Tech Note 978
Troubleshooting ArchestrA System Platform Cross-Domain Login Problems

Topic#: 002803
Created: August 2013

Introduction

When you have created a 2-way trust between 2 Domains, and configured ArchestrA security to use **OS Group Base.** The GR node is on Domain A, and a user from Domain B cannot log on.

Application Versions

- InTouch 10.1 and later
- ArchestrA System Platform 3.1 and later

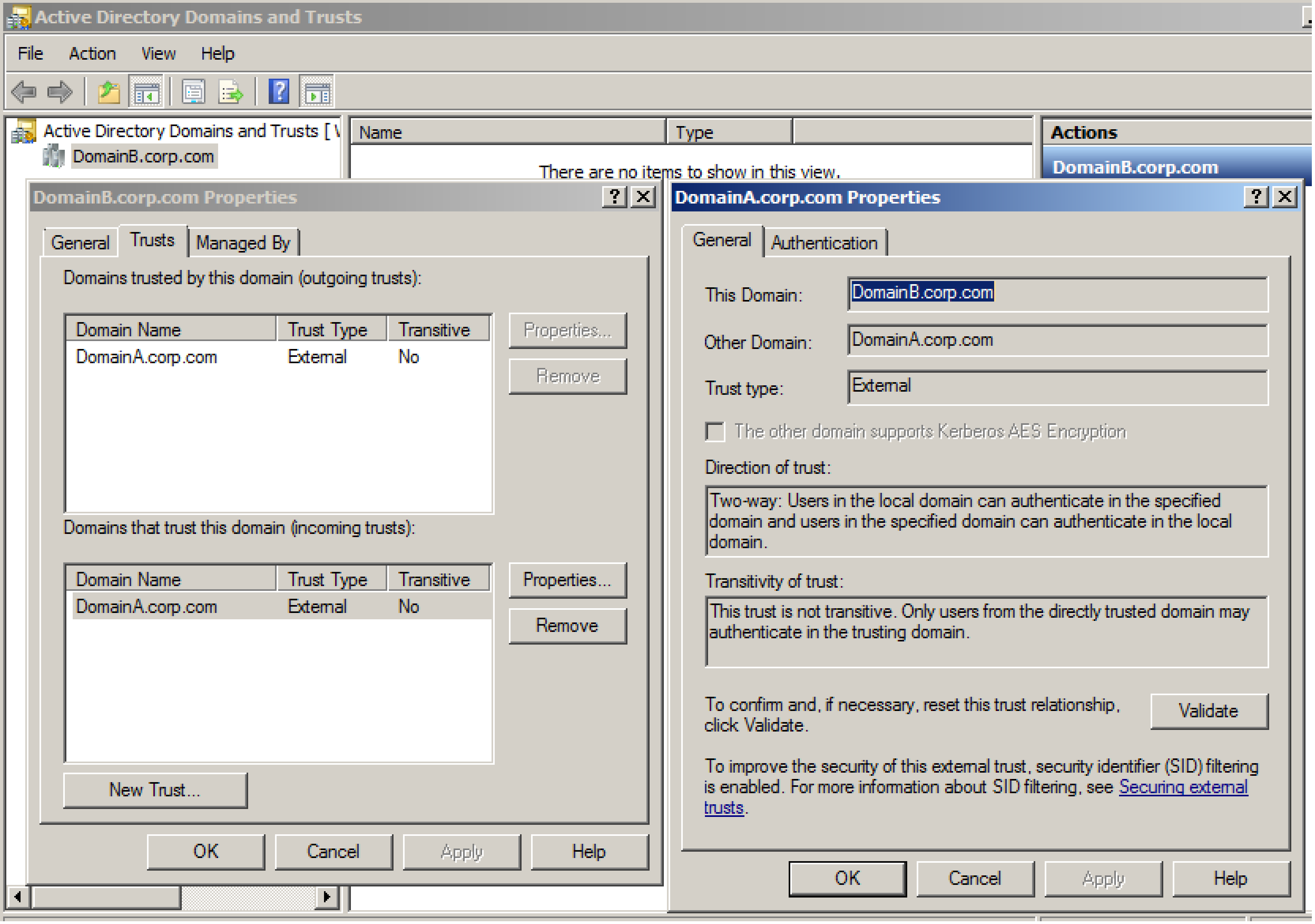
Cause

The 2-way trust between the 2 Domains is not configured properly, and the InTouch security type is set to **OS**.

