

# Release 12

## Security Recommendations

Chuck Kennedy

Susan Behn

Brian Bent

April 16, 2008

**ORACLE** CERTIFIED ADVANTAGE  
PARTNER

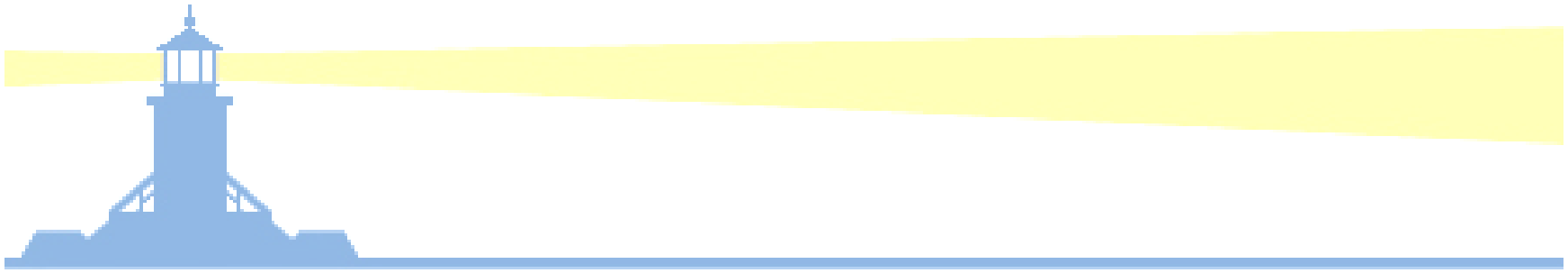


SOLUTION BEACON, LLC  
Real Solutions for the Real World®



# Agenda

- **Presentation (50 minutes)**
  - Who Are You?
  - What Can You Do?
  - What Can You See?
  - What Did You Do?
- **Keeping It Real – Q&A (10 minutes)**
- **More Information**



# Who Are You?





# Who Are You?

- Are You Unique?
- What Keeps You Unique?
- Any Opportunity To Lose Your Uniqueness?





# Generic Application Userids

APPSMGR	IBEGUEST	OP_CUST_CARE_A DMIN	ADSADMIN	OSC (*)
ASGADM (*)	IEXADMIN	OP_SYSADMIN	ADSFWK	OSUSER (*)
ASGUEST	IRC_EMP_GUEST	SYSADMIN (*) (**)	APPSADMIN (*)	OSM_ADMIN (*)
GUEST	IRC_EXT_GUEST	WIZARD	BSC (*)	OSOADMIN
IBE_GUEST	ABM_SYSADMIN	ABM_USER	MOBADM (*)	PRM_ADMIN
AME_INVALID_A PPROVER	IBE_ADMIN	MOBILEADM (*)	MOBDEV (*)	PROFILEOPTION S (*)
	(*) Comes With System Administrator Responsibility	(**) Do Not Recommend Disabling		

- Access with generic userids are NOT recommended
- Release 12 comes seeded with the following application userids
- Strongly recommend changing default passwords!



# Generic Database Userids

- Access with Generic Userids are NOT Recommended
  - Non-Application Schema Database Id's for Release 12 and 10gR2 can have a lot of read/write privileges:

CTXSYS	DBSNMP	MDSYS	ADSADMIN	AD_MONITOR
ANONYMOUS	HTMLDB_PUB	MGDSYS	MOBILEADMI	ODM_MTR
ASGUEST	OLAP_SYS	ORABPEL	OPMOR	ORDPLUGINS
ORDSYS	OUTLN	OWAPUB	ORASSO	ORASSO_PUB
IBE_GUEST	PORTAL_PUB	REPADMIN	SCOTT	TRACESVR
TMSYS	UDDISYS	WCRSYS	WKSYS	WKPROXY

- FNDCPASS has “ALLORACLE” mode to change passwords for all application schemas (as of ATG 11i.PF.H RUP 4)
  - FNDCPASS APPS/xxxxx 0 Y SYSTEM/yyyyy ALLORACLE zzzzz
  - Be careful though – single point of failure with “ALLORACLE”
- Strongly Recommend Changing Default Passwords!

