University System of Georgia

Creating A More Educated Georgia

Banner 8 Security Enhancements – Part 1

Presented by: Les von Holstein
SunGard Higher Education
Wednesday, October 20, 2010
3:30 – 4:15

Focus Group – Thank You!

George Mason University

Georgia State University **

Georgia Board of Regents **

McGill University **

Mississippi State University

Old Dominion University

Texas Tech University

University of Illinois **

University of North Carolina Greensboro

University of New Mexico

University of Notre Dame **

University of Oregon

University of Saskatchewan

** Also participated in the Beta Testing

Focus of the Security enhancements

- Greater efficiency in security maintenance
- Enhanced Banner user account rules
- Additional user login controls
- Improved security auditing capabilities
- Secured delegation of responsibilities for distributed users

Agenda

Part 1 Topics

- Oracle/Banner Security Maintenance GSASECR Changes
  - User
  - Class
  - Object
  - Role
- Security Auditing and Audit History form (GSAAUDT)

Part 2 Topics

- New Security Level (Group Security)
- Distributed Security (GSADSEC)
- Create Distributed Security User (GSADSUM)
- Miscellaneous security enhancements

Definition of terms

- INB User ID = Oracle ID
- Banner ID = Spriden ID

- Oracle Login – means a login to any Oracle product
- Banner INB login is an Oracle ID logging into Banner
- Security Class
  - group of Banner objects
  - controls user access to objects
- Security Group
  - group of Banner objects and classes
  - controls user access to objects

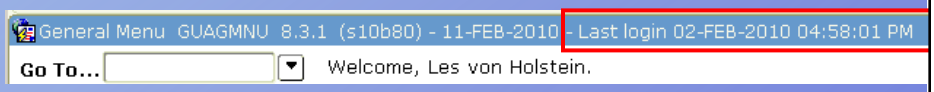
University System of Georgia

Creating A More Educated Georgia

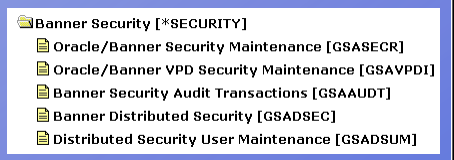
Overview of Enhancements

Banner Access

- New message on login
  - Last login date and time
  - the 'first' last login date will be the time of the first login after Banner 8.x has been installed



- New Security Menu
  - *Security
- New security class
  - BAN_FULL_SECURITY_C



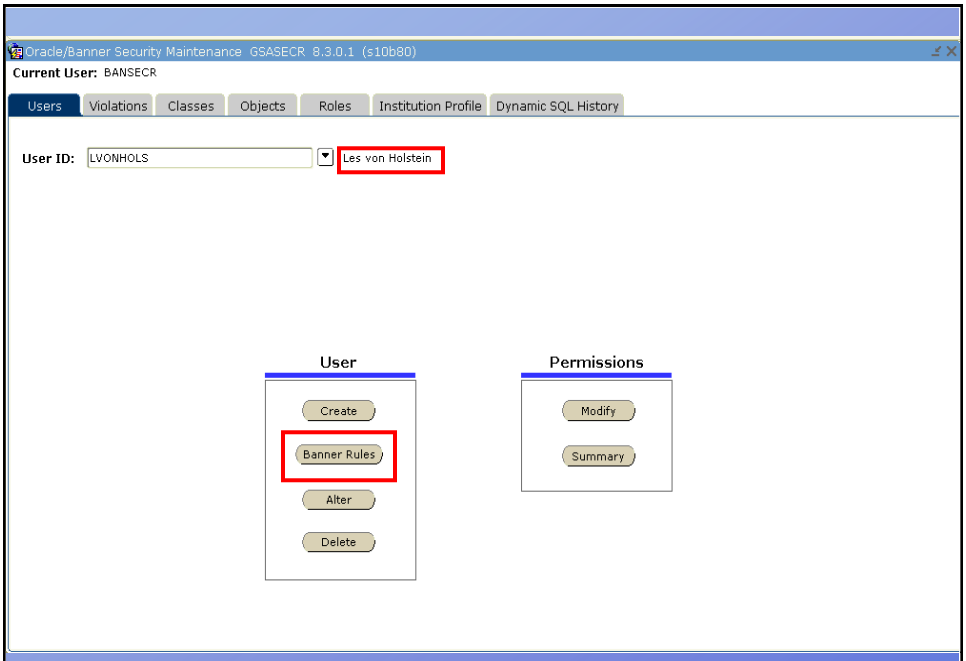
Accessing Security forms via Banner

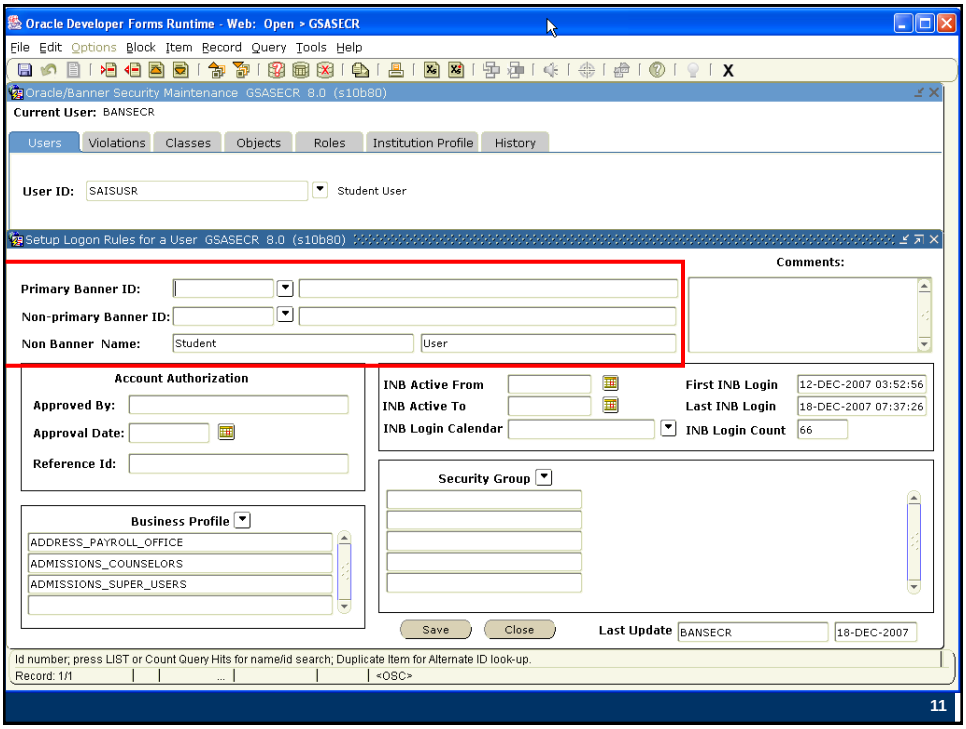
- Previously, GSASECR was accessed directly
- With new security class and menu, Bansecr can log into Banner and access GSASECR, GSAVPDI, GSAAUDT and GSADSEC
- For distributed users
  - Assign ban_full_security_c
  - Or create a new security class with a subset of these forms
  - Or assign forms to users via direct object grant

Note- only BANSECR% users can access any of the 5 security forms

Banner Security Maintenance form - GSASECR

- **Banner rules window**
  - **Oracle ID/ Banner ID**
  - **Authorization information**
  - **Comments**
  - **Active dates**
  - **Calendar**
  - **First login/ last login/number of logins displayed**
  - **Data stored in GURLOGN**
  - **Associate business profile**
  - **Security group assignment**

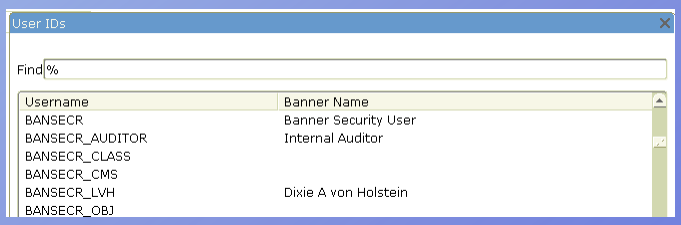




11

Names now associated with Oracle ID's

- **If 'Primary' exists then it will be used, if not then secondary, then non-Banner first/last**
- **May be accessed via call to** g$_security.g$_get_username_name(<oracle id>)
- **Oracle ID drop downs will now include user names**



