

The background of the image is a panoramic view of the Nashville skyline at dusk. The sky is a mix of deep blues and oranges from the setting sun. The city lights are beginning to glow, and the lights from the bridges and buildings are reflected in the water of the river in the foreground. The text 'ODTUG Kscope 24' is overlaid in the center. 'ODTUG' is in a smaller, white, sans-serif font above 'Kscope'. 'Kscope' is in a large, white, sans-serif font. '24' is in a large, multi-colored, geometric font. Below the main title, the text 'nashville, tn' and 'july 14 - 18' is written in a smaller, white, sans-serif font. At the bottom center, the word 'Welcome' is written in a white, sans-serif font.

ODTUG
Kscope 24

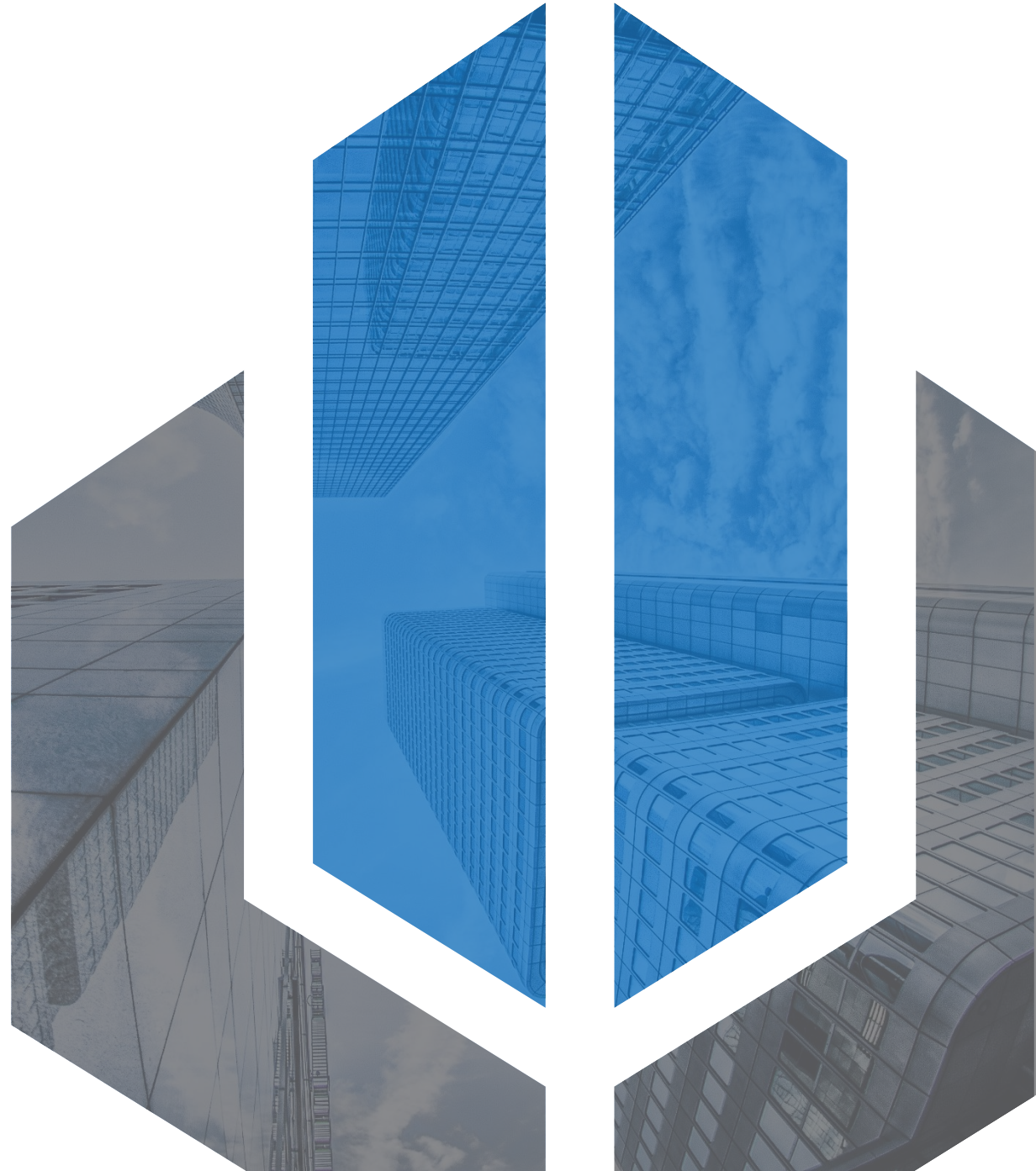
nashville, tn

july 14 - 18

Welcome



EPM Security – Zero to Sixty



AGENDA

Angie Caruthers



Provisioning via OCI



Dimensional Security



Valid Intersections



Cell Level Security



Reporting/Troubleshooting

About the Speaker

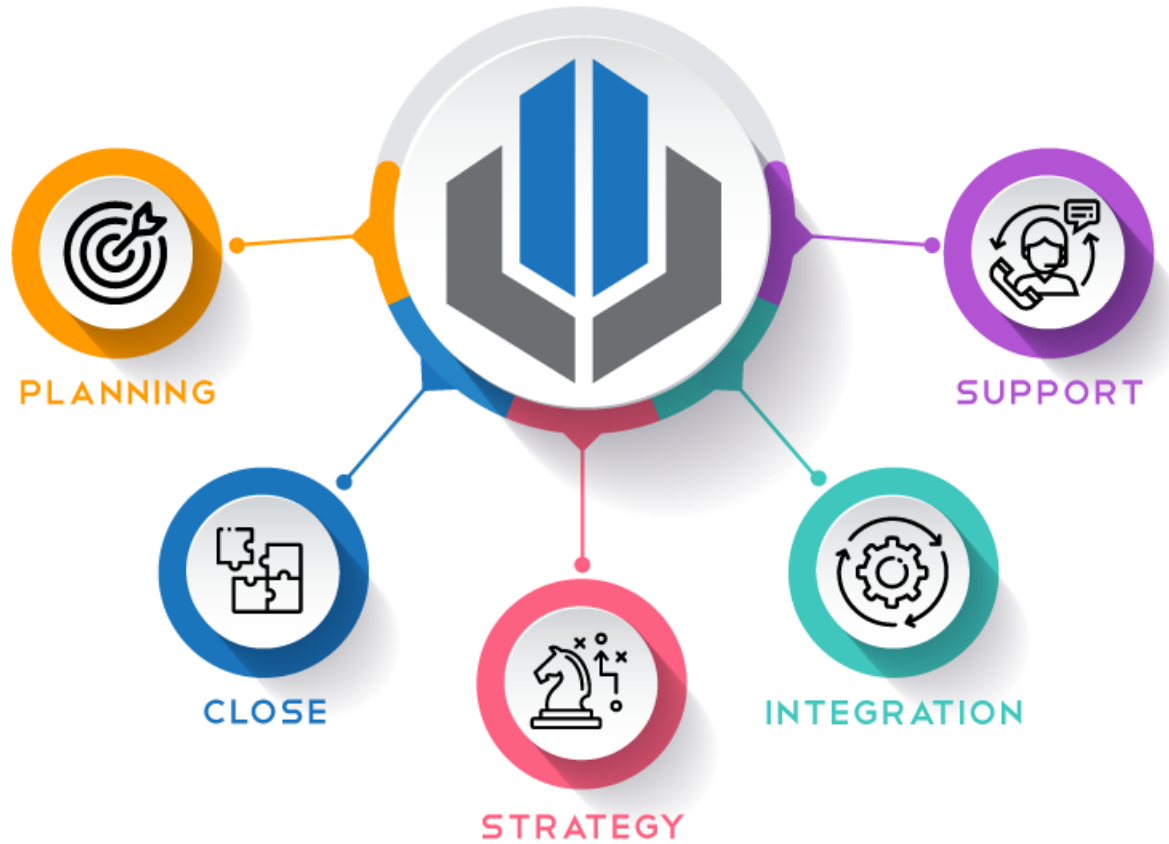


Angie Caruthers

EPM Implementation
Specialist

- 20+ years of Oracle EPM experience
- Kscope Speaker 2013, 2023, 2024
- 2021 Certified Planning Implementation Specialist
- 2021 Certified Narrative Reporting Specialist
- Experienced in Planning, Data Management/Data Integration, Essbase (ASO, BSO and Hybrid), EDMCS and HFM
- Implementations in retail, distribution, software, healthcare and oil & gas industries

About Olympus



Who We Are

Experienced EPM resources with innovative solutions and a diverse skillset to ensure that any project can be successfully executed.

Our Mission

Provide clients with the highest quality EPM experience using a proven methodology that ensures client interaction and satisfaction.

Our Vision

Empower clients to adopt excellent EPM solutions while having a positive impact on the EPM community at large through the knowledge we share.

EPM Security

Why present a full session on EPM security?



- To avoid Goldilocks syndrome in security footprint
 - Too much
 - Not enough
- Client side frequently has minimal security administration training
 - Infrequent updates
 - Limited support/resources
- Security design can take a backseat during technical implementation
 - Focus on user access during UAT
 - Evolving client user access needs
 - Ongoing maintenance process

Security Components

What are the available layers of security?



- **Provisioning** – this represents the EPM *functionality* a user can access (not data access) - MANDATORY
- **Dimension Security** – using access control groups to define what datasets a user can see (Read) and update (Write) - MANDATORY
- **Valid Intersections** – restricting ability to enter data by creating rules that mark certain member intersections as valid (or invalid) for data entry - OPTIONAL
- **Cell Level Security** – further limitation of Dimension access to restrict users from viewing or modifying data values in certain cell intersections - OPTIONAL

AGENDA

Angie Caruthers



Provisioning via OCI



Dimensional Security



Valid Intersections



Cell Level Security



Reporting/Troubleshooting

OCI – Users and Provisioning

Where do I start?



- Start with the basics – we have to create a user and define which application(s) they are provisioned to
- We also have to determine which of the 4 basic provisioning roles to assign to the user for a given application
- Prior to Cloud this was accomplished in Shared Services module

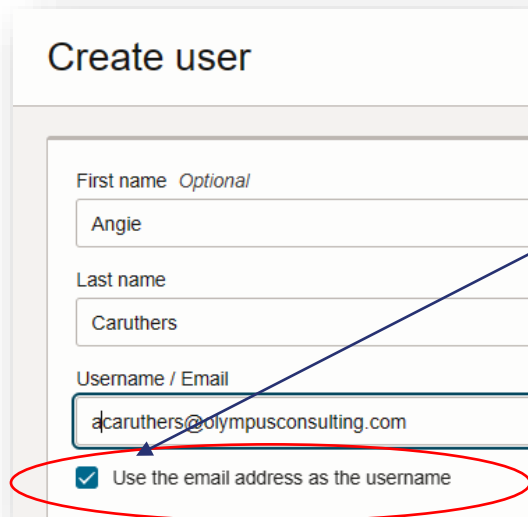
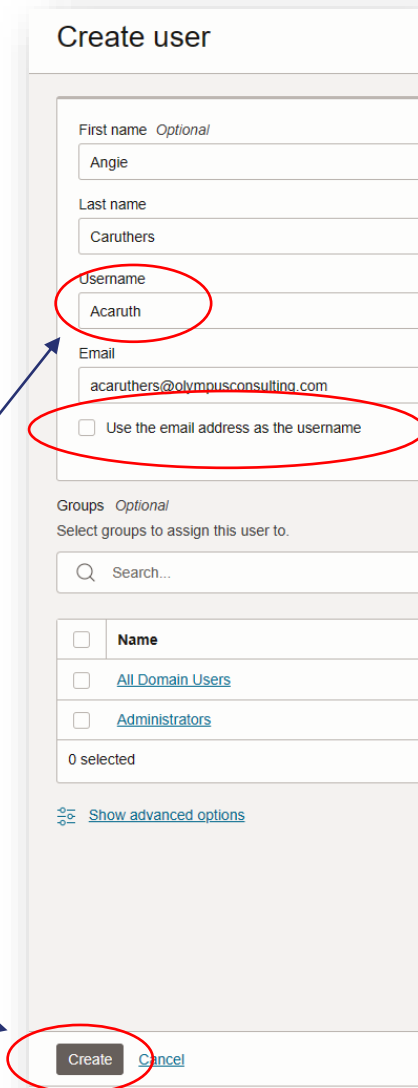
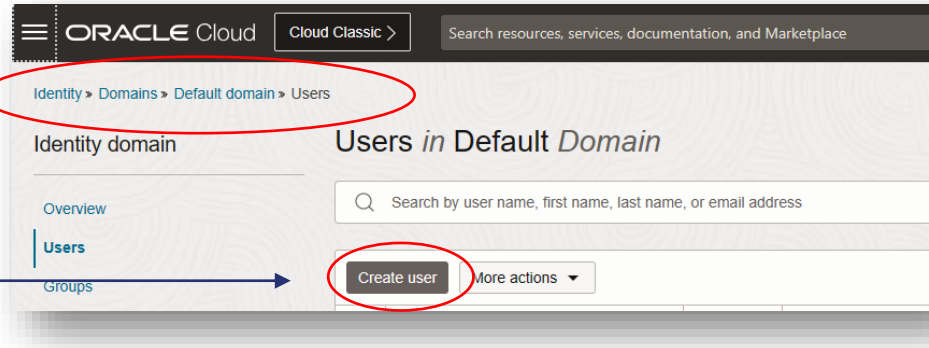
NOTE: Instead of creating users directly in OCI you also have the option enable Single Sign On(SSO) to link all of your Active Directory users to OCI. If you choose this method you just need to provision the users to the application using one of 4 the Application Roles

OCI – Create a User

Creating a Native User

In the OCI URL, navigate to Identity>Domains>Default domain>Users

Click on Create User



TIP: the 'Use email address as Username' is checked by default; I prefer to uncheck this box so I can assign a short user name

Click Create to finish creating the Native User

OCI – Provisioning Roles

What do Provisioning Roles do?



