NWC OT Cybersecurity SCADA Application Minimum Baseline Security Standard Appendix

National Water Company (NWC), KSA

SCADA/OT Information Security Implementation Project

Document Number:	A01001045-MBSS-SCADA-APP
Document Title:	NWC OT Cybersecurity NWC SCADA Application Minimum Baseline Security Standard Appendix
Document Version:	0
NWC Contract No.:	101200487
[atm] PO Ref.:	ATMPO2020-034

1400 Broadfield Blvd Suite 200 Houston TX, 77084
Tel: +1 832 386 5593 | Fax: +1 832 201 0337
Email: sales@acetsolutions.com |
URL: www.acetsolutions.com

NOTES AND COPYRIGHTS

Information contained herein is for the sole use of the customer (NWC) receiving this document. Acceptance of the document by the customer constitutes agreement by the customer & ACET Solutions that either party shall not disclose confidential information to any third party and shall not transmit any documents or copies thereof containing confidential information to any third party except as may by authorized in writing by NWC & ACET Solutions.

NWC has contracted this project to [atm] under contract number 101200487. ACET Solutions is the technical consultant of [atm] responsible for planning and execution of this project. All references to ACET Solutions in this document should be construed as [atm]/ACET Solutions for contractual purpose. Acceptance of this deliverable by NWC shall meet the requirements of the respective deliverable under NWC contract number 101200487.

Questions or comment regarding this deliverable should be directed to the ACET Solutions Project Director.

ACET Solutions LLC
1400 Broadfield Blvd Suite 200
Houston TX, 77084
Email: sales@acetsolutions.com | URL: www.acetsolutions.com

APPROVALS

Name	Company	Signature	Date
Mubarik Mustafa (Project Director)	ACET Solutions		
Abdulhadi G. Alshammari (Project Manager)	NWC		
Ahmed I. Almutairi (Project Sponsor)	NWC		

REVISION HISTORY

Rev No.	Date	Author	Checked By	Approved By	Comments
00	February 17, 2022	MA	SK	MM	Issued For Approval

REFERENCE DOCUMENTS

S/N	Application	Title
1	Galaxy	System Platform 2017 Update 3 Getting Started Guide
2	Galaxy	Wonderware Application Server User’s Guide
3	Galaxy	Galaxy Security
4	Galaxy	Galaxy Database Manager User Guide
5	Galaxy	Aveva System Platform Installation Guide
6	Galaxy	
7	Galaxy	
8	Archestra	Aveva Archestra Protocols User Guide
9	Archestra	
10	Archestra	
11	Archestra	
12	Archestra	
13	InTouch	Intouch Security Modes
14	InTouch	Preventing users from accessing InTouch Window
15	InTouch	InTouch Security
16	InTouch	Configuring Users
17	InTouch	InTouch HMI Application Management
18	InTouch	Aveva System Platform Installation Guide
19	InTouch	
20	InTouch	
21	InTouch	
22	Historian	Managing Historian Security
23	Historian	Aveva System Platform Installation Guide
24	Historian	
25	Historian	
26	Historian	

Table 1: Reference Documents

ACRONYMS

Acronyms	Meaning
ACL	Access Control Lists
AD	Active Directory
ADC	Additional Domain Controller
CA	Certificate Authority
CIP	Critical Infrastructure Protection
DCS	Distributed Control System
DMZ	Demilitarized Zone
DNS	Domain Name System
ECC	Essential Cybersecurity Controls
ePO	ePolicy Orchestrator
EPP	End Point Protection
GPS	Global Positioning System
HMI	Human Machine Interface
HSE	Health, Safety, And Environmental
ICS	Industrial Control System
IDS	Intrusion detection System
IPS	Intrusion Prevention System
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information Technology
LDAP	Light Weight Directory Access Protocol
MBSS	Minimum Baseline Security Standards
MFA	Multi-factor Authentication
NIST	U.S. National Institute of Standards and Technology
NWC	National Water Company
OT	Operational Technology
PLC	Programmable Logic Controller
RDS	Remote Desktop Services
SCADA	Supervisory Control and Data Acquisition
VM	Virtual Machine
VPN	Virtual Private Network

Table of Contents

1. DOCUMENT PURPOSE

This document is an appendix for Minimum Baseline Security Standards for SCADA Applications.