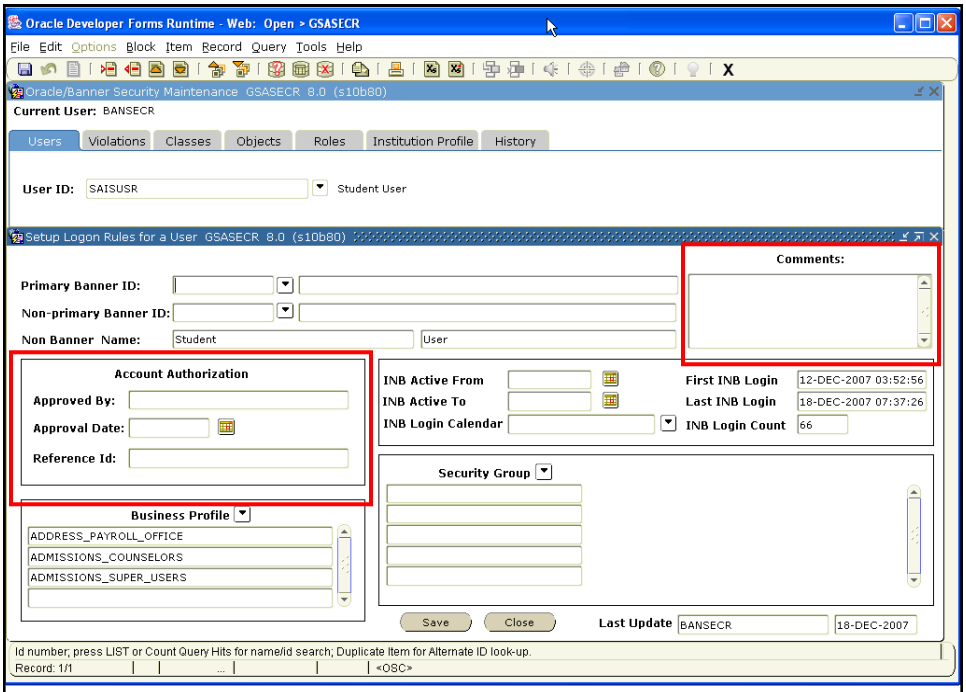
12

Oracle/Banner ID

- **Primary ID – Creates GOBEACC, ties Oracle ID to spriden ID**
  - **This does not change the functionality in GOAEAAC, it adds to it**
- **Non-Primary – Ties spriden ID to the Oracle ID but does not create the GOBEACC record**

Note- SOAIDEN and the extended ID name search window can be accessed from the above fields

- **Non Banner Name – Name associated with a user that does not have a spriden record**



Oracle Developer Forms Runtime - Web: Open > GSASECR

File Edit Options Block Item Record Query Tools Help

Oracle/Banner Security Maintenance GSASECR 8.0 (s10b80)

Current User: BANSECR

Users | Violations | Classes | Objects | Roles | Institution Profile | History

User ID: SAISUSR — Student User

Setup Logon Rules for a User GSASECR 8.0 (s10b80)

Comments:

Primary Banner ID:

Non-primary Banner ID:

Non Banner Name: Student User

Account Authorization

Approved By:

Approval Date:

Reference Id:

INB Active From

INB Active To

INB Login Calendar

First INB Login 12-DEC-2007 03:52:56

Last INB Login 18-DEC-2007 07:37:26

INB Login Count 66

Security Group

Business Profile

ADDRESS_PAYROLL_OFFICE

ADMISSIONS_COUNSELORS

ADMISSIONS_SUPER_USERS

Save | Close

Last Update BANSECR 18-DEC-2007

Id number; press LIST or Count Query Hits for name/id search; Duplicate Item for Alternate ID look-up.

Record: 1/1 | <OSC>

15

Security Calendar for Users

Oracle Developer Forms Runtime - Web: Open > GSADSEC

File Edit Options Block Item Record Query Tools Help

Banner Distributed Security 8.0 (s7s80)

Distributed Groups | Object Owners | Class Owners | Role Owners | Security Groups | Group Details | Calendars

Calendar Code	Description	User Id	Activity Date
STUDENT WORKERS	Student workers can login Mon through Thurs 9 to 6	BANSECR	03-JAN-2008
CASHIERS	Cashiers can only login during window hours	BANSECR_OBJ	08-JAN-2008

Priority	Allow	Disallow	Start Date	End Date	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Start Time	End Time	Activity Date	Comments	User Id
1	●	○	01-JAN-2008		☐	☑	☐	☑	☐	☑	0900	1700	08-JAN-2008	Window is open Mon, Wed and Fri 9 am to 5 pm.	BANSECR
2	●	○	01-JAN-2008		☐	☐	☑	☐	☑	☐	1100	2000	08-JAN-2008	Window is open Tues and Thurs 11 am to 8 pm.	BANSECR
	○	○			☐	☐	☐	☐	☐	☐					
	○	○			☐	☐	☐	☐	☐	☐					
	○	○			☐	☐	☐	☐	☐	☐					

Enter a code to be associated with a logon calendar

Record: 2/2 | <OSC>

16

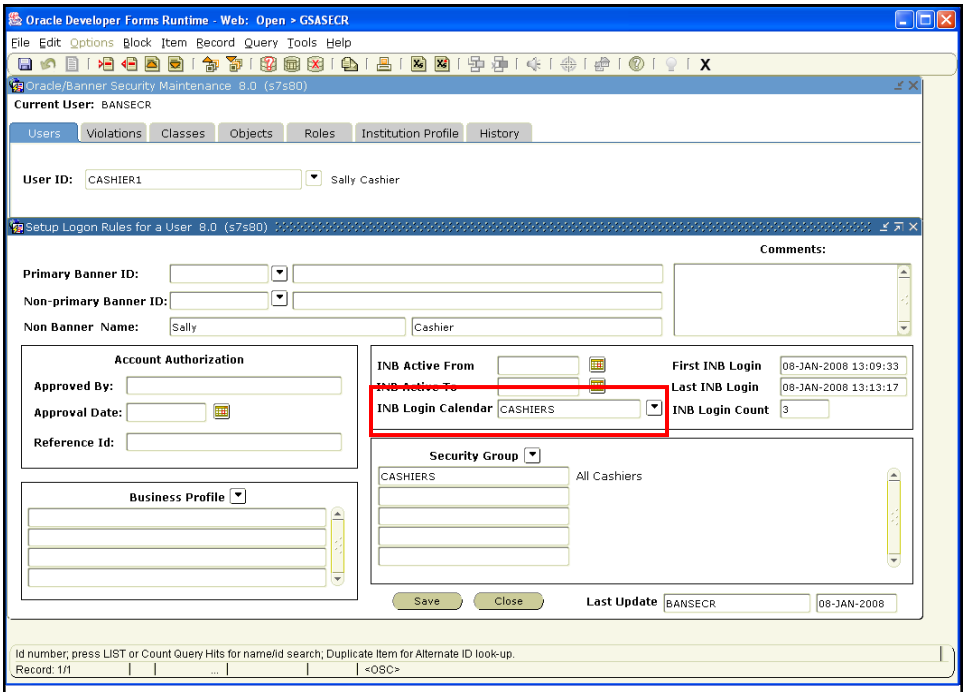
Creating calendar rules

- Create calendar code on the calendar tab
- Cursor on the calendar code, next block to access rules
- Priority
  - Priority 1 is the highest priority
  - Priority is used by the system to determine which rule to apply when there are conflicts between rules
  - End date and end time can be blank to indicate the rule is ongoing

