WebAccess

Driver Configuration Manual

EKI-7659C

BwSNMP.dll

Driver date: 2018/6/7

English Version 1.1

Revision History

Date	Version	Author	Reviewer	Description
2018-08-22	1.0	Alger.Tan	Joseph.Chiu	Initial Release
2018-10-25	1.1	Alger.Tan	Neal.Chen	Update error code

Table of Contents

1. Introduction to BwSNMP Driver

WebAccess SCADA Node provides a BwSNMP driver to connect the all devices use SNMP protocol. Advantech EKI devices supports SNMP.

1.1 BwSNMP

The SNMP Device Driver allows data to be read from an SNMP Agent. SNMP stands for simple network management protocol. It is used to monitor the state of network devices often found in the Telecommunications and computer industries. These devices include routers, servers, even printers and copiers.

SNMP collects information two ways:

- Management stations poll the devices on the network. The WebAccess device driver acts as a management station.
- Devices send alerts to SNMP management stations. The public community may be added to the alert list so all management stations will receive the alert.

An SNMP Agent must be installed on the devices for WebAccess to communicate to the device. In SNMP terms, the device is an Agent and WebAccess is a Management station. The Agent can report in the following ways:

- Baseline - A report outlining the state of the network. WebAccess will poll the agent to get a baseline report of it values.
- Trap - An alert that is sent to a management station by agents. The WebAccess SNMP driver currently does not support 'trap" messages.

Note – the bwUPS device driver does support Trap polling.

1.2 Implementing the SNMP driver in WebAccess

The following standards apply to the connectors for the SNMP device.

- The WebAccess SNMP device driver is configured on TCP/IP connection.
- WebAccess can read data from the assigned to the "Public" community on any SNMP Agent (i.e. the device).
- WebAccess must be assigned to the "Private" community of the SNMP Agent and write must be enabled for the object, in order for WebAccess to write to an object.

1.3 SNMP Name Resolution

SNMP supports the use of IP Addresses, DNS, WINS, HOSTS file, and LMHOSTS file for name resolution.

1.4 SNMP Communities

A “Community” is part of the addressing used by WebAccess to find the SNMP information. An SNMP community is the group that devices and management stations running SNMP belong to. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. SNMP default communities are:

- Write = private
- Read = public

An SNMP community string is a text string that also acts as a password. It is used to authenticate messages that are sent between the management station (the SNMP manager, WebAccess in this case) and the device (the SNMP agent). The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent.

1.5 OID Object Identifier

WebAccess only supports the numeric OID, for example 1.3.6.1.4.1.9.3.3.1

An object identifier (or object ID or OID) uniquely identifies a managed object in the MIB hierarchy. The MIB hierarchy can be depicted as a tree with a nameless root, the levels of which are assigned by different organizations.

A Management Information Base (MIB) is a collection of information that is organized hierarchically. MIBs are accessed using a network-management protocol such as SNMP. They are comprised of managed objects and are identified by object identifiers.

The top-level MIB object IDs belong to different standards organizations, while lower-level object IDs are allocated by associated organizations.

Vendors can define private branches that include managed objects for their own products. MIBs that have not been standardized typically are positioned in the experimental branch.
For example, the managed object “atInput” can be uniquely identified either by the object name in two ways:

iso.identified-organization.dod.internet.private.enterprise.cisco.temporary variables.AppleTalk.atInput
or by the equivalent object descriptor, 1.3.6.1.4.1.9.3.3.1

As noted early, WebAccess supports only the numeric Object Identifier.

The OID can be split in WebAccess into a HEADER OID that is common to all tags on that device and the Tag Address, which specifies the unique portion of the OID for that tag.

1.6 SNMP Security

SNMP is often protected from the Internet with a firewall. Beyond the SNMP community structure, there is one trap that adds some security to SNMP.

The Send Authentication Trap is activated when a device receives an authentication that fails, a trap is sent to a management station.

Other configuration parameters that affect security are:

Accepted Community Names - Only requests from computers in the list of community names will be accepted.

Accept SNMP Packets from Any Host - This is checked by default. Setting specific hosts will increase security.

Only Accept SNMP Packets from These Hosts - Only requests from hosts on the list of IP addresses are accepted. Use IP, or IPX address or host name to identify the host.

