



Aloha POS, Radiant Payment Services, and RBS WorldPay Use Token Replacement Technology to Increase Credit Card Security

In Aloha v6.5, Radiant introduced Token Replacement, a new payment security feature that allocates a unique identifier, or token, to cardholder data at the RBS WorldPay host, to prevent personal information from being stored at the point of sale.

What is Token Replacement?

When using Token Replacement, sensitive cardholder data is sent to the secure RBS WorldPay host in an encrypted form. The host processes the payment and assigns a unique identifier, or token, to the transaction. The token is sent back to the point of sale for future reference, thus eliminating the storage of sensitive credit card data in a recognizable form at the site and increasing data security.

Who can use Token Replacement?

Token Replacement is only available to Radiant Payment Services / RBS WorldPay customers and requires use of Aloha POS v6.5.2 or later and Aloha EDC v6.5.3 or later.

How do you enable Token Replacement?

Customers upgrading to Aloha v6.5 are not always automatically enabled for Token Replacement:

- If you are an Aloha user who was initially using RBS WorldPay and you elected to move to Radiant Payment Services, you are not required to change your processor configuration from RBS WorldPay to Radiant Payment Services, but you must enable Token Replacement for the RBS WorldPay processor in Aloha EDC upon upgrading to Aloha v6.5.
- If you are a new Aloha user, configure Radiant Payment Services as your payment processing provider and Token Replacement will automatically be enabled for you in Aloha EDC.

To configure RBS WorldPay to use Token Replacement:

1. Log in to **Aloha EDC v6.5** or later.
2. Select **File > Stop POS Processing**, if this is started.
3. Select **Configure > Processors**.
4. Select **RBS WorldPay**.
5. Select the **Options** tab.
6. Select **Enable Aloha Payment Guard**.*
7. Click **OK** and exit the **Processors** function.
8. Select **File > Start POS Processing**.

Token Replacement will be in place the next time you process a credit card transaction, ensuring you are storing credit card data in an unrecognizable form at the site level and protecting your system from potential hackers.



*The Aloha Payment Guard name has been changed to Token Replacement. This change will be reflected accurately in the upcoming weeks.



Card Brand Mandates and Plans for 2010

Two major credit card brands, Discover[®] and MasterCard[®], have issued mandates with approaching deadlines of which you need to be aware:

- Discover requires you to also enter the Card Identification Number (CID) for transactions in which you manually enter the credit card number, by April, 2010. The CID is a three-digit security code printed on the back of the card. Requiring the entry of this code helps validate the legitimacy of the card, thus reducing fraud.
- MasterCard requires real-time reversal support for credit and debit card authorizations, by May, 2010, to prevent delays in guests regaining access to their funds when a sale is not completed.
- MasterCard requires partial authorization support for prepaid credit and debit cards, by May, 2010. This support allows a merchant to authorize a portion of the original transaction amount, if the transaction amount exceeds the available balance on the card. Guests can use the remaining balance of a prepaid card as partial payment of a transaction without the risk of being declined, and pay the balance of the transaction using an alternate form of payment.

These mandates require changes to the Aloha POS and Aloha EDC, after which Radiant Systems must recertify with each supported processor. Radiant Systems is prioritizing the recertification of the supported processors based on site count. The following processors are targeted for recertification in Aloha POS and EDC v6.9, which is planned for controlled deployment status in May, 2010:

- VisaNet
- Fifth Third
- RBS WorldPay
- Radiant Payment Systems

All other supported processors are targeted for recertification in later releases as quickly as time permits.



MenuLink Labor Enhanced to Assist Managers in Completing Form I-9

As mentioned in our previous Compliance Newsletter, in MenuLink Labor v6.5, the employee profile screen reflects new citizenship status options and an updated accepted documents list, to meet the new requirements of the U.S. Citizenship and Immigration Services (USCIS). We are also introducing new functionality to make it even easier for a manager to complete Form I-9.

- Upon save, if any fields on the I9 tab were changed and the manager has not selected a supported citizen status option, MenuLink Labor provides the following friendly alert: "I-9 Citizenship Status options were updated in 2009. Any changes to the current I-9 will require the employee's citizenship status to be updated."
- In addition, regardless if the manager made any changes to the I9 tab, MenuLink Labor will now verify a valid citizenship status is entered before printing. If the Form I-9 still reflects an old citizenship status, MenuLink Labor alerts the manager with the following message "This government I-9 form has changed. Please specify citizenship."

Look for all of these new features, and more, in the MenuLink Labor release available for controlled deployment at the end of May.

Refer to <http://www.uscis.gov/files/form/i-9.pdf> to download a copy of the Form I-9 from the USCIS Web site and see a complete list of acceptable documents.

Questions or Comments? ProdMgmt@RadiantSystems.com

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.