

## [Tech Note 998](#)

# Wonderware Application Server Security Troubleshooting Essentials Part 1: Galaxy Security - Runtime Errors and Security Groups Settings

---

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#: 002828

Created: December 2013

## Introduction

This Essentials *Tech Note* is the 1st in a projected series.

Galaxy-type security uses local Galaxy configuration to authenticate users. All security for the Galaxy is specified and contained at the specific Galaxy level. When the user logs on, security credentials are checked and access to areas and activities is granted at the Galaxy level.

In Application Server you can select from three authentication modes to assign security. This *Tech Note* discusses two common Application Server errors experienced with Galaxy type security.

It includes

- The symptoms,
- Root cause analysis, and
- Configurable resolutions.

## Application Versions

- Wonderware Application Server 2012 and later

## Issues

This *Tech Note* details the following cases:

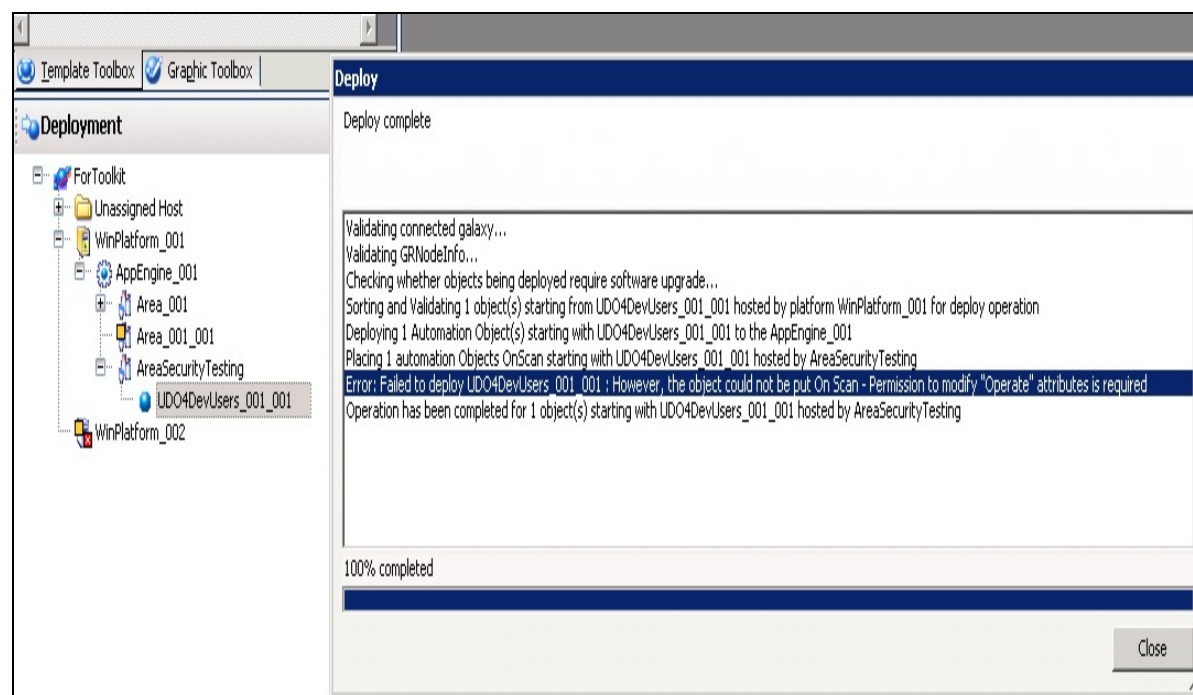
- Case 1: Deployed ArchestrA Object has Error Messages.
- Case 2: Access-Denied Error when Setting a UDA Value from the Object Viewer.

