Tech Note 999
Wonderware Application Server Security Troubleshooting Essentials Part 2: Security Classification & Operational Permissions

All Tech Notes, Tech Alerts and KBCD documents and software are provided "as is" without warranty of any kind. See the **Terms of Use** for more information.

Topic#: 002829
Created: December 2013

Introduction

This Essentials Guide is the 2nd in a projected series.

This *Tech Note* discusses the relationship between the Security Groups and Attribute Security Classification. In addition, we introduce a utility which unifies the security group information covered in this *Tech Note* into a single page and provides Galaxy search functionality as well.

Application Versions

- Wonderware Application Server 2012 and later

Application Server Security Model Review

The attributes on an ArchestrA Automation Object (AA Object) have a configurable security classification setting. This provides the ability to define who can control the attributes of an AA Object.

In a real world Galaxy, there are typically a large amount of AA Objects. **Roles** and **Security Groups** functionality provides the ability to efficiently assign/modify users and their associated security classification on the attributes of AA Objects.

- **Roles**: Generalize users' functional groups, such as Operator, System Engineer, Application Engineer, etc. One Role can be granted permissions to multiple Security Groups.
- **Security Group**: Groups AA Objects together with those that have same set of Operational Permissions.

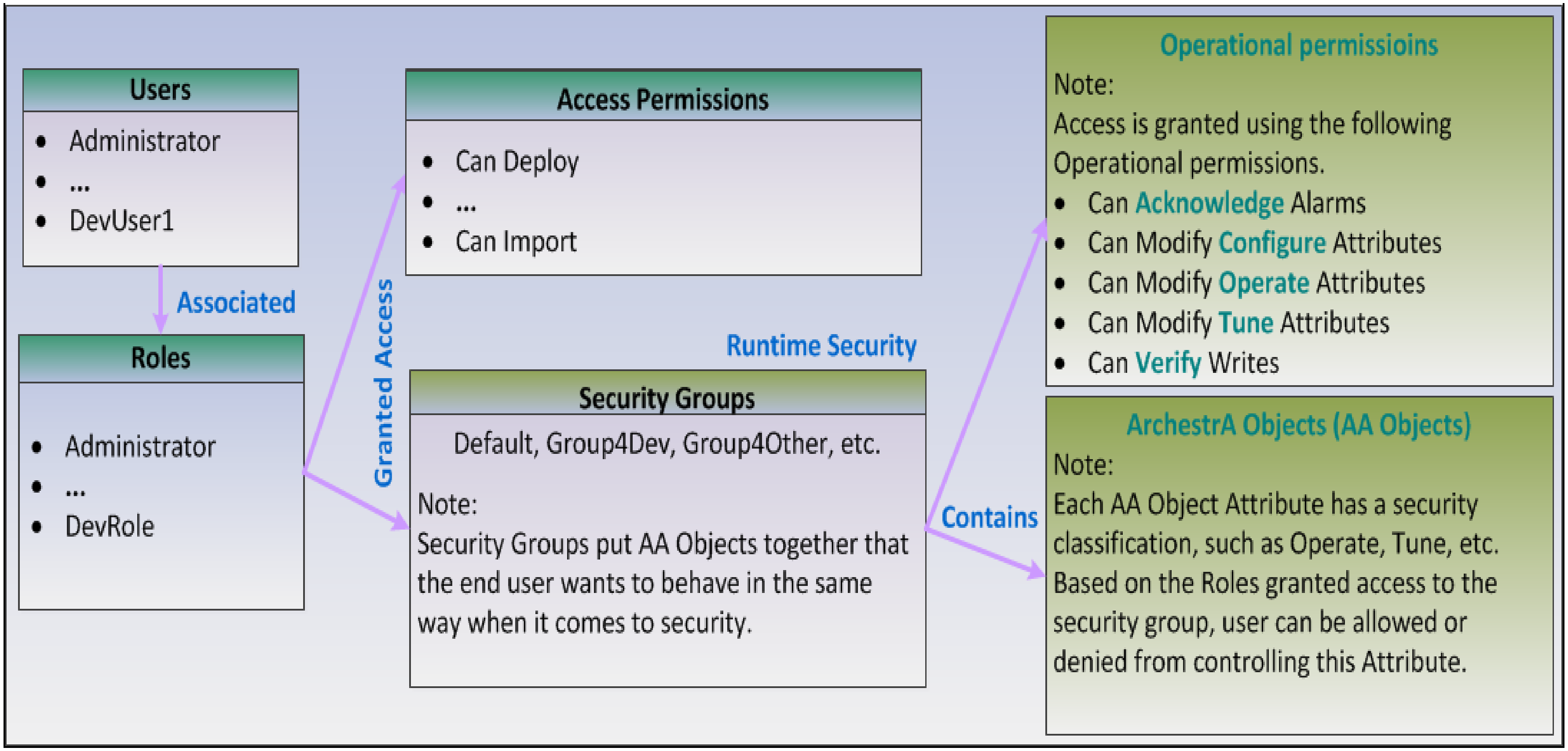

Users
Administrator
...
DevUser1
Associated
Roles
Administrator
...
DevRole
Granted Access
Access Permissions
Can Deploy
...
Can Import
Runtime Security
Security Groups
Default, Group4Dev, Group4Other, etc.
Note:
Security Groups put AA Objects together that the end user wants to behave in the same way when it comes to security.
Contains
Operational permissioins
Note:
Access is granted using the following Operational permissions.
Can Acknowledge Alarms
Can Modify Configure Attributes
Can Modify Operate Attributes
Can Modify Tune Attributes
Can Verify Writes
ArchestrA Objects (AA Objects)
Note:
Each AA Object Attribute has a security classification, such as Operate, Tune, etc. Based on the Roles granted access to the security group, user can be allowed or denied from controlling this Attribute.

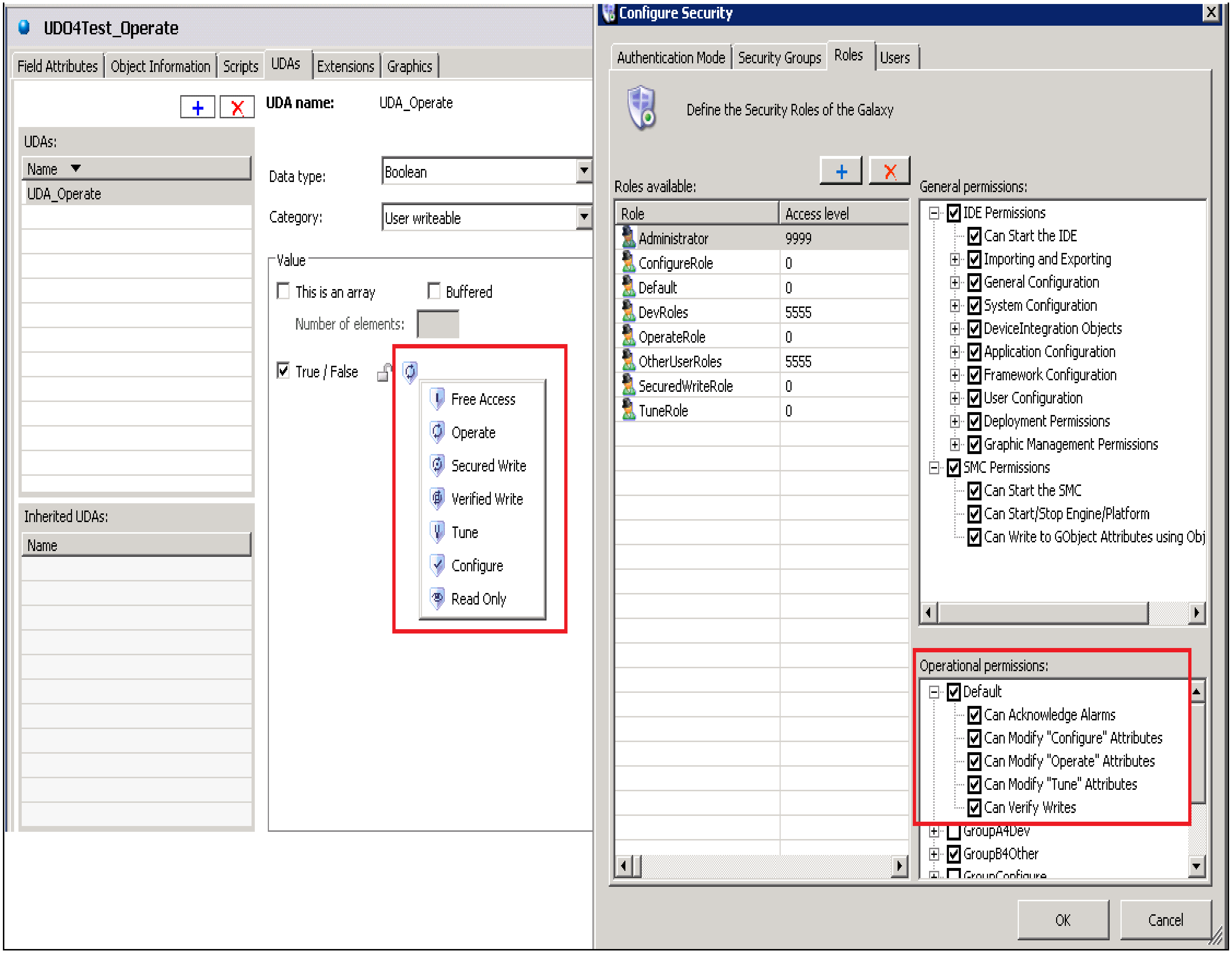
Figure 1: Application Server Security Model

The following table shows the AA Object Attributes' **Security classification** specifications and their corresponding Security Groups' **Operational permissions**.

Security Classification	**Perspective**	**Operational Permission**
FreeAccess	No privileges are required. Any user can write to an attribute that has this setting	
Operate	Allows user to change the value of an attribute during On-Scan or Off-Scan mode Note: Deployment needs the Operate Operational Permission	Operate
Secured Write	Requires the logon user to retype password in order to make the changed value go through.	Operate
Verified Write	Besides the above Secured Write, you must provide the second user's authentication. **Note**: Two users must have **Operate** and **Verify** Operational permissions.	Operate, Verify

Tune	Allows user to write a value to the attribute at the On-Scan or Off-Scan mode.	Tune
Configure	Allows user to write a value to the attribute only at the Off-Scan mode.	Configure
Read Only	Regardless of user's permission, the attribute value cannot be changed at Runtime.	

The following graphic shows **Security classifications** in the center red frame, and the **Operational permissions** at the right.



UD04Test_Operate

Field Attributes | Object Information | Scripts | UDAs | Extensions | Graphics

UDA name: UDA_Operate

UDAs:

Name
UDA_Operate

Data type: Boolean

Category: User writeable

Value

☐ This is an array ☐ Buffered

Number of elements:

☑ True / False

Free Access
Operate
Secured Write
Verified Write
Tune
Configure
Read Only

Inherited UDAs:

Name

Configure Security

Authentication Mode | Security Groups | Roles | Users

Define the Security Roles of the Galaxy

Roles available:

Role	Access level
Administrator	9999
ConfigureRole	0
Default	0
DevRoles	5555
OperateRole	0
OtherUserRoles	5555
SecuredWriteRole	0
TuneRole	0

General permissions:

- ☑ IDE Permissions
  - ☑ Can Start the IDE
  - ☑ Importing and Exporting
  - ☑ General Configuration
  - ☑ System Configuration
  - ☑ DeviceIntegration Objects
  - ☑ Application Configuration
  - ☑ Framework Configuration
  - ☑ User Configuration
  - ☑ Deployment Permissions
  - ☑ Graphic Management Permissions
- ☑ SMC Permissions
  - ☑ Can Start the SMC
  - ☑ Can Start/Stop Engine/Platform
  - ☑ Can Write to GObject Attributes using Obj

Operational permissions:

- ☑ Default
  - ☑ Can Acknowledge Alarms
  - ☑ Can Modify "Configure" Attributes
  - ☑ Can Modify "Operate" Attributes
  - ☑ Can Modify "Tune" Attributes
  - ☑ Can Verify Writes
- ☐ GroupA4Dev
- ☑ GroupB4Other
- ☐ GroupConfigure

Figure 2: Security Classification and Operational Permissions

The following section demonstrates usage of **Operate**, **Secured Write** and **Configure** specifications in detail.

