Simply Better Connections

SN3001 / SN3001P
SN3002 / SN3002P
SN3401 / SN3401P
SN3402 / SN3402P

Secure Serial Device Server

User Manual

Compliance Statements

FEDERAL COMMUNICATIONS COMMISSION INTERFERENCE STATEMENT

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

Warning

Operation of this equipment in a residential environment could cause radio interference.

Achtung

Der Gebrauch dieses Geräts in Wohnumgebung kann Funkstörungen verursachen.

Suggestion

Shielded twisted pair (STP) cables must be used with the unit to ensure compliance with FCC & CE standards.

KCC Statement

유선 제품용 / A 급 기기 (업무용 방송 통신 기기)
이 기기는 업무용 (A 급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며 , 가정 외의 지역에서 사용하는 것을 목적으로 합니다 .

Industry Canada Statement

This Class A digital apparatus complies with Canadian ICES-003.

CAN ICES-003 (A) / NMB-003 (A)

RoHS

This product is RoHS compliant.

User Information

Online Registration

Be sure to register your product at our online support center:

International	http://eservice.aten.com

Telephone Support

For telephone support, call this number:

International	886-2-8692-6959
China	86-400-810-0-810
Japan	81-3-5615-5811
Korea	82-2-467-6789
North America	1-888-999-ATEN ext 4988 1-949-428-1111

User Notice

All information, documentation, and specifications contained in this manual are subject to change without prior notification by the manufacturer. The manufacturer makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties as to merchantability or fitness for any particular purpose. Any of the manufacturer's software described in this manual is sold or licensed *as is*. Should the programs prove defective following their purchase, the buyer (and not the manufacturer, its distributor, or its dealer), assumes the entire cost of all necessary servicing, repair and any incidental or consequential damages resulting from any defect in the software.

The manufacturer of this system is not responsible for any radio and/or TV interference caused by unauthorized modifications to this device. It is the responsibility of the user to correct such interference.

The manufacturer is not responsible for any damage incurred in the operation of this system if the correct operational voltage setting was not selected prior to operation. PLEASE VERIFY THAT THE VOLTAGE SETTING IS CORRECT BEFORE USE.

Product Information

For information about all ATEN products and how they can help you connect without limits, visit ATEN on the web or contact an ATEN authorized reseller. Visit ATEN on the web for a list of locations and telephone numbers:

International	http://www.aten.com
North America	http://www.aten-usa.com

Package Contents

Check to make sure that all of the components are in working order. If you encounter any problem, please contact your dealer.

SN3001 / SN3002 / SN3401 / SN3402

The standard SN3001 / SN3002 / SN3401 / SN3402 package consists of:

1 Secure Serial Device Server (SN3001 / SN3002 / SN3401 / SN3402)
1 power adapter
1 terminal block
1 foot pad set (4 pcs)
1 DIN rail mount kit
1 user instructions

SN3001P / SN3002P / SN3401P / SN3402P

The standard SN3001P / SN3002P / SN3401P / SN3402P package consists of:

1 Secure Serial Device Server with PoE (SN3001P / SN3002P / SN3401P / SN3402P)
1 terminal block
1 foot pad set (4 pcs)
1 DIN rail mount kit
1 user instructions

Contents

Appendix

About This Manual

This manual is provided to help you get the most out of your Secure Serial Device Server. It covers all aspects of the device, including installation, configuration, and operation.

The Secure Serial Device Server models covered in this user manuals include:

Models	Product Names
SN3001	1-Port RS-232 Secure Serial Device Server
SN3001P	1-Port RS-232 Secure Serial Device Server with PoE
SN3002	2-Port RS-232 Secure Serial Device Server
SN3002P	2-Port RS-232 Secure Serial Device Server with PoE
SN3401	1-Port RS-232/RS-422/RS-485 Secure Serial Device Server
SN3401P	1-Port RS-232/RS-422/RS-485 Secure Serial Device Server with PoE
SN3402	2-Port RS-232/RS-422/RS-485 Secure Serial Device Server
SN3402P	2-Port RS-232/RS-422/RS-485 Secure Serial Device Server with PoE

An overview of the information found in the manual is provided below.

Chapter 1, Introduction

Introduces Secure Serial Device Server. Its purpose, features and benefits are presented, and its front and back panel components are described.

Chapter 2, Hardware Setup

Provides step-by-step instructions for setting up Secure Serial Device Server.

Chapter 3, Network Configuration and Login

Explains how to log into the Secure Serial Device Server from a web browser.

Chapter 4, Port Operating Modes

Introduces the Secure Serial Device Server's operating modes, and explains the purpose of each.

Chapter 5, Port Access

Describes how to access the COM ports of the Secure Serial Device Server and start SNViewer.

Chapter 6, Remote Terminal Operation

Describes how the Secure Serial Device Server can be accessed via remote terminal sessions, such as Telnet, SSH, and PuTTY.

Chapter 7, Serial Network Device Manager

Describes how to configure and manage multiple Secure Serial Device Servers using the utility, *Serial Network Device Manager*.

Chapter 8, User Management

Details login accounts and third-party authentication services supported, such as RADIUS.

Chapter 9, Virtual Serial Port Managers

Shows how to install the virtual COM port driver and to set up and manage the virtual COM port.

Chapter 10, MIB Reference

Defines the MIB objects supported by the Secure Serial Console Servers required for integration with network management systems, automated monitoring, and event handling.

Appendix

Provides technical and troubleshooting information at the end of the manual.

Note:

- Read this manual thoroughly and follow the installation and operation procedures carefully to prevent any damage to the unit or connected devices.
- The product may be updated with features and functions added, improved or removed since the release of this manual. For an up-to-date user manual, visit http://www.aten.com/global/en/

Conventions

This manual uses the following conventions:

Monospaced	Indicates text that you should key in.
[ ]	Indicates keys you should press. For example, [Enter] means to press the **Enter** key. If keys need to be chorded, they appear together in the same bracket with a plus sign between them: [Ctrl+Alt].
1.	Numbered lists represent procedures with sequential steps.
♦	Bullet lists provide information, but do not involve sequential steps.
>	Indicates selecting an option (such as on a menu or dialog box), that comes next. For example, Start > Run means to open the *Start* menu, and then select *Run*.
	Indicates critical information.

Chapter 1
Introduction

Overview

The Secure Serial Device Server provides security-assuring, IP-based LAN connectivity for serial devices and supports a wide range of operation modes. It empowers everyday serial devices — PLCs, meters, and sensors — to be connected to a network, and allowing them to be accessed and managed from anywhere over the network.

Equipped with extensive security features, such as Secure Real COM, Secure TCP Client and Server, Secure Serial Tunneling, UDP, and Secure Console Management, the Secure Serial Device Server is the ideal solution for managing serial device in a wide range of security-critical applications.

Fully compatible with existing serial communication software, the Secure Serial Device Server ensures that your former investments in software development are protected. Software designed to work with COM or TTY ports can access the serial devices connected over a TCP/IP network by utilizing the Secure Serial Device Server's Real COM or TTY drivers. This feature also breaks through the port number and distance limitation barriers encountered with PC hardware.

With SSL and SSH protocol support — for encrypting data transmission — the Secure Serial Device Server ensures secured data transmission over both private and public networks.

Installing the Secure Serial Device Server is fast and easy: plugging cables into their appropriate ports is all that is entailed. It also offers a browser-based GUI, Telnet / SSH console sessions, and a Windows software utility, making configuration and operation swift and smooth.

SN3001P / SN3002P / SN3401P / SN3402P provides PoE function, IEEE 802.3af compliant, thus can be powered through an Ethernet cable, by a PoE switch/adapter, without requiring an additional power supply.

All in all, with its advanced features and ease of operation, the Secure Serial Device Server is the most convenient, reliable, and cost-effective way to remotely manage your serial devices.

Features

Serial-to-Ethernet Connectivity

- 1 or 2 RS-232 serial ports for secured serial data over Ethernet transmission (SN3001 / SN3001P / SN3002 / SN3002P only)
- 1 or 2 RS-232/RS-422/RS-485 serial ports for secured serial data over Ethernet transmission (SN3401 / SN3401P / SN3402 / SN3402P only)
- Supports Modbus gateway to convert between Modbus TCP and Modbus RTU/ASCII protocols (SN3401 / SN3401P / SN3402 / SN3402P only)
- Secured operation modes — Secured Real COM, Secured TCP Server/ Client, Secured Serial Tunneling, Console Management (SSH), and Console Management Direct (SSH)
- Standard operation modes — Real COM, TCP Server/Client, Serial Tunneling, UDP, Console Management (Telnet), and Console Management Direct (Telnet)
- Software configurable termination (120Ω) and pull high/low resistor (1K ohms or 150K ohms) integrated to the RS-485 mode to avoid signal reflection (SN3401 / SN3401P / SN3402 / SN3402P only)
- Real COM, Real TTY, and Fixed TTY drivers for Windows, Linux, and UNIX
- Convenient console management access via Java viewer (SSH/Telnet) or third-party clients such as PuTTY
- Easy console port access via Java viewer and Sun Solaris ready (“break-free”)
- Multiple users can simultaneously access the same port — up to 16 connections per port

Hardware

- Redundant power input (power jack and terminal block) for fail-safe power
- IEEE 802.3af-compliant PoE power device equipment (SN3001P / SN3002P / SN3401P / SN3402P only)
- Surge protection for serial, Ethernet, and power
- Wall and DIN-rail mounting, rack mounting (optional kit VE-RMK1U required), and desktop installation available

- Supports baud rates of 110, 134, 150, 300, 600, 1200, 1800, 2400, 4800, 7200, 9600, 19200, 38400, 57600, 115200, 230.4k, 460.8k, 921.6k bps

Security

- Supports secured login from browsers with TLS 1.2 data encryption and RSA 2048-bit certificates
- Configurable user permissions for port access and control
- Local and remote authentication and login
- Third-party authentication (e.g. RADIUS)
- IP address filter for security protection

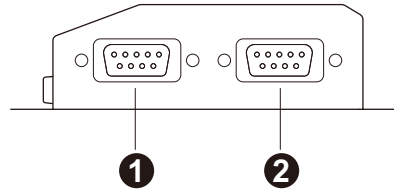
System Management

- Browser access with an intuitive GUI
- Web-based quick setup wizard for fast configuration
- Terminal-based access with a menu-driven UI via Telnet / SSH
- Online / offline detection of connected RS-232 serial devices (including terminal blocks) — automatically send event notifications when the devices are offline (e.g. power failure) for device status monitoring
- System event logs will be saved to internal memory or Syslog server
- Port logs will be saved to internal memory or Syslog server
- SNMP agent (v1/v2c)
- Event notification — supports notification of SMTP email and SNMP trap (v1/v2c)
- Backup / restore system configuration and upgradable firmware
- 64 KB port buffer prevents data loss when the network is down
- NTP for time server synchronization
- Multi-language web-based GUI

Hardware Overview

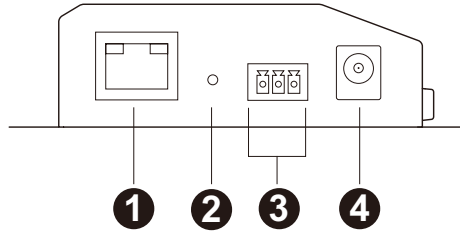
SN3001 / SN3001P / SN3002 / SN3002P

Front View



No.	Component	Description
1	RS-232 serial port 1	Connects to an RS-232 serial device.
2	RS-232 serial port 2	Connects to a second RS-232 serial device. (SN3002 / SN3002P only)

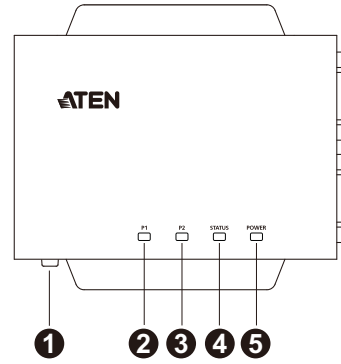
Rear View



No.	Component	Description
1	LAN port	Connects the Secure Serial Device Server to the network. For SN3001P / SN3002P (PoE 802.3af compliant), it can be simultaneously supplied power through a PoE switch.
2	reset button	Pressing and holding for less than three seconds performs a system restart. Pressing and holding for more than three seconds returns its settings (excluding user account settings and privileges) to their default status.
3	power terminal	Connects the Secure Serial Device Server to power via DC electric leads and the terminal block provided.

4	power jack	Connects the Secure Serial Device Server to power using a power adapter.

Top View

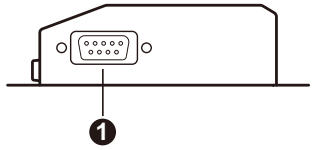


No.	Component	Description
1	grounding terminal	Grounds the unit by connecting to a suitable grounded object using a grounding wire.
2	serial port 1 LED	Lights green or orange when data is being sent or received via the unit's RS-232 serial port 1.
3	serial port 2 LED	Lights green or orange when data is being sent or received via the unit's RS-232 serial port 2. (SN3002 / SN3002P only)
4	status LED	Lights or blinks yellow/green respectively for normal operation or startup, and lights red when an error (i.e. hardware failure and DHCP irregularity) occurs.
5	power LED	Lights green when the Secure Serial Device Server is powered and ready.

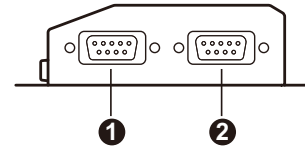
SN3401 / SN3401P / SN3402 / SN3402P

Front View

SN3401 / SN3401P



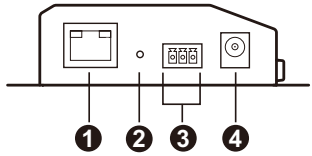
SN3402 / SN3402P



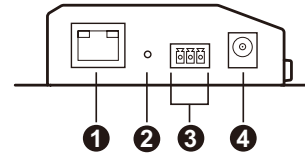
No.	Component	Description
1	serial port 1	Connects to an RS-232 / RS-422 / RS-485 serial device.
2	serial port 2	Connects to a second RS-232 / RS-422 / RS-485 serial device. (SN3402 / SN3402P only)

Rear View

SN3401 / SN3401P



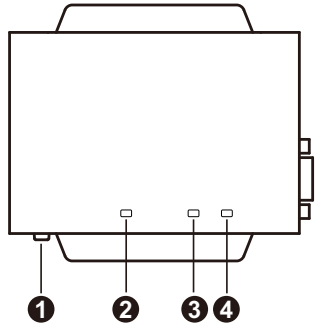
SN3402 / SN3402P



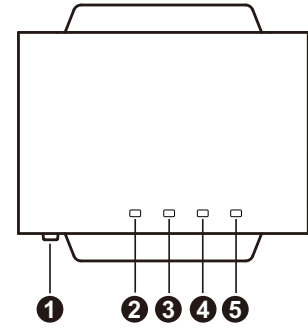
No.	Component	Description
1	LAN port	Connects the Secure Serial Device Server to the network. For SN3401P / SN3402P (PoE 802.3af compliant), it can be simultaneously supplied power through a PoE switch.
2	reset button	Pressing and holding for less than three seconds performs a system restart. Pressing and holding for more than three seconds returns its settings (excluding user account settings and privileges) to their default status.
3	power terminal	Connects the Secure Serial Device Server to power via DC electric leads and the terminal block provided.
4	power jack	Connects the Secure Serial Device Server to power using a power adapter.

Top View

SN3401 / SN3401P



SN3402 / SN3402P



No.	Component	Description
1	grounding terminal	Grounds the unit by connecting to a suitable grounded object using a grounding wire.
2	serial port 1 LED	Lights green or orange when data is being sent or received via the unit's serial port 1.
3	serial port 2 LED	Lights green or orange when data is being sent or received via the unit's serial port 2. (SN3402 / SN3402P only)
4	status LED	Lights or blinks yellow/green respectively for normal operation or startup, and lights red when an error (i.e. hardware failure and DHCP irregularity) occurs.
5	power LED	Lights green when the Secure Serial Device Server is powered and ready.

