



*Restaurant Enterprise Solution
(RES) Version 4.0
ReadMe First*

About This Document

ReadMe First is a comprehensive guide to the new features, enhancements, and revisions added since the Version 4.0 release of the MICROS Restaurant Enterprise Solution (RES) software.

For clarity, information is divided into self-contained chapters, reflecting the additions and modifications made to the following RES products:

- ◆ 3700 Point-of-Sale (POS) System
- ◆ Kitchen Display System (KDS)
- ◆ Guest Service Solutions (GSS)
- ◆ Cash Management (CM)
- ◆ Labor Management (LM)
- ◆ Product Management (PM)
- ◆ Financial Management (FM)
- ◆ RES Platform

Within each section, product information is organized as follows:

- ◆ What's New
- ◆ What's Enhanced
- ◆ What's Revised

Each section begins with an introduction and includes a table that summarizes the features and functionality incorporated in this version of the software. The table provides hypertext links to supplementary text and graphics about the selected topics.

For more information on these features, and step-by-step instructions for configuring them, refer to the product's Online Reference Manual, available from the MICROS website.

3700 POS

What's New

A new feature is defined as one that provides capabilities that were not available in previous versions of the application.

New Features Summarized

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

Module	Feature	Page
POS Operations	Themes (Skins)	4

New Features Detailed

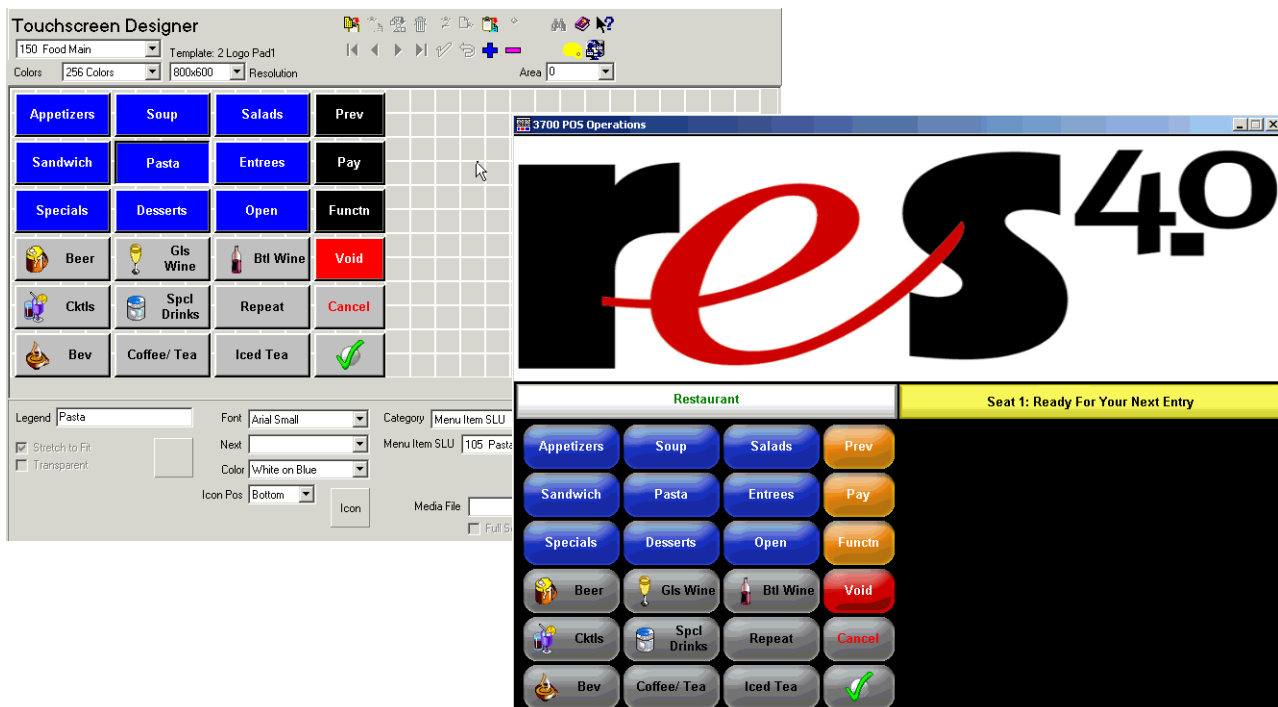
POS Operations

Themes (Skins)

The Theme feature allows users to change the look and feel of the workstation's user interface (UI) by replacing the underlying graphic design.

Themes (also referred to as Skins) are purely decorative in nature. They affect the color, shape, and imagery of the various touchscreen components, including buttons, backgrounds, information areas, prompts, and the check detail. *They DO NOT change the size of a component or its location in the layout of the screen.*

For this release, MICROS has added several themes (**Curved**, **HighTech**, and **Swirled**), which may be used as an alternative to the system default. A sample order screen from the **Curved** theme is shown below. For comparison, the original Touchscreen Designer form is also shown.



In the **Curved** theme example, the touch keys display with rounded edges and are shown against a black background. Note that the imagery is only apparent during operations, at the affected workstation. The buttons as configured in Touchscreen Designer have the traditional look and feel.

Note *Themes are only supported on the 3700 POS System. Theme selections will not affect the back office application interfaces or other RES utilities.*

Adding Themes

Themes are a collection of graphic-intensive files that, when rendered together, produces a desktop look-and-feel with shared imagery. As such, every design element associated with that theme (every button, icon, prompt, background image, scroll bar, etc.) must be created and then copied to their own folder in the **\MICROS\Res\Pos\Themes** directory. Also included is a configuration file (**ThemeInfo.cfg**), which includes all of the parameters that define a particular theme.

Because of the number of files involved, themes are stored on the server and are downloaded to the workstations with the database. Only one theme is stored on the workstation at a time. If a new theme is selected or the existing theme is updated, those files will be copied locally and the previous theme folder will be deleted.

As with other layout and design elements, users can always implement their own custom themes. For guidelines on creating and adding a theme, refer to the support document *RES 4.0 User Interface Theme Creation*, available from the MICROS website.

Note *Due to memory constraints, MICROS does not provide a Theme that can be used on a hand-held device. If assigned, an error message will display indicating a memory problem, when attempting to start a check.*

Enabling the Feature

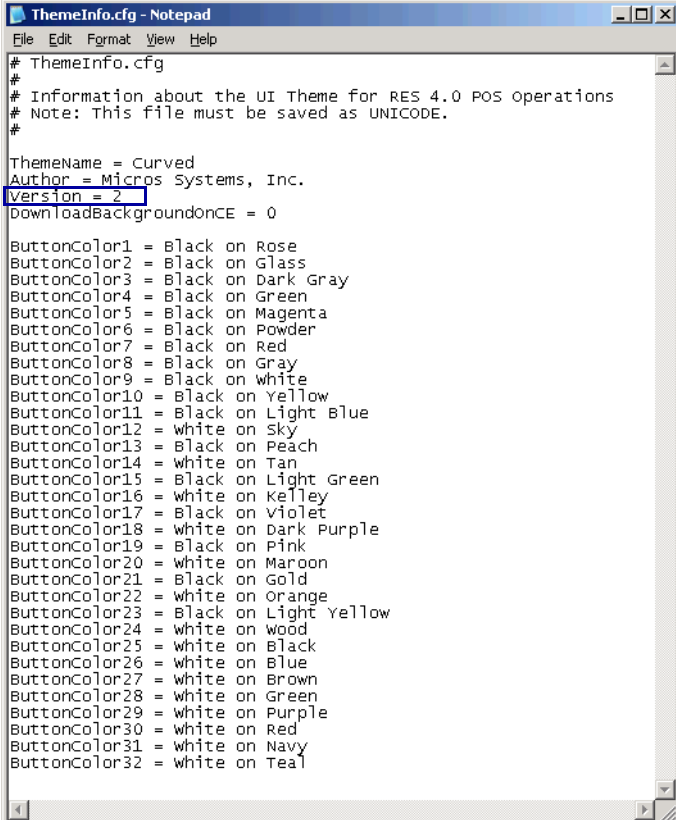
Themes are assigned at the workstation level; a different theme may be selected for each device.

To support this feature, a new option **Theme Name** (*Devices | User Workstations | Options | Display*) was added. The drop-down list contains all of the themes (except for the MICROS default) that are currently in the database. If no entry is selected (i.e., the field is left blank), the system will use the MICROS default.

Updating the Current Theme

The original release of a theme is always identified as Version 1 in the **ThemeInfo.cfg** file. This number is incremented each time the theme is updated on the server. However, installing a new version on the server does not ensure that it will be downloaded to the clients. To load the new settings, users must stop and restart POS Operations at the applicable workstation.

Indicates the
current version
of the theme →



```
# ThemeInfo.cfg
#
# Information about the UI Theme for RES 4.0 POS operations
# Note: This file must be saved as UNICODE.
#
ThemeName = Curved
Author = Micros Systems, Inc.
Version = 2
DownloadBackgroundonce = 0

ButtonColor1 = Black on Rose
ButtonColor2 = Black on Glass
ButtonColor3 = Black on Dark Gray
ButtonColor4 = Black on Green
ButtonColor5 = Black on Magenta
ButtonColor6 = Black on Powder
ButtonColor7 = Black on Red
ButtonColor8 = Black on Gray
ButtonColor9 = Black on White
ButtonColor10 = Black on Yellow
ButtonColor11 = Black on Light Blue
ButtonColor12 = white on Sky
ButtonColor13 = Black on Peach
ButtonColor14 = white on Tan
ButtonColor15 = Black on Light Green
ButtonColor16 = white on Kelley
ButtonColor17 = Black on Violet
ButtonColor18 = white on Dark Purple
ButtonColor19 = Black on Pink
ButtonColor20 = white on Maroon
ButtonColor21 = Black on Gold
ButtonColor22 = white on Orange
ButtonColor23 = Black on Light Yellow
ButtonColor24 = white on Wood
ButtonColor25 = white on Black
ButtonColor26 = white on Blue
ButtonColor27 = white on Brown
ButtonColor28 = white on Green
ButtonColor29 = white on Purple
ButtonColor30 = white on Red
ButtonColor31 = white on Navy
ButtonColor32 = white on Teal
```

What's Enhanced

An enhancement is defined as a change made to improve or extend the functionality of the current 3700 POS application. 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 extends the current process. This differs from a revision (i.e., a bug fix) which corrects a problem not caught in the previous release of the software.

Enhancements Summarized

The table below summarizes the enhancements included in this version.

Module	Feature	Page
Credit Cards	Credit Card Drivers	8
Hand-Held Terminals (HHT)	Symbol MC 50 (CAL Enabled)	8
Kiosk Support	Touchscreen Enhancements	14
	Media Files Support	16
	POS Prompting	33
Manager Procedures	Display Detailed Error Messages	34
POS Configurator	Font Changes	41
	Multiple Touch Key Areas	35
POS Operations	Check Inactivity Timeout	39
	Database Update Progress Bar	40
	Review Order File Format Change	42
	Touchscreen Resolution Enhancements	43
	Updated POS Icon	43

Enhancements Detailed

Credit Cards

Credit Card Drivers

Credit card drivers are no longer included in the RES 4.0 installation. Users will need to install the site's credit card drivers after RES 4.0 setup. Once the credit cards are added, they will not be affected by future RES installations.

Hand-Held Terminals

Symbol MC50 (CAL Enabled)

Use of the Symbol MC50 hand-held device has been enhanced to support implementation of the Client Application Loader (CAL) in a RES 4.0 system.

The Symbol MC50 is a light-weight mobile computer in a hand-held PDA-like form. The device utilizes Microsoft® Pocket PC, a Windows®-based embedded software platform that provides a mobile interface with the look and feel of a desktop computer. The Windows CE environment allows users to run multiple applications at once and is designed to be used on corporate networks.

Configuring the Device

Merchants can purchase their Symbol MC50 hand-held devices either from MICROS or from an outside vendor. Units purchased from MICROS are preconfigured for use in a RES environment. Units purchased from an outside vendor will require more extensive setup.

This section provides instructions for configuring the Symbol MC50 device. Users who have purchased units from outside vendors should execute all of the steps described below. Units purchased from MICROS directly can begin with Step 7.

Definitions

For clarity, the following definitions are provided for terms used during setup:

- ◆ **Cold Boot** —

Simultaneously press the silver **On** button (top right), the **Scan/Reset** button (top silver button on right side of device), and the **Reboot** button (recessed black button on back of device, beneath the battery lock button). This is used to power up the device.



- ◆ **Warm Boot** — Press the

black button beneath the battery release (bottom of unit) with the stylus. This is used to restart the system.

- ◆ **Three-Finger Press** — One at a time, press the green **Phone** key, the **Calendar** key, and then the red **Phone** key. This key sequence provides access to the Windows Start menu *before* CAL has been initiated. This option is used to change the network settings.

Procedures

The Symbol MC50 uses CAL Client Version 3.1.2.49 software or higher. Units purchased from MICROS will have this installed already. For units purchased from a non-MICROS vendor, users will have to install the Client software prior to setup. The CAL software can be downloaded from the Hardware page on the MICROS website.

With CAL installed, follow these steps to configure a new Symbol MC50 to use RES:

1. Set the device for the first sync:
 - ◆ From the Windows Start menu, select *ActiveSync | Tools | Options | Options*.

- ◆ Check **Enable PC sync using this connection**.
 - ◆ Check **Maintain connection**.
 - ◆ Press **OK** twice to exit the form.
 - ◆ Press the **x** button (upper right corner) to close.
2. Download and install ActiveSync on your server PC
- ◆ Go to the Microsoft website (www.microsoft.com) | *Product Resources* page and select *Downloads*.
 - ◆ From the drop-down box, select *ActiveSync*.
 - ◆ Select the most up-to-date version of ActiveSync. Download to your Server's top folder.
 - ◆ Double-click **MSASYNC.EXE** to begin installation. Follow the on-screen instructions provided.
3. Establish a partnership.
- ◆ Set the Symbol MC50 into the cradle connected to the Server.
 - ◆ From the Server's Start Menu, select *Programs* | *Microsoft ActiveSync*. This should bring up a new window and automatically detect the hand-held device.
 - ◆ Go to the *Set Up a Partnership* screen.
 - ◆ Select **Guest Partnership** and press **Next**.
4. Copy CAL to the Symbol MC50.
- ◆ Go to the MICROS website (www.micros.com) | *Hardware Product* page. Download a copy of the **McrsCAL.CAB** file to a *Temp* folder on the Server.
- Copy this file from the *Temp* folder to the *Mobile Device\My Pocket PC\Windows\Start Menu* folder. If prompted about converting files copied to a mobile device, click **OK**.

- ◆ Exit ActiveSync by removing the device from the cradle.
 - ◆ On the HHT, select *Start | McrsCAL* to install the files. (Once the files are installed, this option will be removed from the *Start* menu.)
5. (Optional) Set up the optional Magnetic Stripe Reader.
- ◆ Go to the MICROS website | *Hardware Product* page and download a copy of the **MSRDriver.ARM.CAB** file to a *Temp* folder on the Server.
 - ◆ Establish/reestablish an ActiveSync connection as described in Step 3.
 - ◆ Copy this file from the *Temp* folder to the *Mobile Device\My Pocket PC\Windows\Start Menu* folder.
 - ◆ Exit ActiveSync by removing the device from the cradle.
 - ◆ On the HHT, click *Start | MSRDriver.ARM.CAB* to install the files. (Once the files are installed, this option will be removed from the *Start* menu.)
- NOTE: If the *MSRDriver.ARM.CAB* option is not present on the *Start* menu, it may mean that the user has exceeded the maximum number of files that can be displayed (i.e., it is not an installation failure). Before reinstalling, select *Start | Programs* to manually locate the file.
6. Perform a cold boot of the Symbol MC50.
7. Press the silver circle in the upper-right corner to power up the unit. Tap the screen to begin setup.
8. Using the stylus, follow the system prompts to calibrate the touchscreen and enter the time zone settings.
9. Tap the screen to begin using the device. The *MICROS CAL StartUp* screen will display. Click **OK** to continue.

10. Configure the network settings. This only needs to be done the first-time the Symbol MC50 is started. The settings will persist the next time the device is booted up (cold or warm):
 - ◆ Use the three-fingered press to access the Windows *Start* bar. Select **Today**.
 - ◆ Click the Network icon on the bottom, right-hand side of the screen to open the network utility.
 - ◆ Configure the network, as required.
 - ◆ Perform a warm reboot of the system.
11. Once the reboot is complete, the *MICROS CAL Startup* screen will redisplay. Press **OK** to continue.
12. At the new screen, a message is displayed asking if the user wants to configure CAL. Press **OK** to continue.
 - ◆ Wait while CAL searches for servers. This will only take a few seconds. A list of network servers is displayed.

Note: CAL can display up to 50 servers at a time. If the preferred server is not in the initial list, press the **Search Again** button to show the next set of records.
 - ◆ Highlight the preferred server and click **Next**. A screen displays indicating the Minimum RF Signal Strength. By default, this is set to 30. Unless required for diagnostics, this setting should not be changed.
 - ◆ Press **OK** to continue.
 - ◆ From the **Select Product to Install on Workstation** drop-down list, select *PPCRES*.
 - ◆ The *Workstation Identity* screen displays. (Click **Available workstation list** to view a list of HHT devices configured for this server.)
 - ◆ Select the workstation that you want this device to be.

- ◆ The **Automatic DHCP Configuration** option is already enabled. If the network is configured for static IP Address, clear this box. Otherwise, do not change anything.
 - ◆ Click the **Save** button. The Symbol MC50 will begin to download the files from the selected server, rebooting several times throughout the process.
13. When setup is complete, the *MICROS CAL StartUp* screen will be redisplayed. Once again, a message will display, asking if the user wants to configure CAL. To point the device to a different server, press **OK** and repeat from step 8. Otherwise, do not press anything.
 14. After a 5-second pause, the device will automatically start POS Operations.

Once the Symbol MC50 CAL client is operational, it periodically reconnects back to the server to check for new and updated software. This information is stored on the server in **\Micros\res\CAL\PPC\Files**. Users can add files to the download by copying them to this directory. (Note: To work, the **FileCopyEnabled.dat** must be present in **\Micros\res\CAL\PPC**.)

Kiosk Support

The term “kiosk” is a generic reference to a publicly accessible, electronic device running a self-service computer application. Current examples of the kiosk concept include Automated Teller Machines (ATM), airline flight check-ins, and department store gift registries.

In a restaurant environment, kiosks represent an inexpensive and effective way to advertise products, automate customer services, and provide training for employees. Using custom graphics, videos, and sound, kiosks can be used as self-service POS terminals, guiding customers step-by-step through the order-entry process. Statistics have shown that a thoughtfully designed kiosk can improve customer satisfaction by reducing the amount of time spent in traditional cashier-driven lines. Fewer cashiers also means a reduction in labor costs, from hiring to training to scheduling and managerial oversight.

RES offers several ways to enhance the user interface and provide a more interesting and interactive experience.