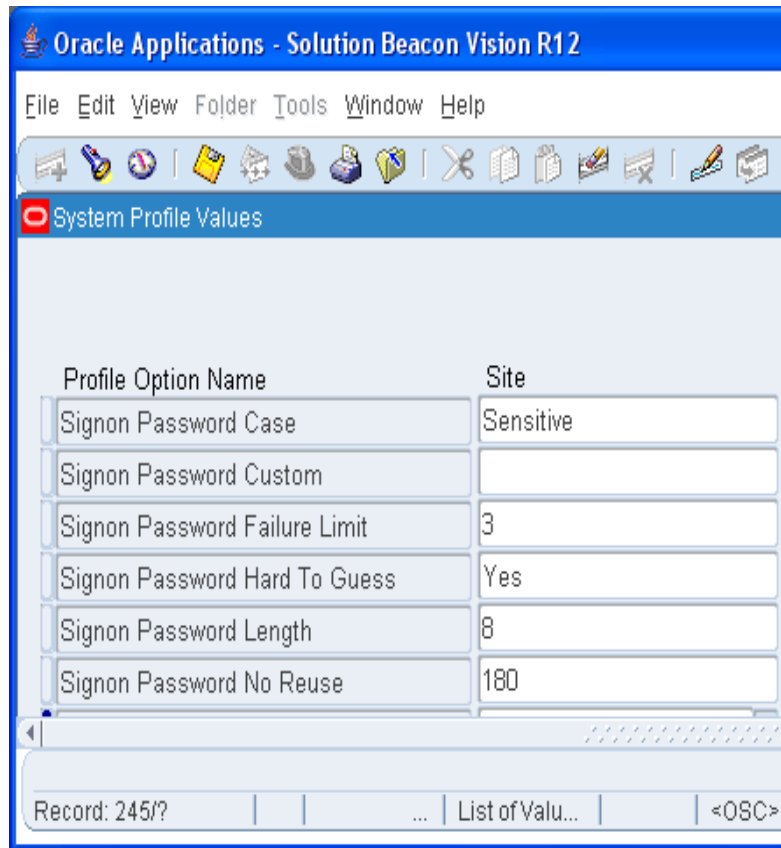




# Network and OS Level Authentication

- **TNSLISTENER**
  - 10g Listeners are “out-of-the-box” secure – local OS authentication
    - As long as the same user that is running the Listener is administering lsnrctl – no password will be solicited.
    - Verify local OS authentication by entering lsnrctl status command
- **REMOTE\_OS\_AUTHENT**
  - Ensure init.ora parameter is set to “false”
  - Prevents bypassing database level authentication
- Use “SUDO” for OS Level Privileged Access
- Restrict Client Access to Database in SQLNET.ora
  - tcp.valid\_node\_checking = YES
  - tcp.invited\_nodes=(I/P#1,I/P#2, I/P#3...)
  - tcp.excluded\_nodes=(I/P#1,I/P#2,I/P#3...)

# Application Passwords



Oracle Applications - Solution Beacon Vision R12

File Edit View Folder Tools Window Help

System Profile Values

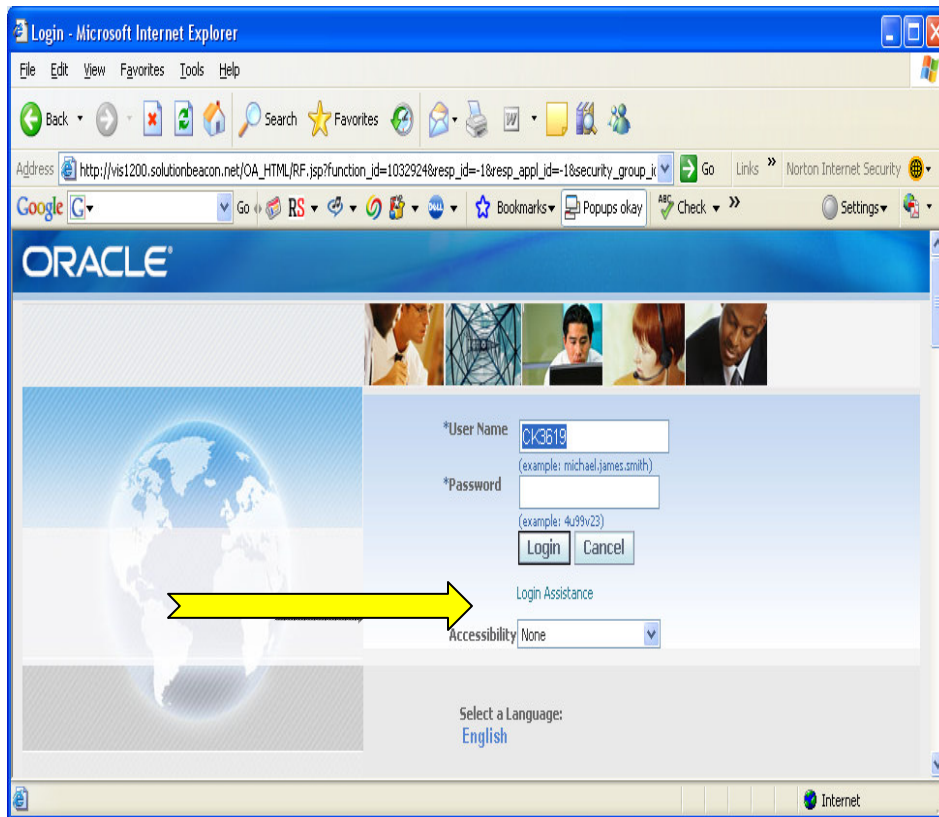
Profile Option Name	Site
Signon Password Case	Sensitive
Signon Password Custom	
Signon Password Failure Limit	3
Signon Password Hard To Guess	Yes
Signon Password Length	8
Signon Password No Reuse	180

Record: 245/? | ... | List of Valu... | <OSC>

- E-Business Suite Password Profile Options
  - Signon Password
    - Requires Case Sensitivity for Password Construction
  - Signon Password Custom
    - Allows Java Class to Be Specified for Custom Rule(s)
  - Signon Password Failure Limit
    - Max # of Logon Attempts with Wrong Password
  - Signon Password Hard To Guess
    - Must contain at least one letter and one number
    - Must not contain the application userid
    - Must not contain any consecutively repeating characters
  - Signon Password Length
    - Minimum length restriction
  - Signon Password No Reuse
    - Number of days before a password can be used again



# E-Business Suite Release 12 Login Assistance



- E-Business Suite Release 12 provides assistance for forgotten passwords
- Password Hints
- Forgotten Userid Hints
- Controlled by profile option “Local Login Mask”





