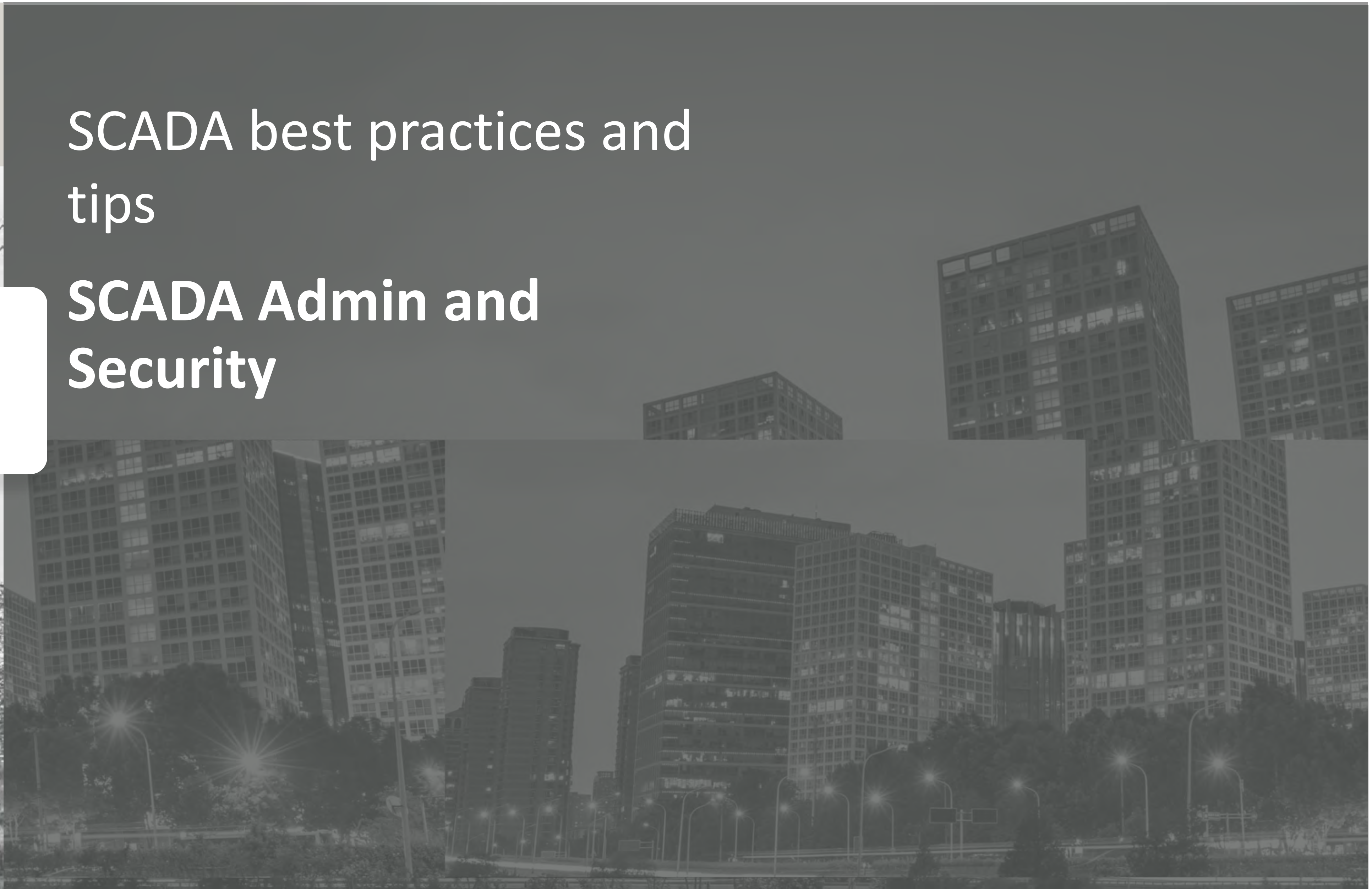
Survalent.

UC

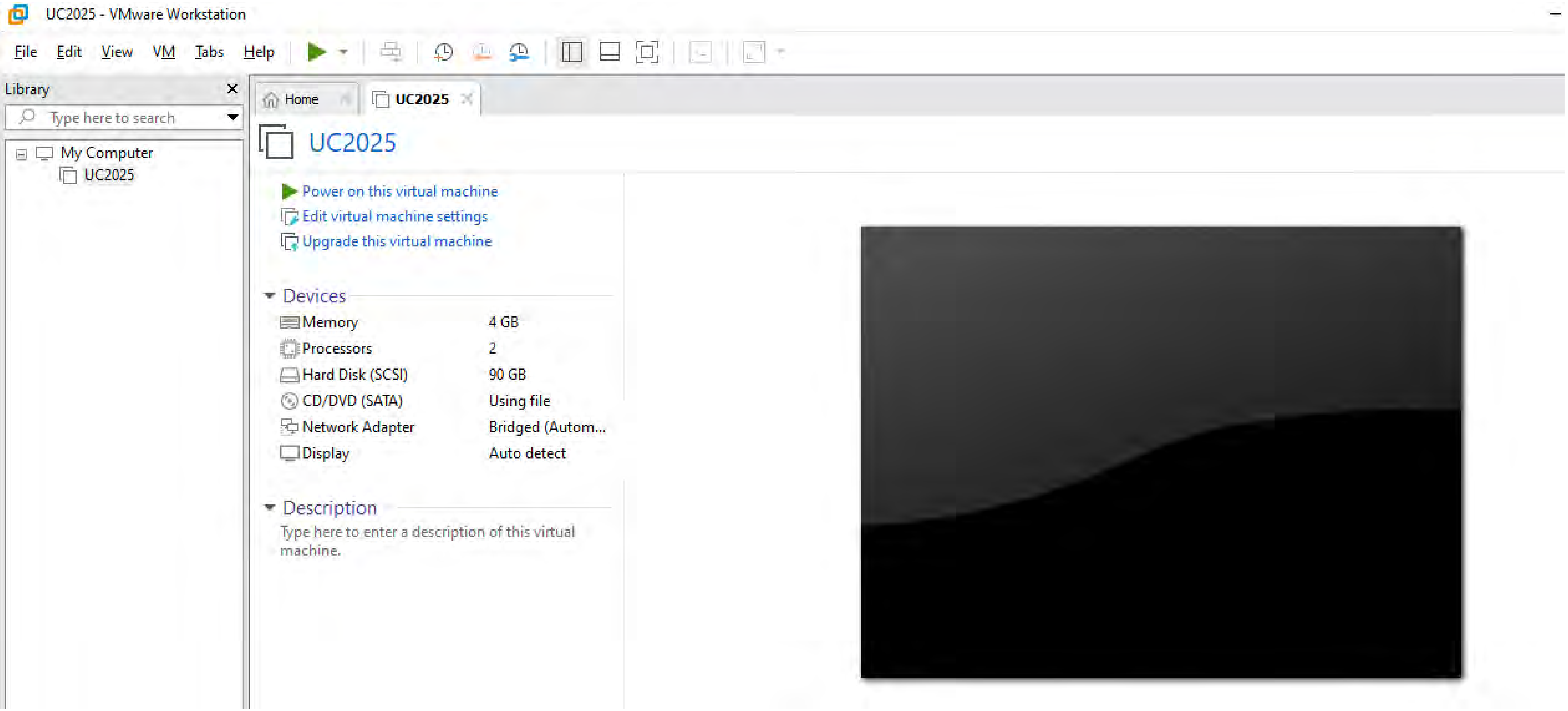
Global User Conference



SCADA best practices and tips

SCADA Admin and Security

VM...



UC2025

- Power on this virtual machine
- Edit virtual machine settings
- Upgrade this virtual machine

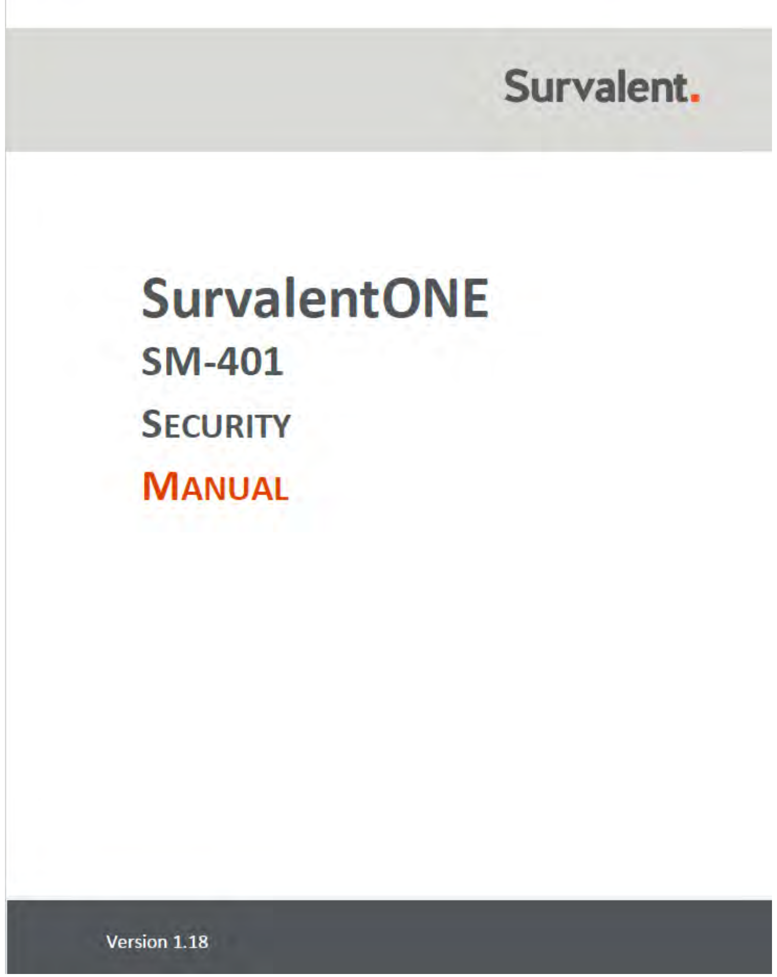
Devices

Memory	4 GB
Processors	2
Hard Disk (SCSI)	90 GB
CD/DVD (SATA)	Using file
Network Adapter	Bridged (Autom...
Display	Auto detect

Description

Type here to enter a description of this virtual machine.

Resources



Survalent.

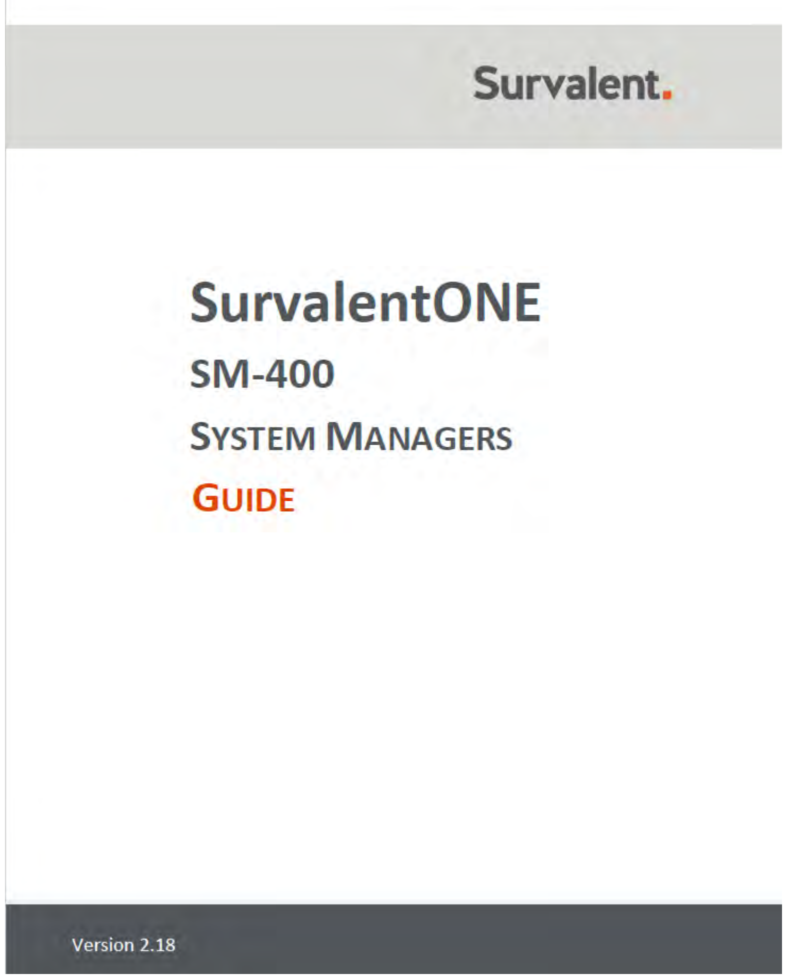
SurvalentONE

SM-401

Security

Manual

Version 1.18



Survalent.

SurvalentONE

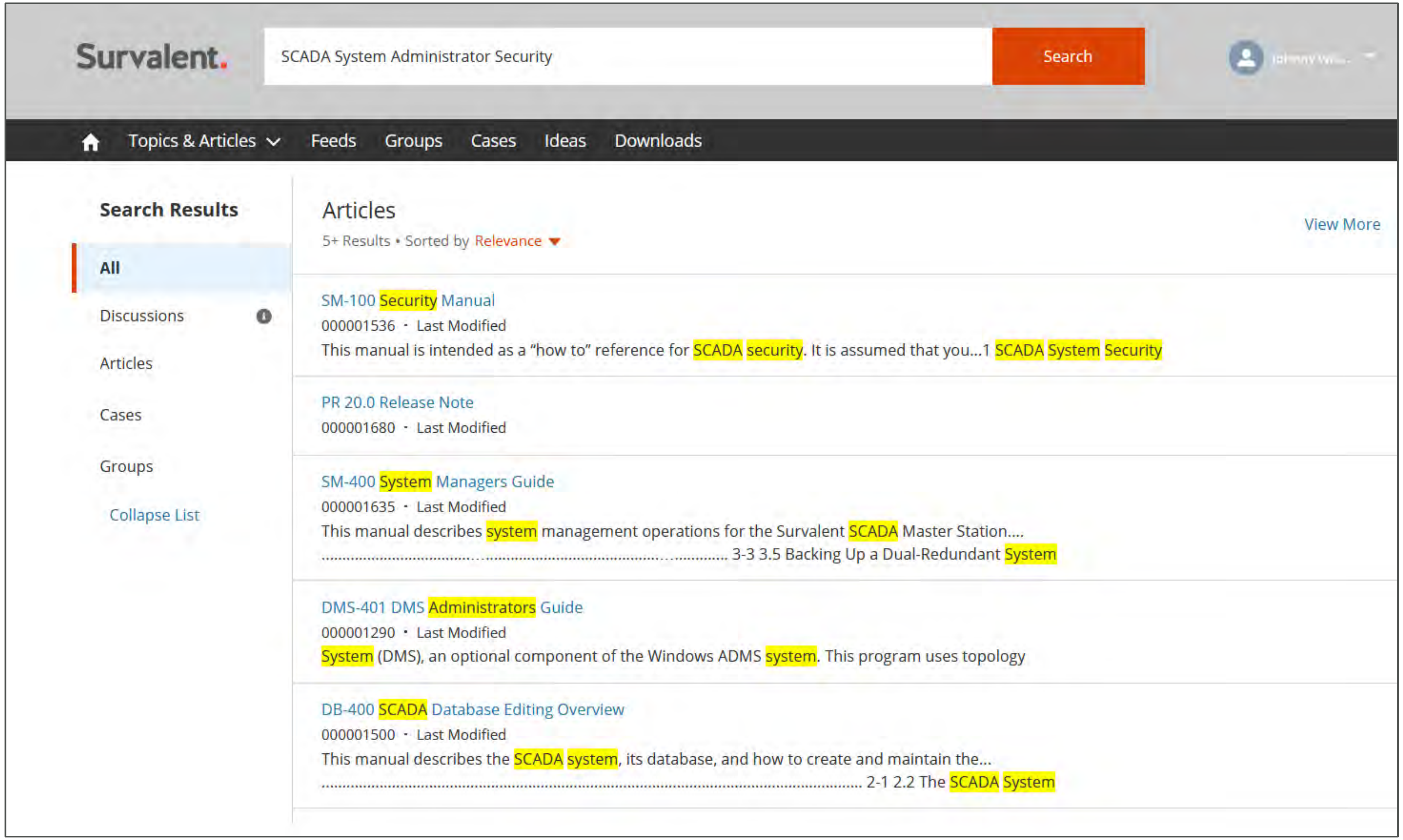
SM-400

System Managers

Guide

Version 2.18

Resources



Articles

5+ Results • Sorted by Relevance

SM-100 Security Manual
000001536 • Last Modified
This manual is intended as a “how to” reference for SCADA security. It is assumed that you...1 SCADA System Security

PR 20.0 Release Note
000001680 • Last Modified

SM-400 System Managers Guide
000001635 • Last Modified
This manual describes system management operations for the Survalent SCADA Master Station....
.... 3-3 3.5 Backing Up a Dual-Redundant System

DMS-401 DMS Administrators Guide
000001290 • Last Modified
System (DMS), an optional component of the Windows ADMS system. This program uses topology

DB-400 SCADA Database Editing Overview
000001500 • Last Modified
This manual describes the SCADA system, its database, and how to create and maintain the...
.... 2-1 2.2 The SCADA System

Table of Contents

POINT DATABASE

USER ACCESS

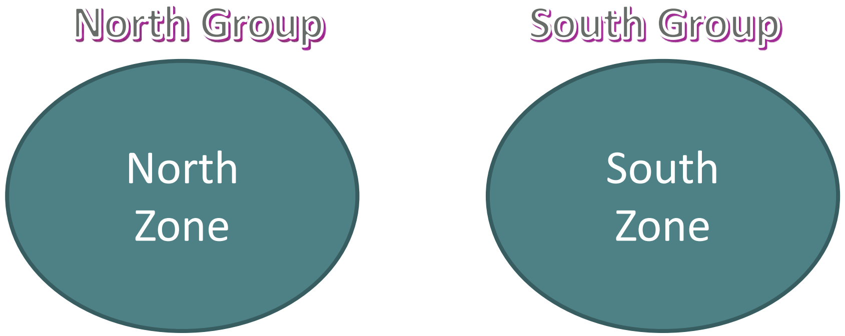
SmartVU UI

SYSTEM CONFIGURATION

ZONES

Database Points

- RECLOSER1,Mechanism3ph – North Group
- RECLOSER10,Mechanism3ph – South Group



North Group

North Zone

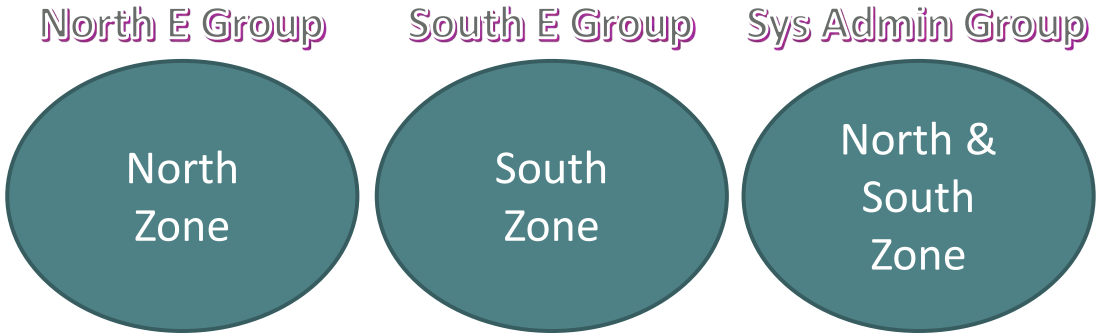
South Group

South Zone

- Points cannot be placed in zones directly
- They are placed in zone groups instead
- Common practise is to place points in fixed zone group

Users

- Ellen Ripley – North E Group
- Dorothy Gale – South E Group
- Regina George – System Admin Group



North E Group

North Zone

South E Group

South Zone

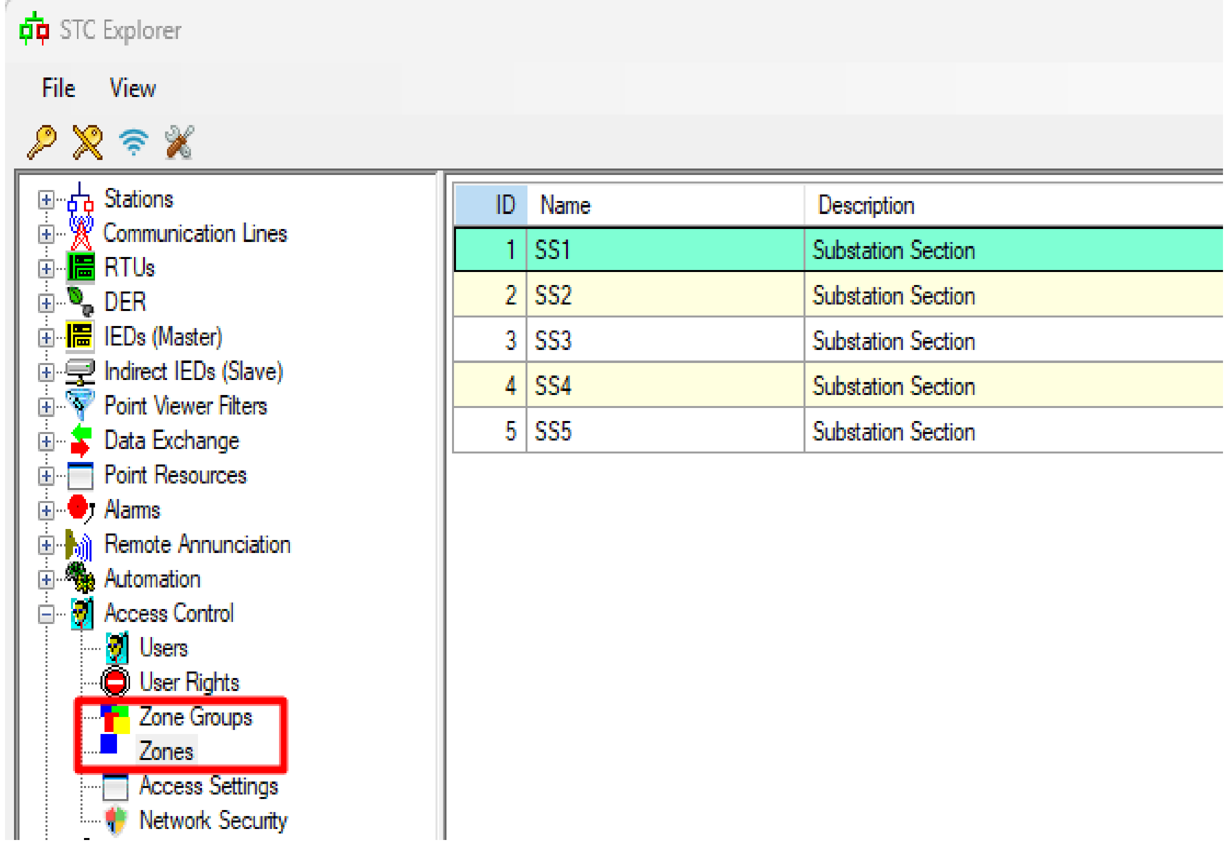
Sys Admin Group

North & South Zone

- Users cannot be placed in zones directly
- They are placed in zone groups instead
- User’s zone group changes as per requirement

ZONES

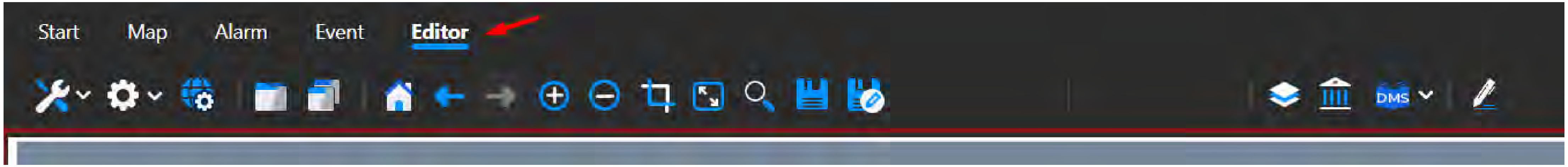
- Points or Users cannot be placed in zones directly, they are placed in Zone groups instead.
- Zones need to match across zone groups for access/control.
- Common practise is to place points in fixed zone group.
- Depending on the Zone group of the user, map layers will be hidden/shown to them in SmartVU.



