

EBM **MILITARY FIELD-GRADE**

EXPANSION BATTERY MODULE

Operator's Guide *Ethernet & SNMP*



EBM-1000-2U

SynQor[®]
Advancing The Power Curve[®]

EBM with Ethernet Interface

Contents

1	Overview	2
2	Initial Configuration	2
2.1	DHCP Server	2
2.2	NetBIOS Hostname	2
2.3	Local Connection.....	2
3	Web Interface	3
3.1	MONITOR Page	4
3.2	CONTROL Page	5
3.3	NETWORK Page.....	7
3.4	ALERTS Page	9
3.5	SNMP Page.....	10
3.6	DEBUG Page	13
3.7	TLS Support	13
3.8	Certificates	14
4	SNMP Interface	17
4.1	SNMP Exposed Objects	17
4.2	SNMP Traps.....	29

1 Overview

The Ethernet Interface on the SynQor EBM-1000 product adds a web interface and an SNMP interface for control, configuration, and reporting. This guide provides information regarding initial setup and functionality of the network interfaces.

The web interface provides a dynamically updated set of pages for user interaction. The SNMP interface exposes the RFC-1628 standard UPS-MIB interface.

2 Initial Configuration

In order to facilitate connecting to the web interface, the EBM network interface provides multiple methods to identify the EBM on the network. The user must load the web interface to enable or configure the SNMP interface.

2.1 DHCP Server

The EBM network interface will recognize a DHCP server on the network and use the IP address assigned by the server. A network administrator can register the MAC address of the network interface with the DHCP server to assign the EBM to a static IP address. The MAC address can be read in two ways: (1) via the RS232 serial command “NETWORK?”; and (2) via the web interface, assuming a connection is made before the static IP address is assigned (see below).

Once a DHCP server assigns an IP address to the EBM, the web interface can be loaded by pointing a web browser to the address <http://x.x.x.x/>, where “x.x.x.x” is the assigned IP address.

2.2 NetBIOS Hostname

The EBM network interface will use NetBIOS to advertise its hostname to the local network. The default hostname is “SYNQOREBM”. If an IP address is assigned via a DHCP server and NetBIOS is permitted on the local network, directing a browser on the network to <http://synqorebm/> or <https://synqorebm/> will load the EBM web interface.

Once an initial connection is made to the web interface, the user should assign a unique hostname on the Network tab (see below), so that the name does not interfere with other SynQor EBM devices on the network.

2.3 Local Connection

The EBM network interface can connect to a host computer directly via an RJ-45 Ethernet cable. Either a straight-through or crossover type cable can be used. In this mode, the web interface is available via the address <http://169.254.1.1/>. The EBM implements its own DHCP server which will provide an IP address on the 169.254 subnet to the host computer. Once a connection is established in this way, the user can configure the default IP address and hostname as desired, as well as read the MAC address for the purposes of assigning a static IP address.

3 Web Interface

The web interface provides a portal to monitor, control, and configure the EBM. Some of the configuration options, such as those to setup the email and SNMP interfaces are only available through the web interface. The interface will work well through any common web browser, though different browsers may render with slight differences. The pages rely on Javascript to do continuous updates and submit forms, so scripting must be enabled in the browser. Older browser versions may not support some of the methods used.

Unsecured HTTP requests are processed at port 80. Secure SSL HTTPS requests are processed at port 443. SSL connections utilize encryption to protect data passed between the UPS and the browser from snooping. Legacy UPS/MPC devices support SSL 3.0 encryption. Certain devices support TLS 1.2 and TLS 1.3 encryption; refer to Section 3.7. Upon initiation of an SSL connection, the UPS will provide a Certificate to the browser to verify its identity. The Certificate served will be a “self-signed” certificate, and the browser will warn that the site is untrusted and request confirmation that you want to continue. Certain devices support loading of a signed certificate; refer to Section 3.8.

To avoid the warning message on future connections, use facilities in most browsers to mark the EBM Certificate as a trusted certificate. Note that the certificate includes the NetBIOS name as the “common-name” as part of its verification criteria, so the certificate is rebuilt after a change to the NetBIOS name (Section 3.3.1). The browser verifies, and may enforce, that the name in the address bar matches the common-name in the certificate. If a static IP address (e.g. <https://20.1.1.24/>) is used to connect to the EBM, NetBIOS can be disabled and the hostname set to the fixed IP address (e.g. 20.1.1.24) to build a certificate with a common-name that matches the loaded address, avoiding a browser security error.

SSL/TLS certificates specify a date range for validity. The web browser may or may not allow access if the access date is outside the validity window. The certificates generated by the EBM have validity range extending twenty years from the date of certificate generation. In order to force certificate regeneration (and hence create a new validity window), change the NetBIOS name and then change it back to the desired value. Times and dates used for the certificate are based on the SNTP time server, see Section 3.3.4.

When SSL or TLS is used, the interface can be locked with a username and password, see Section 3.3.5.

The web interface can be disabled completely, see Section 3.3.6.

3.1 MONITOR Page

The Monitor page is the default page shown when you point the browser at the EBM with no page specified. This page gives an overview of monitored parameters and configuration.