## Symptoms

By default, the Galaxy Administrator account has full privileges. However, the default settings can be changed and the assumption of full

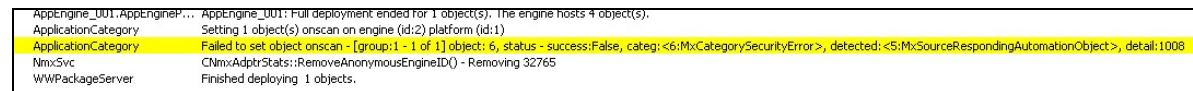
privileges might not always be true.

## Case 1: Deploy an Arcestra Object - UDO4DevUsers\_001\_001 - Has Error Messages



In Figure 1 (at left), you see a one-line error message in the Deploy message window. This error line provides a message that we will use for later analysis. However, if there are a large number of Arcestra objects included in this deployment, this error line could easily go unnoticed.

**FIGURE 1: DEPLOYED WITH ERROR MESSAGE**



In Figure 2 (at left), the warning message does not clearly describe the problem.

**FIGURE 2: WARNING MESSAGE IN THE SMC LOGGER**

In Figure 3 (at left), we see there is a warning icon that tells you this Arcestra object is abnormal, but no any further indication.

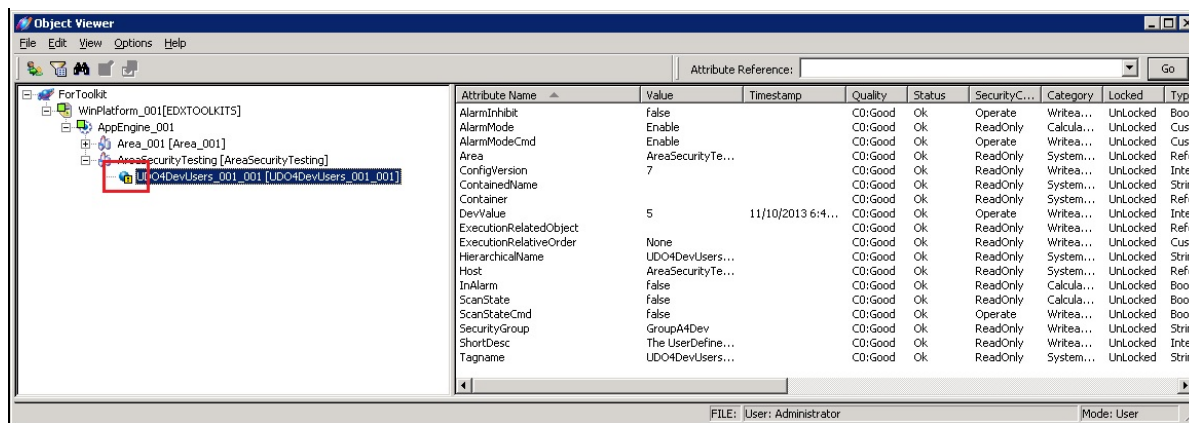
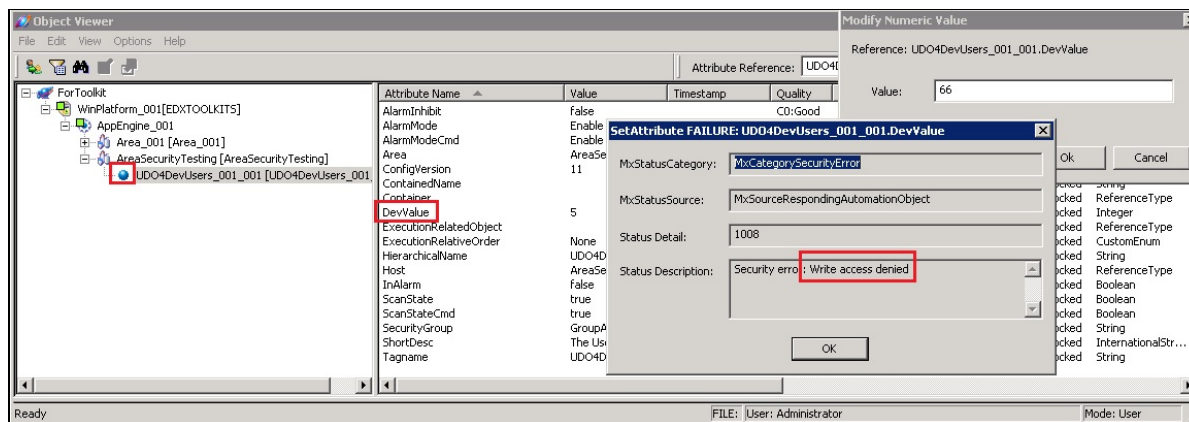