Resolution

Check the Domains' 2-Way Trust Settings

Note: Do this on BOTH Domain Controllers. Galaxy security can be configured using any IDE connected to the Galaxy.



There are no items to show in this view.

DomainB.corp.com Properties

Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
DomainA.corp.com	External	No

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive
DomainA.corp.com	External	No

DomainA.corp.com Properties

This Domain: DomainB.corp.com

Other Domain: DomainA.corp.com

Trust type: External

☐ The other domain supports Kerberos AES Encryption

Direction of trust:

Two-way: Users in the local domain can authenticate in the specified domain and users in the specified domain can authenticate in the local domain.

Transitivity of trust:

This trust is not transitive. Only users from the directly trusted domain may authenticate in the trusting domain.

To confirm and, if necessary, reset this trust relationship, click Validate.

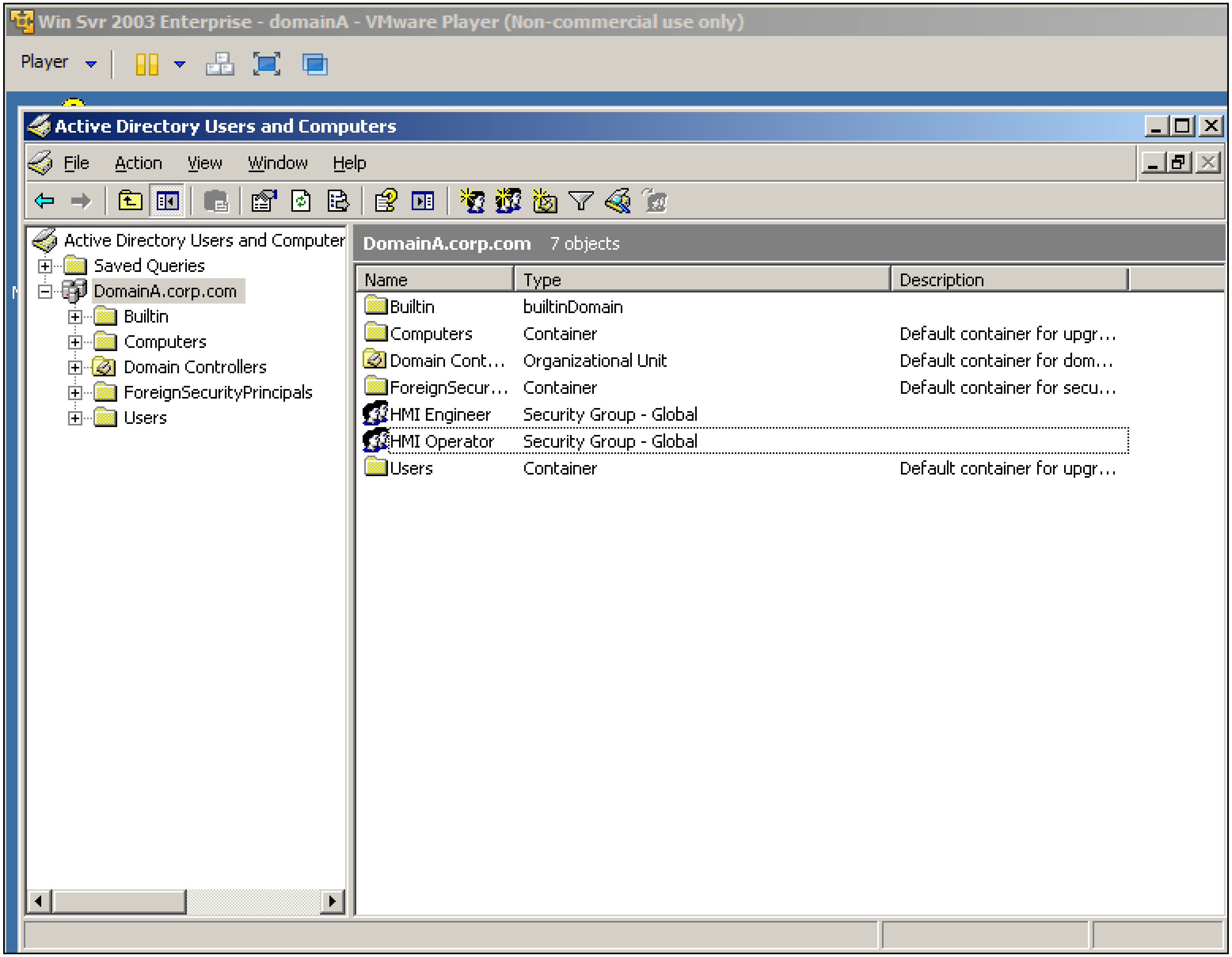
To improve the security of this external trust, security identifier (SID) filtering is enabled. For more information about SID filtering, see Securing external trusts.