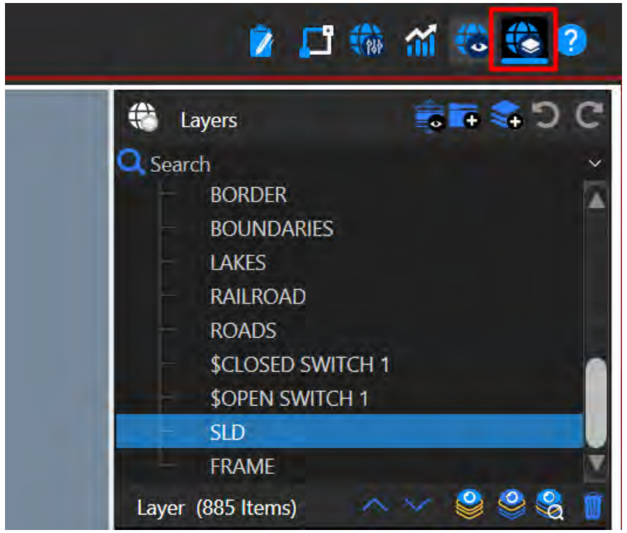
ID	Name	Description
1	SS1	Substation Section
2	SS2	Substation Section
3	SS3	Substation Section
4	SS4	Substation Section
5	SS5	Substation Section

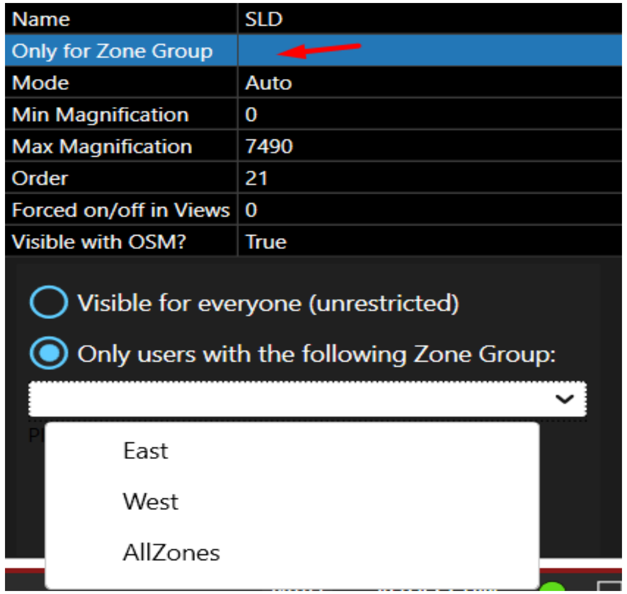
ZONES

In SmartVU, you can change the vibility of the layers depending on the zone configured for the user. This is done in editor mode:



In the layers section, there is an option to select the zone:





Name	SLD
Only for Zone Group	
Mode	Auto
Min Magnification	0
Max Magnification	7490
Order	21
Forced on/off in Views	0
Visible with OSM?	True

○ Visible for everyone (unrestricted)

● Only users with the following Zone Group:

Exercise

Create a new Zone and Zone Group

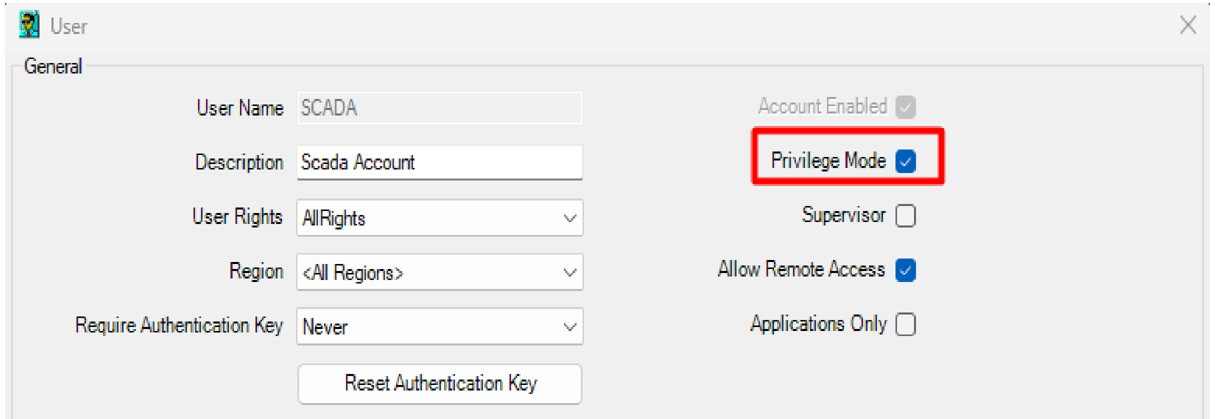
- Using STC Explorer, create:
  - New Zone
  - New Zone Group
- Using SmartVU2, create:
  - A layer that only displays for certain zone groups

Layers

- Additional layer of security other than user rights and zones.
- Commonly used for specific points in the database.
- Applies to below:
  - Control
  - Set Manual
  - Activate/Deactivate
  - Alarm Acknowledge
  - Alarm Block

Privileged Mode

User's configuration



User

General

User Name: SCADA

Description: Scada Account

User Rights: AllRights

Region: <All Regions>

Require Authentication Key: Never

Account Enabled ☑

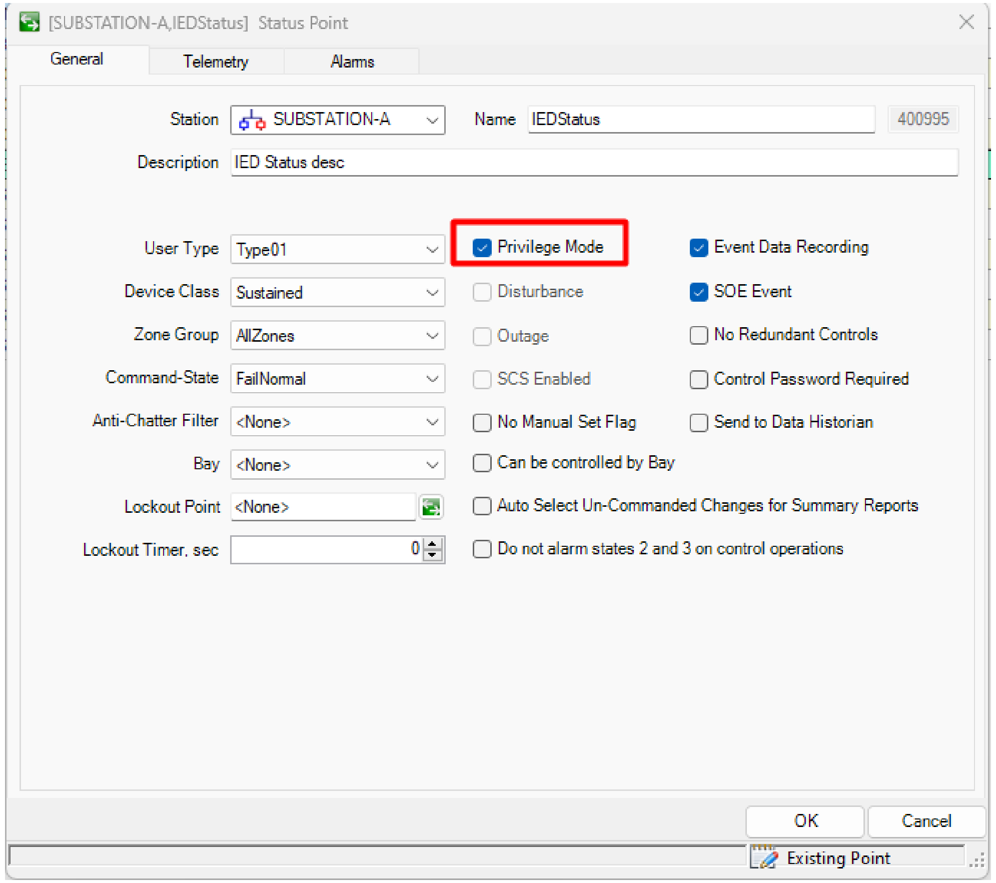
Privilege Mode ☑

Supervisor ☐

Allow Remote Access ☑

Applications Only ☐

Point's configuration



[SUBSTATION-A,IEDStatus] Status Point

Station: SUBSTATION-A

Name: IEDStatus 400995

Description: IED Status desc

User Type: Type01

Device Class: Sustained

Zone Group: AllZones

Command-State: FailNormal

Anti-Chatter Filter: <None>

Bay: <None>

Lockout Point: <None>

Lockout Timer, sec: 0

☑ Privilege Mode

☐ Disturbance

☐ Outage

☐ SCS Enabled

☐ No Manual Set Flag

☐ Can be controlled by Bay

☐ Auto Select Un-Commanded Changes for Summary Reports

☐ Do not alarm states 2 and 3 on control operations

☑ Event Data Recording

☑ SOE Event

☐ No Redundant Controls

☐ Control Password Required

☐ Send to Data Historian

Exercise

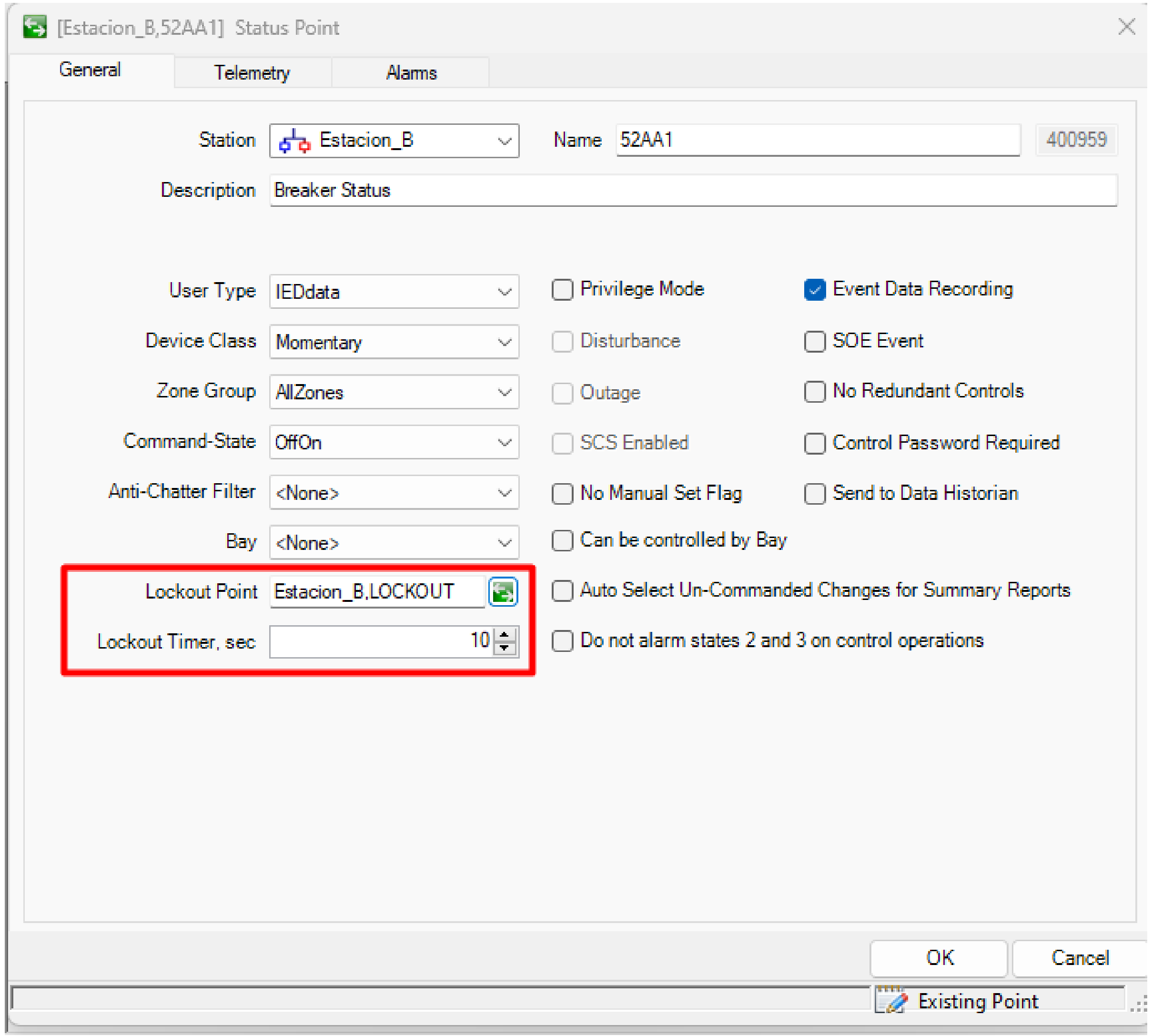
Enable privilege mode

- Using STC Explorer:
  - Edit a point and enable the privilege mode.
- Using SmartVU2:
  - Change the status of the point using control or manual set.

Lockout Point

The SCADA system contains a breaker lockout detection function. If you define an associated lockout point for a breaker, the system will maintain the lockout point as follows:

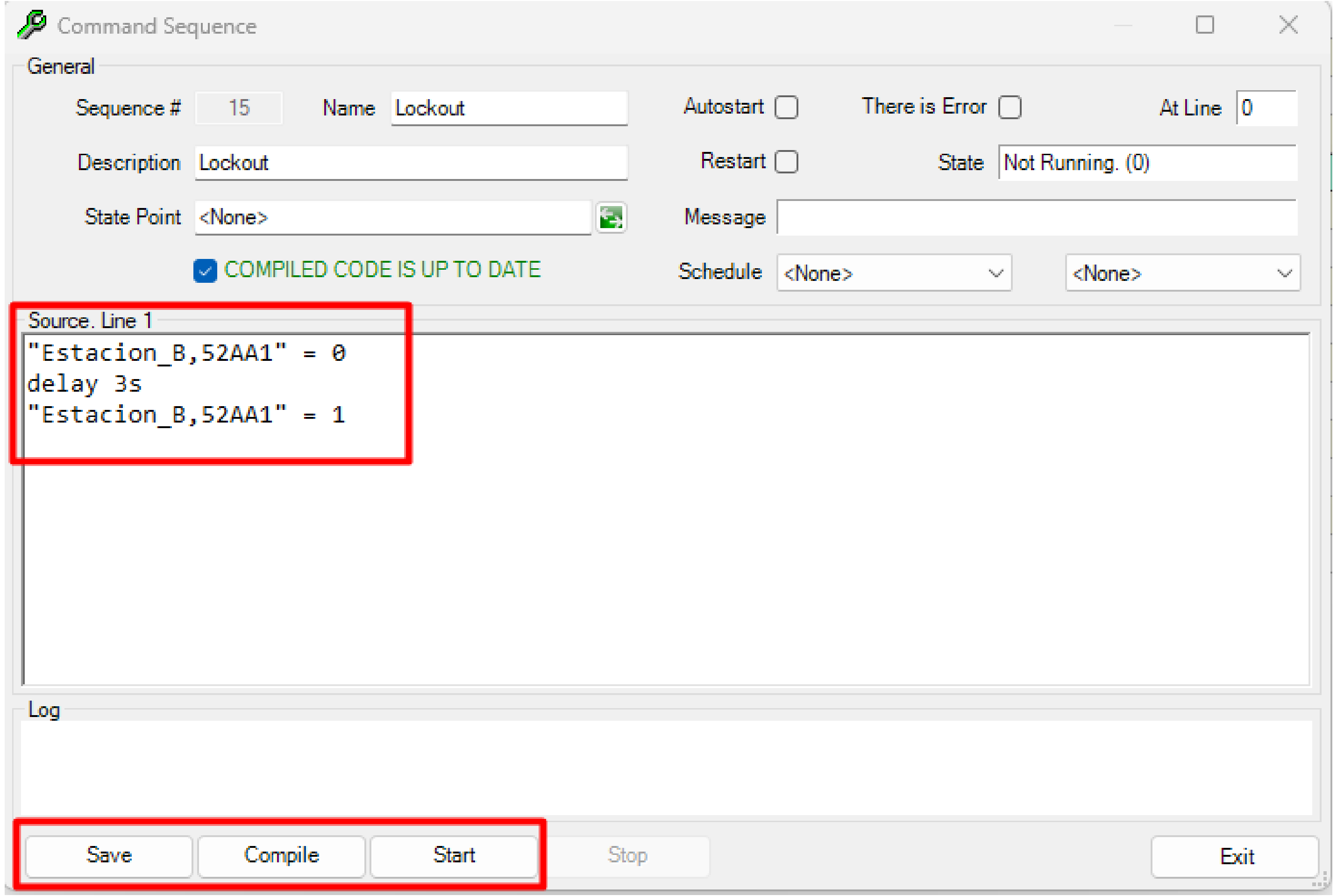
- If the breaker trips unexpectedly and remains tripped for X seconds, then the lockout point is set to state 0 (LOCKOUT)
- As soon as the breaker closes, whether it’s via control, manual set or telemetry, the lockout point is returned to state 1 (NORMAL)
- If the breaker is controlled or manually set to OPEN, nothing happens to the lockout point



[Estacion_B,52AA1] Status Point

Station	Estacion_B	Name	52AA1
			400959
Description	Breaker Status		

User Type	IEDdata	☐ Privilege Mode	☑ Event Data Recording
Device Class	Momentary	☐ Disturbance	☐ SOE Event
Zone Group	AllZones	☐ Outage	☐ No Redundant Controls
Command-State	OffOn	☐ SCS Enabled	☐ Control Password Required
Anti-Chatter Filter	<None>	☐ No Manual Set Flag	☐ Send to Data Historian
Bay	<None>	☐ Can be controlled by Bay	
Lockout Point	Estacion_B,LOCKOUT	☐ Auto Select Un-Commanded Changes for Summary Reports	
Lockout Timer, sec	10	☐ Do not alarm states 2 and 3 on control operations	



Sequence # 15 Name Lockout

Autostart □ There is Error □ At Line 0

Description Lockout

Restart □ State Not Running. (0)

State Point <None>

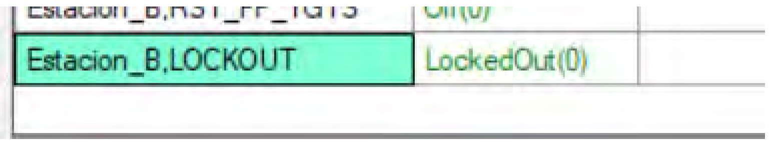
Message

☑ COMPILED CODE IS UP TO DATE

Schedule <None> <None>

```
"Estacion_B,52AA1" = 0
delay 3s
"Estacion_B,52AA1" = 1
```

Normal State lockout =1
Always



Estacion_B,LOCKOUT	LockedOut(0)

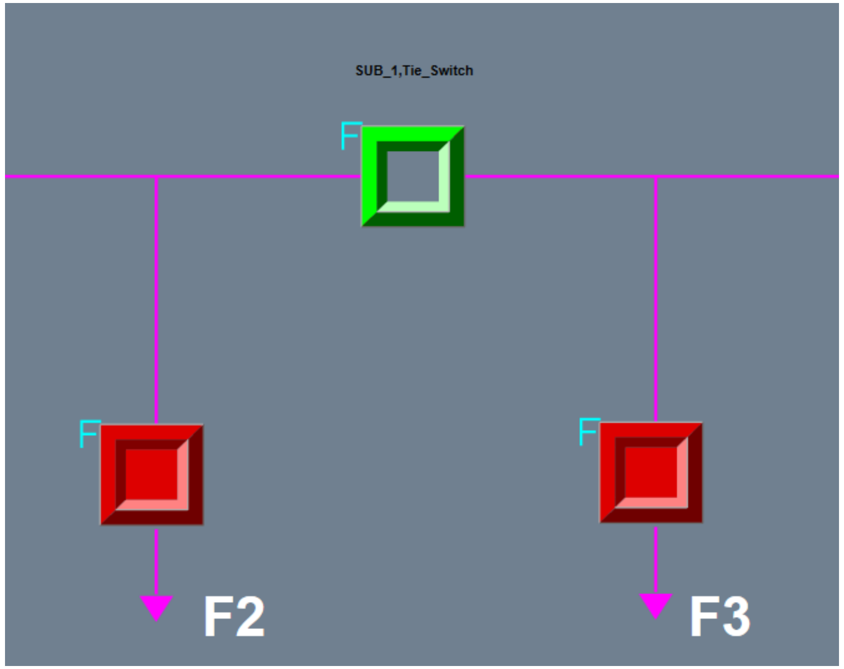
Exercise

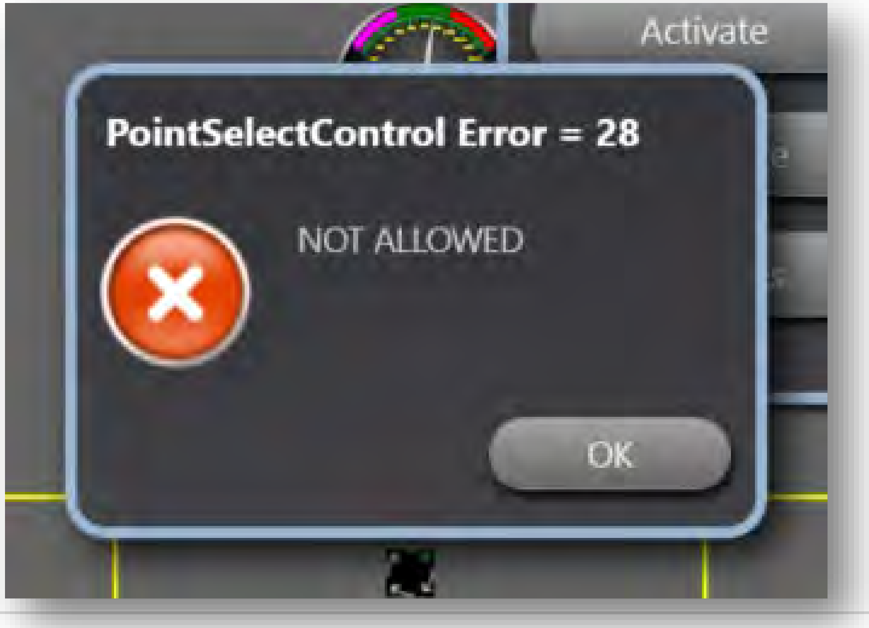
Activate a lockout point

- Using STC Explorer:
  - Assign a lockout point to a breaker and set the timer.
  - Create a command sequence to change the value of the breaker point.

Control permissions

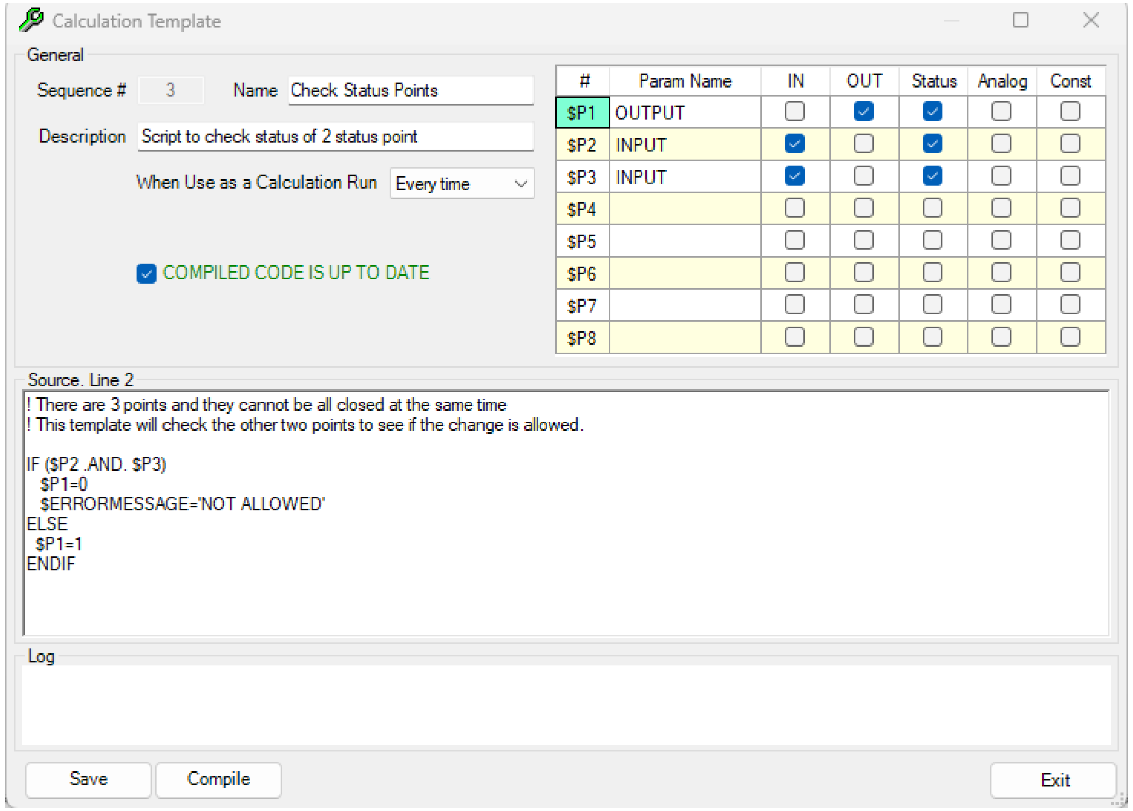
- There might be instances in which we need to control or monitor certain states of our breakers or devices to prevent unwanted situations.
- Control Permissions allow us to dictate the conditions by which certain actions are allowed (or not allowed).




PointSelectControl Error = 28

NOT ALLOWED

- Controls can be blocked at a point level if certain user defined conditions match
- This is implemented as Automation template
- Template is applied on the point under permissions



Sequence # 3 Name Check Status Points

Description Script to check status of 2 status point

When Use as a Calculation Run Every time

☑ COMPILED CODE IS UP TO DATE

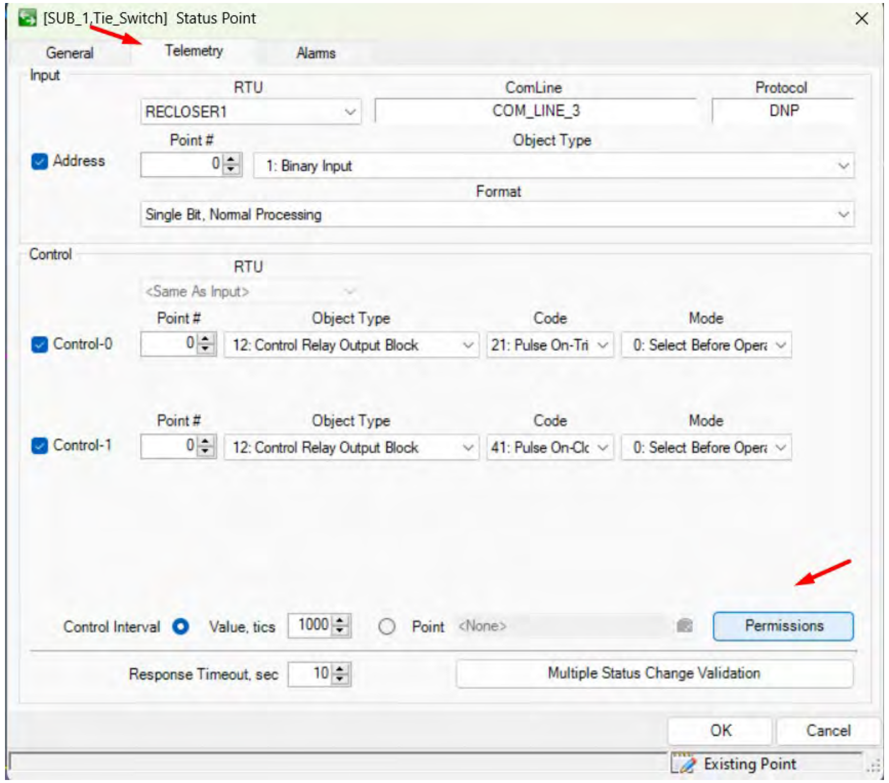
#	Param Name	IN	OUT	Status	Analog	Const
$P1	OUTPUT	☐	☑	☑	☐	☐
$P2	INPUT	☑	☐	☑	☐	☐
$P3	INPUT	☑	☐	☑	☐	☐
$P4		☐	☐	☐	☐	☐
$P5		☐	☐	☐	☐	☐
$P6		☐	☐	☐	☐	☐
$P7		☐	☐	☐	☐	☐
$P8		☐	☐	☐	☐	☐

```
! There are 3 points and they cannot be all closed at the same time
! This template will check the other two points to see if the change is allowed.

IF ($P2 .AND. $P3)
   $P1=0
   $ERRORMESSAGE='NOT ALLOWED'
ELSE
  $P1=1
ENDIF
```

```
IF ($P2 .AND. $P3)
   $P1=0
   $ERRORMESSAGE='NOT ALLOWED'
ELSE
  $P1=1
ENDIF
```

- Once a control permission has been defined, we need to configure it on the correct points i our database.
- This is done on the telemetry tab.