FIGURE 3: WARNING ICON IN THE OBJECT VIEWER

## Case 2: Access-Denied Error When Setting a UDA Value from the Object Viewer



In Figure 4 (at left), we don't see any errors or warnings that were shown above in Figures 1-3. However, we still see the Write access denied error when attempting to set a new value to UDA (DevValue).

What is wrong?

FIGURE 4: WRITE ACCESS DENIED DESCRIPTION WHEN SETTING A VALUE ON THE UDA (DEVVALUE)

## Root Cause & Resolution

The first step in troubleshooting security-related errors is to check the Galaxy SECURITY SETTINGS.

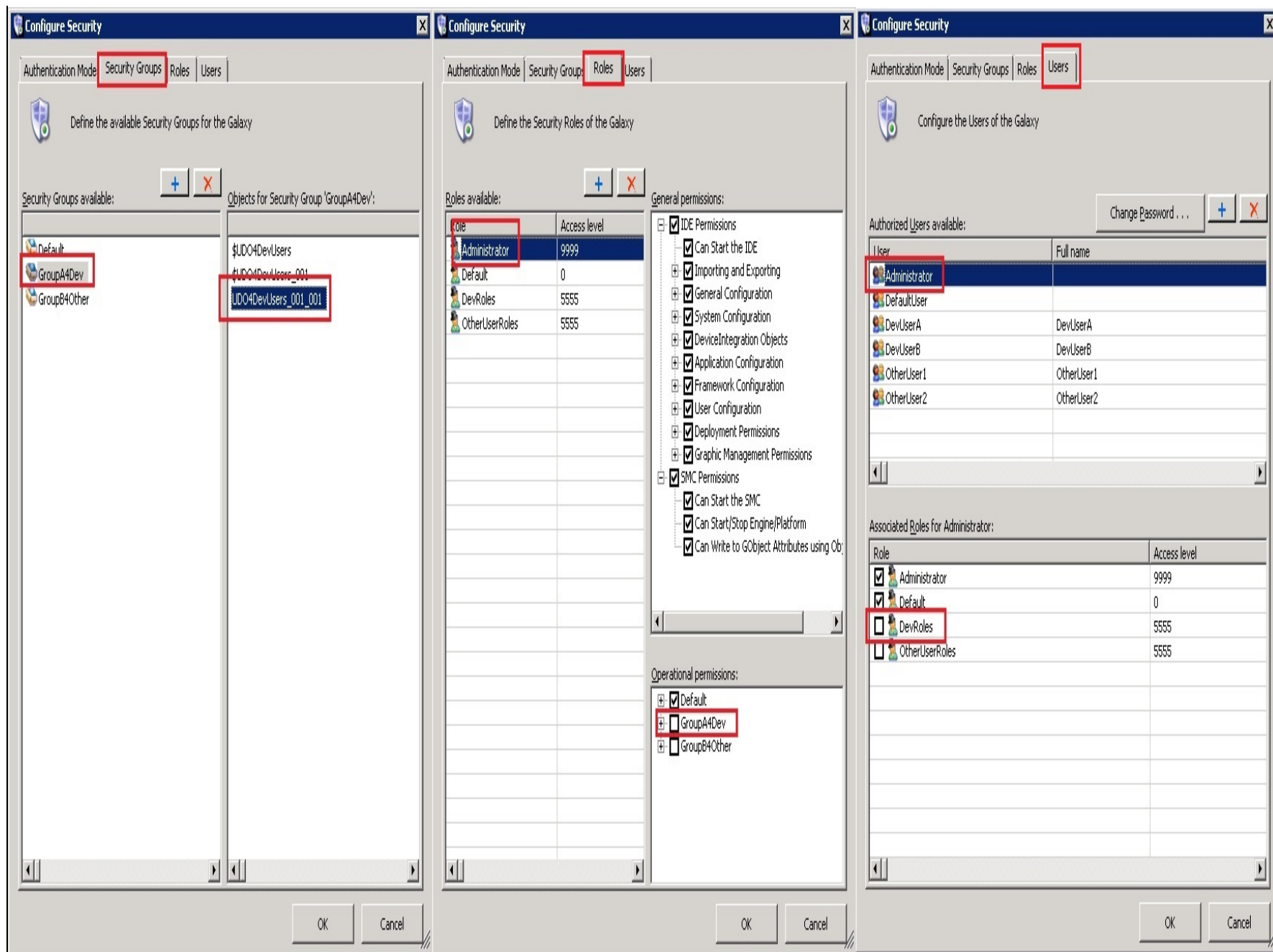
### Case 1: Deploy an Arcestra Object - UDO4DevUsers\_001\_001

