

# Control Access to Manufacturing Work Definitions Using Data Security



**Whitepaper By – Diptikanta Satpathy**

## Contents

Control Access to Manufacturing Work Definitions Using Data Security .....	2
Business Requirement.....	2
Overview .....	2
Data Security Policy.....	2
Actions .....	3
Points to consider .....	4
Use Case.....	5
Enable Data Security for Work Definitions.....	5
Define data security policies .....	5
Navigation .....	5
Manage Data Security Controls for Manufacturing .....	11
Navigation .....	11
Scenario-1: User with View Access tried to create work definition.....	12
Scenario-2: User with Maintain Access tried to create work definition .....	13
Conclusion.....	13
References.....	14
About the author .....	14

## Control Access to Manufacturing Work Definitions Using Data Security

A much-needed functionality in Oracle Fusion Manufacturing related to Work Definition Access control has been released in Update 23D. This has been a sought- after requirement by the Oracle community for quite some time in Oracle Fusion.

### Business Requirement

A set of users need to maintain work definitions of one product group/class called as Laptop, but they should only be able to view work definitions of another product group/class called Desktop. Similarly, another set of users need to maintain work definitions of Desktop, but they should only be able to view work definitions of Laptop. Another set of users need to just view both the work definitions.

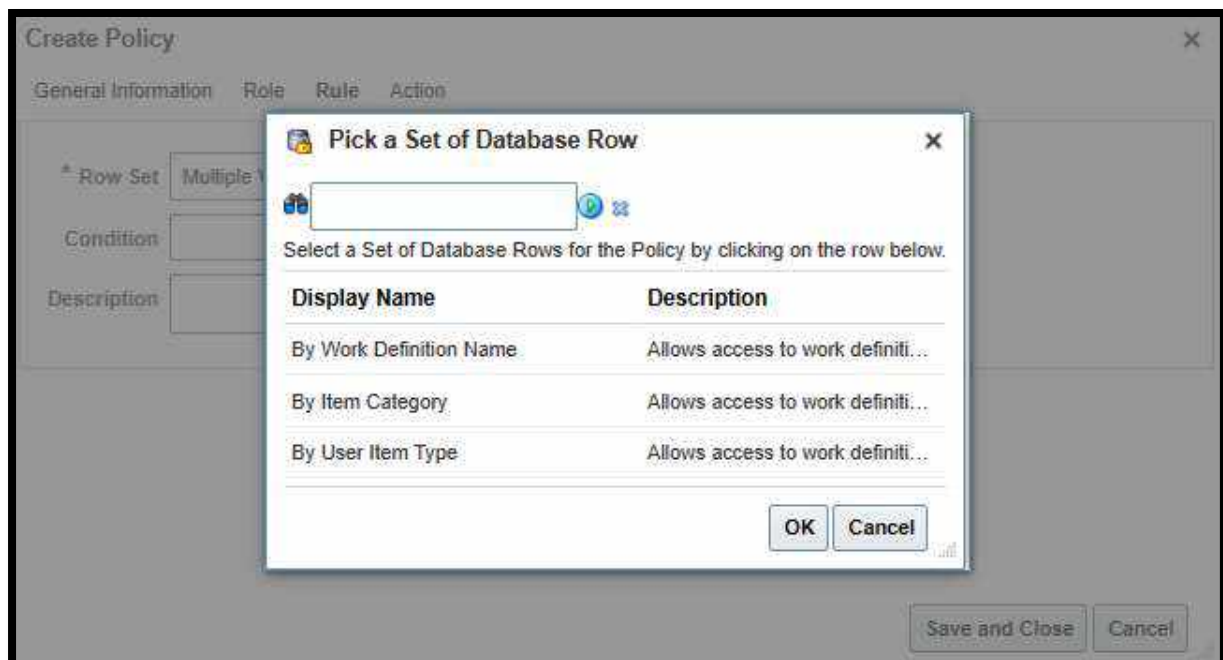
Through Manufacturing Engineer role, either maintain or view access can be provided or restricted to all or none of the users. Till release 23C, providing both maintain and view access to the same set of users was not possible.

### Overview

This functionality controls a user's access to maintain (create, update, delete) or view manufacturing work definitions based on data security policies.

### Data Security Policy

A data security policy is defined by specifying a seeded or custom condition and one or more actions and is assigned to seeded or custom job roles. There are three ways to define a policy using conditions (i) user item type, (ii) item category, and (iii) work definition name.



For user item type and item category, the codes need to be used and for work definition name, the internal name is required to be specified in the parameters.

