



SN3001 / SN3001P

SN3002 / SN3002P

SN3401 / SN3401P

SN3402 / SN3402P

보안 시리얼 장치 서버

사용 설명서

규정 준수 성명서

연방 통신위원회 간섭 성명서

이 제품은 Class A 디지털 장치로서 FCC 규정 15장에 준한 기준에 부합하기 위한 테스트를 받아왔고 그 조건을 갖추었습니다. 이러한 조건들은 장치가 상업 환경에서 동작할 때 유해한 간섭에 대해 적절히 장치를 보호하도록 제작되었습니다. 이 장치는 라디오 주파수 에너지를 생성, 사용하고 방출할 수 있습니다. 만약 본 제품을 설명서를 따라 설치하지 않거나 사용하지 않는다면ⁱⁱ 라디오 통신에 방해가 되는 간섭을 일으킬 수도 있습니다. 거주 지역 내에 이 장치가 동작할 때 사용자가 자비로 해결할 필요가 있는 유해한 간섭이 생길 수 있습니다. 이 장치는 FCC 규정 15장을 준수합니다. 동작은 다음 2가지 조건에 부합합니다. (1) 이 장치는 유해한 간섭을 일으켜서는 안되며 (2) 이 장치는 설사 원하지 않는 동작을 유발하는 어떠한 간섭을 받더라도 받아들여야 합니다.

FCC 경고

규정을 준수할 책임이 있는 당사자에 의해 명시적으로 허가되지 않은 변경이나 수정을 하면 본 장비를 작동하는 사용자의 권한이 무효화될 수 있습니다.

경고

이 장비의 동작은 주거 지역에서 간섭을 일으킬 수 있습니다.

Achtung

Der Gebrauch dieses Geräts in Wohnumgebung kann Funkstörungen verursachen.

제안

FCC 및 CE 표준을 준수하기 위해 장치에는 차폐 연선(STP) 케이블을 사용해야 합니다.



KCC 성명서

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.

캐나다 산업부 선언문

본 Class A 디지털 장치는 캐나다 ICES-003을 준수합니다.

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

RoHS

이 제품은 RoHS 기준을 준수합니다.

사용자 정보

온라인 등록

제품을 온라인 지원 센터에 등록하십시오.

국제	http://eservice.aten.com
----	-----------------------------------------------------------------

전화 연결 지원

전화 연결 지원은 아래 번호로 연락해 주십시오.

국제	886-2-8692-6959
중국	86-400-810-0-810
일본	81-3-5615-5811
한국	82-2-467-6789
북미	1-888-999-ATEN 내선 4988 1-949-428-1111

사용자 공지

이 설명서에 포함된 모든 정보, 문서 및 사양은 사전 통지 없이 변경될 수 있습니다. 제조 업체는 이 문서의 내용과 관련하여 명시적이든 묵시적이든 어떠한 진술이나 보증도 하지 않으며 특정 목적에 대한 상품성 또는 적합성에 대한 보증을 구체적으로 부인합니다. 이 설명서에 설명된 모든 제조 업체의 소프트웨어는 있는 그대로 판매되거나 라이선스가 부여됩니다. 프로그램이 구매 후 결함이 있는 것으로 판명되면 구매자 (제조업체, 유통 업체 또는 대리점이 아님)는 소프트웨어 결함으로 인한 모든 필요한 서비스, 수리 및 우발적 또는 결과적 손해에 대한 전체 비용을 부담합니다.

이 제품의 제조사는 이 제품에 허가되지 않은 변경을 하여 발생하는 라디오 또는 TV 주파수 간섭에 대한 책임이 없습니다. 이러한 주파수 간섭 현상을 처리하는 것은 사용자의 책임입니다. 만약 정확한 동작을 위한 전압 설정이 되지 않았다면 제조사는 이 제품의 동작 중에 발생할 어떠한 피해에도 책임이 없습니다. **사용 전에 전압 설정이 정확한지 확인해 주십시오.**

제품 정보

모든 ATEN 제품군의 정보를 위하여 그리고 사용자가 제한 없이 ATEN 웹사이트나 승인된 ATEN 판매자를 방문할 수 있도록 해드립니다. 지역 목록과 전화번호를 찾으시려면 ATEN 웹사이트를 방문하십시오.

국제	http://www.aten.com
북미	http://www.aten-usa.com

패키지 구성

모든 구성 요소가 정상 작동하는지 확인하십시오. 문제가 발생하면 대리점에 문의하십시오.

SN3001 / SN3002 / SN3401 / SN3402

표준 SN3001 / SN3002 / SN3401 / SN3402 패키지 구성은 다음과 같습니다.

