



## 9700 Version 3.50

# 9700 HMS *ReadMe First*

## General Information

---

---

### About This Document

This *ReadMe First* document is intended as a quick reference guide to provide information about new features and enhancements included in the latest release of the *MICROS 9700 3.50 HMS* software. For each version of the software, the document will provide the information as described in the following sections:

### What's New

This section of the document contains information on the new features of a software release. A new feature is defined as one that provides capabilities that were not available in previous versions of the software.

### What's Enhanced

This section of the document contains information on the enhancements in the software release. An enhancement is defined as a change made to improve or extend the functionality of an existing feature in the software. To qualify as an enhancement, the change must satisfy the following criteria:

- The basic feature or functionality already exists in the previous release of the software.
- The change adds to or expands on the current process—it does not replace it. This differs from a revision (i.e., a bug fix) which corrects a problem not detected in the previous release of the software.

## **What's Revised**

This section of the document contains information on the issues that have been corrected in a software release. A revision is defined as a correction made to an existing form, feature, or function in the currently released version of the software. To qualify as a revision, the change must satisfy the following criteria:

- The basic form, feature, or functionality must be part of the previous version of the software.
- The change must replace the current item or remove it from the application.

---

## **Declarations**

### **Warranties**

Although the best efforts are made to ensure that the information in this document is complete and correct, MICROS Systems, Inc. makes no warranty of any kind with regard to this material, including but limited to the implied warranties of marketability and fitness for a particular purpose.

Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information recording and retrieval systems, for any purpose other than for personal use, without the express written permission of MICROS Systems, Inc.

MICROS Systems, Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connections with the furnishing, performance, or use of this document.

### **Trademarks**

FrameMaker is a registered trademark of Adobe Corporation.  
Microsoft, Microsoft Excel, Win32, Windows, Windows@95, Windows 2000 (Win2K), and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries.  
Visio is a registered trademark of Visio Corporation.  
All other trademarks are the property of their respective owners.

---

**Who Should Be Reading This Document**

This document is intended for the following audiences:

- MICROS Installers/Programmers
- MICROS Dealers
- MICROS Customer Service
- MICROS Training Personnel
- Guest Connection Users

---

**What the Reader Should Already Know**

This document assumes that the reader has the following knowledge or expertise:

- Operational understanding of PCs
- Understanding of basic network concepts
- Experience with Microsoft®, Windows® Server 2003, Windows® XP
- Experience with Microsoft® SQL Server™, Oracle® 10g, or Oracle® 9i
- Familiarity with the Guest Connection software and peripherals

## **PCI Compliance**

---

Visa established the Payment Card Industry (PCI) Data Security Standard to protect Visa cardholder data—wherever it resides—ensuring that members, merchants, and service providers maintain the highest information security standard. To adhere to the PCI standard, changes have been made to the 9700 HMS product.

Please read this section carefully, as well as the accompanying PCI-compliance documentation. For a list of related documents, see the *Documentation Resources* section.

More information about PCI-compliance and related software changes is provided in the following sections:

- Documentation Resources
- PCI Compliance Installation Changes
- Security Announcement

## Documentation Resources

The following documents have been updated with information and procedures needed to maintain PCI-compliance and must be consulted for security purposes prior to upgrading from 9700 HMS Version 3.1 SP5 and below to 9700 HMS 3.1 SP6 and above. These documents are available on the MICROS 9700 HMS Product page of the MICROS Member Services website.

- *9700 PA-DSS Compliance v. 3.20*: This document is a quick reference guide that provides information concerning MICROS' adherence to the PCI Data Security Standard and Payment Application Data Security Standard (PA-DSS) compliance.
- *9700 Secure Default Account Handling*: This document contains detailed information on 9700 v. 3x secure default account handling procedures. These procedures must be followed to prevent compromised security and maintain PCI compliancy.
- *9700 Security Guide*: This document describes 9700's security design, features that monitor employees' actions taken on the system, and features that restrict employee access to the database, reports, and operational procedures.
- *9700 Upgrade Best Practices*: This document is intended to convey the best practice information when upgrading the 9700 HMS application from a non-PCI compliant version (version 2.x) to a PCI compliant version (versions 3.x and greater).
- *MICROS 9700 Encryption Key Management Utility*: This document is a quick reference guide that provides information concerning the 9700 Encryption Key Management Utility, which allows the user to set the encryption passphrase for the 9700 system.
- *MICROS Secure Wipe Tool*: This document provides instructions on how to download and use the secure wipe tool Eraser. The secure deletion of data is necessary when upgrading a non-PCI compliant version of a MICROS software application or when customer data has been collected for troubleshooting purposes and is no longer needed.
- *Wireless Networking Best Practices*: This document explains the steps necessary to connect a wireless workstation for PCI-compliance.

