BMC

SNMP

User's Manual

UM_BMC_SNMP_v1.3_121725

Table of Contents

Preface i
Chapter 1. Introduction 1
1.1 Overview 1
1.2 SNMP Manager 3
1.3 SNMP Agent 3
1.4 MIB 4
1.5 SNMP OID 4
1.6 SNMP Command 5
1.7 SNMP Trap 5
Chapter 2. SNMP Support 6
2.1 Supported SNMP Version and Security 6
2.2 Port 7
2.3 Default Community String for SNMP v1/v2c 7
Chapter 3. SNMP Implementation 8
3.1 Using the SNMP Command (Polling the AIC BMC) 8
3.2 Using the SNMP Trap (AIC BMC actively alerts) 9
Chapter 4. Installing the AIC MIB 10
4.1 SNMP Manager Requirements 10
4.2 Downloading the AIC MIB File 10
4.3 Installing the MIB File 11
Chapter 5. SNMP Command MIB Objects 12
5.1 Command MIB Object Table 12
5.2 systemInfo 12
5.3 sensorInfo 13
Chapter 6. SNMP Trap Mechanism 14
6.1 SNMP Trap Format 14
6.2 SNMP Trap List 16
Chapter 7. SNMP configuration via BMC GUI 20
7.1 Add SNMP access permissions and security settings for user 20
7.2 Delete SNMP access permissions for user 23
7.3 Community string Settings of SNMP v1/v2c 25
7.4 SNMP Trap Settings 26
Chapter 8. SNMP Command & Trap Testing - Example 30
8.1 SNMP Command & Trap Settings in SNMP Manager 30
8.1.1 Load AIC SNMP Command MIB and AIC SNMP Trap MIB file 30
8.1.2 SNMP Command Parameter Setting 32
8.1.3 SNMP Trap Parameter Setting 35
8.2 SNMP Command Testing 37
8.3 SNMP Trap Testing 40
8.3.1 SNMP Trap v1 40
8.3.2 SNMP Trap v2c 41
8.3.3 SNMP Trap v3 42
Chapter 9. Technical Support 43

Document Release History

Release Date	Version	Author	Update Content
March 29, 2024	1.0	Jethro Yeh	1. Initial Release (base on LTS-v12.5) 2. Support SNMP Trap v1/v2c/v3
July 23, 2024	1.1	Jethro Yeh	Uncheck “Event Specific Alert String” in Alert Policies
March 14, 2025	1.2	Daniel Lee	Highlight LAN Channel selection in Alert Policies
December 17, 2025	1.3	Alan Huang	1. Rename trap “trapAddInCardAsserted” to “trapPETAddInCardAsserted_func_0x0” 2. Add trap “trapPETAddInCardAsserted_func_0x1” to “trapPETAddInCardAsserted_func_0xF” in SNMP Trap List

Copyright © 2024 AIC®, Inc. All Rights Reserved.

This document contains proprietary information about AIC® products and is not to be disclosed or used except in accordance with applicable agreements.

Preface

Copyright

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photo-static, recording or otherwise, without the prior written consent of the manufacturer.

Trademarks

All products and trade names used in this document are trademarks or registered trademarks of their respective holders.

Changes

The material in this document is for information purposes only and is subject to change without notice.

Warning

1. A shielded-type power cord is required in order to meet FCC emission limits and also to prevent interference to the nearby radio and television reception. It is essential that only the supplied power cord be used.
2. Use only shielded cables to connect I/O devices to this equipment.
3. You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Disclaimer

AIC® shall not be liable for technical or editorial errors or omissions contained herein. The information provided is provided "as is" without warranty of any kind. To the extent permitted by law, neither AIC® or its affiliates, subcontractors or suppliers will be liable for incidental, special or consequential damages including downtime cost; lost profits; damages relating to the procurement of substitute products or services; or damages for loss of data, or software restoration. The information in this document is subject to change without notice.

Instruction Symbols

Special attention should be given to the instruction symbols below.

NOTE	This symbol indicates that there is an explanatory or supplementary instruction.
CAUTION	This symbol denotes possible hardware impairment. Upmost precaution must be taken to prevent serious hardware damage.
WARNING	This symbol serves as a warning alert for potential body injury. The user may suffer possible injury from disregard or lack of attention.

Chapter 1. Introduction

1.1 Overview

Simple Network Management Protocol (SNMP) is an application layer protocol of an Internet Standard protocol for exchanging management information between Network devices.

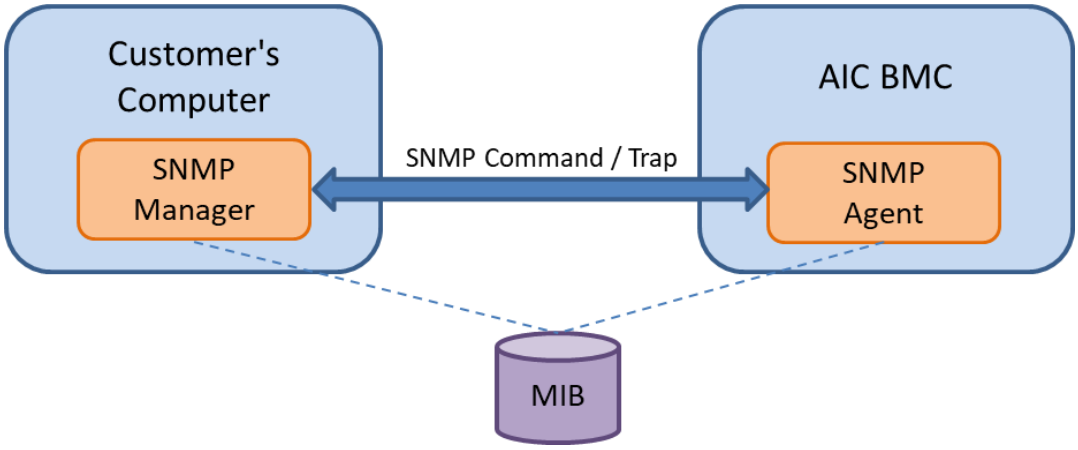
In an SNMP network, there are two key components:

- SNMP Agent:

  The SNMP Agent is a software module running on the AIC's Baseboard Management Controller (BMC), used to collect and store information about the system and motherboard. It responds to requests from SNMP Managers by providing access to specific variables defined in the Management Information Base (MIB) or SNMP Object Identifier (OID). The SNMP Agent acts as an interface between the AIC device and the SNMP Manager, facilitating communication and management operations.

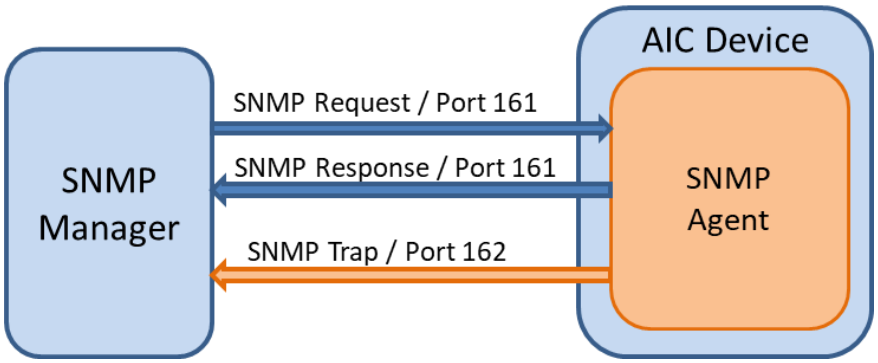
- SNMP Manager:

  The SNMP Manager is a monitoring and control software installed on a computer used to oversee AIC devices. It sends SNMP Command (requests) to retrieve information (responses) from SNMP Agents and receives SNMP Traps for real-time notifications of BMC alarms. The SNMP Manager utilizes MIB files to comprehend the structure and attributes of managed devices.



There are two methodologies of how the SNMP Manager can interact with the SNMP Agent:

- SNMP Command (Request/Response)
- SNMP Trap (Unsolicited events)



The SNMP is sent over User Datagram Protocol (UDP) as the transport protocol.

SNMP ports are utilized via UDP port 161 for SNMP Manager communicating with SNMP Agent using SNMP commands (i.e. polling).

SNMP Agent will send an "SNMP Trap" on UDP port 162 to the SNMP Manager.

These two ports are fundamental defaults. They are the same in all versions of SNMP, since SNMP v1.

1.2 SNMP Manager

The SNMP Manager is a monitoring and control software installed on a computer used to oversee AIC devices. It sends SNMP Command (requests) to retrieve information (responses) from SNMP Agents and receives SNMP traps for real-time notifications of BMC alarms.

The SNMP Manager utilizes MIB files to comprehend the structure and attributes of managed devices.

SNMP Manager's key functions:

- Queries SNMP Agent
- Gets responses from SNMP Agent
- Sets variables in SNMP Agent
- Acknowledges asynchronous events from SNMP Agent

1.3 SNMP Agent

The SNMP Agent, operating on the AIC's BMC, functions to gather and store data related to the system and motherboard. It responds to SNMP managers by SNMP OID or accessing specified variables from the MIB. Additionally, the SNMP Agent proactively sends SNMP Traps to the SNMP Manager to notify about events occurring on the AIC device.

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 SNMP manager.
- Acts as a proxy for some non–SNMP manageable network node.

We use open source **Net-SNMP** as SNMP Agent. Refer to the following URL to access more testing tools and instructions.

- http://www.net-snmp.org/

1.4 MIB

The Management Information Base (MIB) is a database that contains definitions of the variables accessible to SNMP Managers and Agents. MIB files define the structure of managed objects and their attributes, allowing for standardized communication between the SNMP Manager and Agents. By referencing MIB files, SNMP Managers can efficiently monitor, configure, and troubleshoot network devices in a uniform and organized manner.

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 SNMP Agent through the use of private MIBs.

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

Each MIB file describes a specific set of managed objects in a hierarchical manner using SNMP Object Identifier (OID) notation. Each node contains an object of information and is identified with a SNMP OID.

1.5 SNMP OID

SNMP Object Identifier (OID) is a unique identifier assigned to each managed object in the SNMP MIB. The OID is a hierarchical sequence of integers separated by dots that represents a specific attribute or parameter of a network device that can be managed using SNMP. OIDs form a tree-like structure where each node in the tree corresponds to a particular level of the hierarchy.

A typical object ID will be a dotted list of integers. For example, the OID in RFC1213 for "sysDescr" is .1.3.6.1.2.1.1.1

For example, OID value is “.1.3.6.1.” corresponds to text version of the MIB - “iso.org.dod.internet”

When a network administrator wants to monitor or control a specific parameter of a network device using SNMP, they use the OID associated with that parameter to uniquely identify it within the MIB. By querying or setting the value of an OID, administrators can retrieve information about the device's status, performance, or configuration, and also make changes to its settings remotely.

When queried for, the return value of each identifier could be different e.g. Text, Number, Counter, etc...

There are two types of Managed Object or Object ID: Scalar and Tabular.

When a network administrator wants to monitor or control a specific parameter of a network device using SNMP, they use the OID associated with that parameter to uniquely identify it within the MIB. By querying or setting the value of an OID, administrators can retrieve information about the device's status, performance, or configuration, and also make changes to its settings remotely.

1.6 SNMP Command

SNMP Commands are requests initiated by the SNMP Manager to gather information from SNMP Agent and receive responses.

These commands operate by referencing SNMP OID and accessing specified variables from the MIB. The SNMP Manager utilizes MIB files to understand the structure and attributes of managed devices, enabling effective communication with SNMP Agents.

SNMP Commands include querying SNMP Agents, receiving responses, setting variables, and acknowledging asynchronous events. They are sent over the network using the SNMP protocol to communicate with SNMP Agents effectively.

Command	Initiator	Receiver	Description
GET	Manager	Agent	It is performed to retrieve one or more values from the managed device.
GET NEXT	Manager	Agent	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	Manager	Agent	The GETBULK operation is used to retrieve voluminous data from large MIB table.
SET	Manager	Agent	This operation is used by the managers to modify or assign the value of the Managed device.
TRAPS	Agent	Manager	To notify the events occurring on agents.
INFORM	Agent	Manager	INFORM includes confirmation from the SNMP manager on receiving the message. To guarantee delivery of traps to Manager.
RESPONSE	Agent	Manager	It is the command used to carry back the value(s) or signal of actions directed by the SNMP Manager.

1.7 SNMP Trap

SNMP Trap is a kind of proactive notification mechanism. When a monitored device experiences specific events, such as connection failures, errors, etc., the BMC will immediately send Trap information to the SNMP Manager. This enables the SNMP Manager to receive and process critical device status information in real-time.

SNMP Trap helps monitor the operational status of systems and promptly detect issues, thereby improving system availability and efficiency.

Chapter 2. SNMP Support

2.1 Supported SNMP Version and Security

Support for three versions of SNMP:

- SNMP Version 1 (SNMPv1)
- SNMP Version 2c (SNMPv2c)
- SNMP Version 3 (SNMPv3)

Supported Security:

SNMP Protocol Version	Security Mechanism
SNMP v1	Community–based security
SNMP v2c	Community–based security
SNMP v3	User–based security

In SNMP, security measures vary across different protocol versions. SNMP v1 and v2c utilize **Community-based** security, where access control is based on the shared **Community string** provided in the configuration. This security mechanism is relatively simple and lacks robust authentication methods. For the **default Community string**, refer to "**2.3 Default Community String for SNMP v1/v2c**".

On the other hand, SNMP v3 introduces **User-based** security, offering a higher level of security. In this scenario, individual user accounts are set up with authentication through passwords and encryption for access control to ensure data protection. SNMP v3 stands out as the most secure SNMP version, providing comprehensive security measures for enhanced system protection.

The security username is the same configurable administrator username used for the BMC Web GUI management interfaces.

The SNMPv3 security settings are configured through the BMC Web GUI management interface.

The supported security protocols are as follows:

Security Model	Security Level	Authentication	Privacy (Encryption)
V1	NoAuthNoPriv	Community string	None
V2C	NoAuthNoPriv	Community string	None
V3	AuthPriv	SHA256, SHA384 and SHA512	AES, DES

Security Level:

- NoAuthNoPriv: This security level signifies that no authentication or privacy mechanisms are employed. It allows for data exchange without encryption or authentication layers.
- AuthPriv: At this security level, both message authentication and encryption are implemented. It guarantees data integrity and confidentiality during communication within BMC applications using SNMP.

NOTE: Privacy without authentication is invalid.

Authentication:

- Purpose: Authentication in SNMP ensures that the identity of the sender and receiver of SNMP messages is verified, preventing unauthorized access and message tampering.
- Methods: Authentication can be achieved using mechanisms such as SHA256 (Secure Hash Algorithm), which generate hash values to authenticate the integrity of SNMP messages.

PS: SHA and MD5 protocols are deprecated.

Privacy (also known as Encryption):

- Purpose: Privacy in SNMP safeguards the confidentiality of SNMP messages transmitted between devices by encrypting the data, making it indecipherable to unauthorized users.
- Methods: Privacy mechanisms like AES (Advanced Encryption Standard) are commonly used to encrypt SNMP messages, ensuring that the information exchanged between devices remains secure and confidential.

2.2 Port

UDP Port	Function
161	SNMP Command (Request/Response)
162	SNMP Trap (Unsolicited events)

Note: The SNMP agent listens for UDP 161, and the SNMP manager listens for UDP 162.

2.3 Default Community String for SNMP v1/v2c

Default SNMP read-only community string: **rocommstr**

Default SNMP read-write community string: **rwcommstr**

To modify the Community string, refer to "**7.3 Community string Settings of SNMP v1/v2c**".

Chapter 3. SNMP Implementation

To use the SNMP, the AIC MIB must be installed onto the workstation acting as the SNMP manager.

Once installed, the SNMP manager can employ the MIB to interact with the SNMP agent on the AIC BMC. This interaction enables the SNMP manager to retrieve and modify configuration data through SNMP GETs and SETs.

Detailed instructions for installing the AIC MIB can be found in "**Chapter 4 - Installing the AIC MIB**".

The AIC BMC actively listens for SNMP queries on port 161 and transmits information back to the SNMP manager on port 162.

