

ALTUSCEN™

Enterprise KVM Solutions by ATEN

Serial Device Server SN3101 User Manual



FCC Information

This is an FCC Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

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.

RoHS

This product is RoHS compliant.

SJ/T 11364-2006

The following contains information that relates to China.

部件名称	有毒有害物质或元素					
	铅	汞	镉	六价铬	多溴联苯	多溴二苯醚
电器部件	●	○	○	○	○	○
机构部件	○	○	○	○	○	○

- : 表示该有毒有害物质在该部件所有均质材料中的含量均在SJ/T 11363-2006规定的限量要求之下。
- : 表示符合欧盟的豁免条款, 但该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T 11363-2006的限量要求。
- ×: 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T 11363-2006的限量要求。



User Information

Online Registration

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

International		http://support.aten.com
North America	ATEN TECH	http://www.aten-usa.com/product_registration
	ATEN NJ	http://support.aten.com

Telephone Support

For telephone support, call this number:

International		886-2-8692-6959
North America	ATEN TECH	1-888-999-ATEN
	ATEN NJ	1-732-356-1703

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.

Package Contents

Standard Package

The standard SN3101 package consists of:

- 1 SN3101 Serial Device Server
- 1 Power Adapter
- 1 DC Terminal Connector
- 1 Mounting Kit
- 1 User Manual*
- 1 Quick Start Guide
- 1 Software CD

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.

Read this manual thoroughly and follow the installation and operation procedures carefully to prevent any damage to the SN3101 or to any other devices on the SN3101 installation.

* Features may have been added to the SN3101 since this manual was printed. Please visit our website to download the most up to date version of the manual.

Copyright © 2007-2009 ATEN® International Co., Ltd.
Manual Part No. PAPE-0286-1AXG
Manual Date: 2009-01-19

Altusen and the Altusen logo are registered trademarks of ATEN International Co., Ltd. All rights reserved. All other brand names and trademarks are the registered property of their respective owners.

Contents

FCC Information	ii
SJ/T 11364-2006.	ii
User Information	iii
Online Registration	iii
Telephone Support	iii
User Notice	iii
Package Contents.	iv
Standard Package.	iv
About This Manual	ix
Overview	ix
Conventions	x
Product Information.	x
Chapter 1.	
Introduction	
Overview	1
Features	2
Restrictions and Requirements.	3
SN3101 Front View	4
SN3101 Rear View	5
Chapter 2.	
Hardware Setup	
Before you Begin.	7
Mounting	7
Wall Mounting	7
DIN Rail Mounting	8
Installation.	9
Chapter 3.	
Browser Login	
Logging In	11
The SN3101 Main Screen.	12
Chapter 4.	
Administration	
Overview	13
General	13
System Information	14
Administrator	14
Connection Control	14
Backup	15

Network	16
Service Ports	16
IP Installer	17
IP Address	18
ANMS	19
CC Management Settings	19
RADIUS Settings	20
LDAP Settings	21
SNMP Settings	22
Finishing Up	22
Date / Time	23
Firmware	24

Chapter 5.

Port Operating Modes

Overview	25
Console Management	25
Real COM Port	25
TCP Server / TCP Client	26
TCP Server (RAW TCP)	26
TCP Client	26
UDP Mode	27
Modbus	27
Virtual Modem	28
Serial Tunnel	28

Chapter 6.

COM Port Management

Overview	29
Telnet	31
View History	31
Connect – Local	31
Connect – COM Port	32
Port Configuration	35
Port Property Settings:	36
Advanced Settings:	38
User Management	44
Adding and Deleting Accounts	44
Editing an Account:	45
Direct Access	46
Session Info	47
Sys Info	48
Log	49

Chapter 7.**Remote Terminal Operation**

Overview	51
HyperTerminal	51
Telnet	53
Logging In	53
SSH	54
Terminal Session (Linux):	54
Third Party Utility (Windows):	55

Chapter 8.**Virtual Port Management**

Overview	57
Driver Installation	57
Windows 2000 and Higher Installation	57
Uninstalling the Driver 58	
Windows 98 Installation	58
TTY Driver Installation for Linux	59
Uninstalling the Driver 59	
Real COM Port Management – Windows	60
Dialog Box Layout	60
Menu and Toolbar	61
Target Information	61
Target List	62
Port List	63
Port Mapping and Unmapping	64
Port Mapping 64	
Mapped COM Port 65	
Port Unmapping 66	
Real COM Port Management – Linux	67
Mapping/Unmapping Virtual Ports	67
Virtual Port Naming Rules	67

Chapter 9.**Serial Network Device Manager**

Overview	69
Installation	69
Operation	70
Dialog Box Layout	70
The Menu Bar	71
Target 71	
Virtual Port	73
The Button Bar	73
Serial Tunnel Creation	74
Building a Serial Tunnel	74
Removing a Serial Tunnel	75

Chapter 10.**LDAP Server Configuration**

Introduction	77
Active Directory	77
Install the Windows 2003 Support Tools	77
Install the Active Directory Schema Snap-in	78
Create a Start Menu Shortcut Entry	78
Extend and Update the Active Directory Schema	79
The Permission Attribute Value	86
Permission String Characters	86
Permission Examples	87
OpenLDAP	88
OpenLDAP Server Installation	88
OpenLDAP Server Configuration	89
Starting the OpenLDAP Server	90
Customizing the OpenLDAP Schema	91
LDAP DIT Design and LDIF File	92
LDAP Data Structure 92	
DIT Creation 93	
Using the New Schema	94

Appendix

Safety Instructions	95
General	95
DC Power	97
Rack Mounting	98
Technical Support	99
International	99
North America	99
Specifications	100
Administrator Login Failure	101
IP Address Determination	102
Method 1:	102
Method 2:	103
Serial Port Pin Assignments	103
Virtual Modem Details	104
AT Command Set Support	104
S Register Support	106
Troubleshooting	107
Limited Warranty	107

About This Manual

This User Manual is provided to help you get the most from your SN3101 system. It covers all aspects of installation, configuration and operation. An overview of the information found in the manual is provided below.

Overview

Chapter 1, Introduction, introduces you to the SN3101 System. 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 your installation.

Chapter 3, Browser Login, explains how to log into the SN3101 from your browser.

Chapter 4, Administration, explains the administrative procedures that are employed to configure the SN3101's working environment.

Chapter 5, Port Operating Modes, introduces the SN3101's operating modes, and explains the purpose of each.

Chapter 6, COM Port Management, details concepts and procedures involved in the configuration and management of the SN3101's COM port.

Chapter 7, Remote Terminal Operation, describes how the SN3101 can be accessed via remote terminal sessions such as HyperTerminal, Telnet, SSH, and PuTTY.

Chapter 8, Virtual Port Management, shows how to install the virtual COM port driver and to set up and manage the virtual COM port.

Chapter 9, Serial Network Device Manager, explains how to use the Serial Network Device Management utility to create and maintain device groups for easy management of the serial ports on your installation; and as an AP alternative to the browser-based management utilities.

Chapter 10, LDAP Server Configuration, explains how to configure the SN3101 for LDAP / LDAPS authentication and authorization with Active Directory or OpenLDAP.

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

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 the option (on a menu or dialog box, for example), that comes next. For example, Start → Run means to open the *Start* menu, and then select *Run*.
-  Indicates critical information.

Product Information

For information about all ALTUSEN products and how they can help you connect without limits, visit ALTUSEN on the Web or contact an ALTUSEN Authorized Reseller. Visit ALTUSEN on the Web for a list of locations and telephone numbers:

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

Chapter 1

Introduction

Overview

The SN3101 Serial Device Server provides Ethernet connectivity for serial devices used in a wide range of applications, such as industrial control, data acquisition, access control, environment monitoring, remote site management, etc. This allows older serial devices to take advantage of modern methods of communication.

In addition, by making these industrial serial devices *Internet ready*, the SN3101 enables users to access and control those devices from any computer connected to the Internet, whether down the hall, or half way around the world.

The SN3101 offers versatile and diversified serial data access methods to meet a broad range of application requirements – these include Console Management, Real COM, TCP Server, TCP Client, UDP, Modbus, Serial Tunnel, and Virtual Modem. SMTP and SNMP trap event notification are also provided.

The SN3101 can also work in tandem with other remote management products – such as the Altusen PN9108 Power over the NET™ remote power management system – to provide convenient, reliable, and effective, remote data center device management.

Since the SN3101 is fully compatible with existing serial communications software, your current investment in software development is protected. Software designed to work with COM or TTY ports can access serial devices over a TCP/IP network by utilizing the SN3101's Real COM or TTY drivers. This feature also breaks through the port number and distance limitation barriers encountered with PC hardware.

Installation is fast and easy: plugging cables into their appropriate ports is all that is entailed. An offering of browser based GUI, Telnet (SSH), VT console terminal sessions, and a Windows software utility, make configuration and operation smooth and convenient.

The SN3101's firmware is upgradeable over the Net, so you can stay current with the latest improvements simply by downloading updates from our website. With its advanced features and ease of operation, the SN3101 is the most convenient, most reliable, and most cost effective way to centrally manage your serial devices.

Features

- ◆ Provides remote serial access over the Internet for industrial serial devices, serial IT devices and serial over IP appliances
- ◆ Software selectable RS-232/422/485 3-in-1 serial port
- ◆ Built-in 15KV ESD serial port protection
- ◆ Max. baud rate: 460 Kbps; supports Hardware and Software flow control
- ◆ Versatile serial operation modes, including Console Management, Real COM, TCP Server, TCP Client, UDP, Modbus, Serial Tunnel and Virtual Modem
- ◆ Serial data encryption via 128-bit SSL for TCP Server, TCP Client, Virtual Modem and Serial Tunnel operation modes
- ◆ Redundancy support via multiple simultaneous Real COM, TCP Server, and TCP Client connections
- ◆ 64 Kbyte port buffer prevents data loss when the network is down
- ◆ Real COM driver for Windows 2000/XP/2003/Vista; Real TTY driver for Linux
- ◆ Modbus Ethernet-to-Serial support (Modbus/TCP, Modbus/RTU and Modbus ASCII) for seamless integration of serial Modbus devices
- ◆ Works in tandem with other Altusen/Aten appliances - such as the CC Management Center, the PN0108 and the PN9108 – allowing administrators to manage a wide range of data center devices through IP connections
- ◆ Modem emulation enables existing modem-based applications to make connections over IP networks
- ◆ Virtual Terminal support (VT320, VT52, VT100, VT220)
- ◆ Supports ISO646 - US (US ASCII), ISO8859 - 15 (Latin - 9) code set
- ◆ System configuration via Web Console (HTTP/HTTPS), Telnet/SSH Console and Windows utility
- ◆ Backup/restore and firmware upgrading via Web Console (HTTP/HTTPS) and Windows utility
- ◆ Multiple users and privileges support
- ◆ Easy-to-use Windows utility (2000/XP/2003/Vista) for auto discovery, multiple device setting and monitoring
- ◆ External centralized authentication and authorization support – RADIUS, LDAP / LDAPS, and MS Active Directory

- ◆ SNMP MIB II and RS-232 MIB for network management
- ◆ SMTP and SNMP trap event notification
- ◆ Choice of power input: AC—DC adapter or DC direct

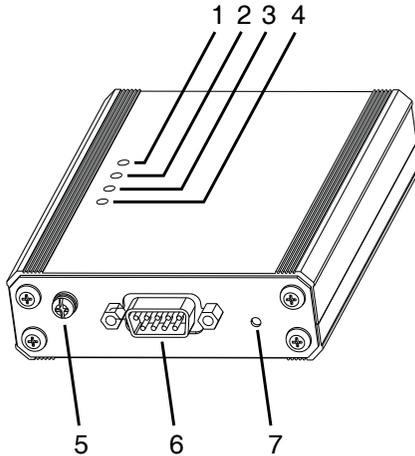
Restrictions and Requirements

- ◆ Sun's Java 2 JRE 1.4.2 or higher must be installed on your computer. Java is available for free download from the Sun Java website:

`http://java.sun.com`

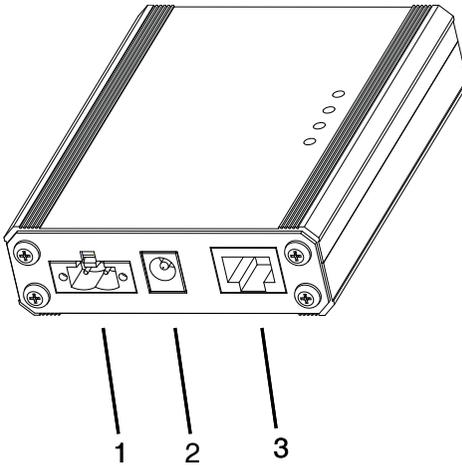
- ◆ The devices that connect to the SN3101 must support one of the following serial protocols:
 - ◆ RS-232 (protocol or terminal operations)
 - ◆ RS-422
 - ◆ RS-485
- ◆ The Virtual COM port driver (Real COM port) support requires Windows 2000 or higher.
- ◆ Under Vista (32-bit version), only the administrator can install the Virtual Port Management Utility – ordinary users can only operate the mapped Real COM ports.
- ◆ The current Linux TTY driver supports kernels up to version 2.6.19.

SN3101 Front View



No.	Component	Description
1	Power LED	Lights GREEN when the SN3101 is powered up and ready to operate.
2	Link LED	Lights GREEN to indicate that the SN3101 is connected to the LAN. It flashes GREEN to indicate that a client program is accessing the device.
3	10/100 Mbps Data LED	The LED lights ORANGE to indicate a 10 Mbps data transmission speed. It lights GREEN to indicate a 100 Mbps data transmission speed.
4	Tx/Rx (ACT) LED	Lights GREEN to indicate that the device attached to the port is online. It flashes GREEN to indicate that data is being transmitted through the port.
5	Grounding Terminal	The grounding wire (used to ground the unit) attaches here.
6	Serial Port	Your serial device connects to this RS-232/RS-422/RS-485 3-in-1 combination serial port.
7	Reset Switch	Pressing and holding this switch in for less than three seconds performs a system reset. Pressing and holding this switch in for more than three seconds returns its settings to their default status.

SN3101 Rear View



No.	Component	Description
1	DC Terminal	If you are using DC power directly, the electric leads from the DC power source attach here. Note: The diagram shows the SN3101 without the DC terminal connector installed.
2	DC Jack	If you are using an AC adapter, the adapter cable plugs in here.
3	LAN Port	The Ethernet cable that connects the SN3101 to the Internet plugs in here.

This Page Intentionally Left Blank

Chapter 2

Hardware Setup

Before you Begin



1. Important safety information regarding the placement of this device is provided on page 95. Please review it before proceeding.
2. Make sure that power to all the devices you will be connecting up have been turned off.

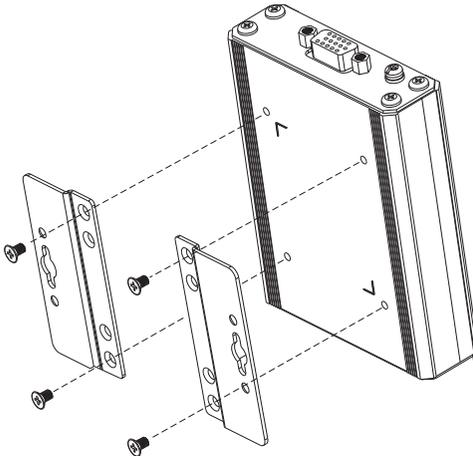
Mounting

For flexibility and convenience, the SN3101 can be wall mounted or DIN rail mounted, as described in the sections that follow.

Wall Mounting

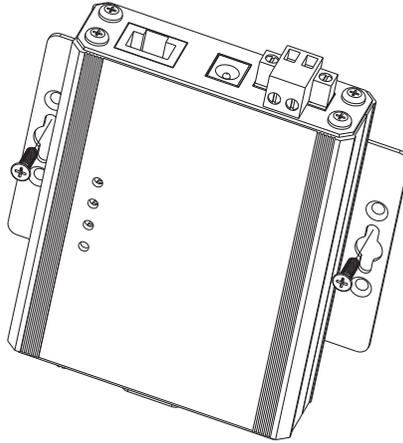
To wall mount the SN3101:

1. Use the smaller screws supplied with the Mounting Kit to screw the mounting brackets into the back of the unit:



Note: If you use third party screws, the length of the shank (the threaded portion) must not exceed 4.50 mm

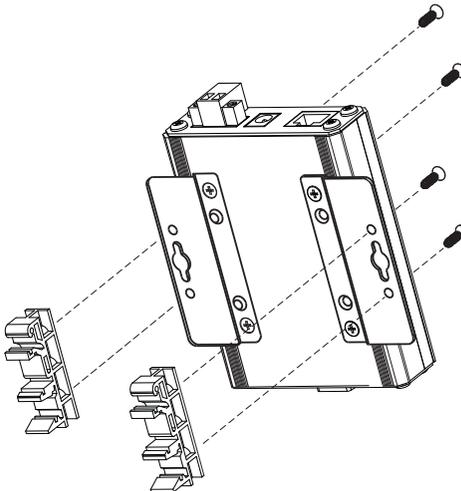
2. Screw the mounting brackets to the wall.



