

# Security Rules (ABAC) In Pega

An Article By Amardeep



What we are trying to Achieve?

In this article we will see how to leverage security rules in Pega .If other than User Operator is accessing the case or creating the case We will try to mask the phone number for security reasons.But if user is accesing the case every details should populate along with Phone no.

Prerequisite:

There should be one section created , data type with records(We can use external database also but I am using Data type for time being, basic obj open method in activity).Operator ID with user access. If we have these things created we will straight move into our security design.

Step1. Create Access Control Policy and choose action as Property Read.

**Create Access Control Policy** Cancel Create and open

**Access Control Policy Record Configuration**

Label \*

MaskPhoneNumber

A short description or title for this record

Identifier

MaskPhoneNumber [Edit](#)

Action

PropertyRead

**Context**

☒ Mahindra Vehicle Insurance  
☐ Mahindra Auto Insurance  
☐ Cosmos Rules  
☐ Pega Platform

Apply to \*  
 Mahi-MahindraV-Work-LoanCase  
[View all](#)

Add to ruleset \*  
 MahindraV 01-01-01

**Current work item**

Work item to associate

Select...

## Step 2. After this create **Access Control Policy Condition**

**Edit Access Control Policy: MaskPhoneNumber [Available]** Actions Save ×

CL: Mahi-MahindraV-Work-LoanCase ID: PropRead - MaskPhoneNumber RS: MahindraV:01-01-01

Definition Specifications History

**TARGET**  
Mahi-MahindraV-Work-LoanCase

**ACTION**  
PropertyRead

**APPLIES TO**  
Listed properties only

☐ Disallow creation of a policy with the same name at a descendant class

Permit access if  is true.

**Property** **Restriction Method**

No items

[+ Add property](#)

## Step 3. Create Access when and call into **Access Control Policy Condition**

**Edit Access Control Policy Condition: CheckUserIsOperator [Available]** Actions Save ×

CL: Mahi-MahindraV-Work-LoanCase ID: CheckUserIsOperator RS: MahindraV:01-01-01

Definition Pages & Classes Data Access Specifications History

**Conditional Logic**

**WHEN**

Permit access if A

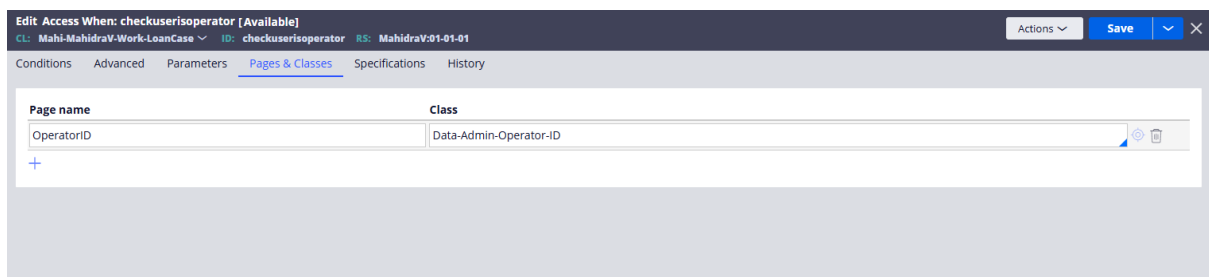
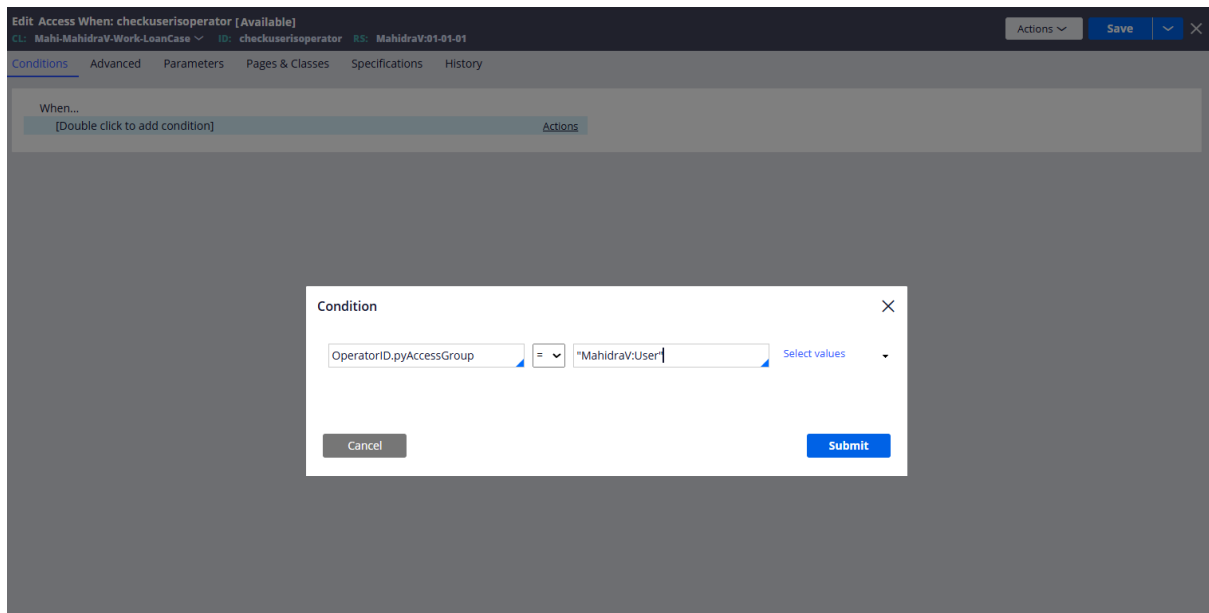
**OTHERWISE**