---

## PCI Compliance Installation Changes

Changes were made to the 9700 installation process for versions 3.10 SP6 and higher, in order to meet the Payment Card Industry Data Security Standard (PCI DSS) requirements. For more information on PCI DSS, please see the *Security Announcement* section on page [10](#).

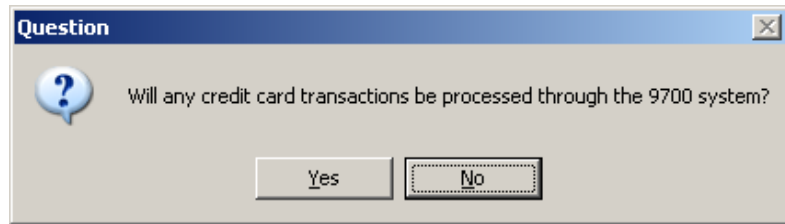
Previous versions of 9700 3.x installed with four default accounts: “9700cfg”, “csremote”, “micros”, and ‘m9700’. MICROS Systems, Inc. previously advised that these default accounts be deleted, renamed, or disabled. To prevent compromised security and maintain PCI compliancy, 9700 Versions 3.10 SP6 and higher have modified or removed these default accounts. For more information, please see the *Documentation Resources* section on page [5](#).

To meet the PCI-compliance requirement, domain-level security or Windows® Workgroups must now be enabled when **both** the Remote Management Console (RMC) remote user account is active and credit card transactions are processed through the 9700 system. Domain-level security must be enabled when the server is on a domain. Windows® Workgroups provides security for servers not on a domain.

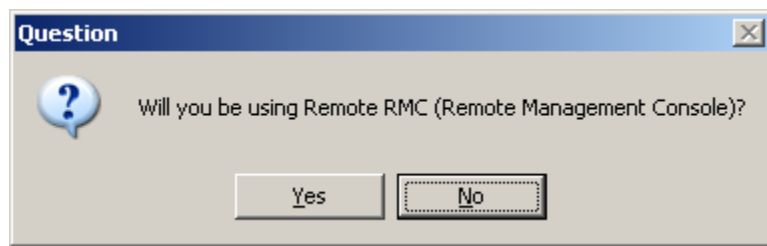
The installation process now recognizes if the server is on the domain or not on the domain. When the server is on the domain, domain-level security is automatically installed by the 9700 installation process. Disabling domain-level security will compromise PCI compliancy. If domain-level security is disabled when the server is on the domain, the CreateUser.exe application must be used to maintain PCI compliancy. For more information on Windows® Workgroups and the CreateUser.exe application, see the *When the Server is Not on the Doain: Configuring Remote RMC in a Windows® Workgroup Environment* section on the next page.

### When the Server is Not on the Doain: Configuring Remote RMC in a Windows® Workgroup Environment

Due to a new PCI security requirement, the 9700 installation now asks if the site processes credit card transactions through the system, as shown below:



If credit cards are processed, the 9700 installation now asks if the site will use the remote RMC, as shown below:

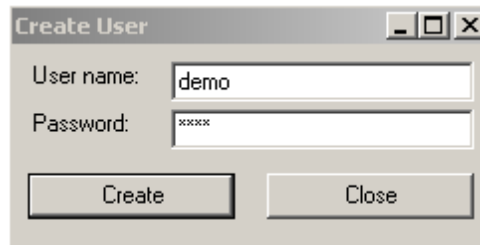


If the site is using remote RMC, credit cards are processed through the 9700 system, and the server is not on the domain, then the following prompt will display:



After clicking [**OK**] to close the prompt, follow the procedures listed below to maintain Payment Card Industry (PCI) compliance in a Windows® Workgroup environment when both credit cards and Remote RMC are used. Follow the steps below after the system has been updated to 9700 3.10 SP6 or a higher version of software, and the server has been rebooted.

