Simply Better Connections

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

Secure Device Server

User Manual

EMC Information

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.

This 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.

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.

About This Manual

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

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

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

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

Chapter 1, Introduction, introduces Secure 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 Device Server.

Chapter 3, Network Configuration and Login, explains how to log into the Secure Device Server from a web browser.

Chapter 4, Web Console, explains the administrative procedures that are employed to configure the Secure Device Server's working environment.

Chapter 5, User Management, details login accounts and third-party authentication services supported, such as RADIUS.

Chapter 6, Port Operating Modes, introduces the Secure Device Server's operating modes, and explains the purpose of each.

Chapter 7, Port Access, describes how to access the COM ports of the Secure Device Server and start SNViewer.

Chapter 8, Remote Terminal Operation, describes how the Secure Device Server can be accessed via remote terminal sessions, such as Telnet, SSH, and PuTTY.

Chapter 9, Virtual Serial Port Manager, shows how to install the virtual COM port driver and to set up and manage the virtual COM port.

Appendix, provides technical and troubleshooting information at the end of the manual.

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.

Package Contents

SN3001 / SN3002 / SN3401 / SN3402

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

1 Secure 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 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*

Check to make sure that all of the components are present and in good order. If anything is missing, or was damaged in shipping, contact your dealer for assistance.

Read this manual thoroughly and follow the installation and operation procedures carefully to avoid any damage to the Secure Device Server or to any other devices on the Secure Device Server installation.

* Features may have been added to the Secure Device Server since this manual was released. Please visit our website to download the most up to date version of the manual.

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

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.

Contents

Chapter 4. Web Console

Chapter 5. User Management

Appendix

This Page Intentionally Left Blank

Chapter 1
Introduction

Overview

The Secure 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 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 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 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 Device Server ensures secured data transmission over both private and public networks.

Installing the Secure 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 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

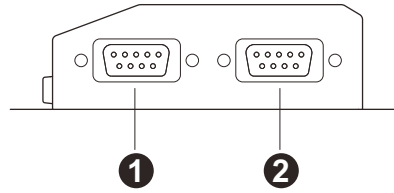
System Management

- 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

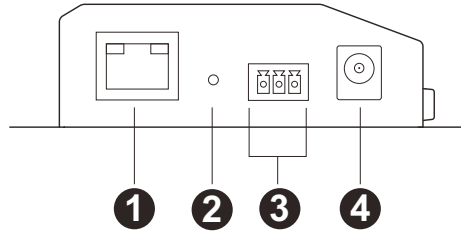
SN3001 / SN3001P / SN3002 / SN3002P

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)

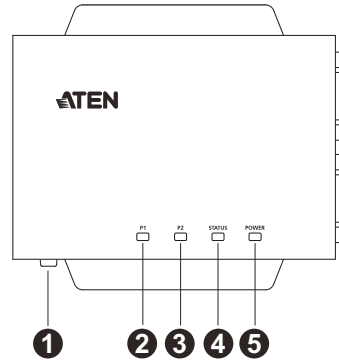
Rear View



No.	Component	Description
1	LAN port	Connects the Secure 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 Device Server to power via DC electric leads and the terminal block provided.

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

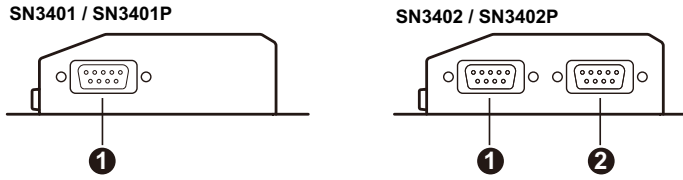
Top View



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 Device Server is powered and ready.

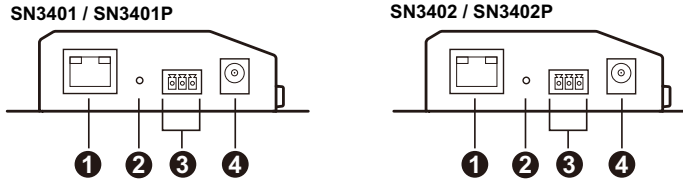
SN3401 / SN3401P / SN3402 / SN3402P

Front View



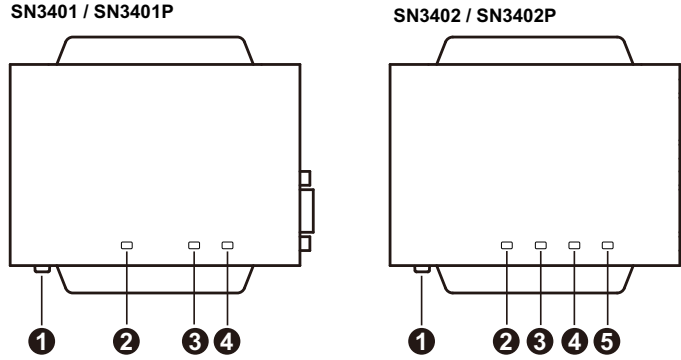
No.	Component	Description
1	serial port 1	Connects to an RS-232 / RS-422 / RS-485 serial device.
2	serial port 2	Connects to a second RS-232 / RS-422 / RS-485 serial device. (SN3402 / SN3402P only)

Rear View



No.	Component	Description
1	LAN port	Connects the Secure 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 Device Server to power via DC electric leads and the terminal block provided.

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 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 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 87. Please review it before proceeding.
2. Make sure the power of all devices to be connected have been turned off.

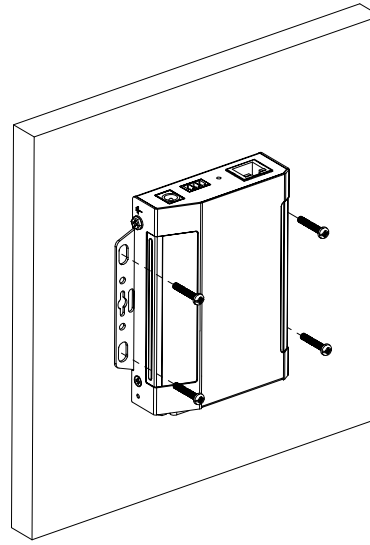
Placement Options

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

Wall Mount

To wall mount the Secure 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.

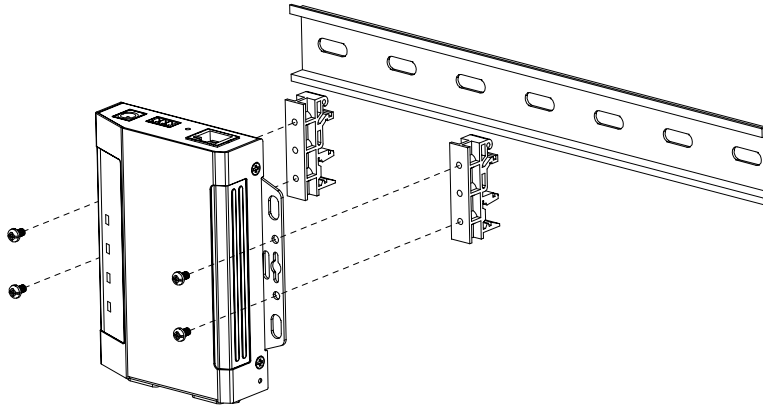


DIN Rail Mount

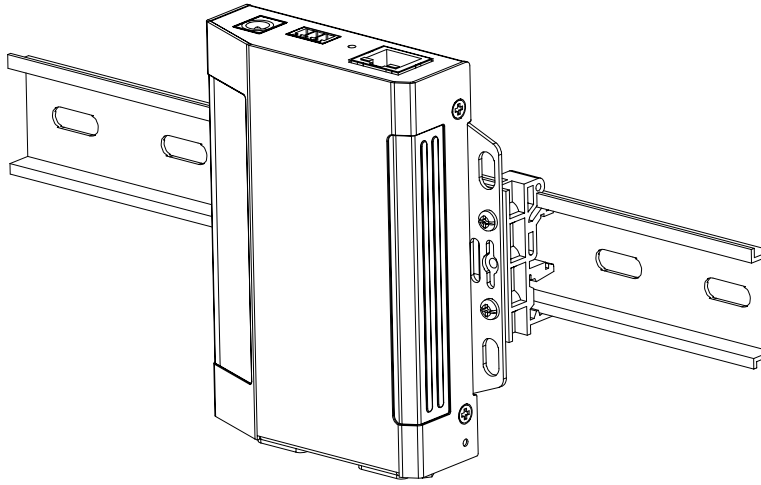
Use the DIN rail mount kit included to mount the Secure Device Server onto a DIN rail, as instructed below:

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.

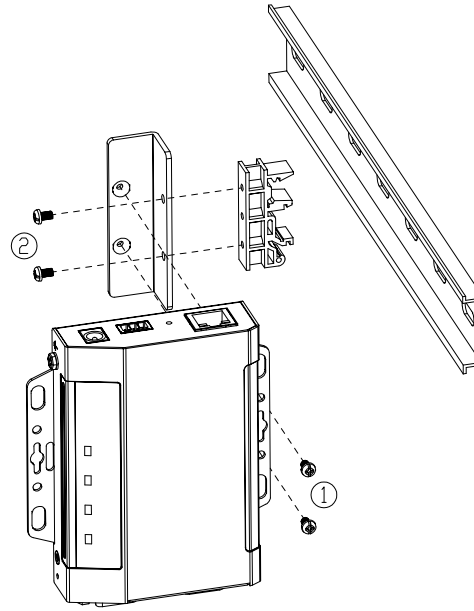


2. Hang the unit onto the DIN rail.

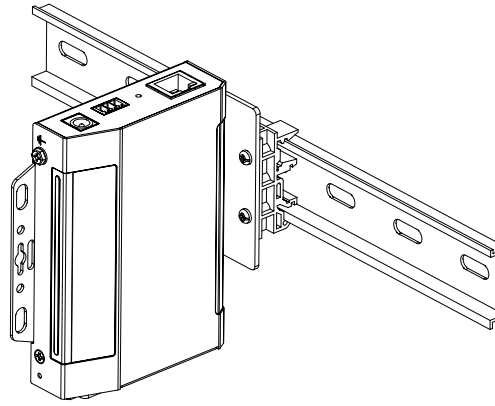


Perpendicular DIN Rail Mount

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.



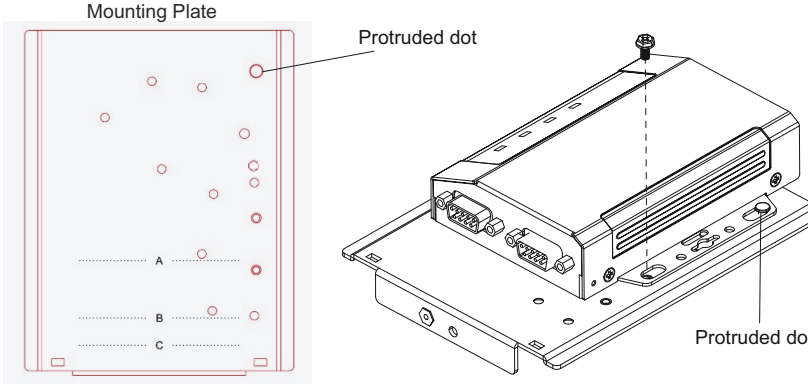
3. Hang the unit onto the DIN rail.



