Соответствие CISP и соблюдение Стандарта PCI-DSS

согласно Стандарту безопасности данных для платежных приложений

Версия 1.2

Этот документ подготовлен **MICROS-Fidelio (**Ирландия**) Ltd.** и доступен избранному кругу лиц для ознакомления. Это конфиденциальный документ, который содержит концепции, методы и другую информацию, являющуюся собственностью. Читатели должны относиться к этой информации, как конфиденциальной.

Информация, содержащаяся в этом документе, может изменяться без предварительного уведомления.

MICROS-Fidelio (Ирландия**) Ltd.** не дает никаких гарантий в отношении этого материала, включая, но не ограничиваясь, подразумеваемыми гарантиями конкурентоспособности и пригодности для тех или иных целей.

MICROS-Fidelio (Ирландия**) Ltd.** не несет ответственности за ошибки, которые могут содержаться в этом документе, а также за случайные или косвенные убытки, связанные с предоставлением или использованием этого материала.

Автор:
Группа Разработчиков версии **8**

Издано в Германии

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

Тел: **+49 2131 137 0**
Факс: **+49 2131 137 464**

История Изменений Документа

Версия	Дата	Изменение
8.8.	11 мая 2009	Исходная версия (FV)
8.8.0.	12 июня 2009	Небольшие исправления (FV)
8.8.0.1	15 июня 2009	Небольшие исправления (FV)

Содержание

Общая Информация

Об этом Документе

Этот документ представляет собой краткое руководство, содержащее информацию о соблюдении **MICROS-Fidelio** Стандарта безопасности данных индустрии платежных карт, утвержденного **Visa USA**, в части соответствия Программе безопасности данных держателей карт **(CISP)**, а также соблюдении **MICROS-Fidelio** стандарта безопасности данных для платежных приложений **(PCI PA-DSS)**, утвержденного Советом по развитию стандартов безопасности данных индустрии платежных карт **(PCI-SSC)**. Этот документ относится исключительно к программному продукту **SUITE8 Hotel Management Solution** версии **8.8** компании **MICROS-Fidelio**.

О Соответствии Программе CISP

Когда клиенты расплачиваются с помощью банковской карточки в точках продаж или совершают покупки через интернет, по телефону или электронной почте, они хотят быть уверенными в безопасности своего банковского счета. Вот почему **Visa** в США и **VISA** в Европе внедрили Программу Безопасности Данных Держателей Карт **(CISP)**. Запущенная в июне **2001** года, эта программа призвана защитить данные держателей карт **Visa** — независимо от места их нахождения —и обеспечить поддержание самого высокого **1**-го уровня информационной безопасности со стороны членов-участников, торгово-сервисных предприятий и провайдеров услуг.

Более подробно о соответствии Программе **CISP** читайте на вэб-сайте **Visa USA CISP**:

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

или на вэб-сайте **Visa Europe CISP**:

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

О Стандарте безопасности данных индустрии платежных карт (PCI-DSS)

Соответствие Программе безопасности данных держателей карт **(CISP)** требуется со стороны всех торгово-сервисных предприятий и провайдеров услуг, которые хранят, обрабатывают или передают данные о держателях карт **Visa**. Эта программа касается всех каналов оплат, включая розничную торговлю через торговые точки, заказы товаров по электронной почте/телефону и интернет-коммерцию. Чтобы соответствовать Программе **CISP**, торгово-сервисные предприятия и провайдеры услуг должны соблюдать Стандарт безопасности данных индустрии платежных карт **(PCI-DSS)**, определяющий единый подход к обеспечению безопасности конфиденциальных данных для всех платежных брендов карточного рынка. Этот Стандарт представляет собой результат совместного сотрудничества между **Visa**, **MasterCard**, **AMEX**, **Discover** и **JCB**, и призван создать общие для индустрии требования безопасности, включая требования **CISP**. Другие карточные бренды, ведущие бизнес в США, также одобрили Стандарт **PCI-DSS** и реализовали его в своих программах. Взяв за основу Стандарт **PCI-DSS**, Программа **CISP** предлагает инструменты и меры защиты против утечки информации и компрометации карт для всей индустрии **PCI**.
Стандарт **PCI-DSS**, описанный ниже, включает двенадцать основных требований, которые детализируются дополнительными требованиями:

---

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

Стандарт **PCI-DSS** является результатом совместного сотрудничества между **Visa, MasterCard, AMEX, Discover** и **JCB,** целью которого было создать общие для индустрии требования безопасности**.** Другие карточные бренды**,** ведущие бизнес в США**,** также одобрили Стандарт **PCI-DSS** и реализовали его в своих программах**.**
Эти нижеописанные **12** требований положены в основу Программы **CISP Visa.**

Стандарт PCI-DSS

Построение и обслуживание защищенной сети

Требование 1: Установить и обеспечить функционирование межсетевых экранов для защиты данных держателей карт

Требование 2: Не использовать настройки системных паролей и других параметров безопасности данных**,** заданных производителем по умолчанию

Защита данных о держателях карт

Требование 3: Обеспечить безопасное хранение данных о держателях карт
Требование 4: Обеспечить шифрование данных о держателях карт при их передаче через открытые сети общего пользования

Программа управления уязвимостями

Требование 5: Использовать и регулярно обновлять антивирусные программы
Требование 6: Разрабатывать и поддерживать системы и приложения безопасности

Внедрение строгих мер контроля доступа

Требование 7: Ограничить доступ к данным о держателях карт служебной необходимостью

Требование 8: Привязать уникальный идентификатор всем**,** у кого есть доступ к ПК

Требование 9: Ограничить физический доступ к данным о держателях карт

Регулярный мониторинг и тестирование сети

Требование 10: Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт

Требование 11: Регулярно тестировать системы и процессы информационной безопасности

Поддержание политики информационной безопасности

Требование 12: Поддерживать политику информационной безопасности

Для кого предназначен этот документ

Этот документ предназначен для следующей аудитории:
• Клиенты **Suite8**
• Установщики**/** Программисты **SUITE8**
• Дилеры **SUITE8**
• Служба Поддержки Клиентов **SUITE8**
• Обучающий персонал по **SUITE8**
• Персонал **MIS**

Необходимые предварительные знания

Данные документ рассчитан на аудиторию**,** имеющую следующие знания или навыки**:**
• Умение работать с ПК
• Понимание базовых сетевых концепций
• Опыт работы с ОС на платформах**,** поддерживаемых **bySuite8**
• Знакомство с программным продуктом **SUITE8 PMS**
• Умение работать с периферийными устройствами **MICROS-Fidelio**

Fidelio Suite 8 версии 8.8 и PCI-DSS

Стандарт PCI-DSS

В то время как **MICROS-Fidelio (**Ирландия**) Ltd.** признает важность поддержания безопасности и целостности данных о держателях платежных карт**,** некоторые параметры Стандарта **PCI-DSS** и Программы **CISP** остаются исключительной ответственностью клиента**.** Настоящий раздел содержит описание **12** пунктов Стандарта **PCI-DSS.** Информация в этом разделе касается только соответствия программного продукта **Fidelio Suite8** версии **8.8** Стандарту **PCI-DSS.**

Более подробно о Стандарте **PCI-DSS** читайте на вэб**-**сайте **Visa USA** в разделе **Cardholder Information Security Program** здесь**:** **http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html**

Построение и обслуживание защищенной сети

1. Установить и обеспечить функционирование межсетевых экранов для защиты данных держателей карт

*Межсетевые экраны - это средства вычислительной техники, контролирующие разрешенный входящий сетевой трафик, а также трафик между сегментами локальной сети разного уровня критичности. Все системы должны быть защищены от неавторизованного доступа через интернет, будь то электронная коммерция, удаленный доступ своих работников через браузер или корпоративная почта. Часто кажущиеся малозначимыми каналы связи с внешней средой могут представлять собой незащищенные пути доступа к ключевым системам. Межсетевые экраны – это основные механизмы обеспечения безопасности любой компьютерной сети.***2**

MICRO-Fidelio GmbH настоятельно рекомендует хранить все системы с конфиденциальной информацией **(**серверы**,** базы данных**,** беспроводные точки доступа**,** и пр**.)** за межсетевыми экранами для защиты этих данных и с целью соответствия Стандартам Совета **PCI-SSC.**

Чтобы быть уверенными в том**,** что конфигурация ваших сетевых экранов настроена в соответствии с Шагом **1** Стандарта **PCI DSS "Установить и обеспечить функционирование межсетевых экранов для защиты данных держателей карт",** ознакомьтесь с разделом **CISP** вэб-сайт**а Visa USA: <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>**

.

2. Не использовать настройки системных паролей и других параметров безопасности данных, заданных производителем по умолчанию

*Хакеры (как на стороне, так и внутри компании) для взлома систем часто прибегают к использованию паролей и других настроек , заданных производителями по умолчанию. Эти пароли и настройки хорошо известны в определенных сообществах и легко находятся через открытые источники информации***.3**

MICRO-Fidelio GmbH. рекомендует клиентам при установке систем поменять все дефолтовые пароли**,** включая те**,** что предназначены для операционных систем**,** беспроводных точек доступа**,** серверов**,** баз данных и пр**.** В **Suite8** есть две дефолтовых учетных записи**,** пароли которых необходимо поменять**,** чтобы соответствовать комплексным требованиям к паролям Программы **CISP;** это учетная запись **SUPERVISOR** в приложении и учетная запись **V8** в базе данных**.**

Более подробно о Шаге **2** Стандарта **PCI-DSS «Не использовать настройки системных паролей и других параметров безопасности данных, заданных производителем по умолчанию»** читайте раздел **CISP** вэб-сайт**а Visa USA <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>.

Защита данных о держателях карт

3. Обеспечить безопасное хранение данных о держателях карт

Шифрование – это лучший механизм защиты, потому что даже если кто-то взломает все другие механизмы защиты и получит доступ к зашифрованным данным, он не сможет их прочитать, не имея ключа шифрования. Шифрование - пример принципа многоуровневой защиты.[4]

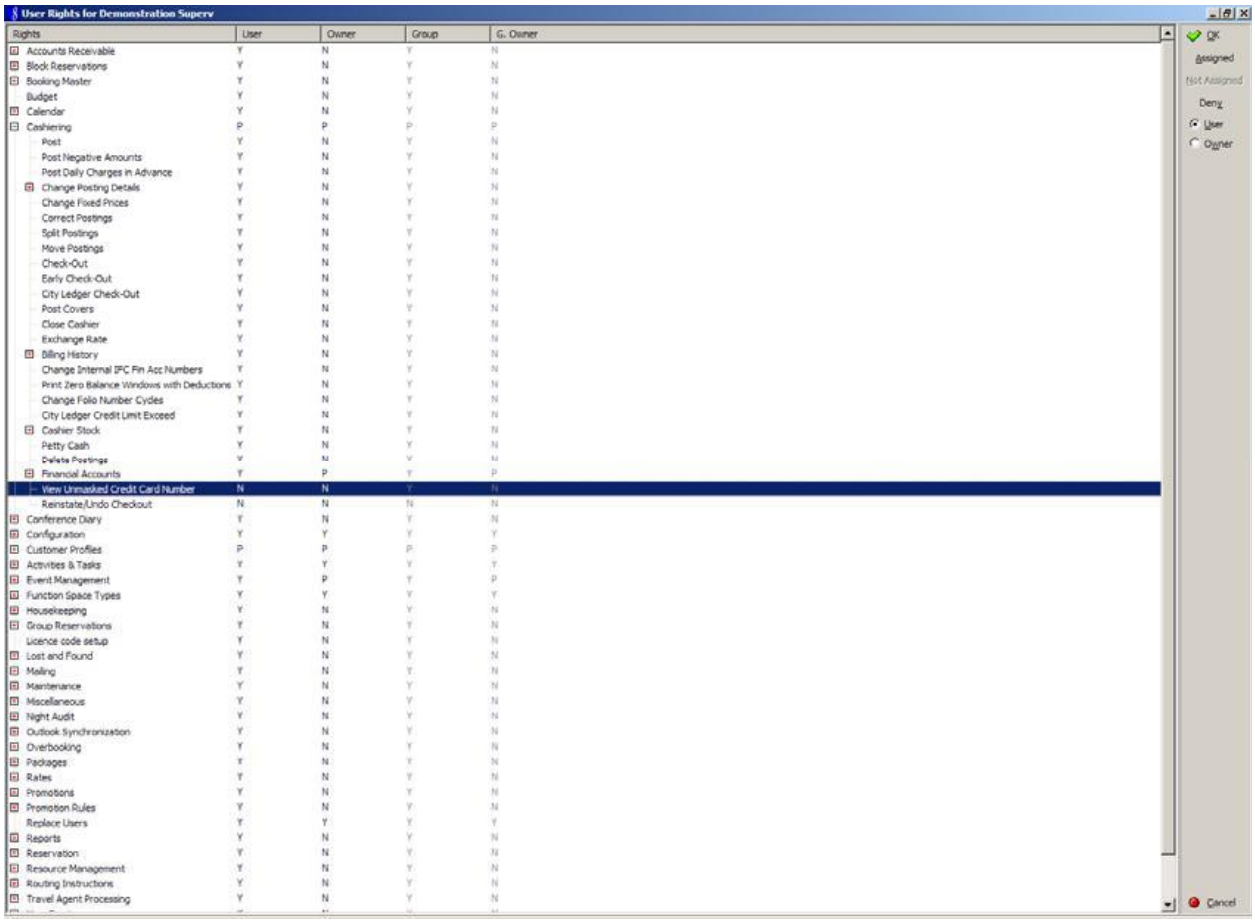
MICROS-Fidelio (Ireland) Ltd. использует маскировку данных кредитных карт и **192-**битное шифрование по алгоритму **Triple-DES** для обеспечения надежного хранения данных держателей карт**,** в соответствии со стандартом PC**I-DSS.** Сервер базы данных должен всегда находиться за межсетевым экраном для защиты от вредоносных интернет-атак**.**