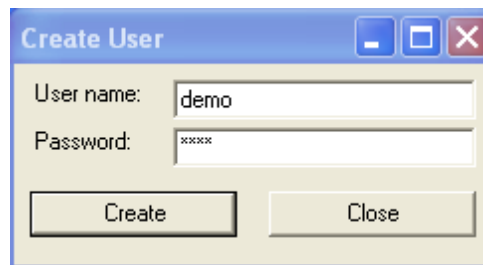
1. From the Windows® Start menu on the 9700 server, select *All Programs / MICROS Applications / CreateUser.exe*.
2. When prompted, enter a unique username and a strong password consisting of at least eight alphanumeric characters. Select [**Create**]. Do not use default usernames or passwords.



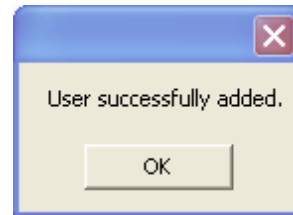
3. Select [**OK**] after the 'User successfully added' message, see below, is displayed:



4. Select [**Close**] within the CreateUser applet.
5. After Remote RMC is installed on the client workstation and updated to match the server version, from the Windows® Start menu select *All Programs / MICROS Applications / CreateUser.exe*.
6. When prompted, enter the identical username and password previously used on the server and then select [**Create**].



7. Select [**OK**] after the 'User successfully added' message, seen below, is displayed:



8. Select [**Close**] within the CreateUser applet. You should now be able to run Remote RMC on the client workstation.
9. Repeat steps 6-9 on each Remote RMC workstation. Be certain to use the same username and password previously used on the server.

MICROS Systems, Inc. mandates that the Remote RMC password on the server and all clients be changed periodically, at least every 90 days, using the CreateUser applet. After creating a new password, be certain to use the same username and password on the server and on all the client workstations.

---

## Security Announcement

### Overview

Due to new, more stringent Payment Card Industry Data Security Standard (PCI DSS) requirements, the encryption key rotation handling procedures, default account handling, and security-related documentation for 9700 version 3.10 SP6 and higher have changed.

### About PCI Compliance

PCI-compliance is required of all merchants and service providers that store, process, or transmit cardholder data. The program applies to all payment channels, including retail (brick-and-mortar), mail/telephone order, and e-commerce.

When customers offer their bankcard at the point-of-sale, over the Internet, on the phone, or through the mail, they want assurance that their account information is safe. That is why the PCI Data Security Standard was established. The program is intended to protect cardholder data—wherever it resides—ensuring that members, merchants, and service providers maintain the highest information security standard.<sup>1</sup>

To achieve compliance with PCI, merchants and service providers must adhere to the PCI Data Security Standard, which offers a single approach to safeguarding sensitive data for all card brands. This standard is a result of collaboration among the credit card industry and is designed to create common industry security requirements, incorporating the PCI requirements. Using the PCI Data Security Standard as its framework, PCI provides the tools and measurements needed to protect against cardholder data exposure and compromise across the entire payment industry.

For more detailed information concerning PCI-compliance, please refer to the PCI Security Standards Council website, <https://www.pcisecuritystandards.org/>.

### Key Management Utility Security Enhancements

In the past, non PCI-compliant versions of software stored the encryption keys used to encrypt and decrypt secure data, such as credit card numbers, in the database.

---

1. Reprinted from “Cardholder Information Security Program”, <[http://use.visa.com/business/accepting\\_visa/ops\\_risk\\_management/cisp.html](http://use.visa.com/business/accepting_visa/ops_risk_management/cisp.html)>.

Now, due to a new PCI DSS requirement that mandates the secure deletion of unused encryption keys, 9700 version 3.10 SP6 and higher use a new encryption scheme that avoids using secondary encryption keys. The secure deletion of the old encrypted passphrase file is accomplished using the secure delete application *SDelete*.

### Warnings!

After the key rotation (the initial key rotation all subsequent rotations) is performed by the Key Management Utility, the database and 9700 application becomes synchronized with new encryption key data.

As a result, users should not swap databases (restoring/replacing the existing database with a different one) until they are absolutely sure that the new database is also in sync with the 9700 application.

Generally speaking, there is no way to determine whether an offline database that is about to be restored by the user is in sync with the 9700 application.

Therefore, the only safe scenario to restore/replace a database is to restore/replace the database with a good database backup that must have been taken prior to performing the key rotation. The database can only be restored/replaced if no key rotation has occurred since uploading the existing database or since the backup database was taken.

Warning: If the passphrase is lost, the encrypted data in the database is unrecoverable. There are no back doors!

For more information and instructions on how to use the Key Management Utility, see the *MICROS 9700 Encryption Key Management Utility* document.