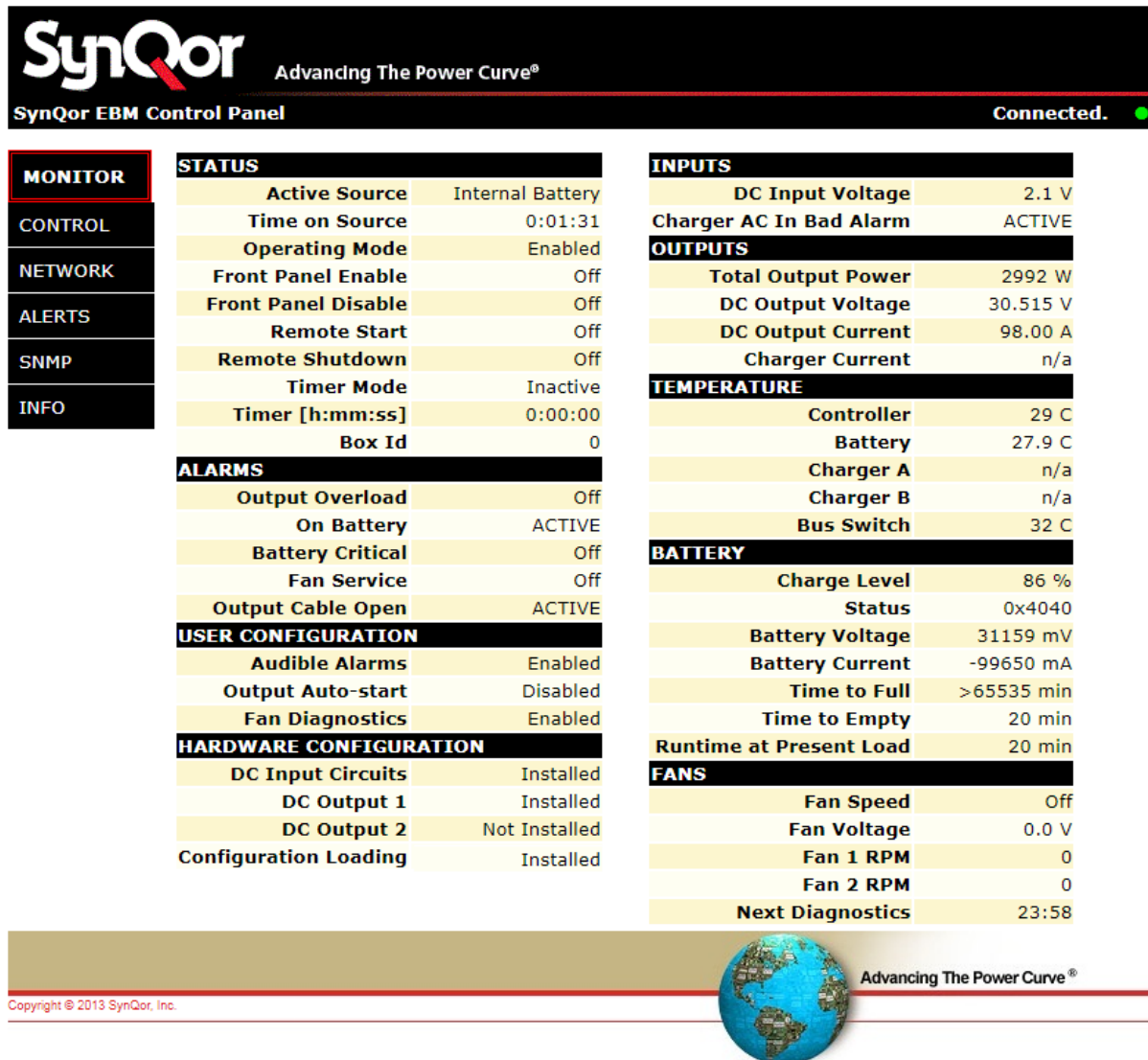


Figure A Monitor Page of Web Interface

The Monitor page (as well as all other pages) has a flashing green dot in the top right of the title bar which indicates that there is a connection to the EBM and the displayed data is continuously updated. If the connection is broken, the dot will turn red to indicate stale data.



Figure B Status "LED" on Webpage Header

3.2 CONTROL Page


The Control page is the main page to use to interact with and configure the EBM. There is a small header section at the top which actively updates to give the present configuration and operational state. Actions available to interact with the EBM:

- Enable and disable the EBM Output
- Silence alarms (if active)
- Run fan diagnostics
- Manually set fan speed
- Set unit to reboot the output after a designated off time
- Set the unit to shut down the output after a designated delay
- Set the unit to enable the output after a designated delay
- Abort a pending startup or shutdown delay

Configuration options available on the Control page are:

- Set / clear alarms to permanent mute
- Set / clear auto-start option for automatic resumption of previous on / off state when power is applied
- Disable automatic operation of fan diagnostics

All actions taken on the Control page take effect immediately. The Configuration options are stored to non-volatile memory. Note that the commands will be acknowledged on the serial interface just as if they were entered through the serial interface.


Advancing The Power Curve®

SynQor EBM Control Panel
Connected. ●

MONITOR

CONTROL

NETWORK

ALERTS

SNMP

INFO

STATUS		USER CONFIGURATION	
Operating Mode	Enabled	Audible Alarms	Enabled
Timer Mode	Inactive	Output Auto-start	Enabled
Timer [h:mm:ss]	0:00:00	Fan Diagnostics	Enabled
HARDWARE CONFIGURATION		Fan Speed	Off
DC Output 1	Installed		
DC Output 2	Not Installed		

Actions


- Enable EBM output(s).
- Disable EBM output(s).
- Silence currently active audible alarms.
- Run fan diagnostics now. Fan diagnostics will step through fan settings and measure fan speeds. Routine will not reduce fans below speed established by the thermal environment.
- Manually set fan speed. Will not allow reduction of fans setting below speed established by the thermal environment.
- Shutdown EBM output(s) immediately, restart after designated number of seconds.
- Shutdown EBM output(s) after designated number of seconds.
- Enable EBM output(s) after designated number of seconds.

Configuration

Configuration settings are stored in non-volatile memory and will persist after power-down.

Audible Output	<input checked="" type="radio"/> On <input type="radio"/> Mute	Piezo alarm beep patterns indicate battery operation, output overload, critical battery charge level, and AC output failure. Audible output can be permanently muted with this configuration setting.
Autostart	<input checked="" type="radio"/> On <input type="radio"/> Off	With Autostart enabled, when EBM receives input power, it will resume the state of the output before power was lost when able. For example, if the output was on, the battery depleted, and the device shuts down, if AC power returns the output will re-enable after the battery recharges to a nominal level. With Autostart disabled, when the EBM receives power it will remain off until it receives an enable command.
Fan Diagnostics	<input checked="" type="radio"/> On <input type="radio"/> Off	Fan diagnostics will cycle the fans through their speed ranges every 24 hours to monitor fan health.
Multi-Unit Control Synchronization	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	Through Config Port interconnect, Enable / Disable Events can be synchronized between devices. An enable event on one unit will cause all connected units to enable simultaneously.

Copyright © 2013 SynQor, Inc.



Advancing The Power Curve®

Figure C Control Page in Web Interface

006-0007045

05/07/21

REV C

6 OF 29

EBM ETHERNET GUIDE

WWW.SYNQOR.COM

3.3 NETWORK Page

The Network page offers options to configure the EBM on the network. Changes on this page do not take effect until the user presses the *Apply* button at the bottom of the page. Configuration changes are stored in non-volatile memory. A status window at the top of the page shows the present configuration on the network.

PRESENT CONFIGURATION		ADDRESS RESOLUTION	
MAC Address	00:04:A3:B5:73:AC	DHCP Enabled	Enabled
IP Address	10.2.6.8	DHCP Server	Detected
Gateway	10.2.0.1	DHCP Binding	Bound
Subnet Mask	255.255.0.0	DHCP Lease Time	185:40:19
Primary DNS	10.2.1.1	AutoIP Active	Not Active
Secondary DNS	10.2.1.32	AutoIP Status	Not Active
NETWORK TIME			
Current Time	Aug 16, 2013 15:34:20 UTC		
Last SNTP Update	Aug 16, 2013 15:24:39 UTC		

Figure D Network Configuration Status Pane

3.3.1 NETBIOS

NetBIOS is a protocol that allows a device to register a default hostname on the network. With this hostname, a user can address a device without knowing the assigned IP address. By default, the EBM is configured to register the hostname "SYNQOREBM". The user has the option to disable NetBIOS, in which case they would need the IP address assigned to the device to use the web interface. The IP address could instead be assigned to a static address by the router based on the MAC address.