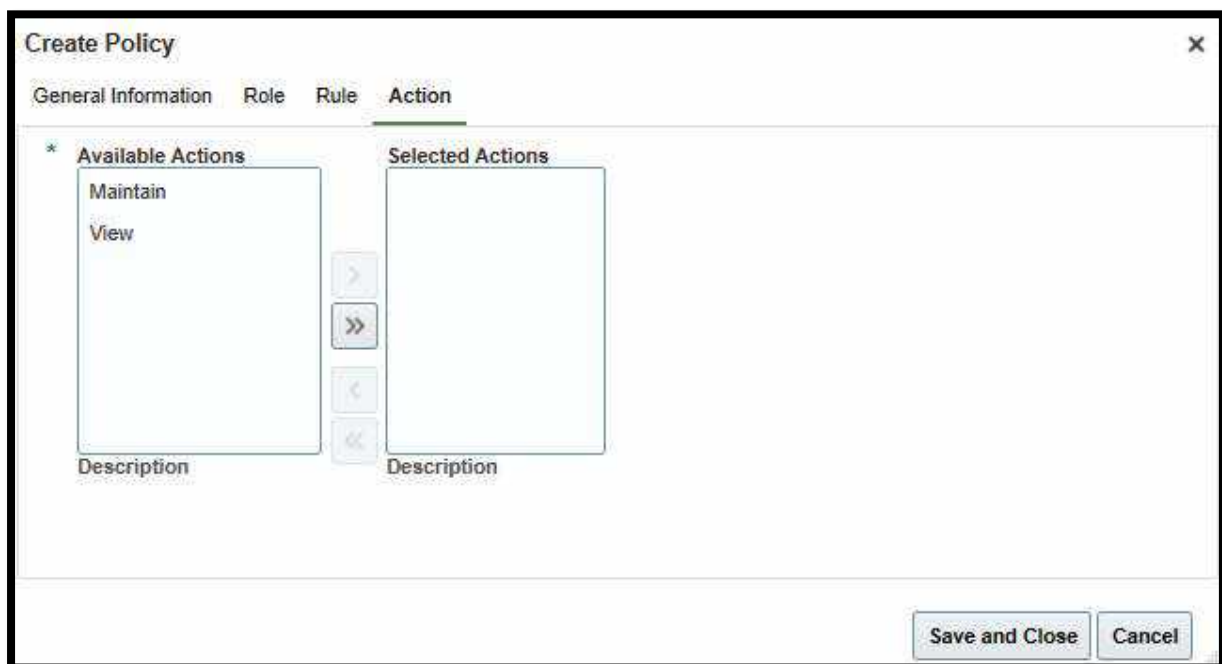
User-defined custom conditions can also be created. When defining a custom condition, either Filter or SQL Predicate can be specified as a condition type. For the attribute tree picker user interface to

define a simple condition, a Filter need to be chosen. SQL Predicate can be chosen when the attributes names of the condition are known. SQL WHERE clause can be used to specify a dynamic condition, using a parameterized SQL predicate. For more information on how to define a custom condition, refer to the Managing Oracle Fusion Applications Data Security Policies documentation.

## Actions

Two seeded actions have been provided in the applications, and system does not allow to define custom actions.

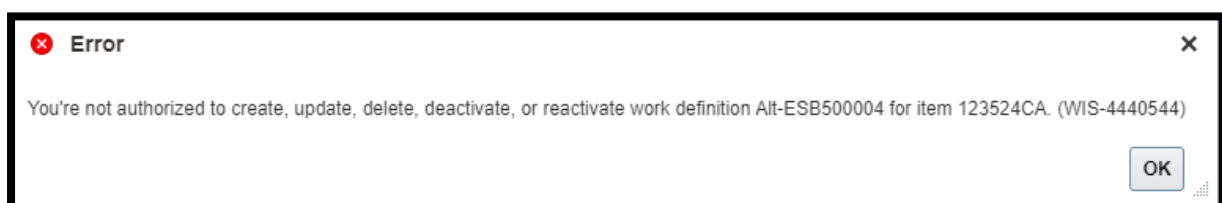
The seeded actions are Maintain and View. The action Maintain allows access to create, update, and delete work definitions, including deactivate and reactivate work definitions. Maintain action does not encompass the View action. The View action allows access to search and view work definitions, including print work definition report.



If a user through their roles has been granted only the View action and not also Maintain action, upon trying to either create, update, delete, deactivate, or reactivate a work definition, they will receive an error message:

“You're not authorized to create, update, delete, deactivate, or reactivate work definition <work definition name> for item <item name> (WIS-4440544).”

e.g., “You're not authorized to create, update, delete, deactivate, or reactivate work definition Alt-ESB500004 for item 123524CA. (WIS-4440544)”





Data security applies to both discrete and process manufacturing, and to all interfaces, which are the user interface, Application Development Framework Desktop Integration (ADFdi), File-Based Data Import (FBDI), and REST service.

### Points to consider

The following points need to be considered before enabling data security for manufacturing work definitions:

- If data security for manufacturing work definition is enabled without first defining data security policies, then users will not have access to any work definitions.
- If there is a need for certain users to be able to access all work definitions, then a policy with a rule where the row set is specified as all values can be defined.
- To maintain work definitions using the user interface and ADFdi, both View and Maintain actions need to be assigned, whereas FBDI and REST, need only Maintain action.
- Between function privilege and data security, the most restrictive access between the privilege and specified action applies. For example, if the user has the Manage Work Definitions function privilege, but the data security policy allows only View action, then they can access the work definitions in view only mode.
- There is no change to organization access, which will continue to be granted using the Manage Manufacturing Plant Data Access for Users task.

## Use Case

### Enable Data Security for Work Definitions

Enabling data security for manufacturing work definitions is a 2-step process.

- I. Define data security policies
- II. Enable data security for manufacturing work definition business object