Operate

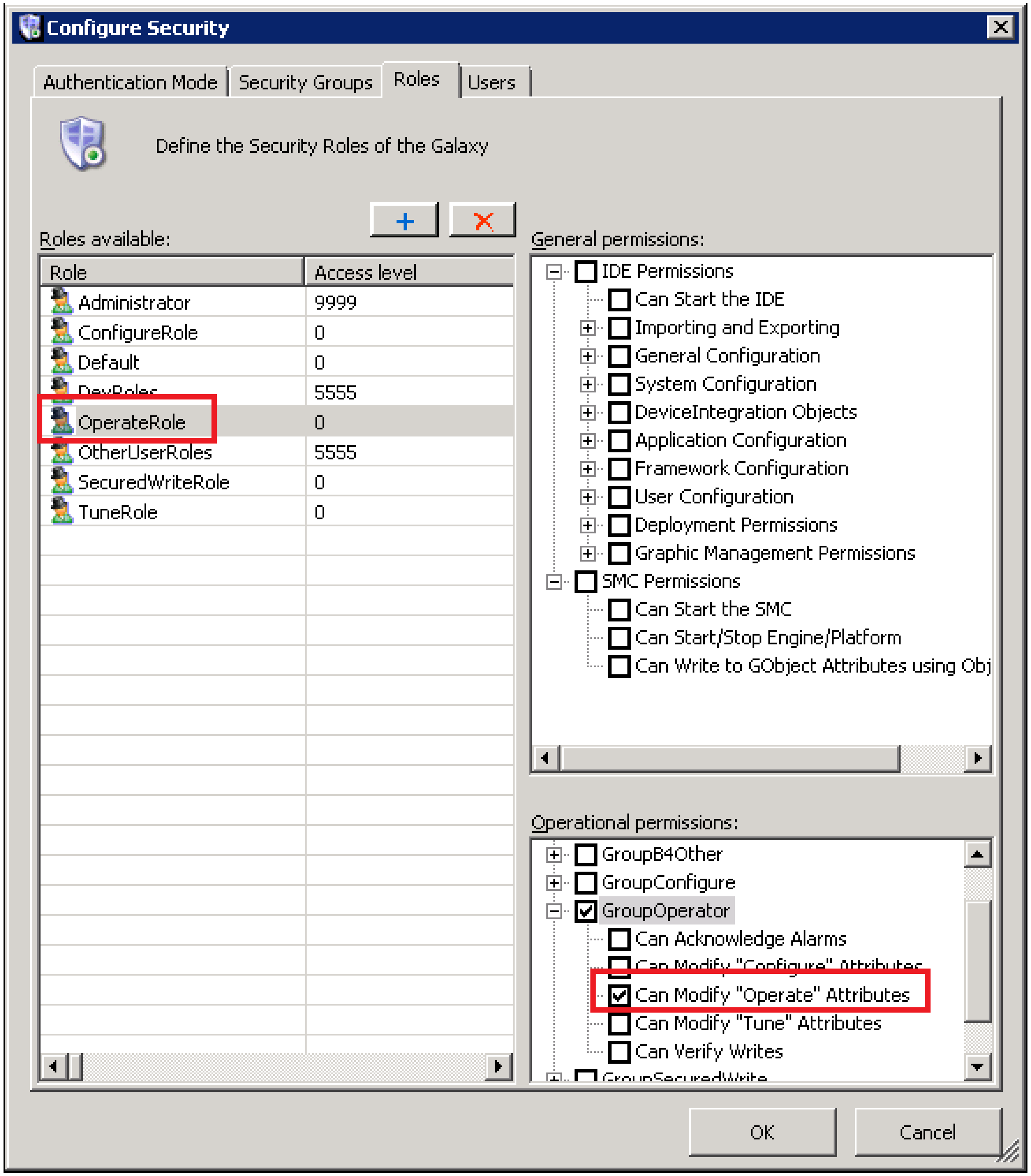
Allows user to change the value of an attribute during On-Scan or Off-Scan mode.

Environment

UDA	UDA_Operate and with Operate type of Security Classification.
UDO	UDO4Test_Operate (AA Object) contains UDA_Operate.
Security Group	GroupOperator contains UDO4Test_Operate (AA Object).
Role	OperateRole
User	OperA

Setup

1. Only OperateRole is granted the access to GroupOperator.
2. Only **OperA** is associated to OperateRole.
3. In GroupOperator, uncheck all options except **Can Modify "Operate" Attribute**.



Define the Security Roles of the Galaxy

Roles available:

Role	Access level
Administrator	9999
ConfigureRole	0
Default	0
DevRoles	5555
OperateRole	0
OtherUserRoles	5555
SecuredWriteRole	0
TuneRole	0

General permissions:

- ☐ IDE Permissions
  - ☐ Can Start the IDE
  - ☐ Importing and Exporting
  - ☐ General Configuration
  - ☐ System Configuration
  - ☐ DeviceIntegration Objects
  - ☐ Application Configuration
  - ☐ Framework Configuration
  - ☐ User Configuration
  - ☐ Deployment Permissions
  - ☐ Graphic Management Permissions
- ☐ SMC Permissions
  - ☐ Can Start the SMC
  - ☐ Can Start/Stop Engine/Platform
  - ☐ Can Write to GObject Attributes using Obj

Operational permissions:

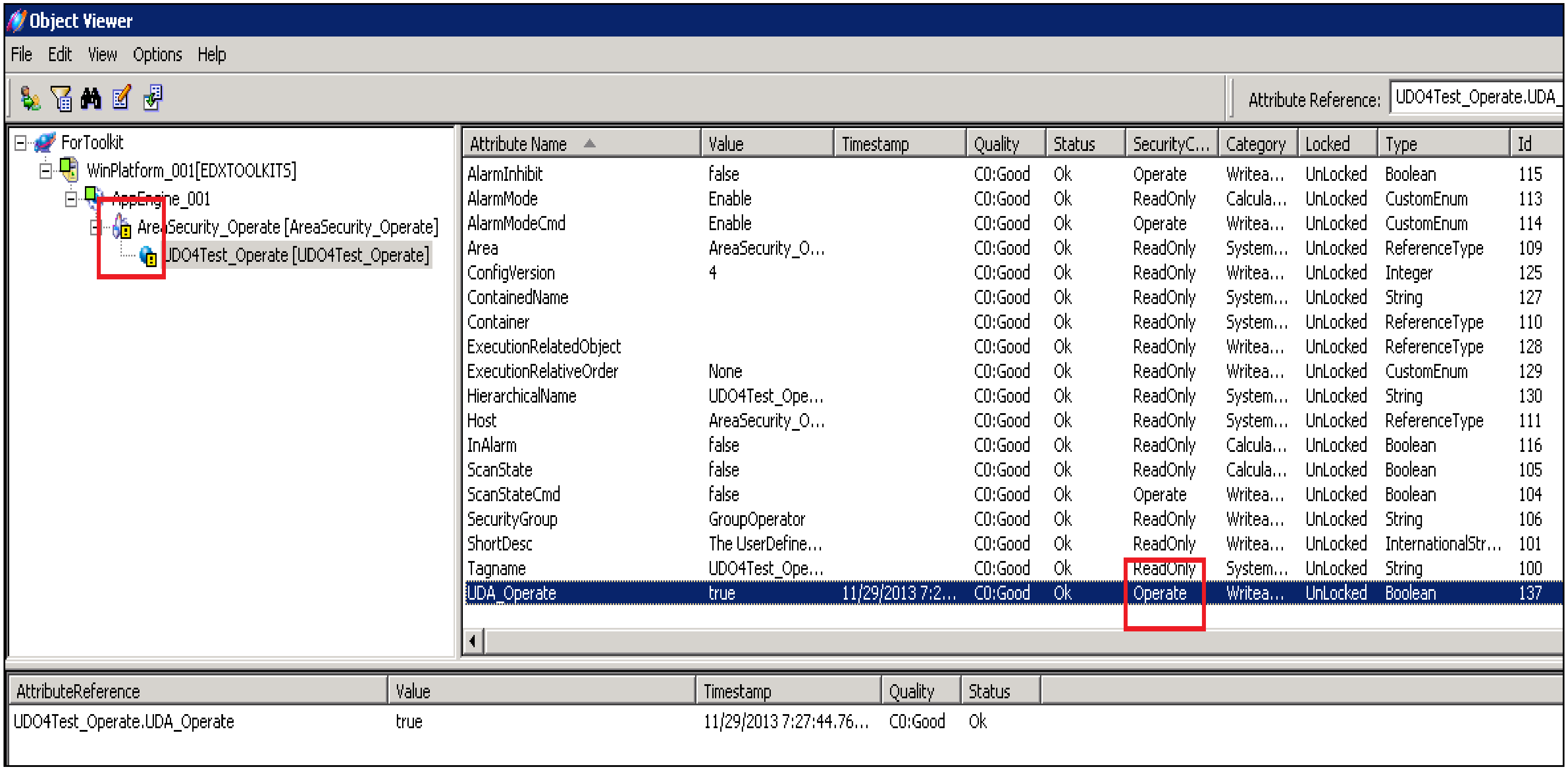
- ☐ GroupB4Other
- ☐ GroupConfigure
- ☑ GroupOperator
  - ☐ Can Acknowledge Alarms
  - ☐ Can Modify "Configure" Attributes
  - ☑ Can Modify "Operate" Attributes
  - ☐ Can Modify "Tune" Attributes
  - ☐ Can Verify Writes
- ☐ GroupSecuredWrite

Figure 3: Select Can Modify "Operate" Attributes Option

Verify

1. Deploy **UDO4Test_Operate** with Off-Scan and open it with the Object Viewer. The object icon in this example indicates the

deployment is in **Off-Scan** state (Figure 4 below).

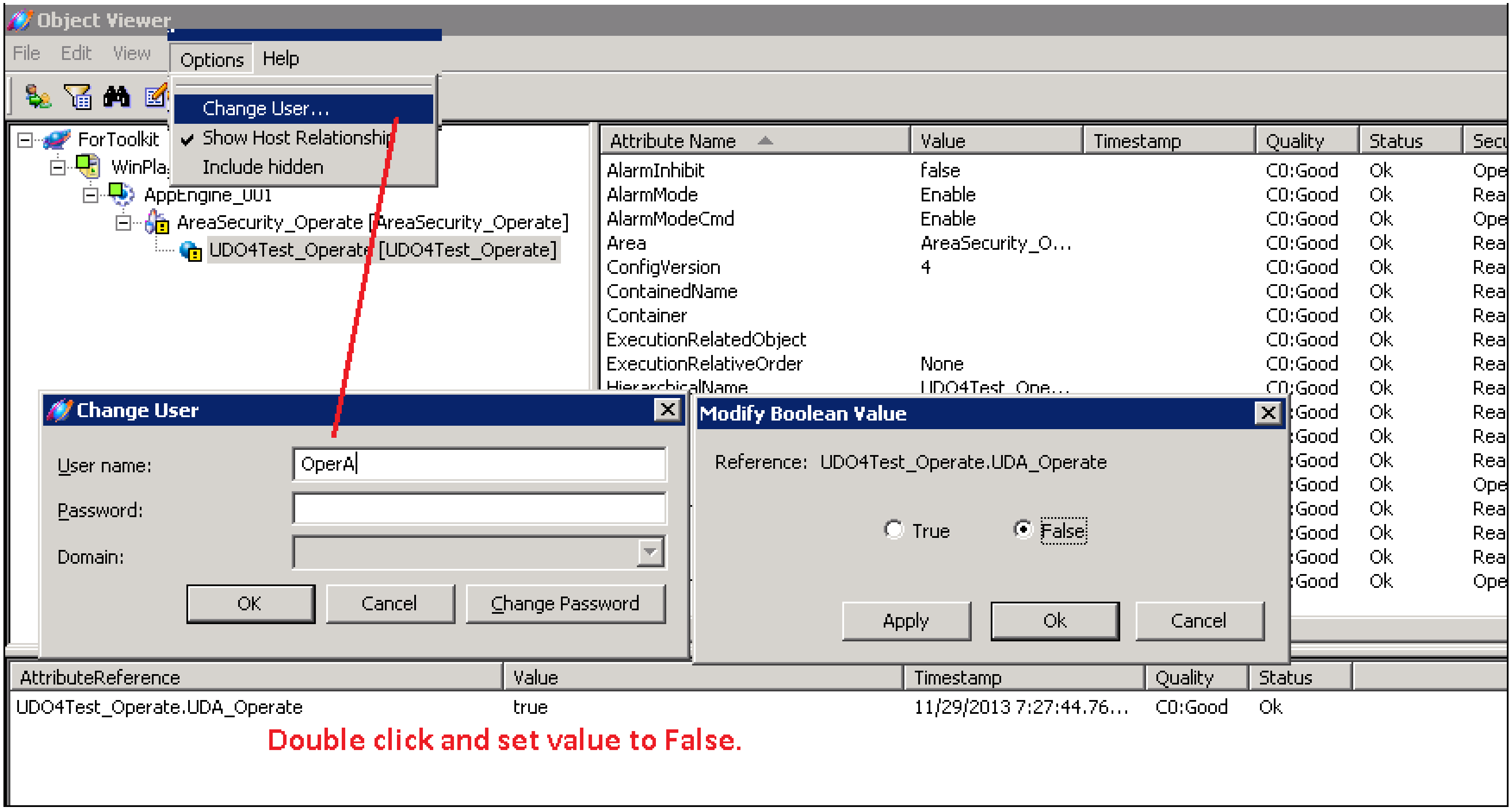

Object Viewer
File Edit View Options Help
Attribute Reference: UDO4Test_Operate.UDA_
ForToolkit
WinPlatform_001[EDXTOOLKITS]
AppEngine_001
AreaSecurity_Operate [AreaSecurity_Operate]
UDO4Test_Operate [UDO4Test_Operate]

