BwSNMP
Broadwin to SNMP Agent
(Simple Network Management Protocol)
Device Driver Guide

Table of Contents

Rev 1 – September 25, 2006

1. SNMP Agent Device Driver

1.1 Introduction to SNMP driver

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***.

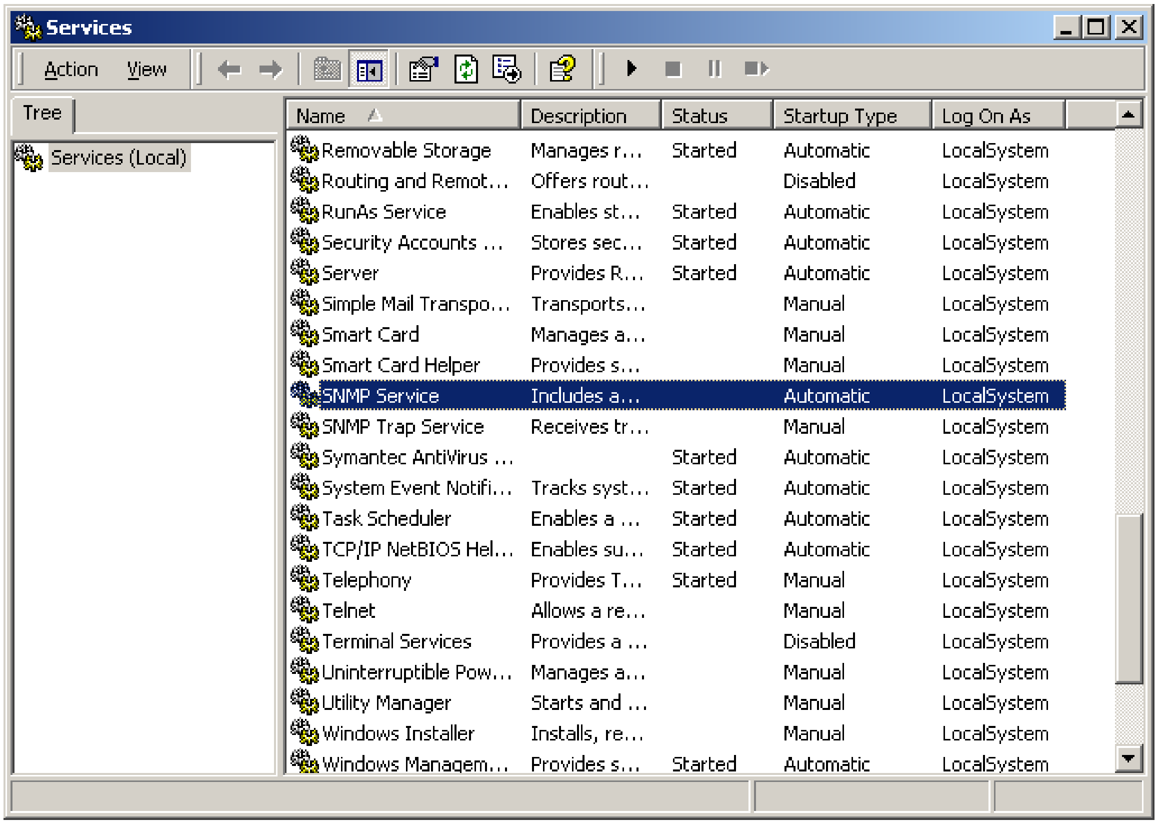
Note – the bwUPS device driver does support Trap polling.

1.2 Implementing the SNMP driver in WebAccess

The WebAccess SNMP device driver is configured on an API port (even though it uses TCP/IP connection).

The SNMP Service in Windows 2000, XP or 2003 must be installed on the SCADA node. The SNMP Trap Service will not work with the WebAccess device driver. To verify this:
Open the Control Panel -> Administrative Tools -> Services

SNMP Service should appear and be started.



Name	Description	Status	Startup Type	Log On As
Removable Storage	Manages r…	Started	Automatic	LocalSystem
Routing and Remot…	Offers rout…		Disabled	LocalSystem
RunAs Service	Enables st…	Started	Automatic	LocalSystem
Security Accounts …	Stores sec…	Started	Automatic	LocalSystem
Server	Provides R…	Started	Automatic	LocalSystem
Simple Mail Transpo…	Transports…		Manual	LocalSystem
Smart Card	Manages a…		Manual	LocalSystem
Smart Card Helper	Provides s…		Manual	LocalSystem
SNMP Service	Includes a…		Automatic	LocalSystem
SNMP Trap Service	Receives tr…		Manual	LocalSystem
Symantec AntiVirus …		Started	Automatic	LocalSystem
System Event Notifi…	Tracks syst…	Started	Automatic	LocalSystem
Task Scheduler	Enables a …	Started	Automatic	LocalSystem
TCP/IP NetBIOS Hel…	Enables su…	Started	Automatic	LocalSystem
Telephony	Provides T…	Started	Manual	LocalSystem
Telnet	Allows a re…		Manual	LocalSystem
Terminal Services	Provides a …		Disabled	LocalSystem
Uninterruptible Pow…	Manages a…		Manual	LocalSystem
Utility Manager	Starts and …		Manual	LocalSystem
Windows Installer	Installs, re…		Manual	LocalSystem
Windows Managem…	Provides s…	Started	Automatic	LocalSystem

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.