For security requirements for each SNMP version, refer to "**2.1 Supported SNMP Version and Security**".

The relevant settings in the SNMP Manager should refer to the documentation of the SNMP Manager software you are using.

3.1 Using the SNMP Command (Polling the AIC BMC)

The SNMP Manager needs to load the AIC's **BMC_SNMP_Command.mib**

SNMP Manager can poll for the AIC BMC using the following OID:

iso.org.dod.internet.private.enterprises.AIC.aicMIB

or

1.3.6.1.4.1.42385.554

For SNMP v1/v2c:

The correct **SNMP Community string** and **IP address of SNMP Agent** needs to be set in the SNMP Manager so that the AIC BMC can respond to this object.

For the default Community string, refer to "**2.3 Default Community String for SNMP v1/v2c**".

For SNMP v3:

The following settings need to be made in the SNMP Manager. When the SNMP manager sends SNMP Command, the AIC BMC will respond to that object.

- **IP address of SNMP Agent**
- **Username, Password**
- **Authentication, Privacy**

For username, authentication and privacy settings on AIC BMC, refer to "**7.1 Add SNMP access permissions and security settings for user**".

For Password, same password used to log in to the BMC Web GUI.

3.2 Using the SNMP Trap (AIC BMC actively alerts)

The SNMP manager needs to load the AIC's **BMC_SNMPv1_Trap.mib** and **BMC_SNMPv2c_v3_Trap.mib**

For SNMP trap v1/v2c:

The following settings need to be made in the SNMP Manager. When AIC BMC actively sends SNMP traps, the SNMP manager can correctly parse them.

- **Authenticate v1/v2c traps (Community)**
- **SNMP Community string**
- **Listening port:** UDP 162

For the default Community string, refer to "**2.3 Default Community String for SNMP v1/v2c**".

For configuring SNMP trap v1/v2c on AIC BMC, refer to "**7.4 SNMP Trap Settings**".

For SNMP trap v3:

The following settings need to be made in the SNMP Manager. When AIC BMC actively sends SNMP traps, the SNMP manager can correctly parse them.

- **Authenticate v3 Trap**
- **Username**
- **Password**
- **Authentication**
- **Privacy**

For username, authentication and privacy settings on AIC BMC, refer to "**7.1 Add SNMP access permissions and security settings for user**".

For Password, same password used to log in to the BMC Web GUI.

For configuring SNMP trap v3 on AIC BMC, refer to "**7.4 SNMP Trap Settings**".

Chapter 4. Installing the AIC MIB

4.1 SNMP Manager Requirements

The SNMP manager must adhere to the following requirements:

- A workstation running on UNIX or Windows
- Installation of an extensible SNMP Network Management System (NMS) application on the workstation
- Adequate free hard disk space to store the AIC MIB file.

4.2 Downloading the AIC MIB File

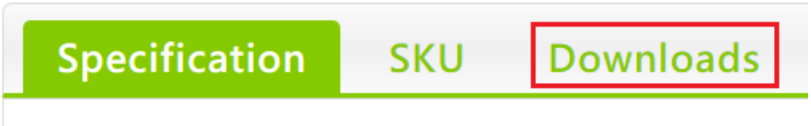
The AIC MIB file can be obtained by downloading it from the **BMC firmware image** directory.

The MIB's version, compatible with your release, is specified in the Release Notes. Make sure to select the appropriate version of the MIB that corresponds to your firmware release.

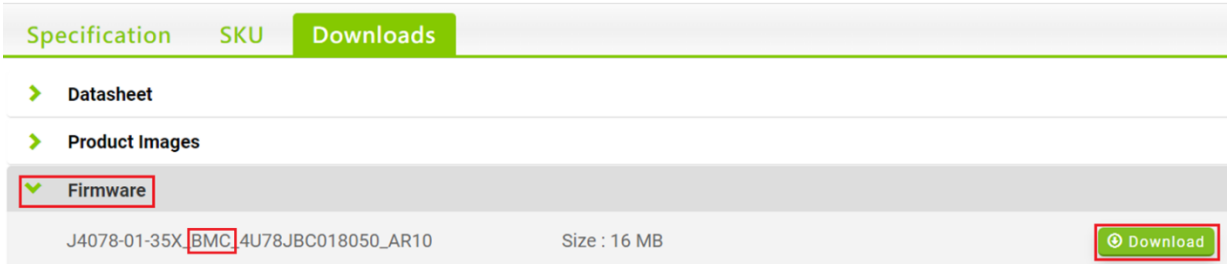
To download the MIB file from the release firmware image directory, follow the steps below:

1. Navigate to the AIC website at https://www.aicipc.com/ .
2. Input the product name in the search bar and click on the search icon.

3. Choose the specific product from the search results.
4. Navigate to the "Downloads" page within the product description.



5. Click on the "Firmware" section, then select the "Download" button to acquire the desired MIB file.



4.3 Installing the MIB File

The procedure for installing the AIC MIB file onto the SNMP manager depends on the SNMP management application you are using. Each SNMP management tool has its distinct installation procedure.

To clarify the process for installing the AIC MIB file on the SNMP manager, kindly consult the respective SNMP management application's documentation.

AIC provides 3 MIB files. SNMP Manager needs to load them.

- **BMC_SNMP_Command**.mib: Used for SNMP command
- **BMC_SNMPv1_Trap**.mib: Used for SNMP Trap v1
- **BMC_SNMPv2c_v3_Trap**.mib: Used for SNMP Trap v2c/v3

Chapter 5. SNMP Command MIB Objects

5.1 Command MIB Object Table

What you can do with the MIB objects depends on the access defined for the specific object.

The top level of the MIB consists of tables that contain all the MIB objects. They are called aicMIB and are used for monitoring the AIC device.

Object Name	Object ID
iso.org.dod.internet.private.enterprises.AIC.aicMIB	1.3.6.1.4.1.42385.554

Lists the MIB objects described in this chapter:

Object Name	Object ID	Description
systemInfo	1.3.6.1.4.1.42385.554.1	Provides the list of system information.
sensorInfo	1.3.6.1.4.1.42385.554.2	Provides the list of sensor information.

5.2 systemInfo

You can use this table to read or set system-related information.

Object Name	Object ID	Description	Type	Access
hostName	1.3.6.1.4.1.42385.554.1.1.0	The host name of BMC.	DisplayString	Read-only
platformName	1.3.6.1.4.1.42385.554.1.2.0	The platform name of system.	DisplayString	Read-only
bmcFwVersion	1.3.6.1.4.1.42385.554.1.3.0	The firmware version of BMC.	DisplayString	Read-only
bmcFwName	1.3.6.1.4.1.42385.554.1.4.0	The firmware name of BMC.	DisplayString	Read-only
powerState	1.3.6.1.4.1.42385.554.1.5.0	The power state of system.	DisplayString	Read-only
powerOnHours	1.3.6.1.4.1.42385.554.1.6.0	Power-On Hours for system.	DisplayString	Read-only
chassisType	1.3.6.1.4.1.42385.554.1.11.0	The type for chassis.	DisplayString	Read-only
chassisPartNum	1.3.6.1.4.1.42385.554.1.12.0	The part number of chassis.	DisplayString	Read-only
chassisSerialNum	1.3.6.1.4.1.42385.554.1.13.0	The serial number of chassis.	DisplayString	Read-only

boardMfr	1.3.6.1.4.1.42385.554.1.21.0	The manufacturer of the motherboard.	DisplayString	Read-only
boardProductName	1.3.6.1.4.1.42385.554.1.22.0	The product name of the motherboard.	DisplayString	Read-only
boardSerialNum	1.3.6.1.4.1.42385.554.1.23.0	The serial number of the motherboard.	DisplayString	Read-only
boardPartNum	1.3.6.1.4.1.42385.554.1.24.0	The part number of the motherboard.	DisplayString	Read-only
productMfr	1.3.6.1.4.1.42385.554.1.31.0	The manufacturer of the product.	DisplayString	Read-only
productName	1.3.6.1.4.1.42385.554.1.32.0	The name of the product.	DisplayString	Read-only
productPartNum	1.3.6.1.4.1.42385.554.1.33.0	The part number of the product.	DisplayString	Read-only
productVersion	1.3.6.1.4.1.42385.554.1.34.0	The version of the product.	DisplayString	Read-only
productSerialNum	1.3.6.1.4.1.42385.554.1.35.0	The serial number of the product.	DisplayString	Read-only
productAssetTag	1.3.6.1.4.1.42385.554.1.36.0	The asset tag of the product.	DisplayString	Read-only
bmcMacAddress1	1.3.6.1.4.1.42385.554.1.41.0	MAC address of the BMC dedicate NIC 1	DisplayString	Read-only

5.3 sensorInfo

You can use this table to read sensor-related information.

Object Name	Object ID	Description	Type	Access
sensorIndex	1.3.6.1.4.1.42385.554.2.1.1.1.**N**	The sensor index of the sensor device.	Integer32	Read-only
sensorName	1.3.6.1.4.1.42385.554.2.1.1.2.**N**	The sensor name of the sensor device.	DisplayString	Read-only
sensorNumber	1.3.6.1.4.1.42385.554.2.1.1.3.**N**	The sensor number of the sensor device.	Integer32	Read-only
sensorValue	1.3.6.1.4.1.42385.554.2.1.1.4.**N**	The value read from the sensor device.	Double	Read-only
sensorStatus	1.3.6.1.4.1.42385.554.2.1.1.5.**N**	The status of the sensor device.	DisplayString	Read-only

PS: N represents a number. The mapping of numbers is the same as that of IPMI SDR.

Chapter 6. SNMP Trap Mechanism

This chapter describes the AIC BMC SNMP trap and alarm handling mechanism.

The SNMP traps generated by the AIC BMC adhere to the **Platform Event Trap Format Specification v1.0**.

In the case of an alarm or event condition, the AIC BMC sends synchronous information to the SNMP Manager in the form of a trap. The trap is sent to the hosts defined in the BMC Web GUI.

The SNMP traps are triggered by system alarms and are distinguished by unique identifiers associated with each alarm. These identifiers are prominently displayed within the traps. In the MIB, the OID of the trap object corresponds directly to the alarm ID.

The customer can use the specific-trap number to identify the trap, and this number can be found in MIB file.

6.1 SNMP Trap Format

The following table is a summary of the SNMP Trap PDU (protocol data unit) format. In addition the SNMP header shall carry the following fields:

Version	SNMP rev-1
Community String	Default = 'public'. This string may optionally be used to hold a vendor-specific string that is used to identify or provide SNMP access to the system that generated the event.

Table 1 - Trap PDU format per RFC 1157

enterprise	OID = iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).wired_for_management(3183).PET(1).version(1)
agent-addr	NetworkAddress
generic-trap	EnterpriseSpecific(6)
specific-trap	See below.
time-stamp	Time elapsed between last (re) initialization of the network entity and the generation of the trap
variable-bindings	Other information, defined below

Specific Trap

The specific-trap and variable-bindings fields carry the heart of the Platform Event Trap information.

The content and definition of these fields is specified in the following tables.

Table 2 -"Specific Trap" field

Field #	Name	size/ type	Description
1	Event	integer	31:24 reserved. 0000_0000b 23:16 Event Sensor Type An *Event Sensor* is a logical entity that is responsible for detecting events. The *Event Sensor Type* field indicates what types of events the sensor is monitoring. E.g. *temperature, voltage, current, BIOS, POST, processor, fan, etc.* (This field corresponds to the IPMI 'Sensor Type' field, and conceptually maps to the 'cause of trap' field in the Phoenix proposal.) 15:8 Event Type Code indicating what type of transition / state change triggered the trap. (Corresponds to IPMI 'Event Type' field) The code is split into the following ranges: 00-0Bh = generic - can be used with any type of sensor 6Fh = sensor specific 70h-7Fh = OEM all other = reserved See Table 4, below, for generic event type codes 7:0 Event Offset Indicates which particular event occurred for a given Event Type. This field allows events to be extended on a per Event Type basis—making it easier to manage the Event Type 'name space'. 7 0 = Assertion Event. (Event occurred when state became asserted) 1 = Deassertion Event. 6:4 reserved. 000b. 3:0 Offset Value. Per IPMI, up to 15 different discrete states are allowed per each Event Type. 0Fh = unspecified.

You can refer to Platform Event Trap Format Specification for more information:

- https://www.intel.com/content/dam/www/public/us/en/documents/product-briefs/platform-event-trap.pdf

6.2 SNMP Trap List

OID: 1.3.6.1.4.1.3183.1.1

Threshold: Please refer to SDR list file in release package.

Sensor Type	Specific Trap (Dec)	Specific Trap (HEX)	Object Name	Description
Temperature	65792	10100	trapTempLNCLowAsserted	Temperature Lower Non-Critical going low - Asserted
Temperature	65794	10102	trapTempLCLowAsserted	Temperature Lower Critical going low - Asserted
Temperature	65796	10104	trapTempLNRLowAsserted	Temperature Lower Non-Recoverable going low - Asserted
Temperature	65799	10107	trapTempUNCHighAsserted	Temperature Upper Non-Critical going high - Asserted
Temperature	65801	10109	trapTempUCHighAsserted	Temperature Upper Critical going high - Asserted
Temperature	65803	1010B	trapTempUNRHighAsserted	Temperature Upper Non-Recoverable going high - Asserted
Temperature	65920	10180	trapTempLNCLowDeasserted	Temperature Lower Non-Critical going low - Deasserted
Temperature	65922	10182	trapTempLCLowDeasserted	Temperature Lower Critical going low - Deasserted
Temperature	65924	10184	trapTempLNRLowDeasserted	Temperature Lower Non-Recoverable going low - Deasserted
Temperature	65927	10187	trapTempUNCHighDeasserted	Temperature Upper Non-Critical going high - Deasserted
Temperature	65929	10189	trapTempUCHighDeasserted	Temperature Upper Critical going high - Deasserted
Temperature	65931	1018B	trapTempUNRHighDeasserted	Temperature Upper Non-Recoverable going high - Deasserted
Voltage	131328	20100	trapVoltageLNCLowAsserted	Voltage Lower Non-Critical going low - Asserted
Voltage	131330	20102	trapVoltageLCLowAsserted	Voltage Lower Critical going low - Asserted
Voltage	131332	20104	trapVoltageLNRLowAsserted	Voltage Lower Non-Recoverable going low - Asserted
Voltage	131335	20107	trapVoltageUNCHighAsserted	Voltage Upper Non-Critical going high - Asserted
Voltage	131337	20109	trapVoltageUCHighAsserted	Voltage Upper Critical going high - Asserted
Voltage	131339	2010B	trapVoltageUNRHighAsserted	Voltage Upper Non-Recoverable going high - Asserted
Voltage	131456	20180	trapVoltageLNCLowDeasserted	Voltage Lower Non-Critical going low - Deasserted

