micros®
9700 HMS

9700 HMS Version 4.0 Maintenance Releases ReadMe First

About this Document

This ReadMe First document is intended as a quick reference guide to provide information about new features, enhancements, and revisions included in the latest release of the MICROS 9700 HMS software. This document contains information on the latest release for MICROS 9700 HMS.

General Information

For each version, this document provides the following information:

What's New

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

What's Enhanced

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

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

What's Revised

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

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

Additionally, all reported issues that are deemed to be BY DESIGN are included in this section as well. These issues will contain the preface BY DESIGN in front of the feature name.

Declarations

Warranties

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

Information in this document is subject to change without notice.

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

Trademarks

Adobe FrameMaker is a registered trademark of Adobe Systems Incorporated.
The following are registered trademarks of the Microsoft® Corporation;
Operating Systems - Microsoft Windows Server® 2008 R2.
Database Platforms - Microsoft SQL Server® 2008 R2.
The following are registered trademarks of the Oracle® Corporation;
Oracle® 11g.
Other products - Microsoft Excel, Win32 and Windows® CE.
Visio is a registered trademark of Visio Corporation.
All other trademarks are the property of their respective owners.

Printing History

New editions of this guide incorporate new and changed material since the previous edition. Minor corrections and updates may be incorporated into reprints of the current edition without changing the publication date or the edition number.

Edition	Month	Year	Software Version
1st	July	2013	4.0 GR
2nd	June	2014	4.0 MR1

Who Should Be Reading This Document

This document is intended for the following audiences:

- MICROS Installers/Programmers
- MICROS Dealers
- MICROS Customer Service
- MICROS Training Personnel
- MIS Personnel

What the Reader Should Already Know

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

- Operational understanding of PCs
- Understanding of basic network concepts
- Experience with Microsoft Windows Server® 2008 R2
- Experience with Microsoft SQL Server® 2008 R2 or Oracle® 11g

PCI Compliance

Visa established the Payment Card Industry (PCI) Data Security Standard to protect Visa cardholder data–wherever it resides–ensuring that members, merchants, and service providers maintain the highest information security standard. To adhere to the PCI standard, changes have been made to the 9700 HMS product. Please read this section carefully, as well as the accompanying PCI-compliance documentation. For a list of related documents, see the *Documentation Resources* section.

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

- Documentation Resources
- Security Announcement
- PCI Compliance Installation Changes

Documentation Resources

The following documents have been updated with information and procedures needed to maintain PCI-compliance and must be consulted for security purposes prior to upgrading from 9700 HMS Version 3.1 SP5 and below to 9700 HMS v3.6 and above. These documents are available on the MICROS 9700 HMS Product page of the MICROS Member Services website.

- *9700 v4.0 PA-DSS Implementation Guide*: This document is a quick reference guide that provides information concerning MICROS' adherence to the PCI Data Security Standard and Payment Application Data Security Standard (PA-DSS) compliance.
- *9700 Secure Default Account Handling*: This document contains detailed information on 9700 v. 4x secure default account handling procedures. These procedures must be followed to prevent compromised security and maintain PCI compliancy.
- *9700 v4.0 Security Guide*: This document describes 9700's security design, features that monitor employees' actions taken on the system, and features that restrict employee access to the database, reports, and operational procedures.
- *9700 Upgrade Best Practices*: This document is intended to convey the best practice information when upgrading the 9700 HMS application from a non-PCI compliant version (version 2.x) to a PCI compliant version (versions 3.x and greater).
- *MICROS 9700 v4.0 Key Manager Application Manual*: This document is a quick reference guide that provides information concerning the 9700 Encryption Key Management Utility, which allows the user to set the encryption passphrase for the 9700 system.
- *MICROS Secure Wipe Tool*: This document provides instructions on how to download and use the secure wipe tool Eraser. The secure deletion of data is necessary when upgrading a non-PCI compliant version of a MICROS software application or when customer data has been collected for troubleshooting purposes and is no longer needed.
- *Wireless Networking Best Practices*: This document explains the steps necessary to connect a wireless workstation for PCI-compliance.