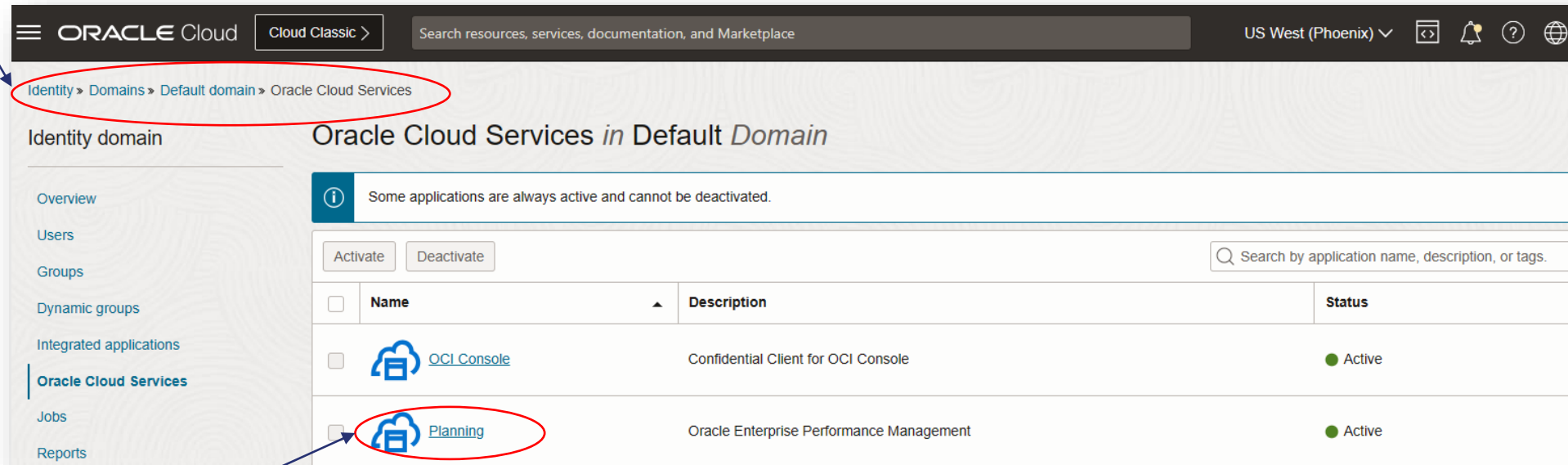
In order to gain access to a given application a user must be assigned one of 4 default Roles for Planning/Freeform applications

- **Service Administrator** – access to ALL functionality; typically this should be no more than 2-3 users
- **Power User** – This role is needed for users who need to view Substitution Variables, modify Form structures or create/update Management Report formats; this should typically represent no more than 5%-10% of users
- **User** – basic Read/Write access including Smartview Adhoc; this should be about 90-95% of your users
- **Viewer** – this only grants read access within the Workspace URL; does not include Smartview adhoc access; it is rarely used in my experience



OCI – Provisioning Roles

How to assign Provisioning to Users

In the OCI URL, navigate to Identity>Domains>Default domain>Oracle Cloud Services



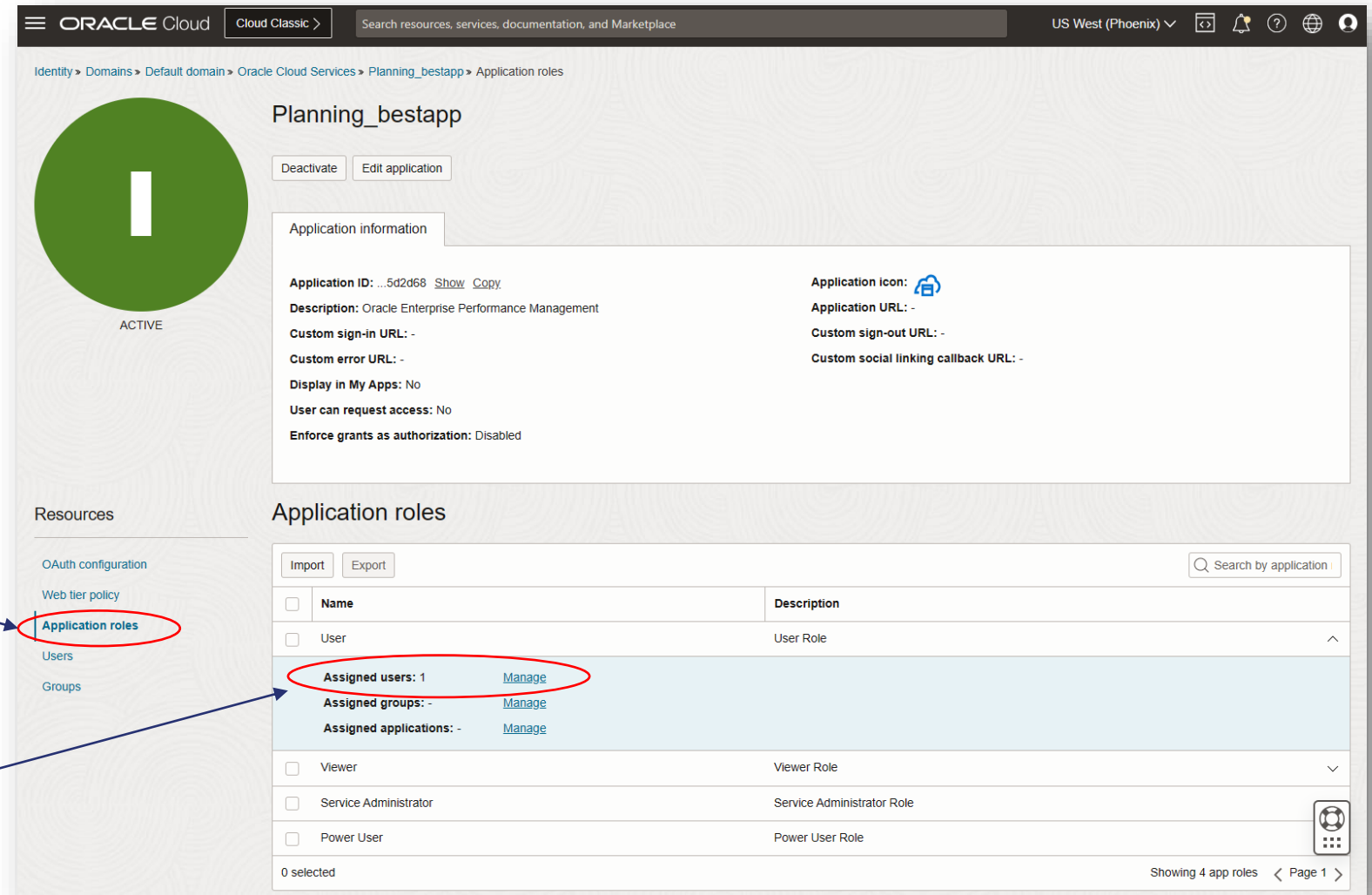
The screenshot shows the Oracle Cloud console interface. The breadcrumb navigation path "Identity > Domains > Default domain > Oracle Cloud Services" is circled in red. The main content area displays "Oracle Cloud Services in Default Domain" with a table of applications. The "Planning" application is circled in red. The table has columns for Name, Description, and Status.

<input type="checkbox"/>	Name	Description	Status
<input type="checkbox"/>	 OCI Console	Confidential Client for OCI Console	● Active
<input type="checkbox"/>	 Planning	Oracle Enterprise Performance Management	● Active

Select the Planning application you wish to provision

OCI – Provisioning Roles

How to assign Provisioning to Users



ORACLE Cloud Cloud Classic > Search resources, services, documentation, and Marketplace US West (Phoenix) > > > > >


Identity > Domains > Default domain > Oracle Cloud Services > Planning_bestapp > Application roles

Planning_bestapp

Deactivate Edit application

ACTIVE

Application information

Application ID: ...5d2d68 [Show](#) [Copy](#) Application icon: 

Description: Oracle Enterprise Performance Management Application URL: -

Custom sign-in URL: - Custom sign-out URL: -

Custom error URL: - Custom social linking callback URL: -

Display in My Apps: No

User can request access: No

Enforce grants as authorization: Disabled

Resources

- OAuth configuration
- Web tier policy
- Application roles**
- Users
- Groups

Application roles

Import Export Search by application

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	User	User Role ^
<input checked="" type="checkbox"/>	Assigned users: 1 Manage	
	Assigned groups: - Manage	
	Assigned applications: - Manage	
<input type="checkbox"/>	Viewer	Viewer Role v
<input type="checkbox"/>	Service Administrator	Service Administrator Role
<input type="checkbox"/>	Power User	Power User Role

0 selected Showing 4 app roles < Page 1 >

Click on the application you want to assign the user to; Then click on **Application Roles**

Expand the Role you want to add the user to and click on **Manage Assigned Users**

OCI – Provisioning Roles

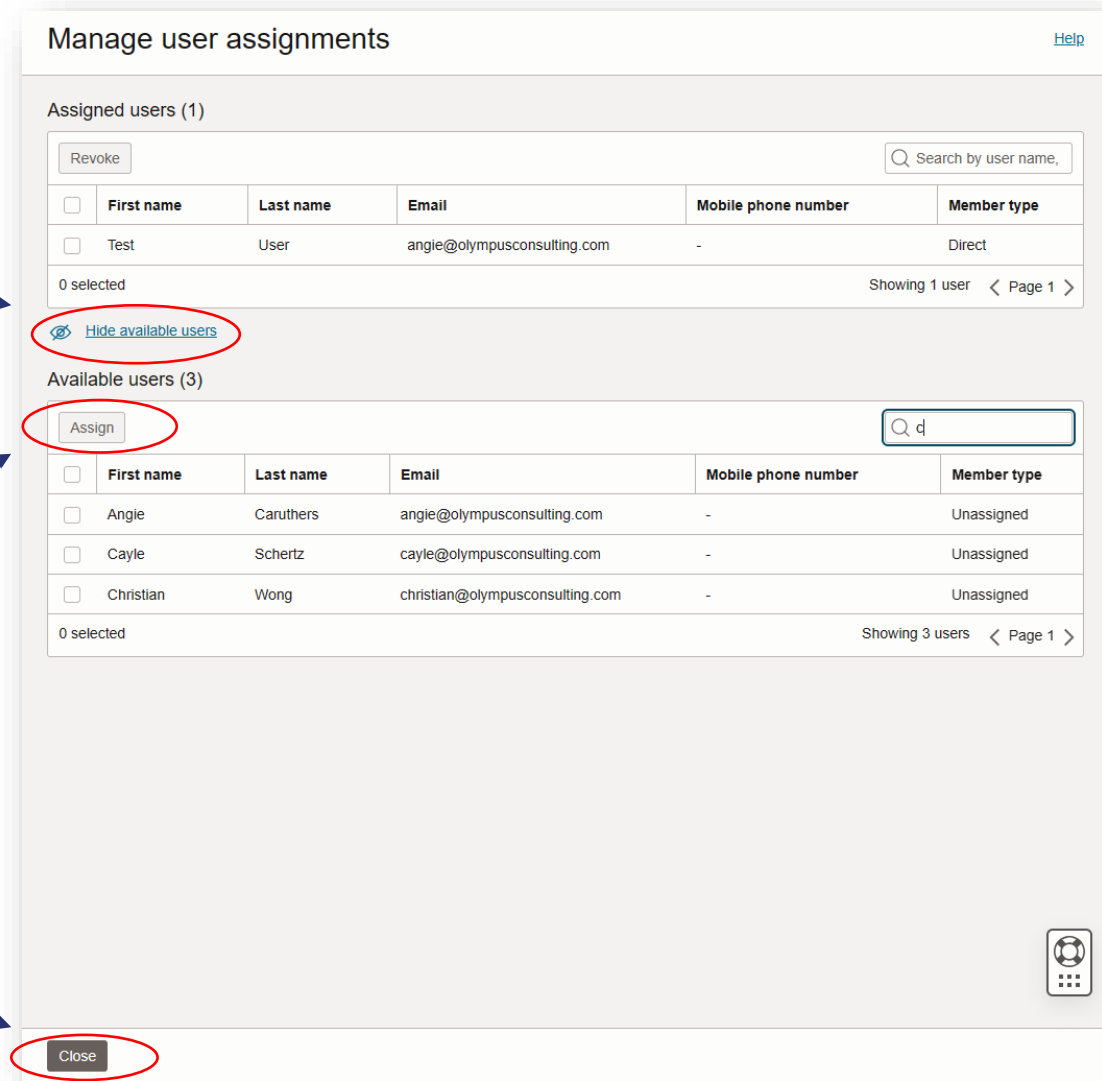
How to assign Provisioning to Users

You will see all users currently assigned to the Role; click on **Show available users**

You can use the filter field to search for the user you need

Check the box next to the user and then click **Assign**; the user name should move to the Assigned Users section

Click **Close**



Manage user assignments [Help](#)

Assigned users (1)

Revoke

<input type="checkbox"/>	First name	Last name	Email	Mobile phone number	Member type
<input type="checkbox"/>	Test	User	angle@olympusconsulting.com	-	Direct

0 selected Showing 1 user < Page 1 >

[Hide available users](#)

Available users (3)

Assign


<input type="checkbox"/>	First name	Last name	Email	Mobile phone number	Member type
<input type="checkbox"/>	Angie	Caruthers	angle@olympusconsulting.com	-	Unassigned
<input type="checkbox"/>	Cayle	Schertz	cayle@olympusconsulting.com	-	Unassigned
<input type="checkbox"/>	Christian	Wong	christian@olympusconsulting.com	-	Unassigned

0 selected Showing 3 users < Page 1 >

Close

Security Components

What are the available layers of security?