Sensor Type	Specific Trap (Dec)	Specific Trap (HEX)	Object Name	Description
Voltage	131458	20182	trapVoltageLCLowDeasserted	Voltage Lower Critical going low - Deasserted
Voltage	131460	20184	trapVoltageLNRLowDeasserted	Voltage Lower Non-Recoverable going low - Deasserted
Voltage	131463	20187	trapVoltageUNCHighDeasserted	Voltage Upper Non-Critical going high - Deasserted
Voltage	131465	20189	trapVoltageUCHighDeasserted	Voltage Upper Critical going high - Deasserted
Voltage	131467	2018B	trapVoltageUNRHighDeasserted	Voltage Upper Non-Recoverable going high - Deasserted
Fan	262400	40100	trapFanLNCLowAsserted	Fan Lower Non-Critical going low - Asserted
Fan	262402	40102	trapFanLCLowAsserted	Fan Lower Critical going low - Asserted
Fan	262404	40104	trapFanLNRLowAsserted	Fan Lower Non-Recoverable going low - Asserted
Fan	262407	40107	trapFanUNCHighAsserted	Fan Upper Non-Critical going high - Asserted
Fan	262409	40109	trapFanUCHighAsserted	Fan Upper Critical going high - Asserted
Fan	262411	4010B	trapFanUNRHighAsserted	Fan Upper Non-Recoverable going high - Asserted
Fan	262528	40180	trapFanLNCLowDeasserted	Fan Lower Non-Critical going low - Deasserted
Fan	262530	40182	trapFanLCLowDeasserted	Fan Lower Critical going low - Deasserted
Fan	262532	40184	trapFanLNRLowDeasserted	Fan Lower Non-Recoverable going low - Deasserted
Fan	262535	40187	trapFanUNCHighDeasserted	Fan Upper Non-Critical going high - Deasserted
Fan	262537	40189	trapFanUCHighDeasserted	Fan Upper Critical going high - Deasserted
Fan	262539	4018B	trapFanUNRHighDeasserted	Fan Upper Non-Recoverable going high - Deasserted
CPU	487169	76F01	trapCPUThermalTripAsserted	CPU Thermal Trip - Asserted
PSU	552704	86F00	trapPSUPresenceAsserted	Power Supply Presence detected - Asserted
PSU	552705	86F01	trapPSUFailureAsserted	Power Supply Failure detected - Asserted
PSU	552707	86F03	trapPSUAClostAsserted	Power Supply AC lost - Asserted
PSU	552709	86F05	trapPSUACOutOfRangeButPresentAsserted	Power Supply AC Out Of Range But Present - Asserted
PSU	552832	86F80	trapPSUPresenceDeasserted	Power Supply Presence detected - Deasserted

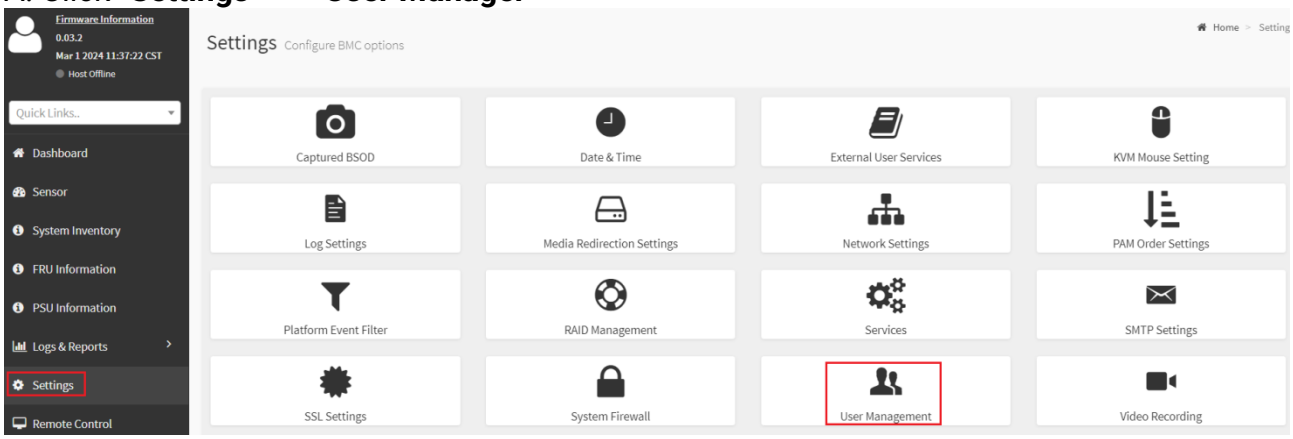
Sensor Type	Specific Trap (Dec)	Specific Trap (HEX)	Object Name	Description
PSU	552833	86F81	trapPSUFailureDeasserted	Power Supply Failure detected - Deasserted
PSU	552835	86F83	trapPSUAClostDeasserted	Power Supply AC lost - Deasserted
PSU	552837	86F85	trapPSUACOutOfRangeButPresentDeasserted	Power Supply AC Out Of Range But Present - Deasserted
DIMM	814848	C6F00	trapDIMMCorrectableECCAsserted	DIMM Correctable ECC Error - Asserted
DIMM	814849	C6F01	trapDIMMUncorrectableECCAsserted	DIMM Uncorrectable ECC Error - Asserted
DIMM	814855	C6F07	trapDIMMConfigurationErrorAsserted	DIMM Configuration Error - Asserted
System	1444352	160A00	trapMEPowerOnAsserted	Microcontroller / Coprocessor Transition to Running - Asserted
Add in card	1535744	176F00	trapPETAddInCardAsserted_func_0x0	Add-in Card Function 0x0 – Asserted
Add in card	1535745	176F01	trapPETAddInCardAsserted_func_0x1	Add-in Card Function 0x1 – Asserted
Add in card	1535746	176F02	trapPETAddInCardAsserted_func_0x2	Add-in Card Function 0x2 – Asserted
Add in card	1535747	176F03	trapPETAddInCardAsserted_func_0x3	Add-in Card Function 0x3 – Asserted
Add in card	1535748	176F04	trapPETAddInCardAsserted_func_0x4	Add-in Card Function 0x4 – Asserted
Add in card	1535749	176F05	trapPETAddInCardAsserted_func_0x5	Add-in Card Function 0x5 – Asserted
Add in card	1535750	176F06	trapPETAddInCardAsserted_func_0x6	Add-in Card Function 0x6 – Asserted
Add in card	1535751	176F07	trapPETAddInCardAsserted_func_0x7	Add-in Card Function 0x7 – Asserted
Add in card	1535752	176F08	trapPETAddInCardAsserted_func_0x8	Add-in Card Function 0x8 – Asserted
Add in card	1535753	176F09	trapPETAddInCardAsserted_func_0x9	Add-in Card Function 0x9 – Asserted
Add in card	1535754	176F0A	trapPETAddInCardAsserted_func_0xA	Add-in Card Function 0xA – Asserted
Add in card	1535755	176F0B	trapPETAddInCardAsserted_func_0xB	Add-in Card Function 0xB – Asserted
Add in card	1535756	176F0C	trapPETAddInCardAsserted_func_0xC	Add-in Card Function 0xC – Asserted
Add in card	1535757	176F0D	trapPETAddInCardAsserted_func_0xD	Add-in Card Function 0xD – Asserted
Add in card	1535758	176F0E	trapPETAddInCardAsserted_func_0xE	Add-in Card Function 0xE – Asserted
Add in card	1535759	176F0F	trapPETAddInCardAsserted_func_0xF	Add-in Card Function 0xF – Asserted
System	1575424	180A00	trapChassisPowerOnAsserted	Chassis Transition to Running - Asserted

Sensor Type	Specific Trap (Dec)	Specific Trap (HEX)	Object Name	Description
System	1575426	180A02	trapChassisPowerOffAsserted	Chassis Transition to Power Off - Asserted
System	1928967	1D6F07	trapSystemRestartAsserted	System Boot / Restart System Restart - Asserted
System	2060037	1F6F05	trapOSBootAsserted	OS Boot ROM Boot Completed - Asserted
System	12585472	C00A00	trapPowerOnAsserted	OEM Transition to Running - Asserted
System	12585474	C00A02	trapPowerOffAsserted	OEM Transition to Power Off - Asserted
System	12611328	C06F00	trapPowerResetAsserted	OEM System Reset Event - Asserted

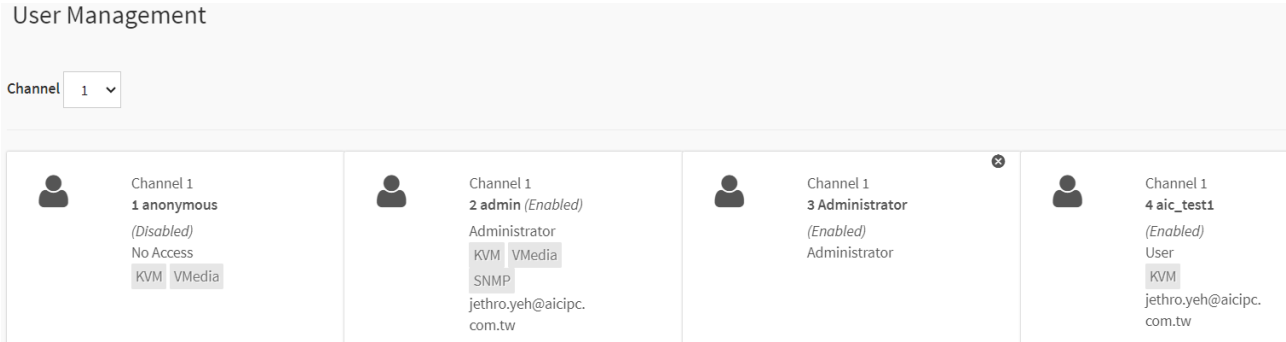
Chapter 7. SNMP configuration via BMC GUI

7.1 Add SNMP access permissions and security settings for user

A. Click “**Settings**” => “**User Manager**”



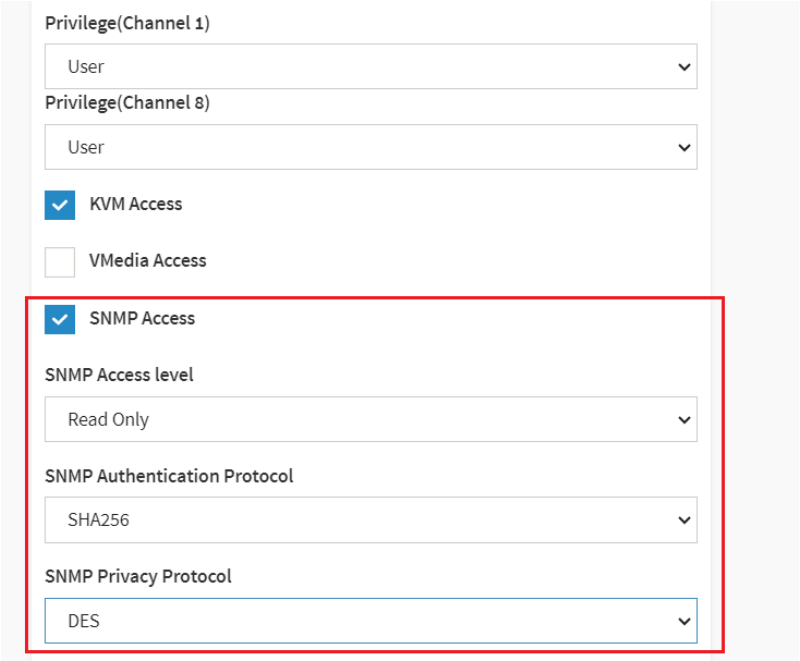
B. Choose the IPMI user to which you want to add SNMP permissions. Then the **User Management Configuration** page will be displayed. (aic_test1 is an example)

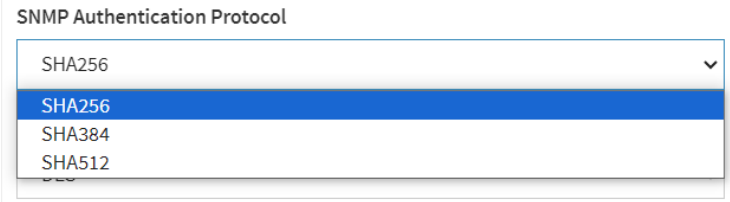


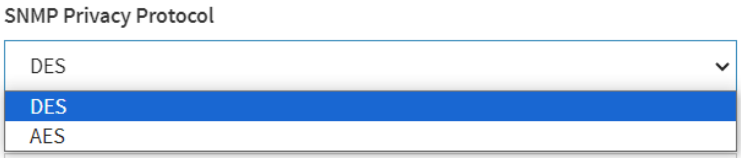
C. Check "**SNMP Access**" and enter SNMP settings in the **User Management Configuration** page.

Use the dropdown menu to select the settings for **SNMP Authentication Protocol** and **SNMP Privacy Protocol**.

PS: SNMP authentication and SNMP privacy are only used in **SNMP v3**.

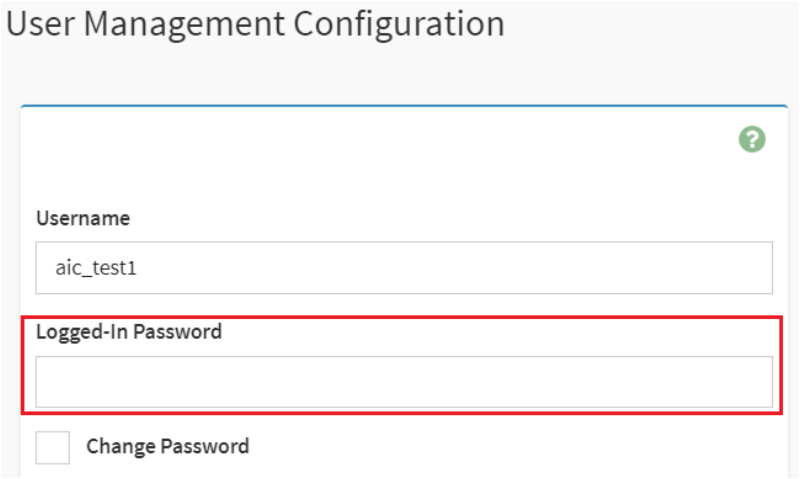




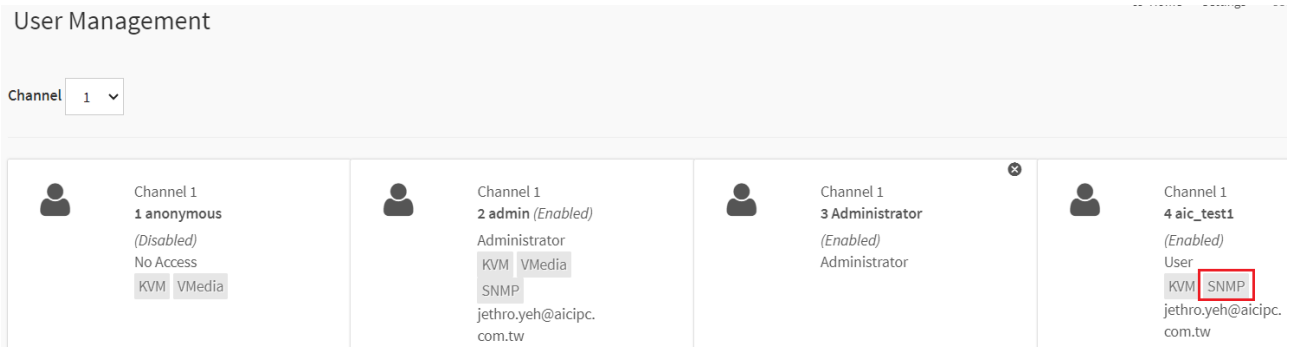


D. Enter the login password in the "**Logged-In Password**" field

=> Click "**Save**" at the bottom.