This Page Intentionally Left Blank

Chapter 2
Hardware Setup

Before you Begin

1. Important safety information regarding the placement of this device is provided on page 95. Please review it before proceeding.
2. Make sure the power of all devices to be connected have been turned off.
3. Please operate the device with caution when under high environment temperatures, as the surface of the device may become overheated under such conditions. For instance, the surface temperature of the device may reach 70 °C (158 °F) or higher when the environmental temperature reaches close to 50 °C (122 °F).

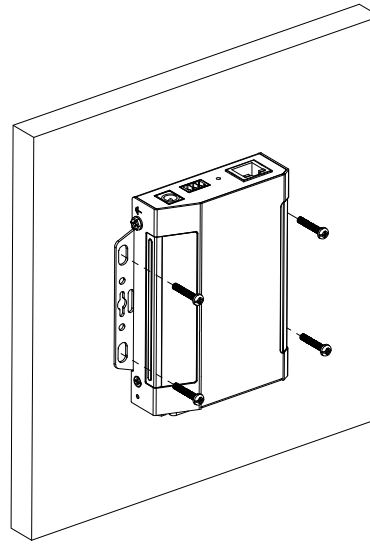
Placement Options

For flexibility and convenience, Secure Serial Device Server can be mounted onto a wall or DIN rail, as described below.

Wall Mount

To wall mount the Secure Serial Device Server, doe the following:

Using 4 self-supplied screws, users can mount the unit onto a wall via the screw holes at its sides, as shown below.

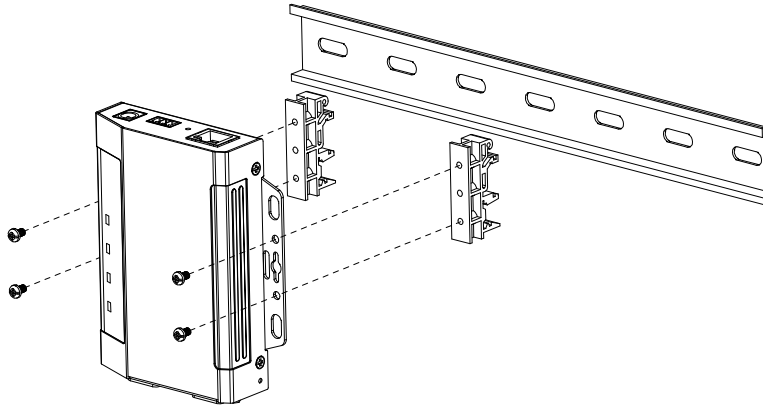


DIN Rail Mount

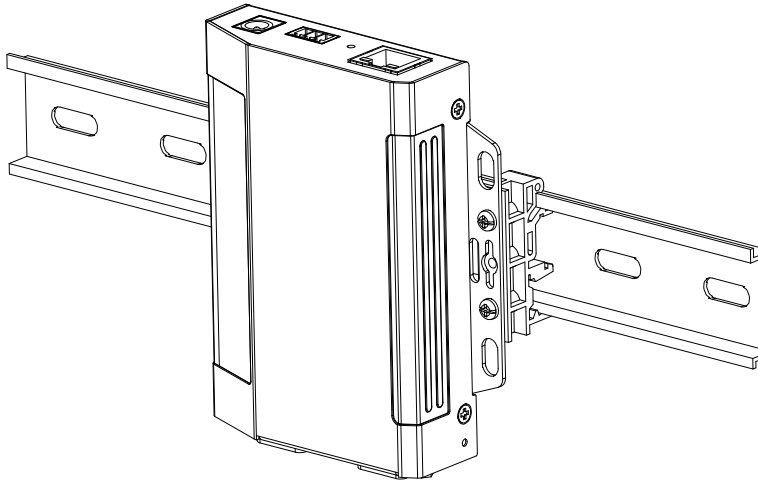
Use the DIN rail mount kit included to mount the Secure Serial Device Server onto a DIN rail, as instructed below:

Parallel DIN Rail Mount

1. To mount the unit parallel to the DIN rail, attach 2 DIN rail mount brackets onto the unit with the 4 screws provided, via its center screw holes.

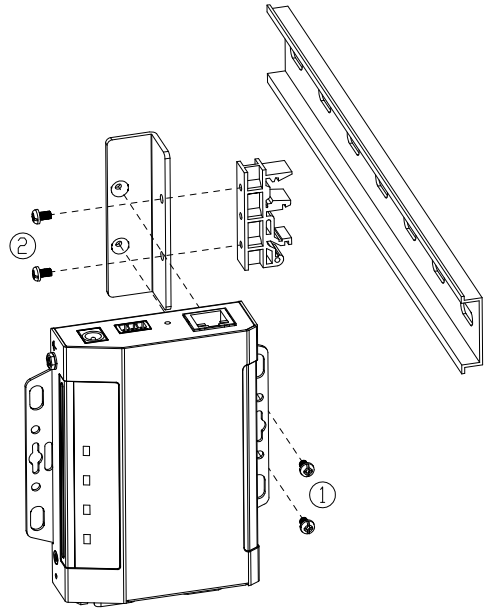


2. Hang the unit onto the DIN rail.

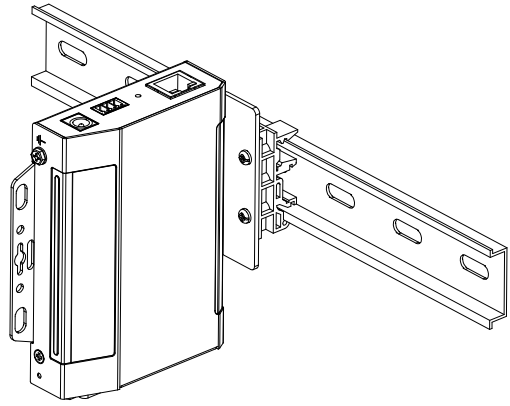


Perpendicular DIN Rail Mount

1. Attach the L-shape mounting bracket onto the unit with 2 M3x6 screws, via its center screw holes at the side opposite to its grounding terminal.
2. Using 2 of the 4 screws enclosed, attach 1 DIN rail mount bracket onto the side of the L-shape mounting bracket.



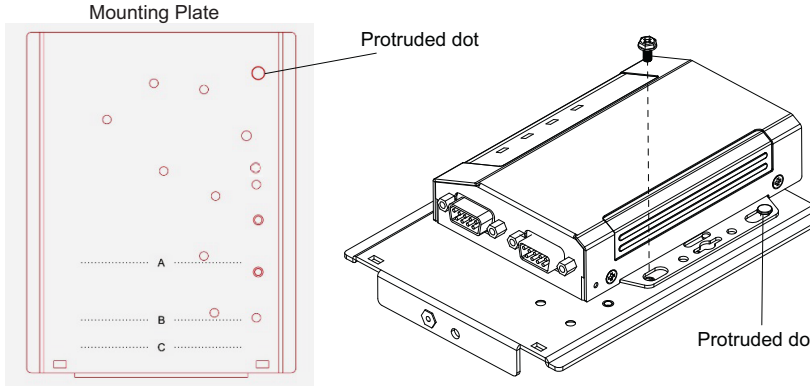
3. Hang the unit onto the DIN rail.



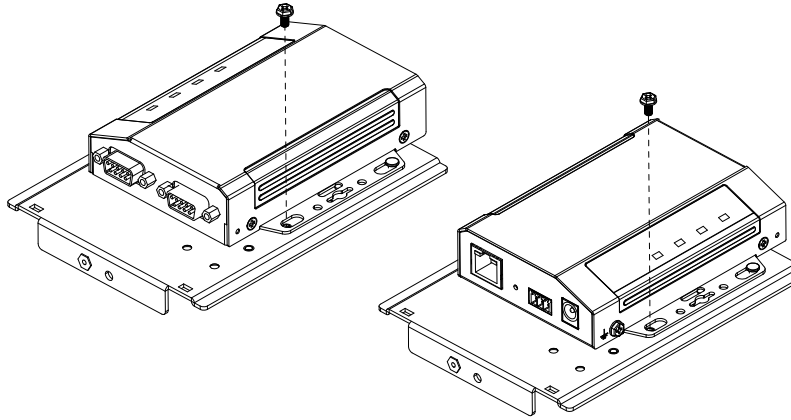
Rack Mount

The Rack Mount Kit (VE-RMK1U) is required for mounting the Secure Serial Device Server onto a rack, as instructed below:

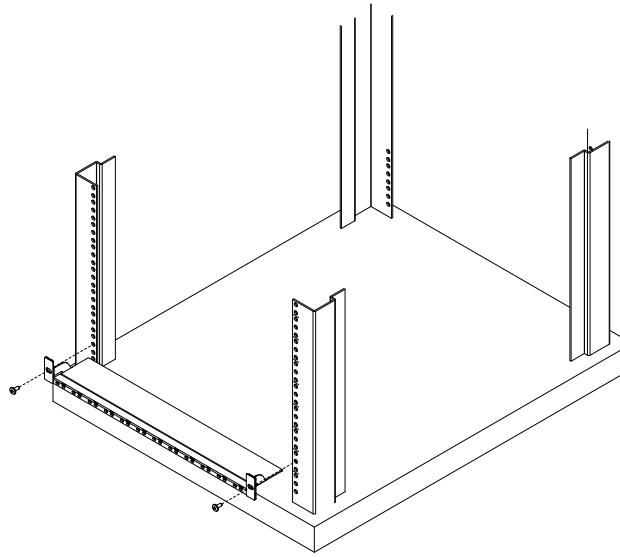
1. Place the device onto the mounting plate while latching one of its rack ears onto the plate's protruded dot, as illustrated below.



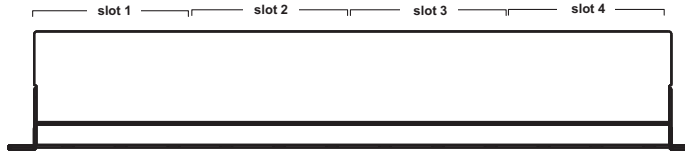
2. Secure the device to the mounting plate using the hexagon head screw supplied. Users can secure the Secure Serial Device Server either with its serial port(s) facing inward or outward.



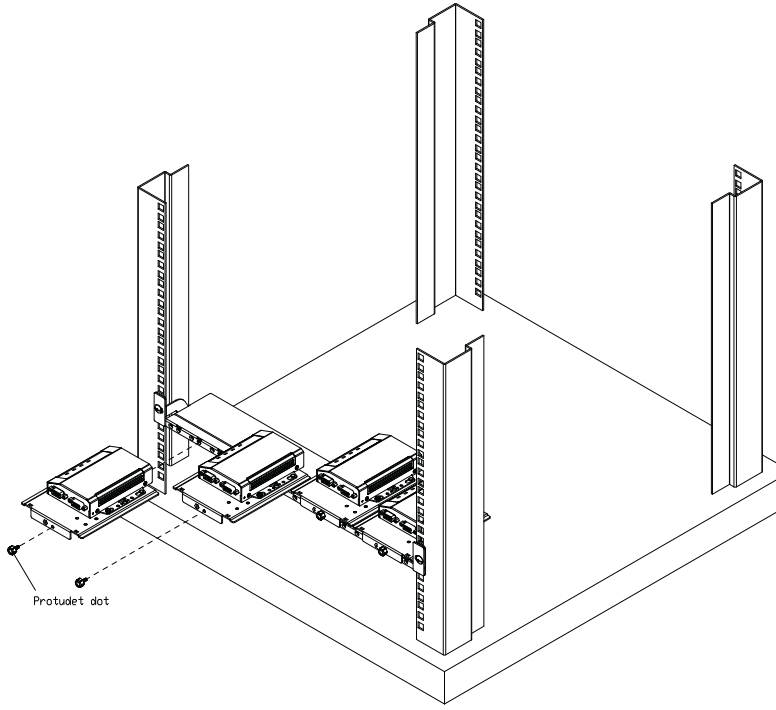
3. Position and align the holes on the VE-RMK1U frame with that of the rack, and secure the frame onto the rack with 2 self-supplied screws, as illustrated below.



4. Align the device and mounting plate assembly to one of the slots on the VE-RMK1U frame, and then secure the mounting plate to the frame with the plastic captive screw provided.



VE-RMK1U Frame

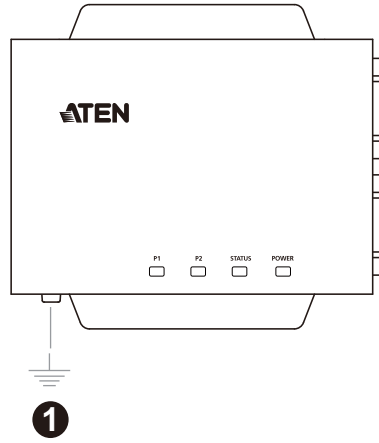


Note: Up to 4 Secure Serial Device Servers can be secured onto a VE-RMK1U frame.

Installation

To install the Secure Serial Device Server, follow the steps below and refer to the diagram on the following page (the number labels correspond to the installation steps).

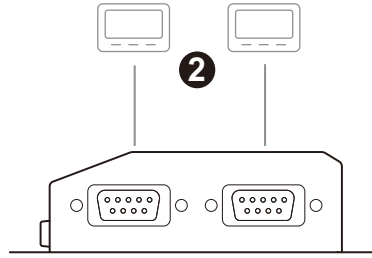
1. Use a grounding wire to ground the unit by connecting one end of the grounding terminal and the other end to a suitable grounded object.



Note: Do not omit this step. Proper grounding helps prevent damage to the unit from power surges and static electricity.

2. Connect the unit's serial port(s) to one or up to two serial device(s).

Note: The SN3001 / SN3001P / SN3002 / SN3002P supports RS-232 connections and SN3401 / SN3401P / SN3402 / SN3402P supports RS-232 / RS-422 / RS-485 connections.



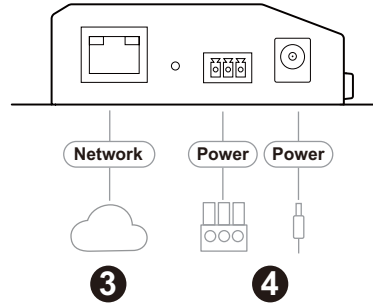
3. Connect the unit's LAN port to the network using a Cat 5e/6 cable. For SN3001P / SN3002P / SN3401P / SN3402P (PoE 802.3af compliant), users can simultaneously supply power to the unit through a PoE switch and skip 4.

4. Connect the unit to power, thereby turning it on, by doing one, or both of the following for power redundancy:

   - Plug the power adapter provided (not included for SN3001P / SN3002P / SN3401P / SN3402P) into an AC power source, and plug its cable into the unit's power jack.

     Note: The temperature tolerance of the power adapter is 0 – 40 °C. If your environment temperature is 40 – 60 °C, you can only power the device via the power terminal.

   - Connect DC + and - wires (DC 9 – 48 V) to the unit's power terminal with the terminal block provided.



5. After supplying power, wait for about 50 seconds for the Secure Serial Device Server to be ready and lights its status LED in constant green.

Note: When more than one power supply is connected, the additional power connections maintain operation when the other is interrupted. For example, if you have the device connected to power via both its power jack and power terminal, the power terminal maintains operation when the power from the power jack fails, and vice versa.

Serial Port Pin Assignments

The pin assignments of Secure Serial Device Server's serial ports are provided below:

Pin	Configuration		
	RS-232	RS-422 RS-485 (4 wires)	RS-485 (2 wires)
1	DCD	RxD - (A)	-
2	RxD	RxD + (B)	-
3	TxD	TxD + (B)	Data + (B)
4	DTR	TxD - (A)	Data - (A)
5	GND	GND	GND
6	DSR	-	-
7	RTS	-	-
8	CTS	-	-
9	-	-	-

This Page Intentionally Left Blank

Chapter 3
Network Configuration and Login

IP Address Determination

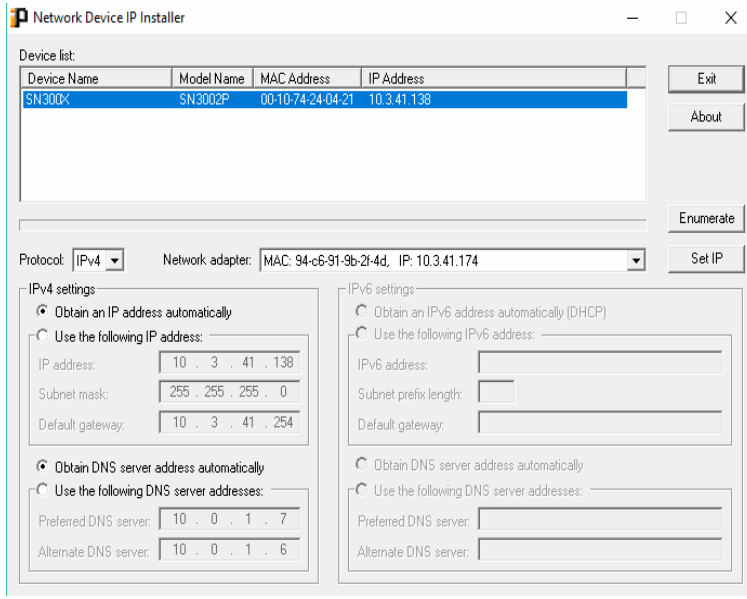
Before you start, make sure the PC you're using is within the same LAN as the Secure Serial Device Server.