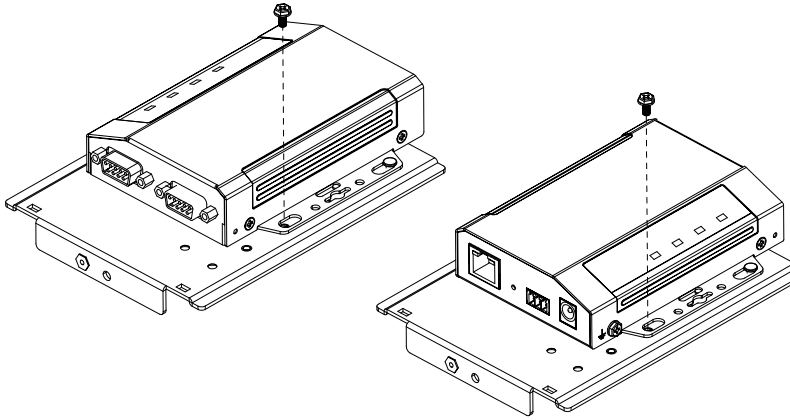
Rack Mount

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

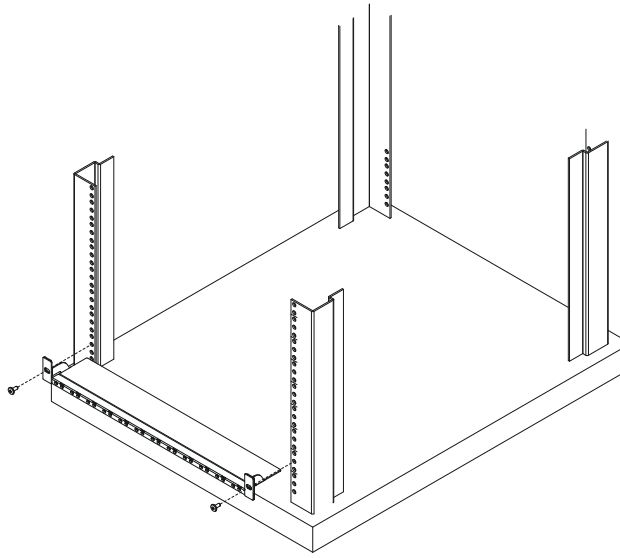
1. Place the device onto the mounting plate while latching one of its rack ears onto the plate's protruded dot, as illustrated below.



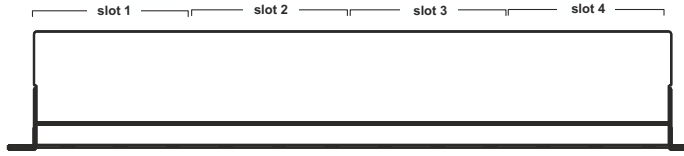
2. Secure the device to the mounting plate using the hexagon head screw supplied. Users can secure the Secure Device Server either with its serial port(s) facing inward or outward.



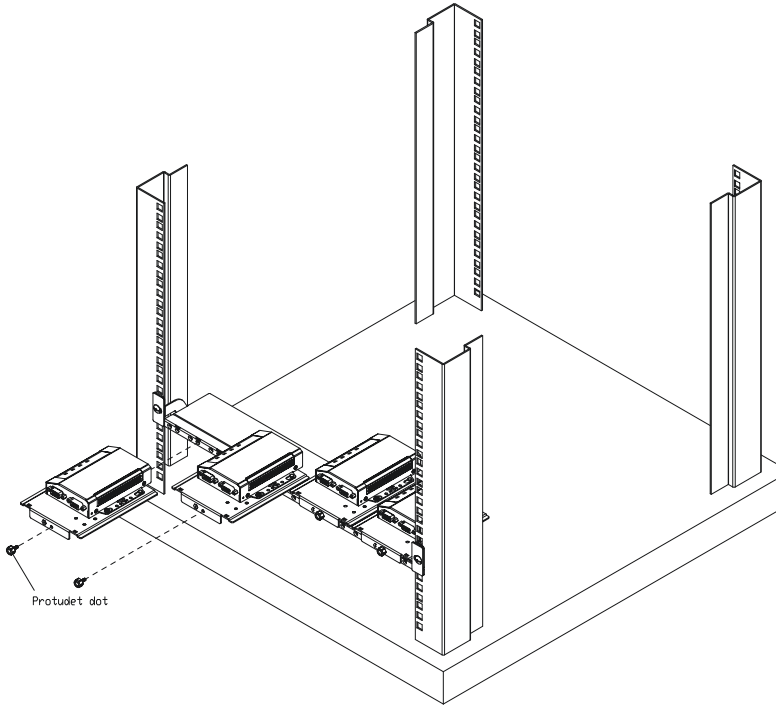
3. Position and align the holes on the VE-RMK1U frame with that of the rack, and secure the frame onto the rack with 2 self-supplied screws, as illustrated below.



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

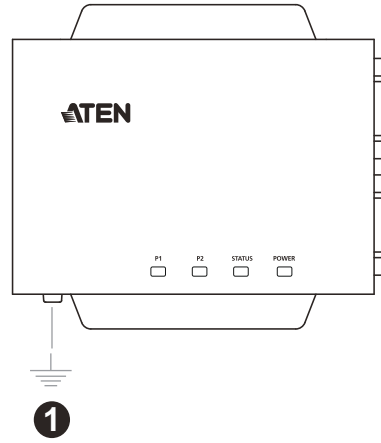


Note: Up to 4 Secure Device Servers can be secured onto a VE-RMK1U frame.

Installation

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

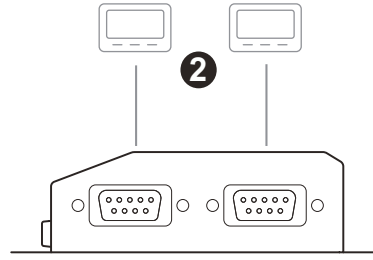
1. Use a grounding wire to ground the unit by connecting one end of the grounding terminal and the other end to a suitable grounded object.



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.



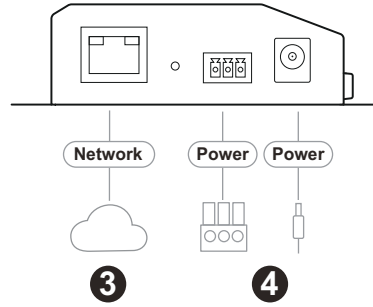
3. Connect the unit's LAN port to the network using a Cat 5e/6 cable. For SN3001P / SN3002P / SN3401P / SN3402P (PoE 802.3af compliant), users can simultaneously supply power to the unit through a PoE switch and skip 4.

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 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 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

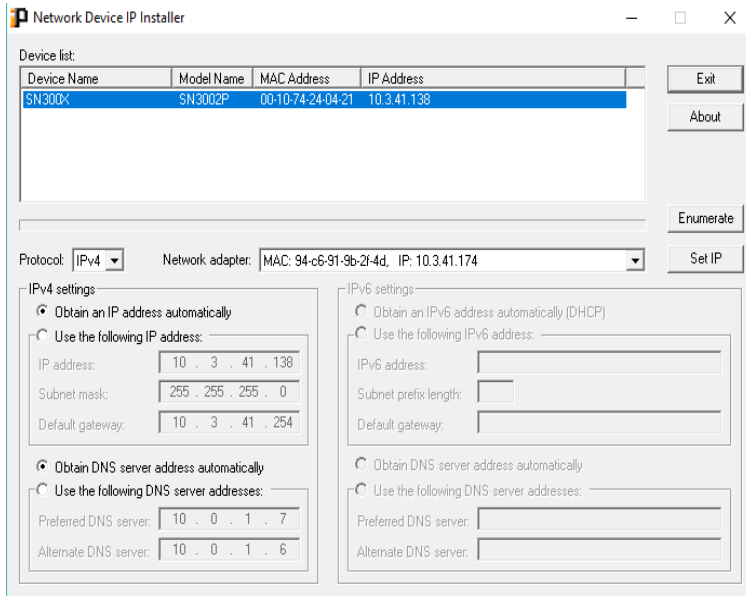
Before you start, make sure the PC you're using is within the same LAN as the Secure Device Server.

There are two methods for determining / setting the IP address of your Secure 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 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 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 Device Server's MAC address is located on its bottom panel.

4. To check the IP address of the Secure 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 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 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 21).
4. On the Secure 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

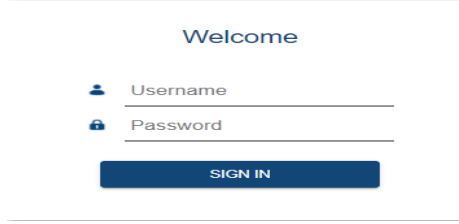
To access Secure Device Server from a web browser, do the following:

1. Open your browser and specify the IP address of the Secure 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 Device Server's IP address are described in *IP Address Determination* (see page 19).

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

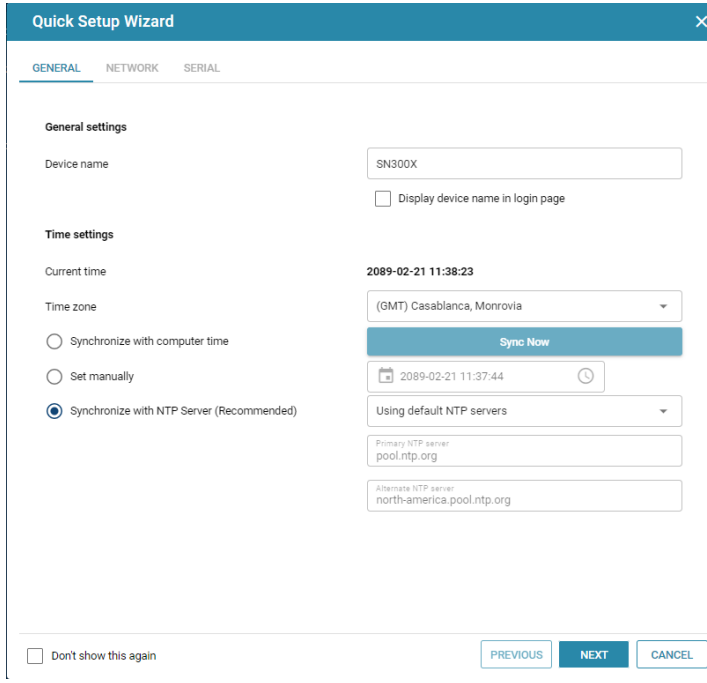
5. Upon first-time login, users are required to change the login password of the Secure Device Server.