-  • **Provisioning** – this represents the EPM *functionality* a user can access (not data access) - MANDATORY
- **Dimension Security** – using access control groups to define what datasets a user can see (Read) and update (Write) - MANDATORY
- **Valid Intersections** – restricting ability to enter data by creating rules that mark certain member intersections as valid (or invalid) for data entry - OPTIONAL
- **Cell Level Security** – further limitation of Dimension access to restrict users from viewing or modifying data values in certain cell intersections - OPTIONAL

AGENDA

Angie Caruthers



Provisioning via OCI



Dimensional Security



Valid Intersections



Cell Level Security



Reporting/Troubleshooting

Dimension Security

Applying Dimension Security via Access Control Groups

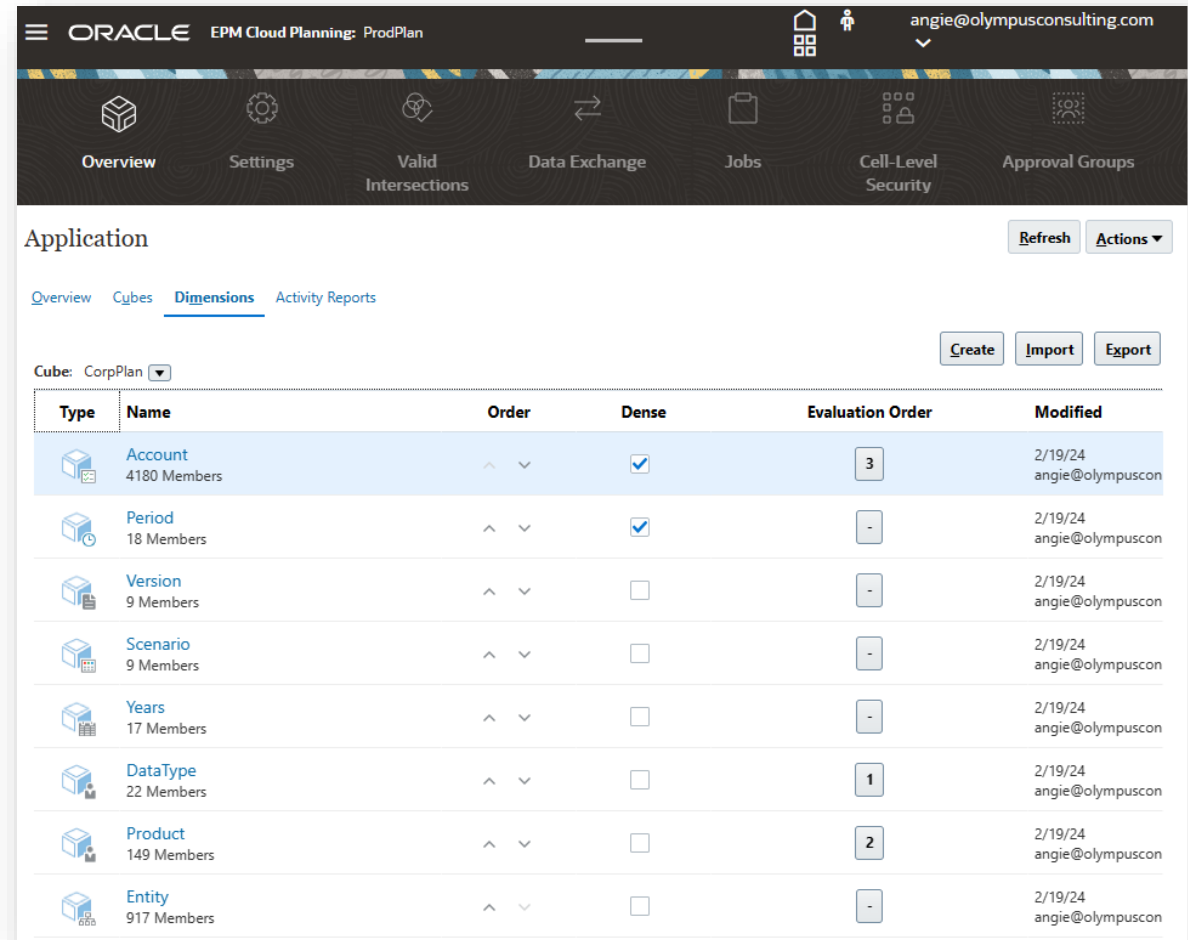


- What happens if I don't apply dimension security?
- Dimension security typically consists of three steps:
 - 1) Apply security to necessary Dimensions
 - 2) Create Access Control Groups and assign users to those groups
 - 3) Assign the Access Control Groups to the hierarchy of each secured Dimension

Dimension Security

Step 1 – Identify which dimensions need security

- Not all dimensions need Security
- For a basic Planning application apply security to:
 - Account
 - Scenario
 - Version
 - Entity
- No need to apply security to Period and Years
- You may or may not need to apply security to other Custom Dimensions such as Product or DataType



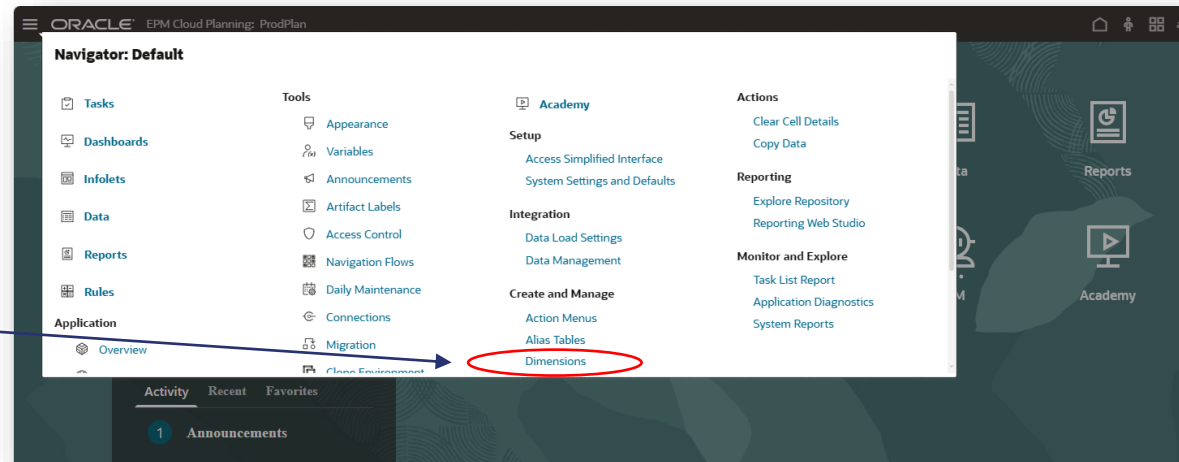
The screenshot shows the Oracle EPM Cloud Planning interface for the 'ProdPlan' application. The 'Dimensions' tab is selected, displaying a table of dimensions for the 'CorpPlan' cube. The table includes columns for Type, Name, Order, Dense, Evaluation Order, and Modified. The 'Account' dimension is highlighted in blue.

Type	Name	Order	Dense	Evaluation Order	Modified
Account	Account 4180 Members	^ v	<input checked="" type="checkbox"/>	3	2/19/24 angie@olympuscon
Period	Period 18 Members	^ v	<input checked="" type="checkbox"/>	-	2/19/24 angie@olympuscon
Version	Version 9 Members	^ v	<input type="checkbox"/>	-	2/19/24 angie@olympuscon
Scenario	Scenario 9 Members	^ v	<input type="checkbox"/>	-	2/19/24 angie@olympuscon
Years	Years 17 Members	^ v	<input type="checkbox"/>	-	2/19/24 angie@olympuscon
DataType	DataType 22 Members	^ v	<input type="checkbox"/>	1	2/19/24 angie@olympuscon
Product	Product 149 Members	^ v	<input type="checkbox"/>	2	2/19/24 angie@olympuscon
Entity	Entity 917 Members	^ v	<input type="checkbox"/>	-	2/19/24 angie@olympuscon

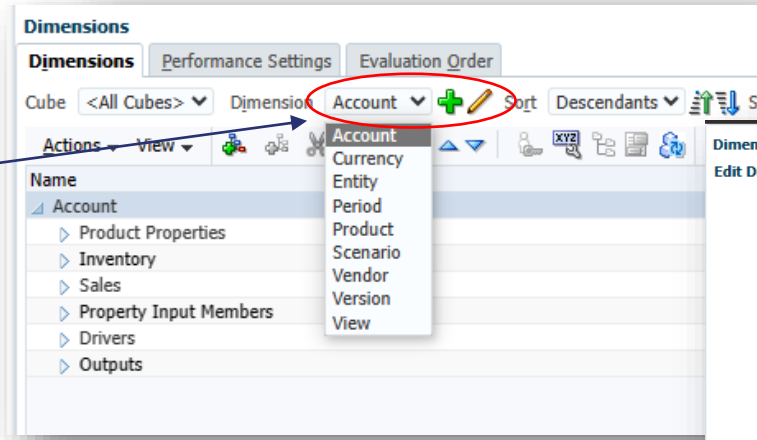
Dimension Security

Enabling security on a dimension

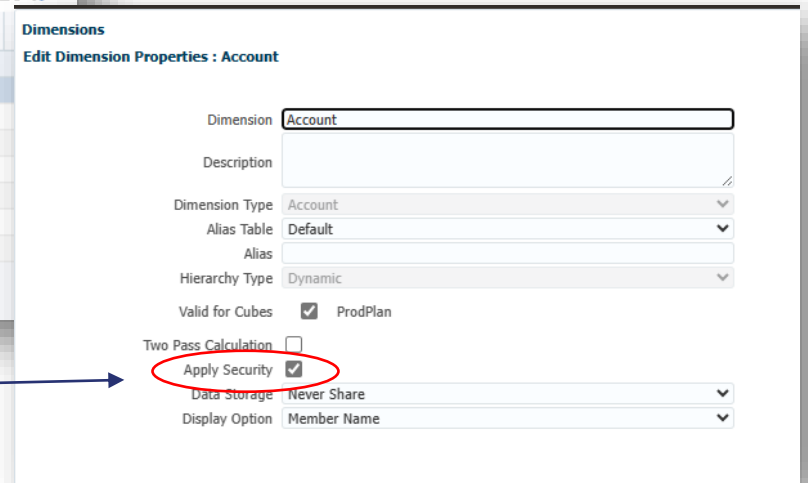
Click on the Navigator and then choose **Dimensions**



Select the dimension from the dropdown list and click the pencil icon to edit



Check the box next to **Apply Security** and click **Save**



Dimension Security

Step 2 - Create Access Control Groups



- Access Control Groups are designed to group users by common access requirements thereby significantly reducing security maintenance
- We typically start with an Umbrella group that provides basic common access to all users
- Then we identify specific user access requirements and create necessary additional groups

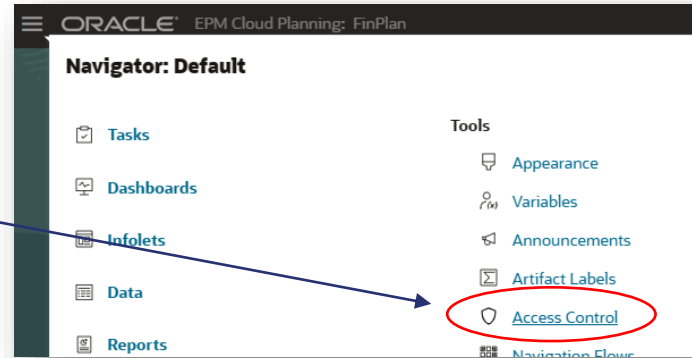
TIP – Your security administrator should aim to assign security to a new user by adding the user to 2-3 groups max: the umbrella group, an entity specific group and MAYBE one other special purpose group

GUIDELINE– the total number of groups should represent no more than 20-30% of total user count i.e. if you have 100 users, you could aim to accomplish security with no more than 20-30 groups

