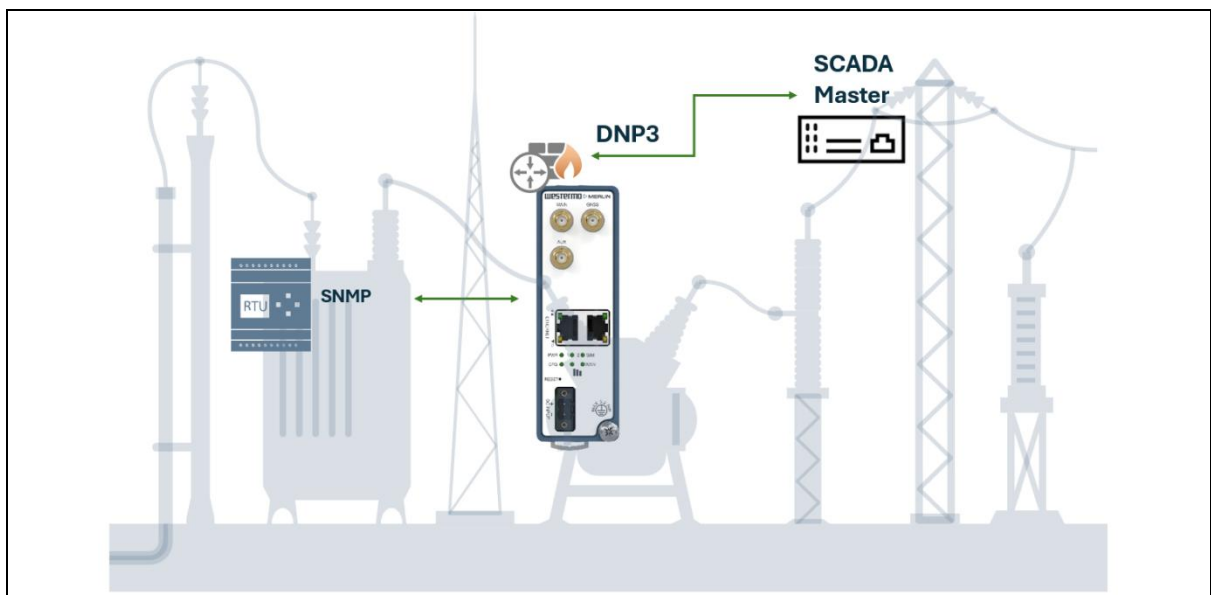


WESTERMO

Merlin SCADA Protocol Conversion

Conversion scenario: SNMP to DNP3

AN-007-WIE



Hardware Models	Merlin Series
Revision	1.02
Approval status	Approved
Date:	17 March 2026
Brief description	Merlin SCADA Protocol Conversion Scenario: SNMP to DNP3

1	Overview	3
1.1	Firmware information	3
1.2	Assumptions.....	3
1.3	Corrections	3
2	Configuring local SNMP server.....	4
2.1	Configuring SNMP	4
2.2	Configuring SNMP Version 3	5
2.3	Custom OIDs using Pass	6
2.4	Testing SNMP	7
3	Configuring IECD application.....	7
3.1	Setting up the scenario.....	8
4	Configuring Server protocol DNP3	8
4.1	Configuring DNP3 TLS.....	9
5	Configuring Master protocol – SNMP.....	10
5.1	Configuring SNMP Master	10
5.2	Configuring SNMP Master (Version 3)	11
6	Configuring data points (signal)	11
6.1	Points configuration – manual.....	11
6.2	Points configuration – CSV file	14
6.3	SNMP to DNP3 Mapping	15
7	Essential OIDs	17
7.1	MOBILE COMMUNICATION	17
7.2	NETWORK.....	18
7.3	SYSTEM.....	19
7.4	GPIOs.....	19
8	Troubleshooting.....	20
8.1	IECD status via the WebUI	20
8.2	IECD status via CLI	21
8.3	Configuring main debug level	21
8.4	Enabling debug per protocol – DNP3 (Server).....	22
8.5	Enabling debug per protocol – SNMP (Master)	22
8.6	Accessing logs using WebUI	22
8.7	Accessing logs via CLI	23

1 Overview

This application note demonstrates how to set up the IECD application for protocol conversion. The example scenario illustrates SNMP as the “Master” interface and DNP3 as the server protocol. The application note will show the typical steps required for protocol conversion configuration through web management.

A knowledge of SNMP and SCADA protocol (DNP3) parameters is required, and the setup is common for all Merlin and Westermo Ireland/Virtual Access brand routers available.

The IECD application is available in the SCADA section. You must configure Master and Server interfaces as well as at least one Data Point for signal mapping. The interfaces used to communicate with local RTUs are referred to as the Master Protocol, while the interface used to communicate with the external Master is referred to as the Server (Slave) Protocol.

The table below shows the supported SNMP protocol conversion scenarios.

Master Protocol	Server Protocol
SNMP	IEC104
SNMP	DNP3 < This Application Note
SNMP	MODBUS
SNMP	IEC61850
SNNP	MQTT

1.1 Firmware information

Firmware version: **SXL-25.05.45.000** or newer.

1.2 Assumptions

This application note shows the Merlin 3100 router and assumes the router has a factory default configuration. Instructions can be applied to other routers in the Merlin Series.

1.3 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to support.ie@westermo.com

Requests for new application notes can be sent to the same address.

2 Configuring local SNMP server

2.1 Configuring SNMP

Browse to the SNMPD configuration page via the WebUI and follow the steps below.

1 Agent System VACM Trap Receiver Inform Receiver USM Users

Generic Agent Configuration

Agent Enabled

Agent Address

- Defines a list of listening addresses, on which to receive incoming SNMP requests

Figure 1: Agent Settings

1. Click **Agent**.
2. Set the **Agent Address**. Default address is 0.0.0.0:161

3 Agent System VACM Trap Receiver Inform Receiver USM Users

VACM Configuration

VACM: COM2SEC Settings

Mapping of SNMPv1 or SNMPv2c community strings to security names

Source	Community String	Security Name
com2sec_1	<input type="text"/>	<input type="text"/>

5 6 7

4 ADD

DELETE

Figure 2: VACM Settings

3. Click **VACM**.
4. Set a name for COM2SEC settings and click **ADD** to create a new COM2SEC rule.
5. Set the **Source** from the dropdown list. Configure custom source by selecting the **custom** option.
6. Set **Community String**.
7. Set **Security Name**.

VACM: Group Settings

Maps a security name into a named group

Security Name	Group	Version
group1_com2sec_pub	public	SNMPv1

9 10 11

8 ADD

DELETE

Figure 3: VACM Settings

8. Set a name for Group Settings and click **ADD** to create a new group rule.

9. Assign the **Security Name**.
10. Select the **Group**. Currently, only two unique groups (public and private) can be selected.
11. Set the **Version**.

Figure 4: VACM Settings

12. Set a name for View Settings and click **ADD** to create a new view rule.
13. Set the **Name**.
14. Set the **Type** (included or excluded)
15. Set the **OID**.

Figure 5: VACM Settings

16. Set a name for Access Settings and click **ADD** to create a new access rule.
17. Select the **Group**. Default value is public.
18. Select the **Version**. Default value is Any.
19. Select the **level**. Default value is noauth. For version 3, select other.
20. Select the **Read**. View name will be displayed here.
21. Click on **Save & Apply** button on the bottom of the page, to save the configuration and run/restart IECD application.

2.2 Configuring SNMP Version 3

To configure SNMP version 3, a USM user needs to be added. This can be done through the "USM Users" tab on the WebUI.

Figure 6: USM Users Settings

1. Click **ADD** to create a new USM User.
2. Set the **Username**.
3. Select the **Authentication Protocol** (None, MD5, or SHA) .
4. Set the **Authentication Password**.
5. Set the **Privacy Protocol** (None, DES, or AES).
6. Set the **Privacy Password**.
7. Set the **OID** to restrict this user to. This is similar to view restrictions in v1 and v2c.

2.3 Custom OIDs using Pass

Custom OIDs can be created using "Pass" feature in SNMP that allows users to define their own custom OIDs and link them to internal User Defined Script. This is useful when the user wants SNMP to return data that isn't available in the device's MIBs. Currently, pass feature can only be configured using CLI.