When the NetBIOS name changes, the EBM rebuilds the SSL Certificate that will be served to browsers connecting to the web interface via an SSL (https://) connection.

3.3.2 QUALIFIED DOMAIN NAME

Devices which support externally signed certificates (see Section 3.8) allow entry of a qualified domain name. The value entered in this field is only used for population of the certificate and certificate signing request (CSR). This is useful when the device will be mapped to an absolute domain name (for example myhost.example.com) via an external Domain Name System. Including the mapped domain name in the certificate may be required for some browsers to recognize the certificate as authentic.

3.3.3 ADDRESS RESOLUTION

DHCP is a protocol which allows the router to assign an IP address to a device on the network. By default, DHCP is enabled and the EBM will be assigned an IP address by a service on the network. A DHCP-assigned address has an expiration time (lease). The EBM will attempt to renew its DHCP lease before it expires. When DHCP is disabled, the EBM reverts to the default IP address specified. In this situation, the EBM will transmit DHCP discovery requests once per minute to determine if a DHCP host is present on the network.

AutoIP is an alternate IP address assignment protocol. With AutoIP, the device starts using a particular address and observes if there are any conflicts. By default, AutoIP is disabled, and DHCP is the recommended address resolution protocol.

The Local DHCP Server option allows the EBM to hand out addresses over a local network, such as when the EBM is directly connected to a computer's Ethernet port. When this option is disabled, the EBM does not respond to DHCP requests and the DHCP discovery requests are halted. The EBM will not respond to DHCP requests if it detects that a DHCP server is present on the network.

3.3.4 DEFAULT ADDRESSES

If DHCP is not enabled or available, the EBM reverts to the default addresses entered here. The default addresses are also used when the network interface first initializes and attempts to locate a DHCP server. DHCP can be disabled if the device is assigned a static address by the network administrator.

The IP Address assigned in the factory is 169.254.1.1. This address can be used when establishing a peer-to-peer connection between a client computer and the SynQor device, as described in Section 2.3. To assign a static IP address to the device, enter the desired address in the "IP Address" field.

3.3.5 TIME SERVER

If enabled, the EBM will poll a network time server to determine the actual clock-time. A dropdown allows the user to select from a standard set of time servers or enter a custom time server. The global time is resynchronized every ten minutes.

The clock-time is used in reporting alerts via the email alert feature and the validity dates of generated SSL/TLS Certificates.

3.3.6 AUTHENTICATION

The authentication feature locks the entire web interface, requiring the user to enter a username and password to load the interface. You should only need to enter the username and password once for a single browser session – the browser will retain the username and password and resend it with each additional request in the session.

In order to protect the password, an SSL or TLS connection is required to enable authentication (and at all times while using an authenticated connection). To access the web interface through an encrypted session type in the browser use the "https" prefix, e.g., **https://{ip-address of the EBM or NETBIOS name}/**.

3.3.7 PROTOCOLS

Certain devices support TLS v1.2 and TLS v1.3, see Section 3.7. On these devices, TLS v1.3 support is disabled by default. Enable the checkbox in the Protocols section to enable TLS v1.3. Due to increased cryptographic handshake requirements of TLS v1.3, performance of the device interface is degraded when this protocol is in use. There will be longer latency in each request between the client and server due to the additional processing required for the encryption operations.

3.3.8 WEB INTERFACE

The Enable Web Interface checkbox completely disables the device from responding to HTTP requests. If this box is unchecked and the Apply button is activated, the interface is disabled and the setting is stored in a non-volatile setting. The only way to restore the web interface in this case is to transmit the RS232 command "NET RESTORE".

When the web interface is disabled, the device will still respond to SNMP commands. Because the SNMP configuration is controlled through the web interface, if the desired configuration is with SNMP active and HTTP disabled, the user must enable and configure SNMP before disabling the web interface.

3.3.9 RESTORE DEFAULTS

Network configuration settings (including the authentication password) can be restored to the factory default values by transmitting the RS232 command “NET RESTORE”.

3.4 ALERTS Page

The Alerts page gives the user the ability to setup email transmissions for selected alarm conditions. The email engine uses SMTP, so the user must provide the address of an SMTP server to transmit the messages. The SMTP server will then decode the email addresses and route the messages accordingly. If no SMTP server is entered, the EBM will attempt to send the message via the domain of the email user selected.

Select any items from the list of alarm conditions desired to initiate an email transmission.

Alert configuration is stored in non-volatile memory after the “Save Settings” button is pressed. The “Send Test Email” button can be used to send a test message to the designated address before modifying the configuration with the “Save Settings” button.

Email / alert configuration settings can be restored to the factory default values by transmitting the RS232 command “EMAIL RESTORE”.

☒ **Enable Email Alerts**

SMTP Server

Host Name:

Port Number:

User Name:

Password:

☐ **Update Username / Password**

MESSAGE INFO

Message To:

EBM Identifier:

Figure E Configure Email Alerts

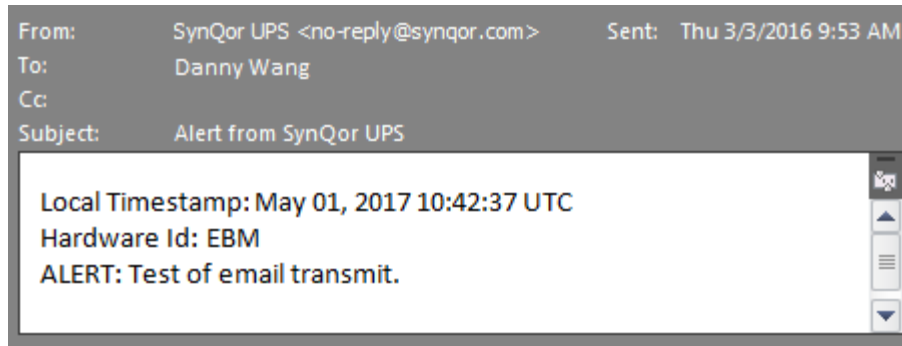


Figure F Test Email Message Example

3.5 SNMP Page

The SNMP page configures the SNMP Interface (see Section 4). The EBM currently supports SNMPv1, SNMPv2, and SNMPv3 messages. SNMPv3 includes options for encryption and authentication of messages. If authentication is required for the SNMP interface, it is highly recommended that the web interface also utilize authentication, see Section 3.3.5. Despite security on the SNMP interface, a malicious actor could simply connect to the EBM via the web interface if the web interface is left unsecured.

