

# Technical Document

## **Snmp V3 Driver Guide**

**April 4, 2022**



# **Snmp V3 Driver Guide**

## **Tridium, Inc.**

3951 Westerre Parkway, Suite 350

Richmond, Virginia 23233

U.S.A.

## **Confidentiality**

The information contained in this document is confidential information of Tridium, Inc., a Delaware corporation ("Tridium"). Such information and the software described herein, is furnished under a license agreement and may be used only in accordance with that agreement.

The information contained in this document is provided solely for use by Tridium employees, licensees, and system owners; and, except as permitted under the below copyright notice, is not to be released to, or reproduced for, anyone else.

While every effort has been made to assure the accuracy of this document, Tridium is not responsible for damages of any kind, including without limitation consequential damages, arising from the application of the information contained herein. Information and specifications published here are current as of the date of this publication and are subject to change without notice. The latest product specifications can be found by contacting our corporate headquarters, Richmond, Virginia.

## **Trademark notice**

BACnet and ASHRAE are registered trademarks of American Society of Heating, Refrigerating and Air-Conditioning Engineers. Microsoft, Excel, Internet Explorer, Windows, Windows Vista, Windows Server, and SQL Server are registered trademarks of Microsoft Corporation. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Mozilla and Firefox are trademarks of the Mozilla Foundation. Echelon, LON, LonMark, LonTalk, and LonWorks are registered trademarks of Echelon Corporation. Tridium, JACE, Niagara Framework, and Sedona Framework are registered trademarks, and Workbench are trademarks of Tridium Inc. All other product names and services mentioned in this publication that are known to be trademarks, registered trademarks, or service marks are the property of their respective owners.

## **Copyright and patent notice**

This document may be copied by parties who are authorized to distribute Tridium products in connection with distribution of those products, subject to the contracts that authorize such distribution. It may not otherwise, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written consent from Tridium, Inc.

Copyright © 2022 Tridium, Inc. All rights reserved.

The product(s) described herein may be covered by one or more U.S. or foreign patents of Tridium.

# Contents

<b>About this guide .....</b>	<b>5</b>
Document change log .....	5
Related documentation .....	5
<b>Chapter 1 Introduction .....</b>	<b>7</b>
SNMPv3 Features.....	7
Prerequisites .....	7
<b>Chapter 2 Agent Configuration .....</b>	<b>9</b>
Adding an SnmpNetwork .....	9
Setting up an Snmp Agent application .....	10
<b>Chapter 3 Security and VACM Configuration.....</b>	<b>13</b>
Creating a UsmUserTable .....	13
VacmContextTable.....	15
VacmGroupTable .....	16
VacmViewTreeTable .....	17
VacmAccessTable.....	18
<b>Chapter 4 Manager Configuration .....</b>	<b>21</b>
Setting up an Snmp manager application.....	21
Configuring the SnmpDevice (Manager) .....	22
<b>Chapter 5 Snmp Plugins.....</b>	<b>25</b>
Snmp Agent Point Manager .....	25
Snmp Device Manager.....	26
Snmp Export Manager.....	28
Snmp Object Manager.....	29
Snmp Point Manager .....	30
Snmp Table Manager .....	31
Snmp Trap Manager .....	32
Usm User Manager View.....	33
Vacm Access Manager View .....	34
Vacm Context Manager View .....	34
Vacm Group Manager View.....	35
Vacm View Tree Manager View .....	36
<b>Chapter 6 Snmp Components .....</b>	<b>39</b>
SnmpNetwork.....	39
SnmpDevice.....	43
Snmp Alarm Device Ext .....	44
Snmp Point Folder.....	46
Snmp Point Device Ext .....	46
Snmp Agent.....	46
Snmp Agent Point Folder .....	46
Snmp Agent Point Device Ext .....	46
Snmp Agent Boolean Proxy Ext .....	47

Snmp Agent Numeric Proxy Ext.....	49
Snmp Agent String Proxy Ext.....	51
Snmp Export Folder .....	53
Snmp Export Table.....	54
Snmp Enum Export .....	54
Snmp Numeric Export .....	55
Snmp Boolean Export.....	55
Snmp Boolean Proxy Ext.....	56
Snmp String Export .....	58
MIB List Table .....	59
Snmp Boolean Object Ext.....	59
Snmp Numeric Object Ext .....	61
Snmp String Object Ext .....	63
Snmp Enum Object Ext.....	65
Usm User table.....	67
Vacm Context .....	69
Vacm Access .....	69
Vacm View Tree.....	70
Vacm Group.....	71
Snmp Device Folder .....	72
Snmp Object Device Ext.....	72
Snmp Boolean Proxy Ext.....	72
Snmp Enum Proxy Ext .....	74
Snmp String Proxy Ext .....	76
Snmp Numeric Proxy Ext .....	78
Snmp Sequence .....	80
Snmp Table.....	80
Snmp Table Row .....	80
N Poll Scheduler.....	81
Trap Table .....	81
snmp-TrapType .....	81
Snmp Recipient .....	82

## About this guide

This topic contains important information about the purpose, content, context, and intended audience for this document.

### Product Documentation

This document is part of the Niagara technical documentation library. Released versions of Niagara software include a complete collection of technical information that is provided in both online help and PDF format. The information in this document is written primarily for Systems Integrators. To make the most of the information in this book, readers should have some training or previous experience with Niagara software, as well as experience working with JACE network controllers.

### Document Content

This document provides information about the SNMPv3 Driver. For information about SNMPv1/v2, see *Snmp V1/V2 Driver Guide*.

This document describes how to include the SNMPv3 features in your SnmpNetwork. The target audience for this document is Systems Integrators.

**CAUTION:** Protect against unauthorized access by restricting physical access to the computers and devices that manage your building model. Set up user authentication with strong passwords, and secure components by controlling permissions. Failure to observe these recommended precautions could expose your network systems to unauthorized access and tampering.

## Document change log

Updates (changes/additions) to the document are listed below.

### April 4, 2022

Updated Components and Plugins Chapter.

### March 10, 2022

Removed MD5 Authentication Protocol reference in the chapter "New features in SNMPv3".

### October 25, 2019

In the topic, "About this guide", added a caution note alerting customers to restrict access to all computers, devices, field buses, components, etc., that manage their building model.

### June 8, 2017

New topics added (Usm User, Vacm Context, Vacm Access, Vacm View Tree, and Vacm Group).

### August 19, 2016

Initial release document.

## Related documentation

This topic lists documents that are related to this guide.

- Niagara Drivers Guide
- Snmp V1/V2 Driver Guide



# Chapter 1 Introduction

## Topics covered in this chapter

- ◆ SNMPv3 Features
- ◆ Prerequisites

These sections describes the major features of the Snmpv3 driver and list some prerequisites for setting up the driver.

## SNMPv3 Features

- These modules provide three levels of security as follows:
  - NoAuthNoPriv Defines communication without authentication and privacy. A User with security level **No Auth No Priv** and context name as noAuth is called noAuthUser.
  - AuthNoPriv Defines communication with authentication and without privacy. The protocol used for authentication is SHA (Secure Hash Algorithm). Users with security level **Auth No Priv** and context name as auth is called authUser.
  - AuthPriv. Defines communication with authentication and privacy. The protocol used for authentication purposes is SHA. The DES (Data Encryption Standard) and AES(Advanced Encryption Standard) protocols for privacy users. Users with security level **AuthPriv** and context name as priv is called privUser.
- The SHA Authentication Protocol supports authentication.
- The DES, Aes 128, Aes192 , and Aes256 Privacy Protocols supports the privacy.
- The UsmUserTable is a part of security.
- Four master Configuration Tables provide user security:  
View-based Access Control Model (VACM): The
  - VacmContextTable
  - VacmGroupTable
  - VacmViewTreeTable
  - VacmAccessTable.
- The AuthPriv exchange of messages is encrypted and decrypted so the MIB walk will take more time.

## Prerequisites

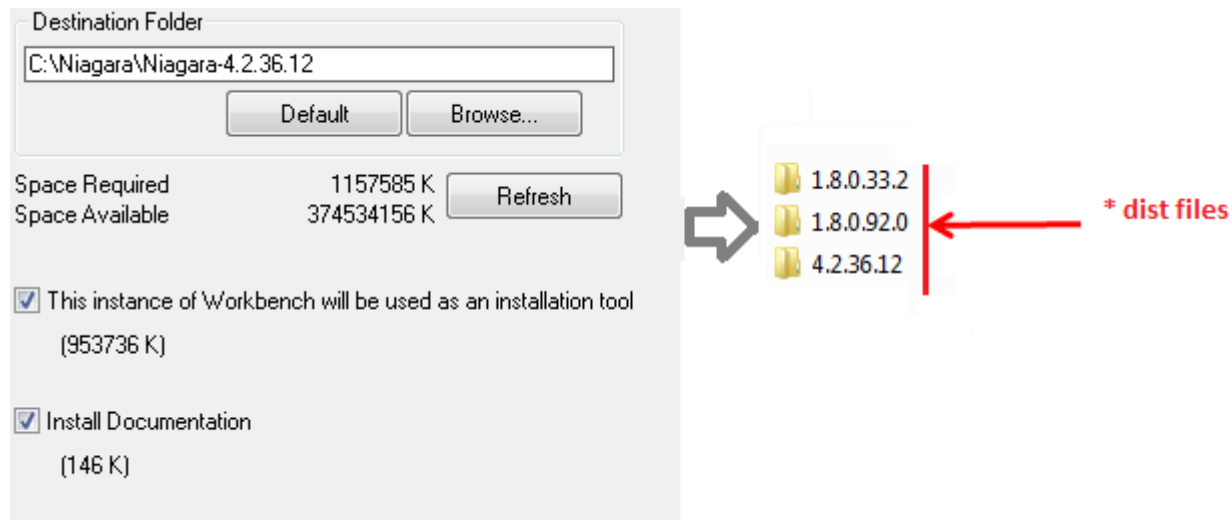
The following information describes what you need to do before installing the SNMPv3 driver.

### Licensing

You have a target controller host that is licensed with the Snmp feature. In addition, other Snmp device limits or proxy point limits may exist in your license.

### Workbench install tool option

From your Supervisor platform, Workbench must have been installed on your Supervisor platform with the "This instance of Workbench will be used as an installation tool" enabled as shown in the following screen capture.



This option installs the needed distribution files (.dist files) for commissioning various models of remote controller platforms. When installed, the dist files are located in your installation directory under a “sw” subdirectory. For details, see the *Niagara Platform Guide*.

### nSnmp module

You installed the nSnmp module plus any specific (private) MIB files and required MIB dependency files. Refer to the *Snmp V1/V2 Driver Guide*.

**NOTE:** All standard MIB files are included as part of the nSnmp module. The MIB files are used in discovering Snmp device data points.

Upgrade any modules shown as “out of date”. For instructions about updating your modules, see the *Niagara Platform Guide*.

The remote controller is now ready for Snmp Network configuration in a running station.



# Chapter 2 Agent Configuration

## Topics covered in this chapter

- ◆ Adding an SnmpNetwork
- ◆ Setting up an Snmp Agent application

This section describes the configuration of the SnmpNetwork in an Agent.

The remote controller is configured as an agent. To configure the SnmpNetwork, first add the SnmpNetwork and then design the SnmpNetwork application.

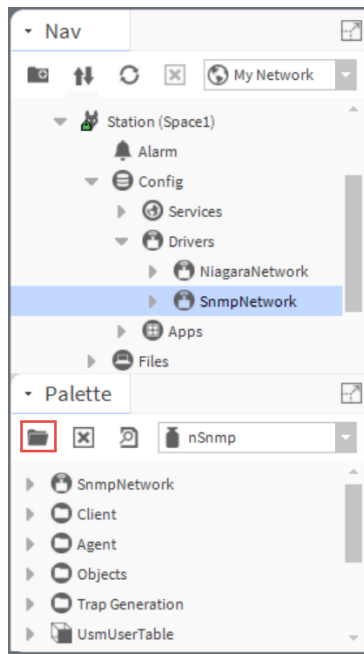
## Adding an SnmpNetwork

This procedure explains to add an **SnmpNetwork** component to a remote controller **SNMP\_AGENT** station.

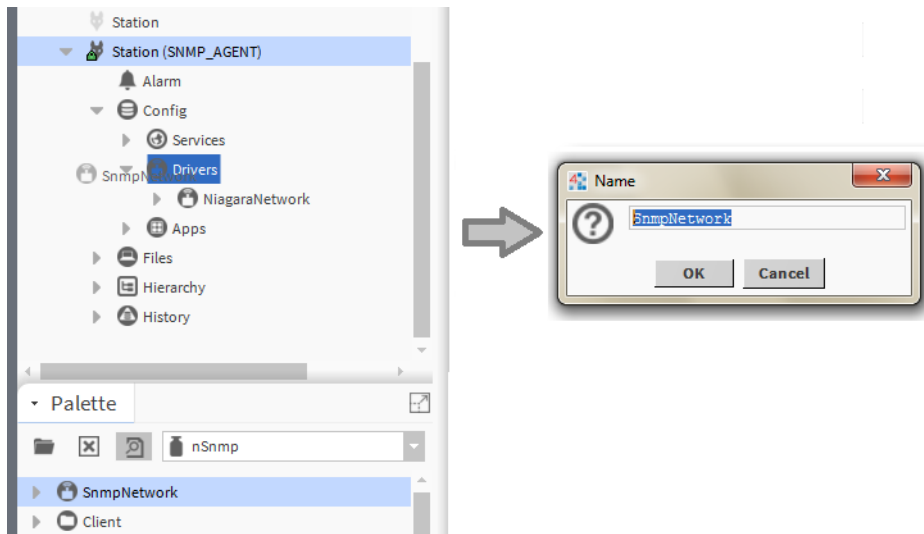
When you add an **SnmpNetwork** to a station, a **Local Device** (  ) component comes with the **SnmpNetwork** component.

Step 1 Open the **nSnmp** palette.

The palette opens.



Step 2 Copy-and-paste (or drag ) **SnmpNetwork** component to the **Drivers** node in the station Nav tree.



The **Name** window opens.

- Step 3** Type a name in the **Name** property (or accept the default name) and click **OK**.

The **SnmpNetwork** appears in the **Driver Manager** view with the name that you assigned. The **Status** should report `{ok}` and **Enabled** property should report `true`. The **SnmpNetwork** node should also appear under your **Drivers** node in the **Nav** tree.

- Step 4** Save and restart the station.

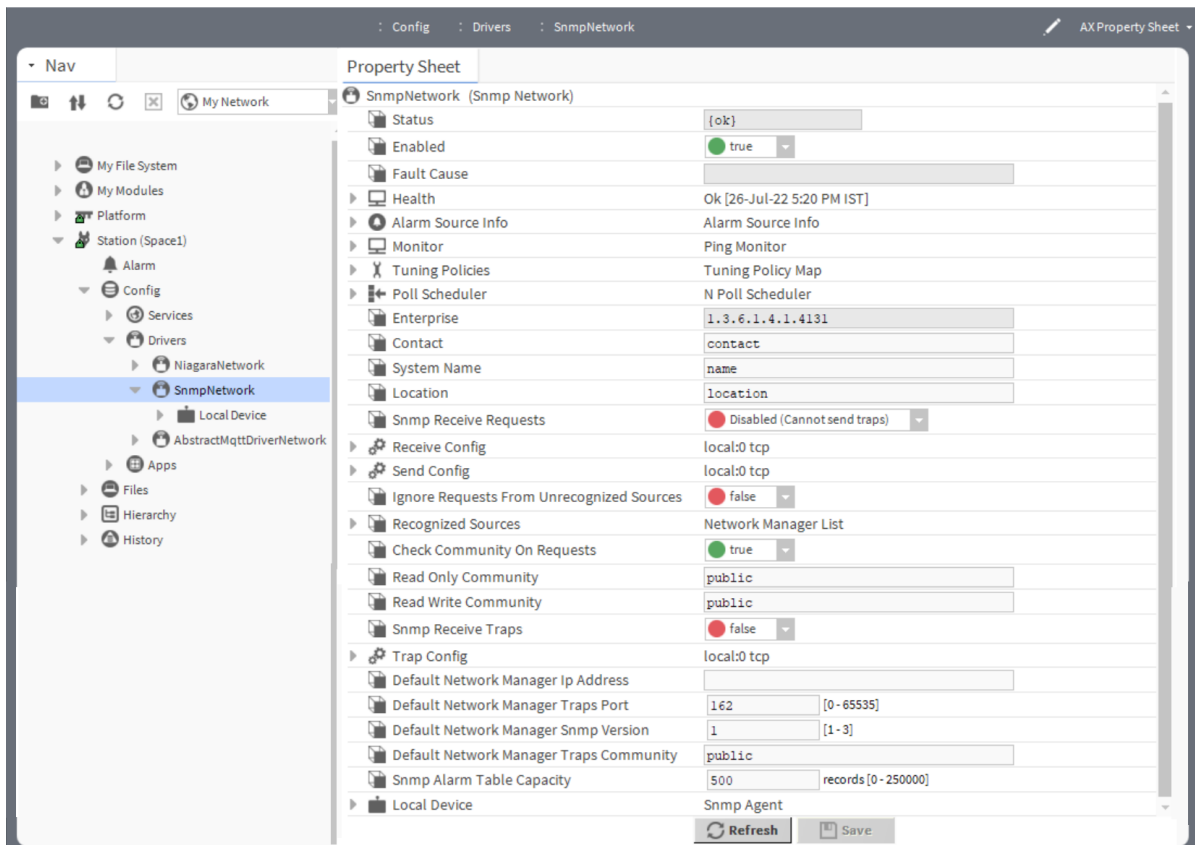
This is required to initiate network communications.

## Setting up an Snmp Agent application

When you add an **SnmpNetwork** object, a **Local Device** component comes with it.

- Step 1** Right-click the **SnmpNetwork** node and select **Views→AX Property Sheet**.

The **Property Sheet** opens and the **Enabled** property should be to `true`.



Step 2 If not enabled, set the **Enabled** option to **true**.

Step 3 Set the **Snmp Receive Requests** property to **Enabled** (can send traps).

This allows the **Local Device** to receive outside request messages from external Snmp sources and to send trap messages.

Step 4 Set the **Default Network Manager Ip Address** property value to the address of your Supervisor host platform.

Step 5 Set the **Default Network Manager Snmp Version** to 3 and click **Save**.

You can see the changed version number.

Step 6 When you set the version to 3 in **SnmpDevice** and click **Save**, sometimes the screen does not automatically reload if necessary, to refresh the screen.



# Chapter 3 Security and VACM Configuration

## Topics covered in this chapter

- ◆ Creating a `UsmUserTable`
- ◆ `VacmContextTable`
- ◆ `VacmGroupTable`
- ◆ `VacmViewTreeTable`
- ◆ `VacmAccessTable`

The user-based Security Model (USM) and View-based Access Control Model (VACM) configuration require you to configure six tables.

You add all tables under the **Local Device** of the controller (SNMP\_AGENT station).

## User-based Security Model (USM)

The USM is the default Security Module for SNMPv3. The U stands for User-based, as it contains a list of users and their attributes. SNMPv3 defines a user-based security mechanism that enables per-message authentication and encryption.

## View-based Access Control Model (VACM)

The VACM determines if access to a specific managed object is authorized. Access control is done at the following points:

- When processing retrieval request messages from the Manager
- When processing modification request messages from the Manager
- When notification messages must be sent to the Manager

## Creating a `UsmUserTable`

To create a `UsmUserTable` in an Agent, you must first have a properly configured `SnmNetwork` with a **Local Device** under it.

**Step 1** In the **Nav** side bar, under the station `SnmNetwork` node, double-click on the **Local Device** node.

The **Property Sheet** opens.

**Step 2** Open the `SnmPalette` in the **Palette** side bar.

**Step 3** From the `SnmPalette`, drag the `UsmUserTable` to the **Local Device** in the Nav tree or to the **Property Sheet** view of the **Local Device**.

The **Name** window opens.

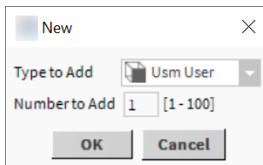
**Step 4** Type a name in the **Name** property (or accept the default name) and click **OK**.

**Step 5** Click on the added `UsmUserTable` in the **Usm User Manager** view.

The **Database** pane opens.

**Step 6** Click the **New** button in the **Database** pane

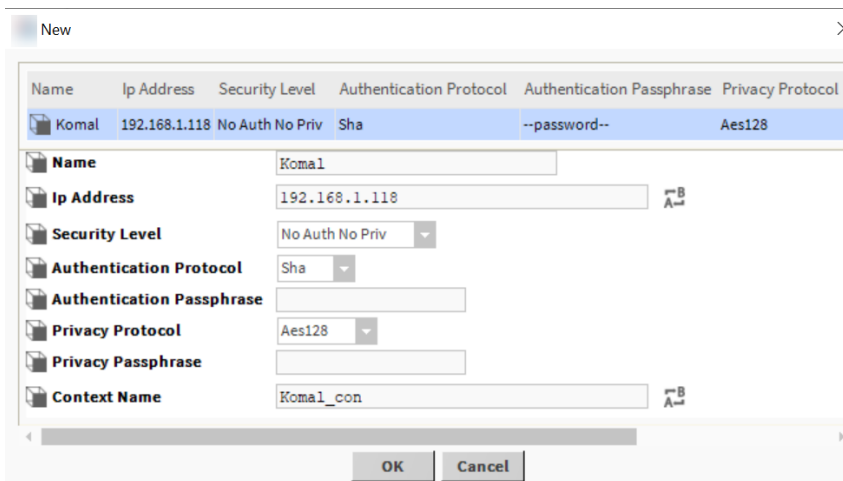
The **New** window opens.



Step 7 In the **New**, do the following:

- In the **Type to Add** field, select the **Usm User** from the option list.
- In the **Number to Add** field, type in a number to indicate the quantity of tables that you want to add.
- Click the **OK** button.

The **New** window opens.



Step 8 In the **New** window, edit the entries and click **OK**.

Note the following about entries in the **Edit** window:

- Name**  
This property represents the USM user name.
- Ip Address**  
This property is a text field for defining the Ip address of the user's Supervisor platform. This Ip address is used to handle traps, each USM user should have a different Ip address.
- Security Level**  
Use this property to select the desired amount of security that you want for messages on your SNMPv3 network. The security level value in this field restricts or allows access and notifications as described below:
  - No Auth No Priv**  
This option specifies communication without authentication or privacy. When you select this level, it is not necessary to enter any authentication or privacy inputs. A User with security level **No Auth No Priv** and context name as **noAuth** is called **noAuthUser**.
  - Auth No Priv**  
This option represents the communication with authentication and without privacy. You have to select the applicable **Authentication Protocol** and enter an **Authentication Passphrase** in the **UsmUserTable**. The protocols used for Authentication is SHA (Secure Hash Algorithm). Users with security level **Auth No Priv** and context name as **auth** is called as **authUser**.

### c. **Auth Priv**

This option represents the communication with authentication and privacy. User has to select the **SHA Authentication Protocol** for authentication and enter an **Authentication Passphrase**. Also select the **DES (Data Encryption Standard)** and **AES (Advanced Encryption Standard) Privacy Protocol** for privacy and enter a **Privacy Passphrase** in **UsmUserTable**. Users with security level **Auth Priv** and context name as **priv** is called as **privUser**.

- **Authentication Protocol**

This property allows you to select the **Authentication Protocol** HMAC-SHA-96. It is used to check the integrity and to authenticate the SNMPv3 message sent on the behalf of this user.

- **Authentication Passphrase**

This property allows user to set the passphrase. This is not applicable for **No Auth No Priv** security level.

- **Privacy Protocol**

This property allows user to select privacy protocol **DES**, **Aes128**, **Aes192** or **Aes256** to protect the SNMPv3 message from disclosure. This is not applicable for **No Auth No Priv** and **Auth No Priv** security levels.

- **Privacy Passphrase**

This property allows user to set the passphrase. This is not applicable for **No Auth No Priv** and **Auth No Priv** security levels.

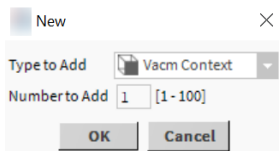
- **Context Name**

This property represents the **Context Name**. The **Context Name** specifies where the desired management object is to be found. The **Context Name** of the **UsmUserTable** must match with the entry in **VacmContextTable**.

## VacmContextTable

To create **VacmContextTable** in an Agent, you must first have a properly configured **SnmpNetwork** with a **Local Device** under it.

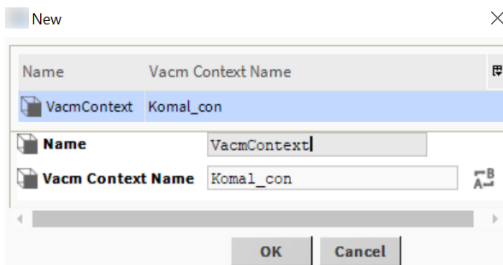
- Step 1 In the **Nav** side bar, under the station **SnmpNetwork** node, double-click on the **Local Device** node.  
The **Property Sheet** opens.
- Step 2 Open the **nSnmp Palette** in the **Palette** side bar.
- Step 3 From the **nSnmp Palette**, drag a **VacmContextTable** to the **Local Device** node in the Nav tree or to the **Property Sheet** view of the **Local Device**.  
The **Name** window opens.
- Step 4 Type a name in the **Name** property (or accept the default name) and click **OK**.  
It creates a new name in the **Local Device**.
- Step 5 Click on the added **VacmContextTable**.  
The **Database** pane opens.
- Step 6 Click the **New** button in the **Database** pane.  
The **New** window opens.



Step 7 In the **New** window, do the following:

- a. In the **Type to Add** property, select the **Vacm Context** from the option list.
- b. In the **Number to Add** property, type in a number to indicate the quantity of tables that you want to add.
- c. Click the **OK** button.

The **New** window opens.



Step 8 In the **New** window, edit the entries and click **OK**.

Note the following about entries in the **New** window:

- **Name**  
This property represents the name of the table.
- **Context Name**  
This property represents the context name. The **Context Name** of the **VacmContextTable** must be the same as per **UsmUserTable**.

## VacmGroupTable

To create **VacmGroupTable** in an Agent, you must first have a properly configured **SnmpNetwork** with a **Local Device** under it.

Step 1 In the **Nav** side bar, under the station **SnmpNetwork** node, double-click on the **Local Device** node.

The **Property Sheet** opens.

Step 2 Open the **Snmp Palette** in the **Palette** side bar.

Step 3 From the **Snmp Palette**, drag a **VacmGroupTable** to the **Local Device** in the Nav tree or to the **Property Sheet** view of the **Local Device**.

The **Name** window opens.

Step 4 Type a name in the **Name** field (or accept the default name) and click **OK**.

