COLLABORATE14

TECHNOLOGY AND APPLICATIONS FORUM
FOR THE ORACLE COMMUNITY

#C14LV

OBIEE Security Examined

Session ID#: 14366

Michael A. Miller, CISSP-ISSMP
Chief Security Officer
Integrigy Corporation

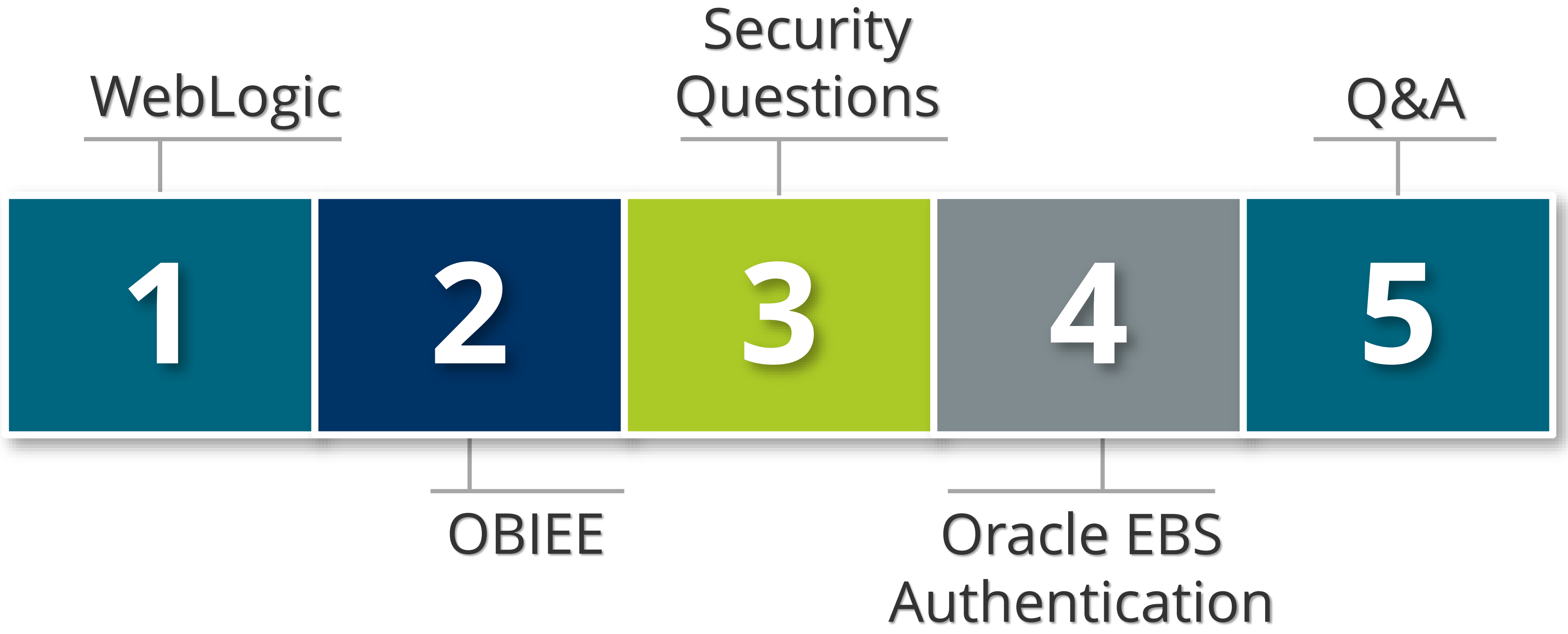
REMINDER

Check in on the
COLLABORATE mobile app

Objectives

- Provide an overview and security risks of the OBIEE 11g technology stack
- Discuss security implications of each layer of the technology stack
- Detail the security of the OBIEE application from authentication through to privileges

Agenda



1 WebLogic

2 OBIEE

3 Security Questions

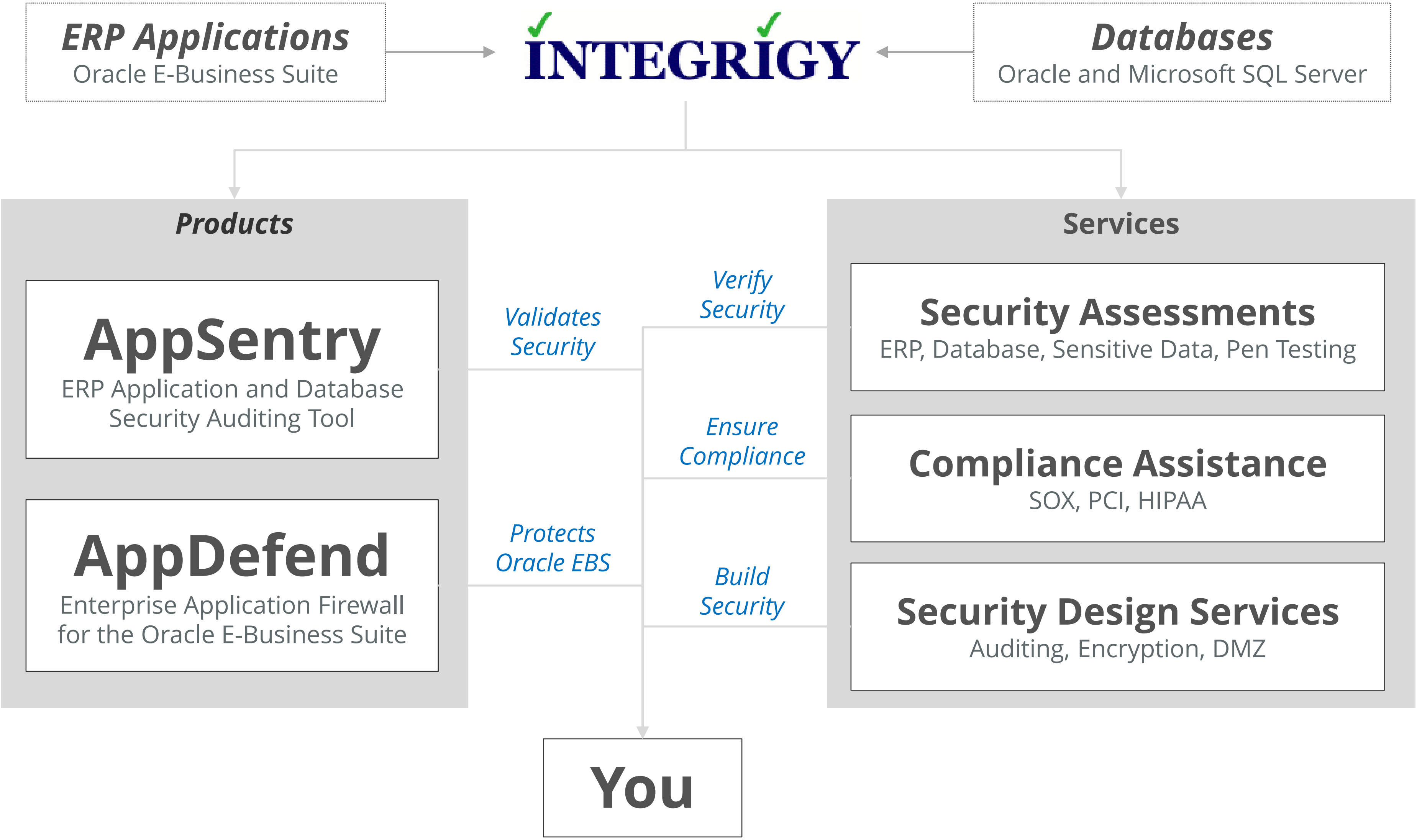
4 Oracle EBS Authentication

5 Q&A

Michael Miller

- 20+ year Oracle technology veteran
  - 17 years Oracle E-Business Suite
  - Held roles of consultant, Director, VP and CSO
- Certified Information Systems Security Professional (CISSP)
- Information Systems Security Management Professional - (ISSMP)
- Cloud Security Alliance Certificate of Cloud Security Knowledge (CCSK)
- ITIL v3 Foundations certified
- Oracle Corporation Customer Advisory Board for Security
  - 2004 – 2007
- FBI Infragard – active member of private sector partnership with FBI

About Integrigy



ERP Applications
Oracle E-Business Suite

INTEGRIGY

Databases
Oracle and Microsoft SQL Server

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

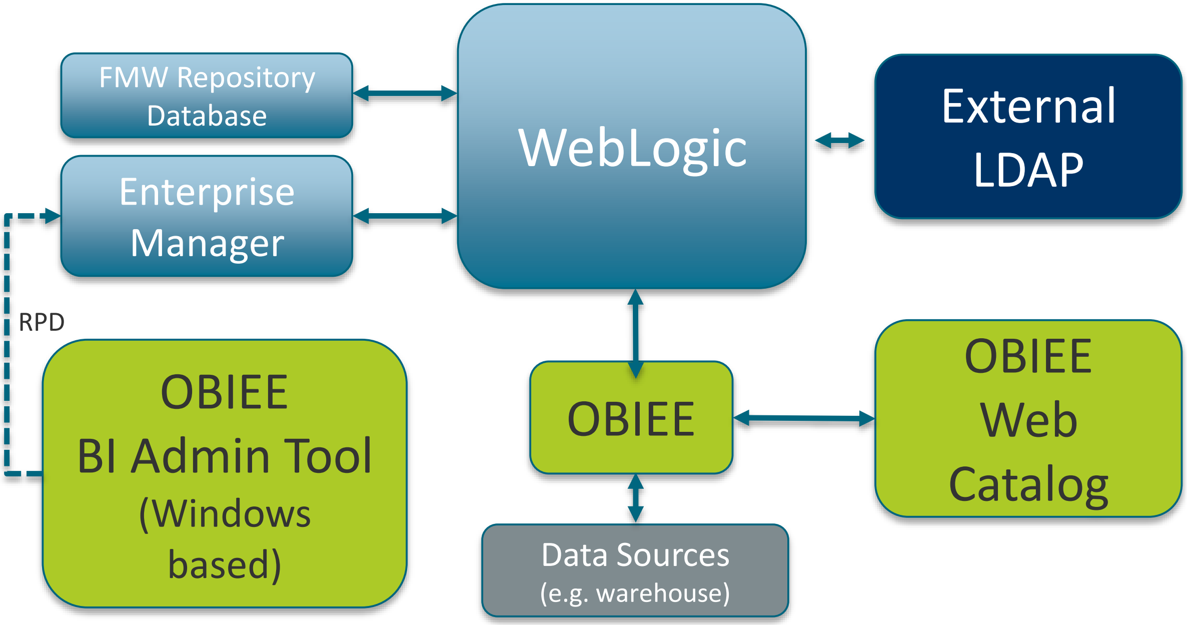
Security Assessments
ERP, Database, Sensitive Data, Pen Testing

Compliance Assistance
SOX, PCI, HIPAA

Security Design Services
Auditing, Encryption, DMZ

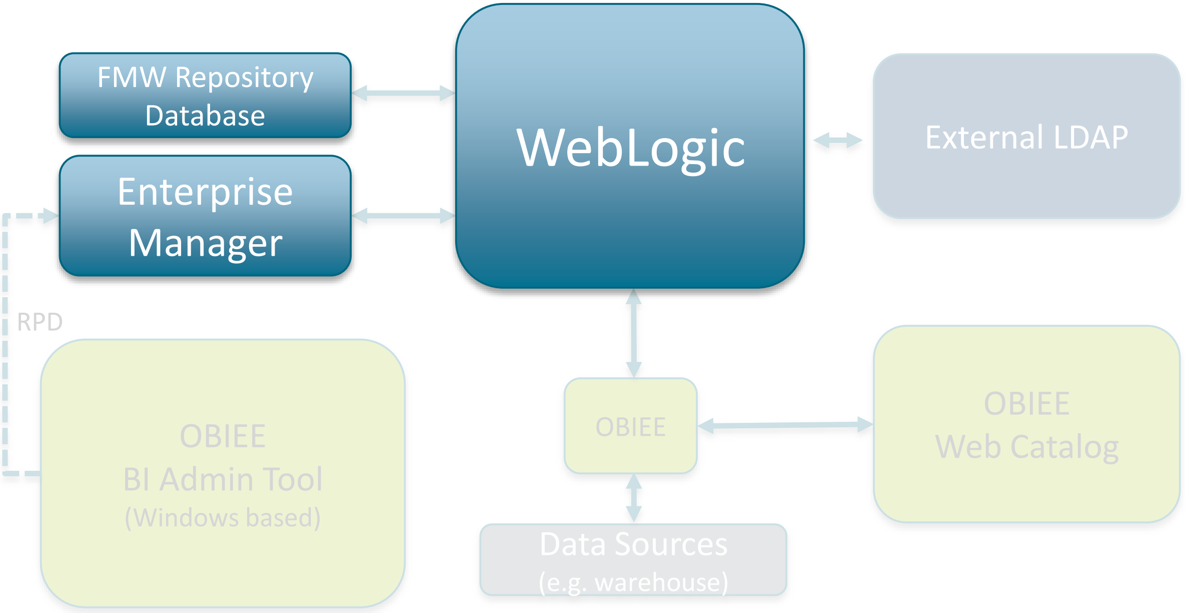
You

OBIEE Security Examined



Size of box proportionate to component's impact on security

Agenda


FMW Repository Database
Enterprise Manager
WebLogic
External LDAP
RPD
OBIEE BI Admin Tool (Windows based)
OBIEE
OBIEE Web Catalog
Data Sources (e.g. warehouse)

WebLogic Security

- **OBIEE runs inside of WebLogic**
  - Authentication
  - Key authorization steps
  - Java and Web services

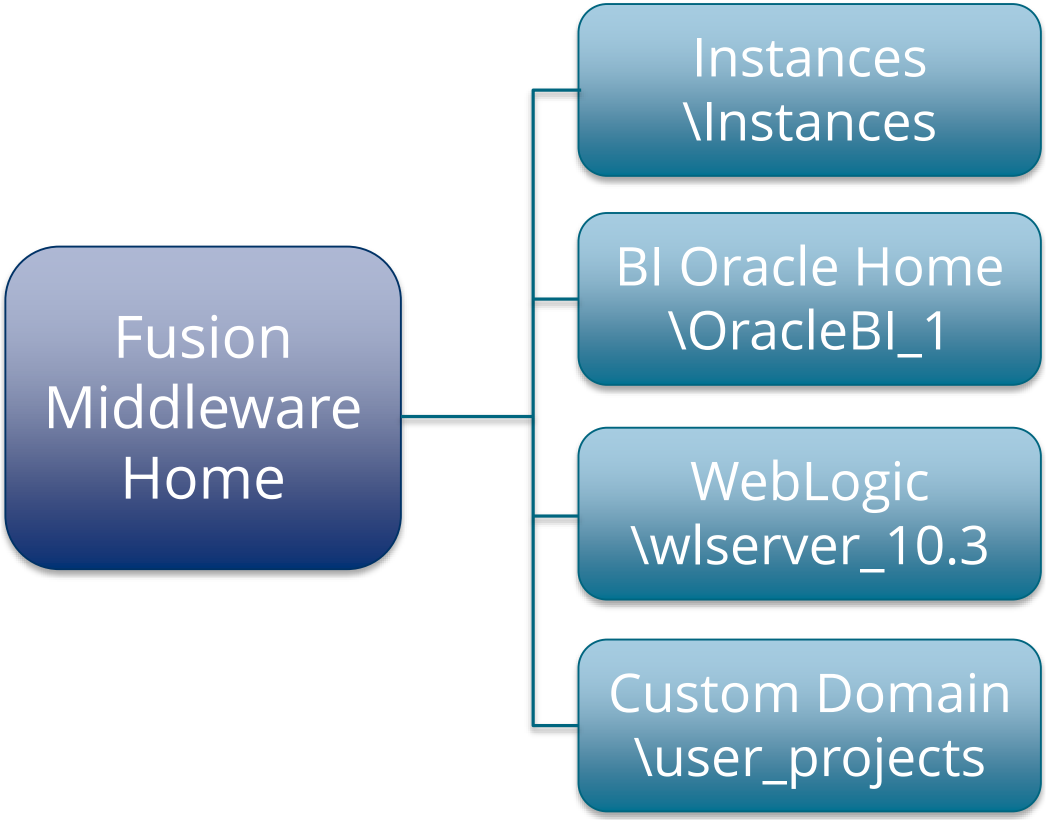
- **Secure WebLogic to Secure OBIEE**

Keep Current with WebLogic Patches

- **10.3.5**
  - Released May 2011
  - Grace period ended August 2013
- **10.3.6**
  - February 2012
  - Grace period ends December 2021
  - Terminal patch set for 11g

WebLogic File system

- Protect the file system
- Do not run WebLogic as root



Fusion Middleware Home

Instances \Instances

RPD files, security ACLs, logs and config. files

BI Oracle Home \OracleBI_1

Binaries for OBIEE components

WebLogic \wlserver_10.3

WebLogic binaries and WLST scripts

Custom Domain \user_projects

BI Domain Server configs, WLST scripts

Public Facing?