2. Appendix I- Schneider Aveva Platform System Galaxy Security

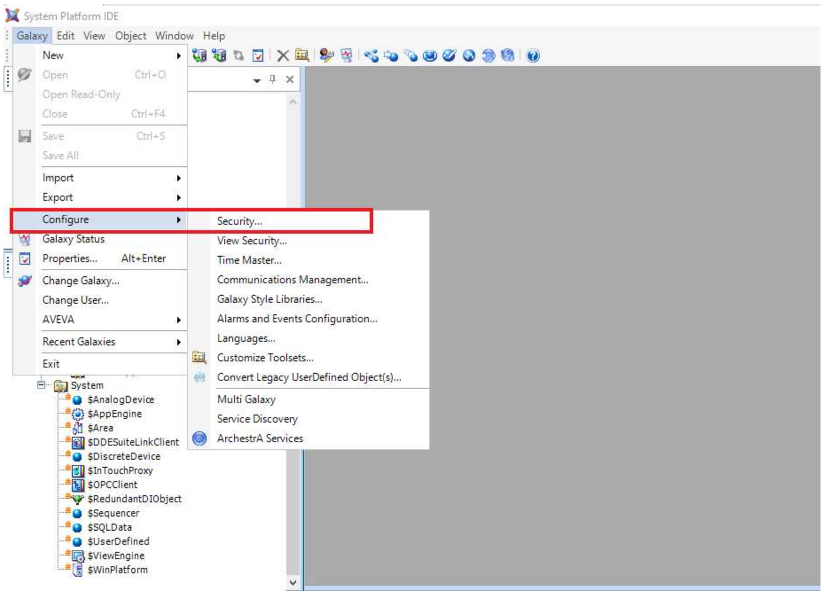
2.1 SECURITY CONFIGURATION

1. Modify Security Model to configure security in the application.

   Refer to Table 1: Reference Documents S/N 2 Page 359

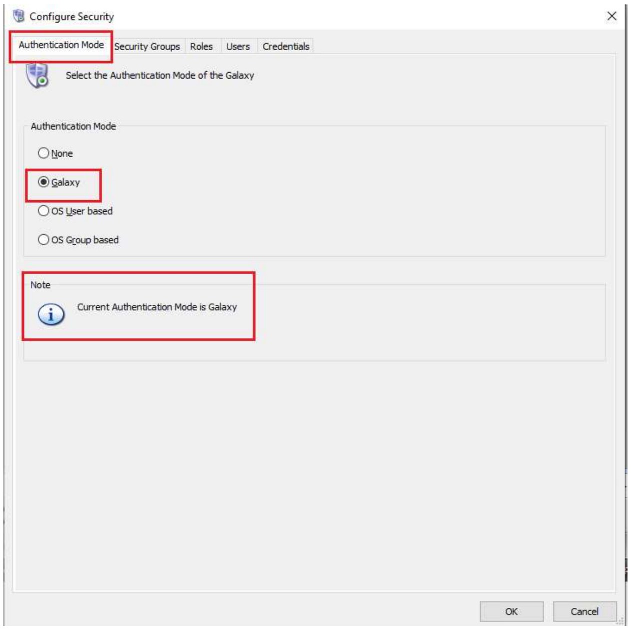
Following are the steps to configure security model in Galaxy:

