

---

# Secure Serial to Ethernet User Manual

NetBurner, Inc.



04/02/2026

# Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	Key Features	3
1.2	Supported Platforms	3
<b>2</b>	<b>Getting Started</b>	<b>4</b>
2.1	What You Need	4
2.2	Powering Up	4
2.3	Finding the Device on Your Network	4
2.4	Accessing the Web Interface	4
2.5	First-Time Configuration Checklist	4
<b>3</b>	<b>Quick Start Guides</b>	<b>5</b>
3.1	Scenario 1: TCP Server (Listen for Incoming Connections)	5
3.2	Scenario 2: TCP Client (Connect to a Remote Host)	5
3.3	Scenario 3: Secure TCP/TLS Connection	5
3.4	Scenario 4: SSH Tunnel for Serial Data	6
3.5	Scenario 5: UDP Broadcast	6
<b>4</b>	<b>Network Configuration</b>	<b>7</b>
<b>5</b>	<b>Protocol Configuration</b>	<b>9</b>
5.1	TCP Configuration	9
5.1.1	TCP Server Mode	9
5.1.2	TCP Client Mode	10
5.1.3	TCP Packetization Options	10
5.2	UDP Configuration	11
5.3	SSH Configuration	12
<b>6</b>	<b>Serial Port Configuration</b>	<b>14</b>
6.1	Serial Port Modes	14
6.2	Serial Port Settings	14
6.3	Serial Port Pin Table	15
<b>7</b>	<b>Security Configuration</b>	<b>16</b>
7.1	Password Configuration	16
7.2	TLS Certificate and Key Management	17
7.3	SSH Server Key Management	18
7.4	SSH Authorized Client Keys	19
7.5	CA Certificate Store	20
<b>8</b>	<b>GPIO Configuration</b>	<b>21</b>
8.1	GPIO Pin Settings	21
8.2	GPIO Network Server Settings	21
8.3	GPIO Network Commands	21
<b>9</b>	<b>I2C Configuration</b>	<b>23</b>
9.1	I2C Settings	23
9.2	Ethernet-to-I2C Commands	23
<b>10</b>	<b>WiFi Configuration</b>	<b>25</b>
10.1	WiFi Network Settings	25
10.2	Connecting to a WiFi Network	25

<b>11 Advanced Diagnostics</b>	<b>26</b>
11.1 Available Tools	26
<b>12 Hardware Factory Reset (SB800EX)</b>	<b>27</b>
12.1 Procedure	27
12.2 What Gets Reset	27
<b>13 AT Command Interface</b>	<b>28</b>
13.1 Enabling AT Commands	28
13.2 Entering and Exiting Command Mode	28
13.3 Command Syntax	28
13.4 Control Commands	29
13.5 Network Configuration Commands	29
13.6 Protocol Mode	29
13.7 Current Network Status (Read-Only)	30
13.8 Serial Port Commands	30
13.9 Credential Commands	31
13.10 SSH Public Key Commands	31
13.11 GPIO Commands	31
13.12 WiFi Commands	31
13.13 Saving Configuration	32
<b>14 Advanced Serial Settings &amp; Message Formatting</b>	<b>33</b>
14.1 Message Formatting Codes	34
<b>15 Advanced Network Settings</b>	<b>35</b>
15.1 TCP Host Identification	35
15.1.1 How It Works	35
<b>16 Troubleshooting</b>	<b>36</b>
16.1 Cannot Access the Web Interface	36
16.2 No Data Flowing Between Serial and Network	36
16.3 TCP Connection Issues	36
16.4 TLS/SSL Issues	37
16.5 SSH Issues	37
16.6 AT Command Issues	38
16.7 General Tips	38
<b>17 Appendix A: Default Settings Reference</b>	<b>39</b>
17.1 Network Defaults	39
17.2 Serial Defaults	39
17.3 SSH Defaults	39
17.4 UDP Defaults	40
17.5 TCP Packetization Defaults	40
17.6 GPIO Defaults	40
17.7 I2C Defaults	40
17.8 Advanced Serial Defaults	40
17.9 Advanced Network Defaults	41
<b>18 Appendix B: Platform Comparison Table</b>	<b>42</b>
<b>19 Appendix C: Pinout Reference</b>	<b>43</b>
19.1 Serial Port 0 Pinout (DB-9)	43
19.2 Serial Port 1 Pinout (DB-9)	43

# 1 Introduction

The NetBurner Secure Serial-to-Ethernet device converts serial data (RS-232, RS-422, RS-485) to Ethernet and back, enabling legacy serial equipment to communicate over modern IP networks. It supports multiple protocols including TCP, TCP/TLS, UDP, and SSH, providing both unencrypted and fully encrypted communication paths.

**Application Version:** 03.02.00

**Supported Platforms:** MODM7AE70, SBE70LC, SOMRT1061, MODRT1171, MOD5441X, NANO54415, SB800EX

## 1.1 Key Features

- **Multi-protocol support** – TCP, TCP/TLS (encrypted), UDP, and SSH
- **Flexible serial modes** – RS-232, RS-422, RS-485 half-duplex, RS-485 full-duplex
- **Two or more serial ports** per device (platform-dependent)
- **Web-based configuration** – all settings configurable through a browser
- **AT command interface** – configure via serial port without a network connection
- **TLS encryption** – secure TCP connections with uploadable certificates and keys
- **SSH tunneling** – encrypted serial data transport with public key authentication
- **CA certificate store** – verify remote server certificates for outgoing TLS connections
- **GPIO control** – remote digital I/O and analog input via TCP (platform-dependent)
- **I2C bridge** – Ethernet-to-I2C bus communication (SBE70LC only)
- **WiFi connectivity** – wireless networking (SB800EX only)
- **DHCP and static IP** – automatic or manual network configuration
- **mDNS/Bonjour** – zero-configuration network discovery
- **NTP time sync** – automatic clock synchronization
- **Advanced diagnostics** – ARP cache, data counters, system diagnostics, ping, firmware update
- **Hardware factory reset** – restore factory defaults via pushbutton (SB800EX)
- **TCP host identification** – send MAC address or custom Site ID on TCP connect

## 1.2 Supported Platforms

Platform	Serial Ports	GPIO	I2C	WiFi	Analog GPIO
<b>MOD5441X</b>	2	–	–	–	–
<b>SB800EX</b>	2	–	–	Yes	–
<b>NANO54415</b>	5	–	–	–	–
<b>MODM7AE70</b>	2 (7*)	Yes**	–	–	Yes
<b>SBE70LC</b>	2	Yes***	Yes***	–	Yes
<b>SOMRT1061</b>	7	Yes	–	–	–
<b>MODRT1171</b>	2	Yes	–	–	–

\* 7 ports available with USE\_E70\_UART\_SERIAL\_PORTS build option \*\* GPIO available when I2C and WiFi features are not compiled in \*\*\* SBE70LC supports either GPIO or I2C, not both simultaneously

## 2 Getting Started

### 2.1 What You Need

- A NetBurner module (one of the supported platforms listed above)
- Ethernet cable connected to your LAN
- Power supply appropriate for your module
- A computer on the same network with a web browser
- (Optional) Serial cable for AT command configuration

### 2.2 Powering Up

1. Connect the Ethernet cable to the module's Ethernet port.
2. Apply power to the module.
3. The module will boot and, by default, request an IP address via DHCP.

### 2.3 Finding the Device on Your Network

**Option 1: NBFind utility** Download and run the NBFind utility from [netburner.com](http://netburner.com). It discovers all NetBurner devices on your local network and displays their IP addresses, names, and MAC addresses.