1.2.1 Addressing in SNMP

An example addressing in SNMP is

IP Address: 10.0.0.2

Community: public

OID (object identifier): 1.3.6.4.1.1.2.2.2.2.1.3.4

Note: The WebAccess device driver only uses numeric OIDs..

Example Access Database – Table named Table1

1.2.2 SNMP Name Resolution

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

1.2.3 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.

1.2.4 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.

1.3 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.

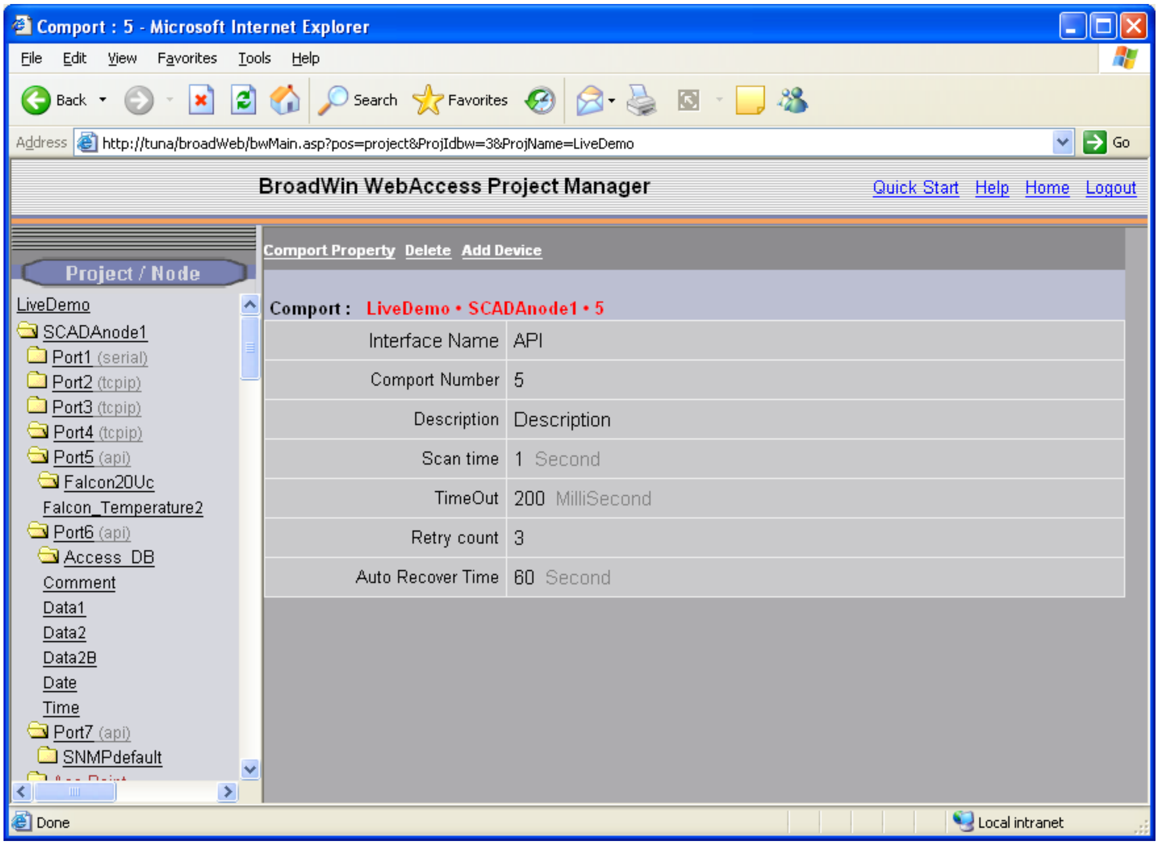
1.4 API Comport and SNMP device

1.4.1 Configure an API Comport and a SNMP Device

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 **Projec**t.
5. Configure a **SCADA node** (the PC that will connect to the automation hardware).
6. Configure a **Comport** for the SCADA Node that is an API type Comport by selecting ADD Comport from SCADA Node Properties.