Step 1: Select Galaxy>>Configure>>Security



Step 2: Select Authentication Mode from the Window that appears

Refer to Table 1: Reference Documents S/N 2, Page 360



Configure Security

Select the Authentication Mode of the Galaxy

Authentication Mode

○ None

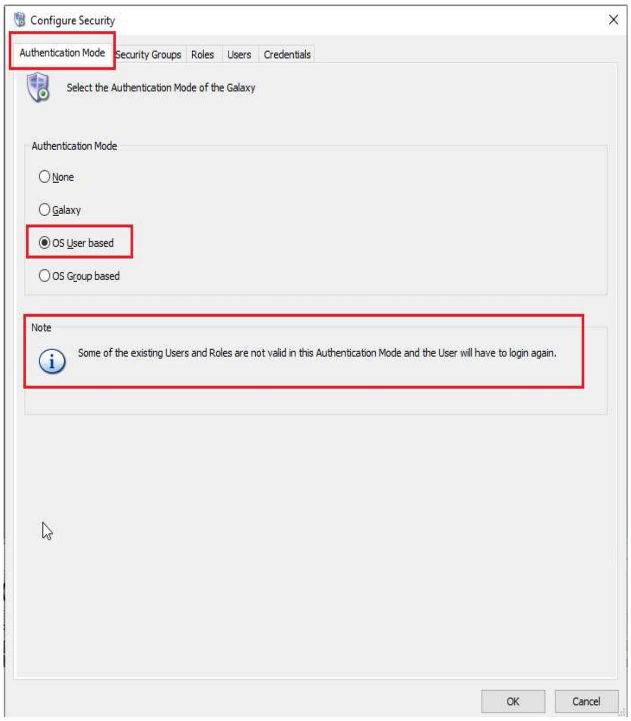
● Galaxy

○ OS User based

○ OS Group based

Note

Current Authentication Mode is Galaxy



Configure Security

Select the Authentication Mode of the Galaxy

Authentication Mode

○ None

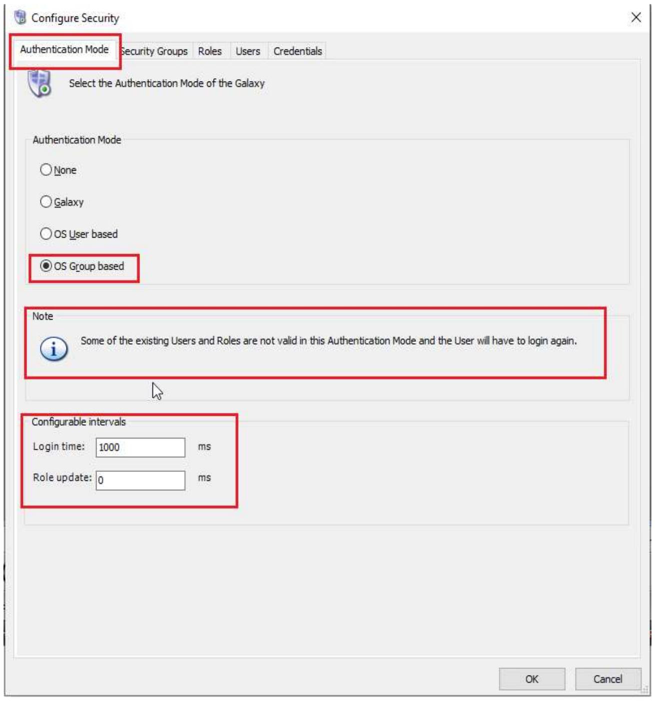
○ Galaxy

● OS User based

○ OS Group based

Note

Some of the existing Users and Roles are not valid in this Authentication Mode and the User will have to login again.



Select the Authentication Mode of the Galaxy

Authentication Mode

○ None

○ Galaxy

○ OS User based

● OS Group based

Note

Some of the existing Users and Roles are not valid in this Authentication Mode and the User will have to login again.