- Web Application Firewall
- WebLogic 10.3.6
- Java 1.6 vs. 1.7
- WebLogic Configurations
  - Robots.txt
  - Powered By
  - Services exposed

Metadata Repository

- **Metadata repository database required for each Fusion Middleware product**
  - Oracle is recommended but not required
  - ‘Repository Creation Utility’ used to create

- **OBIEE metadata schemas**
  - BIPLATFORM
  - MDS

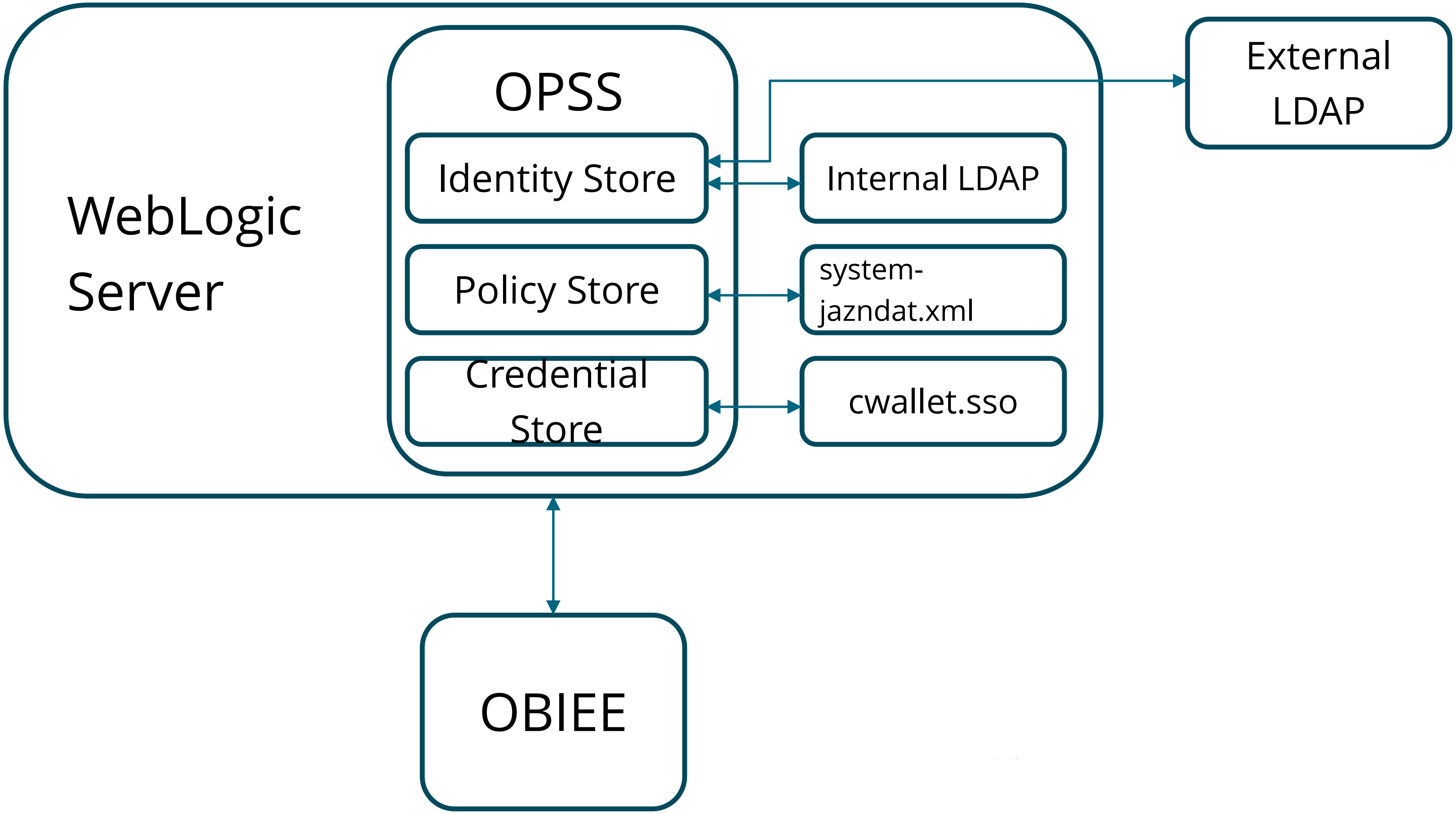
- **Security of metadata repository database is critical**
  - All standard security best practices apply
  - Do not manually edit or allow access

Security Realms

- **OBIEE 11g uses WebLogic for centralized common services**
  - Common security model included
  - Significant change from OBIEE 10g
- **WebLogic common security defined through security realms. Realms define:**
  - Users
  - Groups
  - Security roles and policies
- **Key decision**
  - Use default security realm or custom for OBIEE

Oracle Platform Security Services (OPSS)

Transcends ALL Fusion Middleware Products



WebLogic Scripting Tools (WLST)*

- Command line scripting tool to manage WebLogic
  - Jython based
- On and offline modes
  - — Both are powerful
- Access remotely or console
- WebLogic Security Framework used to enforce same rules as user interface

- Connect using administration port
- Use appropriate WebLogic accounts for WLST scripting
- Do not hardcode credentials
- Do not expose encrypted attributes
  - E.g. listCred()

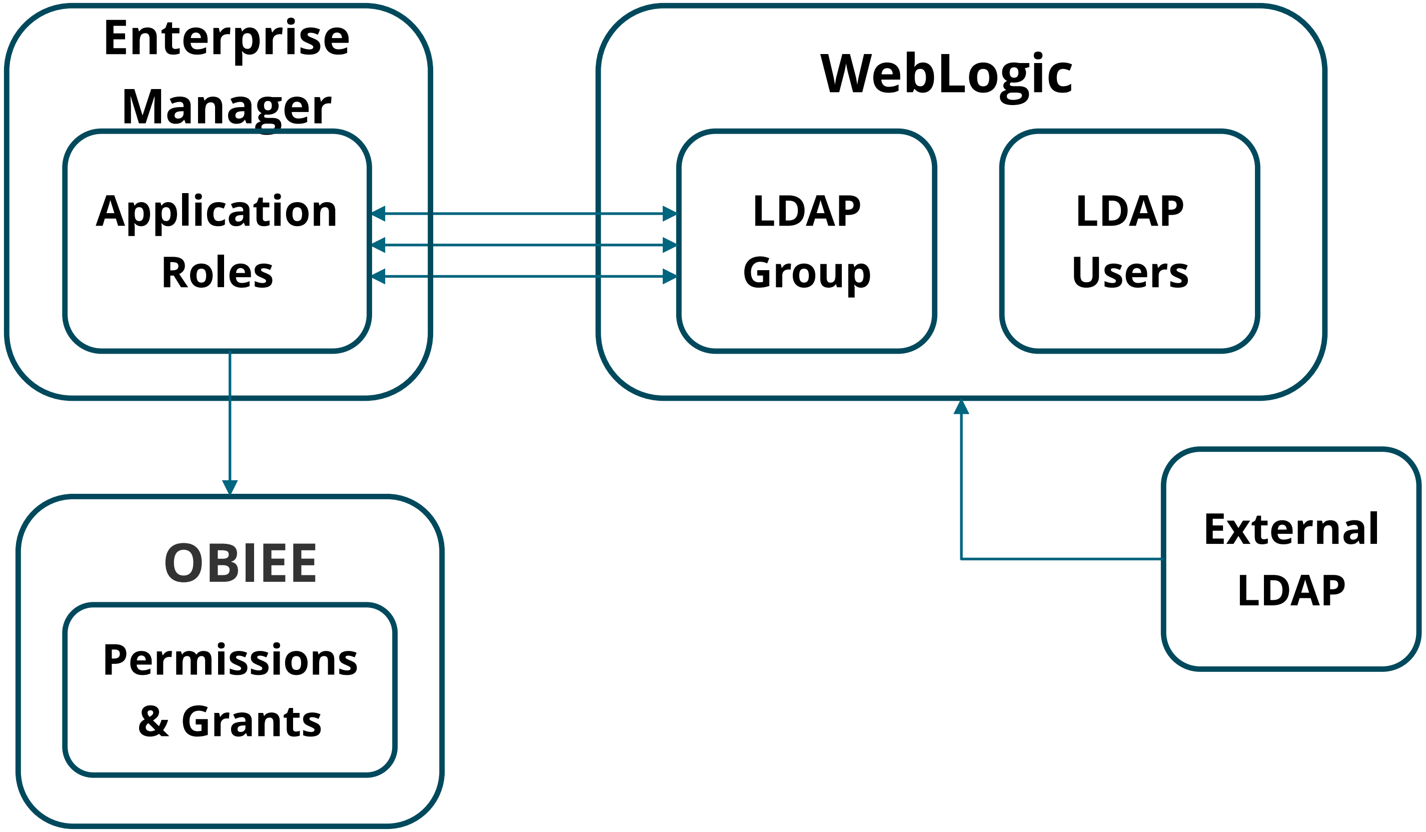
* DBAs use SQL, WebLogic Admins use WLST

WebLogic Auditing

- Prebuilt compliance reporting features
- Flexible and extensive
  - Specific criteria
  - Severity levels
- Authentication history/failures
- Authorization history

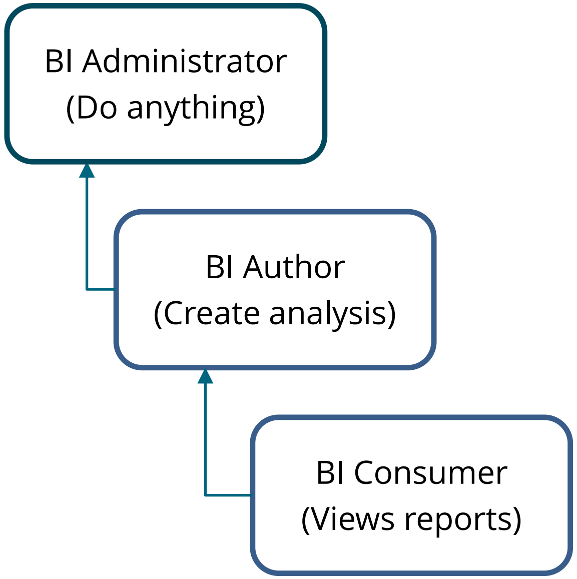
- Common audit record format
- Write audit data to:
  - Database
  - File
- Use audit data in
  - BI Publisher
  - Splunk, ArcSight etc….

Applications Roles

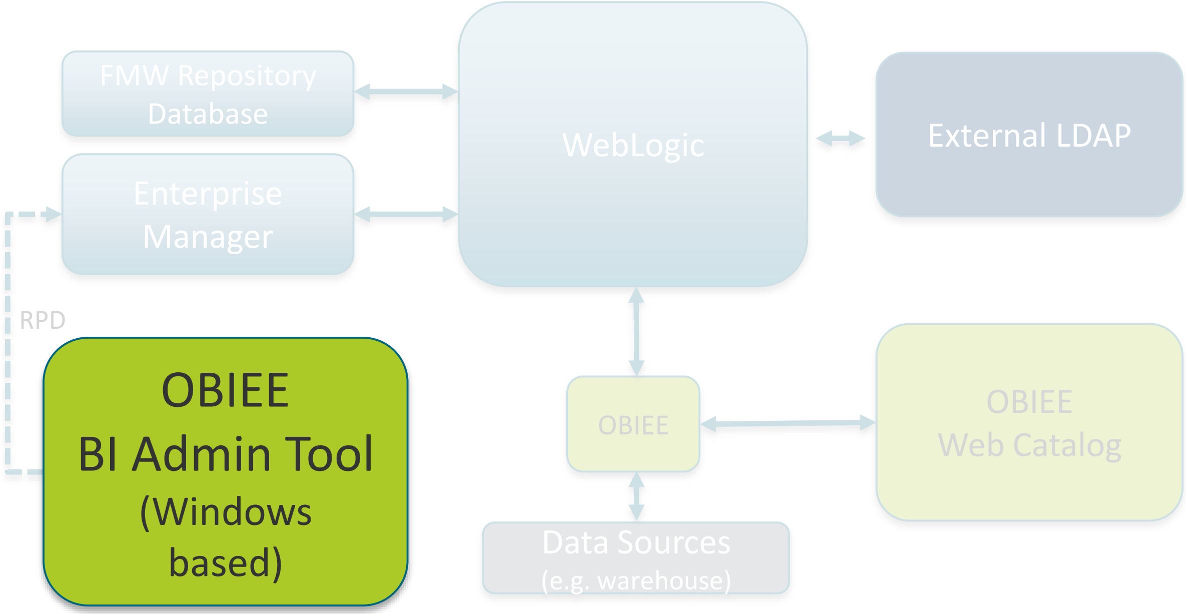


Application Roles

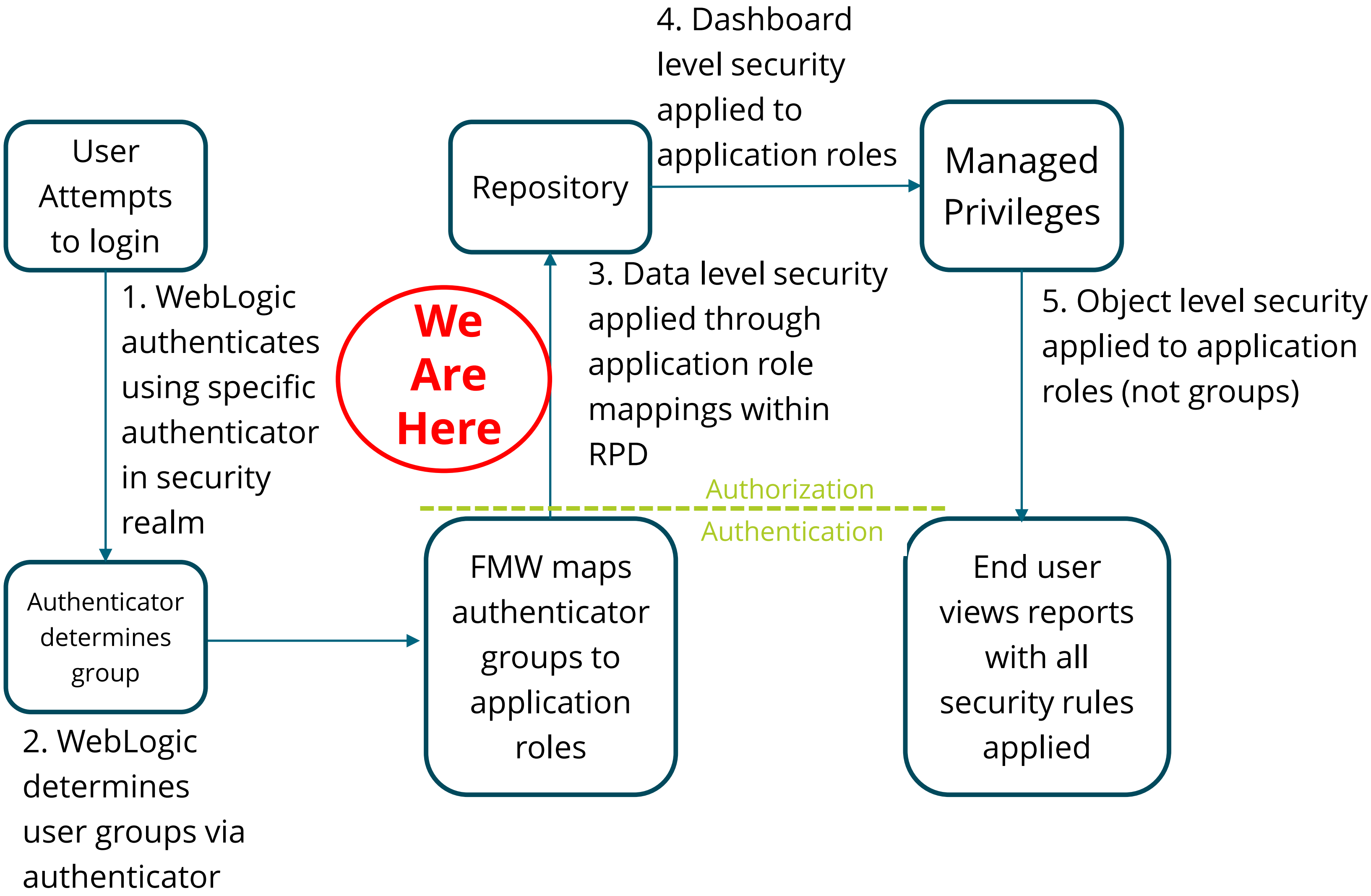
- **Transcend ALL Fusion Products**
- **Defined in Enterprise Manager**
- **Map to LDAP groups**
    - External or internal
- **Key Decision:**
    - Use default or custom



Agenda


FMW Repository Database
Enterprise Manager
WebLogic
External LDAP
RPD
OBIEE BI Admin Tool (Windows based)
OBIEE
OBIEE Web Catalog
Data Sources (e.g. warehouse)

Where Are We?



User Attempts to login

1. WebLogic authenticates using specific authenticator in security realm

Authenticator determines group

2. WebLogic determines user groups via authenticator

FMW maps authenticator groups to application roles

3. Data level security applied through application role mappings within RPD

Repository

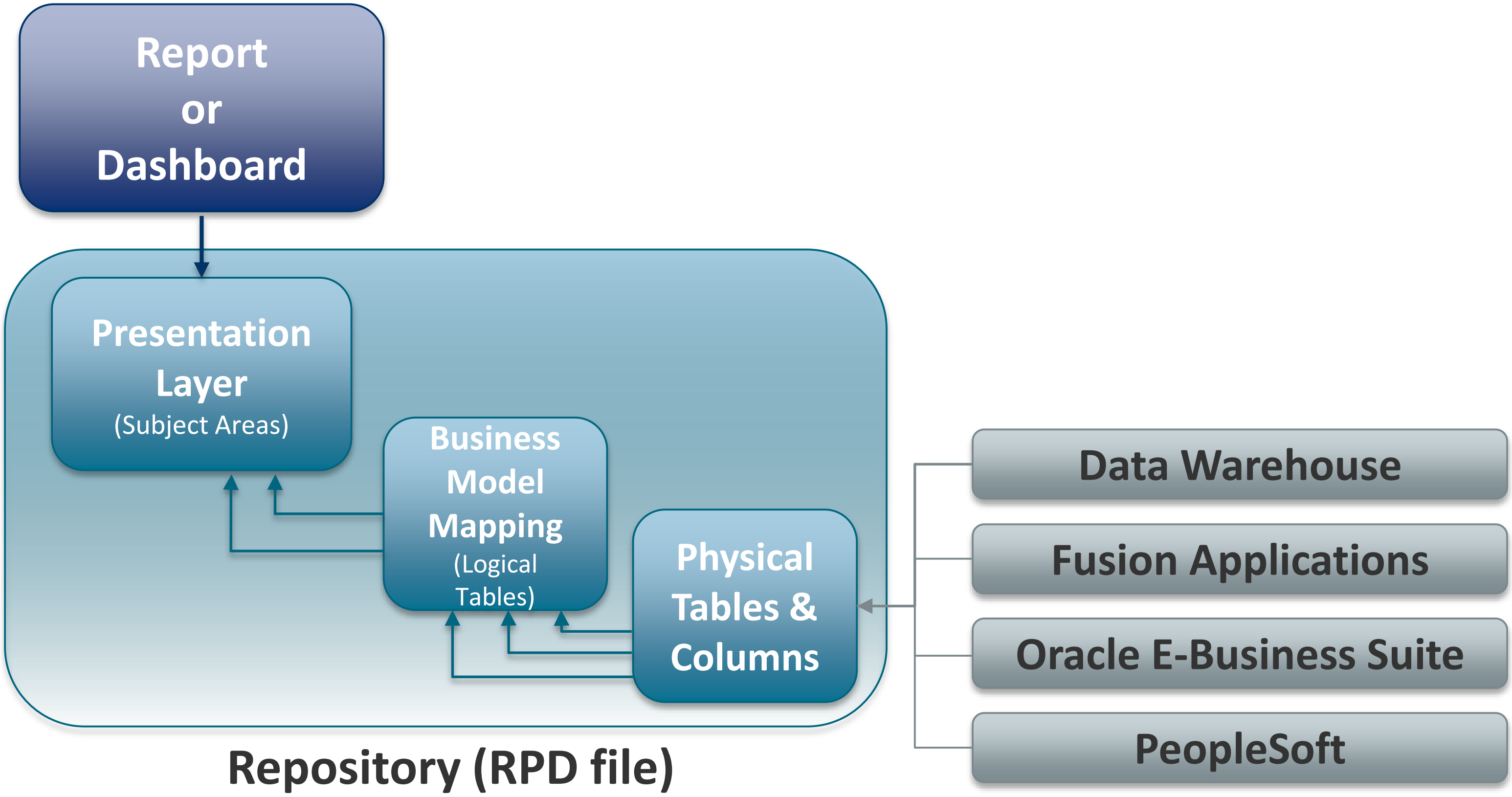
4. Dashboard level security applied to application roles

