ellucian.

Banner Student
Release Guide

Release 8.7.3
February 2015

Revision History

Publication Date	Summary
February 2015	New version that supports Banner Student 8.7.3 software.

Contents

Introduction

The Banner® Student 8.7.3 release contains enhancements and change requests.

Enhancements include:

- Baseline support for updates to the Admissions Application Self-Service PIN.

- Summary information for a Job Submission enhancement that is associated with the Banner General 8.7.3 release.

- Updates to two CAPP tables for the resolution to a change request related to split courses and the count in GPA value.

- Updates to a validation form and table to support Banner Student 9.2 APIs.

Admissions Application PIN

New functionality has been added to enhance admissions application PIN processing and provide strong passwords as requested in IDEA-16385 and IDEA-19248. The changes pertain to first time user account creation and the returning user login process for applicants in Self-Service. Previously, an unsecured PIN of six characters had been created in clear text format. The PIN display is now encrypted, the PIN length has been expanded, and alpha characters can be used in the PIN.

Existing controls on the Enterprise PIN Preferences Form (GUAPPRF) are used for PIN format and length. PINs must conform to the PIN reset format, number or character options, and minimum and maximum length as defined on GUAPPRF. Error messages are displayed if the new PIN does not meet the requirements.

> **Note:** Any changes made to the GUAPPRF preferences for applicants will also apply to current students.

The **PIN** field length on the Electronic Application Process Form (SAAEAPS) has been expanded. The created PIN is displayed as an encrypted value (a series of asterisks). The PIN can be reset by the administrator. It is recommended that the administrator note the PIN before it is reset, so the information can be provided to the applicant.

When first time user login credentials are created in Self-Service Admissions, the rules on GUAPPRF are checked to see if the new password meets the rule criteria. A message is displayed to inform the applicant of the requirements. If the password conforms to the rules, the applicant can continue to log in.

The returning user login is also validated based on the settings on GUAPPRF. If the login does not meet the requirements, the new Change PIN page (`bwskalog.P_DispChangePIN`) is displayed. The applicant must change the PIN to continue by entering the old PIN, entering the new PIN, and re-entering the new PIN for confirmation. The old PIN is validated against the stored PIN. Once it has been authenticated, the new PIN is stored.

When the PIN is successfully updated, the applicant is logged in and taken to the Select an Application Type page (`bwskalog.P_DispChoice`) to start a new application or the Application Menu (`bwskalog.P_DispChoices`) for existing and in process applications.

When the login authentication fails, an error is displayed. Error messages indicate the PIN requirements as defined on GUAPPRF. If an applicant submitted an application before this enhancement was applied, and a PIN was used that does not meet the new requirements, the student will need to change the PIN.

Once the applicant has been admitted to the institution, the secure login and PIN are sent to him/her. The Third Party Access Audit Form (GOATPAD) is then used to manage the PIN.

> **Note:** It is recommended that Info Text for the login pages be reviewed and references to the previous PIN requirements be updated.

Refer to the *Banner Student Self-Service Release Guide 8.7.1* for information on additional changes for this enhancement.

Changed form

The following form has been modified.

Electronic Application Process Form (SAAEAPS)

The Change PIN window/Non-Student PIN Change block has been updated. A new field has been added, and existing fields have been reordered.

The new field order is:

- **Identifier**

- **Web Access Locked**

- **Transaction Packet**

- **PIN** - displayed as ********

- **Confirm New PIN** (new field) - displayed as ********

- **Activity Date**

- **Web Last Access Date**

The length of the **PIN** field has been expanded to 256 characters and is encrypted. This length is used because the encrypted value of the PIN allows for 256 characters. However, the user is not allowed to enter a password of that length. Instead, the value of the **Maximum Length** field on the Enterprise PIN Preferences Form (GUAPPRF) is used to validate the maximum length of the password.

The PIN is no longer displayed as clear text. Therefore, when your institution needs to provide a new PIN for a student who has forgotten his/her PIN, the administrator should make note of the PIN and provide it to the student.

The **Confirm New PIN** field is used to re-enter and verify the PIN entered in the **PIN** field. The following controls defined on GUAPPRF are checked to see if the new PIN meets the required criteria. When the PIN does not meet the required criteria, the necessary corrections are displayed in the auto hint.

