INTEGRIGY

Oracle Business Intelligence Enterprise Edition (OBIEE)

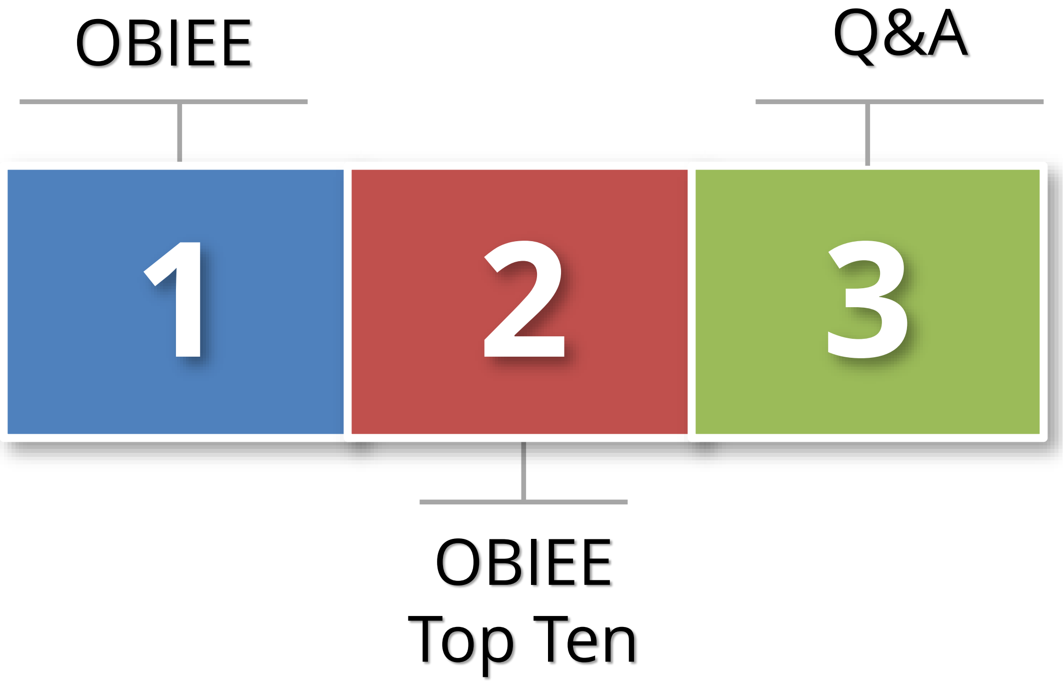
Security Top Ten

June 18, 2014

Michael Miller
Chief Security Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

Agenda

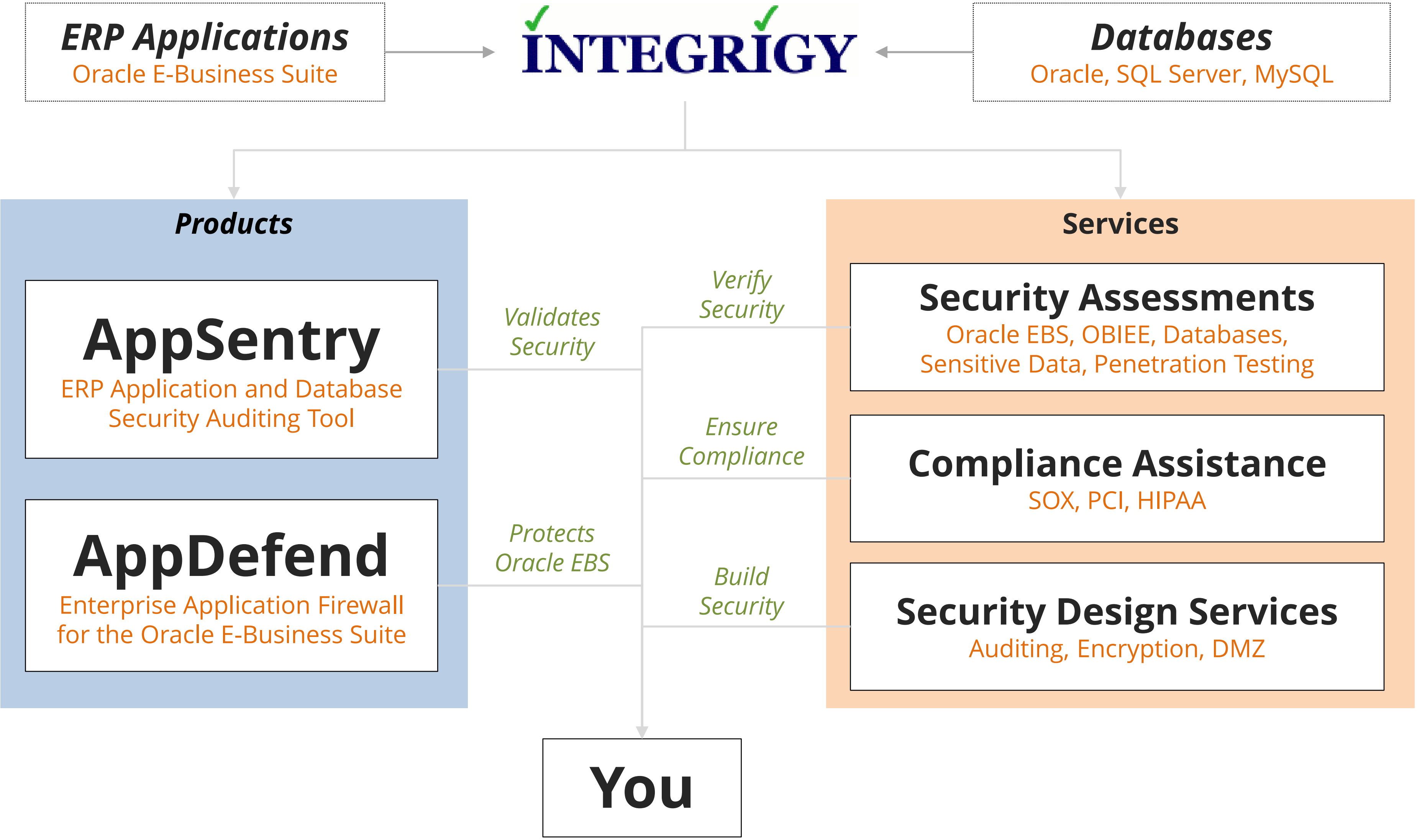


1 OBIEE

2 OBIEE Top Ten

3 Q&A

About Integrigy



ERP Applications
Oracle E-Business Suite

INTEGRIGY

Databases
Oracle, SQL Server, MySQL

Products

AppSentry
ERP Application and Database Security Auditing Tool

AppDefend
Enterprise Application Firewall for the Oracle E-Business Suite

Validates Security

Protects Oracle EBS

Verify Security

Ensure Compliance

Build Security

Services

Security Assessments
Oracle EBS, OBIEE, Databases, Sensitive Data, Penetration Testing