Attribute Name	Value	Timestamp	Quality	Status	SecurityC...	Category	Locked	Type	Id
AlarmInhibit	false		C0:Good	Ok	Operate	Writea...	UnLocked	Boolean	115
AlarmMode	Enable		C0:Good	Ok	ReadOnly	Calcula...	UnLocked	CustomEnum	113
AlarmModeCmd	Enable		C0:Good	Ok	Operate	Writea...	UnLocked	CustomEnum	114
Area	AreaSecurity_O...		C0:Good	Ok	ReadOnly	System...	UnLocked	ReferenceType	109
ConfigVersion	4		C0:Good	Ok	ReadOnly	Writea...	UnLocked	Integer	125
ContainedName			C0:Good	Ok	ReadOnly	System...	UnLocked	String	127
Container			C0:Good	Ok	ReadOnly	System...	UnLocked	ReferenceType	110
ExecutionRelatedObject			C0:Good	Ok	ReadOnly	Writea...	UnLocked	ReferenceType	128
ExecutionRelativeOrder	None		C0:Good	Ok	ReadOnly	Writea...	UnLocked	CustomEnum	129
HierarchicalName	UDO4Test_Ope...		C0:Good	Ok	ReadOnly	System...	UnLocked	String	130
Host	AreaSecurity_O...		C0:Good	Ok	ReadOnly	System...	UnLocked	ReferenceType	111
InAlarm	false		C0:Good	Ok	ReadOnly	Calcula...	UnLocked	Boolean	116
ScanState	false		C0:Good	Ok	ReadOnly	Calcula...	UnLocked	Boolean	105
ScanStateCmd	false		C0:Good	Ok	Operate	Writea...	UnLocked	Boolean	104
SecurityGroup	GroupOperator		C0:Good	Ok	ReadOnly	Writea...	UnLocked	String	106
ShortDesc	The UserDefine...		C0:Good	Ok	ReadOnly	Writea...	UnLocked	InternationalStr...	101
Tagname	UDO4Test_Ope...		C0:Good	Ok	ReadOnly	System...	UnLocked	String	100
UDA_Operate	true	11/29/2013 7:2...	C0:Good	Ok	Operate	Writea...	UnLocked	Boolean	137

AttributeReference	Value	Timestamp	Quality	Status
UDO4Test_Operate.UDA_Operate	true	11/29/2013 7:27:44.76...	C0:Good	Ok

Figure 4: Object Viewer Shows Each Attribute's Security Classification

2. Change the User to **OperA** and set the value on **UDA_Operate** to **False** (Figure 5 below).



Attribute Name	Value	Timestamp	Quality	Status	Secu
AlarmInhibit	false		C0:Good	Ok	Ope
AlarmMode	Enable		C0:Good	Ok	Rea
AlarmModeCmd	Enable		C0:Good	Ok	Ope
Area	AreaSecurity_O...		C0:Good	Ok	Rea
ConfigVersion	4		C0:Good	Ok	Rea
ContainedName			C0:Good	Ok	Rea
Container			C0:Good	Ok	Rea
ExecutionRelatedObject			C0:Good	Ok	Rea
ExecutionRelativeOrder	None		C0:Good	Ok	Rea
HierarchicalName	UDO4Test_Ope...		C0:Good	Ok	Rea
			:Good	Ok	Rea
			:Good	Ok	Rea
			:Good	Ok	Rea
			:Good	Ok	Rea
			:Good	Ok	Ope
			:Good	Ok	Rea
			:Good	Ok	Rea
			:Good	Ok	Rea
			:Good	Ok	Ope

User name: OperA

Password:

Domain:

Reference: UDO4Test_Operate.UDA_Operate

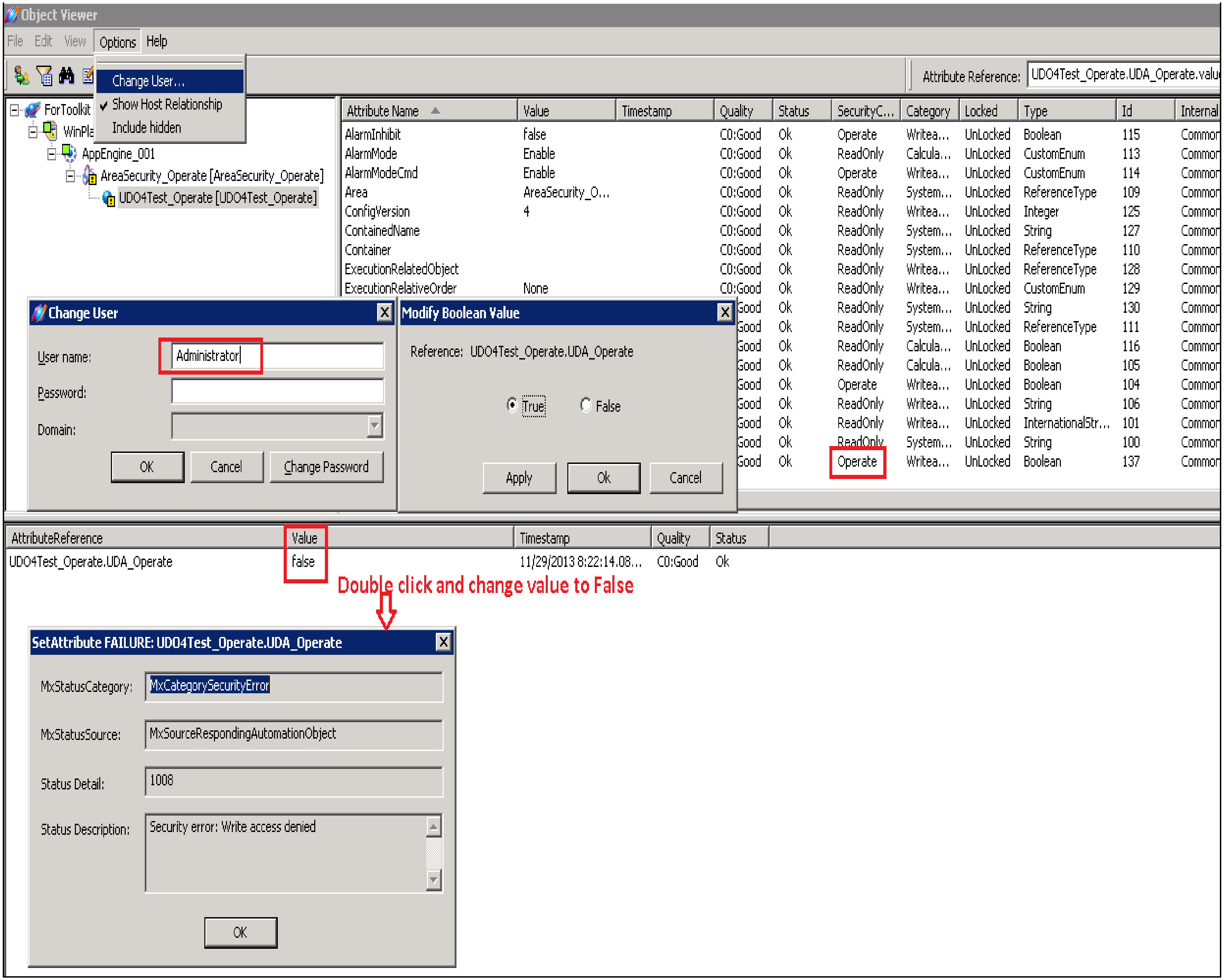
○ True ● False

AttributeReference	Value	Timestamp	Quality	Status
UDO4Test_Operate.UDA_Operate	true	11/29/2013 7:27:44.76...	C0:Good	Ok

Double click and set value to False.

Figure 5: User OperA can Set the Value

3. Change the User to **Administrator**.



Attribute Reference: UDO4Test_Operate.UDA_Operate.valu

Attribute Name	Value	Timestamp	Quality	Status	SecurityC...	Category	Locked	Type	Id	Internal
AlarmInhibit	false		C0:Good	Ok	Operate	Writea...	UnLocked	Boolean	115	Commor
AlarmMode	Enable		C0:Good	Ok	ReadOnly	Calcula...	UnLocked	CustomEnum	113	Commor
AlarmModeCmd	Enable		C0:Good	Ok	Operate	Writea...	UnLocked	CustomEnum	114	Commor
Area	AreaSecurity_O...		C0:Good	Ok	ReadOnly	System...	UnLocked	ReferenceType	109	Commor
ConfigVersion	4		C0:Good	Ok	ReadOnly	Writea...	UnLocked	Integer	125	Commor
ContainedName			C0:Good	Ok	ReadOnly	System...	UnLocked	String	127	Commor
Container			C0:Good	Ok	ReadOnly	System...	UnLocked	ReferenceType	110	Commor
ExecutionRelatedObject			C0:Good	Ok	ReadOnly	Writea...	UnLocked	ReferenceType	128	Commor
ExecutionRelativeOrder	None		C0:Good	Ok	ReadOnly	Writea...	UnLocked	CustomEnum	129	Commor
			Good	Ok	ReadOnly	System...	UnLocked	String	130	Commor
			Good	Ok	ReadOnly	System...	UnLocked	ReferenceType	111	Commor
			Good	Ok	ReadOnly	Calcula...	UnLocked	Boolean	116	Commor
			Good	Ok	ReadOnly	Calcula...	UnLocked	Boolean	105	Commor
			Good	Ok	Operate	Writea...	UnLocked	Boolean	104	Commor
			Good	Ok	ReadOnly	Writea...	UnLocked	String	106	Commor
			Good	Ok	ReadOnly	Writea...	UnLocked	InternationalStr...	101	Commor
			Good	Ok	ReadOnly	System...	UnLocked	String	100	Commor
			Good	Ok	Operate	Writea...	UnLocked	Boolean	137	Commor

User name: Administrator

Password:

Domain:

Reference: UDO4Test_Operate.UDA_Operate

● True ○ False

AttributeReference	Value	Timestamp	Quality	Status
UDO4Test_Operate.UDA_Operate	false	11/29/2013 8:22:14.08...	C0:Good	Ok

MxStatusCategory: MxCategorySecurityError

MxStatusSource: MxSourceRespondingAutomationObject

Status Detail: 1008

Status Description: Security error: Write access denied

Figure 6: Administrator Cannot Set the UDA_Operate Value: Administrator is not in OperateRole

4. (Optional) Repeat this procedure in **On-Scan** Deployment state.

Summary

Operate Security Classification can set attribute value in both On-Scan and Off-Scan deployments if the user is in the correct Role.

Secured Write

Requires the logon user to type the password in order to make the changed value goes through. The Operate Permission is required.

Environment

UDA	UDA_SecuredWrite and with Secured Write type of Security Classification.
UDO	UDO4Test_SecuredWrite (AA Object) contains UDA_SecuredWrite.
Security Group	GroupSecuredWrite contains UDO4Test_SecuredWrite (AA Object).
Role	SecuredWriteRole.
User	OperB_Sec