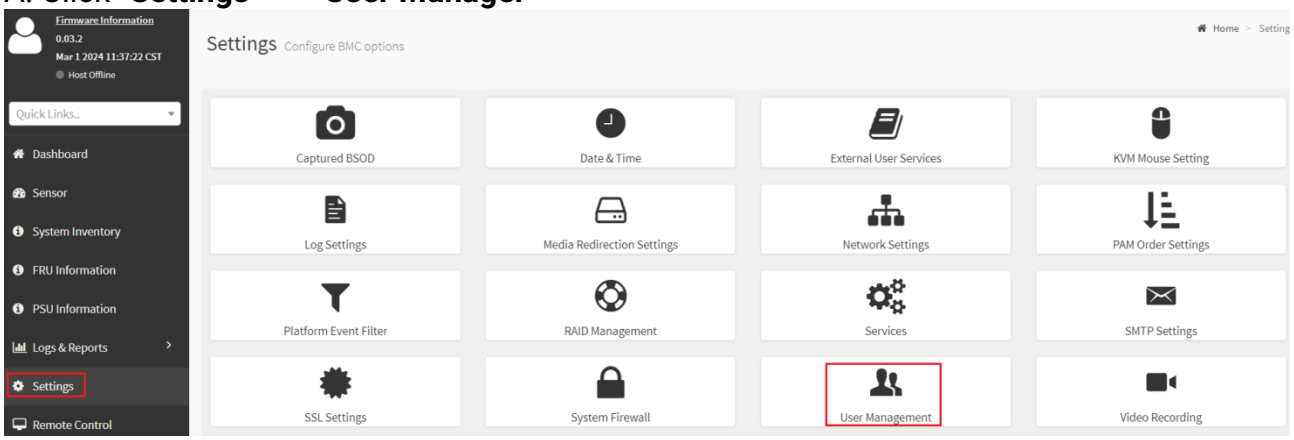


E. SNMP icon of user indicates that they have SNMP access permissions.

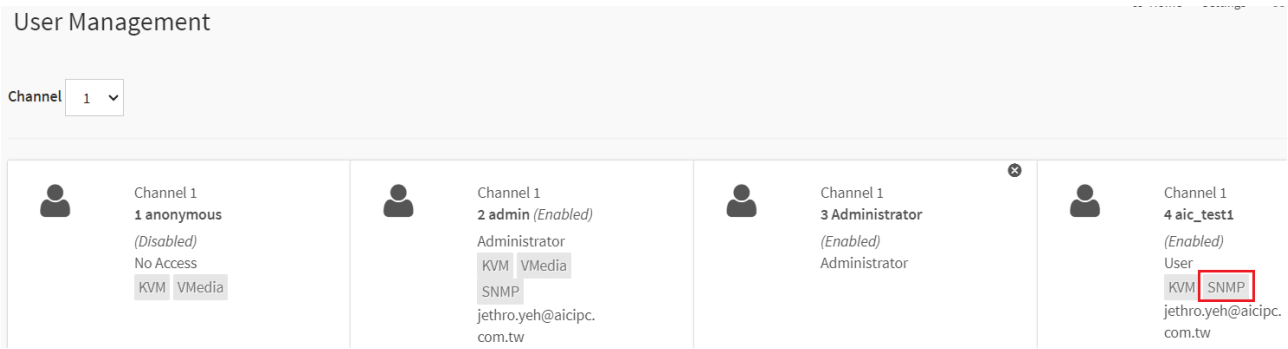


7.2 Delete SNMP access permissions for user

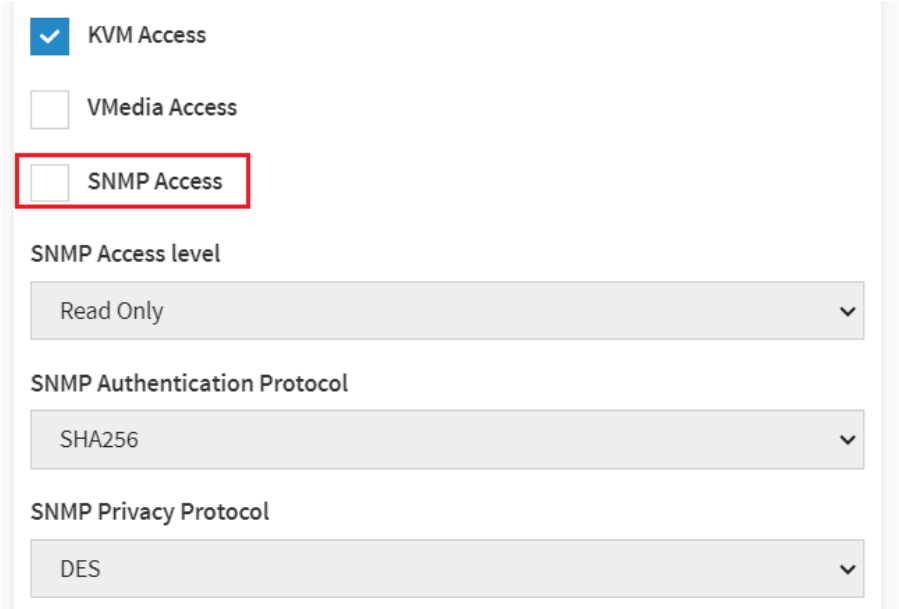
A. Click **"Settings"** => **"User Manager"**



B. Choose the user to which you want to delete SNMP permissions. Then the **User Management Configuration** page will be displayed. (aic_test1 is an example)

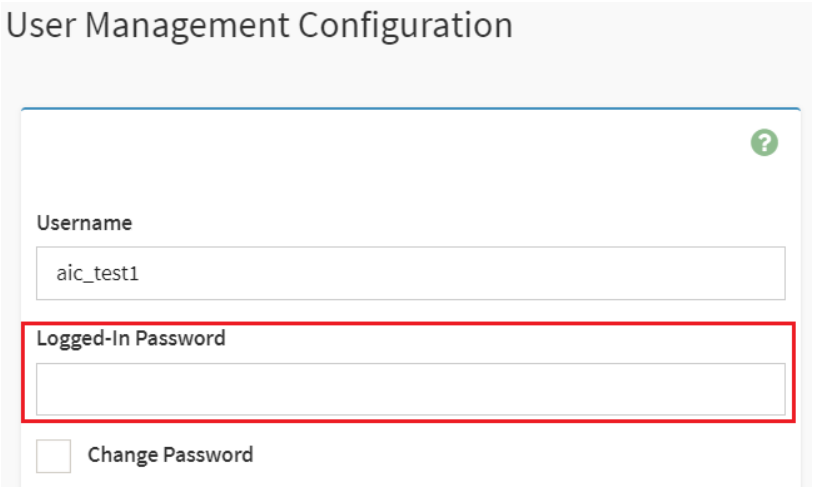


C. Uncheck "**SNMP Access**" in the **User Management Configuration** page.

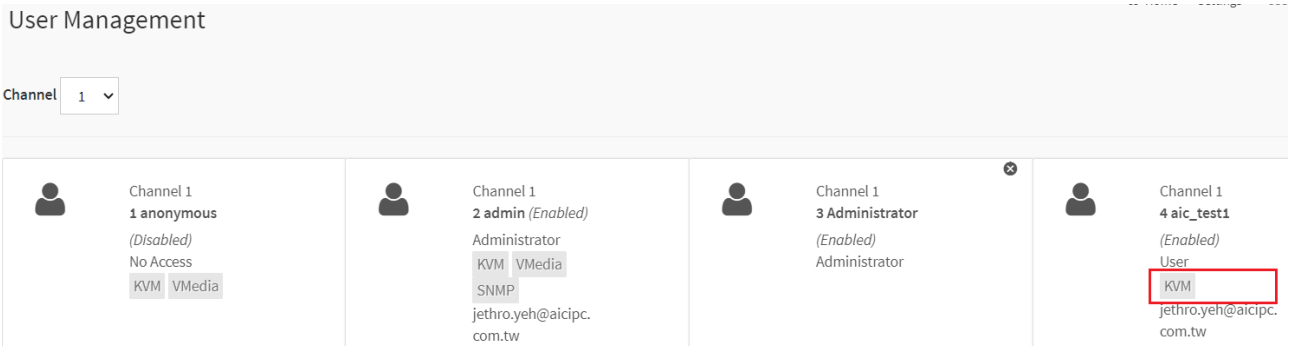


D. Enter the login password in the "**Logged-In Password**" field

=> Click "**Save**" at the bottom.

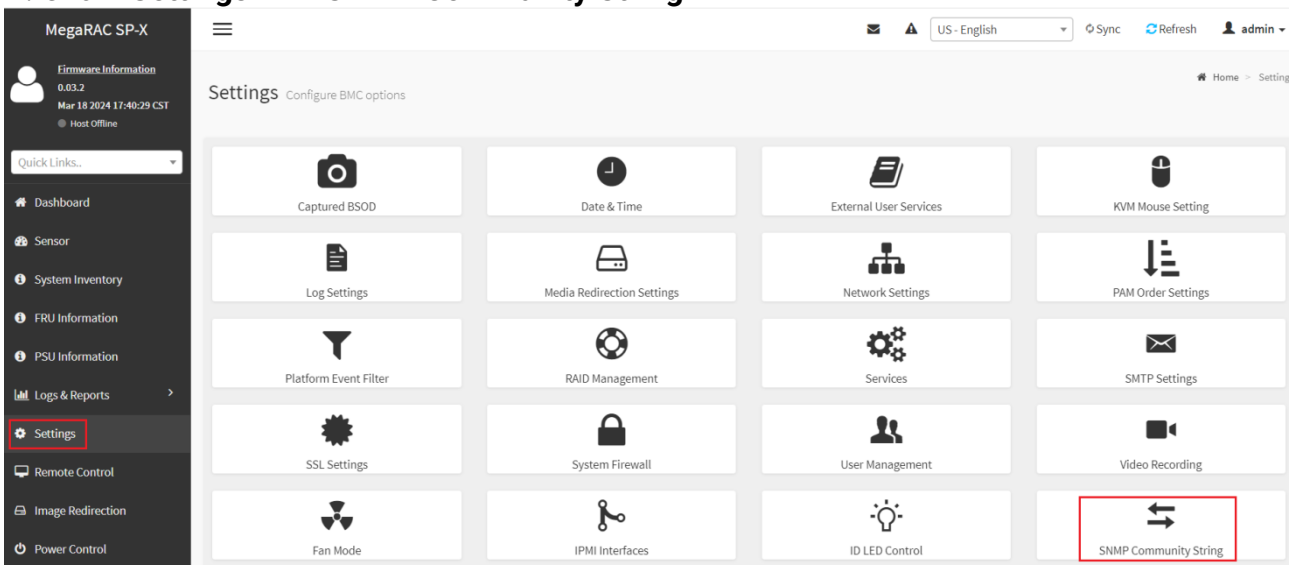


E. The disappearance of the SNMP icon of user indicates that there is no SNMP access permission.



7.3 Community string Settings of SNMP v1/v2c

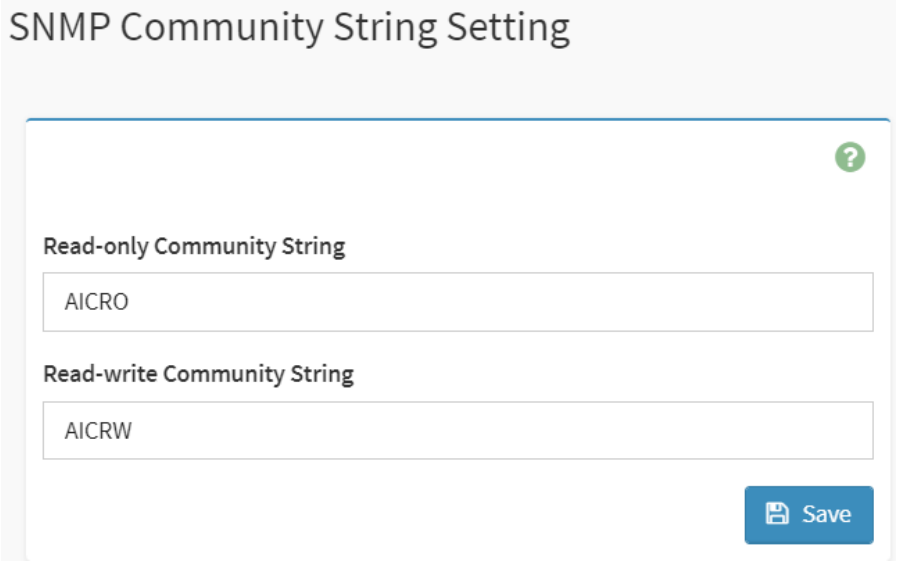
A. Click “**Settings**” => “**SNMP Community String**”



B. Enter the new SNMP community string for read-only in the "**Read-only Community String**" field => Enter the new SNMP community string for read-write in the "**Read-write Community String**" field

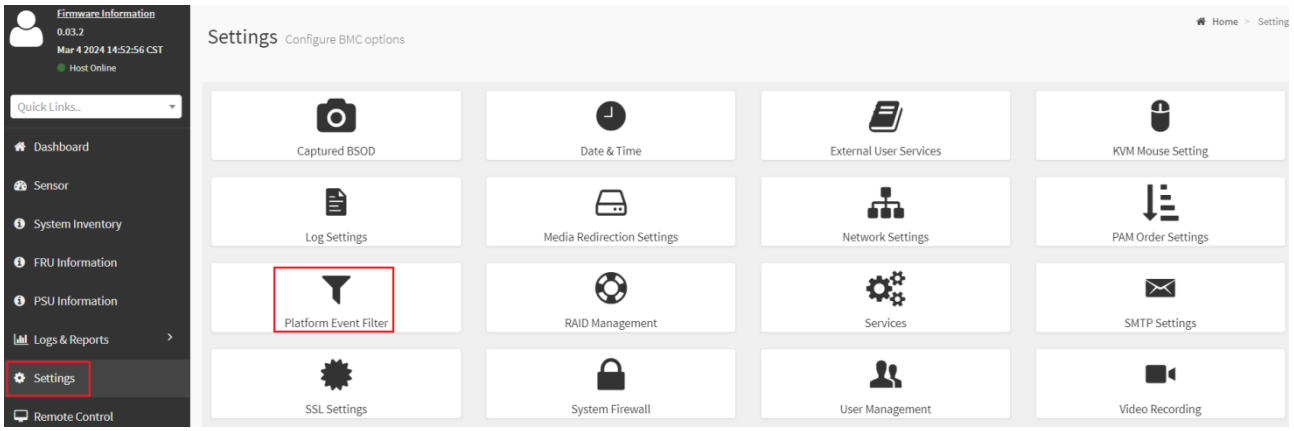
=> Click “**Save**” at the bottom.

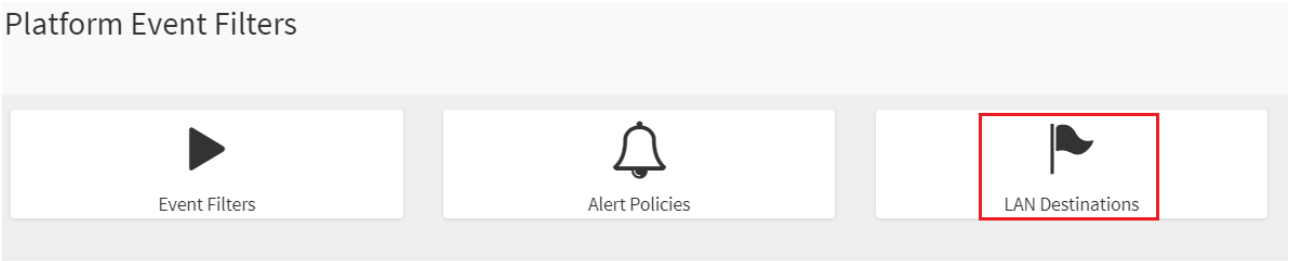
> **NOTE**
>
> 1. SNMP community string is only used in **SNMP v1/v2c**.
> 2. Only accounts with "Administrator" privilege level can modify it.



