Banner General Release Guide

Release 8.0
February 2010 (Revised)

SUNGARD HIGHER EDUCATION

Trademark, Publishing Statement and Copyright Notice

Prepared by: SunGard Higher Education

4 Country View Road
Malvern, Pennsylvania 19355
United States of America
(800) 522 - 4827

Customer Support Center Website

http://connect.sungardhe.com

Documentation Feedback

http://education.sungardhe.com/survey/documentation.html

Distribution Services E-mail Address

distserv@sungardhe.com

Revision History Log

Publication Date	Summary
April 2008	New version that supports Banner General 8.0 software.
February 2009	Clarified PIN encryption information.
February 2010	Revised version to address documentation defect 1-6OZ6TS.

Banner General 8.0 Release Guide

Contents

Section 5 Internationalization - Functional

Section 6 PIN - Technical

Introduction

This guide documents Release 8.0 of the Banner General System. Release 8.0 includes enhancements and problem resolutions.

This document describes the following enhancements, which are new for Release 8.0.

PIN Maintenance

Encryption and other changes have made Self-Service PINs more secure.

Security Administration

The process of managing Banner security has improved, and an extensive security auditing capability has been introduced.

Partial Character Masking

Fields that hold character data can now be partially masked, providing another option for obscuring sensitive data.

Supplemental Data Engine

This new tool lets you store and view supplemental data that is not part of the Banner data model.

Internationalization

The Internationalization enhancement supports global naming and address standards. Bio-demographic and currency fields have been expanded in Banner General to accommodate US and non-US standards.

Documentation Change for Problem Resolutions

Problem resolutions are summarized by module at the end of this release guide. The detailed description, impact, and resolution information for each problem resolution is delivered in a separate `.txt` file. The file for this release is named `general80000resolutions.txt`. As a result of this change, information about problem resolutions is more consistent between release guides and the Customer Support Center.

Cumulative Documentation

This document provides detailed information about the Banner General 8.0 release only. Banner General 8.0 is a cumulative release that also includes enhancements, RPEs, and problem resolutions delivered in the General 7.0.1, 7.1, 7.1.1, 7.2, 7.3, 7.3.1, 7.3.2, 7.4,

7.4.1, 7.4.2, 7.5, and 7.5.1 releases. For complete documentation about these interim releases, please refer to the interim release guides identified in the table that follows.

Release Number	Contents	Release Date
7.0.1	SEVIS	May 2005
7.1	Oracle Reports, Institutional Roles, CBO, Address Source Code	May 2005
7.1.1	APIs	August 2005
7.2	Race and Ethnicity, Common Matching, Intcomp, VBS	October 2005
7.3	Common Matching, Multi-Institution Functionality, API, Large Object Storage, Oracle Reports, WebUtil, Internationalization	May 2006
7.3.1	Institution Role	June 2006
7.3.2	Multi-Institution Functionality for Voice Response	September 2006
7.4	Integration Components, Immunization Information, Data Extract, Multi-Institution Functionality for Job Submission	November 2006
7.4.1	Luminis Platform IV Support	March 2007
7.4.2	SEVIS	September 2007
7.5	Tab-Level Security, SSN Searching in ID Fields, Job Submission Security, Workflow Form Exit Warning	September 2007
7.5.1	Banner Enterprise Identity Services Support	November 2007

1 PIN - Functional

Overview

Release 8.0 introduces several enhancements to improve the security of PINs (passwords) for Banner Self-Service products.

- PINs are stored in encrypted form.
- Institutions can now set and enforce standards for strong passwords.
- A new PIN reset mechanism has been established.

Note

PIN is an abbreviation for *personal identification number*, a term that is usually used to refer to a numeric password. In earlier versions of Banner numeric passwords were used and were called PINs. Although passwords can now be alphanumeric, they are still referred to as PINs. In this document, *PIN* and *password* are used interchangeably.

See “PIN - Technical” on page 65 for more information about this feature.

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.

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_PIN`). See “Bypassing PIN Encryption in GORPAUD” on page 66 for details.

Warning

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. ■

Strong Passwords

If a password can be easily guessed by another person, it does not provide much protection. Security experts recommend using “strong passwords,” ones which are long and complex enough that it would be nearly impossible for someone to guess them.

This release provides support for strong passwords. Because there are varying standards for strong passwords, Banner has introduced a flexible approach based on institutional preferences. Your institution can enforce its own strong password standards for Banner PINs. The institution’s rules are set up on the GUAPPRF form and are stored on the GUBPPRF table.

- You can specify a minimum and maximum permissible length for your users’ PINs.
- You can require that PINs include letters, digits, or both letters and digits.
- You can restrict a user’s re-use of PINs. Specifically, you can set a number of days during which a user’s previous PIN cannot be reused.

Resetting a PIN

For occasions when a user forgets a PIN, the process for resetting the user's PIN has been made more secure. The user can request a PIN reset by answering a series of security questions with answers that the user previously provided.

Your institution can decide how many questions a user must answer for a PIN reset. You can also decide whether users can generate their own security questions, or whether they must use standard questions established by the institution.

The user's answers to security questions are stored in encrypted form, just as the PIN is.

PINs can be reset on the GOATPAD form by typing in the new PIN and then retyping the new PIN in the Confirm PIN field.

PINs can also be reset by clicking the **Reset** button on GOATPAD or GOATPAC. The PIN will be reset based on the settings on GUAPPRF. If the reset format is set to *Random*, you will not be able to determine what the PIN is.

To extract a clear text PIN, you would need to run letter generation and create a letter using a function to reset the PIN again and display the PIN prior to encrypting it.

Impact for Security Administrators

When implementing this release, your institution's security administrators and security policy makers must:

1. Determine if PINs in the PIN History Table (GORPAUD) can be encrypted.
2. Decide on the institution's rules for PINs and security questions.
3. Make appropriate settings in the GUAPPRF form to implement those rules.
4. Establish the institution's standard security questions in GUAQSTN.
5. Manage the conversion of security questions and answers to encrypted form.

   Users' security questions and answers, previously stored in unencrypted form, are migrated to the new tables, with the answers encrypted, during the General 8.0 upgrade. Security administrators should then confirm that the migration was completed successfully. If so, the data in `GOBTPAC_QUESTION`, along with the unencrypted answer data in `GOBTPAC_RESPONSE`, can be considered obsolete, and you can decide when and whether to delete those two columns' data.

Note

The `GOCTPAC_QUESTION` and `GOBTPAC_RESPONSE` columns will be made obsolete in a future release. ■

Impact for End Users

When a Self-Service end user logs in with a PIN for the first time in Release 8.0, the institution's new PIN rules established in GUAPPRF will be enforced. If a user's PIN does not conform to the institution's rules, the user will be prompted to create a new PIN during the login process.

The user will also be prompted to set answers for security questions in accordance with the security question policies established in GUAPPRF.

Tasks

Implementing this release's enhancements may require Self-Service Banner users to change their PINs and set up new security questions after they log on to Self-Service the first time after the implementation of this release. See the *Banner Web General 8.0 Release Guide* for details.

Several tasks for security administrators have changed.

- Creating a Set of Security Questions
- Setting the Institution's PIN Policies
- Verifying a User's Answers to Security Questions
- Resetting a User's PIN
- Using Letter Generation to Notify a User of a New PIN

Creating a Set of Security Questions

Security questions are used as part of the Self-Service PIN reset process. You can allow users to create their own security questions, or you can specify standard security questions that all users at your institution must use—or you can use a combination of institution-defined questions and user-defined questions.

To create a set of standard security questions:

1. Navigate to the PIN Questions form (GOAQSTN).
2. For each question, create a new record with the text of the question.
3. Check the **Display** check box for each question that you want to be visible to Self-Service end users.

Setting the Institution's PIN Policies

The institution's PIN policies are maintained in the Enterprise PIN Preferences form (GUAPPRF). Several new fields have been added, giving you more control over users' PINs, security questions and answers, PIN reset, and PIN notifications.

Verifying a User's Answers to Security Questions

A security administrator can use the GOATPAD form to verify a user's identity by checking the user's answers to security questions. The answers should match the user's previously stored answers to the questions.

Because the user's stored answers are encrypted, you cannot view them directly. Instead, the user's new answers are encrypted using the same hashing process and the two encrypted values are compared.

To verify a user's answers to security questions:

1. Navigate to the Third Party Access Audit form (GOATPAD).
2. In the key block, enter or select the user's ID.
3. Navigate to the **Verify Answers** tab. The user's security questions are displayed.
4. For each question:
   4.1. Ask the user the question.
   4.2. Type the user's answer into the Verify Answer field
5. Click Verify. For each new answer that matches the user's stored answer, the **Verified** check box will be checked.

Resetting a User's PIN

To reset a user's PIN by assigning a new PIN in GOATPAD:

1. Navigate to the Third Party Access Audit form (GOATPAD).
2. In the key block, enter or select the user's ID.
3. Change the PIN using either of these methods:
   - Type a new PIN in the **PIN** and **Confirm New PIN** fields.

- Click the reset button to the right of the **PIN** field.

Note

If you use the reset button, the value of the new PIN depends on the institution's PIN reset value preferences (as established on the GUAPPRF form).

4. Save the record

Using Letter Generation to Notify a User of a New PIN

User PINs are encrypted using a one-way process and cannot be retrieved from the database. If the institution's PIN reset value (selected on the GUAPPRF form) is *Random*, the only way to see the new PIN value in clear text (unencrypted) is to obtain it from the API prior to hashing. You can do this using the Banner Letter Generation process.

To reset PINs and notify users through Letter Generation:

1. Select the single user or group of users who will have their PINs reset.
2. Create a letter which contains the variable `*PINRESET`.

   The `*PINRESET` variable is delivered with Release 8.0. It selects `GB_THIRD_PARTY_ACCESS.F_PROC_PIN(GOBTPAC_PIDM)` from `GENERAL.GOBTPAC`. This variable calls a function which resets the PIN and delivers the clear text PIN to the .doc file when GLRLETR is run.
3. Run GLBDATA for your Population selection to populate it, or manually add people to the Population Selection via GLAEXTR.
4. Run GLBLSEL for your letter that contains the *PINRESET variable
5. Run GLRLETR for your letter which contains the *PINRESET variable. The reset variable will reset the PINs for the population selection and will insert the value of each new PIN in the .doc file.
6. Forward the notification letters to the affected users.

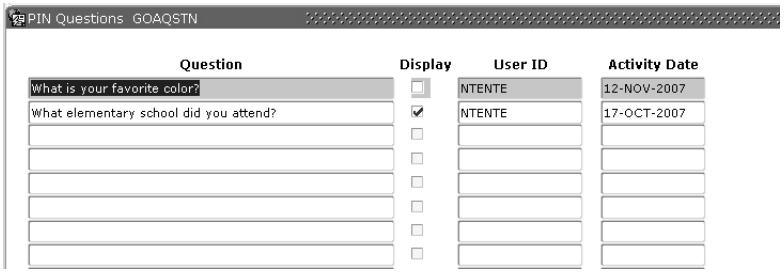
Note

PINs can be generated for users that do not yet have a PIN by running the GURTPAC process. In addition, PINs can be generated when a record is created for that user in any of the tables selected in the Table PIN Creation Controls block on GUAPPRF.

New Forms

PIN Questions (GOAQSTN)

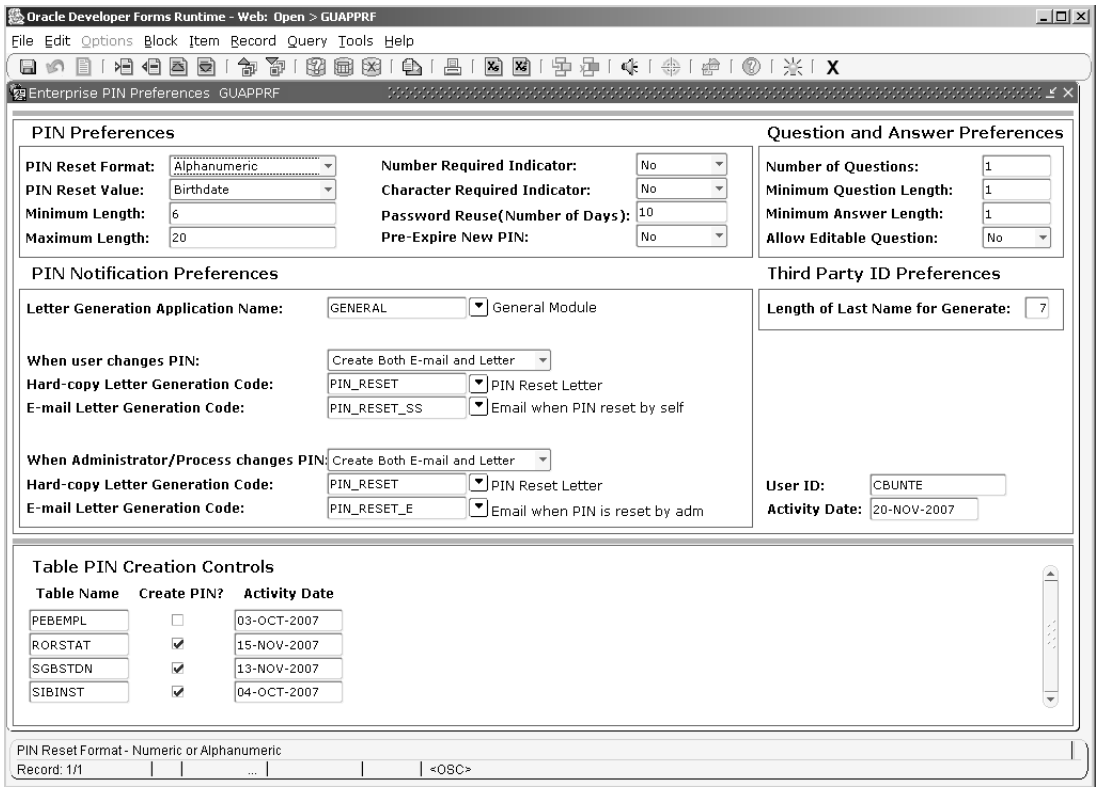
This new form is used to maintain the list of institution-defined security questions stored in the GOBQSTN table.



Fields	Descriptions
Question	The text of the security question.
Display	If selected, the question will appear in the list of questions in Self-Service for users to choose.
User ID	ID of the user who last changed the record.
Activity Date	The date the record was created or last changed.

Changed Forms

Enterprise PIN Preferences (GUAPPRF)



PIN Preferences

Several new fields were added.

Fields	Descriptions
Minimum Length	The minimum permitted length for a user's PIN.
Maximum Length	The maximum permitted length for a user's PIN.
Number Required Indicator	If *Yes*, each user PIN will be required to contain at least one numeric character.

Fields	Descriptions
Character Required Indicator	If *Yes*, each user PIN will be required to contain at least one alphabetic character.
Password Reuse (Number of Days)	The number of days during which a user's previously used PIN will not be allowed to be reused. If you do not want to restrict Password Reuse, set this to *0* (zero). **Note:** This preference is applied only when PINs are changed through Self-Service. PINs changed through GOATPAD, GOATPAC, or Letter Generation are not affected by this value.

Question and Answer Preferences

Use this section to set preferences for the security questions and answers used in the Self-Service PIN reset process.

Fields	Descriptions
Number of Questions	The number of security questions a user is required to answer during the PIN reset process. **Note:** If you reduce the number of questions required, a user's already-defined questions will be retained even though the user will only see a subset of them (the number of questions specified here). Under these circumstances, if a user attempts to change a question, the full set of questions is used when determining if the new question is unique. This could result in error messages that will be confusing to users. Because of this potential for confusion, reducing the number of questions required is not recommended.
Minimum Question Length	The minimum number of characters required for user-created security questions. For example, you can set a value long enough to ensure that a user creates a real question.
Minimum Answer Length	The minimum number of characters accepted in a user's answer to a security question.
Allow Editable Question	If Yes, a user can create a new security question to be used during the PIN reset process. If No, the user may not create a question but must instead select from the set of questions provided by the institution.

Third Party ID Preferences

Use this new section to set preferences for generated third party IDs.

Fields	Descriptions
Length of Last Name for Generate	The number of characters from a user's last name to be used in the generated third party ID.

Third Party Access Audit (GOATPAD)

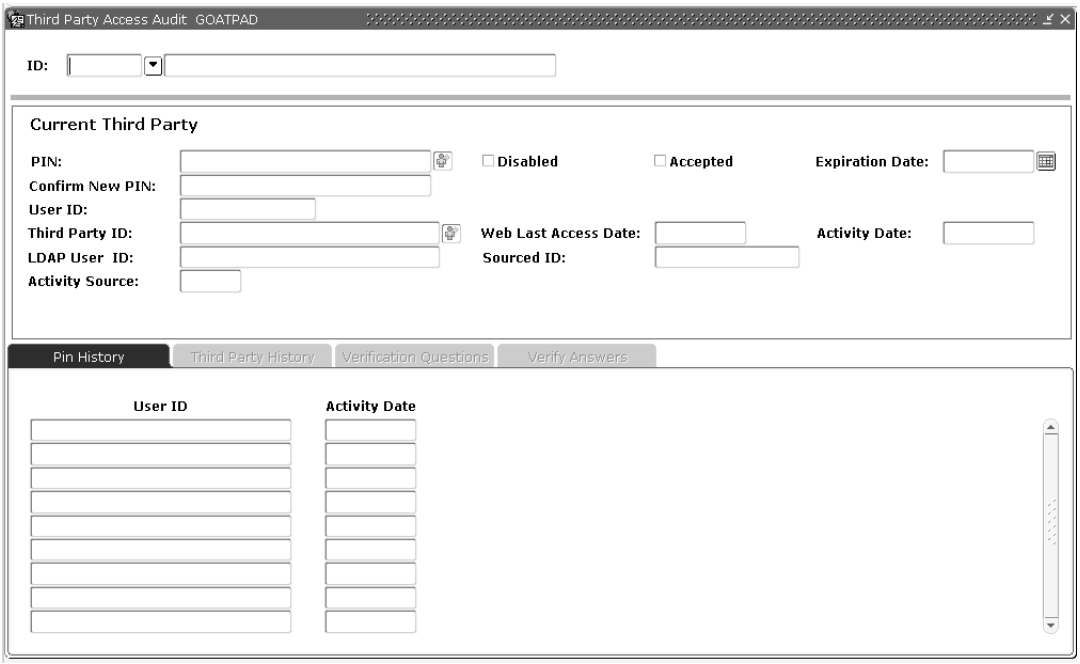
Current Third Party

PIN Hint Question and **PIN Hint Response** have been moved to the **Verification Questions** tab.

A security administrator can use the new **Verify Answers** tab to check a user's security answers when speaking with a person about a PIN reset.

Security questions for resetting PINs are now set up on the GOAQSTN form.

On this window, **PIN** no longer displays clear text. The PIN value is concealed with dots. The new **Confirm PIN** field (also concealed with dots) requires you to enter a PIN a second time to eliminate the possibility of typing errors when entering the PIN value.



