micros®

Restaurant Enterprise Series (RES) Version 3.2 – Service Pack 7 Hot Fix 5 Documentation

About This Document

This document contains updates to Version 3.2 Service Pack 7 release of the MICROS Restaurant Enterprise Series (RES 3000) software. The changes are not cumulative, but describe additions and revisions relevant to Hot Fix 5 only.

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 not limited to the implied warranties of marketability and fitness for a particular purpose.

Information in this document is subject to change without notice.

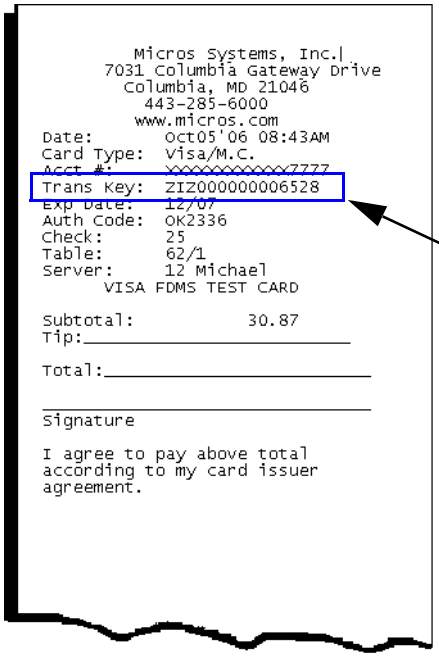
MICROS Systems, Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this document.

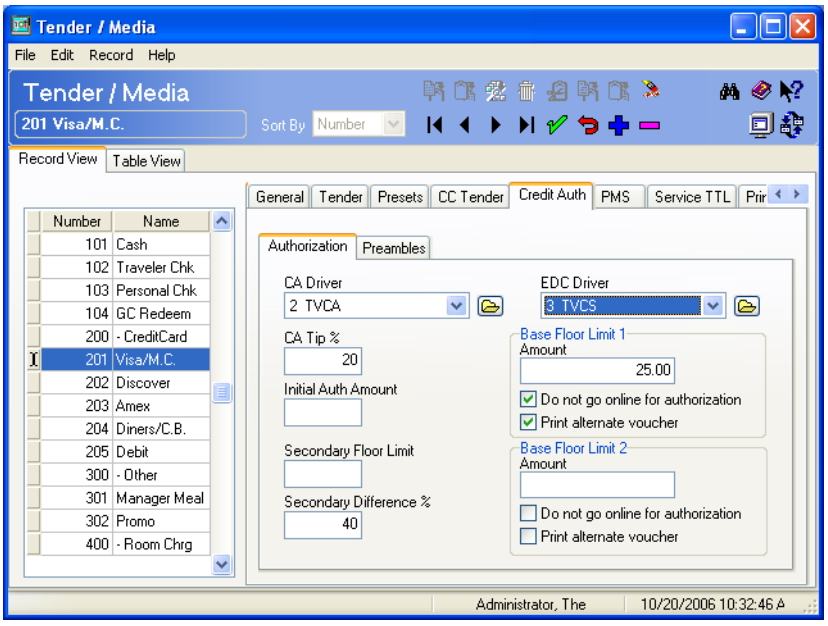
Trademarks

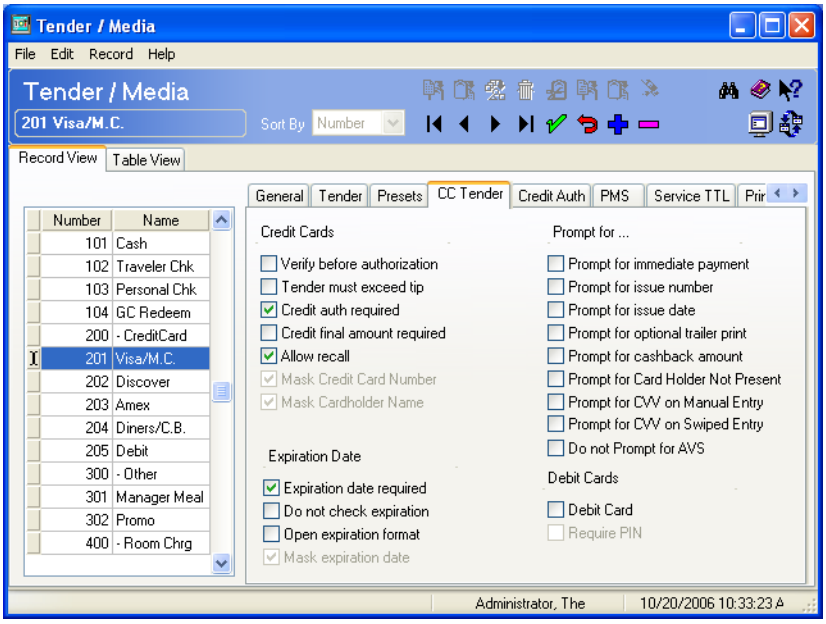
3700 New Features and Enhancements

Module	Feature
CA/EDC	**Settle Credit Card Batches in the Order They are Generated** In previous releases, outstanding credit card batch files were automatically settled by date generated, with the most recent batch being settled first. To improve usability, a new option, **Settle Oldest Batch First** (*System* | *Restaurant* | *Business Settings*) was added in POS Configurator. When checked, the option directs RES to reverse the procedure and settle batches in the order in which they were generated.

Module	Feature
CA/EDC Con't	**TransactionVault Electronic Payment Driver** With this release, RES has added support for Merchant Link's TransactionVault payment solution. Merchant Link's TransactionVault minimizes the vulnerability of the merchant and the POS software. There is no extra hardware to install and maintain, so merchants can continue to use their existing infrastructure. For customers using the MICROS Universal Credit Card Driver processing through Merchant Link, this is the next natural step. At the center of the TransactionVault technology is a key that replaces all cardholder information at the customer site. The key utilizes leading edge encryption technology, which helps to ensure that only TransactionVault can match the key to access the cardholder information. For installation and configuration instructions see the *TransactionVault Payment Driver ReadMe First, MD0003-118*. **How it Works** Traditionally, cardholder data (card number, expiration date, and the cardholder name) is stored by the RES system until it is purged from the system, typically within 90-180 days after settlement. RES automatically detects when TransactionVault payment drivers are installed. When obtaining an authorization for a transaction, the MICROS database will delete the cardholder data from the system, replacing it with a 15-character **TransactionVault Key** obtained from Merchant Link during the authorization process. All cardholder data is stored in Merchant Link's TransactionVault. The TransactionVault Key becomes the reference number for merchants if it is necessary to lookup cardholder data.

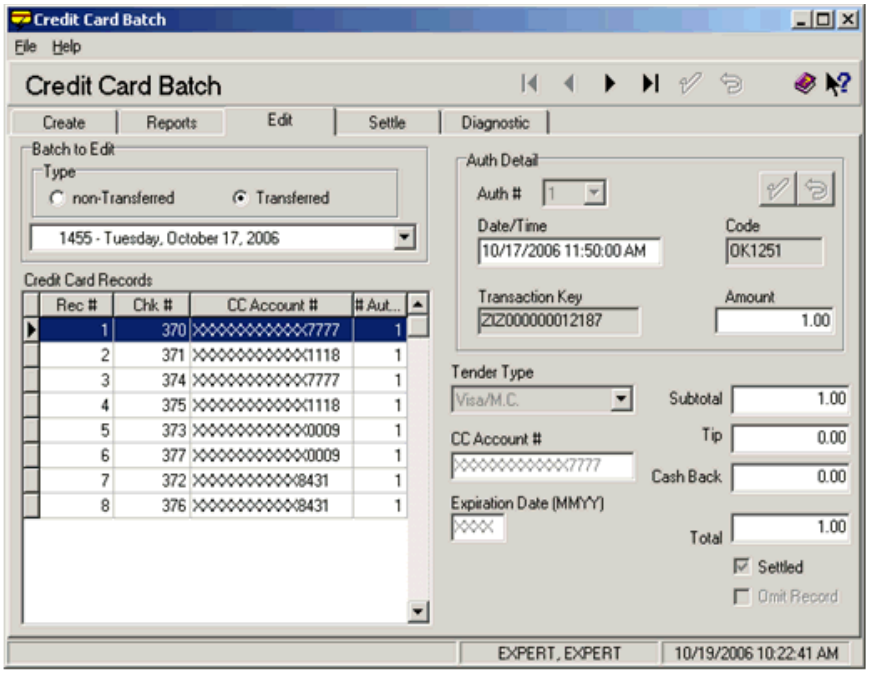
Module	Feature
CA/EDC Con't	The TransactionVault Key is printed on the authorization voucher.  Micros Systems, Inc.| 7031 Columbia Gateway Drive Columbia, MD 21046 443-285-6000 www.micros.com Date: Oct05'06 08:43AM Card Type: Visa/M.C. Acct #: XXXXXXXXXXXX7777 Trans Key: ZIZ000000006528 Exp Date: 12/07 Auth Code: OK2336 Check: 25 Table: 62/1 Server: 12 Michael VISA FDMS TEST CARD Subtotal: 30.87 Tip:_____ Total:_____ _____ Signature I agree to pay above total according to my card issuer agreement. **TransactionVault Key** **NOTE**: The TransactionVault Key must be entered in upper case letters. If there is an error, a message will display the TransactionVault Key number that needs to be altered. There are several instances when cardholder data will be stored on the RES system. We refer to these instances as offline transactions. The following are the four types of offline transactions available through RES: ◆ Credit Transaction ◆ SAR/BSM Transaction ◆ Manual Authorization ◆ Below Floor Limit Transaction Additionally, during authorization, the user will not be prompted to enter Address Verification (AVS) and Credit Card Verification (CVV) for transactions performed offline except for Below Floor Limit Transactions.