Touchscreen Enhancements

Several touchscreens enhancements were introduced to support the use of customer-driven workstations (or kiosks). These include the addition of five new touchscreen templates in POS Configurator:

- ◆ 801 Kiosk1
- ◆ 802 Kiosk2
- ◆ 803 Kiosk3
- ◆ 804 Kiosk Sign In
- ◆ 805 Full Screen

The *Kiosk1*, *Kiosk2*, and *Kiosk3* templates are a variation of the standard *Detail* templates, with two significant additions: 1) the use of animated images; and 2) the ability to customize status messages.

The *Kiosk Sign In* and *Full Screen* templates contain only a touchscreen area. The difference between the two is in the key dimensions. The Full Screen template allows the user to place keys more precisely on the screen when using a background image.

To support the higher resolution of the optional 15-inch touchscreen for the Eclipse and 2010 workstations, all of the workstation touchscreen templates have been modified to include support for 1024 x 768 screen resolution.

Animated Images

The new Kiosk templates include a hard-coded graphic area that can support a series of rotating bitmap images (also referred to as the animation image). In previous releases, bitmap areas were limited to a single static image (e.g., the Corporate Logo that is shown on the Sign-In Screen).

For more on creating and adding animated images on a touchscreen, refer to the discussion beginning on page 23.

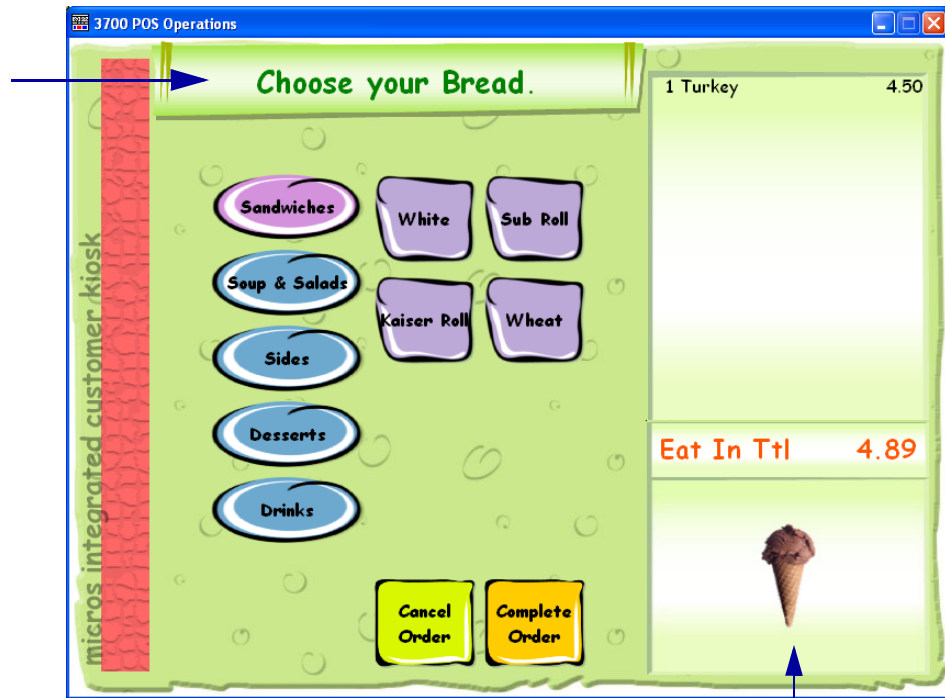
Custom Status Prompts

The Kiosk templates also allow programmers to display a custom text message in the touchscreen's new fixed prompt area. These custom prompts were designed to simplify the information presented to customer/operators, and to help them navigate screen flow in a kiosk-style environment.

To support this function, a new **Fixed Prompt Text** option (*Devices | Touchscreens | Touchscreens*) was added in POS Configurator. During operations, text entered in this field will be displayed in the designated prompt area of each touchscreen.

Typically, when designing a user-defined template, the definition will include either a PromptArea or a FixedPromptArea.

Fixed Prompt Text displays user-defined instructions.



Animation Area
hard-coded in
the Kiosk templates.

Note *Custom prompts will only work if the touchscreen is linked to one of the new kiosk-style templates or to a user-defined template that includes a FixedPromptArea.*

Media Files Support

The use of media files has been added to allow support for interactive, kiosk-style terminals. This section describes the types of media files available to the user, discusses the differences between them, and offers suggestions for how each type can be implemented in a kiosk-style environment.

Note *Although described in the context of a kiosk, most of these options can be applied to any POS workstation.*

Caveats

Media files can be run on both Win32 and CE devices.

If used, a media file must be stored locally on every workstation where it is to be run. Given the size of most image files, hard-drive space can fill quickly — particularly on CE-based workstations such as the WS4 and hand-held units. Also, since the system must paint the screen everytime a new image is displayed, an abundance of graphics can have an impact on system performance. Sites will need to review their devices' storage capabilities before deciding whether or not to use these options.

Finally, media support is dependent on the device's operating system. If the operating system configuration does not support a particular media type, RES cannot override that limitation.

Media Activation Types

Media support can be grouped into three types based on how they are activated:

- ◆ **Touchscreen Media** — Plays at the start of a new touchscreen. The media event begins when the screen appears and continues until it completes or the user touches the display area again.
- ◆ **Idle Media** — Plays when the touchscreen is left idle for a user-specified period of time. The designated media file will repeat at specified intervals until the screen is touched, at which point the station displays the last touchscreen used before reverting to the idle media event.
- ◆ **Touchscreen Key Media** — Plays when a specific touchscreen key is pressed. The media event only plays once per keypress.

Using Bitmap Images

Bitmaps are the traditional media used to improve the look and feel of the user interface. Typically, this was done by adding a logo to the sign-in screen or including an icon on a button. With the introduction of the kiosk concept, the use of bitmaps was enhanced to include the following layout options:

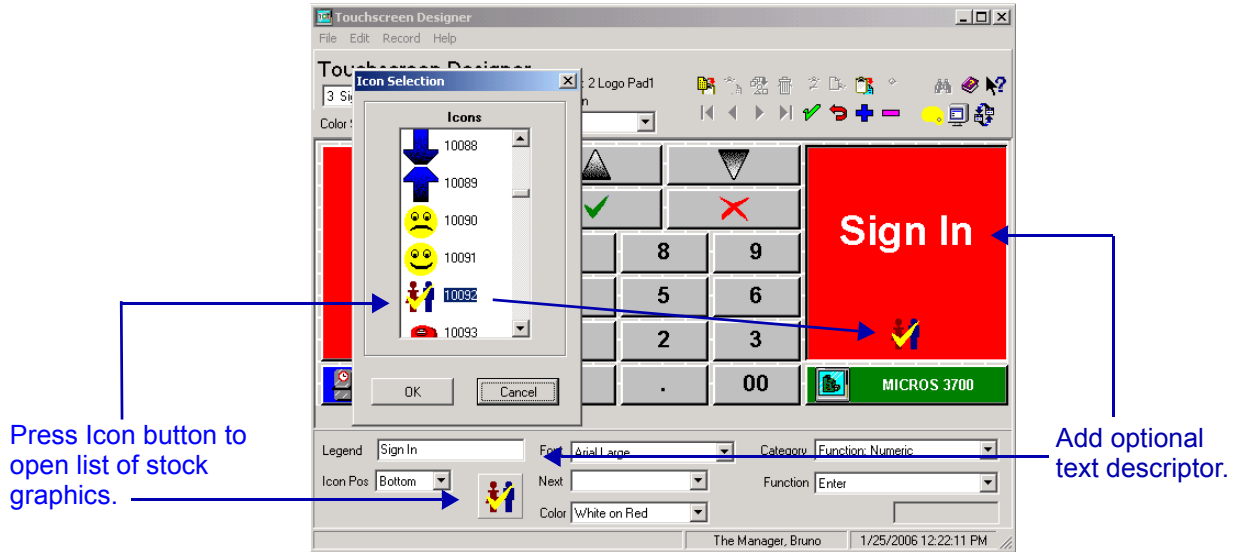
- ◆ Touch Key Bitmap Graphics (updates an existing capability)
- ◆ Background Images
- ◆ Animated Display
- ◆ Watermarks

The implementation of each is described below.

◆ **Touch Key Bitmap Graphics**

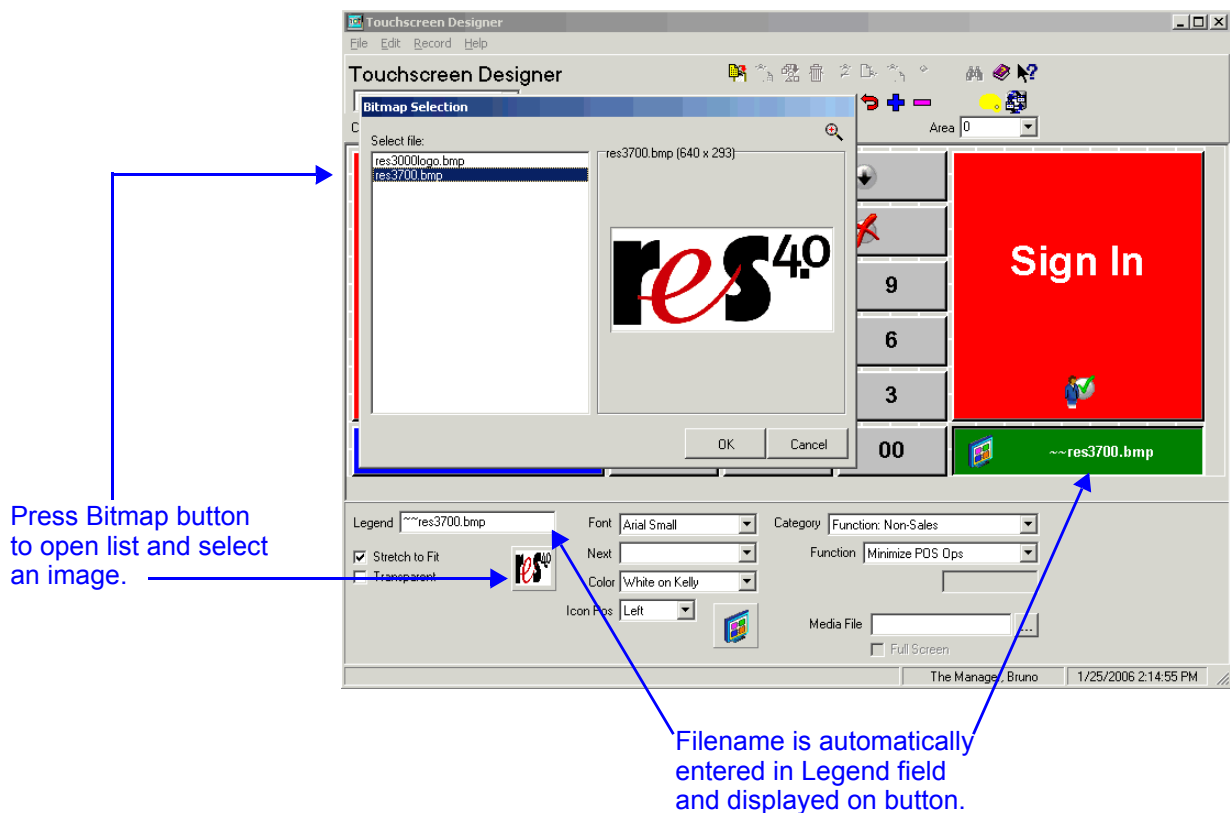
In previous releases, images were used primarily as icons, which were added to touch keys to provide a more graphical user interface. A set of stock images (e.g., arrows, tables settings, food, beverage, etc.) was available in *Touchscreen Designer* for this purpose. Users could also create their own icons via the **Customicon.dll**.

During configuration, users could press the **Icon** button to open the list and select an image to be displayed on the key. The **Icon Pos** field determined where the image would be located (top, bottom, left, right, center). Depending on the size of the button, an optional descriptor or **Legend** could be added.



Users could also link a bitmap image to a button, provided the image was copied into the appropriate folders in the \Micros directory. To insert a custom image, the filename had to be entered in the **Legend** field, preceded by two tildes (e.g., **~~sample.bmp**). Since the **Legend** field was used to identify the image, a separate text identifier was not allowed. To add text to the image, users had to incorporate the label within the graphic itself.

In this release, the options for adding a touch key bitmap graphic have been enhanced and simplified. Now, in addition to typing the filename into the **Legend** field, users can press the new **Bitmap Selection** button to display a list of custom images. Once the selection is made, the filename (with double tildes) is inserted in the **Legend** field and displayed on the button.



Note Adding a separate **Bitmap Selection** field means that users could assign both types of graphics (Bitmap and **Icon**) to the same touch key. The key space can only support one of them.

In the event that both are selected, the Bitmap image has priority and will be drawn instead of the Icon.

Once the bitmap graphic is selected, two options determine how it will be displayed on the touch key. The first is the **Stretch to Fit** option. When checked, the system resizes the graphic to fit the height and width of the touch key. This is the default behavior.

If the **Stretch to Fit** check box is cleared, the system will display as much of the original image as possible. Images that are smaller than the key space will be centered in the middle of that area, while those that are too large will be cropped along their right-hand and bottom edges.

The second attribute is a **Transparency** option. When checked, this option filters out the background color of the bitmap and allows the key to assume the shape of the remaining image/text.



Transparency Off Transparency On

Transparency colors are determined automatically by the system and are based on the first pixel in the upper left-hand corner of the image. In the preceding sample, the first pixel is black. When the transparency option was activated, all of the black pixels were removed, leaving the *Coca-Cola* icon to display in place of the standard touch key.

Note that transparency is NOT based on the dominant background color. If the preceding bitmap had included a blue border, the transparency attribute would have produced a much different result. In that case, the frame would drop out, but the black background would be unchanged.



Transparency Off



Transparency On

- ◆ **Background Images**

Besides touch keys, bitmaps can now be added to touchscreens as static background images. These act as a backdrop for the placement of user-defined objects on the POS screen.

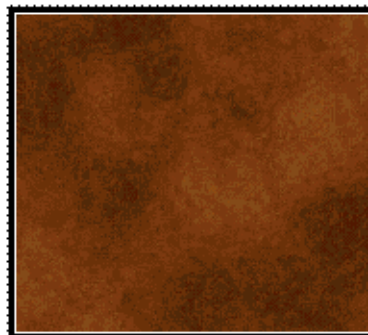
Background bitmaps can be as simple as a change of color (the default is grey) or they can include a more complicated design. For example, when using the *Restaurant View* feature, a programmer could create a bitmap of the restaurant's floor plan and use it as the basis for designing the *Begin Table* touchscreen. Once the background image is in place, the tables, function keys, and other design elements can be added. The result is a more realistic and detailed screen for the POS user.

Limitations

When using background images, keep in mind that the visible portions will only be seen in the open space around the user-defined areas. This limits the number of touchscreens that can support a background graphic as well as the size and complexity of the design.

The following samples illustrate how the selection of a background image affects the presentation of the same set of buttons and detail areas. In this case, the patterned background is visually confusing and clearly detracts from the usability of the screen.

Blank Background Image



Patterned Background Image



In designing a background image, the dimensions must be accurately rendered to fit the touchscreen area. Unlike touch keys, background bitmaps will not stretch to fit the screen, since doing so would distort their resolution.

File size can also be a limiting factor. A color change uses very little space, but the more complicated bitmaps can require a significant amount of memory. This may make them unsuitable for low-storage WinCE devices such as hand-helds or the WS4.

Background images are added at the touchscreen level. If defined, the bitmap will display every time the touchscreen is drawn. Since the system has to paint the screen with each change, using background images can slow response time considerably.

Note *To upgrade the look-and-feel of multiple screens without overloading the system, users should consider creating a custom Theme. For more on this topic, see the feature description beginning on page 4.*

Please note, however, if a background image is defined at both the Touchscreen level and as part of a Theme, the Touchscreen background image will take precedence.

Configuration

To support this function, a new **Background Image** option was added to the *Touchscreens* form (*Devices | Touchscreens*) in POS Configurator. To insert an image, enter the filename (including extension) in this field (e.g., background.bmp).

◆ **Animated Display**

Until now, all of the media options described in this section have involved static displays of a single image. With this release, users can animate the bitmap area by rotating a series of images while the screen is in use. Each image would display briefly, then be replaced by the next one in the set.

This feature is particularly useful in a kiosk environment, where customers are interacting with the workstation. For example, while the customer is debating selections on an order screen, pictures of different sandwiches could be cycling through on the bottom of the display. In this case, the animation becomes a form of subliminal advertisement.

Images

To create an animation file, users must first gather and organize the images that will be displayed. There is no limit to the number of images that can be included. However, each image must have the same basic filename, followed by its sequence number in the rotation.

For example, if there are three images in the Test animation, they should be named:

Test1.bmp

Test2.bmp

Test3.bmp

Bitmaps do not have to be the same size or conform to the dimensions of the display area. During operations, the system will scale each image to fit the defined area.

Transparency is not available with this function.

Configuration

To activate the animation file, two new options were added in POS Configurator (*Devices | Touchscreens | Touchscreens*).

The first is the **Animation Image**, which identifies the series of bitmaps to be displayed. This is done by entering the base filename (minus sequence number) and file extension. Using the sample described above (**Test1.bmp, Test2.bmp, Test3.bmp**), the filename would be entered as **Test.bmp**.

The second option is the **Animation Speed** field, which allows users to specify how long (in seconds) each bitmap will display before moving on to the next image.

Also, in order for an animation file to display, the touchscreen must be linked to a template that has a hard-coded bitmap area set aside for this purpose. In this release, four standard templates have been added that include an animation area:

- ◆ 112 Table Object w/Animation
- ◆ 801 Kiosk1
- ◆ 802 Kiosk2
- ◆ 803 Kiosk3

A discussion of these templates is available, beginning on page 14.

If none of these are suitable, users have the option of creating their own template, or customizing an existing template to include animations. This is done by editing the **OpsDisplayUser.cfg** file.

Note *For information on customizing the POS display, refer to the support document: Restaurant Enterprise Solution, Editing the OPS Display User Configuration File, MD0003-064, Revision A, April 2006, available from the MICROS website.*

Because it affects core programming, changes to the POS configuration file should be handled by a qualified administrator only.

◆ **Watermarks**

Traditionally, a watermark is a translucent design — often a logo — that prints unobtrusively as a backdrop for text displays. In RES, watermarks can be programmed to draw in the check detail area of the touchscreen. Watermarks are drawn by the system from a user-specified bitmap image. If used, the image will not extend into the check summary area.

Sample Watermark
Displays in
Check Detail
Area Only



Watermarks support transparency. The first pixel (upper left-hand corner) of the image is always used as the transparent color to drop-out of the image.

Watermarks are not scaled. When selecting an image, the size of the original must fit within the designated detail area. In other words, if the available space is 200 x 400 pixels (width by height), and the bitmap is 300 x 500, a watermark will not be generated. Conversely, if the image is only 100 x 200 pixels, it will be drawn in the center of the Check Detail area.

Configuration

The option to add a **Watermark Image** is defined at the revenue center level (*Revenue Center | RVC Transactions | General*). Each revenue center may have its own watermark. This allows users to instantly identify the revenue center that the workstation (or hand-held device) is operating in. To complete the field, enter the filename with extension (e.g., **watermark.bmp**).

