



# Oracle Business Intelligence 11g Masterclass

Oracle BI & FMW11g Security

T : +44 (0) 8446 697 995 or (888) 631 1410 (USA) E : [enquiries@rittmanmead.com](mailto:enquiries@rittmanmead.com) W: [www.rittmanmead.com](http://www.rittmanmead.com)

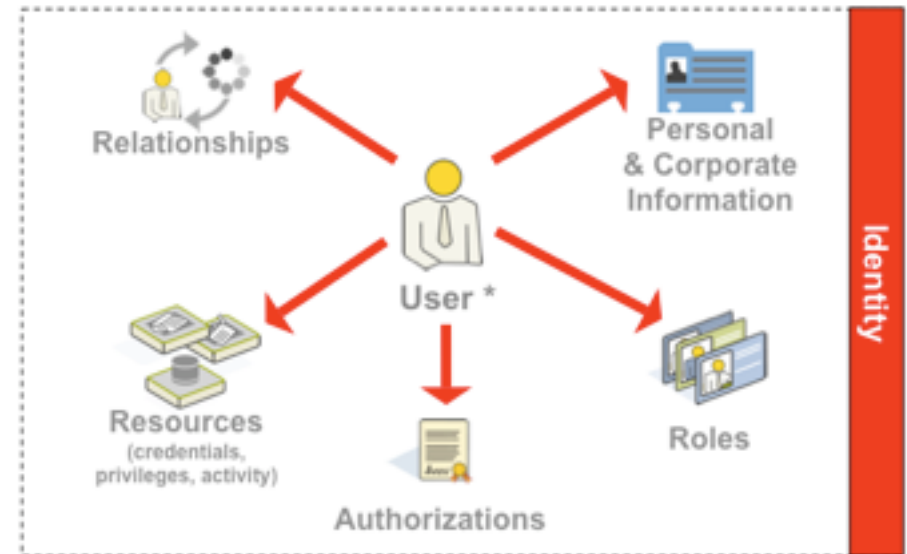
## Agenda

---

- What do we mean by “security”?
- What needs to be managed as part of OBIEE security?
- OBIEE 11g security overview
- Oracle Fusion Middleware 11g security overview
- Backward-compatibility with OBIEE 10g security
- Application Roles and Application Policies explained
- Performing common security tasks

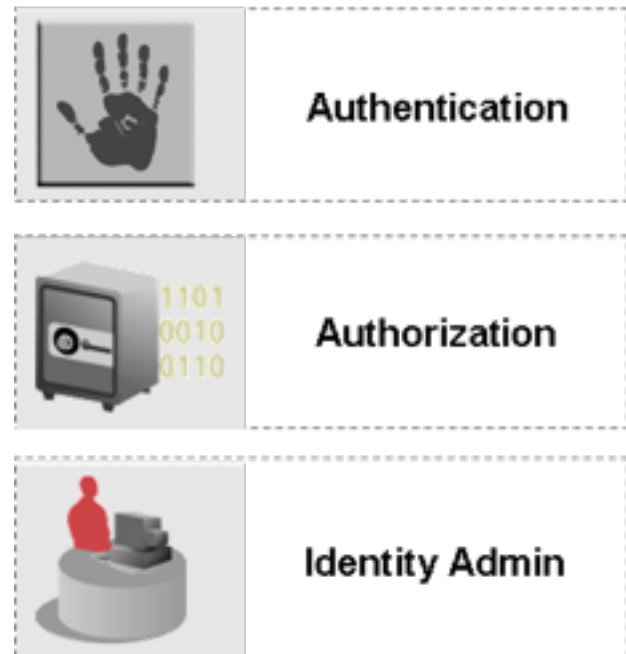
## What Are We Talking About, When We Talk About Security?

- Security encompasses a wide area and set of tasks in OBIEE
- Aspects of security include:
  - ▶ Users logging in and out
  - ▶ User and group directories, internal and external to OBIEE
  - ▶ User and group membership administration
  - ▶ Job roles, rights and permissions
  - ▶ Permissions on BI objects (reports, dashboards, KPIs etc)
  - ▶ Application permissions (to use Answers, to create filters etc)
  - ▶ Security auditing



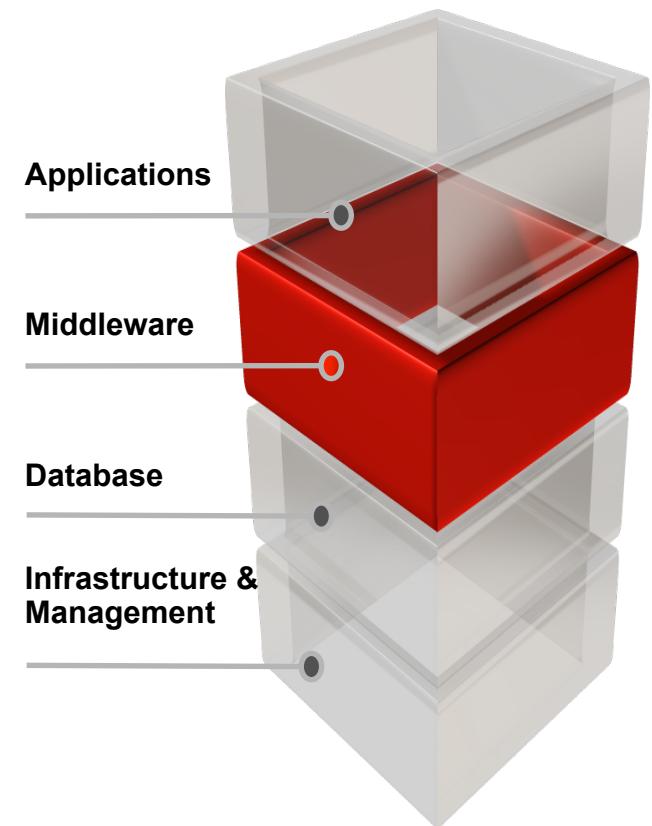
## Authentication, Authorization and Administration

- Security can be thought of as having three major aspects
  - ▶ Authentication: proving you are who you say you are
  - ▶ Authorization: what you have access to, when, where
  - ▶ Profile: attributes about you
- Security also has a lifecycle, and is a continuous process
  - ▶ Initial hire > promotion > departure
- How we “onboard” new users onto the BI system is very important
  - ▶ Granting access to applications
  - ▶ Scoping their view of data



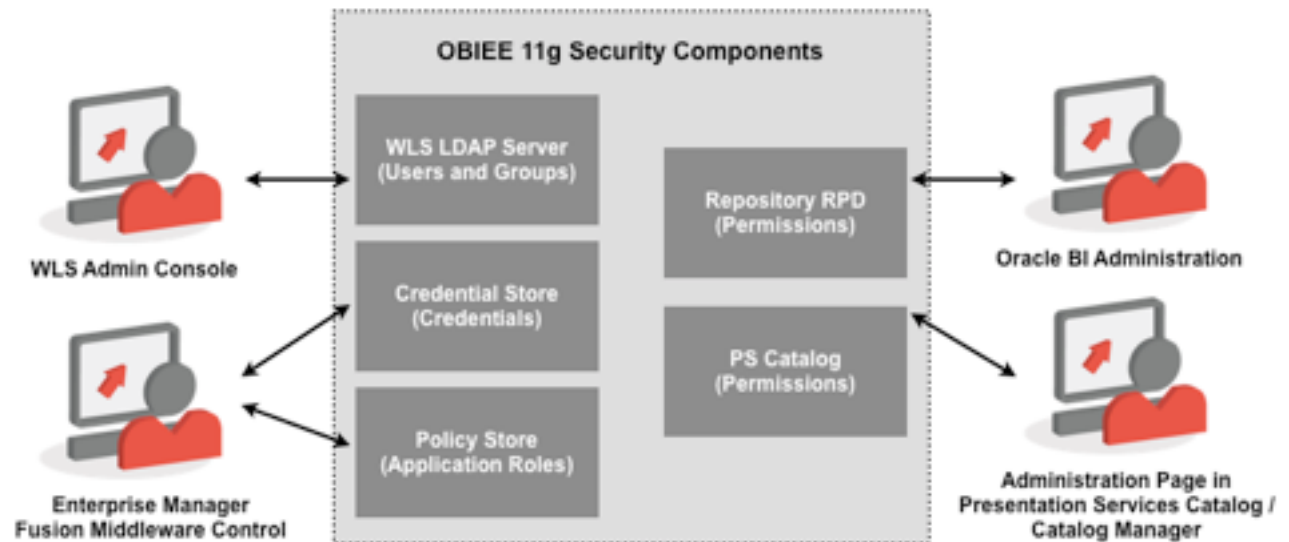
## OBIEE 11g Security and Oracle Fusion Middleware 11g

- OBIEE 11g delegates security to Oracle Fusion Middleware 11g
  - ▶ Leverages Oracle Platform Security Services
- Users and Groups in RPD now moved to embedded WLS LDAP Server
  - ▶ RPD and Webcat groups replaced by FMW11g Application Roles
- Comprehensive SSL and Credentials Management
- Encrypted RPD, plus optional report encryption and watermarking
- Flexible authorization model through WLS and OPSS
- Still backwards compatible with LDAP model in OBIEE 10g



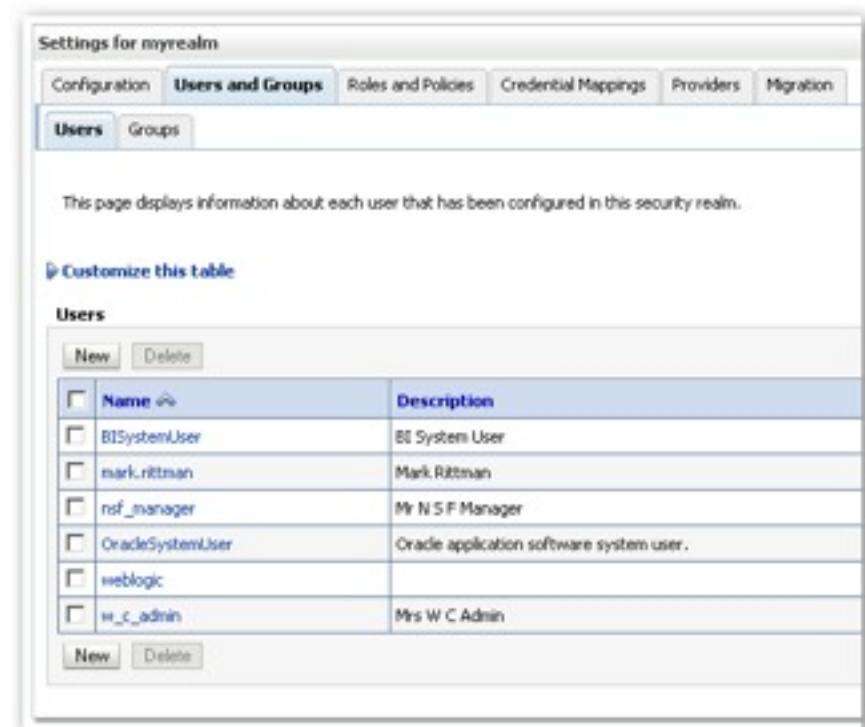
## OBIEE 11g Security Administration Tools

- WebLogic Server Admin Server (LDAP Server, Security Providers)
- Fusion Middleware Control (Application Roles)
- BI Administration tool (subject-area, and row-level security)
- Catalog Manager, and Presentation Services Catalog View (object permissions)
- Presentation Services Administration Page (PS functional permissions)