Requests for additional MIB OID parameters are welcome and should be addressed to support.ie@westermo.com

```
package uds
config script 'test_pass'
    option enabled 'yes'
    option exec_type 'none'
    list text 'param=$1'
    list text 'oid=$2'
    list text '[ param = "-n" ] && exit'
    list text 'echo "$oid"'
    list text 'echo "integer"'
    list text 'ifconfig | grep RX\ packets: | head -n 1 | awk "{print \$2}" | cut -d: -f2'
```

Figure 7: UDS Settings

1. Define the script in the UDS package, the script will be generated in the /var/uds folder.

```
config pass 'test_pass'
    option miboid '.1.3.6.1.4.1.2078.3.14.70'
    option prog '/var/uds/test_pass'
```

Figure 8: SNMPD Settings

2. In SNMPD application, set the script path and assign the custom OID. When this OID is queried, SNMPD will execute the script and return its output as expected.

2.4 Testing SNMP

Basic tests can be performed with NET-SNMP utility available on any Linux distribution. User should load MiBs to the system to enable translation of OID definitions.

```
snmpwalk -v1 -c testpublic -m ALL -M +/usr/share/snmp/mibs -OT <Device IP>:161
.1.3.6.1.4.1.2078

ls -la /usr/share/snmp/mibs
total 372
[...]
-rw-r--r-- 1 bob bob 5650 Feb 19 2024 VA-MODEM-MIB

Out:

[...]
VA-MODEM-MIB::modemGsmImei.1 = STRING: 3597790810141844

---

snmpget -v1 -c testpublic <Device IP>:161 .1.3.6.1.4.1.2078.3.1.2.2.1.14.1
iso.3.6.1.4.1.2078.3.1.2.2.1.14.1 = STRING: "3597790810141844"
```

3 Configuring IECD application

Browse to the IECD configuration page via the WebUI, enable **IECD** and follow the steps below.

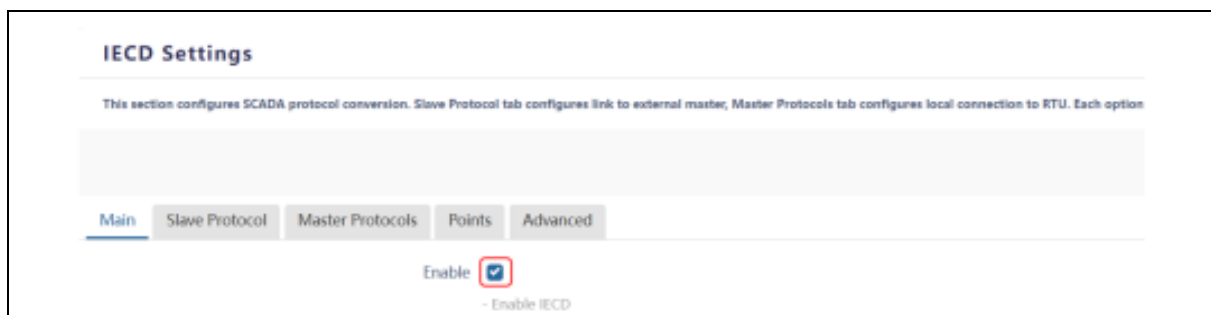


Figure 9: Main Settings

3.1 Setting up the scenario

To set up the scenario, you must configure three key elements: Enable application, the Server protocol, the master protocol and at least one data point for conversion.

Enable the application and click **SAVE & APPLY**. Remember to save and apply your WebUI configuration regularly

4 Configuring Server protocol DNP3

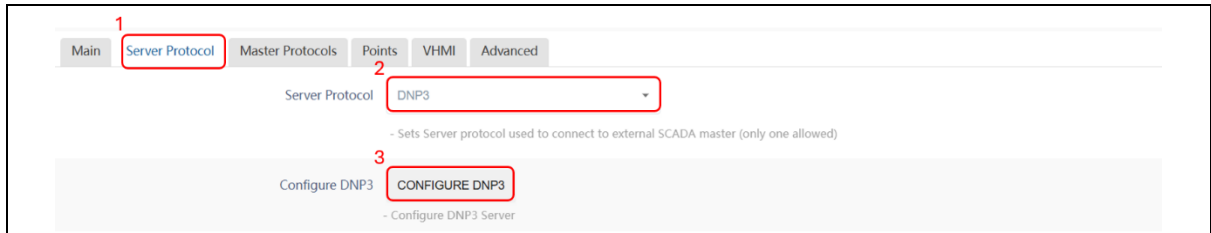


Figure 10: Slave Protocol tab in DNP3 Server Settings

1. Click **Slave Protocol**.
2. Select **DNP3** as the Server protocol.
3. Click **CONFIGURE DNP3**.

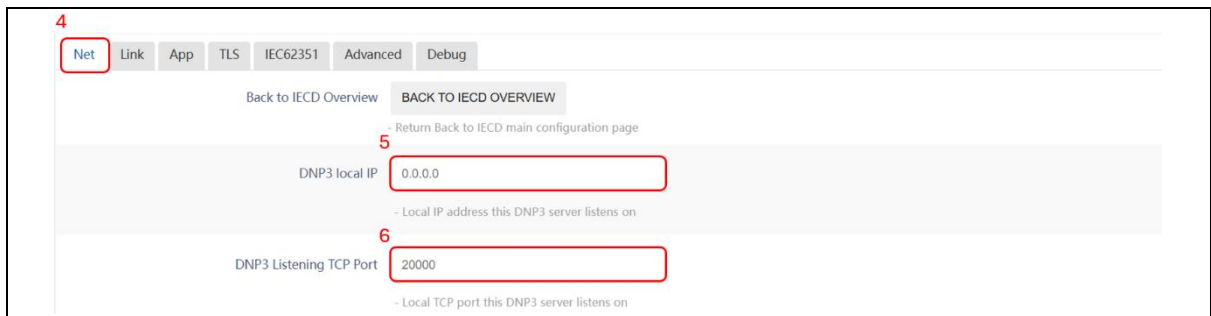


Figure 11: Net tab in DNP3 Server Settings

4. Click **Net**.
5. Set the **DNP3 Local IP**.
6. Set the **DNP3 Listening TCP Port**. Default is **20000**.

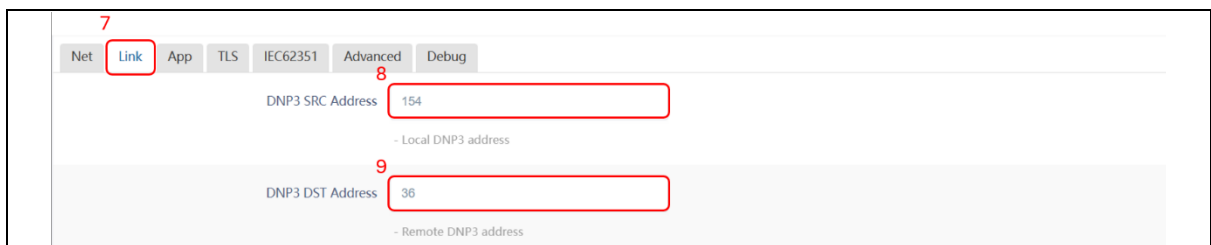


Figure 12: Link tab in DNP3 Server Settings

7. Click **Link**.
8. Set **DNP3 SRC Address**. Default value is 1.

9. Set **DNP3 DST Address**. Default value is 1.

4.1 Configuring DNP3 TLS

At minimum, to enable TLS communication, user needs to provide three files:

- CA certificate
- Client Public key (certificate)
- Client Private key (certificate)

The screenshot displays the 'DNP3 TLS Server Settings' configuration page. The 'App' tab is selected, and the 'TLS' sub-tab is active. The settings are as follows:

- DNP3 Enables TLS IEC62351-3:** Set to 'Enable' (highlighted with a red box and number 2).
- DNP3 TLS Loglevel:** Set to 'Emergency'.
- DNP3 TLS Certificate File:** Empty text field.
- Select DNP3 TLS Certificate File Upload:** 'Choose File' button highlighted with a red box and number 3.
- DNP3 TLS Key Type:** Set to 'PEM'.
- DNP3 TLS Key File:** Empty text field.
- Select DNP3 TLS Key File Upload:** 'Choose File' button highlighted with a red box and number 4.
- DNP3 TLS CA Certificate File:** Empty text field.
- Select DNP3 TLS CA Cert File Upload:** 'Choose File' button highlighted with a red box and number 5.