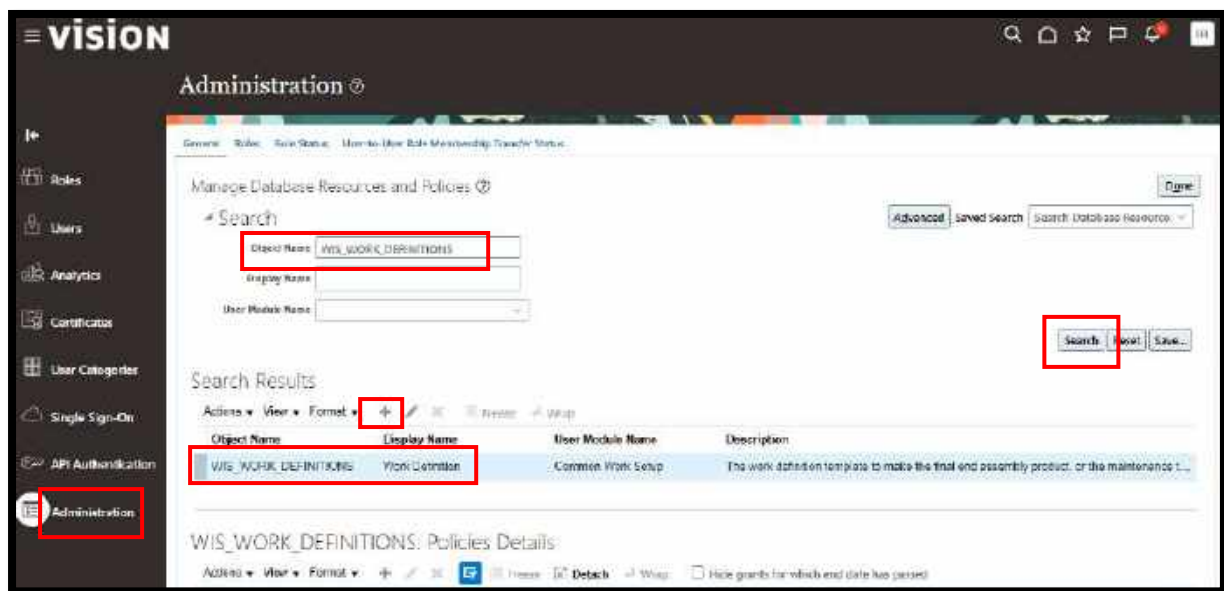
#### Define data security policies

In the Security Console, go to Manage Data Security Policies task. Then, navigate to the Administration page, next to the Manage Database Resources page.

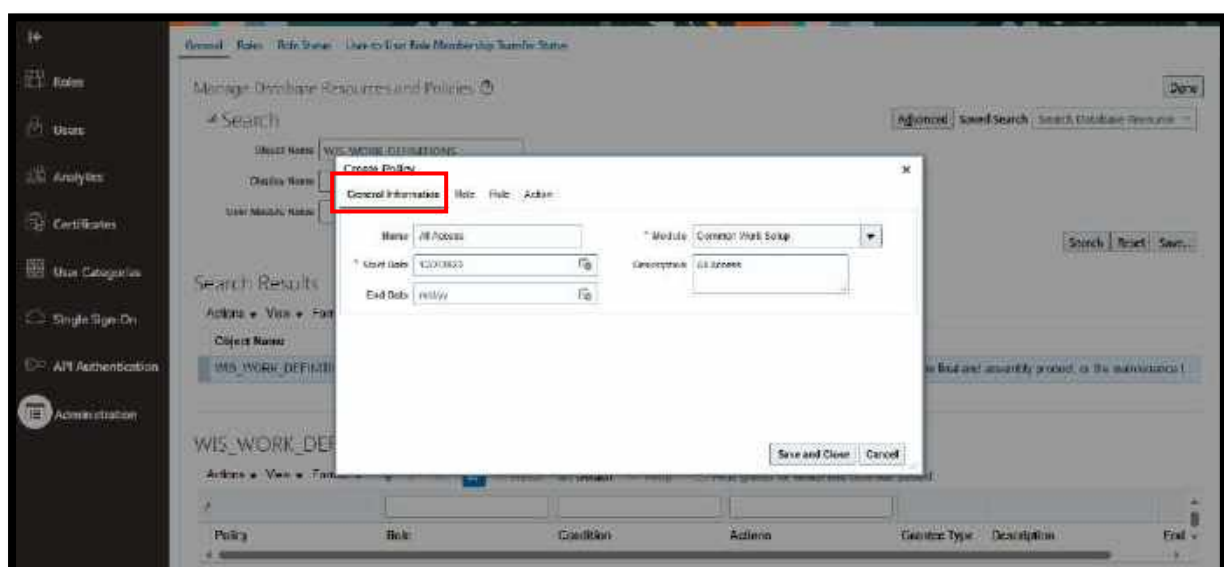
#### Navigation

Tools > Security console > Administration > Manage Database Resources and Policies

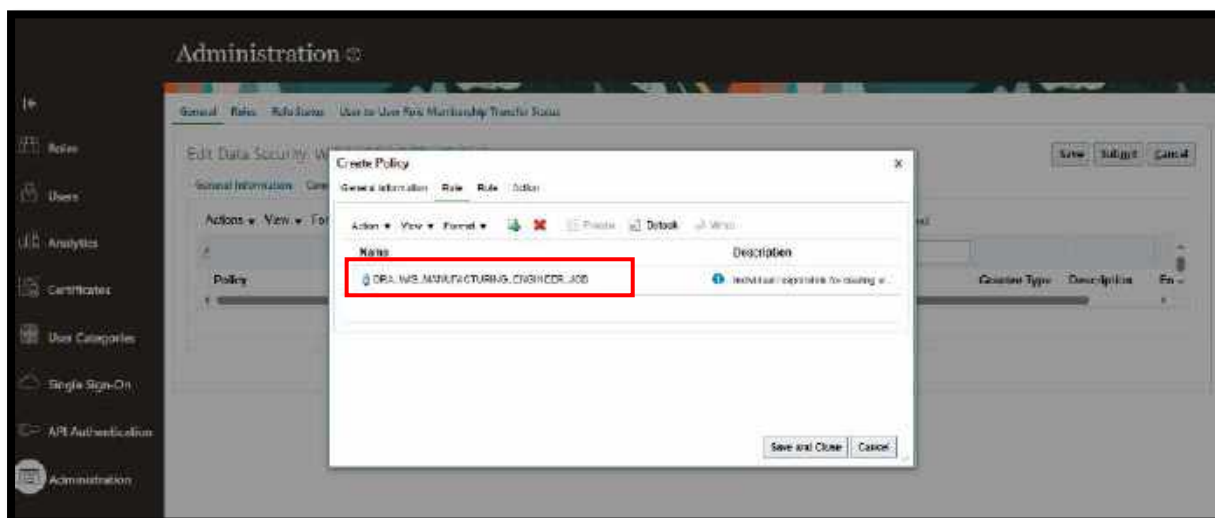
Search for object name WIS\_WORK\_DEFINITIONS and click on the plus icon to create a new policy.



Go to the General information tab and add the detail like Name and Start Date.