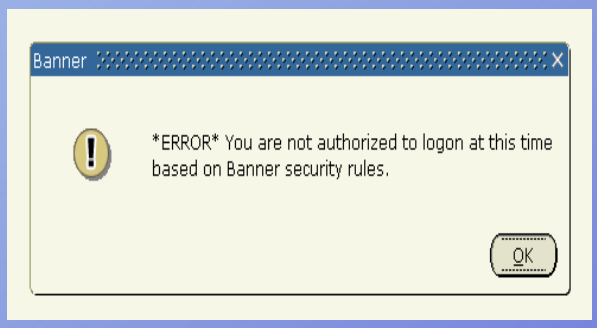
- The allow / disallow of the first date / time to match is used to determine access
- A non-match is defined as 'Disallow'
- If you don't know the 'Day of the week', check them all
- Generally indicate disallow before allow

NO HOLIDAYS OR SUMMER	Allow access only during Spring and Fall excluding holidays	BANSECR

Priority	Allow	Disallow	Start Date	End Date	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Start Time	End Time
10	○	●	01-JAN-2008	01-JAN-2008	☑	☑	☑	☑	☑	☑	☑		
Comments: No access on New Years day												User Id: BANSECR	
20	○	●	31-MAY-2008	31-MAY-2008	☑	☑	☑	☑	☑	☑	☑		
Comments: No access on Memorial Day												User Id: BANSECR	
25	○	●	15-JUN-2008	31-AUG-2008	☑	☑	☑	☑	☑	☑	☑		
Comments: No access during summer												User Id: BANSECR	
30	○	●	25-DEC-2008	25-DEC-2008	☑	☑	☑	☑	☑	☑	☑		
Comments: No access allowed during Christmas												User Id: BANSECR	
100	●	○	01-JAN-2008	31-DEC-2008	☐	☑	☑	☑	☑	☑	☐	0800	1700
Comments: Access the rest of the year during the weekdays from 8:00am - 5:00pm												User Id: BANSECR	

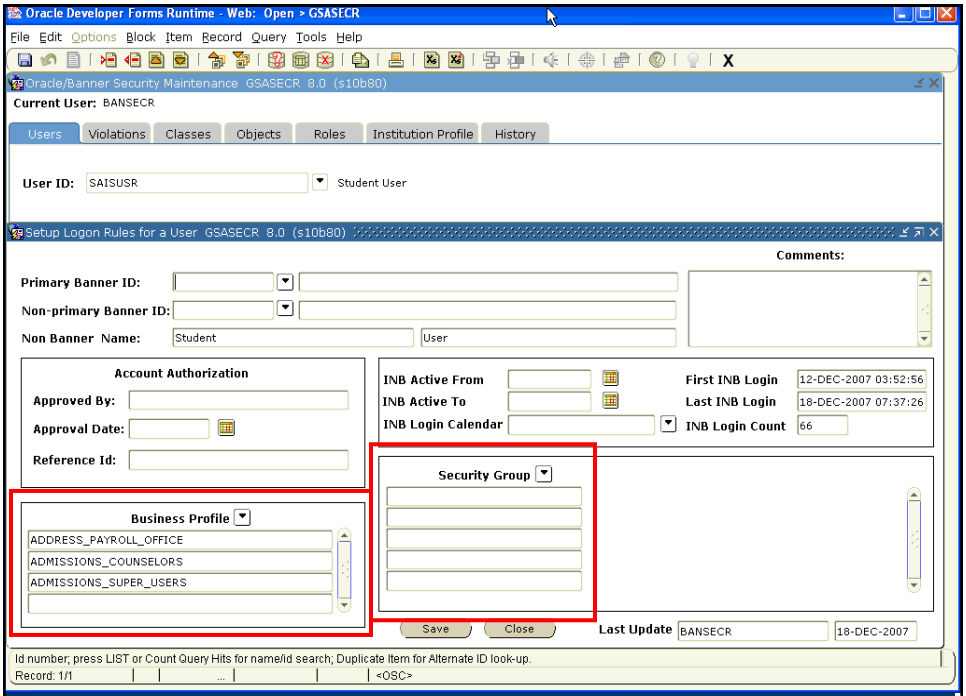


Users who do not have access based on rules



More User Rules

- **Business Profile**
  - Grouping feature used in VBS, PII and Masking
  - A user can now be added to an existing business profile via GSASECR
  - GOAFBPR can still be used to add or delete users from a business profile
- **Security Group**
  - New Grouping feature used in Banner Security
  - It is a grouping of classes and objects
  - Users can be assigned to security groups via GSASECR or GSADSEC



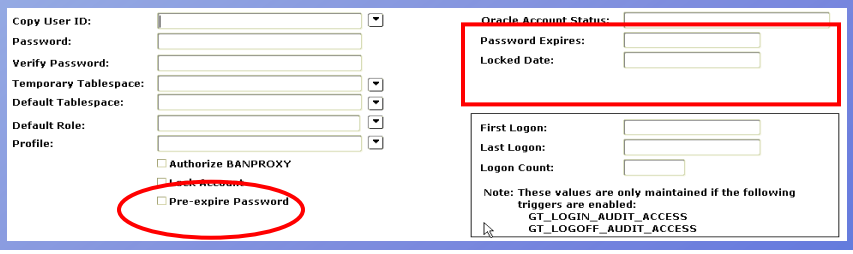
GSASECR – User creation window

- **Oracle Account Status**

  Previously: Lock, Unlock and Expire button

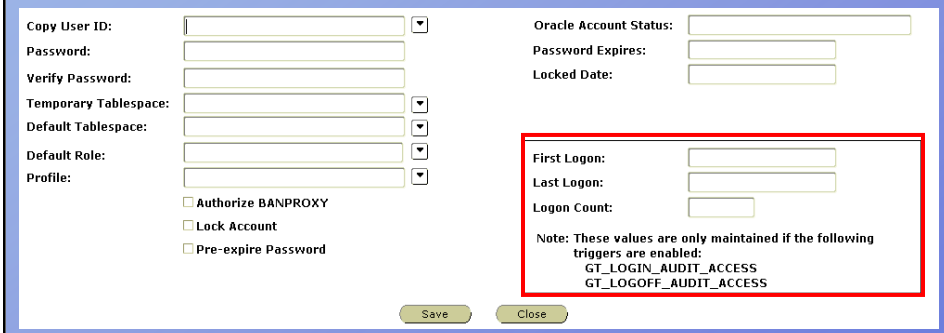
  New:

  - **Locked checkbox (buttons removed)**
  - **Pre-expire password checkbox for account create (this is tied to a new preference on the institution profile tab)**
  - **Status field**
  - **Password expires date**
  - **Account locked date**



Oracle Login and Logoff audits

If GT_LOG% triggers are enabled, Oracle first, last and logon counts will be displayed



Oracle profiles

Oracle Developer Forms Runtime - Web: Open > GSASECR

File Edit Options Block Item Record Query Tools Help

Oracle/Banner Security Maintenance GSASECR 8.0 (s10b80)

Current User: BANSECR

Users | Violations | Classes | Objects | Roles | Institution Profile | Dynamic SQL History

User ID: SAISUSR Student User

Alter or Create an ORACLE User ID GSASECR 8.0 (s10b80)

Password:
Verify Password:
Temporary Tablespace: TEMP
Default Tablespace: USERS
Default Role: BAN_DEFAULT_M
Profile: DEFAULT
Authorize BANPROXY

Oracle Account Status: OPEN
Password Expires:
Locked Date:
Lock | Unlock | Expire Password

First Logon:
Last Logon:
Logon Count:

Note: These values are only maintained if the following triggers are enabled:
GT_LOGIN_AUDIT_ACCESS
GT_LOGOFF_AUDIT_ACCESS

Save | Close

Profile to define the users default permissions at sign-on.