Configurable intervals

Login time: 1000 ms

Role update: 0 ms

2.2 SECURITY GROUPS

1. Acknowledge Alarms

   Refer to Table 1: Reference Documents S/N 2 Page 356

2. Change the attributes values with varying security modes (Configure, Operate, Tune)

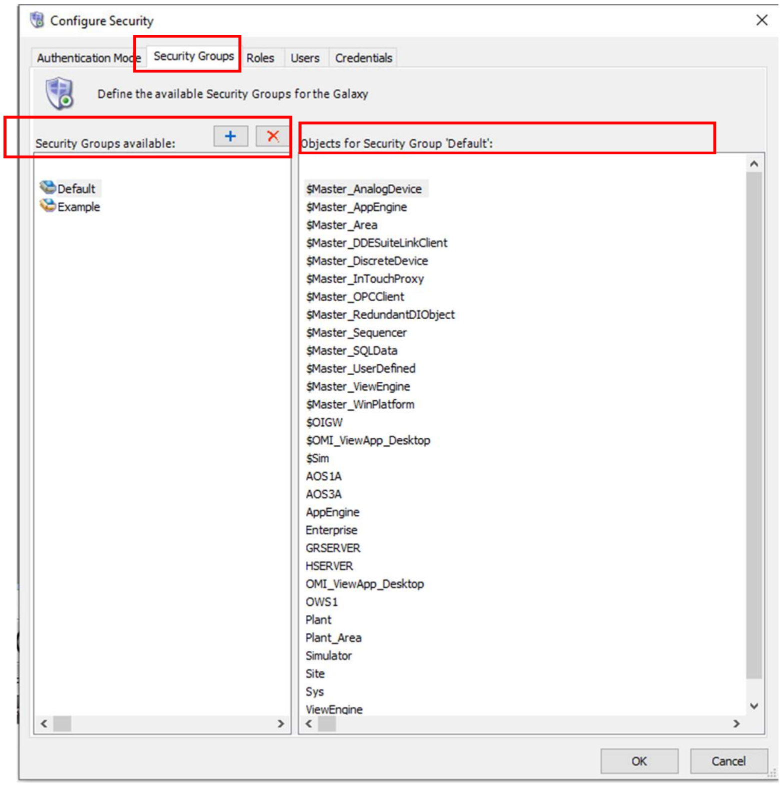
   Refer to Table 1: Reference Documents S/N 2 Page 356

3. Confirm writes to attributes that require Verified Write

   Refer to Table 1: Reference Documents S/N 2 Page 356

Following are the steps to create security groups in Galaxy application:

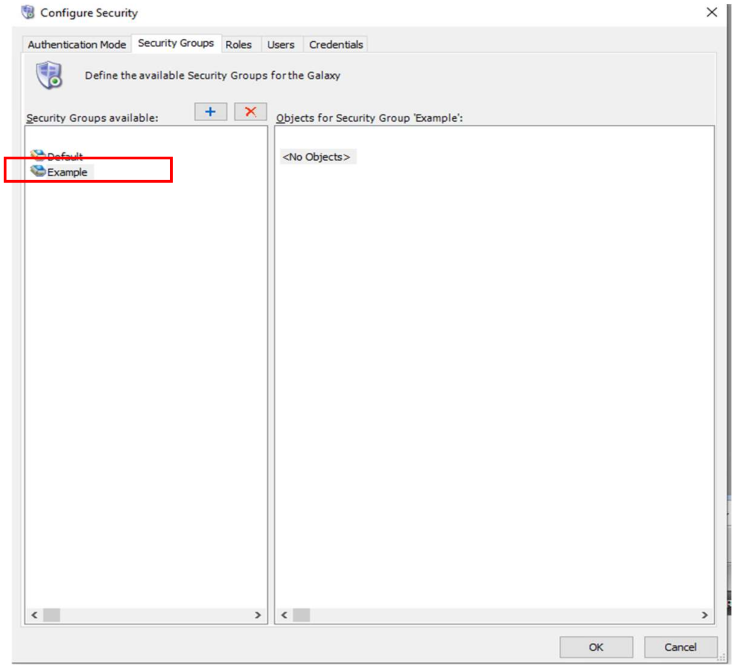
Select Galaxy>> Configure>> Security



Configure Security
Authentication Mode
Security Groups
Roles
Users
Credentials
Define the available Security Groups for the Galaxy
Security Groups available:
Objects for Security Group 'Default':
OK
Cancel

Default
Example

$Master_AnalogDevice
$Master_AppEngine
$Master_Area
$Master_DDESuiteLinkClient
$Master_DiscreteDevice
$Master_InTouchProxy
$Master_OPCClient
$Master_RedundantDIObject
$Master_Sequencer
$Master_SQLData
$Master_UserDefined
$Master_ViewEngine
$Master_WinPlatform
$OIGW
$OMI_ViewApp_Desktop
$Sim
AOS1A
AOS3A
AppEngine
Enterprise
GRSERVER
HSERVER
OMI_ViewApp_Desktop
OWS1
Plant
Plant_Area
Simulator
Site
Sys
ViewEngine



Configure Security
Authentication Mode
Security Groups
Roles
Users
Credentials
Define the available Security Groups for the Galaxy
Security Groups available:
Objects for Security Group 'Example':
OK
Cancel