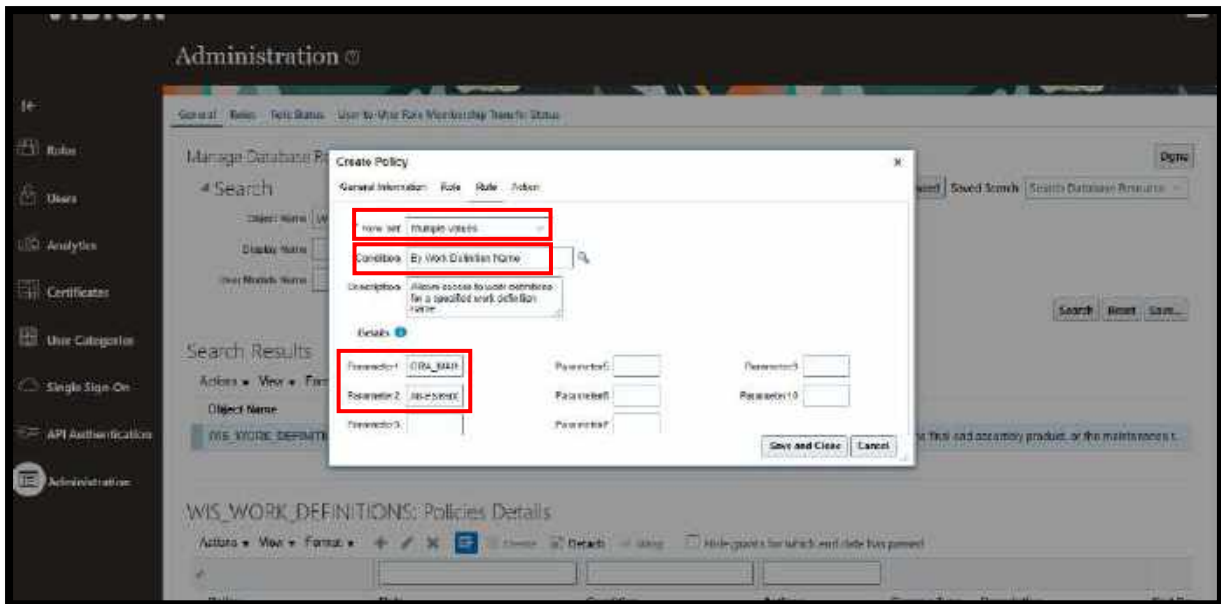
Next, go to the Role tab and select the role name against which the policy is being created. For example, on the following screenshot Manufacturing Engineer role has been used to create the policy.



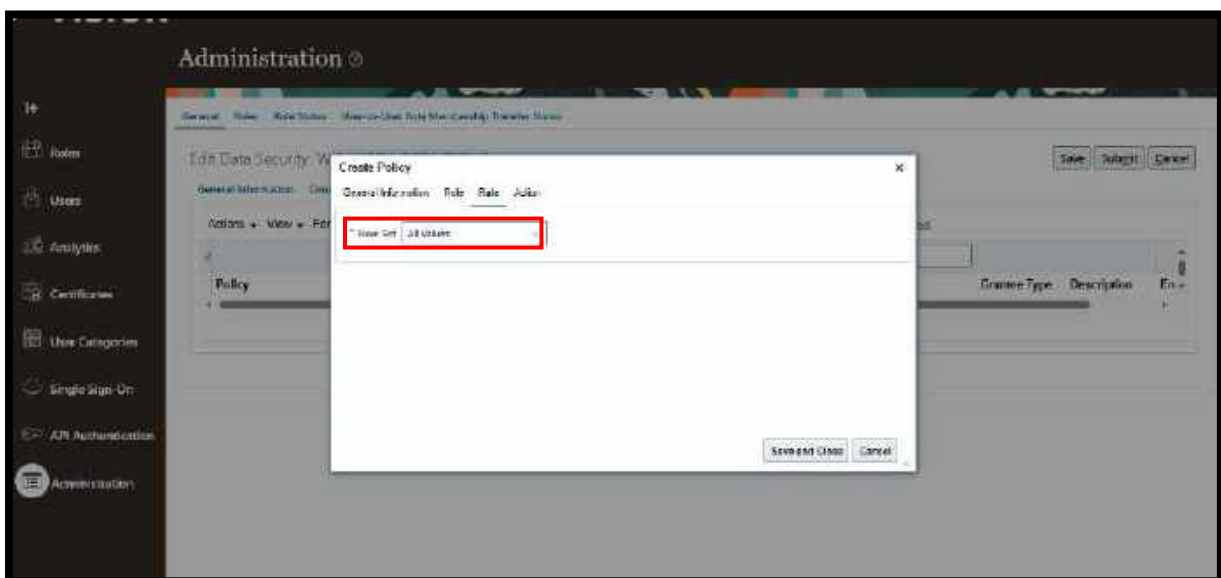
After adding the Role, go to the Rule tab and select the values as required.

There are 3 values for row set: (i) multiple values, (ii) all values, and (iii) single value. If row set is specified as multiple values, user can use either a seeded or custom condition. If row set is specified as all values, then the users will have access to all work definitions. If row set is specified as single value, then user will have to specify the work definition ID, and the users will have access to that specific work definition.

For creating a policy by Work Definition Name, select Multiple Values in the Row set field. Select condition as By Work Definition Name. In the Parameters field, provide the Work definitions Internal Names as shown below.