Managed Privileges

5. Object level security applied to application roles (not groups)

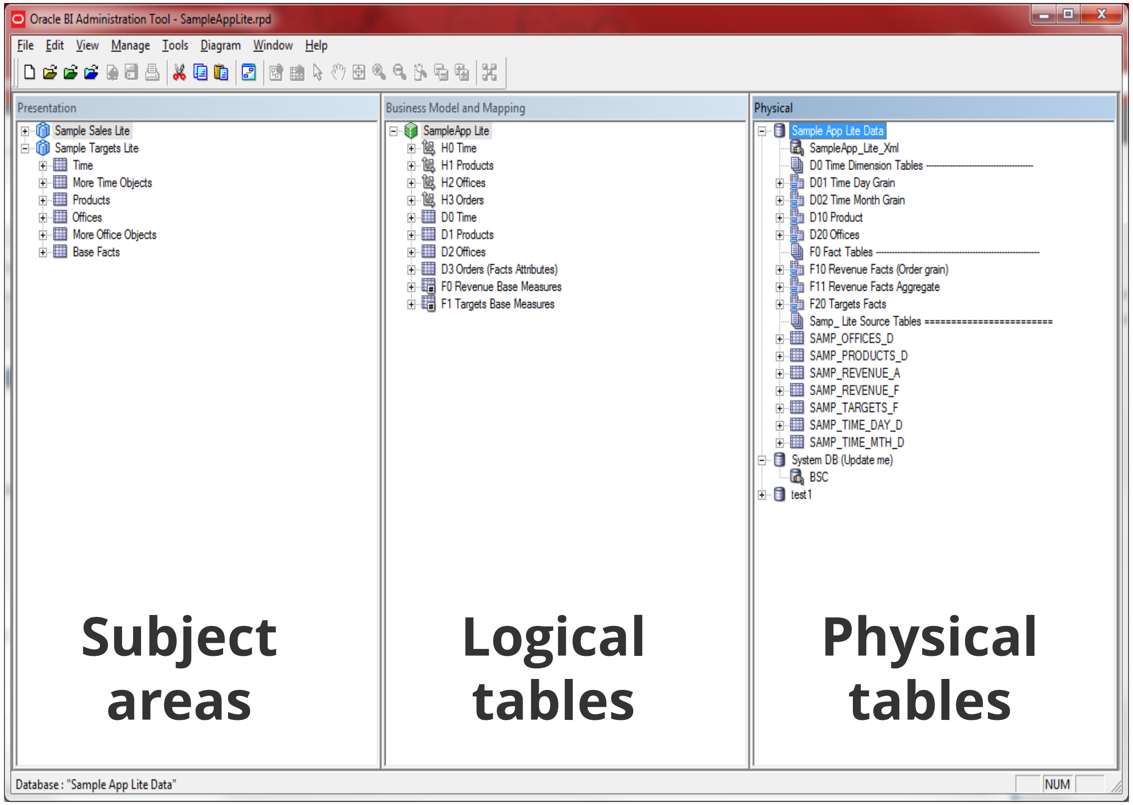
End user views reports with all security rules applied

Oracle Business Intelligence Enterprise Edition



OBIEE Repositories

- OBIEE Solutions are built using Repositories
  - Single file (“RPD”) defines EVERTHING
  - Security included



Presentation

- Sample Sales Lite
- Sample Targets Lite
  - Time
  - More Time Objects
  - Products
  - Offices
  - More Office Objects
  - Base Facts

Business Model and Mapping

- SampleApp Lite
  - H0 Time
  - H1 Products
  - H2 Offices
  - H3 Orders
  - D0 Time
  - D1 Products
  - D2 Offices
  - D3 Orders (Facts Attributes)
  - F0 Revenue Base Measures
  - F1 Targets Base Measures

Physical

- Sample App Lite Data
  - SampleApp_Lite_Xml
  - D0 Time Dimension Tables ---------------------------------
  - D01 Time Day Grain
  - D02 Time Month Grain
  - D10 Product
  - D20 Offices
  - F0 Fact Tables ---
  - F10 Revenue Facts (Order grain)
  - F11 Revenue Facts Aggregate
  - F20 Targets Facts
  - Samp_ Lite Source Tables ========================
  - SAMP_OFFICES_D
  - SAMP_PRODUCTS_D
  - SAMP_REVENUE_A
  - SAMP_REVENUE_F
  - SAMP_TARGETS_F
  - SAMP_TIME_DAY_D
  - SAMP_TIME_MTH_D
- System DB (Update me)
  - BSC
- test1

Database : "Sample App Lite Data"

Subject areas

Logical tables

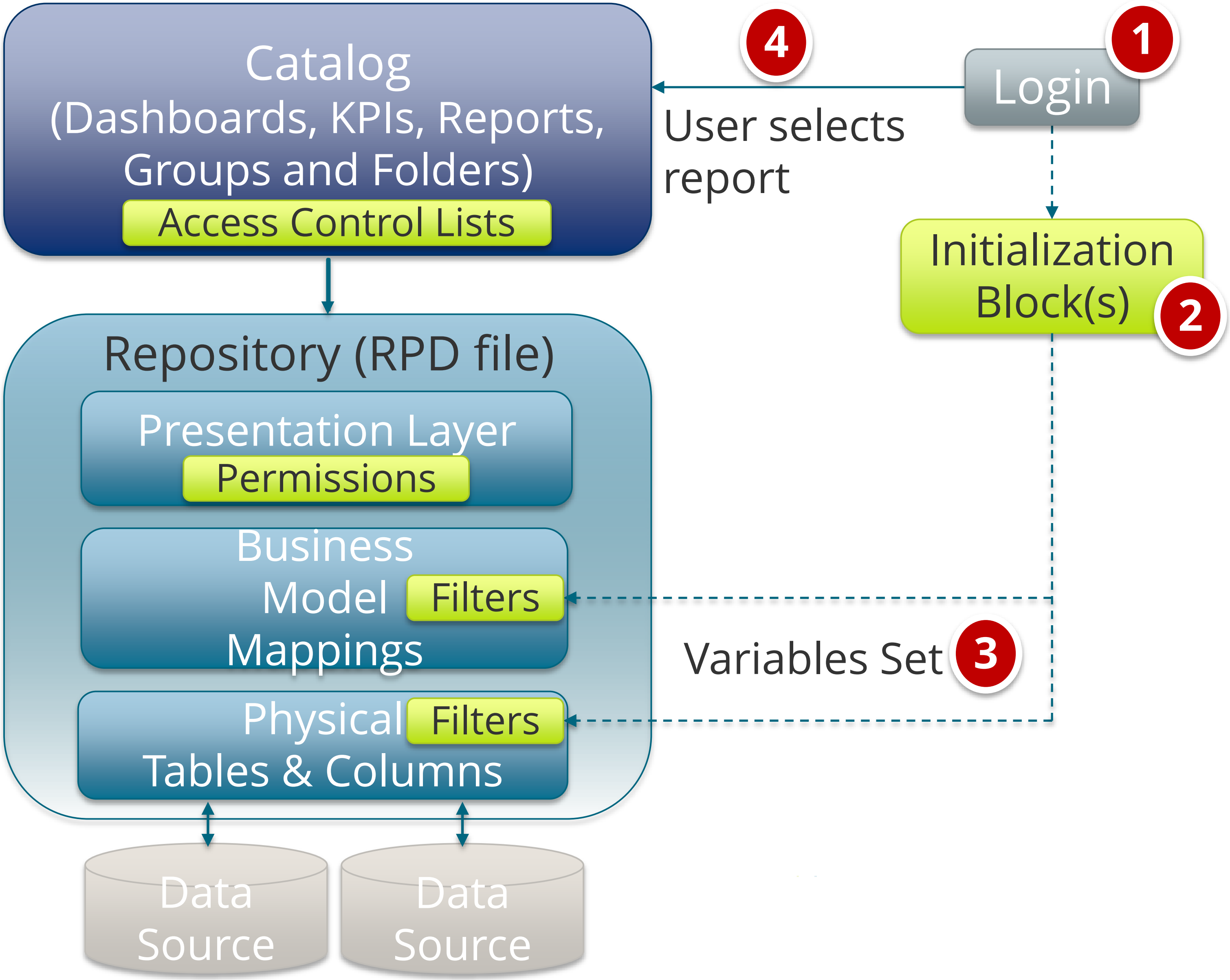
Physical tables

Windows based BI Admin Tool used to create and maintain RPD files

RPD Security

- **Need to Secure RPD files**
  - Data source connection passwords
  - Security rules and filters
- **Password to open**
  - Production vs Non-production
  - Password needed to deploy within Enterprise Manager
- **Encrypted**
  - Password used to encrypt
  - Can export and save as XML files

OBIEE Security



Three Levels of OBIEE Security (Authorization)

Data-level security	▪ Data filters to eliminate rows from result sets ▪ Set in RPD file
Object-level security	▪ Permissions on specific objects such as subject areas, presentation or physical tables and columns ▪ Set in RPD file
Presentation Catalog security	▪ What reports and dashboards are available to specific users, application roles and LDAP groups ▪ Set in catalog

#C14LV

Data Level Security

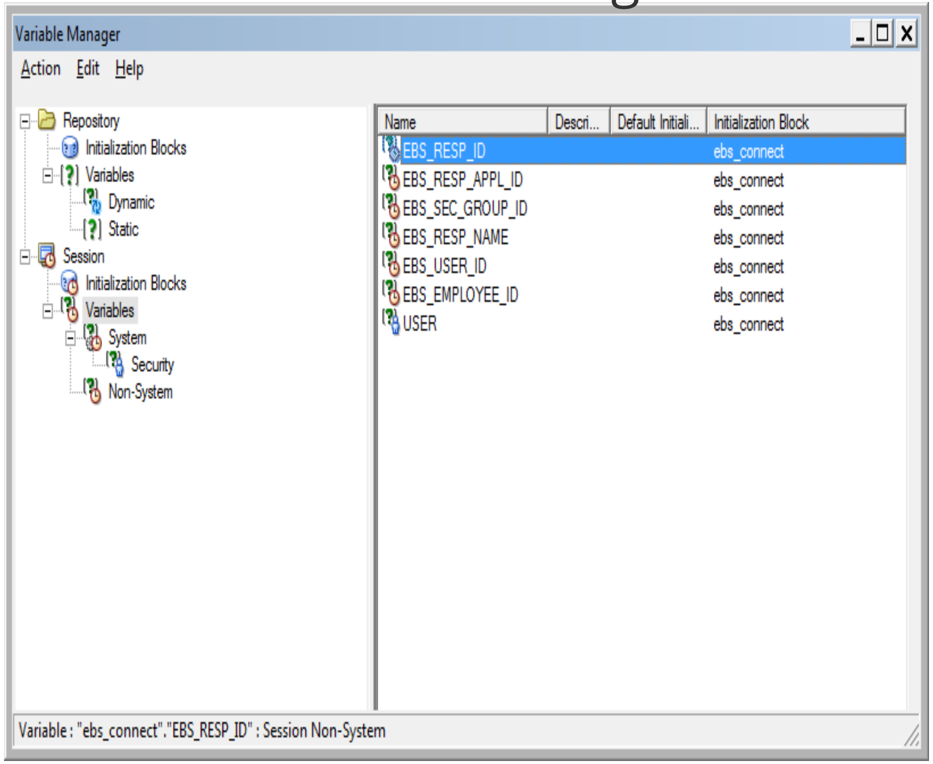
- **Deny or allow access to physical or logical table, row or column**
  - Apply to users or roles
  - Use filters restrict
  - Use variables to define filters

- **Two types of variables are used**
  - Repository **–** Static or dynamic, same for all users
  - Session **–** initialized when user logs in

Data Level Security

- **Initialization block**
  - Set variables (repository & session) when a user connects
- **Two types of session variables**
  - System: reserved names e.g. USER
  - Non-system: defined by author of RPD e.g. EBS_RESP_ID

Variable Manager



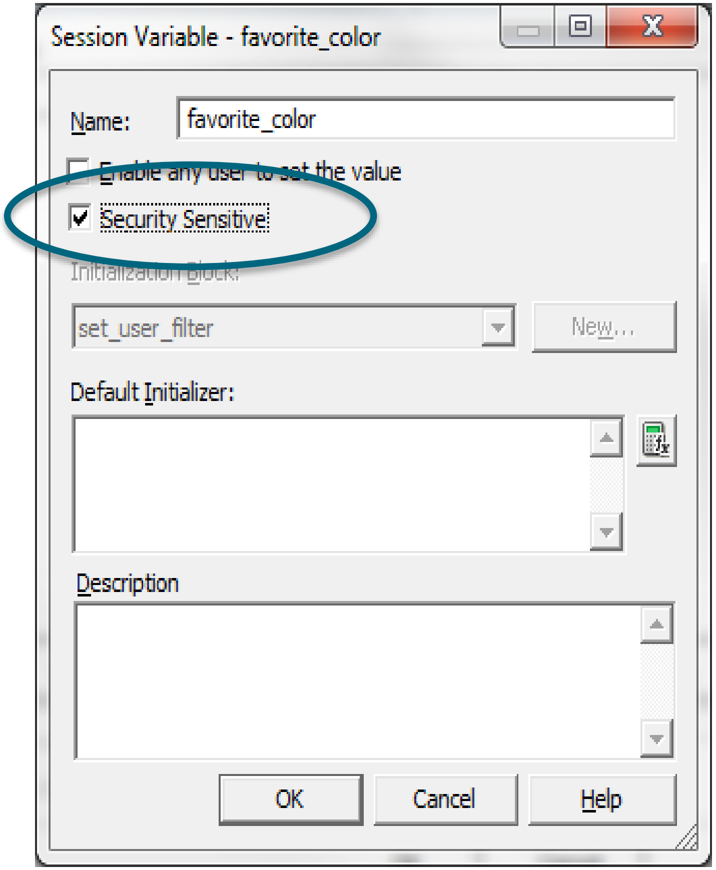
Name	Descri...	Default Initiali...	Initialization Block
EBS_RESP_ID			ebs_connect
EBS_RESP_APPL_ID			ebs_connect
EBS_SEC_GROUP_ID			ebs_connect
EBS_RESP_NAME			ebs_connect
EBS_USER_ID			ebs_connect
EBS_EMPLOYEE_ID			ebs_connect
USER			ebs_connect

Variable : "ebs_connect"."EBS_RESP_ID" : Session Non-System

Data Level Security

- **Be careful of caching with session variables and VPD**
    - DBMS_SESSION.SET_IDENTIFIER

Session Variable



Session Variable - favorite_color

Name: favorite_color

☐ Enable any user to set the value

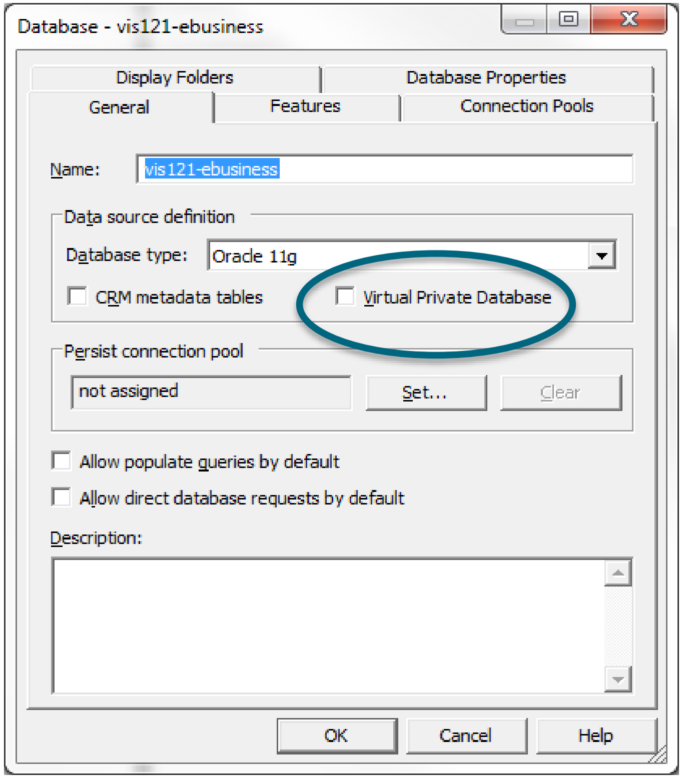
☑ Security Sensitive

Initialization Block: set_user_filter

Default Initializer:

Description

Connection



Database - vis121-ebusiness

Name: vis121-ebusiness

Data source definition

Database type: Oracle 11g

☐ CRM metadata tables

☐ Virtual Private Database

Persist connection pool

not assigned

☐ Allow populate queries by default

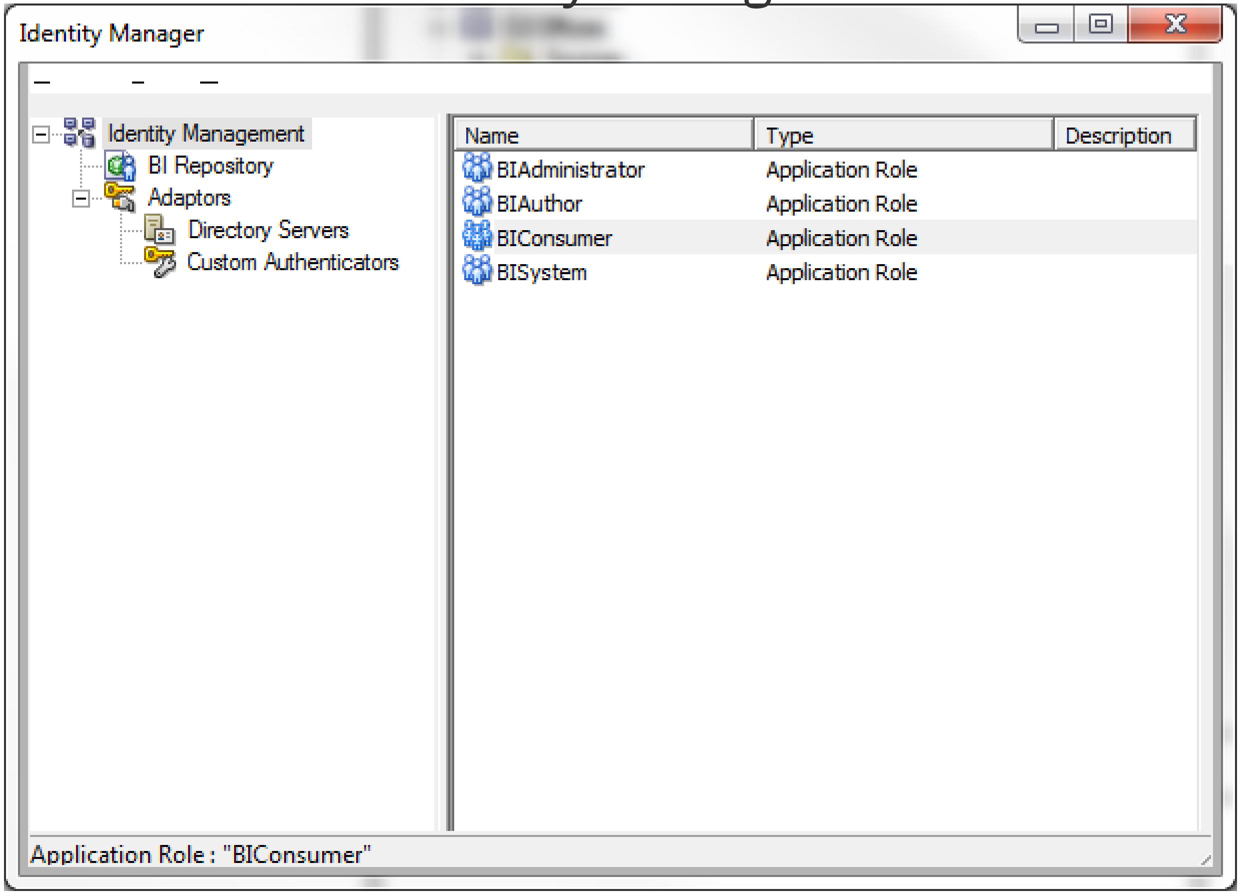
☐ Allow direct database requests by default

Description:

Data Level Security

- Filters defined for Application Roles
  - Identity manager -> select user or role -> click on permissions

Identity Manager



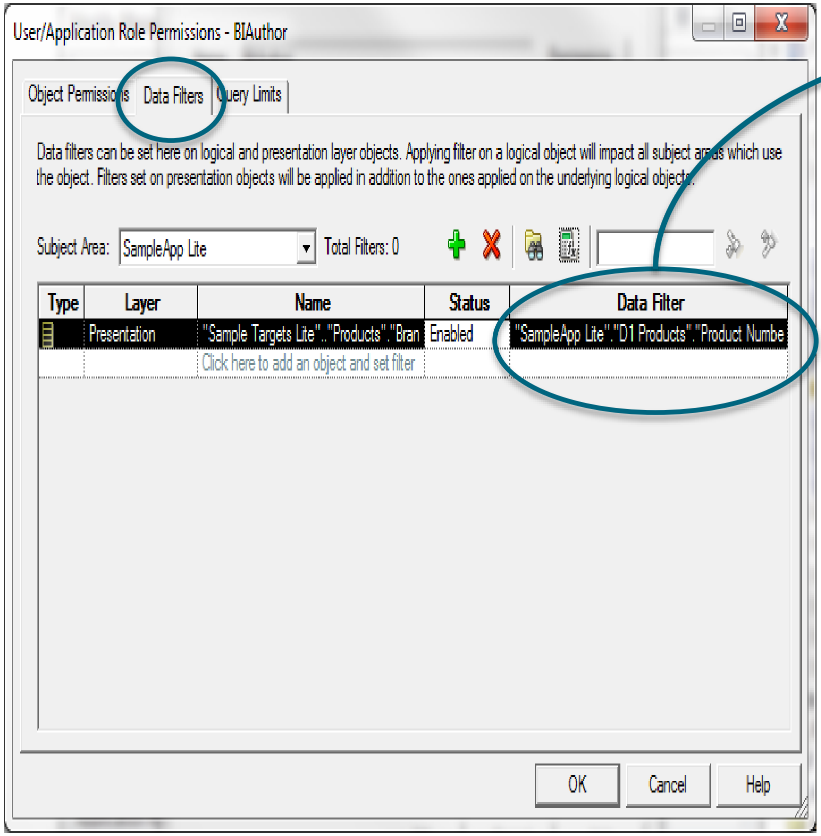
Identity Manager

- Identity Management
  - BI Repository
  - Adaptors
    - Directory Servers
    - Custom Authenticators

Name	Type	Description
BIAdministrator	Application Role	
BIAuthor	Application Role	
BIConsumer	Application Role	
BISystem	Application Role	

Application Role : "BIConsumer"

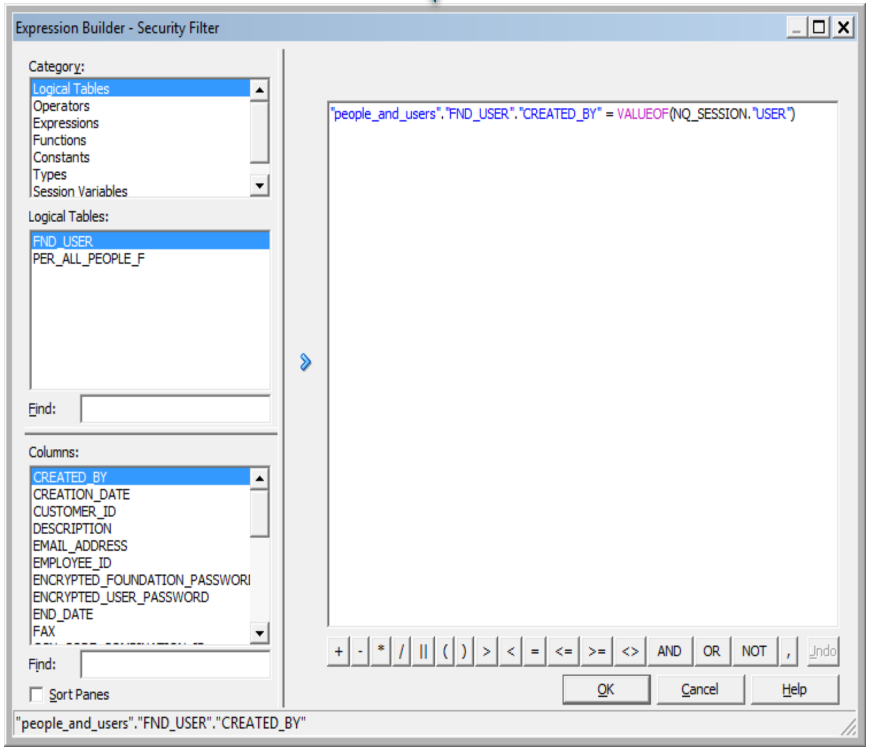
Data Level Security



Data filters can be set here on logical and presentation layer objects. Applying filter on a logical object will impact all subject areas which use the object. Filters set on presentation objects will be applied in addition to the ones applied on the underlying logical objects.

Subject Area: SampleApp Lite

Type	Layer	Name	Status	Data Filter
▤	Presentation	"Sample Targets Lite".."Products"."Bran	Enabled	"SampleApp Lite"."D1 Products"."Product Numbe
		Click here to add an object and set filter		



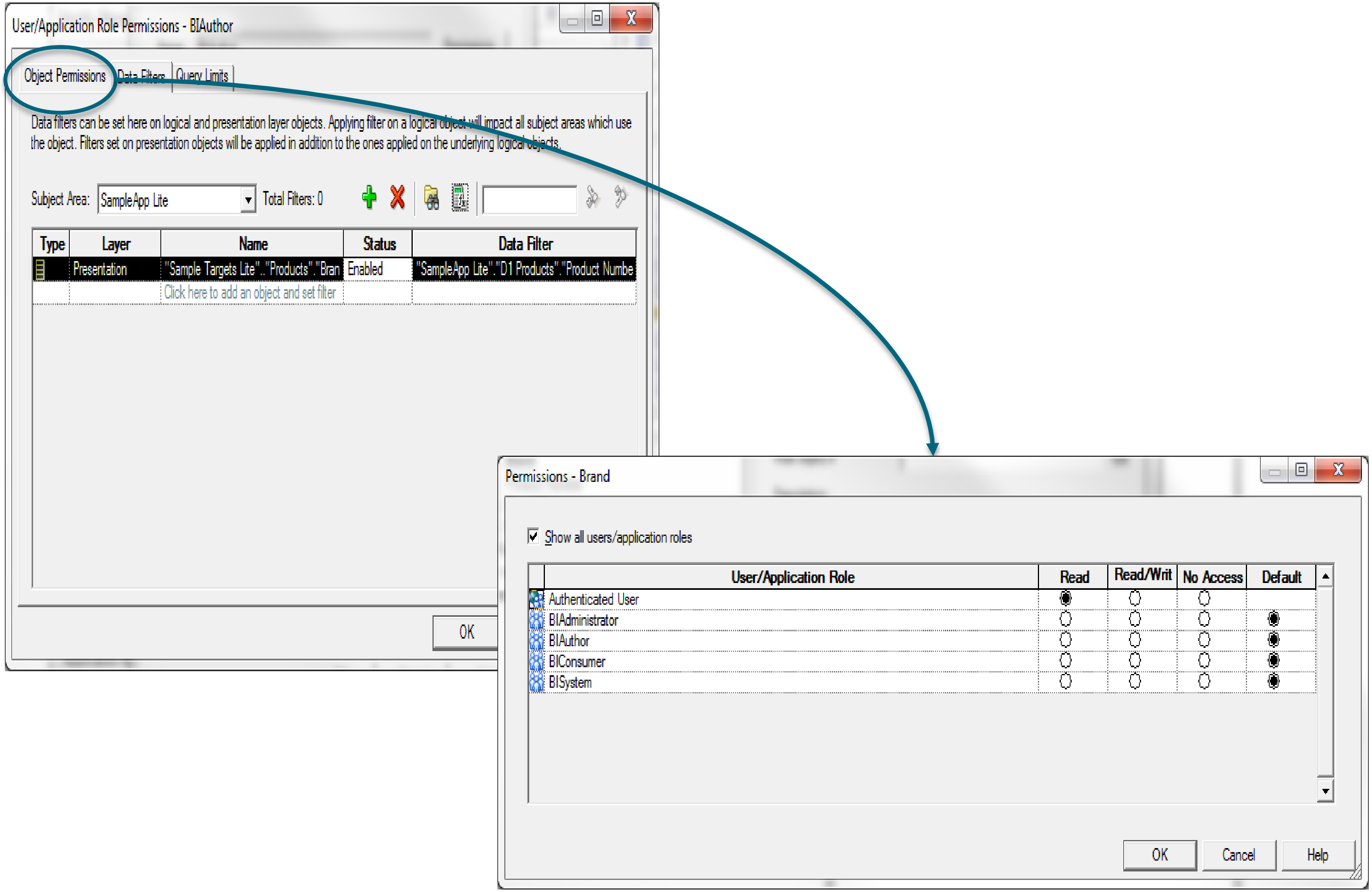
```
"people_and_users"."FND_USER"."CREATED_BY" = VALUEOF(NQ_SESSION."USER")
```

"people_and_users"."FND_USER"."CREATED_BY"

Example

Filter for Oracle E-Business Suite Set RESPONSIBILITY_ID = 200 to see only hourly employees

Object Level Security



User/Application Role Permissions - BIAuthor

Data filters can be set here on logical and presentation layer objects. Applying filter on a logical object will impact all subject areas which use the object. Filters set on presentation objects will be applied in addition to the ones applied on the underlying logical objects.

Subject Area: SampleApp Lite Total Filters: 0

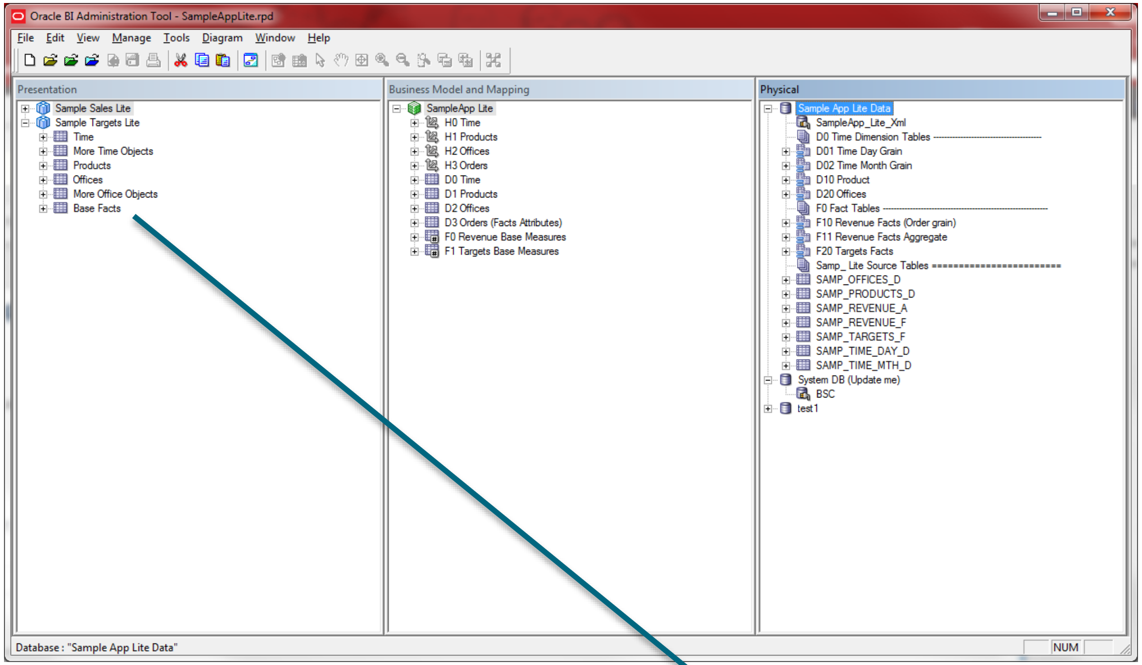
Type	Layer	Name	Status	Data Filter
▤	Presentation	"Sample Targets Lite"."Products"."Bran	Enabled	"SampleApp Lite"."D1 Products"."Product Numbe
		Click here to add an object and set filter		

Permissions - Brand

☑ Show all users/application roles

User/Application Role	Read	Read/Writ	No Access	Default
Authenticated User	●	○	○	
BIAdministrator	○	○	○	●
BIAuthor	○	○	○	●
BIConsumer	○	○	○	●
BISystem	○	○	○	●

Object Level Security



Oracle BI Administration Tool - SampleAppLite.rpd

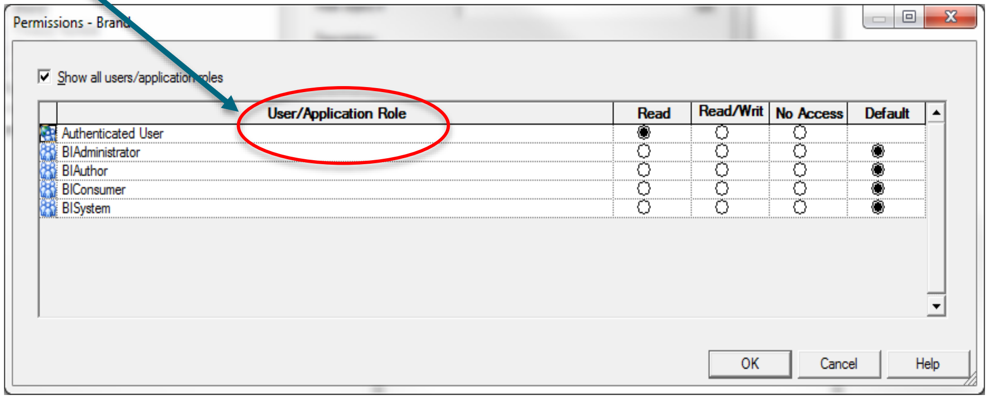
Presentation
- Sample Sales Lite
- Sample Targets Lite
  - Time
  - More Time Objects
  - Products
  - Offices
  - More Office Objects
  - Base Facts

Business Model and Mapping
- SampleApp Lite
  - H0 Time
  - H1 Products
  - H2 Offices
  - H3 Orders
  - D0 Time
  - D1 Products
  - D2 Offices
  - D3 Orders (Facts Attributes)
  - F0 Revenue Base Measures
  - F1 Targets Base Measures

Physical
- Sample App Lite Data
  - SampleApp_Lite_Xml
  - D0 Time Dimension Tables ------------------------------
  - D01 Time Day Grain
  - D02 Time Month Grain
  - D10 Product
  - D20 Offices
  - F0 Fact Tables --
  - F10 Revenue Facts (Order grain)
  - F11 Revenue Facts Aggregate
  - F20 Targets Facts
  - Samp_ Lite Source Tables ========================
  - SAMP_OFFICES_D
  - SAMP_PRODUCTS_D
  - SAMP_REVENUE_A
  - SAMP_REVENUE_F
  - SAMP_TARGETS_F
  - SAMP_TIME_DAY_D
  - SAMP_TIME_MTH_D
- System DB (Update me)
  - BSC
- test1

Database : "Sample App Lite Data"