**Option 2: Check your DHCP server/router** Look for a new device named with the platform prefix (e.g., "MODM7AE70SX") in your router's DHCP client list.

**Option 3: Serial debug output** Connect a serial terminal (115200 baud, 8N1) to the debug port. The device prints its IP address on boot.

### 2.4 Accessing the Web Interface

1. Open a web browser.
2. Navigate to `http://<device-ip-address>` (e.g., `http://192.168.1.100`).
3. If prompted, enter the administrator credentials (default: no username/password).
4. The **Network Configuration** page is displayed.

### 2.5 First-Time Configuration Checklist

1. **Set an administrator password** – Navigate to the **Password** page and set a strong password.
2. **Configure network settings** – Choose DHCP or static IP on the **Network** page.
3. **Select your protocol** – Choose TCP, TCP/TLS, UDP, or SSH on the **Network** page.
4. **Configure serial port(s)** – Set baud rate, data bits, parity, stop bits, and flow control on the **Serial** page to match your serial equipment.
5. **Configure protocol-specific settings** – Set up TCP server/client, UDP endpoints, or SSH as appropriate.
6. **Upload security credentials** (if using TLS or SSH) – Upload certificates and keys via the **TLS** or **SSH Keys** page.
7. **Test connectivity** – Verify data flows between the serial port and network.

## 3 Quick Start Guides

### 3.1 Scenario 1: TCP Server (Listen for Incoming Connections)

Use this when a remote application needs to connect to the device to exchange serial data.

1. On the **Network** page, set **Protocol** to **TCP**.
2. On the **TCP** page:
  - Check **Listen for incoming network connections** for the desired serial port(s).
  - Set the **Listening network port** (default: 23).
  - Optionally set an **inactivity timeout** to auto-disconnect idle clients.
3. On the **Serial** page, configure the baud rate and other serial parameters to match your equipment.
4. Click **Submit New Settings**.
5. From a remote machine, connect using: `telnet <device-ip> <port>` (or any TCP client).
6. Data sent over the TCP connection appears on the serial port, and vice versa.

### 3.2 Scenario 2: TCP Client (Connect to a Remote Host)

Use this when the device should initiate a connection to a remote TCP server.

1. On the **Network** page, set **Protocol** to **TCP**.
2. On the **TCP** page:
  - Set **When to begin making outgoing TCP connections** to either “On power-up” or “When serial data received”.
  - Enter the destination **Connect to this address** (IP or hostname).
  - Set **Connect on network port** (the remote server’s port).
  - Optionally set **Retry failed outgoing connections** interval.
  - Optionally set **Keep-alive interval** to detect broken connections.
3. Configure serial settings on the **Serial** page.
4. Click **Submit New Settings**.
5. The device connects to the remote server automatically based on your trigger setting.

### 3.3 Scenario 3: Secure TCP/TLS Connection

Use this for encrypted serial-to-Ethernet communication using TLS.

1. On the **Network** page, set **Protocol** to **TCP/TLS**.
2. Configure TCP server or client settings on the **TCP** page as described above.
3. On the **TCP** page, ensure **Use TLS rather than TCP for connections** is checked.
4. On the **TLS** page:
  - Review the current certificate and key status.
  - To upload your own certificate and key:
    1. Generate a certificate and private key (see [TLS Certificate Management](#)).
    2. Use **Certificate file to install** and **Key file to install** to upload both files.
    3. Click **Install**.
5. If the device connects as a client to a server with a CA-signed certificate, upload the CA certificate on the **CA Certs** page.
6. Click **Submit New Settings**.
7. Connect using a TLS-capable client (e.g., `openssl s_client -connect <device-ip>:<port>`).

### 3.4 Scenario 4: SSH Tunnel for Serial Data

Use this for the highest level of security with SSH encryption and optional public key authentication.

1. On the **Network** page, set **Protocol** to **SSH**.
2. On the **SSH** page:
  - Check **Listen for incoming network connections**.
  - Set the **Listening network port** (default: 22).
  - Configure timeout settings as needed.
3. On the **SSH Keys** page:
  - Review the current RSA and ECDSA key status.
  - Optionally upload your own keys (see [SSH Key Management](#)).
4. On the **Password** page, set an **SSH Password** for client authentication.
5. Optionally enable public key authentication on the **SSH Authorized Client Keys** page:
  - Enable **Public Key Authentication**.
  - Upload client public keys into the available slots.
6. Click **Submit New Settings**.
7. Connect using an SSH client: `ssh -p <port> <username>@<device-ip>`

### 3.5 Scenario 5: UDP Broadcast

Use this for connectionless serial data transport, such as broadcasting sensor data.

1. On the **Network** page, set **Protocol** to **UDP**.
2. On the **UDP** page:
  - Set the **Incoming Port** for receiving network data.
  - Set the **Outgoing Port** for sending serial data.
  - Enter the **Send output to this address** (destination IP, or broadcast address like 192.168.1.255).
  - Optionally enable **Learn outbound address from last incoming packet**.
  - Configure packetization: character count, delay timer, and/or trigger character.
3. Configure serial settings on the **Serial** page.
4. Click **Submit New Settings**.

## 4 Network Configuration

Network			
Protocol	TCP/TLS (Changing will terminate all existing connections)		
Device Name (for DHCP)	SB800EXSX-B1F9		
Enable mDNS Local Name	<input checked="" type="checkbox"/>		
mDNS Local Name			
Version	03.02.00		
	Static Settings	DHCP Assigned Values	Address Mode
Device IP Address	0.0.0.0	10.1.1.140	DHCP
Device Subnet Mask	0.0.0.0	255.255.252.0	
Device Gateway	0.0.0.0	10.1.1.1	
DNS Server	0.0.0.0	10.1.1.1	
NTP Server	pool.ntp.org	172.104.209.204	Valid NTP time
System Time:	NTP: MAR 5 2026 day: 63 (THU) 03:31:08 UTC (When page was loaded)		
Reset To Factory Defaults		Submit New Settings	

Device Name: SB800EXSX-B1F9 | Version: 03.02.00

**Figure 1:** Network Configuration

The Network Configuration page is the main landing page of the web interface.

Field	Description
<b>Protocol</b>	Selects the network protocol: <b>SSH</b> , <b>TCP</b> , <b>TCP/TLS</b> , or <b>UDP</b> . Changing this enables/disables the relevant navigation links and configuration pages.
<b>Device Name</b>	The device name sent to your DHCP server. Also used as the NETBIOS name for network discovery.
<b>Version</b>	Displays the current firmware version number.
<b>Address Mode</b>	Choose between <b>DHCP</b> (automatic) and <b>Static</b> (manual) IP addressing.
<b>Device IP Address</b>	The device's IP address. If using DHCP, this is assigned automatically and shown in the DHCP column. For static mode, enter your desired address.
<b>Device Subnet Mask</b>	The subnet mask. Same DHCP/static behavior as IP address.
<b>Device Gateway</b>	The default gateway. Required for communication outside your local subnet.
<b>Device DNS</b>	The DNS server address. Required for hostname resolution (e.g., in TCP client mode with a hostname destination).

**Note:** After changing network settings, click **Submit New Settings**. If you change the IP address, you will need to navigate to the new address in your browser.

## 5 Protocol Configuration

Supported Protocols: TCP, UDP, TLS or SSH.