- **PIN Reset Format**

- **Minimum Length**

- **Maximum Length**

- **Number Required Indicator**

- **Character Required Indicator**

Changed table

The following table has been modified.

Electronic Admissions Non-Student Table (SABNSTU)

An existing column has been modified, and a new column has been added.

The `SABNSTU_PIN` column has been expanded from 6 to 256 characters to hold an encrypted password. The value is displayed as "**********..."

The column comment has been updated. It now reads:

> PERSONAL IDENTIFICATION NUMBER. It is used together with the Login ID to access the Admissions Self-Service system. Value must be according to PIN_PREFERENCE rule defined in GUAPPRF form.

A new column has been added to this table.

- `SABNSTU_SALT`   `VARCHAR2(128)    Null`

The column comment is:

> SALT: This column is used internally.

Changed package

The following package and package body have been modified.

SAKLIBS/SAKLIB1

New functions and procedures have been added.

Function/Procedure	Description
`f_sabnstu_rec_exists`	Checks if the record is available in SABNSTU based on the Person Reference Number (AIDM), ID Number (ID), or Row ID (ROWID). Returns Y if a record exists, otherwise N.
`f_check_pin_verifypin_matching`	Checks if the PIN and Confirm PIN values passed are a match. Returns Y if values are matching, otherwise N.

Function/Procedure	Description
f_get_abbreviated_text	Returns text in HTML tag format for abbreviated text, such as PIN, PIDM, and ID. When user points to PIN, PIDM, or ID (on a Self-Service page), the full text for that word is displayed.
	For example, Personal Identification Number for PIN, Internal identification number of the person for PIDM or, Identifier for ID.
f_validate_sabnstu_pin	Authenticates user-entered PIN with the PIN stored in SABNSTU. Returns 1 when user ID and PIN match. Returns 0 when user ID is found but PIN does not match that user ID. Returns -1 when user ID is not found.
f_validate_new_user	Performs general validation for the user ID and PIN entered for creation of a new user account. Returns True or False, error message, and procedure to be executed next.
f_validate_existing_user	Performs general validation for the user ID and PIN entered for login. Returns error message and procedure to be executed next.
f_get_not_web_ind	Returns value of the constant CONST_NOT_WEB_IND declared in the package specification. Required, as the value of constant is used in Oracle forms, and Oracle forms cannot access this directly.
f_get_oldpinencrypted_ind	Returns value of the constant CONST_OLD_PIN_ENCRYPTED_IND declared in the package specification. Required, as the value of constant is used in Oracle forms, and Oracle forms cannot access this directly.
p_change_pin	Performs all validation for **the New PIN** value and saves the new PIN for existing an user who is changing his/her PIN.
	Called from the P_ProcChangePIN procedure in BWSKALOG and the P_ProcChangePIN() procedure used by SAAEAPS.
p_create_upd_sabnstu	Creates and/or updates the SABNSTU record for user logins.
	Returns error message and procedure to be executed next.

New scripts

The following scripts are delivered with this enhancement.

> **Note:** Unless otherwise noted, new scripts are run as part of the upgrade process for a release.

Script	Result
sabnstu_080703_01.sql	Adds new column, expands existing column
sabnstu_080703_02.sql	Adds new column comment, updates existing column comment

Job Submission Enhancement

Updates have been made in Banner General 8.7.3 to protect user passwords from possibly being exposed when Banner baseline job submission is running in a Unix/Linux operating system environment.

> **Note:** Please see the *Banner General Release Guide 8.7.3* for more information on this enhancement. See the *Banner General User Guide* and the *Banner General Technical Reference Manual* for more information on using job submission.

Job submission processing has been changed to not include authentication credentials on the command line, but instead write them to the file system in a read-protected file. The file is only readable by the job submission owner (the GURJOBS process) and is immediately deleted when it is no longer needed by job submission processing.

- The new **Filesystem Credentials** check box on the Process Maintenance Form (GUAJOBS) is used to indicate whether a report or process will use the authentication credential security.

- A corresponding column has been added to the GJBJOBS table. The GJBJOBS_CREDS_IN_FILE column is used to hide the password credentials in job submission.

  - When this column is set to Y, the new password security is used when jobs are run, and credentials are obtained from the file system.

  - When this column is set to N or Null, the job is run in the traditional manner, without the enhanced password security.