There are two methods for determining / setting the IP address of your Secure Serial Device Server, one through the IP Installer Utility on a Windows PC, and one just using a PC (only applicable to non-DHCP network), as described below:

IP Installer Utility

Using a Windows PC, users can search for Secure Serial Device Server's IP address or assign an IP address to it, in a DHCP or non-DHCP network, with the **IP Installer Utility**.

1. Download **IP Installer** zip file under the *Support and Downloads* tab from the product web page.
2. Extract and execute *IPInstaller.exe*. A dialog box similar to the one below appears.



3. :Select the Secure Serial Device Server in the *Device List*.

Note: 1. If the list is empty, or your device doesn't appear, double-check that you have the correct network adapter selected and click **Enumerate** to refresh the Device List.

2. If there is more than one device in the list, use the MAC address to distinguish your device. The Secure Serial Device Server's MAC address is located on its bottom panel.

4. To check the IP address of the Secure Serial Device Server or set an IP address for it, respectively select **Obtain an IP address automatically** or **Use the following IP address**.
   - For setting an IP address, fill in the required IP address, subnet mask and gateway information according to your network environment.
5. Click **Set IP**. The IP address of the Secure Serial Device Server is displayed in the *Device List*.
6. Click **Exit** to close the program.

Without IP Installer (non-DHCP only)

On a non-Windows system, under non-DHCP network, users can assign a static IP address to the Secure Serial Device Server, different from its default of *192.168.0.60*, by following the steps below.

1. Set your PC's IP address to 192.168.0.*XXX*, where *XXX* can be any number except for 10.
2. Type the device's default IP address — *192.168.0.60* — in your browser's URL location bar.
3. Log in with a valid username and password (see page 23).
4. On the Secure Serial Device Server's web interface, assign a fixed IP address for it according to your network environment.
5. Save the settings and log out. After you log out, make sure to reset your PC's IP address to its original value.

Logging In

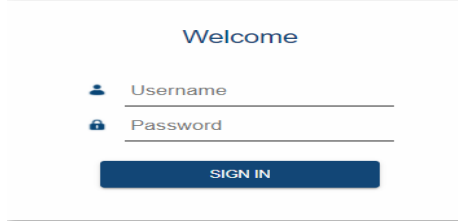
To access Secure Serial Device Server from a web browser, do the following:

1. Open your browser and specify the IP address of the Secure Serial Device Server you want to access in the browser's URL location bar.

   Note: If you are the administrator, and are logging in for the first time, the various ways to determine the Secure Serial Device Server's IP address are described in *IP Address Determination* (see page 21).

2. If a *Security Alert* dialog box appears, accept the certificate — it can be trusted (see *Security Certificate*, page 48, for details). If a second certificate appears, accept it as well.

3. On the login page that appears, provide a valid **username and password** to log in. The default **Username** and **Password** are *administrator* and *password*, respectively.



4. Once successfully logged in, the main screen of the Secure Serial Device Server appears. Upon first-time login, users are required to change the login password of the Secure Serial Device Server.

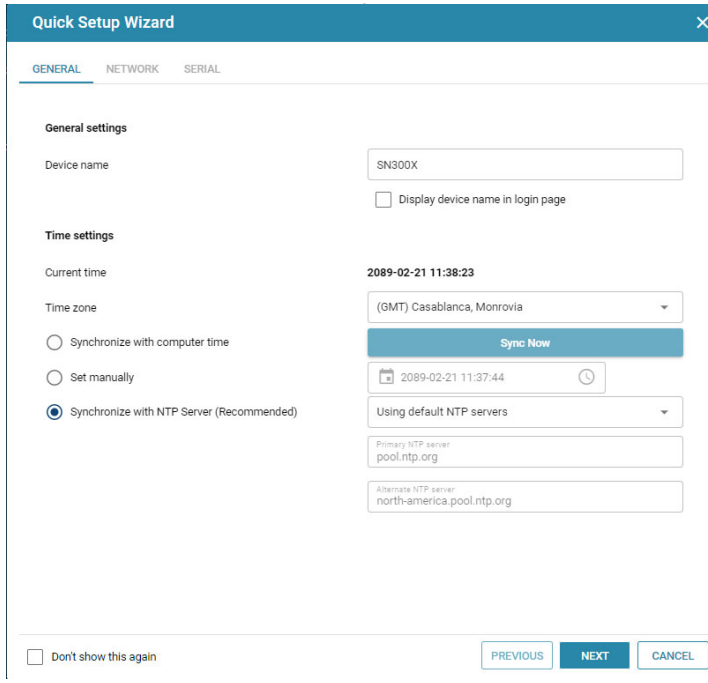
5. Upon first-time login, users are required to change the login password of the Secure Serial Device Server.

6. Once logged in, the *Quick Setup Wizard* is displayed, which takes you through the basic settings of the Secure Serial Device Server.

Quick Setup Wizard

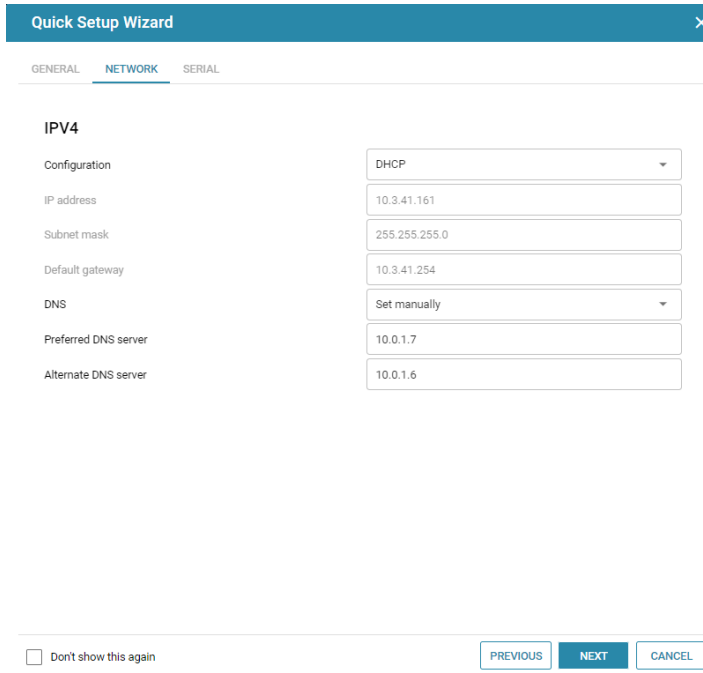
The *Quick Setup Wizard* gets you started with the basic settings of the Secure Serial Device Server.

General



Item	Description
Device name	Displays the name of the Secure Serial Device Server. Change the device name if needed.
Current time	Displays the current time of the device.
Time settings	Sets the time settings of the device. For details, refer to *Time*, page 41.

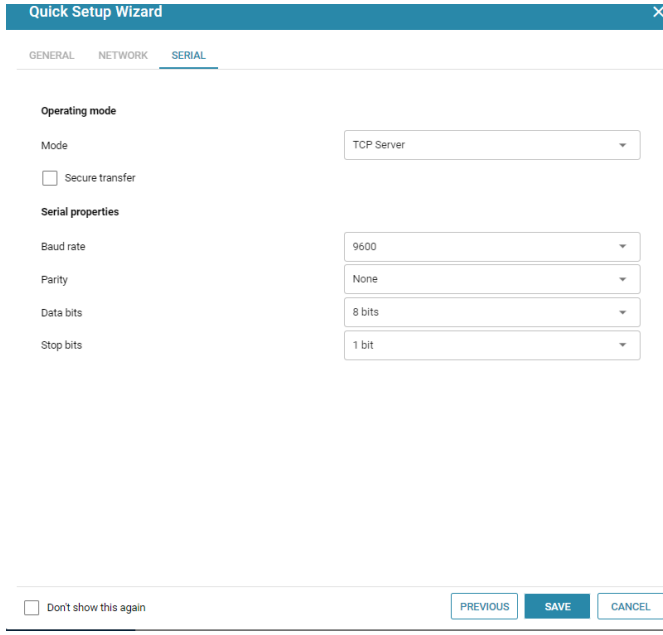
Network



The Network tab sets the network settings of the Secure Serial Device Server. For details, refer to *Network*, page 37.

Serial

Note: Settings on the **Serial** tab applies to all serial ports of the Secure Serial Device Server.



Item	Description
Mode	Selects the operation mode for the Secure Serial Device Server's serial port(s). See *Port Operating Modes*.
Secure transfer	Check for secured data transmission.
Baud rate	Selects the serial ports' data transfer speed.
Parity	Selects to check the integrity of the data transmitted, which shall match the parity setting of the serial device(s) connected
Data bits	Selects the number of bits used to transmit one character of data, and matching the data bit setting of the serial device(s) connected.
Stop bits	Selects the stopping bit, indicating a character has been transmitted, and matching the stop bit setting of the serial device(s) connected.

Click **Save** for the settings to take effect.The Secure Serial Device Server's web console main screen is displayed. See *Web Console* for details.

Chapter 4
Port Operating Modes

Overview

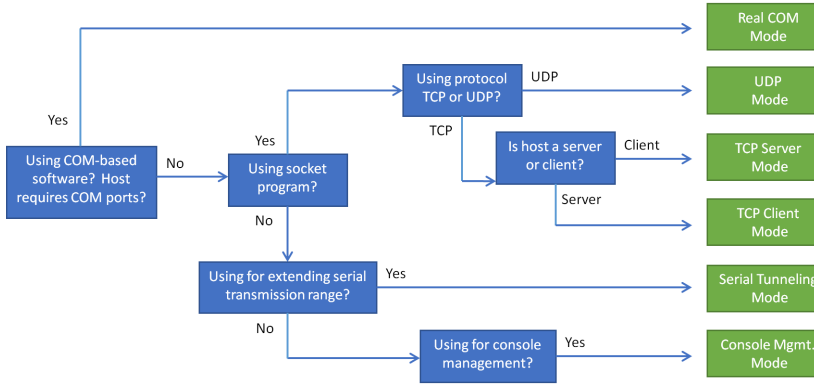
To cover a broad range of serial applications, the Secure Serial Device Server's COM port supports several port operating modes.

These include *Real COM, TCP Server & Client*, *UDP*, *Serial Tunneling Server & Client,* and *Modbus Gateway* modes for serial-to-Ethernet connectivity, *Console Management*, and *Console Management Direct* for device control, as well as applications that require COM ports, serial tunneling, or where TCP/UDP socket functionality is needed.

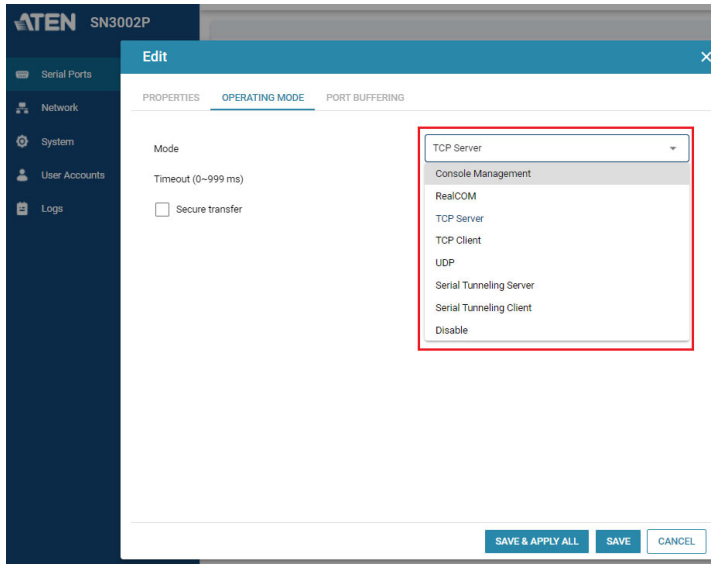
Note: The maximum number of simultaneous connections to any one serial port is 16.

Selecting Operating Mode

The following are some of the questions to consider when selecting the operating mode.



The **Operating Mode** is selectable from Serial Ports > Edit > Operating Mode, as shown below.



From this page, users can set the serial ports of the Secure Serial Device Server to the various Port Operating modes available, as explained below

Operating Mode

To configure the serial ports' operating mode, see *Operating Mode*, page 30.

Real COM

This mode is used in conjunction with a virtual COM port driver installed on a remote PC. (See Chapter 9, *Virtual Serial Port Manager*) When the Secure Serial Device Server's COM port is set to this mode, the device connected appears as if it were directly connected to a COM port on the remote PC.

This mode is useful with devices such POS terminals, bar code readers, serial printers, etc. since it allows users to use software that was written for pure serial communication applications.

The Secure Serial Device Server comes with Real COM drivers for Windows systems (Virtual Serial Port Utility) and TTY drivers for Linux systems.

TCP Server & Client

TCP (Transmission Control Protocol) provides a reliable transport layer for transmitting serial data over the TCP protocol via socket programming.

TCP Server

In *TCP Server* mode, data transmission is bidirectional. In this mode, the host computer initiates contact with the Secure Serial Device Server and requests a connection to its serial port.

Once the connection is established, the host receives data from the serial device. From this point on, data can be transmitted between the host and the device in both directions. SSL data encryption is supported in this operating mode.

The Secure Serial Device Server supports simultaneous connections from up to 16 host computers in this mode, allowing multiple computers to communicate with the serial device at the same time.

Note: Be sure that the *Base socket* entry specified on the *General Settings* page corresponds to the port that the device listens on. 5001 is the Secure Serial Device Server's default setting. (See *General*, page 39.)

TCP Client

In *TCP Client* mode, when serial data comes into the serial port, the Secure Serial Device Server initiates contact with the host computer and begins sending serial data to the to the host. The Secure Serial Device Server can send data to up to 16 host computers simultaneously, and supports SSL data encryption in this operating mode.

For configuring the serial port's operating mode, see *Operating Mode*, page 30.

Serial Tunneling Server & Client

Serial Tunneling involves establishing a direct connection between two Secure Serial Device Servers over Ethernet, working in a *Client-Server* relationship. One unit is designated as the *Serial Tunneling Client*, while the other designated as the *Serial Tunneling Server*.

Note: In this configuration, it doesn't matter which is designated as the Client and/or Server.

The COM port of one of the two units connects to the COM port of a computer, while the COM port of the other unit connects to the serial device to be accessed.

The two units then communicate with each other via their IP and port addresses, and supports SSL data encryption. The port address is set by the *Base socket* entry on the *General Settings* page. See *General*, page 39, for details.

UDP Mode

UDP (User Datagram Protocol) *Mode* is faster and more efficient at communications than TCP. In UDP mode, communications are bilateral. A serial device can send data to, and receive data from, up to 16 host computers via the Secure Serial Device Server's COM port.

Because it doesn't perform error checking in the thorough way that TCP does, UDP is more suitable for real time applications (such as message display) than the slower TCP, which is optimized for data accuracy.

Console Management

Console Management allows users to establish Telnet and/or SSH sessions to the Secure Serial Device Server for managing and controlling the serial devices connected. Users can log in using Java SNViwer application via *Telnet* or *SSH*, or remotely via Telnet, SSH, or PuTTY.

Note: 1. Be sure that the *Base socket* entry specified on the *General Settings* page corresponds to the port that the device listens on. 5001 is the Secure Serial Device Server's default setting (see *General*, page 39).