### 5.1 TCP Configuration

	Port 0	Port 1
<b>Listen for incoming network connections</b>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Listening network port:	<input type="text" value="23"/>	<input type="text" value="24"/>
Timeout and disconnect after this many seconds of inactivity.	<input type="text" value="60"/>	<input type="text" value="60"/>
Allow new connection if the existing connection has been idle for this many seconds.	<input type="text" value="30"/>	<input type="text" value="30"/>
<b>When to begin making outgoing tcp connections:</b>	<input type="text" value="Never"/>	<input type="text" value="Never"/>
Connect on network port:	<input type="text" value="1000"/>	<input type="text" value="1001"/>
Connect to this address:	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
Alternate address:	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
Timeout and disconnect after this many seconds of inactivity.	<input type="text" value="60"/>	<input type="text" value="60"/>
Retry failed outgoing connections after this many seconds.	<input type="text" value="360"/>	<input type="text" value="360"/>
Check and maintain valid connection at intervals in seconds.	<input type="text" value="0"/>	<input type="text" value="0"/>
<b>Use custom packetization logic (below)</b>	<input type="checkbox"/>	<input type="checkbox"/>
Number of characters to accumulate before sending TCP packet:	<input type="text" value="32"/>	<input type="text" value="32"/>
Number msec to wait for accumulated characters: 0 waits forever.	<input type="text" value="100"/>	<input type="text" value="100"/>
Send TCP frame when this character is received: Use a 2 digit hex value, NA to disable.	<input type="text" value="NA"/>	<input type="text" value="NA"/>
Use TLS rather than TCP for connections:	<input type="checkbox"/>	<input type="checkbox"/>
Always Save Serial Chars regardless of connection status:	<input type="checkbox"/>	<input type="checkbox"/>
DTR will reflect current connection status:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<i>Network Settings on Serial Port - <a href="#">Advanced Serial Settings</a></i>		
<input type="button" value="Submit New Settings"/>		

Device Name: SB800EXSX-B1F9 | Version: 03.02.00

Figure 2: TCP Configuration Page

Available when Protocol is set to **TCP** or **TCP/TLS**. Column headings (Port 0, Port 1, etc.) refer to the serial ports. On the SBE70LC, an additional I2C Port column appears.

#### 5.1.1 TCP Server Mode

Field	Description
<b>Listen for incoming network connections</b>	Enable this port to accept incoming TCP connections. Automatically disabled if the serial port is set to “Debug” or “Disabled”.
<b>Listening network port</b>	The TCP port to listen on (default: 23). Each serial port must use a different listen port.
<b>Timeout and disconnect after this many seconds of inactivity</b>	Disconnects if no data flows for this many seconds. Useful for detecting crashed clients. 0 = disabled.
<b>Allow new connection if existing connection has been idle for this many seconds</b>	Allows a new client to take over an idle connection. 0 = disabled.

### 5.1.2 TCP Client Mode

Field	Description
<b>When to begin making outgoing TCP connections</b>	Choose “Never”, “On power-up”, or “When serial data received”.
<b>Connect on network port</b>	The destination port number for outgoing connections.
<b>Connect to this address</b>	The destination IP address or hostname.
<b>Alternate address</b>	A secondary address to try if the primary fails.
<b>Timeout and disconnect after this many seconds of inactivity</b>	Client-side inactivity timeout. 0 = disabled.
<b>Retry failed outgoing connections after this many seconds</b>	How long to wait before retrying a failed connection.
<b>Check and maintain valid connection at intervals in seconds</b>	TCP keep-alive interval. Sends periodic probes to detect broken connections. 0 = disabled.

### 5.1.3 TCP Packetization Options

These apply to both server and client modes and control how serial data is batched into TCP packets.

Field	Description
<b>Use custom packetization logic</b>	Enable/disable custom packetization settings below.
<b>Number of characters to accumulate before sending TCP packet</b>	Maximum characters to buffer from the serial port before sending a TCP packet.
<b>Number of milliseconds to wait for accumulated characters (0 waits forever)</b>	Maximum time to wait for the character threshold. Overrides the character count if the timer expires first.
<b>Send TCP frame when this character is received</b>	Flush accumulated data when this character arrives. Enter a 2-digit hex value, or “NA” to disable.
<b>Use TLS rather than TCP for connections</b>	Enable TLS encryption for this port’s connections.

Field	Description
<b>Always Save Serial Chars regardless of connection status</b>	Continue buffering serial data even when no TCP connection is active.
<b>Network Settings on Serial Port – Advanced Serial Settings</b>	Link to advanced settings for serial messages triggered by network events.

## 5.2 UDP Configuration

Available when Protocol is set to **UDP**.

	Port 0	Port 1
Incoming port:	23	0
Outgoing port:	1000	1001
Send output to this address:	0.0.0.0	0.0.0.0
Learn outbound address from last incoming packet	<input type="checkbox"/>	<input type="checkbox"/>
Number of characters to accumulate before sending UDP packet:	32	32
Number msec to wait for accumulated characters: 0 waits forever.	100	100
Send UDP frame when this character is received: Use a 2 digit hex value, NA to disable.	NA	NA

[Submit New Settings](#)

Device Name: SB800EXSX-B1F9 | Version: 03.02.00

**Figure 3:** UDP Configuration Page

Field	Description
<b>Incoming Port</b>	The UDP port to listen on for incoming network data. Data received here is sent out the associated serial port.
<b>Outgoing Port</b>	The UDP port used for sending serial data to the network.
<b>Send output to this address</b>	The destination IP address for outgoing serial data. Use a broadcast address (e.g., x . x . x . 255) to send to all devices on the subnet.
<b>Learn outbound address from last incoming packet</b>	Send outgoing data to the IP address of the last received UDP packet. Useful when the remote client has a dynamic IP.
<b>Number of characters to accumulate before sending UDP packet</b>	Max characters to buffer (up to 1,480) before sending a UDP packet.
<b>Number of milliseconds to wait for accumulated characters (0 waits forever)</b>	Timeout for character accumulation. Overrides the character count.

Field	Description
<b>Send UDP frame when this character is received (Enter "NA" to disable)</b>	Flush accumulated data when this character arrives from the serial port.

### 5.3 SSH Configuration

Available when Protocol is set to **SSH**.

Network
UDP
TCP
TLS
SSH
Serial
Password
CA Certs
Advanced
Help

**SSH**

	Port 0	Port 1
<b>Listen for incoming network connections</b>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Listening network port:	<input type="text" value="22"/>	<input type="text" value="0"/>
Timeout and disconnect after this many seconds of inactivity.	<input type="text" value="360"/>	<input type="text" value="360"/>
Allow new connection if the existing connection has been idle for this many seconds.	<input type="text" value="180"/>	<input type="text" value="180"/>
<b>Use custom packetization logic (below)</b>	<input type="checkbox"/>	<input type="checkbox"/>
Number of characters to accumulate before sending TCP packet:	<input type="text" value="32"/>	<input type="text" value="32"/>
Number msec to wait for accumulated characters: 0 waits forever.	<input type="text" value="100"/>	<input type="text" value="100"/>
Flush TCP frame when this character is received (Enter NA to disable):	<input type="text" value="NA"/>	<input type="text" value="NA"/>
<a href="#">SSH Keys</a>   <a href="#">SSH Server Keys</a>   <a href="#">SSH Authorized Client Keys</a> <a href="#">Network Settings on Serial Port - Advanced Serial Settings</a>		
<input type="button" value="Submit New Settings"/>		

Device Name: SB800EXSX-B1F9 | Version: 03.02.00

**Figure 4:** SSH Configuration Page

Field	Description
<b>Listen for incoming network connections</b>	Enable incoming SSH connection requests on this port.
<b>Listening network port</b>	The SSH port to listen on (default: 22). Each serial port must use a different listen port.
<b>Timeout and disconnect after this many seconds of inactivity</b>	Disconnect idle SSH sessions. 0 = disabled. Default: 360 seconds.
<b>Allow new connection if existing connection has been idle for this many seconds</b>	Allow a new SSH client to replace an idle session. 0 = disabled. Default: 180 seconds.
<b>Use custom packetization logic</b>	Enable custom packetization for SSH data.
<b>Number of characters to accumulate</b>	Characters to buffer before sending over SSH.

