



Password Management



Password Management Guide HMS 9700

Hospitality Management Systems

Purpose of document

In certain cases Micros-Fidelio will return the responsibility of maintaining user passwords, including the passwords, necessary for providing Support, back to the customer.

This may be necessary to comply with Payment Card Industry Data Security Standard (PCI-DSS) and MICROS-Fidelio Support rules.

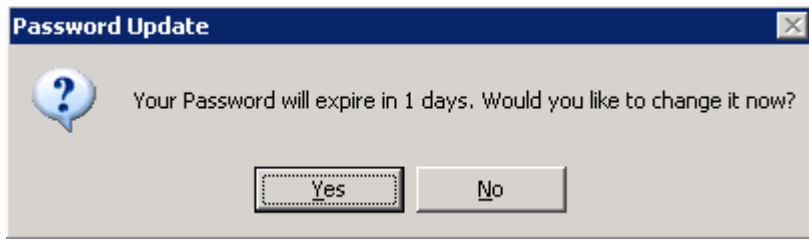
In this paper you find the documentation how to change the passwords, if necessary.

HMS 9700 Application Password

(The below procedures will also change the access password for the reporting tool of HMS 9700)

Changing the password at expiration

- Expiration warning appears, x days before

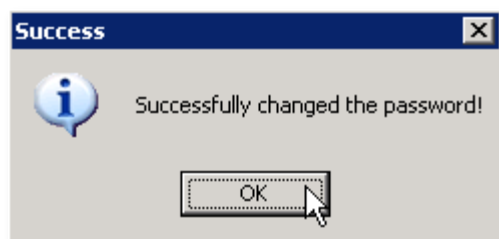


- If you press No, the message will disappear and will ask you again next time opening a backoffice application.
- If you press Yes, the change password screen will appear



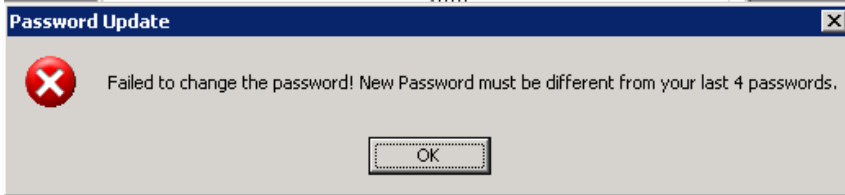
Insert your current password in "Current Password" and insert your new password into the next field and confirm it once.

- If the password has been changed successfully, the following window will appear.



- Following error messages or similar may appear if the password change was not successful.

Password Management Guide

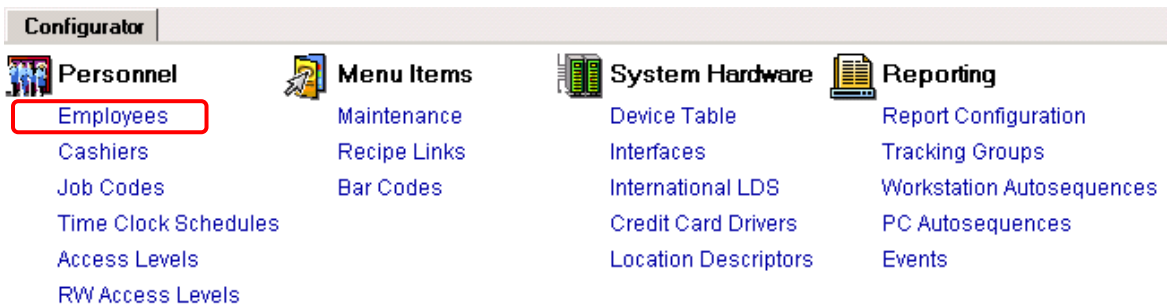


- If so, please press OK and try it again.