DIN Rail Mounting

To mount the SN3101 on a DIN rail:

1. Screw the mounting brackets to the back of the SN3101 as described in step 1 of the wall mounting procedure.
2. Use the larger screws supplied with the Mounting Kit to screw the DIN rail brackets to the mounting brackets – as shown in the diagram, below:

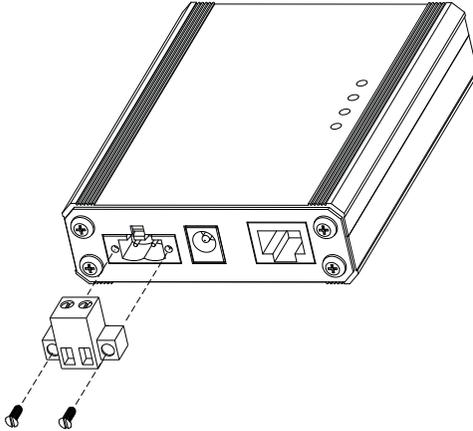


3. Hang the unit on the DIN rail.

Installation

To install the SN3101, do the following:

1. If you intend to use the DC terminal, screw the DC terminal connector to the block – as shown in the following diagram:



2. Refer to the diagram on page 10 (the characters in the diagram correspond to the characters of the steps), as you do the following:
 - a) Use a null modem cable to connect the SN3101's serial port to your serial device.

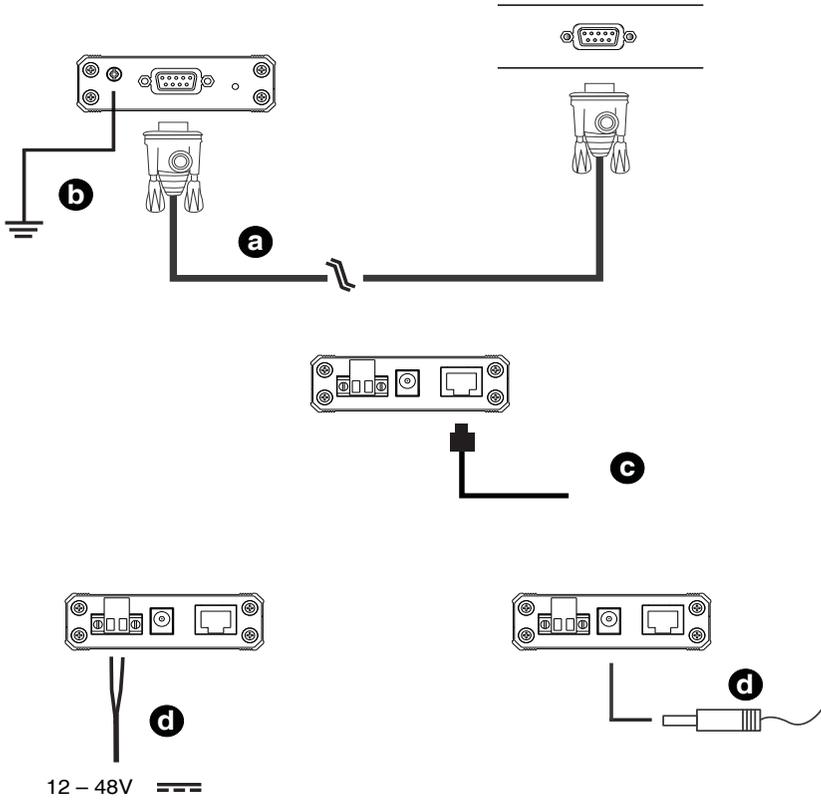
Note: The SN3101 supports the RS-232, RS-422, and RS-485 protocols, and is software configurable. See *Serial Port Pin Assignments*, page 103, for pin assignment details.

- b) Ground the device.
- c) Plug the cable that connects the SN3101 to the network or the Internet into the LAN port.
- d) Connect the DC power source to the device.

Note: The diagram shows both connection methods. Ordinarily, you would connect one or the other.

This completes the SN3101 installation.

SN3101 Installation Diagram:



Chapter 3

Browser Login

Logging In

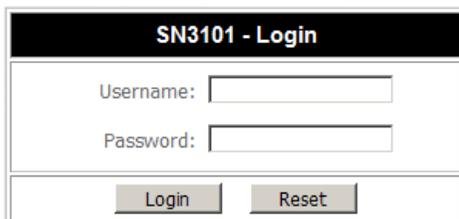
SN3101 operation is Internet browser based. To begin:

1. Open your browser and specify the IP address of the SN3101 you want to access in the browser's URL location bar.

Note: 1. Get the IP address from the SN3101 administrator.

2. If you are the administrator, and are logging in for the first time, the various ways to determine the SN3101's IP address are described in the Appendix on p. 102.
-

2. A *Security Alert* dialog box appears. Accept the certificate.
3. A login dialog box, like the one below, appears:



The image shows a login dialog box titled "SN3101 - Login". It has a black header bar with the title in white. Below the header, there are two input fields: "Username:" followed by a text box, and "Password:" followed by a text box. At the bottom of the dialog, there are two buttons: "Login" and "Reset".

4. Provide a valid Username and Password (set up by the administrator), then Click **Login** to continue.

Note: If you are the administrator, and are logging in for the first time, use the default Username: *administrator*; and the default Password: *password*. For security purposes, we strongly recommend you change these and give yourself a unique Username and Password (see *General*, page 13).

The SN3101 Main Screen

After you have successfully logged in, the Main Screen appears:



- ◆ Except for the *Logout* icon (at the far right), the icons arranged horizontally across the top are only enabled for the administrator. Administrative functions are explained in Chapter 4.

Note: Be sure to click the *Logout* icon when you end your session.

- ◆ The bar along the left side is used to configure and control access to the SN3101's COM port. The functions of each of the buttons is described in Chapter 5.
- ◆ Unless you need to perform administrative functions, you can skip Chapter 4, and go directly to Chapter 5.

Chapter 4 Administration

Overview

The icon bar at the top of the main screen is used by the administrator to configure the SN3101's working environment.



An explanation of each of the configuration functions is given in the sections that follow.



General

When you click the *General* icon, the following dialog box appears:

General Settings

System Information

Device Group:

Station Name:

Station Description:

Administrator

Name:

Old Password:

Password:

Confirm Password:

Comments:

Connection Control

Session timeout: min. (0:Disable)

The dialog box is divided into three main panels, as described below:

System Information

The System Information section displays the name of the group that the SN3101 belongs to, and allows you to provide a name and description for the SN3101 Station.

- ◆ Assigning a *Device Group* name to the SN3101 makes it possible to configure a group of SN3101s at the same time. See Chapter 9, *Serial Network Device Manager*, for details regarding group naming and configuration.
- ◆ Giving each SN3101 a name and description makes it convenient to differentiate among several installed SN3101s.

Note: Providing these names and descriptions is optional, but makes it more convenient to administer your SN3101s in large multi-device installations.

Administrator

This section sets the administrator's login name and password.

- ◆ The default administrator name is: *administrator*
- ◆ The default password is: *password*

For security purposes, we strongly recommend that you change the default values to something unique.

The *Comments* field is optional. It provides administrators with a place to enter personal comments.

Connection Control

Session Timeout sets a timeout value. If there is no input from the logged in operator for the amount of time set with this function, the operator is automatically logged out and the session is terminated. Valid settings are from 0 ~ 255 minutes. A setting of 0 (zero) disables this function. The default is 3 minutes.



Backup

Backup provides the means to backup and restore your SN3101 configuration settings:

Backup and Restore Settings

Backup Configuration

Password:

Restore Configuration

Password:

To backup your configuration settings, do the following:

1. Key in a password for the configuration file, then click **Save**.

Note: Make a note of the password. You will need it when restoring the configuration settings.

2. When the browser asks what to do with the *System.conf* file, choose *Save to Disk* and indicate where to save the file.

To restore your configuration settings, do the following:

1. Key in the password that you specified when you originally saved the configuration file.
2. Click **Browse...**; navigate to the location where you saved the file; and select the configuration file (*System.conf*).
3. Click **Restore**. After a few seconds a message appears informing you that the restore operation is in progress. When the operation completes, the SN3101 automatically resets itself, and you are taken to the login page where you have to log in again.



Network

Network Configuration allows you to set up the network parameters for the SN3101:

Network Configuration	
Service Ports:	HTTP: 80
	HTTPS: 443
	Telnet: 23
	SSH: 22
	Modbus: 502
	Socket: 5001 COMs base socket
IP Installer Setting:	<input checked="" type="radio"/> Enabled <input type="radio"/> View Only <input type="radio"/> Disabled
<input type="checkbox"/> Obtain an IP address automatically [DHCP]	
Primary IP:	10.0.100.101
Primary Subnet Mask:	255.255.255.0
Gateway:	10.0.100.1
Primary DNS Server:	
Alternate DNS Server:	
<input type="checkbox"/> Enable report from the following SMTP Server	
SMTP Server:	
<input type="checkbox"/> My server requires authentication	
Account Name:	
Password:	*****
From:	
To:	
<input type="button" value="Update"/>	

Service Ports

Lets you select the service ports that the SN3101 listens for incoming data on. Unless you have a specific reason for changing them, we recommend you leave the default settings as they are.

(Continues on next page.)

(Continued from previous page.)

A description of the default Service Ports and their functions is given in the table, below:

Service	Port	Description
HTTP	80	Used for web access without encryption.
HTTPS	443	Used for web access with 128-bit encryption.
Telnet	23	Used to access the SN3101's Configuration Menu via Telnet.
SSH	22	Used to access the SN3101's Configuration Menu via SSH.
Modbus	502	In Modbus operation mode, an SN3101 master device accesses SN3101 slave devices via TCP port 502.
Socket	5001	The Base Socket Port: Used for accessing serial devices connected under the SN3101 via Telnet.
	5101	The Base Socket Port + 100: Used for accessing serial devices connected under the SN3101 via SSH.
	5301	The Base Socket Port + 300: Used to accept a Virtual Modem connection from a master SN3101. The Base Socket Port + 300: Used to listen for and accept a TCP connection.

-
- Note:** 1. The *Socket* entry refers to the port that will be used to communicate with serial devices connected to the SN3101's COM port. See *Operating Mode*, page 37, and Chapter 5, *Port Operating Modes*, for details.
2. Under the *Socket* entry, changing the Base Socket Port number will change the two related socket port entry numbers
-

IP Installer

Click a radio button to *Enable/Disable* the IP Installer utility (see *Method 1:*, page 102, for IP Installer details).

Note: If you choose *View Only*, the utility will show the SN3101 in its Device List, but you will not be able to change its IP address.

IP Address

The default is for the SN3101 to have a fixed IP address. It's default IP address is 192.168.0.10.

- ◆ If you are giving the SN3101 a fixed IP address, fill in the *Primary IP* to *Alternate DNS Server* fields with values appropriate to the network you are on.
- ◆ To have the SN3101 obtain its IP address automatically from a DHCP server, put a check in the *Obtain an IP address automatically [DHCP]* checkbox.
- ◆ To have the SN3101 email reports from the SMTP server to you, do the following:
 1. Enable the *Enable report from the following SMTP server*, and key in either the domain name or the IP address of your SMTP server.

Note: If you use the domain name, be sure to fill the Primary and Alternate DNS server information.

2. If your server requires authentication, put a check in the *My server requires authentication* checkbox.
3. Key in the appropriate account information in the *Account Name*, *Password*, and *From* fields.

Note: Only one email address is allowed in the *From* field.

4. Key in the email address (addresses) of where you want the report of the DHCP address sent to in the *To* field.

Note: If you are sending the report to more than one email address, separate the addresses with a comma or a semicolon.

5. When all of your configuration settings have been made, click **Update** to save the information and have the SN3101's DHCP generated IP address emailed to you.

Note: If the SN3101 is on a network that uses DHCP to assign network addresses, and you don't know what the address is, there are several methods you can use to ascertain it. See *IP Address Determination*, page 102 for details.



ANMS

The Authentication Network Management Service dialog box allows you to set up login authorization management from external sources. It is divided into four main panels, as described below:

Authentication Network Management Service	
CC Management Settings	
<input type="checkbox"/> Enable CC Management	
CC Server IP:	192.168.0.100
CC Server Port:	8889
RADIUS Settings	
<input type="checkbox"/> Enable RADIUS	
Primary RADIUS Server IP:	192.168.0.100
Primary RADIUS Service Port:	1812
Alternate RADIUS Server IP:	192.168.0.100
Alternate RADIUS Service Port:	1645
Shared Secret:	Secret (6 characters min.)
Timeout:	3 (seconds)
Retries:	3
LDAP Settings	
<input type="checkbox"/> Enable LDAP	
<input checked="" type="radio"/> Enable LDAP	<input checked="" type="radio"/> Enable LDAPS
LDAP Server IP:	192.168.0.100
LDAP Service Port:	389
Base DN:	ou=users,dc=aten,dc=com
Search DN:	dc=aten,dc=com
Admin User:	LDAPadmin
Admin Pass:	*****
LDAP Timeout:	3 (seconds)
SNMP Settings	
<input type="checkbox"/> Enable SNMP Agent	
<input checked="" type="checkbox"/> Enable SNMP Trap	
Community Name for Read:	public
Community Name for Write:	private
Community Name for Trap:	public
SNMP Manager 1:	192.168.0.100
SNMP Manager 2:	
SNMP Manager 3:	
SNMP Manager 4:	
<input type="button" value="Save"/>	

CC Management Settings

If you want to allow user access to the SN3101 through a CC (Control Center) server, check *Enable CC Management* and fill in the CC Server's IP address and the port that it listens on in the appropriate fields.

RADIUS Settings

If you want to allow authorization for the SN3101 through a RADIUS server, do the following:

1. Check *Enable RADIUS*.
2. Fill in the IP addresses and Service Ports for the Primary and Alternate RADIUS servers.
3. Key the *Shared Secret* character string that you want to use for authentication between the SN3101 and the RADIUS Server.
4. Set the time in seconds that the SN3101 waits for a RADIUS server reply before it times out in the *Timeout* field.
5. Set the number of RADIUS retries allowed in the Retries field.
6. Click **Save** to save the information.
7. On the RADIUS server, set the access rights for each user according to the attribute information in the table, below:

Attribute	Meaning
U	(User) The user has the authority to access and configure some ports. This attribute must be specified for all users who access the system.
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. Upper or lower case work equally well.

2. Characters are comma delimited.

3. An invalid character in the string will prohibit access to the SN3101 for the user.

LDAP Settings

To allow authentication and authorization for the SN3101 via LDAP / LDAPS, refer to the information in the table, below:

Item	Action
Enable LDAP	Put a check in the <i>Enable LDAP</i> checkbox to allow LDAP / LDAPS authentication and authorization.
LDAP / LDAPS	Click a radio button to specify whether to use LDAP or LDAPS.
LDAP Server IP	Fill in the IP address of the LDAP or LDAPS server.
LDAP Service Port	Fill in the port number for the LDAP or LDAPS server. For LDAP, the default port number is 389; for LDAPS, the default port number is 636.
Base DN	The 'root' point for LDAP manager to bind to the server.
Search DN	The distinguished name of the search base. This is the domain name where the search starts for user names.
Admin User	The LDAP manager's user name. (This field is optional.)
Admin Pass	The LDAP manager's password. (This field is optional.)
LDAP Timeout	The time in seconds that the SN3101 waits for an LDAP or LDAPS server reply before it times out.

SNMP Settings

If you want to use SNMP to help with your installation management:

1. Check *Enable SNMP Agent*.
2. Once SNMP Agent has been enabled, the *SNMP Trap* checkbox becomes active. If you want to enable SNMP trap functionality, click to put a check in the checkbox.
3. Key in passwords for the *Community Name* fields. We recommend replacing the defaults (public, private) with an alphanumeric string of at least 8 characters.
4. Key in the IP addresses of the computers that will automatically be notified of SNMP trap events in the *SNMP Manager* fields.

-
- Note:**
1. MIB definitions for the SN3101 are provided on the CD that came with this package.
 2. The following SNMP trap events are sent: string alert; IP received from DHCP server; user login/logout; system bootup.
-

Finishing Up

When you have finished making all your entries, click **Save**, to save them.



Date / Time

The Date / Time function allows you to set the SN3101's date and time. When you click the *Date / Time* icon, the following dialog box appears:

Date / Time	
Current System Time	
Sys. Date (yyyy-mm-dd)	2002-07-01
Sys. Time (hh:mm:ss)	10:06:04
New System Time	
<input checked="" type="radio"/> Synchronize with computer time	
Date (yyyy-mm-dd)	2007-10-30
Time (hh:mm:ss)	15:09:55
<input type="radio"/> Set manually	
Date (yyyy-mm-dd)	2002-07-01
Time (hh:mm:ss)	10:04:02
<input type="radio"/> Synchronize with NTP server	
SN3101's Time Zone	
Time Zone:	(GMT) Casablanca, Monrovia
<input type="checkbox"/> Enable daylight saving time (Summer Time)	
<input type="button" value="Save"/>	

The date and time that the SN3101 is currently set to appear in the upper section. The large lower section offers three methods to set new date and time parameters:

- ◆ Synchronizing the date and time with your computer's date and time
- ◆ Setting the date and time manually
- ◆ Synchronizing the date and time with the date and time of an NTP server on the internet

-
- Note:**
1. If you enable *Synchronize with computer time*, the Date and Time fields are filled with the date and time settings of your computer.
 2. If you enable *Set Manually*, key in the Date and Time in the corresponding fields.
 3. If you enable *Synchronize with NTP server*, select the time zone that corresponds to the SN3101's location from the list box in the Time Zone panel. If you are behind a firewall, you must enable a port for the NTP server.
-

- ◆ Click **Save** to save your changes.