Setup 1

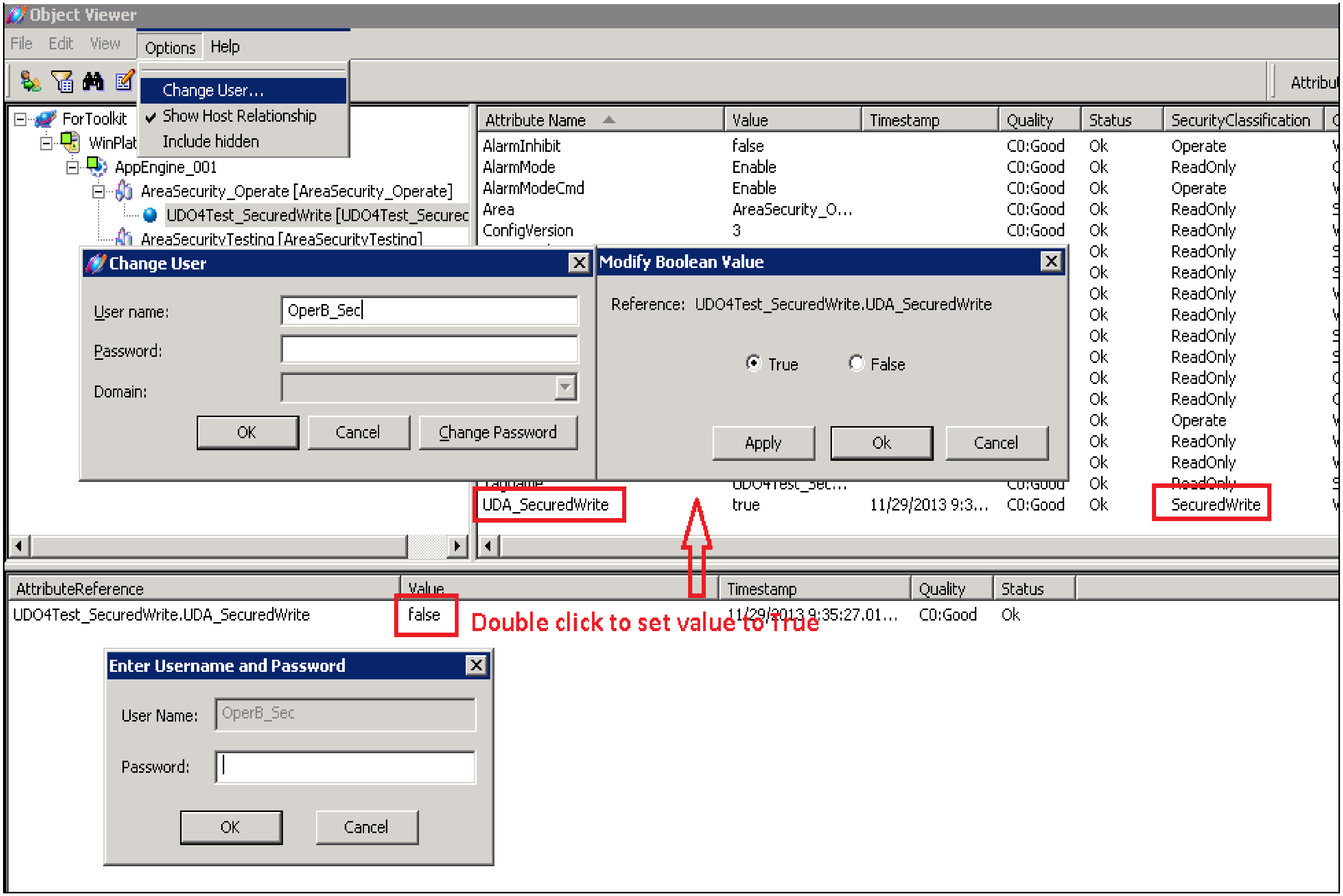
1. Only SecuredWriteRole is granted the access to GroupSecuredWrite.
2. Only OperB_Sec is associated to SecuredWriteRole.

Setup 2

- Same as the Setup 1 but uncheck **Operate** Operational permission from GroupSecuredWrite.

Verify 1

1. Deploy UDA4Test_SecuredWrite (AA Object) and open it with Object Viewer.
2. Change the User to **OperB_Sec** and set the value on UDA_SecuredWrite.


Object Viewer
File Edit View Options Help
Change User...
✓ Show Host Relationship
Include hidden
Attribu
ForToolkit
WinPlat
AppEngine_001
AreaSecurity_Operate [AreaSecurity_Operate]
UDO4Test_SecuredWrite [UDO4Test_Securec
AreaSecurityTesting [AreaSecurityTesting]
Double click to set value to True

Attribute Name	Value	Timestamp	Quality	Status	SecurityClassification
AlarmInhibit	false		C0:Good	Ok	Operate
AlarmMode	Enable		C0:Good	Ok	ReadOnly
AlarmModeCmd	Enable		C0:Good	Ok	Operate
Area	AreaSecurity_O...		C0:Good	Ok	ReadOnly
ConfigVersion	3		C0:Good	Ok	ReadOnly
				Ok	ReadOnly
				Ok	ReadOnly
				Ok	ReadOnly
				Ok	ReadOnly
				Ok	ReadOnly
				Ok	ReadOnly
				Ok	ReadOnly
				Ok	ReadOnly
				Ok	Operate
				Ok	ReadOnly
				Ok	ReadOnly
Tagname	UDO4Test_Sec...		C0:Good	Ok	ReadOnly
UDA_SecuredWrite	true	11/29/2013 9:3...	C0:Good	Ok	SecuredWrite

Change User

User name: OperB_Sec

Password:

Domain:

OK | Cancel | Change Password

Modify Boolean Value

Reference: UDO4Test_SecuredWrite.UDA_SecuredWrite

● True ○ False

Apply | Ok | Cancel

AttributeReference	Value	Timestamp	Quality	Status
UDO4Test_SecuredWrite.UDA_SecuredWrite	false	11/29/2013 9:35:27.01...	C0:Good	Ok

Enter Username and Password

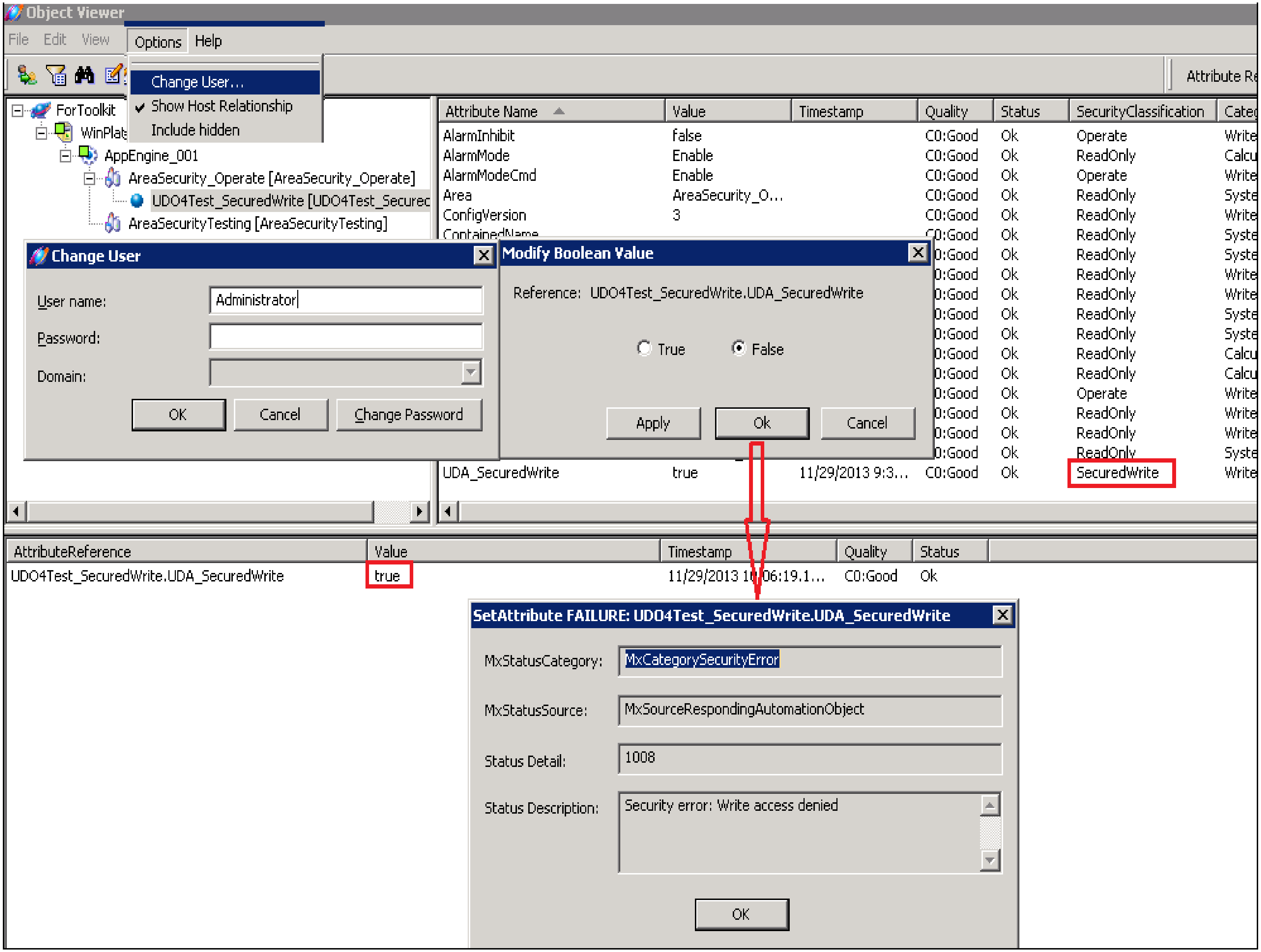
User Name: OperB_Sec

Password:

OK | Cancel

Figure 7: After Clicking the OK Button in the "Enter Username and Password" dialog, the Value of UDA_SecuredWrite Sets to True Successfully

3. Change the User to Administrator and set the value on UDA_SecuredWrite.



Attribute Name	Value	Timestamp	Quality	Status	SecurityClassification	Categ
AlarmInhibit	false		C0:Good	Ok	Operate	Write
AlarmMode	Enable		C0:Good	Ok	ReadOnly	Calcu
AlarmModeCmd	Enable		C0:Good	Ok	Operate	Write
Area	AreaSecurity_O...		C0:Good	Ok	ReadOnly	Syste
ConfigVersion	3		C0:Good	Ok	ReadOnly	Write
ContainedName			C0:Good	Ok	ReadOnly	Syste
			0:Good	Ok	ReadOnly	Syste
			0:Good	Ok	ReadOnly	Write
			0:Good	Ok	ReadOnly	Write
			0:Good	Ok	ReadOnly	Syste
			0:Good	Ok	ReadOnly	Syste
			0:Good	Ok	ReadOnly	Calcu
			0:Good	Ok	ReadOnly	Calcu
			0:Good	Ok	Operate	Write
			0:Good	Ok	ReadOnly	Write
			0:Good	Ok	ReadOnly	Write
			0:Good	Ok	ReadOnly	Syste
UDA_SecuredWrite	true	11/29/2013 9:3...	C0:Good	Ok	SecuredWrite	Write

Change User

User name: Administrator

Password:

Domain:

Modify Boolean Value

Reference: UDO4Test_SecuredWrite.UDA_SecuredWrite

○ True ● False

AttributeReference	Value	Timestamp	Quality	Status
UDO4Test_SecuredWrite.UDA_SecuredWrite	true	11/29/2013 10:06:19.1...	C0:Good	Ok

SetAttribute FAILURE: UDO4Test_SecuredWrite.UDA_SecuredWrite

MxStatusCategory: MxCategorySecurityError

MxStatusSource: MxSourceRespondingAutomationObject

Status Detail: 1008

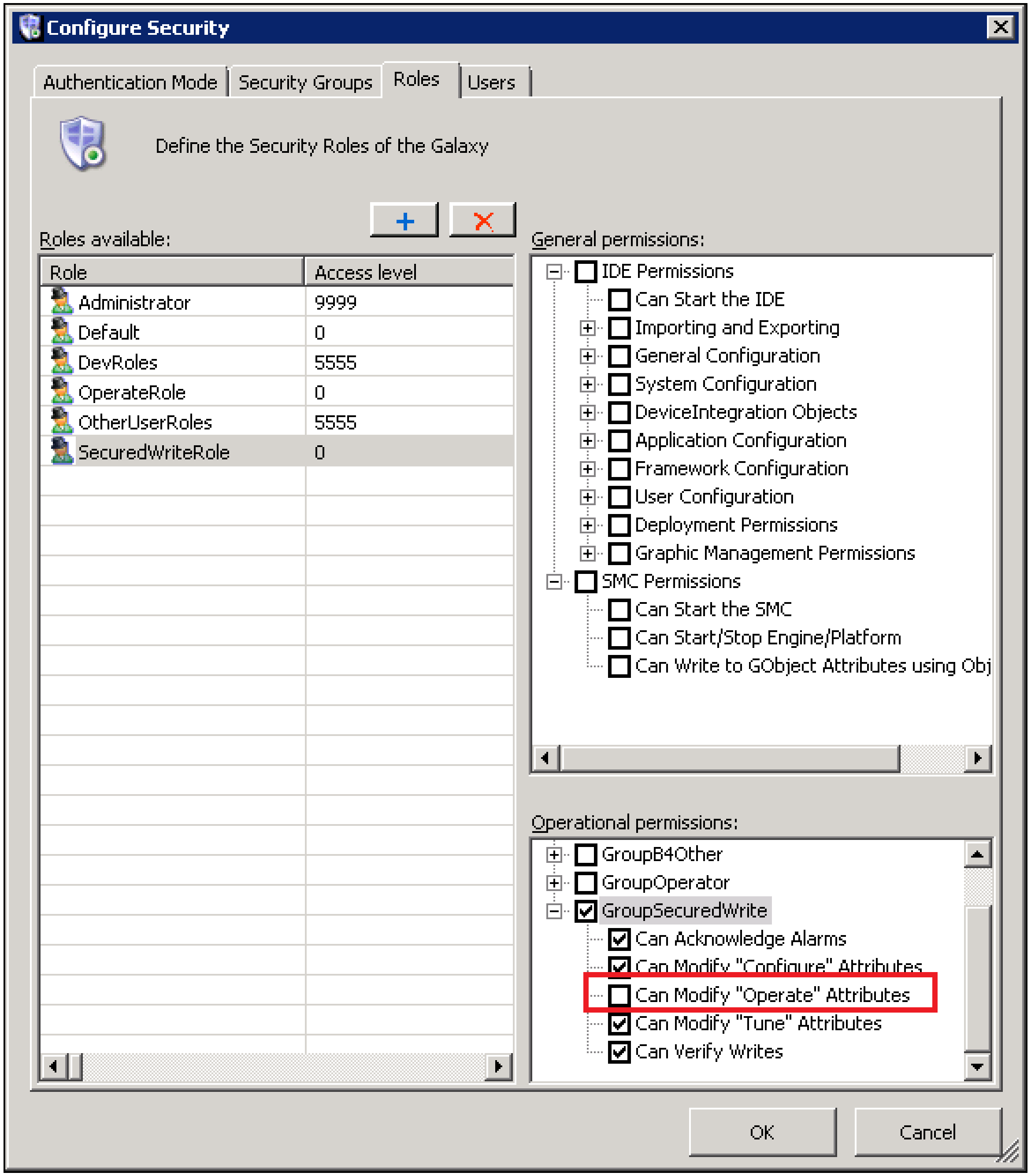
Status Description: Security error: Write access denied

FIGURE 8: THE SECURED WRITE SECURITY CLASSIFICATION DENIES THE WRITE REQUEST: USER ADMINISTRATOR IS NOT IN SECUREDWRITEROLE

Verify 2

The Operate Operational Permission is required.

