Oracle® Hospitality Cruise SPMS

PA-DSS Implementation Guide

Release 7.30.858

December 2015

Contents

Figures **5**

Preface **6**

Note.................... 6

Audience 6

Customer Support.................... 6

Documentation.................... 6

Revision History.................... 6

1 Introduction and Scope **7**

1.1 Introduction.................... 7

1.2 What is Payment Application Data Security Standard (PA-DSS)?.................... 7

1.3 Distribution and Updates 7

1.4 Versions.................... 7

2 Secure Deletion of Sensitive Data and Protection of Stored Cardholder Data.......... **8**

2.1 Merchant and Reseller/Integrator Applicability 8

2.2 Secure Deletion Instructions 9

2.3 Locations of Stored Cardholder Data 12

2.4 Instructions for Annually Rotating Keys.................... 12

2.5 Disable System Restore Points.................... 16

Steps to turn off System Restore 16

2.6 Troubleshooting Procedures 16

PA-DSS Requirements Reference.................... 17

3 Password and Account Settings **18**

3.1 Access Control.................... 18

3.2 Password Controls.................... 24

PA-DSS Requirements Reference:.................... 24

4 Logging **25**

4.1 Merchant Applicability 25

4.1 Configuring Log Settings.................... 25

4.2 PCI Guidelines for Logging.................... 25

PA-DSS Requirements Reference:.................... 25

5 Wireless Networks.................... **26**

5.1 Merchant Applicability 26

5.2 PCI Requirements 26

PA-DSS Requirements Reference.................... 27

6 Network Segmentation.................... **28**

6.1 Merchant Applicability 28

PA-DSS Requirements Reference.................... 28

7 Secure Remote Software Updates **29**

7.1 Merchant Applicability 29

7.2 Acceptable Use Policy 29

7.3 Personal Firewall 29

7.4 Remote Update Procedures....................29

8 Installation of SFTP Client.................... 31

PA-DSS Requirements Reference....................36

9 Remote Access 38

9.1 Merchant Applicability 38

9.2 Remote Access Software Security Configuration....................38

PA-DSS Requirements Reference....................39

10 Encrypting Network Traffic 40

10.1 Transmission of Cardholder data 40

10.2 Email and Cardholder data....................40

10.3 Non-Console administrative access 40

PA-DSS Requirements Reference....................40

Figures

Figure 1 - Test Figure .... **Error! Bookmark not defined.**
Figure 2: ADPI Interface 8
Figure 3: IFT Tools 9
Figure 4: IFT Tools, Encryption Key Manager 10
Figure 5: IFT Tools, Encryption Key Manager Reminder 10
Figure 6: IFT Tools, Encryption Key Manager Completion 11
Figure 7: 14 Day Encryption Key Expiry Warning 12
Figure 8: IFT Tools 13
Figure 9: Encryption Key Manager 13
Figure 10: Encryption Key Manager 14
Figure 11: 15
Figure 12: FC Management, Database Parameters 18
Figure 13: Configure Password History 19
Figure 14: Configure Password Max Age 19
Figure 15: Configure Password Minimum Length 20
Figure 16: Require lower case password characters 20
Figure 17: Require Upper Case password characters 21
Figure 18: Require special characters 21
Figure 19: Require password rotation 22
Figure 20: Require passwords to require numbers 22
Figure 21: Require password expiration 23
Figure 22: WinSCP Installation Security Warning 31
Figure 23: WinSCP Select Language Dialogue 31
Figure 24: WinSCP Setup Wizard 32
Figure 25: WinSCP License Agreement 32
Figure 26: WinSCP Setup Type 33
Figure 27: WinSCP User Settings 33
Figure 28: WinSCP Setup Summary 34
Figure 29: WinSCP Setup Progress Bar 34
Figure 30: WinSCP Login Window 35
Figure 31: WinSCP Save Session 35
Figure 32: WinSCP Stored Session 36
Figure 33: FTP Server RSA2 Key Fingerprint 36

Preface

Note

The rebranding for the latest version of this documentation set is in development as part of post MICROS acquisition activities. References to former MICROS product names may exist throughout this existing documentation set.

Audience

This document is intended for Merchants and Integrators who intend to use Oracle Hospitality Cruise SPMS in a PCI compliant merchant setup.

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

https://support.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screen shots of each step you take

Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at http://docs.oracle.com

Revision History

Date	Description of Change
December 15th, 2015	• Initial publication.

1 Introduction and Scope

1.1 Introduction

The purpose of this PA-DSS Implementation Guide is to instruct merchants on how to implement Ship Property Management System (SPMS) Version 7.30.858 by Oracle Hospitality Cruise, into their environment in a PA-DSS compliant manner. It is not intended to be a complete installation guide. SPMS, if installed according to the guidelines documented here, should facilitate and support a merchant's PCI compliance.

1.2 What is Payment Application Data Security Standard (PA-DSS)?

The Payment Application Data Security Standard (PA-DSS) is a set of security standards that were created by the PCI SSC to guide payment application vendors to implement secure payment applications.

1.3 Distribution and Updates

This PA-DSS Implementation Guide should be disseminated to all relevant application users including merchants. It should be updated at least annually and after changes in the software. The annual review and update should include new software changes as well as changes in the PA-DSS standard.

Updates to the PA-DSS Implementation Guide can be obtained by Oracle Hospitality Cruise technical support.

1.4 Versions

This PA-DSS Implementation Guide references both the PA-DSS and PCI requirements. The following versions were referenced in this guide.

- PA-DSS version 2.0
- PCI DSS version 2.0

2 Secure Deletion of Sensitive Data and Protection of Stored Cardholder Data

2.1 Merchant and Reseller/Integrator Applicability

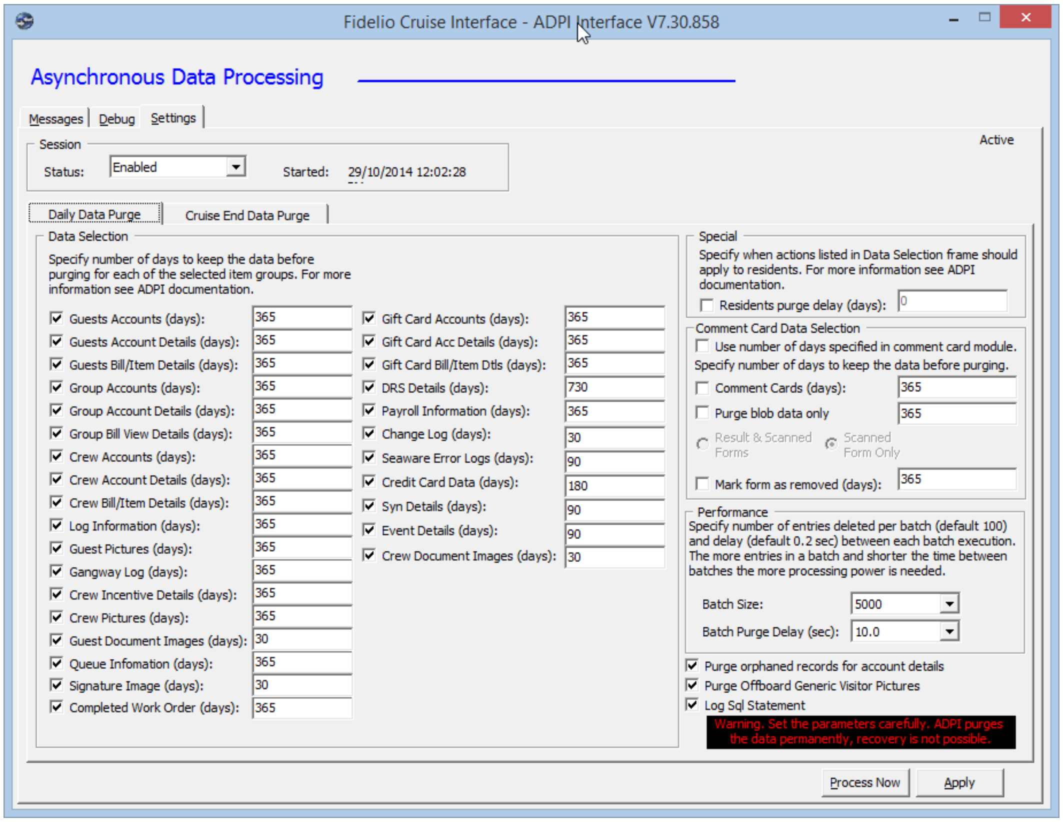
It is the merchant's responsibility to remove any magnetic stripe data, card validation values or codes, PINs or PIN block data, cryptographic key material, or cryptograms stored by previous versions of the SPMS software.

It is the responsibility of Oracle Hospitality Cruise to provide a means to do this. Removal of this prohibited historical data is required for PCI compliance.

To be PCI compliant, a merchant must have a data-retention policy which defines how long cardholder data will be kept. Cardholder data exceeding the customer-defined retention period must be purged.

To do so, follow these instructions:

Launch IFC ADPI.exe and then configure to the customers defined retention period



Fidelio Cruise Interface - ADPI Interface V7.30.858

Asynchronous Data Processing

Session

Status: Enabled

Started: 29/10/2014 12:02:28

Data Selection

Specify number of days to keep the data before purging for each of the selected item groups. For more information see ADPI documentation.

☑ Guests Accounts (days):	365
☑ Guests Account Details (days):	365
☑ Guests Bill/Item Details (days):	365
☑ Group Accounts (days):	365
☑ Group Account Details (days):	365
☑ Group Bill View Details (days):	365
☑ Crew Accounts (days):	365
☑ Crew Account Details (days):	365
☑ Crew Bill/Item Details (days):	365
☑ Log Information (days):	365
☑ Guest Pictures (days):	365
☑ Gangway Log (days):	365
☑ Crew Incentive Details (days):	365
☑ Crew Pictures (days):	365
☑ Guest Document Images (days):	30
☑ Queue Infomation (days):	365
☑ Signature Image (days):	30
☑ Completed Work Order (days):	365
☑ Gift Card Accounts (days):	365
☑ Gift Card Acc Details (days):	365
☑ Gift Card Bill/Item Dtls (days):	365
☑ DRS Details (days):	730
☑ Payroll Information (days):	365
☑ Change Log (days):	30
☑ Seaware Error Logs (days):	90
☑ Credit Card Data (days):	180
☑ Syn Details (days):	90
☑ Event Details (days):	90
☑ Crew Document Images (days):	30

Special

Specify when actions listed in Data Selection frame should apply to residents. For more information see ADPI documentation.

☐ Residents purge delay (days): 0

Comment Card Data Selection

☐ Use number of days specified in comment card module.

Specify number of days to keep the data before purging.

☐ Comment Cards (days): 365

☐ Purge blob data only 365

○ Result & Scanned Forms ● Scanned Form Only

☐ Mark form as removed (days): 365

Performance

Specify number of entries deleted per batch (default 100) and delay (default 0.2 sec) between each batch execution. The more entries in a batch and shorter the time between batches the more processing power is needed.

Batch Size: 5000

Batch Purge Delay (sec): 10.0

☑ Purge orphaned records for account details

☑ Purge Offboard Generic Visitor Pictures

☑ Log Sql Statement

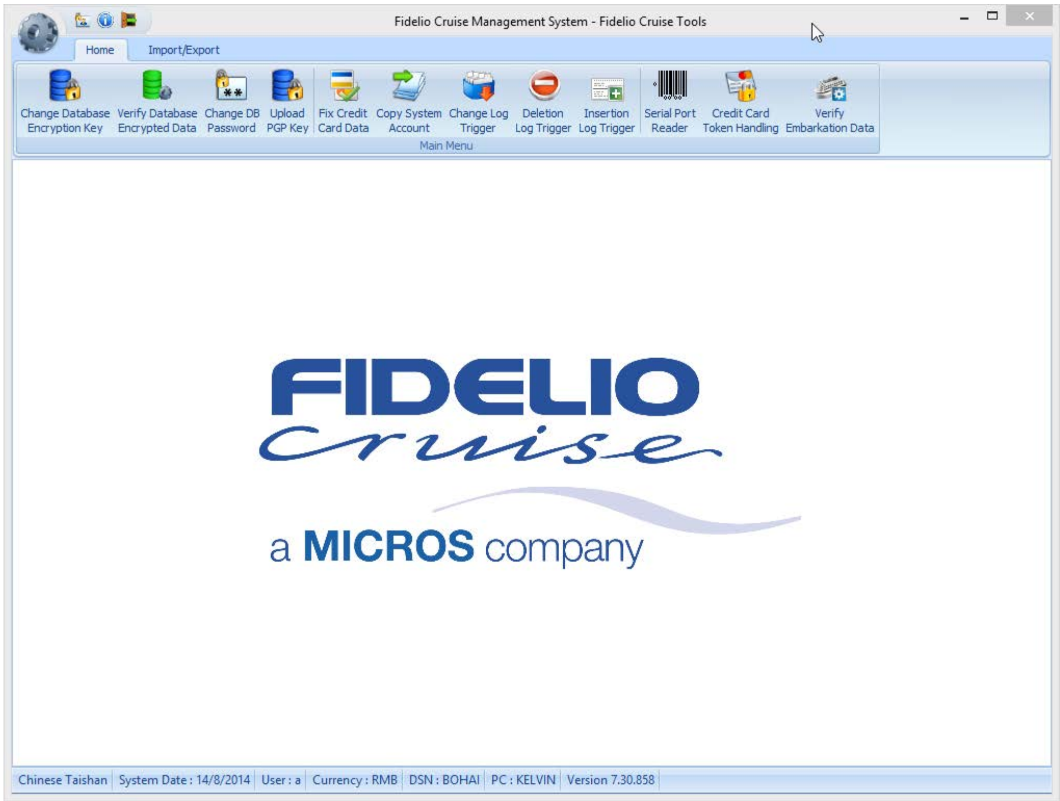
Warning. Set the parameters carefully. ADPI purges the data permanently, recovery is not possible.