It creates a new name in the **Local Device**.

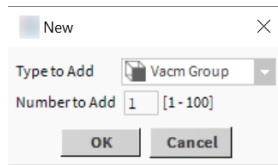
Step 5 Click on the added **VacmGroupTable**.

The **Database** pane opens.

Step 6 Click the **New** button of the **Database** pane.

The **New** window opens.

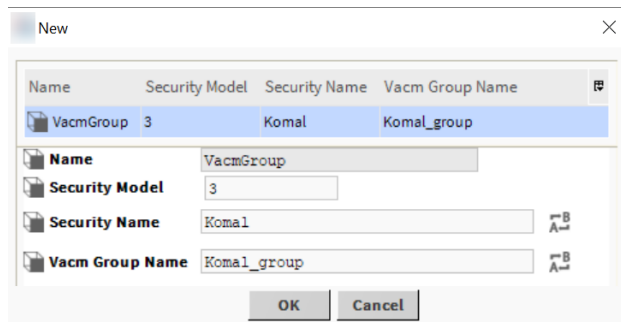




Step 7 In the **New** window, do the following:

- a. In the **Type to Add** field, select the **Vacm Group** from the option list.
- b. In the **Number to Add** field, type in a number to indicate the quantity of tables that you want to add.
- c. Click the **OK** button.

The **New** window opens.



Step 8 In the **New** window, edit the entries and click **OK**.

Note the following about entries in the **New** window:

- **Name**  
This property represents the name of the table.
- **Security Model**  
This property gives the value 3 by default.
- **Security Name**  
This property represents the user name. The **Security Name** should be the same as **Name** in **UsmUserTable**.
- **Vacm Group Name**  
This property represents the Group name of the **VacmGroupTable**.

## VacmViewTreeTable

To create **VacmViewTreeTable** in an Agent, you must first have a properly configured SnmpNetwork with a **Local Device** under it.

The MIB subtree level is restricted to define the views which the user will have access to.

Step 1 In the **Nav** side bar, under the station **SnmpNetwork** node, double-click on the **Local Device** node.

The **Property Sheet** opens.

Step 2 Open the **nSnmp Palette** in the **Palette** side bar.

Step 3 From the **nSnmp Palette**, drag a **VacmViewTreeTable** to the **Local Device** node in the Nav tree or to the **Property Sheet** view of the **Local Device**.

The **Name** window opens.

Step 4 Type a name in the **Name** field (or accept the default name) and click **OK**.

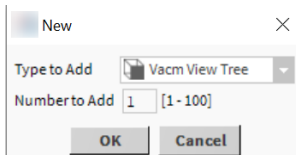
It creates a new name in the **Local Device**.

Step 5 Click on the added **VacmViewTreeTable**.

The **Database** pane opens.

Step 6 Click the **New** button of the **Database** pane.

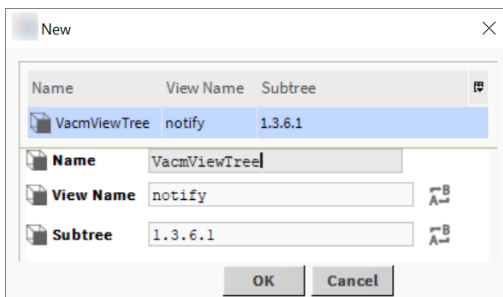
The **New** window opens.



Step 7 In the **New** window, do the following:

- In the **Type to Add** field, select the **Vacm View Tree** from the option list.
- In the **Number to Add** field, type in a number to indicate the quantity of tables that you want to add.
- Click the **OK** button.

The **New** window opens.



Step 8 In the **New** window, edit the entries and click **OK**.

Note the following about entries in the **New** dialog box:

- **Name**  
This property represents the name of the table.
- **View Name**  
This property represents the user access.
- **Subtree**  
This property displays the enterprise OID (Object Identifier) 1.3.6.1 information for the station. The MIB subtree level is restricted to define the views which the user will have access to.

## VacmAccessTable

To create **VacmAccessTable** in an Agent, you must first have a properly configured SnmpNetwork with a **Local Device** under it.

The **VacmAccessTable** is the combination of the all tables.

Step 1 In the **Nav** side bar, under the station **SnmpNetwork** node, double-click on the **Local Device** node.

The **Property Sheet** opens.

Step 2 Open the **nSnmp Palette** in the **Palette** side bar.

Step 3 From the **nSnmp Palette**, drag a **VacmAccessTable** to the **Local Device** or to the **Property Sheet** view of the **Local Device**.

The **Name** window opens.

Step 4 Type a name in the **Name** field (or accept the default name) and click **OK**.

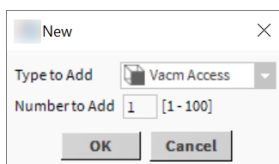
It creates a new name in the **Local Device**.

Step 5 Click on the added **VacmAccessTable**.

The **Database** pane opens.

Step 6 Click the **New** button of the **Database** pane.

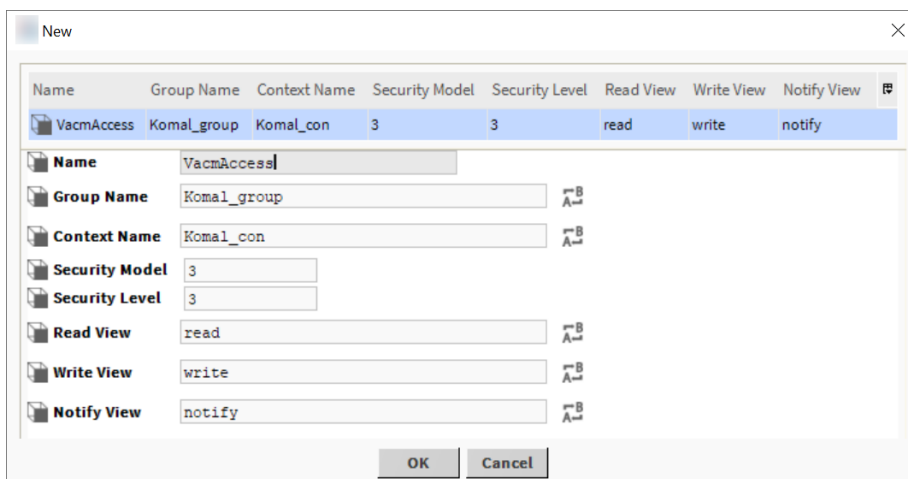
The **New** window opens.



Step 7 In the **New** window, do the following:

- In the **Type to Add** field, select the **Vacm Access** from the option list.
- In the **Number to Add** field, type in a number to indicate the quantity of tables that you want to add.
- Click the **OK** button.

The **New** window opens.



Step 8 In the **New** window, edit the entries and click **OK**.

Note the following about entries in the **New** dialog box:

- **Name**  
This property represents the name of the table.
- **Group Name**  
This property represents the Group name of the **VacmAccessTable**. The **Group Name** must match with the entry made in previous tables.

- **Context Name**

This property represents the **Context Name**. The **Context Name** specifies where the desired management object is to be found. The **Context Name** of the **VacmAccessTable** must match with the entry made in previous tables.

- **Security Model**

This property gives the value 3 by default.

- **Security Level**

Use this property to select the desired amount of security that you want for messages on your SNMPv3 network. The security level value in this field restricts or allows access and notifications as described below:

- a. **No Auth No Priv**

This option specifies communication without authentication or privacy. When you select this level, it is not necessary to enter any authentication or privacy inputs. A User with security level **No Auth No Priv** and context name as noAuth is called **noAuthUser**. The **Security Level** for **No Auth No Priv** is 0.

- b. **Auth No Priv**

This option represents the communication with authentication and without privacy. You have to select the applicable **Authentication Protocol** and enter an **Authentication Passphrase** in the **UsmUserTable**. The protocols used for Authentication is SHA (Secure Hash Algorithm). Users with security level **Auth No Priv** and context name as auth is called as **authUser**. The **Security Level** for **Auth No Priv** is 1.

- c. **Auth Priv**

This option represents the communication with authentication and privacy. User has to select the SHA **Authentication Protocol** for authentication and enter an **Authentication Passphrase**. Also select the DES (Data Encryption Standard) and AES (Advanced Encryption Standard) **Privacy Protocol** for privacy and enter a **Privacy Passphrase** in **UsmUserTable**. Users with security level **Auth Priv** and context name as priv is called as **privUser**. The **Security Level** for **Auth Priv** is 3.

- **Read View**

This is the view name of the **VacmAccessTable**. The **Read View** must match with the entry made in previous tables.

- **Write View**

This is the view name of the **VacmAccessTable**. The **Write View** must match with the entry made in previous tables.

- **Notify View**

This is the view name of the **VacmAccessTable**. The **Notify View** must match with the entry made in previous tables.

# Chapter 4 Manager Configuration

## Topics covered in this chapter

- ◆ Setting up an Snmp manager application
- ◆ Configuring the SnmpDevice (Manager)

This section describes the configuration of the **SnmpNetwork** in a local machine as a Manager.

To configure the **SnmpNetwork**, first add the **SnmpNetwork** and then design the **SnmpNetwork** application.

## Setting up an Snmp manager application

For Snmp manager applications, you add **SnmpDevice** objects to your **SnmpNetwork** to represent actual **Snmp agent devices** that you want to manage.

Step 1 Under the **Drivers** node of your station, double-click on the **SnmpNetwork** node in the Nav tree.

The **Snmp Device Manager** view opens.

Step 2 Using the **Palette** side bar controls, open the local **nSnmp Module** palette, expand the **Client** folder and copy and paste (or drag) an **SnmpDevice** object into the view pane.

The **Name** window opens.

Step 3 Name the **SnmpDevice**, as desired and click the **OK** button.

The device is added to the **SnmpDevice** view and represents one **Snmp agent device** on your network. You can add more of these objects, if needed, each representing a single **Snmp agent device** under your Snmp manager application.

Step 4 Double click on the added device in the **Snmp Device Manager** view.

The **Edit** window appears.

Name	Type	Enabled	Poll Frequency	Snmp Version	Ip Address	Port	Community	Max Variable Bindings
SnmpDevice	Snmp Device	true	Normal	2	192.168.1.8	161	public	10

Name	SnmpDevice
Type	Cannotedit
Enabled	<input checked="" type="checkbox"/> true
Poll Frequency	Normal
Snmp Version	3 [1-3]
Ip Address	192.168.1.8
Port	161 [0-4999]
Community	public
Max Variable Bindings Per Request	10 [0-max]
Retry Count	2
Response Timeout	+000000h 00m 02.000s

OK Cancel

Step 5 In the **Edit** window, set the **Snmp Version** and **Ip Address** of the JACE (Agent), then click the **OK** button.

The **SnmpDevice** is added under the **SnmpNetwork**.

## Configuring the SnmpDevice (Manager)

You place **SnmpDevice** objects under an **SnmpNetwork** to represent actual Snmp devices that you want to communicate with. Then you configure the **SnmpDevice** object, by setting its properties to match the settings for the actual Snmp device. The **SnmpDevice** objects may only exist under an **SnmpNetwork** object.

**Step 1** Edit the following **SnmpDevice** specific properties in the **Property Sheet** to configure the Snmp Manager.

Snmp Device	
Status	{down, alarm, unackedA}
Enabled	<input checked="" type="checkbox"/> true
Fault Cause	
Health	Fail [22-Jun-16 4:00 PM IST] No response
Alarm Source Info	Alarm Source Info
Poll Frequency	Normal
Points	Snmp Point Device Ext
Traps	Snmp Alarm Device Ext
Snmp Version	3 [1 - 3]
Retry Count	2
Response Timeout	+000000h 00m 02.000s
Max Variable Bindings Per Request	10 [0 - max]
Ip Address	192.168.1.8
Port	161 [0 - 4999]
Community	public
Mib	
User Name	Komal
Security Level	Auth Priv
Authentication Protocol	Sha
Authentication Passphrase	*****
Privacy Protocol	Aes128
Privacy Passphrase	*****
Context Name	Komal_con
Engine ID	8000102380C0A80108000000
<input type="button" value="Refresh"/> <input type="button" value="Save"/>	

**Step 2** Set the **Snmp Version** to 3.

When you set the version to 3 in **SnmpDevice** and click **Save**, sometimes the screen does not automatically reload if necessary, to refresh the screen.

**Step 3** Type the Ip adress of the JACE which act as an Snmp agent to the **Ip Address** field to receive the traps.

**Step 4** Type the name of the user in the **User Name** field as per the Agent configuration.

**Step 5** Set the **Security Level** field as per the Agent configuration. Make sure that the Agent and Manager has the same **Security Level** at a time for sending and receiving traps. Refer to [Chapter 3 Security and VACM Configuration, page 13](#) for detail information about the **Security Level**.

**Step 6** Set the **Authentication Protocol** field as per the Agent configuration. Make sure that the Agent and Manager has the same **Authentication Protocol** selected at a time for sending and receiving traps. Refer to [Chapter 3 Security and VACM Configuration, page 13](#) for detail information about the **Authentication Protocol**.

**Step 7** Enter the **Authentication Passphrase** as per the Agent configuration. If not, error message pops up and it stops the coordination between Agent and Manager. Refer to [Chapter 3 Security and VACM Configuration, page 13](#) for detail information about the **Authentication Passphrase**.

- Step 8 Set the **Privacy Protocol** field as per the Agent configuration. Make sure that the Agent and Manager has the same **Privacy Protocol** selected at a time for sending and receiving traps. Refer to [Chapter 3 Security and VACM Configuration, page 13](#) for detail information about the **Privacy Protocol**.
- Step 9 Enter the **Privacy Passphrase** as per the Agent configuration. If not, error message pops up and it stops the coordination between Agent and Manager. Refer to [Chapter 3 Security and VACM Configuration, page 13](#) for detail information about the **Privacy Passphrase**.
- Step 10 Type the context name in the **Context Name** field as per the Agent configuration.
- Step 11 Right-click on the **SnmpDevice** and go to **Action→Ping**.  
This action manually initiates a **Ping**(check device status) on the actual Snmp device that the **SnmpDevice** object represents.
- Step 12 Do a ping. and check the **Status** and **Health** of the **SnmpDevice**.  
The **Status** should be "{ok}" and **Health** should be **Ok** for successful coordination between Manager and Agent.





# Chapter 5 Snmp Plugins

## Topics covered in this chapter

- ◆ Snmp Agent Point Manager
- ◆ Snmp Device Manager
- ◆ Snmp Export Manager
- ◆ Snmp Object Manager
- ◆ Snmp Point Manager
- ◆ Snmp Table Manager
- ◆ Snmp Trap Manager
- ◆ Usm User Manager View
- ◆ Vacm Access Manager View
- ◆ Vacm Context Manager View
- ◆ Vacm Group Manager View
- ◆ Vacm View Tree Manager View

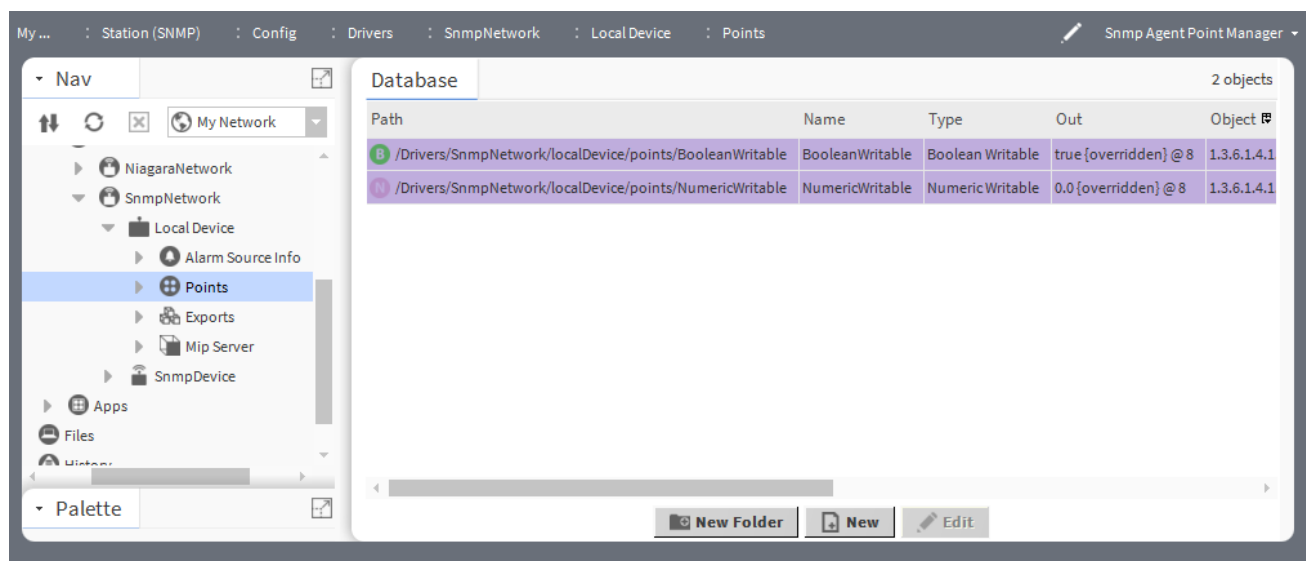
Plugins provide a visualization of a Component. There are many ways to view plugins. One way is directly in the tree. In addition, you can right-click on an item and select one of its views. Plugins provide views of Components. You can access documentation on a Plugin by selecting **Help→ On View (F1)** from the **Menu** bar or pressing F1 while the Plugin is selected.

The following topics describe Snmp plugins:

## Snmp Agent Point Manager

Use the **Snmp Agent Point Manager** to create, edit, access, and delete SnmpAgent proxy points under a SnmpAgent. The **Snmp Agent Point Manager** is the default view for the SnmpAgentPointDeviceExt (**Points** container) under an SnmpAgent. The **Snmp Agent Point Manager** is also the default view for any SnmpAgentPointFolder under the **Points** container of an SnmpAgent.

Figure 1 Snmp Agent Point Manager view



To access this view, expand **Config→Drivers→SnmpNetwork→LocalDevice** and double-click **Points**.

## Columns

Column	Description
Path	Reports the location of the device or point in the station.
Name	Reports the name of the entity or logical grouping.
Type	Reports the type of the point.
Out	Describes the output.
Object Identifier	Specifies the OID of the actual Snmp device where the data is to be read from or written to.
Index	Reports the column index in the Input Table (or Output Table) used to locate the value of the proxy point. This is the last number in the <b>Object Identifier</b> (OID) value. For example, if the index has a value of 1, the OID containing the value of the point is 1.3.6.1.4.1.4131.1.4.1.3.1. If the index is 2, this corresponds to an OID of 1.3.6.1.4.1.4131.1.4.1.3.2, and so on.
Default Value	Reports the property is the default value used for the output of the proxy point on startup prior to being set by an external Snmp SET request. If 'autoSet' is checked, the default value is automatically set (changed) whenever a new external Snmp SET request is received. If 'autoSet' is unchecked, you can specify a permanent default value (any external Snmp SET request will not change the default value). To manually reset the proxy point's output to the default value at any time, by selecting the 'Reset Point To Default' action.
Agent Table Entry Type	Reports the type of table entry.
Enabled	Indicates if the network, device, point or component is active or inactive.
Device Facets	Reports the device's of enumerated state.
Facets	Reports the device's facets.
Conversion	Reports how the system converts proxy extension units to parent point units. <i>Default</i> automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.
Read Value	Reports the last value read from the device, expressed in device facets.
Write Value	Reports the last value written, using device facets.
Tuning Policy Name	Reports the tuning policy used to evaluate both write requests and the acceptability (freshness) of read requests.

## Buttons

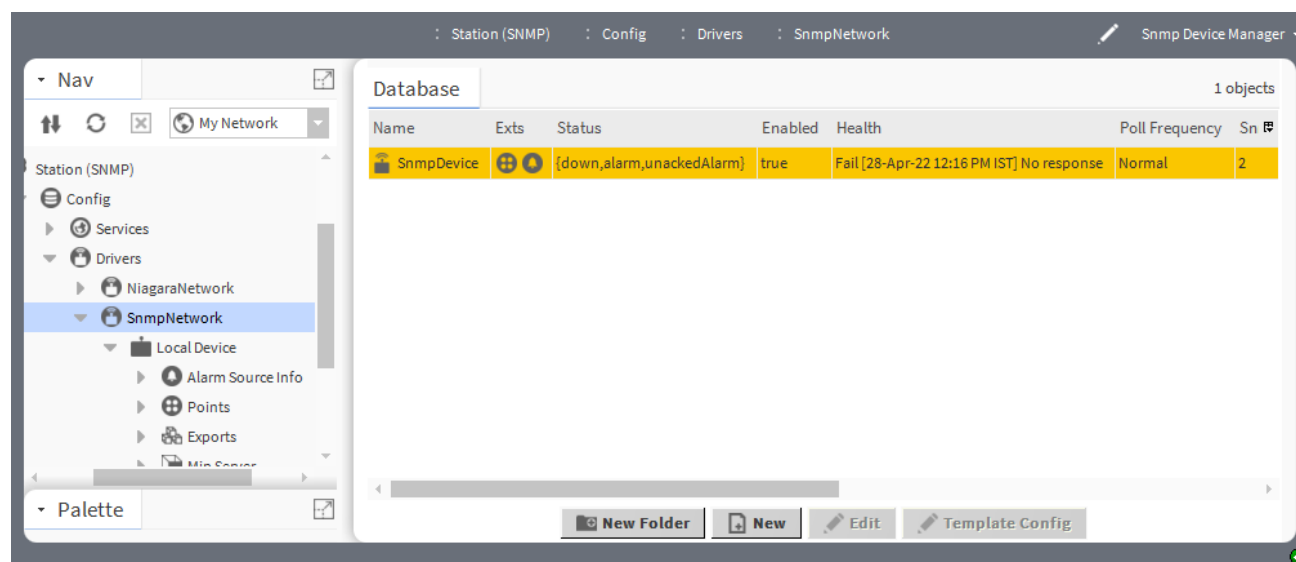
These buttons are available on the **SnmpNetwork's Snmp Agent Point Manager** view.

- **New Folder** creates a new folder for devices. Each such folder provides its own set of manager views.
- **New** creates a new device record in the database.
- **Edit** opens the device's database record for updating.

## Snmp Device Manager

Use the **Snmp Device Manager** to create, edit, and view both **SnmpDevice** and **SnmpAgent** under an **SnmpNetwork**. The **Snmp Device Manager** is the default view on the **SnmpNetwork**.

Figure 2 Snmp Device Manager view



To access this view, expand **Config→Drivers→LocalDevice** and right-click **SnmpNetwork→Views→Snmp Device Manager**.

### Columns

Column	Description
Name	Displays the name of the device.
Exts	Displays the device's extension hyperlinks, including: Points, Alarms, Schedules, Trend Logs and Config.
Status	Reports the current condition of the entity as of the last refresh: {alarm}, {disabled}, {down}, {fault}, {ok}, {stale}, {unackedAlarm}
Enabled	Indicates if the network, device, point or component is active or inactive.
Health	Reports the status of the network, device or component. This advisory information, including a time stamp, can help you recognize and troubleshoot problems but it provides no direct management controls.
Poll Frequency	Displays the polling frequency.
Snmp Version	Displays the Snmp version whether it is Snmp V1 or Snmp V2
IP Address	Reports the IP address of the device.
Port	Displays the port used for outgoing Snmp requests to the corresponding Snmp device for this <b>SnmpDevice</b> .
Community	Displays the community string field used for outgoing Snmp request messages sent to the <b>SnmpDevice</b> .
Max Variable Binding Per Request	Displays the variable bindings included in each Snmp request message sent to the Snmp device.
Retry Count	Displays the number of times any individual Snmp request made to this <b>SnmpDevice</b> will be retried when receiving a null response before considering the request to be a communication failure.
Response Timeout	Displays the maximum amount of time the system waits for a response after sending an Snmp request to this <b>SnmpDevice</b>

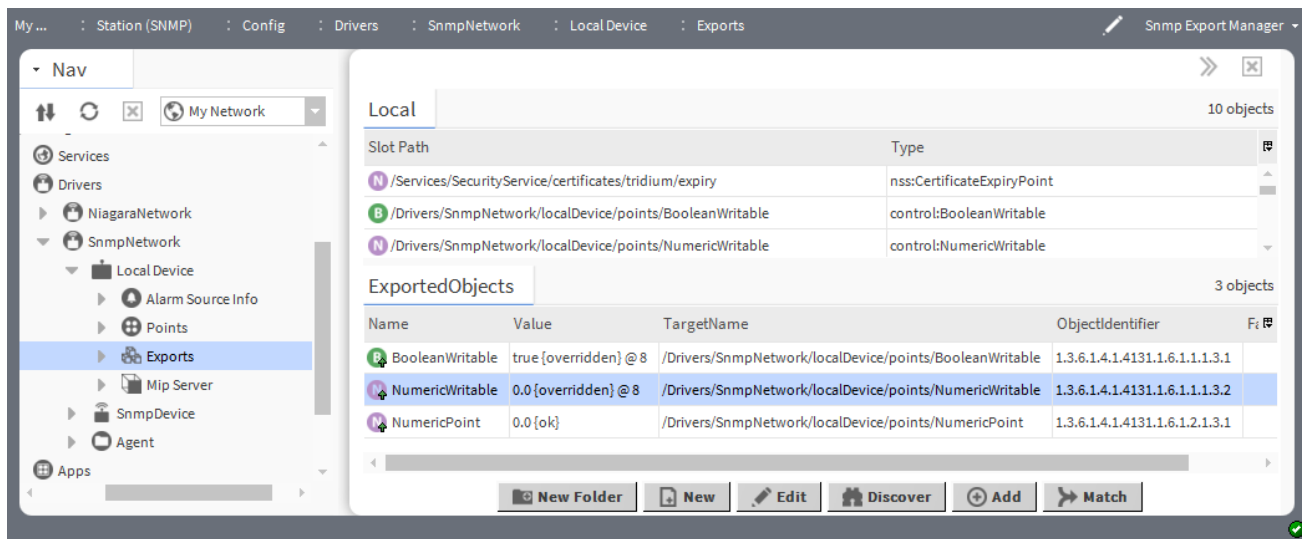
## Buttons

- **New Folder** creates a new folder for devices. Each such folder provides its own set of manager views.
- **New** creates a new device record in the database.
- **Edit** opens the device's database record for updating.
- **Template Config** accesses the station template that defines configuration options. You would select a template to set up the device with pre-configured properties.

## Snmp Export Manager

The **Snmp Export Manager** is the default view of the Snmp Export Table component. The view has an upper (**Local**) and lower (**Exported Objects**) panes that you use for discovering and adding points or tables for exporting Snmp values. Use this view to discover and add points and tables to your Snmp Export Table under the **Snmp Local Device**.