Record: 1/1 ... List of Valu... <OSC>

25

Profile List of Values – Choose from your existing Oracle profiles

Profiles

Find B%

Profile Name	Days password valid	Grace Days	Days locked after failure	Days until password reuse	Password changes bef
BAN_IDLE_TIME	UNLIMITED	UNLIMITED	UNLIMITED	UNLIMITED	UNLIMITED

Find | OK | Cancel

Profiles

Find B%

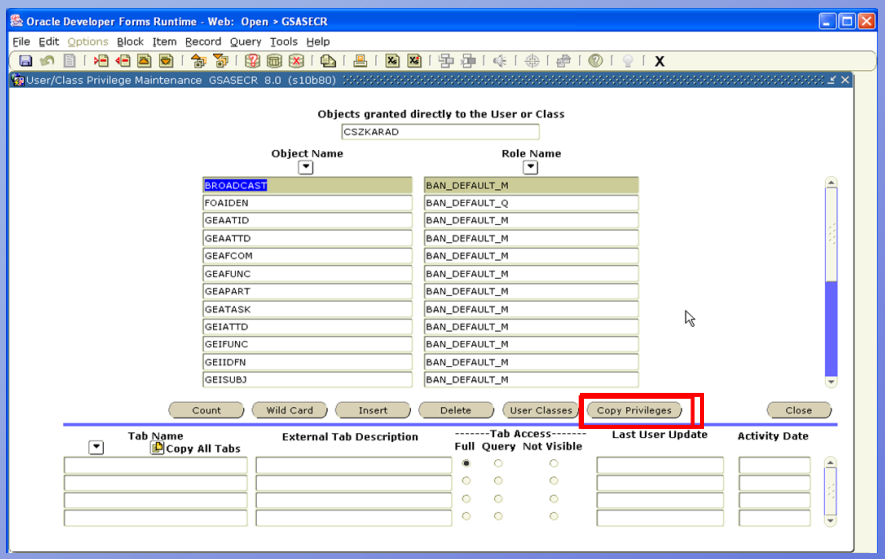
s until password reuse	Password changes before reuse	Failed logins before locking	Activated Time Limits	Connect Time Allowed	Idle Disconnect Time
LIMITED	UNLIMITED	10	FALSE	UNLIMITED	1

Find | OK | Cancel

26

- PASSWORD_VERIFY_FUNCTION
  - Ability to define a function that is to be executed anytime a password is changed
  - Create a PASSWORD_VERIFY_FUNCTION using Oracle's utlpwdmg.sql and allow only these characters to be used in a valid Banner password
    - See also Institution Profile password validation
  - FAQ #10718 - Problem with Oracle complex passwords and special punctuation characters
- Enforced in Banner on:
  - GSASECR – when Security Administrator changes password
  - GUAPSWD- when user changes password
- Enforced on all SQL based password changes

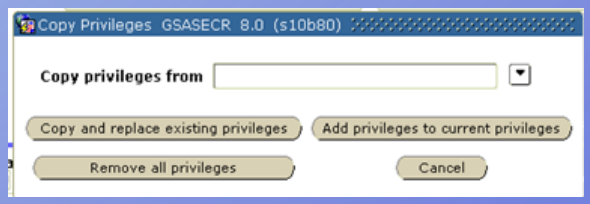
GSASECR – User maintenance improvement



GSASECR – User maintenance improvement

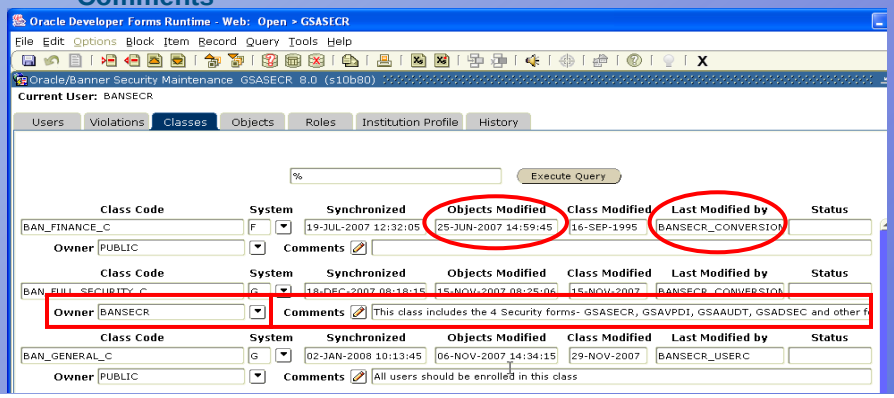
- ‘Objects Granted to Users’ window

  Copy privileges button to copy another user’s privileges to the selected user
  - “Privileges” ➔ objects in GURUTAB, GURUOBJ, GURUCLS
  - Copy and replace existing
  - Add to existing
  - Remove all privileges

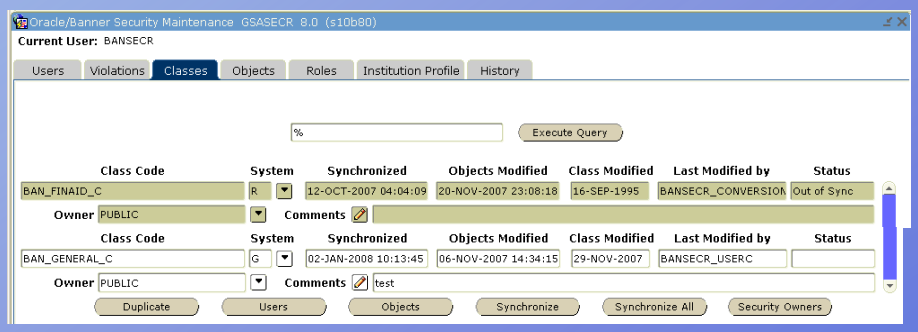


GSASECR class maintenance improvements

- Modified by User
- Objects modified date
- Owner – For distributed security
  - Public, Bansecr or distributed user
- Comments

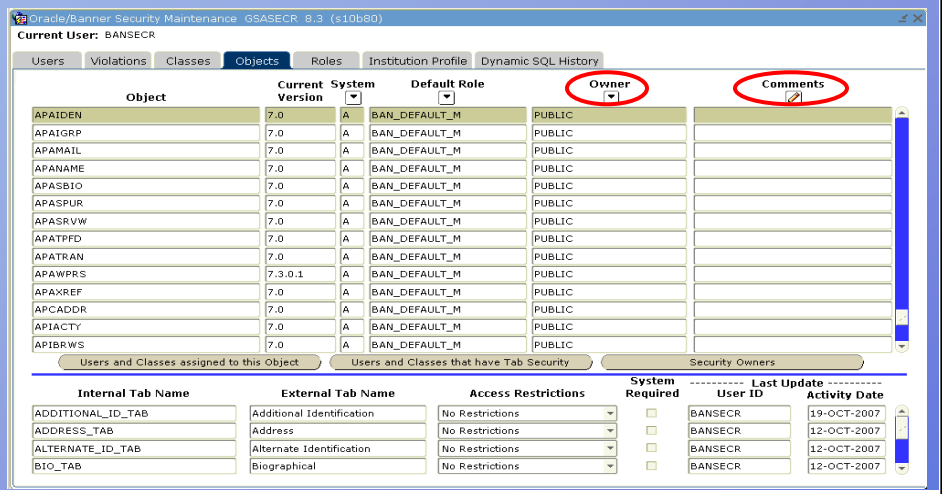


- Duplicate – will copy class attributes, users, and owners
- Users / Objects – will list users / objects associated with class
- Synchronize (All) – will ensure that the ROLE associated with the objects are granted to each user in class
- Security Owners – calls GSADSEC enabling viewing or updating of distributed security user information



GSASECR object maintenance

- Owner – for distributed security
- Comments



GSASECR – Special objects

- BROADCAST
  - Enables sending messages to all users on the Menu
- CHANNELS
  - Required for Luminis access
- EXTENDED_QUERY
  - Enables users to perform complex queries by entering a colon (:) or ampersand (&) when in query mode
  - Note: Oracle 10gR2 restricted the use of extended query via the FORMS_RESTRICT_ENTER_QUERY setting in the default.env file. If extended queries are enabled at the database level, the use of the Banner EXTENDED_ROLE can restrict extended queries on a user by user level within Banner forms.
- SSN_SEARCH
  - Enables ability to search by SSN