By default, the SNMP interface is not enabled, and must be explicitly enabled via the web interface on the SNMP Configuration Pane (see Figure G).

All changes on this page are stored in non-volatile memory when the appropriate Apply button is pressed.

SNMP Configuration

SNMP configuration settings are stored in non-volatile memory and will persist after power-down. When security is required, the web interface must also be protected (see **network tab**). Modify values as desired, then click "Apply" to modify settings.

☒ **Enable SNMP Interface**

The SNMP interface exposes the RFC-1628 UPS MIB to external SNMP monitoring devices

Write Access Communities

SNMPv1 and v2 grant access based on a shared community name. The community name is not encrypted in SNMP packets. To disallow SNMPv1 and v2 access, do not enter any community names.

Community 1:

Community 2:

Community 3:

Read Access Communities

To disallow SNMPv1 and v2 access, do not enter any community names. The EBM also grants read access to write communities.

Community 1:

Community 2:

Community 3:

Access Control for SNMPv3 Users

	Require Authentication	Require Encryption
System MIB Objects	<input type="checkbox"/> Read <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write
UPS MIB Objects	<input type="checkbox"/> Read <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write

Figure G SNMP Configuration Pane

3.5.1 Communities

SNMPv1 and SNMPv2 messages are authenticated by a community name. The interface allows the user to set up three different read and write communities. Write communities are also given read access. The community assigned in the EBM web interface must also be entered on the SNMP monitoring host which will communicate with the EBM.

Community names are not encrypted within SNMP transmissions, so SNMPv1 and SNMPv2 communities offer only very loose security. Community names can be read directly via examination of packets on the network. To disable SNMPv1 and SNMPv2 access, do not enter any community names in the configuration pane.

3.5.2 SNMPv3 Access Control

SNMPv3 messages reference a user which must be defined on the target device (the EBM). The messages may contain authentication or authentication with encryption. An authenticated message contains a password which establishes the identity of the user, but the contents of the message are readable to other devices on the network. A message with authentication and encryption establishes the identity of the user and the message itself is encrypted to protect the content of the message.

Using the SNMP Configuration Pane (see Figure G), you can configure whether the EBM will require either authentication or encryption to allow access to elements of the MIB via SNMP. Separate access control parameters can be set for the System MIB objects and the UPS MIB objects. The System MIB objects reference network parameters, such as access errors, device up-time, and network identification variables. The UPS MIB objects reference parameters related to the operation of the EBM.

3.5.3 SNMPv3 Users

The EBM allows the definition of up to three different users for the purposes of SNMPv3 access. For each user, a separate password can be entered for authentication (access control) and encryption (message privacy). For authentication purposes, a choice is offered between MD5 and SHA1 hashing of the authentication password. Note that even if authentication and encryption passwords are defined for a user, SNMPv3 will still allow a monitoring device to send an unauthenticated or unencrypted message referencing that user name. The access control for the EBM reporting and control must be set separately, see Section 3.5.2.

SNMPv3 Users

SNMPv3 provides authentication and security based on users defined in the agent. The EBM allows up to three user definitions. Authentication and privacy use independent passwords. When security is required, the web interface must also be protected (see [network tab](#)). Enter settings for a single user, then click Save to save the settings for that user.

Select User: User 0

Select user to configure.

Username:

Authentication

Method: SHA1

Password:

Authentication validates the source of SNMP messages. Choose the authentication method or "none" to grant open access under this user. You must reenter the password if you make changes to a user.

Encryption

Method: AES-128

Password:

Encryption secures the content of SNMP messages between the agent and SNMP monitor. Choose the encryption method or "none" to not perform encryption on SNMPv3 messages for this user. You must reenter the password if you make changes to a user.

Save

Reset Form

Figure H SNMPv3 User Setup Pane

3.5.4 SNMP Trap Receivers

An SNMP “Trap” is a message sent from the device (agent) to a monitoring computer. Traps that the EBM will generate are listed in Section 4.2. In general, the messages alert the monitoring computer of alarm conditions so that polling is not required to determine when action needs to be taken. The EBM allows the user to configure up to two receivers for EBM traps.

The hostname of the trap receiver can either be the fully qualified domain name of the computer to receive the traps, or the fixed IP address of the computer. Traps can be sent either via the SNMPv2 message format or the SNMPv3 message format.

SNMPv2 traps have their own community that must be recognized by the receiver. Enter a community name recognized by the receiver to transmit with the trap.

SNMPv3 traps are sent with the credentials of a user defined in the EBM. Select one of the three users defined in the EBM to associate with the trap message. SNMPv3 traps can also be sent with either authentication or authentication and encryption. Select the desired check boxes to protect the trap message contents.

SNMP Trap Receivers

The SNMP agent transmits "Traps" to defined receivers under specific conditions: EBM On-Battery, Alert Added, Alert Removed, Test Complete. Enter up to two SNMP receivers for these trap messages.

Receiver: Trap Receiver 0 ▾
Enable traps: ☒
Hostname / IP:
Message format: SNMP v2 ▾
SNMPv2 Community:
SNMPv3 Credentials: User 0 ▾

☐ Authenticate
☐ Encrypt
☐ Attempt USM Discovery

SNMPv3 contextEngineId:
SNMPv3 Default contextId: Enter hex string:
SNMPv3 contextName:

Select trap receiver to configure. Either enter a hostname to resolve via DNS for each transmission, or a fixed IP address (x.x.x.x format). Receiver can be set to receive traps in SNMPv2 or SNMPv3 format. For SNMPv2, the community included in trap message must be recognized by the receiver. For SNMPv3, select a local user to associate with the message. To transmit with authentication or encryption, the local user must have the appropriate passwords configured. SNMPv3 contextEngineId will be blank on transmitted traps unless USM Discovery is selected and the manager target device responds to the Discovery query, or a default contextId is entered. SNMPv3 contextName will be blank on transmitted traps unless a string is entered in the provided field.

Figure I SNMP Trap Receiver Configuration Pane

3.5.5 RESTORE DEFAULTS

SNMP configuration settings can be restored to the factory default values by transmitting the RS232 command "SNMP RESTORE".

3.6 DEBUG Page

The Debug page does not have a link from the other pages. Select the Debug page by loading <http://synqorebm/debug.htm> (substitute "synqorebm" for the selected hostname or IP address). The debug page provides a scrollable mirror of the RS232 serial interface. The user can also transmit 'virtual' serial commands by entering the commands and clicking the *Send* button.

