Kymera SNMP Driver Module

User Guide

Phone: 1-800-470-2302
Fax: 1-587-400-2746
info@kymerasystems.com

Table of Contents

Phone: 1-800-470-2302
Fax: 1-587-400-2746
info@kymerasystems.com

Introduction

Features

- Gives Ignition the ability to communicate with SNMP devices.
- Can connect over TCP and UDP.

Configuration

- After installation, add a “Kymera SNMP Driver” device.
- Fill in the name parameter.
- Fill in the Connectivity section with the information for your SNMP device.
- The advanced options can be used to further customize the driver, but the defaults should be sufficient in most cases.
- Click create new device.
- Click the “Device MIB” link on the right hand side of the newly created device.
- Click the “Choose File” button and import the MIB file for your SNMP device.
- Select the appropriate MIB type from the drop down box.
- You are now ready to collect data from your SNMP device.

Phone: 1-800-470-2302
Fax: 1-587-400-2746
info@kymerasystems.com

V1 Properties

Name	The name of the device.
Enabled	To enable or disable the device instance.
SNMP Host Name	The host name or IP address assigned to the SNMP device.
SNMP Port	The port your SNMP device is listening over.
SNMP Transport	Transport method used to carry the SNMP data (TCP or UDP).
SNMP Community	SNMP Community used to communicate with the SNMP device.
Maximum Items	The maximum Items that can be added to a read request.
Read Timeout	Period in milliseconds before reporting a read timeout.
Write Timeout	Period in milliseconds before reporting a write timeout.
Retries	The number of retries before reporting a timeout.
Concurrent Requests	The number of concurrent requests supported by the driver.

Phone: 1-800-470-2302
Fax: 1-587-400-2746
info@kymerasystems.com

V2c Properties

Name	The name of the device.
Enabled	To enable or disable the device instance.
SNMP Host Name	The host name or IP address assigned to the SNMP device.
SNMP Port	The port your SNMP device is listening over.
SNMP Transport	Transport method used to carry the SNMP data (TCP or UDP).
Use GetBulk	Do bulk read requests instead of sequential requests for reading data from the tables.
SNMP Community	SNMP Community used to communicate with the SNMP device.
Maximum Items	The maximum Items that can be added to a read request.
Read Timeout	Period in milliseconds before reporting a read timeout.
Write Timeout	Period in milliseconds before reporting a write timeout.
Retries	The number of retries before reporting a timeout.
Concurrent Requests	The number of concurrent requests supported by the driver.

Phone: 1-800-470-2302
Fax: 1-587-400-2746
info@kymerasystems.com

V3 Properties

Name	The name of the device.
Enabled	To enable or disable the device instance.
SNMP Host Name	The host name or IP address assigned to the SNMP device.
SNMP Port	The port your SNMP device is listening over.
SNMP Transport	Transport method used to carry the SNMP data (TCP or UDP).
Use GetBulk	Do bulk read requests instead of sequential requests for reading data from the tables.
Maximum Items	The maximum Items that can be added to a read request.
Read Timeout	Period in milliseconds before reporting a read timeout.
Write Timeout	Period in milliseconds before reporting a write timeout.
Retries	The number of retries before reporting a timeout.
Concurrent Requests	The number of concurrent requests supported by the driver.
SNMPv3 Username	The username associated with the authentication and privacy keys.
SNMPv3 Security Name	The security name associated with the authentication and privacy keys. (Usually the same as the username)
SNMPv3 Context	The context name associated with the authentication and privacy keys.
SNMPv3 Authentication Protocol	The protocol used to authenticate the user during requests.
SNMPv3 Pass phrase	The pass phrase used to authenticate the user during requests.
SNMPv3 Privacy Protocol	The protocol used to encrypt the requests.
SNMPv3 Privacy Pass Phrase	The pass phrase used to encrypt the requests.

Phone: 1-800-470-2302
Fax: 1-587-400-2746
info@kymerasystems.com

Direct OID Addressing

It is possible to directly address an OID through the Ignition Designer. In order to do this, simply create a new OPC tag with the OPC Item Path in the format [%DeviceName%]%OID%. For example, the sysDescr OID from the device snmpDevice can be addressed [deviceName]1.3.6.1.2.1.1.1.0.

