Simply Better Connections

Serial Console Servers
User Manual

Compliance Statements

FEDERAL COMMUNICATIONS COMMISSION INTERFERENCE STATEMENT

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

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

FCC Caution

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

Warning

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

Achtung

Der Gebrauch dieses Geräts in Wohnumgebung kann Funkstörungen verursachen.



KCC Statement

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

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

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

VCCI Statement

The SN0132CO, SN9108CO, and SN9116CO are VCCI compliant.

この装置は、クラスA機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

RoHS
This product is RoHS compliant.

User Information

Online Registration

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

International	http://eservice.aten.com

Telephone Support

For telephone support, call this number:

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

User Notice

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

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

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

Battery Safety Notice



◆There is a risk of explosion if the battery is replaced with an incorrect type. Dispose of used batteries according to the relevant instructions.

Batterie avis de sécurité



◆Il existe un risque d'explosion si la batterie est remplacée par un incorrect tapez. Jeter les piles usagées selon la pertinente instructions.

Product Information

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

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

Package Contents

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

SN1116CO / SN1132CO / SN1148CO

1 SN1116CO / SN1132CO / SN1148CO Serial Console Server

1 laptop USB console (LUC) cable

2 power cords

1 foot pad set (4 pcs)

1 rack mounting kit

1 user instructions

SN1116COD / SN1132COD / SN1148COD

1 SN1116COD / SN1132COD / SN1148COD Serial Console Server

1 laptop USB console (LUC) cable

1 foot pad set (4 pcs)

1 rack mounting kit

1 user instructions

SN0108CO / SN0116CO

1 SN0108CO / SN0116CO Serial Console Servers

2 Lok-U-Plugs

1 Lok-U-Plug Installation Tool

1 laptop USB console (LUC) cable

2 power cords

1 mounting kit

1 foot pad set (4 pcs)

1 user instructions

SN0108COD / SN0116COD

1 SN0108COD / SN0116COD Serial Console Server

1 laptop USB console (LUC) cable

1 mounting kit

1 foot pad set (4 pcs)

1 user instructions

SN0132CO / SN0148CO

1 SN0132CO / SN0148CO Serial Console Servers

1 laptop USB console (LUC) cable

2 power cords

1 mounting kit

1 foot pad set (4 pcs)

1 user instructions

SN0132COD / SN0148COD

1 SN0132COD / SN0148COD Serial Console Servers

1 laptop USB console (LUC) cable

1 mounting kit

1 foot pad set (4 pcs)

1 user instructions

SN9108CO / SN9116CO

1 SN9108CO / SN9116CO Serial Console Servers

1 Lok-U-Plug

1 Lok-U-Plug Installation Tool

1 power cord

1 mounting kit

1 foot pad set (4 pcs)

1 user instructions

Contents

Compliance Statements ii
User Information iv
Online Registration iv
Telephone Support iv
User Notice iv
Battery Safety Notice v
Batterie avis de sécurité v
Product Information vi
Package Contents vii
SN1116CO / SN1132CO / SN1148CO vii
SN1116COD / SN1132COD / SN1148COD vii
SN0108CO / SN0116CO vii
SN0108COD / SN0116COD vii
SN0132CO / SN0148CO viii
SN0132COD / SN0148COD viii
SN9108CO / SN9116CO viii
Contents ix
About This Manual xvii
Overview xvii
Conventions xix
Terminology xix

Chapter 1. **Introduction**

Overview 1
Features 3
System Accessibility and Availability 3
Serial Console Management 3
Security 4
System Management 4
Serial Device Management 5
Language 5
Requirements 6
DTE/DCE Auto-Sensing 7
Browsers 8
Components 9
SN1116CO / SN1116COD Front View 9
SN1132CO / SN1132COD Front View 9
SN1148CO / SN1148COD Front View 9
SN1116CO Rear View 10
SN1116COD Rear View (DC Power) 10
SN1132CO Rear View 10
SN1132COD Rear View (DC Power) 11
SN1148CO Rear View 11
SN1148COD Rear View (DC Power) 11

SN0108CO / SN0108COD Front View 14
SN0116CO / SN0116COD Front View 14
SN0132CO / SN0132COD Front View 17
SN0148CO / SN0148COD Front View 17
SN9108CO Front View 20
SN9116CO Front View 20
SN0108CO Rear View 22
SN0116CO Rear View 22
SN0108COD Rear View (DC Power) 23
SN0116COD Rear View (DC Power) 23
SN0132CO Rear View 24
SN0148CO Rear View 24
SN0132COD Rear View (DC Power) 25
SN0148COD Rear View (DC Power) 25
SN9108CO Rear View 26
SN9116CO Rear View 26

Chapter 2. **Hardware Setup**

Before You Begin 27
Stacking and Rack Mounting 27
Stacking 27
Rack Mounting 29
Rack Mounting - Front 29
Rack Mounting - Rear 31
Serial Console Server Installation 33
SN1116CO / SN1132CO / SN1148CO Installation 33
SN0108CO / SN0116CO / SN0132CO / SN0148CO Installation 35
SN9108CO / SN9116CO Installation 39
Installing Network Switch with USB Console via USB Cable 41
LLDP 42

Chapter 3. **Super Administrator Setup**

Overview 43
First-Time Setup 43
Local Login 43
Laptop USB Console (LUC) Login - SNViewerUSB 44
Console Login - HyperTerminal 44
Local Console Main Menu 45
Remote Login 46
Telnet Login 46
PuTTY Login 46
Browser Login 47
Looking Up the Login IP Address via IP Installer 48
Setup 49
Network Setup 49
Changing the Super Administrator's Login Credentials 50

Chapter 4. The User Interface

Overview . . . 52
Access . . . 52
Local Console Operation . . . 53
Remote Operation . . . 54
Web Browser Login . . . 54
The Web Browser Main Page . . . 55
Page Components . . . 56
The Tab Bar . . . 57
SNViewer . . . 58
SNViewer Control Panel . . . 58
Control Panel Functions . . . 59
Data Import . . . 60
Encode . . . 61
The Message Board . . . 61
Message Display Panel . . . 61
Compose Panel . . . 62
User List Panel . . . 62
Macros . . . 62
Terminal Application . . . 62
Terminal Settings . . . 63
Terminal Application . . . 65
Telnet Menu-Driven Text UI . . . 65
WebClient . . . 68
WebClient More Functions . . . 70

Chapter 5. Port Operating Modes

Overview . . . 71
Operating Mode . . . 72
Console Management . . . 72
Real COM Port . . . 72
TCP Server / TCP Client (Serial Tunnel) . . . 72
TCP Server (RAW TCP) . . . 72
TCP Client . . . 73
UDP Mode . . . 73
Virtual Modem . . . 73
Console Management Direct . . . 74
Disabled . . . 74

Chapter 6. Port Access

Overview . . . 75
The Sidebar . . . 76
The Sidebar Tree Structure . . . 76
Filter . . . 77
Connections . . . 78
Telnet/SSH/WebClient . . . 79

Port Attributes 81
Favorites 82
History 83
Preferences 84
SSH Passwordless Login 86
Setting Up SSH Passwordless Login. 86
Accessing the Serial Console Server's Management Console . . . 89
Sessions 91
Access 92
Properties 94
Save & Copy 96
Port Buffering 96
Operating Mode 98
Console Management 98
Real COM Port 102
TCP Server 102
TCP Client 103
UDP Mode 104
Virtual Modem 104
Console Management Direct 105
Disabled. 106

Chapter 7. User Management

Overview 107
Users 108
Adding Users 109
Modifying User Accounts 112
Deleting User Accounts. 113
Groups 114
Creating Groups 114
Modifying Groups 116
Deleting Groups 116
Users and Groups 117
Assigning Users to a Group From the User's Notebook 117
Removing Users From a Group From the User's Notebook 119
Assigning Users to a Group From the Group's Notebook 120
Removing Users From a Group From the Group's Notebook 121
Device Assignment 122
Assigning Device Permissions under User Settings 122
Assigning Device Permissions under Group Settings 124

Chapter 8. Device Management

Overview 125
Device Information 126
General 126
Mounted Devices. 127
NFS Settings 128

External USB Drives 128
Sensors Settings (SN1100CO / SN1100COD Only) 128
Syslog Settings for Port Logs 129
Port Name Auto Discovery 129
Port Name Settings 130
Network 131
IP Installer 131
Service Ports 131
Network Configuration 132
Enabling 802.1x Security 135
Mobile/WiFi Network Configuration 139
ANMS 143
Event Destination 143
SMTP Settings 143
Log Server 144
SNMP Setup 145
Syslog Server 147
SMS Settings 147
Authentication and Authorization 148
Global Settings 148
RADIUS Settings 149
LDAP / AD Settings 150
TACACS+ Settings 151
Kerberos 152
CC Management Settings 152
OOBC 153
Console Port Settings 154
Enable Dial Back 157
Enable Dial Out 157
Security 160
Login Failures 160
Security Level 161
Misc. 162
IP/MAC Filter 162
Account Policy 164
Association 165
Date/Time 166
Current System Time 166
New System Time 167
Time Zone 167

Chapter 9. **Log**

Overview 168
System Log 168
Filter 169
Log Notification Settings 171

SN1100CO / SN1100COD 171
SN0100CO / SN0100COD / SN9100CO 171

Chapter 10. **Maintenance**

Overview 173
Backup / Restore 173
Backup 174
Restore 174
Restoring an Encrypted Backup 174
Modifying and Restoring an Unencrypted Backup 175
Firmware Upgrade 177
Certificates 178
Private Certificate 178
Certificate Signing Request 179

Chapter 11. **MIB Reference**

Overview 181
MIB Tree Structure 181
Downloading MIB Files 182
OID Format 182
Object Types and Indexing 183
SN01xx and SN91xx Series 185
RS-232 Objects 185
General 185
RS-232 Port Configuration 185
Async Port 189
RS-232 Input Signals 190
RS-232 Output Signals 191
RS-232 Operating Info 192
Session Management Objects 194
Firmware Management Object 196
Device Management Objects 196
Date/Time 198
ANMS Objects 199
SNMP 199
SMTP 200
Log Server 201
Syslog Server 202
CC Management 203
External USB 204
Security Objects 205
Manufacturer Information Object 206
Network Objects 206
Service Ports 206
LAN Port: ETH0 208
LAN Port: ETH1 210
General 213

SN11xx Series 214
RS-232 Objects 214
General 214
RS-232 Port Configuration 214
Async Port 218
RS-232 Input Signals 219
RS-232 Output Signals 220
RS-232 Operating Info 221
Session Management Objects 223
Firmware Management Object 225
Device Management Objects 226
Date/Time 227
Sensor Objects 228
Sensor 1 228
Sensor 2 229
Other Sensors 230
ANMS Objects 231
SNMP 231
SMTP 232
Log Server 233
Syslog Server 234
CC Management 235
External USB 236
Security Objects 237
Manufacturer Information Object 238
Network Objects 239
Service Ports 239
LAN Port: ETH0 240
LAN Port: ETH1 243
General 245

Appendix

Safety Instructions 247
General 247
DC Power 249
Rack Mount 250
Technical Support 251
International 251
North America 251
Specifications 252
SN1116CO / SN1132CO / SN1148CO 252
SN1116COD / SN1132COD / SN1148COD 254
SN0108CO / SN0116CO (AXA Platform) 255
SN0108CO / SN0116CO (AX Platform) 256
SN0108COD / SN0116COD (AXA Platform) 257
SN0108COD / SN0116COD (AX Platform) 258

SN0132CO / SN0148CO (AXA Platform) 259
SN0132CO / SN0148CO (AX Platform) 260
SN0132COD / SN0148COD (AXA Platform) 261
SN0132COD / SN0148COD (AX Platform) 262
SN9108CO / SN9116CO (AXA Platform) 263
SN9108CO / SN9116CO (AX Platform) 264
IP Address Determination 265
The Local Console 265
IP Installer 265
Browser 266
IPv6 267
Link Local IPv6 Address 267
IPv6 Stateless Autoconfiguration 268
Virtual Modem Details 269
AT Command Set Support 269
Port Forwarding 271
Distance vs Baud Rate 271
Clear Login Information 272
Pin Assignment 273
DCE Mode Pin Assignment 273
DTE Mode Pin Assignment 273
DB-9/DB-25 Interface 274
DB-9. 274
DB-25. 274
Self-signing SSL/TLS Certificate. 275
CLI Command Set 276
System Setting Commands. 276
Network Setting Commands 283
User Management Commands 285
Serial Port Setting Commands 290
Backup/Restore Config Commands 292
Firmware Upgrade Commands 296
IP Filter Commands 297
Account Policy Commands 299
ATEN Warranty Policy 301

About This Manual

This User Manual is provided to help you get the most from your Serial Console Server. It covers all aspects of the device, including installation, configuration, and operation

The Serial Console Server models covered in this user manual include:.

Model	Product Name
SN1116CO/ SN1116COD	16-Port Serial Console Server with Dual Power / SFP (AC / DC model)
SN1132CO/ SN1132COD	32-Port Serial Console Server with Dual Power / SFP (AC / DC model)
SN1148CO/ SN1148COD	48-Port Serial Console Server with Dual Power / SFP (AC / DC model)
SN0108CO / SN0108COD	8-Port Serial Console Server with Dual Power/LAN (AC / DC model)
SN0116CO / SN0116COD	16-Port Serial Console Server with Dual Power/LAN (AC / DC model)
SN0132CO / SN0132COD	32-Port Serial Console Server with Dual Power/LAN (AC / DC model)
SN0148CO / SN0148COD	48-Port Serial Console Server with Dual Power/LAN (AC / DC model)
SN9108CO	8-Port Serial Console Server (AC model)
SN9116CO	16-Port Serial Console Server (AC model)

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

Overview

Chapter 1, *Introduction***,** introduces you to the Serial Console Server, its purpose, features, and benefits, with its front and back panel components described.

Chapter 2, *Hardware Setup***,** provides step-by-step instructions for setting up the Serial Console Server.

Chapter 3, *Super Administrator Setup***,** explains the procedures that the super administrator employs to set up the Serial Console Servers network environment, and changing its default username and password.

Chapter 4, *The User Interface***,** describes the layout and components of the Serial Console Server user interface, and how to log in to the Serial Console

Server with each of the available access methods: from a local console, an Internet browser, and Windows application (AP) programs.

Chapter 5, *Port Operating Modes***,** describes the port operating modes, including Console Management and Console Management Direct modes for device control; Real COM Port, Virtual Modem, TCP Server, TCP Client, and UDP Mode for Serial-to-Ethernet connectivity and applications that require COM ports, serial tunneling, or where TCP/UDP Socket functionality is needed.

Chapter 6, *Port Access***,** describes the Port Access page and how to configure the options it provides regarding port and power outlet management.

Chapter 7, *User Management***,** shows super administrators and administrators how to create, modify, and delete users and groups, as well as assign attributes to them.

Chapter 8, *Device Management***,** shows super administrators how to configure and control the overall Serial Console Server operations.

Chapter 9, *Log***,** explains how to install and configure the Log Server.

Chapter 10, *Maintenance***,** explains how to backup, restore, and upgrade the Serial Console Server and its firmware, as well as provides information about private certificates.

Chapter 11, *MIB Reference*, provides detailed information on MIB objects, required for integration with network management systems, automated monitoring, and event handling.

Appendix, provides technical and troubleshooting information.

Note:

- Read this manual thoroughly and follow the installation and operation procedures carefully to prevent any damage to the unit or connected devices.
- ATEN regularly updates its product documentation for new features and fixes. For an up-to-date Serial Console Servers documentation, visit

  http://www.aten.com/global/en/

Conventions

This manual uses the following conventions:

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

Terminology

Throughout the manual we make reference to the terms *Local* and *Remote* in regard to the operators and equipment deployed in a Serial Console Server installation. Depending on the point of view, users and servers can be considered *Local* under some circumstances, and *Remote* under others:

- Serial Console Servers's Point of View
  - Remote users – We refer to a user as a *Remote* user when we think of him as someone who logs into the Serial Console Servers over the net from a location that is *remote from the* Serial Console Servers.
  - Local Console – a computer connected directly to the Serial Console Servers by a physical connection.
  - Servers, Serial Device, or Port Device – any device attached to the Serial Console Servers's ports via cable.
- User's Point of View
  - Local client users – We refer to a user as a *Local user* when we think of him as sitting at his computer performing operations on the devices connected to the Serial Console Servers that is *remote from him*.

When we describe the overall system architecture we are usually speaking from the Serial Console Servers's point of view – in which case the users are considered remote. When we speak about operations users perform via the

browser, viewers, and AP programs over the net, we are usually speaking from the user's point of view – in which case the Serial Console Servers and the devices connected to it are considered remote.

Chapter 1
Introduction

Overview

ATEN SN1100CO Series (SN1116CO / SN1132CO / SN1148CO), SN0100CO Series (SN0108CO / SN0116CO / SN0132CO / SN0148CO), and SN9100CO Series (SN9108CO / SN9116CO) serial console server provides IT and network administrators secure, out-of-band access to serial devices located at data centers or remote sites (such as network switches allowing console operation using RS-232 and USB console[1]). With dual power / SFP[2] in the SN1100CO models, dual power / LAN in SN0100CO models, and single power / LAN in the SN9100CO models, all of them integrate cutting edge technologies to provide convenient installation, secure serial device access, easy management and comprehensive control for data centers.

All series of serial console server features Cisco pin-outs and auto-sensing DTE / DCE function, providing a direct connection to Cisco network switches (and other compatible devices) without rollover cables for more time-saving IT infrastructure deployment. In addition, it support online detection of connected serial devices (including terminal blocks) for device status monitoring. An e-mail notification will be sent to the administrator when connected devices are offline. With dual Ethernet ports and power supplies (AC), the SN1100CO / SN0100CO supports power redundancy as well as failover, or dual IP addresses access, ensuring 24 / 7 availability of access to serial devices. A DC power option is also available for each of the SN1100CO / SN0100CO model for more flexible implementation[3].

The SN1100CO Series supports environmental monitoring through its sensor ports, remaining vigilant around the clock to detect any abnormal conditions. It offers audited and controlled door access using a cabinet lock through its relay port, enhancing security measures. All of the serial console servers can be utilized through ATEN's CC2000 software to provide centralized serial device access and integrated power management.

Available in 8-, 16-, 32- and 48-port models, the SN1100CO / SN0100CO serial console servers offer both in-band and out-of-band (OOB) remote serial console and USB console access to servers and network devices via a direct Telnet / SSH client, Java viewer and WebClient. The OOB management enables IT administrators to manage network devices (e.g. router, switch, UPS) in server rooms using management networks that are separated from the main

/ production networks. Where access difficulty occurs in the production network, the administrators can still access them via the console server. The serial console servers offer out-of-band access methods such as direct console connection from a local computer, USB console connection from a laptop, PSTN connection via modem, or hybrid network connection via the dual SFP or dual LAN ports (one connected to the production network and the other connected to the management network).

Implemented with various security technologies such as TLS 1.2 data encryption, RSA 2048-bit certificates, configurable user permissions for port access and control, local / remote / third-party authentication and authorization, IP / MAC address filter, and FIPS 140-2 certified cryptography, the SN1100CO / SN0100CO / SN9100CO serial console servers assure administrators the security for easy and high-level access. For instance, access rights and privileges can be applied to 8 / 16 / 32 / 48 serial ports individually. Data encryption is provided to ensure that information and control are always protected. Logging and alerting of system events help to quickly resolve issues and mitigate risks. While secured by the above examples, the consolidated password authentication simplifies management.

The serial console servers are used to connect serial devices to an Ethernet network to allow access and control of demanding applications that manage industrial control, data acquisition, environment monitoring, remote facility operations and equipment management. Multiple operational modes are available to administrators including Console Management, Console Management Direct, Real COM Port, TCP Server / Client, UDP Server / Client, and Virtual Modem. With their comprehensive features, the SN1100CO, SN0100CO, and SN9100CO Series help to maximize IT productivity, increase scalability, as well as reduce installation and operational costs with easy and secure remote management of serial devices. The serial console servers save you time and money by allowing administrators to manage their data centers from practically anywhere – minimizing travel and MTTR (Mean Time to Repair) costs, and ensuring the highest availability for data center services.

Note:

- Compatible models: Cisco Catalyst 2960-C series.Fiber (2A-136G, 2A-137G) or copper (2A-143G) modules are sold separately. Please order with SN devices together.
- DC power models include SN1116COD, SN1132COD, SN1148COD, SN0108COD, SN0116COD, SN0132COD, and SN0148COD. They are available at the customer’s request.

Features

System Accessibility and Availability

- Secure in-band, out-of-band remote serial console and USB console[1] access
- Browser access with an intuitive GUI
- Terminal-based access with a menu-driven UI or command-line interface
- Modem dial-in / dial-back / dial-out access
- Front USB ports for storage, USB console[1], and UC232B / UC232BF connection[2]
- Laptop USB Console (LUC) port for local console access via laptop[2]
- Dual Ethernet ports allow fail control or dual IP address access[3]
- Dual power supply[2]

Serial Console Management

- Support sensor ports for environmental monitoring[4]
- Relay port supports cabinet door access control
- Auto-sensing DTE / DCE feature supports a direct connection to Cisco network switches (and other compatible devices) without rollover cables for more convenient IT infrastructure deployment
- Online / Offline detection of connected serial devices (including terminal blocks) – automatically send event notifications when the devices are offline (e.g. power failure) for device status monitoring
- Response Check – checks the system status of the connected serial devices and sends a notification if the check fails (e.g. system crash)
- Convenient and simple serial device access via selectable Telnet / SSH and third-party clients such as PuTTY
- Easy port access via selectable ActiveX, Java serial viewer or WebClient
- Comprehensive viewer functions – copy / paste, logging, data import, macros, broadcasting and message board
- Sun Solaris ready – Sun “break-safe”
- Alert Strings – whenever one of the pre-defined strings matches the message sent from the serial devices, you will be informed by serial console server via SNMP Trap alert and/or an email

- Command filter – administrators can restrict users to execute only pre-defined commands
- Multiple users can simultaneously access the same port – up to 16 connections per port
- Modes for simultaneous access – Exclusive / Occupy / Share mode

Security

- Supports secure login from browsers with TLS 1.2 data encryption and RSA 2048-bit certificates
- Configurable user permissions for port access and control
- Local and remote authentication and login
- Third-party authentication via RADIUS, TACACS+, LDAP/AD and Kerberos
- IP and MAC address filter for enhanced security protection
- High security grade – supports FIPS 140-2 level 1 security standards that use an embedded FIPS 140-2 certified OpenSSL cryptographic module (Certificate #1747, #2398, #2473)
- Supports security level configuration – High, Medium-high, Medium or Custom, to ensure a fine granularity of network access control
- Supports IEEE 802.1X authentication

System Management

- System configuration via web browser, Telnet / SSH client and local console
- System log and event login
- Event Destination – Event logs will be saved to Log server, Syslog server, and USB drive[2] (supports file system FAT8, FAT16 and FAT32)
- SNMP agent v1 / v2 / v3
- Event notification – supports notification of SMTP email and SNMP Trap
- Backup / Restore system configuration and upgradeable firmware
- Multi-browser support – Internet Explorer, Chrome, Firefox
- NTP for time server synchronization
- IPv4 / IPv6 support
- LLDP support[5]
- CLI (command-line interface) support

- Integrates into CC2000 software for centralized data center management
- Integrates into CCVSR software for user session recording

Serial Device Management

- Serial operating modes – Console Management, Console Management Direct, Real Com Port, TCP Server / Client, UDP Server / Client, and Virtual Modem
- Real COM driver for Windows 2000 or higher and Windows Server 2003 / 2008
- Real TTY driver for Linux
- Fixed TTY driver for UNIX[6]
- Supports baud rates of 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 28800, 38400, 57600, 115200, 230400 bps

Language

- Multi-language web-based GUI – available in English, German, Japanese, Korean, Russian, Simplified Chinese and Traditional Chinese

Note:

1. Compatible models: Cisco Catalyst 2960-C series.
2. SN1100CO / SN1100COD / SN0100CO / SN0100COD only.
3. Fiber (2A-136G, 2A-137G) or copper (2A-143G) modules are sold separately. Please order with SN devices together.
4. This is achieved using ATEN sensors.
5. For more information, see *LLDP*, page 42.
6. Fixed TTY Driver support:
   - OpenServer (Sco Unix)
   - UnixWare 7, SVR 5
   - UnixWare 2.1, SVR 4.2
   - QNX 4.25, QNX 6
   - FreeBSD
   - Solaris 10
   - AIX 5.x
   - HP-UX 11i

Requirements

- The devices that connect to the Serial Console Server must support the following serial protocol:
  - RS-232 (protocol or terminal operations)
- For Console Management operating mode; Telnet/SSH client, a third party client such as PuTTY, or web browser must be installed
- For the browser-based WinClient ActiveX, SNViewer for console operating mode, and DirectX 8 must be present, and at least 2MB of memory must be available after installation.
- For the browser-based Java Viewer SNViewer for console management operating mode, Java Runtime Environment (JRE) 8 or later must be installed, and at least 2MB of memory must be available after installation. Java is available for free download from the Sun Java website:

  `http://java.sun.com`
- For the browser-based WebClient for console management operating mode, make sure your browsers support HTML5 or later.
- The Virtual COM port driver (Real COM port) support requires Windows 2000 or later.
- 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 2.2, 2.4, 2.6 (up to 2.6.39), and 3.1 (up to 3.1.5-23).
- The Fixed TTY driver for UNIX supports: Unix, OpenServer; Unix Ware 7, SVR 5; Unix Ware 2.1, SVR 4.2; QNX 4.25, QNX 6; FreeBSD; Solaris 10; AIX 5.x; and HP-UX 11i.
- For the *Log Server*, you must have the driver Microsoft Jet OLEDB 4.0 or later installed.

DTE/DCE Auto-Sensing

To connect to RJ45 cosole ports

- With Cisco pinouts and auto-sensing DTE/DCE feature, serial console server can connect to Cisco switches (and other compatible devices) with straight-through Cat 5e cables.
- For serial port pin outs, please refer to *Pin Assignment* on page 273.

To connect to DB9 or DB25 device interface

- Serial console server can connect to PC COM port (DB9) with Cisco Console Cable.
- If you wish to make a DB9 or DB25 adapter, please refer to *DB-9/DB-25 Interface* on page 274.

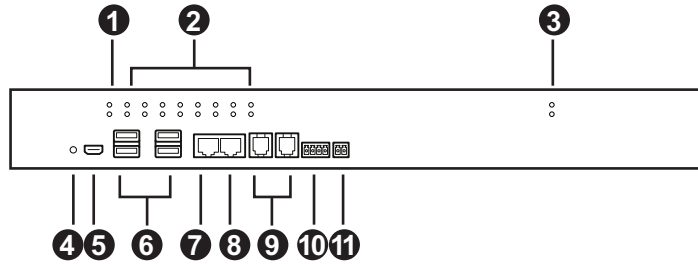
Browsers

Supported browsers for logging into the device include the following:

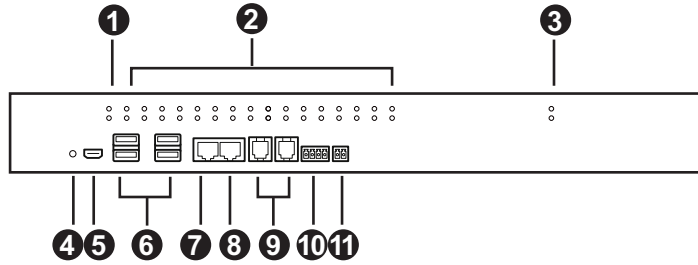
Browser	Version
Chrome	70 or later
Firefox	63 or later
Safari	12 or later
Edge	118 or later

Components

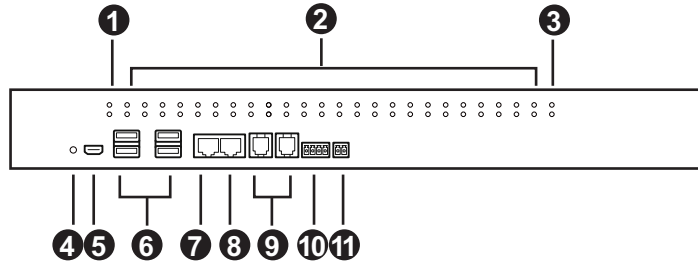
SN1116CO / SN1116COD Front View



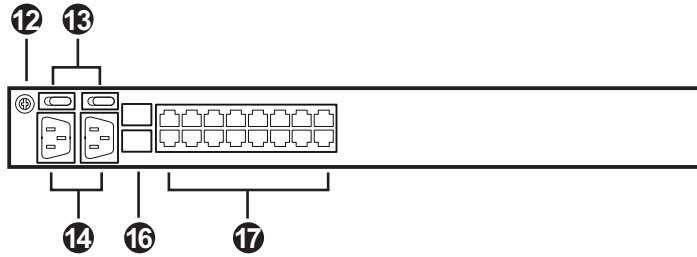
SN1132CO / SN1132COD Front View



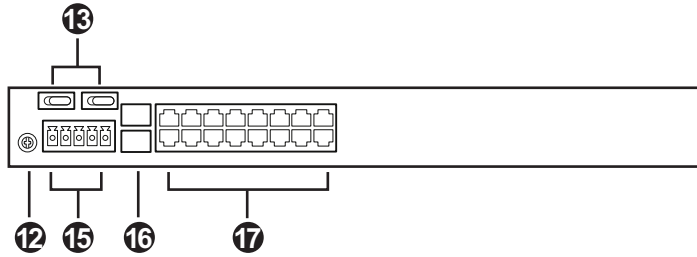
SN1148CO / SN1148COD Front View



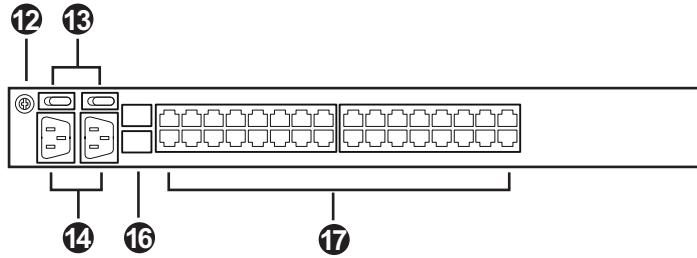
SN1116CO Rear View



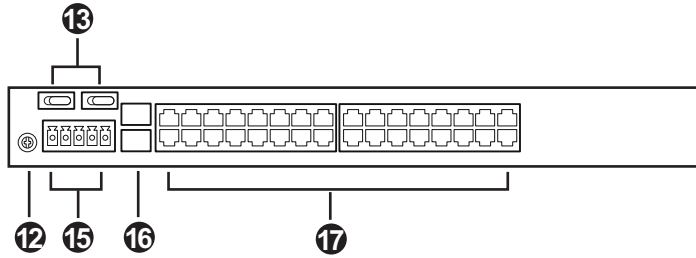
SN1116COD Rear View (DC Power)



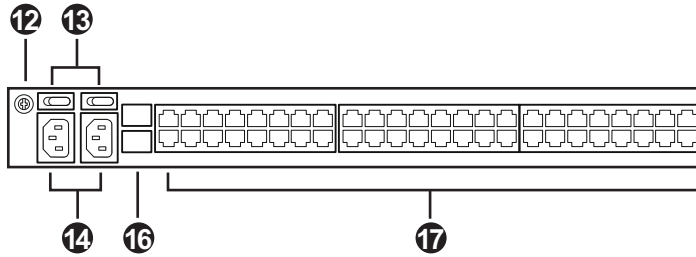
SN1132CO Rear View



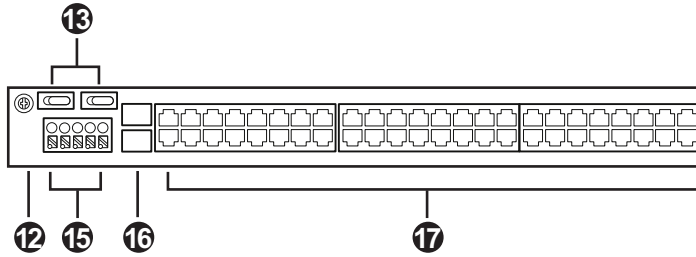
SN1132COD Rear View (DC Power)



SN1148CO Rear View

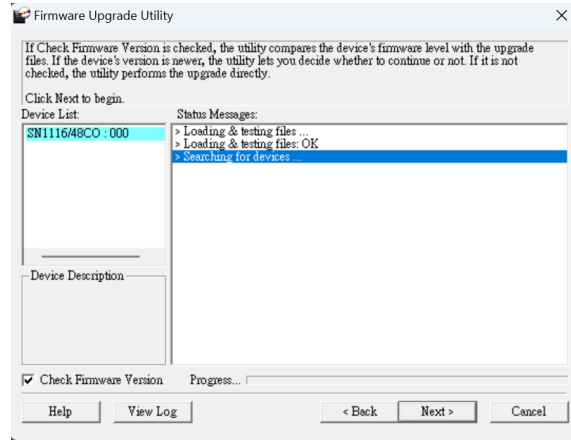


SN1148COD Rear View (DC Power)



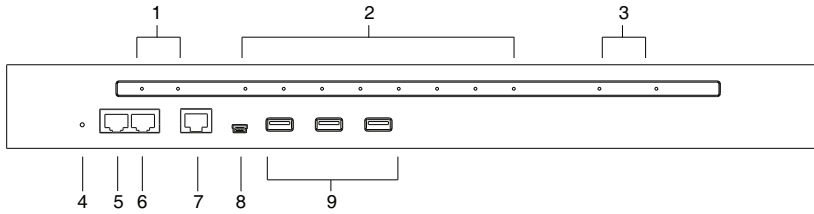
No.	Component	Description
1	power LED	Lights when the unit is powered up and ready to operate.
2	serial port LEDs	The Port LEDs provide status information about their corresponding serial ports. ◆ Lights Green: Online – the serial device attached to the port is powered on and ready. Flashes Green: Active – data is being transmitted through the port

No.	Component	Description
3	LAN LEDs	Primary and Secondary 10/100/1000 Mbps LAN LEDs. ◆ RED: 10 Mbps ◆ RED + GREEN (ORANGE): 100 Mbps ◆ GREEN: 1000 Mbps ◆ Flashes to indicate that the Serial Console Server is being accessed over the LAN.
4	reset switch	◆ Pressing and releasing this switch when the unit is running performs a system reset. ◆ Pressing and holding this switch in for more than three seconds when the unit is running resets its configuration to the factory default settings. **Note:** This does not clear User Account information. See *Clear Login Information*, page 272, for information on clearing user account information. ◆ Pressing and holding this switch while powering on the switch returns the unit to its factory default firmware level, rather than the firmware version that the switch has been upgraded to. This allows you to recover from a failed firmware upgrade and gives you the opportunity to try upgrading the firmware again. **Note:** This operation should only be performed in the event of a firmware upgrade failure that results in the device becoming inoperable. ◆ If the reset button does not work and all the front panel LEDs flash, it means the Serial Console Server is in recovery mode. Please download the .exe firmware upgrade package from our ATEN official website, run the downloaded package and follow the on-screen instructions.

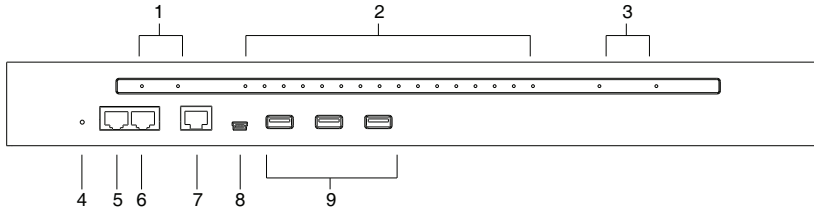


No.	Component	Description
5	laptop USB console port	This mini-USB port allows a PC or laptop to be connected for local access and control. Connect to a PC or laptop to automatically launch a terminal emulator to access the SN text menu.
6	USB Type-A ports	These four Type-A female USB ports can be used to connect USB devices, such as USB storage devices (pen drive / hard drive), USB hubs, and Cisco network switch via USB or serial console. An optional accessory UC232B is recommended when connecting the Cisco network switch via serial console.
7	PON port	Reserved.
8	RJ-45 port (local console)	This RJ45 port allows for local administration and access through a serial terminal connection to a computer. We recommend using the Cisco console cable for this connection.
9	RJ-11 ports (sensor 1 / sensor 2)	These RJ-11 ports can be used to connect temperature, humidity, and/or air pressure sensors.The RJ-11 compatible sensors are as follows: EA1140, EA1240, and EA1340. These sensors are sold separately. Please contact your ATEN dealer for product information.
10	4-pin terminal block (sensor 3)	This 4-pin terminal block can be used to connect door or water leak sensors. The 4-pin terminal block compatible sensors are as follows: EA1440, EA1441, EA1442, and EA1540. These sensors are sold separately. Please contact your ATEN dealer for product information.
11	2-pin terminal block (relay)	This 2-pin terminal block can be used to connect a door access control.
12	grounding terminal	The grounding wire that is used to ground the unit attaches here.
13	power switch	This standard rocker switches power the unit on and off.
14	power socket	The power cable(s) plugs in here.
15	5-pin terminal block (DC power)	The electric leads from your power source connect to this DC terminal block. **Note:** This is available on SN1116COD / SN1132COD / SN1148COD only.
16	SFP ports (LAN 1 / LAN 2)	The fiber or Cat 5e cable that connect the unit to the network interface (10/100/1000 Mbps) plugs in here.The optional accessories are as follows: 2A-136G and 2A-137G SFP Modules or 2A-143G Cooper Module. Please contact your ATEN dealer for product information.
17	RJ-45 ports (serial)	The Cat 5e cables that connect to the serial devices or RJ45-to-Serial adapters plug in here.

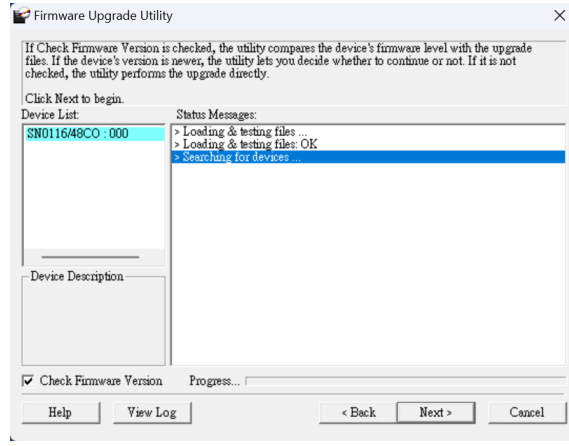
SN0108CO / SN0108COD Front View



SN0116CO / SN0116COD Front View

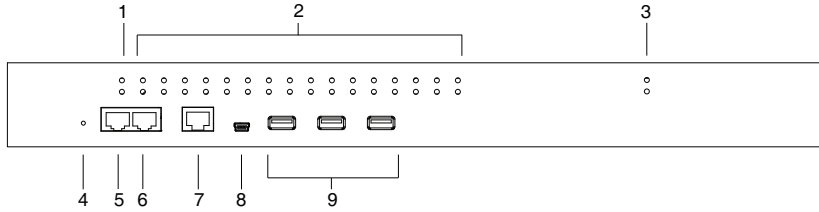


No.	Component	Description
1	power LEDs	Lights when the unit is powered up and ready to operate.
2	port LEDs	The Port ◆ Flashes Green: Active – data is being transmitted through the port
3	LAN LEDs	Primary and Secondary 10/100/1000 Mbps LAN LEDs. ◆ RED: 10 Mbps ◆ RED + GREEN (ORANGE): 100 Mbps ◆ GREEN: 1000 Mbps ◆ Flashes to indicate that the Serial Console Server is being accessed over the LAN.

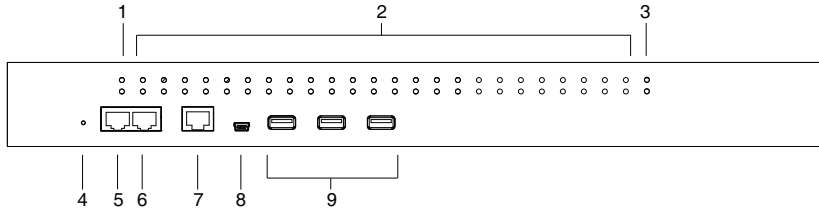
No.	Component	Description
4	reset button	◆ Pressing and releasing this switch when the unit is running performs a system reset. ◆ Pressing and holding this switch in for more than three seconds when the unit is running resets its configuration to the factory default settings. **Note:** This does not clear User Account information. See *Clear Login Information*, page 272, for information on clearing user account information. ◆ Pressing and holding this switch while powering on the switch returns the unit to its factory default firmware level, rather than the firmware version that the switch has been upgraded to. This allows you to recover from a failed firmware upgrade and gives you the opportunity to try upgrading the firmware again. **Note:** This operation should only be performed in the event of a firmware upgrade failure that results in the device becoming inoperable. ◆ If the reset button does not work and all the front panel LEDs flash, it means the Serial Console Server is in recovery mode. Please download the .exe firmware upgrade package from our ATEN official website, run the downloaded package and follow the on-screen instructions. 
5	PON port	Reserved.
6	modem port	For dial in connection should the unit be unavailable over the network. See *Serial Console Server Installation*, page 33, step 6 for installation details.
7	local console port	This RJ45 port allows for local administration and access through a serial terminal connection to a computer. We recommend using the Cisco console cable for this connection.

No.	Component	Description
8	laptop USB console (LUC) port	This mini-USB port allows a PC or laptop to be connected for local access and control. Connect to a PC or laptop to automatically launch a terminal emulator to access the SN text menu.
9	USB ports	These three Type A female USB ports can be used to connect USB devices, such as USB storage devices (pen drive / hard drive), USB hubs, and Cisco network switch via USB or serial console. An optional accessory UC232B is recommended when connecting the Cisco network switch via serial console.

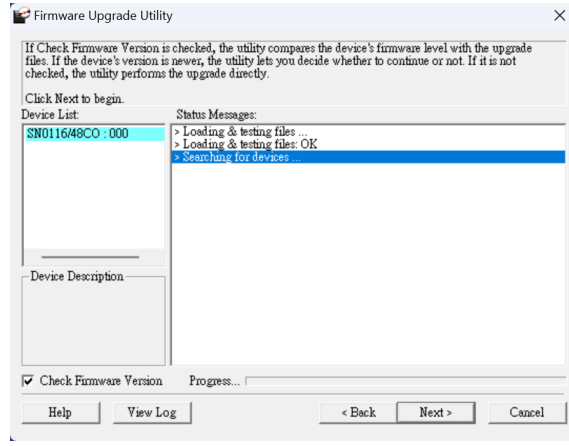
SN0132CO / SN0132COD Front View



SN0148CO / SN0148COD Front View

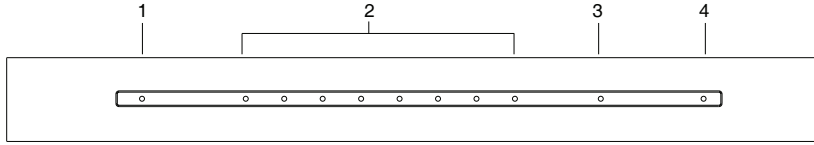


No.	Component	Description
1	power LEDs	Lights when the unit is powered up and ready to operate.
2	port LEDs	The Port LEDs provide status information about their corresponding serial ports. ◆ Lights Green: Online – the serial device attached to the port is powered on and ready. ◆ Flashes Green: Active – data is being transmitted through the port
3	LAN LEDs	Primary and Secondary 10/100/1000 Mbps LAN LEDs. ◆ RED: 10 Mbps ◆ RED + GREEN (ORANGE): 100 Mbps ◆ GREEN: 1000 Mbps ◆ Flashes to indicate that the Serial Console Server is being accessed over the LAN.

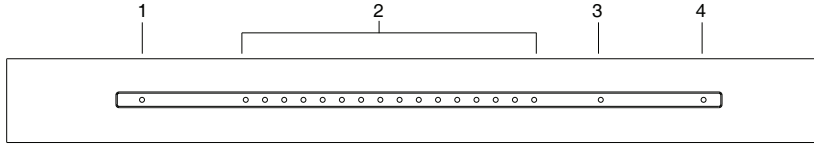
No.	Component	Description
4	reset button	◆ Pressing and releasing this switch when the unit is running performs a system reset. ◆ Pressing and holding this switch in for more than three seconds when the unit is running resets its configuration to the factory default settings. **Note:** This does not clear User Account information. See *Clear Login Information*, page 272, for information on clearing user account information. ◆ Pressing and holding this switch while powering on the switch returns the unit to its factory default firmware level, rather than the firmware version that the switch has been upgraded to. This allows you to recover from a failed firmware upgrade and gives you the opportunity to try upgrading the firmware again. **Note:** This operation should only be performed in the event of a firmware upgrade failure that results in the device becoming inoperable. ◆ If the reset button does not work and all the front panel LEDs flash, it means the Serial Console Server is in recovery mode. Please download the .exe firmware upgrade package from our ATEN official website, run the downloaded package and follow the on-screen instructions. 
5	PON port	Reserved.
6	modem port	For dial in connection should the unit be unavailable over the network. See *Serial Console Server Installation*, page 33, step 6 for installation details.
7	local console port	This RJ45 port allows for local administration and access through a serial terminal connection to a computer. We recommend using the Cisco console cable for this connection.

No.	Component	Description
8	laptop USB console (LUC) port	This mini-USB port allows a PC or laptop to be connected for local access and control. Connect to a PC or laptop to automatically launch a terminal emulator to access the SN text menu.
9	USB ports	These three Type A female USB ports can be used to connect USB devices, such as USB storage devices (pen drive / hard drive), USB hubs, and Cisco network switch via USB or serial console. An optional accessory UC232B is recommended when connecting the Cisco network switch via serial console.

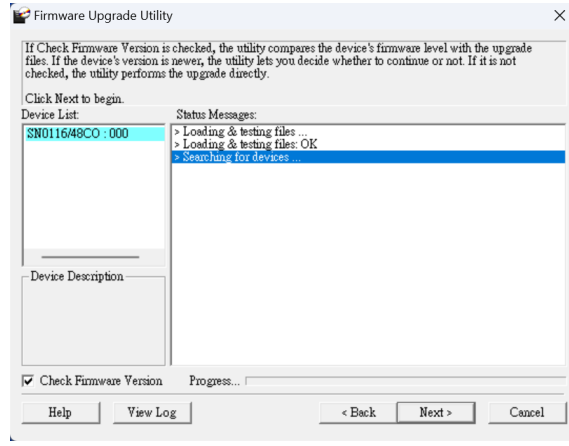
SN9108CO Front View



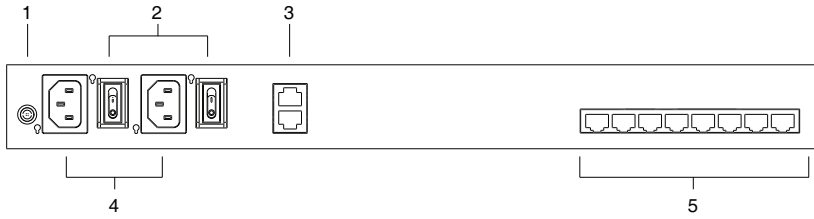
SN9116CO Front View



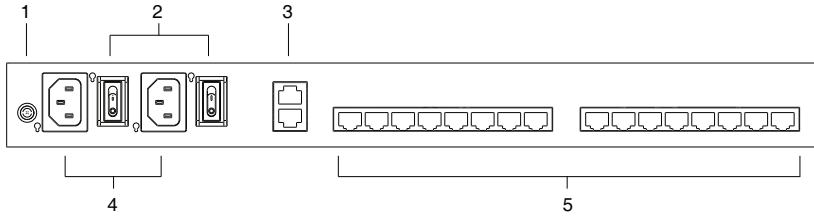
No.	Component	Description
1	power LED	Lights when the unit is powered up and ready to operate.
2	port LEDs	The Port LEDs provide status information about their corresponding serial ports. ◆ Lights Green: Online – the serial device attached to the port is powered on and ready. ◆ Flashes Green: Active – data is being transmitted through the port
3	LAN LED	Primary and Secondary 10/100/1000 Mbps LAN LEDs. ◆ RED: 10 Mbps ◆ RED + GREEN (ORANGE): 100 Mbps ◆ GREEN: 1000 Mbps ◆ Flashes to indicate that the Serial Console Server is being accessed over the LAN.