7. For the **Interface Name**, select **API**. Wait for the page to update.


Comport : 5 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://tuna/broadWeb/bwMain.asp?pos=project&ProjIdbw=3&ProjName=LiveDemo Go
BroadWin WebAccess Project Manager
Quick Start Help Home Logout
Project / Node
LiveDemo
SCADAnode1
Port1 (serial)
Port2 (tcpip)
Port3 (tcpip)
Port4 (tcpip)
Port5 (api)
Falcon20Uc
Falcon_Temperature2
Port6 (api)
Access_DB
Comment
Data1
Data2
Data2B
Date
Time
Port7 (api)
SNMPdefault
Comport Property Delete Add Device
Done
Local intranet

Comport : LiveDemo • SCADAnode1 • 5

Interface Name	API
Comport Number	5
Description	Description
Scan time	1 Second
TimeOut	200 MilliSecond
Retry count	3
Auto Recover Time	60 Second

Figure – API type comport used with SNMP driver

8. Enter a **Comport Number**. This is a virtual communications port. It does not need to match an actual COM port number. It is recommended to use a comport number above 4 to avoid conflicts with a real comport on the SCADA node (for example a serial comport).

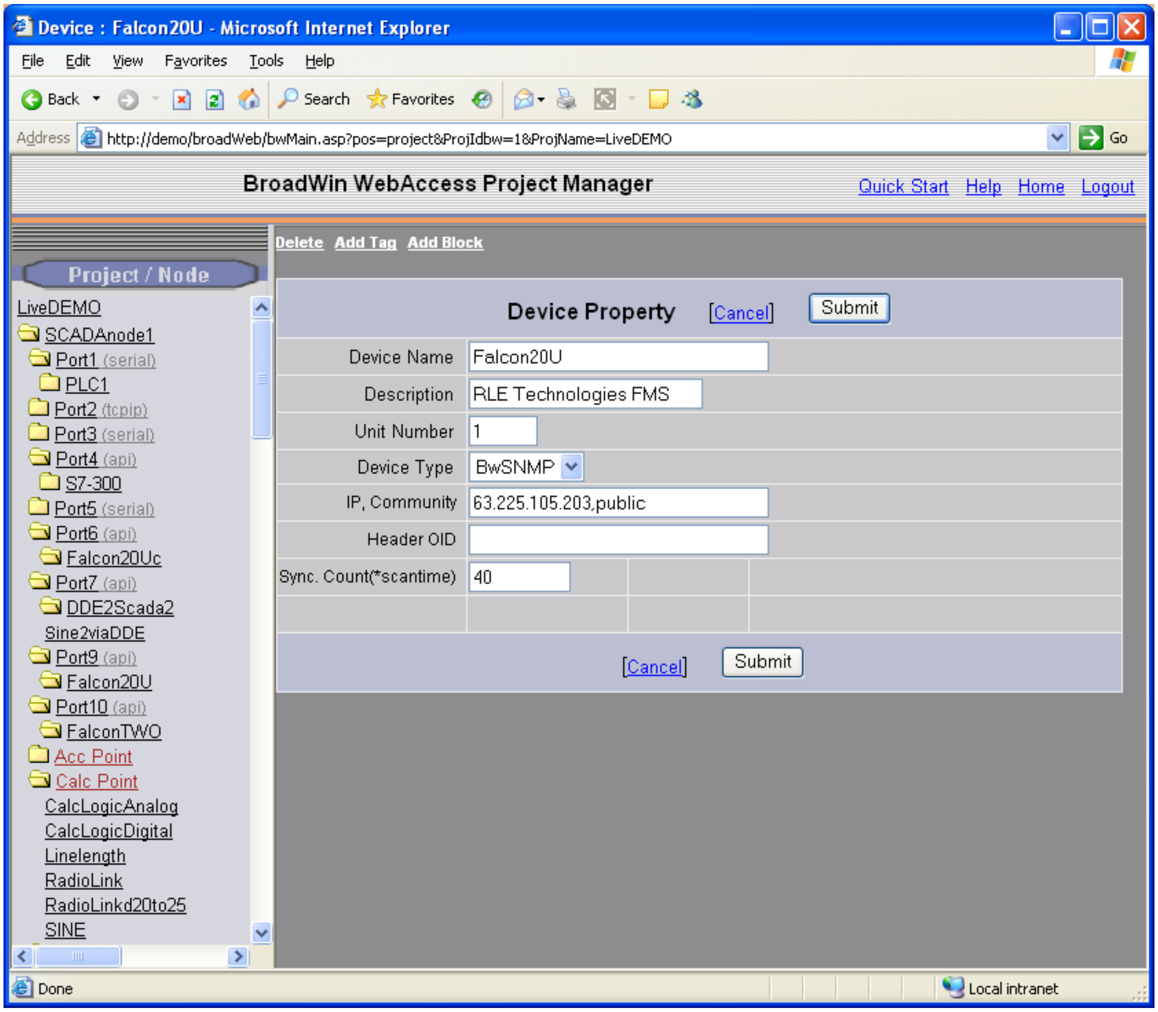
9. Configure **Scan Time**, **Timeout, Retry** and **Auto Recover**.

