



## Managing Windows Auto-Logon on Servers and Terminals

When using a Microsoft® Windows® operating system, it is possible to automate the logon process. While this may be necessary for practical operations on Front-of-House terminals, it poses a security risk when managed improperly. This is because improper management of the auto-logon feature results in the user name and password being stored in the Windows registry in clear text, which violates the PCI DSS requirement for implementing strong access control measures.

To assist you in properly managing the Windows auto-logon feature, Microsoft offers a utility called AutoLogon.exe. This application is a multi-purpose tool that allows you to do one of the following:

- Disable the auto-logon feature.
- Enable the auto-logon feature, but encrypt and move the user name and password information to a secure location.

### Use the following guidelines with regard to using the Windows auto-logon feature on an Aloha system:

- *NEVER* configure the Aloha Back-of-House (BOH) file server to use the Windows auto-logon feature. If the file server is currently set to use auto-logon, run the AutoLogon.exe utility on the BOH file server and follow the prompts to disable the feature immediately.

After running AutoLogon.exe, restart the Aloha BOH file server. Windows should prompt you for a user name and password, indicating the program ran successfully. To access the BOH from this point forward, you will need this user name and password. Keep these credentials in a secure location for your reference. Refer to PCI DSS regulations regarding other requirements, including unique user names and passwords for any BOH user, password complexity rules and rotation requirements, and the like.

- Configuring a Front-of-House (FOH) terminal to use auto-logon is an accepted configuration; however, it is still necessary to ensure this feature is configured properly. You can accomplish this in the following ways:
  1. If you are using Radiant hardware with Radiant Auto Loader (RAL), install RAL version 2.3.1.0 or later. RAL will move the user name and password information to a secure area and store it in an encrypted format.
  2. If you are using Radiant hardware without RAL, or you are not using Radiant hardware, run AutoLogon.exe on each terminal to move the user name and password information to a secure area and store it in an encrypted format.

Click <http://technet.microsoft.com/en-us/sysinternals/bb963905.aspx> to access Microsoft TechNet and download AutoLogon.exe, available as part of Microsoft SysInternals. This utility is also available in the Utilities folder on the Aloha FTP site.

Remember, PCI DSS security requirements apply to all system components, not just the Aloha software and its configuration. It is your responsibility to configure your systems in a secure manner, and ensuring you are using the above “best practices” regarding the auto-logon feature is a must.

Refer to “Managing Separate User Accounts on FOH Terminals - RAL v2.3.1” for a full discussion on using this tool to support unique logon IDs for each FOH terminal and complex, expiring passwords.

Please contact your Aloha reseller or Radiant Systems representative with any questions regarding the implementation of these procedures.



## **Radiant Systems Discontinuing Support of Microsoft Windows 2000 Server, Effective July, 2010**

Per the Microsoft Support Lifecycle policy, Microsoft will discontinue extended support for Windows 2000 Server effective July 13, 2010, and will no longer release software patches for this operating system. The Payment Card Industry Data Security Standards (PCI DSS) require that “all critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.” Although older operating systems that are no longer supported by the vendor are not immediately considered non-compliant, it would be extremely difficult to implement compensating controls to achieve compliance using this operating system.

Radiant Systems is committed to providing secure technology for handling sensitive cardholder data; therefore, Radiant Systems is taking a proactive approach and will also discontinue support for the Windows 2000 Server operating system effective in July, 2010.

### **What does Radiant Systems mean by “discontinue” support?**

As of this writing, Market Ready supported versions of Aloha include v6.2, 6.4, and v6.5. Discontinuing support means:

- Radiant will no longer develop software for operation on this operating system.
- Radiant will no longer test the operation of the supported versions of the POS software on this operating system.
- Radiant will no longer correct product defects in the supported versions of the POS software if the defects result from the operation of software in this environment.
- Radiant will not certify the operation of Aloha POS versions released after July, 2010 to work on this operating system.

Also, per the Microsoft Support Lifecycle policy, support for Windows 2003 Server will end in the year 2015.

Refer to <http://support.microsoft.com/gp/lifepolicy> for questions and answers regarding the Microsoft Support Lifecycle policy.



## Radiant Systems Dedicated to Providing Secure Technology for Protecting Cardholder Data

As part of our ongoing commitment to provide secure technology for handling sensitive cardholder data, several services provided by Radiant Systems have just completed an annual audit and received a Report on Compliance.

- The Radiant Systems Hosted Solutions Group engaged in and successfully completed a Level 1 PCI DSS audit in December, 2009. As a data center, the Hosted Solutions Group is required to comply with a subset of the PCI Data Security Standards. This subset is referred to as a 9 ROC (Report on Compliance) certification, and states that the Hosted Solutions Group is in compliance with the standards laid out in “Requirement 9 – Restrict physical access to cardholder data.”
- As application service providers, Aloha Command Center, Aloha Takeout, and Aloha Online are required to meet all 12 requirements of the PCI Data Security Standards. Each of these service providers engaged in and received a PCI DSS Report on Compliance, also in December, 2009, thus ensuring they handle sensitive cardholder data in a tightly secure environment.