Figure 3 Snmp Export Manager view



To access this view, expand **Config**→**Drivers**→**SnmpNetwork**→**Local Device** and double-click **Exports**.

## Columns

Column	Description
Type	Displays the type of exported object.
Name	Reports the name of the entity or logical grouping.
Value	Displays the output value.
TargetName	Displays the path where the exported object is located.
ObjectIdentifier	Specifies the OID of the actual Snmp device where the data are to be read from or written to.
ExportOrd	Displays the location of the source component or file using standard file Ord notation.
ExportStatus	Displays the status of object export.
FaultCause	Provides a description of the reason for the fault.
DeviceFacets	Reports the device's of enumerated state.

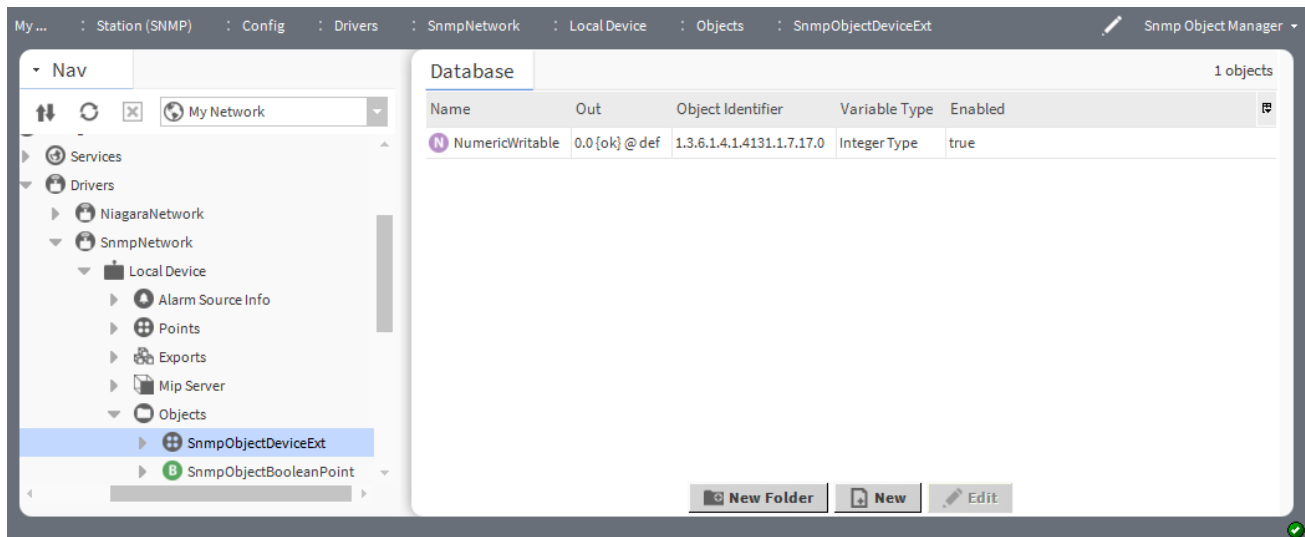
## Buttons

- **New** creates a new device record in the database.
- **Edit** opens the device's database record for updating.
- **Discover** runs a discover job to locate installed devices, which appear in the **Discovered** pane. This view has a standard appearance that is similar to all **Device Manager** views.
- **Add** inserts into the database a record for the discovered and selected object.
- **Match** associates a discovered device with a record that is already in the database.

## Snmp Object Manager

The **Snmp Object Manager** is the default view of the **SnmpObjectDeviceExt**. This view provides a single database pane with which you to add Snmp Object types and folders using the buttons at the bottom of the view. The added Snmp Objects to expose any Snmp ASN data type instead of just the string type supported in the tables.

Figure 4 Snmp Object Manager view



To access this view, expand **Config→Drivers→SnmpNetwork→LocalDevice→Objects** and right-click **SnmpObjectDeviceExt**.

## Columns

Column	Description
Name	Reports the name of the entity or logical grouping.
Type	Reports the type of the object.
Out	Describes the output.
Object Identifier	Specifies the OID of the actual Snmp device where the data is to be read from or written to.
Variable Type	Displays the type of the object variable.
Enabled	Indicates if the object (network, device, point, etc.) is active or inactive.
Facets	Reports the device's of enumerated state.
Conversion	Display how the system converts proxy extension units to parent point units.

Column	Description
	Default automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.
Read Value	Displays the last value read from the device, expressed in device facets.
Write Value	Displays the last value written, using device facets.
Tuning Policy Name	Displays the tuning policy used to evaluate both write requests and the acceptability (freshness) of read requests.
Description	Provides additional information.
Tuning Policy Name	Displays the tuning policy used to evaluate both write requests and the acceptability (freshness) of read requests.

## Buttons

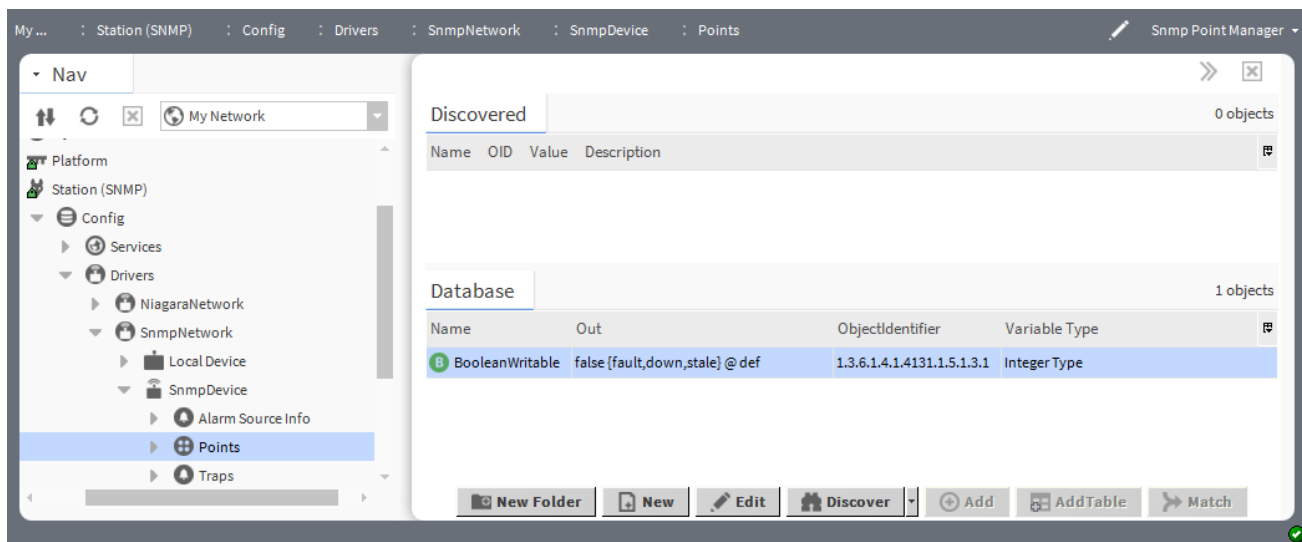
These buttons are available on the **SnmpNetwork's Snmp Object Manager** view.

- **New Folder** creates a new folder for devices. Each such folder provides its own set of manager views.
- **New** creates a new device record in the database.
- **Edit** opens the device's database record for updating.

## Snmp Point Manager

Use the **Snmp Point Manager** to create, edit, access, and delete Snmp proxy points under a **SnmpDevice**. The **Snmp Point Manager** is the default view for the **SnmpPointDeviceExt (Points)** container under an **SnmpDevice**.

Figure 5 Snmp Point Manager view



To access this view, expand **Config→Drivers→SnmpNetwork→SnmpDevice** and double-click **Points**.

## Columns

Column	Description
Path	Reports the location of the device or point in the station.
Name	Reports the name of the entity or logical grouping.
Type	Reports the type of the object.
Out	Describes the output.
Object Identifier	Specifies the OID of the actual Snmp device where the data is to be read from or written to.
Variable Type	Displays the type of the object variable.
Enabled	Indicates if the object (network, device, point, etc.) is active or inactive.
Device Facets	Reports the device's of enumerated state.
Facets	Reports the device's facets.
Conversion	Reports how the system converts proxy extension units to parent point units. <i>Default</i> automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.
Read Value	Displays the last value read from the device, expressed in device facets.
Write Value	Displays the last value written, using device facets.
Tuning Policy Name	Displays the tuning policy used to evaluate both write requests and the acceptability (freshness) of read requests.
Fault Cause	Displays the reason why the point is in fault.

## Buttons

These buttons are available on the **SnmpNetwork's Snmp Point Manager** view.

- **New Folder** creates a new folder for devices. Each such folder provides its own set of manager views.
- **New** creates a new device record in the database.
- **Edit** opens the device's database record for updating.
- **Discover** runs a discover job to locate installed devices, which appear in the **Discovered** pane. This view has a standard appearance that is similar to all **Device Manager** views.
- **Add** inserts into the database a record for the discovered and selected object.
- **Add Table:** inserts the table from the discovered object.
- **Match** associates a discovered device with a record that is already in the database.

## Snmp Table Manager

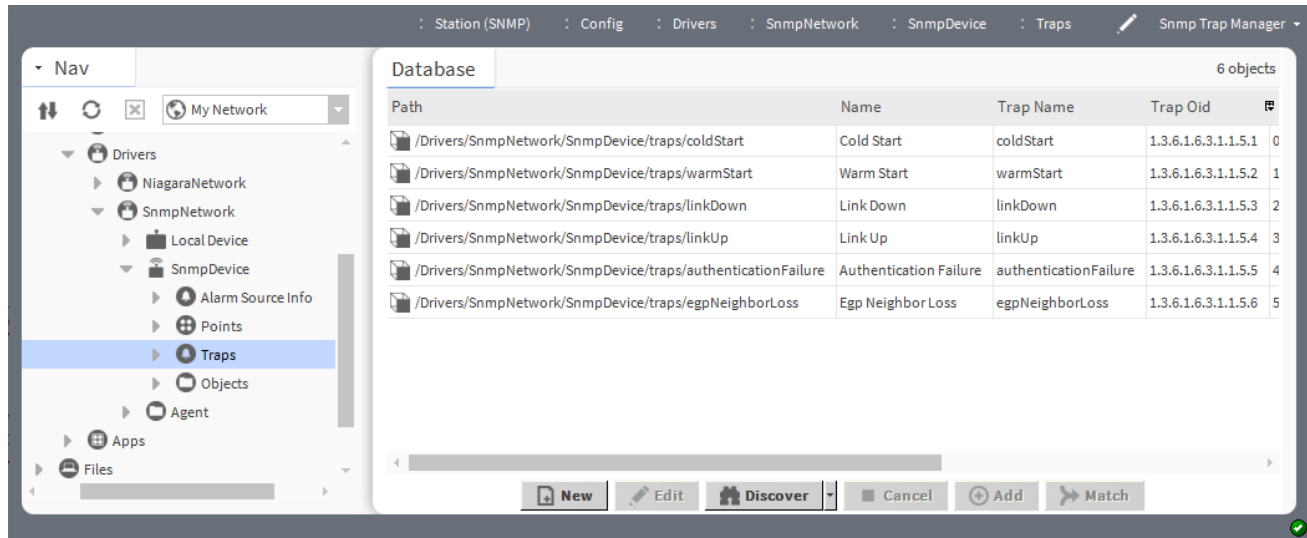
The Snmp Table Manager is the default view of any Snmp Table (outputTable or exportTable).

The view displays an ordered sequence of rows with the output index number, name and value in separate columns. The view has a **WalkMib** button for updating values by walking the MIB.

## Snmp Trap Manager

Use the **Snmp Trap Manager** to discover, compile, display, and store traps from MIB files for an **SnmpDevice**. The **Snmp Trap Manager** is the default view for an **SnmpDevice**'s TrapTable slot (default name Trap Types).

Figure 6 Snmp Trap Manager view



To access this view, expand **Config**→**Drivers**→**SnmpNetwork**→**SnmpDevice** and double-click **Traps**.

### Columns

Column	Description
Path	Displays the path where the trap is located.
Trap Name	Displays the name of the trap.
Trap Oid	Displays the object identifier for each trap.
Generic Type	
Specific Type	
Variable Array	
Reference	
Description	

### Buttons

These buttons are available on the **SnmpNetwork**'s **Snmp Trap Manager** view.

- **New** creates a new device record in the database.
- **Edit** opens the device's database record for updating.
- **Discover** runs a discover job to locate installed devices, which appear in the **Discovered** pane. This view has a standard appearance that is similar to all **Device Manager** views.
- **Cancel** ends the current discovery job.
- **Add** inserts into the database a record for the discovered and selected object.
- **Match** associates a discovered device with a record that is already in the database.

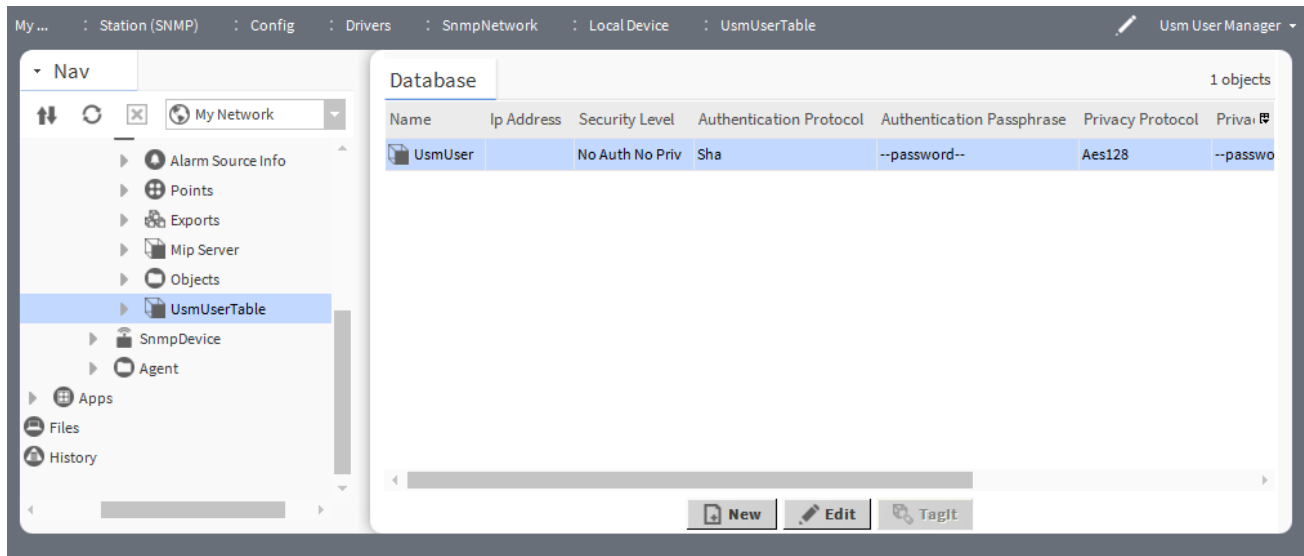


- **TagIt** associates metadata, such as location or unique configuration with the object.

## Usm User Manager View

The **Usm User Manager** view is a default view of **UsmUserTable** which is located under **Local Device**.

Figure 7 Usm User Manager View



To access this view, expand **Config→Drivers→SnmpNetwork→LocalDevice** and double-click **UsmUserTable**.

### Columns

Column	Description
Name	Displays the name of Usm user.
IP Address	Displays the Ip address of the user's Supervisor platform.
Security Level	Displays the select security level for messages on the SNMPv3 network.
Authentication Protocol	Displays the selected authentication protocol to check the integrity and to authenticate the SNMPv3 message sent on behalf of the user.
Authentication Passphrase	Displays the passphrase set for the authentication protocol.
Privacy Protocol	Displays the private protocol to protect the SNMPv3 message from disclosure.
Engine I D	
Context Name	Displays the context name where the desired management object is to be found.

### Buttons

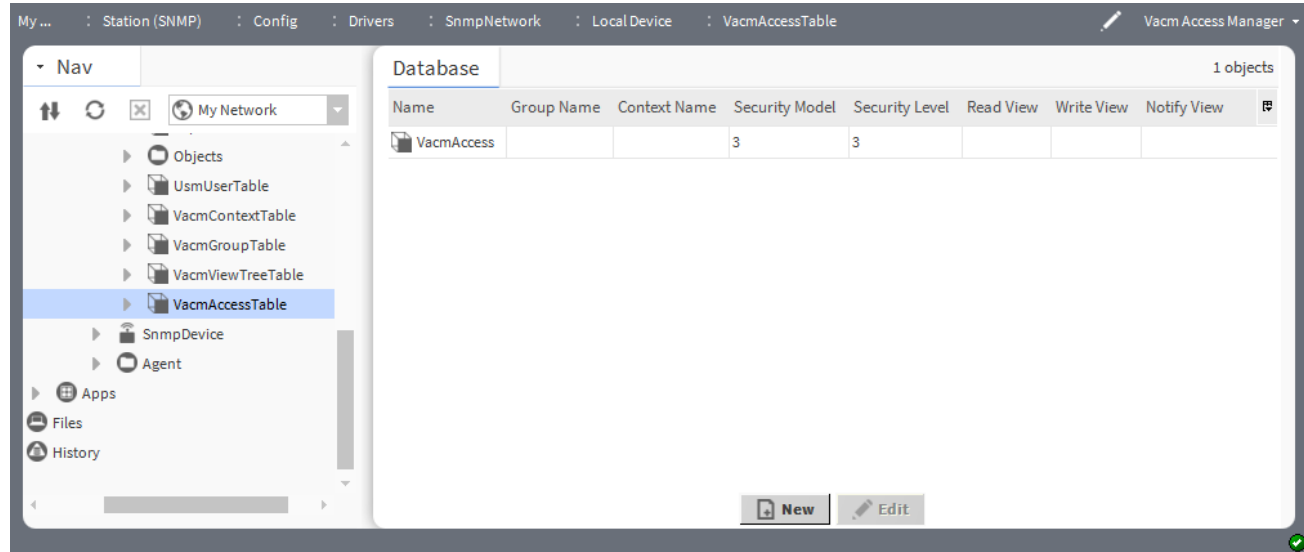
These buttons are available on the **SnmpNetwork's Usm User Manager** view.

- **New** creates a new device record in the database.
- **Edit** opens the device's database record for updating.

## Vacm Access Manager View

The **Vacm Access Manager** view is a default view of **VacmAccessTable** which is located under **Local Device**.

Figure 8 Vacm Access Manager View



To access this view, expand **Config**→**Drivers**→**SnmpNetwork**→**LocalDevice** and double-click **VacmAccessTable**.

### Columns

Column	Description
Name	Displays the name of table.
Group Name	Displays the Group name of the table.
Context Name	Displays the context name.
Security Model	Displays the default value as 3.
Security Level	Displays the desired amount of security for messages on your SNMPv3 network.
Read View	Displays the view name of the VacmAccessTable.
Write View	Displays the view name of the VacmAccessTable.
Notify View	Displays the view name of the VacmAccessTable.

### Buttons

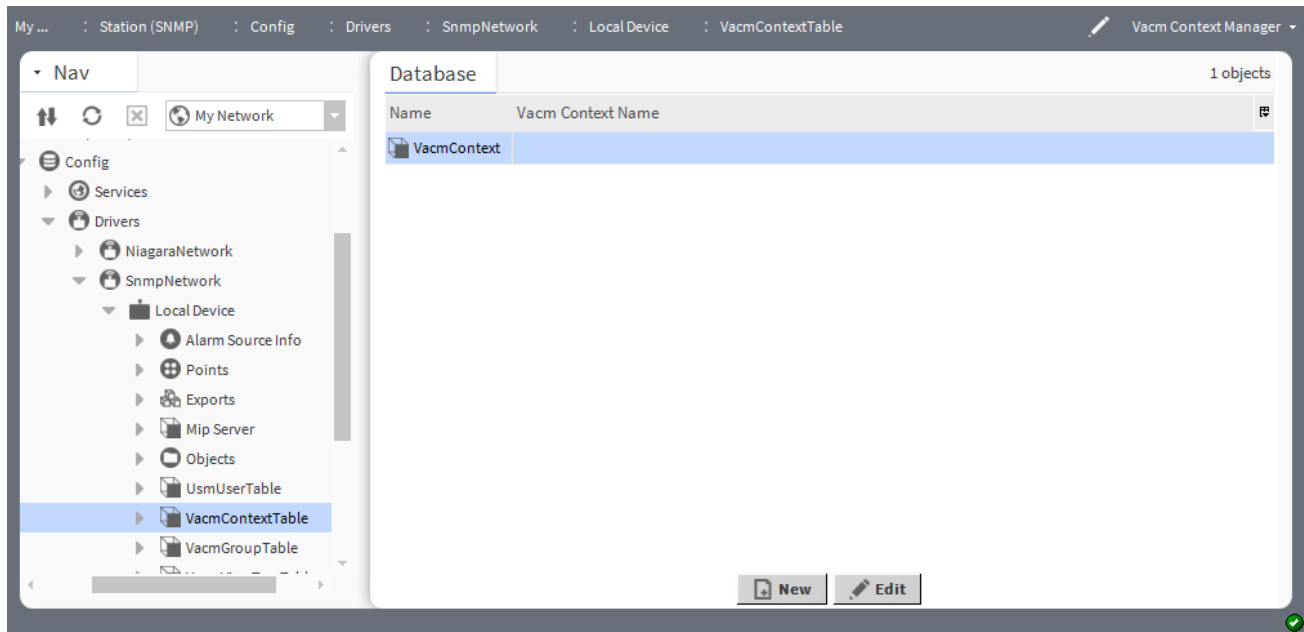
These buttons are available on the **SnmpNetwork**'s **Usm User Manager** view.

- **New** creates a new device record in the database.
- **Edit** opens the device's database record for updating.

## Vacm Context Manager View

The **Vacm Context Manager** view is a default view of **VacmContextTable** which is located under **Local Device**.

Figure 9 Vacm Access Manager View



To access this view, expand **Config**→**Drivers**→**SnmpNetwork**→**LocalDevice** and double —click **VacmContextTable**.

### Columns

Column	Description
Name	Displays the name of Vacm table.
VacmContext	Displays the Vacm context name.

### Buttons

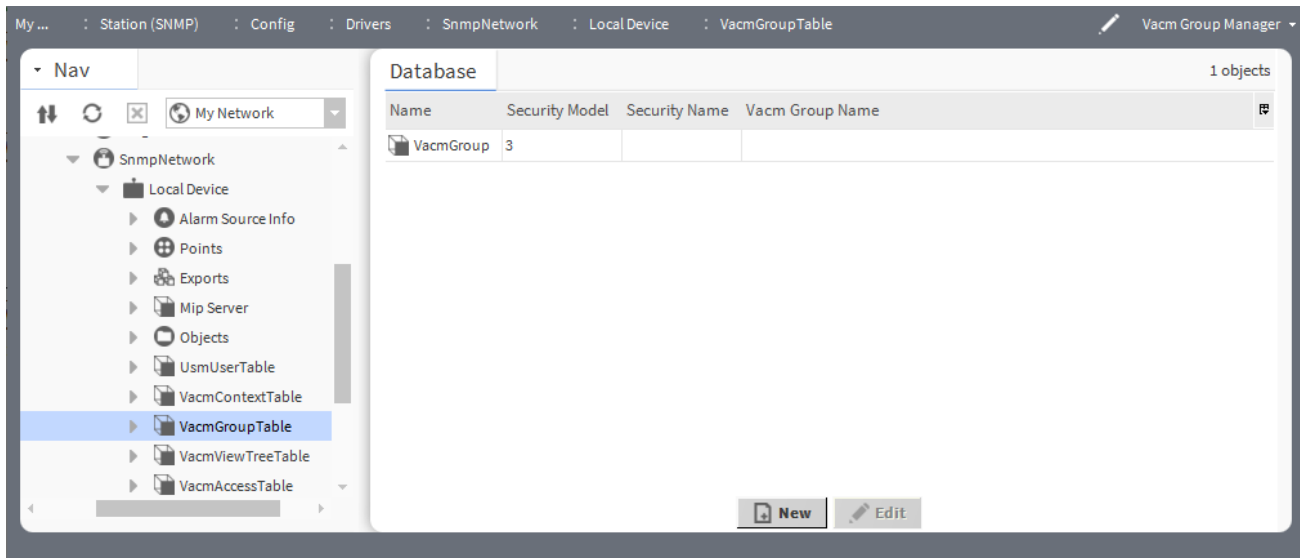
These buttons are available on the **SnmpNetwork**'s **VacmContextTable** view.

- **New** creates a new device record in the database.
- **Edit** opens the device's database record for updating.

## Vacm Group Manager View

The **Vacm Group Manager** view is a default view of **VacmGroupTable** which is located under **Local Device**.

Figure 10 Vacm Group Manager View



To access this view, expand **Config→Drivers→SnmpNetwork→LocalDevice** and double —click **VacmGroupTable**.

### Columns

Column	Description
Name	Displays the <b>VacmGroupTable</b> .
Security Model	Displays the default value as 3.
Security Name	Display the user name.
Vacm Group Name	Displays the Group name of the <b>VacmGroupTable</b>

### Buttons

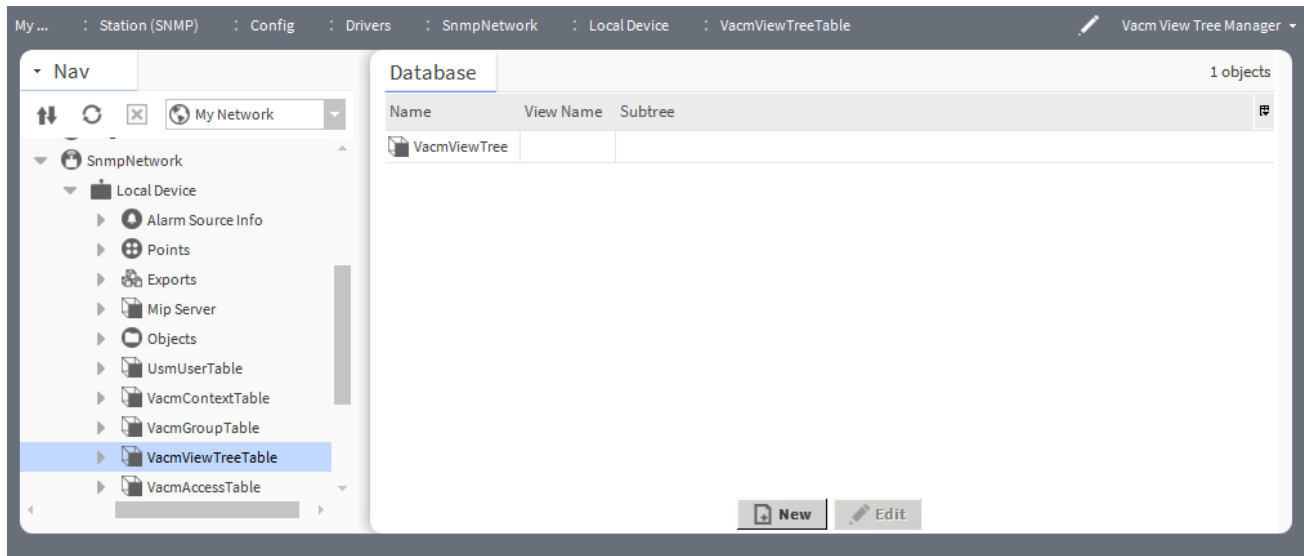
These buttons are available on the **SnmpNetwork's Vacm Group Table** view.

