CISP Compliance and PCI Data Security Standard Adherence

according to the Payment Application-Data Security Standard

Version 1.2

This document has been prepared by MICROS-Fidelio (Ireland) Ltd. and is available to a select group of individuals for informational purposes. This is a confidential document that contains concepts, methods and other proprietary information. Readers are to treat the information herein as confidential.

Information in this document is subject to change without notice.

MICROS-Fidelio (Ireland) Ltd. makes no warranty of any kind with regard to this material, including but not limited to the implied warranties of marketability and fitness for a particular purpose.

MICROS-Fidelio (Ireland) Ltd. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Author:
V8 Development Team

Printed in Germany

MICROS-Fidelio (Ireland) Ltd.
Europadamm 2-6
41460 Neuss
Germany

Tel: +49 2131 137 0
Fax: +49 2131 137 464

Document Change History

Version	Date	Change
Version 8.8	11 May 2009	Initial version (FV)
Version 8.8.0.1	2 June 2009	Smaller corrections (FV)
Verin 8.8.0.1	15 June 2009	Smaller corrections (FV)

Table of Contents

General Information

About This Document

This document is intended as a quick reference guide to provide users with information concerning MICROS-Fidelio's adherence to the Visa USA PCI Data Security Standard concerning CISP compliance and MICROS-Fidelio's adherence to the PCI PA-DSS Data Security standard issued by the PCI Security Standards Council. This document relates specifically to MICROS-Fidelio SUITE8 Version 8.8 Hotel Management Solution software.

About CISP Compliance

When customers offer their bankcard at the point of sale, over the Internet, on the phone, or via mail, they want to ensure that their account information is safe. That's why Visa USA and VISA Europe have implemented the Cardholder Information Security Program (CISP). Mandated since June 2001, the program is designed to protect Visa cardholder data—wherever it resides—ensuring that members, merchants, and service providers maintain the highest information security standard 1.

For more detailed information concerning CISP compliance, please refer to the Visa USA CISP website:

http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html?it=searchQuicklink

or to the Visa Europe CISP website:

http://www.visaeurope.com/acceptingvisa/securitystandard.html[1]

About The PCI Data Security Standard

CISP compliance is required of all merchants and service providers that store, process, or transmit Visa cardholder data. The program applies to all payment channels, including retail (brick-and-mortar), mail/telephone order, and ecommerce. To achieve compliance with CISP, merchants and service providers must adhere to the Payment Card Industry (PCI DSS) Data Security Standard, which offers a single approach to safeguarding sensitive data for all card brands. This Standard is a result of collaboration between Visa, MasterCard, AMEX, Discover, and JCB, and is designed to create common industry security requirements, incorporating the CISP requirements. Other card companies operating in the U.S. have also endorsed the PCI Data Security Standard within their respective programs. Using the PCI Data Security Standard as its framework, CISP provides the tools and measurements needed to protect against cardholder data exposure and compromise across the entire payment industry. The PCI Data Security Standard, seen below, consists of twelve basic requirements supported by more detailed sub-requirements:

[1] Reprinted from Cardholder Information Security Program http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html?it=searchQuicklink

*The **Payment Card Industry (PCI) Data Security Standard** is a result of a collaboration between Visa, MasterCard, AMEX, Discover, and JCB to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. These 12 requirements are the foundation of Visa's CISP.*

PCI Data Security Standard

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data

2. Do not use vendor supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored data

4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software

6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know

8. Assign a unique ID to each person with computer access

9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data

11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

Audiences for this document

This document is intended for the following audiences:

- Suite8 Customers
- SUITE8 Installers/Programmers
- SUITE8 Dealers
- SUITE8 Customer Service
- SUITE8 Training Personnel
- MIS Personnel

Readers knowledge

This document assumes that you have the following knowledge or expertise:

- Operational understanding of PCs
- Understanding of basic network concepts
- Experience with the operating systems platforms supported bySuite8
- Familiarity with the SUITE8 PMS software
- Familiarity with operating MICROS-Fidelio's peripheral devices

Fidelio Suite 8 version 8.8 and the PCI Data Standard

PCI Data Security Standard

While MICROS-Fidelio (Ireland) Ltd. recognizes the importance of upholding card member security and data integrity, certain parameters of the PCI Data Security Standard and CISP compliance are at the responsibility of the client. This section contains a description of the 12 points of the PCI Data Security Standard. Information within this section refers to how the Fidelio Suite8 Version 8.8 software conforms to the PCI Data Security Standard.

For a complete description of the PCI Data Security Standard, please consult Visa USA's website **Cardholder Information Security Program** found at http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data

Firewalls are computer devices that control computer traffic allowed into a company's network from outside, as well as traffic into more sensitive areas within a company's internal network. All systems need to be protected from unauthorized access from the Internet, whether for e-commerce, employees' Internet-based access via desktop browsers, or employees' email access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.[2]

MICRO-Fidelio GmbH strongly recommends that all systems containing sensitive information (servers, databases, wireless access points, etc.) reside behind a firewall in order to protect that data as well as meet Visa CISP Security Standards.

To make sure your firewall configuration is set up in compliance with Step 1 of the PCI Data Security Standard: **Install and maintain a firewall configuration to protect data**, please consult Visa USA's website:
Cardholder Information Security Program, <http://usa.visa.com/ business/accepting_visa/ops_risk_management/cisp.html>

2. Do not use vendor-supplied defaults for system passwords and other security parameters

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.[3]

MICRO-Fidelio GmbH. recommends that customers change all default passwords when installing systems, including those for operating systems, wireless access points, servers, databases, etc. Suite8 provides two default accounts for which the passwords should be changed to meet the CISP complex password requirements; they are SUPERVISOR in the application and V8 in the database.

For more information on Step 2 of The PCI Data Security Standard, 'Do not use vendor-supplied defaults for system passwords and other security parameters', please consult Visa USA's website,

Cardholder Information Security Program, <http://usa.visa.com/ business/accepting_visa/ops_risk_management/cisp.html>

[2] "Payment Card Industry Standard Audit Procedures.doc", p. 5, V. 1.0, December 15, 2004.<http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c| / business/accepting_visa/ops_risk_management/ cisp%2Ehtml|View%20all%20CISP%20downloads>.

[3] "Payment Card Industry Security Audit Procedures.doc", p. 10, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/ cisp%2Ehtml|View%20all%20CISP%20downloads>.

Protect Cardholder Data

3. Protect stored data

Encryption is the ultimate protection mechanism because even if someone breaks through all other protection mechanisms and gains access to encrypted data, they will not be able to read the data without further breaking the encryption. This is an illustration of the defense in depth principle.[4]

MICROS-Fidelio (Ireland) Ltd. uses credit card masking and Triple-DES 192-bit encryption to ensure credit card data is stored in a manner compliant with the PCI Data Standard. The database server should always sit behind a firewall for protection from malicious Internet attacks.

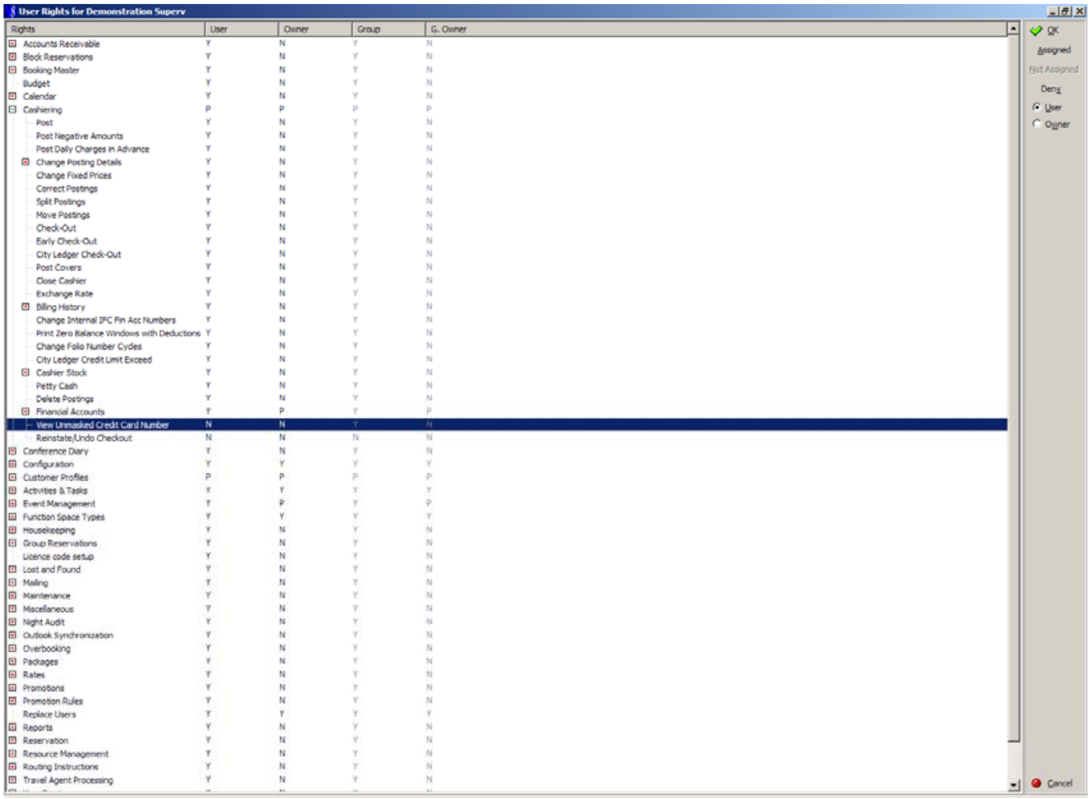
For more information on Step 3 of The PCI Data Security Standard, **Protect stored data**, please consult Visa USA's website,

Cardholder Information Security Program, <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>

[4] "Payment Card Industry Security Audit Procedures.doc", p. 13, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/ cisp%2Ehtml|View%20all%20CISP%20downloads>.