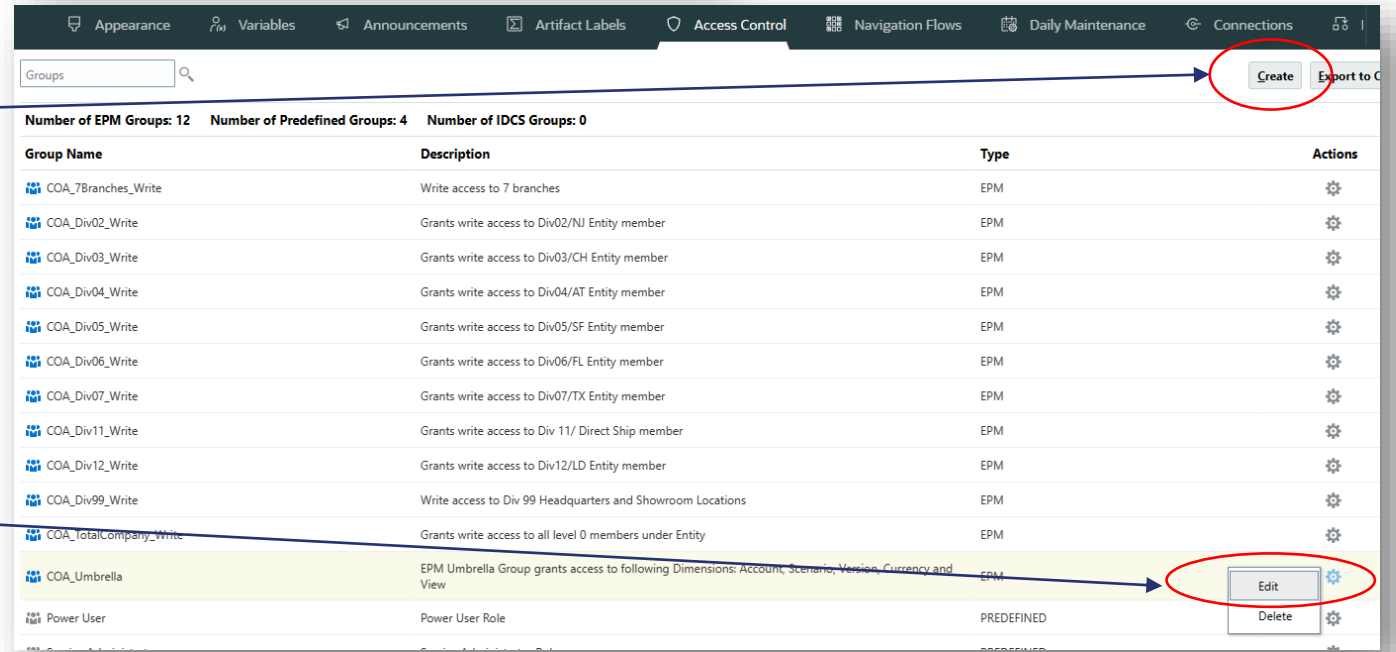
Dimension Security

Create Access Control Groups

From the Navigator click on Access Control



All existing groups are shown and you can click Create to start a new Group



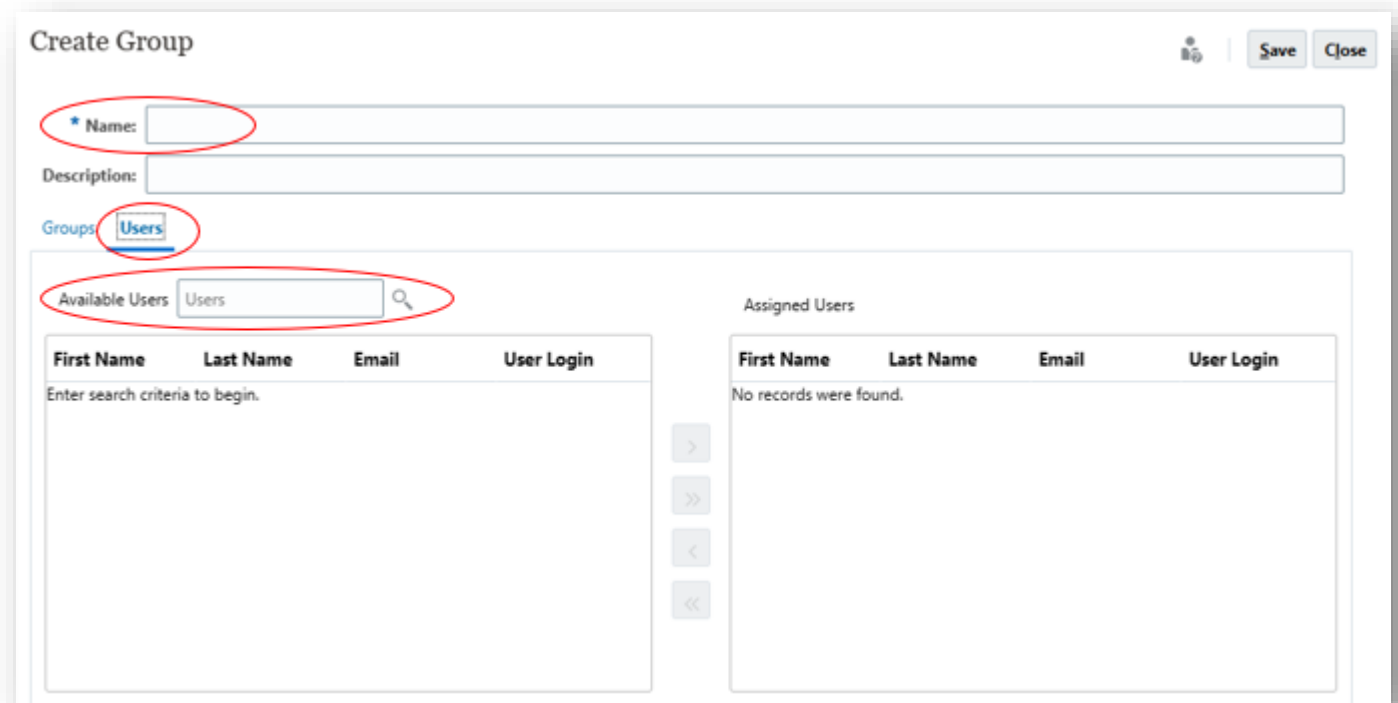
To see current or add/remove users assigned to a group click the Gear icon, then click on Edit

Dimension Security

Adding Users to an Access Control Group

- Give the new group an intuitive Name (required field)
- Add a description mentioning what Dimension(s) the group is used for
- Click on the User tab and click the magnifying glass to display what users have been provisioned to the application and are available to add to the new group
- Click Save

TIP – ONLY assign users to groups; DON'T assign other groups to an access control group because doing so creates difficulties tracing inherited access



Create Group

* Name:

Description:

Groups: **Users**

Available Users:

First Name	Last Name	Email	User Login
Enter search criteria to begin.			

First Name	Last Name	Email	User Login
No records were found.			

> >> < <<

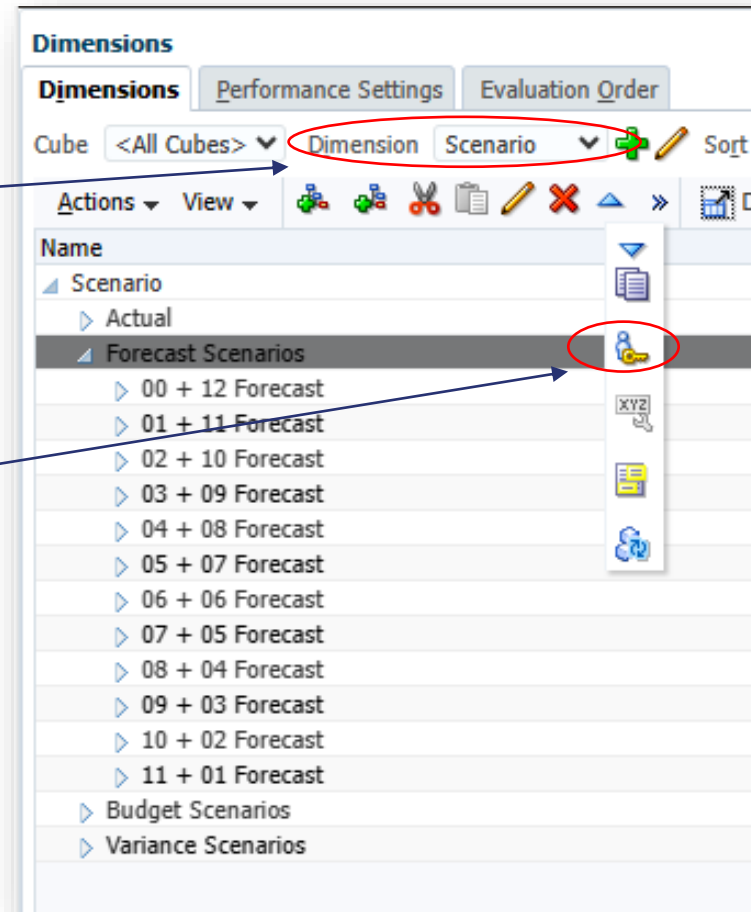
Dimension Security

Step 3 - Assign Access Control groups to hierarchy members in secured Dimensions

From the Navigator click on Dimensions and use the dropdown to select a dimension you applied Security to in step 1 – in this case the Scenario dimension

Highlight the member you wish to assign the Access Control Group to – in this case the Forecast Scenarios parent member - and click the Key icon

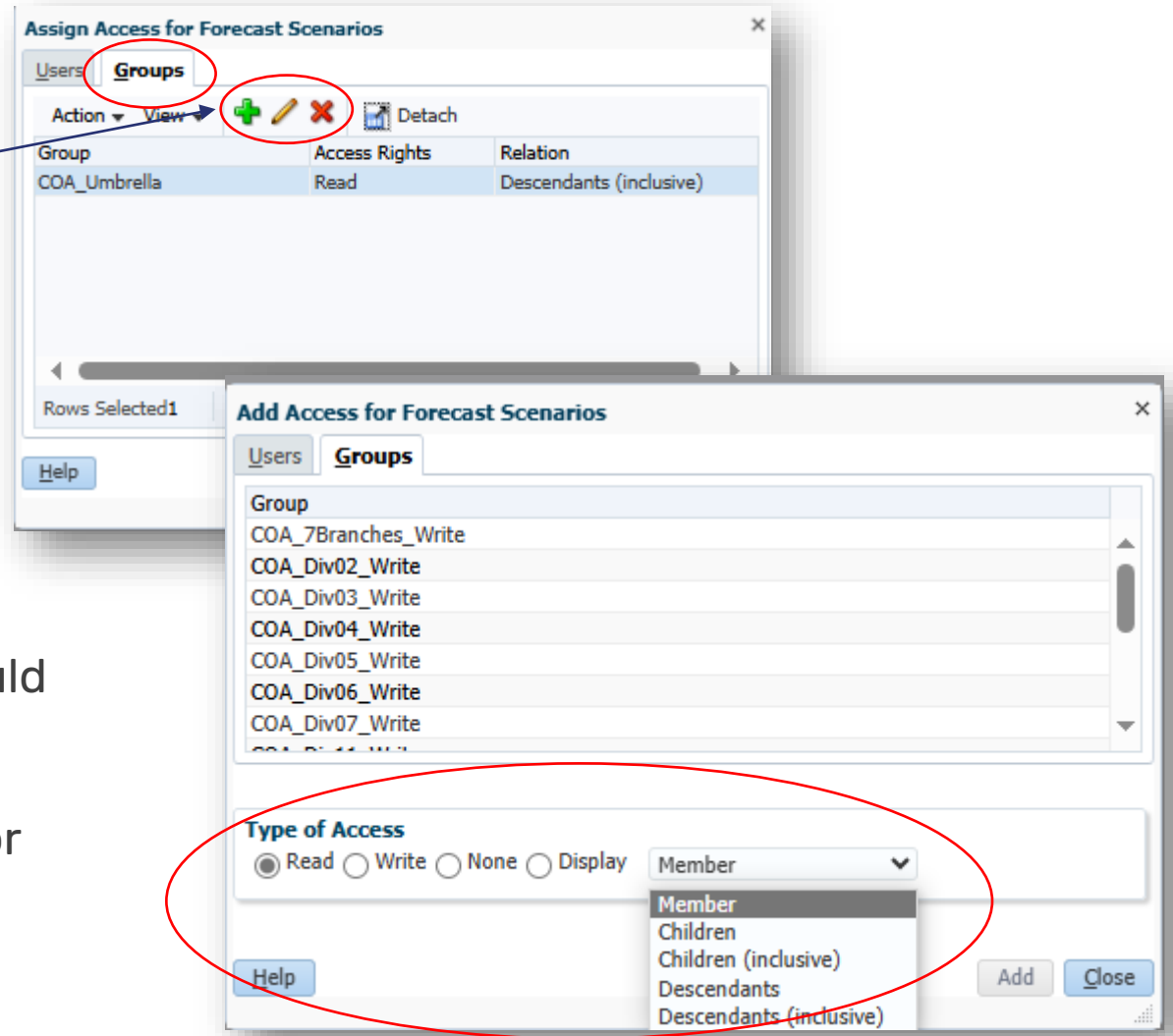
NOTE – access cannot be assigned at the topmost Dimension level



Dimension Security

Step 3 - Assign Access Control groups to hierarchy members in secured Dimensions

The Key icon will bring up the Assign Access dialogue box; Click on the Groups tab then on the Plus sign to add access (if a group has already been assigned you can also highlight that group and click the Pencil to Edit or the X to delete the access)



- Highlight the group you want to assign to the hierarchy member
- Choose the type of access the group should have: Read, Write or None
- Choose the relationship that the access should extend to: Member only, Children or Descendants
- Click Add

Dimension Security

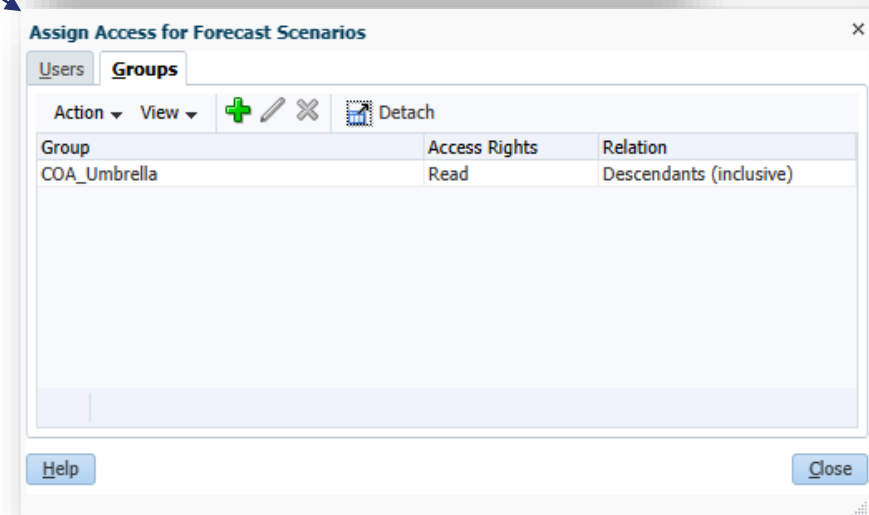
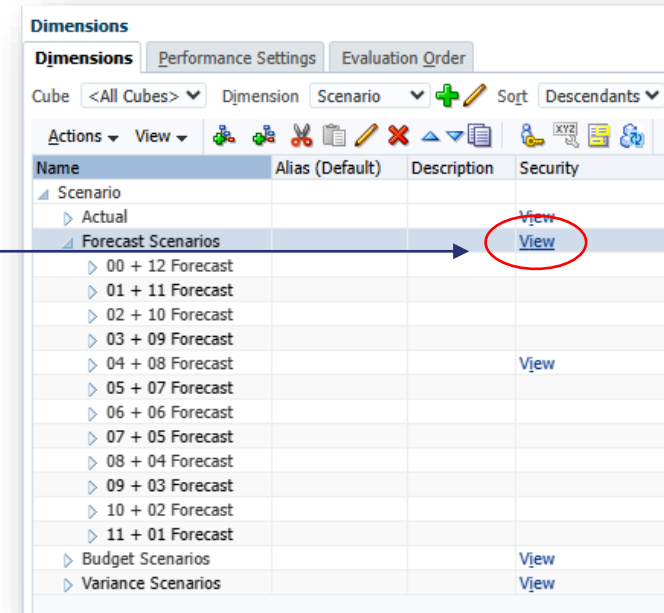
Verify that your desired Access is applied