Более подробно о Шаге **3** Стандарта **PCI-DSS «Защита данных о держателях карт»,** читайте раздел C**ISP** вэб-сайта **Visa USA** **<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>.**

Для обеспечения соответствия с Шагом **3** стандарта **PCI-DSS,** сконфигурите право маскировки данных кредитных карт следующим образом**:**

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



Прим: Вышесказанное может не относиться к работникам и другим лицам**,** которым необходимо видеть полные номера кредитных карт**.**

Прим: *Конфигурация этой опции должнв всегда быть такой, как показано выше, чтобы соответствовать Требованию 3 Стандарта PCI-DSS.*

4. Обеспечить шифрование данных о держателях карт при их передаче через открытые сети общего пользования

Конфиденциальная информация, при передаче ее через интернет, должна зашифровываться, так как хакеру легко и просто перехватить и/или перенаправить такие данные. [5]

MICROS-Fidelio (Ирландия**) Ltd.** использует **128-**битное шифрование по алгоритму **Triple-DES** для обеспечения надежной передачи данных о владельцах карт через сети общего доступа в соответствии со стандартом PC**I-DSS.**

SUITE8 не предназначен для отправки конфиденциальной информации через сети общего доступа**.**
MICROS-Fidelio (Ирландия**) Ltd.** настоятельно рекомендует шифровать **(**используя **VPN, SSL,** и пр**.)** всю передаваемую через интернет конфиденциальную информацию**,** включая беспроводные соединения**, E-mail** и при использовании сервисов**,** типа **Telnet, FTP** и т.п**.**

Более подробно о Шаге **4** Стандарта **PCI-DSS «Обеспечить шифрование данных о держателях карт при их передаче через открытые сети общего пользования»** читайте раздел **CISP** вэб-сайта **Visa USA:**
<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|/busin

ess/accepting_visa/ops_risk_management/ cisp%2Ehtml|View%20all%20CISP%20downloads>.

Программа управления уязвимостями

5. Использовать и регулярно обновлять антивирусные программы

Много уязвимостей и вредоносных вирусов попадает в сеть через электронную почту. Чтобы защититься от них, антивирусные программы должны быть установлены на всех почтовых системах и рабочих столах.[6]

В соответствии со стандартом **PCI-DSS Visa USA, MICROS-Fidelio (Ireland) Ltd.** настоятельно рекомендует постоянно использовать и регулярно обновлять антивирусные программы**.** Конфигурация некоторых серверов **Suite8** требует специальных антивирусных настроек**;** эти настройки подробно описываются в соответствующих инструкциях**.**

Чтобы убедиться в том**,** что ваша антивирусная программа настроена в соответствии с Шагом **5** Стандарта **PCI-DSS "Использовать и регулярно обновлять антивирусные программы",** озакомьтесь с разделом **CISP** вэб**-**сайта **Visa USA** **<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|/busin ess/accepting_visa/ops_risk_management/ cisp%2Ehtml|View%20all%20CISP%20downloads>.**

6. Разрабатывать и поддерживать системы и приложения безопасности

Злоумышленники используют уязвимости в защите для проникновения в системы. Многие из этих уязвимостей устраняются обновлениями безопасности, выпускаемыми производителем, поэтому все системы должны обновляться актуальными программными патчами, защищающими от злоумышленных действий работников, сторонних хакеров и вирусов. Что касается приложений, являющихся продуктом собственных рабработок, то здесь многочисленных уязвимостей можно избежать, используя стандартные процессы разработки систем и защитное кодирование.[7]

Для обеспечения программной целостности и безопасности **MICROS Systems Inc.** использует отдельные среды для разработок и для производства**.** Обновляемые патчи**,** в том числе обновления безопасности**,** доступны через **SUITE FTP** сервер **<ftp.v8.myfidelio.com>** и вашем локальном офисе поддержки**.**

Чтобы убедиться в том**,** что ваш сайт разрабатывает и поддерживает системы и приложения безопасности в соответствии с Шагом **6** Стандарта **PCI-DSS "Разрабатывать и поддерживать системы и приложения безопасности",** ознакомьтесь с содержанием раздела **CISP** вэб-сайта **Visa USA** **<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>.**

Внедрение строгих мер контроля доступа

7. Ограничить доступ к данным держателей карт служебной необходимостью

Доступ к критическим данным предоставляется только авторизованным пользователям.[8]

MICROS-Fidelio (Ireland) Ltd. признает важность контроля доступа к данным и осуществляет этот контроль, предоставляя доступ в зависимости от уровня должности работника. Этот механизм позволяет ограничить доступ к конфиденциальной информации необходимым для выполнения должностных обязанностей объемом знаний и защитить пароли.

Более подробно о Шаге **7** Стандарта **PCI-DSS "Ограничить доступ служебной необходимостью"**, читайте раздел **CISP** вэб-сайта **Visa USA <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>**

8. Привязать уникальный идентификатор всем, у кого есть доступ к ПК

Такая привязка гарантирует, что действия с критическими данными и системами выполняются известными и авторизованными пользователями и могут отслеживаться.[9]

MICROS-Fidelio (Ирландия**) Ltd.** признает важность привязки уникального идентификатора каждому работнику, имеющему доступ к компьютеру. Два разных пользователя **SUITE8** не могут иметь одинаковый идентификатор, что позволяет отслеживать действия каждого при условии, что сайт клиента поддерживает должную конфигурацию и ограничивает уровни привилегий работников служебной необходимостью. В то время как **MICROS-Fidelio (**Ирландия**) Ltd.** прилагает все возможные усилия к тому, чтобы соответствовать Шагу **8** Стандарта **PCI DSS**, некоторые параметры, в т.ч. аутентификация пользователя, удаленный доступ к сети и управление паролями для производственно-технического персонала и администраторов, а также для всех системных компонентов, зависят от специфической практики и политики того или иного сайта.

Для обеспечения строго контроля доступа к **SUITE8 PMS,** всегда привязывайте уникальные имена пользователей и комплексные пароли каждой учетной записи пользователя. **MICROS-Fidelio (**Ирландия**) Ltd.** настоятельно рекомендует применять эти рекомендации не только к паролям **SUITE8,** но и к паролям **Windows** тоже.

Прим: Для удаленного доступа необходима двухфакторная аутентификация для соответствия стандарту **PCI-DSS.**
Для соответствия Требованию **8** стандарта **PCI-DSS** мы рекомендуем клиентам следовать следующим указаниям.

- Убедитесь в том, что поле "Дней до даты истечения срока действия пароля" на экране **Edit User** настроено на значение, не превышающее **90.**

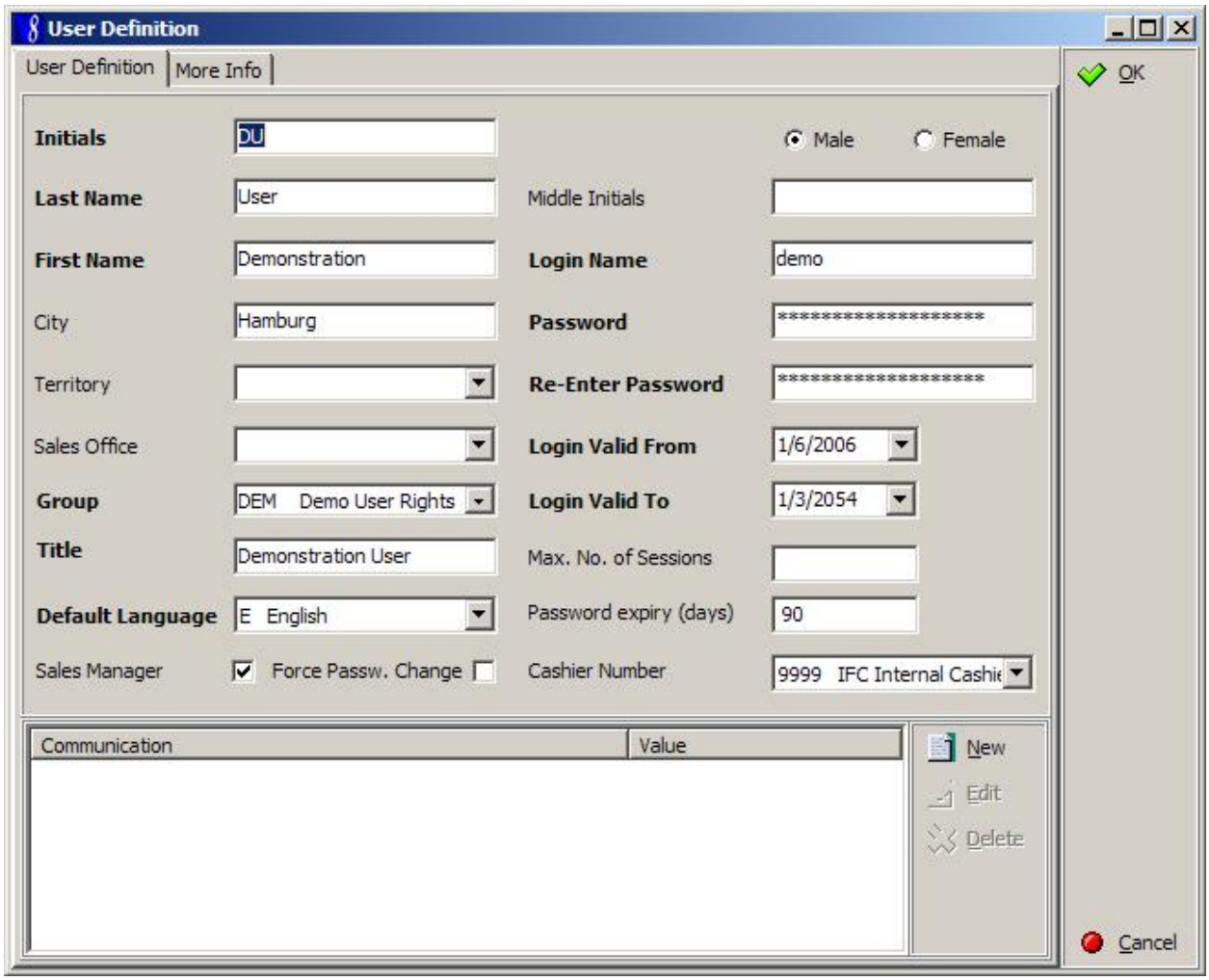
[8] **"Payment Card Industry Security Audit Procedures.doc", p. 26, V. 1.0, December 15, 2004. <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html?it=c|/business/accepting_visa/ops_risk_management/cisp%2Ehtml|View%20all%20CISP%20downloads>.**