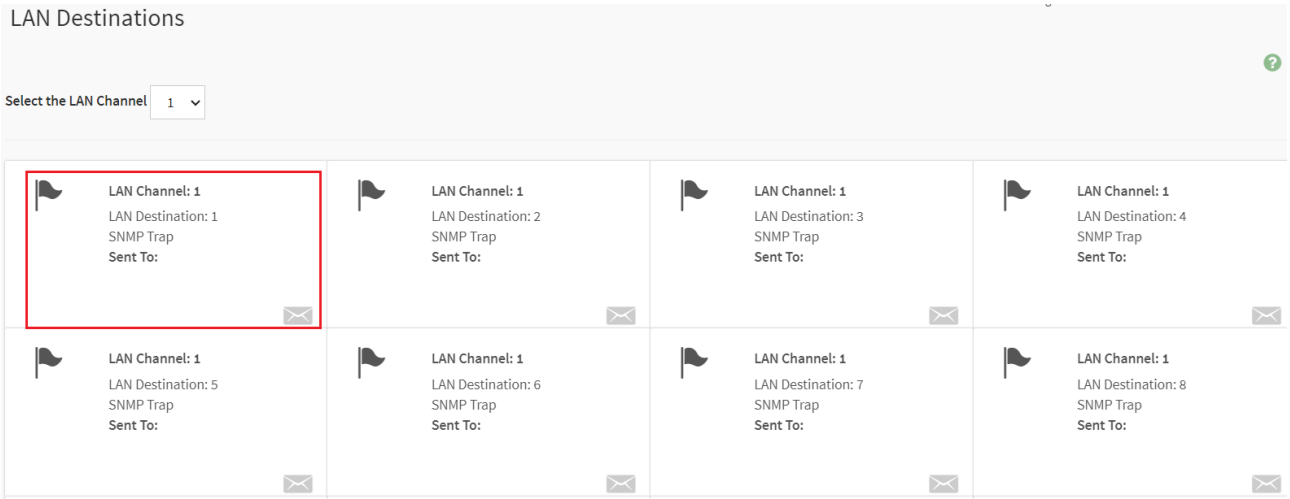
7.4 SNMP Trap Settings

A. Click **"Settings"** => **"Platform Event Filters"** => **"LAN Destinations"**





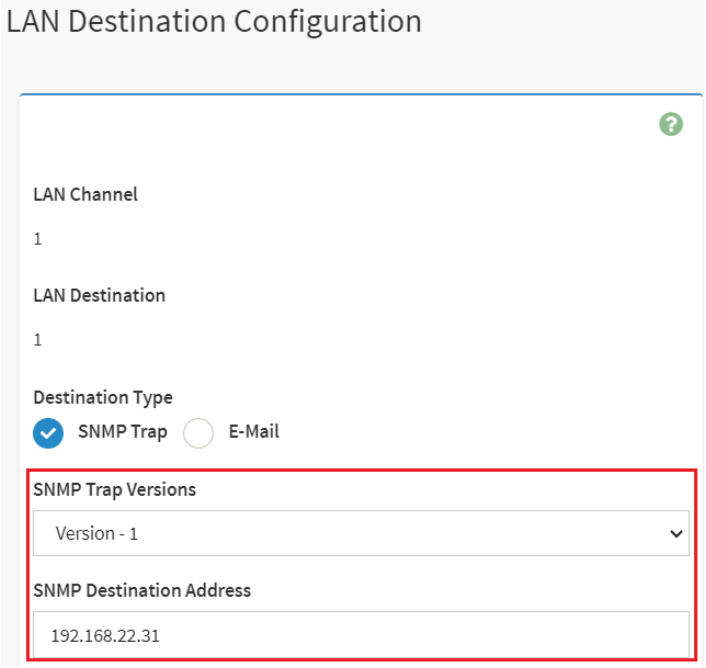
B. Click **"LAN Destination 1"**



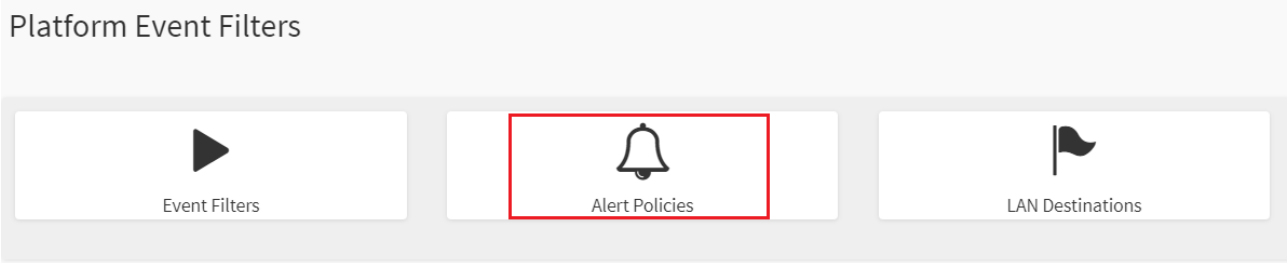
C. Select SNMP trap version from the dropdown menu in the "**SNMP Trap Versions**" field

=> Enter the IP address of the SNMP Manager in the "**SNMP Destination Address**" field. (Example using 192.168.22.31)

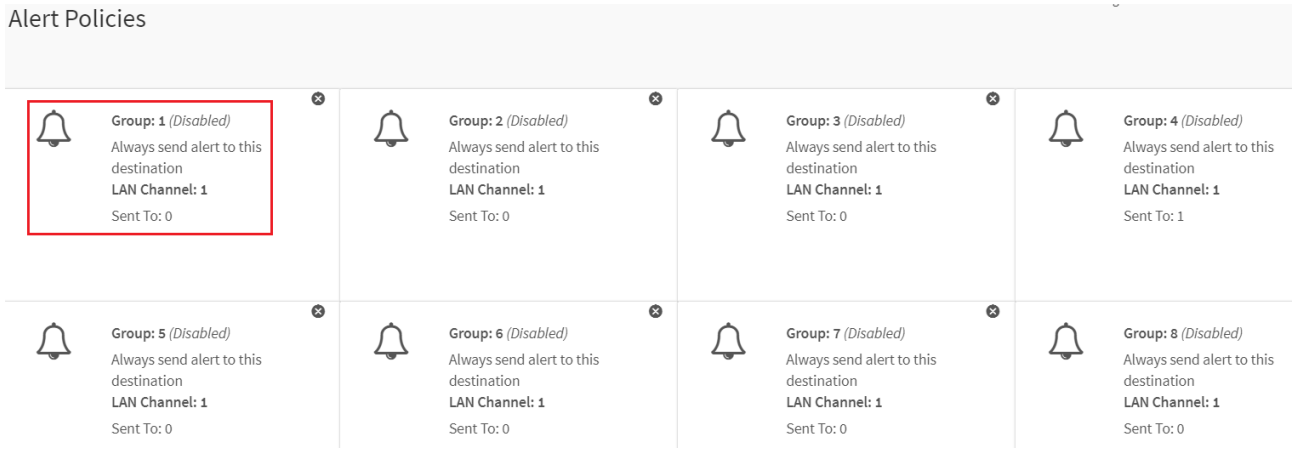
=> Click "**Save**" at the bottom.



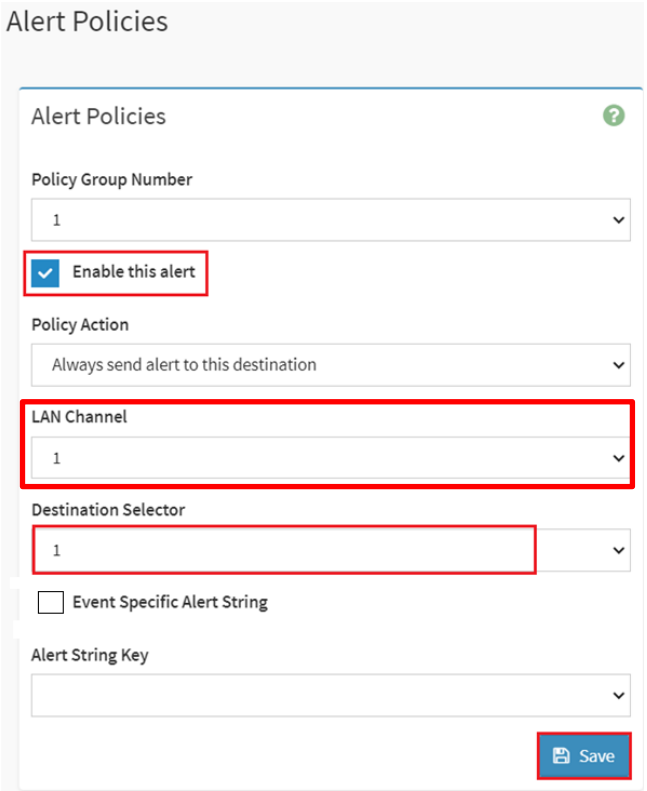
D. Click "**Settings**" => "**Platform Event Filters**" => "**Alert Policies**"



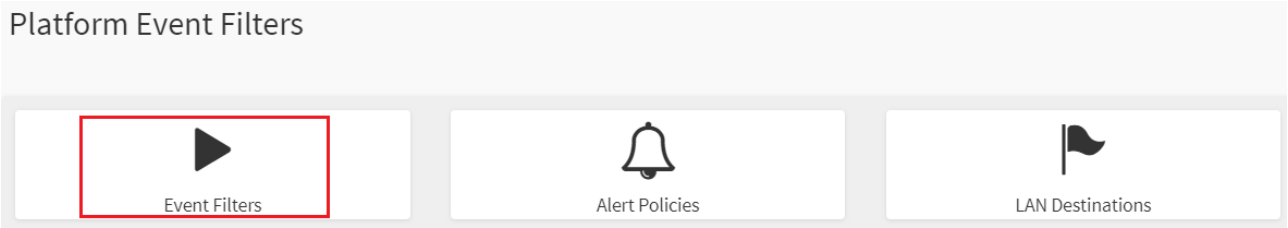
E. Click "**Group 1**"



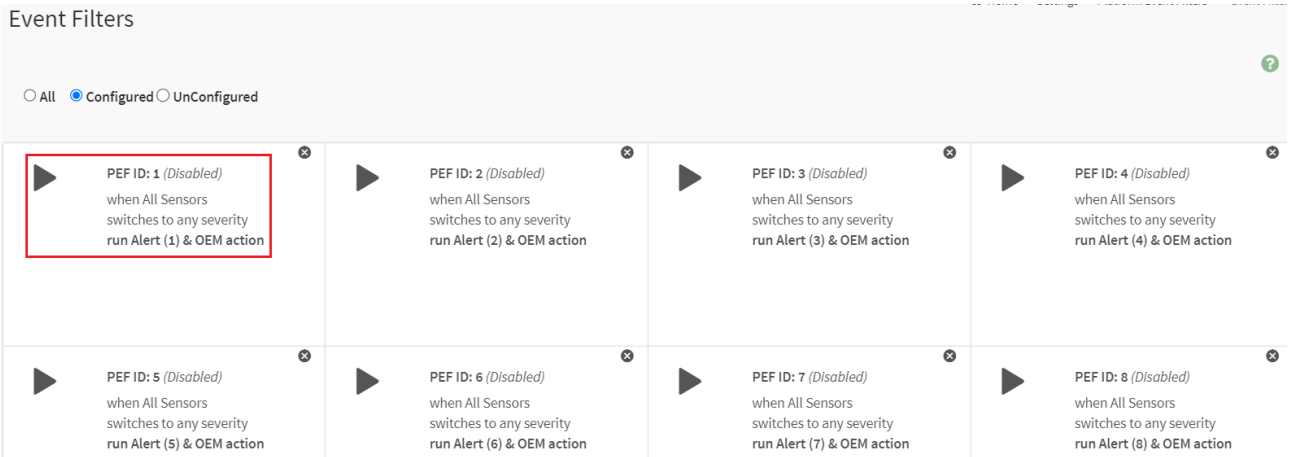
F. Check “**Enable this alert**” => “**Destination Selector**” select 1 => Click “**Save**” at the bottom.



G. Click “**Settings**” => “**Platform Event Filters**” => “**Event Filters**”

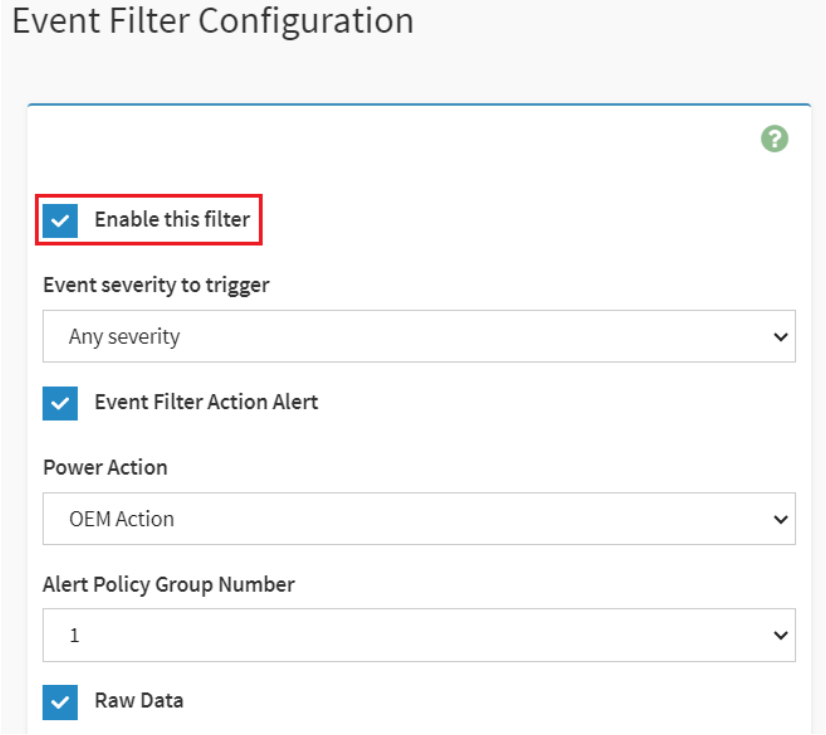


H. Click “**PEF ID 1**”



I. Check “**Enable this filter**” => Click “**Save**” at the bottom.

PS: It will send all SEL log events to the SNMP manager. You can choose to filter events through the options on this page.



Chapter 8. SNMP Command & Trap Testing - Example

Use the iReasoning MIB browser as the SNMP Manager for demonstration.

- https://ireasoning.com/mibbrowser.shtml
- Using Professional Edition for SNMP v3 (30 days Trial)

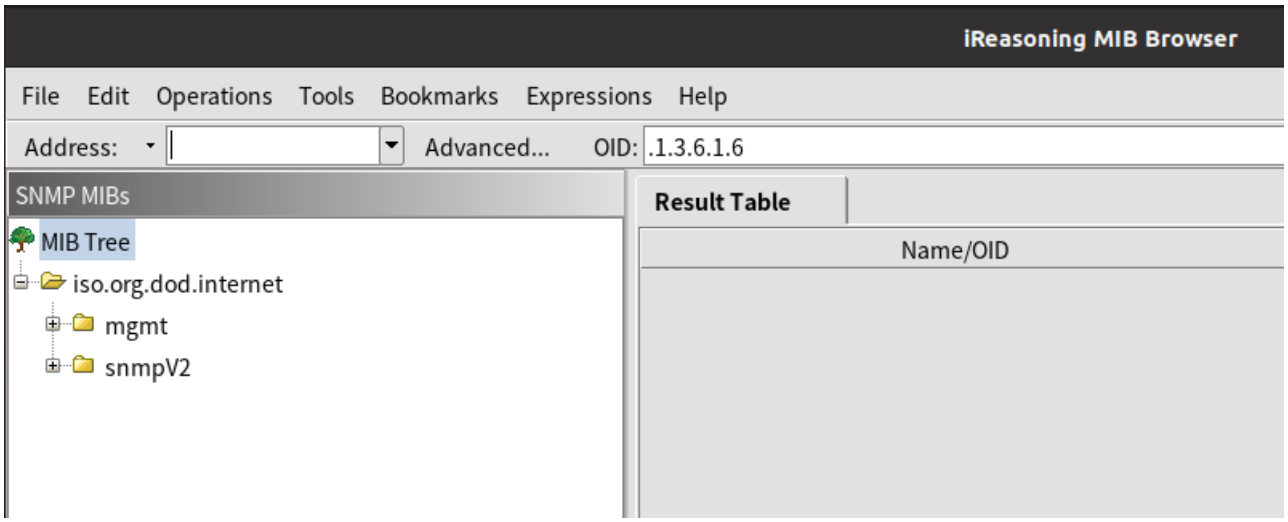
Information for the following example:

- IP address for SNMP Agent: **192.168.22.30**
- IP address for SNMP Manager: **192.168.22.31**
- SNMP read-only Community: **rocommstr**
- Username/password for BMC user account: **aic_test1** / **aic_test1_pw**
- Authentication: **SHA-256**
- Privacy: **DES**