Security Announcement

Overview

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

About PCI Compliance

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

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

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

For more detailed information concerning PCI-compliance, please refer to the PCI Security Standards Council website:

https://www.pcisecuritystandards.org/

Key Management Utility Security Enhancements

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

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

Warnings

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

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

Generally speaking, there is no way to determine whether an offline database that is about to be restored by the user is in sync with the 9700 application. Therefore, the only safe scenario to restore/replace a database is to restore/replace the database with a good database backup that must have been taken prior to performing the new key rotation. The database can only be restored/replaced if no key rotation has occurred since uploading the existing database or since the backup database was taken.

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

For more information and instructions on how to use the Key Management Utility, see the *9700 v4.0 Key Manager Application Manual*.

Secure Default Account Handling

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

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

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

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

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

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

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

PCI Compliance Installation Changes

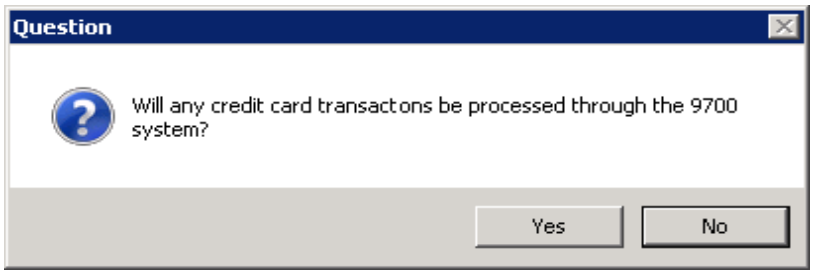
Changes were made to the 9700 installation process for versions 3.10 SP6 and higher, in order to meet the Payment Card Industry Data Security Standard (PCI DSS) requirements. For more information on PCI DSS, please see the Security Announcement section on page 7.

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

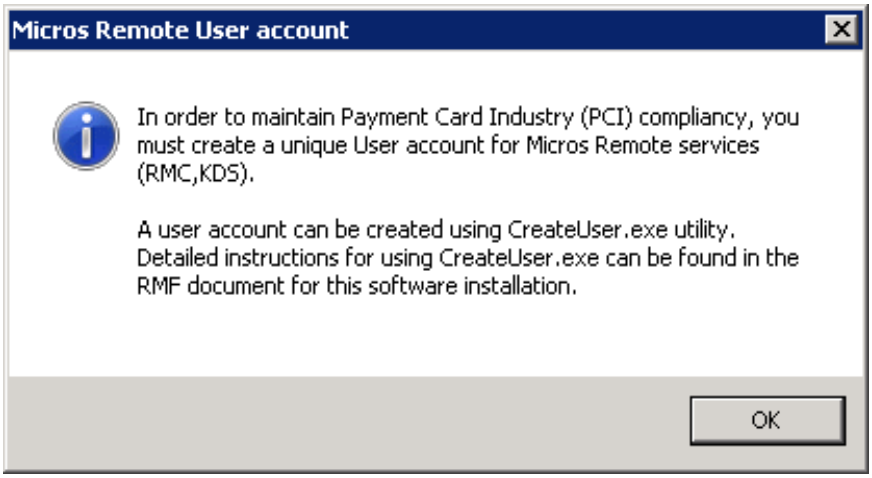
The installation process now recognizes if the server is on the domain or not on the domain. When the server is on the domain, domain-level security is automatically installed by the 9700 installation process. Disabling domain-level security will compromise PCI compliancy. If domain-level security is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