## WLS Embedded LDAP Server

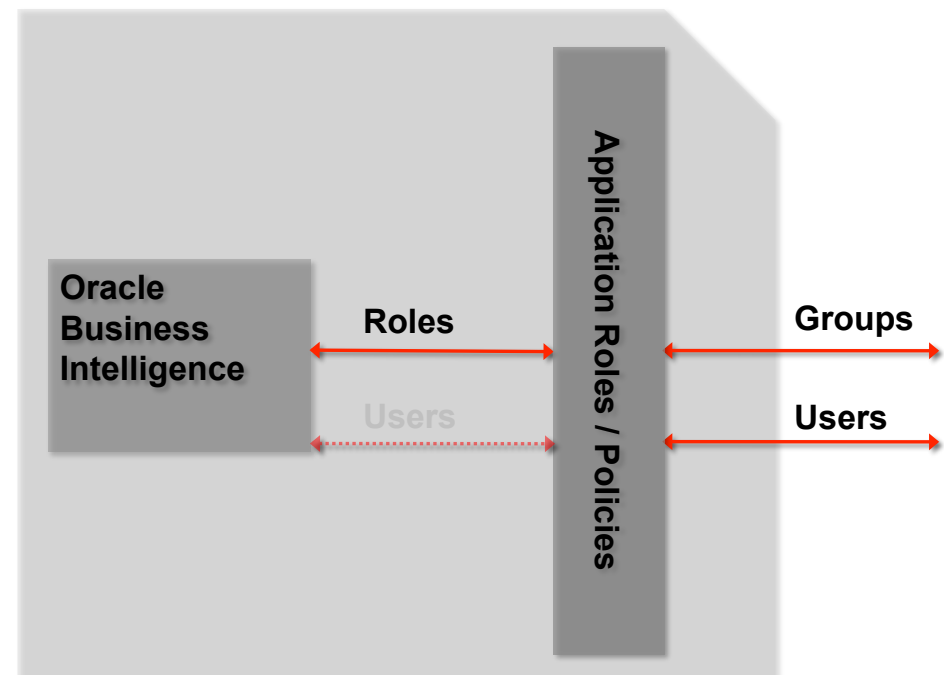
- By default, OBIEE 11g users and groups are now held in the WLS LDAP Server
  - ▶ More robust directory for storing user details
  - ▶ Recommended for >1000 users
- WLS Admin Server Console now used for creating and maintaining users
- BI Server “outsources” all authentication, authorization to FMW11g
- BI Administration tool now used for subject area and row-level security, connection pool passwords only
- WLS LDAP Server can be “swapped out” for alternative directories (MS AD etc)





## Application Roles and Application Policies

- Application roles introduce an indirection between LDAP groups and BI groups
  - ▶ LDAP server provides users, groups
  - ▶ FMW11g provides application roles
  - ▶ Application roles are granted to LDAP users, groups
  - ▶ Permissions are assigned to application roles
- Breaks direct link between groups and roles
- Application roles can be exported between FMW11g environments
- All RPD, webcat permissions secured against application roles





## Application Roles in Use

- Application Roles, Application Policies, and Role-LDAP Group mappings are defined using Fusion Middleware Control
- Oracle BI Administration, and Oracle Presentation Services administration page, are used for assigning permissions to these roles.

**Policy Store Provider**

Scope: WebLogic Domain  
Provider: XML  
Location: ./system-jazn-data.xml

**Search**

Enter search keyword for role name to query roles defined by this application. Use application stripe to s

Select Application Stripe to Search: ☒ obi

Role Name:

**Create** **Create Like** **Edit** **Delete**

Role Name	Members	Description
BISystem	BISystemUser	
BIAdministrator	BIAdministrators	
BIAuthor	BIAuthors, BIAdministrator	
BIConsumer	BIConsumers, BIAuthor, authenticated-role	

**Permissions - Sales - Store Quality**

☒ Show all users/application roles

User/Applicat	Read	Read/Write	No Access	Default
Everyone	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Default
BIAdministrator	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
BIAuthor	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
BICentralSFMan	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
BIConsumer	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
BINorthCAMana	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
BINorthSFMana	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
BIOtherUSAMar	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
BISouthSFMana	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
BISystem	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
BIWebCatAdmin	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
BISystemUser	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
mark.rittman	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

OK Cancel Help



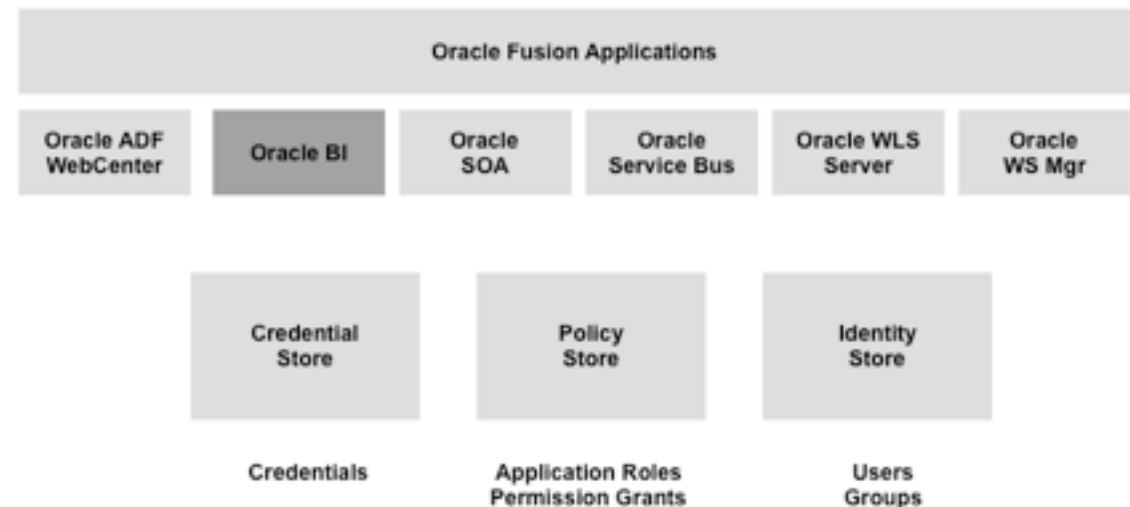
## Demonstration

OBIEE 11g Users, Groups and Application Policies

T : +44 (0) 8446 697 995 or (888) 631 1410 (USA) E : [enquiries@rittmanmead.com](mailto:enquiries@rittmanmead.com) W: [www.rittmanmead.com](http://www.rittmanmead.com)

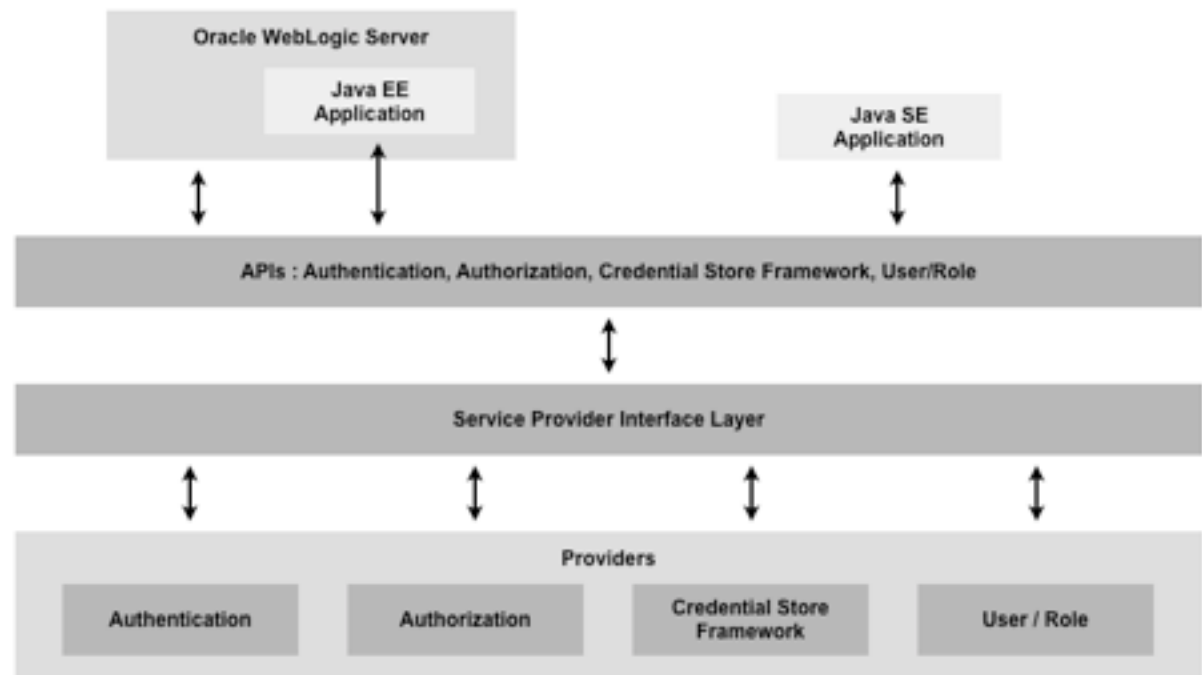
## OBIEE Security Providers

- OBIEE 11g (through FMW11g) uses three **Security Providers**
  - ▶ Authentication Provider (defaults to WLS LDAP Server)
  - ▶ Policy Store Provider (defaults to WLS)
  - ▶ Credential Store Provider (defaults to WLS)
- Flexible security framework that allows easy linking to external security
- All enabled through **Oracle Platform Security Services**



## Oracle Platform Security Services

- Standards-based, portable, integrated enterprise-grade security framework
- Underlying security platform that provides security to Fusion Middleware 11g
- Abstraction layer in the form of API that insulate applications from security infrastructure

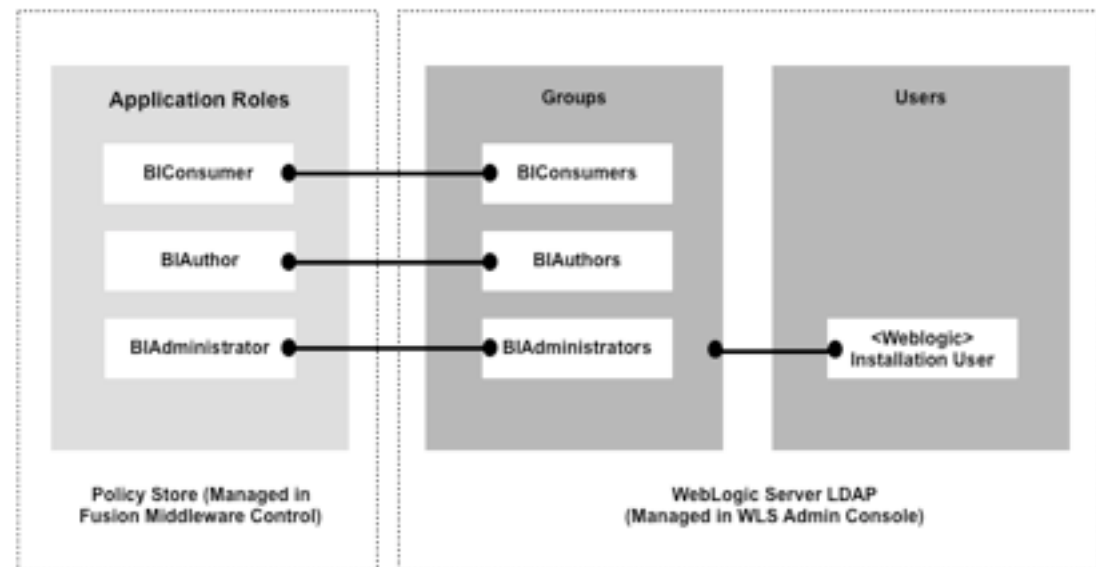


## OPSS Key Concepts

- Application Role
  - ▶ A defined job, role to which permissions are assigned
  - ▶ Example : Marketing Manager, WebCat Administrator
- Credential Store
  - ▶ A secure location for placing usernames, passwords required for inter-application authentication
- Application Policies and Permissions
  - ▶ Application Policies are collections of permissions assigned to roles
- Identity Store
  - ▶ LDAP Server, Database etc that stores users and groups
- Policy Store
  - ▶ Files, database etc that stores application roles and policies
- WLS Embedded LDAP Server
  - ▶ The built-in LDAP Server within WLS (restricted-use license)