To take advantage of "bulk" functionality, you can format an OID such as "[SNMPDevice]MIB_Symbol[1]", where 1 refers to the index of an item in a table. This will signal the driver to batch reads with the proceeding OID together to be more efficient. For example, the ifPhysAddress[1] OID can be addressed [deviceName]1.3.6.1.2.1.2.2.1.2.1 . More complicated indices, such as ipAdEntAddr[192.168.1.1] are also supported, and would be addressed [deviceName]1.3.6.1.2.1.4.20.1.1.192.168.1.1.

To force an OctetString out as parsed text instead of an octet string, append "|tostring" to the end of the OPC Item Path, like [%DeviceName%]%OID%|tostring.

Custom MIB Support

In order to specify a custom MIB configuration, you must choose the "Multiple MIB" setting in the dropdown of the "Device MIB" panel. This reveals a multi-column grid, depending on resolution, with all of our included MIB files, as well as any custom ones uploaded via the interface. Simply check off which MIBs you want to use, and these will be parsed by the driver.

SNMP Trap (Notification) Event Scripting

Scripts can be executed when a trap is received by a configured device. Configuration of these scripts is done from the Designer -> Project -> Scripts -> Snmp Events window.

- Script Name : Used to identify the script to be executed. Unique names are not enforced, but it is highly recommended you use only unique script names to avoid complications.
- Port Number: The port to listen for traps on (default 162). Note: On Unix systems ports less than 1024 require the script to be run as "root", which is often not the case. Using a utility like "authbind" will allow you to listen on any port you desire.
- Community : For v1 and 2c devices, the community is used to limit which scripts get executed on the matching port. If a trap comes in that matches the port and community of a script, the script will be executed. For v3 traps, leave the community empty as the protocol does not use communities. In the case of v3 traps, the script will only execute if the port and device credentials (e.g. user/security names, auth/priv phrases) match that of the trap.
- Address: The IP address of the Ignition server. This address must be one that belongs to the Ignition server and is also on the same network as the SNMP device. The recommended address is 0.0.0.0 (which will bind all available local interfaces) but it is also possible to set this as 127.0.0.1.

SNMP Event Scripts have easy access to the listener and trap properties using the link icon on the right side of the script editing workspace. They also have easy access to the tag browser using the tag icon on the right side of the workspace.

The following snippet updates the Tooltip of a tag to indicate that a trap was handled

```
system.tag.editTag("Tags/Ramp/Ramp0", {"Tooltip":"Trap Handled"})
```

Scripting: trapParameters

In the SNMP scripting window is an accessible variable called trapParameters. It's an object that wraps up many of the properties in an SNMP trap and provides access to them via scripting. The following are methods accessible to trapParameters.

getVersion()

Description

Returns the PDU type as a string.

getRequestId()

Description

Returns the PDU requestId as a string.

getListenerAddress()

Description

Returns the listener address as a string.

getListenerPort()

Description

Returns the listener port as a string.

getSourceAddress()

Description

Phone: 1-800-470-2302
Fax: 1-587-400-2746
info@kymerasystems.com

Returns the trap source as a string. If the device is on a different subnet than the Ignition server, it may return the router address instead.

getTrapCommunity()

Description

Returns the trap community as a string.

getTimestamp()

Description

Returns the timestamp as a string.

getTrapOid()

Description

Returns the OID of the trap as a string.

getVariableBindings()

Description

Returns a Vector array of VariableBindings (see SNMP4J documentation) from the PDU.

getVariableMap()

Description

Returns a HashMap<String, String>. The keys are the variable binding OIDs in dotted string format, and the values are the VariableBindings (see SNMP4J) in string form.

getVariable()

Description

Phone: 1-800-470-2302
Fax: 1-587-400-2746
info@kymerasystems.com

Takes an OID and returns the VariableBinding associated with it as a string. This VariableBinding comes from the above variable map. This will return a null if the OID doesn't exist.