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

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



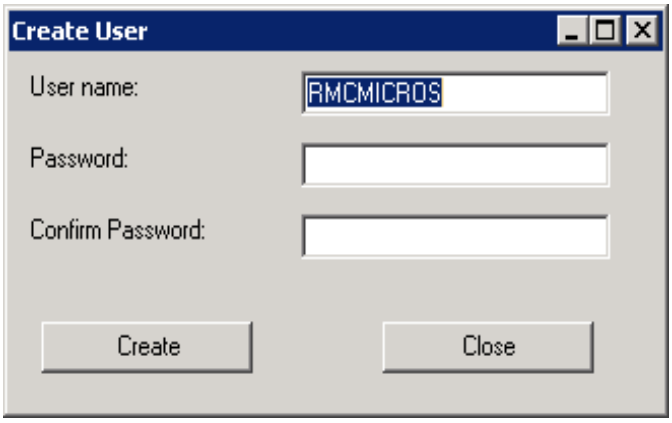
If the site is using remote RMC, credit cards are processed through the 9700 system, and the server is not on the domain, then the following prompt will display:



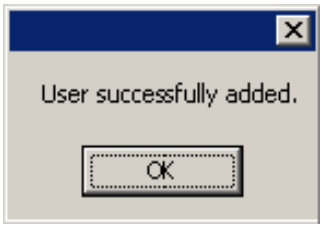
After clicking '**OK**' to close the prompt, follow the procedures listed below to maintain Payment Card Industry (PCI) compliance in a Windows® Workgroup environment when both credit cards and Remote RMC are used. Follow the steps below after the system has been updated to 9700 3.10 SP6 or a higher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

1. From the Windows® *Start* menu on the 9700 server, select *All Programs* | *MICROS Applications* | *CreateUser Utility.*

2. When prompted, enter a unique username and a strong password consisting of at least eight alphanumeric characters. Confirm the password and select '**Create**'. Do ***not*** use default User names or Passwords.



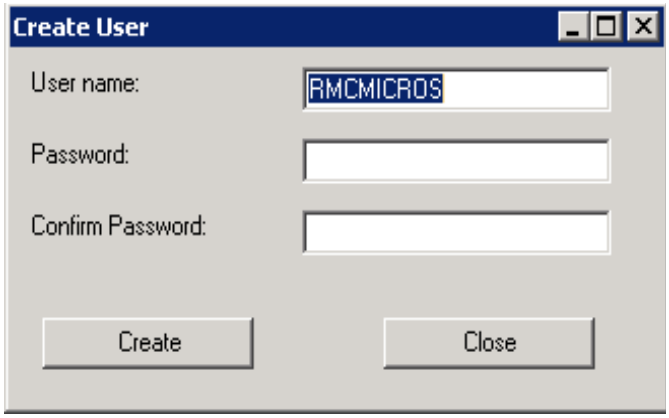
3. Select '**OK**' after the "User successfully added" message (as shown below) is displayed:



4. Select '**Close**' within the 'Create User' applet.

5. After Remote RMC is installed on the client workstation and updated to match the server version, from the Windows® *Start* menu select *All Programs* | *MICROS Applications* | *CreateUserUtility.*

6. When prompted, enter the identical User name and Password previously used on the server and then select '**Create**'.



9700 HMS Version 4.0 Maintenance Release 1

Important Notice!

For those sites running KDS, please see the Addendum section for the *Upgrading a Restaurant Display Controller (RDC) for KDS v2.1* article for important information about Restaurant Display Controller update requirements after upgrading to 9700 HMS v4.0.

What's New

New Features Summarized

There are no new features in this version.

What's Enhanced

Enhancements Summarized

There are no new enhancements in this version.

What's Revised

Revisions Summarized

The table below summarizes the revisions included in this version.