---

Field	Description
<b>Number of milliseconds to wait for accumulated characters</b>	Timeout for character accumulation.
<b>Flush TCP frame when this character is received</b>	Trigger character to flush buffered data.
<b>SSH Keys</b>	Link to the SSH key management page.
<b>Network Settings on Serial Port - Advanced Serial Settings</b>	Link to advanced network-event serial messages.

---

## 6 Serial Port Configuration

Network
UDP
TCP
TLS
SSH
Serial
Password
CA Certs
Advanced
Help

**Serial**

	Port 0	Port 1
Data Port Settings:	RS-232 ▼	DEBUG ▼
Data Baud Rate:	115200 ▼	115200 ▼
Custom Baud Rate:	<input type="text" value="0"/>	<input type="text" value="0"/>
Data Bits:	8 ▼	8 ▼
Data Parity:	None ▼	None ▼
Stop Bits:	1 ▼	1 ▼
Flow Control:	None ▼	None ▼
AT Commands:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Disabled Port Pin Function:	High Impedance ▼	High Impedance ▼
<input type="button" value="Submit New Settings"/>		

**Device Name: SB800EXSX-B1F9 | Version: 03.02.00**

**Figure 5:** Serial Configuration Page

Most platforms provide two TTL-level UARTs (Port 0 and Port 1). External level shifters are required for RS-232, RS-422, and RS-485 signaling.

### 6.1 Serial Port Modes

Mode	Description
<b>RS-232</b>	Standard serial communication. Select for TTL-level or with an RS-232 level shifter.
<b>RS-485</b>	Select if you have an RS-485 level shifter. Supports half-duplex and full-duplex.
<b>DEBUG</b>	Uses the port as stdin/stdout/stderr for debug messages. Valid for TTL or RS-232 modes.
<b>Disabled</b>	Disables the serial port and its associated network connections, TCP/UDP/SSH listeners, and AT commands. The “Disabled Port Pin Function” field controls what happens to the pins.

**Note:** If both ports are set to DEBUG, Port 0 takes priority.

### 6.2 Serial Port Settings

Field	Description
<b>Data Port Settings</b>	Select the serial mode: RS-232, RS-485 Half-Duplex, RS-485 Full-Duplex, RS-422 Full-Duplex, DEBUG, or Disabled. Available modes depend on the platform and port.
<b>Data Baud Rate</b>	Standard rates from 1200 to 921600 baud.
<b>Custom Baud Rate</b>	Enter a non-standard baud rate value. Set to 0 to use the standard rate selection above.
<b>Data Bits</b>	5, 6, 7, or 8 data bits.
<b>Data Parity</b>	None, Odd, or Even.
<b>Stop Bits</b>	1 or 2 stop bits.
<b>Flow Control</b>	None, Xon/Xoff (software), or RTS/CTS (hardware). Hardware flow control requires RS-232 mode.
<b>AT Commands</b>	Enable or disable the AT command interface on this serial port. Disabled by default. See <a href="#">AT Command Interface</a> .
<b>Disabled Port Pin Function</b>	When the serial port mode is “Disabled”, this controls the pin behavior: <b>High Impedance</b> (with internal pull-up), <b>Output High</b> , or <b>Output Low</b> . Only output pins (Tx, RTS) are affected; input pins (Rx, CTS) are always high-impedance.

### 6.3 Serial Port Pin Table

The web interface displays a table of pins associated with each serial port, showing which physical pins are reconfigured when using the “Disabled” serial port mode.

## 7 Security Configuration

### 7.1 Password Configuration

Network
UDP
TCP
TLS
SSH
Serial
Password
CA Certs
Advanced
Help

**Password**

Administrator

User Name:

Password:  (Leave blank for no password)

Repeat Password:

Allow AT Access

SSH User

User Name:

Password:  (Leave blank for no password)

Repeat Password:

Allow AT Access

Device Name: SB800EXSX-B1F9 | Version: 03.02.00

**Figure 6:** Password Configuration Page

Field	Description
<b>User Name</b> (Administrator)	The administrator username for web interface, firmware updates, configuration access, and SSH login.
<b>Password</b> (Administrator)	The administrator password. Leave blank for no password (not recommended for production).
<b>Repeat Password</b>	Confirm the administrator password.
<b>Allow AT Access</b> (Administrator)	When checked, AT commands can query and set the admin username and password.
<b>SSH Password</b>	A separate password for SSH clients without administrative privileges.
<b>Allow AT Access</b> (SSH)	When checked, AT commands can query and set the SSH username and password, and manage SSH authorized keys.

**Important:** Always set a strong administrator password before deploying the device on a production network.

## 7.2 TLS Certificate and Key Management

Device Name: SB800EXSX-B1F9 | Version: 03.02.00

RSA key sizes must be at least 512 and no more than 4096 and in openSSH(openSSL) format. ECDSA key sizes must be at least 192 and no larger than 256.

**Figure 7:** TLS Configuration Page

The TLS page manages certificates and keys used for TCP/TLS encrypted connections and HTTPS web server access.

**Certificate/Key Priority:** 1. **User Installed** – A certificate and key you have uploaded (highest priority). 2. **Default** – Certificate and key compiled into the application firmware. 3. **NetBurner** – Built-in library default (lowest priority, used as fallback).

Field	Description
<b>TLS Public Key Certificate</b>	Displays the current certificate in use and its source.
<b>Public/Private Key Pair</b>	Displays the current keys in use and their source.
<b>Certificate file to install</b>	Select a certificate file (. crt) to upload.
<b>Key file to install</b>	Select a private key file (. key) to upload. Must match the certificate.

**Important:** The certificate and key must be uploaded together. Key sizes must be 512 to 4096 bits in OpenSSH/OpenSSL format.

### Generating a self-signed certificate and key:

```
# Generate a private key
openssl genrsa -out cert.key 2048
```

```
# Generate a self-signed certificate (valid for 365 days)
openssl req -new -x509 -key cert.key -out cert.crt -days 365 -subj "/CN=NetBurner Device"
```

**Using HTTPS:** Once a certificate and key are installed, access the web interface securely at `https://<device-ip>`. The device serves both HTTP and HTTPS simultaneously. With a self-signed certificate, your browser will display a security warning that you must accept.

## 7.3 SSH Server Key Management

Network UDP TCP TLS SSH Serial Password CA Certs Advanced Help

### SSH Keys

RSA Public/Private Key Pair	Default	<a href="#">Display Public Key</a>
ECDSA Public/Private Key Pair	Default	<a href="#">Display Public Key</a>
RSA or ECDSA Key File to Install	<input type="button" value="Choose File"/>	No file chosen

Device Name: SB800EXSX-B1F9 | Version: 03.02.00

**SSH Keys - RSA key sizes must be at least 512 and no more than 4096 and in openSSH(openSSL) format. ECDSA key sizes must be at least 192 and no larger than 256.**

**Figure 8:** SSH Server Keys Configuration Page

The SSH Keys page manages the device's SSH server host keys (RSA and ECDSA).

**Key Priority:** 1. **User Installed** – A key you have uploaded (highest priority). 2. **Default** – Key compiled into the application firmware. 3. **NetBurner** – Built-in library default (lowest priority, used as fallback).