Syntax

getVariable(oid**)**

Parameters

String oid – OID associated with the VariableBinding

Returns

String – String form of the VariableBinding, if it exists. If not, returns null.

Example

trapParameters.getVariable("1.3.6.1.6.3.1.1.4.1.0") # gets the timestamp

getV1Enterprise()

Description

If the PDU is V1, this returns the enterprise OID as a string.

getV1Generic()

Description

If the PDU is V1, this returns the generic trap value as a string.

getV1Specific()

Description

If the PDU is V1, this returns the specific trap value as a string.

Example code:

#copy/paste the following into the scripting window and trigger a trap to see results in the #gateway log

tp = trapParameters

ver = tp.getVersion()

Phone: 1-800-470-2302
Fax: 1-587-400-2746
info@kymerasystems.com

```
reqId = tp.getRequestId()
listAdd = tp.getListenerAddress()
oid = tp.getTrapOid()
ts = tp.getTimestamp()
map = tp.getVariableMap()
source = tp.getSourceAddress()
args = [ver, source, reqId, listAdd, oid, ts, map]
system.util.getLogger("snmp").info(str(args))
```

Scripting: Adding devices using code

The following is some sample code that can allow users to add SNMP devices programmatically using Ignition's system.device.addDevice() function.

```
type1 = "snmpv1"
type2 = "snmpv2"
type3 = "snmpv3"

params1 = {
"enabled":True,
"snmphostname":"10.99.1.1",
"snmpport":161,
"snmptransport":"UDP",
"snmpcommunity":"public",
"maximumitems":25,
"readtimeout":1000,
"writetimeout":1000,
```

Phone: 1-800-470-2302
Fax: 1-587-400-2746
info@kymerasystems.com

"retries":2,

"concurrentrequests":5,

"mibtype":"Generic device", # must be one of the 4 options in MIB page dropdown, case sensitive

"custommibpath":"" # can be empty

}

params2 = {

"enabled":True,

"snmphostname":"10.99.1.1",

"snmpport":161,

"snmptransport":"UDP",

"usegetbulk":True,

"snmpcommunity":"public",

"maximumitems":25,

"readtimeout":1000,

"writetimeout":1000,

"retries":2,

"concurrentrequests":5,

"mibtype": "Custom MIB",

"custommibpath": "/ietf/DNS-SERVER-MIB" # note that the path separator depends Ignition server's OS; Windows is \, Linux /

}

params3 = {

"enabled":True,

"snmphostname":"10.99.1.1",

"snmpport":161,

"snmptransport":"UDP",

Phone: 1-800-470-2302
Fax: 1-587-400-2746
info@kymerasystems.com

"usegetbulk":True,

"maximumitems":25,

"readtimeout":1000,

"writetimeout":1000,

"retries":2,

"concurrentrequests":5,

"snmp3username":"username",

"snmp3securityname":"username",

"snmp3contextname":"",

"snmp3authenticationprotocol":"SHA",

"snmp3authenticationpassphrase":"passphrase",

"snmp3privacyprotocol":"AES128",

"snmp3privacypassphrase":"passphrase",

"mibtype": "Custom MIB",

"custommibpath":"/ietf/DIRECTORY-SERVER-MIB,/ietf/DNS-SERVER-MIB" # note the comma separated value for multiple MIBs

}

system.device.addDevice(deviceType=type1, deviceName="v1", deviceProps=params1)

system.device.addDevice(deviceType=type2, deviceName="v2", deviceProps=params2)

system.device.addDevice(deviceType=type3, deviceName="v3", deviceProps=params3)

Patch Notes

July 2023 build 1751: Added support for 8.1.26. Added v3 traps functionality.

Support

1 year of technical support during regular business hours - Monday - Friday 8AM to 4PM MST.

- Free Upgrades with Ignition updates (I.E. 8.0 to 8.01).
- Support may be contacted via email, at support@kymerasystems.com, or via phone, at 1-800-470-2302. Please allow up to 24 hours for a response from our support team.