Revision	CR ID#	SCR ID#	Page
Credit Card Driver			
Credit Card (CC) data Memory handling has been improved in the VisaD CC Driver and SSLgw	34893	8371	16
EMC			
EMC wasn't properly handling the configuration of certain Report Writer (RW) Access levels	35123	8394	17
Ops			
Over tendering a check when Tender Media Rounding was enabled did not fire open the Cash drawer as expected		8284	17
Some Credit Card preambles were being rejected despite being configured in the EMC	34792	8361	18
Intermittently, SarOps would crash on WS5A POS Ready 2009Workstations	35071	8388	18
Other			
Rounding by Tender Media was not working as expected when the Currency Conversion function was used for an Alternate Currency		8261	18
POS API			
When a Transaction Services (TS) Credit Card (CC) transaction 'Amount Due' and 'Tip' amount were entered, the subsequent CC authorization amount erroneously added the Tip amount twice	34560	8340	19

Revision	CR ID#	SCR ID#	Page
RMC			
When logging onto the Remote Management Console (RMC), when an incorrect login attempt was made, users received an incorrect message	32767	5658	19
SAR			
Signature Captures were not posting to the PMS Interface when Mobile MICROS MC55A and MC70 handhelds were utilized	34426	8321	20
The encryption of secure Credit Card (CC) data on local databases stored on SAR clients has been improved		8360	20

Revisions Detailed

Credit Card Driver

Credit Card (CC) data Memory handling has been improved in the VisaD CC Driver and SSLgw

SCR 8371
CR ID# 34893
The VisaD CC Driver and SSLgw have been modified to clear the transmission buffer once the CC data request is sent.

EMC

EMC wasn't properly handling the configuration of certain Report Writer (RW) Access levels

SCR 8394
CR ID# 35123
Previously, assigning certain RW Access levels were being improperly handled by EMC. This resulted in connectivity problems with the database server or network when opening the *EMC-> **Menu Item Maintenance*** module. This has been corrected.

Built file(s): EMC.exe and EMCFramework.dll files.

Ops

Over tendering a check when Tender Media Rounding was enabled did not fire open the Cash drawer as expected

SCR 8284
CR ID# N/A
Previously, when the *EMC-> System Information-> Tender Media-> Cash record-> **Options tab**-> POS Behavior section->* **[Enable Tender Rounding]** and *Hardware Options section->* **[Open Cash Drawer]** options were enabled, the Cash drawer was not firing open as expected when a check was tendered. This issue occurred when the *EMC-> Revenue Center Information-> RVC Parameters->* **Posting and Control tab-** > *Control option->* **[7 - Open Drawer Only if Balance Due is 0.00]** was enabled as well. This has been corrected.

Built file(s): Ops.exe and SarOps.exe files.

Some Credit Card preambles were being rejected despite being configured in the EMC

SCR 8361
CR ID# 34792
Previously, CC preamble configuration was less complex because there were fewer cards using the same preamble CC numbers. This is no longer the case. Currently, specific ranges of CC numbers are being used by different companies that sometimes contain the same first digit. When the same CC preamble ranges were assigned to differing Credit Cards, Ops was unable to determine exactly which CC to charge. This has been corrected so that the 9700 Credit Card setup now supports China Unionpay CC preambles.

Built file(s): EMC.exe.

Intermittently, SarOps would crash on WS5A POS Ready 2009 Workstations

SCR 8388
CR ID# 35071
Previously, SarOps would crash on an intermittent basis on WS5A POS Ready 2009 Workstations. This has been corrected.

Built file(s): SarOps.exe.

Other

Rounding by Tender Media was not working as expected when the Currency Conversion function was used for an Alternate Currency

SCR 8261
CR ID# N/A
Previously, if Rounding by Tender Media was enabled for both the Base and Alternate Currencies and the option located in the *EMC-> System Information-> Currency-> Alternate tab->* ***Options***-> **[1- ON = Divide Base Currency; OFF = Multiply Base Currency]** was enabled, when the Currency Conversion function was used and then tendered using the Alternate Currency, users would receive an '**Entry must be Rounded Amount**' message. This has been corrected.

Built file(s): Ops.exe and SarOps.exe files.

POS API

When a Transaction Services (TS) Credit Card (CC) transaction 'Amount Due' and 'Tip' amount were entered, the subsequent CC authorization amount erroneously added the Tip amount twice

SCR 8340
CR ID# 34560
Previously, when a TS CC transaction was authorized that included a Tip amount, the CC authorization amount doubled the entered Tip amount. This has been corrected.