Default
Example

<No Objects>

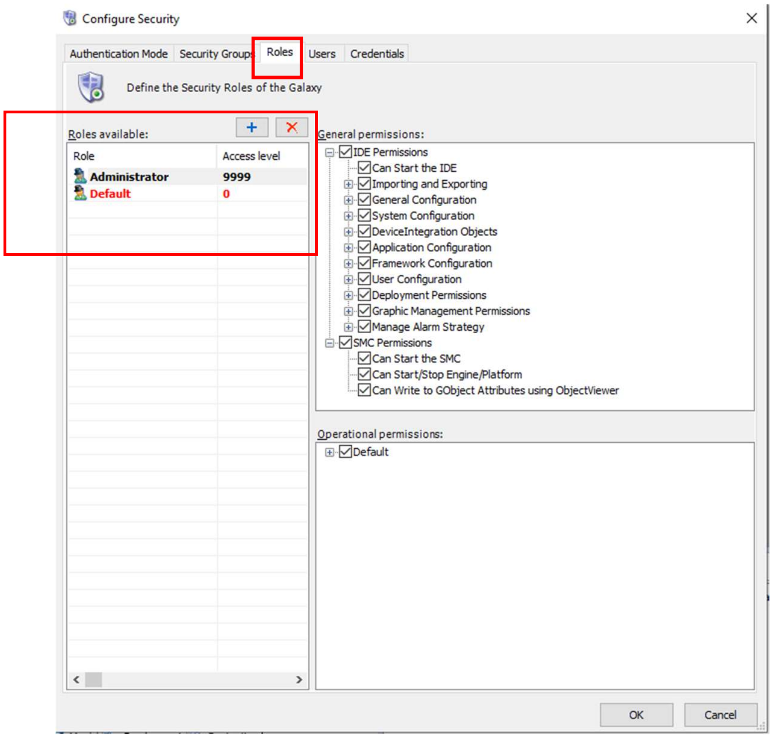
2.3 ROLE BASED ACCESS

1. Set Role based access for ensuring security of application

   Refer to Table 1: Reference Documents S/N 2 Page 357

Following are the steps followed for defining role-based access in application:

Step 1: Select Galaxy>>Configure>>Security>>Roles



Define the Security Roles of the Galaxy

Role	Access level
Administrator	**9999**
Default	**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
  - ☑ Manage Alarm Strategy
- ☑ SMC Permissions
  - ☑ Can Start the SMC
  - ☑ Can Start/Stop Engine/Platform
  - ☑ Can Write to GObject Attributes using ObjectViewer

Operational permissions:

- ☑ Default

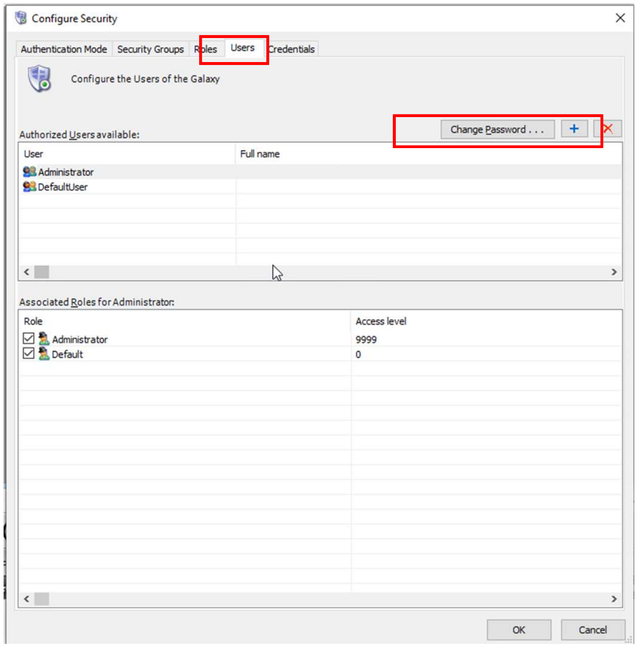
Step 2: Define general and operational permissions for the roles.