   See 1.3.2 API Comport Properties in the following section for more information.

10. Press **Submit** to save the API Comport properties.

11. Select the API Comport (Port 6 in the Example) from the left menu list.

12. Configure a SNMP Device (determines the communications Protocol or Device Driver) using **Add Device**.



http://demo/broadWeb/bwMain.asp?pos=project&ProjIdbw=1&ProjName=LiveDEMO

Device Property [Cancel] Submit

Device Name	Falcon20U
Description	RLE Technologies FMS
Unit Number	1
Device Type	BwSNMP
IP, Community	63.225.105.203,public
Header OID	
Sync. Count(*scantime)	40

[Cancel] Submit

Figure – Example SNMP Device without Header OID. The full OID must be entered in each tag's address field

13. Select the **Device Type** is **SNMP.** Wait for the Page to update.

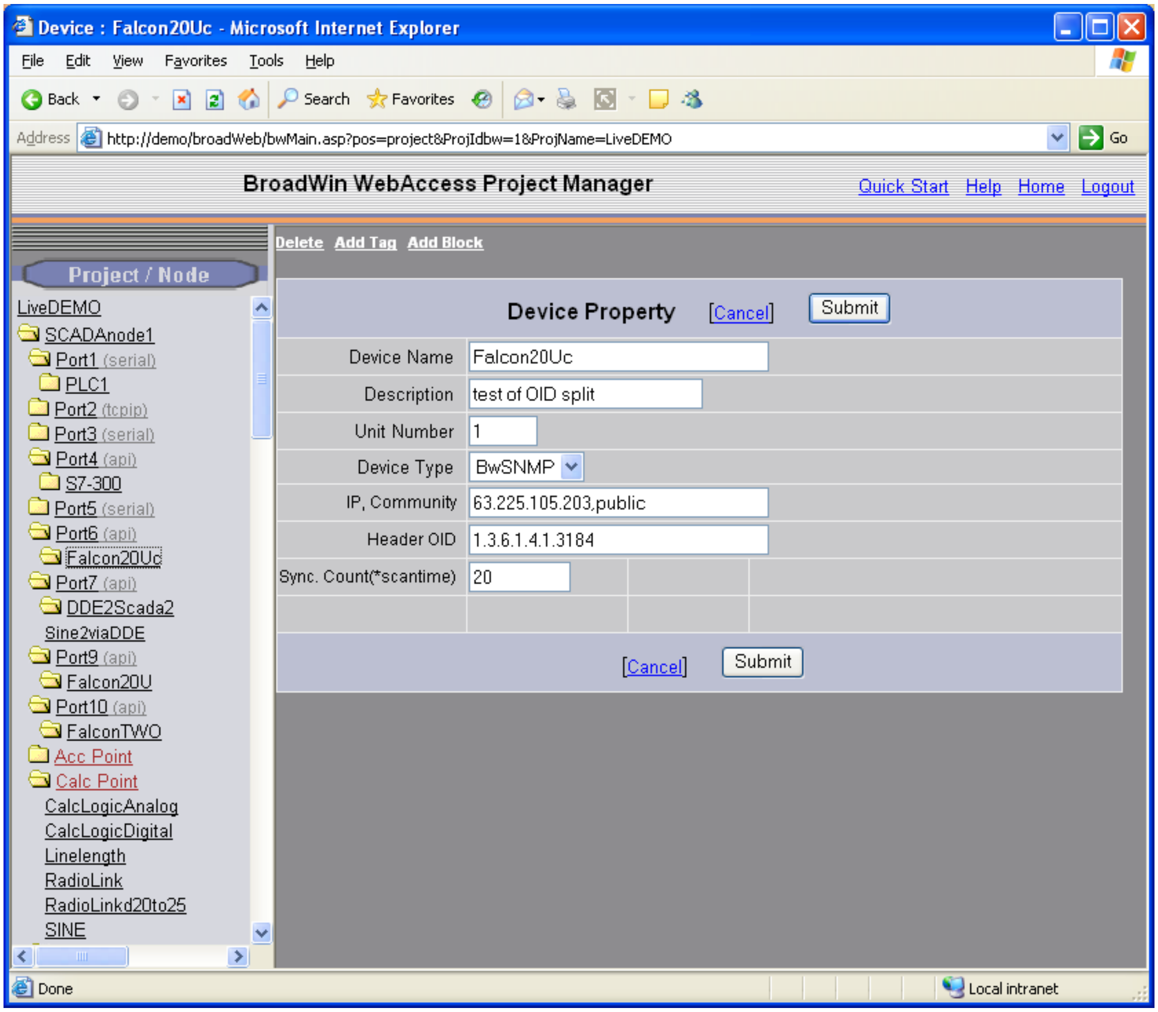
14. Enter a **Unit Number**. This is a virtual number. Use whatever makes sense to your end user.