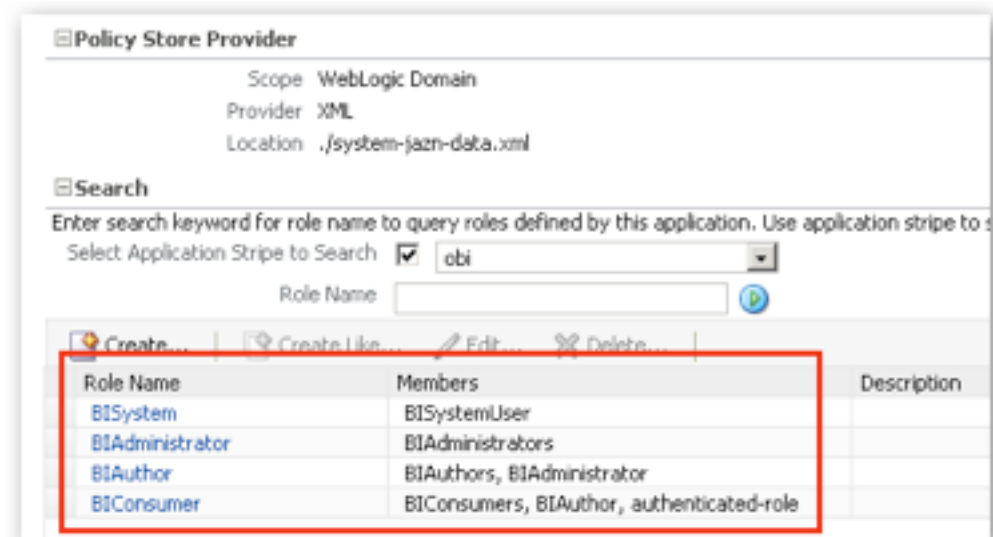
## OBIEE 11gR1 Default Security Configuration

- OBIEE 11gR1 comes with a Default Security Configuration
  - WLS LDAP Server is the default Authentication Provider
  - WLS file-based policy and credential stores are used for Policy Store Provider and Credential Provider
- Default application roles and groups
- WLS admin user (weblogic) is default administrator
- Default configuration can be amended or extended as required
  - Create new roles
  - Plug-in external directory



## Default Application Roles

- **BIAdministrator** (mapped to BIAdministrators LDAP group)
  - ▶ Can edit and create new RPDs, web catalog
  - ▶ Full control over all aspects of OBIEE
- **BIAuthor** (mapped to BIAuthors LDAP group)
  - ▶ Can create and amend Answers analyses, dashboards etc
  - ▶ Can create and amend BI Publisher reports etc
- **BIConsumer** (mapped to BIConsumers LDAP group)
  - ▶ Can run existing analyses, dashboards, reports



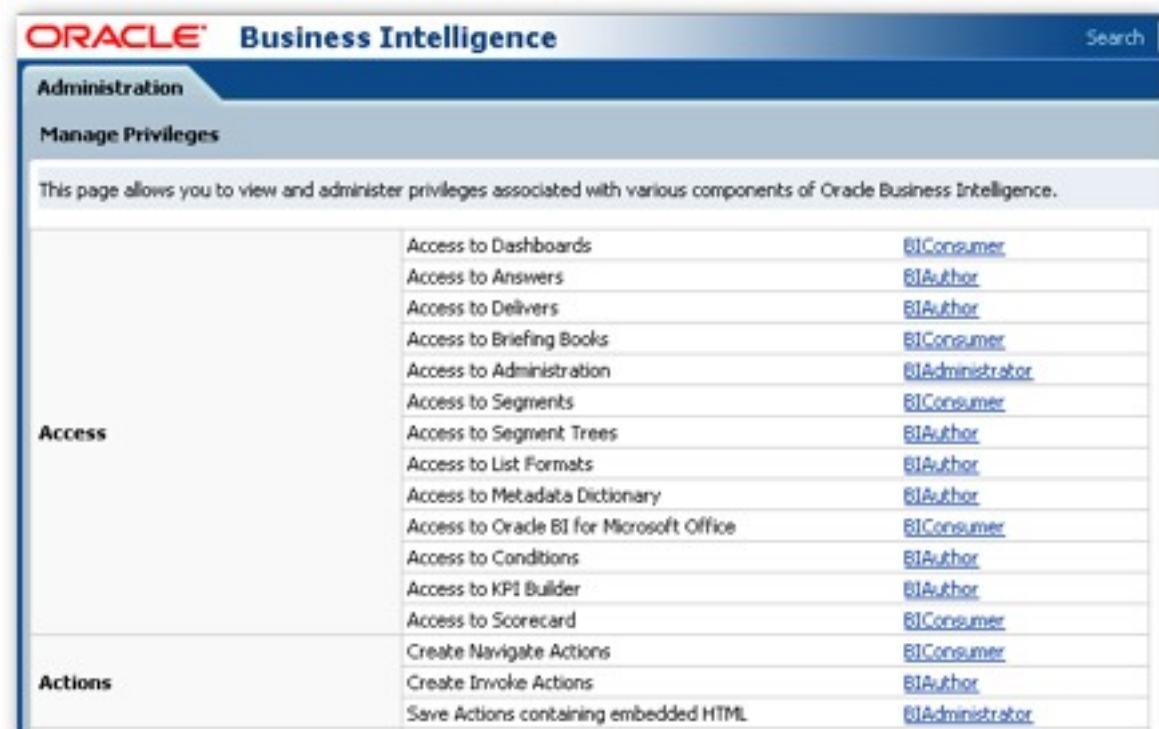


- Policies are containers for permissions, made up of resource types and resource permissions, for example
  - ▶ `resourceType=oracle.bi.server.permission`
  - ▶ `resourceName=oracle.bi.server.manageRepositories`
- Used at high-level for OBIEE system components to provide admin rights
  - ▶ RPD and Webcat permissions provide granular control
- Used more granularly for Java components (BIP etc)
- Granted to application roles, and both stored together in the policy store

**T : +44 (0) 8446 697 995 or (888) 631 1410 (USA) E : [enquiries@rittmanmead.com](mailto:enquiries@rittmanmead.com) W: [www.rittmanmead.com](http://www.rittmanmead.com)**

## Granting Granular Presentation Server Privileges

- Whilst the policy store determines at high level whether web catalog can be accessed or edited, Presentation Services Administration page determines more granular application rights
  - ▶ Access to Answers
  - ▶ Create Action Types
  - ▶ Execute Direct SQL
  - ▶ Download Briefing Book
  - ▶ Edit Column Formulas
  - ▶ etc

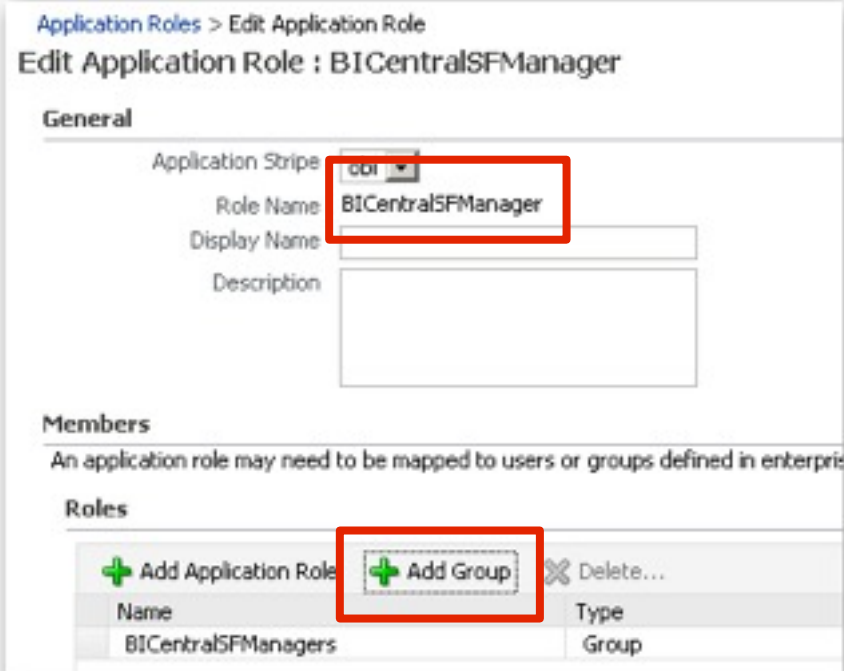


The screenshot shows the 'Manage Privileges' page in the Oracle Business Intelligence Administration console. It lists various components and the privileges assigned to them. The page is divided into two main sections: 'Access' and 'Actions'.

Category	Privilege	Assigned To
Access	Access to Dashboards	<a href="#">BIConsumer</a>
	Access to Answers	<a href="#">BIAuthor</a>
	Access to Delivers	<a href="#">BIAuthor</a>
	Access to Briefing Books	<a href="#">BIConsumer</a>
	Access to Administration	<a href="#">BIAdministrator</a>
	Access to Segments	<a href="#">BIConsumer</a>
	Access to Segment Trees	<a href="#">BIAuthor</a>
	Access to List Formats	<a href="#">BIAuthor</a>
	Access to Metadata Dictionary	<a href="#">BIAuthor</a>
	Access to Oracle BI for Microsoft Office	<a href="#">BIConsumer</a>
	Access to Conditions	<a href="#">BIAuthor</a>
	Access to KPI Builder	<a href="#">BIAuthor</a>
	Access to Scorecard	<a href="#">BIConsumer</a>
Actions	Create Navigate Actions	<a href="#">BIConsumer</a>
	Create Invoke Actions	<a href="#">BIAuthor</a>
	Save Actions containing embedded HTML	<a href="#">BIAdministrator</a>

## Mapping Roles to LDAP Groups

- Roles are mapped to LDAP groups through role grants
  - Roles are granted to LDAP groups, or to users
  - Roles are then assigned permissions (policy store) and RPD/webcat privs
- Role assignment carried out through EM Fusion Middleware Control
- For clarity, create roles names as singular, groups as plural
  - BIConsumer : application role
  - BIConsumers : LDAP group



Application Roles > Edit Application Role

Edit Application Role : BICentralSFManager

**General**

Application Stripe: obi

Role Name: BICentralSFManager

Display Name:

Description:

**Members**

An application role may need to be mapped to users or groups defined in enterprise

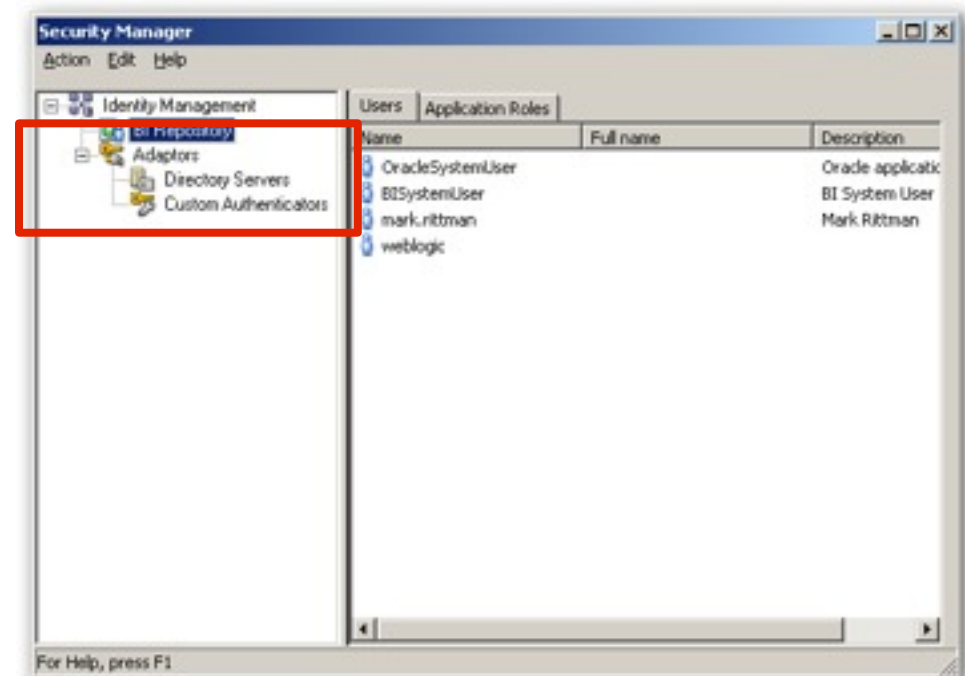
**Roles**

+ Add Application Role + Add Group X Delete...