[SUB_1,Tie_Switch] Status Point

Input

RTU	ComLine	Protocol
RECLOSER1	COM_LINE_3	DNP

☑ Address — Point #: 0 — Object Type: 1: Binary Input

Format: Single Bit, Normal Processing

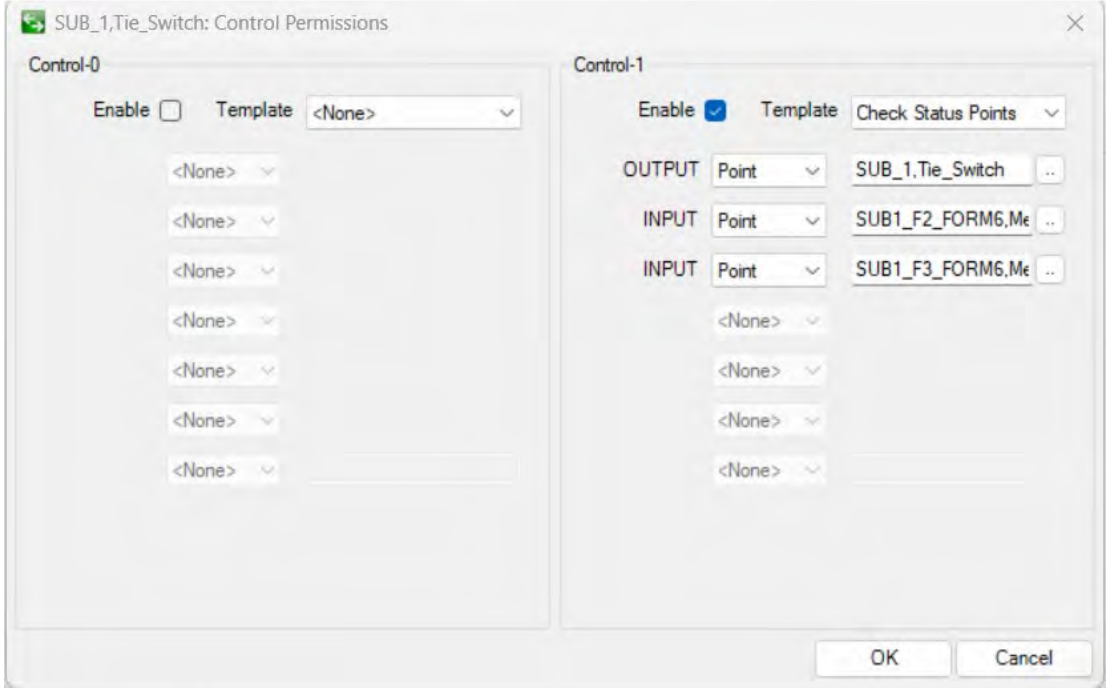
Control

RTU: <Same As Input>

	Point #	Object Type	Code	Mode
☑ Control-0	0	12: Control Relay Output Block	21: Pulse On-Tri	0: Select Before Oper:
☑ Control-1	0	12: Control Relay Output Block	41: Pulse On-Clc	0: Select Before Oper:

Control Interval ● Value, tics 1000 ○ Point <None>

Response Timeout, sec 10



SUB_1,Tie_Switch: Control Permissions

Control-0

Enable □ Template <None>

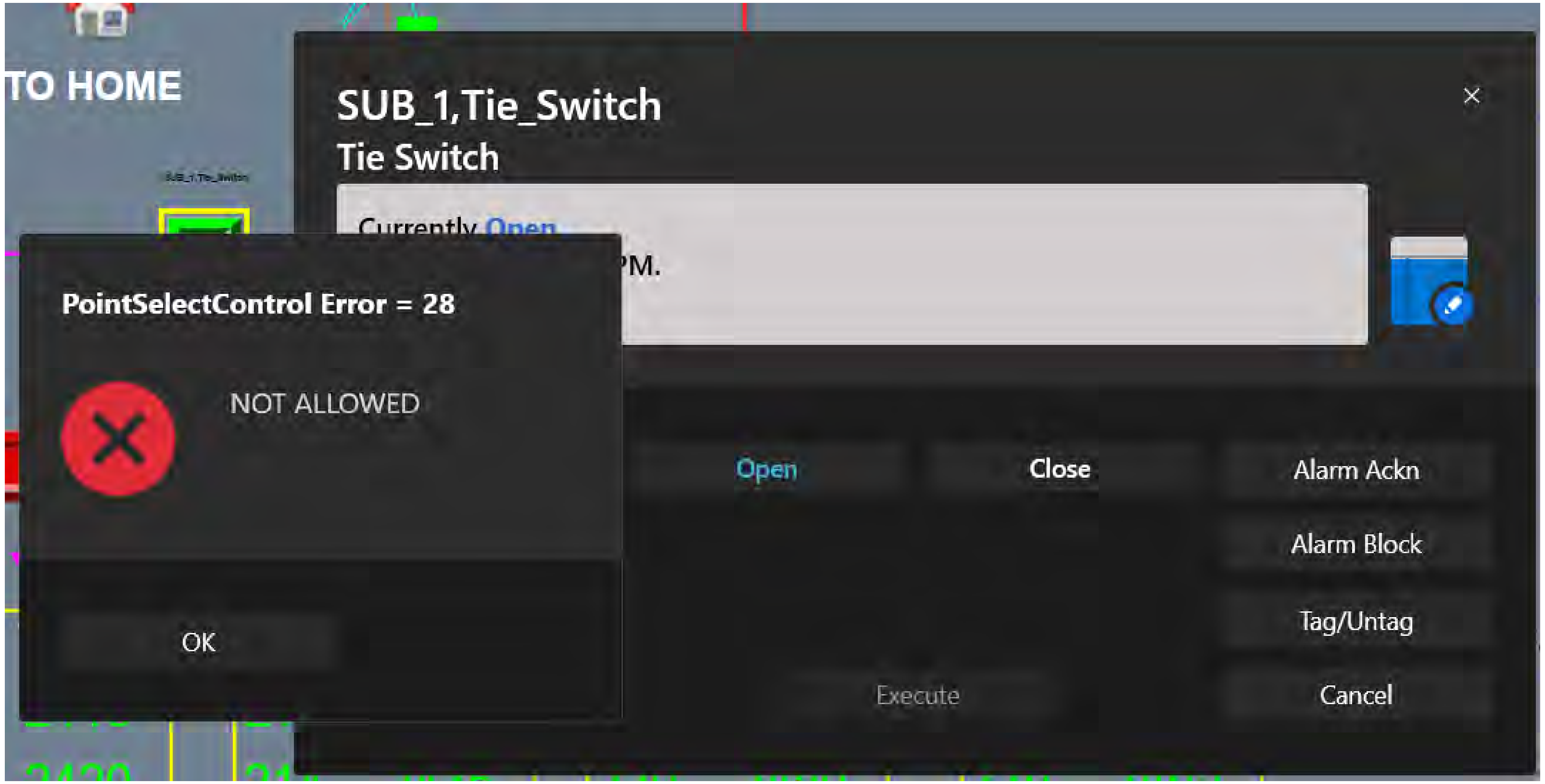
<None>
<None>
<None>
<None>
<None>
<None>
<None>

Control-1

Enable ☑ Template Check Status Points

OUTPUT	Point	SUB_1,Tie_Switch
INPUT	Point	SUB1_F2_FORM6,Me
INPUT	Point	SUB1_F3_FORM6,Me
	<None>	
	<None>	
	<None>	
	<None>	

- If the control permissions are defined correctly, we can test its behaviour by triggering the conditions by which the control command cannot be executed.

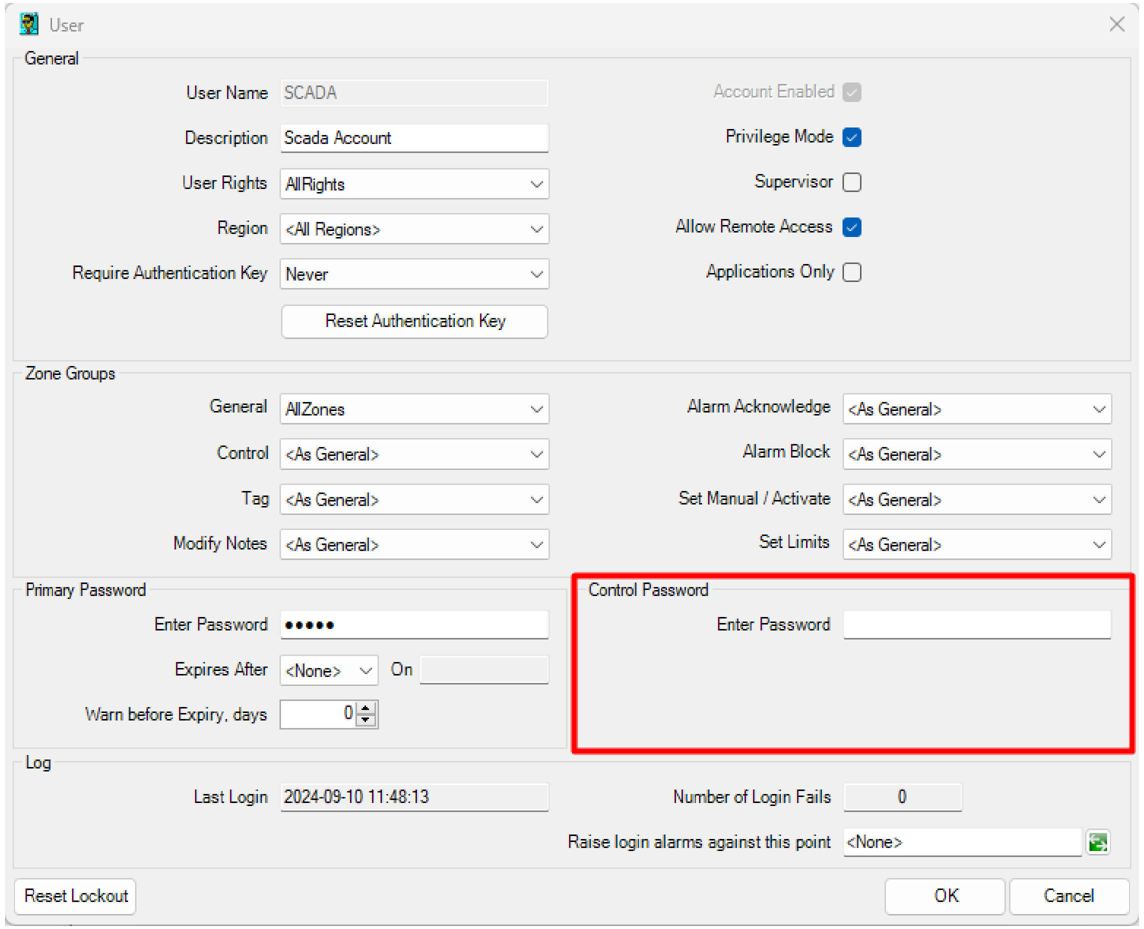


PointSelectControl Error = 28

NOT ALLOWED

Control Password

- Additional layer of security
- Password exclusive for sending control commands
- Control password can be enabled system-wide or per point.
- The control password needs to be set up for each user who needs to send a command



User

General

User Name: SCADA

Account Enabled ☑

Description: Scada Account

Privilege Mode ☑

User Rights: AllRights

Supervisor □

Region: <All Regions>

Allow Remote Access ☑

Require Authentication Key: Never

Applications Only □

Zone Groups

General: AllZones

Alarm Acknowledge: <As General>

Control: <As General>

Alarm Block: <As General>

Tag: <As General>

Set Manual / Activate: <As General>

Modify Notes: <As General>

Set Limits: <As General>

Primary Password

Enter Password: •••••

Expires After: <None> On

Warn before Expiry, days: 0

Control Password

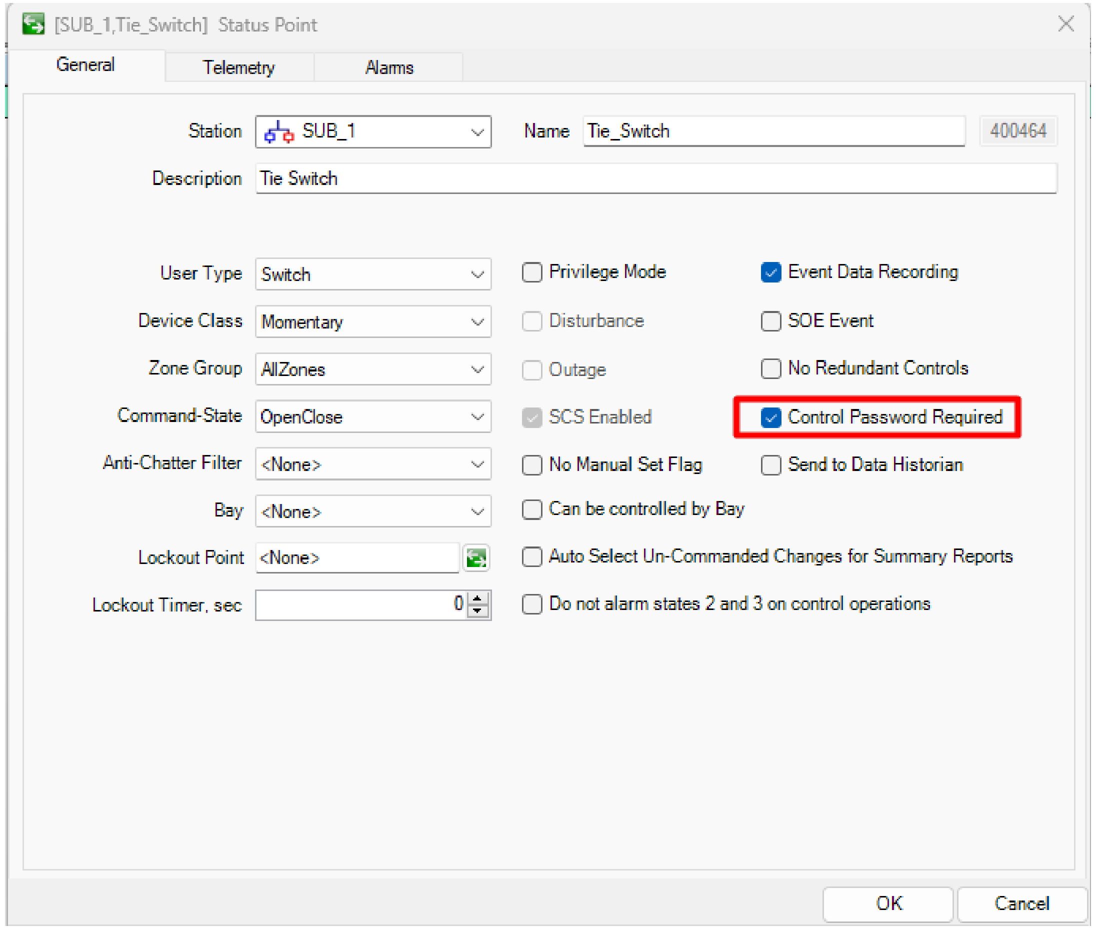
Enter Password:

Log

Last Login: 2024-09-10 11:48:13

Number of Login Fails: 0

Raise login alarms against this point: <None>



[SUB_1,Tie_Switch] Status Point

Station: SUB_1

Name: Tie_Switch 400464

Description: Tie Switch

User Type: Switch

Device Class: Momentary

Zone Group: AllZones

Command-State: OpenClose

Anti-Chatter Filter: <None>

Bay: <None>

Lockout Point: <None>

Lockout Timer, sec: 0

□ Privilege Mode

□ Disturbance

□ Outage

☑ SCS Enabled

□ No Manual Set Flag

□ Can be controlled by Bay

□ Auto Select Un-Commanded Changes for Summary Reports

□ Do not alarm states 2 and 3 on control operations

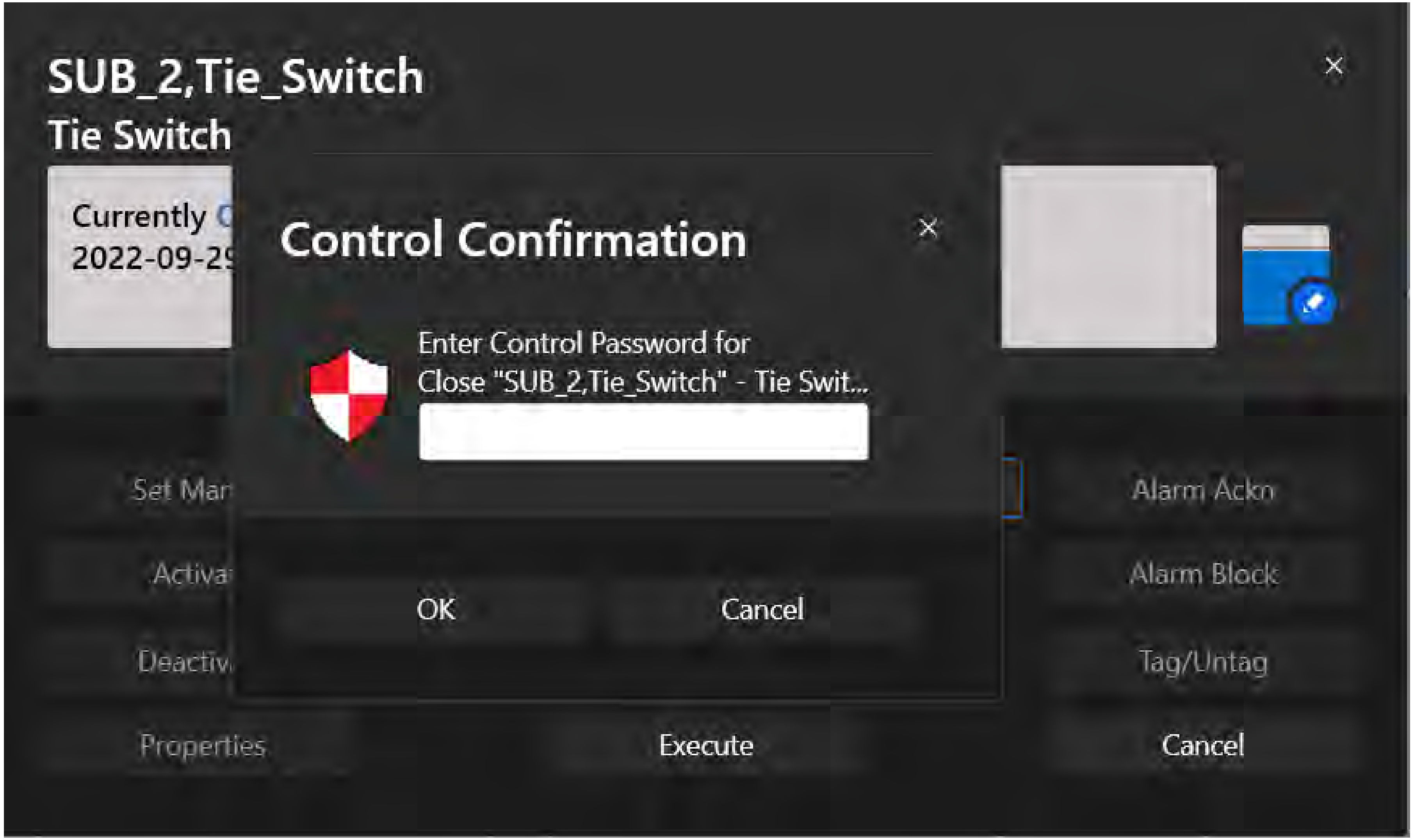
☑ Event Data Recording

□ SOE Event

□ No Redundant Controls

☑ Control Password Required

□ Send to Data Historian



SUB_2,Tie_Switch

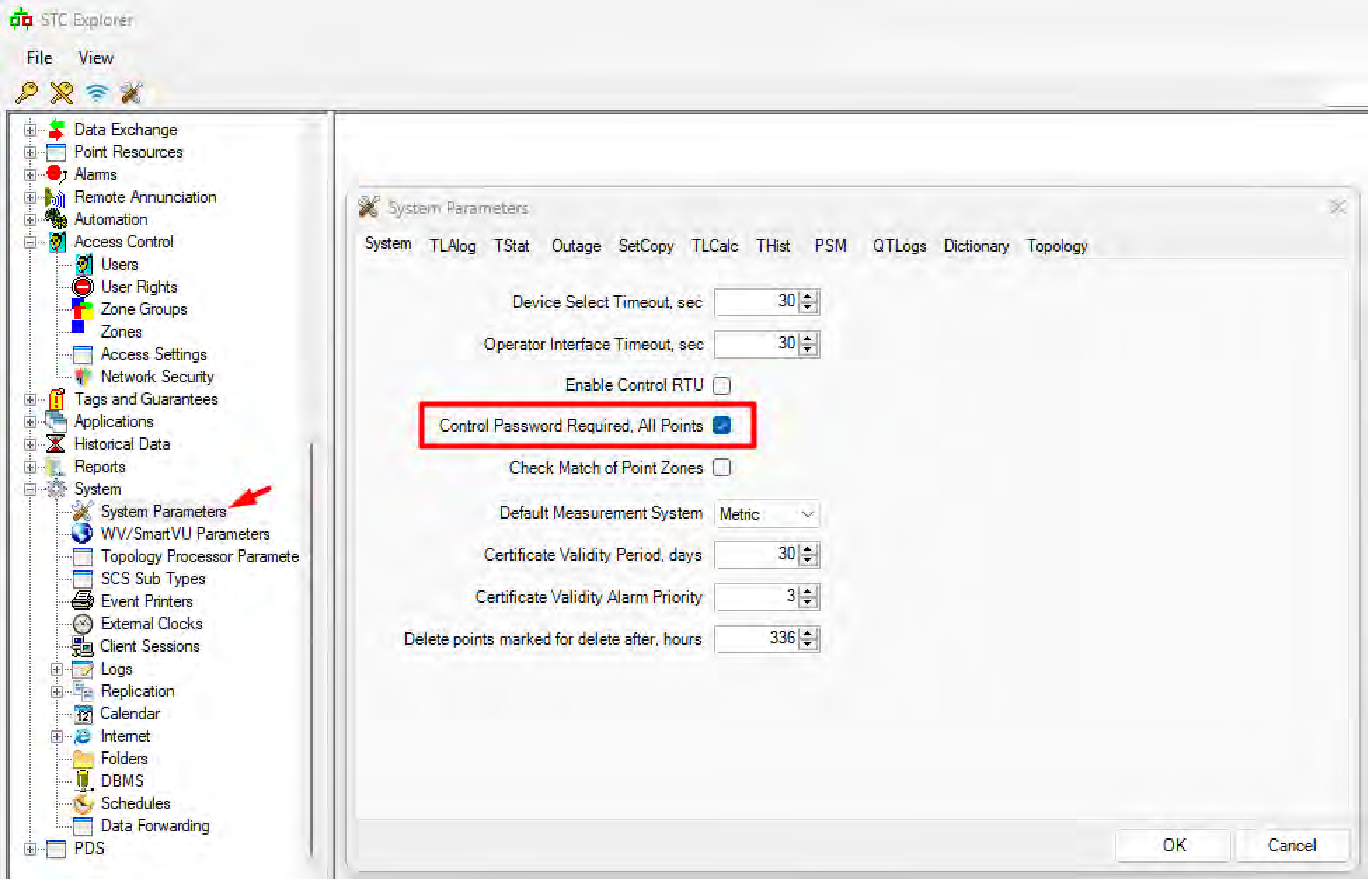
Tie Switch

Currently C
2022-09-2

Control Confirmation

Enter Control Password for
Close "SUB_2,Tie_Switch" - Tie Swit...

Control Password



Device Select Timeout, sec 30

Operator Interface Timeout, sec 30

Enable Control RTU ☐

Control Password Required, All Points ☑

Check Match of Point Zones ☐

Default Measurement System Metric

Certificate Validity Period, days 30

Certificate Validity Alarm Priority 3

Delete points marked for delete after, hours 336

Exercise

Use the control restrictions

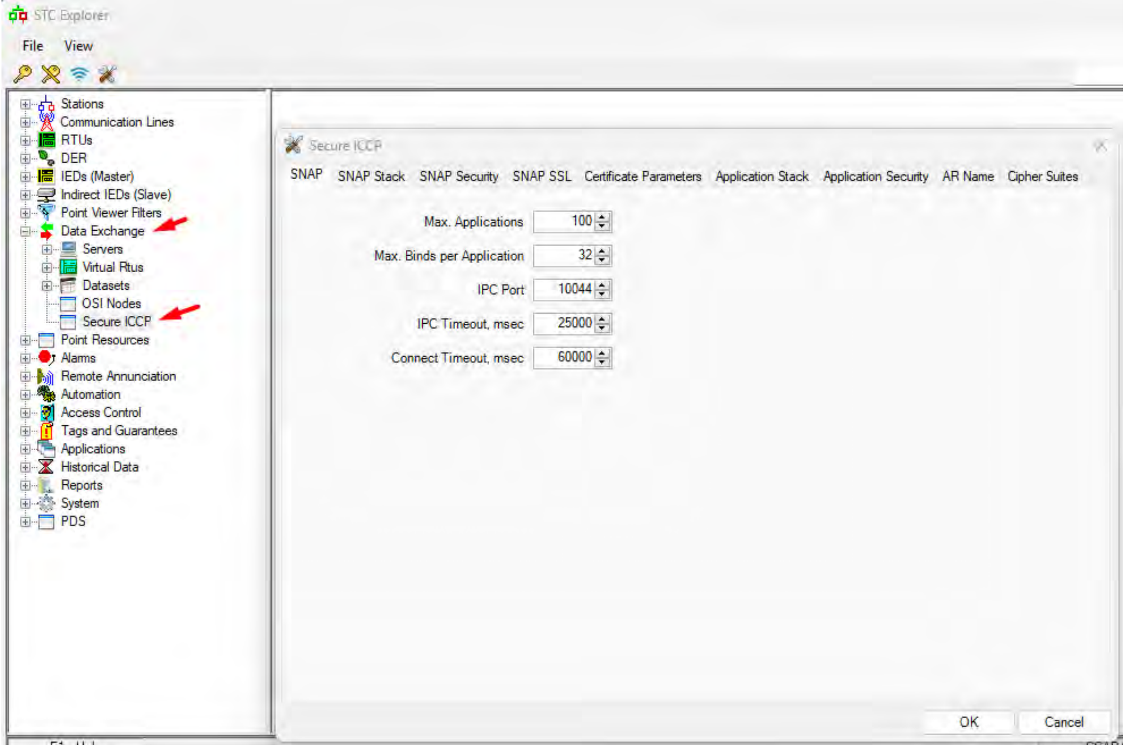
- Using STC Explorer:
  - Set a control password for a user.
  - Enable the control password option in a point.
  - Enable the control password in all points.
- Using SmartVU:
  - Perform a control in one of the points recently edited.