Figure 1: ADPI Interface

2.2 Secure Deletion Instructions

The following instructions can be used to securely delete prohibited historical data and to purge cardholder data after expiration:

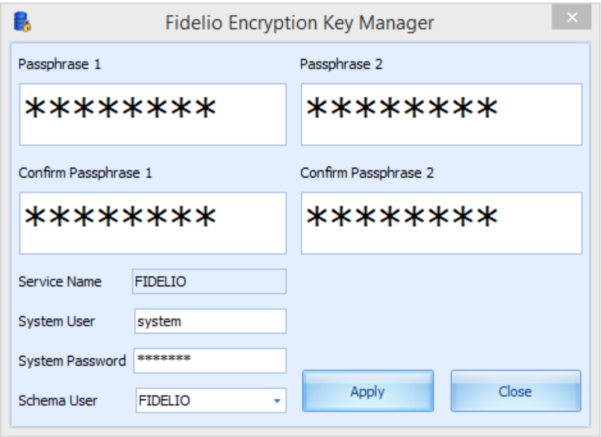
1. Start the application IFT Tools.exe.
2. At the login screen, enter your credentials.
3. After a successful authentication, the user will have access to the application and the screen shown in figure 2 will be displayed.



Chinese Taishan | System Date : 14/8/2014 | User : a | Currency : RMB | DSN : BOHAI | PC : KELVIN | Version 7.30.858

Figure 2: IFT Tools

4. Click on Change Database Encryption Key button. The Fidelio Encryption Key Manager screen popup.
5. The key custodians will have to enter their part of the passphrase in the text boxes labeled Passphrase 1 and Passphrase 2. They will be required to confirm the input and the application will validate the passphrases.
6. Once the passphrase is entered and validated, another login process, this time to the database, is required. The user needs to know the name of the Oracle connection and have a user ID and a password that grant necessary permissions to the target Oracle schema:



Fidelio Encryption Key Manager

Passphrase 1: ********

Passphrase 2: ********

Confirm Passphrase 1: ********

Confirm Passphrase 2: ********

Service Name: FIDELIO

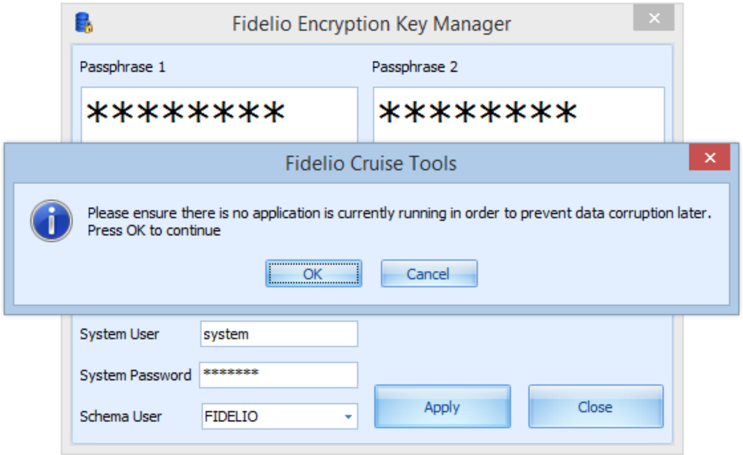
System User: system

System Password: *******

Schema User: FIDELIO

Figure 3: IFT Tools, Encryption Key Manager

7. Once all information is filled in the user clicks in Apply and a reminder pops up:



Fidelio Encryption Key Manager

Passphrase 1: ********

Passphrase 2: ********

System User: system

System Password: *******

Schema User: FIDELIO

Fidelio Cruise Tools

Please ensure there is no application is currently running in order to prevent data corruption later.
Press OK to continue

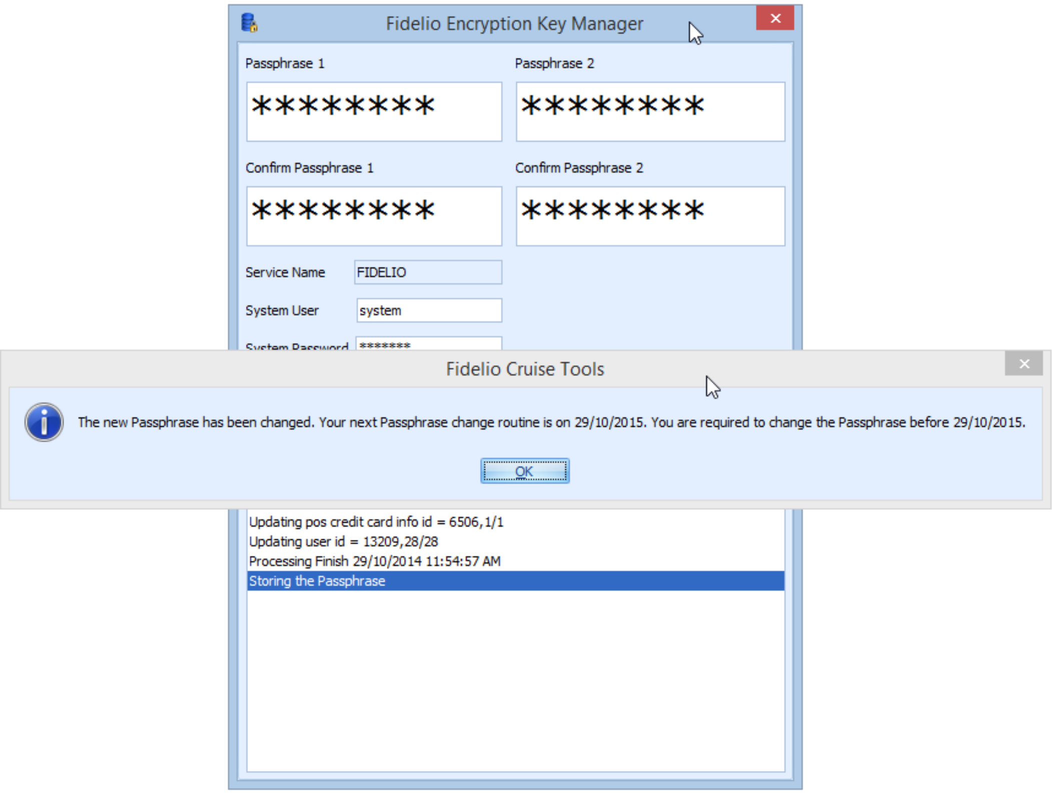
Figure 4: IFT Tools, Encryption Key Manager Reminder

8. Once the user presses OK, the application will create a new DEK and KEK. The cardholder data stored by previous versions will be decrypted in memory, and encrypted with the new DEK.

   The cardholder data stored by the previous version is securely deleted and replaced with the 128-bt AES encrypted data using the new DEK.

   The DEK used by the old version will be securely deleted and replaced with the new DEK.

   Previous versions did not have a KEK. In figure 5 we can see the screen of the application once the process is completed.



Passphrase 1: ********

Passphrase 2: ********

Confirm Passphrase 1: ********

Confirm Passphrase 2: ********

Service Name: FIDELIO

System User: system

System Password: *******

The new Passphrase has been changed. Your next Passphrase change routine is on 29/10/2015. You are required to change the Passphrase before 29/10/2015.

```
Updating pos credit card info id = 6506,1/1
Updating user id = 13209,28/28
Processing Finish 29/10/2014 11:54:57 AM
Storing the Passphrase
```

Figure 5: IFT Tools, Encryption Key Manager Completion

2.3 Locations of Stored Cardholder Data

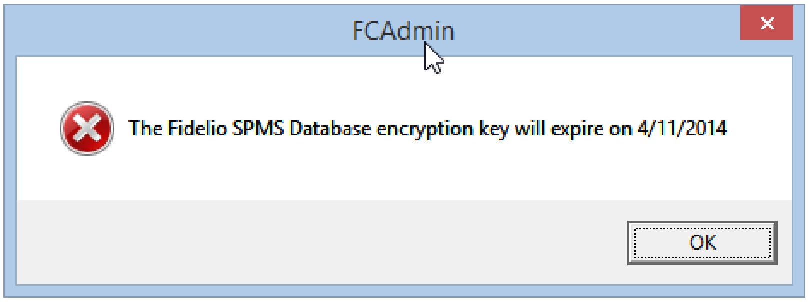
For the merchants reference the following locations contain cardholder data:

Table Name	Columns
CCA	CCA_CCNUM, CCA_CARD_EXPIRE
CCT	CCT_NUMBER, CCT_EXP, CCT_TRACK1, CCT_TRACK2
CRD	CRD_NO, CRD_EXP, CRD_TRACK1, CRD_TRACK2, CRD_TRACK3
POS	POS_CC_NUMBER, POS_CC_EXP
RES	RES_CC_NUMBER, RES_CC_EXP, RES_CC_TRACK1, RES_CC_TRACK2

2.4 Instructions for Annually Rotating Keys

DEK and KEK generation process

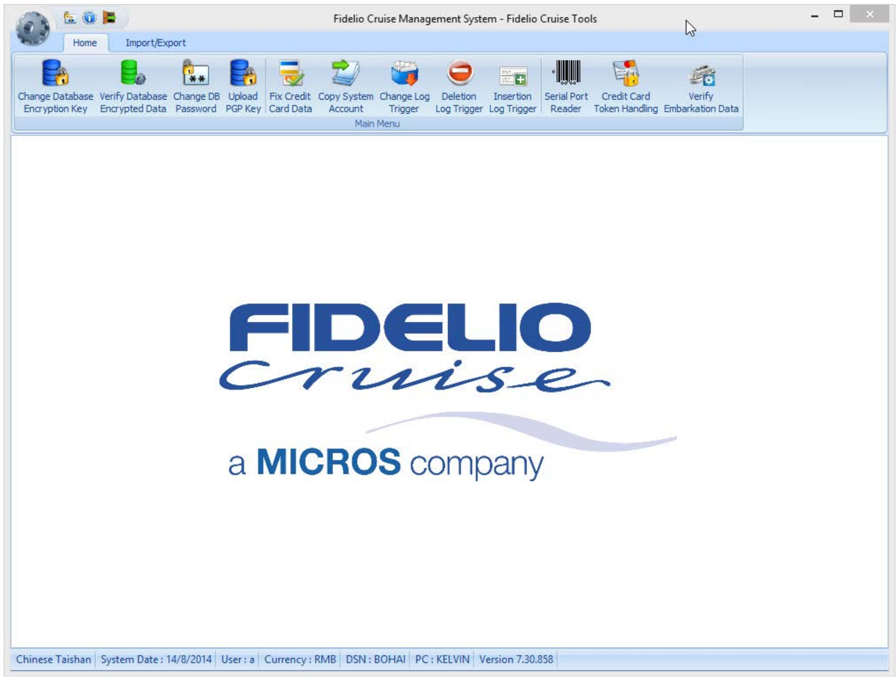
1. When the encryption key will expire in 14 days, the system will prompt the below warning to inform the shipboard to renew the encryption key.



The Fidelio SPMS Database encryption key will expire on 4/11/2014

Figure 6: 14 Day Encryption Key Expiry Warning

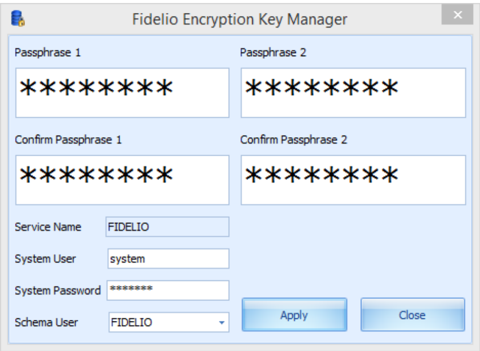
2. Start the application IFT Tools.exe.
3. At the login screen, enter your credentials.
4. After a successful authentication the user will have access to the application and the screen shown in figure 2 will be displayed.