Compliance Assistance
SOX, PCI, HIPAA

Security Design Services
Auditing, Encryption, DMZ

You

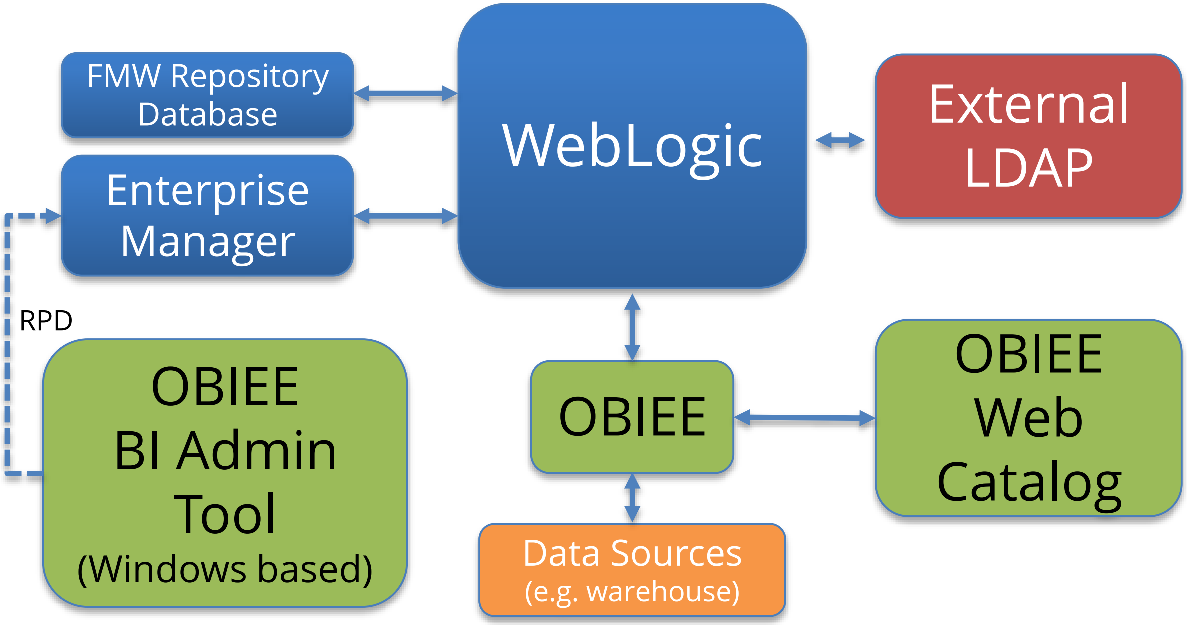
Agenda

1 OBIEE

2 OBIEE Top Ten

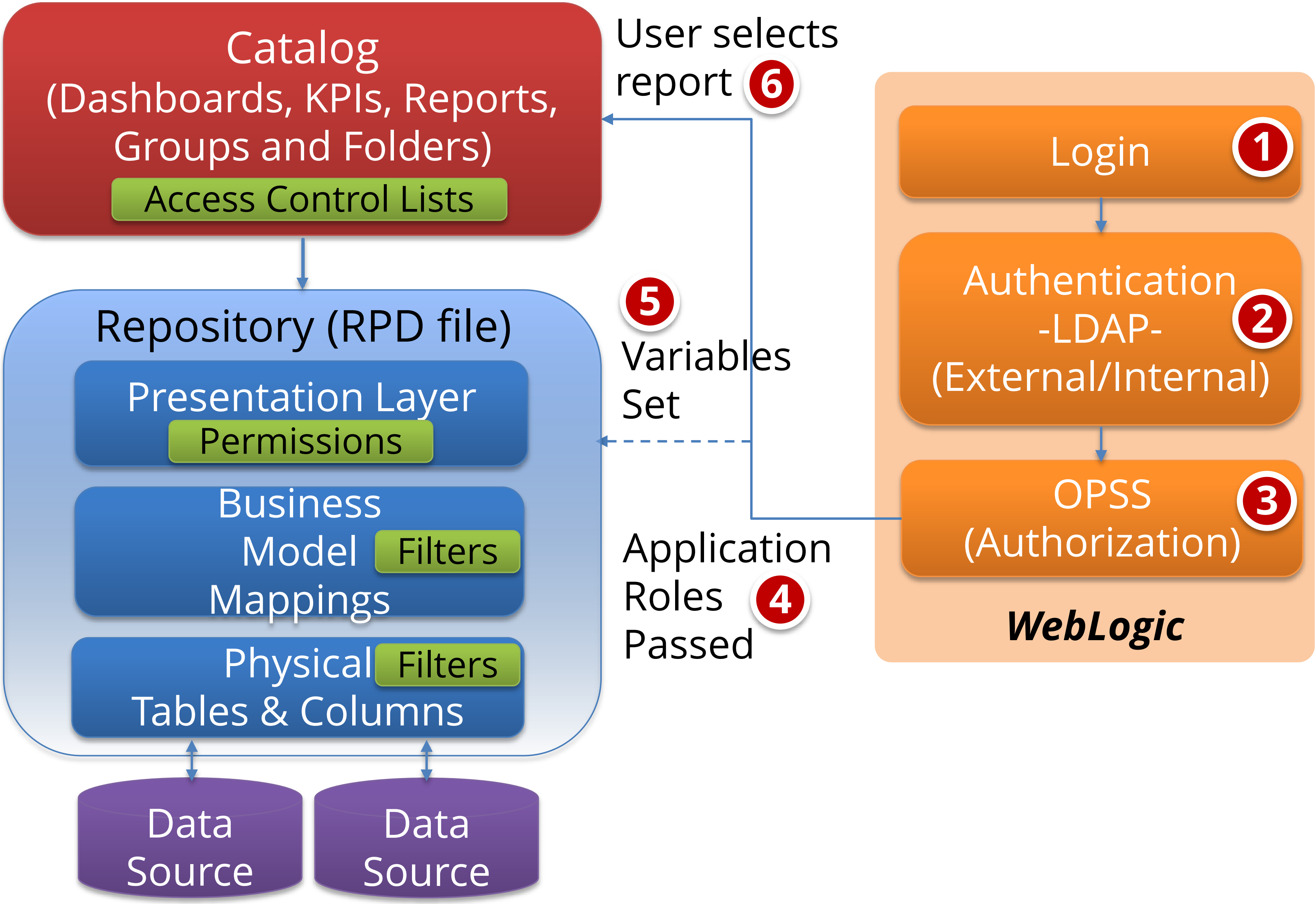
3 Q&A

OBIEE Security Examined



Size of box proportionate to component's impact on security

OBIEE Security



Agenda

OBIEE

Q&A

1

2

3

OBIEE
Top Ten

Top 10 OBIEE Security Vulnerabilities

1. Patching Policies and Procedures
2. Metadata database security
3. Key accounts not secured
4. RPD security
5. Weak overall security
6. Sensitive data not protected
7. Direct SQL access allowed
8. Write-Back enabled
9. Go URL and SQL access
10. No Usage Tracking

Patch Levels

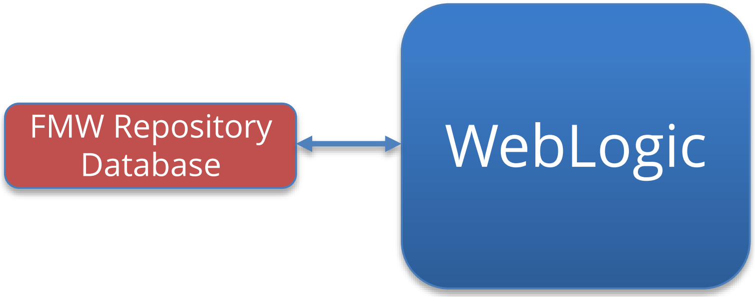
- **OBIEE 11.1.1.6.x end-of-life 2-April-2014**
  - Sustaining support

- **Recommend**
  - Upgrade to OBIEE 11.1.1.7.x

Metadata Database Security

- **Metadata repository database required for each Fusion Middleware product**
  - OBIEE schemas: BIPLATFORM, MDS

- **Recommendations**
  - All standard database security best practices apply
  - Apply CPU patches
  - Do not manually edit or allow access
  - Do not use for Usage Tracking



Key Accounts Not Secured

OS owner of WebLogic	Try not use to ‘weblogic’ or to use welcome1 for a password
OS user that runs WebLogic	Do not use root or a privileged user. Do not hardcode this user’s credentials in startup/shutdown scripts
WebLogic administration user(s)	End-user(s) with full Administration rights to WebLogic – only appropriate people should have access
BI Admin User	Seeded end-user with full Administration rights to OBIEE