After you've successfully applied Access to a hierarchy member you should see a clickable **View** link in the Security column for that member

Click on **View** to confirm that your desired parameters are applied

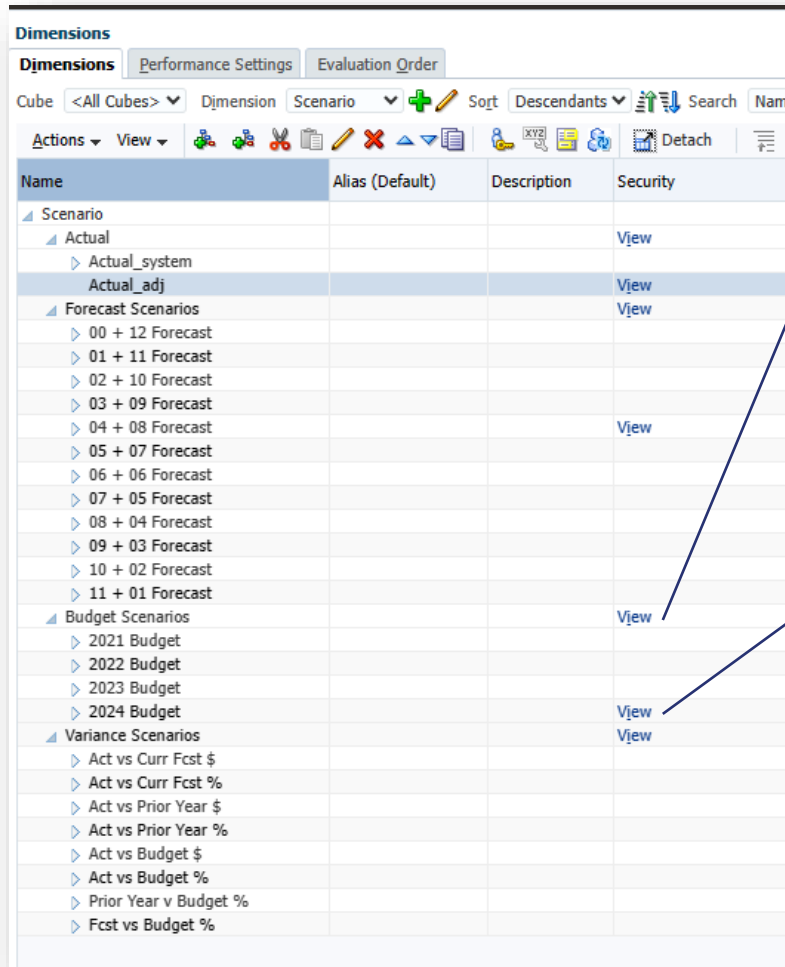
TIP – use the Descendants or Children relationship function wherever possible to reduce maintenance by applying security primarily at upper parent levels.

BEST PRACTICE – use the Member only relationship only for exception-based security – example is the current Forecast scenario set to Write access for the member only

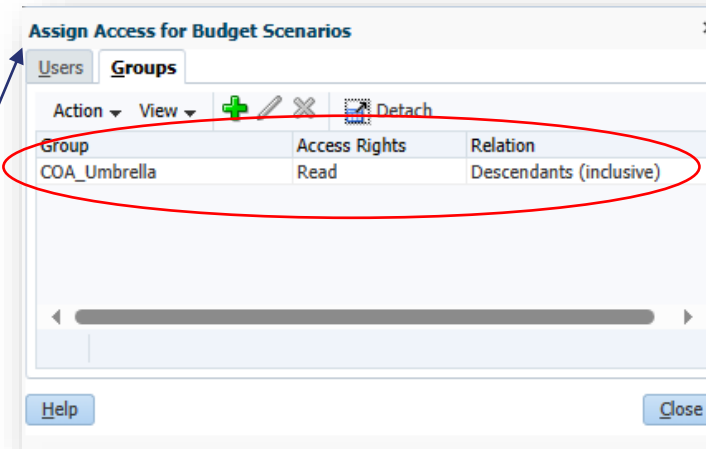


Dimension Security

Evaluating Dimension security needs – Scenario dimension

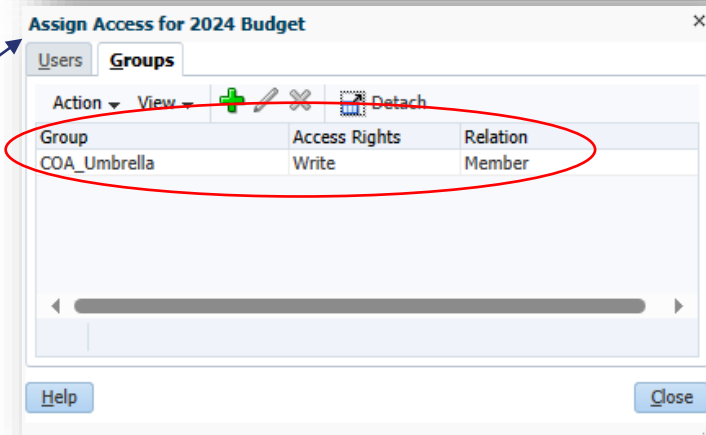


Name	Alias (Default)	Description	Security
Scenario			
Actual			View
Actual_system			
Actual_adj			View
Forecast Scenarios			View
00 + 12 Forecast			
01 + 11 Forecast			
02 + 10 Forecast			
03 + 09 Forecast			
04 + 08 Forecast			View
05 + 07 Forecast			
06 + 06 Forecast			
07 + 05 Forecast			
08 + 04 Forecast			
09 + 03 Forecast			
10 + 02 Forecast			
11 + 01 Forecast			
Budget Scenarios			View
2021 Budget			
2022 Budget			
2023 Budget			
2024 Budget			View
Variance Scenarios			View
Act vs Curr Fcst \$			
Act vs Curr Fcst %			
Act vs Prior Year \$			
Act vs Prior Year %			
Act vs Budget \$			
Act vs Budget %			
Prior Year v Budget %			
Fcst vs Budget %			



Group	Access Rights	Relation
COA_Umbrella	Read	Descendants (inclusive)

Read access is granted to all users for all Scenario members for reporting and analysis



Group	Access Rights	Relation
COA_Umbrella	Write	Member

Write access is granted to all users for the active Forecast and Budget scenarios and sometimes to Actual_Adj scenario

Dimension Security

Evaluating Dimension security needs – Version dimension

Dimensions

Dimensions | Performance Settings | Evaluation Order

Cube <All Cubes> | Dimension Version | Sort Descendants

Actions | View

Name	Alias (Default)	Description	Security
Version			
Working			View
Final			View
1st Pass			View
2nd Pass			View
3rd Pass			View

Assign Access for Working

Users | Groups

Action View + - ✕ Detach

Group	Access Rights	Relation
COA_Umbrella	Write	Member

Help Close

Assign Access for 1st Pass

Users | Groups

Action View + - ✕ Detach

Group	Access Rights	Relation
COA_Umbrella	Read	Member

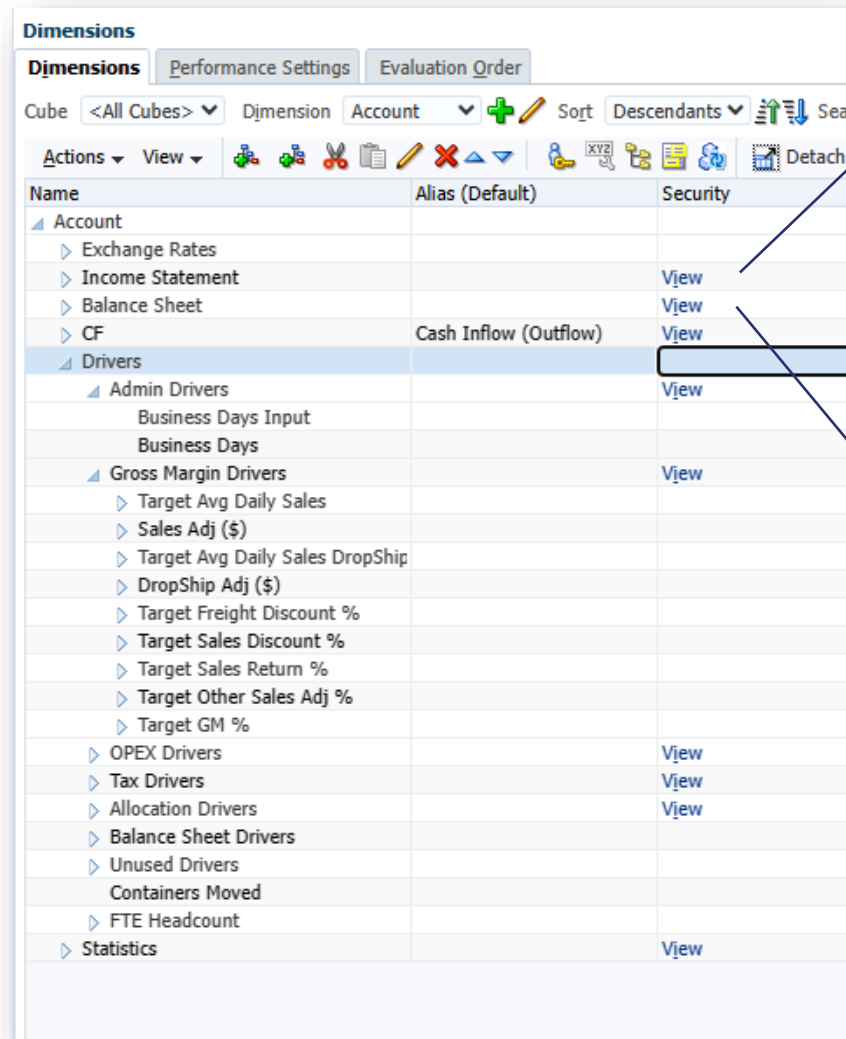
Help Close

Write access is granted to all users for the Working version member for active data entry to Forecast and Budget

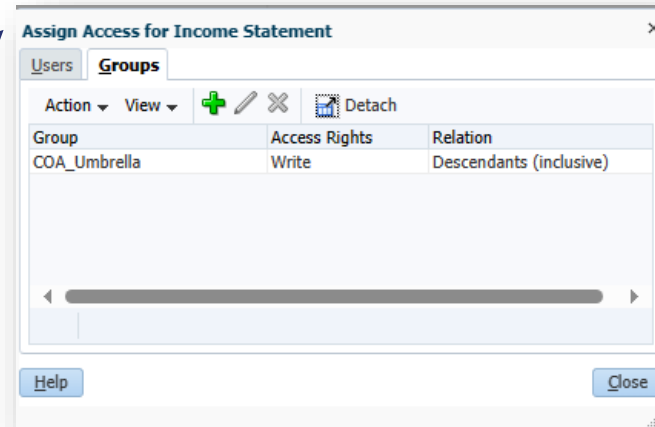
Read access is granted to Final member and all other Version members

Dimension Security

Evaluating Dimension security needs – Account dimension

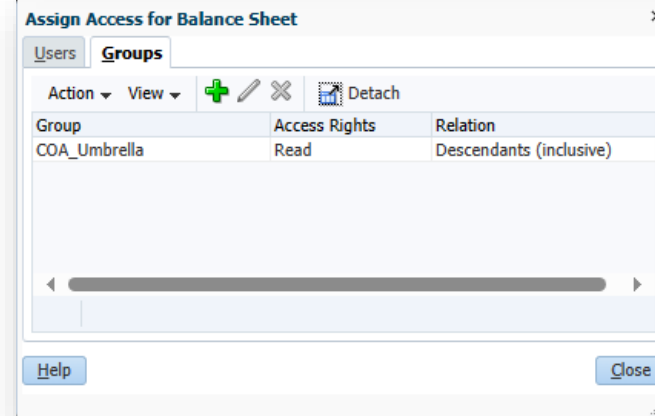


Name	Alias (Default)	Security
Account		
Exchange Rates		
Income Statement		View
Balance Sheet		View
CF	Cash Inflow (Outflow)	View
Drivers		View
Admin Drivers		View
Business Days Input		
Business Days		
Gross Margin Drivers		View
Target Avg Daily Sales		
Sales Adj (\$)		
Target Avg Daily Sales DropShip		
DropShip Adj (\$)		
Target Freight Discount %		
Target Sales Discount %		
Target Sales Return %		
Target Other Sales Adj %		
Target GM %		
OPEX Drivers		View
Tax Drivers		View
Allocation Drivers		View
Balance Sheet Drivers		
Unused Drivers		
Containers Moved		
FTE Headcount		
Statistics		View



Group	Access Rights	Relation
COA_Umbrella	Write	Descendants (inclusive)

Write access is granted to all users for all members of the IncStmnt hierarchy and to specific Driver input members to support Forecast and Budget entry

