



SIPROTEC 5: (and for other DG EA products)
Handling of SNMPv3 (secure SNMP)
DGPI (asset monitoring) & **DGSM** (audit log)
via SNMP

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

APN-091, Edition 1.0, 01.10.2021

Content

1	Introduction	4
1.1	What is SNMP (https://www.manageengine.com/network-monitoring/what-is-snmp.html)	5
1.2	SNMP basic components and their functionalities.....	5
1.2.1	SNMP Manager	5
1.2.2	Managed Devices.....	5
1.2.3	SNMP Agent	5
1.2.4	Management Information database or Management Information Base (MIB).....	6
1.2.5	Basic commands of SNMP	9
1.2.6	SNMPv3	10
2	Activation of SNMP functionality	11
2.1	Activation of SNMP functionality in SIPROTEC 5 relays	11
2.2	Activation of SNMP in EN100 module for SIPROTEC relays	12
2.3	Activation of SNMP in Reyrolle relays	12
2.4	Activation of SNMP functionality for SICAM PAS/PQS	13
2.5	Activation of SNMP functionality for A8000 RTUs	14
2.5.1	Activation of SNMP functionality for CP-8000/8021/8022	14
2.5.2	Activation of SNMP functionality for CP-8050/8031	14
2.6	Activation of SNMP functionality for SICAM Q100/200.....	16
3	User administration of SNMPv3	17
3.1	SNMPv3 general information.....	17
3.2	SNMPv3 availability in DG EA products.....	17
3.3	User administration with SNMPv3 in DG EA products.....	18
3.3.1	User administration for DG EA products with default user accounts	18
3.3.2	User administration for DG EA products via device setting tools	28
4	DG common MIBs DGPI and DGSM	33
4.1	Preparation for the DGPI and DGSM MIBs	34
4.1.1	Loading the needed standard and DG common MIBs	34
4.1.2	Receiving security monitoring notifications -> Target-MIB	34

4.1.3	Receiving security monitoring notifications -> Notification-MIB.....	37
4.1.4	Enabling SNMP traps on SNMP Agent side.....	38
4.1.5	Testing SNMP traps	39
4.1.6	Deleting SNMP settings	41
4.1.7	Decrypting SNMPv3 PDUs in Wireshark	42
4.2	Reading DGPI and DGSM information	43
4.2.1	Getting values of the DGPI product inventory MIB.....	43
4.2.2	Getting values of the DGSM Security Monitoring MIB.....	45
5	Link collection to further documents	46

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

1 Introduction

This application note provides information about:

- SNMP basic information
- How to activate SNMP in SIPROTEC 5 devices and in other DG EA products
- **The focus** of this APN is on **SNMPv3 security** functionality and on the
 - **DG Product Inventory MIB** = DGPI (digitalGridProductInventory.mib)
 - **DG Security Monitoring MIB** = DGSM (digitalGridSecurityMonitoring.mib)
- How to set up the security related SNMPv3 functionality in SIPROTEC 5 and in other DG EA products
- How to set up the DGPI & DGSM functionality in SIPROTEC 5 and in other DG EA products

The newly available DGPI & DGSM for our SIPROTEC 5 triggered the creation of this Application Note, however SNMPv3 and the DG Product Inventory MIB and the DG Security Monitoring MIB are also implemented in other products from our DG EA portfolio. Therefore the handling and setting for these products are additionally described in the APN.

1.1 What is SNMP (<https://www.manageengine.com/network-monitoring/what-is-snmp.html>)

SNMP (Simple Network Management Protocol) is a network protocol used to monitor or control network components (e.g., Router, Switches, Server or IEDs like Protection relays, Automation units (RTUs) or Power Quality recorder from a central station.

SNMP is one of the widely accepted network protocols to manage and monitor network elements. Most of the professional-grade network elements come with bundled SNMP agent. These agents must be enabled and configured to communicate with the network monitoring tools or network management system (NMS).

The protocol controls the communication between the monitored devices (SNMP Agents) and the monitoring station (SNMP Manager).

1.2 SNMP basic components and their functionalities

A SNMP system consists of:

- SNMP Manager
- Managed devices
- SNMP agent
- Management Information Database Otherwise called as Management Information Base (MIB)

1.2.1 SNMP Manager

A manager or management system is a separate entity that is responsible to communicate with the SNMP agent implemented network devices. This is typically a computer that is used to run one or more network management systems.

SNMP Manager's key functions:

- Queries agents
- Gets responses from agents
- Sets variables in agents
- Acknowledges asynchronous events from agents

In the Siemens portfolio, the following systems can take over the function as SNMP Manager:

- SICAM SCC (with the option: Network Manager)
- SICAM PAS (but **limited**)
- SICAM GridEdge (but **limited**)
- SINEC NMS = Network Management System from Siemens Digital Industry

1.2.2 Managed Devices

A managed device or the network element is a part of the network that requires some form of monitoring and management e.g., SIPROTEC relays, Reyrolle5 relays, SICAM A8000 RTUs, SICAM Q100/Q200 power quality recorder

1.2.3 SNMP Agent

The agent is a program that is packaged within the network element. Enabling the agent allows it to collect the management information database from the device locally and makes it available to the SNMP manager, when it is queried for. These agents could be standard (e.g., Net-SNMP) or specific to a vendor.

SNMP agent's key functions:

- Collects management information about its local environment
- Stores and retrieves management information as defined in the MIB.
- Signals an event to the manager.
- Acts as a proxy for some non-SNMP manageable network node.

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

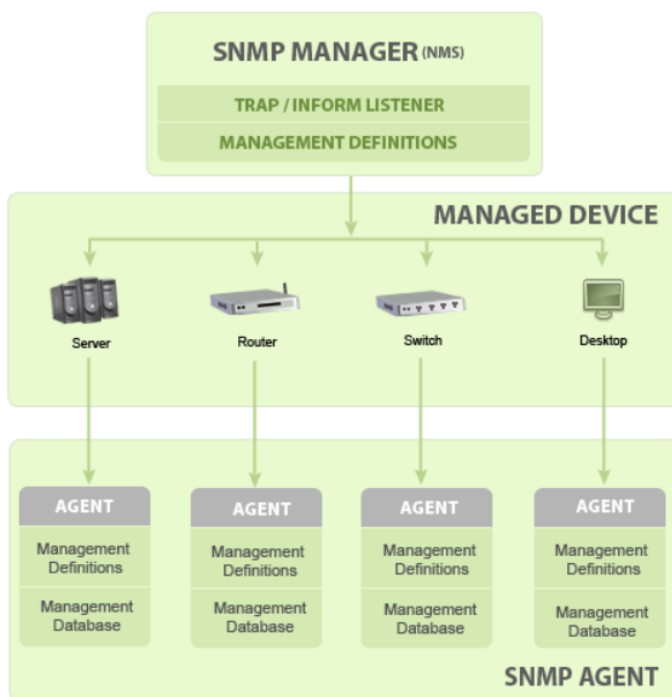


Figure 1.1 Basic SNMP Communication Diagram (<https://www.manageengine.com/network-monitoring/what-is-snmp.html>)

1.2.4 Management Information database or Management Information Base (MIB)

Every SNMP agent maintains an information database describing the managed device parameters. The SNMP manager uses this database to request the agent for specific information and further translates the information as needed for the Network Management System (NMS). This commonly shared database between the Agent and the Manager is called Management Information Base (MIB).

Typically, these MIB contains standard set of statistical and control values defined for hardware nodes on a network. SNMP **also allows the extension of these standard values** with values specific to a particular agent using **private MIBs**.

In short, MIB files are the set of questions that a SNMP Manager can ask the agent. Agent collects these data locally and stores it, as defined in the MIB. So, the SNMP Manager should be aware of these standard and private questions for every type of agent.

MIB structure and Object Identifier (Object ID or OID)

The Management Information Base (MIB) is a collection of Information for managing network element. The MIBs comprises of managed objects identified by the name Object Identifier (Object ID or OID).

Each Identifier is unique and denotes specific characteristics of a managed device. When queried for, the return value of each identifier could be different e.g., Text, Number, Counter, etc...

Every Object ID is organized hierarchically in MIB. The MIB hierarchy can be represented in a tree structure with individual variable identifier. For vendor specific MIBs the vendor must register its MIBs to keep the concept with unique identifiers. Siemens DG has registered for its private MIBs and has the node 22638.

In the following figures the basic structure showing the different Standard nodes with ID and the path for the private MIBs can be seen.

- Figure 1.2 is showing the standard path with IDs especially down to the MIB-2 what is supported and used for most of our products.
- Figure 1.3 is showing the path for the private MIB structure with IDs for different components of our portfolio.

- Figure 1.4 is showing the private path down for the common DG Project inventory MIB (DGPI)

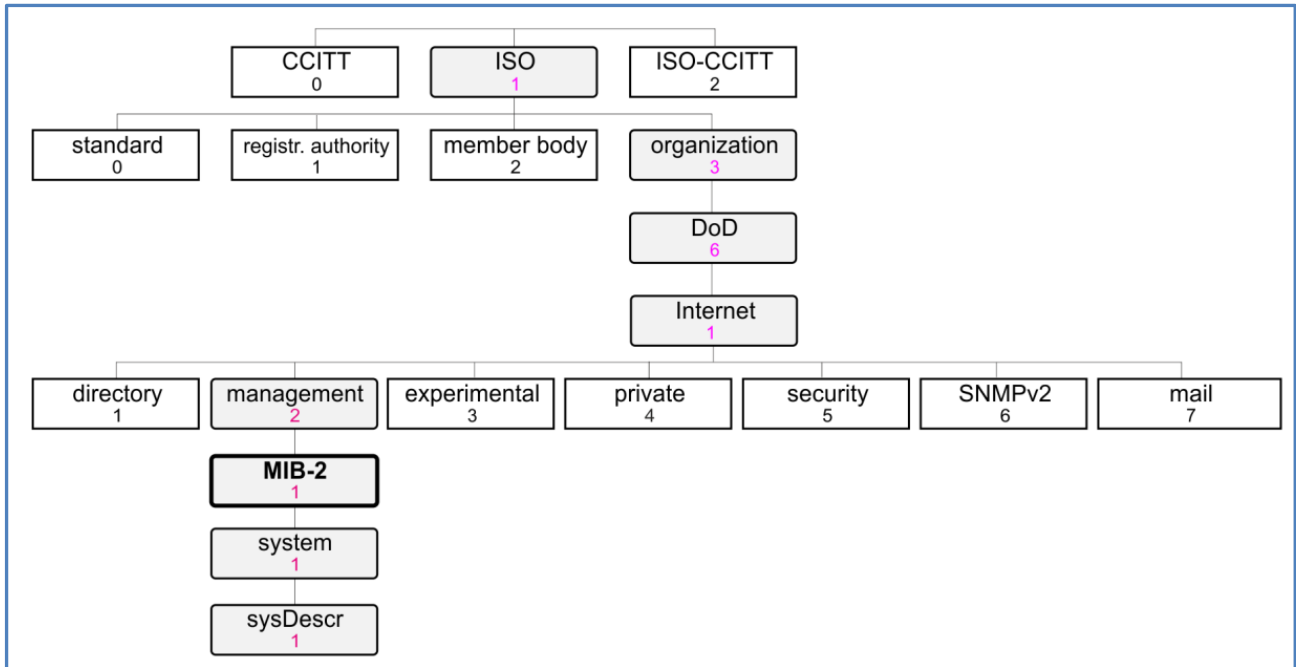


Figure 1.2 MIB structure for "Standard MIBs" with example path
iso.org.dod.internet.management.MIB-2.system.sysDescr (1.3.6.1.2.1.1.1)

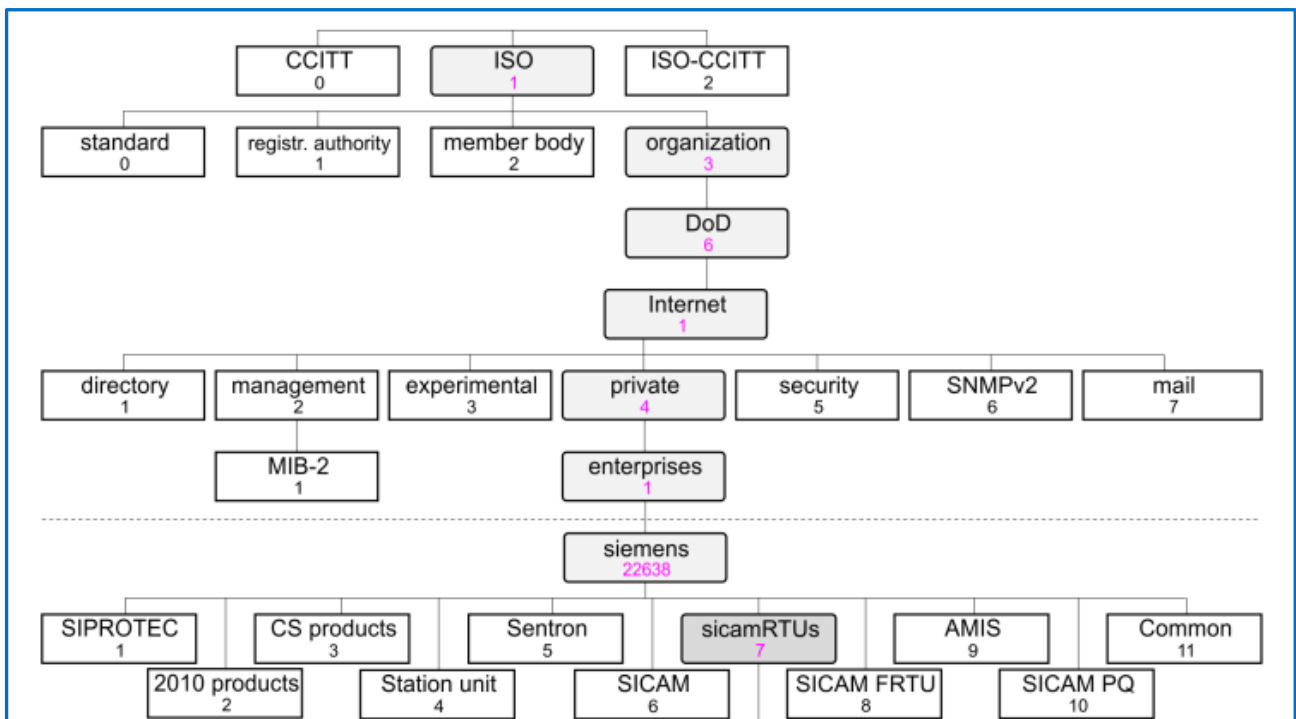


Figure 1.3 MIB structure for "Private MIBs for sicamRTUs with
Path: iso.org.dod.internet.private.enterprises.siemens.sicamRTUs (1.3.6.1.4.1.22638.7)

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

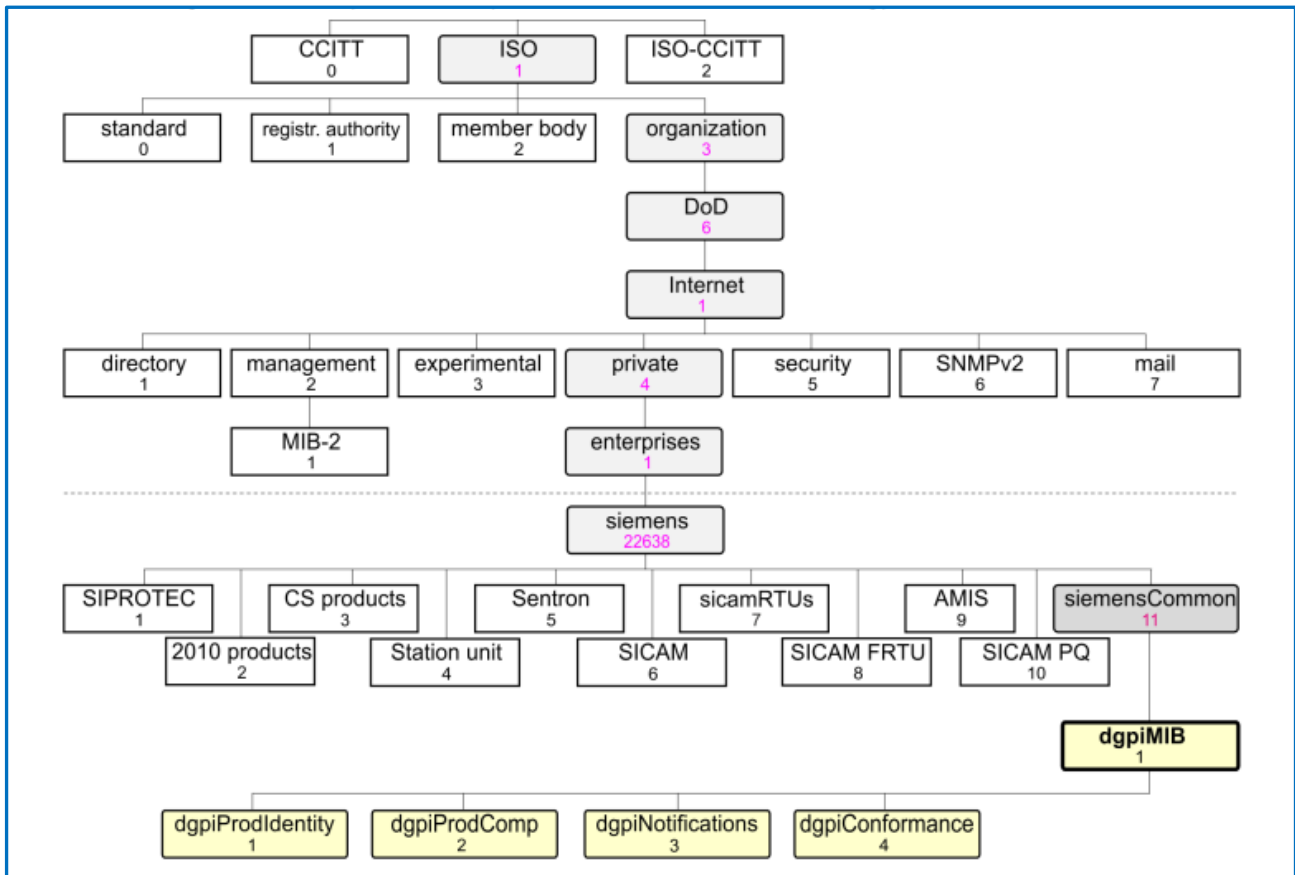


Figure 1.4 MIB structure for “common DG Project inventory MIB” with
Path: iso.org.dod.internet.private.enterprises.siemens.siemensCommon.dgpiMIB (1.3.6.1.4.1.22638.11.1)

In the following documents, you can find the supported “Standard” and “Private” MIBs of the DG EA products (see link collection in chapter ****)

- [1] SIPROTEC 5 Communication Protocols – Manual (chapter 10.11.2/3)
- [2] SIPROTEC 4/SIPROTEC Compact/Reyrolle IEDs Ethernet Module EN100 for IEC 61850 – Manual (chapter 6.1.4 / 7.4)
- [3] Reyrolle 7SR5 Communication Protocol – Manual (chapter 7.8)
- [4] SICAM PAS / PQS - Configuration and Operation – Manual (chapter 6.8)
- [5] SICAM A8000 Series, Manual CP-8050 (chapter 13.23.2)
- [6] SICAM A8000 Series CP-8000, CP-8021, CP-8022 – Manual (chapter 12.21.2)
- [7] SICAM Q100 - 7KG95xx - Power Monitoring Device and Class A Power Quality Recorder (chapter 2.5.5.2)
- [8] SICAM Q200 - 7KG97 - Multifunctional Recorder - Device Manual (chapter 2.5.5.2)

The “private” / “common DG MIBs” can be downloaded from SIOS portal / are stored on the installation DVD / or can be downloaded from the Web-UI of the device

[9] SIPROTEC 5 SNMP MIB

<https://support.industry.siemens.com/cs/document/109742125/siprotec-5-snmp-mib?dti=0&pnid=24232&lc=en-WW>

[10] SICAM RTUs SNMP MIB File

<https://support.industry.siemens.com/cs/document/109773392/sicam-rtus-snmp-mib-file?dti=0&pnid=24232&lc=en-WW>

[11] EN100 Communication Module – Protocols (MIBs for SIP4, SIP Compact, Reyrolle)

<https://support.industry.siemens.com/cs/document/109745821/en100-communication-module-protocols?dti=0&pnid=24232&lc=en-WW>

SICAM PAS (stored on the Software DVD)

SICAM Q100 (private MIB can be downloaded via the integrated Webserver); SICAM Q200 does not use a “Private” MIB

1.2.5 Basic commands of SNMP

The simplicity in information exchange has made the SNMP as widely accepted protocol. The main reason being concise set of commands, here are they listed below:

- **GET:** The GET operation is a request sent by the manager to the managed device. It is performed to retrieve one or more values from the managed device.
- **GET NEXT:** This operation is similar to the GET. The significant difference is that the GET NEXT operation retrieves the value of the next OID in the MIB tree.
- **GET BULK:** The GETBULK operation is used to retrieve voluminous data from large MIB table.
- **SET:** This operation is used by the managers to modify or assign the value of the Managed device.
- **TRAPS:** Unlike the above commands which are initiated from the SNMP Manager, TRAPS are initiated by the Agents. It is a signal to the SNMP Manager by the Agent on the occurrence of an event.
- **INFORM:** This command is similar to the TRAP initiated by the Agent, additionally INFORM includes confirmation from the SNMP manager on receiving the message.
- **RESPONSE:** It is the command used to carry back the value(s) or signal of actions directed by the SNMP Manager.