2. In this mode, the Secure Serial Device Server can also be connected to a Cisco Network Switch using the Cisco console cable (DB-9 to RJ-45).

Console Management Direct

When the **Direct** option under *Console Management* mode is enabled, users can establish a Telnet or SSH session directly from a PC to a serial device connected to the Secure Serial Device Server without requiring to log in via a web browser. Users can log in to a connected serial device using *Telnet*, *SSH*, or *PuTTY* directly from a PC. For configuring the serial port's operating mode, see *Operating Mode*, page 30.

Disable

In this mode, the serial port of the Secure Serial Device Server is disabled.

For configuring the serial port's operating mode, see *Operating Mode*, page 30.

Modbus Gateway

For SN3401 / SN3401P / SN3402 / SN3402P to function as a gateway that converts data between Modbus TCP and Modbus RTU/ASCII protocols, configure the operation mode to Modbus master or Modbus slave.

Typical applications

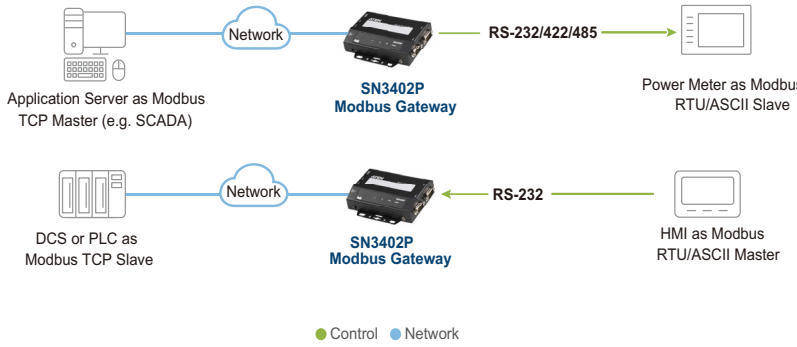
- **An Ethernet Client with Multiple Serial Slaves**

  When you have a TCP client (e.g. SCADA system) with multiple serial slaves, you can set up an SN3401 / SN3401P / SN3402 / SN3402P as a Modbus slave, which supports communication from up to 31 slave devices at the same time.

- A Serial Master with Multiple Ethernet Servers

  When you have a serial master device, for example, an HMI (Human Machine Interface) system with multiple TCP servers, you can set up an

SN3401 / SN3401P / SN3402 / SN3402P as a Modbus master, which supports communication from up to 32 servers at the same time.



This Page Intentionally Left Blank

Chapter 5
Port Access

Overview

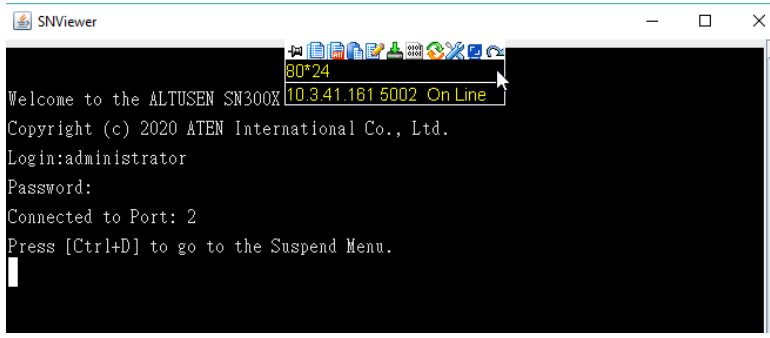
Upon login of the Secure Serial Device Server's web interface, the **Serial Ports** page appears. Use the buttons, described below, to access and control the device's serial COM ports.

Button	Function
EDIT	Edits the serial port's settings. See *Editing Serial Ports*, page 27.
TELNET	Opens a Telnet session with the Secure Serial Device Server using *SNViewer* to access either its configuration menu, or a serial device connect to its COM port. See *Telnet / SSH*, page 36, for details.
SSH	Opens an SSH session with the Secure Serial Device Server using *SNViewer* to access either its configuration menu, or a serial device connect to its COM port. See *Telnet / SSH*, page 36, for details.
DUMP BUFFER	Downloads the port activity logs (up to 128 KB) of the serial port as a *log.txt* file. See *Port Buffering*, *page 28*.

Note: Buttons are only active for the functions that the user is authorized to perform.

Telnet / SSH

To access the Secure Serial Device Server's configuration menu, or a serial device connected to its COM port via Telnet or SSH, click the **Telnet** or **SSH** button on the *Serial Ports* page. A Java application — *SNViewer* — appears and opens a *Telnet* / *SSH* session, as exemplified below.



Note: 1. JRE 8 must be installed to run SNViewer.

2. In order for the Telnet / SSH buttons to appear, the Secure Serial Device Server's COM port must be set to *Console Management* mode (see *Operating Mode*, page 30).

SNViewer

The *SNViewer* is a Java application used to access serial devices connected to the Secure Serial Device Server on the web via Telnet / SSH protocol.

Moving the mouse cursor over the *SNViewer* brings up its control panel, which consists of three rows: an icon row and two text rows.

- By default, the upper text row shows the width and height of the window. As the mouse cursor moves over the icons in the control panel, the information in the upper text row changes to indicate the icon's function.
- The lower row shows the IP address and port of the device you are accessing, along with the current connection status.

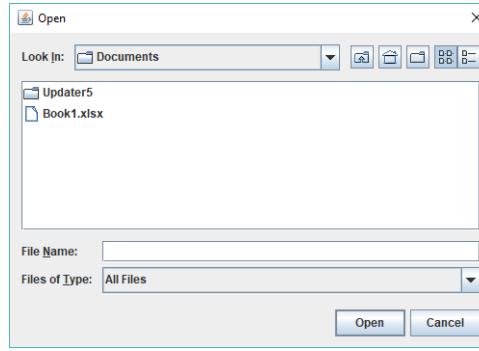
Control Panel Functions

The Control Panel functions are described in the table below and the sections that follow.

Icon	Function
	Pins / unpins the Control Panel to appear *Always On Top* or *Auto Hide* mode.
	Copies the selected text on the screen.
	Copies all text displayed on the screen.
	Pastes the copied text.
	Toggles *Logging on / Logging off*. This starts a log file of characters sent from the serial device to the SNViewer. You must first create and import a text-based log file (see *Logs*, page 53).
	Browses for data files to import (see *Data Import*, page 38).
	Changes the page encoding (see *Encode*, page 38).
	Resets the terminal to its default settings.
	Changes the font, color and other display settings of the SNViewer (see *Terminal Settings*, page 38).
	Adjusts the width of the SNViewer window.
	Exits the viewer.

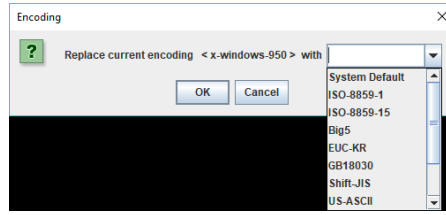
Data Import

The *Data Import* option opens a standard browse menu to import data files, as shown below.



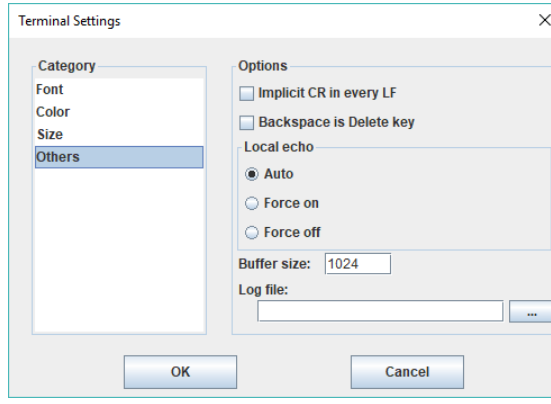
Encode

The *Encode* option selects the type of encoding to be used, as illustrated below.



Terminal Settings

The Terminal Settings option allows users to change the display parameters and settings of the terminal session, as described below.



Category	Description
Font	Configures the SNViewer's font settings, including the font type, size, and style. An example of the setting is displayed on the right.
Color	Changes the *Foreground*, *Background*, *Cursor Text*, and/or *Cursor* colors. Use the *HSL*, *Swatches*, and *HSV* tabs to make detailed adjustments and select the colors. Below the tab is a **Preview** of how the color changes will look like. Click **OK** to save the changes; **Cancel** to remove the changes and exit; or **Reset** to revert to default color settings.
Size	The size of the window determines the amount of information displayed. Change the SNViewer's window size by configuring the *Column* and *Row* sizes.
Others	Use this section to set the following: ◆ *Implicit CR in every LF*: Checking this box adds an extra Carriage Return when the [Enter] key is used, so the cursor returns aligned on the left margin. Use this function if the text is not lining up on the left margin after you hit [Enter]. ◆ *Backspace is Delete Key* ◆ *Local echo*: An echo is a response from the serial device of character(s) that have been inputted. ◆ **Auto**: Characters that are typed in are echoed but not displayed on the screen. ◆ **Force On**: Characters that are typed in are echoed and displayed on the screen as they are entered. *Passwords are displayed when enabled.* ◆ **Force Off**: Characters are not echoed from the serial device. ◆ *Buffer Size*: This is the maximum size of the Log file. ◆ *Log File*: The log file generates a log of characters sent from the connected serial device to the SNViewer. The log must first be created as a text file using an external editor such as Note or Microsoft Word, then opened here. Next, you must enable *Logging on* from the SNViewer Control Panel (see *Control Panel Functions*, page 37).

This Page Intentionally Left Blank

Chapter 6
Remote Terminal Operation

Overview

The Secure Serial Device Server can be accessed via remote terminal sessions via several methods, including Telnet, SSH, or PuTTY, as described in the sections that follow.

Terminal Login

Aside from using a web browser, users can also log in remotely using a text-based terminal application, such as Telnet, SSH, or PuTTY.

Telnet Login

Start a terminal (command line) session and type the IP address of the Secure Serial Device Server in the following format:

```
telnet [IP Address]
```

Press [**Enter**]

Note: The default telnet port is 23. To control a device connected to the Secure Serial Device Server's COM port — rather than opening its main menu — specify the port number as set by the *Base socket* entry in General Settings (see *General Settings*, page 39).For example: **`telnet 192.168.0.60`***`5001`*

A login prompt appears:

For first-time login, type the default username — *administrator*, press [Enter], then type the default password — *password*, and press [Enter] again to log in.

SSH Login (Linux)

Start a terminal (command line) session and type the IP address of the Secure Serial Device Server in the following format:

```
ssh [username@IP Address]
```

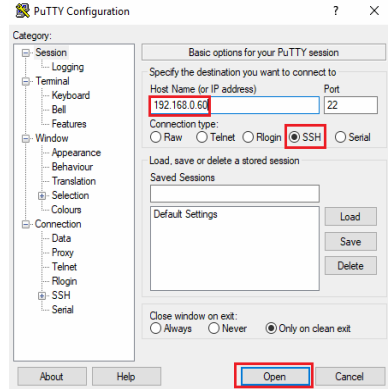
Press [**Enter**] then enter the password of the Secure Serial Device Server to log in.

Note: The default SSH port is 22. To control a device connected to the Secure Serial Device Server's COM port — rather than opening its main menu — specify the port number that was sby the *Base socket* entry in General Settings (see *General Settings*, page 39). For example: **`ssh administrator@192.168.0.60-`***`P5001`*.

Third-party Utility (Windows)

SSH sessions can also be accessed on Windows with the use of third-party utilities, such as PuTTY — a free implementation of Telnet and SSH for Win32 and Unix platforms. To make an SSH connection via PuTTY, do the following:

1. Under *Host Name*, enter IP address of the Secure Serial Device Server.

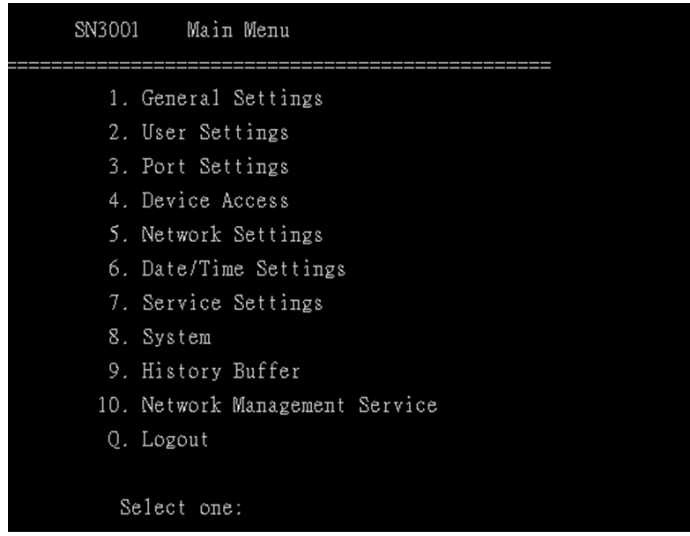


2. Select **SSH** under *Protocol* and click **Open**.
3. Once connected, provide a valid username and password to log in to the Secure Serial Device Server.

Note: If the login fails, the SSH protocol doesn't allow you to try again. You must close the PuTTY and start over.

Terminal Main Menu

Once logged in, the following text-based main menu appears.



The terminal session main menus contain text-based configurations similar to that of the web browser previously described, but with a few limitations, such as unable to perform firmware upgrade and setting backup & restore.

Users can refer to the information provided in the browser version (see *Web Console*, page 25) while working through the submenus.

Note: As with the browser version, access to many of these submenus are restricted to the administrator or users with COM port access permissions. If you select a submenu that you are not authorized for, nothing will happen.

Users can access the serial devices connected to the Secure Serial Device Server via *4. Device Access*.

Note: To access a connected serial device, the Operating Mode of the serial port must be set to *Console Management* (see *Operating Mode*, page 30).

To close the terminal session, bring up the Main Menu and press [**Q**] to log out. Then close the window.

This Page Intentionally Left Blank

Chapter 7
Serial Network Device Manager

Overview

To help manage your Secure Serial Device Server installation more conveniently and efficiently, a Windows-based configuration and management utility — **Serial Network Device Manager** — can be found on the product page. This chapter describes the features provided by the utility.

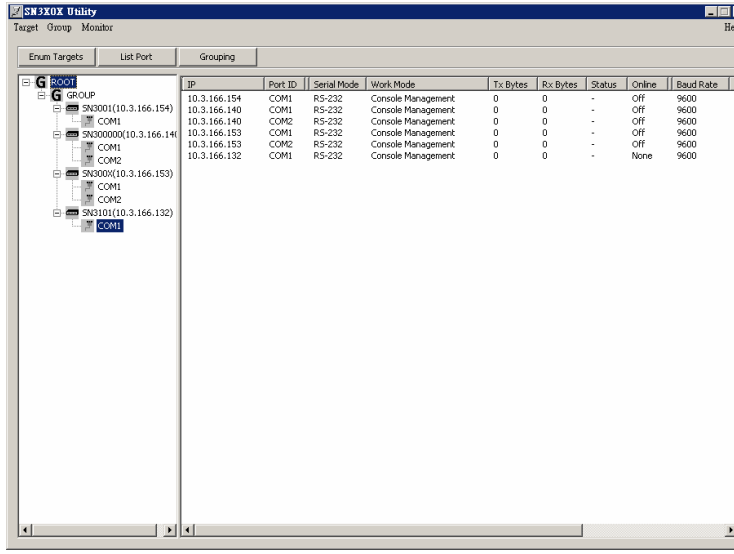
Note: The Serial Network Device Manager does not support Windows versions prior to Windows 2000.

Installation

The Serial Network Device Manager gets installed when you install the virtual COM port driver (see *Virtual Serial Port Manager*, page 59).

Operation

Start **Serial Network Device Manager** (*Start > Virtual Port Management Utility > Serial Network Device Manager*). the following dialog box appears.



Interface Layout

The Serial Network Device Manager interface is laid out as follows:

- A menu bar at the top that allows you to view and manage your SN devices.
- A button bar below the menu bar that allows you to view and manage your SN devices.
- Below the button bar, the screen is divided into two panels:
  - When the program runs, it searches and lists (enumerates) all SN target devices found in a tree view in the left panel.
  - If you select a port and click the *List Port* button, information about the port appears in the right panel.