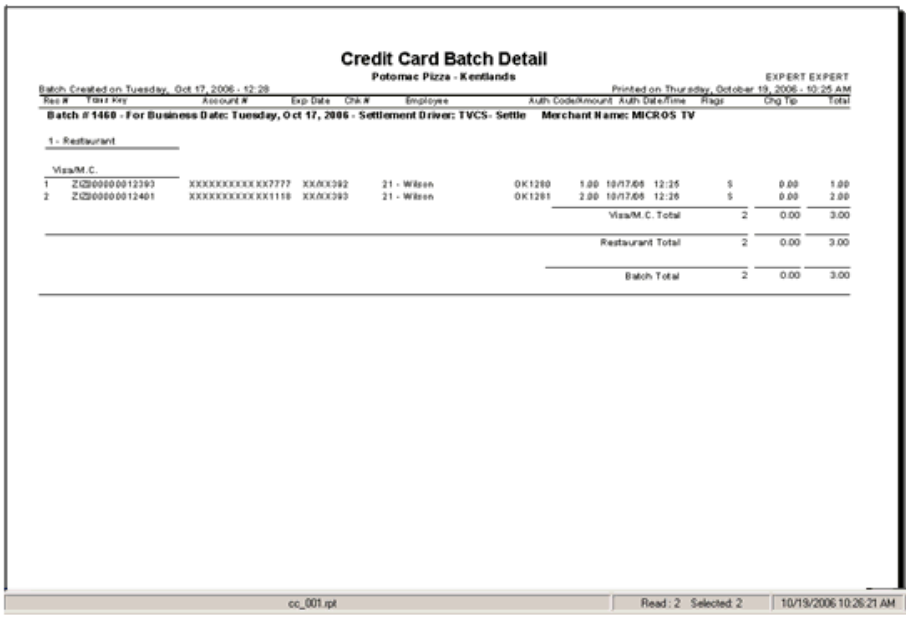
Module	Feature
CA/EDC Con't	When an offline transaction is performed, the system will encrypt and store the cardholder data until the system is online and does a settlement. The settlement process has been enhanced to first process offline transactions, obtaining a TransactionVault Key for each of these transactions, and then deleting cardholder data from the system. Once complete, normal settlement will occur processing all transactions via their TransactionVault Key. **Linking the Driver to a Tender** For installation and configuration instructions see the *TransactionVault Payment Driver ReadMe First, MD0003-118*. The TV Driver is activated by linking it to a tender in POS Configurator. This driver can be linked to any credit card tender. Follow these steps to link a tender to the TV Authorization and Settlement drivers: 1. Go to the *POS Configurator* | *Sales* | *Tender Media* | *Credit Auth* form. 

Module	Feature
CA/EDC Con't	2. Select the tender to be configured (e.g., Visa/ Mastercard). 3. Go to the **CA Driver** drop down box and select the **TVCA** driver. 4. Go to the **EDC Driver** drop down box and select the **TVCS** driver. 5. Save the record. Disabled Options Certain security features present in the TV Driver, such as masked card numbers, cannot be disabled in POS Configurator. Once the TV driver is enabled for a tender, POS Configurator will automatically disable the following options on the *Sales* | *Tender Media* | *CC Tender* form:  ◆ Mask Credit Card Numbers ◆ Mask Cardholder Name ◆ Mask Expiration Date

Module	Feature
CA/EDC Con't	**Corrective Authorization** Occasionally, customer information may be transmitted to the credit card processor with incorrect information. For example, if a customer's card is used on the wrong transaction. When this occurs, the merchant must perform a corrective authorization to adjust the transaction information. When a corrective authorization is performed, the user will be prompted for the **Transaction Key,** the **Authorization Code** and the last 4 digits of the **Account Number**. This information is available on the authorization voucher. If the merchant is unable to retrieve the information, they can contact Merchant Link, LLC. to obtain customer account information. After a corrective authorization is performed, an asterisk will print next to the customer account number and the authorization code on the credit card voucher to indicate that a corrective authorization was performed. For security reasons, the corrective authorization feature is an employee privileged function. To allow an employee to perform this function, enable the **Corrective Authorization** option for the appropriate employee class (*POS Configurator* | *Employees* | *Employee Classes* | *Transactions* | *Transaction Control*).

Module	Feature
CA/EDC Con't	**Settlement** Batch settlement with the Transaction Vault Driver is a two step process. The first step is to submit all offline authorizations to the processor. During this step, the settlement process scans the batch records for any offline authorizations. All offline transactions are processed to Merchant Link where they receive a TransactionVault Key. After all of the records have been issued TransactionVault Keys, the settlement process begins to transmit the batch to the processor. Unlike traditional drivers, TV does not transmit customer information. Instead the RES system sends the TransactionVault Key and the total amount owed to the processor. The processor will then match the TransactionVault Key to the appropriate customer account. Following a successful batch no customer information is stored in the RES system. In previous Credit Card Drivers, an option to Disable Auth Code Limit was available. This option has been omitted from the POS Configurator with the Transaction Vault Driver and it is now enabled by default. If a manual authorization is performed, and the user enters a value greater than 6 characters in the Auth Code field, the settlement driver will truncate the code down to the first 6 characters only. The record will then be settled with the truncated Auth Code. Purge Pre-existing Sensitive Data with the TV Settlement Driver When a site switches to the TransactionVault Driver, there will be transaction and batch detail information resident in the database containing unmasked account numbers, expiration dates, and customer names. To mask this data, the user should perform a settlement using the TV Driver. This will mask all pre-existing data that contains sensitive customer information.

Module	Feature
CA/EDC Con't	Credit Card Batch Utility To support the addition of the TransactionVault Key, a new column has been added in the Credit Card Batch Utility. The **TransactionVault Key** column will list all of the assigned transaction keys. The new column replaces the Customer Name column in the Utility. The Transaction Key can be edited if it is entered manually due to a corrective authorization.  **Touchscreen Keys** The TransactionVault driver requires the addition of the following new touchscreen key to the Payment screen: ◆ **Corrective Authorization** – Allows a privileged user to alter a previously transmitted authorization.

Module	Feature
CA/EDC Con't	**Reports** The following report has been altered to support TransactionVault: ◆ **Credit Card Batch Detail Report –** A TransactionVault Key column has been added to this report. The 15-digit TransactionVault Key associated with the transaction will be listed in this column. The customer name column has been removed from the report.  Credit Card Batch Detail Potomac Pizza - Kentlands Batch Created on Tuesday, Oct 17, 2006 - 12:28 Printed on Thursday, October 19, 2006 - 10:25 AM Batch # 1460 - For Business Date: Tuesday, Oct 17, 2006 - Settlement Driver: TVCS- Settle Merchant Name: MICROS TV 1 - Restaurant Visa/M.C. cc_001.rpt Read: 2 Selected: 2 10/19/2006 10:26:21 AM When a **Corrective Authorization** is performed, an **R** will appear in the *Status* column for that record.
Database	**Two New Columns Added to the mi_dtl Table** The **mi_dtl.ob_is_condiment** and the **mi_dtl.parent_dtl.seq** columns have been added to the **mi_dtl** table to track condiments and their parent items. This information will be available in *mymicros.net* in the future.

Module	Feature
Platform	**Minimum Platform Version Required for UWS4s** In version 3.2 SP7 HF5 the 3700 POS application has changed to support encrypting credit card data. As a result, RES version 3.2 SP7 HF5 or higher requires a minimum platform version for the UWS4's. The WS4 platform must be at GR22 or higher. This platform contains WinCE version 4.2 and MICROS Build version 12.95. If a WS4 at a site is running a lower version and the site is using CA/EDC, the 3700 POS will be unable to properly encrypt the credit card data. This may cause issues when multiple credit cards are on a single check. Follow these steps to verify that your clients are on the correct platform: 1. On the WS4, open Windows Explorer and browse to the *DOC\Utilities* folder. 2. Open **DiagUtility.exe** 3. Verify the WinCE Version is **4.2** and the MICROS Build Version is **12.95**.

Module	Feature
Platform Con't	**RES Security Solution** The release of RES 3.2 SP7 HF5 marks the addition of several data security features. The new and enhanced features described in this section address vulnerability concerns in an increasingly complex and rapidly changing technical environment. RES 3.2 SP7 HF5, when installed with the Transaction Vault Payment Driver Version 4.3, is a Visa Payment Application Best Practice Certified Solution. The MICROS security solution implements strong data encryption (Triple DES 128-bit) at the application level to protect sensitive data wherever it is stored within the RES System. By targeting the application level, the MICROS solution eliminates problems associated with hardware- or transmission-specific processes and protocols. This allows sites to retain their existing hardware or network infrastructure as long as it meets MICROS RES minimum system requirements. In many cases, hardware- or protocol-level security can be enabled as an added means to secure sensitive data. This section provides an overview of the RES Security Solution and discusses the areas that are affected by the changes. Topics covered include: ◆ Encryption ◆ Default User Changes ◆ Security Log ◆ Network Shares **NOTE:** Product design alone does not ensure system security. MICROS customers also bear responsibility for implementing their own security policies and procedures with regard to hiring practices, system access, and network firewalls.

Module	Feature
Platform Con't	**Encryption** Securing the system involves protecting the following type of data: ◆ **Data at Rest** – Refers to data stored on persistent media, such as the system database or in the operating system's file system. To secure data in this state, RES employs strong data encryption using an industry-standard algorithm, Triple DES. This algorithm is based on a complex system of mathematics that are used to scramble the original data, rendering it unreadable to anyone outside the secure system. The encryption mechanism includes the creation and storage of one or more software 'keys' that are used to encrypt and decrypt the data. Encrypted Areas The RES system includes a number of data storage and relay components where data is accessible. For this reason, data encryption is applied in multiple layers across the following area: ◆ **Data at Rest** RES stores information (data at rest) in three areas: 1) the in-store database, 2) the backup server database, and 3) the SAR client (standalone resilience) database. Each of these areas contains both *sensitive* and *non-sensitive* information. The server retains a copy of all three, but only the last two are kept locally on each client. The in-store database is a long-term storage component for the site's data. The majority of information stored by RES is considered *non-sensitive*. That is, it includes all the options necessary to configure and run the program (touchscreen layouts, number of devices, business settings, etc.), as well as the historical transaction data (items, quantities, prices) gathered in the course of business. *Sensitive* data refers to personal credit card information (customer names, account numbers, expiration dates) that are protected by law and must be guarded against accidental or improper disclosure.

<table>
<tr><th>Module</th><th>Feature</th></tr>
<tr><td>Platform Con’t</td><td>
For the in-store database, encryption is applied to sensitive data before it is stored in the database. This is done at the application level, by the program that writes the data to the database. When required, only those applications that need to will decrypt the data. For all other users, this data will appear encrypted when accessed via SQL tools.