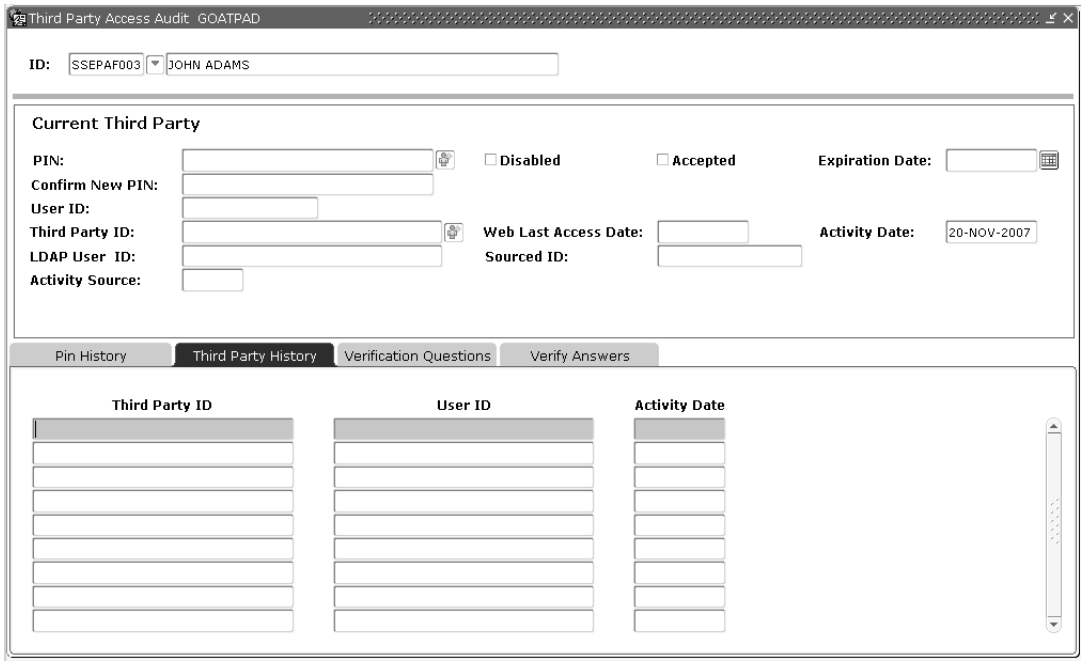
PIN History

This tab shows the history of changes to the user's PIN. The PIN itself is no longer shown on this form; only the User ID and Activity Date of the PIN change event are shown.

The form has been redesigned so that the history of PIN changes is separate from the history of Third Party ID changes.

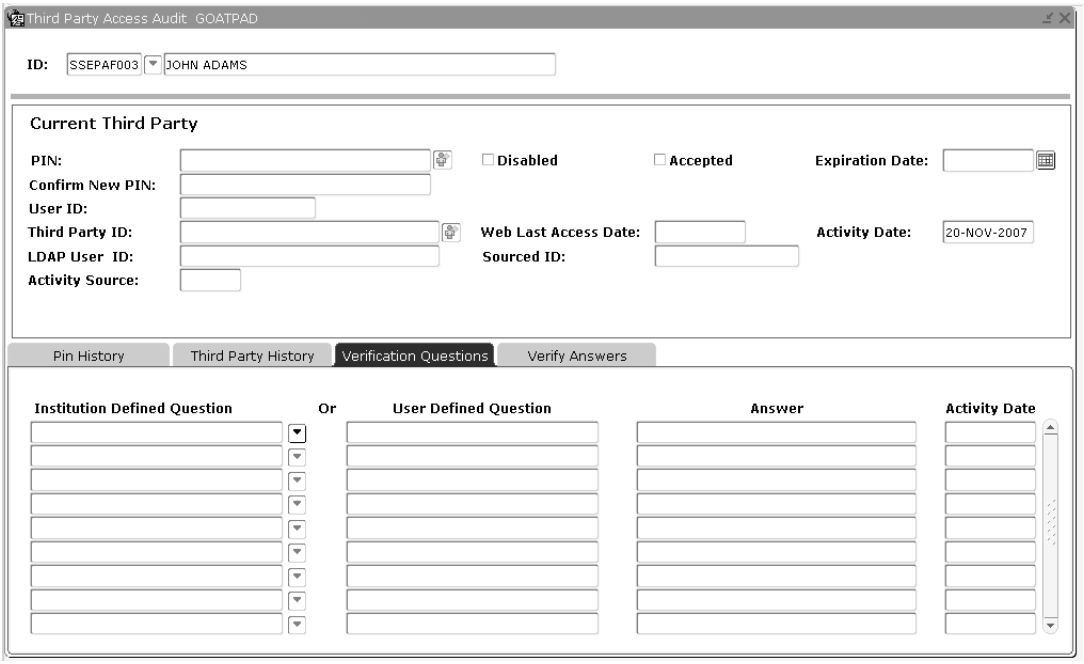
Third Party History

This tab shows the history of changes to the user's Third Party ID.



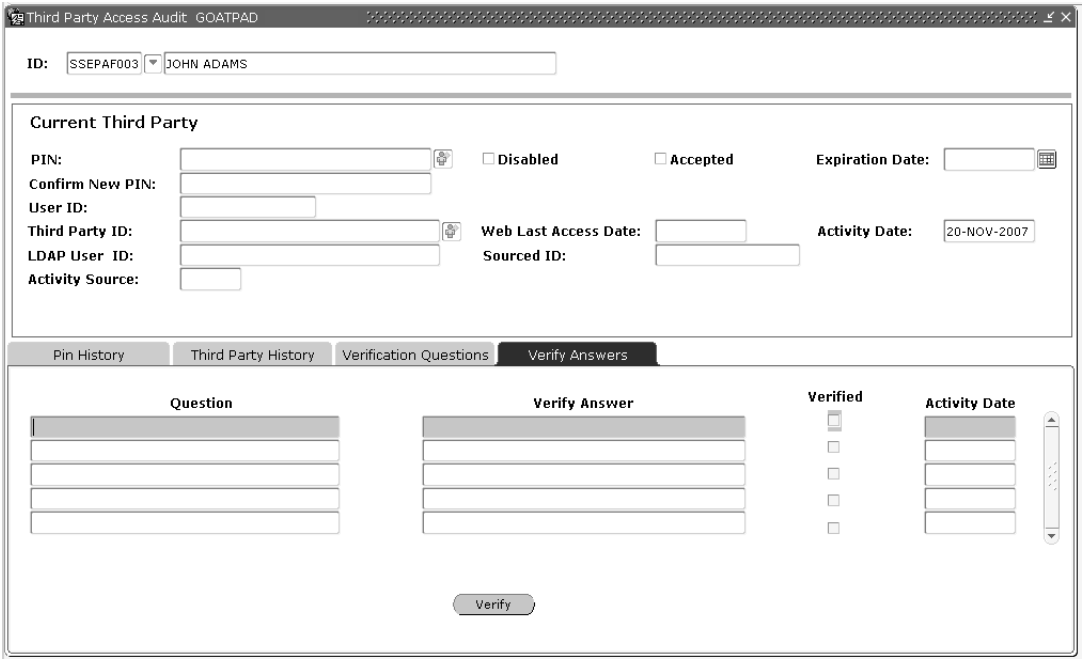
Verification Questions

This tab shows the history of the user's security questions and answers. Answers are encrypted and show as a string of asterisks *(******)* in the **Answer** field.



Fields	Descriptions
Institution Defined Question	A security question defined by the institution.
User Defined Question	A security question created by the users. This field is blank when an institution defined question was selected.
Answer	Because the user's answer is encrypted, this field shows a string of asterisks (******).
Activity Date	The date the user's question and answer was saved.

Verify Answers



This new tab can be used to verify answers to the user's security questions. For example, if a user calls with a request for a password reset, you can use this tab to ask the person's security questions and check their answers against the user's previously stored (encrypted) answers.

To use this tab, enter the user's verbal responses to security questions and then click the **Verify** button. If the answers match, the **Verified** check boxes become checked, and you then know that it is safe to reset the PIN for that user.

Note

When comparing hashed answers for verification, spaces and special characters (including punctuation) are ignored. The compare process also ignores case—capital letters are converted to lowercase before comparing. For example, if the stored, hashed answer is *newyork*, then *New York*, *new-york*, and *NEW YORK* would all match successfully. ■

Fields	Descriptions
Question	The security question.
Verify Answer	Type the user's answer to the question in this field.
Verified	Checked if the user's answer matched the stored answer (after you click the **Verify** button)
Activity Date	The date that verification occurred.

2 Security Administration - Functional

Several improvements have been made in Release 8.0 for security administration.The changes are focused on new user setup, user account maintenance, distributed security, and security auditing.

A detailed description of the new features can be found in the *Banner Security Administration Handbook* (formerly titled *Banner Security Technical Reference Manual*). The *Banner Security Administration Handbook* (general80000security.pdf) is available through the Software Download area in the Customer Support Center. For security reasons, it is not posted in the Documentation Download area or published in the Banner Bookshelf.

See “Security Administration - Technical” on page 71 for more information about this feature.

New Security Administration Features

Managing User Accounts

The following changes provide more flexibility in creating and maintaining user IDs:

- When creating a new user account, you can optionally associate the new user to an existing ID record from the SPRIDEN table. Also, a name can optionally be created for Banner users who do not exist in SPRIDEN.
- Business profiles can now be assigned to users in GSASECR. Business profiles are used in the setup of Fine-Grained Access Control (FGAC) rules. Previously, after you created a user in GSASECR, you had to go to an FGAC setup form to assign the user to a business profile.
- Security groups offer a new layer of structure to give you more flexibility in setting up security for users with similar permissions. Security classes, objects, and users can be assigned to a security group.
- When an Oracle user ID is created on GSASECR, you can now create it in locked status. You can also create an Oracle user ID with a pre-expired password.
- You can create logon calendars that limit users’ access to designated time periods with a specified start and end date. You can also use logon calendars to limit the times of day or days of the week that a user can log on.

Distributed Security

A new Distributed Security form (GSADSEC) allows you to assign limited security administration privileges to users. Thus you can delegate responsibility for specific areas of security maintenance to users that are specifically empowered for those responsibilities.

Banner's Distributed Security architecture gives you a great deal of flexibility to set up your security procedures and areas of responsibility. You can assign owners to security roles, security classes, and Banner objects.

Security Auditing

This release adds more support for auditing Banner security activity.

- User and date/time records can now be logged for changes to Banner tables containing security related data.
- The new GURLOGN table saves a log with information on every Banner logon.
- New tables have been created to optionally store detailed history of Banner security activity.
- A new Banner Security Table Audit form (GSAAUDT) provides easy, secure access to the security audit records.
- New fields have been added to show more details of changes to security classes in GSASECR.
- On the History tab of GSASECR, the user ID is now displayed with each command. In addition, the Command field has been made searchable.

To help you manage security auditing:

- On the GSASECR form, you can select the security tables the will be audited at your institution.
- Because the security logs could grow to be quite large, the new GSAAUDT form lets designated security administrators purge old records from the security audit tables.

Other Changes

This release brings a few miscellaneous security changes.

- A new *SECURITY menu provides convenient access to the expanded family of security administration forms.
- The user's last login date and time, now displays on the GUAGMNU form upon login to Banner. Additionally, if user's Banner ID has been tied to a SPRIDEN ID, the user's SPRIDEN name will appear in the welcome message. If the ID has not

been tied to a SPRIDEN ID, but a name has been created for the user on GSASECR, the user's name will display in the welcome message.

Security Setup Procedures

Set Up Security Access for the Security Forms

You should use the new security class BAN_FULL_SECURITY_C to provide security users (*BANSECR%* users) access to the security forms (GSASECR, GSAVPDI, GSADSEC, GSAUDIT) and other forms to provide at least the minimum needed for login and GSASECR usage.

1. Review existing security classes for the presence of GSASECR or GSAVPDI. It is recommended that classes that have users other than BANSECR% users enrolled do not include either of these security forms.

2. Enroll BANSECR in BAN_FULL_SECURITY_C.

3. Copy BAN_FULL_SECURITY_C to one or more new classes which can be modified to establish permissions for distributed security users.

   Depending on your usage of distributed security, you might want to limit distributed users to GSASECR access only, or you might also want to provide access to GSADSEC with tab security applied.

4. For the group of distributed security users who will have a access to GSADSEC set up tab-level security to restrict access to the various tabs in the form (for example, you may want to make the Calendar tab query-only for distributed users).

Enable Audit Triggers

The new security audit feature lets you turn auditing on and off for individual security tables. To set up security auditing:

1. Decide which security tables will be audited at your institution.

   See the “Security Administration - Technical” on page 71 for a complete list of security audit tables.

2. On the GSASECR form, open the Institution Preference tab.

3. For each table that will be audited, choose *Enable* from the pull-down list.

Note

A switch can be set during the Banner General 8.0 installation process to have all security audit triggers initially enabled or disabled. See the *Banner General 8.0 Upgrade Guide* for details. ■

Note

Regardless of your other audit settings or your installation options, logging of Banner INB logins is always enabled. ■

Set Up BAN_DEFAULT_NO_ACCESS Role

The `BAN_DEFAULT_NO_ACCESS` security role provides the ability to directly limit a user's access to an object. If a user is given a direct object grant with a role of `BAN_DEFAULT_NO_ACCESS` this overrides any other privileges that have been established for this user/object.

This role can be thought of as an *exception* to a user's object permissions established through the user's memberships in security classes and security groups.

The advantage to using this role is that a user can now be enrolled in a class where the user has access to most of the objects and the user can be given a direct object grant for an object to exclude that object for the user. Previously, the way to accomplish this same result would have been to create a new class that contained the subset of objects the user is permitted to access.

You must manually set up this role before you can use it. To create `BAN_DEFAULT_NO_ACCESS` with the properties described above:

1. On the GSASECR form click the role tab
2. Enter the role name *BAN_DEFAULT_NO_ACCESS*
3. Click the **Create New Role** button

Warning

Do not copy another role to create this role, and do not add any role privileges to this role. ■

New Forms

Banner Security Table Audits (GSAAUDT)

This new form allows you to view the various security audit records contained in the new security audit tables. See the *Banner Security Administration Handbook* for details.

Banner Distributed Security (GSADSEC)

This new form allows the most-trusted security administrators to set up specific permissions for other security administrators. Group Security can be established on this form, and Logon Calendars can be managed on this form. See the *Banner Security Administration Handbook* for details.

Changed Forms

Oracle/Banner Security Maintenance (GSASECR)

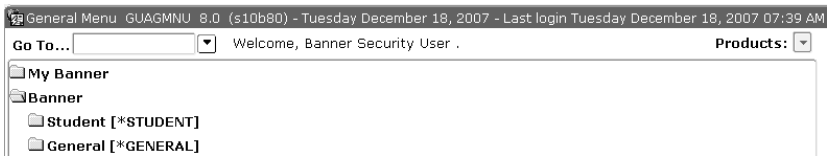
This form has many changes intended to make setting up new users accounts quicker and easier, and to provide more flexibility in managing user accounts. See the *Banner Security Administration Handbook* for details.

Banner Global Initialization (GUAINIT)

This form, which initializes Banner sessions, has a new trigger that capture Banner logons and saves them for later auditing.

General Menu (GUAGMNU)

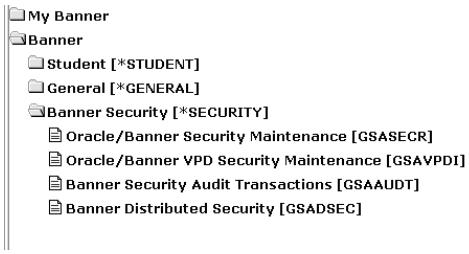
The user's last login date and time now displays on the GUAGMNU form upon login to Banner.



New Menus

*SECURITY

The new *SECURITY menu provides convenient access to the security administration forms.



Previously, the Banner security forms GSASECR and GSAVPDI were not accessible through menus; they could only be run as standalone forms in separate sessions.

Note

This new menu will be visible to any user who is a member of a security class with permissions for any of the Banner security forms or if they are enrolled in the BAN_SHOWALLMENU_C class. (Those users still cannot access the forms—only BANSECR and other explicitly assigned user IDs can access the security forms). It is recommended that you review security classes and remove any permissions to security forms where necessary to prevent regular users from seeing the *SECURITY menu. ■

New Security Class

BAN_FULL_SECURITY_C

This new security class is delivered with permissions for the Banner security objects and other forms needed for security administration. BAN_FULL_SECURITY_C includes permissions for the following objects:

- GSAAUDT
- GSADSEC
- GSASECR
- GSAVPDI
- GUAABOT
- GUACALN
- GUAERRM
- GUAGMNU
- GUAHELP
- GUAINIT
- GUAPMNU
- GUAPSWD
- GUAUPRF
- GUIALTI
- GUIOBJS
- SOACOMP
- SOAIDEN
- SOQMENU

It is recommended that you assign this class to the BANSECR user ID.

You can copy `BAN_FULL_SECURITY_C` to create a separate class with some limitations for distributed users. These users, for example, should have a `_Q` role establishing query-only access to the new GSAAUDT form, so they will be unable to delete security audit records.

Note

With the introduction of this new security class, you should use it as the basis of permissions for BANSECR and other security administrators. It is recommended that you remove GSASECR and GSAVPDI permissions from classes like `BAN_GENERAL_C` and `BAN_ADMIN_C`, and any other class which contains non-security users.

3 Partial Character Masking - Functional

Overview

Banner 7.0 introduced the ability to hide, conceal, or mask the full contents of a field containing sensitive information. In addition, number and date fields could be partially masked. For example, you could choose to display the month and date of a birthdate while masking the year.

With Banner 8.0, the ability to partially mask a field has been extended to character fields as well. For example, you could choose to mask most of a Social Security Number field, while leaving just a few characters readable to allow a user to verify that the number in the field is the correct one.

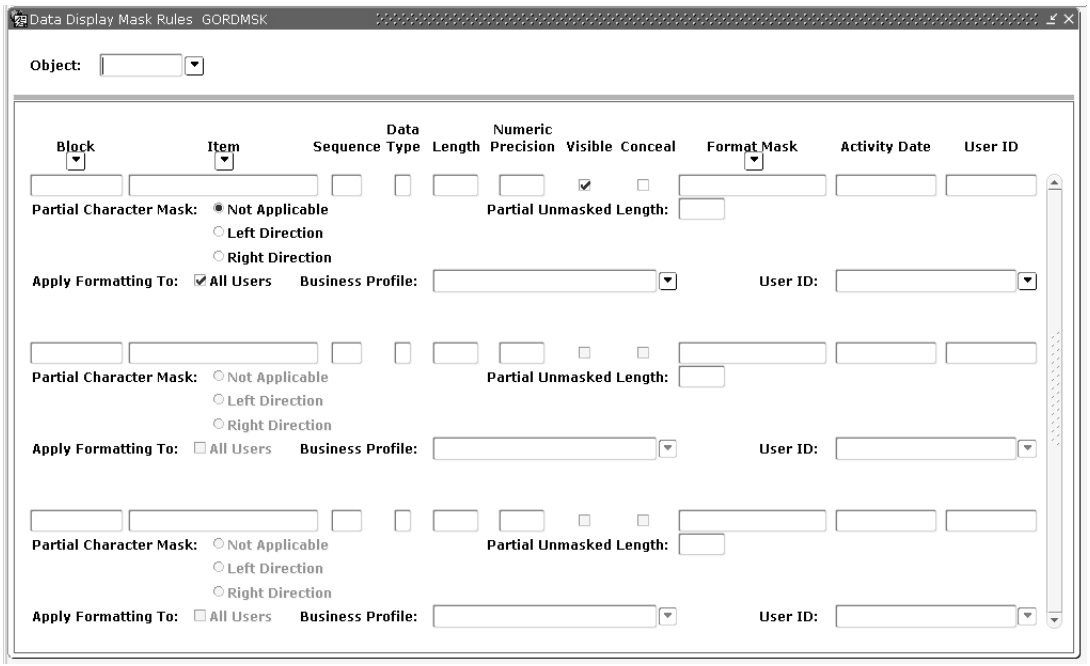
With this new partial character masking solution, you can allow a specified number of characters at the right side or the left side of the field to remain readable, while the rest of the value is masked.

This new partial character masking solution replaces the limited character masking solution provided with Release 7.0. That solution required custom programming and was not usable in some forms and fields. With this new method, partial character masking can be set up as easily as any other masking option.

See “Partial Character Masking - Technical” on page 85 for more information about this feature.

Changed Forms

Data Display Mask Rules (GORDMSK)



Two new fields have been added to support partial character masking.