FIGURE 1: DOMAIN TRUST SETTINGS

- Ensure the direction of the trust is **Two-way**.
- Authentication is **Domain-wide authentication**.
- Click **Validate** to validate the trust.

Create Security Groups on Both Machines for the Users

Create **Security Groups** on each Domain to group the users. This security group is used in the System Platform security roles configuration. Assign the users to their respective security groups.

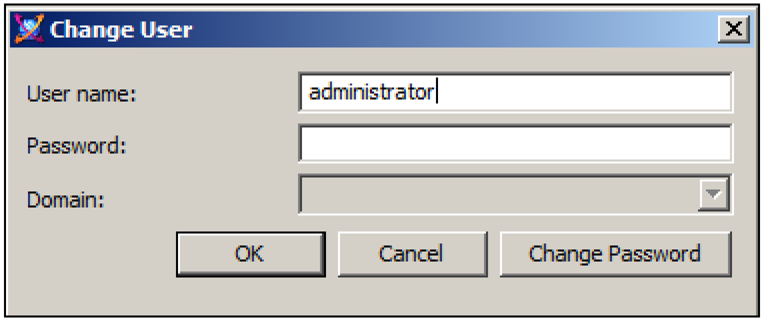

Win Svr 2003 Enterprise - domainA - VMware Player (Non-commercial use only)
Player
Active Directory Users and Computers
File
Action
View
Window
Help
Active Directory Users and Computer
Saved Queries
DomainA.corp.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
DomainA.corp.com 7 objects

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for upgr…
Domain Cont…	Organizational Unit	Default container for dom…
ForeignSecur…	Container	Default container for secu…
HMI Engineer	Security Group - Global	
HMI Operator	Security Group - Global	
Users	Container	Default container for upgr…

Figure 2: HMI Engineer and HMI Operator Users in the System PlaTform Security Groups

System Platform Security - OS Group Base

By default, new Galaxy is created without security. When you configure the security to use **OS Group Base** for the first time, IDE automatically logs out and prompts you to log back on. Since nothing has been configured, log on with the default built-in **Administrator** account with no password.