- **New** creates a new device record in the database.
- **Edit** opens the device's database record for updating.

## Vacm View Tree Manager View

The **Vacm View Tree** view is a default view of **VacmViewTreeTable** which is located under **Local Device**.

Figure 11 Vacm View Tree Manager View



To access this view, expand **Config→Drivers→SnmpNetwork→LocalDevice** and double —click **VacmViewTreeTable**.

### Columns

Column	Description
Name	Displays the name of <b>VacmViewTreeTable</b> .
View Name	Displays the user access.
Subtree	Displays the enterprise OID (Object Identifier) 1.3.6.1 information for the station.

### Buttons

These buttons are available on the **SnmpNetwork'sVacmViewTreeTable** view.

- **New** creates a new device record in the database.
- **Edit** opens the device's database record for updating.



# Chapter 6 Snmp Components

## Topics covered in this chapter

- ◆ SnmpNetwork
- ◆ SnmpDevice
- ◆ Snmp Alarm Device Ext
- ◆ Snmp Point Folder
- ◆ Snmp Point Device Ext
- ◆ Snmp Agent
- ◆ Snmp Agent Point Folder
- ◆ Snmp Agent Point Device Ext
- ◆ Snmp Agent Boolean Proxy Ext
- ◆ Snmp Agent Numeric Proxy Ext
- ◆ Snmp Agent String Proxy Ext
- ◆ Snmp Export Folder
- ◆ Snmp Export Table
- ◆ Snmp Enum Export
- ◆ Snmp Numeric Export
- ◆ Snmp Boolean Export
- ◆ Snmp Boolean Proxy Ext
- ◆ Snmp String Export
- ◆ MIB List Table
- ◆ Snmp Boolean Object Ext
- ◆ Snmp Numeric Object Ext
- ◆ Snmp String Object Ext
- ◆ Snmp Enum Object Ext
- ◆ Usm User table
- ◆ Vacm Context
- ◆ Vacm Access
- ◆ Vacm View Tree
- ◆ Vacm Group
- ◆ Snmp Device Folder
- ◆ Snmp Object Device Ext
- ◆ Snmp Boolean Proxy Ext
- ◆ Snmp Enum Proxy Ext
- ◆ Snmp String Proxy Ext
- ◆ Snmp Numeric Proxy Ext
- ◆ Snmp Sequence
- ◆ Snmp Table
- ◆ Snmp Table Row
- ◆ N Poll Scheduler
- ◆ Trap Table
- ◆ snmp-TrapType
- ◆ Snmp Recipient

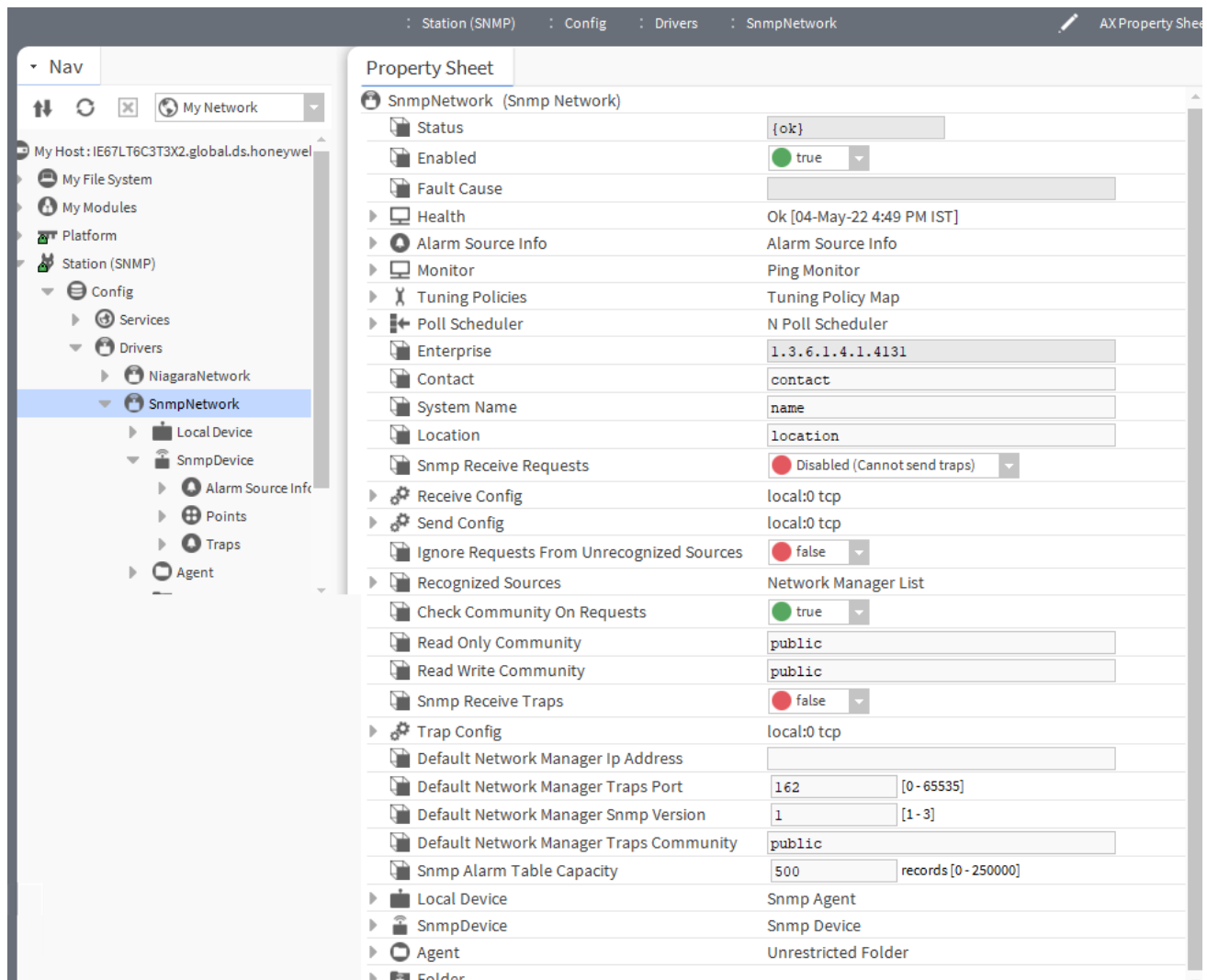
These topics provide help on common Snmp components.

Summary information is provided on components specific to the Snmp module.

## SnmpNetwork

SnmpNetwork represents a network of manageable Snmp devices. Can also be configured to handle sending and receiving Snmp trap messages, as well as respond to Snmp requests from outside managers. The SnmpNetwork is available in the nSnmp module. Bajadoc is available at [BSnmpNetwork.bajadoc](#).

Figure 12 SnmpNetwork Properties



To access this view, expand **Config→Drivers→SnmpNetwork**.

In addition to the standard properties (Status, Enabled and Fault Cause), these properties are unique to this component.

Property	Value	Description
Health	read-only	Reports the status of the network, device or component. This advisory information, including a time stamp, can help you recognize and troubleshoot problems but it provides no direct management controls.
Alarm Source Info	additional properties	Contains a set of properties for configuring and routing alarms when this component is the alarm source.
Monitor	additional properties	Configures a network's ping mechanism, which verifies network health. This includes verifying the health of all connected objects (typically, devices) by pinging each device at a repeated interval.



Property	Value	Description
Tuning Policies	additional properties	Selects a network tuning policy by name. This policy defines stale time and minimum and maximum update times.  During polling, the system uses the tuning policy to evaluate both write requests and the acceptability (freshness) of read requests.
Poll Scheduler	additional properties	Configures the frequency with which the driver polls points and devices.
Enterprise	numeric	Configures the enterprise OID (Object Identifier) 1.3.6.1.4.1.4131 information for the station.
Contact	text	Configures the system contact information for the station. This contact information is stored for the station and is read/write accessible via Snmp requests made to the station for OID 1.3.6.1.2.1.1.4.0.
System Name	text	Configures the system name information for the station. This name information is stored for the station and is read/write accessible via Snmp requests made to the station for OID 1.3.6.1.2.1.1.5.0.
Location	text	Configures the system location information for the station. This location information is stored for the station and is read/write accessible via Snmp requests made to the station for OID 1.3.6.1.2.1.1.6.0.
Snmp Received Requests	drop-down list	Configures the ability for Snmp request messages to be received by the station (only supports receiving GET, GETNEXT, or SET Snmp V1 or Snmp V2 messages) is enabled or disabled. When enabled, reception of Snmp request messages from external Snmp sources is possible (subject to the constraints placed on the reception of Snmp requests by the next six property fields). When disabled, reception of Snmp requests is not possible and any requests sent to it will be dropped.
Recieve Config	additional properties	Configures additional parameters to receive Snmp requests from external Snmp sources.
Send Config	additional properties	Configures additional parameters to send Snmp requests from external Snmp sources.
Ignore Requests From Unrecognized Sources	true or false (default)	Configures whether to enable or disable the ability for Snmp request messages to be received from only recognized sources (specified in the 'Recognized Sources' property). When set to true, a received Snmp request message is first checked for its source Ip, and if this source Ip matches any one of the source Ip addresses specified in the 'Recognized Sources' field, the request is processed. If the source Ip does not match, then the request is disregarded. When set to false, Snmp requests from any source Ip will be processed.
Recognized Sources	additional properties	Configures source Ip addresses to specify a list of recognized network managers. This list is used if the 'Snmp Receive Requests' and 'Only Accept Requests From Recognized Sources' properties are both enabled. It contains a list of source Ip addresses that are searched whenever an incoming Snmp request is received, and if the source of that request matches a

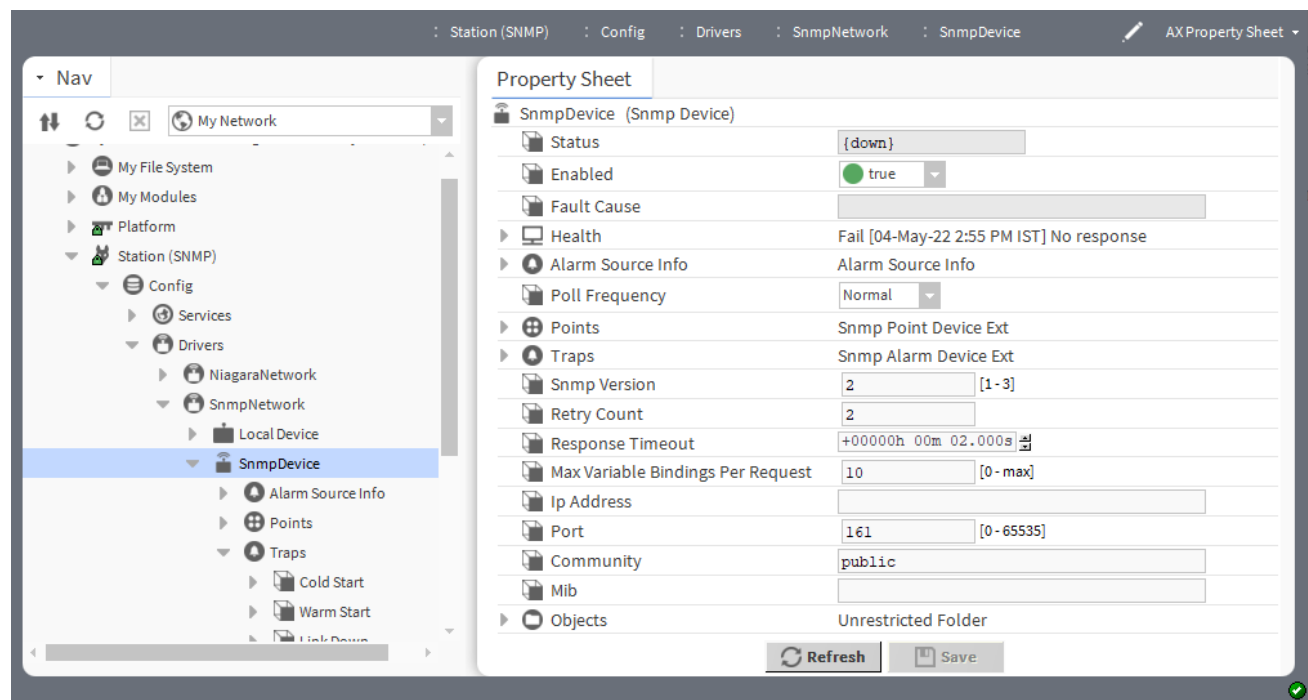
Property	Value	Description
		source Ip in this list, then the request will be processed. Otherwise, the request will be dropped. Useful for security purposes to ensure that the station only responds to known sources.
Check Community of Request	true (default) or false	Configures the community string field on a received Snmp request message before processing the request. When set to true, a received Snmp request message is first checked for its community string, and if this community string matches the community string specified in the 'Read Only Community' field (for GET or GETNEXT requests) or the 'Read Write Community' field (for GET, GETNEXT, or SET requests), the request is processed. If the community string does not match for the appropriate read/write access, then the request is disregarded. When set to false, Snmp requests with any community string field will be processed.
Read only Community	public (default)	Configures the community string field that incoming Snmp request messages must contain in order to process a read-only request (GET or GETNEXT request). The default value is public.
Read Write Community	public (default)	Configures the community string field that incoming Snmp request messages must contain in order to process a read-write request (GET, GETNEXT, or SET request). The default value is "public". <b>NOTE:</b> This is valid if the 'Check Community On Requests' property is enabled.
Snmp Receive Traps	true or false (default)	the ability for Snmp trap messages to be received by the station. When set to true, reception of Snmp trap messages from external Snmp devices is enabled, and any received trap messages will be routed to the Alarm Class specified by the 'Alarm Class For Received Traps' property, subject to the constraints of the 'Only Process Recognized Traps' property.
Trap Config	additional properties	Configures additional parameters for Trap configuration.
Default Network Manager IP Address	Ip Address	Configures the default Ip address of the network manager to use for reporting information.
Default Network Manager Traps Port	numeric (defaults to 162)	Configures the port to use for outgoing Snmp trap messages sent to the default network manager (i.e. the port on the default network manager where Snmp trap messages are received).
Default Network Manager Snmp Version	numeric	Configures the Snmp version whether it is Snmp V1 or Snmp V2.
Default Network Manager Traps Community	text (defaults to public)	Configures the community string field to use for outgoing Snmp trap messages (sent to the default network manager).

Property	Value	Description
Snmp Alarm table Capacity	numeric	Configures the maximum size of the Snmp Alarm Table. The default size is 500 records. Using this property, you can disable the Snmp Alarm Table by setting the value to zero. The purpose of limiting the table size is to conserve memory. You can also choose to disable Snmp alarm storage by choosing to set the SnmpRecipient's Snmp Alarm Table property to Do not Store Received.
Local Device	container	Added by default with Snmp network.

## SnmpDevice

**SnmpDevice** represents a remote Snmp device that is treated as an agent. The **SnmpDevice** is available in the nSnmp module. Bajadoc is available at [BSnmpDevice.bajadoc](#).

Figure 13 SnmpDevice Properties



To access this view, expand **Config**→**Drivers**→**SnmpNetwork**→**Snmp Device**.

In addition to the standard properties (Status, Enabled and Fault Cause), these properties are unique to this component.

Property	Value	Description
Health	read-only	Reports the status of the network, device or component. This advisory information, including a time stamp, can help you recognize and troubleshoot problems but it provides no direct management controls.
Alarm Source Info	additional properties	Contains a set of properties for configuring and routing alarms when this component is the alarm source.

Property	Value	Description
Poll Frequency	drop-down list (defaults to <code>Normal</code> )	Selects among three rates (Fast, Normal and Slow) to determine how often to query the component for its value. The network's Poll Service or Poll Scheduler defines these rates in hours, minutes and seconds. For example:  <code>Fast</code> may set polling frequency to every second. <code>Normal</code> may set poll frequency to every five seconds. <code>Slow</code> may set poll frequency to every 30 seconds.  This property applies to all proxy points.
Points	container	Contains the points associated with this device.
Traps	container	Contains the alarm associated with the device.
Snmp Version	number	Select the version of the Snmp protocol to use for communication with this <b>SnmpDevice</b>
Retry Count	number	Configures how many times to repeat a network read request, if no response is received before the response timeout interval elapses.
Response Timeout	hours, minutes, seconds, milliseconds (defaults to 2 seconds)	Configures the length of time before the system times out when interrogating a device on the network. Start by setting this value to a large number, such as 40 seconds. Then, reduce it depending on the number of devices and on the discovery performance.  <b>NOTE:</b> Baud rate also impacts performance especially if each device has a different baud rate.
Max Variable Bindings Per Request	number	Configures the maximum number of variable bindings to include in each Snmp request message sent to the Snmp device. The default value is 10, however, this value can be any integer value greater than or equal to 1.
IP Address	IP address	Identifies a device, which is connected to a network that uses the Internet Protocol for communication.
Port	numeric	Identifies the port number on the controller or computer used to connect to the network.  If using fox streaming, which uses the station to render the video stream, this port should be different from the station's fox port. If you are not using fox streaming, this port should be the same as the station's fox port.
Community	Text	Specifies the community string field to use for outgoing Snmp request messages sent to the <b>SnmpDevice</b> . The default value is public.
Mib	ord	Configure the Mib path.

## Snmp Alarm Device Ext

Snmp Alarm Device Ext contains the standard generic Snmp trap-types. These are: Cold Start, Warm Start, Link Down, Link Up, Authentication Failure, EGP Neighbor Loss.

Figure 14 Snmp Alarm Device Ext Properties

To access this view, expand **Config→Drivers→SnmpNetwork→SnmpDevice**, right-click **Traps→Views→AX Property Sheet**.

Property	Value	Description
Alarm Class	drop-down list	Defines alarm routing options and priorities. Typical alarm classes include <b>High</b> , <b>Medium</b> and <b>Low</b> . An alarm class of <b>Low</b> might send an email message, while an alarm class of <b>High</b> might trigger a text message to the department manager.
Last Received Time	read-only	Displays a timestamp of the last time (since station startup) that an Snmp trap message was received from the actual Snmp device represented by this <b>SnmpDevice</b> .
Last Received Trap	Text	This StringElement output displays the detailed message of the last received Snmp trap message for this <b>SnmpDevice</b> since station startup.
Ignore Unrecognized Traps	true or false (default)	This <b>true or false</b> option allows you to filter out any traps that are not recognizable based on the stored trap types for the source <b>SnmpDevice</b> . If this property is set to <b>true</b> , the received unrecognized trap message will be disregarded (no alarms generated). If this property is set to <b>false</b> , all received trap messages will be handled and routed to the specified <b>Alarm Class</b> whether they are recognizable or not.
Cold Start	additional properties	Configure additional parameters for trap types according to the requirement. <b>NOTE:</b> This applies to all the trap types.

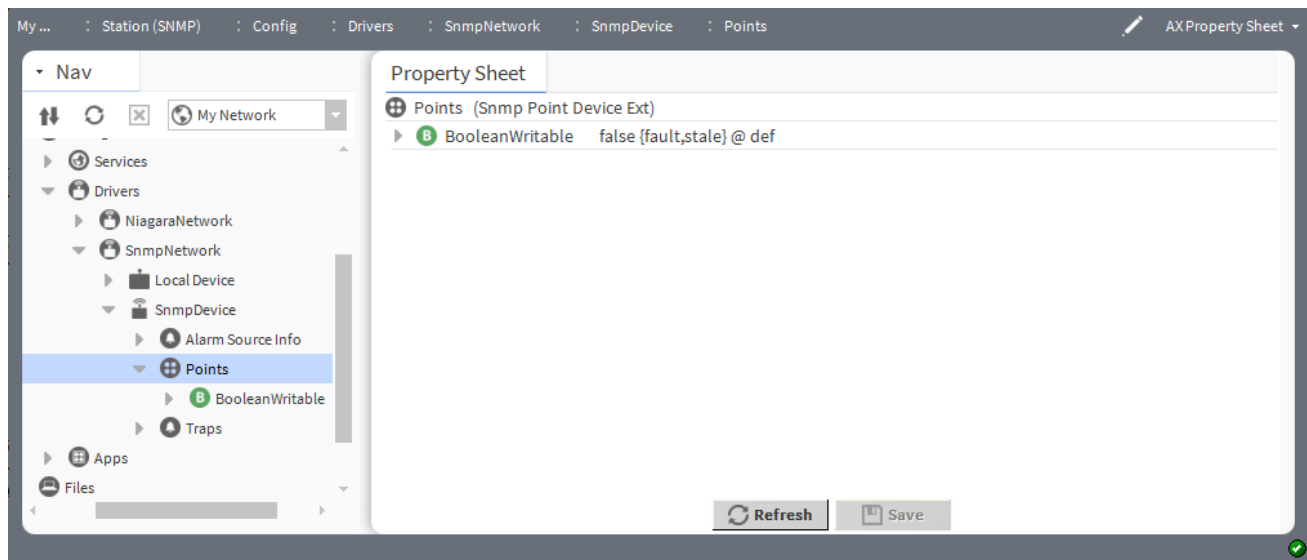
## Snmp Point Folder

Snmp Point Folder is the Snmp implementation of a folder under a **SnmpDevice Points** extension. You add such folders using the **New Folder** button in the **Snmp Point Manager** view of the Snmp Point Device extension. Each Snmp Point Folder has its own view (**Snmp Point Manager** view). The Snmp Point Folder is also available in the **nSnmp Palette**.

## Snmp Point Device Ext

Snmp Point Device Ext is the container for Snmp proxy points representing **SnmpDevice** data values.


Figure 15 Snmp Point Device Ext Property




To access this view, expand **Config→Drivers→SnmpNetwork→SnmpDevice**, right-click **Points→View-s→AX Property Sheet**.

This is a container for all the points.

## Snmp Agent

 Snmp Agent represents the local station as an Snmp agent device holding agent data that can be viewed and changed via Snmp from an outside Snmp manager. The Snmp Agent is available in the nSnmp module. Bajadoc is available at [BSnmpAgent.bajadoc](#).

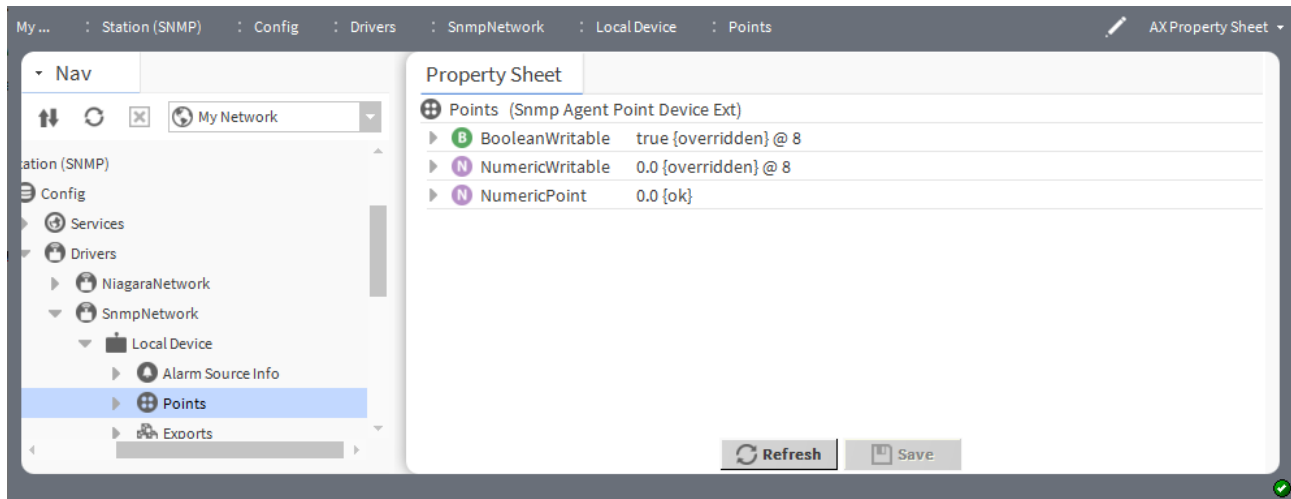
## Snmp Agent Point Folder

 Snmp Agent Point Folder is the Snmp implementation of a folder under a Snmp Agent's Points extension. You add such folders using the **New Folder** button in the view of the **Points** extension. Each Snmp Agent Point Folder has its own view. The Snmp Agent Point Folder is also available in the **nSnmp Palette**. Bajadoc is available at [BSnmpAgentPointFolder.bajadoc](#).

## Snmp Agent Point Device Ext

Snmp Agent Point Device Ext is the container for Snmp agent proxy points representing Snmp agent data values. The Snmp Agent Point Device Ext is available in the nSnmp module

Figure 16 Snmp Agent Point Device Ext property

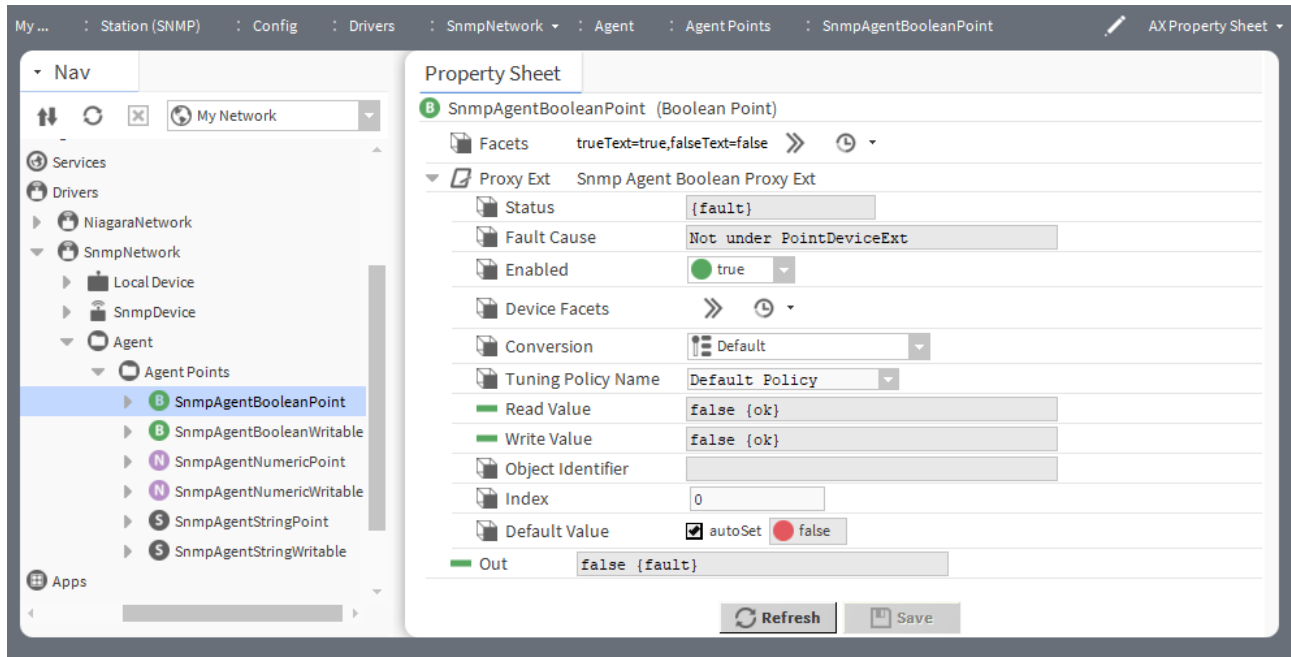


To access this view, expand **Config→Drivers→SnmpNetwork→Local Device**, right-click in the nav tree **Points→Views→AX Property Sheet**.