Figure 13: DNP3 TLS Server Settings

1. Click **TLS** tab.
2. Select Enable in **DNP3 ENABLE TLS**.
3. Click **Choose File** to upload Client Public key.
4. Click **Choose File** to upload Client Private key.
5. Click **Choose File** to upload CA public key.

Click **SAVE & APPLY** at the bottom of the page.

5 Configuring Master protocol – SNMP

5.1 Configuring SNMP Master

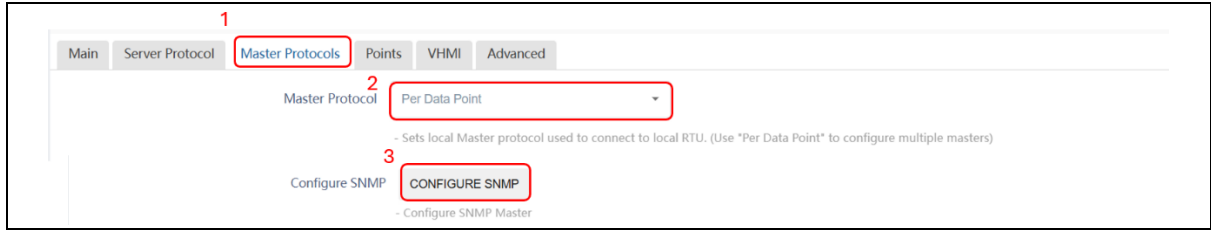


Figure 14: Master Protocols tab in IECD Settings

1. Click on **Master Protocols** tab.
2. Select **Per Data Point** as the **Master protocol** from the drop-down list.
3. Click on **Configure SNMP**.

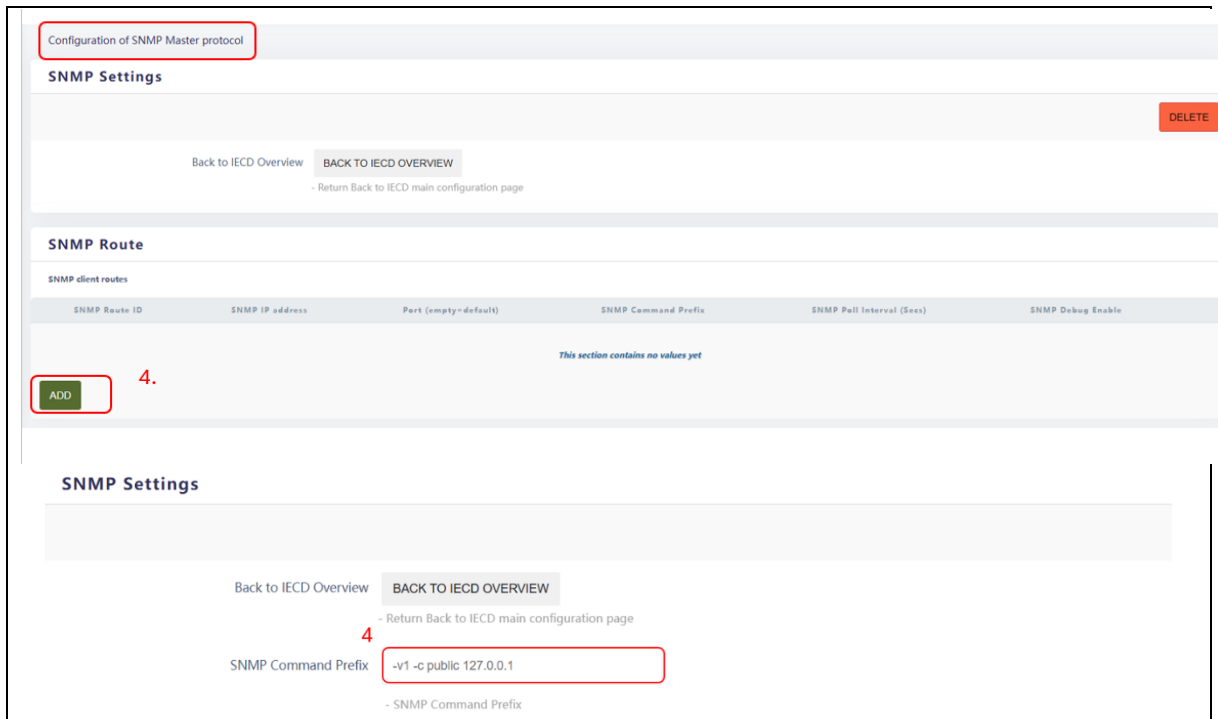


Figure 15: Master Protocols tab in IECD Settings

4. Click **ADD** in **SNMP Route** section

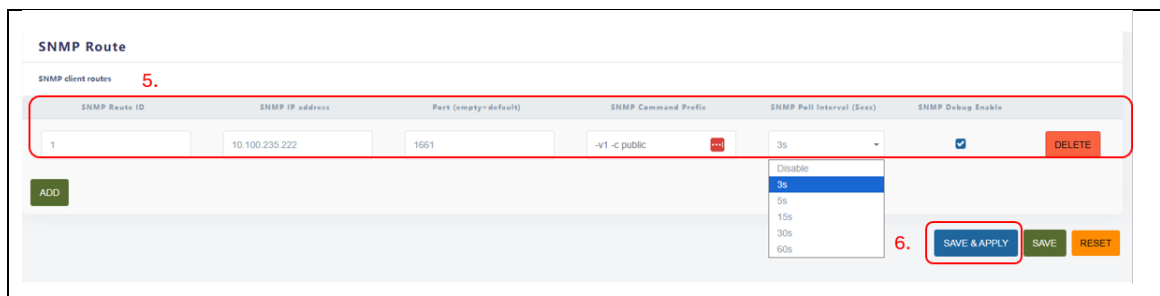


Figure 16: New SNMP Route

5. Configure **SNMP ROUTE** with required parameters. The prefix default value is "-v1 -c public" this corresponds to SNMP version 1 and community string public. It is recommended to test communication as described in section 2.4
6. To save the configuration and restart the IECD application, scroll to the bottom of the page and click **SAVE & APPLY**.

Note: Only SNMP GET is supported. SNMP SETS are not supported.

5.2 Configuring SNMP Master (Version 3)

SNMP Version 3 incorporates authentication and encryption features, and its command prefix must contain the appropriate security parameters. All required parameters should be included within the SNMP Route Command prefix field.

1. -v3 -- SNMP version 3
2. -l -- security level
3. -u -- configured username
4. -a -- authentication protocol
5. -A -- authentication password
6. -x -- privacy protocol
7. -X -- privacy password
8. SNMP agent IP

Example **-v3 -u user1 -a MD5 -A insertpass -x DES -X insertpass -l authPriv**

6 Configuring data points (signal)

Data points are essential for protocol conversion, requiring users to develop a data addressing/type map to facilitate the conversion between two distinct protocols. Each data point represents an individual value, such as mapping a Modbus Holding register to an IEC104 Measured Value. The configuration of data points adheres to the same principles as configuring communication interfaces, necessitating appropriate values for both the slave and Master sides.

6.1 Points configuration – manual

Navigate to the main IECD page.