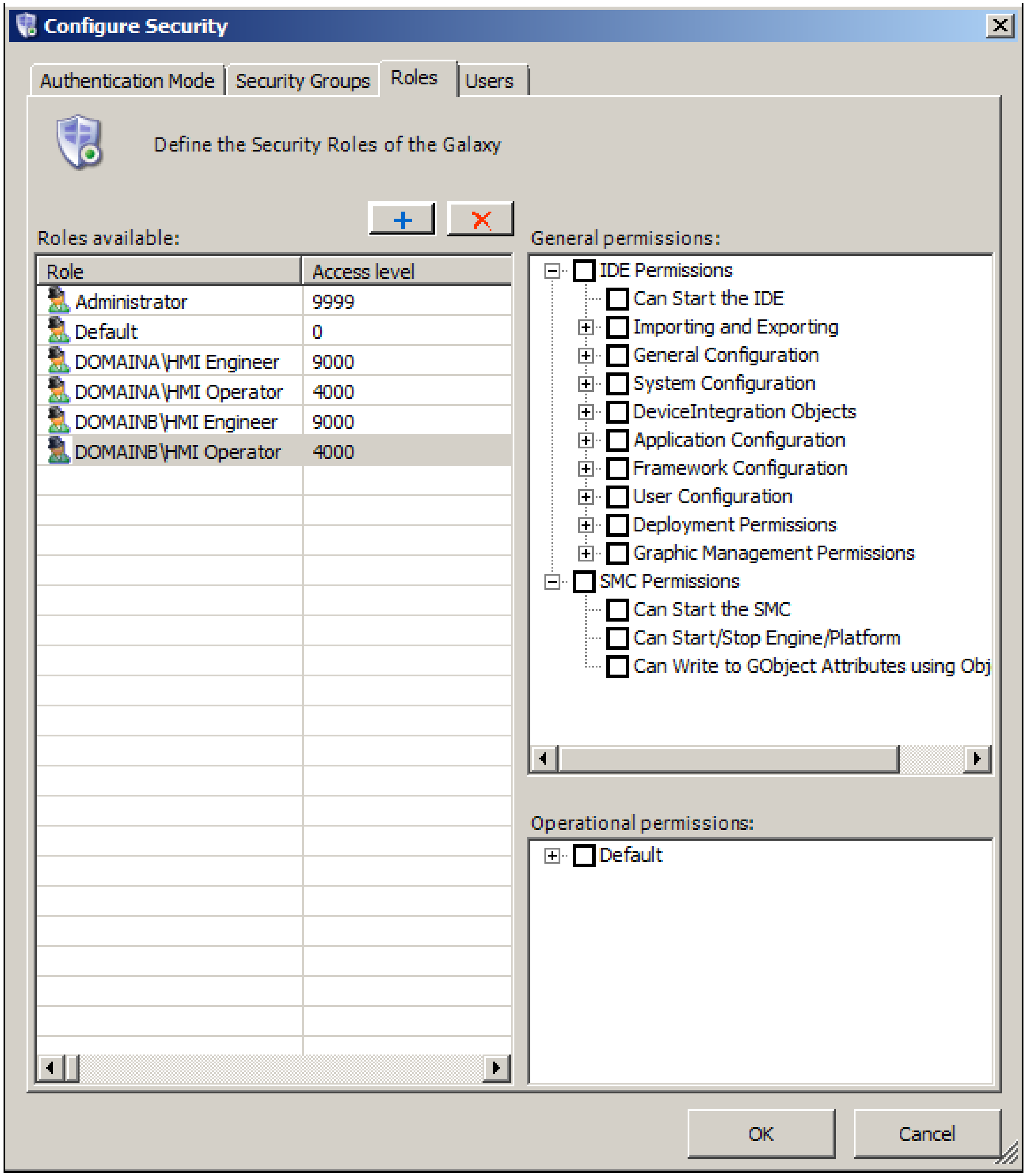
User name: administrator

Password:

Domain:

FIGURE 3: ADMINISTRATOR ACCOUNT WITHOUT PASSWORD

- Open the security configuration and click the **Roles** tab. Import the security groups created on both domains and configure their permission as required. All users will also be in the **Default** role so no permission should be granted for that role.



Define the Security Roles of the Galaxy

Roles available:

Role	Access level
Administrator	9999
Default	0
DOMAINA\HMI Engineer	9000
DOMAINA\HMI Operator	4000
DOMAINB\HMI Engineer	9000
DOMAINB\HMI Operator	4000

General permissions:

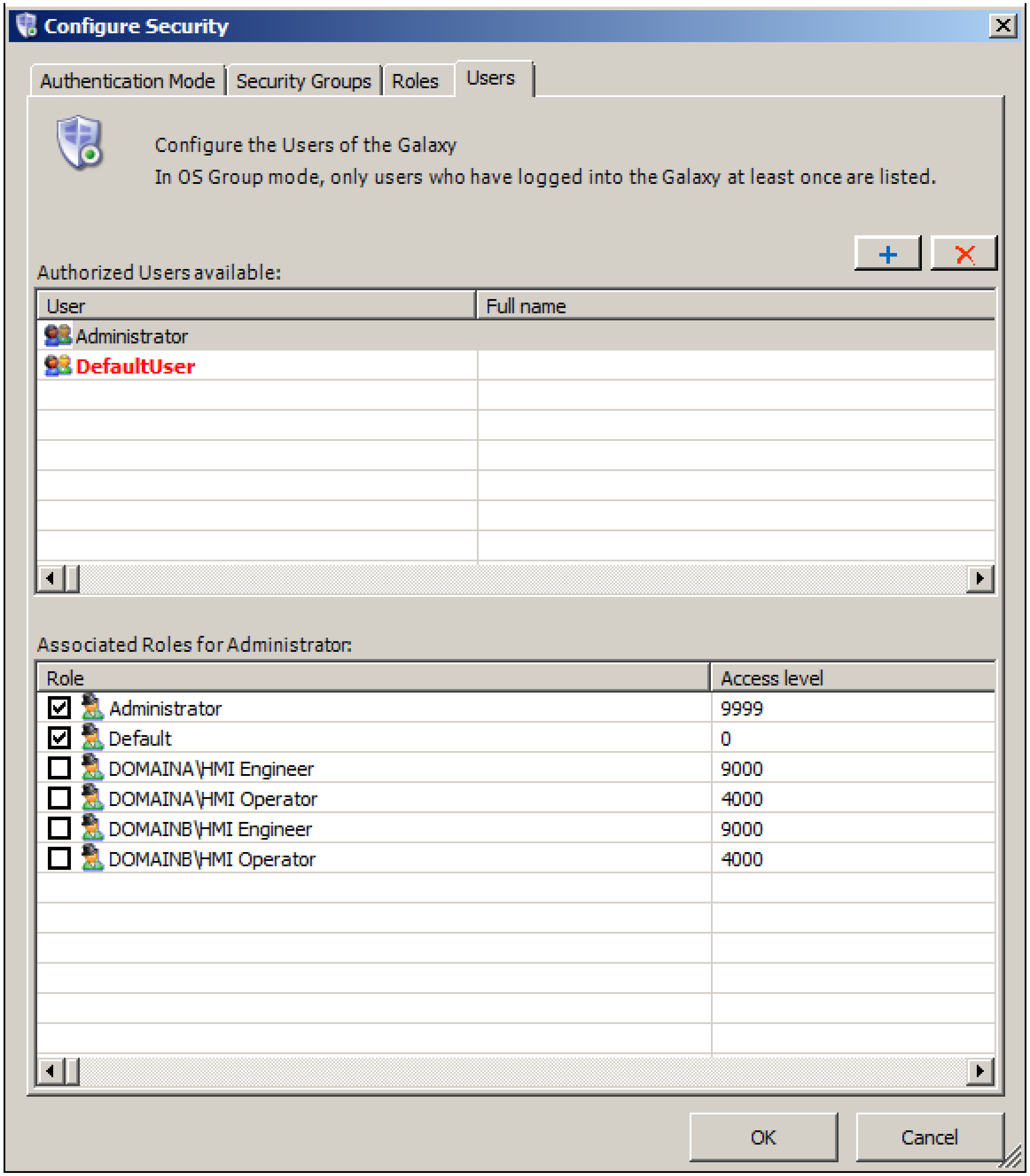
- ☐ IDE Permissions
  - ☐ Can Start the IDE
  - ☐ Importing and Exporting
  - ☐ General Configuration
  - ☐ System Configuration
  - ☐ DeviceIntegration Objects
  - ☐ Application Configuration
  - ☐ Framework Configuration
  - ☐ User Configuration
  - ☐ Deployment Permissions
  - ☐ Graphic Management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

Operational permissions:

- ☐ Default

Figure 4: Default Role Assignment

On the **Users** tab, you will not see any user until they have physically logged on to the Operating System and to the IDE.



Configure the Users of the Galaxy
In OS Group mode, only users who have logged into the Galaxy at least once are listed.

Authorized Users available:

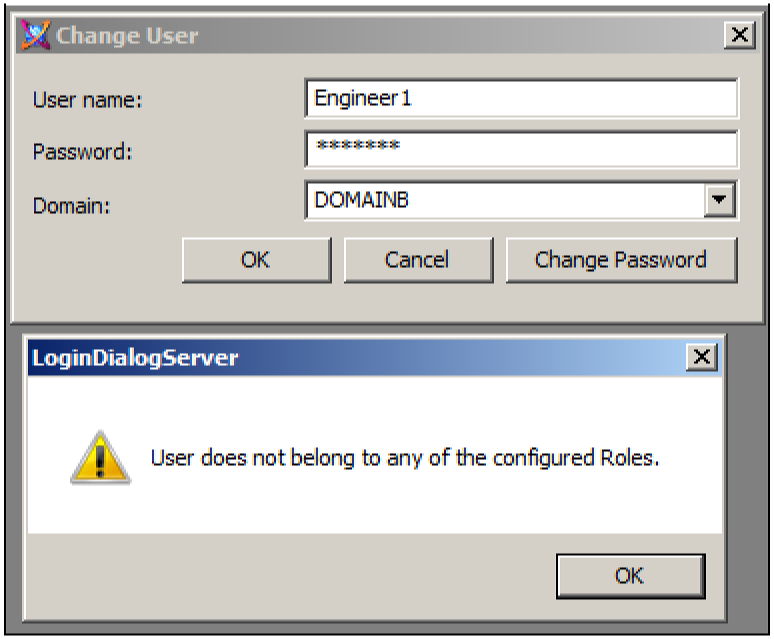
User	Full name
Administrator	
DefaultUser	