Name	Type
BICentralSFManagers	Group

## Backwards-Compatibility with OBIEE 10g Security

- Application roles, use of the WLS LDAP Server, OPSS etc are all new with 11g
- Some things are still the same though as in OBIEE 10g
  - ▶ Init Blocks
  - ▶ External Authenticators
  - ▶ Custom Authenticators
  - ▶ Database Authentication
  - ▶ SA System Subject Area
  - ▶ RPD access control
  - ▶ Web Catalog access control
- FMW11g Upgrade Assistant will migrate RPD users, groups to WLS LDAP Server, and create corresponding mapped application roles



## Common OBIEE 11g Security Tasks

---

1. Adding new users to the LDAP server, adding to groups
2. Mapping groups to application roles
3. Creating and amending application roles, and assigning policies/permissions
4. Scoping RPD subject areas and row-level security to application roles
5. Integrating with external directories (MS Active Directory)
6. Managing Single Sign-On

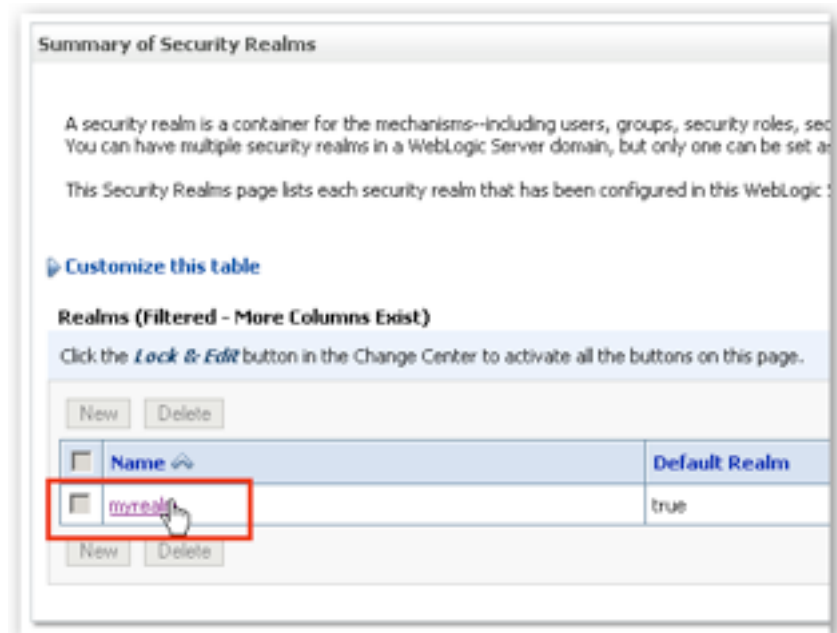
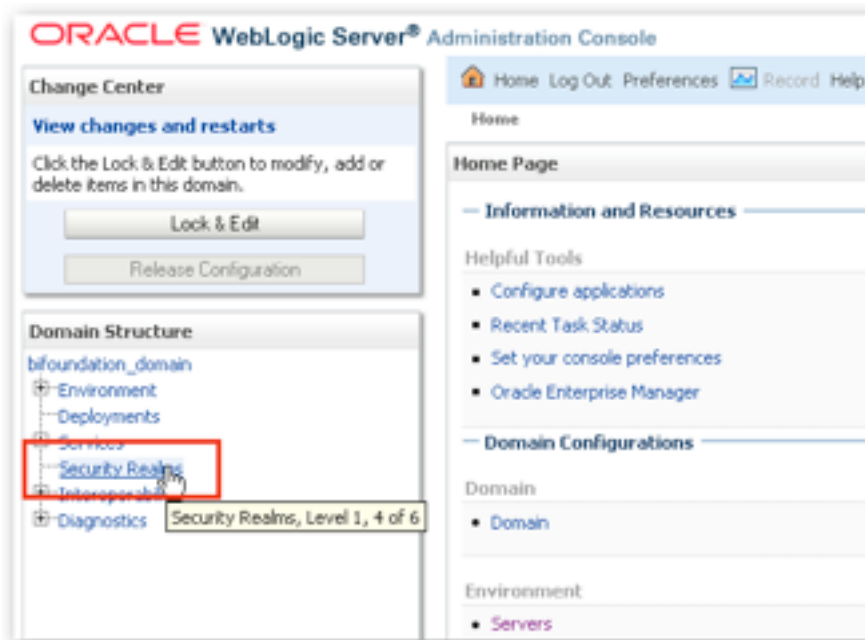
## Creating New Users, Adding to Groups

---

- For the embedded WLS LDAP Server, user and group maintenance is carried out through WLS Admin Server Console
- For alternative authentication providers, user and group administration is carried out using the provider's own administration screen
  - ▶ WLS Admin Server Console view becomes read-only

## Adding a New User Step 1 : Select Security Realm

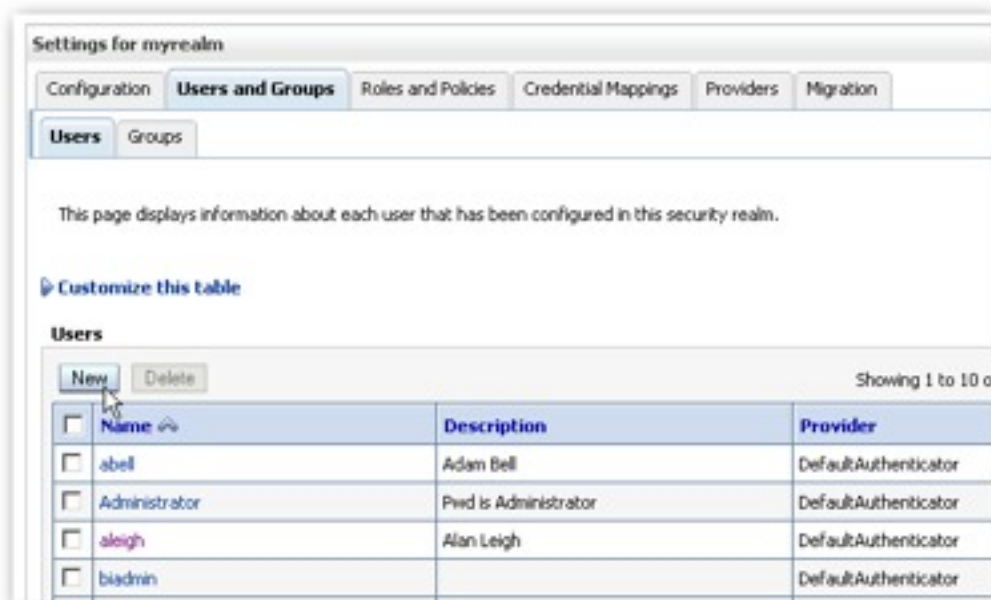
- Using WLS Admin Server Console, navigate to security realm
  - **bifoundation\_domain > Security Realms > myrealm**
- Security Realms are containers for settings, only one can be active at one time





## Adding a New User Step 2 : Create User

- Press **New** and enter details for the new user
- User will appear immediately in BI Administration tool Security Manager



Create a New User

OK Cancel

**User Properties**

The following properties will be used to identify your new User.

\* Indicates required fields

What would you like to name your new User?

\* Name: w\_c\_admin

How would you like to describe the new User?

Description: Mrs WC Admin

Please choose a provider for the user.

Provider: DefaultAuthenticator

The password is associated with the login name for the new User.

\* Password: .....

\* Confirm Password: .....

## Adding a New User Step 3 : Assign to Groups

- Assign user to relevant LDAP groups
- These groups then have application roles granted to them using Fusion Middleware Control

**Groups**

New Delete

<input type="checkbox"/> Name	Description
<input type="checkbox"/> AdminChannelUsers	AdminChannelUsers can access the admin channel.
<input type="checkbox"/> Administrators	Administrators can view and modify all resource attributes and start and stop servers.
<input type="checkbox"/> AppTesters	AppTesters group.
<input type="checkbox"/> BIAdministrators	BI Administrators Group
<input type="checkbox"/> BIAuthors	BI Authors Group
<input type="checkbox"/> BICentralSFManagers	GCBC Central SF Regional Managers
<input type="checkbox"/> BIConsumers	BI Consumers Group
<input type="checkbox"/> BINorthCAManagers	GCBC Northern California Regional Managers
<input type="checkbox"/> BINorthSFManagers	GCBC North SF Regional Managers
<input type="checkbox"/> BIOtherUSAManagers	GCBC Other USA Regional Managers

New Delete



**Settings for nsf\_manager**

General Passwords Attributes **Groups**

Save

Use this page to configure group membership for this user.

**Parent Groups:**

**Available:**

- ☐ BIAdministrators
- ☐ BIAuthors
- ☐ BICentralSFManagers
- ☐ BIConsumers
- ☐ BINorthCAManagers
- ☐ BIOtherUSAManagers
- ☐ BISouthSFManagers

**Chosen:**

- ☐ BINorthSFManagers

Save

## Mapping Groups to Application Roles

- Mapping process is carried out using Fusion Middleware Control
- Roles and Policies, and role grants are held in the policy store
- Roles can be granted to users, but best practice is groups
- Roles can also be recursively granted to other roles

**Policy Store Provider**

Scope WebLogic Domain  
Provider XML  
Location ./system-jazn-data.xml

**Search**

Enter search keyword for role name to query roles defined by this application. Use application stripe to