Field	Description
<b>RSA Public/Private Key Pair</b>	Displays the current RSA key in use and its source.
<b>ECDSA Public/Private Key Pair</b>	Displays the current ECDSA key in use and its source.
<b>RSA or ECDSA Key File to Install</b>	Select a private key file to upload. The public key is extracted automatically. Click "Install Key" to upload.

**Important:** Key sizes must be 512 to 4096 bits in OpenSSH/OpenSSL format.

### Generating SSH host keys:

```
# Generate an RSA key
ssh-keygen -t rsa -b 2048 -f rsa.key -N ""
```

```
# Generate an ECDSA key
ssh-keygen -t ecdsa -b 256 -f ecdsa.key -N ""
```

## 7.4 SSH Authorized Client Keys

Device Name: SB800EXSX-B1F9 | Version: 03.02.00

**SSH Authorized Client Keys - Upload OpenSSH format public key files (.pub) for key-based authentication. Supports RSA, ECDSA, and Ed25519 key types.**

**Figure 9:** SSH Authorized Client Keys Configuration Page

The SSH Authorized Client Keys page enables public key authentication for SSH clients, providing passwordless login.

Field	Description
<b>Public Key Authentication</b>	Enable or disable SSH public key authentication globally.
<b>Slot 0/1/2 – Authorized Key</b>	Displays the status of each key slot (Empty or Installed with size and type). Up to 3 client public keys can be installed.
<b>Key Slot to Install</b>	Select which slot (0, 1, or 2) to install the key into.
<b>OpenSSH Public Key File (.pub)</b>	Select the client’s public key file to upload. Supports RSA, ECDSA, and Ed25519 key types.
<b>Delete All Authorized Keys</b>	Removes all installed authorized keys.

### Setting up key-based SSH authentication:

```
# On the client machine, generate a key pair (if you don't have one)
ssh-keygen -t ecdsa -b 256 -f ~/.ssh/netburner_key

# Upload the PUBLIC key (.pub file) to the device via the web interface
# Then connect without a password:
ssh -i ~/.ssh/netburner_key -p <port> <username>@<device-ip>
```

## 7.5 CA Certificate Store

Network	UDP	TCP	TLS	SSH	Serial	Password	CA Certs	Advanced	Help
<b>Common Name</b>			<b>Public Key Link</b>				<b>Delete</b>		
Certificate Authority Certificate to Install						Choose File	No file chosen		Add New client CA

RSA key sizes must be at least 512 and no more than 4096 and in openSSH(openSSL) format. ECDSA key sizes must be at least 192 and no larger than 256.

**Figure 10:** Certificate Authority Configuration Page

The CA Certificates page manages trusted Certificate Authority certificates used to verify remote servers during outgoing TLS connections.

Field	Description
<b>Certificate list</b>	Table showing installed CA certificates with Common Name, Public Key link, and Delete option.
<b>Certificate Authority Certificate to Install</b>	Select a CA certificate file (. crt) to upload. Click “Add New client CA” to install.

**Note:** RSA key sizes must be 512–4096 bits. ECDSA key sizes must be 192–256 bits. Files must be in OpenSSH/OpenSSL format.

## 8 GPIO Configuration

Available on: SBE70LC (without I2C), MODM7AE70 (without I2C/WiFi), SOMRT1061, MODRT1171

The GPIO page provides remote control and monitoring of general-purpose I/O pins and analog-to-digital inputs via a TCP network server.

### 8.1 GPIO Pin Settings

Field	Description
<b>Pin Number</b>	Physical pin number on the module header.
<b>Pin Usage</b>	The function assigned to each pin (GPIO, ADC, fixed function, etc.). Configured via this web page.
<b>Power-up Pin Settings</b>	The pin state on device boot (Input, Output High, Output Low).
<b>Current Setting</b>	The current pin state/value.
<b>Save pin changes to flash</b>	When enabled, pin configuration changes are stored persistently in flash. Increases flash write cycles if pins change frequently.
<b>Enable high current drive</b>	Low = 2 mA drive strength; High = 10 mA drive strength.

### 8.2 GPIO Network Server Settings

Field	Description
<b>Enable remote GPIO server</b>	Enable or disable the TCP-based GPIO control server.
<b>GPIO server port</b>	TCP port the GPIO server listens on (default: 1000).
<b>Timeout and disconnect after this many seconds of inactivity</b>	Auto-disconnect idle GPIO connections.
<b>Maximum simultaneous connections allowed</b>	Limit on concurrent GPIO client connections.

### 8.3 GPIO Network Commands

Connect to the GPIO server via TCP (e.g., `telnet <device-ip> 1000`) and use these commands. All commands must be terminated with a line feed (0x0A).

#### Digital I/O:

Command	Description
Pxx=0	Set pin xx output low
Pxx=1	Set pin xx output high
Pxx=I	Set pin xx as input
Pxx?	Read pin xx input value (automatically sets pin as input)

**Analog Input (SAME70 platforms only – MODM7AE70, SBE70LC):**

Command	Description
Pxx?	Read ADC value (0–4095 counts, ratiometric to 3.3V reference)

**Network and Utility:**

Command	Description
X	Disconnect from the GPIO server
E	Enable character echo
e	Disable character echo
V	Query firmware version

**Response Format:** - Success: 0, OK\r\n - Read value: <value>, OK\r\n - Error: <negative code>, <description>\r\n

**Error Codes:** - -1: Pin not in GPIO mode - -2: Invalid pin number - -3: Command syntax error

## 9 I2C Configuration

Available on: SBE70LC only

**Figure 11:** I2C Configuration Page

The Ethernet-to-I2C feature allows remote I2C bus access over a TCP connection.

### 9.1 I2C Settings

Field	Description
<b>Bus Speed</b>	I2C bus clock speed in Hz (default: 100000).
<b>Connected I2C Devices</b>	Displays addresses of devices detected on the I2C bus. The scan is performed when the page loads.

### 9.2 Ethernet-to-I2C Commands

Connect to the I2C port via TCP (default port: 26). All commands begin with # and are executed with Enter. Input values are two-digit hex. Disconnect with Ctrl+D.

Command	Description	Returns
#WB<addr><data>	Write a byte	<byte written> OK
#WW<addr><len><data>	Write a buffer	<bytes written> OK
#RB<addr>	Read a byte	<byte read> OK
#RR<addr><len>	Read a buffer	<bytes read> OK
#WR<addr><data>	Write a byte, then read a byte	<written>, <read> OK
#WA<addr><data><len>	Write a byte, then read a buffer	<written>, <bytes read> OK
#ST	Print I2C bus status	<status> OK
#RE	Reset the I2C bus	OK
#SC	Scan for active devices	<addr>, <addr>, ... OK
#MENU or #HELP or ?	Print main menu	<menu>

**Examples:** - #WB39AC – Write 0xAC to address 0x39 - #RB39 – Read a byte from address 0x39 - #RR390A – Read 10 bytes from address 0x39

## 10 WiFi Configuration

Available on: SB800EX only

The WiFi page configures the wireless network interface, which operates independently from the wired Ethernet interface.