1. Remove the **Operate** Operational permission from GroupSecuredWrite (Security Group).



Roles available:

Role	Access level
Administrator	9999
Default	0
DevRoles	5555
OperateRole	0
OtherUserRoles	5555
SecuredWriteRole	0

General permissions:

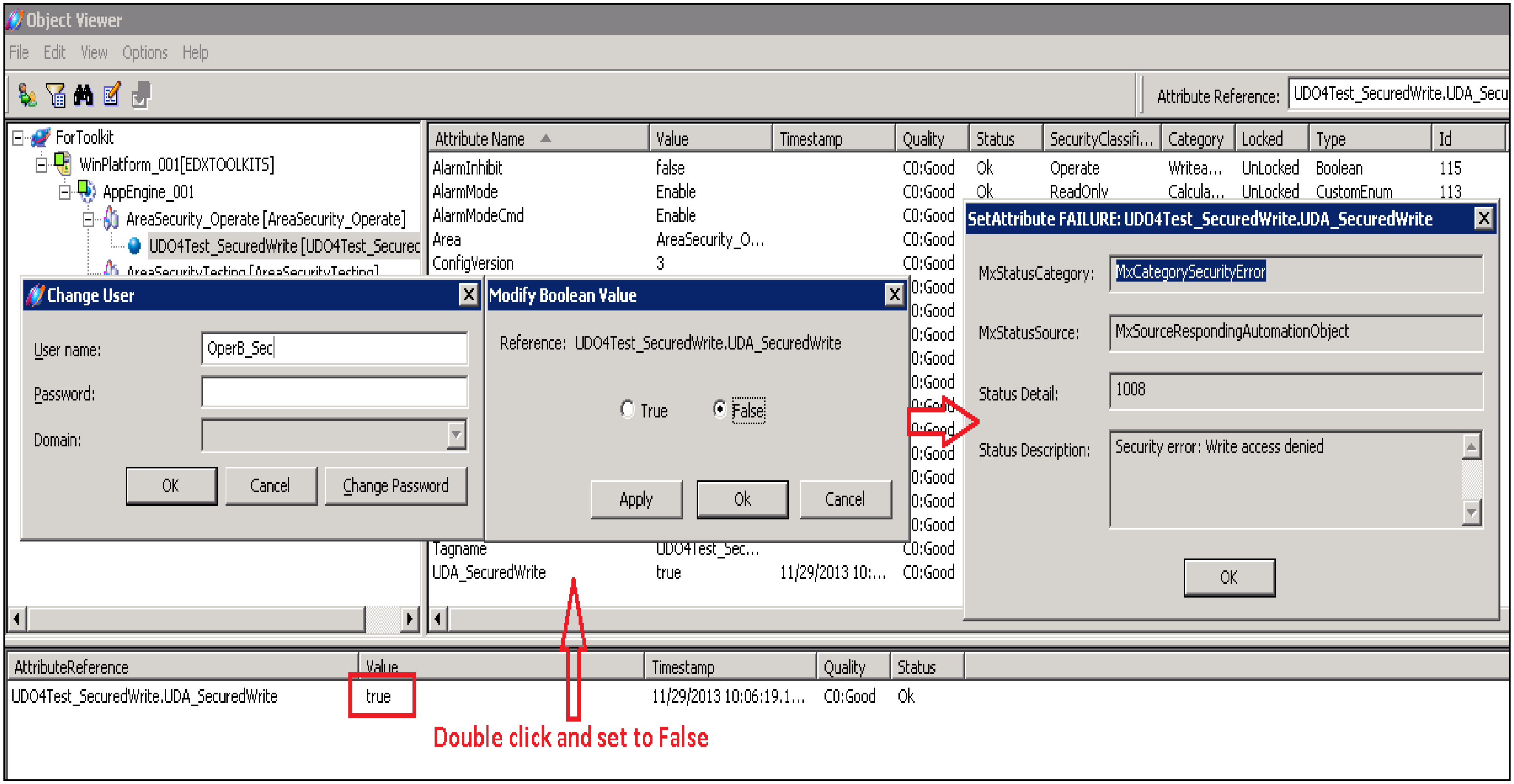
- □ IDE Permissions
  - □ Can Start the IDE
  - □ Importing and Exporting
  - □ General Configuration
  - □ System Configuration
  - □ DeviceIntegration Objects
  - □ Application Configuration
  - □ Framework Configuration
  - □ User Configuration
  - □ Deployment Permissions
  - □ Graphic Management Permissions
- □ SMC Permissions
  - □ Can Start the SMC
  - □ Can Start/Stop Engine/Platform
  - □ Can Write to GObject Attributes using Obj

Operational permissions:

- □ GroupB4Other
- □ GroupOperator
- ☑ GroupSecuredWrite
  - ☑ Can Acknowledge Alarms
  - ☑ Can Modify "Configure" Attributes
  - □ Can Modify "Operate" Attributes
  - ☑ Can Modify "Tune" Attributes
  - ☑ Can Verify Writes

FIGURE 9: UNCHECK CAN MODIFY "OPERATE" ATTRIBUTES

2. Repeat the verification shown in Figure 5 (above). You will see the **Write Access Denied** Error (Figure 10 below).


Object Viewer
File Edit View Options Help
Attribute Reference: UDO4Test_SecuredWrite.UDA_Secu
ForToolkit
WinPlatform_001[EDXTOOLKITS]
AppEngine_001
AreaSecurity_Operate [AreaSecurity_Operate]
UDO4Test_SecuredWrite [UDO4Test_Securec
AreaSecurityTesting [AreaSecurityTesting]
Change User
OK
Cancel
Change Password
Modify Boolean Value
Apply
Ok
Cancel
OK

Attribute Name	Value	Timestamp	Quality	Status	SecurityClassifi...	Category	Locked	Type	Id
AlarmInhibit	false		C0:Good	Ok	Operate	Writea...	UnLocked	Boolean	115
AlarmMode	Enable		C0:Good	Ok	ReadOnly	Calcula...	UnLocked	CustomEnum	113
AlarmModeCmd	Enable		C0:Good						
Area	AreaSecurity_O...		C0:Good						
ConfigVersion	3		C0:Good						
Tagname	UDO4Test_Sec...		C0:Good						
UDA_SecuredWrite	true	11/29/2013 10:...	C0:Good						

Change User

User name: OperB_Sec

Password:

Domain:

Modify Boolean Value

Reference: UDO4Test_SecuredWrite.UDA_SecuredWrite

○ True ● False

SetAttribute FAILURE: UDO4Test_SecuredWrite.UDA_SecuredWrite

MxStatusCategory: MxCategorySecurityError

MxStatusSource: MxSourceRespondingAutomationObject

Status Detail: 1008

Status Description: Security error: Write access denied

AttributeReference	Value	Timestamp	Quality	Status
UDO4Test_SecuredWrite.UDA_SecuredWrite	true	11/29/2013 10:06:19.1...	C0:Good	Ok

Double click and set to False

Figure 10: Write Access Denied

Summary

Secured Write Security Classification needs the Operate Operational permission even if the user is in the correct Role.

Configure

Allows the user to write a value to the attribute only at the **Off-Scan** mode.

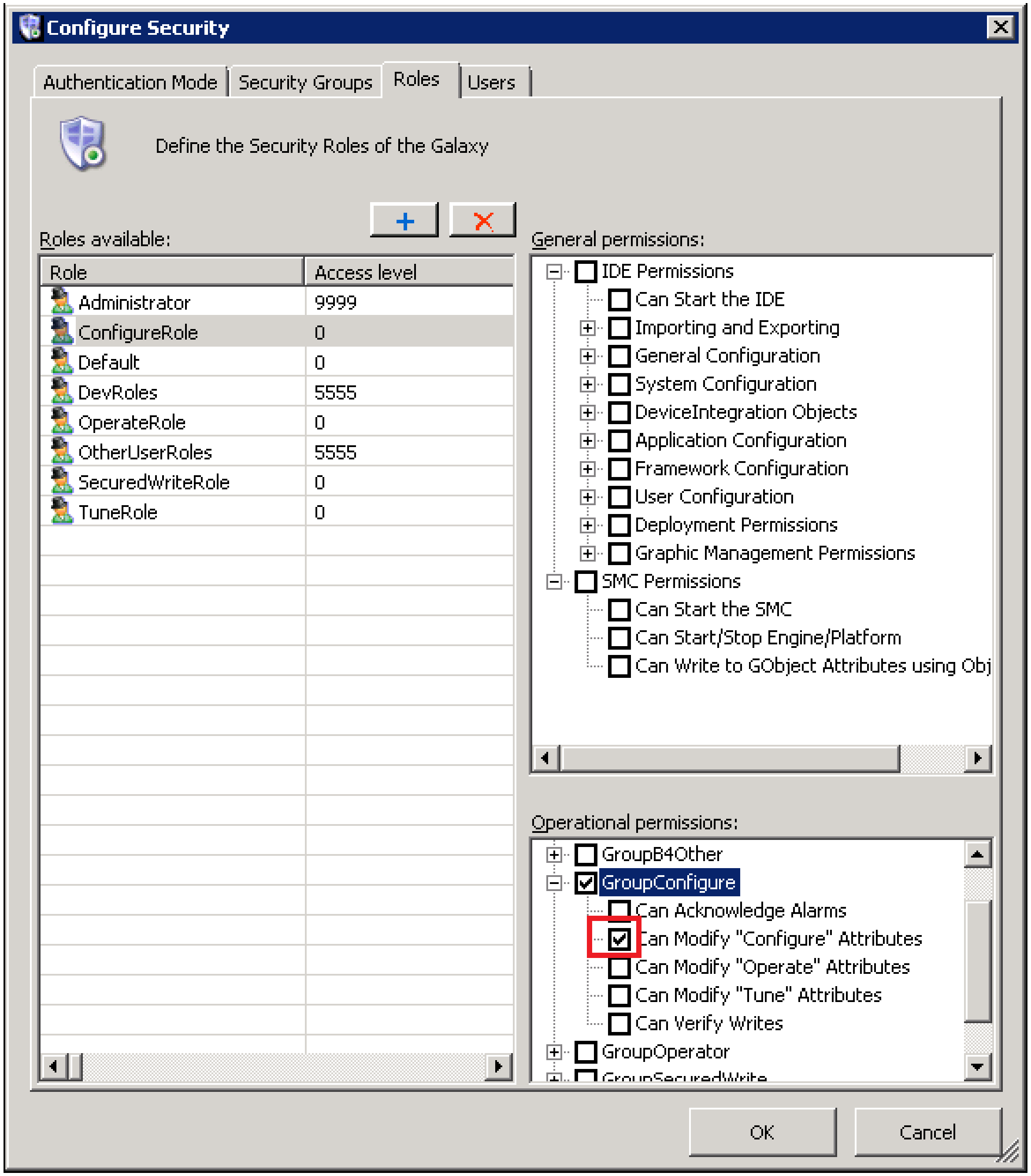
Environment

UDA	UDAConfigure and with **Configure** type of Security Classification.

UDO	UDO4Test_Configure (AA Object) contains UDA_Configure.
Security Group	GroupConfigure contains UDO4Test_Configure (AA Object).
Role	ConfigureRole.
User	ConfigUser

Setup

1. ConfigureRole is granted the access to GroupConfigure.
2. ConfigUser is associated to ConfigureRole.
3. Deploy UDO4Test_Configure (AA Object) with **On-Scan** mode
4. In GroupConfigure, uncheck all options except **Can Modify Configure Attribute**.