No.	Component	Description
4	reset button	◆ Pressing and releasing this switch when the unit is running performs a system reset. ◆ Pressing and holding this switch in for more than three seconds when the unit is running resets its configuration to the factory default settings. **Note:** This does not clear User Account information. See *Clear Login Information*, page 272, for information on clearing user account information. ◆ Pressing and holding this switch while powering on the switch returns the unit to its factory default firmware level, rather than the firmware version that the switch has been upgraded to. This allows you to recover from a failed firmware upgrade and gives you the opportunity to try upgrading the firmware again. **Note:** This operation should only be performed in the event of a firmware upgrade failure that results in the device becoming inoperable. ◆ If the reset button does not work and all the front panel LEDs flash, it means the Serial Console Server is in recovery mode. Please download the .exe firmware upgrade package from our ATEN official website, run the downloaded package and follow the on-screen instructions. 

SN0108CO Rear View

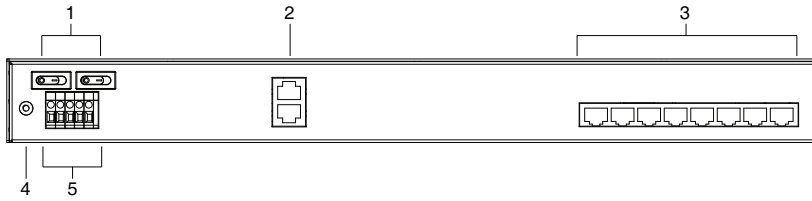


SN0116CO Rear View

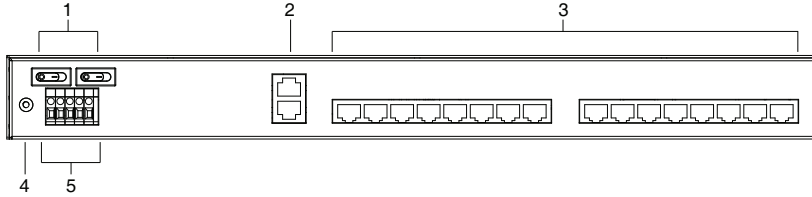


No.	Component	Description
1	grounding terminal	The grounding wire that is used to ground the unit attaches here.
2	power switches	These standard rocker switches power the unit on and off.
3	LAN ports	The cables that connect the unit to the primary and the backup network interfaces (10/100/1000 Mbps) plug in here.
4	power sockets	The power cable(s) plugs in here.
5	serial ports	The Cat 5e cables that connect to the serial devices or RJ45-to-Serial adapters plug in here.

SN0108COD Rear View (DC Power)

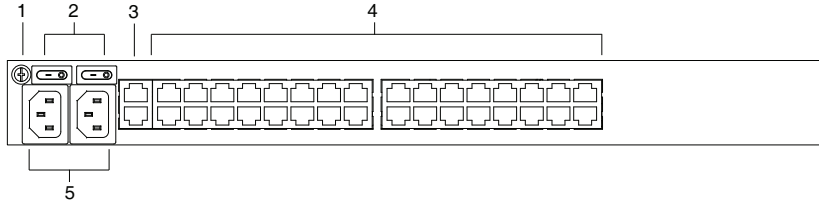


SN0116COD Rear View (DC Power)

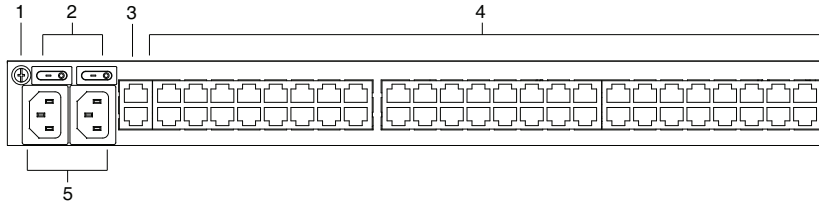


No.	Component	Description
1	power switches	These standard rocker switches power the unit on and off. **Note:** After you turn off the power switches, please wait for at least 2 seconds before you can turn on the power switches.
2	LAN ports	The cables that connect the unit to the primary and the backup network interfaces (10/100/1000 Mbps) plug in here.
3	serial ports	The Cat 5e cables that connect to the serial devices or RJ45-to-Serial adapters plug in here.
4	grounding terminal	The grounding wire that is used to ground the unit attaches here.
5	DC terminal block	The electric leads from your power source connect to this DC terminal block.

SN0132CO Rear View

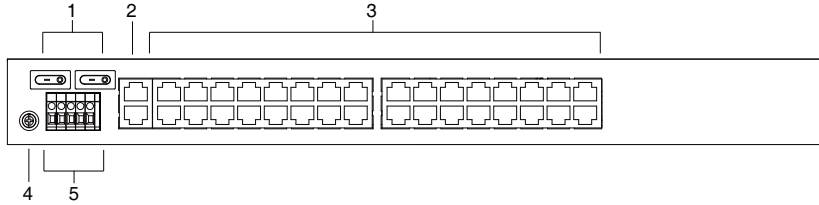


SN0148CO Rear View

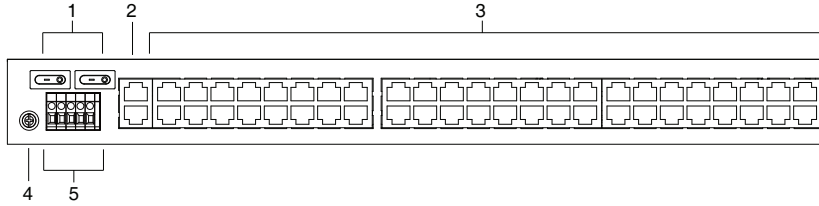


No.	Component	Description
1	grounding terminal	The grounding wire that is used to ground the unit attaches here.
2	power switches	These standard rocker switches power the unit on and off.
3	LAN ports	The cables that connect the unit to the primary and the backup network interfaces (10/100/1000 Mbps) plug in here.
4	serial ports	The Cat 5e cables that connect to the serial devices or RJ45-to-Serial adapters plug in here.
5	power sockets	The power cable(s) plugs in here.

SN0132COD Rear View (DC Power)

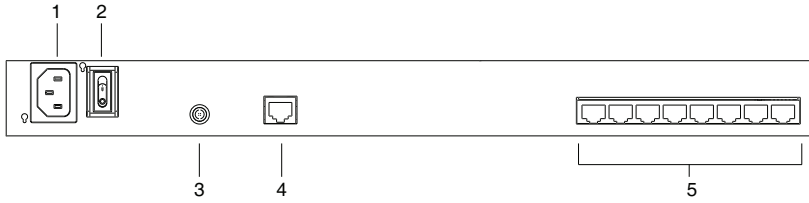


SN0148COD Rear View (DC Power)

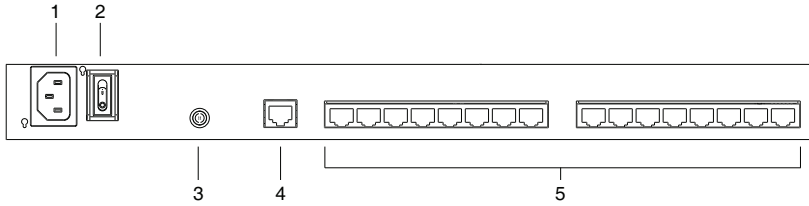


No.	Component	Description
1	power switches	These standard rocker switches power the unit on and off. **Note:** After you turn off the power switches, please wait for at least 2 seconds before you can turn on the power switches.
2	LAN ports	The cables that connect the unit to the primary and the backup network interfaces (10/100/1000 Mbps) plug in here.
3	serial ports	The Cat 5e cables that connect to the serial devices or RJ45-to-Serial adapters plug in here.
4	grounding terminal	The grounding wire that is used to ground the unit attaches here.
5	DC terminal block	The electric leads from your power source connect to this DC terminal block.

SN9108CO Rear View



SN9116CO Rear View



No.	Component	Description
1	power socket	The power cable(s) plugs in here.
2	power switch	This standard rocker switches power the unit on and off.
3	grounding terminal	The grounding wire that is used to ground the unit attaches here.
4	LAN port	The cable that connect the unit to the network interface (10/100/1000 Mbps) plugs in here.
5	serial ports	The Cat 5e cables that connect to the serial devices or RJ45-to-Serial adapters plug in here.

Chapter 2
Hardware Setup

Before You Begin



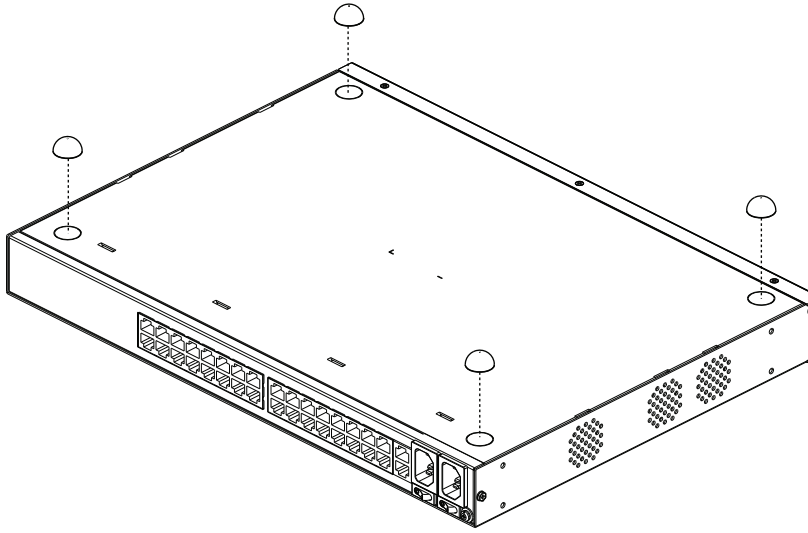
1. Important safety information regarding the placement of this device is provided on page 247. Please review it before proceeding.
2. Make sure that the power to any device that you connect to the installation has been turned off. You must unplug the power cords

Stacking and Rack Mounting

The Serial Console Server can be stacked on the desktop or rack mounted in a variety of ways. The following sections take you through the procedures for each method.

Stacking

The Serial Console Server can be placed on any appropriate level surface that can safely support its weight plus the weight of its attached cables. To place the device, or to stack units if you are daisy-chaining them, remove the backing material from the bottom of the rubber feet that came with your package, and stick them onto the device's bottom panel at the corners, as shown in the diagram, on the following page:



Note: To ensure adequate ventilation, allow at least 5.1 cm on each side, and 12.7 cm behind the unit for power cord and cable clearance.

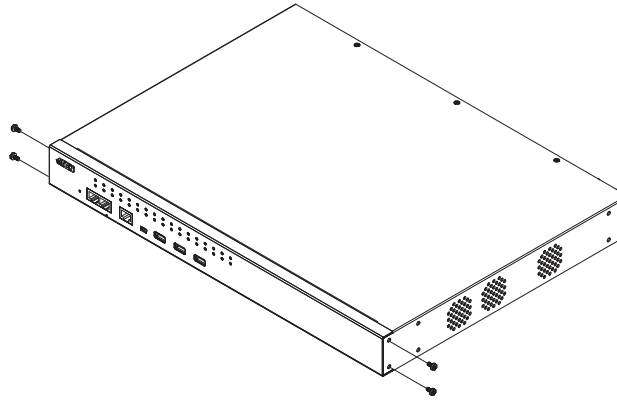
Rack Mounting

The Serial Console Server can be mounted in a 19" (1U) rack. The mounting brackets can screw into either the front or the back of the unit so that it can attach to the front or the back of the rack.

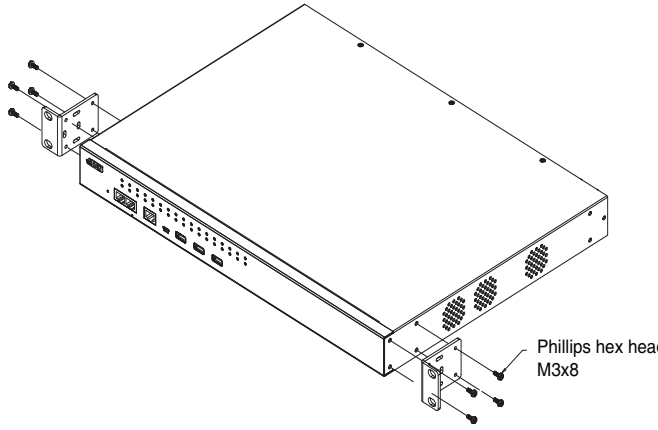
Rack Mounting - Front

To mount the unit at the front of the rack, do the following:

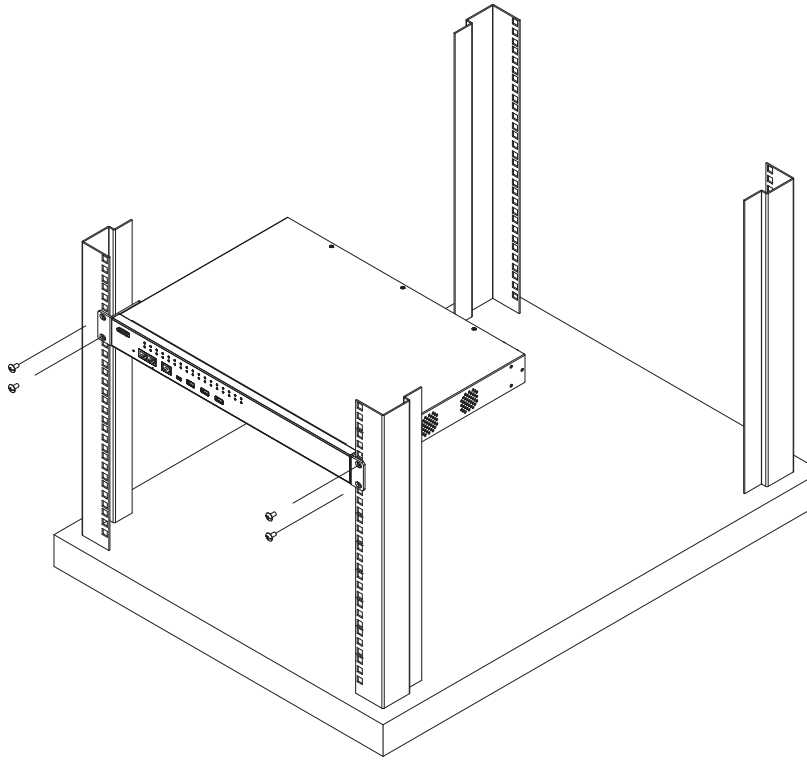
1. Remove the four screws at the front of the unit.



2. Use the M3 x 8 Phillips head hex screws supplied with the rack mount kit to screw the rack mounting brackets into the front of the unit.



3. Position the device in the front of the rack and align the holes in the mounting brackets with the holes in the rack. Screw the mounting brackets to the rack.

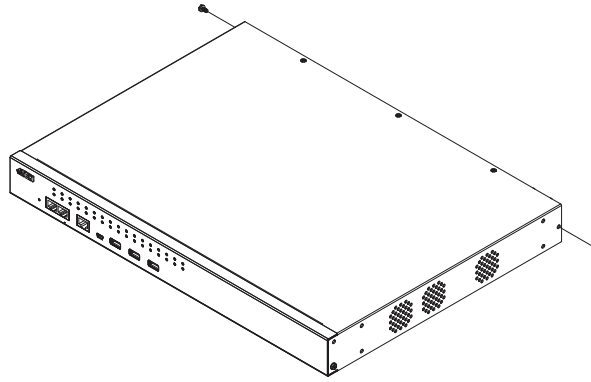


Note: Cage nuts are provided for racks that are not pre-threaded.

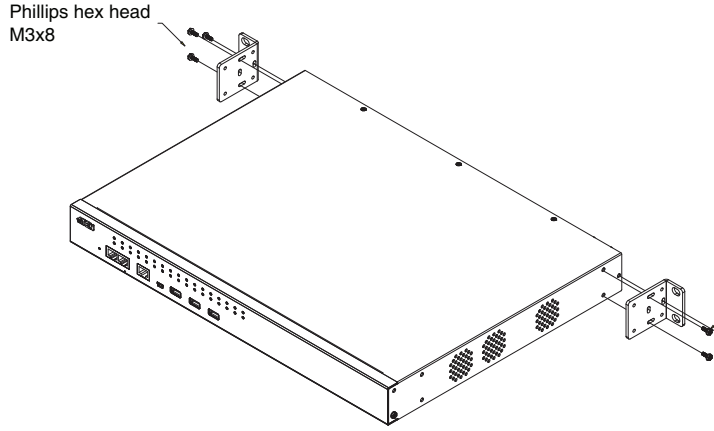
Rack Mounting - Rear

To mount the unit at the rear of the rack, do the following:

1. Remove the two screws at the rear of the unit.

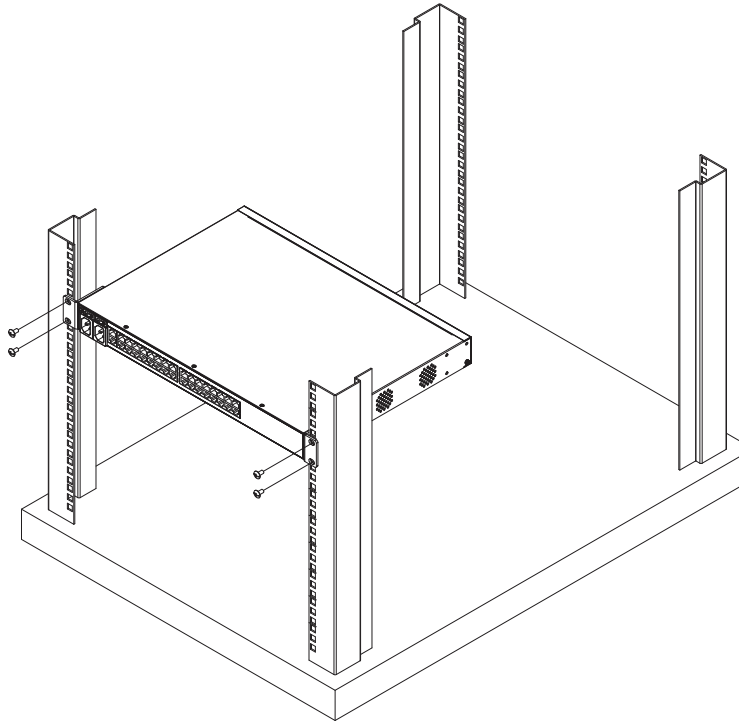


2. Use the M3 x 8 Phillips head hex screws supplied with the rack mounting kit to screw the rack mounting brackets into the rear of the unit.



3. Position the device in the rack and align the holes in the mounting brackets with the holes in the rack.

4. Screw the mounting brackets to the rear of the rack.



Note: Cage nuts are provided for racks that are not pre-threaded.

Serial Console Server Installation

SN1116CO / SN1132CO / SN1148CO Installation

To set up your SN1116CO / SN1132CO / SN1148CO installation, refer to the Installation Diagram on page 35. The numbers in the diagram correspond to the numbers of the instruction steps, below:

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

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

2. Use any of the following methods to connect servers/serial devices and/or network switches.
   - For each server or serial device with a DB-9 connector, connect a Cisco console cable or a Cat 5e cable with RJ-45 to DB-9(F) adapter between its serial port and any available RJ-45 port on the unit's rear panel.

     Note: Refer to *DB-9/DB-25 Interface* on page 274 for pin assignments.

   - Connect a Cat 5e cable between a Cisco network switch (or any compatible network switch) and any available RJ-45 port on the unit's rear panel.

     Note: For a compatible network switch, please make sure the RJ-45 port pin definition of the target device matches the unit. Examples of compatible network switches: Juniper, HPE, Dell, Huawei, H3C, EdgeCore, TRENDnet, Fortinet and ATEN ES0152 / ES0154.

3. For remote control purpose, connect the unit to the network by connecting both the LAN 1 and LAN 2 SFP ports on the unit's rear panel to the network switch with fiber or Cat 5e cables via optional accessories 2A-136G and 2A-137G SFP Modules or 2A-143G Copper Module. Please contact your ATEN dealer for product information.
4. To use a console terminal connection, do any of the following.

- Use a Cisco console cable to connect between the local console port on the unit's front panel and the DB-9 connector of a console terminal or a computer.
- For the console terminal or computer without DB-9 connector, use a Cat 5e cable with UC232BF to connect between the local console and USB ports of the console terminal or computer.

Note: The UC232BF USB to RJ-45 (RJ-232) Console Adapter is sold separately. Please contact your ATEN dealer for product information.

5. (Optional) To control the unit locally using a laptop, connect a laptop via the supplied laptop USB console cable to the unit's laptop USB console port on the front panel.
6. (Optional) Connect up to four USB peripheral devices to the unit's USB Type-A ports on the front panel.
   - USB flash drive.

   Note: The supported file system for USB storage devices are FAT8, FAT16 and FAT32.

   - Network switch via its USB console port.
   - Network switch via its serial console port using an UC232BF USB to RJ-45 (RS-232) Console Adapter.

   Note: When connecting another network switch, make sure to use only one of the following method, either via the serial console port on the rear panel or the USB console port on the front panel.

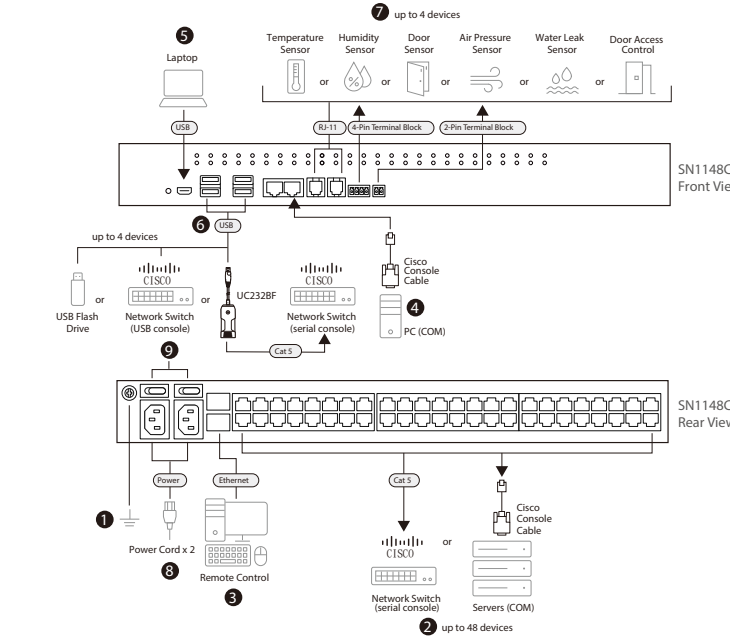
7. (Optional) To use sensors for data readings, connect up to four sensors to the unit's RJ-11 ports (sensor 1 and sensor 2), 4-pin terminal block (sensor 3), and 2-pin terminal block (relay).
   - RJ-11 compatible sensors: EA1140, EA1240, and EA1340.
   - 4-pin terminal block compatible sensors: EA1440, EA1441, EA1442, and EA1540.

   Note: These sensors are sold separately. Please contract your ATEN dealer for product information.

   - To use a door access control, connect the door access control device to the unit's 2-pin terminal block (relay).

8. For AC models (SN1116 CO / SN1132CO / SN1148CO): Connect the supplied AC power cords to the unit's power sockets to an AC power source. For DC models (SN1116COD / SN1132COD / SN1148COD): Connect the DC power source to the unit's DC terminal block.
9. Turn on the power switches.

SN1116CO / SN1132CO / SN1148CO Installation Diagram



Note: A SN1148CO serial console server is used as an example to illustrate the installation. As for other serial console servers, the installation is identical with fewer serial ports.

SN0108CO / SN0116CO / SN0132CO / SN0148CO Installation

To set up your SN0108CO / SN0116CO / SN0132CO / SN0148CO installation, refer to the Installation Diagram on page 38. The numbers in the diagram correspond to the numbers of the instruction steps, below:

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

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

2. Use any of the following methods to connect servers/serial devices and/or network switches.
   - For each server or serial device with a DB-9 connector, connect a Cisco console cable or a Cat 5e cable with RJ-45 to DB-9(F) adapter between its serial port and any available RJ-45 port on the unit's real panel.

     Note: Refer to *DB-9/DB-25 Interface* on page 274 for pin assignments.

   - Connect a Cat 5e cable between a Cisco network switch (or any compatible network switch) and any available RJ-45 port on the unit's real panel.

     Note: For a compatible network switch, please make sure the RJ-45 port pin definition of the target device matches the unit. Examples of compatible network switches: Juniper, HPE, Dell, Huawei, H3C, EdgeCore, TRENDnet, Fortinet and ATEN ES0152 / ES0154.

3. For remote control purpose, connect the unit to the network by connecting both the LAN 1 and LAN 2 ports on the unit's rear panel to the network with Cat 5e cables.
4. (Optional) To use a serial modem for OOB operation, connect a Cisco console cable to a null modem adapter. Connect the DB-9 connector to the modem and the RJ-45 connector to the modem port on the unit's front panel.
5. (Optional) For power management, connect a Cat 5e cable between an ATEN PDU and the PON port on the unit's front panel.
6. To use a console terminal connection, do any of the following.
   - Use Cisco console cable to connect between the local console port on the unit's front panel and the DB-9 connector of a console terminal or a computer.

   For the console terminal or computer without DB-9 connector, use a Cat 5e cable with UC232BF to connect between the local console and USB ports of the console terminal or computer.

   Note: The UC232BF USB to RJ-45 (RS-232) Console Adapter is sold separately. Please contact your ATEN dealer for product information.

7. (Optional) To control the unit locally using a laptop, connect a laptop via the supplied laptop USB console cable to the unit's laptop USB console port on the front panel.
8. (Optional) Connect up to three USB peripheral devices to the unit's USB Type-A ports on the front panel.
   - USB flash drive.

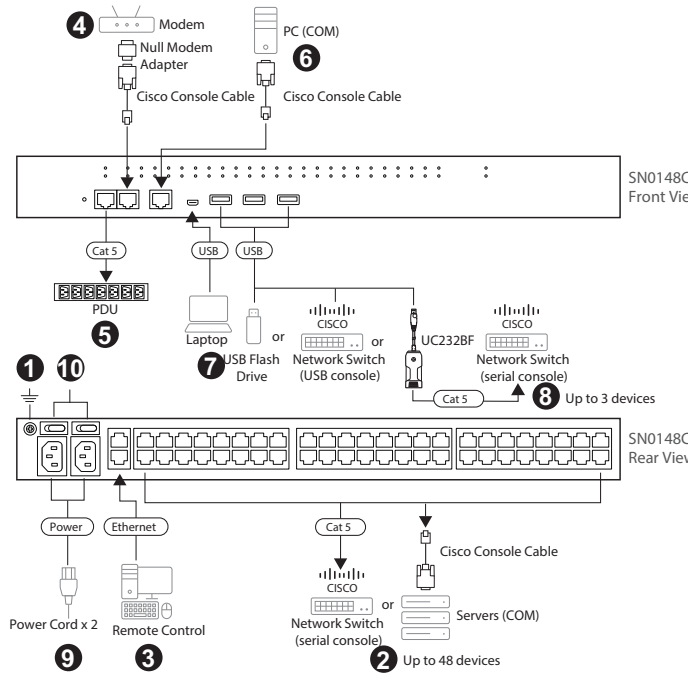
     Note: The supported file system for USB storage devices are FAT8, FAT16 and FAT32.

   - Network switch via its USB console port.
   - Network switch via its serial console port using an UC232BF USB to RJ-45 (RS-232) Console Adapter.

     Note: When connecting another network switch, make sure to use only one of the following method, either via the serial console port on the rear panel or the USB console port on the front panel.

9. For AC models (SN0108CO / SN0116CO / SN0132CO / SN0148CO): Connect the supplied AC power cords to the unit's power sockets to an AC power source. For DC models (SN0108COD / SN0116COD / SN0132COD / SN0148COD): Connect the DC power source to theunit's DC terminal block.
10. Turn on the power switch.

SN0108CO / SN0116CO / SN0132CO / SN0148CO Installation Diagram



Note: A SN0148CO serial console server is used as an example to illustrate the installation. As for other serial console servers, the installation is identeical with fewer serial ports.

Note: The example above shows a SN0148CO Serial Console Server. The SN0108CO / SN0116CO / SN0132CO units have the same ports and switches but with slightly different layouts. See *Components*, page 9 for details.

SN9108CO / SN9116CO Installation

To set up your SN9108CO / SN9116CO installation, refer to the Installation Diagram on page 40. The numbers in the diagram correspond to the numbers of the instruction steps, below:

1. Use a grounding wire to ground the unit by connecting one end of the wire to the Serial Console Server's grounding terminal (located on the back panel), and the other end of the wire to a suitable grounded object.

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

2. For each server or serial device with a DB-9 connector, connect a Cisco Console Cable or a Cat 5e cable with RJ-45-to-DB-9(F) adapter between its serial port and any available RJ-45 port on the Serial Console Server's rear panel.

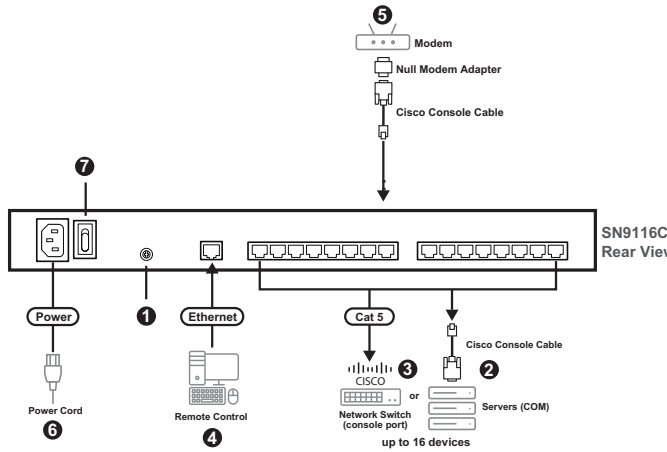
   Note: Refer to *DB-9/DB-25 Interface* on page 274 for pin assignments.

3. Connect a Cat 5e cable between a Cisco Network Switch (or any compatible network switch) and any available RJ-45 port on the Serial Console Server's rear panel.

   Note: For a compatible network switch, please make sure the RJ-45 port pin definition of the target device matches the Serial Console Server.

4. Connect the Serial Console Server to the network by connecting the LAN port to the network with Cat 5e cables.
5. (Optional) If you choose to install a serial modem for OOB operation, connect a Cisco Console Cable to a null modem adapter. Plug the DB-9 connector into the Modem and the RJ-45 connector into any available RJ-45 port on the Serial Console Server's front panel.
6. For AC models: Use the AC power cord provided with this package to connect the SN9108CO/SN9116CO's Power Socket to an AC power source.
7. Turn on the power switch.

SN9108CO / SN9116CO Installation Diagram

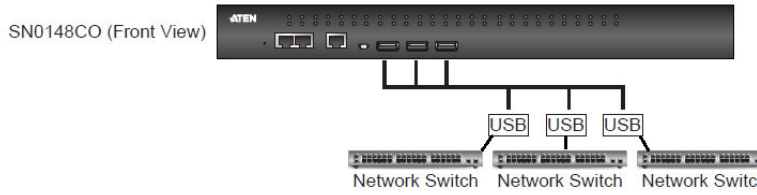


Installing Network Switch with USB Console via USB Cable

Optionally, you can connect up to 3 (SN0100CO / SN0100COD) / 4 (SN1100CO / SN1100COD) network switches to the USB ports on the Serial Console Server.

Note:

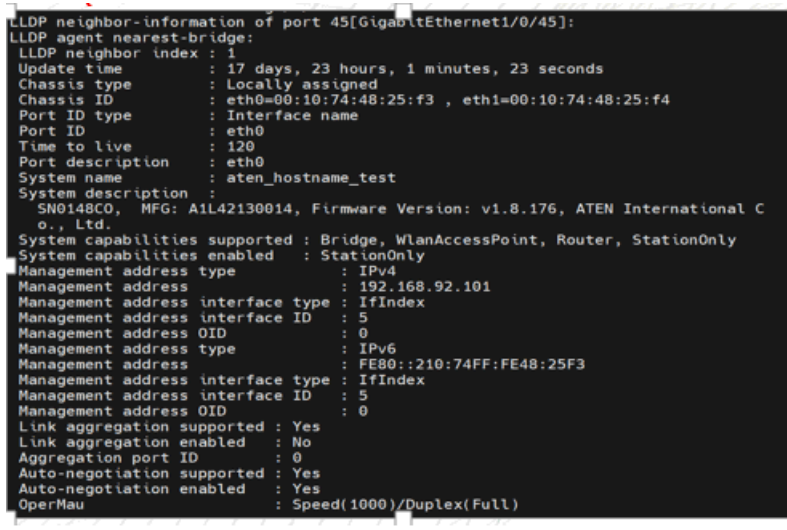
- Please refer to the product page for up-to-date supported network switches.
- When connecting another network switch, make sure to use only one of the following method.
  - Using the serial console port on the rear panel.
  - Using the USB port (via UC232B) on the front panel. When the USB port is used with the UC232B, only console management and console management direct modes are supported.



LLDP

When the Serial Console Server is connected to a network switch, LLDP related commands can be used to retrieve information on the Serial Console Server from the network switch console. Below is an example.

Note: Please refer to the network switch's user manual or user guide for more information on how to execute the LLDP related commands.



Chapter 3
Super Administrator Setup

Overview

This chapter discusses the administrative procedures that the super administrator performs to get the Serial Console Server set up for the first time.

First-Time Setup

Once the Serial Console Server has been cabled up, the super administrator needs to set up the unit for operation. This involves setting the network parameters, and changing the default super administrator login. The most convenient way to do this for the first time is from a local console (local VT console or a local computer running terminal application software, such as Microsoft HyperTerminal), or a Laptop USB Console (LUC) running the SNViewerUSB application (SN1100CO / SN1100COD / SN0100CO / SN0100COD only). Setup can also be done remotely over the web via the GUI using the unit's IP address.

Note: For remote methods of setting up the network, see *IP Address Determination*, page 265.

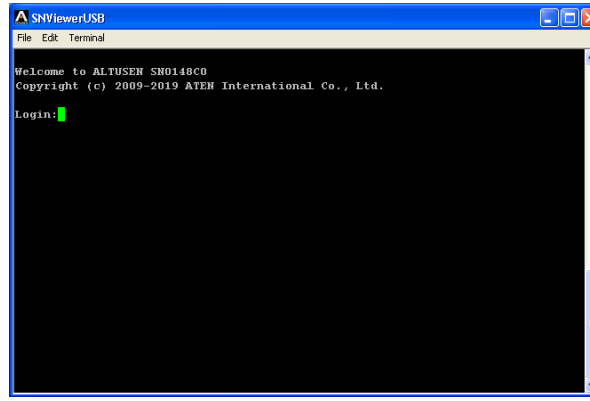
Local Login

You can log in locally from a computer or laptop (SN1100CO / SN1100COD / SN0100CO / SN0100COD only) connected directly to the Serial Console Server (see *Serial Console Server Installation*, page 33). There are two methods for logging in locally *SNViewerUSB* and *HyperTerminal*.

The local login main menu is the text based of the browser based configuration and control functions described throughout this manual. For a complete configuration and control functions, we recommend using the browser based web GUI. You can reference the detailed information provided for the web browser version (*After logging in, the system will force you to change the password, the password must not be the same as the default.*, page 47) as you work your way through the submenus to configure the settings discussed in this chapter.

Laptop USB Console (LUC) Login - SNViewerUSB

The *SNViewerUSB* application appears automatically when a Laptop USB Console (LUC) connection (SN1100CO / SN1100COD / SN0100CO / SN0100COD only) has been established, and you will be prompted to log in, as shown here:



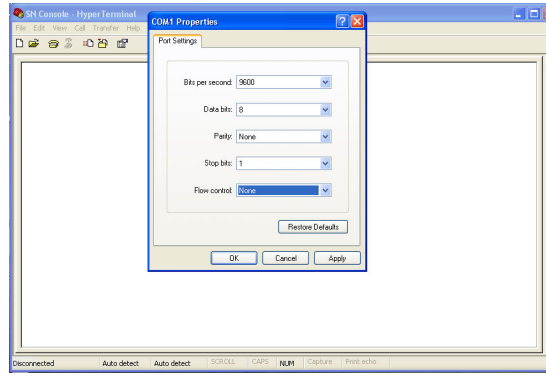
Since this is the first time you are logging in, use the default username: *administrator*; and the default password: *password*.

After logging in, the system will force you to change the password, the password must not be the same as the default.

Console Login - HyperTerminal

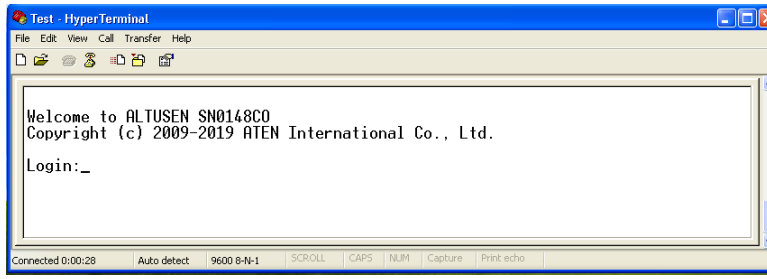
Once a physical connection from a computer to the Serial Console Server has been made you can establish a HyperTerminal session using the instructions below.

1. Open *HyperTerminal*, and configure the port settings for the COM1 port:



Bits per Second: **9600**, Data Bits: **8**, Parity: **None**, Stop bits: **1**, Flow Control: **None**.

2. When configured correctly the login prompt appears, as shown here:

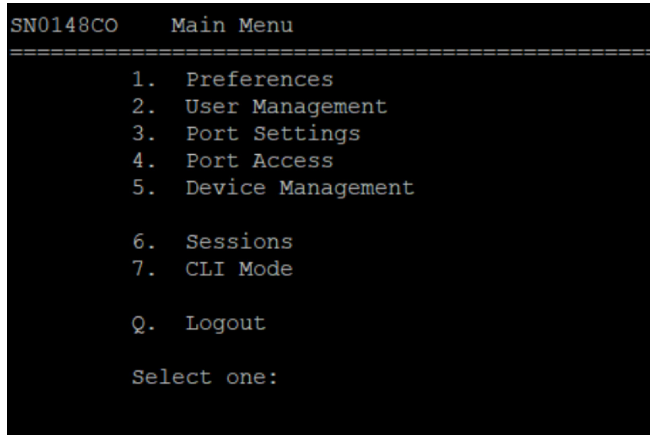


Since this is the first time you are logging in, use the default username: *administrator*; and the default password: *password*.

After logging in, the system will force you to change the password, the password must not be the same as the default.

Local Console Main Menu

After you log in via *HyperTerminal* or *SNViewerUSB* the text based menu appears:



The main menu is the text based equivalent of the browser based configuration and control functions described throughout this manual. You can reference the information provided for the browser version as you work your way through the submenus.

Remote Login

You can log in remotely from a computer running *Telnet, PuTTY*, or via *Web Browser*. The remote login main menu for *Telnet* and *PuTTY* are a text-based equivalent of the browser-based GUI and control functions as described throughout this manual. You can refer to the detailed information provided for the web browser version as you work your way through the text submenus and configure the settings discussed in this chapter.

Telnet Login

Start Telnet, type "*open 192.168.0.60*", press **Enter**, and a login prompt will appear, as show here:

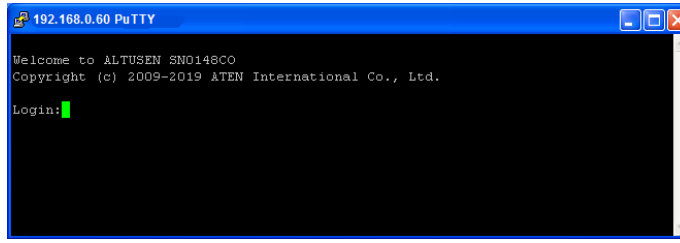


Since this is the first time you are logging in, use the default username: *administrator*; and the default password: *password*.

After logging in, the system will force you to change the password, the password must not be the same as the default.

PuTTY Login

Start PuTTY, enter the Serial Console Server's default IP address (*192.168.0.60*), click **Open**, and a login prompt will appear, as shown here:



Since this is the first time you are logging in, use the default username: *administrator*; and the default password: *password*.

After logging in, the system will force you to change the password, the password must not be the same as the default.

Browser Login

Once the Serial Console Server has been connected to the LAN, it can be accessed via an Internet browser running on any platform. To access the Serial Console Server, do the following:

1. Open the web browser and specify the default IP address (*192.168.0.60*) of the Serial Console Server in the browser's location bar, and press **Enter**.

2. When a Security Alert dialog box appears, accept the certificate, it can be trusted.

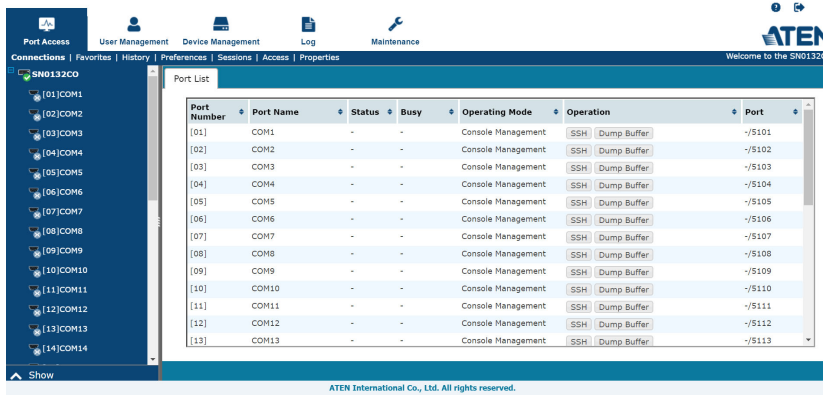
   Once you accept the certificate(s), the login page appears:



3. Since this is the first time you are logging in, use the default username: *administrator*; and the default password: *password*.

   After logging in, the system will force you to change the password, the password must not be the same as the default.

   After you successfully log in, the main page appears:



Looking Up the Login IP Address via IP Installer

If you are unable to login using the Serial Console Server's default IP address (*192.168.0.60*), it means the Serial Console Server have been assigned a different IP address from another network device (DHCP or fixed). You can download the IP Installer utility from our ATEN official website to locate the new IP address.

Follow the steps below to download IP Installer utility, and use the utility to look up the IP address of your Serial Console Server.

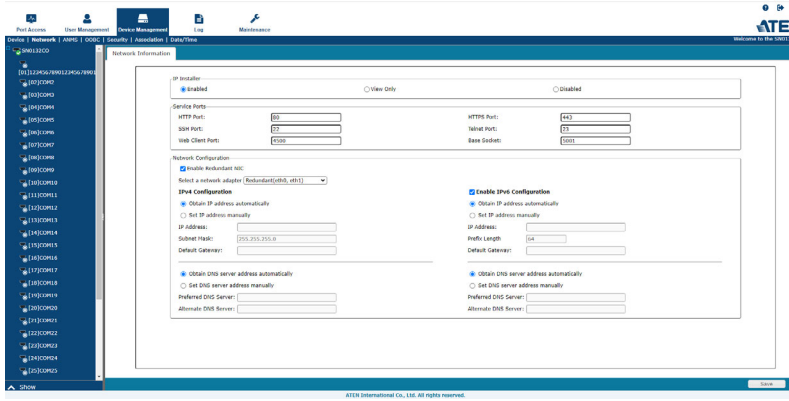
1. Go to the download link below:
   https://www.aten.com/global/en/supportcenter/downloads/
2. Type in Serial Console Server in the field below "Download materials for other products" and press **OK**.
3. Scroll down the page and click any available Serial Console Server.
4. Scroll down the page to find IP Installer zip file under "Software & Drivers". Click the file to download.
5. Unzip and execute the downloaded IP Installer. The Network Device IP Installer screen appears.
6. Click **Enumerate** to search for ATEN devices in the network. The detected devices are shown in Device List.
7. Use the IP address of any Serial Console Server to log in.

Setup

Network Setup

To set up the network, do the following:

1. Click the **Device Management tab.**
2. Select the **Network** tab.



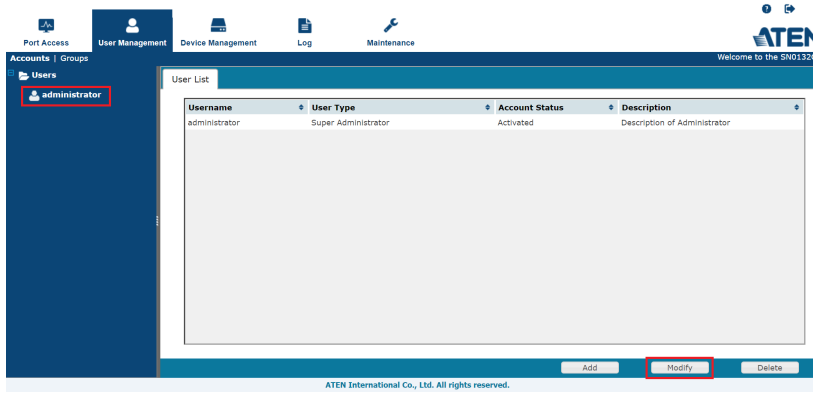
3. Fill in the fields according to the information provided under *Network*, page 131.

Changing the Super Administrator's Login Credentials

To change the default super administrator username and password, do the following:

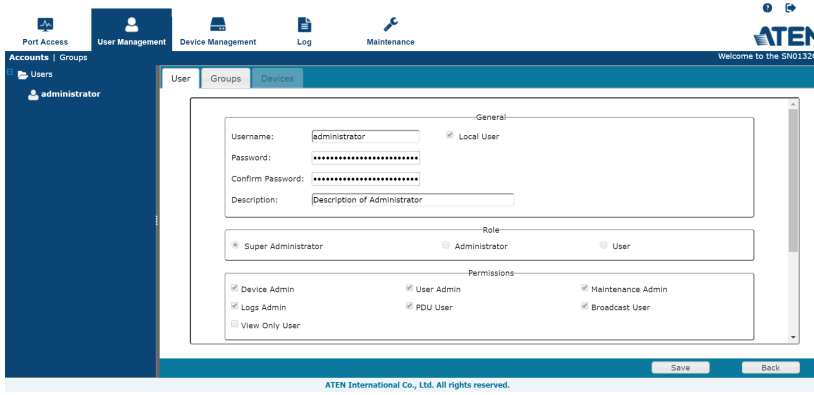
1. At the top of the screen, click the **User Management** tab.

   The User Management page has a list of Users and Groups in the sidebar at the left, and a more detailed list of users – with more information about them – in the large central panel. Since this is the first time the page is being accessed, only the super administrator appears:



2. Click on the account in the left panel or select it in the central panel, then click **Modify** (at the bottom of the page.)

The *User Information* page appears:



3. Change the username and password to something unique.

4. Enter the password again in the *Confirm Password* field to confirm it is correct.
5. Click **Save** (located at the bottom of the page).
6. When the dialog box informing you that the change completed successfully appears, Click **OK**.

Chapter 4
The User Interface

Overview

Once you have successfully logged in, the Serial Console Server's Main Page appears. The look of the page varies slightly, depending on which method you used to log in. Each of the interfaces is described in the sections that follow.

Access

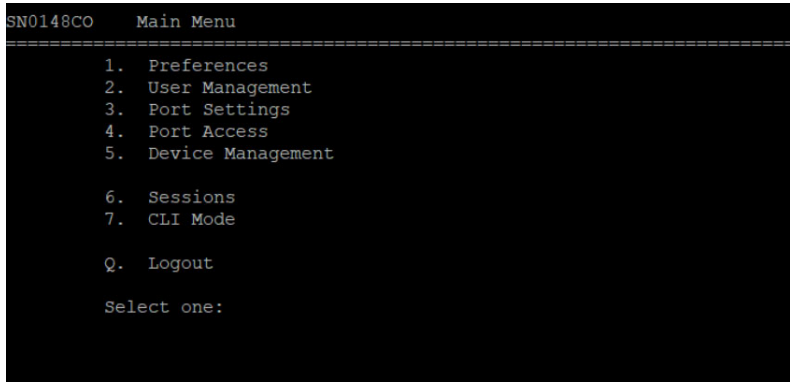
The Serial Console Server can be accessed from a local console (locally connected computer or laptop) running terminal application software (such as Microsoft HyperTerminal) or the SNViewerUSB application; or from a remote computer using Telnet (SSH), PuTTY, or web-based browser (see *First-Time Setup*, page 43 for details).

No matter which access method you choose, the Serial Console Server's authentication procedure requires you to submit a valid username and password. If you supply invalid login information, the authentication routine will return an *Invalid Username or Password*, or *Login Failed* message. If you see this type of message, log in again with a correct username and password.

Note: If the number of invalid login attempts exceeds a specified amount, a timeout period is invoked. You must wait until the timeout period expires before you can attempt to log in again. See *Login Failures*, page 160 for further details.