Associated Roles for Administrator:

Role	Access level
☑ Administrator	9999
☑ Default	0
□ DOMAINA\HMI Engineer	9000
□ DOMAINA\HMI Operator	4000
□ DOMAINB\HMI Engineer	9000
□ DOMAINB\HMI Operator	4000

Figure 5: Users Tab

You will not be able to log on to IDE with that user until they have physically logged on to the Operating System of the IDE node.



User name: Engineer1

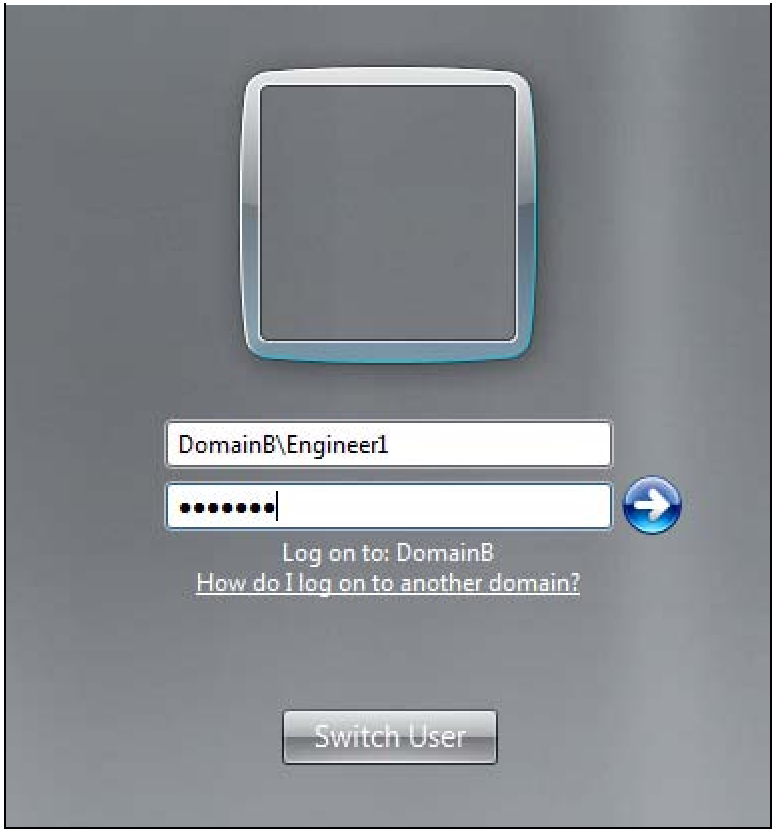
Password: ********

Domain: DOMAINB

User does not belong to any of the configured Roles.

Figure 6: User Doesn't Exist Until They Log On to the IDE Node

Log out of the Operating System and log in with the user's account. Start IDE and login with the user.