## Snmp Agent Boolean Proxy Ext

SNMP Agent Boolean Proxy Ext contains the information necessary to hold a boolean data value an outside SNMP Manager can set.

Figure 17 Snmp Agent Boolean Proxy Ext Properties



To access this view, expand **Config→Drivers→SnmpNetwork→Agents**, double-click **SnmpAgentBooleanPoint**.

In addition to the standard properties (Status, Enabled and Fault Cause), these properties are unique to this component.

Property	Value	Description
Facets	read-only	<p>Determine how values are formatted for display depending on the context and the type of data. For example, instead of the Boolean facets <code>trueText</code> and <code>falseText</code> you may want to display <b>ON</b> and <b>OFF</b>, <b>Access Granted</b> and <b>Access Denied</b> or <b>Locked</b> and <b>Unlocked</b>.</p> <p>You access facets by clicking an <b>Edit</b> button or a chevron <b>&gt;&gt;</b>. Both open an <b>Edit Facets</b> window.</p>
Device Facets	additional properties	<p>Configures additional parameters for the device proxy point facets for how the value should be displayed in Niagara. <b>Please confirm.</b></p>
Conversion	drop-down list	<p>Defines how the system converts proxy extension units to parent point units.</p> <p><code>Default</code> automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.</p> <p><b>NOTE:</b> In most cases, the standard <code>Default</code> conversion is best.</p> <p><code>Linear</code> applies to voltage input, resistive input and voltage output writable points. Works with linear-acting devices. You use the <code>Scale</code> and <code>Offset</code> properties to convert the output value to a unit other than that defined by device facets.</p> <p><code>Linear With Unit</code> is an extension to the existing linear conversion property. This specifies whether the unit conversion should occur on "Device Value" or "Proxy Value". The new linear with unit convertor, will have a property to indicate whether the unit conversion should take place before or after the scale/offset conversion.</p> <p><code>Reverse Polarity</code> applies only to Boolean input and relay output writable points. Reverses the logic of the hardware binary input or output.</p> <p><code>500 Ohm Shunt</code> applies to voltage input points only. It reads a 4-to-20mA sensor, where the <code>Ui</code> input requires a 500 ohm resistor wired across (shunting) the input terminals.</p> <p><code>Tabular Thermistor</code> applies to only a Thermistor input point and involves a custom resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Thermistor Type 3</code> applies to an Thermistor Input point, where this selection provides a "built-in" input resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Generic Tabular</code> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. <code>Generic Tabular</code> uses a lookup table method similar to the "Thermistor Tabular" conversion, but without predefined output units.</p>
Tuning Policy Name	drop-down list	<p>Configures network rules for evaluating both write requests to writable proxy points as well as the acceptable freshness of read requests.</p>

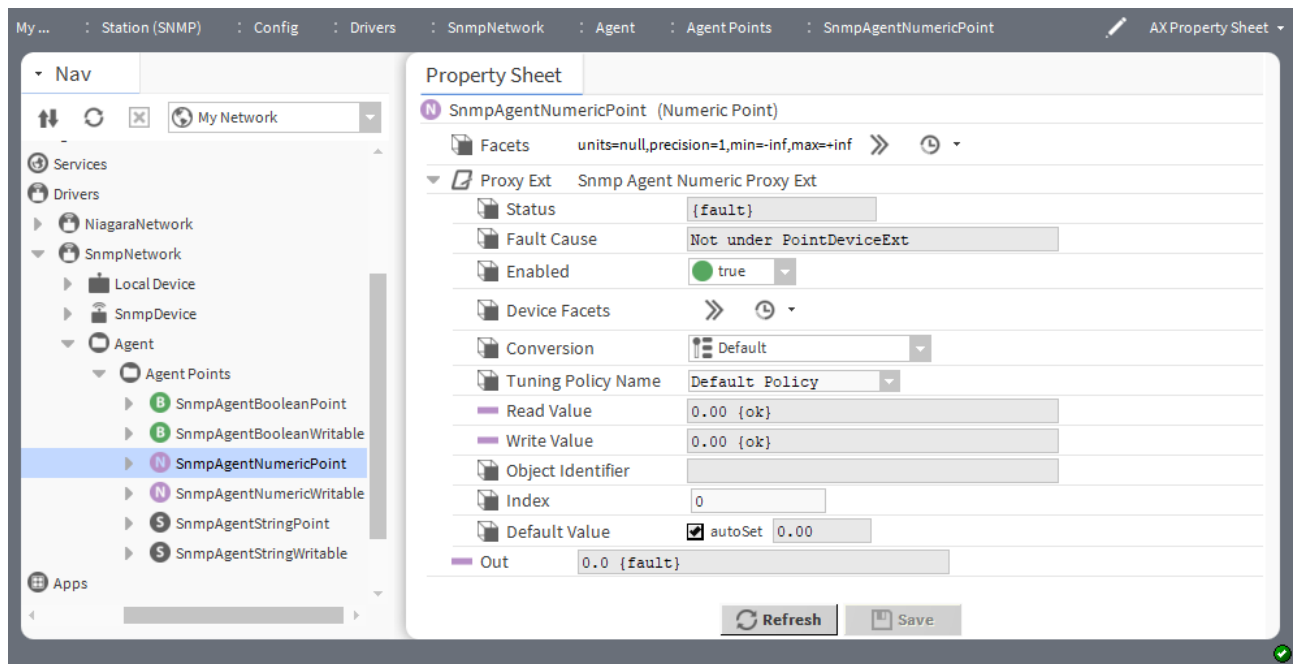


Property	Value	Description
Read Value	read-only	Displays the last value read from the device, expressed in device facets.
Write Value	read-only	Displays the last value written, using device facets.
Object Identifier	read-only	Displays the full OID to use for accessing the data value for this point from the Input Table (or Output Table) by an outside Snmp manager. Snmp GET or SET requests would use this full OID to access the value of the proxy point.
Index	number	Need Information
Out	read-only	Represents the point slot that contains the value to output.
Override Expiration	read-only	Reports how long a value that has been set manually (using an action) remains valid.
Min Active Time	hours minutes seconds (defaults to 00000h 00m 00s)	<p>Defines a minimum up time.</p> <p>This property works independently of Min Inactive Time. You typically use this property to prevent the short-cycling of equipment controlled by the point.</p> <p>The default disables the timer.</p>
Min Inactive Time	hours minutes seconds (defaults to 00000h 00m 00s)	<p>Defines a minimum down time.</p> <p>This property works independently of Min Active Time. You typically use this property to prevent the short-cycling of equipment controlled by the point.</p> <p>The default disables the timer.</p>
Set Min Active Time on Start	true or false (default)	Determines if the minimum inactive time applies at station start.

## Snmp Agent Numeric Proxy Ext

Snmp Agent Numeric Proxy Ext contains information necessary to hold a float (or integer) data value which can be set by an outside Snmp manager.

Figure 18 Snmp Agent Numeric Proxy Ext Properties



To access this view, expand **Config→Drivers→SnmpNetwork→Agents**, double-click **SnmpAgentNumericPoint**.

In addition to the standard properties (Status, Enabled and Fault Cause), these properties are unique to this component.

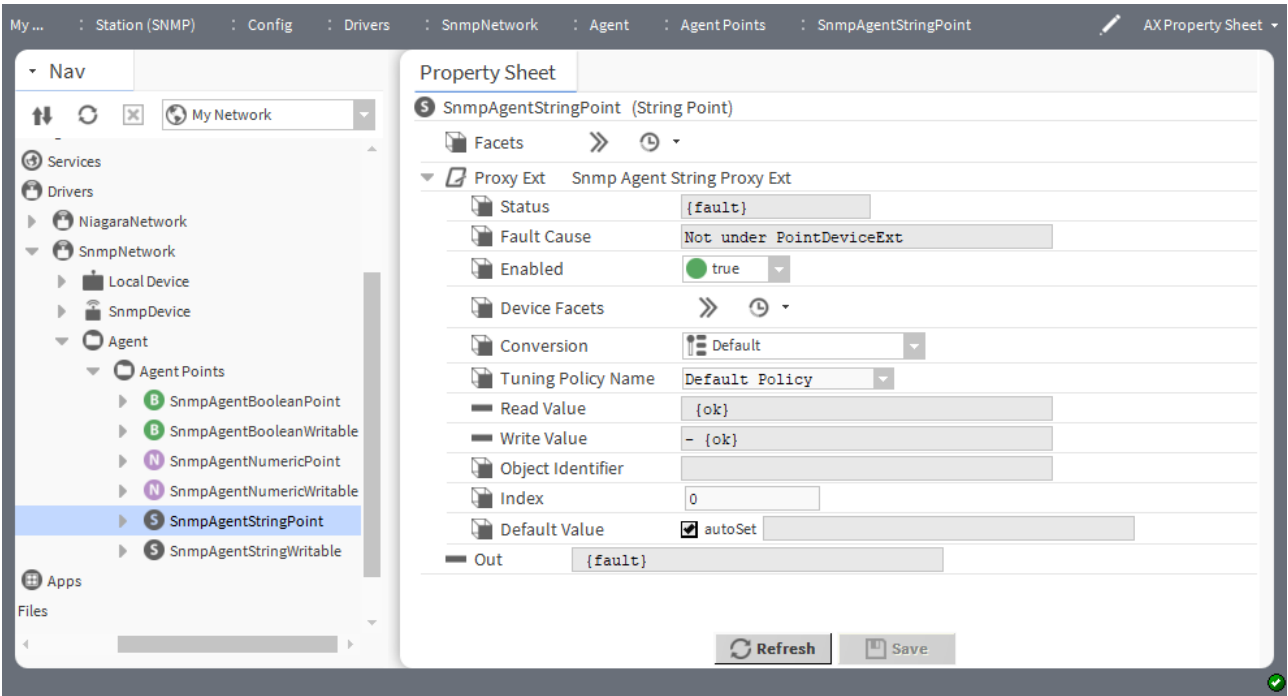
Property	Value	Description
Facets	read-only	Determine how values are formatted for display depending on the context and the type of data. For example, instead of the Boolean facets <code>trueText</code> and <code>falseText</code> you may want to display <b>ON</b> and <b>OFF</b> , <b>Access Granted</b> and <b>Access Denied</b> or <b>Locked</b> and <b>Unlocked</b> .  You access facets by clicking an <b>Edit</b> button or a chevron <b>&gt;&gt;</b> . Both open an <b>Edit Facets</b> window.
Device Facets	additional properties	Configures additional parameters for the device proxy point facets for how the value should be displayed in Niagara. <b>Please confirm.</b>
Conversion	drop-down list	Defines how the system converts proxy extension units to parent point units.  Default automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.  <b>NOTE:</b> In most cases, the standard <code>Default</code> conversion is best.  <code>Linear</code> applies to voltage input, resistive input and voltage output writable points. Works with linear-acting devices. You use the <code>Scale</code> and <code>Offset</code> properties to convert the output value to a unit other than that defined by device facets.  <code>Linear With Unit</code> is an extension to the existing linear conversion property. This specifies whether the unit conversion

Property	Value	Description
		<p>should occur on "Device Value" or "Proxy Value". The new linear with unit convertor, will have a property to indicate whether the unit conversion should take place before or after the scale/offset conversion.</p> <p><code>Reverse Polarity</code> applies only to Boolean input and relay output writable points. Reverses the logic of the hardware binary input or output.</p> <p><code>500 Ohm Shunt</code> applies to voltage input points only. It reads a 4-to-20mA sensor, where the Ui input requires a 500 ohm resistor wired across (shunting) the input terminals.</p> <p><code>Tabular Thermistor</code> applies to only a Thermistor input point and involves a custom resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Thermistor Type 3</code> applies to an Thermistor Input point, where this selection provides a "built-in" input resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Generic Tabular</code> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. Generic Tabular uses a lookup table method similar to the "Thermistor Tabular" conversion, but without predefined output units.</p>
Tuning Policy Name	drop-down list	Configures network rules for evaluating both write requests to writable proxy points as well as the acceptable freshness of read requests.
Read Value	read-only	Displays the last value read from the device, expressed in device facets.
Write Value	read-only	Displays the last value written, using device facets.
Object Identifier	read-only	Displays the full OID to use for accessing the data value for this point from the Input Table (or Output Table) by an outside Snmp manager. Snmp GET or SET requests would use this full OID to access the value of the proxy point.
Index	number	Need Information
Out	read-only	Represents the point slot that contains the value to output.
Default Value	number	Need Information

## Snmp Agent String Proxy Ext

Snmp Agent String Proxy Ext contains information necessary to hold string data value which can be set by an outside Snmp manager

Figure 19 Snmp Agent String Proxy Ext Properties



To access this view, expand **Config→Drivers→SnmpNetwork→Agents**, double-click **SnmpAgentStringPoint**.

In addition to the standard properties (Status, Enabled and Fault Cause), these properties are unique to this component.

Property	Value	Description
Facets	read-only	Determine how values are formatted for display depending on the context and the type of data. For example, instead of the Boolean facets <code>trueText</code> and <code>falseText</code> you may want to display <code>ON</code> and <code>OFF</code> , <code>Access Granted</code> and <code>Access Denied</code> or <code>Locked</code> and <code>Unlocked</code> .  You access facets by clicking an <b>Edit</b> button or a chevron <code>&gt;&gt;</code> . Both open an <b>Edit Facets</b> window.
Device Facets	additional properties	Configures additional parameters for the device proxy point facets for how the value should be displayed in Niagara. <b>Please confirm.</b>
Conversion	drop-down list	Defines how the system converts proxy extension units to parent point units.  Default automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.  <b>NOTE:</b> In most cases, the standard <code>Default</code> conversion is best.  Linear applies to voltage input, resistive input and voltage output writable points. Works with linear-acting devices. You use the <code>Scale</code> and <code>Offset</code> properties to convert the output value to a unit other than that defined by device facets.

Property	Value	Description
		<p><code>Linear With Unit</code> is an extension to the existing linear conversion property. This specifies whether the unit conversion should occur on "Device Value" or "Proxy Value". The new linear with unit convertor, will have a property to indicate whether the unit conversion should take place before or after the scale/offset conversion.</p> <p><code>Reverse Polarity</code> applies only to Boolean input and relay output writable points. Reverses the logic of the hardware binary input or output.</p> <p><code>500 Ohm Shunt</code> applies to voltage input points only. It reads a 4-to-20mA sensor, where the Ui input requires a 500 ohm resistor wired across (shunting) the input terminals.</p> <p><code>Tabular Thermistor</code> applies to only a Thermistor input point and involves a custom resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Thermistor Type 3</code> applies to an Thermistor Input point, where this selection provides a "built-in" input resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Generic Tabular</code> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. Generic Tabular uses a lookup table method similar to the "Thermistor Tabular" conversion, but without predefined output units.</p>
Tuning Policy Name	drop-down list	Configures network rules for evaluating both write requests to writable proxy points as well as the acceptable freshness of read requests.
Read Value	read-only	Displays the last value read from the device, expressed in device facets.
Write Value	read-only	Displays the last value written, using device facets.
Object Identifier	read-only	Displays the full OID to use for accessing the data value for this point from the Input Table (or Output Table) by an outside Snmp manager. Snmp GET or SET requests would use this full OID to access the value of the proxy point.
Index	number	Need Information
Out	read-only	Represents the point slot that contains the value to output.
Default Value	number	need information

## Snmp Export Folder

The Snmp Enum Export is a component that exports an enumerated value from an **SnmpNetwork**. **Local Device** to an SnmpNetwork Manager (Client). Add Snmp export components under the Snmp Export Table or under folders that can be nested under the Snmp Export Table. Use the **Snmp Export Manager** view to discover control points in your station and to add them to the Snmp Export Table

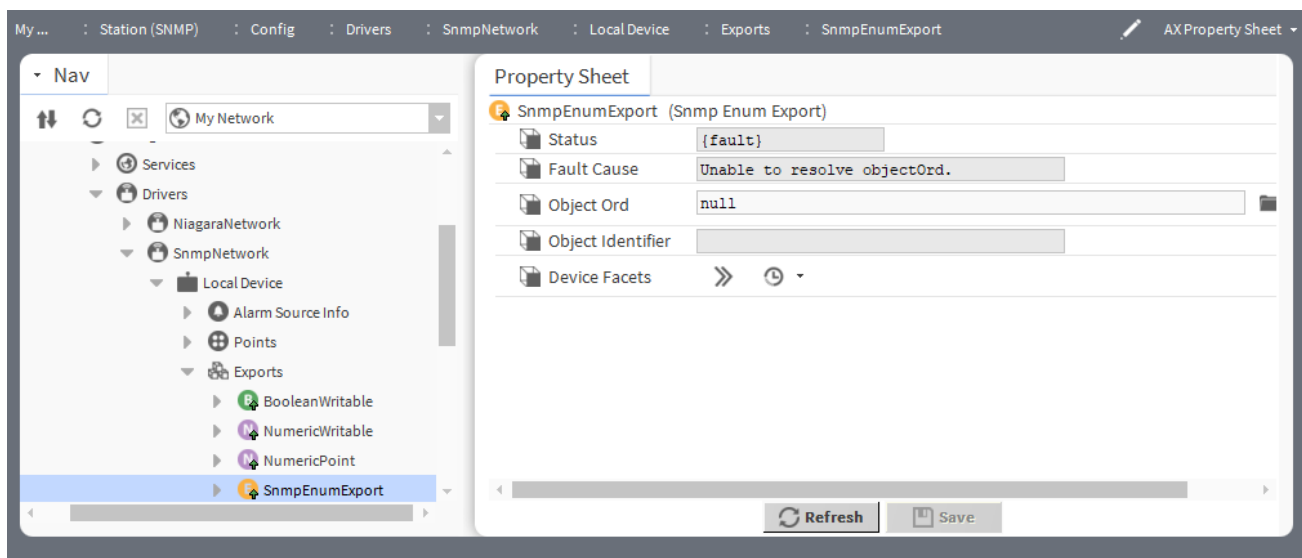
## Snmp Export Table

Snmp Export Table is a container for the Snmp export objects: **SnmpBooleanExport**, **SnmpEnumExport**, **SnmpNumericExport**, and **SnmpStringExport**. It can also contain nested folders for organizing export components. The default view of this component is the **Snmp Export Manager** view, where you can discover, add, and match to place export points in the Snmp Export Table.

## Snmp Enum Export

The Snmp Enum Export is a component that exports an enumerated value from an **SnmpNetwork Local Device** to an SnmpNetwork Manager (Client). Add Snmp export components under the Snmp Export Table or under folders that can be nested under the Snmp Export Table. Use the **Snmp Export Manager** view to discover control points in your station and to add them to the Snmp Export Table.

Figure 20 Snmp Enum Export Properties



To access this view, expand **Config**→**Drivers**→**SnmpNetwork**→**Local Device**→**Exports**, double-click **SnmpEnumExport**.

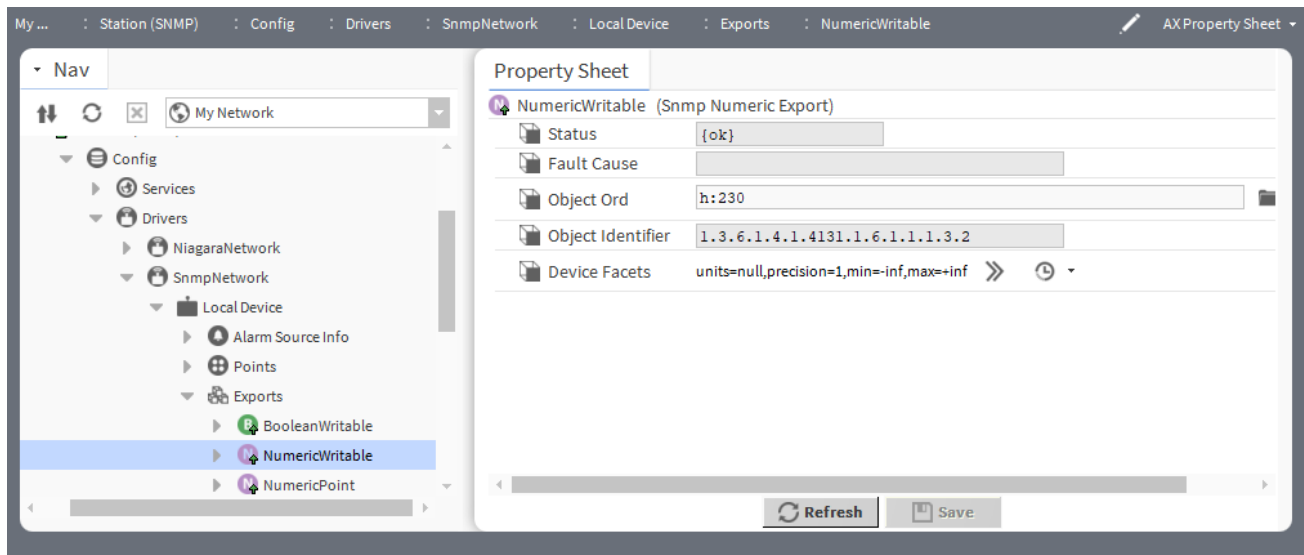
In addition to the standard properties (Status and Fault Cause), these properties are unique to this component.

Property	Value	Description
Object Ord	text	Specifies the OID of the actual Snmp device where the data is to be read from or written to.
Object Identifier	number	Displays the full OID to use for accessing the data value for this point from the Input Table (or Output Table) by an outside Snmp manager. Snmp GET or SET requests would use this full OID to access the value of the proxy point.
Device Facets	additional properties	configure additional parameters that represents the device proxy point facets for how the value should be displayed in Niagara.

## Snmp Numeric Export

The Snmp Numeric Export is a component that exports a numeric value from an **SnmpNetworkLocal Device** to an **SnmpNetwork Manager (Client)**. Add Snmp export components under the Snmp Export Table or under folders that can be nested under the Snmp Export Table. Use the **Snmp Export Manager** view to discover control points in your station and to add them to the Snmp Export Table

Figure 21 Snmp Numeric Export properties



To access this view, expand **Config**→**Drivers**→**SnmpNetwork**→**Local Device**→**Exports**, double-click **SnmpNumericExport**.

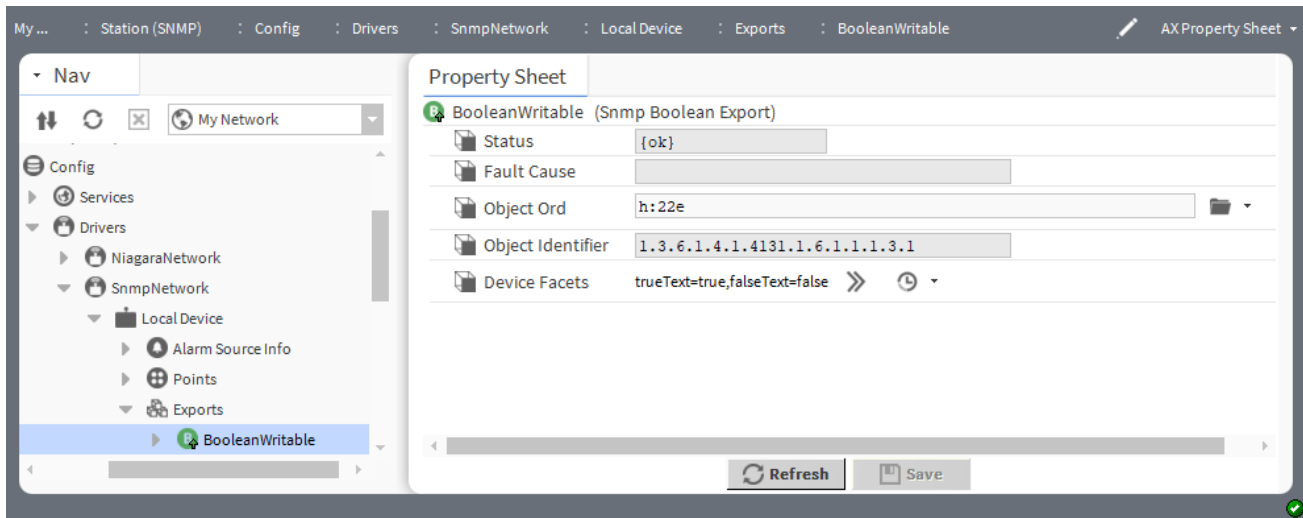
In addition to the standard properties (Status and Fault Cause), these properties are unique to this component.

Property	Value	Description
Object Ord	text	Specifies the OID of the actual Snmp device where the data is to be read from or written to.
Object Identifier	number	Displays the full OID to use for accessing the data value for this point from the Input Table (or Output Table) by an outside Snmp manager. Snmp GET or SET requests would use this full OID to access the value of the proxy point.
Device Facets	additional properties	configure additional parameters that represents the device proxy point facets for how the value should be displayed in Niagara.

## Snmp Boolean Export

The Snmp Boolean Export is a component that exports a boolean value from an **SnmpNetwork Local Device** to an **SnmpNetwork Manager (Client)**. Add Snmp export components under the Snmp Export Table or under folders that can be nested under the Snmp Export Table. Use the **Snmp Export Manager** view to discover control points in your station and to add them to the Snmp Export Table.

Figure 22 Snmp Boolean Export Properties



To access this view, expand **Config→Drivers→SnmpNetwork→Local Device→Exports**, double-click **Snmp Boolean Export**.