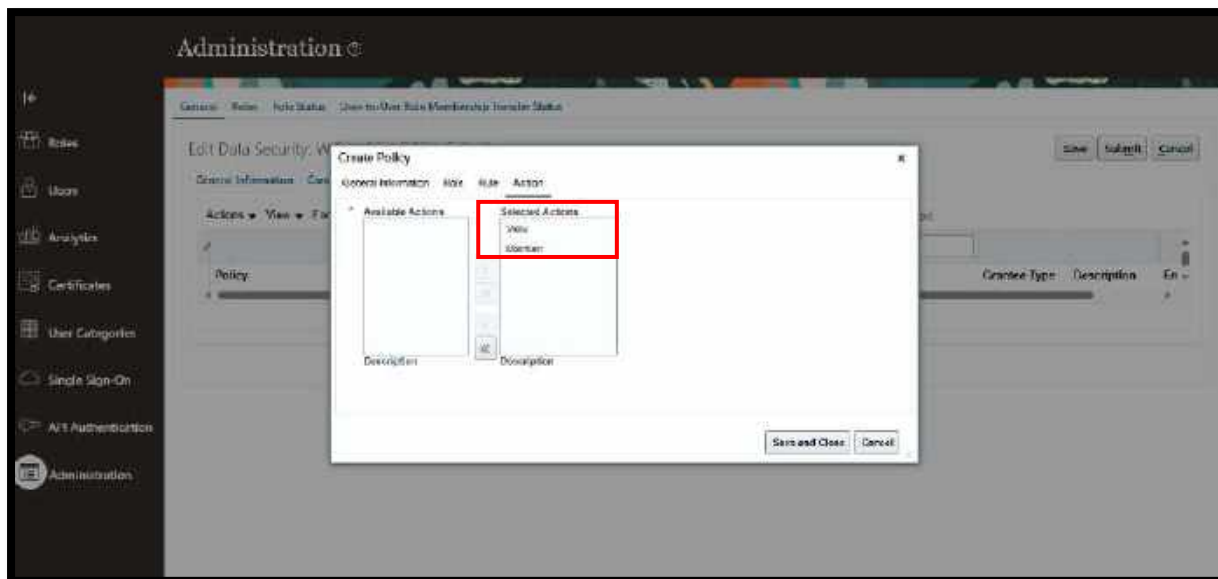
Add all the Work Definition names for which the policy needs to be defined.



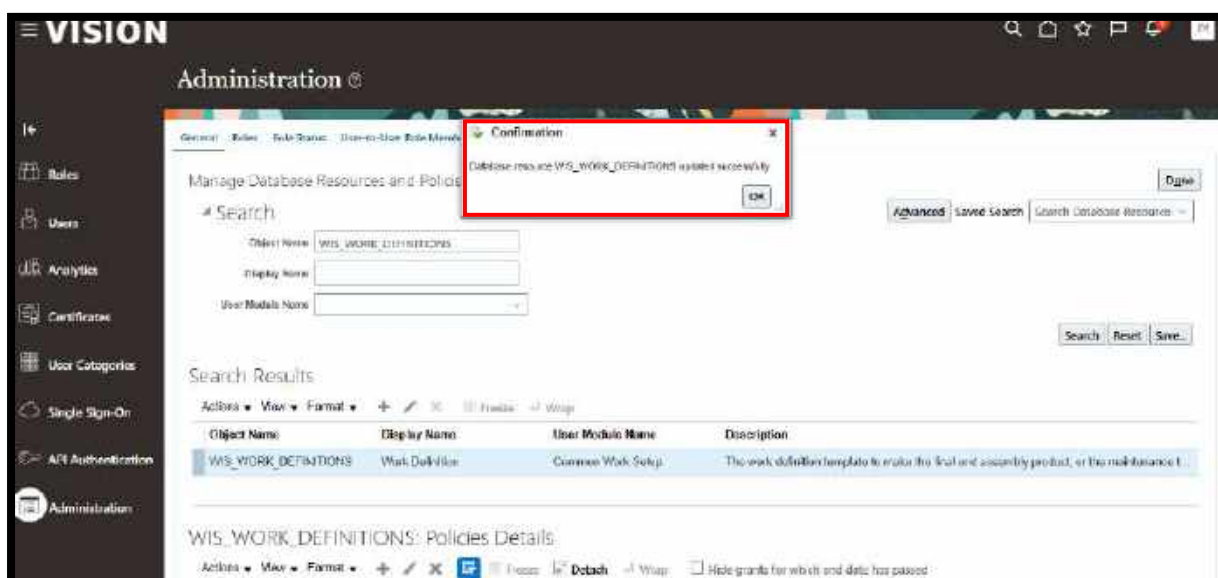
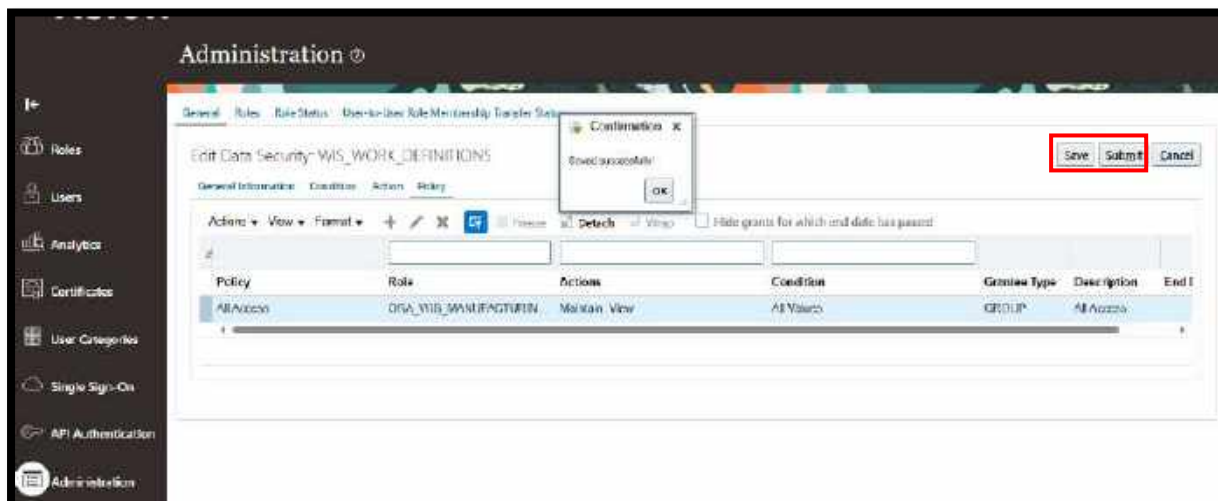
Lastly, one must specify the actions. The two seeded actions are Maintain and View, and user cannot create custom actions.