Fields	Descriptions
Partial Character Mask	*Not Applicable:* Partial character masking will not be applied. *Left Direction:* The leftmost characters will be readable, while the rest of the field will be masked. For example, *123*******. *Right Direction:* The rightmost characters will be readable, while the rest of the field will be masked. For example, *******789*.
Partial Unmasked Length	The number of characters that will still be readable (unmasked) when partial character masking is applied.

In addition, for character items, the **Format Mask** field has been disabled. Instead of entering a format mask, you can use the **Partial Character Mask** and **Partial Unmasked Length** fields to mask a portion of the character data.

4 Supplemental Data Engine - Functional

Overview

Supplemental Data Engine (SDE) is a simple way to add data fields to Banner forms. SDE allows you to store data that is not part of the existing Banner data model.

No customization of Banner forms or tables is needed to capture and use additional data with SDE. The new data is displayed in a popup window, the Supplemental Data Window, and is stored in a supplemental data table. Because no customization is needed, supplemental data is generally not impacted by Banner upgrades.

See “Supplemental Data Engine - Technical” on page 87 for more information about this feature.

The Structure of SDE

Each supplemental data record created through SDE is tied to a specific Banner table. The Banner table’s unique key enables a specific record on the source table to be linked to a specific record on the Supplemental Data table. Through SDE you can create additional fields associated with a specific Banner table but stored in a separate table, the Supplemental Data Table.

Although it is natural to think of supplemental data in terms of extra fields on Banner forms, SDE is tied to forms only indirectly.

If the same table is used by two or more forms, supplemental data associated with the table will automatically be viewable on all of those forms.

When you are setting up SDE for a form with multiple data blocks, each associated with a different table, each data block’s SDE must be set up separately by setting up the table that supplies the data for each block.

Limitations of SDE

Not all Tables, Blocks, and Forms Work with SDE

Supplemental data is not guaranteed to work in every instance. There may be some forms and blocks where SDE cannot be used.

Supplemental data can only be associated with tables; therefore, any form that relies on a view to display data cannot use SDE. For example, the AOAIDEN form displays data from a view and, as a result, SDE cannot be displayed on that form.

The security tables owned by BANSECR cannot be used with supplemental data. Because SDE's architecture is incompatible with the security requirements of the BANSECR-owned security forms, these forms will not be SDE-enabled in future releases.

Because of technical limitations, there are certain Banner forms where SDE does not work at all or does not function correctly. At the time of Release 8.0, SDE cannot be used in the forms listed below.

Banner General Forms

GOAFBPI	GOIFBPR	GSAVPDI
GOAFBPR	GORFEOB	GTVADID
GOAFPUD	GORVPDI	GTVLFST
GOAINTL	GSADSEC	GTVPARS
GOAQSTN	GSASECR	GTVSVCA

Banner Student Forms

SAAETBL	SHARQTS	SSASCHW
SAARRFT	SHARTYP	STVCACT
SAAWADF	SHATATC	STVCSTS
SAAWATR	SOACTRL	STVELMT
SAQOLIB	SOAMAUD	STVGCMT
SCACRSE	SOIHCUR	STVLMOD
SCARRES	SORCACT	STVMECL
SFAEPRT	SORCSTS	STVWPYO
SHAGCOM	SORLCDF	STVWSCF
SHAGRUL	SRAPREL	STVWSSO
SHARPAR	SSARRES	

Note

If you encounter other table/form/canvas combinations where there are issues with SDE, you are encouraged to raise an RPE through the Customer Support Center.

Multi-Entity Processing

The combination of SDE with Virtual Private Database (VPD) is currently not supported. If you use VPD to implement Multi-Entity Processing (MEP), you should be aware the SDE does not work automatically with VPD. If you want to apply VPD rules to the SDE table, this must be planned for and set up as part of your VPD implementation.

Masking

Masking is not currently supported with SDE. Supplemental data fields cannot be masked, concealed, or hidden.

Using the Supplemental Data Engine

Planning for Supplemental Data Setup

Some things to think about before you start your SDE setup:

- The form(s) where you want the data to be viewed/edited
- The name(s) of the underlying table(s)
- Whether you want the SDE fields to add to or replace baseline fields in views that use the data
- Do you want to add a single SDE field or multiple fields? If multiple, how do you want to differentiate them?
- What labels should end users see on the SDE window? What hint text will help your users enter data correctly?
- Where else in the system do you want the SDE data to be visible? What views might you need to create to use the data? Do you want the SDE data to be available in Self-Service?

Administrative Setup for SDE

Enabling the <Ctrl-D> Keystroke

The <Ctrl-D> keystroke is a convenient way for users to show and hide the Supplemental Data window. To enable this keystroke for users at your institution, add the following line to your fmrweb.res file in your $ORACLE_HOME/forms/java directory on your Oracle Application Server.

```
68   : 2 : "Ctrl+D"          : 11022 : "Accelerator1"
```

Setting Up a Supplemental Data Attribute

Overview of the process.

1. Enable the underlying table for SDE processing. Before you can create supplemental data for a Banner table, the table must be added in the GTVSDTB form. See “Tables with Existing Supplemental Data Attributes (GTVSDTB)” on page 42 for details.

2. Create discriminators, if necessary. If you want to add multiple, related supplemental data fields under a single SDE attribute, you must use a discriminator to differentiate the fields. You can use an existing discriminator, if a suitable one has been previously created. If not, you can set up a new discriminator in the Supplemental Data Discriminators form (GOADISC).

   There are different kinds of discriminators that give you different options. See “Supplemental Data Discriminators (GOADISC)” on page 51 for details.

   If you are creating a single SDE field, no discriminator is necessary, and you can skip this step.

3. Set up the attribute on the Supplemental Data Attribute Definition form (GOASDMD). You must specify the field’s data type and how it will appear to users. See “Supplemental Data Attribute Definition (GOASDMD)” on page 44 for details.

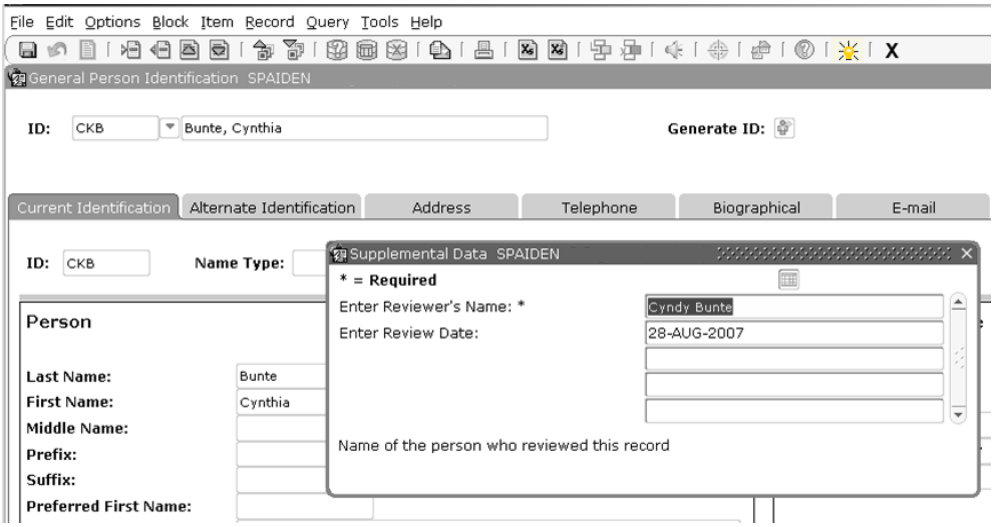
4. Generate DDL and create a view if necessary. If you plan to use this SDE attribute in Banner Self-Service or in some other context that requires a view, you can generate DDL code for the view in GOASDMD. See “Generate DDL” on page 48 for details.

5. Modify Self-Service if necessary. To make full use of supplemental data in Self-Service, custom modifications must be made in Banner Self-Service packages. This step should be undertaken by a programmer experienced with SQL. See “Using Supplemental Data in Self-Service” on page 95 for an example.

New Forms

Supplemental Data Window

Supplemental data columns, after they have been set up for your institution, are displayed in the Supplemental Data window. If you have the appropriate permissions, you can add or edit data on this window. Your permissions in the Supplemental Data window match your permissions in the form displayed in the main Banner window.



The Lightbulb Icon

A new lightbulb icon on the Banner toolbar lets you know when there is supplemental data to be seen.

	A grayed-out lightbulb icon indicates that there is no Supplemental Data window for the database table in the current block.
	A colored lightbulb icon indicates that there is a Supplemental Data window for the current block, but it does not contain any data. You can click the lightbulb icon to open the Supplemental Data window and enter data.
	An active lightbulb-with-rays icon indicates that supplemental data exists for the current record. You can click the lightbulb icon to open the Supplemental Data window and view or edit the data.

Entering Supplemental Data

The Supplemental Data window is accessed by clicking the lightbulb icon in the Banner toolbar. The window will display one or more fields where you can enter data related to the data in the current main Banner window.

Tip

You can also show and hide the Supplemental Data window from the menu bar with **Block > View Supplemental Data**, or by pressing <Ctrl-D> (if the <Ctrl-D> keystroke has been enabled for your institution). ■

Any fields you see in the Supplemental Data window have been specifically set up for your institution. Look for hint text that provides guidance on what to enter in the supplemental data fields.

If you see an existing set of numbered fields (for example, labeled **Comment 1** and **Comment 2**), you can open the next available field in the series by clicking one of the fields and then selecting **Record>Duplicate** from the menu bar.

If a supplemental data field is marked with an asterisk (*), that means it is a required field. You must enter a value for it before you close the Supplemental Data window.

When you are done viewing or editing supplemental data, you can close the Supplemental Data window. To close the window, do any of the following:

- Click the **Close SDE Window** button in the window
- Click the SDE icon in the Banner toolbar
- Press <Ctrl-D> (if the <Ctrl-D> keystroke has been enabled for your institution)

You can also leave the Supplemental Data Window open while you return to the main Banner window. If you navigate to a different record or to a different block in the main Banner window, the Supplemental Data window automatically updates to show the supplemental data for the new record or block.

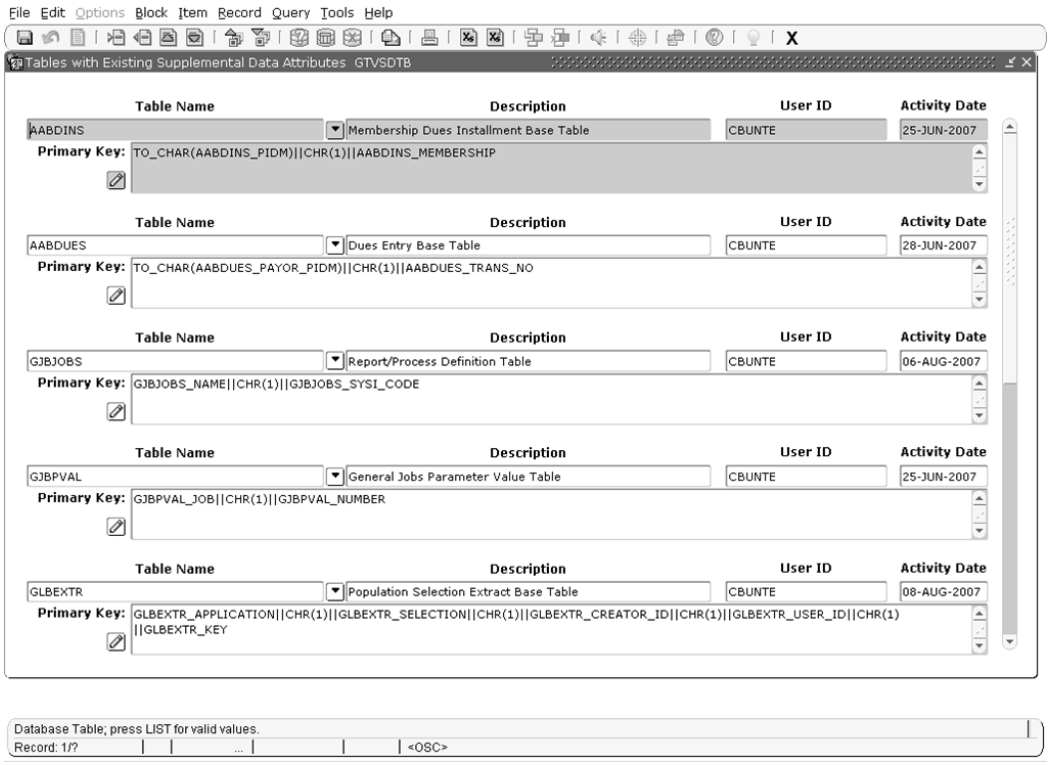
You can move the Supplemental Data window as needed, by dragging the window by its title bar.

Supplemental data is saved automatically when you save the record in the main Banner window, or you can save while in the Supplemental Data Window.

Tables with Existing Supplemental Data Attributes (GTVSDTB)

This new validation form is used to list Banner tables that are enabled for SDE. Before you can begin to set up SDE data for a table, the table must first be listed on this form.

The data entered on this form is saved in the GOBSDTB table.



Field	Description
Table Name	Name of the Banner table enabled for SDE.
Description	Description of the table
User ID	The ID of the user who last changed the record.
Activity Date	The date the record was created or last changed.
Primary Key	The Dynamic SQL statement that identifies the primary key of the table. This field should be automatically populated from the primary key in the database table. If the field is not automatically populated, you should seek technical support to determine the unique key for the table. **Warning** In order to successfully create supplemental data, this key must be a unique key. ■

Supplemental Data Attribute Definition (GOASDMD)

This form can be used to define the attributes for supplemental data fields that will be displayed on the Supplemental Data window.

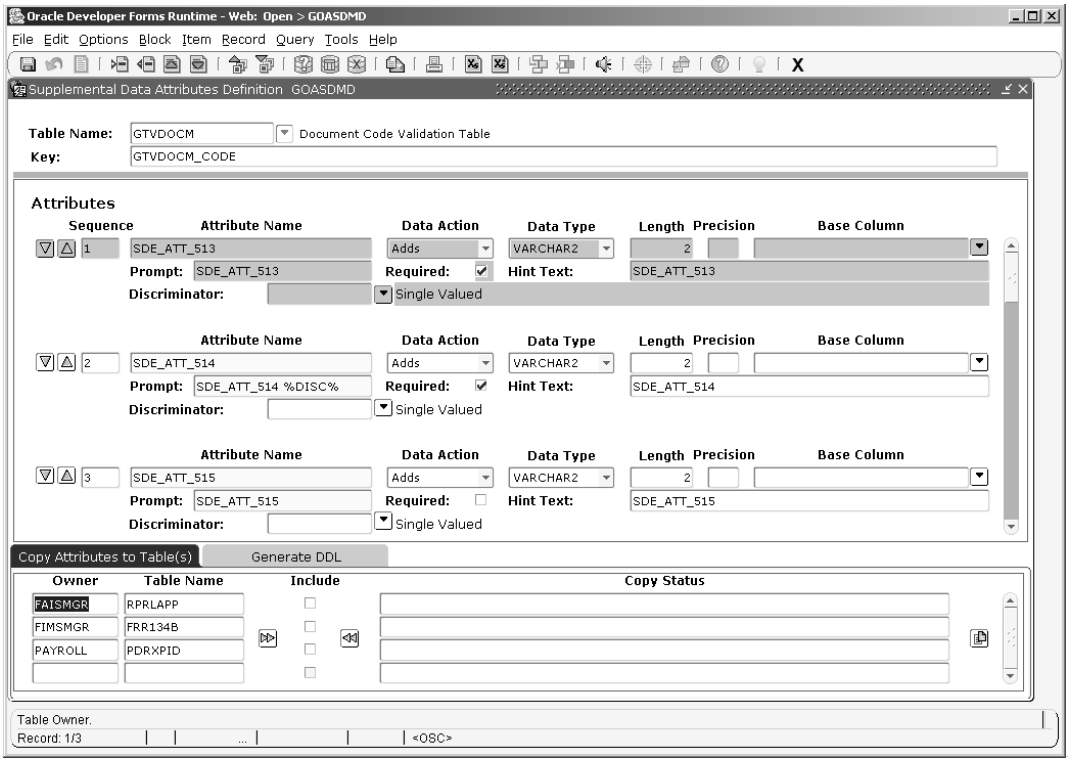
Note

An attribute cannot be changed if the change will affect existing supplemental data.

You can also use this form to create views incorporating supplemental data. These views can be used to modify Self-Service applications and for reporting purposes.

If you plan to use a discriminator to allow more than one supplemental data field for an attribute, you should create the discriminator first before creating the attribute. Use the Supplemental Data Discriminators form (GOADISC) to set up discriminators.

Because the successful use of the GOASDMD form requires an understanding of the Banner database, and because this form can be used to create views that are saved to the database, it is recommended that access to this form be restricted to users who have database administrator (DBA) privileges.



Key Block

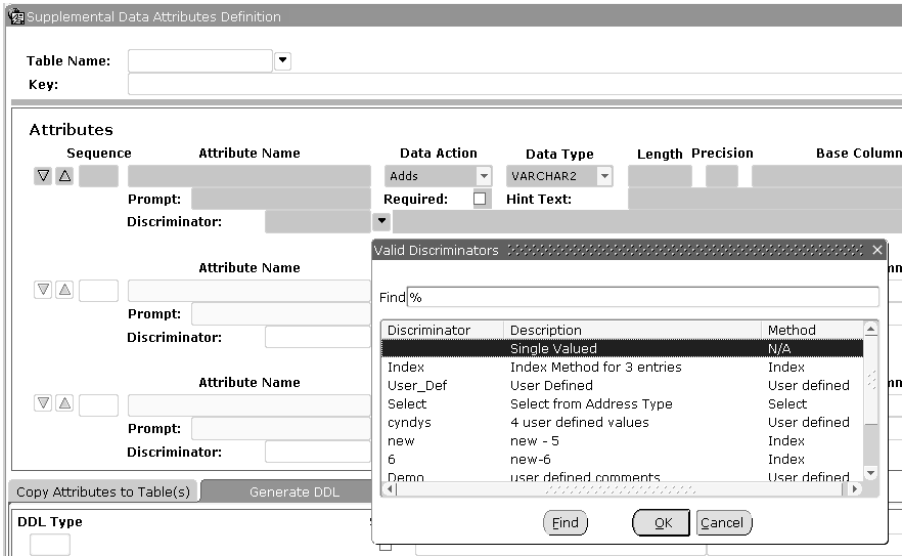
Fields	Descriptions
Table Name	Name of the table to which you want to add supplemental data. Only tables which have been SDE-enabled will display. If you want to use a table that is not listed, you can add it in the Tables with Existing Supplemental Data Attributes form (GTVSDTB).
Key	Database primary key. This field is automatically populated from GTVSDTB

Attributes

Fields	Descriptions
(Sort arrows)	Moves the selected row up or down. The value in the **Sequence** field will change according to the new position of the row.
Sequence	Order that the supplemental data fields will appear when the Supplemental Data window is opened from a form. This field is display only. Use the sort arrow buttons to change the order of supplemental data fields.
Attribute Name	Name of the attribute. The value entered is an identifier, and cannot be changed once the record is saved.
Data Action	Indicates how the data will be used in a view: *Adds* or *Substitutes*. (This value is relevant only if you will be creating a view in the **Generate DDL** block.) *Adds:* The supplemental data will be an displayed in an additional column in the view generated. *Substitutes:* The supplemental data will display in the view in place of the data from the Base Column field. **Note:** If you choose *Substitutes* you must choose the same **Data Type** as the column you are substituting. If you select *Substitutes*, then you must enter a value in the **Base Column** field to indicate the baseline column being replaced. **Note:** The substitution only relates to the view that is created. Existing forms and processes will not use the substituted columns unless the correct database synonyms are generated. It is advised that these objects be created only with expert knowledge of the forms and processes that are affected.