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_fa

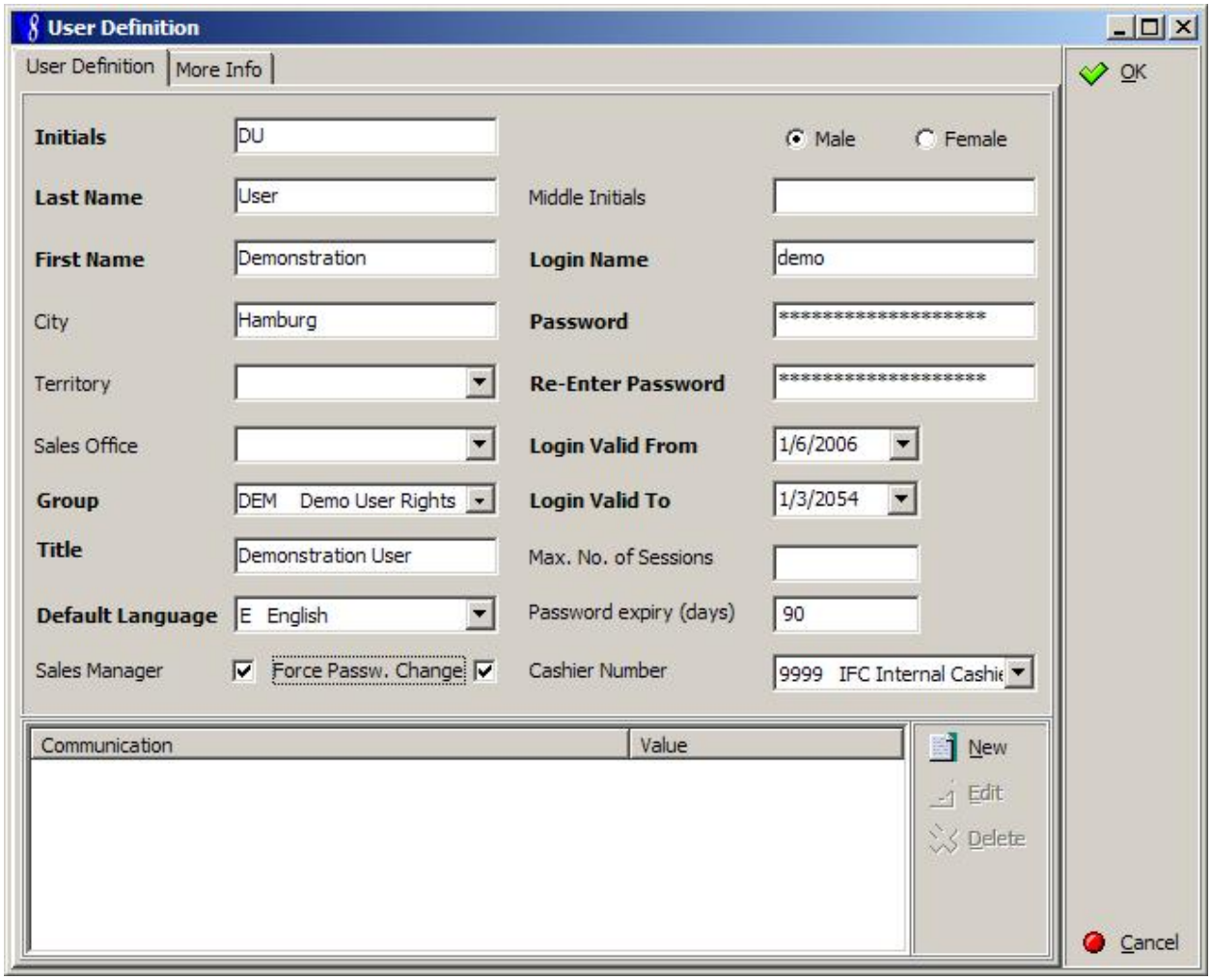
q.html?it=l2|/business/accepting_visa/ops_risk_management/cisp.html|Tools%20and%20FAQ

- Убедитесь в том, что длина паролей пользователей насчитывает не менее **7** знаков.
- Убедитесь в том, что пароли пользователей содержат как буквенные, так и цифровые символы.

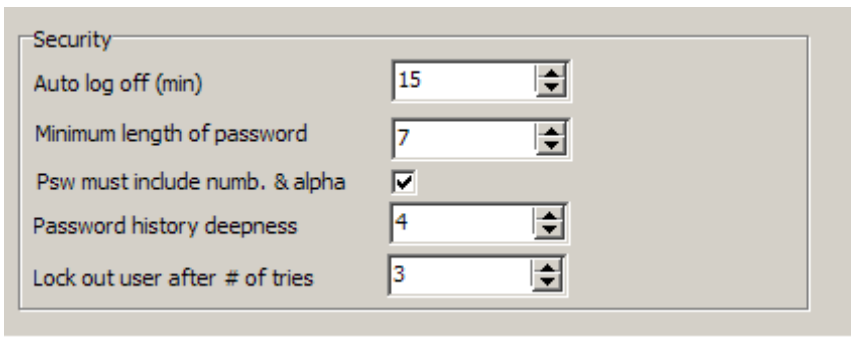
Более подробно о Требовании **8** стандарта **PCI-DSS «Привязать уникальный идентификатор всем, у кого есть доступ к ПК»** читайте раздел **CISP** вэб-сайта **Visa USA**
<http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>



В поле “Дней до даты истечения срока действия пароля” поставьте значение**.** Не превышающее **90** дней**.**



Задайте принудительную смену пароля для каждого нового пользователя в системе, так чтобы пользователю нужно было при первом входе в систему вводить новый пароль.
CONFIGURATION\GLOBAL SETTINGS\GENERIC3



- В поле **Auto-Log-Off** поставьте значение **3** минуты
- в поле минимальная длина пароля поставьте **7 с**имволов
- Задайте обязательное использование цифровых и буквенных символов для паролей
- Сохраняйте историю паролей глубиной минимум **4** уровня
- Задайте блокировку пользователей после **3** неудачных попыток входа

9. Ограничить физический доступ к данным держателей карт

Любой физический доступ к данным или системам с данными о держателях карт создает условия для доступа к устройствам или информации, с возможностью удалить систему или бумажную копию документа, и должен быть надлежащим образом ограничен.[10]

В соответствии со стандартом **PCI-DSS Visa USA, MICROS-Fidelio (Ireland) Ltd.** настоятельно рекомендует ограничивать физический доступ к данным о держателях карт**.**

Чтобы убедиться в том**,** что ваш сайт настроен в соответствии с Шагом **9** Стандарта **PCI-DSS “Ограничить физический доступ к данным о держателях карт”,** читайте раздел **CISP** вэб-сайт**а Visa USA** **<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

Регулярный мониторинг и тестирование сети

10. Контролировать и отслеживать любой доступ к сетевым ресурсам и данным держателей карт

Механизмы ведения записей о событиях, а также возможность отслеживать действия пользователей совершенно необходимы. Наличие записей во всех средах позволяет провести тщательное расследование и проанализировать инциденты. Определить причину инцидентов, если отсутствуют записи событий, очень трудно[11]

MICROS-Fidelio (Ирландия**) Ltd.** включает в **SUITE8** всеобъемлющую аудиторскую утилиту**,** позволяющую привилегированным пользователям отслеживать события в **SUITE8.** Появление структур с открытой базой данных означает**,** что любой пользователь с системным уровнем доступа к серверу базы данных **(Oracle),** имеет также доступ к системным компонентам**,** а следовательно**,** его вход и действия протоколируются**,** как описано в Шаге **10** Стандарта **PCI-DSS. MICROS Fidelio (**Ирландия**) Ltd.** настоятельно рекомендует блокировать интернет**-**доступ к серверу базы данных**.**

Чтобы убедиться в том**,** что ваш сайт соответствует Шагу **10** Стандарта **PCI-DSS "Контролировать и отслеживать любой доступ к сетевым ресурсам и данным держателей карт",** смотрите раздел **CISP** вэб**-**сайт**a Visa USA <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>**

11. Регулярно тестировать системы и процессы информационной безопасности

Уязвимости то и дело обнаруживаются хакерами/разработчиками, а также появляются вместе с новыми программными продуктами. Системы, процессы и написанные на заказ программы необходимо часто тестировать, чтобы быть уверенными в их защищенности по мере того, как идет время и вносятся изменения[12]

В соответствии со стандартом **PCI-DSS Visa USA, MICROS-Fidelio (**Ирландия**) Ltd.** настоятельно рекомендует регулярно тестировать системы и процессы безопасности**.**

Чтобы убедиться в том**,** что системы и процессы безопасности вашего сайта настроены в соответствии с Шагом **11** Стандарта **PCI-DSS "Регулярно тестировать системы и процессы информационной безопасности",** читайте раздел **CISP** вэб**-**сайт**a Visa USA <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>.**

Поддержание политики информационной безопасности

12. Поддерживать политику информационной безопасности

Строгая политика информационной безопасности задает нужный тон в компании в целом и дает работникам представление о том, что от них ожидается. Все работники должны быть осведомлены о конфиденциальности данных и своей ответственности по их защите.[13]

В соответствии со стандартом **PCI-DSS Visa USA, MICROS-Fidelio (**Ирландия**) Ltd.** настоятельно рекомендует поддерживать политку информационной безопасности**.**

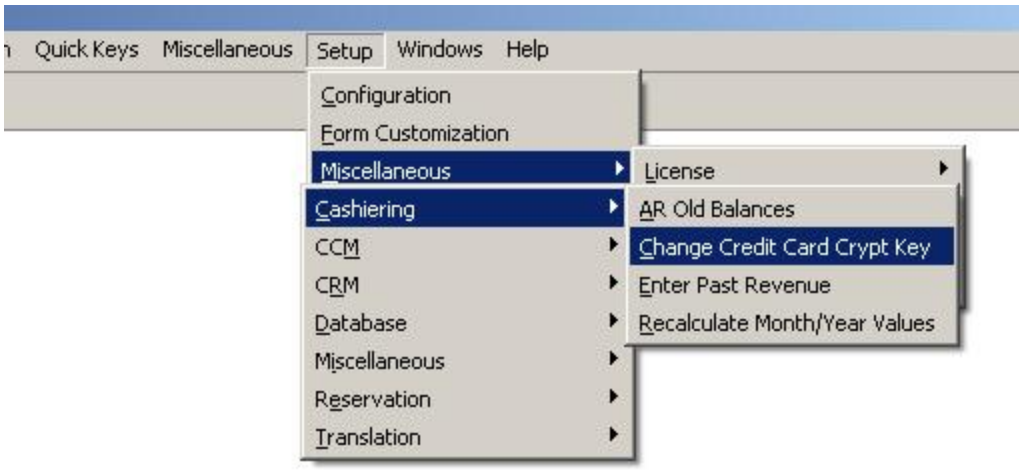
Чтобы убедиться в том**,** что ваша политика информационной безопасности настроена в соответствии с Шагом **12** Стандарта **PCI-DSS «Поддерживать политку информационной безопасности»,** читайте раздел **CISP** вэб**-**сайта **Visa USA <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>**

.

[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>.**

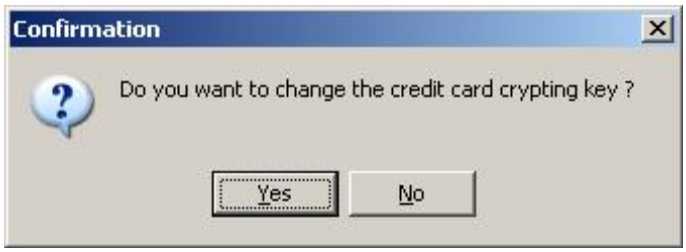
Безопасность в Fidelio Suite 8

Безопасность на уровне базы данных



В **Suite 8** добавлена опция**,** которая будет проверять базу данных на наличие в ней незашифрованных номеров кредитных карт предыдущих старых версий **Suite 8** и будет шифровать их**.**

Эта опция может также использоваться для повторной зашифровки с помощью другого ключа всех номеров кредитных карт в базе данных**.**

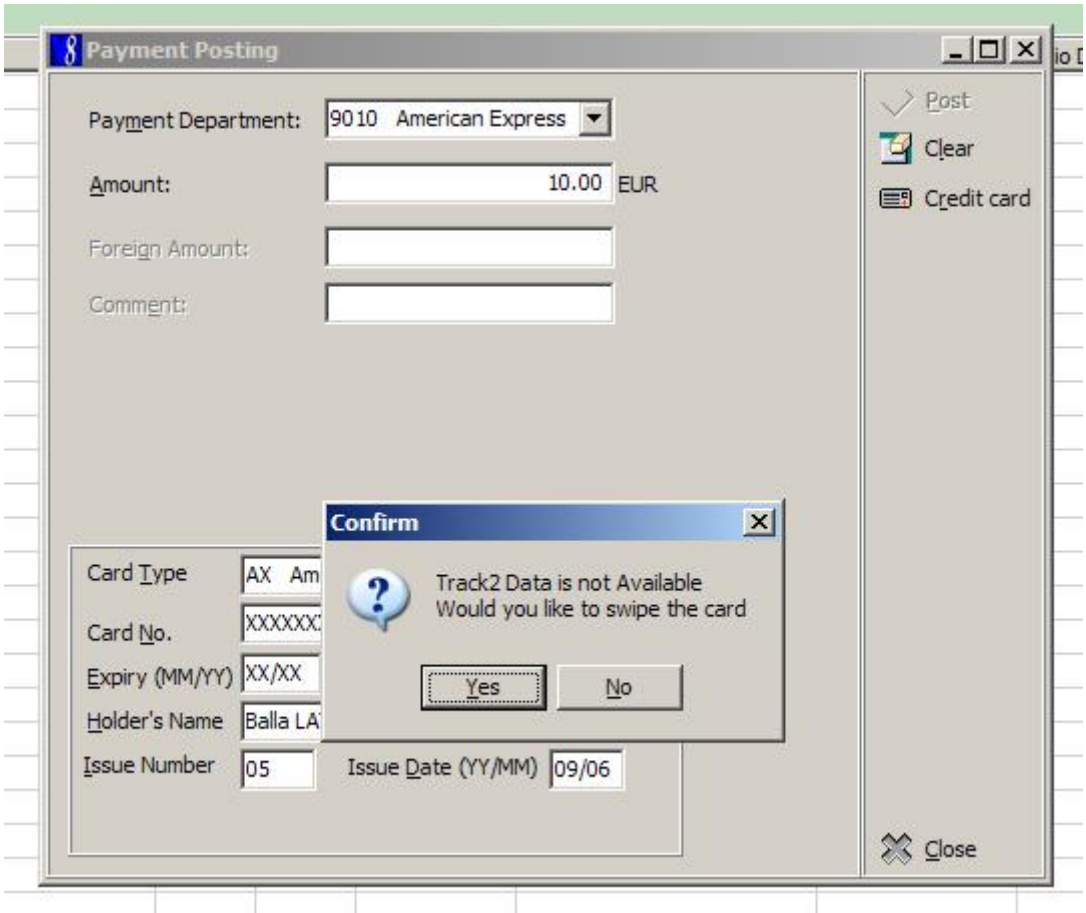


Для зашифровки конфиденциальной информации используется ключ шифрования, вводимый пользователем. Этот ключ можно изменить в любое время.
Изменение ключа приведет к повторной зашифровке всей конфиденциальной информации в базе данных.