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

Quick Setup Wizard

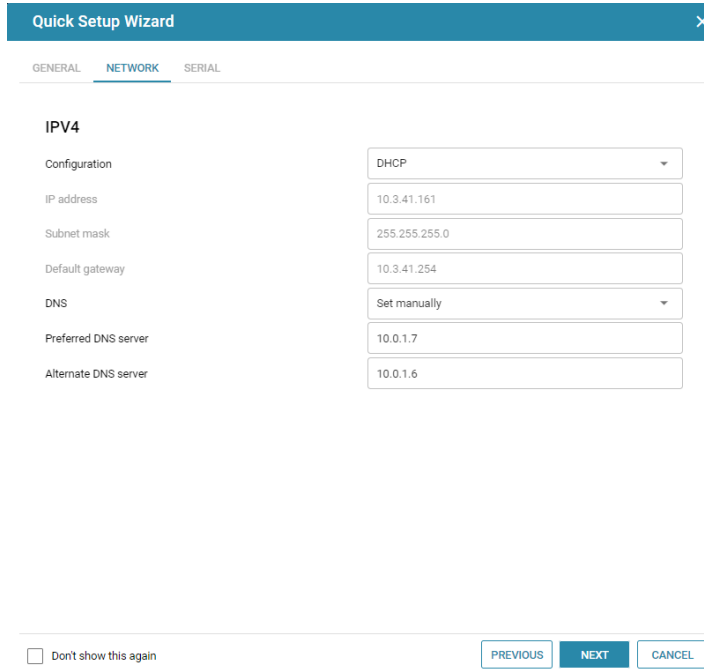
The *Quick Setup Wizard* gets you started with the basic settings of the Secure Device Server.

General



Item	Description
Device name	Displays the name of the Secure 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.

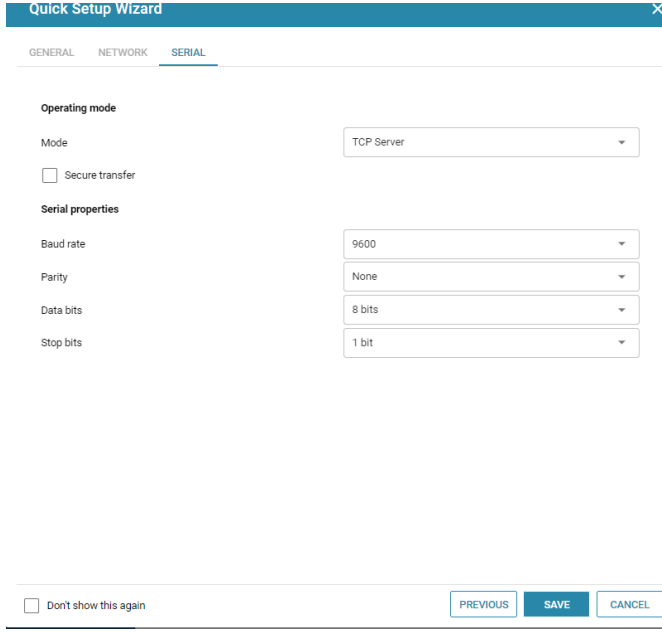
Network



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

Serial

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



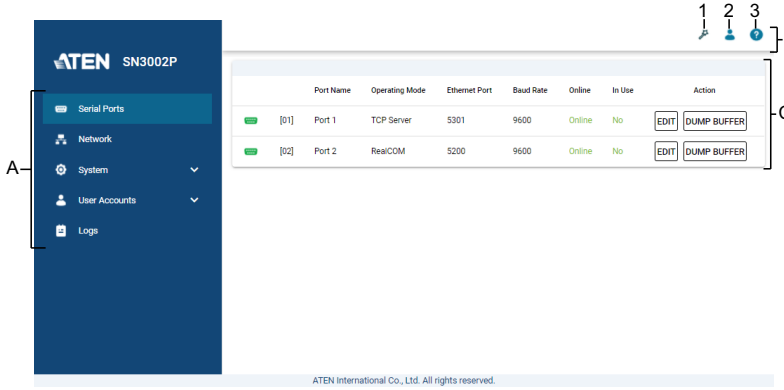
Item	Description
Mode	Selects the operation mode for the Secure Device Server's serial port(s). See *Port Operating Modes*.
Secure transfer	Check for secured data transmission.
Baud rate	Selects the serial ports' data transfer speed.
Parity	Selects to check the integrity of the data transmitted, which 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 Device Server's web console main screen is displayed. See *Web Console* for details.

Chapter 4
Web Console

Web Interface

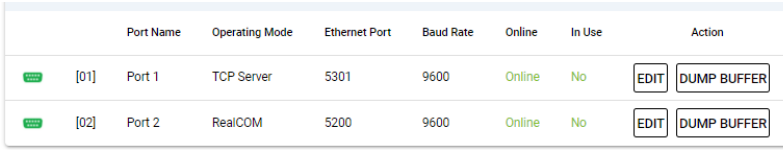
The web interface of the Secure Device Server and its components are shown and explained below:



No.	Item	Description
A	Sidebar Menu	Provides a selection of configuration pages. Click to select a configuration page and/or expand submenus.
B	Task Bar	Contains access to the Quick Setup Wizard, user settings (including logout) and the device info.
C	Interactive Display Panel	Displays the configuration page currently selected.
1	Quick Setup Wizard	Takes users through the basic settings of the Secure Device Server. See p. 22.
2	Personal	Click to display the user currently logged in, the time of login, user preference option, change password, and logout options. Click *Preferences* to change the language of the interface. Click *Change password* to change the password for the current user account.
3	About	Click to display the model number and the firmware version of the device.

Serial Ports

The Serial Ports page provides an overview of the Secure Device Server's serial COM port(s), including its settings and the serial devices connected.

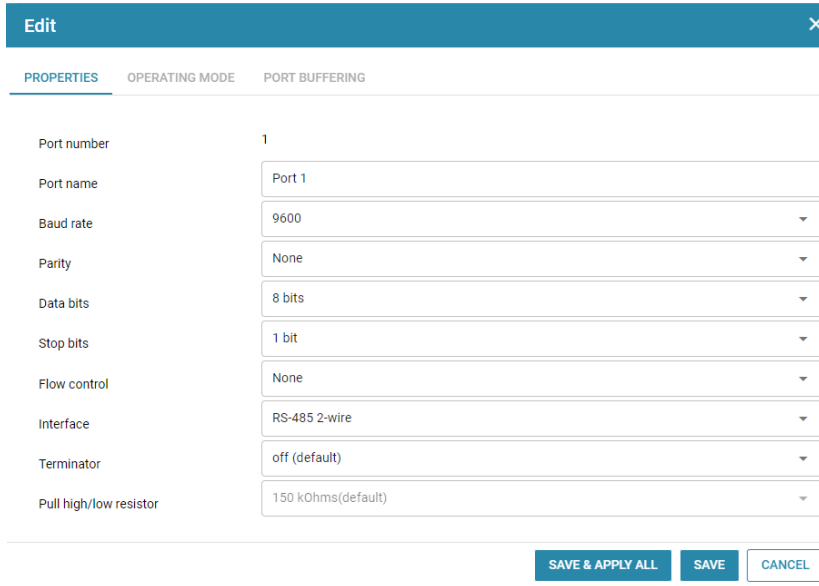


Item	Description
	Indicates whether the RS-232 serial port is online or offline. **Note:** This function is only applicable to RS-232 connections. For any RS-422 or RS485 connection, a gray icon shows in this field.
Port Name	Displays the name of the serial port.
Operating Mode	Displays the current operating mode of the serial port. See *Operating Mode*, page 30.
Ethernet Port	Displays the network port value of the serial port.
Baud Rate	Displays the baud rate of the serial port.
Online	Indicates whether the RS-232 serial port is online or offline. **Note:** This function is only applicable to RS-232 connections. For any RS-422 or RS485 connection, a gray icon shows in this field.
In Use	Indicates whether the serial port has active data transmission.
Action	◆ *Edit*: Click to edit the serial port's settings. ◆ *Dump Buffer*: Click to download the port activity logs of the serial port from the device as a *.txt* file. This function is only available when the port activity logs are saved to the device's memory. See *Port Buffering*, *page 28*. ◆ *Telnet / SSH:* Click to configure the Secure Device Server or access and control the connected serial device via Telnet / SSH protocol. This function is only available when the port's operating mode is set to Console Management. See *Operating Mode*, page 30, and *Telnet / SSH*, page 70. **Note:** The maximum number of simultaneous connections to any one serial port is 16.

Editing Serial Ports

Click the **EDIT** button to modify the settings of a serial COM port. The edit window, with *Properties*, *Operating Mode*, and *Port Buffering* tabs, appears.

Properties



Item	Description
Port number	Displays the number of the serial port.
Port name	Sets the name of the serial port.
Baud rate	Selects the serial ports' data transfer speed. Default = "9600"
Parity	Selects to check the integrity of the data transmitted, which shall match the parity setting of the serial device connected. Default = "None"
Data bits	Selects the number of bits used to transmit one character of data, and matching the data bit setting of the serial device connected. Default = "8"
Stop bits	Selects the stopping bit, indicating a character has been transmitted, and matching the stop bit setting of the serial device connected. Default = "1"
Flow control	Selects how the data flow is controlled, and matching the flow control setting of the serial device connected. Default = "None"
Interface	Sets the type of serial interface for the COM port.

Item	Description
Terminator	Enable this setting to prevent reflections of RS-485 signals and data corruption.
Pull high/low resistor	Configure the pull high/low resistors correctly to for an RS-485 connection.

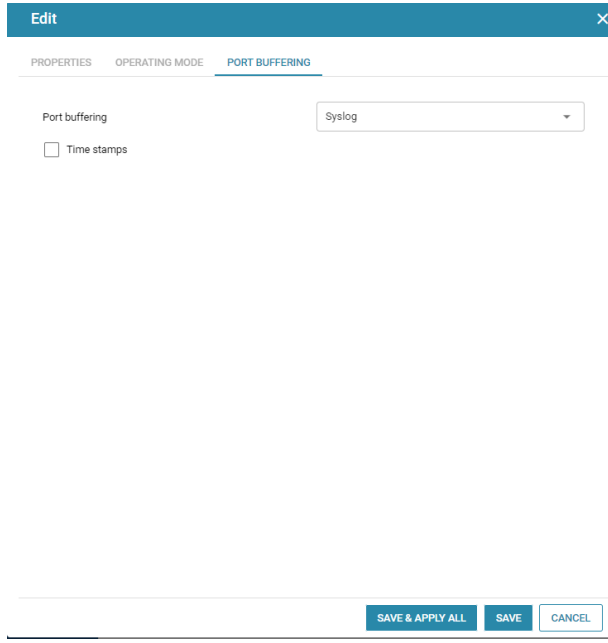
Click **Save** for the changes to take effect.

Optionally click **Save & Apply All** to apply the same settings to all of the Secure Device Server's serial ports.

Port Buffering

Port buffering creates a log of the activities conducted when a port is accessed. You can save the log to the internal memory of the Secure Device Server, for up to 128 KB, or a Syslog server.

To enable Port Buffering, select **Memory** or **Syslog Server** from the drop-down list in the *Port Buffering* tab. Optionally check *Time Stamps* to add time stamps to the logs created.



Click **Save** for the changes to take effect.

Note: Before Syslog can be selected, make sure to enable Syslog server, see *Syslog*, page 44.

Optionally click **Save & Apply All** to apply the same settings to all of the Secure Device Server's serial ports.

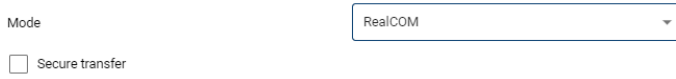
Operating Mode

The Operating Mode tab determines how the serial COM port of the Secure Device Server is accessed.