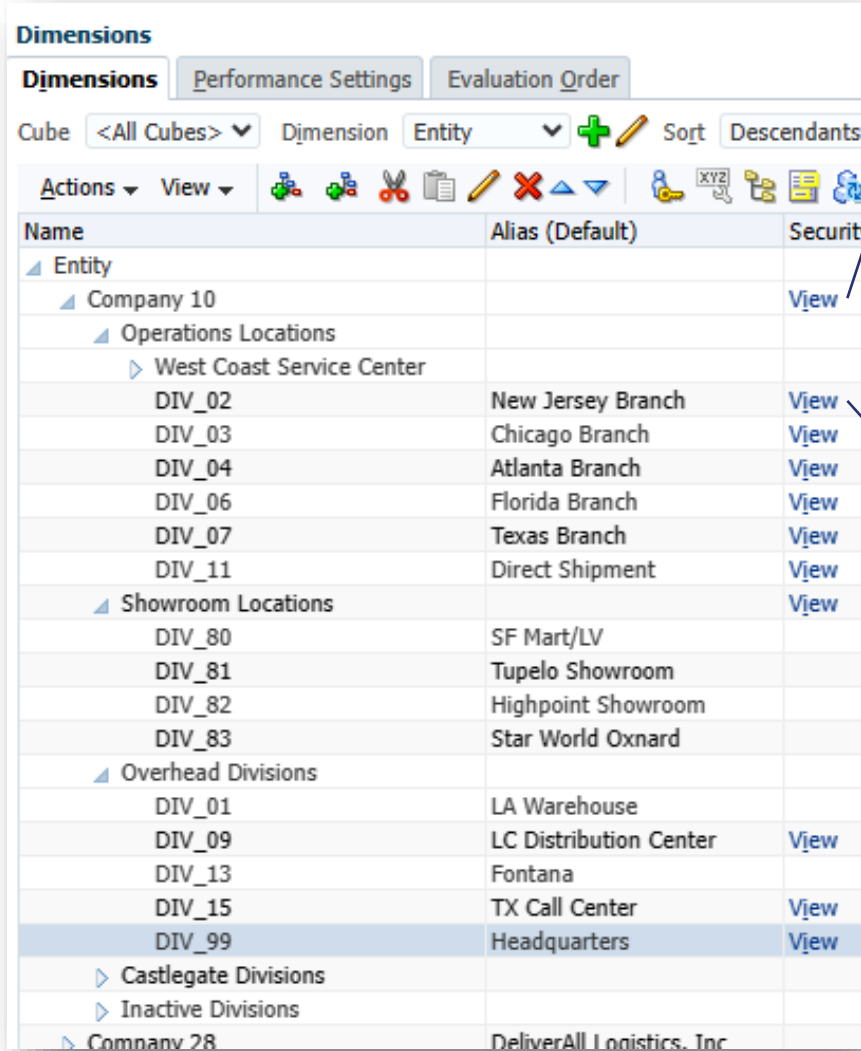


Group	Access Rights	Relation
COA_Umbrella	Read	Descendants (inclusive)

Read access is granted to Balance Sheet, Cash Flow Admin Drivers and Statistics since these do not require inputs from users

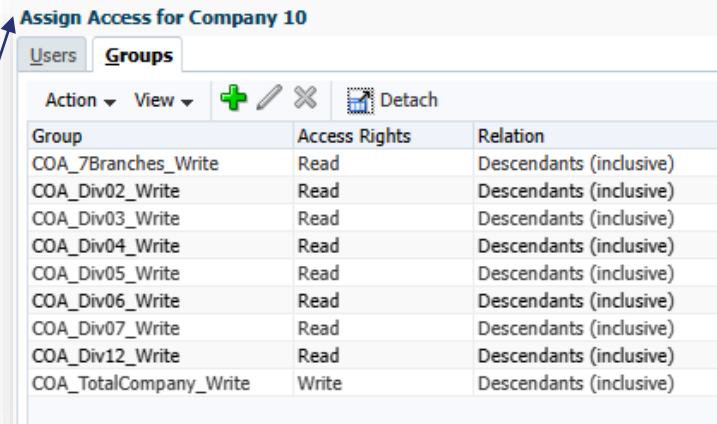
Dimension Security

Evaluating Dimension security needs – Entity dimension



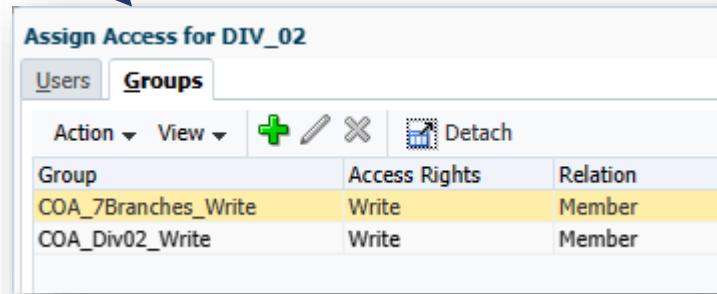
The screenshot shows the 'Dimensions' application interface. The 'Entity' dimension is selected, and the tree view is expanded to show 'Company 10' and its sub-divisions. The 'DIV_99' (Headquarters) is highlighted.

Name	Alias (Default)	Security
Entity		
Company 10		View
Operations Locations		
West Coast Service Center		
DIV_02	New Jersey Branch	View
DIV_03	Chicago Branch	View
DIV_04	Atlanta Branch	View
DIV_06	Florida Branch	View
DIV_07	Texas Branch	View
DIV_11	Direct Shipment	View
Showroom Locations		View
DIV_80	SF Mart/LV	
DIV_81	Tupelo Showroom	
DIV_82	Highpoint Showroom	
DIV_83	Star World Oxnard	
Overhead Divisions		
DIV_01	LA Warehouse	
DIV_09	LC Distribution Center	View
DIV_13	Fontana	
DIV_15	TX Call Center	View
DIV_99	Headquarters	View
Castlegate Divisions		
Inactive Divisions		
Company 28	DeliverAll Logistics, Inc	



The 'Assign Access for Company 10' dialog box shows a table of groups and their access rights. The 'Groups' tab is selected.

Group	Access Rights	Relation
COA_7Branches_Write	Read	Descendants (inclusive)
COA_Div02_Write	Read	Descendants (inclusive)
COA_Div03_Write	Read	Descendants (inclusive)
COA_Div04_Write	Read	Descendants (inclusive)
COA_Div05_Write	Read	Descendants (inclusive)
COA_Div06_Write	Read	Descendants (inclusive)
COA_Div07_Write	Read	Descendants (inclusive)
COA_Div12_Write	Read	Descendants (inclusive)
COA_TotalCompany_Write	Write	Descendants (inclusive)



The 'Assign Access for DIV_02' dialog box shows a table of groups and their access rights. The 'Groups' tab is selected.

Group	Access Rights	Relation
COA_7Branches_Write	Write	Member
COA_Div02_Write	Write	Member

Entity dimension access typically requires more specific access

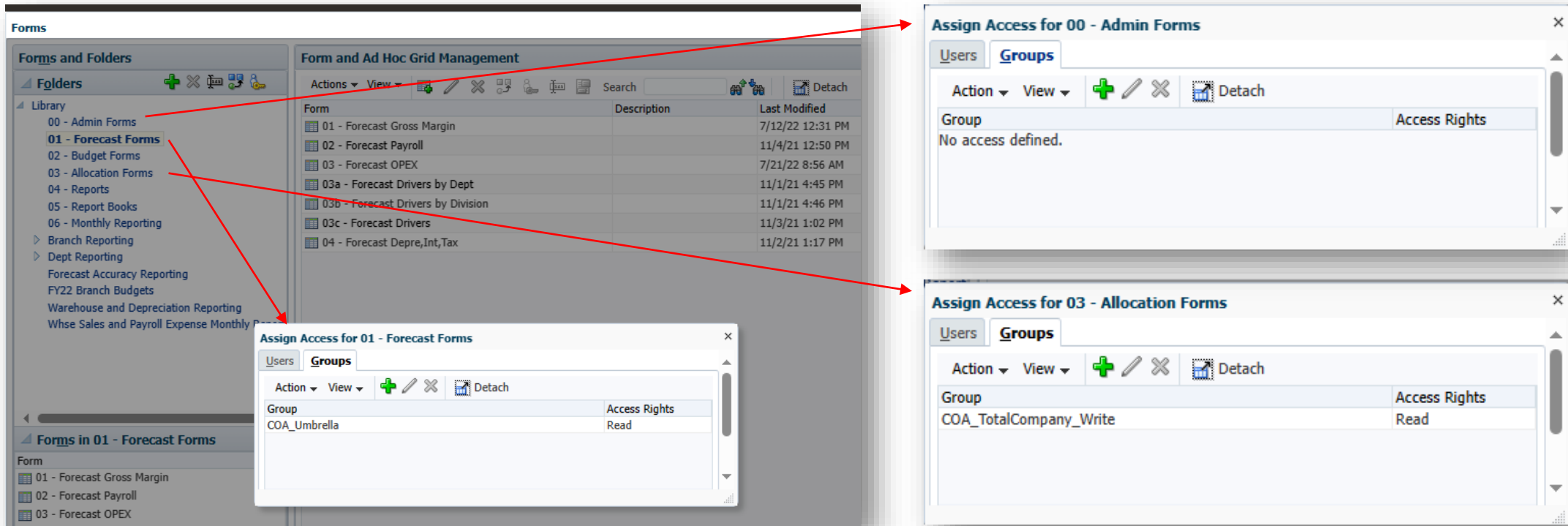
Groups for specific areas of responsibility have been created

Read access is granted at total company level but Write access is much more controlled

Business Rule and Form Access

Access Control Groups are for more than just Dimensions

- Typically use the Umbrella Group to ensure that users have ability to use Forms and Launch Business Rules
- Restricted Access forms/business rules can use one of the specific use Groups to grant access



The screenshot displays the 'Forms' management interface. On the left, a 'Forms and Folders' tree shows a hierarchy starting with '00 - Admin Forms' and '01 - Forecast Forms'. The main area, 'Form and Ad Hoc Grid Management', lists various forms with columns for 'Form', 'Description', and 'Last Modified'. Three 'Assign Access' dialog boxes are overlaid on the interface, each showing a table of 'Groups' and their 'Access Rights'. Red arrows indicate the flow from the folder tree to the dialog boxes.

Assign Access for 01 - Forecast Forms

Group	Access Rights
COA_Umbrella	Read

Assign Access for 00 - Admin Forms

Group	Access Rights
No access defined.	

Assign Access for 03 - Allocation Forms

Group	Access Rights
COA_TotalCompany_Write	Read

Security Components

What are the available layers of security?

- **Provisioning** – this represents the EPM *functionality* a user can access (not data access) - MANDATORY
- **Dimension Security** – using access control groups to define what datasets a user can see (Read) and update (Write) - MANDATORY
 - **Valid Intersections** – restricting ability to enter data by creating rules that mark certain member intersections as valid (or invalid) for data entry - OPTIONAL
 - **Cell Level Security** – further limitation of Dimension access to restrict users from viewing or modifying data values in certain cell intersections - OPTIONAL

AGENDA

Angie Caruthers



Provisioning via OCI



Dimensional Security



Valid Intersections



Cell Level Security



Reporting/Troubleshooting

Valid Intersections

What are they and why should I care?

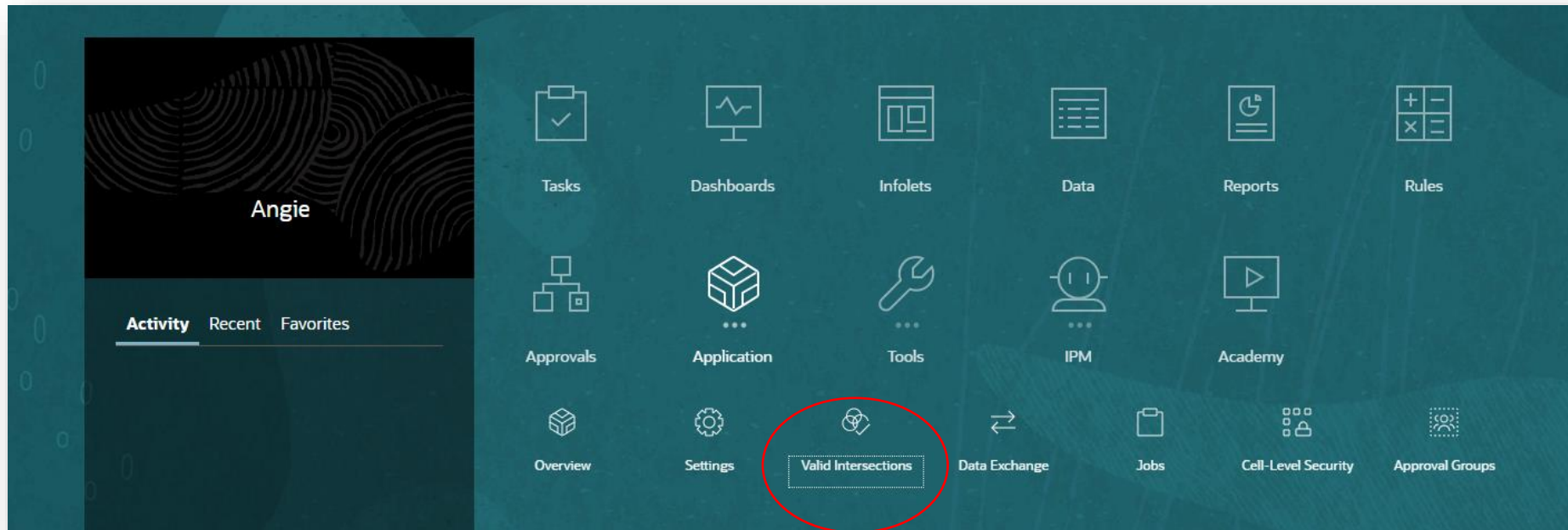


- Used to streamline data input forms for users and prevent data input in improper intersections.
 - limits available drop down choices,
 - condenses Forms to a smaller, more manageable format,
 - speeds background calculations by eliminating irrelevant membersets
- Valid intersection groups DON'T grant access per se to dimension members.
- Valid intersection groups DO further restrict the subset of dimension members viewable or editable to an application user.
- ALWAYS test to make sure your definition does what you intended
- Did not exist in On-Prem environments

Valid Intersections

Where Do I find Valid Intersection Rules?