Этот ключ необходимо менять, по меньшей мере, раз в год; **Micros-Fidelio** рекомендует делать это чаще.

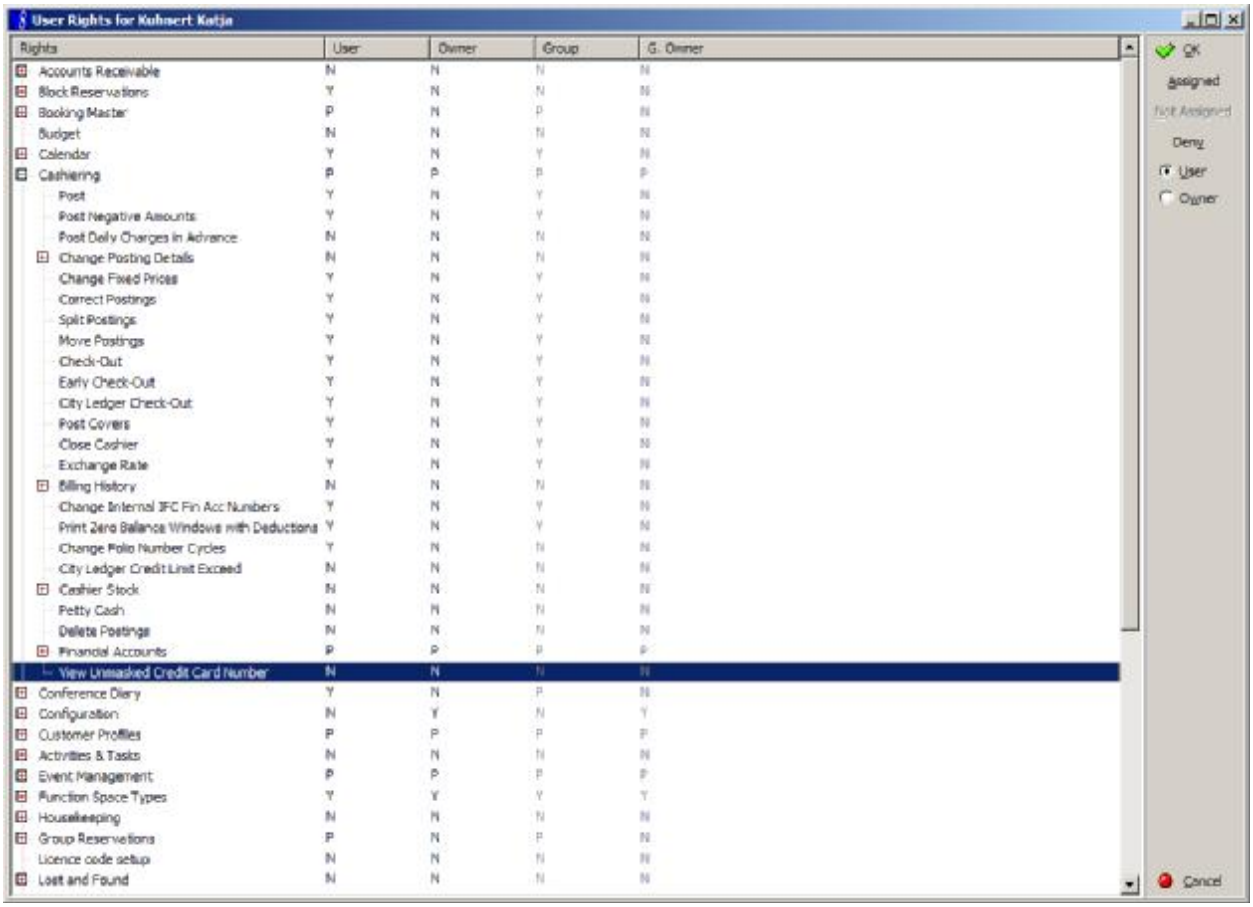
Безопасность конфиденциальных данных о держателях кредитных карт (Дорожка 2)

Данные **2**-ой дорожки считываются с карты во время прокатывания, но они никогда не будут сохранены, а следовательно, не будут доступны для последующих транзакций. Пользователь получит подсказку прокатать карту снова, если необходимо:



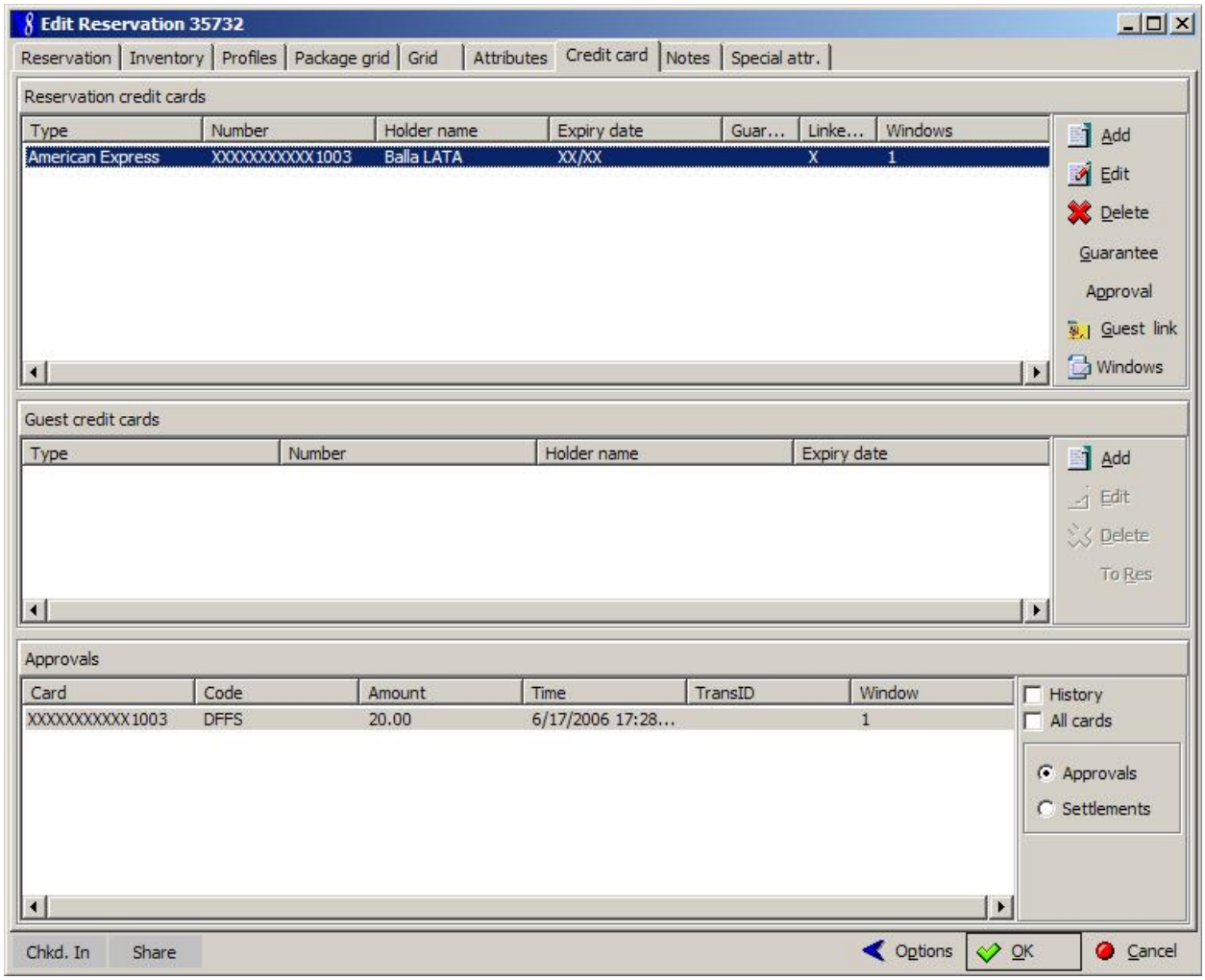
Безопасность на уровне пользователя

Добавлено право пользователя, определяющее, может пользователь видеть полный номер кредитной карты гостя или не может:

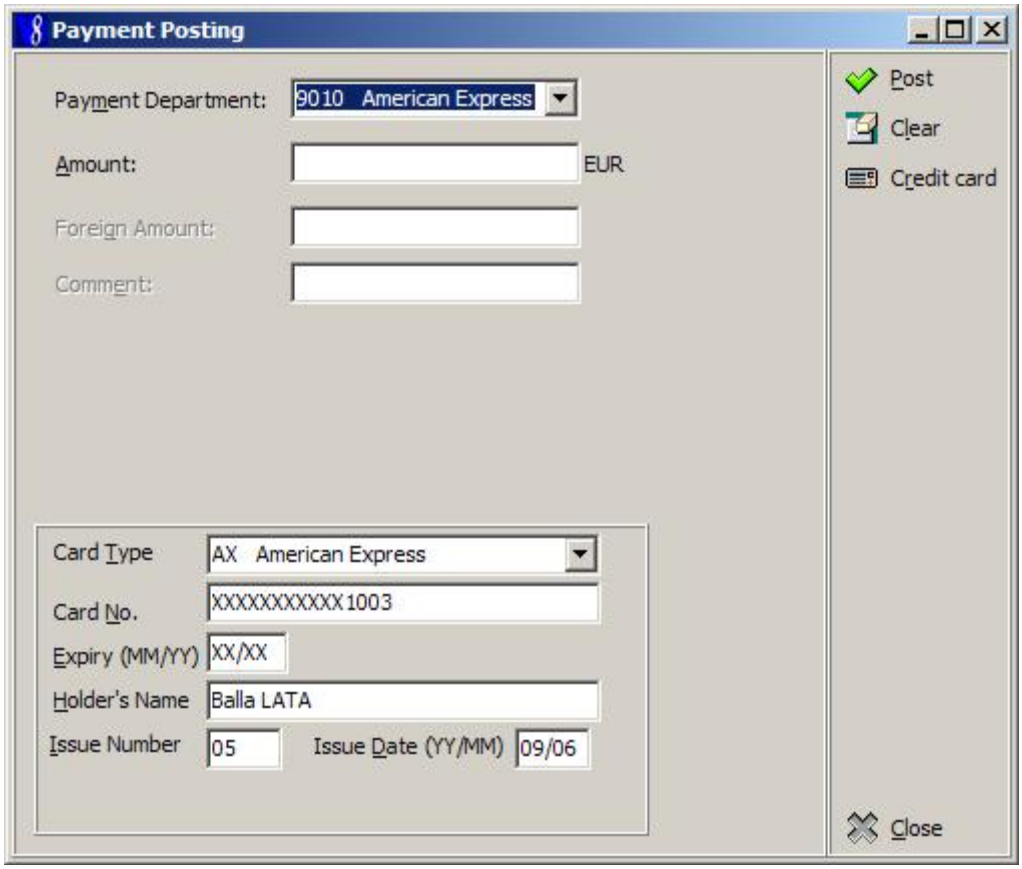


Пользователи, к которым не привязано это право, будут видеть только последние четыре цифры номера карты во всех диалоговых окнах:

Бронь:



Оплата:


Payment Posting
Payment Department:
9010 American Express
Amount:
EUR
Foreign Amount:
Comment:
Card Type
AX American Express
Card No.
XXXXXXXXXX1003
Expiry (MM/YY)
XX/XX
Holder's Name
Balla LATA
Issue Number
05
Issue Date (YY/MM)
09/06
Post
Clear
Credit card
Close

Приведение в соответствие согласно PA-DSS

Отношения между PCI-DSS и PA-DSS

Требования к Стандарту безопасности данных для платежных приложений **(PA-DSS)** базируются на тебованиях и процедурах оценки безопасности Стандарта **PCI-DSS.** В этом документе, который можно найти по адресу: **www.pcisecuritystandards.org**, детально рассказывается о том, что необходимо для соответствия стандарту **PCI-DSS (**а следовательно, каким должно быть платежное приложение, чтобы обеспечить соблюдение клиентом стандарта **PCI-DSS).**

Обычный стандарт **PCI-DSS** не относится напрямую к поставщикам платежных приложений, поскольку большинство поставщиков не хранят, не обрабатывают и не передают информацию о держателях платежных карт. Однако, поскольку эти платежные приложения используются клиентами для хранения, обработки и передачи данных держателей карт, а от клиентов требуется соответствие стандарту **PCI-DSS**, эти платежные приложения должны облегчать, а не затруднять соблюдение клиентами Стандарта **PCI-DSS.**

Вот несколько примеров того, как платежные приложения могут затруднять соответствие Стандарту.
1. Сохранение данных магнитной полосы в клиентской сети после авторизации;
2. Приложения, для надлежащего функционирования которых требуется отключить настройки, которые в Стандарте описаны, как обязательные, например, анти-вирусные программы или межсетевые защитные экраны; и
3. Использование поставщиком небезопасных методов подключения к приложению для предоставления клиентской поддержки.