2. Configure EKI-7659C connection by using BwSNMP

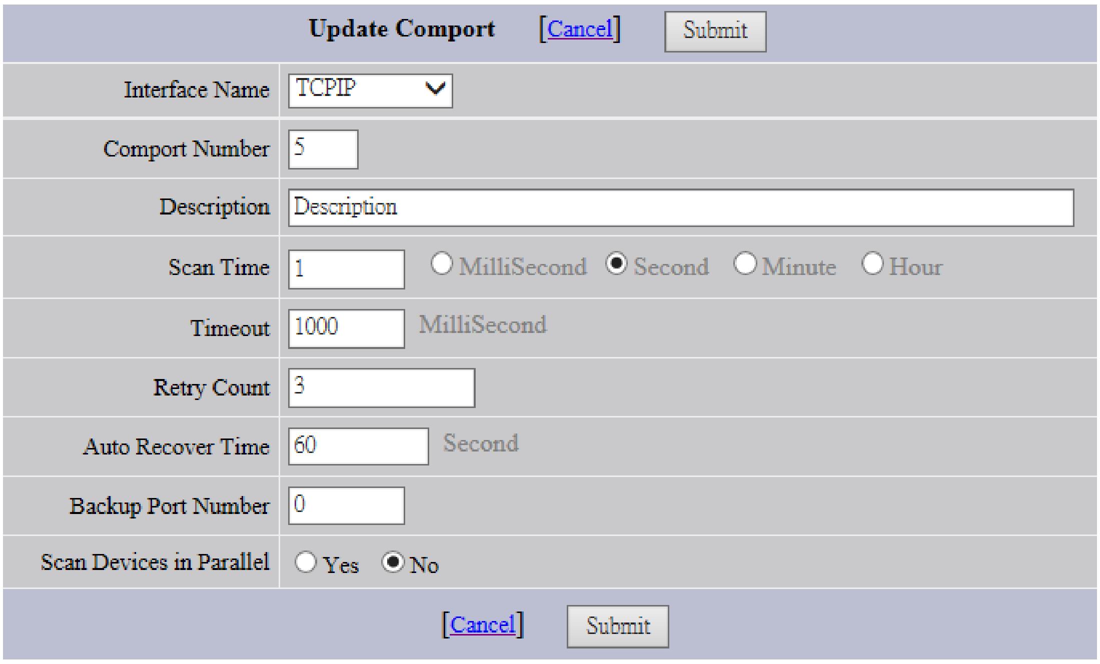
The steps, in summary, are:

1. Start Internet Explorer **Web Browser**.
2. Enter IP address of the **Project Node**.
3. Use **WebAccess Configuration**.
4. Open or Create a **Project**.
5. Configure a **SCADA node** (the PC that will connect to the automation hardware).
6. Configure a **Comport** for the SCADA Node that is a TCPIP type Comport by selecting ADD Comport from SCADA Node Properties.

Note - It is recommended to select a Comport number greater than 2 so that it does not conflict with a Serial comport that you may want to use later.

2.1 TCPIP Comport Properties

The TCPIP Comport is usually associated with an Ethernet Network Interface Card on the SCADA Node PC. Any TCPIP compatible medium is supported as long as it complies with Microsoft TCPIP protocol stack. The user should give the setting of comport number, scan time, timeout, retry count, auto recover time & scan devices in parallel by the actual connection requirements.