COBOL files have been modified to use secure credentials in Linux. The pseudo password NOTVALIDPSSWD is used when a job is run, while the actual username and password are written to a file and are not shown on the command line.

The following COBOL `.shl` files in Banner Student have been modified to use this security.

- `crqc3000.shl`

- `schc3000.shl`

- `sctc1000.shl`

- `sctc1500.shl`

- `sctc2000.shl`

- `sctd0600.shl`

- `scth1000.shl`

- `slrsche.shl`

CAPP Updates

CAPP changes are delivered for the resolutions to change requests CMS-DFCT103851 and 1-FCEILK.

The issue concerned the following situation. When credits from a transfer course were split, the split credits were counted in the GPA hours in a subsequent area, even though the **Count in GPA** flag on SHAGRDE was unchecked. This resulted in an incorrect GPA calculation.

The split hours were being counted because the wrong value was available for the course in the `course_grde_gpa_ind` variable. This variable is used to look at the setting of the **Count in GPA** flag on SHAGRDE (checked or unchecked) and tell compliance whether or not the credits for the course are counted in the GPA. This checking is performed in the `count_cred_crse()` procedure.

The SMTSPAT and SMTSPLT temporary tables are used to store the split course data. A new column has been added to each table to store the SHAGRDE **Count in GPA** flag value for the split course.

The SMREVAL process has also been modified to use the new table columns.

Changed tables

The following tables have been modified.

Compliance Split Course Attribute Temporary Table (SMTSPAT)

A new column has been added to store the course grade GPA indicator.

- `SMTSPAT_CRSE_GRDE_GPA_IND    VARCHAR2(1)   Null`

The column comment is:

> COURSE GRADE GPA INDICATOR.Yes or No flag to indicate if course should be counted in GPA hours.

Compliance Split Courses Temporary Table (SMTSPLT)

A new column has been added to store the course grade GPA indicator.

- `SMTSPLT_CRSE_GRDE_GPA_IND    VARCHAR2(1)   Null`

The column comment is:

> COURSE GRADE GPA INDICATOR.Yes or No flag to indicate if course should be counted in GPA hours.

New scripts

The following scripts are delivered with this enhancement.

Note: Unless otherwise noted, new scripts are run as part of the upgrade process for a release.

Script	Result
smtspat_080703_01.sql	Adds new column
smtspat_080703_02.sql	Adds column comment
smtsplt_080703_01.sql	Adds new column
smtsplt_080703_02.sql	Adds column comment

Validation Update

Changes have been made to support the Banner Student API 9.2 release.

Changed form

Two new fields have been added to the Academic Year Validation Form (STVACYR). These fields are used by integrated third party systems to store academic year start and end dates. The dates are used for transactions that occur within a date range rather than a term range. The fields can be Null.

These changes support the Banner Intelligent Learning Platform (ILP) integration and the Higher Education Data Model (HEDM) APIs. The HEDM schema requires the provision of start and end dates. The associated API exposes academic periods (terms, parts of term, and academic years) from Banner.

Fields	Description
Start Date	Academic year start date for the academic year code.
End Date	Academic year end date for the academic year code.

Changed table

Two new columns have been added to the Academic Year Validation Table (STVACYR).

- `STVACYR_START_DATE` `DATE` `Null`

- `STVACRY_END_DATE` `DATE` `Null`

The column comments are:

- ACADEMIC YEAR START DATE: This field identifies the academic year start date.

- ACADEMIC YEAR END DATE: This field identifies the academic year end date.

New scripts

The following scripts are delivered with this enhancement.

Note: Unless otherwise noted, new scripts are run as part of the upgrade process for a release.

Script	Result
stvacyr_080703_01.sql	Adds new columns
stvacyr_080703_02.sql	Adds new column comments

Resolutions

The *Banner Student Resolutions Report 8.7.3* is a companion to this release guide. The Resolutions Report provides summary information about the change requests that are resolved in Banner Student 8.7.3. Use the following steps to access the Resolutions Report on the Ellucian Support Center:

1. Go to the Ellucian Client Support web site: http://www.ellucian.com/Solutions/Ellucian-Client-Support.

2. Click the **Ellucian Hub** button to log in to the Ellucian Hub.

3. Choose the Ellucian Download Center application.

    or

    Choose the Ellucian Support Center application.