GSASECR – Special objects (General 8.4)

- RESET_PIN
  - Enables GB_THIRD_PARTY_ACCESS.F_PROC_PIN to reset the PIN via Letter Gen
- SDE_SQL_VALIDATION
  - Enables update of the GORRSQL Process / Rule (used for 'free form' dynamic validation of values) on GOASDMD. It also enables testing of those rules.
- SDE_SQL_TESTING
  - This object (or SDE_SQL_VALIDATION) enables execution of the GORRSQL procedure as part of the 'Test Data' process.
  - NOTE: No special security is needed to execute the procedure during normal LOV validation at SDE value data entry

GSASECR – Special objects

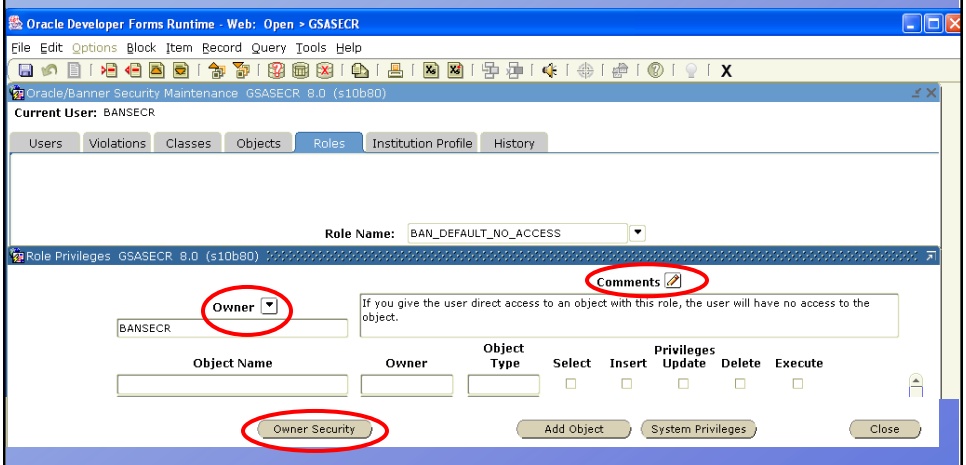
- SDE_LOV_<table>
  - Allows the user to modify data on GTVSDLV for the specified table.
  - NOTE: if you can modify the LOV's, you can also test
- SDE_TEST_<table>
  - Allows the user to test LOVs for the specified table with 'Test Data'.

➢ The table may be 'DEFAULT' to modify the generic tables or 'ALL' to indicate they can update any table on GTVSDLV
i.e. SDE_LOV_ALL, SDE_TEST_SPRIDEN, SDE_LOV_DEFAULT

➢ Note: In order to allow everyone to update and test all fields of GOASDMD you should create SDE_SQL_VALIDATION and SDE_LOV_ALL and assign them to the BAN_GENERAL_C class. Needless to say security can be set up as fine grained as needed (i.e. by table, class, user)

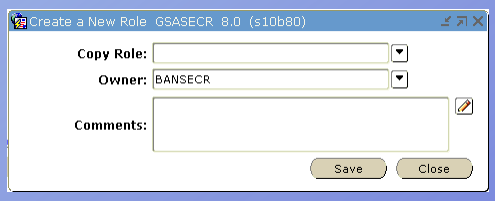
GSASECR role maintenance

- Owner – for distributed security / button to modify
- Comments



GSASECR – Create Role

- Copy an existing role
- Owner defaults to current user
- Comments default to those of role being copied, but can be overridden



New security role

BAN_DEFAULT_NO_ACCESS

Purpose is to eliminate the need for classes that are similar but have a few object differences

This role can be applied at the user level as an override

When an object is granted with this role the user will not have access to the object

Note 1: plus/gchksec.sql checks to make sure no Oracle privileges have been assigned to this role

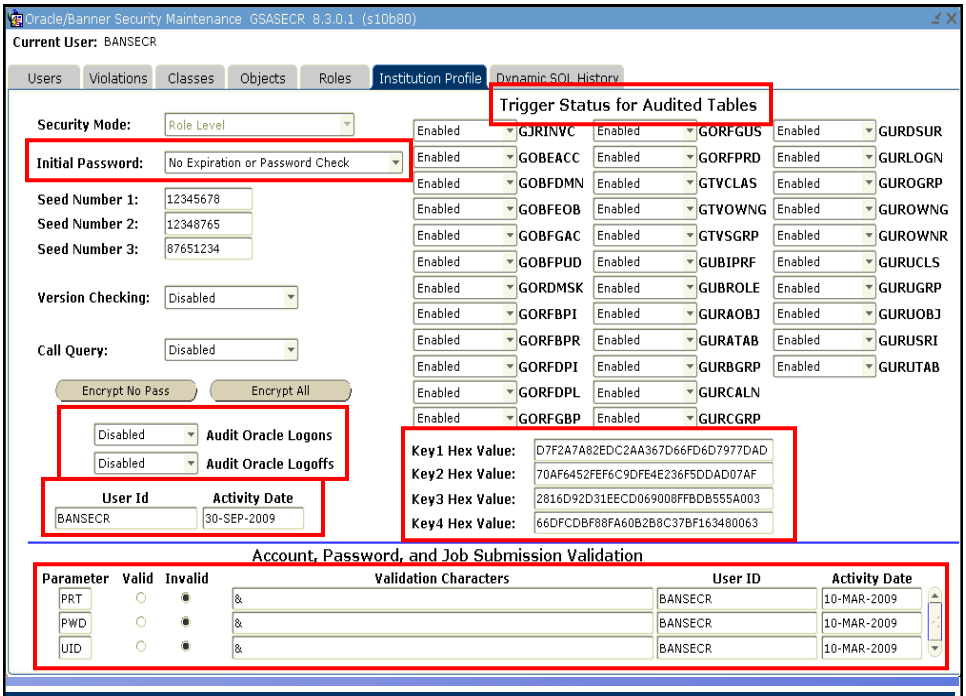
Note 2: Manually created in 8.0, part of install or upgrade in 8.1

GSASECR Institution Profile

- Initial password rule
- Audit Oracle logons
- Trigger status for audited tables
- User ID and activity date
- Parameter validation added in 7.5

  Added to GSASECR in 8.0
  - Special print (PRT) – Job submission
  - Password (PWD) – Password creation and job submission
  - Random Pin Generation (RPG) – GOATPAD Pin Generation (8.4)
  - User ID (UID) – Account creation and job submission
  - Choices are to define:
    - valid characters
    - invalid characters
    - leave blank for no validation
  - FAQ about Oracle complex characters passwords

    Title: CMS-10718



University System of Georgia

Creating A More Educated Georgia

Security Auditing

Banner Security Auditing Form (GSAAUDT)

- A new audit table added for each security table
- All security tables audited via table triggers – your choice on enabling triggers
- Option to selectively delete history
  - For each table
  - By date range
- Who can access?
  - BANSECR
  - Distributed users created with gssaudt.sql script have query access to the forms
    - You can create a separate distributed user for your auditor to view the history of transactions
    - You will have to grant delete access manually, if desired, for any non-BANSECR account

Oracle Developer Forms Runtime - Web: Open > GSAAUDT

File Edit Options Block Item Record Query Tools Help

Banner Security Audit Transactions GSAAUDT 8.0 (s10b80)

Institution | User Security | Logon Audits | Object Security | Bus Profiles | FGAC Rules | FGAC | Group Security

Profile | User / Password Validation | Security Classes | Roles | Dynamic Security SQL

Audit Time	Action	Version Checking	Security Mode	Institution	Seed Number 1	Seed Number 2	Seed Number 3	Call Query	User Id

Auditing of GUBIPRF is currently ENABLED

Press Button to Selectively Delete Audit Trail Records

Enter a query; press F8 to execute, Ctrl+Q to cancel.

