

# Wonderware Operations Integration - SNMP OI Server 1.1 (Series-G1.2) User Guide



© 2016 Schneider Electric Software, LLC. All rights reserved.

No part of this documentation shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Schneider Electric Software, LLC. No liability is assumed with respect to the use of the information contained herein.

Although precaution has been taken in the preparation of this documentation, Schneider Electric Software, LLC assumes no responsibility for errors or omissions. The information in this documentation is subject to change without notice and does not represent a commitment on the part of Schneider Electric Software, LLC. The software described in this documentation is furnished under a license agreement. This software may be used or copied only in accordance with the terms of such license agreement.

ArchestrA, Avantis, DYNsIM, eDNA, EYESIM, Foxboro, Foxboro Evo, I/A Series, InBatch, InduSoft, InStep, IntelaTrac, InTouch, PIPEPHASE, PRiSM, PRO/II, PROVISION, ROMeo, Schneider Electric, SIM4ME, SimCentral, SimSci, Skelta, SmartGlance, Spiral Software, VISUAL FLARE, WindowMaker, WindowViewer, and Wonderware are trademarks of Schneider Electric SE, its subsidiaries, and affiliated companies. An extensive listing of Schneider Electric Software, LLC trademarks can be found at: <http://software.schneider-electric.com/legal/trademarks/>. All other brands may be trademarks of their respective owners.

Schneider Electric Software, LLC  
26561 Rancho Parkway South  
Lake Forest, CA 92630 U.S.A.  
(949) 727-3200

<http://software.schneider-electric.com/>

Publication date: 9/12/2016

# Contact Us

## Contact Schneider Electric Software Technical Support

### Avantis Technical Support

Listing of regional and local country contacts: <http://software.schneider-electric.com/support/avantis/>

Technical support: <http://softwaresupport.schneider-electric.com/>

For Avantis.PRO, Avantis Approvals, Avantis.DSS, and Condition Manager:

- Email: [support.pro@avantis.net](mailto:support.pro@avantis.net)
- Phone (8:30 a.m. to 5:00 p.m. Monday to Friday, Eastern Time):
  - Toll-Free U.S. and Canada: 1-888-262-7111
  - Toll-Free EMEA: 1-800-4670-6466
  - Direct dial: 1-905-632-0635

For Avantis.XA:

- Email: [support.xa@avantis.net](mailto:support.xa@avantis.net)
- Phone (8:30 a.m. to 5:00 p.m. Monday to Friday, Eastern Time):
  - Toll-Free U.S. and Canada: 1-800-991-8000
  - Toll-Free EMEA: 1-800-4670-6466
  - Direct dial: 1-905-632-4122

### SimSci Technical Support

Listing of regional and local country contacts: <http://software.schneider-electric.com/support/simsci/>

Technical support: <http://softwaresupport.schneider-electric.com/>

- Phone (USA 8:00 a.m. to 5:00 p.m. Central Time)
  - Toll-Free U.S. and Canada: 1-800-746-7241
- Email U.S. and Canada: [support.simsci@schneider-electric.com](mailto:support.simsci@schneider-electric.com)

### Wonderware Technical Support

Listing of regional and local country contacts: <https://www.wonderware.com/contact/contact-support/>

Technical support: <http://softwaresupport.schneider-electric.com/>

- Priority email for Customer FIRST Members: [custfirstsupport@wonderware.com](mailto:custfirstsupport@wonderware.com)
- Email for customers without a support agreement: [wwsupport@wonderware.com](mailto:wwsupport@wonderware.com)
- Phone
  - Toll-Free North America and Latin America: 1-800-966-3371
  - Direct dial: 1-949-639-8500

### InStep Technical Support

Contact page: <http://www.instepsoftware.com/contact-us>

Technical support: <https://support.instepsoftware.com/>

- Email: [instepsupport@schneider-electric.com](mailto:instepsupport@schneider-electric.com)
- Phone (USA 8:00 a.m. to 5:00 p.m. Central Time)
  - 1-312-894-7870

### **Schneider Electric – Smart Water Software Technical Support**

- Help desk email: [DK-HSO-Support@schneider-electric.com](mailto:DK-HSO-Support@schneider-electric.com)
- Help desk telephone hotline: +45 88 30 20 77 (09:00 to 16:00 Monday to Thursday, Friday 09:00 to 15:00, Central European Time)

### **Contact Schneider Electric Software Learning Services**

Contact Software Learning Services for assistance regarding classes, schedule, offerings, frequently asked questions, tuition, policies, and more.

- Email: [software.training@schneider-electric.com](mailto:software.training@schneider-electric.com)
- Toll-Free U.S. and Canada: 1-866-998-7246
- Direct: 1-949-639-8508
- Fax: 1-949-639-1847

# Contents

Chapter 1 Getting Started with the SNMP OI Server .....	7
About the SNMP OI Server .....	7
Determining the Hierarchical Structure .....	7
Working with a Basic Hierarchy .....	8
Configuring More than One Channel Selector.....	8
Building the Hierarchical Structure in the SMC .....	8
Chapter 2 Configuring the SNMP OI Server .....	11
Setting Up an SNMP OI Server for the First Time .....	11
Adding and Configuring Channel Selector Objects .....	11
Adding and Configuring Device Selector Objects .....	14
Device Group Definitions .....	16
Device Item Definitions .....	17
Configuring SNMP Redundancy .....	18
Chapter 3 SNMP OI Server References .....	19
Supported Software Environments and Devices .....	19
Station Parameters .....	19
I/O Address Syntax .....	20
Data Types.....	21
Using Traps.....	21
Common SNMP Item References.....	22
Configuring an SNMP Agent in Windows .....	23
Chapter 4 Troubleshooting the SNMP OI Server .....	29
Checking Status Codes .....	29
Status Codes.....	30



# CHAPTER 1

## Getting Started with the SNMP OI Server

This document describes the technical specifications and configuration options for the Wonderware® Operations Integration - Supervisory Simple Network Management Protocol (SNMP) Server.

### In This Chapter

About the SNMP OI Server .....	7
Determining the Hierarchical Structure .....	7

### About the SNMP OI Server

Use the Wonderware SNMP OI Server to monitor and manage devices on IP networks. Using the SNMP OI Server, you can add and configure channels and the devices to be monitored and managed using your choice of Management Information Base (MIB) browser.

---

**Note:** This OI Server is hosted by the OI Server Manager, a Microsoft Management Console (MMC) snap-in, which is a part of the ArcestrA System Management Console (SMC) suite of utilities. Many high-level functions and user-interface elements of the OI Server Manager are universal to all OI Servers, and only the documentation for the OI Server Manager contains descriptions of those universal functions/UI elements. Therefore, reading the documentation for both the MMC and the OI Server Manager is critical to understanding this user's guide. To read the documentation about the MMC and OI Server Manager, right-click the OI Server Manager icon and select the Help menu. Both the MMC Help and the OI Server Manager Help are displayed.

---

An SNMP agent must be installed and configured on each device managed by the SNMP OI server. For information about installing and configuring an SNMP in Windows, see *Configuring an SNMP Agent in Windows* on page 23.

### Determining the Hierarchical Structure

Determine the hierarchical structure of the networked devices environment to which you plan to connect. The SNMP OI Server is configured in a two-tier hierarchy, with Channel Selector connection parent objects and associated Device Selector connection child objects.

---

**Note:** This device hierarchy is different and separate from the hierarchical namespace containing Object Identifiers and associated variables visible and manageable through a Management Information Base (MIB) browser.