Define the Security Roles of the Galaxy

Roles available:

Role	Access level
Administrator	9999
ConfigureRole	0
Default	0
DevRoles	5555
OperateRole	0
OtherUserRoles	5555
SecuredWriteRole	0
TuneRole	0

General permissions:

- □ IDE Permissions
  - □ Can Start the IDE
  - □ Importing and Exporting
  - □ General Configuration
  - □ System Configuration
  - □ DeviceIntegration Objects
  - □ Application Configuration
  - □ Framework Configuration
  - □ User Configuration
  - □ Deployment Permissions
  - □ Graphic Management Permissions
- □ SMC Permissions
  - □ Can Start the SMC
  - □ Can Start/Stop Engine/Platform
  - □ Can Write to GObject Attributes using Obj

Operational permissions:

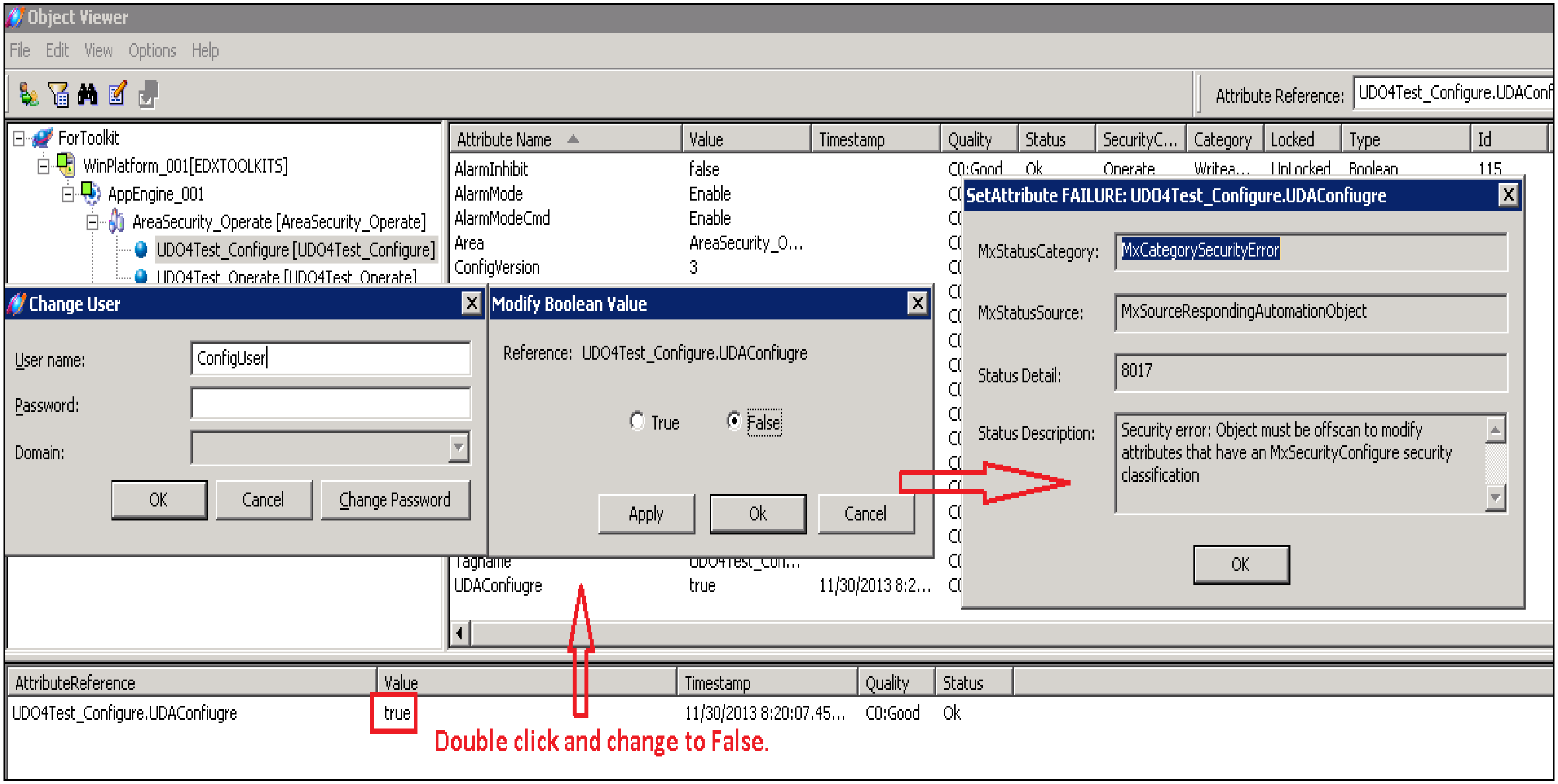
- □ GroupB4Other
- ☑ GroupConfigure
  - □ Can Acknowledge Alarms
  - ☑ Can Modify "Configure" Attributes
  - □ Can Modify "Operate" Attributes
  - □ Can Modify "Tune" Attributes
  - □ Can Verify Writes
- □ GroupOperator
- □ GroupSecuredWrite

Figure 11: Leave Can Modify "Configure" Attributes Option Checked

Verify

1. Open UDO4Test_Configure (AA Object) in the Object Viewer.

2. Change value of UDAConfigure. The **Security Error 8017** Error will be returned.


Object Viewer
File Edit View Options Help
Attribute Reference: UDO4Test_Configure.UDAConf
ForToolkit
WinPlatform_001[EDXTOOLKITS]
AppEngine_001
AreaSecurity_Operate [AreaSecurity_Operate]
UDO4Test_Configure [UDO4Test_Configure]
UDO4Test_Operate [UDO4Test_Operate]
Change User
OK
Cancel
Change Password
Modify Boolean Value
Apply
Ok
Cancel
OK

Attribute Name	Value	Timestamp	Quality	Status	SecurityC...	Category	Locked	Type	Id
AlarmInhibit	false		C0:Good	Ok	Operate	Writea...	UnLocked	Boolean	115
AlarmMode	Enable		C(						
AlarmModeCmd	Enable		C(						
Area	AreaSecurity_O...		C(						
ConfigVersion	3		C(						
Tagname	UDO4Test_Con...		C(						
UDAConfiugre	true	11/30/2013 8:2...	C(						

Change User

User name: ConfigUser

Password:

Domain:

Modify Boolean Value

Reference: UDO4Test_Configure.UDAConfiugre

○ True ● False

SetAttribute FAILURE: UDO4Test_Configure.UDAConfiugre

MxStatusCategory: MxCategorySecurityError

MxStatusSource: MxSourceRespondingAutomationObject

Status Detail: 8017

Status Description: Security error: Object must be offscan to modify attributes that have an MxSecurityConfigure security classification

AttributeReference	Value	Timestamp	Quality	Status
UDO4Test_Configure.UDAConfiugre	true	11/30/2013 8:20:07.45...	C0:Good	Ok

Double click and change to False.

Figure 12: SetAttribute FAILURE

Summary

Configure Security Classification only works while in **Off-Scan** Deployment state.

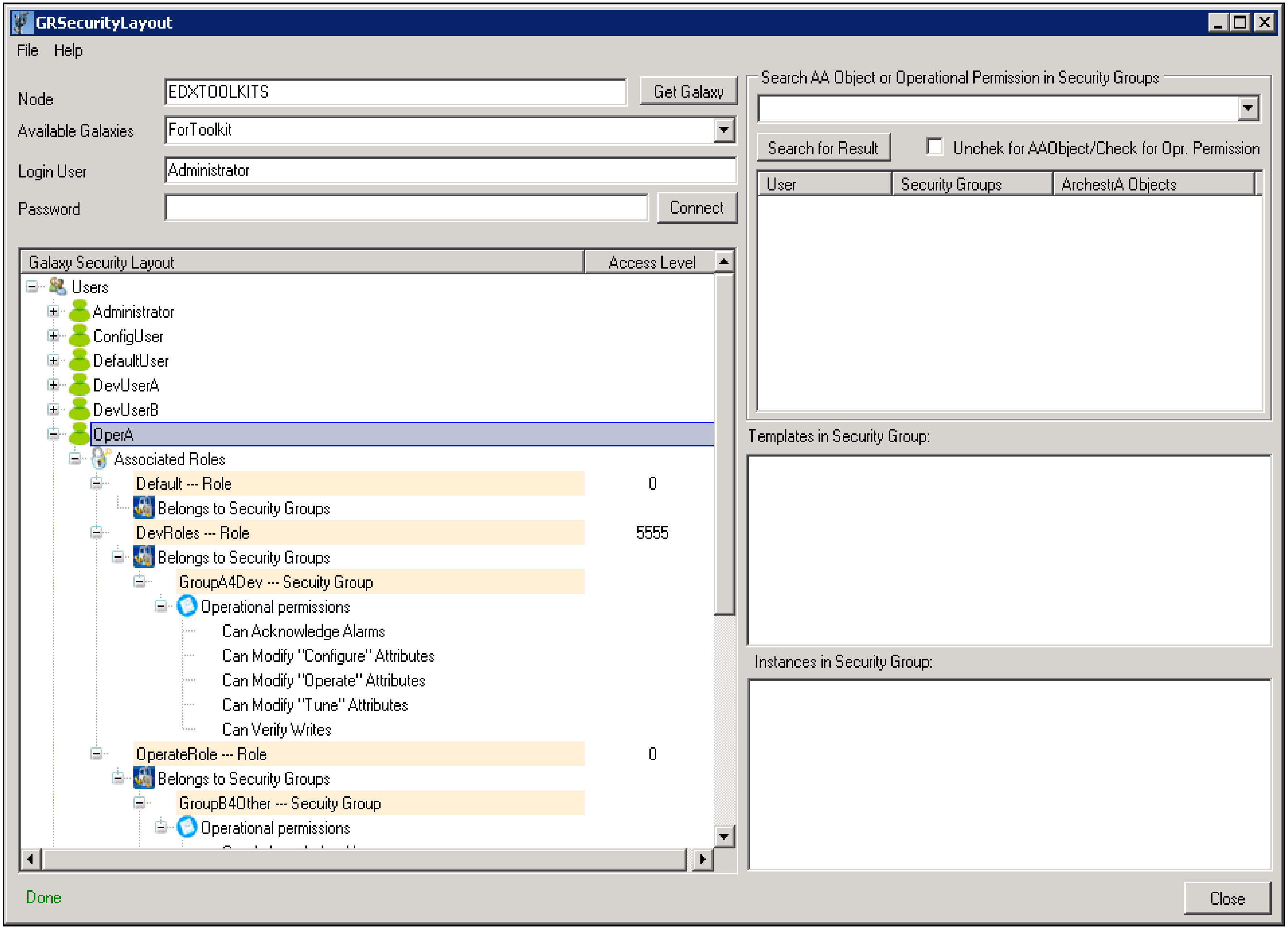
GRSecurityLayout Utility

This Read-Only Utility provides a quick way to view and search the Galaxy Security Settings on Security Groups with AA Objects and Operational permissions, Roles and Users, within a single page.

Download the GRSecurityLayout Utility

Note: This Utility is developed with Wonderware Galaxy Repository Access (GRAccess) Toolkit. Therefore, like the IDE, running this Utility will consume one Dev_Session_Count License Feature count which is listed in ArchestrA.lic. The Utility's main functions are as follows:

- **Galaxy User Oriented Tree-View**: Shows each Galaxy user's Runtime Security Relationships.