Firmware

The Firmware Upgrade function provides a smooth, automated process for upgrading the SN3101's firmware. New firmware upgrade packages are posted on our web site as they become available. Check the site regularly to find the latest packages.

To upgrade your firmware, do the following:

1. From your computer, go to our Internet support site and choose the SN3101 to get a list of available Firmware Upgrade Packages.
2. Choose the Firmware Upgrade Package you want to install (usually the most recent), and download it to your computer.
3. From the computer that you downloaded the upgrade file to, log into the SN3101.
4. Click the *Firmware* icon. A dialog box similar to the one below appears:

Firmware Upgrade	
<input checked="" type="checkbox"/> Check Firmware Version	
Firmware Image File:	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Upgrade"/>	

5. Click the *Browse* button; navigate to the upgrade file on your computer, and select it.
6. Click **Upgrade** to perform the upgrade.

-
- Note:**
1. If you enable *Check Firmware Version*, the upgrade function compares the station's firmware level with that of the upgrade files. If it finds that the SN3101's current version is equal to, or higher than, the upgrade version, it won't overwrite the SN3101's version.
 2. If you do not enable *Check Firmware Version*, the Utility installs the upgrade files without checking whether they are a higher level, or not.
-

Chapter 5

Port Operating Modes

Overview

To cover a broad range of serial applications, the SN3101's COM port supports several port operating modes. These include Virtual Modem, Serial Tunnel, Console Management, and Real COM Port modes, for device control sessions, plus TCP Server/Client, UDP, and Modbus modes for socket application purposes. An explanation of the functions performed by the various operating modes is provided in the sections that follow.

Console Management

In Console Management mode, multiple users can establish a Telnet or SSH session to the SN3101 to manage a server or serial device connected to its COM port. Users can log in using the browser Telnet function, a direct Telnet session, SSH or PuTTY.

Note: Be sure that the *Socket* entry specified on the *Network* page corresponds to the port that the device listens on. 5001 is the SN3101's default setting (see *Network*, page 16, and *Socket*, page 17).

Real COM Port

This mode is used in conjunction with a virtual COM port driver installed on the remote users's local computer. (See Chapter 8, *Virtual Port Management* for virtual port management details.) When the SN3101's COM port set to this mode, the device connected to the port appears as if it were a device directly connected to a COM port on the remote users's local computer.

This mode is useful with devices such POS terminals, Bar Code Readers, Serial printers, etc. since it allows you to use software that was written for pure serial communication applications. It can be used with other Altusen management products, such as the PN9108 Power Over the NET™.

The SN3101 comes with Real COM drivers for Windows systems and TTY drivers for Linux systems. See Chapter 8, *Virtual Port Management* for installation and operation details.

Note: Real COM Port mode supports the *Direct Access* function (see *Direct Access*, page 46, for details).

TCP Server / TCP Client

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

TCP Server (RAW TCP)

In *TCP Server* (RAW TCP) mode, data transmission is bidirectional. In this mode, the host computer initiates contact with the SN3101 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. 128-bit SSL data encryption is supported in this operating mode.

The SN3101 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:** 1. Be sure that the *Socket* entry specified on the *Network* page corresponds to the port that the device listens on. 5001 is the SN3101's default setting. (See *Network*, page 16, and *Socket*, page 17.)
2. TCP Server mode supports the *Direct Access* function (see *Direct Access*, page 46, for details).
-

TCP Client

In *TCP Client* mode, when serial data comes into the SN3101's serial port, the SN3101 initiates contact with the host computer and begins sending serial data to the to the host. The SN3101 can send data to up to 16 host computers simultaneously, and supports 128-bit SSL data encryption in this operating mode.

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 SN3101'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.

Modbus

Modbus follows a Master/Slave model that allows communication between many serial devices connected to the same network. It is often used to connect a supervisory computer with a remote terminal unit (RTU) in supervisory control and data acquisition (SCADA) systems.

In *Modbus* mode, the SN3101 acts as a gateway to link individual serial Modbus devices. Acting as a Modbus master, the SN3101 initiates transactions and the slaves respond with the requested data. Because it communicates using TCP over the Internet, the SN3101 eliminates the distance limitations of traditional Modbus serial communications.

Note: Modbus RTU and Modbus ASCII slave modes support the *Direct Access* function (see *Direct Access*, page 46, for details).

Virtual Modem

In *Virtual Modem* mode, the SN3101's COM port emulates a modem. The port acts as if it were a real modem for communication with a remote server. This allows software designed to transmit data over a serial modem-to-modem link, to perform serial operations over a TCP/IP ethernet connection. In this mode, the SN3101 "dials into" the remote server's IP specifying the appropriate port address for the transmission. For example:

```
atd 10.0.100.101:5000
```

A detailed description of the data structures and related functions of the SN3101's virtual modem function is provided on page 104.

Note: 128-bit SSL data encryption is supported in this operating mode.

Serial Tunnel

Serial Tunnel involves establishing a direct connection between two SN3101's over ethernet. Serial Tunnel works in a *master/slave* relationship. One unit is designated master, the other designated slave.

Note: In this configuration, it doesn't matter which one is designated master and which one is designated slave.

The COM port of one unit connects to the COM port of a computer; the COM port of the other unit connects to the serial device that will be accessed.

The units communicate with each other via their IP and port addresses. The port address is set with the Socket entry of the Network Configuration settings. See *Network*, page 16, and *Socket*, page 17, for details.

Note: 1. Serial Tunnel cannot be configured with the browser interface. It must be configured with the *Serial Network Device Manager* software. (See *Serial Network Device Manager*, page 69.)

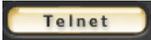
2. 128-bit SSL data encryption is supported in this operating mode.

Chapter 6

COM Port Management

Overview

After you log into the SN3101, the Main Screen appears (see *The SN3101 Main Screen*, page 12). The bar along the left side is used to configure and control access to the SN3101's COM port. The functions of each of the buttons is described in the following table:

Button	Authorization	Function
	Administrator and Permitted Users	Clicking this button brings up the <i>Serial Port Status</i> screen. This is the same screen that displays after a log in (see page 12).
	Administrator and Permitted Users	Clicking this button brings up the Telnet page. This page allows the administrator and all users to open a telnet session with the SN3101 to access either its configuration menu, or a serial device connect to its COM port. See <i>Telnet</i> , page 31, for details.
	Administrator and Permitted Users	This page allows the administrator and users with configuration permission (see <i>User Management</i> , page 44), to set up the SN3101's COM port parameters (see <i>Port Configuration</i> , page 35).
	All	This button has two effects depending on whether the administrator or an ordinary user clicks it: <ul style="list-style-type: none">◆ The administrator can use this function to Create, Edit, and Delete user profiles (see <i>User Management</i>, page 44, for details).◆ Ordinary users can only use this function to change their passwords and personal information (see <i>User Management</i>, page 44). Note: Operators who have logged in via a RADIUS server (see <i>RADIUS Settings</i> , page 20) can view User Manager information, but cannot make any changes to that information.

(Continues on next page.)

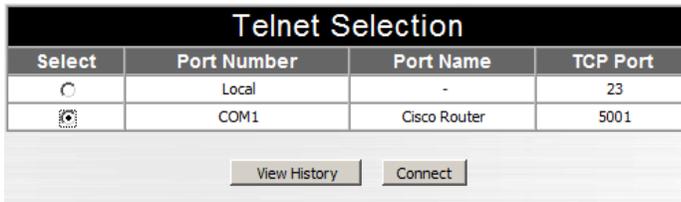
(Continued from previous page.)

Button	Authorization	Function
	Administrator Only	For security purposes, Direct Access can limit the users attempting to access a port that has been configured for Real COM, TCP Server (RAW TCP), and Modbus Slave, operating modes (see <i>Operating Mode</i> , page 37, for details).
	Administrator Only	This page allows the administrator to see information about all the users who are currently logged into the SN3101 (see <i>Session Info</i> , page 47).
	Administrator Only	This page shows information about the SN3101's configuration (see <i>Sys Info</i> , page 48).
	Administrator Only	Clicking this button brings up the <i>Event Log</i> dialog box which allows the administrator to view all of the events that took place on the SN3101 (see <i>Log</i> , page 49).

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

Telnet

To access the SN3101's configuration menu, or a device attached to the SN3101's COM port, click the *Telnet* button. A screen similar to the one below appears:



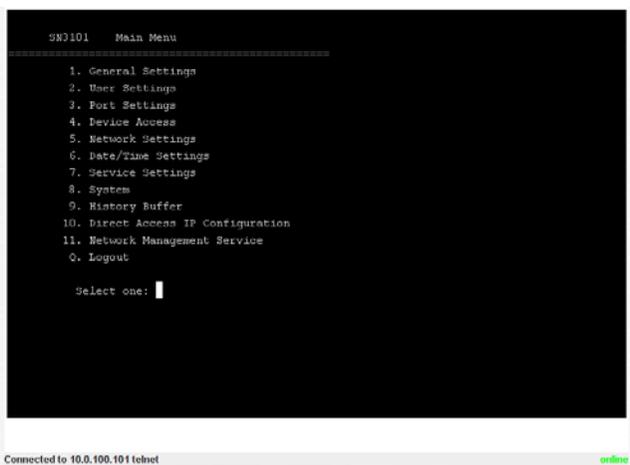
Note: In order for the COM1 entry to appear, the SN3101's COM port must be set to *Console Management* mode (see *Operating Mode*, page 37).

View History

To view a record of the Telnet activity that took place over the SN3101's COM port, click **View History**. A screen showing the events that took place appears. When you are finished, click the browser's *Back* button to return to the *Telnet Selection* screen.

Connect – Local

Selecting *Local* and clicking *Connect* brings up the Main Menu:



The Main Menu is the text based equivalent of the browser based configuration and control functions described in this chapter, and in the *Administration* chapter. You can reference the information provided for the browser version as you work your way through the submenus.

-
- Note:**
1. As with the browser version, access to many of these submenus are restricted to the administrator or users with configuration permission. If you select a submenu that you are not authorized for, nothing will happen.
 2. Some of the submenus do not have an *Exit* choice. In these cases, you can return to the previous menu without making any changes by pressing **Enter** twice.
 3. You can bring up the Main Menu at any time during your session.
 4. This menu can also be accessed from remote terminal sessions, such as Telnet, SSH, and PuTTY. See Chapter 7, *Remote Terminal Operation*. for details.
-

When you have finished with your session, bring up the Main Menu and press **Q** to log out. After you are offline, you can simply close the window.

Connect – COM Port

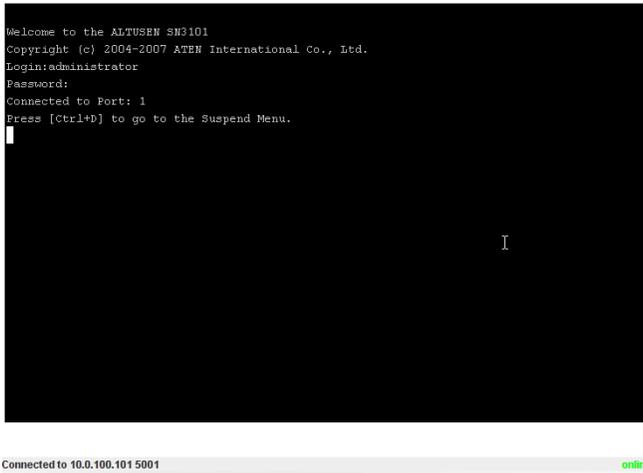
To access a device connected to the COM port, select *COM1*, then click **Connect**.

Note: The SN3101's COM port must be set to *Console Management* mode (see *Operating Mode*, page 37), in order for the COM1 entry to appear.

(Continues on next page.)

(Continued from previous page.)

When you connect, a screen similar to the one below appears:



```
Welcome to the ALTUSEN SW3101
Copyright (c) 2004-2007 ATEN International Co., Ltd.
Login: administrator
Password:
Connected to Port: 1
Press [Ctrl+B] to go to the Suspend Menu.
|
```

Connected to 10.0.100.101 5001 online

- ◆ If you are connected to a computer and want to go to a terminal session or command line to operate it, Press **[Enter]**. When you have finished with the session, log out, then press the suspend character combination to bring up the Main Menu.
- ◆ If you are connected to another device, enter the command that brings it up. In some cases, you may only need to press **[Enter]**. Other devices may require more than that. For example, if you are connected to a PN9108, you would key in: **[???] [Enter]**. When you have finished with the session, log out, then press the suspend character combination to bring up the Main Menu.

(Continues on next page.)

(Continued from previous page.)

- ◆ To display the Suspend Menu, Press **[Ctrl+x]**.

Where **x** represents the Suspend Character set by the Administrator (see *Suspend Character*, page 37). The screen will prompt you as to the correct character. In this example, it is **[Ctrl+D]** (see the prompt on the previous screenshot). The Suspend Menu screen, similar to the one below, appears:



```
SN3101 Suspend Menu
-----
1. Send Break
Q. Goto Main Menu

Select one: |

I

Connected to 10.0.100.101 5001 online
```

- ◆ Press **1** to issue a *Send Break* command to the attached device. This is used to put a Sun system in *OK Mode*.
- ◆ Press **Q** to bring up the Main Menu:
This menu is the same as the one discussed under *Connect – Local*. Refer to page 31, for details.

When you have finished with the Telnet session, bring up the Main Menu and press **Q** to log out. After you are offline, you can simply close the window.

Port Configuration

The administrator and users with port configuration permission (see *User Management*, page 44), can set up the operating parameters for the SN3101's COM (serial) port by clicking the *Port Config* button to bring up the Port Configuration dialog box:

Port Configuration			
Select	Port Number	Port Name	TCP Port
<input checked="" type="radio"/>	COM1	COM1	5001

To set up the serial communications parameters for the SN3101's COM port, click **Property Settings** to bring up the *Port Property Settings* dialog box.

Port Property Settings	
Port ID:	COM1
Port Name:	<input type="text"/>
Interface:	RS-232 <input type="button" value="v"/>
Baud Rate:	9600 bps <input type="button" value="v"/>
Data Bits:	8 bits <input type="button" value="v"/>
Parity:	None <input type="button" value="v"/>
Stop Bits:	1 bit <input type="button" value="v"/>
Flow Control:	None <input type="button" value="v"/>
Enable Toggle DTR:	No <input type="button" value="v"/>
Online Detect:	DSR <input type="button" value="v"/>
Out CRLF Translation:	None <input type="button" value="v"/>
Suspend Character:	<input type="text" value="D"/>
Operating Mode:	Console Management <input type="button" value="v"/> <input type="checkbox"/> Enable Data Encode
Timeout:	3 <input type="text"/> min. (0: Disable)
Authorized Operators:	administrator

Port Property Settings:

The meanings of the property settings are given in the following table:

Setting	Meaning
Port ID	Each port on SN series devices has a port ID number. The value in this field indicates the port that is being configured. Since the SN3101 only has one port, the value is COM1.
Port Name	You can give a port an appropriate name by editing the <i>Port Name</i> field.
Interface	Select the type of serial interface for the port. Choices are RS-232; RS-422; RS-485 (2 Wire).
Baud Rate	This sets the port's data transfer speed. Choices are from 300—460800 (drop down the list to see them all). Set this to match the baud rate setting of the connected device. Default is 9600 (which is a basic setting for many serial devices).
Data Bits	This sets the number of bits used to transmit one character of data. Choices are: 5, 6, 7 and 8. Set this to match the data bit setting of the connected device. Default is 8 (which is the default for the majority of serial devices).
Parity	This bit checks the integrity of the transmitted data. Choices are: None; Odd; Even; Mark; Space. Set this to match the parity setting of the connected device. Default is None (which is the default for the majority of serial devices).
Stop Bits	This indicates that a character has been transmitted. Set this to match the stop bit setting of the connected device. Choices are: 1, 1.5, and 2. Default is 1 (which is the default for the majority of serial devices).
Flow Control	This allows you to choose how the data flow will be controlled. Choices are: None, Hardware (RTS/CTS), and XON/XOFF. Set this to match the flow control setting of the connected device. Default is None.
Enable Toggle DTR	Enabling this parameter allows the DTR signal to toggle between disabled and enabled when the port is occupied. Choices are: No, and Yes. Default is No. Note: For some devices, in order for Enabled to work correctly, you must first disable DTR (select <i>No</i> , then click Update), then Enable it (select <i>Yes</i> , then click Update).
Online Detect	This allows you to set the DSR signal to detect online status or not. Choices are: None and DSR. Default is DSR.

(Continues on next page.)

(Continued from previous page.)