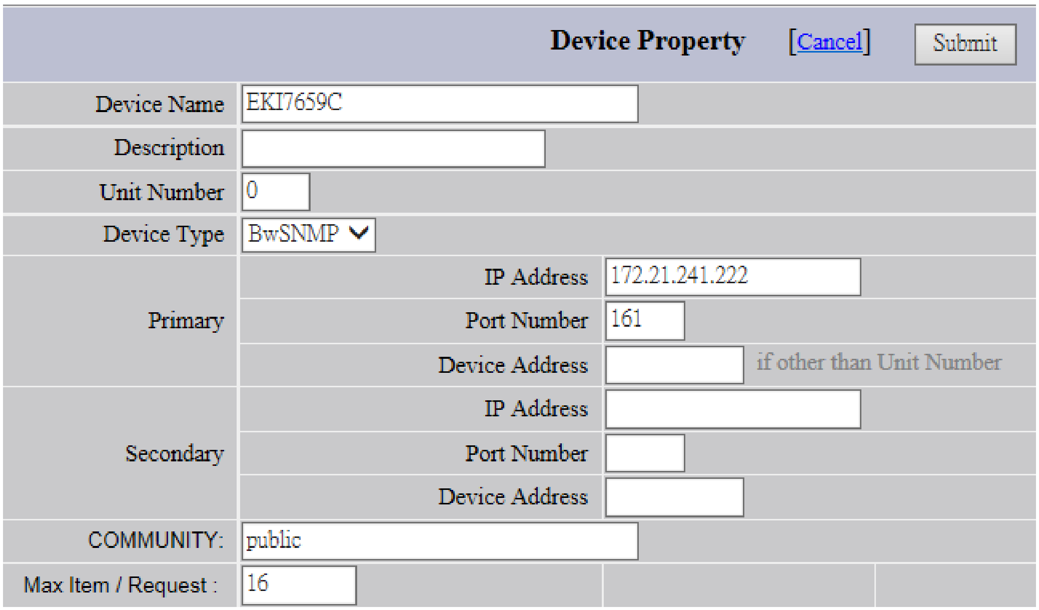


Update Comport	[Cancel] Submit
Interface Name	TCPIP
Comport Number	5
Description	Description
Scan Time	1 ○ MilliSecond ● Second ○ Minute ○ Hour
Timeout	1000 MilliSecond
Retry Count	3
Auto Recover Time	60 Second
Backup Port Number	0
Scan Devices in Parallel	○ Yes ● No
	[Cancel] Submit

Figure 2.1 TCPIP Comport properties

2.2 Device Setting

The user needs to set the device name, unit number, device type and the IP address and port number by the EKI-7659C setting. The default port number of the BwSNMP protocol is “**161**”



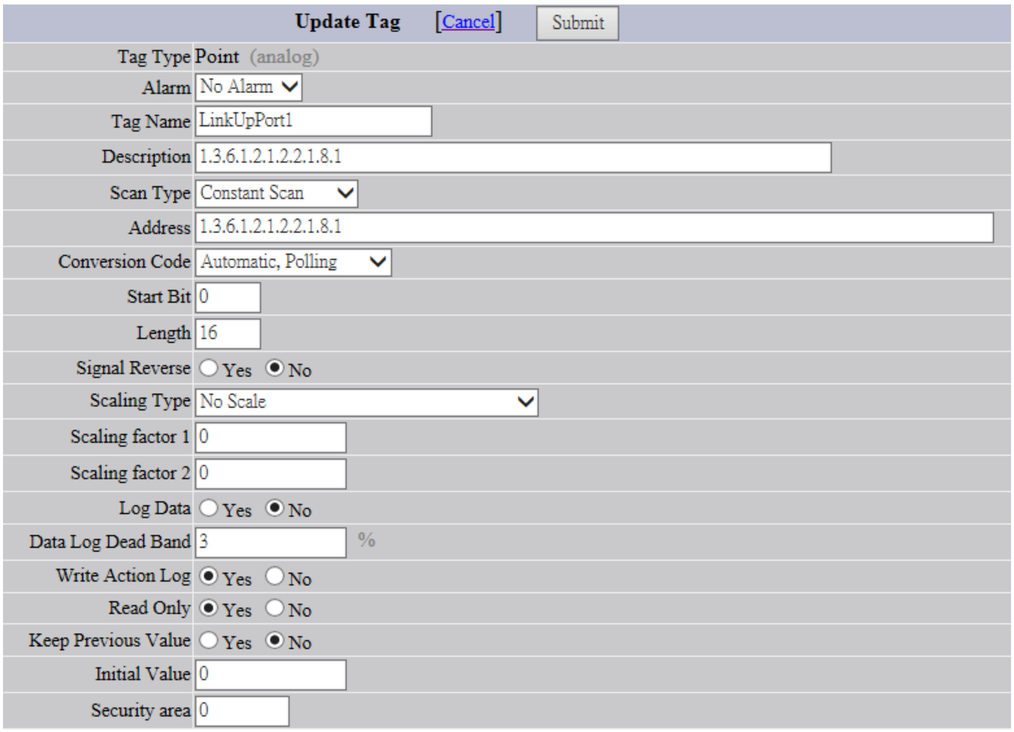
	Device Property	[Cancel] Submit	
Device Name	EKI7659C		
Description			
Unit Number	0		
Device Type	BwSNMP		
Primary	IP Address	172.21.241.222	
	Port Number	161	
	Device Address		if other than Unit Number
Secondary	IP Address		
	Port Number		
	Device Address		
COMMUNITY:	public		
Max Item / Request :	16		

Figure 2.2 BwSNMP device properties

2.3 Tag property

In the WebAccess SCADA, there are two data types for the analog and text tags. The below screenshots are the samples for the tag property setting for the EKI-7659C.