---

## Working with a Basic Hierarchy

You can create more than one Channel Selector object, but a basic configuration calls for a single Channel Selector object with child Device Selector objects representing individual devices. This typical configuration is common for the following reasons:

- Traps are received from the port specified in the Channel Selector settings, with port 162 as the default. To receive traps correctly, only one Channel Selector can be bound to the specified port. If multiple channel selectors share the same port, only one of them will receive traps.
- In real world applications, traps are sent to port 162 by default when using SNMP Windows Agents or devices (PLCs routers, printers etc. that support SNMP) . You can specify any valid port, but in most cases when talking to real devices with SNMP, the port 162 is used. Hence, the default value for the TRAP port has been configured to 162.

However, in some cases you can change the default trap port that the device or machine can send traps to.

- The same conditions, guidelines, and recommendations apply if you want to clone multiple instances of the SNMP OI server on the same machine. Traps will function only in the first running version of any SNMP servers. Any subsequent instances of the SNMP server will not receive any trap packets.

## Configuring More than One Channel Selector

Use the Channel Selector for the Trap Port setting, but also to set the number of Simultaneous Requests you want to make to your managed devices.

- With multiple simultaneous requests configured, tests have shown an improvement in throughput and performance.
- Even without multiple simultaneous requests, using the default setting (1), a new thread is created for each new Channel Selector. Multiple threads instead of single one, will also improve performance.

If you observe performance issues in your SNMP configuration, we recommend the following hierarchy:

1. Create one Channel Selector for the devices from which you want to receive wants traps.
2. Create additional Channel Selectors to improve performance of the OI server and to use simultaneous connections for devices from which you don't want to receive traps, but from which you want to process values for greater numbers of OIDs.

---

**Note:** A limitation of multiple Channel Selectors or a channel selector with enabled simultaneous requests is that these configurations will show higher memory and CPU usage by the OI server.

---

## Building the Hierarchical Structure in the SMC

### To build the hierarchical structure

1. Configure the new SNMP OI Server.
  - a. In the console tree, right-click **Configuration** and then click **Add ChannelSelector Connection**.



- b. Edit the object name to appropriately describe components of your specific hardware environment. If you do not rename the object at this time, a numeric sequencing system is applied. You can rename the hierarchy entry later.
2. Right-click the New\_ChannelSelector\_000 object you created in the tree and then click **Add DeviceSelector Connection** to create a Device Selector object.
3. Optionally create device groups for each logical end-point object.

---

**Important:** When the OI Server or any of its configuration views are selected and you open multiple instances of the OI Server Manager, the OI Server Manager places the configuration views from the subsequent instances of the same OI Server into read-only mode. Access to the second instance of the OI Server resumes after the first one has been deselected or closed. Likewise, access to the OI Server configuration will be unlocked for the next instance in this order.

---



## CHAPTER 2

# Configuring the SNMP OI Server

### In This Chapter

Setting Up an SNMP OI Server for the First Time .....	11
Adding and Configuring Channel Selector Objects.....	11
Adding and Configuring Device Selector Objects .....	14
Device Group Definitions .....	16
Device Item Definitions.....	17
Configuring SNMP Redundancy .....	18

## Setting Up an SNMP OI Server for the First Time

If you are setting up an OI Server for the first time, perform the following tasks in the order listed:

1. Locate the OI Server in the System Management Console (SMC). In the OI Server Manager tree, under the Local node, the OI Server base instance name is OI.SNMPDIR.1.
2. Configure the global parameters. See "Configuring Global Parameters" in the OI Server Manager help.
3. Add one or more channel selector connections. See *Adding and Configuring Channel Selector Objects* on page 11.
4. Add one or more device selector connections. See *Adding and Configuring Device Selector Objects* on page 14.
5. Add one more device groups. See *Device Group Definitions* on page 16.
6. Add device items. See *Device Item Definitions* on page 17.
7. Activate the OI Server. See "Activating/Deactivating the OI Server" in the OI Server Manager help.
8. Troubleshoot any problems.

---

**Note:** (Optional) You can also use any commercially available MIB browser to find the OIDs to use as item references on the OI Server.

---

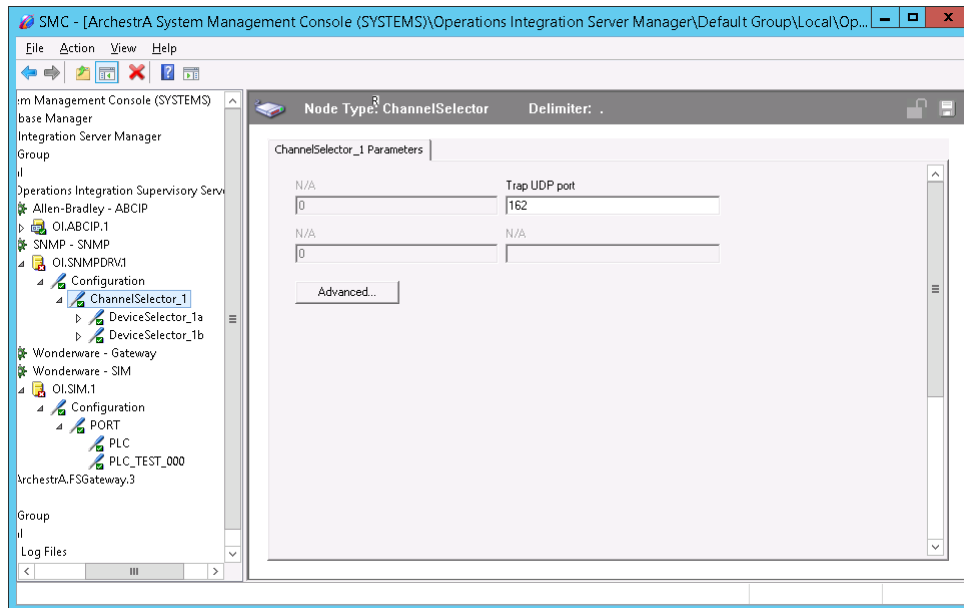
## Adding and Configuring Channel Selector Objects

The server-specific configuration portion of the SNMP OI Server hierarchy tree under the OI Server Manager starts at the Channel Selector object. This object lets you set server parameters for communication with agents (devices) in the hierarchy tree.

See *Determining the Hierarchical Structure* on page 7 for more information about setting up your device hierarchy.

### To add a Channel Selector object to your SNMP hierarchy

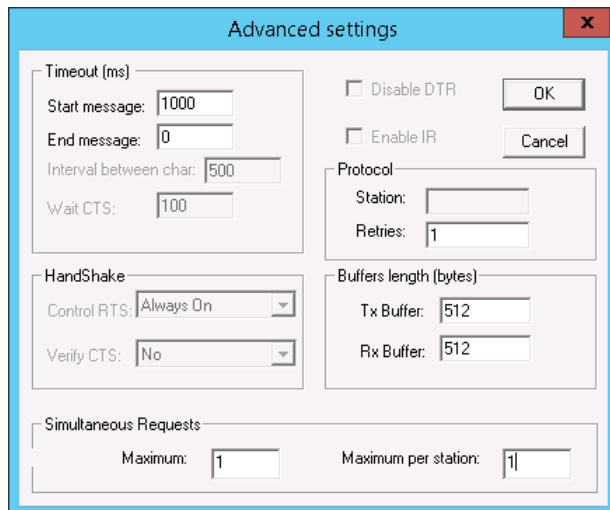
1. In the console tree, right-click Configuration and then click **Add Channel Selector Connection**. The "New\_ChannelSelector\_000" object appears in the hierarchy.



Edit the object name to appropriately describe components of your specific hardware environment. If you do not rename the object at this time, a numeric sequencing system is applied. You can rename the hierarchy entry later.