Fields	Descriptions
Data Type	Data type for the attribute: *VARCHAR2*, *NUMBER*, or *DATE*. **Note:** When you enter a **Base Column**, this field is populated from the data type of the specified base column.
Length	Length of data (in digits or characters) users will be permitted in the supplemental data field(s). The maximum length you can enter here is *2000*. If no value is entered, the default is *2000* for VARCHAR2 and *22* for NUMBER. **Note:** When you enter a **Base Column**, this field is populated from the length of the specified base column.
Precision	Number of digits to the right of the decimal point. For example, a scale of *2* indicates one-hundredths of a unit, as in .99. This field is used only when the **Data Type** is *NUMBER*.
Base Column	If the **Data Action** is *Substitutes*, you must enter a column name in the **Base Column** field. When the view is generated, the supplemental data will display instead of the data from the base column. When the view is generated, the base column entered here will be replaced by the attribute. The base column name will be replaced by the value in the **Attribute Name** field in the view.
Prompt	Prompt for the attribute. The prompt will appear as the field label on the Supplemental Data window. Use *%DISC%* as a placeholder here to display the discriminator value as all or part of the prompt. The *%DISC%* placeholder will take its value depending on what is chosen in the **Method** field on GOADISC. • If the method is *Index*, then *%DISC%* will be replaced with the next number in the attribute sequence up to the maximum number designated by the entry in the GOADISC **Validation** field. • If the method is *Select*, then *%DISC%* will be replaced with the values from the description column returned from the `SELECT` statement entered in GOADISC's **Validation** field. One attribute will be created for each row returned in that `SELECT` statement. • If the method is *User defined*, then *%DISC%* will be replaced with the values in the **Discriminator Value Description** field from GOADISC.

Fields	Descriptions
Required	Indicates if users are required to enter data for the supplemental data field in the Supplemental Data window. The supplemental data field will be marked with an asterisk (*) to indicate that the field is required.
Hint Text	Hint or additional information about the attribute that will be displayed on the Supplemental Data window. **Note:** When the discriminator method is Index, the default hint text is *Use Record Duplicate to add additional entries,* to remind users that additional indexed fields are available if needed. You can edit or add to this default hint text.
Discriminator	Discriminator code. A discriminator distinguishes multiple fields with distinct values for the same attribute. The discriminator code entered here must match a discriminator code that has been defined on the Supplemental Data Discriminators form (GOADISC). When no code is entered here, only one field will be displayed on the Supplemental Data window for the attribute.



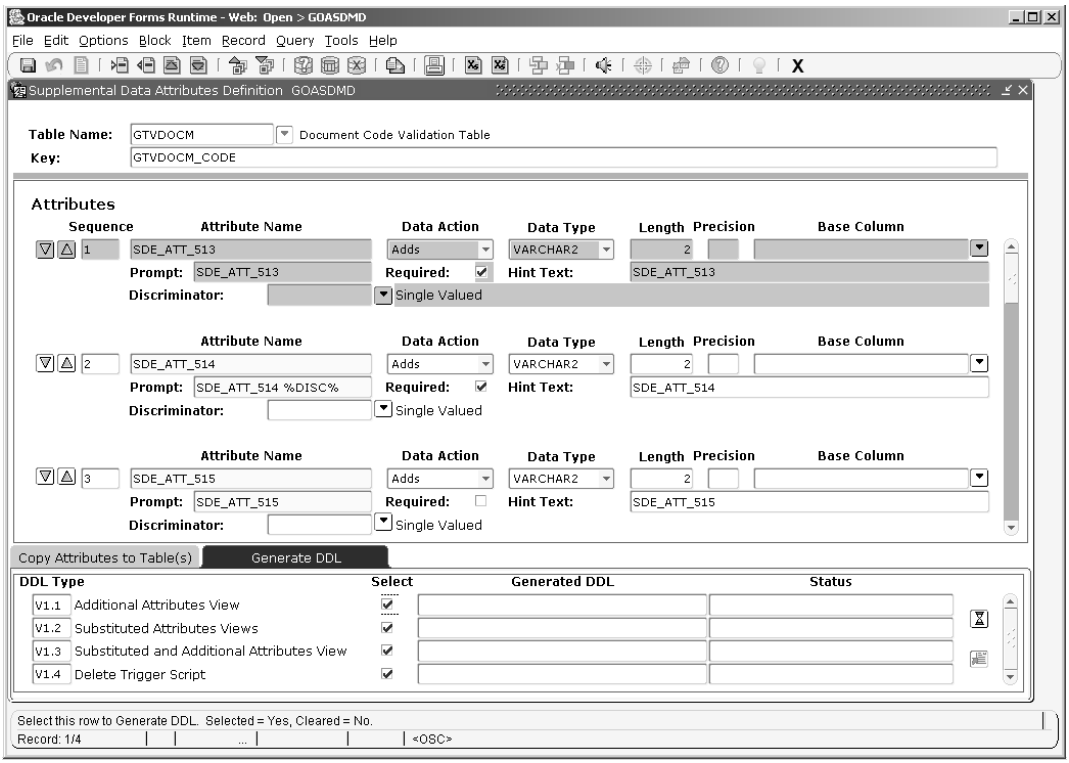
Copy Attributes to Table(s)

Use this tab to copy all of this table's SDE attributes to one or more specified tables.

Fields	Descriptions
Owner	The Oracle ID that normally owns the table. You can perform a query from this field.
Table Name	Name of the table from which the code and description will be taken. You can perform a query from this field.
Include	Indicates if the attributes should be copied to this table. If checked, the table is included as a target for copying.
Copy Status	Indicates the status of the copy.
(Include All) >>	Click this button to select all of the **Include** check boxes.
(Exclude All) <<	Click this button to clear all of the **Include** check boxes.
Copy	Click this button to initiate the copy to the selected table.

Generate DDL

You can use this tab to create and apply a data definition language (DDL) script that creates one or more views in the database. These views will include the supplemental data columns.



Fields	Descriptions
DDL Type	Indicates the type of view to generate. Possible values are • *V1.1 Additional Attributes View:* The generated view will contain only the supplemental data from the attributes that have the **Data Action** of *Adds*. • *V1.2 Substituted Attributes View:* The generated view will contain only the supplemental data from the attributes that have the **Data Action** of *Substitutes*. • *V1.3 Substituted and Additional Attributes View:* The generated view will contain supplemental data from the attributes that have the **Data Action** of either *Adds* or *Substitutes*. • *V1.4 Delete Trigger Script:* This script contains code that can be applied to the database table so that if a base record is removed, the associate supplemental data will also be removed. **Note:** The delete trigger script cannot be applied through the GOASDMD form. It must be manually copied and applied to the database by a DBA.
Select	Check the check box to include the DDL type in the generated view.
Generated DDL	This field displays the DDL code that was generated for the view. **Tip** SunGard recommends that you copy the code from this field, paste it into a text editor, and save it. This is your only way to retain the generated code for source integrity purposes. The generated DDL code is not saved on this form. ■
Status	Indicates the Oracle status message returned by the generation.

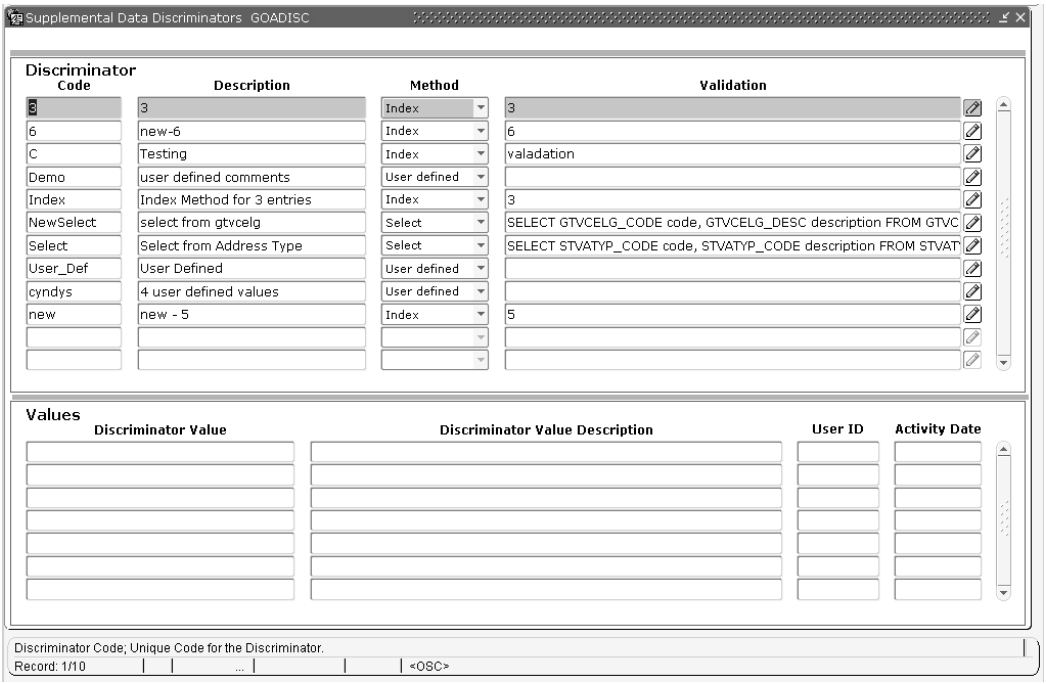
Fields	Descriptions
(Generate)	Clicking this button generates the code that will be used to create a view that includes the supplemental data columns and base table columns. **Tip** The generated code is not saved, except in the form of a view if you click **Apply** to create the view in the database. If you want to retain the generated code for later use, you must manually save it, for example, in a text editor. You can also generate the code again at any time. ■
(Apply)	Clicking this button applies the DDL code to the database and creates a view that includes the supplemental data columns and the base table columns. **Note:** You must first generate DDL code (by clicking **Generate**) before the code can be applied to the database. The name of the created view will be the table name (from the Key block) followed by _ADD for View with Additional Attributes, _SUB for View with Substituted Attributes, or _ADS for View with Additional and Substituted Attributes. **Tip** To be able to create a view, you need view creation privileges. If you do not have these privileges, you can copy the code from the Generated DDL field, paste it into a text editor, save it as an SQL file, and ask your DBA to apply the DDL code to the database. ■ **Warning** The DDL is checked prior to being applied to confirm that the statements are valid and complete. However, it is possible to alter data values in the DDL prior to applying to the database. Use caution if editing the DDL. ■

Supplemental Data Discriminators (GOADISC)

Use this form to identify discriminator codes for SDE, and to define the discriminator methods that will dynamically handle supplemental data.

Note

This form is necessary only for cases where multiple entries will be used for an SDE field. If only a single value will be entered for an SDE attribute, then it is not necessary to set up discriminators for the attribute in this form.



Discriminator

Fields	Descriptions
Code	Discriminator code. This code will be used on the Supplemental Data Attributes Definition Form (GOASDMD).
Description	Description of the discriminator code.
Method	The discriminator method: *Index*, *Select*, or *User defined*. See detailed discussion below.

Fields	Descriptions
Validation	Discriminator validation. The value to be entered in this field depends on the value in the **Method** field. See detailed discussion below.
(text edit button)	Edit discriminator validation SELECT statement in a separate window.

Using the Index Method

If you enter *Index* in the **Method** field, users will be able to enter multiple fields in the Supplemental Data window, up to the maximum number entered in the **Validation** field. If **Validation** is left blank, then no maximum number of fields is enforced, and the user in the Supplemental Data window can enter as many fields as necessary.

If the value in the **Prompt** field on the GOASDMD form contains *%DISC%*, then the value entered here in the **Validation** field will be used to designate the index number.

For example, if you enter *5* in the **Validation** field, the affected field in the Supplemental Data window can be displayed up to five times (by using **Record>Duplicate**), with the labels **1, 2, 3, 4,** and **5.**

Note

Initially, only the first record will display in the SDE Window. To display additional fields the user must perform the **Record>Duplicate** function. ■

Using the Select Method

If you enter *Select* in the **Method** field, you must then enter or build a `SELECT` statement in the **Validation** field. The results of that `SELECT` statement will be a list of codes that will be used as labels for the multiple fields on the Supplemental Data window if *%DISC%* is used in the **Prompt** field on GOASDMD.

The `SELECT` statement in the Validation field must be in the following format:

```
SELECT COLUMN_NAME code, COLUMN_NAME description FROM TABLE
```

where *COLUMN_NAME* is the column and *TABLE* is the table from which the attribute values will be taken.

You can type or paste a `SELECT` statement directly into the **Validation** field, or you can click the edit button (pencil icon) to open the Select Columns for Discriminators wizard. To use the wizard, you must query for a table, then select a value for the **Code** and then a value for the **Description** in order to enable the **OK** button.

Note

The edit button is disabled if there is text in the **Validation** field. If you start to type a select statement and then change your mind and want to

use the Select Columns for Discriminators window instead, you must blank out the **Validation** field before clicking the edit button. ■

Warning

The select statement is run dynamically when the Supplemental Data window is opened. This means that if you change the select statement, or if the data returned by the select statement changes over time, a different list will appear on the Supplemental Data window, and orphaned supplemental data records could result. ■

Using the User Defined Method

If you enter *User defined* in the **Method** field, you can use the Values area at the bottom of the window to manually create a set of codes and values to be used as discriminators.

Values

Use this area to manually create discriminator codes and descriptions when you select *User defined* in the **Method** field.

Fields	Descriptions
Discriminator Value	A value used to identify the discriminator. The code is not visible in the Supplemental Data window.
Discriminator Value Description	A description that will be displayed in the Supplemental Data window as label for the Supplemental Data field if *%DISC%* is used in the **Prompt** field on GOASDMD when creating an attribute.
User ID	ID of the user who created or last changed the record.
Activity Date	Date the record was last changed.

Select Columns for Discriminator

This window is used to choose columns for a `SELECT` statement when *Select* is entered in the **Method** field. You open this window by clicking the edit button.

For the `SELECT` statement to work, you must query for a table first. Then select one **Code** column and one **Description** column. Once you have chosen a Code and Description the **OK** button will become enabled. Click **OK** to close this window. The columns you have selected are returned to the **Validation** field.

Fields	Descriptions
Owner	The Oracle ID that normally owns the table. You can perform a query from this field.
Table Name	Name of the table from which the code and description will be taken. You can perform a query from this field.
Column Name	Columns that are in the selected table. You can perform a query from this field.
Data Type	Data type for the selected column.
Data Length	Length (in characters) for data in the selected column.
Code	Indicates if the data in the selected column should be used as the code in the discriminator `SELECT` statement. The code is not visible in the Supplemental Data window.
Description	Indicates if the data in the selected column should be used as the description in the discriminator `SELECT` statement. The data that is in the column designated *Description* will be displayed in the Supplemental Data window as labels for the Supplemental Data fields.

New Menus

Supplemental Data Engine (*GENSDE)

The new Supplemental Data Engine menu (*GENSDE) contains the new SDE forms:

- Tables with Existing Supplemental Data Attributes (GTVSDTB)
- Supplemental Data Attributes Definition (GOASDMD)
- Supplemental Data Discriminators (GOADISC)

Changed Menus

System Functions/Administration (*GENSYS)

The new Supplemental Data Engine menu (*GENSDE) was added to the System Functions/Administration menu (*GENSYS).

5 Internationalization - Functional

Overview

The Banner system is used by higher education institutions worldwide. As Banner is enhanced and modernized, one major initiative is to make the system more adaptable for use in different countries and with different languages. This ongoing effort is called internationalization (and often abbreviated I18N). Internationalization reduces the amount of custom modifications required to make Banner usable for clients in various countries.

For this release, several major changes were made to support internationalization.

See “Internationalization - Technical” on page 103 for more information about this feature.

Unicode Support

With this release, Banner supports the Unicode international character set through the character standard UTF8. As a part of the installation process for Release 8.0, Banner’s Oracle database is converted to the UTF8 standard.

Previously, Banner data was generally limited to the ASCII character set. Now you can type or paste non-ASCII characters into Banner fields, including characters such as å, é, and ö, characters used in non-Roman alphabets, and technical symbols used in a variety of academic disciplines.

From a technical perspective, the transition from ASCII to UTF8 is a major change, but it has no impact on end users, except for instances where your data can now take advantage of the availability of non-ASCII characters.

Additional IDs

A new table, the Additional Identification Table (GORADID), allows you to store any number of extra IDs for a person. Each Additional ID must be assigned an ID Type. You can set up Additional ID Types using the new Additional Identification Type Validation form (GTVADID) and Additional Identification Type Validation Table (GTVADID).

A new **Additional ID** tab on Banner identification forms displays the Additional ID information. The Additional ID tab will be available on SPAIDEN, APAIDEN, PPAIDEN, and FOAIDEN. As with other tabs on these forms, you can use tab-level security to make the new tab available to some users and not to others.

Note

If you previously set up tab-level security for any of the four %IDEN forms, you must define tab security privileges for the new tab. See "Tab-Level Security" in the *Banner Security Administration Handbook* for details. ■

Enhanced Person Information Fields

For this release, many fields have been expanded on Banner tables and forms. These fields can now accommodate longer data values that may be needed in some countries. To accomplish this change:

- Table columns have been expanded
- Forms have been modified to accept longer values
- In some cases forms have been visually redesigned to display longer fields
- Where it is impractical to display the entire possible length of a field, the field has been made scrollable. Thus, when a long value appears in the field, you will be able to scroll to read the entire value.
- In some cases, tooltip displays have been added. These tooltips, which appear when the cursor hovers over a field, show the full value of a field in places where the full value may not be visible onscreen.
- Banner APIs have been modified where needed to handle the longer values.
- In most cases, processes and reports have *not* been modified for this release to handle the longer values. Long values will be truncated where necessary for processes and reports.

Expanded Name Fields

All fields that show a person's first name (`_FIRST_NAME`) or middle name (`_MI`) have been expanded to allow values of up to 60 characters. Fields that show a person's full legal name (`_LEGAL_NAME`) have been expanded to 500 characters.

Note

Fields for a person's last name were already 60 characters in length prior to this release. ■

A few combined name fields, created by concatenating first and last names, have been expanded to 120 characters.

New Name Fields

A new Surname Prefix field (_SURNAME_PREFIX) has been added to database tables that store name information.

Note

Although this field has been added to database tables, it has not been made visible on Banner forms or accessible through Banner APIs with this release.

Expanded Address Fields

Street address fields (_STREET_LINE1, _STREET_LINE2, and _STREET_LINE3) have been expanded to 75 characters. City fields (_CITY) have been expanded to 50 characters. Postal code fields (_ZIP) have been expanded to 30 characters.

New Address Fields

A fourth line of 75 characters for street address information (_STREET_LINE4), and a house number field of 10 characters (HOUSE_NUMBER), have been added to tables with address information.

Note

Although these fields have been added to database tables, they have not been made visible on Banner forms or accessible through Banner APIs with this release.

Expanded Telephone Fields

Telephone area code fields (_PHONE_AREA) have been expanded to 6 characters, telephone number fields (_PHONE_NUMBER) have been expanded to 12 characters, and telephone extension fields (_PHONE_EXT) have been expanded to 10 characters.

New Telephone Fields

A Country Code field (_CTRY_CODE_PHONE) has been added to tables with telephone information.

Note

Although this field has been added to database tables, it has not been made visible on Banner forms with this release.

Expanded E-mail Fields

E-mail address fields (_EMAIL_ADDRESS) have been expanded to 128 characters.

Expanded ID Fields

SSN fields (_SSN), which store Social Security Number information in the US and other ID information in other countries, have been expanded to 15 characters.

A rule on GUAINST sets the data entry length of the SSN. The rule is being delivered with a value of *9* to maintain the previous behavior of SSN fields. If you want to allow SSN values between 9 and 15 characters, you can update the rule on GUAINST.