The following chart lists by table and field, the information that is encrypted before it is posted to the database:

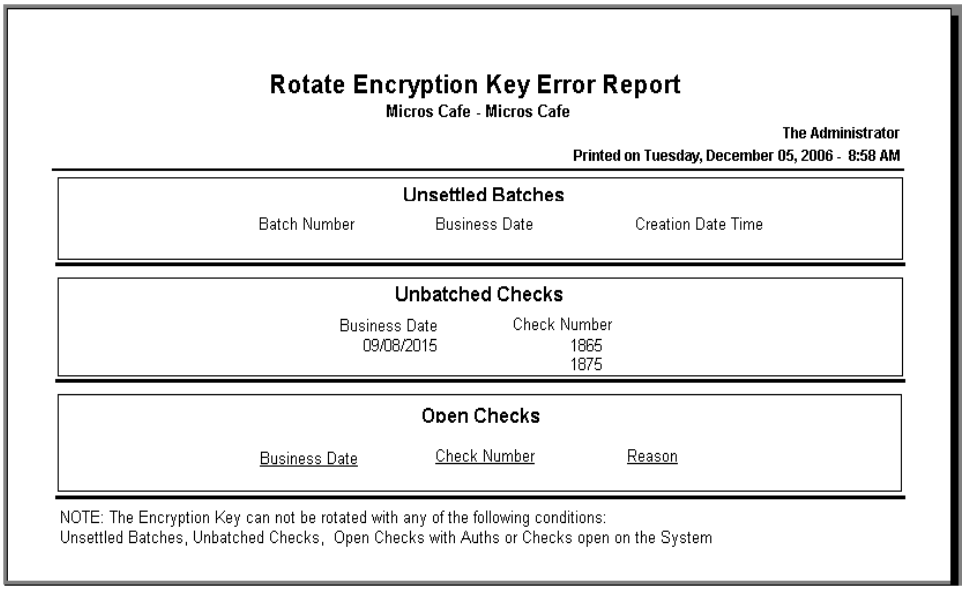
<table>
<tr><th>Table</th><th>Field</th></tr>
<tr><td>cc_auth_dtl</td><td>cc_acct_num
customer_name
expiration_date
track_2_data</td></tr>
<tr><td>cc_batch_item_dtl</td><td>cc_acct_num
customer_name
expiration_date
track_2_data</td></tr>
<tr><td>cc_batch_xfer_item_status</td><td>cc_acct_num (stored masked)
expiration_date (stored masked)</td></tr>
<tr><td>cc_vchr_dtl</td><td>cc_acct_num</td></tr>
<tr><td>tmed_dtl</td><td>cc_acct_num
expiration_date</td></tr>
<tr><td>ref_dtl</td><td>ref (only if reference entry is a credit card number)</td></tr>
</table>

RES addresses the problem of data temporarily stored on a workstation, including devices configured for Standalone Resiliency (SAR) or Backup Server Mode (BSM), by applying Triple DES encryption to the sensitive data before storing it in temporary files on the RES client. These temporary files are only retained for a short period of time before being deleted from the system. For added security, hardware- and transportation-level protocols such as IPSEC, WEP, and WPA can be used to encrypt transmissions.
</td></tr>
</table>

Module	Feature
Platform Con't	Key Generation and Storage The RES security paradigm requires the use of encryption keys in three areas: ◆ Encryption of sensitive data in the database. ◆ Encryption of sensitive data in the Standalone Resiliency files on each client (also known as the local database). ◆ Encryption of sensitive data in the Backup Server files (SAR files managed at a central server). Encryption keys are typically generated by inputting a pass-phrase and a series (typically 12 or more) of random bits known as a *Salt* value into a key derivation function or algorithm. This algorithm produces a key that is stored encrypted in the database or an access-controlled section of the *Registry,* referred to as the **Key Store**. During the initial installation or conversion to RES 3.2 SP7 HF5, a default key is provided. The default key allows sites to run the system. MICROS recommends that the key be rotated on a regular basis or if it is suspected that the system has been compromised. To secure this data, RES uses the Microsoft Crypto API. The data is encrypted using the Triple DES symmetric key algorithm. This algorithm supports 168 bit key length, uses cipher block chaining, and the block size is 643 bits. The RES pass phrase is generated from two different sources. The first source is the **Windows registry**. POS clients test for the presence of this key. If this key fails to exist (because it was deleted, or it never existed to begin with), the POS clients will generate a random 256 byte pass phrase using the Windows API function. This random pass phrase will combine with a pass phrase contained inside the application to create a unique pass phrase, which in turn will create a unique encryption key for each POS client. This key will be used to encrypt sensitive data contained within the SAR and BSM local databases.

Module	Feature
Platform Con't	The second source is the **RES database**. Similar to the POS clients, the RES Database Service will check for the existence of the pass phrase in the database. If the pass phrase does not exist (because it was deleted, or never existed to begin with), the RES Database Service will generate a random 256 byte pass phrase. This random pass phrase will combine with a pass phrase contained inside the application to create a unique pass phrase, which will in turn create a unique encryption key for the database. This key will be used to encrypt sensitive data contained within the RES database on the Server. Sensitive Data With this release, there are several changes to the way that sensitive data is stored: 1. We now encrypt sensitive card data stored in the database. Sensitive data is defined as the following: ◆ Credit Card Number ◆ Credit Card Expiration Date ◆ Cardholder Name The data is encrypted in both the database on the server and in the local database when SAR or BSM is enabled. The sensitive data encryption key is used to encrypt this data. Please see the next section for more information on how to rotate the sensitive data encryption key. 2. When the Transaction Vault Payment Drivers are installed, all tenders linked to those drivers will mask the card number and expiration date when it is printed, displayed, and stored.

Module	Feature
Platform Con't	3. When tenders are not linked to the Transaction Vault Payment Driver, the card number and expiration date will be masked and stored. The system will print and display card numbers and expiration dates based on the following Tender/Media settings: ◆ POS Configurator | Sales | Tender/Media | CC Tenders | Mask Credit Card Number ◆ POS Configurator | Sales | Tender/Media | CC Tenders | Mask Expiration Date 4. The employee class option to override credit card masking (*POS Configurator* | *Employees* | *Employee Classes* | *Privileges* | *Privilege Options* | *Override credit card masking)* no longer works in this version. ◆ **Rotate the Sensitive Data Encryption Key** The end user has the ability to rotate their system's Sensitive Data Encryption Key as part of their maintenance process. This provides added security to the user. Periodic rotation will significantly decrease the likelihood that the encryption key will be compromised by an outside party. MICROS recommends that the encryption key be rotated periodically. If you believe that your encryption key has been compromised then rotate the key immediately. In order for rotation to be successful the following criteria must be met: ◆ All checks must be service totaled (not open on the system). ◆ All checks with an authorization must be closed. ◆ All checks with credit card tenders must be batched. ◆ All credit card batches must be settled.

Module	Feature
Platform Con't	A new report has been added to assist the user in determining if all criteria has been met. The **Rotate Encryption Failure Report (cc_003.rpt)** will list all open checks, initial authorizations that have not been finalized, unsettled credit card batches, and unbatched checks. 

Rotate Encryption Key Error Report

Micros Cafe - Micros Cafe

The Administrator

Printed on Tuesday, December 05, 2006 - 8:58 AM

Unsettled Batches

Batch Number	Business Date	Creation Date Time

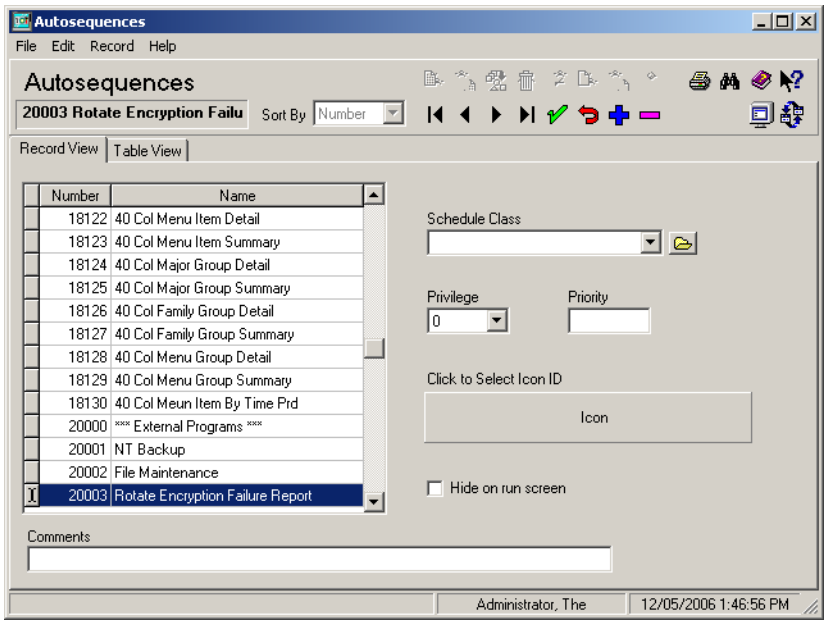
Unbatched Checks

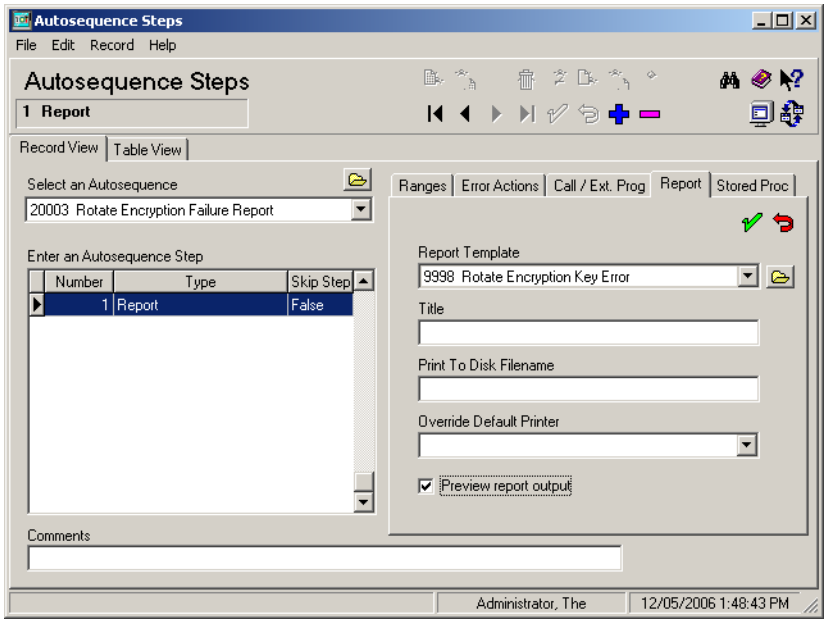
Business Date	Check Number
09/08/2015	1865
	1875