## Secure Default Account Handling

This section contains detailed information on secure default account handling procedures. These procedures must be followed to prevent compromised security and maintain Payment Card Industry (PCI) compliance.

---

**WARNING!** *Important Security Warning: The use of default accounts is not PCI compliant. Therefore, 9700 versions 3.10 SP6 and higher eliminate the option to operate in a non-compliant fashion by automatically deleting or disabling the existing default accounts via the installation/ upgrade process.*

*Disabling or deleting the existing default accounts could potentially disable functionality in the system where these accounts were used. However, these default accounts must be securely disabled or deleted to operate in a PCI compliant manner.*

---

In the past, 9700 versions installed with four default accounts: “9700cfg”, “csremote”, “micros”, and ‘m9700”. MICROS Systems, Inc. previously advised that these default accounts be deleted, renamed, or disabled. To prevent compromised security and maintain PCI compliance, 9700 Versions 3.10 SP6 and higher have modified or removed these default accounts.

The “micros’ and “csremote’ legacy accounts will no longer be installed. These accounts have been removed from the installation process as they are not used and, when not securely deleted, can compromise PCI compliance. When upgrading to Version 3.10 SP6 or higher from a lower version of software, these accounts will be disabled after the upgrade process completes.

The legacy “m9700” and “9700cfg” accounts will be disabled after the installation/ upgrade process completes.

For more information on secure default account handling, see the *9700 Secure Default Account Handling* document.

## **Internet Explorer 8 Compatibility Mode**

---

If upgrading to Internet Explorer 8 on a 9700 application server, the browser needs to be configured to run in compatibility mode.

### **Configuration**

To configure IE 8 to run in compatibility mode for all websites, complete the following steps:

1. Open Internet Explorer
2. From the Menu Bar, select Tools > Compatibility View Settings
3. Enable the 'Display all websites in Compatibility View' option

## 9700 3.50 GR in a Single Oracle Environment

---

After installing 9700 3.50 GR HMS on an Oracle 10g shared application and database server, apply the following steps once the installation is complete and the server has rebooted:

1. Navigate to the *Windows / Assembly Directory* on the server and do the following:
  - a. Delete the two instances of the *Policy.10.1.Oracle.DataAccess*
  - b. Delete the two instances of the *Policy.9.2.Oracle.DataAccess*
2. Navigate to the *9700 / EMC* folder and copy the *OraOps10.dll*. Navigate to the *9700 / bin* folder and replace the *OraOps10.dll* with the one that was copied from the *EMC* folder. The version in the *bin* folder should be *10.1.0.200*.

---

**Note:** *These steps will leave the *Policy.10.2.Oracle.DataAccess* in the assembly directory and the updated *.dll* will allow users to run *Key Manager* and log into *EMC* successfully.*

---

3. To run SQLPlus from a command line, it is necessary to set the *tns\_admin* environment variable in each command prompt window opened. For this setting, do the following:
  - a. Open a command prompt and navigate to the drive that Oracle is installed.
  - b. Type in the following:
    - i. set *tns\_admin*=<appropriate drive letter>:\oracle\product\10.2.0\db\_1\NETWORK\ADMIN
  - c. This variable should not be set as a global environment variable as it could cause issues with other programs. This variable will need to be set each time a user needs to log into the SQLPlus command line.

---

**Note:** *This allows the user to log into SQLPlus without any issues. No DLLS should be moved from one directory to another and no changes be made to any paths.*

---

## 9700 HMS Version 3.50 Release

---

### What's New

#### New Features Summarized

The table below summarizes the new features included in this version.

Feature	CR ID#	Page
<b>TMS</b>		
Rollback Reservation Update Status from Guest Connection is now Supported		<a href="#">15</a>
POS now Sends Updated Information on Changes to the Number of Guests to TMS		<a href="#">16</a>

#### New Features Detailed

---

#### TMS

##### ***Rollback Reservation Update Status from Guest Connection is now Supported***

*SCR 7497*

Support for the Rollback Reservation Update Status from Guest Connection has been introduced to 9700.

- If a reservation is rolled back, a message sent to 9700 will cause the check that was opened upon seating the reservation to be closed out.
- The check may be closed out by setting the guest count to '0' and then tendering it to cash.
- The check may be closed out by canceling the transaction.
- A revenue center level option bit has been added to enable or disable this rollback functionality.