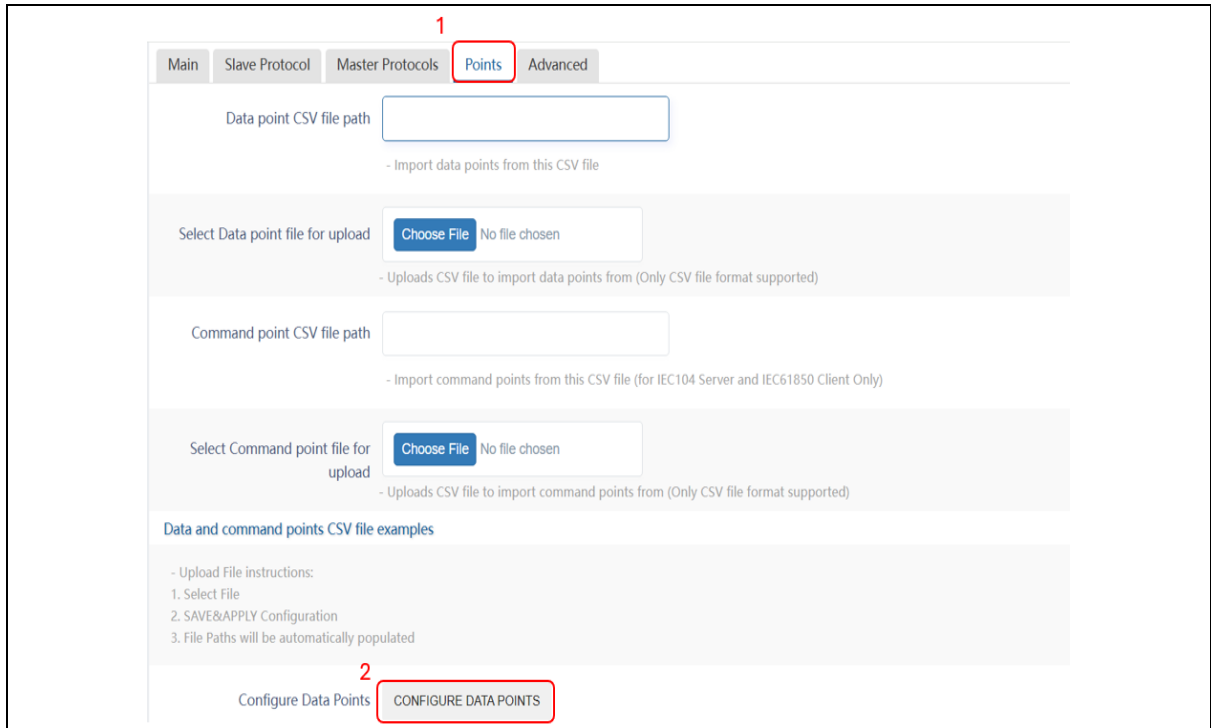


Figure 17: Points tab in data point configuration

1. Click **Points**.
2. Click **CONFIGURE DATA POINTS**.



Figure 18: Data point configuration

3. Click **ADD** to create a point.
4. Click **EDIT** to configure the added point.

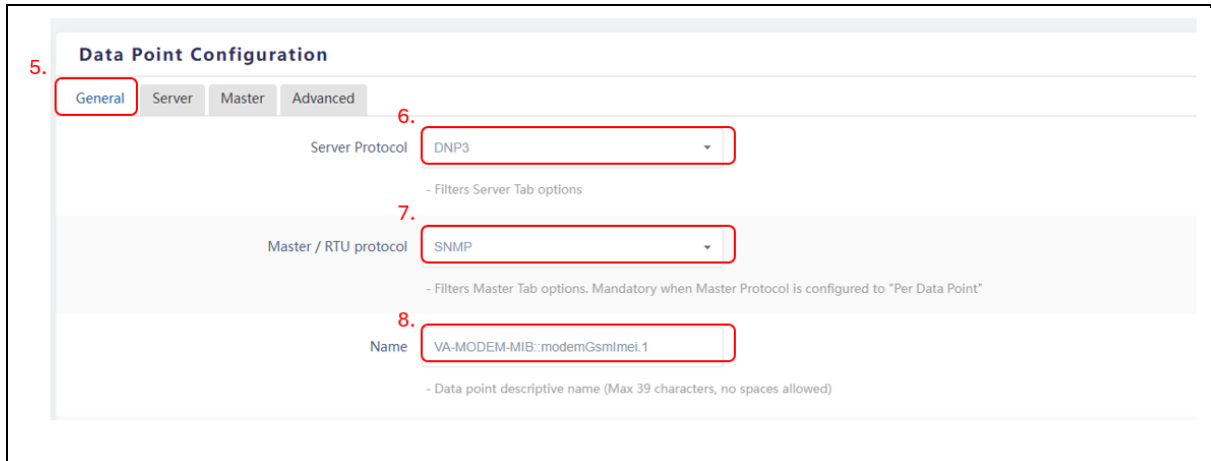


Figure 19:Data point configuration

5. On the Data Point Configuration page, click **GENERAL** tab.
6. Set the Slave Protocol as **DNP3**.
7. Set the Master/RTU protocol as **SNMP**.
8. Assign a name to the data point (optional).

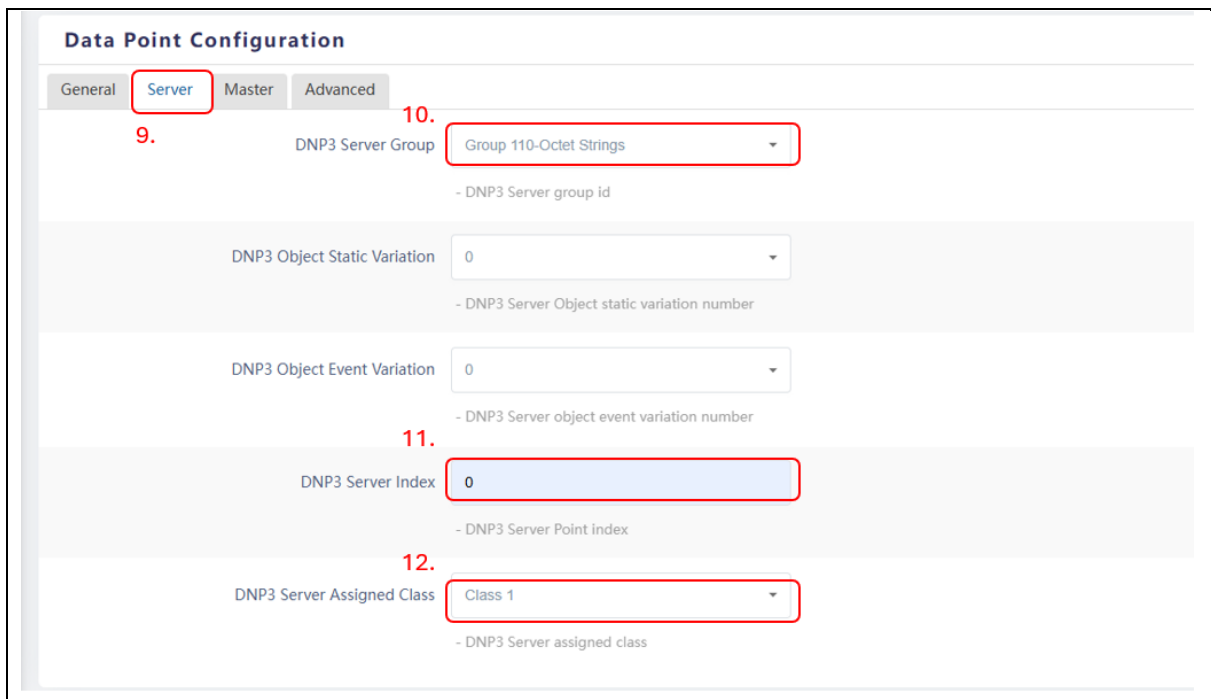


Figure 20:Data point configuration

9. Click on **Server** tab.
10. Select the **DNP3 Server Group** from the drop-down list.
11. Set the **DNP3 Server Index**.
12. Select **the DNP3 Server Assigned Class** from the drop-down list.

Data Point Configuration

General Server **Master** Advanced

13. **Master**

14. SNMP Route ID: 1
- User Configurable SNMP Route ID

15. SNMP Var Type: String
- Specifies the SNMP variable type

16. SNMP OID: 1.3.6.1.4.1.2078.3.1.2.2.1.14.1
- SNMP OID

SAVE & APPLY SAVE RESET

Figure 21: Data point configuration

13. Click on **Master** tab.

14. Set the **SNMP Route ID**

15. **SNMP Var Type** from the drop-down list.