In addition to the standard properties (Status and Fault Cause), these properties are unique to this component.

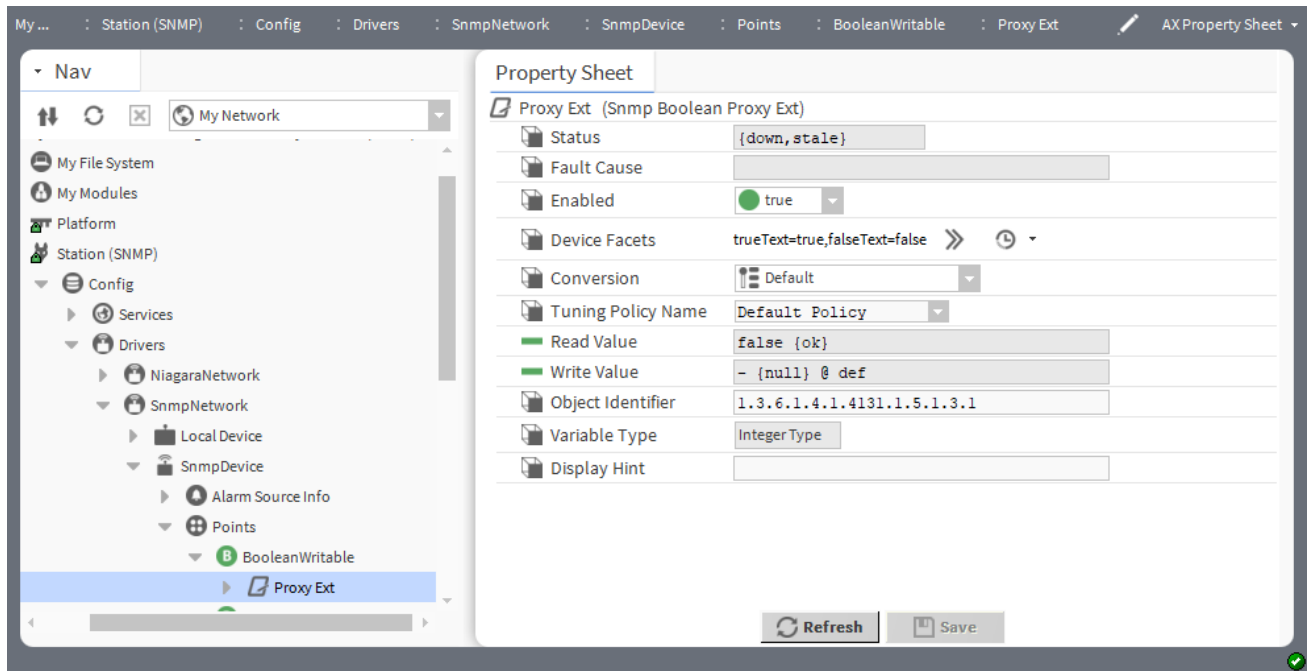
Property	Value	Description
Object Ord	text	Specifies the OID of the actual Snmp device where the data is to be read from or written to.
Object Identifier	number	Displays the full OID to use for accessing the data value for this point from the Input Table (or Output Table) by an outside Snmp manager. Snmp GET or SET requests would use this full OID to access the value of the proxy point.
Device Facets	additional properties	configure additional parameters that represents the device proxy point facets for how the value should be displayed in Niagara.

## Snmp Boolean Proxy Ext

Snmp Boolean Proxy Ext contains information necessary to read a boolean data value from an **SnmpDevice**. For numeric read Snmp data types, a value of zero is interpreted as a false, and anything else is interpreted as a true. For a read String Snmp data type, the string read will be compared with the true/false text for the point in order to determine the boolean value. The default is false (also used if cannot interpret). Each read-only proxy point that represents a readable boolean Snmp data quantity will have an Snmp Boolean Proxy Ext to describe how to read the point.



Figure 23 Snmp Boolean Proxy Ext Properties



To access this view, expand **Config→Drivers→SnmpNetwork→SnmpDevice→Points→Boolean Point**, double-click **Proxy Ext**.

In addition to the standard properties (Status, Enabled and Fault Cause), these properties are unique to this component.

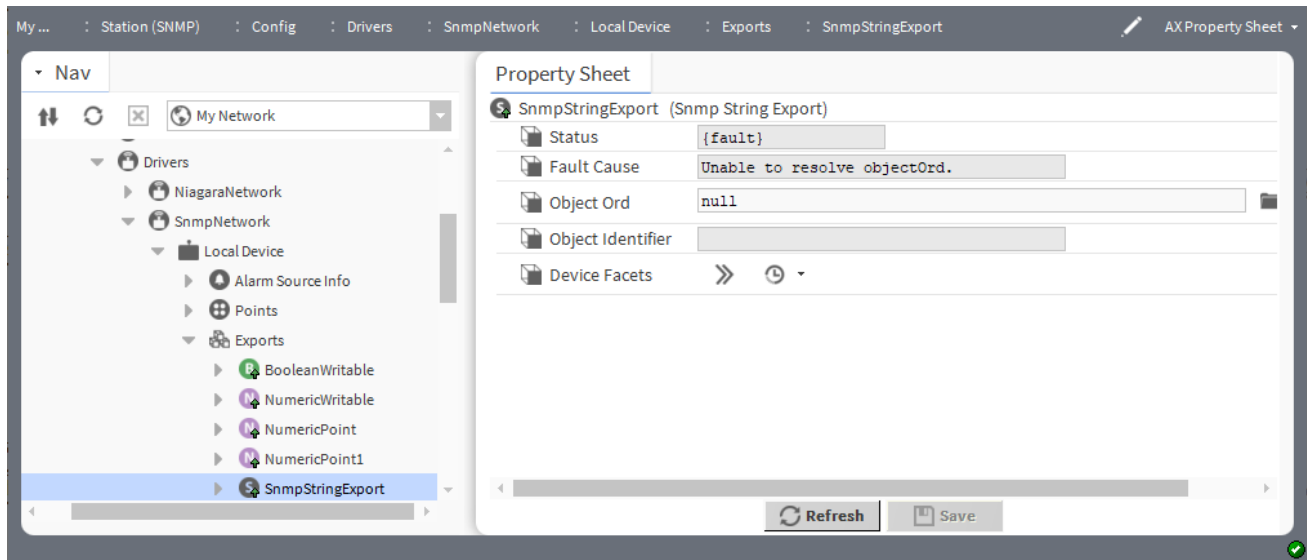
Property	Value	Description
Device Facets	additional properties	Configures additional parameters for the device proxy point facets for how the value should be displayed in Niagara. <b>Please confirm.</b>
Conversion	drop-down list	<p>Defines how the system converts proxy extension units to parent point units.</p> <p>Default automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.</p> <p><b>NOTE:</b> In most cases, the standard Default conversion is best.</p> <p>Linear applies to voltage input, resistive input and voltage output writable points. Works with linear-acting devices. You use the Scale and Offset properties to convert the output value to a unit other than that defined by device facets.</p> <p>Linear With Unit is an extension to the existing linear conversion property. This specifies whether the unit conversion should occur on "Device Value" or "Proxy Value". The new linear with unit convertor, will have a property to indicate whether the unit conversion should take place before or after the scale/offset conversion.</p> <p>Reverse Polarity applies only to Boolean input and relay output writable points. Reverses the logic of the hardware binary input or output.</p>

Property	Value	Description
		<p><b>500 Ohm Shunt</b> applies to voltage input points only. It reads a 4-to-20mA sensor, where the Ui input requires a 500 ohm resistor wired across (shunting) the input terminals.</p> <p><b>Tabular Thermistor</b> applies to only a Thermistor input point and involves a custom resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><b>Thermistor Type 3</b> applies to an Thermistor Input point, where this selection provides a "built-in" input resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><b>Generic Tabular</b> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. Generic Tabular uses a lookup table method similar to the "Thermistor Tabular" conversion, but without predefined output units.</p>
Tuning Policy Name	drop-down list	Configures network rules for evaluating both write requests to writable proxy points as well as the acceptable freshness of read requests.
Read Value	read-only	Displays the last value read from the device, expressed in device facets.
Write Value	read-only	Displays the last value written, using device facets.
Object Identifier	read-only	Displays the full OID to use for accessing the data value for this point from the Input Table (or Output Table) by an outside Snmp manager. Snmp GET or SET requests would use this full OID to access the value of the proxy point.
Variable Type		Need Information
Display Hint		Need Information

## Snmp String Export

The Snmp String Export is a component that exports a string value from an **SnmpNetworkLocal Device** to an **SnmpNetwork Manager (Client)**. Add Snmp export components under the Snmp Export Table or under folders that can be nested under the Snmp Export Table. Use the **Snmp Export Manager** view to discover control points in your station and to add them to the Snmp Export Table.

Figure 24 Snmp String Export Properties



To access this view, expand **Config→Drivers→SnmpNetwork→Local Device→Exports**, double-click **SnmpStringExport**.

In addition to the standard properties (Status and Fault Cause), these properties are unique to this component.

Property	Value	Description
Object Ord	text	Specifies the OID of the actual Snmp device where the data is to be read from or written to.
Object Identifier	number	Displays the full OID to use for accessing the data value for this point from the Input Table (or Output Table) by an outside Snmp manager. Snmp GET or SET requests would use this full OID to access the value of the proxy point.
Device Facets	additional properties	configure additional parameters that represents the device proxy point facets for how the value should be displayed in Niagara.

## MIB List Table

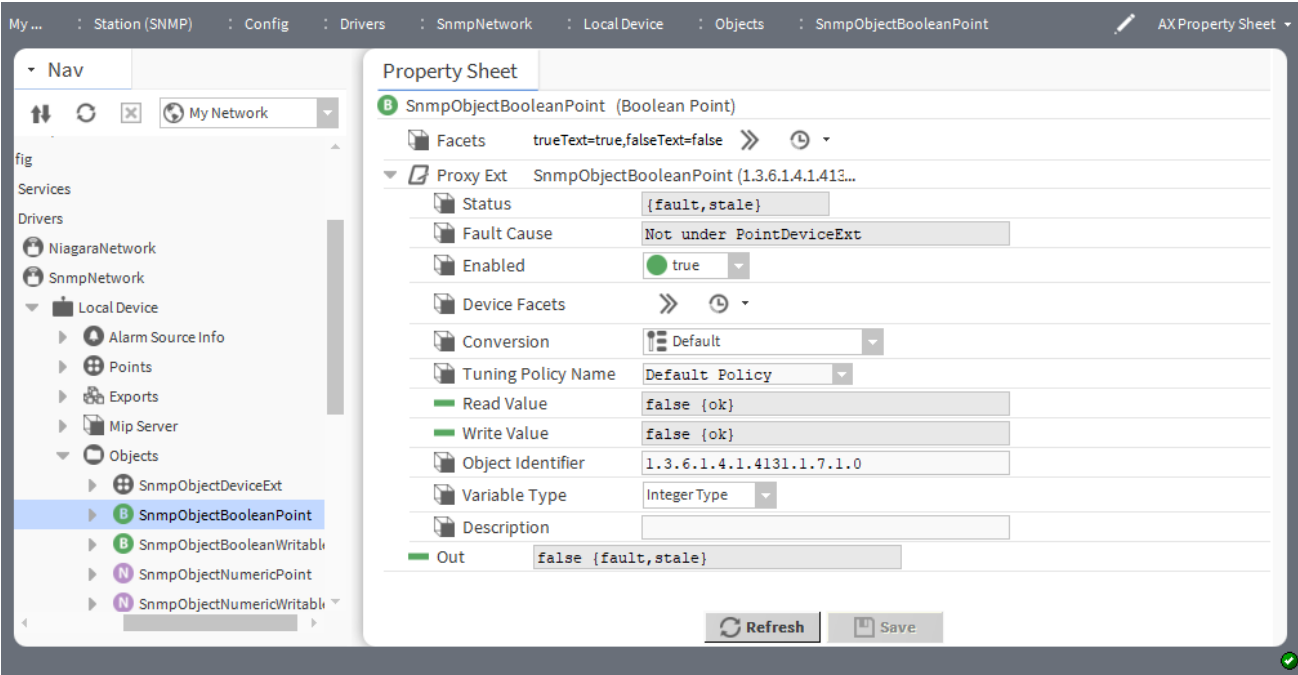
The **MIB List Table** captures information about MIB entries within SnmpDevices.

The **MIB List Table** is available in the nSnmp module. Bajadoc is available at `BMIBListTable.bajadoc`.

## Snmp Boolean Object Ext

An Snmp Boolean Object Ext is the container for **SnmpObjectBooleanPoint** and **SnmpObjectBooleanWritable** objects. The Snmp Boolean Object Ext is available in the nSnmp module.

Figure 25 Snmp Boolean Object Ext Properties



To access this view, expand **Config→Drivers→SnmpNetwork→Local Device→Objects→SnmpObjectBooleanPoint**, double-click **Proxy Ext**

In addition to the standard properties (Status and Fault Cause), these properties are unique to this component.

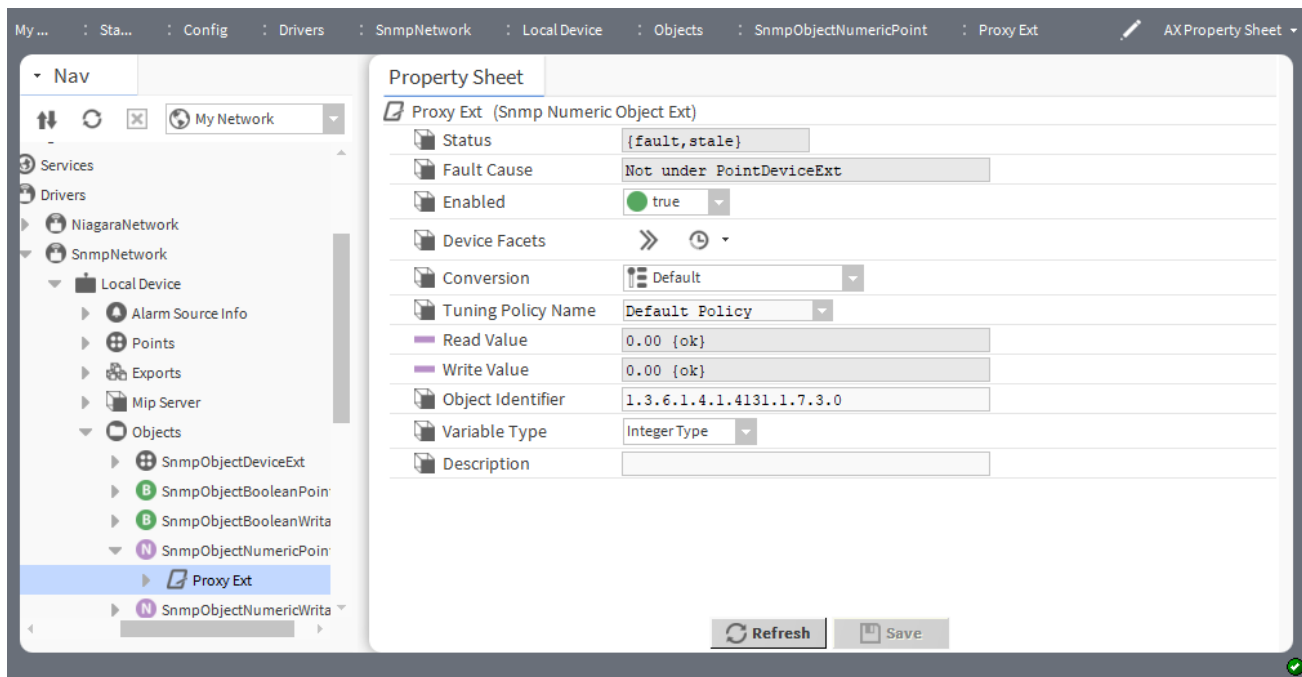
Property	Value	Description
Device Facets	additional properties	Configures additional parameters for the device proxy point facets for how the value should be displayed in Niagara. Please confirm.
Conversion	drop-down list	<p>Defines how the system converts proxy extension units to parent point units.</p> <p>Default automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.</p> <p><b>NOTE:</b> In most cases, the standard Default conversion is best.</p> <p>Linear applies to voltage input, resistive input and voltage output writable points. Works with linear-acting devices. You use the Scale and Offset properties to convert the output value to a unit other than that defined by device facets.</p> <p>Linear With Unit is an extension to the existing linear conversion property. This specifies whether the unit conversion should occur on "Device Value" or "Proxy Value". The new linear with unit convertor, will have a property to indicate whether the unit conversion should take place before or after the scale/offset conversion.</p> <p>Reverse Polarity applies only to Boolean input and relay output writable points. Reverses the logic of the hardware binary input or output.</p>

Property	Value	Description
		<p><b>500 Ohm Shunt</b> applies to voltage input points only. It reads a 4-to-20mA sensor, where the Ui input requires a 500 ohm resistor wired across (shunting) the input terminals.</p> <p><b>Tabular Thermistor</b> applies to only a Thermistor input point and involves a custom resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><b>Thermistor Type 3</b> applies to an Thermistor Input point, where this selection provides a "built-in" input resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><b>Generic Tabular</b> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. Generic Tabular uses a lookup table method similar to the "Thermistor Tabular" conversion, but without predefined output units.</p>
Tuning Policy Name	drop-down list	Configures network rules for evaluating both write requests to writable proxy points as well as the acceptable freshness of read requests.
Read Value	read-only	Displays the last value read from the device, expressed in device facets.
Write Value	read-only	Displays the last value written, using device facets.
Object Identifier	read-only	Displays the full OID to use for accessing the data value for this point from the Input Table (or Output Table) by an outside Snmp manager. Snmp GET or SET requests would use this full OID to access the value of the proxy point.
Variable Type		Need Information
Description		Need Information
Out	read-only	Represents the point slot that contains the value to output.

## Snmp Numeric Object Ext

An Snmp Numeric Object Ext is the container for SnmpObjectNumericPoint and SnmpObjectNumericWritable objects. module. The Snmp Numeric Object Ext is available in the nSnmp.

Figure 26 Snmp Numeric Object Ext Properties



To access this view, expand **Config→Drivers→SnmpNetwork→Local Device→Objects→SnmpObjectNumericPoint**, double-click **Proxy Ext**

In addition to the standard properties (Status and Fault Cause), these properties are unique to this component.

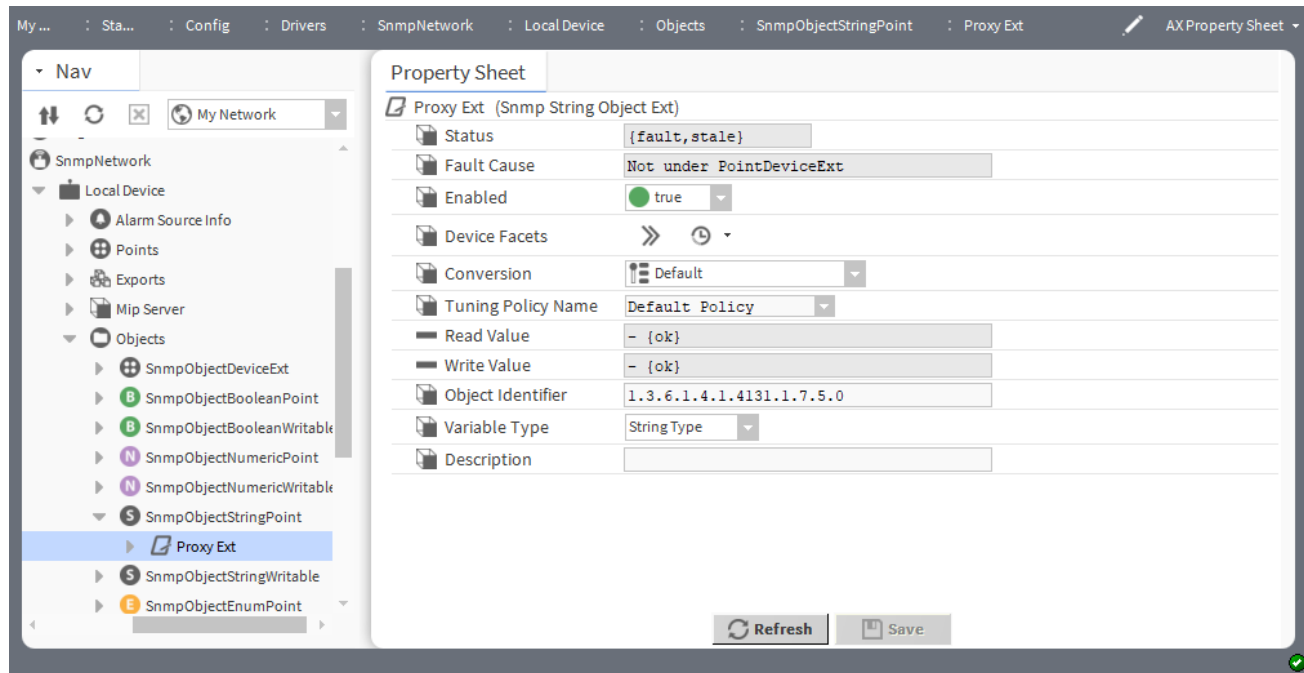
Property	Value	Description
Device Facets	additional properties	Configures additional parameters for the device proxy point facets for how the value should be displayed in Niagara. <b>Please confirm.</b>
Conversion	drop-down list	<p>Defines how the system converts proxy extension units to parent point units.</p> <p><b>Default</b> automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.</p> <p><b>NOTE:</b> In most cases, the standard <b>Default</b> conversion is best.</p> <p><b>Linear</b> applies to voltage input, resistive input and voltage output writable points. Works with linear-acting devices. You use the <b>Scale</b> and <b>Offset</b> properties to convert the output value to a unit other than that defined by device facets.</p> <p><b>Linear With Unit</b> is an extension to the existing linear conversion property. This specifies whether the unit conversion should occur on "Device Value" or "Proxy Value". The new linear with unit convertor, will have a property to indicate whether the unit conversion should take place before or after the scale/offset conversion.</p> <p><b>Reverse Polarity</b> applies only to Boolean input and relay output writable points. Reverses the logic of the hardware binary input or output.</p>

Property	Value	Description
		<p><b>500 Ohm Shunt</b> applies to voltage input points only. It reads a 4-to-20mA sensor, where the Ui input requires a 500 ohm resistor wired across (shunting) the input terminals.</p> <p><b>Tabular Thermistor</b> applies to only a Thermistor input point and involves a custom resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><b>Thermistor Type 3</b> applies to an Thermistor Input point, where this selection provides a "built-in" input resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><b>Generic Tabular</b> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. Generic Tabular uses a lookup table method similar to the "Thermistor Tabular" conversion, but without predefined output units.</p>
Tuning Policy Name	drop-down list	Configures network rules for evaluating both write requests to writable proxy points as well as the acceptable freshness of read requests.
Read Value	read-only	Displays the last value read from the device, expressed in device facets.
Write Value	read-only	Displays the last value written, using device facets.
Object Identifier	read-only	Displays the full OID to use for accessing the data value for this point from the Input Table (or Output Table) by an outside Snmp manager. Snmp GET or SET requests would use this full OID to access the value of the proxy point.
Variable Type		Need Information
Description		Need Information

## Snmp String Object Ext

An Snmp String Object Ext is the container for `SnmpObjectStringPoint` and `SnmpObjectStringWritable` objects. The Snmp String Object Ext is available in the `nSnmp` module.

Figure 27 Snmp String Object Ext Properties



To access this view, expand **Config**→**Drivers**→**SnmpNetwork**→**Local Device**→**Objects**→**SnmpObjectStringPoint**, double-click **Proxy Ext**

Property	Value	Description
Device Facets	additional properties	Configures additional parameters for the device proxy point facets for how the value should be displayed in Niagara. <b>Please confirm.</b>
Conversion	drop-down list	<p>Defines how the system converts proxy extension units to parent point units.</p> <p><b>Default</b> automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.</p> <p><b>NOTE:</b> In most cases, the standard <b>Default</b> conversion is best.</p> <p><b>Linear</b> applies to voltage input, resistive input and voltage output writable points. Works with linear-acting devices. You use the <b>Scale</b> and <b>Offset</b> properties to convert the output value to a unit other than that defined by device facets.</p> <p><b>Linear With Unit</b> is an extension to the existing linear conversion property. This specifies whether the unit conversion should occur on "Device Value" or "Proxy Value". The new linear with unit convertor, will have a property to indicate whether the unit conversion should take place before or after the scale/offset conversion.</p> <p><b>Reverse Polarity</b> applies only to Boolean input and relay output writable points. Reverses the logic of the hardware binary input or output.</p> <p><b>500 Ohm Shunt</b> applies to voltage input points only. It reads a 4-to-20mA sensor, where the Ui input requires a 500 ohm resistor wired across (shunting) the input terminals.</p>

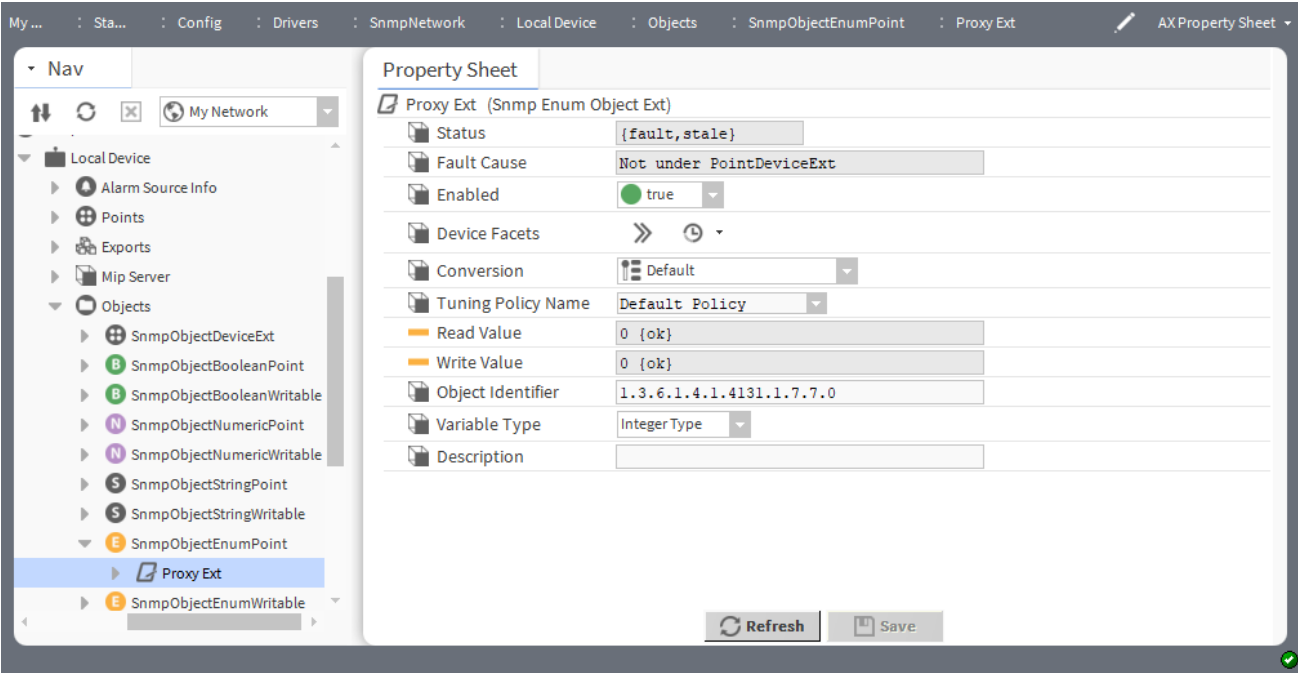


Property	Value	Description
		<p><code>Tabular Thermistor</code> applies to only a Thermistor input point and involves a custom resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Thermistor Type 3</code> applies to an Thermistor Input point, where this selection provides a “built-in” input resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Generic Tabular</code> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. Generic Tabular uses a lookup table method similar to the “Thermistor Tabular” conversion, but without predefined output units.</p>
Tuning Policy Name	drop-down list	Configures network rules for evaluating both write requests to writable proxy points as well as the acceptable freshness of read requests.
Read Value	read-only	Displays the last value read from the device, expressed in device facets.
Write Value	read-only	Displays the last value written, using device facets.
Object Identifier	read-only	Displays the full OID to use for accessing the data value for this point from the Input Table (or Output Table) by an outside Snmp manager. Snmp GET or SET requests would use this full OID to access the value of the proxy point.
Variable Type		Need Information
Description		Need Information

## Snmp Enum Object Ext

An Snmp Enum Object Ext is the container for **SnmpObjectEnumPoint** and **SnmpObjectEnumWritable** objects. The Snmp Enum Object Ext is available in the nSnmp module.