BI System User	Seeded account not intended to be used by users. Change password by following the specific Oracle support instructions.
OracleSystemUser	Seeded account created during installation. User name can be change later but need to follow instructions

Act-As and Impersonation

	Impersonate	Act-As
Level of access	Full access	Full or read-only access, on a single user
Users whose identity can be assumed by the proxy user	Any and all users, anytime	Defined list of users
Access method	Construct URL manually	Standard functionality of UI
How to know if being used	No indication given	Both proxy and Target are shown in the UI
Security risk	Credentials exposed in plain text when URL submitted	Little to none

Key Account Recommendations

- **Key accounts**
  - Reconcile as part of full audit of OBIEE
  - Regularly rotate all passwords per Oracle Support
    - Note 1365210.1
    - Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition 11g (E10543-08) – Appendix C Troubleshooting Security in Oracle Business Intelligence

- **Act-As and Impersonation**
  - OBIEE security assessment
  - Set and/or review policy for using
  - Use Act-As if at all possible
  - Implement Usage Tracking
  - Log and Monitor

RPD Security

- **Password to encrypt and open RPD**
  - Protect all meta data and security rules

- **Export to XML option**
  - Connection pool passwords ARE encrypted

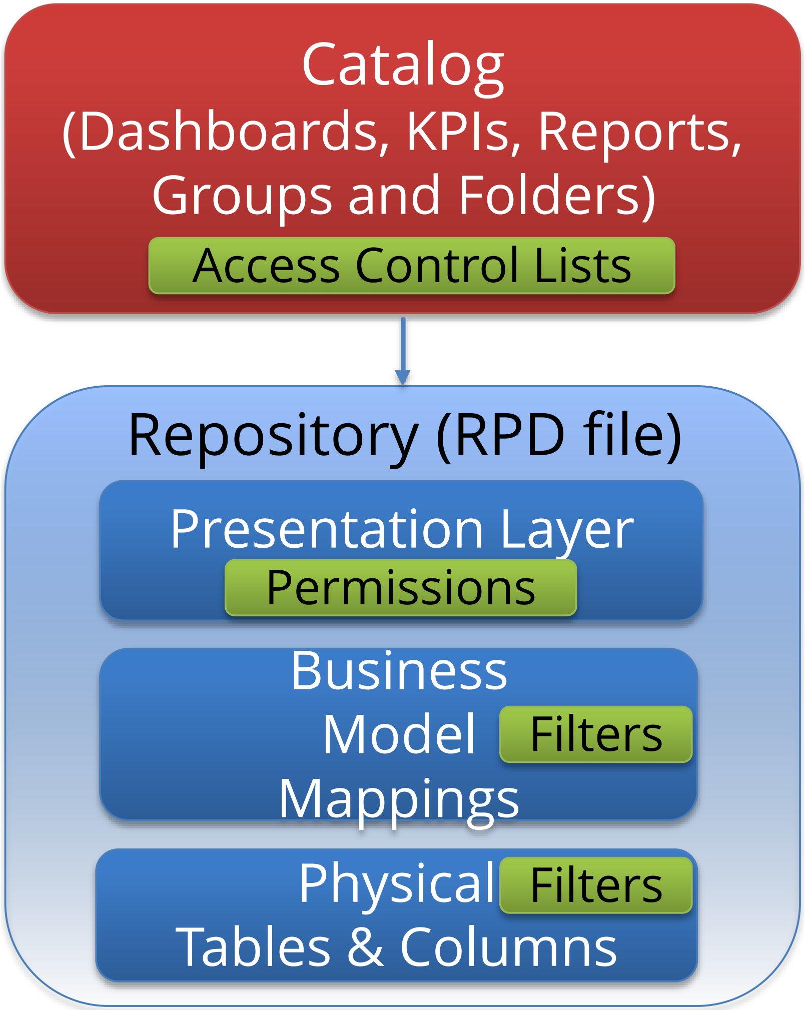
- **Recommendation**
  - Use complex passwords and regularly rotate password
  - Use different password for production
  - Secure access to XML export and put RPD under source code control