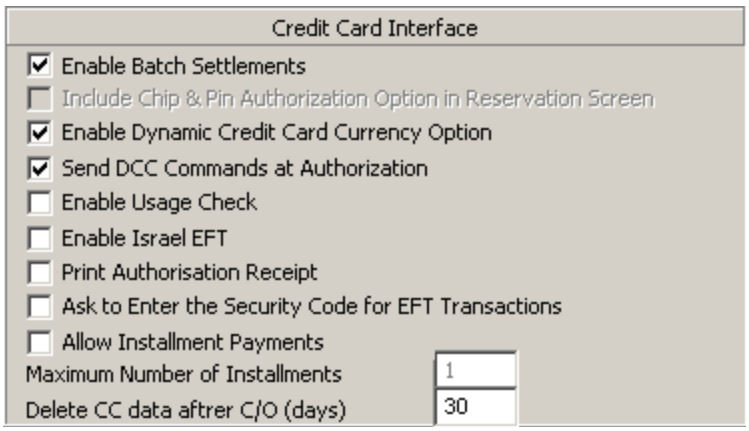
Обеспечивающие безопасность данных платежные приложения, работающие в условиях, где соблюдается стандарт **PCI-DSS**, будут минимизировать риск появления слабых мест в защите, ведущих к компрометации полных данных магнитной полосы, валидационных кодов и значений карт **(CAV2**, **CID**, **CVC2**, **CVV2)**, ПИН-кодов и ПИН-блоков, и наносящих ущерб, являющийся следствием этих слабых мест.

Требования PA-DSS

Следующие требования взяты из ***Стандарта Безопасности Данных для Платежных Приложений*** версии **1.2** от октября **2008г.**

1.1.4 Удалить конфиденциальные данные аутентификации, которые сохранялись предыдущими версиями платежных приложений

Для удаления **PAN** номеров**,** которые сохранялись предыдущими версиями **Fidelio Suite8,** пожалуйста**,** воспользуйтесь следующей опцией**:**



Данные магнитной полосы**,** валидационные коды карт и **PIN-**блоки не хранятся в **Suite8,** а следовательно**,** их не надо удалять**.**

Удаление конфиденциальных данных аутентификации абсолютно необходимо для соответствия стандарту **PCI-DSS.**

Из требований Стандарта **PCI-DSS:**
3.2 Не хранить конфиденциальные данные аутентификации после авторизации (даже в зашифрованном виде).

1.1.5 Удалить любые конфиденциальные данные аутентификации (предварительная авторизация), собранные в результате диагностики и исправления сбоев платежного приложения

Ни при каких обстоятельствах **Suite8** не хранит конфиденциальные данные аутентификации во время операций по диагностике и исправлению неисправностей**.** Вообще отсутствует метод**,** который бы позволял сохранять конфиденциальные данные для целей диагностики и исправления неисправностей**.**

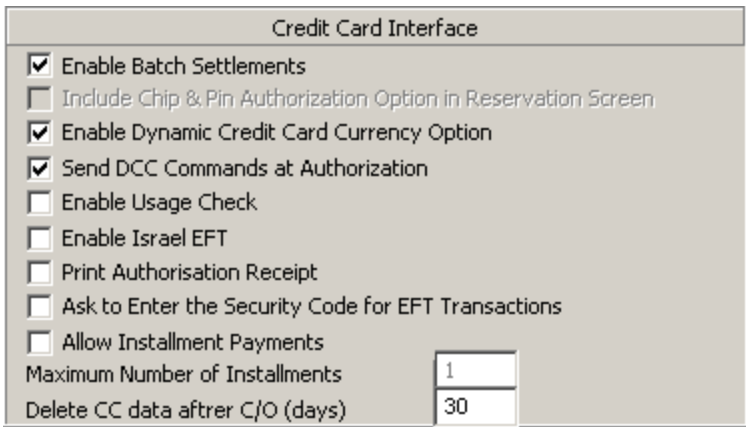
Из требований Стандарта **PCI-DSS:**
3.2 Не хранить конфиденциальные данные аутентификации после авторизации (даже в зашифрованном виде).

2.1 Стереть данные о держателях карт после предопределенного клиентом периода хранения

Из требований Стандарта **PCI-DSS**
3.1 Сократить до минимума хранение данных о держателях карт. Разработать политику сохранения и удаления данных. Ограничить сроки и объемы хранения бизнес необходимостью, юридическими и/или регламентирующими требованиями, задокументированными в политике удаления данных.

Можно указать в конфигурации количество дней хранения номеров кредитных карт, после чего эти данные будут удаляться.

Ввиду поддержания целостности данных, запись базы данных **(XCCS_NUMBER** в таблице **XCCS)** не удаляется, но зашифрованный номер затирается текстовой строкой, уведомляющей об этом пользователя, если позднее пользователь попытается получить доступ к удаленному номеру.



По умолчанию, номер кредитной карты удаляется через **30** дней после выезда гостя.

2.7 Удалить зашифрованные с помощью криптографических ключей материалы или криптограммы, которые сохранялись предыдущими версиями платежного приложения

Из требований **PCI-DSS:**
3.6 Полностью документировать и строго выполнять все процессы и процедуры по использованию криптографических ключей для зашифровки данных о держателях карт.

Suite 8 предлагает функциональность для повторной зашифровки сохраненных номеров кредитных карт**,** для чего используется новый ключ**.** Смотрите подробнее раздел '**Security at the database level**'

Полные данные шифровальных ключей не хранятся в базе данных **Suite8,** так что нет необходимости в инструменте удаления устаревшей криптографической информации**.**

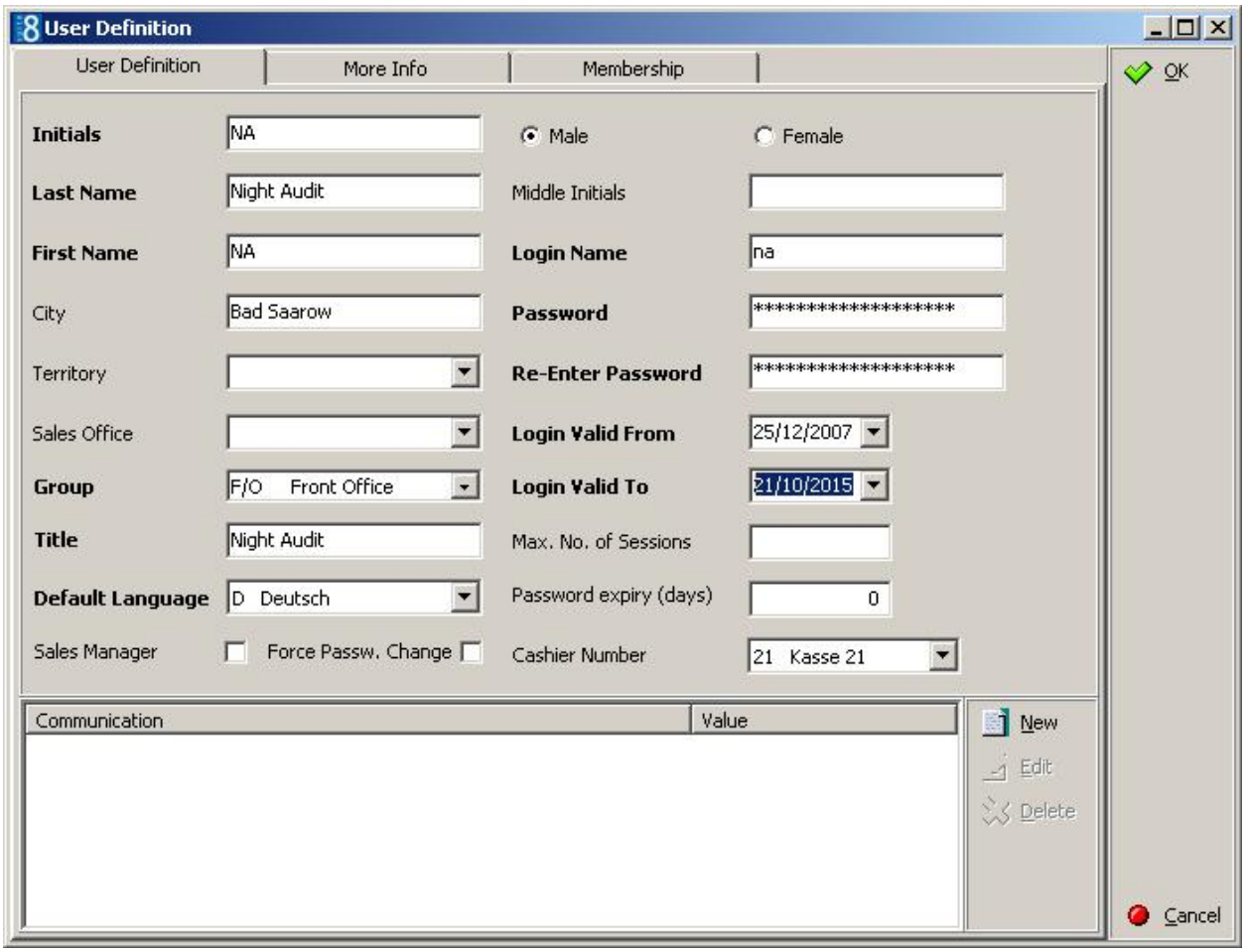
Удаление криптографического материала или криптограмм абсолютно необходимо для соответствия стандарту **PCI-DSS.**

3.1 Использовать уникальные идентификаторы пользователей и надежную аутентификацию для входа под администратором и доступа к данным держателей карт

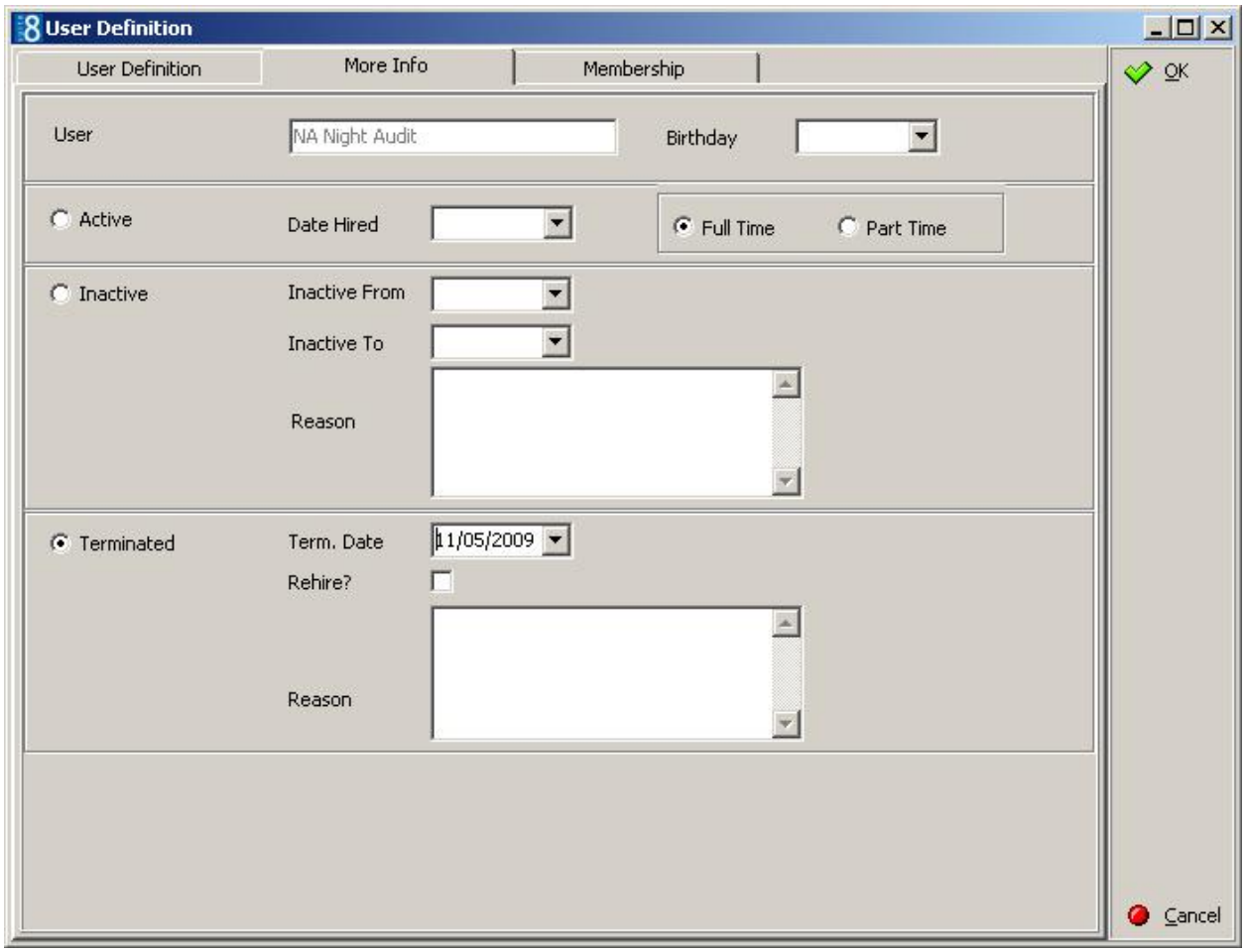
Чтобы соответствовать этому требованию, выполните следующее:

- Никогда не используйте дефолтовые учетные записи/пароли администраторов для входа в **Suite8**
- Убедитесь в том, что аутентификации для дефолтовых учетных записей надежно защищена.
- Отключите учетные записи, которые не используются:

Необходимо либо определить дату истечения срока действия для неиспользуемых учетных записей:



либо отключить их:



- Используйте всегда, если возможно, надежную аутентификацию для доступа к **Suite8** и системе
- Следите за созданием надежной аутентификации для входа в **Suite8**, в соответствии с требованиями стандарта **PCI-DSS**, как указано ниже:

Из требований стандарта **PCI-DSS:**

8.5.8 Не использовать групповые, общие или типовые учетные записи и пароли.