# Database Passwords

Database Password Mgmt Policies	Recommendation
FAILED_LOGIN_ATTEMPTS	3
PASSWORD_REUSE_TIME	180
PASSWORD_REUSE_MAX	15
PASSWORD_GRACE_TIME	10
PASSWORD_VERIFY_FUNCTION	function_name
PASSWORD_LOCK_TIME	.0416

- Applies to database accounts only
- Potential conflict with E-Business Suite Release 12 applications
- Passwords aged to perpetuity is NOT recommended under any circumstance



# Password Management Tips

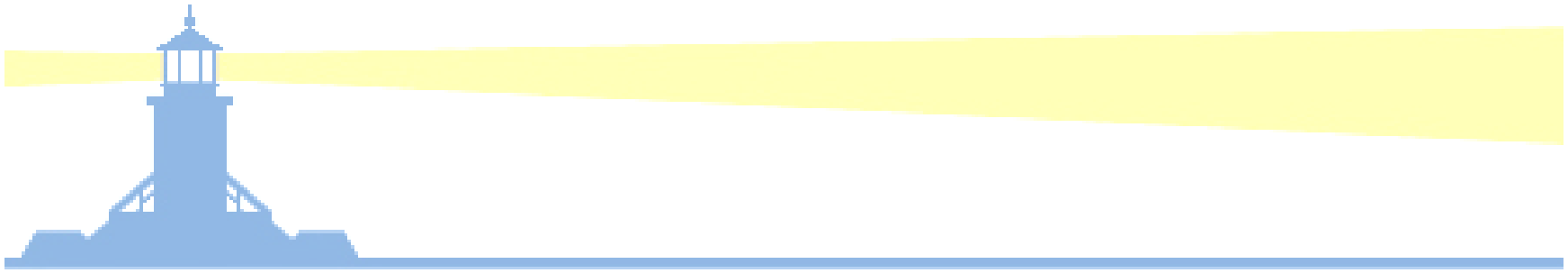
- Desktop screen savers
- Deploy the hard 'guessability' factor
  - Avoid:
    - Family member first names
    - City/State names
    - Calendar dates (birthdates in particular)
  - Consider:
    - Words from another language
    - Combine letters and numbers, use mixed case
- Who's using that yellow sticky note under the keyboard?



# Application Timeout Parameters

- Application timeout helps protect your identity when you're away from your desk
- Persistent application sessions can be taken over by someone else
- Profile options work to establish maximum allowable time for E-Business Suite Release 12 application sessions

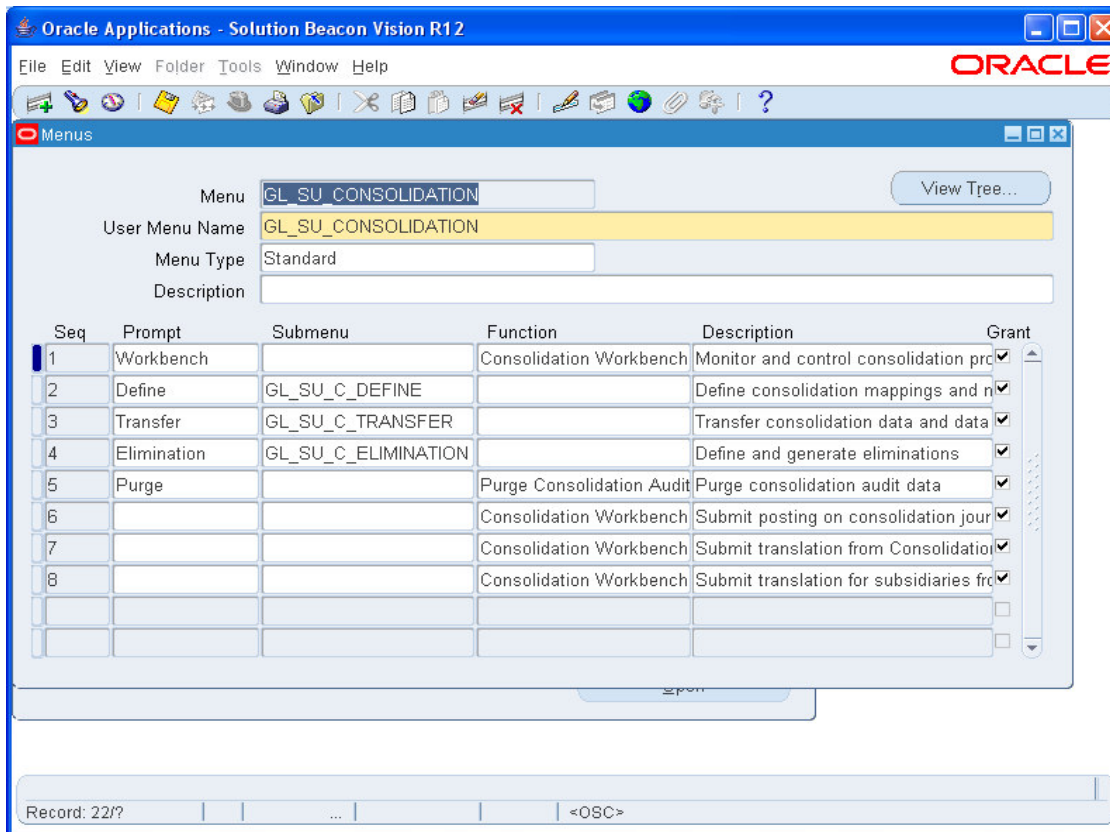
Application Timeout Profile Options	Recommendation
ICX: Session Timeout	30 minutes
ICX: Limit Time	4 hours
ICX: Limit Connect	2000
JTF_INACTIVE_TIMEOUT_SESSION	30 minutes



# What Can You Do?



# Application Menus



Oracle Applications - Solution Beacon Vision R12

File Edit View Folder Tools Window Help

ORACLE

Menu:  View Tree...