2. Specify the **Trap UDP Port**. The default is 162.
3. Click **Advanced**. The **Advanced settings** dialog appears.

The SNMP OI server will function with the advanced settings defaults. It is unnecessary to change the default settings to complete your SNMP OI server connectivity. .



- o The following parameters are configurable in the SNMP OI server:

Parameter	Default	Description
Timeout: Start message	1000 ms	Specify the timeout for the message start.

Protocol: Retries	1	Enter value to specify the number of attempts to execute the same communication before considering a communication error for this command.
Simultaneous Requests: Maximum	1	Specify the maximum number of requests that can be sent simultaneously to all connected devices.  If you plan to listen to traps sent by different devices (which are configured as device selector stations), leave the maximum and minimum at 1.
Simultaneous Requests: Maximum per station	1	Specify the maximum number of requests that may be sent simultaneously to a single device.  If you do not plan to listen to traps sent by different devices, you can set maximum and minimum values higher than 1.

- The following parameters are not applicable in the SNMP OI server, or are pre-set and are not configurable in the SNMP OI server. Descriptions are provided here for information purposes:

Parameter	Description
Timeout: End message	Reserved. Do not modify.
Timeout: Interval between char	Specifies the timeout between each character.
Timeout: Wait CTS	Specifies the timeout for the Clear to Send wait.
Handshake: Control RTS	Specifies whether to use the Request to Send control.
Handshake: Verify CTS	Specifies whether to use the Clear to Send verification type.
Disable DTR	When disabled, no DTR signal is sent before starting a communication.
Enable IR	Available only on Windows Embedded target systems. Enables use of Infrared interface (COM2 port) rather than a standard serial port to communicate with devices.
Protocol: Station	Used to specify a slave address where required.
Buffers length: Tx Buffer	Reserves memory for data transmission to the SNMP devices.  <b>Reserved. Do not modify.</b>
Buffers length: Rx Buffer	Reserves memory for data received from the SNMP devices.  <b>Reserved. Do not modify.</b>

Tx Buffer reserves the memory for data transmission to the SNMP devices.

Rx Buffer reserves the memory for data received from the SNMP devices

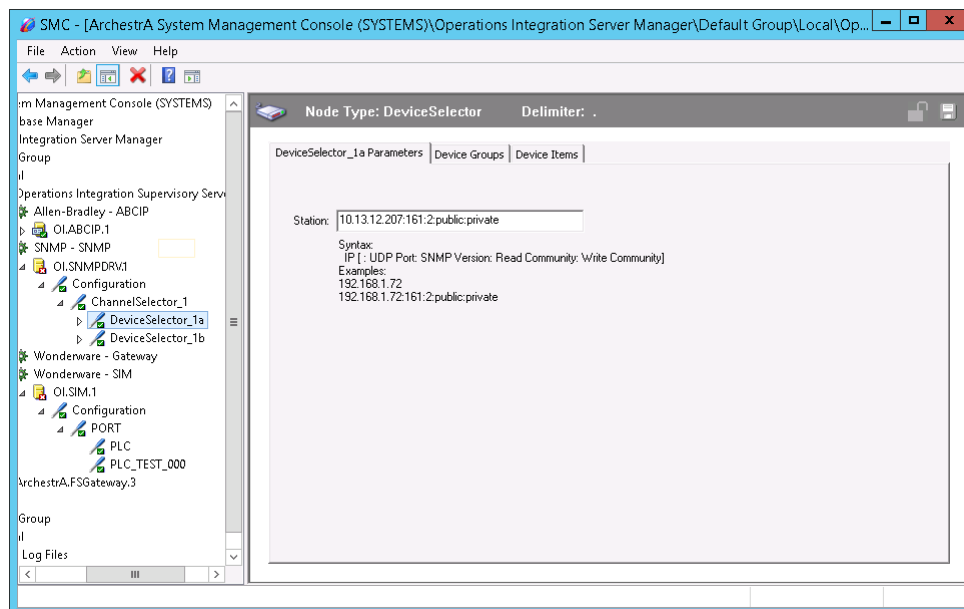
## Adding and Configuring Device Selector Objects

The SNMP OI Server can connect to different Windows agents, PLCs, and other data sources. These connections are modeled in the hierarchy by means of Device Selector objects, each of which models the end-point of the communications path.

From the **ChannelSelector** branch of the OI Server hierarchy, create the new **DeviceSelector** object.

### To add a Device Selector connection to your SNMP hierarchy

1. In the console tree, right-click the **ChannelSelector** object, and then click **Add DeviceSelector Connection**. The **New\_DeviceSelector\_000** object and associated **Parameters** configuration view appear



2. Rename the object as needed to reflect the connection.
3. Configure the **Station**.

The Station field cannot be empty. It uses the following syntax:

```
<IP Address>:<Port>:<SNMP Version>:<ReadCommunity>:<WriteCommunity>.
```

The IP address is required. Other syntax elements are optional.

Parameter	Default Value	Description
IP Address	none	The IP network address of the target device where the agent is configured. <b>Required.</b>
Port	161	The port number used by the driver for performing GET and SET operations to the OIDs. <b>Optional.</b> If not specified, the default value is used.
Version	1	The version of SNMP used. Possible values are 1 and 2, for SNMP versions 1 and 2, respectively.

		<b>Optional.</b> If not specified, the default value is used.
Read Community	public	The read community name. Case sensitive. <b>Optional.</b> If not specified, the default value is used.
Write Community	public	The write and read community name. Case sensitive. <b>Optional.</b> If not specified, the default value is used.

Communities configured in the SMC must match the communities configured in the SNMP agent. Typically, the PLC will have the settings. Refer to your PLC documentation for SNMP configuration in the specific PLC. For more information, see *Station Parameters* (on page 19).

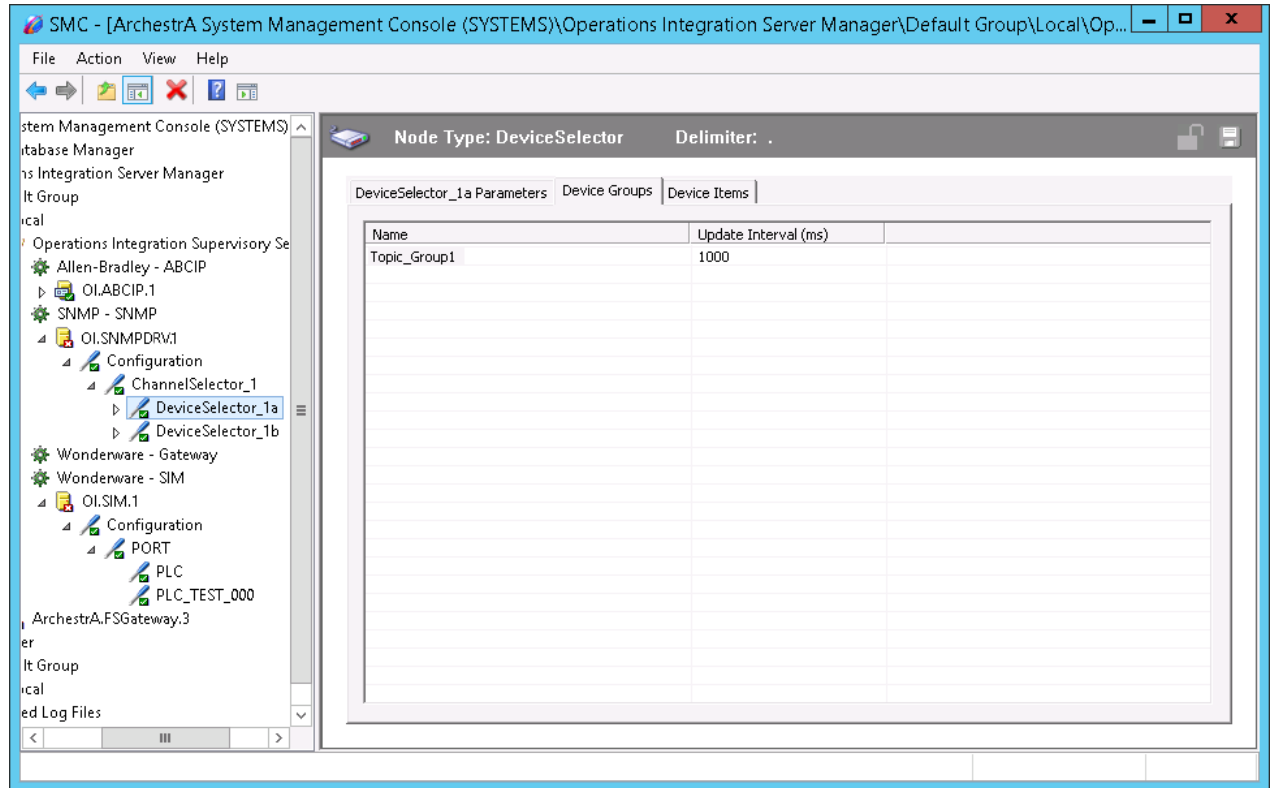
#### 4. Configure **Device Groups** and **Device Items**.