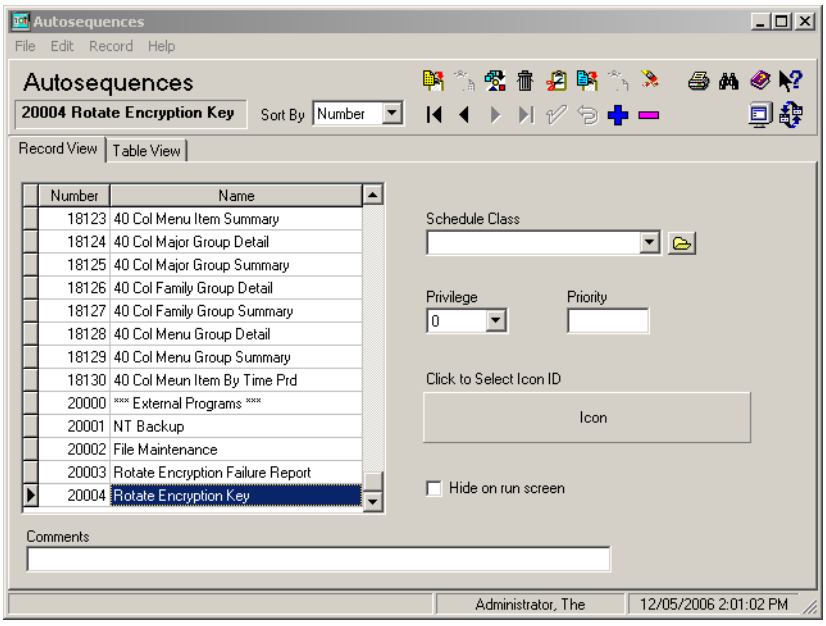
Open Checks

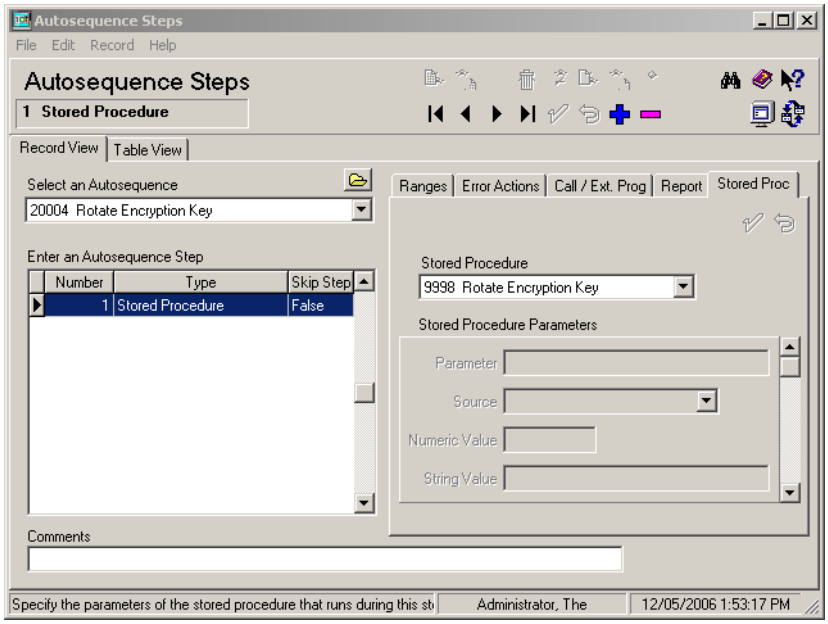
Business Date	Check Number	Reason

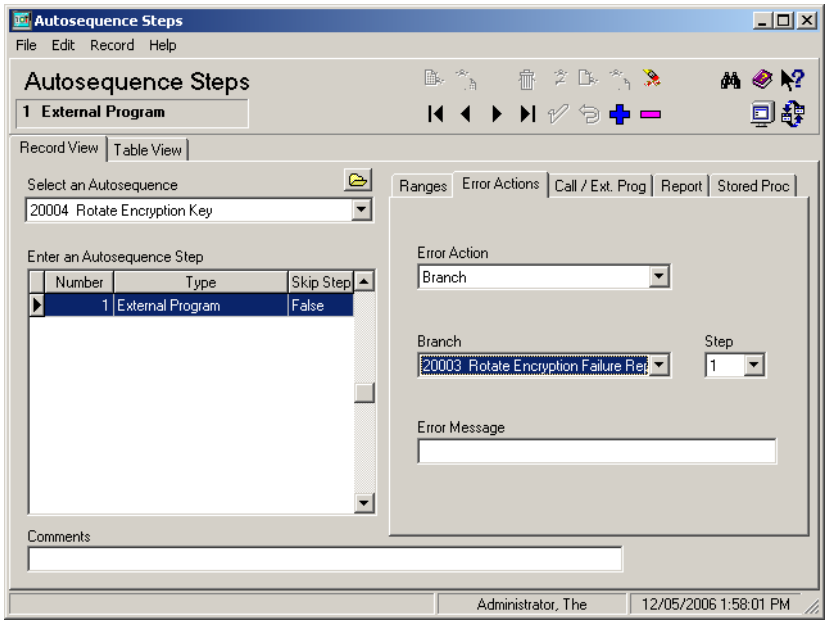
NOTE: The Encryption Key can not be rotated with any of the following conditions:
Unsettled Batches, Unbatched Checks, Open Checks with Auths or Checks open on the System

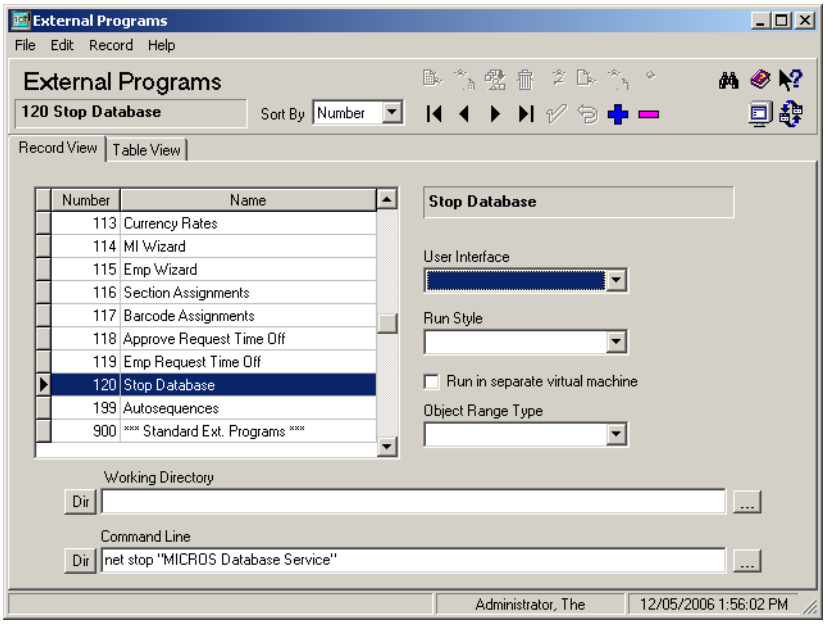
Module	Feature
Platform Con't	◆ **Rotate Encryption Key Autosequences** To support this feature two new autosequences should be added. Do not run these steps as part of a scheduled autosequence, a user should be present when these autosequences are run. ◆ **Rotate Encryption Failure Report**. Generates a report to identify why the encryption key rotation failed. Follow these steps to add this autosequence:  1. Go to *POS Configurator*	*Reporting*	*Autosequences* and add an autosequence record. Configure the following fields: ◆ Under the *Name* column enter **Rotate Encryption Failure Report** and *Save* the record.

Module	Feature
Platform Con't	2. Go to *POS Configurator* | *Reporting* | *Autosequence Steps* and select the **Rotate Encryption Failure Report** record created in the previous step.  3. Add a new autosequence step and configure the following fields: ◆ Under the *Type* column select **Report**. ◆ From the **Report Template** drop-down menu select number **9998 Rotate Encryption Key Error**. ◆ Enable the **Preview Report Output** option. 4. Save all changes.

Module	Feature
Platform Con't	◆ **Rotate Encryption Key**. Allows the user to rotate the system's encryption key and then stops the database. Follow these steps to add this autosequence: 1. Go to *POS Configurator* | *Reporting* | *Autosequences* and add an autosequence record. Configure the following field:  ◆ Under the *Name* column enter **Rotate Encryption Key**.

Module	Feature
Platform Con't	2. Go to *POS Configurator* | *Reporting* | *Autosequence Steps* and select the **Rotate Encryption Key** created in the previous step.  3. Add a new autosequence step and configure the following fields: ◆ Under the *Type* column select **Stored Procedure**. ◆ From the **Stored Procedure** drop-down menu select number **9998 Rotate Encryption Key**.

Module	Feature
Platform Con't	4. Go to the *Error Actions* tab and configure the following fields:  ◆ From the **Error Action** drop-down menu select **Branch**. ◆ Use the **Branch** drop-down menu to select an autosequence that will run if an error occurs. Select the **Rotate Encryption Failure Report**. ◆ In the *Step* drop-down menu select the value of **1**.

Module	Feature
Platform Con't	5. Now you will need to create an external program that stops the database. *Go to POS Configurator* | *System* | *External Programs* and add a record. Configure the following fields:  ◆ Under the *Name* column enter **Stop MICROS Database Service**. ◆ In the **Command Line** enter the following: **net stop "MICROS Database Service"** ◆ Save the record. 6. Go to *POS Configurator* | *Reporting* | *Autosequence Steps* | *Rotate Encryption Key.* ◆ In the *Type* column, add an additional record and select **External Program**. ◆ Select the **Stop MICROS Database Service** external command that was created in step 5. 7. Save the record.

Module	Feature
Platform Con't	Follow these steps to rotate the sensitive data encryption key: 1. Make sure no one is using the 3700 POS. Use the Control Panel to take the system to the database level. 2. Run the **Rotate Encryption Key** autosequence. 3. If the autosequence is successful then reboot the system. 4. If the autosequence fails, review the **Rotate Encryption Failure Report** and correct the issues. When finished follow the steps to rotate the key again. If this autosequence runs successfully then the following will occur: ◆ The encryption key will be changed for all new posted transactions. ◆ The Database Service will stop so that the new encryption key can be in place for the next transaction. If this autosequence does not run successfully then the following will occur: ◆ The encryption key will not change. ◆ The Rotate Encryption Key Error Report will display with information regarding why the system did not rotate the key.

Module	Feature
Platform Con't	**Default User Changes** To provide additional security, the following default user changes have occurred: New DBA and MICROS Database Passwords Changed The DBA and MICROS database passwords have been changed. Required Windows microssvc User Changes Once 3.2 SP7 HF5 is installed, by default, **scheduled autosequences will no longer be run as the microssvc user**. Depending upon what your autosequences do, you need to make changes to re-enable the autosequence server to successfully run autosequences as the microssvc user. Some known reasons that autosequences may need to be run as the microssvc user include: ◆ They depend upon the default Windows printer of the microssvc user. ◆ They require access to network resources for: ◆ Backing up files to network shares ◆ Printing to networked Windows printers

Module	Feature
Platform Con't	**After 3.2 SP7 HF5 has been installed, follow the steps below to configure the Windows "microssvc" user.** **<u>Part 1:</u> Give the microssvc user rights to allow it to log on as a batch job** 1. For a new installation log on as *microssvc*, select a Default Printer, and log off. Sites upgrading do not need to do this. 2. As an Administrator go to *Programs* | *Administrative Tools* | *Local Security Policy.* 3. Expand **Local Policies**. 4. Select **User Rights Assignment**. 5. Double-click on **Log on as a batch job**. 6. Click **Add**. 7. Select *microssvc* from the list of users (the **Look In**: field should be the local PC name by default). 8. Click **Add** and then click **Ok**. 9. Verify that the *microssvc* user has been added to the displayed list. 10. Close the *Local Security Settings* window.