DomainB\Engineer1

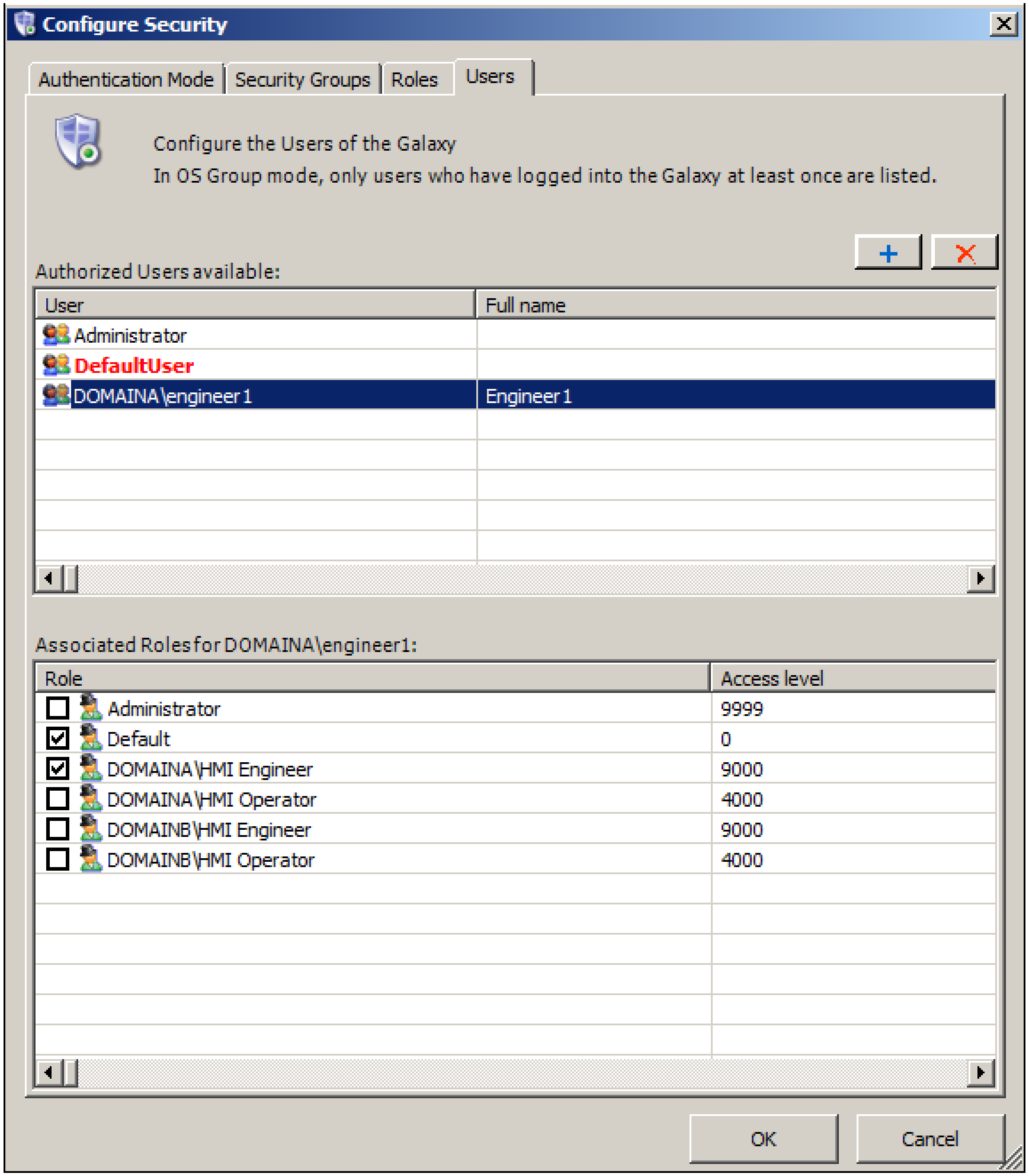
•••••••

Log on to: DomainB

FIGURE 7: LOG ON USING THE USER ACCOUNT

Open **Security Configuration -> Users.** You will now see the user in the list. Check that the user is ticked against the correct role.

Note: All users will always be in the **Default** role so no permission should be given to the **Default** role.



Configure the Users of the Galaxy
In OS Group mode, only users who have logged into the Galaxy at least once are listed.

Authorized Users available:

User	Full name
Administrator	
DefaultUser	
DOMAINA\engineer1	Engineer1

Associated Roles for DOMAINA\engineer1:

Role	Access level
□ Administrator	9999
☑ Default	0
☑ DOMAINA\HMI Engineer	9000
□ DOMAINA\HMI Operator	4000
□ DOMAINB\HMI Engineer	9000
□ DOMAINB\HMI Operator	4000