Record: 1/1 | Enter-Qu... | <OSC>

43

Oracle Developer Forms Runtime - Web: Open > GSAAUDT

File Edit Options Block Item Record Query Tools Help

Banner Security Audit Transactions GSAAUDT 8.0 (s10b80)

Institution | User Security | Logon Audits | Object Security | Bus Profiles | FGAC Rules | FGAC | Group Security

Profile | User / Password Validation | Security Classes | Roles | Dynamic Security SQL

Audit Time	Action	Version Checking	Security Mode	Institution	Seed Number 1	Seed Number 2	Seed Number 3	Call Query	User Id

Auditing of GUBIPRF is currently ENABLED

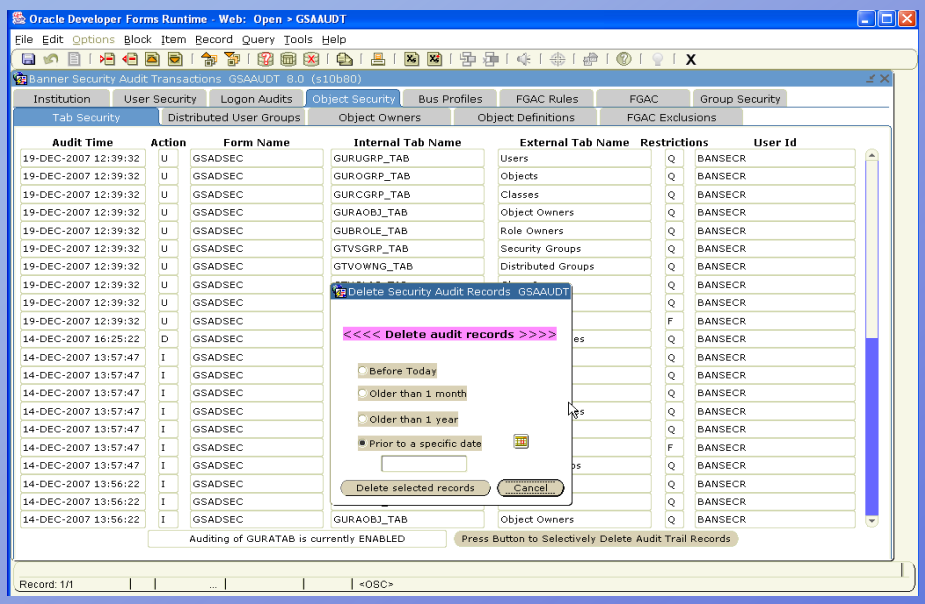
Press Button to Selectively Delete Audit Trail Records

Enter a query; press F8 to execute, Ctrl+Q to cancel.

Record: 1/1 | Enter-Qu... | <OSC>

Press this button to delete records

44



Audit Trigger Naming Conventions

- **Base Table:** **GURATAB**
- **Audit Table:** **GURAATB**
  - **Generally 'GUR'**
  - **'A' for Audit**
  - **Last 3 characters related to base table name**
- **Trigger Name:** **gt_guratab_audit_row**
  - **gt_<base table name>_audit_row**
- **Script Name:** **gutatab0.sql**
  - **Base table name with third character replaced with a 't' (indicating a trigger) followed by a 'sequence number'**

Base Tables and Related Audit Tables

Audit Table	Base Table	Comments
GURAINV	GJRINVC	Job Submission Character Validation Table
GURAEAC	GOBEACC	Enterprise Oracle Access Table
GURADMN	GOBFDMN	FGAC Domain Driver Table
GURAEOB	GOBFEOB	Objects excluded from FGAC processing rules
GURAGAC	GOBFGAC	FGAC Group Access Rules
GURAPUD	GOBFPUD	FGAC Personal User Defaults
GURAMSK	GORDMSK	Display Mask Column Rules
GURABPI	GORFBPI	FGAC PII domain business profile assignments
GURABPR	GORFBPR	FGAC business profile assignments
GURADPI	GORFDPI	FGAC PII Policys
GURADPL	GORFDPL	FGAC Domain Policy

47

Base Tables and Related Audit Tables

Audit Table	Base Table	Comments
GURAGBP	GORFGBP	FGAC Profiles per Predicate and Domain
GURAGUS	GORFGUS	FGAC Users defined for predicate and domain
GURAPRD	GORFPRD	FGAC Predicate per Domain
GURAVCL	GTVCLAS	Validation table of user classes
GURAVOG	GTVOWNG	Validation table of security group owners
GURASGR	GTVSGRP	Validation table of security groups
GURAIPF	GUBIPRF	Site profile record
GUBAROL	GUBROLE	Definitions of Banner roles
GURALGN	n/a	Login / Logout audit information
GURAAOB	GURAOBJ	All valid Banner objects
GURAATB	GURATAB	Forms and tabs that can be used in tab security

48

Base Tables and Related Audit Tables

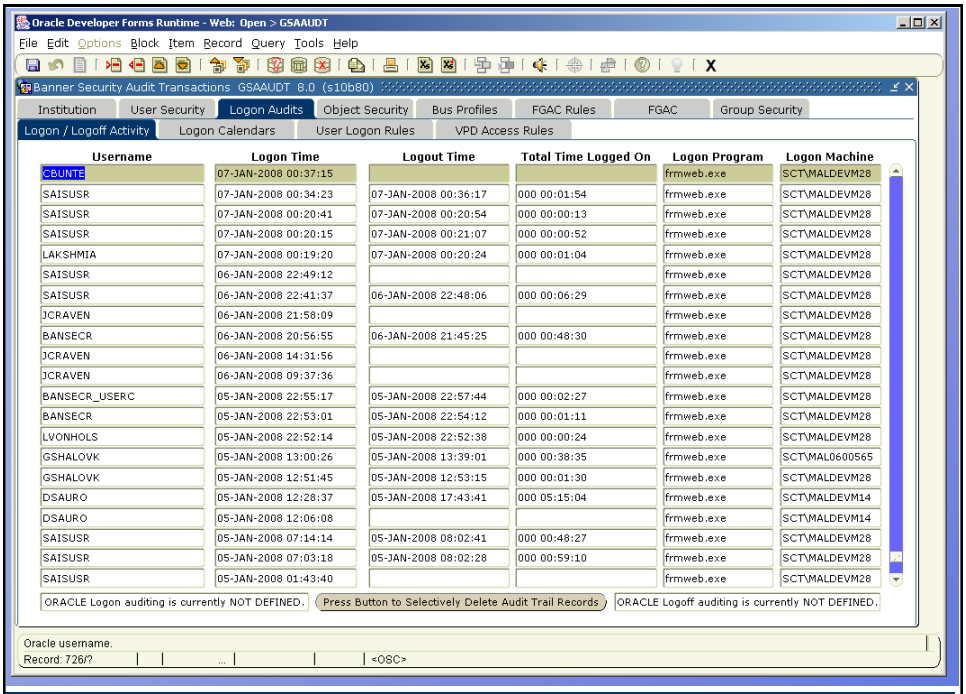
Audit Table	Base Table	Comments
GURABGP	GURBGRP	Business profiles belonging to a security group
GURACAL	GURCALN	Calendars used for logon verification
GURACGP	GURCGRP	Classes belonging to a security group
GURADSU	GURDSUR	Rules for distributed security users
GURAULG	GURLOGN	Banner Logon rules
GURAOGP	GUROGRP	Objects belonging to a security group
GURAOWG	GUROWNG	Distributed security groups
GURAOWN	GUROWNR	Object access for distributed security users
GURACLS	GURUCLS	Security classes a user is authorized to access
GURAUGP	GURUGRP	Users belonging to a security group

Base Tables and Related Audit Tables

Audit Table	Base Table	Comments
GURAUOB	GURUOBJ	Type of access, by userid, for each Banner object
GURAUSI	GURUSRI	VPD Institution/Banner User Table
GURAUTB	GURUTAB	User tab security access