SNMP Traps:

SNMP traps enable an agent to notify the SNMP manager of significant events by an **unsolicited (spontaneous) SNMP message**. **SNMP Traps** are especially **of interest** for the DG Product Inventory MIB = **DGPI** and the DG Security Monitoring MIB = **DGSM**, because **security related events** (DGSM) and **changes of the device Hardware or Firmware** (DGPI only for CP-8031/50) **can be transferred spontaneous** to the SNMP Manager.

The Figures 1.5 and 1.6 show the Principle of the communication between SNMP Manager and SNMP Agent

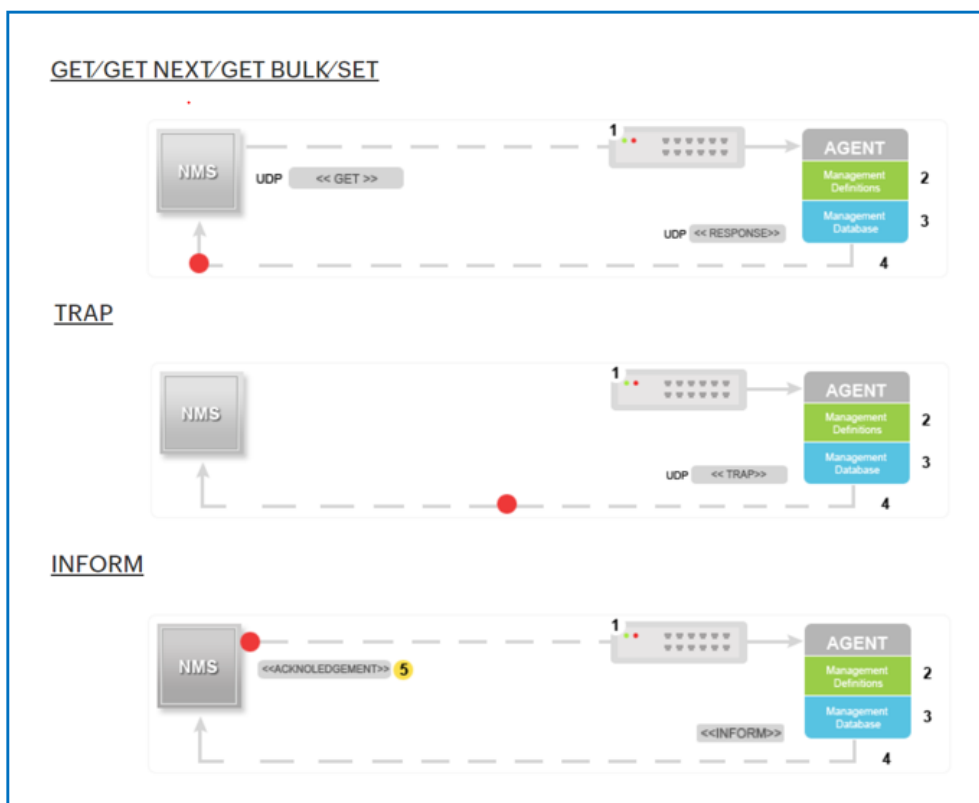


Figure 1.5 Principle of the communication between SNMP Manager and SNMP Agent (<https://www.manageengine.com/network-monitoring/what-is-snmp.html>)

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

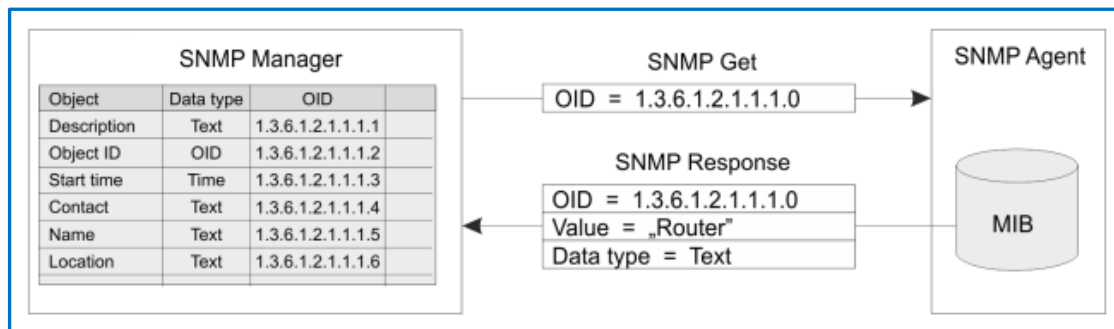


Figure 1.6 Example of a SNMP Get command chain

Being the part of TCP/IP protocol suite, the SNMP messages are wrapped as User Datagram Protocol (UDP) and intern wrapped and transmitted in the Internet Protocol.

By default, the **SNMP port is 161** and **TRAP/INFORM uses SNMP port 162** for communication.

1.2.6 SNMPv3

SNMPv3 defines the secure version of the SNMP. SNMPv3 protocol also facilitates remote network monitoring configuration of the SNMP entities. It is defined by RFC = Request for Comments. Though each version had matured towards rich functionalities, additional emphasis was given to the security aspect on each upgrade.

Security was one of the biggest weakness of SNMP until v3. Authentication in SNMP Versions 1 and 2 amounts to nothing more than a password (community string) sent in clear text between a manager and agent. Each SNMPv3 message contains security parameters which are encoded as an octet string. The meaning of these security parameters depends on the security model being used.

The security approach in v3 targets:

- Confidentiality – Encryption of packets to prevent snooping by an unauthorized source.
- Integrity – Message integrity to ensure that a packet has not been tampered while in transit including an optional packet replay protection mechanism.
- Authentication – to verify that the message is from a valid source.

SNMPv3 also defines the USM (**U**ser-based **S**ecurity **M**odel) and VACM (**V**iew-based **A**ccess **C**ontrol **M**odel), which were later followed by a transport security model (TSM).

- USM (User-based Security Model) provides authentication and privacy (encryption) functions and operates at the message level.
- VACM (View-based Access Control Model) determines whether a given principal is allowed access to a particular MIB object to perform specific functions and operates at the PDU level.
- TSM (Transport Security Model) provides a method for authenticating and encrypting messages over external security channels.

Definition of different **authentication** and privacy protocols. Authentication protocols like MD5 are recommended to encrypt the User/Password to establish the communication; Privacy protocols like AES are recommended to encrypt additionally the content of the message (depending on the source and used communication stack the below listed names can differ even if the algorithm a functionality is identical):

- MD5, SHA and HMAC-SHA-2 authentication protocols and the
- DES / CBC_DES and AES128 / CFB_AES_128 privacy protocols are supported in the USM.

2 Activation of SNMP functionality

The SNMP agent functionality is supported in the DG EA portfolio for our protection devices, for our substation automation devices and for our Power Quality recorder.

Protection devices:

- SIPROTEC 5 devices (with Ethernet ETH-** communication modules)
- SIPROTEC 4, SIPROTEC Compact, Reyrolle, (with EN100 communication module) and Reyrolle 5

Substation Automation Systems:

- SICAM PAS
- A8000 RTUs (CP-8000, CP-8021, CP-8022, CP-8031, CP-8050)

Power Quality recorder:

- SICAM Q100
- SICAM Q200

2.1 Activation of SNMP functionality in SIPROTEC 5 relays

The SNMP functionality in our SIPROTEC 5 relays can be activated on the Ethernet communication modules (ETH-BA-2EL, ETH-BB-2FO and ETH-BD-2FO) using the DIGSI 5 setting tool.

For activation of the SNMP function, open in the project tree the “Hardware and Protocol” Editor of the SIPROTEC 5 device: select in the main working area the communication module for what you want to enable the SNMP function and move in the “Properties” Area to “Protocol” -> “Network” and hook-up the SNMP function

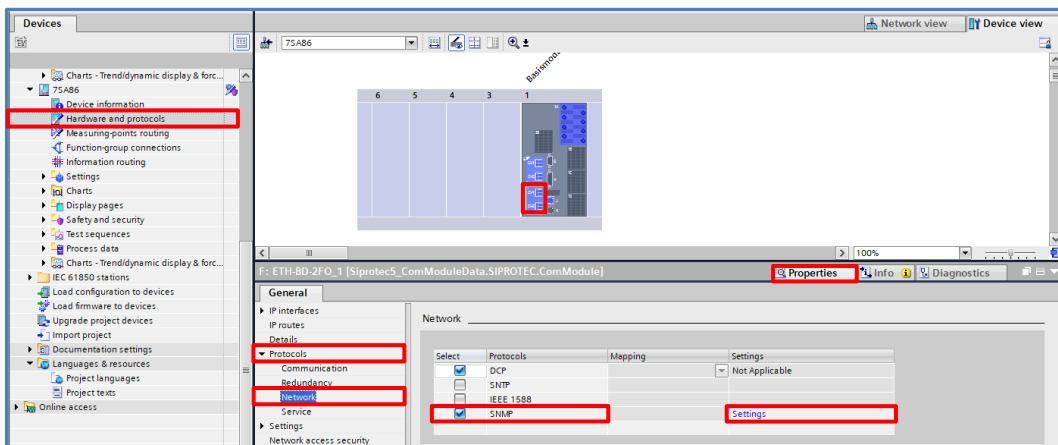


Figure 2.1 Enabling of SNMP in DIGSI 5

The default port for an SNMP Agent is 161 (see chapter 1.2.5); this port is used as default in the SIPROTEC 5 relays, in case you need to change the port number, please select “Settings”

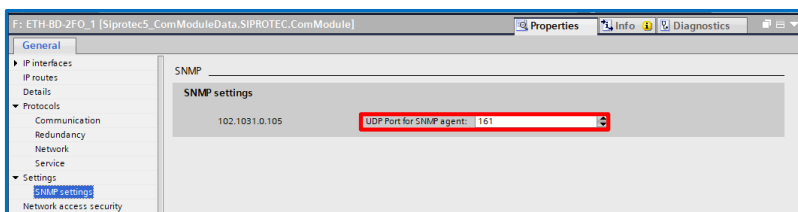


Figure 2.2 Modifying the used port of the SNMP Agent in DIGSI 5

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

2.2 Activation of SNMP in EN100 module for SIPROTEC relays

For SIPROTEC 4 and SIPROTEC Compact devices with EN100 module, the SNMP functionality is per default setting activated. You can check this by using DIGSI 4 and open the settings. Open "Interfaces" with double-click and select in the newly opened dialog box "Interface Setting": "Ethernet on devices" -> there you can see if the SNMP Service is activated.

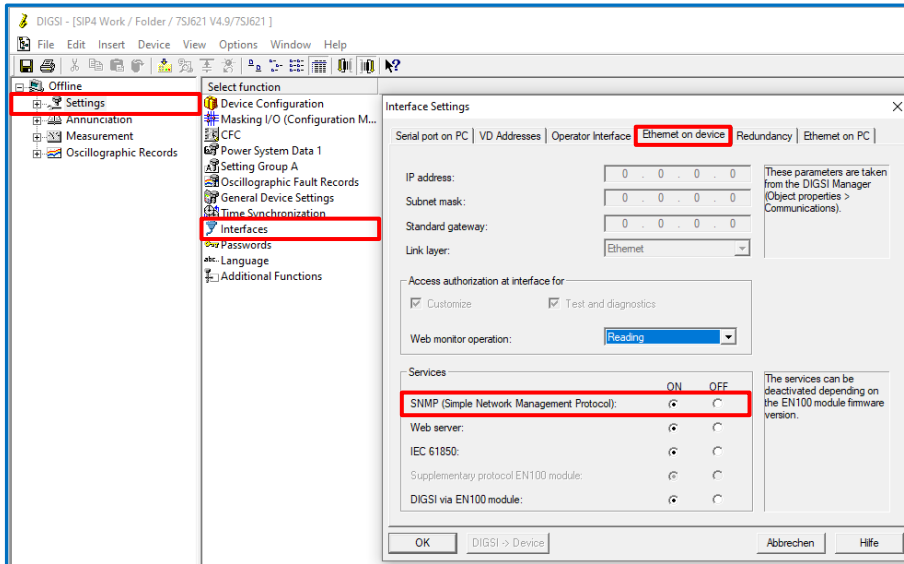


Figure 2.3 Checking of SNMP in DIGSI 4

2.3 Activation of SNMP in Reyrolle relays

For Reyrolle devices with EN100 module and Reyrolle 5, the SNMP functionality is per default setting activated. You can check this by using Reydisp Manager / Reydisp Manager 2 and select the Reyrolle relay. Select in the Editor Area "Ethernet Interface" with double-click and select in the newly opened dialog box: "Services" -> there you can see if the SNMP Service is activated.

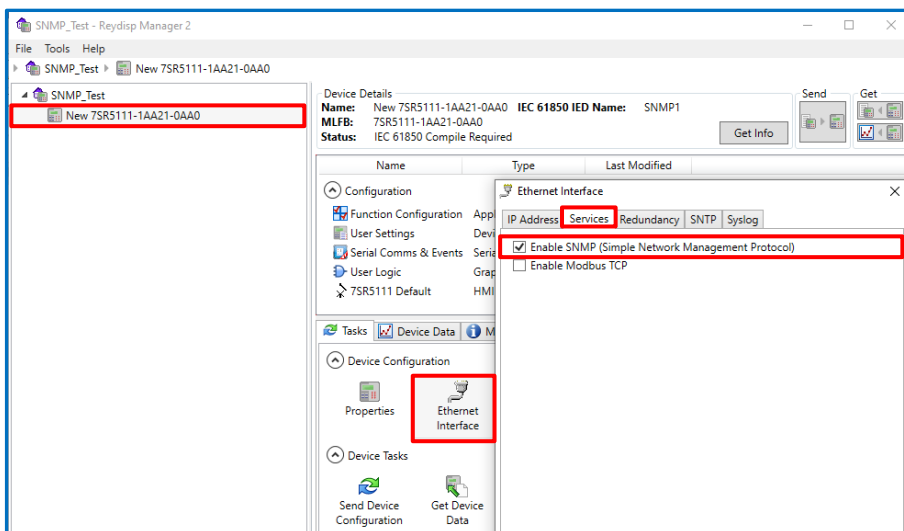


Figure 2.4 Checking of SNMP in Reydisp Manager / Reydisp Manager 2

2.4 Activation of SNMP functionality for SICAM PAS/PQS

In this Application note **only the SNMP Agent functionality** is covered (SICAM PAS/PQS can also have the option to work as a SNMP Client -SNMP Manager-).

As SICAM PAS/PQS is a software-based system and can be installed on more-or-less any PC the SNMP Agent covered in this APN is not related to any information sent from the hardware where the SICAM PAS/PQS software is installed (depending on the PC-Hardware used there may be also SNMP agent functionality available from the PC supplier) but only information regarding the software and the SICAM PAS/PQS applications. The **DG common Product Inventory MIB** is providing information like product name, installed software and database versions, date of last configuration changes, and enabled features etc., and the **DG Security Monitoring MIB** is providing information concerning Security related logs, for example, user login/logout, start/stop of system components, modifications in the archive (import records, import PQDIF, delete records, delete reports, add or edit traffic lights).

The SNMP Agent functionality is not enabled via the SICAM PS/ PQS UI-Configuration like the other functions, but via the SICAM PAS/PQS User Administration. For the initial login after the new installation of SICAM PAS/PQS, enter the username: **Administrator** and the default password: **Admin**.

- To use the Windows access rights, select Use Windows users; or -
- To define individual access rights, select Use internal SICAM PAS/PQS users

The default password must be changed (**forced**) because it is public. Your new password will be maintained even if you have secured all other user rights by using the Windows access rights.

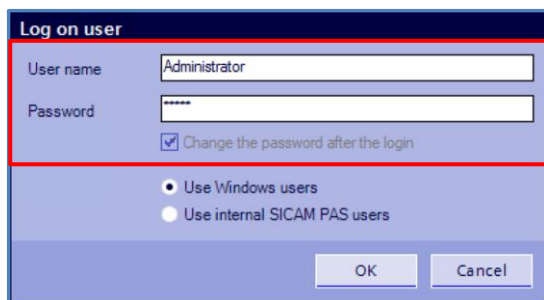


Figure 2.5 SICAM PAS – User Administration

After the SICAM PAS/PQS User Administration UI opens, you can activate / enable the SNMP Agent functionality for the DG Project Inventory MIB (Enable asset monitoring) and for the DG Security Monitoring MIB (Enable security notification) separately and independent from each other. For doing this, use the **"Security"** menu button and select in the selection drop-down **"Enable (SNMP Agent)"**.

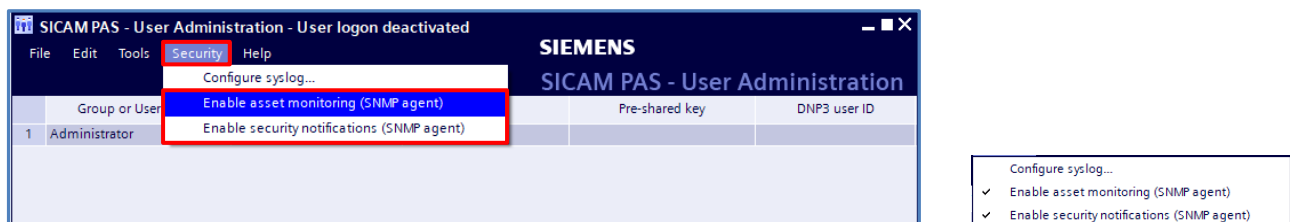


Figure 2.6 SICAM PAS – User Administration enabling SNMP Agents

After activation you can check the status in selecting again the "Security" menu button; the activated SNMP Agents are "hooked-up" (right side small picture in Figure 2.6)

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

2.5 Activation of SNMP functionality for A8000 RTUs

The SNMP function can be enabled either via the TOOLBOX II setting tool or via SICAM Device Manager. In this APN only the SICAM Device Manager as main setting tool for SICAM A8000 RTUs is described; in the CP-850 Manual [5] "SICAM A8000 Series, Manual CP-8050" (chapter 13.23.3) and in the CP-8000, CP-8021, CP-8022 - Manual [6] "SICAM A8000 Series CP-8000, CP-8021, CP-8022 – Manual" (chapter 12.21.3) you can find configuration of SNMP for TOOLBOX II.

2.5.1 Activation of SNMP functionality for CP-8000/8021/8022

For enabling the SNMP agent functionality, the tile "RTU Settings" must be selected from the main Dashboard for the CP-8000/21/22.

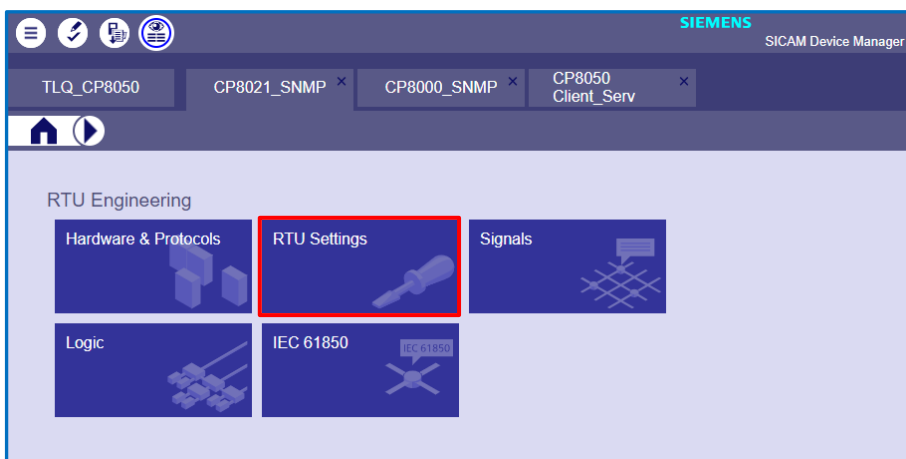


Figure 2.7 SICAM Device Manager main Dashboard

After selecting the tile "RTU Settings" a new setting windows will open. The settings for SNMP are advanced settings and needs to be activated via the  button. Scroll down to "Network settings" and there you can find "SNMP".