Figure 28 Snmp Enum Object Ext Properties



To access this view, expand **Config→Drivers→SnmpNetwork→Local Device→Objects→SnmpObjectEnumPoint**, double-click **Proxy Ext**

In addition to the standard properties (Status and Fault Cause), these properties are unique to this component.

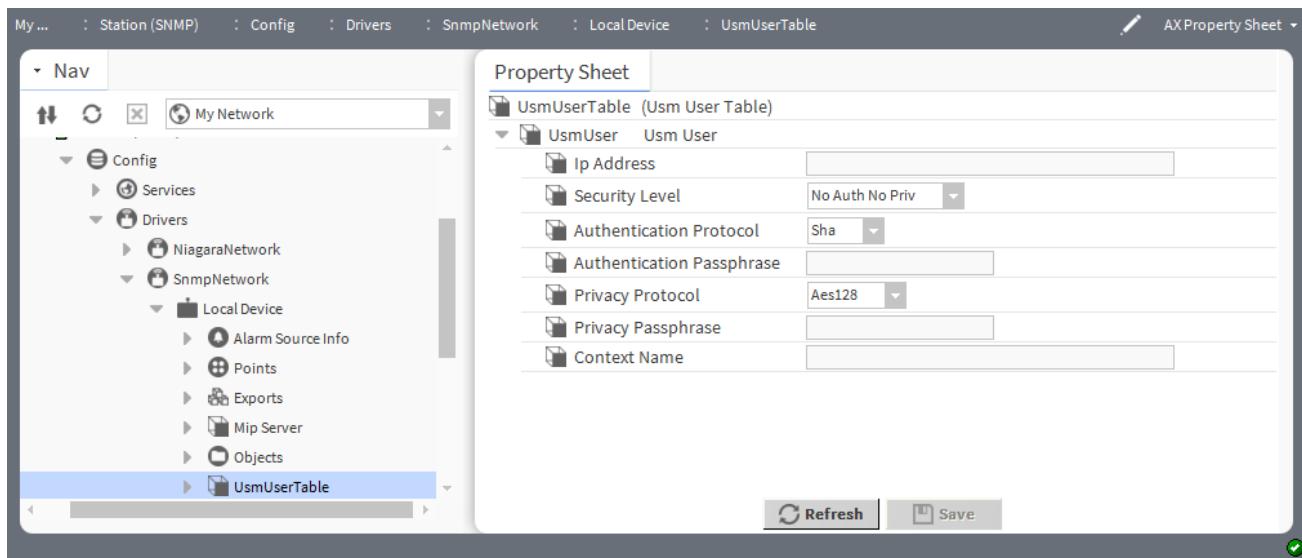
Property	Value	Description
Device Facets	additional properties	Configures additional parameters for the device proxy point facets for how the value should be displayed in Niagara. <b>Please confirm.</b>
Conversion	drop-down list	<p>Defines how the system converts proxy extension units to parent point units.</p> <p>Default automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.</p> <p><b>NOTE:</b> In most cases, the standard Default conversion is best.</p> <p>Linear applies to voltage input, resistive input and voltage output writable points. Works with linear-acting devices. You use the Scale and Offset properties to convert the output value to a unit other than that defined by device facets.</p> <p>Linear With Unit is an extension to the existing linear conversion property. This specifies whether the unit conversion should occur on "Device Value" or "Proxy Value". The new linear with unit convertor, will have a property to indicate whether the unit conversion should take place before or after the scale/offset conversion.</p> <p>Reverse Polarity applies only to Boolean input and relay output writable points. Reverses the logic of the hardware binary input or output.</p>

Property	Value	Description
		<p><b>500 Ohm Shunt</b> applies to voltage input points only. It reads a 4-to-20mA sensor, where the Ui input requires a 500 ohm resistor wired across (shunting) the input terminals.</p> <p><b>Tabular Thermistor</b> applies to only a Thermistor input point and involves a custom resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><b>Thermistor Type 3</b> applies to an Thermistor Input point, where this selection provides a "built-in" input resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><b>Generic Tabular</b> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. Generic Tabular uses a lookup table method similar to the "Thermistor Tabular" conversion, but without predefined output units.</p>
Tuning Policy Name	drop-down list	Configures network rules for evaluating both write requests to writable proxy points as well as the acceptable freshness of read requests.
Read Value	read-only	Displays the last value read from the device, expressed in device facets.
Write Value	read-only	Displays the last value written, using device facets.
Object Identifier	read-only	Displays the full OID to use for accessing the data value for this point from the Input Table (or Output Table) by an outside Snmp manager. Snmp GET or SET requests would use this full OID to access the value of the proxy point.
Variable Type		Need Information
Description		Need Information

## Usm User table

A Usm user is available in the nSnmp module. The Usm user is a row of the **UsmUserTable**. The Usm user row contains an object for each element that is represented in the **UsmUserTable**.

Figure 29 Usm User Table Properties



To access this view, expand **Config→Drivers→SnmpNetwork→Local Device**, right-click **UsmUserTable→Views→AX Property Sheet**.

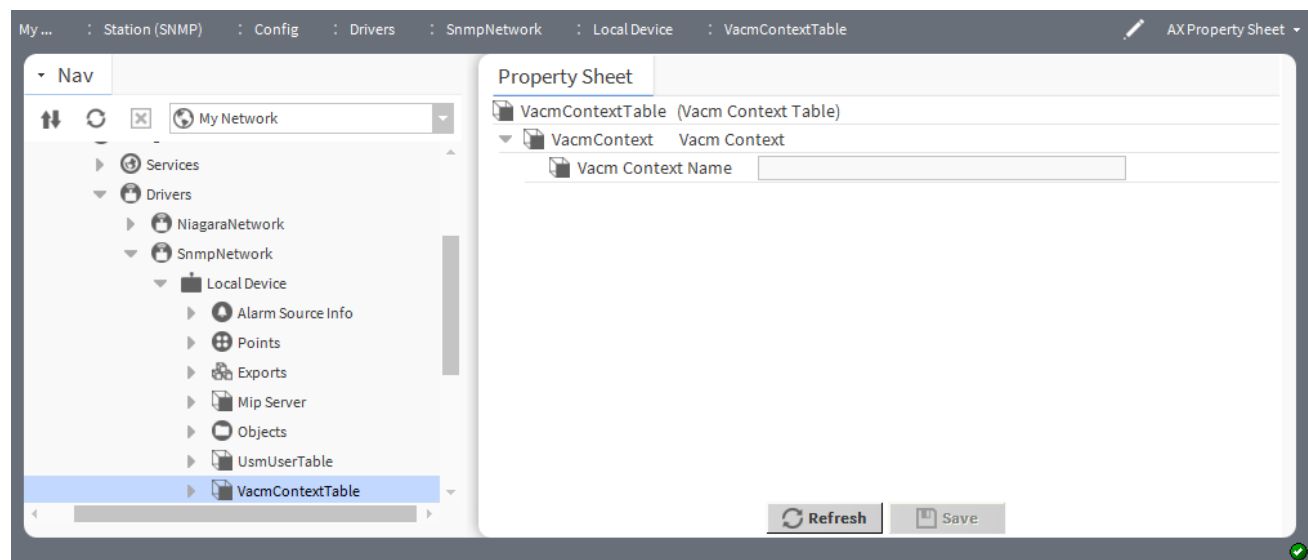
Property	Value	Description
IP Address	text	Reports the IP address of the device.
Security Level	drop-down list	<p>The security level value in this field restricts or allows access and notifications as described below:</p> <p><b>No Auth No Priv:</b> This option specifies communication without authentication or privacy. When you select this level, it is not necessary to enter any authentication or privacy inputs. A User with security level <b>No Auth No Priv</b> and context name as <b>noAuth</b> is called <b>noAuthUser</b>.</p> <p><b>Auth No Priv:</b> This option represents the communication with authentication and without privacy. You have to select the applicable Authentication Protocol and enter an <b>Authentication Passphrase</b> in the <b>UsmUserTable</b>. The protocols used for Authentication is SHA (Secure Hash Algorithm). Users with security level <b>Auth No Priv</b> and context name as <b>auth</b> is called as <b>authUser</b>.</p> <p><b>Auth Priv:</b> This option represents the communication with authentication and privacy. User has to select the SHA <b>Authentication Protocol</b> for authentication and enter an <b>Authentication Passphrase</b>. Also select the DES (Data Encryption Standard) and AES (Advanced Encryption Standard) <b>Privacy Protocol</b> for privacy and enter a <b>Privacy Passphrase</b> in <b>UsmUserTable</b>. Users with security level <b>Auth Priv</b> and context name as <b>priv</b> is called as <b>privUser</b>.</p>
Authentication Protocol	drop-down list	This property allows you to select the Authentication Protocol HMAC-SHA-96. It is used to check the integrity and to authenticate the SNMPv3 message sent on the behalf of this user.
Authentication Passphrase	text	This property allows user to set the passphrase. This is not applicable for No Auth No Priv security level.

Property	Value	Description
Privacy Protocol	drop-down list	This property allows user to select privacy protocol DES, Aes128, Aes192 or Aes256 to protect the SNMPv3 message from disclosure. This is not applicable for No Auth No Priv and Auth No Priv security levels.
Privacy Passphrase	text	This property allows user to set the passphrase. This is not applicable for No Auth No Priv and Auth No Priv security levels.
Context Name	text	This property represents the Context Name. The Context Name specifies where the desired management object is to be found. The Context Name of the UsmUserTable must match with the entry in VacmContextTable.

## Vacm Context

A Vacm Context is available in the nSnmp module. A Vacm Context is a row of the **VacmContextTable**. The Vacm Context row contains an object for each element that is represented in the **VacmContextTable**. User can edit the **VacmContextTable** properties by double clicking on the Vacm Context row.

Figure 30 Vacm Context Table Properties



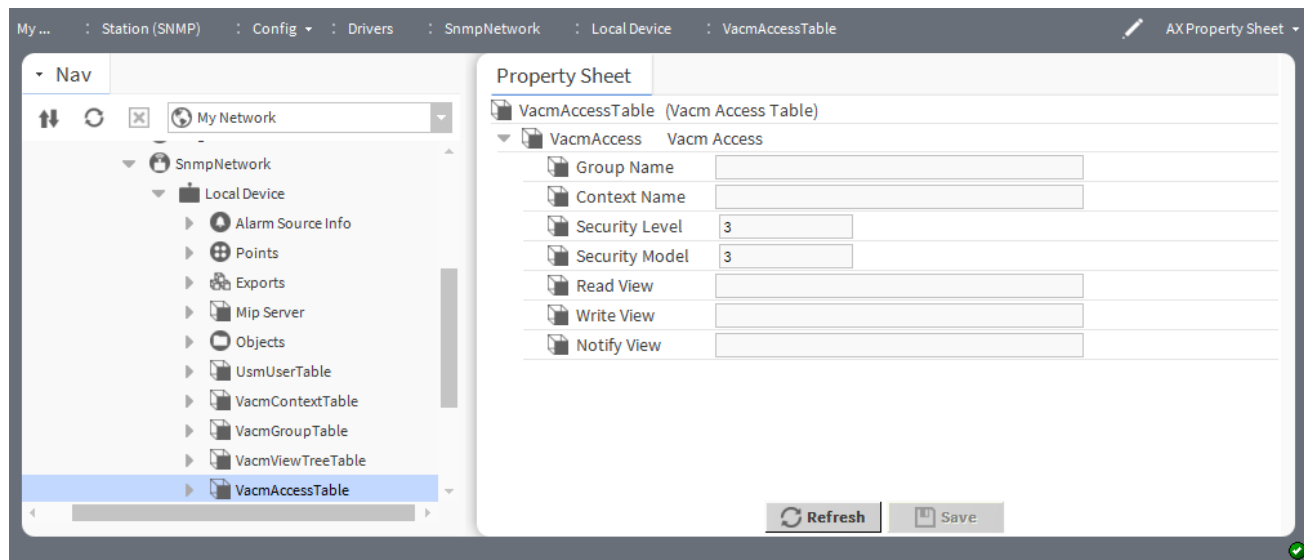
To access this view, expand **Config→Drivers→SnmpNetwork→Local Device**, right-click **VacmContextTable→Views→AX Property Sheet**.

Property	Value	Description
Vacm Context Table	text	Enter the context name.

## Vacm Access

A Vacm Access is available in the nSnmp module. The Vacm Access is a row of the **VacmAccessTable**. The Vacm Access row contains an object for each element that is represented in the **VacmAccessTable**. User can edit the **VacmAccessTable** properties by double clicking on the Vacm Access row.

Figure 31 Vacm Access Properties



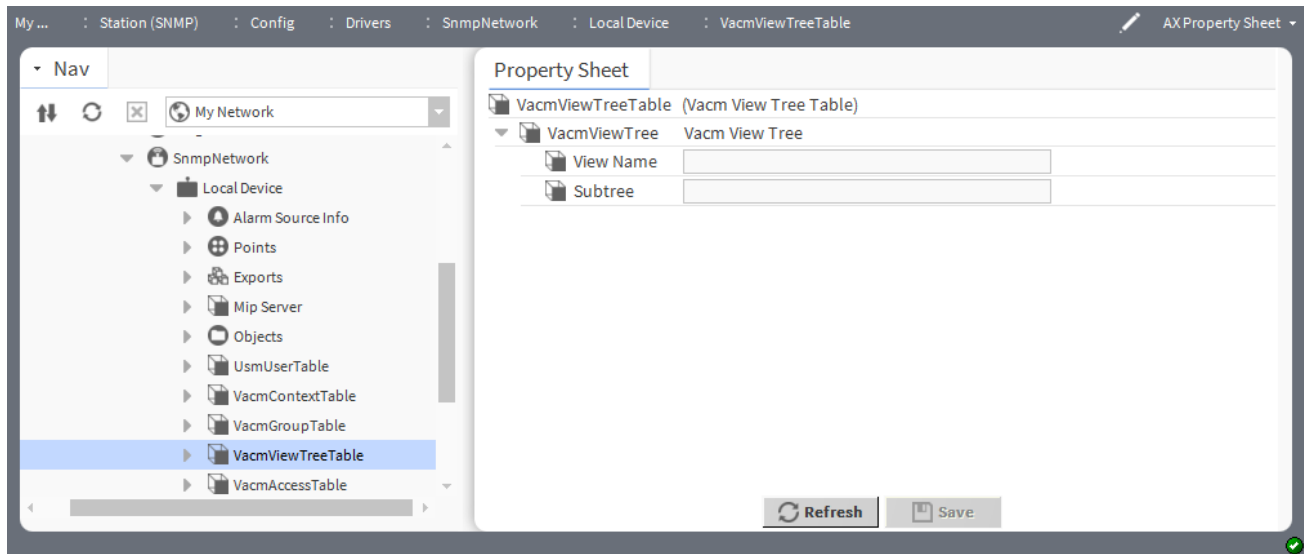
To access this view, expand **Config**→**Drivers**→**SnmpNetwork**→**Local Device**, right-click **VacmAccessTable**→**Views**→**AX Property Sheet**.

Property	Value	Description
Group Name	text	Enter the group name.
Context Name	text	Enter the context name. The Context Name specifies where the desired management object is to be found.
Security Level	number	Enter the desired amount of security you want for messages on your SNMPv3 network.
Security Model	number	Default number is 3. <b>need more info</b>
Read View	text	Enter the view name of VacmAccessTable. <b>please confirm</b>
Write View	text	Enter the view name of VacmAccessTable.
Notify view	text	Enter the view name of VacmAccessTable.

## Vacm View Tree

A Vacm View Tree is available in the nSnmp module. The Vacm View Tree is a row of the **VacmViewTreeTable**. The Vacm View Tree row contains an object for each element that is represented in the **VacmViewTreeTable**. User can edit the **VacmViewTreeTable** properties by double clicking on the Vacm View Tree row.

Figure 32 Vacm View Tree Properties



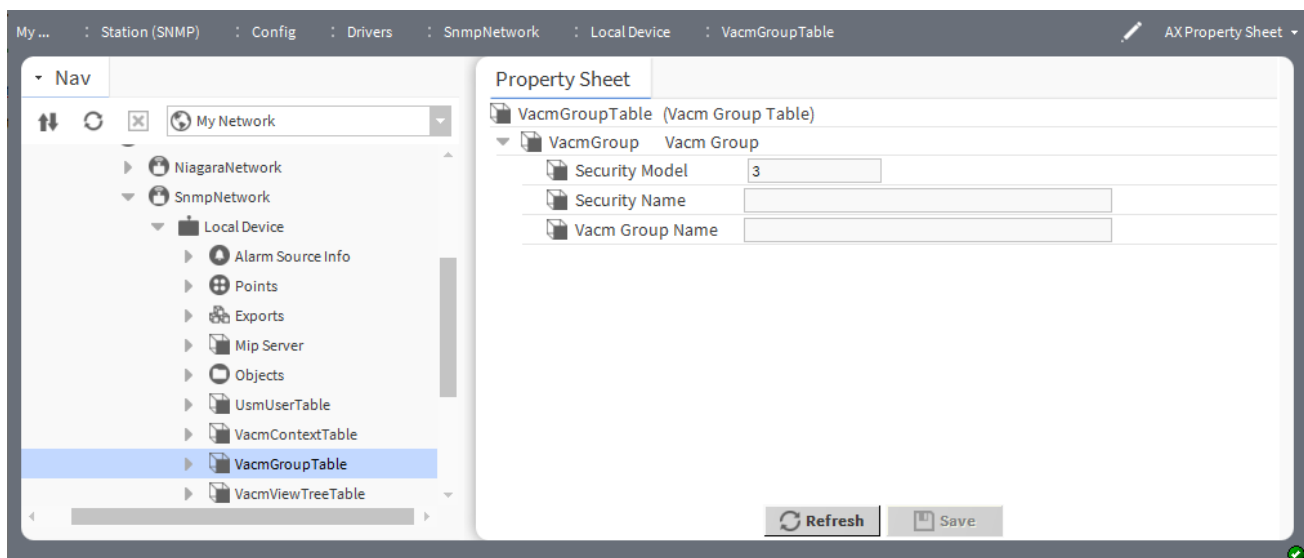
To access this view, expand **Config→Drivers→SnmpNetwork→Local Device**, right-click **VacmViewTreeTable→Views→AX Property Sheet**.

Property	Value	Description
View Name	text	Enter the user access name.
Subtree	text	Enter the enterprise ord which is restricted to define the views which user will have access. <b>please confirm</b>

## Vacm Group

A Vacm Group is available in the nSnmp module. The Vacm Group is a row of the **VacmGroupTable**. The Vacm Group row contains an object for each element that is represented in the **VacmGroupTable**. User can edit the **VacmGroupTable** properties by double clicking on the Vacm Group row.

Figure 33 Vacm Group Properties



To access this view, expand **Config→Drivers→SnmpNetwork→Local Device**, right-click **VacmGroupTable→Views→AX Property Sheet**.

Property	Value	Description
Security Model	number	This number defaults to 3.
Security Name	text	Enter the user name.
Vacm Group Name	text	Enter the group name of VacmGroupTable.

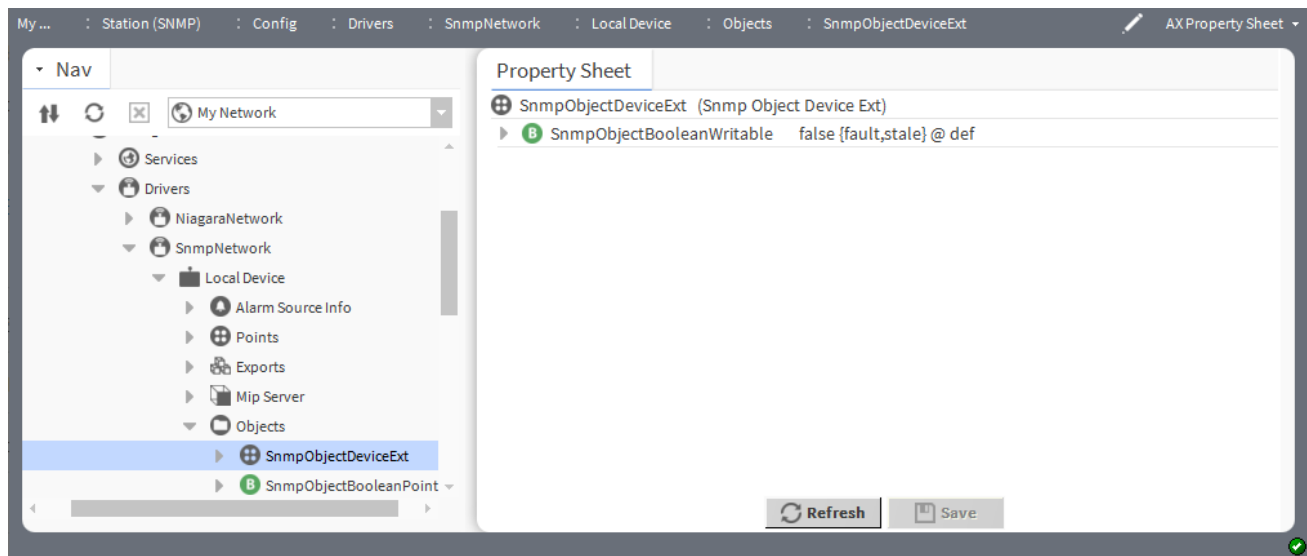
## Snmp Device Folder

Snmp Device Folder is the Snmp implementation of a folder under an **SnmpNetwork**. You add such folders using the **New Folder** button in the **Snmp Device Manager** view of the **SnmpNetwork**. Each Snmp Device Folder has its own **Snmp Device Manager** view. Bajadoc is available at `BSnmpDeviceFolder.bajadoc`.

## Snmp Object Device Ext

Snmp Object Device Ext is a container for any of the set of Snmp Object types. This includes read and read-write components for: **SnmpObjectBooleanPoint**, **SnmpObjectEnumPoint**, **SnmpObjectNumericPoint**, **SnmpObjectStringPoint**. The default view of this extension is the **Snmp Object Manager** view.

Figure 34 Snmp Object Device Ext Property



To access this view, expand **Config→Drivers→SnmpNetwork→Local Device→Objects**, right-click **SnmpObjectDeviceExt→Views→AX Property Sheet**.

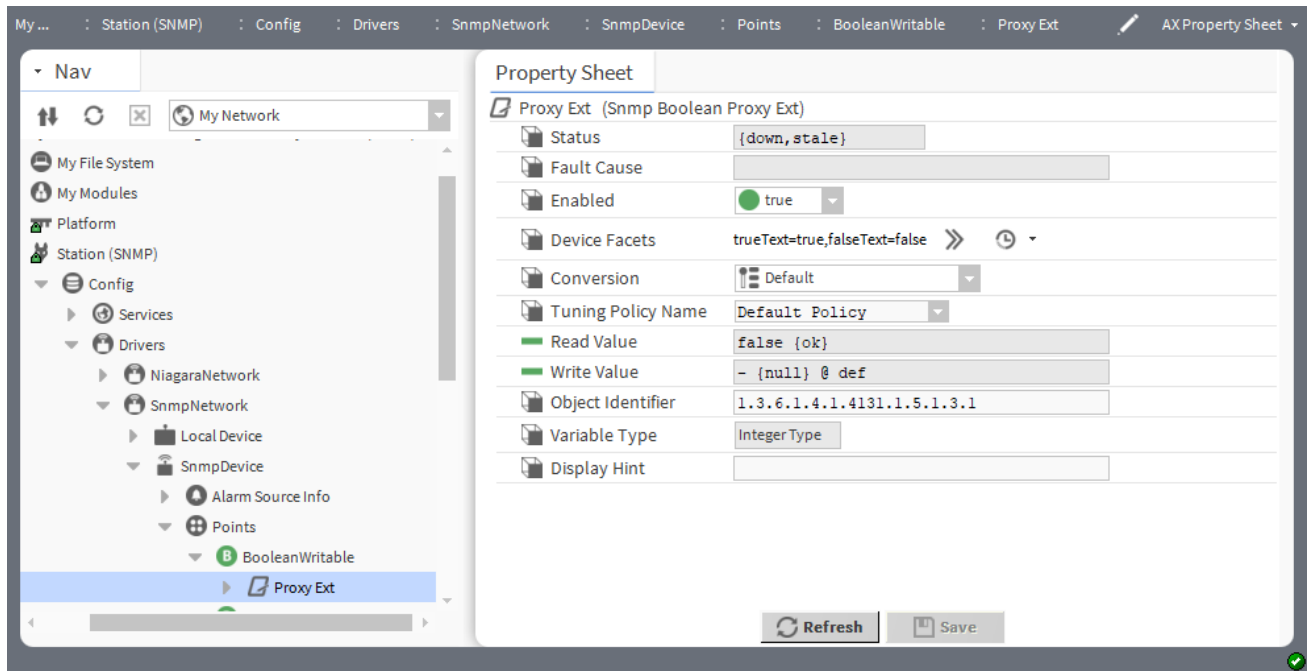
This container is used to add object points.