Weak Overall OBIEE Security

- **No easy way to reconcile security and authorization. Three security solutions:**
  - Catalog (ACLs)
  - Presentation Layer permission grants
  - Data level filters

- **Commonly find**
  - Rogue groups and users
  - Errors and gaps

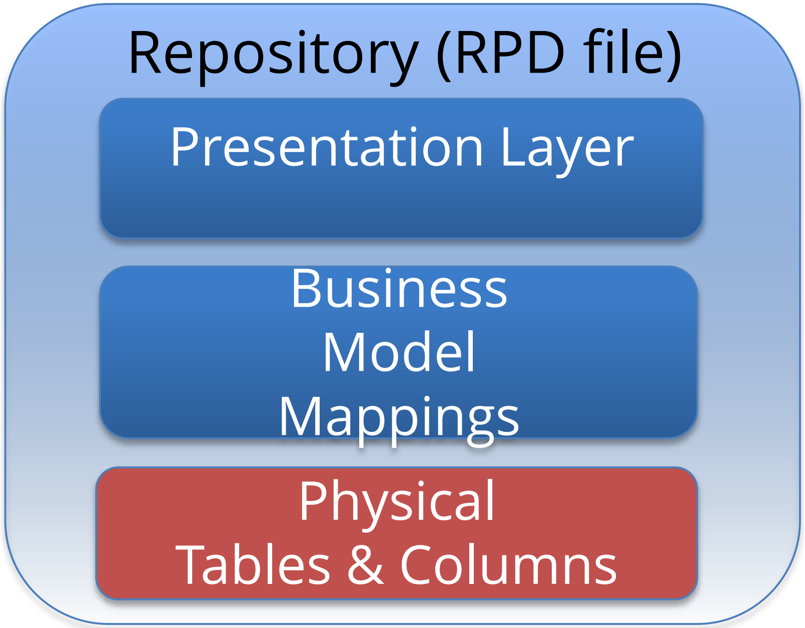
- **Recommendation**
  - OBIEE security assessment



Sensitive Data Not Protected

- **Need to protect if defined in RPD**
  - May not need or realize exists
  - Can be result of prior engagement or accidental metadata import

- **Examples:**
  - Social security, credit cards, bank accounts
  - Salaries, sales and customer records
  - E-Business User table and passwords