Chinese Taishan | System Date : 14/8/2014 | User : a | Currency : RMB | DSN : BOHAI | PC : KELVIN | Version 7.30.858

Figure 7: IFT Tools

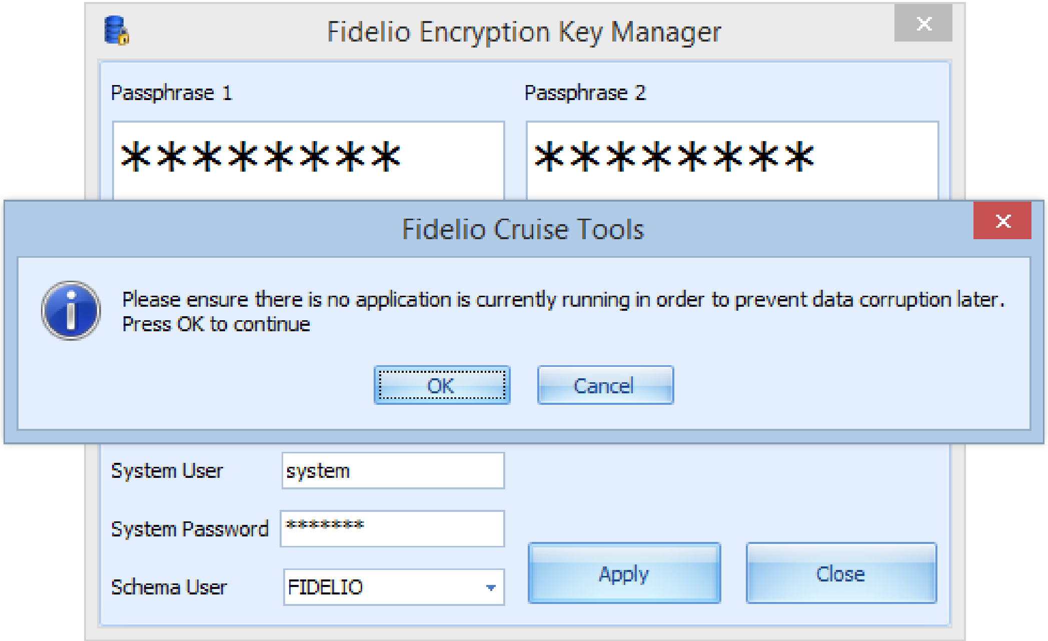
5. Click on Change Database Encryption Key button. The Fidelio Encryption Key Manager screen popup.
6. The key custodians will have to enter their part of the passphrase in the text boxes labeled Passphrase 1 and Passphrase 2. They will be required to confirm the input and the application will validate the passphrases.
7. Once the passphrase is entered and validated another login process, this time to the database is required. The user needs to know the name of the Oracle connection and have a user ID and a password that grant necessary permissions to the target Oracle schema. See figure 3.



Passphrase 1: ********
Passphrase 2: ********
Confirm Passphrase 1: ********
Confirm Passphrase 2: ********
Service Name: FIDELIO
System User: system
System Password: *******
Schema User: FIDELIO

Figure 8: Encryption Key Manager

8. Once all information is filled in the user clicks in Apply and a reminder pops-up, see figure 4.



Please ensure there is no application is currently running in order to prevent data corruption later.
Press OK to continue

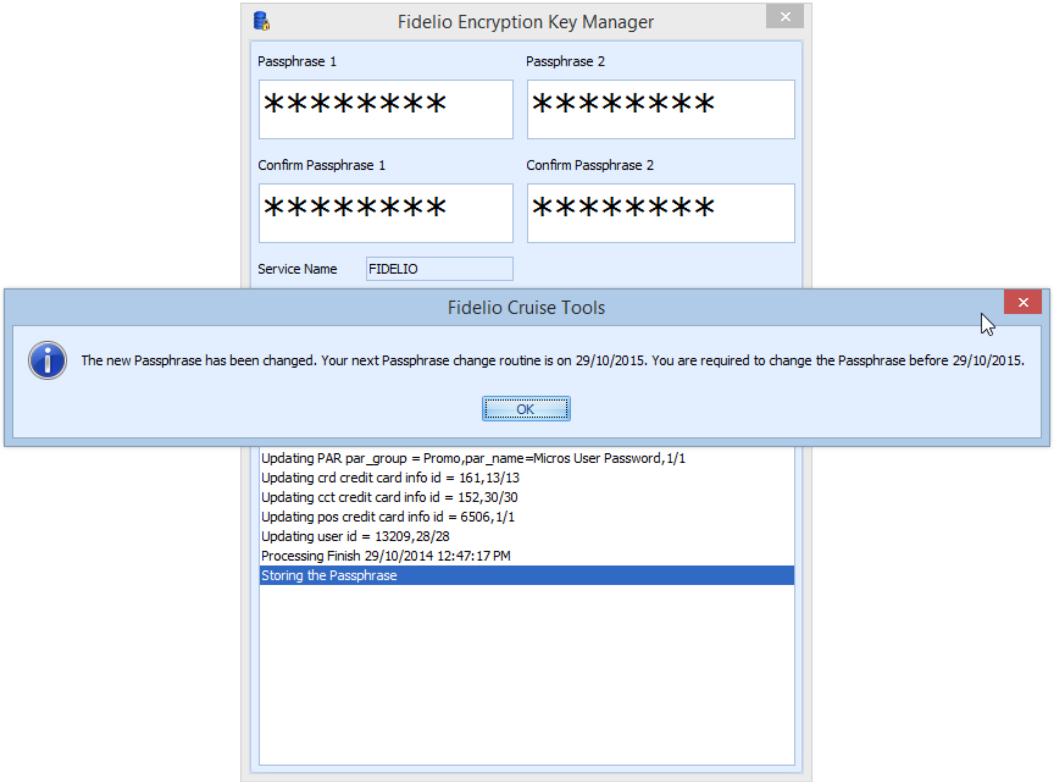
System User: system

System Password: ********

Schema User: FIDELIO

Figure 9: Encryption Key Manager

9. During the rotation of the keys all the database infrastructure is in place and the cardholder data information residing in the database will be unencrypted using the soon to be replaced (old) DEK and once the new DEK is in place the information will be encrypted using the new DEK. These processes take place in memory, and the newly encrypted cardholder data is written to the database. In figure 5 we can see the screen of the application once the process is completed.



Passphrase 1: ********

Passphrase 2: ********

Confirm Passphrase 1: ********

Confirm Passphrase 2: ********

Service Name: FIDELIO

The new Passphrase has been changed. Your next Passphrase change routine is on 29/10/2015. You are required to change the Passphrase before 29/10/2015.

```
Updating PAR par_group = Promo,par_name=Micros User Password,1/1
Updating crd credit card info id = 161,13/13
Updating cct credit card info id = 152,30/30
Updating pos credit card info id = 6506,1/1
Updating user id = 13209,28/28
Processing Finish 29/10/2014 12:47:17 PM
Storing the Passphrase
```

Figure 10:

2.5 Disable System Restore Points

If you use Microsoft Windows XP or Windows Vista, turn off System Restore on the System Properties screen. System Restore creates and uses restore points to track changes in Windows. These restore points may retain sensitive cardholder data. When you turn off System Restore, the operating system automatically removes existing restore points and stops the creation of new restore points.

Steps to turn off System Restore

1. Click Start, right-click My Computer, and then click Properties.
2. In the System Properties dialog box, click the System Restore tab.
3. Click to select the Turn off System Restore check box. Or, click to select the Turn off System Restore on all drives check box.
4. Click OK.
5. When you receive the following message, click Yes to confirm that you want to turn off System Restore:

   You have chosen to turn off System Restore. If you continue, all existing restore points will be deleted, and you will not be able to track or undo changes to your computer.

   Do you want to turn off System Restore?

   After a few moments, the System Properties dialog box closes.

2.6 Troubleshooting Procedures

Oracle Hospitality Cruise support team will not collect or request sensitive authentication data or cardholder data for any support issue. However, for the customers’ knowledge the following is the PA-DSS requirements for troubleshooting procedures that require the collection of sensitive authentication data or cardholder data.

When troubleshooting issues, care must be taken to properly protect cardholder data.

When gathering data, the following restrictions must be followed:

- Collect sensitive authentication only when needed to solve a specific problem.
- Store such data only in specific, known locations with limited access.
- Collect only the limited amount of data needed to solve a specific problem.
- Encrypt sensitive authentication data while stored.
- Securely delete such data immediately after use.

PA-DSS Requirements Reference

1.1.4

Securely delete any magnetic stripe data, card validation values or codes, and PINs or PIN block data stored by previous versions of the software.

- That historical data must be removed (magnetic stripe data, card validation codes, PINs, or PIN blocks stored by previous versions of the software).
- How to remove historical data.
- That such removal is absolutely necessary for PCI compliance.

1.1.5

Securely delete any sensitive authentication data (pre-authorization data) used for debugging or troubleshooting purposes from log files, debugging files, and other data sources received from customers, to ensure that magnetic stripe data, card validation codes or values, and PINS or PIN block data are not stored on software vendor systems.

- That sensitive data (pre-authorization) must only be collected when needed to solve a specific problem.
- That such data must be stored only in specific, known locations with limited access.
- That only a limited amount of such data must be collected as needed to solve a specific problem.
- That sensitive authentication data must be encrypted while stored.
- That such data must be securely deleted immediately after use.

2.1

Software vendor must provide guidance to customers regarding purging of cardholder data after expiration of customer-defined retention period.

- That cardholder data must be purged after it exceeds the customer-defined retention period.
- That cardholder data must be purged at all locations where the payment application stores cardholder data.

2.7

Securely delete any cryptographic key material or cryptogram stored by previous versions of the software. This could be cryptographic keys used for computation or verification of cardholder data or sensitive authentication data.

Include the following instructions:

- That cryptographic material must be removed.
- How to remove cryptographic material.
- That such removal is absolutely necessary for PCI compliance.
- How to re-encrypt historic data with new keys.

3 Password and Account Settings

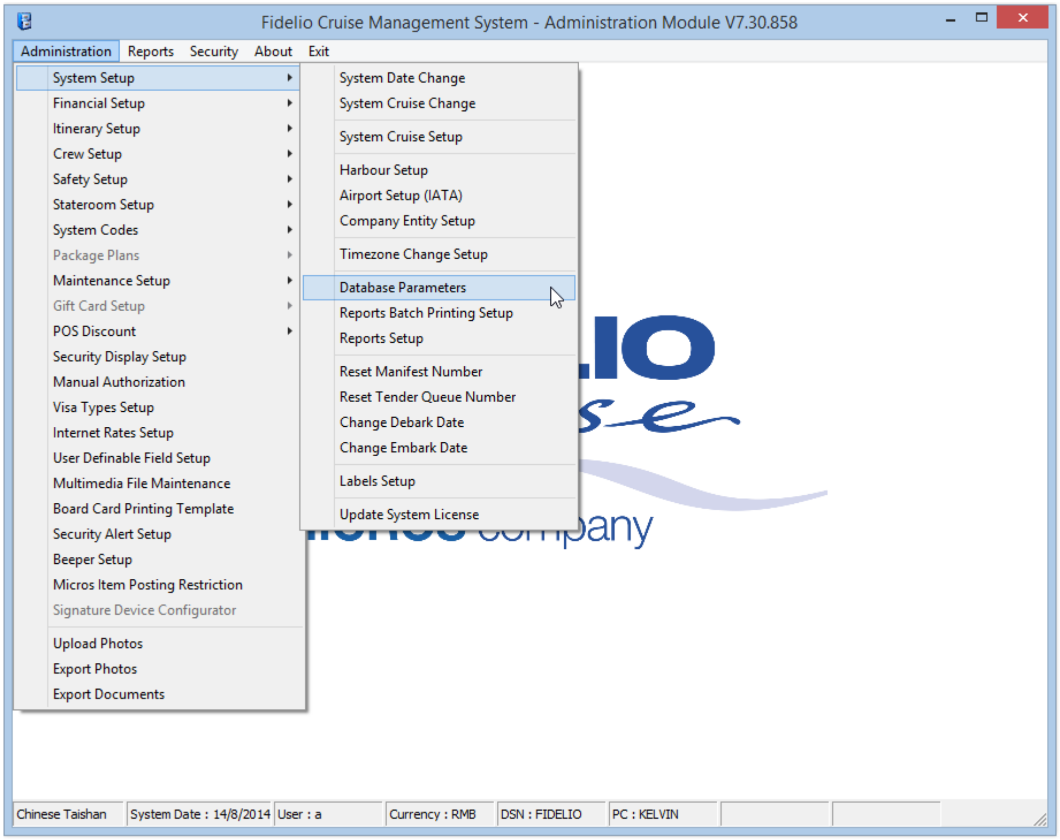
3.1 Access Control

Merchants, resellers and integrators are advised to control access, via unique username and PCI DSS compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data.