16. Set the **SNMP OID**. (Note: It must be full numerical OID value)

Click **SAVE & APPLY** at the bottom of the page.

It's essential to match the SNMP variable type with the corresponding DNP3 Group correctly, any mismatch can lead to conversion errors, incorrect data interpretation, and/or failures.

6.2 Points configuration – CSV file

Data points can be configured via CSV file upload. The CSV file shall include all required options in its header and their corresponding values in subsequent rows. Further instructions are available on the page via 'Data and command points CSV file examples' link, highlighted in Figure 22 below.

IECD Settings

This section configures SCADA protocol conversion. Slave Protocol tab configures link to external master. Master Protocols tab configures local connection to RTU. Each option has default values.

Main Slave Protocol Master Protocols **Points** Advanced

1. **Points**

2. Data point CSV file path: [Text Field]
- Import data points from this CSV file

Select Data point file for upload: **Choose File** No file chosen
- Uploads CSV file to import data points from (Only CSV file format supported)

Command point CSV file path: [Text Field]
- Import command points from this CSV file (for IEC104 Server and IEC61850 Client Only)

Select Command point file for upload: **Choose File** No file chosen
- Uploads CSV file to import command points from (Only CSV file format supported)

[Data and command points CSV file examples](#)

Figure 22: Points tab in data point configuration

1. On the IECD Settings page, click **Points**.

2. Click **Choose File** and select the CSV file.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
dummy_s	rtu_proto	name	dnp3s_index	dnp3s_assigned_class	log_vaevent_on_change	di_invert	ai_scaler_op	vhmi_on	vhmi_regaddr	vhmi_dword	dnp3s_group	dnp3s_static_variation	dnp3s_event_variation	snmpc_var_type	snmpc_oid_str	snmpc_route_id
1	laveDP	VA-MODEM-MIB	0	1	0	0	0	0	0	0	110	0	0	0	4.1.3.6.1.4.1.2078.3.1.2.2.1.14.1	1
3	dnp3s	snmp	modemGsmReg	0	1	0	0	0	0	0	30	0	0	0	1.1.3.6.1.4.1.2078.3.1.2.2.1.6.1	1
4	dnp3s	snmp	modemConnec	1	1	0	0	0	0	0	30	0	0	0	1.1.3.6.1.4.1.2078.3.1.2.2.1.3.1	1
5	dnp3s	snmp	modemGsmSig	2	1	0	0	0	0	0	30	0	0	0	1.1.3.6.1.4.1.2078.3.1.2.2.1.5.1	1
6	dnp3s	snmp	modemGsmAc	4	1	0	0	0	0	0	30	0	0	0	1.1.3.6.1.4.1.2078.3.1.2.2.1.10.1	1
7	dnp3s	snmp	modemGsmNe	5	1	0	0	0	0	0	30	0	0	0	1.1.3.6.1.4.1.2078.3.1.2.2.1.9.1	1
8	dnp3s	snmp	modemMobile	7	1	0	0	0	0	0	30	0	0	0	1.1.3.6.1.4.1.2078.3.1.2.2.1.23.1	1
9	dnp3s	snmp	modemGsmSim	9	1	0	0	0	0	0	30	0	0	0	1.1.3.6.1.4.1.2078.3.1.2.2.1.35.1	1
10	dnp3s	snmp	modemGsmLoc	10	1	0	0	0	0	0	30	0	0	0	1.1.3.6.1.4.1.2078.3.1.2.2.1.7.1	1
11	dnp3s	snmp	ifStatus	12	1	0	0	0	0	0	30	0	0	0	1.1.3.6.1.4.1.2078.3.2.66.1.1.2.1	1
12	dnp3s	snmp	icmpInMsgs	15	1	0	0	0	0	0	30	1	1	1	3.1.3.6.1.2.1.5.1.0	1
13	dnp3s	snmp	tcpInErrs	16	1	0	0	0	0	0	30	0	0	0	3.1.3.6.1.2.1.6.14.0	1
14	dnp3s	snmp	udpInErrors	17	1	0	0	0	0	0	30	0	0	0	3.1.3.6.1.2.1.7.3.0	1
15	dnp3s	snmp	hrSystemUptime	20	1	0	0	0	0	0	30	0	0	0	1.1.3.6.1.2.1.25.1.1.0	1
16	dnp3s	snmp	hrMemorySize	21	1	0	0	0	0	0	30	0	0	0	1.1.3.6.1.2.1.25.2.2.0	1
17	dnp3s	snmp	hrSystemNumU	23	1	0	0	0	0	0	30	1	1	1	3.1.3.6.1.2.1.25.1.5.0	1
18	dnp3s	snmp	digitalInputPor	26	1	0	0	0	0	0	30	0	0	0	1.1.3.6.1.4.1.2078.3.1.1.7.1.1.1	1
19	dnp3s	snmp	digitalInputPor	28	1	0	0	0	0	0	30	0	0	0	1.1.3.6.1.4.1.2078.3.1.1.7.1.4.1	1
20	dnp3s	snmp	digitalOutputPo	29	1	0	0	0	0	0	30	0	0	0	1.1.3.6.1.4.1.2078.3.1.1.8.1.1.1	1
21	dnp3s	snmp	digitalOutputPo	31	1	0	0	0	0	0	30	0	0	0	1.1.3.6.1.4.1.2078.3.1.1.8.1.4.1	1

Figure 23: CSV file format

```

dummy_slaveDP,rtu_proto,name,dnp3s_index,dnp3s_assigned_class,log_vaevent_on_change,di_invert,ai_scaler_op,vhmi_on,vhmi_regaddr,vhmi_dword,dnp3s_group,dnp3s_static_variation,dnp3s_event_variation,snmpc_var_type,snmpc_oid_str,snmpc_route_id
dnp3s,snmp,VA-MODEM-MIB::modemGsmImei.1,0,1,0,0,0,0,0,0,110,0,0,4,,1.3.6.1.4.1.2078.3.1.2.2.1.14.1,1
dnp3s,snmp,modemGsmRegistrationStatus,0,1,0,0,0,0,0,0,30,0,0,1,,1.3.6.1.4.1.2078.3.1.2.2.1.6.1,1
dnp3s,snmp,modemConnectionState,1,1,0,0,0,0,0,0,30,0,0,1,,1.3.6.1.4.1.2078.3.1.2.2.1.3.1,1
dnp3s,snmp,modemGsmSignalStrength,2,1,0,0,0,0,0,0,30,0,0,1,,1.3.6.1.4.1.2078.3.1.2.2.1.5.1,1
dnp3s,snmp,modemGsmActiveSimSlot,4,1,0,0,0,0,0,0,30,0,0,1,,1.3.6.1.4.1.2078.3.1.2.2.1.10.1,1
dnp3s,snmp,modemGsmNetworkTechnology,5,1,0,0,0,0,0,0,30,0,0,1,,1.3.6.1.4.1.2078.3.1.2.2.1.9.1,1
dnp3s,snmp,modemMobileState,7,1,0,0,0,0,0,0,30,0,0,1,,1.3.6.1.4.1.2078.3.1.2.2.1.23.1,1
dnp3s,snmp,modemGsmSimIn,9,1,0,0,0,0,0,0,30,0,0,1,,1.3.6.1.4.1.2078.3.1.2.2.1.35.1,1
dnp3s,snmp,modemGsmLocationAreaCode,10,1,0,0,0,0,0,0,30,0,0,1,,1.3.6.1.4.1.2078.3.1.2.2.1.7.1,1
dnp3s,snmp,ifStatus,12,1,0,0,0,0,0,0,30,0,0,1,,1.3.6.1.4.1.2078.3.2.66.1.1.2.1,1
dnp3s,snmp,icmpInMsgs,15,1,0,0,0,0,0,0,30,1,1,3,,1.3.6.1.2.1.5.1.0,1
dnp3s,snmp,tcpInErrs,16,1,0,0,0,0,0,0,30,0,0,3,,1.3.6.1.2.1.6.14.0,1
dnp3s,snmp,udpInErrors,17,1,0,0,0,0,0,0,30,0,0,3,,1.3.6.1.2.1.7.3.0,1
dnp3s,snmp,hrSystemUptime,20,1,0,0,0,0,0,0,30,0,0,1,,1.3.6.1.2.1.25.1.1.0,1
dnp3s,snmp,hrMemorySize,21,1,0,0,0,0,0,0,30,0,0,1,,1.3.6.1.2.1.25.2.2.0,1
dnp3s,snmp,hrSystemNumUsers,23,1,0,0,0,0,0,0,30,1,1,3,,1.3.6.1.2.1.25.1.5.0,1
dnp3s,snmp,digitalInputPortIndex,26,1,0,0,0,0,0,0,30,0,0,1,,1.3.6.1.4.1.2078.3.1.1.7.1.1.1,1
dnp3s,snmp,digitalInputPortState,28,1,0,0,0,0,0,0,30,0,0,1,,1.3.6.1.4.1.2078.3.1.1.7.1.4.1,1
dnp3s,snmp,digitalOutputPortIndex,29,1,0,0,0,0,0,0,30,0,0,1,,1.3.6.1.4.1.2078.3.1.1.8.1.1.1,1
dnp3s,snmp,digitalOutputPortState,31,1,0,0,0,0,0,0,30,0,0,1,,1.3.6.1.4.1.2078.3.1.1.8.1.4.1,1