To be in compliance with Step 3 of the PCI Data Security Standard, please ensure the following right for **Credit Card Masking** is configured as follows:

USERRIGHTS\CASHIERING -> *View Unmasked Credit Card Number* = **N**



User Rights for Demonstration Superv

Rights	User	Owner	Group	G. Owner
⊞ Accounts Receivable	Y	N	Y	N
⊞ Block Reservations	Y	N	Y	N
⊞ Booking Master	Y	N	Y	N
Budget	Y	N	Y	N
⊞ Calendar	Y	N	Y	N
⊟ Cashiering	P	P	P	P
Post	Y	N	Y	N
Post Negative Amounts	Y	N	Y	N
Post Daily Charges in Advance	Y	N	Y	N
⊞ Change Posting Details	Y	N	Y	N
Change Fixed Prices	Y	N	Y	N
Correct Postings	Y	N	Y	N
Split Postings	Y	N	Y	N
Move Postings	Y	N	Y	N
Check-Out	Y	N	Y	N
Early Check-Out	Y	N	Y	N
City Ledger Check-Out	Y	N	Y	N
Post Covers	Y	N	Y	N
Close Cashier	Y	N	Y	N
Exchange Rate	Y	N	Y	N
⊞ Billing History	Y	N	Y	N
Change Internal IFC Fin Acc Numbers	Y	N	Y	N
Print Zero Balance Windows with Deductions	Y	N	Y	N
Change Folio Number Cycles	Y	N	Y	N
City Ledger Credit Limit Exceed	Y	N	Y	N
⊞ Cashier Stock	Y	N	Y	N
Petty Cash	Y	N	Y	N
Delete Postings	Y	N	Y	N
⊞ Financial Accounts	Y	P	Y	P
View Unmasked Credit Card Number	N	N	Y	N
Reinstate/Undo Checkout	N	N	N	N
⊞ Conference Diary	Y	N	Y	N
⊞ Configuration	Y	Y	Y	Y
⊞ Customer Profiles	P	P	P	P
⊞ Activities & Tasks	Y	Y	Y	Y
⊞ Event Management	Y	P	Y	P
⊞ Function Space Types	Y	Y	Y	Y
⊞ Housekeeping	Y	N	Y	N
⊞ Group Reservations	Y	N	Y	N
Licence code setup	Y	N	Y	N
⊞ Lost and Found	Y	N	Y	N
⊞ Mailing	Y	N	Y	N
⊞ Maintenance	Y	N	Y	N
⊞ Miscellaneous	Y	N	Y	N
⊞ Night Audit	Y	N	Y	N
⊞ Outlook Synchronization	Y	N	Y	N
⊞ Overbooking	Y	N	Y	N
⊞ Packages	Y	N	Y	N
⊞ Rates	Y	N	Y	N
⊞ Promotions	Y	N	Y	N
⊞ Promotion Rules	Y	N	Y	N
Replace Users	Y	Y	Y	Y
⊞ Reports	Y	N	Y	N
⊞ Reservation	Y	N	Y	N
⊞ Resource Management	Y	N	Y	N
⊞ Routing Instructions	Y	N	Y	N
⊞ Travel Agent Processing	Y	N	Y	N

Note: The above may not apply to employees and other parties with a specific need to see full credit card numbers.

***Note** This option must remain configured as shown above, in order to comply with Requirement 3 of The PCI Data Security Standard.*

4. Encrypt transmission of cardholder data and sensitive information across public networks

Sensitive information must be encrypted during transmission over the Internet, because it is easy and common for a hacker to intercept and/or divert data while in transit. [5]

MICROS-Fidelio (Ireland) Ltd. uses Triple-DES 128-bit encryption to ensure credit card data is transmitted across private networks in a manner compliant with the PCI Data Security Standard.

SUITE8 has no design to send sensitive data over public networks.

MICROS-Fidelio (Ireland) Ltd. strongly recommends each site use some sort of encryption (VPN, SSL, etc) when sending any sensitive information over the Internet, including wireless connections, E-mail, and when using services such as Telnet, FTP, etc.

For more information on Step 4 of The PCI Data Security Standard, ‘Encrypt transmission of cardholder data and sensitive information across public networks’, please consult Visa USA’s website,

Cardholder Information Security Program, <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>

[5] “Payment Card Industry Security Audit Procedures.doc”, p. 18, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/ cisp%2Ehtml|View%20all%20CISP%20downloads>.

Maintain a Vulnerability Management Program

5. Encrypt transmission of cardholder data and sensitive information across

Many vulnerabilities and malicious viruses enter the network via employees'email activities. Anti-virus software must be used on all email systems and desktops to protect systems from malicious software.[6]

In accordance with the Visa USA PCI Data Security Standard, MICROS-Fidelio (Ireland) Ltd., strongly recommends regular use and regular updates of anti-virus software. Some Suite8 servers may require specific antivirus configuration settings; these settings are detailed in the implementation instructions.

To make sure your anti-virus software is set up in compliance with Step 5 of the PCI Data Security Standard, **Use and regularly update anti-virus software**, please consult Visa USA's website,

Cardholder Information Security Program, <http://usa.visa.com/ business/accepting_visa/ops_risk_management/cisp.html>

[6] "Payment Card Industry Security Audit Procedures.doc", p. 20, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/ cisp%2Ehtml|View%20all%20CISP%20downloads>.

6. Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed via vendor security patches, and all systems should have current software patches to protect against exploitation by employees, external hackers, and viruses. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.[7]

MICROS Systems Inc., uses separate development and production environments to ensure software integrity and security. Updated patches and security updates are available via the the SUITE FTP-Server, <ftp.v8.myfidelio.com> and your local support office.

To make sure your site develops and maintains secure systems and applications in compliance with Step 6 of The PCI Data Security Standard, **Develop and Maintain Secure Systems and Applications**, please consult Visa USA's website, Cardholder Information Security Program, <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>

[7] "Payment Card Industry Security Audit Procedures.doc", p. 21, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/ cisp%2Ehtml|View%20all%20CISP%20downloads>.

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know

This ensures critical data can only be accessed in an authorized manner.[8]

MICROS-Fidelio (Ireland) Ltd., recognizes the importance of data control, and does so by establishing access based upon employee job level. This mechanism ensures access to sensitive information is restricted, password protected, and based on a need-to-know basis.

For more information on Step 7 of The PCI Data Security Standard, 'Restrict access to data by business need-to-know', please consult Visa USA's website, "Cardholder Information Security Program", <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>

8. Assign a unique ID to each person with computer access

This ensures that actions taken on critical data and systems are performed by and can be traced to, known and authorized users.[9]

MICROS-Fidelio (Ireland) Ltd. recognizes the importance of establishing unique ID's for each person with computer access. No two SUITE8 users can have the same ID, and each person's activities can be traced provided the client site maintains proper configuration and adheres to privilege level restrictions based on a need-to-know basis. While MICROS-Fidelio (Ireland) Ltd. makes every possible effort to conform to Step 8 of the PCI Data Security Standard, certain parameters, including proper user authentication, remote network access, and password management for non-consumer users and administrators, for all system components, depend on site specific protocol and practices. To ensure strict access control of the SUITE8 PMS, always assign unique usernames and complex passwords to each account. MICROS-Fidelio (Ireland) Ltd. strongly recommends applying these guidelines to not only SUITE8 passwords, but to Windows passwords as well.

Note: 2 factor authentication is required for remote access in order to meet PCI compliance.
To be in compliance with Requirement 8 of the PCI Data Security Standard, we recommend that customers follow these guidelines.

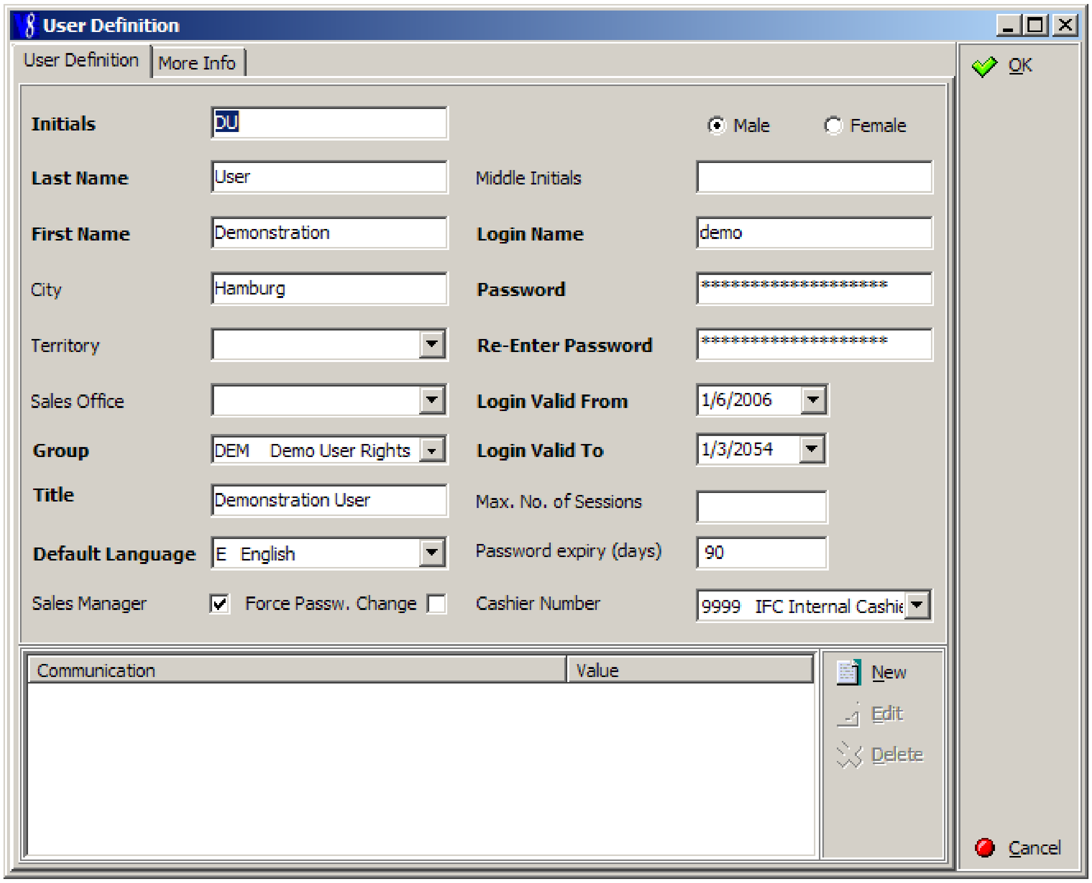
- Ensure 'Password Expiration Days' set on the Edit User screen is not greater than 90.

[8] "Payment Card Industry Security Audit Procedures.doc", p. 26, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/cisp%2Ehtml|View%20all%20CISP%20downloads>.

[9] **Payment Card Industry Security Audit Procedures.doc**, p. 27, V. 1.0, December 15, 2004. http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=l2|/business/accepting_visa/ops_risk_management/cisp.html|Tools%20and%20FAQ

- Ensure that user passwords are at least 7 characters in length.
- Ensure that user passwords include alphabetic and numeric characters.