Passwords used in SMPS must also follow the security guidelines.

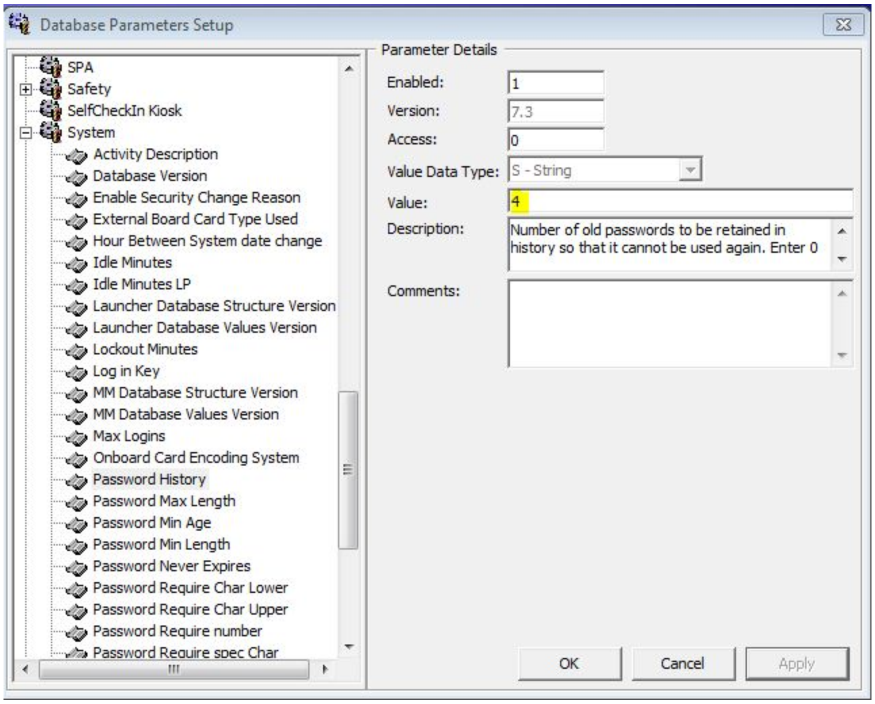
The application must require unique usernames and secure authentication for all administrative access and for all access to cardholder data.

To configure SPMS to require strong password controls, follow these instructions:



Chinese Taishan | System Date : 14/8/2014 | User : a | Currency : RMB | DSN : FIDELIO | PC : KELVIN

Figure 11: FC Management, Database Parameters


Database Parameters Setup
SPA
Safety
SelfCheckIn Kiosk
System
Activity Description
Database Version
Enable Security Change Reason
External Board Card Type Used
Hour Between System date change
Idle Minutes
Idle Minutes LP
Launcher Database Structure Version
Launcher Database Values Version
Lockout Minutes
Log in Key
MM Database Structure Version
MM Database Values Version
Max Logins
Onboard Card Encoding System
Password History
Password Max Length
Password Min Age
Password Min Length
Password Never Expires
Password Require Char Lower
Password Require Char Upper
Password Require number
Password Require spec Char
OK
Cancel
Apply

Parameter Details

Enabled: 1

Version: 7.3

Access: 0

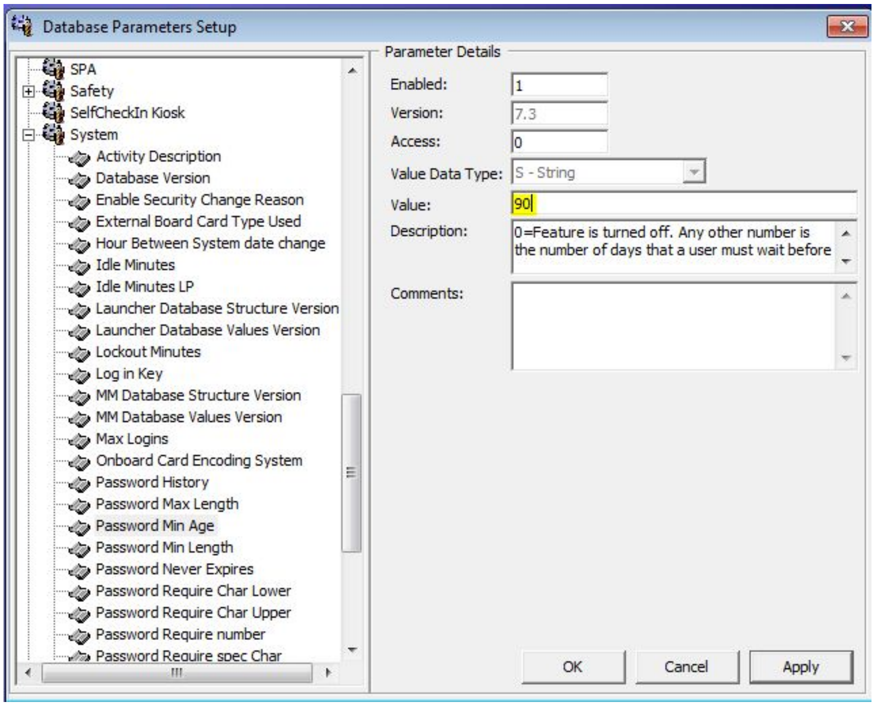
Value Data Type: S - String

Value: 4

Description: Number of old passwords to be retained in history so that it cannot be used again. Enter 0

Comments:

Figure 12: Configure Password History


Database Parameters Setup
SPA
Safety
SelfCheckIn Kiosk
System
Activity Description
Database Version
Enable Security Change Reason
External Board Card Type Used
Hour Between System date change
Idle Minutes
Idle Minutes LP
Launcher Database Structure Version
Launcher Database Values Version
Lockout Minutes
Log in Key
MM Database Structure Version
MM Database Values Version
Max Logins
Onboard Card Encoding System
Password History
Password Max Length
Password Min Age
Password Min Length
Password Never Expires
Password Require Char Lower
Password Require Char Upper
Password Require number
Password Require spec Char
OK
Cancel
Apply

Parameter Details

Enabled: 1

Version: 7.3

Access: 0

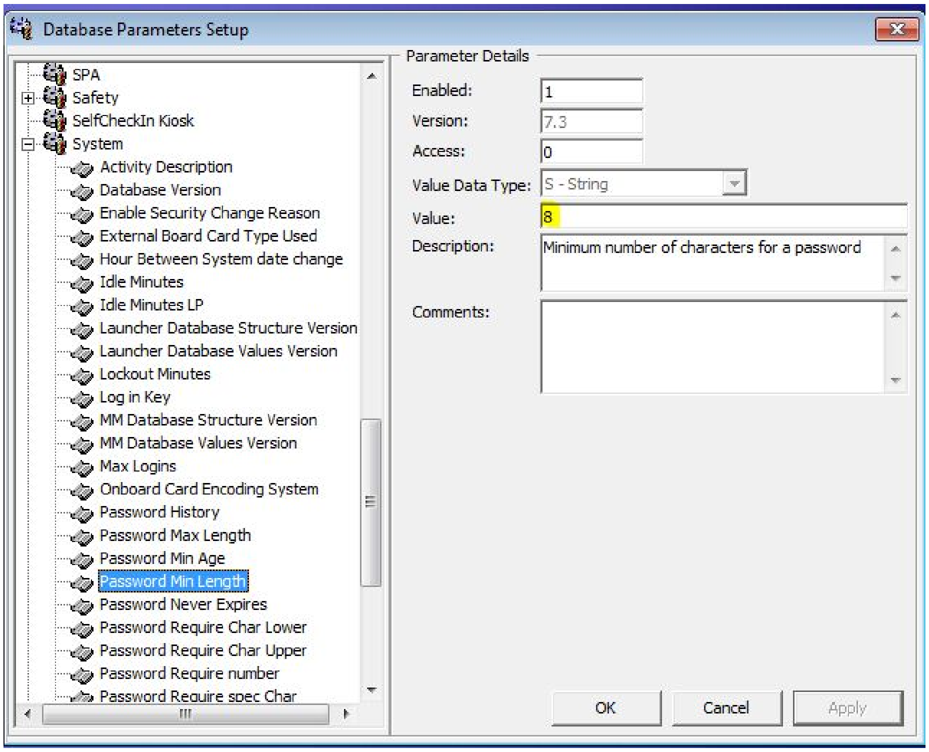
Value Data Type: S - String

Value: 90

Description: 0=Feature is turned off. Any other number is the number of days that a user must wait before

Comments:

Figure 13: Configure Password Max Age


SPA
Safety
SelfCheckIn Kiosk
System
Activity Description
Database Version
Enable Security Change Reason
External Board Card Type Used
Hour Between System date change
Idle Minutes
Idle Minutes LP
Launcher Database Structure Version
Launcher Database Values Version
Lockout Minutes
Log in Key
MM Database Structure Version
MM Database Values Version
Max Logins
Onboard Card Encoding System
Password History
Password Max Length
Password Min Age
Password Min Length
Password Never Expires
Password Require Char Lower
Password Require Char Upper
Password Require number
Password Require spec Char
OK
Cancel
Apply

Database Parameters Setup

Parameter Details

Enabled: 1

Version: 7.3

Access: 0

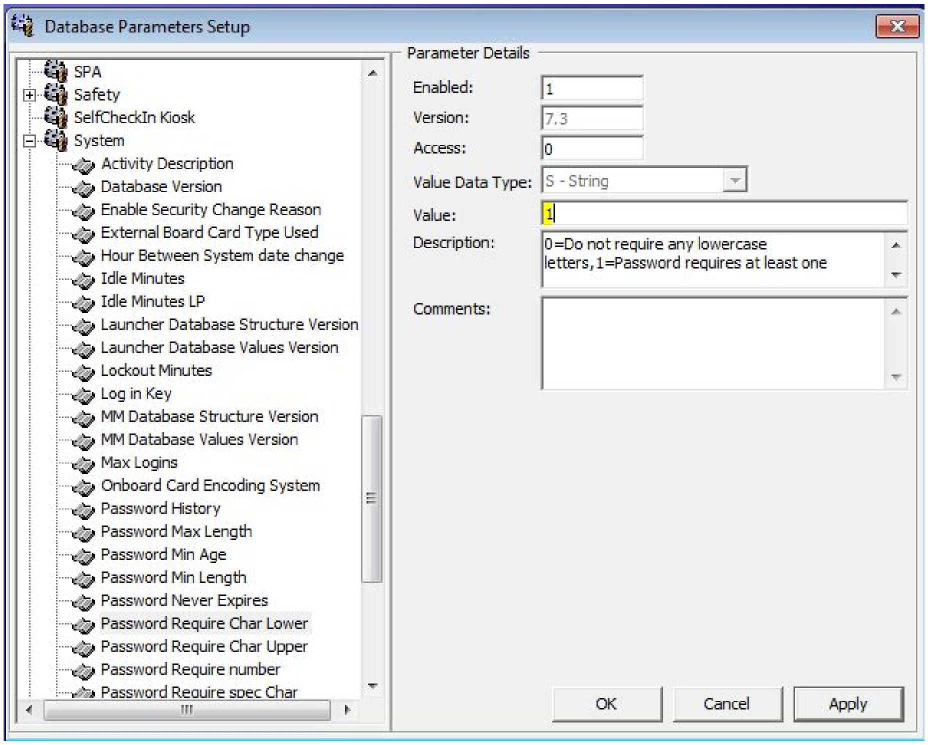
Value Data Type: S - String

Value: 8

Description: Minimum number of characters for a password

Comments:

Figure 14: Configure Password Minimum Length


SPA
Safety
SelfCheckIn Kiosk
System
Activity Description
Database Version
Enable Security Change Reason
External Board Card Type Used
Hour Between System date change
Idle Minutes
Idle Minutes LP
Launcher Database Structure Version
Launcher Database Values Version
Lockout Minutes
Log in Key
MM Database Structure Version
MM Database Values Version
Max Logins
Onboard Card Encoding System
Password History
Password Max Length
Password Min Age
Password Min Length
Password Never Expires
Password Require Char Lower
Password Require Char Upper
Password Require number
Password Require spec Char
OK
Cancel
Apply