In the below screenshot, both Maintain and View actions have been chosen.

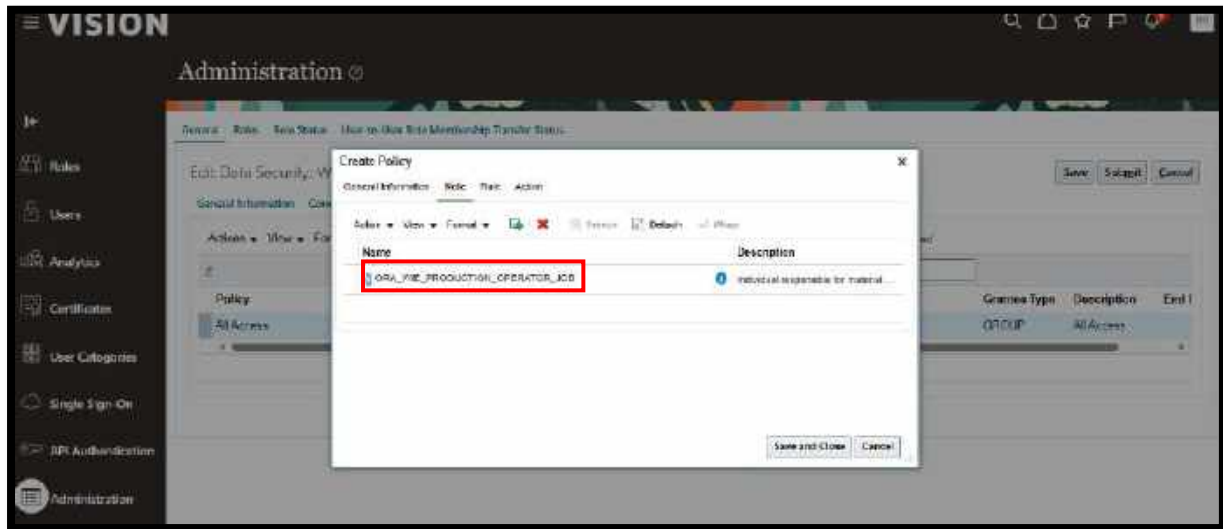




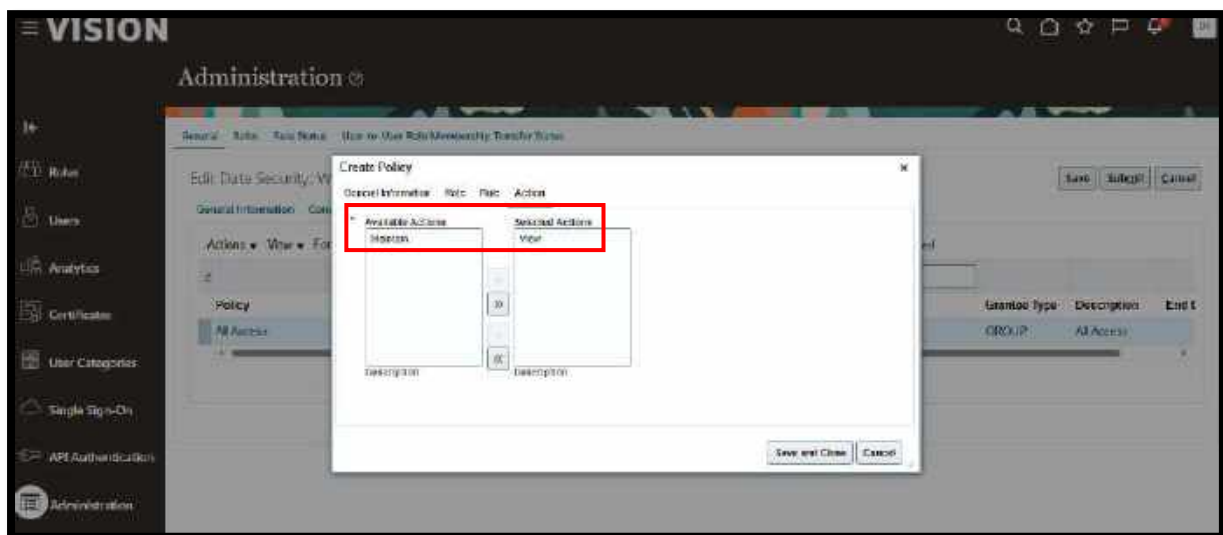
Next, click on Save and Submit. A confirmation message will be displayed as highlighted below.



For this use case, another policy has been set up for demonstration of View Access. Production Operator role has been used for View Access demonstration.



In the Action tab only View has been selected under Selected Actions.



There are two policies created as shown below – one for all access (Maintain and View) and another for view access.

Manage Database Resources and Policies Done

# Search Advanced | Sound Search | Search Database Resource

Object Name:    
 Display Name:    
 New Module Name:

Search | Reset | Save

Search Results

Actions: View | Format |        Hide grants for which and date for parent

Object Name	Display Name	New Module Name	Description
WIS_WORK_DEFINITIONS	Work Definition	Common Work Setup	The work definition template to make the final end assembly product of the maintenance i...