8.1 SNMP Command & Trap Settings in SNMP Manager

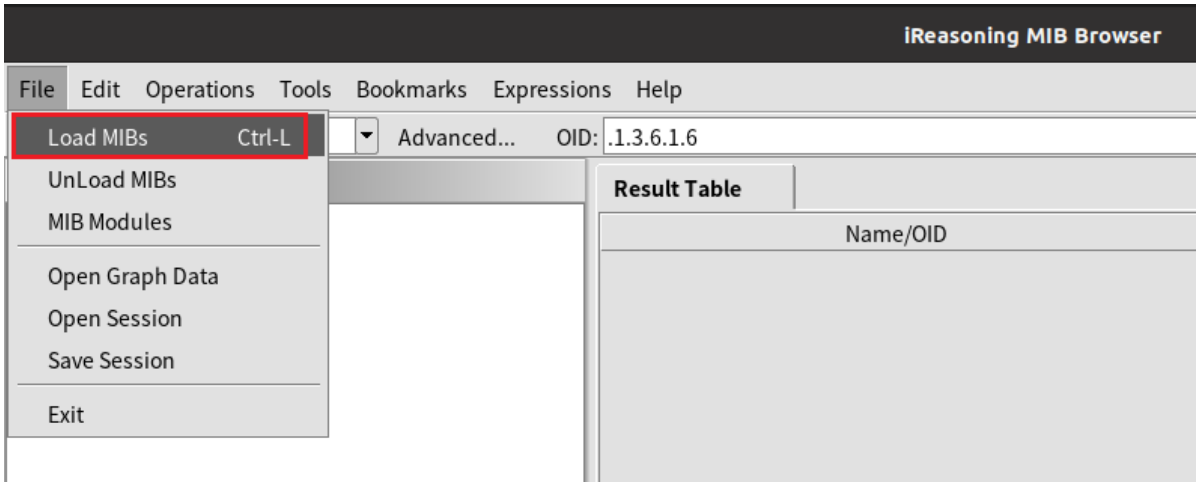
8.1.1 Load AIC SNMP Command MIB and AIC SNMP Trap MIB file

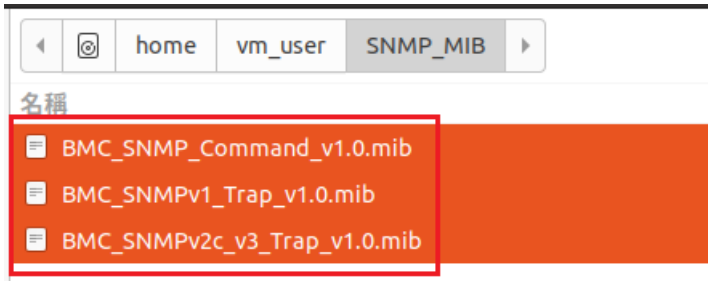
A. iReasoning MIB browser home screen



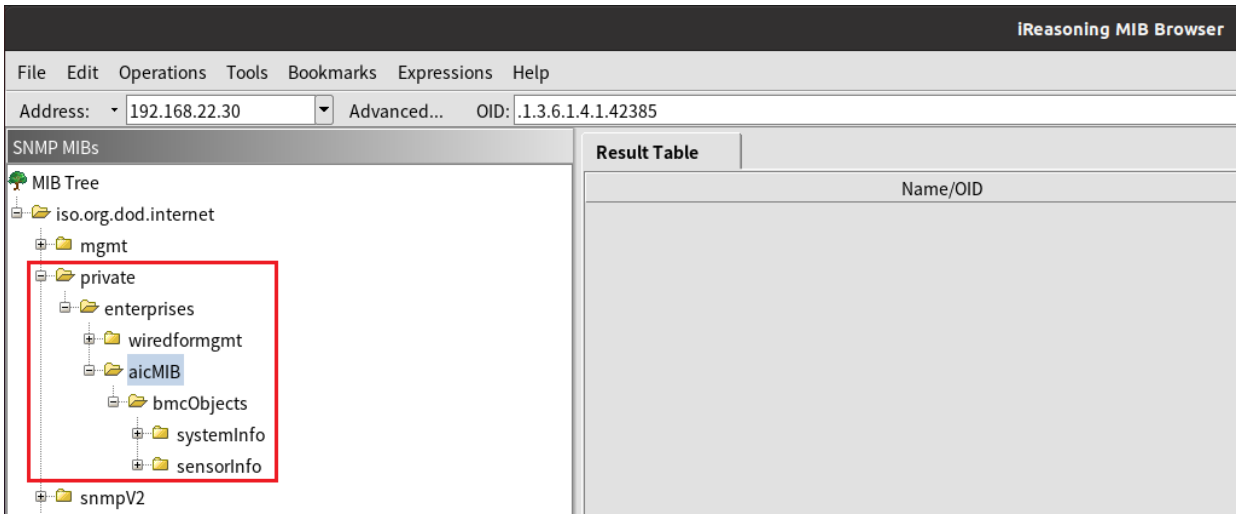
B. Load MIBs: Select AIC SNMP Command MIB and AIC SNMP Trap MIB file.

- Click “**File**” => “**Load MIBs**”





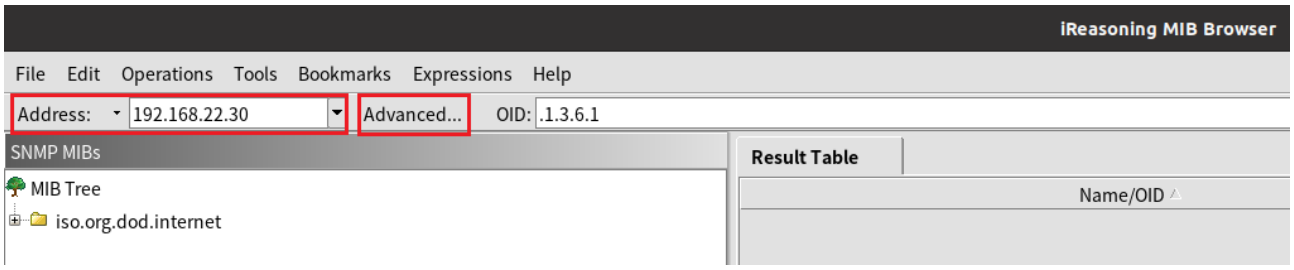
C. Automatically add **aicMIB** objects after loading the AIC SNMP Command MIB.



8.1.2 SNMP Command Parameter Setting

A. Launch the **Advanced Properties of SNMP Agent**

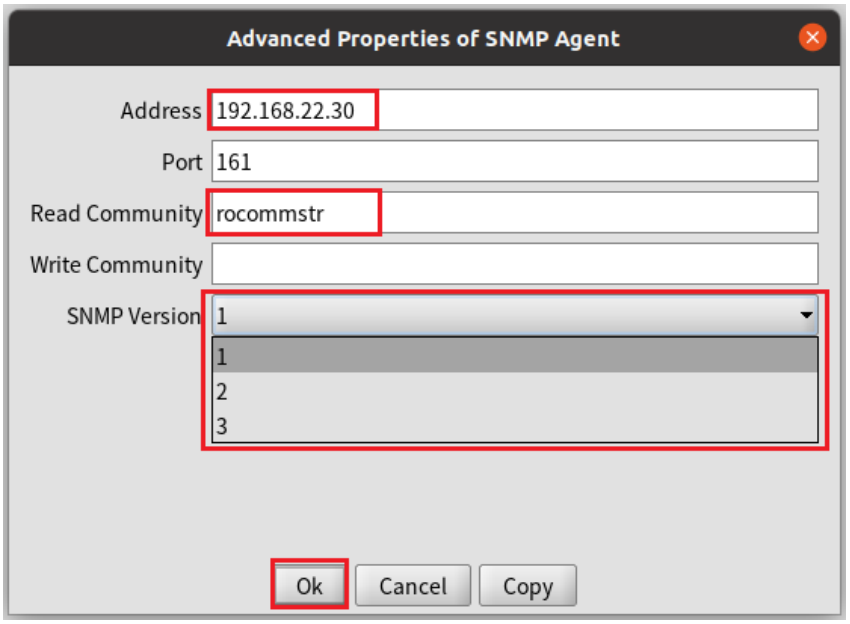
- Enter the IP address of the SNMP Agent in the "**Address:**" field.
- Click "**Advanced…**"



B. For **SNMP v1** setting:

- **SNMP Version**: Select **1**
- **Address**: Enter IP address of SNMP Agent
- **Read Community**: Set Read Community String

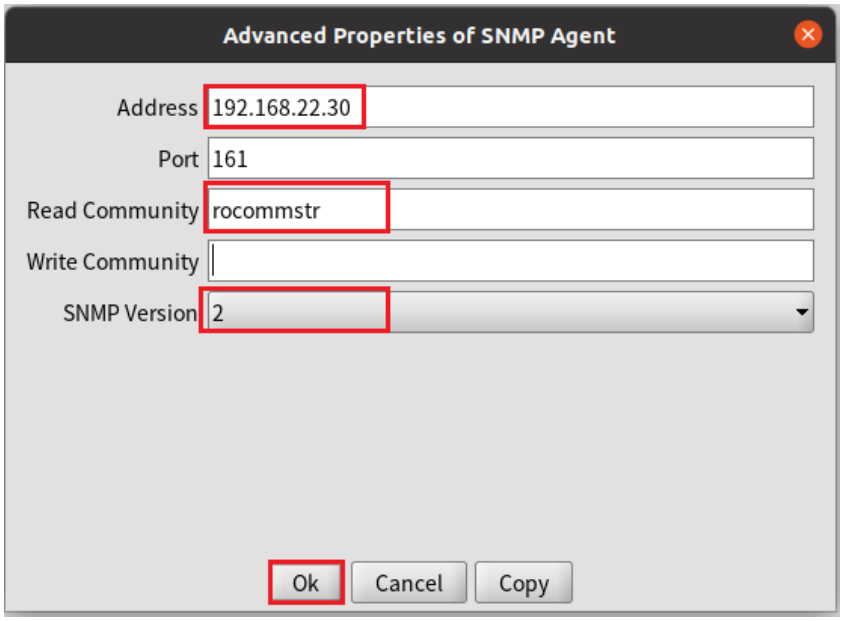
=> Click "**OK**" at the bottom



C. For **SNMP v2c** setting:

- **SNMP Version**: Select **2**
- **Address**: Enter IP address of SNMP Agent
- **Read Community**: Set Read Community String

=> Click "**OK**" at the bottom

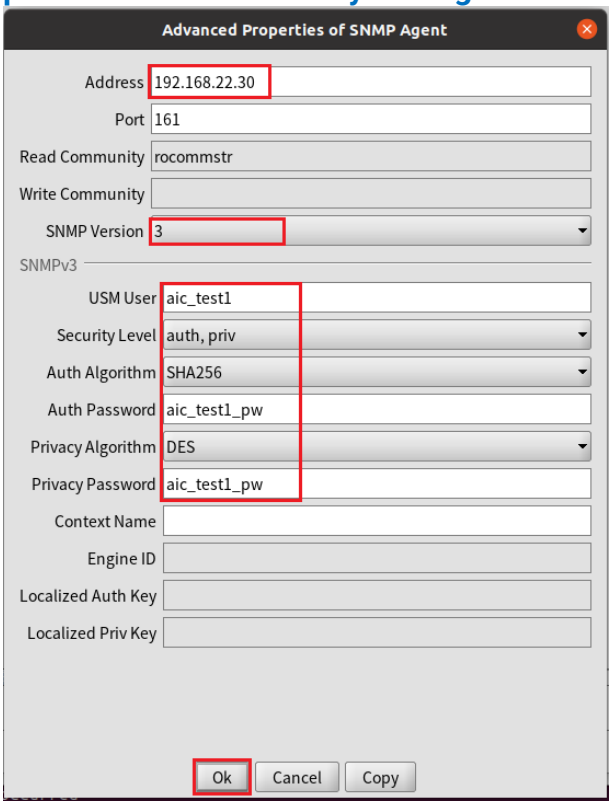


D. For **SNMP v3** setting:

- **SNMP Version**: Select **3**
- **Address**: Enter IP address of SNMP Agent
- **USM User**: Enter BMC user account name
- **Auth Password**: Enter BMC user account password
- **Privacy Password**: Enter BMC user account password
- **Security Level**: Select “auth, priv”
- **Auth Algorithm**: Select “SHA256”
- **Privacy Algorithm**: Select “DES”

=> Click “OK” at the bottom

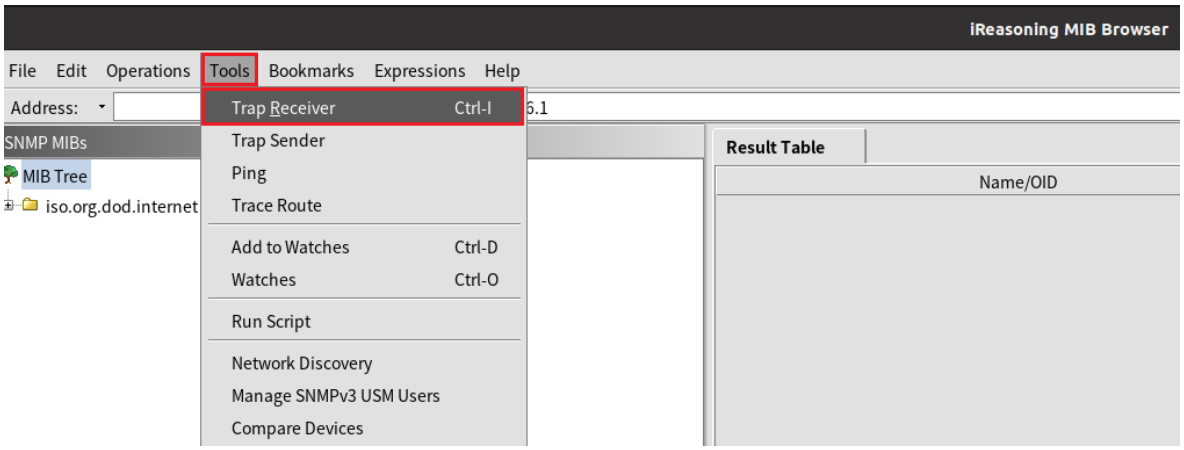
PS: Before configuring these values, you need to refer to "**7.1 Add SNMP access permissions and security settings for user**" to set up the BMC user account.

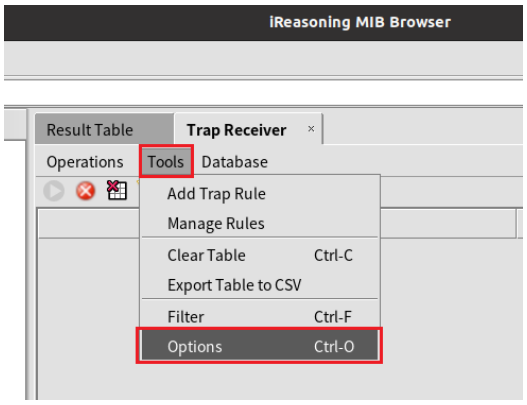


8.1.3 SNMP Trap Parameter Setting

A. Launch the **Trap Receiver Settings**

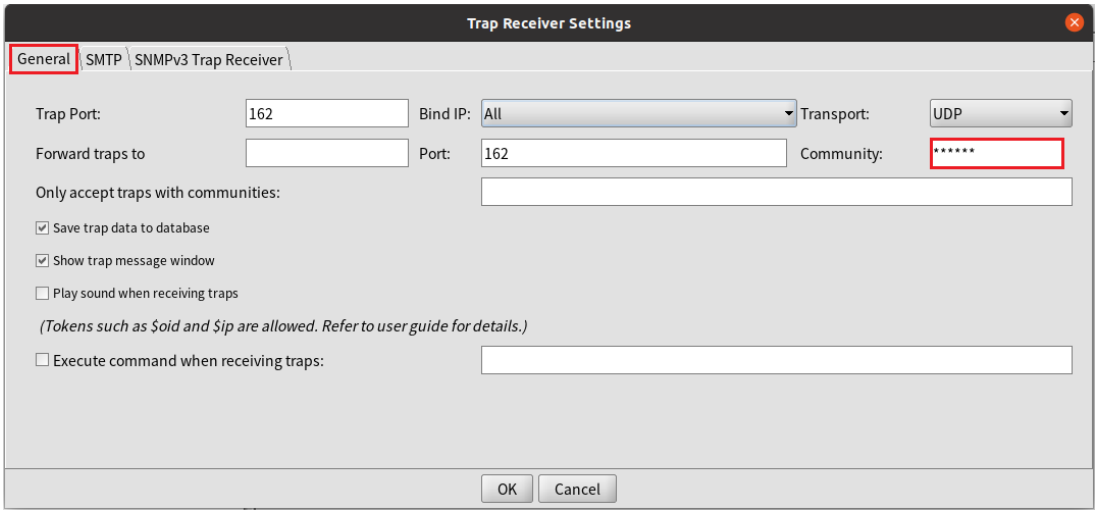
- Click "**Tools**" => "**Trap Receiver**"
- Click "**Tools**" in "**Trap Receiver**" page => "**Options**"





