADIANTSYSTEMS.COM OR CONTACT US AT 877.794.RADS

ATLANTA • DALLAS • LONDON • LOS ANGELES • MELBOURNE • MEMPHIS • PRAGUE • SINGAPORE

CN-HOSP-0807 | © 2007 Radiant Systems, Inc. All rights reserved. Radiant Systems and design is a registered trademark of Radiant Systems, Inc. All other trademarks are the property of their respective owners.