GRSecurityLayout

Node: EDXTOOLKITS

Available Galaxies: ForToolkit

Login User: Administrator

Password:

Search AA Object or Operational Permission in Security Groups

□ Unchek for AAObject/Check for Opr. Permission

User	Security Groups	ArchestrA Objects

Templates in Security Group:

Instances in Security Group:

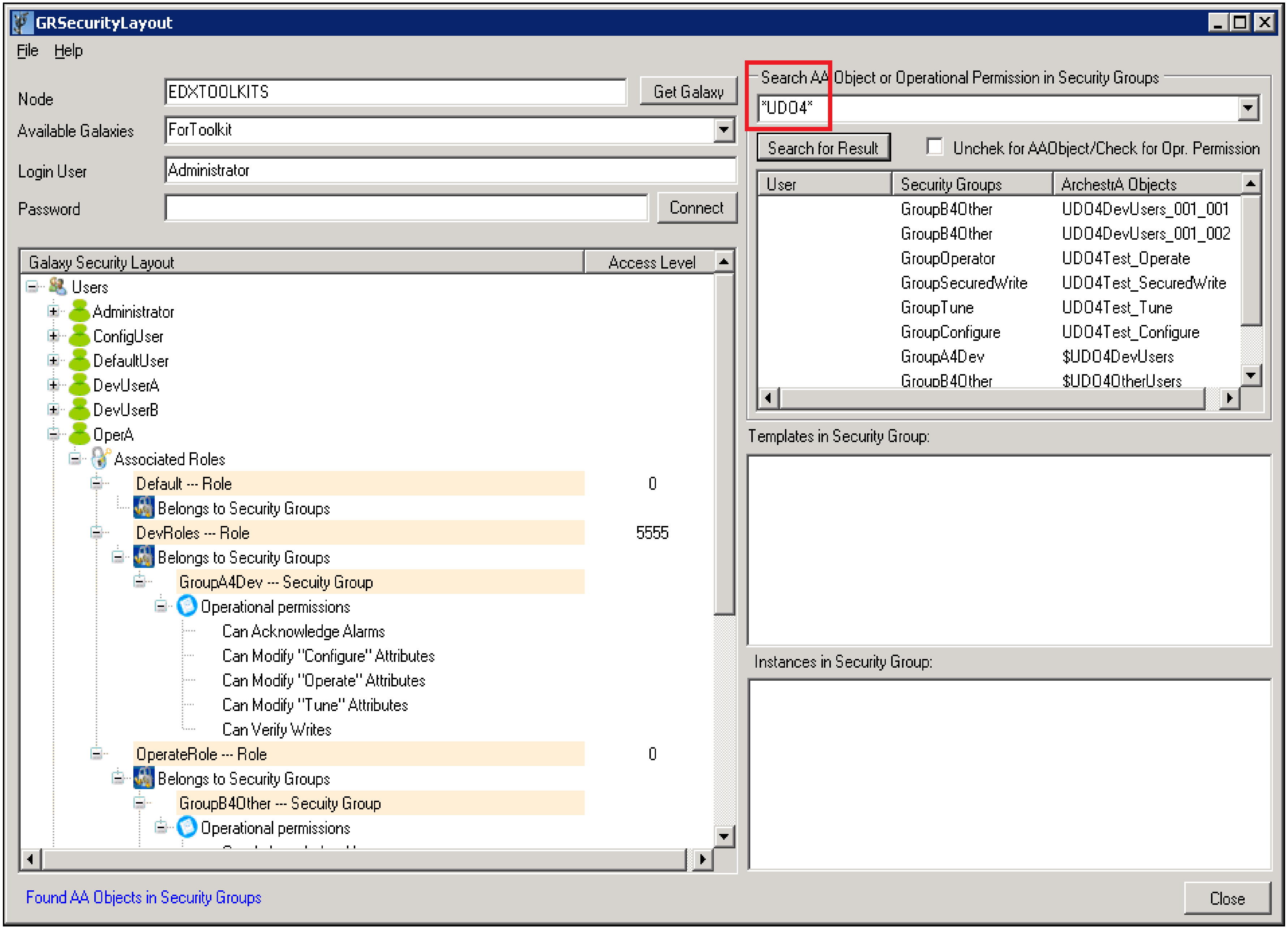
Galaxy Security Layout	Access Level
Users	
Administrator	
ConfigUser	
DefaultUser	
DevUserA	
DevUserB	
OperA	
Associated Roles	
Default --- Role	0
Belongs to Security Groups	
DevRoles --- Role	5555
Belongs to Security Groups	
GroupA4Dev --- Secuity Group	
Operational permissions	
Can Acknowledge Alarms	
Can Modify "Configure" Attributes	
Can Modify "Operate" Attributes	
Can Modify "Tune" Attributes	
Can Verify Writes	
OperateRole --- Role	0
Belongs to Security Groups	
GroupB4Other --- Secuity Group	
Operational permissions	

Done

Figure 13: User-Based Security View

- **Wildcard Search AA Objects and their belonging Security Groups**: In a real world Galaxy, there are usually a large number of AA Objects. Quickly finding any AA Object's associated Security Groups is very important during the Security Design and

Verification procedures.



GRSecurityLayout

Node	EDXTOOLKITS
Available Galaxies	ForToolkit
Login User	Administrator
Password	

Search AA Object or Operational Permission in Security Groups: *UD04*

☐ Unchek for AAObject/Check for Opr. Permission

User	Security Groups	ArchestrA Objects
	GroupB4Other	UD04DevUsers_001_001
	GroupB4Other	UD04DevUsers_001_002
	GroupOperator	UD04Test_Operate
	GroupSecuredWrite	UD04Test_SecuredWrite
	GroupTune	UD04Test_Tune
	GroupConfigure	UD04Test_Configure
	GroupA4Dev	$UD04DevUsers
	GroupB4Other	$UD04OtherUsers

Galaxy Security Layout	Access Level
Users	
Administrator	
ConfigUser	
DefaultUser	
DevUserA	
DevUserB	
OperA	
Associated Roles	
Default --- Role	0
Belongs to Security Groups	
DevRoles --- Role	5555
Belongs to Security Groups	
GroupA4Dev --- Secuity Group	
Operational permissions	
Can Acknowledge Alarms	
Can Modify "Configure" Attributes	
Can Modify "Operate" Attributes	
Can Modify "Tune" Attributes	
Can Verify Writes	
OperateRole --- Role	0
Belongs to Security Groups	
GroupB4Other --- Secuity Group	
Operational permissions	

Templates in Security Group:

Instances in Security Group:

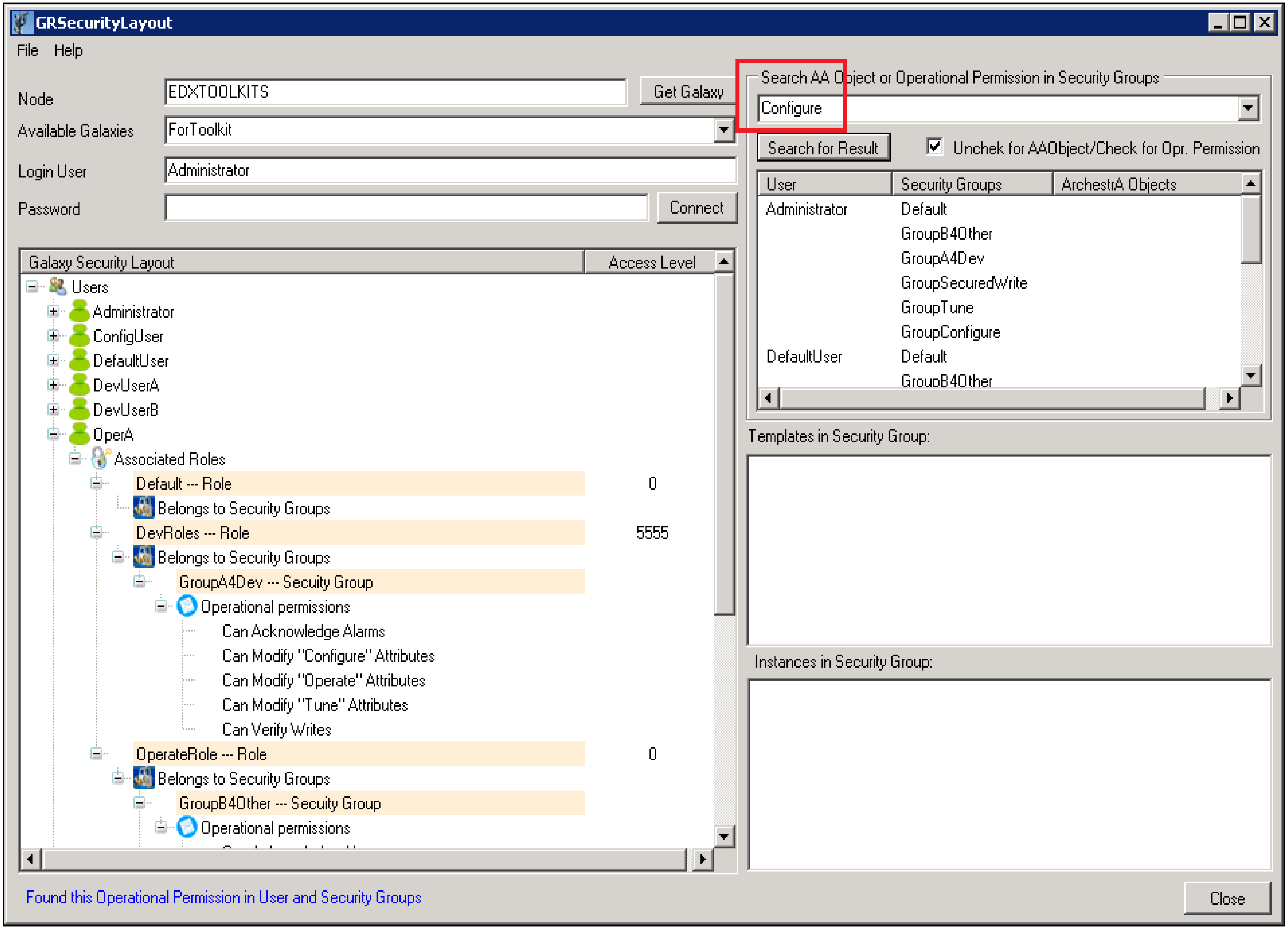
Found AA Objects in Security Groups

Figure 14: Wildcard Search Returns Security Group List That Contains All AA Objects Containing the Value

- Search the Users and Security Groups that have the given Operational permission.

In Figure 15 (below), we search all the Security Groups that contain the **Configure** Operational permission and the users in these

Security Groups.



Node: EDXTOOLKITS

Available Galaxies: ForToolkit

Login User: Administrator

Password:

Search AA Object or Operational Permission in Security Groups: Configure

☑ Unchek for AAObject/Check for Opr. Permission

User	Security Groups	ArchestrA Objects
Administrator	Default	
	GroupB4Other	
	GroupA4Dev	
	GroupSecuredWrite	
	GroupTune	
	GroupConfigure	
DefaultUser	Default	
	GroupB4Other	

Templates in Security Group:

Instances in Security Group:

```
Galaxy Security Layout                                   Access Level
Users
  Administrator
  ConfigUser
  DefaultUser
  DevUserA
  DevUserB
  OperA
    Associated Roles
      Default --- Role                                   0
        Belongs to Security Groups
      DevRoles --- Role                                  5555
        Belongs to Security Groups
          GroupA4Dev --- Secuity Group
            Operational permissions
              Can Acknowledge Alarms
              Can Modify "Configure" Attributes
              Can Modify "Operate" Attributes
              Can Modify "Tune" Attributes
              Can Verify Writes
      OperateRole --- Role                               0
        Belongs to Security Groups
          GroupB4Other --- Secuity Group
            Operational permissions
```

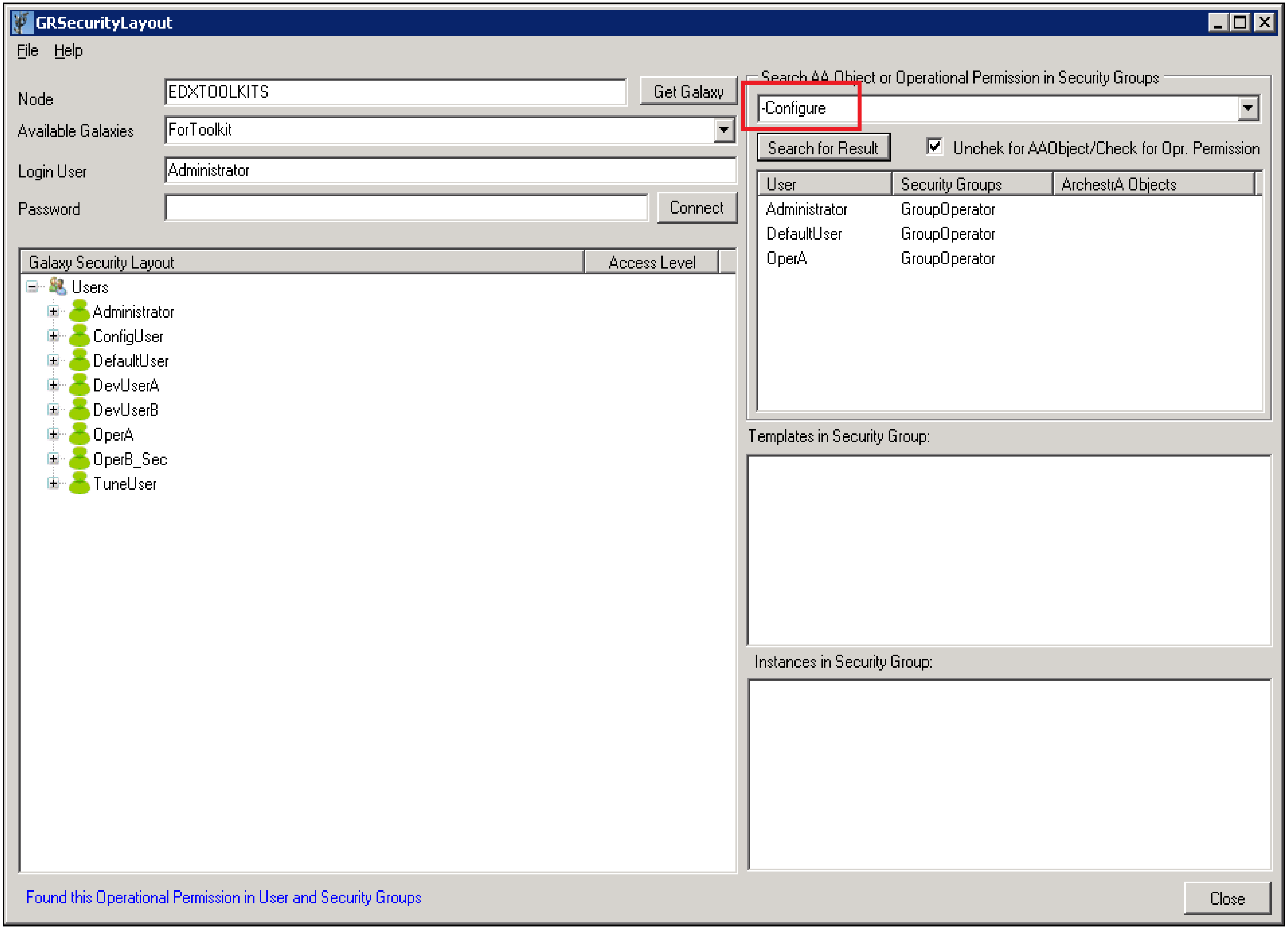
Found this Operational Permission in User and Security Groups

Figure 15: Search By Security Group

- Search the Users and Security Groups that *do not* have the given Operational permission.