SECURE ICCP

- Secure ICCP provides two distinct and independent facilities for security:
  - MACE (MMS Application Certification Exchange) for application authentication
  - SSL/TLS as a secure transport layer provides positive identification of the remote node and SSL/TLS data encryption using bi-directional certificate exchange.
  - Follows IEC 62351-3 (TLS) and IEC 62351-4 (MMS/ICCP)
  - Requires SISCO SNAP-Lite stack (Third party protocol stack)
  - Recommended to upgrade to SNAP Lite if you are using discontinued OSI stack from SISCO
  - Secure ICCP is separately licensed product

Secure ICCP

- Server specific configuration of Secure ICCP



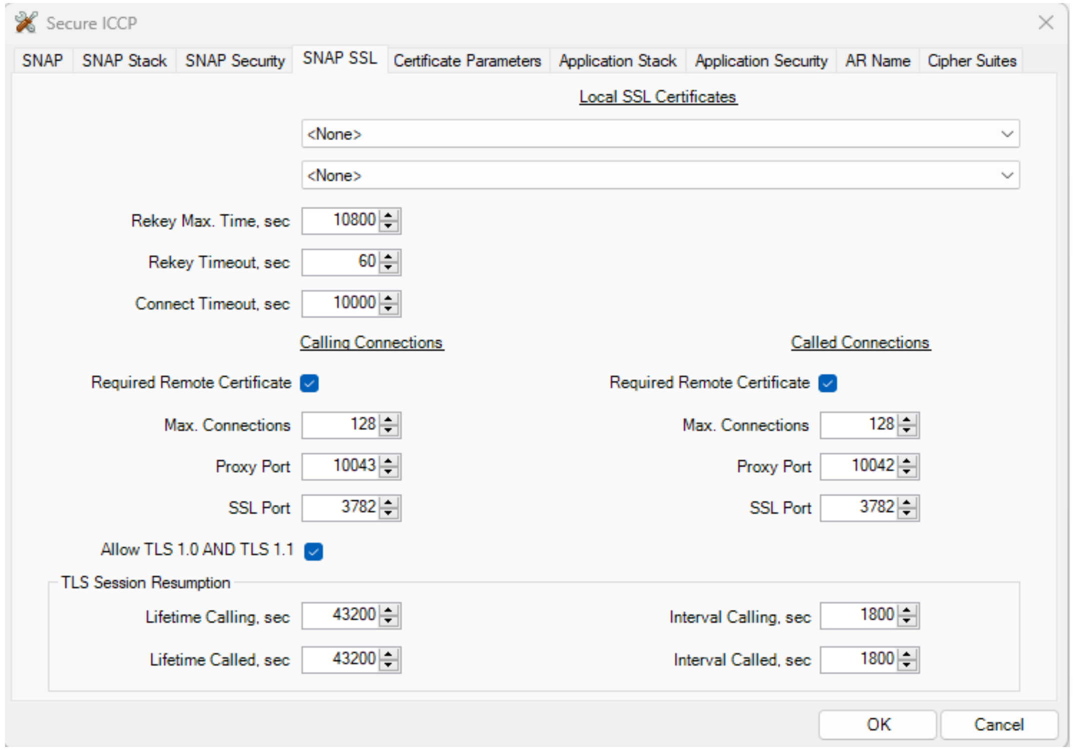
Max. Applications 100

Max. Binds per Application 32

IPC Port 10044

IPC Timeout, msec 25000

Connect Timeout, msec 60000



Local SSL Certificates

<None>

<None>

Rekey Max. Time, sec 10800

Rekey Timeout, sec 60

Connect Timeout, sec 10000

Calling Connections		Called Connections	
Required Remote Certificate	☑	Required Remote Certificate	☑
Max. Connections	128	Max. Connections	128
Proxy Port	10043	Proxy Port	10042
SSL Port	3782	SSL Port	3782

Allow TLS 1.0 AND TLS 1.1 ☑

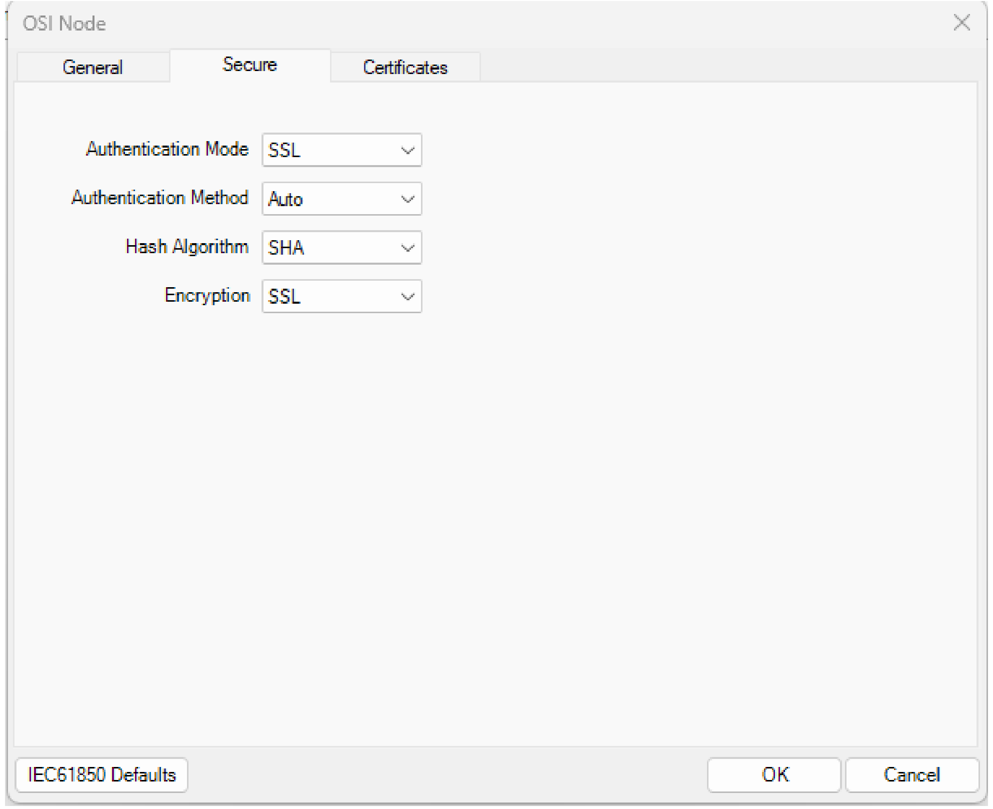
TLS Session Resumption

Lifetime Calling, sec	43200	Interval Calling, sec	1800
Lifetime Called, sec	43200	Interval Called, sec	1800

TOC

Secure ICCP

- Node specific configuration of Secure ICCP



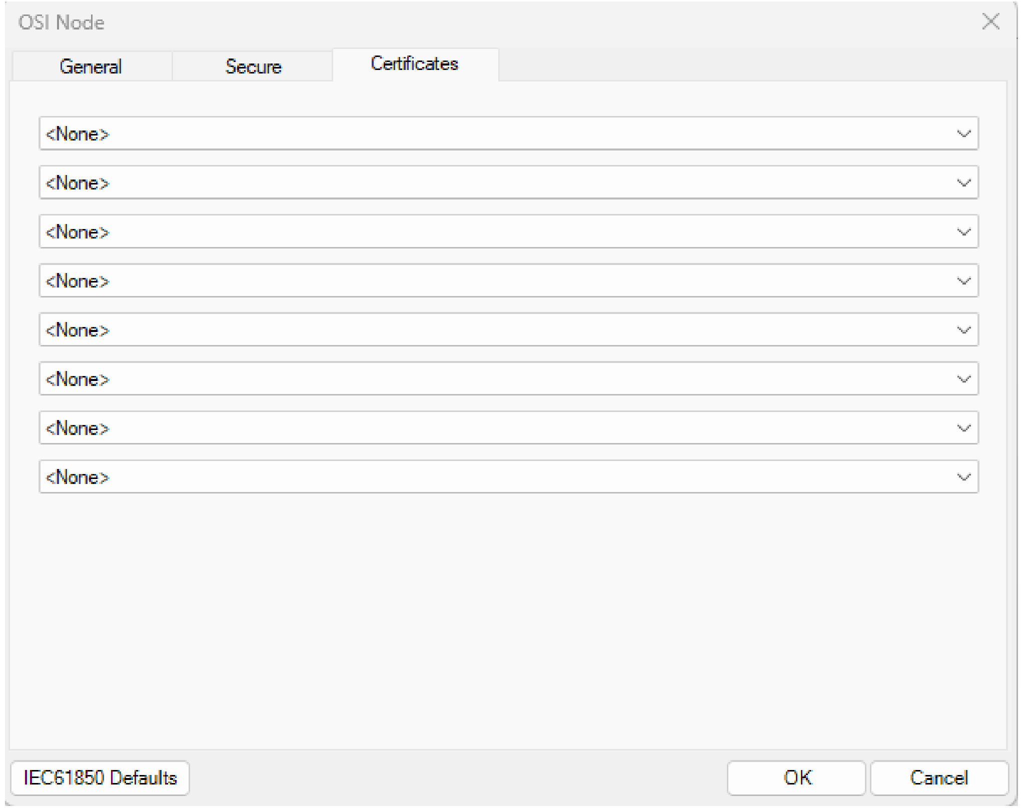
OSI Node

Authentication Mode: SSL

Authentication Method: Auto

Hash Algorithm: SHA

Encryption: SSL



OSI Node

<None>

<None>

<None>

<None>

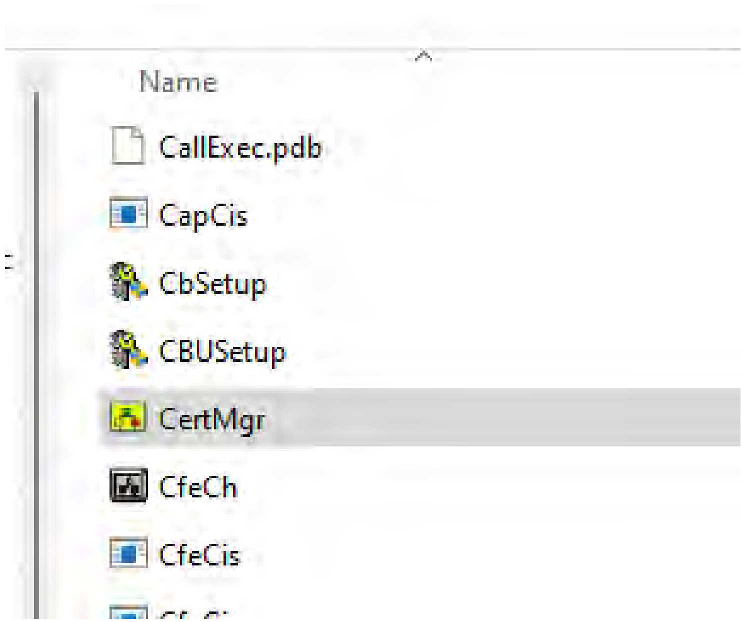
<None>

<None>

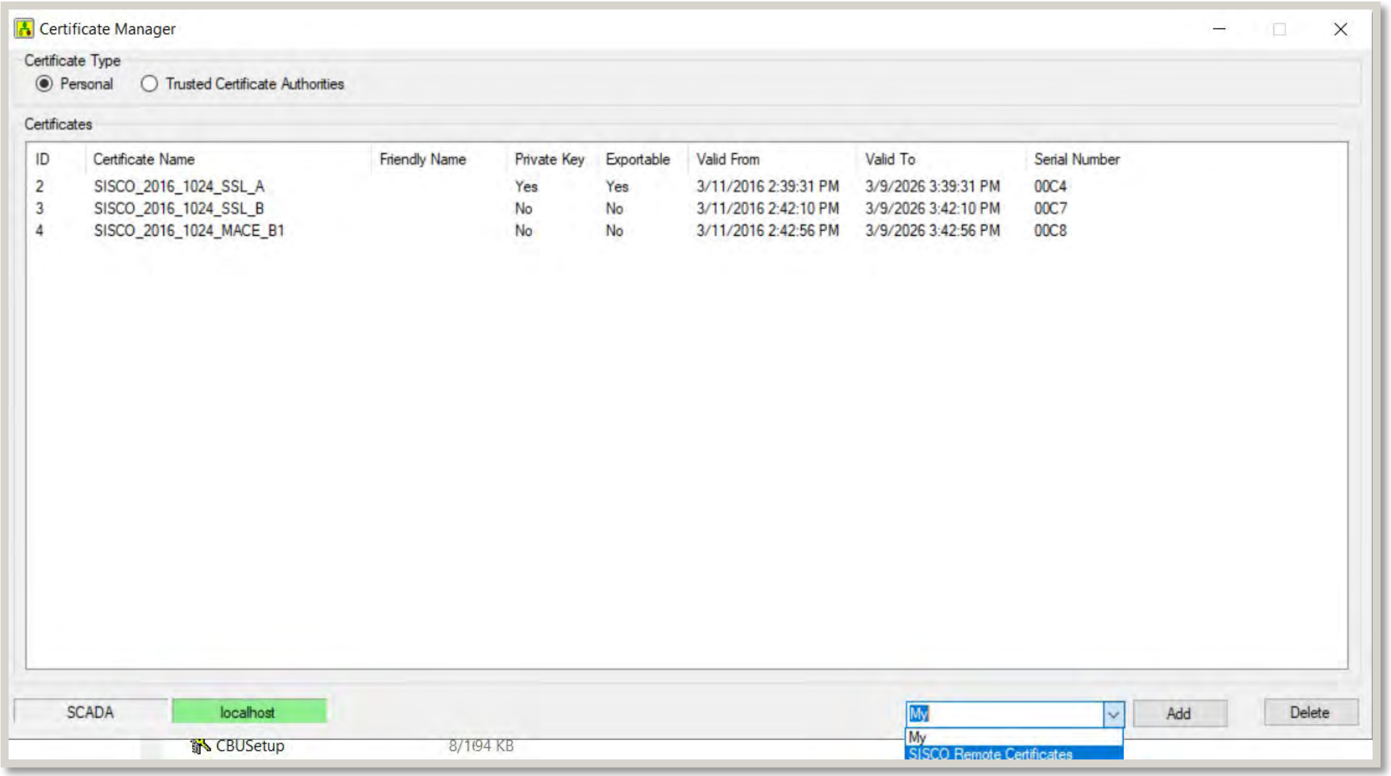
<None>

<None>

- Certificate that are added in Microsoft Management Console store needs to be referenced in SCADA database



Name
- CallExec.pdb
- CapCis
- CbSetup
- CBUSetup
- CertMgr
- CfeCh
- CfeCis



Certificate Manager

Certificate Type
● Personal ○ Trusted Certificate Authorities

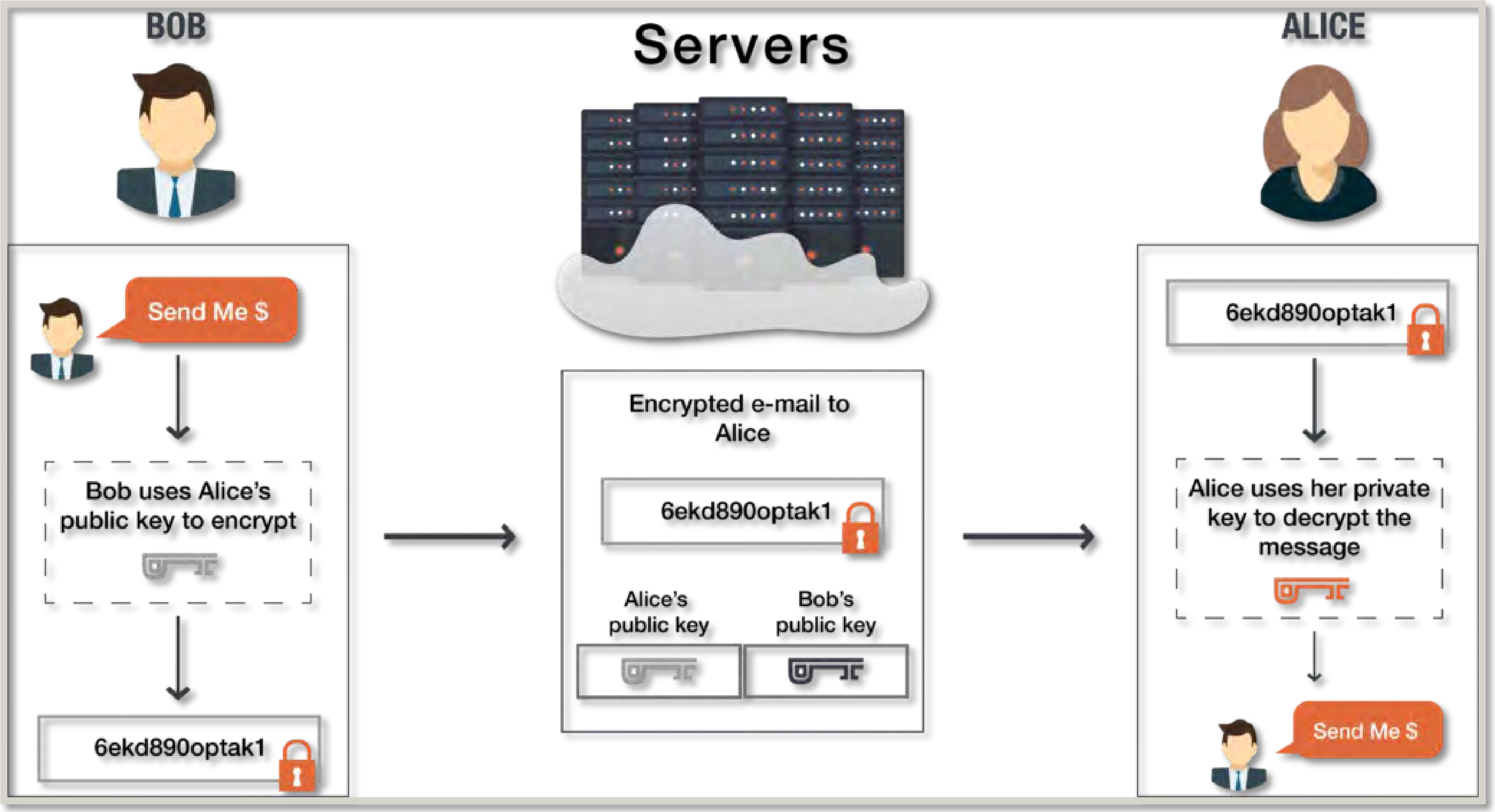
Certificates

ID	Certificate Name	Friendly Name	Private Key	Exportable	Valid From	Valid To	Serial Number
2	SISCO_2016_1024_SSL_A		Yes	Yes	3/11/2016 2:39:31 PM	3/9/2026 3:39:31 PM	00C4
3	SISCO_2016_1024_SSL_B		No	No	3/11/2016 2:42:10 PM	3/9/2026 3:42:10 PM	00C7
4	SISCO_2016_1024_MACE_B1		No	No	3/11/2016 2:42:56 PM	3/9/2026 3:42:56 PM	00C8

SCADA | localhost

My
- My
- SISCO Remote Certificates

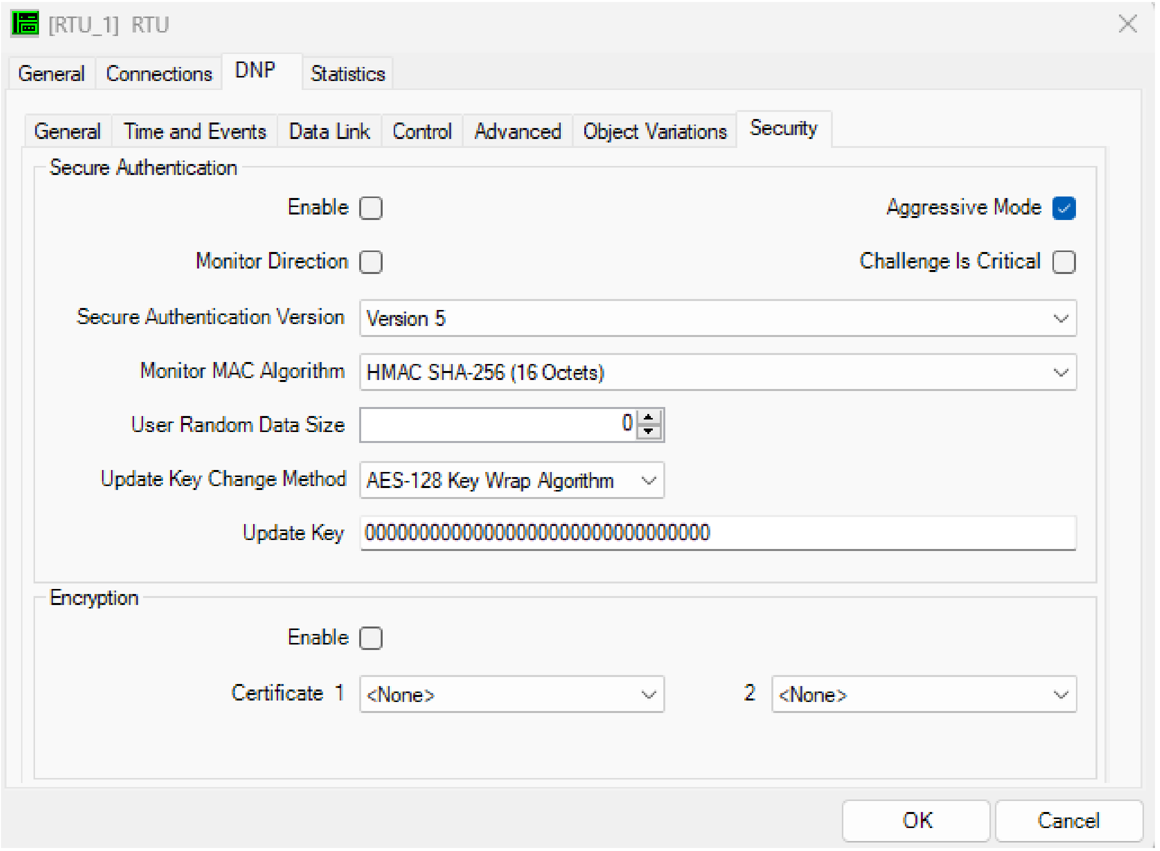
Secure ICCP


BOB
Servers
ALICE
Send Me $
Bob uses Alice's public key to encrypt
6ekd890optak1
Encrypted e-mail to Alice
6ekd890optak1
Alice's public key
Bob's public key
6ekd890optak1
Alice uses her private key to decrypt the message
Send Me $

Secure DNP

- Secure DNP consists of two parts
  - Secure Authentication
  - Encryption
- Secure Authentication provides a way for master and outstation devices to authenticate unambiguously when communicating.
- This uses remote update key change mechanism for authentication.
- Encryption is the scrambling of messages at the TCP/IP level.
- This uses certificates to verify the identity of the connected device.