```

Figure 24: CSV file content

With any text editor, save the content of the Figure 24 with **.csv** extension, upload that file to the router and click **SAVE & APPLY** at the bottom of the page. Router will parse the file and configure the data points.

6.3 SNMP to DNP3 Mapping

SNMP data types must be mapped to equivalent IECD Variable types.

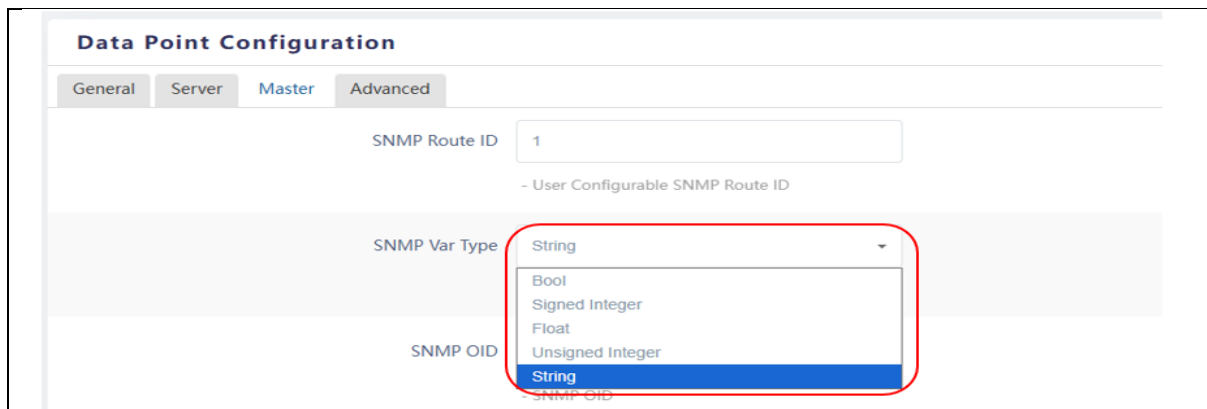


Figure 25: SNMP Var Type

Following table shows the mapping of SNMP with DNP3 types and other SCADA protocols.

***Note:** IEC104 supports signed 16-bit integer value only, if input value is greater the value will overflow. Example : A 32-bit value of 123456 is truncated to a 16-bit value -7616

SNMP TYPE	IECD Var Type	DNP3 Group	Other SCADA
INTEGER (32 bits)	INTEGER	GROUP 30 Static Variation 1 Event Variation 1	IEC104 – TI9 * IEC 61850 - MV (Measured value) MODBUS – HR signed 32 MQTT - standard message
COUNTER 32	INTEGER	GROUP 30 / GROUP 20 Static Variation 1 Event Variation 1	IEC104 – TI9 * IEC 61850 - MV (Measured value) MODBUS – HR signed 32 MQTT - standard message
GAUGE 32	INTEGER	GROUP 30 Static Variation 1 Event Variation 1	IEC104 – TI9 * IEC 61850 - MV (Measured value) MODBUS – HR signed 32 MQTT - standard message
TIMETICKS	INTEGER	GROUP 30 Static Variation 1 Event Variation 1	IEC104 – TI9 * IEC 61850 – MV (Measured value) MODBUS – HR signed 32 MQTT - standard message
OPAQUE	FLOAT	GROUP 30 Static Variation 5 Event Variation 5	IEC104 – TI13 * IEC 61850 – MV (Measured value) MODBUS – HR (float 32) MQTT - standard message
STRING	STRING	GROUP 110 Static Variation 0 Event Variation 0	MQTT - standard message

Requests for support of additional SNMP TYPES are welcome and should be addressed to support.ie@westermo.com

7 Essential OIDs

7.1 MOBILE COMMUNICATION

Object Name	Description	OID	SNMP Type	IECD Var Type
modemGsmRegistrationStatus	GSM registration status: not registered/not searching(1), registered home(2), not registered/searching(3), registration denied(4), unknown(5), registered roaming(6)	.1.3.6.1.4.1.2078.3.1.2.2.1.6.1	INTEGER	INTEGER
modemConnectionState	Modem connection state: up(1), down(2)	.1.3.6.1.4.1.2078.3.1.2.2.1.3.1	INTEGER	INTEGER
modemGsmSignalStrength	GSM signal strength (RSSI, dBm)	.1.3.6.1.4.1.2078.3.1.2.2.1.5.1	INTEGER	INTEGER
modemGsmActiveSimSlot	Active SIM slot: simSlotOne(1), simSlotTwo(2)	.1.3.6.1.4.1.2078.3.1.2.2.1.10.1	INTEGER	INTEGER
modemGsmNetworkTechnology	Currently used network technology: unknown(1), gsm(2), gprs(3), edge(4), umts(5), umtsHsdpa(6), umtsHsupa(7), umtsHsdpaHsupa(8), lte(9)	.1.3.6.1.4.1.2078.3.1.2.2.1.9.1	INTEGER	INTEGER
modemMobileState	state of mobile modem: unknown(1), idle(2), initialising(3), scanning(4), connecting(5), connected(6)	.1.3.6.1.4.1.2078.3.1.2.2.1.23.1	INTEGER	INTEGER
modemGsmSimIn	SIM inserted in the current slot or not	.1.3.6.1.4.1.2078.3.1.2.2.1.35.1	INTEGER	INTEGER
modemGsmLocationAreaCode	Location Area Code (LAC) of the currently used cell. For non-GPRS/3G modems this will be always zero.	.1.3.6.1.4.1.2078.3.1.2.2.1.7.1	INTEGER	INTEGER

7.2 NETWORK

Object Name	Description	OID	SNMP Type	IECD Var Type
ifStatus.x	Interface status: up(1), down(2)	.1.3.6.1.4.1.2078.3.2.66.1.1.2.X	INTEGER	INTEGER
icmpInMsgs	total number of ICMP messages received	.1.3.6.1.2.1.5.1.0	Counter 32	INTEGER
tcpInErrs	TCP input errors: number of TCP segments received in error	.1.3.6.1.2.1.6.14.0	Counter 32	INTEGER

udpInErrors	UDP input errors	.1.3.6.1.2.1.7.3.0	Counter 32	INTEGER
-------------	------------------	--------------------	---------------	---------

7.3 SYSTEM

Object Name	Description	OID	SNMP TYPE	IECD Var Type
hrSystemUptime	System uptime: time (in hundredths of a second) since last reinitialisation	.1.3.6.1.2.1.25.1.1.0	TimeTicks	INTEGER
hrMemorySize	Total physical memory size (in kilobytes)	.1.3.6.1.2.1.25.2.2.0	INTEGER	INTEGER
hrSystemNumUsers	number of users currently logged into the host system	.1.3.6.1.2.1.25.1.5.0	Gauge32	INTEGER

7.4 GPIOs

Object Name	Description	OID	SNMP TYPE	Value
digitalInputPortIndex.x	Unique number for each digital input port	.1.3.6.1.4.1.2078.3.1.1.7.1.1.X	INTEGER	INTEGER
digitalInputPortState.x	Current state of digital input port: open (1), closed (2)	.1.3.6.1.4.1.2078.3.1.1.7.1.4.X	INTEGER	INTEGER

digitalOutputPortInd.x	Unique number for digital output port	.1.3.6.1.4.1.2078.3.1.1.8.1.1.X	INTEGER	INTEGER
digitalOutputPortState.x	Current state of digital output port: open (1), closed (2)	.1.3.6.1.4.1.2078.3.1.1.8.1.4.X	INTEGER	INTEGER

8 Troubleshooting

8.1 IECD status via the WebUI

Basic troubleshooting such as verifying connections quality, values, mapping or addressing can be accessed via the dedicated IECD status page.