In the setting area you can enable the SNMP agent by selecting "yes" from the drop-down menu. Additionally, at least 1 IP address of the counter part of the SNMP agent = SNMP Manager (2 are possible) must be filled in. For the CP-8000/21/22 there is a selection for the SNMP version (either only SNMPv3 or SNMPv2 + SNMPv3)

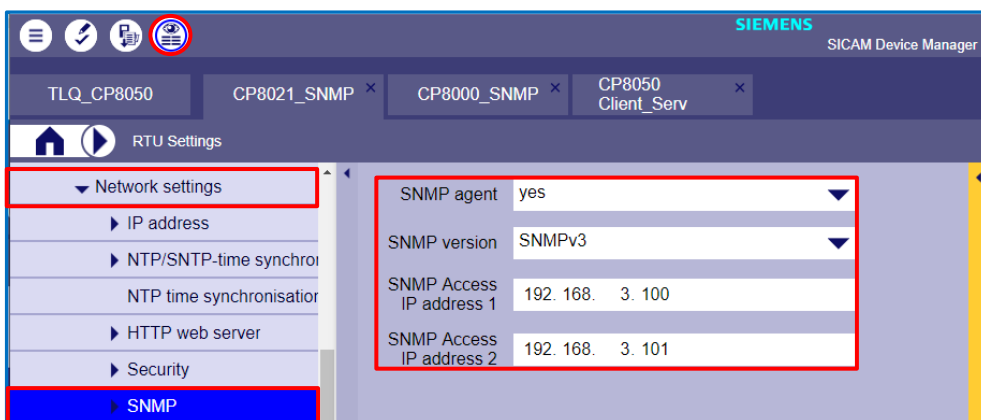


Figure 2.8 Enabling and setting of the SNMP agent in SICAM Device Manager

2.5.2 Activation of SNMP functionality for CP-8050/8031

For enabling the SNMP agent functionality, the tile "Communication" must be selected from the main Dashboard for the CP-8050/31.

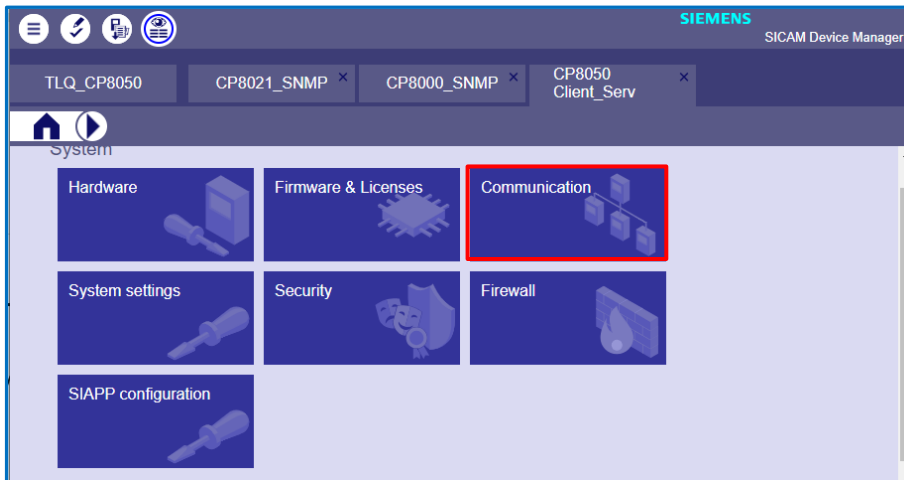


Figure 2.9 SICAM Device Manager main Dashboard

After selecting the tile "Communication" a new setting windows will open. Select first **"LAN interface"**. You can use for SNMP communication either an already existing LAN interface or create via the **"Add"-button** a new interface with the fitting IP-Address. **For the CP-8050/31 1 x physical interface (Port group) can have different IP-addresses.**

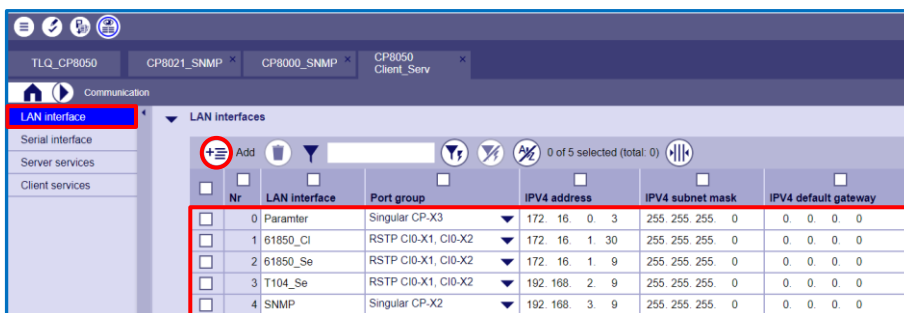


Figure 2.10 Selecting / adding the LAN interface for SNMP communication

Select then **"Server services"** and scroll down to **"Simple Network Management Protocol (SNMP)"**. Use the **"Add"-button** under **"Access list configuration"** to enter the IP-address of the counter part of the SNMP agent = SNMP Manager (2 are possible) and under **"Agent Configuration"** the LAN interface used in the CP-8050/31 for the SNMP communication.

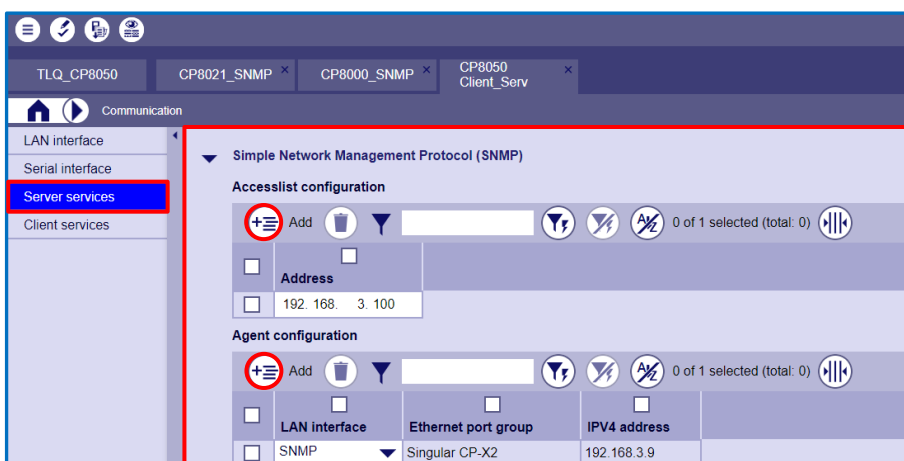


Figure 2.11 Enabling and setting of the SNMP agent and connection to SNMP Manager

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

2.6 Activation of SNMP functionality for SICAM Q100/200

The settings of the SICAM Power Quality recorder SICAM Q100 & Q200 using an internal Web browser with HTML pages from the connected computer (preferred).

In addition, a parameterization of the device is possible with use of the 4 softkeys and display on the front of the device. Not all parameters can be changed (SNMPv3 settings can only be modified via the Web UI).

The IP-Address for SICAM Q100 & Q200 is 192.168.0.55 (for Q200 in case you select 2 independent interfaces the default IP-Address for the second interface is 192.168.1.55)

After connection to the SICAM Q100/200 PQ recorder via the integrated Webserver, you need to navigate to "Configuration" -> "Basic configuration" -> "Communication".

For SICAM Q100 the SNMP agent functionality is enabled via selection **yes in the Checkbox**

For SICAM Q200 the SNMP agent functionality is activated and assigned to one or two Ethernet channels (the option Ch1 and the option Ch2 are only available for **Function** = Two interfaces)

NOTE: Only after pressing the "Send" button the changes are activated in the SICAM Power Quality Recorder

Configuration ► Basic configuration ► Communication

▼ Communication Ethernet

Parameter	
IP address	192.168.2.198
Subnet mask	255.254.0.0
Default gateway	192.168.0.1
Ethernet switch on	☒ no ☐ yes
SNMP	☒ no ☐ yes
Bus protocol	-none-

Send

Note: Please do not operate HTML page during downloading.

SICAM Q100

Configuration ► Basic configuration ► Communication

▼ Ethernet configuration

Parameter	
Function	Switch

▼ Ethernet

Parameter	
DHCP	☒ no ☐ yes
IP address	192.168.97.141
Subnet mask	255.255.0.0
Default gateway	192.168.97.1

▼ Protocol assignment

Parameter	
IEC 61850	-none-
Modbus TCP	-none-
HTTPS	Ch1, Ch2
SNMP	-none-
DNP3 IP	-none-

Send

SICAM Q200

Figure 2.11 Enabling and setting of the SNMP agent for SICAM Q100 and SICAM Q200

3 User administration of SNMPv3

3.1 SNMPv3 general information

SNMPv3 defines the secure version of the SNMP. SNMPv3 protocol also facilitates remote network monitoring configuration of the SNMP entities.

Security was one of the biggest weakness of SNMP until v3. Authentication in SNMP Versions 1 and 2 amounts to nothing more than a password (community string) sent in clear text between a manager and agent. The meaning of these security parameters depends on the security model being used.

The security approach in v3 targets:

- Confidentiality – Encryption of packets to prevent snooping by an unauthorized source.
- Integrity – Message integrity to ensure that a packet has not been tampered while in transit including an optional packet replay protection mechanism.
- Authentication – to verify that the message is from a valid source.

SNMPv3 also defines the USM (**U**ser-based **S**ecurity **M**odel) and VACM (**V**iew-based **A**ccess **C**ontrol **M**odel).

- USM (User-based Security Model) provides authentication and privacy (encryption) functions and operates at the message level.
- VACM (View-based Access Control Model) determines whether a given principal is allowed access to a particular MIB object to perform specific functions and operates at the PDU level.

Definition of different **authentication** and privacy protocols:

- MD5, SHA and HMAC-SHA-2 authentication protocols and the
- CBC_DES and CFB_AES_128 privacy protocols are supported in the USM.

3.2 SNMPv3 availability in DG EA products

The secure SNMPv3 version is available in the following DG EA products

- SIPROTEC 5 relays with Ethernet communication module:
 - **since V1**
- SIPROTEC 4 / Compact / Reyrolle relays with EN100 communication module:
 - needs **EN100 Firmware Version V4.35 or higher**
- Reyrolle 5 relays:
 - **device FW V2.20 or higher and**
 - **communication FW 1.20 or higher**
- SICAM PAS
 - SNMP Client (Manager): V7.01 or higher
 - SNMP Agent: **V8.13 (DGPI)** or higher / **V8.16 (DGSM)** or higher
- SICAM A8000
 - CP-8000 / CP-8021 / CP-8022: **CPC80 Central Processing/Communication Release 09 or higher**
 - CP-8050: **CPCI85 Central Processing/Communication Release 0101 (V1.01) or higher**
 - CP-8031: **CPCI85 Central Processing/Communication Release 0441 (V4.41) or higher**
- SICAM PQ recorder:
 - SICAM Q100: **Firmware version 2.30** or higher and **Hardware Version /DD** or higher
 - SICAM Q200: Since **Firmware Version V1.0**
 - SICAM P855: not supported yet (after new Hardware version will be released)

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

3.3 User administration with SNMPv3 in DG EA products

Essential for the secure communication between the SNMP Agent and the SNMP Manager is the use of SNMPv3, because only with this version the secure communication is possible.

SNMPv3 protocol facilitates a remote configuration from the SNMP Manager of the SNMP Agents user and user rights. Depending on the DG EA product used, there are two possibilities to add and manage the user and the user rights:

- Add and manage the initial users via the device setting tool, that is possible for:
 - SICAM A8000 RTUs
 - SICAM Q100 & Q200 Power Quality Recorder
- Using already existing default / initial user accounts, created with enabling of the SNMP functionality:
 - SIPROTEC 5
 - SIPROTEC 4 / Compact; Reyrolle / Reyrolle 5
 - SICAM PAS

3.3.1 User administration for DG EA products with default user accounts

From the DG EA product portfolio SIPROTEC 5, SIPROTEC 4 & Compact, Reyrolle and Reyrolle 5 protection relays with Ethernet Communication interface and the SICAM PAS substation system are using default user accounts with default credentials.

NOTE:

This default user accounts and especially the default credentials are needed for the first connection and are used as "template" for creation of secure new user accounts with new credentials. After that is done the "template / default" user accounts should be deactivated or better deleted to keep the system secure.

The management of the user accounts are done from a SNMP Manager or a MIB Browser. In this Application Note the **MIB Browser from iReasoning** is used to have an easy grasp of the workflow.

You can download this MIB Browser from: <https://ireasoning.com/download.shtml>. The same or greater functionality is also covered by an open-source tool called **net-snmp** which can also be downloaded from <http://www.net-snmp.org/> (the net-snmp is not coming with a UI but needs to be handled by command line, recommended only for experts)

Attention:

The MIB Browser **Free Personal Edition** **is not supporting** the needed functionality, therefore the MIB Browser **Professional Edition** coming with a 30-day trial period is required.

Precondition for the SNMPv3 user management are the following Standard MIBs what must be available in the MIB Browser before you start:

- rfc3414 SNMP User-based Security Model (USM).mib (or old rfc2574)
- rfc3415 SNMP View-based Access Control Model (VACM).mib (or old rfc2575)

You can use "SNMPLink.org - Standard (RFC, IANA, ATM Forum) MIB Documentation" for accessing and downloading Standard MIBs: <http://www.snmplink.org/OnLineMIB/Standards/>

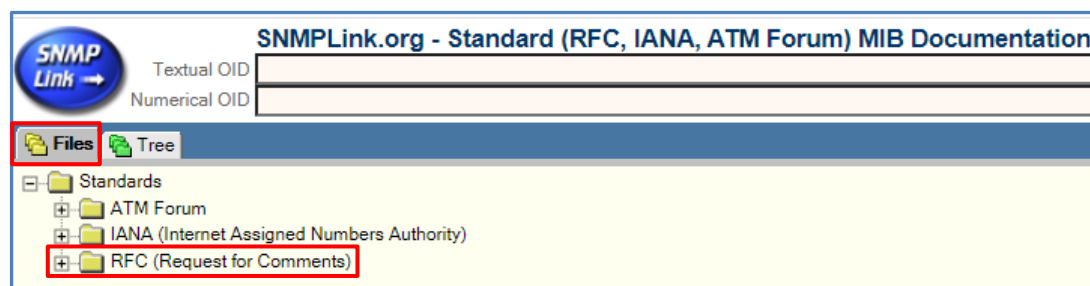


Figure 3.1 SNMP MIB documentation from SNMPLink.org

Open the RFC (Request for Comments) folder under "Files" by clicking on the + sign.

Scroll down until you find the MIB you need (here rfc3414 / rfc3415) and click the MIB (Figure 3.2). In the left-side Window, a new "selector" MIB is created showing the tree structure to the selected MIB the selected MIB will be shown in the right-side Window (Figure 3.3)

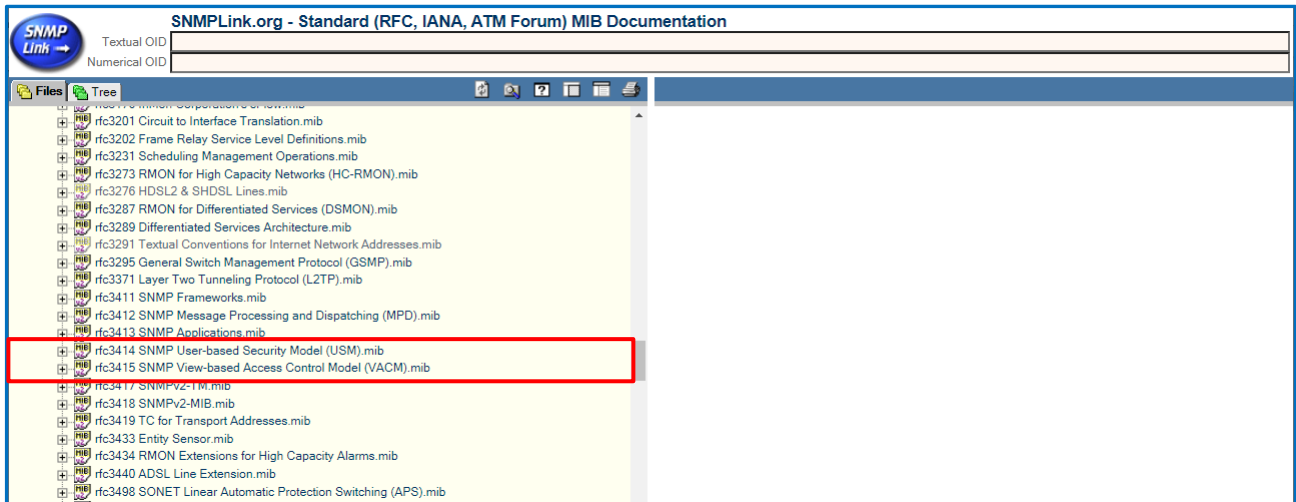


Figure 3.2 SNMP MIB tree under Files, showing all standard MIBs

Now you can select the complete text of the MIB from the right-side Windows (e.g., with CTRL "a") and copy everything (e.g., with "CTRL "c"), create a next *.txt document and paste the text in there (e.g., with CTRL "v") and save the text document.

Now rename the documents e.g., to VACM-MIB / USM -MIB and important also the type of the document to **.mib**: VACM-MIB.mib and USM-MIB.mib (USM MIB is already in the iReasoning MIB-Browser, but maybe not in another Browser)

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

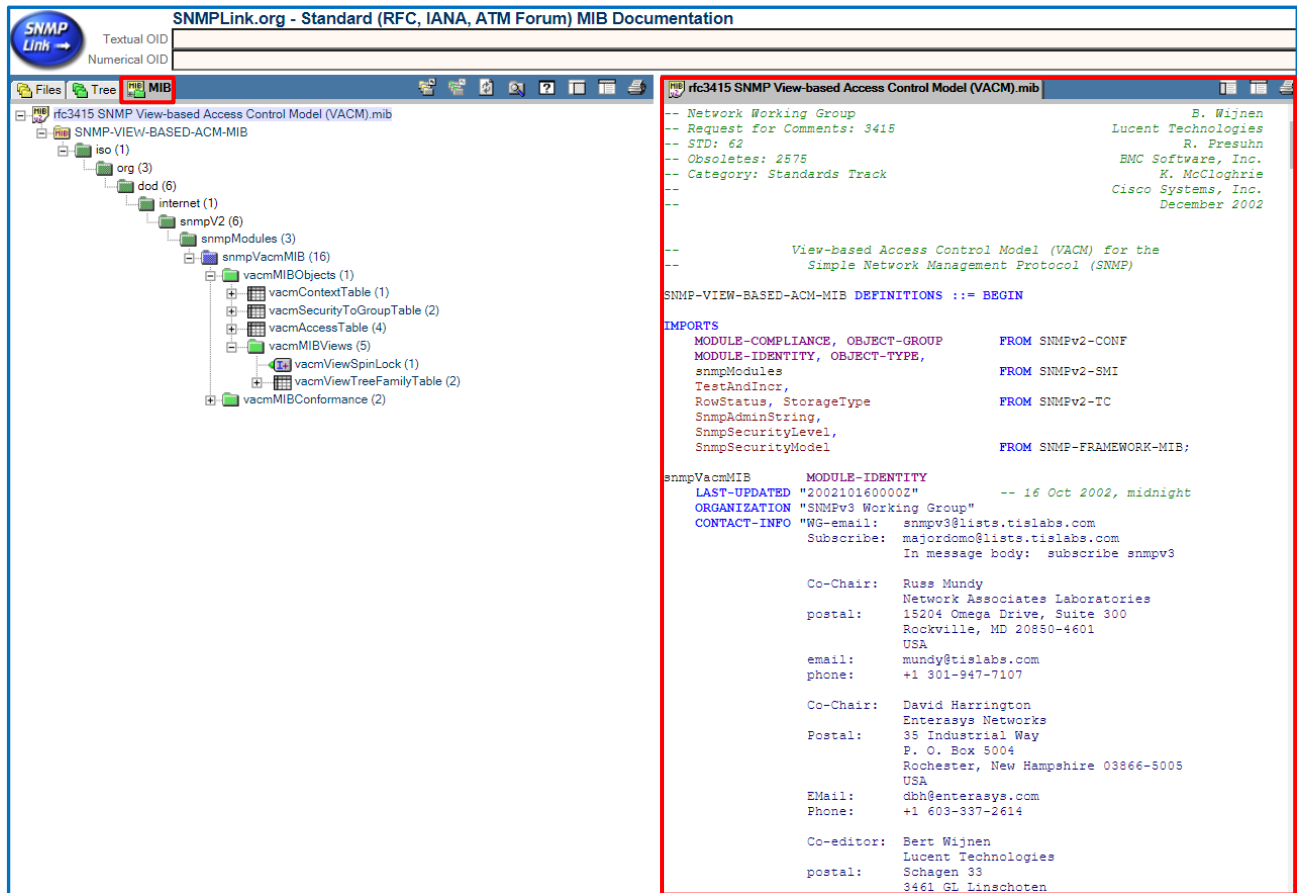


Figure 3.3 MIB tree structure and text description

The user administration via a SNMP Manager or like shown here via the MIB-Browser from iReasoning will take several steps:

Step 1:

Ensure that the needed USM- and VACM-MIB is loaded; if not load / import the missing MIBs first

Step2:

Connect your SNMP agent device via default user account to the SNMP Manager (in our case iReasoning MIB-Browser)

Step 2a:

Check if the connection was successful.

Step 3:

Create a new user with new credentials as "clone" from the default user

Step 4:

Add the new created user into the access list (**View-based Access Control Model**)

Step 4a:

Check is the new user account with new credentials is working

Step 5:

Delete the default user accounts

Step1: Ensure that the needed USM- and VACM-MIB is loaded

Open the iReasoning MIB-Browser and check what MIBs are already loaded.