Secure DNP



Secure Authentication

Enable □

Aggressive Mode ☑

Monitor Direction □

Challenge Is Critical □

Secure Authentication Version: Version 5

Monitor MAC Algorithm: HMAC SHA-256 (16 Octets)

User Random Data Size: 0

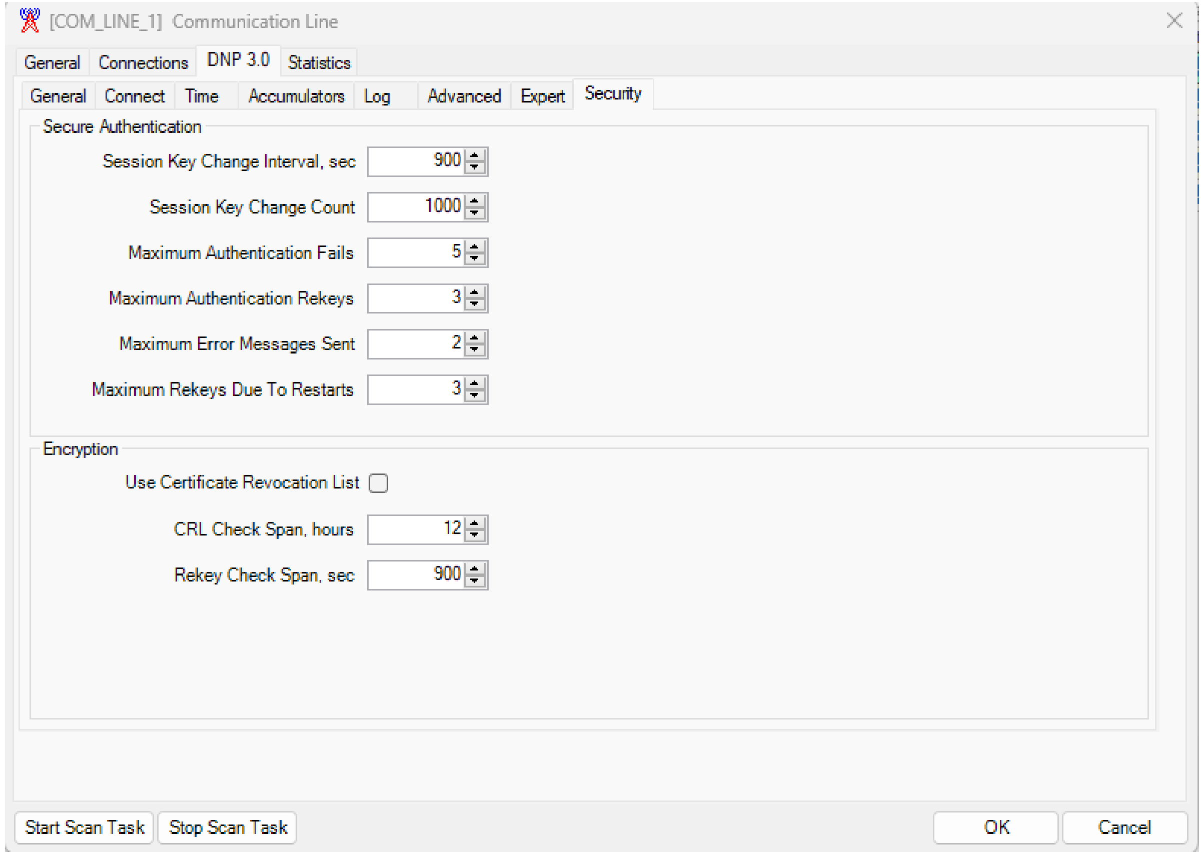
Update Key Change Method: AES-128 Key Wrap Algorithm

Update Key: 00000000000000000000000000000000

Encryption

Enable □

Certificate 1 <None> 2 <None>



Secure Authentication

Session Key Change Interval, sec: 900

Session Key Change Count: 1000

Maximum Authentication Fails: 5

Maximum Authentication Rekeys: 3

Maximum Error Messages Sent: 2

Maximum Rekeys Due To Restarts: 3

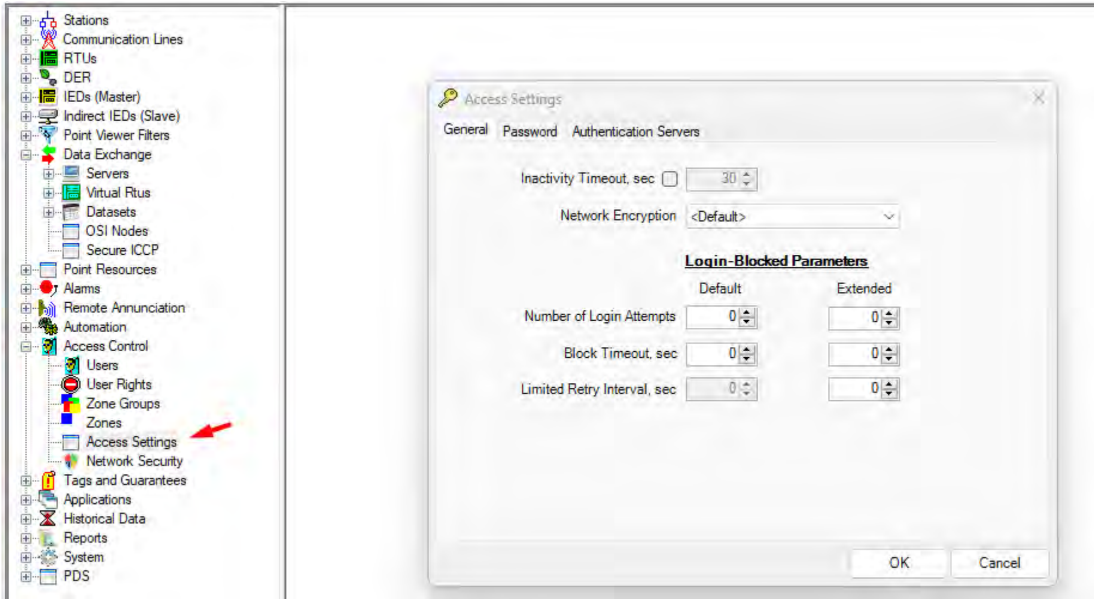
Encryption

Use Certificate Revocation List □

CRL Check Span, hours: 12

Rekey Check Span, sec: 900

- Rules that applies to all SCADA users
- You can set up the login and password parameters



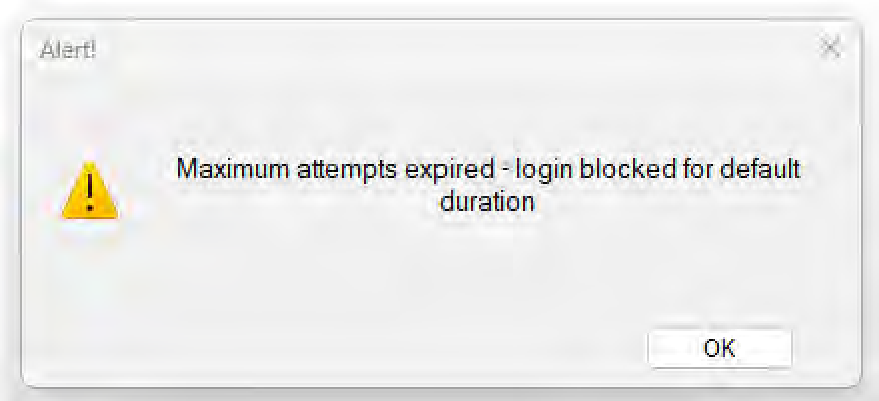
Inactivity Timeout, sec ☐ 30

Network Encryption <Default>

Login-Blocked Parameters

	Default	Extended
Number of Login Attempts	0	0
Block Timeout, sec	0	0
Limited Retry Interval, sec	0	0

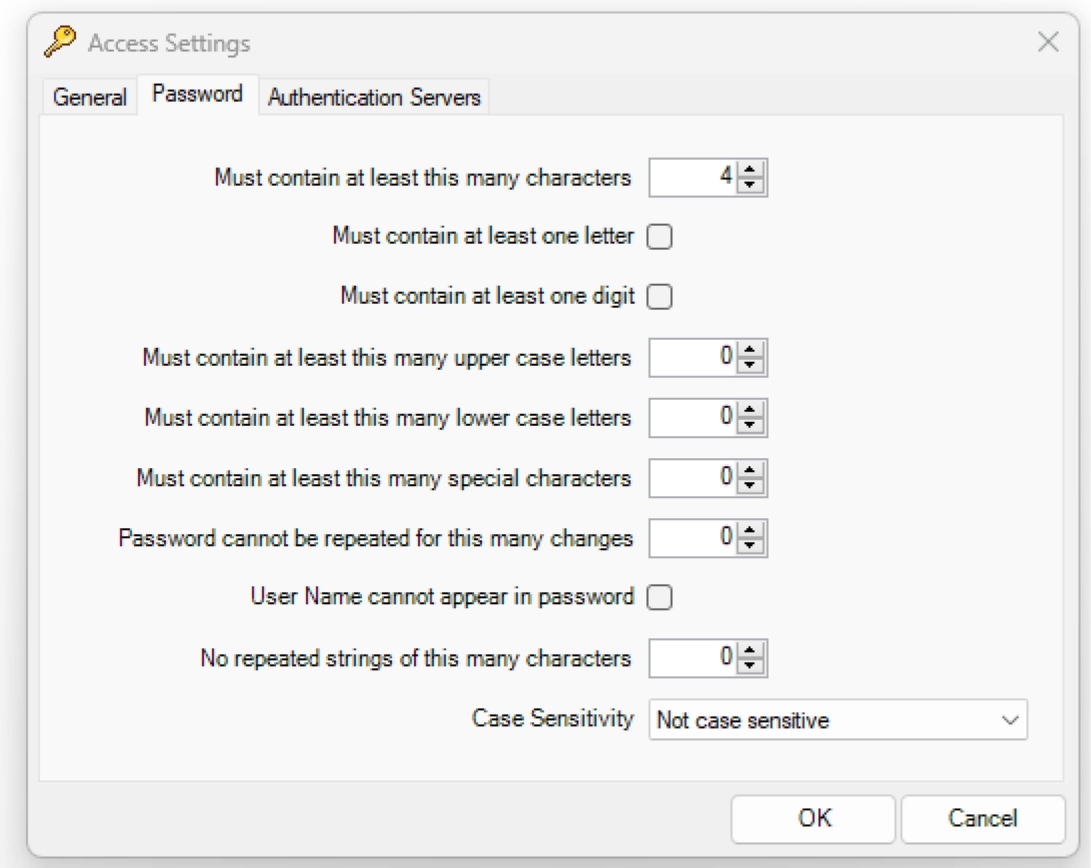
- Block access of a user after certain number of failed login attempts
- User is allowed to attempt login after certain Block Timeout
- Block can be extended if the user makes certain number of failed attempts in limited retry interval
- Locked out user can be reset by another user with sufficient rights



Maximum attempts expired - login blocked for default duration

Password

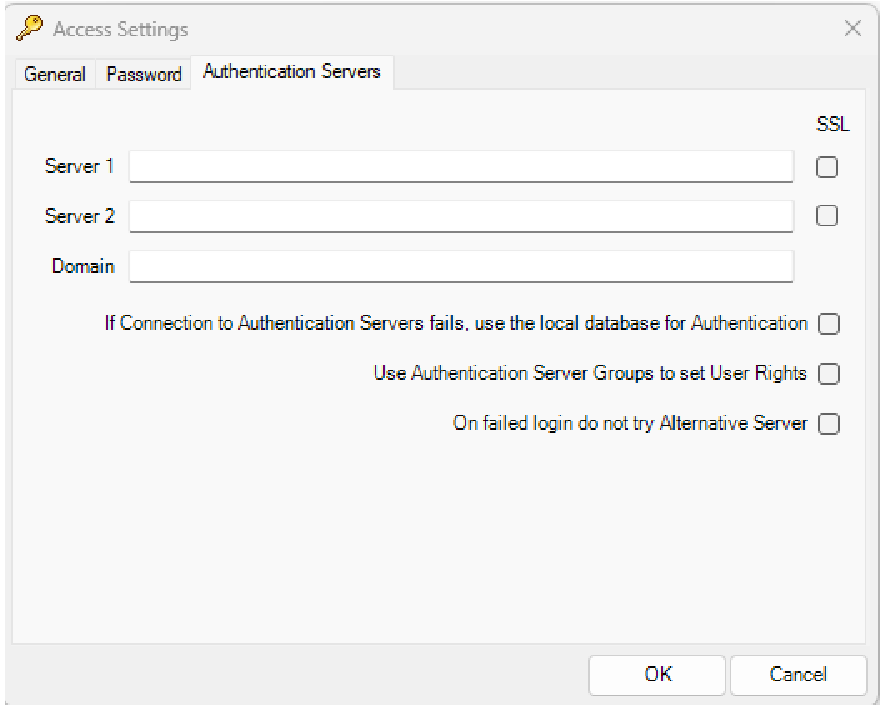
- Options to ensure that the password is strong



Must contain at least this many characters	4
Must contain at least one letter	□
Must contain at least one digit	□
Must contain at least this many upper case letters	0
Must contain at least this many lower case letters	0
Must contain at least this many special characters	0
Password cannot be repeated for this many changes	0
User Name cannot appear in password	□
No repeated strings of this many characters	0
Case Sensitivity	Not case sensitive

LDAP

- LDAP authentication is also an option to add another layer of security.
- Use organization authentication servers to login to SCADA
- Use same credentials as your domain login



Access Settings

		SSL
Server 1		□
Server 2		□
Domain		

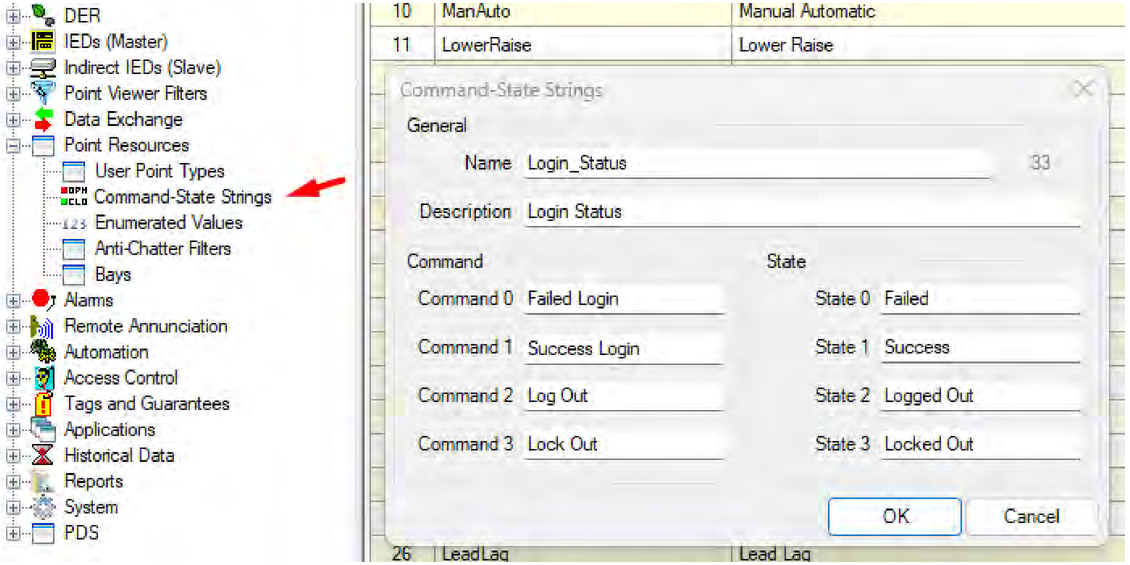
If Connection to Authentication Servers fails, use the local database for Authentication □

Use Authentication Server Groups to set User Rights □

On failed login do not try Alternative Server □

Command String

- Alarms can be raised for login attempts against a database point



10	ManAuto	Manual Automatic
11	LowerRaise	Lower Raise
26	LeadLag	Lead Lag

Command-State Strings

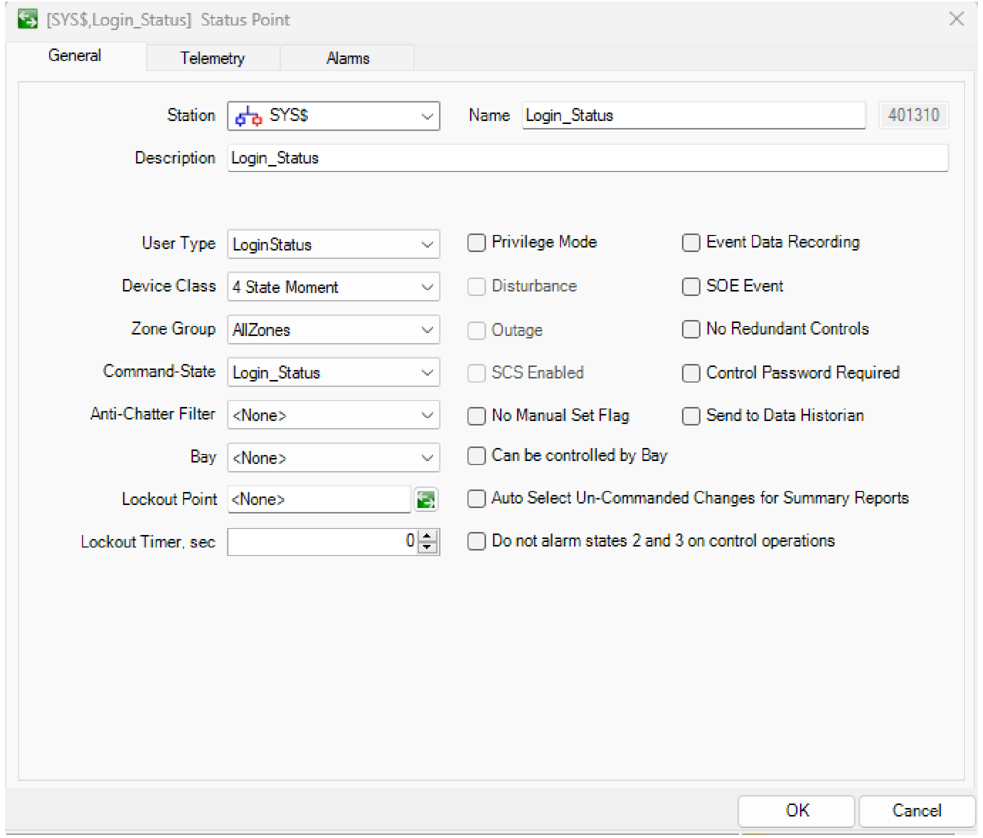
General

Name: Login_Status 33

Description: Login Status

Command		State	
Command 0	Failed Login	State 0	Failed
Command 1	Success Login	State 1	Success
Command 2	Log Out	State 2	Logged Out
Command 3	Lock Out	State 3	Locked Out

OK Cancel



[SYS$,Login_Status] Status Point

General | Telemetry | Alarms

Station: SYS$ Name: Login_Status 401310

Description: Login_Status

User Type: LoginStatus

Device Class: 4 State Moment

Zone Group: AllZones

Command-State: Login_Status

Anti-Chatter Filter: <None>

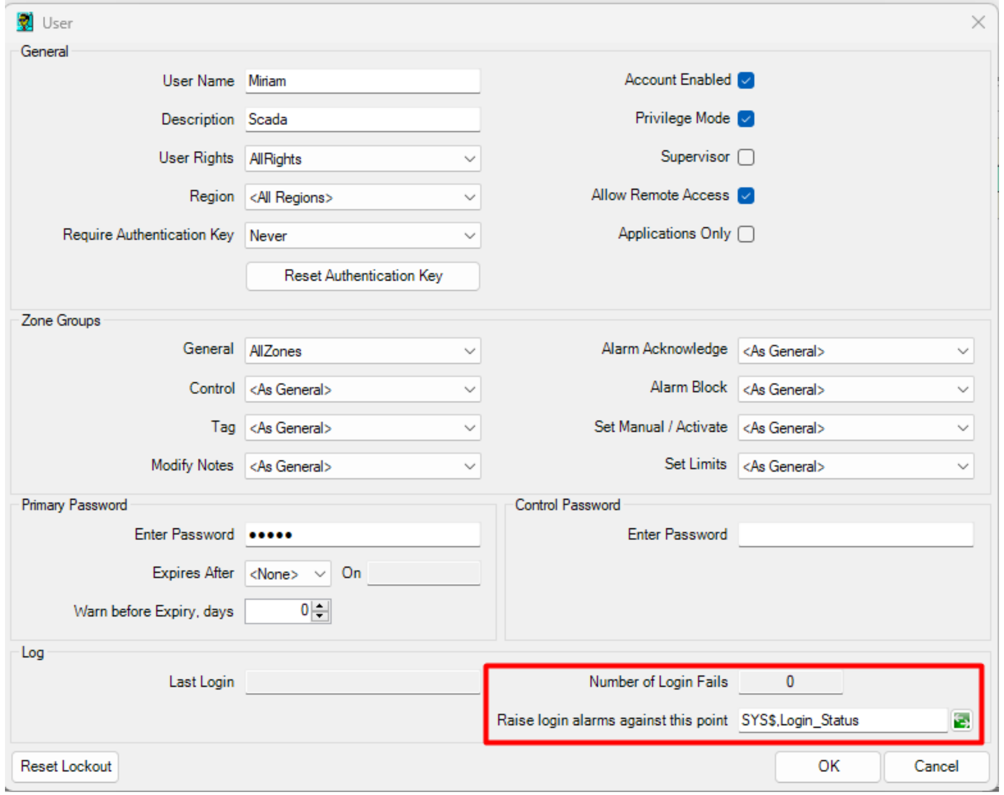
Bay: <None>

Lockout Point: <None>

Lockout Timer, sec: 0

- ☐ Privilege Mode
- ☐ Disturbance
- ☐ Outage
- ☐ SCS Enabled
- ☐ No Manual Set Flag
- ☐ Can be controlled by Bay
- ☐ Auto Select Un-Commanded Changes for Summary Reports
- ☐ Do not alarm states 2 and 3 on control operations
- ☐ Event Data Recording
- ☐ SOE Event
- ☐ No Redundant Controls
- ☐ Control Password Required
- ☐ Send to Data Historian

OK Cancel



User

General

User Name: Miriam

Description: Scada

User Rights: AllRights

Region: <All Regions>

Require Authentication Key: Never

Reset Authentication Key

Account Enabled ☑

Privilege Mode ☑

Supervisor ☐

Allow Remote Access ☑

Applications Only ☐

Zone Groups

General: AllZones

Control: <As General>

Tag: <As General>

Modify Notes: <As General>

Alarm Acknowledge: <As General>

Alarm Block: <As General>

Set Manual / Activate: <As General>

Set Limits: <As General>

Primary Password

Enter Password: •••••

Expires After: <None> On

Warn before Expiry, days: 0

Control Password

Enter Password:

Log

Last Login:

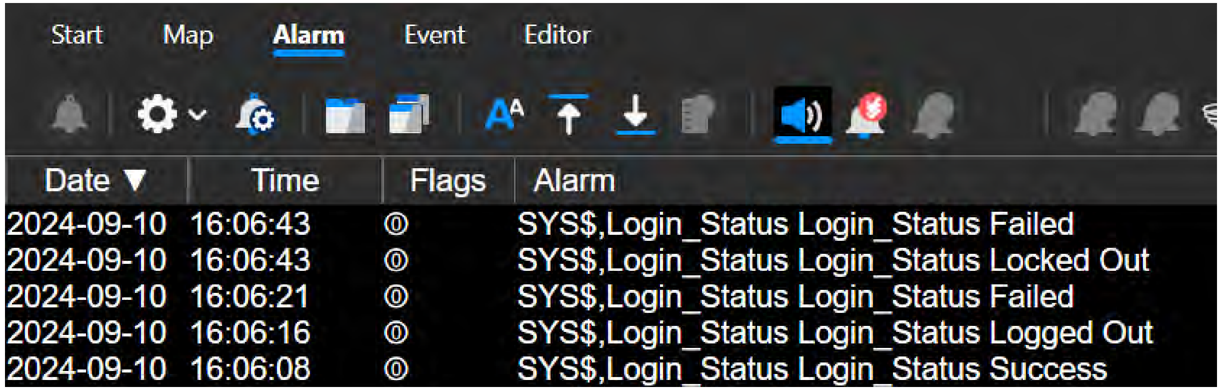
Number of Login Fails: 0

Raise login alarms against this point: SYS$,Login_Status

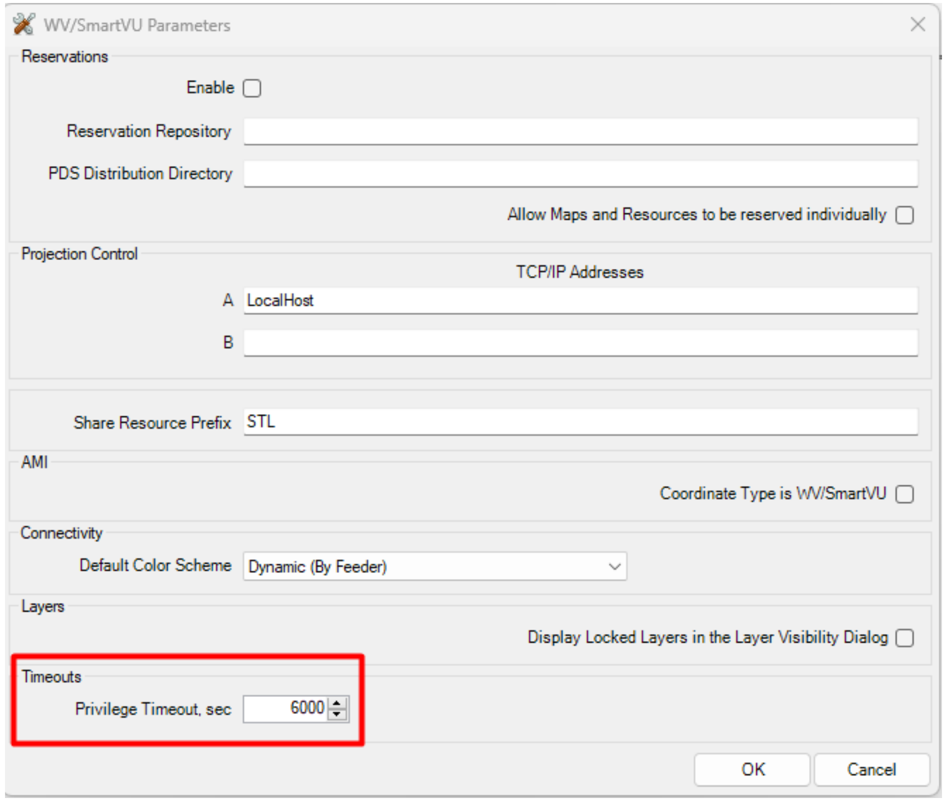
Reset Lockout

OK

Cancel



Date ▼	Time	Flags	Alarm
2024-09-10	16:06:43	⓪	SYS$,Login_Status Login_Status Failed
2024-09-10	16:06:43	⓪	SYS$,Login_Status Login_Status Locked Out
2024-09-10	16:06:21	⓪	SYS$,Login_Status Login_Status Failed
2024-09-10	16:06:16	⓪	SYS$,Login_Status Login_Status Logged Out
2024-09-10	16:06:08	⓪	SYS$,Login_Status Login_Status Success



WV/SmartVU Parameters

Reservations

Enable ☐

Reservation Repository

PDS Distribution Directory

Allow Maps and Resources to be reserved individually ☐

Projection Control

TCP/IP Addresses

A LocalHost

B

Share Resource Prefix STL

AMI

Coordinate Type is WV/SmartVU ☐

Connectivity

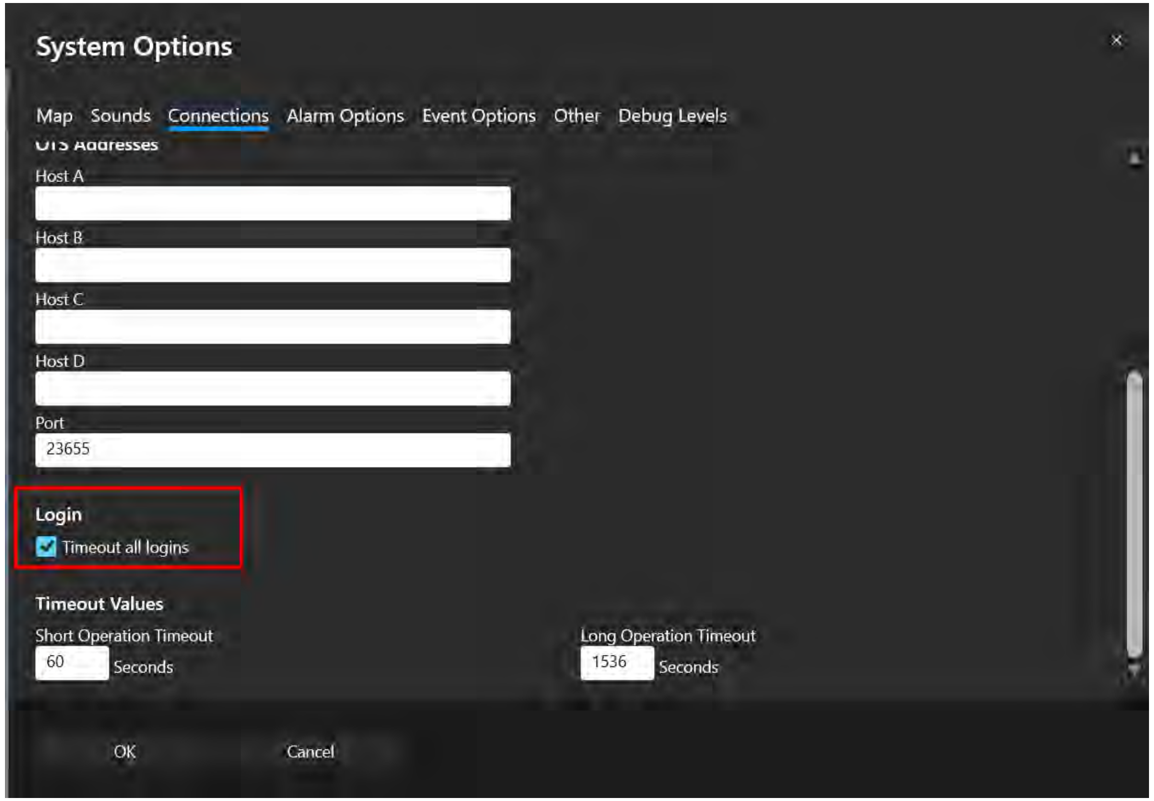
Default Color Scheme Dynamic (By Feeder)