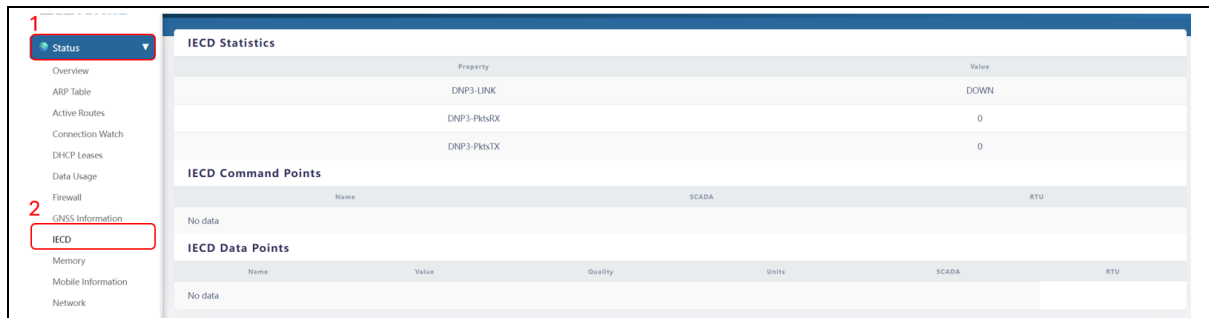


Figure 26: IECD status WebUI

1. On the main page, click **Status**.
2. Click **IECD**.

8.2 IECD status via CLI

```
root@FC-We-Merlin4407:~# iec show stats
2025.11.21 12:23:30.661

Running protocols: (0x00041000)
* DNP3 Slave
* SNMP Client

Serial interfaces:
  0: /dev/serial1 : -
  1: /dev/serial2 : -

** DNP3S App Stats:
Fragments Rx / Tx: 5 / 3
Fragments Rx timeout: 0
Fragments Rx Errors: 0
Fragments Rx Dups: 0
Operate timeouts: 0
Event queue overflow: 0

** DNP3S DL Stats:
State: SecUnResetIdle
Link Uptime    0 hrs 9 mins 54 secs
Frames Rx 43 Tx 41 TxQ Overrun 0
CRC Errors 0 Length Errors 0 Bad Addr Errors 0

** DNP3S TS Stats:
appFrgsTx: 3
appFrgsRx: 5
tsSecTx: 2
```

Figure 27: IECD status CLI output

1. To check the IECD status using CLI, connect to the router via SSH and enter the command `iec show stats`.
2. This will display the running protocols, serial interface in use, server and master protocol statistics such as the number of transmitted and received frames, and more. This information serves as a starting point for basic troubleshooting.

8.3 Configuring main debug level

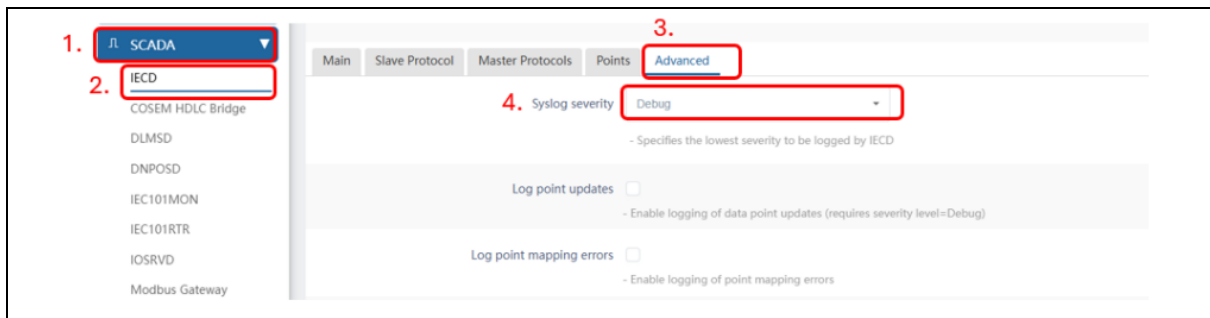


Figure 28: Enabling IECD logs

1. Click **SCADA**.
2. Click **IECD**.
3. Click **Advanced**.
4. From the Syslog severity drop-down menu, set the Syslog severity to **Debug**.
5. To save the configuration and restart the IECD application, scroll to the bottom of the page and click **SAVE & APPLY**.

8.4 Enabling debug per protocol – DNP3 (Server)



Figure 29: Enabling server protocol logs

Via the WebUI, access IEC Server settings.

Click **Server Protocol** and then **CONFIGURE DNP3**.

1. Click **Debug**.
2. Enable additional logging settings.

8.5 Enabling debug per protocol – SNMP (Master)



Figure 30: Enabling master protocol logs

1. Click Master Protocol and then CONFIGURE SNMP.
2. Check **SNMP Debug Enable** in SNMP Route .
3. To save the configuration and restart the IECD application, scroll to the bottom of the page and click **SAVE & APPLY**.

8.6 Accessing logs using WebUI

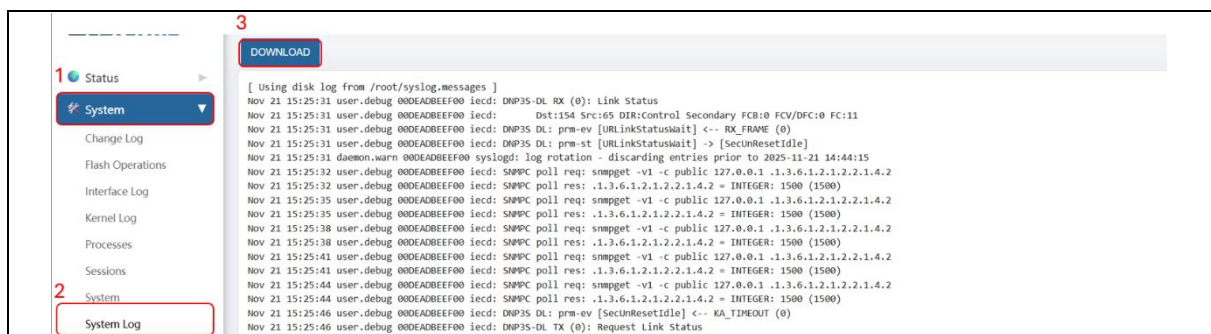


Figure 31: Enabling system logs

1. To check the logs, in the left-hand menu, click **System**.

2. Click **System Log** and search for logs related to IECD. These logs will have the name **iecd**.
3. To download the logs, click **Download**.