Note

As noted above, a new **Additional ID** table can store one or more additional IDs associated with a person. ■

SSN Search and the Expanded ID Fields

The SSN search feature introduced in Release 7.5 does not work with SSN values longer than 9 characters.

The SSN search feature allows users to enter a SSN value in an ID field when searching for a person record. If your institution is using SSN search, you should keep the length of the SSN set to *9* in GUAINST so that this feature will continue working as before.

A future enhancement will update Banner's SSN search capabilities so that it works with longer values in the SSN field.

Expanded Currency Fields

To better support a variety of international currencies, currency amount fields have been expanded to a 17,2 precision. Thus, fields that show amounts of money will accept 15 digits before the decimal point and two digits after the decimal point, allowing amounts as large as *999,999,999,999,999.99* to be entered.

Previously, currency amount fields in Banner varied from 11 to 13 digits.

Note

All currency amount fields in Banner General and Banner Finance have been expanded for this release, but currency amount fields in Banner Accounts Receivable, Banner Financial Aid, Banner Human Resources, and Banner Student have not been changed at this time. ■

New Forms

Additional Identification Type Validation Form (GTVADID)

This new validation form is used to maintain ID types associated with Additional IDs. Additional IDs, new with Release 8.0, are stored on the GORADID table and displayed on the SPAIDEN, APAIDEN, FOAIDEN, and PPAIDEN forms.

Field	Description
Additional ID Type	The code for the type of additional ID (GTVADID_CODE).
Description	The description of the additional ID type (GTVADID_DESC).
Activity Date	The date that the record was created or last updated (GTVADID_ACTIVITY_DATE).

Changed Forms

Common Forms Object Library (GOQCLIB)

This library supports the common windows that display identification and personal information in Banner. A new window added to GOQCLIB displays Additional ID information on the SPAIDEN, APAIDEN, PPAIDEN, and FOAIDEN forms.

Additional ID Window

This window is used to enter extra IDs for a person. Click the Additional ID tab to access this window.

Each additional ID must be assigned an ID type. You can set up additional ID types using the Additional Identification Type Validation form (GTVADID).

Note

If your institution is already using Banner's tab-level security feature, you may need to set up tab-level security records for the Additional Identification tab/window. If you do nothing, any user with security access to SPAIDEN, APAIDEN, PPAIDEN, or FOAIDEN will have access to the Additional Identification tab/window. See “Tab-Level Security” in the *Banner Security Administration Handbook* for details.

Field	Description
ID Type	Type of additional ID. List of Values/Search: Additional Identification Type Validation (GTVADID)
Description	Description of additional ID.
Additional Identification	Enter the Additional ID in this field.
Activity Date	Date on which the record was last updated. Display only.
User	ID of the user who last updated the record. Display only.

Expanded Person Information Fields

Forms that display name, address, telephone, e-mail, or ID information have been modified to handle the greater length of the fields listed below.

Field	New Length
First Name (_FIRST_NAME)	60
Middle Name (_MI)	60
Legal Name (_LEGAL_NAME)	500
Street Address Line 1 (_STREET_LINE1)	75
Street Address Line 2 (_STREET_LINE2)	75
Street Address Line 3 (_STREET_LINE3)	75
City (_CITY)	50
ZIP (_ZIP)	30
Area Code (_PHONE_AREA)	6
Telephone (_PHONE_NUMBER)	12
Extension (_PHONE_EXT)	10
E-mail Address (_EMAIL_ADDRESS)	128
SSN (_SSN)	15

In some cases, the forms have been visually redesigned to allow more display space for these fields. In other cases, where the onscreen display of a field is not large enough to display the longest possible value for the field, the field has been made scrollable so that you still read the full value where necessary. In addition, hover text has been added so that more of the value will be displayed when the cursor rests over the field.

To scroll through a field with a long value, click the field, then press and hold the right arrow key.

The following forms have had changed related to expanded person information fields:

GEAATID	GOAINTL	GTVZIPC
GEAPART	GOAMTCH	GUAINST
GEATASK	GOAPGEO	GUAMESG
GLAEXTR	GOASEVR	GUIALTI
GLIEXTR	GOASEVS	GUITINH
GOAADDR	GOQCLIB	
GOAEMAL	GOQOLIB	

Expanded Currency Fields

In addition to the fields listed above, all fields that contain currency amounts and currency conversion rates have been expanded. These fields' names vary based on the purpose of the money. The changed database columns are listed in Chapter 10, "Internationalization - Technical".

Type of Field	New Length
Currency	17,2

The following forms had changes in this release related to expanded currency fields:

- GOASEVR
- GOASEVS
- GXADIRD

Changed Menus

*GENMISC

Additional Identification Type Validation Form (GTVADID) was added to the *GENMISC menu.

Changed Reports and Processes

Reports and processes have not been updated in response to the expanded database fields delivered in this release. Long values in the newly expanded fields will be truncated when necessary for processing by reports and processes.

C Processes

Many of Banner's C processes were updated so that they could correctly handle data in the UTF8 character set. The following Banner General C processes were updated for UTF8 in Release 8.0.

gjrrpts.pc	gupdelt.pc	gurskel.pc
glrletr.pc	gurdetl.pc	gurtabl.pc
gorpgeo.pc	gurhelp.pc	gurtext.pc
gorseve.pc	gurinso.pc	gurtpac.pc
gorsgeo.pc	gurirol.pc	guanlst.pc
gppaddr.pc	gurjobs.pc	gurnlst.pc
guaorac2.pc	gurpded.pc	gurtpac.pc

6 PIN - Technical

See “PIN - Functional” on page 13 for an overview of this feature.

PIN Encryption

PINs are no longer stored as clear text in the database. Instead they are encrypted using one-way cryptographic hash, and the encrypted form is stored in the database. For added security, the PIN value is salted before encryption.

Answers to security questions are encrypted in the same way.

This new GSPCRPT package handles encryption. GSPCRPT calls the Oracle package `DBMS_CRYPTO` to perform cryptographic hashing, using the `HASH_SH1` algorithm. `HASH_SH1` is a secure hash algorithm (SHA) that produces a 160-bit hash.

Encryption Glossary

Cryptographic Hash Function

A hash function with certain additional security properties to make it suitable for use as a primitive in various information security applications, such as authentication and message integrity.

A hash function takes a long string (sometimes called a *message*) of any length as input and produces a fixed-length string as output, sometimes termed a *message digest* or a *digital fingerprint*.

One-Way Hash Function

Takes a variable-length input string, the data, and converts it to a fixed-length (generally smaller) output string called a hash value. When a one-way hash is used, the original value cannot be recreated.

Hash Value

Serves as a unique identifier (like a fingerprint) of the input data. Though it cannot be decrypted, the hash value can be used to verify whether data has been changed or not.

Salt

Additional text appended to a password before hashing to make the password more random. Adding salt makes decryption even more difficult.

Salted Hash

The hashed value generated from the original value appended with a salt. For example, if the password was *ABC* and the salt was *123*, the combined string *ABC123* would be the input for the hash algorithm.

HASH_SH1

A Secure Hash Algorithm (SHA) which produces a 160-bit hash.

DBMS_CRYPTO

An Oracle package new with 10g.

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_PIN`).

Note

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 for GORPAUD, 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

Regardless of these settings, PINs are always encrypted on `GOBTPAC_PIN`. ■

New Tables

The following tables were introduced to support the new PIN functionality.

- GOBQSTN: stores a list of PIN questions.
- GOBANSR: stores users' PIN questions and answers.

Changed Tables

The following tables were updated to support new PIN functionality.

- GOBTPAC: Third party access table for storing PIN and access related information
- GORPAUD: Third party PIN history table
- GUBPPRF: Stores preferences for PIN

New Packages

GSPCRPT

This new package handles encryption of PINs and encryption of answers to security questions.

The GSPCRPT package calls the Oracle package `DBMS_CRYPTO` to perform cryptographic hashing, using the `HASH_SH1` algorithm. `HASH_SH1` is a secure hash algorithm (SHA) that produces a 160-bit hash.

- The `f_get_salt` function returns a random string of a specified length. This value, called *salt*, is appended to the string being encrypted before encryption takes place.
- The `p_salted_hash` procedure takes a password string and salt and uses the `dbms_crypto.hash` function to create a hash.
- The internal `p_banner_hash` procedure accepts a string and uses the `dbms_crypto.encrypt` function to generate an encrypted version of the string.

Changed Packages

Several packages were updated to handle the increased length of the PIN field and the encrypted form of the PIN.

GOKFUNC

The GOKFUNC package is delivered in the files gokfun1.sql and gokfunc.sql. This package's `f_get_current_pin` function has been updated.

GOKLIBS

The GOKLIBS package is delivered in the files goklib1.sql and goklibs.sql. This packages's `f_pinreused` and `f_pinlength` functions have been updated.

GOKMODS

The GOKMODS package is delivered in the files gokmod1.sql and gokmods.sql. This package's `p_update_gobtpac` procedure has been updated.

GOKSELS

The GOKSELS package is delivered in the files goksel1.sql and goksels.sql. This package's `f_get_current_pin` function has been updated.

GOKSEVN

The GOKSEVN package is delivered in the files goksev1.sql and goksevn.sql. This package's `p_change_pin` procedure has been updated.

GOKTPT1

The goktpt1.sql file. This package's `p_insert_gobtpac` procedure, `f_reset_pin` function, and `f_validate_pin` function have been updated.

New APIs

PIN Question API (gb_pin_question)

This package provides the Common Business interface for the PIN Question API (gb_pin_question).

Table	Objects	API Object Name	API Entity Name	Task Performed
GOBQSTN		gb_pin_question	PIN_QUESTION	Stores and retrieves security questions used in the PIN reset process.

PIN Answer API (gb_pin_answer)

This package provides the Common Business interface for the PIN Question API (gb_pin_answer).

Table	Objects	API Object Name	API Entity Name	Task Performed
GOBANSR		gb_pin_answer	PIN_ANSWER	Stores answers to security questions and compares the answers provided by users during the PIN reset process.

Changed APIs

Third Party Access API (gb_third_party_access)

This API has been updated to handle hashing for GOBTPAC_PIN.

7 Security Administration - Technical

See “Security Administration - Functional” on page 27 for an overview of this feature.

New Tables

The following tables have been added to support this release’s new security features.

Owner	Table Name	Table Comment
BANSECR	GTVCALN	Validation entries for calendars used in security logon validation.
BANSECR	GTVOWNG	Validation entries for the security owner groups used in distributed security.
BANSECR	GTVSGRP	Validation entries for security groups.
BANSECR	GURBGRP	This table defines business profiles belonging to a security group. **Note:** This table is for future use.
BANSECR	GURCALN	This table defines calendars used for logon verification.
BANSECR	GURCGRP	This table defines classes belonging to a security group.
BANSECR	GURLOGN	This table stores additional information related to an Oracle User that has access to Banner.
BANSECR	GUROGRP	This table defines individual objects belonging to a security group.
BANSECR	GUROWNG	This table defines groups of users for distributed security.

Owner	Table Name	Table Comment
BANSECR	GUROWNR	This table defines the objects owned by distributed security users and their access for each object.
BANSECR	GURUGRP	This table defines users belonging to a security group.

New Audit Tables

The following new tables support the security auditing capabilities introduced with this release.

Owner	Table Name	Table Comment
BANSECR	GUBAROL	This table stores audit information for the GUBROLE table.
BANSECR	GURAAOB	This table stores audit information for the GURAOBJ table.
BANSECR	GURAATB	This table stores audit information for the GURATAB table.
BANSECR	GURABGP	This table stores audit information for the GURBGRP table.
BANSECR	GURABPI	This table stores audit information for the GURABPI table.
BANSECR	GURABPR	This table stores audit information for the GORPBPR table.
BANSECR	GURACAL	This table stores audit information for the GURCALN table.
BANSECR	GURACGP	This table stores audit information for the GURCGRP table.
BANSECR	GURACLS	This table stores audit information for the GURACLS table.
BANSECR	GURADMN	This table stores audit information for the GOBFDMN table.

Owner	Table Name	Table Comment
BANSECR	GURADPI	This table stores audit information for the GORFDPI table.
BANSECR	GURADPL	This table stores audit information for the GORFDPL table.
BANSECR	GURAEAC	This table stores audit information for the GOBEACC table.
BANSECR	GURAEOB	This table stores audit information for the GOBFEOB table.
BANSECR	GURAGAC	This table stores audit information for the GOBFGAC table.
BANSECR	GURAGBP	This table stores audit information for the GORFGBP table.
BANSECR	GURAGUS	This table stores audit information for the GORFGUS table.
BANSECR	GURAINV	This table stores audit information for the GJRINVC table.
BANSECR	GURAIPF	This table stores audit information for the GUBIPRF table.
BANSECR	GURALGN	This table stores information related to logins to Oracle by users of Banner as defined in GURUCLS, GURUOBJ or GURUGRP.
BANSECR	GURAMSK	This table stores audit information for the GORDMSK table.
BANSECR	GURAOGP	This table stores audit information for the GUROGRP table.
BANSECR	GURAOWG	This table stores audit information for the GUROWNG table.
BANSECR	GURAOWN	This table stores audit information for the GUROWNR table.
BANSECR	GURAPRD	This table stores audit information for the GORFPRD table.

Owner	Table Name	Table Comment
BANSECR	GURAPUD	This table stores audit information for the GOBFPUD table.
BANSECR	GURAUGP	This table stores audit information for the GURUGRP table.
BANSECR	GURAULG	This table stores audit information for the GURLOGN table.
BANSECR	GURAUOB	This table stores audit information for the GURUOBJ table.
BANSECR	GURAUSI	This table stores audit information for the GURUSRI table.
BANSECR	GURAUTB	This table stores audit information for the GURUTAB table.
BANSECR	GURAVCL	This table stores audit information for the GTVCLAS table.

Changed Tables

GUBROLE

The following columns were added.

Column	Data Type	Description
GUBROLE_USER_ID	VARCHAR2(30) NOT NULL	USER ID: User ID of the user who created or last updated the record.
GUBROLE_OWNER	VARCHAR2(30)	OWNER: The owner of the role for use by distributed security.
GUBROLE_COMMENTS	VARCHAR2(4000)	COMMENTS: Comments related to this role.
GUBROLE_DATA_ORIGIN	VARCHAR2(30)	DATA ORIGIN: Source system that created or updated the row.

GUBIPRF

The following columns were added.

Column	Data Type	Description
GUBIPRF_USER_ID	VARCHAR2(30) NOT NULL	USER ID: User ID of the user who created or last updated the record.
GUBIPRF_DATA_ORIGIN	VARCHAR2(30)	DATA ORIGIN: Source system that created or updated the row.

GTVCLAS

The following columns were added.

Column	Data Type	Description
GTVCLAS_USER_ID	VARCHAR2(30) NOT NULL	USER ID: User ID of the user who created or last updated the record.
GTVCLAS_OWNER	VARCHAR2(30)	OWNER: The owner of the class for use by distributed security.
GTVCLAS_COMMENTS	VARCHAR2(4000)	COMMENTS: Comments related to this role.
GTVCLAS_DATA_ORIGIN	VARCHAR2(30)	DATA ORIGIN: Source system that created or updated the row.

GURAOBJ

The following columns were added.

Column	Data Type	Description
GURAOBJ_USER_ID	VARCHAR2(30) NOT NULL	USER ID: User ID of the user who created or last updated the record.
GURAOBJ_OWNER	VARCHAR2(30)	OWNER: The owner of the object for use by distributed security.
GURAOBJ_COMMENTS	VARCHAR2(4000)	COMMENTS: Comments related to this object.
GURAOBJ_DATA_ORIGIN	VARCHAR2(30)	DATA ORIGIN: Source system that created or updated the row.

GURUOBJ

The following columns were added.

Column	Data Type	Description
GURUOBJ_USER_ID	VARCHAR2(30) NOT NULL	USER ID: User ID of the user who created or last updated the record.
GURUOBJ_COMMENTS	VARCHAR2(4000)	COMMENTS: Comments related to this object.
GURUOBJ_DATA_ORIGIN	VARCHAR2(30)	DATA ORIGIN: Source system that created or updated the row.

GURUSRI

The following columns were added.

Column	Data Type	Description
GURUSRI_USER_ID	VARCHAR2(30) NOT NULL	USER ID: User ID of the user who created or last updated the record.
GURUSRI_DATA_ORIGIN	VARCHAR2(30)	DATA ORIGIN: Source system that created or updated the row.

GURSQLL

The following columns were added.

Column	Data Type	Description
GURSQLL_USER_ID	VARCHAR2(30) NOT NULL	USER ID: User ID of the user who created or last updated the record.
GURSQLL_DATA_ORIGIN	VARCHAR2(30)	DATA ORIGIN: Source system that created or updated the row.

One column’s data type was changed.

Column	Data Type	Description
GURSQLL_CMD	CLOB (previously was VARCHAR2(4000))	COMMAND: The dynamic SQL command that was executed.

GURUCLS

The following columns were added.

Column	Data Type	Description
GURUCLS_USER_ID	VARCHAR2(30) NOT NULL	USER ID: User ID of the user who created or last updated the record.
GURUCLS_COMMENTS	VARCHAR2(4000)	COMMENTS: Comments related to this role.
GURUCLS_DATA_ORIGIN	VARCHAR2(30)	DATA ORIGIN: Source system that created or updated the row.

Changed Packages

The following security packages were changes for this release.

- GSPSECR: New security related procedures and functions were added to this package.
- GSPOSEC: Security groups were added to this package's processing logic.
- GSPAUTH: Security groups were added to this package's processing logic.

New Sequence

gos_audit_seq.sql

The gos_audit_seq.sql file creates the sequence BAN_SECURITY_AUDIT_SEQUENCE, which provides a unique suffix for use in the primary key of the common security audit tables.

New Triggers

The following triggers were delivered with this release to support security auditing.

SQL File	Trigger Name	Security Table
gutcgrp0.sql	gt_gurcgrp_audit_row	GURCGRP
gutalgn0.sql	gt_guralgn_audit_logon	database logon trigger
gutalgn2.sql	gt_guralgn_audit_logoff	database logoff trigger
gutaobj0.sql	gt_guraobj_audit_row	GURAOBJ
gutatab0.sql	gt_guratab_audit_row	GURATAB
gutbgrp0.sql	gt_gurbgrp_audit_row	GURBGRP
gutcaln0.sql	gt_gurcaln_audit_row	GURCALN
gutclas0.sql	gt_gtvclas_audit_row	GTVCLAS
gutdmsk0.sql	gt_guraobj_audit_row	GORDMSK
guteacc0.sql	gt_gobeacc_audit_row	GOBEACC
gutfbpi0.sql	gt_gorfdpi_audit_row	GORFDPI
gutfbpr0.sql	gt_gorfbpr_audit_row	GORFBPR
gutfdmn0.sql	gt_gobfdmn_audit_row	GOBFDMN
gutfdpi0.sql	gt_gorfdpi_audit_row	GORFDPI
gutfdpl0.sql	gt_gorfdpl_audit_row	GORFDPL
gutfeob0.sql	gt_gobfeob_audit_row	GOBFEOB
gutfgac0.sql	gt_gobfgac_audit_row	GOBFGAC
gutfgbp0.sql	gt_gorfgbp_audit_row	GORFGBP
gutfgus0.sql	gt_gorfgus_audit_row	GORFGUS
gutfprd0.sql	gt_gorfprd_audit_row	GORFPRD
gutfpud0.sql	gt_gobfpud_audit_row	GOBFPUD
gutinvc0.sql	gt_gjrinvc_audit_row	GJRINVC

SQL File	Trigger Name	Security Table
gutiprf0.sql	gt_gubiprf_audit_row	GUBIPRF
gutlogn0.sql	gt_gurlogn_audit_row	GURLOGN
gutogrp.sql	gt_gurogrp_audit_row	GUROGRP
gutowng0.sql	gt_gurowng_audit_row	GUROWNG
gutownr0.sql	gt_gurownr_audit_row	GUROWNR
gutrole0.sql	gt_gubrole_audit_row	GUBROLE
gutucls1.sql	gt_gurucls_audit_row	GURUCLS
gutugrp.sql	gt_gurugrp_audit_row	GURUGRP
gutuobj0.sql	gt_guruobj_audit_row	GURUOBJ
gutusri0.sql	gt_gurusri_audit_row	GURUSRI
gututab0.sql	gt_gurutab_audit_row	GURUTAB

New Scripts

Distributed Security Script gssaudt.sql

This new distributed security script gives the user inquiry access to the audit history tables. This script is not run as part of the 8.0 installation process.