Layers

Display Locked Layers in the Layer Visibility Dialog ☐

Timeouts

Privilege Timeout, sec 6000



System Options

UTS Addresses

Host A

Host B

Host C

Host D

Port

23655

Login

☑ Timeout all logins

Timeout Values

Short Operation Timeout 60 Seconds

Long Operation Timeout 1536 Seconds

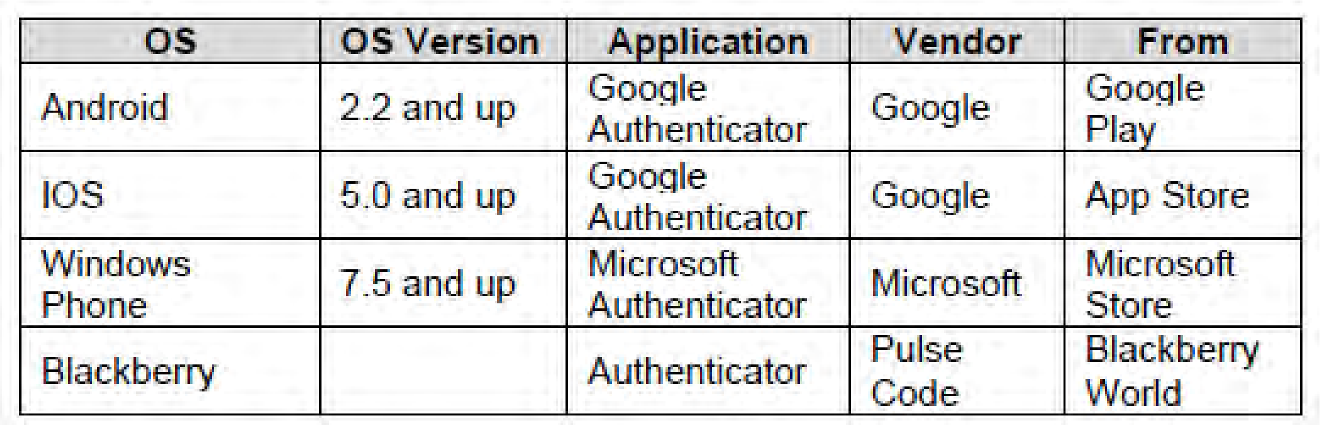
Exercise

Change and use the access settings

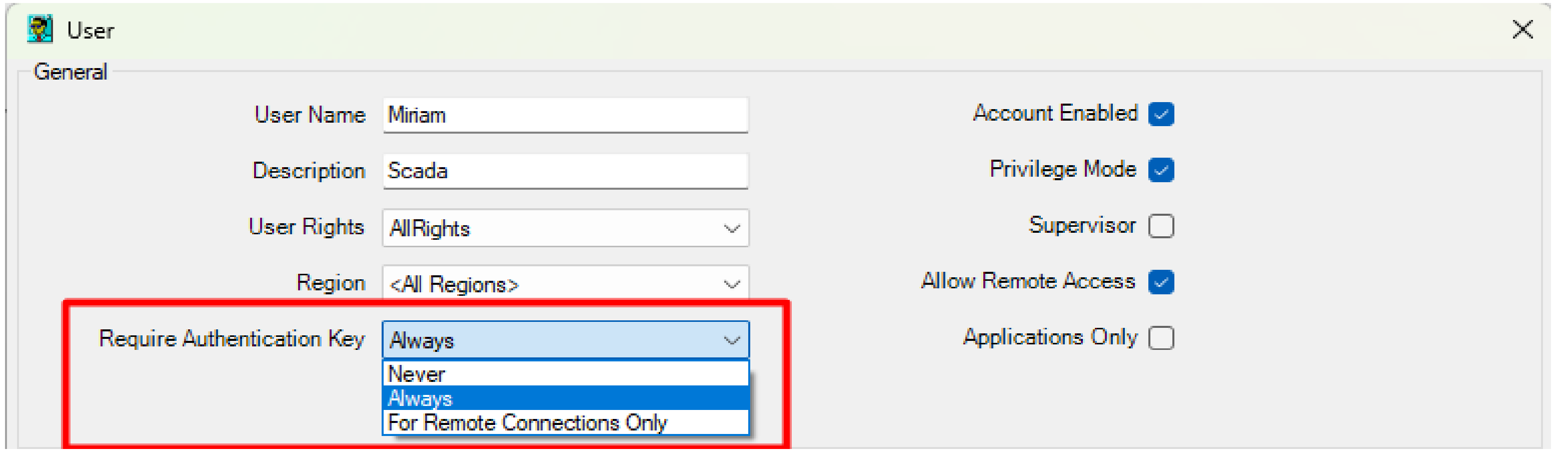
- Using STC Explorer:
  - Enable the inactivity timeout for the system.
  - Set a number of login attempts.
  - Set password requirements.

- Using SmartVU:
  - Enable the timeout logins.

- Survalent 2FA uses Time Based One-Time Password Algorithm
- No internet connectivity required
- Time must match between SCADA and authenticator app
- Authentication key can be reset from user editor.
- Supported applications:



OS	OS Version	Application	Vendor	From
Android	2.2 and up	Google Authenticator	Google	Google Play
IOS	5.0 and up	Google Authenticator	Google	App Store
Windows Phone	7.5 and up	Microsoft Authenticator	Microsoft	Microsoft Store
Blackberry		Authenticator	Pulse Code	Blackberry World



User

General

User Name: Miriam

Description: Scada

User Rights: AllRights

Region: <All Regions>

Require Authentication Key: Always

- Never
- Always
- For Remote Connections Only

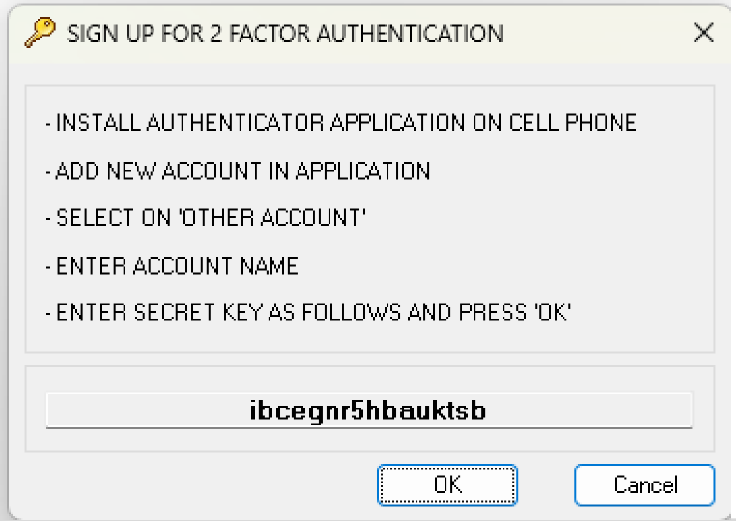
Account Enabled ☑

Privilege Mode ☑

Supervisor □

Allow Remote Access ☑

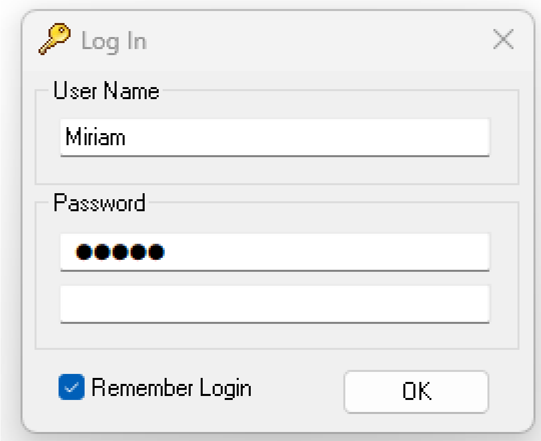
Applications Only □



SIGN UP FOR 2 FACTOR AUTHENTICATION

- INSTALL AUTHENTICATOR APPLICATION ON CELL PHONE
- ADD NEW ACCOUNT IN APPLICATION
- SELECT ON 'OTHER ACCOUNT'
- ENTER ACCOUNT NAME
- ENTER SECRET KEY AS FOLLOWS AND PRESS 'OK'

ibcegnr5hbauktsb

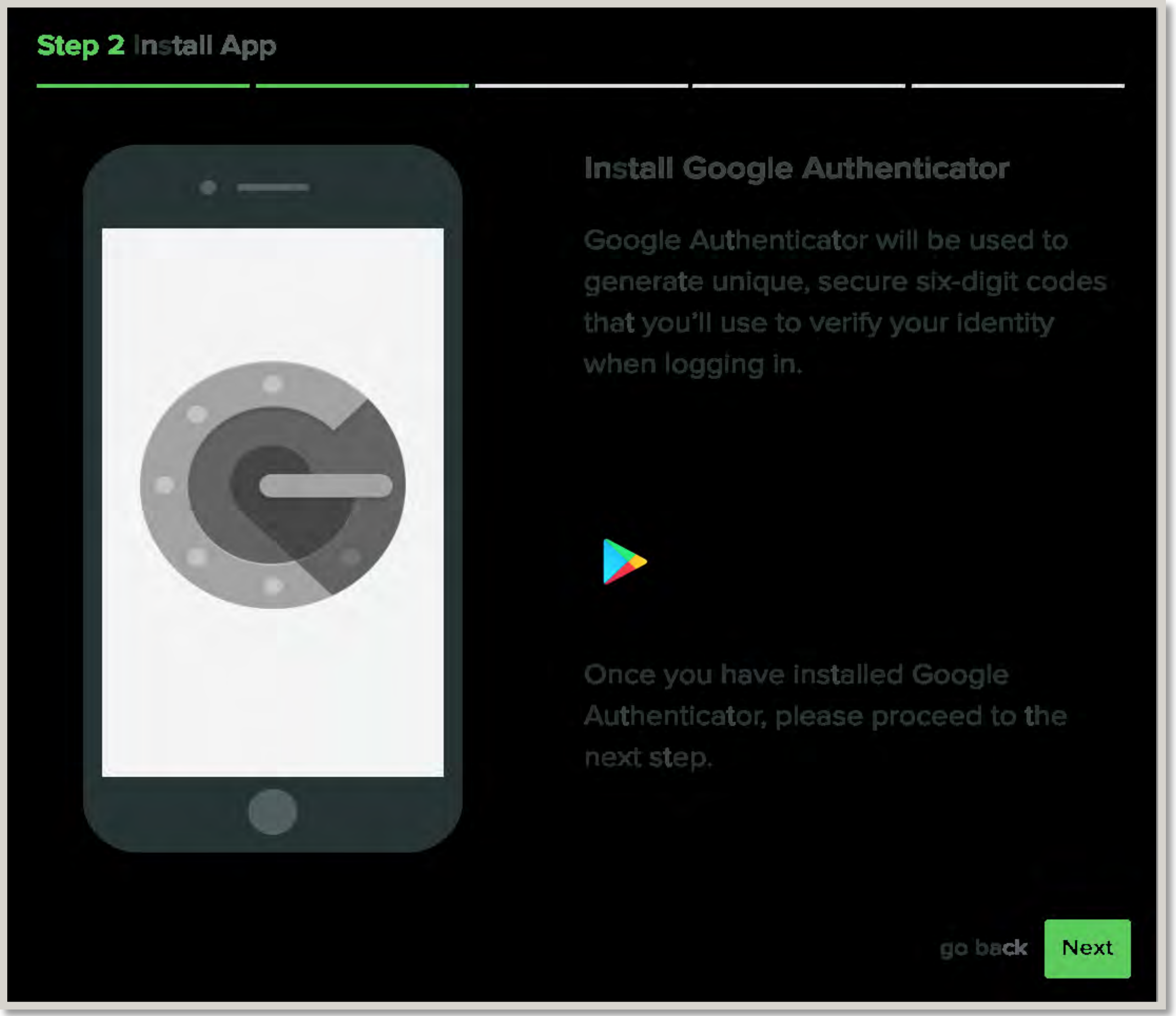


Log In

User Name: Miriam

Password: ●●●●●

☑ Remember Login

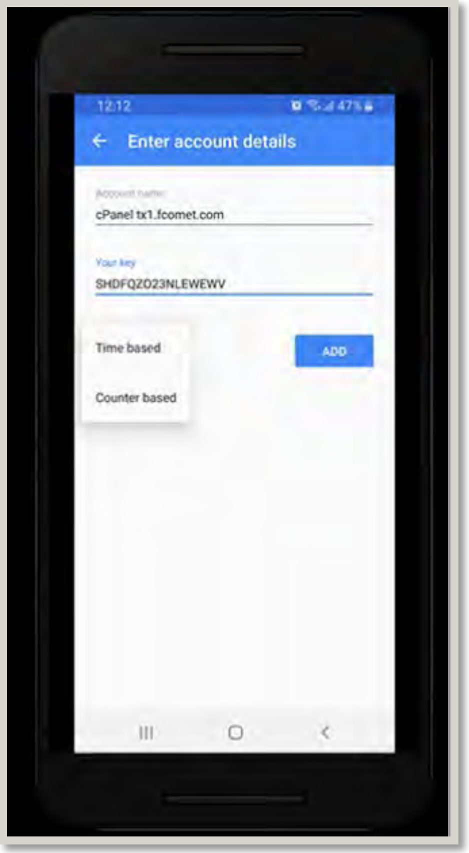


Step 2 Install App

Install Google Authenticator

Google Authenticator will be used to generate unique, secure six-digit codes that you'll use to verify your identity when logging in.

Once you have installed Google Authenticator, please proceed to the next step.



12:12 47%

Enter account details

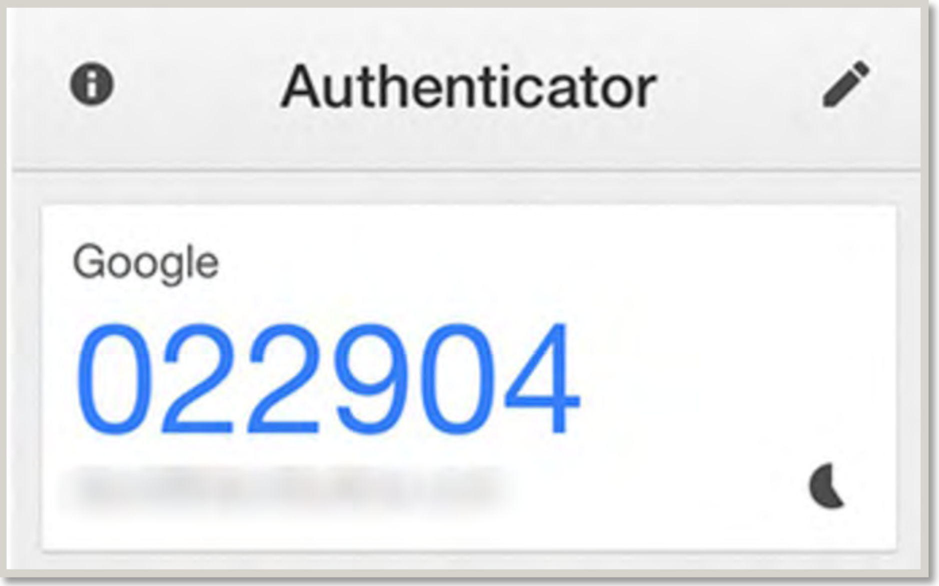
Account name
cPanel tx1.fcomet.com

Your key
SHDFQZO23NLEWEWV

Exercise

Enable Two-Factor Authentication

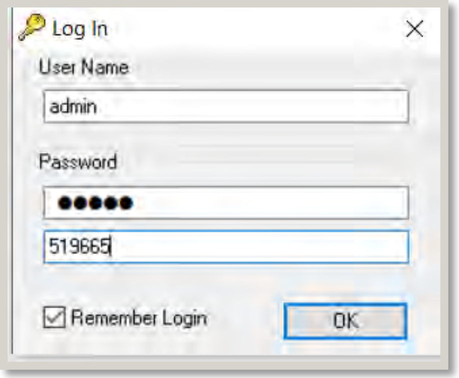
- Using STC Explorer:
  - Enable the key requirement for a user.
  - Set it to Always.
- Using your cellphone:
  - Download Google Authenticator and follow the instructions to sign up:
    - Add new account in the application
    - Select ‘Other Account’
    - Enter account name
    - Enter secret key and press ok



Authenticator

Google

022904



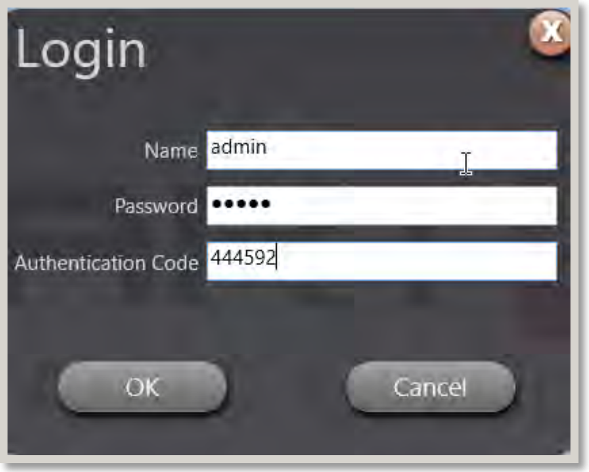
Log In

User Name: admin

Password: ●●●●●

519665

☑ Remember Login



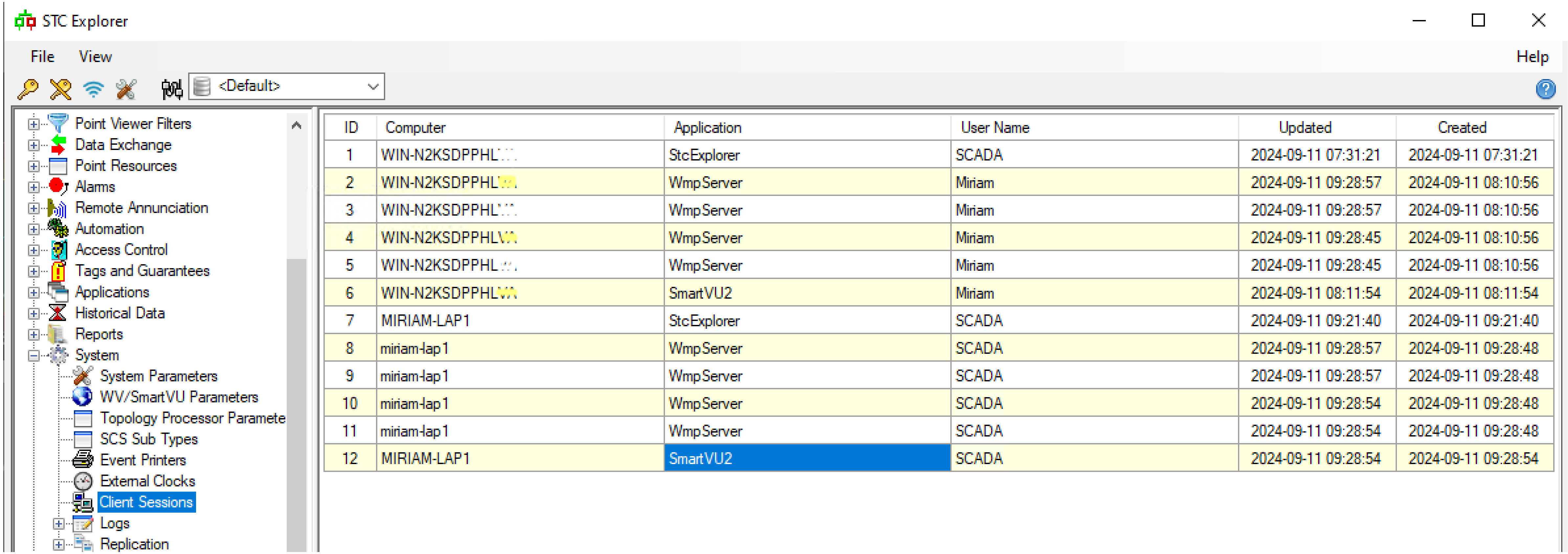
Login

Name: admin

Password: •••••

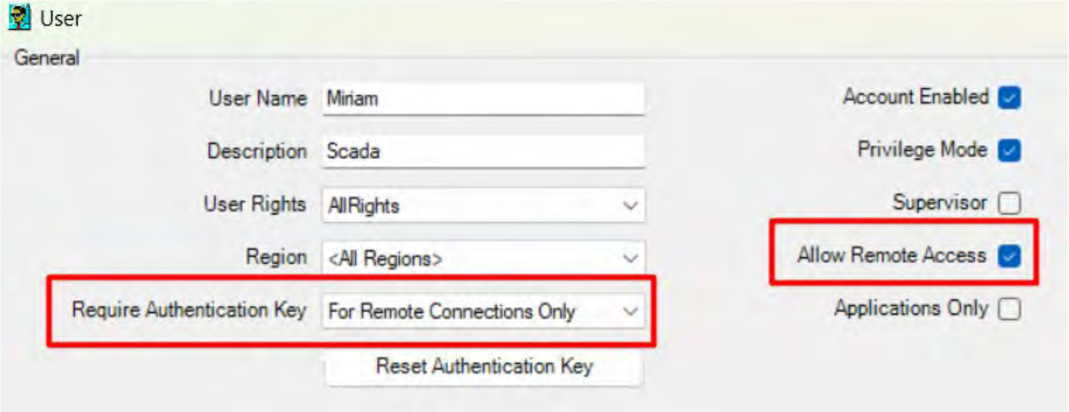
Authentication Code: 444592

- List of active sessions of client application connected to server
- Includes Scada Explorer, Point Viewers, SmartVU
- Shows computer name on which session is active
- Helpful to manage situation where there's limited concurrent SmartVU licenses



ID	Computer	Application	User Name	Updated	Created
1	WIN-N2KSDPPHL	StcExplorer	SCADA	2024-09-11 07:31:21	2024-09-11 07:31:21
2	WIN-N2KSDPPHL	WmpServer	Miriam	2024-09-11 09:28:57	2024-09-11 08:10:56
3	WIN-N2KSDPPHL	WmpServer	Miriam	2024-09-11 09:28:57	2024-09-11 08:10:56
4	WIN-N2KSDPPHLV	WmpServer	Miriam	2024-09-11 09:28:45	2024-09-11 08:10:56
5	WIN-N2KSDPPHL	WmpServer	Miriam	2024-09-11 09:28:45	2024-09-11 08:10:56
6	WIN-N2KSDPPHL	SmartVU2	Miriam	2024-09-11 08:11:54	2024-09-11 08:11:54
7	MIRIAM-LAP1	StcExplorer	SCADA	2024-09-11 09:21:40	2024-09-11 09:21:40
8	miriam-lap1	WmpServer	SCADA	2024-09-11 09:28:57	2024-09-11 09:28:48
9	miriam-lap1	WmpServer	SCADA	2024-09-11 09:28:57	2024-09-11 09:28:48
10	miriam-lap1	WmpServer	SCADA	2024-09-11 09:28:54	2024-09-11 09:28:48
11	miriam-lap1	WmpServer	SCADA	2024-09-11 09:28:54	2024-09-11 09:28:48
12	MIRIAM-LAP1	SmartVU2	SCADA	2024-09-11 09:28:54	2024-09-11 09:28:54

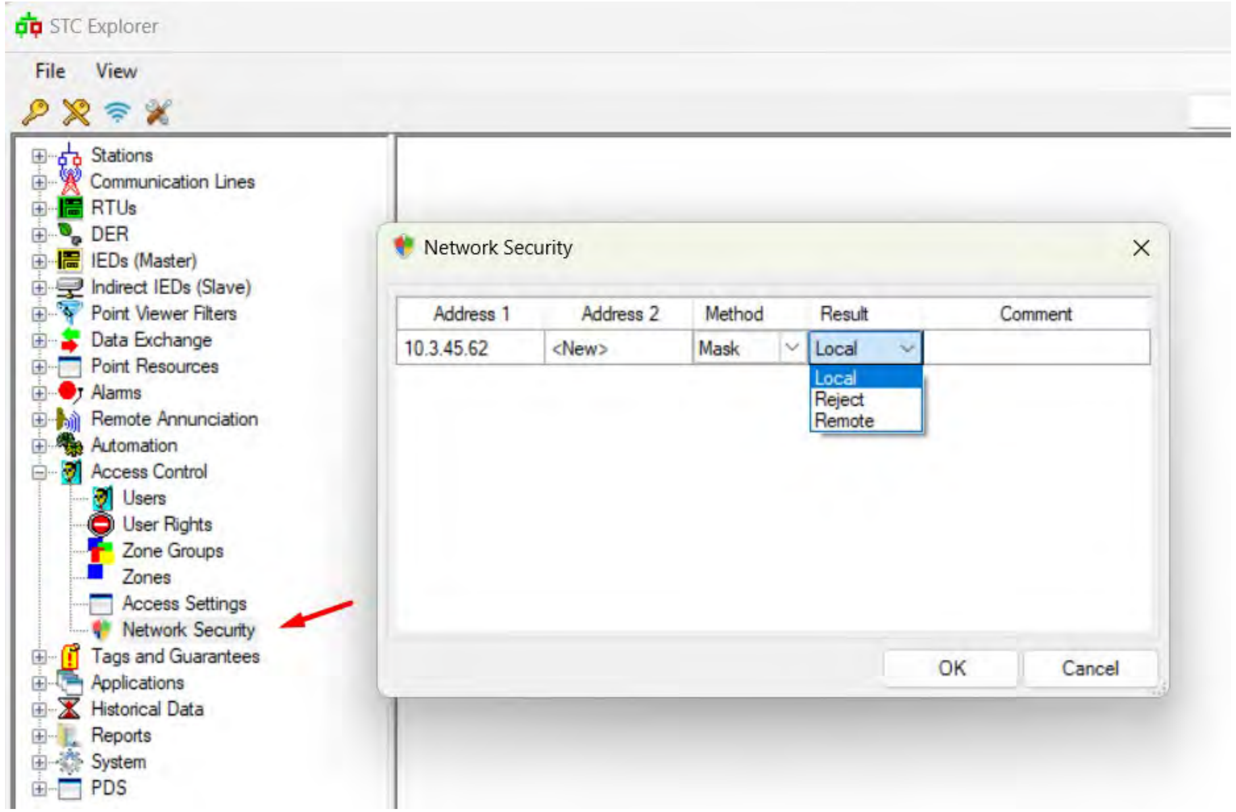
- Client Connection to Scada Server can be administered using Scada explorer
- Access Control > Network Security
- Rules can be added to restrict access to certain subnet/range of network IP address
- Each rule can mark the IP address as Local, Remote or Reject.
- Certain range of IP address may be present in multiple rules with different results
- Rules evaluation stops at the first match.
- Users can be setup to have remote connection ability
- Two factor authentication can be restricted to remote connections



User

General

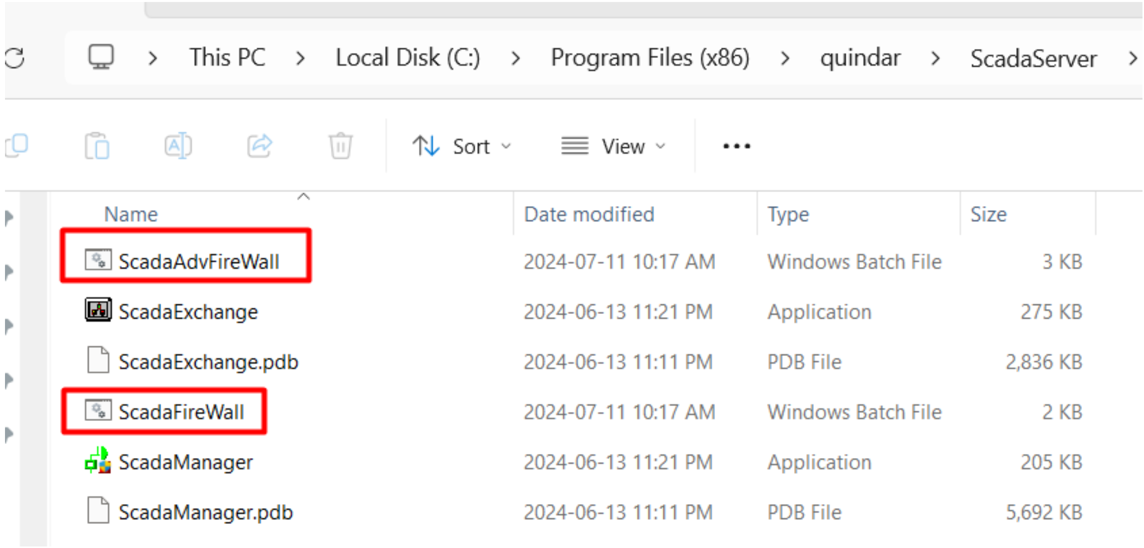
User Name	Miriam	Account Enabled	☑
Description	Scada	Privilege Mode	☑
User Rights	AllRights	Supervisor	□
Region	<All Regions>	Allow Remote Access	☑
Require Authentication Key	For Remote Connections Only	Applications Only	□



Network Security

Address 1	Address 2	Method	Result	Comment
10.3.45.62	<New>	Mask	Local	

- Windows firewall block traffic by default if enabled.
- Batch file is provided in Scada Server installation by default to make exceptions
- These exceptions are specific for SCADA application to be able to communicate
- Two files ScadaFireWall.bat and ScadaAdvFireWall.bat
- ScadaAdvFireWall.bat is suitable for newer windows version
- Run it using by double clicking it.