Local Console Operation

When a local console is attached (SN1100CO / SN1100COD / SN0100CO / SN0100COD only, see page 35), you can use the *HyperTerminal* or *SNViewerUSB* application to log in (See *Local Login*, page 43 for details). Simply key in your valid username and password, then hit **[Enter]** to bring up the Local Console Main Page.



The main menu is the text based of the browser based configuration and control functions described throughout this manual. For a complete configuration and control functions, we recommend using the browser based web GUI. You can reference the information provided for the browser version as you work your way through the submenus.

Note:

- As with the browser version, access to many of these submenus are restricted by the user's permissions. If you select a submenu that you are not authorized for, nothing happens.Some of the submenus do not have an *Exit* choice. In these cases, you can return to the previous menu without making changes by pressing **Enter** twice.
- You can bring up the main menu at any time during your session.
- This menu can also be accessed from remote terminal sessions, such as Windows Telnet Client, and PuTTY.

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.

Remote Operation

You can access the Serial Console Server remotely using a *web browser*, or text based terminal application such as *Telnet* or *PuTTY*, as described below.

Web Browser Login

Serial Console Server units can be accessed via an Internet browser running on any platform. To access the Serial Console Server, do the following:

1. Open the browser and specify the IP address (See *After logging in, the system will force you to change the password, the password must not be the same as the default.*, page 47 for details) of the Serial Console Server you want to access in the browser's location bar.
2. When a security alert dialog box appears, accept the certificate – it can be trusted. If a second certificate appears, accept it as well.

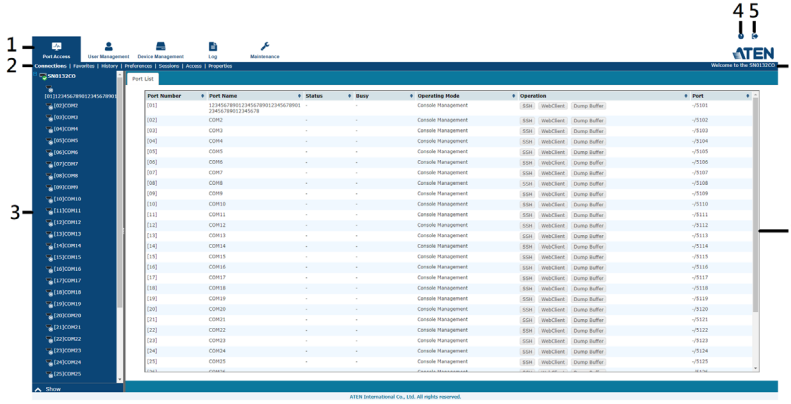
   Once you accept the certificate(s), the login page appears:



3. Provide your username and password (see *After logging in, the system will force you to change the password, the password must not be the same as the default.*, page 47), then click **Login** to bring up the web browser main page, described on the next page.

The Web Browser Main Page

To ensure multi-platform operability, access to the Serial Console Server can be accomplished with most standard web browsers. The chapters following this one give detailed information about each section of the web browser. Once users log in and are authenticated (see page 54), the *Web Browser Main Page* comes up, with the Port Access page displayed:



Note: The screen depicts a super administrator's page. Depending on a user's type and permissions, not all of these elements appear.

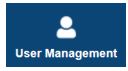
Page Components

The web page screen components are described in the table, below:

No.	Item	Description
1	Tab Bar	The tab bar contains the Serial Console Server main operation categories. The items that appear in the tab bar are determined by the user's type, and the authorization options that were selected when the user's account was created.
2	Menu Bar	The menu bar contains operational sub-categories that pertain to the item selected in the tab bar. The items that appear in the menu bar are determined by the user's type, and the authorization options that were selected when the user's account was created.
3	Sidebar	The sidebar provides a tree view listing of ports that relate to the various tab bar and menu bar selections. Clicking a node in the sidebar brings up a page with the details that are relevant to it. There is a *Filter* button at the bottom of the sidebar that lets you expand or narrow the scope of the ports that appear in the tree.
4	About	About provides information regarding the Serial Console Server's current firmware version.
5	Logout	Click this button to log out of your Serial Console Server session.
6	Welcome Message	If this function is enabled (see *Welcome Message*, page 85), a welcome message displays here.
7	Interactive Display Panel	This is your main work area. The screens that appear here reflect your menu choices and sidebar node selection.

The Tab Bar

The number and type of icons that appear on the tab bar at the top of the page are determined by the user's type (Super Administrator, Administrator, User) and the permissions assigned when the user's account was created. The chapters following this one give detailed information about each section of the web browser. The functions associated with each of the icons are explained in the table below:

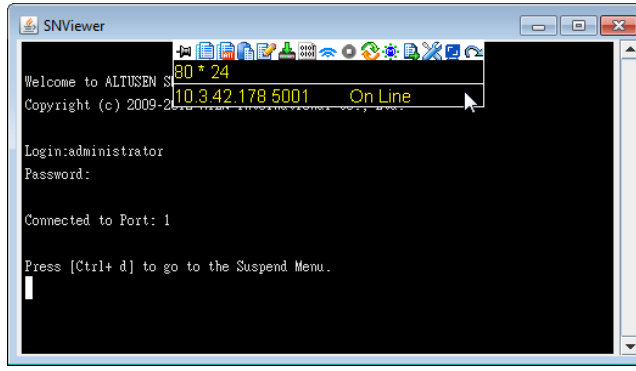
Icon	Function
	**Port Access:** The Port Access page is used to access and control the devices on the Serial Console Server installation. This page is available to all users. Port Access is discussed on page 75.
	**User Management:** The User Management page is used to create and manage users and groups. It can also be used to assign devices to them. This tab is available to the super administrator, as well as administrators and users who have been given User Management permission. The tab doesn't appear for other administrators and users. User Management is discussed on page 107.
	**Device Management:** The Device Management page is used to configure and control the overall operation of the Serial Console Server. This page is available to the super administrator, as well as administrators and users who have been given Device Management permission. The tab doesn't appear for other administrators and users. Device Management is discussed on page 125.
	**Log:** The Log page displays the contents of the log file. The Log page is discussed on page 168.
	**Maintenance:** The Maintenance page is used to install new firmware; backup and restore configuration and account information; restore default values; and import Certificates. This page is available to the Super Administrator (and Administrators and Users with *Maintenance* permission). The icon doesn't display on the page of ordinary administrators and users. The Maintenance page is discussed on page 173.

There are two small icons at the extreme right of the page. Their functions are described in the table, below:

Icon	Function
	Click this icon to bring up a panel with information about the Serial Console Server's firmware version.
	Click this icon to log out and end your Serial Console Server session.

SNViewer

The *SNViewer* is the main application used to access serial devices via web browser. The *SNViewer* opens from the *Port Access - Connections* page, when you click the **Telnet** or **SSH** button for a serial device (see *Telnet/SSH/ WebClient*, page 79 for details). When the *SNViewer* opens there is a Control Panel toolbar that appears when your mouse moves over it, which allows you to configure your session, as shown here:



SNViewer Control Panel

The SNViewer provides a Control Panel that is hidden at the upper center of the screen, and becomes visible when your mouse moves over it. The panel consists of three rows: an icon row at the top, and two text rows below it:



- By default, the upper text row shows the width and height of the window size. As the mouse pointer moves over the icons in the icon bar, however, the information in the upper text row changes to describe the icon's function. In addition, if a message from another user is entered in the message board, and you have not opened the message board in your session, the message board window will pop open automatically.
- The lower row shows the IP address and port of the device you are accessing on the left side, and the connection status on the right.

Control Panel Functions

The Control Panel functions are described below and in the following sections:

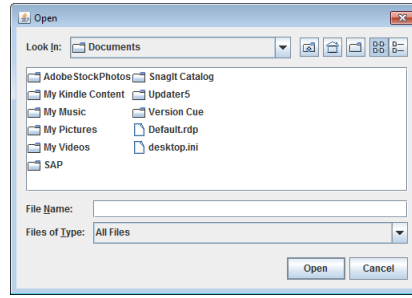
Icon	Function
	This is a toggle. Click to make the Control Panel appear *Always On Top* – i.e., always displays on top of the SNViewer screen. Click again to have it display in *Auto Hide* mode– allowing it to only appear when the mouse is moved over it.
	Use this to copy the selected text on the screen.
	Use this to copy all text that is displayed on the screen.
	Use this to paste the copied text.
	Use this icon to toggle *Logging on / Logging off*. This starts a log file of characters sent from the serial device to the SNViewer. You must first create and import a text based log file (See *Terminal Settings, Others - Log File*, page 64).
	Use this to browse for data files to import (see *Data Import*, page 60).
	Use this to change the page encoding (see *Encode*, page 61).
	Use this icon to enable broadcasting. Broadcasting allows you to access and make changes on a single port and the same changes will be made across all Broadcast Ports. Before using the broadcast function, set the *Broadcast Timeout* and *Broadcast Ports* (see *Preferences*, page 84 for details). For broadcasting to work, you must first access a port set as a Broadcast Port and then click the Broadcast icon on the control panel.
	Click to send a Break command.

Icon	Function
	Use this to reset the terminal to its default settings.
	Click to bring up the Message Board (see *The Message Board*, page 61).
	Click to open a window and create a list of custom text macros (see *Macros*, page 62).
	Use this to change the font, color and other SNViewer settings (see *Terminal Settings*, page 63).
	Use this button to adjust the width of the SNViewer window.
	Click to exit the viewer.



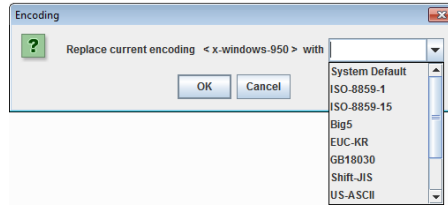
Data Import

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



Encode

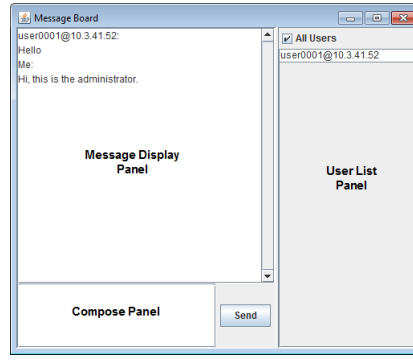
Encoding allows you select which type of encoding you want to use. Make your selection from the drop down menu and click **OK**, as shown below:



Note: Try choosing a different encoding if you get garbled code. For example, if you've named your port name in Korean, Japanese, traditional or simplified Chinese, try UTF-8 encoding and choose Monospaced for Font.

The Message Board

The Serial Console Server supports multiple user logins, which may cause access conflicts. To alleviate the problem, a message board has been provided, which allows users to communicate with each other:



Message Display Panel

Messages that users post to the board are display in this panel.

Compose Panel

Key in the messages that you want to post to the board in this panel. Click **Send** to post the message to the board.

User List Panel

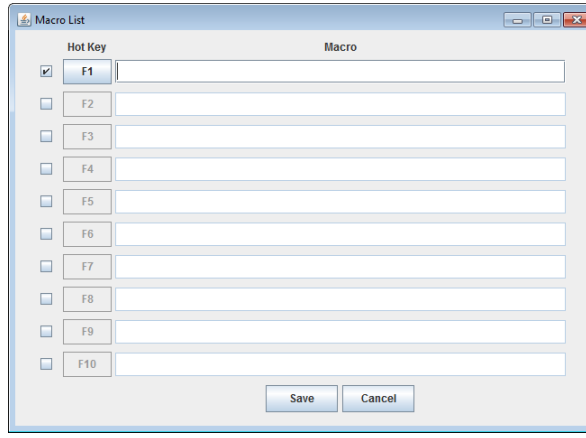
The username and IP address of all the logged in users are listed in this panel.

- If you check **All Users**, messages are posted to all users. To post a message to one individual user, select the user's name before sending your message.
- If a user's name is selected, and you want to post a message to all users, select **All Users** before sending your message.



Macros

Macros allow you to create custom text macros to use within the SNViewer application. When you click the Macros icon the following screen appears:



Simply check a box, type in the text macro and click **Save**. Use the associated function key (F1-F12) to run the custom text macro(s) you created.

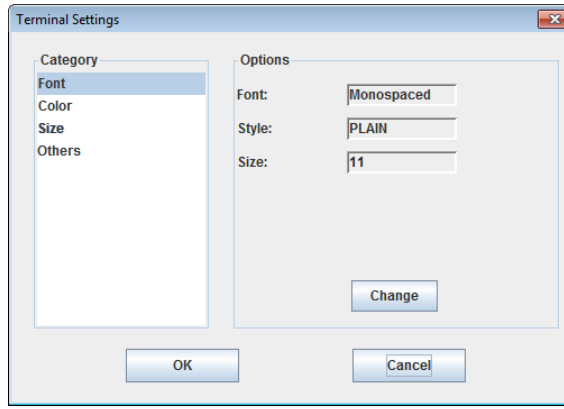
Terminal Application

You can log in remotely using a text based terminal application such as *Telnet*, or *PuTTY*. For information on how to connect and login, see *Remote Login*, page 46 for details.

The *Telnet* and *PuTTY* main menus are the text based equivalent of the browser based configuration and control functions described throughout this manual. You can reference the information provided for the browser version as you work your way through the submenus. Once you login, the following text based menu's appear:

Terminal Settings

The *Terminal Settings* page allows you make changes to the appearance of the terminal window, as described below:



Category	Description
Font	Click **Change** to configure the SNViewer's Font settings. You can change the *Font* type, *Size*, and *Style*. On the right side of the window you can view an example of the font you have set.
Color	Select an **Option:** *Foreground* color, *Background* Color, *Cursor Text* color, or *Cursor Color*, and Click **Change** to adjust the color settings. Use the *HSL*, *Swatches*, and *HSV* tabs to make detailed adjustments and select the colors. Below the tab is a **Preview** section you can use to see how the color change will look. Click **OK** to save the changes; **Cancel** to remove the changes and exit; or **Reset** to revert to the default color settings.
Size	The size of the window may determine the amount of displayed information. You can configure the SNViewer's window size by going to this category and change the *Column size* and *Row size* fields.

Category	Description
Others	Use this section to set: ◆ *Implicit CR in every LF*: Checking this box adds an extra Carriage Return when the [Enter] key is used, so the cursor returns flush on the left margin. Use this function if the text is not lining up on the left margin after you hit [Enter]. ◆ *Backspace is Delete Key* ◆ *Local echo*: An echo is a response from the serial device of character(s) that have been input. ◆ **Auto**: Characters that are typed in are echoed but not displayed on the screen. ◆ **Force On**: Characters that are typed in are echoed and displayed on the screen as they are entered. *Passwords are displayed on the screen if this mode is used.* ◆ **Force Off**: Characters are not echoed from the serial device. ◆ *Buffer Size*: This is the maximum size of the Log file. ◆ *Log File*: The log file generates a log of characters sent from the connected serial device to the SNViewer. The log must first be created as a text file using an external editor such as Note or Microsoft Word, then opened here. Next you must turn *Logging on* from the SNViewer Control Panel (see *Control Panel Functions*, page 59).

Terminal Application

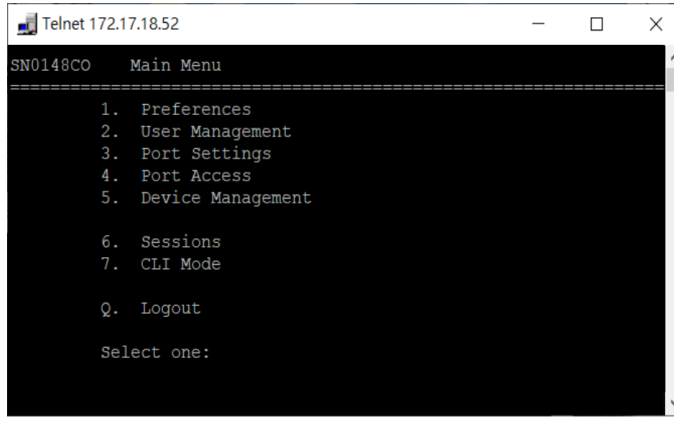
You can log in remotely using a text-based terminal application, such as Telnet, or PuTTY. The Telnet and PuTTY main menus are the text-based equivalent of the browser-based configuration and control functions described throughout this manual.

Note:

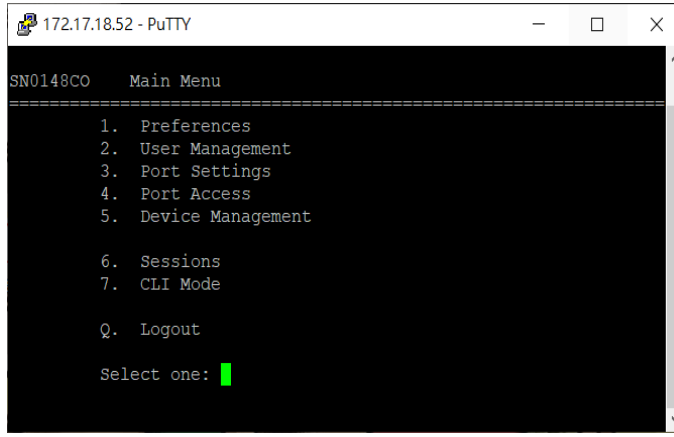
- CLI mode is available only to super administrator accounts.
- For details on logging in to the Serial Consoler Server using a text-based terminal application, see *Remote Login*, page 46.
- For full information on the functions and settings available through the text-based terminal interface, refer to the corresponding sections in this user manual.

Once you log in, the following text-based menus appear:

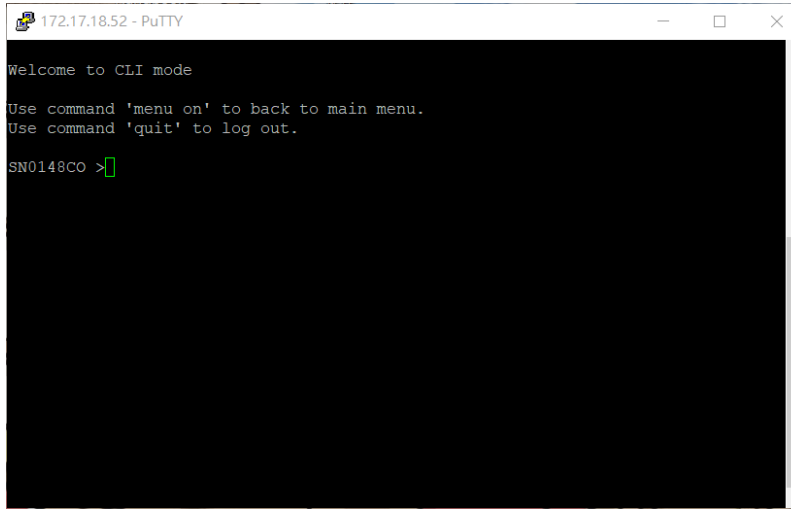
Telnet Menu-Driven Text UI



PuTTY Menu-Driven Text UI



If you prefer to enter text commands to perform specific tasks, you can switch from the menu-driven text UI to the command-line interface (CLI) by selecting option **7. CLI Mode**.

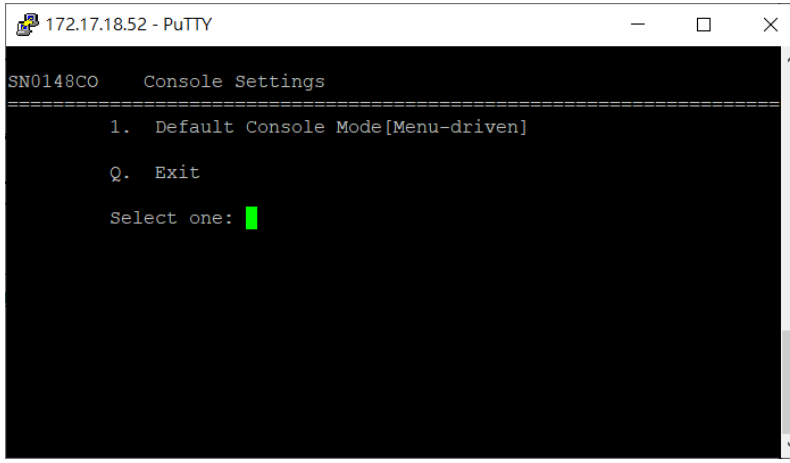


To switch the interface from CLI mode to the menu-driven mode, enter the command "`menu on`".



For more commands for control and configuration, please refer to *CLI Command Set*, page 276.

To set the text based menu or CLI mode to be your default mode, please go to 5. Device Management > 17. Console Settings > 1. Default Console Mode [Menu-driven].



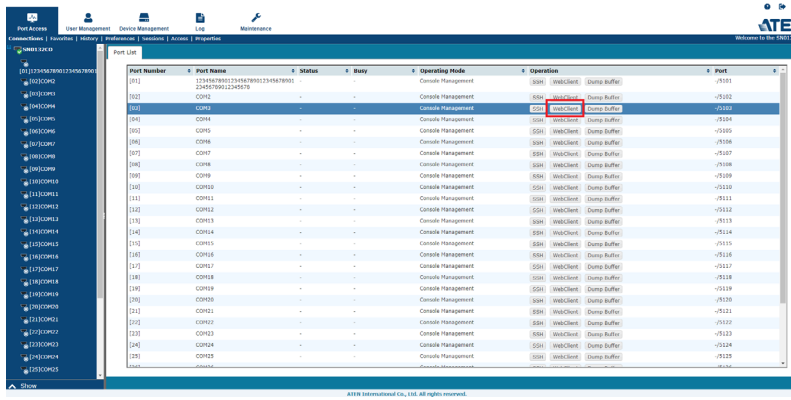
WebClient

To access the WebClient (please refer to the firmware release notes for more information) to manage the Serial Console Server, follow the steps below.

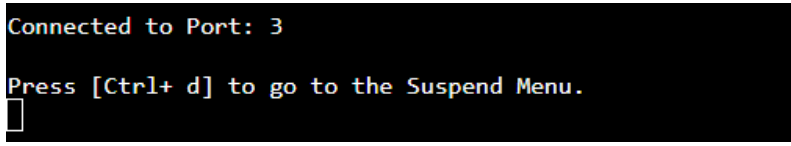
Note: Make sure the port 4500 is open and available for access.



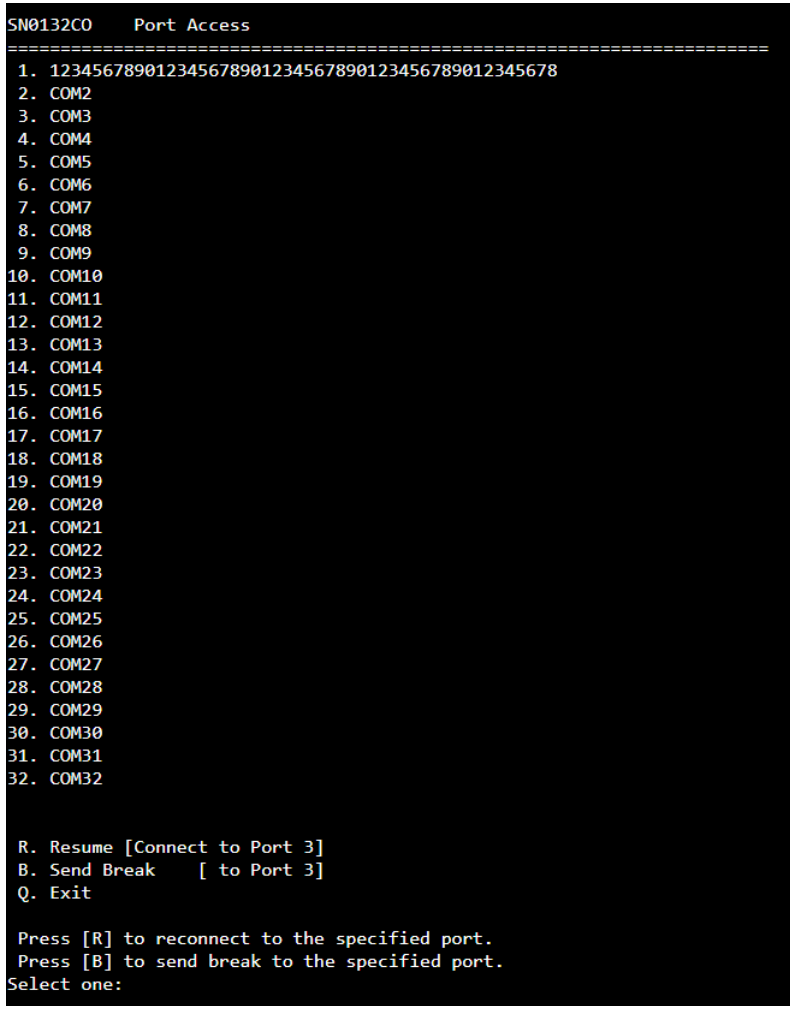
1. Go to *Port Access* - *Connections* page, select a port you want to configure from the *Port List* and click **WebCleint** under *Operation* menu.



2. A pop-up window opens up, press **[Ctrl]** + **[d]** to go to the Suspend Menu.



3. You can select another port for configuration by entering a **port ID** and press **[Enter]**. To go to the configuration page, press **[q]** + **[Enter]**.



4. The Main Menu appears. The main menu is the text based of the browser based configuration and control functions described throughout this manual. For a complete configuration and control functions, we recommend using the browser based web GUI. You can reference the information provided for the browser version as you work your way through the submenus.

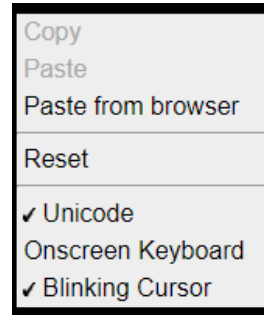
Note: 1. As with the browser version, access to many of these submenus are restricted by the user's permissions. If you select a submenu that you are not authorized for, nothing happens.

2. You can bring up the main menu at any time during your session.

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.

WebClient More Functions

When you are in the WebClient, you can right-click the mouse to bring up more functions.

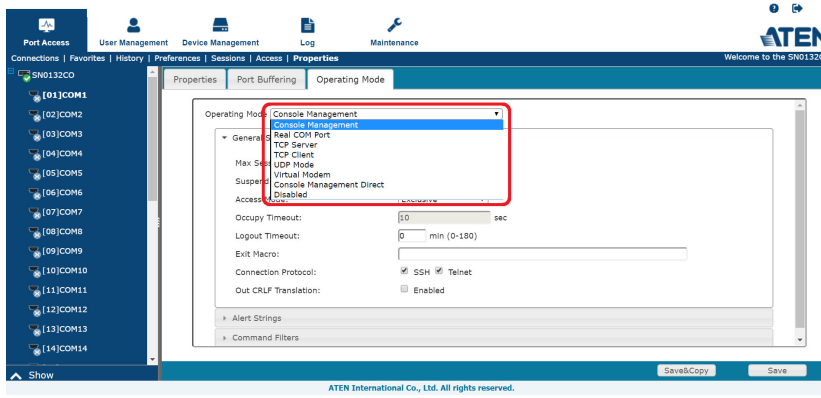


Function	Description
Copy	Copies any highlighted text in the WebClient.
Paste	Pastes any text copied from the WebClient.
Paste from browser	Pastes any copied text that is not copied from the WebClient.
Reset	Resets the current port.
Unicode	Checks if you encounter any garbled text in the WebClient.
Onscreen Keyboard	Checks to bring up an on-screen keyboard.
Blinking Cursor	Checks to enable the blinking cursor.

Chapter 5
Port Operating Modes

Overview

To cover a broad range of serial applications, the Serial Console Server's COM ports support several port operating modes. These include *Console Management* and *Console Management Direct* modes for device control; and *Real COM Port*, *Virtual Modem*, *TCP Server*, *TCP Client*, and *UDP Mode* for Serial-to-Ethernet connectivity and applications that require COM ports, serial tunneling, or where TCP/UDP Socket functionality is needed. An explanation of the functions performed by the various operating modes is provided in the sections that follow.



The **Operating Mode** is selectable from the *Port Access* - *Properties* page, under the *Operation Mode* tab, as shown above. From this page you can set the Port Operating Modes that are discussed in this chapter. See *Operating Mode*, page 98, for further details on configuring all the settings.

Operating Mode

For detailed information about the settings in each of the Operating Modes, see *Operating Mode*, page 98.

Console Management

Console Management mode is the most common Operating Mode used, allowing users to establish Telnet or SSH sessions to the Serial Console Server to manage the serial devices. In this mode users can log in using the web browser's built in SNViewer application via *Telnet* or *SSH*; remotely via Telnet or PuTTY; or directly using the HyperTerminal or SNViewerUSB applications.

For information about configuring *Console Management* settings, see page 98.

Note: Be sure that the *Socket* entry specified on the *Network* page corresponds to the port that the device listens on. 5001 is the Serial Console Server's default setting (see *Network*, page 131, and *Base Socket*, page 132).

Real COM Port

This mode is used in conjunction with a virtual COM port driver installed on the remote user's local computer. When the Serial Console Server's COM port is 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 user'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.

The Serial Console Server comes with Real COM drivers for Windows systems and TTY drivers for Linux systems.

For information about configuring *Real COM Port* settings, see page 98.

TCP Server / TCP Client (Serial Tunnel)

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 Serial Console Server and requests a connection to its serial port.

Once the connection is established, the host receives data from the serial device. From this point on, data can be transmitted between the host and the device in both directions.128-bit/256-bit SSL (TLS v1.0 / TLS v1.1 / TLS v1.2) data encryption is supported in this operating mode.

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

For information about configuring *TCP Server* settings, see page 102.

Note: Be sure that the *Socket* entry specified on the *Network* page corresponds to the port that the device listens on. 5301 is the Serial Console Server's default setting. (see *Network*, page 131, and *Base Socket*, page 132).

TCP Client

In *TCP Client* mode, when serial data comes into the Serial Console Server's serial port, the Serial Console Server initiates contact with the host computer and begins sending serial data to the to the host. The Serial Console Server can send data to up to 16 host computers simultaneously, and supports 128-bit/256-bit SSL (TLS v1.0 / TLS v1.1 / TLS v1.2) data encryption in this operating mode.

For information about configuring *TCP Client* settings, see page 102.

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 Serial Console Server's COM port.

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

For information about configuring *UDP Mode* settings, see page 104.

Virtual Modem

In *Virtual Modem* mode, the Serial Console Server'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 Serial Console Server "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 Serial Console Server's virtual modem function is provided on page 269.

For information about configuring *Virtual Modem* settings, see page 104.

Note: 128-bit/256-bit SSL (TLS v1.0 / TLS v1.1 / TLS v1.2) data encryption is supported in this operating mode.

Console Management Direct

In this mode, users establish a Telnet or SSH session directly from a PC to a server or serial device connected to a port. There is no need to log in to the Serial Console Server via web browser to establish the connection. Users can log in to a serial device using Telnet, SSH or PuTTY directly from a PC. For Telnet session, user can login to a server or serial device despite the user role and permission that is set to.

For information about configuring *Console Management Direct* settings, see page 105.

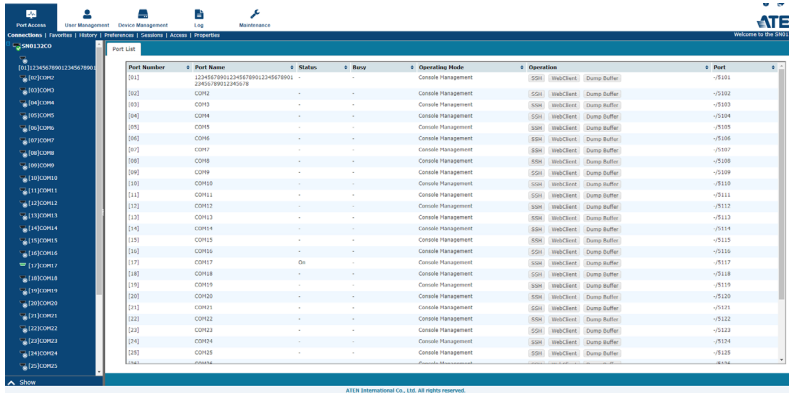
Disabled

In this mode, the serial port on the Serial Console Server is disabled.

Chapter 6
Port Access

Overview

Once you have logged in from a web browser, the Main Screen appears with the *Port Access - Connections* page displayed:

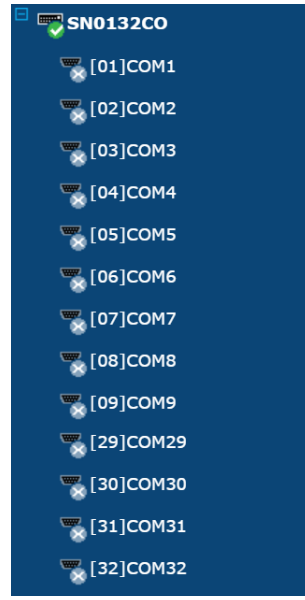


The *Connections* page is organized into several main areas. All the devices, ports, and outlets that a user is permitted to access are listed in the sidebar at the left of the page.

After selecting a port in the sidebar, clicking entries on the menu bar opens information and configuration pages related to the item selected in the sidebar.

The Sidebar

All connected Serial Console Servers, port devices, Cisco Catalyst 2960-C series (please refer to the product page for up-to-date supported network switches.) via its USB console port (please refer to the firmware release notes for more information), and PDU devices – including their ports and outlets – are listed in a tree structure in the sidebar at the left of the screen:



The Sidebar Tree Structure

The characteristics of the sidebar tree structure are:

- Users are only allowed to see the devices and ports that they have access permission for.
- Ports become green to show that the serial device is online.

- Ports become green and a green tick is shown when they are accessed by a user.

- Ports and child devices can be nested under their parent devices. Click the + in front of a device to expand the tree and see the ports nested underneath it. Click the - to collapse the tree and hide the nested ports.

Filter

A “Show” is displayed on the bottom-left hand corner of the page. It is a filter function that allows you to control the number and type of ports that display in the sidebar. When you click “Show”, the bottom of the panel changes to look similar to the image below:

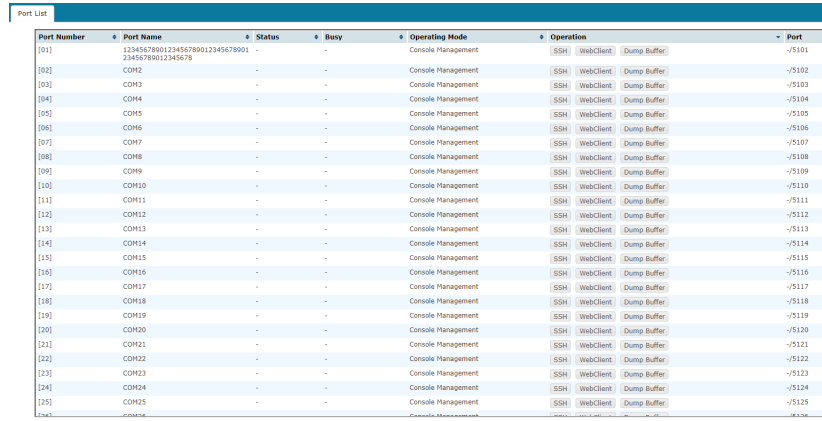


The meanings of the choices are explained in the following table:

Choices	Explanation
Search	If you key in a search string and click **Search**, only port names that match the search string display in the tree. Wildcards (? for single characters; * for multiple characters) and the keyword **or** are supported, so that more than one port can show up in the list. For example: 1. If you key in **Web***, both Web Server 1 and Web Server 2 show up in the list. 2. If you key in **W*1 or M*2**, both Web Server 1 and Mail Server 2 show up in the list.

Connections

The main panel on the *Connections* page displays the *Port List.* From here you can select and connect to the serial devices via the port they are connected to.

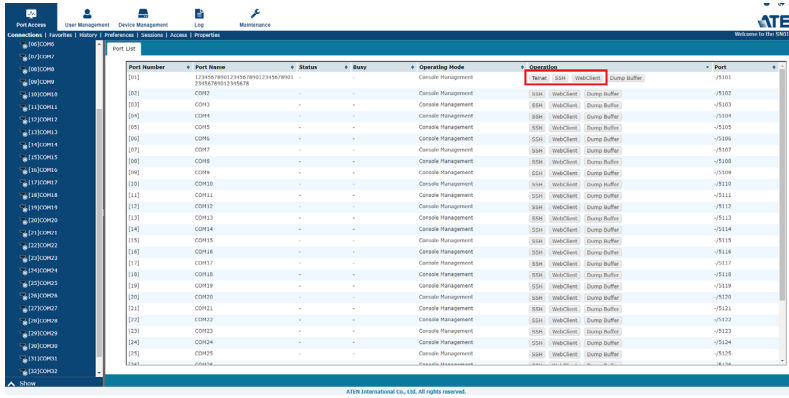


Heading	Description
Port Number	This column represents the physical port that the device is connected to on the rear of the Serial Console Server.
Port Name	This column shows the port name which can be changed from the *Port Access - Properties* page (See page 94 for details). A maximum of 48 characters is allowed including special characters !#*{}%@&,.$.
Status	This column shows the **On** or **Off** status of a device connected to the port. If no device is connected to the port a "**-**" will appear.
Busy	This column will show **Busy** when the port is being accessed by a user through the Serial Console Server.
Operation Mode	This column lists the **Work Mode** that the port is set to for access. The most common setting is *Console Management,* which is set on the *Port Access - Properties* page, under the *Operation Mode* tab (See *Operating Mode*, page 98 for details). **Note:** Console Management is the means of accessing a serial device for operations on it.

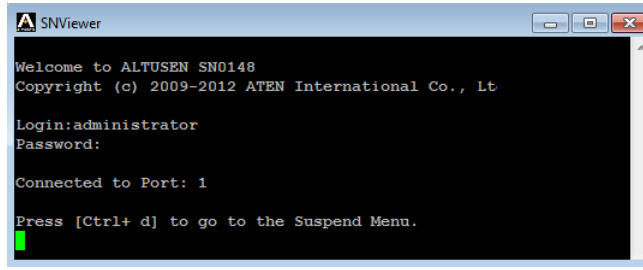
Heading	Description
Operation	Lists Console Management access methods: **Telnet** and **SSH** for managing a port device. Clicking either one opens the SNViewer application to manage that serial device (See *Telnet/SSH/ WebClient*, page 79, below). **Dump Buffer**: This button allows you to dump and view the buffer log of activity conducted on the device. Click to save the log. (See *Save & Copy*, page 96 for details).
Port	Shows the respective Telnet and SSH Port number configured for access to the serial device (See *Service Ports*, page 131 for details).

Telnet/SSH/WebClient

To access a serial device connected to the Serial Console Server, click the port's **Telnet**, **SSH** or **WebClient** (see *WebClient*, page 68) button from the *Port Access - Connections* page:



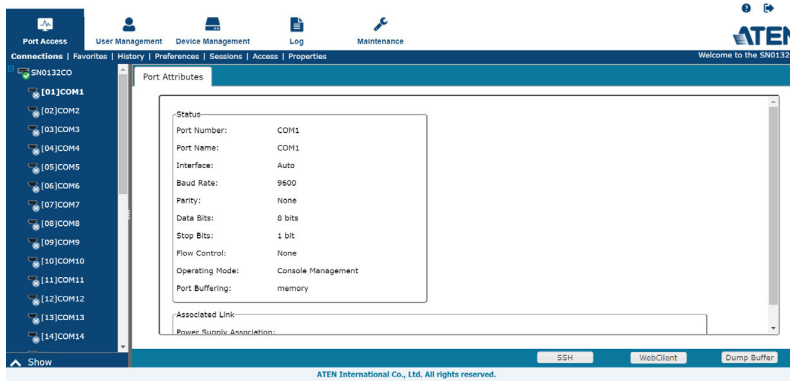
The Serial Console Server opens *SNViewer* to start your session with the serial device, and a screen similar to the one below appears:



From the *SNViewer* can you login and perform management activities on the serial device. For more information on using the SNViewer, see *SNViewer*, page 58 for details.

Port Attributes

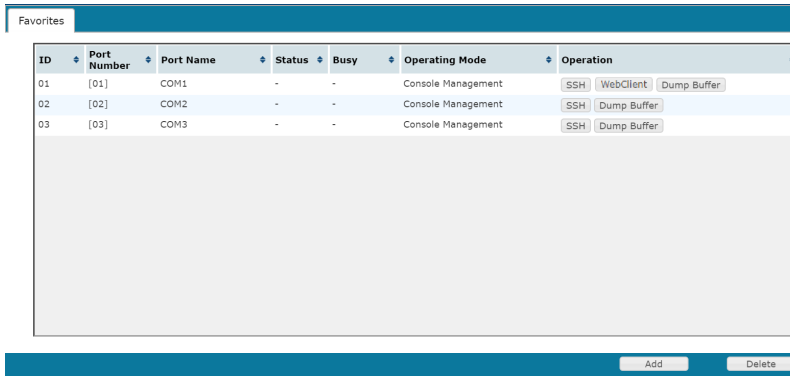
Clicking a device on the sidebar from the *Port Access - Connections* page brings up the **Port Attributes** page with detailed information about the device and Power Over the Net™ reboot options, as shown here:



From here you can use the **Telnet**, **SSH**, and **Dump Buffer** buttons at the bottom of the page.

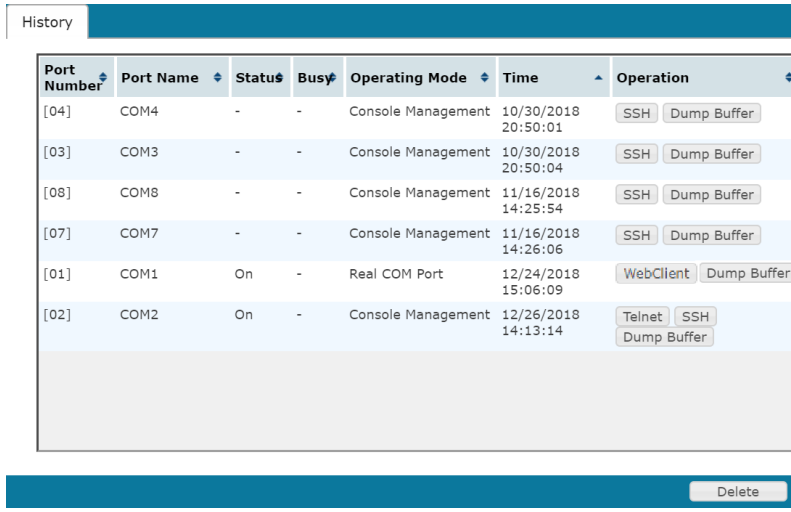
Favorites

The *Favorites* tab allows you to keep all the connections that you access most frequently in one convenient place. To add a port to Favorites, right-click on it from the sidebar and select **Add to Favorites,** or select a port and click **Add**. The layout and functions available on the Favorites tab are exactly the same as those found on the Port List tab (See *Connections*, page 78 for details).



History

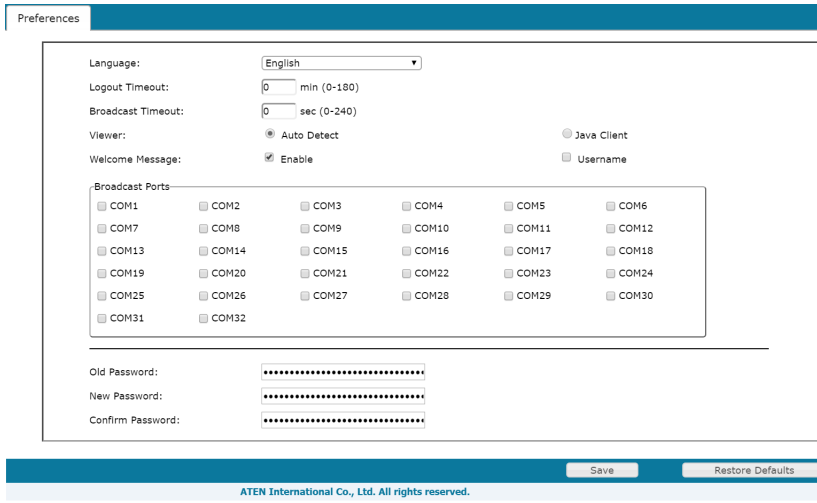
The History page provides a record of each time that a port was accessed. It provides quick access to the most recently used ports. You can access a port shown in the main panel by clicking it's **Telnet**, SSH, or **WebClient** button.



- If there are more entries than there is room on the screen, a scroll bar appears to let you scroll up and down to see the entire record.
- To clear the record, click the *Delete* button at the bottom right of the page.
- You can change the sort order by clicking the column headings.

Preferences

The *Preferences* page allows users to set up their own, individual, working environments. The Serial Console Server stores a separate configuration record for each user profile, and sets up the working configuration according to the *Username* that was keyed into the Login dialog box:



The page settings are explained in the following table:

Setting	Function
Language	Select the language that the web GUI uses.
Logout Timeout	If there is no user input for the amount of time set with this function, the user is automatically logged out. Once logged out, a login is necessary before the Serial Console Server can be accessed again.
Broadcast Timeout	If there is no user input for the amount of time set here, the Broadcast function is automatically ended. Key in a value from 0 to 240 seconds. A setting of 0 (zero) has the same effect as disabling the function. For more information on the Broadcast function, see *Broadcast Ports* within this table.

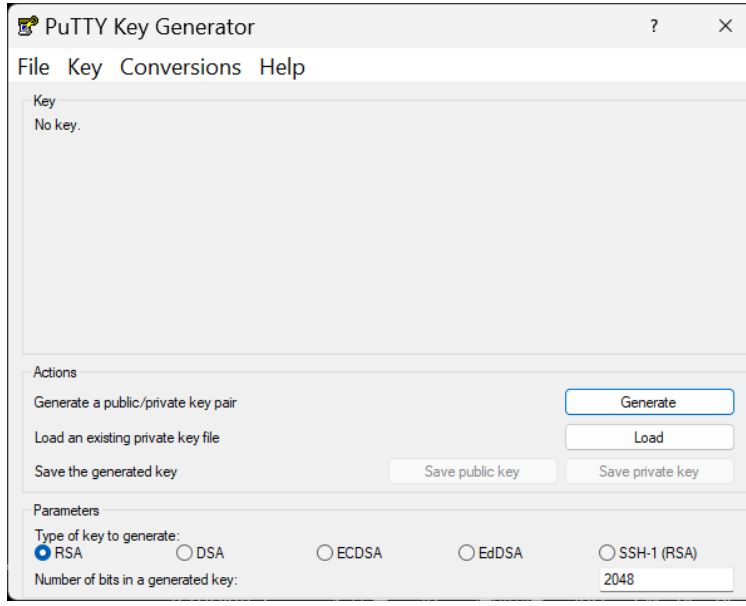
Setting	Function
Viewer	You can choose which viewer is used when accessing a serial device: ◆ **Auto Detect** will select the appropriate viewer based on the web browser used; WinClient for Windows Internet Explorer, Java Client for other web browsers (ex. Firefox). ◆ **Java Client** will open the Java based viewer regardless of the web browser being used.
Welcome Message	You can choose to hide or show the *Welcome Message* and/or *User Name* displayed in the submenu bar. The default is disabled.
Broadcast Ports	Select the ports to receive broadcast commands by selecting the boxes. Selecting Broadcast Ports allows you to access and make changes on a single port and the same change will be made across all Broadcast Ports. **Note:** For broadcasting to work, you must access a Broadcast Port using the SNViewer and turn **Broadcast** on from the Control Panel (See *Control Panel Functions*, page 59).
Changing a Password	In the Browser GUI, to change a user's password, key in the old password and new password into their input boxes; key the new password into the *Confirm* input box, then click **Change Password** to apply the change.
SSH Passwordless Login	This is a key-based authentication that allows the administrator to log in to the management console of a Serial Console Server without needing to enter a password each time. For a detailed setup procedure, see *SSH Passwordless Login*, page 86.

SSH Passwordless Login

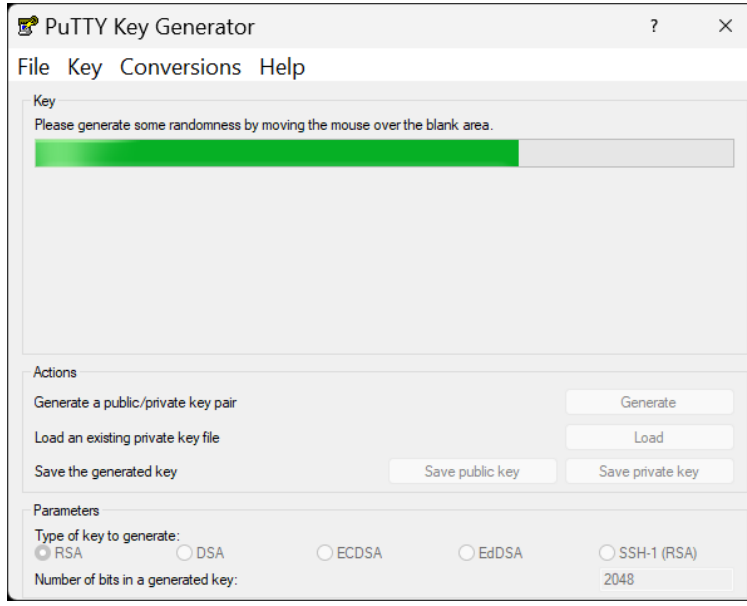
This is a key-based authentication that allows the user to log in to the Serial Console Server without needing to enter a password each time. The management console verifies identity with an SSH key stored on the access computer and a matching key stored on the management console.