- If the check has any check details beyond what should be there after seating the guest (i.e., menu items, discounts, etc.), 9700 ignores the request and the check must be closed out manually.

***POS now Sends Updated Information on Changes to the  
Number of Guests to TMS***

*SCR 7536*

A new option bit, 'Send Guest Count to TMS', has been added to EMC. This bit sends the guest counts from 9700 to Guest Connection. The addition of this option bit allows continued compatibility with older versions of Guest Connection as well as older versions of the TMS interface.

---

## What's Enhanced

### Enhancements Summarized

The table below summarizes the enhancements included in this version.

Enhancement	CR ID#	Page
<b>Credit Card Driver</b>		
Partial Payment on Prepaid Credit Cards has been Introduced		<a href="#">17</a>
<b>Install</b>		
Improvements have been made to the Install/Upgrade Process	26180	<a href="#">18</a>
<b>NetVuPoint</b>		
NetVuPoint is no longer Dependant on the i-net Driver		<a href="#">18</a>

### Enhancements Detailed

---

#### Credit Card Driver

##### *Partial Payment on Prepaid Credit Cards has been Introduced*

*SCR 7481*

With this release, 9700 has added functionality to allow the CAPMS driver to process prepaid credit cards with the option of partial payment. The CAPMS driver can now be used in conjunction with the Credit Card option 'Supports Partial Authorization'. This functionality also supports balance inquiries of prepaid credit cards.

---

## **Install**

### ***Improvements have been made to the Install/Upgrade Process***

SCR 7221

CR ID# 26180

Previously, temporary install information written to the install path was not cleaned up in instances where the install failed. Each install attempt thereafter would add additional temporary information to the path and result in buildup preventing the applications (setup, EMC, logviewer) from working correctly. The buildup would only get cleared from a system reboot.

This has been corrected by using a prerequisite CD where the applications included on the CD are installed once, making the patch smaller and eliminating the system reboot. The path is cleaned up following a successful install.

---

## **NetVuPoint**

### ***NetVuPoint is no longer Dependant on the i-net Driver***

SCR 7499

With this release, a new mymicros.net build has removed NetVuPoint's dependence on the i-net driver.

## What's Revised

### Revisions Summarized

The table below summarizes the revisions included in this version.

Revision	CR ID#	Page
<b>Audit Trail</b>		
Audit Trail Utility no longer Fails Due to Large Number of Records		<a href="#">20</a>
<b>Control Panel</b>		
Partially Settled Records are no longer Resent During the Settlement Process	25845	<a href="#">21</a>
<b>Credit Card Driver</b>		
The VisaD Driver now sends '10' as the Response Code for Partial Authorization Settlement Records		<a href="#">21</a>
<b>Install</b>		
SDelete is no longer Required in RMC Client Installs	25315	<a href="#">21</a>
<b>Internationalization</b>		
Service Charges in a Japanese Database with Inclusive Tax Post Correctly	25447	<a href="#">22</a>
Check Sharing with Inclusive Tax and No Decimal Currency Balances Correctly	25865	<a href="#">22</a>
<b>Mobile MICROS</b>		
Cyrillic Display is now Supported on HHT Screen		<a href="#">22</a>
<b>NetVuPoint</b>		
NetVuPoint Reports now Run without Errors Due to Null Values	25146	<a href="#">22</a>

Revision	CR ID#	Page
<b>OPS</b>		
The Amount of Tax Charged Displays on both the Financial Reports and the Guest Check	27099	<a href="#">23</a>
Japanese Tax Enabled Environments Calculate System and Guest Taxes Correctly	27123	<a href="#">23</a>
Japanese Tax Environments with Item Discounts Produce Accurate Financial Reports	27426	<a href="#">23</a>
Service Charges Post Correctly when a Tax Exempt Item is Voided from a Reopened Check	27573	<a href="#">24</a>
Splitting a Check with Non-decimal Japanese Tax Enabled Post Accurately to Financial Reports	27555	<a href="#">24</a>
Voiding and Reapplying the Discount Resulting in Double Posting of Inclusive Tax Amount Has Been Fixed	27843	<a href="#">24</a>
<b>SAR</b>		
The Formatting of Response Data Printing on Authorization Chits has Changed	24810	<a href="#">24</a>
<b>Winstation</b>		
All Menu Items now Display Correctly on the Check when using the Split Check Function	26849	<a href="#">25</a>

**Revisions  
Detailed**

---

**Audit Trail**

***Audit Trail Utility no longer Fails Due to Large Number of Records***

*SCR 6894*

Audit Trail Utility would fail with a memory error when there were a large number of records present in the 'Audit Trail' table. This has been corrected.