##### **Connection Tips**

1. The minimum entry parameter is the <IP Address>. If only IP address is specified, the other parameters will use the following default values: <IP Address>:161:1:Public:Public. You must ensure these parameters match the device that you are connecting to.
2. The connection port specified for regular connection to SNMP devices is different than the trap port used. The typical port for read/write operations is 161.

## Device Group Definitions

Use the Device Groups dialog box, which appears by clicking the **Device Groups** tab in the Device Selector configuration editor to create, add, delete, and define device groups. You can also configure default update intervals for the objects and edit update intervals in this dialog box.



**Note:** When you select another part of the OI Server tree hierarchy, you are prompted to save the modifications to the configuration set.

### To create or add device groups

1. Right-click in the Device Groups box and click Add.
2. Enter a unique name up to 32 characters long for the device group.

### To delete device groups

- Right-click on the device group to be deleted from the list and select Delete.

### To edit device groups

- Use the Edit option from the Device Groups tab only for configuring the OI Server's unsolicited message handling.

### To configure default update intervals

- To configure a default update interval for the object, right-click in the Device Groups box and then click Config Default Update Interval.

### To edit update intervals

- To edit the update interval for an object, double-click its value in the Update Interval column and make the edits.

or



- Right-click its value in the Update Interval column and then click Modify Update Interval.

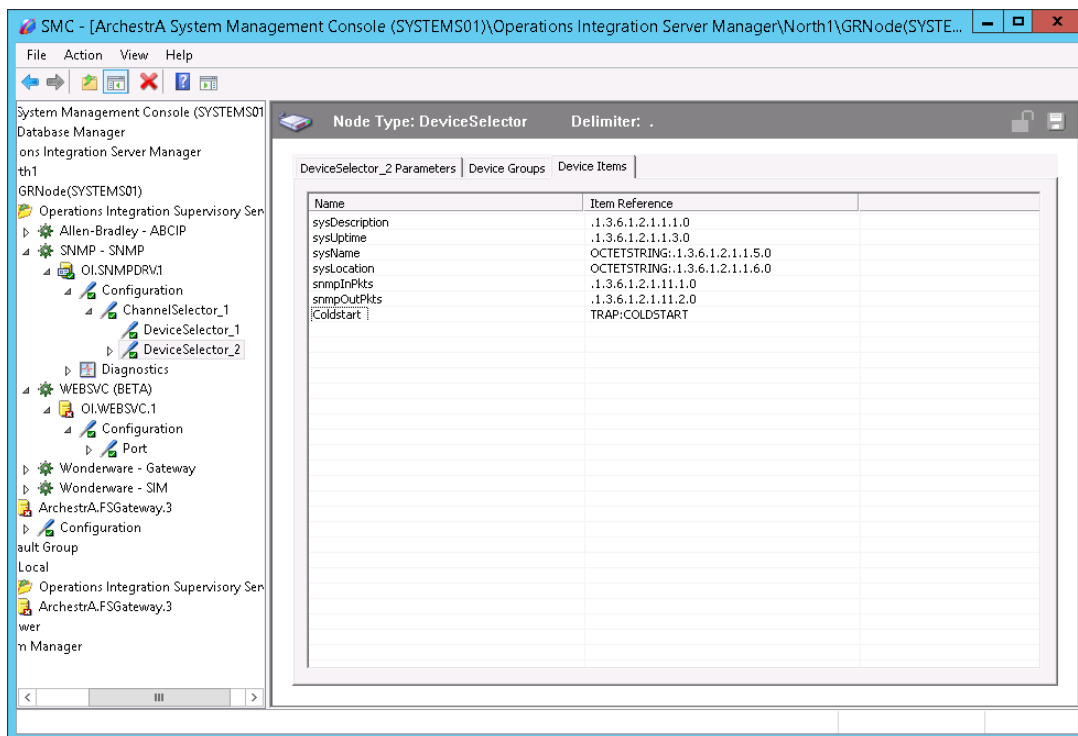
The update interval is the frequency, in milliseconds, that the SNMP OI Server acquires data from the topics associated with that device group.

Different topics can be polled at different rates from a PLC by defining multiple device group names for the same PLC and setting a different update interval for each device group.

## Device Item Definitions

Device item configuration is optional, but is strongly recommended.

You may want to use the Device Item Definition table to create more user friendly names by associating the OID with an alias or name similar to its definition as seen in the MIB file. Once the device items are so configured, you can browse by name or by item reference.



After you configure item names, the SNMP OI Server can perform GET and SET operations. Item names and references must follow these syntax guidelines:

- The **Name** is the SNMP property or object name, or a user-defined alias.
- The **Item Reference** must be the full OID, all decimals and digits.
- When using the OID as the item reference, the **Item Reference** must start with a decimal point, same as the OID.
- Alternatively, the Item Reference can incorporate the datatype as a prefix with the full OID.  
Use <datatype>:OID in the **Item Reference** in order to use device item names in reads/writes.
- Most operations with SNMP devices are read operations. The <datatype>:OID syntax is required to perform write/SET operations to an item.

In the illustration, two item references are configured with this syntax, **sysName** and **sysLocation**. These items permit read/write access. The datatype prefix allows writes to the item name.

For more information, see *Common SNMP Item References and Data Types*.

- You can specify a trap using the following syntax: <TRAP>:<TRAPTYPE>.

the TrapType can be a type of trap like COLDSTART or an OID when it is an Enterprise type trap.

The illustration shows a device item trap named "COLDSTART" with an item reference "TRAP:COLDSTART".

In this example, you could provide an OID in place of the type of trap, such as: TRAP:.1.3.6.1.6.3.1.1.5.4.

For more information, see *Using Traps* on page 21.

### To create or add device items

1. Right-click in the **Device Items** box and click **Add**.
2. In the **Name** column, type a unique item name. The maximum is 32 characters. For example, "snmplnTraps.0."
3. Double-click the line in the **Item Reference** column and enter the correlated item reference for the name you created. For SNMP, this is the OID.

### To rename device items

- Right-click the device item to be renamed and click **Rename**. Make the changes.

### To delete device items

- Right-click the device item to be deleted from the list and click **Delete**.

### To clear all device items

- Right-click in the **Device Items** box and click **Clear All**. All the device items listed are cleared after you confirm their deletion.

---

**NOTE:** You can import a .csv file containing your item definitions to help streamline configuration. See "Exporting and Importing CSV Files" in the *Wonderware Operations Integration - OI Server Manager (G-1 Series) Help*.