User Menu Name:

Menu Type:

Description:

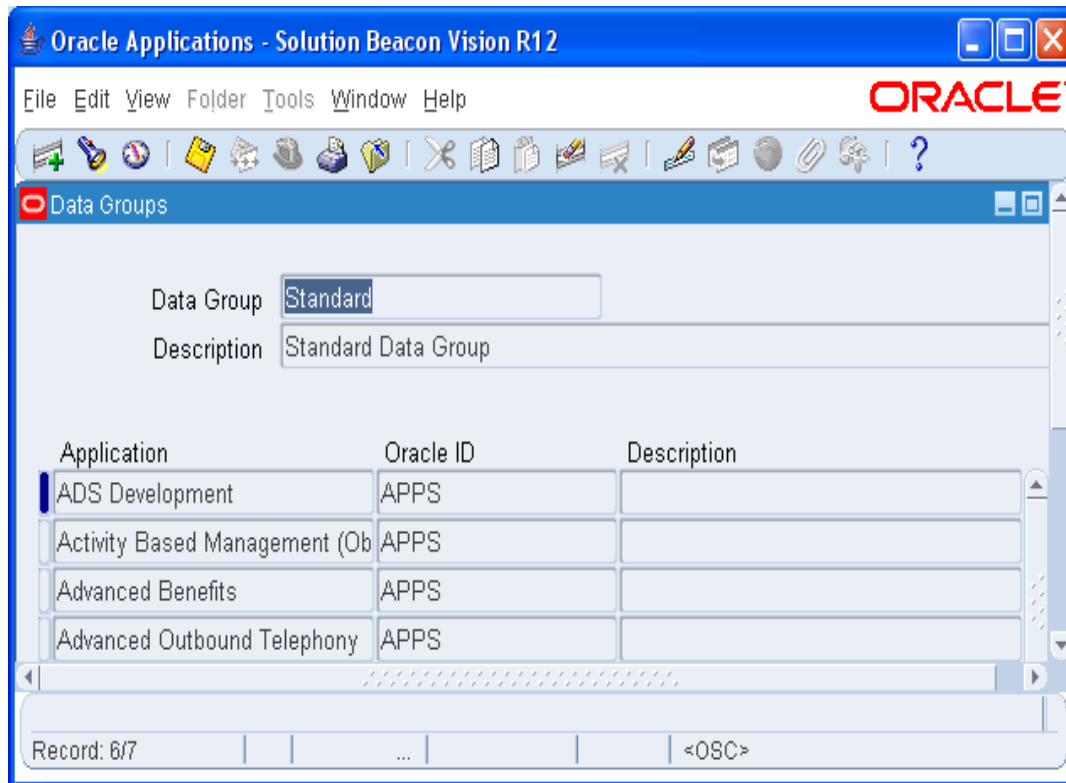
Seq	Prompt	Submenu	Function	Description	Grant
1	Workbench		Consolidation Workbench	Monitor and control consolidation pro	<input checked="" type="checkbox"/>
2	Define	GL_SU_C_DEFINE		Define consolidation mappings and n	<input checked="" type="checkbox"/>
3	Transfer	GL_SU_C_TRANSFER		Transfer consolidation data and data	<input checked="" type="checkbox"/>
4	Elimination	GL_SU_C_ELIMINATION		Define and generate eliminations	<input checked="" type="checkbox"/>
5	Purge		Purge Consolidation Audit	Purge consolidation audit data	<input checked="" type="checkbox"/>
6			Consolidation Workbench	Submit posting on consolidation jour	<input checked="" type="checkbox"/>
7			Consolidation Workbench	Submit translation from Consolidatio	<input checked="" type="checkbox"/>
8			Consolidation Workbench	Submit translation for subsidiaries fro	<input checked="" type="checkbox"/>
					<input type="checkbox"/>
					<input type="checkbox"/>

Record: 22/?

- Application menus bring together a navigable group of functions and submenus to perform a job responsibility
- Oracle provides great privilege with their seeded menus
- Underlying tables FND\_MENUS and FND\_MENU\_ENTRIES are audit candidates
- “Great Privilege” is bad!



# Data Groups



- Specifies available database schemas
- Request Group must align with Data Group
- Backward compatible – Release 12 Oracle Applications Framework does NOT use/reference



# Request Groups

Oracle Applications - Solution Beacon Vision R12

File Edit View Folder Tools Window Help

ORACLE

Request Groups

Group: GL Concurrent Program Group

Application: General Ledger

Code: GL\_CONCURRENT\_PROGRAM\_GROUP

Description: Program group that includes all other GL program groups

Requests

Type	Name	Application
Program	Open Period	General Ledger
Program	General Ledger - (132 Char)	General Ledger
Program	Journals - General(132 Char)	General Ledger
Program	Trial Balance - Additional Segment Detail	General Ledger
Program	Trial Balance	General Ledger
Program	Trial Balance - Detail	General Ledger
Program	Account Analysis - (132 Char)	General Ledger
Program	Program - Delete Journal Import Data	General Ledger

Record: 2/?

