FAQ 1-4UJFZM - Is PIN encryption optional in Banner 8.0

Q: Is PIN encryption optional in Banner 8.0?
A: No, beginning with Banner 8.0, PINs are always encrypted in GOBTPAC_PIN. The only option involves whether or not to encrypt the PIN in the history table (GORPAUD_PIN).

PIN Encryption

Current PINs are stored in GOBTPAC_PIN. The history of PIN changes, including the current PIN, are stored in GORPAUD_PIN.

Starting with release 8.0, GOBTPAC_PIN and GORPAUD_PIN values are stored in the database in encrypted form.

A cryptographic hash is used to transform the PIN before it is stored, so that the unencrypted form of the PIN can never be retrieved from the database.
The cryptographic transformation is a one-way process, so that even if someone were able to retrieve the encrypted PIN from the database and learned the details of the encryption process, they still would not be able to decode the original, unencrypted form of the password.

Note
One-way encryption means that even the security administrator cannot retrieve the PIN. If a user forgets a PIN, you cannot look up the PIN for the user. The only recourse in that situation is to reset the user's PIN.
"Resetting a User's PIN" on page 17 of the Banner General 8.0 Release Guide

For additional security, the PIN is "salted" before it is encrypted. *Salt*, in this context, refers to a randomly generated string that is added to the PIN before encryption. This adds another layer of complexity to the encryption.
When a user enters a PIN to gain access to the system, the user's entered PIN is transformed using the same cryptographic function. The transformed string entered by the user is then compared to the hashed PIN stored in the database. If the values match, the user is allowed to proceed.

Bypassing PIN Encryption in GORPAUD

Encryption of the PIN history in the GORPAUD table is optional at this time to allow for integration with third party systems such as Web CT or Blackboard.

If your institution finds it necessary to retrieve an unencrypted PIN from Banner, you can bypass PIN encryption on the PIN History Table (GORPAUD_PI) If your institution is using e-Learning products (such as Web CT or Blackboard), you should check whether the version you are running supports PIN hashing. If it does not

support PIN hashing, you should not encrypt user PINs on GORPAUD. Even if your e-Learning software supports PIN hashing, you should check whether Banner's change to PIN hashing will require changes to the e-Learning system.

PIN encryption is performed during the Banner General 8.0 upgrade process, when the script gdrgorpaud_080000.sql executes a conversion of the PIN field in the GORPAUD audit table to a hashed value and turns on hashing.
To bypass PIN encryption, do not run the gdrgorpaud_080000.sql script during the upgrade. See the Banner General 8.0 Upgrade Guide for details of the upgrade process.
You must also set the New GTVSDAX flag with internal code GENPIN to N in order to have PINs saved unencrypted to the GORPAUD table.

NOTE: PINs are always encrypted on GOBTPAC_PIN.