Auditing Logons and Logoffs

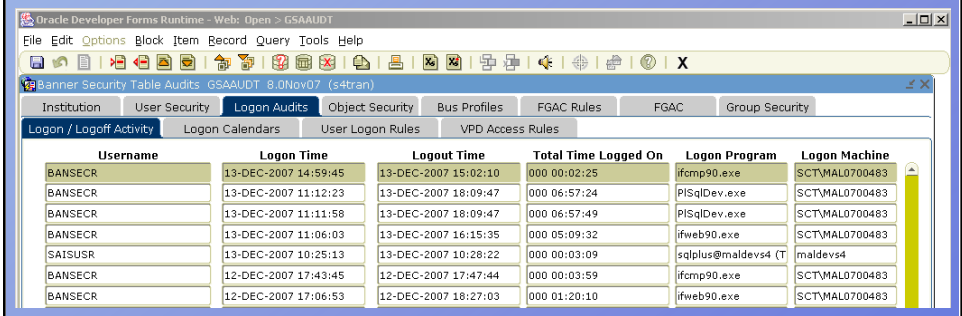
- **Logon / logoff to INB will always be audited**
- **Logon / logoff to Oracle may optionally be audited**
  - **Enable gt_login_audit_access or gt_logoff_audit_access**
  - **Oracle logons are only audited for users that are defined to have Banner access**
    - **i.e. the user id must have an entry in one of these:**
      - **GURUCLS – access granted via a class**
      - **GURUOBJ – access granted by a direct grant**
      - **GURUGRP – access granted by being in a group**
- **If user terminates connection without logging off then the logoff time will not be recorded and total connect time can not be computed**



Username	Logon Time	Logout Time	Total Time Logged On	Logon Program	Logon Machine
CBUNTE	07-JAN-2008 00:37:15			frmweb.exe	SCT\MALDEVM28
SAISUSR	07-JAN-2008 00:34:23	07-JAN-2008 00:36:17	000 00:01:54	frmweb.exe	SCT\MALDEVM28
SAISUSR	07-JAN-2008 00:20:41	07-JAN-2008 00:20:54	000 00:00:13	frmweb.exe	SCT\MALDEVM28
SAISUSR	07-JAN-2008 00:20:15	07-JAN-2008 00:21:07	000 00:00:52	frmweb.exe	SCT\MALDEVM28
LAKSHMIA	07-JAN-2008 00:19:20	07-JAN-2008 00:20:24	000 00:01:04	frmweb.exe	SCT\MALDEVM28
SAISUSR	06-JAN-2008 22:49:12			frmweb.exe	SCT\MALDEVM28
SAISUSR	06-JAN-2008 22:41:37	06-JAN-2008 22:48:06	000 00:06:29	frmweb.exe	SCT\MALDEVM28
JCRAVEN	06-JAN-2008 21:58:09			frmweb.exe	SCT\MALDEVM28
BANSECR	06-JAN-2008 20:56:55	06-JAN-2008 21:45:25	000 00:48:30	frmweb.exe	SCT\MALDEVM28
JCRAVEN	06-JAN-2008 14:31:56			frmweb.exe	SCT\MALDEVM28
JCRAVEN	06-JAN-2008 09:37:36			frmweb.exe	SCT\MALDEVM28
BANSECR_USERC	05-JAN-2008 22:55:17	05-JAN-2008 22:57:44	000 00:02:27	frmweb.exe	SCT\MALDEVM28
BANSECR	05-JAN-2008 22:53:01	05-JAN-2008 22:54:12	000 00:01:11	frmweb.exe	SCT\MALDEVM28
LVONHOLS	05-JAN-2008 22:52:14	05-JAN-2008 22:52:38	000 00:00:24	frmweb.exe	SCT\MALDEVM28
GSHALOVK	05-JAN-2008 13:00:26	05-JAN-2008 13:39:01	000 00:38:35	frmweb.exe	SCT\MAL0600565
GSHALOVK	05-JAN-2008 12:51:45	05-JAN-2008 12:53:15	000 00:01:30	frmweb.exe	SCT\MALDEVM28
DSAURO	05-JAN-2008 12:28:37	05-JAN-2008 17:43:41	000 05:15:04	frmweb.exe	SCT\MALDEVM14
DSAURO	05-JAN-2008 12:06:08			frmweb.exe	SCT\MALDEVM14
SAISUSR	05-JAN-2008 07:14:14	05-JAN-2008 08:02:41	000 00:48:27	frmweb.exe	SCT\MALDEVM28
SAISUSR	05-JAN-2008 07:03:18	05-JAN-2008 08:02:28	000 00:59:10	frmweb.exe	SCT\MALDEVM28
SAISUSR	05-JAN-2008 01:43:40			frmweb.exe	SCT\MALDEVM28

With Oracle Logon / Logoff Auditing Enabled

- Compiles
- PL/SQL Developer / TOAD
- SQL*Plus
- Any logon to the Oracle database



Username	Logon Time	Logout Time	Total Time Logged On	Logon Program	Logon Machine
BANSECR	13-DEC-2007 14:59:45	13-DEC-2007 15:02:10	000 00:02:25	ifcmp90.exe	SCT\MAL0700483
BANSECR	13-DEC-2007 11:12:23	13-DEC-2007 18:09:47	000 06:57:24	PlSqlDev.exe	SCT\MAL0700483
BANSECR	13-DEC-2007 11:11:58	13-DEC-2007 18:09:47	000 06:57:49	PlSqlDev.exe	SCT\MAL0700483
BANSECR	13-DEC-2007 11:06:03	13-DEC-2007 16:15:35	000 05:09:32	ifweb90.exe	SCT\MAL0700483
SAISUSR	13-DEC-2007 10:25:13	13-DEC-2007 10:28:22	000 00:03:09	sqlplus@maldevs4 (T	maldevs4
BANSECR	12-DEC-2007 17:43:45	12-DEC-2007 17:47:44	000 00:03:59	ifcmp90.exe	SCT\MAL0700483
BANSECR	12-DEC-2007 17:06:53	12-DEC-2007 18:27:03	000 01:20:10	ifweb90.exe	SCT\MAL0700483

Data Captured in Logon Audit (from v$session)

- SADDR — Session address
- SID — Session identifier
- SERIAL# — Session serial number. Used to uniquely identify the object in a session. Guarantees that session-level commands are applied to the correct session objects if the session ends and another session begins with the same session ID.
- AUDSID — Auditing session ID
- USERNAME — Oracle username
- PROCESS — Operating system client process ID
- MACHINE — Operating system machine name
- LOGON TIME — Time of logon
- IP ADDRESS — The IP address of the user logging on
  - SYS_CONTEXT('USERENV', 'IP_ADDRESS', 15)

Data Captured in Logon Audit (from v$session) cont.

- **OSUSER** — Operating system client user name
- **TERMINAL** — Operating system terminal name
- **PROGRAM** — Operating system program name executing during login
- **MODULE** — Name of the currently executing module as set by executing the procedure DBMS_APPLICATION_INFO .SET_MODULE during logon
- **SERVICE NAME** — Service name of the session
- **LOGOFF TIME** — Time of logoff. Value will be NULL if session is not logged off normally.
- **TOTAL TIME** — The length of time logged on. If either the logon on logoff time are null, then this value will be null.

Data Captured in Logon Audit (from v$session) cont.