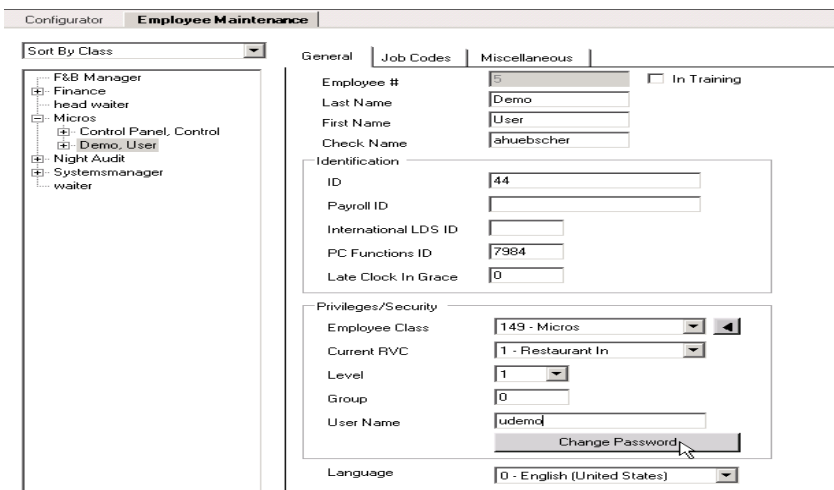
Set new password

- **EMC configuration**

Open Enterprise Management Console (EMC), select Employee Maintenance.

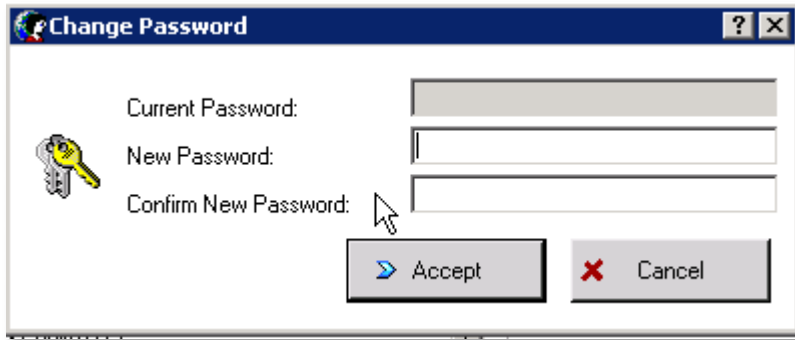


Search for all or for the employee you want to change, double click on the entry you want to change and get into the detail configuration.



Press the button "Password" and the password change dialogue will open.

Password Management Guide

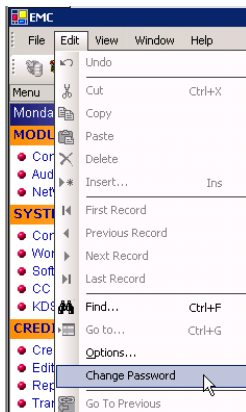


- Type in the new password and confirm the new password. Please note this is only a password which is valid for the next logon, where the employee is forced to change the password.

Changing the password manually

- **EMC configuration**

Open Enterprise Management Console (EMC), select Edit and Change Password.



Security Guidelines

- Each employee with the access to the MICROS applications, should have its own user name and password; Passwords should never be shared.
- In PCI-DSS* compliant systems, passwords have to be changed, at least every 90 days. For not PCI-DSS* compliant system it is recommended as well.
- The passwords must meet strong password rules.
- Maintaining Micros Support user password:
- There should be a support user in the MICROS HMS 9700 System, to ensure the support from MICROS-FIDELIO on 2nd and 3rd level support.
This password of the support user needs to be changed whenever the password has been given to an authorized MICROS-FIDELIO support agent and the agent has finished working on the system.

Access level of Micros Support user:

- Micros Support user should always have access to the whole system and all functions on an administrator level.

Database Passwords

Premise

- HMS 9700 supports 2 different database types: Microsoft SQL Server and Oracle. The change of the passwords are different and therefore there is a section for each database type which describes how the DB user passwords can be changed.
- After changing the DB user passwords it is necessary to change the connection parameters for the HMS 9700 application.
- Before any database passwords can be changed, all existing connections to the database must be disconnected. Therefore all Micros HMS 9700 related service must be stopped. Please open the Command Line and type

```
c:\C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
E:\MICROS\LES\POS\9700>micros ops down y_
```

```
c:\C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
E:\MICROS\LES\POS\9700>micros ops down y
E:\MICROS\LES\POS\9700>micros dbs down y_
```

```
c:\C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
E:\MICROS\LES\POS\9700>micros ops down y
E:\MICROS\LES\POS\9700>micros dbs down y
E:\MICROS\LES\POS\9700>micros stop y_
```