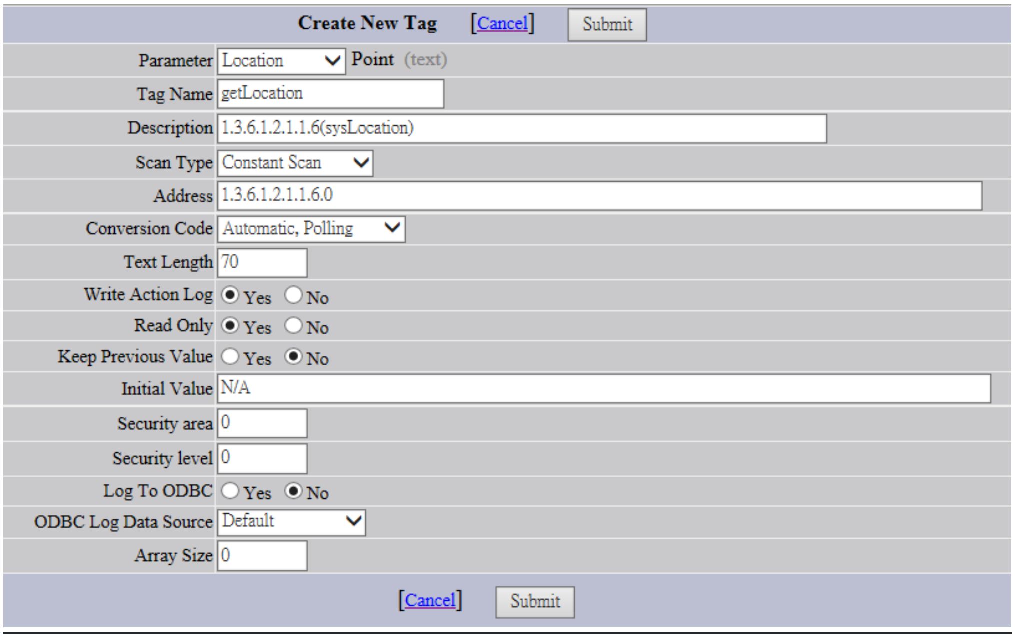
Analog tag property



Update Tag	[Cancel] Submit
Tag Type	Point (analog)
Alarm	No Alarm
Tag Name	LinkUpPort1
Description	1.3.6.1.2.1.2.2.1.8.1
Scan Type	Constant Scan
Address	1.3.6.1.2.1.2.2.1.8.1
Conversion Code	Automatic, Polling
Start Bit	0
Length	16
Signal Reverse	○ Yes ● No
Scaling Type	No Scale
Scaling factor 1	0
Scaling factor 2	0
Log Data	○ Yes ● No
Data Log Dead Band	3 %
Write Action Log	● Yes ○ No
Read Only	● Yes ○ No
Keep Previous Value	○ Yes ● No
Initial Value	0
Security area	0

Figure 2.3 The analog tag property

Text tag property



Create New Tag	[Cancel] Submit
Parameter	Location Point (text)
Tag Name	getLocation
Description	1.3.6.1.2.1.1.6(sysLocation)
Scan Type	Constant Scan
Address	1.3.6.1.2.1.1.6.0
Conversion Code	Automatic, Polling
Text Length	70
Write Action Log	● Yes ○ No
Read Only	● Yes ○ No
Keep Previous Value	○ Yes ● No
Initial Value	N/A
Security area	0
Security level	0
Log To ODBC	○ Yes ● No
ODBC Log Data Source	Default
Array Size	0
	[Cancel] Submit

Figure 2.4 The text tag property

2.4 Parameter List

Parameter	Date Type	Description	Address format
Services	Analog	1.3.6.1.2.1.1.7(sysServices)	1.3.6.1.2.1.1.7.0
UpTime	Analog	1.3.6.1.2.1.1.3(sysUpTime)	1.3.6.1.2.1.1.3.0
Contact	Text	1.3.6.1.2.1.1.4(sysContact)	1.3.6.1.2.1.1.4.0
Descript	Text	1.3.6.1.2.1.1.1(sysDescr)	1.3.6.1.2.1.1.1.0
Location	Text	1.3.6.1.2.1.1.6(sysLocation)	1.3.6.1.2.1.1.6.0
Name	Text	1.3.6.1.2.1.1.5(sysName)	1.3.6.1.2.1.1.5.0
ObjectID	Text	1.3.6.1.2.1.1.2(sysObjectID)	1.3.6.1.2.1.1.2.0
T_UpTime	Text	1.3.6.1.2.1.1.3(sysUpTime Full Text)	1.3.6.1.2.1.1.3.0

3. Error Code

8002 Binding error

8003 Open session failed

8004 Request failed

800C Timeout

8101 OID error

8104 Data type is not supported

8105 Null data

81XX Device returned error code