---

## Configuring SNMP Redundancy

The Wonderware Operations Integration Server Manager supports device redundancy. However, setting up redundant devices in the SNMP hierarchy is not recommended.

- Redundancy is not supported for traps.
- The redundant device requires a Ping Item, which for SNMP is a specific OID.

# CHAPTER 3

## SNMP OI Server References

### In This Chapter

Supported Software Environments and Devices .....	19
Station Parameters.....	19
I/O Address Syntax .....	20
Using Traps .....	21
Common SNMP Item References.....	22
Configuring an SNMP Agent in Windows.....	23

## Supported Software Environments and Devices

The SNMP OI Server supports SNMP protocol versions 1 and 2c, and all SNMP-enabled devices.

## Station Parameters

Many PLCs support SNMP version 1. By default the Read and Read/Write communities are public, as shown in the following parameters table. You can use this configuration if you want to test if your PLC or device supports SNMP. If it doesn't work, contact your device manufacturer. For a sample list of PLCs that support SNMP, see *Supported Software Environments and Devices* on page 19.

The **Station** field in the Device Selector parameters window cannot be empty. It uses the following syntax:

```
<IP Address>:<Port>:<SNMP Version>:<ReadCommunity>:<WriteCommunity>
```

Parameter	Default Value	Description
IP Address	none	The IP network address of the agent configured. Required.
Port	161	The port number used by the driver for performing GET and SET operations to the OIDs. Optional. If not specified, the default value is used.
Version	1	The version of SNMP used. Possible values are 1 and 2, for SNMP versions 1 and 2, respectively. Optional. If not specified, the default value is used.

Read Community	public	The read community name. Case sensitive. Optional. If not specified, the default value is used.
Write Community	public	The write and read community name. Case sensitive. Optional. If not specified, the default value is used.

If an IP address is not specified, an error will be returned during run time.

Following are examples of valid stations:

- 192.186.0.1
- 192.186.0.1:161
- 192.186.0.1:161:1
- 192.186.0.1:161:2:public:private

---

**Note:** The minimum required parameter in the **Station** field is the IP address. If only IP address is specified, the other parameters will use the following default values: However, we recommend specifying all parameters as in the example **192.186.0.1:161:2:public:private**.

---

Communities configured in the SMC must be identical to the communities configured in the SNMP agent. Typically, the PLC will have the settings. Refer to your PLC documentation for SNMP configuration in the specific PLC.

## I/O Address Syntax

### OID Address

Both Wonderware Application Server and Wonderware InTouch HMI can read and write to items in devices using either a reference name or the item's OID. Specify the address of the OID (used for GET and SET operations) with the following syntax:

```
Datatype:OID
```

- OID is the object identifier of the variable (when performing GET and SET operations). This parameter is required.
- The Datatype parameter is required for SET (write) actions to the OIDs, but is optional for GET (read) actions.

**Examples** of valid addresses when performing GET and SET operations:

- OCTETSTRING:.1.3.6.1.2.1.1.1.0

In this example, you can use OCTETSTRING:.1.3.6.1.2.1.1.1.0 or .1.3.6.1.2.1.1.1.0 when performing GET operations.

In this example, to perform a SET the OID should support Write actions and the item reference must be configured as INT:.1.3.6.1.2.1.1.1.0.

- OCTETSTRING:.1.3.6.1.2.1.1.1.2
- COUNTER32:.1.3.6.1.2.1.1.1.7
- TIMETICKS:.1.3.6.1.2.1.1.1.8

## Data Types

When performing GET and SET operations, Datatype is the data type of the OID. This parameter is optional when performing GET operations, and it is required when performing SET operations.

The supported values for Datatype are shown in the following table:

Value	Description
INT	When performing read and write operations with integers.
OCTETSTRING	When performing read and write operations with octet strings.
OCTETSTRINGHEX	When performing read and write operations with octet strings. Sometimes the values are reading hexadecimal, use this header to change to string.
OID	When performing read and write operations with OID values.
IPADDRESS	When performing read and write operations with IP address datatypes.
COUNTER32	When performing read and write operations with 32-bit counter datatypes.
GAUGE	When performing read and write operations with gauge datatypes.
TIMETICKS	When performing read and write operations with timeticks datatypes.
OPAQUE	When performing read and write operations with opaque datatypes.
COUNTER64	When performing read and write operations with 64-bit counter datatypes.
UINT	When performing read and write operations with unsigned integers datatypes.

## Using Traps

### About Traps

SNMP traps are alerts or events generated by agents on a managed device. Traps typically contain statistical or status information relating to a component of the device sending the trap.

SNMP managers - including the SNMP OI server - listen for traps on port 162 by default.

### Trap Syntax

Specify the address of the trap with the following syntax:

```
TRAP:OID/Variable Binding
```

When using traps, the OID can be either the object identifier of a specific trap, including enterprise traps, or it can be referenced as one of the following generic traps:

COLDSTART	The SNMP agent on the managed device reinitialized its configuration tables.
WARMSTART	
LINKDOWN	A network interface card (NIC) on the managed device

LINKUP	either fails or reinitializes.
AUTHFAIL	The SNMP agent on a managed device receives a request from an unrecognized community name.
EGPLOSS	The SNMP agent on a managed device cannot communicate with its EGP (Exterior Gateway Protocol) peer.

An enterprise trap contains vendor-specific error conditions and error codes, specific to the managed device. This type of trap is usually received with a Trap OID.

### Variable Binding

Variable Binding is the binding for the particular trap OID that is specified in the OID parameter. This parameter is optional, and is used only for traps.

If Variable Binding is specified, the item reference associated with the address will receive the value of the trap. If Variable Binding is not specified, the value of the associated item will be incremented each time a trap is received.

### Trap Address Examples

Following are examples of valid addresses when using traps. Use addresses as illustrated here as item references when configuring device items. For more information, see *Device Item Definitions* on page 17.

- TRAP:.1.3.6.1.6.3.1.1.5.4
- TRAP:COLDSTART
- TRAP:WARMSTART
- TRAP:LINKDOWN/.1.3.6.1.2.1.2.2.1.1.19
- TRAP:LINKUP/.1.3.6.1.2.1.2.2.1.1.11
- TRAP:AUTHFAIL
- TRAP:EGPLOSS
- TRAP:LINKUP
- TRAP:LINKDOWN

## Common SNMP Item References

The following table provides a list of the most commonly used attributes and associated item references, read/write access, and datatype. To get OIDs for attributes specific to a managed device, see the device documentation, or use a commercially available MIB browser.