In Figure 16 (below), we search all the Security Groups that do not contain the **Configure** Operational permission and the users in these Security Groups.

The "**-**" (dash character) in the search criteria means **Not Contain**.



Node: EDXTOOLKITS

Available Galaxies: ForToolkit

Login User: Administrator

Password:

-Configure

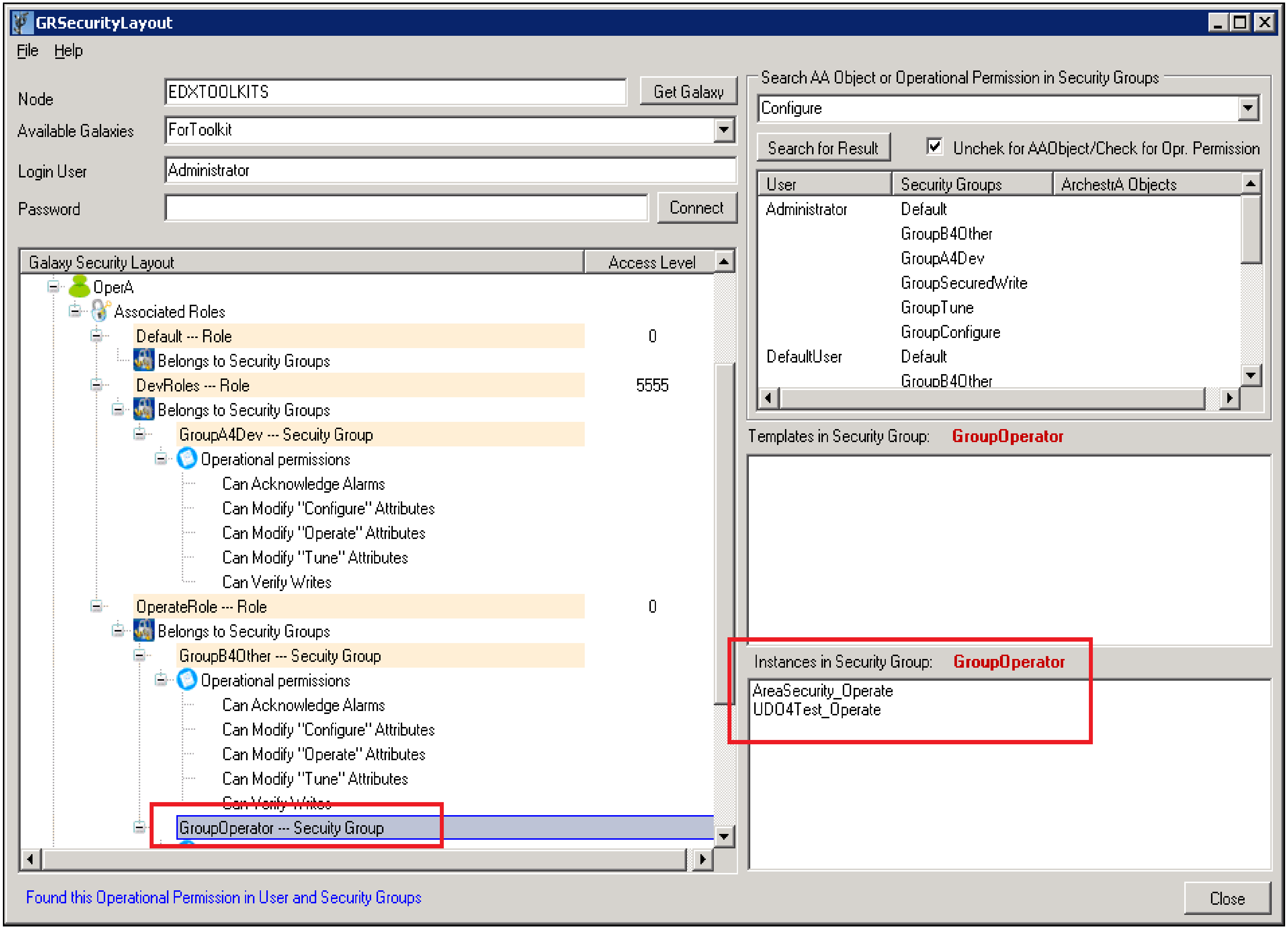
☑ Unchek for AAObject/Check for Opr. Permission

User	Security Groups	ArchestrA Objects
Administrator	GroupOperator	
DefaultUser	GroupOperator	
OperA	GroupOperator	

Found this Operational Permission in User and Security Groups

Figure 16: Filter using the Dash Character

- Quick retrieve AA Objects, Templates and Instances, within any selected Security Group.



Node: EDXTOOLKITS

Available Galaxies: ForToolkit

Login User: Administrator

Password:

Search AA Object or Operational Permission in Security Groups: Configure

☑ Unchek for AAObject/Check for Opr. Permission

User	Security Groups	ArchestrA Objects
Administrator	Default	
	GroupB4Other	
	GroupA4Dev	
	GroupSecuredWrite	
	GroupTune	
	GroupConfigure	
DefaultUser	Default	
	GroupB4Other	

```
Galaxy Security Layout                                   Access Level
OperA
  Associated Roles
    Default --- Role                                     0
      Belongs to Security Groups
    DevRoles --- Role                                    5555
      Belongs to Security Groups
        GroupA4Dev --- Secuity Group
          Operational permissions
            Can Acknowledge Alarms
            Can Modify "Configure" Attributes
            Can Modify "Operate" Attributes
            Can Modify "Tune" Attributes
            Can Verify Writes
    OperateRole --- Role                                 0
      Belongs to Security Groups
        GroupB4Other --- Secuity Group
          Operational permissions
            Can Acknowledge Alarms
            Can Modify "Configure" Attributes
            Can Modify "Operate" Attributes
            Can Modify "Tune" Attributes
            Can Verify Writes
        GroupOperator --- Secuity Group
```

Templates in Security Group: **GroupOperator**

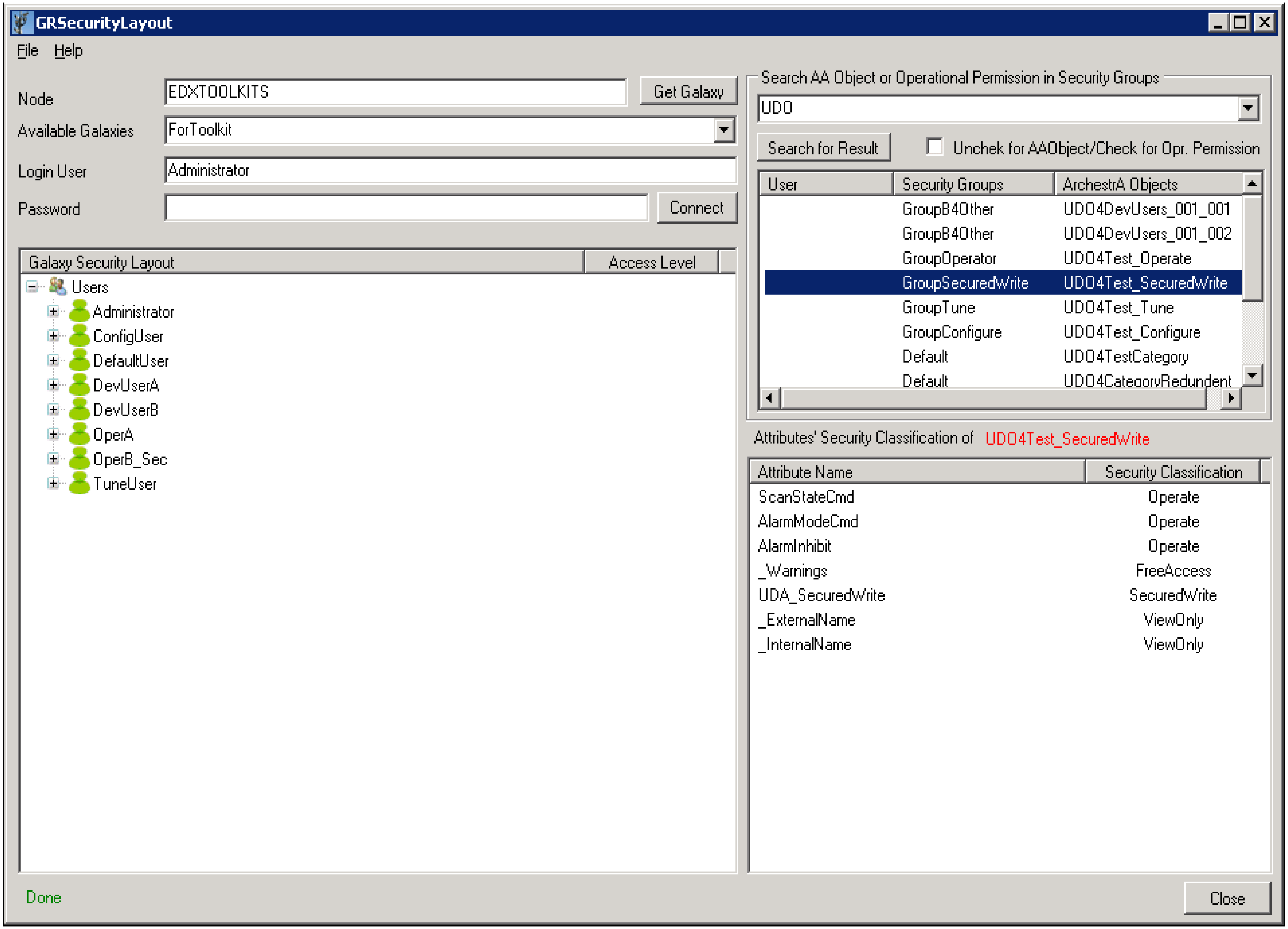
Instances in Security Group: **GroupOperator**

AreaSecurity_Operate
UDO4Test_Operate

Found this Operational Permission in User and Security Groups

Figure 17: Highlight Any Security Group Level in the Tree View to see the contained AA Objects (Template or Instance)

- Quick retrieve AA Objects' attribute names and their corresponding Security Classification (Figure 18 below).



Node: EDXTOOLKITS

Available Galaxies: ForToolkit

Login User: Administrator

Password:

Galaxy Security Layout	Access Level
Users	
Administrator	
ConfigUser	
DefaultUser	
DevUserA	
DevUserB	
OperA	
OperB_Sec	
TuneUser	

Search AA Object or Operational Permission in Security Groups: UDO

☐ Unchek for AAObject/Check for Opr. Permission

User	Security Groups	ArchestrA Objects
	GroupB4Other	UDO4DevUsers_001_001
	GroupB4Other	UDO4DevUsers_001_002
	GroupOperator	UDO4Test_Operate
	GroupSecuredWrite	UDO4Test_SecuredWrite
	GroupTune	UDO4Test_Tune
	GroupConfigure	UDO4Test_Configure
	Default	UDO4TestCategory
	Default	UDO4CategoryRedundent

Attributes' Security Classification of UDO4Test_SecuredWrite

Attribute Name	Security Classification
ScanStateCmd	Operate
AlarmModeCmd	Operate
AlarmInhibit	Operate
_Warnings	FreeAccess
UDA_SecuredWrite	SecuredWrite
_ExternalName	ViewOnly
_InternalName	ViewOnly

Done

Figure 18: AA Object, UDO4Test_SecuredWrite's Attribute Names, and Corresponding Security Classification

References

- Wonderware Application Server 2012 R2 – IDE.PDF

A. Rantos, E. Xu

Tech Notes are published occasionally by Wonderware Technical Support. Publisher: Invensys Systems, Inc., 26561 Rancho Parkway South, Lake Forest, CA 92630. There is also technical information on our software products at **Wonderware Technical Support.**

For technical support questions, send an e-mail to **wwsupport@invensys.com**.

Back to top