

Trams PCI FAQ's

The purpose of this document is to explain the encryption process and other changes in Trams software products with the goal of helping agencies be PCI compliant.

DISCUSSION POINTS:

- What is PCI?
- How Does Encryption Work?
- Does Encryption Delete or Hide Credit Card Numbers in the Database?
- What Other Changes Will I See in the Database after Encryption?
- How Do I Know if the Database is Encrypted?
- What Type of Encryption Does Trams Use?
- What Are Other Changes in Trams Software in Future Releases?
- Where Can I Find More Information?

What is PCI?

The payment card industry (PCI) compliance and validation regulations spell out what security measures must be taken to protect the private information during any transaction occurring with the use of a paycard. The PCI Data Security Standard is used by all card brands to assure the security of the data gathered when transacting on behalf of a customer.

There are two different types of PCI standards:

1. PCI-DSS
2. PA-DSS

PCI-DSS covers the overall security of Credit Card data storage and transmission.

PA-DSS covers turnkey software that is installed on the client premises that needs to be PCI-compliant.

For more information regarding PCI please visit: <https://www.pcisecuritystandards.org/index.shtml>

Fundamental PCI Guidelines

- Don't store CC data if it's not absolutely needed.
- Mask CC data as much as possible.
- Encrypt CC data wherever it is stored.
- Implement controls so only people who need access to the unmasked CC data can see it.

Current State of Trams Products

TBO/CBW/CBB-Standalone

- As of TBO 3.3 and CBW 3.6, all regular CC and customer bank account data stored in the database is encrypted, (AES 256-bit encryption) and access to unencrypted data is controlled and logged.

Database Central/CBMS

- All sync copies in DBC are either encrypted (CBW 3.4 and up) or are not storing Credit Card data.

Live Connect and Sync

- These systems pass encrypted data from ClientBase via web services or web apps.
- The data transmissions use SSL and HTTPS to encrypt data being sent from CB to the booking engine or Sync Web Service.

Password Security (CBW 3.06.xx and TBO 3.04)

- Password Strength: At least 8 chars, alpha + numeric.
- Forced Renewal: Password must be changed every 60 days.
- No repeating Passwords: System remembers the last 4 passwords entered.
- Requires Interbase XE

ENCRYPTION

How Does Encryption Work?

Our first step into encryption was in 2008 with the releases of CBW 3.04, TBO 3.01 and CBB 2.0. If your database was updated to TBO 3.01 and then CBW 3.04 (in that order), then during running the cbplusup.exe database update, any existing credit card numbers were standardized by a cleaning process, then masked and encrypted. If your database was not on those versions, then the encryption may have taken place during a later update (for example, TBO 3.02 and CBW 3.05). If you only subscribe to one Trams product, then you would still need to run the database update for both CBW and TBO. In subsequent releases, we added a re-masking routine for valid credit card numbers that were missed in the first round of encryption.

Does Encryption Delete or Hide Credit Card Numbers in the Database?

No, the encryption process does not hide, remove, or delete credit card numbers from your database. However, in all Trams programs we do not display the full credit card number unless absolutely necessary. Most screens will display a masked version (example: Should be changed to read VI 41-XXXX-1111). In ClientBase and Trams Back Office, viewing the full credit card number is controlled with user permission so the agency can determine which users have access to full credit card numbers.

What Other Changes Will I See in the Database after Encryption?

When entering credit card data, we perform a validation on the card number. If ClientBase detects the number is invalid, it prompts the user with a message. Trams Back Office currently does not have this functionality.

Along with encryption, a unique encryption key was generated for each agency that can be used in product development for applications that will need to read the full credit card number. Documentation for use is available upon request by e-mailing support@trams.com.

In ClientBase, we added a prompt when connecting to a Live Connect provider that uses HTTP and not the secure connection (HTTPS).

In ClientBase, we added an option to clear the Credit Card security codes from your database and hide that field.

How Do I Know if the Database is Encrypted?

In ClientBase Windows, go to Help|About ClientBase. If CC Encryption Done = Yes, then your database is encrypted.

In Trams Back Office, go to Help|About. If Database Encrypted = Yes, then your database is encrypted.

In ClientBase Browser, go to Tools|About. If CC Encryption Done = Yes, then your database is encrypted.

ClientBase Online has always been encrypted.

What Type of Encryption Does Trams Use?

Trams' encryption is AES 128-bit. Passwords are stored encrypted in the admin.ib file on the server. Interbase password encryption is DES.

Can encryption key access can be restricted in terms of access?

Key is generated from a password. Only provide password to those with permission to generate key.

What Recent Additions Have Been Added?

- In all products, the encryption password is changed with each new release.
- In TBO 3.03 and CBW 3.06, a purging routine was added that masks full credit card numbers permanently based on a user definable as of date to conform to PCI compliance regulations.
- In TBO 3.03, a user permission to view the full credit card number and to run reports that display the full credit card number.
- CBO (version 2.3 and higher) now locks users out after X number of failed attempts.

What Are Other Changes in Trams Software in Future Releases?

In TBO and CBW, allow user to change their own password, as well as Password.

In TBO and CBW, lock users out after X number of attempts logging in.

Where Can I Find More Information?**Trams Back Office Encryption Release Notes:**

<http://static.trams.com/tramslibrary/documentation/encryption/tboEncryptionReleaseNotes.pdf>

ClientBase Windows Encryption Release Notes:

<http://static.trams.com/tramslibrary/documentation/encryption/cbwEncryptionReleaseNotes.pdf>

ClientBase Browser Encryption Release Notes:

<http://static.trams.com/tramslibrary/documentation/encryption/CBbEncryptionReleaseNotes.pdf>