Setting Up SSH Passwordless Login

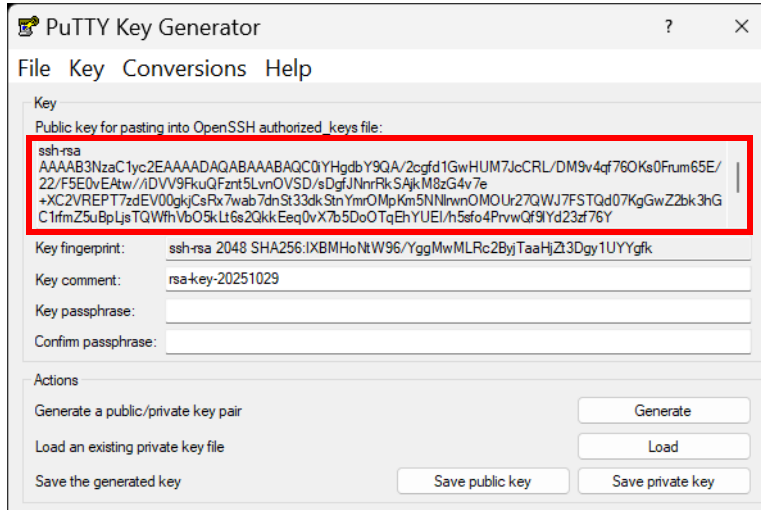
1. Generate an SSH key.
   a) Download and install a key generation utility. In this procedure, PuTTYgen is used for demonstration.
   b) Run PuTTYgen. This window appears.



c) From the Actions section, click **Generate**. A key starts to generate. Move your cursor across the PuTTYgen window a few times (to help randomize the generation) until the key is generated.



d) An OpenSSH public key is generated. Copy and paste this key into a note pad or keep this window open for later setup reference.

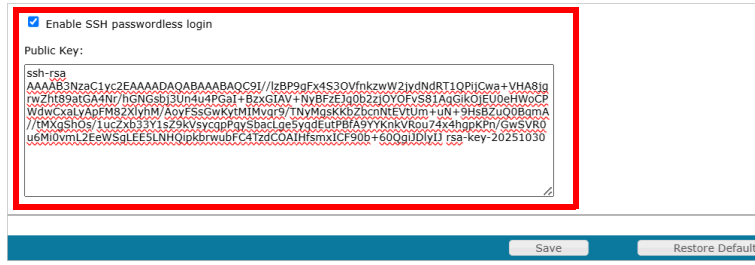


e) To access the Serial Console Server from a Windows-based server, click **Save private key** to save the private key to the local folder.

2. Set up the SSH passwordless login in the Serial Console Server's management console.

   a) From the Serial Console Server's management console, go to **Port Access** > **Preferences**.

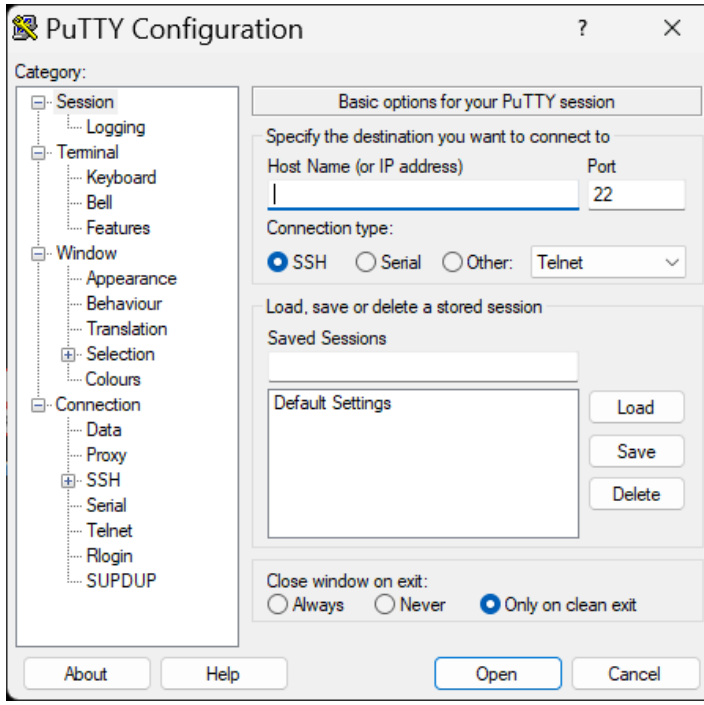
   b) Enable **SSH passwordless login**, and then copy and paste the generated public key into the indicated field.



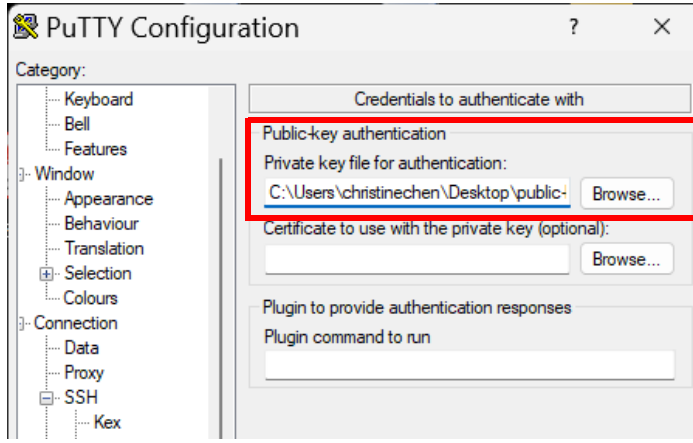
   c) Click **Save**.

Accessing the Serial Console Server's Management Console

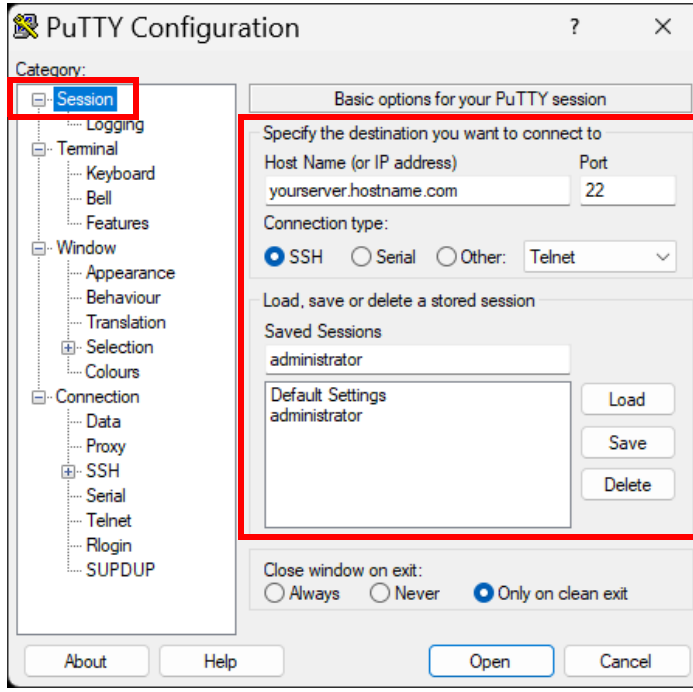
1. On the computer that you use to access the Serial Console Server's management console, run PuTTY.



2. From the **Category** tree, click **Connection** > **SSH** > **Auth** > **Credentials**, browse for the saved private key.



3. Click **Session** and configure the following settings.
   - **Host Name:** Type in the host name or the host's IP address.
   - **Port:** 22
   - **Connection type:** SSH
   - **Saved Sessions:** Create a name for the session and lick **Save**.



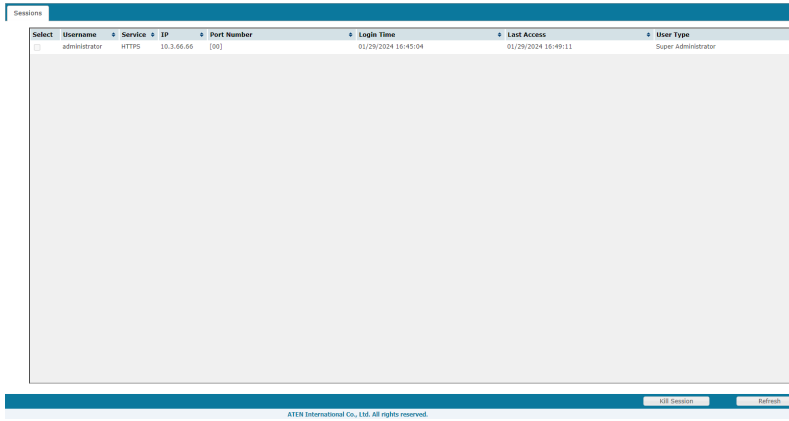
4. Click **Open** to start a connection session.
5. After entering a username, you will be logged in immediately.

Note: For the first login, you will be prompted to verify the fingerprint. This ensures that the server's public key is legitimate and not being spoofed by an attacker. For example, visit the following web page for detailed information: https://help.dreamhost.com/hc/en-us/articles/360004634231--The-authenticity-of-host-can-t-be-established-warning

---

Sessions

The *Session* page lets the administrator and users with User Management permissions see at a glance which users are currently logged into the Serial Console Server, and provides information about each of their sessions.



Note: 1. The Session page is not available for ordinary users.

2. Users with User Management permissions can only see the sessions of ordinary users.

3. The sort order of the information displayed can be changed by clicking the column headings.

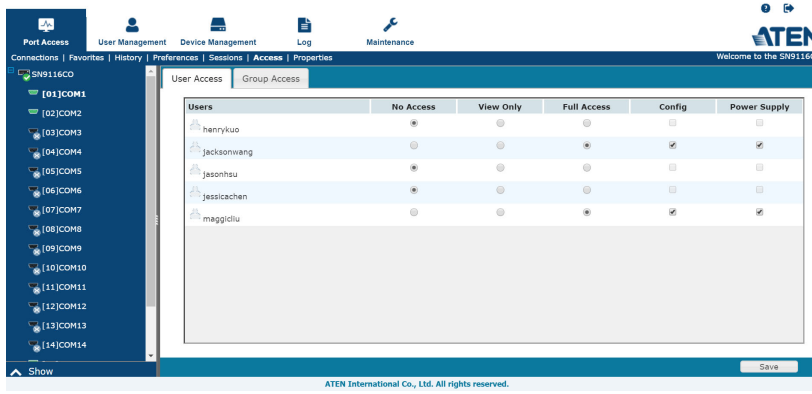
The meanings of the headings at the top of the page are fairly straightforward.

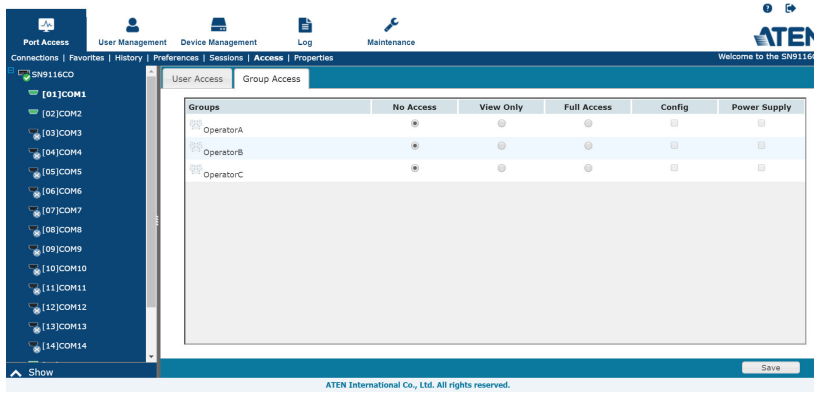
Heading	Description
Username	Refers to the user that logged in.
Service	Displays the type of session (HTTP, HTTPS) established to log in.
IP	Refers to the IP address that the user has logged in from.
Login Time	Indicates the date and time the user logged in.
Last Access	Indicates when the user last accessed the system for use.
User Type	Lists the type of user who has logged in: SA (Super Administrator), Administrator (Administrator), or Normal user (User).

This page also gives the administrator the option of forcing a user logout by checking the **Select** box for the user and clicking **Kill Session** at the bottom of the main panel.

Access

Administrators use the *Access* page to set user and group access and configuration rights for Serial Console Server ports and PDU devices. The Access page only appears for those users with User Management permissions and is not available for other users. Access rights can be set on a user-by-user or a group-by-group basis. See *User Management*, page 107, to setup groups and users.





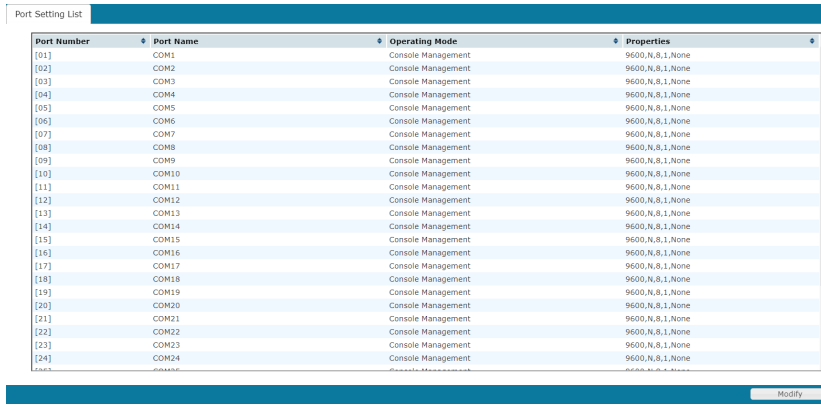
Use the radio buttons to configure access rights on the *User Access* and *Group Access* page. The meaning of the columns are given in the table, below:

User Access	Each user created on the Serial Console Server (excluding Super Administrator accounts) is listed to set access and configuration rights for each device listed on the sidebar. Select a device from the sidebar to set the access and configuration rights of each user.

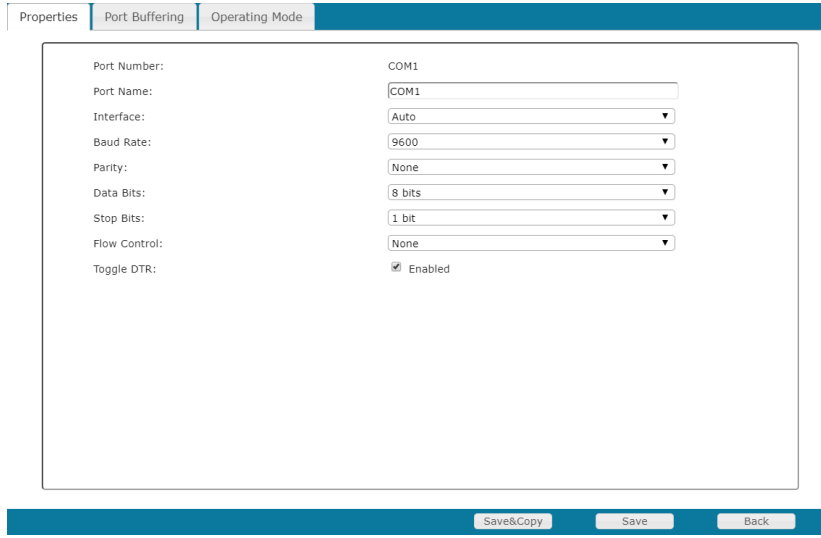
Group Access	Each group created on the Serial Console Server is listed to set access and configuration rights for each device listed on the sidebar. Select a device from the sidebar to set the access and configuration rights of each group.	
Access Rights	The Access columns are where access rights are set. The meaning of each is explained below.	
	Full Access	The user can view the device and can perform operations on the device.
	View Only	The user can only view the device; he cannot perform any operations on it.
	No Access	The device will not show up on the User's list on the Main Screen.
Config	Sets or denies permission for the user to make changes to a port's configuration settings. A check mark (√) indicates that the user has permission; an empty box means that the user does not have permission.	
Power Supply	This column permits/restricts the configuration and power operation of ports that have Power Over the Net™ devices connected to them. A check mark (√) indicates that the user has permission; an empty box means that the user does not have permission.	

Properties

When you click the Properties tab, the *Port Settings List* page appears:



When a port is double clicked from the *Port Settings List* or from the *Sidebar*, the **Properties** page appears and looks similar to the one below:

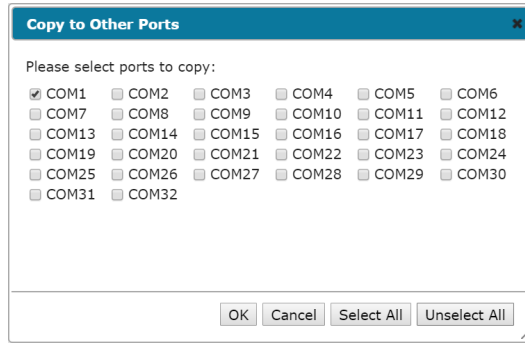


This panel allows you to make configuration settings for the selected port, as explained in the table below:

Setting	Meaning
Port ID	Each port on the Serial Console Server has a port ID number. The value in this field indicates the port that is being configured.
Port Name	You can give a port an appropriate name by editing the *Port Name* field.
Interface	Choose between **Auto** (default), **DTE** or **DCE**.
Baud Rate	This sets the port's data transfer speed. Choices are from 300 to 230400 (drop down the list to see all options). Set this to match the baud rate setting of the connected device. Default is 9600 (which is a default 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 a default setting for many serial devices).
Parity	This bit checks the integrity of the transmitted data. Choices are: None; Odd; Even. Set this to match the parity setting of the connected device. Default is None (which is a default setting for many 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 a default setting for many 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.
Toggle DTR	Enabling this parameter allows the DTR signal to toggle between enabled and disabled. A check mark (√) enables Toggle DTR.

Save & Copy

At the bottom right side of each Properties page you can click *Save* to save the settings for the selected port, or *Save&Copy* which allows you to copy and save the current port settings for any/all other ports, as shown here:



Simply select the ports you want to save the current setting to and click **OK**.

Port Buffering

Port Buffering creates a log of activity conducted when a port is accessed. You can save the log to memory on the Serial Console Server, or to a USB drive. A USB drive provides more storage space, while the Serial Console Server is limited to it's internal memory.

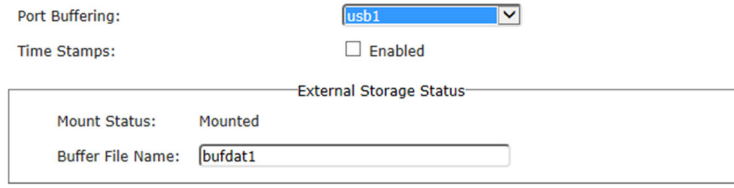
Note: USB drive is only supported on SN1100 CO / SN1100 COD / SN0100CO / SN0100COD models.

To enable Port Buffering, from the drop-down menu: select *Memory*, *NFS, Syslog Server* or select a mounted USB drive. Select *Disable* to disable Port Buffering. Use the check box to enable/disable *Time Stamps*.

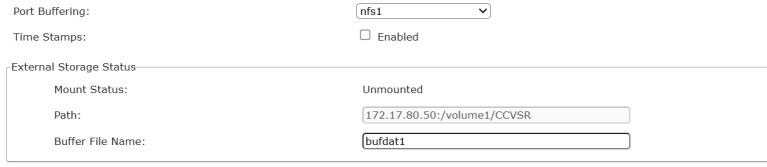


If you selected a mounted USB drive or NFS1, the external storage status information is provided.

- USB device
  - Mount Status – indicates if the USB drive is detected
  - Buffer File Name – optionally type to rename the buffer file



- NFS1
  - Path – indicates the location of the network file system
  - Buffer File Name – optionally type to rename the buffer file.



For more information on Syslog Server, NFS and mounted USB drive, please refer to *Overview* on page 125.

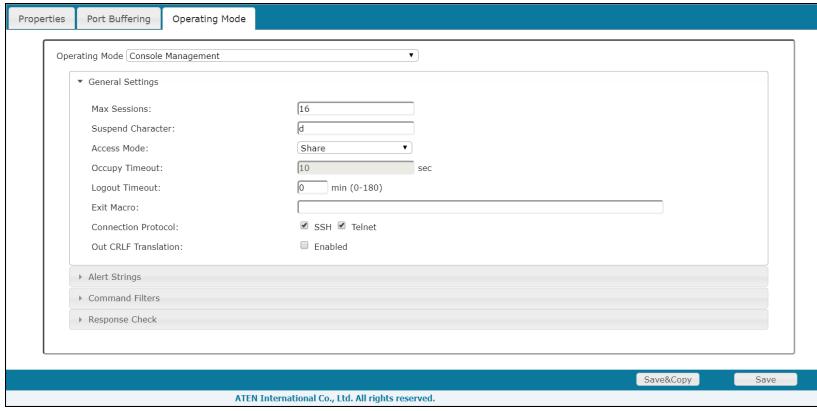
Operating Mode

The *Operating Mode* page allows you to configure settings for access and management of each port. This determines how each serial device is accessed via operating modes. For a detailed explanation of each operating mode, see *Operating Mode*, page 72

Operating Mode – This sets the mode you use to access the port device for management. The most common setting is **Console Management**, which allows for Telnet/SSH sessions from the *Port Access* - *Connections* page. Select the port's work mode from the drop-down menu.

Note: *See Port Operating Modes*, **page 71**, for full details of the different port operating modes that are available from the drop-down list.

Console Management

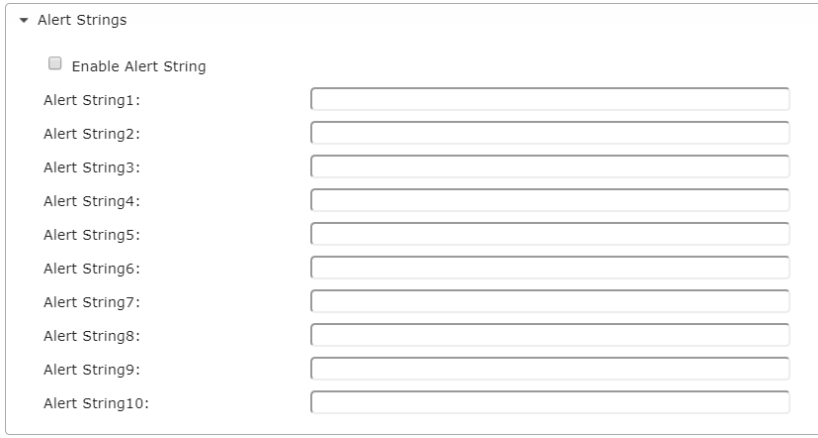


◆ General Settings

Setting	Meaning
Max Sessions	Set the maximum number of concurrent sessions here.
Suspend Character	The Suspend character is used to bring up the Suspend Menu in Telnet sessions**.** Valid characters are A–Z, except H, I, J, and M - which may not be used.
Access Mode	Defines how the port is to be accessed when multiple users have logged on, as follows: **Exclusive**The first user to access the port has exclusive control over the port. No other users can view the port. The *Timeout* function does not apply to ports which have this setting. **Occupy**The first user to access the port has control over the port. However, additional users may view the port. If the user who controls the port is inactive for longer than the time set in the *Timeout* box, port control is transferred to the next user who makes a change on the system. **Share**Users simultaneously share control over the port. Input from the users is placed in a queue and executed chronologically.
Occupy 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.
Logout Timeout	Some applications do not require a user to login and in such a situation the *Occupy Timeout* setting will not work since the timer is set according to the user's operations. In such a case, use the Logout Timeout option. With this feature, if there is no user input for the amount of time set, the user is automatically logged out. Once logged out, a login is necessary before the device can be accessed again.
Exit Macro	Set the Exit Macro here.You can create a macro that will execute when exiting the serial device.
Connection Protocol	Use the check boxes to enable/disable SSH and Telnet connection protocols.
CRLF Translation	This allows you to select whether to send a Carriage Return and Line Feed signal (CRLF).

- **Alert Strings**

The Port *Alert Strings* dialog box provides a way for you to be informed about problems that occur on the devices connected to the Serial Console Server's ports.

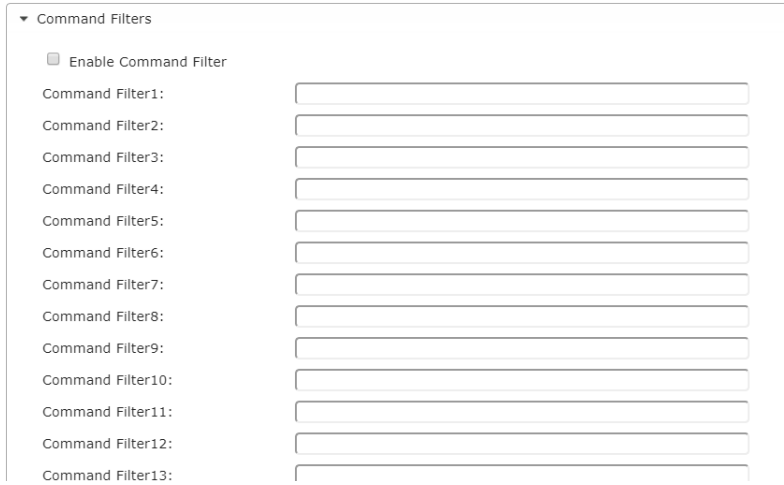


When a device has a problem – such as a critical error that requires a reboot, or an SNMP Trap event has been triggered – debug messages can be sent through its serial port to the Serial Console Server's COM port.

When the Serial Console Server 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.

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

- **Command Filters**



On this page you can specify up to 16 command filters.

- **Response Check**



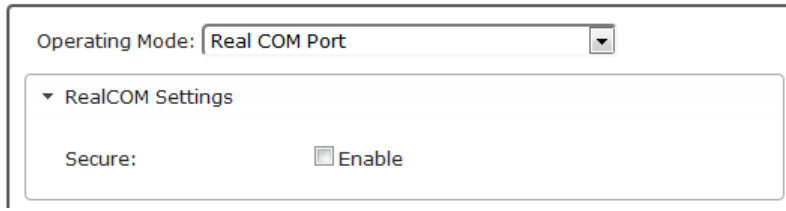
When enabled, this function allows the system to check if the device is responding normally to make sure the system is functioning normally.

Note: This function is only supported under Console Management and Console Management Direct modes.

If the device does not respond, a “Response check failed” notification (if this notification is enabled) will be sent out.

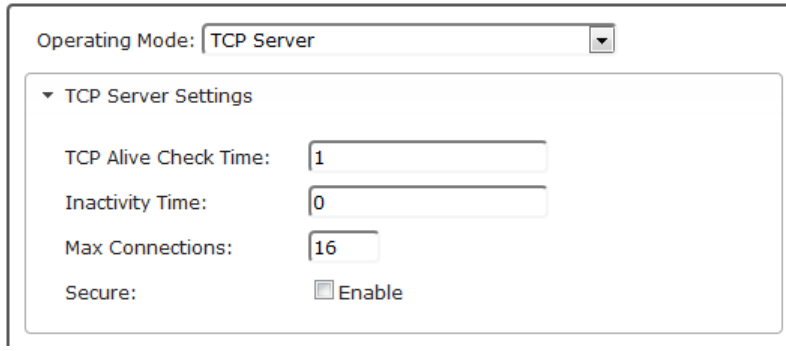
- **Probe string** is the string the system sends for response check. The default is \x0D (\x0D represents [Enter], \x1B represents [ESC]).
- **Query frequency** is how often you send the response check. The default is 30 (in seconds), enter a number between 10-9999.

Real COM Port



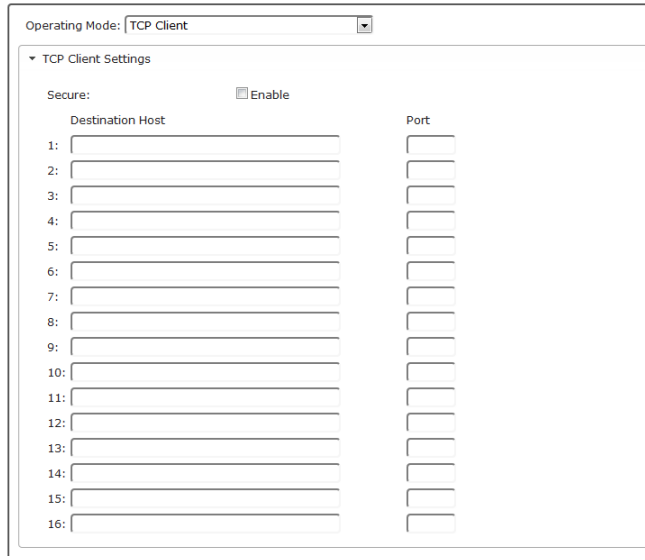
Check **Enable** to encrypt all data being transfered through the session.

TCP Server



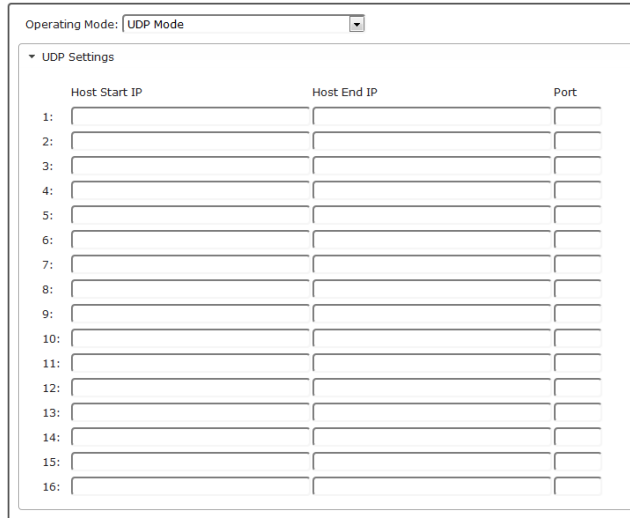
Setting	Meaning
TCP Alive Check Time	This setting defines how often the Serial Console Server should check the TCP socket connection to the host computer to determine whether it is up, or if it has gone down. Enter the number of minutes the Serial Console Server should wait before checking the TCP connection to the host computer.
Inactivity Time	This setting defines how long to wait when there is no data transfered between the Serial Console Server and host computer before the connection drops. Enter the number of minutes that can pass before the Serial Console Server drops the connection.
Max Connections	Enter the maximum number of concurrent connections allowed. The Serial Console Server can establish up to 16 connections simultaneously.
Secure	Check **Enable** to encrypt all data being transfered through the session.

TCP Client



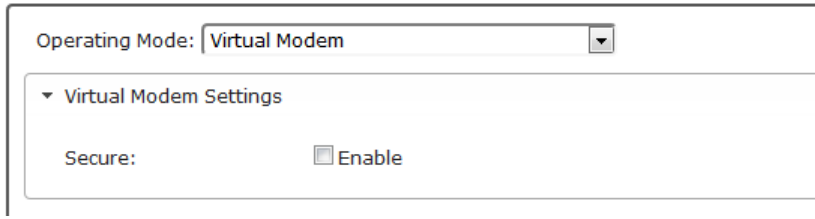
Setting	Meaning
Secure	Check **Enable** to encrypt all data being transfered through the session.
Destination Host / Port	Key-in the IP address and service port of Destination Host or another Serial Console Server (TCP Server) to create a serial tunnel for transmitting the data by between. The Serial Console Server can send data to up to 16 host computers simultaneously.

UDP Mode



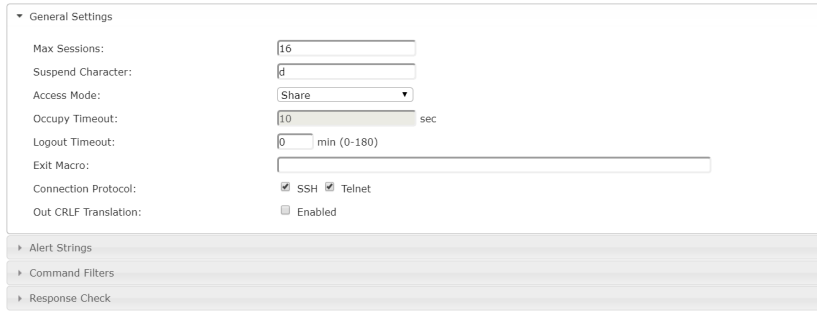
Setting	Meaning
Host Start IP / Host End IP and Port	Use this setting to establish connections via the UDP protocol. Enter a single or range of IP addresses and the TCP/IP port number.

Virtual Modem



Check **Enable** to encrypt all data being transfered through the session.

Console Management Direct



◆ General Settings

Setting	Meaning
Max Sessions	Set the maximum number of concurrent sessions here.
Suspend Character	The Suspend character is used to bring up the Suspend Menu in Telnet sessions**.** Valid characters are A–Z, except H, I, J, and M - which may not be used.
Access Mode	Defines how the port is to be accessed when multiple users have logged on, as follows: **Exclusive:** The first user to access the port has exclusive control over the port. No other users can view the port. The *Timeout* function does not apply to ports which have this setting. **Occupy:** The first user to access the port has control over the port. However, additional users may view the port. If the user who controls the port is inactive for longer than the time set in the *Timeout* box, port control is transferred to the next user who makes a change on the system. **Share:** Users simultaneously share control over the port. Input from the users is placed in a queue and executed chronologically.
Occupy 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.
Logout Timeout	Some applications do not require a user to login and in such a situation the *Occupy Timeout* setting will not work since the timer is set according to the user's operations. In such a case, use the Logout Timeout option. With this feature, if there is no user input for the amount of time set, the user is automatically logged out. Once logged out, a login is necessary before the device can be accessed again.
Exit Macro	Set the Exit Macro here.You can create a macro that will execute when exiting the serial device.
Connection Protocol	Use the check boxes to enable/disable SSH and Telnet connection protocols.
CRLF Translation	This allows you to select whether to send a Carriage Return and Line Feed signal (CRLF).

For information regarding the *Alert Strings*, *Command Filters* and *Response Check*, see page 100.

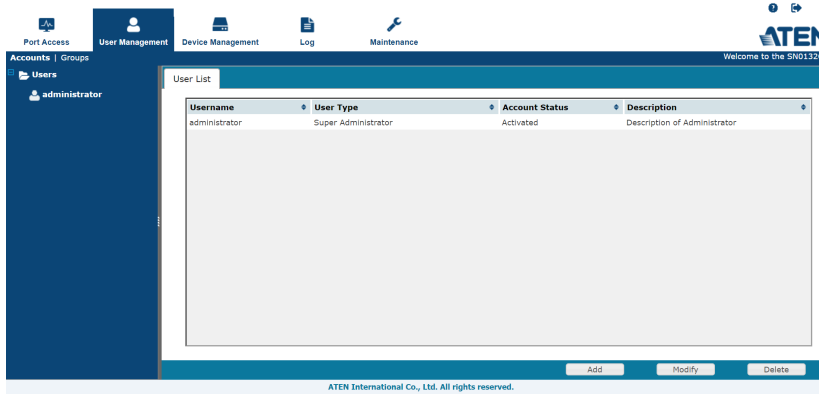
Disabled

Select this option to disable use of the serial port on the Serial Console Server.

Chapter 7
User Management

Overview

When you select the *User Management* tab, the *Accounts* page is displayed:



The page is arranged into two parts: an account / group list on the left, and a main panel on the right.

- A list of users and groups are displayed in the list, and the main panel provides the detailed information of each at-a-glance.
  - The browser GUI has separate menu bar entries for Accounts (Users) and Groups. Depending on the menu item selected, either Users or Groups are listed.
- In the browser GUI, the order in which the information is displayed can be changed by clicking on the main panel's column headings.
- The buttons below the main panel are used to manage users and groups, as shown in the sections that follow.

Users

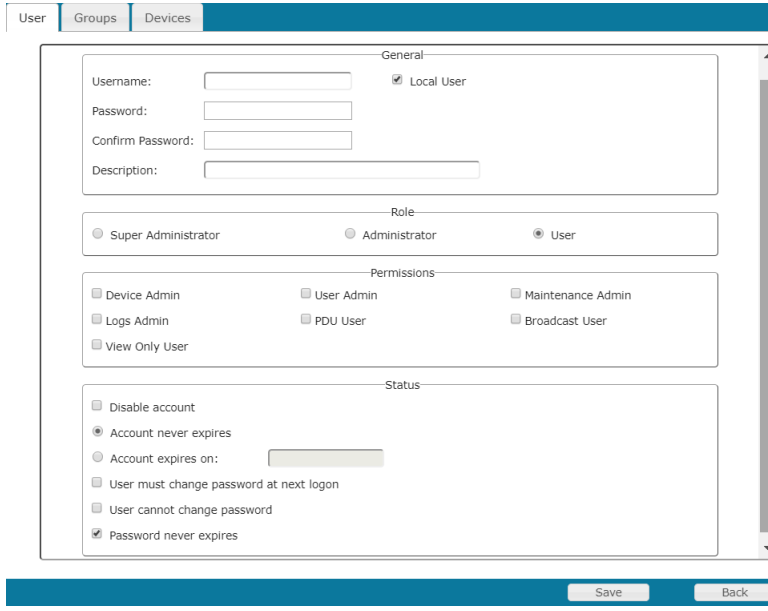
The Serial Console Server supports three user types, as shown in the table, for up to a maximum of 64 users — allowing 64 concurrent logins to access the system:

User Type	Role/Privileges
Super Administrator	◆ Access and manage all ports and devices. ◆ Manage Users and Groups. ◆ Configure the overall installation. ◆ Configure personal working environment. ◆ Access to both the Telnet menu-driver Text UI and CLI mode using terminal applications.
Administrator	◆ Access and manage authorized ports and devices. ◆ Manage Users and Groups. ◆ Configure personal working environment. ◆ Access to the Telnet menu-driver Text UI.
User	◆ Access authorized ports and devices. ◆ Manage authorized ports and devices. ◆ Configure personal working environment. **Note:** Users who have been given permission to do so, may also manage other users. ◆ Access to the Telnet menu-driver Text UI.

Adding Users

To add a user, and assign user permissions, do the following:

1. Select *Users* in the sidebar.
2. Click **Add** at the bottom of the main panel. The User notebook opens, with the *User* tab selected:



3. Enter the required information in the appropriate fields. A description of each of the fields is given in the table below:

Field	Description
Username	From 1 to16 characters are allowed depending on the Account Policy settings. See *Account Policy*, page 164.
Password	From 0 to16 characters are allowed depending on the Account Policy settings. See *Account Policy*, page 164.
Confirm Password	To be sure there is no mistake in the password, you are asked to enter it again. The two entries must match.
Description	Additional information about the user that you may wish to include.

Field	Description
Role	There are three categories: Super Administrator, Administrator and User. There is no limitation on the number of accounts that can be created in each category. ◆ The Super Administrator is responsible for the overall installation configuration and maintenance; user management; and device and port assignments. The Super Administrator's permissions are automatically assigned by the system and cannot be altered. ◆ The Administrators default permissions include everything except *Device Admin* and *User Admin*, but the permissions can be altered for each Administrator by checking or unchecking any of the permissions checkboxes. ◆ The Users default permissions include *PDU User* and *Broadcast User*, but the permissions can be altered for each User by checking or unchecking any of the permissions checkboxes.
Permissions	◆ Enabling *Device Admin* allows a user to configure and control the settings for overall Serial Console Server operations (see *Device Management*, page 125). ◆ Enabling *User Admin* allows a user to create, modify, and delete user and group accounts. ◆ Enabling *Maintenance Admin* allows a user to perform all the Maintenance operations available under the Maintenance tab (see *Maintenance*, page 173). ◆ Enabling *Logs Admin* allows a user to access the system log (see *Log*, page 168). ◆ Enabling *PDU User* allows users to configure Power Over the Net? devices ◆ Enabling *Broadcast User* allows the use of Broadcasting ◆ Enabling *View Only User* limits users to only being able to view the display of connected devices and cannot input any keyboard and mouse signals. Additionally, all port settings features under the *Properties*, *Port Buffering*, and *Operating Mode* sections (see page 94) becomes inaccessible and cannot be configured.

Field	Description
Status	Status allows you to control the user's account and access to the installation, as follows: ◆ *Disable Account* lets you suspend a user's account without actually deleting it, so that it can be easily reinstated in the future. ◆ If you don't want to limit the time scope of the account, select *Account never expires*; if you do want to limit the amount of time that the account remains in effect, select *Account expires on*, and key in the expiration date. ◆ To require a user to change his password at the next logon, select *User must change password at next logon*. This can be used by the administrator to give the user a temporary password to log in for the first time, and then let the user set the password of his choice for future logins. ◆ To make a password permanent, so that the user cannot change it to something else, select *User cannot change password*. ◆ For security purposes, administrators may want users to change their passwords from time to time. ◆ If not, select *Password never expires*. This allows users to keep their current passwords for as long as they like. ◆ If so, select *Password expires after*, and key in the number of days allowed before the password expires. Once the time is up, a new password must be set.

4. At this point you can assign the new user to a group by selecting the *Groups* tab – the Groups page is discussed on page 117. You can also assign the user's port access rights by selecting the *Devices* tab – the Devices page is discussed on page 122.

Note: Optionally, you can skip this step now to add more users and create groups, and come back to it later.

5. When your selections have been made click **Save**.
6. When the *Operation Succeeded* message appears, click **OK**.
7. Click **Users** in the sidebar to return to the main screen. The new user appears in the sidebar list and in the main panel, as well.
   - The sidebar *Users* list can expand and collapse. If the list is expanded, click the minus symbol (–) next to the *Users* icon to collapse it; if it is collapsed there is a plus symbol (+) next to the icon. Click the plus symbol to expand it.
   - The icon for super administrators has two black bands; the icon for administrators has one red band.

- The large main panel shows the user's name; the description that was given when the account was created; and whether the account is currently active or has been disabled.

Modifying User Accounts

To modify a user account, do the following:

1. In the sidebar *User* list, click the user's name

   – or –

   In the main panel, select the user's name

2. Click **Modify**.
3. In the *User* page that comes up, make your changes, then click **Save**.

Note: The *User* page is discussed on page 109; the *Groups* page is discussed on page 117, the *Devices* page is discussed on page 122.

Deleting User Accounts

To delete a user account do the following:

1. In the main panel, select the user's name.
2. Click **Delete**.
3. Click **OK**.

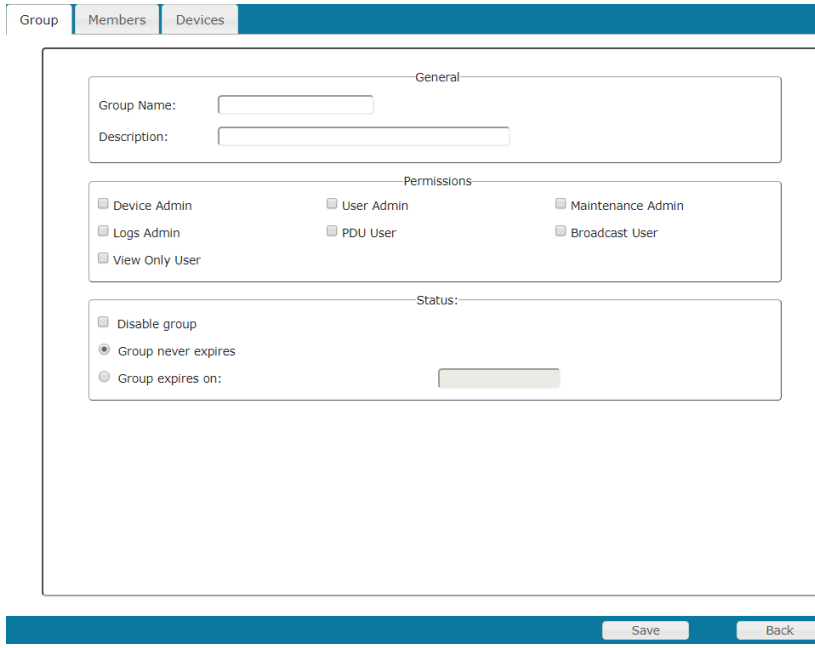
Groups

Groups allow administrators to easily manage users and the associated device access/configuration rights. When device access rights are applied to a group, the same rights are applied to everyone who is a member of that group. Up to 16 groups can be defined for allowing certain users access to specific devices, while restricting others from accessing them.

Creating Groups

To create a group, do the following:

1. Select *Groups* on the menu bar.
2. Click **Add** at the bottom of the main panel. The Group notebook opens, with the *Group* tab selected:



3. Enter the required information in the appropriate fields. A description of each of the fields is given in the table below:

Field	Description
Group Name	A maximum of 16 characters is allowed.
Description	Additional information about the user that you may wish to include. A maximum of 63 characters is allowed.
Permissions	Permissions and restrictions for groups are set by checking the appropriate boxes. These are the same permissions as the ones specified for Users. See *Permissions*, page 110 for details

4. At this point you can assign users to the group by selecting the *Members* tab – the Members page is discussed on page 120. You can also assign the group's port access rights by selecting the *Devices* tab – the Devices page is discussed on page 122.

Note: Optionally, you can skip this step now to add more groups and assign users to them, and come back to it later.

5. When your selections have been made click **Save**.
6. When the *Operation Succeeded* message appears, click **OK**.
7. Click **Group** in the sidebar to return to the main screen. The new group appears in the sidebar group list and in the main panel.
   - The sidebar *Group* list can expand and collapse. If the list is expanded, click the minus symbol (–) next to the *Users* icon to collapse it; if it is collapsed there is a plus symbol (+) next to the icon. Click the plus symbol to expand it.
   - The large main panel shows the group's name, and the description that was given when the group was created

Repeat the above procedure to add additional groups.

Note: You must perform Step 7 before attempting to add a new group, or else the new group you are creating will replace the group you just finished creating.

Modifying Groups

To modify a group, do the following:

1. In the sidebar *Group* list, click the group's name

   – or –

   In the main panel, select the group's name.

2. Click **Modify**.

3. In the *Group* notebook that comes up, make your changes, then click **Save**.

Note: The *Group* page is discussed on page 114; the *Members* page is discussed on page 120, The *Devices* page is discussed on page 122.

Deleting Groups

To delete a group do the following:

1. In the sidebar, click the *Groups* icon.

2. In the main panel, select the group's name.

3. Click **Delete**.

4. Click **OK**.

Users and Groups

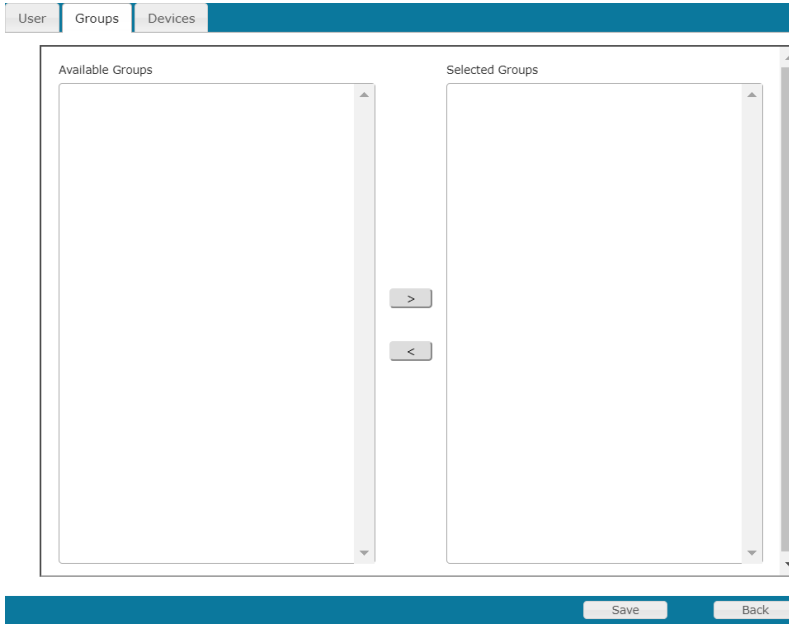
There are two ways to manage users and groups: from the Users notebook; and from the Group notebook.

Note: Before you can assign users to groups, you must first create them. See *Adding Users*, page 109 for details.

Assigning Users to a Group From the User's Notebook

To assign a user to a group from the User's notebook, do the following:

1. In the sidebar *User* list, click the user's name
   – or –
   In the main panel, select the user's name
2. Click **Modify**.
3. In the *User* notebook that comes up, select the *Groups* tab. A screen, similar to the one below, appears:



4. In the *Available* column, select the group that you want the user to be in.
5. Click the **Right Arrow** to put the group's name into the *Selected* column.