<OSC>

- Specifies what can be submitted to the Concurrent Managers which include:
  - Concurrent Programs
  - Concurrent Request Sets
- Request Groups and Data Groups must be in sync



# Application Responsibilities

The screenshot displays the Oracle Applications interface for defining a responsibility. The window title is 'Oracle Applications - Solution Beacon Vision R12'. The menu bar includes 'File', 'Edit', 'View', 'Folder', 'Tools', 'Window', and 'Help'. The 'Responsibilities' form is open, showing the following details:

- Responsibility Name:** General Ledger Super User
- Application:** General Ledger
- Responsibility Key:** GENERAL\_LEDGER\_SUPER\_USER
- Description:** Super User responsibility for Oracle Gen
- Effective Dates:** From 01-JAN-1951, To (empty)
- Available From:** Oracle Applications (selected), Oracle Self Service Web Applications, Oracle Mobile Applications
- Data Group:** Name Standard, Application General Ledger
- Request Group:** Name GL Concurrent Program Group, Application General Ledger
- Menu:** GL\_SUPERUSER
- Web Host Name:** (empty)
- Web Agent Name:** (empty)

Below the form, there are tabs for 'Menu Exclusions', 'Excluded Items', and 'Securing Attributes'. The 'Menu Exclusions' tab is active, showing a table with the following data:

Type	Name	Description
Menu	GL_SU_GIS	

At the bottom of the window, it shows 'Record: 1/?' and '<OSC>'.

- Defines what functions, data and reports a user may access
- Intersection of the following access mechanisms:
  - Menu
  - Data Group
  - Request Group
- Cannot be removed – can only be end-dated.
- Allows for submenus and functions to be excluded.
- Underlying table **FND\_RESPONSIBILITY** should be considered an audit candidate



# Role Based Access Control (RBAC) and Oracle User Management (UMX)

- What is RBAC?
  - MetaLink Doc. ID: 290525.1 “Role Based Access Control (RBAC) is an ANSI standard (ANSI INCITS 359-2004) supported by the National Institute of Standards & Technology (NIST).
  - The RBAC standard supports the mapping of user access control based upon the role that the user plays within the organization rather than upon the user's individual identity.
  - Responsibilities aggregates menus/functions for navigation
  - Roles correlate functions to specific data access
  - Role inheritance reduces user administration
    - (i.e. add function to a role and all assigned users gain access)



# Role Based Access Control (RBAC) and Oracle User Management (UMX)

- Grants
  - Grant specific users access to roles and/or responsibilities
  - Grant specific users to Data Security Policies
- Data Security Policies
  - Regulates specific data accesses – can be for a specific occurrence of data (instance) or a group of data occurrences (instance set)
  - Note – OAF forms do not look at Data Group specified on any given responsibility
- Registration Processes
  - New user registration integrates with AME for approvals
  - Default registration policy is “email”
    - That’s why Self Service userids are usually email format



## Role Based Access Control (RBAC) and Oracle User Management (UMX)

Attribute	Attribute Value
Username Hint	01
Password Hint	02
Cancel Button	04
Forgot Password Link	08
Register Here Link	16
Language Images	32
Sarbanes Oxley Text	64

- New login screen recognizes profile option “Local Login Mask” which drives hints for user login
- Add up the desired attribute values for mask value



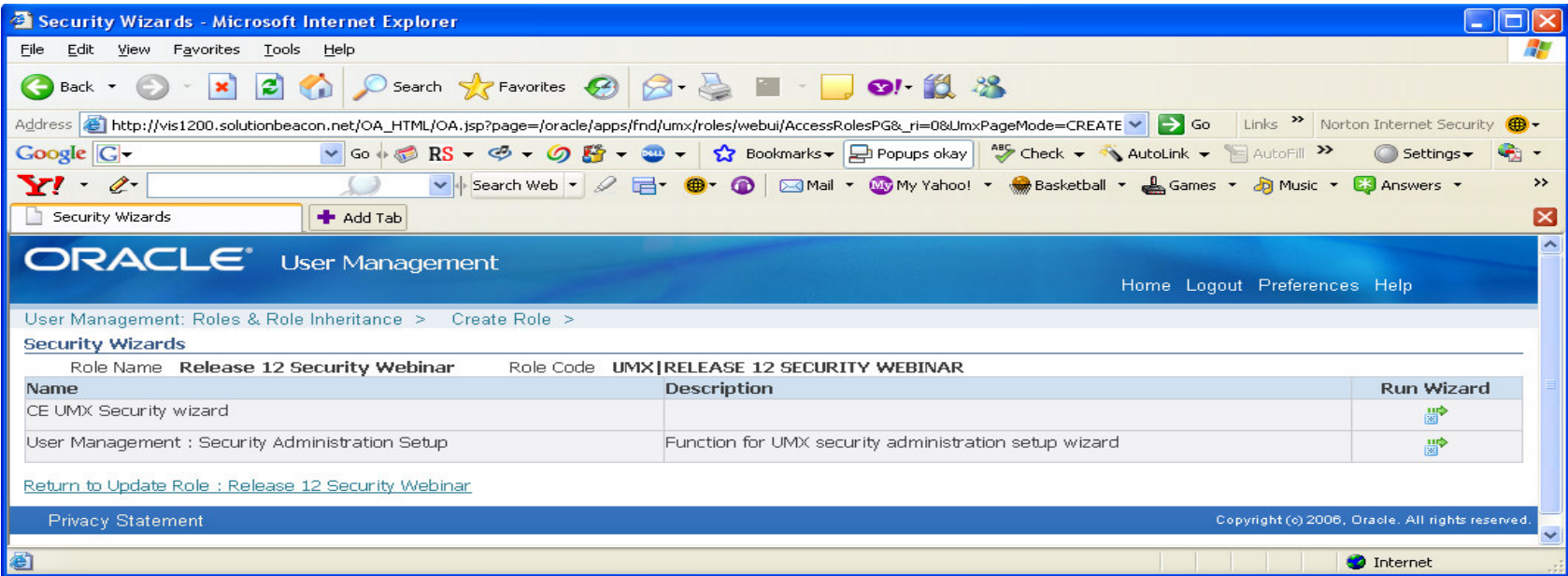
# Role Based Access Control (RBAC) and Oracle User Management (UMX)