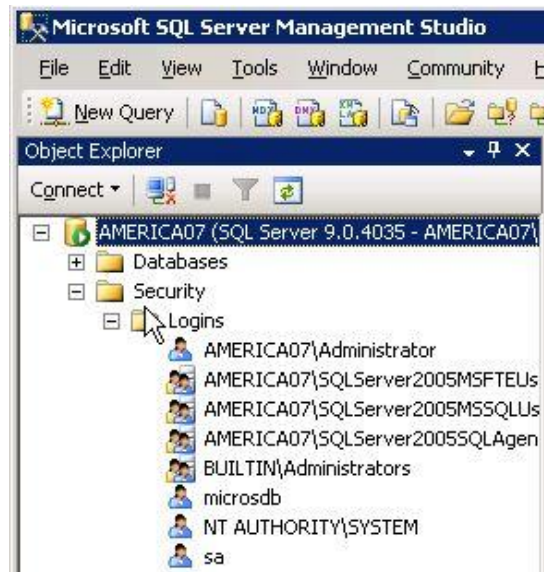
```
c:\Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
D:\MICROS\LES\POS\9700>micros kill all y_
```

Microsoft SQL Server Database Passwords

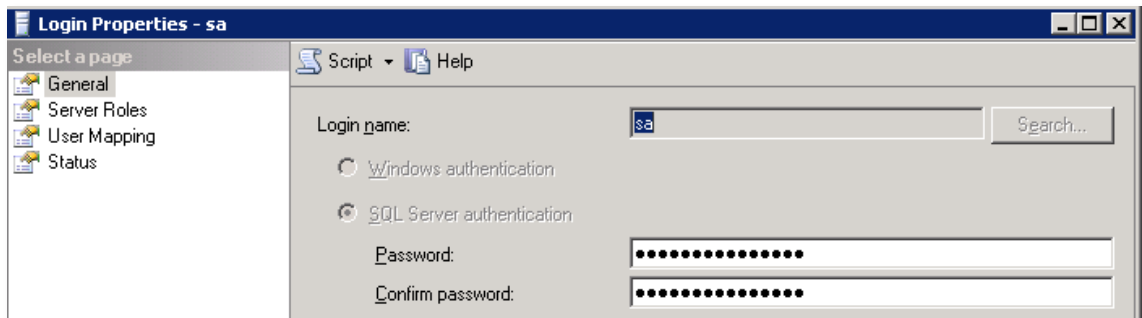
If you are using Oracle, please go to page 7

Changing the database password (1st step for Microsoft MS-SQL):

1. Open the "SQL Server Enterprise Manager". This is usually under "Start"-->"Programs"-->"Microsoft SQL Server".
2. Login with the user sa and the appropriate credentials.
3. Navigate to the "Logins" object under the "Security" folder on the SQL Server you wish to administer. Then, right click on the 'sa' account and select "Properties".



4. Now, enter a new password in the "Password" field under the "General" options.



Please repeat these steps for these MICROS HMS 9700 related users.