Built file(s): PosSrv.exe.

RMC

When logging onto the Remote Management Console (RMC), when an incorrect login attempt was made, users received an incorrect message

SCR 5658
CR ID# 32767
Previously, when an incorrect login attempt was made to access RMC, users received an incorrect message. This has been corrected. With this release, the system response has been updated to read, "**Your login credentials have failed. Please re-enter your username and password.**"

SAR

Signature Captures were not posting to the PMS Interface when Mobile MICROS MC55A and MC70 handhelds were utilized

SCR 8321
CR ID# 34426
Previously, when Mobile MICROS MC55A and MC70 handhelds were being used, Signature Capture information wasn't making it from the 9700 Transaction database to the PMS interface. Ultimately, users would receive a blank display screen on the Mobile MICROS and no error message displayed. This has been corrected.

Built file(s): HHTCEOPS.exe.

The encryption of secure Credit Card (CC) data on local databases stored on SAR clients has been improved

SCR 8360
CR ID# N/A
The encryption of secure Credit Card (CC) data on local databases stored on SAR clients has been improved. With this release, the 9700 Key Manager utility has been enhanced so that a pair of Asymmetrical Keys can be generated. One key will reside on the 9700 Application Server and another key will get downloaded to SAR clients to increase the encryption of secure Credit Card (CC) data on the locally store database on SAR clients. See the *9700 Key Manager Application Manual* for more information.

9700 HMS Version 4.0 General Release

Important Notice!

For those sites running KDS, please see the Addendum section for the *Upgrading a Restaurant Display Controller (RDC) for KDS v2.1* article for important information about Restaurant Display Controller update requirements after upgrading to 9700 HMS v4.0.

What's New

New Features Summarized

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

Feature	CR ID#	Page
Install		
Support for the installation of 9700 on Windows Server® 2008 R2 has been added		21
Support for running 9700 on Microsoft SQL Server® 2008 R2 has been added		22
Support for running 9700 on Oracle® 11g has been added		22

New Features Detailed

Install

Support for the installation of 9700 on Windows Server® 2008 R2 has been added

SCR 7689
CR ID# N/A
With this release, support for installing 9700 on the Windows Server® 2008 R2 operating system has been added.

Support for running 9700 on Microsoft SQL Server® 2008 R2 has been added

SCR 7909
CR ID# N/A

With this release, MICROS 9700 HMS v4.0 will be installable and supported on Microsoft SQL Server® 2008 R2. New customers will benefit by having the option to install the latest version of Microsoft SQL Server 2008 R2 software. There will be MICROS installation media for the Workgroup, Standard and Enterprise editions of the database platform. The installation media will only be capable of setting up the database for a single database server. Advanced features like clustering and mirroring will ***not*** be configurable with the MICROS installation media.

Support for running 9700 on Oracle® 11g has been added

SCR 7910
CR ID# N/A

With this release, MICROS 9700 HMS v4.0 will be installable and supported on Oracle® 11g. New customers will benefit by having the option to install the latest version of Oracle software (at the time of this release). The Standard and Enterprise editions of the Oracle 11g database platform have been tested. The installation media must be downloaded from the Oracle website using the following link: http://www.oracle.com/technetwork/database/enterprise-edition/downloads/index.html

What's Enhanced

Enhancements Summarized

The table below summarizes the enhancements included in this version.

Enhancement	CR ID#	Page
Documentation		
KDS v2.1 software has been integrated into 9700	30350	23
EMC		
A new 9700 v4.x Activation Code named 'Feat 4x Code' is introduced in the EMC		24