Database Parameters Setup

Parameter Details

Enabled: 1

Version: 7.3

Access: 0

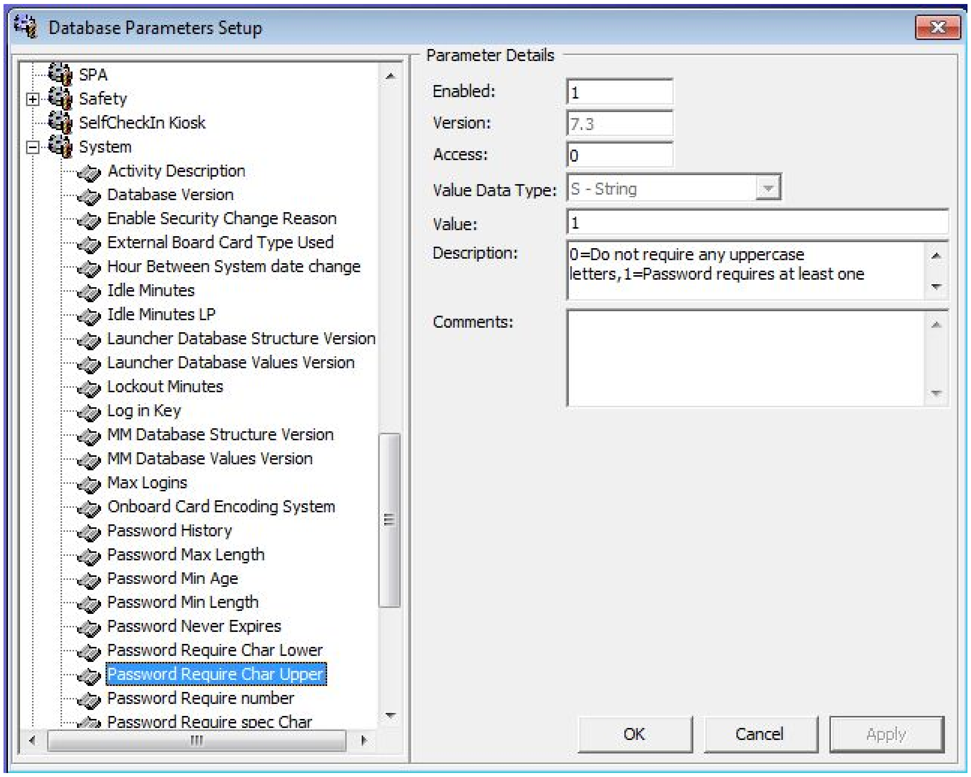
Value Data Type: S - String

Value: 1

Description: 0=Do not require any lowercase letters,1=Password requires at least one

Comments:

Figure 15: Require lower case password characters


Database Parameters Setup
SPA
Safety
SelfCheckIn Kiosk
System
Activity Description
Database Version
Enable Security Change Reason
External Board Card Type Used
Hour Between System date change
Idle Minutes
Idle Minutes LP
Launcher Database Structure Version
Launcher Database Values Version
Lockout Minutes
Log in Key
MM Database Structure Version
MM Database Values Version
Max Logins
Onboard Card Encoding System
Password History
Password Max Length
Password Min Age
Password Min Length
Password Never Expires
Password Require Char Lower
Password Require Char Upper
Password Require number
Password Require spec Char
OK
Cancel
Apply

Parameter Details

Enabled: 1

Version: 7.3

Access: 0

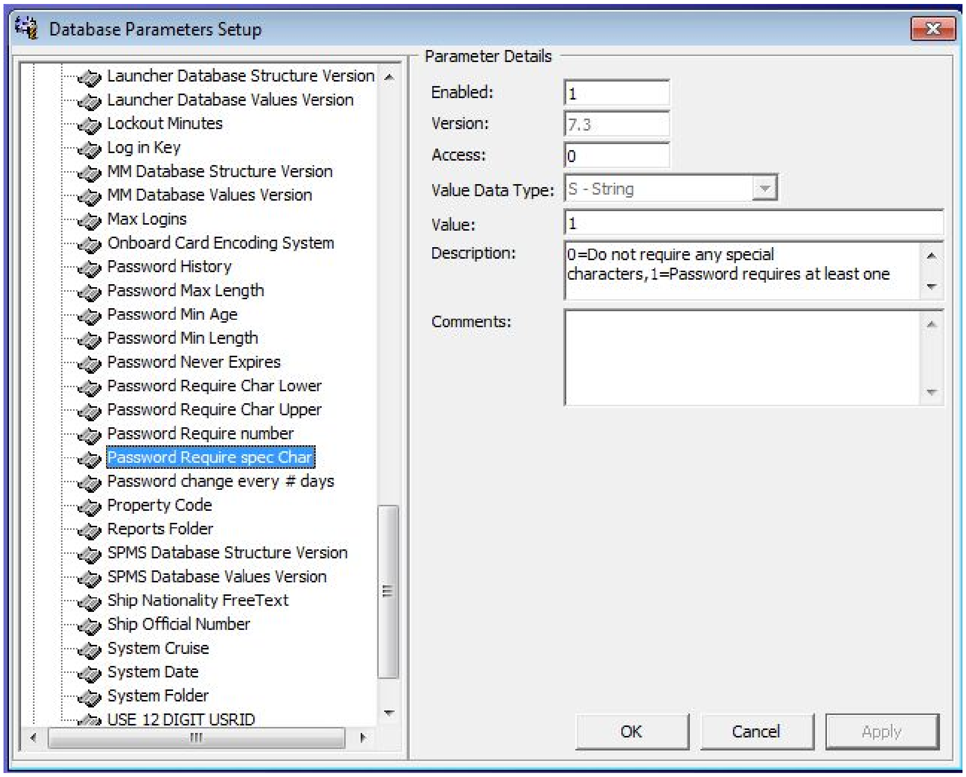
Value Data Type: S - String

Value: 1

Description: 0=Do not require any uppercase letters, 1=Password requires at least one

Comments:

Figure 16: Require Upper Case password characters


Database Parameters Setup
Launcher Database Structure Version
Launcher Database Values Version
Lockout Minutes
Log in Key
MM Database Structure Version
MM Database Values Version
Max Logins
Onboard Card Encoding System
Password History
Password Max Length
Password Min Age
Password Min Length
Password Never Expires
Password Require Char Lower
Password Require Char Upper
Password Require number
Password Require spec Char
Password change every # days
Property Code
Reports Folder
SPMS Database Structure Version
SPMS Database Values Version
Ship Nationality FreeText
Ship Official Number
System Cruise
System Date
System Folder
USE 12 DIGIT USRID
OK
Cancel
Apply

Parameter Details

Enabled: 1

Version: 7.3

Access: 0

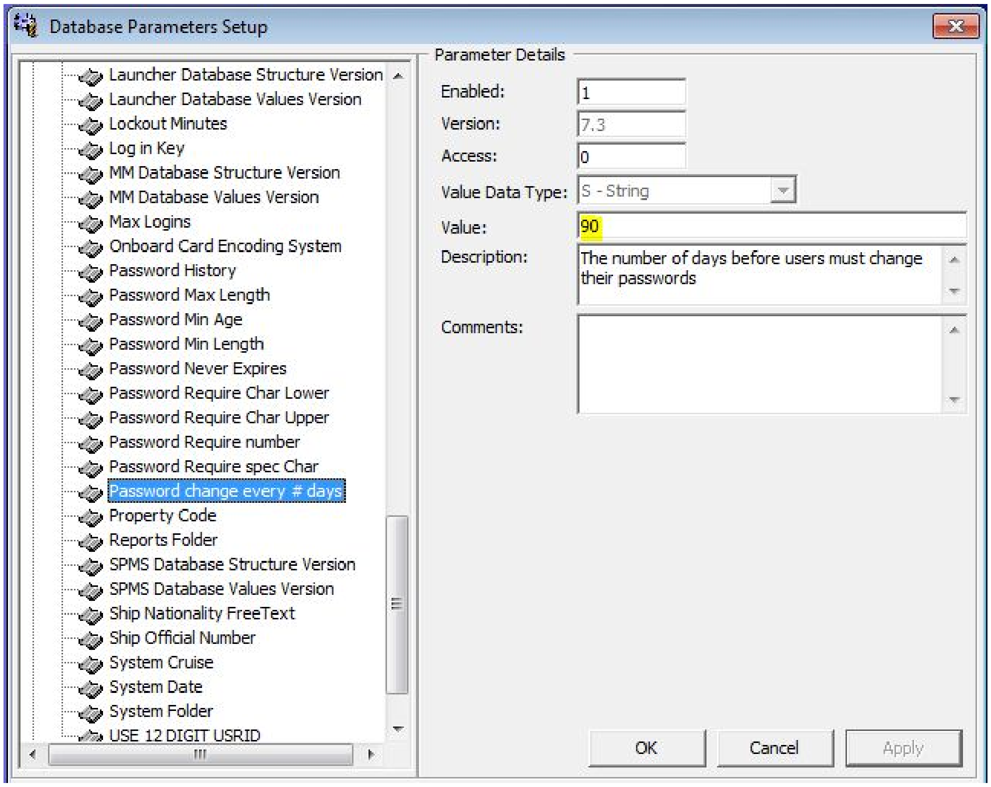
Value Data Type: S - String

Value: 1

Description: 0=Do not require any special characters, 1=Password requires at least one

Comments:

Figure 17: Require special characters


Database Parameters Setup
Launcher Database Structure Version
Launcher Database Values Version
Lockout Minutes
Log in Key
MM Database Structure Version
MM Database Values Version
Max Logins
Onboard Card Encoding System
Password History
Password Max Length
Password Min Age
Password Min Length
Password Never Expires
Password Require Char Lower
Password Require Char Upper
Password Require number
Password Require spec Char
Password change every # days
Property Code
Reports Folder
SPMS Database Structure Version
SPMS Database Values Version
Ship Nationality FreeText
Ship Official Number
System Cruise
System Date
System Folder
USE 12 DIGIT USRID
Parameter Details
OK
Cancel
Apply

Enabled: 1

Version: 7.3

Access: 0

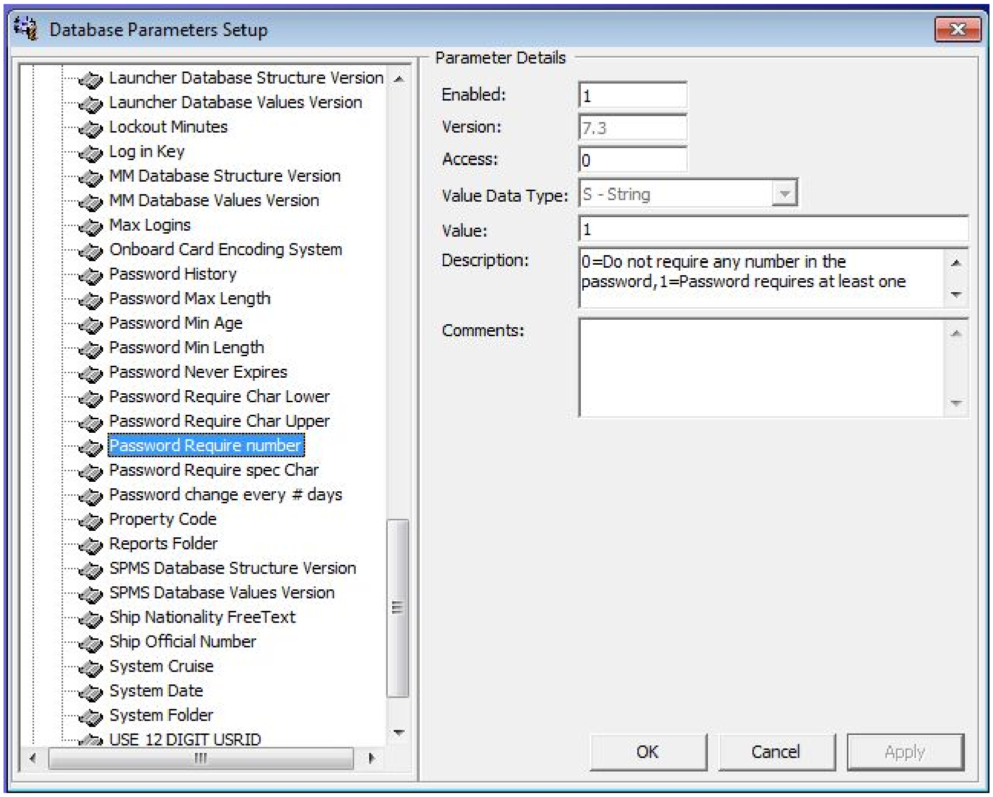
Value Data Type: S - String

Value: 90

Description: The number of days before users must change their passwords

Comments:

Figure 18: Require password rotation


Database Parameters Setup
Launcher Database Structure Version
Launcher Database Values Version
Lockout Minutes
Log in Key
MM Database Structure Version
MM Database Values Version
Max Logins
Onboard Card Encoding System
Password History
Password Max Length
Password Min Age
Password Min Length
Password Never Expires
Password Require Char Lower
Password Require Char Upper
Password Require number
Password Require spec Char
Password change every # days
Property Code
Reports Folder
SPMS Database Structure Version
SPMS Database Values Version
Ship Nationality FreeText
Ship Official Number
System Cruise
System Date
System Folder
USE 12 DIGIT USRID
Parameter Details
OK
Cancel
Apply