From the information we collected above in Figures 1-3, checking the Security Settings is our priority focus for continued troubleshooting. For this case, let's look closer at the impact of the security settings:

Check which Security Group UDO4DevUsers\_001\_001 belongs to. Figure 5 (below) shows the **Configure Security** window with the respective tabs' checkpoints.

- **Security Groups** tab: UDO4DevUsers\_001\_001 belongs to the **GroupA4Dev** Security Group.

- **Roles** tab: The **Administrator** Role does not have GroupA4Dev Operational permissions. In this example, only the **DevRoles** Role has GroupA4Dev Operational permissions.
- **Users** tab: The **Administrator** user is not in **DevRoles** Role. **DevRoles** is the only role that has **GroupA4Dev** Operational permissions.



**FIGURE 5: GALAXY SECURITY SETTINGS**

After this side by side comparison, it's clear the root cause of the problem. In fact, even when we login as the Galaxy Administrator, the Galaxy security rules still need to be kept in mind.

To fix the issue, check the **DevRoles** role in the **Associated Roles for Administrator** panel of the **Users** tab and re-deploy the ArchestraA object (for this example, **UDO4DevUsers\_001\_00**).

## Case 2: Access-Denied Error When Setting a UDA Value from the Object Viewer

In Figure 4, you were unable to set the value of the UDA DevValue. You also know that there are no error messages during the ArchestraA Object deployment.

The next step is to check the security settings on the Object and on the UDA. The following steps will help you determine the root cause.