6. Repeat the above for any other groups that you want the user to be in.
7. Click **Save** when you are done.

Note: If a user has permissions in addition to the ones assigned to the group, the user keeps those permissions in addition to the group ones.

Removing Users From a Group From the User's Notebook

To remove a user from a group from the User's notebook, do the following:

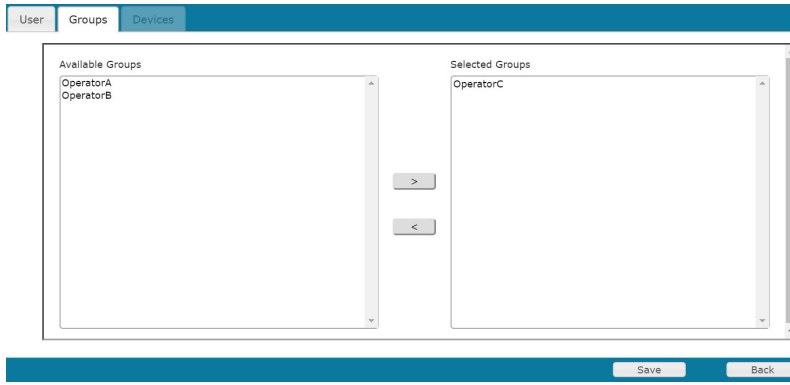
1. In the sidebar *User* list, click the user's name

   – or –

   In the main panel, select the user's name.

2. Click **Modify**.

3. In the *User* notebook that comes up, select the *Groups* tab. A screen, similar to the one below, appears:



4. In the *Selected* column, select the group that you want to remove the user from.

5. Click the **Left Arrow** to remove the group's name from the *Selected* column. (It goes back into the *Available* column.)

6. Repeat the above for any other groups that you want to remove the user from.

7. Click **Save** when you are done.

Assigning Users to a Group From the Group's Notebook

To assign a user to a group from the Group notebook, do the following:

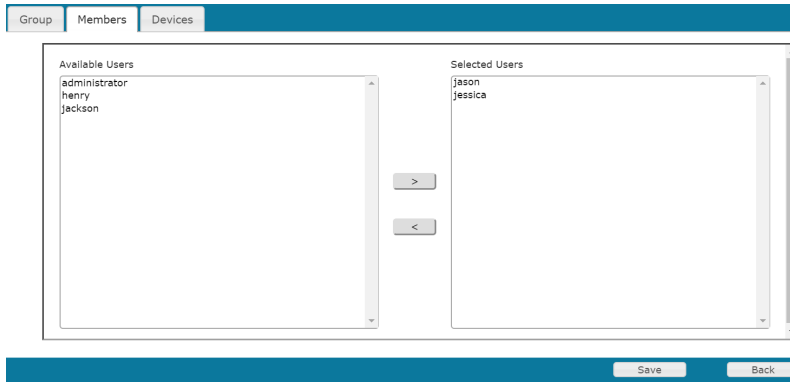
1. In the sidebar *Group* list, click the group's name

   – or –

   In the main panel, select the group's name.

2. Click **Modify**.

3. In the *Group* notebook that comes up, select the *Members* tab. A screen, similar to the one below, appears:



4. In the *Available* column, select the user that you want to be a member of the group.

5. Click the **Right Arrow** to put the user's name into the *Selected* column.

6. Repeat the above for any other users that you want to be members of the group.

7. Click **Save** when you are done.

Note: If a user has permissions in addition to the ones assigned to the group, the user keeps those permissions in addition to the group ones.

Removing Users From a Group From the Group's Notebook

To remove a user from a group from the Group's notebook, do the following:

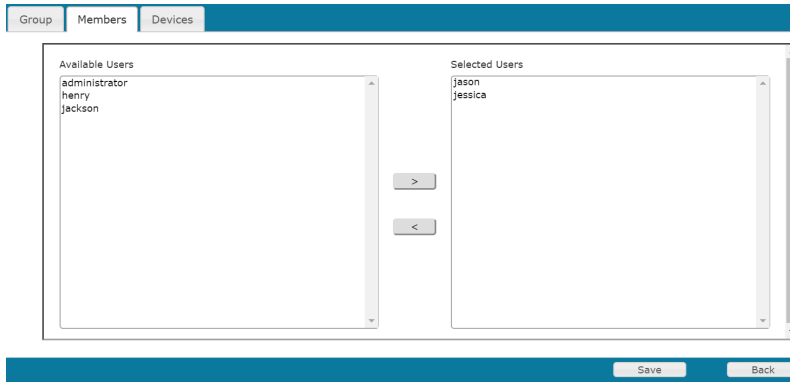
1. In the sidebar *Group* list, click the group's name

   – or –

   In the main panel, select the group's name.

2. Click **Modify**.

3. In the *Group* notebook that comes up, select the *Members* tab. A screen, similar to the one below, appears:



4. In the *Selected* column, select the user that you want to remove from the group.

5. Click the **Left Arrow** to remove the user's name from the *Selected* column. (It goes back into the *Available* column.)

6. Repeat the above for any other users that you want to remove from the group.

7. Click **Save** when you are done.

Device Assignment

When a user logs in to the Serial Console Server, the interface comes up with the Port Access page displayed. All the ports that the user is permitted to access are listed in the sidebar at the left of the page. Access permissions for those ports and the devices connected to them are assigned on a port-by-port basis from the *User* or *Group* list on the sidebar of the User Management page.

Assigning Device Permissions under User Settings

To assign a device permissions to a user from the *User's* notebook, do the following:

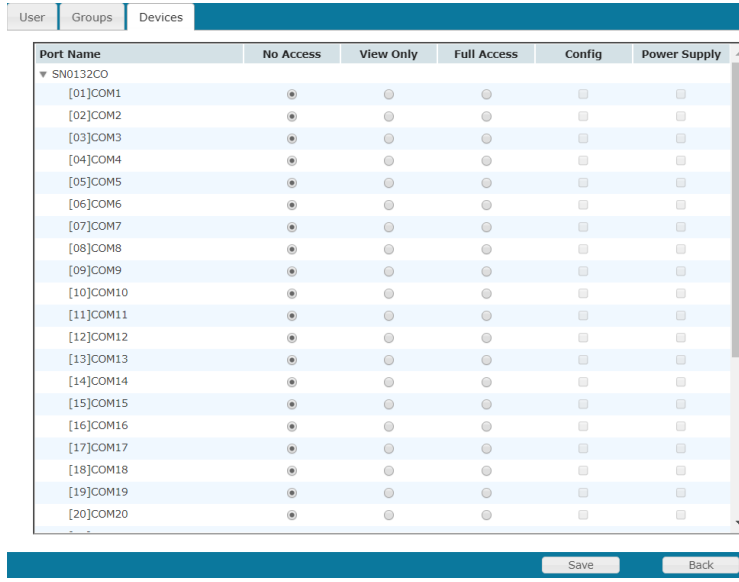
1. In the sidebar *User* list, click the user's name

   – or –

   In the main panel, select the user's name.

2. Click **Modify**.

3. In the *User* notebook that comes up, select the *Devices* tab. A screen, similar to the one below, appears:



4. Make your permission settings for each port according to the information provided below:

<table>
<tr><td>Name:</td><td colspan="2">Each port accessible to the user is listed under the Names column.</td></tr>
<tr><td>Access:</td><td colspan="2">The Access column is where device access rights are set. Click the radio buttons in the rows that corresponds your choices. The meanings are described, below:</td></tr>
<tr><td></td><td>Full Access</td><td>The user can view the remote screen and can perform operations on the remote server from his keyboard.</td></tr>
<tr><td></td><td>View Only</td><td>The user can only view the remote screen; he cannot perform any operations on it.</td></tr>
<tr><td></td><td>No Access</td><td>No access rights - the Port will not show up on the User's list on the Main Screen.</td></tr>
<tr><td></td><td colspan="2">Note:
◆ Local User: The real permission for the local user is a combined result of the configuration that is set under the Devices tab for Accounts and Groups. The priority is as follows: Full Access > View Only > No Access.
◆ Domain User: The real permission for the domain user is a combined result of the configuration that is set under the ANMS, Authentication & Authorization tab (page 148) and Groups, Devices tab. Make sure the identical group name is created in the third-party authentication & authorization server and in the group list (page 114). The priority is as follows: Full Access > View Only > No Access.
◆ When the View Only User is selected under Permissions, User tab (page 108), the priority is as follows: View Only User > Full Access >View Only > No Access.</td></tr>
<tr><td>Config:</td><td colspan="2">The Config column is where a user’s permission to make changes to a port’s configuration settings are permitted/restricted. A check mark (√) indicates that the user has permission to make changes to the port’s configuration settings; an empty box means that the user is denied permission to make configuration changes.</td></tr>
<tr><td>Power Supply:</td><td colspan="2">The Power Supply column permits/restricts the configuration and power operation of ports that have Power Over the Net™ devices connected to them. A check mark (√) indicates that the user has permission; an empty box means that the user does not have permission.
Reserved to be used with PG series PDU.</td></tr>
</table>

5. When you have finished making your choices, click **Save**.
6. In the confirmation popup that appears, click **OK**.

Note: In any of the columns, you can use Shift-Click or Ctrl-Click to select a group of ports to configure. Clicking to cycle through the choices on any one of the selected ports causes all of them to cycle in unison.

Assigning Device Permissions under Group Settings

To assign a device permissions to a group of users, do the following:

1. In the sidebar *Groups* list, click the group's name

   – or –

   In the main panel, select the group's name.

2. Click **Modify**.

3. In the *Groups* notebook that comes up, select the *Devices* tab.

4. The screen that comes up is the same one that appears in the User's notebook. The only difference is that whatever settings you make apply to all members of the group instead of just one individual member.

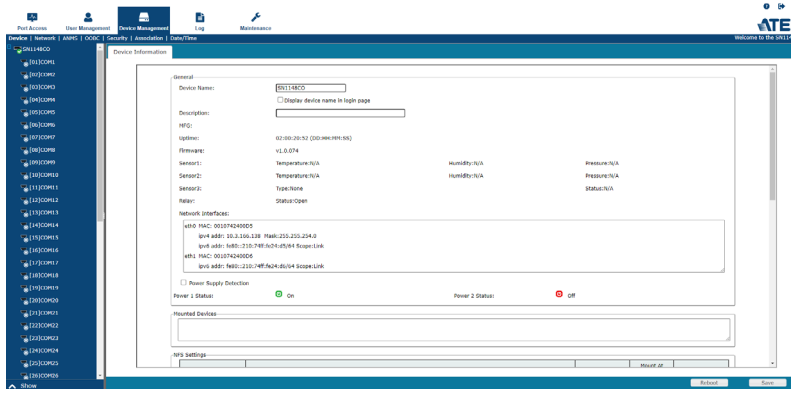
   Make your device assignments according to the information described under *Assigning Device Permissions under User Settings*, page 122.

Chapter 8
Device Management

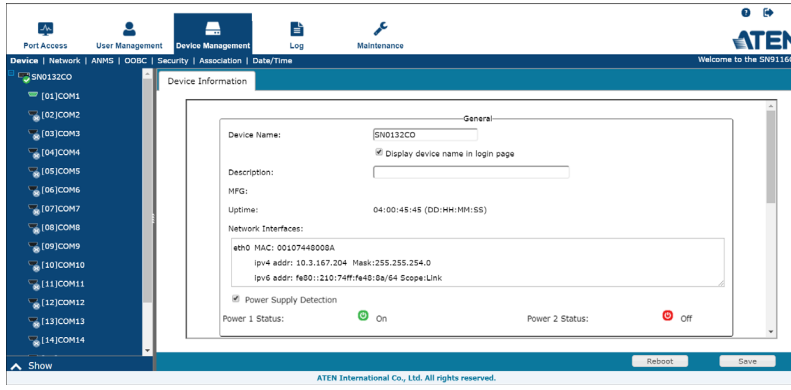
Overview

The Device Management page opens with the top-level Serial Console Server selected in the sidebar, with all its ports nested below, and the *Device Information* page displayed in the main panel:

SN1100CO / SN1100COD



SN0100CO / SN0100COD / SN9100CO



Device Information

General

The *General* section of the Device Information page provides basic information for the selected Serial Console Server, and any attached network interfaces.

- **Device Name:** Indicates the model name of the selected Serial Console Server. Type in the field to rename it.
- **Description:** Optionally add more information here.
- **MFG:** Indicates the manufacturing information of the Serial Console Server.

  Note: The "MFG Number / Product Serial Number" (Manufacturing Number / Product Serial Number) is an internal serial number used by ATEN's factory and technical support staff to identify products. This number does not affect products' warranty. If your product requires after-sales services, you may provide the MFG Number / Product Serial Number to ATEN's sales or technical support staff to identify the product and model number. The MFG Number comes with 11 digit number xxxxxxxxxxx and the Product Serial Number comes with 13 digit number xxxx-xxx-xxxx.

- **Uptime:** Indicates the amount of time the Serial Console Server has been continuously running since the last power-on or reboot.
- **Firmware:** Indicates the firmware version of the Serial Console Server.
- **Sensor:** Indicates the detected values of any installed sensors.
- **Relay:** Indicates the relay status of the Serial Console Server.

  Network interfaces: Indicates the MAC address and IP address of the network interface card or USB Mobile/WiFi dongle for the selected Serial Console Server.

Check the function **Display device name in login page** to have the device name displayed below the area where you enter the login credentials. An example is shown:



- **Power Supply Detection (for SN01XX series & SN11XX series):** This setting is enabled by default. When this setting is enabled and one of the power is off, the administrator is alerted with a confirmation message on the local console and a beep sound from the device. If the intention is to only have one source of power, there are two ways to stop the beeping:

  1) Confirm the intention in the dialog box. Do this if you only want to disable the warning temporarily. With this method, the warning function will be back in effect after the next system reset.

  2) Disable the Power Supply Detection setting. Do this if you want to disable this function on a permanent basis.

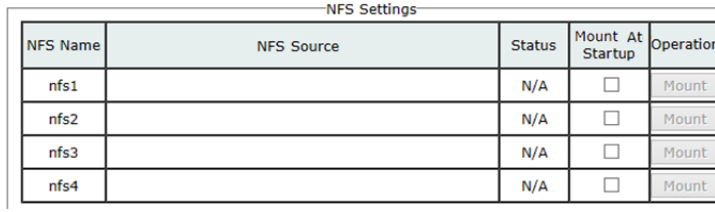
- **Power status:** Indicates power status (on or off) of the Serial Console Server.

Mounted Devices

The *Mounted Devices* section displays information about USB and NFS storage devices connected for use. When a USB drive is plugged into the front of the Serial Console Server (SN1100CO / SN1100COD / SN0100CO / SN0100COD only), or NFS storage locations are set (see *NFS Settings*, page 128), they appear here with detailed information about the mounted device, as shown below.



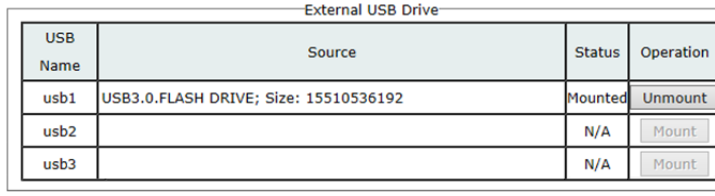
NFS Settings


NFS Settings

NFS Name	NFS Source	Status	Mount At Startup	Operation
nfs1		N/A	☐	Mount
nfs2		N/A	☐	Mount
nfs3		N/A	☐	Mount
nfs4		N/A	☐	Mount

NFS (Network File System) allows you to mount storage devices across the network. You can mount up to 4 devices. Fill in the **Source** with the storage devices network location (IP Address or Network Name) including the full path of the location you want to mount. Next, click **Mount** to mount the NFS storage device. The **Status** column indicates *N/A*, *Mounted*, or *Unmounted*. *Unmounted* shows if the storage device is not accessible. If this happens make sure the device is accessible on the network, and check that the *Source* information you typed in is correct. Check **Mount At Startup** to automatically mount the NFS storage devices once when the system starts up.

External USB Drives

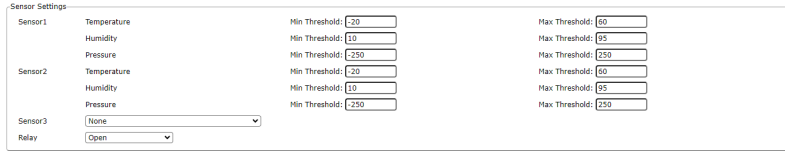

External USB Drive

USB Name	Source	Status	Operation
usb1	USB3.0.FLASH DRIVE; Size: 15510536192	Mounted	Unmount
usb2		N/A	Mount
usb3		N/A	Mount

You can mount up to 3 (SN0100CO / SN0100COD) / 4 (SN1100CO / SN1100COD) external USB drives. Click **Mount** or **Unmount** to mount or unmount the drive. The **Status** column indicates *N/A*, *Mounted*, or *Unmounted*.

The supported file system for USB drives are FAT8, FAT16 and FAT32.

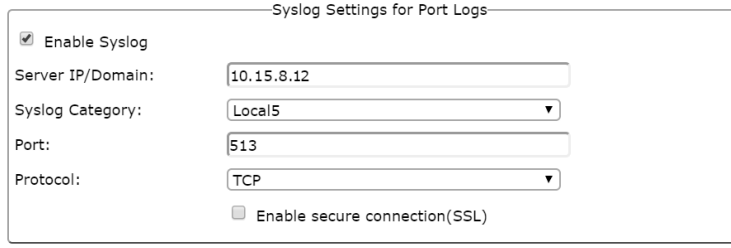
Sensors Settings (SN1100CO / SN1100COD Only)



You can setup up to 3 sensors and a relay for door access control.

- Sensor 1 & Sensor 2: Adjusts the minimum and maximum threshold for temperature, humidity, and air pressure sensors. The RJ-11 compatible sensors are as follows: EA1140, EA1240, and EA1340. These sensors are sold separately. Please contact your ATEN dealer for product information.
- Sensor 3: Select an available door sensor from Photo Door Sensor (EA1440) / Inductive Proximity Door Sensor (EA1441) / Reed Door Sensor (EA1442) / Capacitive Leakage Sensor (EA1540). These sensors are sold separately. Please contract your ATEN dealer for product information.
- Relay: Adjusts to relay for door access control from Open / Close / Pulse.
  - Open: Opens the electrical circuit.
  - Close: Closes the electrical circuit.
  - Pulse: Closes the electrical circuit for 3 seconds and then changes the electrical circuit to normally open.

Syslog Settings for Port Logs

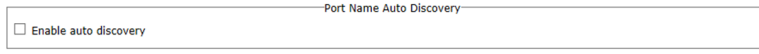


You can allow users to store logs on pre-defined Syslog servers.

To activate the function, check the “Enable Syslog” option to enable the function. When this function is activated, “Syslog server” option will then become available in the *Port Buffering* function.

Enter/select the server information in the fields shown in the diagram.

Port Name Auto Discovery



By default, this function is **disabled** (unchecked) and the server will display the port names according to the default naming rule (e.g. COM1, COM2, etc.).

When this function is **enabled** (checked), the server will automatically send probe strings to retrieve and display the port name of the connected network switches. The port name is displayed according to the device information (brand and model).

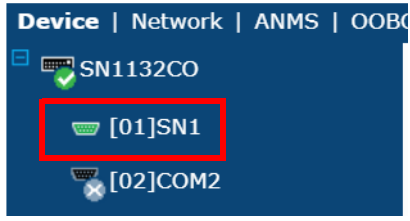
When the network switches cannot be recognized, the server will display the port names according to the default naming rule.

If the network switch needs verification initially, the server will also only display the default name. However, if you are verified (logged in to the switch), you can try and reconnect the serial port to see if the server can recognize the network switch in attempt to display the switch's information.

Compatible network switches include Cisco, Juniper, HPE, Dell, Huawei, H3C, EdgeCore, TRENDnet, Fortinet and ATEN ES0152.

Port Name Settings

The sidebar of the Serial Console Server GUI identifies connected devices by showing their device name, as shown below.



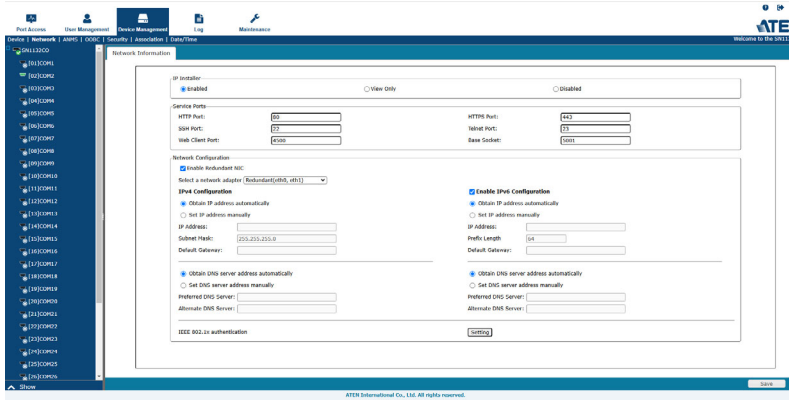
You can configure the Serial Console Server to check if any previously connected serial device is offline, and automatically revert the displayed name to its default at a user-specified time. For example, once the "SN1" device (as shown in the image above) goes offline, the system will change the name back to "COM1" at a user-specified time.

To set up the function:

1. Go to **Device Management > Device**. The Device Information page appears.
2. Scroll down to find Port Name Settings.
3. Click to enable **Change port name to default if serial devices is not online at the following time** and set the starting time for reflecting this update.
4. Click **Save**.

Network

The Network page is used to specify the network environment.



Each of the elements on this page is described in the sections that follow.

Note: The *Enable Redundant NIC* option is only available for SN1100CO / SN1100COD / SN0100CO / SN0100COD serial console servers.

IP Installer

The IP Installer is an external Windows-based utility for assigning IP addresses to the Serial Console Server.

Click one of the radio buttons to select *Enable*, *View Only*, or *Disabled* for the IP Installer utility. See *IP Installer*, page 265, for IP Installer details.

Note: 1. If you select *View Only*, you will be able to see the Serial Console Server in the IP Installer's Device List, but you will not be able to change the IP address.

2. For security, we strongly recommend that you set this to *View Only* or *Disable* after each use.

Service Ports

As a security measure, if a firewall is being used, the administrator can specify the port numbers that the firewall will allow. If a port other than the default is used, users must specify the port number as part of the IP address when they

log in. If an invalid port number (or no port number) is specified, the Serial Console Server will not be found. An explanation of the fields is given in the table below:

Field	Explanation
HTTP	The port number for a browser login. The default is 80.
HTTPS	The port number for a secure browser login. The default is 443.
SSH Port	The port for SSH access. The default is 22.
Telnet Port	The port for Telnet access. The default is 23.
Base Socket	The port used to listen for and accept a TCP connection

Note: 1. Valid entries for all of the Service Ports are from 1 to 65535.

2. Service ports cannot have the same value. You must set a different value for each one.
3. If there is no firewall (on an intranet, for example), it doesn't matter what these numbers are set to, since they have no effect.
4. Please refer to *Port Forwarding*, page 271 for how to connect SN1100CO / SN1100COD / SN0100CO / SN0100COD series device(s) through the Internet.

Network Configuration

- Redundant NIC*

  The SN1100CO / SN1100COD / SN0100CO / SN0100COD are designed with two network interfaces. If *Enable Redundant NIC* is enabled (the default), both interfaces make use of the IP address of network adapter *eth0*.

  Under this configuration, the second interface is usually inactive. If there is a network failure on the first interface, the Serial Console Server automatically switches to the second interface.

  - Redundant NIC Enabled – Single IP Address for Both Interfaces

    To enable the Redundant NIC function, do the following:

    1. Click to put a check in the *Enable Redundant NIC* checkbox.
    2. *eth0* is selected in the network adapter listbox, and the listbox is disabled – you cannot configure *eth1*.
    3. Configure the IP and DNS server addresses for *eth0* (see the sections below).

- Redundant NIC Not Enabled – Two IP Addresses

  If you choose not to enable the Redundant NIC function, the two NICs can be configured with separate interfaces. Users can log into the SN1100CO / SN1100COD / SN0100CO / SN0100COD with either IP address. To set up the Serial Console Server with this configuration, do the following:

  1. If there is a check in the *Enable Redundant NIC* checkbox, click to remove it.
  2. In the network adapter listbox; select *eth0*.
  3. Configure the IP and DNS server addresses for *eth0* (see the sections below).
  4. Drop down the network adapter listbox; select *eth1*.
  5. Configure the IP and DNS server addresses for *eth1*.

Note: Only available for SN1100CO / SN1100COD / SN0100CO / SN0100COD devices. To configure SN9100CO serial console servers, see *IPv4 Settings*, page 133,

- IPv4 Settings
  - IP Address:

    IPv4 is the traditional method of specifying IP addresses. The Serial Console Server can either have its IP address assigned dynamically (DHCP), or it can be given a fixed IP address.

    - For dynamic IP address assignment, select the *Obtain IP address automatically* radio button. (This is the default setting.)
    - To specify a fixed IP address, select the *Set IP address manually* radio button and fill in the fields with values appropriate for your network.

    Note:

    - If you choose *Obtain IP address automatically*, when the unit starts up it waits to get its IP address from the DHCP server. If it hasn't obtained the address after one minute, it automatically reverts to its factory default IP address (192.168.0.60 / 61.)
    - If the unit is on a network that uses DHCP to assign network addresses, and you need to ascertain its IP address, see *IP Address Determination*, page 265, for information.

- DNS Server
  - For automatic DNS Server address assignment, select the *Obtain DNS Server address automatically* radio button.
  - To specify the DNS Server address manually, select the *Set DNS server address manually* radio button, and fill in the addresses for the Preferred and Alternate DNS servers with values appropriate for your network.

Note: Specifying the Alternate DNS Server address is optional.

- IPv6 Settings
  - Enable the *Enable IPv6 configuration* to make configuration to the IPv6 settings.
  - IP Address:

    IPv6 is the new (128-bit) format for specifying IP addresses. (See *IPv6*, page 267 for further information.) The Serial Console Server can either have its IPv6 address assigned dynamically (DHCP), or it can be given a fixed IP address.

    - For dynamic IP address assignment, select the *Obtain IP address automatically* radio button. (This is the default setting.)
    - To specify a fixed IP address, select the *Set IP address manually* radio button and fill in the fields with values appropriate for your network.
  - DNS Server
    - For automatic DNS Server address assignment, select the *Obtain DNS Server address automatically* radio button.
    - To specify the DNS Server address manually, select the *Set DNS server address manually* radio button, and fill in the addresses for the Preferred and Alternate DNS servers with values appropriate for your network.

Note: Specifying the Alternate DNS Server address is optional.

Enabling 802.1x Security

This setting allows you to enable IEEE 802.1X authentication to enhance the security level to your wired LAN on each LAN port.

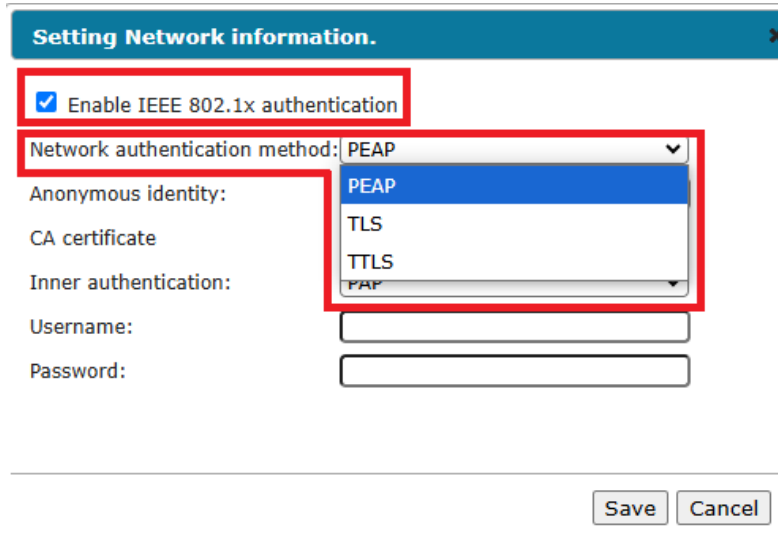
Note: Please make sure your network switch is IEEE 802.1X authentication-supported network switch.

To enable and configure the IEEE 802.1X authentication, follow the steps below.

1. Click **Settings**.

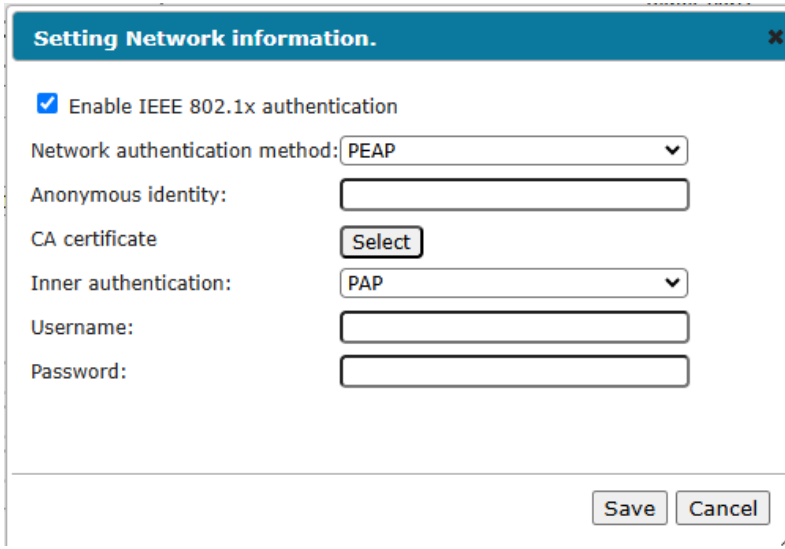


2. The 802.1X Setting Network Information page appears. Check the **Enable IEEE 802.1X Authentication** checkbox and select your authentication method from the Network Authentication Method section. The supported authentication methods are listed below.
   - PEAP
   - TLS
   - TTLS



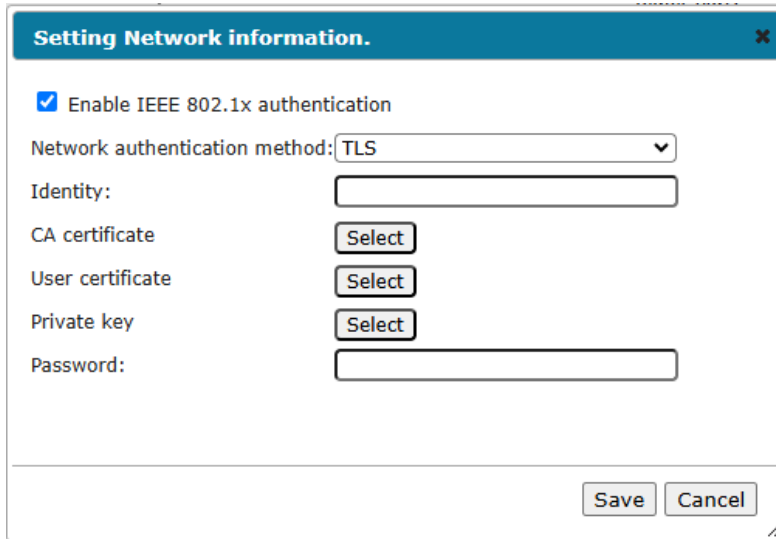
3. Refer to the tables below for configuration details. The required fields may vary depending on the network authentication method you select.

PEAP



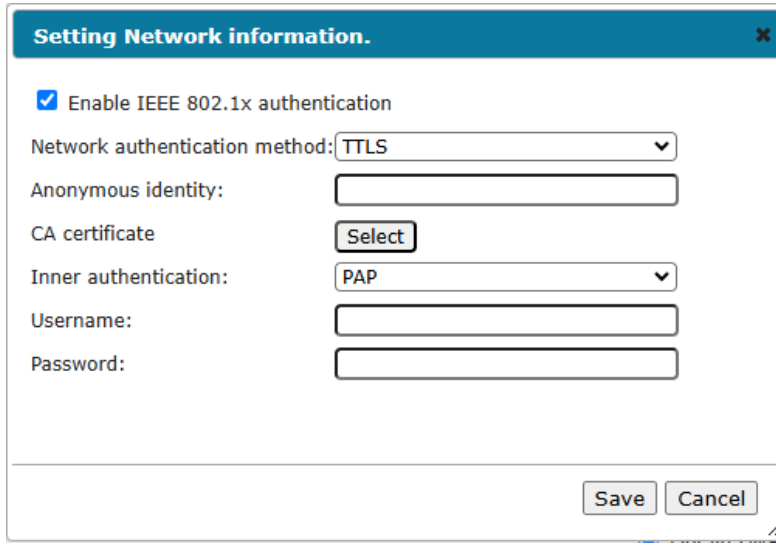
Entry	Explanation
Anonymous Identity	Enter the anonymous identity here.
CA Certificate	To browse and select a CA certificate, click **Select**.
Inner Authentication	The inner authentication options are as follow. ◆ PAP ◆ CHAP ◆ MSCHAPv2
User Name	Enter the username here.
Password	Enter the password here.

TLS



Entry	Explanation
Identity	Enter the identity here.
CA Certificate	To browse and select a CA certificate, click **Select**.
User Certificate	To browse and select an user certificate, click **Select**.
Private Key	To browse and select a client private key, click **Select**.
Password	Enter the password here.

TTLS



Entry	Explanation
Anonymous Identity	Enter the anonymous identity here.
CA Certificate	To browse and select a CA certificate, click **Select**.
Inner Authentication	The inner authentication options are as follow. ◆ PAP ◆ CHAP ◆ MSCHAPv2
User Name	Enter the username here.
Password	Enter the password here.

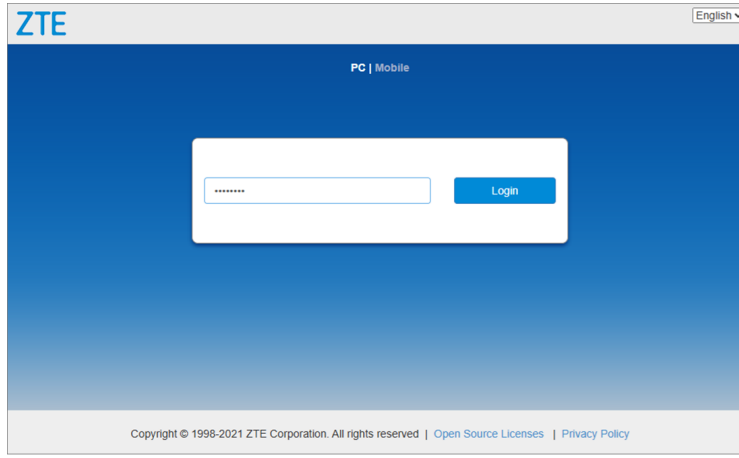
4. To check the IEEE 802.1X authentication status, please go to the **Log** tab and check the log information.

Mobile/WiFi Network Configuration

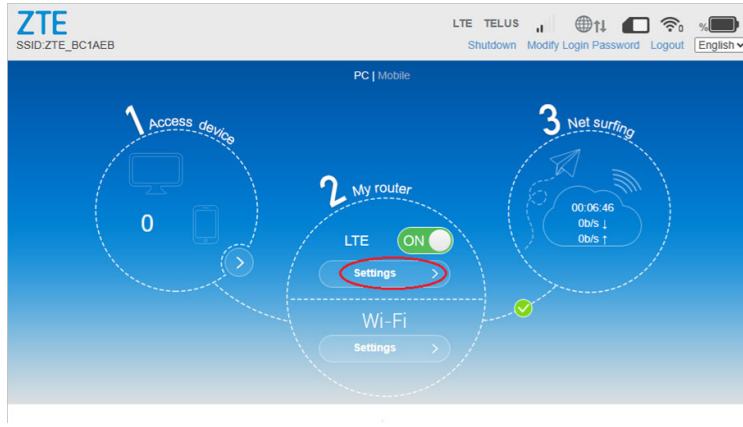
When inserted a USB Mobile/WiFi dongle to the Serial Console Server, configure the following settings.

Note: Mobile/WiFi connectivity is only supported on the SN11XX series.

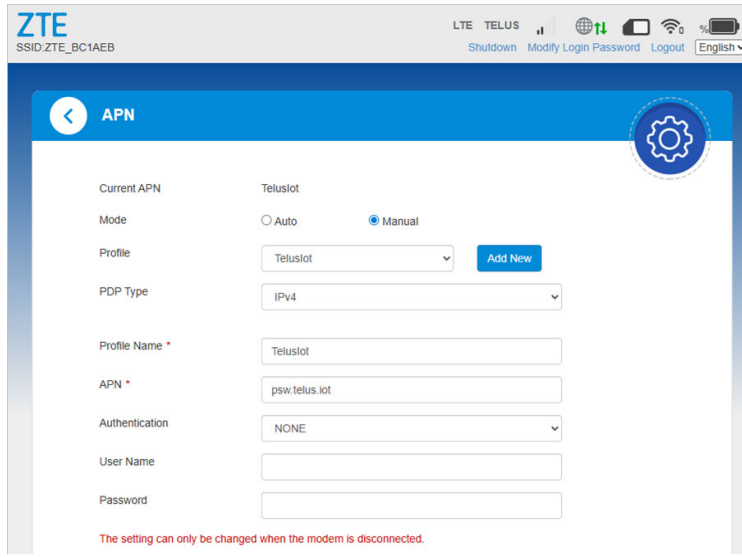
1. Configure the ZTE MF79U dongle.
   a) Plug the dongle into a Window-based PC.
   b) In a web browse, type in the default URL **http://192.168.0.1** to access its configuration page.



   c) Type in the password (provided with the package) and click **Login**. This page appears.

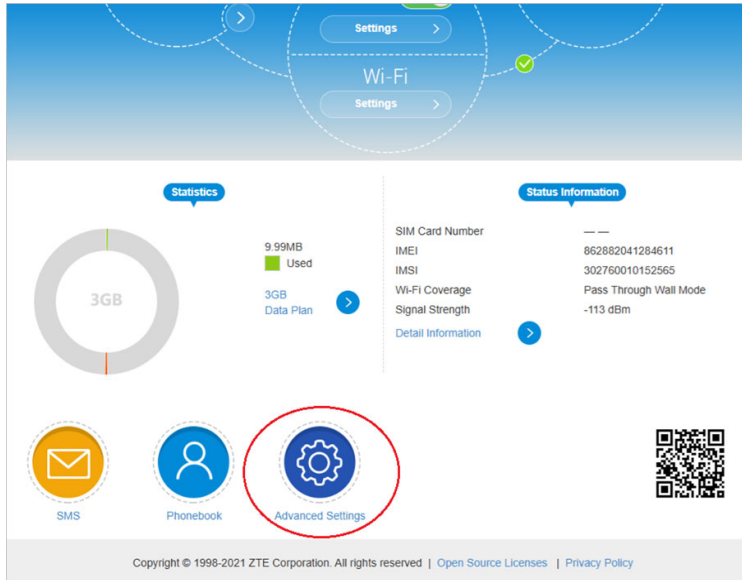


d) From 2 My Router, click to enable **LTE**, and then go to **Settings > Connection > APN**. This screen appears.

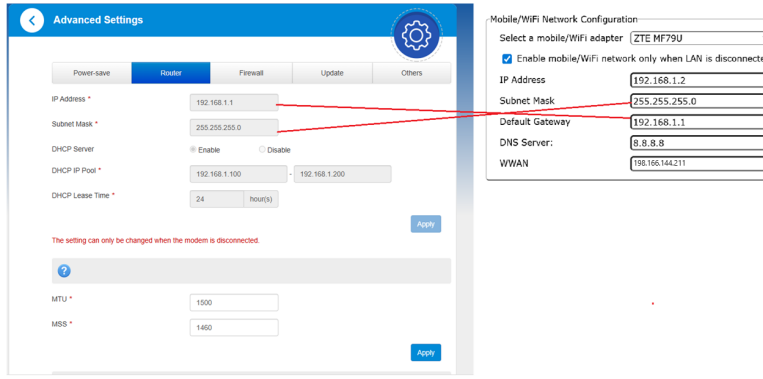


e) Fill in the APN information (provided by the Internet Service Provider). The ISP will then assign a public IP address to the Serial Console Server based on the APN configuration.

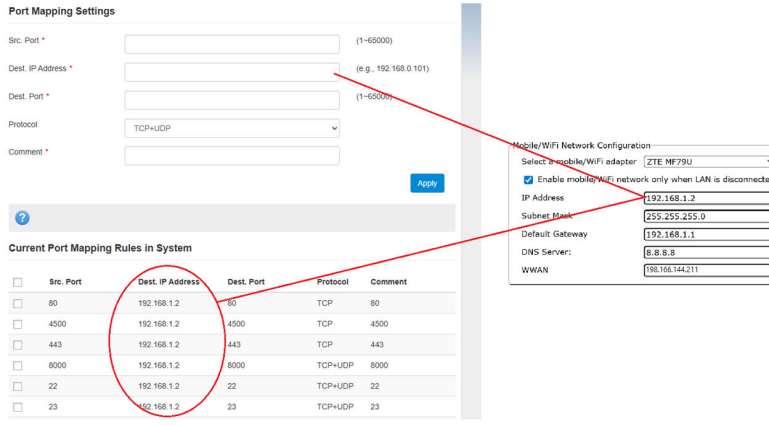
f) Go back to the main screen and go to **Advanced Settings**.



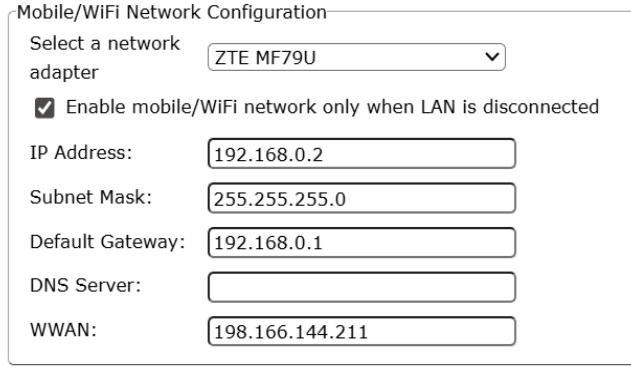
g) In the Router tab, configure the IP address and the subnet mask. Make sure they match the setup on the Serial Console Server, as indicated below.



h) Click the Firewall tab and configure the port mapping settings based on your network setup. For example:



2. On Serial Console Server, configure the following settings.



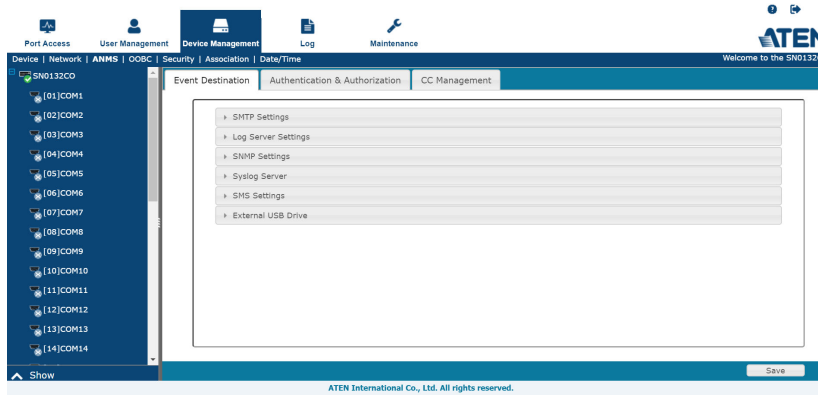
- **Select a network adapter:** Select **ZTE MF79U** from the drop-down menu.
- **Enable Mobile/WiFi network only when LAN is disconnected:** Enable this setting to prioritize the LAN connection and make mobile/WiFi accessible only when LAN is not available. When disabled, both LAN and mobile/WiFi are accessible.
- **IP Address, Subnet Mask, Default Gateway:** Fill in the network settings of the inserted mobile/WiFi dongle.
- **DNS Server:** Fill in the IP address of the public DNS server.
- **WWAN**: Fill in the SIM card public IP address.

3. Click **Save** to apply the settings. You can now access the Serial Console Server web console through web browsers or PuTTY with the public IP address.

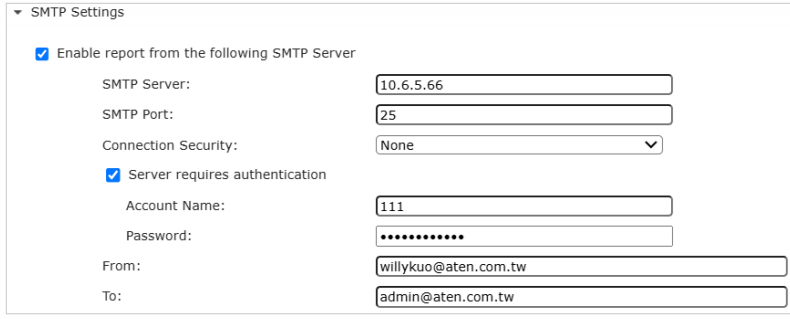
ANMS

The ANMS (Advanced Network Management Settings) page is used to set up login authentication and authorization management from external sources. It is organized as a notebook with three tabs – each with a series of related panels, as described, below:

Event Destination



SMTP Settings



To have the Serial Console Server 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 IPv4 address, IPv6 address, or domain name of the SMTP server.

2. Key in the SMTP port.
3. Configure the SMTP security settings using the Connection Security drop-down list. Select one of the following:
   - **None:** No encryption when sending email notifications.
   - **STARTTLS:** Email notifications are first sent unencrypted to the mail server, and only encrypted when forwarded to the recipients.
   - **SSL/TLS:** Email notifications are encrypted from the very start.
4. If your server requires authentication, put a check in the *Server requires authentication* checkbox, and key in the appropriate account information in the *Account Name* and *Password* fields.
5. Key in the email address of where the report is being sent from in the *From* field.

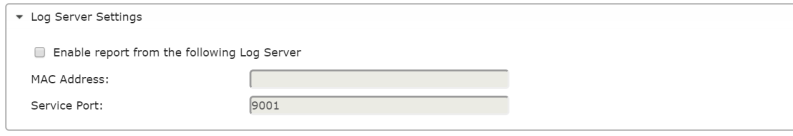
Note:

- Only one email address is allowed in the From field, and it cannot exceed 64 Bytes.
- 1 Byte = 1 English alphanumeric character.

6. Key in the email address (addresses) of where you want the SMTP reports sent to in the *To* field.

Note: If you are sending the report to more than one email address, separate the addresses with a semicolon. The total cannot exceed 256 Bytes.

Log Server



Important transactions that occur on the Serial Console Server, such as logins and internal status messages, are kept in an automatically generated log file.

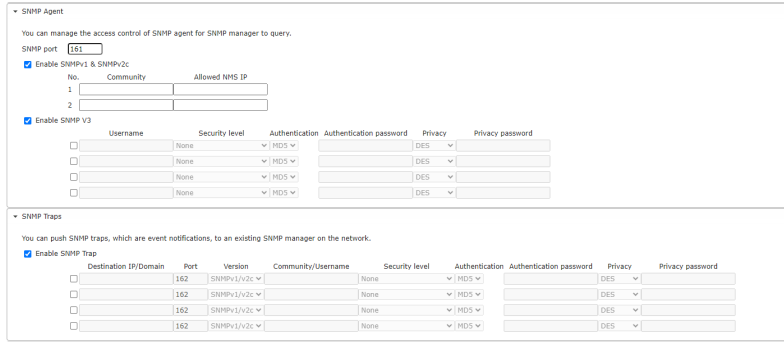
- To enable this, put a check in the *Enable report from the following Log Server* checkbox.
- Specify the MAC address of the computer that the Log Server runs on in the *MAC address* field.

- Specify the port used by the computer that the Log Server runs on to listen for log details in the *Service Port* field. The valid port range is 1–65535. The default port number is 9001.

Note: The port number must different than the one used for the *Program* port.

SNMP Setup

The ATEN Serial Console Server supports SNMP and functions as an SNMP agent that collects information about device's status, configuration, and performance metrics, and then provide this data to the requested network management system (NMS).



Note:

- SNMP Trap supports SNMP v1/v2c/v3.
- SNMP Agent supports SNMP v1/v2c/v3.
- For detailed information about the defined MIB objects and traps, see Chapter 11, *MIB Reference*.

For the Serial Console Server to send SNMP notifications, follow the steps below to set up the function.

1. In the Serial Console Server's web console, go to **Device Management** > **ANMS** > **Event Destination**.
2. Configure the SNMP Agent tab.
   a) Specify the SNMP port.

b) Select the SNMP version by checking the checkboxes. If the **Enable SNMPv1 and SNMPV2c** checkbox is checked, specify Community and optionally the Allowed NMS IP.

c) If **Enable SNMP V3** is selected, configure the following.