Enhancements Detailed

Documentation

KDS v2.1 software has been integrated into 9700

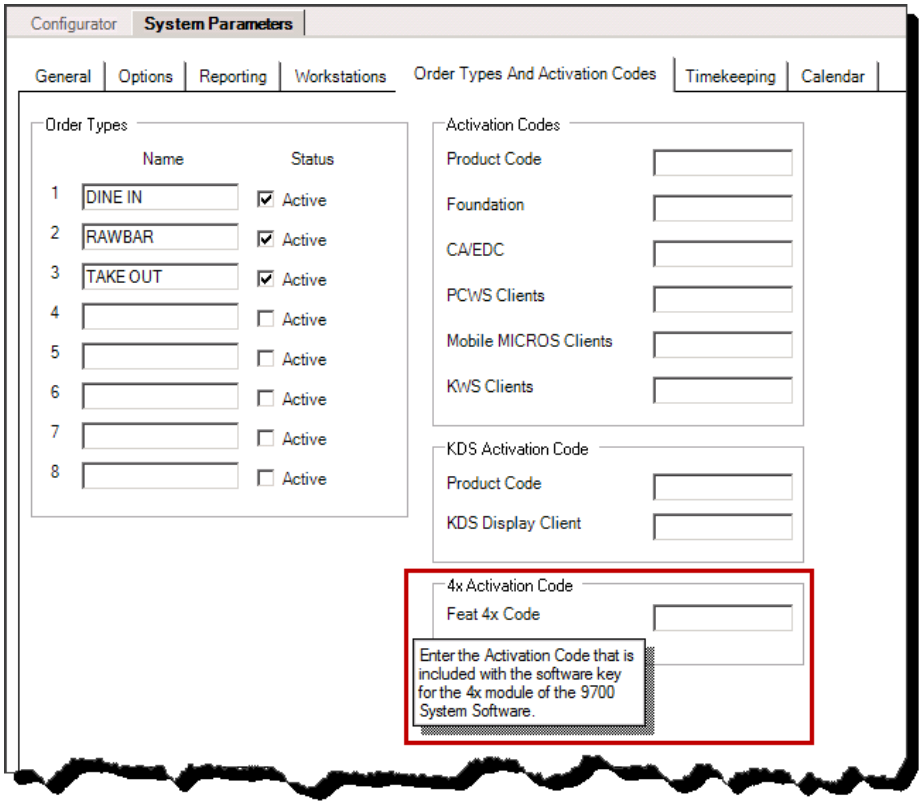
SCR 8002
CR ID# 30350
With this release, KDS v2.1 software has been in integrated into 9700. For those sites that wish to perform an upgrade to 9700 v4.0 and currently utilize KDS devices, note that this will require a platform upgrade to the sites Restaurant Display Controller(s) (RDC). Please refer to the Addendum on page 27 for instructions on how to perform such an upgrade.

EMC

A new 9700 v4.x Activation Code named 'Feat 4x Code' is introduced in the EMC

SCR 8291
CR ID# N/A

With this release, an additional 9700 v4.x License Code field has been added to the EMC-> Configurator-> System Parameters-> Order Types and Activation Codes tab. This code ***must*** be ordered and entered for a 9700 v4.x system to operate for both Keyless and USB key licensing methods. Demo mode will continue to function as in previous versions.



What's Revised

Revisions Summarized

The table below summarizes the revisions included in this version.

Revision	CR ID#	SCR ID#	Page
EMC			
On Oracle® systems, the Remote EMC would not install on a computer running Windows 7 (32-bit)		8002	25
Install			
Uninstalling a remote RMC will cause the remote EMC to no longer work as expected if they're installed on the same machine		8263	26

Revisions Detailed

EMC

On Oracle® systems, the Remote EMC would not install on a computer running Windows 7 (32-bit)

SCR 8002
CR ID# 30350

Previously, at sites running on the Oracle® database platform, upon attempting to install a Remote EMC on a computer running Windows 7 (32-bit), users would receive a "**Unable to detect the ORACLE_HOME location from the registry!"** message. This has been corrected. With this release, a Remote EMC can be successfully installed on computers running Windows 7 at sites running the Oracle® 11g database platform.