Using Video/Sound

In addition to traditional graphics, the introduction of a kiosk-style workstation increased the need for alternate forms of media, such as sound and video clips. The following file types are supported by RES:

- ◆ midi
- ◆ avi
- ◆ mp3
- ◆ wav
- ◆ wmv

Exceptions to this list are determined by the device's operating system.

Implementation

Like bitmaps, sound and video files can be linked to either a touchscreen or to one of the keys on the screen.

- ◆ **Touchscreen Media**

Media files that are linked to a touchscreen are designed to play while that touchscreen is displayed. The trigger is controlled by the system, and can occur immediately, with the change of screen, or may occur after the screen has been displayed for a while.

Active Media

If the file is programmed to play immediately, it is considered to be *active* media. In a kiosk environment, active media files can be used to set up a training system for new employees, or walk a customer through the ordering process. As customers advance through the order, each new screen can trigger a different audio/video clip with simple directions for the next entry.

Inactive Media

With *inactive* media, audio/video files are programmed to play *after* the touchscreen has been idle for a specified period of time. A screen-saver is an example of a simple, idle media file. Another example would be an audio prompt. Once a transaction has been started, the system could be programmed to play a sound clip (e.g., “Select Next Item, Please”) when the amount of time between entries exceeds a programmed maximum.

Configuration

Media files are linked to the touchscreen. To support this functionality, the following options were added to the *Devices | Touchscreens | Touchscreens* form in POS Configurator:

- ◆ **Media File** — For *active* media. This option allows users to specify the filename and extension (e.g., **StartOrder.wmv**) of the video or sound file to be played when the touchscreen is accessed.
- ◆ **Idle Media File** — For *inactive* media. This option specifies the filename and extension (e.g., **PromptOrder.wav**) to be played on an inactive screen.
- ◆ **Idle Media Time** — Specifies how long the screen must be inactive before the **Idle Media File** is played. This entry is also used to determine repeatability (i.e., how long the system will wait before playing the file again).

Time values are in seconds. For example, if the time is set to 30, the **Idle Media File** will be triggered after the touchscreen has been idle for 30 seconds and will repeat at 30 second intervals until the screen changes.

Touchscreens can have both active and inactive media files linked to the same template. Using the ordering process as an example, the system could play an instructional video when the screen is first displayed. If no action is taken by the user in the next 30 seconds, the system could prompt for the next entry and repeat the prompt until the user either makes a selection, or cancels the transaction.

- ◆ **Touch Key Media**

Media files that are linked to a touch key are designed to play when the key is pressed. With media keys, the user controls when the file is started and stopped. The play sequence can be interrupted by touching the screen while the file is still playing.

Configuration

Media key support is configured like any other touch key function — by linking it to a defined key in *Devices | Touchscreen Designer*. A new **Media File** option allows the user to specify which file will be played when the touch key is pressed during operations. Users can enter the filename manually, or use the search button ([...]) to open a file dialog box and browse to a viable entry.

Unlike other media files, users can determine how much of the screen will be used when the video displays. When enabled, the **Full Screen** option directs the system to play the file across the entire touchscreen. If cleared, the system will confine the display to the dimensions of the key.

Media File Location

Media files must be stored locally on every device where they are expected to run. In the past, this would have required sites to manually copy the files to each workstation. With this release, RES uses Client Application Loader (CAL) technology to periodically scan, locate, and download the most recent files from the Server directory to corresponding folders at each client location.

To add or update a media file, the bitmap or video/sound should be placed in the appropriate folder(s) on the Server. A separate copy is required for each client type. (Note: If a folder does not exist, it will have to be manually added for each Client.)

◆ **BPAD**

\MICROS\Res\CAL\BPAD\Flashdisk\Micros\Bitmaps
\MICROS\Res\CAL\BPAD\Flashdisk\Micros\Media
\MICROS\Res\CAL\BPAD\Flashdisk\Micros\TrainingMedia

◆ **HHT**

\MICROS\Res\CAL\HHT\Micros\Bitmaps
\MICROS\Res\CAL\HHT\Micros\Media
\MICROS\Res\CAL\HHT\Micros\TrainingMedia

◆ **WS4**

\MICROS\Res\CAL\WS4\Files\CF\Micros\Bitmaps
\MICROS\Res\CAL\WS4\Files\CF\Micros\Media
\MICROS\Res\CAL\WS4\Files\CF\Micros\TrainingMedia

◆ **Win32 Client**

\MICROS\Res\CAL\Win32\Files\Micros\Res\Pos\Bitmaps
\MICROS\Res\CAL\Win32\Files\Micros\Res\Pos\Media
\MICROS\Res\CAL\Win32\Files\Micros\Res\Pos\
TrainingMedia

◆ **Server** (if also running POS Operations)

\MICROS\Res\Pos\Bitmaps
\MICROS\Res\Pos\Media
\MICROS\Res\Pos\TrainingMedia

For employees who are designated as **In Training** (*POS Configurator* | *Employees* | *Employees* | *POS*), the audio and video files will be played from the TrainingMedia folder.

New Options

To summarize, the following options were added to POS Configurator to support the enhanced media:

- ◆ *Devices | Touchscreens | Touchscreens*
 - ◆ **Animation Image** — Identifies a group of images to be shown as a set of rotating images on the selected touchscreen. To be included in the animation set, all images in the series must have the same name followed by an incremented sequence number before the file extension (e.g., Test1.bmp, Test2.bmp, Test3.bmp, etc.).
 - ◆ **Animation Speed** — Specifies how long the system will wait (in seconds) before displaying the next image in an animation sequence. After reaching the last file in the sequence, the system will return to the first and continue to rotate through the images for as long as the screen is active.
 - ◆ **Media File** — Specifies the name of a media file to be played whenever the selected touchscreen is accessed. Supports midi, avi, mp3, and wav files, depending on the limitations of the workstation's operating system.
 - ◆ **Background Image** — Specifies a bitmap image to be displayed in the background of the selected touchscreen. If left blank, or if the specified file is not found, the system reverts to the default background color (grey).

When adding an image, it is important to be precise about the dimensions. Background images are not scalable -- that is, they will not expand to fill the display area. Doing so would distort the resolution and interfere with the touchscreen layouts.

- ◆ **Idle Media File** — Identifies the default media file to be played continuously as long as the workstation is inactive. Once a customer touches the screen, the file stops playing and the system's sign-in or splash screen is displayed. If the touchscreen is idle for a certain amount of time, the system will begin to play this file again.

- ◆ **Idle Media Time** — Indicates the amount of time (in seconds) that the touchscreen must be inactive before the workstation begins to play the idle media file. Once it has finished, this value represents the amount of time the system will pause before replaying the media file.
- ◆ *Devices | Touchscreen Designer*
 - ◆ **(Bitmap Selection)** — Specifies the bitmap image to be displayed in this defined touch key area.
 - ◆ **Stretch to Fit** — When checked, resizes the bitmap image to fit the width and height of the touch key. This is the default behavior.
 - ◆ **Transparent** — Displays the selected bitmap with a transparent background. When selected, the system automatically uses the color of the first pixel in the upper left-hand corner of the image as the transparency color.

The transparency option is only applicable when a bitmap is designated for a touch key button.
 - ◆ **Media File** — This is the media key support option. Specifies the media file to be played when this touch key is pressed.
 - ◆ **Full Screen** — When checked, uses the full screen to display the media file when the touch key is pressed. If cleared, runs within the designated key space only.
- ◆ *Revenue Center | RVC Transactions | General*
 - ◆ **Watermark Image** — Displays the selected bitmap as a transparent background image in the check detail. Uses the color of the first pixel (upper left-hand corner) as the transparent color. Watermark images are not scaled to fit the area. If the size of the image exceeds the detail area, it will not display.

POS Prompting

In the course of normal operations, users are presented with system prompts based on options selected in POS Configurator. Handling these choices presumes a level of knowledge not always applicable in a kiosk-style environment, where the device is typically customer-driven.

To avoid confusion, a new **Is Kiosk** option (*Devices | User Workstations | Kiosk Support*) was added to differentiate between workstations that are used as regular POS devices and those that function as kiosk-style devices. When checked, the system will handle system prompts and error messages as described below.

System Prompts

During operations, the system will either bypass the prompt associated with the following selections or simply disable the function:

- ◆ Do not confirm begin check (*Revenue Center | RVC Transactions*)
- ◆ Don't confirm uto-combo recognition (*Sales | Combo Meals | Revenue Center Options*)
- ◆ Beverage Control options (*Revenue Center | RVC Transactions | General*)
- ◆ CA Status options (*Revenue Center | RVC Credit Cards | General*)
- ◆ Supervised printing (sets all printing to unsupervised)

Error Messages

In the event of a system error, kiosk customers will not be equipped to correct the problem themselves. In this case, normal error prompts will be replaced with a generic dialog box, directing the customer to "Seek Assistance" from a store employee or manager.

The message box will also include a **Detail** button. When pressed, this will display the relevant error message to assist the manager in correcting the problem.

Manager Procedures

Display Detailed Error Messages

When an error occurs in Manager Procedures, the system displays the generic message “A system error has occurred.” and a **Show Detail** button that can be pressed for more information. By default, this detail screen is always blank.

The amount of information provided in the detail box is determined by an error mode configuration setting. To change this setting:

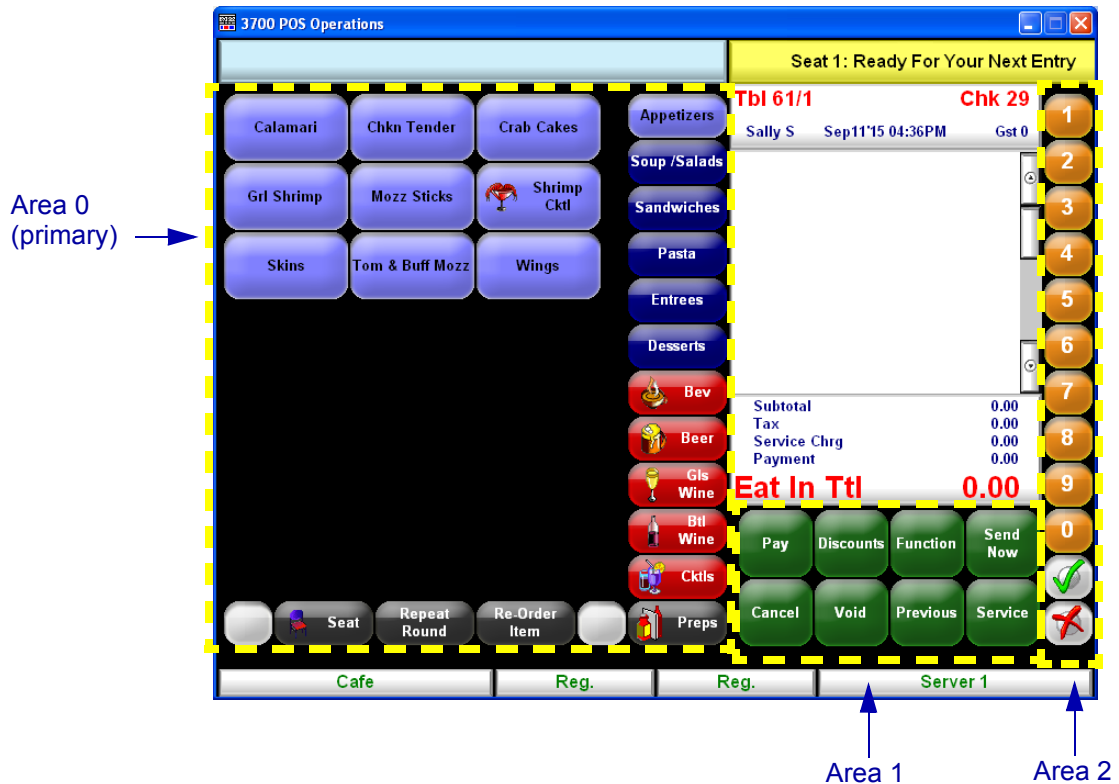
1. Navigate to the *Micros\Common\ManagerProcsASP* folder and locate the **web.config** file.
2. Double-click to open the file in Notepad.
3. Locate the **CustomErrors Mode** setting and change the value to one of the following:
 - ◆ **On** — Displays the generic error message on all clients. This is the default setting.
 - ◆ **Off** — Displays detailed information on all clients. (Be advised, that in an enhanced security environment, this may expose too much detail at the client level.)
 - ◆ **RemoteOnly** — Displays detailed information on the local server only. Remote clients will see the generic message only. This is the recommended security setting, as it prevents remote users from viewing application detail.
4. Save and Close.

POS Configurator

Multiple Touch Key Areas

One of the limitations of touchscreen design has been its strict adherence to a single, programmable key area. On a typical touchscreen, this area consists of a rectangular box (or design grid) in which the hard-coded touch keys are placed. Programmers are free to add as many keys as the space allows, as long as they do not exceed the boundaries of the rectangle.

To enhance the design possibilities, changes were made in the template structure to support multiple touch key areas. During operations, these multiple areas can be combined to create a more complex touchscreen layout. The following sample uses the U-shaped template to create three distinct, and programmable areas.



The parameters of each design area (width, height, and screen position) are coded in the template definition. To differentiate between them, a unique number (or identifier) is assigned to each. (In template configuration, this is referred to as the **TsID**.)

By default, the primary **Area** is always listed as **0**. This is important, because during operations, **Area 0** is where the system-generated SLUs will be displayed. Any space that is not explicitly covered with hard-coded keys will be used for this purpose. This is the standard for single area touchscreens, as well.

When additional key areas are provided, each area is assigned the next number in the sequence. For example, if the template has two key areas, they would be numbered 0 (for the default) and 1. If there are three, the **Area** values would be 0, 1, 2.

Standard Templates

In this release, RES provides four standard templates that include more than one configurable key area. They are:

- ◆ **201 Check Detail L** — Provides 2 programmable areas that combine to form an L-shaped key layout. During operations, the check detail occupies the upper, right-side of the screen.
- ◆ **202 Check Detail U** — Provides 3 programmable areas that combine to form a U-shaped key layout. During operations, the check detail occupies the open center of the screen with the main touchscreen area to the right.
- ◆ **203 Check Detail U2** — Provides 3 programmable areas that combine to form a U-shaped key layout. During operations, the check detail occupies the open center of the screen with the main touchscreen area to the left.
- ◆ **302 QSR Order Detail L** — Provides 2 programmable areas that combine to form an L-shaped key layout. During operations, the check detail occupies the upper, left-side of the screen.

Custom Templates

Future releases may provide additional multi-area templates. As always, users have the option of creating their own templates, or customizing an existing template to define their own key areas. This is done by editing the **OpsDisplayUser.cfg** file.

Note For information on customizing the POS display, refer to the support document: *Restaurant Enterprise Solution, Editing the OPS Display User Configuration File, MD0003-064, Revision A, April 2006, available from the MICROS website.*

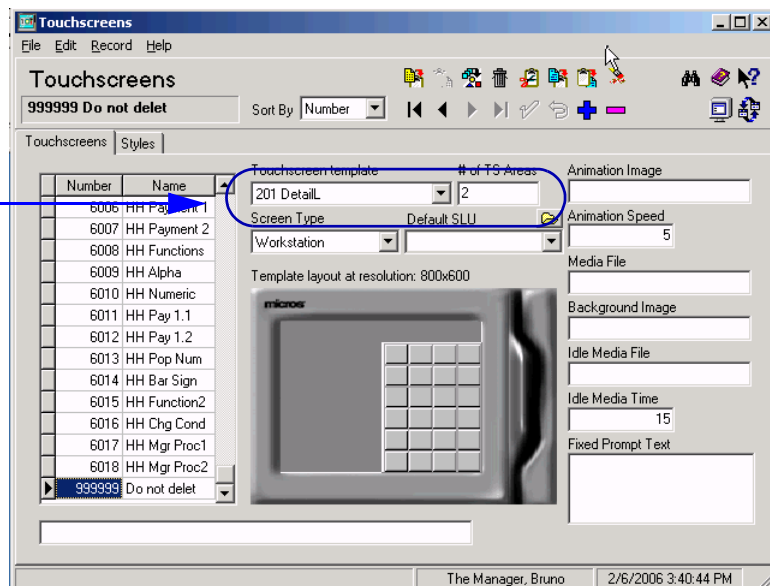
Because it affects core programming, changes to the POS configuration file should be handled by a qualified administrator only.

Enabling the Feature

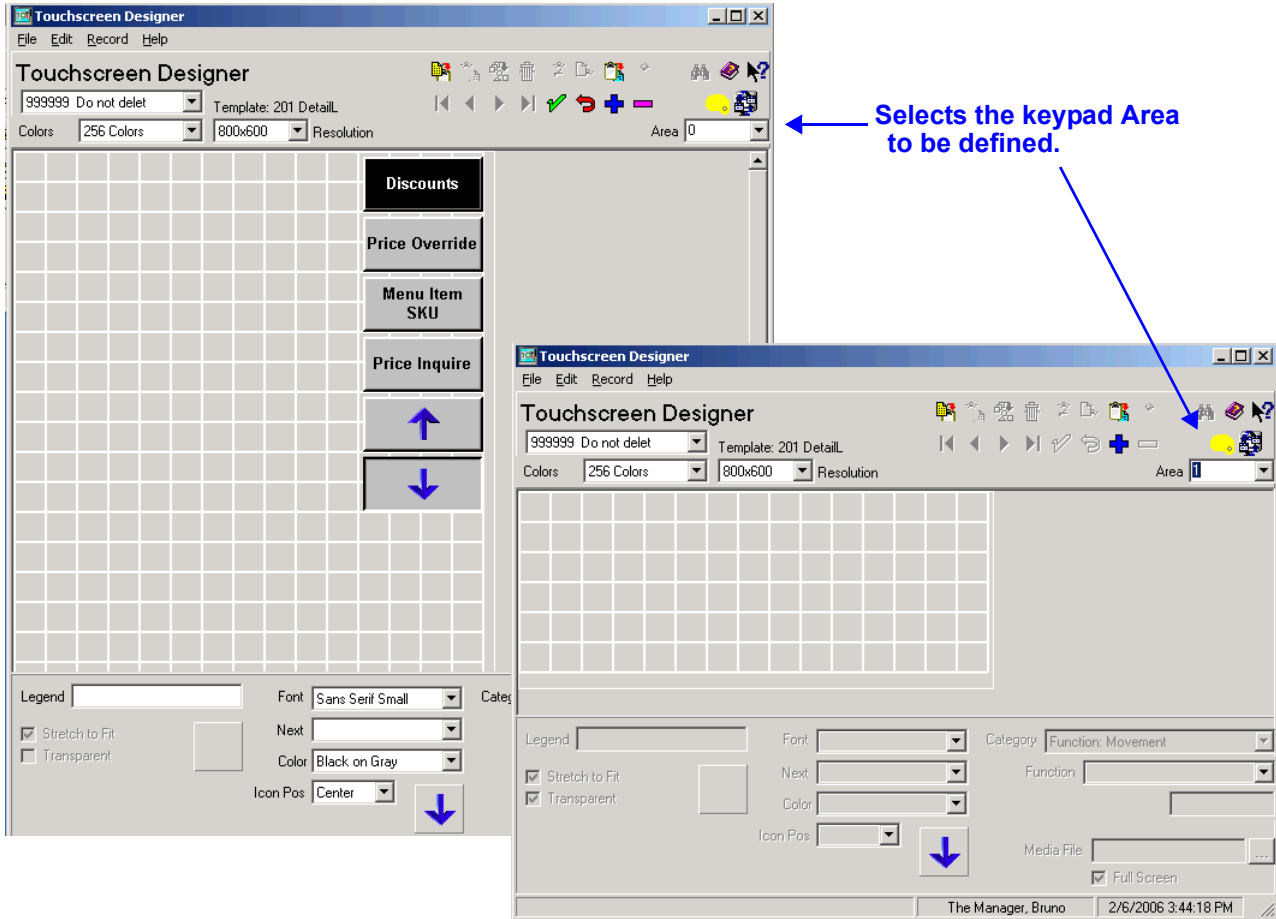
To support this feature, the following options were added to POS Configurator:

- ◆ **# of TS Areas** (*Devices | Touchscreens | Touchscreens*) — Indicates the number of user-definable touch key areas available on this touchscreen template. This is a read-only field.