### 10.1 WiFi Network Settings

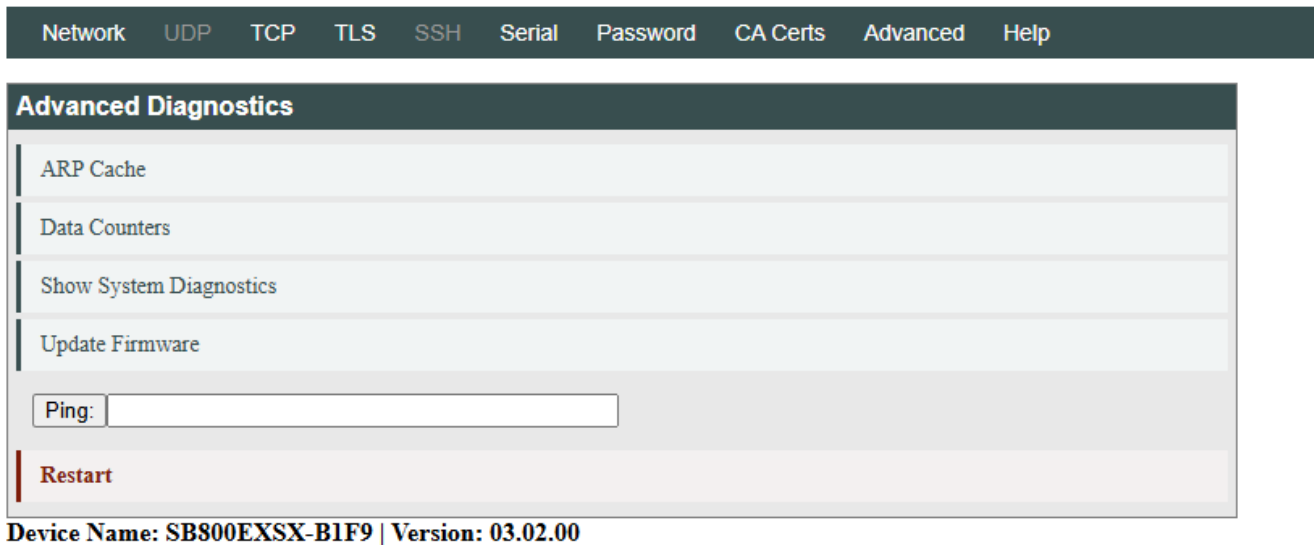
Field	Description
<b>Device IP Address</b>	WiFi interface IP. Supports DHCP (automatic) or Static addressing.
<b>Device Subnet Mask</b>	WiFi subnet mask.
<b>Device Gateway</b>	WiFi gateway address.
<b>DNS Server</b>	WiFi DNS server.
<b>Address Mode</b>	DHCP or Static for the WiFi interface.
<b>SSID</b>	The configured WiFi network name.
<b>Connection Status</b>	Displays the current WiFi connection state.
<b>Scan</b>	Scans for available WiFi networks.

### 10.2 Connecting to a WiFi Network

1. Navigate to the **WiFi** page.
2. Click **Scan** to discover available networks.
3. Enter or select the desired **SSID**.
4. Enter the network password.
5. Select **DHCP** or **Static** addressing.
6. Click **Submit New Settings**.

**Note:** WiFi credentials can also be configured via AT commands (see AT#WICON, AT#WICLR, AT#WISSID?, AT#WIIP?).

## 11 Advanced Diagnostics



**Figure 12:** Advanced Diagnostics Page

The Advanced Diagnostics page provides system-level tools for monitoring and troubleshooting.

### 11.1 Available Tools

Tool	Description
<b>ARP Cache</b>	Displays the device's ARP (Address Resolution Protocol) cache, showing known IP-to-MAC address mappings.
<b>Data Counters</b>	Shows network data transfer statistics.
<b>Show System Diagnostics</b>	Displays detailed RTOS task information, memory usage, socket status, and other system internals.
<b>Update Firmware</b>	Downloads and installs the latest firmware from the internet. Requires internet connectivity. Prompts for confirmation before proceeding.
<b>Ping</b>	Sends ICMP ping requests to a specified IP address or hostname. Useful for verifying network connectivity.
<b>Restart</b>	Reboots the device. Prompts for confirmation before proceeding.

**Tip:** The Ping tool defaults to the configured outgoing connection addresses. You can enter any IP or hostname to test.

## 12 Hardware Factory Reset (SB800EX)

On the SB800EX platform, a hardware pushbutton can be used to restore all settings to factory defaults without network or serial access. This is useful when the device is unreachable due to misconfigured network settings or a forgotten password.

### 12.1 Procedure

1. **Power off** the device.
2. **Press and hold** the reset button (pin E1) on the SB800EX module.
3. **While holding the button**, apply power to the device.
4. Continue holding the button for approximately **7 seconds**. During this time, both LEDs will blink alternating **red** and **green** to indicate the reset is in progress.
5. When the LEDs turn **off**, the factory reset is complete. Release the button.
6. The device will continue booting with all factory default settings, including DHCP enabled.

### 12.2 What Gets Reset

The hardware factory reset restores **all** settings to their factory defaults, including:

- Network configuration (IP address mode set to DHCP, device name regenerated)
- Serial port settings (baud rate, data bits, parity, stop bits, flow control)
- Protocol and connection settings
- Administrator and SSH passwords (cleared)
- TLS certificates and keys (restored to factory defaults)
- SSH server keys (restored to factory defaults)
- SSH authorized client keys (removed)
- WiFi SSID and password (cleared)
- SNMP settings (reset to defaults)

**Note:** The hardware factory reset is equivalent to issuing AT&F followed by AT&P and rebooting, but does not require serial or network access.

## 13 AT Command Interface

The AT command interface allows configuration of the device via the serial port, without requiring network access. This is useful for initial setup, field configuration, and automation.

### 13.1 Enabling AT Commands

The screenshot shows the 'Serial' configuration page. The 'Serial' tab is highlighted with a red box and a '1'. The 'AT Commands' checkbox for Port 0 is checked and highlighted with a red box and a '2'. The 'Submit New Settings' button is highlighted with a red box and a '3'. The device name and version are shown at the bottom: 'Device Name: SB800EXSX-B1F9 | Version: 03.02.00'.

**Figure 13:** How to Enable AT Commands

AT commands are **disabled by default**. To enable: 1. Navigate to the **Serial** page in the web interface. 2. Check the **AT Commands** checkbox for the desired port(s). 3. Click **Submit New Settings**.

### 13.2 Entering and Exiting Command Mode

**Entering:** Send +++ (three plus characters) with at least 1 second of silence before and after. The device responds:

```
Starting AT Command
OK>
```

**Exiting:** - AT0 or AT&X – Exit without saving changes - AT&P – Exit and save all changes to flash

**Inactivity Timeout:** Command mode exits automatically after 30 seconds of inactivity.

### 13.3 Command Syntax

Form	Syntax	Description
Query	AT#CMD?	Returns the current value

Form	Syntax	Description
Set	AT#CMD=<value>	Sets a new value
Action	AT#CMD	Performs an action
Per-port	AT#SERnCMD	n = port number (0–9)

**Response Format:** - Success: <value>\r\nOK (query) or \r\nOK (set/action) - Error: \r\nERR - Unknown: Unknown Command [<cmd>]\r\nERR>

### 13.4 Control Commands

Command	Description
ATO	Exit AT command mode without saving
AT&X	Exit AT command mode without saving
AT&P	Exit and save configuration to flash
AT&F	Restore factory defaults in memory (does not save)

### 13.5 Network Configuration Commands

Command	Description	Values
AT#SYSIP	IP address	Dotted-decimal (e.g., 192.168.1.100)
AT#SYSMK	Subnet mask	Dotted-decimal
AT#SYSGW	Gateway	Dotted-decimal
AT#SYSDN	DNS server	Dotted-decimal
AT#SYSDH	DHCP enable	1 = DHCP, 0 = static
AT#SYSEMDNS	Enable/disable mDNS	1 = enable, 0 = disable
AT#SYSMDNS	mDNS local name	String

### 13.6 Protocol Mode

Command	Description
AT#SYSMD=T	Set to TCP
AT#SYSMD=L	Set to TCP/TLS
AT#SYSMD=U	Set to UDP
AT#SYSMD=S	Set to SSH

### 13.7 Current Network Status (Read-Only)

Command	Description
AT#CURMA?	Current MAC address
AT#CURIP?	Current IP address
AT#CURMK?	Current subnet mask
AT#CURGW?	Current gateway
AT#CURDN?	Current DNS server
AT#CURST?	Port status for current AT port
AT#CURSn?	Port status for port n

### 13.8 Serial Port Commands

All use AT#SERn prefix where n is the port number.