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

For detailed information of the various port operating modes, see Chapter 6, *Port Operating Modes*.

■ Real COM



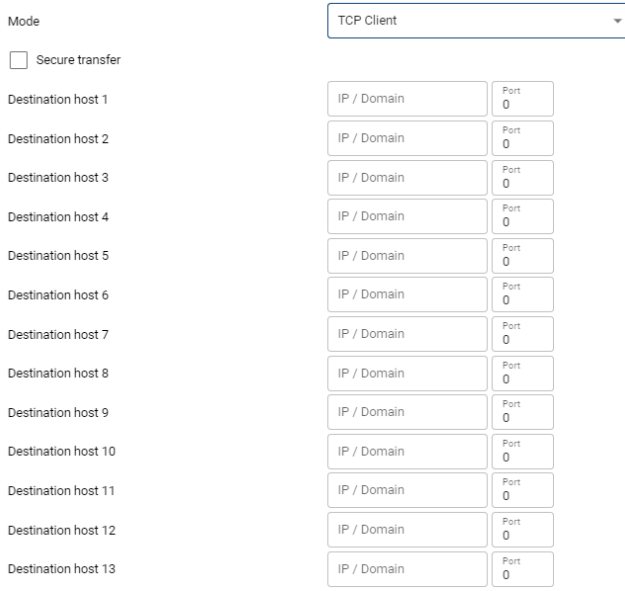
Check **Secure transfer** to encrypt all data being transfered, using SSL, through the serial COM port.

Note: Real COM operating mode must be used in conjunction with ATEN's Virtual COM Port Utility, see *Virtual Serial Port Manager*, page 79.

■ TCP Server

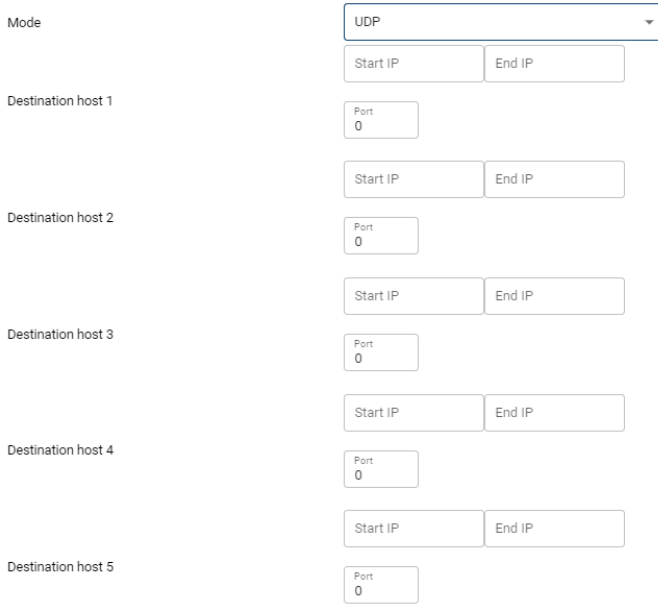
Item	Description
Secure transfer	Check to encrypt all data being transferred between Secure Device Servers' serial COM ports via TCP Server-Client modes, using SSL.

■ TCP Client



Item	Description
Secure transfer	Check to encrypt all data being transferred between Secure Device Servers' serial COM ports via TCP Client-Server modes, using SSL.
Destination host	Enter the IP address and service port of a destination host for data transmission. The device can simultaneously send data to up to 16 destination hosts.

■ UDP



Item	Description
Destination host	Enter the range of IP address(es) and the port values for connections to destination hosts via the UDP protocol. The Secure Device Server can simultaneously connect to up to 16 destination hosts.

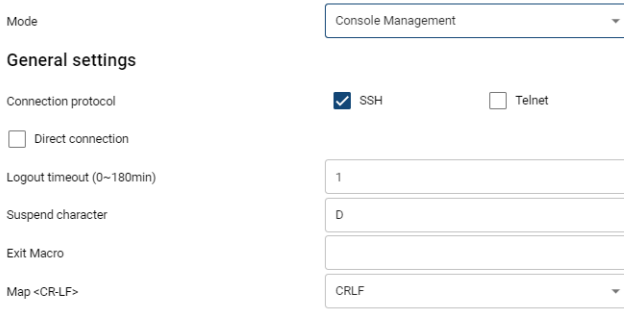
■ Serial Tunneling Server

Item	Description
TCP port	Sets the TCP/IP port value of the serial port operating as a serial tunneling server.
Secure transfer	Check to encrypt all data being transferred through the serial COM ports between two Secure Device Server via Serial Tunneling Server-Client., using SSL.

■ Serial Tunneling Client

Item	Description
Destination	Enter the IP address and port value of the serial tunneling server for sending data to.
Secure transfer	Check to encrypt all data being transferred through the serial COM ports between two Secure Device Servers via Serial Tunneling Client-Server, using SSL.

■ Console Management



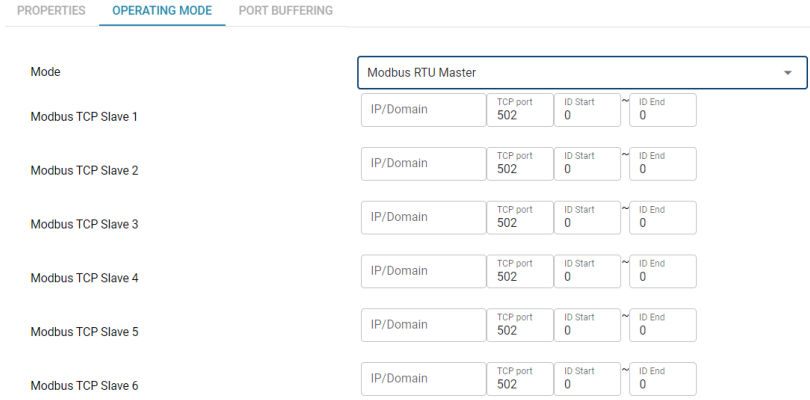
Item	Description
Connection protocol	Check / uncheck to enable / disable SSH and Telnet connection protocols.
Direct connection	Select for Console Management Direct operating mode. For detailed information on the various available operating modes, see Chapter 6, *Port Operating Modes*.
Logout timeout (0 ~ 180 min)	Automatically logs out user(s) accessing when there is no input by the user for the amount of time set. “0” means the user will never be automatically logged out.
Suspend character	The suspend character is used to bring up the Suspend Menu in Telnet sessions. Valid characters include A – Z, except for H, I, J, and M.
Exit Macro	Sets the Exit Macro that will be executed upon exiting the serial device.
Map <CR-LF>	Select to send Carriage Return (CR) and/or Line Feed (LF) signals.

■ Modbus RTU/ASCII Master

Select this option to set the Secure Device Server as an RTU/ASCII mater device. An RTU/ASCII master device can initiate communication to up to 16 slave devices at the same time. Optionally fill in up to 16 sets of settings for TCP slave devices.

Note:

- This mode is only applicable to SN3401 / SN3401P / SN3402 / SN3402P.
- For SN3402 / SN3402P, the selected operation mode will be applied to both serial ports on the unit.



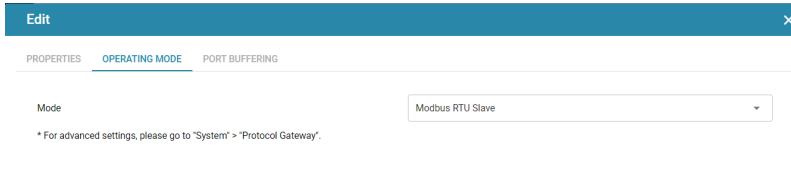
Item	Description
IP/Domain	Enter the IP address of the slave device.
TCP port	Enter the TCP port for the slave device.
ID Start	Enter the start and end ID of the slave device(s). A valid range is 1 to 247.
ID End	

■ Modbus RTU/ASCII Slave

Select this option to set the Secure Device Server as an RTU/ASCII slave device. An RTU/ASCII slave device can receive requests from up to 16 master devices.

Note:

- This mode is only applicable to SN3401 / SN3401P / SN3402 / SN3402P.
- For SN3402 / SN3402P, the selected operation mode will be applied to both serial ports on the unit.

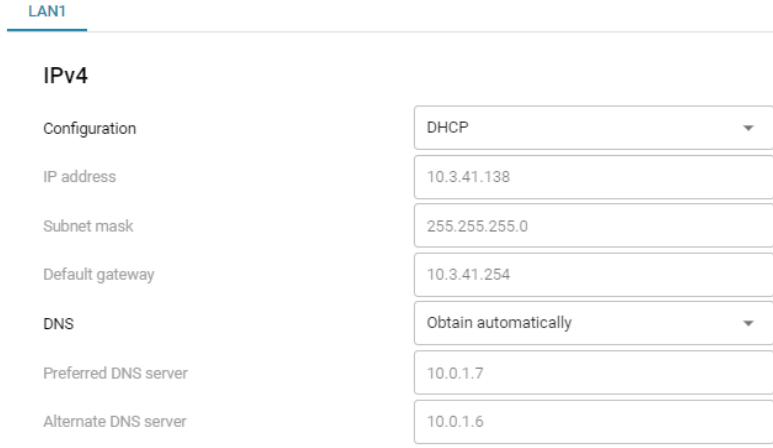


■ Disable

Select to disable the use of the serial port.

Network

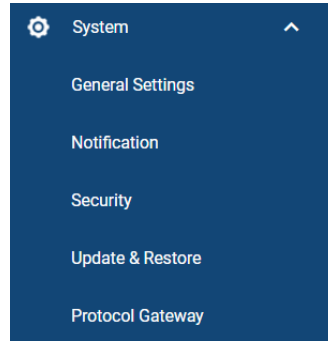
The Network page contains the network settings of the Secure Device Server, as described in the table below.



Item	Description
Configuration	Selects the type of configuration for setting the Secure Device Server's IP address, from DHCP or Static IP.
IP address Subnet mask Default gateway	For static IP, set the IP address, subnet mask, and gateway of the device according to your network environment.
DNS	Selects the method of obtaining DNS server, from *Obtain automatically* or *Set manually*.
Preferred DNS server Alternate DNS server	For setting the DNS server manually, type the preferred and alternate DNS server address for the device.

System

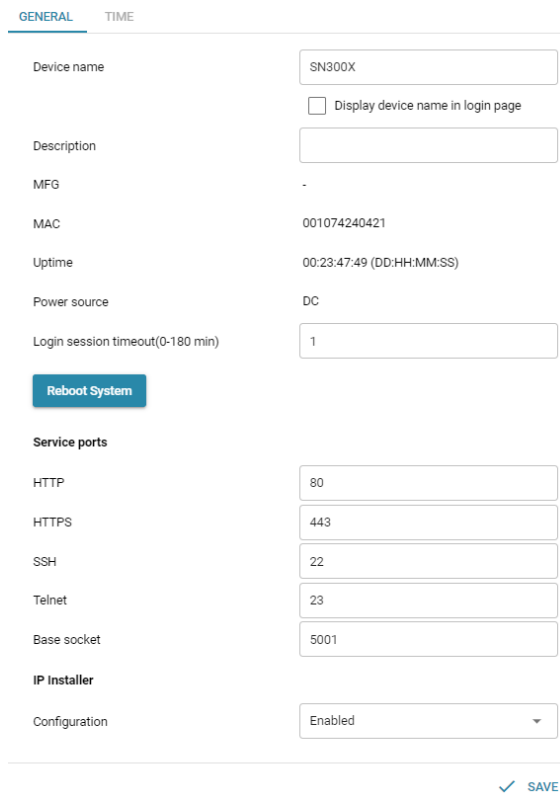
Click to expand the System submenu for all of the system related settings of the Secure Device Server, including **General settings**, **Notification**, **Security**, **Update & Restore**, and **Protocol Gateway**.