Indicates the number of definable keypad areas available when using the DetailL template.



- ◆ **Area** (*Devices | Touchscreen Designer*) — Provides a drop-down list of the touch key areas that can be configured on this screen. The number of entries (and the dimensions of the programming grid) are determined by the selected touchscreen template. The default or primary touch key area is 0. This is where the system-generated SLU keys will display, if any are required.



POS Operations

Check Inactivity Timeout

The Check Inactivity Timeout feature prevents users from tying up a workstation by starting a check and then walking away without completing or canceling the transaction.

The feature was designed for a kiosk-style environment, where the system is relying on customer/operators to place their own orders. It is equally applicable in a non-kiosk environment (i.e., a restaurant or bar) where employees can access any open terminal.

Enabling the Feature

To support this feature, the following options were added in POS Configurator (*Devices* | *User Workstations* | *Kiosk Support*)

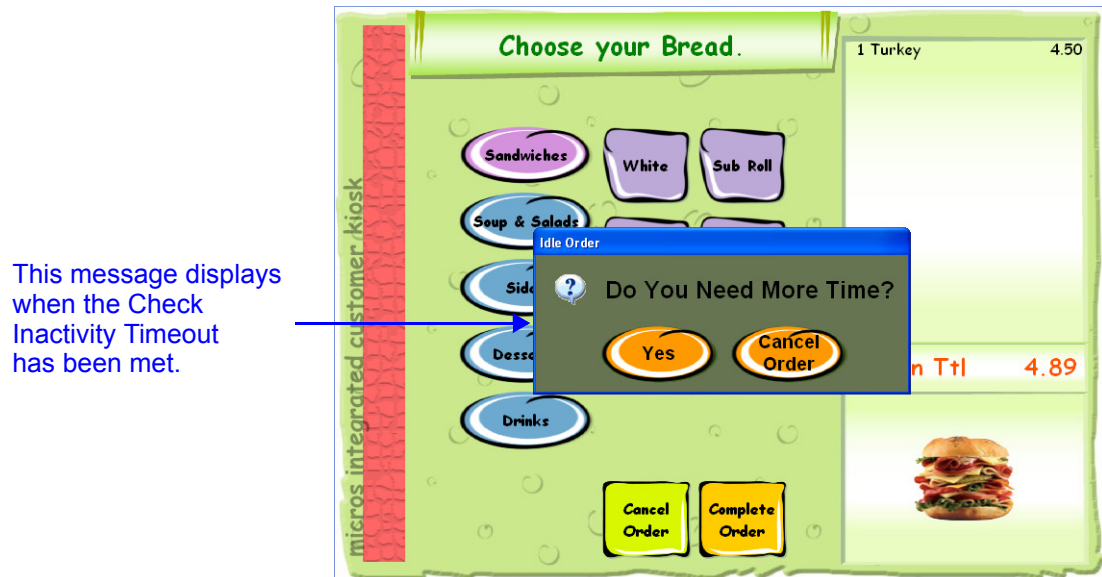
- ◆ **Check Inactivity Timeout** — Specifies how long an open check can remain idle before the transaction times out and the user is prompted for the next entry. Values are in seconds.
- ◆ **Check Inactivity Dialog Timeout** — Once a check timeout prompt is displayed, specifies how long the system will wait before cancelling the transaction. Values are in seconds.

Note *If the system is using Dynamic Order Mode (DOM), the current order will be cancelled along with all previous round items. In non-DOM environments, only the current round will be cancelled.*

Example

The Mike Rose Café uses kiosks to reduce overhead costs and allow customers to place orders at their own pace. To keep the terminals functioning, the **Check Inactivity Timeout** is set to **30**, and the **Check Inactivity Dialog Timeout** is set to **10**.

George, a new customer, uses the kiosk terminal to scan the menu. He begins a check and enters a sandwich before deciding that he'd rather go someplace else. Instead of canceling the order, he simply walks away. After being idle for 30 seconds, the system prompts for the next entry. Ten seconds later, the order is canceled automatically and the system returns to the *Start* screen.



Database Update Progress Bar

In previous releases, the system displayed a progress bar in the upper right-hand corner of POS touchscreens to monitor when configuration changes had been uploaded to the database. This setting is no longer included in the default setup.

To activate the progress bar, users will have to manually add the following DWORD value in the Registry:

HKLM\Software\MICROS\3700\Ops\DbUpdateDialog

and assign it a value of 1.

Font Changes

The check detail and review order areas of the operations touchscreen were reprogrammed to use proportionally spaced fonts, rather than the traditional fixed-width (or monospaced) ops08x10 font. The change eliminates the character distortion that occurred as the OPS font was scaled to larger sizes.

For Win32 and WS4 clients, the new default font is Arial. Hand-held terminals also support proportional fonts; however, their default font has not been changed at this time. They will continue to use the Courier New font.

Although proportional fonts are supported for all languages, not all languages will be able to use the system default. To work properly, sites may need to install other fonts and then modify the corresponding touchscreen display areas via the **OpsDisplaySys.cfg** file.

Note *For information on customizing the POS display, refer to the support document: Restaurant Enterprise Solution, Editing the OPS Display User Configuration File, MD0003-064, Revision A, April 2006, available from the MICROS website.*

Because it affects core programming, changes to the POS configuration file should be handled by a qualified administrator only.

When selecting an alternative, be sure to test thoroughly to ensure viability of the new font.

Review Order File Format Change

The review order text file (<workstation>rvo.rvo — located in the \MICROS\Res\Pos\Etc folder on the workstation) has been modified. Now, instead of mirroring the chit form (as the Journal file does), each line of the review order file will be differentiated from the next by a line separator. The format change was necessary to accommodate RES 4.0 support for proportional fonts, which allow more characters per line than fixed-width fonts.

A sample of the before and after formats is shown below:

Journal-style entries

```
Tbl 10/1   chk 1985   Gst 2
901 The Manager   Server
CE:   901 CC:     1 TC:   1
Trn 342   Mar15'06 10:36AM
-----
Eat In
1 Crab Cakes           6.95
1 Crab Cakes           6.95
1 Iced Tea              1.25
1 Iced Tea              1.25
Cash                   17.83
Subtotal               16.40
Tax                    1.43
Payment                17.83
=====
```

New line-delimited format

```
Review order File version:2.0
-----header_seperator-----
Chk 1886
10:22AM
-----line_seperator-----
2
Crab cakes
13.90
0
-----line_seperator-----
2
Iced Tea
2.50
0
-----line_seperator-----
Cash
17.83
0
-----line_seperator-----
15 %
0
-----line_seperator-----
15% Grat.
2.46
0
-----line_seperator-----
Cash
2.46
0
-----detail_seperator-----
-----header_seperator-----
Chk 1887
```

Touchscreen Resolution Enhancements

All standard touchscreen templates have been updated to support 1024 x 768 resolution. Previously, the options were limited to 640 x 480 and 800 x 600 resolutions.

Updated POS Icons

All of the standard POS icons have been updated for RES 4.0 with a new, modern look and support for three sizes:

- ◆ **16 x 16** (for HHTs)
- ◆ **32 x 32** (for 640 x 480 and 800 x 600 resolutions)
- ◆ **48 x 48** (for 1024 x 768 or higher resolutions)

For best results, users are cautioned to select a touchscreen that matches the resolution on their monitor. Failure to do so can cause problems in the display.

For example, if a touchscreen is designed to work at 800 x 600 but is run at the higher 1024 x 768 resolution, the icons may not appear on the keys. This is because the icon size for the 1024 x 768 display are 48 x 48. The key height and width of an 800 x 600 touchscreen are not large enough to support the larger icons.

To ensure that a template runs on the new 1024 x 768 resolution, users will need to adjust the key sizes.

What's Revised

A revision is defined as a correction made to any existing form, feature, or function currently resident in the 3700 POS 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.

Revisions Summarized

The table below summarizes the revisions included in this version.

Module	Feature	CR ID	Page
Database	Order Type Posting Fails on Transferred Checks	21869	45
Manager Procedures	Use of 1.1.Net Framework Causes Manager Procedures to Fail	14889	45
POS Operations	Function 'Initial Auth for Check Amount' Not Working Properly	N/A	46
	Sign-In Status Prompt Not Displaying on WS4	15028	46
Printing	Tilde Symbol (~) In Menu Item Names Causes Print Job to Fail	15451	47
Reports	Credit Card Batch Transfer Status Report Does Not Mask Credit Card Number	N/A	47

Revisions Detailed

Database

Order Type Posting Fails on Transferred Checks

CR ID #: 21869

Totals failed to post correctly when a check was started and service totaled by one employee, then transferred to a second employee who changed the order type before cashing out the check. The failure occurred even though the option **Post all check totals to current order type** (*Revenue Center | RVC Posting | Options*) had been enabled. This problem has been corrected.

Manager Procedures

Use of 1.1 .Net Framework Causes Manager Procedures to Fail

CR ID #: 14889

Occasionally, when running Manager Procedures, the system would fail after generating the following error:

```
A system error has occurred please close and  
restart the application.
```

Attempts to reopen Manager Procedures would cause a blank Explorer window to display.

The problem was caused by a conflict between the application and the updated 1.1 .Net Framework. This has been corrected.

POS Operations

Function 'Initial Auth for Check Amt' Not Working Properly

CR ID #: N/A

During operations, if a check was tendered to a credit card using the **[Initial Auth for Check Amt]** function, the system would ignore the actual check total and would request authorization for the amount specified in POS Configurator as the credit card's **Initial Auth Amount** (*Sales | Tender/Media | Credit Auth*).

For example, if the defined initial amount was set at \$50, but the check total was only \$35, the system would still request authorization for the full \$50 amount when the check was tendered. This occurred even if the operator was using the more specific check amount function key. This has been corrected.

Sign-In Status Prompt Not Displaying on WS4

CR ID #: 15028

During operations, the system status prompt was not displaying on WS4s. The problem occurred because the **signin.txt** file was being loaded from the wrong folder in the **\MICROS** directory. This has been corrected.

Note that the **signin.txt** file is not included with the WS4 package and must be created by the user or copied from the server's *\Res\Pos\Etc* folder to the *\Res\CAL\WS4\Files\CF\Micros\etc* folder for download to the WS4 device. If this folder does not exist, it will need to be manually created.

Printing

Tilde Symbol (~) In Menu Item Names Causes Print Job to Fail

CR ID #: 15451

In previous releases, sent from a WS4 failed to print a menu item if the name included a tilde (~) in it. If the menu item was preceded by two tildes (~~), the entire print job would fail.

The problem occurs because of internal conflicts with the print controller. Within the printing system, the tilde character is used to issue certain formatting commands. The character was chosen specifically because it is not frequently used and is never necessary. To prevent this problem, tildes should not be included in printable fields (i.e. Menu Item names, Discount names, etc.) in POS Configurator.

Reports

Credit Card Batch Transfer Status Report Does Not Mask Credit Card Number

CR ID #: N/A

In RES 3.x releases, credit card numbers were stored unmasked in the database, but would be included in the Credit Card Batch Transfer Status report unless the option **Override Credit Card Masking** (*Employees | Employee Classes | Privileges | Options*) was enabled.

With the RES 4.0 enhanced security, this is no longer permitted. All sensitive credit card information is now masked in the database and the option to **Override Credit Card Masking** has been removed from POS Configurator.

Kitchen Display System (KDS)

What's New

There are no new features in this version of the software.

What's Enhanced

An enhancement is defined as a change made to improve or extend the functionality of the current KDS application. 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 extends the current process. This differs from a revision (i.e., a bug fix) which corrects a problem not caught in the previous release of the software.

Enhancements Summarized

The table below summarizes the enhancements included in this version.

Module	Feature	Page
User Interface	New KDS Toolbar Icons	48

Enhancements Detailed

User Interface

New KDS Toolbar Icons

The KDS toolbar icons have been given a fresher, more modern look. The design is consistent with the updated look-and-feel of the user interface and is compatible with the new, selectable Themes feature.

What's Revised

There are no revisions in this version of the software.

Guest Service Solutions (GSS)

What's New

There are no new features in this version of the software.

What's Enhanced

An enhancement is defined as a change made to improve or extend the functionality of the current GSS application. 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 extends the current process. This differs from a revision (i.e., a bug fix) which corrects a problem not caught in the previous release of the software.

Enhancements Summarized

The table below summarizes the enhancements included in this version.

Module	Feature	Page
Operations	Support for MICROS Login Form	49

Enhancements Detailed

Operations

Support for MICROS Login Form

Access to the GSS back office application has been modified to support the standard MICROS Login form. This change allows GSS users to implement either standard or enhanced security for MICROS employees.

What's Revised

There are no revisions in this version of the software.

Cash Management (CM)

What's New

There are no new features in this version of the software.

What's Enhanced

There are no enhancements in this version of the software.

What's Revised

There are no revisions in this version of the software.

Labor Management (LM)

What's New

There are no new features in this version of the software.

What's Enhanced

There are no enhancements in this version of the software.

What's Revised

There are no revisions in this version of the software.

Product Management (PM)

What's New

There are no new features in this version of the software.

What's Enhanced

There are no enhancements in this version of the software.

What's Revised

A revision is defined as a correction made to any existing form, feature, or function currently resident in the PM 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.

Revisions Summarized

The table below summarizes the revisions included in this version.

Module	Feature	CR ID	Page
Ordering	Minimum Stock Not Converted to New Cost Center Units	N/A	53

Revisions Detailed

Ordering

Minimum Stock Not Converted to New Cost Center Units

CR ID #: N/A

In a multiple cost center environment, if the user created a new order; selected a **Vendor**, **Quantity**, and **Price**; and then switched the cost center from the default selection to another (e.g., restaurant to bar); the **Minimum Stock** units were not converted to the new cost center's order units. This occurred when the option **Min Stock Override** (*PM | Setup | Par Levels*) was enabled for the new Cost Center. That problem has been corrected.

Financial Management (FM)

What's New

There are no new features in this version of the software.

What's Enhanced

There are no enhancements in this version of the software.

What's Revised

A revision is defined as a correction made to any existing form, feature, or function currently resident in 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.

Revisions Summarized

The table below summarizes the revisions included in this version.

Module	Feature	CR ID	Page
Setup	Invalid Date Error When Setting Up New Periods	N/A	55

Revisions Detailed

Setup

Invalid Date Error When Setting Up New Periods

CR ID #: N/A

After setting up the first period of a new fiscal year, attempts to configure additional periods would trigger an error message indicating that an invalid date had been entered. This occurred because the system would incorrectly set an end date for the new period that exceeded the number of days in the calendar month (e.g., setting 30 as the end of day for the month of February). This problem has been corrected.

RES Platform

Introduction

This chapter comprises changes made to the RES Platform, which includes the following applications:

- ◆ MICROS Desktop
- ◆ License Manager
- ◆ Reports Explorer
- ◆ Language Translation Utility
- ◆ System Security
- ◆ Database Manager

What's New

A new feature is defined as one that provides capabilities that were not available in previous versions of the application.

New Features Summarized

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

Module	Feature	Page
System	RES Security Solution	58
	◆ Encryption	59
	◆ Password Management	63
	◆ MICROS Security Log	71
	◆ Risk Management	82
Utilities	Database Manager	85

New Features Detailed

System

RES Security Solution

The release of RES 4.0 marks the introduction of a comprehensive data security package. The new and enhanced features described in this section address vulnerability concerns in an increasingly complex and rapidly changing technical environment.

The MICROS security solution implements strong data encryption at the application level to protect sensitive data wherever it resides on, or is transmitted 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.

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.*

This section provides an overview of the RES Security Solution and discusses the areas that are affected by the changes. Topics covered include:

- ◆ Encryption
- ◆ Password Management
- ◆ Security Log
- ◆ Risk Management

Encryption

Securing the system involves protecting two types 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.
- ◆ **Data in Transit** — Refers to data transmitted from one computer process to another, where the process resides on different computers and the data must be transmitted across a network.

To secure data in these states, RES employs strong data encryption using industry-standard algorithms such as 3DES and AES. These algorithms are 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.

Current encryption algorithms are divided into two classes:

- ◆ **Symmetric** — Uses a single key to both encrypt and decrypt the data. This is the faster, though less secure method.
- ◆ **Asymmetric** — Uses separate but related keys (also referred to as a key pair), one to encrypt and one to decrypt the data. Functions are not assigned. That is, either key may be used to encrypt, but its opposite **MUST** be used to decrypt the results. This is the slower, more secure method.

Encrypted Areas

The RES 4.0 system includes a number of data storage and relay components where data are accessible. For this reason, data encryption is applied in multiple layers across the following areas:

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 (stand-alone 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.

For the in-store database, RES 4.0 encrypts the entire database using standard AES encryption. This process is transparent to applications that are working within the RES system and are authorized to access the database via standard SQL tools. The encryption of the database file prevents unauthorized access through binary editors and/or hex dump utilities.

In addition to the primary database encryption, a second level of 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	Field
cc_auth_dtl	cc_acct_num customer_name expiration_date track_2_data
cc_batch_item_dtl	cc_acct_num customer_name expiration_date track_2_data

Table	Field
cc_batch_item_xfer_status	cc_acct_num expiration_date
cc_batch_item_dtl_temp	cc_acct_num expiration_date track_2_data
cc_vchr_dtl	cc_acct_num
tmed_dtl	cc_acct_num expiration_date
gss_customer_def	cc_card_number cc_expire_date
ref_dtl	ref (only if reference entry is a credit card number)
emp_password_def	emp_pwd

RES 4.0 addresses the problem of data temporarily stored on a workstation, including devices configured for Standalone Resiliency (SAR) or Backup Server Mode (BSM), by applying RSA 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.

Data In Transit

During operations, data passes from the encrypted in-store database to a RES workstation and back. Typically, data is transported across a closed system such as a private LAN. This does not guarantee that the network is secure — particularly if the LAN includes wireless devices.