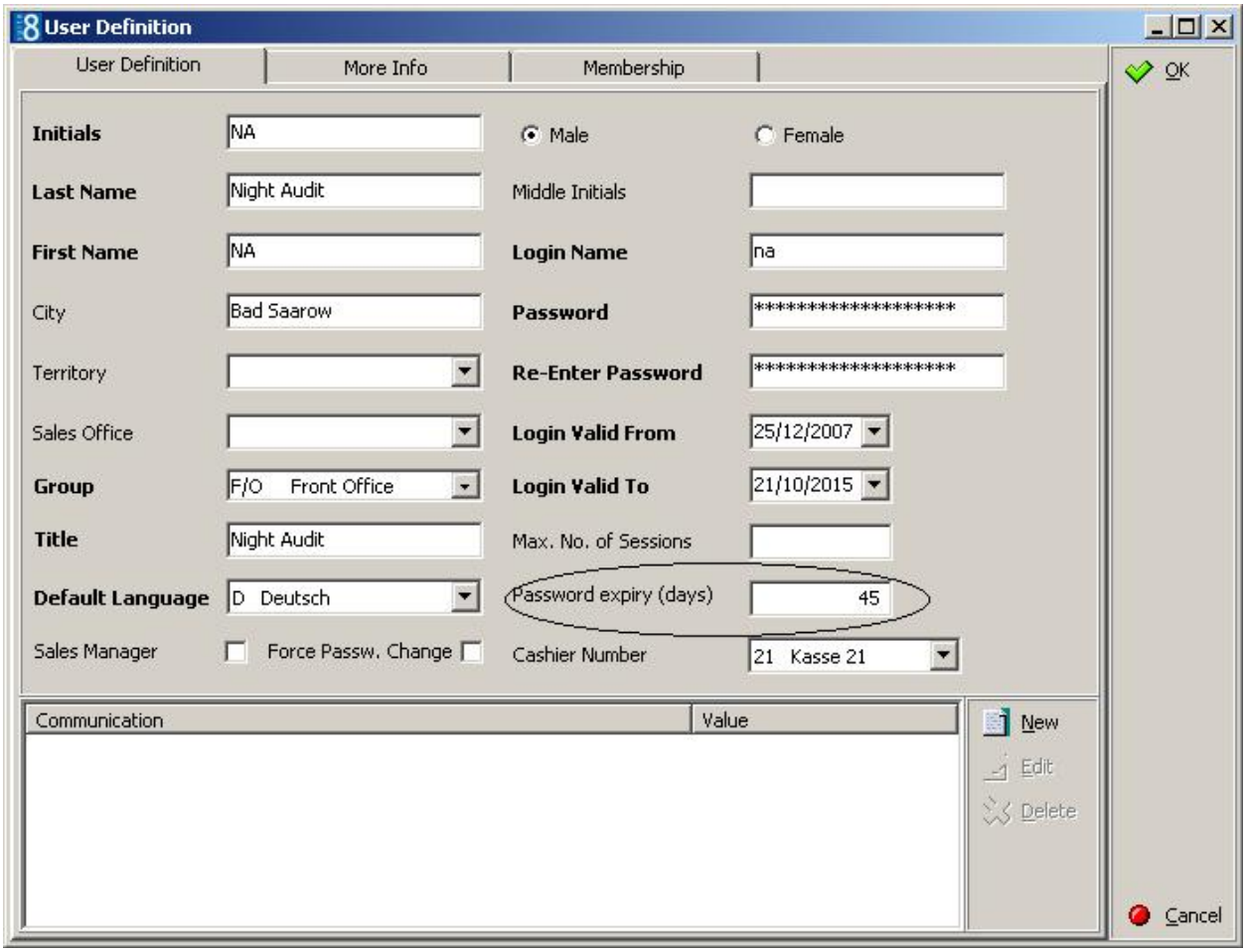
8.5.8.a В части системных компонентов, проверить списки идентификаторов пользователей и убедиться в том, что:

- Типовые учетные записи и идентификаторы пользователей отключены или удалены.
- Общие идентификаторы пользователей для функций системного администратора или других важных операций отсутствуют.
- Общие и типовые идентификаторы пользователей не используются для администрирования каких бы то ни было системных компонентов.

8.5.8.b Проверить политики/процедуры выдачи паролей и убедиться в том, что групповые и общие пароли однозначно запрещены.

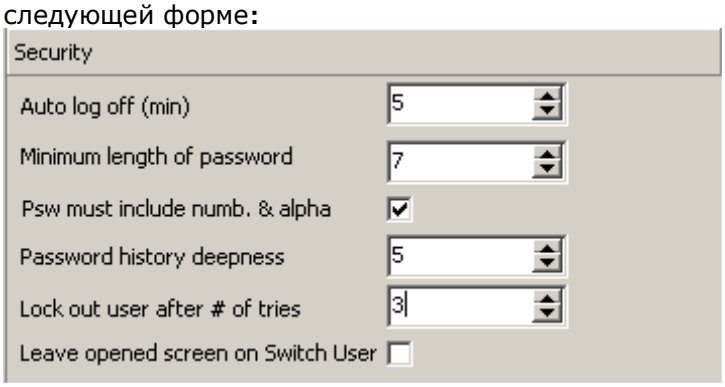
8.5.8.c Заручиться подтверждением системных администраторов в том, что групповые и общие пароли не раздаются даже с учетом просьбы.

8.5.9 Менять пароли пользователей, по меньшей мере, каждые **90** дней.



Убедитесь в том, что срок истечения паролей для всех пользователей настроен на **90** дней максимум.

8.5.10 Использовать пароль длиной не менее семи символов.
Настройки безопасности пароля, используемого при входе в систему, можно задать в следующей форме:

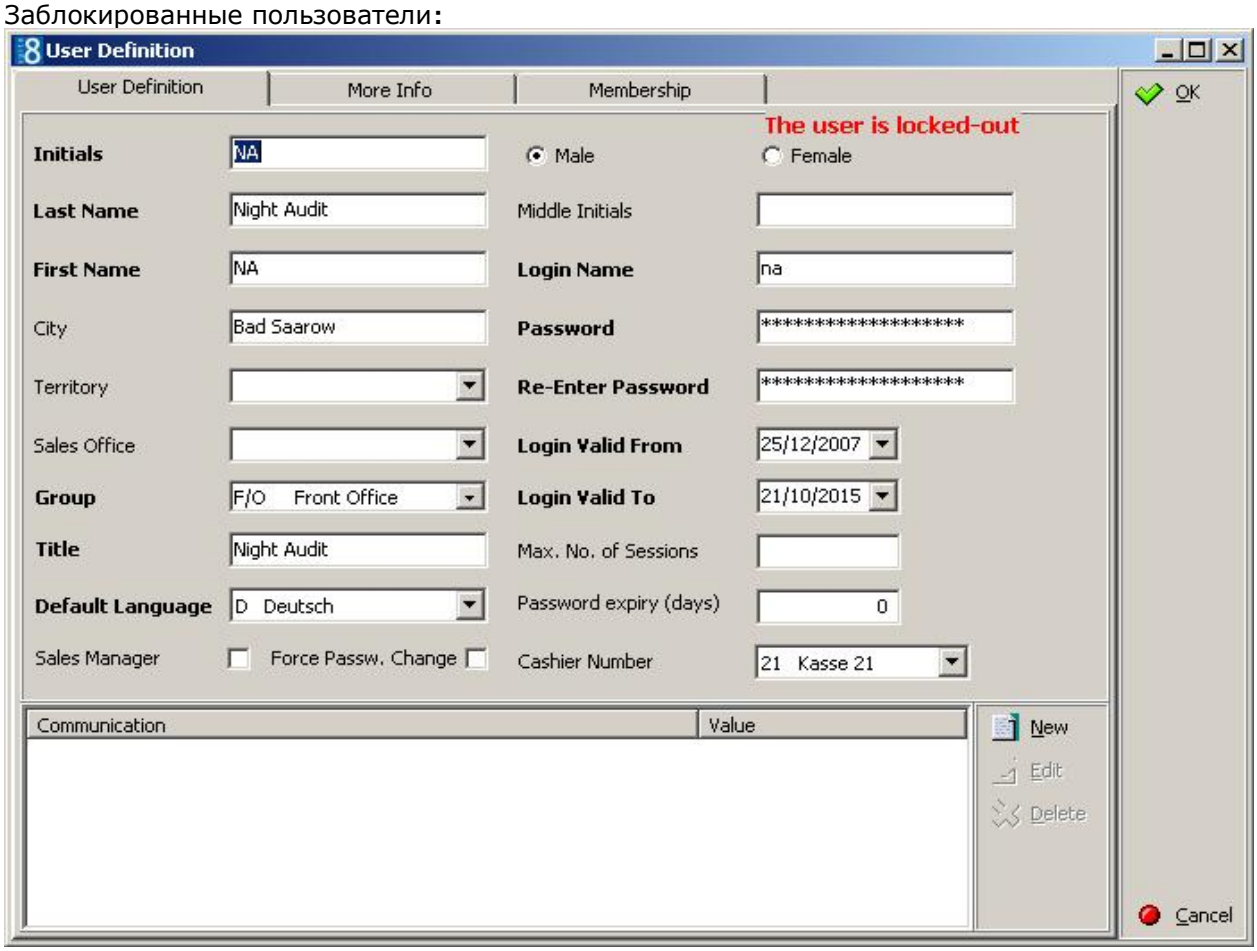


К вышеприведенной форме также относятся следующие требования:

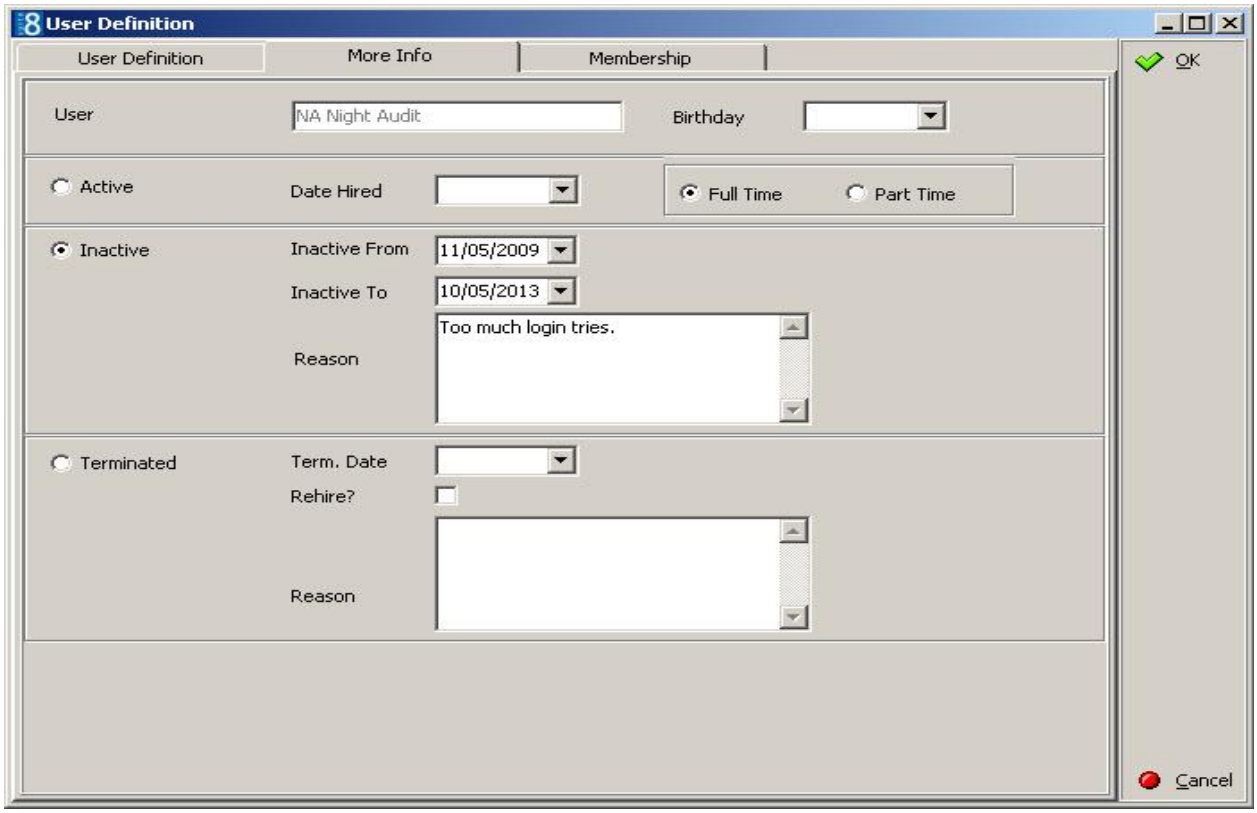
8.5.11 Использовать пароли, содержащие как цифровые, так и буквенные символы.
8.5.12 Не разрешать пользователям при смене пароля вводить в качестве нового пароль, который уже использовался в одной из последних четырех смен паролей.
8.5.13 Ограничить количество неуспешных повторяющихся попыток входа блокировкой идентификатора, если пользователь уже использовал, максимум, **6** попыток.
8.5.14 Настроить продолжительность блокировки на **30** минут минимум, или до тех пор, пока администратор не активирует идентификатор пользователя.
8.5.15 Если сессия находится в простое более **15** минут, требовать от пользователя повторного ввода

пароля для активации терминала.

Заблокированные пользователи:



В **Suite8** отсутствует таймер, позволяющий пользователю залогиниться после многочисленных неудачных попыток входа по истечении заданного периода времени. Подобного пользователя должен активировать супервизор:



3.2 Испольовать уникальные идентификаторы пользователей и надежную аутентификацию для административного доступа и доступа к данным о держателях карт.

Из требований **PCI-DSS:**
8.1 Привязать всем пользователям уникальный идентификатор, перед тем как разрешать им доступ к системным компонентам или данным о держателях карт.
8.2 Помимо привязки уникального идентификатора, использовать, по меньшей мере, один из нижеперечисленных методов аутентификации любого из пользователей:

- Пароль или фраза-пароль
- Двух-факторная аутентификация (например, генераторы одноразовых паролей (токены), смарт-карты, биометрическая идентификация или ключи общего пользования)

Убедитесь в том, что каждый пользователь системы имеет свою уникальную учетную запись, так что доступ к данным о держателях карт всегда привязан к той или иной уникальной учетной записи.

4.2 Включить автоматический контроль событий

Для автоматического контроля событий включите вход в ОС **Windows:**
(article cc 758201 for Microsoft TechNet)

Включить контроль системы защиты

Сервер **2003 Microsoft® Windows®** использует журнал безопасности и системный журнал для хранения собранных событий в системе безопасности.
Перед включением системного журнала и журнала безопасности, необходимо включить аудит для системного журнала и определить количество событий для записи в журнале безопасности. Конфигурируя **а**удит, вы кастомизируете события системного журнала. **А**удит - это процесс, отслеживающий действия пользователей и процессы, благодаря записям выбранных типов событий в журнале безопасности вэб-сервера. Вы можете включить аудит, который будет выполняться с учетом категорий событий безопасности, например:

- Любые изменения в учетных записях пользователей и разрешениях доступа к ресурсам.
- Любые неудачные попытки входа пользователей.

- Любые неудачные попытки доступа к ресурсам.
- Любое изменение системных файлов.

Среди событий в системе безопасности, которые записываются на вэб-сервер, чаще всего встречаются учетные записи пользователей и доступы к ресурсам.

Требования

- Учетные данные: Принадлежность к группе администраторов на локальном компьютере.
- Инструменты: Консоль Управления **Microsoft (MMC)**; Локальная Политика Безопасности

Рекомендация

С точки зрения безопасности, самым правильным будет логиниться на компьютере, используя учетную запись, которая не входит в группу администраторов, а затем использовать команду **Run as** для запуска **IIS Manager**, в качестве администратора. При появлении подсказки, введите **runas /user:*administrative_accountname* "mmc %systemroot%\system32\inetsrv\iis.msc"**.

Процедуры

Чтобы определить или изменить настройки политики безопасности для категории событий на локальном вэб-сервере

1. Откройте **Administrative Tools, a** затем выберите **Local Security Policy.**

2. В консольном дереве, выберите **Local Policies, a** затем **- Audit Policy.**

3. В области деталей, дважды кликните по категории событий, для которых вы хотите изменить настройки политики аудита.

4. На стр. **Properties** для категории событий, выполните следующие требования **(**одно или оба**):**
- При удачной попытке аудита, поставьте галочку в поле **Success.**
- При неудачной попытке аудита, поставьте галочку в поле **Failure.**

5. Нажмите **OK.**

Выполните следующую процедуру на контроллере домена.

Для определения или изменения настроек политики аудита для категории событий в домене или организационной единице, когда вэб-сервер подключен к домену

1. Откройте **Administrative Tools** и затем выберите **Active Directory Users and Computers.**

2. Кликните правой клавишей по соответствующему домену, сайту или организационной единице и затем выберите **Properties.**

3. В закладке **Group Policy**, выберите существующий объект Политики Группы с целью изменения политики.

4. В **Group Policy Object Editor**, в дереве консолей, разверните **Computer Configuration -> Windows Settings -> Security Settings -> Local Policy**, и затем выберите **Audit Policy.**

5. В области деталей, дважды кликните по категории событий, для которых вы хотите изменить настройки политики аудита.

6. Если вы впервые определяете настройки политики аудита для категории событий, поставьте галочку в поле **Define these policy settings.**

7. Выполните следующие действия **(**одно или оба**):**
- При удачной попытке аудита, поставьте галочку в поле **Success.**

- При неудачной попытке аудита, поставьте галочку в поле **Failure**.

8. Нажмите **OK.**

Требование **4.2** соотносится с Требованием **10** стандарта **PCI-DSS:**

Требование 10: Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт

10.1 Установить процесс для увязки всех доступов к системным компонентам **(**особенно доступов с администраторскими привилегиями, например, корневыми**)** с индивидуальным ипользователями.
10.2 Выполнять автоматическую проверку всех системных компонентов для воссоздания следующих событий:
10.2.1 Весь доступ работников к данным о держателях карт
10.2.2 Все действия, выполняемые работником с корневыми или административными привилегиями
10.2.3 Доступ ко всем журналам регистрации событий
10.2.4 Неуспешные попытки логического доступа
10.2 5 Использование механизмов идентификации и аутентификации
10.2.6 Инициализация контрольных журналов
10.2.7 Создание и удаление объектов системного уровня
10.3 Записывать, по меньшей мере, следующие контрольные события для всех системных компонентов по каждому событию:
10.3.1 Идентификация пользователя
10.3.2 Тип события
10.3.3 Дата и время
10.3.4 Индикация успешного или неуспешного события
10.3.5 Происхождение события
10.3.6 Идентичность или название соответствующих данных, системного компонента или ресурса
10.4 Синхронизация всех важных системных часов и времени.
10.5 Безопасность контрольных журналов, недопущение каких-либо изменений в них.
10.5.1 Ограничение просмотров контрольного журнала теми работниками, которым это необходимо в силу служебных обязанностей.
10.5.2 Защита файлов контрольного журнала от неавторизованных изменений.
10.5.3 Делать быстро бэкап файлов контрольного журнала на централизованном лог-сервере или носителях информации, которые трудно изменить.
10.5.4 4 Записывать логи для наружных технологий на лог-сервер на внутреннюю **LAN.**
10.5.5 Использовать мониторинг целостности файлов или ПО для обнаружения изменений в логах, чтобы не допустить изменений существующих лог-данных без принудительной генерации алертов **(**хотя добавляемые новые данные не должны вызывать алерты**).**
10.6 По меньшей мере, один раз в день проверять логи для всех системных компонентов. Проверять логи надо на тех серверах, которые выполняют защитные функции. Например, система обнаружения вторжения **(IDS)** и серверы **(**например, **RADIUS)** протоколов AAA **(**аутентификация, авторизация и учет**).** Прим: Сбор логов, парсинг и алерты могут использоваться в целях соответствия требованию **10.6**
10.7 Храните историю контрольного журнала, по меньшей мере, один год, причем так, чтобы моментально можно было поднять для анализа данные за три месяца **(**например, в режиме он-лайн, архивные данные или восстанавливаемые из бэкапа**).**

Все пользовательские лог-файлы версии **8** записываются автоматически и не могут быть изменены никем из пользователей.

4.2.b Отключение ведения записей

Журнал пользователей **Suite8** не может быть деактивирован. Никакой другой журнал записей не может быть ни при каких обстоятельствах деактивирован, так как это бы противоречило стандарту **PCI-DSS.**

6.1 Безопасно работать с беспроводными технологиями

Если для работы с **Suite8** используются беспроводные технологии**,** убедитесь в том**,** что подходящий межсетевой экран установлен**,** как описано в **PCI-DSS (**требование **1.2.3).**

Если используются беспроводные подключения**,** убедитесь в том**,** что внешние межсетевые экраны установлены между беспроводными сетями и системами**,** хранящими данные о держателях карт**,** и что эти межсетевые экраны не пропускают или контролируют любой трафик от беспроводной среды к среде данных о держателях карт**.**

Из требований **PCI-DSS:**
1.2.3 Установите внешние межсетевые экраны между беспроводными сетями и средой данных о держателях карт, и сконфигурите эти межсетевые экраны, так чтобы они не пропускали или контролировали (если такой трафик необходим для ведения бизнеса) любой трафик от беспроводной среды к среде данных о держателях карт.

2.1.1 Для беспроводных сред, подсединенных к среде данных о держателях карт или передающих данные о держателях карт, измените дефолтовые настройки производителя, включая, но не ограничиваясь дефолтовой настройкой ключей шифрования, паролей и строк имени и пароля SNMP. Убедитесь в том, что настройки безопасности беспроводного устройства включены для использования технологии криптостойкого шифрования для аутентификации и передачи данных.

6.2 Безопасно передавать данные о держателях карт через беспроводные сети

Если беспроводные технологии используются в среде **Suite8,** убедитесь в том**,** что подходящий межсетевой экран установлен**,** как описано в стандарте **PCI-DSS (**требования **1.2.3 , 2.1.1** и **4.1.1),** и что соблюдаются нижеупомянутые требования**:**

1.2.3
Если используются беспроводные технологии**,** убедитесь в том**,** что установлены внешние межсетеве экраны между беспроводными сетями и системами**,** хранящими данные о держателях карт**,** и что эти межсетевые экраны не пропускают или контролируют любой трафик от беспроводной среды к среде данных о держателях карт**.**

2.1.1

- Дефолтовые ключи шифрования изменены в процессе установки, и меняются всякий раз, когда кто-либо, владеющий соответствующей информацией, увольняется, или изменяется его должность
- Дефолтовые строки имени и пароля SNMP на беспроводных устройствах изменены
- Дефолтовые пароли/фразы-пароли на точках доступа изменены
- Оборудование или беспроводные устройства обновляются для поддержания криптостойкого шифрования для аутентификации и передачи данных через беспроводные сети (например, WPA/WPA2)
- Прочее в вопросах безопасности-

4.1.1
Убедитесь в том**,** что беспроводные сети**,** передающие данные о держателях карт или подключенные к среде данных о держателях карт**,** используют **use** наиболее эффективные методы **(**например**, IEEE 802.11i)** для криптостойкого шифрования для аутентификации и передачи данных**.**

- Ø В случае новых беспроводных установок запрещается использование **WEP** позднее **31** марта **2009**г**.**
- Ø В случае текущих беспроводных установок запрещается использование **WEP** позднее **30** июня **2010**г**.**

9.1 Данные о держателях карт никогда не хранить на сервере, подключенном к Интернету

Не храните данные о держателях карт в системах, доступных через интернет (например, на вэб-сервере, и сервер базы данных должен быть отдельным).

Хранение данных о держателях карт на сервере, подсоединенном к интернету, будет означать несоблюдение стандарта **PCI-DSS.**

Из требований **PCI-DSS:**
1.3.2 Ограничить входящий трафик IP адресами в DMZ

10.1 Надежно доставлять обновления платежных приложений через удаленный доступ

Если обновления для платежного приложения доставляются посредством удаленного доступа в системы клиентов, то производители программного обеспечения должны сказать своим клиентам, что переход на технологии удаленного доступа нужен только для загрузки данных от производителя, и что по завершении загрузки удаленный доступ надо немедленно отключить. Если обновления доставляются через VPN или другое высоко-скоростное соединение, то производители программного обеспечения должны посоветовать клиентам должным образом сконфигурить межсетевой экран или персональный межсетовой экран для обеспечения постоянного соединения.