- New Security Wizards in Release 12
  - Assist Role Creation – as of 12.0.0 the following are available
    - CE – Cash Management
    - Security Administration Setup (MetaLink Doc. ID: 401463.1)



# Role Based Access Control (RBAC) and Oracle User Management (UMX)

- New Security Wizards in Release 12
  - Assist Role Creation – as of 12.0.0 the following are available
    - CE – Cash Management
    - Security Administration Setup (MetaLink Doc. ID: 401463.1)





# Multi-Org Access Control - MOAC

- Profile Value
- MO: Security Profile
- MO: Default Operating Unit
- MO: Operating Unit

Global Security Profile

Name: **Global Computers**

View Employees: **All**

View Contingent Workers: **All**

View Applicants: **All**

View Contacts: **All**

View Candidates: **All**

View All Records

Allow Granted Users

Restrict on Individual Assignments

Organization Security | Supervisor Security | Miscellaneous Security | Custom Security | Static Lists

Security Type: **Secure organizations by organization hierarchy and/or organization list**

Organization Hierarchy: \_\_\_\_\_

Specify Top Organization: \_\_\_\_\_

Use the Organization on the User's Assignment(s) as the Top Organization

Include Top Organization  Exclude Business Groups

Classification	Organization Name	Include	Exclude
Operating Unit	Vision Operations	<input type="radio"/>	<input type="radio"/>
Operating Unit	Vision Communications (USA)	<input type="radio"/>	<input type="radio"/>
		<input type="radio"/>	<input type="radio"/>
		<input type="radio"/>	<input type="radio"/>





# Oracle 10g Database Level

- Don't forget about your database ids!
  - Can Unique (non-generic) id's Access Base Application Tables?
  - What can they do? Any of these privileges?
    - ALTER
    - CREATE
    - DROP
    - BECOME USER
    - UPDATE
    - EXECUTE
    - LOCK
    - INSERT
  - Examine the privileges very carefully!
    - DBA\_USERS
    - DBA\_SYS\_PRIVS
    - DBA\_ROLE\_PRIVS
    - DBA\_TAB\_PRIVS
  - Beware inheritance – it's usually a bad thing!





- Do you know where your files have been?
  - Are OS file permissions ok?

<code>\$ORACLE_HOME/bin</code>	751 or less
All Other <code>\$ORACLE_HOME</code>	750 or less
<code>Listener.ora</code> and <code>SQLNET.ora</code>	600 or less
<code>TNSNAMES.ora</code>	644 or less

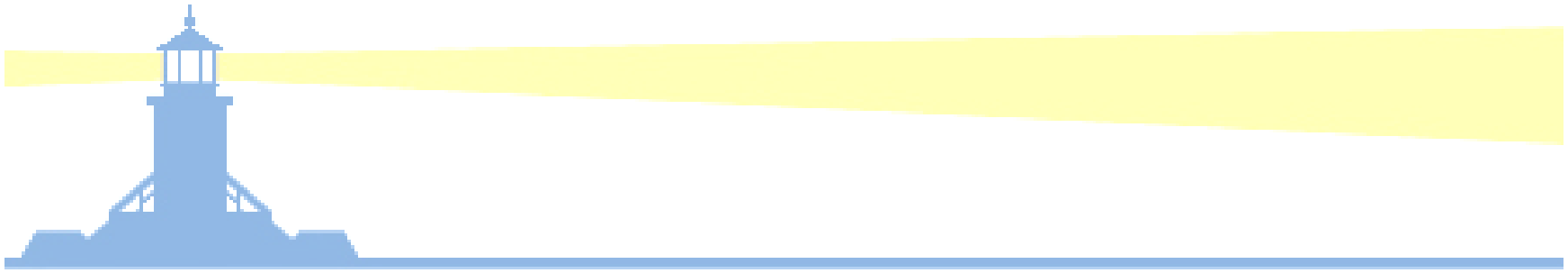
- What about ownership? DBA? SYSTEM? Someone else?
- Don't forget to check `UTL_FILE_DIR` directories in `INIT.ORA`
  - Target directory of \* could be hazardous



# Some Forms Accept SQL!

- Watch Out for Forms That Accept SQL Statements!