The Menu Bar

The Menu Bar contains five items, with each discussed in the sections below:

Target

After you select a device or device group from the list in the left panel, this menu offers dialog boxes for viewing and configuring their properties. The configuration choices are similar to the ones discussed in the *Web Console* and *Port Operating Modes* chapters, as shown in the table below.

Item	Action
System Info	Lists all the settings that have been configured for the device..
General Settings	This is similar to the browser-based page. See *General*, page 34.
Network Settings	This is similar to the browser-based page. See *Network*, page 25.
ANMS Settings	This is similar to the browser-based Notification page. See *Notification*, page 37.
Log	This is similar to the browser-based page. See *Logs*, page 47.
Backup/Restore	This is similar to the browser-based page. See *Backup & Restore*, page 45.
Firmware Upgrade	This is similar to the browser-based page. See *Firmware Update*, page 44.
Serial Tunnel	Select this item to build a Serial Tunnel connection between two Secure Serial Device Server units. See *Serial Tunneling Server & Client*, page 30, for more information on Serial Tunneling.

Group

This function allows users to configure and manage a number of Secure Serial Device Server devices at the same time by assigning them to groups. To configure the settings for a group, select it from the list in the left panel. The changes made (described below), affect all members of the selected group.

Item	Action
Grouping	Clicking this item causes all the groups to appear (each group under its own tab) in the right. Click a tab to see the members of the group.
Add a New Group	Brings up a dialog box that allows you to key in the name for a new group. After you click **OK** and exit, the group is added to the group list in the left panel tree. To assign a device to a group, use the *General Settings* function of the *Target* Menu and key the Group Name in the appropriate entry field.
Group Rename	First, select a group from the left panel, then select this item to rename it. After you click **OK** and exit, the new name replaces the old one in the left panel tree.
Group General Settings	This is similar to the browser-based page. See *General*, page 34.
Group Network Settings	This is similar to the browser-based page. See *Network*, page 25.
Group ANMS Settings	This is similar to the browser-based Notification page. See *Notification*, page 37.
Restore	This is similar to the browser-based page. See *Backup & Restore*, page 45.
Firmware Upgrade	This is similar to the browser-based page. See *Firmware Update*, page 44.
Port Basic Settings	This is similar to the port settings dialog box. See *Editing Serial Ports*, page 24

Monitor

This menu allows you to keep track of the serial ports on your installation. There are three items on the menu, as described in the table below.

Item	Action
Enum Targets	Selecting this item causes the program to search for and list (enumerate) all SN target devices found in a tree view in the left panel.
Refresh Port (Static)	Clicking *Refresh Port (Static)*, information about each of the enumerated ports appears in the right panel.
Refresh Port (Dynamic)	This item is similar to the Refresh Port (Static) item, except that instead of refreshing the ports manually, it automatically refreshes the list at the time interval set. Valid time intervals include 10 sec, 30 sec, 60 sec, 2 min, 5 min, and 10 min.

Virtual Port

Selecting this item brings up the *Virtual Serial Port Manager*. See page 59 for details.

The Button Bar

The buttons on the button bar offer quick implementations of the functions available through the menus.

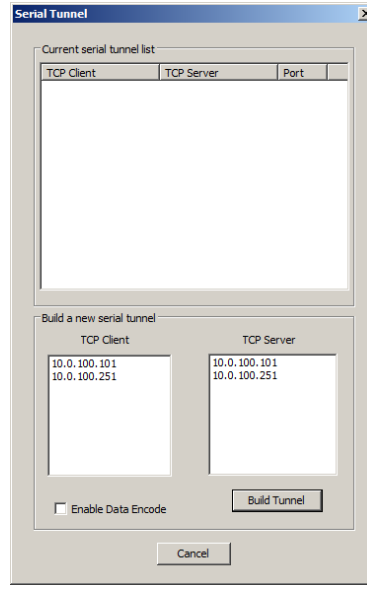
- **Enum Targets** — performs the same function as the Enum Targets entry on the Monitor menu.
- **List Port** — performs the same function as the Refresh Port (Static) entry on the Monitor menu.
- **Grouping** — performs the same function as the Grouping entry on the Group menu.

Serial Tunnel Creation

Building a Serial Tunnel

To build a Serial Tunnel connection between two Secure Serial Device Server units, do the following:

1. From the Menu Bar, select **Target > Serial Tunnel** to bring up the *Serial Tunnel* dialog box:



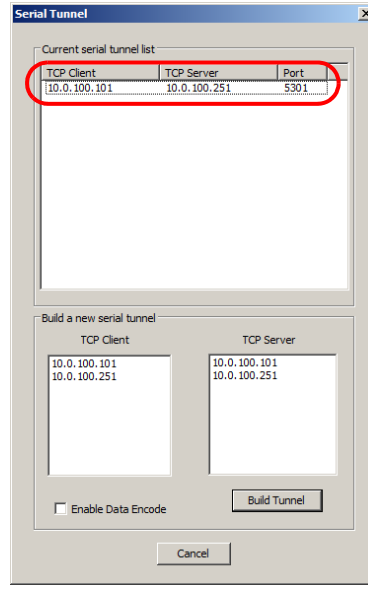
   If any Serial Tunnels have already been established, they are displayed in the upper panel.

2. Select the unit to be set as the Client from the list in the lower left panel; select the unit to be set as the Server from the list in the lower right panel.

3. If you want the transmitted data to be encoded, check the *Enable Data Encoding* checkbox.

4. Click **Build Tunnel**.

After a moment or two, the newly built tunnel appears in the upper panel.



5. When you have finished building all your serial tunnels, click **Cancel** to close the dialog box.

Removing a Serial Tunnel

Since a serial tunnel is composed of a Serial Tunneling Client and a Serial Tunneling Server, removing a serial tunnel is accomplished by simply changing the operating mode of either Secure Serial Device Server (see *Operating Mode*, page 27).

This Page Intentionally Left Blank

Chapter 8
User Management

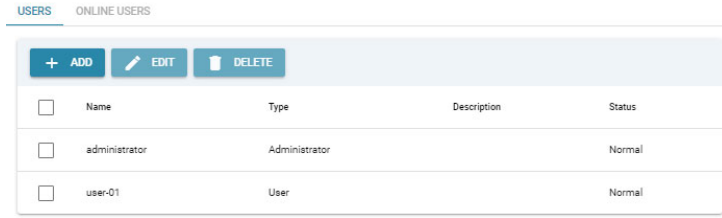
Overview

This chapter takes users through how to add or edit the login accounts of Secure Serial Device Server, including the *administrator*, as well as using third-party authentication services.

User

The Secure Serial Device Server supports up to 16 user accounts, with two types of users, as described below:

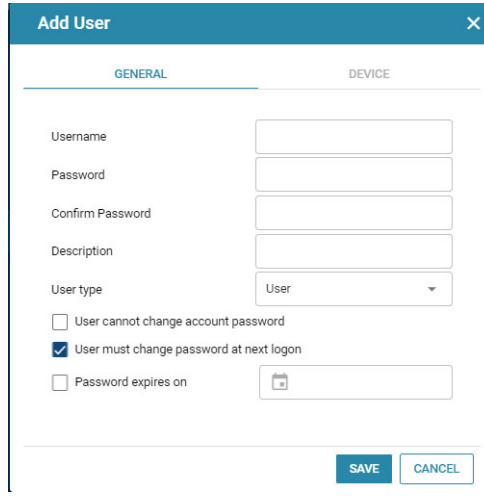
User Type	Role
Administrator	Able to access and configure all serial ports, and manage other login accounts
User	Only able to access and/or configure the authorized serial ports, as permitted by the administrator, and unable to configure any of the device's system settings.



Item	Description
Name	Displays the username of the user account.
Type	Displays the account type, *Administrator* or *User*.
Description	Additional information used to describe the user account.
Status	Displays the status of the user account, which includes: ◆ *Normal:* The account functions normally. ◆ *Password Expired:* The account's password has expired and must be changed.

Adding Users

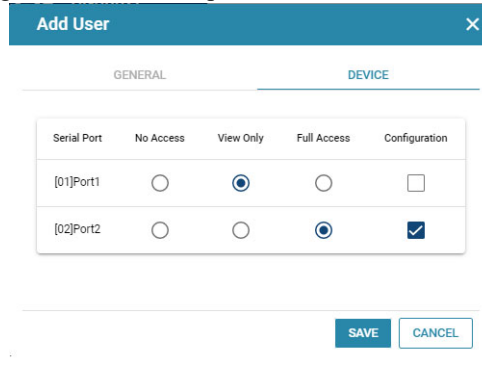
1. Click **User Accounts** > **User** > **Users** on the web interface of the Secure Serial Device Server.
2. Click **Add**. The *Add User* window's **General** tab appears. Enter the required fields, as described in the table below.



Item	Description
Username	From 1 to 32 characters are allowed depending on the Account Policy settings. See *Account Policy*, page 47.
Password	From 1 to16 characters are allowed depending on the Account Policy settings. See *Account Policy*, page 47.
Confirm Password	Match the *Password* field to confirm the password entry.
Description	Additional information about the user that you may wish to include.
User type	Select *Administrator* for full access and configuration rights or select *User* permit only the access and configuration rights of the serial ports, as set.
User cannot change account password	Check to restrict the user from changing the account's password
User must change password at next login	Check to require the user to change his password upon next login.

Item	Description
Password expires on	Specifies the date on which the password of the login account shall expire, and be redefined. **Note:** After a user's password expires, he can still log in with the old password, but will be forced to change it upon login.

3. Only for user types — *User*, click the **Device** tab to permit access and/or configure rights for each serial port, as described in the table below.



Item	Description
No Access	Select to restrict access to the serial port.
View Only	Select to only allow view access to the serial port, while restricting Telnet and SSH sessions.
Full Access	Select to allow full access to the serial port.
Configuration	Check to allow configuration for the serial port, including its *Properties*, *Operating Mode*, and *Port Buffering* settings. See *Editing Serial Ports*, page 27.

4. Click **Save** to finish.
5. When the *Operation Succeeded* message appears, click **OK**.

Editing Users

To edit a user account, select it and click **Edit**.

In the *Edit User* window, make your changes by referring to *Adding Users*, page 54, then click **Save**.

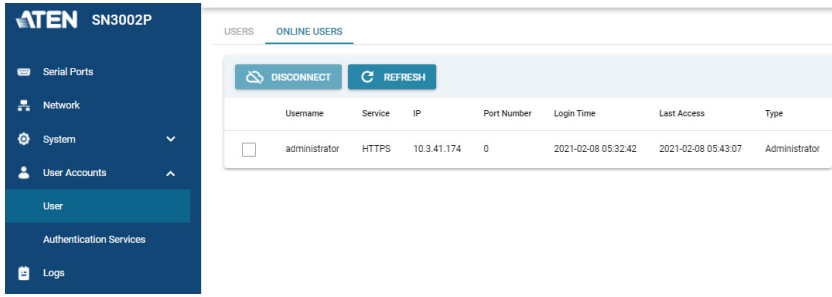
Deleting Users

To delete user account(s), select them and click **Delete**.

When asked *Are you sure to delete?*, Click **OK** to confirm.

Online Users

The **Online Users** tab displays the user accounts that are currently accessing the Secure Serial Device Server.



The administrator can check to select any other user accounts currently logged in, and click **Disconnect** to terminate those users' access sessions.

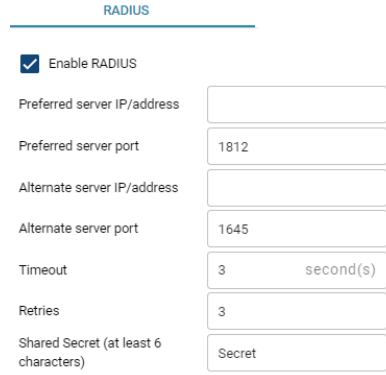
Authentication Services

The Secure Serial Device Server allows external, third-party authentication services, namely *RADIUS* for managing and authenticating its user accounts.

Note: When using RADIUS for authentication, only PAP is supported.

To enable such services, click **User Accounts** > **Authentication Services** on its web interface.

RADIUS



1. To use authentication via RADIUS, enable the service on the Secure Serial Device Server, by referring to the table below.

Item	Description
Preferred server IP/ address and server port	Fill in the IP address and service port of the primary (preferred) RADIUS server.
Alternate server IP/ address and server port	Fill in the IP address and service port of the alternate RADIUS server.
Timeout	Sets the time, in seconds, that the Secure Serial Device Server shall wait for the RADIUS server for.
Retries	Sets the number of allowed RADIUS retries.
Shared Secret (at least 6 characters)	Enter the character string that you want to use for authentication between the Secure Serial Device Server and the RADIUS server.

2. On the RADIUS server, set the access rights for each according to the attribute information provided in the following table.

Attribute	Description
U	(User) The user has the authority to access and configure some ports. This attribute must be specified for all users who access the device.
T	(True) The user has the authority to access and configure the ports that are specified with it.
F	(False) The user cannot configure any ports.
A	(All) The user has the authority to access and configure all ports.

Example:

```
U, T, 1
```

The user can access and configure port 1.

Note: 1. The characters are not case sensitive, i.e. uppercase and lowercase work equally well, and comma-separated.

2. An invalid character in the string will prohibit access to the Secure Serial Device Server for the user.

Chapter 9
Virtual Serial Port Manager

Overview

The Secure Serial Device Server offers a Virtual COM port driver for Windows, Real TTY driver for Linux, and Fixed TTY driver for OpenServer, Solaris, FreeBSD, AIX, and Mac.

By running the driver on a PC, devices connected to the Secure Serial Device Server's COM ports, appear as if they were directly connected to the COM ports of that PC.

Note: The Operating Mode of the serial ports must be set as *Real COM* to be configured as a virtual port (see *Operating Mode*, page 30).

Data transmission takes place over the Ethernet between the PC's virtual COM port and the devices connected to the Secure Serial Device Server's COM ports.

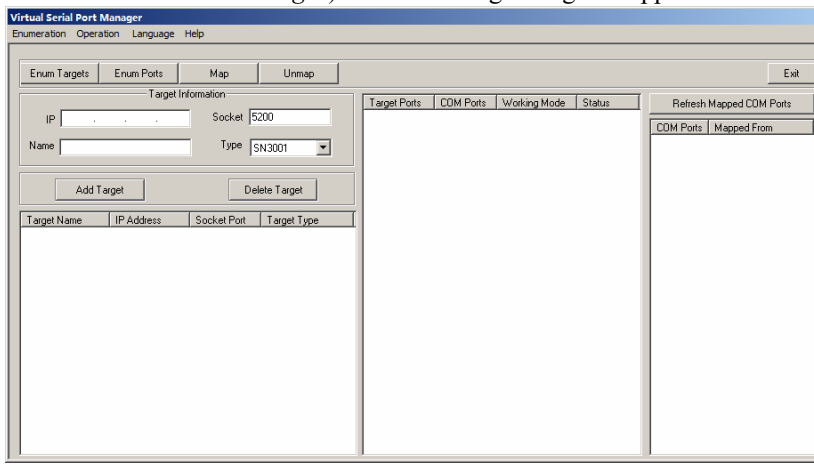
Users can download and install the driver corresponding to their PC OS from the Secure Serial Device Server's product web page.

Real COM Port Management — Virtual Serial Port Manager

The Virtual Serial Port Manager is a utility that provides a convenient interface for COM port mapping.

Note: The Virtual Serial Port Manager only supports Windows and Linux with Kernel 4.15.0-43 and 4.2.0-27. For other versions of Linux systems, see *Real COM Port Management — Linux Commands*, page 66.

Start **Virtual Serial Port Manager** (*Start* > *Virtual Port Management Utility* > *Virtual Serial Port Manager*). The following dialog box appears.



Utility Interface

The Virtual Serial Port Manager's interface is laid out as follows:

- The menu and button bars allow the automatic enumeration and listing of devices and ports.
- Below the menu and button bars is an area to input the required information for manually listing devices if the target device doesn't appear using the automatic enumeration method.
- All devices found through enumeration or manually entered are listed in the left panel.
- All ports found on the device selected are enumerated in the central panel.
- The right panel displays any virtual COM port mapping that have been made.

Menu and Toolbar

The Virtual Serial Port Manager menu and toolbar consist of the same functions. Users can either click the menu items or buttons to invoke the desired function, as described in the table below.