8.7 Accessing logs via CLI

```

Nov 21 15:28:06 user.debug 00DEADBEEF00 iecd: SNMPC poll res: .1.3.6.1.2.1.2.2.1.4.2 = INTEGER: 1500 (1500)
Nov 21 15:28:09 user.debug 00DEADBEEF00 iecd: SNMPC poll req: snmpget -v1 -c public 127.0.0.1 .1.3.6.1.2.1.2.2.1.4.2
Nov 21 15:28:09 user.debug 00DEADBEEF00 iecd: SNMPC poll res: .1.3.6.1.2.1.2.2.1.4.2 = INTEGER: 1500 (1500)
Nov 21 15:28:12 user.debug 00DEADBEEF00 iecd: SNMPC poll req: snmpget -v1 -c public 127.0.0.1 .1.3.6.1.2.1.2.2.1.4.2
Nov 21 15:28:12 user.debug 00DEADBEEF00 iecd: SNMPC poll res: .1.3.6.1.2.1.2.2.1.4.2 = INTEGER: 1500 (1500)
Nov 21 15:28:15 user.debug 00DEADBEEF00 iecd: SNMPC poll req: snmpget -v1 -c public 127.0.0.1 .1.3.6.1.2.1.2.2.1.4.2
Nov 21 15:28:15 user.debug 00DEADBEEF00 iecd: SNMPC poll res: .1.3.6.1.2.1.2.2.1.4.2 = INTEGER: 1500 (1500)
Nov 21 15:28:17 user.debug 00DEADBEEF00 iecd: DNP3S DL: prm-ev [SecUnResetIdle] <-- KA_TIMEOUT (0)
Nov 21 15:28:17 user.debug 00DEADBEEF00 iecd: DNP3S-DL TX (0): Request Link Status
Nov 21 15:28:17 user.debug 00DEADBEEF00 iecd: Dst:65 Src:154 DIR:Monitor Primary FCB:0 FCV/DFC:0 FC:9
Nov 21 15:28:17 user.debug 00DEADBEEF00 iecd: DNP3S-DL: TxDUMP(10): 05 64 05 49 41 00 9a 00 b2 59
Nov 21 15:28:17 user.debug 00DEADBEEF00 iecd: DNP3S DL: prm-st [SecUnResetIdle] -> [URLinkStatusWait]
Nov 21 15:28:17 user.debug 00DEADBEEF00 iecd: DNP3S-DL: RxDUMP(10): 05 64 05 8b 9a 00 41 00 98 ac
Nov 21 15:28:17 user.debug 00DEADBEEF00 iecd: DNP3S-DL RX (0): Link Status
Nov 21 15:28:17 user.debug 00DEADBEEF00 iecd: Dst:154 Src:65 DIR:Control Secondary FCB:0 FCV/DFC:0 FC:11
Nov 21 15:28:17 user.debug 00DEADBEEF00 iecd: DNP3S DL: prm-ev [URLinkStatusWait] <-- RX_FRAME (0)
Nov 21 15:28:17 user.debug 00DEADBEEF00 iecd: DNP3S DL: prm-st [URLinkStatusWait] -> [SecUnResetIdle]
Nov 21 15:28:18 user.debug 00DEADBEEF00 iecd: SNMPC poll req: snmpget -v1 -c public 127.0.0.1 .1.3.6.1.2.1.2.2.1.4.2
Nov 21 15:28:18 user.debug 00DEADBEEF00 iecd: SNMPC poll res: .1.3.6.1.2.1.2.2.1.4.2 = INTEGER: 1500 (1500)
Nov 21 15:28:21 user.debug 00DEADBEEF00 iecd: SNMPC poll req: snmpget -v1 -c public 127.0.0.1 .1.3.6.1.2.1.2.2.1.4.2
Nov 21 15:28:21 user.debug 00DEADBEEF00 iecd: SNMPC poll res: .1.3.6.1.2.1.2.2.1.4.2 = INTEGER: 1500 (1500)
Nov 21 15:28:24 user.debug 00DEADBEEF00 iecd: SNMPC poll req: snmpget -v1 -c public 127.0.0.1 .1.3.6.1.2.1.2.2.1.4.2
Nov 21 15:28:24 user.debug 00DEADBEEF00 iecd: SNMPC poll res: .1.3.6.1.2.1.2.2.1.4.2 = INTEGER: 1500 (1500)
Nov 21 15:28:24 user.debug 00DEADBEEF00 iecd: SNMPC poll req: snmpget -v1 -c public 127.0.0.1 .1.3.6.1.2.1.2.2.1.4.2
Nov 21 15:28:27 user.debug 00DEADBEEF00 iecd: SNMPC poll req: snmpget -v1 -c public 127.0.0.1 .1.3.6.1.2.1.2.2.1.4.2
Nov 21 15:28:27 user.debug 00DEADBEEF00 iecd: SNMPC poll res: .1.3.6.1.2.1.2.2.1.4.2 = INTEGER: 1500 (1500)
Nov 21 15:28:30 user.debug 00DEADBEEF00 iecd: SNMPC poll req: snmpget -v1 -c public 127.0.0.1 .1.3.6.1.2.1.2.2.1.4.2
Nov 21 15:28:30 user.debug 00DEADBEEF00 iecd: SNMPC poll res: .1.3.6.1.2.1.2.2.1.4.2 = INTEGER: 1500 (1500)
Nov 21 15:28:32 user.debug 00DEADBEEF00 iecd: DNP3S DL: prm-ev [SecUnResetIdle] <-- KA_TIMEOUT (0)
Nov 21 15:28:32 user.debug 00DEADBEEF00 iecd: DNP3S-DL TX (0): Request Link Status
Nov 21 15:28:32 user.debug 00DEADBEEF00 iecd: Dst:65 Src:154 DIR:Monitor Primary FCB:0 FCV/DFC:0 FC:9
Nov 21 15:28:32 user.debug 00DEADBEEF00 iecd: DNP3S-DL: TxDUMP(10): 05 64 05 49 41 00 9a 00 b2 59
Nov 21 15:28:32 user.debug 00DEADBEEF00 iecd: DNP3S DL: prm-st [SecUnResetIdle] -> [URLinkStatusWait]
Nov 21 15:28:32 user.debug 00DEADBEEF00 iecd: DNP3S-DL: RxDUMP(10): 05 64 05 8b 9a 00 41 00 98 ac
Nov 21 15:28:32 user.debug 00DEADBEEF00 iecd: DNP3S-DL RX (0): Link Status
Nov 21 15:28:32 user.debug 00DEADBEEF00 iecd: Dst:154 Src:65 DIR:Control Secondary FCB:0 FCV/DFC:0 FC:11
Nov 21 15:28:32 user.debug 00DEADBEEF00 iecd: DNP3S DL: prm-ev [URLinkStatusWait] <-- RX_FRAME (0)
Nov 21 15:28:32 user.debug 00DEADBEEF00 iecd: DNP3S DL: prm-st [URLinkStatusWait] -> [SecUnResetIdle]
Nov 21 15:28:33 user.debug 00DEADBEEF00 iecd: SNMPC poll req: snmpget -v1 -c public 127.0.0.1 .1.3.6.1.2.1.2.2.1.4.2
Nov 21 15:28:33 user.debug 00DEADBEEF00 iecd: SNMPC poll res: .1.3.6.1.2.1.2.2.1.4.2 = INTEGER: 1500 (1500)
Nov 21 15:28:36 user.debug 00DEADBEEF00 iecd: SNMPC poll req: snmpget -v1 -c public 127.0.0.1 .1.3.6.1.2.1.2.2.1.4.2
Nov 21 15:28:36 user.debug 00DEADBEEF00 iecd: SNMPC poll res: .1.3.6.1.2.1.2.2.1.4.2 = INTEGER: 1500 (1500)
Nov 21 15:28:39 user.debug 00DEADBEEF00 iecd: SNMPC poll req: snmpget -v1 -c public 127.0.0.1 .1.3.6.1.2.1.2.2.1.4.2
Nov 21 15:28:39 user.debug 00DEADBEEF00 iecd: SNMPC poll res: .1.3.6.1.2.1.2.2.1.4.2 = INTEGER: 1500 (1500)
Nov 21 15:28:42 user.debug 00DEADBEEF00 iecd: SNMPC poll req: snmpget -v1 -c public 127.0.0.1 .1.3.6.1.2.1.2.2.1.4.2
Nov 21 15:28:42 user.debug 00DEADBEEF00 iecd: SNMPC poll res: .1.3.6.1.2.1.2.2.1.4.2 = INTEGER: 1500 (1500)
Nov 21 15:28:45 user.debug 00DEADBEEF00 iecd: SNMPC poll req: snmpget -v1 -c public 127.0.0.1 .1.3.6.1.2.1.2.2.1.4.2

```

Figure 32: Enabling CLI logs output

1. To check the IECD logs using the CLI, connect via SSH and enter the command `logread -f`.
2. Logs related to the server and master protocols will be displayed.

Note: users can download the log file, as `syslog.messages` in the root directory, via WinSCP.