- **LOGON COMMENT** — An optional comment recorded at logon time - GUAINT POST-LOGIN trigger and

```
create or replace trigger GT_LOGIN_AUDIT_ACCESS
after LOGON ON DATABASE
  call G$_SECURITY.g$_audit_banner_logon('ORACLE',
   'Database Logon Trigger')
```

- **LOGOFF COMMENT** — An optional comment recorded at logoff time – gt_logoff_audit_access trigger and

```
GUAGMNU  ON-LOGOUT trigger
   G$_SECURITY.g$_audit_banner_logoff(
     p_comment => 'Logoff from forms');
```

Table Audits are 'always' in effect

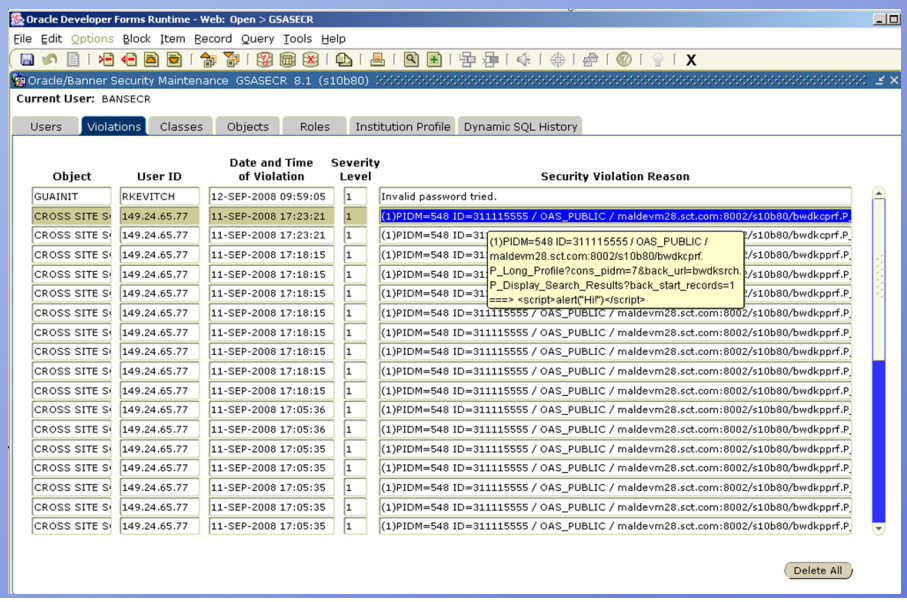
- Since these are database triggers, any insert, delete, or modify (even in SQL*Plus) will be audited
- New /plus scripts will save and restore status
  - GSAVTRIG – saves the status of the 36 new triggers
  - GRESTRIG – restores the status saved by GSAVTRIG
- Based upon local requirements for auditing batch processing (including upgrades) there may be a desire for triggers to be disabled before the process and then restored when the process is complete
- Refer to the install guides for additional information on altering the status when performing upgrades

USER_ID added to several tables

- GTVCLAS
- GUBIPRF
- GUBROLE
- GURAOBJ
- GURSQLL
- GURUCLS
- GURUOBJ
- GURUSRI

- Conversion value is 'BANSECR_CONVERSION'
- DEFAULT VALUE is sys_context('USERENV','SESSION_USER')

Violation reasons now searchable



Current User: BANSECR

Object	User ID	Date and Time of Violation	Severity Level	Security Violation Reason
GUAINIT	RKEVITCH	12-SEP-2008 09:59:05	1	Invalid password tried.
CROSS SITE S	149.24.65.77	11-SEP-2008 17:23:21	1	(1)PIDM=548 ID=311115555 / OAS_PUBLIC / maldevm28.sct.com:8002/s10b80/bwdkcprf.P_
CROSS SITE S	149.24.65.77	11-SEP-2008 17:23:21	1	(1)PIDM=548 ID=31 /s10b80/bwdkcprf.P_
CROSS SITE S	149.24.65.77	11-SEP-2008 17:18:15	1	(1)PIDM=548 ID=31 /s10b80/bwdkpprf.P_
CROSS SITE S	149.24.65.77	11-SEP-2008 17:18:15	1	(1)PIDM=548 ID=31 /s10b80/bwdkpprf.P_
CROSS SITE S	149.24.65.77	11-SEP-2008 17:18:15	1	(1)PIDM=548 ID=31 /s10b80/bwdkpprf.P_
CROSS SITE S	149.24.65.77	11-SEP-2008 17:18:15	1	(1)PIDM=548 ID=311115555 / OAS_PUBLIC / maldevm28.sct.com:8002/s10b80/bwdkpprf.P_
CROSS SITE S	149.24.65.77	11-SEP-2008 17:18:15	1	(1)PIDM=548 ID=311115555 / OAS_PUBLIC / maldevm28.sct.com:8002/s10b80/bwdkpprf.P_
CROSS SITE S	149.24.65.77	11-SEP-2008 17:18:15	1	(1)PIDM=548 ID=311115555 / OAS_PUBLIC / maldevm28.sct.com:8002/s10b80/bwdkpprf.P_
CROSS SITE S	149.24.65.77	11-SEP-2008 17:18:15	1	(1)PIDM=548 ID=311115555 / OAS_PUBLIC / maldevm28.sct.com:8002/s10b80/bwdkpprf.P_
CROSS SITE S	149.24.65.77	11-SEP-2008 17:18:15	1	(1)PIDM=548 ID=311115555 / OAS_PUBLIC / maldevm28.sct.com:8002/s10b80/bwdkpprf.P_
CROSS SITE S	149.24.65.77	11-SEP-2008 17:05:36	1	(1)PIDM=548 ID=311115555 / OAS_PUBLIC / maldevm28.sct.com:8002/s10b80/bwdkpprf.P_
CROSS SITE S	149.24.65.77	11-SEP-2008 17:05:36	1	(1)PIDM=548 ID=311115555 / OAS_PUBLIC / maldevm28.sct.com:8002/s10b80/bwdkpprf.P_
CROSS SITE S	149.24.65.77	11-SEP-2008 17:05:35	1	(1)PIDM=548 ID=311115555 / OAS_PUBLIC / maldevm28.sct.com:8002/s10b80/bwdkpprf.P_
CROSS SITE S	149.24.65.77	11-SEP-2008 17:05:35	1	(1)PIDM=548 ID=311115555 / OAS_PUBLIC / maldevm28.sct.com:8002/s10b80/bwdkpprf.P_
CROSS SITE S	149.24.65.77	11-SEP-2008 17:05:35	1	(1)PIDM=548 ID=311115555 / OAS_PUBLIC / maldevm28.sct.com:8002/s10b80/bwdkpprf.P_
CROSS SITE S	149.24.65.77	11-SEP-2008 17:05:35	1	(1)PIDM=548 ID=311115555 / OAS_PUBLIC / maldevm28.sct.com:8002/s10b80/bwdkpprf.P_
CROSS SITE S	149.24.65.77	11-SEP-2008 17:05:35	1	(1)PIDM=548 ID=311115555 / OAS_PUBLIC / maldevm28.sct.com:8002/s10b80/bwdkpprf.P_

```
(1)PIDM=548 ID=311115555 / OAS_PUBLIC /
maldevm28.sct.com:8002/s10b80/bwdkcprf.
P_Long_Profile?cons_pidm=7&back_url=bwdksrch.
P_Display_Search_Results?back_start_records=1
===> <script>alert("Hi!")</script>
```

Documentation

- Security Technical Reference Manual (TRM) changed to

  Security Administration Handbook

- Available through Customer Support Center Download area - not the normal Documentation area

- 8.x Release Guide contains some security changes

- Security Administration Handbook has full documentation about the Banner General 8.x security and many other improvements to the document

Summary

- Oracle/Banner Security Maintenance GSASECR Changes
  - User – new attributes, tracking and restricting logons
  - Class – added owner and comments
  - Object – added owner and comments
  - Role – added owner and comments, new role ban_default_no_access
  - Profile – audit triggers, password options, last update
- Security Auditing and Audit History form (GSAAUDT)
  - Tables, inquiry forms, triggers
- Documentation
  - New name, new processes, new look

61

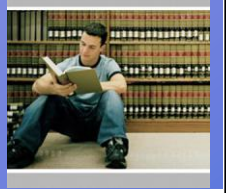
Security part 2

- New Security Level (Group Security)
- Distributed Security (GSADSEC)
- Create Distributed Security User (GSADSUM)
- Miscellaneous security enhancements
- Wednesday, October 20, 4:30 – 5:15

62

Questions and Answers

Thank you!



Thank You!

Les von Holstein
Les.vonHolstein@sungardhe.com