Item	Action
Enum Targets	This function searches and lists all SN devices within the LAN — these include Secure Serial Device Server, as well as ATEN Serial Console Servers. The results are shown in the Target List panel (see *Target List*, page 62, for details). Beware that all devices listed in the Target List will be deleted when the delete function is invoked. Be sure to remove any devices from the list that you don't want to delete before invoking the delete function.
Enum Ports	This function lists the existing ports for the target device currently selected in the Target List. The results are shown in the Port List panel.
Map	After selecting a port from the *Port List* panel, selecting this function maps the device's COM port to a virtual COM port on the user's PC.
Unmap	After selecting a port from the *Mapped Ports* list, selecting this function removes the mapping between the PC and the device's COM port.

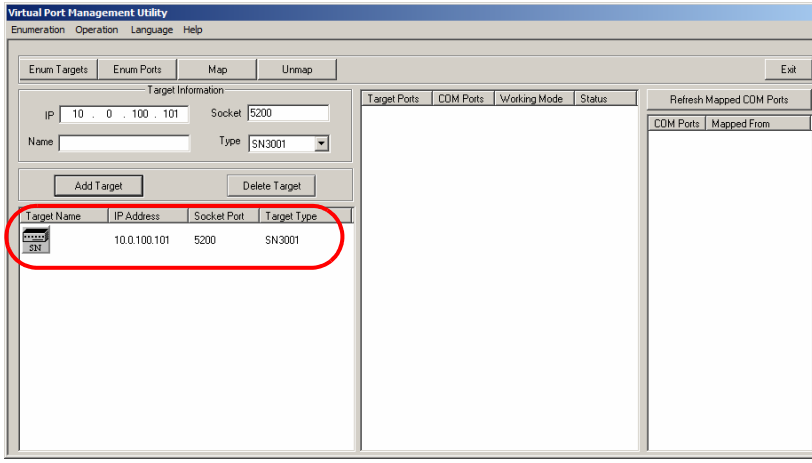
Target Information

The Target Information fields allow users to install (map) ports on an offline target device, as described below.

Field	Action
Target IP Address	Input the IP address of the target that you want to map COM ports to.
Base Socket Port	The base socket port of the target device. For Real COM port operation, the default base socket port is 5200.
Target Name	The name of the target. If it is different from the target's real name, will be replaced by the real one. Note that the name is not related to the mapping / unmapping process. Only the IP address, socket port and target type are relevant.
Target Type	The type of target to be mapped. SN3001 / SN3002 and ATEN Serial Console Servers are valid target types. **Note:** SN3001 includes SN3001P, and SN3002 includes SN3002P.
Add Target	Creates an entry in the Target List based on the above information.
Delete Target	Remove the currently selected target from the Target List.

Target List

The left panel displays all the devices that were found with the *Enumeration* function, as well as any devices that were manually added with the *Target Information* fields.

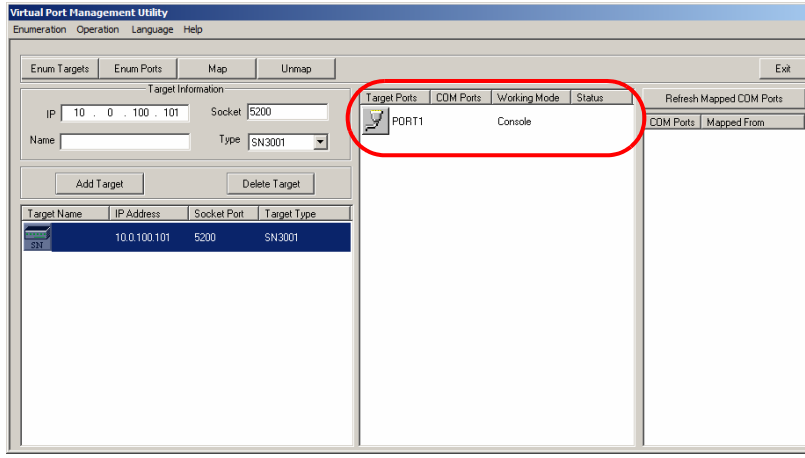


Note: Double-clicking an item in the list invokes the same function as selecting **Enum Ports**, which displays the numbers and working modes of the selected target's ports in the *Port List* column.

- If a device was automatically listed as a result of the *Enumeration* procedure, the icon to its left is drawn with green dots and lines to show that the target is online and ready to be mapped.
- If a device was added to the list manually and is offline, the icon to its left is drawn with black dots and lines. Double-clicking a manually added item shall display its information in the *Port List*, but the working mode information is not accurate and we must assume that all the device's ports are in Real COM mode. See *Operating Mode*, page 30, for details about port modes.
- If the target is offline or is online but does not respond within 2 seconds of asking to enumerate its ports, the working mode information is not accurate and we must assume that all the device's ports are in Real COM mode. See *Operating Mode*, page 30, for details about port modes.

Port List

This list displays the port information of the selected target (only one target can be selected at a time).



- The left column lists the target's port number, the second column shows the COM port it is mapped to (if any), the third column shows its working mode, and the right column shows its status.

  Note: The working mode refers to the operating mode that the serial port is set as. See *Operating Mode*, page 30, for details.

- Double-clicking a port in the Port List brings up the *Port Mapping* dialog box. See *Port Mapping*, page 64 for mapping details.

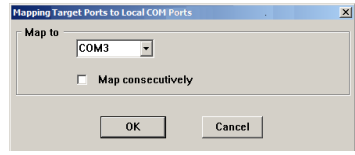
  Note: The *Port Mapping* dialog box can also be invoked either by clicking MapTo… on the toolbar or selecting MapTo… from the menu.

Port Mapping and Unmapping

Port Mapping

To map a virtual COM port:

1. Double-click your Target item in the Port List to brings up the *Port Mapping* dialog box:



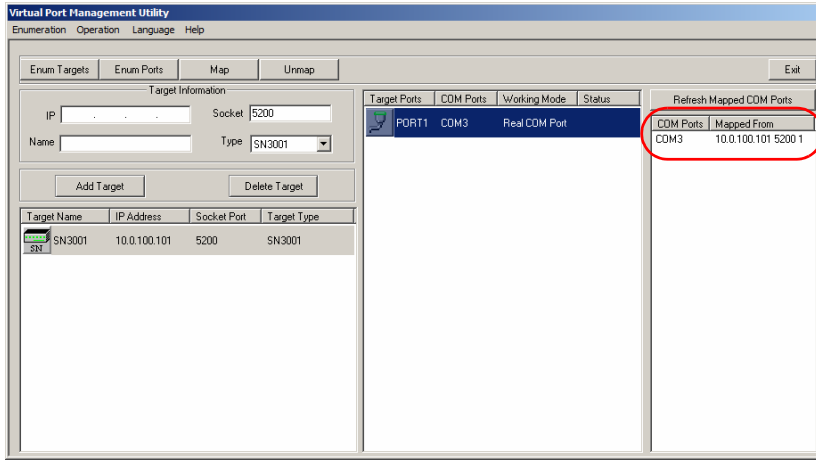
2. From the drop-down list, select the desired COM port to map the Target port to.
3. Click **OK**.

Note: If a warning dialog box comes up, you can safely ignore it. Click **Continue Anyway** to complete the operation

---

Mapped COM Port

The far-right panel on the *Virtual Port Management* displays the mapped COM port. The entry is generated as soon as the application starts, and is updated whenever the mapped COM port configuration changes as a result of installations and removals.

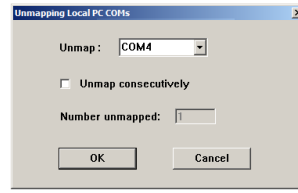


Up to 256 ports can be mapped on a Windows system.

Port Unmapping

To unmap a virtual COM port, do the following:

1. Select the mapped COM port (in the far-right panel) to bring up the *Port Unmapping* dialog box:



Note: If the dialog box doesn't come up, either click **Unmap…** on the button bar, or select *Unmap…* from the menu.

2. Click **OK** to complete the operation.

Real COM Port Management — Linux Commands

Mapping / Unmapping Virtual Ports

To map or unmap virtual ports, do the following:

1. As root, go to the /usr/lib/AtenVPort directory.
2. Issue the following command:

   ```
   /AtenVPMapping
   ```

The process can run in either *Interactive* mode or *Fast* mode. With Interactive mode, users are not required to specify any parameters on the command line. They make mapping/unmapping choices based on questions generated as the program runs.

With Fast mode, users must specify parameters on the command line to indicate their mapping/unmapping choices — as shown in the following examples:

1. Mapping (input should be all within one line):

   ./AtenVPMapping map(1) PCPort(0-255) TargetIP(a.b.c.d) TargetPort(1-48) NumberofMapping(1-48)

2. Unmapping (input should be all within one line):

   ./AtenVPMapping unmap(0) PCPort(0-255) NumberofUnMapping(1-48)

Up to 256 ports can be mapped on a Linux system.

Virtual Port Naming Rules

All of the ATEN SN virtual ports under Linux have the prefix *ttya*.

Mapped virtual ports can be found in the /dev dir. They all have a prefix of *ttya* (ttya000, ttya001, etc.). The range is from ttya000 – ttya255.

Chapter 10
MIB Reference

This section provides information about the MIBs (version 1.0.085) supported in Secure Serial Device Servers, which are used for integration with network management systems, automated monitoring, and event handling. Specifically, the section covers:

- Subtree structure and organization for object grouping and navigation
- A list of supported MIB objects, including OIDs, access types, data formats, and descriptions
- Definitions of SNMP traps, including trap OIDs, trigger conditions (descriptions), and associated parameters

This chapter includes the following sections:

MIB Tree Structure

- atenProducts `(.1.3.6.1.4.1.21317.1)`
  This is the root node for all ATEN products.
- overip `(.1.3.6.1.4.1.21317.1.3)`
  This is a subtree for ATEN IP-based products.
  - **serialoverip** `(.1.3.6.1.4.1.21317.1.3.3)`
    Defines the MIB objects and traps for ATEN Secure Serial Device and Secure Serial Device Servers.
    - Servers.SN300X series `(.1.3.6.1.4.1.21317.1.3.3.5)`

Downloading MIB Files

To download the latest MIB files:

1. Visit the official product page of your target Secure Serial Device Server.
2. Scroll down to locate the **MIB File** section. For example:

MIB File

	MIB Files	v1.0.085	2022-12-19	SN300X_Mibs_File_v1.0.085.zip
	MIB Files	v1.0.073	2021-05-17	SN300X_Mibs_File_v1.0.073.zip

3. Download the latest MIB file.

OID Format

In this document, all object identifiers (OIDs) are presented in their numeric form without a leading period.

For example, the OID may be displayed by some SNMP tools as:

```
.1.3.6.1.4.1.21317.1.2.1.1.1.1.0
```

In this document, it is written as:

```
1.3.6.1.4.1.21317.1.2.1.1.1.1.0
```

Both notations are equivalent. The leading period is omitted for consistency and readability.

Object Types and Indexing

SNMP objects can be scalar or table-based. When sending GET requests, ensure to distinguish between scalar objects and instance objects, and their correct OID usage.

- Scalar Objects

  A scalar object is an object that contains a discrete piece of data. Since scalar objects are always defined as having one instance, and to distinguish this type of object from instance objects, append **".0"** to the OID when referencing scalar objects in GET requests.

  For example:

  If the `DeviceName` object is defined as:

Object Name	OID
DeviceName	1.3.6.1.4.1.21317.1.3.3.3.7.1

  Using SNMP version 2c, with community string 'public', to retrieve the value of the scalar object `DeviceName.0` from the SNMP agent at IP 192.168.1.10, the GET request will be:

```
snmpget -v2c -c public 192.168.1.10 DeviceName.0
or
snmpget -v2c -c public 192.168.1.10 1.3.6.1.4.1.21317.1.3.3.3.7.1.0
```

  Result:

```
SNMPv2-MIB::DeviceName.0 = STRING: ServerA
```

Note: When ".0" is omitted, SNMP agents will not be able to find the instance and returns an error or invalid message.

- Instance Objects

  As opposed to scalar objects, some objects may contain multiple instances, e.g. network interfaces for a device. An instance object is one of the multiple pieces of data that exist in an SNMP table. To refer to these pieces of data correctly in a GET request, use the OIDs that are appended with index numbers.

  For example:

  If the MIB defines the column OID of interface card as `1.3.6.1.2.1.2.2.1.2`

  and the device has two interfaces:

Interface Index	Description
1	Ethernet 0
2	Ethernet 1

  Using SNMP version 2c, with community string ‘public’, to retrieve the value of the instance 2, from the SNMP agent at IP 192.168.1.10, the SNMP command would be:

```
snmpget -v2c -c public 192.168.1.10 1.3.6.1.2.1.2.2.1.2.2
```

SN300X Series MIB Objects

This section defines the MIB objects supported by the SN3000X series. These MIB objects are organized into the following types:

- *RS232 Objects*
- *User Configuration Objects*
- *Session Objects*
- *Firmware Management Object*

RS232 Objects

RS232 General

- `rs232Number`

OID	`1.3.6.1.4.1.21317.1.3.3.5.1.1`
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The number of ports (regardless of their current state) in the RS-232-like general port table

RS232 Port Configuration

- `rs232PortIndex`

OID	`1.3.6.1.4.1.21317.1.3.3.5.1.2.1.1`
Syntax	InterfaceIndex
Max-Access	read-only
Status	current
Description	The value of ifIndex for the port. By convention and if possible, hardware port numbers map directly to external connectors. The value for each port must remain constant at least from one re-initialization of the network management agent to the next.

- rs232PortType

OID	1.3.6.1.4.1.21317.1.3.3.5.1.2.1.2
Syntax	INTEGER {other (1), rs232 (2), rs422 (3), rs423 (4), v35 (5), x21 (6)}
Max-Access	read-only
Status	current
Description	The port's hardware type.

- rs232PortInSigNumber

OID	1.3.6.1.4.1.21317.1.3.3.5.1.2.1.3
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The number of input signals for the port in the input signal table (rs232PortInSigTable). The table contains entries only for those signals the software can detect and that are useful to observe.

- rs232PortOutSigNumber

OID	1.3.6.1.4.1.21317.1.3.3.5.1.2.1.4
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The number of output signals for the port in the output signal table (rs232PortOutSigTable). The table contains entries only for those signals the software can assert and that are useful to observe.

- rs232PortInSpeed

OID	1.3.6.1.4.1.21317.1.3.3.5.1.2.1.5
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The port's input speed in bits per second. Note that non-standard values, such as 9612, are probably not allowed on most implementations.

- `rs232PortOutSpeed`

OID	`1.3.6.1.4.1.21317.1.3.3.5.1.2.1.6`
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The port's output speed in bits per second. Note that non-standard values, such as 9612, are probably not allowed on most implementations.

- `rs232PortInFlowType`

OID	`1.3.6.1.4.1.21317.1.3.3.5.1.2.1.7`
Syntax	INTEGER {none (1), ctsRts (2), dsrDtr (3)}
Max-Access	read-only
Status	current
Description	The port's type of input flow control. 'none' indicates no flow control at this level. 'ctsRts' and 'dsrDtr' indicate use of the indicated hardware signals.

- `rs232PortOutFlowType`

OID	`1.3.6.1.4.1.21317.1.3.3.5.1.2.1.8`
Syntax	INTEGER {none (1), ctsRts (2), dsrDtr (3)}
Max-Access	read-only
Status	current
Description	The port's type of output flow control. 'none' indicates no flow control at this level. 'ctsRts' and 'dsrDtr' indicate the use of the specified hardware signals.

RS232 Async Port

- `rs232AsyncPortIndex`

OID	`1.3.6.1.4.1.21317.1.3.3.5.1.3.1.1`
Syntax	InterfaceIndex
Max-Access	read-only
Status	current
Description	A unique value for each port. Its value is the same as `rs232PortIndex` for the port.

- `rs232AsyncPortBits`

OID	`1.3.6.1.4.1.21317.1.3.3.5.1.3.1.2`
Syntax	INTEGER (5..8)
Max-Access	read-only
Status	current
Description	The port's number of bits in a character.

- `rs232AsyncPortStopBits`

OID	`1.3.6.1.4.1.21317.1.3.3.5.1.3.1.3`
Syntax	INTEGER {one (1), two (2), oneAndHalf (3), dynamic (4)}
Max-Access	read-only
Status	current
Description	The port's number of stop bits.