**Note:** The addition of these certifications to the list of PCI DSS Compliant Service Providers published by Visa is currently pending.

Merchants required to be PCI compliant must use validated payment applications. With each new POS release, Radiant continues to invest in the development effort required to meet or exceed the data security standards in effect at the time of the release. Currently the standard in effect is known as the Payment Application Data Security Standards (PA DSS).

### As a reminder, the following Radiant POS applications are currently listed on the PCI DSS List of Validated Payment Applications:

Version number:	Validated against PABP/PA DSS version:	Current validation expires on:
Aloha POS v6.1	PABP v1.3	June 2, 2010
Aloha POS v6.2	PABP v1.4	December 2, 2010
Aloha Takeout v1.1	PABP v1.4	December 2, 2010
Aloha POS v6.4	PA DSS v1.2	October 2, 2013
Aloha POS v6.5	PA DSS v1.2	October 2, 2013
Aloha POS v6.7	PA DSS v1.2 – Addition to the PCI SSC validated list of payment applications is pending.	Not established.

\*Radiant Systems submitted an Annual Attestation of Validation for Aloha Takeout v1.1 in November, 2009 and plans to undergo PA DSS assessment of v1.2 prior to its release, which will be before the December, 2010 expiration date of v1.1.

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

[https://www.pcisecuritystandards.org/security\\_standards/pa\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml)

As PCI Data Security Standards continue to evolve, Radiant Systems is committed to continuously increasing security to protect cardholders and merchants. We strongly encourage clients to adopt the most recent market-ready Aloha release to stay current with security-related enhancements.



## Revised Employee Eligibility Verification Form I-9 Available in MenuLink Labor v6.5

In an effort to improve homeland security, U.S. Citizenship and Immigration Services (USCIS) released new requirements for Form I-9, used to verify a newly hired employee's identity and authorization to work in the United States. Effective April 3, 2009, employers must use the revised I-9 form for all new employees and also for all existing employees whose employment authorization expires after that date.

The most significant change to Form I-9 stipulates that all documents presented during the verification process must be unexpired and must establish both identity and employment authorization. As a result, several documents that are no longer issued and have expired were removed from the list of acceptable documents that establish both identity and employment authorization. Documents not containing an expiration date, such as a Social Security Card, are considered unexpired and still acceptable.

### Documents removed from List A:

- Form I-688 (Temporary Resident Card)
- Forms I-688A and I688B (outdated Employment Authorization Cards)

### Documents added to List A:

- A temporary Form I-551 (also referred to as Green Card) printed notation on a machine-readable immigrant visa in addition to the foreign passport with a temporary I-551 stamp.
- Passports for citizens of the Federated States of Micronesia (FSM) and the Republic of the Marshall Islands (RMI), along with a valid Form I-94 or Form I-94A indicating nonimmigrant admission under the Compact of Free Association Between the United States and the FSM or RMI.

MenuLink Labor provides the ability to capture the types of forms you examined when verifying employment authorization of a new hire in the Employee Profile screen, which can then be printed for appropriate signatures and retention by the employer. Effective with MenuLink Labor v6.5, the employee profile screen reflects new citizenship status options and an updated accepted documents list, to meet the new requirements. The revision date of 08/07/09 (lower right corner), and the expiration date of 08/31/12 (top right corner) also appear on the updated Form I-9.

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.

### Sources:

U.S. Department of Homeland Security, U.S. Citizenship and Immigration Services, "Questions and Answers: USCIS Revises Employment Eligibility Verification Form" retrieved on 12/08/2009.

## SAS 70 Type II Certification Can Save Radiant Customers Time and Money



In November, 2009, the Radiant Systems Hosted Solutions Group completed a voluntary, comprehensive SAS 70 Type II audit of the internal control activities in place with regard to protecting customer information. SAS 70, the acronym for "Statement on Auditing Standards (SAS) 70, Service Organizations," is a widely recognized auditing standard created by the American Institute of Certified Public Accountants (AICPA).

A Type II audit is a much more extensive audit in that it includes the information contained in a Type I audit but goes beyond and also includes the service auditor's opinion on how effective the service organization's internal controls operated during the period under review. The Radiant Systems Hosted Solutions Group chose to undergo a Type II audit because a service organization's customer can provide their user auditor a copy of the Type II audit, which can substantially reduce the time and expense required by the customer for their own user audit.

Independent service auditors examined the following Web-based applications hosted by the Radiant Systems Hosted Solutions Group and found them to successfully comply with the requirements of the SAS 70 Type II audit:

- Aloha Command Center
- Aloha Configuration Center
- Aloha Guest Manager
- Aloha Insight
- Aloha Takeout
- MenuLink Inventory
- MenuLink Labor

Volunteering for and receiving SAS 70 Type II certification differentiates Radiant Systems from other service organizations in that it demonstrates the company's commitment to establishing sufficient controls and security measures to effectively host and process customer data.

Questions or Comments? [ProdMgmt@RadiantSystems.com](mailto: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.