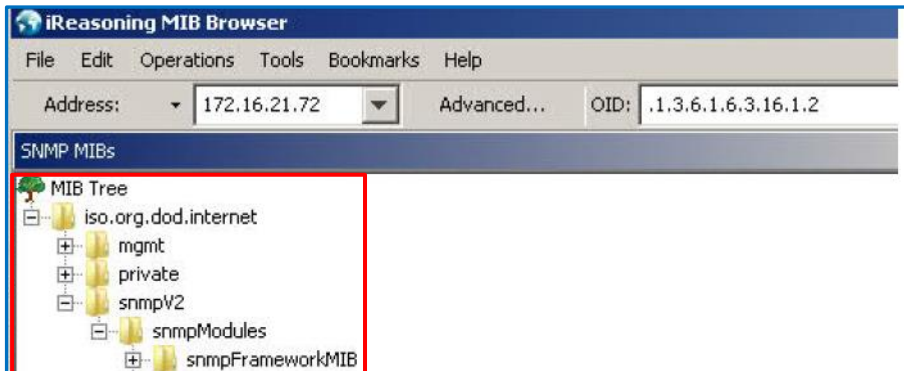


Figure 3.4 iReasoning MIB-Browser with installed MIBs

The USM MIB is already loaded when using the **Professional Edition** with 30-day trial period, but not the VACM-MIB.

The saved VACM-MIB.mib (Figure 3.3) must now be loaded / imported first into the MIB Tree of the iReasoning MIB-Browser.

Select "File" and in the drop-down menu "Load MIBs". A new dialog box will open to select the location folder on your PC or USB drive => select there the location where you saved the VACM-MIB.mib (eventually you need to enter as File type *.*) and the file itself and press the "Open button" for importing the MIB file.

For the "Private" / "Common DG" MIBs (see chapter 1.2.4) the same loading / importing process is used.

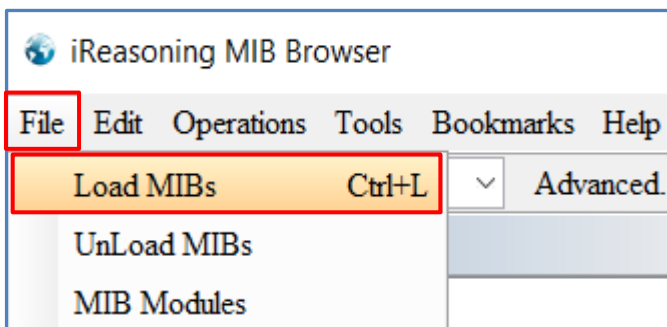


Figure 3.5 Loading VACM-MIB into the MIB Tree

Check after the import if the VACM-MIB is now visible in the MIB Tree of the iReasoning MIB-Browser.

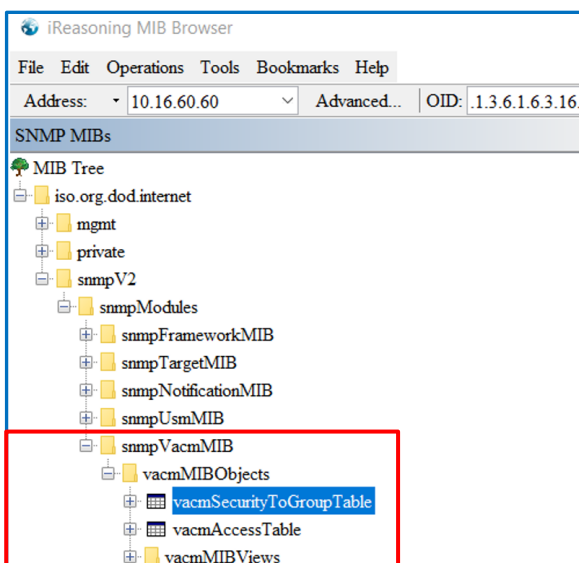


Figure 3.6 iReasoning MIB-Browser with installed MIBs

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

Step2: Connect your SNMP agent device via default user account to the SNMP Manager

For the first connection from your physical device with SNMP Agent functionality to the SNMP Manager / iReasoning MIB-Browser, you need to use the initial / default user account with the default credentials.

The following initial / default user and credentials are defined:

SIPROTEC 5: ETH-BA-2EL / ETH-BB-2FO / ETH-BD-2FO communication modules

User	Authentication Algorithm	Authentication Password	Encryption/Privacy Algorithm	Privacy Password	Access Rights
Initial ¹	No	No	No	No	Read
templateMD5	MD5	12345678	DES	12345678	Read, Write
templateSHA	SHA	12345678	DES / AES ²	12345678	Read, Write

¹ User „initial“ is not available in ETH-BD-2FO module due to security reasons

¹ Encryption algorithm is AES for ETH-BD-2FO module due to security reasons, in the rest of the modules it is DES

SIPROTEC 4 / Compact / Reyrolle: EN100 E+/O+ communication modules

User	Authentication Algorithm	Authentication Password	Encryption/Privacy Algorithm	Privacy Password	Access Rights
Initial	No	No	No	No	Read
managersha256aes	SHA256	sha256authpw	AES	sha256privpw	Read, Write

Reyrolle 5:

User	Authentication Algorithm	Authentication Password	Encryption/Privacy Algorithm	Privacy Password	Access Rights
Initial	No	No	No	No	Read
templateMD5	(HMAC-) MD5	12345678	DES	12345678	Read, Write
templateSHA	(HMAC-) SHA	12345678	AES	12345678	Read, Write

SICAM PAS/PQS:

User	Authentication Algorithm	Authentication Password	Encryption/Privacy Algorithm	Privacy Password	Access Rights
Admin	SHA512	12345678	AES128	12345678	Read, Write

For establishing an online connection, you need to put the IP-Address of your SNMP Agent device in the Address fields and press the “Advanced...” button

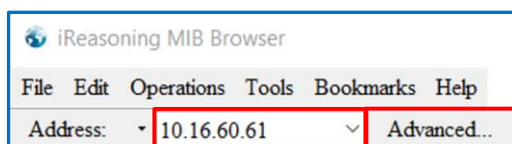


Figure 3.7 Connecting to the SNMP Agent device

The Advanced Properties Dialog-Box will open; there you need to enter the port number 161 (standard SNMP port, if not modified in DIGSI 5) and the SNMP Version: 3

The user and credentials as shown in the tables above (depending what device type is connected) needs to be entered and for the “Security Level”: auth, priv. When finished with the entrees, press the “Ok” button

Advanced Properties of SNMP Agent

Address: 10.16.60.61

Port: 161

Read Community:

Write Community:

SNMP Version: 3

SNMPv3

USM User: templateMD5

Security Level: auth, priv

Auth Algorithm: MD5

Auth Password: *****

Privacy Algorithm: DES

Privacy Password: *****

Context Name:

Engine ID: 0x 80 00 58 6E 03 00 A0 1E 10 3C 3D

Localized Auth Key: 0x 3D A1 4E 1D 2E 8B DA 25 70 0F C7 0A 88 32 66 CA

Localized Priv Key: 0x 3D A1 4E 1D 2E 8B DA 25 70 0F C7 0A 88 32 66 CA

Ok Cancel

Figure 3.8 Entering the user and credential information

Step 2a: Check if the connection was successful

Press the 'Go' button and you should get some SNMP readings on the 'Result Table'

iReasoning MIB Browser

File Edit Operations Tools Bookmarks Help

Address: 10.16.60.61 Advanced... OID: 1.3.6.1.2.1.2.1.0 Operations: Get Next Go

SNMP MIBs

MIB Tree

iso.org.dod.internet

Result Table

Name/OID	Value	Type	IP-Port
#Number.0	3	Integer	10.16.60.61

Figure 3.9 Checking if the connection was successful

Step 3: Create a new user with new credentials as "clone" from the default user

To create a new User, you need to clone an existing default User which will be the recommended way instead creating a new user.

Important:

You need to be logon on with an Account based on the same Auth Protocol you want to clone. Otherwise, the password change for Authentication may fail.

Go to "Tools" and select in the drop-down menu "Manage SNMP v3 USM Users" (Figure 3.10) and select in the right-side working area "USM Users" and select the line you want to use as template (MD5/SHA) and press 'Clone' (Figure 3.11)

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

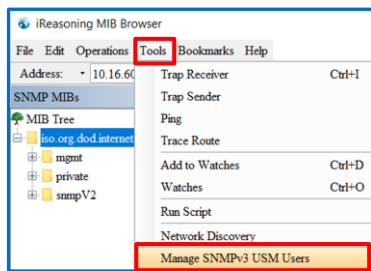


Figure 3.10 Managing SNMPv3 Users

Result Table						
USM Users						
Clone		Activate	Password	Deactivate	Delete	 Refresh
	User Name	Auth Protocol	Priv Protocol	Storage	Status	
1	initial	No Auth	No Priv	nonVolatile (3)	active (1)	
2	templateMD5	HMAC-MD5	DES	nonVolatile (3)	active (1)	
3	templateSHA-1	HMAC-SHA-1	DES	nonVolatile (3)	active (1)	

Figure 3.11 Selecting the default / initial user as Template for the new user

After pressing the Clone button has been pressed a new dialog windows will be opened (Figure 3.12); enter there the **New Username** and press the **Ok** button,

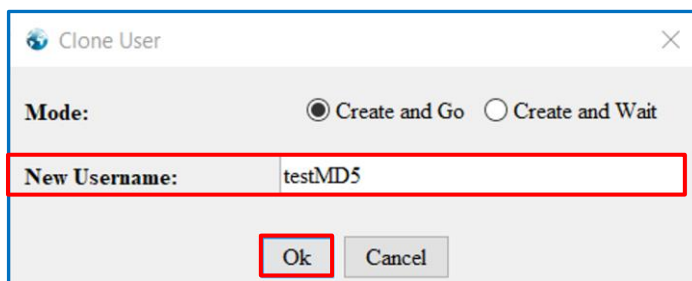


Figure 3.12 Entering the new username

Right click on the new user (Figure 3.13) and change the Authentication/Privacy password (Figure 3.14 for Auth. PW)

You need to provide **the old password and the new password**. Password requires minimum 8 characters which can include (not must) uppercase and lowercase letters, numbers, and special characters.

Result Table		USM Users ×				
Clone		Activate	Password	Deactivate	Delete	 Refresh
	User Name	Auth Protocol	Priv Protocol	Storage	Status	
1	initial	No Auth	No Priv	nonVolatile (3)	active (1)	
2	testMD5	HMAC-MD5	DES	nonVolatile (3)	active (1)	
3	templateMD5	Clone User		nonVolatile (3)	active (1)	
4	templateSHA	Activate User		nonVolatile (3)	active (1)	
		Change Authentication Password				
		Change Privacy Password				
		Deactivate User				
		Delete User				

Figure 3.13 Modify the credentials for the new user

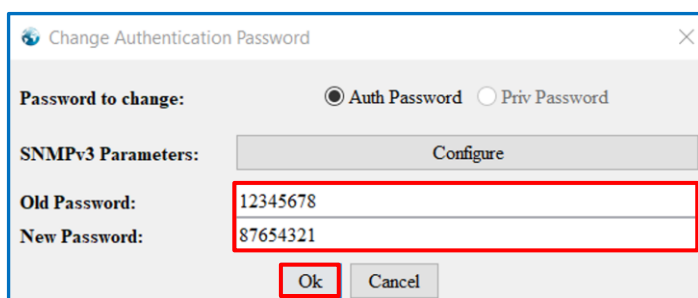


Figure 3.14 Modify the credentials for the new user

Step 4: Add the new created user into the access list (View-based Access Control Model)

The new user is now entered and known for **User-based Security Model**; but needs to be added and activated with its rights additionally into the **View-based Access Control Model** group.

For doing this, please select in the MIB Tree under **snmpVacmMIB** -> **vacmSecurityToGroupTable** (Figure 3.15) and select **"Table View"** to open the Table with activated Users.

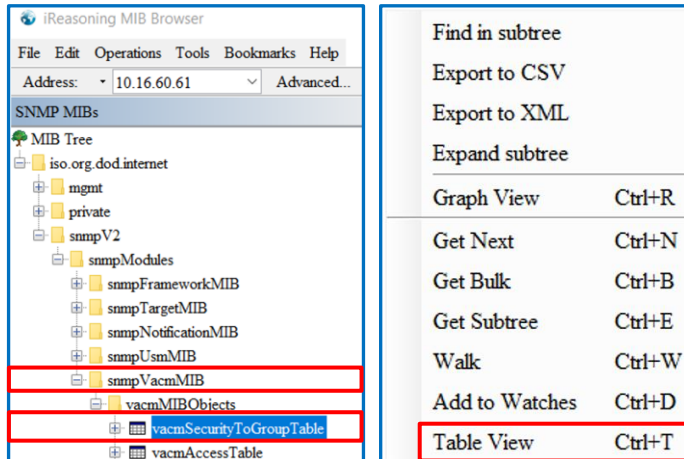


Figure 3.15 VACM node for opening the Table with activated users

You can see the default / initial users in this table, **but not the newly cloned user**. Select in the working area the **VACM-SecurityToGroup Table** and push **"Create Row"** (Figure 3.16)

Result Table					
USM Users					
10.16.60.61 - vacmSecurityToGroupTable					
					Index Value
3	initial	initial	nonVolatile	active	[1] 3.7.105.110.105.116.105.97.108
3	templateMD5	initial	nonVolatile	active	[2] 3.11.116.101.109.112.108.97.116.101.77.68.53
3	templateSHA	initial	nonVolatile	active	[3] 3.11.116.101.109.112.108.97.116.101.83.72.65

Figure 3.16 Creating a new entree for the new user

In the new Dialog-Box (Figure 3.17), you need to enter **exactly the name of the new closed user** under **vacmSecurityName** and the shown other settings. When finished, press the **Ok** button.

The image shows a 'Create a new row' dialog box. It has several input fields and dropdown menus. The 'vacmSecurityModel' field is set to '3' with a data type of 'Integer'. The 'vacmSecurityName' field is set to 'testMD5' with a data type of 'OctetString'. The 'Action' dropdown is set to 'Create And Go'. Below these fields, there is a section for 'Additional variable bindings to be included in request (optional, empty values are ignored)'. This section contains two rows: 'vacmGroupName' with a data type of 'OctetString' and a value of 'initial', and 'vacmSecurityToGroupStorageType' with a data type of 'Integer' and a value of '3'. At the bottom of the dialog, there are 'Ok' and 'Cancel' buttons. The 'Ok' button is highlighted with a red box.

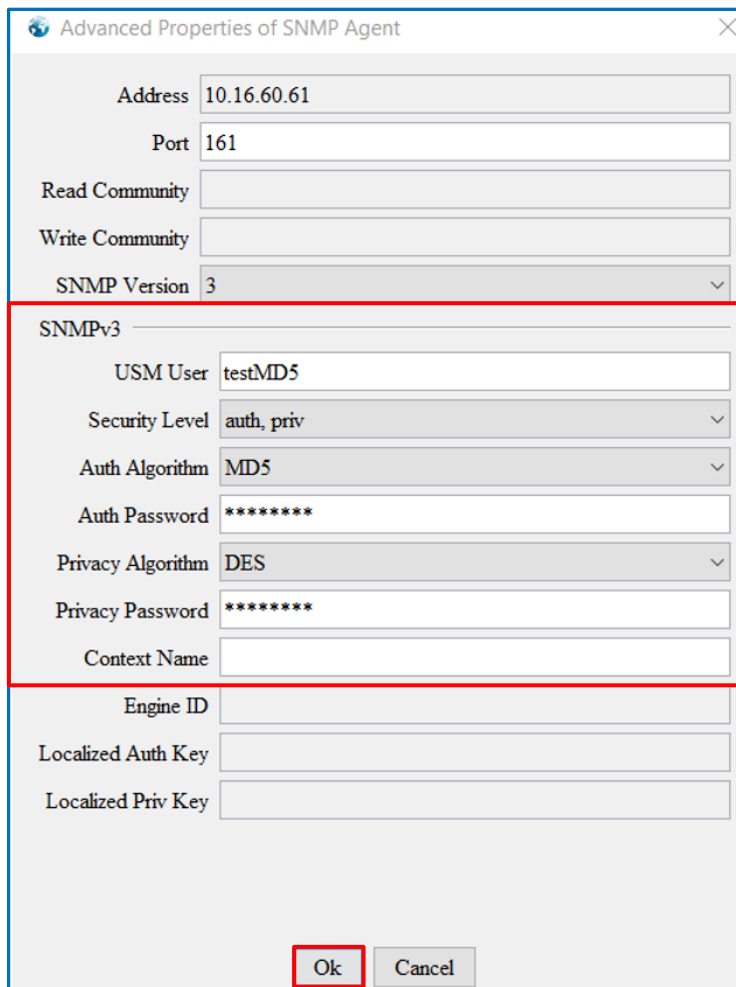
Figure 3.17 Entering the detail for the new user

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

Step 4a: Check is the new user account with new credentials is working

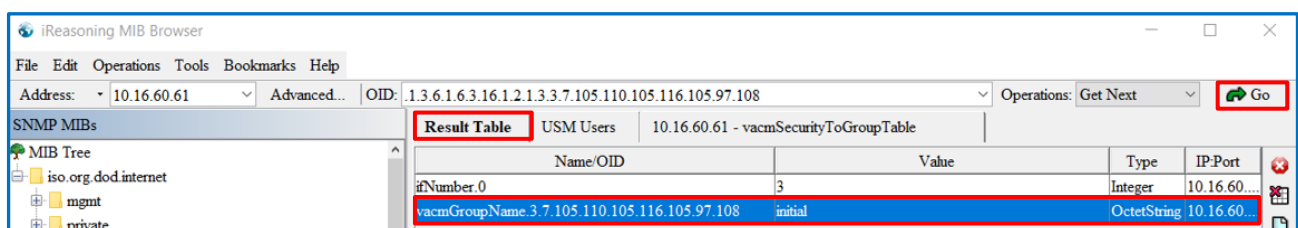
Check by clicking on **"Advanced"** (see Figures 3.7) and use the new **username & settings** as shown in Figures 3.19



The image shows a dialog box titled "Advanced Properties of SNMP Agent". It contains several input fields and dropdown menus. The "Address" field is set to "10.16.60.61" and the "Port" field is set to "161". The "Read Community" and "Write Community" fields are empty. The "SNMP Version" dropdown is set to "3". A red rectangular box highlights the "SNMPv3" section, which includes the following fields: "USM User" (testMD5), "Security Level" (auth, priv), "Auth Algorithm" (MD5), "Auth Password" (masked with asterisks), "Privacy Algorithm" (DES), "Privacy Password" (masked with asterisks), and "Context Name" (empty). Below the "SNMPv3" section, there are fields for "Engine ID", "Localized Auth Key", and "Localized Priv Key", all of which are empty. At the bottom of the dialog, there are "Ok" and "Cancel" buttons, with the "Ok" button highlighted by a red rectangular box.

Figure 3.18 Entering the detail for the new user

After the login information under the newly created user has been entered press the **"Go"** button and you should get some new SNMP readings on the **"Result Table"** (Figure 3.19)



The image shows a screenshot of the "iReasoning MIB Browser" application. The "Address" field is set to "10.16.60.61" and the "OID" field is set to ".1.3.6.1.6.3.16.1.2.1.3.3.7.105.110.105.116.105.97.108". The "Operations" dropdown is set to "Get Next". A red rectangular box highlights the "Go" button. The "Result Table" is displayed, showing the following data:

Name/OID	Value	Type	IP:Port
ifNumber.0	3	Integer	10.16.60....
vacmGroupName.3.7.105.110.105.116.105.97.108	initial	OctetString	10.16.60...

Figure 3.19 Checking if the newly created user is activated

Step 5: Delete the default user accounts

It is strongly recommended deactivating or better removing the Default / Initial Accounts and no longer used Accounts in the USM Users Table. Only than the Cyber Security Aspect is really considered.

Open the USM User Table via "Tools" and drop-down menu "Manage SNMPv3 USM Users" (Figure 3.20)

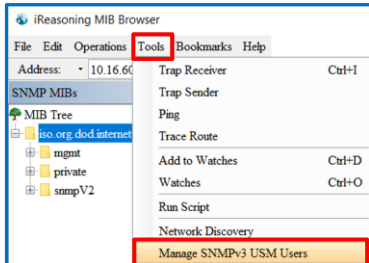


Figure 3.20 Managing SNMPv3 Users

Select the "USM Users" Tab and select one Default / Initial User or no longer used/needed User and press the "Delete" button, repeat this for all other Default / Initial User or no longer used/needed User until all of them are deleted.

Result Table	USM Users	10.16.60.61 - vacmSecurityToGroupTable			USM Users
Clone	Activate	Password	Deactivate	Delete	 Refresh
	User Name	Auth Protocol	Priv Protocol	Storage	Status
1	initial	No Auth	No Priv	nonVolatile (3)	active (1)
2	testMD5	HMAC-MD5	DES	nonVolatile (3)	active (1)
3	templateMD5	HMAC-MD5	DES	nonVolatile (3)	active (1)
4	templateSHA	HMAC-SHA-1	DES	nonVolatile (3)	active (1)

Figure 3.21 Selecting the default / initial user as Template for the new user

Note:

If the parameterization / activation for SNMP is removed and these changes are loaded in the device, all previous settings made for SNMP on the Ethernet communication module are deleted. This means that the initial state applies when parameterizing /activating the SNMP again. If you modify the configuration of SIPROTEC5 device without modifying SNMP, then SNMP remains just as before. This behavior is driven by Cyber Security rules and should be generally valid.