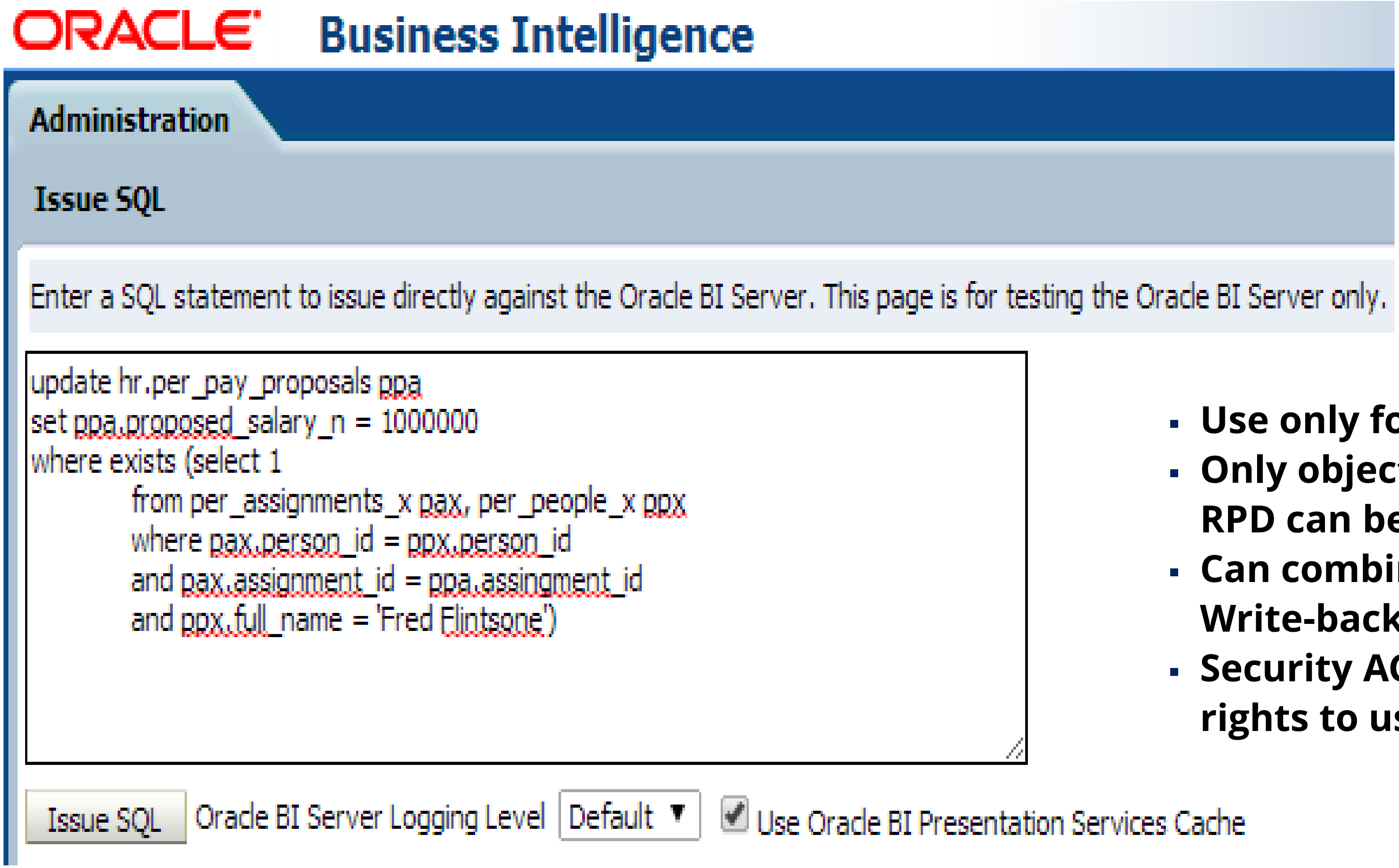


Sensitive Data Not Protected

- **Need to project against**
  - Weak or no security within RPD and catalog
  - Direct SQL access
  - Write Back
  - GO URL SQL access

- **Recommendation**
  - OBIEE security assessment, inclusive of sensitive data discovery

Direct SQL Access And Write-Back



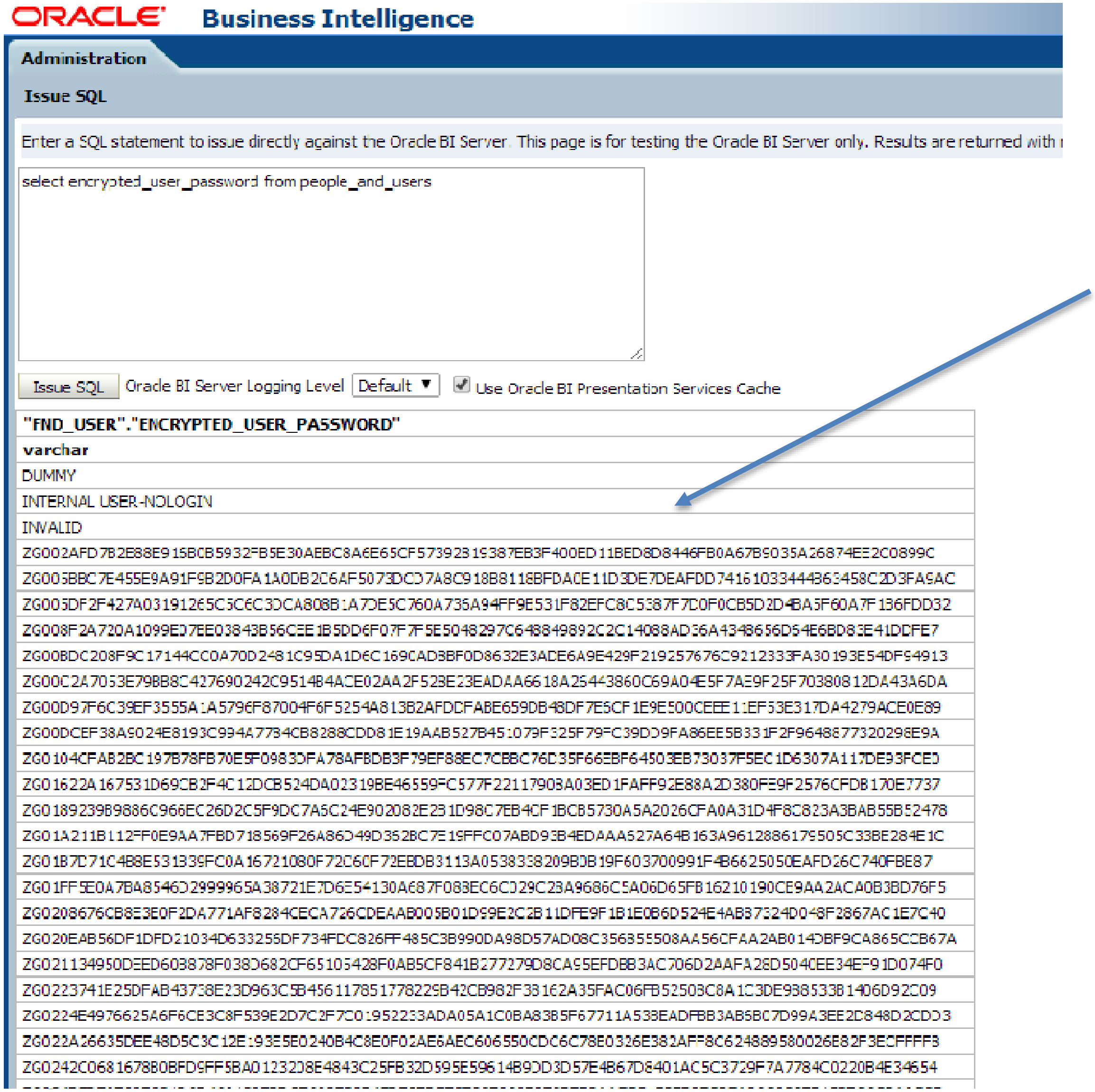
Enter a SQL statement to issue directly against the Oracle BI Server. This page is for testing the Oracle BI Server only.

```
update hr.per_pay_proposals ppa
set ppa.proposed_salary_n = 1000000
where exists (select 1
        from per_assignments_x pax, per_people_x ppx
        where pax.person_id = ppx.person_id
        and pax.assignment_id = ppa.assingment_id
        and ppx.full_name = 'Fred Flintsone')
```

Issue SQL   Oracle BI Server Logging Level   Default ▼   ☑ Use Oracle BI Presentation Services Cache

- Use only for debug
- Only objects in RPD can be queried
- Can combine with Write-back
- Security ACL grants rights to use

Direct SQL Access



Enter a SQL statement to issue directly against the Oracle BI Server. This page is for testing the Oracle BI Server only. Results are returned with

```
select encrypted_user_password from people_and_users
```