Setting	Meaning
Out CRLF Translation	This allows you to select whether to send a Carriage Return and Line Feed signal (CRLF), or only a Carriage Return signal (CR). Choices are: None (which sends CRLF) and CRLF to CR (which only sends CR), Default is None. Note: If your device outputs double spaced lines, it means that a line feed is automatically added to a carriage return signal. In that case, choose CRLF to CR.
Suspend Character	The <i>Suspend character</i> is used to bring up the Suspend Menu in Telnet sessions (see <i>Telnet</i> , page 43). Note: Valid characters are from A–Z, except H, I, J, and M. Those four characters may not be used.
Operating Mode	Drop down the list to choose the operating mode you want to use. Details regarding the operating modes are provided in Chapter 5, <i>Port Operating Modes</i> . Note: Serial Tunnel cannot be configured with the browser interface. It must be configured with the <i>Serial Network Device Manager</i> software. (See <i>Serial Network Device Manager</i> , page 69.)
Enable Data Encode	Put a check in the box to enable 128-bit SSL encoding of the data before it is sent out over the network. This function applies to the TCP Server, TCP Client, Virtual Modem, and Serial Tunnel operating modes.
Timeout	If there is no input on this port for the amount of time set with this function, the port is released for use by another user.
Authorized Operators	The <i>Authorized Operators</i> field indicates the users that are authorized to operate the port (see <i>User Management</i> , page 44). The information in this field is for viewing purposes only. It can't be changed on this page.

- ◆ When you have finished making your settings choices, click **Update** to save them.
- ◆ To abandon the settings choices without saving them, simply leave the page.

Advanced Settings:

Depending on your *Operating Mode* choice, there may be some further settings that have to be specified. Click the **Port Config** button to get back to the *Port Configuration* screen (see page 35), then click **Advanced Settings**.

Operating Modes that require advanced settings include: Console Management; TCP Client; UDP Mode; and Modbus. Refer to the sections, below for an explanation of the advanced settings dialog boxes that appear.

- ◆ Console Management

The Port Alert Settings dialog box provides a way for you to be informed about problems that occur on the devices connected to the SN3101's ports.

Port Alert Settings	
Port ID:	COM1
Alert String 1:	
Alert String 2:	
Alert String 3:	
Alert String 4:	
Alert String 5:	
Alert String 6:	
Alert String 7:	
Alert String 8:	
Alert String 9:	
Alert String 10:	
<input type="checkbox"/> Enable report from the following SMTP Server	
SMTP Server:	
<input type="checkbox"/> My server requires authentication	
Account Name:	
Password:	*****
From:	
To:	
Update	

When a device has a problem – such as a critical error that requires a reboot, or an SNMP Trap event has been triggered – debug messages can be sent through its serial port to the SN3101's COM port.

When the SN3101 receives such a message, it can send an SNMP Trap alert and/or an email to inform the user specified here of the problem. You can specify up to 10 types of alerts.

To configure a port to provide alert notification, do the following:

1. Use the *Alert String* fields to specify the alerts you want to receive.
2. Enable the *Enable report from the following SMTP Server* checkbox, and key in the IP address or domain name of your SMTP server.
3. If your server requires authentication, put a check in the *My server requires authentication* checkbox.
4. Key in the appropriate account information in the *Account Name*, *Password*, and *From* fields.

Note: Only one email address is allowed in the *From* field.

5. Key in the email address (addresses) of where you want the report sent to in the *To* field.

Note: If you are sending the report to more than one email address, separate the addresses with a comma or a semicolon.

6. When all of your configuration settings have been made, click **Update** to save the information.

After setting up this page, whenever one of the specified alerts is generated, you will be informed by of its occurrence.

(Continues on next page.)

(Continued from previous page.)

◆ TCP Client

In TCP Client Mode, when there is serial data being transmitted from the SN3101's serial port, the SN3101 builds bidirectional TCP connections with up to 16 hosts and sends the serial data to each of these hosts at the same time. The *TCP Client Settings* dialog box allows you to specify the addresses and ports of the hosts that the SN3101 communicates with.

The image shows a dialog box titled "TCP Client Setting". Inside the dialog, there is a section titled "TCP Client Settings". This section contains two columns of input fields. The left column is labeled "Destination Host:" and the right column is labeled "Port:". Each column has 16 rows of input fields. At the bottom center of the dialog, there is a "Save" button.

To configure the settings, do the following:

1. Key in either the hostname or IP address of the device that the SN3101 will communicate with in the *Destination Host* field.
2. Key in the port number that the devices listen for data from the SN3101 on in the *Port* field.
3. When you have made all your specification entries, click **Save** to save the settings.

(Continues on next page.)

(Continued from previous page.)

The configuration settings are described in the following table:

Setting	Explanation
Initial Delay Time	This is the amount of time to wait after the SN3101 boots up before Modbus starts. This gives attached devices (PLCs, IEDs, etc.), time to initialize.
Remote Slave IP*	These are the IP addresses of the SN3101s whose COM ports have been configured as Modbus slaves (ones that have Modbus slave devices connected to them).
TCP Port*	The port that an SN3101 whose COM port has been configured as a Modbus slave listens for data on. The default port number is 502.
ID Range*	The range of numbers for devices (PLCs, IEDs, etc.), connected to the SN3101 whose COM port has been configured as a Modbus slave. The SN3101 configured for Modbus Master decides which SN3101 Modbus slave to communicate with depending on the ID specified in the packet sent by the host.
Auto Slave Unit ID	<ul style="list-style-type: none"> ◆ <i>Enable</i>: Modbus data from the master Modbus device is sent out over the serial port without changing the Modbus ID contained in the Modbus packet ◆ <i>Disable</i>: Modbus data from the master Modbus device is sent out over the serial port with the Modbus ID contained in the Modbus packet changed to a user-specified ID. Specify the desired ID (from 1 – 247), when this parameter is selected.
Character Timeout	This parameter is used when the SN3101 is configured for <i>Modbus RTU Mode</i> . It is used for Modbus to identify the start / end of a packet. Valid settings are from 0 – 3000ms. A setting of zero indicates that the SN3101 should use the standard Modbus timeout value.
Message Timeout	This parameter is used when the SN3101 is configured for <i>Modbus RTU/ASCII Mode</i> . If the Modbus device does not receive a response within the time specified here, the communication times out. Valid settings are from 10 – 3000ms.
Modbus/TCP Exception	If set to Yes, error messages (TCP exception codes) are generated if a problem (such as a message timeout) should occur during Modbus operations.

* These fields only need to be filled in for an SN3101 whose COM port has been configured as a Modbus Master (an SN3101 that has a Modbus master device connected to it).

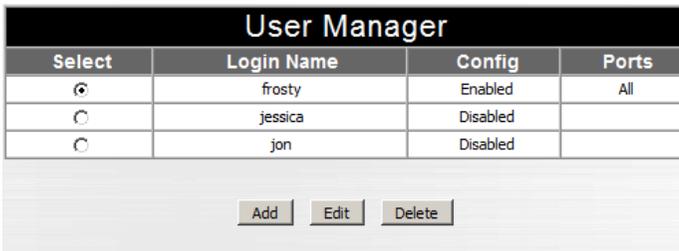
User Management

Clicking the *User Manager* button brings up the User Management dialog box. If this is the first time you are accessing this function, or no user accounts have been created yet, the following screen displays:



Click **New** to begin setting up user accounts.

If user accounts have been set up, the *User Manager* dialog box appears:



This dialog box allows the administrator to add, delete, and edit user accounts. Up to 15 user accounts can be established. Operators must provide the Usernames and Passwords established here, in order to log in.

Adding and Deleting Accounts

- ◆ To add a user account, click **Add**.
- ◆ To delete a user account, select it and click **Delete**.

(Continues on next page.)

(Continued from previous page.)

When you click *Add*, a dialog box similar to the one below appears:

User Information				
Username:	<input type="text"/>	Comments:	<input type="text"/>	
Password:	<input type="text"/>	Reenter password:	<input type="text"/>	
<input type="checkbox"/> Port Config Permission				
Enable	Port Number	Port Name	TCP Port	Shared
<input type="checkbox"/>	COM1	COM1	5001	Yes
<input type="button" value="Add"/> <input type="button" value="Back"/>				

1. Key in the user's Username and Password (up to 16 characters for each).
2. Reenter the password to confirm that it is correct.
3. Key in any Comments you wish to make concerning the user. (optional)
4. If you want the user to have Port Configuration permission, put a check in the *Port Config Permission* checkbox (see *Port Configuration*, page 35), otherwise, leave it blank.
5. Check *Enable*, if you want to allow the user to be able to see the port's status, and to carry out data transactions over the port.
6. The other items in the dialog box are for information only – they are configured in the Port Properties dialog box (see *Port Property Settings*, page 36)

Note: The term "Yes" in the *Shared* column means that other users have access permission to the port.

7. Click **Add** to save your changes.

Editing an Account:

1. To Edit a user account, select the user, then click **Edit**. The user's *User Information* dialog box appears:
2. Make your changes in the appropriate fields and checkboxes.
3. To save your changes, click **Update**.
4. To exit without saving any changes, click **Back**.

Direct Access

The *Direct Access* function works in conjunction with SN3101 COM ports whose operating modes have been specified as *Real COM*, *TCP Server*, and *Modbus Slave* (see *Operating Mode*, page 37).

Direct Access IP Configuration	
IP 01:	<input type="text"/>
IP 02:	<input type="text"/>
IP 03:	<input type="text"/>
IP 04:	<input type="text"/>
IP 05:	<input type="text"/>
IP 06:	<input type="text"/>
IP 07:	<input type="text"/>
IP 08:	<input type="text"/>
IP 09:	<input type="text"/>
IP 10:	<input type="text"/>
IP 11:	<input type="text"/>
IP 12:	<input type="text"/>
IP 13:	<input type="text"/>
IP 14:	<input type="text"/>
IP 15:	<input type="text"/>
IP 16:	<input type="text"/>
IP 17:	<input type="text"/>
IP 18:	<input type="text"/>
IP 19:	<input type="text"/>
IP 20:	<input type="text"/>
IP 21:	<input type="text"/>
IP 22:	<input type="text"/>
IP 23:	<input type="text"/>
IP 24:	<input type="text"/>
IP 25:	<input type="text"/>
IP 26:	<input type="text"/>
IP 27:	<input type="text"/>
IP 28:	<input type="text"/>
IP 29:	<input type="text"/>
IP 30:	<input type="text"/>
IP 31:	<input type="text"/>
IP 32:	<input type="text"/>

If no IP addresses are specified here, any host can open a TCP/IP session to the SN3101's COM port and use the SN3101's IP address and socket base port for data transmission.

If specific IP addresses are entered here, however, only hosts at those addresses can open a TCP/IP session to access the port.

To impose limitations on the ability to directly access the affected ports, key in the IP addresses that will be allowed access.

Session Info

Clicking the *Session Info* button brings up the Active Sessions display:

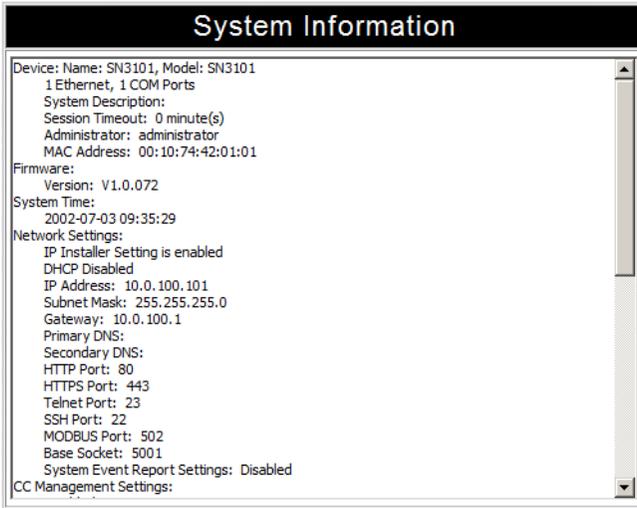
Active Sessions								
Select	Login Name	Local User	Admin	Port	Service	IP	UP Time	Last Access
<input checked="" type="radio"/>	administrator	Yes	Yes	Local	HTTPS	10.0.13.229	08:48:54	08:58:03
<input type="radio"/>	frosty	Yes	-	Local	HTTPS	10.0.13.228	08:50:22	08:54:50
<input type="radio"/>	jessica	Yes	-	Local	HTTPS	10.0.13.227	08:56:49	08:57:10

This display lets the administrator see at a glance all the users currently logged into the SN3101, and provides information about each of their sessions.

It also gives the administrator the option of forcing a user logout by selecting the user and clicking **End Session**.

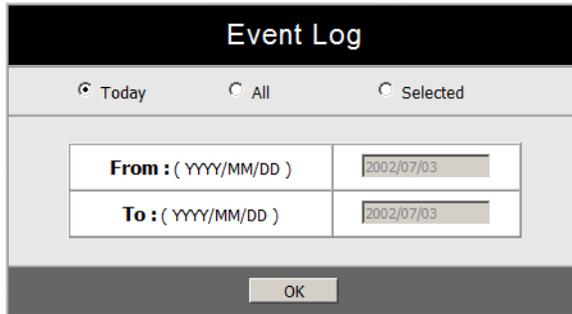
Sys Info

The System Information dialog box provides information about all aspects of the SN3101's configuration:



Log

Clicking the *Log* button brings up the Event Log dialog box:



The Event Log dialog box features a title bar with the text "Event Log". Below the title bar are three radio buttons: "Today" (which is selected), "All", and "Selected". The main area contains two rows of input fields. The first row is labeled "From : (YYYY/MM/DD)" and has a text box containing "2002/07/03". The second row is labeled "To : (YYYY/MM/DD)" and also has a text box containing "2002/07/03". At the bottom center of the dialog is an "OK" button.

The SN3101 maintains a log file of the events that take place on it. This dialog box allows you to select the range of events you wish to view:

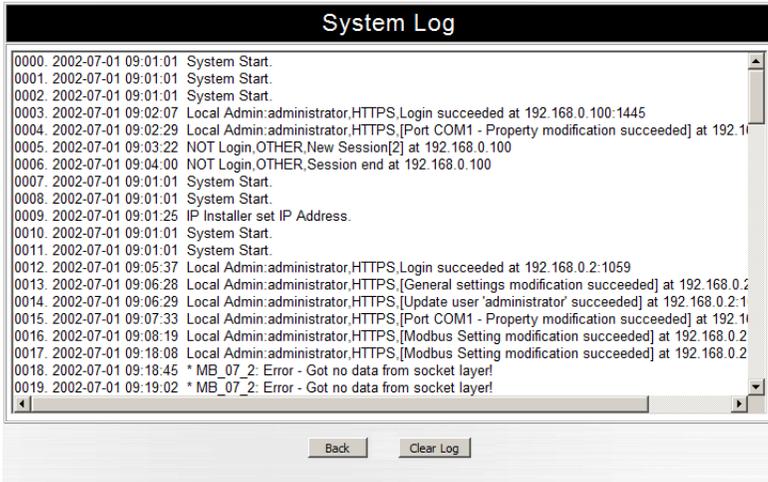
- ♦ Choose **Today** then click **OK** to see a listing of only today's events.
- ♦ Choose **All** then click **OK** to see a listing of events for the entire log file.
- ♦ Choose **Selected**; key in the desired range of dates in the *From* and *To* fields; then click **OK** to see a listing of events for a specific time period.

Note: The maximum number of events contained in the log file is 512. Once that amount is reached, the oldest events are discarded as new ones are recorded.

(Continues on next page.)

(Continued from previous page.)

Once you make a choice and click OK an Event Log List, similar to the one below, appears:



When you have finished viewing the event list:

- ◆ If you want to return to the Event Log dialog box, click **Back**.
- ◆ If you want to erase the contents of the entire log file, click **Clear All**.
- ◆ To exit, select a different function from the button bar.

Chapter 7

Remote Terminal Operation

Overview

The SN3101 can be accessed via a remote terminal session using a number of methods, including HyperTerminal, Telnet, SSH, or PuTTY, as described in the sections that follow.

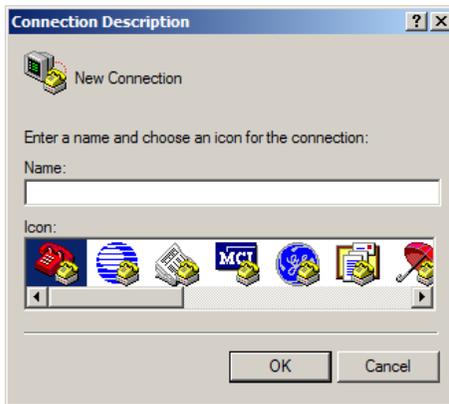
HyperTerminal

HyperTerminal is a program included with Windows that can be used to establish a Telnet session with the SN3101. To establish the connection, do the following:

1. On your PC, run the HyperTerminal program:

Start → Programs → Accessories → Communications → HyperTerminal → Hypertrm.exe

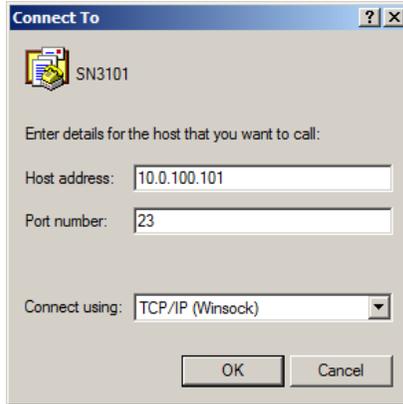
The following dialog box appears:



(Continues on next page.)

(Continued from previous page.)