## Snmp Boolean Proxy Ext

Snmp Boolean Proxy Ext contains information necessary to read a float (or integer) data value from a **SnmpDevice**. Each read-only proxy point that represents a readable float (integer) Snmp data quantity will have a Snmp Boolean Proxy Ext to describe how to read the point.



Figure 35 Snmp Boolean Proxy Ext Properties



To access this view, expand **Config→Drivers→SnmpNetwork→SnmpDevice→Points→Boolean Point**, double-click **Proxy Ext**.

In addition to the standard properties (Status, Enabled and Fault Cause), these properties are unique to this component.

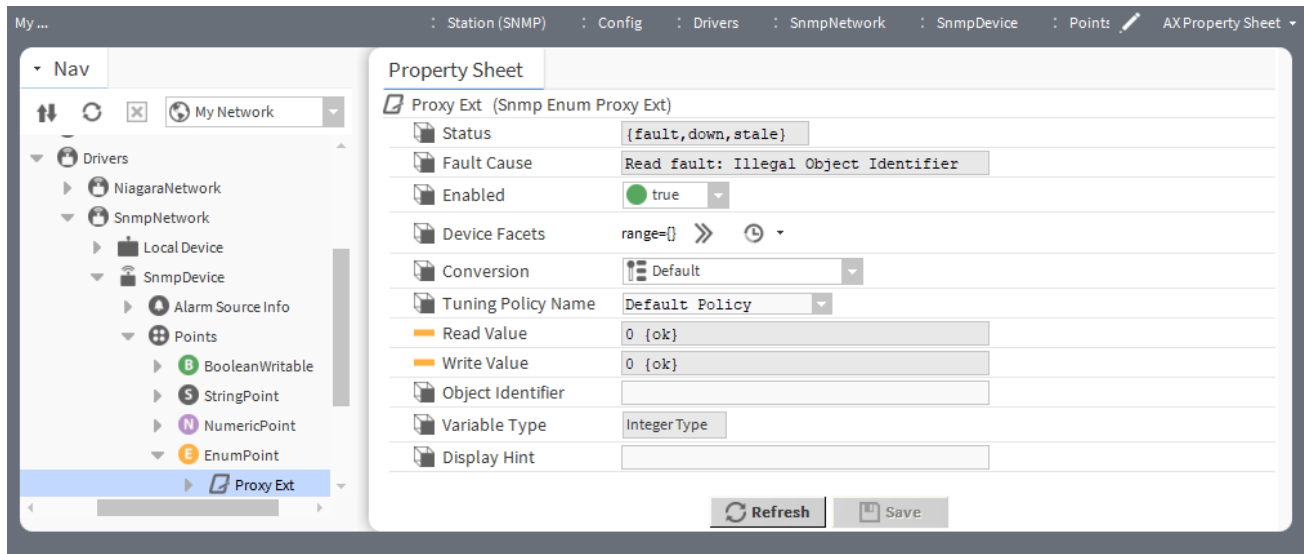
Property	Value	Description
Device Facets	additional properties	Configures additional parameters for the device proxy point facets for how the value should be displayed in Niagara. <b>Please confirm.</b>
Conversion	drop-down list	<p>Defines how the system converts proxy extension units to parent point units.</p> <p>Default automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.</p> <p><b>NOTE:</b> In most cases, the standard Default conversion is best.</p> <p>Linear applies to voltage input, resistive input and voltage output writable points. Works with linear-acting devices. You use the Scale and Offset properties to convert the output value to a unit other than that defined by device facets.</p> <p>Linear With Unit is an extension to the existing linear conversion property. This specifies whether the unit conversion should occur on "Device Value" or "Proxy Value". The new linear with unit convertor, will have a property to indicate whether the unit conversion should take place before or after the scale/offset conversion.</p> <p>Reverse Polarity applies only to Boolean input and relay output writable points. Reverses the logic of the hardware binary input or output.</p>

Property	Value	Description
		<p><b>500 Ohm Shunt</b> applies to voltage input points only. It reads a 4-to-20mA sensor, where the Ui input requires a 500 ohm resistor wired across (shunting) the input terminals.</p> <p><b>Tabular Thermistor</b> applies to only a Thermistor input point and involves a custom resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><b>Thermistor Type 3</b> applies to an Thermistor Input point, where this selection provides a "built-in" input resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><b>Generic Tabular</b> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. Generic Tabular uses a lookup table method similar to the "Thermistor Tabular" conversion, but without predefined output units.</p>
Tuning Policy Name	drop-down list	Configures network rules for evaluating both write requests to writable proxy points as well as the acceptable freshness of read requests.
Read Value	read-only	Displays the last value read from the device, expressed in device facets.
Write Value	read-only	Displays the last value written, using device facets.
Object Identifier	read-only	Displays the full OID to use for accessing the data value for this point from the Input Table (or Output Table) by an outside Snmp manager. Snmp GET or SET requests would use this full OID to access the value of the proxy point.
Variable Type	read-only	Displays the type of the point.
Display Hint		<b>Need Information</b>

## Snmp Enum Proxy Ext

Snmp Enum Proxy Ext contains information necessary to read a float (or integer) data value from a **SnmpDevice**. Each read-only proxy point that represents a readable float (integer) Snmp data quantity will have a Snmp Enum Proxy Ext to describe how to read the point.

Figure 36 Snmp Enum Proxy Ext Properties



To access this view, expand **Config→Drivers→SnmpNetwork→SnmpDevice→Points→Enum Point**, double-click **Proxy Ext**.

In addition to the standard properties (Status, Enabled and Fault Cause), these properties are unique to this component.

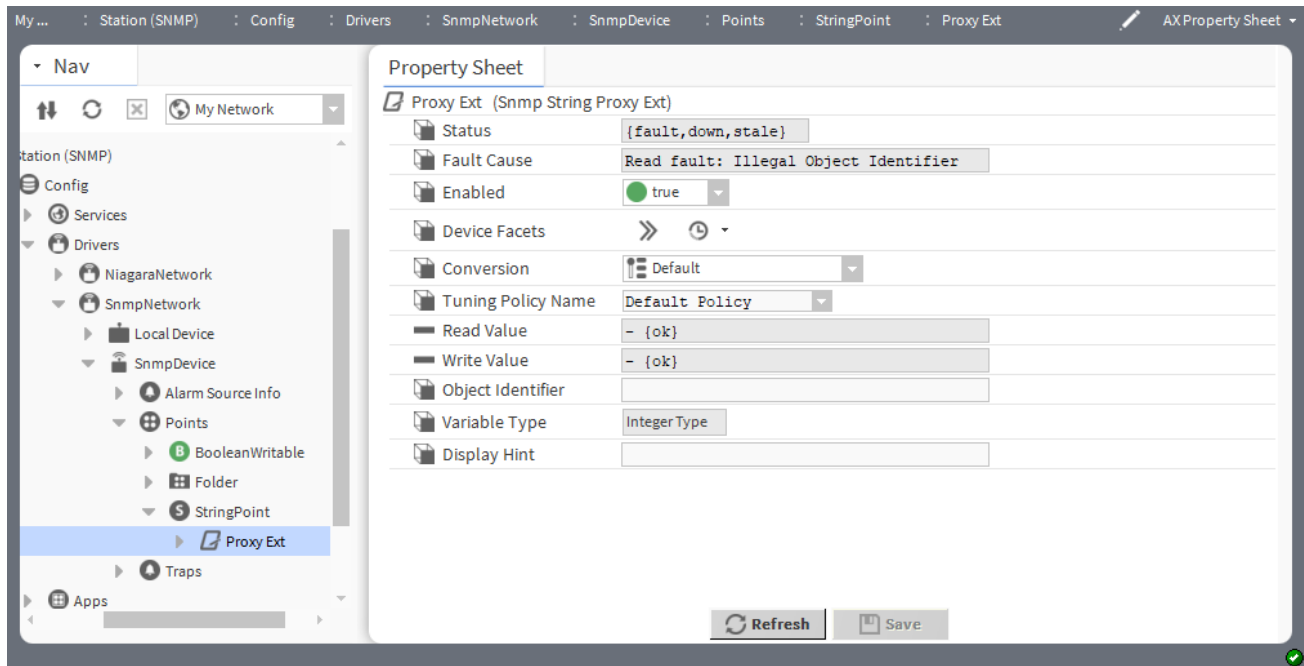
Property	Value	Description
Device Facets	additional properties	Configures additional parameters for the device proxy point facets for how the value should be displayed in Niagara. <b>Please confirm.</b>
Conversion	drop-down list	<p>Defines how the system converts proxy extension units to parent point units.</p> <p>Default automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.</p> <p><b>NOTE:</b> In most cases, the standard Default conversion is best.</p> <p>Linear applies to voltage input, resistive input and voltage output writable points. Works with linear-acting devices. You use the Scale and Offset properties to convert the output value to a unit other than that defined by device facets.</p> <p>Linear With Unit is an extension to the existing linear conversion property. This specifies whether the unit conversion should occur on "Device Value" or "Proxy Value". The new linear with unit convertor, will have a property to indicate whether the unit conversion should take place before or after the scale/offset conversion.</p> <p>Reverse Polarity applies only to Boolean input and relay output writable points. Reverses the logic of the hardware binary input or output.</p> <p>500 Ohm Shunt applies to voltage input points only. It reads a 4-to-20mA sensor, where the Ui input requires a 500 ohm resistor wired across (shunting) the input terminals.</p>

Property	Value	Description
		<p><code>Tabular Thermistor</code> applies to only a Thermistor input point and involves a custom resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Thermistor Type 3</code> applies to an Thermistor Input point, where this selection provides a “built-in” input resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Generic Tabular</code> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. Generic Tabular uses a lookup table method similar to the “Thermistor Tabular” conversion, but without predefined output units.</p>
Tuning Policy Name	drop-down list	Configures network rules for evaluating both write requests to writable proxy points as well as the acceptable freshness of read requests.
Read Value	read-only	Displays the last value read from the device, expressed in device facets.
Write Value	read-only	Displays the last value written, using device facets.
Object Identifier	read-only	Displays the full OID to use for accessing the data value for this point from the Input Table (or Output Table) by an outside Snmp manager. Snmp GET or SET requests would use this full OID to access the value of the proxy point.
Variable Type	read-only	Displays the type of the point.
Display Hint		Need Information

## Snmp String Proxy Ext

Snmp String Proxy Ext contains information necessary to read a String data value from a **SnmpDevice**. Each read-only proxy point that represents a readable string Snmp data quantity will have an Snmp String Proxy Ext to describe how to read the point

Figure 37 Snmp String Proxy Ext Properties



To access this view, expand **Config**→**Drivers**→**SnmpNetwork**→**SnmpDevice**→**Points**→**String Point**, double-click **Proxy Ext**

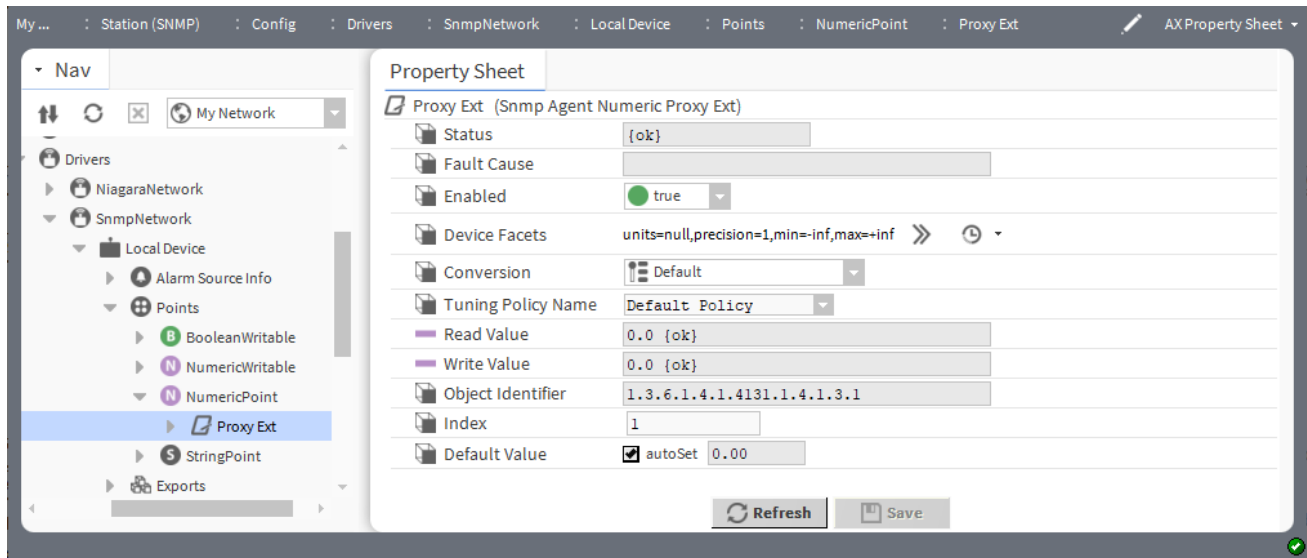
In addition to the standard properties (Status and Fault Cause), these properties are unique to this component.

Property	Value	Description
Device Facets	additional properties	Configures additional parameters for the device proxy point facets for how the value should be displayed in Niagara. <b>Please confirm.</b>
Conversion	drop-down list	<p>Defines how the system converts proxy extension units to parent point units.</p> <p>Default automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.</p> <p><b>NOTE:</b> In most cases, the standard Default conversion is best.</p> <p>Linear applies to voltage input, resistive input and voltage output writable points. Works with linear-acting devices. You use the Scale and Offset properties to convert the output value to a unit other than that defined by device facets.</p> <p>Linear With Unit is an extension to the existing linear conversion property. This specifies whether the unit conversion should occur on "Device Value" or "Proxy Value". The new linear with unit convertor, will have a property to indicate whether the unit conversion should take place before or after the scale/offset conversion.</p> <p>Reverse Polarity applies only to Boolean input and relay output writable points. Reverses the logic of the hardware binary input or output.</p>

Property	Value	Description
		<p><code>500 Ohm Shunt</code> applies to voltage input points only. It reads a 4-to-20mA sensor, where the Ui input requires a 500 ohm resistor wired across (shunting) the input terminals.</p> <p><code>Tabular Thermistor</code> applies to only a Thermistor input point and involves a custom resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Thermistor Type 3</code> applies to an Thermistor Input point, where this selection provides a "built-in" input resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Generic Tabular</code> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. Generic Tabular uses a lookup table method similar to the "Thermistor Tabular" conversion, but without predefined output units.</p>
Tuning Policy Name	drop-down list	Configures network rules for evaluating both write requests to writable proxy points as well as the acceptable freshness of read requests.
Read Value	read-only	Displays the last value read from the device, expressed in device facets.
Write Value	read-only	Displays the last value written, using device facets.
Object Identifier	read-only	Displays the full OID to use for accessing the data value for this point from the Input Table (or Output Table) by an outside Snmp manager. Snmp GET or SET requests would use this full OID to access the value of the proxy point.
Variable Type		Need Information
Description		Need Information
Out	read-only	Represents the point slot that contains the value to output.

## Snmp Numeric Proxy Ext

Snmp Numeric Proxy Ext contains information necessary to read a float (or integer) data value from a **SnmpDevice**. Each read-only proxy point that represents a readable float (integer) Snmp data quantity will have a Snmp Numeric Proxy Ext to describe how to read the point.

**Figure 38** Snmp Numeric Proxy Ext Properties


To access this view, expand **Config→Drivers→SnmpNetwork→SnmpDevice→Points→Numeric Point**, double-click **Proxy Ext**.

In addition to the standard properties (Status, Enabled and Fault Cause), these properties are unique to this component.

Property	Value	Description
Device Facets	additional properties	Configures additional parameters for the device proxy point facets for how the value should be displayed in Niagara. <b>Please confirm.</b>
Conversion	drop-down list	<p>Defines how the system converts proxy extension units to parent point units.</p> <p>Default automatically converts similar units (such as Fahrenheit to Celsius) within the proxy point.</p> <p><b>NOTE:</b> In most cases, the standard Default conversion is best.</p> <p>Linear applies to voltage input, resistive input and voltage output writable points. Works with linear-acting devices. You use the Scale and Offset properties to convert the output value to a unit other than that defined by device facets.</p> <p>Linear With Unit is an extension to the existing linear conversion property. This specifies whether the unit conversion should occur on "Device Value" or "Proxy Value". The new linear with unit convertor, will have a property to indicate whether the unit conversion should take place before or after the scale/offset conversion.</p> <p>Reverse Polarity applies only to Boolean input and relay output writable points. Reverses the logic of the hardware binary input or output.</p> <p>500 Ohm Shunt applies to voltage input points only. It reads a 4-to-20mA sensor, where the Ui input requires a 500 ohm resistor wired across (shunting) the input terminals.</p>

Property	Value	Description
		<p><code>Tabular Thermistor</code> applies to only a Thermistor input point and involves a custom resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Thermistor Type 3</code> applies to an Thermistor Input point, where this selection provides a “built-in” input resistance-to-temperature value response curve for Type 3 Thermistor temperature sensors.</p> <p><code>Generic Tabular</code> applies to non-linear support for devices other than for thermistor temperature sensors with units in temperature. Generic Tabular uses a lookup table method similar to the “Thermistor Tabular” conversion, but without predefined output units.</p>
Tuning Policy Name	drop-down list	Configures network rules for evaluating both write requests to writable proxy points as well as the acceptable freshness of read requests.
Read Value	read-only	Displays the last value read from the device, expressed in device facets.
Write Value	read-only	Displays the last value written, using device facets.
Object Identifier	read-only	Displays the full OID to use for accessing the data value for this point from the Input Table (or Output Table) by an outside Snmp manager. Snmp GET or SET requests would use this full OID to access the value of the proxy point.
Index	number	Need Information
Default Value	number	Need Information

## Snmp Sequence



Snmp Sequence objects contain an Output Index, Output Name, and Output Value slot (properties) that correspond to the columns in each **Snmp Table Row**. Each of these has the following editable properties: OID, Element Name, Element Type, Variable Type, Writable option and Display Hint.

## Snmp Table



The Snmp Table component supports MIB tables. This object represents Snmp data in a collection of BStatusValue objects that are organized in a sequence of rows, as they are “discovered” in a device. Each row consists of an object for each element, as represented in the MIB. The default view of the Snmp Table object is the **Table Manager** view, which presents the data in a table format. The row elements can be linked to other control objects. Read-only values can be linked to inputs and read-write values can be linked to inputs or outputs.


## Snmp Table Row




The Snmp Table Row contains an object for each element that is represented in the MIB table for the **SnmpDevice**. The row has an index, name, type, and value.



## N Poll Scheduler

 N Poll Scheduler. The N Poll Scheduler is available in the nSnmp module. Bajadoc is available at BSnmpPollScheduler.bajadoc.

## Trap Table

 Trap Table captures information about stored trap types within an **SnmpDevice**. It is a frozen slot in an **SnmpDevice** (default name Trap Types), and contains child Trap Type slots. The default view for an **SnmpDevice**'s Trap Table is the **Snmp Trap Manager**. Bajadoc is available at BTrapTable.bajadoc.

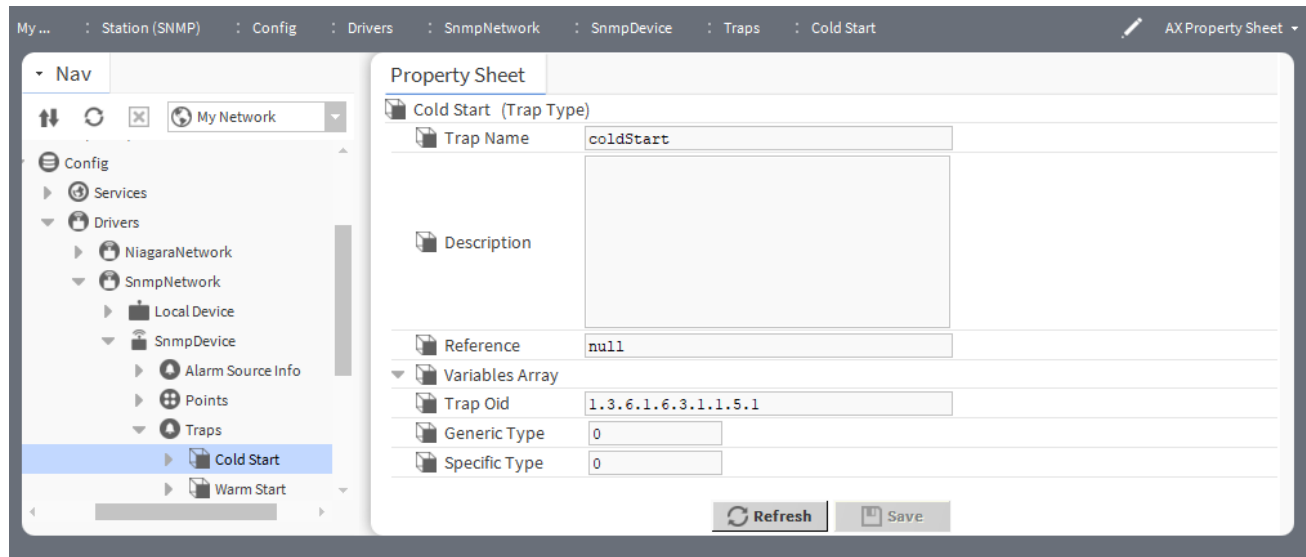
## snmp-TrapType

TrapType stores a possible trap type for an **SnmpDevice**, and resides under an SnmpDevice's TrapTable. Bajadoc is available at BTrapType.bajadoc.

Following are the available trap types:

- Cold Start
- Warm Start
- Link Down
- Link Up
- Authentication Failure
- Egg Neighbor Loss

Figure 39 Snmp-TrapType Properties



Property Sheet	
Cold Start (Trap Type)	
Trap Name	coldStart
Description	
Reference	null
Variables Array	
Trap Old	1.3.6.1.6.3.1.1.5.1
Generic Type	0
Specific Type	0

Refresh Save

To access this view, expand **Config→Drivers→SnmpNetwork→SnmpDevice→Traps**, double-click **Cold Start**.

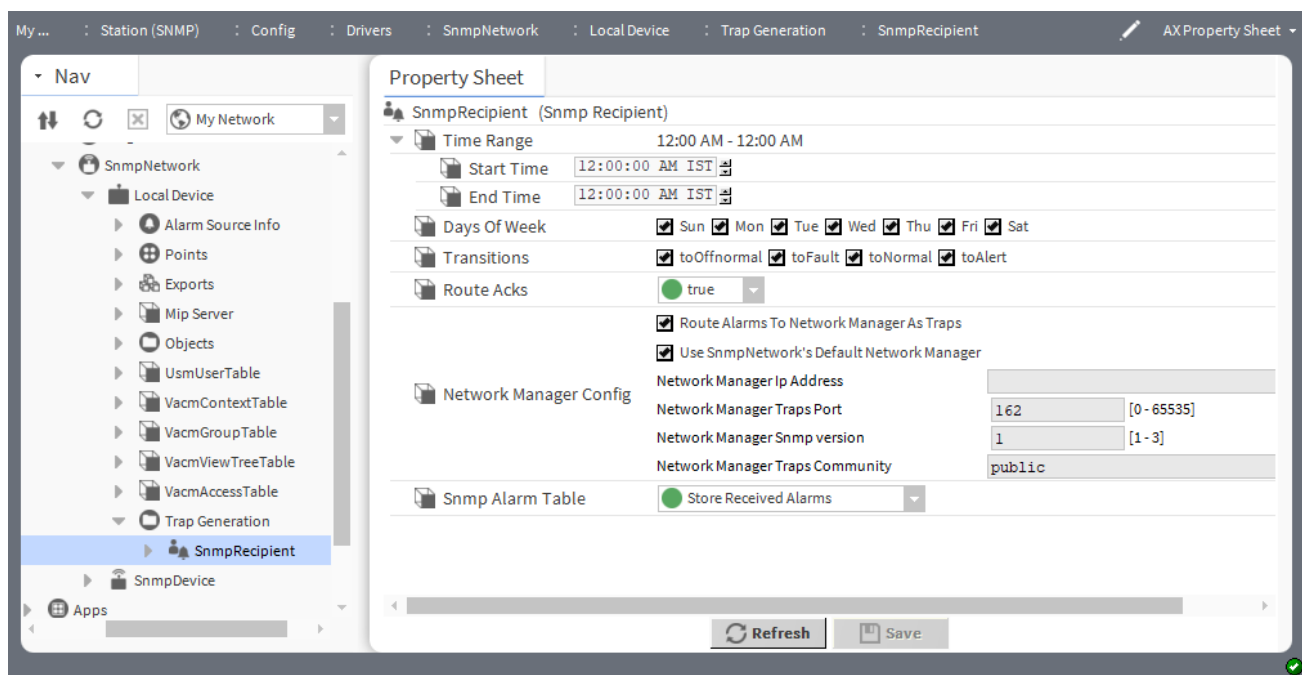
All the other trap types have same properties mentioned in the below property table.

Property	Value	Description
Trap Name	text	Enter the name of the trap type.
Description	text	Enter the description for trap type.
Reference	text	Enter any reference for the trap type. <b>Please Confirm</b>
Variables Array		<b>Need Information</b>
Trap Oid	Numeric	<b>Need Information</b>
Generic Type	Numeric	Configure the generic type of the trap type. <b>Please Confirm</b>
Specific Type	Numeric	Configure the specific type of the trap type. <b>Please Confirm</b>

## Snmp Recipient

Snmp Recipient recipient class is used to send alarm traps to an SnmpNetwork manager and to store alarms until acknowledged. The Snmp Recipient is available in the nSnmp module

Figure 40 Snmp Recipient Properties



To access this view, expand **Config→Drivers→SnmpNetwork→Local Device→TrapGeneration→SnmpReceipient**.

Property	Value	Description
Time Range	hours:minutes:seconds	Sets the time of day to begin and stop the function (for example, trigger schedule, alarm event).
Days of Week	check box	Specifies the days of the week to include in the function.
Transitions	check box	Selects which alarm transitions to display in the console. Only those transitions selected display although the station saves all transitions in alarm history.

Property	Value	Description
Route Acks	true (default) or false	Enables (true) and disables (false) the routing of alarm acknowledgements to the recipient. Trap (event notification) acknowledgements are not routed if false is selected.
Network Manager Config	additional properties	Configure additional parameters to configure Snmp Network. Please Confirm
Snmp Alarm Table	drop-down list	Configures the alarms that are routed to this recipient are also cached in the Snmp Alarm Table. This is the default option.