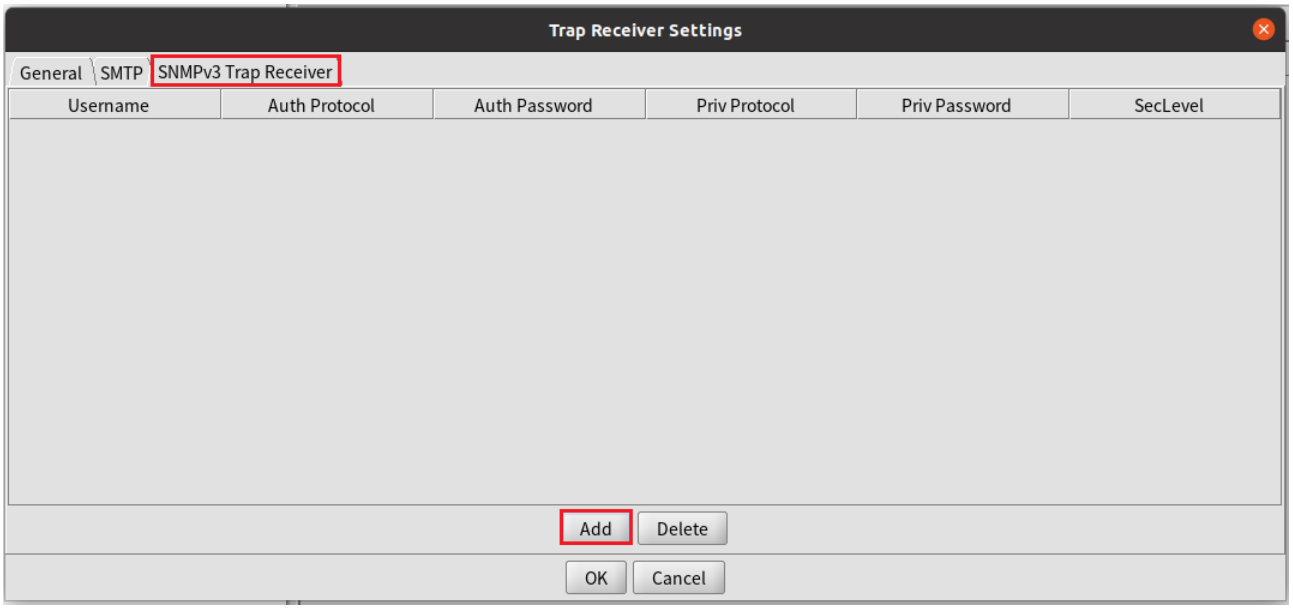
B. **For SNMP v1/v2c setting**

- **Community**: Set read community string



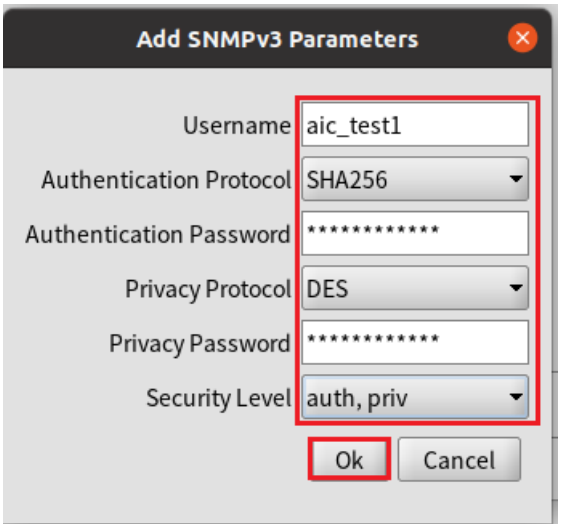
C. For SNMP v3 setting

- Click "**SNMPv3 Trap Receiver**" page => "**Add**"



- Add SNMPv3 Parameters:
  - **Username**: Enter BMC user account name
  - **Authentication Password**: Enter BMC user account password
  - **Privacy Password**: Enter BMC user account password
  - **Security Level**: Select "auth, priv"
  - **Authentication Protocol**: Select "SHA256"
  - **Privacy Protocol**: Select "DES"

  => Click "**OK**" at the bottom



8.2 SNMP Command Testing

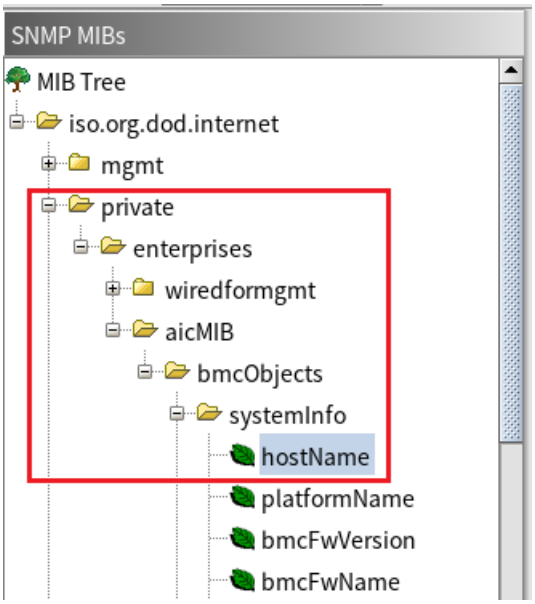
Before testing, refer to "**7.1 Add SNMP access permissions and security settings for user**" for configuration.

A. For SNMP Command v1, v2c, and v3, the corresponding SNMP version needs to be set in the iReasoning MIB Browser. Refer to "**8.1.2 SNMP Command Parameter Setting**" for details.

B. Get host name of BMC.

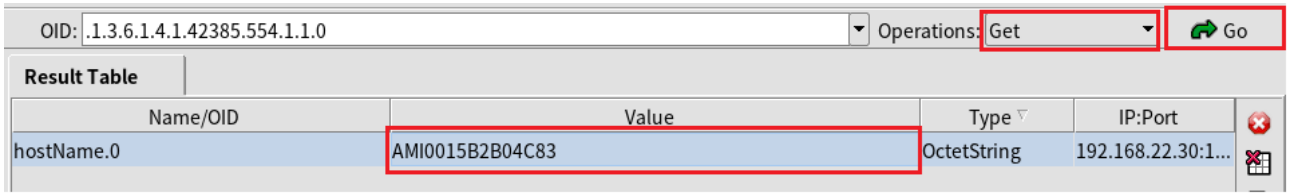
   a. In SNMP MIBs, expand private => enterprises => aicMIB => bmcObjects => systemInfo

      => Click **hostName**



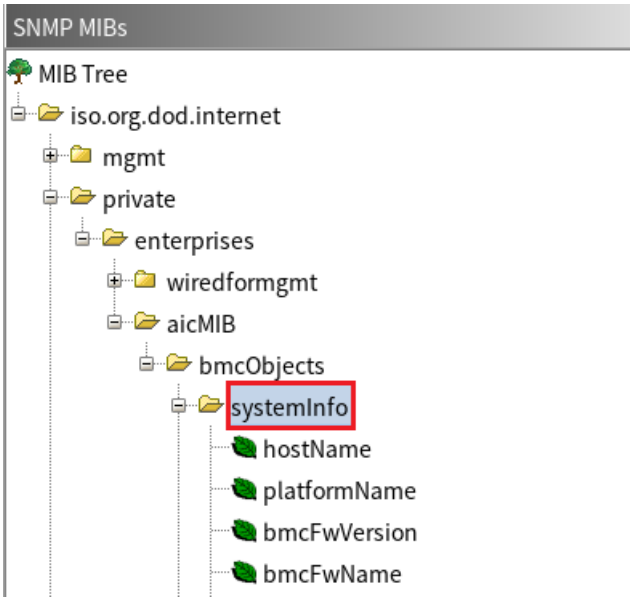
   b. Select "**Get**" in the "**Operations**" field => Click "**GO**".

      - Then the contents of **hostName** will be displayed in the "**Value**" field.



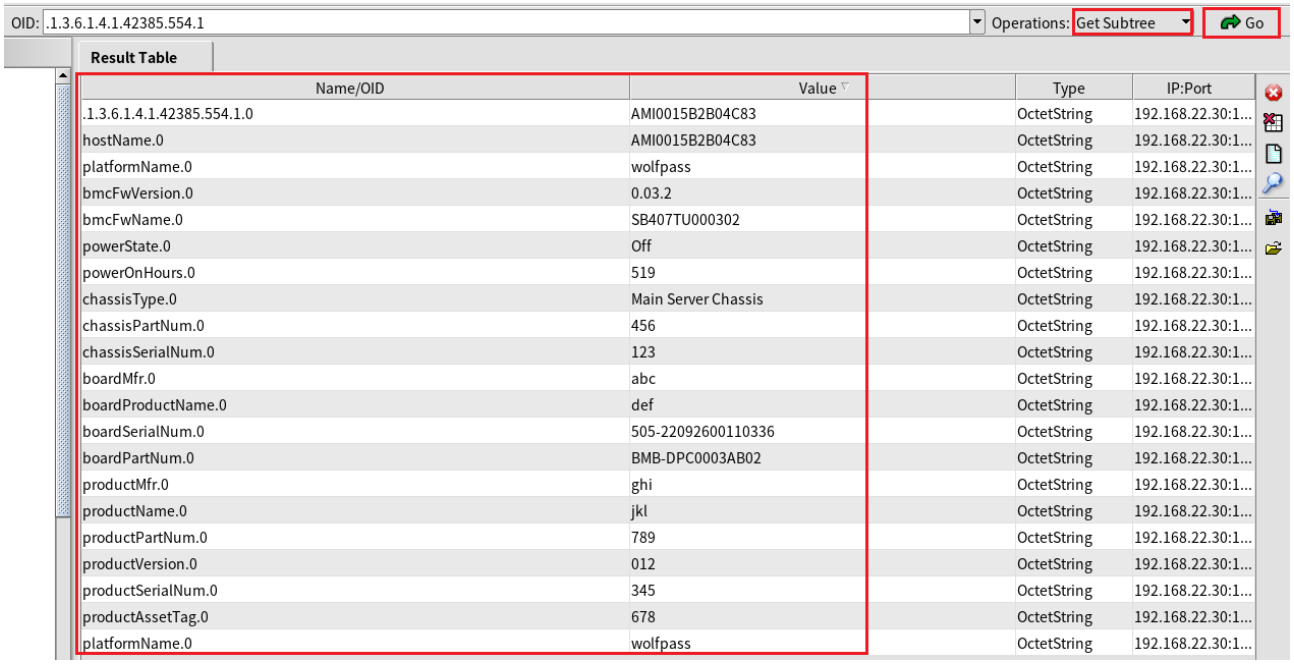
C. Get all contents of system information of BMC.

a. In SNMP MIBs, expand private => enterprises => aicMIB => bmcObjects => Click **systemInfo**



b. Select "**Get Subtree**" in the "**Operations**" field => Click "**GO**".

- Then the all contents of **systemInfo** will be displayed in the "**Value**" field.



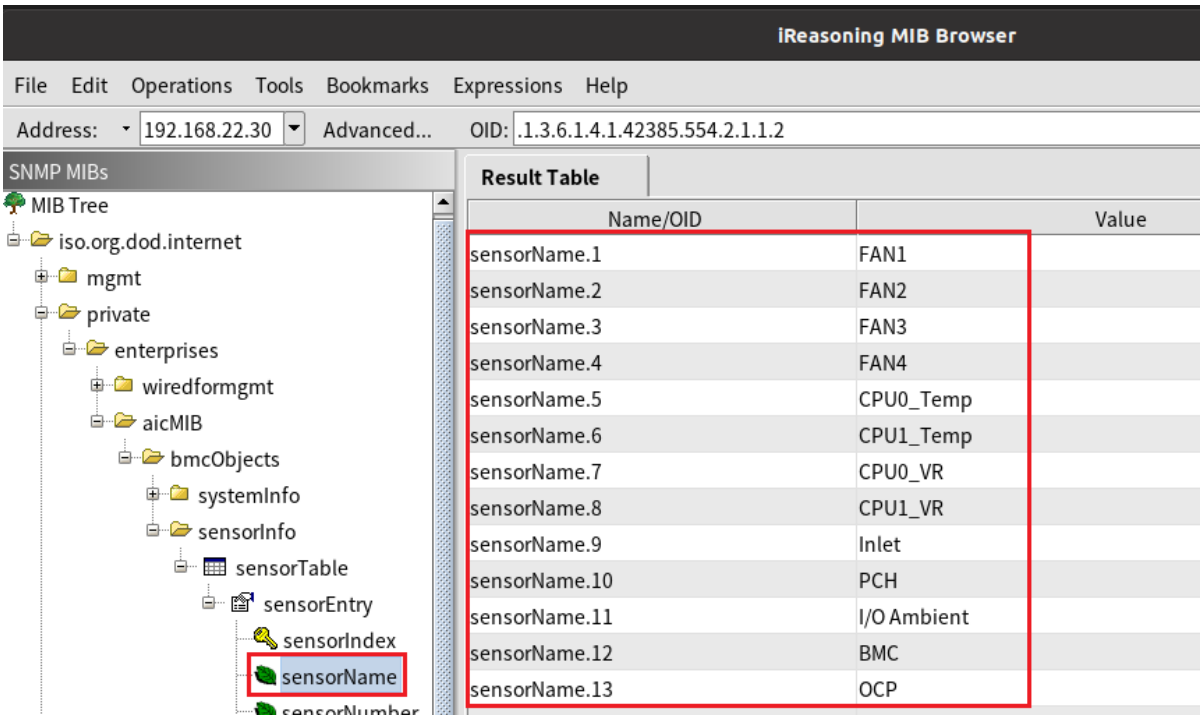
Name/OID	Value	Type	IP:Port
.1.3.6.1.4.1.42385.554.1.0	AMI0015B2B04C83	OctetString	192.168.22.30:1...
hostName.0	AMI0015B2B04C83	OctetString	192.168.22.30:1...
platformName.0	wolfpass	OctetString	192.168.22.30:1...
bmcFwVersion.0	0.03.2	OctetString	192.168.22.30:1...
bmcFwName.0	SB407TU000302	OctetString	192.168.22.30:1...
powerState.0	Off	OctetString	192.168.22.30:1...
powerOnHours.0	519	OctetString	192.168.22.30:1...
chassisType.0	Main Server Chassis	OctetString	192.168.22.30:1...
chassisPartNum.0	456	OctetString	192.168.22.30:1...
chassisSerialNum.0	123	OctetString	192.168.22.30:1...
boardMfr.0	abc	OctetString	192.168.22.30:1...
boardProductName.0	def	OctetString	192.168.22.30:1...
boardSerialNum.0	505-22092600110336	OctetString	192.168.22.30:1...
boardPartNum.0	BMB-DPC0003AB02	OctetString	192.168.22.30:1...
productMfr.0	ghi	OctetString	192.168.22.30:1...
productName.0	jkl	OctetString	192.168.22.30:1...
productPartNum.0	789	OctetString	192.168.22.30:1...
productVersion.0	012	OctetString	192.168.22.30:1...
productSerialNum.0	345	OctetString	192.168.22.30:1...
productAssetTag.0	678	OctetString	192.168.22.30:1...
platformName.0	wolfpass	OctetString	192.168.22.30:1...

D. Get sensor name of the sensor device.

a. In SNMP MIBs, expand private => enterprises => aicMIB => bmcObjects => sensorInfo => sensorTable => sensorEntry

=> Quickly press "**sensorName**" twice.

- Then the contents of **sensorName** will be displayed in the "**Value**" field.