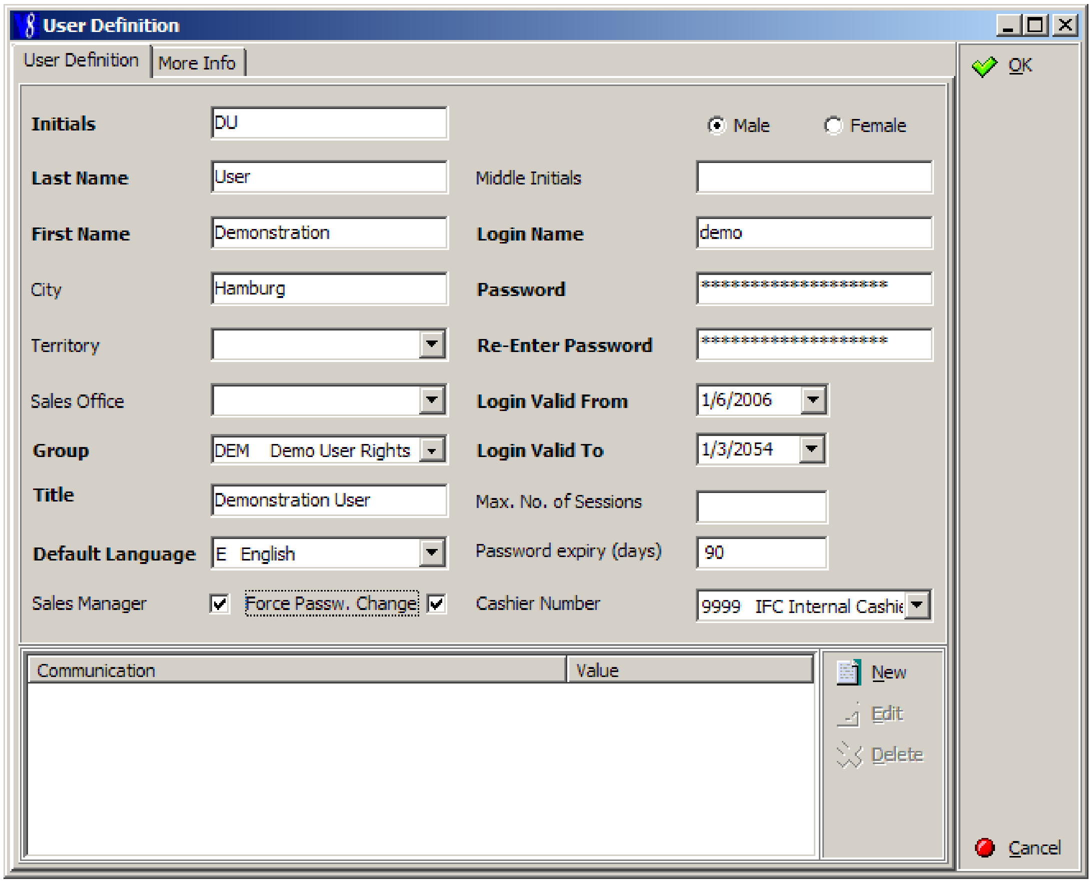
For more information on Requirement 8 of the PCI Data Security Standard, ‘Assign a unique ID to each person with computer access’, please consult Visa USA’s website, ‘Cardholder Information Security Policy’, <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>.



Initials	DU	● Male	○ Female
Last Name	User	Middle Initials	
First Name	Demonstration	**Login Name**	demo
City	Hamburg	**Password**	********************
Territory		**Re-Enter Password**	********************
Sales Office		**Login Valid From**	1/6/2006
Group	DEM Demo User Rights	**Login Valid To**	1/3/2054
Title	Demonstration User	Max. No. of Sessions	
Default Language	E English	Password expiry (days)	90
Sales Manager	☑ Force Passw. Change □	Cashier Number	9999 IFC Internal Cashie

Communication	Value

Set the password expiry to a maximum of 90 days.

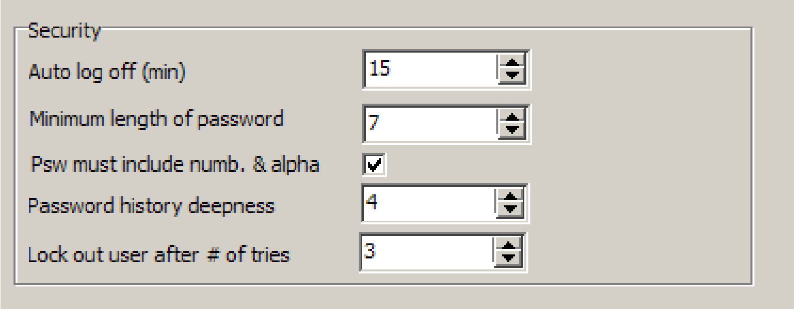


Initials	DU		● Male ○ Female
Last Name	User	Middle Initials	
First Name	Demonstration	**Login Name**	demo
City	Hamburg	**Password**	********************
Territory		**Re-Enter Password**	********************
Sales Office		**Login Valid From**	1/6/2006
Group	DEM Demo User Rights	**Login Valid To**	1/3/2054
Title	Demonstration User	Max. No. of Sessions	
Default Language	E English	Password expiry (days)	90
Sales Manager	☑ Force Passw. Change ☑	Cashier Number	9999 IFC Internal Cashie

Communication	Value

Force a password change for every new user which is added to the system, so that the user needs to apply a new password upon first login.

CONFIGURATION\GLOBAL SETTINGS\GENERIC3



Security

Auto log off (min)	15
Minimum length of password	7
Psw must include numb. & alpha	☑
Password history deepness	4
Lock out user after # of tries	3

- Set Auto-Log-Off to 3 minutes
- Set minimum password length to 7 characters
- Define that passwords need to include numeric and alpha values
- Keep a password history of minimum 4 levels deep
- Define that users are locked after 3 unsuccessful login attempts

9. Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data allows the opportunity to access devices or data, and remove systems or hardcopies, and should be appropriately restricted.[10]

In accordance with the Visa USA PCI Data Security Standard, MICROS-Fidelio (Ireland) Ltd. strongly recommends restricting physical access to cardholder data.

To make sure your site is set up in compliance with Step 9 of The PCI Data Security Standard, **Restrict physical access to cardholder data**, please consult Visa USA's website,
Cardholder Information Security Program, <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>

[10] **Payment Card Industry Security Audit Procedures.doc**, p. 33, V. 1.0, December 15, 2004. http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=l2|/business/accepting_visa/ops_risk_management/cisp.html|Tools%20and%20FAQ

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.[11]

MICROS-Fidelio (Ireland) Ltd. provides a comprehensive audit trail utility, within the SUITE8 system, that allows privileged users to track SUITE8 specific activities. The advent of open database structure means that anyone with system level access to the database server (Oracle) has access to system components covered under this requirement, and thus would require logging of user access and activity as detailed in Step 10 of the PCI Data Security Standard. MICROS-Fidelio (Ireland) Ltd. strongly recommends the database server not be web-accessible.

To make sure your site is in compliance with Step 10 of The PCI Data Security Standard, **Track and monitor all access to network resources and cardholder data**, please consult Visa USA's website, Cardholder Information Security Program, <http://usa.visa.com/ business/accepting_visa/ops_risk_management/cisp.html>

11. Regularly test security systems and processes

Vulnerabilities are continually being discovered by hackers/researchers and introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is being maintained over time and through changes.[12]

In accordance with the Visa USA PCI Data Security Standard, MICROS-Fidelio (Ireland) Ltd. strongly recommends regular testing of security systems and processes.

To make sure your site's security systems and processes are setup in compliance with Step 11 of The PCI Data Security Standard, **Regularly test security systems and processes**, please consult Visa USA's Web site, Cardholder Information Security Program, <http://usa.visa.com/ business/accepting_visa/ops_risk_management/cisp.html>

[11] "Payment Card Industry Security Audit Procedures.doc", p. 37, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/cisp%2Ehtml|View%20all%20CISP%20downloads>.

[12] "Payment Card Industry Security Audit Procedures.doc", p. 41, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/cisp%2Ehtml|View%20all%20CISP%20downloads>.

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

A strong security policy sets the security tone for the whole company, and lets employees know what is expected of them. All employees should be aware of the sensitivity of the data and their responsibilities for protecting it.[13]

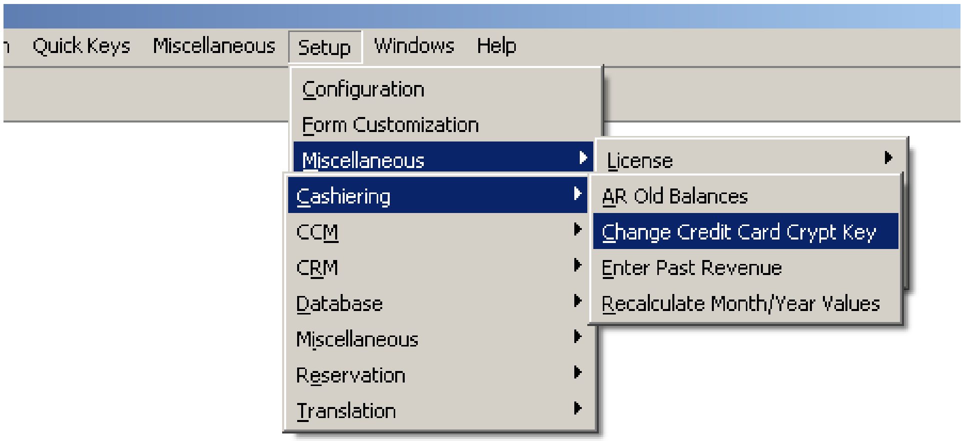
In accordance with the Visa USA PCI Data Security Standard, MICROS-Fidelio (Ireland) Ltd. strongly recommends maintaining a policy that addresses information security.

To make sure your information security policy is setup in compliance with Step 12 of The PCI Data Security Standard, **Maintain a policy that addresses information security**, please consult Visa USA's Web site, Cardholder Information Security Program, <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>

[13] "Payment Card Industry Security Audit Procedures.doc", p. 44, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/cisp%2Ehtml|View%20all%20CISP%20downloads>.

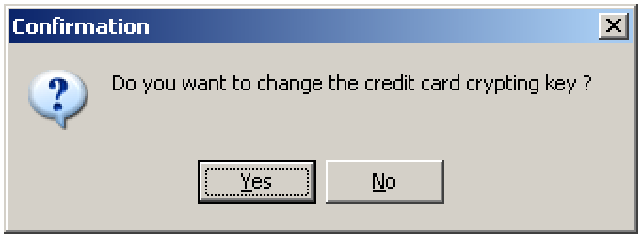
Security in Fidelio Suite 8

Security at database level

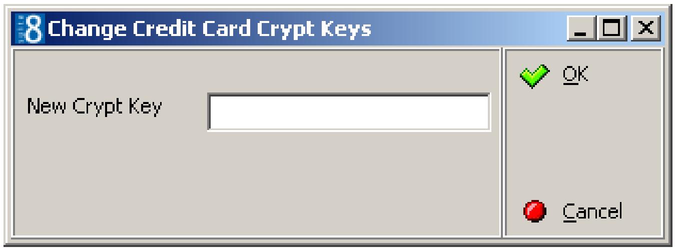


A maintenance option has been added to Suite 8 which will check the database for unencrypted credit card number entries from very old Suite 8 versions and will encrypt all these.