To address this issue, a separate transport key is used to encrypt all sensitive data before it is passed along the network. This is done at the application level and prevents unauthorized users from deciphering the files, regardless of how they are transported (LAN, WAN, WiFi). For added security, hardware- and transport-level protocols such as IPSEC, WEP, and WPA can be used to further encrypt transmissions.

Key Generation and Storage

The RES security paradigm requires the use of encryption keys in three areas:

- ◆ Encryption of the database.
- ◆ Encryption of the sensitive fields in the database.
- ◆ Encryption of sensitive data transmitted over the network.

Encryption keys are 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 an access-controlled section of the *Registry*, referred to as the **Key Store**.

During the initial installation or conversion to RES 4.0, a default key is provided. The default key allows sites to start-up the newly encrypted database.

Changing the Key

RES allows users to change the default key by modifying the pass-phrase. This is referred to as *key rotation*. During key rotation, the entire database must be unloaded and reloaded, and all historical information is re-encrypted. This may require up to several hours to complete.

Throughout the process, the POS must be down and the entire system will need to be rebooted once the rotation is finished.

WARNING!!!

Encryption Keys should NOT be changed unless required by the site and with permission from the customer's security expert.

Be advised that the loss of the pass-phrase will render the encrypted data unrecoverable. MICROS will be unable to help the site restore a database if the encryption key is changed and the pass-phrase is not available.

The mechanism for handling a key rotation is the new **Database Manager** utility. For more on this topic, refer to the security discussion, beginning on page 86.

Password Management

For added security, several significant changes were made to the way passwords are managed in the RES 4.0 System. Among the changes was the addition of greater control over the use of password IDs to log onto RES applications. The changes are consistent with industry standards for data security, which includes establishing guidelines for password length and format, rotation periods, and monitoring activity while logged into the system.

Password management occurs on three distinct levels:

Database User

When RES 4.0 is first installed, the system creates two active users with a default password and administrative privileges. One is the database administrator (DBA), which may not be deleted from the system. The other is the MICROS user. At the system level, all MICROS applications are run as the MICROS user. Passwords for these accounts can be changed in accordance with established security guidelines and are stored in encrypted format in the Key Store.

If necessary, sites can create additional database users for their own purposes through the new Database Manager utility. Typically, these are designed to allow third-party access to the database (e.g., for vendors or support functions).

Users added in RES 4.0 are limited to the following database functions:

- ◆ Read-only access to all MICROS tables.
- ◆ Create custom objects (tables, stored procedures, views, etc.).
- ◆ Run all MICROS stored procedures and views.

Note that these privileges represent a change from previous releases, in that new users will not be able to modify definition tables in the database.

Activating Existing Users

When upgrading from a RES 3.x database, the system retains all of the existing users, but disables their passwords. Users can be activated in the RES 4.0 system by entering a password through the Database Manager utility. For security reasons, MICROS recommends entering a new password, rather than reentering the existing, inactive value.

Caution! *Database passwords for “dba” and ‘micros’ users MUST be changed through Database Manager, not Sybase Central.*

Once a password has been changed through Sybase, that user will no longer be able to run any of the MICROS applications.

Users who have been ported over and reactivated from a RES 3.x database will retain all the rights and privileges assigned to them in the previous release, including the ability to modify the definition tables. MICROS recommends evaluating these user privileges and then adjusting them according to the needs of the customer.

Administrative Services User

At the operating system level, Microsoft® Windows creates a default administrative user with the necessary rights to manage Services on the local device. However, to communicate between devices and across the network, the system requires an administrative-level user with broader access privileges.

In previous RES versions, the **microsvc** user was created during setup as a MICROS auto logon with the required administrative permissions. This allowed the system to run autosequences, to copy files from one PC to another, and to manage network printing.

In RES 4.0, the MICROS services user (i.e., the **microsvc** user) was discontinued as part of the security upgrade. As a result, some changes had to be made to ensure that requisite stored procedures, autosequences, and print operations would continue to execute across the network.

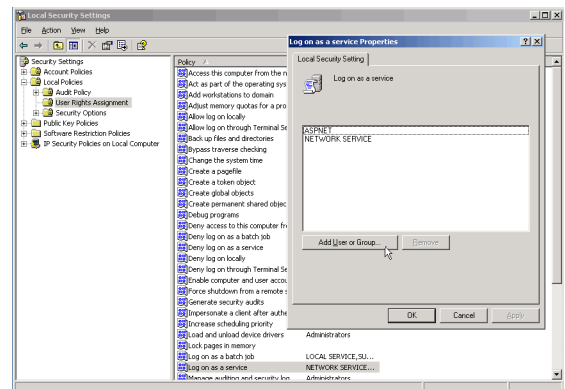
The primary change was to the Autosequence Server, which was retooled and added as a system Service (*Control Panel | Administrative Tools | Services*). Like all Services, it is set by default to execute as a Local System Account, with local permissions. This will work most of the time, but there are some tasks that will fail because of a permissions issue. Usually, this occurs when attempting to copy files across the network.

If an autosequence fails to execute because of a permissions issue, the Autosequence Server Service must be manually configured to run as a user with administrative privileges on both the local and network PCs. The options for setting the account permissions has always been available by navigating through the Windows Control Panel and right-clicking on a Service to open the *Properties* form.

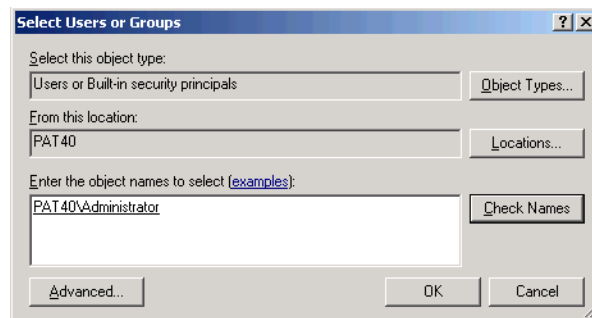
To simplify setup in RES 4.0, these options were also added to the *System | Restaurant | Security* form in POS Configurator. The Windows functionality is the same. Setting them in either form (POS Configurator or Windows Control Panel) will update the other.

One of the side effects of these changes is that, in the absence of the **microsvc** user, the system does not automatically allow the Windows user administrative rights to log on to the autosequence service. These must be assigned manually, as follows:

1. From the Windows Start Menu, select *Control Panel | Administrative Tools | Local Security Policy*.
2. When the form opens, navigate to *Local Policies | User Rights and Assignments* and double-click the **Log on as a service** option. The *Local Security Setting* form will display.



3. Click the **Add User or Group** button. A dialog box will display.



4. Enter the name of a privileged user and click the **Check Names** button. If the user is accepted, the entry will be underlined. Otherwise, a dialog box will display indicating that the system could not locate a Windows user with that name.
5. Click **OK** to continue. The form will close and the user will be added to the list of approved users and groups.
6. Click **OK** to accept the entry.

Note *After modifying an account link or user passwords, you must stop and restart the Service before the changes will be implemented.*

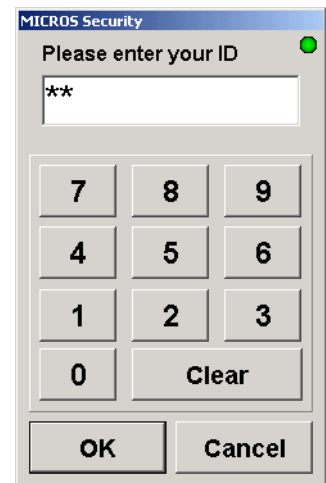
RES Application User

At the application level, MICROS requires employees to log in using an employee ID and password. In previous RES releases (Version 3.2 or earlier), employees were assigned their user ID when hired, and generally kept it for the duration of their employment.

During POS operations, or when launching any of the RES applications or utilities, a MICROS Security form would display. The user would be prompted to enter a valid **Password ID** in order to open the application. This is referred to as *MICROS Classic Security*.

Enhanced Passwords

In RES 4.0, users have the option of keeping the Classic Security model or implementing stricter control over password assignments. Classic Security is the default setting.



The enhanced security model does not apply to the following RES applications:

- ◆ POS Operations
- ◆ Cash Management
- ◆ Manager Procedures

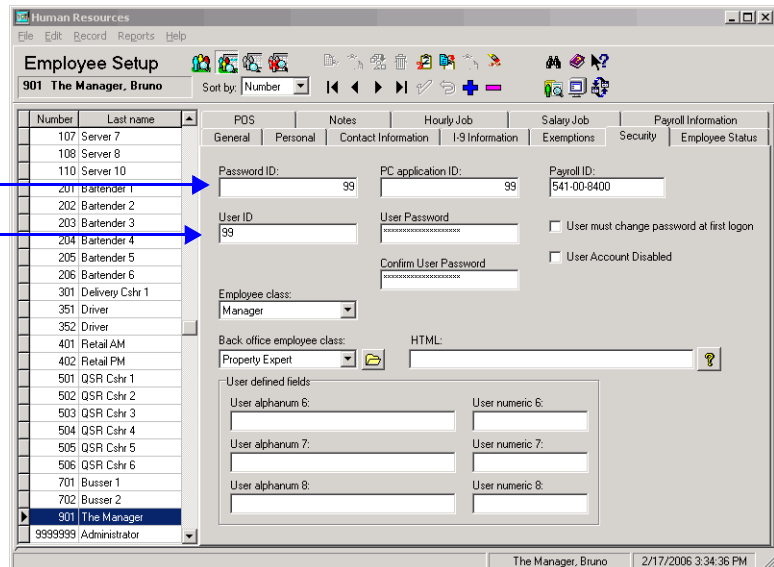
Sites that opt for the enhanced security model will need to make the following changes in POS Configurator:

- ◆ Disable the **Use Micros Classic security** option (*System | Restaurant | Security*).
- ◆ Complete the *Enhanced Password Security* section to control the way passwords are created, validated, and maintained in the alternate system.
- ◆ Assign valid **User IDs and Passwords** (*Employee Setup | Security*) to all active employees.

To differentiate from Classic Security, a second set of options was added for this purpose (see following image). Only one set is valid at a time. Rules for creating and maintaining passwords (length, duration, etc.) is only applicable in the Enhanced Security model.

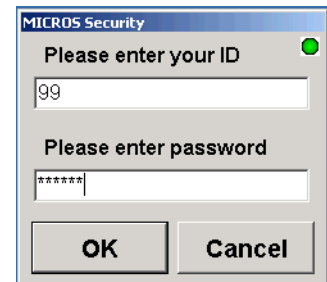
Classic User
Security
Passwords

Enhanced
Security
Passwords



Caution! Before closing POS Configurator, be sure to set the new passwords for at least one administrative-level employee. Once this application is closed, users will not be able to sign onto any application without a valid User ID and Password.

With Enhanced Security enabled, users who attempt to log on to RES applications will be presented with a different MICROS Security window. The new window prompts for both a valid **User ID** and a corresponding **Password** before launching the application. To support alphanumeric passwords, an attached keyboard is required.



User IDs must be unique for the system. However, different users may have the same password.

New Options

To support this feature, the following options were added to POS Configurator:

- ◆ *System | Restaurant | Security*
 - ◆ **Use Micros Classic Security** — When checked, allows sites to retain basic password security without implementing the more stringent criteria concerning password lengths, usage, rotation periods, etc.
 - ◆ **Days Until Password Expires** — Specifies the number of days that a password will be active. As the expiration time nears, the system will automatically notify the user and prompt for a new password.
 - ◆ **Minimum Password Length** — Establishes the smallest value allowed for a valid password.
 - ◆ **Maximum Idle Time in Minutes** — Specifies how long the current open application may remain idle before the system terminates the secure session.
 - ◆ **Maximum Failed Logins** — Limits the number of times a user may unsuccessfully attempt to login before being blocked by the system.
 - ◆ **Require AlphaNumeric Passwords** — When checked, requires valid passwords to include a combination of letters and numbers. This option is disabled if the site is using Micros classic security.
 - ◆ **Password Repeat Interval** — Specifies how many times the password entry must be changed before the current one can be repeated.

◆ *AutoSeqServ Logon Options*

The following options only need to be changed if additional system access is required to run certain autosequences, such as network report printing and external programs that access network shares.

- ◆ **Local System account** — Directs the current service to log on using the local account and local permissions. This is the default option. Clear this option to have the service log on using a separate account, as defined under the **This account** option.
- ◆ **Allow service to interact with desktop** — When checked, provides a user interface on the desktop that can be accessed by whomever is logged on when the service is started. This option is only enabled when the service is running as a Local System account.
- ◆ **This account** — Directs the service to log on using a specifically defined user account. This allows the user to have access to resources such as files and folders protected by the Windows operating system. This option must be enabled when using enhanced security access.

In addition to selecting the radio button, programmers must provide a **User Name** for the account and enter the **Password** (and **Confirm Password**). Refer to the *Administrative Services User* section (beginning on page 64) for instructions on configuring this user.

Note *Enabling this option requires a reboot of the server.*

- ◆ *Employees | Employees | Security* — These options are only relevant if Micros Classic Security is disabled.
- ◆ **User ID** — Specifies an identifier for the employee log-on. Up to 20 characters may be entered.

- ◆ **User Password** — Specifies the entry needed to authenticate the **User ID** and permit access to the system. Password length and composition (text, numbers, or alphanumeric combination) are defined under Enhanced Password security on the *System | Restaurant | Security* form.
- ◆ **Confirm User Password** — Duplicates the **User Password** for confirmation of entry.
- ◆ **User must change password at first logon** — When checked, requires the user to immediately change his/her password at the next logon. Although intended for new employees, this option can also be used to reset an employee password after the account was disabled.
- ◆ **User Account Disabled** — When checked, prevents a user from logging onto the system, even with a valid **User ID** and **Password**. This option may be triggered automatically if the employee exceeded the **Minimum Failed Logins** (*System | Restaurant | Security*) required to access the system.

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 4.0 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 4.0 application. Auditable activities are determined by the system and are posted automatically to the Log.

The following table lists the MICROS applications, options, and activities that are tracked in the Security Log.

Application	Activity
Autosequences & Reports (AutoSeqExec.exe)	<ul style="list-style-type: none">◆ All successful and unsuccessful login attempts◆ Report preview or Report print (including the name of the specific report)
Autosequence Server (AutoSeqExec.exe)	<ul style="list-style-type: none">◆ 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)
Credit Card Utility (CreditCards.exe)	<ul style="list-style-type: none">◆ 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
Report Explorer (RptExpl.exe)	<ul style="list-style-type: none">◆ All successful and unsuccessful login attempts◆ Report preview or Report print (including the name of the specific report)

Application	Activity
<p>POS Configurator (Poscfg.exe)</p>	<ul style="list-style-type: none"> ◆ All successful and unsuccessful login attempts ◆ Access, Edit, or Delete to the following forms: <ul style="list-style-type: none"> ◆ System Restaurant <ul style="list-style-type: none"> ◆ Business Settings: <ul style="list-style-type: none"> - (Save Batch Records) Number of Days ◆ Security: <ul style="list-style-type: none"> - (Enhanced Password) <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> - (Restrict Access to Employee Data) <ul style="list-style-type: none"> No Access Limitation Same level or lower Lower level only - (Date/Time) <ul style="list-style-type: none"> European date format European time format - Weight in kilograms ◆ Taxes: <ul style="list-style-type: none"> - Enable US tax or Canadian GST - Enable Singapore Tax - Enable Canadian Tax - Enable Florida surcharge tax - Enable Japan tax - (VAT Tax Method) <ul style="list-style-type: none"> Post taxable totals only VAT by round VAT by item - Australian GST is active - GST Prompt Threshold - Enable Thai Tax

Application	Activity
POS Configurator (Poscfg.exe)	<ul style="list-style-type: none">◆ Sales Tender/Media<ul style="list-style-type: none">◆ General:<ul style="list-style-type: none">- Type◆ Tender:<ul style="list-style-type: none">- Post to charge receipts- Post to gross receipts◆ CC Tender:<ul style="list-style-type: none">- 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:<ul style="list-style-type: none">- CA Driver- EDC Driver- CA tip %- Initial Auth Amount- Secondary Floor Limit- Secondary Difference %◆ Printing:<ul style="list-style-type: none">- Print with lookup

Application	Activity
<p>POS Configurator (Poscfg.exe)</p>	<ul style="list-style-type: none"> ◆ Revenue Center RVC Credit Cards <ul style="list-style-type: none"> ◆ General: <ul style="list-style-type: none"> - 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) <ul style="list-style-type: none"> Enable CA status display Display for entire RVC ◆ Headers: <ul style="list-style-type: none"> - CC Voucher Header ◆ Trailers: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - Enable secondary floor limit % - Enable secondary floor limit amount ◆ Printing: <ul style="list-style-type: none"> - 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

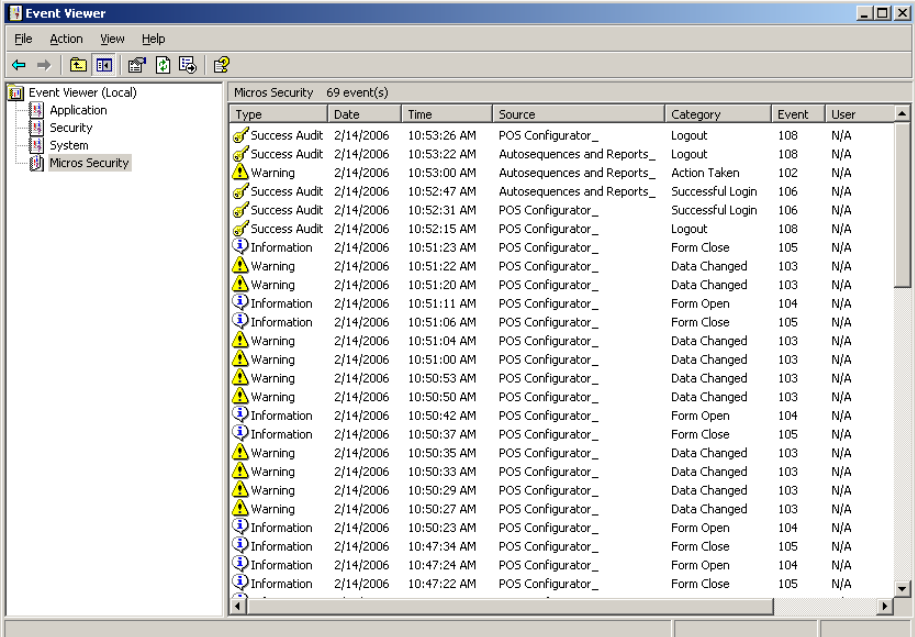
Application	Activity
<p>POS Configurator (Poscfg.exe)</p>	<ul style="list-style-type: none"> ◆ Revenue Center RVC Transactions <ul style="list-style-type: none"> ◆ General: <ul style="list-style-type: none"> - Tax Florida Surcharge - Print/Display lb. weight with 2 decimal places ◆ Employees Employee Classes <ul style="list-style-type: none"> ◆ Privileges Privilege Levels: <ul style="list-style-type: none"> - Mgr Procedures - POS Config. ◆ Privileges Privilege Options: <ul style="list-style-type: none"> - Use Reports - Clear all totals - Access to apps using password ID - (Credit Card Batch) <ul style="list-style-type: none"> Create Edit Reporting Settle ◆ Options: <ul style="list-style-type: none"> - Pay canceled credit auth - Mgr Procedures emp ID - POS Configurator emp ID ◆ Printing: <ul style="list-style-type: none"> - Reprint Credit Card Voucher ◆ Employees Employees <ul style="list-style-type: none"> ◆ Security: <ul style="list-style-type: none"> - User Account Disabled - User must change password at first logon - User ID - User Password ◆ POS Configurator Totals <ul style="list-style-type: none"> ◆ Clear All Totals ◆ Clear Labor Totals ◆ Clear Sales Totals