- **Username:** Enter the name of the SNMPv3 user account.
- **Security Level:** Use the drop-down menu to select a security level.
- **Authentication:** Select an authentication protocol.
- **Authentication Password:** Enter the password of the SNMP v3 user.
- **Privacy & Privacy Password:** Set the encryption type and the password.

Note:

- Both the Authentication Password and Privacy Password support the following special characters: .,{}:|~!@#%&_=><*+?$-()[]/^.
- Up to 4 SNMP agent receivers can be specified. Make sure that the port number you specify here matches the port number used by the SNMP receiver computer.

---

3. Configure the SNMP Traps tab.

a) Click the **Enable SNMP Trap** setting.

b) Click an entry and configure the following.

- **Destination IP/domain:** the IP address of the device or server that will receive SNMP traps.
- **Port:** the service port used to notify monitored events. The valid port range is **1–65535**. The default port number is **162**.
- **Version:** Select the SNMP version that the monitored devices support.
- **Community/username:** Enter the community string for the selected SNMP version.

c) If the SNMPv3 version is selected, configure the following.

- **Security Level (*only applicable to SNMPv3*):** Use the drop-down menu to select a security level.
- **Authentication:** Select an authentication protocol.
- **Authentication Password:** Enter the password of the SNMP v3 user.

- **Privacy & Privacy Password:** Set the encryption type and the password.

Note:

- Both the Authentication Password and Privacy Password support the following special characters: .,{}:|~!@#%&_=><*+?$-()[]/^.
- Up to 4 SNMP trap receivers can be specified. Make sure that the port number you specify here matches the port number used by the SNMP receiver computer.

Syslog Server

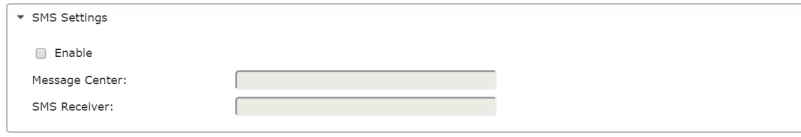


To record all the events that take place on Serial Console Server and write them to a Syslog server, do the following:

1. Check *Enable*.
2. Key in either the IPv4 address, IPv6 address, or domain name of the Syslog server.
3. Key in the port number. The valid port range is 1-65535.

Note: Up to 2 Syslog Servers can be specified.

SMS Settings



To receive notifications via SMS, do the following:

1. Check *Enable*.
2. Enter the telephone numbers for the *Message Center* and *SMS Receiver*.

Note: When you have made all your changes, remember to click *Save* at the bottom right corner of the page.

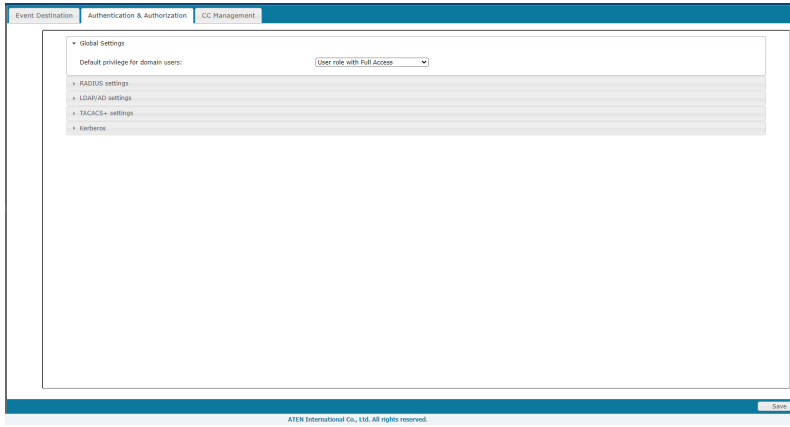
- External USB Drive



To record all the events that take place on Serial Console Server and write them to an external USB drive, do the following:

1. Check *Enable*.
2. Select the drive you wish to write the events to.
3. Key in the file name for the log.

Authentication and Authorization



Global Settings

Selects a role and access privilege for the domain users.

- User Role with No Access: Sets the domain users to user role with no accessibility and edit right to all serial ports.
- User Role with Full Access (default): Sets the domain users to user role with accessibility and edit right to all serial ports.

- Administrator Role with Full Access: Sets the domain users to administrator role with accessibility and edit right to all serial ports.

Note:

- Domain User: The real permission for the domain user is a combined result of the configuration that is set under the *ANMS*, *Authentication & Authorization* tab and *Groups, Devices* tab (page 123). Make sure the identical group name is created in the third-party authentication & authorization server and in the group list (page 114). The priority is as follows: Full Access > View Only > No Access.
- When the View Only User is selected under Permissions, User tab (page 108), the priority is as follows: View Only User > Full Access >View Only > No Access.

RADIUS Settings

To allow authentication and authorization for the Serial Console Server through a RADIUS server, do the following:

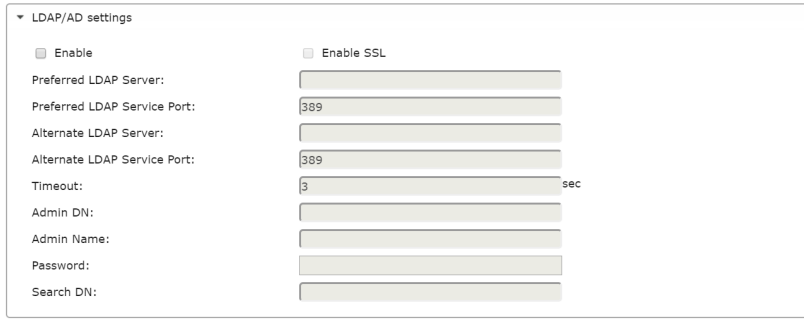
1. Check **Enable**.
2. Fill in the IP addresses and service port numbers for the Preferred and Alternate RADIUS servers. You can use the IPv4 address, the IPv6 address or the domain name in the IP fields.
3. In the *Timeout* field, set the time in seconds that the Serial Console Server waits for a RADIUS server reply before it times out.
4. In the *Retries* field, set the number of allowed RADIUS retries.
5. In the *Shared Secret* field, key in the character string that you want to use for authentication between the Serial Console Server and the RADIUS Server. A minimum of 6 characters is required. The Shared Secret support the following special characters: .,{}:|~!@#%&_=><*+?$-()[]/^.
6. On the RADIUS server, Users can be authenticated with any of the following methods:
   - Set the entry for the user as **su/xxxx**

     Where *xxxx* represents the username given to the user when the account was created on the Serial Console Server.
   - Use the same username on both the RADIUS server and the Serial Console Server.

- Use the same group name on both the RADIUS server and the Serial Console Server.
- Use the same username/group name on both the RADIUS server and the Serial Console Server.

In each case, the user's access rights are the ones assigned that were assigned when the user of group was created on the Serial Console Server. (See *Adding Users*, page 109.)

LDAP / AD Settings



To allow authentication and authorization for the Serial Console Server via LDAP / AD, refer to the information in the table, below:

Item	Action
Enable	Check the *Enable* checkbox to enable LDAP, and *Enable SSL* checkbox to enable LDAPS authentication and authorization.
LDAP Server IP and LDAP Service Port	Fill in the IP address and port number for the LDAP or LDAPS server. ◆ You can use the IPv4 address, the IPv6 address or the domain name in the *LDAP Server* field. ◆ For LDAP, the default port number is 389; for LDAPS, the default port number is 636.
Alternate LDAP Server and Alternate LDAP Service Port	Fill in the IP address and port number for the alternate LDAP or LDAPS server. ◆ You can use the IPv4 address, the IPv6 address or the domain name in the *Alternate LDAP Server* field. ◆ For an *Alternate LDAP Service Port,* the default port number is 389; for an *Alternate LDAPS Service Port*, the default port number is 636.

Item	Action
Admin DN	Consult the LDAP / LDAPS administrator to ascertain the appropriate entry for this field. For example, the entry might look like this: ou=kn4132,dc=aten,dc=com
Admin Name	Key in the LDAP administrator's username.
Admin Password	Key in the LDAP administrator's password. The Admin Password support the following special characters: .,{}:|~!@#%&_=><*+?$-()[]/^.
Search DN	Set the distinguished name of the search base. This is the domain name where the search starts for user names.
Timeout	Set the time in seconds that the Serial Console Server waits for an LDAP or LDAPS server reply before it times out.

On the LDAP / AD server, Users can be authenticated with any of the following methods:

- Without schema – Only the usernames used on the Serial Console Server are matched to the names on the LDAP / LDAPS server. User privileges are the same as the ones configured on the Serial Console Server.
- Without schema – Only groups in AD are matched. User privileges are the ones configured for the groups he belongs to on the Serial Console Server.
- Without schema – usernames and groups in AD are matched. User privileges are the ones configured for the user and the groups he belongs to on the Serial Console Server.

TACACS+ Settings



- **Enable** TACACS+ and enter the following information:
  - Preferred TACACS+ Server
  - Preferred TACACS+ Service Port
  - Shared Secret 1
  - Alternate TACACS+ Server
  - Alternate TACACS+ Service Port
  - Shared Secret 2

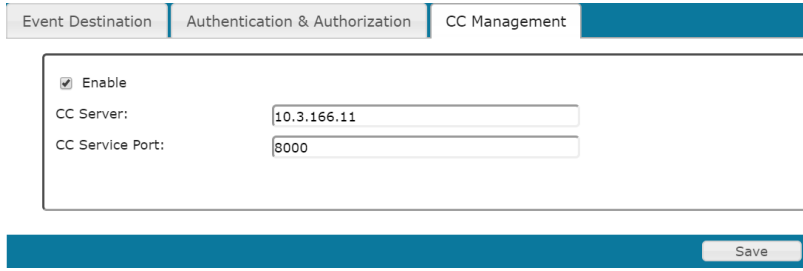
- Authentication Type: Use the drop-down menu to select between PAP/CHAP and MSCHAP.

Kerberos



- Enable Kerberos and enter the following information:
  - Kerberos Server
  - Kerberos Service Port
  - Kerberos Realm

CC Management Settings

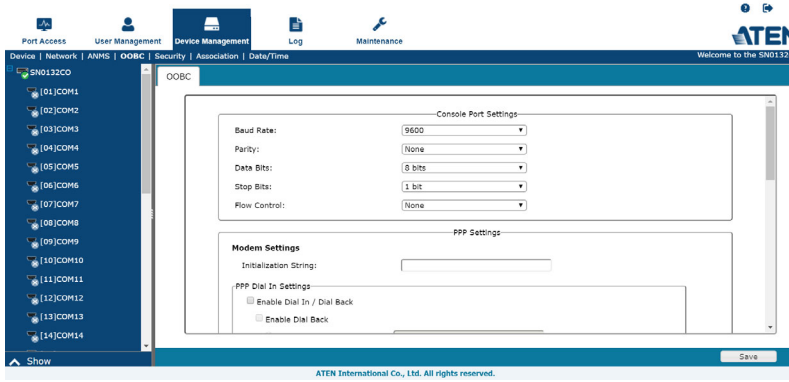


To allow authorization for the Serial Console Server through a CC (Control Center) server, check *Enable* and fill in the CC Server's IP address and Service port in the appropriate fields. You can use the IPv4 address, the IPv6 address or the domain name in the *CC Server IP* field.

Note: If this function is enabled, PON devices do not appear in the sidebar, even if they are configured on the Serial Console Server. This is because they are managed via the CC server.

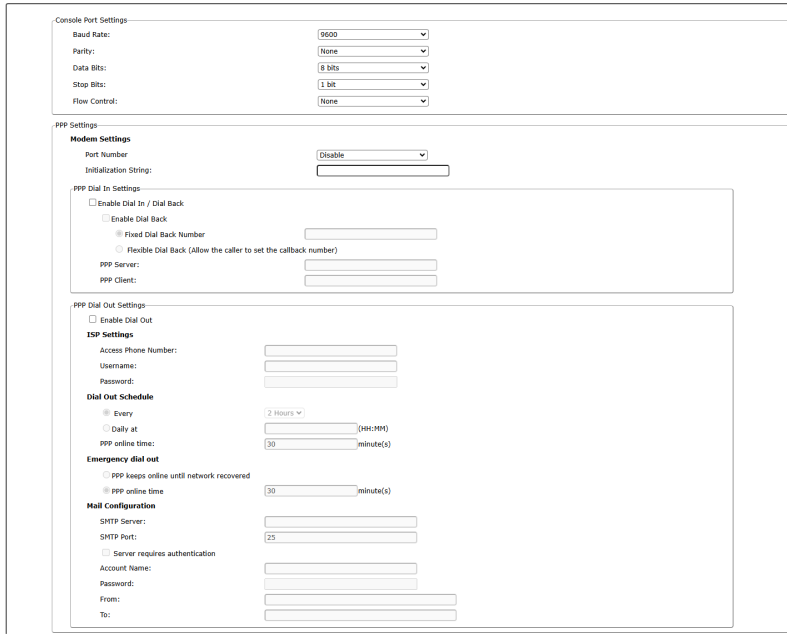
OOBC

In case the Serial Console Server cannot be accessed with the usual LAN-based methods, it can be accessed via the Serial Console Server's modem port or one of the serial ports (SN1100CO / SN9108CO / SN9116CO) configured for a modem.

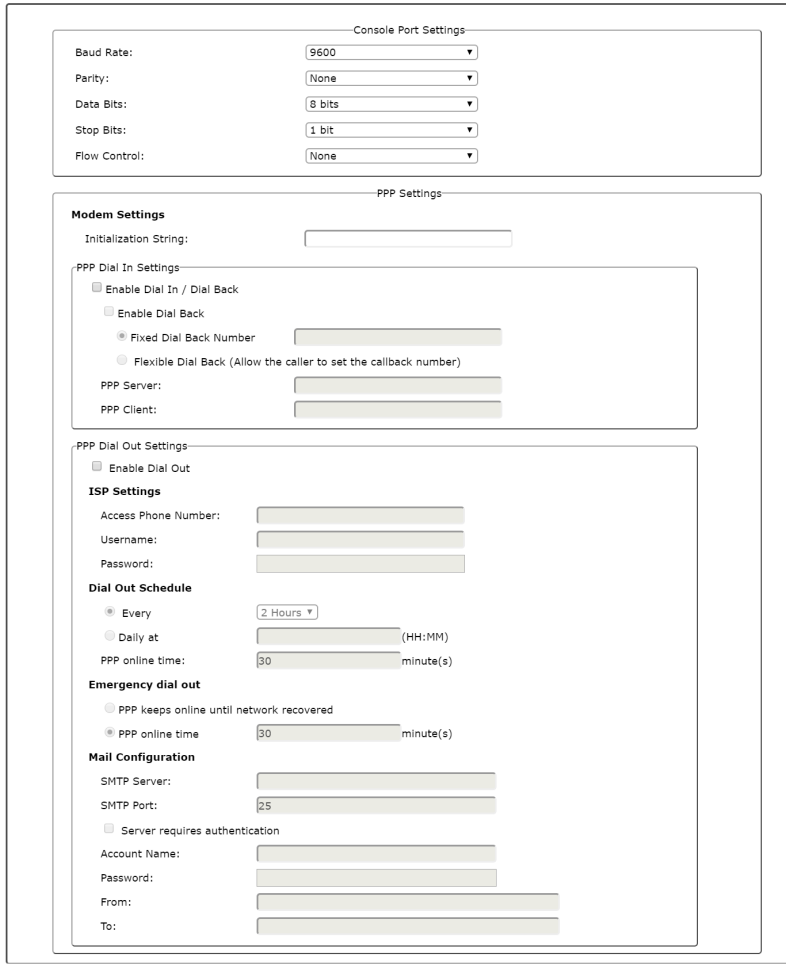


Console Port Settings

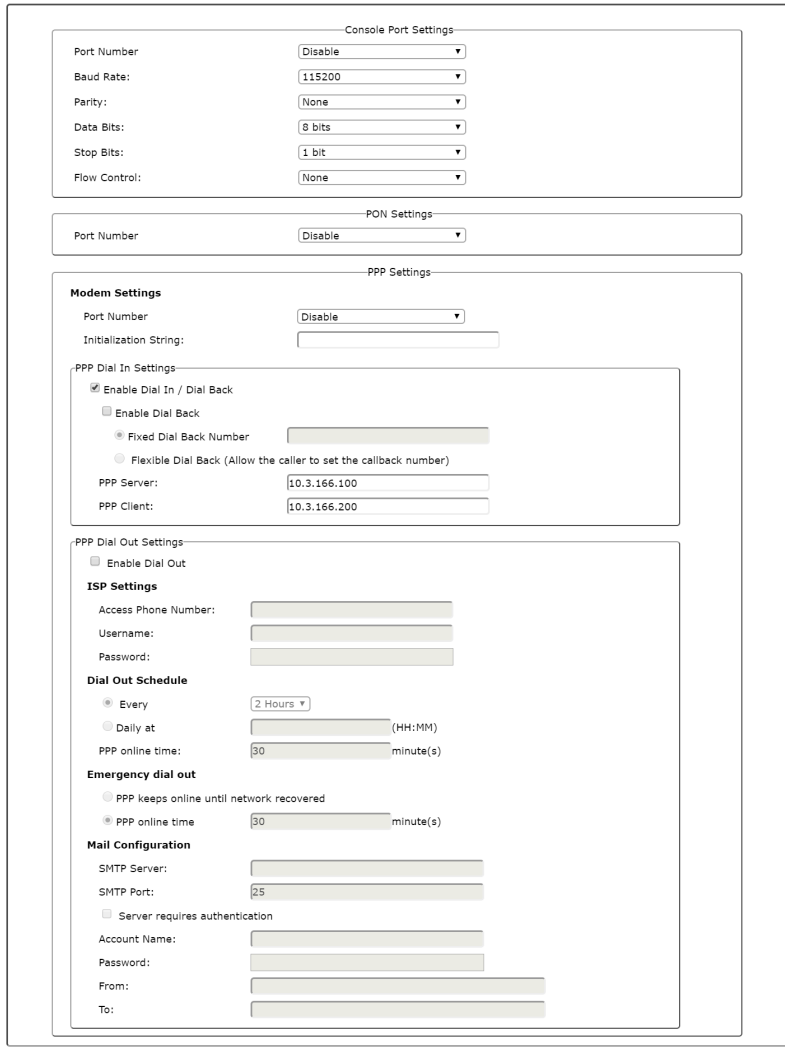
SN1100CO / SN1100COD



SN0100CO / SN0100COD



SN9100CO



Select the Port Number that the *Console*, *PON (reserved)* and *Modem* is connected to on the rear of the SN9100CO. By default, the Port Number of the SN9100CO's *Console Port* is disabled.

Enable Dial Back

When you enable Out of Band Access, the *Enable Dial Back*, and *Enable Dial Out* functions become available, as described in the sections that follow. As an added security feature, if this function is enabled, the Serial Console Server disconnects the calls that dial in to it, and dials back to one of the entries specified in the table below:

Item	Action
Enable Fixed Number Dial Back	If *Fixed Number Dial Back* is enabled, when there is an incoming call, the Serial Console Server hangs up the modem and dials back to the modem whose phone number is specified in the Phone Number field. Key the phone number of the modem that you want the Serial Console Server to dial back to in the *Phone Number* field.
Enable Flexible Dial Back	If *Flexible Dial Back* is enabled, the modem that the Serial Console Server dials back to doesn't have to be fixed. It can dial back to any modem that is convenient for the user, as follows: 1. Key the password that the users must specify in the *Password* field. 2. When connecting to the Serial Console Server's modem, users specify the phone number of the modem that they want the Serial Console Server to dial back to as their username, and specify the password set in the *Password* field for their password.

Enable Dial Out

For the dial out function, you must establish an account with an Internet Service Provider, and use a modem to dial up to your ISP account. An explanation of the Enable Dial Out items is given in the table below:

Item	Action
ISP Settings	Specify the telephone number, account name (username), and password that you use to connect to your ISP.

Item	Action
Dial Out Schedule	This entry sets up the times you want the Serial Console Server to dial out over the ISP connection. ◆ *Every* provides a listing of fixed times from every hour to every four hours. ◆ If you select *Every two hours* (for example), the Serial Console Server will start dialing out every two hours beginning at 00:00. ◆ If you don't want the Serial Console Server to dial out on a fixed schedule, select **Never** from the list. ◆ *Daily at* will dial out once a day at a specified time. Use the hh:mm format to specify the time. ◆ *PPP online time* specifies how long you want the ISP connection to last before terminating the session and hanging up the modem. A setting of zero means it is always on line.
Emergency Dial Out	If the Serial Console Server gets disconnected from the network, or the network goes down, this function puts the Serial Console Server on line via the ISP dial up connection. ◆ If you choose *PPP stays online until network recovery*, the PPP connection to the ISP will last until the network comes back up or the Serial Console Server reconnects to it. ◆ If you choose *PPP online time*, the connection to the ISP will terminate after the amount of time that you specify is up. A setting of zero means it is always on line.

Item	Action
Mail Configuration	This section provides email notification of problems that occur on the devices connected to the Serial Console Server's ports (see *SMTP Settings*, page 143). **Note:** This email notification differs from the one configured under *SMTP Settings*, page 143, in that it uses the ISP mail server rather than the internal company's mail server. ◆ Key in the IPv4 address, IPv6 address, or domain name of your SMTP server in the SMTP Server IP Address field. ◆ Key in the SMTP Port of the SMTP Server. The default is port 25. If you don't know the port number, ask your SMTP server administrator. ◆ If your server requires authentication, check the *SMTP server requires authentication* checkbox, then key in the authentication account name and password in the fields. If you don't know the authentication account name and password or if you don't know whether the server requires authentication, ask your SMTP server administrator. ◆ Key in the email address of the person responsible for the SMTP server (or some other equally responsible administrator) in the *From* field. ◆ Key in the email address (addresses) of where you want the report sent to in the *To* field. If you are sending the report to more than one email address, separate the addresses with a comma or a semicolon.

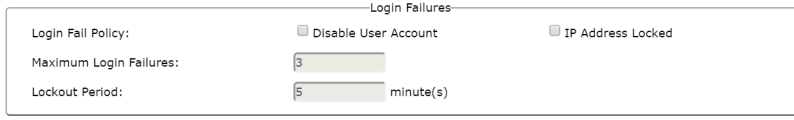
When you have finished making your settings on this page, click **Save**.

Security

The Security page is divided into 4 main panels, as described in the sections that follow.

Login Failures

For increased security, the Login Failures section allows administrators to set policies governing what happens when a user fails to log in successfully.



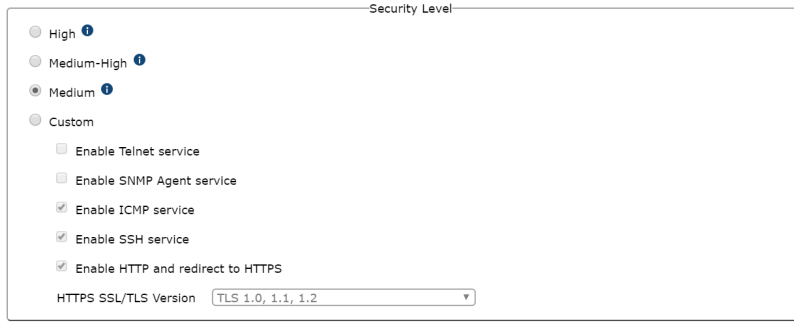
To set Login Failures, check one of the Login Fail Policy checkboxes. The meanings of the entries are explained in the table below:

Entry	Explanation
Login Fail Policy	This determines what happens when a user fails to log in according to the security parameters that are set here. When a user exceeds the maximum login failures, you can set the Serial Console Server to: ◆ Disable User Account ◆ IP Address Locked The amount of time the policy takes effect is set in the Lockout Period.
Maximum login Failures	This field sets the number of failed attempts a user is allowed before the Login Fail Policy is activated.
Lockout Period	Sets the amount of time the User Account is disabled or IP Address is Locked before access will be reactivated.

Note: If a Login Fail Policy is not enabled, users can attempt to log in an unlimited number of times with no restrictions. For security purposes, we recommend that you enable this function and enable the lockout policies.

Security Level

For increased security, you can check or uncheck the boxes to High, Medium - high, Medium or Custom security features.



1. High (Disable all services except: SSHv2, HTTPS(TLS v1.2))
2. Medium-high (Enables SSHv2, redirect HTTP to HTTPS, HTTPS(TLS v1.2), ICMP)
3. Medium (Enables SSHv2, redirect HTTP to HTTPS, HTTPS(TLS v1.0, 1.1, 1.2), SNMP Agent, ICMP) (**Default**)
4. Custom: Click to check the following security options you wish to apply:
   - Enable Telnet service
   - Enable SNMP Agent service
   - Enable ICMP service
   - Enable SSH service (checked by default)
   - Enable HTTP and redirect to HTTPS (checked by default)
   - HTTPS SSL/TLS version: Select between “TLS 1.2”, ”TLS 1.0, 1.1, 1.2” (default), and “SSL 3.0, TLS 1.0, 1.1, 1.2”.

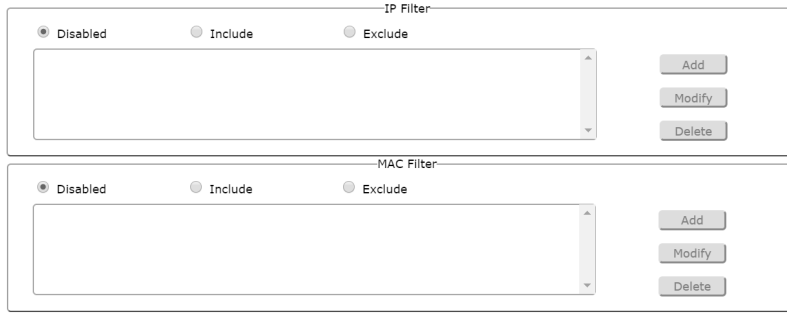
Misc.



For increased security, you can enable the following settings:

- **Enable FIPS 140-2:** Enable this setting for cryptographic modules.
- **Enable host header protection:** Enable this setting for the Serial Console Server to validate the host header in incoming HTTP requests to prevent web attacks.

IP/MAC Filter



- IP and MAC Filtering

  IP and MAC Filters control access to the Serial Console Server based on the IP and/or MAC addresses of the client computers attempting to connect. A maximum of 100 IP filters and 100 MAC filters are allowed. If any filters have been configured, they appear in the IP Filter and/or MAC Filter list boxes.

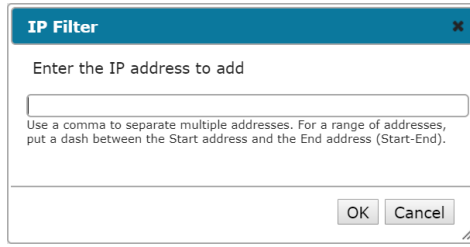
  To enable IP and/or MAC filtering, select one of the following radio buttons:

  - If the **Include** button is selected, all the addresses within the filter are allowed access; all other addresses are denied access.
  - If the **Exclude** button is selected, all the addresses within the filter are denied access; all other addresses are allowed access.

- Adding Filters

  To add an IP filter, do the following:

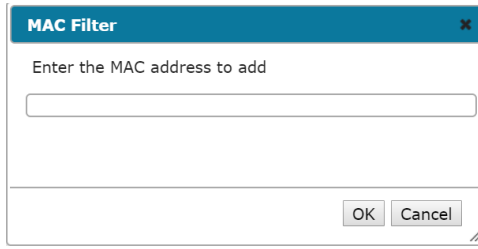
1. Click **Add**. A dialog box appears.



2. Key the IP address you want to filter.
3. After filling in the address, click **OK**.
4. Repeat these steps for any additional IP addresses you want to filter.

To add a MAC filter, do the following:

1. Click **Add**. A dialog box appears.



2. Specify the MAC address in the dialog box, then click **OK**.
3. Repeat these steps for any additional MAC addresses you want to filter.

- IP Filter / MAC Filter Conflict

  If there is a conflict between an IP filter and a MAC filter – in other words, if a computer's address is allowed by one filter but blocked by the other – then the blocking filter takes precedence (the computer's access is blocked).

- Modifying Filters

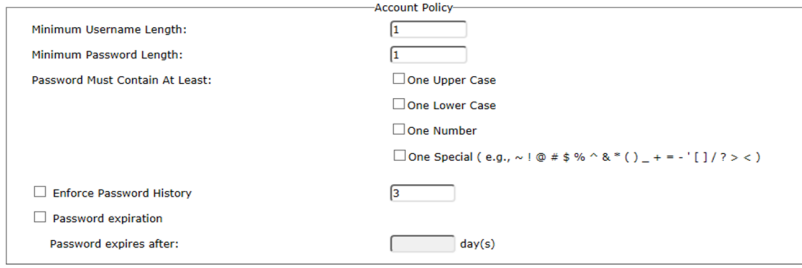
  To modify a filter, select it in the IP Filter or MAC Filter list boxes and click **Modify**. The Modify dialog box is similar to the Add dialog box. When it comes up, simply delete the old address(es) and replace it with the new one(s).

- Deleting Filters

  To delete a filter, select it in the IP Filter or MAC Filter list box and click **Delete**.

Account Policy

In the Account Policy section, system administrators can set policies governing usernames and passwords.

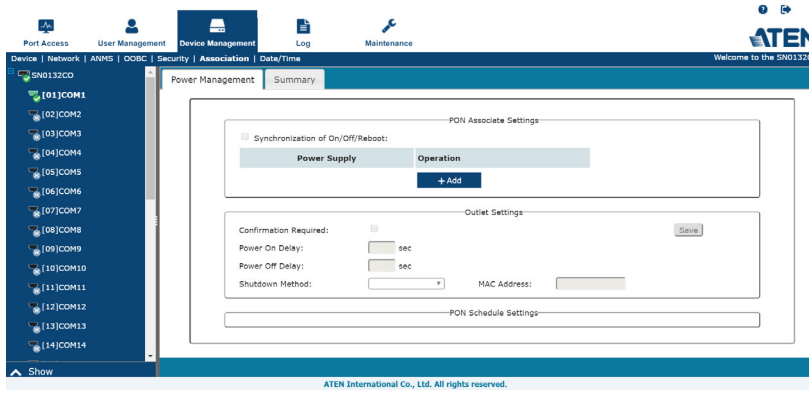


The meanings of the Account Policy entries are explained in the table below:

Entry	Explanation
Minimum Username Length	Sets the minimum number of characters required for a username. Acceptable values are from 1 to 16. The default is 6.
Minimum Password Length	Sets the minimum number of characters required for a password. Acceptable values are from 0 to 16. A setting of 0 means that no password is required. Users can log in with only a username. The default is 6.
Password Must Contain At Least	Checking any of these items requires users to include at least one uppercase letter, one lowercase letter, one number or one special character in their password. **Note:** This policy only affects user accounts created after this policy has been enabled, and password changes to existing user accounts. Users accounts created before this policy was enabled, and there is no change to the existing passwords, are not affected.
Enforce Password History	Checking this box will require users to create a unique password that does not match the last x passwords they've used prior. X equals the number entered in the dialog box.
Password Expiration	Enter a value (in days) for all passwords to expire.

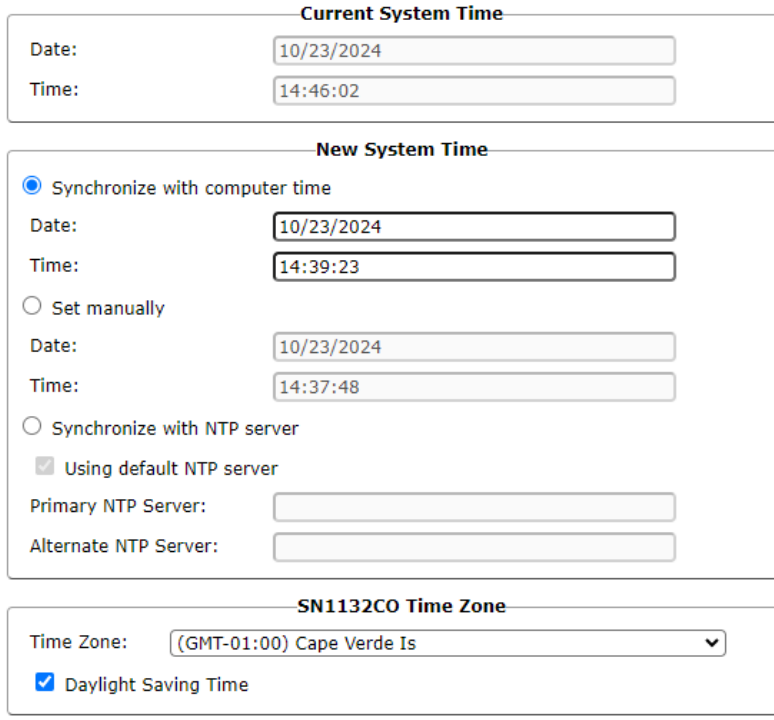
Association

The *Association* tab is currently reserved.



Date/Time

The Date/Time dialog page sets the Serial Console Server time parameters:



Set the parameters according to the information below.

Current System Time

This section displays the time and date that the switch is currently set to. The time and date fields are for information purposes and cannot be edited.

Note: In the Browser UI, the system time displays the time relative to the time zone that the web browser session originates from – not the time zone of the Switch. If the web browser session originates from a time zone that is different from the switch's time zone, the time shown in the display will be different from the switch's time.

New System Time

Use these fields to change the switch's time and date settings, as follows:

- To set the switch's time and date to match the time and date of the computer you are logged in to, select the Synchronize with computer time radio button.

Note: Your computer's time and date are displayed in the fields just below the heading. These fields are for information purposes only.

- To set the time and date to values of your choosing, select the **Set manually** radio button and key the settings into their appropriate fields using the *YYYY-MM-DD* and *HH:MM:SS* formats.

Note: Date/time formats may differ depending on the selected interface language.

- To have the time automatically synchronized to a network time server, select the **Synchronize with NTP server** radio button:
  - If you want to use your network's default time server, put a check in the *Using default NTP server* checkbox.
  - If you want to specify a time server, make sure that the *Using default NTP server* checkbox is unchecked, then key in the IP address of the time server of your choice in the *Primary NTP Server* field. If you want to configure an alternate time server, key in the IP address of the time server in the *Alternate NTP Server* field.
  - Click **Save** to apply the changes.

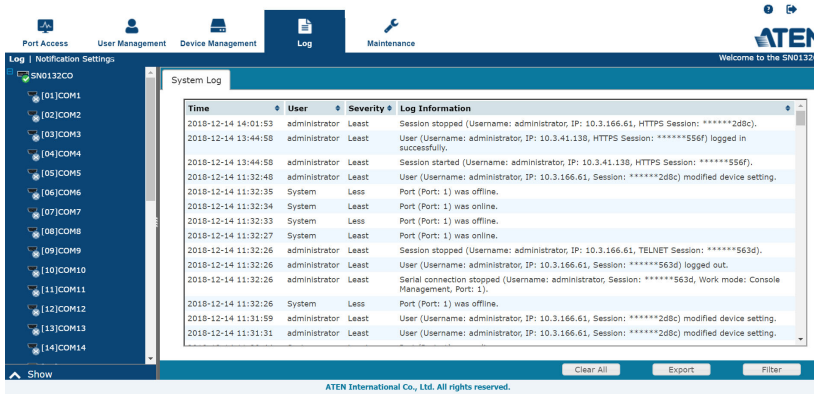
Time Zone

- To establish the time zone that the Serial Console Server is located in, drop down the *Time Zone* list and choose the city that most closely corresponds to where it is located.
- If you want to enable daylight saving time, make sure that the *Daylight Saving Time* checkbox is checked.
- Click **Save** to apply the changes.

Chapter 9
Log

Overview

The Serial Console Server logs all the events that take place on it. To view the contents of the log, click the *Log* tab. The device's System Log page appears:



System Log

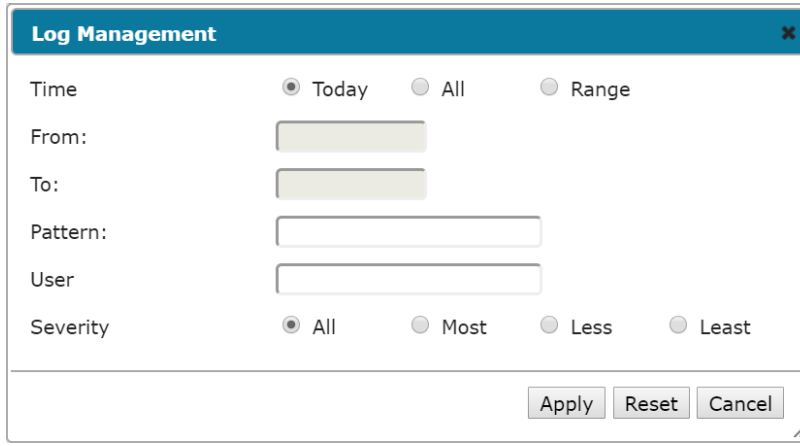
The System Log page displays events that take place on the Serial Console Server, and provides a breakdown of the time, the severity, the user, and a description of each one. You can change the sort order of the display by clicking on the column headings.

The memory size of the System Log is 1 MB, it can display minimum 512 events or more, depending on the log contents. When the limit is reached, the oldest events get discarded as new events come in. The purpose of the buttons at the bottom of the page are described in the table:

Button	Explanation
Clear Log	Clicking *Clear Log* clears the log file.
Export Log	Clicking *Export Log* lets you save the contents of the log to a file on your computer.
Filter	Clicking *Filter* allows you to search for particular events by date or by specific words or strings, as described in the next section.

Filter

Filter lets you narrow the log event display to ones that occurred at specific times; ones containing specific words or strings; or ones involving specific users. When you access this function, the log filter dialog box appears at the bottom of the page:



A description of the filter items is given in the table, below:

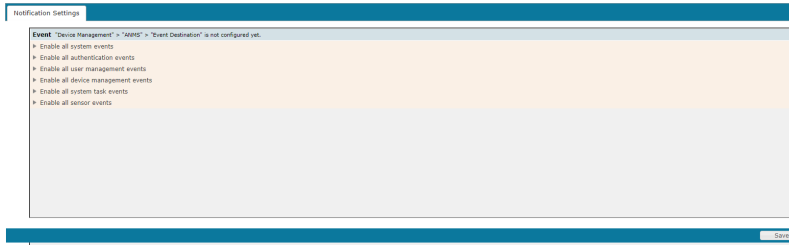
Item	Description
Time	This feature lets you filter for events that occurred at specific times, as follows: **Today:** Only the events for the current day are displayed. **All:** Select this radio button to filter results for all the records in the log file. **Range:** Select this radio button to filter results for records for a particular time period, then click the **From** and **To** fields and a calendar will appear for you to select the dates.
Pattern	Filters for a particular word or string. Key the word or string into the *Information* text box. Only events containing that word or string are displayed. Wildcards (? for single characters; * for multiple characters) and the keyword **or** are supported. E.g., h*ds would return hands and hoods; h?nd would return hand and hind, but not hard; h*ds or h*ks would return hands and hooks.
User	Filters for specific users. Key in the user's username; then click **Apply**. Only events containing that username are displayed. **Note:** If the *User* does not exist or the spelling is incorrect, no results will appear.

Item	Description
Severity	Filters based on the severity rating of the event. Least severe events appear in black; Less severe events appear in blue; Most severe events appear in red. Check the radio button for the severity level that you want to display: *All*, *Most*, *Less*, or *Least*. Only events that match the severity level you specified appear in the display.
Apply	Click to apply the filter choices.
Reset	Click this button to clear the entries in the dialog box and start with a clean slate.
Cancel	Click this button to exit the log filter function without applying changes.

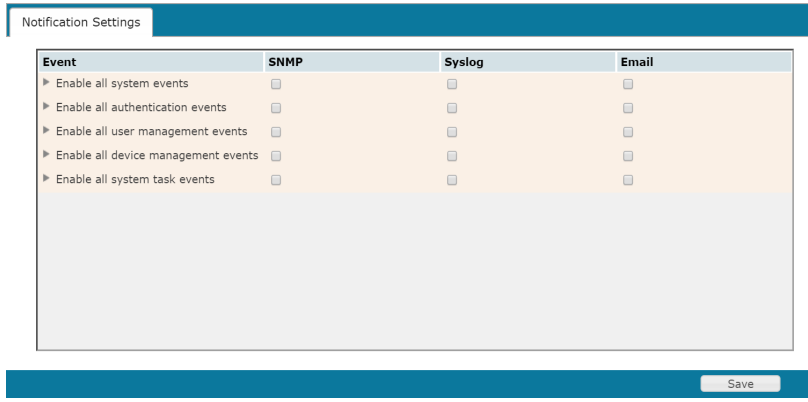
Log Notification Settings

The Notification Settings page lets you decide which events trigger a notification:

SN1100CO / SN1100COD



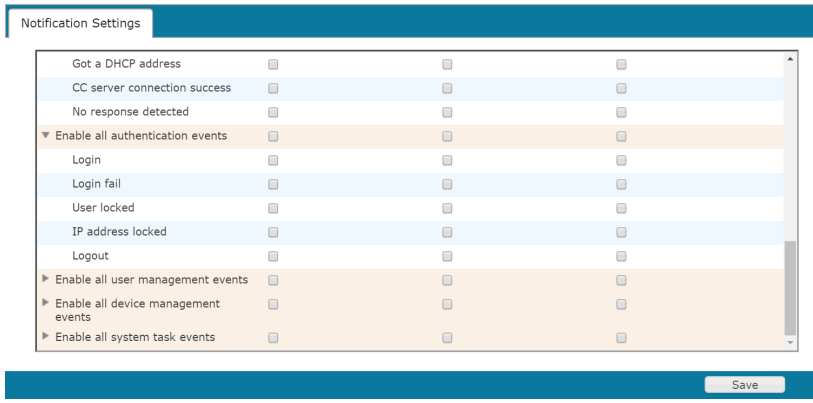
SN0100CO / SN0100COD / SN9100CO



The notifications are grouped into six groups: You can choose to enable the following:

- All system events
- All authentication events
- All user management events
- All device management events
- All system task events
- All sensor events (SN1100CO / SN1100COD Only)

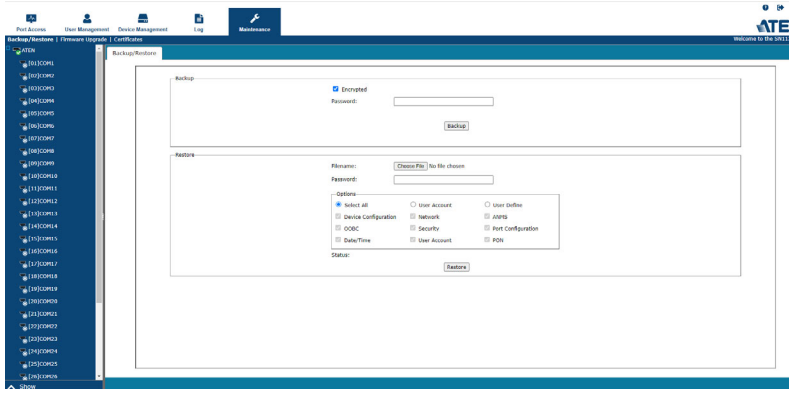
If you wish to turn on/off a particular notification, you may click on the icon to expand the groups to check/uncheck the individual notification:



Chapter 10
Maintenance

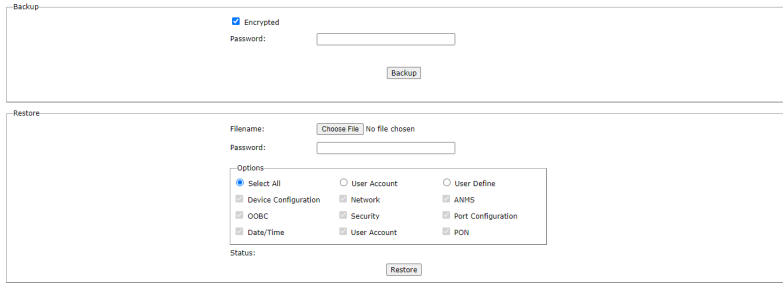
Overview

The *Maintenance* function is used to upgrade firmware; backup and restore configuration and account information; and restore default values.



Backup / Restore

When you click on the *Maintenance* tab, it opens with the Backup/Restore page. This page gives you the ability to back up the Serial Console Server's configuration and user profile information:



Backup

To backup the device's settings do the following:

1. If you do not want your backup configuration encrypted, uncheck the *Encrypted* checkbox, or check the *Encrypted* checkbox and key in a password for the backup configuration in the *Password* field.

   Note: 1. Setting a password for the encrypted backup configuration is optional. If you do not set one, the file can be restored without specifying a password.

   2. If you do set a password, make a note of it, since you will need it to be able to restore the file.

   3. When the backup configuration is unencrypted, you can modify the backup configuration and only the settings of Device Management and Port Properties are modifiable.

2. Click **Backup**.
3. When the browser asks what you want to do with the file, select *Save to disk*; then save it in a convenient location.

Restore

Restoring an Encrypted Backup

To restore a previous backup, do the following:

1. Click **Browse**; navigate to the file and select it.

   Note: If you renamed the file, you can leave the new name. There is no need to return it to its original name.

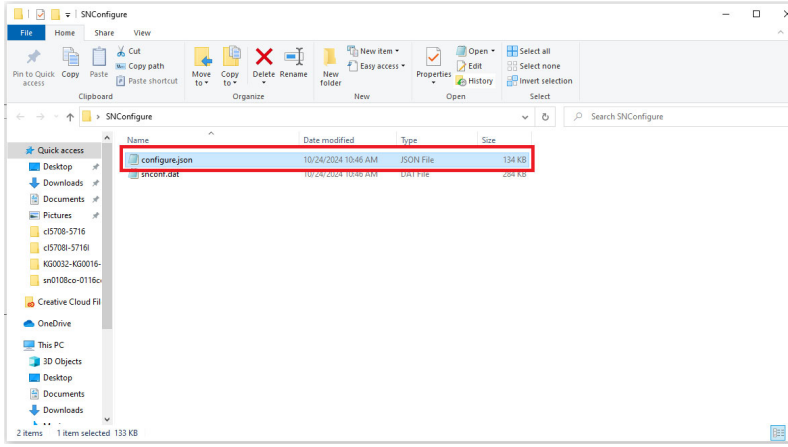
2. If you set a password when you created the file, key it in the *Password* field.
3. Select as many of the options that are presented as you wish to restore.
4. Click **Restore**.

   After the file is restored, a message appears to inform you that the procedure succeeded.

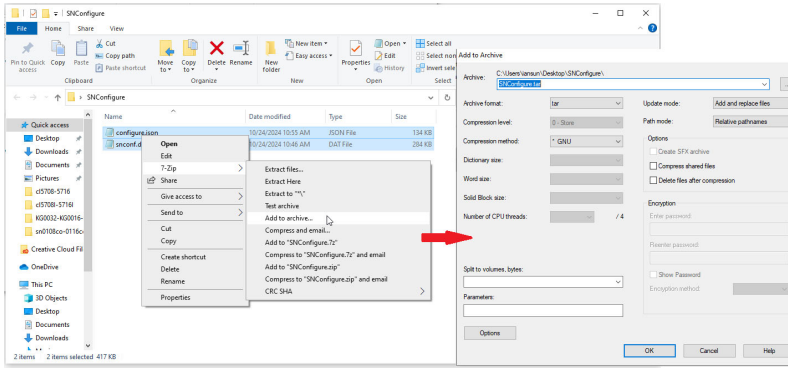
Modifying and Restoring an Unencrypted Backup

To modify and restore a previous backup, do the following:

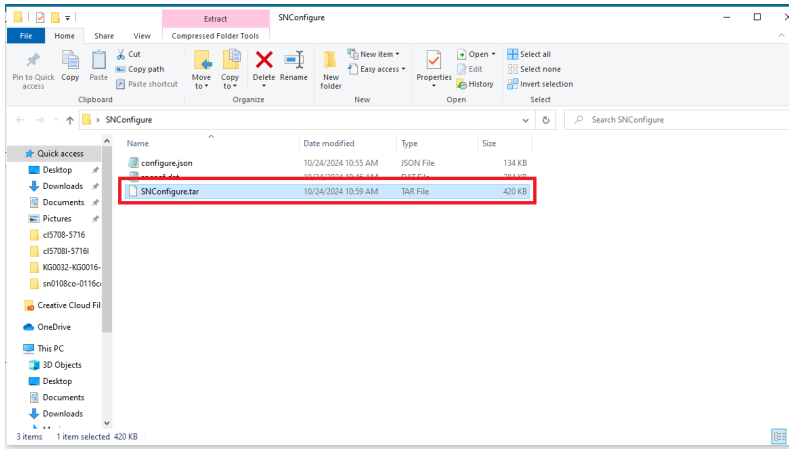
1. Unzip the backup file .tar (e.g., SNConfigure.tar).
2. Double-click the unzipped file folder, locate the file .json (e.g., configure.json), and open it using Notepad.