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

3.3.2 User administration for DG EA products via device setting tools

The following DG EA products are not using default / initial users for the SNMP Agent functionality, but the users must be defined within the device setting tools

- SICAM A8000 RTUs (CP-8000/21/22 and CP8050/31)
- SICAM Power Quality Recorder (Q100 & Q200)

Settings for A8000 RTUs CP-8000/21/22:

Please see the screenshots shown in Figure 2.7 and 2.8 showing the activation of the SNMP Agent functionality

Main Dashboard -> select there **RTU Settings** enable in RTU Settings the **expert view** and scroll down to **Network Settings** and select **SNMP**

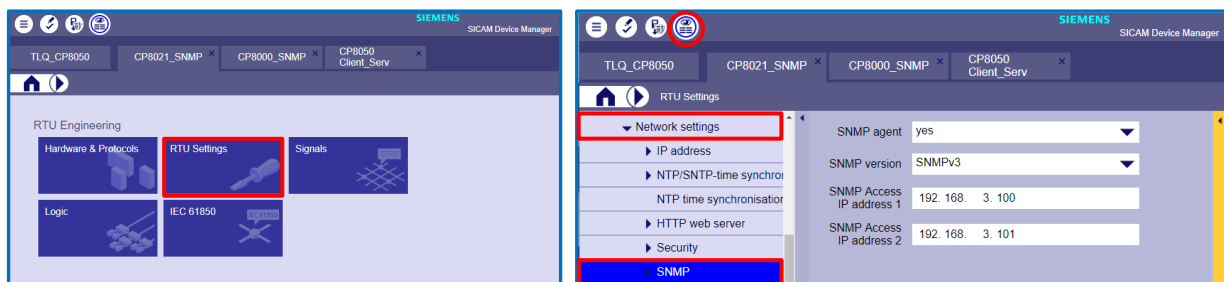


Figure 3.22 SNMP Settings for CP-8000/21/22

Under the node SNMP you can find the settings for the **SNMPv3** security settings (Figure 3.23). The Security level is fixed and cannot be changed (highest level for SNMPv3).

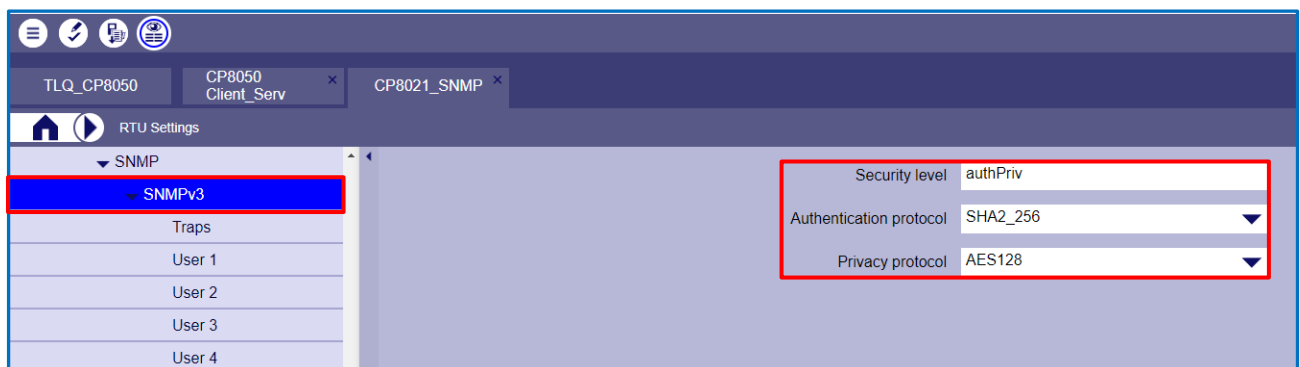


Figure 3.23 SNMP Security Settings for CP-8000/21/22

The used algorithms for the Authentication and the Privacy protocol can be selected from a drop-down menu (Figure 3.24) and are common for all users what are created.

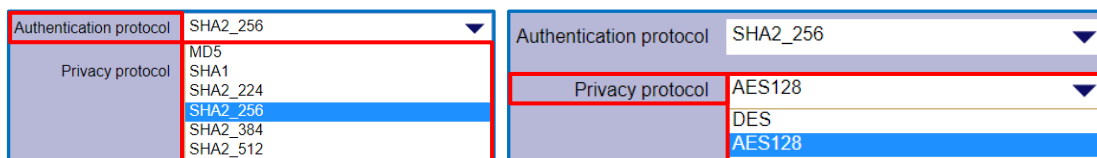


Figure 3.24 SNMP Security Algorithms for CP-8000/21/22

Up to 4 users can be created (Figure 3.25). Each user must be **enabled** (preparation in advance possible and enabling later) and have a Username and Passwords for the Authentication and for the Privacy (Encryption). Also, the allowed rights read only or read and write rights can be selected here.

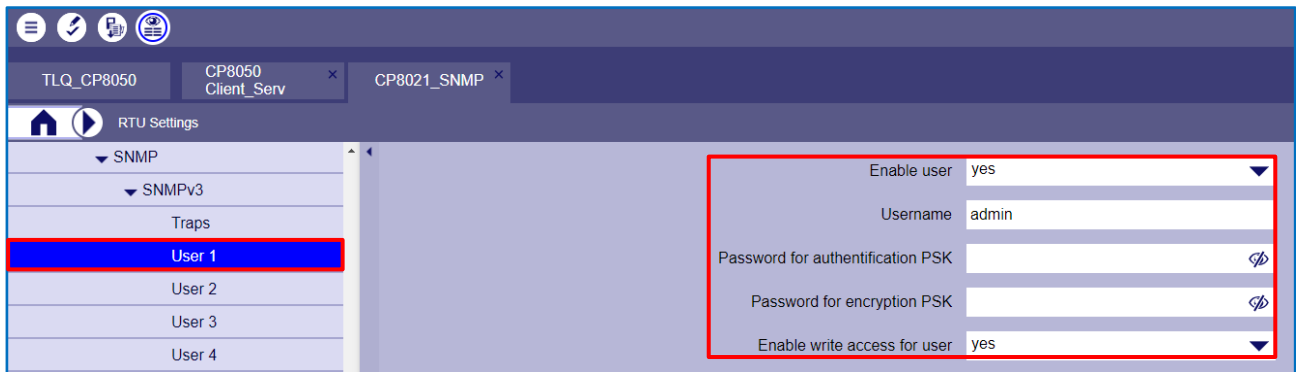


Figure 3.25 SNMPv3 User

The A8000 RTUs also allow unsolicited / spontaneous sent information to the SNMP Manager => so-called **Traps**; this is **only possible for diagnostic information via the private sicamRTU MIB** (see [6] SICAM A8000 Series CP-8000, CP-8021, CP-8022 – Manual Chapter 12.21.5.2).

The Trap function is running per default over port 162 and needs to be enabled (**Enable traps and Diagnostic traps**) for the SNMP Agent and of course also protected via **passwords for the Authentication and for the Privacy**.

The IP-Address of the SNMP Manager receiving the spontaneous sent information also needs to be entered here

Note:

The necessary settings and action on SNMP Manager / iReasoning side for receiving traps will be covered in Chapter 5.

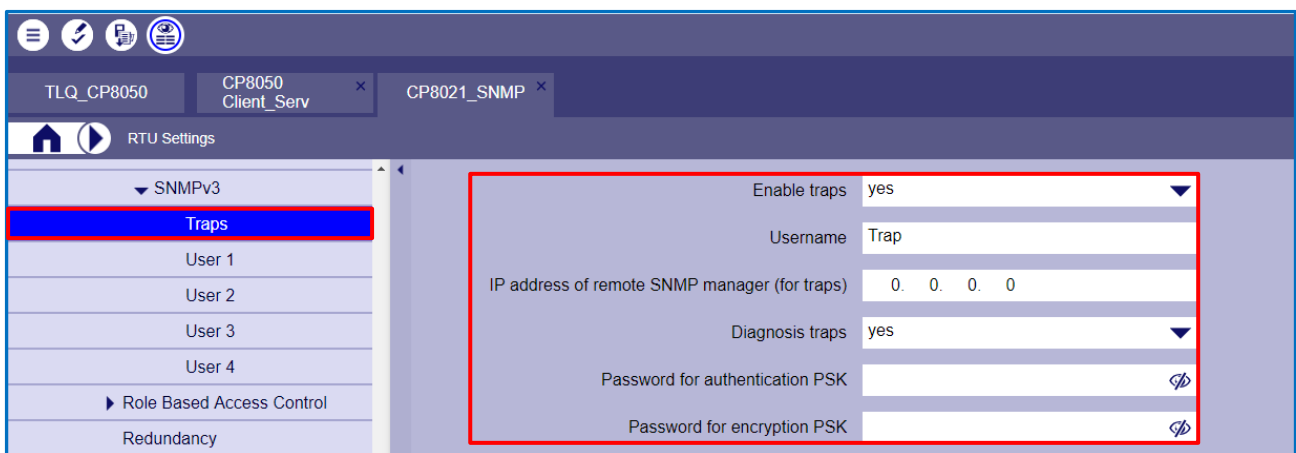


Figure 3.26 SNMPv3 Trap configuration

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

Settings for A8000 RTUs CP-8031/50:

Please see the screenshots shown in Figure 2.9 and 2.11 showing the activation of the SNMP Agent functionality

Main Dashboard -> select the **Communication** tile and define under **Accesslist configuration** up to two SNMP Manager IP-addresses what can access the information and under **Agent configuration** the network(s) for the communication of the SNMP information exchange (Figure 3.27).

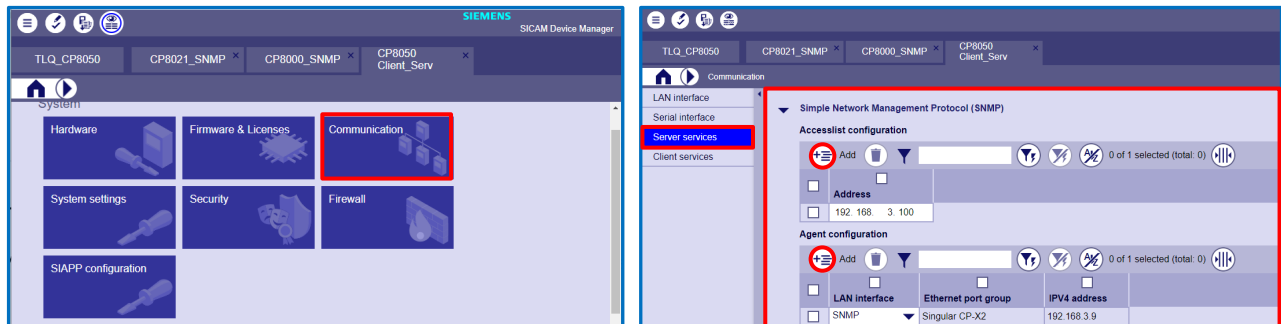


Figure 3.27 SNMP Settings for CP-8000/21

Up to 4 users can be created under **User Configuration** (Figure 3.28) via the **Add** button. Each user must be **enabled** (preparation in advance possible and enabling later) and have a Username and must be **assigned** to one of five possible sets of credentials (Passwords for the Authentication and for the Privacy / Encryption). The allowed rights read only or read and write rights can be selected here. Under **Crypto Settings** the credentials are created via the **Add** button and then configured (up to five sets are possible).

The used algorithms for the Authentication and the Privacy protocol can be selected from a **drop-down menu** (Figure 3.29). Up to five different crypto settings can be created (for up to 4 users & 1 credentials for the traps)

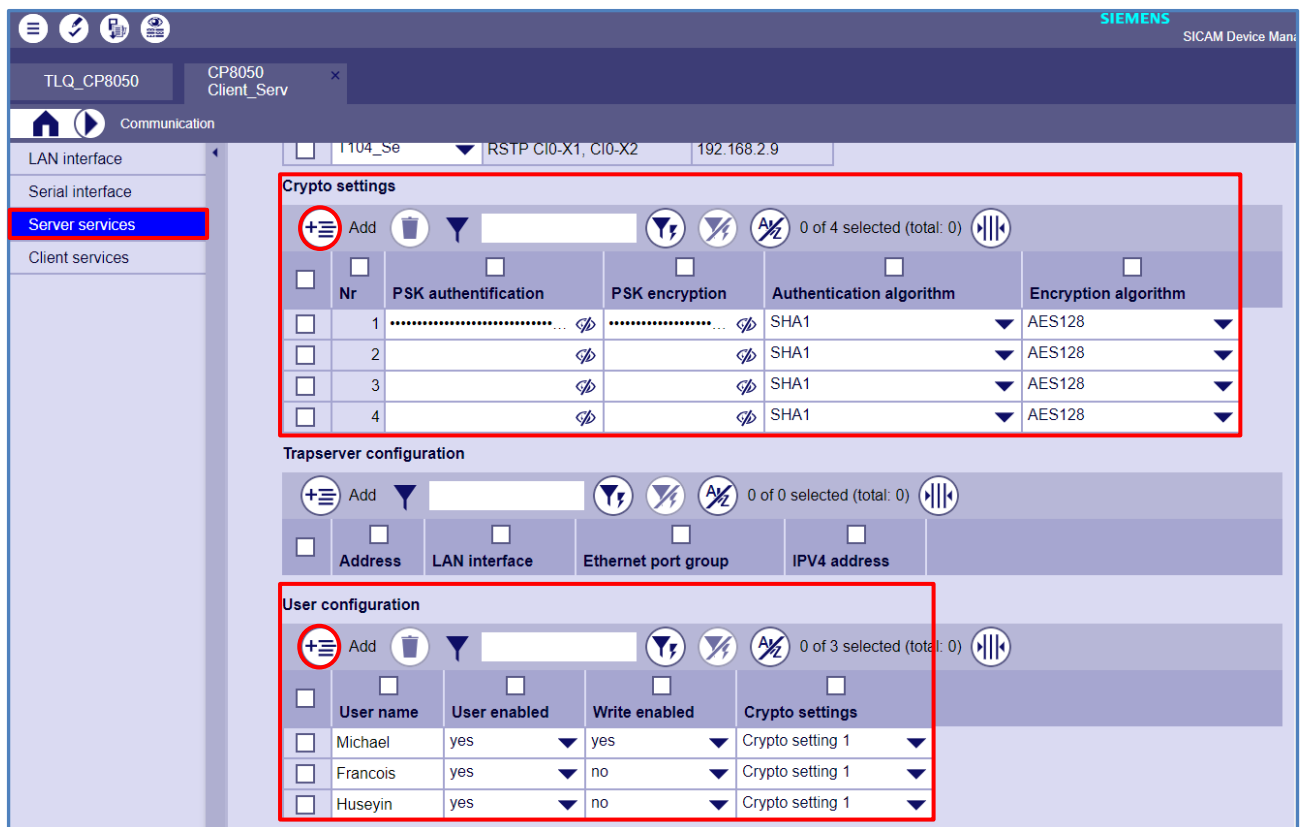


Figure 3.28 SNMPv3 Users with properties and assigned credentials (privacy / encryption & authentication)

Figure 3.29 SNMP Security Algorithms for CP-8031/50

The A8000 RTUs also allow unsolicited / spontaneous sent information to the SNMP Manager => so-called **Traps**; this is available for **diagnostic information via the private sicamRTU MIB** and for information via the **DG Product Inventory MIB** (see [5] SICAM A8000 Series, Manual CP-8050 Chapter 13.23.5.2&3).

The Trap function is running per default over port 162 and needs to be enabled (**Enable traps and Diagnostic traps**) for the SNMP Agent and of course also protected via **passwords for the Authentication and for the Privacy**.

Under **Trapserver configuration** up to two receivers for the traps can be entered (**IP-Address and used LAN**) of the SNMP (Figure 3.30). As soon as at least one Trapserver is configured a **new entrée directly under the SNMP node** appears where the **used Crypto Settings for the traps** must be entered and the **Traps for Diagnostic and/or DGPI** can be enabled

Note:

The necessary settings and action on SNMP Manager / iReasoning side for receiving traps will be covered in Chapter 5.

Nr	PSK authentication	PSK encryption	Authentication algorithm	Encryption algorithm
1			SHA1	AES128
2			SHA1	AES128
3			SHA1	AES128
4			SHA1	AES128
5			SHA1	AES128

Address	LAN interface	Ethernet port group	IPv4 address
192.168.3.101	SNMP	Singular CP-X2	192.168.3.9
192.168.2.101	T104_Se	RSTP CIO-X1, CIO-X2	192.168.2.9

Figure 3.30 SNMPv3 Trap configuration

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

Settings for SICAM Q100 & Q200 Power Quality Recorder:

The settings of the SICAM Power Quality recorder SICAM Q100 & Q200 using an internal Web browser with HTML pages from the connected computer. The IP-Address for SICAM Q100 & Q200 is 192.168.0.55 (for Q200 in case you select 2 independent interfaces the default IP-Address for the second interface is 192.168.1.55)

After connection to the SICAM Q100/200 PQ recorder via the integrated Webserver, you need to navigate to “**Configuration**” -> “**Basic configuration**” -> “**Communication**”.

Precondition: The SNMP protocol must be assigned to 1 Ethernet interface. To change the SNMPv3 settings in the Configuration tab, proceed as follows:

In the navigation window, **click SNMP protocol**.

- **Only 1 user** is possible, adding or removing of extra users is not possible
- With the default values (all are empty), access via SNMPv3 is not possible. The parameters must be set before accessing data via SNMP access
- The valid character range for username and passwords is limited to:
 - Numbers (0-9)
 - Latin characters (A-Z, a-z)
 - Basic special characters in the ASCII-character code range (33 to 126)
- Maximum length of a username is 32 characters.
- Maximum length of a SNMPv3 password is 24 characters.
- Passwords must be at least 8 characters long.
- **Authentication with MD5 algorithm**
- **Encryption with DES algorithm**
- SNMP must be enabled via parameterization.
- Only read access is allowed.
- RFC1213 MIB and the device-specific MIB (only for Q100 -> for Q200 the “Download device MIB file” button is not available, because only standard MIBs are used) are supported.
- Changes of SNMPv3 settings are only possible via Web browser, not via the device display
- **Click Send. The changed passwords are immediately valid.**

Parameter	
User name	
Authentication password	
Privacy password	

Figure 3.31 Configuration Tab, SNMPv3 Settings for SICAM Q100

4 DG common MIBs DGPI and DGSM

Out of special interest and nowadays required more and more information about assets (like installed hardware components and installed firmware versions) and security relevant information (like login attempts, start/stop of system components, modifications ...).

These can be provided via special SNMPv3 MIBs; for Siemens Smart Infrastructure Digital Grid Products two common MIBs has been released for this purpose:

- DG Product Inventory MIB = DGPI (digitalGridProductInventory.mib) => asset information
- DG Security Monitoring MIB = DGSM (digitalGridSecurityMonitoring.mib) => audit log via SNMP trap

The following DG EA products support the **DGPI** = DG Product Inventory MIB:

- **SIPROTEC 5**
 - Only the Ethernet communication module **ETH-BD-2FO** supports the DGPI MIB
 - Needed Firmware & Protocol version: V8.80 or higher
- **SIPROTEC 4 / SIPROTEC Compact**
 - EN100 E+/O+ with Firmware Version V4.35 or higher
 - IEC61850_SNMP_MIB_V01.07.01 or higher
- **Reyrolle 5**
 - Device FW: V2.30 or higher and fitting communication FW (planned for end of 2021)
- **SICAM A8000 RTUs**
 - CP-8000/21/22: CPC80 revision 15 or higher
 - CP-8031/50: CPC85 revision 02 or higher
 - SICAMRTUs_SNMP_MIB_V05.00.00 or higher
 - CP-8031/50 supports spontaneous / unsolicited information for DPGI = trap
- **SICAM PAS/PQS**
 - Version V8.13 or higher

The following DG EA products support the **DGSM** = DG Security Monitoring MIB:

- **SIPROTEC 5**
 - Only the Ethernet communication module **ETH-BD-2FO** supports the DGSM MIB
 - Needed Firmware & Protocol version: V8.80 or higher
- **SICAM PAS/PQS**
 - Version V8.16 or higher

For the security relevant information unsolicited / spontaneous notification is essential to have the important audit related information as soon as possible (spontaneously) available. => **DGSM Security Monitoring MIB**

Therefore, SNMP defines for such kind of information the **SNMP traps** (see chapter 1.2.5) using as default UDP port 162 for sending spontaneously the information from the SNMP Agent to the SNMP Manager.

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

4.1 Preparation for the DGPI and DGSM MIBs

As necessary preparation, the needed MIBs must be loaded and additional work on the SNMP Manager (iReasoning in this APN) and on the SNMP Agent must be done for enabling the trap functionality and allow to receive notification (spontaneous) information.