- `rs232AsyncPortParity`

OID	`1.3.6.1.4.1.21317.1.3.3.5.1.3.1.4`
Syntax	INTEGER {none (1), odd (2), even (3), mark (4), space (5)}
Max-Access	read-only
Status	current
Description	The port's sense of a character parity bit.

- rs232AsyncPortAutobaud

OID	1.3.6.1.4.1.21317.1.3.3.5.1.3.1.5
Syntax	INTEGER {enabled (1), disabled (2)}
Max-Access	read-only
Status	current
Description	A control for the port's ability to automatically sense input speed. When rs232PortAutoBaud is 'enabled', a port may autobaud to values different from the set values for speed, parity, and character size. As a result a network management system may temporarily observe values different from what was previously set.

RS232 Input Signals

- rs232InSigPortIndex

OID	1.3.6.1.4.1.21317.1.3.3.5.1.5.1.1
Syntax	InterfaceIndex
Max-Access	read-only
Status	current
Description	The value of rs232PortIndex for the port to which this entry belongs.

- rs232InSigName

OID	1.3.6.1.4.1.21317.1.3.3.5.1.5.1.2
Syntax	INTEGER {rts (1), cts (2), dsr (3), dtr (4), ri (5), dcd (6), sq (7), srs (8), srts (9), scts (10), sdcd (11)}
Max-Access	read-only
Status	current
Description	Identification of a hardware signal, as follows: rts Request to Send cts Clear to Send dsr Data Set Ready dtr Data Terminal Ready ri Ring Indicator dcd Received Line Signal Detector sq Signal Quality Detector srs Data Signaling Rate Selector srts Secondary Request to Send scts Secondary Clear to Send sdcd Secondary Received Line Signal Detector

- `rs232InSigState`

OID	`1.3.6.1.4.1.21317.1.3.3.5.1.5.1.3`
Syntax	INTEGER {none (1), on (2), off (3)}
Max-Access	read-only
Status	current
Description	The current signal state.

RS232 Output Signals

- `rs232OutSigPortIndex`

OID	`1.3.6.1.4.1.21317.1.3.3.5.1.6.1.1`
Syntax	InterfaceIndex
Max-Access	read-only
Status	current
Description	The value of `rs232PortIndex` for the port to which this entry belongs

- `rs232OutSigName`

OID	`1.3.6.1.4.1.21317.1.3.3.5.1.6.1.2`
Syntax	INTEGER {rts (1), cts (2), dsr (3), dtr (4), ri (5), dcd (6), sq (7), srs (8), srts (9), scts (10), sdcd (11)}
Max-Access	read-only
Status	current
Description	Identification of a hardware signal, as follows: rts Request to Send cts Clear to Send dsr Data Set Ready dtr Data Terminal Ready ri Ring Indicator dcd Received Line Signal Detector sq Signal Quality Detector srs Data Signaling Rate Selector srts Secondary Request to Send scts Secondary Clear to Send sdcd Secondary Received Line Signal Detector

- rs232OutSigState

OID	1.3.6.1.4.1.21317.1.3.3.5.1.6.1.3
Syntax	INTEGER {none (1), on (2), off (3)}
Max-Access	read-only
Status	current
Description	The current signal state.

User Configuration Objects

General

- usrcfgNumber

OID	1.3.6.1.4.1.21317.1.3.3.5.2.1
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The number of users (regardless of their current state) in the SN300X series user configuration

UsrcfgEntry

- usrIndex

OID	1.3.6.1.4.1.21317.1.3.3.5.2.2.1.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The value of usrIndex for the user.

- usrType

OID	1.3.6.1.4.1.21317.1.3.3.5.2.2.1.2
Syntax	INTEGER {administrator (1), operator (2)}
Max-Access	read-only
Status	current
Description	The user's type.

- usrName

OID	1.3.6.1.4.1.21317.1.3.3.5.2.2.1.3
Syntax	DISPLAYSTRING
Max-Access	read-only
Status	current
Description	A textual string containing name of the user

- usrPassword

OID	1.3.6.1.4.1.21317.1.3.3.5.2.2.1.4
Syntax	DISPLAYSTRING
Max-Access	read-only
Status	current
Description	A textual string containing password of the user

- usrConfigPort

OID	1.3.6.1.4.1.21317.1.3.3.5.2.2.1.5
Syntax	INTEGER {disable (0), enable (1)}
Max-Access	read-only
Status	current
Description	This indicates whether the user has port configuration permissions

- usrAllowedPort

OID	1.3.6.1.4.1.21317.1.3.3.5.2.2.1.6
Syntax	DISPLAYSTRING
Max-Access	read-only
Status	current
Description	A textual string containing the name of ports which can be used by this user.

- usrStatus

OID	1.3.6.1.4.1.21317.1.3.3.5.2.2.1.7
Syntax	INTEGER {inactive (0), active (1)}
Max-Access	read-only
Status	current
Description	Indicates the user status. When the user logs in SN300X series, its status is active (1).

Session Objects

- sessionNumber

OID	1.3.6.1.4.1.21317.1.3.3.5.3.1
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The number of active sessions in the SN300X series

sessionTable

- sessionIndex

OID	1.3.6.1.4.1.21317.1.3.3.5.3.2.1.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The value of session Index for the session

- sessionOwner

OID	1.3.6.1.4.1.21317.1.3.3.5.3.2.1.2
Syntax	DISPLAYSTRING
Max-Access	read-only
Status	current
Description	User name who starts this session

- `sessionService`

OID	`1.3.6.1.4.1.21317.1.3.3.5.3.2.1.3`
Syntax	DISPLAYSTRING
Max-Access	read-only
Status	current
Description	HTTP, HTTPS, and so on.

- `sessionIP`

OID	`1.3.6.1.4.1.21317.1.3.3.5.3.2.1.4`
Syntax	IpAddress
Max-Access	read-only
Status	current
Description	The NetworkAddress (e.g., the IP address) of connection

- `sessionUpTime`

OID	`1.3.6.1.4.1.21317.1.3.3.5.3.2.1.5`
Syntax	DISPLAYSTRING
Max-Access	read-only
Status	current
Description	The time when the session was last initialized

- `sessionLastAccess`

OID	`1.3.6.1.4.1.21317.1.3.3.5.3.2.1.6`
Syntax	DISPLAYSTRING
Max-Access	read-only
Status	current
Description	The time when the session was last accessed

Firmware Management Object

- imageCurrentVersion

OID	1.3.6.1.4.1.21317.1.3.3.5.4
Syntax	DisplayString (SIZE (0..255))
Max-Access	read-only
Status	current
Description	The current firmware image version of the SN300X series.

SN340X Series MIB Objects

This section defines the MIB objects supported by the SN340X series. These MIB objects are organized into the following types:

- *RS232 Objects*
- *User Configuration Objects*
- *Session Objects*
- *Firmware Management Object*

RS232 Objects

RS232 General

- `rs232Number`

OID	`1.3.6.1.4.1.21317.1.3.3.6.1.1`
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The number of ports (regardless of their current state) in the RS-232-like general port table

RS232 Port Configuration

- `rs232PortIndex`

OID	`1.3.6.1.4.1.21317.1.3.3.6.1.2.1.1`
Syntax	InterfaceIndex
Max-Access	read-only
Status	current
Description	The value of ifIndex for the port. By convention and if possible, hardware port numbers map directly to external connectors. The value for each port must remain constant at least from one re-initialization of the network management agent to the next.

- rs232PortType

OID	1.3.6.1.4.1.21317.1.3.3.6.1.2.1.2
Syntax	INTEGER {other (1), rs232 (2), rs422 (3), rs423 (4), v35 (5), x21 (6)}
Max-Access	read-only
Status	current
Description	The port's hardware type.

- rs232PortInSigNumber

OID	1.3.6.1.4.1.21317.1.3.3.6.1.2.1.3
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The number of input signals for the port in the input signal table (rs232PortInSigTable). The table contains entries only for those signals the software can detect and that are useful to observe.

- rs232PortOutSigNumber

OID	1.3.6.1.4.1.21317.1.3.3.6.1.2.1.4
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The number of output signals for the port in the output signal table (rs232PortOutSigTable). The table contains entries only for those signals the software can assert and that are useful to observe.

- rs232PortInSpeed

OID	1.3.6.1.4.1.21317.1.3.3.6.1.2.1.5
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The port's input speed in bits per second. Note that non-standard values, such as 9612, are probably not allowed on most implementations.

- `rs232PortOutSpeed`

OID	`1.3.6.1.4.1.21317.1.3.3.6.1.2.1.6`
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The port's output speed in bits per second. Note that non-standard values, such as 9612, are probably not allowed on most implementations.

- `rs232PortInFlowType`

OID	`1.3.6.1.4.1.21317.1.3.3.6.1.2.1.7`
Syntax	INTEGER {none (1), ctsRts (2), dsrDtr (3)}
Max-Access	read-only
Status	current
Description	The port's type of input flow control. 'none' indicates no flow control at this level. 'ctsRts' and 'dsrDtr' indicate use of the indicated hardware signals.

- `rs232PortOutFlowType`

OID	`1.3.6.1.4.1.21317.1.3.3.6.1.2.1.8`
Syntax	INTEGER {none (1), ctsRts (2), dsrDtr (3)}
Max-Access	read-only
Status	current
Description	The port's type of output flow control. 'none' indicates no flow control at this level. 'ctsRts' and 'dsrDtr' indicate the use of the specified hardware signals.

RS232 Async Port

- rs232AsyncPortIndex

OID	1.3.6.1.4.1.21317.1.3.3.6.1.3.1.1
Syntax	InterfaceIndex
Max-Access	read-only
Status	current
Description	A unique value for each port. Its value is the same as rs232PortIndex for the port.

- rs232AsyncPortBits

OID	1.3.6.1.4.1.21317.1.3.3.6.1.3.1.2
Syntax	INTEGER (5..8)
Max-Access	read-only
Status	current
Description	The port's number of bits in a character.

- rs232AsyncPortStopBits

OID	1.3.6.1.4.1.21317.1.3.3.6.1.3.1.3
Syntax	INTEGER {one (1), two (2), oneAndHalf (3), dynamic (4)}
Max-Access	read-only
Status	current
Description	The port's number of stop bits.

- rs232AsyncPortParity

OID	1.3.6.1.4.1.21317.1.3.3.6.1.3.1.4
Syntax	INTEGER {none (1), odd (2), even (3), mark (4), space (5)}
Max-Access	read-only
Status	current
Description	The port's sense of a character parity bit.

- rs232AsyncPortAutobaud

OID	1.3.6.1.4.1.21317.1.3.3.6.1.3.1.5
Syntax	INTEGER {enabled (1), disabled (2)}
Max-Access	read-only
Status	current
Description	A control for the port's ability to automatically sense input speed. When rs232PortAutoBaud is 'enabled', a port may autobaud to values different from the set values for speed, parity, and character size. As a result a network management system may temporarily observe values different from what was previously set.

RS232 Input Signals

- rs232InSigPortIndex

OID	1.3.6.1.4.1.21317.1.3.3.6.1.5.1.1
Syntax	InterfaceIndex
Max-Access	read-only
Status	current
Description	The value of rs232PortIndex for the port to which this entry belongs.

- rs232InSigName

OID	1.3.6.1.4.1.21317.1.3.3.6.1.5.1.2
Syntax	INTEGER {rts (1), cts (2), dsr (3), dtr (4), ri (5), dcd (6), sq (7), srs (8), srts (9), scts (10), sdcd (11)}
Max-Access	read-only
Status	current
Description	Identification of a hardware signal, as follows: rts Request to Send cts Clear to Send dsr Data Set Ready dtr Data Terminal Ready ri Ring Indicator dcd Received Line Signal Detector sq Signal Quality Detector srs Data Signaling Rate Selector srts Secondary Request to Send scts Secondary Clear to Send sdcd Secondary Received Line Signal Detector

- rs232InSigState

OID	1.3.6.1.4.1.21317.1.3.3.6.1.5.1.3
Syntax	INTEGER {none (1), on (2), off (3)}
Max-Access	read-only
Status	current
Description	The current signal state.

RS232 Output Signals

- rs232OutSigPortIndex

OID	1.3.6.1.4.1.21317.1.3.3.6.1.6.1.1
Syntax	InterfaceIndex
Max-Access	read-only
Status	current
Description	The value of rs232PortIndex for the port to which this entry belongs

- rs232OutSigName

OID	1.3.6.1.4.1.21317.1.3.3.6.1.6.1.2
Syntax	INTEGER {rts (1), cts (2), dsr (3), dtr (4), ri (5), dcd (6), sq (7), srs (8), srts (9), scts (10), sdcd (11)}
Max-Access	read-only
Status	current
Description	Identification of a hardware signal, as follows: rts Request to Send cts Clear to Send dsr Data Set Ready dtr Data Terminal Ready ri Ring Indicator dcd Received Line Signal Detector sq Signal Quality Detector srs Data Signaling Rate Selector srts Secondary Request to Send scts Secondary Clear to Send sdcd Secondary Received Line Signal Detector

- rs232OutSigState

OID	1.3.6.1.4.1.21317.1.3.3.6.1.6.1.3
Syntax	INTEGER {none (1), on (2), off (3)}
Max-Access	read-only
Status	current
Description	The current signal state.

User Configuration Objects

General

- usrcfgNumber

OID	1.3.6.1.4.1.21317.1.3.3.6.2.1
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The number of users (regardless of their current state) in the SN340Xseries user configuration

UsrcfgEntry

- usrIndex

OID	1.3.6.1.4.1.21317.1.3.3.6.2.2.1.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The value of usrIndex for the user.

- usrType

OID	1.3.6.1.4.1.21317.1.3.3.6.2.2.1.2
Syntax	INTEGER {administrator (1), operator (2)}
Max-Access	read-only
Status	current
Description	The user's type.

- usrName

OID	1.3.6.1.4.1.21317.1.3.3.6.2.2.1.3
Syntax	DISPLAYSTRING
Max-Access	read-only
Status	current
Description	A textual string containing name of the user

- usrPassword

OID	1.3.6.1.4.1.21317.1.3.3.6.2.2.1.4
Syntax	DISPLAYSTRING
Max-Access	read-only
Status	current
Description	A textual string containing password of the user

- usrConfigPort

OID	1.3.6.1.4.1.21317.1.3.3.6.2.2.1.5
Syntax	INTEGER {disable (0), enable (1)}
Max-Access	read-only
Status	current
Description	This indicates whether the user has port configuration permissions

- usrAllowedPort

OID	1.3.6.1.4.1.21317.1.3.3.6.2.2.1.6
Syntax	DISPLAYSTRING
Max-Access	read-only
Status	current
Description	A textual string containing the name of ports which can be used by this user.

- usrStatus

OID	1.3.6.1.4.1.21317.1.3.3.6.2.2.1.7
Syntax	INTEGER {inactive (0), active (1)}
Max-Access	read-only
Status	current
Description	Indicates the user status. When the user logs in SN340Xseries, its status is active (1).

Session Objects

- sessionNumber

OID	1.3.6.1.4.1.21317.1.3.3.6.3.1
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The number of active sessions in the SN340X series

sessionTable

- sessionIndex

OID	1.3.6.1.4.1.21317.1.3.3.6.3.2.1.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The value of session Index for the session

- sessionOwner

OID	1.3.6.1.4.1.21317.1.3.3.6.3.2.1.2
Syntax	DISPLAYSTRING
Max-Access	read-only
Status	current
Description	User name who starts this session

- sessionService

OID	1.3.6.1.4.1.21317.1.3.3.6.3.2.1.3
Syntax	DISPLAYSTRING
Max-Access	read-only
Status	current
Description	HTTP, HTTPS, and so on.

- sessionIP

OID	1.3.6.1.4.1.21317.1.3.3.6.3.2.1.4
Syntax	IpAddress
Max-Access	read-only
Status	current
Description	The NetworkAddress (e.g., the IP address) of connection

- sessionUpTime

OID	1.3.6.1.4.1.21317.1.3.3.6.3.2.1.5
Syntax	DISPLAYSTRING
Max-Access	read-only
Status	current
Description	The time when the session was last initialized

- sessionLastAccess

OID	1.3.6.1.4.1.21317.1.3.3.6.3.2.1.6
Syntax	DISPLAYSTRING
Max-Access	read-only
Status	current
Description	The time when the session was last accessed

Firmware Management Object

- imageCurrentVersion

OID	1.3.6.1.4.1.21317.1.3.3.6.4
Syntax	DisplayString (SIZE (0..255))
Max-Access	read-only
Status	current
Description	The current firmware image version of the SN340X series.