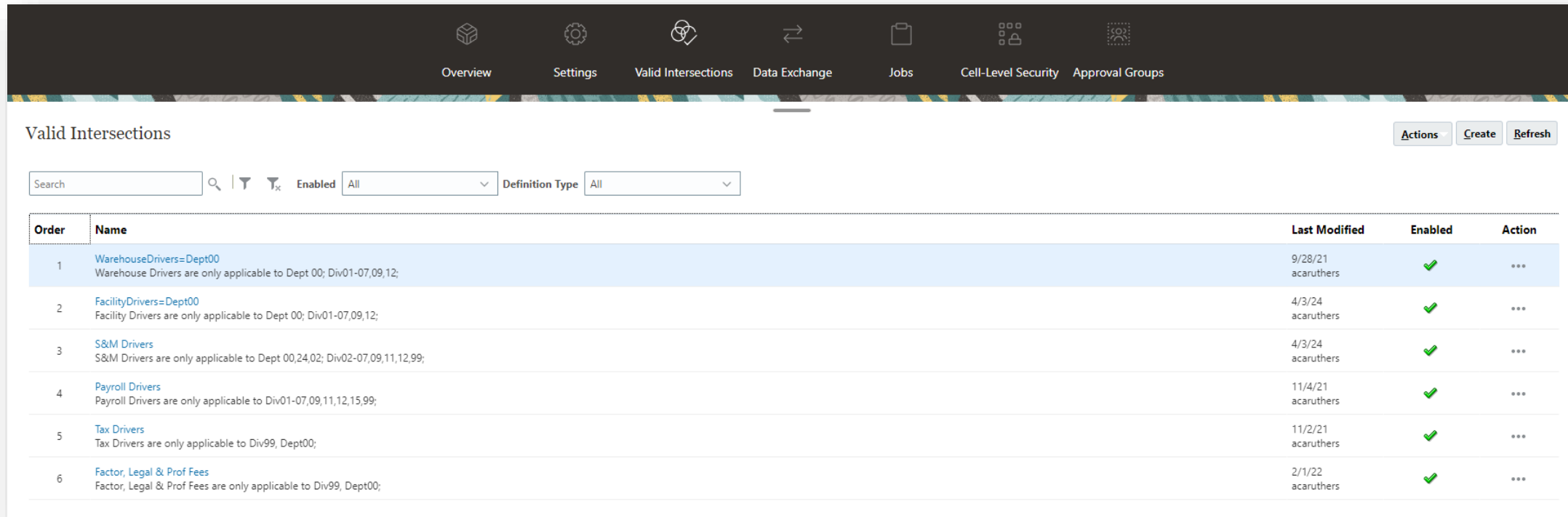
- From the Home screen click on the **Application** tile and then on the **Valid Intersections** tile



Valid Intersections

Where Do I find Valid Intersection Rules?

- Here you can view/edit what Valid Intersection rules exist and/or create new ones
 - You can Enable or Disable a rule
 - You can use Definition Type to see whether a rule defines Valid Intersections or Invalid Intersections



The screenshot shows a web application interface for managing Valid Intersections. At the top, there is a navigation bar with icons and labels for Overview, Settings, Valid Intersections (selected), Data Exchange, Jobs, Cell-Level Security, and Approval Groups. Below the navigation bar, the page title is "Valid Intersections" with "Actions", "Create", and "Refresh" buttons on the right. A search bar and filter controls are present, including a search input, a magnifying glass icon, a funnel icon, a filter icon, an "Enabled" dropdown set to "All", and a "Definition Type" dropdown set to "All". The main content is a table with the following data:

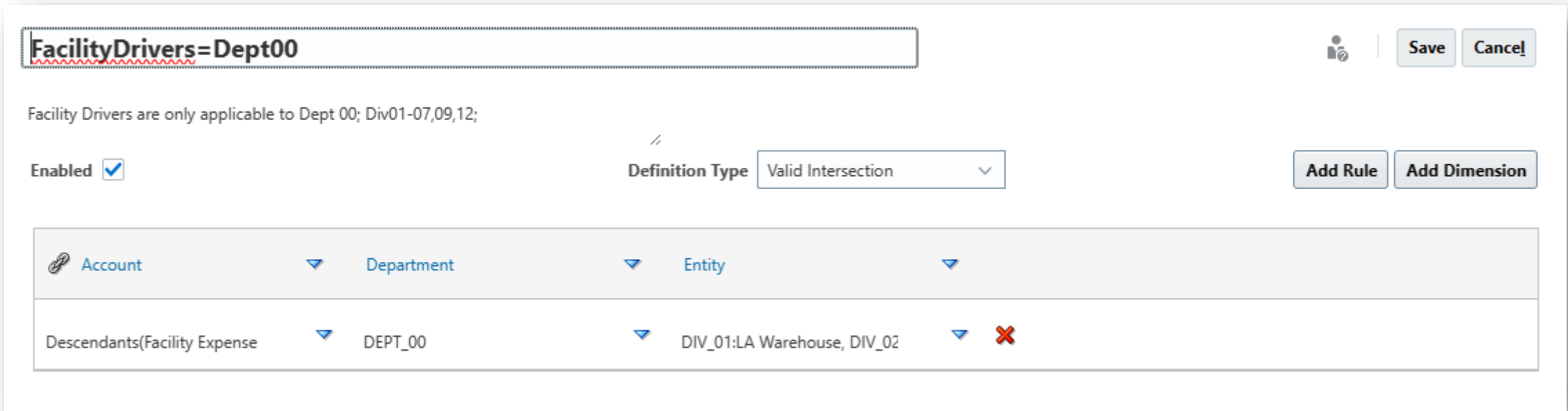
Order	Name	Last Modified	Enabled	Action
1	WarehouseDrivers=Dept00 Warehouse Drivers are only applicable to Dept 00; Div01-07,09,12;	9/28/21 acaruthers	✓	...
2	FacilityDrivers=Dept00 Facility Drivers are only applicable to Dept 00; Div01-07,09,12;	4/3/24 acaruthers	✓	...
3	S&M Drivers S&M Drivers are only applicable to Dept 00,24,02; Div02-07,09,11,12,99;	4/3/24 acaruthers	✓	...
4	Payroll Drivers Payroll Drivers are only applicable to Div01-07,09,11,12,15,99;	11/4/21 acaruthers	✓	...
5	Tax Drivers Tax Drivers are only applicable to Div99, Dept00;	11/2/21 acaruthers	✓	...
6	Factor, Legal & Prof Fees Factor, Legal & Prof Fees are only applicable to Div99, Dept00;	2/1/22 acaruthers	✓	...

Valid Intersections – Use Case

Limit inputs to specific member combinations

In this case the client wanted to ensure that Facility expense is Forecasted only at specific Department/Division combinations

- First we specified that the Rule defines Valid Intersections – anything not specified will automatically be considered Invalid
- Next we have defined the Account dimension as the anchor dimension in which we have specified that this rule applies to all members under Facility Expense Drivers parent
- Then we have added the Department dimension and specified that ONLY department 00 can support entry in the Facility driver account members
- Finally, we have further added the Entity dimension to restrict inputs to the nine Divisions shown



The screenshot shows a configuration window for a rule named "FacilityDrivers=Dept00". The rule is enabled and has a "Valid Intersection" definition type. It is configured with three dimensions: Account (Descendants(Facility Expense)), Department (DEPT_00), and Entity (DIV_01:LA Warehouse, DIV_02). The interface includes buttons for "Save", "Cancel", "Add Rule", and "Add Dimension".

Account	Department	Entity
Descendants(Facility Expense)	DEPT_00	DIV_01:LA Warehouse, DIV_02

Security Components

What are the available layers of security?

- **Provisioning** – this represents the EPM *functionality* a user can access (not data access) - MANDATORY
- **Dimension Security** – using access control groups to define what datasets a user can see (Read) and update (Write) - MANDATORY
- **Valid Intersections** – restricting ability to enter data by creating rules that mark certain member intersections as valid (or invalid) for data entry - OPTIONAL
- **Cell Level Security** – further limitation of Dimension access to restrict users from viewing or modifying data values in certain cell intersections - OPTIONAL

AGENDA

Angie Caruthers



Provisioning via OCI



Dimensional Security



Valid Intersections



Cell Level Security



Reporting/Troubleshooting

Cell Level Security

What is Cell level security?

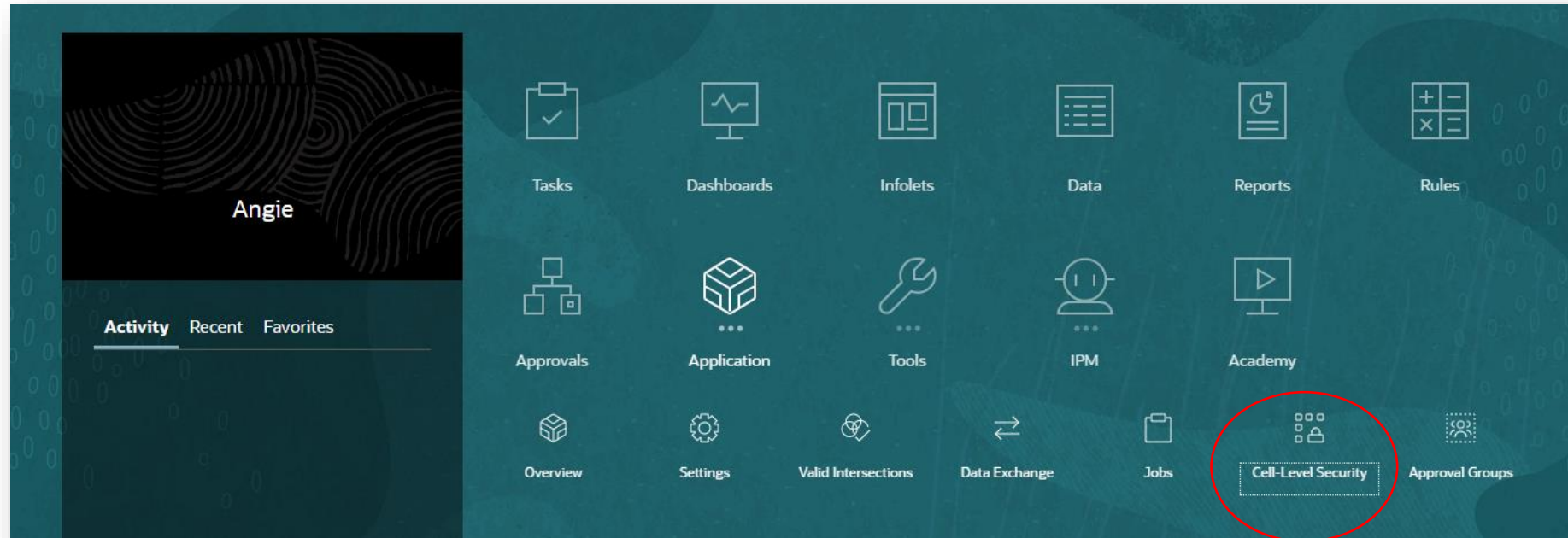


- Exception based security that applies ON TOP OF the regular dimension based security
 - Use to plug any small gaps in overall dimension security
- This is Optional security - if you don't need it, don't use it
- Don't go overboard with these - if you have more than a handful your Dimensional security is likely not optimized

Cell Level Security

Where Do I find Cell Level Security Rules?

- From the Home screen click on the **Application** tile and then on the **Cell Level Security** tile



Cell Level Security

Where Do I find Cell Level Security Rules?

- Here you can view/edit what Cell Level Security rules exist and/or create new ones
 - You can Enable or Disable a rule
 - You can enter a user in the Effective Assignment box to see which rules impact a given user's dimensional security
 - You can filter rules to see which ones restrict Write access and which ones restrict Read access
 - You can also use the Test functionality to see how a rule affects a given user on a given Form

Cell-Level Security Definitions [Actions](#) [Test](#) [Create](#) [Refresh](#)

Search | Effective Assignment Enabled Restriction

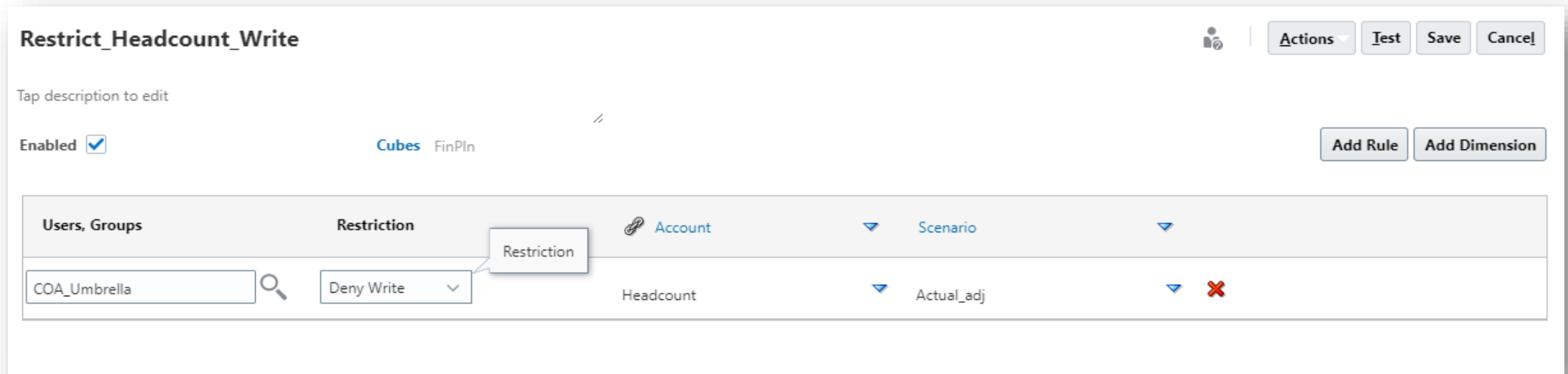
Order	Name	Last Modified	Enabled	Action
1	Restrict_Headcount_Write	10/1/21 Not Available	✓	...
2	Restrict HQ Personnel Read access	7/15/22 acaruthers	✓	...