In addition to running this script, you must also give the user a direct object grant or access to the GSADSEC form through a class or a security group.

Note

Only the BANSECR user can delete security audit records through the GSAAUDT form. No others users can delete records in GSAAUDT unless that user has been manually granted delete access to the history tables.

Audit Trigger Scripts

New scripts have been provided to help manage the new security audit triggers. These scripts can be used for times when you want to temporarily turn off all security auditing and later restore the full set of audit triggers to their previous state.

Script Name	Purpose
gsavtrig.sql	This script saves the current status of the audit triggers so that they can be restored
grestrigs.sql	This script restores audit triggers to their saved state
gursavt.sql	This script contains support SQL used when gsavtrig.sql is run

Table Scripts

The following new tables scripts are run as part of the 8.0 installation process.

Script Name	Script Purpose
gtvcaln_080000_01.sql	GTVCALN - Security calendar validation table create
gtvcaln_080000_02.sql	GTVCALN - Security calendar validation table create index
gtvcaln_080000_03.sql	GTVCALN - Security calendar validation table comments
gtvclas_080000_01.sql	GTVCLAS - add new columns
gtvclas_080000_02.sql	GTVCLAS - convert data
gtvclas_080000_03.sql	GTVCLAS - set column to null
gtvclas_080000_04.sql	GTVCLAS - set column comments
gtvownr_080000_01.sql	GTVOWNR - Distributed owner validation table create
gtvownr_080000_02.sql	GTVOWNR - Distributed owner validation table create index
gtvownr_080000_03.sql	GTVOWNR - Distributed owner validation table comments
gubrole_080000_01.sql	GUBROLE - add new columns
gubrole_080000_02.sql	GUBROLE - convert data
gubrole_080000_03.sql	GUBROLE - set column to null
gubrole_080000_04.sql	GUBROLE - set column comments
guraatb_080000_01.sql	GURAUTB audit for GURATAB table create
guraatb_080000_02.sql	GURAUTB audit for GURATAB table create index
guraatb_080000_03.sql	GURAUTB audit for GURATAB table comments

Script Name	Script Purpose
guraipf_080000_01.sql	GURAIPF audit for GUBIPRF table create
guraipf_080000_02.sql	GURAIPF audit for GUBIPRF table create index
guraipf_080000_03.sql	GURAIPF audit for GUBIPRF table comments
guralgn_080000_01.sql	GURALGN - Login audit table create
guralgn_080000_02.sql	GURALGN - Login audit table create index
guralgn_080000_03.sql	GURALGN - Login audit table comments
guraobj_080000_01.sql	GURAOBJ - add new columns
guraobj_080000_02.sql	GURAOBJ - convert data
guraobj_080000_03.sql	GURAOBJ - set column to null
guraobj_080000_04.sql	GURAOBJ - set column comments
guraowg_080000_01.sql	GURAOWG audit for GUROWNG table create
guraowg_080000_02.sql	GURAOWG audit for GUROWNG table create index
guraowg_080000_03.sql	GURAOWG audit for GUROWNG table comments
gurautb_080000_01.sql	GURAUTB audit for GURUTAB table create
gurautb_080000_02.sql	GURAUTB audit for GURUTAB table create index
gurautb_080000_03.sql	GURAUTB audit for GURUTAB table comments
guravcl_080000_01.sql	GURAVCL audit for GTVCLAS table create
guravcl_080000_02.sql	GURAVCL audit for GTVCLAS table create index
guravcl_080000_03.sql	GURAVCL audit for GTVCLAS table comments
gurawog_080000_01.sql	GURAUTB audit for GUROWNG table create
gurawog_080000_02.sql	GURAUTB audit for GUROWNG table create index
gurawog_080000_03.sql	GURAUTB audit for GUROWNG table comments
gurcaln_080000_01.sql	GURCALN - Security calendar table create
gurcaln_080000_02.sql	GURCALN - Security calendar table create index
gurcaln_080000_03.sql	GURCALN - Security calendar table comments

Script Name	Script Purpose
gurlogn_080000_01.sql	GURLOGN - Login rules and data table create
gurlogn_080000_02.sql	GURLOGN - Login rules and data table create index
gurlogn_080000_03.sql	GURLOGN - Login rules and data table comments
gurowng_080000_01.sql	GUROWNG - Distributed owner group table create
gurowng_080000_02.sql	GUROWNG - Distributed owner group table create index
gurowng_080000_03.sql	GUROWNG - Distributed owner group table comments
gursqll_080000_01.sql	Convert GURSQLL cmd from LONG to CLOB
gursqll_080000_02.sql	Add USER_ID and DATA_ORIGIN
gursqll_080000_03.sql	Populate data origin
gursqll_080000_04.sql	Set column to not null
gursqll_080000_05.sql	GURSQLL - comments for new columns
gurucls_080000_01.sql	GURUCLS - add new columns
gurucls_080000_02.sql	GURUCLS - convert data
gurucls_080000_03.sql	GURUCLS - set column to null
gurucls_080000_04.sql	GURUCLS - set column comments
guruobj_080000_01.sql	GURUOBJ - add new columns
guruobj_080000_02.sql	GURUOBJ - convert data
guruobj_080000_03.sql	GURUOBJ - set column to null
guruobj_080000_04.sql	GURUOBJ - set column comments
gurusri_080000_01.sql	GURUSRI - add new columns
gurusri_080000_02.sql	GURUSRI - convert data
gurusri_080000_03.sql	GURUSRI - set column to null
gurusri_080000_04.sql	GURUSRI - set column comments

Changed Scripts

The following scripts were changed for this release. These scripts are not run as part of 8.0 installation.

Script Name	Purpose of Change
gssbasg.sql	Added grants for the audit tables
gssclsm.sql	Added grants required to do Class Maintenance
gssobjm.sql	Added grants required to do Object Maintenance
gssprfm.sql	Added `ALTER ANY TRIGGER` privilege for common security and grants to GJRINVC
gsspriv.sql	Added synonyms for the audit tables
gssrolc.sql	Added grants required to do Role Create Maintenance
gssrold.sql	Added grants required to do Role Drop Maintenance
gssrolm.sql	Added grants required to do Role Maintenance
gsssysg.sql	Added grants for `sys.dba_triggers` and `sys.gv_$parameter` for common security and `EXECUTE ANY PROCEDURE` for running SDE
gssusra.sql	Added grants required to do User Alter Maintenance
gssusrc.sql	Added grants required to do User Create Maintenance
gssusrd.sql	Added grants required to do User Drop Maintenance
gssusrm.sql	Added grants required to do User Maintenance
gssviol.sql	Added delete grants for auditing tables

8 Partial Character Masking - Technical

See “Partial Character Masking - Functional” on page 35 for an overview of this feature.

Changed Tables

GORDMSK

Two columns were added to this table to support partial character masking.

- GORDMSK_MASK_DIRECTION: Determines which side of the character string will be visible: left, right, or not applicable
- GORDMSK_MASK_LENGTH: The number of characters left unmasked.

Changed Packages

BannerUI.jar

This Java file performs new processing to implement the partial character masking feature.

Changed APIs

GB_DISPLAYMASK

This API was updated to support the new partial character masking solution.

9 Supplemental Data Engine - Technical

See “Supplemental Data Engine - Functional” on page 37 for an overview of this feature.

New Tables

SDE Code Templates Table (GOBSDCT)

This new table stores views to be generated.

Column	Data Type	Description
GOBSDCT_NAME	VARCHAR2(4) NOT NULL	Template Name: The Name for a template
GOBSDCT_DESC	VARCHAR2(50) NOT NULL	Template Description: The description of the template
GOBSDCT_TEMPLATE	CLOB NOT NULL	Template: The code template.
GOBSDCT_ACTIVITY_DATE	DATE NOT NULL	The date that the information for the row was inserted or updated in the GOBSDCT table
GOBSDCT_USER_ID	VARCHAR2(30) NOT NULL	The unique identification of the user
GOBSDCT_DATA_ORIGIN	VARCHAR2(30)	Source system that created or updated the row

SDE Discriminator Table (GOBSDDC)

This new table stores discriminators.

Column	Data Type	Description
GOBSDDC_CODE	VARCHAR2(10) NOT NULL	The discriminator code
GOBSDDC_DESC	VARCHAR2(64) NOT NULL	Description of the discriminator
GOBSDDC_METHOD	VARCHAR2(1) NOT NULL	Method used to discriminate Supplemental Data. *I* for Index, *S* for Select Statement, *U* for User defined in table GORSDDV.
GOBSDDC_VALIDATION	VARCHAR2(1024)	Discriminator Validation: The Select statement to build a list of values or the maximum Index
GOBSDDC_ACTIVITY_DATE	DATE NOT NULL	Date that information for the row was inserted or last updated
GOBSDDC_USER_ID	VARCHAR2(30) NOT NULL	The unique identification of the user
GOBSDDC_DATA_ORIGIN	VARCHAR2(30)	Source system that created or updated the row

SDE Banner Tables Table (GOBSDTB)

This new table stores the names of SDE-enabled Banner tables.

Column	Data Type	Description
GOBSDTB_TABLE_NAME	NOT NULL VARCHAR2(30)	Primary key
GOBSDTB_OWNER	NOT NULL VARCHAR2(30)	Banner table owner
GOBSDTB_PK_DYNSQL	VARCHAR2(2000)	Primary key Dynamic SQL
GOBSDTB_ACTIVITY_DATE	NOT NULL DATE	Date that information for the row was inserted or last updated

Column	Data Type	Description
GOBSDTB_USER_ID	NOT NULL VARCHAR2(30)	The unique identification of the user
GOBSDTB_DATA_ORIGIN	VARCHAR2(30)	Source system that created or updated the row

SDE Metadata Table (GORSDAM)

This new table stores Metadata (rules for the data being extended).

Column	Data Type	Description
GORSDAM_TABLE_NAME	NOT NULL VARCHAR2(30)	Table name. Primary Key
GORSDAM_ATTR_NAME	NOT NULL VARCHAR2(30)	Attribute name. Primary Key
GORSDAM_ATTR_TYPE	NOT NULL VARCHAR2(1)	S=Substitute, A=Add Attribute
GORSDAM_ATTR_ORDER	NOT NULL NUMBER(3)	Display order of Attributes
GORSDAM_ATTR_REQD_IND	NOT NULL VARCHAR2(1)	Required indicator: *Y* or *N*
GORSDAM_ATTR_DATA_TYPE	NOT NULL VARCHAR2(30)	*VARCHAR2*, *DATE*, or *NUMBER*
GORSDAM_ATTR_PROMPT	NOT NULL VARCHAR2(50)	Prompt to show on form
GORSDAM_ACTIVITY_DATE	NOT NULL DATE	Date that information for the row was inserted or last updated
GORSDAM_USER_ID	NOT NULL VARCHAR2(30)	The unique identification of the user
GORSDAM_ATTR_DATA_LEN	NUMBER(8)	Size of the attribute
GORSDAM_ATTR_DATA_SCALE	NUMBER(2)	Number of decimal places
GORSDAM_ATTR_INFO	VARCHAR2(1024)	Default hint or help text

Column	Data Type	Description
GORSDAM_ATTR_BASE_COL	VARCHAR2(30)	Base column substituted for
GORSDAM_SDDC_CODE	VARCHAR2(10)	Associated discriminator
GORSDAM_DATA_ORIGIN	VARCHAR2(30)	Source system that created or updated the row

SDE Attribute Values Table (GORSDAV)

This new table stores the supplemental data value.

Column	Data Type	Description
GORSDAV_TABLE_NAME	NOT NULL VARCHAR2(30)	Table Name: The name of the table supplemented by the attribute
GORSDAV_ATTR_NAME	NOT NULL VARCHAR2(30)	Attribute Name: The name of the attribute
GORSDAV_DISC	NOT NULL VARCHAR2(64)	Discriminator: The discriminator value for multiple valued attributes
GORSDAV_PK_PARENTTAB	NOT NULL VARCHAR2(512)	Primary Key of the row in Parent Table
GORSDAV_VALUE	NOT NULL SYS.ANYDATA	Value: The Attribute Value (of type ANYTYPE: can be any data type).
GORSDAV_ACTIVITY_DATE	NOT NULL DATE	Date that information for the row was inserted or last updated
GORSDAV_USER_ID	NOT NULL VARCHAR2(30)	The unique identification of the user
GORSDAV_DATA_ORIGIN	VARCHAR2(30)	Source system that created or updated the row

SDE Discriminator Values Table (GORSDDV)

This new table stores user-defined Discriminator values

Column	Data Type	Description
GORSDDV_SDDC_CODE	VARCHAR2(10) NOT NULL	Code: The Discriminator Code of the Discriminator Value
GORSDDV_DISC	VARCHAR2(64) NOT NULL	Discriminator: The discriminator value that is allowed
GORSDDV_DESC	VARCHAR2(64) NOT NULL	Description: The description for the discriminator value
GORSDDV_ACTIVITY_DATE	DATE NOT NULL	Date that information for the row was inserted or last updated
GORSDDV_USER_ID	VARCHAR2(30) NOT NULL	The unique identification of the user
GORSDDV_DATA_ORIGIN	VARCHAR2(30)	Source system that created or updated the row

SDE Temporary Discriminator Query Table (GOTSDCR)

This new temporary table stores values from Dynamic Query.

Column	Data Type	Description
GOTSDCR_TABLE_NAME	VARCHAR2(30) NOT NULL	Table Name: The name of the table supplemented by the attribute
GOTSDCR_ATTR_NAME	VARCHAR2(30) NOT NULL	Attribute Name: The name of the attribute
GOTSDCR_DISC	VARCHAR2(64) NOT NULL	Discriminator: The discriminator value for multiple valued attributes
GOTSDCR_DESC	VARCHAR2(64)	Description: The description for the discriminator value

New APIs

GB_SDE_DISCRIMINATOR

Table	Objects	API Object Name	API Entity Name	Task Performed
GOBSDDC		gb_sde_discriminator	SDE_DISCRIMINATOR	Stores and retrieves discriminator information for SDE processing.

GB_SDE_DISCRIM_VALUE

Table	Objects	API Object Name	API Entity Name	Task Performed
GORSDDV		gb_sde_discrim_value	DISCRIM_VALUE	Stores and retrieves discriminator values for SDE processing.

GB_SDE_METADATA

Table	Objects	API Object Name	API Entity Name	Task Performed
GORSDAM		gb_sde_metadata	SDE_METADATA	Stores and retrieves metadata for SDE attributes.

GB_SDE_TABLE

Table	Objects	API Object Name	API Entity Name	Task Performed
GOBSDTB		gb_sde_table	SDE_TABLE	Stores and retrieves information on Banner tables that have been extended with supplemental data through SDE.

Changed Packages

The following libraries and packages were changed to support SDE processing.

- GOQOLIB
- GOQRPLS
- GUMAPPL

New Scripts

The following scripts are run as part of the 8.0 installation process.

Note

Some of these scripts perform actions that are applicable only for institutions that used a custom version of Supplemental Data Engine prior to this 8.0 baseline version of SDE. For example, `gobsdct_080000_04.sql` drops a column that existed in the previous version of SDE. These scripts will not cause any problems when run for institutions implementing SDE for the first time, so you should run the full sequence of scripts regardless of whether your institution used a previous version of SDE.

Script Name	Script Purpose
`gobsdct_080000_01.sql`	Creates the table GOBSDCT
`gobsdct_080000_02.sql`	Adds comments on table and columns
`gobsdct_080000_03.sql`	Adds a constraint
`gobsdct_080000_04.sql`	Removes the `_CREATE_SOURCE` column, which is no longer needed
`gobsddc_080000_01.sql`	Creates the table GOBSDDC
`gobsddc_080000_02.sql`	Adds comments on table and columns
`gobsddc_080000_03.sql`	Adds a constraint
`gobsddc_080000_04.sql`	Drops a constraint in order to recreate it according to baseline standards
`gobsddc_080000_05.sql`	Adds a constraint

Script Name	Script Purpose
gobsddc_080000_06.sql	Removes the _CREATE_SOURCE column, which is no longer needed
gobsdtb_080000_01.sql	Creates the table GOBSDTB
gobsdtb_080000_02.sql	Adds comments on table and columns
gobsdtb_080000_03.sql	Adds a constraint
gobsdtb_080000_04.sql	Removes the _CREATE_SOURCE column, which is no longer needed
gorsdam_080000_01.sql	Creates the table GORSDAM
gorsdam_080000_02.sql	Adds comments on table and columns
gorsdam_080000_03.sql	Adds a constraint
gorsdam_080000_04.sql	Drops a constraint in order to recreate it according to baseline standards
gorsdam_080000_05.sql	Adds a constraint
gorsdam_080000_06.sql	Drops a constraint in order to recreate it according to baseline standards
gorsdam_080000_07.sql	Adds a constraint
gorsdam_080000_08.sql	Drops a constraint in order to recreate it according to baseline standards
gorsdam_080000_09.sql	Adds a constraint
gorsdam_080000_10.sql	Drops a constraint in order to recreate it according to baseline standards
gorsdam_080000_11.sql	Adds a constraint
gorsdam_080000_12.sql	Removes the _CREATE_SOURCE column, which is no longer needed
gorsdav_080000_01.sql	Creates the table GORSDAV
gorsdav_080000_02.sql	Adds comments on table and columns
gorsdav_080000_03.sql	Adds a constraint
gorsdav_080000_04.sql	Drops a constraint in order to recreate it according to baseline standards

Script Name	Script Purpose
gorsdav_080000_05.sql	Adds a constraint
gorsdav_080000_06.sql	Creates an index
gorsdav_080000_07.sql	Removes the _CREATE_SOURCE column, which is no longer needed
gorsddv_080000_01.sql	Creates the table GORSDDV
gorsddv_080000_02.sql	Adds comments on table and columns
gorsddv_080000_03.sql	Adds a constraint
gorsddv_080000_04.sql	Drops a constraint in order to recreate it according to baseline standards
gorsddv_080000_05.sql	Adds a constraint
gorsddv_080000_06.sql	Removes the _CREATE_SOURCE column, which is no longer needed
gotsdcr_080000_01.sql	Creates the table GOTSDCR
gotsdcr_080000_02.sql	Adds comments on table and columns
gotsdcr_080000_03.sql	Adds a constraint
ggobsdcti_080000.sql	Inserts seed data
ggurmesgi_080000.sql	Inserts seed data

Using Supplemental Data in Self-Service

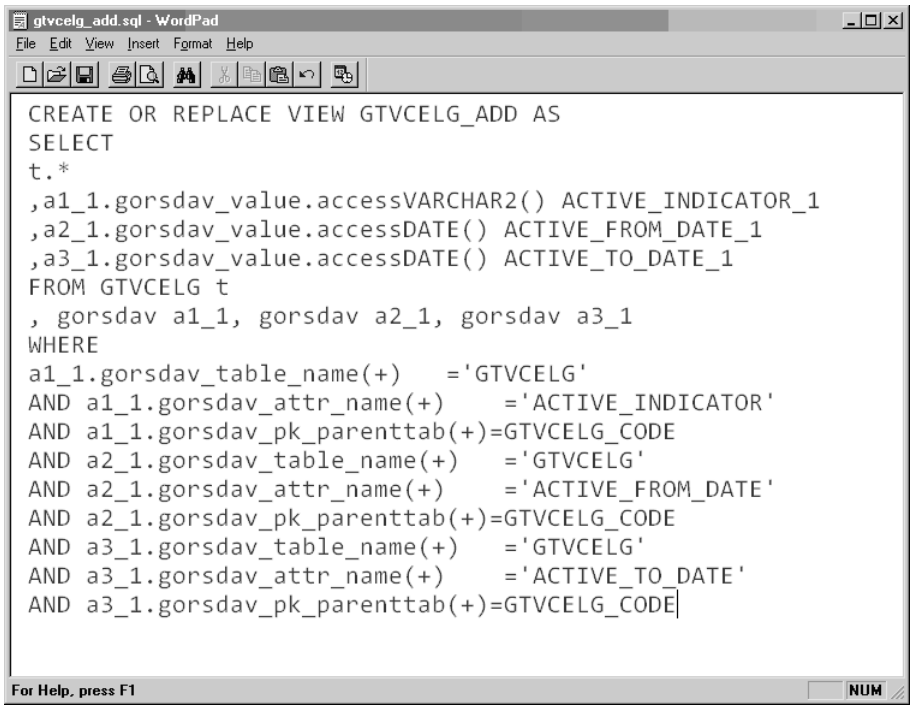
Supplemental data can be used in Banner Self-Service with a limited amount of custom programming. The following narrative illustrates the steps of the process in a typical example.