Module	Feature
Platform Con't	**<u>Part 2: Give the microssvc user rights to the MachineKeys Crypto folder</u>** 1. Log on as a Windows User with Administrative Privileges. 2. Open Windows Explorer and navigate to <*Windows Drive*> | *Documents and Settings* | *All Users* | *Application Data* | *Microsoft* | *Crypto* | *RSA* | *MachineKeys* folder. 3. Right-click on the *MachineKeys* folder and select **Properties**. 4. Select the *Security* tab and click **Add**. 5. Select *microssvc* from the list of users (the **Look In:** field should be the local PC name by default). 6. Click **Add** and then click **Ok**. 7. Verify that the *microssvc* user has been added to the displayed list. In the *Permissions***:** list, check the **Read**, **Read & Execute**, and the **List Folder Contents** boxes. 8. Click **Ok** to save, then close Windows Explorer. 9. Reboot the system.

Module	Feature
Platform Con't	Recommended Windows microssvc User Security Changes MICROS recommends changing the characteristics of the Windows microssvc user to ensure your system is secure. The applications that require the microssvc user have been changed so that the microssvc user can be setup to deny interactive logon. By doing this the system can be setup so that no unauthorized user may log onto the Windows desktop using the microssvc account. **Once 3.2 Sp7 HF5 is installed, the following steps should be taken to ensure that the microssvc user is secure on the RES Server:** 1. For a new installation log on as *microssvc*, select a Default Printer, and log off. Sites upgrading do not need to do this. 2. As an Administrator open *Programs* | *Administrative Tools* | *Local Security Policy.* 3. Expand **Local Policies.** 4. Select **User Rights Assignment**. 5. Double-click on **Deny logon locally**. 6. Click **Add**. 7. Select *microssvc* from the list of users (the **Look In:** field should be the local PC name by default). 8. Click **Add** and then click **Ok**. 9. Verify that the *microssvc* user has been added to the displayed list. 10. Close the *Local Security Settings* window and Reboot. Once set, you should not be able to logon as the microssvc user, but Autosequences will run as the microssvc user and use the Default Printer originally assigned to the microssvc user as needed.

Module	Feature
Platform Con't	**MICROS Security Log** Many financial agencies (e.g., VISA, CISP, AIS, PCI) now require an audit trail (or log) of all activities that involve access to sensitive data. The entries posted to the log must be reviewed on a regular basis for irregularities and an audit trail history must be maintained. Should a problem arise with an account, the audit trail would allow investigators to assess whether or not security has been breached, and if so, determine how to prevent such actions in the future. To comply with the business requirement, a new MICROS Security Log was added. The Security Log is installed as a custom plug-in to the Microsoft® Event Viewer along with the rest of the RES software. The default setting is enabled. Audited Activities The Security Log was designed to record when potentially sensitive or security-related data is accessed, edited, or deleted on any RES application. Auditable activities are determined by the system and are posted automatically to the Log.

<table>
<tr><th>Module</th><th>Feature</th></tr>
<tr><td>Platform Con’t</td><td>The following table lists the MICROS applications, options, and activities that are tracked in the Security Log.
<table>
<tr><th>Application</th><th>Activity</th></tr>
<tr><td>Autosequences & Reports (AutoSeqExec.exe)</td><td>All successful and unsuccessful login attempts
Report preview or Report print (including the name of the specific report)</td></tr>
<tr><td>Autosequence Server (AutoSeqExec.exe)</td><td>Anytime a report is previewed or printed via a scheduled autosequence (records autosequence number, step, and report name)
Anytime a report is run via POS Operations (records name of logged-in user and report)</td></tr>
<tr><td>Credit Card Utility (CreditCards.exe)</td><td>All successful and unsuccessful login attempts
Batch creation
Report preview or Report print (including the name of the specific report)
Access to the batch edit form
Any edits to credit card data (account number, expiration date) on the batch edit form
Batch settlement</td></tr>
<tr><td>Report Explorer (RptExpl.exe)</td><td>All successful and unsuccessful login attempts
Report preview or Report print (including the name of the specific report)</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Module</th><th>Feature</th></tr>
<tr><td>Platform Con’t</td><td>
<table>
<tr><th>Application</th><th>Activity</th></tr>
<tr><td>POS Configurator
(Poscfg.exe)</td><td>
• All successful and unsuccessful login attempts
• Access, Edit, or Delete to the following forms:
• System | Restaurant
• Business | Settings:
- (Save Batch Records) Number of Days
• Security:
- (Enhanced Password)
Use MICROS Classic Security
Days Until Password Expires
Maximum Idle Time in Minutes
Minimum Password Length
Maximum Failed Logins
Require AlphaNumeric Passwords
Password Repeat Intervals
• Options:
- (Restrict Access to Employee Data)
No Access Limitation
Same level or lower
Lower level only
- (Date/Time)
European date format
European time format
- Weight in kilograms
• Taxes:
- Enable US tax or Canadian GST
- Enable Singapore Tax
- Enable Canadian Tax
- Enable Florida surcharge tax
- Enable Japan tax
- (VAT Tax Method)
Post taxable totals only
VAT by round
VAT by item
- Australian GST is active
- GST Prompt Threshold
- Enable Thai Tax
</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Module</th><th>Feature</th></tr>
<tr><td>Platform Con’t</td><td>
<table>
<tr><th>Application</th><th>Activity</th></tr>
<tr><td>POS Configurator
(Poscfg.exe)</td><td>
• Sales | Tender/Media

• General:
- Type

• Tender:
- Post to charge receipts
- Post to gross receipts

• CC Tender:
- Verify before authorization
- Tender must exceed tip
- Credit auth required
- Credit final amount required
- Allow recall
- Mask Credit Card Number
- Mask Cardholder Name
- Debit Card
- Require PIN
- Prompt for immediate payment
- Prompt for issue number
- Prompt for issue date
- Prompt for option trailer print
- Prompt for cashback amount
- Prompt for Card Holder Not Present
- Expiration date required
- Do not check expiration
- Open expiration format
- Mask expiration date

• Credit Auth:
- CA Driver
- EDC Driver
- CA tip %
- Initial Auth Amount
- Secondary Floor Limit
- Secondary Difference %

• Printing:
- Print with lookup
</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Module</th><th>Feature</th></tr>
<tr><td>Platform Con’t</td><td>
<table>
<tr><th>Application</th><th>Activity</th></tr>
<tr><td>POS Configurator
(Poscfg.exe)</td><td>
Revenue Center | RVC Credit Cards

General:
- Suppress amount on initial authorization
- Suppress linefeeds after voucher
- Authorize below CA floor message
- Allow 20 reference characters
- Confirm customer signature
- Disable charged tip
- Do not add estimated tips to CC authorization
- Disable prompt for Card Holder Not Present
- (CA Status)
Enable CA status display
Display for entire RVC

Headers:
- CC Voucher Header

Trailers:
- Customer CC Trailer
- Customer Initial Auth Trailer
- Customer Optional 2nd Trailer
- Customer Cashback Trailer
- Merchant CC Trailer
- Merchant Initial Auth Trailer
- Merchant Optional 2nd Trailer
- Merchant Cashback Trailer

Floor Limits:
- Enable secondary floor limit %
- Enable secondary floor limit amount

Printing:
- Print two vouchers
- Print voucher in background
- Print initial credit authorization voucher
- Print voucher after secondary authorization
- Do not print customer name on voucher
- Show REPRINT on voucher
- Print TOTAL on voucher
</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Module</th><th>Feature</th></tr>
<tr><td>Platform Con’t</td><td>
<table>
<tr><th>Application</th><th>Activity</th></tr>
<tr><td>POS Configurator
(Poscfg.exe)</td><td>
• Revenue Center | RVC Transactions

• General:
- Tax Florida Surcharge
- Print/Display lb. weight with 2 decimal places

• Employees | Employee Classes

• Privileges | Privilege Levels:
- Mgr Procedures
- POS Config.

• Privileges | Privilege Options:
- Use Reports
- Clear all totals
- Access to apps using password ID
- (Credit Card Batch)
Create
Edit
Reporting
Settle

• Options:
- Pay canceled credit auth
- Mgr Procedures emp ID
- POS Configurator emp ID

• Printing:
- Reprint Credit Card Voucher

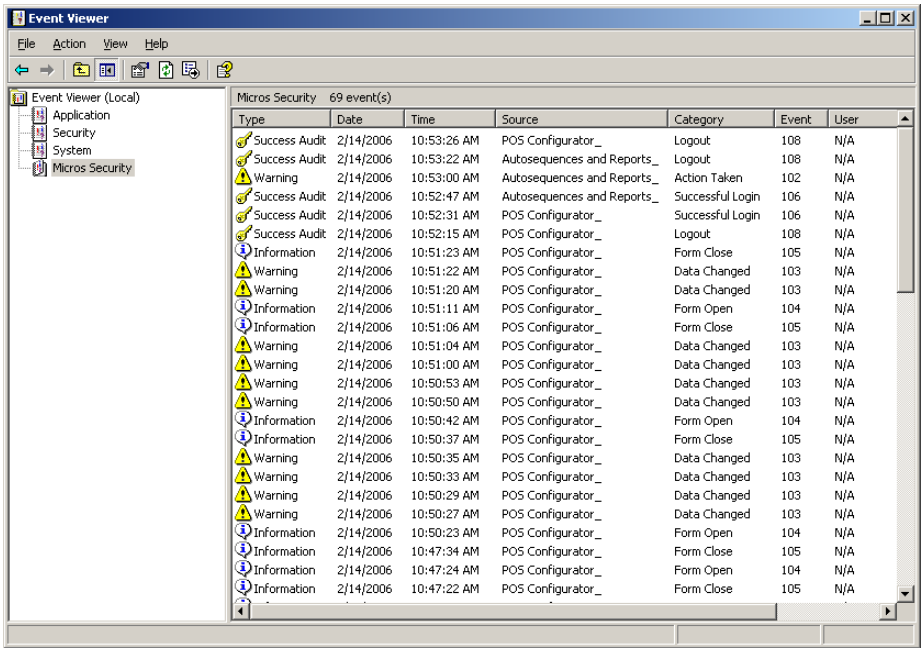
• Employees | Employees

• Security:
- User Account Disabled
- User must change password at first logon
- User ID
- User Password