Figure 8: Only Users that Log In are Shown Here

Configure InTouch Security

The security type on the Managed Application Intouch should be **ArchestrA.**

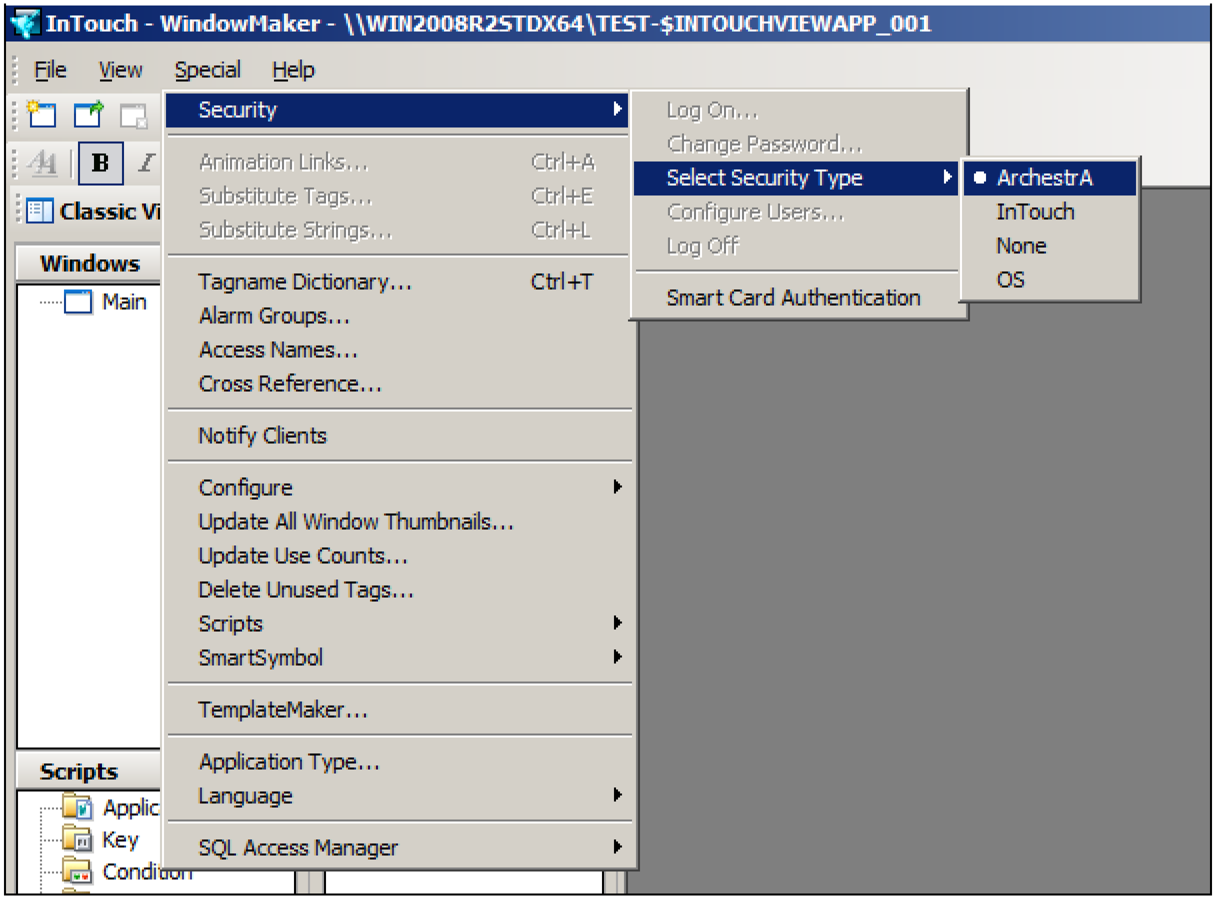
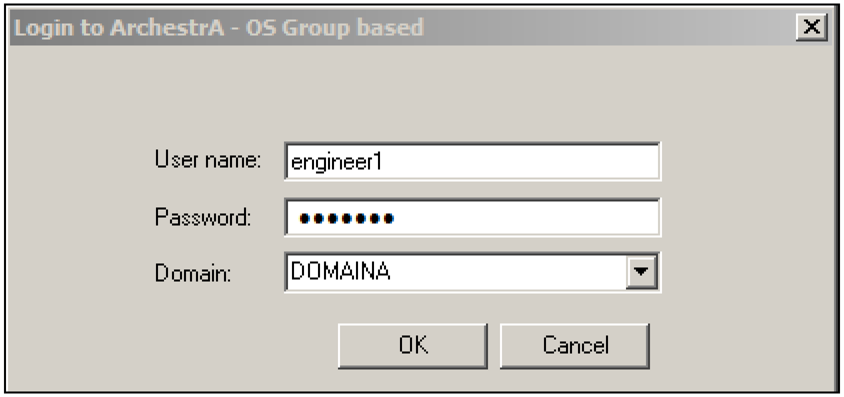


Figure 9: ArchestrA Security Type

Now you can able to log on to WindowViewer with the Domain user name.


Login to ArchestrA - OS Group based

User name: engineer1

Password: •••••••

Domain: DOMAINA

Figure 10: Log In with InTouch

M. Ang

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