4.1.1 Loading the needed standard and DG common MIBs

Before enabling the SNMP Manager to receive trap information from a SNMP Agent it is necessary to load / Import the necessary Standard and DG Common MIBS like described in Chapter 3.3.1 Step1.

The following Siemens common MIBs needs to be loaded / Imported (see chapter 5 for download links)

1. SIEMENS-SMI.mib
2. DGPI MIB (Siemens Smart Infrastructure Digital Grid Product Inventory MIB)
3. DGSM MIB (Siemens Smart Infrastructure Digital Grid Security Monitoring MIB)

The following Standard MIB needs to be loaded / Imported:

(e.g., download Standard MIBs from: <http://www.snmpLink.org/OnLineMIB/Standards/>)

4. Target & Notification MIB (RFC 3413, formerly 2573) and Transport Mappings SNMPv2 (RFC 3417)

After successful loading / importing of above mention MIBs you can see them in the MIB Tree of iReasoning (Figure 4.1).

The Siemens Common MIBs under:

.. **private** -> **enterprises** -> **siemens** (SIEMENS-SMI.mib creates the node) -> **siemensCommon**.

The Standard Target & Notification MIB under:

..**snmpV2** -> **snmpModules**

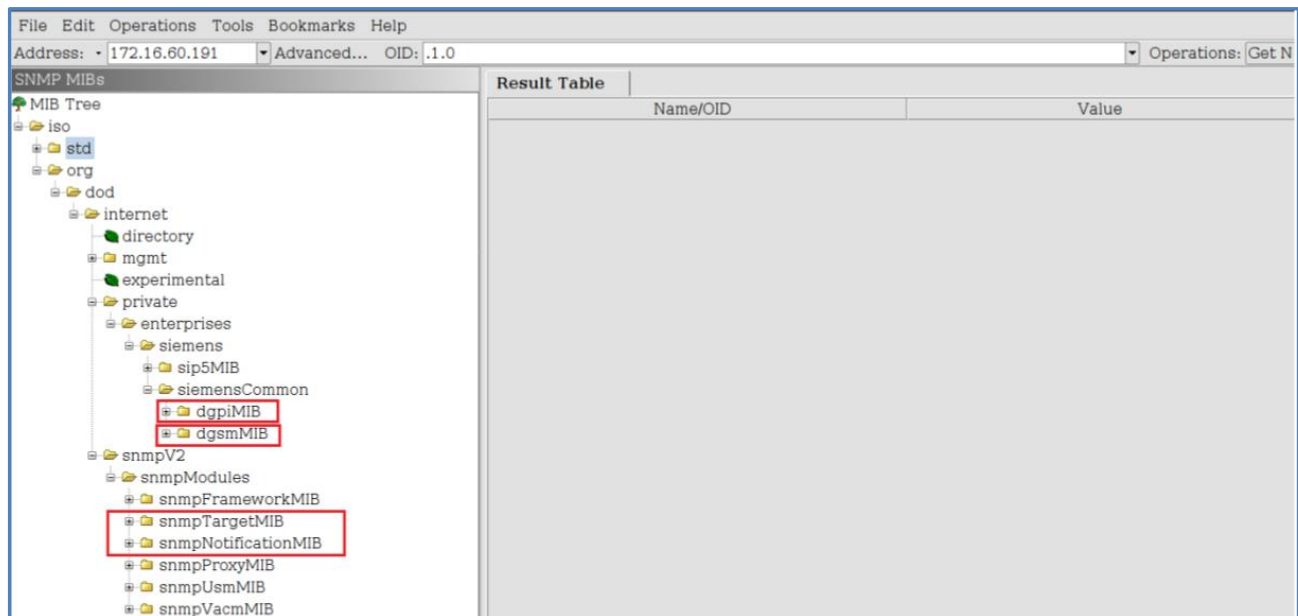


Figure 4.1 MIB Tree with needed MIBs for DGPI and DGSM MIBs and for traps preparation

4.1.2 Receiving security monitoring notifications -> Target-MIB

For receiving traps from the SNMP Agent, you need to configure this functionality on the SNMP Manager side (iReasoning MIB-Browser in this APN). First an online connection must be established between SNMP Agent and SNMP Manager (see chapter 3.3.1): you need to **put the IP-Address** (1) of your SNMP Agent device in the Address fields and press the **"Advanced..."** (2) button.

Best would be if you use for the connection an already created new user (and deleted the default initial users), but of course it is also possible using a default / initial user for testing everything first before deleting the default / initial users.

Figure 4.2 is showing the steps to establish the online connection with a default user (templateMD5) with the credentials (3) as shown in Chapter 3.3.1 Step2)

User	Authentication Algorithm	Authentication Password	Encryption/Privacy Algorithm	Privacy Password	Access Rights
templateMD5	MD5	12345678	DES	12345678	Read, Write
templateSHA	SHA	12345678	AES	12345678	Read, Write

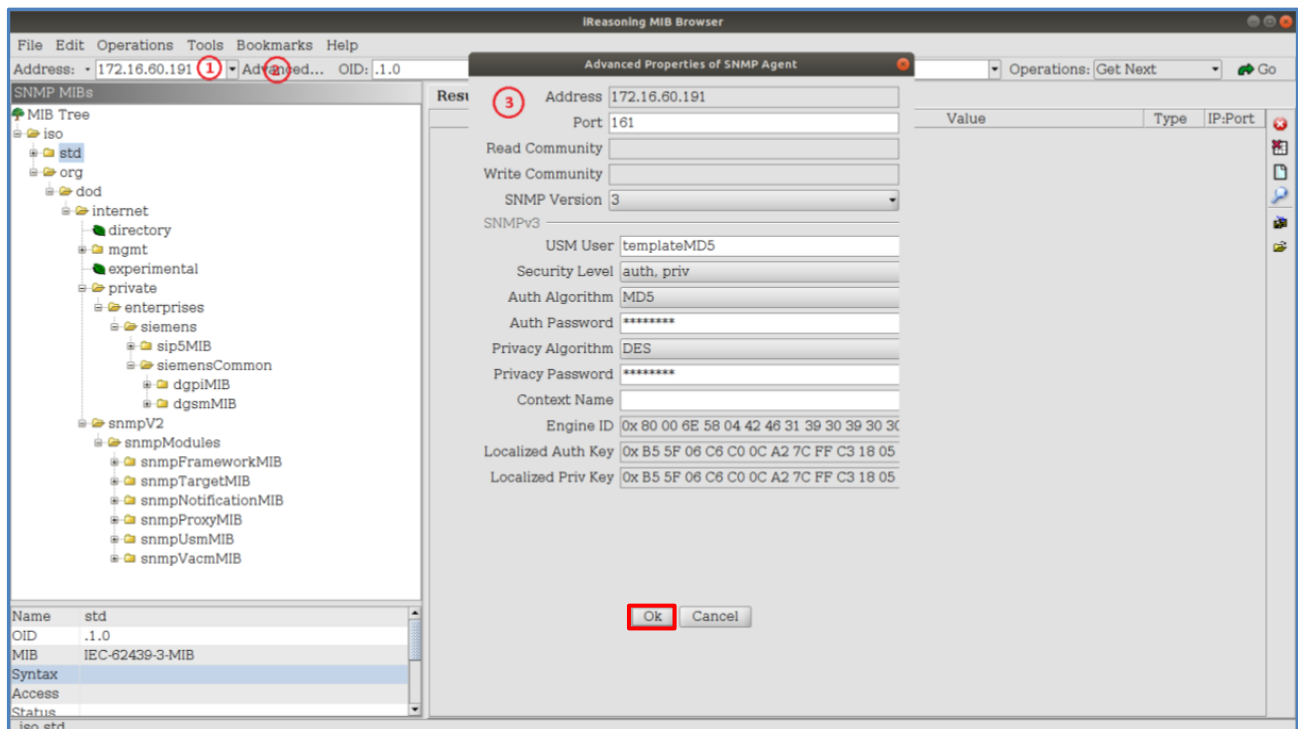


Figure 4.2 Connecting to the SNMP Agent device with user and credentials

The next step after the connection has been successfully established is, to configure the Address table and the Parameter table in the node **snmpTargetMIB** -> **snmpTargetObjects** -> **snmpTargetAddrTable**. There is no default setting related to notifications, you need to create your own row for each table and set the parameter for the tables.

Step1: Creating a new row for the Address Table (Figure 4.3)

1. Select in the node **snmpTargetMIB** -> **snmpTargetObjects** -> **snmpTargetAddrTable**
2. In the main working area press **"Create Row"**
3. Enter in the new Pop-up Windows the values shown in below table (RFC 3417 required to "translate" the AddrTDomain)

Name	Value
snmpTargetAddrName	TrapTarget
snmpTargetAddrTDomain	.1.3.6.1.6.1.1
snmpTargetAddrTAddress	0xAC103CB400A2 (IP-Address of the trap receiver -SNMP Manager-)
snmpTargetAddrTagList	NotifyTag
snmpTargetAddrParams	TargetParam

The Address must be entered in HEX, see the example below how to convert the IP-Address of the SNMP Manager

snmpTargetAddrTAddress: 0xAC 10 3C B4 00A2
 IP ↓ ↓ ↓ ↓ ↓ Port
 172. 16 .60. 180 : 162

4. When finished, press the **Ok** button

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

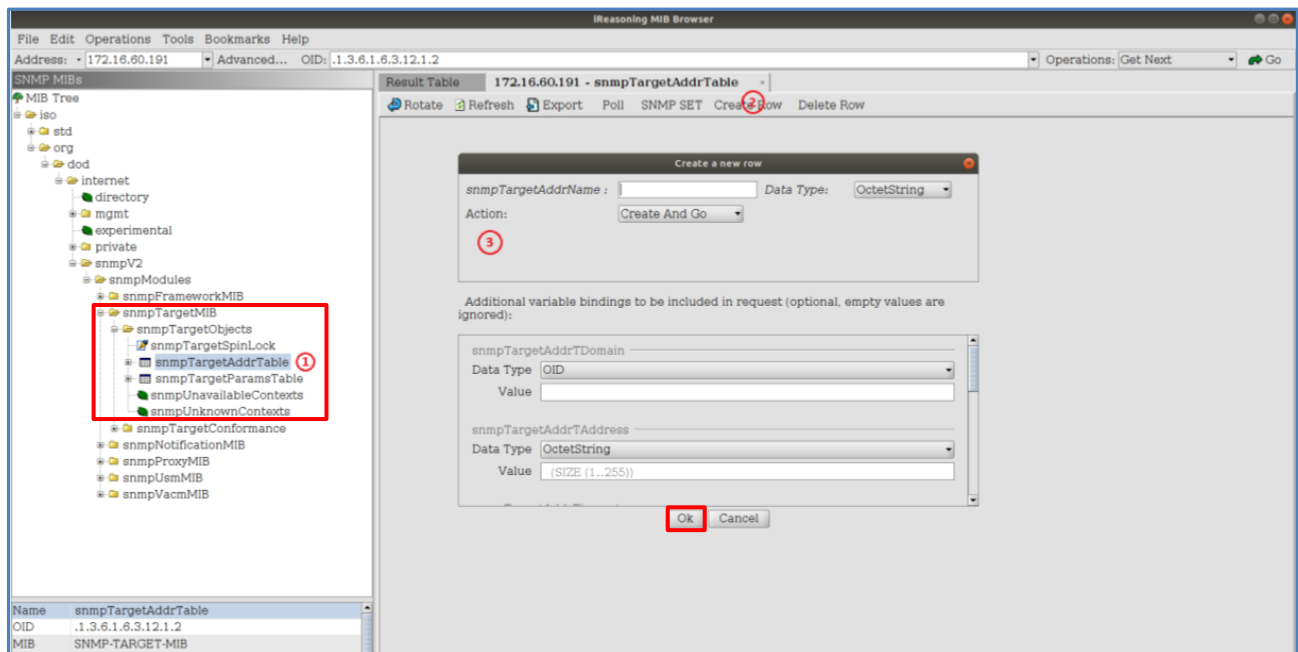


Figure 4.3 Creating a new row for trap receiving in the address table

Step2: Creating a new row for the Parameter Table (Figure 4.4)

1. Select in the node **snmpTargetMIB** -> **snmpTargetObjects** -> **snmpTargetParamsTable**
2. In the main working area press "Create Row"
3. Enter in the new Pop-up Windows the values shown in below table (...SecurityName must fit to your used username)

Name	Value
snmpTargetParamsName	TargetParam
snmpTargetParamsMPModel	3
snmpTargetParamsSecurityModel	3
snmpTargetParamsSecurityName	templateMD5 (is only an example, must fit to real user)
snmpTargetParamsSecurityLevel	3

4. When finished, press the **Ok** button

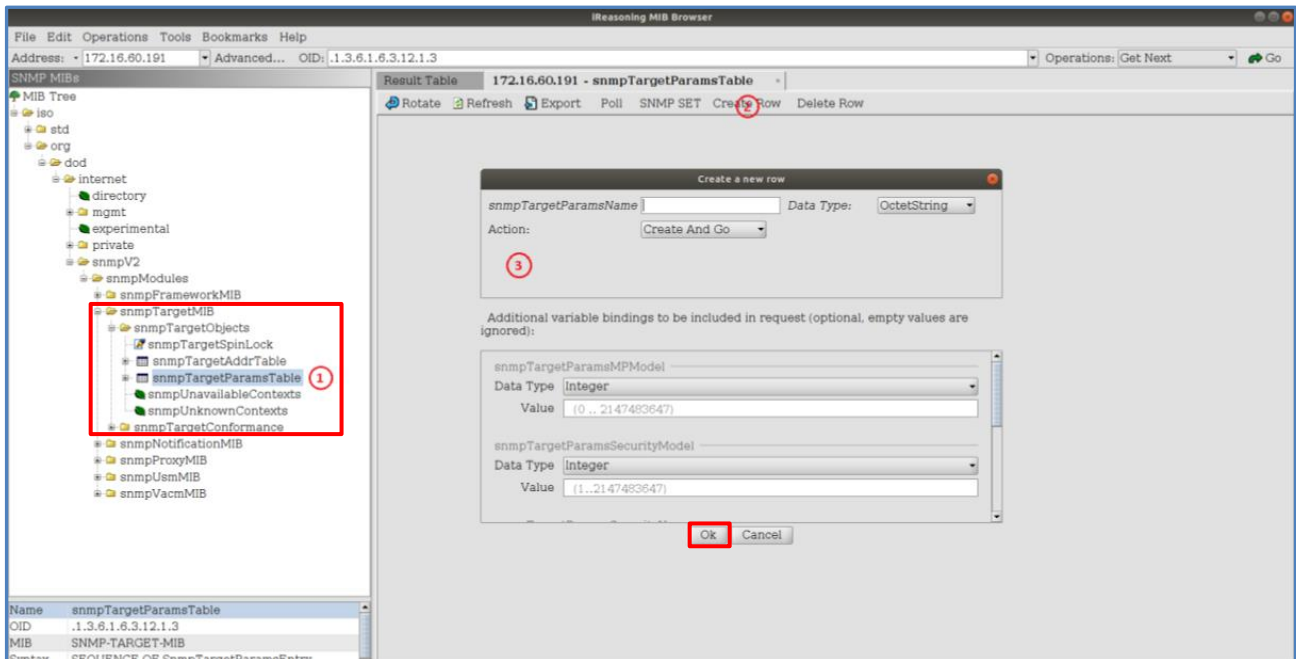


Figure 4.4 Creating a new row for trap receiving in the Parameter table

4.1.3 Receiving security monitoring notifications -> Notification-MIB

The SNMP Manager (here iReasoning MIB-Browser) must be enabled to receive trap information sent from a SNMP Agent; that must be done via settings in the snmpNotificationMIB.

Step3: Creating a new row for the Parameter Table (Figure 4.5)

1. Select in the node **snmpNotificationMIB** -> **snmpNotifyObjects** -> **snmpNotifyTable**
2. In the main working area press **"Create Row"**
3. Enter in the new Pop-up Windows the values shown in below table

Name	Value
snmpNotifyName	Trap
snmpNotifyTag	NotifyTag
snmpNotifyType	1

4. When finished, press the **Ok button**

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

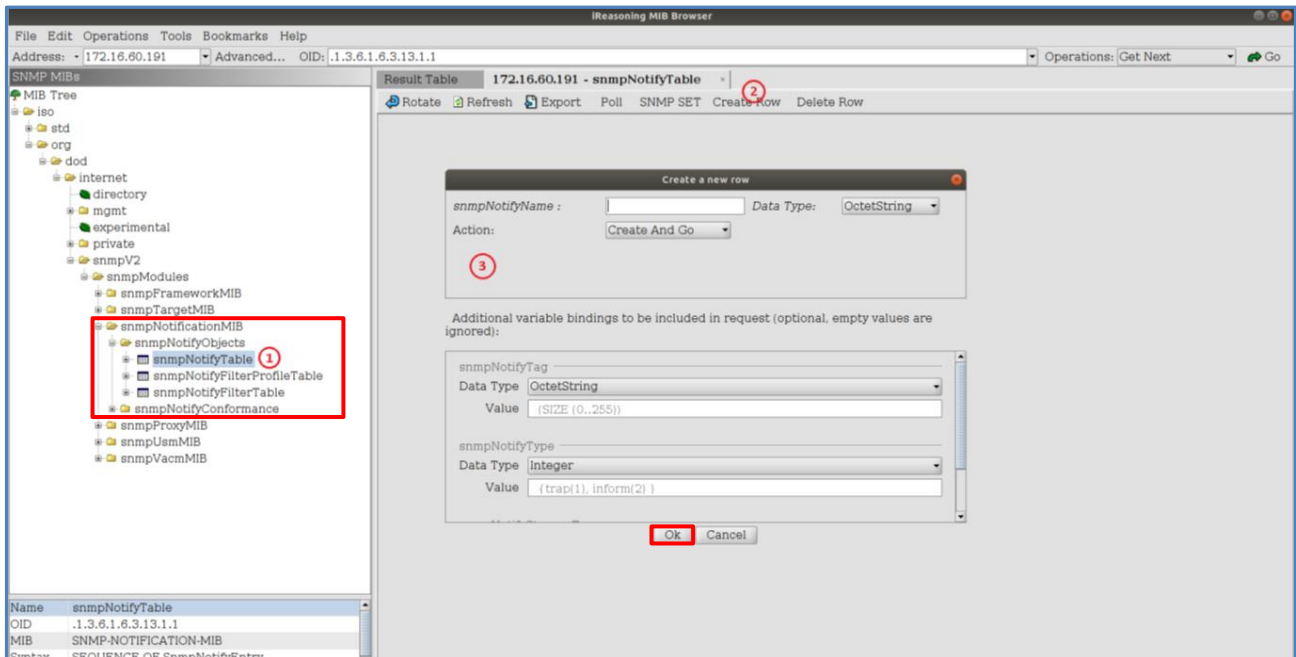


Figure 4.5 Creating a new row for trap receiving in the Notify table

4.1.4 Enabling SNMP traps on SNMP Agent side

The feature of the SNMP Agent to send traps must be enabled. In the CP-8050/31 that is done in the engineering tool, but for other products the default setting is set to "no". To check or change the setting you need to have an online access to the SNMP Agent.

- Select under siemens -> siemensCommon -> dgsmMIB -> **dgsmNotificationEnabled** (for CP-8050 also dgpi possible)
- Open the context menu with right mouse click and select "Set" (1)
- Fill in as Value "2" (enabled or yes; "1" means disabled or no) (2)
- Confirm with the **Ok button**

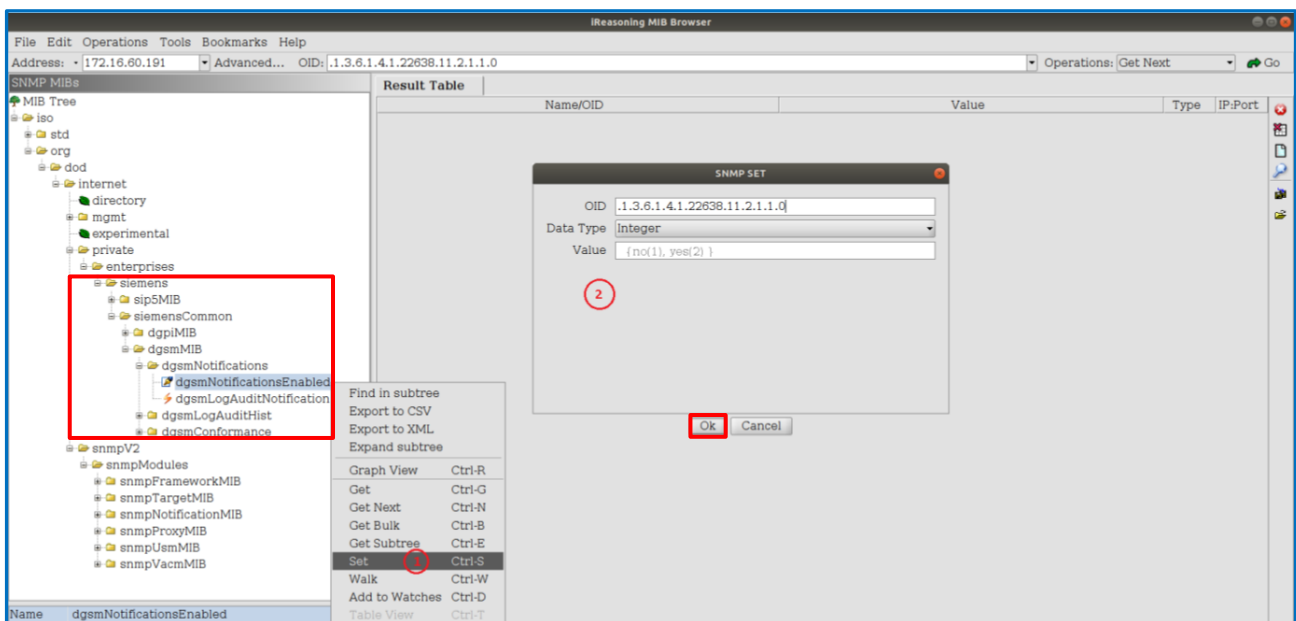
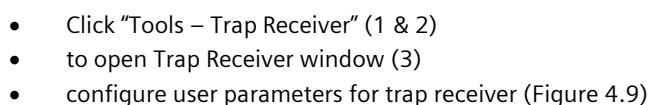


Figure 4.6 Enabling / checking trap sending on SNMP agent

Decrypting SNMPv3 PDUs in Wireshark chapter to see how it is achieved.



SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

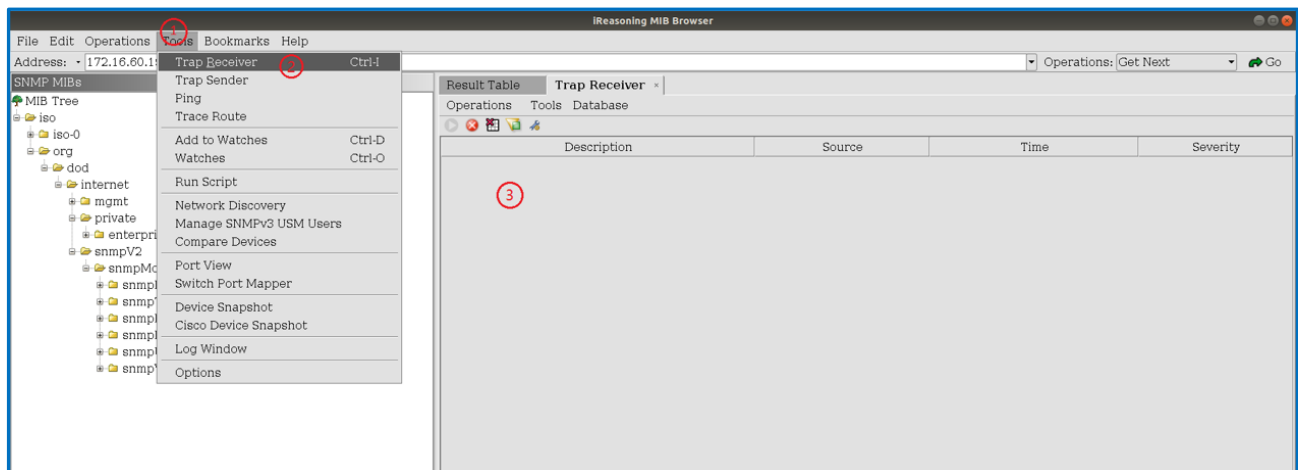


Figure 4.8 Preparing Trap Receiver

To configure the Trap Receiver in iReasoning the following steps needs to be done:

- Select the context menu for Trap Receiver with **Tools** (1)
- Select **Options** (2)
- Use the **Add** button for adding a Trap Receiver (3)
- Enter in the new pop-up Window a **valid user with his credentials** (4)
- Confirm the setting with the **Ok** button (5)

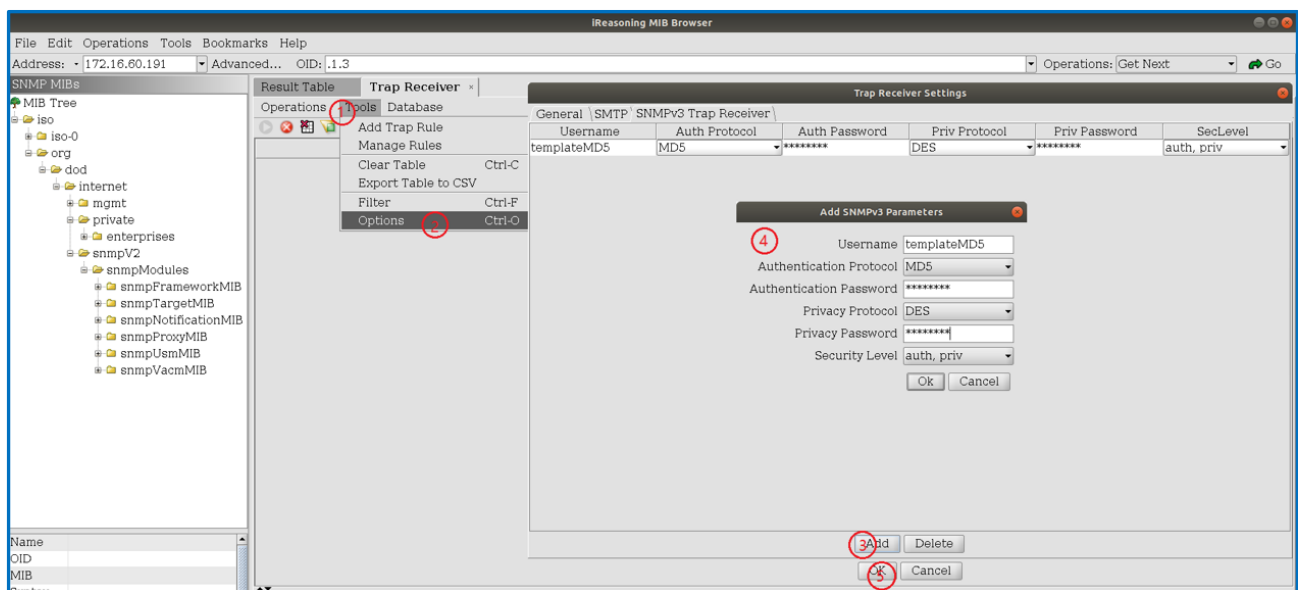


Figure 4.9 Configuring Trap Receiver

Now trigger a security relevant event for example via the local HMI of a SIPROTEC 5 relay when opening the “security log” in navigating: Main Menu -> Test&Diagnosis -> Logs -> Securitylog

And check if this event is visible (Figure 4.10)

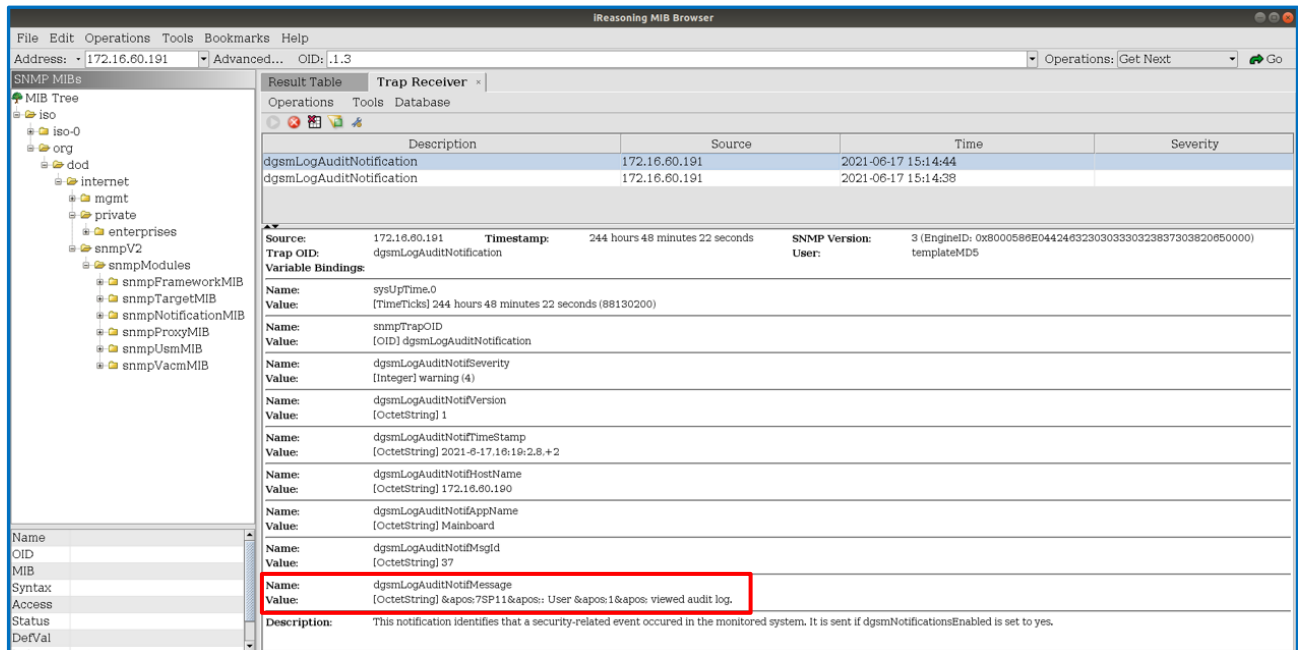


Figure 4.10 Checking Trap Reception

4.1.6 Deleting SNMP settings

In case you want to delete the rows created above (chapter 4.1.2 / 4.1.3), set the value to '6' as shown in Figure 4.11.

- Select in the (snmpTargetAddrTable / snmpTargetParamsTable) the row / line you want to delete (1)
- Use the **SNMP SET** menu option (2)
- Enter in the new pop-up Menu as **Value "6"** (3)
- Confirm with the **Ok** button

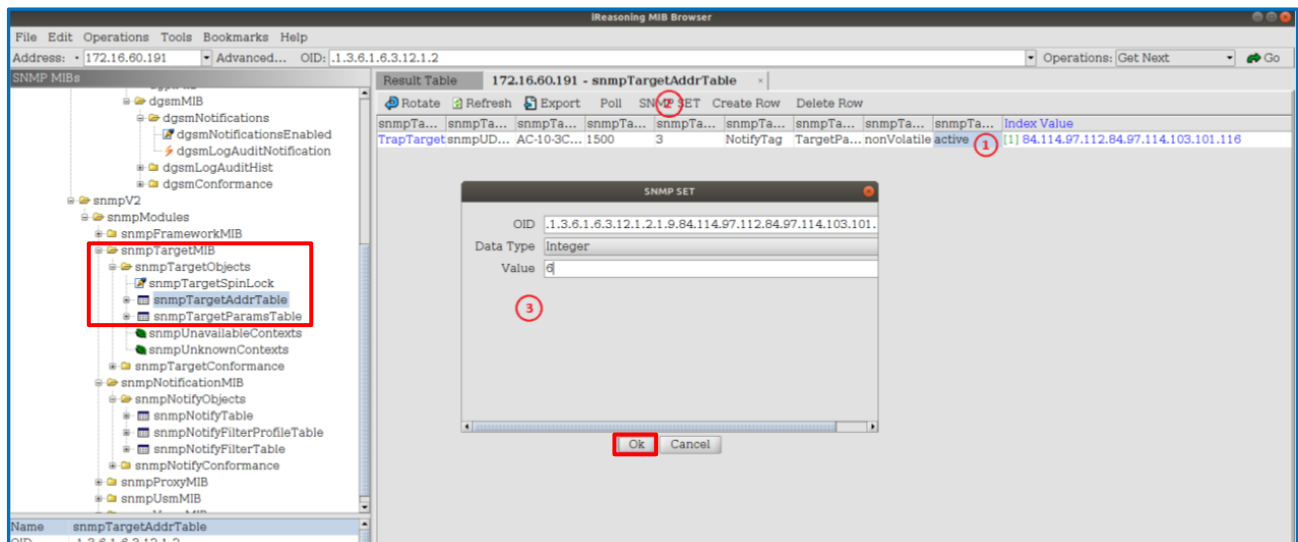


Figure 4.11 Deleting the created rows

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

4.1.7 Decrypting SNMPv3 PDUs in Wireshark

- Open the captured packets using the Wireshark application
- Go to Edit > Preferences > Protocols
- Select SNMP from the protocol list
- Edit the user table settings:

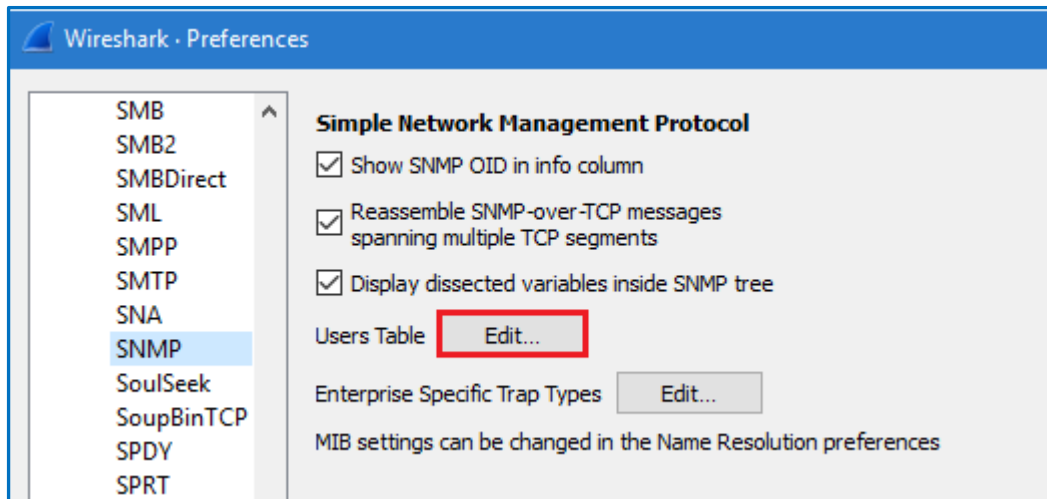


Figure 4.12 Wireshark SNMP Protocol Settings

- Click on Add button and put the following details:
 - Engine ID
 - SNMPv3 username
 - Choose the authentication model (MD5 | SHA1)
 - Put the password for authentication model
 - Choose the privacy protocol (DES | AES | AES192 | AES256)
 - Put the privacy password

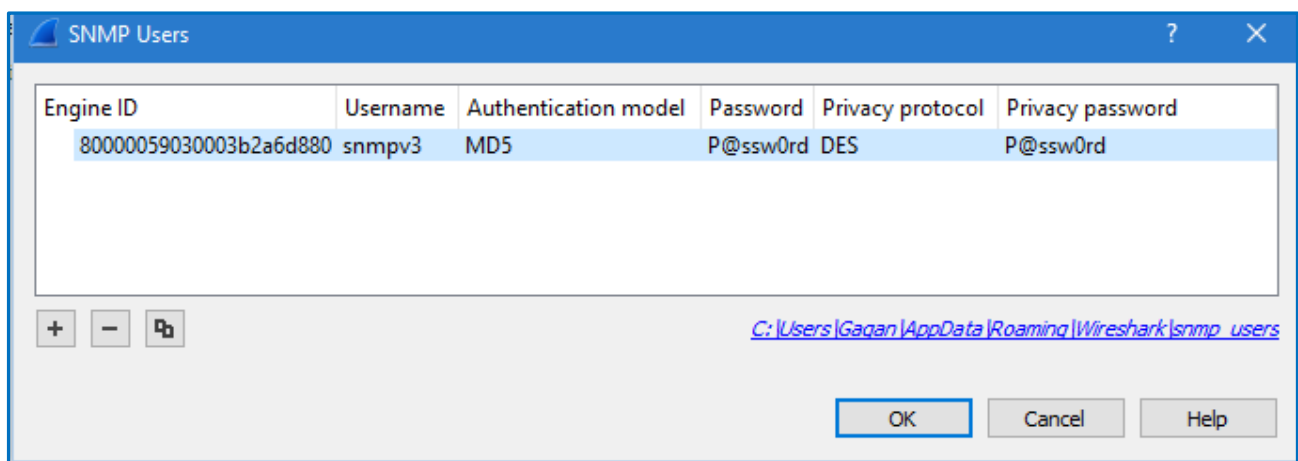


Figure 4-13 Wireshark SNMPv3 Users

4.2 Reading DGPI and DGSM information

After the preparation described in chapter 4.1 has been done, you can now use the SNMP Manager to access the information provided via the DGPI MIB.

4.2.1 Getting values of the DGPI product inventory MIB

Expand the MIB tree and find **"dgpiProductComponentsTable"** (Figure 4.12) and open with right click the Menu content. You can use all Get or Walk commands, but the best overview of the asset information will be presented when selecting **"Table View"** (see Figure 4.13 & 4.14).

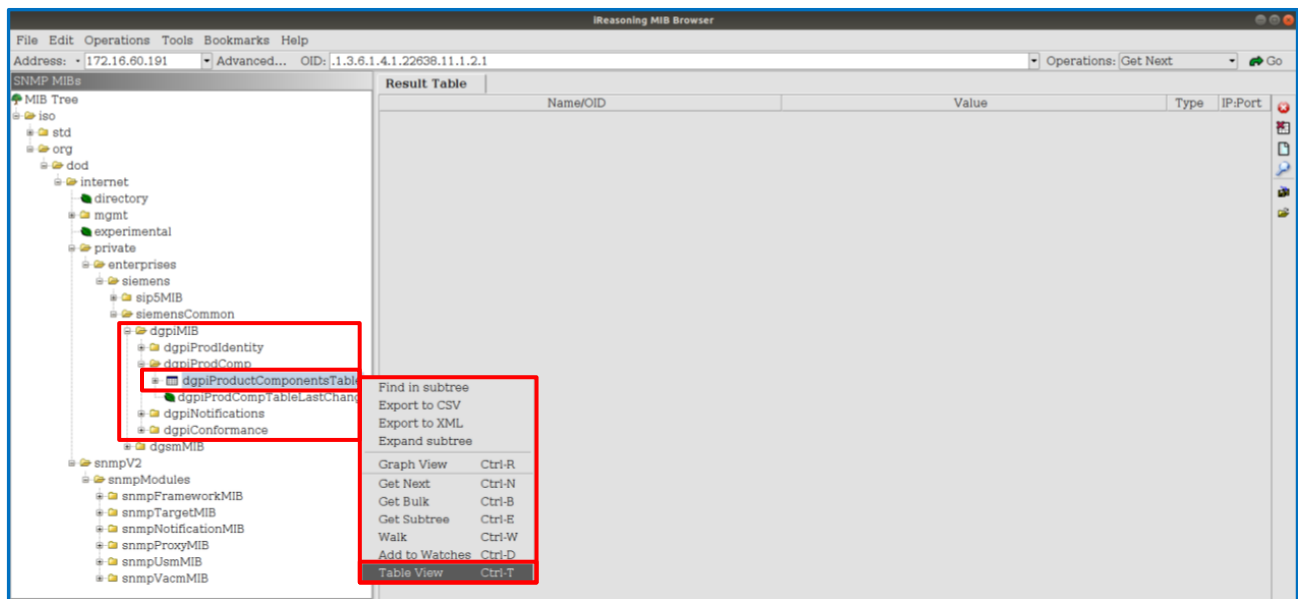
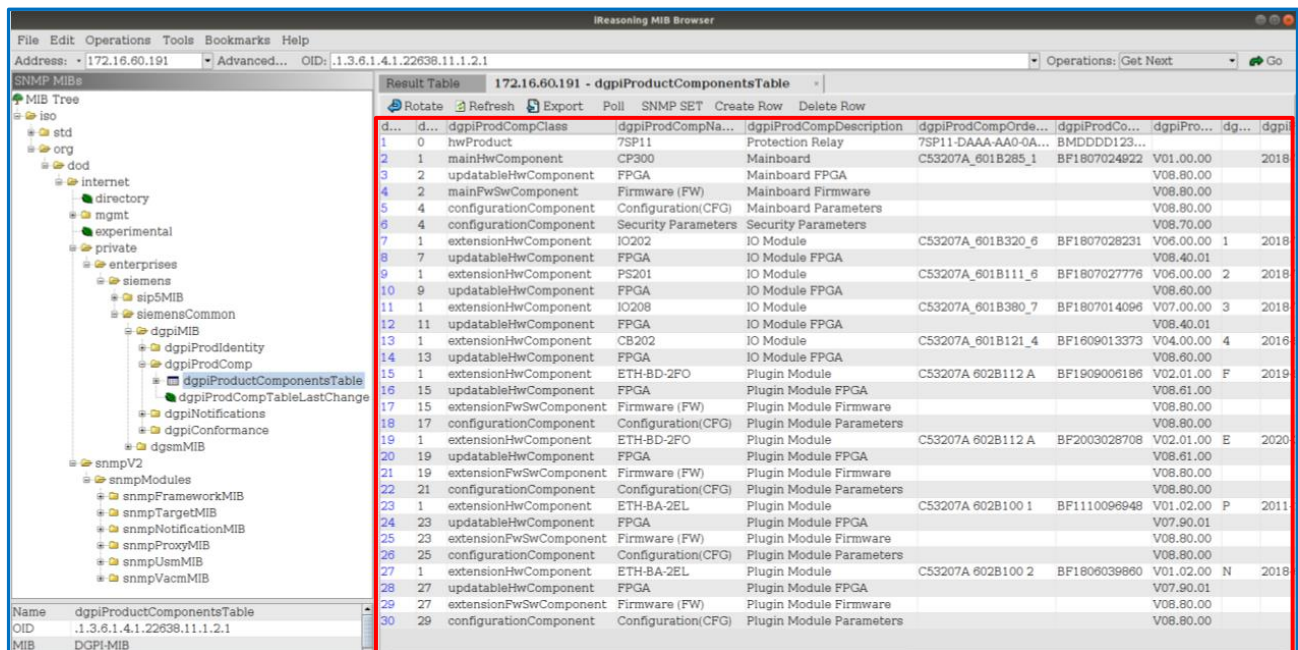


Figure 4.14 Opening the Table View for the DGPI asset information

After this selection the DGPI Product Component Table is opened in the main window, showing the asset information. Each entry in this table represents single component in device which can be various types defined in the **"dgpiProdCompClass"** column. The components have hierarchical relation linked in **"dgpiProdCompContainedIn"** and **"dgpiProdCompContainedIn"** columns. The component id in the **"dgpiProdCompContainedIn"** represents the parent component's index id. I.e: Component Id=5: "Configuration(CFG)" is a subcomponent of id=4 "Mainboard Firmware" and that's the subcomponent of id=2 "CP300" Hardware and that's the subcomponent of id=0 root component 7SP11 device for below figure.