• POS Configurator | Totals

• Clear All Totals
• Clear Labor Totals
• Clear Sales Totals
</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Module</th><th>Feature</th></tr>
<tr><td>Platform Con’t</td><td>
<table>
<tr><th>Application</th><th>Activity</th></tr>
<tr><td>GSS Backoffice
(GSS.exe)</td><td>• All successful and unsuccessful login attempts
• Access to all forms (edits not recorded)</td></tr>
<tr><td>Export Utility
(ExportUtility.exe)</td><td>• All successful and unsuccessful login attempts
• All queries run</td></tr>
<tr><td>Transaction Analyzer
(Analyzer.exe)</td><td>• All successful and unsuccessful login attempts
• Whenever a query is created
• Whenever a query is run
• Whenever a query is saved
• Records all query details</td></tr>
<tr><td>Forecast Setup
(ForecastSetup.exe)</td><td>• All successful and unsuccessful login attempts</td></tr>
<tr><td>Forecasting
(Forecasting.exe)</td><td>• All successful and unsuccessful login attempts</td></tr>
<tr><td>Human Resources
(HumanResources.exe)</td><td>• All successful and unsuccessful login attempts</td></tr>
<tr><td>Labor Management
(LM.exe)</td><td>• All successful and unsuccessful login attempts</td></tr>
<tr><td>Language Administration
(Translate.exe)</td><td>• All successful and unsuccessful login attempts</td></tr>
<tr><td>MICROS Security Audit Log</td><td>• Logs rotation of Event Viewer Log (adds an entry to existing log and new log</td></tr>
<tr><td>Payroll Preprocessing
(PayrollPre.exe)</td><td>• All successful and unsuccessful login attempts</td></tr>
<tr><td>Product Management
(PM.exe)</td><td>• All successful and unsuccessful login attempts</td></tr>
<tr><td>Scheduling
(Scheduling.exe)</td><td>• All successful and unsuccessful login attempts</td></tr>
</table>
</td></tr>
</table>

Module	Feature
Platform Con't	Viewing Events Events posted to the Security Log can be viewed through the Microsoft® Event Viewer utility (*Start* | *Programs* | *Administrative Tools* | *Event Viewer*). A sample report is shown below:  **NOTE:** All users on the Windows 2000 platform will have read-only rights to the Event Viewer log. To manipulate the file (i.e., backup, delete, etc.), a user must be logged in with Administrative-level privileges. Users can temporarily limit the number of entries displayed by applying a data filter (*Action* | *Properties* | *Filter*). Filters are only applicable for the current session. Once the Event View is closed, the filter is removed.

<table>
<tr><th>Module</th><th>Feature</th></tr>
<tr><td>Platform Con’t</td><td>

- **Viewing Details**

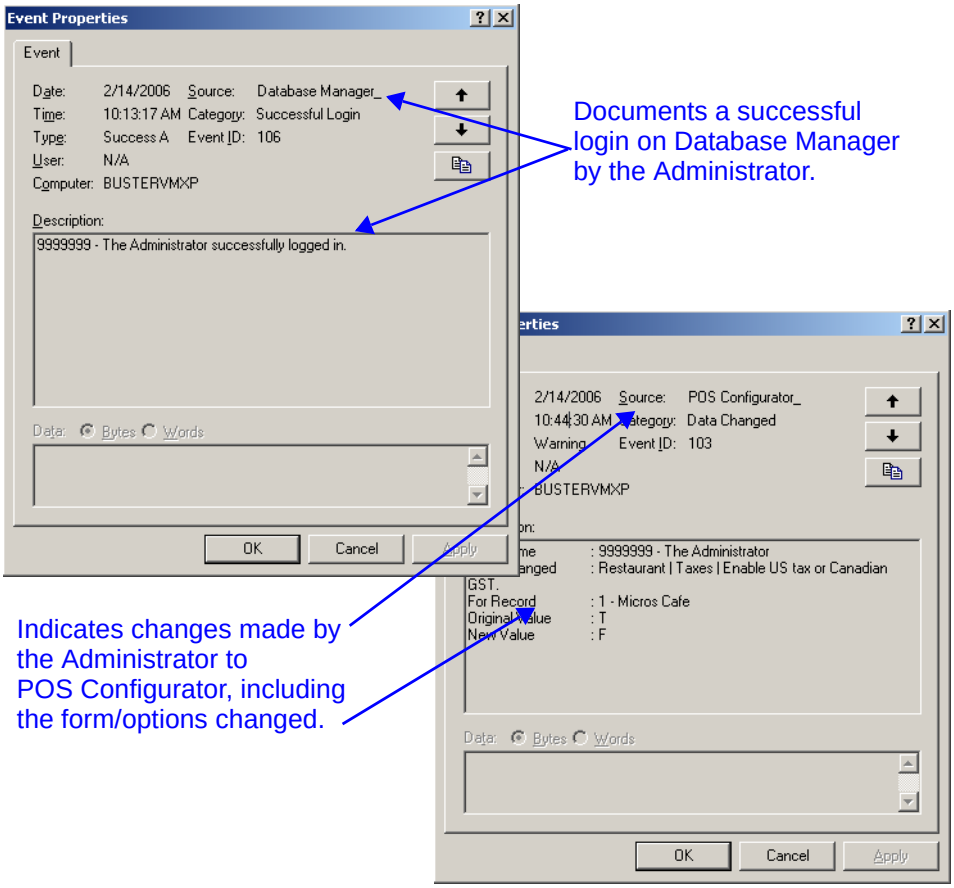
Event details can be viewed by double-clicking the item and opening the individual record. For each event logged, the system provides these details:

- **Date** — Date action occurred.
- **Time** — Time action occurred.
- **Source** — RES application where the activity occurred.
- **Type/Category** — Event label and descriptor. The options are:

<table>
<tr><th>Type</th><th>Category</th></tr>
<tr><td>Success Audit</td><td>Successful Login
Logout</td></tr>
<tr><td>Failure Audit</td><td>Failed Login</td></tr>
<tr><td>Warning</td><td>Data Changed</td></tr>
<tr><td>Information</td><td>Form open
Form close
Action Taken</td></tr>
</table>

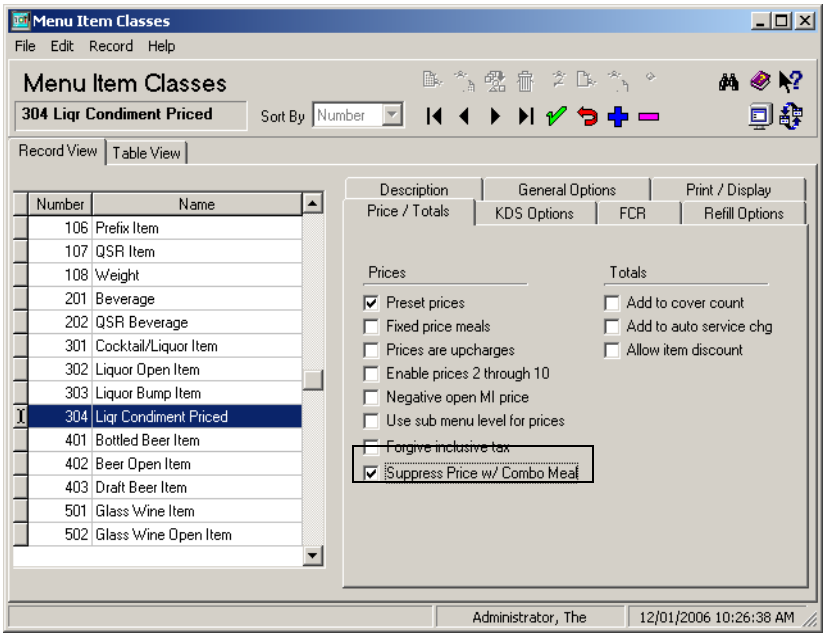
- **Event** — ID number.
- **User** — Name of the remote operating system user, if any.
- **Computer** — Computer name where event occurred.
- **Description** — Details of the event, including the user name, forms accessed (if any), and any changes made to the actual options.

</td></tr>
</table>

Module	Feature
Platform Con't	For example: 

Module	Feature
Platform Con't	Audit Trail History One of the auditing requirements is the ability to retain a backup copy of the MICROS Security Log for historical purposes. This can be done either in the Event Viewer or from the MICROS Security Utility. ◆ **Event Viewer** Users can backup the MICROS Security Log from the Event Viewer by selecting *Action* | *Save Log File As* from the toolbar. The system will prompt for a file name and location. By default, all logs are saved as **xxx.evt** files, which cannot be read except through the Event Viewer. They can also be saved as text (***.txt**) and comma-delimited (***.csv**) files for import into an external application. ◆ **MICROS Security Utility** The MICROS Security Utility includes options for backing up the MICROS Security Log. Users can only specify where to store the backup. The default filename is **Microssecuritylogyyyymmdd.evt**. For example: *Microssecurityutil.exe -b d:\logbackup* MICROS recommends backing up the Event log as part of your nightly file maintenance routine. The utility can be added to your End of Night Autosequence.

Module	Feature
Platform Con't	**Network Shares** Security Enhancement to MICROS Shares Previously, all users were given full control to access the MICROS share files. As a security precaution, share permissions are now limited to Read Only for all users. This change effects the following MICROS share drives: ◆ MICROS_APP ◆ MICROS_DB ◆ NETSETUP **Risk Management** Maintaining a secure network requires more than encryption and passwords. To ensure data privacy, users must assume some responsibility for establishing a secure work environment and for implementing policies and procedures that protect their system as well as their customer's personal information.

Module	Feature
POS Operations	**Option Added to Ignore Condiment Pricing When Rung as Part of a Combo Meal** The user now has the ability to determine whether a condiment's price, when rung up as part of a combo meal, will be ignored or added to the price of the meal. To ignore the condiment price when included in a combo meal enable the **Suppress Price w/Combo Meal** option (*POS Configurator* | *Sales* | *Menu Item Classes* | *Price / Totals*). This option is only available if the Menu Item Class is identified as a condiment. This option is disabled by default. 