- Получите удаленные обновления платежного приложения через защищенные модемы, согласно стандарту **PCI-DSS,** требование **12.3.**
- Если компьютер подключен через **VPN** или другое высоко-скоростное соединение, получите удаленные обновления платежного приложения через межсетевой экран или персональный межсетевой экран, согласно стандарту **PCI-DSS (**требование **1** или **12.3.9).**

Из требований **PCI-DSS:**
Требование 1: Установите и поддерживайте конфигурацию межсетевого экрана для защиты данных о держателях карт
12.3.9 Активируйте технологии удаленного доступа только по просьте производителей, когда это необходимо, и немедленно отключайте после использования

11.2 Использовать двух-факторную аутентификацию для удаленного доступа к платежному приложению

Используйте двух-факторную аутентификацию (идентификатор пользователя и пароль и в качестве дополнительной аутентификации, например, сертификат), если в **Suite8** можно зайти удаленно.

Из требований **PCI-DSS:**
8.3 используйте двух-факторную аутентификацию для удаленного доступа (доступ сетевого уровня, происходящий от внешней сети) к сети работниками, администраторами и третьими сторонами. Используйте технологие, такие как, например, удаленная аутентификация и служба удаленной аутентификации по телефонным линиям (RADIUS); система управления доступом для контроллера доступа к терминалу (TACACS) с токенами; или VPN (на базе SSL/TLS или IPSEC) с индивидуальными сертификатами.

11.3 Осуществлять защищенный удаленный доступ к ПО

Установить и использовать защищенные опции для ПО удаленного доступа, если ПО удаленного доступа необходимо для удаленного доступа к платежному приложению или платежной среде.

- Клиенты и все службы **Micros-Fidelio** получили инструкцию изменить все дефолтовые настройки в ПО удаленного доступа, и также изменить дефолтовые пароли на уникальные для каждой учетной записи.
- Клиентам и всем службам **Micros-Fidelio** дана рекомендация принимать подключения только от известных/определенных **IP** и **MAC а**дресов.
- Клиентам и всем службам **Micros-Fidelio** дана рекомендация использовать сильную аутентификацию или комплексные пароли для всех пользователей, согласно требованиям **8.1, 8.3** и **8.5.8-8.5.15** стандарта **PCI-DSS.**

- **А**утентификация и комплексные пароли для регистрации входа, в сответствии с требованиями **8.1,8.3** и **8.5.8-8.5.15** стандарта **PCI-DSS.**
  - **PCI-DSS 8.1** Все удаленные пользователи должны иметь уникальное имя пользователя.
  - **PCI-DSS 8.3** Дополнительная аутентификация необходима для каждого уникального пароля. Руководство содержит примеры дополнительной аутентификации, коими могут быть пароли, токены и биометрики.
  - **PCI-DSS 8.5.8** Клиентам и всем службам **Micros-Fidelio** рекомендуется не использовать общие, групповые и типовые идентификаторы для удаленного доступа, и также ни одна учетная запись не должна иметь общий пароль.
  - **PCI-DSS 8.5.9** Клиенты и все службы **Micros-Fidelio** получили инструкцию заставлять пользователей менять свои пароли удаленного доступа, по меньшей мере, каждые **90** дней.
  - **PCI-DSS 8.5.10** Клиенты и все службы **Micros-Fidelio** получили инструкцию следить за тем, чтобы пароли пользователей были не менее семи символов в длину для всех удаленных соединений.
  - **PCI-DSS 8.5.11** Клиенты и все службы **Micros-Fidelio** получили инструкцию следить за тем, чтобы пароли для удаленного доступа пользователей включали как цифровые, так и буквенные символы.
  - **PCI-DSS 8.5.12** Клиенты и все службы **Micros-Fidelio** получили инструкцию следить за тем, чтобы новые пароли удаленного доступа отличались от пяти предыдущих паролей, которые были в использовании.
  - **PCI DSS 8.5.13** Клиенты и все службы **Micros-Fidelio** получили инструкцию следить за тем, чтобы удаленные учетные записи пользователей блокировались после трех неправильных попыток входа.
  - **PCI DSS 8.5.14** Клиенты и все службы **Micros-Fidelio** получили инструкцию следить за тем, чтобы заблокированная учетная запись удаленного доступа пользователя оставалась заблокированной на **30** минут или до тех пор, пока системный администратор не перегрузит учетную запись.
  - **PCI DSS 8.5.15** Клиенты и все службы **Micros-Fidelio** получили инструкцию проследить за тем, чтобы в настройках времени для прерывания сессий/системы из простоя было проставлено значение **15** минут или меньше для решений удаленного доступа.

- **PCI-DSS 4.1** Клиенты и все службы **Micros-Fidelio** получили инструкцию Использовать протоколы криптостойкого шифрования, такие как **SSL/TLS** или **IPSEC** при использовании решений удаленного доступа.
- **PCI-DSS 4.1.a** Клиентам и всем службам **Micros-Fidelio** рекомендовано использовать кодирование всякий раз при передаче данных о держателях карт или получении их через открытые сети общего пользования, такие как интернет.
- Проверять, что криптостойкое шифрование используется при передаче данных
- Для подключения **SSL**, убедитесь в том, что **HTTPS** появляется как часть **browser Universal Record Locator (URL)**, и что никакие данные о держателях карт не требуются, когда **HTTPS** не появляется в **URL**
- Убедитесь в том, что принимаются только проверенные **SSL/TLS** ключи**/се**ртификаты
- Убедитесь в том, что надлежащая криптографическая сложность используется для методологии шифрования **(**Проверьте рекомендации**/** позитивный опыт производителей**)**

- **PCI-DSS 4.1.1.a** Надлежащая методология шифрования используется для любых беспроводных передач данных, например: защищенный доступ по **Wi-Fi (WPA** или **WPA2)**,**IPSEC VPN**, или **SSL/TLS**
- **PCI-DSS 4.1.1.b** Если используется **WEP:**
  - Минимум **104-**битный шифровальный ключ и **24-**битное значение инициализации.
  - Используется только в сочетании с защищенным достутом по **Wi-Fi** технологии **(WPA** или **WPA2), VPN** или **SSL/TLS**
  - Общие **WEP** ключи меняются, по меньшей мере, один раз в квартал **(**или автоматически, если технология позволяет**)**
  - Общие **WEP** ключи меняются всякий раз, когда изменяется доступ персонала к ключам
  - Доступ ограничивается и зависит от **MAC а**дресов
- **PCI-DSS 8.5.13** Клиенты и торговые посредники**/**специалисты по системной интеграции получили инструкции следить за тем, чтобы учетные записи удаленного доступа блокировались после трех неудачных попыток входа.
- Удаленные пользователи получили инструкции инициировать **VPN со**единение через межсетевые защитные экраны.
- Полное ведение журнальных записей должно быть активировано для всех удаленных сессий.
- Клиенты и торговые посредники**/**специалисты по системной интеграции получили инструкции ограничить доступ к паролям клиентов авторизованным персоналом специалистов по системной интеграции.
- Все пароли клиентов устанавливаются в соответствии с требованиями **requirements 8.1,8.2,8.4** и **8.5** стандарта **PCI-DSS:**
- **PCI-DSS 8.1** У всех клиентов и торговых посредников**/**специалистов по системной интеграции должны быть идентификаторы с уникальным именем пользователя.
- **PCI-DSS 8.2** Все идентификаторы удаленных пользователей для клиентов и торговых посредников**/**специалистов по системной интеграции должны также включать дополнительную аутентификацию. Эта практика должна быть должным образом задокументирована.
- **PCI-DSS 8.4** Шифруйте все пароли при передаче данных или при хранении их на всех системных компонентах.
- **PCI-DSS 8.5.1** Контролируйте удаление и изменение идентификаторов пользователей, параметров доступа и других объектов идентификации.
- **PCI-DSS 8.5.2** Проверяйте идентификатор пользователя, перед тем как выполнить обнуление паролей.
- **PCI-DSS 8.5.3** Установите для паролей новых пользователей уникальное значение для каждого пользователя сразу же после первого входа в систему.
- **PCI-DSS 8.5.4** Немедленно аннулируйте доступ для уволившихся пользователей.

- **PCI-DSS 8.5.5** Удаляйте неактивные учетные записи пользователей, по меньшей мере, каждые **90** дней.
- **PCI-DSS 8.5.6** Включайте учетные записи, используемые поставщиками для удаленной поддержки, только на необходимый отрезок времени.
- **PCI-DSS 8.5.7** Передайте процедуры, касающиеся паролей, всем пользователям. У которых есть доступ к данным о держателях карт.
- **PCI-DSS 8.5.8** Групповые, общие и типовые идентификаторы никогда не должны использоваться.
- **PCI-DSS 8.5.9** Пароли необходимо менять каждые **90** дней.
- **PCI-DSS 8.5.10** Пароли должны включать минимум семь символов.
- **PCI-DSS 8.5.11**Пароли должны быть буквенно-цифровыми.
- **PCI-DSS 8.5.12** История паролей должна быть настроена таким образом, чтобы не разрешать использование предыдущих пяти паролей.
- **PCI-DSS 8.5.13** Доступ должен блокироваться после не более пяти неудачных попыток аутентификации.
- **PCI-DSS 8.5.14** Продолжительность блокировки должна быть не менее **30** минут.
- **PCI-DSS 8.5.15** Сессии должны блокироваться после **15** минут бездействия.
- **PCI-DSS 8.5.16** Аутентифицируйте доступ к любой базе данных, содержащей данные о держателях карт.

12.1 Защищенная передача данных о держателях карт через сети общего пользования

Suite8 Micros Fidelio никогда не будет требовать передачи конфиденциальной информации о держателях карт через сети общего пользования**.** Если же когда**-**либо понадобится это сделать**,** выполняйте следующие шаги**:**

Внедрите и используйте **SSL** для защищенной передачи данных о держателях карт через сети общего пользования**,** в соответствии с требованием **4.1** стандарта **PCI-DSS.**

Из требований **PCI-DSS:**

4.1 Используйте криптостойное шифрование и защищенные протоколы типа **SSL/TLS** или **IPSEC** для сохранения конфиденциальной информации о держателях карт во время передачи через открытые сети общего пользования**.**
*Примеры открытых сетей общего пользования**,** оговариваемых в **PCI-DSS:***
- *Интернет**,***
- *Беспроводные технологии**,***
- *Глобальная система для мобильной коммуникации **(GSM)** и*
- *Общая служба пакетной радиопередачи **(GPRS).***

12.2 Зашифровывать данные о держателях карт**,** отправляемые с помощью технологий отправки сообщений конечному пользователю

Suite8 Micros Fidelio никогда не потребует передачи конфиденциальной информации о держателях карт с помощью технологий отправки сообщений конечному пользователю**.** Если когда**-**либо это понадобится сделать**,** выполняйте следующие шаги**:**

Убедитесь в том**,** что незакодированные номера **PAN (**номера кредитных карт**)** НИКОГДА не отправляются с использованием технологий отправки сообщений конечному пользователю **(**например**, e-mail,** мгновенные сообщения**,** чат**).**
Suite8 не содержит механизмов отправки сообщений**.**

Из требований **PCI-DSS:**
4.2 Никогда не отправляйте незакодированные PAN номера с использованием технологий отправки сообщений конечному пользователю (например, e-mail, мгновенные сообщения, чат).

13.1 Зашифровывать административный неконсольный доступ

Подключения к клиентам для неконсольного администрирования должны выполняться через надежное **CISCO** или **ASTARO VPN** соединение**.** ***Telnet** или **rlogin** никогда не должны использоваться для административного доступа.*

Внедрить и использовать **SSH, VPN** или **SSL/TLS** для кодирования любого неконсольного административного доступа к платежному приложению или серверам в среде данных о держателях карт**.**

Из требований **PCI-DSS:**
2.3 Шифровать любой административный неконсольный доступ. Использовать технологии типа SSH, VPN или SSL/TLS для управления через интернет и другого административного неконсольного доступа.

Базы данных Oracle

Suite8 устанавливается на базе данных О**racle.**
Micros-Fidelio регулярно проверяет Базу Данных **Oracle** на уязвимости через информационный бюллетень разработчиков и **Oracle-Metaframe.**
Любая коррекция уязвимости по мере ее выхода будет добавляться в установочную документацию по **Suite8 Micros-Fidelio (Suite8 Installshield).**

Об этом Руководстве

Это руководство ежегодно пересматривается и обновляется, как это необходимо, всеми изменениями, как основными, так и менее значимыми, которые добавляются в ПО **Fidelio Suite8.**

Это ежегодно пересматриваемое и обновляемое руководство отображает любые изменения, вносимые в документацию по стандарту **PA-DSS.**