WIS\_WORK\_DEFINITIONS: Policies Details

Actions: View | Format |        Hide grants for which and date for parent

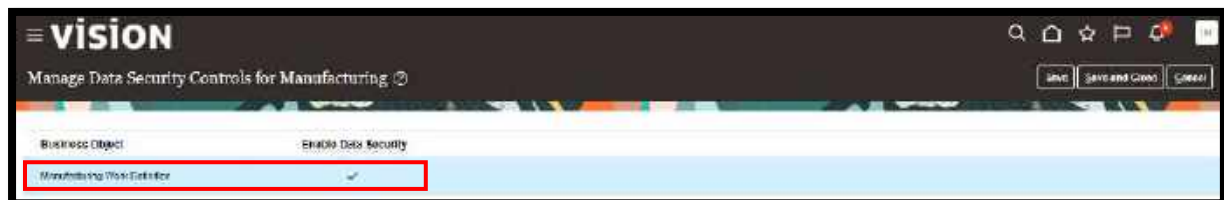
Policy	Role	Condition	Action	Grantee Type	Description	End Of
All Access	ORA_WF_PRODUCTION_SUPER	By Work Definition Name	Maintain View	GROUP	All Access	
View Access	ORA_WF_PRODUCTION_OFFER	By Work Definition Name	View	GROUP	View Access	

## Manage Data Security Controls for Manufacturing

To enable data security for manufacturing work definition business object, user has to go to the Manage Data Security Controls for Manufacturing task in the Setup and Maintenance Work Area. The Enable Data Security check box is defaulted to unchecked in the current update. Select the check box and save the setting. Now data security for manufacturing work definitions has been enabled.

### Navigation

Setup and Maintenance > Manage Data Security Controls for Manufacturing



## Scenario-1: User with View Access tried to create work definition

The below screenshot shows that the user has got Production Operator job role. As per the previous setups the policy against the Production Operator job role is for view access only.



**vision** User Account Details: DIPTIKANTA SATPATHY

Account Information: Password Expiration Date: 2/16/24

User Information:
 

- User Category: DEFAULT
- User Name: DIPTIKANTA.SATPATHY
- First Name: DIPTIKANTA
- Last Name: SATPATHY
- Email: DIPTIKANTA.SATPATHY@TRINAMIX.COM

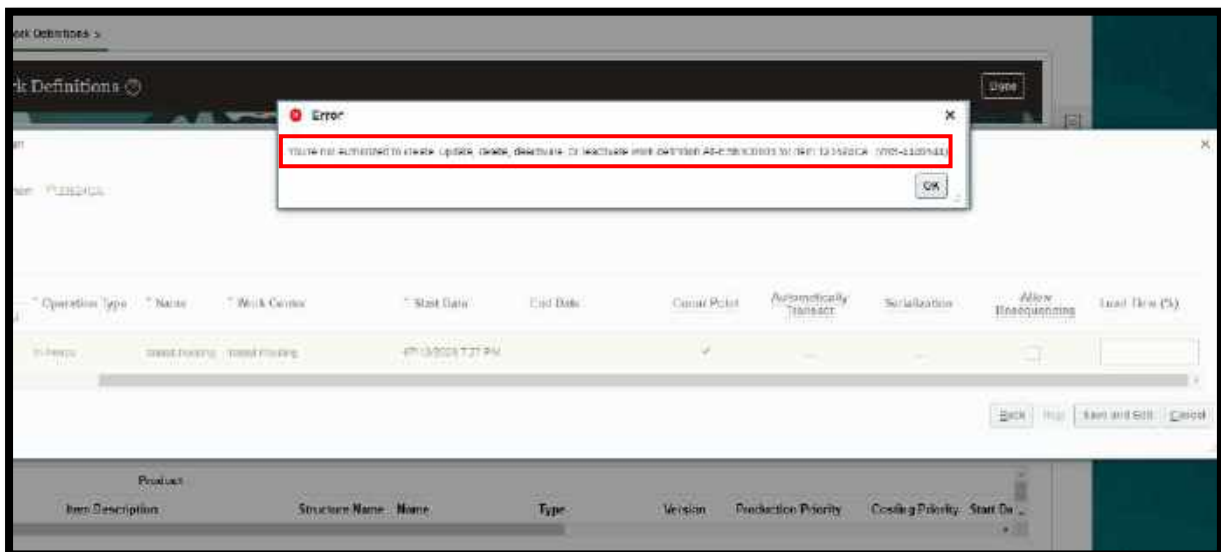
Advanced Information:
 

- Enable Administrative Access for Sign-In Sign-Out Audit REST API

Roles:

Role	Role Code	Assignable	Auto-Provisioned
Application Administrator	FND_APPLICATION_ADMINISTRATOR_JOB	No	No
Application Administrator	ORA_FND_APPLICATION_ADMINISTRATOR_JOB	No	No
Manufacturing Engineer	ORA_WIE_MANUFACTURING_ENGINEER_JOB	Yes	No
Production Operator	ORA_WIE_PRODUCTION_OPERATOR_JOB	Yes	No

Next, go to Supply Chain Execution and Work Definition to create a work definition. As the user does not have access as per the setups, the following error pops up. However, the user can view the existing work definitions.



**Work Definitions**

Error: You are not authorized to create work definition. Contact your administrator for more information.