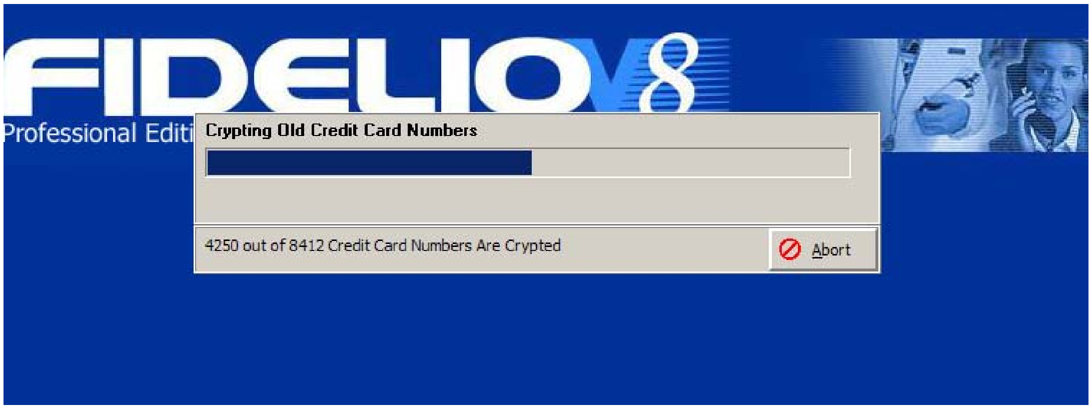
This option can as well be used to re-encrypt all credit card numbers in the database with a different key.



Do you want to change the credit card crypting key ?



A part of the key which is used for encrypting sensitive data is an Encryption key which needs to be entered by the user. This key can be changed at any time. Changing the key will result in re-encryption of all sensitive data in the database.

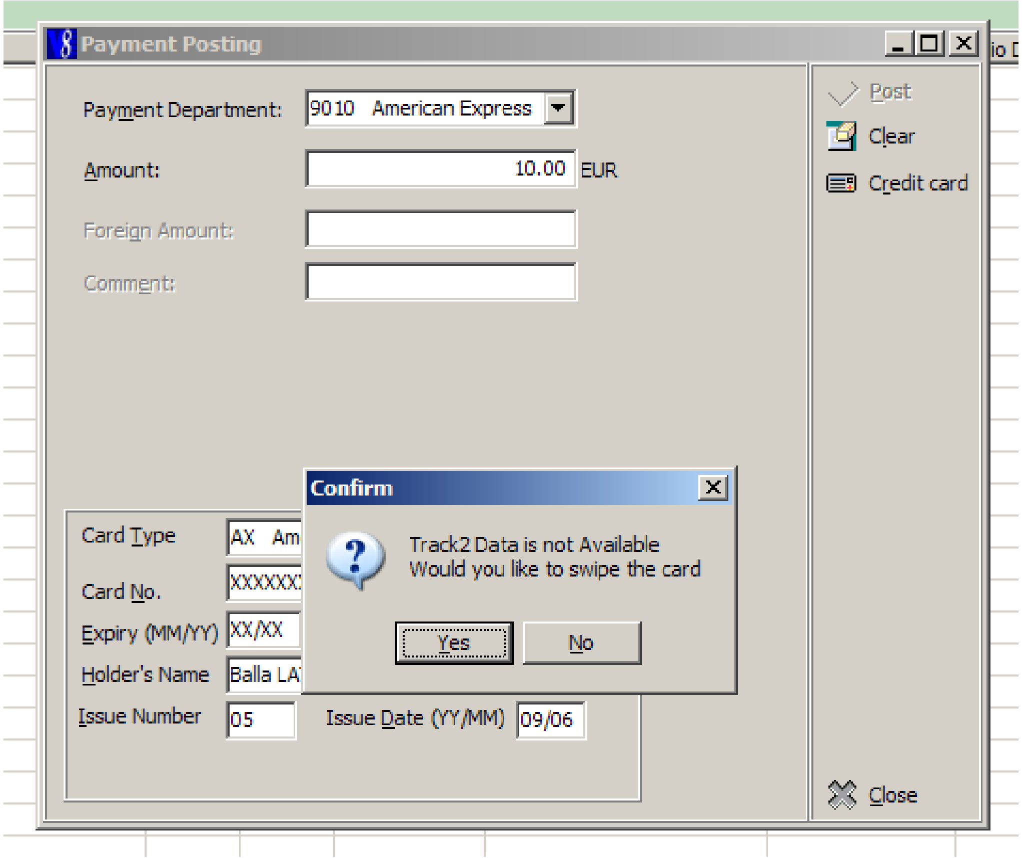


4250 out of 8412 Credit Card Numbers Are Crypted

The key must be changed at least annually; Micros-Fidelio recommended to do this more frequently.

Security for sensitive creditcard data (Track2)

Track2 data is read from a card when swiped but will never be stored and is subsequently not available for further transactions.
The user will be prompted to swipe the card again, if applicable:



Payment Posting

Payment Department: 9010 American Express

Amount: 10.00 EUR

Foreign Amount:

Comment:

Card Type AX Am

Card No. XXXXXX

Expiry (MM/YY) XX/XX

Holder's Name Balla LA

Issue Number 05

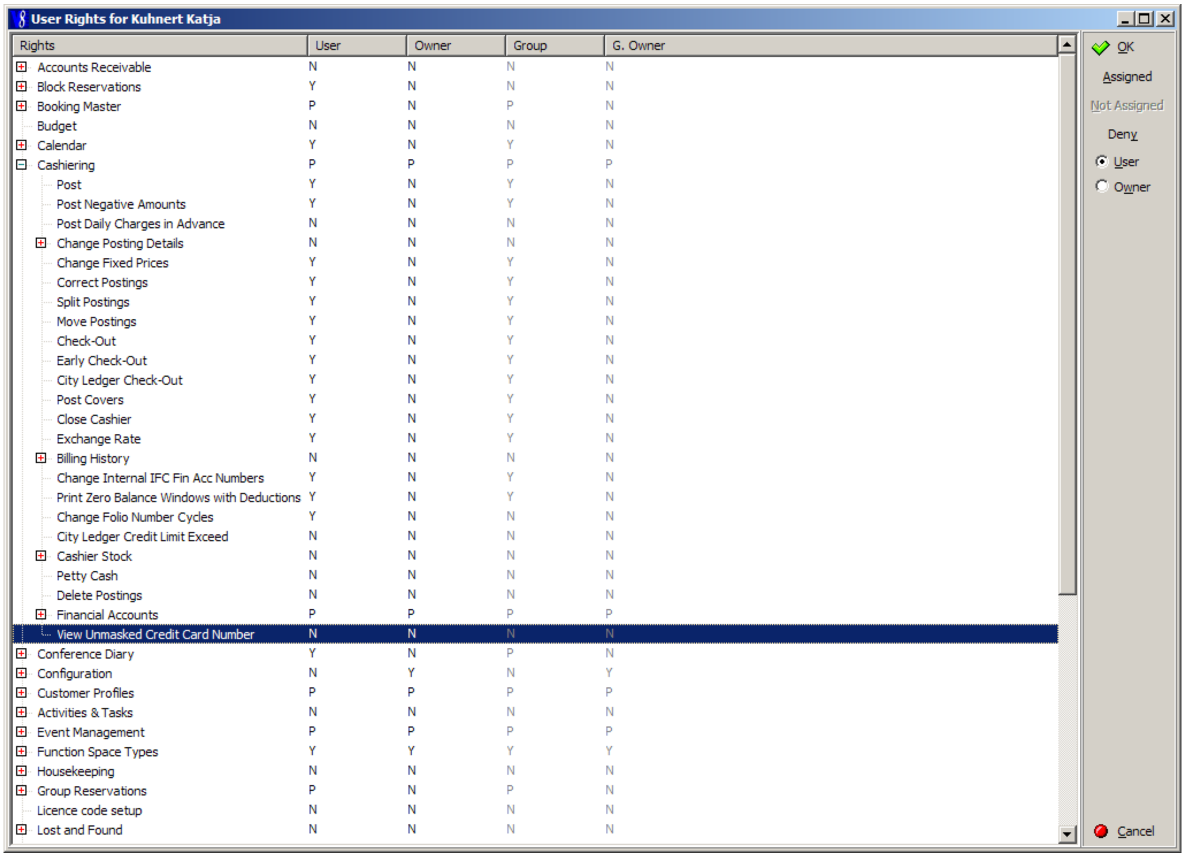
Issue Date (YY/MM) 09/06

Confirm

Track2 Data is not Available
Would you like to swipe the card

Security at user level

A user right has been added which defines, if a user may see the full guest credit card number or not:

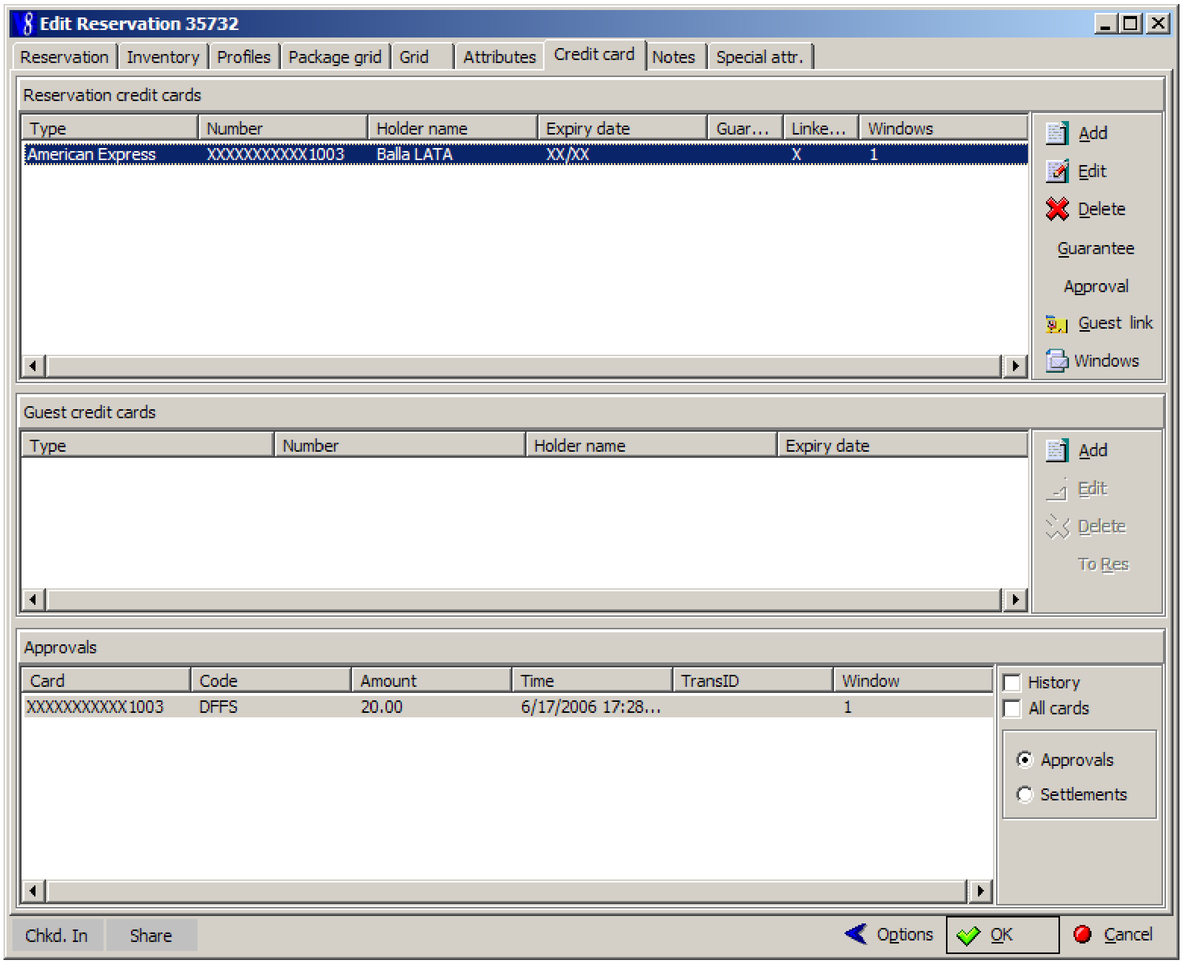


User Rights for Kuhnert Katja

Rights	User	Owner	Group	G. Owner
⊞ Accounts Receivable	N	N	N	N
⊞ Block Reservations	Y	N	N	N
⊞ Booking Master	P	N	P	N
Budget	N	N	N	N
⊞ Calendar	Y	N	Y	N
⊟ Cashiering	P	P	P	P
Post	Y	N	Y	N
Post Negative Amounts	Y	N	Y	N
Post Daily Charges in Advance	N	N	N	N
⊞ Change Posting Details	N	N	N	N
Change Fixed Prices	Y	N	Y	N
Correct Postings	Y	N	Y	N
Split Postings	Y	N	Y	N
Move Postings	Y	N	Y	N
Check-Out	Y	N	Y	N
Early Check-Out	Y	N	Y	N
City Ledger Check-Out	Y	N	Y	N
Post Covers	Y	N	Y	N
Close Cashier	Y	N	Y	N
Exchange Rate	Y	N	Y	N
⊞ Billing History	N	N	N	N
Change Internal IFC Fin Acc Numbers	Y	N	Y	N
Print Zero Balance Windows with Deductions	Y	N	Y	N
Change Folio Number Cycles	Y	N	N	N
City Ledger Credit Limit Exceed	N	N	N	N
⊞ Cashier Stock	N	N	N	N
Petty Cash	N	N	N	N
Delete Postings	N	N	N	N
⊞ Financial Accounts	P	P	P	P
View Unmasked Credit Card Number	N	N	N	N
⊞ Conference Diary	Y	N	P	N
⊞ Configuration	N	Y	N	Y
⊞ Customer Profiles	P	P	P	P
⊞ Activities & Tasks	N	N	N	N
⊞ Event Management	P	P	P	P
⊞ Function Space Types	Y	Y	Y	Y
⊞ Housekeeping	N	N	N	N
⊞ Group Reservations	P	N	P	N
Licence code setup	N	N	N	N
⊞ Lost and Found	N	N	N	N

Users not assigned to this right will only see the last four digits of a card number on all dialog boxes:

Reservation:



Reservation credit cards

Type	Number	Holder name	Expiry date	Guar...	Linke...	Windows
American Express	XXXXXXXXXXX1003	Balla LATA	XX/XX		X	1

Guest credit cards

Type	Number	Holder name	Expiry date

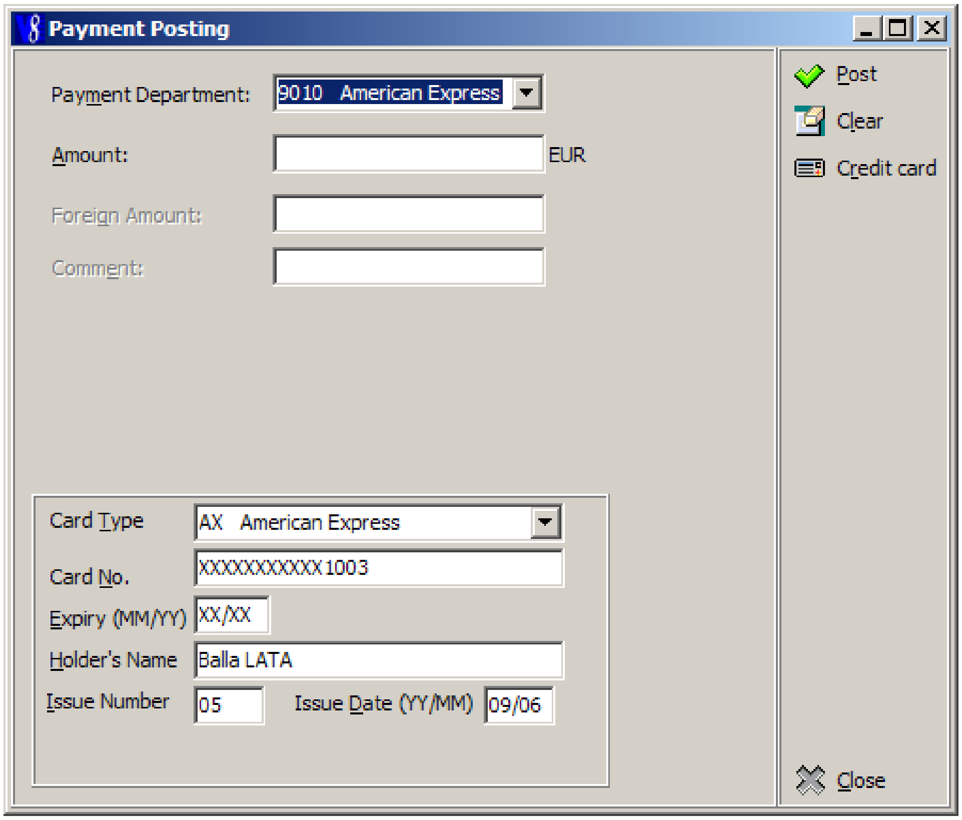
Approvals

Card	Code	Amount	Time	TransID	Window
XXXXXXXXXXX1003	DFFS	20.00	6/17/2006 17:28...		1

□ History
□ All cards

● Approvals
○ Settlements

Payment:



Payment Department: 9010 American Express

Amount: EUR

Foreign Amount:

Comment:

Card Type AX American Express

Card No. XXXXXXXXXXX1003

Expiry (MM/YY) XX/XX

Holder's Name Balla LATA

Issue Number 05 Issue Date (YY/MM) 09/06

PA-DSS Implementation guide

Relationship between PCI DSS and PA-DSS

The requirements for the Payment Application Data Security Standard (PA-DSS) are derived from the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Security Assessment Procedures*. This document, which can be found at www.pcisecuritystandards.org, details what is required to be PCI DSS compliant (and therefore what a payment application must support to facilitate a customer's PCI DSS
compliance).
Traditional PCI Data Security Standard compliance may not apply directly to payment application vendors since most vendors do not store,process, or transmit cardholder data. However, since these payment applications are used by customers to store, process, and transmitcardholder data, and customers are required to be PCI Data Security Standard compliant, payment applications should facilitate, and not prevent,the customers' PCI Data Security Standard compliance. Just a few of the ways payment applications can prevent compliance follow.
1. Storage of magnetic stripe data in the customer's network after authorization;
2. Applications that require customers to disable other features required by the PCI Data Security Standard, like anti-virus software orfirewalls, in order to get the payment application to work properly; and
3. Vendor's use of unsecured methods to connect to the application to provide support to the customer.

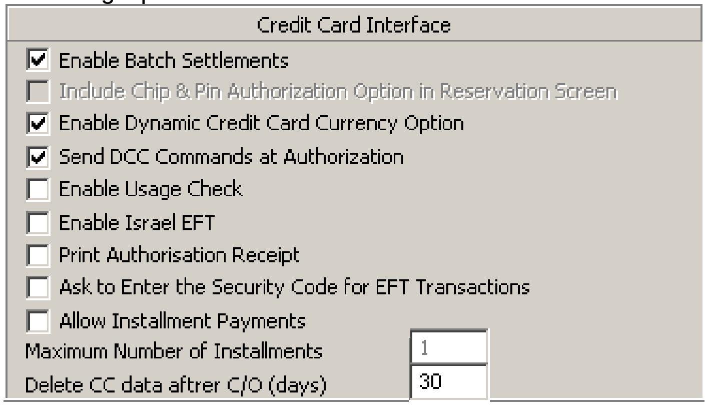
Secure payment applications, when implemented in a PCI DSS-compliant environment, will minimize the potential for security breaches leading to compromises of full magnetic stripe data, card validation codes and values (CAV2, CID, CVC2, CVV2), PINs and PIN blocks, and the damaging fraud resulting from these breaches.

PA-DSS Requirements

The following requirements are taken from ***Payment Application Data Security Standard*** version 1.2 from October 2008

1.1.4 Delete sensitive authentication data stored by previous payment application versions

To delete PANs stored by previous versions of Fidelio Suite8, please use the following option:



Credit Card Interface

☑ Enable Batch Settlements
□ Include Chip & Pin Authorization Option in Reservation Screen
☑ Enable Dynamic Credit Card Currency Option
☑ Send DCC Commands at Authorization
□ Enable Usage Check
□ Enable Israel EFT
□ Print Authorisation Receipt
□ Ask to Enter the Security Code for EFT Transactions
□ Allow Installment Payments
Maximum Number of Installments: 1
Delete CC data aftrer C/O (days): 30

Magnetic stripe data, card validation codes or PIN-blocks have not been stored in Suite8 and thus do not need to be removed.

Removal of sensitive authentication data is absolutely necessary for PCI-DSS compliance.

<u>From the PCI-DSS Requirements:</u>
3.2 Do not store sensitive authentication data after authorization (even if encrypted).

1.1.5 Delete any sensitive authentication data (pre-authorization) gathered as a result of troubleshooting the payment application

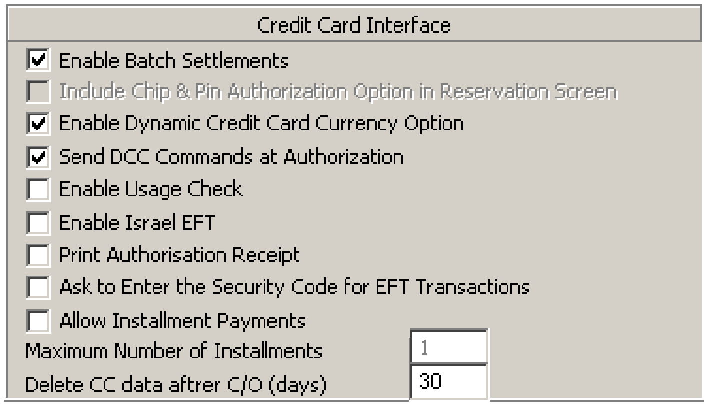
Suite8 does not store sensitive authentication data under any circumstances during a trouble-shooting operation. There is no method to store sensitive data for troubleshooting purposes.