Select Application Stripe to Search ☒ obi

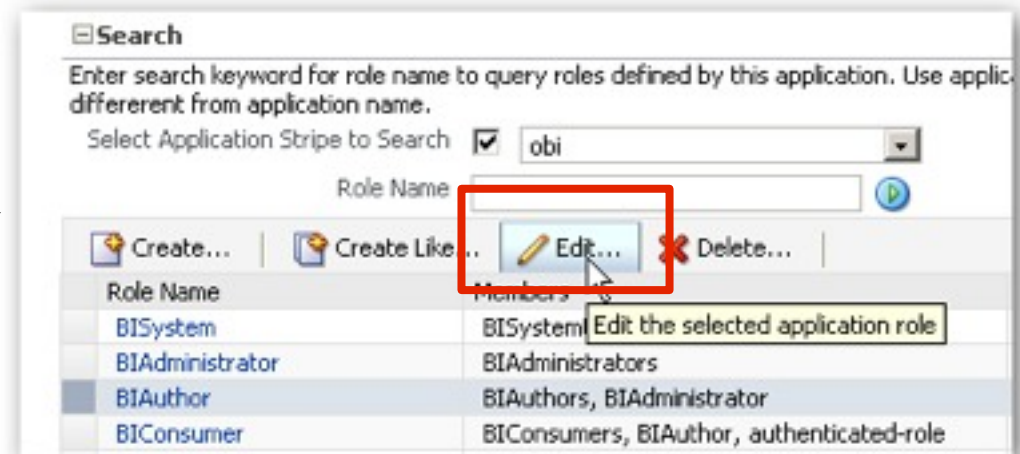
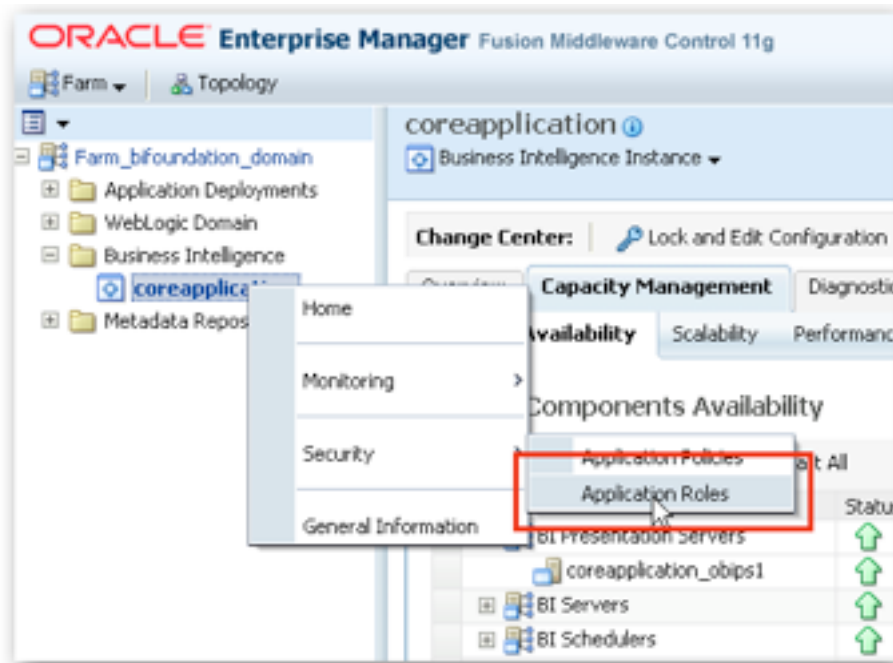
Role Name

[Create...](#) [Create Like...](#) [Edit...](#) [Delete...](#)

Role Name	Members	Description
BISystem	BISystemUser	
BIAdministrator	BIAdministrators	
BIAuthor	BIAuthors, BIAdministrator	
BIConsumer	BIConsumers, BIAuthor, authenticated-role	

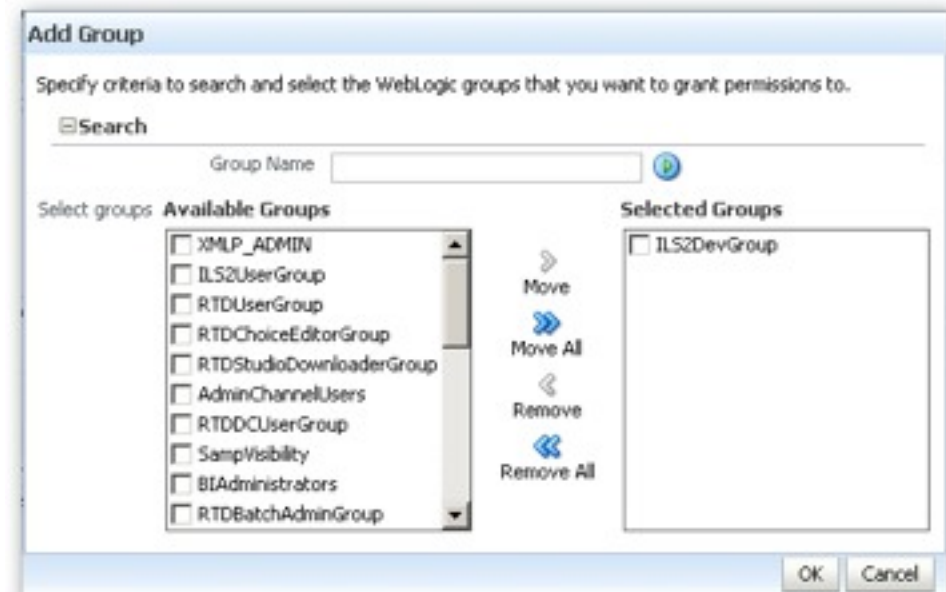
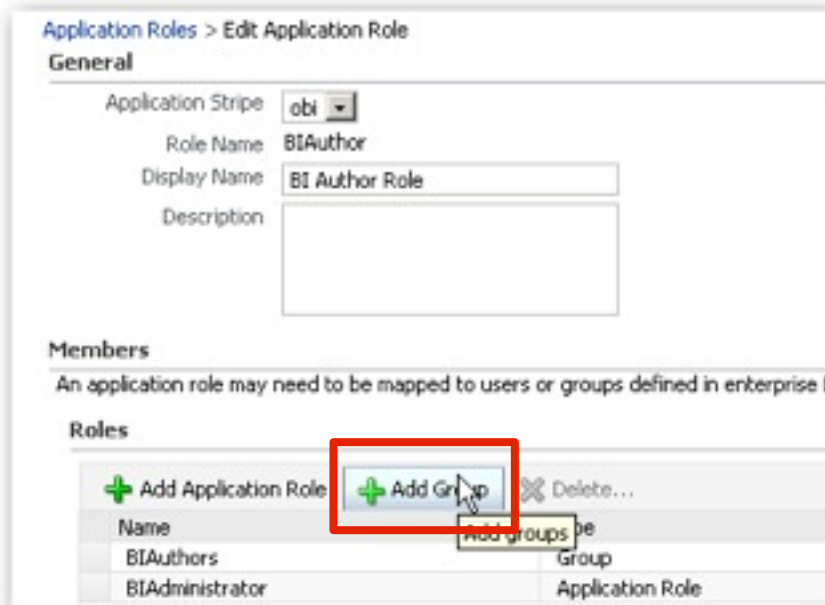
## Mapping Roles to Groups Step 1 : Select Role for Editing

- Right-click on **Business Intelligence** > **coreapplication** > **Security**, and select **Application Roles**



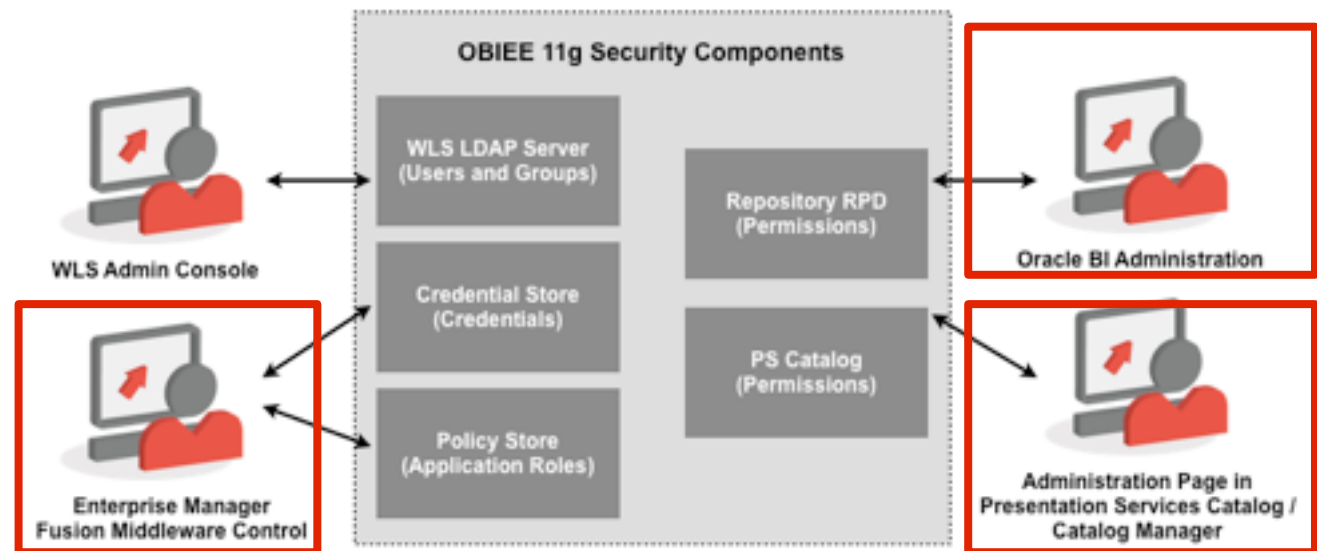
## Mapping Roles to Groups Step 2 : Grant Role to Group

- Click **Add Group** to bring up the groups selector
- Select groups for which the role will be granted
- Restart BI Server after process, to reflect changes in BI Administration tool



## Creating Application Roles and Assigning Policies

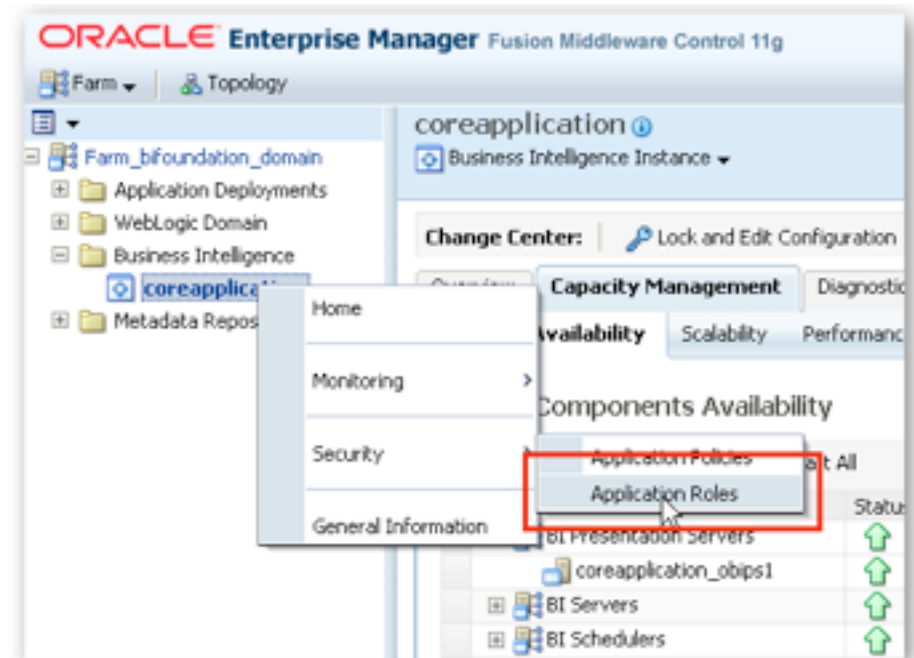
- Application roles are containers for permissions, and are assigned to users and groups
- Roles can be used just for data filtering, or can be assigned permissions
- Permissions are granted using **Application Policies** (FMW Control) and through various legacy OBIEE tools (BI Administration, Presentation Server Admin etc)