15. Enter **IP** (Data Source Name) and **Community** separated by comma (,). For example 63.225.105.203,public

16. Optionally enter a Header OID. This header will be pre-appended to the OID address in each tag associated with this device. The Header OID is intended to save typing the common part of the OID in every tag.

Note – if the Header OID is not used, the full OID must be specified in the Tag's address field.

If a Header OID is specified, that part of the OID should be removed from the Tag's address field.



Device Property [Cancel] Submit

Device Name	Falcon20Uc
Description	test of OID split
Unit Number	1
Device Type	BwSNMP
IP, Community	63.225.105.203,public
Header OID	1.3.6.1.4.1.3184
Sync. Count(*scantime)	20

[Cancel] Submit

Figure – Header OID will be pre-appended to each Tag associated with this device.

17. Press **Submit** to save the SNMP device properties.

1.4.2 API Comport Properties

1.4.2.1 Comport Number

This is a virtual communications port. It does not need to match an actual COM port number. It is recommended to use a comport number above 4 to avoid conflicts with a real comport on the SCADA node (for example a serial comport).

1.4.2.2 Description

This is an optional field used for user reference.

1.4.2.3 Scan Time

This is the time in milliseconds, seconds, minutes or hours to scan the DSN and the Database. This must match the ability of the network and Database to respond. Very large databases, with many records may take a long time to respond.

If the network, DSN and database cannot respond as fast as the SCAN Time entered, WebAccess will scan at a slower rate.

1.4.2.4 Timeout

Timeout is the time waited before re-sending a communications packet that did not have a reply. Timeout is in milliseconds.

TimeOut specifies how long the software waits for a response to a data request, specifically to wait for a reply from one packet. A recommended value is 3 seconds, longer if the communication device is slow. This is protocol dependent: some protocols do not allow changes in time out.

Combined with Retry count, TimeOut also determines time to consider a device or port as BAD. Timeout is the time to wait since last communication packet sent without a reply. Time is in milliseconds. The slow or poor quality communications require longer timeout. The faster the communications network or device, the shorter the timeout required. Shorter timeouts notify operators of communications failure more quickly.

1.4.2.5 Retry Count

Number of times to retry communications if no reply is received from a device. Combined with Timeout, also determines time to consider a device or port as BAD.

In addition, Indicates the number of times after the first attempt has failed that communication should be attempted before indicating a failure. Specifically, how many times to send a single packet after the DSN or Database fails to respond to the first packet. After the retry count is exceeded, all the tags in the packet are marked with asterisks and the next packet of requests is sent. A reasonable value is 3 to 5 times. After this number of tries, the tags in this packet are marked as "fail to respond" (i.e. asterisks) and are disabled. In reality, increasing the number of retries hides failures on the part of the DSN or Database to respond to a request. Essentially, increasing the retries gives the DSN or Database more chances to reply.

1.4.2.6 Auto Recover Time

Auto Recover Time is the time to wait before attempting to re-establish communications with a BAD device or port.

1.4.3 BWDB Device Properties

1.4.3.1 Unit Number

This is a virtual number. Use whatever makes sense to your end user. This will appear in Detail Displays and Communication Status Display.

1.4.3.2 IP, Community

An example in SNMP is 10.0.0.2, public

IP Address: 10.0.0.2

Community: public

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.

1.4.3.3 OID HEADER– Object Identifier Header

OID Header is Optional.   It will be pre-appended to the address of each tag to form the complete OID.