1. In the **UDAs** tab of the Object, check the DevValue's current **Operational Permission** level (Figure 6 below):

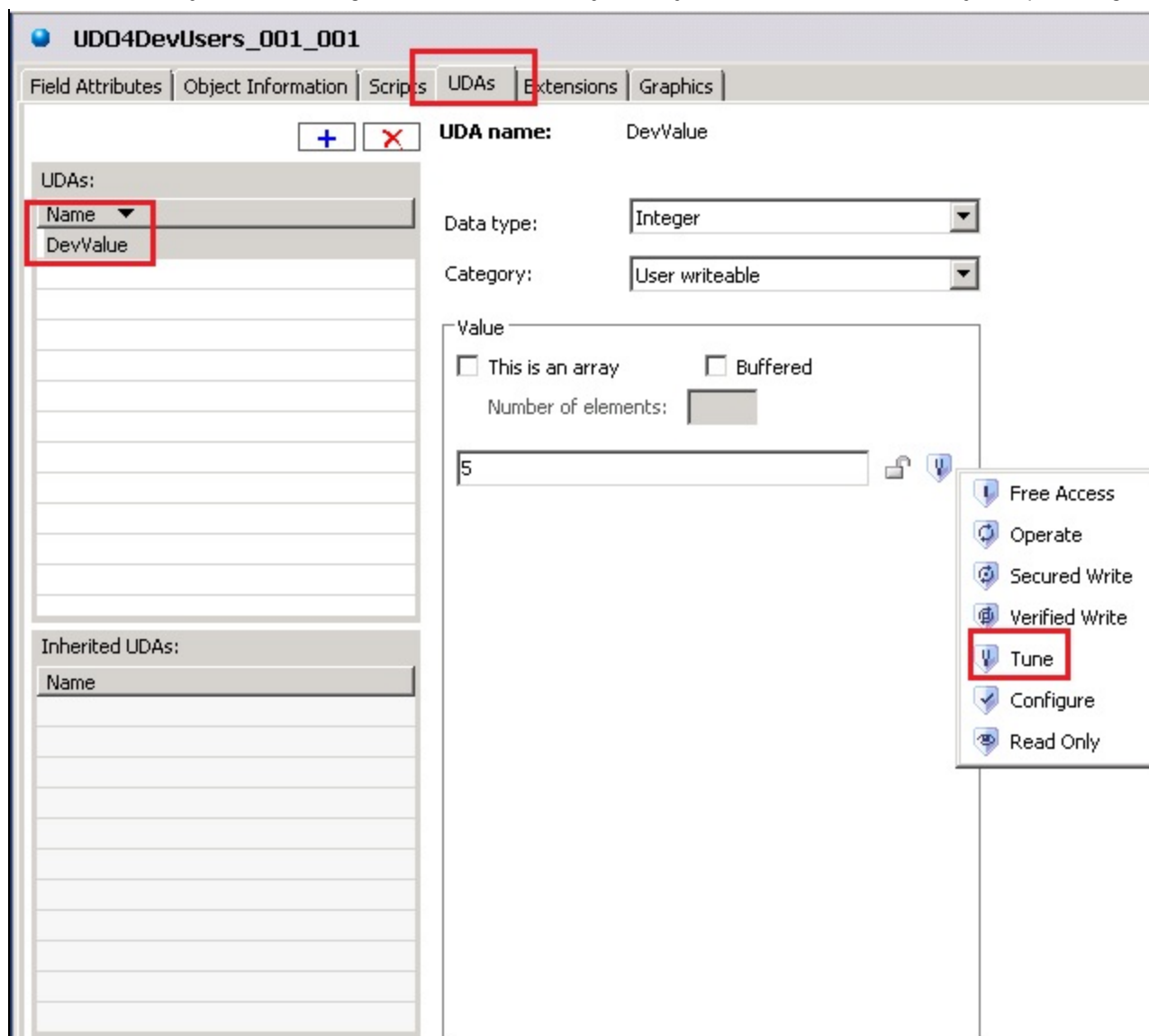
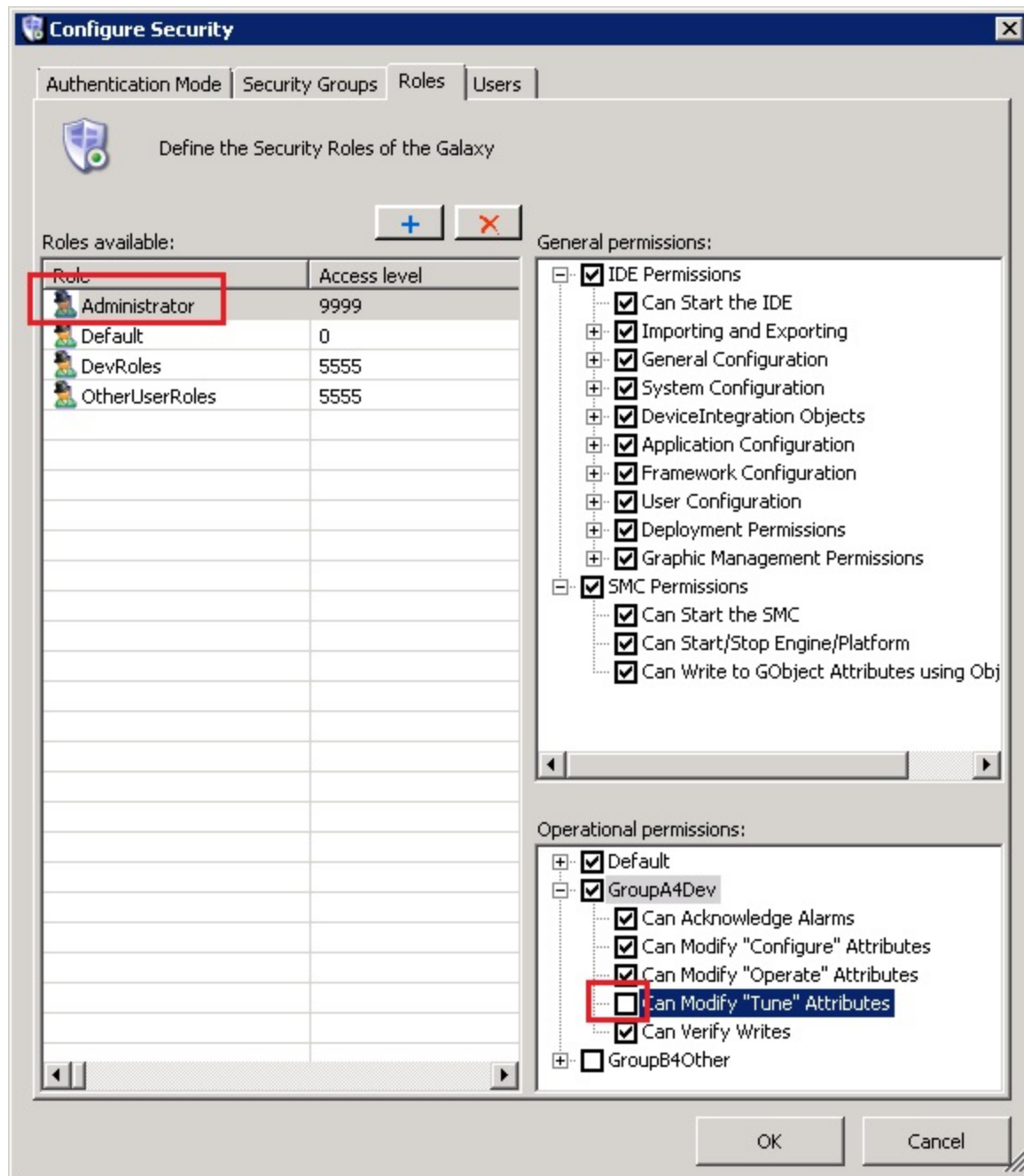


FIGURE 6: UDA DevValue HAS THE TUNE OPERATIONAL PERMISSION

2. Check to see if the Administrator has **Tune** Operational permissions (**Configure Security** window):



**FIGURE 7: ADMINISTRATOR ROLE HAS NO "MODIFY" OPERATIONAL PERMISSION**

Figures 6 and 7 (above) show that the value of the UDA (DevValue) requires Tune Operational permissions in order to write. However, the current logon user (administrator) does not have the Tune Operational permission.

- To fix the problem, make sure the current Galaxy logged on user has **Tune** Operational permissions.



## References

- Wonderware Application Server 2012 R2 – IDE.PDF: IDE User Guide for AppServer 2012 R2
- [Tech Note 295 Security Features in InTouch 8.x](#)

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](mailto:wwsupport@invensys.com).



[Back to top](#)

©2013 Invensys Systems, Inc. All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, broadcasting, or by any information storage and retrieval system, without permission in writing from Invensys Systems, Inc.

[Terms of Use](#).