General Settings

The General Settings contains 2 tabs: *General* and *Time*.

General



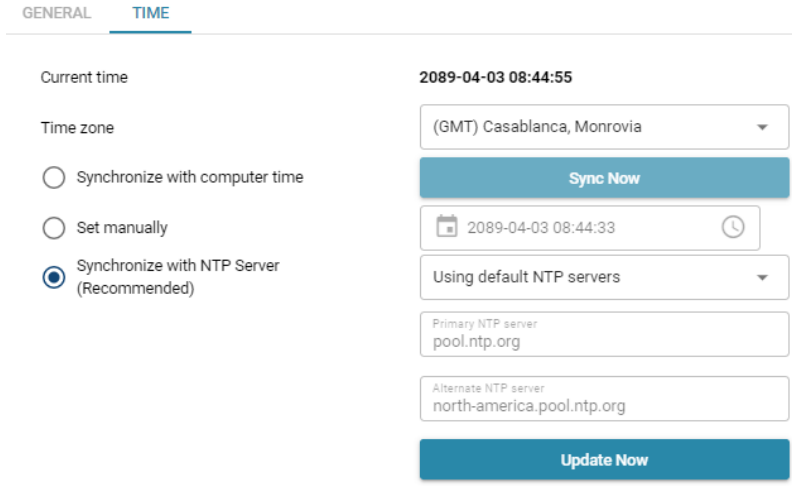
Item	Description
Device name	Sets the device name for the Secure Device Server.
Description	Enter a description for the device if needed.
MFG	Displays the MFG (Manufacturing Number) of the device. **Note:** The Manufacturing Number is an internal serial number used by ATEN's factory and technical support staff to identify products.
MAC	Displays the MAC address of the Secure Device Server.
Uptime	Displays the amount of time the device has been running for.
Power source	Displays the device's current power source.

Item	Description
Login session timeout (0 ~ 180 min)	Automatically logs out user(s) when there are no actions done on the Secure Device Server's web interface for the amount of time set. "0" means the user will never be automatically logged out.
Reboot System	Reboots the Secure Device Server.
Service ports	Sets the service port values for the following: ◆ *HTTP*: used for browser access (default = 80) ◆ *HTTPS*: used for secure browser access (default = 443) ◆ *SSH*: used for SSH access (default = 22) ◆ *Telnet*: used for Telnet access. (default = 23) ◆ *Base socket*: used for receiving and accepting TCP connections (default = 5001). For example, when the base socket value is 5001, the device's TCP port value for Port 1/2 via Telnet and SSH will be 5001/5002 and 5101/5102, respectively. **Note:** 1. Valid entries for all service ports are from 1 – 65535. 2. A system restart is required when any of the service port settings have been changed.
IP Installer Configuration	Select to determine if the IP Installer utility can detect for and/or change the Secure Device Server's IP address. ◆ *Enabled*: IP Installer can detect for and change the unit's IP address. ◆ *View Only*: IP Installer can only detect for but unable to change the unit's IP address. ◆ *Disabled*: IP Installer cannot detect for and change the unit's IP address.

Click **Save** for the changes to take effect.

Time

The Time tab contains the time settings of the Secure Device Server, as described in the table below.

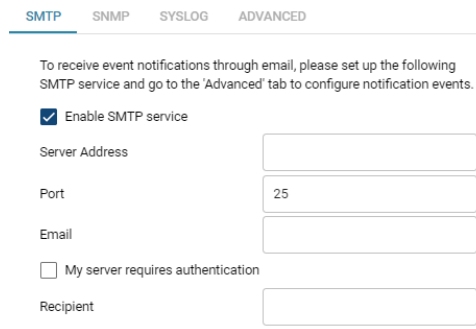


Item	Description
Time zone	Select one of the following to set the time of the Secure Device Server. ◆ *Synchronize with computer time:* Synchronizes with the time of the client PC. ◆ *Set manually:* Manually set a desired time for the device. ◆ *Synchronize with NTP Server:* Synchronizes the time of the device to an NTP server. **Note:** ◆ If you use *Synchronize with computer time* or *Set manually*, the time settings must be reconfigured whenever the Secure Device Server is restarted. ◆ It is recommended to use the **Synchronize with NTP Server** setting to avoid time discrepancies especially when the Secure Device Server has operated for a while.

Notification

The Notification page contains 4 tabs: *SMTP*, *SNMP*, *Syslog*, and *Advanced*.

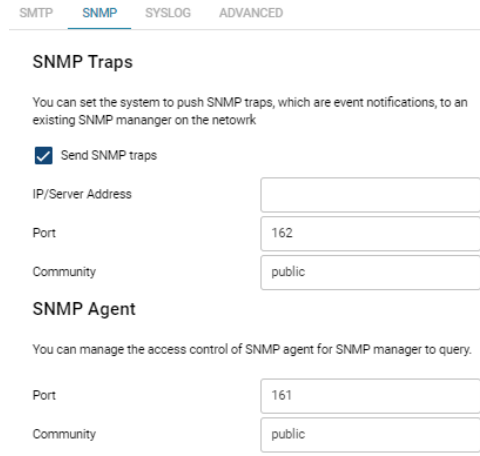
SMTP



Item	Description
Enable SMTP service	Check to enable SMTP service for sending event notifications via email, as specified by the *Advanced* tab (see page 45).
Server Address / Port	Enter the SMTP server's address and service port value.
Email	Enter the sender's email address.
My server requires authentication	Check if your SMTP server requires authentication and enter a valid username and password.
Recipient	Enter the recipient's email address.

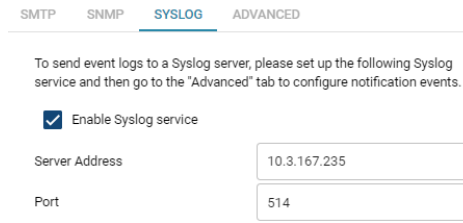
SNMP

Note: Before SNMP can be used, make sure to **Enable SNMP Agent service** in *System* > *Security* > *Security Level*.



Item	Description
Send SNMP traps	Check to enable SNMP service for sending SNMP trap event notifications, as specified by the *Advanced* tab (see page 45). SNMP v1 and v2c are supported.
IP/Server Address	Enter the IP/server address to receive the SNMP trap events.
Port	Enter the service port of the server to receive SNMP trap events.
Community	Enter the SNMP community.
SNMP Agent	Enter the service port and community for an SNMP agent.

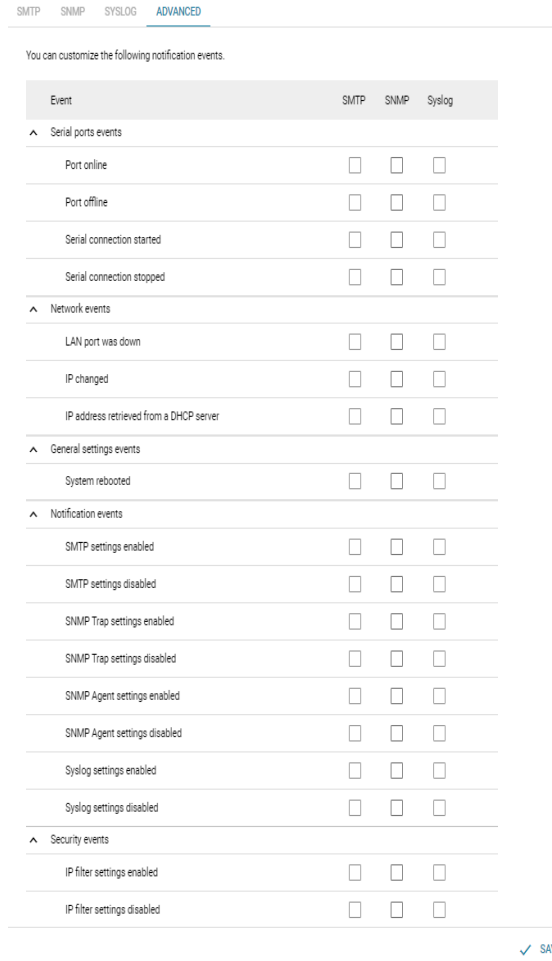
Syslog



Item	Description
Enable Syslog service	Check to enable Syslog service for sending event notifications to a Syslog server, as specified by the *Advanced* tab (see page 45).
Server Address / Port	Enter the Syslog server's address and port value.

Advanced

The Advanced tab sets the types of event notifications to be sent via SMTP, SNMP, and/or Syslog server. Options include but are not limited to the example given below



Check the SMTP / SNMP / Syslog checkboxes next to each event type for sending SMTP / SNMP / Syslog notifications when those events occur.

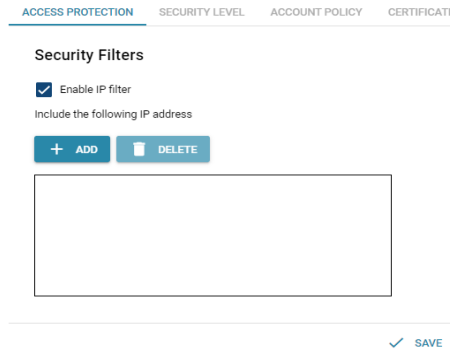
Note: For the specified notifications to be sent, make sure the required SMTP / SNMP / Syslog service have been properly configured.

Security

The Security page contains the security settings and certificate information of the Secure Device Server, distributed into 4 tabs: *Access Protection*, *Security Level*, *Account Policy*, and *Certificate*.

Access Protection (IP Filter)

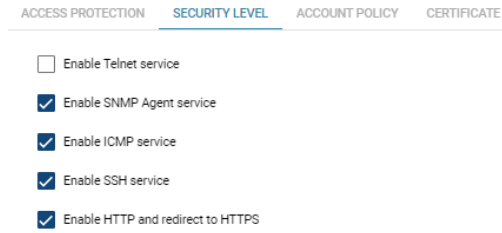
The Access Protection function sets IP filters to allow remote access only from the IP address(es) added, and denying all other remote access.



To enable exclusive access only for certain IP address(es), check **Enable IP filter**, and click the **ADD** button to add the desired IP address(es).

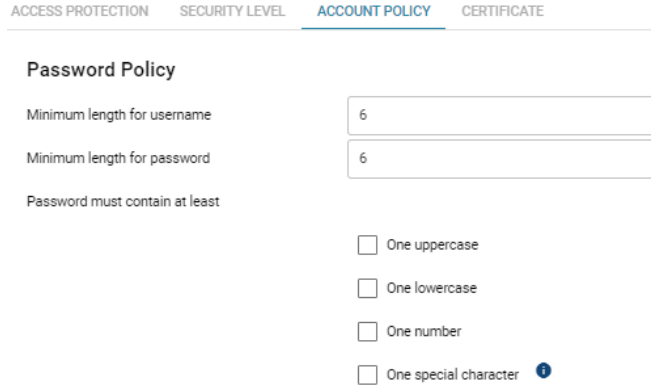
Click **Save** for the changes to take effect.