Attribute	Item Reference	Access	Datatype
sysDescription	.1.3.6.1.2.1.1.1.0	Read-only	OCTETSTRING
sysUptime	.1.3.6.1.2.1.1.3.0	Read-only	TIMETICKS
sysObjectID	.1.3.6.1.2.1.1.2.0	Read-only	OID
sysContact	.1.3.6.1.2.1.1.4.0	Read/Write	OCTETSTRING
sysName	.1.3.6.1.2.1.1.5.0	Read/Write	OCTETSTRING
sysLocation	.1.3.6.1.2.1.1.6.0	Read/Write	OCTETSTRING
sysServices	.1.3.6.1.2.1.1.7.0	Read-only	INTEGER

snmplnPkts	.1.3.6.1.2.1.11.1.0	Read-only	COUNTER32
snmpOutPkts	.1.3.6.1.2.1.11.2.0	Read-only	COUNTER32
snmplnBadVersions	.1.3.6.1.2.1.11.3.0	Read-only	COUNTER32
snmplnBadCommunityNames	.1.3.6.1.2.1.11.4.0	Read-only	COUNTER32
snmplnBadCommunityUses	.1.3.6.1.2.1.11.5.0	Read-only	COUNTER32
snmplnASNParseErrs	.1.3.6.1.2.1.11.6.0	Read-only	COUNTER32
snmplnTooBig	.1.3.6.1.2.1.11.8.0	Read-only	COUNTER32
snmplnNoSuchNames	.1.3.6.1.2.1.11.9.0	Read-only	COUNTER32
snmplnBadValues	.1.3.6.1.2.1.11.10.0	Read-only	COUNTER32
snmplnReadOnly	.1.3.6.1.2.1.11.11.0	Read-only	COUNTER32
snmplnGenErrs	.1.3.6.1.2.1.11.12.0	Read-only	COUNTER32
snmplnTotalReqVars	.1.3.6.1.2.1.11.13.0	Read-only	COUNTER32
snmplnTotalSetVars	.1.3.6.1.2.1.11.14.0	Read-only	COUNTER32
snmplnGetRequests	.1.3.6.1.2.1.11.15.0	Read-only	COUNTER32
snmplnGetNexts	.1.3.6.1.2.1.11.16.0	Read-only	COUNTER32
snmplnSetRequests	.1.3.6.1.2.1.11.17.0	Read-only	COUNTER32
snmplnGetResponses	.1.3.6.1.2.1.11.18.0	Read-only	COUNTER32
snmplnTraps	.1.3.6.1.2.1.11.19.0	Read-only	COUNTER32
snmpOutTooBig	.1.3.6.1.2.1.11.20.0	Read-only	COUNTER32
snmpOutNoSuchNames	.1.3.6.1.2.1.11.21.0	Read-only	COUNTER32
snmpOutBadValues	.1.3.6.1.2.1.11.22.0	Read-only	COUNTER32
snmpOutGenErrs	.1.3.6.1.2.1.11.24.0	Read-only	COUNTER32
snmpOutGetRequests	.1.3.6.1.2.1.11.25.0	Read-only	COUNTER32
snmpOutGetNexts	.1.3.6.1.2.1.11.26.0	Read-only	COUNTER32
snmpOutSetRequests	.1.3.6.1.2.1.11.27.0	Read-only	COUNTER32
snmpOutGetResponses	.1.3.6.1.2.1.11.28.0	Read-only	COUNTER32
snmpOutTraps	.1.3.6.1.2.1.11.29.0	Read-only	COUNTER32
snmpEnableAuthenTraps	.1.3.6.1.2.1.11.30.0	Read/Write	INTEGER
hostSysUptime	.1.3.6.1.2.1.25.1.1.0	Read-only	TIMETICKS
SysDate	.1.3.6.1.2.1.25.1.2.0	Read/Write	DATEANDTIME
sysFreeSpace (on drives 1,2,3...)	.1.3.6.1.2.1.25.2.3.1.6.( 1,2,3 ...)	Read-only	INTEGER (kb)

## Configuring an SNMP Agent in Windows

The SNMP OI server runs on the manager - the node hosting the network management station (NMS). This manager computer monitors and manages a group of managed devices. Each managed device runs an SNMP agent, which receives instructions from and reports information to the manager.

The manager - the machine hosting the SNMP OI server - does not need an SNMP agent installed, nor SNMP Windows services enabled.

Each managed device must have an SNMP agent installed and configured. The following procedures apply with minor variations to different Windows operating systems to enable and configure the Windows SNMP service which can act as an SNMP agent to act as a target device for the OI server to manage.

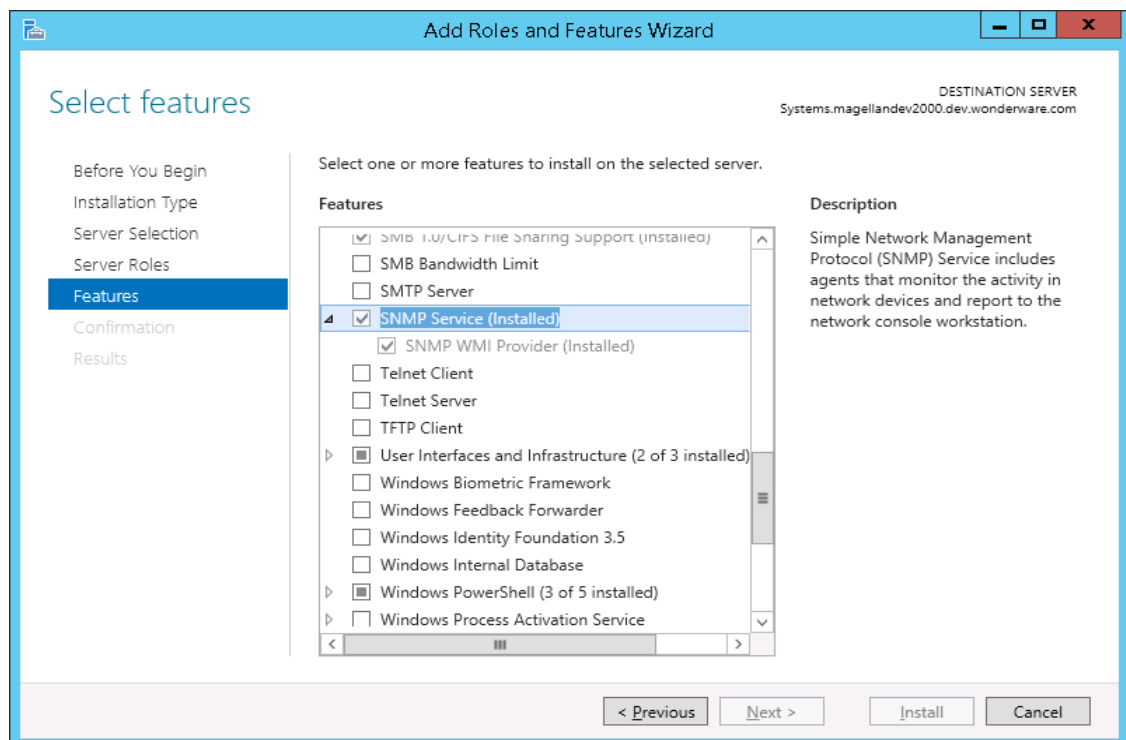
A Windows 2012 server operating system is used for illustration purposes.

### To install an SNMP agent

1. Open Windows **Control Panel**, then **Programs and Features**.

On a Windows server OS, you can use **Server Manager** to open and run the **Add Roles and Features Wizard**.

2. In the Windows features window, select **Simple Network Management Protocol (SNMP)**. Optionally, you can also select its child feature, **SNMP WMI Provider**.



3. Click **OK**. Windows installs the SNMP agent components.

### To configure an SNMP agent

1. Open **Control Panel**, then **Administrative Tools**, then **Computer Management**.

On a Windows server OS, open the **Server Manager** then select **Tools**, then **Computer Management**.