Step 1 Set Up SDE Attributes

SDE attributes have been created for table GTVCELG to add three SDE fields: an **Active Indicator**, a **From Date**, and a **To Date**.

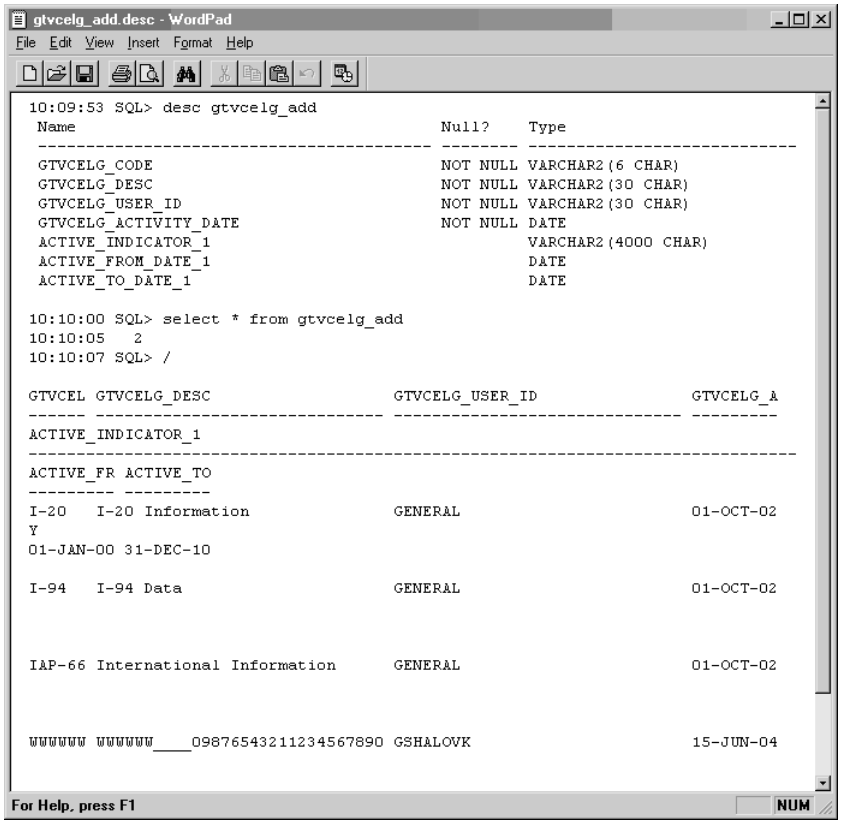
Step 2 Generate DDL

In the Generate DDL block of GOASDMD, **DDL Type** is set to *Additional Attributes View*, and the **Generate** (hourglass) button is clicked. A script is generated. The script is copied from GOASDMD and pasted into the text editor window shown below.



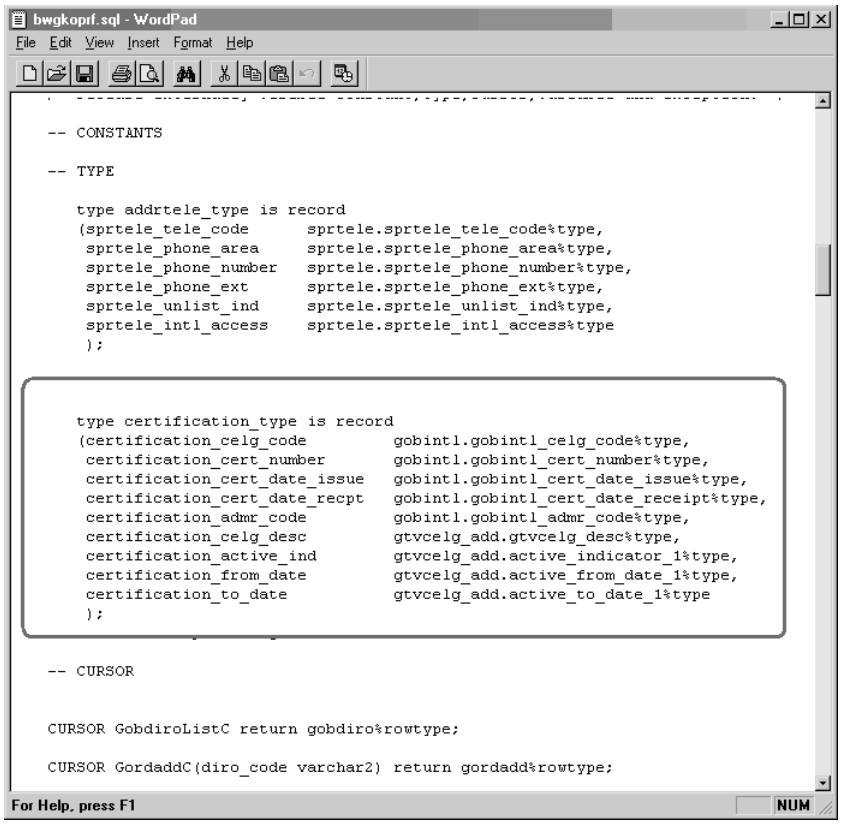
Step 3 Generate View

The Apply button is clicked, and the view shown below is created in the database.



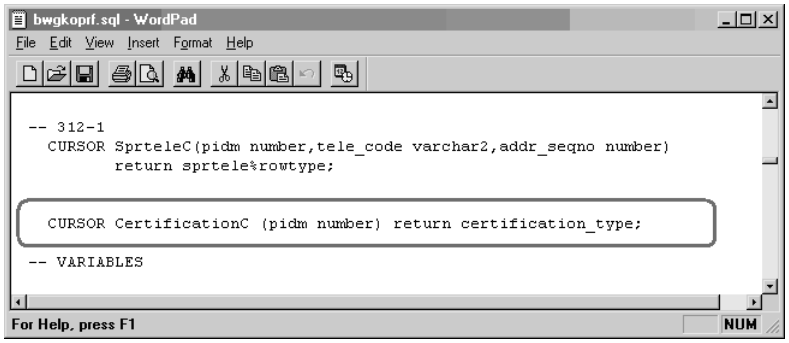
Step 4 Modify the Record Type in the Self-Service Package

The code from the view is inserted into the Self-Service package header bwgkoprf.sql. First, the record type is modified to include new columns from the view.



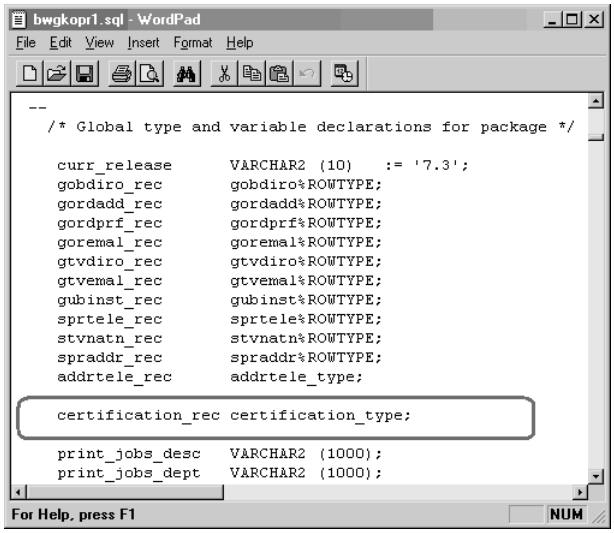
Step 5 Add Cursor Type

A cursor type for the new columns is added.



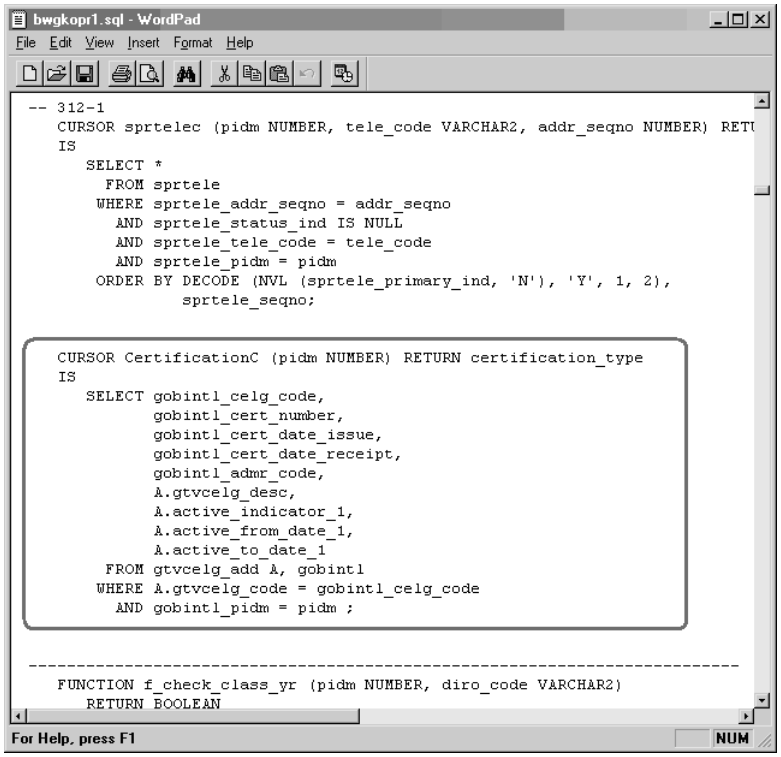
Step 6 Add Record Reference

In the self-service package body, bwgkopr1.sql, a record reference is added.



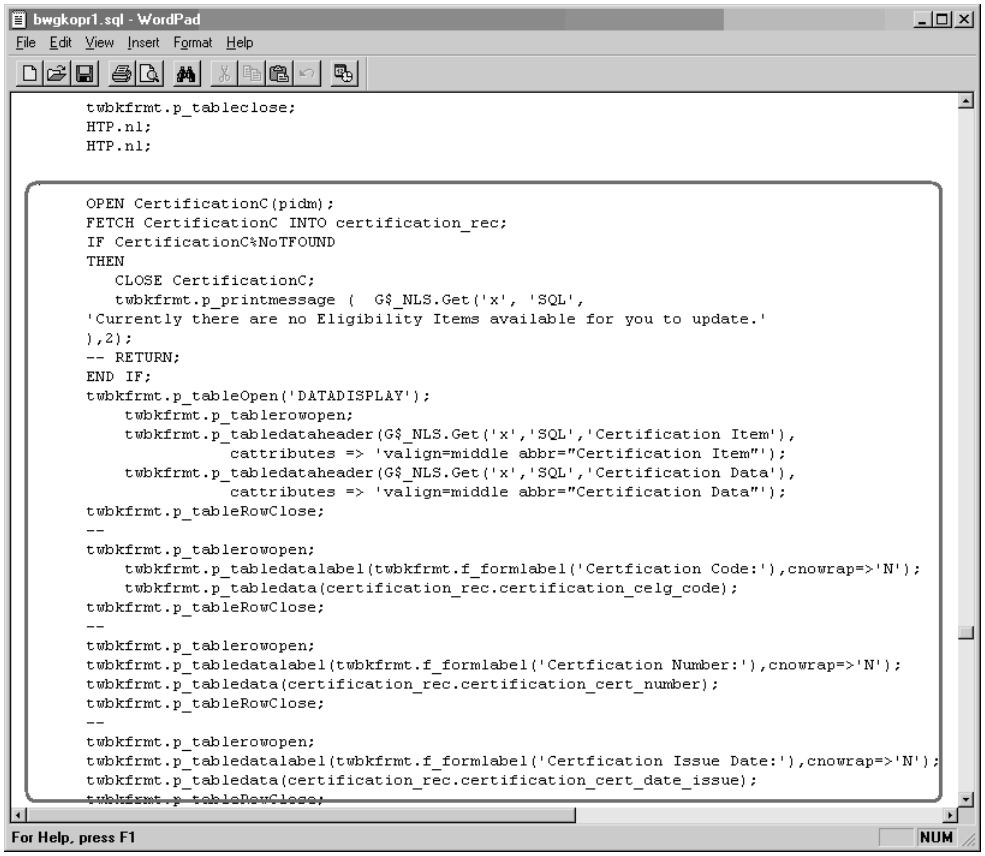
Step 7 Add Cursor Body

In the self-service package body, the cursor body is added.



Step 8 Add Cursor Open and Fetch

The cursor open and fetch is added, along with data display statements.



The resulting new block can be seen on the existing Directory Profile page, which is displayed by the BWGKOPRF package.

10 Internationalization - Technical

See “Internationalization - Functional” on page 57 for an overview of this feature.

Database Change to UTF8

Before installing Banner General 8.0, Banner’s Oracle database must be converted to enable the UTF8 character set. UTF8 is a specific implementation of the Unicode standard. This change will allow Banner data to employ any international alphabet and any other Unicode character.

As part of this conversion, the database semantics must be changed from *byte* to *char*. This change is necessary because the UTF8 standard allows for a variable number of bytes per character.

Note

This change should be transparent to database processes and should not require any source code changes, except for calculations that are based on assumptions about the number of bytes a piece of data contains. If these exist in your source code, they should be changed so that they are based on characters rather than bytes.

Because of the change to UTF8 and other technical changes associated with Banner 8.0, there are significant steps that must be taken *before* beginning the 8.0 installation. See *Banner 8.0 Pre-Installation Guide* (general80000pre-in.pdf) for more information.

New Tables

Additional ID Table (GORADID)

This new table stores additional ID information. One or more additional IDs can be associated with a specific person record (PIDM). Each additional ID must have a designated additional ID type.

Additional IDs are maintained through a new Additional ID window on several *%IDEN* forms.

Column	Data Type	Description
GORADID_PIDM	NUMBER(8)	The internal identifier of the person associated with the additional ID.
GORADID_ADDITIONAL_ID	VARCHAR2(50)	The identification number for this additional ID.
GORADID_ADID_CODE	VARCHAR2(4)	The additional ID type code.
GORADID_USER_ID	VARCHAR2(30)	The ID of the user who created or updated the record.
GORADED_ACTIVITY_DATE	DATE	The date the record was created or last updated.
GORADID_DATA_ORIGIN	VARCHAR2(30)	The system that created or updated the record.

Additional ID Type Validation Table (GTVADID)

This new validation table stores type codes and descriptions for additional ID records on the Additional ID Table (GORADID).

Additional ID type codes are maintained on the new Additional Identification Type Validation Form (GOBADID).

Column	Data Type	Description
GTVADID_CODE	VARCHAR2(4)	A code for the type of additional ID.
GORADID_DESC	VARCHAR2(30)	A description of the type of additional ID.
GTVADID_USER_ID	VARCHAR2(30)	The ID of the user who created or updated the record.
GTVADID_ACTIVITY_DATE	DATE	The date the record was created or last updated.
GTVADID_DATA_ORIGIN	VARCHAR2(30)	The system that created or updated the record.

Changed Tables

The following Banner General tables have new or changed columns for internationalization. The changes are detailed in the sections below.

GLRCALC	GORSEVS	GUBINST
GOBINTL	GORSVAH	GURALMP
GOBSEVS	GORSVAS	GURAPAY
GORCCAU	GORSVEH	GURCURR
GOREMAL	GORSVEI	GURFDED
GORNAME	GOTCMME	GURFEED
GORSEVD	GTVZIPC	GUTWUSR
GORSEVH	GUBGISL	GXRDIRD

New and Expanded Fields

New Person Information Fields

The four new fields listed below have been added to every table containing related information. Note that these new fields, which support international name, address, and telephone information, have not been made visible on any Banner form in this release.

Field	Length
House Number (_HOUSE_NUMBER)	10
Street Address Line 4 (_STREET_LINE_4)	75
Telephone Country Code (_CTRY_CODE_PHONE)	4
Surname Prefix (_SURNAME_PREFIX)	10

Expanded Person Information Fields

Tables that store name, address, telephone, e-mail, or ID information have been modified to handle the greater length of the fields listed below.

Field	New Length
First Name (_FIRST_NAME)	60
Middle Name (_MI)	60

Field	New Length
Legal Name (_LEGAL_NAME)	500
Street Address Line 1 (_STREET_LINE1)	75
Street Address Line 2 (_STREET_LINE2)	75
Street Address Line 3 (_STREET_LINE3)	75
City (_CITY)	50
ZIP (_ZIP)	30
Area Code (_PHONE_AREA)	6
Telephone (_PHONE_NUMBER)	12
Extension (_PHONE_EXT)	10
E-mail Address (_EMAIL_ADDRESS)	128
SSN (_SSN)	15
Name Tag Name (_NAME_TAG_NAME)	120
Place Card Name (_PLACE_CARD_NAME)	120

Expanded Currency Fields

All Banner General fields that store currency values have been expanded to a precision of 17,2.

Tables with New or Expanded Columns

The Banner General tables with new or expanded columns for internationalization are listed below in alphabetical order.