Enabled: 1

Version: 7.3

Access: 0

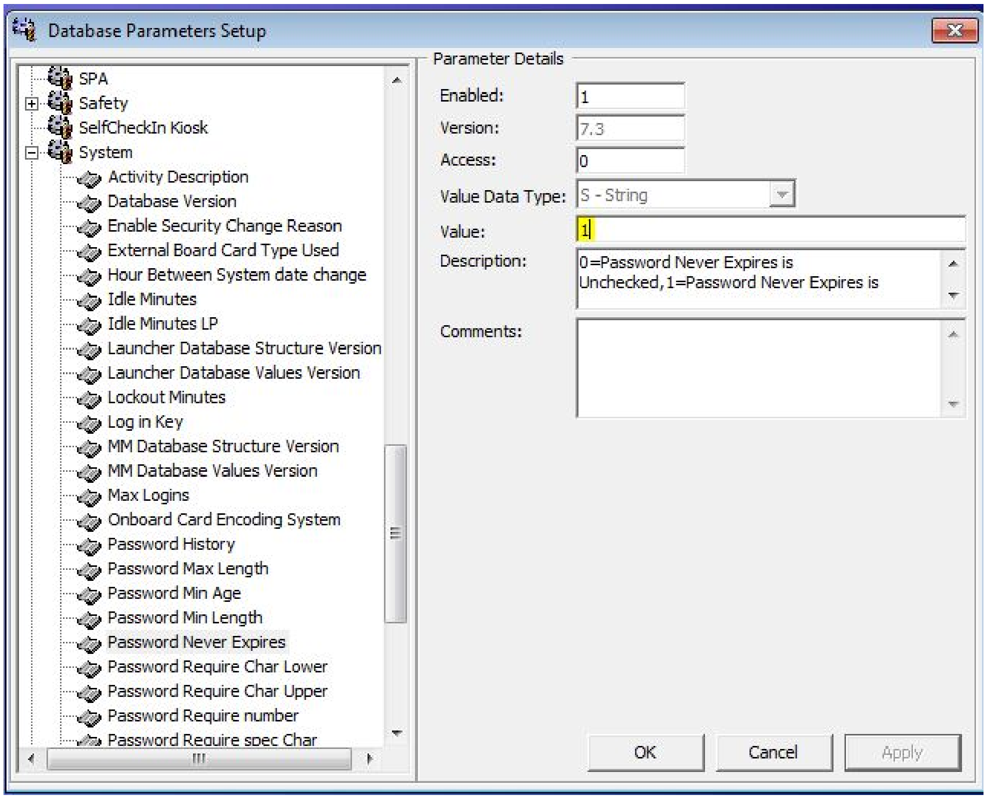
Value Data Type: S - String

Value: 1

Description: 0=Do not require any number in the password,1=Password requires at least one

Comments:

Figure 19: Require passwords to require numbers


Database Parameters Setup
SPA
Safety
SelfCheckIn Kiosk
System
Activity Description
Database Version
Enable Security Change Reason
External Board Card Type Used
Hour Between System date change
Idle Minutes
Idle Minutes LP
Launcher Database Structure Version
Launcher Database Values Version
Lockout Minutes
Log in Key
MM Database Structure Version
MM Database Values Version
Max Logins
Onboard Card Encoding System
Password History
Password Max Length
Password Min Age
Password Min Length
Password Never Expires
Password Require Char Lower
Password Require Char Upper
Password Require number
Password Require spec Char
OK
Cancel
Apply

Parameter Details

Enabled: 1

Version: 7.3

Access: 0

Value Data Type: S - String

Value: 1

Description: 0=Password Never Expires is Unchecked,1=Password Never Expires is

Comments:

Figure 20: Require password expiration

3.2 Password Controls

The following guidelines must be followed.

- Customers are advised against using administrative accounts for application logins (e.g., don’t use the “sa” account for application access to the database). (PA-DSS 3.1c)
- Customers are advised to assign strong passwords to these default accounts (even if they won’t be used), and then disable or do not use the accounts. (PA-DSS 3.1c)
- Customers are advised to assign strong application and system passwords whenever possible. (PA-DSS 3.1c)
- Customers are advised how to create PCI DSS-compliant complex passwords to access the payment application, per PCI Data Security Standard 8.5.8 through 8.5.15. (PA-DSS 3.1c)
- Customers are advised to control access, via unique username and PCI DSS-compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data. (PA-DSS 3.2)

Passwords should meet the requirements set in PCI DSS section 8.5.8 through 8.5.15, as listed here.

- Do not use group, shared, or generic accounts and passwords.
- Change user passwords at least every 90 days.
- Require a minimum password length of at least seven characters.
- Use passwords containing both numeric and alphabetic characters.
- 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.
- Limit repeated access attempts by locking out the user ID after not more than 6 attempts.
- Set the lockout duration to thirty minutes or until administrator enables the user ID.
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.

PA-DSS Requirements Reference:

3.1

Application as provided by vendor must require unique usernames and secure authentication for all administrative access and for all access to cardholder data.

3.2

Access to PCs, servers, and databases with payment applications must require a unique username and secure authentication.

4 Logging

4.1 Merchant Applicability

Currently, for SPMS version 7.30.868, there is no end-user, configurable, logging settings. All logging settings are hardcoded to conform to PCI DSS version 2.0 requirements 10.2.1-10.2.7 and 10.3.1-10.3.6.

Logs must be enabled and disabling them will make Product non-compliant with PCI DSS.

4.1 Configuring Log Settings

PA-DSS compliant logging is hardcoded within SPMS and no outside configuration is needed.

4.2 PCI Guidelines for Logging

Implement automated audit trails for all system components to reconstruct the following events:

- All individual accesses to cardholder data.
- All actions taken by any individual with root or administrative privileges.
- Access to all audit trails.
- Invalid logical access attempts.
- Use of identification and authentication mechanisms.
- Initialization of the audit logs.
- Creation and deletion of system-level objects.

Record at least the following audit trail entries for all system components for each event:

- User identification.
- Type of event.
- Date and time.
- Success or failure indication.
- Origination of event.
- Identity or name of affected data, system component, or resource.

PA-DSS Requirements Reference:

4.2

Payment application must implement an automated audit trail to track and monitor access, per PCI Data Security Standard version 2.0 requirements 10.2.1-10.2.7 and 10.3.1-10.3.6.

5 Wireless Networks

5.1 Merchant Applicability

For SPMS to function properly, using wireless technology is not a requirement. However, if wireless is used or implemented in the payment environment or application, the wireless environment must be configured per PCI DSS version 2.0 requirements 1.2.3, 2.1.1, and 4.1.1. Wireless technology must be securely implemented and transmissions of cardholder data over wireless networks must be secure.

5.2 PCI Requirements

Install and configure perimeter firewalls between wireless networks and systems that store credit card data to deny or control access so that traffic is restricted to only those sockets that are required from the wireless environment, per PCI DSS version 2.0 requirement 1.2.3.

Modify default wireless settings, as follows, per PCI DSS 2.1.1:

- Change wireless equivalent privacy (WEP) keys
- Change default service set identifier (SSID)
- Disable SSID broadcasts
- Change default passwords
- Change SNMP community strings
- Enable Wi-Fi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.

For wireless networks transmitting cardholder data, encrypt the transmissions by using Wi-Fi protected access (WPA or WPA2) technology, IPSEC VPN, or SSLv.3/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. (PA-DSS 6.2 and PCI DSS 4.1.1)

If WEP is used, do the following, per PCI DSS 4.1.1:

- Use with a minimum 104-bit encryption key and 24 bit-initialization value
- Use ONLY in conjunction with Wi-Fi protected access (WPA or WPA2) technology, VPN, or SSLv.3/TLS
- Rotate shared WEP keys quarterly (or automatically if the technology permits)
- Rotate shared WEP keys whenever there are changes in personnel with access to keys
- Restrict access based on media access code (MAC) address

For new wireless implementations it is prohibited to implement WEP, as the deadline expired on the 31st of March, 2009. For current wireless implementations it is prohibited to use WEP after the 30th of June, 2010.

PA-DSS Requirements Reference

6.1

For payment application using wireless technology, the wireless technology must be implemented securely, per PCI DSS version 2.0 requirements 1.2.3, 2.1.1 and 4.1.1.

6.2

For wireless networks transmitting cardholder data, encrypt the transmissions by using Wi-Fi protected access (WPA or WPA2) technology, IPSEC VPN, or SSLv.3/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN.

6 Network Segmentation

6.1 Merchant Applicability

Credit card data cannot be stored on systems directly connected to the Internet. For example, web servers and database servers should not be installed on the same server. A DMZ must be set up to segment the network so that only machines on the DMZ are Internet accessible. SPMS does not require a direct connection to the Internet.

PA-DSS Requirements Reference

9.1

The payment application must be developed such that the database server and web server are not required to be on the same server, nor is the database server required to be in the DMZ with the web server, per PCI DSS version 2.0 requirement 1.3.2.

7 Secure Remote Software Updates

7.1 Merchant Applicability

Oracle Hospitality Cruise securely delivers remote payment applications by secure VPN connections. Merchants should develop an acceptable use policy for critical employee-facing technologies, per the guidelines below. If merchant is receiving updates via modem, the modem should only be activated when downloads are needed.

For VPN, or other high-speed connections, updates are received through a firewall or personal firewall, per PCI DSS 1 and 1.3.9.

- Use a firewall if the computer is connected via VPN or other high-speed connection, and to secure these connections by limiting only the sockets necessary for the application to function.
- Only activate remote access when needed and immediately inactivate after use.

7.2 Acceptable Use Policy

The merchant should develop usage policies for critical employee-facing technologies, like modems and wireless devices, as per PCI DSS requirement 12.3. These usage policies should include:

- Explicit management approval for use
- Authentication for use
- A list of all devices and personnel with access
- Labeling the devices with owner
- Contact information and purpose
- Acceptable uses of the technology
- Acceptable network locations for the technologies
- A list of company approved products
- Allowing use of modems for vendors only when needed and deactivation after use
- Prohibition of storage of cardholder data onto local media when remotely connected

7.3 Personal Firewall

Any "always-on" connections from a computer to a VPN or other high-speed connection should be secured by using a personal firewall product, per PCI DSS 1.3.9. The firewall is configured by the organization to meet specific standards and not alterable by the employee.

7.4 Remote Update Procedures

Oracle Hospitality Cruise provides an FTP server that is capable of communicating via secure FTP (SFTP) protocol.

The server's hostname is: ftp.fcruise.com

SFTP Protocol uses port 22 (instead of 21 with regular FTP).

Oracle Hospitality Cruise Support provides customers with user credentials for the server.

Please follow the instructions below for configuring the SFTP client and to download updates.

8 Installation of SFTP Client

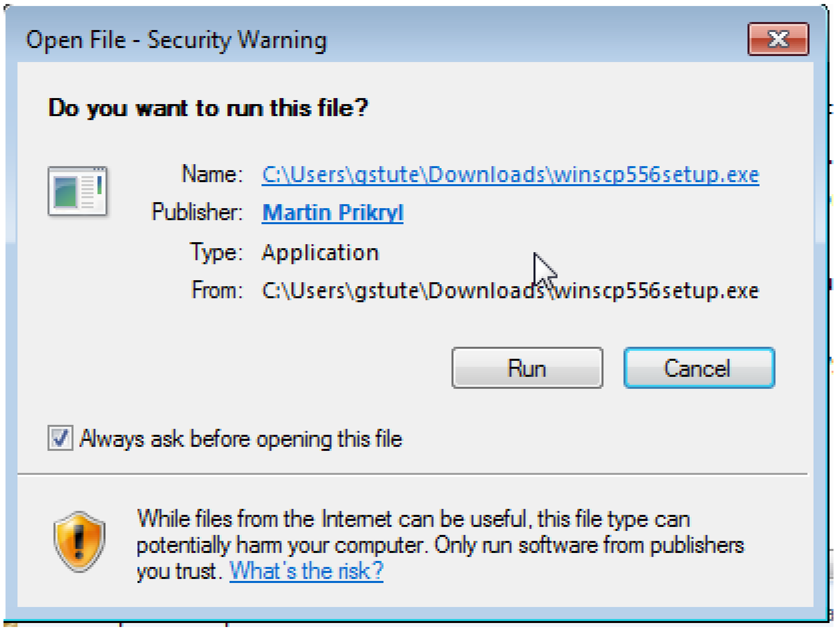
An SFTP client is required to obtain files from the Secure FTP server. In this example, WinSCP is used as example. This is not an endorsement for this particular product.