## Creating Application Roles Step 1 : Select Roles from Menu

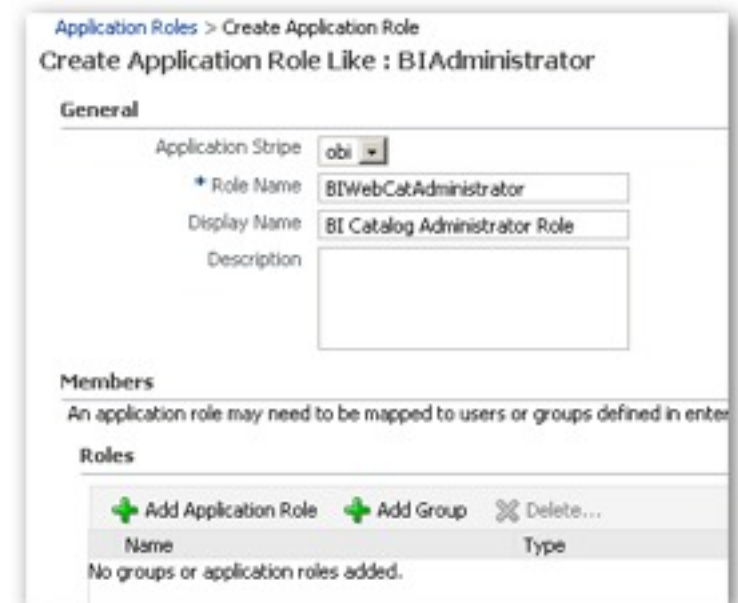
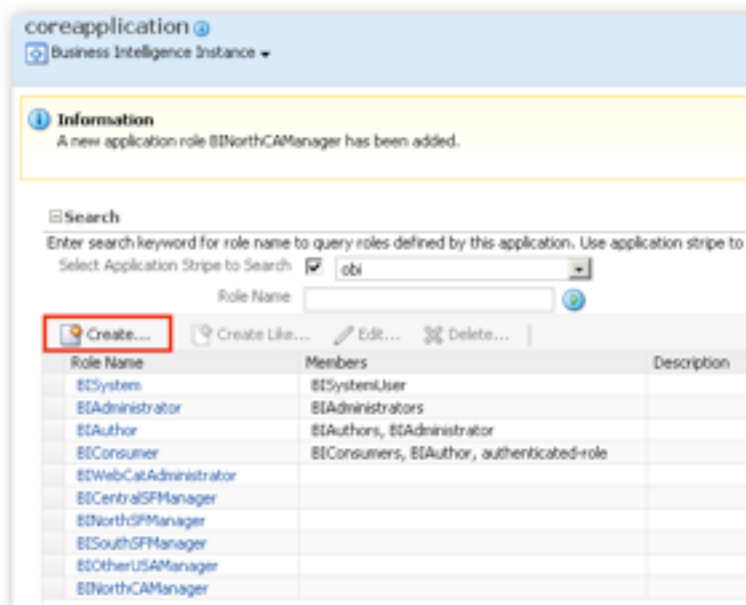
- Right-click on **Business Intelligence > coreapplication > Security**, and select **Application Roles**





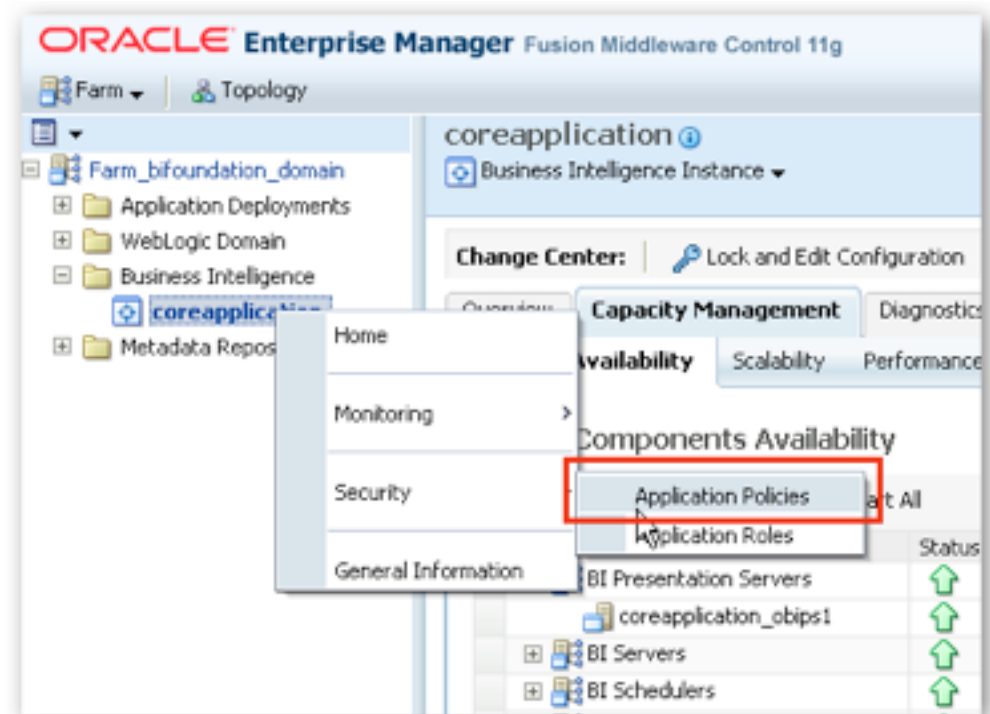
## Creating Application Roles Step 2 : Create New Role

- Select **Create...** button just above list of existing roles, enter details for new role
- Use **Create Like...** button to create role with same grants (not policy) as existing role
- Perform initial mapping to LDAP groups, or grant role recursively to other roles



## Creating Application Roles Step 3 : Create Policy for Role

- If role is to be used to grant application privileges, then policy may be required
  - ▶ High-level for legacy OBIEE, detail-level for java components



## Creating Application Roles Step 4 : Define Policy

- Use **Create Like...** to base policy on another, deleting or adding as necessary

The screenshot shows the Oracle BI Application Policies console. On the left, a list of principals is shown: BIAAdministrator, BISystem, and BIConsumer. The 'Create Like...' button is highlighted with a red box. A tooltip for this button reads: 'Create a new application security grant like the selected one'. An arrow points from this button to the 'Create Application Grant Like : BIAAdministrator' dialog box on the right.

The dialog box has the following sections:

- Grant Details:** Scope is 'Application Policy', Application Stripe is 'obi'.
- Permissions:** A table with columns 'Permission Class', 'Resource Name', and 'Permission Actions'. The first row is selected and highlighted. A red box highlights the 'Delete...' button in the top right of this section. A tooltip for this button reads: 'Delete the selected permission'.
- Grantee:** A section for selecting grantees with buttons: '+ Add User', '+ Add Application Role', '+ Add Group', and 'X Delete...'. Below these are columns for 'Name' and 'Type'.

## Creating Application Roles Step 5 : Set OBIPS Privileges

- Policy store only sets high-level permissions for Presentation Server
  - Edit catalog, access catalog etc
- Individual component and feature privileges need to be set using PS Admin page

The screenshot shows the Oracle Business Intelligence Administration console. The 'Manage Privileges' page is active, displaying a list of components and their associated privileges. An arrow points from the 'Access to Administration' row in the list to a dialog box titled 'Privilege: Access to Administration'.

**Oracle Business Intelligence Administration - Manage Privileges**

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

Access	Privilege
Access to Dashboards	BIConsumer
Access to Answers	BIAuthor
Access to Delivers	BIAuthor
Access to Briefing Books	BIConsumer
Access to Administration	BIAdministrator
Access to Segments	BIConsumer
Access to Segment Trees	BIAuthor
Access to List Formats	BIAuthor
Access to Metadata Dictionary	BIAuthor
Access to Oracle BI for Microsoft Office	BIConsumer
Access to Conditions	BIAuthor
Access to KPI Builder	BIAuthor
Access to Scorecard	BIConsumer
Actions	
Create Navigate Actions	BIConsumer
Create Invoke Actions	BIAuthor
Save Actions containing embedded HTML	BIAdministrator

**Privilege: Access to Administration**

Hive: Access

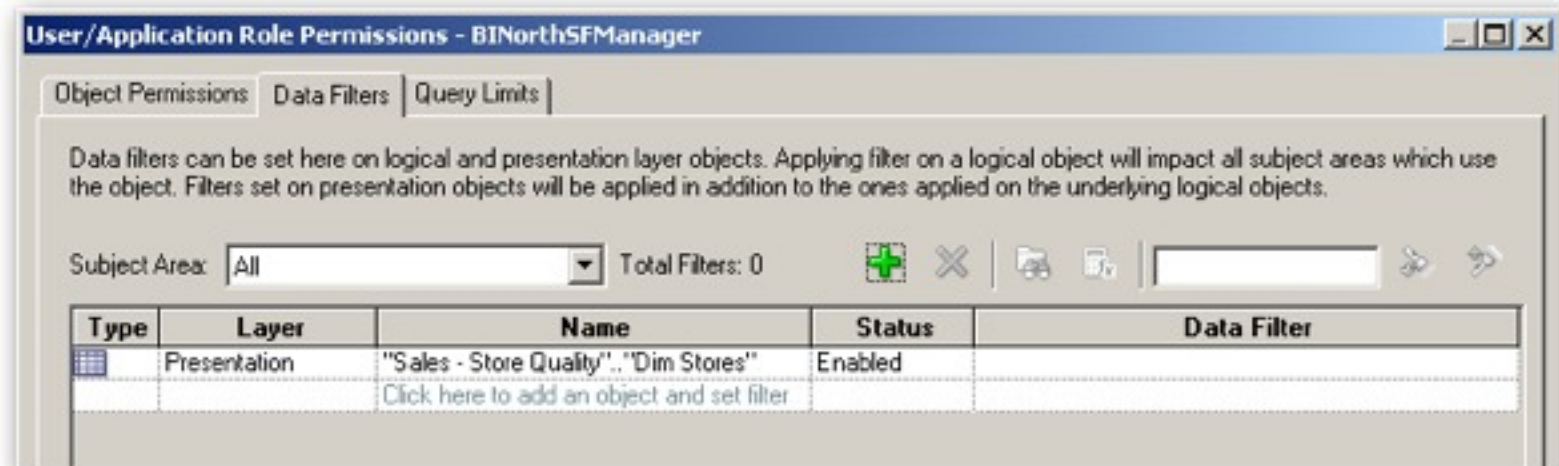
**Permissions**

Accounts	Permission
BIAdministrator	Granted
BIAuthor	Granted
BIConsumer	Granted

Help OK Cancel

## Scoping RPD and Web Catalog using Application Roles

- Once application roles are configured, RPD and webcat elements can be scoped as with OBIEE 10g
- Set permissions on subject areas, and set row-level security
- Set permissions on web catalog objects
- Set privileges for Presentation Server functionality
- Set permissions on connection pools etc



## Connecting to Alternative Directories

- WLS LDAP Server is the default authenticator for OBIEE 11g (and FMW11g)
- Other directories and authentication providers can be used instead (or together)
  - ▶ Microsoft Active Directory
  - ▶ Oracle Internet Directory
  - ▶ Other LDAP servers
  - ▶ Database authentication
  - ▶ etc
- Connection is made through WLS and OPSS
  - ▶ Direct connection through RPD is still supported, but deprecated
- Only one directory (authentication provider) can be active at any one time, but **weblogic/welcome1** superuser will keep working to log into WLS/EM (as long as it remains in WLS LDAP directory)





## Registering Active Directory Step 1 : Select Security Realm

- Using WLS Admin Server Console, navigate to security realm
  - bifoundation\_domain > Security Realms > myrealm**

The screenshot shows the Oracle WebLogic Server Administration Console. On the left, the 'Domain Structure' tree is expanded to 'Security Realms'. A red box highlights 'Security Realms' in the tree, and a tooltip shows 'Security Realms, Level 1, 4 of 6'. An arrow points to the right, where the 'Summary of Security Realms' page is shown. This page contains a table of security realms. A red box highlights the 'myrealm' entry in the table, which is the default realm.

**Summary of Security Realms**

A security realm is a container for the mechanisms—including users, groups, security roles, security policies, and security providers. You can have multiple security realms in a WebLogic Server domain, but only one can be set as the default realm.

This Security Realms page lists each security realm that has been configured in this WebLogic Server domain.