FNDCPMCP	Define Concurrent Programs		FNDCPMPE	Define Concurrent Executables
ALRALERT	Define Alerts		PERWSSCP	Security Profile
FNDCPMPE	Descriptive Flexs		FNDFFMVS	Value Sets
FNDPOMPO	Profile Options		FNDSCDDG	Data Groups
FNDSCMOU	Oracle ID		PSBSTPTY	Attribute Types
MSDCSDFN	MSD Definitions		MSDCSDFA	MSD Definitions
MSDAUDIT	MSD Audit		JTFRSDGR	JTF Groups
JTFBRWKB	BRM Rules		OEXPCFVT	OE Constraints
OEXDEFWK	OE Rules Defn		JTFTKOBT	JTF Objects
JTFGRDMD	JTF Datasources		JTFGDIAG	JTF Datasources
JTFGANTT	JTF Gantt		QPXPRFOR	Price Formulas
QPXPTMAP	Attr Sourcing		GMAWFPCL	Procedure Defn



# What Can You See?



# Data Obfuscation

- Obfuscate, Obfuscate, Obfuscate!
  - Non-Production Environments
    - Bank Accounts
    - Credit Card Numbers
    - Payroll and HR data
    - SSN's
    - Employee Age, Phone Numbers, Gender
    - Payroll Deductions, especially medical
    - Employee Vendors (Expense statements)
    - Watch Descriptive Flexfields
      - Especially Payables to GL journals (employee expense statements)
  - Make it Part of Non-Production Environment Delivery
  - Consider Intended Use of the Environment
  - Watch Offshore Elements on Major Projects
  - <http://www.solutionbeacon.com/security>



# Forms and OAF Personalizations

- OAF Personalizations are controlled by the following profile options:
  - Disable Self-Service Personal
  - FND: Personalization Region Link Enabled
  - Personalize Self-Service Defn
- Personalization Page will appear and then can “render” columns hidden to the form for sensitive data columns
- Forms Personalizations are accessed through
  - Help/Diagnostics/Custom Code/Personalize
  - Must have APPS id password to perform
  - Must have knowledge of underlying form, it’s regions and blocks
  - Event code is inserted to the personalization which can serve to hide sensitive data columns



# What Can Be Done for Production?

- What About Your Production Environment?
- Do You Know What EBS Data is Sensitive To You?
- Review the following in light of sensitive EBS data:
  - Application Responsibilities
  - Database Read Roles
  - Database System Privileges
  - Database Role Privileges
  - Database Tab Privileges
- UTL\_FILE\_DIR Directories in INIT.ora
  - Make sure “\*” isn’t a valid directory



# What Can Be Done for Production?

- Don't Forget About Your Temp and Work Tables!
- How about Discoverer EUL? Or B.O. Universes?
- Watch the Flat Files Extracted for Outbound Interfaces
- Understand where Inbound Flat Files Come to Rest
- Create Separate Database Read Roles for Sensitive Data
  - Require Incremental Business Process Owner Approval
- Make Sure Read Access Locked Down for SYS.LINK\$



# Oracle Payments Bank Accounts

- Encryption is available and recommended for bank account information
- IBY\_BANKACCT should be considered an audit candidate

The screenshot shows the Oracle SQL Developer interface. The main window displays the following SQL query:

```
select bankaccountid,  
routingno,  
finame,  
branchname,  
account_holder_name  
from apps.iby_bankacct;
```

The Results pane shows the following data:

BANKACCOUNTID	ROUTINGNO	FINAME	BRANCHNAME	ACCOUNT HOLDER NAME
1 MTizNDU2Nzg5MQ==	NDExMTExMTExMTExMTExMTE=	Bank of America	Belmont	Sm9obiBTbW0aA==
2 MTizMTI0MzQ1	MTizNjczMjM0MQ==	Bank of America	Belmont	QnVzaW5lc3MgV29ybGQ=
3 MTizNDU2NTEyMQ==	MTizMTI1NDY3OAA==	Bank of America	Belmont	QUmgTmV0d29ya3M=
4 MDEyMzExMjMyMzE=	MTizMjQzNTQyMzI=	Bank of America	Burlingame	QVQmVCBVbml2ZXJzYWwGQ2FyZA==
5 MjMxMjMxMjMzMQ==	MTg5ODISMwNw==	Bank of America	France	QS5DLIBOXR3b3Jrcw==
6 NTizMjMxMjMx	MzQ1ODkxMjEyMw==	Bank of America	Redwood City	Q29tCHV0ZXIglU2VydmljZSBhbmQgUmVudGFs

The interface also shows a menu bar, a toolbar, and a status bar at the bottom indicating "All Rows Fetched: 11" and "Line 1 Column 1 Insert Windows: CR/... Editing".

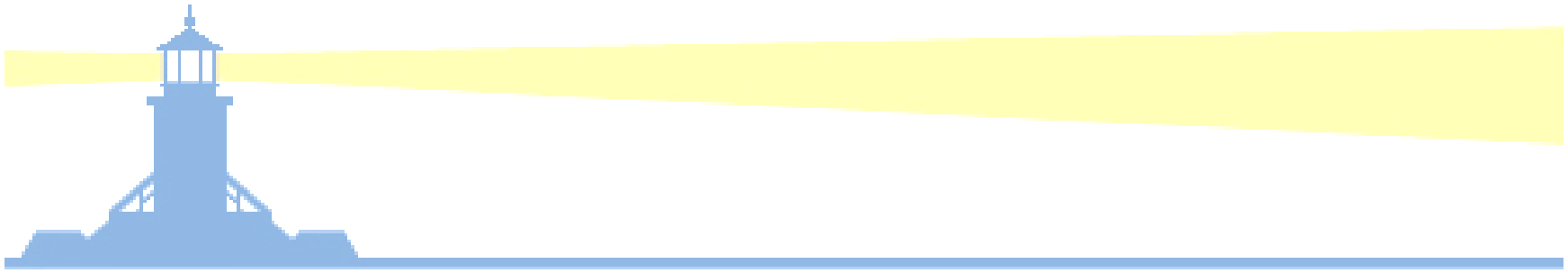






# Oracle Payments Credit Card Numbers

- Encryption is available and recommended for credit card numbers
- IBY\_CREDITCARD should be considered an audit candidate