Install

Uninstalling a remote RMC will cause the remote EMC to no longer work as expected if they're both installed on the same machine

SCR 8263
CR ID# N/A

On machines that have both a remote RMC and EMC installed, if a user uninstalls the remote RMC, restarts the machine and then attempts to open the remote EMC, they'll receive the following error message:

'**Unable to read translated text file. Could not find part of the path 'C:\etc\EMCText.xml**'

It's been determined that this is working as designed. In order to resolve this issue, users are required to uninstall and reinstall the remote EMC after uninstalling the remote RMC.

Addendum

Upgrading a Restaurant Display Controller (RDC) for KDS v2.1

KDS Controller Update Instructions

Overview

A new version of the Kitchen Display System (KDS) software has been integrated into 9700 HMS v4.0. There are many features in this version of the KDS software, some of which require that a platform update be performed on the Remote Display Controller (RDC) that the KDS client software operates on. By following these instructions, the RDC will be upgraded to the new platform, returned to factory settings and then loaded with the new KDS client. There are two RDC models, and each model has a different platform. The part number on the RDC will indicate which model the unit is. The platform updates can be obtained from the MICROS 'Hardware Portal' site. The version of the RDC Platform Update is 4.2.2.0 and it will be able to automatically identify which model of RDC is being utilized and install the correct files.

- Part Number 700876-200 is the GX model
- Part Number 700876-210 is the LX model

Upgrade Process

Follow these steps to upgrade the operating system to the required platform:

There were two different hardware versions of the RDC and these updates will update either device when encountered. The RDCPlatformUpdate zip File consists of two self extracting zip files that are to be executed on an existing CAL server. The files are:

1. CALClientUpdate(4.1.3.66).exe:

Self extracting zip file that contains the updated CAL Client for both RDC's (GX/LX). This .exe will create the CAL package on the CAL server to deploy the CAL client to the RDC. ClientOSUpdate(4.2.2.0).exe:

Self extracting zip file that contains the updated RDC OS image for both RDC's (GX/LX). This .exe will create the CAL package on the CAL server to deploy the OS Update to the RDC.

How to install the updates

Warning: *It is important that these updates be installed in the order specified below!*

1. Run the CALClientUpdate(4.1.3.66).exe. Note that this version of CAL client is also the version that has been shipping on newer RDC's for the past few years, so you may notice that the CAL package doesn't appear to update some RDC's. This is OK.

2. Run the ClientOSUpdate(4.2.2.0).exe. Each of these CAL packages will reboot the RDC several times during the update. Do ***not*** be alarmed by this behavior.

Revert to Factory Settings

Depending upon the history of the device and what was previously running on it, there could be previous configuration data that can interfere with the new platform and software. To facilitate the best possible upgrade, the unit should be returned to the factory settings prior to loading the new KDS software.

1. Start | Settings | Control Panel | Save Settings

    a. Select the '**Default Settings**' tab

    b. Select the '**Reset to Default Settings**' box

    c. Click '**Yes**'

2. The unit will reboot after resetting the configuration

Set the Correct Date and Time

Set the date and time on the unit to be current. If the date and time on the unit is not close to that of the server, then the Client Application Loader (CAL) software will not work properly. Typically, the Property list will fail to load when these values are not correct.

Configure the IP Address

Set the IP address of the RDC to be a static value that will work on the network. It has been seen that some units will not be able to pick up a DHCP issued IP address after the upgrade. This issue can be worked around by assigning a static IP address to the unit, which the KDS client software requires anyway. The unit does not require DNS or WINS entries. To test the network configuration, open up Internet Explorer on the RDC and enter in the URL to the service that is hosting the CAL server. If this URL can be accessed, the network configured is ready for connecting to the server.

Install the Kitchen Display System Client

The following tips may be helpful:

- If you are typing with a keyboard and nothing is going into the fields, press '**F12**' and try again.
- When selecting the RDC from the list:
    - Ensure that the '**Automatic DHCP Address**' is turned off.
    - Ensure that there are values in the '**Netmask**' and '**Default Gateway**' fields.
    - Ignore the value in '**Select Product to Install on Workstation**' field.