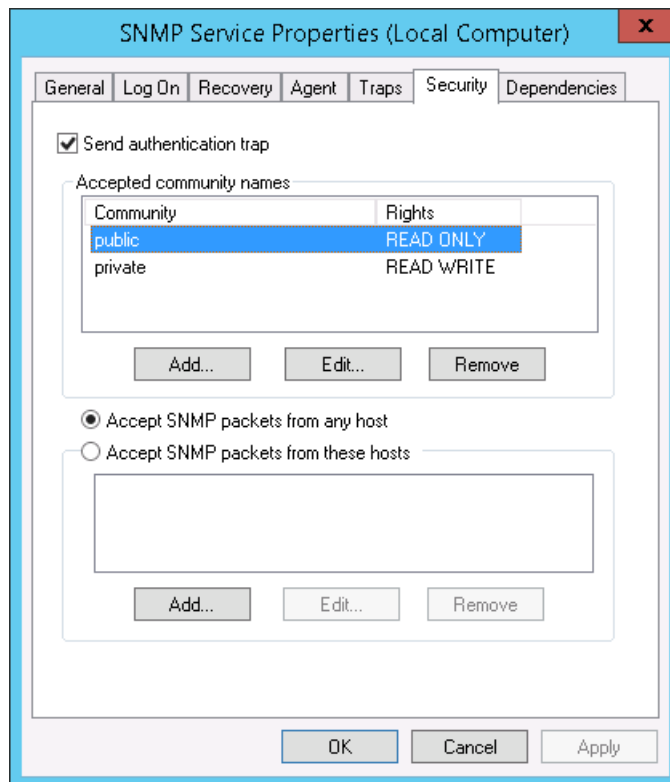
2. In the left pane, click **Services and Applications** then **Services**. The **Services** list appears.
3. In the list, right click **SNMP Services** and select **Properties** in the context menu. The **SNMP Service Properties** dialog appears.

The minimum configuration required to perform SET and GET to windows agents are:

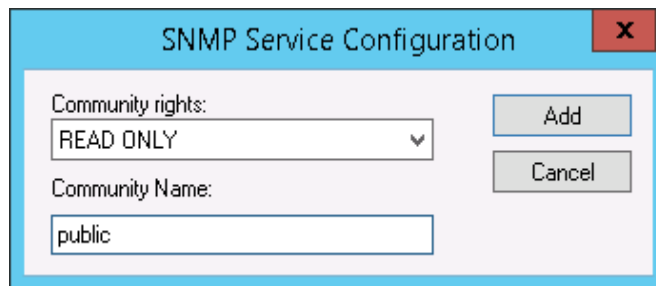
- o Add a Read Only community



- o Select **Accept SNMP packets from any host**.

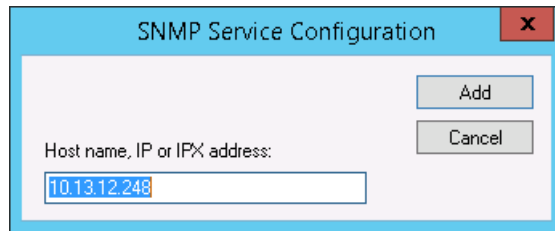


4. Click the **Security** tab.
  - a. Select **Send authentication trap** if you want the managed device to send a trap message when authentication fails.
  - b. Under **Accepted community names**, click **Add**. The **SNMP Service Configuration** dialog appears.

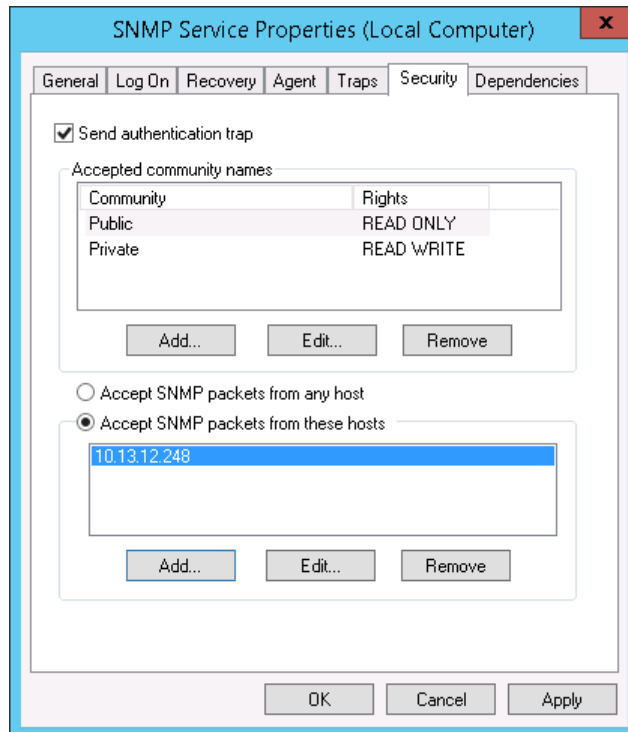


- c. Under **Community rights**, select a permission level from the list box for this node to handle SNMP requests from the selected community.
- d. Under **Community name**, enter a community name and click **Add**. The community name is case-sensitive.
- e. Choose to accept SNMP packets from any host by selecting the **Accept SNMP packets from any host** radio button.
- f. Alternatively, you can choose to accept SNMP packets from specific hosts by selecting the **Accept SNMP packets from these hosts** radio button, click **Add** to add a host address.

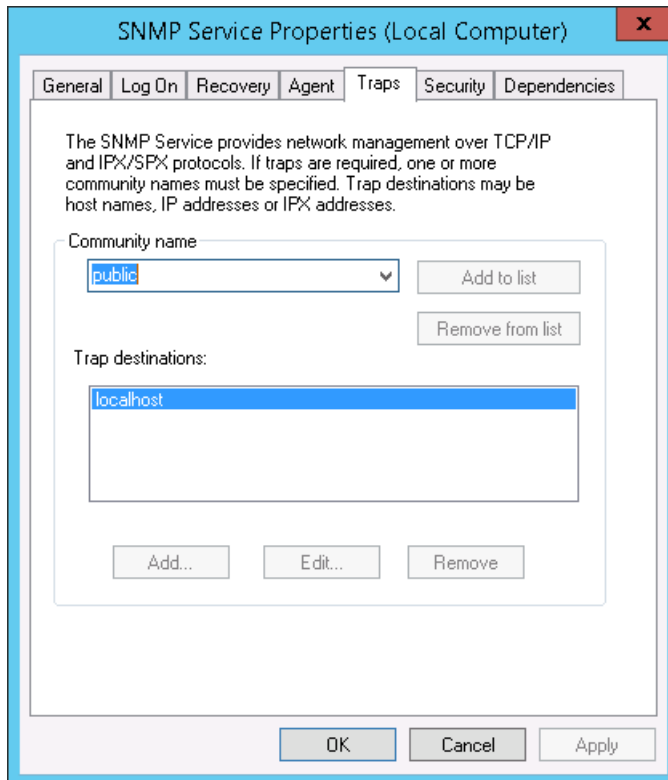
The SNMP Service Configuration, Host address dialog appears. Enter the host name or address and click **Add**.



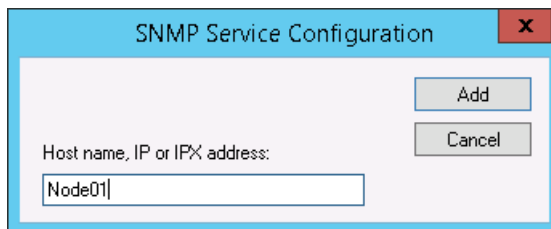
The host name or address appears in the SNMP Service Properties dialog.



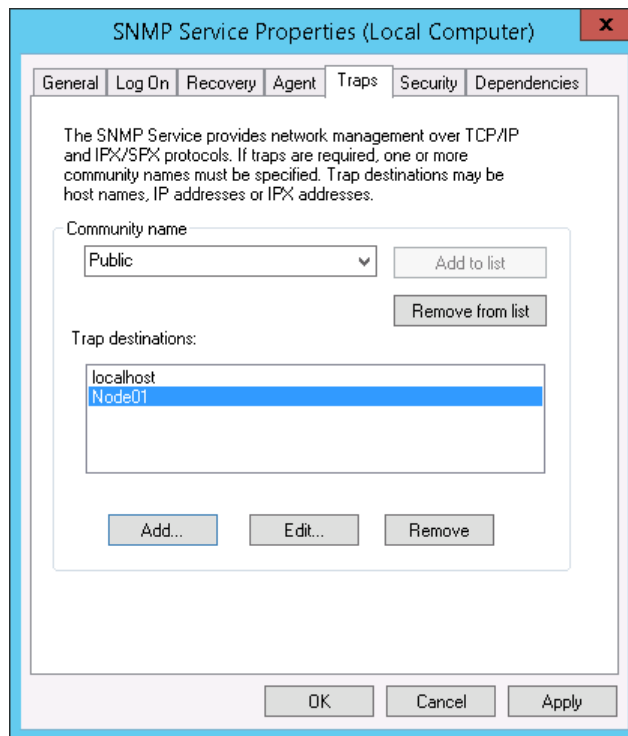
5. If you want to enable traps, click the **Traps** tab.