Command	Description	Values
AT#SERnSM	Serial mode	R=RS-232, D=Debug, H=RS-485 Half, F=RS-485 Full
AT#SERnBR	Baud rate	Standard rates or any custom value
AT#SERnDB	Data bits	8, 7, 6, 5
AT#SERnPR	Parity	N=None, O=Odd, E=Even
AT#SERnST	Stop bits	1, 2
AT#SERnFL	Flow control	N=None, S=XON/XOFF, H=RTS/CTS
AT#SERnLN	Listen enable	1=listen, 0=don't
AT#SERnSS	Use TLS	1=enable, 0=disable
AT#SERnSP	Listen port	0-65535
AT#SERnSD	Inactivity timeout (sec)	0+
AT#SERnSO	New connection override (sec)	0+
AT#SERnCI	Outgoing destination IP/hostname	IP or hostname string
AT#SERnCP	Outgoing destination port	0-65535
AT#SERnCM	Connect mode	N=Never, P=Power-up, R=Serial data
AT#SERnCD	Outgoing idle timeout (sec)	0+
AT#SERnCR	Connection retry (sec)	0+
AT#SERnKA	Keep-alive interval (sec)	0+
AT#SERnUL	UDP learn mode	1=enable, 0=disable

### 13.9 Credential Commands

Requires AT access to be enabled on the Password web page.

Command	Description
AT#SYSUN / AT#SYSPW	Set/query combined username/password (admin + SSH)
AT#SYSAUN / AT#SYSAPW	Set/query admin-only username/password
AT#SYSSUN / AT#SYSSPW	Set/query SSH-only username/password

### 13.10 SSH Public Key Commands

Requires SSH AT access to be enabled. Key commands save to flash immediately.

Command	Description
AT#SYSSKA=<slot>, <key>	Install authorized key (slots 0–2, OpenSSH format)
AT#SYSSKA?	Query all key slot status
AT#SYSSKE	Enable public key authentication
AT#SYSSKD	Disable public key authentication
AT#SYSSKR	Remove all authorized keys

### 13.11 GPIO Commands

*Platforms with GPIO support only.*

Command	Description	Values
AT#SYSGS	Enable/disable GPIO server	1/0
AT#SYSGP	GPIO server port	0–65535
AT#SYSGF	Save GPIO to flash	1/0
AT#P<nn>	Read/set digital pin nn	Query: returns GPIO In=<0   1>, Set: 0/1
AT#PA<nn>	Read analog pin nn (SAME70 only)	Returns GPIO In=<adc>

### 13.12 WiFi Commands

*SB800EX only.*

Command	Description
AT#WICON=<ssid>, <pass>	Connect to WiFi network
AT#WICLR	Disconnect and clear credentials
AT#WISSID?	Query WiFi SSID
AT#WIIP?	Query WiFi IP address

---

Command	Description
---------	-------------

---

### 13.13 Saving Configuration

---

Action	Behavior
AT&P	Exits and saves all settings to flash
ATO / AT&X	Exits without saving
AT&F	Restores factory defaults in memory (does not save)
SSH key commands	Save to flash <b>immediately</b> (no AT&P needed)

---

## 14 Advanced Serial Settings & Message Formatting

The **Advanced Serial Settings** page (accessed via the link on the TCP or SSH configuration page) allows you to configure serial messages that are sent in response to network events.

**Advanced Serial**

**Port 0: Serial Data Notification Settings**

Send serial message when TCP connection is established

Send serial message when TCP connection is lost  
 Message to send:

[Message Formatting Codes](#)

Send serial break when incoming TCP connection is established  
 Break interval (in tenths of a second):

Send serial break when incoming character is received (2-digit hex, i.e. "02"):

**Port 1: Serial Data Notification Settings**

Send serial message when TCP connection is established

Send serial message when TCP connection is lost  
 Message to send:

[Message Formatting Codes](#)

Send serial break when incoming TCP connection is established  
 Break interval (in tenths of a second):

Send serial break when incoming character is received (2-digit hex, i.e. "02"):

**Figure 14:** Advanced Serial Settings Configuration Page

These settings enable the device to output configurable messages on the serial port when specific network events occur, such as when a TCP connection is established or lost.

Setting	Description
<b>Send message on connect</b>	When enabled, sends a configurable message out the serial port when a network connection is established.
<b>Send message on connection lost</b>	When enabled, sends a configurable message when the network connection is terminated.
<b>Send break on connect</b>	Sends a serial break signal when a network connection is established.
<b>Break interval</b>	Duration of the serial break signal in milliseconds (default: 20).
<b>Break key</b>	When enabled, a specific character received from the network triggers a serial break signal.

---

Setting	Description
<b>Break key value</b>	The hex value of the character that triggers a break (default: 02).

---

## 14.1 Message Formatting Codes

When composing connect/disconnect messages, the following formatting codes can be used:

---

Code	Data Item
%%	Literal “%” character
%r	Line feed (ASCII 10)
%n	Carriage return (ASCII 13)
%x	Any hex value, e.g., %X20 for ASCII space

---

## 15 Advanced Network Settings

The **Advanced Network Settings** page provides additional per-port network options. Access it by navigating to the **Advanced Network** link in the web interface.

### 15.1 TCP Host Identification

When a TCP connection is established, the device can automatically send an identification string to the remote host. This is useful for identifying which device is connecting when multiple units report to a central server.

Setting	Description
<b>Send identification to TCP host</b>	When enabled, sends an identification string to the remote TCP host each time a connection is established.
<b>Custom Site ID</b>	A custom identifier string (up to 12 characters) sent on connect. If left blank, the device's MAC address is sent instead.

#### 15.1.1 How It Works

1. Enable the **Send identification to TCP host** checkbox for the desired serial port.
2. Optionally enter a **Custom Site ID** (up to 12 characters). If left blank, the device's MAC address will be used as the identifier.
3. Click **Submit New Settings** to save.
4. Each time a TCP connection is established on that port, the configured identifier is sent to the remote host before any serial data is forwarded.

**Tip:** Use a meaningful Custom Site ID (e.g., a location code or equipment label) to easily identify devices in multi-unit deployments. Leave it blank to use the MAC address, which is guaranteed to be unique.

## 16 Troubleshooting

### 16.1 Cannot Access the Web Interface

Symptom	Possible Cause	Solution
Browser cannot connect	Wrong IP address	Use NBFind utility or check DHCP server for the device's IP. Connect a serial debug terminal to see the boot IP.
Browser cannot connect	Device on different subnet	Ensure your computer and the device are on the same subnet, or configure a route.
Connection refused	Firewall blocking	Check that no firewall is blocking HTTP (port 80) or HTTPS (port 443).
Password prompt	Password was set	Enter the administrator credentials. If forgotten, use AT command AT&F to restore factory defaults (clears password).

