



CSF International, Inc.
1629 Barber Road
Sarasota, FL 34240-9392
USA

NEWS • NEWS • NEWS • NEWS • NEWS • NEWS • NEWS • NEWS

CSF INTERNATIONAL, Inc.
Marketing Flash
Worldwide Sales & Marketing Communication

SWITCHWARE® Release 3.12
Product Update

SARASOTA FL, - July 1, 2010 – CSF International (CSFi) announces the upcoming release of SWITCHWARE® 3.12 scheduled for general customer availability during the 4thQ of 2010. This new release will offer many exciting new features including the incorporation of fraud monitoring and prevention, adherence to Visa issuer security rules, PCI-DSS and PA-DSS compliance, ATM personal preferences and base system enhancements such as CCM maker/checker functions.

Overview

General Information

Release 3.12 represents a major milestone for SWITCHWARE® as it incorporates real-time and background fraud prevention techniques, greater cardholder security measures in complying with PCS-DSS and PA-DSS standards plus adds enhanced functions including ATM personal preference selection and CCM maker/checker functions.

New Features in SWITCHWARE 3.12

The upcoming release of SWITCHWARE 3.12 will be available for general customer availability during the 4thQ of 2010. The items discussed in this section summarize the new features and functions incorporated into this new release:

UPGRADED FUNCTIONALITY & FEATURES v. 3.12	
1	Fraud Protection and Monitoring
2	PA-DSS Compliance
3	Denial of Foreign Transactions for a Cardholder
4	Limit Foreign Cardholder ATM Withdrawal Activity
5	ATM Personal Preferences
6	Removal of Card Sensitive Data in Online Process Trace Files
7	SSH Masking for SWITCHWARE Clients
8	Audit in all SWITCHWARE Clients
9	Maker/Checker Function for the CCM Client
10	Reason for Changing Card Status in CCM Client
11	EMV Issuer Enhancements

FRAUD PROTECTION AND MONITORING

SWITCHWARE release 3.12's fraud protection consists of monitoring transactions for fraudulent conditions plus configuring and managing the rules providing fraud protection. The outcome of transactions is based on rules validation performed in both real-time and background modes.

This is accomplished by...

- Identifying potential fraudulent activity based on pre-defined rules
- Providing transactional-based rules validation
- Managing the outcome of rules violations
- Providing dynamic rules configuration
- Maintaining a history of suspected fraud activity
- Implementing real-time and background mode processing

Unique qualities and characteristics associated with the new Fraud Protection and Monitoring features are identified as...

- A standalone SWITCHWARE interface
- Handling on-us cards only
- Real-time transaction processing
- Background transaction processing
- Offering both real-time and background mode – one application with the ability to run in different modes
- Configuration rules (parameters, active or inactive, reporting, etc) via a new client application
- View individual transaction data, rules validation results, statistics via a new client application

PA-DSS COMPLIANCE

PA-DSS (Payment Application Data Security Standard) is the worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands. It involves 12 basic rules that govern how every application, database, and business activity is to be maintained. SWITCHWARE release 3.12 meets the necessary PA-DSS requirements for properly storing, handling and disseminating sensitive cardholder data. SWITCHWARE 3.12 employs the latest developments in cardholder data protection standards. Prior to release, SWITCHWARE 3.12 will have completed the audit process and received certification for compliance with the PA-DSS requirements.

DENIAL OF FOREIGN TRANSACTIONS FOR A CARDHOLDER

This new feature will allow users to prohibit cardholder accounts from performing foreign transactions. This feature presents two new fields in the SWITCHWARE client application. Users will be able to “check” a box that will deny cardholders foreign transactions and a new field to identify the cardholder’s country of origin by setting the ISO country code. With these two pieces of information, the SWITCHWARE system can determine which transactions are foreign and decide whether to approve or void the activity.

LIMIT FOREIGN CARDHOLDER ATM WITHDRAWAL ACTIVITY

This new feature will allow users to manage foreign cardholder withdrawals. By creating new data elements and functions, SWITCHWARE can determine if a transaction is from a foreign cardholder, retain the information about this cardholder, and manage the withdrawal activity to prevent amounts from exceeding the daily foreign cardholder limit.