Note that the debug.htm form should only be accessed from a single browser at a time. If two browsers simultaneously view the page, the output pane will not display accurately.

Serial Command:

```

OUTPUT ENA
Output Enabled.

SynQor>OUTPUT DIS
Output Disabled.

SynQor>?
?
ALARM DISABLE
ALARM ENABLE

```

Figure J debug.htm Serial Interface Mirror

3.7 TLS Support

SynQor network-enabled devices built after a cut-off date include support for TLS v1.2 and TLS v1.3 protocols during communication with the HTTPS interface. This replaces the older SSL v3.0 protocol used in older SynQor devices. By default, TLS v1.3 is disabled for performance reasons, but can be

enabled on the NETWORK web page (see Section 3.3.7). Devices which support TLS encryption also provide features for the user to load a signed certificate that can be used for authentication purposes, rather than using the device-generated self-signed certificate (see Section 3.8).

3.8 Certificates

As part of an SSL or TLS transaction for an HTTPS request, the server presents the client with a certificate, which the client can use to verify the identity of the server. The client verifies the cryptographic signature in the certificate against the recognized Certificate Authorities (CAs) installed on the client by the network administrator. If the client does not recognize the credentials of the server, it may prohibit the connection or allow the user to proceed with a warning that the host is “unsafe”. The user may be allowed to install the certificate on the client to allow this session and future sessions.

For communication with a SynQor web-enabled device, the SynQor device is the server, and the user web browser or web-enabled application is the client. Legacy SynQor devices with SSL 3.0 support will only support a self-signed certificate, populated with the NetBIOS name as the server name. Newer SynQor devices support TLS encryption, and will either serve a self-signed certificate, or a certificate the user uploads signed by a CA recognized on the client network. The remainder of this section refers to certificate support in SynQor devices with TLS support.

Devices with TLS support include multiple entries in the Name / AltName fields of the certificate. These devices will populate the NetBIOS name, the Fully Qualified Domain Name (FQDN), and the default IP address as possible server names in the certificate. This aids clients authenticating the certificate in the user browser, supporting the various ways the client may address the SynQor device. Note that some clients will not authenticate a server with a NetBIOS-style shortened name. If this is applicable, an FQDN can be specified, with the FQDN name mapped to the SynQor device in the network infrastructure DNS system.

Whenever the user or administrator modifies one of the fields populated in the certificate via the NETWORK web configuration page, the device will generate a new certificate with the entered data. The device generates a self-signed certificate in this case, and also a Certificate Signing Request (CSR). The CSR can be used by the network administrator to create and upload an externally signed certificate. After modifying any one of the fields on the NETWORK page used in the certificate, if the user had previously installed a signed certificate in the device, that certificate will no longer be used, and the device will revert to the new self-signed certificate. The new CSR can be signed and uploaded to the device. In order to generate a self-signed certificate or a CSR, the SynQor device must have a valid time available per SNTP (see Section 3.3.5).

The signed certificate uploaded to the SynQor device **must** be derived from the latest CSR generated by that specific device. Each CSR contains a unique public key, which will only be matched by the private key stored within the device. The device generates a new key pair every time the CSR is recomputed.

Note that if the server certificate from the SynQor device is manually installed on the client, any change to the configuration that involves a regeneration of the certificate will require installation of the new certificate on the client.

3.8.1 Installation of a Signed Certificate

Certain SynQor network enabled devices allow the installation of an externally signed server certificate. The below steps outline the process to install an externally signed certificate. SynQor cannot provide assistance on the step of actually signing the certificate with a Certificate Authority which will be recognized on the target network. This step must be done with tools compatible with the management of the target network, provided by the network administrator.

1. Configure device parameters (NetBIOS name, FQDN, static IP address, SNTP) as appropriate; See Section 3.3.
2. Download device CSR; See Section 3.8.2.
3. Sign CSR using third-party tools with a Certificate Authority (CA) which will be recognized on the target network.
4. Upload the signed certificate to the SynQor device; See Section 3.8.3.

3.8.2 Download Device Certificate Signing Request (CSR)

The device provides its computed CSR in PEM format (Base64 ASCII). There are two ways to retrieve the CSR. The first way is to download the file `CertRequest.pem` from the device. For example, you could point a connected client browser to <http://synqorups/CertRequest.pem> (where “synqorups” represents the assigned NetBIOS name or IP address), and the browser will download the ASCII readable file to the host computer. The second way to retrieve the CSR is via the `certificate.htm` web page. This page contains a text box with the CSR content, which can then be copied and pasted as required on the host computer system.