3700 POS Revisions

Module	Feature	CR ID
CA/EDC	**User Not Prompted for CVV Value When Using the Credit Card Lookup Function** When the **Prompt for CVV on Manual Entry** option (*POS Configurator* | *Sales* | *Tender Media* | *CC Tender*) was enabled, and the Credit Card lookup option was used, the system would not prompt the user to enter the CVV number. This has been corrected.	**23325**
Database	**Dly_Sys_Fixed_Period_Ttl and the Dly_RVC_Fixed_Period_Ttl Tables Would Be Mismatched Until Totals Were Reposted** Previously, it was possible for the **Dly_Sys_Fixed_Period_Ttl** and the **Dly_RVC_Fixed_Period_Ttl** tables to not match until all totals were reposted at the end of the day. This issue has been corrected.	**22417**

Module	Feature	CR ID
Enterprise Management	**EM Stores Unable to Receive Packages from Corporate** Previously, in certain instances, EM stores were unable to receive packages distributed by EM Corporate. ◆ An existing EM store that upgraded to RES 3.2 SP7 HF5 will **not be affected**. ◆ An existing store that upgraded to RES 3.2 SP7 HF5 that had to re-install EM **will be affected**. There are two ways to solve this problem: ◆ After re-installing EM, re-install RES as well. ◆ Install a database that has been upgraded to fix this issue (attached to the clarify solution). Contact Micros support staff for more information. ◆ A site with a version of RES greater than or equal to 3.2 SP7 HF5 but less than 3.2 SP8 that is installing EM for the first time **will be affected**. To resolve the issue install a database that has been upgraded to correct this issue (attached to the clarify solution) after installing EM. Contact Micros support staff for more information.	**23315**
Hand Held Device	**Symbol 2800 Requires Operating System and Platform Upgrade to be Compatible With RES 3.2 SP7 HF5** In order for the Symbol 2800 device to function properly running RES 3.2 SP7 HF5 or higher, the Operating System and the Platform must be upgraded. Follow the instructions below to perform the upgrade. A single cradle charging unit is required to update successfully.	**N/A**

Module	Feature	CR ID
Hand Held Device Cont'd	1. Upgrade the Symbol 2800 Operating System to PocketPC 2003, using the utilities and instructions provided in the MICROS Upgrade Kit (*Part Number 600456-070*). **NOTE**: Only the Color Model of the Symbol 2846 (64MB RAM) can be upgraded at this time. The Monochrome 2846 (32MB RAM) is not compatible with the RES 3.2 SP7 HF5 software. 2. Connect via Active Sync to the handheld device and navigate to the *\Temp* directory. Select *Explorer* | *My Windows Mobile Device* | *Temp*. 3. Delete any files remaining from the MicroP image update. 4. Copy the **POSLoader.ARM.CAB** file from the Host PC *\MICROS\RES\CAL\HHT* directory to the *\Temp* folder on the hand held. 5. Disconnect the HHT from ActiveSync. 6. Using the Start menu on the HHT, select *Programs* | *File Explorer.* 7. Navigate to the *Temp* folder, and run the P**OSLoader.ARM.CAB** file. This will install the POSLoader into the hand held's persistent memory. 8. After the CAB file extraction is complete, navigate to the *Windows* folder and select the **POSLoadInstaller**. 9. Exit the File Explorer and click on the Network Icon in the Task Tray. Select **WLAN** Profiles. 10) Select **New**, and enter all Wireless Network settings.	**N/A**

Module	Feature	CR ID
Hand Held Device Cont'd	11. Test the connection by highlighting the profile, and clicking **Connect**. Ensure that the status indicator in the Task Bar indicates that the connection has been established, then click **Close**. 12. From the Start Menu, launch Configure POS by navigating to *Start* | *Programs* | *MICROS Setup* | *Configure POS*. 13. Enter all of the appropriate POS Settings and exit the utility. 14. Reboot the handheld device and complete device setup.	**N/A**
Logging	**Security Log Does Not Display After Installing the Patch** After installing the RES 3.2 SP7 HF5 patch, the security log would fail to record activity such as autosequences, and applications opening. This issue has been corrected.	**N/A**

Module	Feature	CR ID
POS Operations	**A Menu Item Split Across Multiple Checks Will not Recombine Correctly** When a menu item was split across multiple checks and then recombined into a single check, the item would fail to return to its original state. This has been corrected.	**22843**
	Applying Multiple Discounts Configured as Limited Discounts to the Same Check May Cause the Discount Amounts to be Incorrect When using discounts setup as Limited Discounts, applying multiple discounts to the same check would cause the discount amount to be wrong for some of the discounts due to rounding errors. This issue has been corrected.	**22855**
	Discounts Decrease by the Amount of Times That the Authorization Code is Incorrectly Entered When attempting to apply a discount to a check that needs to be authorized by another employee, the total discount would decrease by a percentage when the authorization code was entered incorrectly. Now, users only receive one chance to properly enter the authorization code before having to re-apply the discount.	**22941**
	Guest Counts can be Inaccurate When Using the Filter Seat Function to Close out Individual Seats Previously, when the filter seat function was used to allow individuals at a table to pay their check separately, the guest count could be recorded inflated. This issue has been corrected.	**22192**

Module	Feature	CR ID
POS Operations Con't	**Menu Item Consolidation Cannot be Turned Off** Previously, if the **Menu Item Consolidation** option was turned off, and two identical menu items were rung in a combo meal, the items would still be consolidated. As a result, attempting to add or remove condiments would generate an error. This issue has been corrected.	**22873**
	Reprint of Closed Check Shows Wrong Date on Trailer When using the Reopen Closed Check or Reopen Review Order Check functions to reprint a check, the system would show the check closed time as either Jan 01 1970 or Dec 31 1969, depending on the regional offset. This problem has been corrected.	**22939**
	Taxable Amount for Menu Items with a 0% Tax Rate Will Not Display in Check Info or on Reports When a menu item on a guest check was rung as tax free, the tax free total would not display in the check information nor would it display on a tax report. This issue has been corrected.	**22341**
Reports	**Cancelled Check Posting to Checks Begun Total When the System is in DOM** When the system was running in Dynamic Order Mode (DOM), certain checks, when cancelled, were posting to the Checks Begun total, rather than posting to the Void and Credit totals. This has been corrected.	**22900**

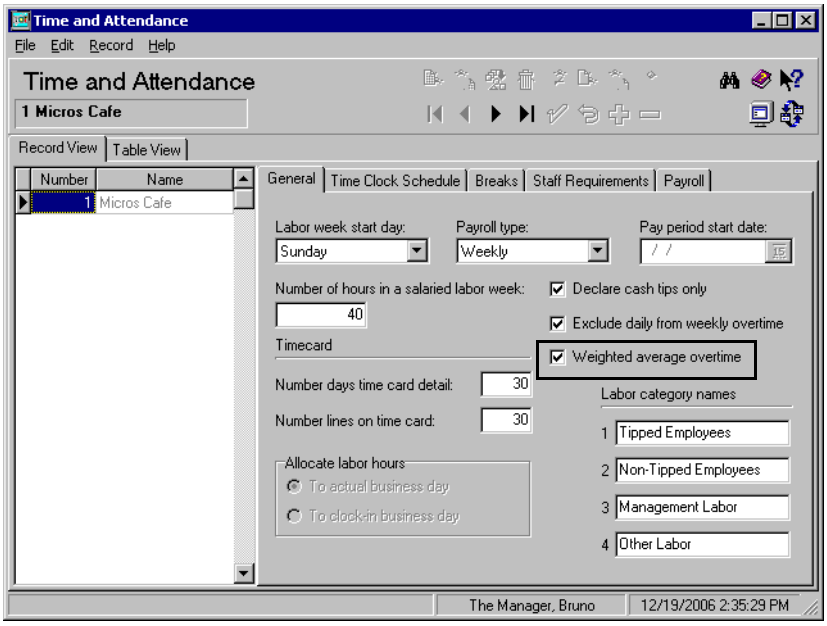
Guest Services Solution (GSS) New Features and Enhancements

Module	Feature
Operations	**Support for MICROS Login Form** Access to the GSS back office application has been modified to support the standard MICROS Login form.

Labor Management (LM) New Features/ Enhancements

Module	Feature
Operations	**Weighted Average Overtime** With this release, RES has added support for the Weighted Average Overtime feature. This feature calculates an hourly employee's overtime based on their weighted average rate of pay when working multiple jobs with different pay rates. In this situation the employee's overtime rate is a combination of the rates they are paid from each job. This feature is compatible with the California and New Jersey state labor laws. At this time other states may allow, but do not require Weighted Average Overtime to be computed. Weighted Average Overtime applies to the overtime accrued weekly when an employee exceeds the value listed in the **Hours Before Labor Week Overtime** field (*Labor Management* | *Rules/Laws* | *Overtime Definition* | *Overtime rule/level definition*). This feature does not effect the computation of other forms of overtime such as Daily, and Consecutive Day. When it is enabled, the Weighted Average Overtime calculation is performed automatically, although the calculation cannot begin until the end of the current labor week. If the Weighted Average Overtime feature is turned off, the updated calculation will not begin until the end of the current labor week. Once the calculation begins, the Weighted Average Overtime rate can be calculated at any time.

Module	Feature
Operations Con't	**Terminology** The following terms are relevant to the discussion of Weighted Average Overtime. Examples of all calculations can be found beginning on page 55. ◆ **Regular Rate** – If an employee is paid more than one rate by the same employer during the work week**,** the regular rate is the total sum of those wages without overtime. The regular rate should be calculated separately for each job. This number is calculated by multiplying the employee's rate of pay by the total hours worked during the week (including regular and overtime hours). ◆ **Tip Credit –** A law in several states allows employers to pay tipped employees a certain amount less than minimum wage because their hourly pay combined with their tips will be equal to or higher than the minimum wage rate. The tip credit is the difference between the minimum wage and the pay rate that the tipped employee is actually paid. For example, if the minimum wage is $5.25 and the state allows a $2.12 tip credit, then the tipped employee can be paid a minimum of $2.13 an hour. ◆ **Total Pay** – The sum that the employee has earned for the pay period including regular pay and overtime. ◆ **Wage Multiplier –** Used to determine how much additional pay someone should earn if they have worked overtime. The wage multiplier is multiplied by the employee's regular rate to determine their overtime pay. For example, some states mandate time and a half (a 1.5 wage multiplier) for all employees working overtime. ◆ **Weighted Average Rate** – If an employee is working more than one job at different hourly rates, the Weighted Average Rate indicates the mean pay that the employee will receive for work done that week.

Module	Feature
Operations Con't	**Implementation** To support this feature the **Weighted average overtime** option (*POS Configurator* | *Time and Attendance*) has been added. Enabling this option will turn on the Weighted Average Overtime feature and automatically perform the calculations described in the next section.  When Weighted Average Overtime is turned on or off, the user will receive a warning indicating that the feature will not go into or out of effect until the next pay period. This is because the Weighted Average Rate cannot be calculated for a portion of the pay period. 

Module	Feature
Operations Con't	**Reports** All reports that calculate overtime have been adjusted to account for weighted average overtime. No new reports have been created for this feature. Labor reports can be printed anytime during the pay period, however, the calculated overtime uses the current Weighted Average Rate, that may change throughout the labor week. If Weighted Average Overtime is enabled, a note will appear at the bottom of all overtime reports indicating that the totals are estimated and may not reflect the final total until the labor week is final.