3. Modify the configuration and save it. Only the settings of Device Management and Port Properties are modifiable.
4. Zip both files into a tar file.



5. A file .tar (e.g., SNConfigure.tar) should appear in the file folder.



6. Click **Browse**; navigate to the file and select it.

Note: If you renamed the file, you can leave the new name. There is no need to return it to its original name.

7. If you set a password when you created the file, key it in the *Password* field.
8. Select as many of the options that are presented as you wish to restore.
9. Click **Restore**.

   After the file is restored, a message appears to inform you that the procedure succeeded.

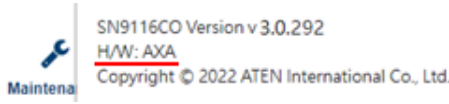
Note: If your modified settings did not apply after the restore, it means that the system detects incorrect parameters or formats in your .json file (e.g., configure.json) and the system automatically restores the .dat file (e.g., snconf.dat) instead.

Firmware Upgrade

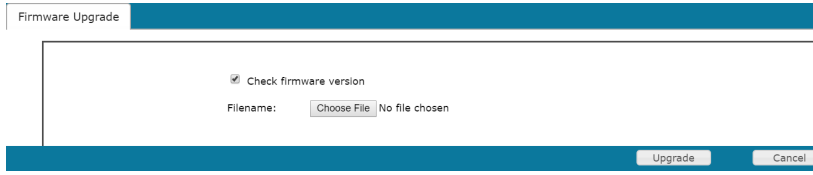
To upgrade the main firmware, do the following:

1. Check the hardware platform (AX or AXA) of the Serial Console Server by clicking ? from the web interface.

   For example:



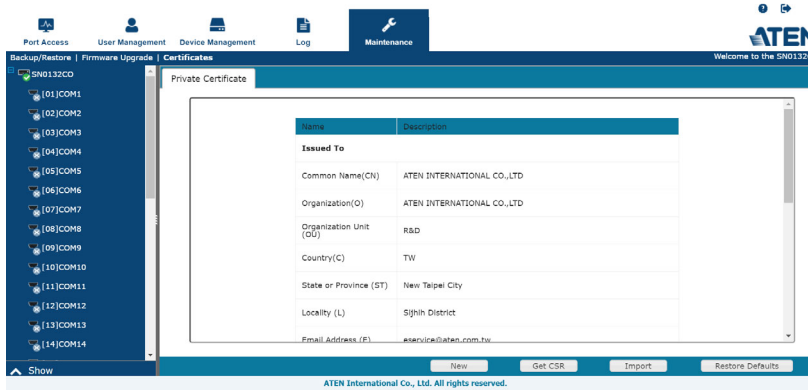
2. Download a firmware file based on the hardware platform of your Serial Console Server.
3. Log in to the Serial Console Server and click the *Maintenance* tab. Then, open the *Firmware Upgrade* page:



4. Click **Browse**; navigate to the directory that the new firmware file is in and select the file.
5. Click **Upgrade Firmware** to start the upgrade procedure.
   - If you enabled *Check Firmware Version* the current firmware level is compared with that of the upgrade file. If the current version is equal to or higher than the upgrade version, a popup message appears, to inform you of the situation and stops the upgrade procedure.
   - If you didn't enable *Check Firmware Version*, the upgrade file is installed without checking what its level is.
   - As the upgrade proceeds, progress information is shown in the *Progress* bar.
   - Once the upgrade completes successfully, the Serial Console Server resets itself.
6. Log in again, and check the firmware version to be sure it is the new one.

Certificates

This page provides information on the Private Certificates:



Private Certificate

When logging in over a secure (SSL) connection, a signed certificate is used to verify that the user is logging in to the intended site. For enhanced security, the *Private Certificate* section allows you to use your own private encryption key and signed certificate, rather than the default ATEN certificate.

- There are two methods for establishing your private certificate: generating a self-signed certificate; and importing a third-party certificate authority (CA) signed certificate.
- Obtaining a CA-Signed SSL Server Certificate

  For the greatest security, we recommend using a third-party certificate authority (CA) signed certificate. To obtain a third-party-signed certificate, see *Certificate Signing Request*, page 179.
- Generating a Self-Signed Certificate

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

  Privately-trusted SSL/TLS certificates should only be used to authenticate users and devices within an **internal** network. See *Self-signing SSL/TLS Certificate*, page 275 for details.

Note: Clicking **Restore Defaults** returns the device to using the default ATEN certificate.

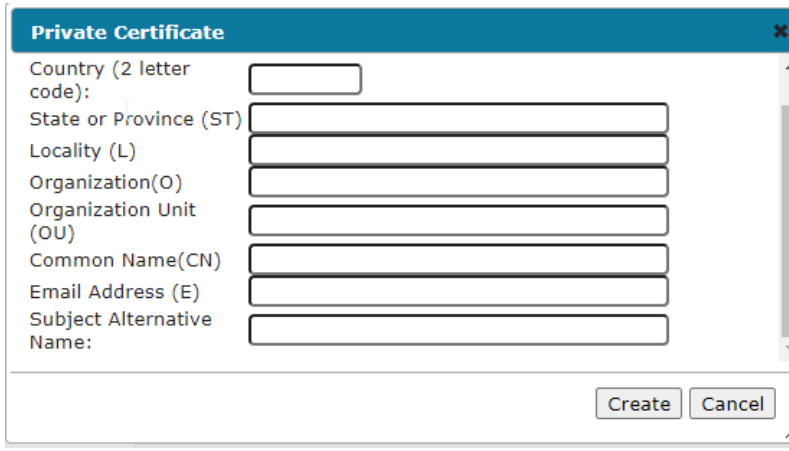
Certificate Signing Request

The Certificate Signing Request (CSR) section provides an automated way of obtaining and installing a CA-signed SSL server certificate.



To perform this operation do the following:

1. Click **New**. The following dialog box appears:



2. Fill in the form – with entries that are valid for your site – according to the example information in the following table:

Information	Example
Country (2 letter code)	TW
State or Province	Taiwan
Locality	Taipei
Organization	Your Company, Ltd.
Unit	Tech Department
Common Name	mycompany.com **Note:** This must be the exact domain name of the site that you want the certificate to be valid for. If the site's domain name is *www.mycompany.com*, and you only specify *mycompany.com*, the certificate will not be valid.
Email Address	administrator@yourcompany.com

Information	Example
Subject Alternative Name	DNS: aten.com email: ian@aten.com.tw URI: http://www.aten.com.tw IP: 10.0.0.1 **Note:** Only PEM format is supported.

3. After filling in the form (all fields are required), click **Create**.

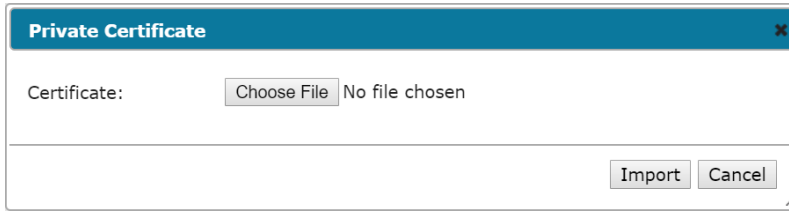
   A self-signed certificate based on the information you just provided is now stored into the SN device.

4. Click **Get CSR**, and save the certificate file (*custom.csr*) to a convenient location on your computer.

   This is the file that you give to the third party CA to apply for their signed SSL certificate.

5. After the CA sends you the certificate, save it to a convenient location on your computer.

6. Click **Import** from the lower menu bar and the *Private Certificate* window pops up, as shown here:



7. Click **Choose File** to locate the certificate and select it as the *Certificate Filename*; then click **Import** to store it on the Serial Console Server.

Note: When you upload the file, the Serial Console Server checks the file to make sure the specified information still matches. If it does, the file is accepted; if not, it is rejected.

If you want to remove the certificate (to replace it with a new one because of a domain name change, for example), simply click **Restore Defaults**.

Chapter 11
MIB Reference

Overview

This section provides information about the MIBs supported on Serial Console Servers. Refer to the following table for the latest supported MIB version for each product series.

Serial Console Servers		MIB Version
Product Series	**Models**	
SN01xx Series	SN0108CO, SN0116CO, SN0132CO, SN0148CO	v3.3.327
SN91xx Series	SN9108CO, SN9116CO	
SN11xx Series	SN1116CO, SN1132CO, SN1148CO	v1.1.102

This section provides detailed information required for integration with network management systems, automated monitoring, and event handling. Specifically, the section covers:

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

MIB Tree Structure

- **atenProducts** (.1.3.6.1.4.1.21317.1)
  This is the root node for all ATEN products.
- **overip** (.1.3.6.1.4.1.21317.1.3)
  This is a subtree for ATEN IP-based products.
  - **serialoverip** (.1.3.6.1.4.1.21317.1.3.3)
    Defines the MIB objects and traps for ATEN Serial Console Servers.
    - **SN01xx series & SN91xx series** (.1.3.6.1.4.1.21317.1.3.3.3)
    - **SN11xx series** (.1.3.6.1.4.1.21317.1.3.3.7)

Downloading MIB Files

To download the latest MIB files:

1. Visit the official product page of your target serial console server.
2. Scroll down to locate the **MIB File** section. For example:



MIB File				
	MIB Files	v3.2.318	2025-01-07	SN-Mibs-File-v3.2.318.004.zip
	MIB Files	v1.8.179	2024-11-07	SN-Mibs-File-v1.8.179.006.zip

3. Download the latest MIB file.

OID Format

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

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

```
.1.3.6.1.4.1.21317.1.2.1.1.1.1.0
```

In this document, it is written as:

```
1.3.6.1.4.1.21317.1.2.1.1.1.1.0
```

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

Object Types and Indexing

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

- **Scalar Objects**

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

  For example:

  If the `DeviceName` object is defined as:

Object Name	OID
DeviceName	1.3.6.1.4.1.21317.1.3.3.3.7.1

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

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

  Result:

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

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

- **Instance Objects**

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

  For example:

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

and the device has two interfaces:

Interface Index	Description
1	Ethernet 0
2	Ethernet 1

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

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

SN01xx and SN91xx Series

This section lists and defines the MIB objects used for the SN01xx and SN91xx series:

- *RS-232 Objects*
- *Session Management Objects*
- *Firmware Management Object*
- *Device Management Objects*
- *ANMS Objects*
- *Security Objects*
- *Manufacturer Information Object*
- *Network Objects*

RS-232 Objects

General

- `rs232Number`

OID	`1.3.6.1.4.1.21317.1.3.3.3.1.1`
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The number of ports (regardless of their current state) in the RS-232-like general port table

RS-232 Port Configuration

- `rs232PortIndex`

OID	`1.3.6.1.4.1.21317.1.3.3.3.1.2.1.1`
Syntax	InterfaceIndex
Max-Access	read-only
Status	current
Description	The value of ifIndex for the port

- rs232PortType

OID	1.3.6.1.4.1.21317.1.3.3.3.1.2.1.2
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The port's hardware type: rs232ATEN(0),rs232CISCO(1), rs422(2), rs485(3)

- rs232PortInSigNumber

OID	1.3.6.1.4.1.21317.1.3.3.3.1.2.1.3
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The number of input signals for the port in the input signal table

- rs232PortOutSigNumber

OID	1.3.6.1.4.1.21317.1.3.3.3.1.2.1.4
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The number of output signals for the port in the output signal table

- rs232PortInSpeed

OID	1.3.6.1.4.1.21317.1.3.3.3.1.2.1.5
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The port's input speed in bits per second

- rs232PortOutSpeed

OID	1.3.6.1.4.1.21317.1.3.3.3.1.2.1.6
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The port's output speed in bits per second

- rs232PortInFlowType

OID	1.3.6.1.4.1.21317.1.3.3.3.1.2.1.7
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The port's type of input flow control: none(1), ctsRts(2), dsrDtr(3)

- rs232PortOutFlowType

OID	1.3.6.1.4.1.21317.1.3.3.3.1.2.1.8
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The port's type of output flow control: none(1), ctsRts(2), dsrDtr(3)

- rs232PortName

OID	1.3.6.1.4.1.21317.1.3.3.3.1.2.1.9
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	Port Name, should be utf-8 coding, newly added for SN01xx series and SN91xx series.

- rs232ToggleDTR

OID	1.3.6.1.4.1.21317.1.3.3.3.1.2.1.10
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	Toggle DTR, newly added for SN0148: disable(0), enable(1)

- rs232OnlineStatus

OID	1.3.6.1.4.1.21317.1.3.3.3.1.2.1.11
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	Online status, newly added for SN0148: online, offline, busy

- rs232OperatingMode

OID	1.3.6.1.4.1.21317.1.3.3.3.1.2.1.12
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	Operating Mode (WorkMode), newly added for SN01xx series and SN91xx series

- rs232SocketPort

OID	1.3.6.1.4.1.21317.1.3.3.3.1.2.1.13
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	rs232SocketPort, newly added for SN01xx series and SN91xx series

Async Port

- `rs232AsyncPortIndex`

OID	`1.3.6.1.4.1.21317.1.3.3.3.1.3.1.1`
Syntax	InterfaceIndex
Max-Access	read-only
Status	current
Description	A unique value for each port. Its value is the same as rs232PortIndex for the port.

- `rs232AsyncPortBits`

OID	`1.3.6.1.4.1.21317.1.3.3.3.1.3.1.2`
Syntax	INTEGER (5..8)
Max-Access	read-only
Status	current
Description	The number of data bits used in each character for this port

- `rs232AsyncPortStopBits`

OID	`1.3.6.1.4.1.21317.1.3.3.3.1.3.1.3`
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The port's number of stop bits: one(1), two(2), oneAndHalf(3), dynamic(4)

- `rs232AsyncPortParity`

OID	`1.3.6.1.4.1.21317.1.3.3.3.1.3.1.4`
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The port's parity sense for each character: none(1), odd(2), even(3), mark(4), space(5)

- rs232AsyncPortAutobaud

OID	1.3.6.1.4.1.21317.1.3.3.3.1.3.1.5
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	A control for the port's ability to automatically sense input speed: enabled(1), disabled(2)

RS-232 Input Signals

- rs232InSigPortIndex

OID	1.3.6.1.4.1.21317.1.3.3.3.1.5.1.1
Syntax	InterfaceIndex
Max-Access	read-only
Status	current
Description	The value of rs232PortIndex for the port to which this entry belongs

- rs232InSigName

OID	1.3.6.1.4.1.21317.1.3.3.3.1.5.1.2
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	Identification of a hardware signal: rts(1), cts(2), dsr(3), dtr(4), ri(5), dcd(6), sq(7), srs(8), srts(9), scts(10), sdcd(11)

- rs232InSigState

OID	1.3.6.1.4.1.21317.1.3.3.3.1.5.1.3
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The current signal state: none(1), on(2), off(3)

RS-232 Output Signals

- `rs232OutSigPortIndex`

OID	`1.3.6.1.4.1.21317.1.3.3.3.1.6.1.1`
Syntax	InterfaceIndex
Max-Access	read-only
Status	current
Description	The value of rs232PortIndex for the port to which this entry belongs

- `rs232OutSigName`

OID	`1.3.6.1.4.1.21317.1.3.3.3.1.6.1.2`
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	Identification of a hardware signal: rts(1), cts(2), dsr(3), dtr(4), ri(5), dcd(6), sq(7), srs(8), srts(9), scts(10), sdcd(11)

- `rs232OutSigState`

OID	`1.3.6.1.4.1.21317.1.3.3.3.1.6.1.3`
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The current signal state: none(1), on(2), off(3)

RS-232 Operating Info

- rs232PortOperatingIndex

OID	1.3.6.1.4.1.21317.1.3.3.3.1.7.1.1
Syntax	InterfaceIndex
Max-Access	read-only
Status	current
Description	The value of ifIndex for the port

- rs232MaxSessions

OID	1.3.6.1.4.1.21317.1.3.3.3.1.7.1.2
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	The max number of sessions for the port

- rs232SuspendChar

OID	1.3.6.1.4.1.21317.1.3.3.3.1.7.1.3
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	The suspend character for the port

- rs232AccessMode

OID	1.3.6.1.4.1.21317.1.3.3.3.1.7.1.4
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	The access mode for the port

- rs232OccupyTimeout

OID	1.3.6.1.4.1.21317.1.3.3.3.1.7.1.5
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	The occupy timeout for the port

- rs232ExitMacro

OID	1.3.6.1.4.1.21317.1.3.3.3.1.7.1.6
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	The exit macro for the port

- rs232ConnProtocol

OID	1.3.6.1.4.1.21317.1.3.3.3.1.7.1.7
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	The connection protocol for the port

- rs232OutCRLFTranslation

OID	1.3.6.1.4.1.21317.1.3.3.3.1.7.1.8
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	The out CRLF translation for the port

Session Management Objects

sessionNumber

OID	1.3.6.1.4.1.21317.1.3.3.3.3.1
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The number of active sessions in the SN01xx series and SN91xx series

- sessionIndex

OID	1.3.6.1.4.1.21317.1.3.3.3.3.2.1.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The value of session Index for the session

- sessionOwner

OID	1.3.6.1.4.1.21317.1.3.3.3.3.2.1.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The name of the user who started this session

- sessionService

OID	1.3.6.1.4.1.21317.1.3.3.3.3.2.1.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	HTTP, HTTPS, and so on.

- sessionIP

OID	1.3.6.1.4.1.21317.1.3.3.3.3.2.1.4
Syntax	IpAddress
Max-Access	read-only
Status	current
Description	The network address (e.g., the IP address) of connection

- sessionUpTime

OID	1.3.6.1.4.1.21317.1.3.3.3.3.2.1.5
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The time when the session was last initialized

- sessionLastAccess

OID	1.3.6.1.4.1.21317.1.3.3.3.3.2.1.6
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The time when the session was last accessed

- sessionPortNumber

OID	1.3.6.1.4.1.21317.1.3.3.3.3.2.1.7
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The port number of the session

- sessionOwnerType

OID	1.3.6.1.4.1.21317.1.3.3.3.3.2.1.8
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The user type of the current user: SuperAdmin(0), Admin(1), User(2)

Firmware Management Object

currentVersion

OID	1.3.6.1.4.1.21317.1.3.3.3.4.1
Syntax	DisplayString (SIZE (0..255))
Max-Access	read-only
Status	current
Description	The current version of image of SN01xx series and SN91xx series

Device Management Objects

- DeviceName

OID	1.3.6.1.4.1.21317.1.3.3.3.7.1
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The name for the device

- PSU1

OID	1.3.6.1.4.1.21317.1.3.3.3.7.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The device power 1 status

- PSU2

OID	1.3.6.1.4.1.21317.1.3.3.3.7.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The device power 2 status

- ModelName

OID	1.3.6.1.4.1.21317.1.3.3.3.7.4
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The model name of device

- MFG

OID	1.3.6.1.4.1.21317.1.3.3.3.7.5
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The MFG of device

Date/Time

- NTP-Status

OID	1.3.6.1.4.1.21317.1.3.3.3.7.7.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The NTP status of the device: Disabled(0), Enabled(1)

- NTP-Server

OID	1.3.6.1.4.1.21317.1.3.3.3.7.7.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The NTP server used by the device

- Timezone

OID	1.3.6.1.4.1.21317.1.3.3.3.7.7.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The device's time zone

- MemoryUsage

OID	1.3.6.1.4.1.21317.1.3.3.3.7.8
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The memory information for the device

- CPUUsage

OID	1.3.6.1.4.1.21317.1.3.3.3.7.9
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The CPU information for the device

ANMS Objects

SNMP

- SNMP_Enable

OID	1.3.6.1.4.1.21317.1.3.3.3.11.14.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The status of SNMP: False(0), True(1)

- SNMP_Port

OID	1.3.6.1.4.1.21317.1.3.3.3.11.14.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The port number of SNMP

- SNMP_V3_Enable

OID	1.3.6.1.4.1.21317.1.3.3.3.11.14.3
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The status of SNMP V3: False(0), True(1)

- SNMP_Trap_Enable

OID	1.3.6.1.4.1.21317.1.3.3.3.11.14.4
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The status of SNMP Trap: False(0), True(1)

- SNMP_Agent_Community

OID	1.3.6.1.4.1.21317.1.3.3.3.11.14.5
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The Community of SNMP Agent

- SNMP_Trap_Receiver

OID	1.3.6.1.4.1.21317.1.3.3.3.11.14.6
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The Receiver of SNMP Trap

SMTP

- SMTP_Enable

OID	1.3.6.1.4.1.21317.1.3.3.3.11.15.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The status of SMTP: False(0), True(1)

- SMTP_Server

OID	1.3.6.1.4.1.21317.1.3.3.3.11.15.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The server of SMTP

- SMTP_Port

OID	1.3.6.1.4.1.21317.1.3.3.3.11.15.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The port number of SMTP

Log Server

- LogServer_Enable

OID	1.3.6.1.4.1.21317.1.3.3.3.11.16.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The status of Log Server: False(0), True(1)

- LogServer_MAC

OID	1.3.6.1.4.1.21317.1.3.3.3.11.16.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The MAC address of the Log Server

- LogServer_Port

OID	1.3.6.1.4.1.21317.1.3.3.3.11.16.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The port number of the Log Server

Syslog Server

- SyslogServer_Enable

OID	1.3.6.1.4.1.21317.1.3.3.3.11.17.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The status of the Syslog Server: False(0), True(1)

- SyslogServer_IP

OID	1.3.6.1.4.1.21317.1.3.3.3.11.17.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The server IP address of the Syslog Server

- SyslogServer_Port

OID	1.3.6.1.4.1.21317.1.3.3.3.11.17.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The port number of the Syslog Server

- SyslogServer_Enable2

OID	1.3.6.1.4.1.21317.1.3.3.3.11.17.4
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The status of Syslog Server 2: False(0), True(1)

- SyslogServer_IP2

OID	1.3.6.1.4.1.21317.1.3.3.3.11.17.5
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The server IP address of Syslog Server 2

- SyslogServer_Port2

OID	1.3.6.1.4.1.21317.1.3.3.3.11.17.6
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The port number of Syslog Server 2

CC Management

- CCManagement_Enable

OID	1.3.6.1.4.1.21317.1.3.3.3.11.18.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The status of CC2000: False(0), True(1)

- CCManagement_Server

OID	1.3.6.1.4.1.21317.1.3.3.3.11.18.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The server IP of CC2000

- CCManagement_Port

OID	1.3.6.1.4.1.21317.1.3.3.3.11.18.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The port number of CC2000

External USB

- ExternalUSB_Enable

OID	1.3.6.1.4.1.21317.1.3.3.3.11.19.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The status of external USB drive: False(0), True(1)

Security Objects

SecurityLevel

- TelnetServiceEnable

OID	1.3.6.1.4.1.21317.1.3.3.3.13.1.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The Telnet setting of the device: False(0), True(1)

- SSHServiceEnable

OID	1.3.6.1.4.1.21317.1.3.3.3.13.1.2
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The SSH setting of the device: False(0), True(1)

AccountPolicy

- AccountPolicyMinUsername

OID	1.3.6.1.4.1.21317.1.3.3.3.13.2.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The minimum required username of the device

- AccountPolicyMinPassword

OID	1.3.6.1.4.1.21317.1.3.3.3.13.2.2
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The minimum required password of the device

Manufacturer Information Object

- manufacturerInfo

OID	1.3.6.1.4.1.21317.1.3.3.3.14.1
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The manufacturer information

Network Objects

Service Ports

- HTTP

OID	1.3.6.1.4.1.21317.1.3.3.3.15.1.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The HTTP port

- HTTPs

OID	1.3.6.1.4.1.21317.1.3.3.3.15.1.2
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The HTTPs port

- SSH

OID	1.3.6.1.4.1.21317.1.3.3.3.15.1.3
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The SSH port

- Telnet

OID	1.3.6.1.4.1.21317.1.3.3.3.15.1.4
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The Telnet port

- BaseSocket

OID	1.3.6.1.4.1.21317.1.3.3.3.15.1.5
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The base socket

LAN Port: ETH0

- ETH0_MAC

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.1.1
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The MAC for ETH0

ETH0 IPv4

- ETH0_IPV4_IP

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.1.2.1
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV4 IP of ETH0

- ETH0_IPV4_Subnet

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.1.2.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV4 subnet mask of ETH0

- ETH0_IPV4_gateway

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.1.2.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV4 gateway of ETH0

- ETH0_IPV4_DNS_Preferred

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.1.2.4
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The preferred IPV4 DNS of ETH0

- ETH0_IPV4_DNS_Alternate

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.1.2.5
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The alternate IPV4 DNS of ETH0

ETH0 IPv6

- ETH0_IPV6_IP

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.1.3.1
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV6 IP of ETH0

- ETH0_IPV6_Prefix

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.1.3.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV6 subnet mask of ETH0

- ETH0_IPV6_gateway

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.1.3.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV6 gateway of ETH0

- ETH0_IPV6_DNS_Preferred

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.1.3.4
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The preferred IPV6 DNS of ETH0

- ETH0_IPV6_DNS_Alternate

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.1.3.5
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The alternate IPV6 DNS of ETH0

LAN Port: ETH1

- ETH1_MAC

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.2.1
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The MAC for ETH1

ETH1 IPv4

- ETH1_IPV4_IP

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.2.2.1
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV4 IP of ETH1

- ETH1_IPV4_Subnet

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.2.2.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV4 subnet mask of ETH1

- ETH1_IPV4_gateway

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.2.2.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV4 gateway of ETH

- ETH1_IPV4_DNS_Preferred

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.2.2.4
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The preferred IPV4 DNS of ETH1

- ETH1_IPV4_DNS_Alternate

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.2.2.5
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The alternate IPV4 DNS of ETH1

ETH1 IPv6

- ETH1_IPV6_IP

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.2.3.1
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV6 IP of ETH1

- ETH1_IPV6_Prefix

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.2.3.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV6 subnet mask of ETH1

- ETH1_IPV6_gateway

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.2.3.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV6 gateway of ETH1

- ETH1_IPV6_DNS_Preferred

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.2.3.4
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The preferred IPV6 DNS of ETH1

- ETH1_IPV6_DNS_Alternate

OID	1.3.6.1.4.1.21317.1.3.3.3.15.2.2.3.5
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The alternate IPV6 DNS of ETH1

General

- RedundantNICEnable

OID	1.3.6.1.4.1.21317.1.3.3.3.15.3
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The redundant NIC enable status of the device: False(0), True(1)

- IPv6Enable

OID	1.3.6.1.4.1.21317.1.3.3.3.15.4
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The IPv6 enable status of the device: False(0), True(1)

SN11xx Series

This section lists the supported objects for the SN11xx series:

- *RS-232 Objects*
- *Session Management Objects*
- *Firmware Management Object*
- *Device Management Objects*
- *Sensor Objects*
- *ANMS Objects*
- *Security Objects*
- *Manufacturer Information Object*
- *Network Objects*

RS-232 Objects

General

- `rs232Number`

OID	`1.3.6.1.4.1.21317.1.3.3.7.1.1`
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The number of ports (regardless of their current state) in the RS-232-like general port table

RS-232 Port Configuration

- `rs232PortIndex`

OID	`1.3.6.1.4.1.21317.1.3.3.7.1.2.1.1`
Syntax	InterfaceIndex
Max-Access	read-only
Status	current
Description	The value of ifIndex for the port

- rs232PortType

OID	1.3.6.1.4.1.21317.1.3.3.7.1.2.1.2
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The port's hardware type: rs232ATEN(0), rs232CISCO(1), rs422(2), rs485(3)

- rs232PortInSigNumber

OID	1.3.6.1.4.1.21317.1.3.3.7.1.2.1.3
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The number of input signals for the port in the input signal table

- rs232PortOutSigNumber

OID	1.3.6.1.4.1.21317.1.3.3.7.1.2.1.4
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The number of output signals for the port in the output signal table

- rs232PortInSpeed

OID	1.3.6.1.4.1.21317.1.3.3.7.1.2.1.5
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The port's input speed in bits per second

- rs232PortOutSpeed

OID	1.3.6.1.4.1.21317.1.3.3.7.1.2.1.6
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The port's output speed in bits per second

- rs232PortInFlowType

OID	1.3.6.1.4.1.21317.1.3.3.7.1.2.1.7
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The port's type of input flow control: none(1), ctsRts(2), dsrDtr(3)

- rs232PortOutFlowType

OID	1.3.6.1.4.1.21317.1.3.3.7.1.2.1.8
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The port's type of output flow control: none(1), ctsRts(2), dsrDtr(3)

- rs232PortName

OID	1.3.6.1.4.1.21317.1.3.3.7.1.2.1.9
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	Port Name, should be utf-8 coding, newly added for SN11xx series

- rs232ToggleDTR

OID	1.3.6.1.4.1.21317.1.3.3.7.1.2.1.10
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	Toggle DTR, newly added for SN11xx series: disable(0), enable(1)

- rs232OnlineStatus

OID	1.3.6.1.4.1.21317.1.3.3.7.1.2.1.11
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	Online status, newly added for SN11XXseries: online, offline, busy

- rs232OperatingMode

OID	1.3.6.1.4.1.21317.1.3.3.7.1.2.1.12
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	Operating Mode (WorkMode), newly added for SN11xx series

- rs232SocketPort

OID	1.3.6.1.4.1.21317.1.3.3.7.1.2.1.13
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	rs232SocketPort, newly added for SN11xx series

Async Port

- rs232AsyncPortIndex

OID	1.3.6.1.4.1.21317.1.3.3.7.1.3.1.1
Syntax	InterfaceIndex
Max-Access	read-only
Status	current
Description	A unique value for each port. Its value is the same as rs232PortIndex for the port.

- rs232AsyncPortBits

OID	1.3.6.1.4.1.21317.1.3.3.7.1.3.1.2
Syntax	INTEGER (5..8)
Max-Access	read-only
Status	current
Description	The number of data bits used in each character for the port

- rs232AsyncPortStopBits

OID	1.3.6.1.4.1.21317.1.3.3.7.1.3.1.3
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The port's number of stop bits: one(1), two(2), oneAndHalf(3), dynamic(4)

- rs232AsyncPortParity

OID	1.3.6.1.4.1.21317.1.3.3.7.1.3.1.4
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The port's parity sense for each character: none(1), odd(2), even(3), mark(4), space(5)

- rs232AsyncPortAutobaud

OID	1.3.6.1.4.1.21317.1.3.3.7.1.3.1.5
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	A control for the port's ability to automatically sense input speed: enabled(1), disabled(2)

RS-232 Input Signals

- rs232InSigPortIndex

OID	1.3.6.1.4.1.21317.1.3.3.7.1.5.1.1
Syntax	InterfaceIndex
Max-Access	read-only
Status	current
Description	The value of rs232PortIndex for the port to which this entry belongs

- rs232InSigName

OID	1.3.6.1.4.1.21317.1.3.3.7.1.5.1.2
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	Identification of a hardware signal: rts(1), cts(2), dsr(3), dtr(4), ri(5), dcd(6), sq(7), srs(8), srts(9), scts(10), sdcd(11)

- rs232InSigState

OID	1.3.6.1.4.1.21317.1.3.3.7.1.5.1.3
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The current signal state: none(1), on(2), off(3)

RS-232 Output Signals

- `rs232OutSigPortIndex`

OID	`1.3.6.1.4.1.21317.1.3.3.7.1.6.1.1`
Syntax	InterfaceIndex
Max-Access	read-only
Status	current
Description	The value of rs232PortIndex for the port to which this entry belongs

- `rs232OutSigName`

OID	`1.3.6.1.4.1.21317.1.3.3.7.1.6.1.2`
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	Identification of a hardware signal: (rts(1), cts(2), dsr(3), dtr(4), ri(5), dcd(6), sq(7), srs(8), srts(9), scts(10), sdcd(11)

- `rs232OutSigState`

OID	`1.3.6.1.4.1.21317.1.3.3.7.1.6.1.3`
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The current signal state: none(1), on(2), off(3)

RS-232 Operating Info

- rs232PortOperatingIndex

OID	1.3.6.1.4.1.21317.1.3.3.7.1.7.1.1
Syntax	InterfaceIndex
Max-Access	read-only
Status	current
Description	The value of ifIndex for the port

- rs232MaxSessions

OID	1.3.6.1.4.1.21317.1.3.3.7.1.7.1.2
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	The max number of sessions for the port

- rs232SuspendChar

OID	1.3.6.1.4.1.21317.1.3.3.7.1.7.1.3
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	The suspend character for the port

- rs232AccessMode

OID	1.3.6.1.4.1.21317.1.3.3.7.1.7.1.4
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	The access mode for the port

- rs232OccupyTimeout

OID	1.3.6.1.4.1.21317.1.3.3.7.1.7.1.5
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	The occupy timeout for the port

- rs232ExitMacro

OID	1.3.6.1.4.1.21317.1.3.3.7.1.7.1.6
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	The exit macro for the port

- rs232ConnProtocol

OID	1.3.6.1.4.1.21317.1.3.3.7.1.7.1.7
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	The connection protocol for the port

- rs232OutCRLFTranslation

OID	1.3.6.1.4.1.21317.1.3.3.7.1.7.1.8
Syntax	DisplayString (SIZE (0..64))
Max-Access	read-only
Status	current
Description	The out CRLF translation for the port

Session Management Objects

sessionNumber

OID	1.3.6.1.4.1.21317.1.3.3.7.3.1
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The number of active sessions in the SN11XXseries

- sessionIndex

OID	1.3.6.1.4.1.21317.1.3.3.7.3.2.1.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The value of session Index for the session

- sessionOwner

OID	1.3.6.1.4.1.21317.1.3.3.7.3.2.1.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The name of the user who started the session.

- sessionService

OID	1.3.6.1.4.1.21317.1.3.3.7.3.2.1.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	HTTP, HTTPS, and so on

- sessionIP

OID	1.3.6.1.4.1.21317.1.3.3.7.3.2.1.4
Syntax	IpAddress
Max-Access	read-only
Status	current
Description	The Network Address (e.g., the IP address) of connection

- sessionUpTime

OID	1.3.6.1.4.1.21317.1.3.3.7.3.2.1.5
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The time when the session was last initialized

- sessionLastAccess

OID	1.3.6.1.4.1.21317.1.3.3.7.3.2.1.6
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The time when the session was last accessed

- sessionPortNumber

OID	1.3.6.1.4.1.21317.1.3.3.7.3.2.1.7
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The port number of the session

- sessionOwnerType

OID	1.3.6.1.4.1.21317.1.3.3.7.3.2.1.8
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The user type of the current user: SuperAdmin(0), Admin(1), User(2)

Firmware Management Object

currentVersion

OID	1.3.6.1.4.1.21317.1.3.3.7.4.1
Syntax	DisplayString (SIZE (0..255))
Max-Access	read-only
Status	current
Description	The current version of image of SN11xx series

Device Management Objects

- DeviceName

OID	1.3.6.1.4.1.21317.1.3.3.7.7.1
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The name for the device

- PSU1

OID	1.3.6.1.4.1.21317.1.3.3.7.7.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The status of device power 1

- PSU2

OID	1.3.6.1.4.1.21317.1.3.3.7.7.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The status of device power 2

- ModelName

OID	1.3.6.1.4.1.21317.1.3.3.7.7.4
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The model name of device

- MFG

OID	1.3.6.1.4.1.21317.1.3.3.7.7.5
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The MFG of device

Date/Time

- NTP-Status

OID	1.3.6.1.4.1.21317.1.3.3.7.7.7.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The NTP status of the device: Disabled(0), Enabled(1)

- NTP-Server

OID	1.3.6.1.4.1.21317.1.3.3.7.7.7.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The NTP server used by the device

- Timezone

OID	1.3.6.1.4.1.21317.1.3.3.7.7.7.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The device's time zone

Sensor Objects

Sensor 1

- SENSOR1_Summary

OID	1.3.6.1.4.1.21317.1.3.3.7.7.8.1.1
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The summary of SENSOR1

- SENSOR1_T

OID	1.3.6.1.4.1.21317.1.3.3.7.7.8.1.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The temperature of SENSOR1

- SENSOR1_H

OID	1.3.6.1.4.1.21317.1.3.3.7.7.8.1.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The humidity of SENSOR1

- SENSOR1_P

OID	1.3.6.1.4.1.21317.1.3.3.7.7.8.1.4
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The pressure of SENSOR1

Sensor 2

- SENSOR2_Summary

OID	1.3.6.1.4.1.21317.1.3.3.7.7.8.2.1
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The summary of SENSOR2

- SENSOR2_T

OID	1.3.6.1.4.1.21317.1.3.3.7.7.8.2.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The temperature of SENSOR2

- SENSOR2_H

OID	1.3.6.1.4.1.21317.1.3.3.7.7.8.2.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The humidity of SENSOR2

- SENSOR2_P

OID	1.3.6.1.4.1.21317.1.3.3.7.7.8.2.4
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The pressure of SENSOR2

Other Sensors

- SENSOR3

OID	1.3.6.1.4.1.21317.1.3.3.7.7.8.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The status of SENSOR3

- RELAY

OID	1.3.6.1.4.1.21317.1.3.3.7.7.8.4
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The status of RELAY

- MemoryUsage

OID	1.3.6.1.4.1.21317.1.3.3.7.7.9
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The memory information for the device

- CPUUsage

OID	1.3.6.1.4.1.21317.1.3.3.7.7.10
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The CPU information for the device

ANMS Objects

SNMP

- SNMP_Enable

OID	1.3.6.1.4.1.21317.1.3.3.7.11.14.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The status of SNMP: False(0), True(1)

- SNMP_Port

OID	1.3.6.1.4.1.21317.1.3.3.7.11.14.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The port number of SNMP

- SNMP_V3_Enable

OID	1.3.6.1.4.1.21317.1.3.3.7.11.14.3
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The status of SNMP V3: False(0), True(1)

- SNMP_Trap_Enable

OID	1.3.6.1.4.1.21317.1.3.3.7.11.14.4
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The status of SNMP Trap: False(0), True(1)

- SNMP_Agent_Community

OID	1.3.6.1.4.1.21317.1.3.3.7.11.14.5
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The Community of SNMP Agent

- SNMP_Trap_Receiver

OID	11.3.6.1.4.1.21317.1.3.3.7.11.14.6
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The Receiver of SNMP Trap

SMTP

- SMTP_Enable

OID	1.3.6.1.4.1.21317.1.3.3.7.11.15.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The status of SMTP: False(0), True(1)

- SMTP_Server

OID	1.3.6.1.4.1.21317.1.3.3.7.11.15.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The server of SMTP

- SMTP_Port

OID	11.3.6.1.4.1.21317.1.3.3.7.11.15.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The port number of SMTP

Log Server

- LogServer_Enable

OID	1.3.6.1.4.1.21317.1.3.3.7.11.16.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The status of the Log Server: False(0), True(1)

- LogServer_MAC

OID	1.3.6.1.4.1.21317.1.3.3.7.11.16.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The MAC address of the Log Server

- LogServer_Port

OID	1.3.6.1.4.1.21317.1.3.3.7.11.16.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The port number of the Log Server

Syslog Server

- SyslogServer_Enable

OID	1.3.6.1.4.1.21317.1.3.3.7.11.17.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The status of the Syslog Server: False(0), True(1)

- SyslogServer_IP

OID	1.3.6.1.4.1.21317.1.3.3.7.11.17.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The server IP of the Syslog Server

- SyslogServer_Port

OID	1.3.6.1.4.1.21317.1.3.3.7.11.17.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The port number of Syslog Server

- SyslogServer_Enable2

OID	1.3.6.1.4.1.21317.1.3.3.7.11.17.4
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The status of Syslog Server 2: False(0), True(1)

- SyslogServer_IP2

OID	1.3.6.1.4.1.21317.1.3.3.7.11.17.5
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The server IP of Syslog Server 2

- SyslogServer_Port2

OID	1.3.6.1.4.1.21317.1.3.3.7.11.17.6
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The port number of Syslog Server 2

CC Management

- CCManagement_Enable

OID	1.3.6.1.4.1.21317.1.3.3.7.11.18.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The status of CC2000: False(0), True(1)

- CCManagement_Server

OID	1.3.6.1.4.1.21317.1.3.3.7.11.18.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The server IP of CC2000

- CCManagement_Port

OID	1.3.6.1.4.1.21317.1.3.3.7.11.18.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The port number of CC2000

External USB

- ExternalUSB_Enable

OID	1.3.6.1.4.1.21317.1.3.3.7.11.19.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The status of external USB drive: False(0), True(1)

Security Objects

Security Level

- TelnetServiceEnable

OID	1.3.6.1.4.1.21317.1.3.3.7.13.1.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The Telnet setting of the device: False(0), True(1)

- SSHServiceEnable

OID	1.3.6.1.4.1.21317.1.3.3.7.13.1.2
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The SSH setting of the device: False(0), True(1)

Account Policy

- AccountPolicyMinUsername

OID	1.3.6.1.4.1.21317.1.3.3.7.13.2.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The minimum required username of the device

- AccountPolicyMinPassword

OID	1.3.6.1.4.1.21317.1.3.3.7.13.2.2
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The minimum required password of the device

Manufacturer Information Object

- `manufacturerInfo`

OID	`1.3.6.1.4.1.21317.1.3.3.7.14.1`
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The manufacturer information

Network Objects

Service Ports

- HTTP

OID	1.3.6.1.4.1.21317.1.3.3.7.15.1.1
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The HTTP port

- HTTPs

OID	1.3.6.1.4.1.21317.1.3.3.7.15.1.2
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The HTTPs port

- SSH

OID	1.3.6.1.4.1.21317.1.3.3.7.15.1.3
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The SSH port

- Telnet

OID	1.3.6.1.4.1.21317.1.3.3.7.15.1.4
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The Telnet port

- BaseSocket

OID	1.3.6.1.4.1.21317.1.3.3.7.15.1.5
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The base socket

LAN Port: ETH0

- ETH0_MAC

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.1.1
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The MAC for ETH0

ETH0 IPv4

- ETH0_IPV4_IP

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.1.2.1
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV4 IP of ETH0

- ETH0_IPV4_Subnet

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.1.2.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV4 subnet mask of ETH0

- ETH0_IPV4_gateway

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.1.2.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV4 gateway of ETH0

- ETH0_IPV4_DNS_Preferred

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.1.2.4
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The preferred IPV4 DNS of ETH0

- ETH0_IPV4_DNS_Alternate

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.1.2.5
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The alternate IPV4 DNS of ETH0

ETH0 IPv6

- ETH0_IPV6_IP

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.1.3.1
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV6 IP of ETH0

- ETH0_IPV6_Prefix

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.1.3.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV6 subnet mask of ETH0

- ETH0_IPV6_gateway

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.1.3.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV6 gateway of ETH0

- ETH0_IPV6_DNS_Preferred

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.1.3.4
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The preferred IPV6 DNS of ETH0

- ETH0_IPV6_DNS_Alternate

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.1.3.5
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The alternate IPV6 DNS of ETH0

LAN Port: ETH1

- ETH1_MAC

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.2.1
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The MAC for ETH1

ETH1 IPv4

- ETH1_IPV4_IP

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.2.2.1
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV4 IP of ETH1

- ETH1_IPV4_Subnet

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.2.2.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV4 subnet mask of ETH1

- ETH1_IPV4_gateway

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.2.2.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV4 gateway of ETH

- ETH1_IPV4_DNS_Preferred

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.2.2.4
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The preferred IPV4 DNS of ETH1

- ETH1_IPV4_DNS_Alternate

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.2.2.5
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The alternate IPV4 DNS of ETH1

ETH1 IPv6

- ETH1_IPV6_IP

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.2.3.1
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV6 IP of ETH1

- ETH1_IPV6_Prefix

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.2.3.2
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV6 subnet mask of ETH1

- ETH1_IPV6_gateway

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.2.3.3
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The IPV6 gateway of ETH1

- ETH1_IPV6_DNS_Preferred

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.2.3.4
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The preferred IPV6 DNS of ETH1

- ETH1_IPV6_DNS_Alternate

OID	1.3.6.1.4.1.21317.1.3.3.7.15.2.2.3.5
Syntax	DisplayString
Max-Access	read-only
Status	current
Description	The alternate IPV6 DNS of ETH1

General

- RedundantNICEnable

OID	1.3.6.1.4.1.21317.1.3.3.7.15.3
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The redundant NIC enable status of the device: False(0), True(1)

- IPv6Enable

OID	1.3.6.1.4.1.21317.1.3.3.7.15.4
Syntax	INTEGER
Max-Access	read-only
Status	current
Description	The IPv6 enable status of the device: False(0), True(1)

Appendix

Safety Instructions

General

- This product is for indoor use only.
- 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.
- Avoid circuit overloads. Before connecting equipment to a circuit, know the power supply's limit and never exceed it. Always review the electrical specifications of a circuit to ensure that you are not creating a dangerous condition or that one doesn't already exist. Circuit overloads can cause a fire and destroy equipment.
- The device should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.
- To prevent damage to your installation it is important that all devices are properly grounded.
- The device is designed for IT power distribution systems with 230V phase-to-phase voltage.
- 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 un-interruptible power supply (UPS).
- Position system cables and power cables carefully; Be sure that nothing rests on any cables.
- When connecting or disconnecting power to hot-pluggable power supplies, observe the following guidelines:
  - Install the power supply before connecting the power cable to the power supply.
  - Unplug the power cable before removing the power supply.
  - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.
- 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.

DC Power

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

access can only be gained by service personnel through the use of a special tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.