CSR in PEM Format:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBZzCCAQ0CAQIwFjELMAkGA1UEBhMCVVMxFTABAgNVBAgMDU1hc3NhY2h1c2V0
dHMxEzARBgNVBAcMCKJveGJvcmlZ2gxZDASBgNVBAoMC1N5b1FvcjBjbmuMRGw
FgYDVQQLDA9VUFMgQ29uZm1nIFBhZ2UxEjAQBgNVBAMMCVNZTlFPULVQUzBZMBMG
ByqGSM49AgEGCCqGSM49AwEHA0IABMPZyA5du4j/d68Fp4c81LzPDLT1cZnV/AZR
sDJmXnq1Af2cC0/iyN2f+j62ZPaJ4cTuUvOuG2sU1YAtFL9B83SgLTArBgkqhkiG
9w0BCQ4xHjAcMBoGA1UdEQQTMGGCCVNZTlFPULVQU4cEqf4BATAKBggqhkiG9w0D
AgNIADBFAiEAswZKHwJa2XnoySbGbm7YSjdEHsDnGVRv2BvyJVik+QkCIBUtvkwz
1ARV2N7Ms6ICZT7jVORLycseHR/RuU4L6J9U
-----END CERTIFICATE REQUEST-----
```

Figure K CSR Textbox on `certificate.htm` page

3.8.3 Upload Signed Certificate

After retrieving the device CSR, the user or administrator will create a signed certificate using the appropriate tools for their network. The certificate should be signed by a Certificate Authority which will be recognized on their network. The signed certificate can then be uploaded to the SynQor network-enabled device using a PEM format (Base64 ASCII). The signed certificate must be less than 4096 bytes long.

The signed certificate is uploaded via the `certificate.htm` web page, using one of two methods. The content of the certificate can be copy / pasted into the appropriate text box on the page, then clicking the “Upload Certificate” button.

Enter Signed Certificate in PEM Format:

Upload Certificate

Figure L Entry box for signed certificate on `certificate.htm` page

Alternately, activate the “Choose File” button, and select a file containing the signed certificate on the host computer.

4 SNMP Interface

The SNMP interface exposes the industry standard [RFC-1628](#) UPS Management Information Base (MIB). This guide is not meant to provide a description of the SNMP protocol or recommendations for software to be installed on any monitoring computer.

By default, the SNMP Agent in the EBM network interface is disabled, and it must be enabled via the web interface SNMP page (see Section 3.5). Enter a community for read and write operations, and enter these same community names on the monitoring device along with the device IP address.

The EBM SNMP Agent will recognize SNMPv1 and SNMPv2 formatted messages. Transmitted traps use the SNMPv2 format, per the RFC-1628 specification. (SNMPv3 messages use the same format as SNMPv2 messages, with the addition of authentication and encryption.)

4.1 SNMP Exposed Objects

In the following list of objects exposed by the SynQor EBM, the Object ID references the upsObjects prefix, which has the address 1.3.6.1.2.1.33.1.

4.1.1 upsIdent Group

Object Name: upsIdentManufacturer

OID: upsObjects.1.1

Type: String

Access: Read-Only

Returns "SynQor Inc."

Object Name: upsIdentModel

OID: upsObjects.1.2

Type: String

Access: Read-Only

Returns the SynQor assigned full model number for this device.

Object Name: upsIdentUPSSoftwareVersion

OID: upsObjects.1.3

Type: String

Access: Read-Only

Object returns a summary of the code revisions of the modules internal to the EBM: Mother Board and Charger. The Charger's reported code revision is only valid if the charger is enabled.

Object Name: upsIdentAgentSoftwareVersion

OID: upsObjects.1.4

Type: String

Access: Read-Only

Object returns the SynQor assigned code revision of the communications card implementing the network interface.

Object Name: upsIdentName

OID: upsObjects.1.5

Type: String

Access: Read-Write

This field is a user assignable name available to identify this device. Default value is blank.

Object Name: upsIdentAttachedDevices

OID: upsObjects.1.6

Type: String

Access: Read-Write

This field is a user assignable string available to identify this device. Default value is blank.

4.1.2 upsBattery Group

Object Name: upsBatteryStatus

OID: upsObjects.2.1

Type: Integer, {unknown=1, batteryNormal=2, batteryLow=3, batteryDepleted=4}

Access: Read-Only

This object returns the status of the installed battery. The “batteryLow” status is determined by comparing the projected runtime at the present load to the value stored in the “upsConfigLowBattTime” object.

Object Name: upsSecondsOnBattery

OID: upsObjects.2.2

Type: Integer

Access: Read-Only

Object value is the number of seconds the EBM has been running on battery; value is zero if the EBM is not currently running from battery power.

Object Name: upsEstimatedMinutesRemaining

OID: upsObjects.2.3

Type: Integer

Access: Read-Only

Object value is the current estimate of the time the battery could support the present load based on the current battery charge level.

Object Name: upsEstimatedChargeRemaining

OID: upsObjects.2.4

Type: Integer

Access: Read-Only

Object value is the estimate of the battery charge remaining, expressed as a percentage of the estimate of the fully charged battery capacity.

Object Name: upsBatteryVoltage

OID: upsObjects.2.5

Type: Non-negative Integer

Access: Read-Only

Object returns the battery voltage expressed in tenths of Volts.

Object Name: upsBatteryCurrent

OID: upsObjects.2.6

Type: Integer

Access: Read-Only

Value returned is the present battery current, expressed in tenths of amps. A negative current represents a discharge current. A positive current represents a current charging the battery.

Object Name: upsBatteryTemperature

OID: upsObjects.2.7

Type: Integer

Access: Read-Only

Object value is a reading of the battery internal temperature. Units are degrees Celsius.

4.1.3 upsInput Group

Object Name: upsInputLineBads

OID: upsObjects.3.1

Type: Counter32

Access: Read-Only

Object returns the count of times an input voltage transitions from good to bad.

Object Name: upsInputNumLines

OID: upsObjects.3.2

Type: Non-negative Integer

Access: Read-Only

Object reports the number of inputs installed on this EBM.

4.1.3.1 *upsInputTable*

The *upsInputTable* object (UPSObjects.3.3) contains a single entry for each input installed in the device. Each entry contains up to two fields, as listed here.

Object Name: upsInputFrequency

OID: UPSObjects.3.3.1.2

Type: Non-negative Integer

Access: Read-Only

Object returns the measured frequency from this input source in tenths of Hertz. A DC input will return a value of 0.

Object Name: upsInputVoltage

OID: upsObjects.3.3.1.3

Type: Non-negative Integer

Access: Read-Only

Object returns the measured input voltage of this source. DC input sources return the voltage in units of tenths of Volts.

4.1.4 *upsOutput Group*

Object Name: upsOutputSource

OID: upsObjects.4.1

Type: Integer, {other=1, none=2, normal=3, bypass=4, battery=5, booster=6, reducer=7}

Access: Read-Only

Object returns the present source of output power. If the output is not presently on, the value returned will be 2 (none). If the output is enabled and running from DC input power, the value returned will be 3 (normal). When running from battery power, the value returned will be 5 (battery). The other enumeration values are unused by the SynQor Agent.

Object Name: upsOutputFrequency

OID: upsObjects.4.2

Type: Non-negative Integer

Access: Read-Only

Object returns the present frequency setpoint of the Output source in tenths of Hertz. Because the EBM output is DC, the return value will always be zero.

Object Name: upsOutputNumLines

OID: upsObjects.4.3

Type: Non-negative Integer

Access: Read-Only

Object returns the number of outputs installed in the EBM device (1).

4.1.4.1 *upsOutputTable*