Permissions for Application Roles by Subject Area



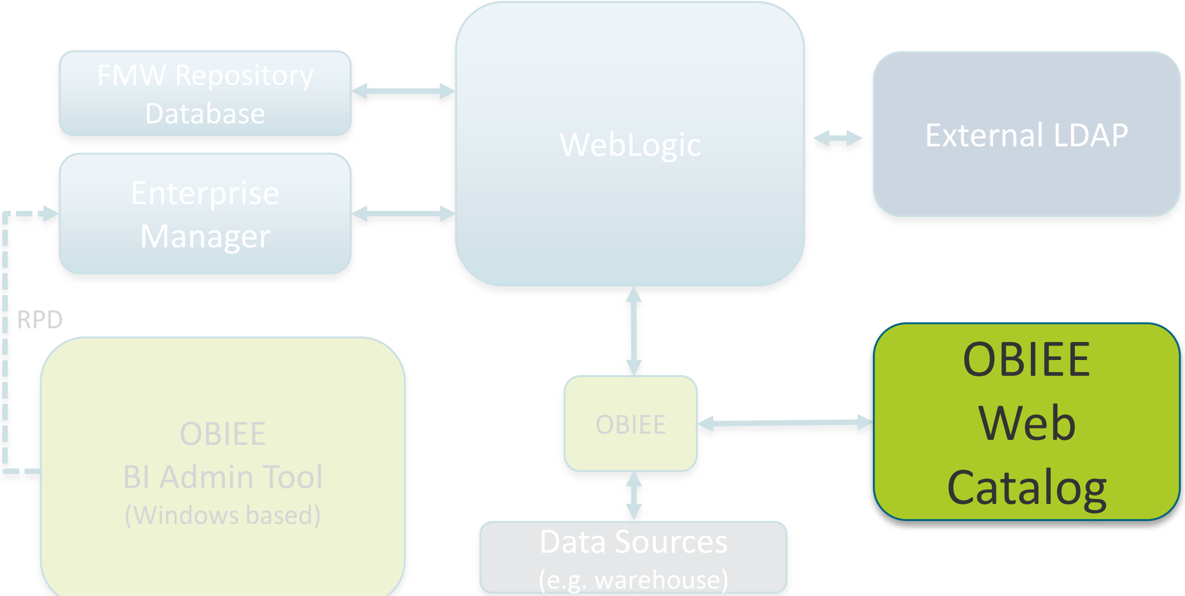
Permissions - Brand

☑ Show all users/application roles

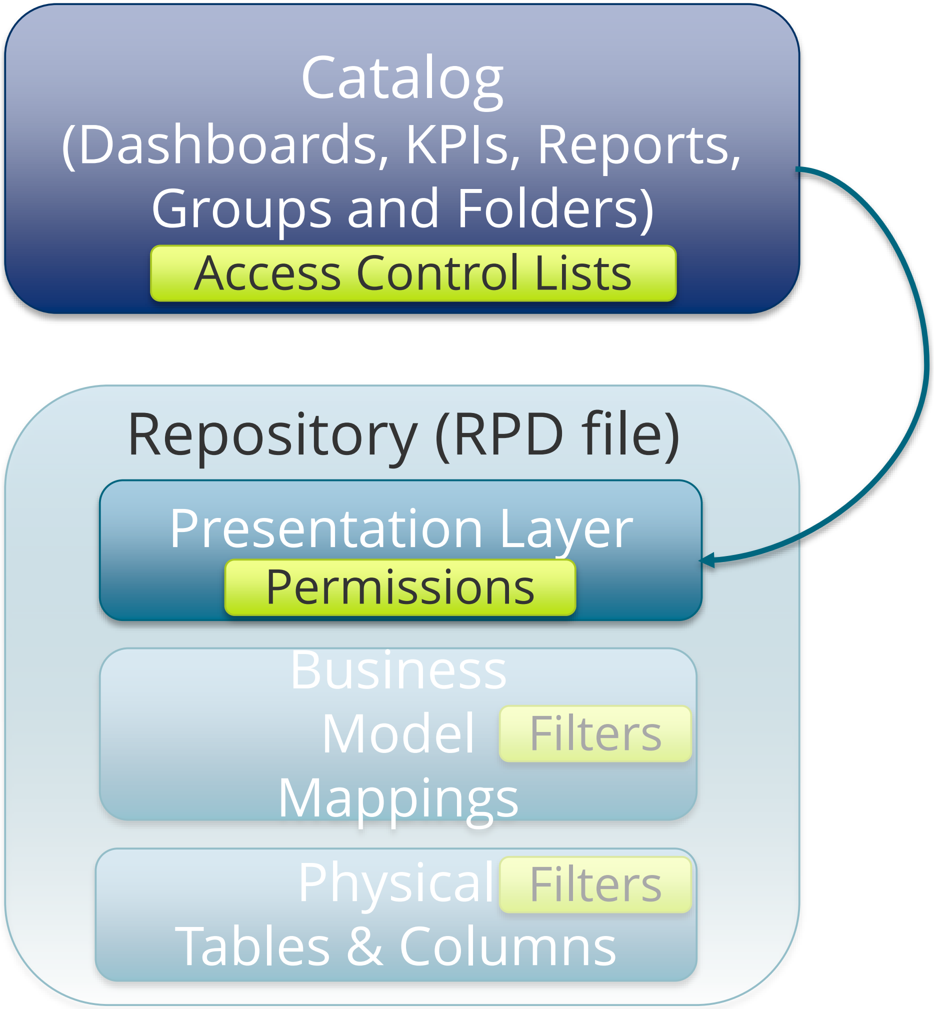
User/Application Role	Read	Read/Writ	No Access	Default
Authenticated User	●	○	○	
BIAdministrator	○	○	○	●
BIAuthor	○	○	○	●
BIConsumer	○	○	○	●
BISystem	○	○	○	●

By Application Role

Agenda


FMW Repository Database
Enterprise Manager
WebLogic
External LDAP
RPD
OBIEE BI Admin Tool (Windows based)
OBIEE
OBIEE Web Catalog
Data Sources (e.g. warehouse)

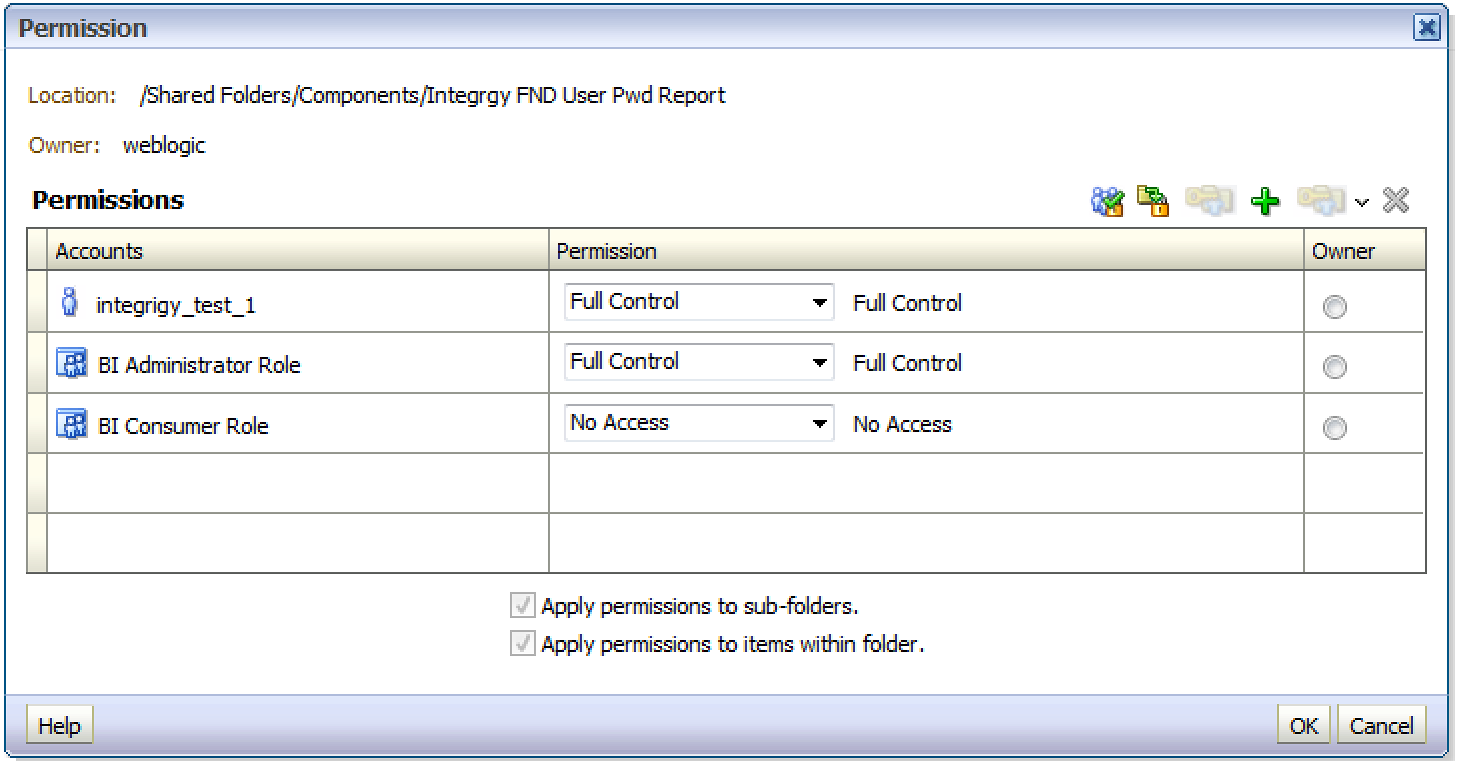
OBIEE Web Catalog



- Reports only see Subject Areas within Presentation Layer
- Reports defined within Catalog
- Catalog ACLs determine who can see what report

OBIEE Web Catalog

- Permissions for reports and folders
  - By Role or User



Permission

Location: /Shared Folders/Components/Integrgy FND User Pwd Report

Owner: weblogic

Permissions

Accounts	Permission		Owner
integrigy_test_1	Full Control	Full Control	○
BI Administrator Role	Full Control	Full Control	○
BI Consumer Role	No Access	No Access	○

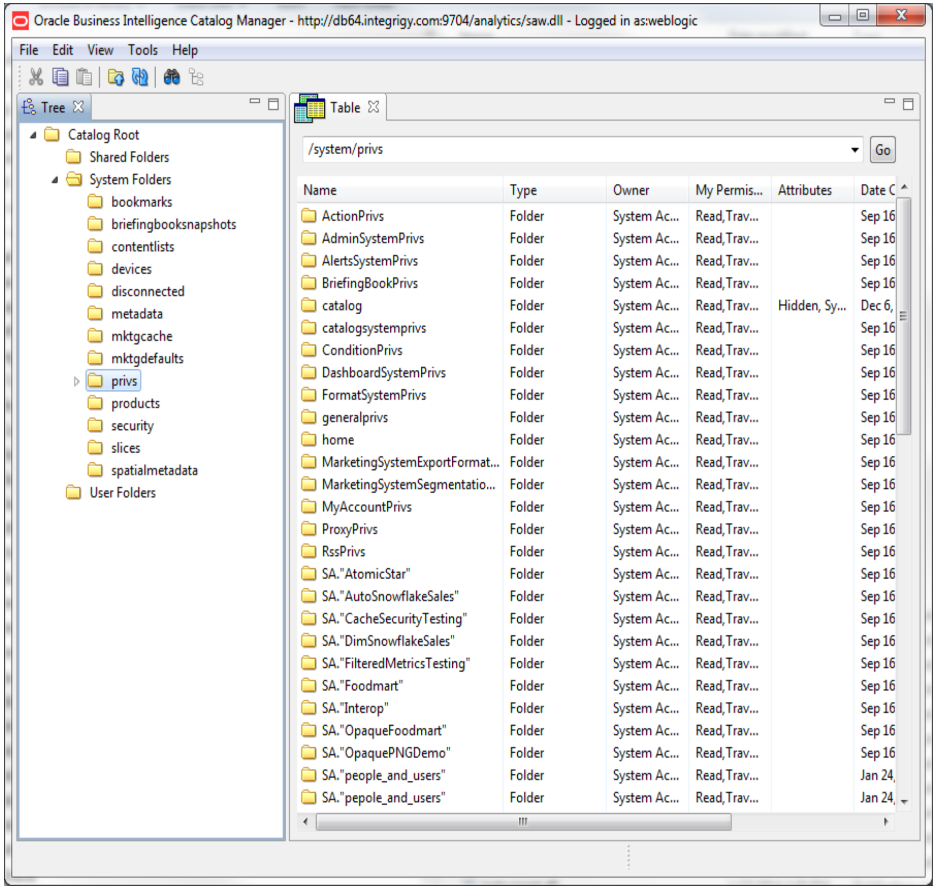
☑ Apply permissions to sub-folders.

☑ Apply permissions to items within folder.

Presentation Catalog Security

- **Access Control List (ACL) defined for each object**
  - Stored in *.ATR files
- **Works only at the subject area level of RPD**
- **BI Publisher is a separate catalog**
- **Catalog of permissions:**
  - Dashboards
  - Reports
  - KPIs
  - Groups of folders

Windows Catalog Client



Oracle Business Intelligence Catalog Manager - http://db64.integrigy.com:9704/analytics/saw.dll - Logged in as:weblogic

- Catalog Root
  - Shared Folders
  - System Folders
    - bookmarks
    - briefingbooksnapshots
    - contentlists
    - devices
    - disconnected
    - metadata
    - mktgcache
    - mktgdefaults
    - privs
    - products
    - security
    - slices
    - spatialmetadata
  - User Folders

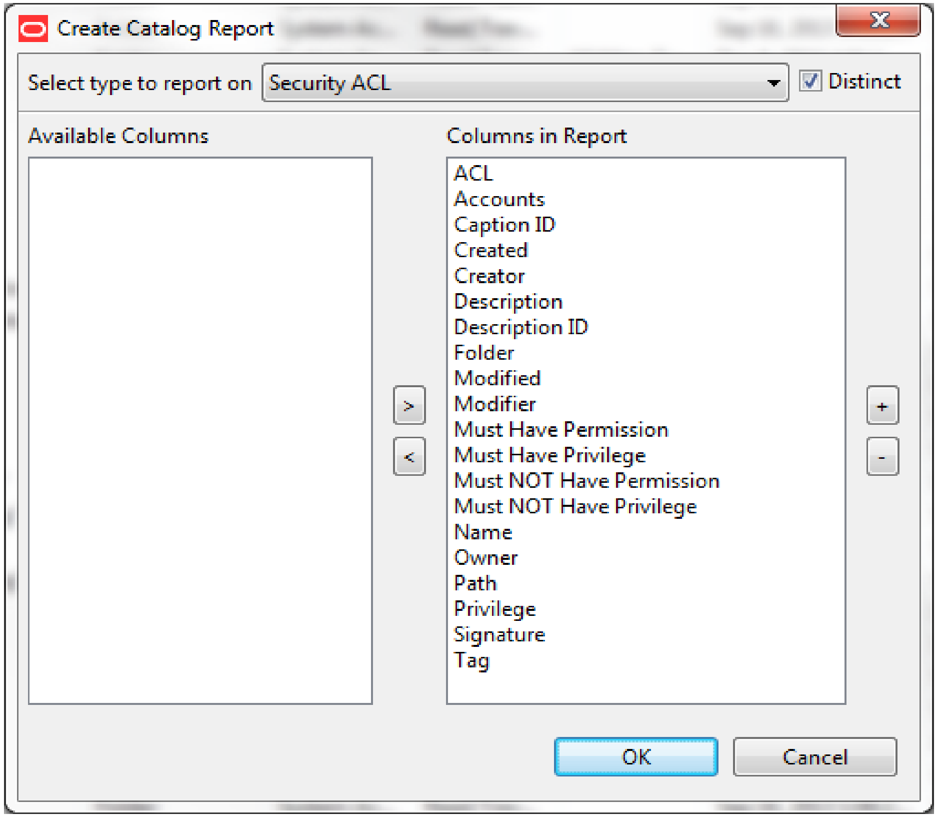
/system/privs

Name	Type	Owner	My Permis...	Attributes	Date C
ActionPrivs	Folder	System Ac...	Read,Trav...		Sep 16
AdminSystemPrivs	Folder	System Ac...	Read,Trav...		Sep 16
AlertsSystemPrivs	Folder	System Ac...	Read,Trav...		Sep 16
BriefingBookPrivs	Folder	System Ac...	Read,Trav...		Sep 16
catalog	Folder	System Ac...	Read,Trav...	Hidden, Sy...	Dec 6,
catalogsystemprivs	Folder	System Ac...	Read,Trav...		Sep 16
ConditionPrivs	Folder	System Ac...	Read,Trav...		Sep 16
DashboardSystemPrivs	Folder	System Ac...	Read,Trav...		Sep 16
FormatSystemPrivs	Folder	System Ac...	Read,Trav...		Sep 16
generalprivs	Folder	System Ac...	Read,Trav...		Sep 16
home	Folder	System Ac...	Read,Trav...		Sep 16
MarketingSystemExportFormat...	Folder	System Ac...	Read,Trav...		Sep 16
MarketingSystemSegmentatio...	Folder	System Ac...	Read,Trav...		Sep 16
MyAccountPrivs	Folder	System Ac...	Read,Trav...		Sep 16
ProxyPrivs	Folder	System Ac...	Read,Trav...		Sep 16
RssPrivs	Folder	System Ac...	Read,Trav...		Sep 16
SA."AtomicStar"	Folder	System Ac...	Read,Trav...		Sep 16
SA."AutoSnowflakeSales"	Folder	System Ac...	Read,Trav...		Sep 16
SA."CacheSecurityTesting"	Folder	System Ac...	Read,Trav...		Sep 16
SA."DimSnowflakeSales"	Folder	System Ac...	Read,Trav...		Sep 16
SA."FilteredMetricsTesting"	Folder	System Ac...	Read,Trav...		Sep 16
SA."Foodmart"	Folder	System Ac...	Read,Trav...		Sep 16
SA."Interop"	Folder	System Ac...	Read,Trav...		Sep 16
SA."OpaqueFoodmart"	Folder	System Ac...	Read,Trav...		Sep 16
SA."OpaquePNGDemo"	Folder	System Ac...	Read,Trav...		Sep 16
SA."people_and_users"	Folder	System Ac...	Read,Trav...		Jan 24,
SA."pepole_and_users"	Folder	System Ac...	Read,Trav...		Jan 24,