ATM PERSONAL PREFERENCES

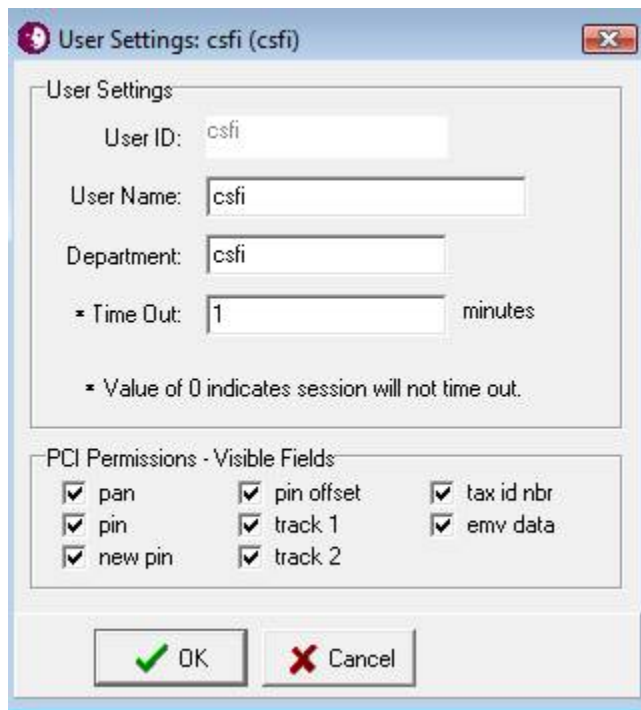
This feature enables the ATM user to define several transaction preferences at the ATM. After these preferences have been defined, the ATM program will present the cardholder

with a personalized experience when subsequent ATM transactions are performed by the cardholder. The preferences include:

- Language
- Favorite withdrawal amount
- Receipt / no receipt option for transactions
- Allow / deny transactions acquired in other countries

REMOVAL OF CARD SENSITIVE DATA IN ONLINE PROCESS TRACE FILES

The card sensitive data contained in the online process trace files (i.e. TPlog, SWXlog, etc.) can be removed in accordance with PCI-DSS standards. This new feature involves the modification in all the SWITCHWARE processes to remove or mask card sensitive data from log files that could potentially be compromised. The information in the database remains in the clear unless you implement an optionally-purchased data encryption method (not packaged with SWITCHWARE 3.12). You will be able to control whether or not the card sensitive data is masked by setting the appropriate permissions at the user level in SWITCHWARE's User Profiles client application (see Figure 1 below). Once these parameters are set, it will mask the data anywhere it's displayed in the SWITCHWARE client applications (System Monitor, Customer Card Management, etc.).



(Figure 1)

SSH SUPPORT FOR SWITCHWARE CLIENTS

This feature enhances the SWITCHWARE client to server communications protocol and upgrades the communication channels conducted using telnet. The older versions of SWITCHWARE incorporated a generic telnet protocol as the standard client/server communication protocol. The new version of SWITCHWARE offers a secure telnet protocol for client to server communications.

MAKER/CHECKER FUNCTION FOR CCM CLIENT

This feature enhances the SWITCHWARE software by creating a validation mechanism in the CCM client. This Maker/Checker feature is designed to validate any data that is entered or changed in the CCM client application. For any change made at least two people are now required to complete the modification. This new feature will create stricter controls on any changes made, and errors will be spotted sooner allowing corrections to be achieved before the changes can be finalized in the production system.

REASON FOR CHANGING CARD STATUS IN CCM CLIENT

This new feature improves the SWITCHWARE software by modifying the CCM client application, by creating a new table, and by modifying the existing cardholder table. Now when a user changes the card status in the CCM client from “Active” to anything other status a combo box will appear with all possible reason codes in order to describe why the change in status is occurring. The user can select any one of the pre-defined reason codes in this combo box to explain the reason for the change.

EMV ISSUER ENHANCEMENTS

This new feature will enhance the way in which SWITCHWARE supports post issuance scripts for EMV card products issued. Some of these enhancements include...

- When a card status is changed, the CCM client will insert a command based on the EMV block type found in the cardholder status table to block the card, or block the application or do nothing.
- Provides a new rule which will automatically unblock offline PIN access if the online PIN is validated.
- Provides a new rule to validate PIN first against the new PIN, but if it fails, the system will validate the PIN against the old online PIN and replace the new online PIN with the old online value if it succeeds.
- System will decode CVR and TVR for any EMV transaction inserts the data into the log-record and cardholder transaction tables.
- A new rule that will decline a transaction based on electronic signature.

ADDITIONAL MODIFICATIONS

Several database tables are being modified to include log record tables, providing host systems that the ability to support different types of interface functions and automatic updates to SWITCHWARE.