Please download the latest version of "WinSCP" from http://winscp.net. As of this writing, version 5.5.6 is the latest stable release.

Verify the checksum to make sure the downloaded file is not tampered with.

In order to start the installation process, please press "Run".

The publisher is identified as "Martin Prikryl".



Open File - Security Warning

Do you want to run this file?

Name: C:\Users\gstute\Downloads\winscp556setup.exe

Publisher: Martin Prikryl

Type: Application

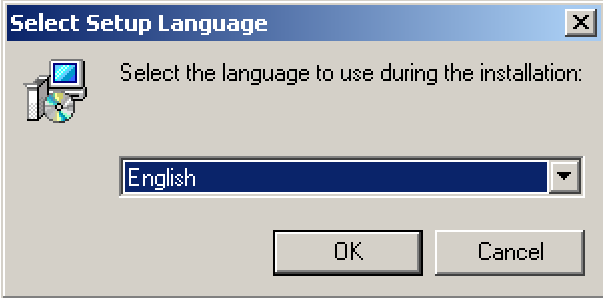
From: C:\Users\gstute\Downloads\winscp556setup.exe

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

Figure 21: WinSCP Installation Security Warning

Please select the language for the installation:



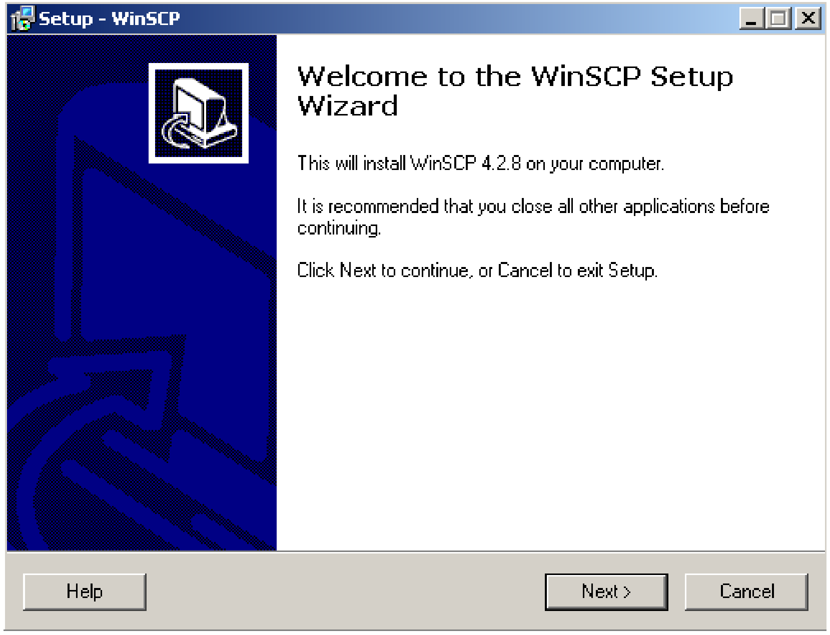
Select Setup Language

Select the language to use during the installation:

English

Figure 22: WinSCP Select Language Dialogue

Now the installation begins. Please go forward by using the “Next” button:



Welcome to the WinSCP Setup Wizard

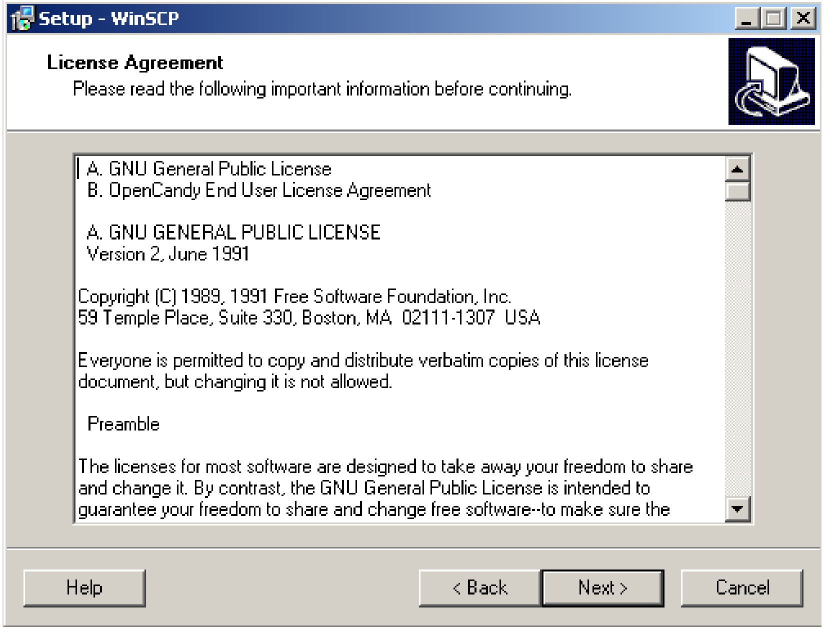
This will install WinSCP 4.2.8 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Figure 23: WinSCP Setup Wizard

Please read the license agreement carefully:



License Agreement

Please read the following important information before continuing.

A. GNU General Public License
B. OpenCandy End User License Agreement

A. GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

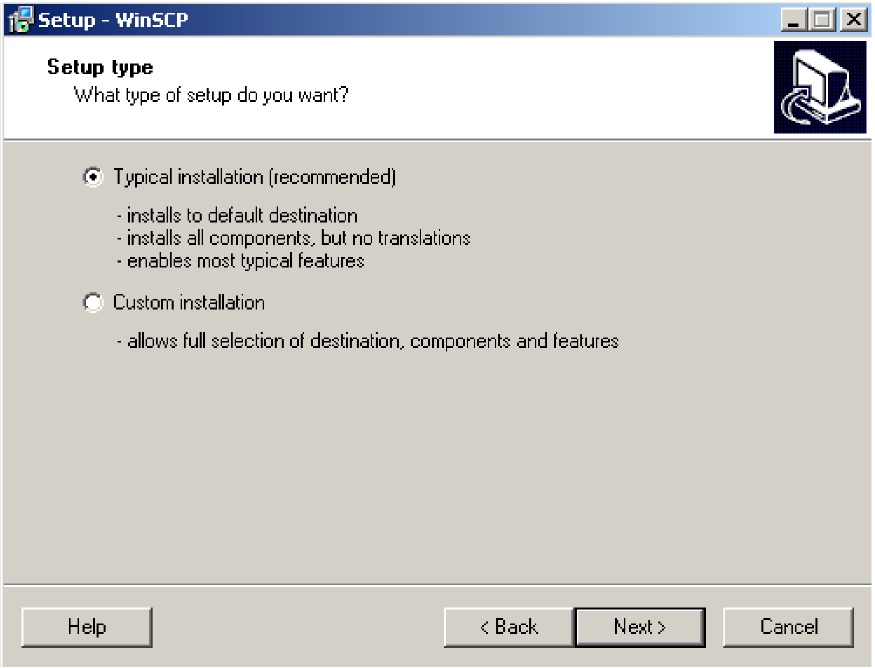
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the

Figure 24: WinSCP License Agreement

The easiest would be to use the recommendations by the installer. You can simply use the typical installation:


Setup - WinSCP

Setup type
What type of setup do you want?

● Typical installation (recommended)

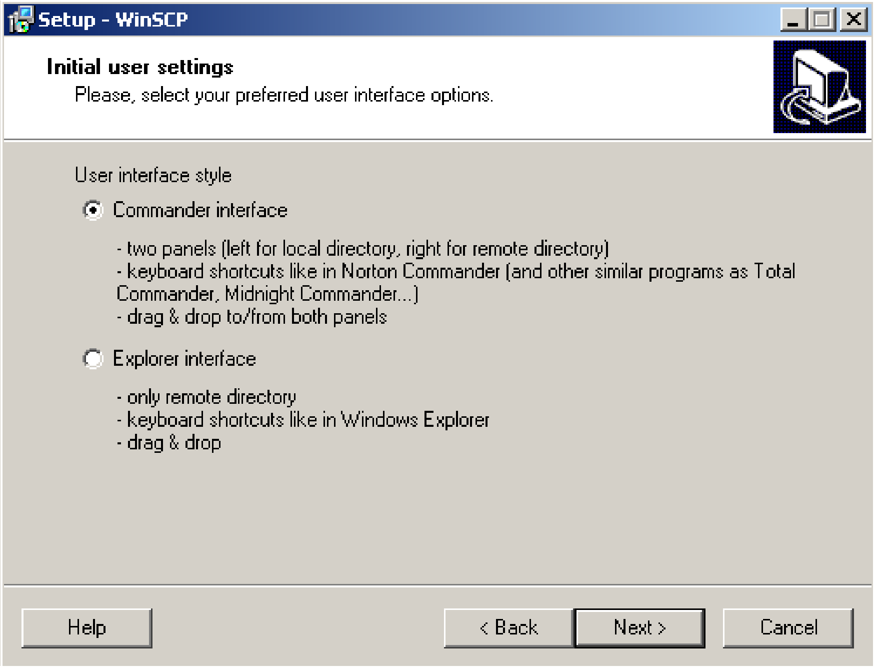
- installs to default destination
- installs all components, but no translations
- enables most typical features

○ Custom installation

- allows full selection of destination, components and features

Figure 25: WinSCP Setup Type

Follow the recommendations by the installer and use the "Commander interface":


Setup - WinSCP

Initial user settings
Please, select your preferred user interface options.

User interface style

● Commander interface

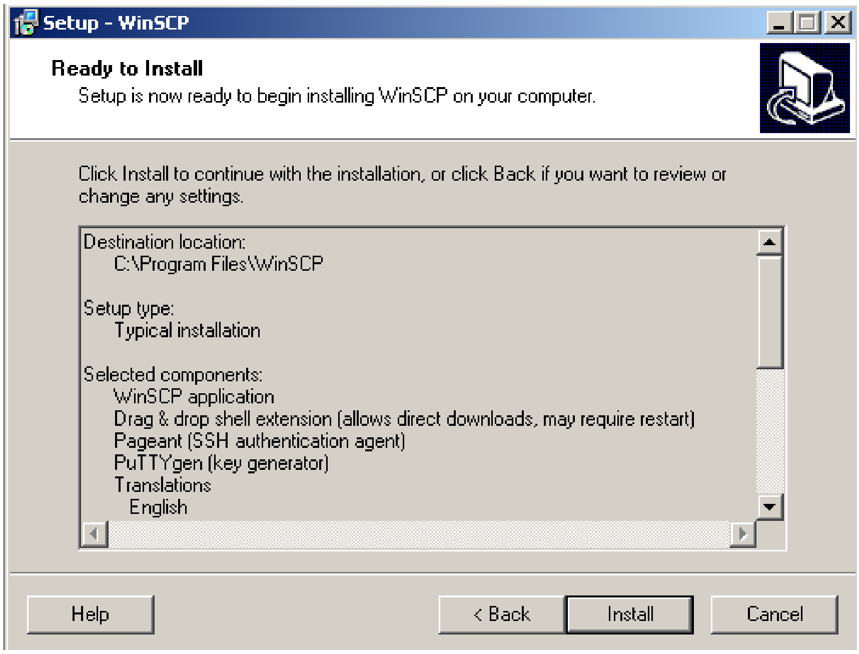
- two panels (left for local directory, right for remote directory)
- keyboard shortcuts like in Norton Commander (and other similar programs as Total Commander, Midnight Commander...)
- drag & drop to/from both panels

○ Explorer interface

- only remote directory
- keyboard shortcuts like in Windows Explorer
- drag & drop

Figure 26: WinSCP User Settings

After these few questions, you will get a summary of all settings which will be used. When using the “Install” button, the installation will start:



Ready to Install

Setup is now ready to begin installing WinSCP on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

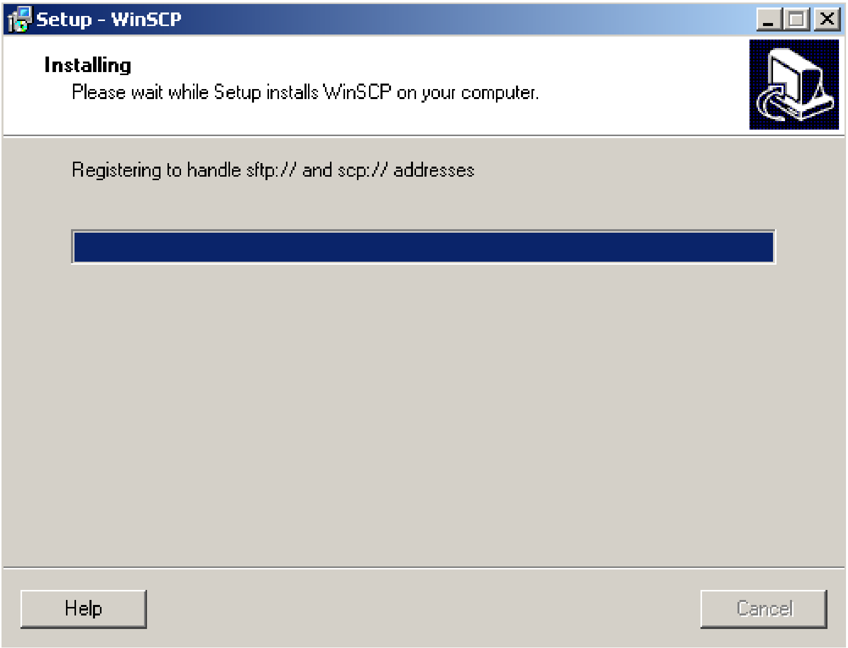
```
Destination location:
    C:\Program Files\WinSCP

Setup type:
    Typical installation

Selected components:
    WinSCP application
    Drag & drop shell extension (allows direct downloads, may require restart)
    Pageant (SSH authentication agent)
    PuTTYgen (key generator)
    Translations
      English
```

Figure 27: WinSCP Setup Summary

The installation should be done very quickly. You may see some status messages.