Presentation Catalog Reports

- Catalog reports are critical feature
- Export to Excel for analysis and reporting

Select ACL and columns to report



Create Catalog Report

Select type to report on: Security ACL

☑ Distinct

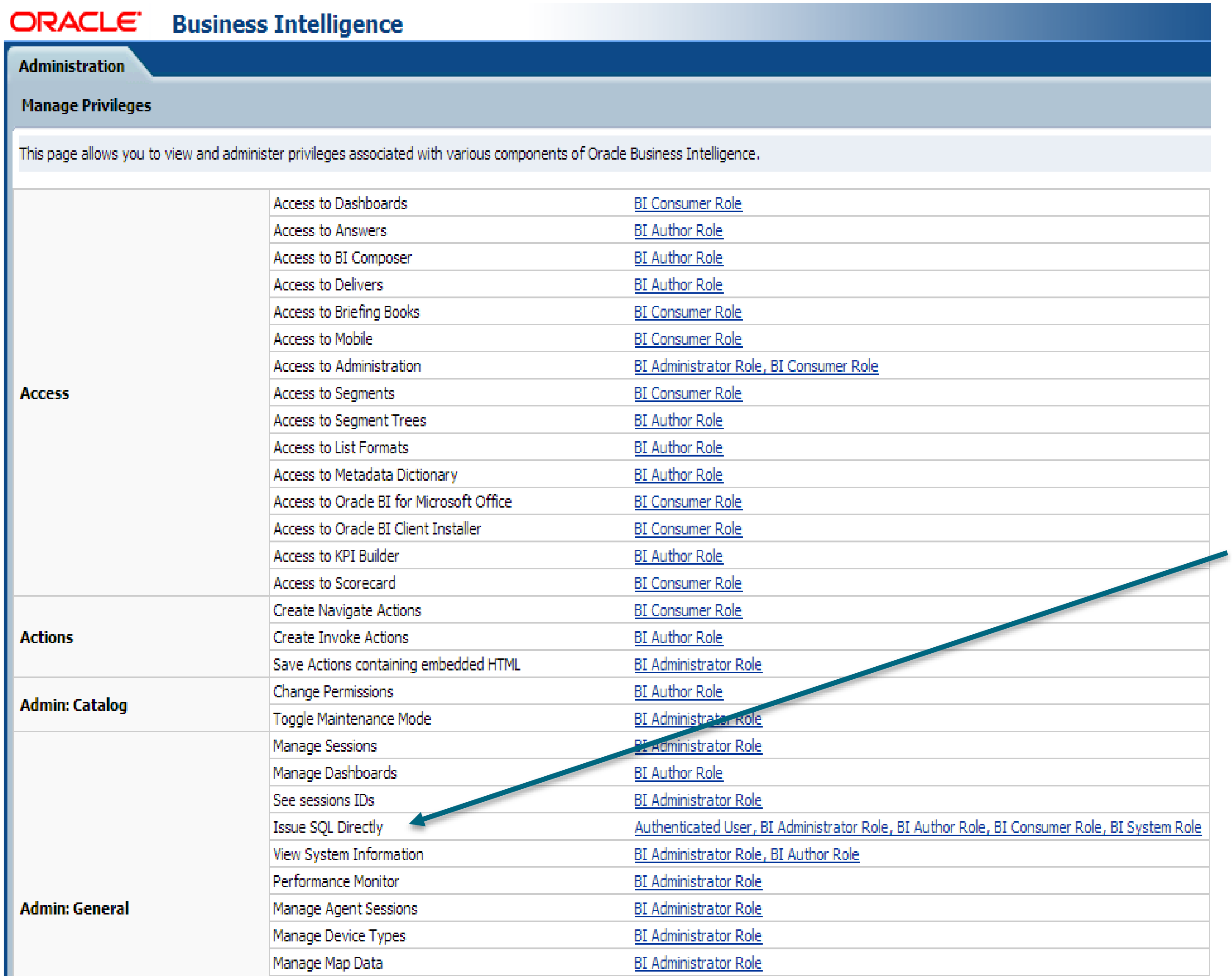
Available Columns

Columns in Report:

- ACL
- Accounts
- Caption ID
- Created
- Creator
- Description
- Description ID
- Folder
- Modified
- Modifier
- Must Have Permission
- Must Have Privilege
- Must NOT Have Permission
- Must NOT Have Privilege
- Name
- Owner
- Path
- Privilege
- Signature
- Tag

Presentation Catalog Security

- Administration Rights also set with ACLs
  - **Security ACL** is very important



Manage Privileges

This page allows you to view and administer privileges associated with various components of Oracle Business Intelligence.

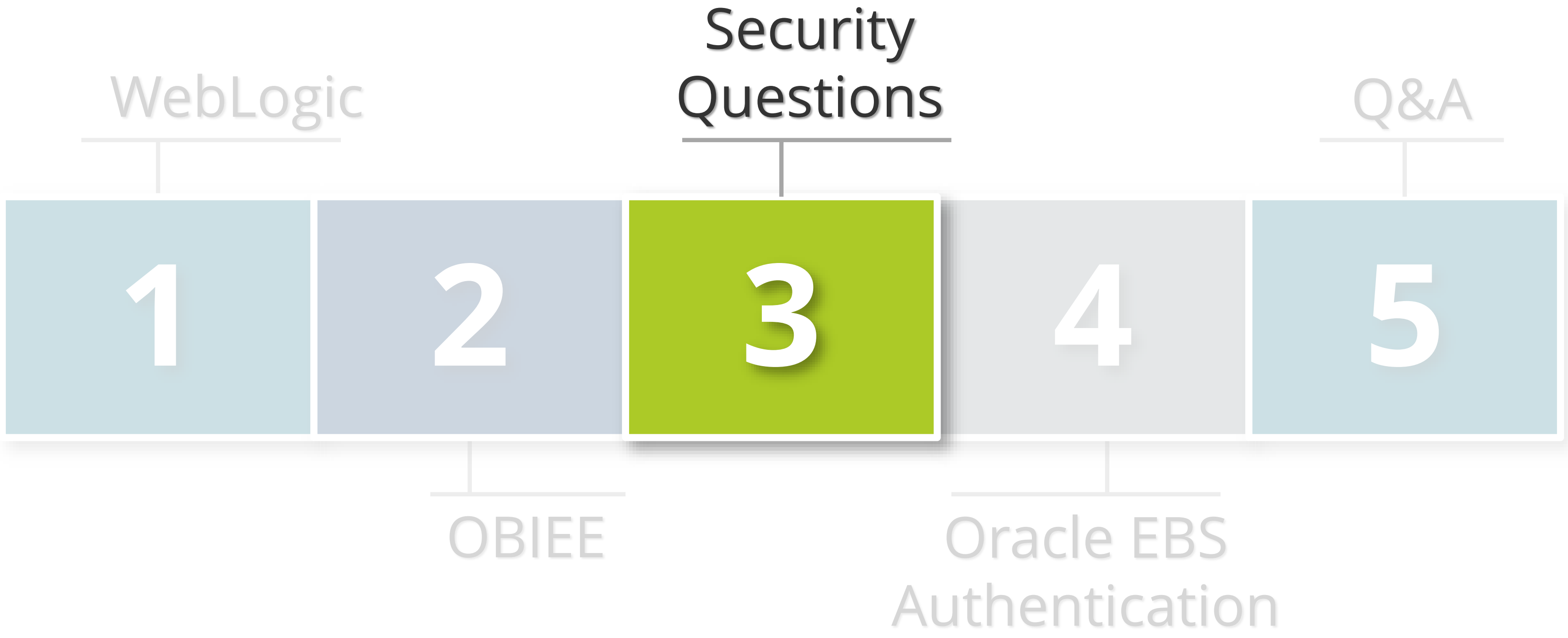
Access	Access to Dashboards	BI Consumer Role
	Access to Answers	BI Author Role
	Access to BI Composer	BI Author Role
	Access to Delivers	BI Author Role
	Access to Briefing Books	BI Consumer Role
	Access to Mobile	BI Consumer Role
	Access to Administration	BI Administrator Role, BI Consumer Role
	Access to Segments	BI Consumer Role
	Access to Segment Trees	BI Author Role
	Access to List Formats	BI Author Role
	Access to Metadata Dictionary	BI Author Role
	Access to Oracle BI for Microsoft Office	BI Consumer Role
	Access to Oracle BI Client Installer	BI Consumer Role
	Access to KPI Builder	BI Author Role
	Access to Scorecard	BI Consumer Role
Actions	Create Navigate Actions	BI Consumer Role
	Create Invoke Actions	BI Author Role
	Save Actions containing embedded HTML	BI Administrator Role
Admin: Catalog	Change Permissions	BI Author Role
	Toggle Maintenance Mode	BI Administrator Role
Admin: General	Manage Sessions	BI Administrator Role
	Manage Dashboards	BI Author Role
	See sessions IDs	BI Administrator Role
	Issue SQL Directly	Authenticated User, BI Administrator Role, BI Author Role, BI Consumer Role, BI System Role
	View System Information	BI Administrator Role, BI Author Role
	Performance Monitor	BI Administrator Role
	Manage Agent Sessions	BI Administrator Role
	Manage Device Types	BI Administrator Role
	Manage Map Data	BI Administrator Role

For example: Who can Issue SQL direct

OBIEE Security Changes with 11g

- **Users and groups no longer defined in RPD**
  - Defined now in WebLogic & OEM
- **Security policies mapped to Application Roles not groups**
  - Roles transcend ALL Fusion Applications
- **No more Administration user**
  - Any number of users have Admin privileges

Agenda



1 WebLogic

2 OBIEE

3 Security Questions

4 Oracle EBS Authentication

5 Q&A

#C14LV

OBIEE Security and Discussion Questions

- Permission reports
- Usage Tracking
- Key Accounts
- Act As/Impersonation
- Direct SQL Access
- GO URL

- Configuration migrations
- Writeback
- Time limits
- VPD support
- Source code control
- Logging and log levels

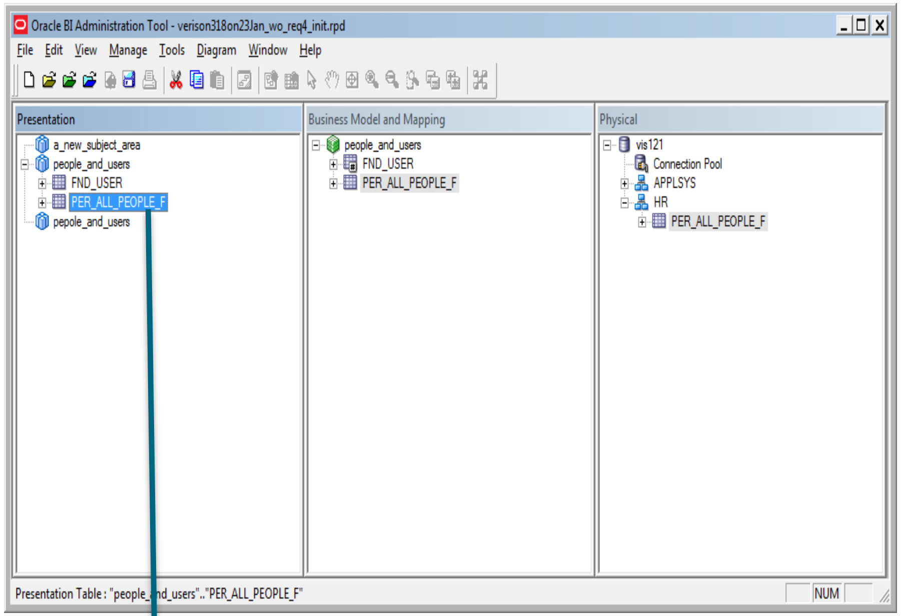
Key Accounts

Account	Security Issue
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
BI Admin User	Seeded end-user with full Administration rights to OBIEE
BI System User	Seeded account used for service-to-service authentication. Not intended to be used by users. Do not change password without following the specific Oracle support instructions.
OracleSystemUser	Seeded account created during installation. User name can be change later but need to follow instructions

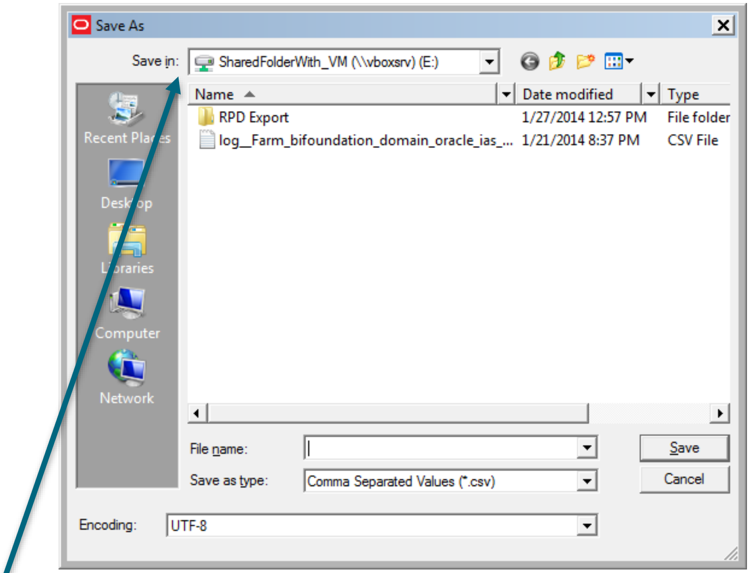
Ask Questions About …

Write-backs	▪ Connection pools can be flagged to allow users to update the database ▪ Who can and to what? ▪ Can they also issue Direct SQL?
Security configurations & migrations	▪ How are OPSS (policies and credentials) migrated from non-production to production? ▪ GUI or WLST?
Source code control	▪ Are RPD files under source code control? ▪ Are XML exports being used?

Ask For RPD Permission Reports



Presentation Table : "people_and_users".."PER_ALL_PEOPLE_F"



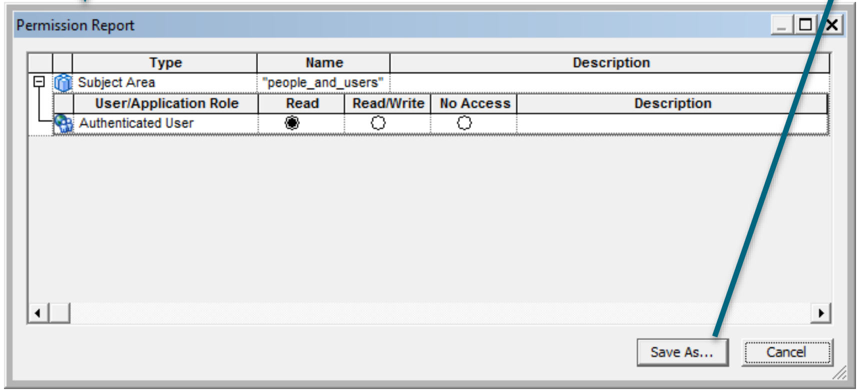
Save in: SharedFolderWith_VM (\\vboxsrv) (E:)

Name	Date modified	Type
RPD Export	1/27/2014 12:57 PM	File folder
log__Farm_bifoundation_domain_oracle_ias_...	1/21/2014 8:37 PM	CSV File

File name:

Save as type: Comma Separated Values (*.csv)

Encoding: UTF-8



Type	Name	Description
Subject Area	"people_and_users"	

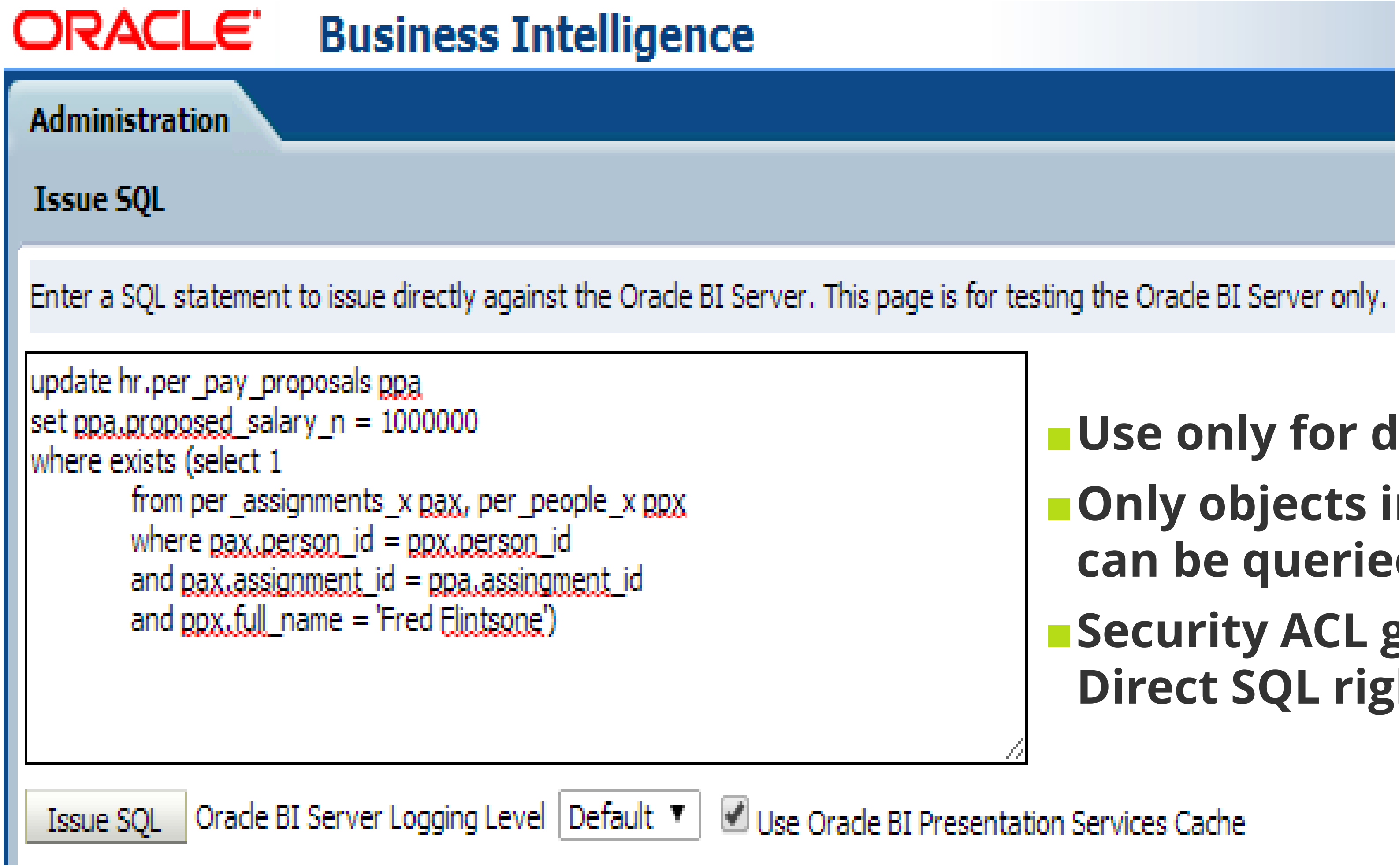
User/Application Role	Read	Read/Write	No Access	Description
Authenticated User	●	○	○	