Security Level



Item	Description
Enable Telnet / SNMP Agent / ICMP / SSH service	Check or uncheck to enable or disable Telnet / SNMP Agent / ICMP / SSH service. **Note:** A system restart is required when the SNMP Agent setting has been changed.
Enable HTTP and redirect to HTTPS	Check to enable HTTP and automatically redirect all HTTP access to HTTPS, for secured web browser access. **Note:** A system restart is required when this setting has been changed.

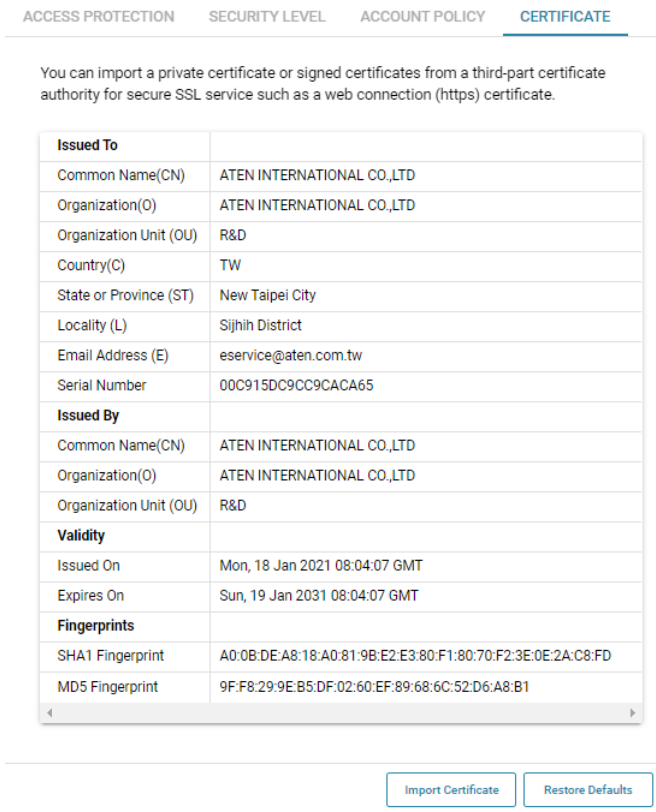
Account Policy



Item	Description
Minimum length for username / password	Sets the minimum number of characters required for all newly set login usernames / passwords. Default = “6”
Password must contain at least	Check to require at least one uppercase / lowercase / number / special character for all newly set passwords.

Security Certificate

The Security Certificate tab displays the information of the security certificate used.



For enhanced security, users can use their own private encryption key and signed certificate, rather than the default ATEN certificate.

There are two methods for establishing your private certificate:

- Generating a Self-Signed Certificate

  If you wish to create your own self-signed certificate, a free utility — openssl.exe — is available for download over the web.

- Obtaining a CA-Signed SSL Server Certificate

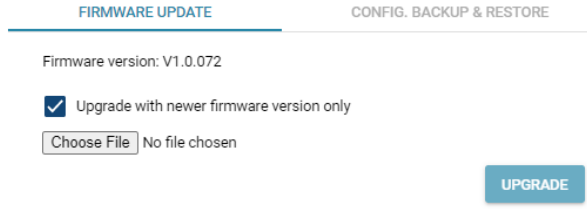
  To ensure security, it is recommended to use a third-party CA-signed SSL certificate obtained from a CA (Certificate Authority) website. Make sure to save the obtained certificate and its private encryption key on the PC.

Item	Description
Import Certificate	Imports a private or CA-signed security certificate from the PC.
Restore Defaults	Reverts to using the default ATEN certificate.

Update & Restore

The Update & Restore page can upgrade the Secure Device Server's firmware and back up and/or restore its device settings.

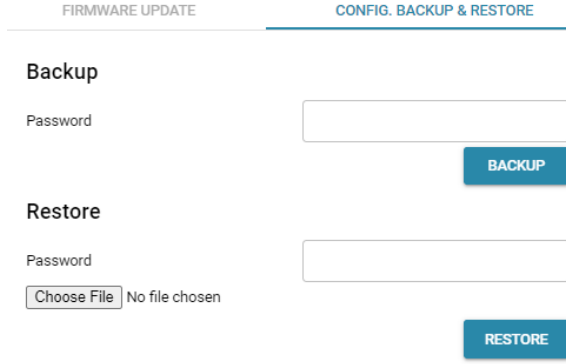
Firmware Update



Item	Description
Firmware version	Displays the current firmware version.
Upgrade with newer firmware version only	Check to only permit firmware upgrades with newer firmware versions.
Choose File	Selects the firmware update file to be used for upgrading.
UPGRADE	Upgrades the device firmware with the firmware file selected.

Backup & Restore

The Backup & Restore page allows users to back up or restore the system settings of the Secure Device Server.



■ Backing up System Settings

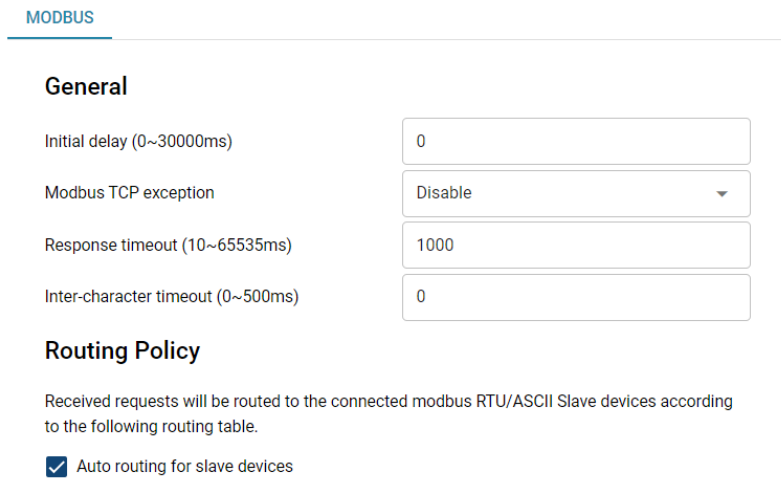
To back up the system settings of the Secure Device Server, enter a *Password*, which will be used for restoring, and click **Backup** to save the system setting backup file, as *System.conf*, to the PC, which also include account-related settings, such as passwords and user privileges.

■ Restoring System Settings

To restore a previously backed up system settings file, enter its *Password*, click *Choose File* to locate it on the PC, and click **Restore**.

Protocol Gateway

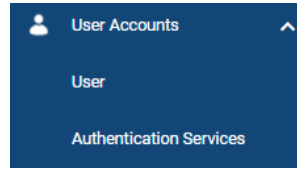
Use this page to configure the settings for Modbus communication.



Item	Description
Initial delay	Sets a duration that the Modbus mater needs to wait before it can send its first request to a slave device. This is used to reduce repeated exception during the initial boot-up, especially when some slave devices take more time to boot up than others in the environment.
Modbus TCP exception	Enable this setting for the Secure Device Server to be able to return an exception response from the Modbus slave when the request is not recognizable by the slave or when an error occurs while sending the request.
Response timeout	Sets the time limit for receiving a response from a Modbus slave device before the mater device gives up the request and starts sending the next one.
Inter-character timeout	Sets the time limit between each character of a request. If the time is out before all the characters of a request is received, the request will be discarded.
Auto-routing	Select this setting for the Secure Device Server to automatically routes any received requests to the connected RTU/ASCII slave devices. If disabled, received request will only be forwarded to the specified slave device (ID).

User Accounts

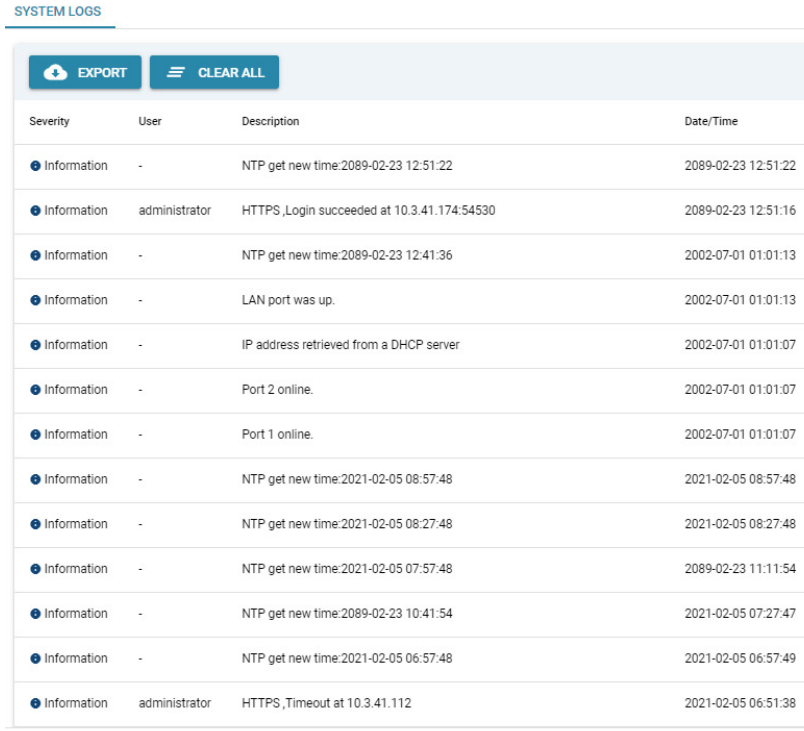
The *User Accounts* submenu consists of **User** and **Authentication Services** pages, which allow users to add/edit login accounts or utilize third-party authentication services for managing the user accounts of the Secure Device Server, respectively.



For details on configuring user accounts and third-party authentication services, see Chapter 5, *User Management*.

Logs

The Logs page lists all of the system log information of the Secure Device Server.



Item	Description
Export	Exports and downloads the logs onto the PC as a *log.txt* file.
Clear All	Clears all log information.

Up to 2048 logs can be stored and displayed on this page.

This Page Intentionally Left Blank

Chapter 5
User Management

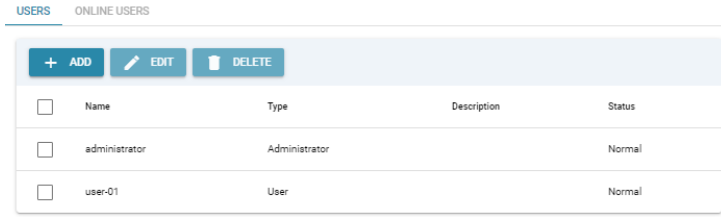
Overview

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

User

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

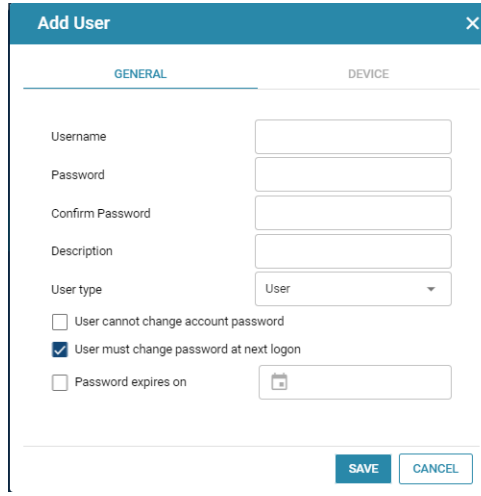
User Type	Role
Administrator	Able to access and configure all serial ports, and manage other login accounts
User	Only able to access and/or configure the authorized serial ports, as permitted by the administrator, and unable to configure any of the device's system settings.