### 16.2 No Data Flowing Between Serial and Network

Symptom	Possible Cause	Solution
Serial data not reaching network	Wrong serial settings	Verify baud rate, data bits, parity, and stop bits match your serial device exactly.
Serial data not reaching network	Port set to Debug or Disabled	Check the Serial page – the port mode must be RS-232 or RS-485.
Serial data not reaching network	No network connection	For TCP server mode, verify a client is connected. For client mode, verify the destination is reachable.
Network data not reaching serial	Flow control mismatch	If using hardware flow control (RTS/CTS), ensure the serial device supports it and cables are properly wired.
Intermittent data loss	Packetization settings	Adjust the character accumulation count, wait timer, and trigger character on the TCP/UDP/SSH page.

### 16.3 TCP Connection Issues

Symptom	Possible Cause	Solution
Cannot connect to device	Listen not enabled	Check that “Listen for incoming network connections” is checked on the TCP page.
Cannot connect to device	Wrong port	Verify the listening port number matches what the client is connecting to.
Connection drops unexpectedly	Inactivity timeout	Increase the inactivity timeout value or set to 0 to disable.
Client mode not connecting	Wrong destination	Verify the “Connect to this address” and port number are correct. Use Ping on the Advanced page to test.
Client mode not connecting	Connection mode set to Never	Set the connection trigger to “On power-up” or “When serial data received”.

## 16.4 TLS/SSL Issues

Symptom	Possible Cause	Solution
TLS handshake fails	Certificate/key mismatch	Upload a matching certificate and key pair together.
TLS handshake fails	Key format wrong	Ensure keys are in OpenSSH/OpenSSL format, 512–4096 bits.
Browser shows security warning	Self-signed certificate	Expected with self-signed certificates. Add an exception in your browser, or install a CA-signed certificate.
Client cannot verify server	Missing CA certificate	Upload the server’s CA certificate on the CA Certs page.

## 16.5 SSH Issues

Symptom	Possible Cause	Solution
SSH connection refused	Protocol not set to SSH	Change Protocol to SSH on the Network page.
Authentication fails	Wrong password	Verify the SSH password on the Password page. The admin password also works for SSH.

Symptom	Possible Cause	Solution
Public key auth fails	Key not installed	Upload the client's .pub file on the Authorized Client Keys page. Ensure "Public Key Authentication" is enabled.
Public key auth fails	Wrong key type	Ensure the key is in OpenSSH format. Supported types: RSA, ECDSA, Ed25519.

## 16.6 AT Command Issues

Symptom	Possible Cause	Solution
+++ not entering command mode	AT commands disabled	Enable "AT Commands" on the Serial page for the port in use.
+++ not entering command mode	Guard time not met	Ensure 1 second of silence before and after the +++ sequence.
Commands return ERR	Wrong syntax	Use AT#CMD? for query, AT#CMD=value for set. Check port numbers in serial commands.
Credential commands fail	AT access disabled	Enable "Allow AT Access" on the Password page for admin and/or SSH credentials.
Changes lost after reboot	Forgot to save	Use AT&P to save changes before exiting command mode.

## 16.7 General Tips

- **Factory Reset:** Use AT&F via serial to restore all settings to factory defaults (in memory only). Follow with AT&P to save, then reboot. On SB800EX, you can also hold the physical reset button during power-on for ~7 seconds to perform a hardware factory reset without serial or network access.
- **Firmware Update:** Use the Advanced Diagnostics page to check for and install firmware updates.
- **Check Diagnostics:** The Advanced Diagnostics page provides ARP cache, data counters, and system diagnostics that can help identify network or resource issues.
- **Multiple Connections:** Up to 5 simultaneous TCP connections are supported per port.

## 17 Appendix A: Default Settings Reference

These are the factory default values. Use AT&F to restore these settings in memory.

### 17.1 Network Defaults

Setting	Default Value
Protocol	TCP/TLS
Address Mode	DHCP
Listen Port	23 (Telnet)
Inactivity Timeout	60 seconds
New Connection Timeout	30 seconds
Outgoing Connection Mode	Never
Outgoing Port	1000
Outgoing Address	0.0.0.0 (none)
Outgoing Idle Timeout	60 seconds
Outgoing Retry Timeout	360 seconds
Keep-alive Interval	0 (disabled)
Max TCP Connections	5
NTP Server	pool.ntp.org

### 17.2 Serial Defaults

Setting	Default Value
Baud Rate	115200
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None
AT Commands	Disabled
Custom Baud Rate	0 (use standard)
Disabled Port Pin Function	High Impedance

### 17.3 SSH Defaults

Setting	Default Value
Inactivity Timeout	360 seconds
New Connection Timeout	180 seconds

## 17.4 UDP Defaults

Setting	Default Value
Accumulated Characters	32
Wait Time (ticks)	100
Trigger Character	NA (disabled)
Learn Mode	Disabled

## 17.5 TCP Packetization Defaults

Setting	Default Value
Custom Packetization	Disabled
Accumulated Characters	32
Wait Time (ticks)	100
Trigger Character	NA (disabled)

## 17.6 GPIO Defaults

Setting	Default Value
GPIO Server	Enabled
GPIO Port	1000
Save to Flash	Enabled
High Current Drive	Disabled

## 17.7 I2C Defaults

Setting	Default Value
Bus Speed	100000 Hz
Listen Port	26

## 17.8 Advanced Serial Defaults

Setting	Default Value
Send Message on Connect	Disabled
Send Message on Connection Lost	Disabled
Break on Connect	Disabled

---

Setting	Default Value
Break Interval	20 ms
Break Key	Disabled
Break Key Value	02 (hex)

---

## 17.9 Advanced Network Defaults

---

Setting	Default Value
Send ID On Connect	Disabled
Custom Site ID	(empty)

---

## 18 Appendix B: Platform Comparison Table

Feature	MOD5441X	SB800EX	NANO54415	MODM7AE70	SBE70LC	SOMRT1061	MODRT1171
<b>Serial Ports</b>	2	2	5	2 (7*)	2	7	2
<b>RS-232</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>RS-485</b>	Yes	Yes	Port 0-1	Port 0-1	Yes	Yes	Yes
<b>GPIO Server</b>	-	-	-	Yes**	Yes***	Yes	Yes
<b>Analog GPIO (ADC)</b>	-	-	-	Yes	Yes	-	-
<b>I2C Bridge</b>	-	-	-	-	Yes***	-	-
<b>WiFi</b>	-	Yes	-	-	-	-	-
<b>TCP/TLS</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>SSH</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>UDP</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Hardware Factory Reset</b>	-	Yes	-	-	-	-	-

\* With USE\_E70\_UART\_SERIAL\_PORTS build option \*\* When I2C and WiFi are not compiled in \*\*\* GPIO and I2C are mutually exclusive on SBE70LC

## 19 Appendix C: Pinout Reference

### 19.1 Serial Port 0 Pinout (DB-9)

Pin	RS-232 Function	RS-422/485 Function
1	CD (in)	–
2	Rx (in)	B Tx and Half-Duplex Rx
3	Tx (out)	A Tx and Half-Duplex Rx
4	DTR (out)	–
5	Ground	Ground
6	DSR (in)	B/Z Rx for Full-Duplex
7	RTS (out)	A/Y Rx for Full-Duplex
8	CTS (in)	–
9	RI (in)	–

### 19.2 Serial Port 1 Pinout (DB-9)

Pin	RS-232 Function
1	CD (in)
2	Rx (in)
3	Tx (out)
4	DTR (out)
5	Ground
6	DSR (in)
7	RTS (out)
8	CTS (in)
9	RI (in)

**Note:** Port 0 can be configured for RS-232 or RS-422/485. Port 1 is always RS-232. Pinouts shown are for the standard DB-9 connector configuration. Actual pin assignments may vary by platform – consult your hardware documentation.