103 - TORI Fong **292930**

Job # and Name	Clock In/Out	Date and Time	Hours	Status	Adjusted By
10 - Server	IN	Mon 11/27/2006 11:56am		On Time	
	OUT	6:58pm	7.03	Mgr Clock Out	
10 - Server	IN	Tue 11/28/2006 6:55am		On Time	
	OUT	3:00pm	8.07	On Time	
10 - Server	IN	Wed 11/29/2006 7:57am		On Time	
	OUT	3:36pm	7.65	Late	

Total Hours Worked This Week: 22.75 **Regular:** 22.75 **Overtime:** 0.00

Job Totals	Regular Hours	Overtime Hours
10 - Server	22.75	
Total Hours Worked This Pay Period:	**22.75**	**22.75**	**0.00**

103 - VICTOR Foning **132930**

Job # and Name	Clock In/Out	Date and Time	Hours	Status	Adjusted By
40 - Supervisor	IN	Sun 11/26/2006 10:00am		Late	
	OUT	12:28pm	2.47		VICTOR Foning
40 - Supervisor	IN	Sun 11/26/2006 12:28pm			
	OUT	12:31pm	0.06		

Note: If Weighted Average Overtime is enabled, totals are estimates until the labor week is final.

Module	Feature
Operations Con't	**Calculate Weighted Average Overtime** This section describes how Weighted Average Overtime is calculated. 1. When calculating Weighted Average Overtime the user must first calculate the employee's pay as if they did not accrue any overtime. The employee's Regular Pay must be calculated separately for each job worked at a different rate of pay. The **Regular Pay** is calculated as follows: Pay Rate x Number of Hours Worked --- Regular Pay 2. Now the user must calculate the overtime accrued separately. This overtime is calculated based on the weighted average rate that the employee was paid for the entire week, rather than by using the employee's rate for the job. Calculate the Weighted Average Rate by performing the following: 1. For each time card punch, multiply the rate by the number of hours worked. Pay Rate x Hours Accrued During Time Card Punch --- Total Earned During Time Punch Perform this calculation for every time card punch in the pay period.

Module	Feature
Operations Con't	2. Add all of the time card punches together. Pay for Time Card Punch for Job #1 on Wednesday + Pay for Time Card Punch for Job #2 on Wednesday + Pay for Time Card Punch for Job #1 on Thursday --- Sum of all Time Card Punches 3. Divide the sum by the total number of hours the employee worked for that week. The remaining total is the employee's **Weighted Average Rate**. Sum of all Time Card Punches ÷ Hours Worked for Week --- **Weighted Average Rate** 3. Now that you have the Weighted Average Rate, the **Overtime Pay** can be calculated: Weighted Average Rate x (Wage Multiplier - 1) x Number of Hours Worked --- **Overtime Pay for the Week** 4. The **Total Pay** is then calculated as follows: Regular Pay + Overtime Pay --- **Total Pay**

Module	Feature
Operations Con't	**Sample Calculation** The following is an example intended to illustrate how Weighted Average Overtime is calculated when tip credits are not used. This example is intended for illustrative purposes only. Josh works as both a bartender and a server at the Mike Rose Cafe. The Cafe pays the rate of $10.00 an hour for a bartender, and $8.00 and hour for a server. The Cafe is located in Bakersfield, California, where the wage multiplier for overtime is 1.50. The table below indicates the number of hours he worked last week. The table breaks out the hours he has worked for both jobs.

Days of Week	Hours as Bartender	Hours as Server	Total Hours by Day
Sunday	-	-	0
Monday	2	6	8
Tuesday	4	4	8
Wednesday	2	6	8
Thursday	-	8	8
Friday	2	8	10
Saturday	-	-	0
Total	10	32	42

Josh's Weighted Average Overtime is calculated as follows:

1. Determine Josh's Regular Pay for the week. In one week Josh has worked 10 hours as a Bartender at $10.00 an hour, and 32 hours as a Server at $8.00 an hour.

   10 x $10.00 = $100.00 **Regular Pay as a Bartender**

   32 x $8.00 = $256.00 **Regular Pay as a Server**

   $356.00 Total Regular Pay

<table>
<tr><th>Module</th><th>Feature</th></tr>
<tr><td>Operations Con't</td><td>
2. In a separate calculation determine Josh's Weighted Average Rate of Pay as follows.

1. Calculate the Total Pay for each time card punch. The calculation below is for Monday.

<u>Bartender</u>
$10.00
x 2.00

$20.00

<u>Server</u>
$8.00
x 6.00

$48.00

The table below lists the Total Pay for all time card punches:

<table>
<tr><th>Days of Week</th><th>Pay as Bartender</th><th>Pay as Server</th></tr>
<tr><td>Sunday</td><td>-</td><td>-</td></tr>
<tr><td>Monday</td><td>$20.00</td><td>$48.00</td></tr>
<tr><td>Tuesday</td><td>$40.00</td><td>$32.00</td></tr>
<tr><td>Wednesday</td><td>$20.00</td><td>$48.00</td></tr>
<tr><td>Thursday</td><td>-</td><td>$64.00</td></tr>
<tr><td>Friday</td><td>$20.00</td><td>$64.00</td></tr>
<tr><td>Saturday</td><td>-</td><td>-</td></tr>
<tr><td>Total</td><td>$100.00</td><td>$256.00</td></tr>
</table>
2. Calculate the sum of all Time Card Punches.

$100.00
+ $256.00

$356.00

3. Divide the sum by the total number of hours the employee worked for that week. The remaining total is the employee's Weighted Average Rate.

$356.00
÷ 42.00

$8.48 Weighted Average Rate
</td></tr>
</table>

Module	Feature
Operations Con't	4. Determine Josh's **Overtime Pay**. $8.48 — $4.24 x 0.5 (Wage Multiplier 1.5 - 1) — x 2.00 (Hours of Overtime) ------ — ------ $4.24 — **$8.48 Total Overtime Pay** 5. Determines Josh's **Total Pay** for the week. $356.00 + $8.48 ---------- **$364.48 Total Pay**

Module	Feature
Operations Con't	**Calculate Weighted Average Overtime With Tip Credit** This section describes how Weighted Average Overtime is calculated when the tip credit is in effect. 1. Calculate the employee's **Regular Pay**. Pay Rate x Number of Hours Worked ---------- Regular Pay 2. In a separate equation, calculate the **Weighted Average Rate.** When the tip credit is in effect, the pay rate for each job cannot be below minimum wage. This is because a sub-minimum wage total would allow more than the legal tip credit to be subtracted from the employee's hourly pay. Calculate the rate as follows. 1. For each job determine whether the minimum wage or the employee's pay rate is larger. 2. Using the larger of the two numbers, multiply the rate by the number of hours for each time card punch. Higher Pay Rate x Number of Hours Worked ---------- Pay for Time Card Punch

Module	Feature
Operations Con't	3. Add all totals for each time card punch. Pay for Time Card Punch for Job #1 on Wednesday + Pay for Time Card Punch for Job #2 on Wednesday + Pay for Time Card Punch for Job #1 on Thursday --- Sum of all Time Card Punches 4. Divide the sum by the total number of hours the employee worked for that week. Sum of all Time Card Punches ÷ Hours Worked for Week --- Weighted Average Rate 3. Now that you have the Weighted Average Rate, the **Overtime Pay** can now be calculated: Weighted Average Rate x (Wage Multiplier - 1) x Number of Hours Worked --- Overtime Pay for the Week 4. The **Total Pay** is then calculated as follows: Regular Pay + Overtime Pay --- Total Pay

Module	Feature
Operations Con't	**Sample Calculation with Tip Credit** The following is an example intended to illustrate how Weighted Average Overtime is calculated in a situation when tip credits is in effect. This example is intended for illustrative purposes only. Josh works as both a bartender and a server at the Mike Rose Cafe. The Cafe pays the rate of $10.00 an hour for a bartender, and $4.00 and hour for a server. The Cafe is located in Boston, Massachusetts where the Minimum Wage is $6.75 an hour. The Wage Multiplier for overtime is 1.5. The table below lists the number of hours Josh worked last week. The table breaks out the hours worked in both jobs.

Days of Week	Hours as Bartender	Hours as Server	Total Hours by Day
Sunday	-	-	0
Monday	2	6	8
Tuesday	4	4	8
Wednesday	2	6	8
Thursday	-	8	8
Friday	2	8	10
Saturday	-	-	0
Total	10	32	42

Josh's Weighted Average Overtime is calculated as follows:

1. Determine Josh's **Regular Pay** for each job worked.

10 x $10.00 = $100.00 **Regular Pay as a Bartender**
32 x $4.00 = $128.00 **Regular Pay as a Server**

$228.00 Total Regular Pay

<table>
<tr><th>Module</th><th>Feature</th></tr>
<tr><td>Operations Con't</td><td>
2. Determine Josh's Weighted Average Rate for each job.

1. Determine whether the minimum wage or the Josh's pay rate is larger.

Josh earns $10.00 an hour as a bartender, which is more than the Massachusetts minimum wage.

Josh earns $4.00 an hour as a server, which is less than the Massachusetts minimum wage. For this calculation, use the Massachusetts minimum wage rate of $6.75.

2. Multiply the rate by the number of hours for each time card punch. The calculation below shows Josh's hours on Monday.

<u>Bartender</u> $10.00 x 2.00 ------- $20.00

<u>Server</u> $6.75 x 6.00 ------- $40.50

3. Perform this calculation for every time card punch. The table below lists all of the totals for Josh's time card punches

<table>
<tr><th>Days of Week</th><th>Pay as Bartender</th><th>Pay as Server</th></tr>
<tr><td>Sunday</td><td>-</td><td>-</td></tr>
<tr><td>Monday</td><td>$20.00</td><td>$40.50</td></tr>
<tr><td>Tuesday</td><td>$40.00</td><td>$27.00</td></tr>
<tr><td>Wednesday</td><td>$20.00</td><td>$40.50</td></tr>
<tr><td>Thursday</td><td>-</td><td>$54.00</td></tr>
<tr><td>Friday</td><td>$20.00</td><td>$54.00</td></tr>
<tr><td>Saturday</td><td>-</td><td>-</td></tr>
<tr><td>Total</td><td>$100.00</td><td>$216.00</td></tr>
</table>
</td></tr>
</table>

Module	Feature
Operations Con't	4. Divide the sum by the total number of hours the employee worked for that week. $316.00 ÷ 42.00 --------- **$7.52 Weighted Average Rate** 3. Now that you have Josh's Weighted Average Rate, his **Overtime Pay** can be calculated: $7.52 $3.76 x 0.5 (Wage Multiplier 1.5 - 1) x 2.00 (Hours of Overtime) ------ ------ $3.76 **$7.52 Overtime Pay** 4. Josh's **Total Pay** is then calculated as follows: $228.00 + $7.52 --------- **$235.52 Total Pay**