<u>From the PCI-DSS Requirements:</u>
3.2 Do not store sensitive authentication data after authorization (even if encrypted).

2.1 Purge cardholder data after customer defined retention period

From the PCI-DSS Requirements:
3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.

It is possible to delete stored creditcard numbers after a configurable number of days.
The database record (XCCS_NUMBER in table XCCS) is not deleted for integrity reasons, but the encrypted number is overwritten with a text-string which notifies the user accordingly should he try to access a deleted number at a later stage.



Credit Card Interface

☑ Enable Batch Settlements
□ Include Chip & Pin Authorization Option in Reservation Screen
☑ Enable Dynamic Credit Card Currency Option
☑ Send DCC Commands at Authorization
□ Enable Usage Check
□ Enable Israel EFT
□ Print Authorisation Receipt
□ Ask to Enter the Security Code for EFT Transactions
□ Allow Installment Payments

Maximum Number of Installments 1
Delete CC data aftrer C/O (days) 30

As default creditcard number should be deleted 30 after C/O of the guest.

2.7 Delete cryptographic key material or cryptograms stored by previous payment application versions

From the PCI-DSS Requirements:
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data,.

Suite 8 offers functionality to re-encrypt stored creditcard numbers with a new key, See 'Security at the database level'

The full crypting keys have never been stored in Suite8's database, so there is no need for a tool which removes outdated crypting information.

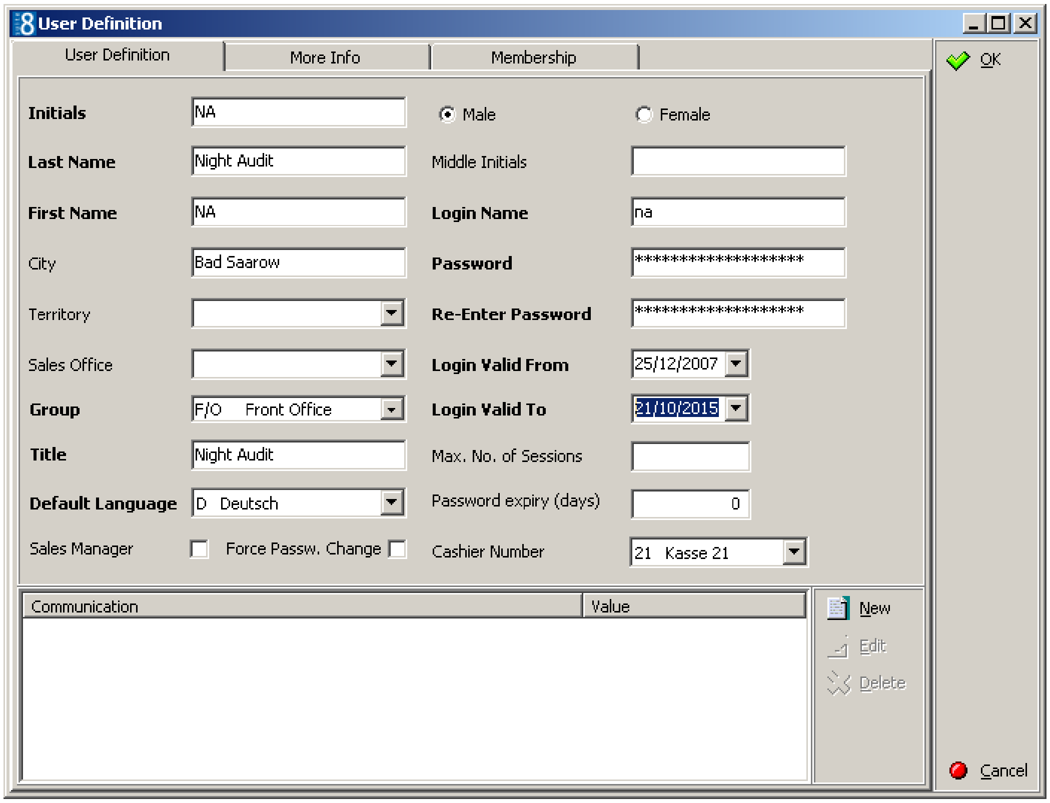
Deletion of cryptographic material or cryptograms is absolutely necessary for PCI-DSS compliance.

3.1 Use Unique user IDs and secure authentication for administrative access and access to cardholder data

To comply with this requirement please be sure to:

- Never use default administrative accounts/passwords for the log-on to Suite8
- Make sure that the authentication for default accounts is secure.
- Disable accounts which are not used:

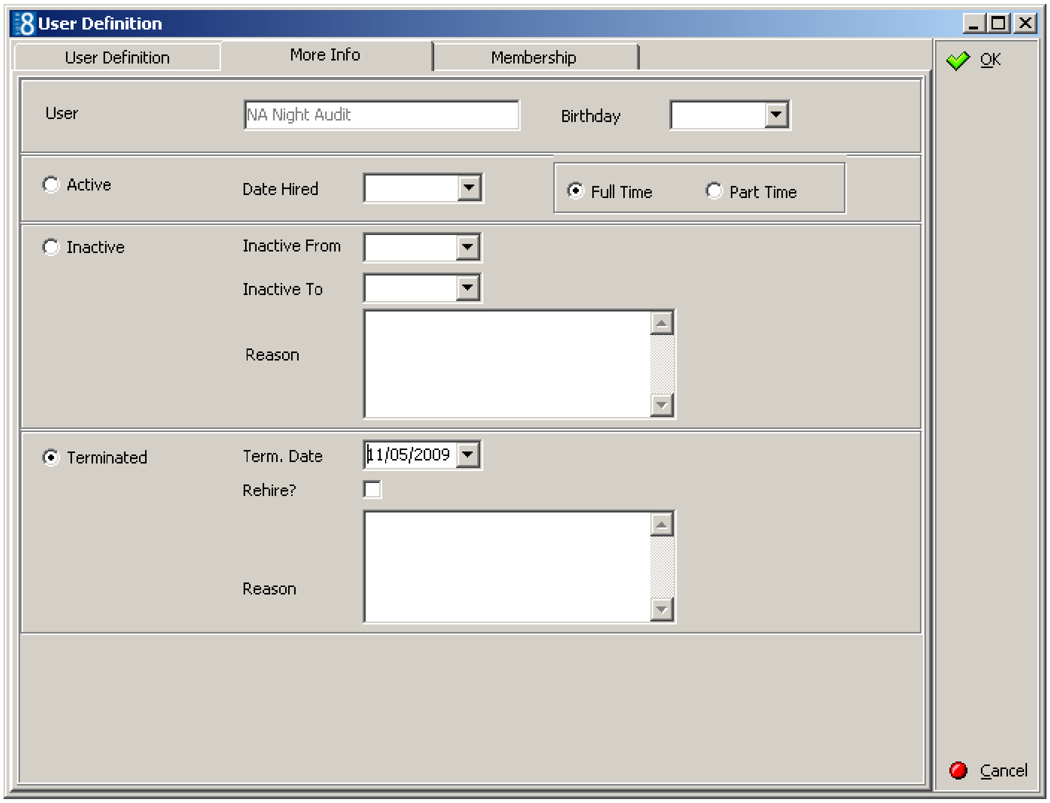
Either you need to define an expiry date of 'today' for not-used accounts:



Initials	NA	● Male	○ Female
Last Name	Night Audit	Middle Initials	
First Name	NA	**Login Name**	na
City	Bad Saarow	**Password**	********************
Territory		**Re-Enter Password**	********************
Sales Office		**Login Valid From**	25/12/2007
Group	F/O Front Office	**Login Valid To**	21/10/2015
Title	Night Audit	Max. No. of Sessions	
Default Language	D Deutsch	Password expiry (days)	0
Sales Manager □	Force Passw. Change □	Cashier Number	21 Kasse 21

Communication	Value

or you need to disable the account:



User NA Night Audit
Birthday
○ Active
Date Hired
● Full Time ○ Part Time
○ Inactive
Inactive From
Inactive To
Reason
● Terminated
Term. Date 11/05/2009
Rehire? □
Reason

- Use secure authentication for access to Suite8 and the system wherever possible
- Ensure that you create secure authentication to access suite per the PCI DSS Requirements as stated below:

From the PCI-DSS Requirements:

8.5.8 Do not use group, shared, or generic accounts and passwords.

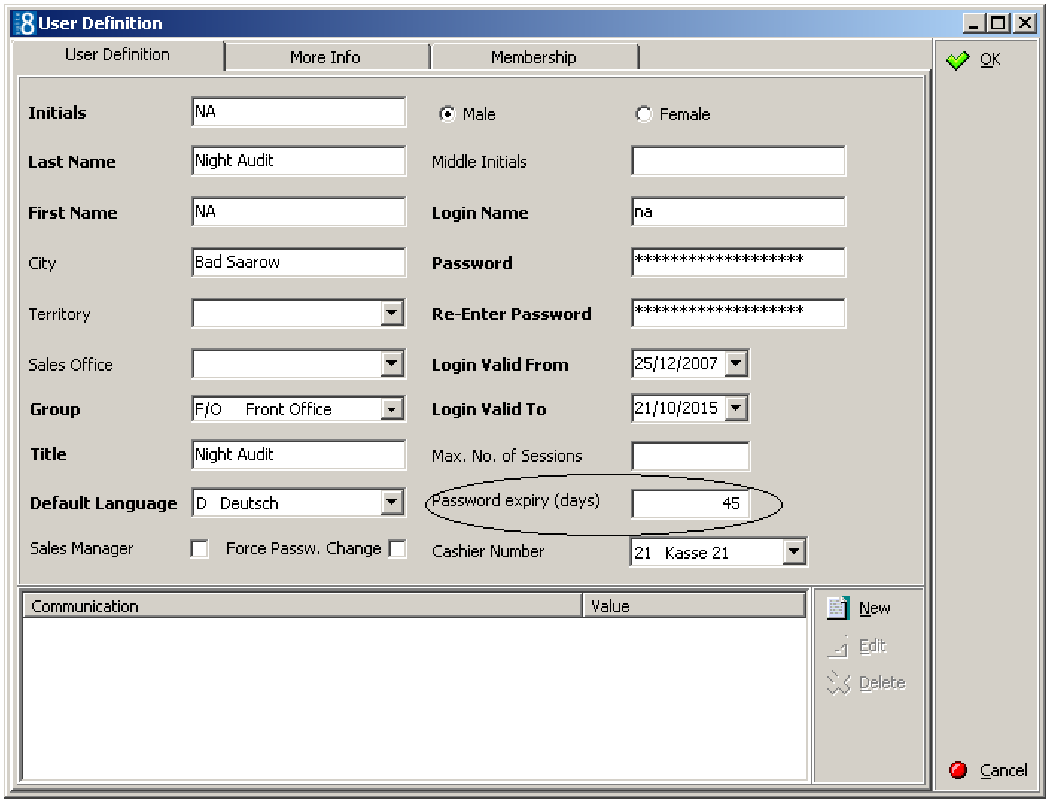
8.5.8.a For a sample of system components, examine user ID lists to verify the following

- Generic user IDs and accounts are disabled or removed.
- Shared user IDs for system administration activities and other critical functions do not exist.
- Shared and generic user IDs are not used to administer any system components.