[Customize this table](#)

**Realms (Filtered - More Columns Exist)**

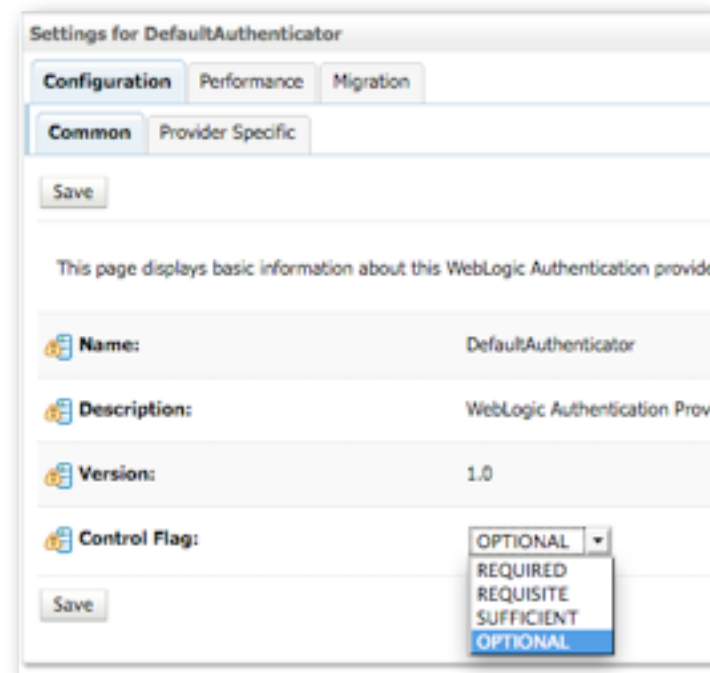
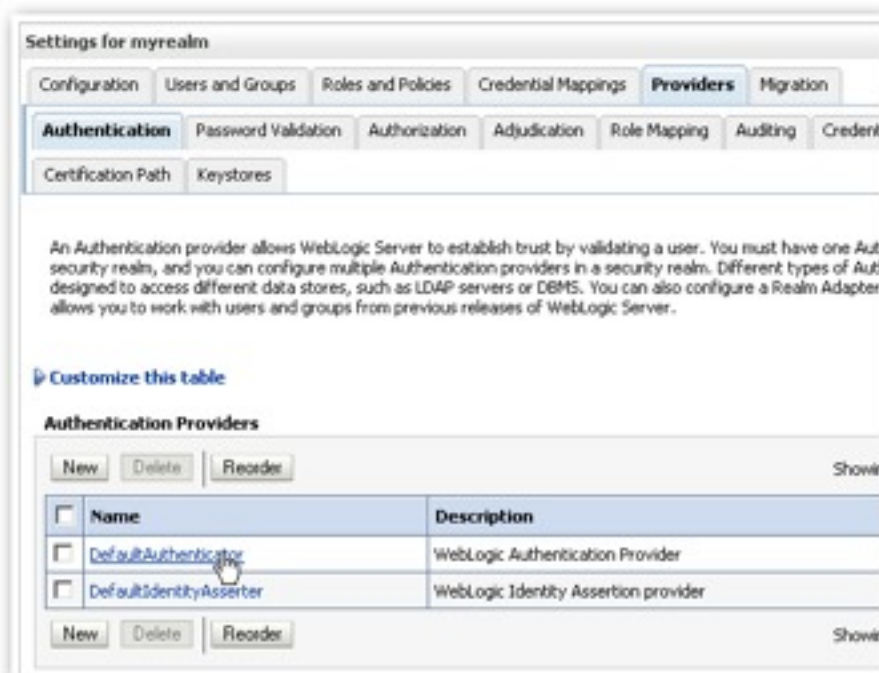
Click the **Lock & Edit** button in the Change Center to activate all the buttons on this page.

Name	Default Realm
myrealm	true



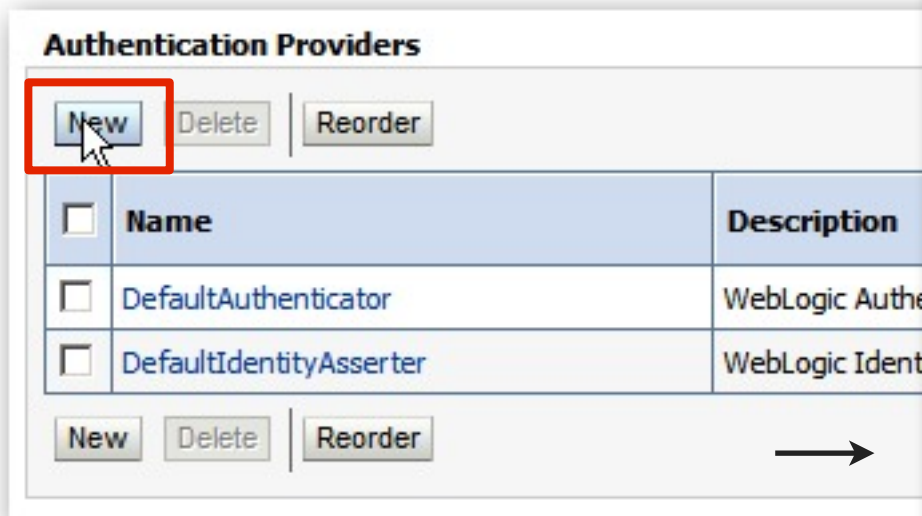
## Registering Active Directory Step 2 : Amend Existing Provider

- Click on **Providers > Authentication**, then select **DefaultAuthenticator**
- Set **Control Flag** to **Optional**
  - Removes requirement for OPSS to authenticate through WLS LDAP



## Registering Active Directory Step 3 : Create New Provider

- Select **Providers** tab, then press **New**
- Enter name for provider, and select **ActiveDirectoryAuthenticator** as the type



Create a New Authentication Provider

OK Cancel

Create a new Authentication Provider

The following properties will be used to identify your new Authentication Provider.

\* Indicates required fields

The name of the authentication provider.

\* Name: MSAD

This is the type of authentication provider you wish to create.

Type: ActiveDirectoryAuthenticator

OK Cancel

## Registering Active Directory Step 4 : Enter Connection Details

- Select Configuration > Provider Specific
- Enter connection details for the Active Directory server
  - ▶ These will be different for each domain
  - ▶ See documentation, and your AD details, for correct settings
  - ▶ Ensure User Name Attribute is set to sAMAccountName

The screenshot shows a configuration window titled 'Users'. It contains several fields for setting up an Active Directory connection:

- User Base DN:** CN=Users,DC=venkatad,DC
- All Users Filter:** (empty text box)
- User From Name Filter:** (&(cn=%u)(objectclass=user)
- User Search Scope:** subtree (dropdown menu)
- User Name Attribute:** sAMAccountName (highlighted with a red box)
- User Object Class:** user
- Use Retrieved User Name as Principal:** (unchecked checkbox)

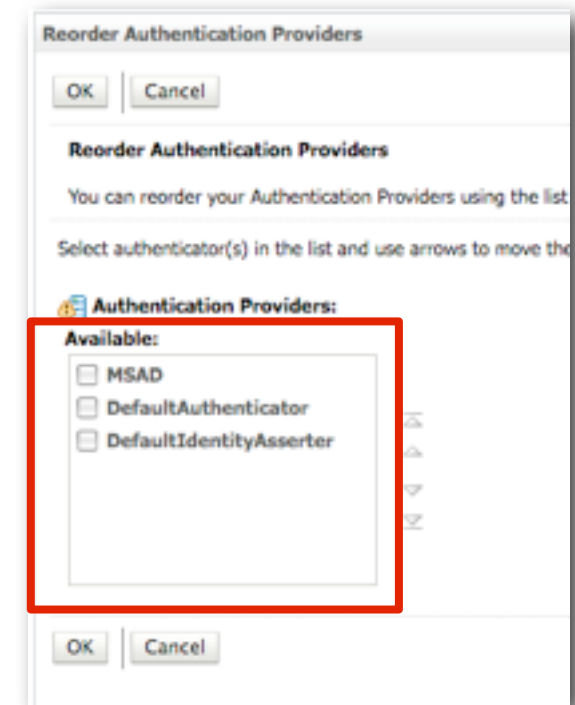
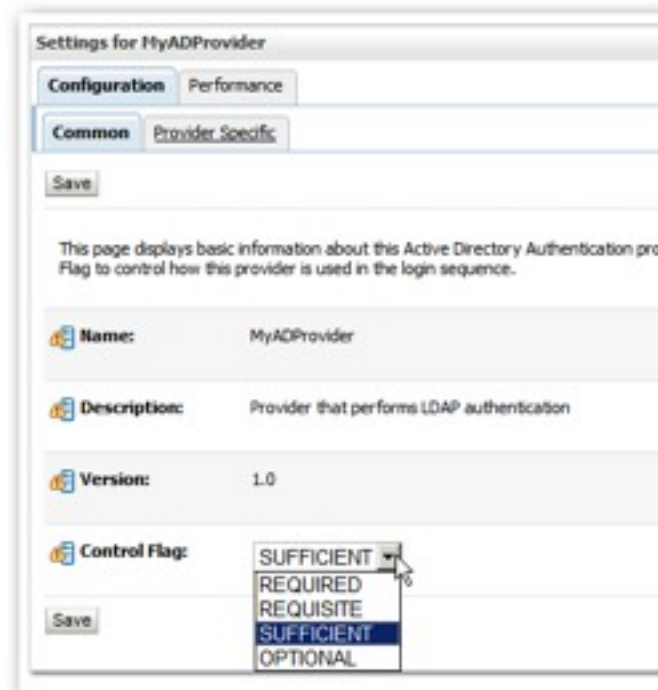
## Registering Active Directory Step 5 : Check Users/Groups Appear

- Restart the WLS Admin Server
- Navigate back to **myrealm > Users and Groups**, and check that AD users now appear in the Users and Groups listing
  - ▶ If they do not, check your AD settings

<input type="checkbox"/>	hmayes	DefaultAuthenticator
<input type="checkbox"/>	hoffmand	DefaultAuthenticator
<input type="checkbox"/>	hyperion	DefaultAuthenticator
	IUSR_VENKATAD	MSAD
	IWAM_VENKATAD	MSAD
<input type="checkbox"/>	jimenezal	DefaultAuthenticator
<input type="checkbox"/>	joannam	DefaultAuthenticator
<input type="checkbox"/>	Kennedydm	DefaultAuthenticator
<input type="checkbox"/>	kolosvaryec	DefaultAuthenticator
<input type="checkbox"/>	kowalchukv	DefaultAuthenticator
	krbtgt	MSAD
<input type="checkbox"/>	kurupm	DefaultAuthenticator
<input type="checkbox"/>	linzingdm	DefaultAuthenticator
<input type="checkbox"/>	lykebt	DefaultAuthenticator
<input type="checkbox"/>	marty	DefaultAuthenticator
<input type="checkbox"/>	miaoc	DefaultAuthenticator
<input type="checkbox"/>	micheldt	DefaultAuthenticator
<input type="checkbox"/>	mlombar	DefaultAuthenticator
<input type="checkbox"/>	mlynarcikj	DefaultAuthenticator
<input type="checkbox"/>	morleydl	DefaultAuthenticator
	MSADAdmin	MSAD

## Registering Active Directory Step 6 : Set Provider Order

- Select **Configuration > Common**, and set **Control Flag** to Sufficient
  - ▶ Tells OPSS to authenticate against AD if possible, and allow in if OK
- Set provider order to search AD first



## Registering Active Directory Step 7 : Recreate BSystem User

- From the **Users** view, delete the **BSystemUser** user from the default authenticator (WLS LDAP)
  - ▶ BSystemUser is used for running agents and other automated processes
- Then recreate it in Active Directory (you will use it in a moment)
- User the **Users** view to check it is now present in the AD directory