2. Key a name to describe the connection in the *Name* field (we chose SN3101); select an icon to represent the connection; then click **OK**. A dialog box similar to the one below comes up:



3. For the *Connect using:* field, select TCP/IP (Winsock); then click OK. HyperTerminal opens up a Telnet session and you can log in to the SN3101 with your Username and Password to bring up the SN3101's Main Menu. See *Telnet*, page 31 for Telnet operation.

Note: To control a device connected to the SN3101's COM port – rather than opening the SN3101's Main Menu – replace the port number (23) with the port number that was set for the *Socket* entry under *Network* configuration (see *Service Ports*, page 16).

4. When you close HyperTerminal, save the SN3101 entry – the next time you run the program, you can find it under *Open* in the File Menu and run it directly without going through the setup steps.

Telnet

Logging In

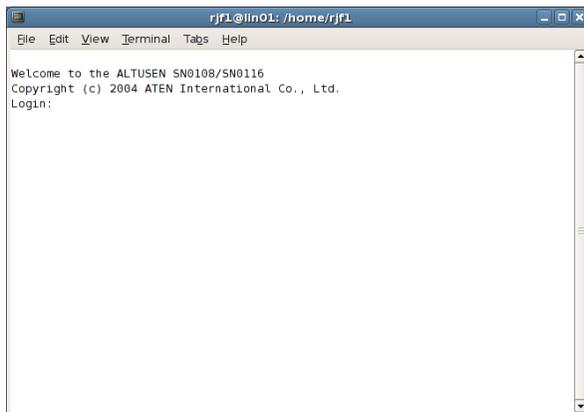
1. On your computer, open a terminal (command line) session.
2. At the prompt, key in the SN3101's IP Address in the following way:

```
telnet [IP Address]
```

Note: The default telnet port is 23. To control a device connected to the SN3101's COM port – rather than opening the SN3101's Main Menu – specify the port number that was set for the *Socket* entry under *Network* configuration (see *Service Ports*, page 16). For example: **telnet [IP Address]5001**

3. Press **Enter**.

The following screen appears:



4. At the login prompt, provide your Username and Password.

Note: If you cannot see the login prompt click *Terminal/Preferences* on the telnet session's menu bar, then select *VT-100/ANSI*.

Once a Telnet connection to the device is established, the SN3101 Main Menu comes up. See *Telnet*, page 31 for Telnet operation.

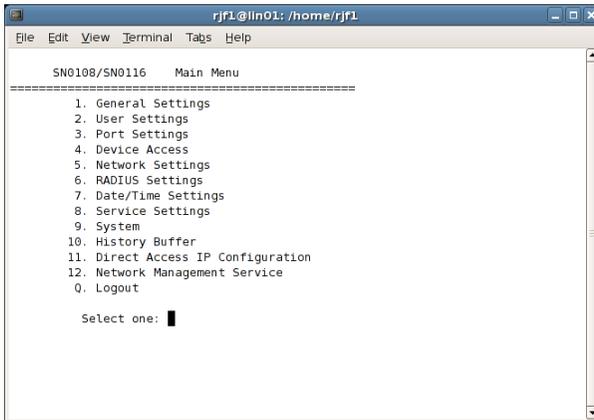
SSH

Terminal Session (Linux):

1. Open a terminal (command line) on your computer.
2. At the prompt, key in your SN3101 Username and the SN3101's IP Address in the following way:

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

3. Press **Enter**
4. When you are prompted for a password, use your SN3101 password.
Once an SSH connection to the device is established, the SN3101 Main Menu comes up:



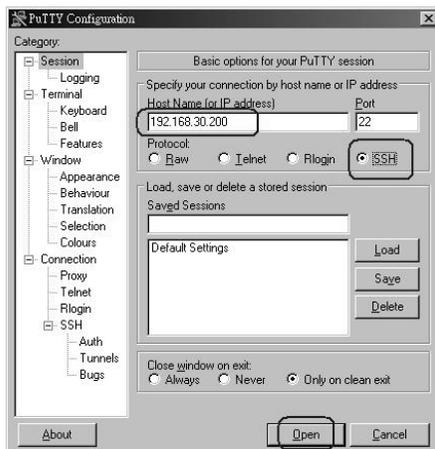
This menu is the same as the main menu that appears with Telnet sessions (see *Telnet*, page 31 for Telnet operation).

Note: The default SSH port is 22. To control a device connected to the SN3101's COM port – rather than opening the SN3101's Main Menu – specify the port number that was set for the *Socket* entry under *Network* configuration (see *Service Ports*, page 16). For example:
SSH [username@IP Address] -P 5101

Third Party Utility (Windows):

SSH sessions can be implemented under Windows with the use of third party utility software, such as PuTTY, a free implementation of Telnet and SSH for the Win32 and Unix platforms. To make an SSH connection with PuTTY, do the following:

1. In the *Host Name* box, enter the Internet host name of the server you want to connect to.



2. Select *SSH* from the Protocol buttons.
3. Click **Open** (at the bottom of the dialog box)
4. After you have connected, provide your SN3101 username and password at the login prompts.

Note: If you make a mistake keying in the username, the SSH protocol doesn't allow you to try again. You must close PuTTY and start over.

Once an SSH connection to the device is established, the SN3101 Main Menu comes up. This menu is the same as the main menu that appears with Telnet sessions (see *Telnet*, page 31 for Telnet operation).

Note: The default SSH port is 22. To control a device connected to the SN3101's COM port – rather than opening the SN3101's Main Menu – specify the port number that was set for the *Socket* entry under *Network* configuration (see *Service Ports*, page 16). For example:
 SSH [username@IP Address] -P 5101

This Page Intentionally Left Blank

Chapter 8

Virtual Port Management

Overview

The SN3101 offers Virtual COM Port support – *Real COM Port* drivers for Windows, as well as a TTY driver for Linux. By running the driver on a local computer, devices connected to the SN3101's COM port, appear as if they are directly connected to a COM port on the local computer. Data transmission takes place over the Internet between the local computer's virtual COM port and the device connected to the SN3101's COM port.

Note: Only a port designated as a Real COM Port can be configured as a virtual port. See *Operating Mode*, page 37, for details.

This mode is useful with serial devices such as POS terminals, Bar Code Readers, Serial printers, etc. In addition, this mode can be used with other Altusen management products, such as the PN9108 Power Over the NET.

Driver Installation

In order to utilize virtual COM port management, the Altusen virtual COM port driver must be installed. To install the driver, do the following:

Windows 2000 and Higher Installation

To install the Windows 2000 and higher driver, do the following:

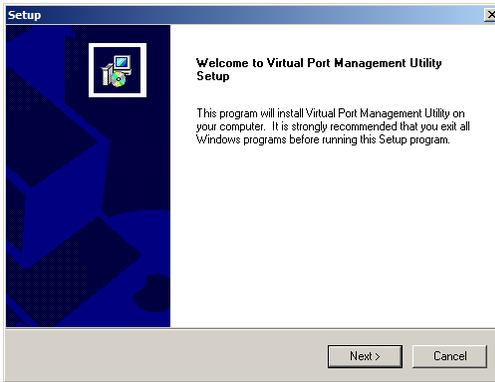
1. On the software CD that came with your SN3101 package, locate the file:
SN3101 Virtual Port vxxx.exe

Note: The *vxxx* specified above stands for the driver's version number. The file on the CD will show an actual version number.

(Continues on next page.)

(Continued from previous page.)

2. Double click the filename to start the installation. The Setup screen appears:



3. Click **Next** to move on.
4. Click **Yes** to accept the License Agreement.
5. Continue through the setup screens to complete the driver installation.

Uninstalling the Driver

To uninstall the driver do the following:

1. Open the Windows Start menu.
2. Select: All Programs → Virtual Port Management Utility → Uninstall Manager.

Windows 98 Installation

Windows 98 driver installation is the same as that of the Windows 2000 and HIgher installation described, above. The only difference is that the file you will use is named: *SN3101 Virtual Port for Win98 vxxx.exe*.

Uninstalling the driver follows the same procedure as mentioned above.

TTY Driver Installation for Linux

To install the TTY driver for Linux, do the following:

1. On the software CD that came with your SN3101 package, locate the file: *AtenVPInstall_vxxx.tgz*.

Note: The *vxxx* specified above stands for the driver's version number. The file on the CD will show an actual version number.

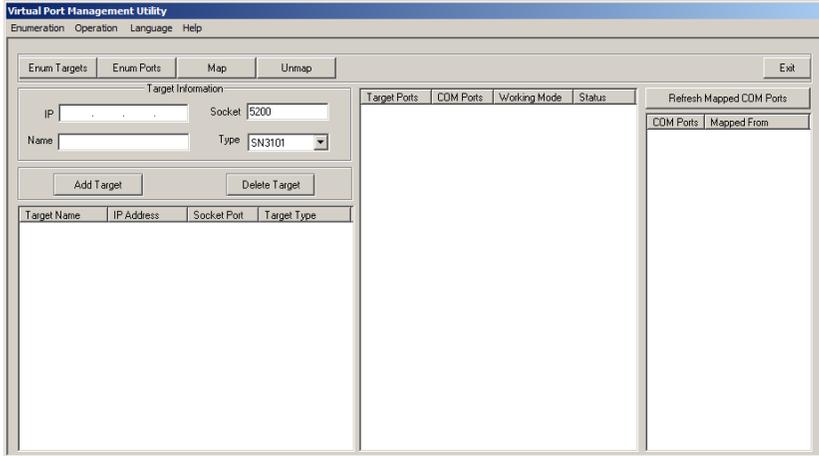
2. Unpack the file to a convenient location on your hard disk.
3. Execute the file: *AtenVPInstall*.
4. After the installation completes, log out and then log back in.

Uninstalling the Driver

To uninstall the driver, execute the file: *AtenVPUnInstall*.

Real COM Port Management – Windows

The Virtual Port Management Utility for Windows provides a convenient interface to COM port mapping. When you run the *Virtual Serial Port Manager* program (Start → Virtual Port Management Utility → Virtual Serial Port Manager), the following dialog box appears:



Dialog Box Layout

The Virtual Port Management Utility dialog box 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, there is an area to input information in order to manually list target devices if the device doesn't appear using the automatic enumeration method.
- ◆ All target devices that were found by enumeration or manually entered are listed in the left side panel.
- ◆ All ports that were found for a selected target device are enumerated in the central panel.
- ◆ The right side panel displays the virtual COM port mappings that you have made.

Menu and Toolbar

The Virtual Port Management Utility menu and toolbar have the same captions and functions. Users can either click the menu items or buttons to invoke the desired function, as shown in the table below:

Item	Action
Enum Targets	This function searches and lists all SN devices on the LAN – these include SN0108 and SN0116 devices, as well as SN3101s. The results are shown in the Target List panel (see <i>Target List</i> , page 62, for details). Be aware 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 <i>Port List</i> panel, selecting this function maps the device's COM port to a virtual COM port on the user's computer.
Unmap	After selecting a port from the <i>Mapped Ports</i> list, selecting this function removes the mapping between the computer and the device's COM port.

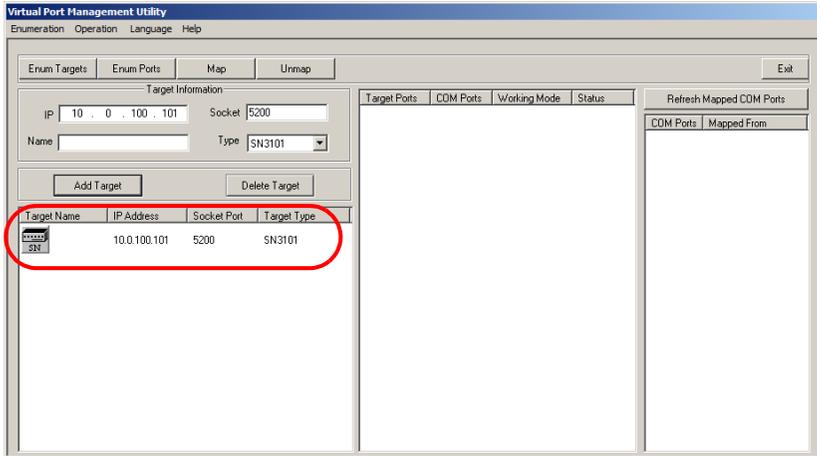
Target Information

The Target Information fields allow a user to install (map) ports on an offline target device, as follows:

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, it will be replaced by the real one. Note that the name is not related to the mapping or unmapping process. Only the IP address, socket port and target type are relevant.
Target Type	The type of target to be mapped. SN3101, SN0108, and SN0116 devices are valid target types.
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 side 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.

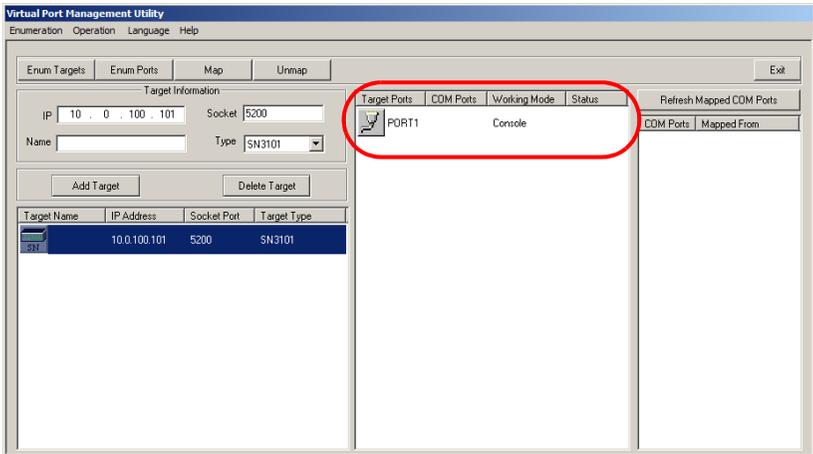


Note: Double clicking an item in the list invokes the same function as selecting **Enum Ports** – which displays the numbers and working modes of the selected target’s ports in the *Port List* column.

- ◆ 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 on line and is ready to be mapped.
- ◆ If a device was added to the list manually and is off line, the icon to its left is drawn with black dots and lines. Double clicking a manually added item can get some information and display it in the *Port List*, but the working mode information is not accurate and we must assume that all the device’s ports are in Virtual Port mode. See *Operating Mode*, page 37 for details about port modes.
- ◆ If the target is off line or is on line 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 Virtual Port mode. See *Operating Mode*, page 37 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 setting for the port that was specified when the port was configured. See *Port Configuration*, page 35, for details.

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

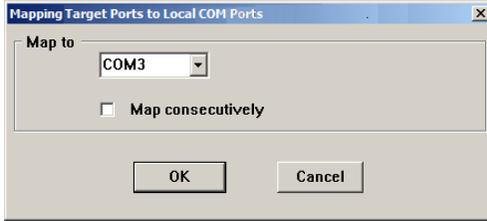
Note: The *Port Mapping* dialog box can also be invoked either by clicking MapTo... on the toolbar or selecting MapTo... from the menu.

Port Mapping and Unmapping

Port Mapping

To map a virtual COM port:

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



2. Drop down the list of available COM ports and select the COM port you wish to map the Target port to.
3. Click **OK**.

Note: 1. Since there is only one COM port to map, you can disregard the *Map consecutively* checkbox.

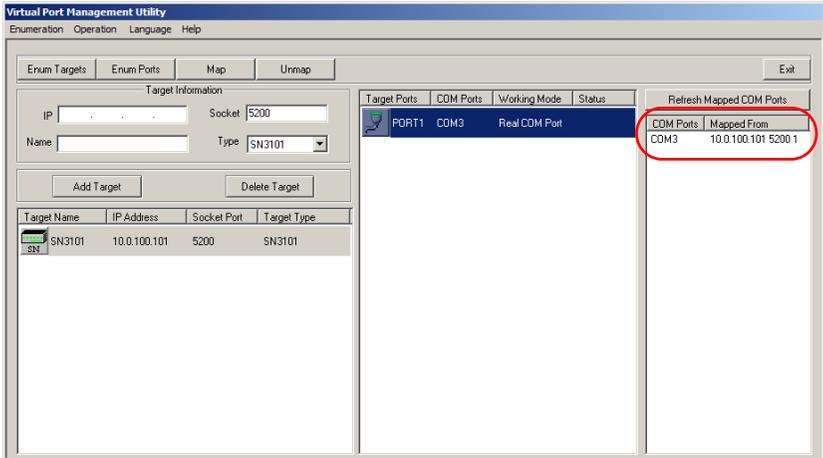
2. If a warning dialog box comes up, you can safely ignore it. Click **Continue Anyway** to complete the operation

(Continues on next page.)

(Continued from previous page.)

Mapped COM Port

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



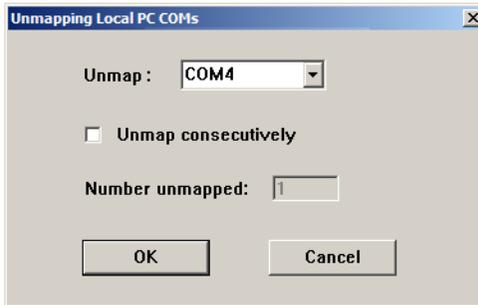
(Continues on next page.)

(Continued from previous page.)

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.

Note: Since there is only one COM port to unmap, you can disregard the *Unmap consecutively* checkbox.