Rack Mount

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

Technical Support

International

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

North America

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

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

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

Specifications

SN1116CO / SN1132CO / SN1148CO

Function		SN1116CO	SN1132CO	SN1148CO
Serial Connections		16	32	48
Connectors	Serial	16 x RJ45 Female	32 x RJ45 Female	48 x RJ45 Female
	LAN	2 x SFP Slots **Note:** Optional fiber (2A-136G, 2A-137G) or copper (2A-143G) modules available.		
	Power	2 x IEC60320/C14		
	Local Console	1 x RJ-45 Female		
	PON	1 x RJ-45 Female (Reserved)		
	Laptop USB Console (LUC) Port	1 x Mini USB		
	USB Ports	4 x USB Type-A Female		
	Environment Sensor Ports	2 x RJ-11 Female 1 x 4-Pin Terminal Block **Note:** Optional sensors (EA1140, EA1240, EA1340, EA1440, EA1441, EA1442, and EA1540) available.		
	Relay	1 x 2-Pin Terminal Block *Normally open, isolated Relays; *Contact Rating: Max. 24 VDC, 2A		
Switches	Reset	1 x Recessed Pushbutton		
	Power	2 x Rocker Switches		
LEDs	Serial Port Status	16 (Green)	32 (Green)	48 (Green)
	10 / 100 / 1000 Mbps	2 (Red / Orange / Green)		
	Power	2 (Blue)		
I/P Rating	AC	100-240VAC; 50/60 Hz; 1.0A		
Power Consumption		AC110V:9.2W:96BTU/h AC220V:9.3W:96BTU/h	AC110V:11.2W:105BTU/h AC220V:11.3W:105BTU/h	AC110V:11.8W:108BTU/h AC220V:12W:109BTU/h
		Note: ◆ The measurement in Watts indicates the typical power consumption of the device with no external loading. ◆ The measurement in BTU/h indicates the power consumption of the device when it is fully loaded.		
Mode of Operation		Console Management, Console Management Direct, Real Com Port, TCP Server/Client, UDP Server/Client, Virtual Modem		

Function		SN1116CO	SN1132CO	SN1148CO
Environment	Operating Temp.	0–55° C		
	Storage Temp.	-20–60° C		
	Humidity	0–80% RH Noncondensing		
Physical Properties	Housing	Metal		
	Weight	4.51 kg (9.93 lb)	4.60 kg (10.13 lb)	4.67 kg (10.29 lb)
	Dimensions L x W x H	43.84 x 32.84 x 4.40 cm (17.26 x 12.93 x 1.73in)		

SN1116COD / SN1132COD / SN1148COD

Function		SN1116COD	SN1132COD	SN1148COD
Serial Connections		16	32	48
Connectors	Serial	16 x RJ45 Female	32 x RJ45 Female	48 x RJ45 Female
	LAN	2 x SFP Slots **Note:** Optional fiber (2A-136G, 2A-137G) or copper (2A-143G) modules available.		
	Power	1 x 5-Pin Terminal Block (Green)		
	Local Console	1 x RJ-45 Female		
	PON	1 x RJ-45 Female (Reserved)		
	Laptop USB Console (LUC) Port	1 x Mini USB		
	USB Ports	4 x USB Type-A Female		
	Environment Sensor Ports	2 x RJ-11 Female 1 x 4-Pin Terminal Block **Note:** Optional sensors (EA1140, EA1240, EA1340, EA1440, EA1441, EA1442, and EA1540) available.		
	Relay	1 x 2-Pin Terminal Block *Normally open, isolated Relays; *Contact Rating: Max. 24 VDC, 2A		
Switches	Reset	1 x Recessed Pushbutton		
	Power	2 x Rocker Switches		
LEDs	Serial Port Status	16 (Green)	32 (Green)	48 (Green)
	10 / 100 / 1000 Mbps	2 (Red / Orange / Green)		
	Power	2 (Blue)		
I/P Rating	DC	36-48 V DC; 1.6 A in 5-Pin Terminal Block		
Power Consumption		DC48V:9.3W	DC48V:11.3W	DC48V:12W
		Note: ◆ The measurement in Watts indicates the typical power consumption of the device with no external loading.		
Mode of Operation		Console Management, Console Management Direct, Real Com Port, TCP Server/Client, UDP Server/Client, Virtual Modem		
Environment	Operating Temp.	0–55° C		
	Storage Temp.	-20–60° C		
	Humidity	0–80% RH Noncondensing		
Physical Properties	Housing	Metal		
	Weight	4.51 kg (9.93 lb)	4.60 kg (10.13 lb)	4.67 kg (10.29 lb)
	Dimensions L x W x H	43.84 x 32.84 x 4.40 cm (17.26 x 12.93 x 1.73in)		

SN0108CO / SN0116CO (AXA Platform)

Function		SN0108CO	SN0116CO
Serial Connections		8	16
Connectors	Serial	8 x RJ45 Female	16 x RJ45 Female
	LAN	2 x RJ45	
	Power	2 x IEC 60320/C14	
	PON	1 x RJ45 Female (Reserved)	
	Modem	1 x RJ45 Female	
	USB	3 x USB Type A Female	
	USB Console (LUC)	1 x Mini USB	
	Local Console	1 x RJ45 Female	
Switches	Reset	1 x Recessed Pushbutton	
	Power	2 x Rocker Switch	
LEDs	Serial Port Status	8 (Green)	16 (Green)
	10 / 100 / 1000 Mbps	2 (Red / Orange / Green)	
	Power	2 (Blue)	
I/P Rating	AC	100–240V~; 50/60Hz; 1A	
Power Consumption		AC110V:5.3W:57BTU/h AC220V:5.2W:56BTU/h	AC110V:5.5W:58BTU/h AC220V:5.5W:58BTU/h
		Note: ◆ The measurement in Watts indicates the typical power consumption of the device with no external loading. ◆ The measurement in BTU/h indicates the power consumption of the device when it is fully loaded.	
Mode of Operation		Console Management, Console Management Direct, Real Com Port, TCP Server/Client, UDP Server/Client, Virtual Modem	
Environment	Operating Temp.	0–40° C	
	Storage Temp.	-20–60° C	
	Humidity	0–80% RH Noncondensing	
Physical Properties	Housing	Metal	
	Weight	4.35 kg	4.38 kg
	Dimensions L x W x H	43.72 x 32.98 x 4.40 cm (19”1U)	43.72 x 32.98 x 4.40 cm (19”1U)

SN0108CO / SN0116CO (AX Platform)

Function		SN0108CO	SN0116CO
Serial Connections		8	16
Connectors	Serial	8 x RJ45 Female	16 x RJ45 Female
	LAN	2 x RJ45	
	Power	2 x IEC 60320/C14	
	PON	1 x RJ45 Female (Reserved)	
	Modem	1 x RJ45 Female	
	USB	3 x USB Type A Female	
	USB Console (LUC)	1 x Mini USB	
	Local Console	1 x RJ45 Female	
Switches	Reset	1 x Recessed Pushbutton	
	Power	2 x Rocker Switch	
LEDs	Serial Port Status	8 (Green)	16 (Green)
	10 / 100 / 1000 Mbps	2 (Red / Orange / Green)	
	Power	2 (Blue)	
I/P Rating	AC	100–240V~; 50/60Hz; 1A	
Power Consumption		AC110V:14.1W:98BTU/h AC220V:14W:98BTU/h	AC110V:15.4W:104BTU/h AC220V:14.9W:102BTU/h
		Note: ◆ The measurement in Watts indicates the typical power consumption of the device with no external loading. ◆ The measurement in BTU/h indicates the power consumption of the device when it is fully loaded.	
Mode of Operation		Console Management, Console Management Direct, Real Com Port, TCP Server/Client, UDP Server/Client, Virtual Modem	
Environment	Operating Temp.	0–40° C	
	Storage Temp.	-20–60° C	
	Humidity	0–80% RH Noncondensing	
Physical Properties	Housing	Metal	
	Weight	4.45 kg	4.48 kg
	Dimensions L x W x H	43.72 x 32.98 x 4.40 cm (19”1U)	43.72 x 32.98 x 4.40 cm (19”1U)

SN0108COD / SN0116COD (AXA Platform)

Function		SN0108COD	SN0116COD
Serial Connections		8	16
Connectors	Serial	8 x RJ45 Female	16 x RJ45 Female
	LAN	2 x RJ45	
	Power	1 x 5-Pin Terminal Block (Green)	
	PON	1 x RJ45 Female (Reserved)	
	Modem	1 x RJ45 Female	
	USB	3 x USB Type A Female	
	USB Console (LUC)	1 x Mini USB	
	Local Console	1 x RJ45 Female	
Switches	Reset	1 x Recessed Pushbutton	
	Power	2 x Rocker Switch	
LEDs	Serial Port Status	8 (Green)	16 (Green)
	10 / 100 / 1000 Mbps	2 (Red / Orange / Green)	
	Power	2 (Blue)	
I/P Rating	DC	36-48 V DC; 1.6 A in 5-Pin Terminal Block	
Power Consumption		DC48V:5.3W	DC48V:5.5W
		Note: ◆ The measurement in Watts indicates the typical power consumption of the device with no external loading.	
Mode of Operation		Console Management, Console Management Direct, Real Com Port, TCP Server/Client, UDP Server/Client, Virtual Modem	
Environment	Operating Temp.	0–40° C	
	Storage Temp.	-20–60° C	
	Humidity	0–80% RH Noncondensing	
Physical Properties	Housing	Metal	
	Weight	4.55 kg	4.59 kg
	Dimensions L x W x H	43.72 x 32.85 x 4.40 cm	

SN0108COD / SN0116COD (AX Platform)

Function		SN0108COD	SN0116COD
Serial Connections		8	16
Connectors	Serial	8 x RJ45 Female	16 x RJ45 Female
	LAN	2 x RJ45	
	Power	1 x 5-Pin Terminal Block (Green)	
	PON	1 x RJ45 Female (Reserved)	
	Modem	1 x RJ45 Female	
	USB	3 x USB Type A Female	
	USB Console (LUC)	1 x Mini USB	
	Local Console	1 x RJ45 Female	
Switches	Reset	1 x Recessed Pushbutton	
	Power	2 x Rocker Switch	
LEDs	Serial Port Status	8 (Green)	16 (Green)
	10 / 100 / 1000 Mbps	2 (Red / Orange / Green)	
	Power	2 (Blue)	
I/P Rating	DC	36-48 V DC; 1.6 A in 5-Pin Terminal Block	
Power Consumption		DC48V:15.79W	DC48V:16.22W
		Note: ◆ The measurement in Watts indicates the typical power consumption of the device with no external loading.	
Mode of Operation		Console Management, Console Management Direct, Real Com Port, TCP Server/Client, UDP Server/Client, Virtual Modem	
Environment	Operating Temp.	0–40° C	
	Storage Temp.	-20–60° C	
	Humidity	0–80% RH Noncondensing	
Physical Properties	Housing	Metal	
	Weight	4.46 kg	4.5 kg
	Dimensions L x W x H	43.72 x 32.85 x 4.40 cm	

SN0132CO / SN0148CO (AXA Platform)

Function		SN0132CO	SN0148CO
Serial Connections		32	48
Connectors	Serial	32 x RJ45 Female	48 x RJ45 Female
	LAN	2 x RJ45	
	Power	2 x IEC 60320/C14	
	PON	1 x RJ45 Female (Reserved)	
	Modem	1 x RJ45 Female	
	USB	3 x USB Type A Female	
	USB Console (LUC)	1 x Mini USB	
	Local Console	1 x RJ45 Female	
Switches	Reset	1 x Recessed Pushbutton	
	Power	2 x Rocker Switch	
LEDs	Serial Port Status	32 (Green)	48 (Green)
	10 / 100 / 1000 Mbps	2 (Red / Orange / Green)	
	Power	2 (Blue)	
I/P Rating	AC	100-240V~; 50/60Hz; 1.8A	
Power Consumption		AC110V:9.8W:78BTU/h AC220V:9.7W:77BTU/h	AC110V:10.3W:80BTU/h AC220V:10.2W:80BTU/h
		Note: ◆ The measurement in Watts indicates the typical power consumption of the device with no external loading. ◆ The measurement in BTU/h indicates the power consumption of the device when it is fully loaded.	
Mode of Operation		Console Management, Console Management Direct, Real Com Port, TCP Server/Client, UDP Server/Client, Virtual Modem	
Environment	Operating Temp.	0–40° C	
	Storage Temp.	-20–60° C	
	Humidity	0–80% RH Noncondensing	
Physical Properties	Housing	Metal	
	Weight	4.55 kg	4.61 kg
	Dimensions L x W x H	43.84 x 32.77 x 4.40 cm	

SN0132CO / SN0148CO (AX Platform)

Function		SN0132CO	SN0148CO
Serial Connections		32	48
Connectors	Serial	32 x RJ45 Female	48 x RJ45 Female
	LAN	2 x RJ45	
	Power	2 x IEC 60320/C14	
	PON	1 x RJ45 Female (Reserved)	
	Modem	1 x RJ45 Female	
	USB	3 x USB Type A Female	
	USB Console (LUC)	1 x Mini USB	
	Local Console	1 x RJ45 Female	
Switches	Reset	1 x Recessed Pushbutton	
	Power	2 x Rocker Switch	
LEDs	Serial Port Status	32 (Green)	48 (Green)
	10 / 100 / 1000 Mbps	2 (Red / Orange / Green)	
	Power	2 (Blue)	
I/P Rating	AC	100-240V~; 50/60Hz; 1.8A	
Power Consumption		AC110V:22.5W:137BTU/h AC220V29.9W:143BTU/h	AC110V:29.5W:170BTU/h AC220V:29.9W:172BTU/h
		Note: ◆ The measurement in Watts indicates the typical power consumption of the device with no external loading. ◆ The measurement in BTU/h indicates the power consumption of the device when it is fully loaded.	
Mode of Operation		Console Management, Console Management Direct, Real Com Port, TCP Server/Client, UDP Server/Client, Virtual Modem	
Environment	Operating Temp.	0–40° C	
	Storage Temp.	-20–60° C	
	Humidity	0–80% RH Noncondensing	
Physical Properties	Housing	Metal	
	Weight	4.84 kg	4.92 kg
	Dimensions L x W x H	43.84 x 32.77 x 4.40 cm	

SN0132COD / SN0148COD (AXA Platform)

Function		SN0132COD	SN0148COD
Serial Connections		32	48
Connectors	Serial	32 x RJ45 Female (Black)	48 x RJ45 Female (Black)
	LAN	2 x RJ-45 (Black)	
	Power	1 x 5-Pin Terminal Block (Green)	
	PON	1 x RJ45 Female (Reserved)	
	Modem	1 x RJ45 Female	
	USB	3 x USB Type A Female	
	USB Console (LUC)	1 x Mini USB	
	Local Console	1 x RJ45 Female	
Switches	Reset	1 x Recessed Pushbutton	
	Power	2 x Rocker Switch	
LEDs	Serial Port Status	32 (Green)	48 (Green)
	10 / 100 / 1000 Mbps	2 (Red / Orange / Green)	
	Power	2 (Blue)	
I/P Rating	DC	36-48 V DC; 1.6 A in 5-Pin Terminal Block	
Power Consumption		DC48V:9.8W	DC48V:10.3W
		Note: ◆ The measurement in Watts indicates the typical power consumption of the device with no external loading.	
Mode of Operation		Console Management, Console Management Direct, Real Com Port, TCP Server/Client, UDP Server/Client, Virtual Modem	
Environment	Operating Temp.	0–40° C	
	Storage Temp.	-20–60° C	
	Humidity	0–80% RH Noncondensing	
Physical Properties	Housing	Metal	
	Weight	4.83 kg	4.89 kg
	Dimensions L x W x H	43.84 x 32.77 x 4.40 cm	

SN0132COD / SN0148COD (AX Platform)

Function		SN0132COD	SN0148COD
Serial Connections		32	48
Connectors	Serial	32 x RJ45 Female (Black)	48 x RJ45 Female (Black)
	LAN	2 x RJ-45 (Black)	
	Power	1 x 5-Pin Terminal Block (Green)	
	PON	1 x RJ45 Female (Reserved)	
	Modem	1 x RJ45 Female	
	USB	3 x USB Type A Female	
	USB Console (LUC)	1 x Mini USB	
	Local Console	1 x RJ45 Female	
Switches	Reset	1 x Recessed Pushbutton	
	Power	2 x Rocker Switch	
LEDs	Serial Port Status	32 (Green)	48 (Green)
	10 / 100 / 1000 Mbps	2 (Red / Orange / Green)	
	Power	2 (Blue)	
I/P Rating	DC	36-48 V DC; 1.6 A in 5-Pin Terminal Block	
Power Consumption		DC48V:22.1W	DC48V:27.3W
		Note: ◆ The measurement in Watts indicates the typical power consumption of the device with no external loading.	
Mode of Operation		Console Management, Console Management Direct, Real Com Port, TCP Server/Client, UDP Server/Client, Virtual Modem	
Environment	Operating Temp.	0–40° C	
	Storage Temp.	-20–60° C	
	Humidity	0–80% RH Noncondensing	
Physical Properties	Housing	Metal	
	Weight	4.99 kg	5.06 kg
	Dimensions L x W x H	43.84 x 32.77 x 4.40 cm	

SN9108CO / SN9116CO (AXA Platform)

Function		SN9108CO	SN9116CO
Serial Connections		8	16
Connectors	Serial	8 x RJ45 Female	16 x RJ45 Female
	LAN	1 x RJ45	
	Power	1 x IEC60320/C14	
Switches	Reset	1 x Recessed Pushbutton	
	Power	1 x Rocker Switch	
LEDs	Serial Port Status	8 (Green)	16 (Green)
	10 / 100 / 1000 Mbps	1 (Red / Orange / Green)	
	Power	1 (Blue)	
I/P Rating	AC	100-240V~, 50/60 Hz, 1A	
Power Consumption		AC110V:4.9W:23BTU/h AC220V:4.8W:23BTU/h	AC110V:5.5W:26BTU/h AC220V:5.4W:25BTU/h
		Note: ◆ The measurement in Watts indicates the typical power consumption of the device with no external loading. ◆ The measurement in BTU/h indicates the power consumption of the device when it is fully loaded.	
Mode of Operation		Console Management, Console Management Direct, Real Com Port, TCP Server/Client, UDP Server/Client, Virtual Modem	
Environment	Operating Temp.	0–40° C	
	Storage Temp.	-20–60° C	
	Humidity	0–80% RH Noncondensing	
Physical Properties	Housing	Metal	
	Weight	3.12 kg	3.16 kg
	Dimensions L x W x H	43.72 x 21.76 x 4.40 cm (19”1U)	43.72 x 21.76 x 4.40 cm (19”1U)

SN9108CO / SN9116CO (AX Platform)

Function		SN9108CO	SN9116CO
Serial Connections		8	16
Connectors	Serial	8 x RJ45 Female	16 x RJ45 Female
	LAN	1 x RJ45	
	Power	1 x IEC60320/C14	
Switches	Reset	1 x Recessed Pushbutton	
	Power	1 x Rocker Switch	
LEDs	Serial Port Status	8 (Green)	16 (Green)
	10 / 100 / 1000 Mbps	1 (Red / Orange / Green)	
	Power	1 (Blue)	
I/P Rating	AC	100-240V~, 50/60 Hz, 1A	
Power Consumption		AC110V:9.7W:45BTU/h AC220V:9.6W:45BTU/h	AC110V:10.9W:51BTU/h AC220V:11.6W:54BTU/h
		Note: ◆ The measurement in Watts indicates the typical power consumption of the device with no external loading. ◆ The measurement in BTU/h indicates the power consumption of the device when it is fully loaded.	
Mode of Operation		Console Management, Console Management Direct, Real Com Port, TCP Server/Client, UDP Server/Client, Virtual Modem	
Environment	Operating Temp.	0–40° C	
	Storage Temp.	-20–60° C	
	Humidity	0–80% RH Noncondensing	
Physical Properties	Housing	Metal	
	Weight	3.12 kg	3.16 kg
	Dimensions L x W x H	43.72 x 21.76 x 4.40 cm (19”1U)	43.72 x 21.76 x 4.40 cm (19”1U)

IP Address Determination

If you are an administrator logging in for the first time, you need to access the Serial Console Server in order to give it an IP address that users can connect to. There are three methods to choose from. In each case, your client computer must be on the same network segment as the Serial Console Server. After you have connected and logged in you can give the Serial Console Server its fixed network address. (See *Network*, page 131.)

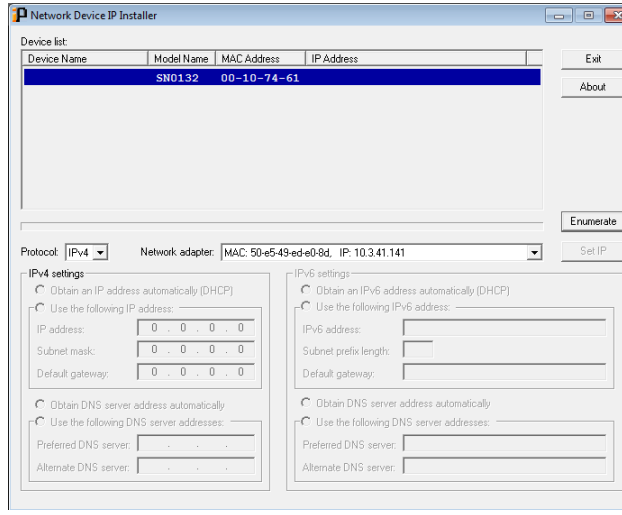
The Local Console

The easiest way to assign an IP address is from the local console. Refer to *First-Time Setup*, page 43, for details on the procedure involved.

IP Installer

For client computers running Windows, an IP address can be assigned with the *IP Installer* utility. The utility can be obtained from the *Download* area of our website. Look under *Driver/SW*, and the model of your Serial Console Server. After downloading the utility to your client computer, do the following:

1. Unzip the contents of *IPInstaller.zip* 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 Serial Console Server 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 Serial Console Server 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**. See *IP Installer*, page 131 for more information.

Browser

1. Set your client computer's IP address to 192.168.0.*XXX*

   Where *XXX* represents any number or numbers except 60. (192.168.0.60 is the default address of the Serial Console Server.)
2. Specify the Serial Console Server's default IP address (192.168.0.60) in your browser, and you will be able to connect.
3. Assign a fixed IP address for the Serial Console Server that is suitable for the network segment that it resides on.
4. After you log out, reset your client computer's IP address to its original value.

IPv6

At present, the Serial Console Server supports three IPv6 address protocols: *Link Local IPv6 Address*, *IPv6 Stateless Autoconfiguration*, and *Stateful Autoconfiguration (DHCPv6)*.

Link Local IPv6 Address

At power on, the Serial Console Server is automatically configured with a Link Local IPv6 Address (for example, fe80:210:74ff:fe61:1ef). To find out what the Link Local IPv6 Address is, log in with the Serial Console Server IPv4 address and open the *Device Management* → *Device Information* page. The address is displayed in the *General* list box (see page 126).

Once you have determined what the IPv6 address is, you can use it when logging in from a browser or the Win and Java Client AP programs.

For example:

If you are logging in from a browser, you would key in

```
http://[fe80:2001:74ff:fe6e:59%5]
```

for the URL bar.

If you are logging in with the AP program, you would key:

```
fe80:2001:74ff:fe6e:59%5
```

for the *IP* field of the *Server* panel (see *Remote Login*, page 46).

Note: 1. To log in with the Link Local IPv6 Address, the client computer must be on the same local network segment as the Serial Console Server

2. The %5 is the %interface used by the client computer. To see your client computer's IPv6 address: from the command line issue the following command: `ipconfig /all`. The % value appears at the end of the IPv6 address.

IPv6 Stateless Autoconfiguration

If the Serial Console Server network environment contains a device (such as a router) that supports the IPv6 Stateless Autoconfiguration function, the Serial Console Server can obtain its prefix information from that device in order to generate its IPv6 address. For example, 2001:74ff:fe6e:59.

As above, the address is displayed in the *General* list box of the *Device Management* → *Device Information* page (see page 126).

Once you have determined what the IPv6 address is, you can use it when logging in from a browser or the Win and Java Client AP programs.

For example:

If you are logging in from a browser, you would key in

```
http://[2001:74ff:fe6e:59]
```

for the URL bar.

If you are logging in with the AP program, you would key:

```
2001:74ff:fe6e:59
```

for the *IP* field of the *Server* panel.

Virtual Modem Details

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

AT Command Set Support

The Serial Console Server 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*n*[CR]	Where n 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*n*[CR]	Inquiry command. (Where n represents a numeric character; 0 or 1.): E0: Display *ATEN International Co. Ltd.* E1: Display Serial Console Server	If successful: OK[CR][LF] If failure: ERROR[CR][LF]
ATO*n*[CR]	Return to on-line data mode. (Where n 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*n*[CR]	Result code control command. (Where n 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*n*?[CR]	Reports the value of the *S* register. (Where n is the register's number.)	If successful: OK[CR][LF] If failure: ERROR[CR][LF]
ATS*n*=*v*[CR]	Sets the S register's value. (Where n is the register's number; and v is the S register value.)	If successful: OK[CR][LF] If failure: ERROR[CR][LF]
ATV*n*[CR]	Result code return type. (Where n 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&C*n*[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&D*n*[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]

Port Forwarding

For devices located behind a router, port forwarding allows the router to pass data coming in over a specific port to a specific device. By setting the port forwarding parameters, you tell the router which device to send the data that comes in over a particular port to.

For example, if the Serial Console Server connected to a particular router has an IP address of 192.168.1.180, you would log into your router's setup program and access the Port Forwarding (sometimes referred to as *Virtual Server*) configuration page. You would then specify 192.168.1.180 for the IP address and the port number you want opened for it (9000 for internet access, for example).

Since configuration setup can vary somewhat for each brand of router, refer to the router's User Manual for specific information on configuring port forwarding for it.

Distance vs Baud Rate

The serial ports support different baud rates, which, in turn, determine the distance of the serial port connection.

Refer to the table below:

Baud Rate	Distance
300	90m (295ft)
9,600 (default)	30m (98ft)
115,200	3m (9ft)
230,400	1.5m (4ft)

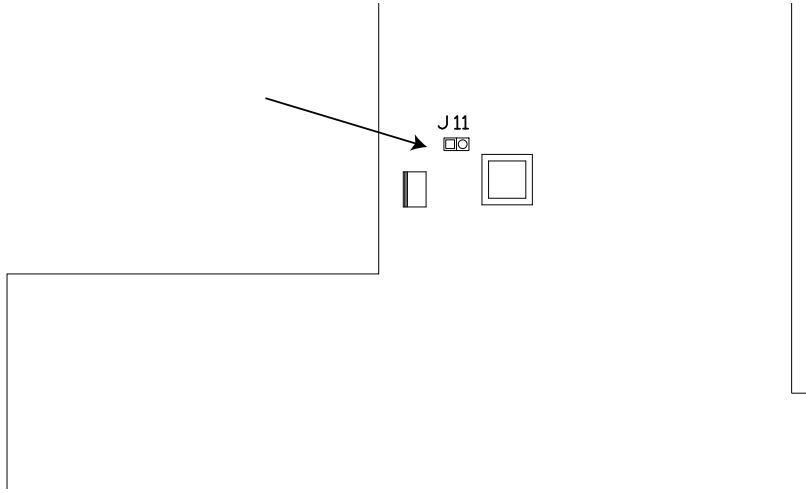
Clear Login Information

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.

Note: Performing this procedure also returns all settings to their defaults.

To clear the login information (and return all settings to their defaults), do the following:

1. Power off the Serial Console Server and remove its housing.
2. Use a jumper cap to short the mainboard jumper labeled **J11/J18** (for SN0132/SN0148/SN1132/SN1148 as shown in the diagram below) or **J17/J18** (for SN9108/SN9116/SN0108/SN0116/SN1116).



3. Power on the Serial Console Server.
4. When the unit starts beeping, power off the Serial Console Server.
5. Remove the jumper cap from **J11/J18** (SN0132/SN0148/SN1132/SN1148) or **J17/J18** (SN9108/SN9116/SN0108/SN0116/SN1116).
6. Close the housing and start the Serial Console Server.

   After powering on the unit, you can use the default super administrator username and password (see *First-Time Setup*, page 43) to log in.

   The system will force you to change the password as you log in for the first time after performing this procedure.

Pin Assignment

The Serial Console Server has DTE/DCE auto-sensing feature to connect directly to Cisco network switches and other compatible devices.

The pin assignment for the serial ports under different mode is shown below:

DCE Mode Pin Assignment

Pin	Definition
1	CTS
2	DSR
3	RxD
4	GND
5	GND
6	TxD
7	DTR
8	RTS

DTE Mode Pin Assignment

Pin	Definition
1	RTS
2	DTR
3	TxD
4	GND
5	GND
6	RxD
7	DSR
8	CTS

DB-9/DB-25 Interface

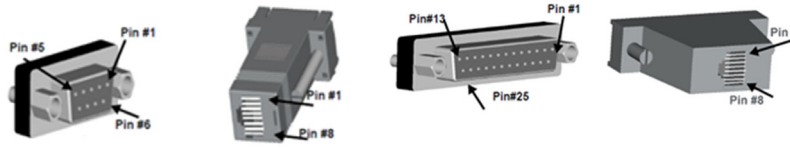
If you wish to use DB-9 or DB-25 interface, please refer to the tables below:

DB-9

RJ-45 Pin	Signal	DB-9F Pin	Signal
1	CTS	7	RTS
2	DSR	4	DTR
5	GND		
3	RxD	3	TxD
4	GND	5	GND
6	TxD	2	RxD
7	DTR	1	GND
		6	DSR
8	RTS	8	CTS

DB-25

RJ-45 Pin	Signal	DB-25F Pin	Signal
1	CTS	4	RTS
2	DSR	20	DTR
5	GND		
3	RxD	2	TxD
4	GND	7	GND
6	TxD	3	RxD
7	DTR	6	GND
		8	DSR
8	RTS	5	CTS



Self-signing SSL/TLS Certificate

Privately-trusted SSL/TLS certificates should only be used to authenticate users and devices within an **internal** network.

1. On the SN device's web browser, go to **Maintenance > Private Certificate**.
2. Click **Get CSR** from the bottom of the Private Certificate page, as shown here. A *custom.csr* file is obtained.



3. Utilizing *openssl.exe*, use the following commands to generate a *new.cer* file:
   - openssl req -new -newkey rsa:2048 -days 3653 -nodes -x509 -keyout *ca.key* -out *ca.cer*
   - openssl ca -policy policy_anything -config openssl.cnf -cert *ca.cer* -in *custom.csr* -keyfile *ca.key* -days 360 -out *new.cer*
4. Click **Import** to import the *new.cer* file into your SN device.

CLI Command Set

CLI commands are used in CLI Mode when accessing the Serial Console Server through Telnet or SSH for basic configuration and control.

System Setting Commands

set hostname=<host_name>

Example:

```
set hostname=SN9108CO
```

Description:
Set SN9108CO as the hostname or the device name of the Serial Console Server.

read sysinfo

Example:

```
read sysinfo
```

Description:

Show the system information.

reboot

Example:

```
reboot
```

Description:

Reboot the system.

read log

Example:

```
read log
```

Description:

Show the system logs.

quit

Example:

```
quit
```

Description:

Log out the system.

help

Example:

```
help
```

Description:

Show all available commands.

menu on

Example:

```
menu on
```

Description:

Switch to the menu-driven mode.

set logintimeout=<timeout_minutes>

Example:

```
set logintimeout=1
```

Description:

Set the login timeout as 1 minute. Specify the timeout value, <timeout_minutes>, in the range 0 - 180 minutes. The value 0 means never timeout.

set securitylevel=<1/2/3>

Example:

```
set securitylevel=1
```

Description:

Set the security level as 1.

The available security level are listed below:

- 1 = High
  Disable all services except of SSHv2 and HTTPS(TLS v1.2).
- 2 = Medium-High
  Enable SSHv2, and redirect from HTTP to HTTPS, HTTPS (TLS v1.2), or ICMP.
- 3 = Medium
  Enable SSHv2, and redirect from HTTP to HTTPS, HTTPS (TLS v1.0, 1.1, 1.2), SNMP Agent, or ICMP.

nfs

Example:

```
nfs
```

Description:

Show the settings of the NFS.

nfs name <nfs1/nfs2/nfs3/nfs4> startup <on/off>

Example:

```
nfs name nfs1 startup on
```

Description:

Automatically mount the NFS1 storage device once when the system starts up.

nfs name <nfs1/nfs2/nfs3/nfs4> mount

Example:

```
nfs name nfs1 mount
```

Description:

Mount the NFS1 storage device.

nfs name <nfs1/nfs2/nfs3/nfs4> unmount

Example:

```
nfs name nfs1 unmount
```

Description:

Unmount the NFS1 storage device.

set systime=<YYYMMDDHHMMSS>

Example:

```
set systime=20221005133400
```

Description:

Sets the system time manually with date = 10/05/2022, time = 13:34:00 (YYYY: year, MM: month, DD: day, HH: hour, MM: minute, and SS: second).

set ntp=<pref_NTPaddr> <alter_NTPaddr>

Example:

```
set ntp=192.168.0.31 192.168.0.32
```

Description:

Syncs system time with NTP servers 192.168.0.31 as the preferred NTP address and 192.168.0.32 as alternate NTP address.

set timezone=<timezone_number>

Example:

```
set timezone=61
```

Description:

Sets system timezone to (GMT+09:00) Osaka, Sapporo, Tokyo. For timezone number, please refer to the timezone list below.

Timezone List:

1. (GMT-12:00) Eniwetok, Kwajalein
2. (GMT-11:00) Midway Island, Samoa
3. (GMT-10:00) Hawaii
4. (GMT-09:00) Alaska
5. (GMT-08:00) Pacific Time (US & Canada); Tijuana
6. (GMT-07:00) Mountain Time (US & Canada)
7. (GMT-07:00) Arizona
8. (GMT-06:00) Central Time (US & Canada)
9. (GMT-06:00) Mexico City
10. (GMT-06:00) Saskatchewan
11. (GMT-06:00) Central America
12. (GMT-05:00) Eastern Time (US & Canada)
13. (GMT-05:00) Indiana (East)
14. (GMT-05:00) Bogota, Lima, Quito
15. (GMT-04:00) Atlantic Time (Canada)
16. (GMT-04:00) Caracas, La Paz
17. (GMT-04:00) Santiago
18. (GMT-03:30) Newfoundland
19. (GMT-03:00) Buenos Aires, Georgetown
20. (GMT-03:00) Brasilia
21. (GMT-03:00) Greenland
22. (GMT-02:00) Mid-Atlantic
23. (GMT-01:00) Azores
24. (GMT-01:00) Cape Verde Is
25. (GMT) Casablanca, Monrovia
26. (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
27. (GMT+01:00) Amsterdam, Copenhagen, Madrid, Paris, Vilnius
28. (GMT+01:00) West Central Africa
29. (GMT+01:00) Belgrade, Sarajevo, Skopje, Sofija, Zagreb
30. (GMT+01:00) Bratislava, Budapest, Ljubljana, Prague, Warsaw

31. (GMT+01:00) Brussels, Berlin, Bern, Rome, Stockholm, Vienna
32. (GMT+02:00) Cairo
33. (GMT+02:00) Harare, Pretoria
34. (GMT+02:00) Jerusalem
35. (GMT+02:00) Bucharest
36. (GMT+02:00) Helsinki, Riga, Tallinn
37. (GMT+02:00) Athens, Istanbul, Minsk
38. (GMT+03:00) Kuwait, Riyadh
39. (GMT+03:00) Nairobi
40. (GMT+03:00) Baghdad
41. (GMT+03:00) Moscow, St. Petersburg, Volgograd
42. (GMT+03:30) Tehran
43. (GMT+04:00) Abu Dhabi, Muscat
44. (GMT+04:00) Baku, Tbilisi, Yerevan
45. (GMT+04:30) Kabul
46. (GMT+05:00) Islamabad, Karachi, Tashkent
47. (GMT+05:00) Ekaterinburg
48. (GMT+05:30) Calcutta, Chennai, Mumbai, New Delhi
49. (GMT+05:45) Kathmandu
50. (GMT+06:00) Astana, Dhaka
51. (GMT+06:00) Sri Jayawardenepura
52. (GMT+06:00) Almaty, Novosibirsk
53. (GMT+06:30) Rangoon
54. (GMT+07:00) Bangkok, Hanoi, Jakarta
55. (GMT+07:00) Krasnoyarsk
56. (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi
57. (GMT+08:00) Perth
58. (GMT+08:00) Kuala Lumpur, Singapore
59. (GMT+08:00) Taipei
60. (GMT+08:00) Irkutsk, Ulaan Bataar
61. (GMT+09:00) Osaka, Sapporo, Tokyo
62. (GMT+09:00) Seoul
63. (GMT+09:00) Yakutsk
64. (GMT+09:30) Darwin
65. (GMT+09:30) Adelaide
66. (GMT+10:00) Canberra, Melbourne, Sydney
67. (GMT+10:00) Brisbane
68. (GMT+10:00) Guam, Port Moresby
69. (GMT+10:00) Hobart

70. (GMT+10:00) Vladivostok
71. (GMT+11:00) Magadan, Solomon Is, New Caledonia
72. (GMT+12:00) Fiji, Kamchatka, Marshall Is.
73. (GMT+12:00) Auckland, Wellington
74. (GMT+13:00) Nuku'alofa

snmpagent <v1v2c/v3> <on/off>

Example:

snmpagent v1v2c on

Description:

Enable SNMP agent v1v2c

snmptrap <on/off>

Example:

snmptrap off

Description:

Disable SNMP trap

snmpevent <on/off>

Example:

snmpevent on

Description:

Enable all SNMP event notifications

smtpevent <on/off>

Example:

smtpevent on

Description:

Enable all SMTP event notifications

syslogevent <on/off>

Example:

syslogevent on

Description:

Enable all Syslog event notifications

Network Setting Commands

To configure the network settings through CLI commands, you can use the parameter that indicates the network interface name on the CLI command to specify your setting:

- **eth0**: LAN port 1
- **eth1**: LAN port 2
- **bond**: eth0 and eth1 are redundant

netconfig

Example:

```
netconfig
```

Description:

Show the IPv4 & IPv6 network configuration and the service ports.

netconfig if <eth0/eth1/bond> <v4/v6> ip <IP_address> nm <subnet_mask> gw <gateway_address>

Example:

```
netconfig if eth0 v4 ip 192.168.1.1 nm 255.255.255.0 gw
192.168.1.255
```

Description:

To set the followings:

- IP address of LAN port 1: *192.168.1.1*
- Subnet mask: *255.255.255.0*
- Gateway address: *192.168.1.255*

netconfig if <eth0/eth1/bond> <dhcp/dhcpv6>

Example:

```
netconfig if eth0 dhcp
```

Description:

Set the IP address of LAN port 1 through DHCP.

netconfig service <http/https/ssh/telnet/base> port <port_number>

Example 1:

```
netconfig service http port 8080
```

Description 1:

Set 8080 to be the service port of HTTP.

Example 2:

```
netconfig service base port 10000
```

Description 2:

Set 10000 to be the service port of base socket.

dnsconfig if <eth0/eth1/bond> <v4/v6> set <pref_DNSaddr> <alter_DNSaddr>

Example:

```
dnsconfig if eth0 v4 set 192.168.0.22 192.168.0.23
```

Description:

Set “192.168.0.22” as the preferred IPv4 DNS address of “LAN port 1” and set “192.168.0.23” as the alternate IPv4 DNS address.

dnsconfig if <eth0/eth1/bond> <dhcp/dhcpv6>

Example:

```
dnsconfig if eth0 dhcp
```

Description:

Set the IPv4 DNS address of LAN port 1 through DHCP.

netconfig ipv6 <on/off>

Example:

```
netconfig ipv6 off
```

Description:

Disable the functionality of IPv6.

service port 9000 <enable/disable>

Example:

```
service port 9000 enable
```

Description:

Enable the service port 9000.

User Management Commands

user

Example:

```
user
```

Description:

Display the user list.

user name <username>

Example:

```
user name gene
```

Description:

Show the user information of “gene”.

group

Example:

```
group
```

Description:

Display the group list.

group name <groupname/*>

Example 1:

```
group name SD1
```

Description 1:

Show the group information of “SD1”.

Example 2:

```
group name *
```

Description 2:

List the information of all group.

session

Example:

```
session
```

Description:

List the currently logged-in users.

session name <username> delete

Example:

```
session name willy delete
```

Description:

Kill the specific session “willy”.

session index <index_number> delete

Example:

```
session index 1 delete
```

Description:

Kill the specific session with index 1.

user name <username> pwd <password> group <group name> role <1/2/3> add

Example:

```
user name gene pwd pppWWW group SD1 role 1 add
```

Description:

Create a user account whose user name is “gene”, the password is “pppWWW”, the assigned user role type is “role 1", and the group is “SD1”.

Note:

- The following parameters are the user role types to be assigned:
  - role 1: super administrator
  - role 2: administrator
  - role 3: user
- The permissions to each role are based on what the system assigns for them by default.

user name <username> pwd <password>

Example:

```
user name gene pwd pppWWW
```

Description:

Set “pppWWW” as the password for the account whose user name is “gene”.

user name <username> group <group name>

Example:

```
user name gene group SD1
```

Description:

Assign the user account “gene” to the group “SD1”.

group name <group name> user <username> remove

Example:

```
group name SD1 user gene remove
```

Description:

Remove the user account “gene” from the group “SD1”.

user name <username> port <port number> priv <0000/0100/0101/0010/0011>

Example:

```
user name gene port 1,2,3,8,9 priv 0010
```

Description:

Assign the privilege “Full Access” to serial port 1, serial port 2, serial port 3, serial port 8, and serial port 9 of the user “gene”.

Note:

The privilege levels to be assigned are:

- **0000**: No Access
- **0100**: View Only
- **0101**: View Only + Config
- **0010**: Full Access
- **0011**: Full Access + Config

---

user name <username> delete

Example:

```
user name gene delete
```

Description:

Delete the user account “gene”.

group name <group_name> role <1/2/3> add

Example:

```
group name SD1 role 1 add
```

Description:

Create a group which is named “SD1” and assign the role type “role 1" to this newly created group.

Note:

- The following parameters are the role types to be assigned:
  - **role 1**: super administrator
  - **role 2**: administrator
  - **role 3**: user
- The permissions to each role are based on what the system assigns for them by default.

group name <group_name> port <port_number> priv <0000/0100/0101/0010/0011>

Example:

```
group name SD1 port 1,2,3,5,8,9 priv 0010
```

Description:

Assign the privilege “Full Access” to serial port 1, serial port 2, serial port 3, serial port 8, and serial port 9 of the group “SD1”.

Note:

The privilege levels to be assigned are:

- **0000**: No Access
- **0100**: View Only
- **0101**: View Only + Config
- **0010**: Full Access
- **0011**: Full Access + Config

group name <group_name> delete

Example:

```
group name SD1 delete
```

Description:

Delete the group “SD1”.

Serial Port Setting Commands

serial

Example:

```
serial
```

Description:

Show the serial port list.

serial port <port_number>

Example:

```
serial port 1
```

Description:

Display the serial port properties of serial port 1.

serial port <port_number> log

Example:

```
serial port 1 log
```

Description:

Display the port log of serial port 1.

> **Note:** The command works with the premise that Port Buffering is enabled. See *Port Buffering*, page 96 for details.

serial port <port_number> baud <300/600/1200/1800/2400/4800/9600/19200/28800/38400/57600/115200/230400>

Example:

```
serial port 1,4,7,12 baud 9600
```

Description:

Set the baud rate of serial port 1, serial port 4, serial port 7, and serial port 12 to be 9600 bps.

serial port <port_number> mode <00/11/12/13/21/22/23>

Example:

```
serial port 1,3,9 mode 13
```

Description:

For serial port 1, serial port 3, and serial port 9, set the operating mode to be "Console Management", and enable SSH and Telnet as well.

Note: Configure the operating mode for the serial port(s) by using the following parameters on the command line:

- **mode 00: Disabled**
- **mode 11**: Console Management. SSH is enabled.
- **mode 12**: Console Management. Telnet is enabled.
- **mode 13**: Console Management. Both SSH and Telnet are enabled.
- **mode 21**: Console Management Direct. SSH is enabled.
- **mode 22**: Console Management Direct. Telnet is enabled.
- **mode 23**: Console Management Direct. Both SSH and Telnet are enabled.

serial port <port_number> access

Example:

```
serial port 1 access
```

Description:

Access serial port 1.

Note: To return to SN console, please press [Ctrl+d].

serial port <port_number> name <port_name>

Example:

```
serial port 1 name Cisco
```

Description:

Set the port name of serial port 1 to be “Cisco”.

serial port <port_number> copyto <*/port_numbers>

Example:

```
serial port 1 copyto *
```

Description:

Copy the properties of the serial port 1 to all the serial ports.

Note:

- Use a comma to separate multiple ports for port_numbers. (e.g. 1, 3, 9, 16)
- For a range of ports, put a dash between the starting port and the ending port. (e.g. 3-16)

Backup/Restore Config Commands

backup pwd <password> path <usb1/usb2/usb3/usb4>

Example:

```
backup pwd pppWWW path usb1
```

Description:

Backup the system configuration and save it to the external USB drive “USB1”. Also encrypt this backup file with the password “pppWWW”.

Note: This feature is for SN1100CO / SN1100COD / SN0100CO / SN0100COD only.

restore pwd <password> path <usb1/usb2/usb3/usb4> filename <file_name>

Example:

```
restore pwd pppWWW path usb1 filename sysconf.dat
```

Description:

Restore the encrypted system configuration file “sysconf.dat” from the root directory of the external drive “USB1”, and decrypt it with the password “pppWWW”.

> **Note:** This feature is for SN1100CO / SN1100COD / SN0100CO / SN0100COD only.

backup pwd <password> path <tftp://host_address/folder>

Example:

```
backup pwd pppWWW path tftp://192.168.0.100/ATEN
```

Description:

Backup the system configuration to the TFTP site whose IP is “192.168.0.100” and the path is “/ATEN”. Also encrypt this backup file with the password “pppWWW”.

restore pwd <password> path <tftp://host_address/folder> filename <file_name>

Example:

```
restore pwd pppWWW path tftp://192.168.0.100/ATEN
filename sysconf.dat
```

Description:

Restore the encrypted system configuration file “sysconf.dat” from the TFTP site whose IP is “192.168.0.100” and the path is “/ATEN”, and decrypt it with the password “pppWWW”.

backup pwd <password> path <ftp://host_address/folder> ftpuser <username> ftppwd <password>

Example:

```
backup pwd pppWWW path ftp://192.168.0.100/ATEN ftpuser
willy ftppwd pppWWW
```

Description:

Backup the system configuration and save it to the FTP site whose IP is “192.168.0.100” and the path is “/ATEN”, and encrypt this backup file with the password “pppWWW”. The user name for logging in to the FTP site is “willy” and the login password is “pppWWW”.

restore pwd <password> path <ftp://host_address/folder> filename <file_name> ftpuser <username> ftppwd <password>

Example:

```
restore pwd pppWWW path ftp://192.168.0.100/ATEN
filename sysconf.dat ftpuser willy ftppwd pppWWW
```

Description:

Restore the system configuration file “sysconf.dat” from the FTP site whose IP is “192.168.0.100” and the path is “/ATEN”, and decrypt it with the password “pppWWW”. The user name for logging in to the FTP site is “willy” and the login password is “pppWWW”.

restore pwd <password> path < usb1/usb2/usb3 or tftp://host_address/folder/ or ftp://host_address/folder> filename <file_name> ftpuser <username> ftppwd <password> netconfig if <eth0/eth1/bond> <v4/v6> ip <IP_address> nm <subnet_mask> gw <gateway_address> set hostname=<host_name>

Example:

```
restore pwd pppWWW path ftp://192.168.0.100/ATEN
filename sysconf.dat ftpuser willy ftppwd pppWWW
netconfig if eth0 v4 ip 192.168.1.1 nm 255.255.255.0 gw
192.168.1.255 set hostname=SN9108CO
```

Description:

Restore the system configuration file “sysconf.dat” from the FTP site whose IP is “192.168.0.100” and the path is “/ATEN”, and decrypt it with the password “pppWWW”. The user name for logging in to the FTP site is “willy” and the login password is “pppWWW”.

Meanwhile, set the IP address of LAN port 1 to be 192.168.1.1, the subnet mask to be 255.255.255.0, and the gateway address to be 192.168.1.255. Set “SN9108CO” as the hostname or the device name of the serial console server.

Note: The parameters “ftpuser” and “ftppwd” are required when obtaining the backup file from a FTP site for performing a restore operation.

Firmware Upgrade Commands

update path <usb1/usb2/usb3> filename <file_name>

Example:

```
update path usb1 filename SN01_SN91xx_V1.7.161.001.fw
```

Description:

Update the firmware with the update file "SN01_SN91xx_V1.7.161.001.fw" which is stored on the root directory of the external drive "USB1".

> **Note:** This feature is for SN01xxCO / SN01xxCOD only.

update path <tftp://host_address/folder> filename <file_name>

Example:

```
update path tftp://192.168.0.100/ATEN filename
SN01_SN91xx_V1.7.161.001.fw
```

Description:

Update the firmware with the update file “SN01_SN91xx_V1.7.161.001.fw” which is stored on the TFTP site whose IP is “192.168.0.100” and the path is “/ATEN/”.

update path <ftp://host_address/folder> filename <file_name> ftpuser <username> ftppwd <password>

Example:

```
update path ftp://192.168.0.100/ATEN filename
SN01_SN91xx_V1.7.161.001.fw ftpuser willy ftppwd pppWWW
```

Description:

Update the firmware with the update file “SN01_SN91xx_V1.7.161.001.fw” stored on the FTP site whose IP is “192.168.0.100”, the path is “/ATEN/”, and user name for logging in to the FTP site is “willy”, and the login password is “pppWWW”.

IP Filter Commands

ipfilter <include/exclude>

Example:

```
ipfilter include
```

Description:

Enable IP filter function on include mode.

ipfilter off

Example:

```
ipfilter off
```

Description:

Disable IP filter function.

ipfilter

Example:

```
ipfilter
```

Description:

Show a list of all the filter conditions.

ipfilter cond <filter_condition> add

Example:

```
ipfilter cond 192.168.0.10 add
```

Description:

Add “192.168.0.10” to be one of the filter conditions to include/exclude this IP address.

Note:

- Use a comma to separate multiple addresses. (e.g. 192.168.1.10, 192.168.1.99)

- For a range of IP addresses, put a dash between the starting address and the ending address. (e.g. 192.168.0.10-192.168.0.100)

ipfilter index <index_number> delete

Example:

```
ipfilter index 1 delete
```

Description:

Delete the filter condition with index 1.

Account Policy Commands

acctp

Example:

```
acctp
```

Description:

Display the settings of the account policy.

acctp name <min_length>

Example:

```
acctp name 8
```

Description:

Set the minimum length of the username to at least a value of 8. The available value of the parameter `<min_length>` is from 1 to 32.

acctp pwd <min_length>

Example:

```
acctp pwd 8
```

Description:

Set the minimum length of password to at least a value of 8. The available value of the parameter `<min_length>` is from 1 to 32.

acctp pwdup <on/off>

Example:

```
acctp pwdup on
```

Description:

Require that the password must include at least one uppercase character.

acctp pwdlow <on/off>

Example:

```
acctp pwdlow on
```

Description:

Require that the password must include at least one lowercase character.

acctp pwdnum <on/off>

Example:

```
acctp pwdnum on
```

Description:

Require that the password must contain at least one digit.

acctp pwdspec <on/off>

Example:

```
acctp pwdspec on
```

Description:

Require that the password must contain at least one special character (symbol).

ATEN Warranty Policy

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

© Copyright 2026 ATEN® International Co., Ltd.
Released: 2026-07-27

ATEN and the ATEN 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.