8.3 SNMP Trap Testing

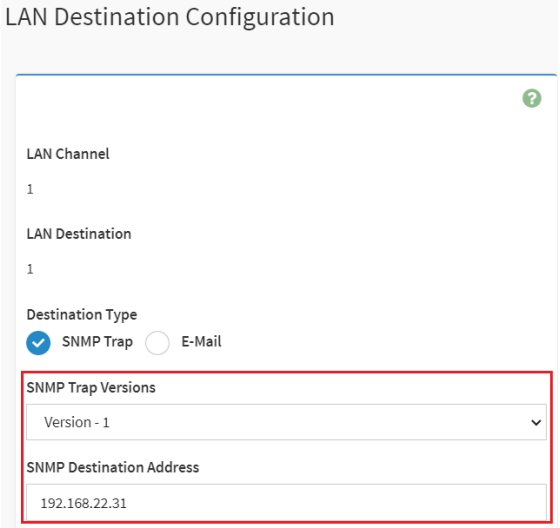
Before testing, refer to "**7.1 Add SNMP access permissions and security settings for user**" and "**7.4 SNMP Trap Settings**" and "**8.1 SNMP Command & Trap Settings in SNMP Manager**" for configuration.

NOTE

1. During testing, turn off your network firewall or configure the network firewall not to block the port used by SNMP.
2. Due to the use of UDP transport, the SNMP manager may have a low probability of losing packets.

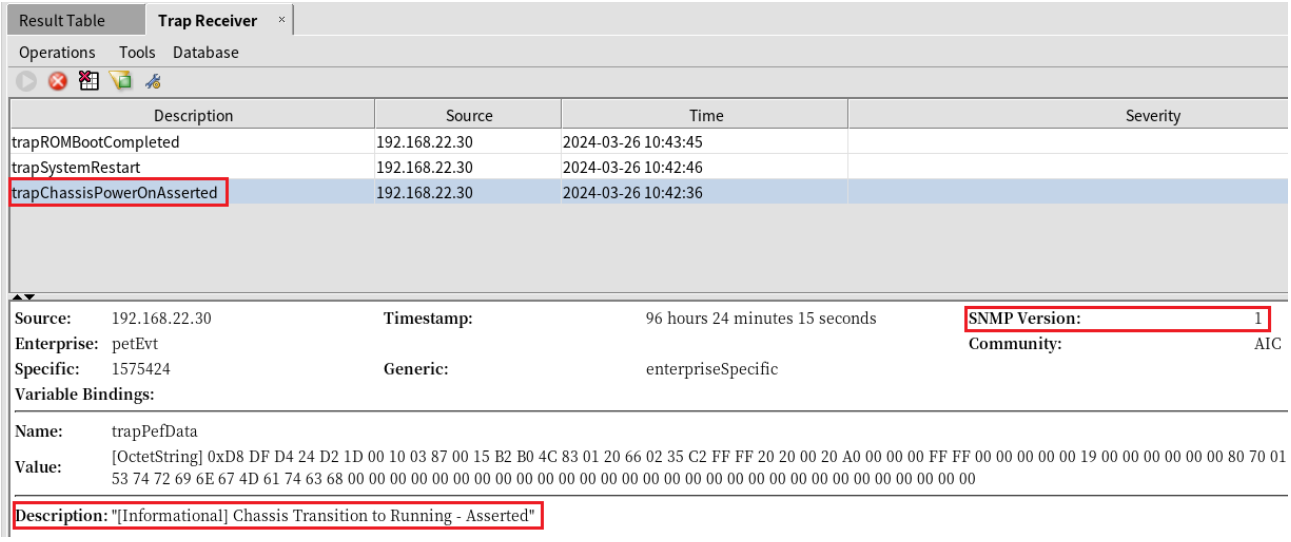
8.3.1 SNMP Trap v1

A. Configure "**SNMP Trap v1**" and "**SNMP Manager's IP address**" in the BMC GUI. Refer to "**7.4 SNMP Trap Settings**".



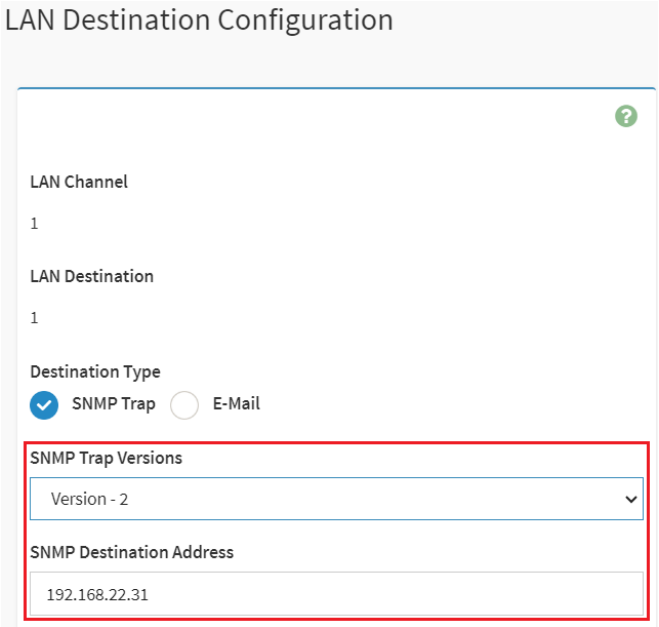
B. Power on the AIC device, wait 2 minutes.

C. See the following event log in "**Trap Receiver**" window of iReasoning MIB Browser.



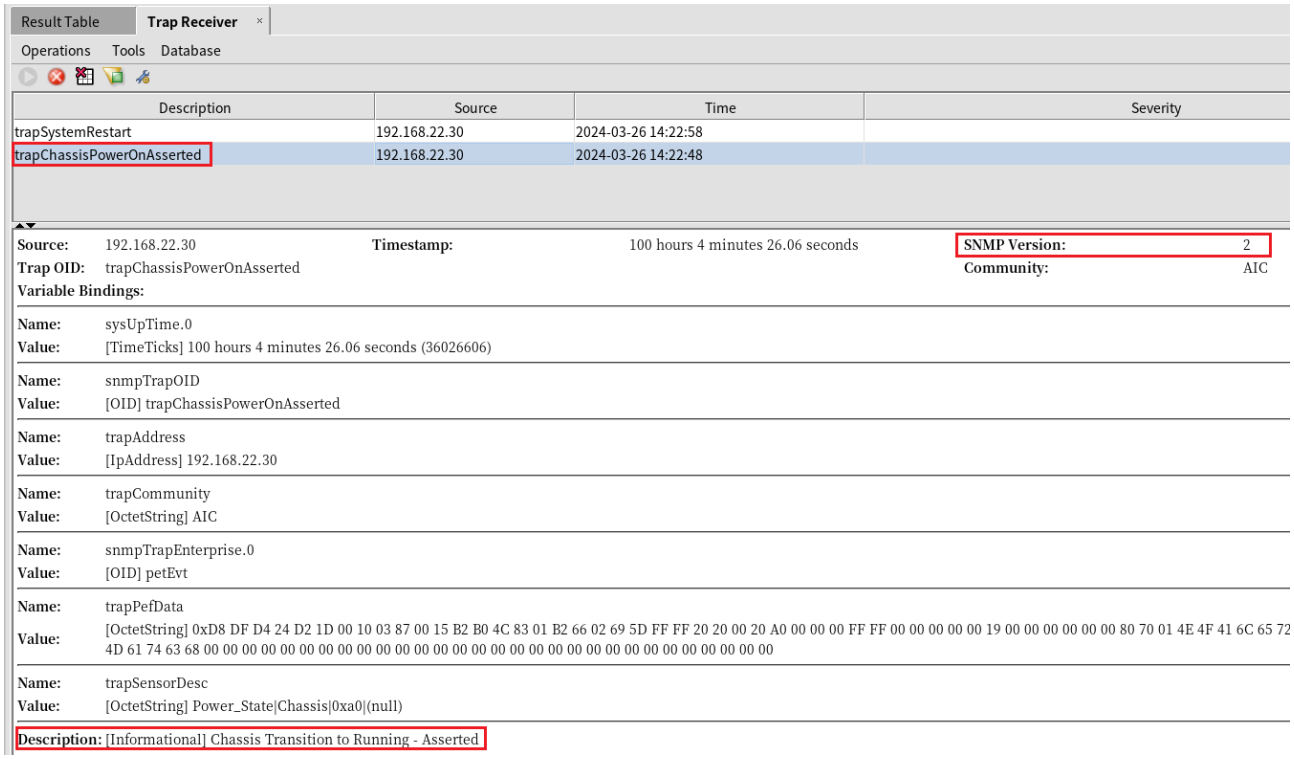
8.3.2 SNMP Trap v2c

A. Configure “**SNMP Trap v2**” and “**SNMP Manager's IP address**” in the BMC GUI. Refer to "**7.4 SNMP Trap Settings**".



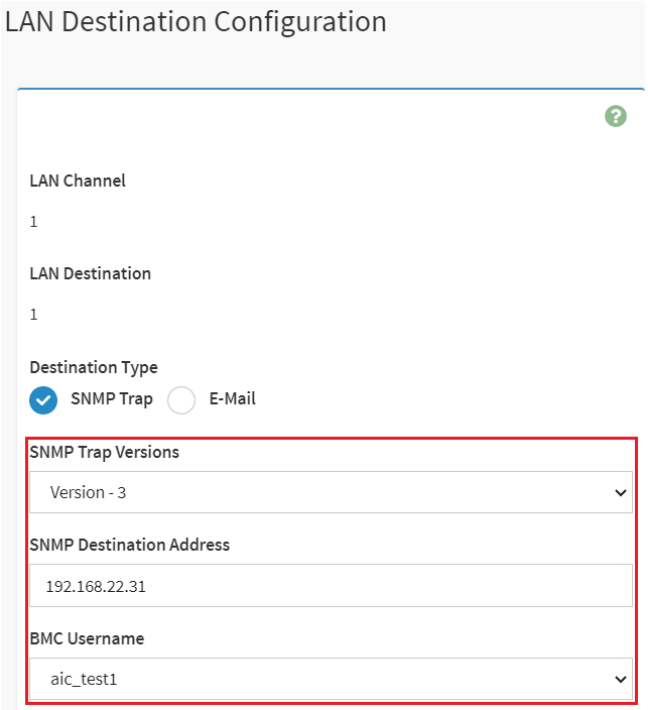
B. Power on the AIC device, wait 2 minutes.

C. See the following event log in “**Trap Receiver**” window of iReasoning MIB Browser.



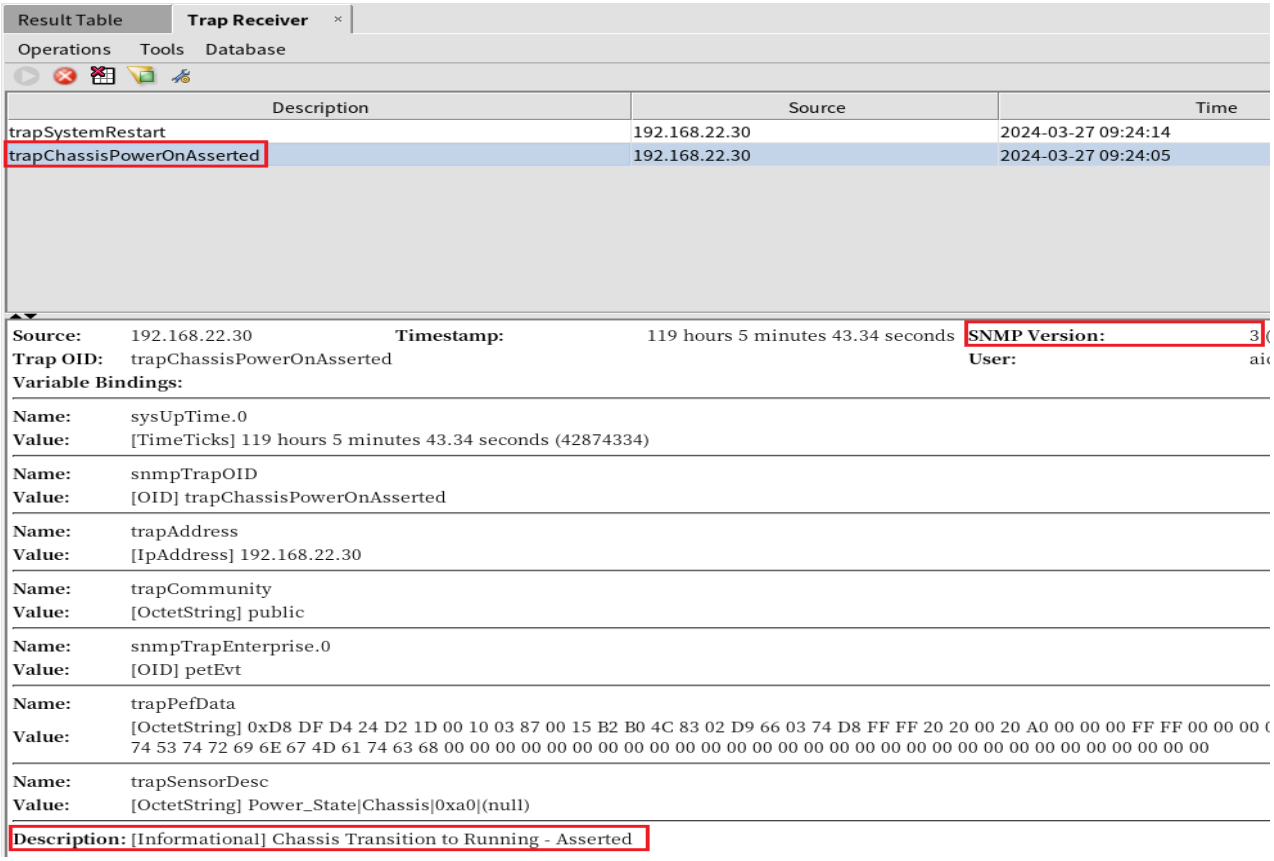
8.3.3 SNMP Trap v3

A. Configure “**SNMP Trap v3**” and “**SNMP Manager's IP address**” and “BMC Username” in the BMC GUI. Refer to "**7.4 SNMP Trap Settings**".



B. Power on the AIC device, wait 2 minutes.

C. See the following event log in “**Trap Receiver**” window of iReasoning MIB Browser.



Chapter 9. Technical Support

www.aicipc.com

Taiwan, Global Headquarters

Address: No. 152, Section 4, Linghang N. Rd, Dayuan District, Taoyuan City 337, Taiwan
Tel: +886-3-433-9188
Fax: +886-3-287-1818
Sales Email: sales@aicipc.com.tw
Support Email: support@aicipc.com

Shanghai, China

Address: Room 215, Building 4, No.471 Guiping Road, Xuhui District, Shanghai City, 200233 China
Tel: +86-21-54961421
Sales Email: sales@aicipc.com.cn
Support Email: support@aicipc.com

Moscow, Russia

Address: No. 500, 5th Floor, 5th Entrance, 32A, Khoroshevskoye Shosse, Moscow, 123007
Tel: +7-4997019998
Sales Email: support-ru@aicipc.com.tw
Support Email: rma.russia@aicipc.com.tw

North California, United States

Address: 48531 Warm Springs Boulvard Suite 404 Fremont, CA 94539, United States Tel: +1-510-573-6730
Sales Email: sales@aicipc.com
Support Email: support@aicipc.com

South California, United States

Address: 21808 Garcia Lane City of Industry, CA 91789, United States
Toll free: + 1-866-800-0056
Tel: +1-909-895-8989
Fax: +1-909-895-8999
Sales Email: sales@aicipc.com
Support Email: support@aicipc.com

New Jersey, United States

Address: 322 Route 46 West Suite 100 Parsippany, NJ 07054 United States
Tel: +1-973-884-8886
Fax: +1-973-884-4794
Sales Email: sales@aicipc.com
Support Email: support@aicipc.com

Houten, The Netherlands

Address: Peppelkade 58, 3992AK, Houten, The Netherlands
Tel: +31-30-6386789
Fax: +31-30-6360638
Sales Email: sales@aicipc.nl
Support Email: support@aicipc.com

For additional technical support or questions about trouble shooting, please contact the AIC® representative nearest to you or visit our AIC® website for more information.
AIC® website: **https://www.aicipc.com/en/faq**.