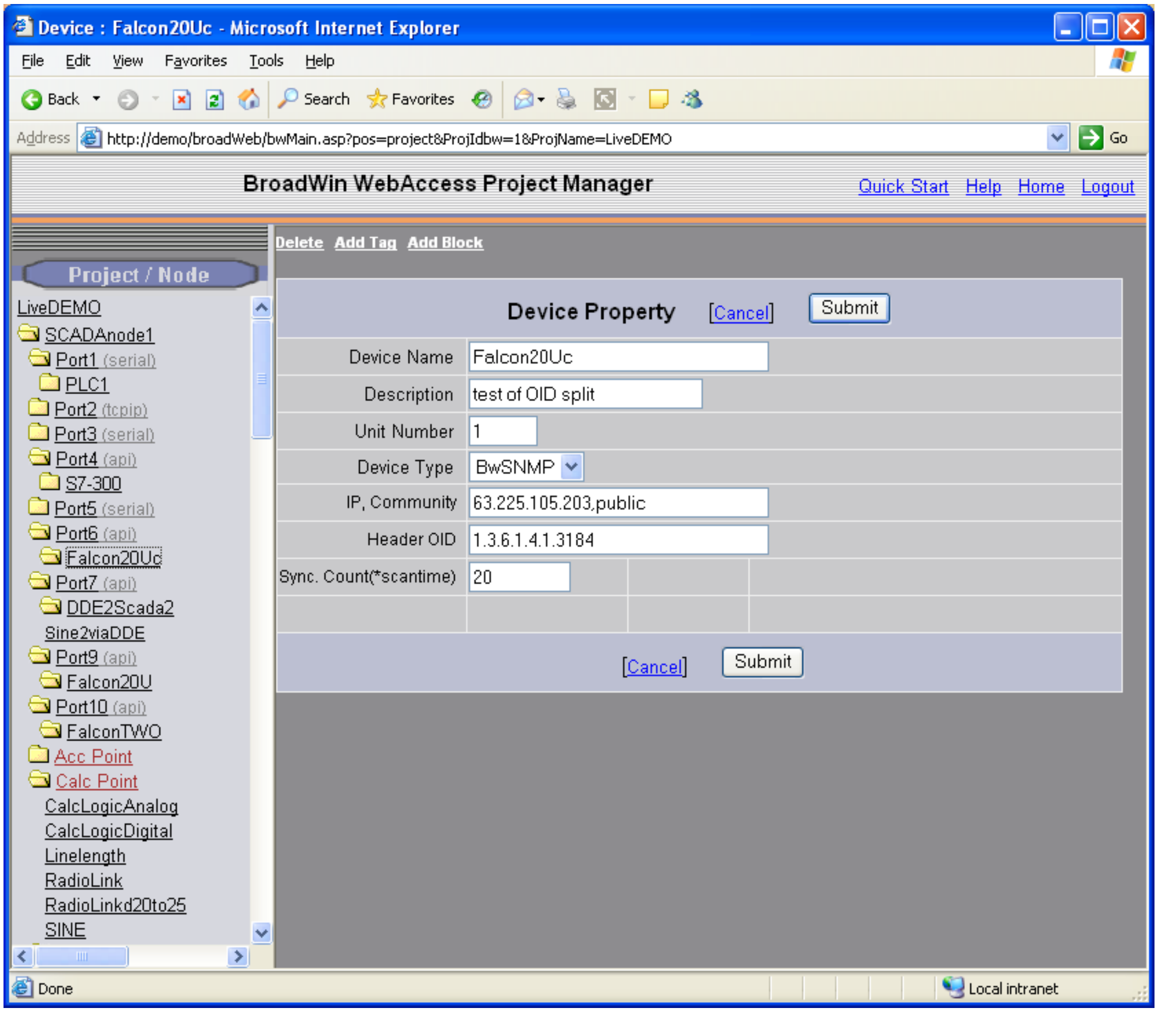
Note - WebAccess only supports the numeric OID, for example 1.3.6.1.4.1.9.3.3.1

1.4.3.4 Sync. Count

This is the number of scans before the entire device is polled again.