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

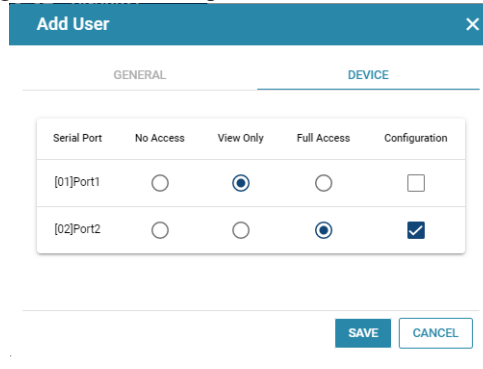
1. Click **User Accounts** > **User** > **Users** on the web interface of the Secure Device Server.
2. Click **Add**. The *Add User* window's **General** tab appears. Enter the required fields, as described in the table below.



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 56, then click **Save**.

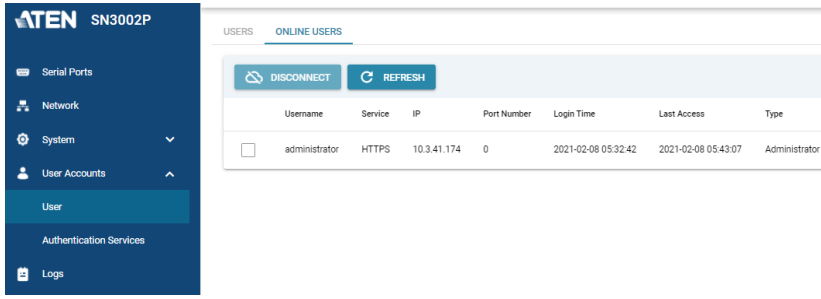
Deleting Users

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 Device Server.



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

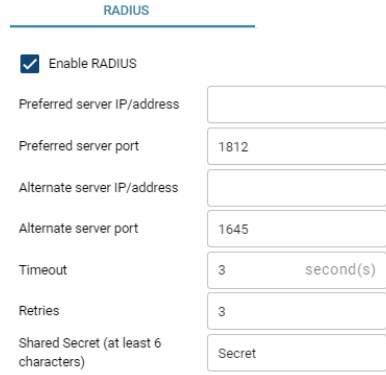
Authentication Services

The Secure 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 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 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 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 Device Server for the user.

Chapter 6
Port Operating Modes

Overview

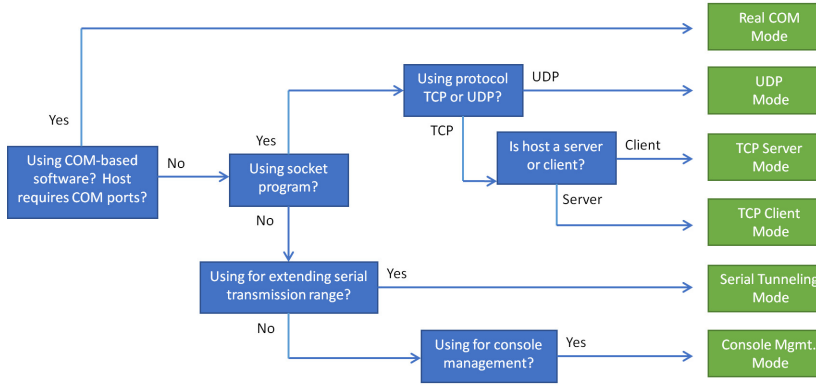
To cover a broad range of serial applications, the Secure Device Server's COM port supports several port operating modes.

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.

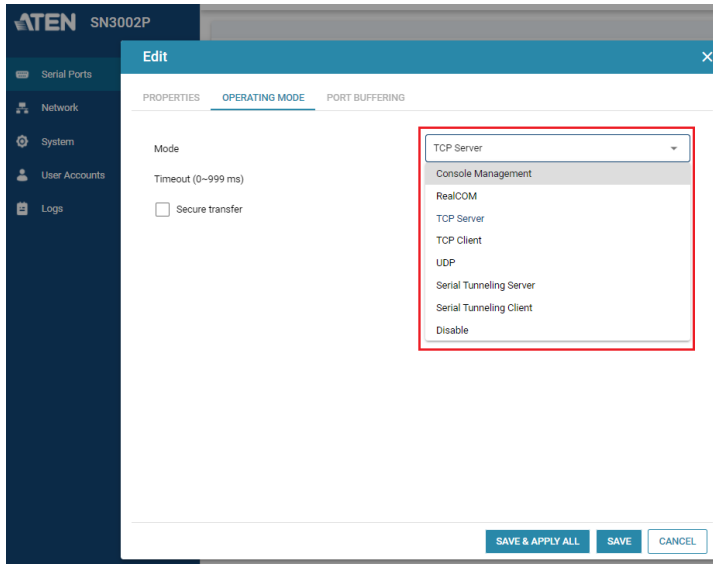
Note: The maximum number of simultaneous connections to any one serial port is 16.

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 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 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 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 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 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 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 Device Server initiates contact with the host computer and begins sending serial data to the to the host. The Secure 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 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 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 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 Device Server's default setting (see *General*, page 39).

2. In this mode, the Secure 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 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 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

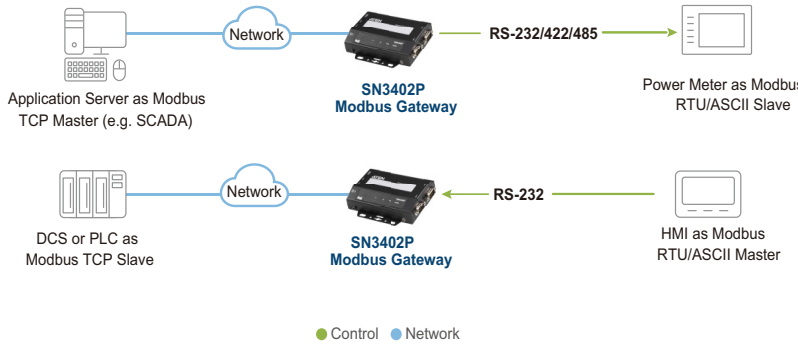
- **An Ethernet Client with Multiple Serial Slaves**

  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 7
Port Access

Overview

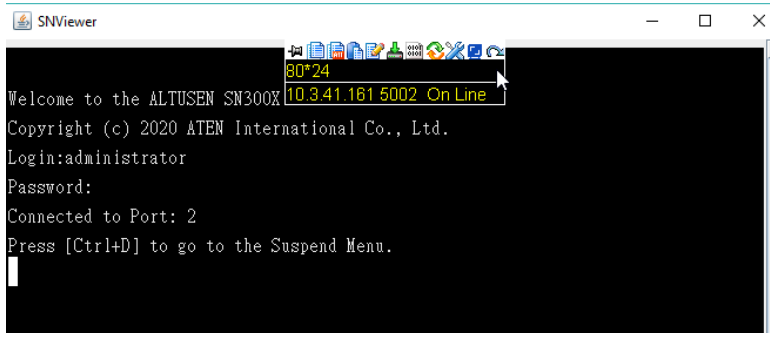
Upon login of the Secure Device Server's web interface, the **Serial Ports** page appears. Use the buttons, described below, to access and control the device's serial COM ports.

Button	Function
EDIT	Edits the serial port's settings. See *Editing Serial Ports*, page 27.
TELNET	Opens a Telnet session with the Secure Device Server using *SNViewer* to access either its configuration menu, or a serial device connect to its COM port. See *Telnet / SSH*, page 70, for details.
SSH	Opens an SSH session with the Secure Device Server using *SNViewer* to access either its configuration menu, or a serial device connect to its COM port. See *Telnet / SSH*, page 70, 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 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 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 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.

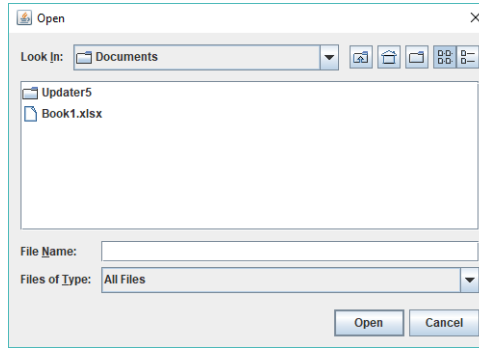
Control Panel Functions

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 72).
	Changes the page encoding (see *Encode*, page 72).
	Resets the terminal to its default settings.
	Changes the font, color and other display settings of the SNViewer (see *Terminal Settings*, page 72).
	Adjusts the width of the SNViewer window.
	Exits the viewer.

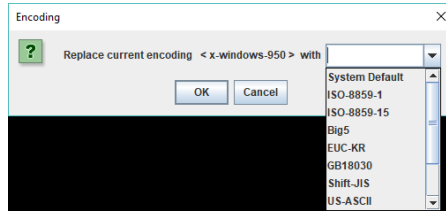
Data Import

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



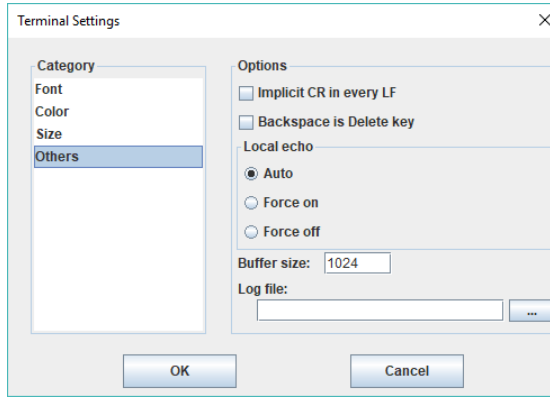
Encode

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 71).

This Page Intentionally Left Blank

Chapter 8
Remote Terminal Operation

Overview

The Secure 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 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 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 Device Server in the following format:

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

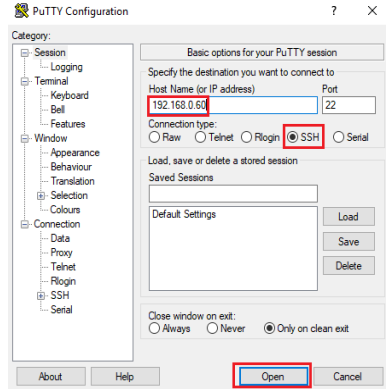
Press [**Enter**] then enter the password of the Secure Device Server to log in.

Note: The default SSH port is 22. To control a device connected to the Secure 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 Device Server.