Permit access if B

[+ Add conditional logic](#)

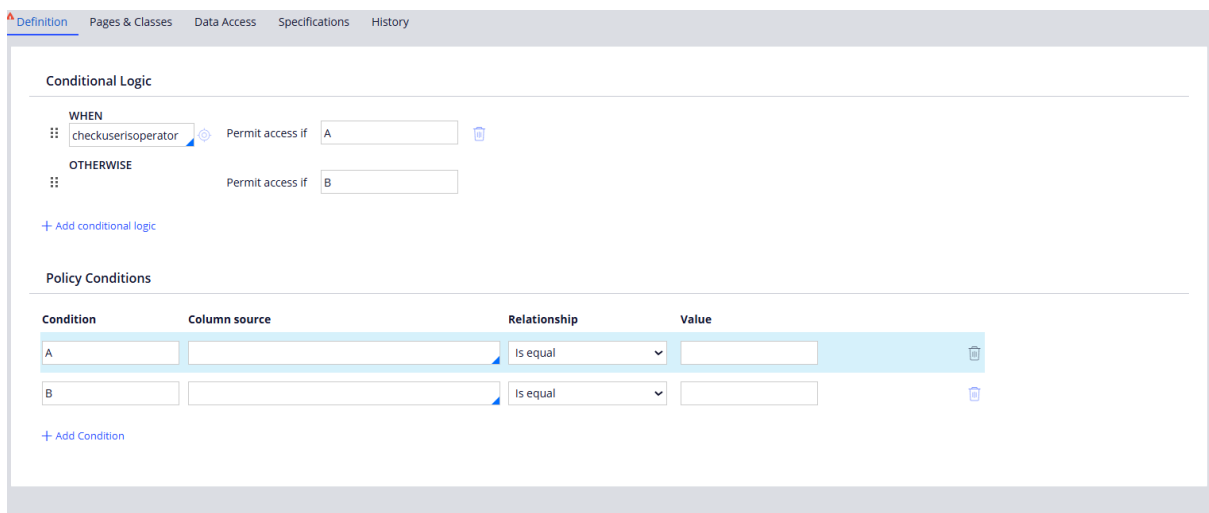
**Policy Conditions**

## Step IV. Access when configuration :



We here when rule is checking the operator who is logging into case has the User access specifically is this or not. And accordingly it will function.

Step 4. Go back to **Access Control Policy Condition** and add the Necessary logic.



Here it will check two condition A should always be satisfied and based on that only it will check the user access group or not. We cannot removed otherwise wise condition so for time being I am making condition B be always false so action will depend on Only A logic part i.e it will check the Access group.

**Edit Access Control Policy Condition: CheckUserIsOperator [Available]**  
 CL: Mahi-MahidraV-Work-LoanCase ID: CheckUserIsOperator RS: MahidraV:01-01-01

Definition Pages & Classes Data Access Specifications History

**Conditional Logic**

WHEN  
 :: checkuserisoperator Permit access if A

OTHERWISE  
 :: Permit access if B

+ Add conditional logic

**Policy Conditions**

Condition	Column source	Relationship	Value
A	.pxCreateDateTime	Is not null	<input checked="" type="checkbox"/> Treat Empty As Null
B	.pxCreateDateTime	Is null	<input checked="" type="checkbox"/> Treat Empty As Null

+ Add Condition

Step V. Come back to **Access Control Policy**. And add the page property that hold the Phone number select that and do as is configuration.

Definition Specifications History

**TARGET**  
 Mahi-MahidraV-Work-LoanCase

**ACTION**  
 PropertyRead

**APPLIES TO**  
 Listed properties only

☐ Disallow creation of a policy with the same name at a descendant class

Permit access if CheckUserIsOperator is true

**Property** **Restriction Method**

.CustomerSearchPage.Ph	Mask all but last 'N'
------------------------	-----------------------

+ Add property

**Masking and Formatting Options**

Restricting Property: .CustomerSearchPage.PhoneNumber

Restriction Method: Mask all but last 'N'

Masking character: \*

Number of unmasked characters: 4

☒ Display length is fixed ☐ Display length matches value

Display characters length: 10

Cancel Submit

**Edit Access Control Policy: MaskPhoneNumber [Available]**  
 CL: Mahi-MahidraV-Work-LoanCase ID: PropRead • MaskPhoneNumber RS: MahidraV:01-01-01

Definition Specifications History

**TARGET**  
 Mahi-MahidraV-Work-LoanCase

**ACTION**  
 PropertyRead

**APPLIES TO**  
 Listed properties only

☐ Disallow creation of a policy with the same name at a descendant class

Permit access if CheckUserIsOperator is true.

**Property** **Restriction Method**

.CustomerSearchPage.Ph	Mask all but last 'N'
------------------------	-----------------------

+ Add property

Done Lets test it.

Testing Part :

Another Operator(which is not User Operator) is Initiating the case :

New LoanCase

Enter Customer Details

Customer ID

100

SearchReset

Search Result

Customer ID

100

Email

amardeepsri@email.com

Gender

Male

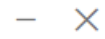
Phone number

\*\*\*\*\*8888

CancelSubmit

Now Login with user Operator :

## New LoanCase



### Enter Customer Details

Customer ID

Search

Reset

### Search Result

Customer ID

100

Email

amardeepsri@email.com

Gender

Male

Phone number

8888888888

Cancel

Submit

Done.