The *UPSOutputTable* object (UPSObjects.4.4) contains an entry for each output installed in the EBM device. Each output contains up to four fields, as listed here.

Object Name: upsOutputVoltage

OID: UPSObjects.4.4.1.2

Type: Non-negative Integer

Access: Read-Only

Object returns the output voltage of the corresponding EBM output in units of Volts.

Object Name: upsOutputCurrent

OID: upsObjects.4.4.1.3

Type: Non-negative Integer

Access: Read-Only

Object returns the output current of the corresponding EBM output in units of tenths of Amps.

Object Name: upsOutputPower

OID: upsObjects.4.4.1.4

Type: Non-negative Integer

Access: Read-Only

Object returns the output voltage of the corresponding EBM output in units of Watts.

Object Name: upsOutputPercentLoad

OID: upsObjects.4.4.1.5

Type: Non-negative Integer

Access: Read-Only

Object returns the output voltage of the corresponding EBM output as a percentage of the rated output power of the device.

4.1.5 *upsBypass Group*

The *UPSByypass* group is not implemented by the SynQor EBM SNMP Agent because the EBM models do not contain internal bypass devices.

4.1.6 *upsAlarm Group*

Object Name: upsAlarmsPresent

OID: upsObjects.6.1

Type: Non-negative Integer

Access: Read-Only

Object returns the total number of active alarms in the upsAlarmsTable.

4.1.6.1 *upsAlarmTable*

The *upsAlarmTable* (UPSObjects.6.2) contains an entry for each active alarm condition. Any given alarm condition will only appear in the table once.

Object Name: upsAlarmDescr

OID: upsObjects.6.2.1.2

Type: OID (object identifier)

Access: Read-Only

Object returns the object identifier for the alarm condition represented by a given entry in the Alarm table. The list of possible alarm conditions is defined in the [RFC-1628](#) group *upsWellKnownAlarms*.

Object Name: upsAlarmTime

OID: upsObjects.6.2.1.3

Type: Timestamp

Access: Read-Only

Object returns the timestamp that the given alarm condition was first detected. The timestamp is the value of the *sysUpTime* object (1.3.6.1.2.1.1.3) at the time of detection.

4.1.7 *upsTest Group*

The *UPSTest* group provides an interface to launch self-tests of the EBM hardware. To initiate a test, the monitoring computer must execute a write instruction which includes both the *upsTestId* object and the *upsTestSpinLock* object. The OID of the desired test sequence is written to *upsTestId*. The value written to *upsTestSpinLock* must be the present value read from *upsTestSpinLock*. The spin-lock provides a semaphore, allowing only one device to launch a self-test sequence at a time. Once a test sequence completes, the *upsTestSpinLock* variable increments by one.

Object Name: upsTestId

OID: upsObjects.7.1

Type: OID (object identifier)

Access: Read-write

This object identifies the test in progress or last completed. As described above, to initiate a test a single PDU write must be issued to *upsTestId* and *upsTestSpinLock*. To abort a test in progress, send the OID *upsTestAbortTestInProgress* (1.3.6.1.2.1.33.1.7.7.2). Valid OIDs for self-test sequences are defined by the *upsWellKnownTests* group. The three test options are *upsTestGeneralSystemsTest*, *upsTestQuickBatteryTest*, and *upsTestDeepBatteryCalibration*. The EBM output must be enabled for these tests to return a passing result. The *upsTestDeepBatteryCalibration* sequence discharges the battery to 20% charge to determine runtime; the test time will vary strongly based on the load configuration.

Object Name: upsTestSpinLock

OID: upsObjects.7.2

Type: Test-and-Increment

Access: Read-write

To initiate a test, the monitoring computer must read this object value, and return the present value along with a valid OID for *upsTestId*. The value of this object increments after a self-test completes.

Object Name: upsTestResultsSummary

OID: upsObjects.7.3

Type: Integer, {done/pass=1, done/warning=2, done/error=3, aborted=4, in progress=5, no test initiated=6}

Access: Read-Only

This object returns a summary of the result of a previously initiated self-test routine.

Object Name: upsTestResultsDetail

OID: upsObjects.7.4

Type: String

Access: Read-Only

Value of this object is a string describing the result of the last self-test routine. If the test ended with an error or warning, the string will describe the error or warning.

Object Name: upsTestStartTime

OID: upsObjects.7.5

Type: Timestamp

Access: Read-Only

Object returns the value of the *sysUpTime* object (1.3.6.1.2.1.1.3) at the time the previous self-test was initiated.

Object Name: upsTestElapsedTime

OID: upsObjects.7.6

Type: Time-interval

Access: Read-Only

Object returns the elapsed running time of the previous self-test.

4.1.8 upsControl Group

Object Name: upsShutdownType

OID: upsObjects.8.1

Type: Integer, {output = 1, system = 2}

Access: Read-Only

For the SynQor EBM, all commanded shutdowns disable the outputs, and do not power-down the EBM hardware. This object will always return a value of 1, indicating output-shutdown.

Object Name: upsShutdownAfterDelay

OID: upsObjects.8.2

Type: Integer

Access: Read-write

A write to this object will initiate a shutdown of the EBM outputs after the designated number of seconds. A write of the value 0 will cause the EBM outputs to shut down immediately. A write of -1 will abort a pending shutdown.

Object Name: upsStartupAfterDelay

OID: upsObjects.8.3

Type: Integer

Access: Read-write

A write to this object will initiate a startup of the EBM outputs after the designated number of seconds. A subsequent write of -1 will abort the timer. A write of the value 0 will cause the EBM outputs to start immediately.

Object Name: upsRebootWithDuration

OID: upsObjects.8.4

Type: Integer

Access: Read-write

The Reboot with Duration feature will automatically disable the EBM outputs for a period indicated by the number of seconds from upsShutdownType, after which time, the EBM output will be enabled.

Object Name: upsAutoRestart

OID: upsObjects.8.5

Type: Integer, {on=1, off=2}

Access: Read-write

The auto-restart feature will automatically return the EBM outputs to the state they were in before power was lost when the device receives input power from a powered-off state. This feature is enabled by default. A write of the value 2 to this object will disable the auto-restart feature. The setting is stored in non-volatile memory.

4.1.9 upsConfig Group

Object Name: upsConfigInputVoltage

OID: upsObjects.9.1

Type: Non-negative Integer

Access: Read-Only

Object returns the nominal designed input voltage of the device.

Object Name: upsConfigInputFreq

OID: upsObjects.9.2

Type: Non-negative Integer

Access: Read-Only

Object returns the nominal designed input frequency of the device. This object will always return the value 0, as this is a DC input device.

Object Name: upsConfigOutputVoltage

OID: upsObjects.9.3

Type: Non-negative Integer

Access: Read-Only

Object returns the nominal designed output voltage of the device. The units for reading and writing are Volts.

Object Name: upsConfigOutputFreq

OID: upsObjects.9.4

Type: Non-negative Integer

Access: Read-write

Object sets or returns the output frequency of the device. This object will always return the value 0, as this is a DC output device.

Object Name: upsConfigOutputVA

OID: upsObjects.9.5

Type: Non-negative Integer

Access: Read-Only

Object returns the Volt-Amp rating of the EBM device, in units of Volts·Amps.