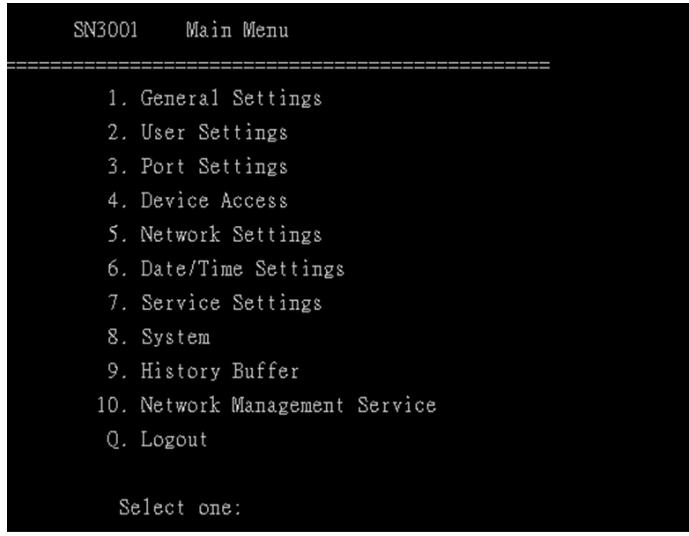


2. Select **SSH** under *Protocol* and click **Open**.
3. Once connected, provide a valid username and password to log in to the Secure Device Server.

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 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 9
Virtual Serial Port Manager

Overview

The Secure 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 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 Device Server's COM ports.

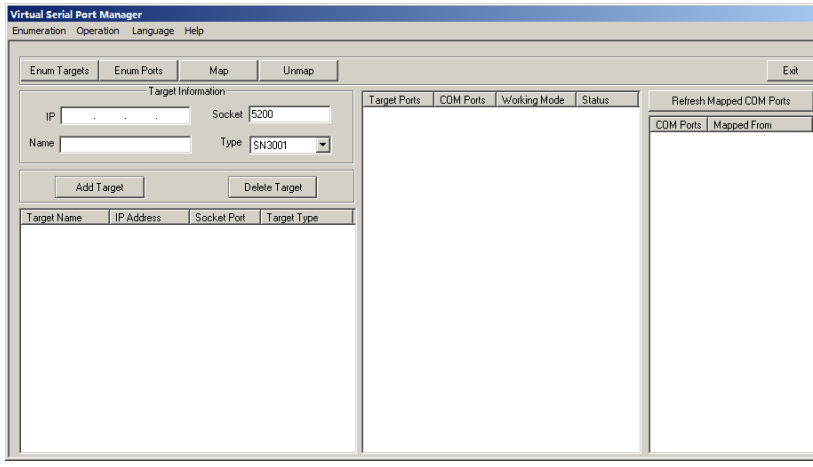
Users can download and install the driver corresponding to their PC OS from the Secure Device Server's product web page.

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 86.

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 Device Server, as well as ATEN Serial Console Servers. The results are shown in the Target List panel (see *Target List*, page 82, 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.

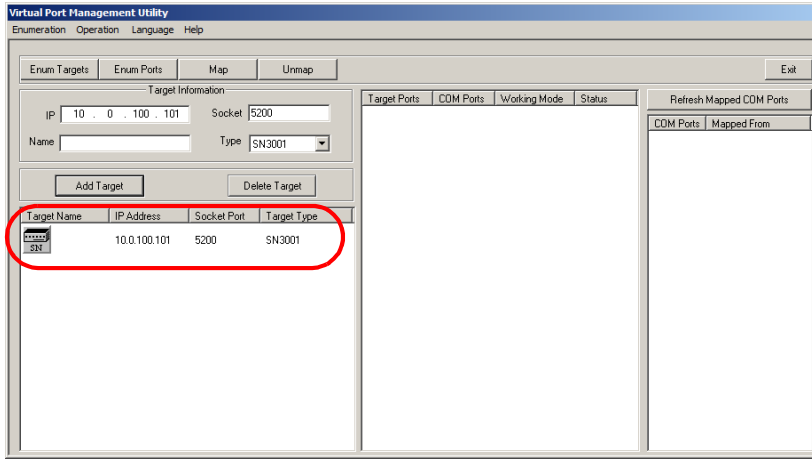
Target Information

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.

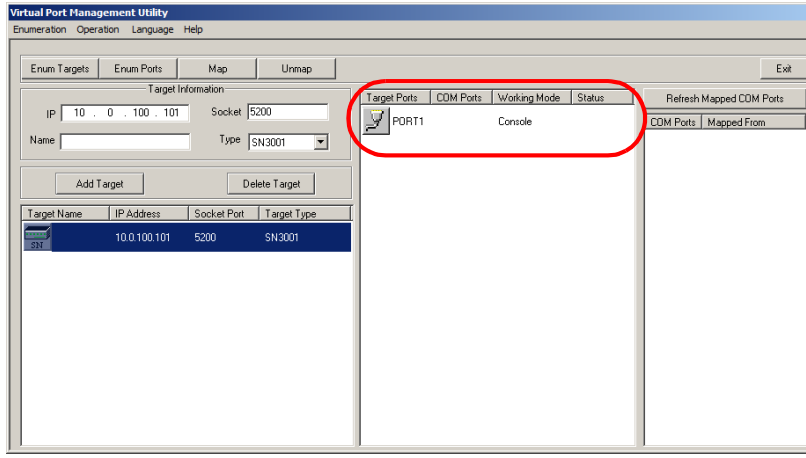


Note: Double-clicking an item in the list invokes the same function as selecting **Enum Ports**, which displays the numbers and working modes of the selected target's ports in the *Port List* column.

- 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 84 for mapping details.

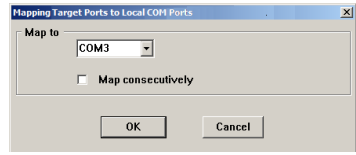
  Note: The *Port Mapping* dialog box can also be invoked either by clicking MapTo… on the toolbar or selecting MapTo… from the menu.

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:



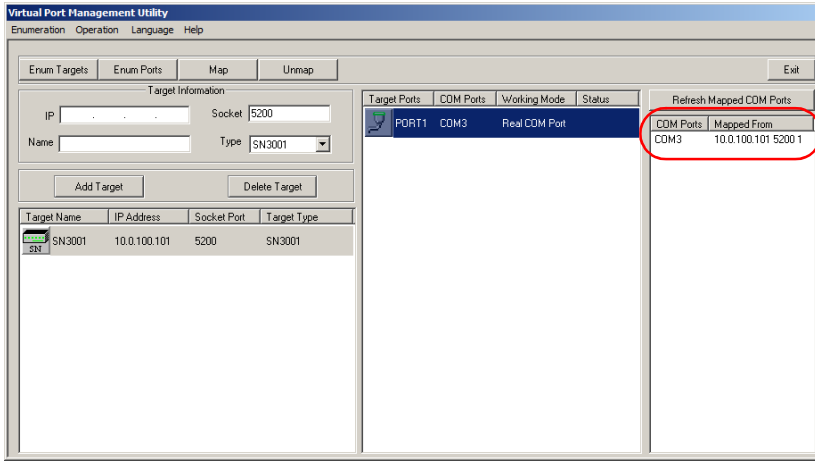
2. From the drop-down list, select the desired COM port to map the Target port to.
3. Click **OK**.

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.

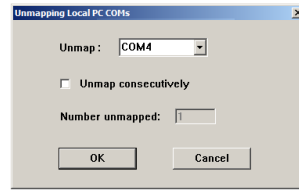


Up to 256 ports can be mapped on a Windows system.

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.

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 vi.

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	DC 9 V : 0.634 W : 3 BTU DC 48 V : 0.804 W : 4 BTU
		SN3002	DC 9 V : 0.769 W : 4 BTU DC 48 V : 0.939 W : 4 BTU
		SN3001P	DC 9 V : 0.805 W : 4 BTU DC 48 V : 0.975 W : 5 BTU PoE: 1.22 W : 6 BTU
		SN3002P	DC 9 V : 0.94 W : 4 BTU DC 48 V : 1.11 W : 5 BTU PoE: 1.39 W : 7 BTU

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 ºC
	Storage Temp.		-40 – 75 ºC
	Humidity		5 – 95% RH, Non-condensing
Physical Properties	Housing		Metal
	Weight	SN3001	0.20 kg
		SN3002	0.21 kg
		SN3001P	0.21 kg
		SN3002P	0.22 kg
	Dimensions (L x W x H)		9.80 x 11.7 x 2.60 cm

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	9V:1.18W:6BTU 48V:1.30W:6BTU	9V:1.19W:6BTU 48V:1.30W:6BTU	DC 9V:1.18W:6BTU DC 48V:1.30W:6BTU	DC 9V:1.19W:6BTU DC48V:1.30W:6BTU
PoE	N/A	N/A	1.475W: 7BTU	1.48V: 7BTU
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	0.21 kg	0.21 kg	0.22 kg

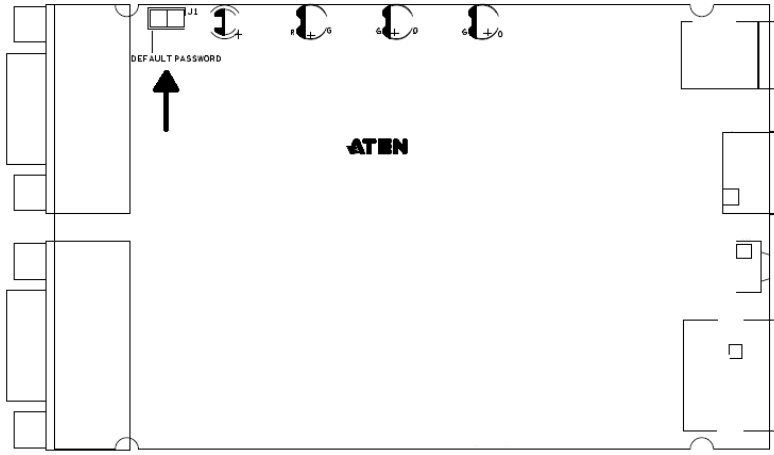
	SN3401	SN3402	SN3401P	SN3402P
Dimensions (L x W x H)	9.80 x 11.70 x 2.60 cm			
Installation	◆ Desktop ◆ Wall Mounting ◆ Din-Rail Mounting ◆ Rack Mounting using the VE-RMK1U **Note:** The rack mounting kit (VE-RMK1U) is sold separately.			

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



3. Power on the Secure 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 21.

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.

Limited Warranty

ATEN warrants its hardware in the country of purchase against flaws in materials and workmanship for a Warranty Period of two [2] years (warranty period may vary in certain regions/countries) commencing on the date of original purchase. This warranty period includes the LCD panel of ATEN LCD KVM switches. Select products are warranted for an additional year (see *A+ Warranty* for further details). Cables and accessories are not covered by the Standard Warranty.

What is covered by the Limited Hardware Warranty

ATEN will provide a repair service, without charge, during the Warranty Period. If a product is detective, ATEN will, at its discretion, have the option to (1) repair said product with new or repaired components, or (2) replace the entire product with an identical product or with a similar product which fulfills the same function as the defective product. Replaced products assume the warranty of the original product for the remaining period or a period of 90 days, whichever is longer. When the products or components are replaced, the replacing articles shall become customer property and the replaced articles shall become the property of ATEN.

To learn more about our warranty policies, please visit our website:
http://www.aten.com/global/en/legal/policies/warranty-policy/