SIPROTEC 5 Application

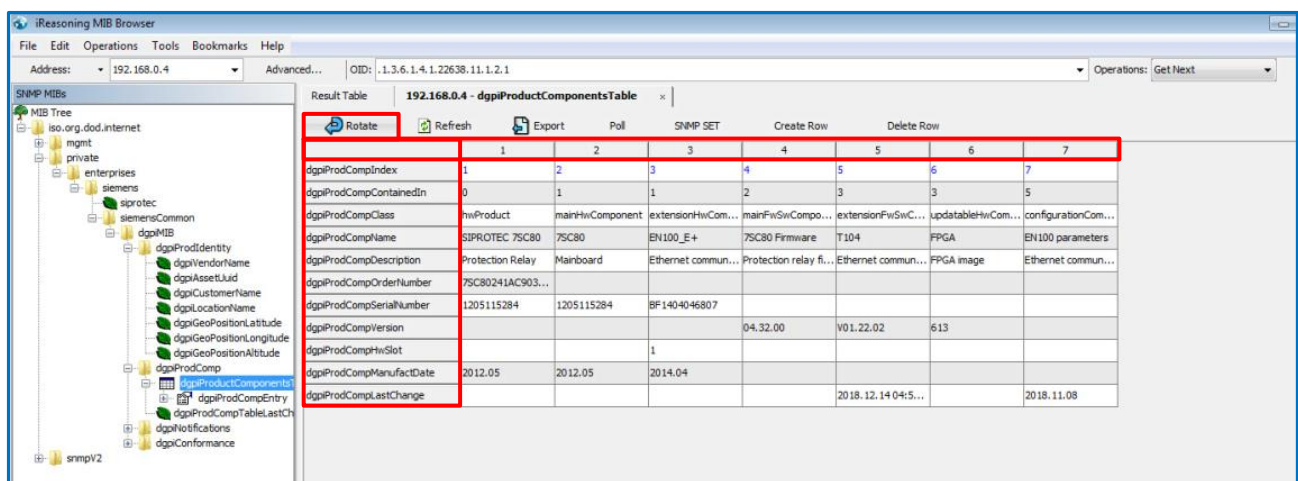
Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP



d...	d...	dgpiProdCompClass	dgpiProdCompNa...	dgpiProdCompDescription	dgpiProdCompOrds...	dgpiProdCo...	dgpiPro...	dg...	dgpi...
1	0	hwProduct	7SP11	Protection Relay	7SP11-DAAA-AA0-0A...	BMDDDD123...			
2	1	mainHwComponent	CP300	Mainboard	C53207A_601B285_1	BF1807024922	V01.00.00		2018
3	2	updateableHwComponent	FPGA	Mainboard FPGA			V08.80.00		
4	2	mainFwSwComponent	Firmware (FW)	Mainboard Firmware			V08.80.00		
5	4	configurationComponent	Configuration(CFG)	Mainboard Parameters			V08.80.00		
6	4	configurationComponent	Security Parameters	Security Parameters			V08.70.00		
7	1	extensionHwComponent	IO202	IO Module	C53207A_601B320_6	BF1807028231	V08.00.00	1	2018
8	7	updateableHwComponent	FPGA	IO Module FPGA			V08.40.01		
9	1	extensionHwComponent	PS201	IO Module	C53207A_601B111_6	BF1807027778	V08.00.00	2	2018
10	9	updateableHwComponent	FPGA	IO Module FPGA			V08.80.00		
11	1	extensionHwComponent	IO208	IO Module	C53207A_601B380_7	BF1807014066	V07.00.00	3	2018
12	11	updateableHwComponent	FPGA	IO Module FPGA			V08.40.01		
13	1	extensionHwComponent	CB202	IO Module	C53207A_601B121_4	BF1809013373	V04.00.00	4	2018
14	13	updateableHwComponent	FPGA	IO Module FPGA			V08.60.00		
15	1	extensionHwComponent	ETH-BD-2FO	Plugin Module	C53207A_602B112_A	BF1809006186	V02.01.00	F	2019
16	15	updateableHwComponent	FPGA	Plugin Module FPGA			V08.61.00		
17	15	extensionFwSwComponent	Firmware (FW)	Plugin Module Firmware			V08.80.00		
18	17	configurationComponent	Configuration(CFG)	Plugin Module Parameters			V08.80.00		
19	1	extensionHwComponent	ETH-BD-2FO	Plugin Module	C53207A_602B112_A	BF2003028708	V02.01.00	E	2020
20	19	updateableHwComponent	FPGA	Plugin Module FPGA			V08.80.00		
21	19	extensionFwSwComponent	Firmware (FW)	Plugin Module Firmware			V08.80.00		
22	21	configurationComponent	Configuration(CFG)	Plugin Module Parameters			V08.80.00		
23	1	extensionHwComponent	ETH-BA-2EL	Plugin Module	C53207A_602B100_1	BF1110096948	V01.02.00	P	2011
24	23	updateableHwComponent	FPGA	Plugin Module FPGA			V07.90.01		
25	23	extensionFwSwComponent	Firmware (FW)	Plugin Module Firmware			V08.80.00		
26	25	configurationComponent	Configuration(CFG)	Plugin Module Parameters			V08.80.00		
27	1	extensionHwComponent	ETH-BA-2EL	Plugin Module	C53207A_602B100_2	BF1806039660	V01.02.00	N	2018
28	27	updateableHwComponent	FPGA	Plugin Module FPGA			V07.90.01		
29	27	extensionFwSwComponent	Firmware (FW)	Plugin Module Firmware			V08.80.00		
30	29	configurationComponent	Configuration(CFG)	Plugin Module Parameters			V08.80.00		

Figure 4.15 Table with the asset information

You can change the representation via the "Rotate" button; the columns and lines will be changed (the content of the columns is now shown in the lines and vice-versa) what gives you a better overview (Figure 4.14 -attention is from another device-)



	1	2	3	4	5	6	7
dgpiProdCompIndex	1	2	3	4	5	6	7
dgpiProdCompContainedIn	0	1	1	2	3	3	5
dgpiProdCompClass	hwProduct	mainHwComponent	extensionHwCom...	mainFwSwCompo...	extensionFwSwC...	updateableHwCom...	configurationCom...
dgpiProdCompName	SIPROTEC 7SC80	7SC80	EN100_E+	7SC80 Firmware	T104	FPGA	EN100 parameters
dgpiProdCompDescription	Protection Relay	Mainboard	Ethernet commun...	Protection relay f...	Ethernet commun...	FPGA image	Ethernet commun...
dgpiProdCompOrderNumber	7SC80241AC903...						
dgpiProdCompSerialNumber	1205115284	1205115284	BF1404046807				
dgpiProdCompVersion				04.32.00	V01.22.02	613	
dgpiProdCompHwSlot			1				
dgpiProdCompManufactDate	2012.05	2012.05	2014.04				
dgpiProdCompLastChange					2018.12.14 04:5...		2018.11.08

Figure 4.16 Table with the asset information -rotated view-

4.2.2 Getting values of the DGSM Security Monitoring MIB

Expand the MIB tree and find “**dgsmLogAuditHistTable**” (Figure 4.15) and open with right click the Menu content. You can use all Get or Walk commands, but the best overview of the Security information will be presented when selecting “**Table View**” (see Figure 4.16). The **Audit Log History Table** stores up to the last 50 via trap send security related information.

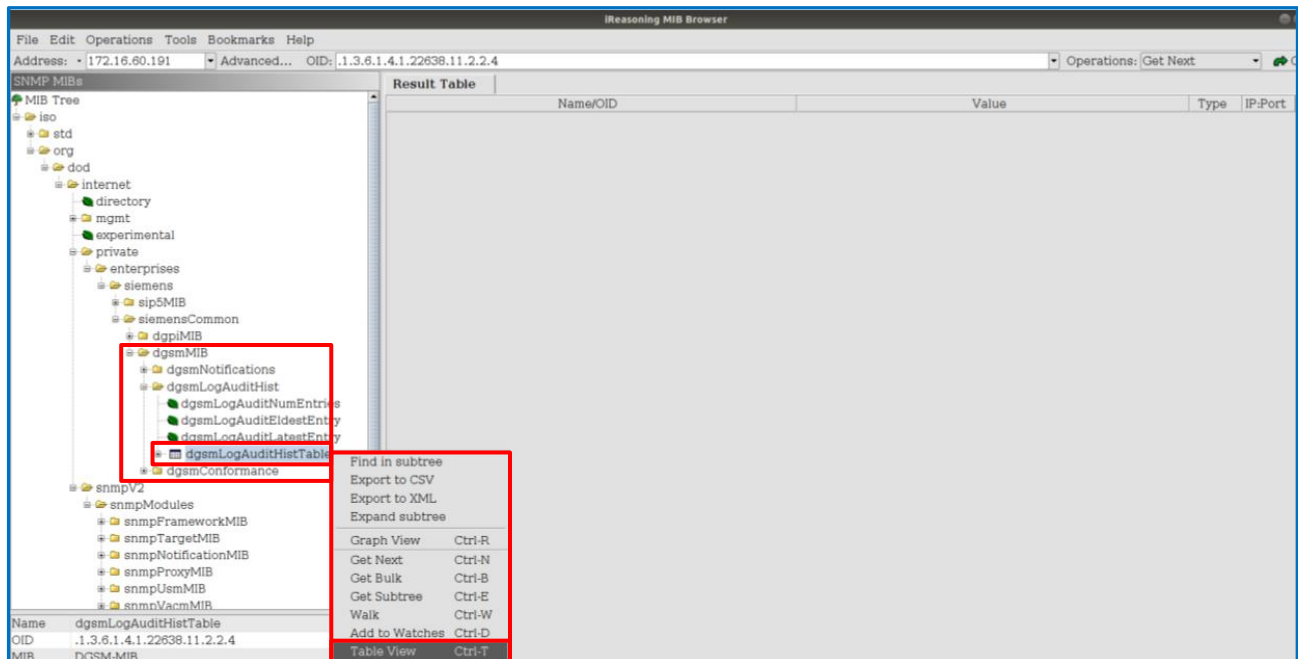


Figure 4.17 Opening the Table View for the DGSM security monitoring information

After this selection the DGPI Product Component Table is opened in the main window, showing the asset information. You can change the representation via the “Rotate” button; the columns and lines will be changed (the content of the columns is now shown in the lines and vice-versa). For Security Monitoring events the rotation view is not so helpful. It is better to see the sequence of security events via the “standard” view.

Index	Value	Index Value
1	warning 1 2021-6-16-14:42:30.0+2:0 172.16.60.190 Mainboard 9 7SP11_OnlineReset: A user has ended an interact...	[1] 1
2	warning 1 2021-6-16-14:42:32.5+2:0 172.16.60.190 Mainboard 4 7SP11_OnlineReset: A user has initiated a remote...	[2] 2
3	warning 1 2021-6-16-14:42:32.6+2:0 172.16.60.190 Mainboard 27 7SP11_OnlineReset: Configuration settings were ...	[3] 3
4	warning 1 2021-6-16-14:42:37.9+2:0 172.16.60.190 Mainboard 27 7SP11_OnlineReset: Configuration settings were ...	[4] 4
5	warning 1 2021-6-16-14:43:3.6+2:0 172.16.60.190 Mainboard 38 7SP11_OnlineReset: Audit log was downloaded fr...	[5] 5
6	warning 1 2021-6-16-15:1:32.0+2:0 172.16.60.190 Mainboard 27 7SP11_OnlineReset: Configuration settings were ...	[6] 6
7	warning 1 2021-6-16-15:1:38.4+2:0 172.16.60.190 Mainboard 27 7SP11_OnlineReset: Configuration settings were ...	[7] 7
8	warning 1 2021-6-16-15:1:41.3+2:0 172.16.60.190 Mainboard 38 7SP11_OnlineReset: Audit log was downloaded fr...	[8] 8
9	warning 1 2021-6-16-16:0:4.8+2:0 172.16.60.190 Mainboard 27 7SP11_OnlineReset: Configuration settings were ...	[9] 9
10	warning 1 2021-6-16-16:0:10.2+2:0 172.16.60.190 Mainboard 27 7SP11_OnlineReset: Configuration settings were ...	[10] 10
11	warning 1 2021-6-16-16:0:13.4+2:0 172.16.60.190 Mainboard 38 7SP11_OnlineReset: Audit log was downloaded fr...	[11] 11
12	warning 1 2021-6-16-16:13:1.3+2:0 172.16.60.190 Mainboard 27 7SP11_OnlineReset: Configuration settings were ...	[12] 12
13	warning 1 2021-6-16-16:13:6.7+2:0 172.16.60.190 Mainboard 27 7SP11_OnlineReset: Configuration settings were ...	[13] 13
14	warning 1 2021-6-16-16:13:9.1+2:0 172.16.60.190 Mainboard 38 7SP11_OnlineReset: Audit log was downloaded fr...	[14] 14
15	alert 1 2021-6-16-16:15:1.4+2:0 172.16.60.190 Mainboard 65 7SP11_OnlineReset: Attempted use of illegitimate...	[15] 15
16	warning 1 2021-6-16-16:15:11.9+2:0 172.16.60.190 Mainboard 9 7SP11_OnlineReset: A user has ended an interact...	[16] 16
17	alert 1 2021-6-16-16:15:25.2+2:0 172.16.60.190 Mainboard 65 7SP11_OnlineReset: Attempted use of illegitimate...	[17] 17
18	alert 1 2021-6-16-16:24:49.7+2:0 172.16.60.190 Mainboard 65 7SP11_OnlineReset: Attempted use of illegitimate...	[18] 18
19	alert 1 2021-6-16-16:25:3.2+2:0 172.16.60.190 Mainboard 65 7SP11_OnlineReset: Attempted use of illegitimate...	[19] 19
20	alert 1 2021-6-16-16:25:18.2+2:0 172.16.60.190 Mainboard 65 7SP11_OnlineReset: Attempted use of illegitimate...	[20] 20
21	warning 1 2021-6-16-16:27:12.5+2:0 172.16.60.190 Mainboard 4 7SP11_OnlineReset: A user has initiated a remote...	[21] 21
22	alert 1 2021-6-16-16:27:21.3+2:0 172.16.60.190 Mainboard 63 7SP11_OnlineReset: Restart initiated from '192.1...	[22] 22
23	warning 1 2021-6-16-16:27:21.7+2:0 172.16.60.190 Mainboard 4 7SP11_OnlineReset: A user has initiated a remote...	[23] 23
24	warning 1 2021-6-16-16:27:48.9+2:0 172.16.60.190 Mainboard 35 7SP11_OnlineReset: Firmware version 'V08.80' w...	[24] 24
25	alert 1 2021-6-16-16:28:19.3+2:0 172.16.60.190 Mainboard 63 7SP11_OnlineReset: Restart initiated from '192.1...	[25] 25
26	warning 1 2021-6-16-16:33:38.4+2:0 172.16.60.190 Mainboard 4 7SP11_OnlineReset: A user has initiated a remote...	[26] 26
27	warning 1 2021-6-16-16:33:50.9+2:0 172.16.60.190 Mainboard 9 7SP11_OnlineReset: A user has ended an interact...	[27] 27
28	warning 1 2021-6-16-16:34:19.5+2:0 172.16.60.190 Mainboard 4 7SP11_OnlineReset: A user has initiated a remote...	[28] 28
29	alert 1 2021-6-16-16:34:25.0+2:0 172.16.60.190 Mainboard 63 7SP11_OnlineReset: Restart initiated from '172.1...	[29] 29
30	warning 1 2021-6-16-16:35:28.8+2:0 172.16.60.190 Mainboard 29 7SP11_OnlineReset: Configuration settings were ...	[30] 30
31	alert 1 2021-6-16-16:35:30.3+2:0 172.16.60.190 Mainboard 63 7SP11_OnlineReset: Restart initiated from '172.1...	[31] 31

Figure 4.18 Table with the security monitoring information

SIPROTEC 5 Application

Handling of secure SNMP (SNMPv3), asset monitoring and security monitoring via SNMP

5 Link collection to further documents

[1] SIPROTEC 5 Communication Protocols - Manual

<https://support.industry.siemens.com/cs/document/109742443/siprotec-5-communication-protocols-manual?dti=0&pnid=24237&lc=en-WW>

[2] SIPROTEC 4/SIPROTEC Compact/Reyrolle IEDs Ethernet Module EN100 for IEC 61850 - Manual

<https://support.industry.siemens.com/cs/document/109744540/siprotec-4-siprotec-compact-reyrolle-ieds-ethernet-module-en100-for-iec-61850-with-electrical-optical-100-mbit-interface?dti=0&pnid=24238&lc=en-WW>

[3] Reyrolle 7SR5 Communication Protocol - Manual

https://wse06.siemens.com/content/P0009270/Documents/7SR5%20Communication%20Protocol%20Manual,%20,%20en_US.pdf

[4] SICAM PAS / PQS - Configuration and Operation - Manual

<https://support.industry.siemens.com/cs/document/109758084/sicam-pas-pqs-configuration-and-operation?dti=0&pnid=24615&lc=en-WW>

[5] SICAM A8000 Series, Manual CP-8050

<https://support.industry.siemens.com/cs/document/109757272/sicam-a8000-series-manual-cp-8050?dti=0&pnid=24618&lc=en-WW>

[6] SICAM A8000 Series CP-8000, CP-8021, CP-8022 - Manual

<https://support.industry.siemens.com/cs/document/109757713/hb-sicam-a8000-series-cp-8000-cp-8021-cp-8022?dti=0&pnid=24618&lc=en-WW>

[7] SICAM Q100 - 7KG95xx - Power Monitoring Device and Class A Power Quality Recorder - Device Manual

<https://support.industry.siemens.com/cs/document/109744874/sicam-q100-7kg95xx-power-monitoring-device-and-class-a-power-quality-recorder-device-manual?dti=0&pnid=24644&lc=en-CN>

[8] SICAM Q200 - 7KG97 - Multifunctional Recorder - Device Manual

<https://support.industry.siemens.com/cs/document/109744896/sicam-q200-7kg97-multifunctional-recorder-device-manual?dti=0&pnid=24645&lc=en-CN>

[9] SIPROTEC 5 SNMP MIB

<https://support.industry.siemens.com/cs/document/109742125/siprotec-5-snmp-mib?dti=0&pnid=24232&lc=en-WW>

[10] SICAM RTUs SNMP MIB File

<https://support.industry.siemens.com/cs/document/109773392/sicam-rtus-snmp-mib-file?dti=0&pnid=24232&lc=en-WW>

[11] EN100 Communication Module – Protocols (MIBs for SIP4, SIP Compact, Reyrolle)

<https://support.industry.siemens.com/cs/document/109745821/en100-communication-module-protocols?dti=0&pnid=24232&lc=en-WW>

Published by
Siemens AG

Smart Infrastructure
Digital Grid
Humboldtstrasse 59
90459 Nuremberg, Germany

www.siemens.com/siprotec

For more information,
please contact our
Customer Support Center.

Tel.: +49 180 524 70 00

Fax: +49 180 524 24 71

(Charges depending on provider)

Customer Support: www.siemens.com/csc

For the U.S. published by
Siemens Industry Inc.

100 Technology Drive
Alpharetta, GA 30005
United States

© 2020 Siemens. Subject to changes and errors.
The information given in this document only contains
general descriptions and/or performance features which
may not always specifically reflect those described, or
which may undergo modification in the course of further
development of the products. The requested performance
features are binding only when they are expressly agreed
upon in the concluded contract.

For all products using security features of OpenSSL, the
following shall apply:
This product includes software developed by the OpenSSL
Project for use in the OpenSSL Toolkit.
(<http://www.openssl.org/>)
This product includes cryptographic software written by
Eric Young (ey@cryptsoft.com)
This product includes software developed by Bodo Moeller.