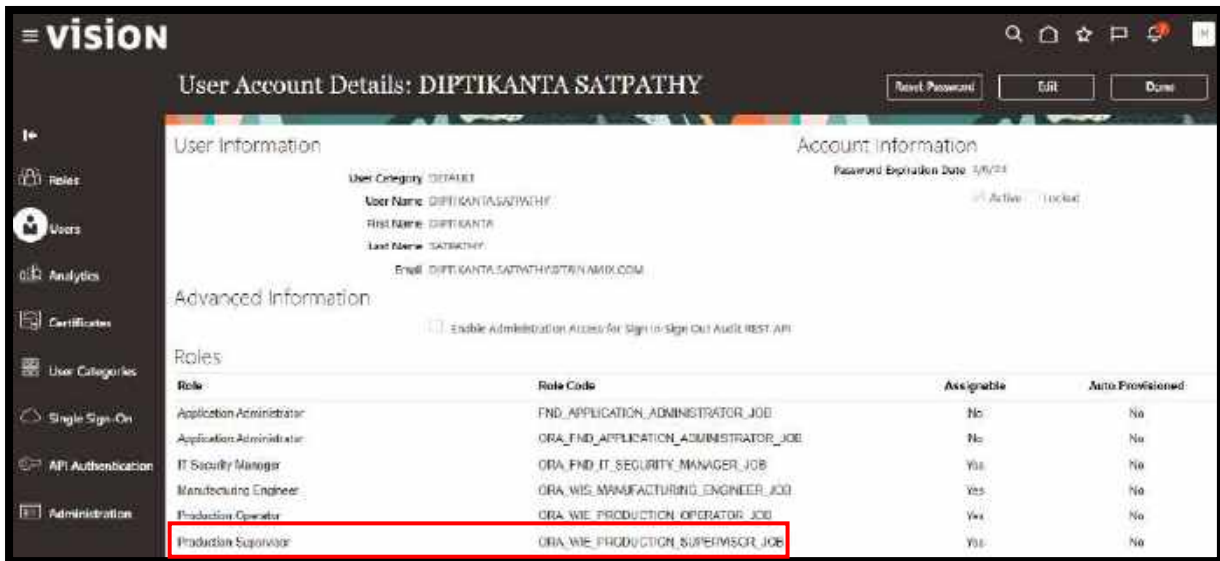
Operation Type	Name	Work Center	Start Date	End Date	Control Point	Automatically Transfer	Serialisation	Allow Requeueing	Lead Time (h)
Inventory	TRANSFER	TRANSFER	4/13/2024 7:27 PM						

Product:
 

Item Description	Structure Name	Name	Type	Version	Production Priority	Costing Priority	Start Da
------------------	----------------	------	------	---------	---------------------	------------------	----------

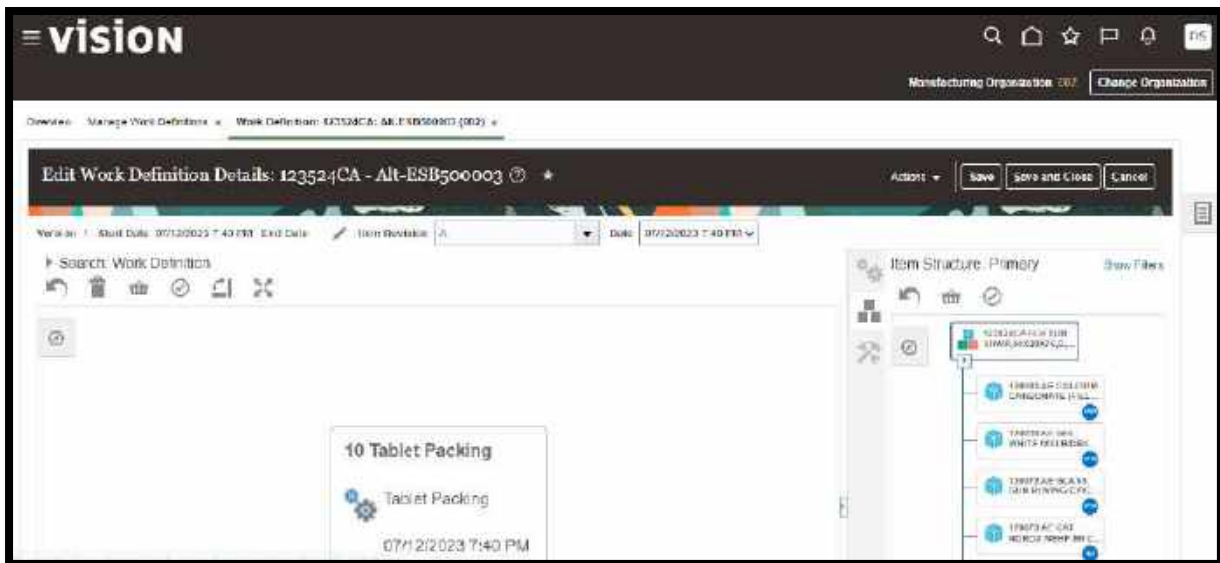
## Scenario-2: User with Maintain Access tried to create work definition

The below screenshot shows that the user has got Production Supervisor job role. As per the previous setups the policy against the Production Operator job role is for view access only.



Role	Role Code	Assignable	Auto-Provisioned
Application Administrator	FND_APPLICATION_ADMINISTRATOR_JOB	No	No
Application Administrator	ORA_FND_APPLICATION_ADMINISTRATOR_JOB	No	No
IT Security Manager	ORA_FND_IT_SECURITY_MANAGER_JOB	Yes	No
Manufacturing Engineer	ORA.WIS.MANUFACTURING_ENGINEER_JOB	Yes	No
Production Operator	ORA.WIE.PRODUCTION.OPERATOR_JOB	Yes	No
<b>Production Supervisor</b>	<b>ORA.WIE.PRODUCTION.SUPERVISOR_JOB</b>	Yes	No

Next, go to Supply Chain Execution and Work Definition to create a work definition. With the above setups, the user was able to create a work definition.



## Conclusion

This functionality will be of great use for providing access to a set of users that need to maintain work definitions of one product group/class, but they should only be able to view work definitions of another product group/class.

## References

<https://docs.oracle.com/en/cloud/saas/supply-chain-and-manufacturing/23d/faumf/how-you-enable-data-security-for-work-definitions.html#u30244232>

## About the author

Diptikanta is an experienced ERP professional in the area of Manufacturing and Supply Chain. He has more than 17 years of experience in Steel Manufacturing, Supply Chain and ERP consulting domain. He holds a Master's degree in Business Administration in Finance and Marketing and a Bachelor's degree in Metallurgical engineering. He is a PMP certified professional and a Black Belt in Six Sigma.