Appendix

Safety Instructions

General

- Read all of these instructions. Save them for future reference.
- This product is for indoor use only.
- Follow all warnings and instructions marked on the device.
- Do not place the device on any unstable surface (cart, stand, table, etc.). If the device falls, serious damage will result.
- Do not use the device near water.
- Do not place the device near, or over, radiators or heat registers.
- The device cabinet is provided with slots and openings to allow for adequate ventilation. To ensure reliable operation, and to protect against overheating, these openings must never be blocked or covered.
- The device should never be placed on a soft surface (bed, sofa, rug, etc.) as this will block its ventilation openings. Likewise, the device should not be placed in a built in enclosure unless adequate ventilation has been provided.
- Never spill liquid of any kind on the device.
- Unplug the device from the wall outlet before cleaning. Do not use liquid or aerosol cleaners. Use a damp cloth for cleaning.
- The device should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.
- To prevent damage to your installation it is important that all devices are properly grounded.
- Do not allow anything to rest on the power cord or cables. Route the power cord and cables so that they cannot be stepped on or tripped over.
- Position system cables and power cables carefully; Be sure that nothing rests on any cables.
- Never push objects of any kind into or through cabinet slots. They may touch dangerous voltage points or short out parts resulting in a risk of fire or electrical shock.
- Do not attempt to service the device yourself. Refer all servicing to qualified service personnel.

- When connecting or disconnecting power to hot-pluggable power supplies, follow the guidelines below:
  - Install the power supply before connecting the power cable to the power supply.
  - Unplug the power cable before removing the power supply.
  - If the system has multiple sources of power, disconnecting power from the system by unplugging all power cables from the power supplies.
- If the following conditions occur, unplug the device from the wall outlet and bring it to qualified service personnel for repair.
  - The power cord or plug has become damaged or frayed.
  - Liquid has been spilled into the device.
  - The device has been exposed to rain or water.
  - The device has been dropped, or the cabinet has been damaged.
  - The device exhibits a distinct change in performance, indicating a need for service.
  - The device does not operate normally when the operating instructions are followed.
- Only adjust those controls that are covered in the operating instructions. Improper adjustment of other controls may result in damage that will require extensive work by a qualified technician to repair.
- The socket-outlet shall be installed near the equipment and shall be easily accessible.

DC Power

- The system relies on the protective devices in the building installation for protection against short-circuit, overcurrent, and earth (grounding) fault. Ensure that the protective devices in the building installation are properly rated to protect the system, and that they comply with national and local codes.
- Ensure that there is a readily accessible disconnect device incorporated in the building's installation wiring.
- A separate protective earthing terminal is provided on this product and shall be permanently connected to earth.
- For the DC supply circuit, select a DC supply cable that is certified by UL, AWM VW-1 Style 1015, minimum 16 AWG, minimum 105º C, minimum 300 V.
- ⚠ **CAUTION**: This equipment is designed to permit the connection of the earthed conductor of the DC supply circuit to the earthing conductor at the equipment. If this connection is made, all of the following conditions must be met:
  - This equipment shall be connected directly to the DC supply system earthing electrode conductor or to a bonding jumper from an earthing terminal bar or bus to which the DC supply system earthing electrode conductor is connected.
  - This equipment shall be located in the same immediate area (such as adjacent cabinets) as any other equipment that has a connection between the earthed conductor of the same DC supply circuit and the earthing conductor, and also the point of earthing of the DC system. The DC system shall not be earthed elsewhere.
  - The DC supply source is to be located within the same premises as this equipment.
  - Switching or disconnecting devices shall not be in the earthed circuit conductor between the DC source and the point of connection of the earthing electrode conductor.
- **WARNING**: This unit is intended for installation in restricted access areas. A restricted access area (server room, data center, etc.) is where access can only be gained by service personnel through the use of a special tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.

Rack Mounting

- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.
- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Make sure that the rack is level and stable before extending a device from the rack.
- Use caution when pressing the device rail release latches and sliding a device into or out of a rack; the slide rails can pinch your fingers.
- After a device is inserted into the rack, carefully extend the rail into a locking position, and then slide the device into the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Make sure that all equipment used on the rack – including power strips and other electrical connectors — is properly grounded.
- Ensure that proper airflow is provided to devices in the rack.
- Ensure that the operating ambient temperature of the rack environment does not exceed the maximum ambient temperature specified for the equipment by the manufacturer
- Do not step on or stand on any device when servicing other devices in a rack.

Technical Support

International

- For online technical support – including troubleshooting, documentation, and software updates: **http://support.aten.com**
- For telephone support, see *Telephone Support*, page v.

North America

Email Support		support@aten-usa.com
Online Technical Support	Troubleshooting Documentation Software Updates	http://support.aten.com
Telephone Support		1-888-999-ATEN ext 4988 1-949-428-1111

When you contact us, please have the following information ready beforehand:

- Product model number, serial number, and date of purchase.
- Your computer configuration, including operating system, revision level, expansion cards, and software.
- Any error messages displayed at the time the error occurred.
- The sequence of operations that led up to the error.
- Any other information you feel may be of help.

Specifications

SN3001 / SN3001P / SN3002 / SN3002P

Function			Specification
Connectors	Serial		1 x DB-9 Male (Black) 1 x DB-9 Male (Black; SN3002 / SN3002P only)
	Network		1 x RJ-45 Female (Black)
	Power	PWR1	1 x DC Jack (Balck)
		PWR2	1 x 3-pole Terminal (Green)
		PWR3	1 x RJ-45 PoE, IEEE 802.3af (SN3001P / SN3002P only)
Switches	Reset		1 x Semi-recessed button
LEDs	Power		1 x Green
	Status		1 x Yellow Green / Red
	Port 1 / Port 2		1 x Green / Orange 1 x Green / Orange (SN3002 / SN3002P only)
	10 / 100 Mbps		1 x Green 1 x Orange
Power Input	Power Jack		9 V DC
	Power Terminal		9 - 48 V DC
	PoE		48 V DC (SN3001P / SN3002P only)
Power Consumption		SN3001	DC9V:0.634W:3BTU/h DC48V:0.804W:4BTU/h
		SN3002	DC9V:0.769W:4BTU/h DC48V:0.939W:4BTU/h
		SN3001P	DC48V:0.975W:5BTU/h PoE:1.22W:6BTU/h
		SN3002P	DC48V:1.11W:5BTU/h PoE:1.39W:7BTU/h
			Note: ◆ The measurement in Watts indicates the typical power consumption of the device with no external loading. ◆ The measurement in BTU/h indicates the power consumption of the device when it is fully loaded.

Interfaces	Serial	Standards	RS-232
		Baud Rate	110, 134, 150, 300, 600, 1200, 1800, 2400, 4800, 7200, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600
		RS-232 Signals	TxD, RxD, RTS, CTS, DTR, DSR, DCD, GND
		Parity	None, Even, Odd, Mark, Space
		Data Bits	5, 6, 7, 8
		Stop Bits	1, 1.5, 2
		Flow Control	RTS/CTS, DTR/DSR, XON/XOFF, None
	Network	Standards	10/100BaseTX; Autosensing
		Protection	1.5 KV Magnetic Isolation
		Protocols	ARP, DHCP, DNS, HTTP, HTTPS, ICMP, IP, TCP, UDP, NTP, PPP, RADIUS, Telnet, SNMP, SNMP Trap, SMTP, SSH
Standard and Compliance		EMC	EN55032/35
		EMI	CISPR 32, FCC Part 15B Class A
		EMS	IEC 61000-4-2 ESD: Contact: 4 kV; Air: 8 kV IEC 61000-4-3 RS: 80 MHz to 1 GHz: 3 V/m IEC 61000-4-4 EFT: Power: 1 kV; Signal: 0.5 kV IEC 61000-4-5 Surge: Power: 2 kV (Power Adapter), 1 kV (Terminal Block); Signal: 1 kV IEC 61000-4-6 CS: 150 kHz to 10 MHz: 3 V/m; 10 kHz to 30 MHz: 3 to 1 V/m; 30 kHz to 80 MHz: 1 V/m IEC 61000-4-8 PFMF IEC 61000-4-11 DIPs
		Safety	UL 60950-1 and UL 62368-1 standards compliant
		RoHS	
Environment	Operating Temp.		0 – 60 °C
	Storage Temp.		-40 – 75 °C
	Humidity		5 – 95% RH, Non-condensing
Physical Properties	Housing		Metal
	Weight	SN3001	0.20 kg (0.44 lb)
		SN3002	0.21 kg (0.46 lb)
		SN3001P	0.21 kg (0.46 lb)
		SN3002P	0.22 kg (0.48 lb)
	Dimensions (L x W x H)		9.80 x 11.7 x 2.60 cm (3.86 x 4.61 x 1.02 in)

SN3401 / SN3401P / SN3402 / SN3402P

	SN3401	SN3402	SN3401P	SN3402P
Connectors				
Serial	1 x DB-9 Male	2 x DB-9 Male	1 x DB-9 Male	2 x DB-9 Male
Network	1 x RJ-45 Female			
Power	◆ 1 x DC Jack ◆ 1 x 3-pole Terminal Block		◆ 1 x DC Jack ◆ 1 x 3-pole Terminal Block ◆ 1 x RJ-45 (PoE, IEEE 802.3af)	
Switches				
Reset	1 x semi-recessed pushbutton			
LEDs				
Power	1 (Green)			
Status	1 (Yellow Green / Red)			
10/100 Mbps	2 (Green / Orange)			
Ports	1 (Green / Orange)	2 (Green / Orange)	1 (Green / Orange)	2 (Green / Orange)
Input Voltage				
DC Jack	9 V DC (Power Adapter: 9 V DC 100-240 V AC 50~60 Hz)		DC Jack: 9 V DC **Note:** Power adapter is not included in the package, but is available for purchase.	
Terminal Block	9-48 V DC		9-48 V DC	
PoE	N/A		48 V DC	
Power Consumption				
DC	DC9V:1.18W:6BTU/h DC48V:1.30W:6BTU/h	DC9V:1.19W:6BTU/h DC48V:1.30W:6BTU/h	DC48V:1.30W:6BTU/h	DC48V:1.30W:6BTU/h
PoE	N/A	N/A	PoE:1.475W: 7BTU/h	PoE:1.48W: 7BTU/h
	Note: ◆ The measurement in Watts indicates the typical power consumption of the device with no external loading. ◆ The measurement in BTU/h indicates the power consumption of the device when it is fully loaded.			
Interfaces				

	SN3401	SN3402	SN3401P	SN3402P
Serial	◆ **RS-232:** TxD, RxD, RTS, CTS, DTR, DSR, DCD, GND ◆ **RS-422:** Tx+, Tx-, Rx+, Rx-, GND ◆ **RS-485 (4-wire):** Tx+, Tx-, Rx+, Rx-, GND ◆ **RS-485 (2-wire):** Data+, Data-, GND ◆ **Pull High/Low Resistor for RS-485:** 1 kilo-ohm, 150 kilo-ohms ◆ **Baud Rate:** 110, 134, 150, 300, 600, 1200, 1800, 2400, 4800, 7200, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600 bps ◆ **Data Bits:** 5, 6, 7, 8 ◆ **Parity:** None, Even, Odd, Space, Mark ◆ **Stop Bits:** 1, 1.5, 2 ◆ **Flow Control:** RTS/CTS, DTR/DSR, XON/XOFF			
Network	10 / 100 Base TX; Built-in 1.5 kV Magnetic Isolation Protection			
Industrial Protocols	◆ Ethernet: Modbus TCP Client (Master), Modbus TCP Server (Slave) ◆ Serial: Modbus RTU/ASCII Master, Modbus RTU/ASCII Slave ◆ Max. 16 connections under Modbus Master mode and 32 connections under Modbus Slave mode.			
Compliance	◆ EMC: EN 55032/35 ◆ EMI: CISPR 32, FCC Part 15B Class A ◆ EMS: IEC 61000-4-2 ESD: Contact: 4 kV; Air: 8 kV ◆ IEC 61000-4-3 RS: 80 MHz to 1 GHz: 3 V/m ◆ IEC 61000-4-4 EFT: Power: 1 kV; Signal: 0.5 kV ◆ IEC 61000-4-5 Surge: Power: 2 kV (Power Adapter), 1kV (Terminal Block); Signal: 1 kV ◆ IEC 61000-4-6 CS: 150 kHz to 10 MHz: 3 V/m; 10 kHz to 30 MHz: 3 to 1 V/m; 30 kHz to 80 MHz: 1 V/m ◆ IEC 61000-4-8 PFMF ◆ IEC 61000-4-11 DIPs ◆ Safety: UL 60950-1 and UL 62368-1 standards compliant ◆ RoHS			
Environmental				
Operating Temperature	0 – 60 °C			
Storage Temperature	-40 – 75 °C			
Humidity	5 – 95% RH, Non-condensing			
Physical Properties				
Housing	Metal			
Weight	0.20 kg (0.44 lb)	0.21 kg (0.46 lb)	0.21 kg (0.46 lb)	0.22 kg (0.48 lb)

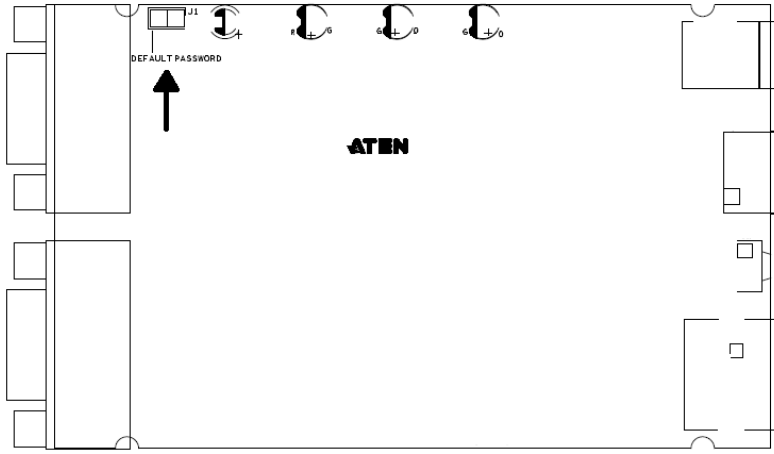
	SN3401	SN3402	SN3401P	SN3402P
Dimensions (L x W x H)	9.80 x 11.70 x 2.60 cm (3.86 x 4.61 x 1.02 in)			
Installation	◆ Desktop ◆ Wall Mounting ◆ Din-Rail Mounting ◆ Rack Mounting using the VE-RMK1U **Note:** The rack mounting kit (VE-RMK1U) is sold separately.			

Clear Login Information

If you are unable to perform an Administrator login (such as due to login credentials being corrupted or lost) you can clear the login information by doing the following.

Note: Performing this procedure also reverts all settings back to their factory default.

1. Power off the Secure Serial Device Server and remove its housing.
2. Use a jumper cap to short the jumper labeled **J1** (*DEFAULT PASSWORD*).



3. Power on the Secure Serial Device Server.
4. When the Status LED flashes, power off the device.
5. Remove the jumper cap from **J1**.
6. Close the housing and start the device.

   After powering on, you can use the default Administrator username and password to log in, see *Logging In*, page 23.

You will be prompted to change the password upon your first-time login after performing this procedure.

Troubleshooting

Operation problems can be due to a variety of causes. The first step in solving them is to make sure that all cables are securely attached and seated completely in their sockets.

In addition, updating the product's firmware may solve problems that have been discovered and resolved since the prior version was released. If your product is not running the latest firmware version, we strongly recommend that you upgrade. See *Firmware Update*, page 49, for upgrade details.

ATEN Standard Warranty Policy

The warranty policy may vary by product category and region of purchase. For details, please visit ATEN's official website, select your purchase counties/ regions and then go to the Support Center, or contact your local ATEN sales representative for further assistance.