Refer to Table 1: Reference Documents S/N 2 Page 357

2.4 USER BASED ACCESS

1. Enable Password for Users

   Refer to Table 1: Reference Documents S/N 2 Page 358



Configure the Users of the Galaxy

Authorized Users available:

User	Full name
Administrator	
DefaultUser	

Associated Roles for Administrator:

Role	Access level
☑ Administrator	9999
☑ Default	0

3. Appendix II- Schneider Aveva Platform System SQL Server Security

1. Enable the SQL Server Security Mode.

   - Legacy Mode
   - Enhanced Security Mode

Legacy Mode	Enhanced Security Mode
Authenticated users have sysadmin privileges.	Default mode, removes the sysadmin privileges
Not restricted from any SQL Server activity	Retains minimum privileges needed for normal operations
Preferred option if user will be frequently restoring galaxies created with previous application server	Users need to provide SQL sysadmin user credentials when restoring galaxy created with previous application server

   Refer to Table 1: Reference Documents S/N 5, Page 74

2. Set the suitable authentication type

   - Windows Authentication
   - SQL Server Authentication

Windows Authentication	SQL Server Authentication
User can login with Windows credentials and doesn't need to provide separate SQL credentials	Independent of Windows Users Account
Security is integrated with Windows	New Logins are created, Credentials are stored in syslogins table

   Refer to Table 1: Reference Documents S/N 5, Page 74

3. Manage SQL sysadmin login credentials (Username and Password)

   Refer to Table 1: Reference Documents S/N 5, Page 74

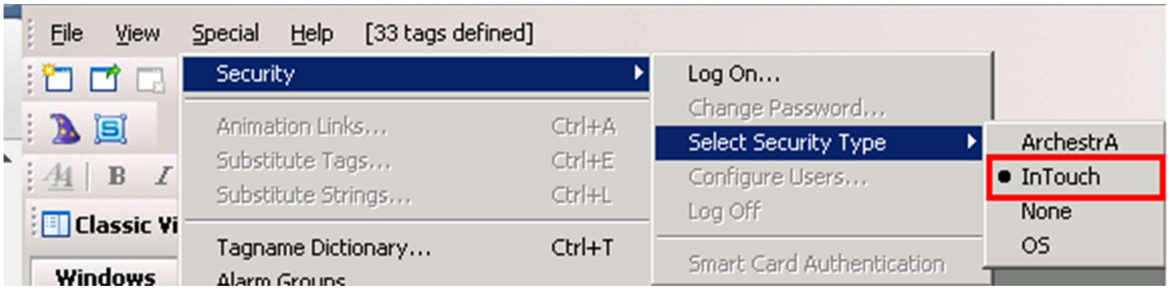
4. Appendix IV- Schneider Aveva System Platform Intouch Security Configuration

1. Configure Application Security Model

   Refer to Table 1: Reference Documents S/N 13

Following are the steps followed to configure application security model:

Step 1: Select Special>>Security>>Select Security Type>>InTouch



2. Set Credentials for the security Model

   Refer to Table 1: Reference Documents S/N 13

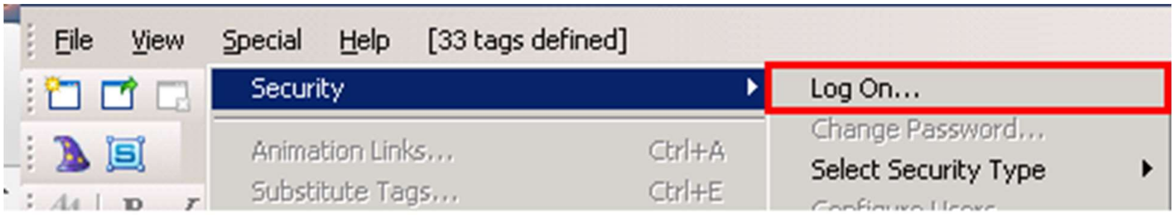
3. Managing Users and Setting their authorization levels

   Refer to Table 1: Reference Documents S/N 16, S/N 17 Page 147-155

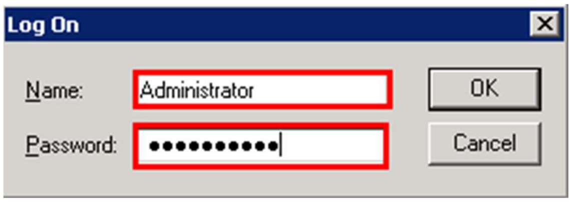
Following are the steps to configure users in Intouch Application:

Step 1: Log on to the security option in InTouch security mode.