Issue SQL | Oracle BI Server Logging Level: Default ▼ | ☑ Use Oracle BI Presentation Services Cache

"FND_USER"."ENCRYPTED_USER_PASSWORD"
varchar
DUMMY
INTERNAL USER-NOLOGIN
INVALID
ZG002AFD7B2E88E915B0B5932FB5E30AEBC8A6E65CF57392319387EB3F400ED11BED8D8446FB0A67B9035A26874EE2C0899C
ZG005BBC7E455E9A91F9B2D0FA1A0DB2C6AF5073DCD7A8C918B8118BFDA0E11D3DE7DEAFDD74161033444363458C2D3FA9AC
ZG005DF2F427A0319126 5C5C6C3DCA808B1A7DE5C760A735A94FF9E531F82EFC8C5387F7D0F0CB5D2D4BA5F60A7F136FDD32
ZG008F2A720A1099ED7EE03843B56CEE1B5DD6F07F7F5E5048297C648849892C2C14088AD36A4348656D54E6BD83E41DDFE7
ZG00BDC208F9C17144CC0A70D2481C95DA1D6C169CAD3BF0D8632E3ADE6A9E429F219257676C9212333FA30193E54DF94913
ZG00C2A7053E79BB8C427690242C9514B4ACE02AA2F523E23EADAA6618A25443860C69A04E5F7AE9F25F70380812DA43A6DA
ZG00D97F6C39EF3555A1A5796F87004F6F5254A813B2AFDCFABE659DB48DF7E5CF1E9E500CEEE11EF53E317DA4279ACE0E89
ZG00DCEF38A9024E8193C994A7734CB8288CDD81E19AAB527B451079F325F79FC39DD9FA86EE5B331F2F9648877320298E9A
ZG0104CFAB2BC197B78FB70E5F0983DFA78AFBDB3F79EF88EC7CBBC76D35F66EBF64503EB73037F5EC1D6307A117DE93FCED
ZG01622A167531D69CB2F4C12DCB524DA02319BE46559FC577F22117903A03ED1FAFF92E88A2D380FE9F2576CFD8170E7737
ZG0189239B9886C966EC26D2C5F9DC7A5C24E902082E231D98C7EB4CF1BCB5730A5A2026CFA0A31D4F8C823A3BAB55B52478
ZG01A211B112FF0E9AA7FBD718569F26A86D49D352BC7E19FFC07ABD93B4EDAAA527A64B163A9612886179505C33BE284E1C
ZG01B7D71C4B8E531339FC0A16721080F72C60F72EBDB3113A0538338209B0B19F603700991F4B6625050EAFD26C740FBE87
ZG01FF5E0A7BA8546D2999965A38721E7D6E54130A687F083EC6CD29C23A9686C5A06D65FB16210190CE9AA2ACA0B3BD76F5
ZG0208676CB8E3E0F2DA771AF8284CECA726CDEAAB005B01D99E2C2B11DFE9F1B1E0B6D524E4AB37324D048F2867AC1E7C40
ZG020EAB56DF1DFD21034D633255DF734FDC826FF485C3B990DA98D57AD08C356355508AA56CFAA2AB014DBF9CA865CCB67A
ZG021134950DEED603878F038D682CF65105428F0AB5CF841B277279D8CA95EFDBB3AC706D2AAFA28D5040EE34EF91D074F0
ZG0223741E25DFAB43738E23D963C5B456117851778229B42CB982F33162A35FAC06FB52503C8A1C3DE938533B1406D92C09
ZG0224E4976625A6F6CE3C8F539E2D7C2F7C01952233ADA05A1C0BA83B5F67711A533EADFBB3AB5B07D99A3EE2D848D2CDD3
ZG022A26635DEE48D5C3C12E193E5E0240B4C8E0F02AE6AEC606550CDC6C78E0326E382AFF8C624889580026E82F3ECFFFF3
ZG0242C0681678B0BFD9FF5BA0123208E4843C25FB32D595E59614B9DD3D57E4B67D8401AC5C3729F7A7784C0220B4E34654

Example of exposing Oracle E-Business Suite Passwords from APPLSYS.FND_USER

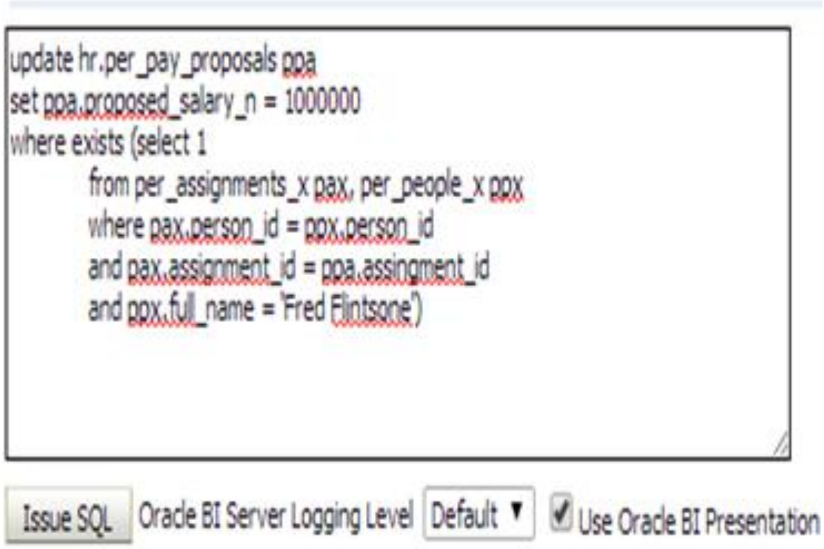
Recommend

- OBIEE logging, monitoring and auditing
- Full audit of Security ACL

Write-Back

- **Connection pools can be defined to allow users to create or update data**
  - Has write back been enabled?
  - What tables allow write-back?
  - Who has security to access?
  - Can they also issue Direct SQL?