Application	Activity
GSS Backoffice (GSS.exe)	<ul style="list-style-type: none"> ◆ All successful and unsuccessful login attempts ◆ Access to all forms (edits not recorded)
Export Utility (ExportUtility.exe)	<ul style="list-style-type: none"> ◆ All successful and unsuccessful login attempts ◆ All queries run
Transaction Analyzer (Analyzer.exe)	<ul style="list-style-type: none"> ◆ 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
Database Manager (DM.exe)	<ul style="list-style-type: none"> ◆ All successful and unsuccessful login attempts ◆ Records all DM functions, whether implemented through the user interface (GUI) or from the Command Line.
EM (Mecu.exe)	<ul style="list-style-type: none"> ◆ All successful and unsuccessful login attempts
EM (EMStoreTotalsSynch.exe)	<ul style="list-style-type: none"> ◆ All successful and unsuccessful login attempts
EM (Store Employee Import Utility)	<ul style="list-style-type: none"> ◆ All successful and unsuccessful login attempts
EM (UCTconfig.exe)	<ul style="list-style-type: none"> ◆ All successful and unsuccessful login attempt
EM (MIPriceWiz.exe)	<ul style="list-style-type: none"> ◆ All successful and unsuccessful login attempts
Forecast Setup (ForecastSetup.exe)	<ul style="list-style-type: none"> ◆ All successful and unsuccessful login attempts
Forecasting (Forecasting.exe)	<ul style="list-style-type: none"> ◆ All successful and unsuccessful login attempts
Human Resources (HumanResources.exe)	<ul style="list-style-type: none"> ◆ All successful and unsuccessful login attempts
Labor Management (LM.exe)	<ul style="list-style-type: none"> ◆ All successful and unsuccessful login attempts

Application	Activity
Language Administration (Translate.exe)	◆ All successful and unsuccessful login attempts
MICROS Security Audit Log	◆ Logs rotation of Event Viewer Log (adds an entry to existing log and new log)
Payroll Preprocessing (PayrollPre.exe)	◆ All successful and unsuccessful login attempts
Product Management (PM.exe)	◆ All successful and unsuccessful login attempts
Scheduling (Scheduling.exe)	◆ All successful and unsuccessful login attempts

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:



The screenshot shows the Windows Event Viewer window with the 'Micros Security' log selected. The log contains 69 events. The following table represents the data visible in the screenshot:

Type	Date	Time	Source	Category	Event	User
Success Audit	2/14/2006	10:53:26 AM	POS Configurator_	Logout	108	N/A
Success Audit	2/14/2006	10:53:22 AM	Autosequences and Reports_	Logout	108	N/A
Warning	2/14/2006	10:53:00 AM	Autosequences and Reports_	Action Taken	102	N/A
Success Audit	2/14/2006	10:52:47 AM	Autosequences and Reports_	Successful Login	106	N/A
Success Audit	2/14/2006	10:52:31 AM	POS Configurator_	Successful Login	106	N/A
Success Audit	2/14/2006	10:52:15 AM	POS Configurator_	Logout	108	N/A
Information	2/14/2006	10:51:23 AM	POS Configurator_	Form Close	105	N/A
Warning	2/14/2006	10:51:22 AM	POS Configurator_	Data Changed	103	N/A
Warning	2/14/2006	10:51:20 AM	POS Configurator_	Data Changed	103	N/A
Information	2/14/2006	10:51:11 AM	POS Configurator_	Form Open	104	N/A
Information	2/14/2006	10:51:06 AM	POS Configurator_	Form Close	105	N/A
Warning	2/14/2006	10:51:04 AM	POS Configurator_	Data Changed	103	N/A
Warning	2/14/2006	10:51:00 AM	POS Configurator_	Data Changed	103	N/A
Warning	2/14/2006	10:50:53 AM	POS Configurator_	Data Changed	103	N/A
Warning	2/14/2006	10:50:50 AM	POS Configurator_	Data Changed	103	N/A
Information	2/14/2006	10:50:42 AM	POS Configurator_	Form Open	104	N/A
Information	2/14/2006	10:50:37 AM	POS Configurator_	Form Close	105	N/A
Warning	2/14/2006	10:50:35 AM	POS Configurator_	Data Changed	103	N/A
Warning	2/14/2006	10:50:33 AM	POS Configurator_	Data Changed	103	N/A
Warning	2/14/2006	10:50:29 AM	POS Configurator_	Data Changed	103	N/A
Warning	2/14/2006	10:50:27 AM	POS Configurator_	Data Changed	103	N/A
Information	2/14/2006	10:50:23 AM	POS Configurator_	Form Open	104	N/A
Information	2/14/2006	10:47:34 AM	POS Configurator_	Form Close	105	N/A
Information	2/14/2006	10:47:24 AM	POS Configurator_	Form Open	104	N/A
Information	2/14/2006	10:47:22 AM	POS Configurator_	Form Close	105	N/A

Note *All users on the Windows 2003 and XP Professional platforms 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. However, on Windows 2003 system, Administrators can use the Policy Editor to assign these rights to non-administrative users.

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.

Viewing Details

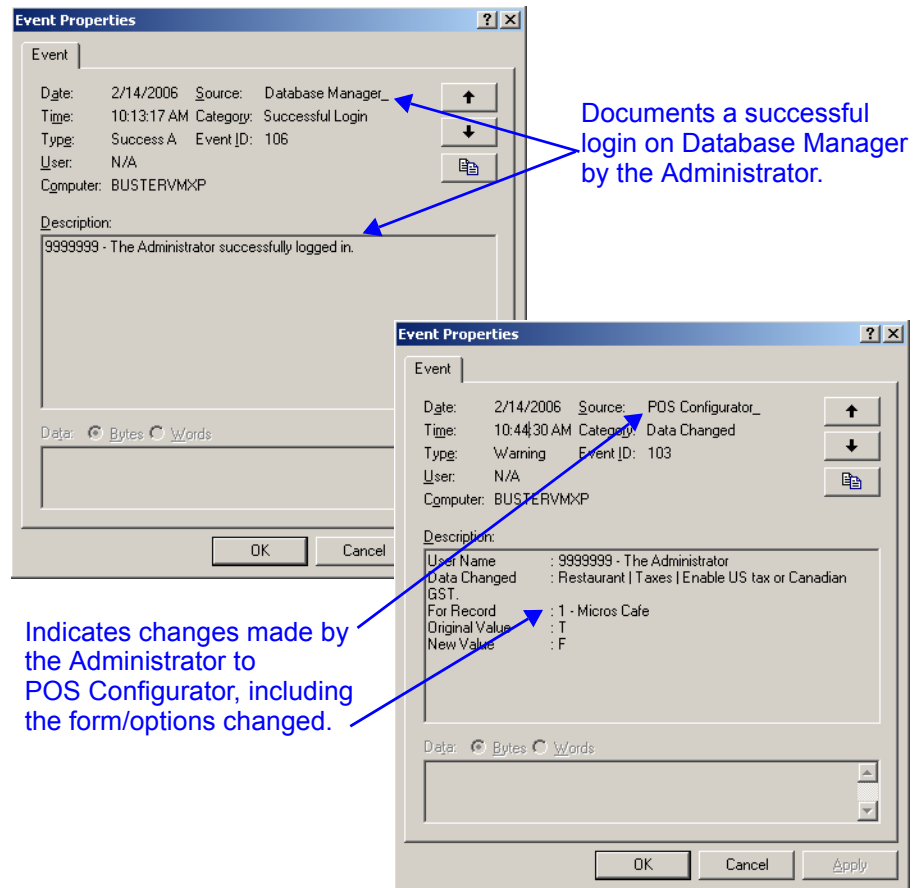
Event details can be viewed by double-clicking the item and opening the individual record. For each event logged, the system provides these details:

- ◆ **Date** — Date action occurred.
- ◆ **Time** — Time action occurred.
- ◆ **Source** — RES 4.0 application where the activity occurred.
- ◆ **Type/Category** — Event label and descriptor. The options are:

Type	Category
Success Audit	Successful Login Logout
Failure Audit	Failed Login
Warning	Data Changed
Information	Form open Form close Action Taken

- ◆ **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.

For example:



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 Database Manager application.

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.

Database Manager

The Database Manager also includes options for backing up the MICROS Security Log, but these are limited. Users can only enter a filename and specify where to store the backup. The default filename is **Microsecuritylogyyyymmdd.evt**. For more on this topic, refer to the Security Log discussion beginning on page 97.

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.

This section includes recommendations for risk management in a highly computerized environment. In addition to standard practices, it describes a number of programming options and processes that, while not explicitly prevented, are strongly discouraged as they may cause problems with and/or compromise the system.

Security Standards

In a secure environment, users are responsible for:

- ◆ **Securing the Network** — This includes installing and maintaining a firewall, monitoring network access, and regularly performing diagnostics to test the integrity of the security system.
- ◆ **Changing Passwords** — Once a user is added, it is up to the site to enforce rules on password rotation. Regularly changing passwords (e.g., every 60 or 90 days) reduces the probability that they will be obtained and used by someone outside the system. Similarly, when installing third-party applications, users are responsible for securing the interface by changing default settings and passwords.
- ◆ **Hiring Policies** — A system is only as secure as the people who operate it. Sites have sole responsibility for their hiring practices, assignment of user IDs, and granting access to the network, servers, workstations, key cards, or other physical devices that might provide access to the data.

Limitations and Recommendations

The following items represent known issues that will impact the secure database:

- ♦ **Sybase Updates** — All RES products are designed to work with the specific version of Sybase 9 software that is included with the current installation. Users are strongly advised to avoid downloading Sybase updates (either from the Sybase website or by using the automatic upload option from the DBISQL Help option) and applying them to the system.
- ♦ **PMS/SIM Interface Configuration** — When setting up an interface at an enhanced security site, the option **Log Transactions** (*POS Configurator | Devices | General*) must be disabled. Otherwise, the system will create a file using the **Outgoing Message Name** (e.g., **GuestConnection.log**) which will then record (unmasked and unencrypted) all information that is passed between the designated interface and RES. This includes all credit card numbers, expiration dates, and cardholder names. (This option should be used for troubleshooting purposes only.)
- ♦ **Fast User Switching** — This option allows 2 users to log onto the computer simultaneously, and to switch between active users without having the current user log off first. RES 4.0 does not support this option on the Windows XP platform. If enabled, it may cause some applications and/or processes to fail.

To disable, open the Windows Control Panel and select *User Accounts | Change the way users log on or off*. When the form displays, clear the option **Use Fast User Switching**.

- ♦ **SIM Scripts** — Sites using SIM scripts to read track data from a magnetic stripe card should be aware that the FULL track data will be exposed by SIM. For security reasons, users should evaluate any SIM script that involves credit card track data to assess whether or not the script should be used in RES 4.0.

- ◆ **Enhanced Security** — When using enhanced security, user passwords are not stored in the database in plain text. They are stored with one-way encryption (hashed). Third parties that wished to add employees to the MICROS database (micros.emp_def) must insert the employee record without the user password.

These users will have access to POS Operations, Manager Procedures, and Cash Management through their **Password ID**, but will not have access to other RES applications until a privileged user opens *POS Configurator | Employees | Employees | Security* and assigns a **User Password**.

Utilities

Database Manager

The new Database Manager (DM) is a Windows-style application designed to handle common database functions in the RES 4.0 enhanced security environment. DM is only available on the Server.

There are two ways to access Database Manager:

- ◆ **From the User Interface** — Requires a valid MICROS user to log into the application.
- ◆ **From a Command Line** — Requires a valid MICROS user or a valid System DBA user to log into the application.

Description

The application provides a user-friendly interface that simplifies database handling in three key areas:

- ◆ **Security** — Manages database encryption keys and limits access via user passwords.
- ◆ **Maintenance** — Installs, updates, and converts existing databases without rerunning system setup.
- ◆ **Diagnosis** — Provides access to log files and related utilities.

The following sections describe these functions in greater detail.

Database Security

One of the key features of Database Manager is the ability change the encryption keys and to limit access via database passwords.

WARNING!!!

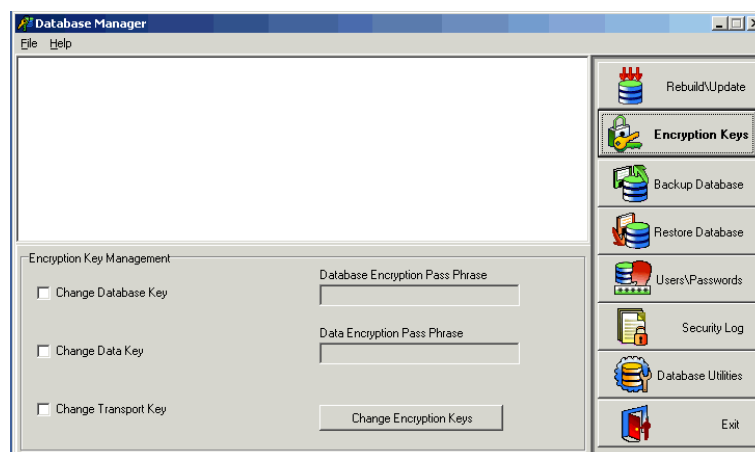
Encryption Keys should NOT be changed unless required by the site and with permission from the customer's security expert.

Be advised that the loss of the pass-phrase will render the encrypted data unrecoverable. MICROS will be unable to help the site restore a database if the encryption key is changed and the pass-phrase is not available.

Encryption Keys

In the initial installation or conversion to a RES 4.0 database, a default encryption key is provided to secure data in two of the three areas of vulnerability: 1) general database information, and 2) sensitive credit card data. There is no default key for the third area, data in transit. Transport keys must be created during initial installation as described in the *RES 4.0 Installation Guide (MD0003-086)*. (For more on Encryption, see page 59).

For security purposes, sites may want to change keys at regular intervals. In DM, the *Encryption Keys* form provides the necessary configuration settings to manage this process.



Options. The following list summarizes the available options. Note that none of the changes are implemented until the **Change Encryption Keys** button is pressed

- ◆ **Change Database Key** — When checked, allows the user to change the database encryption key. This key is required to start the database.

WARNING!!!

Changing the database key requires the system to be at the Database level. This will rebuild the database.

During key rotation, the entire database will be unloaded and reloaded and all historical information is re-encrypted. This may take several hours. Upon completion, reboot the entire system, including all clients.

-
- ◆ **Database Encryption Pass Phrase** — Specifies the phrase that will be used to create a new database encryption key. This field is not enabled unless the option **Change Database Key** is checked.
 - ◆ **Change Data Key** — When checked, allows the user to change the key that encrypts sensitive data.

WARNING!!!

Changing the data key requires the system to be at the Database level.

During key rotation, all historical information is re-encrypted. This may take several minutes. Upon completion, reboot the entire system, including all clients.

-
- ◆ **Data Encryption Pass Phrase** — Specifies the phrase that will be used to create a new secure data encryption key. This field is not enabled unless the option **Change Data Key** is checked.

- ◆ **Change Transport Key** — When checked, allows the user to change the key that encrypts data for transfer between workstations.

WARNING!!!

Once the transport key is changed, reboot the entire system, including all the clients.

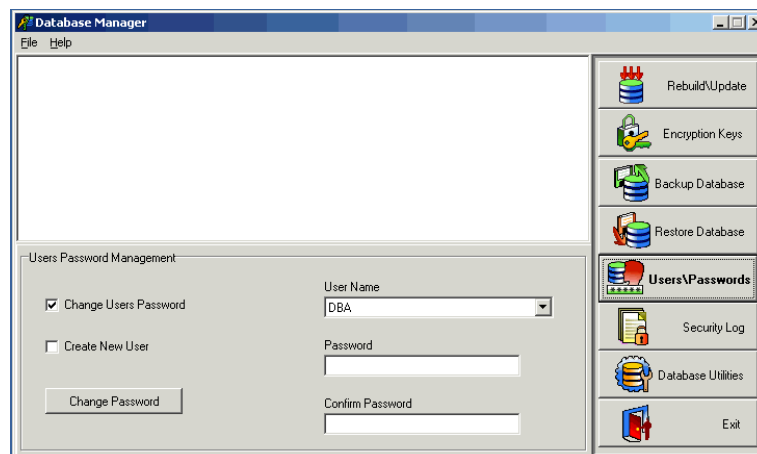
Do not change the transport key while any of the clients are in standalone or backup server mode. This will result in a loss of all data stored on those clients.

User Passwords

The *Users\Passwords* form controls the addition/activation of database users and the assignment of passwords in the RES 4.0 system. Users cannot be deleted from this form.

In a clean installation, the system generates two users — a DBA and a Micros user — with administrative-level privileges. A default password is assigned, but is not displayed, even as a masked entry.

Passwords may be changed by anyone with privileges to do so (*POS Configurator | Employees | Employee Classes | Privileges | Privilege Options*). To change a password in DM, simply enter a new value in the **Password** and **Confirm Password** fields and press the **Change Password** button.



If necessary, users may be added by checking the **Create New User** box and completing the name and password fields. Users added in RES 4.0 have limited functionality that includes:

- ◆ Read-only access to all MICROS tables.
- ◆ Creating custom objects (tables, stored procedures, views, etc.).
- ◆ Running all MICROS stored procedures and views.

Upgrades. When upgrading from a 3.x database, the existing users will be imported and listed in the **User Name** drop-down field, but will not have a valid password. To activate a user, managers must enter a new password (and confirmation).

***Note** Reactivated users retain all the rights and privileges assigned to them previously. This includes the ability to modify definition tables, which is NOT available to new RES 4.0 users.*

Options. The following summarizes the options available on the *Users\Passwords* form.

- ◆ **Change Users Password** — When checked, allows the user to select a **User Name** and to change their password.
- ◆ **Create New User** — When checked, allows the user to create a new database user. These users will have read-only access to all Micros objects. This includes executing of Micros stored procedures and views.
- ◆ **User Name** — If changing a password for a user, select a name from the drop-down list. If creating a new user, enter a name in the **User Name** field. Up to 20 characters is allowed and may include text, numbers, and/or special characters.

***Exceptions** User names and passwords cannot begin or end with white spaces, and may not include single quotes, double quotes, percent symbols, or semi-colons.*

- ◆ **Password** — Type in an appropriate entry to identify the user during secure log on.
- ◆ **Confirm Password** — Enter the **Password** a second time to confirm the entry.

Database Maintenance

Database Manager provides an organized and structured interface for maintenance options (backup, validate, rebuild, and restore) that were run as external programs in RES 3.x releases. The DM forms replace the individual utilities previously accessed from the Windows Start menu (*Program | MICROS Applications | Utilities | Database*).