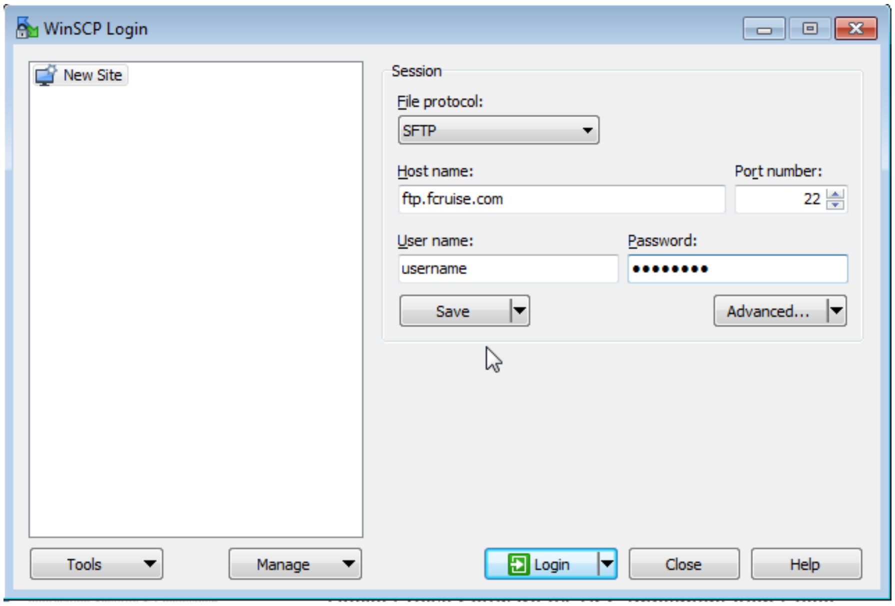
Installing

Please wait while Setup installs WinSCP on your computer.

Registering to handle sftp:// and scp:// addresses

Figure 28: WinSCP Setup Progress Bar

Please start WinSCP by double-clicking the desktop icon or from the WinSCP menu in the start menu.


WinSCP Login

New Site

Session

File protocol: SFTP

Host name: ftp.fcruise.com

Port number: 22

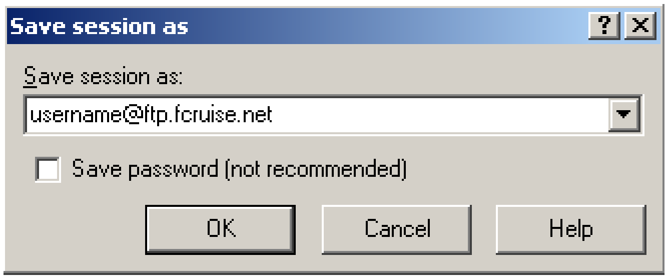
User name: username

Password: ••••••••

Figure 29: WinSCP Login Window

To get valid login credentials, please contact Oracle Hospitality Cruise Support. The server host name is ftp.fcruise.com at the moment of writing this document. It is important to select “SFTP” as file protocol.

You may save the server address and protocol settings for future use. While saving the session you can also save the password if you want. That would avoid the program to ask always for the password.


Save session as

Save session as: username@ftp.fcruise.net

□ Save password (not recommended)

Figure 30: WinSCP Save Session

After saving the session, and also when starting the WinSCP application, you will always get a list of your current saved sessions. From here you always can select a session and create a new connection without entering the login details again.

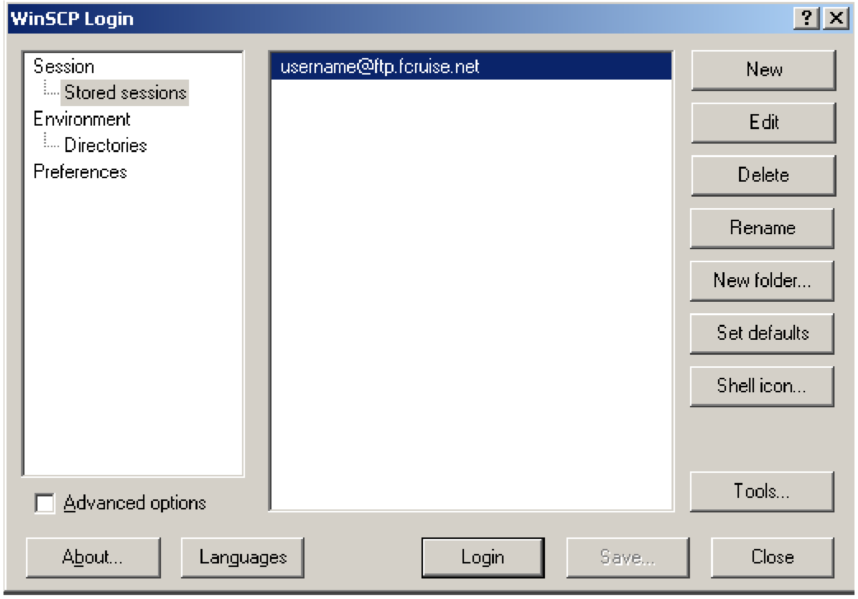
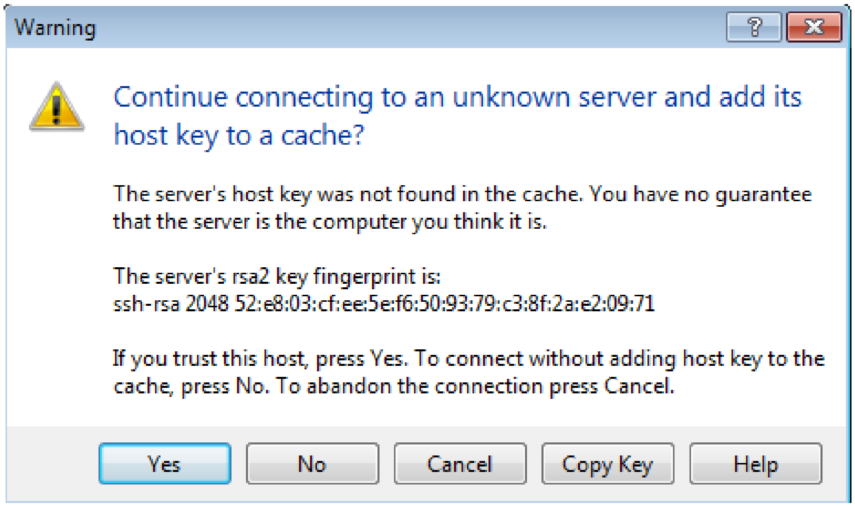


Figure 31: WinSCP Stored Session

It’s recommended to not save the password.

When you connect for the first time, you are asked to save the host key to the key cache. The rsa2 fingerprint shown below is the correct one of the server ftp.fcruise.com:



Continue connecting to an unknown server and add its host key to a cache?

The server's host key was not found in the cache. You have no guarantee that the server is the computer you think it is.

The server's rsa2 key fingerprint is:
ssh-rsa 2048 52:e8:03:cf:ee:5e:f6:50:93:79:c3:8f:2a:e2:09:71

If you trust this host, press Yes. To connect without adding host key to the cache, press No. To abandon the connection press Cancel.

Figure 32: FTP Server RSA2 Key Fingerprint

A small notification window will show you the state of the connection attempt.

PA-DSS Requirements Reference

10.1 If software updates are delivered via remote access into customers’ systems, software vendors must tell customers to turn on modem only when needed for downloads from vendor, and to turn off immediately after download completes. Alternatively, if delivered via VPN or other high-speed connection, software vendors must advise customers to properly configure a firewall or personal firewall product to secure “always-on” connections, per PCI DSS version 2.0 requirements 1 and 12.3.9.

Oracle Hospitality Cruise does not deliver automatically software updates via remote access.

9 Remote Access

9.1 Merchant Applicability

If Oracle Hospitality Cruise SPMS can be accessed remotely, all network connectivity should be performed using two-factor authentication per PCI DSS requirement 8.3. Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSLv.3/TLS or IPSEC) with individual certificates.

9.2 Remote Access Software Security Configuration

Implement the following applicable security features for all remote access software used by the merchant, reseller or integrator.

- Change default settings in the remote access software (for example, change default Passwords and use unique Passwords for each customer)
- Allow connections only from specific (known) IP/MAC addresses.
- Use strong authentication or complex passwords for logins.
- Enable encrypted data transmission.
- Enable account lockout after a certain number of failed login attempts.
- Configure the system so a remote user must establish a Virtual Private Network (“VPN”) connection via a firewall before access is allowed.
- Enable the logging function.
- Restrict access to customer Passwords to authorized reseller/integrator personnel.
- Establish customer Passwords according to PCI DSS requirements 8.1, 8.2, 8.4, and 8.5.
    - All users should be assigned a unique username.
    - The authentication methods should be consistent with the documentation.
    - Encrypt all passwords during transmission or storage on all system components.
    - Control the deletion and modification of user IDs, credentials and other identifier objects.
    - Verify user identity before performing password resets.
    - Set first-time passwords to a unique value for each user change immediately after each use.
    - Immediately revoke access for any terminated users.
    - Remove inactive user accounts at least every 90 days.
    - Enable accounts used by vendors for remote maintenance only during the time period needed.
    - Communicate password procedures for all users that have access to cardholder data.
    - Generic user IDs and accounts should be disabled or removed. Shared user IDs for system administration activities and other critical functions

should not be used. Shared and generic user IDs should not be used to administer devices in the environment. The use of wireless is expressly prohibited.

- The use of shared access IDs, including their use for administration purposes, is forbidden.
- Group and shared passwords are forbidden.
- Configuration settings should be set to enforce users to change passwords at least every 90 days.
- Configuration settings should be set to enforce user passwords to be at least seven characters long.
- Configuration settings should be set to enforce user passwords to contain both numeric and alphabetic characters.
- Configuration settings should be set to enforce new passwords to be different from the four previously used passwords.
- Configuration settings should be set to enforce user accounts to be locked out after not more than six invalid logon attempts.
- Configuration settings should be set to require a locked user account to remain locked for thirty minutes or until a system administrator resets the account.
- Configuration settings should be set to require that system/session idle time out features are set to 15 minutes or less.
- Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.

PA-DSS Requirements Reference

11.2

If the payment application may be accessed remotely, remote access to the payment application must be authenticated using a two-factor authentication mechanism, per PCI DSS 8.3.

11.3

If vendors, resellers/integrators, or customers can access customers’ applications remotely, the remote access software must be implemented securely, per PCI DSS 8.3.

10 Encrypting Network Traffic

10.1 Transmission of Cardholder data

Product uses encryption, such as SSLv.3/TLS or IPSEC, for transmission of cardholder data over public networks, per PCI DSS 4.1.

SPMS does not send cardholder data over public networks. The third-party EFT application is responsible for this action.

10.2 Email and Cardholder data

SPMS does not natively support the sending of email. As per PCI DSS requirement 4.2, cardholder data should never be sent unencrypted via email.

10.3 Non-Console administrative access

Product uses VPN for encryption of for all non-console administrative access to payment application or servers in cardholder data environment. Telnet or other non-encrypted access methods must not be used.

PA-DSS Requirements Reference

12.1

The payment application must use strong cryptography and security protocols such as secure sockets layer (SSLv.3) / transport layer security (TLS) and, internet protocol security (IPSEC)) to safeguard sensitive cardholder data during transmission over open, public networks, per PCI DSS 4.1.

Examples of open, public networks that are in scope of the PCI DSS are the Internet, Wi-Fi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS).

12.2

The application must never send unencrypted PANs by e-mail.

13.1

Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSLv.3/TLS for web-based management and other non-console administrative access, per PCI DSS 2.3.