1.5 Configure a TAG

1. Use **Add Tag** to create tags from Device Properties page.



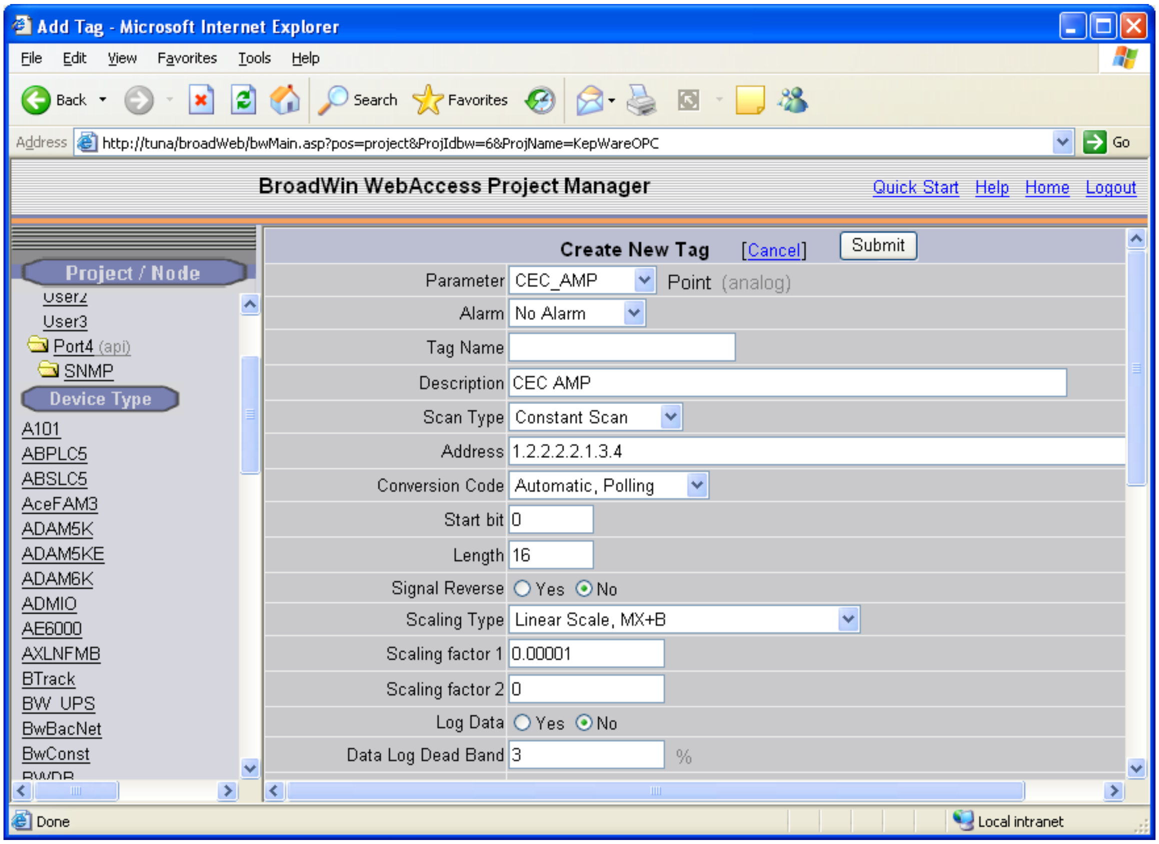
Device Property [Cancel] Submit

Device Name	Falcon20Uc
Description	test of OID split
Unit Number	1
Device Type	BwSNMP
IP, Community	63.225.105.203,public
Header OID	1.3.6.1.4.1.3184
Sync. Count(*scantime)	20

[Cancel] Submit

Figure – Use Add Tag or Add Block to create Tags in SNMP device

2. The **Create New Tag** page opens.



Create New Tag [Cancel] Submit

Parameter	CEC_AMP Point (analog)
Alarm	No Alarm
Tag Name	
Description	CEC AMP
Scan Type	Constant Scan
Address	1.2.2.2.2.1.3.4
Conversion Code	Automatic, Polling
Start bit	0
Length	16
Signal Reverse	○ Yes ● No
Scaling Type	Linear Scale, MX+B
Scaling factor 1	0.00001
Scaling factor 2	0
Log Data	○ Yes ● No
Data Log Dead Band	3 %

3. Select a **Parameter** to match the type of data to be read or written (from the example above, select Analog1 or Date).

4. Select ALARM to enable alarming for Analog or Discrete Tags. The page will refresh if ALARM is selected, so it is best select alarm first before entering any other data. You can always enable alarming after saving the Tag.

5. Enter a **Tag Name**. This is how users, graphic displays, scripts and dialog boxes will refer to the information.

6. Optionally enter or modify the **Description**.

7. Modify the **Address**. The **Address** is the OID (Object Identifier) in the MIB of the SNMP Agent. A typical OID is the part after the word private or public.

An example addressing in SNMP is

IP Address: 10.0.0.2

Community: public

OID (object identifier): 1.3.6.4.1.1.2.2.2.2.1.3.4

If you have used an OID Header in the device configuration, remove the OID Header from the address used at the tag.

8. Optionally modify the **Scan Type**.

   Constant Scan will scan at the configured Scan Rate of the Com Port.

   Display Scan will read the Tag only if it appears in a Graphic Display. Real-Time Trend, Detail Display or Dialog Box (e.g. Point Info Dialog Box).

9. Optionally modify the **Conversion Code**.

   For the SNMP device (bwSNMP) **only Automatic, Polling is supported!**

   The Automatic, Trap is used only with the bwUPS device.

1.5.1 Analog Tag

10. For an Analog Tag, optionally modify the Scaling Type.

    No Scale uses the value as it is entered in the database.

    For more information see the Engineering Manual, section 4.2.13 (Click on Help in the Project Manager to open the Engineering Manual).

Note – the SNMP device driver ignores Start Bit and Length.

11. For an Analog Tag, assign **Alarms**, **Scaling**, **Engineering Units**, Description and other features

    Refer to the Engineering Manual, section 4.2 Analog Tag Properties, for more information on configuring Analog Tags.