8.5.8.b Examine password policies/procedures to verify that group and shared passwords are explicitly prohibited.

8.5.8.c Interview system administrators to verify that group and shared passwords are not distributed, even if requested.

8.5.9 Change user passwords at least every 90 days.



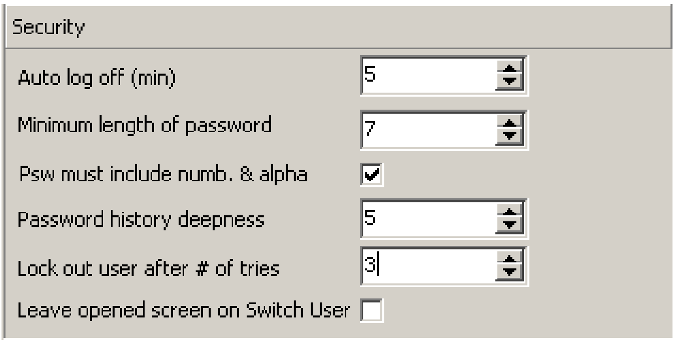
Initials	NA	● Male	○ Female
Last Name	Night Audit	Middle Initials	
First Name	NA	**Login Name**	na
City	Bad Saarow	**Password**	********************
Territory		**Re-Enter Password**	********************
Sales Office		**Login Valid From**	25/12/2007
Group	F/O Front Office	**Login Valid To**	21/10/2015
Title	Night Audit	Max. No. of Sessions	
Default Language	D Deutsch	Password expiry (days)	45
Sales Manager	□ Force Passw. Change □	Cashier Number	21 Kasse 21

Communication	Value

Ensure that the expiry of passwords for all users is set to a maximum of 90 days.

8.5.10 Require a minimum password length of at least seven characters

Log-on relevant security setting can be set in the following form:



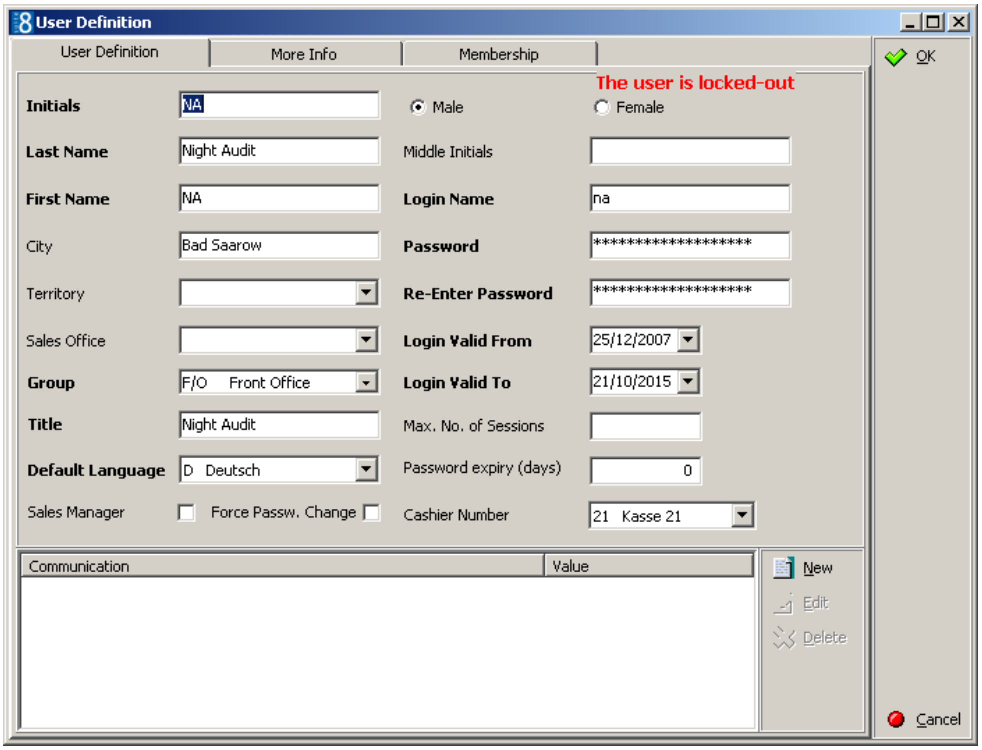
Security

Auto log off (min)	5
Minimum length of password	7
Psw must include numb. & alpha	☑
Password history deepness	5
Lock out user after # of tries	3
Leave opened screen on Switch User	□

The above form applies to the following requirements too:

8.5.11 Use passwords containing both numeric and alphabetic characters.
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.
8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.
8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to reactivate the terminal.

Locked out users:

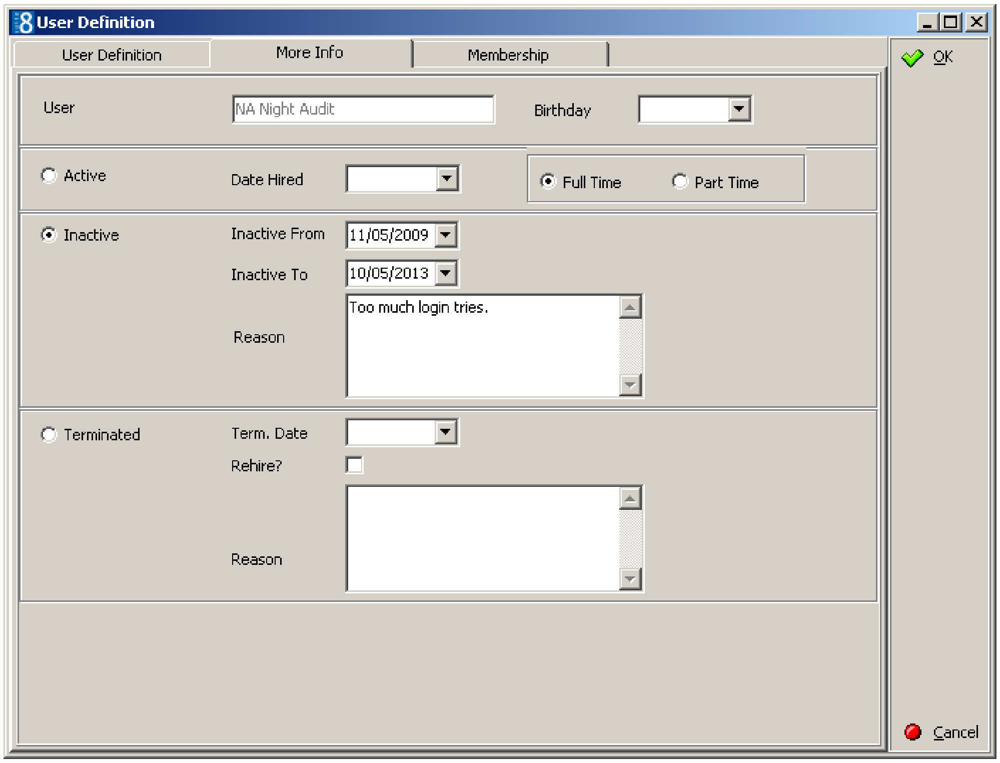


The user is locked-out

Initials: NA
● Male ○ Female
Last Name: Night Audit
Middle Initials:
First Name: NA
Login Name: na
City: Bad Saarow
Password: *******************
Territory:
Re-Enter Password: *******************
Sales Office:
Login Valid From: 25/12/2007
Group: F/O Front Office
Login Valid To: 21/10/2015
Title: Night Audit
Max. No. of Sessions:
Default Language: D Deutsch
Password expiry (days): 0
Sales Manager □
Force Passw. Change □
Cashier Number: 21 Kasse 21

Communication	Value

There is no timer in Suite8 which allows a user to log-on again after too many unsuccessful tries after a period of time. Such a user needs to be reactivated by a supervisor:



User: NA Night Audit
Birthday:
○ Active
Date Hired:
● Full Time ○ Part Time
● Inactive
Inactive From: 11/05/2009
Inactive To: 10/05/2013
Reason: Too much login tries.
○ Terminated
Term. Date:
Rehire? □
Reason:

3.2 Use unique user IDs and secure authentication for administrative access and access to cardholder data.

From the PCI-DSS Requirements:
8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.
8.2 In addition to assigning a unique ID**,** employ at least one of the following methods to authenticate all users:

- Password or passphrase
- Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)

Always ensure that each system user has his/her own unique user account so that logging of access to cardholder data can be linked to each user.

4.2 Implement automated audit trails

To implement automated auditing enable logging in the windows OS:
(article cc 758201 for Microsoft TechNet)

Enable Security Auditing

Microsoft® Windows® Server 2003 uses security and system logs to store collected security events. Before enabling the system and security logs, you need to enable auditing for the system log and establish the number of events you want recorded in the security log. You customize system log events by configuring *auditing*. Auditing is the process that tracks the activities of users and processes by recording selected types of events in the security log of the Web server. You can enable auditing based on categories of security events such as:

- Any changes to user account and resource permissions.
- Any failed attempts for user logon.
- Any failed attempts for resource access.
- Any modification to the system files.

The most common security events recorded by the Web server are associated with user accounts and resource permissions.

Requirements

- Credentials: Membership in the Administrators group on the local computer.
- Tools: Microsoft Management Console (MMC); Local Security Policy

Recommendation

As a security best practice, log on to your computer using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. At the command prompt, type **runas /user:***administrative_accountname* **"mmc %systemroot%\system32\inetsrv\iis.msc"**.

Procedures

To define or modify auditing policy settings for an event category on the local Web server

1. Open Administrative Tools, and then click **Local Security Policy**.

2. In the console tree, click **Local Policies**, and then click **Audit Policy**.

3. In the details pane, double-click an event category for which you want to change the auditing policy settings.

4. On the **Properties** page for the event category, do one or both of the following:

   - To audit successful attempts, select the **Success** check box.
   - To audit unsuccessful attempts, select the **Failure** check box.

5. Click **OK**.

Perform the following procedure on the domain controller.

To define or modify auditing policy settings for an event category within a domain or organizational unit, when the Web server is joined to a domain

1. Open Administrative Tools, and then click **Active Directory Users and Computers**.

2. Right-click the appropriate domain, site, or organizational unit and then click **Properties**.

3. On the **Group Policy** tab, select an existing Group Policy object to edit the policy.

4. In **Group Policy Object Editor**, in the console tree, expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policy**, and then click **Audit Policy**.

5. In the details pane, double-click an event category for which you want to change the auditing policy settings.

6. If you are defining auditing policy settings for this event category for the first time, select the **Define these policy settings** check box.

7. Do one or both of the following:

   - To audit successful attempts, select the **Success** check box.
   - To audit unsuccessful attempts, select the **Failure** check box.