- **Recommend**
  - OBIEE security assessment
  - Logging and monitoring



```
update hr.per_pay_proposals ppa
set ppa.proposed_salary_n = 1000000
where exists (select 1
        from per_assignments_x pax, per_people_x ppx
        where pax.person_id = ppx.person_id
        and pax.assignment_id = ppa.assingment_id
        and ppx.full_name = 'Fred Flintsone')
```

Oracle BI Server Logging Level: Default ▼

☑ Use Oracle BI Presentation

Go URL And SQL Access

- **Go URL used to integrate Presentation Services with external portals and applications**
  - Set variables, session attributes

- **Security concerns**
  - Must authenticate first
    - Do you have a PUBLIC user?
  - Bypasses certain parts of security
  - Creates OHS (Apache) log entries
  - Can Issue SQL

Go URL & SQL Access

Authenticate

http://<host>:<port>/analytics/saw.dll?GO&NQUser=weblogic&NQPassword=Password1

Issue SQL

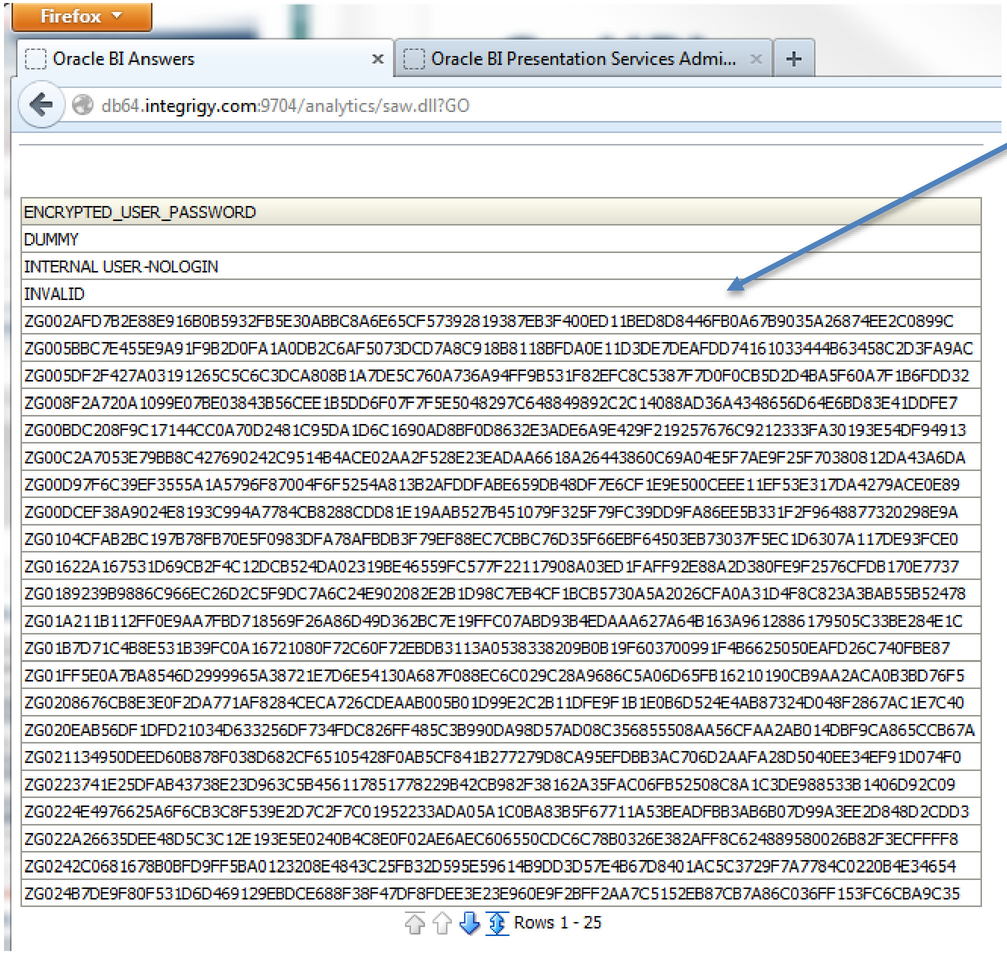
http://<host>:<port>/analytics/saw.dll?Go&SQL=select+thecolumn+from+subject_area

http://<host>:<port>/analytics/saw.dll?Go&SQL=select+person+salary+from+hr_salary_info

http://<host>:<port>/analytics/saw.dll?Go&SQL=select+encrypted_user_password+from+people_and_users

Go URL SQL Access

http://<host>:<port>/analytics/saw.dll?GO&NQUser=integrigy_test_1&NQPassword=test1234&SQL=select+encrypted_user_password+from+people_and_users


Firefox
Oracle BI Answers
Oracle BI Presentation Services Admi...
db64.integrigy.com:9704/analytics/saw.dll?GO
Rows 1 - 25