Note: Permission reports do NOT include BMM or Physical filters and limits

Use OBIEE Usage Tracking

- **Oracle provides sample RPD**
  - Manually copy components into your RPD
- **Reports on changes to**
  - Enterprise manager configuration changes
  - RPD changes
  - Who ran what report when
- **Recommend redirect to log files**
  - Set STORAGE_DIRECTORY in NQSConfig.ini
  - Pass to centralized logging (e.g. Spunk, ArcSight, etc…)
  - Part of holistic log and audit solution

Direct SQL Access



Issue SQL

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')
```

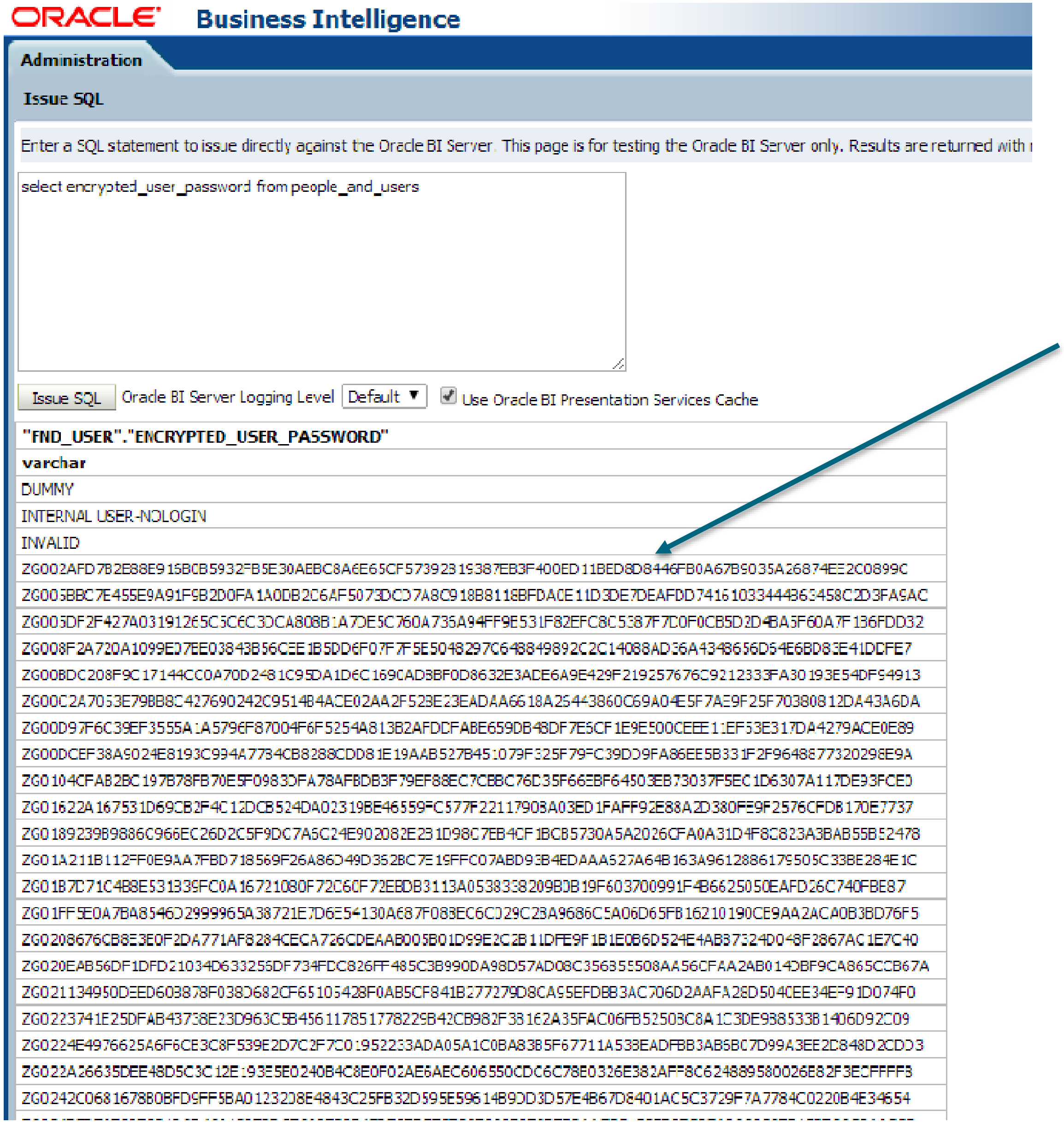
Oracle BI Server Logging Level: Default

☑ Use Oracle BI Presentation Services Cache

- Use only for debug
- Only objects in RPD can be queried
- Security ACL grants Direct SQL rights

#C14LV

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
```

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

"FND_USER"."ENCRYPTED_USER_PASSWORD"
varchar
DUMMY
INTERNAL USER-NOLOGIN
INVALID
ZG002AFD7B2E88E915B0B5932FB5E30AEBC8A6E65CF573923193387EB3F400ED11BED8D8446FB0A67B9035A26874EE2C0899C
ZG005BBC7E455E9A91F9B2D0FA1A0DB2C6AF5073DCD7A8C918B8118BFDA0E11D3DE7DEAFDD7416103344363458C2D3FA9AC
ZG005DF2F427A03191265C5C6C3DCA808B1A7DE5C760A735A94FF9E531F82EFC8C5387F7D0F0CB5D2D4BA5F60A7F136FDD32
ZG008F2A720A1099ED7EE03843B56CEE1B5DD6F07F7F5E5048297C648849892C2C14088AD36A4348656D54E6BD83E41DDFE7
ZG00BDC208F9C17144CC0A70D2481C95DA1D6C169CAD3BF0D8632E3ADE6A9E429F219257676C9212333FA30193E54DF94913
ZG00C2A7053E79BB8C427690242C9514B4ACE02AA2F523E23EADAA6618A25443860C69A04E5F7AE9F25F70380812DA43A6DA
ZG00D97F6C39EF3555A1A5796F87004F6F5254A813B2AFDCFABE659DB48DF7E5CF1E9E500CEEE11EF53E317DA4279ACE0E89
ZG00DCEF38A9024E8193C994A7734CB8288CDD81E19AAB527B451079F325F79FC39DD9FA86EE5B331F2F9648877320298E9A
ZG0104CFAB2BC197B78FB70E5F0983DFA78AFBDB3F79EF88EC7CBBC76D35F66EBF64503EB73037F5EC1D6307A117DE93FCED
ZG01622A167531D69CB2F4C12DCB524DA02319BE46559FC577F22117903A03ED1FAFF92E88A2D380FE9F2576CFDB170E7737
ZG0189239B9886C966EC26D2C5F9DC7A5C24E902082E231D98C7EB4CF1BCB5730A5A2026CFA0A31D4F8C823A3BAB55B52478
ZG01A211B112FF0E9AA7FBD718569F26A86D49D352BC7E19FFC07ABD93B4EDAAA527A64B163A9612886179505C33BE284E1C
ZG01B7D71C4B8E531339FC0A16721080F72C60F72EBDB3113A0538338209B0B19F603700991F4B6625050EAFD26C740FBE87
ZG01FF5E0A7BA8546D2999965A38721E7D6E54130A687F083EC6CD29C23A9686C5A06D65FB16210190CE9AA2ACA0B3BD76F5
ZG0208676CB8E3E0F2DA771AF8284CECA726CDEAAB005B01D99E2C2B11DFE9F1B1E0B6D524E4AB37324D048F2867AC1E7C40
ZG020EAB56DF1DFD21034D633256DF734FDC826FF485C3B990DA98D57AD08C356355508AA56CFAA2AB014DBF9CA865CCB67A
ZG021134950DEED603878F038D682CF65105428F0AB5CF841B277279D8CA95EFDBB3AC706D2AAFA28D5040EE34EF91D074F0
ZG0223741E25DFAB43738E23D963C5B456117851778229B42CB982F38162A35FAC06FB52503C8A1C3DE938533B1406D92C09
ZG0224E4976625A6F6CE3C8F539E2D7C2F7C01952233ADA05A1C0BA83B5F67711A533EADFBB3AB5B07D99A3EE2D848D2CDD3
ZG022A26635DEE48D5C3C12E193E5E0240B4C8E0F02AE6AEC606550CDC6C78E0326E382AFF8C624889580026E82F3ECFFFF3
ZG0242C0681678B0BFD9FF5BA0123208E4843C25FB32D595E59614B9DD3D57E4B67D8401AC5C3729F7A7784C0220B4E34654

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

Go URL 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
- Two options to issue SQL:
  - To data source(s) through RPD using saw.dll?Go&SQL
  - Directly against Oracle BI Server using saw.dll?Go&IssueRawSQL
- Syntax

  http://<yourserver>.com:9704/analytics/saw.dll?Go&SQL=select+thecolumn+from+subject_area

Go URL & SQL Access

- **Examples:**

Authenticate
http://db64.integrigy.com:9704/analytics/saw.dll?GO&NQUser=weblogic&NQPassword=Password1

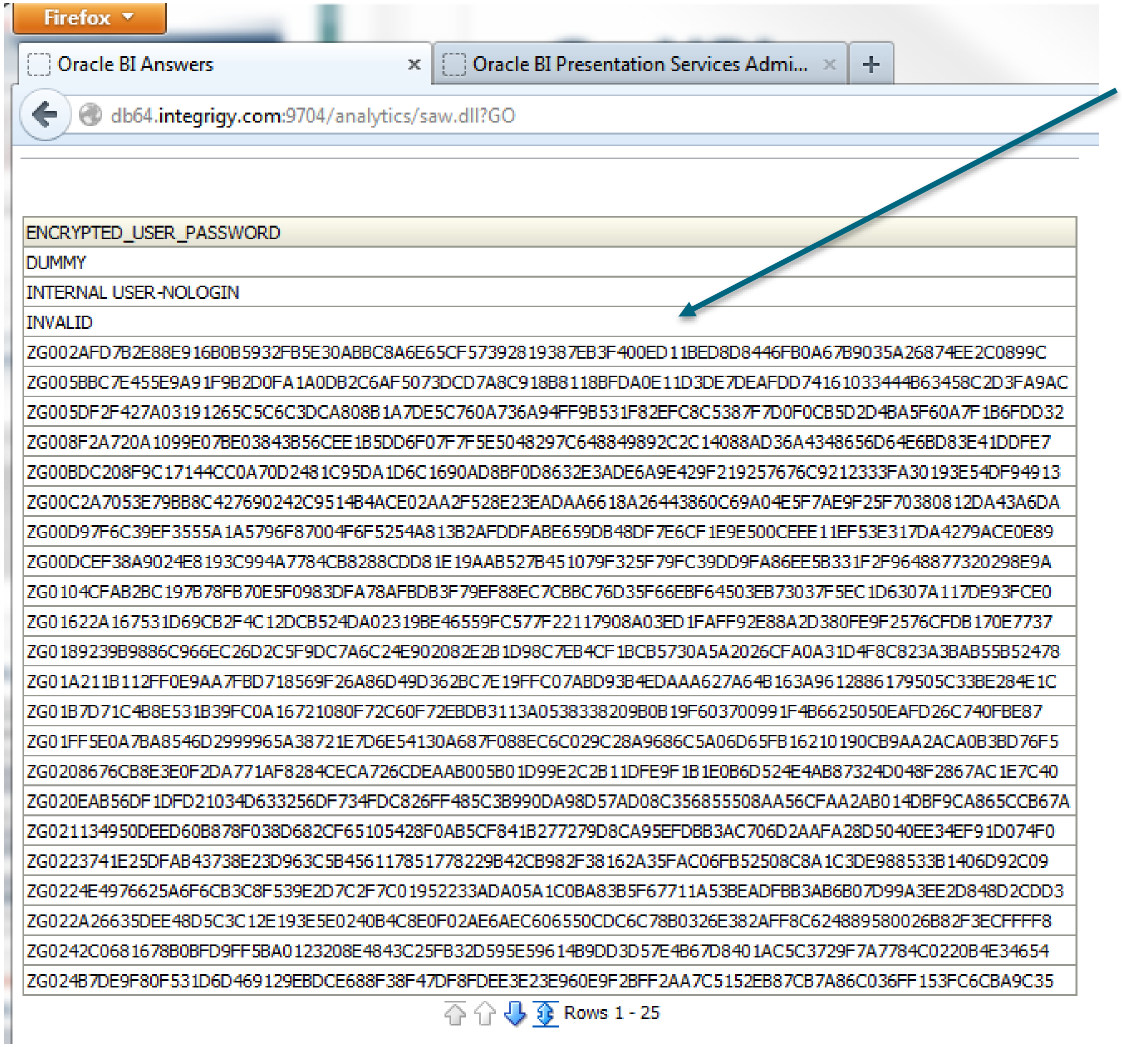
Issue SQL
http://testobiee:9704/analytics/saw.dll?Go&SQL=**select+person+salary+from+hr_salary_info**

http://db64.integrigy.com:9704/analytics/saw.dll?Go&SQL=select+**encrypted_user_password**+from+people_and_users

The FROM clause is the name of the Subject Area to query

Go URL SQL Access

http://db64.integrigy.com:9704/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
ZG005BBC7E455E9A91F9B2D0FA1A0DB2C6AF5073DCD7A8C918B8118BFDA0E11D3DE7DEAFDD74161033444B63458C2D3FA9AC
ZG005DF2F427A03191265C5C6C3DCA808B1A7DE5C760A736A94FF9B531F82EFC8C5387F7D0F0CB5D2D4BA5F60A7F1B6FDD32
ZG008F2A720A1099E07BE03843B56CEE1B5DD6F07F7F5E5048297C648849892C2C14088AD36A4348656D64E6BD83E41DDFE7
ZG00BDC208F9C17144CC0A70D2481C95DA1D6C1690AD8BF0D8632E3ADE6A9E429F219257676C9212333FA30193E54DF94913
ZG00C2A7053E79BB8C427690242C9514B4ACE02AA2F528E23EADAA6618A26443860C69A04E5F7AE9F25F70380812DA43A6DA
ZG00D97F6C39EF3555A1A5796F87004F6F5254A813B2AFDDFABE659DB48DF7E6CF1E9E500CEEE11EF53E317DA4279ACE0E89
ZG00DCEF38A9024E8193C994A7784CB8288CDD81E19AAB527B451079F325F79FC39DD9FA86EE5B331F2F9648877320298E9A
ZG0104CFAB2BC197B78FB70E5F0983DFA78AFBDB3F79EF88EC7CBBC76D35F66EBF64503EB73037F5EC1D6307A117DE93FCE0
ZG01622A167531D69CB2F4C12DCB524DA02319BE46559FC577F22117908A03ED1FAFF92E88A2D380FE9F2576CFDB170E7737
ZG0189239B9886C966EC26D2C5F9DC7A6C24E902082E2B1D98C7EB4CF1BCB5730A5A2026CFA0A31D4F8C823A3BAB55B52478
ZG01A211B112FF0E9AA7FBD718569F26A86D49D362BC7E19FFC07ABD93B4EDAAA627A64B163A9612886179505C33BE284E1C
ZG01B7D71C4B8E531B39FC0A16721080F72C60F72EBDB3113A0538338209B0B19F603700991F4B6625050EAFD26C740FBE87
ZG01FF5E0A7BA8546D2999965A38721E7D6E54130A687F088EC6C029C28A9686C5A06D65FB16210190CB9AA2ACA0B3BD76F5
ZG0208676CB8E3E0F2DA771AF8284CECA726CDEAAB005B01D99E2C2B11DFE9F1B1E0B6D524E4AB87324D048F2867AC1E7C40
ZG020EAB56DF1DFD21034D633256DF734FDC826FF485C3B990DA98D57AD08C356855508AA56CFAA2AB014DBF9CA865CCB67A
ZG021134950DEED60B878F038D682CF65105428F0AB5CF841B277279D8CA95EFDBB3AC706D2AAFA28D5040EE34EF91D074F0
ZG0223741E25DFAB43738E23D963C5B456117851778229B42CB982F38162A35FAC06FB52508C8A1C3DE988533B1406D92C09
ZG0224E4976625A6F6CB3C8F539E2D7C2F7C01952233ADA05A1C0BA83B5F67711A53BEADFBB3AB6B07D99A3EE2D848D2CDD3
ZG022A26635DEE48D5C3C12E193E5E0240B4C8E0F02AE6AEC606550CDC6C78B0326E382AFF8C624889580026B82F3ECFFFF8
ZG0242C0681678B0BFD9FF5BA0123208E4843C25FB32D595E59614B9DD3D57E4B67D8401AC5C3729F7A7784C0220B4E34654
ZG024B7DE9F80F531D6D469129EBDCE688F38F47DF8FDEE3E23E960E9F2BFF2AA7C5152EB87CB7A86C036FF153FC6CBA9C35