Users

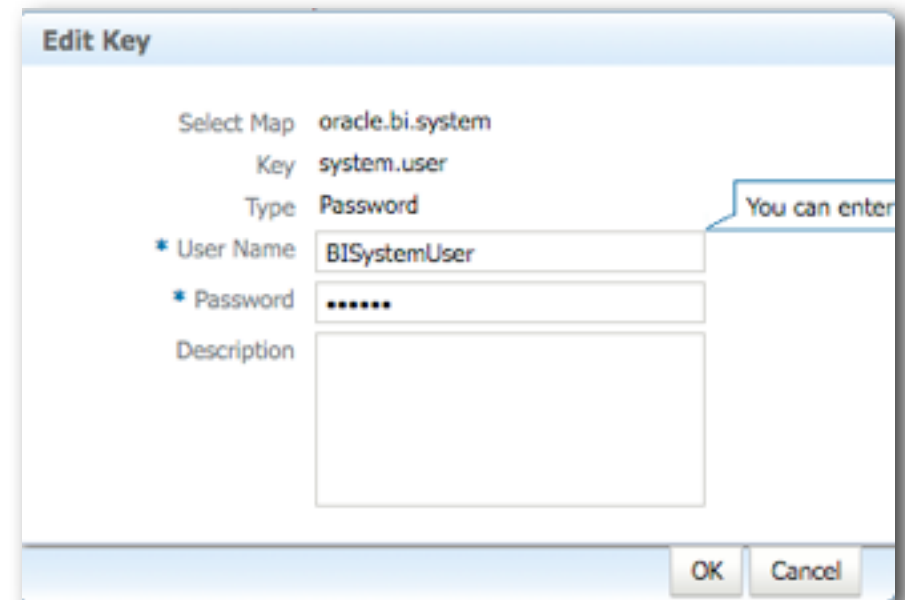
New Delete Showing 1 to 101 of 101 Previous | Next

<input type="checkbox"/>	Name ^	Provider
<input type="checkbox"/>	abell	DefaultAuthenticator
	Administrator	MSAD
<input type="checkbox"/>	Administrator	DefaultAuthenticator
<input type="checkbox"/>	aleigh	DefaultAuthenticator
<input type="checkbox"/>	bendoraitisw	DefaultAuthenticator
<input type="checkbox"/>	biadmin	DefaultAuthenticator
<input type="checkbox"/>	bicc	DefaultAuthenticator
<input type="checkbox"/>	bieeuser1	DefaultAuthenticator
<input type="checkbox"/>	BIImpersonateUser	DefaultAuthenticator
	<b>BSystemUser</b>	MSAD
<input type="checkbox"/>	blanchardj	DefaultAuthenticator
<input type="checkbox"/>	bozzias	DefaultAuthenticator



## Registering Active Directory Step 8 : Set Trusted User

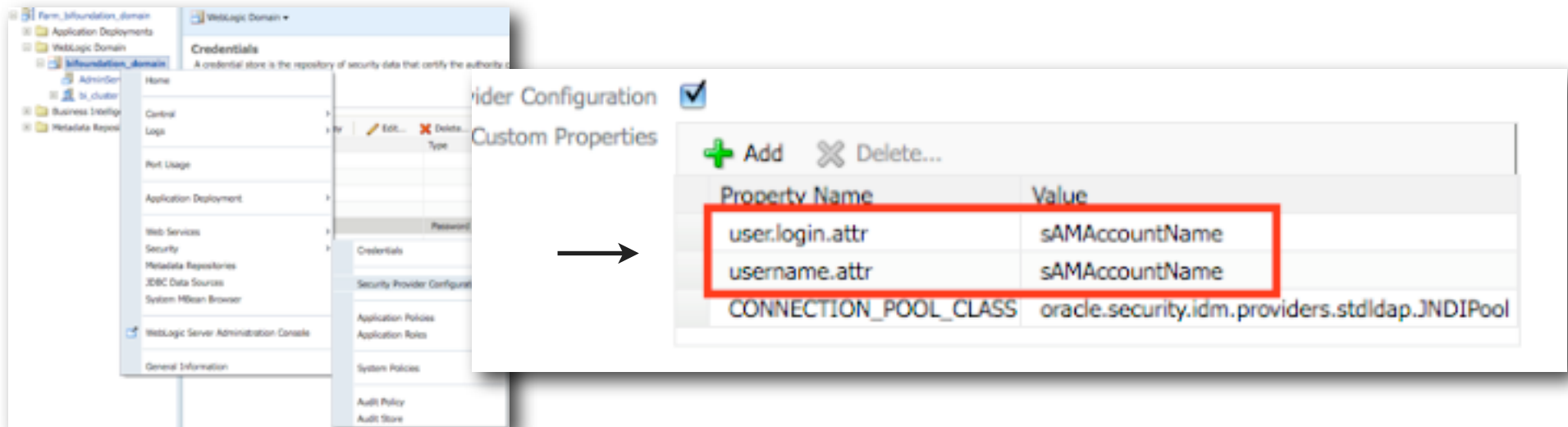
- Using EM, grant the **BISystemUser** account the **BISystem** application role
- If you wish to use set a different password for the **BISystemUser** account, edit Enterprise Manager Credential Store entry and change the password
  - ▶ Also use this setting if you have change the account name from **BISystemUser**





## Registering Active Directory Step 9 : Configure User Name Attrib.

- Required as AD uses a different attribute as the user name attribute
- From EM, open WebLogic Domain > bifoundation\_domain, select **Security > Security Provider Configuration**
- Click on the **Configure** button of the Identity Store Provider and add the 2 entries
  - ▶ `user.login.attr = sAMAccountName`
  - ▶ `username.attr = sAMAccountName`



The screenshot shows the WebLogic Domain console for the bifoundation\_domain. The 'Security' tab is selected, and the 'Security Provider Configuration' page is displayed. The 'Custom Properties' table is shown with the following entries:

Property Name	Value
user.login.attr	sAMAccountName
username.attr	sAMAccountName
CONNECTION_POOL_CLASS	oracle.security.idm.providers.stdldap.JNDIPool

## Registering Active Directory Step 10 : Create and Test User

- Create new user in AD, assign to the **BIAuthor** application role using EM
- Check that user has been granted role, and log into OBIEE to test



**New Object - User**

Create in: venkstad.venkatlap.com/Users

First name: ADReportAuthor Initials: [ ]

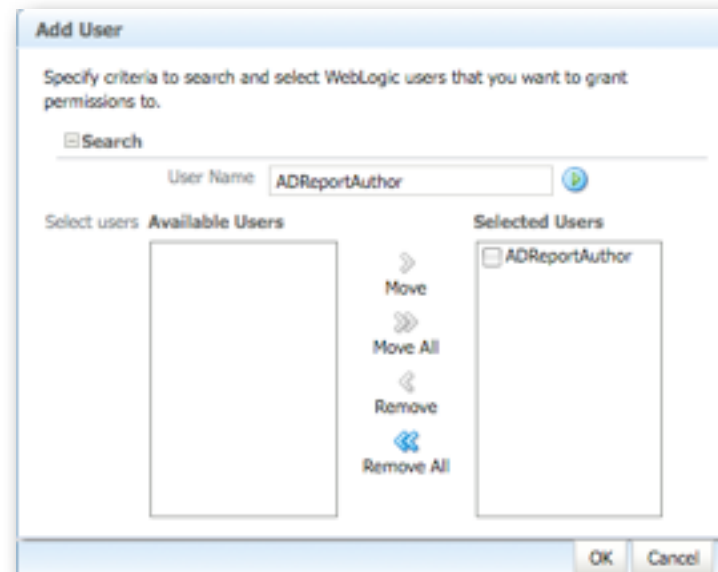
Last name: [ ]

Full name: ADReportAuthor

User logon name: ADReportAuthor @venkstad.venkatlap.com

User logon name (pre-Windows 2000): VENKATAD01 ADReportAuthor

< Back Next > Cancel

**Add User**

Specify criteria to search and select WebLogic users that you want to grant permissions to.

Search

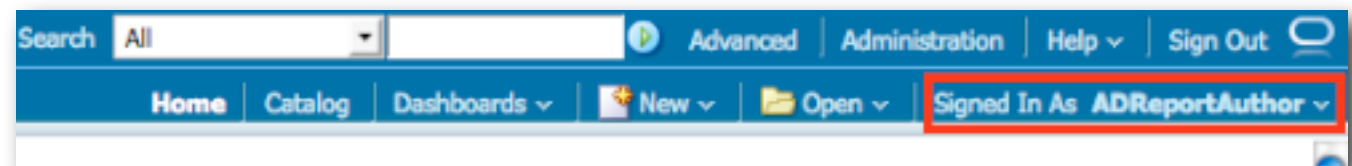
User Name: ADReportAuthor

Select users Available Users Selected Users

ADReportAuthor

Move Move All Remove Remove All

OK Cancel

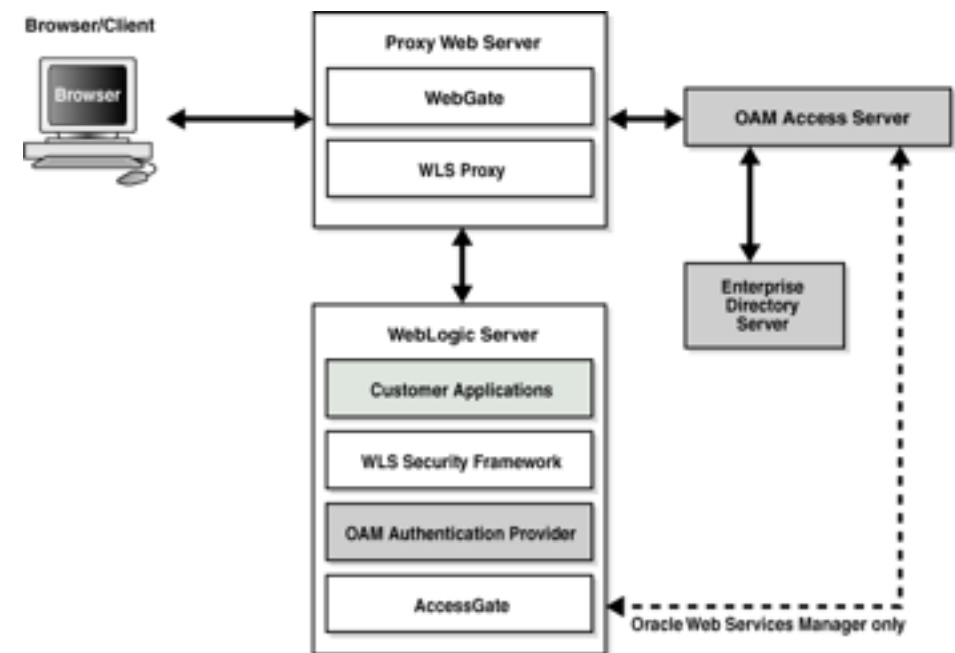



Search All Advanced Administration Help Sign Out

Home Catalog Dashboards New Open Signed In As ADReportAuthor

## Single Sign-On

- Recommended SSO solution is Oracle Access Manager
- SSO is performed through WebLogic Server and OAM
- Requires some setup at the WLS level
- After SSO is set up, OBIPS accepts incoming request as SSO authenticated
- OBIPS then connects to OBIS and uses the impersonation feature
- Full details are in  
*Enabling SSO Authentication within Oracle® Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition 11g Release 1 (11.1.1)*



## Summary

---

- Security in OBIEE 11g has significantly changed compared to 10g
- Identity Store is embedded LDAP server (WLS)
- Users available everywhere
- Application Roles available everywhere
- User Profile derived from LDAP server
- Users/Groups no longer defined in RPD
- Administrator and Administrators not hard-coded
- RPD protected by RPD Password
- Administrator user not used for Inter-Process Communication (component to component)
- Some aspects are still however the same as 10g (RPD scoping, Webcat scoping)
- Update Assistant from 10g will load RPD users into WLS LDAP Server
- Main user and development change is to start working with application roles



# Oracle Business Intelligence 11g Masterclass

Oracle BI & FMW11g Security

T : +44 (0) 8446 697 995 or (888) 631 1410 (USA) E : [enquiries@rittmanmead.com](mailto:enquiries@rittmanmead.com) W: [www.rittmanmead.com](http://www.rittmanmead.com)