# What Did You Do?



# Application Level Auditing

- Application Level Auditing
  - Profile Options
    - Sign-On: Audit Level (recommended to be set to FORM at the site level)
    - AuditTrail: Activate
  - Audit Reports
    - Signon Audit Concurrent Requests
    - Signon Audit Forms
    - Signon Audit Responsibilities
    - Signon Unsuccessful Logins
    - Signon Audit Users
  - Recommend that audit reports be reviewed at least quarterly and evidence of review filed away as audit artifacts
  - Recommend more frequent audits for sensitive data



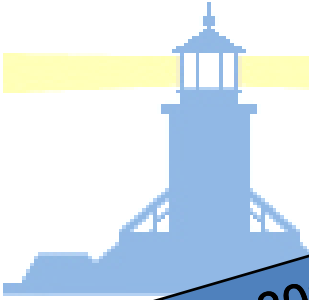
# Database Level Auditing

- Database Level Auditing – SYS.DBA\_AUDIT\_TRAIL
  - Static Tables
  - Test it Out First!
  - Include Key Application Tables Based on Installed Apps
    - (i.e. PER\_ALL\_PEOPLE\_F, IBY\_BANKACCT,...)
  - Include Key FND Tables
  - Don't Forget to Audit the Audit Tables
  - Include Update Activity
  - Include Trusted Accounts
  - Make sure output is readable and that exceptions can be readily identified
  - List of audit candidate tables for Release 12 Applications will be placed on <http://www.solutionbeacon.com/security>



# References

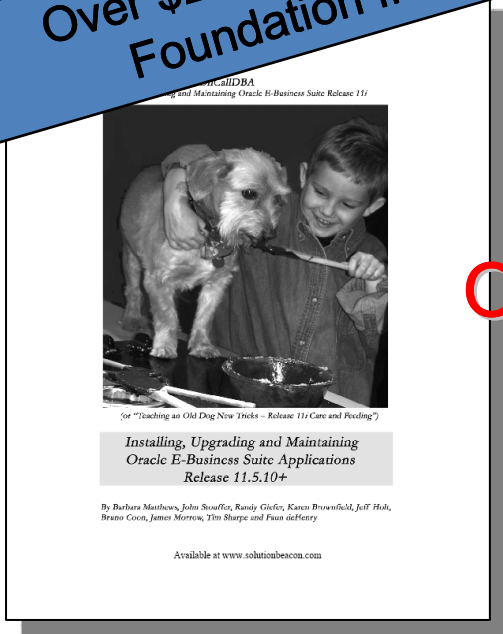
- Better Release 11/Security in 3 Days – Keeping The Bad Guys Away (Part II) – Randy Giefer, Solution Beacon - Collaborate 07
- Application Security – What Are My Options – Susan Behn, Solution Beacon – Collaborate 07
- MetaLink Doc. ID: 189367.1 – Best Practices for Securing Oracle E-Business Suite Release 12
- Solution Beacon Security Pocket Guide
- MetaLink Doc. ID: 260986.1 – Setting Listener Passwords with 10g Listener
- MetaLink Doc. ID: 385445.1 – Oracle Applications Framework Profile Options for Release 12



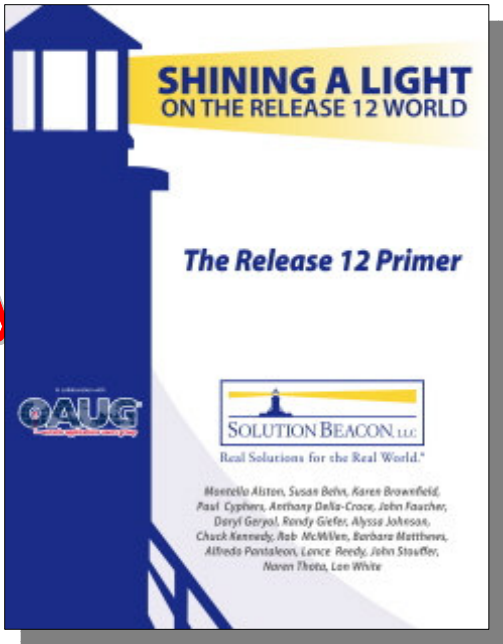
Over \$24,800 donated to the Solution Beacon Foundation from the sale of our books!

# Got Oracle? Get the Books!

Order Your Copy Today



Installing, Upgrading and Maintaining Oracle E-Business Suite Applications 11.5.10.2+



The Release 12 Primer – Shining a Light on the Release 12 World

Available at [www.solutionbeacon.com](http://www.solutionbeacon.com)





# Oracle Applications Users Group (OAUG)

- THE world's largest knowledgebase for Oracle Applications users
- Networking opportunities with over 118,000 members worldwide
- Access to over 50,000 white papers in the online OAUG Conference Paper Database
- FREE online training every Tuesday, Wednesday and Thursday for OAUG members





# Questions and Answers

Thank You!

Chuck Kennedy

[ckennedy@solutionbeacon.com](mailto:ckennedy@solutionbeacon.com)

Susan Behn

[sbehn@solutionbeacon.com](mailto:sbehn@solutionbeacon.com)

Brian Bent

[bbent@solutionbeacon.com](mailto:bbent@solutionbeacon.com)

[www.solutionbeacon.com](http://www.solutionbeacon.com)

*Real Solutions for the Real World*<sup>®</sup>



Copyright 2008 Solution Beacon, LLC All Rights Reserved Any other commercial product names herein are trademark, registered trademarks or service marks of their respective owners.