Real COM Port Management – Linux

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 don't specify any parameters on the command line. They make mapping/unmapping choices based on questions generated as the program runs.

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

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

```
./AtenVPMapping map(1) PCPort(0-255) TargetIP(a.b.c.d)  
TargetPort(1-48) NumberofMapping(1-48)
```
2. Unmapping (input should all be on one line):

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

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`.

This Page Intentionally Left Blank

Chapter 9

Serial Network Device Manager

Overview

To help manage your SN3101 installation more conveniently and efficiently, a Windows-based configuration and management utility – the *Serial Network Device Manager* – has been provided on the software CD that came with your package. This chapter describes the installation, features, and use of the utility.

Note: The Serial Network Device Manager only supports Windows 2000 and higher.

Installation

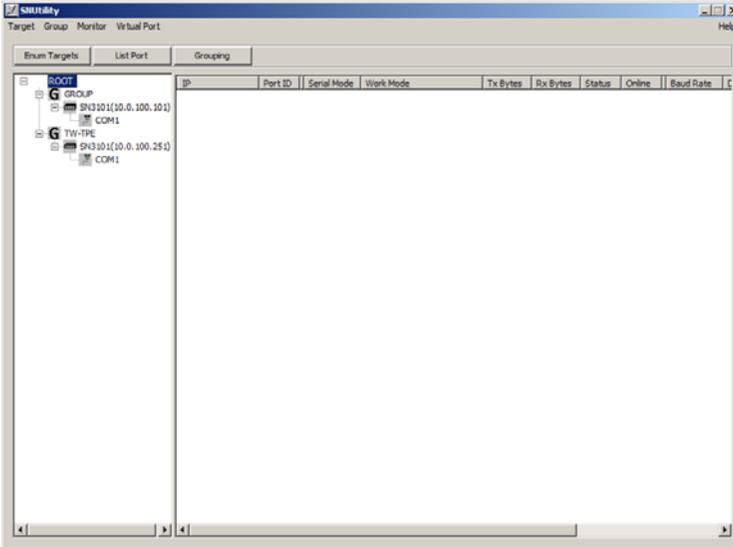
The Serial Network Device Manager gets installed when you install the virtual COM port driver (see *Virtual Port Management*, page 57).

(Continues on next page.)

(Continued from previous page.)

Operation

When you run the *Serial Network Device Manager* program (Start → Virtual Port Management Utility → Serial Network Device Manager), the following dialog box appears:



Dialog Box Layout

The Serial Network Device Manager dialog box is laid out as follows:

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

The Menu Bar

The Menu Bar contains five items. Each is discussed in the sections that follow:

Target

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

Item	Action
System Info	Lists all the settings that have been configured for the device. See <i>Sys Info</i> , page 48.
General Settings	This is similar to the browser-based page. See <i>General</i> , page 13.
Network Settings	This is similar to the browser-based page. See <i>Network</i> , page 16.
ANMS Settings	This is similar to the browser-based page. See <i>ANMS</i> , page 19.
Log	This is similar to the browser-based page. See <i>Log</i> , page 49.
Backup/Restore	This is similar to the browser-based page. See <i>Backup</i> , page 15.
Firmware Upgrade	This is similar to the browser-based page. See <i>Firmware</i> , page 24.
Serial Tunnel	Select this item to build a Serial Tunnel connection between two SN3101 units. See <i>Serial Tunnel</i> , page 28 for more information on Serial Tunnels. See <i>Serial Tunnel Creation</i> , page 74 for information on building Serial Tunnels.

Group

This function allows you to configure and manage a number of SN3101 devices at the same time by assigning them to groups. To configure the settings for a group, select it from the list in the left panel. The changes that you make to the various settings (described below), affect all the members of the selected group.

The meanings of the menu entries are provided in the table below:

Item	Action
Grouping	Clicking this item causes all the groups to appear (each group under its own tab) in the right hand panel. Click a tab to see the members of the group.
Add a New Group	Brings up a dialog box that allows you to key in the name for a new group. After you click OK and exit, the group is added to the group list in the left panel tree. To assign a device to a group, use the <i>General Settings</i> function of the <i>Target Menu</i> and key the Group Name in the appropriate entry field.
Group Rename	First select the group from the left panel, then select this item to key in the new name for the group. After you click OK and exit, the new name replaces the old one in the left panel tree.
Group General Settings	This is similar to the browser-based page. See <i>General</i> , page 13.
Group Network Settings	This is similar to the browser-based page. See <i>Network</i> , page 16.
Group ANMS Settings	This is similar to the browser-based page. See <i>ANMS</i> , page 19.
Restore	This is similar to the browser-based page. See <i>Backup</i> , page 15.
Firmware Upgrade	This is similar to the browser-based page. See <i>Firmware</i> , page 24.
Port Basic Settings	This is similar to the Port Property Settings dialog box. See <i>Port Configuration</i> , page 35
Port Alert String Settings	This is similar to the Port Alert Settings dialog box. See <i>Console Management</i> , page 38
Port Modbus Settings	This is similar to the Modbus Settings dialog box. See <i>Modbus.</i> , page 42

Monitor

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

Item	Action
Enum Targets	Selecting this item causes the program to search and list (enumerate), all SN target devices that it finds in a tree view in the left panel of the screen.
Refresh Port (Static)	Clicking <i>Refresh Port (Static)</i> , information about each of the enumerated ports appears in the right panel of the screen.
Refresh Port (Dynamic)	This item is similar to the Refresh Port (Static) item, except that instead of refreshing the ports manually, you can have the ports be automatically refreshed at a set time interval. Valid time intervals are 10 sec., 30 sec., 60 sec., 2 min., 5 min., and 10 min.

Virtual Port

Selecting this item brings up the *Virtual Port Management Utility*. See page 60 for details.

The Button Bar

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

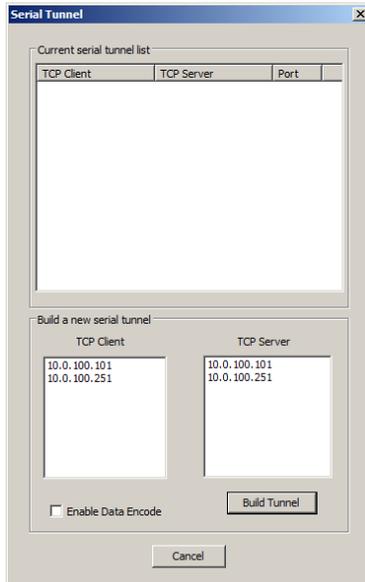
- ◆ **Enum Targets** — performs the same function as the Enum Targets entry on the Monitor menu performs.
- ◆ **List Port** — performs the same function as the Refresh Port (Static) entry on the Monitor menu performs.
- ◆ **Grouping** — performs the same function as the Grouping entry on the Group menu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

Serial Tunnel Creation

Building a Serial Tunnel

To build a Serial Tunnel connection between two SN3101 units, do the following:

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



If any Serial Tunnels have already been established, they show in the large upper panel.

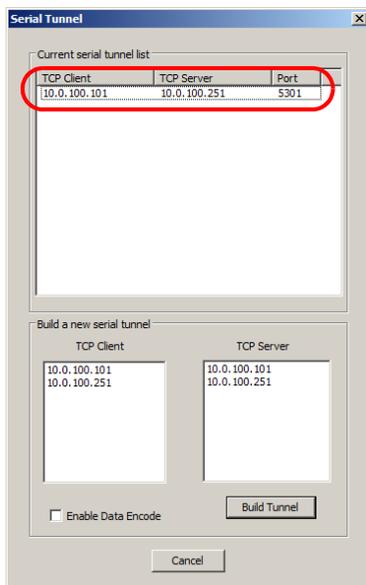
2. Select the unit that will be the Client from the list in the lower left panel; select the unit that will be the Server from the list in the lower right panel.
3. If you want the transmitted data to be encoded, click to put a checkmark in the *Enable Data Encoding* checkbox.

(Continues on next page.)

(Continued from previous page.)

4. Click **Build Tunnel**.

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



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

Removing a Serial Tunnel

Since a serial tunnel is composed of a master SN3101 (acting as a TCP server) and a slave SN3101 (acting as a TCP client), removing a serial tunnel is accomplished by simply changing the operating mode of either SN3101.

This Page Intentionally Left Blank

Chapter 10

LDAP Server Configuration

Introduction

The SN3101 allows log in authentication and authorization through external programs. This chapter describes how to configure Active Directory and OpenLDAP for SN3101 authentication and authorization.

Active Directory

To allow authentication and authorization for the SN3101 via LDAP or LDAPS, the Active Directory's LDAP *Schema* must be extended so that an extended attribute name for the SN3101 – *accessPort* – is added as an optional attribute to the *person* class.

Note: *Authentication* refers to determining the authenticity of the person logging in; *authorization* refers to assigning permission to use the device's various functions.

In order to configure the LDAP server, you will have to complete the following procedures: 1) Install the Windows Server Support Tools; 2) Install the Active Directory Schema Snap-in; and 3) Extend and Update the Active Directory Schema.

The following section provides an example of configuring LDAP under Windows 2003 Server.

Install the Windows 2003 Server Support Tools

To install the Windows 2003 ServerSupport Tools, do the following:

1. On your Windows Server CD, open the Support → Tools folder.
2. In the right panel of the dialog box that comes up, double click **SupTools.msi**.
3. Follow along with the Installation Wizard to complete the procedure.

Install the Active Directory Schema Snap-in

To install the Active Directory Schema Snap-in, do the following:

1. Open a Command Prompt.
2. Key in: `regsvr32 schmmgmt.dll` to register schmmgmt.dll on your computer.
3. Open the *Start* menu; click **Run**; key in: `mmc /a`; click **OK**.
4. On the *File* menu of the screen that appears, click **Add/Remove Snap-in**; then click **Add**.
5. Under *Available Standalone Snap-ins*, double click **Active Directory Schema**; click **Close**; click **OK**.
6. On the screen you are in, open the *File* menu and click **Save**.
7. For *Save in*, specify the `C:\Windows\system32` directory.
8. For *File name*, key in **schmmgmt.msc**.
9. Click **Save** to complete the procedure.

Create a Start Menu Shortcut Entry

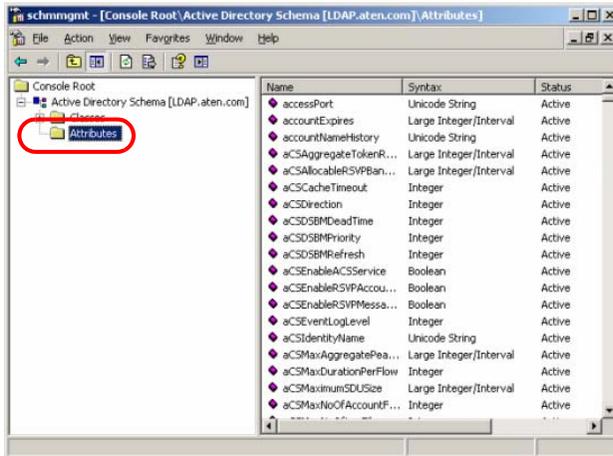
To create a shortcut entry on the Start Menu for the Active Directory Schema, do the following:

1. Right click Start; select: **Open all Users** → **Programs** → **Administrative Tools**.
2. On the *File* menu, select **New** → **Shortcut**
3. In the dialog box that comes up, browse to, or key in the path to schmmgmt.msc (`C:\Windows\system32\schmmgmt.msc`), then click **Next**.
4. In the dialog box that comes up, key in *Active Directory Schema* as the name for the shortcut, then click **Finish**.

Extend and Update the Active Directory Schema

To extend and update the Active Directory Schema, do the following 3 procedures:

1. Create a New Attribute named *accessPort*:
 - a) Start → Administrative Tools → Active Directory Schema.
 - b) In the left panel of the screen that comes up, right-click **Attributes**:



- c) Select New → Attribute.
- d) In the warning message that appears, click **Continue** to bring up the *Create New Attribute* dialog box.

(Continues on next page.)

(Continued from previous page.)

- e) Fill in the dialog box to match the entries shown below, then click **OK** to complete step 1 of the procedure.

Note: The Unique X500 Object ID uses periods, not commas.

Create New Attribute ? X

Create a New Attribute Object

Identification

Common Name: accessPort

LDAP Display Name: accessPort

Unique X500 Object ID: 1.3.6.1.4.1.21317.1.1.4.2.1

Description: Access right to UART ports

Syntax and Range

Syntax: Unicode String

Minimum: 1

Maximum: 255

Multi-Valued

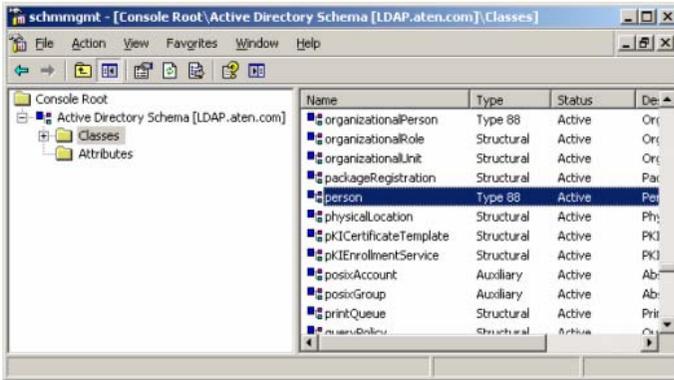
OK Cancel

2. Extend the Object Class With the New Attribute:
- Control Panel → Administrative Tools → Active Directory Schema.
 - In the left panel of the screen that comes up, select **Classes**.

(Continues on next page.)

(Continued from previous page.)

c) In the right panel, right-click **person**:



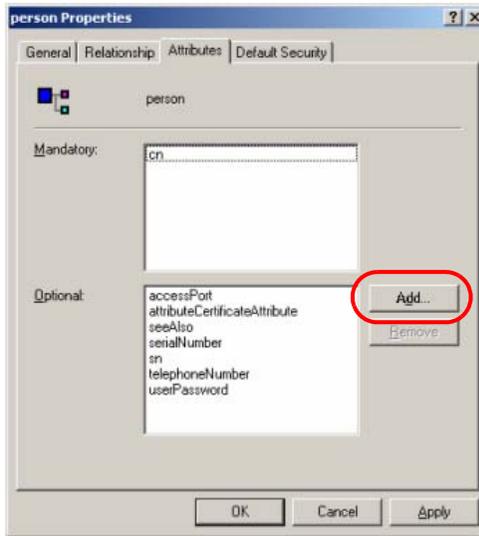
d) Select **Properties**; the *person Properties* dialog box comes up with the *General* page displayed. Click the *Attributes* tab.



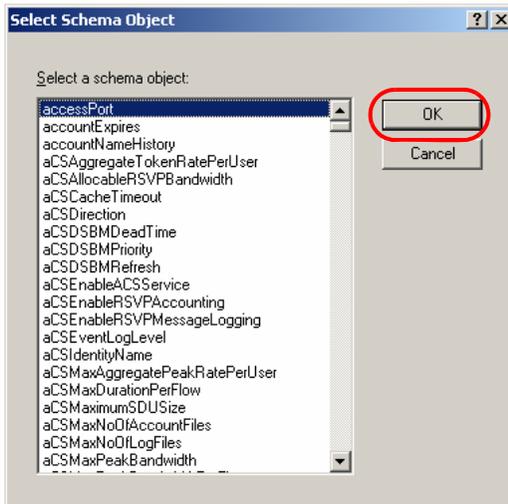
(Continues on next page.)

(Continued from previous page.)

e) On the *Attributes* page, click **Add**:

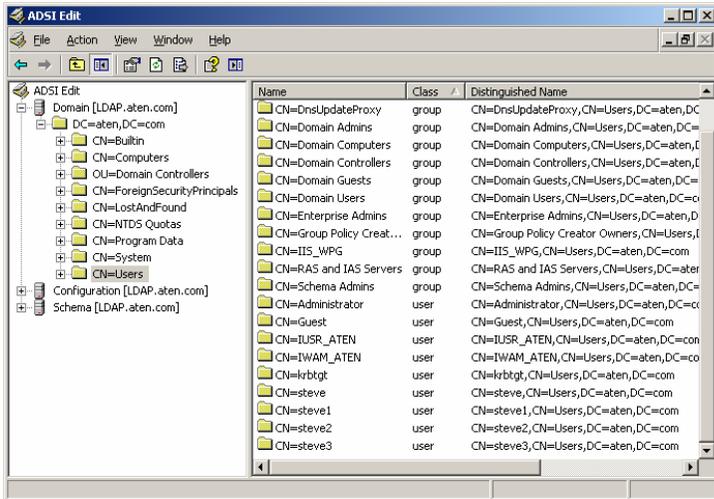


f) In the list that comes up, select **accessPort**, then click **OK** to complete step 2 of the procedure.



3. Edit Active Directory Users With the Extended Schema:

- a) Run **ADSI Edit**. (Installed as part of the *Support Tools*.)
- b) Open **domain**, and navigate to the *cn=users dc=aten dc=com* node.
- c) Locate the user you wish to edit. (Our example uses *steve3*.)