This PC > Local Disk (C:) > Program Files (x86) > quindar > ScadaServer >

Name	Date modified	Type	Size
ScadaAdvFireWall	2024-07-11 10:17 AM	Windows Batch File	3 KB
ScadaExchange	2024-06-13 11:21 PM	Application	275 KB
ScadaExchange.pdb	2024-06-13 11:11 PM	PDB File	2,836 KB
ScadaFireWall	2024-07-11 10:17 AM	Windows Batch File	2 KB
ScadaManager	2024-06-13 11:21 PM	Application	205 KB
ScadaManager.pdb	2024-06-13 11:11 PM	PDB File	5,692 KB

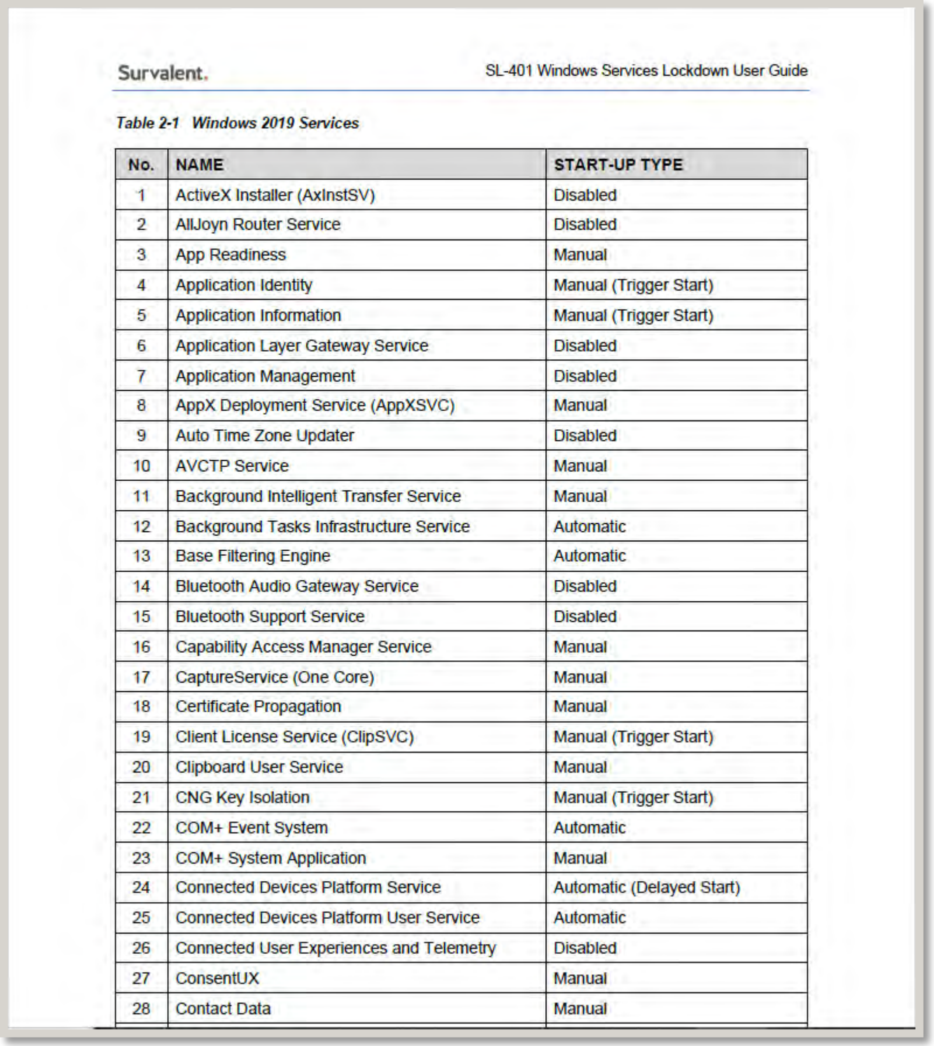
Survalent.

SurvalentONE

SL-401

Windows Services Lockdown Guide

User Guide



Survalent. SL-401 Windows Services Lockdown User Guide

Table 2-1 Windows 2019 Services

No.	NAME	START-UP TYPE
1	ActiveX Installer (AxInstSV)	Disabled
2	AllJoyn Router Service	Disabled
3	App Readiness	Manual
4	Application Identity	Manual (Trigger Start)
5	Application Information	Manual (Trigger Start)
6	Application Layer Gateway Service	Disabled
7	Application Management	Disabled
8	AppX Deployment Service (AppXSVC)	Manual
9	Auto Time Zone Updater	Disabled
10	AVCTP Service	Manual
11	Background Intelligent Transfer Service	Manual
12	Background Tasks Infrastructure Service	Automatic
13	Base Filtering Engine	Automatic
14	Bluetooth Audio Gateway Service	Disabled
15	Bluetooth Support Service	Disabled
16	Capability Access Manager Service	Manual
17	CaptureService (One Core)	Manual
18	Certificate Propagation	Manual
19	Client License Service (ClipSVC)	Manual (Trigger Start)
20	Clipboard User Service	Manual
21	CNG Key Isolation	Manual (Trigger Start)
22	COM+ Event System	Automatic
23	COM+ System Application	Manual
24	Connected Devices Platform Service	Automatic (Delayed Start)
25	Connected Devices Platform User Service	Automatic
26	Connected User Experiences and Telemetry	Disabled
27	ConsentUX	Manual
28	Contact Data	Manual

- SL-401 Windows Service Lockdown
- Eliminate services that are not required to run ADMS system
- Enhance overall security and reliability of ADMS server
- Available for Windows server 2019, 2016, 2012 and Windows 10
- In place when servers provided by Survalent

- Changes made by client application such as Scada explorer, point viewers can be logged.
- STC Explorer > System > Logs
- Up to 100 tables can be audited. Below are the suggested tables:

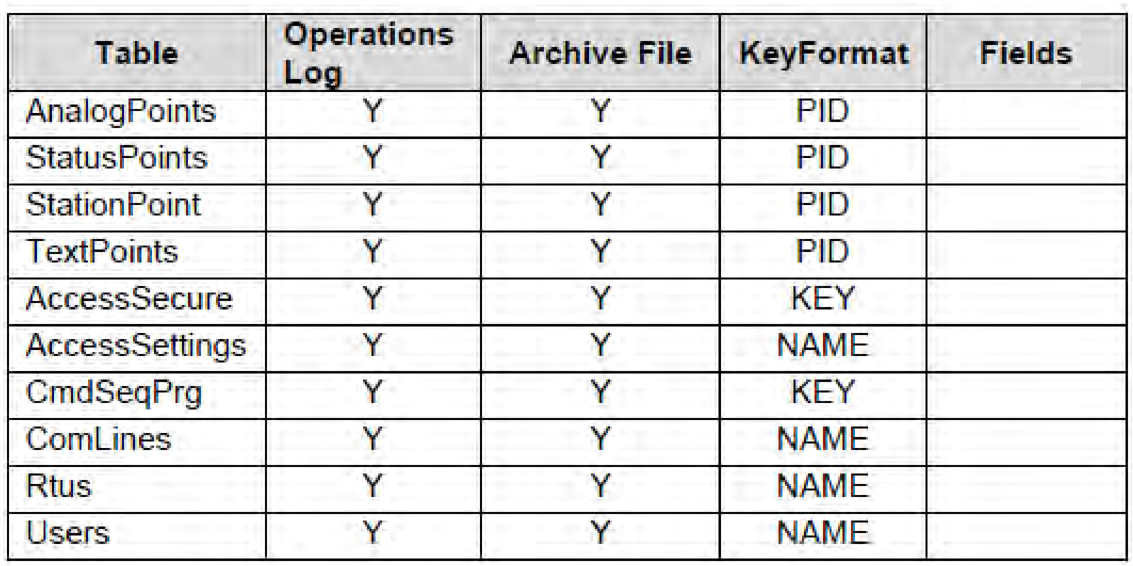
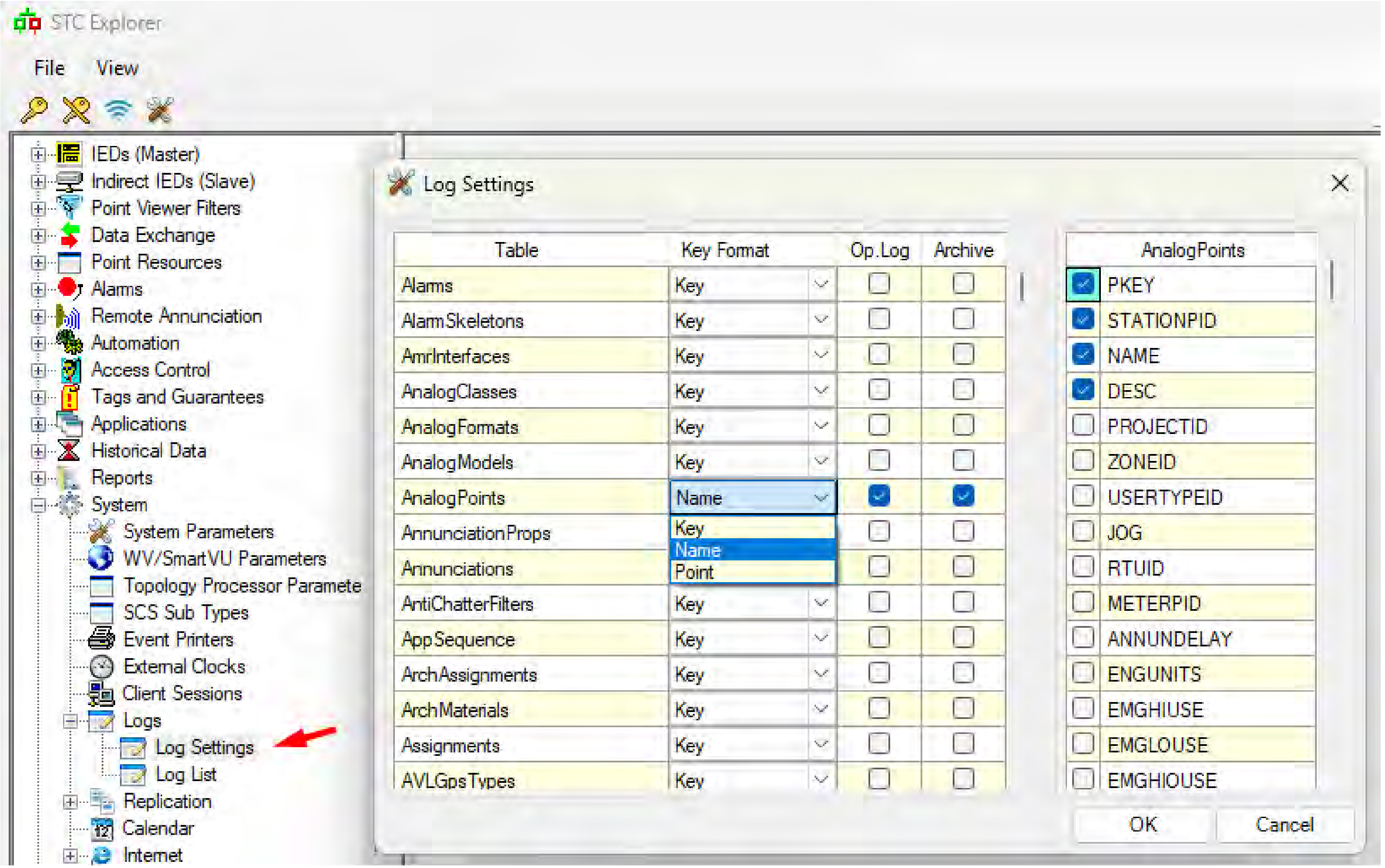


Table	Operations Log	Archive File	KeyFormat	Fields
AnalogPoints	Y	Y	PID	
StatusPoints	Y	Y	PID	
StationPoint	Y	Y	PID	
TextPoints	Y	Y	PID	
AccessSecure	Y	Y	KEY	
AccessSettings	Y	Y	NAME	
CmdSeqPrg	Y	Y	KEY	
ComLines	Y	Y	NAME	
Rtus	Y	Y	NAME	
Users	Y	Y	NAME	

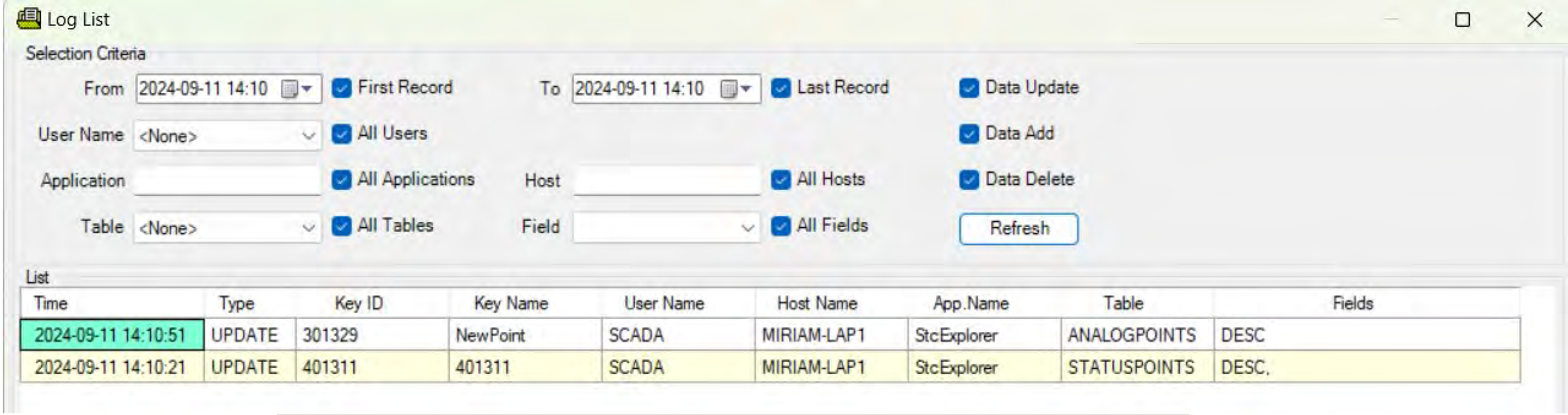


- IEDs (Master)
- Indirect IEDs (Slave)
- Point Viewer Filters
- Data Exchange
- Point Resources
- Alarms
- Remote Annunciation
- Automation
- Access Control
- Tags and Guarantees
- Applications
- Historical Data
- Reports
- System
  - System Parameters
  - WV/SmartVU Parameters
  - Topology Processor Paramete
  - SCS Sub Types
  - Event Printers
  - External Clocks
  - Client Sessions
  - Logs
    - Log Settings
    - Log List
  - Replication
  - Calendar
  - Internet

Log Settings

Table	Key Format	Op.Log	Archive
Alarms	Key	□	□
AlarmSkeletons	Key	□	□
AmrInterfaces	Key	□	□
AnalogClasses	Key	□	□
AnalogFormats	Key	□	□
AnalogModels	Key	□	□
AnalogPoints	Name	☑	☑
AnnunciationProps		□	□
Annunciations		□	□
AntiChatterFilters	Key	□	□
AppSequence	Key	□	□
ArchAssignments	Key	□	□
ArchMaterials	Key	□	□
Assignments	Key	□	□
AVLGpsTypes	Key	□	□

	AnalogPoints
☑	PKEY
☑	STATIONPID
☑	NAME
☑	DESC
□	PROJECTID
□	ZONEID
□	USERTYPEID
□	JOG
□	RTUID
□	METERPID
□	ANNUNDELAY
□	ENGUNITS
□	EMGHIUSE
□	EMGLOUSE
□	EMGHIOUSE



Log List

Selection Criteria

From 2024-09-11 14:10 ☑ First Record To 2024-09-11 14:10 ☑ Last Record ☑ Data Update

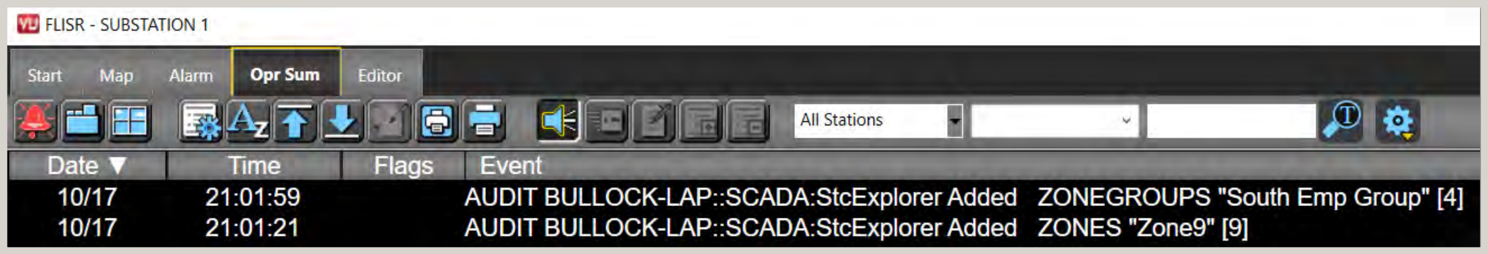
User Name <None> ☑ All Users ☑ Data Add

Application ☑ All Applications Host ☑ All Hosts ☑ Data Delete

Table <None> ☑ All Tables Field ☑ All Fields

List

Time	Type	Key ID	Key Name	User Name	Host Name	App.Name	Table	Fields
2024-09-11 14:10:51	UPDATE	301329	NewPoint	SCADA	MIRIAM-LAP1	StcExplorer	ANALOGPOINTS	DESC
2024-09-11 14:10:21	UPDATE	401311	401311	SCADA	MIRIAM-LAP1	StcExplorer	STATUSPOINTS	DESC,



FLISR - SUBSTATION 1

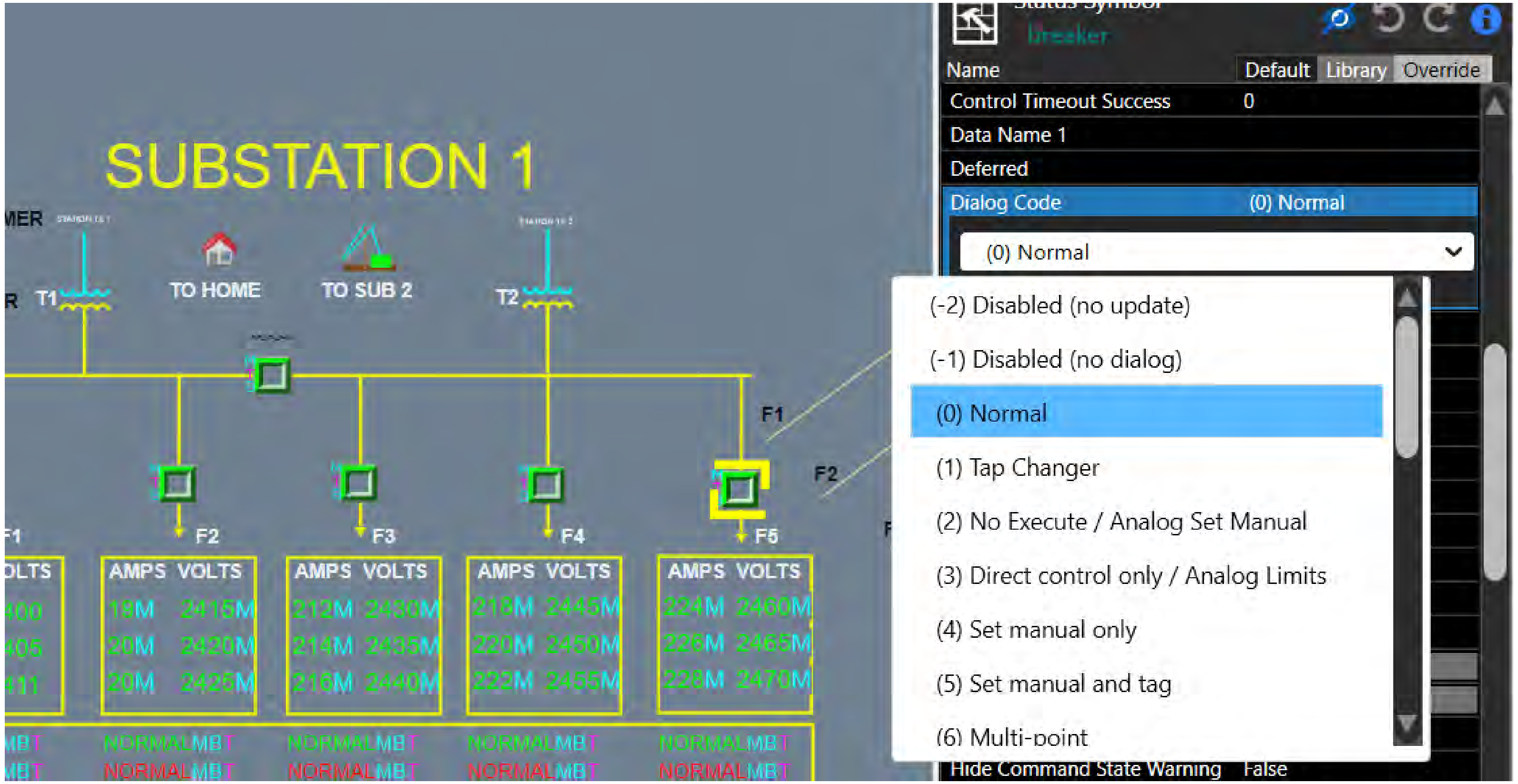
```
Date ▼   Time       Flags  Event
10/17    21:01:59          AUDIT BULLOCK-LAP::SCADA:StcExplorer Added  ZONEGROUPS "South Emp Group" [4]
10/17    21:01:21          AUDIT BULLOCK-LAP::SCADA:StcExplorer Added  ZONES "Zone9" [9]
```

Exercise

Enable the audit logging

- Using STC Explorer:
  - Enable the logging for the StatusPoints table. Select key as format and the first 4 options: pkey, stationpid, name, desc.
  - Create a new status point and edit another one.
  - Enable the logging for the AnalogPoints table. Select name as format and the first 4 options: pkey, stationpid, name, desc.
  - Create a new analog point and edit another one.