Cell Level Security – Use Case 1

Use case for restricting Write access

In this case, Headcount is a driver that users input to create their Forecast/Budget. They inherit Write access to the Headcount member from the Drivers parent in the Account dimension. However, users also have Write access to the Actual_Adj scenario in order to input any operational metrics that aren't sourced from the General Ledger. Since Actual Headcount values aren't sourced from the GL, an Administrator is loading those values to the Actual_Adj scenario. This creates a conflict in that we don't want operational users to be able to update the Headcount member in the Actual_Adj intersection. We can limit this access with a very specific exception using Cell Level Security

- Define the User/Group that needs restriction (in this case it's the Umbrella group that contains all non-admin users)
- Determine whether the additional security is meant to limit Write access or Read access
- Specify the Account dimension member to be restricted
- Specify the Scenario dimension member to be restricted



Restrict_Headcount_Write Actions Test Save Cancel

Tap description to edit

Enabled Cubes FinPln Add Rule Add Dimension

Users, Groups	Restriction	Account	Scenario
COA_Umbrella	Deny Write	Headcount	Actual_adj

Cell Level Security – Use Case 2

Use case for restricting Read access

In this case, we want to restrict Branch Manager's visibility to Payroll Expenses to only their Branch

- We need to use multiple rules
 - Define the User/Group that needs restriction
 - Determine whether the additional security is meant to limit Write access or Read access
 - Specify the Account dimension members to be restricted
 - Specify the Entity members to be restricted

Restrict HQ Personnel Read access Actions Test Save Cancel

Tap description to edit

Enabled Cubes FinPln,FinRpt Add Rule Add Dimension

Users, Groups	Restriction	Account	Entity
COA_Div06_Write,COA_Div04_	Deny Read	Descendants(PB:Total Personn	DIV_99:Headquarters
COA_Div07_Write	Deny Read	Descendants(PR:Payroll)	DIV_02:New Jersey Branch, DI'
COA_Div02_Write	Deny Read	Descendants(PR:Payroll)	DIV_03:Chicago Branch, DIV_C
COA_Div03_Write	Deny Read	Descendants(PR:Payroll)	DIV_02:New Jersey Branch, DI'

Security Components

What are the available layers of security?

- **Provisioning** – this represents the EPM *functionality* a user can access (not data access) - MANDATORY
- **Dimension Security** – using access control groups to define what datasets a user can see (Read) and update (Write) - MANDATORY
- **Valid Intersections** – restricting ability to enter data by creating rules that mark certain member intersections as valid (or invalid) for data entry - OPTIONAL
- **Cell Level Security** – further limitation of Dimension access to restrict users from viewing or modifying data values in certain cell intersections - OPTIONAL

AGENDA

Angie Caruthers



Provisioning via OCI



Dimensional Security



Valid Intersections



Cell Level Security



Reporting/Troubleshooting

Security Reporting

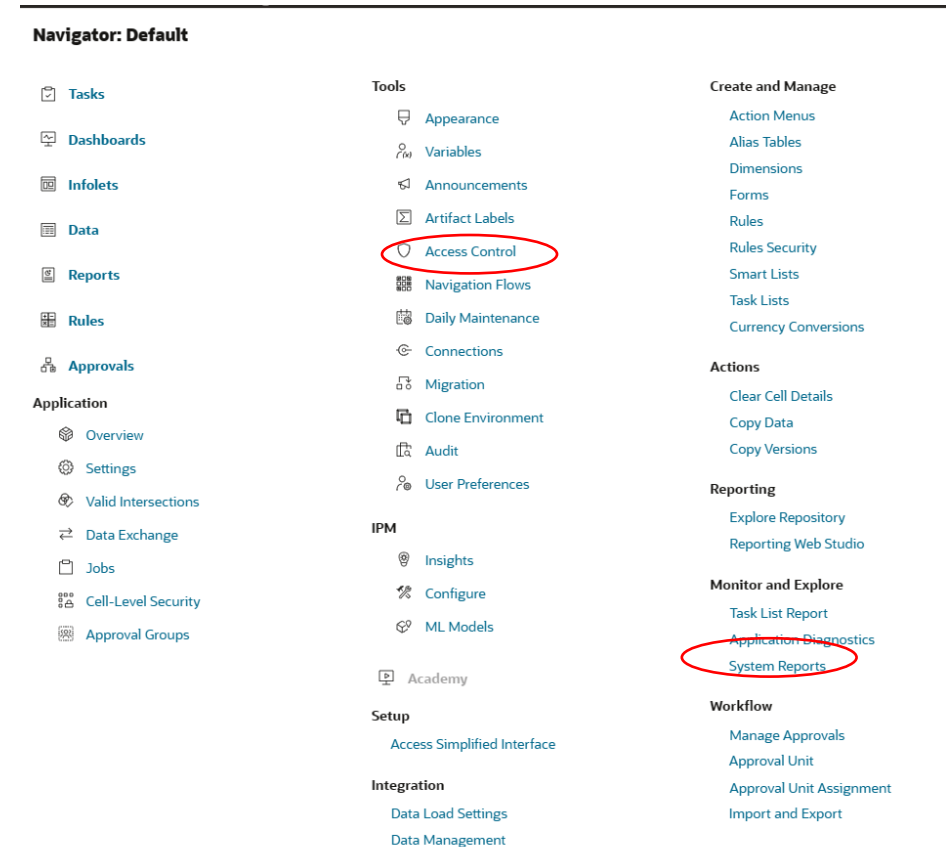
How can I tell what security is applied in my current environment?

Access Control reports show:

- Available Groups
- Available Users
- Users provisioned roles
- User Group assignment report
- User Login report

System Reports show:

- Users access assigned vs effective
- Dimension security assignments



The screenshot shows a navigation menu titled "Navigator: Default" with several categories of items. The "Tools" category includes "Access Control", which is circled in red. The "Monitor and Explore" category includes "System Reports", also circled in red. Other categories include Tasks, Dashboards, Infolets, Data, Reports, Rules, Approvals, Application, IPM, Setup, Integration, Create and Manage, Actions, Reporting, and Workflow.

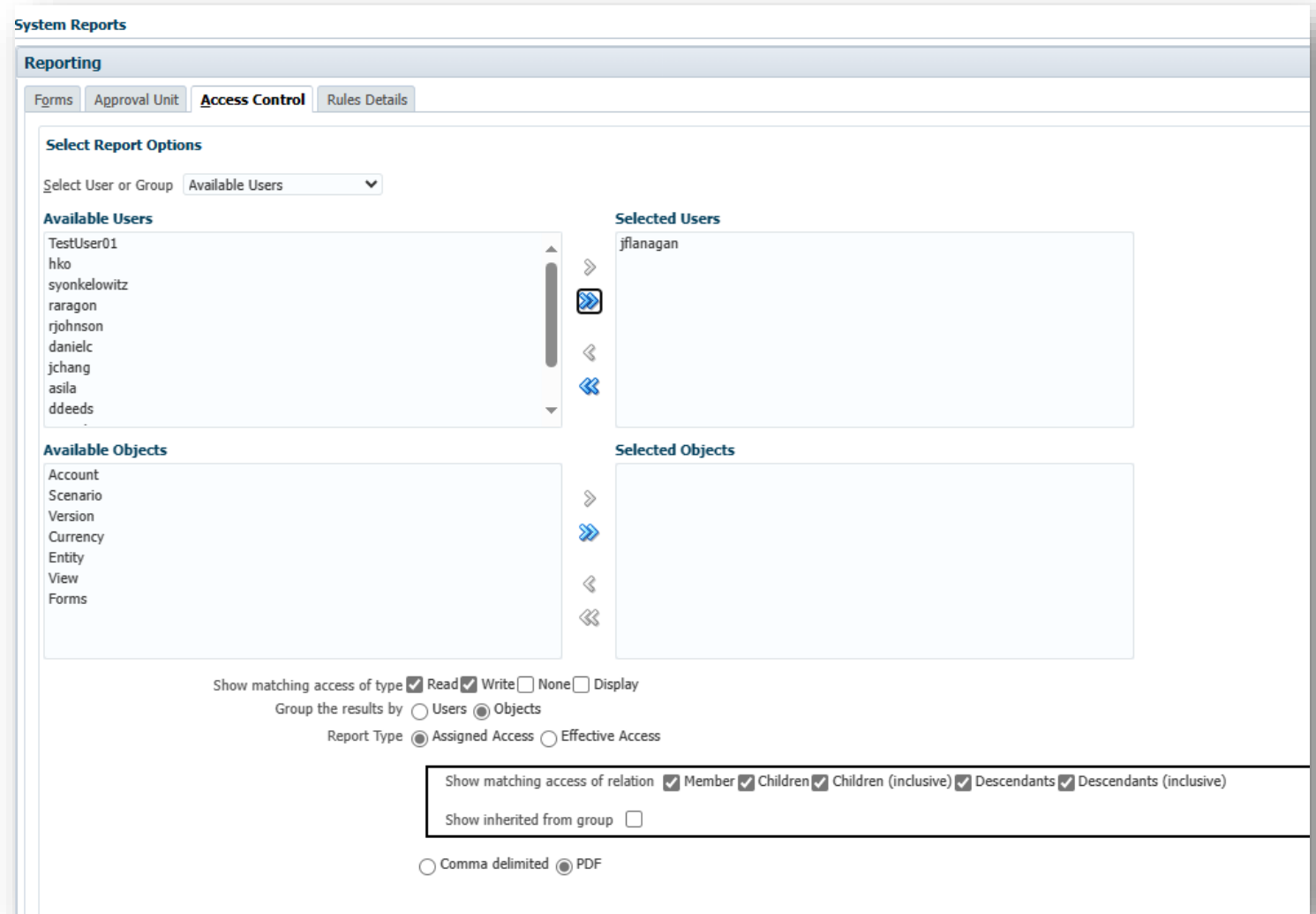
- Navigator: Default**
 - Tasks
 - Dashboards
 - Infolets
 - Data
 - Reports
 - Rules
 - Approvals
 - Application
 - Overview
 - Settings
 - Valid Intersections
 - Data Exchange
 - Jobs
 - Cell-Level Security
 - Approval Groups
 - IPM
 - Insights
 - Configure
 - ML Models
 - Academy
 - Setup
 - Access Simplified Interface
 - Integration
 - Data Load Settings
 - Data Management
- Tools**
 - Appearance
 - Variables
 - Announcements
 - Artifact Labels
 - Access Control**
 - Navigation Flows
 - Daily Maintenance
 - Connections
 - Migration
 - Clone Environment
 - Audit
 - User Preferences
- Create and Manage**
 - Action Menus
 - Alias Tables
 - Dimensions
 - Forms
 - Rules
 - Rules Security
 - Smart Lists
 - Task Lists
 - Currency Conversions
- Actions**
 - Clear Cell Details
 - Copy Data
 - Copy Versions
- Reporting**
 - Explore Repository
 - Reporting Web Studio
- Monitor and Explore**
 - Task List Report
 - Application Diagnostics**
 - System Reports**
- Workflow**
 - Manage Approvals
 - Approval Unit
 - Approval Unit Assignment
 - Import and Export

Security Reporting

System Reports

From System Reports click on Access Control tab:

- Select a specific user OR group
- Select any or all dimensions
- Can choose to see directly assigned access or 'effective' access inherited from group assignments



The screenshot shows the 'System Reports' interface with the 'Reporting' section selected. The 'Access Control' tab is active, displaying a 'Select Report Options' form. The form includes a dropdown for 'Select User or Group' set to 'Available Users'. Below this are two columns: 'Available Users' and 'Selected Users'. The 'Available Users' list contains: TestUser01, hko, syonkelowitz, raragon, rjohnson, danielc, jchang, asila, and ddeeds. The 'Selected Users' list contains: jflanagan. There are also 'Available Objects' and 'Selected Objects' lists. The 'Available Objects' list contains: Account, Scenario, Version, Currency, Entity, View, and Forms. The 'Selected Objects' list is empty. At the bottom of the form, there are several checkboxes and radio buttons for configuring the report: 'Show matching access of type' with checkboxes for Read (checked), Write (checked), None (unchecked), and Display (unchecked); 'Group the results by' with radio buttons for Users (unchecked) and Objects (checked); 'Report Type' with radio buttons for Assigned Access (checked) and Effective Access (unchecked); 'Show matching access of relation' with checkboxes for Member (checked), Children (checked), Children (inclusive) (checked), Descendants (checked), and Descendants (inclusive) (checked); 'Show inherited from group' (unchecked); and 'Comma delimited' (unchecked) and 'PDF' (checked) radio buttons.

Troubleshooting Tips

How do I figure out why a user can't see certain data?



- Get a screenshot from the user!
- Verify that the user's member selection for each secured dimension matches the access granted by their group assignment
- Verify that the user has Group Assignments that cover all secured dimensions
- Use a Test User id to replicate the groups assigned to the problem user

Security Optimization Checklist

My Security footprint is a mess – how do I fix it?



- Users receive access via Groups only
- Groups are not assigned to other Groups (nested security)
- Ratio of Groups to Users is between 20-30%
- All dimension access can be assigned using an Umbrella Group and 1 or 2 other specialty groups

THANK YOU

Angie Caruthers



469.867.9017



www.olympusconsulting.com



angie@olympusconsulting.com



Frisco, Texas



ODTUG Kscope24

nashville, tn

july 14 - 18



Don't Forget To Fill Out Your Evals