In the past, maintenance options were also accessible from a command line prompt or as part of an autosequence. This is still true in RES 4.0. However, if run from a command line, be advised that the formatting requirements and command line switches have changed. (For more on this topic, see discussion beginning on page 100).

Backup/Validate

The *Backup Database* form allows users to choose the level of effort applied during the current backup process and to specify a location for the output files. Because of the new security features, a database backup now generates the following files in the *\MICROS\Database\Data\Backup* folder:

- ◆ **Micros.db** — a copy of the current database.
- ◆ **MicrosKeyBackup.mbz** — a copy of the encryption key and user passwords.

Notice that the **Micros.log** file is not included. This is because the log is immediately applied to the database. The backed-up database is completely up-to-date to the last committed transaction.

During this process, an *Archive* subfolder is also created. In it, the two backup files are consolidated into a single **.mbz**, which is then labeled with the date/time that the file was generated. For example, if the database was backed up on 2/20/06 at 10:24 am, the archive file would be labeled **MicrosBackup_2006_02_20_10_24.mbz**.

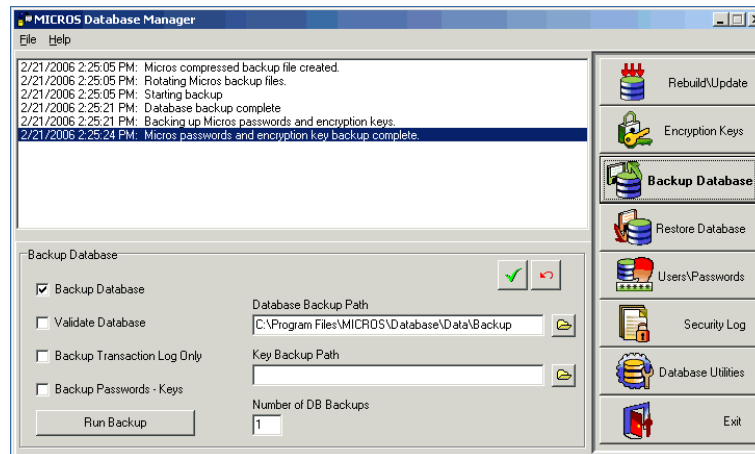
MICROS recommends running the Backup Database function once a day.

Multiple Backups. RES allows sites to store more than one backup database in the archives. An option is provided on this form to specify the number of copies. (This can also be done in *POS Configurator* | *System* | *Restaurant* | *Options*.)

Backup files are retained based on their timestamp, with the most recent copy replacing the oldest in the *Archive* subfolder. The *Backup* folder will keep only the latest version and key file.

Selected Processes. To save time, the system can update most recent backup files by simply applying the latest data from the Transaction Log. This option updates the **Micros.db** only. It does not affect the backup key file and does not update the archives.

Also, for added security, users can opt to save a copy of the key file, **MicrosBackupKey.mbz**, to a second location, designated by the user. Selecting this option does not update the key file in the primary backup folder.



Options. The following summarizes the options available on this form. Note that no action is taken until the **[Run Backup]** button is pressed:

- ◆ **Backup Database** — When checked, generates the appropriate backup and archive files and replaces previous versions.

- ◆ **Database Backup Path** — Specifies the location (directory path) where the backup files will be posted. The archived backups will be located under this directory path in a folder called Archives.
- ◆ **Validate Database** — When checked, confirms the integrity of the database. MICROS recommends running this option nightly, as part of the end-of-day procedures.
- ◆ **Backup Transaction Log Only** — When checked, updates the latest backup **Micros.db** using data from the current Transaction Log. This option will not affect the **MicrosKeyBackup.mbz** or update the compressed Archive file.

***Note** Once a site has been upgraded, you must run a full backup of the database before a “backup transaction log only” function can be performed. Failure to do this will cause the backup log file to get out of sync with the backup database.*

MICROS recommends running this function every 15 minutes while the business is operational. Once this function is performed, the micros.db should be copied to a safe location. It should only be used in the event of a server failure.

- ◆ **Backup Passwords - Keys** — When checked, creates a second backup file of the user passwords and encryption pass phrases.

This option may be run independent of the database backup process. The resulting **.mbz** file is posted to the location specified in the **Key Backup Path** field.

- ◆ **Key Backup Path** — Specifies the location (directory path) where the duplicate user password/encryption key backup file will be posted.
- ◆ **Number of DB Backups** — Specifies the number of database backups to be stored in the Archive folder of the backup directory. (The number of **micros.db** files will always be 1.) Only the most recent copies will be retained; all others will be purged from the system.

Example: If "2" is entered here, the Archive folder will store the

database from Monday and Tuesday. On Wednesday, the backup process will delete the Monday database and store the Tuesday and Wednesday database.

This option can also be set in *POS Configurator | System | Restaurant | Options*.

Rebuild\Update

The *Rebuild\Update* form eliminates the need to rerun setup whenever the database is upgraded, modified or repaired. Because of database encryption, updating versions and converting the decimal places can only be done on a RES 4.0 database.

The update/upgrade option is used to bring an existing database (either 3.x or 4.x) up to the version currently installed on the system. If the source database is a RES 3.x version, a rebuild will be performed automatically.

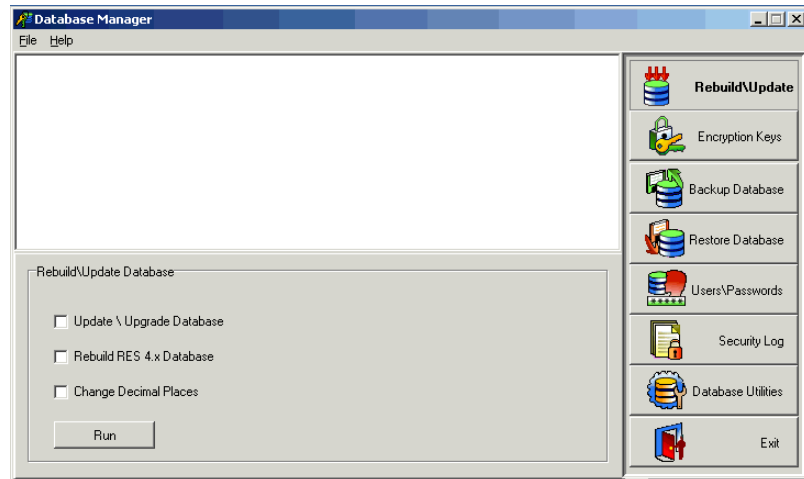
Note *Client databases that are already at a higher build number than what is currently installed on the server will not be changed since downgrading is not supported.*

The rebuild option has two functions:

1. Fix inconsistencies in the current 4.x database, and
2. Consolidate unused space (defrag) to reduce the size of the database file and improve system performance. Typically, this is done after clearing all totals.

When the database is rebuilt, the system unloads data from the current database and reloads it into a new shell. The existing decimal place setting is retained.

During setup, the system will convert the database automatically, provided one is present. If the database is not present, or if a different database is substituted after a RES 4.x installation, users can run DM as a standalone process to convert any RES 3.x database.



Options. The following summarizes the options available on this form. All actions are taken on the database located in *\MICROS\Database\Data*. Users must copy the database to this location before performing one of these functions. Note that no action is taken until the **[Run]** button is pressed.

- ◆ **Update \ Upgrade Database** — When checked, updates the existing database (either 3.x or 4.x) to the version currently installed on the server. If the database is a 3.x version, then a rebuild will automatically take place as well.
- ◆ **Rebuild RES 4.x Database** — When checked, converts an existing RES 4.x database to the current version. This option can also be used to improve system performance by cleaning up (defragging) the RES 4.x database.
- ◆ **Change Decimal Places** — When checked, recompiles the database to the number of decimal places specified. The options are 0, 2, or 3 decimal places.

Restore

The *Restore Database* options allow users to replace the current database and/or encryption keys with another database version. The restore function can be used for disaster recovery or (in the case of test labs) to swap out entire database setups.

To restore a full database, users must have access to the full version of the archived **.mbz** file (both database and encryption keys). This file is stored in the Archive folder as **MicrosBackup<timestamp>.mbz**.

Warning! *DM Backup allows you to create a separate .mbz file for the encryption keys only (**MicrosKeyBackup.mbz**).*

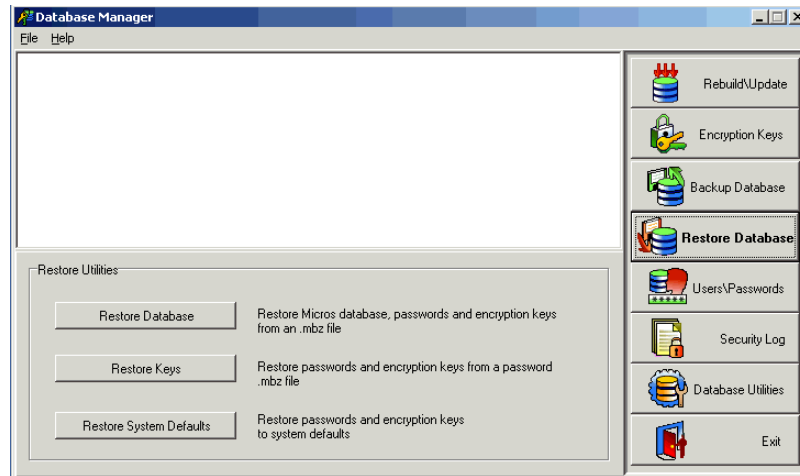
When restoring the database be sure to select the FULL .mbz version and NOT the encryption key backup.

Selecting the key file (which has no database!) will cause the restore process to fail and will leave the system in a disabled state.

When the option is implemented, the system does three things:

1. Saves the current database to the *Database | Data* folder and renames it to **ReplaceMicrosDB_<Date/Time>.mbz**. Should a problem arise with the newly restored files, users will be able to recover this database.
2. Decompresses the archived **.mbz** and copies in the **Micros.db**.

3. Resets the user passwords, encryption keys, and pass phrases.



Options. The following summarizes the options available on this form:

- ◆ **Restore Database** — Replaces the existing database with files restored from an archived database.
- ◆ **Restore Keys** — Replaces the current passwords and encryption keys with those belonging to a user-specified **.mbz** file.
- ◆ **Restore System Defaults** — Resets the passwords and encryption keys to the original default settings.

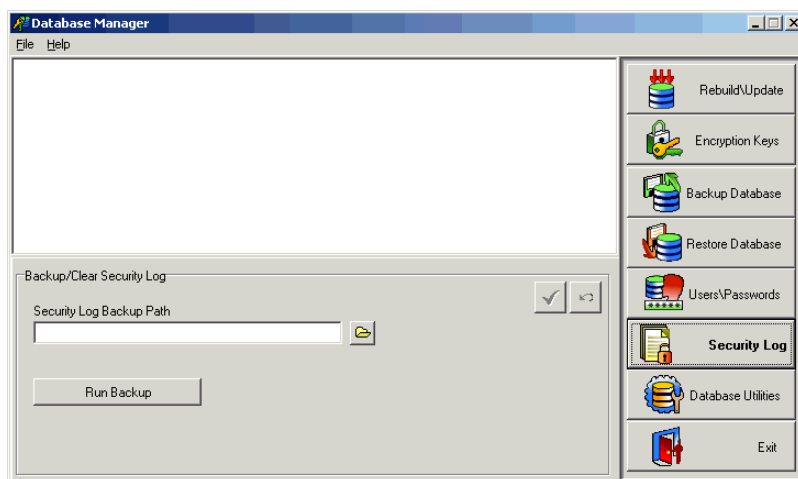
***Note** This option allows sites to start over, in the event that the encryption keys or pass phrases become lost. It CANNOT be used as a back door to restore a locked database if the encryption key is changed and the new key files are missing.*

Diagnostics

This section describes the log files and other utilities that are relevant to database management.

Security Log

The *Security Log* form allows privileged users to create a backup log of sensitive or secure data transactions, and to specify the path where the log will be saved. (For more on the contents, refer to the Security Audit Log discussion, beginning on page 71.)



Note *The Security Log can be managed directly from the Microsoft Event Viewer or from a Command Line prompt. For privileged functions, users must have operating system administrative rights. Otherwise, the system will prompt for a username and password before proceeding.*

An administrative user is not required when run from a scheduled autosequence, since the action is taken in the context of the system account.

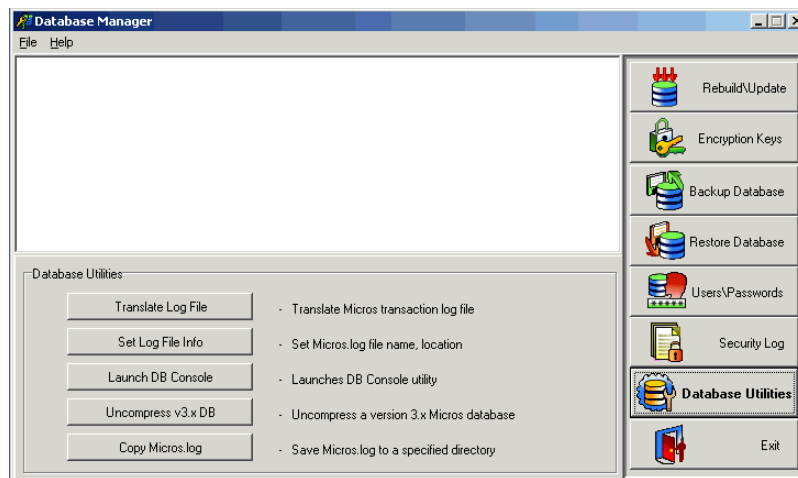
By default, the backup file is named **Microssecuritylogyyymmdd.evt**. When the backup file is generated, the system automatically adds a line to both the old and new logs, indicating that the log file has been rotated.

Options. The following option is not executed until the **[Run Backup]** button is pressed:

- ◆ **Security Log Backup Path** — Specifies the location (directory path) where the Security Log's backup file will be stored.

Database Utilities

The *Database Utilities* form organizes and consolidates in one location a variety of additional programs and processes used to access, modify, and manipulate the database. The specifics of each program are discussed in the **Options** section, below.



Options. The following summarizes the options available on this form:

- ◆ **Translate Log File** — Launches a wizard that allows a user to translate a non-running transaction log file into a SQL command file. To work, the selected file must be located on the local computer, or a drive must be mapped to the computer where that log file resides.

Translating a log file creates a SQL command file, which is a text file that contains SQL statements. The SQL command file can be run against a database to apply the operations that were recorded in the transaction log file.

- ◆ **Set Log File Info** — Allows a user to open a dialog box and select the file that will become the RES database. All transactions posted to this database will be recorded in the **Micros.log** file. The log file will always reside in the same directory as the database.
- ◆ **Launch DB Console** — Opens the Adaptive Server Anywhere Console utility, which provides access to the database connection information.
- ◆ **Uncompress v3.x DB** — Launches a wizard that allows a user to uncompress a RES 3.x database file.

Note: Uncompressing a database creates a new database file, but leaves the original compressed database file unchanged.

- ◆ **Copy Micros Log** — Generates a **Micros.log** file. When pressed, a dialog box displays prompting the user to specify a destination folder where the file will be posted.

The **Micros.log** file records all the transactions that have been posted since the last time the database was backed up.

Command Line Parameters

Because of encryption, the database can no longer be started from a command line. Other functions handled by Database Manager can be run, provided the user has database administrative rights (dba). For privileged options, a username and password is also required.

To backup the local database, for example, the user would specify:

```
DM -UID <Username> -PWD <User Password> -B
```

Note *User IDs and passwords are required to run Database Manager as an External Program within an Autosequence. For security reasons, the system will mask passwords before writing to the 3700d log or displaying information in the Autosequences and Reports window. The word/value following the -PWD switch (which is not case-sensitive) is replaced by six Xs (e.g., XXXXXX).*

Options

DM recognizes the following command line switches. Those options requiring a user name and password are indicated by an **X** in the **PWD Reqd** column.

Name	Function	PWD Reqd
-UID USERNAME	User login name	
-PWD PASSWORD	User password	
-U	Update or upgrade a specified DB	-
-R	Rebuild a 4.x DB	X
-C <0, 2, 3>	Convert decimal places to 0, 2, or 3 places	X
-B	Backup DB	X
-V	Validate DB	X
-T	Backup transaction log only	X
-K	Backup passwords and keys	X
-L	Backup/clear security audit log	X

Name	Function	PWD Reqd
-EK <PASS PHRASE>	Change DB encryption key.	X
-DK <PASS PHRASE>	Change sensitive data encryption key	X
-TK	Change transsport encryption keys	X
-RD	Restore default passwords and keys	-
-S <BACKUP FILE> [SAVE FILE]	Restore DB filename, save current DB	X
-P <USERNAME> <PASSWORD>	Change database user password	X
-A <USERNAME> <PASSWORD>	Add new database user	X
-CON	Launch dbconsole.exe	X
-TL <LOG FILE>	Translate micros.log file	X
-CL <DIR PATH>	Copy log file to specified path	X
-SL <DATABASE FILE>	Set micros.log filename	-
-N <DATABASE FILE>	Uncompress Micros Version 3.2 database	X
-F <DATABASE FILE>	Force Micros database to start	-
-Q	Suppress GUI interface	-
-?	Display this help list	-
<p>NOTES:</p> <ul style="list-style-type: none"> ◆ The -C (change decimal) switch can be used with the -U (update) or -R (rebuild) switch. ◆ The -B (DB backup), -V (validate), and -K (backup passwords/keys) switches can be used together. ◆ The -EK, -DK, and -TK (encryption key) switches can all be used together. ◆ The -Q switch can be used with all other switches. 		

Note *Command line options will NOT work if Database Manager is already open. Attempts to call a process under these circumstances will simply bring the DM application into focus.*

Access and Availability

Database Manager is accessed via the Window Start Menu (*Program | MICROS Applications | Utilities | Database | Database Manager*). On startup, the system displays a secure sign-in dialog before opening the application. Employees must be privileged to open the form or make changes to the current parameters.

DM Privileges

Users are granted access to Database Manager functions by checking one or more of the following options in POS Configurator (*Employees | Employee Classes | Privileges | Privilege Options*).

- ◆ Allow DB Rebuild
- ◆ Allow Encryption Key Change
- ◆ Allow DB Backup
- ◆ Allow DB Restore
- ◆ Allow User Edit
- ◆ Allow Security Log Access
- ◆ Allow DB Utilities

When checked, members of the designated employee class will have access to all the options on the corresponding DM screen.

Log Files

Database Manager logs activities to both the **3700d.log** and to its own **DM.log** file, located in the `\MICROS\Common\Etc` folder.

The **DM.log** should be considered for log management along with the other logs that are handled through scripts or as part of the end-of-night autosequences.

What's Enhanced

An enhancement is defined as a change made to improve or extend the functionality of the current application. 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 extends the current process. This differs from a revision (i.e., a bug fix) which corrects a problem not caught in the previous release of the software.

Enhancements Summarized

The table below summarizes the enhancements included in this version.