- Select or enter a community name in the **Community name** list box and click **Add to list**.
- Click **Add** under the **Trap destinations** text box. Enter the destination name or address in the address dialog.



Click **Add**. The destination name or address appears in the **Traps destination** list.



6. Click **OK** or **Apply** to accept the properties configuration.

# CHAPTER 4

## Troubleshooting the SNMP OI Server

### In This Chapter

Checking Status Codes.....	29
Status Codes.....	30

### Checking Status Codes

The OI Server Manager provides access to diagnostics and other statistical data. The Log Viewer provides access to event messages logged during the operation of the SNMP OI Server.

Each message sent to the System Management Console (SMC) Logger by an installed component belongs to a specific message category. Each message category has an associated log flag.

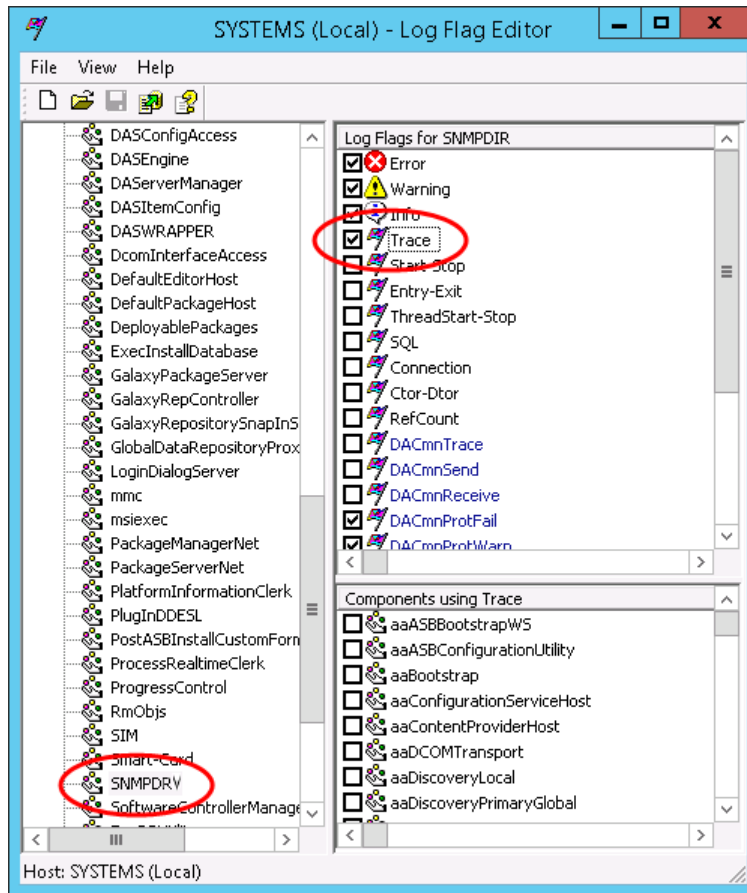
The status of a log flag indicates whether messages that belong to the message category are logged or not. When a log flag is active, messages in the associated category are logged. An inactive log flag prevents messages in the associated category from being logged.

For troubleshooting purposes, we recommend setting the SNMP **Trace** log flag in the SMC log flag editor. The **Trace** log flag determines if trace messages are logged. Trace messages for SNMP describe internal object states, variable values, and other low-level data from the SNMP OI server.

#### To set the Trace log flag for SNMP

1. Select **SNMPDRV** from the Component List view. The Log Flags view shows the log flags for the component you selected.

- In the Log Flags view, select the **Trace** check box.



- On the **File** menu, click **Apply**.

## Status Codes

Error	Description	Possible Causes	Procedure To Solve
20	Invalid Station, please check the station format.	The station format is incorrect or the field is blank.	Please refer to the correct station format supported by the server in the sections above.
21	Failed to initialize the SNMP Library.	SNMP library failed to initialize.	Internal error, restart server. If issue persists please contact support
22	Connection Failure	Failed to make a connection with the agent	Check if the IP address of the station is valid. Check if the station port and SNMP version number are valid.
23	Invalid Write	Attempted to write to an OID (perform a SET operation) which does not support it.	Check if a SET operation can be performed on the OID. Check if the datatype of the OID is included in the address. Check that the datatype of the OID in the address is correct. Note: SET operation is not supported on traps so write to the OID is not supported when header TRAP is used in the address.
25	Invalid Port Number	The port number is not valid or is not	Check the port number used. The default port for SNMP is 161 for SET and GET operations and is 162 for TRAPS.

		available on the device.	
26	Invalid Trap Session	The Trap session is not working as expected.	Check the Trap port number. Check to see if Traps are enabled on the device and if the IP address of the station is correct. Restart the server if changes are made to the Trap Port. Contact support if problem persists
27	SNMP version 3 is not supported	The station has the SNMP version number parameter configured as 3.	The server currently only supports SNMP versions 1 and 2. Check the device and see if communication can be successfully done with SNMP version 2.
28	Invalid SNMP version	The station has SNMP version number parameter configured as a value other than 1 or 2.	The server currently only supports SNMP versions 1 and 2. Check the device and see if communication can be successfully done with SNMP version 1 or 2.
29	Invalid port number	The port for the station or the trap is not available on the device.	Check the Trap port number. Check the port number used for SET and GET operations on the station. The default values for trap port and station port are 162 and 161 respectively. Restart the server if changes are made.
30	Request failed	The server is not able to successfully request data for the OIDs.	Check the station format and validity. Check that the device for which server requests data supports SNMP and that the SNMP agent is running on it. Check the OID format and validity for the request. Restart the server if changes are made. Contact Support if problem persists.
31	Response is too big	The server is not able to successfully receive data for the OIDs because the agent is not able to send the data successfully.	Check the block size of the OIDs in the request. Force a smaller block size by adding the OIDs to a Standard server sheet instead of the Main Server Sheet (maximum allowed = 50, so make the block size smaller than 50). Restart the server if changes are made.
32	No such name	The server is not able to successfully receive data for the OID requested.	Check if the OID exists in the device.
33	Bad value	The server is not able to successfully receive or write data for the OID requested.	Check if the OID has a datatype supported by the server. This usually occurs if a SET operation is performed with an incompatible type of data for the OID.
34	Read Only	The server tried to perform a SET operation on an OID that does not support it.	Check if the OID supports a SET operation. If it does, check that the datatype specified for the OID on the address is correct.

35	Response error	The server is not able to receive a response for the request.	Check the station format and validity. Check that the device for which server requests data supports SNMP. Check the OID format and validity for the request. Check that a SET operation is not being performed on an OID that doesn't support it. Restart the server if changes are made. Contact Support if problem persists.
36	Response timeout	The server is not able to receive a response for the request due to timeout with the agent.	Check the timeout settings on the server. Check the station format and validity. Check that the device for which server requests data supports SNMP. Check the OID format and validity for the request. Check that a SET operation is not being performed on an OID that doesn't support it. Restart the server if changes are made. Contact Support if problem persists.