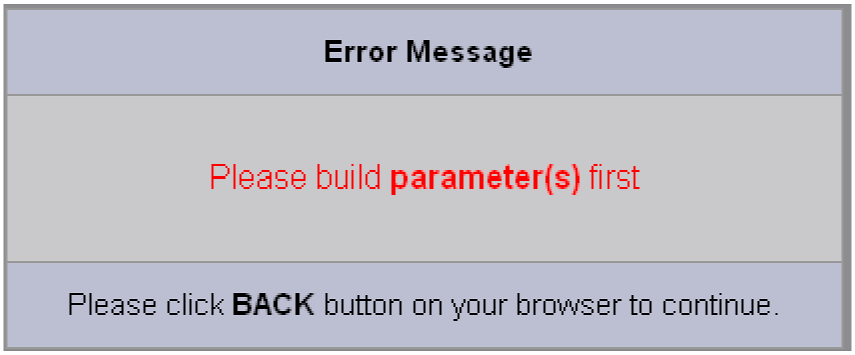
12. Press **Submit** to save this Tag.

13. **Download** to the SCADA node.

1.5.2 Discrete Tag

Note – there are no discrete parameters in the default bwSNMP driver. You will have to configure a discrete parameter before adding any discrete tags.

If you have not built any parameters you will get an error message. Please refer to the previous section on building parameters,



Error Message

Please build **parameter(s)** first

Please click **BACK** button on your browser to continue.

Figure – configure Parameters before you can build Tags in BWDB device

1. Optionally enter a **Scan Type**.

   Constant Scan will scan at the configured Scan Rate of the Com Port.

   Display Scan will read the Tag only if it appears in a Graphic Display. Real-Time Trend, Detail Display or Dialog Box (e.g. Point Info Dialog Box).

2. For the **Conversion Code**, select **Number** from the drop-down menu.

3. Optionally enter a **State Descriptors** for State 0, State 1, State 2, etc.

   The 'NotUsed' entry disables that state. States must be continuous.

   If STATE 0 and STATE1 are used, then this is a Digital Tag (e.g. 2-State, one bit).

   If STATE 0, STATE 1 and STATE 2 are used, then this is a 3-State Tag, (behaves as if two bits are read).

Note – the SNMP device driver ignores Start Bit and Length.

4. Press **Submit** to save the Discrete Parameter.

1.5.3 Addresses

The **Address** is the Field Name or Column in the Database Table.

You have to use the actual Field Names (column names) in your database. You will need a copy of the Database Software program to open the Database to see the Field Names (Column Names). For an Access Database example, see section **錯誤! 找不到參照來源。** Example Access Database and Table.

1.5.4 Conversion Code

The conversion code is used to interpret the data as number, discrete state, or text.

For a number (e.g. Analog tag), use **Number**.

For a Discrete or Digital Tag, use **Number**.

For a Text or character data, use **Text**.

1.5.5 Start Bit

The SNMP driver ignores the Start Bit field.

1.5.6 Length

The SNMP driver ignores the Length field. The Analog and Discrete Tags always read the full number in the Database. The Discrete Tags use the number of State Descriptors that are used to determine the number of States.

1.5.7 State 0, State 1, State 2, etc.

State Descriptors for State 0, State 1, State 2, through State 7 are used to determine the number of states for a discrete tag

The 'NotUsed' entry disables that state. States must be continuous.

If STATE 0 and STATE1 are used, then this is a Digital Tag (e.g. 2-State, one bit).

If STATE 0, STATE 1 and STATE 2 are used, then this is a 3-State Tag, (behaves as if two bits are read).

If STATE 0 through STATE 7 are used, then this is a 7-State Tag, (behaves as if three bits are read).

Note – the SNMP device driver ignores Start Bit and Length.

1.6 Blocks

Currently, there are no pre-configured block types in the SNMP driver. You must configure parameters and blocks

1.7 Troubleshooting

1.7.1 * [8000]

Follow these steps:

1 . Ping the device.

If the device is accessible by Ping, then its IP address is valid and you may have a problem with the SNMP setup. Go to step 5.

If the device is not accessible by Ping, then there is a problem with either the path or the IP address.

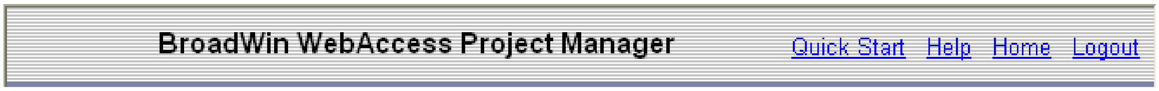
2 . If your management station is on a separate subnetwork, make sure that the gateway address and subnet mask are set correctly.

4 . Using another management application, perform an SNMP Get and an SNMP Set (that is, try to poll the device or change a configuration using management software).

5 . If you cannot reach the device using SNMP, access the device's console and make sure that your SNMP community strings and traps are set correctly.

1.8 Open the Engineering Manual

The Engineering Manual can be opened from a hyperlink in the Project Manager at the top left of every page.


BroadWin WebAccess Project Manager

This will open the Web Help version of the Engineering Manual from any Web Browser.