GERATTD

Column	Previous Length	New Length
GERATTD_NAME_TAG_NAME	60	120
GERATTD_PLACE_CARD_NAME	60	120

GLRCALC

Column	Previous Length	New Length
GLRCALC_AMT01		17,2
GLRCALC_AMT02		17,2
GLRCALC_AMT03		17,2
GLRCALC_AMT04		17,2
GLRCALC_AMT05		17,2
GLRCALC_AMT06		17,2
GLRCALC_AMT07		17,2
GLRCALC_AMT08		17,2
GLRCALC_AMT09		17,2
GLRCALC_AMT10		17,2
GLRCALC_AMT11		17,2
GLRCALC_AMT12		17,2
GLRCALC_AMT13		17,2
GLRCALC_AMT14		17,2
GLRCALC_AMT15		17,2
GLRCALC_AMT16		17,2
GLRCALC_AMT17		17,2
GLRCALC_AMT18		17,2
GLRCALC_AMT19		17,2
GLRCALC_AMT20		17,2

GOBSEVS

Column	Previous Length	New Length
GOBSEVS_BINATION_FUNDS		17,2
GOBSEVS_DEPENDENT_EXPENSES		17,2
GOBSEVS_EMPLOYER_CITY	60	No change
GOBSEVS_EMPLOYER_FIRST_NAME	40	60
GOBSEVS_EMPLOYER_SURNAME_PREFIX	New	10
GOBSEVS_EMPLOYER_ZIP	9	30
GOBSEVS_EMPLOYMENT_FUNDS		17,2
GOBSEVS_EV_GOVT_FUNDS		17,2
GOBSEVS_GOVT_ORG_FUNDS		17,2
GOBSEVS_GOVT_ORG_FUNDS_2		17,2
GOBSEVS_INTL_ORG_FUNDS		17,2
GOBSEVS_INTL_ORG_FUNDS_2		17,2
GOBSEVS_LIVING_EXPENSES		17,2
GOBSEVS_OTHER_EXPENSES		17,2
GOBSEVS_OTHER_FUNDS		17,2
GOBSEVS_OTHER_ORG_FUNDS		17,2
GOBSEVS_PERSONAL_FUNDS		17,2
GOBSEVS_PROGRAM_SPONSOR_FUNDS		17,2
GOBSEVS_SCHOOL_FUNDS		17,2
GOBSEVS_TUITION_EXPENSE		17,2

GORCCAU

Column	Previous Length	New Length
GORCCAU_STREET_LINE1	30	75
GORCCAU_STREET_LINE2	30	75
GORCCAU_ZIP	10	30

GOREMAL

Column	Previous Length	New Length
GOREMAL_EMAIL_ADDRESS	90	128

GORSEVD

Column	Previous Length	New Length
GORSEVD_DEP_FIRST_NAME	25	60
GORSEVD_DEP_SURNAME_PREFIX	New	10

GORSEVH

Column	Previous Length	New Length
GORSEVH_DEP_FIRST_NAME	25	60
GORSEVH_DEP_SURNAME_PREFIX	New	10

GORSEVS

Column	Previous Length	New Length
GORSEVS_ACT_SITE_CITY	60	No change
GORSEVS_ACT_SITE_ZIP	9	30
GORSEVS_BINATION_FUNDS		17,2
GORSEVS_DEPENDENT_EXPENSES		17,2
GORSEVS_EMPLOYER_CITY	60	No change

Column	Previous Length	New Length
GORSEVS_EMPLOYER_FIRST_NAME	40	60
GORSEVS_EMPLOYER_SURNAME_PREFIX	New	10
GORSEVS_EMPLOYER_ZIP	9	30
GORSEVS_EMPLOYMENT_FUNDS		17,2
GORSEVS_EV_GOVT_FUNDS		17,2
GORSEVS_FIRST_NAME	25	60
GORSEVS_GOVT_ORG_FUNDS		17,2
GORSEVS_GOVT_ORG_FUNDS_2		17,2
GORSEVS_HOUSE_NUMBER	New	10
GORSEVS_INTL_ORG_FUNDS		17,2
GORSEVS_INTL_ORG_FUNDS_2		17,2
GORSEVS_LIVING_EXPENSES		17,2
GORSEVS_MI	25	60
GORSEVS_NONUSA_CITY	60	No change
GORSEVS_NONUSA_STREET_LINE1	60	75
GORSEVS_NONUSA_STREET_LINE2	60	75
GORSEVS_NONUSA_STREET_LINE3		75
GORSEVS_NONUSA_STREET_LINE4	New	75
GORSEVS_NONUSA_ZIP	20	30
GORSEVS_OTHER_EXPENSES		17,2
GORSEVS_OTHER_FUNDS		17,2
GORSEVS_OTHER_ORG_FUNDS		17,2
GORSEVS_PERSONAL_FUNDS		17,2
GORSEVS_PROGRAM_SPONSOR_FUNDS		17,2
GORSEVS_SCHOOL_FUNDS		17,2

Column	Previous Length	New Length
GORSEVS_SURNAME_PREFIX	New	10
GORSEVS_TUITION_EXPENSE		17,2
GORSEVS_USA_CITY	60	No change
GORSEVS_USA_STREET_LINE1	60	75
GORSEVS_USA_STREET_LINE2	60	75
GORSEVS_USA_STREET_LINE3		75
GORSEVS_USA_STREET_LINE4	New	75
GORSEVS_USA_ZIP	9	30

GORSVAH

Column	Previous Length	New Length
GORSVAH_CITY	60	No change
GORSVAH_HOUSE_NUMBER	New	10
GORSVAH_STREET_LINE1	60	75
GORSVAH_STREET_LINE2	60	75
GORSVAH_STREET_LINE3		75
GORSVAH_STREET_LINE4	New	75
GORSVAH_ZIP	5	30

GORSVAS

Column	Previous Length	New Length
GORSVAS_CITY	60	No change
GORSVAS_HOUSE_NUMBER	New	10
GORSVAS_STREET_LINE1	60	75
GORSVAS_STREET_LINE2	60	75

Column	Previous Length	New Length
GORSVAS_STREET_LINE3		75
GORSVAS_STREET_LINE4	New	75
GORSVAS_ZIP	10	30

GORSVEH

Column	Previous Length	New Length
GORSVEH_CITY	60	No change
GORSVEH_HOUSE_NUMBER	New	10
GORSVEH_STREET_LINE1	60	75
GORSVEH_STREET_LINE2	60	75
GORSVEH_STREET_LINE3		75
GORSVEH_STREET_LINE4	New	75
GORSVEH_ZIP	5	30

GORSVEI

Column	Previous Length	New Length
GORSVEI_CITY	60	No change
GORSVEI_HOUSE_NUMBER	New	10
GORSVEI_STREET_LINE1	60	75
GORSVEI_STREET_LINE2	60	75
GORSVEI_STREET_LINE3		75
GORSVEI_STREET_LINE4	New	75
GORSVEI_ZIP	10	30

GOTCMME

Column	Previous Length	New Length
GOTCMME_CITY	20	50
GOTCMME_CTRY_CODE_PHONE	New	4
GOTCMME_EMAIL_ADDRESS	90	128
GOTCMME_FIRST_NAME	15	60
GOTCMME_HOUSE_NUMBER	New	10
GOTCMME_MI	15	60
GOTCMME_PHONE_AREA	3	6
GOTCMME_PHONE_EXT	4	10
GOTCMME_PHONE_NUMBER	7	12
GOTCMME_STREET_LINE1	30	75
GOTCMME_STREET_LINE2	30	75
GOTCMME_STREET_LINE3	30	75
GOTCMME_STREET_LINE4	New	75
GOTCMME_SURNAME_PREFIX	New	10
GOTCMME_ZIP	10	30

GTVZIPC

Column	Previous Length	New Length
GTVZIPC_CITY	20	50

GUBGISL

Column	Previous Length	New Length
GUBGISL_ZIPC_CITY	20	50

GUBINST

Column	Previous Length	New Length
GUBINST_CITY	20	50
GUBINST_CTRY_CODE_PHONE	New	4
GUBINST_HOUSE_NUMBER	New	10
GUBINST_PHONE	7	12
GUBINST_PHONE_AREA	3	6
GUBINST_PHONE_EXT	4	10
GUBINST_STREET_LINE1	30	75
GUBINST_STREET_LINE2	30	75
GUBINST_STREET_LINE3	30	75
GUBINST_STREET_LINE4	New	75
GUBINST_ZIP	10	30

GURALMP

Column	Previous Length	New Length
GURALMP_PAYMENT_AMT		17,2

GURAPAY

Column	Previous Length	New Length
GURAPAY_CITY	20	50
GURAPAY_FIRST_NAME	15	60
GURAPAY_HOUSE_NUMBER	New	10
GURAPAY_MI	1	60
GURAPAY_STREET_LINE1	30	75
GURAPAY_STREET_LINE2	30	75

Column	Previous Length	New Length
GURAPAY_STREET_LINE3	30	75
GURAPAY_STREET_LINE4	New	75
GURAPAY_SURNAME_PREFIX	New	10
GURAPAY_TRANS_AMT		17,2
GURAPAY_ZIP	10	30

GURFDED

Column	Previous Length	New Length
GURFDED_INSTALL_AMT		17,2
GURFDED_TOTAL_DED_AMT		17,2

GURFEED

Column	Previous Length	New Length
GURFEED_FOREIGN_AMOUNT		17,2
GURFEED_TRANS_AMT		17,2

GUTWUSR

Column	Previous Length	New Length
GUTWUSR_EMAIL_ADDRESS	90	128
GUTWUSR_FIRST_NAME	15	60
GUTWUSR_SURNAME_PREFIX	New	10

GXRDIRD

Column	Previous Length	New Length
GXRDIRD_AMOUNT		17,2

Changed Libraries

GOQOLIB

This library's routines have been modified where necessary to handle longer values for name fields.

In addition, two new classes, `G$_CHAR_FIELD_CLASS` and `G$_CHAR_MULTILINE_CLASS`, support tooltip display of long field values.

GOQCLIB

This library was updated to support Additional ID information and expanded name and bio/demographic person information fields.

GOQRPLS

This library's routines have been modified where necessary to handle longer values for name and ID fields.

Changed Packages

The following packages were changed to support internationalization.

- gupdintl.sql
- gupdintl_tbd.sql

New APIs

GB_ADDITIONAL_IDENT

Table	Objects	API Object Name	API Entity Name	Task Performed
GORADID		`gb_additional_ident`	`ADDITIONAL_IDENT`	Stores and retrieves additional ID information.

Changed APIs

The following APIs were updated for this release to support newly expanded person, address, and telephone fields.

- GB_BIO
- GB_BLDGDEFINITION
- GB_ROOMDEFINITION
- GB_ADDRESS
- GB_EMAIL
- GB_EMERGENCY_CONTACT
- GB_IDENTIFICATION
- GB_TELEPHONE

11 Miscellaneous Enhancements

Support for Banner Enterprise Identity Services

Banner General 8.0 delivers some objects that were updated to support Single Sign-On (SSO) integration through Banner Enterprise Identity Services.

Note

These changes have no impact to institutions that are not using Banner Enterprise Identity Services.

Refer to the *Banner Enterprise Identity Services Handbook* for detailed information on the features and configuration of Banner Enterprise Identity Services.

New Objects

baniam.jar

This new JAR file contains Java classes that support SSO through Banner Enterprise Identity Services and run on Banner's Oracle*Forms server.

Changed Objects

Banner Global Initialization (GUAINIT)

This form, which initializes Banner sessions, was changed to support SSO through Banner Enterprise Identity Services.

GUAINIT's `ON-LOGON` trigger was modified to inspect the Oracle*Forms parameter `PARAMETER.IAMTICKET` as part of establishing a user's identity.

GOQWFLW

This library, which contains procedures to support Banner Workflow, was changed to support SSO through Banner Enterprise Identity Services.

Documentation Changes

With the release of Banner 8.0, you will notice significant changes to the documentation.

- The look and feel of the documentation has been modernized. This new design incorporates new fonts, increased character size, and color to make the manuals easier to read and to use.
- Detailed forms information has been moved from the user guides into online help. This change will dramatically reduce the size of all user guides delivered with Banner 8.0. A standalone version of the forms information in HTML format will also be delivered with the release, so you can continue to access forms information directly without first logging into Banner.
- For some products, defects information in the release guide now includes an abbreviated description of each defect correction. For additional details, refer to the supplemental text file delivered along with your release guides. This text file includes detailed problem, impact, and resolution information for each defect extracted directly from the Customer Support Center.
- Each manual now includes a publication date that reflects the actual month and year of publication. Any document that is revised will include an updated publication date to make it easier to identify revised materials.
- A revision history log has been added to the copyright page of each manual to identify any revised versions and associated changes.
- A link to a feedback form has been added to the copyright page of each manual, in the bookmarks of all PDF files, and into online help to enable you to provide input about the documentation.

New API/ERD Index

A new API/ERD Index provides a single starting point for HTML-based API documentation and Entity Relationship Diagrams. This new file will be available on the Customer Support Center as `api_erd_index_guide.zip`.

Desupport of Electronic Documents

The Electronic Documents module is being desupported with this release. This feature is being used by very few clients and has been superseded by newer technology.

With this change, the following Electronic Documents forms have been made obsolete:

- GOAWFIZ
- GORWFDD

- GORWFDB
- GOAWFED
- GORWFDS
- GTVWFED
- GOQWFED

In addition, the Electronic Documents (*GENWFED) menu has been removed.

Scripts delivered with this release will remove the Electronic Documents forms listed above from Banner menus and from personal options menus.

Tables, views, and packages that support Electronic Documents will be obsoleted in a future release.

12 Problem Resolutions

This section lists the problem resolutions included in Release 8.0. For details about a problem resolution, refer to the general80000resolutions.txt file that accompanies this release.

Summary of Problem Resolutions

Object	Number	Summary
API Guide	1-2BF2LP	API Guide 7.3 correction for p_delete user exit.
geaatid.fmb, soaiden.fmb and insert script	1-E0RB0	GEAATID search option not working properly (SEARCH AND DISPLAY MORE DETAIL)
geapart.fmb	CMS-DFCT95341	Problems with GEAPART query mode.
gjajobs.com	CMS-DFCT94995	Problem with VMS gjajobs.com related to calling java 14x setup after orauser.com
gjapctl.fmb	1-2O0Q6N	'Special Print Stock' default values don't always work after enhancement in General 7.2
gjapctl.fmb	1-C9NV1	Errors when running GJAPCTL after OAS Forms 9.0.4.3 - FRM-40508
gjapctl.fmb	CMS-DFCT90476	Problem with Job Submission Parameter Validation OKPVAL when process name is > 7 chars.
gjaswpt.fmb	1-2TI8NU	When using rdbms 10g - Process and Printer LOVs do not sort on GJASWPT.

Object	Number	Summary
gjirevo.fmb	1-3FSLJU	Processes ran on GJIREVO are not alphabetized on an Oracle 10.2.0.3 instance Defect 1-3FSLJU
glaextr.fmb,gliextr.fmb	1-2M6GRO	Deceased and Confidential warnings do not display at the correct time.
glblsel.pco, spvadds.sql	1-1UWGWO	Letter Generation - GLBLSEL fails with ORA-00936 error when using some SPVADDS columns
GLOLETT.pco	1-2MUOVR	GLBLSEL fails when a *SUB variable has a 2 character or longer table alias.
glrslct.fmb	1-PDHXK	GLRSLCT- Insert Record gives error ORA-1400 for clients on OAS 9.0.4.3
glrvrbl.fmb	LN73-0005-1753	Error on compile after date typed in format "09-11-2007"
goadprf.fmb	1-2URRFP	GOADPRF will not generate if Advancment module is not installed because it is looking table ATVDONR
goafbpr.fmb	1-2PBR43	GOAFBPR - form should sort user ID list
goaimmu.fmb	1-2C79RM	GORIMMU_USER_ID doesn't get updated when updates are made to an existing ID on GOAIMMU
goaintl.fmb	1-2TFT2K	GOAINTL stuck in infinite processing loop - Another Visa with unspecified dates exists
goamtch.fmb	1-1V1V4D	'Undefined function key' attempting rollback in goamtch from saaeaps
gokout1.sql	CMS-DFCT93346	Problem with GJIREVO and show document with line of over 2000 characters.
GOKRSQL.f_validate_sql_rule	1-29WWZO	Bind variable validation fails in some cases where variables begin with the same substring

Object	Number	Summary
goqrpls.fmb	CMS-DFCT105656	Problem with IDLE_TIME and "Reconnect to Database" causing ORA-942 errors
goqrpls.pll; goqolib.fmb	1-STTLU	SDE: SMAPRLE does not process SDE Correctly
gorccrd.fmb	1-2S12KF	Problem with GORCCRD and Discover credit cards needing more then 4 check digits
goriccr.fmb	1-3AFCEO	GORICCR key stroke navigation error from Translation Field
gostage	1-34OC0W	Gostage problem if Student not installed.
gsasecr.fmb	1-2CD1IB	Problem in GSASECR when duplicating a class.
gsasecr.fmb	1-30BYUC	When you Rename a class the list of users is deleted.
gsasecr.fmb	1-5N6DA	Banner Form error FRM-40735 with FGAC and non Role Security Mode.
gsasecr.fmb	1-CGB3G	Running GSASECR -- Security Mode = NONE and getting FRM-40735: DO_FORM_CALL trigger error.
gtvpars.fmb	CMS-DFCT101404	The ability to RECORD/REMOVE is disabled on GTVPARS.
gtvprnt.fmb,gjirevo.fmb, gtvprnt_080000_01.sql	1-1VMGHZ	Remove obsolete client/server GJIREVO fields from GTVPRNT form/table
guamesg.fmb	1-1MI6S0	In form GUAMESG, the LOV for 'Recipient' field is not correct. It should include all Banner users.
guaoptm.fmb	1-1FAOSD	On form GUAOPTM, in data block, form item 'Sequence Number' suppresses trailing zeros.
guaoptm.fmb	1-2AADI5	Query (F7) does not work properly in detail block on GUAOPTM Defect 1-2AADI5

Object	Number	Summary
gukmen1.sql	1-28K7F6	Spurious forms appear in GURHMNU when not all modules are installed.
gupdjar.shl	CMS-DFCT101822	UNIX Problem with gupdjar.shl not updating the $BANNER_LINKS\gurjbif.jar
Oracle Reports	CMS-DFCT105152	Use of Wildcards in params causes error on Oracle Reports
security70500trm.pdf	1-3D4IB5	Documentation - security70500trm.pdf - needs details Tab Level Access Privs assignment information.
SPVADDS.sql	1-1UWGWJ	SPVADDS view - column names not standard - causes ORA-00918 error in letter gen (GLBLSEL)
Supplemental Data Engine 7.1	1-1MN0FL	SDE install: missing instructions on how to install the provided *.gif
transporter.jar	1-21QF5X	VMS Only - The Gen73 upgrade never issued the SET FILE/ATTR on TRANSPORTER.JAR
Upgrade, BANENV	CMS-DFCT88808	BANENV, CBANENV, BANLOGIC.COM need to remove FORMS45_PATH

A Developer Guidelines for Banner 8.0 Forms

Every baseline Banner form has been updated and redelivered for Release 8.0 to support new Internationalization standards and new product-wide features. If you are manually updating a 7.x form, follow this checklist to make sure that your form conforms to Banner 8.0 standards.

Step 1 Create an 8.0 Audit Trail Entry

In the form's audit trail, create a new entry for version 8.0.

Step 2 Modify the load_current_release trigger

Modify the `load_current_release` trigger for a current release of 8.0.

Step 3 Check WHEN-NEW-RECORD-INSTANCE

If your form has a `WHEN-NEW-RECORD-INSTANCE` with a hierarchy property of *OVERRIDE*, change the hierarchy property to *AFTER*.

This change is necessary so that your form will work with the new Supplemental Data Engine.

Step 4 Add Support for Tooltips

Banner 8.0 introduces support for tooltips on data fields where the data values may be too long to fully display in the field.

Check each text item on your form. If an item has a class of `G$_GRADE_CODE_CLASS`, `G$_CODE_CLASS`, `G$_ID_CLASS` or `G$_NAME_CLASS` it will automatically inherit the tooltip feature. If a text item does not have one of those four classes, then add one of the following classes:

- For a normal, single-line field, add `G$_CHAR_FIELD_CLASS`
- For a multiline text field, add `G$_CHAR_MULTILINE_FIELD_CLASS`

Step 5 Observe Standards for Field Lengths

For Banner 8.0, new standards were established for fields containing certain kinds of data, and many fields were expanded to match these new standards.

Check the fields in your form to see if any of these length standards apply.

Field	Standard Length for Banner 8.0 Forms
First Name (_FIRST_NAME)	60
Middle Name (_MI)	60
Last Name (_LAST_NAME)	60
Legal Name (_LEGAL_NAME)	500
Street Address Line 1 (_STREET_LINE1)	75
Street Address Line 2 (_STREET_LINE2)	75
Street Address Line 3 (_STREET_LINE3)	75
City (_CITY)	50
ZIP (_ZIP)	30
Area Code (_PHONE_AREA)	6
Telephone (_PHONE_NUMBER)	12
Extension (_PHONE_EXT)	10
E-mail Address (_EMAIL_ADDRESS)	128
SSN (_SSN)	15
Any field that holds currency values	17,2
Currency Conversion Rate (_CONV_RATE)	17,7