This test user CANNOT issue Direct SQL but still can query with Go URL

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

Act-As and Impersonation

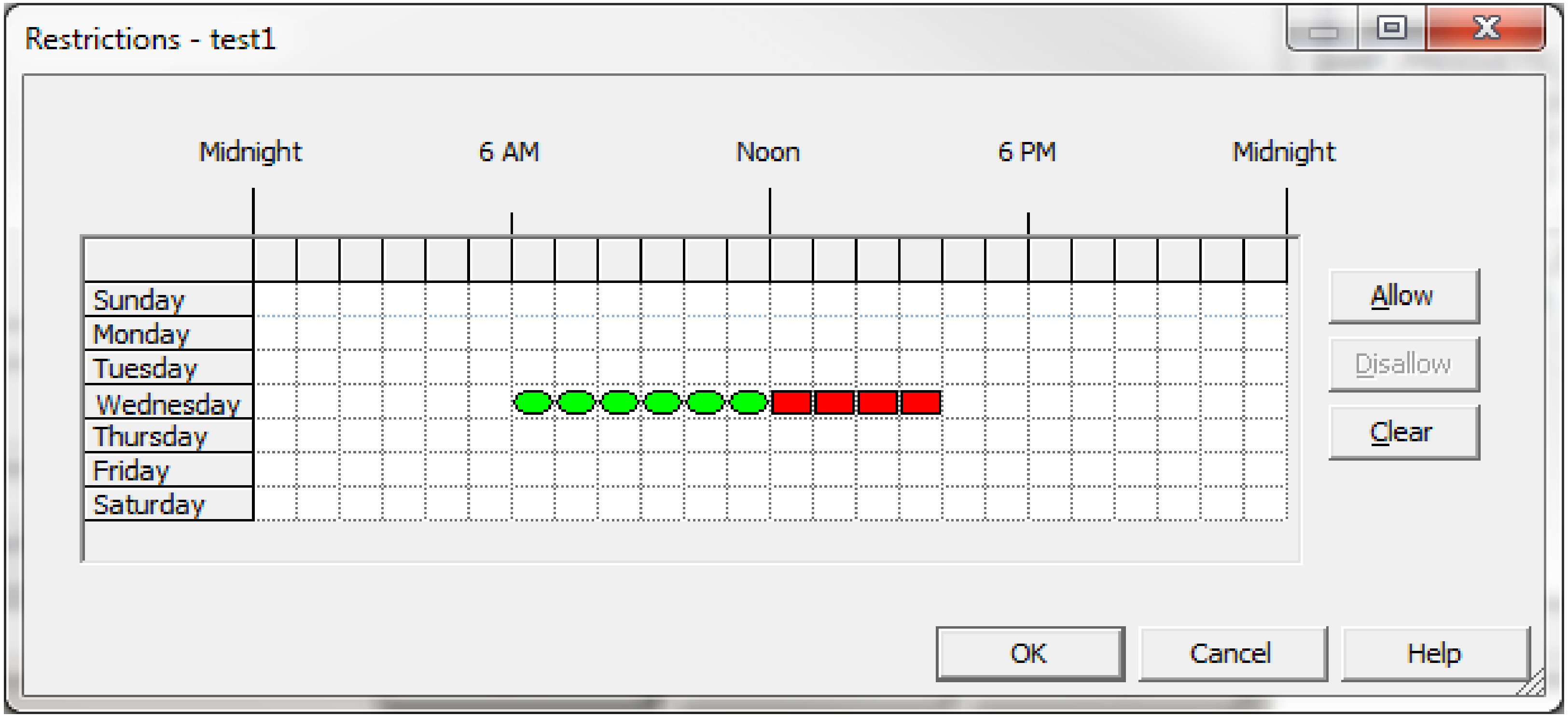
	Impersonate	Act-As
Level of access	Full access	Full or read-only access, on a single user
Users whose identity can be assumed by the proxy user	Any and all users, anytime	Defined list of users
Access method	Construct URL manually	Standard functionality of UI
How to know if being used	No indication given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

Log Levels and Logs

BI Component	Log File
OPMN	debug.log
OPMN	opmn.log
BI Server	nqserver.log
BI Server Query	nquery<n>.log <n>=data and timestamp for example nqquery-20140109-2135.log
BI Cluster Controller	nqcluster.log
Oracle BI Scheduler	nqscheduler.log
Usage Tracking	NQAcct.yyymmdd.hhmmss.log
Presentation Services	sawlog*.log (for example, sawlog0.log)
BI JavaHost	jh.log

- Holistic logging solution
  - WebLogic
  - OBIEE
  - Data sources
- OBIEE Logging Level
  - Set in BI Admin Tool
    - Users only, not possible for roles
  - Log Levels 0 to 7

Time Restrictions for Roles and Users



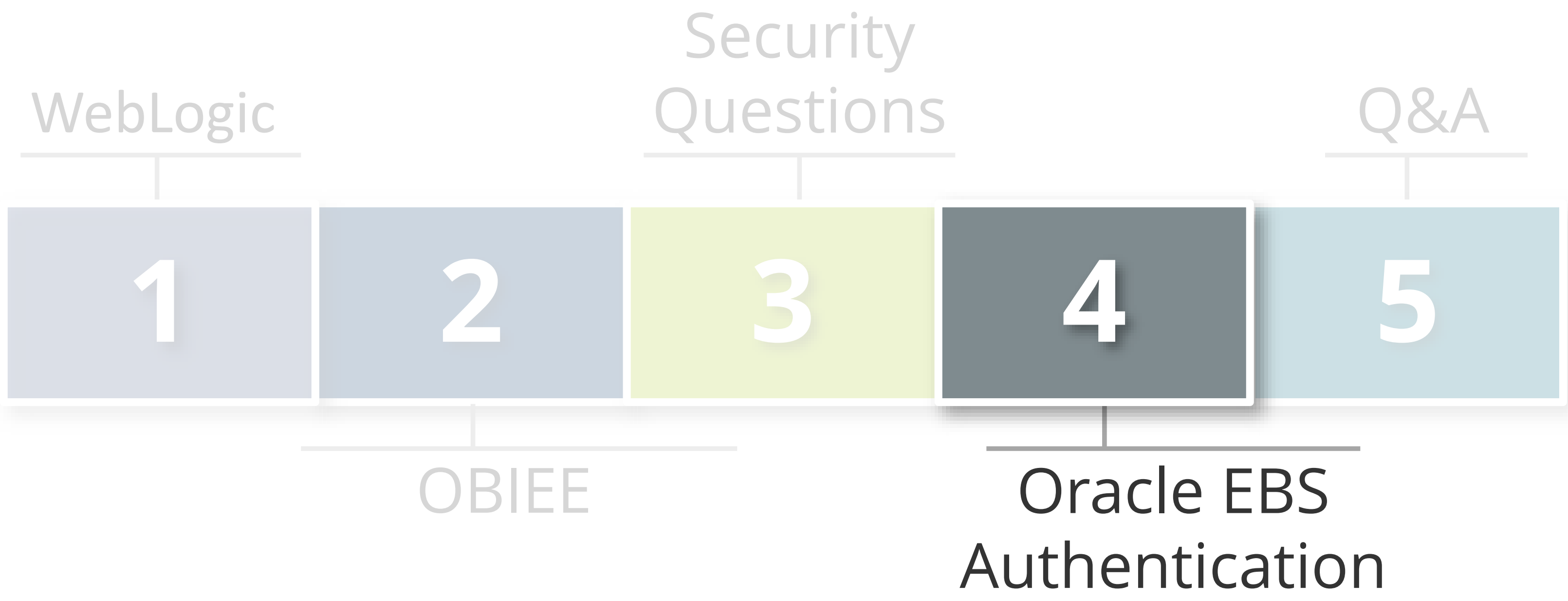
Sunday																								
Monday																								
Tuesday																								
Wednesday							🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟥								
Thursday																								
Friday																								
Saturday																								

VPD, Data Vault and Row Level Security

- **Is a connection with VPD or Data Vault being used?**
  - What are the rules?

- **Which is better VPD, Data Vault or OBIEE row level security?**
  - VPD and Data Vault protect data at the data source
    - Is OBIEE the only consumer or user?

Agenda



1 WebLogic

2 OBIEE

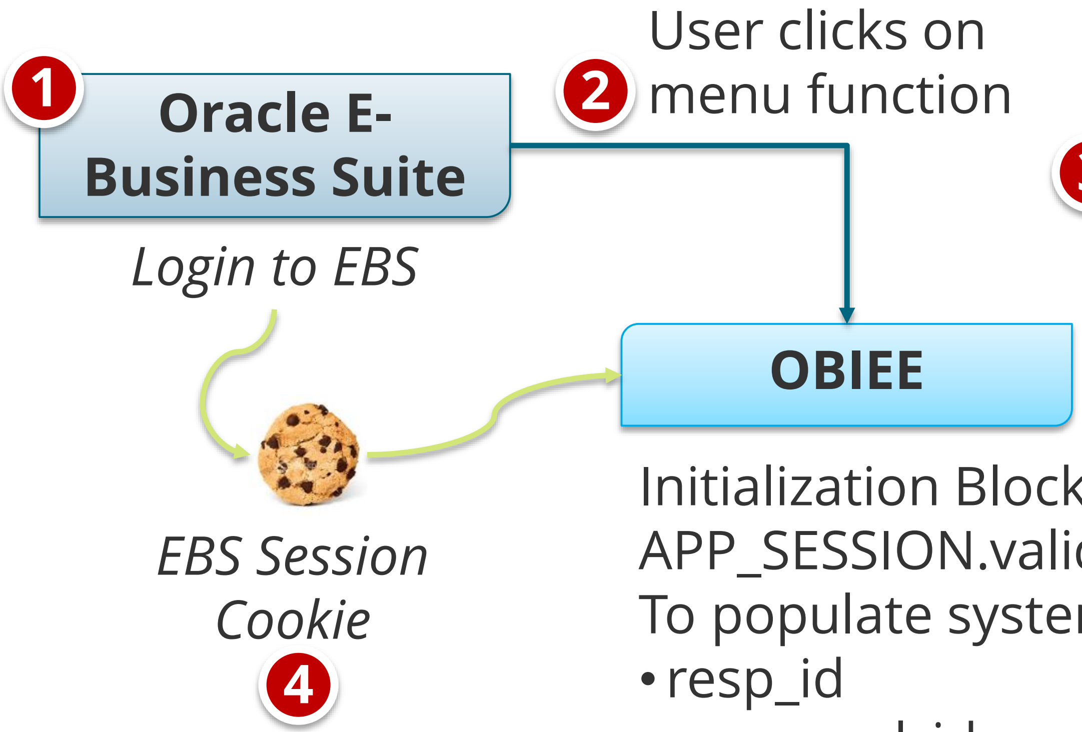
3 Security Questions

4 Oracle EBS Authentication

5 Q&A

Oracle E-Business Suite Authentication

Access through E-Business not SSO



1 Oracle E-Business Suite

Login to EBS

2 User clicks on menu function

OBIEE

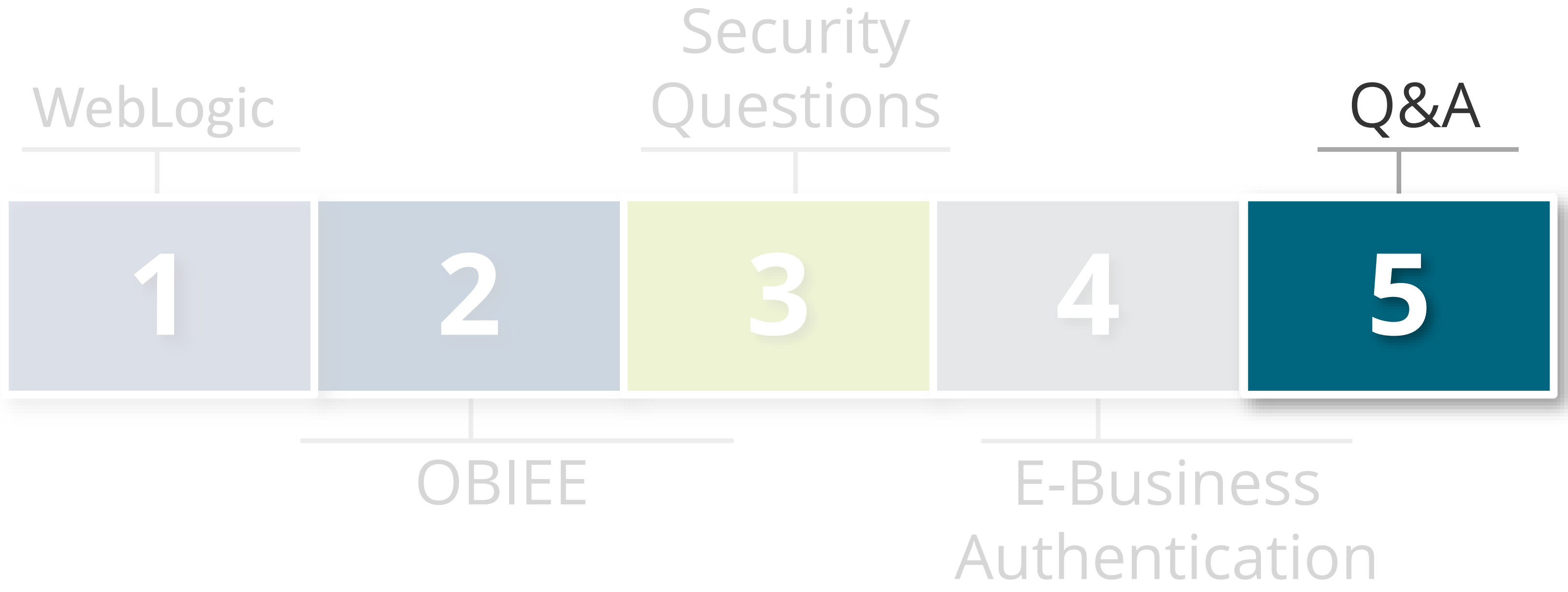
EBS Session Cookie 4

3 Function built using SSW OracleOasis.jsp which generates URL based on System Profile Option ‘FND: Oracle Business Intelligence Suite EE base URL’

Initialization Block calls EBS APP_SESSION.validate_icx_session
To populate system variables for:

- resp_id
- resp_appl_id
- security_group_id
- resp_name
- user_id
- employee_id
- user_name

Agenda



1 WebLogic

2 OBIEE

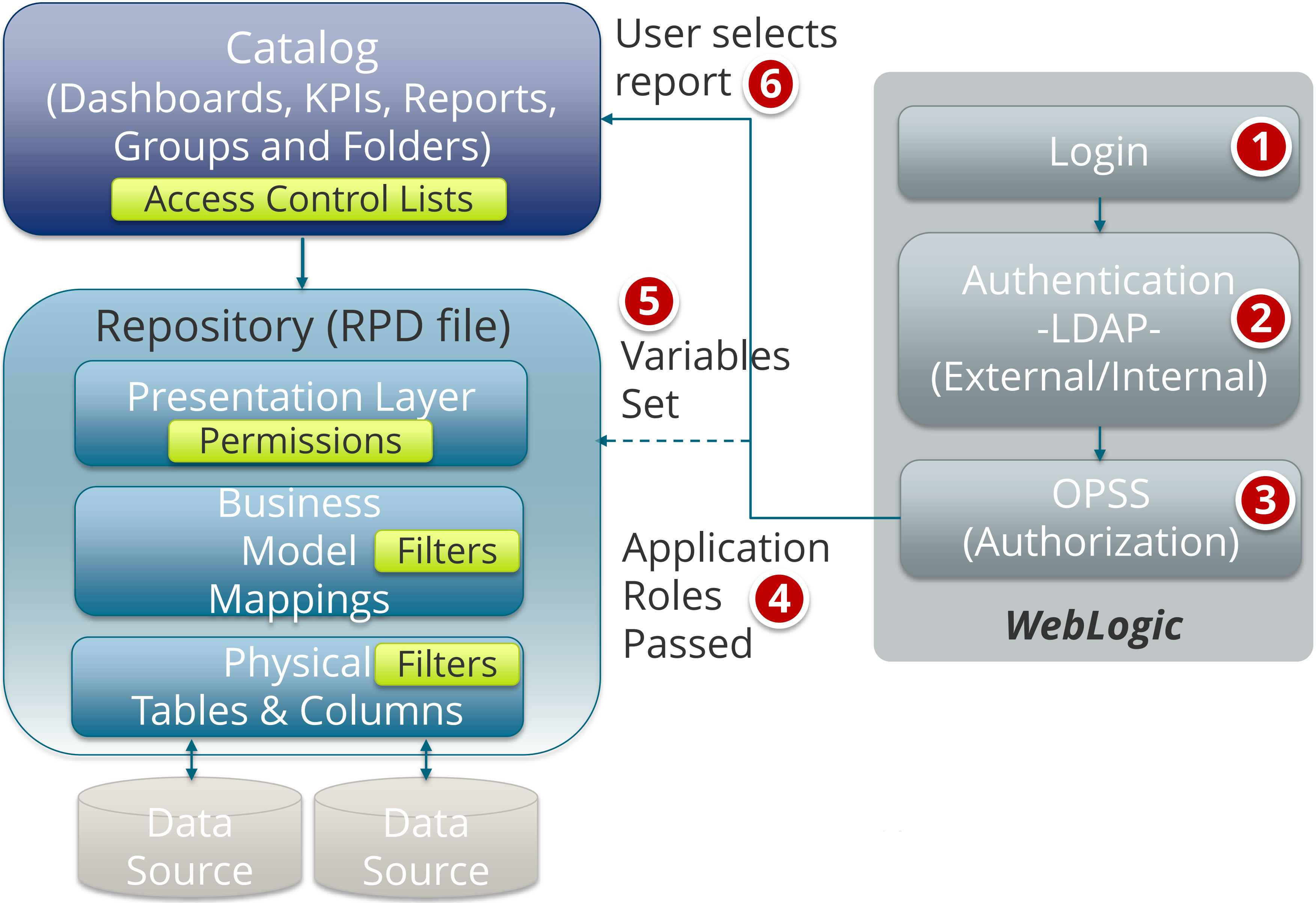
3 Security Questions

4 E-Business Authentication

5 Q&A

#C14LV

OBIEE Security



Really Good References

- OBIEE Security Examined, Integrigy, March 2014
  - http://www.integrigy.com/security-resources/obiee-security-examined
- Oracle Business Intelligence Enterprise Edition (OBIEE) Product Information Center (PIC) ID 1267009.1
- “Oracle Fusion Middleware Security Overview, 11*g* Release 1 (11.1.1)”, Oracle Corporation, May 2009, E12889-01
- “Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server 11*g* Release 1 (10.3.4)”, Oracle Corporation, January 2011, E13705-04
- “Oracle WebLogic Server WebLogic Scripting Tool10g Release 3 (10.3)”, Oracle Corporation, July 2008, E15051-01

Contact Information

Mike Miller

Chief Security Officer

Integrigy Corporation

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

web: **www.integrigy.com**

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

youtube: **youtube.com/integrigy**