---

## Control Panel

### *Partially Settled Records are no longer Resent During the Settlement Process*

SCR 7124

CR ID# 25845

Previously, CAPMS partially settled batch records were being transferred again during the settlement process. This has been corrected.

---

## Credit Card Driver

### *The VisaD Driver now sends '10' as the Response Code for Partial Authorization Settlement Records*

SCR 7433

Previously, when doing a batch settlement for batch records that were partial authorizations, the VisaD driver was sending the wrong response code, '00'. Now, during batch creation, the VisaD driver checks for a flag marking a record as a partial authorization; these partial authorization flags cause the VisaD driver to send '10' as the response code for these records.

---

## Install

### *SDelete is no longer Required in RMC Client Installs*

SCR 6971

CR ID# 25315

Previously, **SDelete** was required for RMC client installations. Since no credit card details or other secure data is ever pulled to the local disk, the need for **SDelete** in the client RMC installations is no longer required.

---

## **Internationalization**

### ***Service Charges in a Japanese Database with Inclusive Tax Post Correctly***

SCR 7026

CR ID# 25447

When adding a check to another in a Japanese database with inclusive tax, the service charge posted incorrectly. This has been corrected.

### ***Check Sharing with Inclusive Tax and No Decimal Currency Balances Correctly***

SCR 7131

CR ID# 25865

Check sharing in a system with inclusive tax and no decimal currency did not balance correctly. This has been corrected.

---

## **Mobile MICROS**

### ***Cyrillic Display is now Supported on HHT Screen***

SCR 7529

Cyrillic letters did not display correctly on an HHT screen. This has been corrected.

---

## **NetVuPoint**

### ***NetVuPoint Reports now Run without Errors Due to Null Values***

SCR 6931

CR ID# 25146

Previously, the following NetVuPoint reports returned errors due to queries not being able to handle null values in the xml reports:

1. Cost of Goods Sold Daily Detail Report

2. All Menu Items Report
3. Price Average Group Report

This has been corrected.

---

## **OPS**

### ***The Amount of Tax Charged Displays on both the Financial Reports and the Guest Check***

SCR 7425

CR ID# 27099

In a system using Japanese tax, low value transactions did not display the tax amount charged on the financial reports; they only displayed on the guest check. This has been corrected.

### ***Japanese Tax Enabled Environments Calculate System and Guest Taxes Correctly***

SCR 7428

CR ID# 27123

In a system with Japanese tax enabled, the inclusive tax was calculated incorrectly on large checks with voided auto-service charges and discounts. These incorrect calculations posted to RMC report totals. This has been corrected.

### ***Japanese Tax Environments with Item Discounts Produce Accurate Financial Reports***

SCR 7467

CR ID# 27426

Previously, when an Item Discount was applied in an environment in which Japanese Tax was enabled, financial reports were inaccurate. This has been corrected.

***Service Charges Post Correctly when a Tax Exempt Item is  
Voided from a Reopened Check***

SCR 7482

CR ID# 27537

When an item was voided from a reopened check containing a tax exemption, service charges did not post correctly. This has been corrected.

***Splitting a Check with Non-decimal Japanese Tax Enabled  
Post Accurately to Financial Reports***

SCR 7486

CR ID# 27555

When Japanese tax was enabled with no decimals, splitting a check caused inaccurate financial reports. This has been corrected.

***Voiding and Reapplying the Discount Resulting in Double  
Posting of Inclusive Tax Amount Has Been Fixed***

SCR 7554

CR ID# 27843

When voiding a discount on a check and then reapplying the discount, a double posting of the inclusive tax amount would occur. This has been corrected.

---

**SAR**

***The Formatting of Response Data Printing on Authorization  
Chits has Changed***

SCR 6816

CR ID# 24810

Some credit card drivers may contain specific response data in their authorization response that, if configured to be included, can be printed on authorization chits. Previously, the workstation appended the formatting and labels of the response data. The formatting and labels has been removed.

---

## Winstation

### *All Menu Items now Display Correctly on the Check when using the Split Check Function*

SCR 7387

CR ID# 26849

Previously, if a check included 12 or more menu items, the final item on the check did not display when using the **[557 - Split Check]** function on a WS4LX client running Winstation. This has been corrected.