- sa
- microsdb

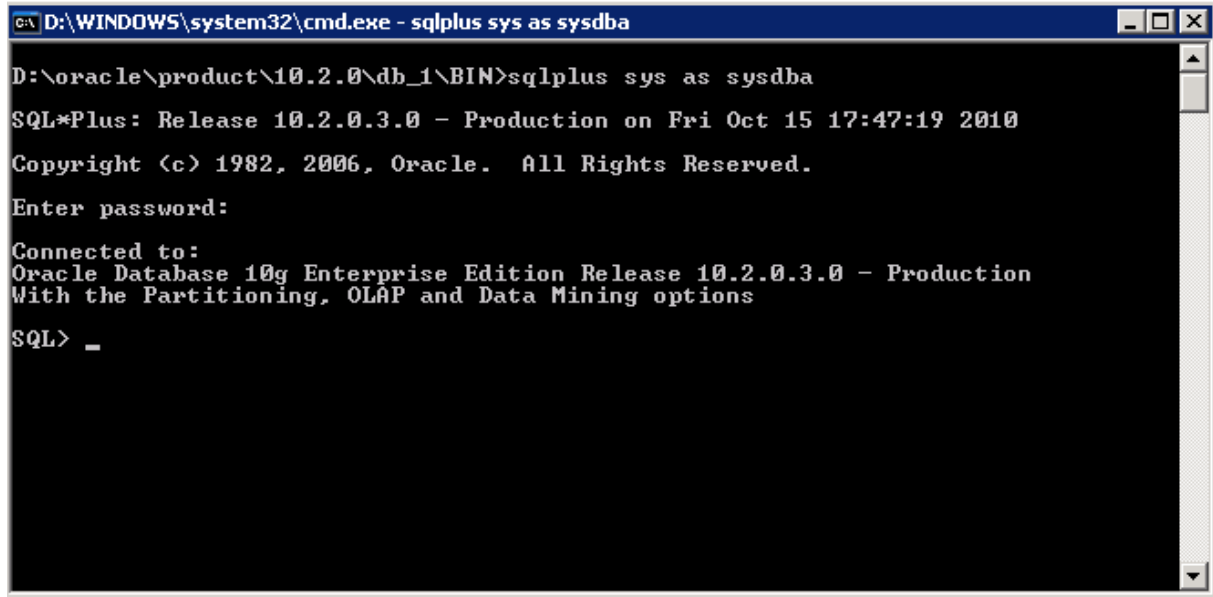
Oracle Database Passwords

If you are using Microsoft SQL Server, please proceed with page 6

Changing the database password (1st step for Oracle):

To change the Password, we need to alter the database for all HMS 9700 related database users existing. (SYS/system/MICROSDB/Location_Activity_DB/Portal/Core/RTA)

- connect to sqlplus as sysdba



```
D:\WINDOWS\system32\cmd.exe - sqlplus sys as sysdba
D:\oracle\product\10.2.0\db_1\BIN>sqlplus sys as sysdba
SQL*Plus: Release 10.2.0.3.0 - Production on Fri Oct 15 17:47:19 2010
Copyright (c) 1982, 2006, Oracle. All Rights Reserved.
Enter password:
Connected to:
Oracle Database 10g Enterprise Edition Release 10.2.0.3.0 - Production
With the Partitioning, OLAP and Data Mining options
SQL> _
```

!Please be absolute sure that by now ALL Database connections have been stopped, please check the premise above!

Run alter command (password equals here XXXX and has to be modified; numbers are mandatory in password, but it is not permitted to start a password with numbers)

System users below:

SYS

SQL> alter user sys identified by XXXX;

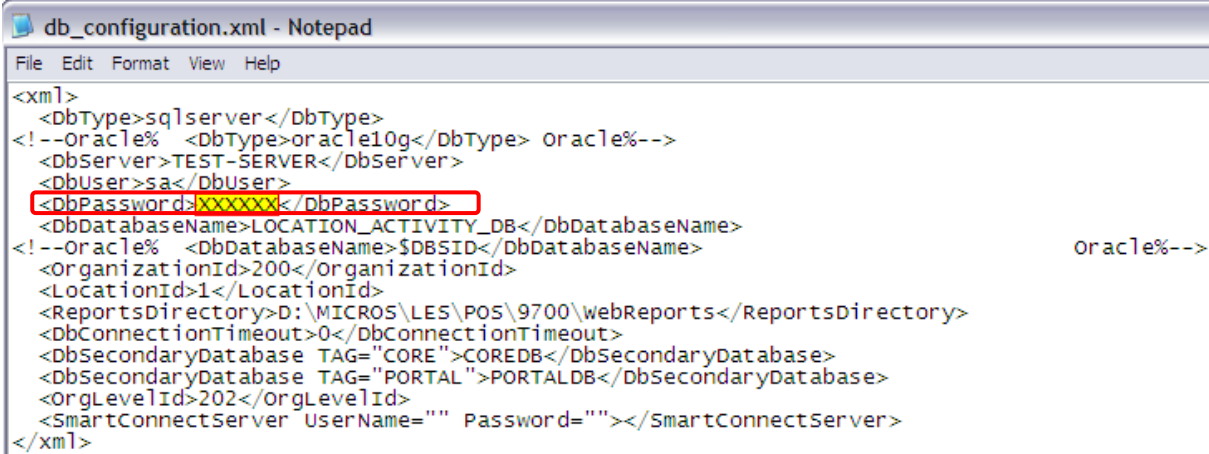
SYSTEM

SQL> alter user sys identified by XXXX;

Please alter the password for all db users used in the HMS 9700 connection strings.