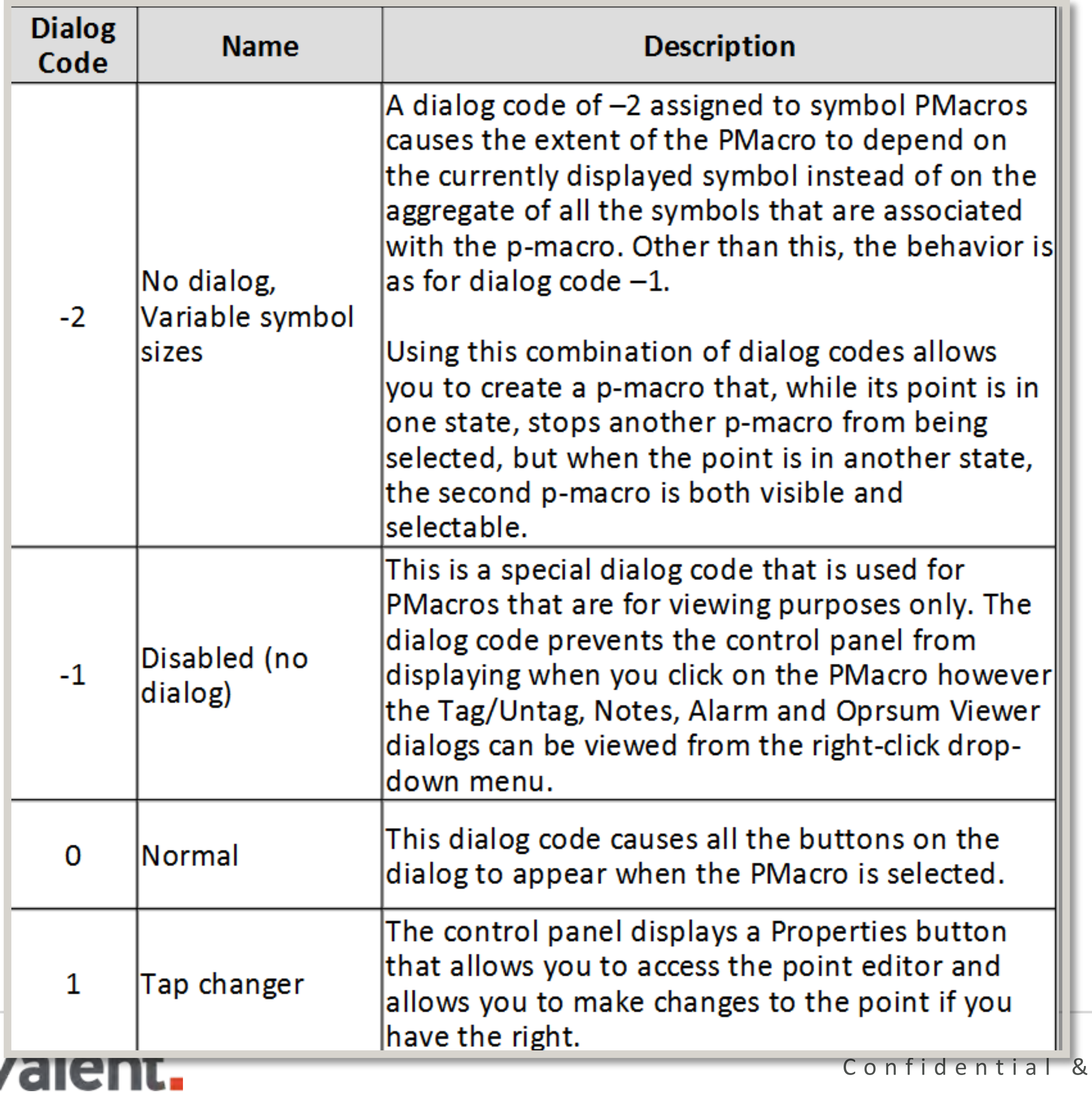
- Pmacros in SmartVU map can be restricted to have limited dialogue options

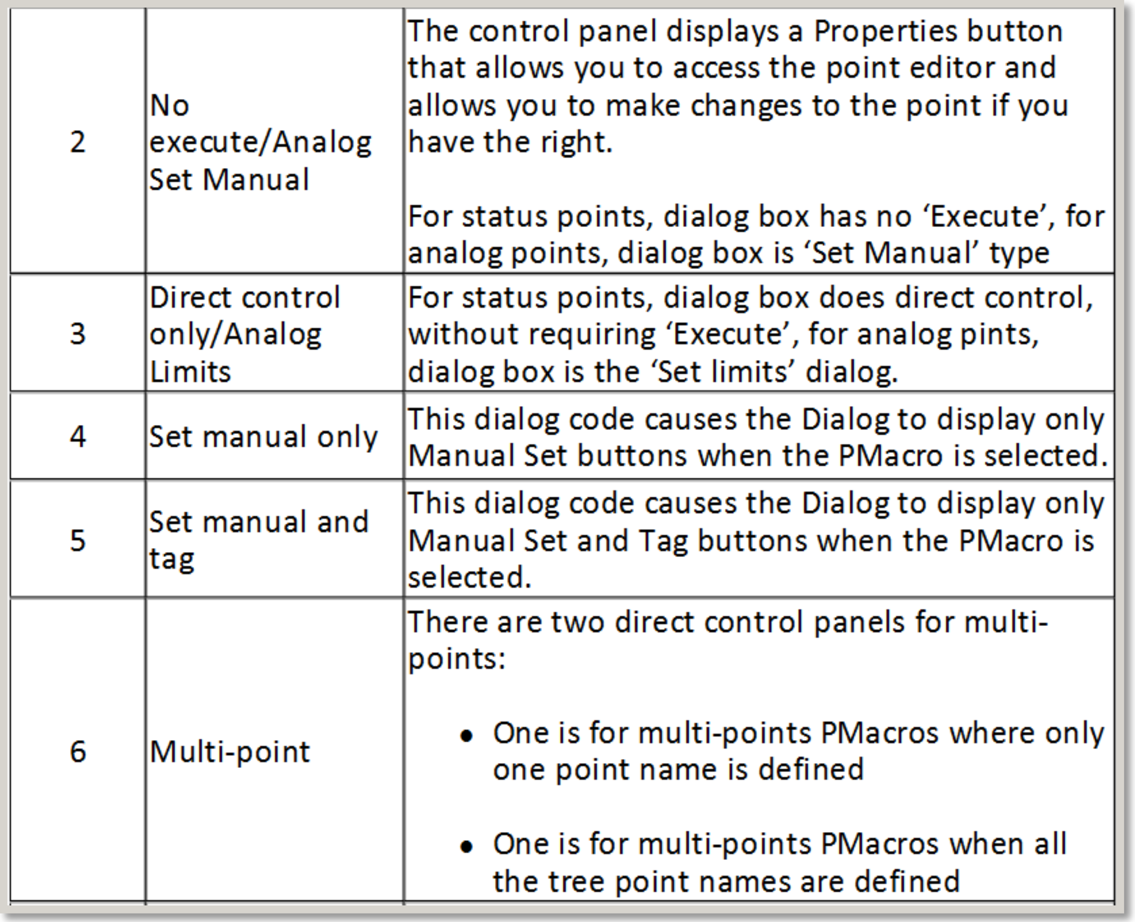


Name	Default	Library	Override
Control Timeout Success	0		
Data Name 1			
Deferred			
Dialog Code	(0) Normal		
Hide Command State Warning	False		

(0) Normal

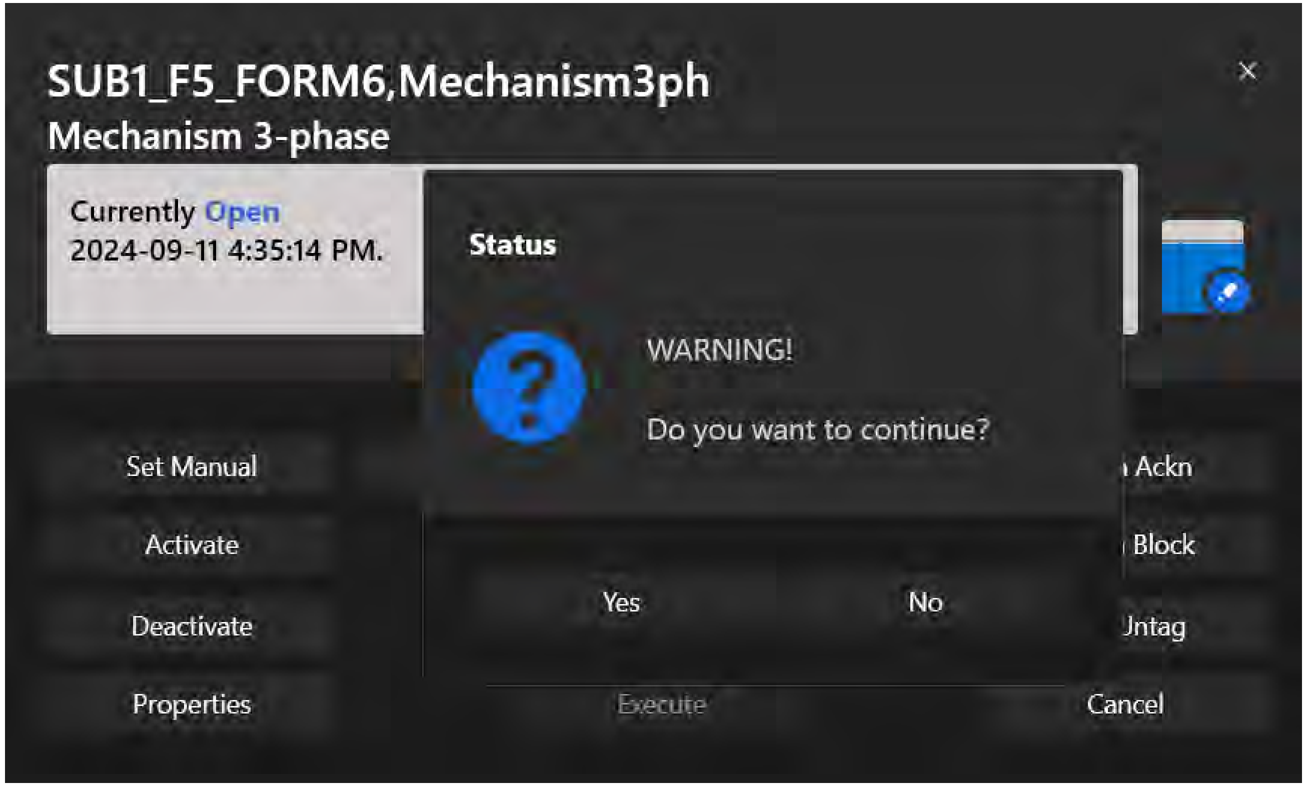
- (-2) Disabled (no update)
- (-1) Disabled (no dialog)
- (0) Normal
- (1) Tap Changer
- (2) No Execute / Analog Set Manual
- (3) Direct control only / Analog Limits
- (4) Set manual only
- (5) Set manual and tag
- (6) Multi-point





Dialog Code	Name	Description
-2	No dialog, Variable symbol sizes	A dialog code of –2 assigned to symbol PMacros causes the extent of the PMacro to depend on the currently displayed symbol instead of on the aggregate of all the symbols that are associated with the p-macro. Other than this, the behavior is as for dialog code –1. Using this combination of dialog codes allows you to create a p-macro that, while its point is in one state, stops another p-macro from being selected, but when the point is in another state, the second p-macro is both visible and selectable.
-1	Disabled (no dialog)	This is a special dialog code that is used for PMacros that are for viewing purposes only. The dialog code prevents the control panel from displaying when you click on the PMacro however the Tag/Untag, Notes, Alarm and Oprsum Viewer dialogs can be viewed from the right-click drop-down menu.
0	Normal	This dialog code causes all the buttons on the dialog to appear when the PMacro is selected.
1	Tap changer	The control panel displays a Properties button that allows you to access the point editor and allows you to make changes to the point if you have the right.
2	No execute/Analog Set Manual	The control panel displays a Properties button that allows you to access the point editor and allows you to make changes to the point if you have the right. For status points, dialog box has no 'Execute', for analog points, dialog box is 'Set Manual' type
3	Direct control only/Analog Limits	For status points, dialog box does direct control, without requiring 'Execute', for analog pints, dialog box is the 'Set limits' dialog.
4	Set manual only	This dialog code causes the Dialog to display only Manual Set buttons when the PMacro is selected.
5	Set manual and tag	This dialog code causes the Dialog to display only Manual Set and Tag buttons when the PMacro is selected.
6	Multi-point	There are two direct control panels for multi-points: • One is for multi-points PMacros where only one point name is defined • One is for multi-points PMacros when all the tree point names are defined

- Pmacro in SmartVU can be configured to have additional warning message for Control
- Message can be customized in Pmacro resources



SUB1_F5_FORM6,Mechanism3ph

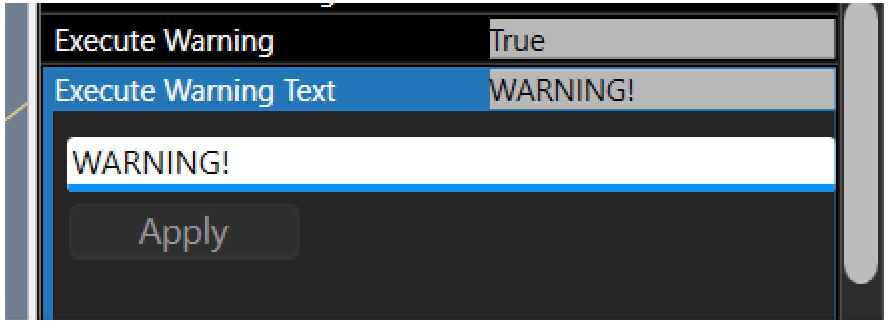
Mechanism 3-phase

Currently Open
2024-09-11 4:35:14 PM.

Status

WARNING!

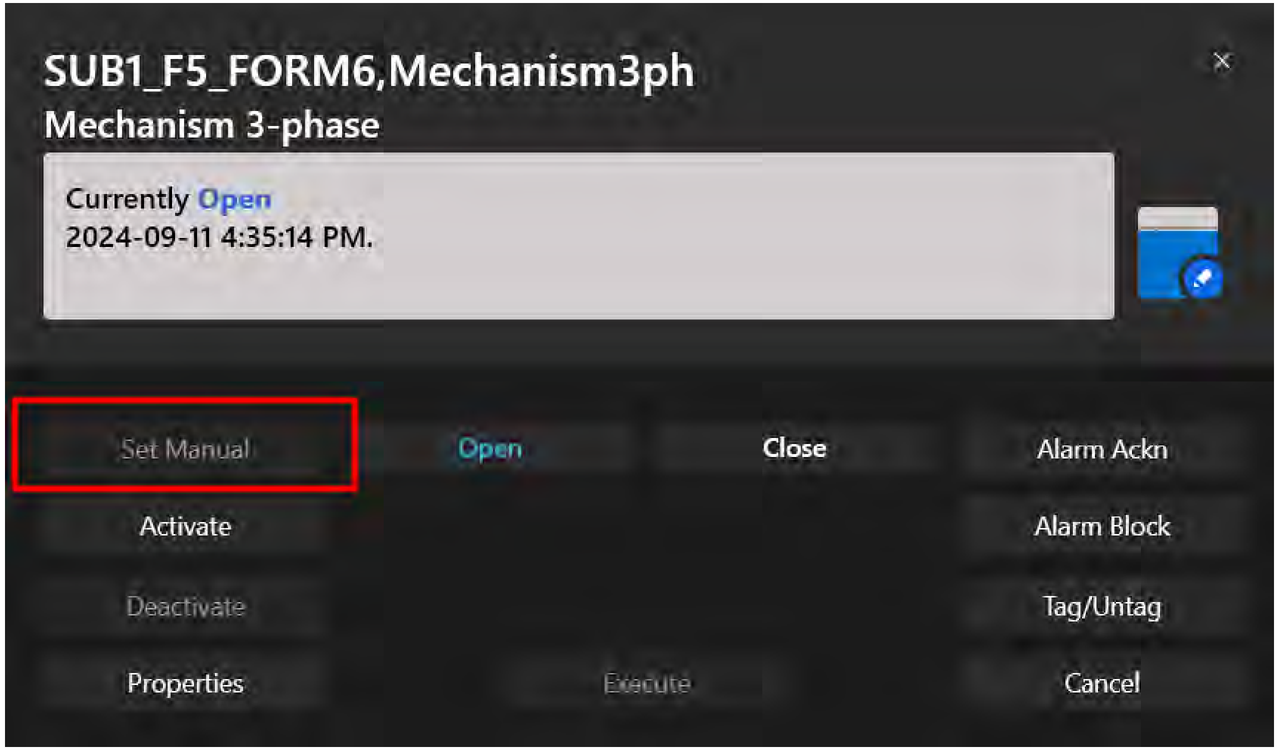
Do you want to continue?



Execute Warning	True
Execute Warning Text	WARNING!

WARNING!

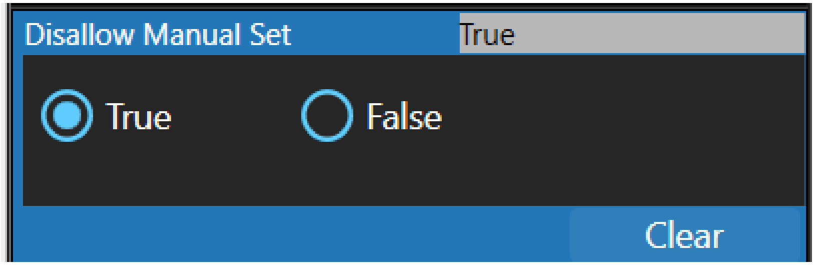
- Pmacro in SmartVU can be configured to block set manual operation



SUB1_F5_FORM6,Mechanism3ph

Mechanism 3-phase

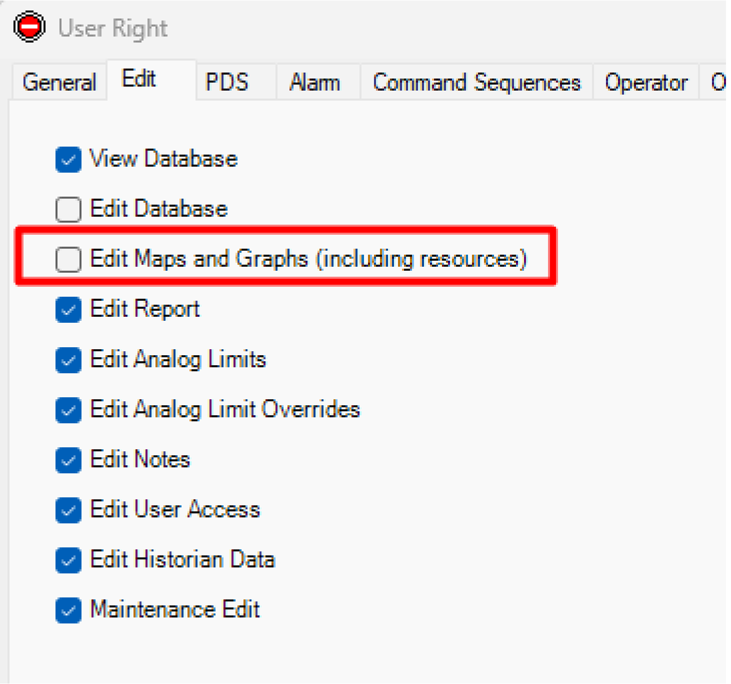
Currently Open
2024-09-11 4:35:14 PM.



Disallow Manual Set True

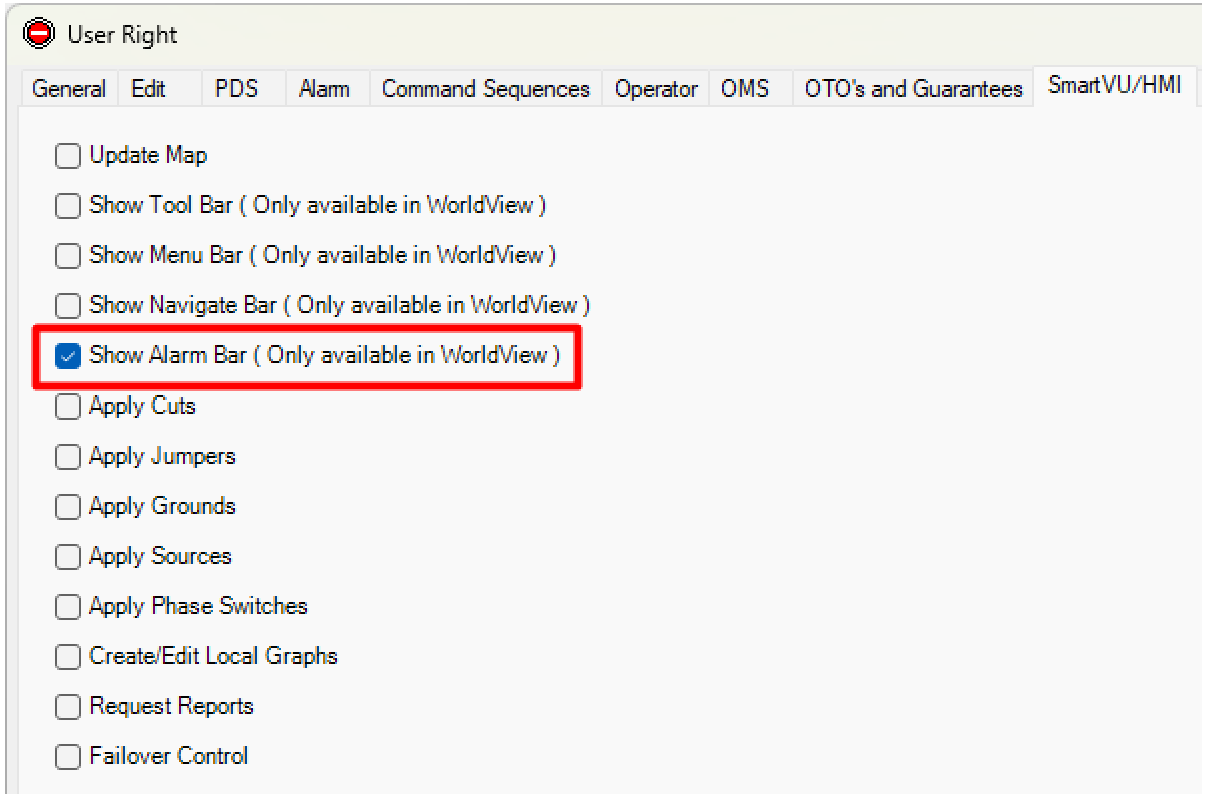
● True ○ False

- Using the User Rights, access to Alarm, OprSum tabs and Edit Mode can be disabled.



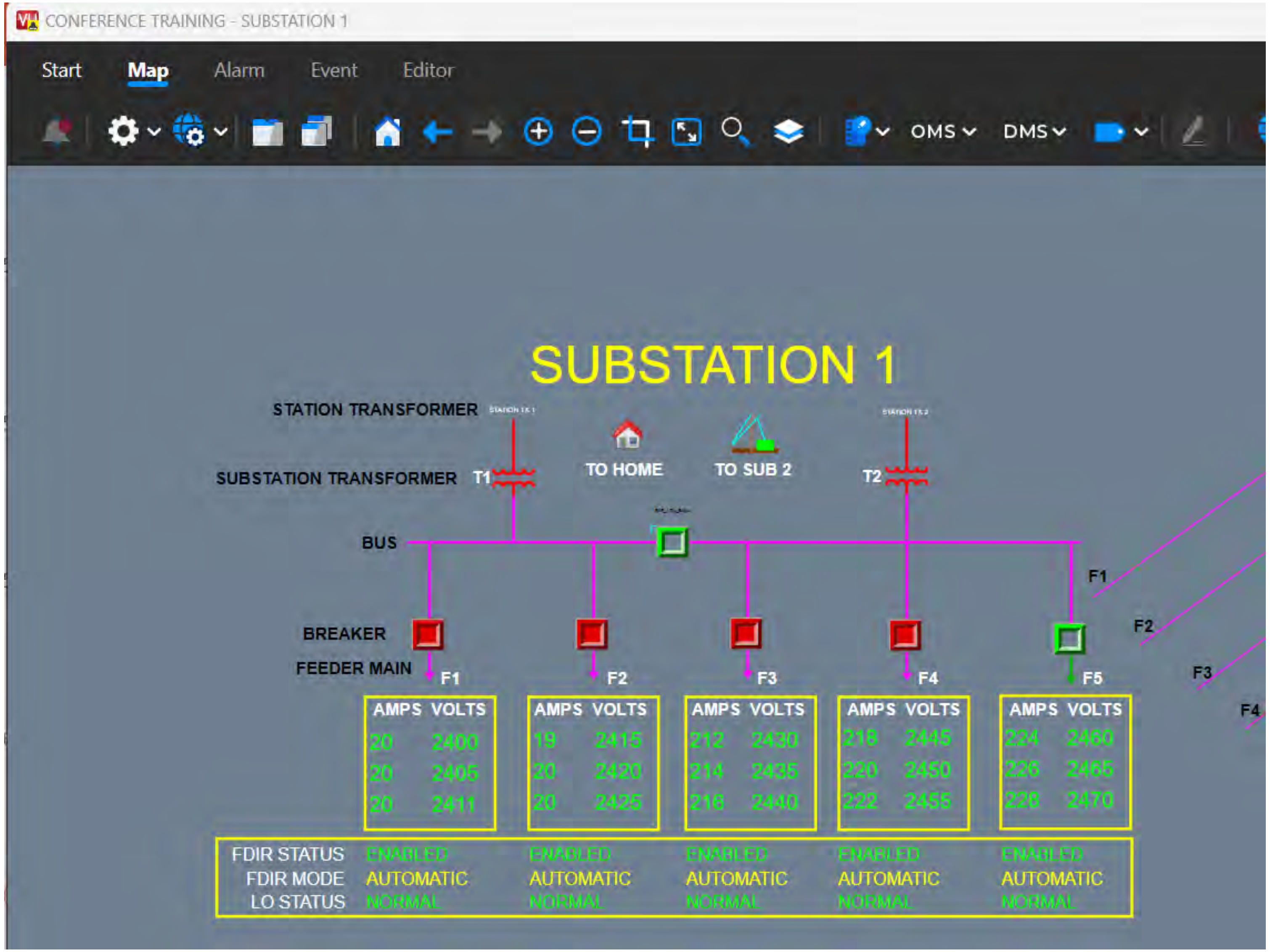
User Right

☑ View Database
□ Edit Database
□ Edit Maps and Graphs (including resources)
☑ Edit Report
☑ Edit Analog Limits
☑ Edit Analog Limit Overrides
☑ Edit Notes
☑ Edit User Access
☑ Edit Historian Data
☑ Maintenance Edit



User Right

□ Update Map
□ Show Tool Bar (Only available in WorldView)
□ Show Menu Bar (Only available in WorldView)
□ Show Navigate Bar (Only available in WorldView)
☑ Show Alarm Bar (Only available in WorldView)
□ Apply Cuts
□ Apply Jumpers
□ Apply Grounds
□ Apply Sources
□ Apply Phase Switches
□ Create/Edit Local Graphs
□ Request Reports
□ Failover Control



F1 AMPS	F1 VOLTS	F2 AMPS	F2 VOLTS	F3 AMPS	F3 VOLTS	F4 AMPS	F4 VOLTS	F5 AMPS	F5 VOLTS
20	2400	19	2415	212	2430	218	2445	224	2460
20	2405	20	2420	214	2435	220	2450	226	2465
20	2411	20	2425	216	2440	222	2455	228	2470

FDIR STATUS	ENABLED	ENABLED	ENABLED	ENABLED	ENABLED
FDIR MODE	AUTOMATIC	AUTOMATIC	AUTOMATIC	AUTOMATIC	AUTOMATIC
LO STATUS	NORMAL	NORMAL	NORMAL	NORMAL	NORMAL

Exercise

SmartVU access

- Using SmartVU:
  - Change the dialog code for in a status or analog pmacro
  - Create a warning message when executing controls.
- Using STC Explorer:
  - Change the rights to allow the access to edit mode

Survalent.

UC

Global User Conference

Questions?

CONTACT:

To create a support case, please send an email to
support@survalent.com
Please contact us for any inquiries about training or to sign up for Survalent trainings
training@survalent.com

Survalent.

UC

Global User Conference

Thank you