Select Special>>Security>>Log On



Step 2: Enter Username and Password

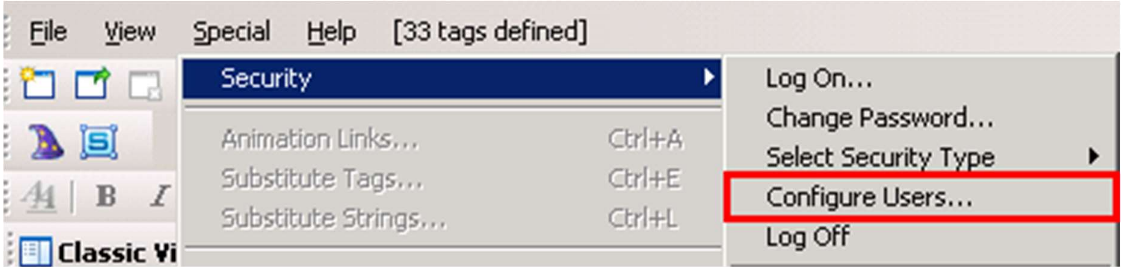

Log On

Name: Administrator

Password: ●●●●●●●●●●

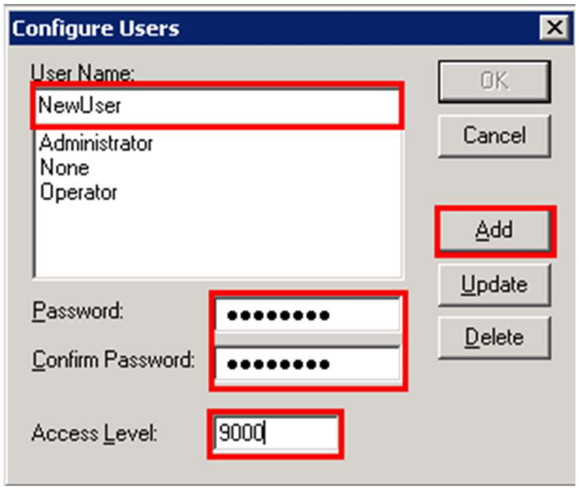
Step 3: Configure Users by selecting the option

Special>>Security>>Configure Users



Step 4: Assign Access level to Passwords to the users

Refer to Table 1: Reference Documents S/N 13, S/N 2 Page 369, S/N 17 Page 148-155



User Name: NewUser

Administrator
None
Operator

Password: ●●●●●●●●

Confirm Password: ●●●●●●●●

Access Level: 9000

4. Set an in-activity time-out period

   Refer to Table 1: Reference Documents S/N 17 Page 126-129

5. Lock/Disable System Keys

   Refer to Table 1: Reference Documents S/N 17 Page 129-131

6. Hide Menus at run-time

   Refer to Table 1: Reference Documents S/N 17 Page 132-134

7. Enable Authentication and Authorization based security

   Refer to Table 1: Reference Documents S/N 17 Page 135-138

8. Retrieve Information about currently logged on user

   Refer to Table 1: Reference Documents S/N 17 Page 165-170

5. Appendix V- Schneider Aveva System Platform Historian Security Configuration

1. Manage Logins

    - User shall be part of Active Directory.

    Refer to Table 1: Reference Documents S/N 22, Page 167-170

2. Manage Users and Roles for Authentication and Authorization

    Refer to Table 1: Reference Documents S/N 22, Page 171-173

3. Manage Permissions for users and roles

    Refer to Table 1: Reference Documents S/N 22, Page 173-175

4. Managing Passwords

    Refer to Table 1: Reference Documents S/N 22, Page 176

ACET
SOLUTIONS

ACET Solutions LLC
1400 Broadfield Blvd Suite 200 Houston TX, 77084.
United States of America.
Tel: +1 832 386 5593 | Fax: +1 832 201 0337
sales@acetsolutions.com | www.acetsolutions.com