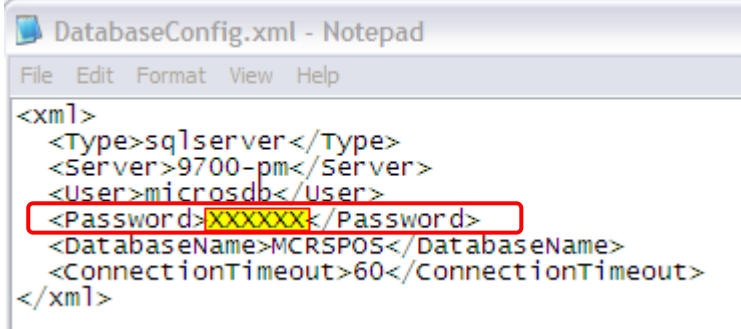
Changing the database connection parameters for the HMS 9700 application (2nd step):

- Open the “Password Change 1.0.X.exe” utility which reads and encrypts the password for the HMS 9700 application.
- Choose your MICROS 9700 Installation Location-Drive
- After the utility opened, please change the password in the db_configuration.xml



```
db_configuration.xml - Notepad
File Edit Format View Help
<xml>
  <DbType>sqlserver</DbType>
  <!--Oracle% <DbType>oracle10g</DbType> Oracle%-->
  <DbServer>TEST-SERVER</DbServer>
  <DbUser>sa</DbUser>
  <DbPassword>XXXXXX</DbPassword>
  <DbDatabaseName>LOCATION_ACTIVITY_DB</DbDatabaseName>
  <!--Oracle% <DbDatabaseName>$DBSID</DbDatabaseName> Oracle%-->
  <OrganizationId>200</OrganizationId>
  <LocationId>1</LocationId>
  <ReportsDirectory>D:\MICROS\LES\POS\9700\webReports</ReportsDirectory>
  <DbConnectionTimeout>0</DbConnectionTimeout>
  <DbSecondaryDatabase TAG="CORE">COREDB</DbSecondaryDatabase>
  <DbSecondaryDatabase TAG="PORTAL">PORTALDB</DbSecondaryDatabase>
  <OrgLevelId>202</OrgLevelId>
  <SmartConnectServer UserName="" Password=""></SmartConnectServer>
</xml>
```

- Set the DbPassword (“XXXXXX”) to your new sa Password
- Please save the db_configuration.xml an close this Notepad
- After the utility opened, please change the password in the DatabaseConfig.xml



```
DatabaseConfig.xml - Notepad
File Edit Format View Help
<xml>
  <Type>sqlserver</Type>
  <Server>9700-pm</Server>
  <User>microsdb</User>
  <Password>XXXXXX</Password>
  <DatabaseName>MCR5POS</DatabaseName>
  <ConnectionTimeout>60</ConnectionTimeout>
</xml>
```

- Set the Password (“XXXXXX”) to your new microsdb Password
- Please save the DatabaseConfig.xml an close this Notepad
- Exit the Password-Change Tool with Finish

Changing the database connection parameters for the NetVupoint Reporting (3rd step):

- Micros Portal Service
- Locate the following file and open the file with notepad.