ENCRYPTED_USER_PASSWORD
DUMMY
INTERNAL USER-NOLOGIN
INVALID
ZG002AFD7B2E88E916B0B5932FB5E30ABBC8A6E65CF57392819387EB3F400ED11BED8D8446FB0A67B9035A26874EE2C0899C
ZG005BBC7E455E9A91F9B2D0FA1A0DB2C6AF5073DCD7A8C918B8118BFDA0E11D3DE7DEAFDD7416103344B63458C2D3FA9AC
ZG005DF2F427A03191265C5C6C3DCA808B1A7DE5C760A736A94FF9B531F82EFC8C5387F7D0F0CB5D2D4BA5F60A7F1B6FDD32
ZG008F2A720A1099E07BE03843B56CEE1B5DD6F07F7F5E5048297C648849892C2C14088AD36A4348656D64E6BD83E41DDFE7
ZG00BDC208F9C17144CC0A70D2481C95DA1D6C1690AD8BF0D8632E3ADE6A9E429F219257676C9212333FA30193E54DF94913
ZG00C2A7053E79BB8C427690242C9514B4ACE02AA2F528E23EADAA6618A26443860C69A04E5F7AE9F25F70380812DA43A6DA
ZG00D97F6C39EF3555A1A5796F87004F6F5254A813B2AFDDFABE659DB48DF7E6CF1E9E500CEEE11EF53E317DA4279ACE0E89
ZG00DCEF38A9024E8193C994A7784CB8288CDD81E19AAB527B451079F325F79FC39DD9FA86EE5B331F2F9648877320298E9A
ZG0104CFAB2BC197B78FB70E5F0983DFA78AFBDB3F79EF88EC7CBBC76D35F66EBF64503EB73037F5EC1D6307A117DE93FCE0
ZG01622A167531D69CB2F4C12DCB524DA02319BE46559FC577F22117908A03ED1FAFF92E88A2D380FE9F2576CFDB170E7737
ZG0189239B9886C966EC26D2C5F9DC7A6C24E902082E2B1D98C7EB4CF1BCB5730A5A2026CFA0A31D4F8C823A3BAB55B52478
ZG01A211B112FF0E9AA7FBD718569F26A86D49D362BC7E19FFC07ABD93B4EDAAA627A64B163A9612886179505C33BE284E1C
ZG01B7D71C4B8E531B39FC0A16721080F72C60F72EBDB3113A0538338209B0B19F603700991F4B6625050EAFD26C740FBE87
ZG01FF5E0A7BA8546D2999965A38721E7D6E54130A687F088EC6C029C28A9686C5A06D65FB16210190CB9AA2ACA0B3BD76F5
ZG0208676CB8E3E0F2DA771AF8284CECA726CDEAAB005B01D99E2C2B11DFE9F1B1E0B6D524E4AB87324D048F2867AC1E7C40
ZG020EAB56DF1DFD21034D633256DF734FDC826FF485C3B990DA98D57AD08C356855508AA56CFAA2AB014DBF9CA865CCB67A
ZG021134950DEED60B878F038D682CF65105428F0AB5CF841B277279D8CA95EFDBB3AC706D2AAFA28D5040EE34EF91D074F0
ZG0223741E25DFAB43738E23D963C5B456117851778229B42CB982F38162A35FAC06FB52508C8A1C3DE988533B1406D92C09
ZG0224E4976625A6F6CB3C8F539E2D7C2F7C01952233ADA05A1C0BA83B5F67711A53BEADFBB3AB6B07D99A3EE2D848D2CDD3
ZG022A26635DEE48D5C3C12E193E5E0240B4C8E0F02AE6AEC606550CDC6C78B0326E382AFF8C624889580026B82F3ECFFFF8
ZG0242C0681678B0BFD9FF5BA0123208E4843C25FB32D595E59614B9DD3D57E4B67D8401AC5C3729F7A7784C0220B4E34654
ZG024B7DE9F80F531D6D469129EBDCE688F38F47DF8FDEE3E23E960E9F2BFF2AA7C5152EB87CB7A86C036FF153FC6CBA9C35

This test user <u>CANNOT</u> issue Direct SQL but still can query with Go URL

Being able to see passwords from APPLSYS.FND_USER is a BAD IDEA

Recommend to DISABLE GO URL

No Usage Tracking

- **Oracle provides sample RPD**
  - Manually copy or configure required components into your RPD

- **Reports on changes to**
  - Enterprise manager configuration changes
  - RPD changes
  - Who ran what report when

- **Recommendation**
  - Create new schema. Do not write to metadata schemas: BIPLATFORM or MDS
  - Make part of holistic log and audit solution
    - Integrigy Framework for Logging and Auditing
    - Pass to centralized logging (e.g. Spunk, ArcSight, etc…)

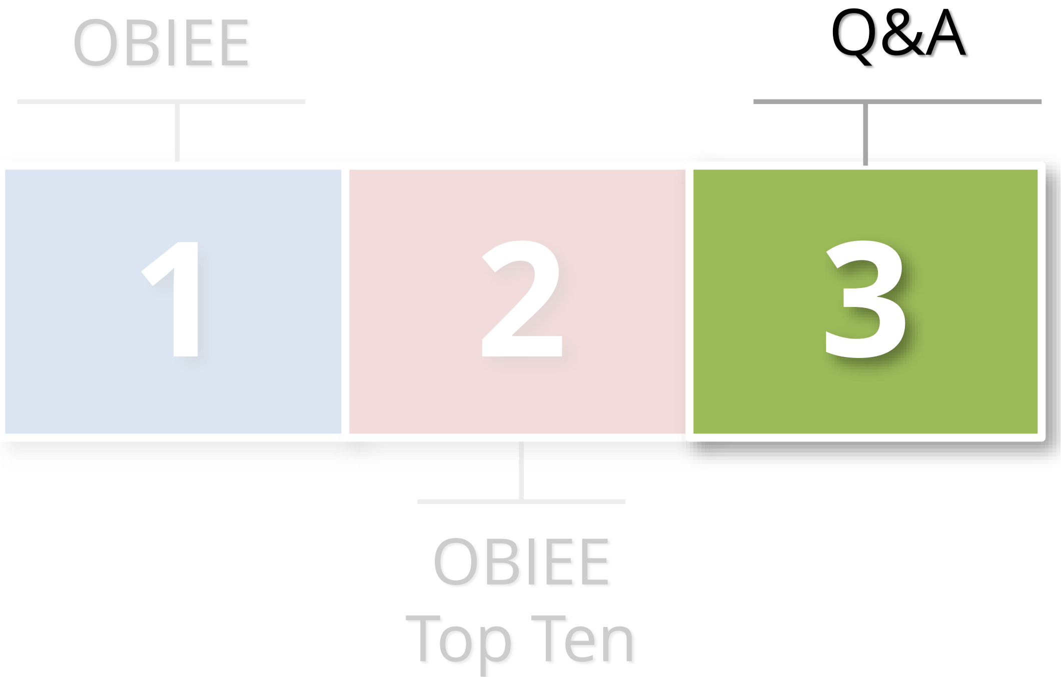
OBIEE Evaluate Function(s)

- **Evaluate function(s) bypass all OBIEE security**
    - Any DML statement may be issued directly against database: select, update and delete

- **Any user can use. Not limited by Security ACL or by WebLogic**
    - Limited only by database privileges of account used in connection pool

- **Recommend to Disable**
    - 11g only

Agenda



1 OBIEE

2 OBIEE Top Ten

3 Q&A

Contact Information

Mike Miller

Chief Security Officer

Integrigy Corporation

web: **www.integrigy.com**

e-mail: **info@integrigy.com**

blog: **integrigy.com/oracle-security-blog**