Object Name: upsConfigOutputPower

OID: upsObjects.9.6

Type: Non-negative Integer

Access: Read-Only

Object returns the rated power of the EBM device, in units of Watts.

Object Name: upsConfigLowBattTime

OID: upsObjects.9.7

Type: Non-negative Integer

Access: Read-write

Object sets or returns the threshold for low-battery alerts and traps in units of minutes. Alerts trigger based on the estimated run time at the present device load current and battery capacity calculations.

Object Name: upsConfigAudibleStatus

OID: upsObjects.9.8

Type: Integer, {disabled=1, enabled=2, muted=3}

Access: Read-write

Object returns or sets the state of the audible alarms.

- A read value of 1 indicates that audible alarms are disabled and will never be triggered.
- A read value of 2 indicates that audible alarms are enabled (default state)
- A read value of 3 indicates that an audible alarm is currently active, but has been muted by a user action.
- A write value of 1 will disable audible alarms (non-volatile setting)
- A write value of 2 will enable audible alarms (non-volatile setting)
- A write value of 3 will mute an audible alarm if one is currently active. If a new alarm condition triggers, the audible alarm will resume.

Object Name: upsConfigLowVoltageTransferPoint

OID: upsObjects.9.9

Type: Non-negative Integer

Access: Read-Only

Object returns the low rated line voltage of the DC Input, 21 volts.

Object Name: upsConfigHighVoltageTransferPoint

OID: upsObjects.9.10

Type: Non-negative Integer

Access: Read-Only

Object returns the maximum rated line voltage of the DC Input, 35 volts.

4.1.10 Non-UPS MIB Objects

The EBM also exposes a number of objects defined in the SNMPv2 MIB.

Object Name: sysDescr

OID: 1.3.6.1.2.1.1.1

Type: String

Access: Read-Only

Object returns the SynQor model number of this UPS device. The value returned by this object is identical to that returned by the *upsIdentModel* object.

Object Name: sysObjectID

OID: 1.3.6.1.2.1.1.2

Type: OID

Access: Read-Only

Object returns the object identifier of the UPS MIB, 1.3.6.1.2.1.33.

Object Name: sysUpTime

OID: 1.3.6.1.2.1.1.3

Type: Timeticks

Access: Read-Only

Object returns the time-ticks value since the network interface first powered up.

Object Name: sysContact

OID: 1.3.6.1.2.1.1.4

Type: String

Access: Read-Write

Object provides a user-settable string to enter contact information for management of this device. The default value is an empty string.

Object Name: sysName

OID: 1.3.6.1.2.1.1.5

Type: String

Access: Read-Write

Object provides a user-settable string to enter an identifier for this device. The value returned by this object is identical to that returned by the *upsIdentName* object.

Object Name: sysLocation

OID: 1.3.6.1.2.1.1.6

Type: String

Access: Read-Write

Object provides a user-settable string to enter an identifier for this device. The value returned by this object is identical to that returned by the *upsIdentAttachedDevices* object.

Object Name: sysServices

OID: 1.3.6.1.2.1.1.7

Type: Integer

Access: Read-Only

Object returns the value 64, indicating the EBM SNMP agent provides applications services.

Object Name: snmpEnableAuthenTraps

OID: 1.3.6.1.2.1.11.30

Type: Integer, {enabled=1, disabled=2}

Access: Read-Write

This object sets or returns whether the EBM Agent should transmit *authenticationFailure* traps when receiving SNMP messages with an incorrect community string. This setting is stored in non-volatile memory, and the default setting is enabled.

Object Name: snmpEngineID

OID: 1.3.6.1.6.3.10.2.1.1

Type: Octet String

Access: Read-Only

This is the uniquely defined snmpEngineID used for SNMPv3 identification and localization. This object is only accessible when using SNMPv3 messages.

Object Name: snmpEngineBoots

OID: 1.3.6.1.6.3.10.2.1.2

Type: Integer

Access: Read-Only

This is the number of times the SNMP engine has booted. This parameter is used for SNMPv3 message authentication. Message authentication requires messages include the proper snmpEngineBoots parameter from the target device to prevent message replay attacks. This object is only accessible when using SNMPv3 messages.

Object Name: snmpEngineTime

OID: 1.3.6.1.6.3.10.2.1.3

Type: Integer

Access: Read-Only

This is the time since the SNMP engine last booted. This parameter is used for SNMPv3 message authentication. Message authentication requires messages include a recent snmpEngineTime parameter (within the last 150 seconds) from the target device to prevent message replay attacks. This object is only accessible when using SNMPv3 messages.

Object Name: snmpEngineMaxMessageSize

OID: 1.3.6.1.6.3.10.2.1.4

Type: Integer

Access: Read-Only

This is maximum messages size (in bytes) that can be sent or received by the EBM SNMP engine. This object is only accessible when using SNMPv3 messages.

4.2 SNMP Traps

The SynQor EBM SNMP Agent will issue SNMP traps as defined in the RFC-1628 UPS MIB. The agent will also issue an authentication failure trap when addressed with an incorrect community name. In order for traps to be transmitted, the SNMP interface must be enabled as described in Section 3.5, and the hostname or IP address of the intended trap-receiver computers must also be configured as described in Section 3.5.4.

4.2.1 *upsTrapOnBattery* Trap

The *upsTrapOnBattery* trap (OID = 1.3.6.1.2.1.33.2.1) issues when the EBM is running from battery power. The trap includes the estimated runtime remaining, the number of seconds the EBM has been running on battery, and the value of the *upsConfigLowBattTime* alert warning level. This trap will re-issue at one minute intervals until power is restored on the battery capacity is depleted.

4.2.2 *upsTrapTestCompleted* Trap

The *upsTrapTestCompleted* trap (OID = 1.3.6.1.2.1.33.2.2) issues after a user-initiated self-test sequence completes within the UPS. The trap data includes all objects in the *upsTest* group, providing a summary of the test results.

4.2.3 *upsTrapAlarmEntryAdded* Trap

The *upsTrapAlarmEntryAdded* trap (OID = 1.3.6.1.2.1.33.2.3) issues every time a new alarm entry is added to the *upsAlarmTable* table. Two exceptions are that there is no notification for the *upsAlarmOnBattery* or *upsAlarmTestInProgress* alarms. The trap data includes the index of the new entry and the OID of the alarm description.

4.2.4 *upsTrapAlarmEntryRemoved* Trap

The *upsTrapAlarmEntryRemoved* trap (OID = 1.3.6.1.2.1.33.2.4) issues whenever an entry is removed from the *upsAlarmTable* table. This means that the specified alarm condition is no longer active. One exception is that there is no trap issued when the *upsAlarmTestInProgress* alarm clears. The trap data includes the index of the entry removed and the description of the alarm.

4.2.5 *authenticationFailure* Trap

The *authenticationFailure* trap (OID = 1.3.6.1.6.3.1.1.5.5) issues when the UPS SNMP agent receives an improperly authenticated message. For SNMPv1 and SNMPv2 message, this means that an unrecognized community value was included in the message. This trap will not be retransmitted more frequently than once per second. The *authenticationFailure* trap may be suppressed by setting the *snmpEnableAuthenTraps* object (OID = 1.3.6.1.2.1.11.30).

EBM **MILITARY FIELD-GRADE**

EXPANSION BATTERY MODULE

Operator's Guide *Ethernet & SNMP*



Made in USA

006-0007045

Rev C

07/15/2021

SynQor[®]