<drive> :\Micros\NetVuPoint\MyMicrosV4

1. The microsConfig.properties contains the passwords which are used to build the connection to the database.
2. Please check the user name for the
 - db.user= → This is the user for the db.password entry
3. Note the usernames for both users and create encrypted user passwords following the below steps:
4. the sa password is already encrypted (db.password). To encrypt the new password you have to follow these steps:
 - Open cmd shell (Start -> Run -> cmd [Enter])
 - Go to folder <drive>:\Micros\NetVupoint\MyMicrosV4
 - Enter the following command **java -cp ConfigClient.jar com.micros.config.common.CE XXXXXXXXXX (please replace the XXXXXX with the password for the above users**
 - Note down the encrypted password hash
5. Now insert the new encrypted password for the db.user at the line db.password and for the db.user at the line db.password, please see example below

```
## DB Authentication
# Default user name
# [default] db.user=sa

# Default encrypted password
# NOTE: To determine the encrypted value for a password, use the utility embedded bin/ConfigClient.jar with the
# following command line: java -cp bin/ConfigClient.jar com.micros.config.common.CE password
# [default] db.password=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
db.password=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

After all changes have been made, please reboot the server and verify after the restart the following:

- EMC Access works
- Micros workstations operate online and posted revenue appears in the NetVupoint reporting
- Verify you the login into NetVuPoint works.

Security Guidelines

- Normal user should have no access to the database, but the passwords needs to be maintained.
- In PCI-DSS* compliant systems, password for DBA and Micros user have to be changed before first use. For non PCI-DSS* compliant systems it is still recommended to change the default passwords.
- It is recommended, to keep all the passwords secure, but available on request (Responsibility of the manager).

Maintaining Micros Support user password:

- To ensure the support form MICROS-FIDELIO, the passwords of the DBA and the Micros users should be available to hand out to the support representative if necessary.
The password of the database user needs to be changed whenever the password has been given to an authorized MICROS-FIDELIO support agent and the agent has finished working on the system.

Access level of Micros Support agent, if database access is required:

- 1st level support requires no database password.
- 2nd level support may require the Micros user password.
- 3rd level support may require the DBA user password.

Changing Microsoft Windows OS Account Passwords

Domain Accounts:

- On the domain controller use the User Maintenance Tool to change the password. In programs which use the password, such as Backup Exec, amend the configuration with the new password.

Local Accounts:

- Use the Local Users section of the Computer Management Tool to amend the password. In programs which use the password, such as Backup Exec, amend the configuration with the new password.

Password Management Guide

Copyright & Legal Information

© 2010 Micros-Fidelio GmbH. This document is published by Micros-Fidelio GmbH, Europadamm 2-6, 41460 Neuss, Germany. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express prior written consent of the publisher. MICROS-Fidelio GmbH retains the right to update or change the contents of this document without prior notice. MICROS-Fidelio GmbH assumes no responsibility for the contents of this document. Any unauthorized use, distribution or reproduction of this document, in full or in part, is expressly prohibited.

Legal Notice

This document is provided on an 'as is' basis only and MICROS-Fidelio GmbH makes no warranty or representation (whether express or implied) of any kind with regard to this material, including but not limited to the implied warranties of accuracy, reliability, marketability or fitness for a particular purpose. Further, MICROS-Fidelio does not warrant or represent that any of the information contained herein will satisfy the requirements of the Payment Card Industry Data Security Standards. In no event shall Micros-Fidelio be liable for any errors or omissions contained herein and MICROS-Fidelio is not responsible for and accepts no liability whatsoever for any direct, indirect or consequential loss or damages arising from or connected with the furnishing, performance or the use of this information.

About MICROS-Fidelio

Serving the hospitality and speciality retail industries, we are the world's leading developer of enterprise applications. Our global presence and local support have helped us build a long list of references – hotels, restaurants, conference centres, retail, stadiums, theme parks, casinos and cruise ships. We maintain an intense dialogue with colleagues throughout these industries. The result is a wide range of integrated software, hardware and business technology solutions and services. These help to optimise your operation and increase profits by providing your guests with a personalised service.

MICROS-FIDELIO GmbH

Europadamm 2-6
41460 Neuss
Germany
Phone: +49-(0)2131-137 0
Fax: +49-(0)2131-137 777

www.micros-fidelio.eu

micros® and micros-fidelio® are registered trademarks of MICROS Systems, Inc. Certain product and company names appearing here may be the trademarks or service marks owned and/or registered by third parties. All other product and brand names are the property of their respective owners.

© Copyright 2010 MICROS Systems, Inc. All rights reserved.