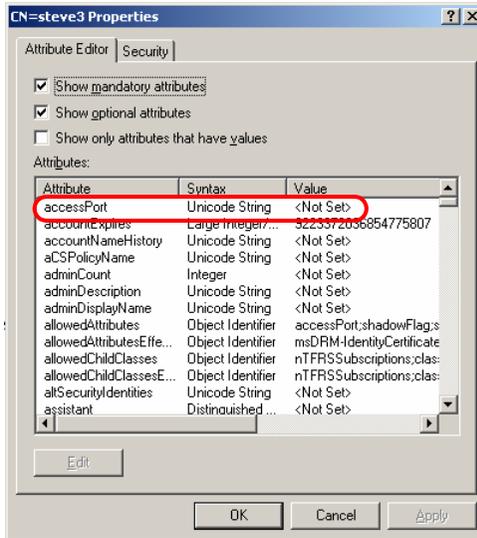


- d) Right-click on the user's name and select **properties**.

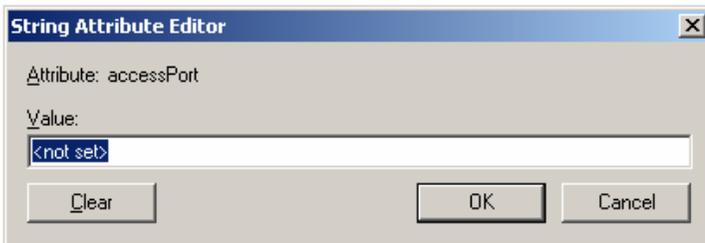
(Continues on next page.)

(Continued from previous page.)

- e) On the *Attribute Editor* page of the dialog box that appears, select **accessPort** from the list.



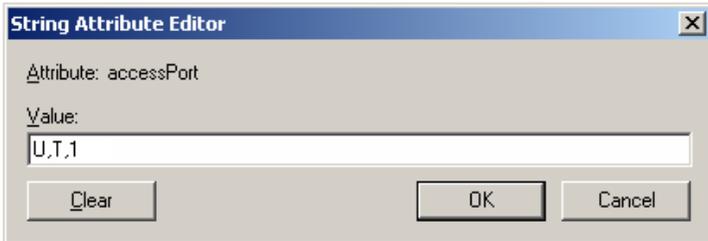
- f) Click **Edit** to bring up the *String Attribute Editor*:



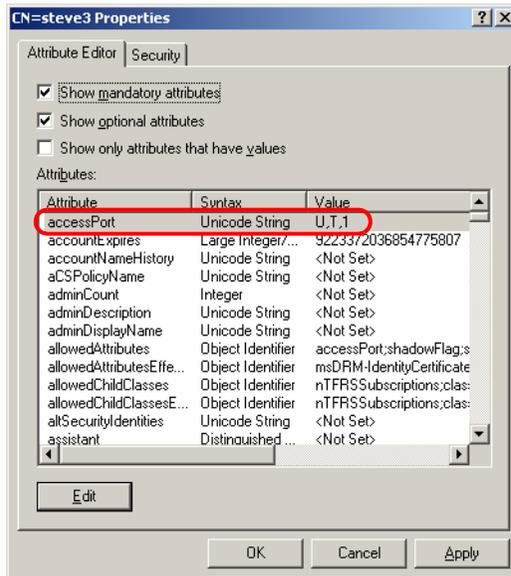
(Continues on next page.)

(Continued from previous page.)

- g) Key in the desired SN3101 permission attribute values (see *The Permission Attribute Value*, page 86 for details). For example:



- h) Click **OK**. When you return to the *Attribute Editor* page, the *accessPort* entry now reflects the new permissions:



- i) Click **Apply** to save the change and complete the procedure.
- j) Repeat Step 3 (*Edit Active Directory Users With the Extended Schema*;) for any other users you wish to add.

The Permission Attribute Value

The attribute value for *accessPort* is made up of two parts: 1) the IP address of the SN3101 a user will access; and 2) a string that indicates the access rights the user has on the SN3101 at that IP address. For example:

```
192.168.0.80&u,t,1;u,f
```

The makeup of the permission entry is as follows:

- ◆ An ampersand (&) connects the SN3101's IP with the access rights string.
- ◆ The access rights string is made up of various combinations of the following characters: u, t, f, a, and 1 (one). The characters can be entered in upper or lower case. The meanings of the characters is provided in the *Permission String Characters* table, below.
- ◆ The characters in the access rights string are separated by a comma (,). There are no spaces before or after the comma.
- ◆ If a user has access rights to more than one SN3101, each permission segment is separated by a semicolon (;). There are no spaces before or after the semicolon.

Permission String Characters

Character	Meaning
U	(User) User has port access rights.
T	(True) User has port configuration rights.
F	(False) User does not have port configuration rights.
A	(All) User has rights to all ports.
1	(One) User has rights to port 1.

Permission Examples

Access rights examples are given in the table, below:

User	String	Meaning
User1		User has default rights for all SN3101 devices. This means that the user can access port 1 of all SN3101 devices, but cannot configure any of them.
User2	10.0.0.166&U,T,1	<ol style="list-style-type: none"> 1. User can access and configure port 1 of an SN3101 whose IP is 10.0.0.166. 2. User has default rights for all other SN3101 devices.
User3	10.0.0.164&U,T,1;10.0.0.166&U,T,1	<ol style="list-style-type: none"> 1. User can access and configure port 1 of an SN3101 whose IP is 10.0.0.164. 2. User can access and configure port 1 of an SN3101 whose IP is 10.0.0.166. 3. User has default rights for all other SN3101 devices.
User4	U,F,A;10.0.0.164&U,T,1	<ol style="list-style-type: none"> 1. User can access and configure port 1 of an SN3101 whose IP is 10.0.0.164. 2. User has default rights for all other SN3101 devices.
User5	U,T,1	User can access and configure port 1 of all SN3101 device.
User6	U,F	User cannot access or configure any SN3101 devices.
User7	10.0.0.165&U,F	<ol style="list-style-type: none"> 1. User cannot access or configure port 1 of an SN3101 whose IP is 10.0.0.165. 2. User has default rights for all other SN3101 devices.

OpenLDAP

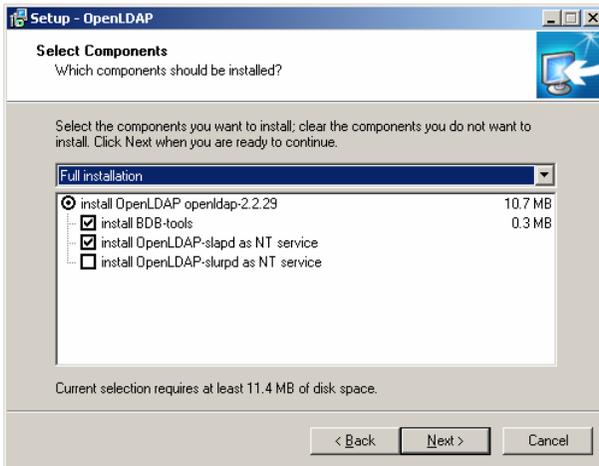
OpenLDAP is an Open source LDAP server designed for Unix platforms. A Windows version can be downloaded from:

```
http://download.bergmans.us/openldap/openldap-2.2.29/  
openldap-2.2.29-db-4.3.29-openssl-0.9.8a-  
win32_Setup.exe.
```

OpenLDAP Server Installation

After downloading the program, launch the installer, select your language, accept the license and choose the target installation directory. The default directory is: *c:\Program Files\OpenLDAP*.

When the *Select Components* dialog box appears, select *install BDB-tools* and *install OpenLDAP-slapd as NT service*, as shown in the diagram, below:



OpenLDAP Server Configuration

The main OpenLDAP configuration file, *slapd.conf*, has to be customized before launching the server. The modifications to the configuration file will do the following:

- ◆ Specify the Unicode data directory. The default is *./ucdata*.
- ◆ Choose the required LDAP schemas. The core schema is mandatory.
- ◆ Configure the path for the OpenLDAP *pid* and *args* start up files. The first contains the server pid, the second includes command line arguments.
- ◆ Choose the database type. The default is *bdb* (Berkeley DB).
- ◆ Specify the server suffix. All entries in the directory will have this suffix, which represents the root of the directory tree. For example, with suffix *dc=aten,dc=com*, the fully qualified name of all entries in the database will end with *dc=aten,dc=com*.
- ◆ Define the name of the administrator entry for the server (*rootdn*), along with its password (*rootpw*). This is the server's super user. The rootdn name must match the suffix defined above. (Since all entry names must end with the defined suffix, and the rootdn is an entry.)

An example configuration file is provided in the figure, below:

```
ucdata-path ./ucdata
include ./schema/core.schema

pidfile ./run/slapd.pid
argsfile ./run/slapd.args

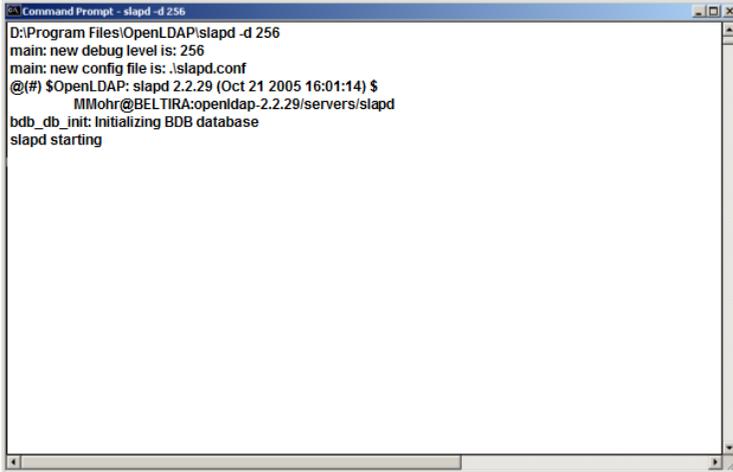
database bdb
suffix "dc=aten,dc=com"
rootdn "cn=Manager,dc=aten,dc=com"
rootpw secret
directory ./data
```

Starting the OpenLDAP Server

To start the OpenLDAP Server, run **slapd** (the OpenLDAP Server executable file) from the command line. *slapd* supports a number of command line options, the most important option is the **d** switch that triggers debug information. For example, a command of:

```
slapd -d 256
```

would start OpenLDAP with a debug level of 256, as shown in the following screenshot:



```
Command Prompt - slapd -d 256
D:\Program Files\OpenLDAP\slapd -d 256
main: new debug level is: 256
main: new config file is: .\slapd.conf
@(#) $OpenLDAP: slapd 2.2.29 (Oct 21 2005 16:01:14) $
MMohr@BELTIRA:openldap-2.2.29/servers/slapd
bdb_db_init: Initializing BDB database
slapd starting
```

Note: For details about slapd options and their meanings, refer to the OpenLDAP documentation.

Customizing the OpenLDAP Schema

The schema that slapd uses may be extended to support additional syntaxes, matching rules, attribute types, and object classes.

In the case of the SN3101, the *objectclass* and *attributeTypes* configuration file directives are used to define new schema. The extended schema file used to authenticate and authorize users logging in to the SN3101 is shown in the figure, below:

```
#####
##
##
## Copyright (C) 2005-2006 ATEN CANADA TECHNOLOGIES INC.
## All Rights Reserved.
## Author: Judy Liu
## Date: Nov.21,2006
## Summary: Define the LDAP schema used in SN3101
##
##
#####
#
# ATEN OID::={1.3.6.1.4.1.21437}
#
# 1.3.6.1.4.1.21437.1      SNMP elements
# 1.3.6.1.4.1.21437.2      LDAP elements
# 1.3.6.1.4.1.21437.2.1    AttributeTypes
# 1.3.6.1.4.1.21437.2.1.1  myAttributeTypes
# 1.3.6.1.4.1.21437.2.2    ObjectClasses
# 1.3.6.1.4.1.21437.2.2.1  myObjectClasses
#
#
#      aten      OBJECT IDENTIFIER ::= { enterprises 21437 }
#      LDAP elements OBJECT IDENTIFIER ::= { aten 2 }
#      AttributeTypes OBJECT IDENTIFIER ::= { LDAP elements 1 }
#      ObjectClasses OBJECT IDENTIFIER ::= { LDAP elements 2 }

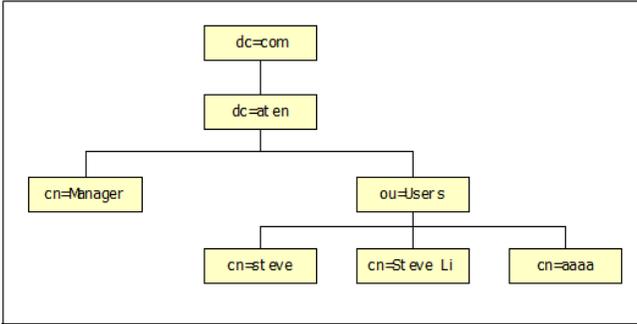
attributetype ( 1.3.6.1.4.1.21437.2.1.1
    NAME 'accessPort'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
    SINGLE-VALUE )

objectclass ( 1.3.6.1.4.1.21437.2.2.1
    NAME 'sn3101User'
    SUP organizationalPerson
    STRUCTURAL
    MAY ( accessPort $ userCertificate ) )
```

LDAP DIT Design and LDIF File

LDAP Data Structure

An LDAP Directory stores information in a tree structure known as the Directory Information Tree (DIT). The nodes in the tree are directory entries, and each entry contains information in attribute-value form. An example of the LDAP directory tree for the SN3101 is shown in the figure, below:



(Continues on next page.)

(Continued from previous page.)

DIT Creation

The LDAP Data Interchange Format (LDIF) is used to represent LDAP entries in a simple text format (please refer to RFC 2849). The figure below illustrates an LDIF file that creates the DIT for the SN3101 directory tree (shown in the figure, above).

```
#####
##
##
## Copyright (C) 2005-2006 ATEN CANADA TECHNOLOGIES INC.
## All Rights Reserved.
## Author: Judy Liu
## Date: Nov.21,2006
## Summary: Define the LDAP users for SN3101
##
##
#####

dn: dc=aten,dc=com
objectclass: top
objectClass: dcObject
objectClass: organization
o: ATEN Canada Technologies Inc.
dc:aten
description: SN3101 root DIT!!! *_*

dn: cn=Manager,dc=aten,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: Manager
sn: Manager

dn: ou=Users,dc=aten,dc=com
objectclass: top
objectclass: organizationalUnit
ou: Users

dn: cn=steve,ou=Users,dc=aten,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: sn3101User
cn: steve
sn: steve
accessPort: U,T,1
userPassword: password
```

Using the New Schema

To use the new schema, do the following:

1. Save the new schema file (e.g., sn3101.schema) in the */OpenLDAP/schema/* directory.
2. Add the new schema to the slapd.conf file, as shown in the figure, below:

```
ucdata-path    ./ucdata
include        ./schema/core.schema
include        ./schema/cosine.schema
include        ./schema/inetorgperson.schema
include        ./schema/openldap.schema
include        ./schema/sn3101.schema

# Define global ACLs to disable default read access.
access to dn.children="ou=Users,dc=aten,dc=com"
    by dn="cn=Manager,dc=aten,dc=com" write
    by self read
    by anonymous auth
    by * none

# Do not enable referrals until AFTER you have a working directory
# service AND an understanding of referrals.
#referral      ldap://root.openldap.org

pidfile        ./run/slapd.pid
argsfile       ./run/slapd.args

#####
# BDB database definitions
#####

database       bdb
suffix         "dc=aten,dc=com"
rootdn        "cn=Manager,dc=aten,dc=com"
# Cleartext passwords, especially for the rootdn, should
# be avoided. See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw        secret
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory     ./data
# Indices to maintain
index         objectClass eq
```

3. Restart the LDAP server.
4. Write the LDIF file and create the database entries in *init.ldif* with the *ldapadd* command, as shown in the following example:

```
ldapadd -f init.ldif -x -D "cn=Manager,dc=aten,dc=com"
-w secret
```

Safety Instructions

General

- ◆ Read all of these instructions. Save them for future reference.
- ◆ 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.
- ◆ The device is designed for IT power distribution systems with 230V phase-to-phase voltage.
- ◆ To prevent damage to your installation it is important that all devices are properly grounded.
- ◆ The device is equipped with a 3-wire grounding type plug. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your obsolete outlet. Do not attempt to defeat the purpose of the grounding-type plug. Always follow your local/national wiring codes.
- ◆ 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.

- ◆ If an extension cord is used with this device make sure that the total of the ampere ratings of all products used on this cord does not exceed the extension cord ampere rating. Make sure that the total of all products plugged into the wall outlet does not exceed 15 amperes.
- ◆ To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- ◆ 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.
- ◆ 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.
- ◆ Do not connect the RJ-11 connector marked “UPGRADE” to a public telecommunication network.

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 105° 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

Technical support is available both by email and online (with a browser over the web):

International

Email Support		support@aten.com
Online Support	Technical Support	http://support.aten.com
	Troubleshooting Documentation Software Updates	http://www.aten.com
Telephone Support		886-2-8692-6959

North America

Email Support		ATEN TECH	support@aten-usa.com
		ATEN NJ	sales@aten.com
Online Support	Technical Support	ATEN TECH	http://www.aten-usa.com/support
		ATEN NJ	http://support.aten.com
	Troubleshooting Documentation Software Updates	ATEN TECH	http://www.aten-usa.com
		ATEN NJ	http://www.aten.com
Telephone Support		ATEN TECH	1-888-999-ATEN
		ATEN NJ	1-732-356-1703

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.