8. Click **OK**.

Requirement 4.2 is in relation to Requirement 10 from the PCI-DSS requirements:

Requirement 10: Track and monitor all access to network resources and cardholder data

10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.
10.2 Implement automated audit trails for all system components to reconstruct the following events:
10.2.1 All individual accesses to cardholder data
10.2.2 All actions taken by any individual with root or administrative privileges
10.2.3 Access to all audit trails
10.2.4 Invalid logical access attempts
10.2 5 Use of identification and authentication mechanisms
10.2.6 Initialization of the audit logs
10.2.7 Creation and deletion of system-level objects
10.3 Record at least the following audit trail entries for all system components for each event:
10.3.1 User identification
10.3.2 Type of event
10.3.3 Date and time
10.3.4 Success or failure indication
10.3.5 Origination of event
10.3.6 Identity or name of affected data, system component, or resource
10.4 Synchronize all critical system clocks and times.
10.5 Secure audit trails so they cannot be altered.
10.5.1 Limit viewing of audit trails to those with a job-related need.
10.5.2 Protect audit trail files from unauthorized modifications.
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).
10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).

All user-logfiles from V8 are written automatically and cannot be altered by any user.

4.2.b Disabling of logging

The Suite8-Userlog cannot be deactivated. Any other logfile may not be deactivated under any circumstance as that would result in non-compliance with PCI-DSS regulations.

6.1 Securely implement wireless technology

If wireless technologies are used within the Suite8 environment, ensure that a corresponding firewall is installed as outlined in the PCI-DSS requirement 1.2.3

If wireless is being used ensure that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and these firewalls deny or control any traffic from the wireless environment into the cardholder data environment.

From the PCI-DSS Requirements:
1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.

6.2 Secure transmissions of cardholder data over wireless networks

If wireless technologies are used within the Suite8 environment, ensure that a corresponding firewall is installed as outlined in the PCI-DSS requirements 1.2.3 , 2.1.1 and 4.1.1 and that the below mentioned requirements are followed:

1.2.3
If wireless is being used ensure that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and these firewalls deny or control any traffic from the wireless environment into the cardholder data environment.

2.1.1

- Encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions
- Default SNMP community strings on wireless devices were changed
- Default passwords/passphrases on access points were changed
- Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (for example, WPA/WPA2)
- Other security-

4.1.1
Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.

- For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.
- For current wireless implementations, it is prohibited to use WEP after June 30, 2010.

9.1 Cardholder data must never be stored on a server connected to the Internet

Do not store cardholder data on Internet-accessible systems (for example, a web server and a database server must not be on same server).

Storing cardholder data on a server which is connected to the internet will result in non-compliance to PCI-DSS regulations.

From the PCI-DSS Requirements:
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ

10.1 Securely deliver remote payment application updates

If payment application updates are delivered via remote access into customers' systems, software vendors must tell customers to turn on remote-access technologies only when needed for downloads from vendor, and to turn off immediately after download completes. Alternatively, if delivered via VPN or other highspeed connection, software vendors must advise customers to properly configure a firewall or a personal firewall product to secure "always-on" connections.

- Receive remote payment application updates via secure modems, per PCI DSS Requirement 12.3.
- If the computer is connected via VPN or other highspeed connection, receive remote payment application updates via a firewall or a personal firewall per PCI DSS Requirement 1 or 12.3.9.

From the PCI-DSS Requirements:
Requirement 1: Install and maintain a firewall configuration to protect cardholder data
12.3.9 Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use

11.2 Implement two factor authentication for remote access to the payment application

Use two-factor authentication (user ID and password and an additional authentication item such as a certificate) if Suite8 may be accessed remotely.

From the PCI-DSS Requirements:
8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

11.3 Securely implement remote access software

Implement and use remote access software security features if remote access software is used to remotely access the payment application or payment environment.

- Customers and all Micros-Fidelio offices are instructed to change all default settings in the remote access software, and also to change default passwords to unique ones for each account.
- Customers and all Micros-Fidelio offices are advised to only accept connections from known/specific IP or MAC addresses.
- Customers and all Micros-Fidelio offices are advised of the use of strong authentication or complex passwords should be used for each user according to PCI DSS requirements 8.1, 8.3 and 8.5.8-8.5.15.

- Authentication and complex passwords for logins according to PCI DSS requirements 8.1,8.3, and 8.5.8-8.5.15
  - PCI DSS 8.1 All remote users must be identified with a unique user name.
  - PCI DSS 8.3 Additional authentication is required for each unique password. The guide gives examples of additional authentication as passwords, tokens, or biometrics.
  - PCI DSS 8.5.8 Customers and all Micros-Fidelio offices are advised not to use shared, group, or generic ID's for remote access, and no account should have a shared password either.
  - PCI DSS 8.5.9 Customers and all Micros-Fidelio offices are instructed to enforce users to change their remote access passwords at least every ninety days.
  - PCI DSS 8.5.10 Customers and all Micros-Fidelio offices are instructed to enforce user passwords to be at least seven characters long for all remote access connections.
  - PCI DSS 8.5.11 Customers and all Micros-Fidelio offices are instructed to enforce remote access user passwords that include both numeric and alphabetic characters.
  - PCI DSS 8.5.12 Customers and all Micros-Fidelio offices are instructed to enforce new remote access passwords to be different than the five previously used passwords.
  - PCI DSS 8.5.13 Customers and all Micros-Fidelio offices are instructed to enforce that remote user accounts should be locked out after three invalid logon attempts.
  - PCI DSS 8.5.14 Customers and all Micros-Fidelio offices are instructed to require a locked remote access user account to remain locked for thirty minutes or until a system administrator resets the account.
  - PCI DSS 8.5.15 Customers and all Micros-Fidelio offices are instructed that system/session idle timeout features are set to fifteen minutes or less for remote access solutions.

- PCI DSS 4.1 Customers and all Micros-Fidelio offices are instructed to use strong encryption protocols such as SSL/TLS or IPSEC when using remote access solutions.
- PCI DSS 4.1.a Customers and all Micros-Fidelio offices are advised that encryption is used wherever cardholder data is transmitted or received over open, public networks, such as the internet.
- Verify that strong encryption is used during data transmission
- For SSL implementations, verify that HTTPS appears as a part of the browser Universal Record Locator (URL), and that no cardholder data is required when HTTPS does not appear in the URL
- Verify that only trusted SSL/TLS keys/certificates are accepted
- Verify that the proper encryption strength is implemented for the encryption methodology in use (Check vendor recommendations/best practices)

➢ PCI DSS 4.1.1.a Appropriate encryption methodologies are used for any wireless transmissions, such as: Wi-Fi Protected Access(WPA or WPA2), IPSEC VPN, or SSL/TLS

➢ PCI DSS 4.1.1.b If WEP is used:

- A minimum 104-bit encryption key and a 24-bit initialisation value.
- It is used only in conjunction with Wi-Fi protected access (WPA or WPA2) technology, VPN, or SSL/TLS
- Shared WEP keys are rotated at least quarterly (or automatically if the technology is capable)
- Shared WEP keys are rotated whenever there are changes in personnel with access to keys
- Access is restricted based on MAC addresses

➢ PCI DSS 8.5.13 Customers and resellers/integrators are instructed to enforce that remote user accounts should be locked out after three invalid logon attempts.

➢ Remote users are instructed to initiate a VPN connection through a firewall.

➢ Full logging is to be enabled for all remote access sessions.

➢ Customers and resellers/integrators are instructed to restrict access to customer passwords to authorized integrator personnel.

➢ All customer passwords are established according to PCI DSS requirements 8.1,8.2,8.4,8.5:

➢ PCI DSS 8.1 Customer and resellers/integrators created remote users must be identified with a unique user name.

➢ PCI DSS 8.2 All customer and resellers/integrators created remote user id's must also incorporate additional authentication. This should be consistent with the documentation.

➢ PCI DSS 8.4 Encrypt all passwords during transmission or storage on all system components.

➢ PCI DSS 8.5.1 Control the deletion and modification of user IDs, credentials and other identifier objects.

➢ PCI DSS 8.5.2 Verify user identity before performing password resets.

➢ PCI DSS 8.5.3 Set first-time passwords to a unique value for each user change immediately after each use.

➢ PCI DSS 8.5.4 Immediately revoke access for any terminated users.

- PCI DSS 8.5.5 Remove inactive user accounts at least every 90 days.
- PCI DSS 8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed.
- PCI DSS 8.5.7 Communicate password procedures for all users that have access to cardholder data.
- PCI DSS 8.5.8 Group, shared, or generic IDs should never be used.
- PCI DSS 8.5.9 Passwords must be changed every 90 days.
- PCI DSS 8.5.10 Passwords must be a minimum of seven characters.
- PCI DSS 8.5.11 Passwords must be alphanumeric.
- PCI DSS 8.5.12 Password history must be set to not allow the previous five passwords.
- PCI DSS 8.5.13 Access must be locked out after no more than five failed authentication attempts.
- PCI DSS 8.5.14 Lockout duration must be at least 30 minutes.
- PCI DSS 8.5.15 Sessions must lock after 15 minutes of being idle.
- PCI DSS 8.5.16 Authenticate access to any database containing cardholder data.

12.1 Secure transmissions of cardholder data over public networks

Micros Fidelio's Suite8 will never require transfer of sensitive cardholder data over public networks. If there ever is a need follow these steps:

Implement and use SSL for secure cardholder data transmission over public networks, in accordance with PCI DSS Requirement 4.1

From the PCI-DSS Requirements:

4.1 Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.
Examples of open, public networks that are in scope of the PCI DSS are:

- *The Internet,*
- *Wireless technologies,*
- *Global System for Mobile communications (GSM), and*
- *General Packet Radio Service (GPRS).*

12.2 Encrypt cardholder data sent over end-user messaging technologies

Micros Fidelio's Suite8 will never require transfer of sensitive cardholder data over end-user messaging technologies. If there ever is a need follow these steps:

Ensure that unencrypted PANs (creditcard numbers) are NEVER sent by end-user messaging technologies (for example, e-mail, instant messaging, chat).
Suite8 does not include integration of messaging engines.

From the PCI-DSS Requirements:
4.2 Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).

13.1 Encrypt non-console administrative access

Connections to customers for non-console administration must be made through a secure CISCO or ASTARO VPN connection. *Telnet or rlogin must never be used for administrative access.*

Implement and use SSH, VPN, or SSL/TLS for encryption of any non-console administrative access to payment application or servers in cardholder data environment.

From the PCI-DSS Requirements:
2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for webbased management and other non-console administrative access.

Oracle databases

Suite8 is installed on an oracle database.
Micros-Fidelio regularly checks for vulnerabilities in the Oracle Database system through developer-newsletters and Oracle-Metaframe.
Any available correction to a vulnerability will be added to Micros-Fidelio's Suite8 Installshield.

About this Implementation Guide

This implementation guide is reviewed on an annual basis and is updated as needed to document all major and minor changes to Fidelio Suite8.

This implementation guide is reviewed on an annual basis and is updated as needed to show any changes in the PA-DSS documentation.