Module	Feature	Page
MICROS Desktop	Secure Mode Enhancements	104
Setup	Client Support for RES 4.0	104
	Database Installation	106
	RES Program Installation	106
System	Command and Control Enhancements	107
	Windows Host File Changes	116
	Windows Theme Support	116

Enhancements Detailed

MICROS Desktop

Secure Mode Enhancements

In previous (3.2 and lower) releases, the **microssvc** user was used to auto-logon to the MICROS Secure Desktop. For security reasons, the **microssvc** user has been eliminated in RES 4.0. In its place, users have the option of creating a **Power User** entry (*Control Panel | Administrative Tools | Computer Management | Local Users and Groups*). Power Users are one step below **Administrators**. They have sufficient privileges to perform the necessary logging functions, but prevent access to sensitive files on the system.

Note *Limited users have even less access and will not satisfy the auto-logon requirements.*

Setup

Client Support for RES 4.0

In RES 3.2, Windows 2000 and NT clients could run all of the RES applications. Because of the new security features, RES 4.0 limits the applications that can be run on certain platforms.

The following table specifies the applications that are supported on the various RES 4.0 clients:

Client Type	Operating System	Application Supported
MICROS Ultra	Win NT	3700 POS, GSS Front-of-House, Delivery Dispatch, Manager Procedures, KDS Client
MICROS Eclipse	Win NT Win 2000	3700 POS, GSS Front-of-House, Delivery Dispatch, Manager Procedures, KDS Client
MICROS Eclipse	Win XP Pro SP2	All Applications

Client Type	Operating System	Application Supported
MICROS 2010	Win 2000	3700 POS, GSS Front-of-House, Delivery Dispatch, Manager Procedures, KDS Client
MICROS 2010	Win XP Pro SP2	All Applications
MICROS WS4	CE 4.1 CE 4.2	3700 POS, GSS Front-of-House, Delivery Dispatch, Manager Procedures, KDS Client
Symbol 8846	Pocket PC 2003	3700 POS, GSS Front-of-House, Manager Procedures
Symbol MC50	Pocket PC 2003	3700 POS, GSS Front-of-House, Manager Procedures
Fujitsu BPAD	CE.net	3700 POS, GSS Front-of-House, Manager Procedures
MICROS Restaurant Display Controller (RDC)	CE.net 5.0	KDS Client
Non-MICROS Personal Computer	Win NT Win 2000	3700 POS, GSS Front-of-House, Delivery Dispatch, Manager Procedures, KDS Client
	Win XP Pro SP2 Win 2003 Server	All Applications

Database Installation

The RES 4.0 setup program will no longer install the following:

- ◆ **Sample Database** — The sample database and supporting files (bitmaps, desktop images, etc.) will be included in a separate sample database installation that will be available after the RES 4.0 General Release. The sample database can be accessed via the MICROS Website. As an alternative, users can take the sample database from RES 3.2 and convert it to RES 4.0 through the new Database Manager utility.
- ◆ **Standard Database** — The standard database has been retired. To obtain a RES 4.0 version, users will need to obtain a standard database from RES 3.2 and convert it to RES 4.0.

RES Program Installation

During setup, users have the option of specifying where to install the RES program files on the server. By default, the system places them in *C:\Program Files\MICROS*.

Before installing to a location other than *\MICROS*, users should make sure that custom applications will support the new directory structure.

Client Installation

For Win32 clients, users may change the drive only. Program files are automatically installed under *\MICROS*.

System

Command and Control Enhancements

To create a more secure, streamlined operation, significant changes were made to the command and control areas of the RES 4.0 application. The primary change was the elimination of Remote Procedure Calls (RPC) for non-interactive server (i.e., non-GUI) processes. These are increasingly viewed as a security risk and vulnerable to hackers. Accordingly, Microsoft has declared its intention to phase-out support for them on all Windows OS platforms.

In RES 3.2, the RPC Server processes included:

- ◆ Credit Card Server
- ◆ Autosequences Server
- ◆ Print Controller
- ◆ Interface Server

In RES 4.0, the RPC Servers have been replaced by out-of-process COM Servers that run as NT services. These services fall into two categories: on-demand and configuration-based.

On-Demand Services

On-demand services are not started until needed by the system. Once started, they continue to run until the computer is shut down. The Credit Card Server, Autosequences Server, Print Controller, and ResDBS are all handled as on-demand services.

Configuration-Based Services

Configuration-based services start on boot-up, but will shut down automatically if the network node is not configured properly. The Interface Server, ILDS, and ResBSM are examples of configuration-based services.

To setup one of these services, users must:

1. Configure the feature in POS Configurator, as required.

2. Open the MICROS Control Panel. Highlight **Restaurant** and press the **Reload DB** button. This will propagate the configuration changes down to the client.
3. Reboot the device that has been configured to run the server service.

Other Changes

The removal of RPC Server processing has had a trickle-down affect on system start-up, resulting in changes in the following areas:

POS Operations

Client-side processes are no longer controlled by 3700d.exe. All processes now run as NT services with the exception of POS Operation and KDS Display.

RES Clients

On the Client side, **3700d.exe** has been replaced with the Application Starter program (**AppStarter.exe**) for all Win32 clients. Previously, AppStarter was only found on WinCE devices (WS4 and hand-helds) and it would start automatically when the client was booted up. For Win32 clients, the application will not run until an operating system user is logged on with "Power User" privileges or higher.

With AppStarter, all workstations are treated as thin clients that are controlled as a group. That is, users cannot start/stop clients or processes individually. On client bootup, the application starts POS Operations and KDS (if configured to run on that device).

Note *Because of the OS auto-logon requirement, if someone logs off a client, POS and KDS will be stopped.*

At this point, POS Operations checks the state of the system (*OFF, Database, Back-of-House, Front-of-House*). If the Restaurant is not set to *Front-of-House*, a **System Closed** message will display across the OPS Sign-In screen. KDS will always display on the client, as long as the state of the Restaurant is *Database* or higher.

RES Server

On the Server side, 3700d is still used, but with limited functionality. As with clients, the utility is no longer used to control the RPC (non-GUI) processes, but will manage **RunDBMS.exe** to start/stop the database.

Also, 3700d will still write to the server log file for certain applications. However, because of changes in the way logging messages are reported, client entries will not be listed chronologically even though they are timestamped accurately. Some may be missed entirely due to an overflow of the logging mechanism. If this occurs, a “log overflow” entry will be posted.

Finally, the reduced role for 3700d means that AppStarter has become the mechanism for starting POS Operations on the Server. This is done manually, using the new **Start RES** shortcut on the Windows Start menu (*Start | All Programs | MICROS Applications*). The option to **Run OPS on server** (*System | Restaurant | Options*) has been removed from POS Configurator.

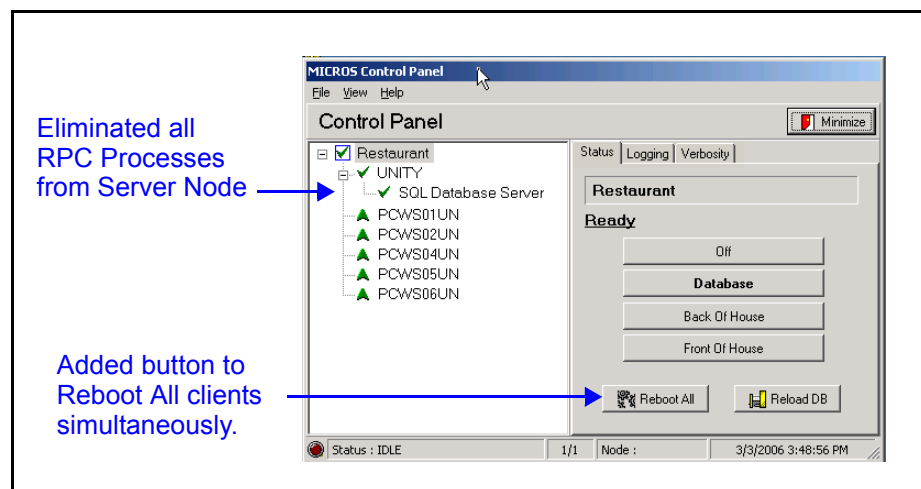
MICROS Control Panel

In RES 4.0, the MICROS Control Panel is only available on the Server. Clients will not be able to access the Server's Control Panel, which means the clients will have no control over the state of their individual workstations (as discussed in the section above).

On the Server, the look and feel of the Control Panel's user interface has been redesigned to reflect its more streamlined functionality, which includes the following:

Status Tab

- ◆ Removed all the RPC Processes (Credit Card Server, Print Controller, ILDS, Autosequence Server, etc.). The SQL Database Server is all that remains, displayed beneath the Server node.

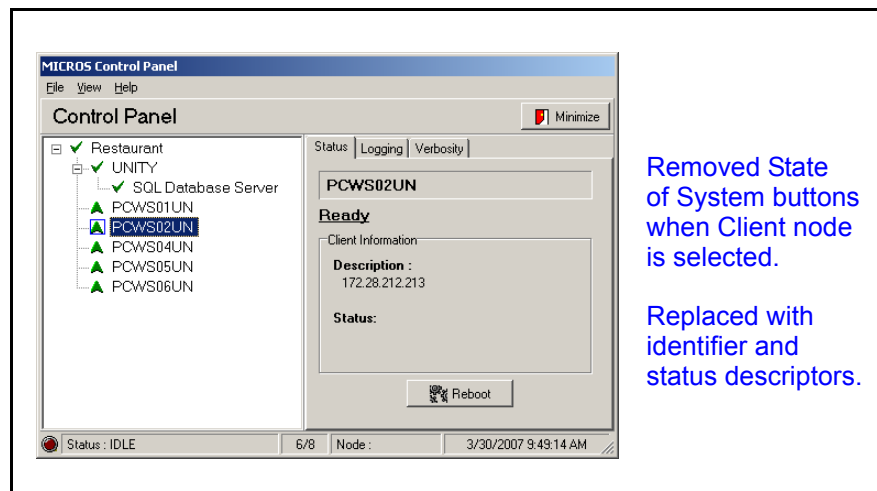


Note *ILDS has been converted to run as an NT Service. When an ILDS Device (POS Configurator | Devices | Devices) is linked to a Win32 Client, the ILDS Service on that client will start and sit dormant until the system reaches at least Back Of House status.*

If a Win32 client does not have an ILDS Device linked to it, the ILDS Service will shut down.

- ◆ Relabeled the **Reload** button as **Reload DB**, to more accurately describe its function. This option is only available at the Restaurant level.
- ◆ Added a **Reboot All** button to reboot all of the Win32, WS4, and HHT clients simultaneously. This option is only available at the Restaurant Level.
- ◆ Individual clients can be rebooted by highlighting the node and pressing the **Reboot** button. This option is only available for Win32, WS4, and HHT clients. Restaurant Display Controller (RDC) clients cannot be rebooted from the control panel (either individually or as part of a **Reboot All**). RDC clients must be manually rebooted.

When a client is selected, the buttons controlling the state of the system (*OFF, Database, BOH, FOH*) are replaced by a descriptor and status information boxes that were previously displayed only for WS4 and hand-held nodes. (In RES 4.0, system status buttons are only displayed at the Restaurant Level.)



Removed State of System buttons when Client node is selected.

Replaced with identifier and status descriptors.

Note *Although the system allows you to add up to 99 clients (POS Configurator | Devices | Network Nodes), the Control Panel will only display the first 80 nodes.*

Logging Tab

Unchanged in this release.

Feature Info Tab.

Removed.

Verbosity Tab

An option was added to the **View** menu drop-down list to display the **Verbosity** tab after the Control Panel is opened. Previously, the only way to make this tab visible was to start the application from a Command Line using the /verbosity switch.

This option is not implemented on RDC clients.

Note *Selecting a down client (indicated by a red arrow) while on the Verbosity tab will cause Control Panel to become non-responsive for up to 90 seconds. After that, the Verbosity window will be populated and Control Panel will be active again.*

Licensing Tab

The read-only **Licensing** tab has been removed from the Control Panel. Licensing is controlled through the License Manager utility and may be viewed from there.

Other Commands

Changed the key sequence to exit the Control Panel from **Alt-F-e** to **Alt-F-x**.

Command Line Control

Changes made to the MICROS Control Panel also affect the Command Line Control utility (**ClControl.exe**). This program performs all the functions of the Control Panel, but from an MS DOS prompt instead of the graphical user interface. Therefore, options that were removed from the Control Panel (e.g., RPC Processes and access to individual clients) will no longer be available through ClControl.

The advantage of executing from the command line is that it allows users to schedule the stopping and starting of the system as part of a batch process. The format for entering a command is *ClControl* followed by the appropriate switch(es) and/or text.

Options

ClControl recognizes the following command line switches:

Name	Function
/SYSTEM FOH /SYSTEM BOH /SYSTEM DB /SYSTEM IDLE /SYSTEM STATUS	Sets state to Front-of-House Sets state to Back-of-House Sets state to Database Shuts down System Displays current status of system. Possible return codes are: 0 (Fault) 1 (Idle) 2 (DB) 3 (BOH) 4 (FOH) 5 (Busy)
NOTE: /SYSTEM commands can have SYNC appended to indicate that the request should be issued to all nodes at once.	

Name	Function
<p>/NODE <NNN> /PROCESS <PPP> ON /NODE <NNN> /PROCESS <PPP> OFF /NODE <NNN> /PROCESS <PPP> RELOAD /NODE <NNN> /PROCESS <PPP> STATUS</p> <p>NOTE: Only affects Server node.</p>	<p>Start process <PPP> on node <NNN> Stop process <PPP> on node <NNN> Reload process <PPP> on node <NNN> Display status of process <PPP> on node <NNN>. Possible return codes are:</p> <ul style="list-style-type: none">0 — FAULT1 — OFF2 — ON3 — RELOADING4 — BUSY
<p>/M <text></p> <p>/CLEAR</p> <p>/LIST <path> NODES</p> <p>/LIST <path> /NODE <NNN> PROCESS</p> <p>/?</p>	<p>Insert <text> in 3700d log file</p> <p>Clear the 3700d log file</p> <p>List nodes in file <path></p> <p>List node <NNN> processes in <path></p> <p>Display this help list</p>

Autosequences

In RES 3.2 and earlier, if the user changed the time that an autosequence was scheduled to run, the change would not be implemented until the Autosequence Server was stopped and restarted. In addition, there were two ways to update the list of autosequences from the database:

1. **Manually** — After making changes to autosequences in POS Configurator, the user would open the MICROS Control Panel, select the Autosequences Server node, and press the [Reload] button.
2. **Automatically** — Every hour, the Autosequence Server would retrieve all autosequence information from the database.

With the removal of the Autosequence Server node from the RES 4.0 Control Panel, stopping and starting the new Autosequence Server Service is no longer required. When changes are made, users can manually update the autosequences by simply pressing the relabeled **[Reload DB]** button. The message “Received reload request from 3700d.” will be added to the 3700d.log to show that this action has taken place.

Hourly reloads will still occur automatically.

Windows Host File Changes

RES has always managed the Windows **hosts** file on Win32 machines. This file is located in the *(system root)\system32\drivers\etc* folder.

Updates to the host file occur whenever a change is made to a node in POS Configurator (*Devices | Network Node*). In RES 3.x releases, the revised host file was automatically posted to the Netsetup share. From there, it was only downloaded to the clients when **Netsetup.exe** was run. If the nodes were configured before running Netsetup, the snapshot of the host file that was installed to the client would be up-to-date. However, if clients were updated or added after setup, the new host file would have to be manually propagated around the system.

In RES 4.0, this process has changed. The crumMDS (which has always created and propagated the **MdsHosts.xml** file) is the new mechanism for distributing the Windows host file. On database startup or reload, it will automatically copy the host file down to the Win32 clients.

Note *Users may wish to disable this feature, particularly in network environments where anti-virus software is installed. Typically, these programs resist changes to the host files by outside applications.*

To disable the feature, users will need to create the following Registry key:

*HKLM\Software\Microsoft\DSM\DoNotManageWindowsHostsFile
and setting the DWORD value to 1.*

Windows Theme Support

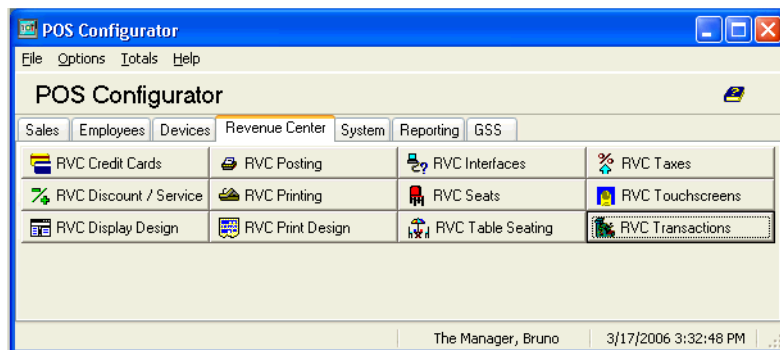
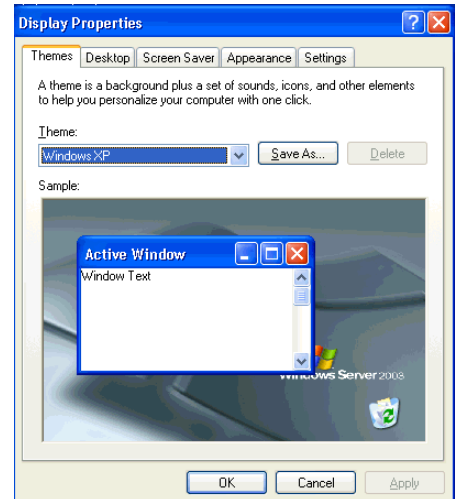
RES 4.0 has updated all back office applications to support Windows Themes on the XP and 2003 platforms. A theme is a predefined set of icons, fonts, colors, sounds, and other Windows elements that determine the look-and-feel of the desktop. (A more detailed discussion of this feature is available online from the Microsoft Windows support center.)

Themes can be changed by selecting *Start | Control Panel | Display* to open the **Display Properties** form.

On the *Themes* tab, select from the drop-down list and press **Apply**.

Once the theme is changed, all RES applications will inherit the visual settings of the Windows desktop.

For example, when opening POS Configurator with the Windows XP theme enabled, the RES application would display as follows:



Disabling the Feature

The use of Windows Themes is optional. However, the option can be disabled on RES sites by locating the following Registry key:

HKLM\Software\Microsoft\DisableThemes

and setting the DWORD value to 1. If the value does not exist (the default) or the DWORD is set to 0, Themes will be enabled.

What's Revised

A revision is defined as a correction made to any existing form, feature, or function currently resident in 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.

Revisions Summarized

The table below summarizes the revisions included in this version.

Module	Feature	CR ID	Page
Common	MICROS Security Login Does Not Retain Focus	14444	118

Revisions Detailed

Common

MICROS Security Login Does Not Retain Focus

CR ID #: 14444

When starting any of the RES applications (POS or Backoffice), the MICROS Security Login form would display briefly and, if the user did not click on the form quickly enough, would flicker briefly before losing screen focus. Users would have to bring the form to the foreground before entering their passwords. This problem has been corrected.