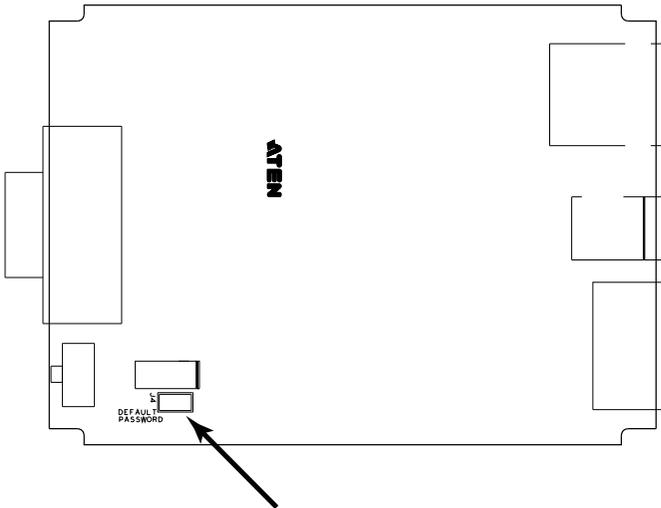
Specifications

Function		Specification	
Connectors	Serial		1 x DB-9 M (Black)
	Network		1 x RJ-45 (Black)
	Power	PWR1	1 x 2-pin Terminal Block (Green)
		PWR2	1 x DC Jack (Black)
Switches	Reset		1 x Semi-recessed Pushbutton
LEDs	Power		1 x Green
	Link		1 x Green
	10/100 Mbps		1 x Orange/Green
	TxRx (ACT)		1 x Green
Power Input	PWR1		12—48V DC (2-pin Terminal Block)
	PWR2		9—30V DC (Power Adapter Jack)
	Power Adapter		100—240V AC; 50—60 Hz
	Power Line Protection		4KV burst (EFT), EN61000-4-4 2KV surge, EN61000-4-4
Power Consumption			9V, 2.7W
Interfaces	Serial	Standards	RS-232/422/485; Software selectable
		Baud Rate	460Kbps
		RS-232 Signals	TxD, RxD, RTS, CTS, DTR, DSR, DCD, GND
		RS-422 Signals	Tx+, Tx-, Rx+, Rx-, RTS+, RTS-, CTS+, CTS-, GND
		RS-485 Signals	Data+, Data-, GND
		Serial Protection	15 KV ESD Protection for the serial port
		Parity	None, Even, Odd, Mark, Space
		Stop Bits	5, 6, 7, 8
		Flow Control	None, XON/XOFF, RTS/CTS
	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	
Regulatory Approval			FCC Class A, CE Class A, RoHS
Environment	Operating Temp.		0–60° C
	Storage Temp.		-20–85° C
	Humidity		0–95% RH
Physical Properties	Housing		Metal
	Weight		0.22 kg
	Dimensions (L x W x H)		10.69 x 7.90 x 2.44 cm

Administrator Login Failure

If you are unable to perform an Administrator login (because the Username and Password information has become corrupted, or you have forgotten it, for example), you can clear the login information with the following procedure:

1. Power off the SN3101 and remove its housing.
2. Use a jumper cap to short the jumper labeled J4 (*DEFAULT PASSWORD*).



3. Power on the switch.
4. When the Link and 10/100Mbps LEDs flash, power off the switch.
5. Remove the jumper cap from J4.
6. Close the housing and start the SN3101 back up.
After you start back up, you can use the default Username and Password (see *Logging In*, page 11) to log in.

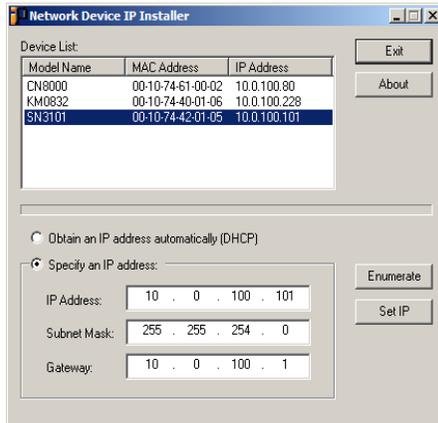
IP Address Determination

If you are an administrator logging in for the first time, you need to access the SN3101 in order to give it an IP address that users can connect to. There are two methods to choose from. In either case, your computer must be on the same network segment as the SN3101. After you have connected and logged in you can give the SN3101 its fixed network address. See *Network*, page 16 for details.

Method 1:

For computers running Windows, an IP address can be assigned with the IP Installer utility:

1. Unzip the contents of IPInstaller.zip (found on the Software CD that came with your SN3101 package) to a directory on your hard drive.
2. Go to the directory that you unzipped the IPInstaller program to and run *IPInstaller.exe*. A dialog box similar to the one below appears



3. Select the SN3101 in the *Device List*.

Note: 1. If the list is empty, or your device doesn't appear, click **Enumerate** to refresh the Device List.

2. If there is more than one device in the list, use the MAC address to pick the one you want. The SN3101's MAC address is located on its bottom panel.
-

4. Select either *Obtain an IP address automatically (DHCP)*, or *Specify an IP address*. If you chose the latter, fill the IP Address, Subnet Mask, and Gateway fields with the information appropriate to your network.
5. Click **Set IP**.
6. After the IP address shows up in the Device List, click **Exit** to end the program.

Method 2:

1. Set your computer's IP address to 192.168.0.XXX
Where XXX represents any number or numbers except 10. (192.168.0.10 is the default address of the SN3101.)
2. Specify the switch's default IP address (192.168.0.10) in your browser, and you will be able to connect.
3. Assign a fixed IP address for the SN3101 that is suitable for the network segment that it resides on.
4. After you log out, be sure to reset your computer's IP address to its original value.

Serial Port Pin Assignments

The serial port pin assignments are given in the table, below:

Pin	Configuration		
	RS-232	RS-422	RS-485
1	DCD	RX-	
2	/RXD	RX+	
3	/TXD	TX+	D+
4	DTR	TX-	D-
5	GND	GND	GND
6	DSR	CTS-	
7	RTS	CTS+	
8	CTS	RTS+	
9		RTS-	

Virtual Modem Details

The SN3101's *Virtual Modem* function emulates a hardware modem to provide high speed serial modem functionality over an Ethernet LAN or WAN using the TCP/IP protocol rather than over slower, less-reliable, telephone lines.

AT Command Set Support

The SN3101 supports a subset of the standard Hayes command set, as well as some extended commands, as shown in the following table:

Command	Operation	Response
+++	Return to command mode. The escape character can be changed by modifying the S2 register.	none
A/	Repeat the last command string	If successful: OK[CR][LF] If failure: ERROR[CR][LF]
ATA[CR]	Answer mode. Allow virtual modem to listen for a TCP connection on the provided listen port: 5301.	If successful: OK[CR][LF] If failure: ERROR[CR][LF]
ATD(T) Remote IP:Remote Port[CR]	Try to establish a TCP connection and connect to the specified remote host. e.g. ATDT10.0.0.72:50001 Note: The SN3101 accepts T and P additions to the ATD command, but ignores them.	If successful: CONNECT[CR][LF] If connection failure: NO CARRIER[CR][CF] If other error: ERROR[CR][LF]
ATE <i>n</i> [CR]	Where <i>n</i> represents a numeric character (0 or 1): E0: disable command echo E1: enable command echo	If successful: OK[CR][LF] If failure: ERROR[CR][LF]
ATH[CR]	Hang up current TCP connection if a connection is active. Note: ATH, ATH0, and ATH1 all act the same.	If successful: OK[CR][LF] If failure: ERROR[CR][LF]
ATI <i>n</i> [CR]	Inquiry command. (Where <i>n</i> represents a numeric character; 0 or 1.): E0: Display <i>ATEN International Co. Ltd.</i> E1: Display <i>SN3101</i>	If successful: OK[CR][LF] If failure: ERROR[CR][LF]
ATO <i>n</i> [CR]	Return to on-line data mode. (Where <i>n</i> represents a numeric character; 0 or 1.) If the modem is in the on-line command mode, the modem enters on-line data mode. If the modem is in the off-line command mode (no TCP connection established), an ERROR is returned. O0, O1: If there is an active connection, switch the modem to data mode.	If an active TCP connection: OK[CR][LF] Otherwise: ERROR[CR][LF]
ATQ <i>n</i> [CR]	Result code control command. (Where <i>n</i> represents a numeric character; 0 or 1.) Q0: Enable result code to DTE (default) Q1: Disable result code to DTE.	If successful: OK[CR][LF] If failure: ERROR[CR][LF]
ATS <i>n</i> ?[CR]	Reports the value of the <i>S</i> register. (Where <i>n</i> is the register's number.)	If successful: OK[CR][LF] If failure: ERROR[CR][LF]
ATS <i>n</i> = <i>v</i> [CR]	Sets the <i>S</i> register's value. (Where <i>n</i> is the register's number; and <i>v</i> is the <i>S</i> register value. See <i>S Register Support</i> , page 106.)	If successful: OK[CR][LF] If failure: ERROR[CR][LF]
ATV <i>n</i> [CR]	Result code return type. (Where <i>n</i> represents a numeric character; 0 or 1.) V0: Response is: <numeric code>[CR][LF] V1: Response is: <verbal description>[CR][LF]	If successful: OK[CR][LF] If failure: ERROR[CR][LF]

(Continued from previous page.)

Command	Operation	Response
ATZ[CR]	Reset modem command. Close active connections and reset the S registers and general option status to their saved values.	If successful: OK[CR][LF] If failure: ERROR[CR][LF]
AT&Cn[CR]	DCD option. (Where n represents a numeric character; 0 or 1.) &C0: DCD is ON at all times. &C1: DCD matches the state of the TCP connection.	If successful: OK[CR][LF] If failure: ERROR[CR][LF]
AT&Dn[CR]	DTR option. (Where n represents a numeric character; 0 – 3.) &D0: DTR is assumed to be ON. Modem ignores the DTR line. &D1: DTR OFF causes the modem to switch to command mode without disconnecting. &D2: DTR OFF switches modem to command mode; hangs up; and disables auto answer. (Default) &D3 DTR OFF initializes the modem.	If successful: OK[CR][LF] If failure: ERROR[CR][LF]
AT&F[CR]	Restore factory configuration. Reset S registers and general option status to default values.	If successful: OK[CR][LF] If failure: ERROR[CR][LF]
AT&W[CR]	Save configuration. Write the current configuration settings into memory, including the S register values and general option status.	If successful: OK[CR][LF] If failure: ERROR[CR][LF]
ATB[CR]	None	OK[CR][LF]
ATC[CR]	None	OK[CR][LF]
ATL[CR]	None	OK[CR][LF]
ATM[CR]	None	OK[CR][LF]
ATN[CR]	None	OK[CR][LF]
ATX[CR]	None	OK[CR][LF]
ATY[CR]	None	OK[CR][LF]
ATW[CR]	None	OK[CR][LF]
Other AT Commands	None	OK[CR][LF]

S Register Support

The S registers that the SN3101 supports, and their values, are described in the table, below:

Register	Function	Range	Units	Default
S0	Number of rings to wait before auto answering.	0—255	Rings	0
S1	Ring Counter Specify the current number of rings. S1 is incremented each time the modem detects a ring signal on the telephone line. S1 is cleared when the existing connection is established, or when it is dropped.	0—255	Rings	0
S2	Escape Character If this value is greater than 127, the escape process is disabled.	0—127	ASCII	43
S3	Carriage Return Character Sets the value of the carriage return character used when displaying commands or results.	0—127	ASCII	13
S4	Line Feed Character Sets the character recognized as the line feed when displaying commands or results. If verbose result code format is in use, the line feed character is output after the carriage return character.	0—127	ASCII	10
S5	Backspace Character Sets the character recognized as a backspace. Used to erase the last character typed on the command line.	0—32	ASCII	8
S12	Escape Prompt Delay The amount of time required before and after an escape sequence (+++) is entered in order for the modem to transition from data mode to command mode.	0—255	0.02ms	50 (1 sec.)
S25	DTR Delay and Asynchronous/Synchronous Time Delay The amount of time that the modem will delay before taking the action specified by the <i>AT&Dn</i> command.	0—255	0.01s for DTR 1s for asynchronous mode	5

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*, page 24, for upgrade details.

Limited Warranty

ALTUSEN warrants this product against defects in material or workmanship for a period of one (1) year from the date of purchase. If this product proves to be defective, contact ALTUSEN's support department for repair or replacement of your unit. ALTUSEN will not issue a refund. Return requests can not be processed without the original proof of purchase.

When returning the product, you must ship the product in its original packaging or packaging that gives an equal degree of protection. Include your proof of purchase in the packaging and the RMA number clearly marked on the outside of the package.

This warranty becomes invalid if the factory-supplied serial number has been removed or altered on the product.

This warranty does not cover cosmetic damage or damage due to acts of God, accident, misuse, abuse, negligence or modification of any part of the product. This warranty does not cover damage due to improper operation or maintenance, connection to improper equipment, or attempted repair by anyone other than ALTUSEN. This warranty does not cover products sold AS IS or WITH FAULTS.

IN NO EVENT SHALL ALTUSEN'S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT. FURTHER, ALTUSEN SHALL NOT BE RESPONSIBLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION. ALTUSEN SHALL NOT IN ANY WAY BE RESPONSIBLE FOR, WITHOUT LIMITATION, LOSS OF DATA, LOSS OF PROFITS, DOWNTIME, GOODWILL, DAMAGE OR REPLACEMENT OF EQUIPMENT OR PROPERTY, AND ANY EXPENSES FROM RECOVERY, PROGRAMMING, AND REPRODUCTION OF ANY PROGRAM OR DATA.

ALTUSEN makes no warranty or representation, expressed, implied, or statutory with respect to its products, contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose.

ALTUSEN reserves the right to revise or update its product, software or documentation without obligation to notify any individual or entity of such revisions, or update.

For details about extended warranties, please contact one of our dedicated value added resellers.

This Page Intentionally Left Blank

Index

A

- Active Directory
 - LDAP configuration, 77
- Administration, 13
 - ANMS settings, 19
 - Date and time, 23
 - Firmware upgrade, 24
 - General settings, 13
 - Network settings, 16
- Administrator Login Failure, 101
- Administrator password, 14
- Advanced settings
 - Modbus, 42
 - Port alert, 38
 - TCP Client, 40
 - UDP Mode, 41
- ANMS
 - Radius Settings, 20
 - SNMP Settings, 22
- ANMS settings, 19
- AT Command Set Support, 104

B

- Browser
 - Main screen, 12
- Browser log in, 11
- Browser operation
 - Overview, 29
 - Telnet, 31

C

- Connection Control, 14
- Corrupt Password, 101

D

- Date and time, 23

- DIN Rail Mounting, 8
- Direct Access, 46

F

- Firmware upgrade, 24
- Forgotten Password, 101

G

- General settings, 13

I

- Installation, 9
 - PC, 9
- IP Address, 18
- IP address determination, 102

L

- LDAP
 - Active Directory configuration, 77
 - Permission attributes, 86
 - Permission examples, 87
- Log, 49
- Logging in
 - browser, 11

M

- Modbus Mode
 - settings, 42
- Mounting, 7
 - DIN Rail, 8
 - Wall, 7

N

- Network
 - IP Address, 18
 - Service Ports, 16
- Network settings, 16

O

Online

Registration, iii

OpenLDAP

Server Configuration, 89

Server Installation, 88

Operating Mode, 37

Overview, 1

P

Port alert

settings, 38

Port configuration, 35

Advanced settings, 38

Property settings, 36

serial settings, 36

Port Mapping, 64

Port Unmapping, 66

Property settings, 36

PuTTY, 55

R

Rack Mounting

Safety information, 97

Radius Settings, 20

RAW TCP, 26

Real COM Port, 25

Real COM Port Driver Installation

Windows, 57

Real COM Port Management, 57

Linux, 67

Windows, 60

Real COM Port. See Virtual COM Port

RoHS, ii

S

S Register Support, 106

Safety Instructions

DC Power, 97

General, 95

Rack Mounting, 98

Serial Network Device Manager, 69

Serial port settings, 36

Serial Tunnel, 28, 71

Building, 74

Removing, 75

Service Ports, 16

Session Info, 47

SJ/T 11364-2006, ii

SN3101

Front view, 4

Rear View, 5

SNMP Settings, 22

Specifications, 100

SSH

terminal (Linux) session, 54

third party utility (Windows), 55

System Information, 48

T

TCP

Client Mode, 26

Server Mode, 26

TCP Client

settings, 40

Technical Support, 99

Telephone support, iii

Telnet, 31, 53

TTY, 59

U

UDP Mode

settings, 41

User Management, 44

User Notice, iii

V

Virtual COM Port, 25

Virtual COM Port Driver Installation

- Windows, 57
- Virtual Modem, 28, 104
- Virtual Port Management, 57
 - Dialog box layout, 60, 70
 - Port Mapping and Unmapping, 64
- Windows, 60
- Virtual Port Utility
 - Menu and toolbar, 61

- Port List, 63
- Port Mapping, 64
- Port Unmapping, 66
- Target information, 61
- Target list, 62

W

- Wall Mounting, 7