- ◆ 1 x 보안 시리얼 장치 서버 (SN3001 / SN3002 / SN3401 / SN3402)
- ◆ 1 x 전원 아답터
- ◆ 1 x 터미널 블록
- ◆ 1 x 고무 패드 세트 (4 pcs)
- ◆ 1 x DIN 레일 마운트 키트
- ◆ 1 x 사용자 설명서*

SN3001P / SN3002P / SN3401P / SN3402P

표준 SN3001P / SN3002P 패키지 구성은 다음과 같습니다.

- ◆ 1 x 보안 시리얼 장치 서버 (PoE 지원) (SN3001P / SN3002P / SN3401P / SN3402P)
- ◆ 1 x 터미널 블록
- ◆ 1 x 고무 패드 세트 (4 pcs)
- ◆ 1 x DIN 레일 마운트 키트
- ◆ 1 x 사용자 설명서*

목차

규정 준수 성명서.	ii
사용자 정보.	iv
온라인 등록.	iv
전화 연결 지원.	iv
사용자 주의사항.	iv
제품 정보.	v
패키지 구성.	vi
SN3001 / SN3002 / SN3401 / SN3402	vi
SN3001P / SN3002P / SN3401P / SN3402P	vi
목차.	vii
설명서에 관하여.	xi
규정.	xiii

1장. 소개

개요.	1
기능.	2
시리얼-이더넷 연결.	2
하드웨어.	2
보안.	3
시스템 관리.	3
하드웨어 개요.	4
SN3001 / SN3001P / SN3002 / SN3002P	4
전면	4
후면	4
상단	5
SN3401 / SN3401P / SN3402 / SN3402P	6

2장. 하드웨어 설치

시작하기 전에.	9
배치 옵션.	9
월 마운트.	9
DIN 레일 마운트.	10
병렬 DIN 레일 마운트.	10
수직 DIN 레일 마운트.	11
랙 마운트.	12
설치.	15
시리얼 포트 핀 할당	17

3장. 네트워크 환경 구성 및 로드인

IP 주소 결정.	19
IP 인스톨러 유틸리티.	19

IP 인스톨러 미사용 (non-DHCP 전용).	20
로그인.	21
빠른 설정 마법사.	22
일반.	22
네트워크.	23
시리얼.	24

4장. 웹 콘솔

웹 인터페이스.	25
시리얼 포트.	26
시리얼 포트 편집.	27
속성.	27
포트 버퍼링.	28
동작 모드.	30
네트워크.	37
시스템.	38
일반 설정.	39
일반.	39
시간.	41
알림.	42
SMTP.	42
SNMP.	43
Syslog.	44
고급.	45
보안.	46
접속 보호 (IP 필터).	46
보안 수준.	47
계정 정책.	47
보안 인증서.	48
업데이트 및 복원.	49
펌웨어 업데이트.	49
백업 및 복원.	50
프로토콜 게이트웨이.	51
사용자 계정.	52
로그.	53

5장. 사용자 관리

개요.	55
사용자.	55
사용자 추가.	56
사용자 편집.	57
사용자 삭제.	58
온라인 사용자.	58
인증 서비스.	59
RADIUS.	59

6장. 포트 동작 모드

개요.	61
동작 모드 선택.	61
동작 모드.	63
Real COM.	63
TCP 서버 및 클라이언트.	63
TCP 서버.	63
TCP 클라이언트.	64
시리얼 터널링 서버 및 클라이언트.	64
UDP 모드.	65
콘솔 관리.	65
콘솔 관리 다이렉트.	66
비활성화.	66
Modbus 게이트웨이.	66
일반적인 애플리케이션.	66

7장. 포트 접속

개요.	69
Telnet / SSH.	70
SNViewer.	70
컨트롤 패널 기능.	71
데이터 가져오기.	72
인코딩.	72
터미널 설정.	72

8장. 원격 터미널 동작

개요.	75
터미널 로그인.	75
Telnet 로그인.	75
SSH 로그인 (Linux).	76
써드파티 유틸리티 (Windows).	76
터미널 메인 메뉴.	77

9장. 버추얼 시리얼 포트 관리자

개요.	79
Real COM 포트 관리 — 버추얼 시리얼 포트 관리자.	80
유틸리티 인터페이스.	80
메뉴 및 도구 모음.	81
대상 정보.	81
대상 목록.	82
포트 목록.	83
포트 매핑 및 매핑 해제.	84
포트 매핑.	84
매핑된 COM 포트.	84
포트 매핑 해제.	85

Real COM 포트 관리 — Linux 명령어.	86
버추얼 포트 매핑/매핑 해제.	86
버추얼 포트 이름 설정 규칙.	86

부록

안전 지시 사항.	87
일반	87
DC 전원	89
랙 마운팅.	90
기술 지원.	91
국제 지역.	91
북미 지역	91
사양.	92
SN3001 / SN3001P / SN3002 / SN3002P	92
SN3401 / SN3401P / SN3402 / SN3402P	94
로그인 정보 삭제.	97
문제 해결	98
보증 제한.	99

설명서에 관하여

본 사용자 설명서는 보안 시리얼 장치 서버를 이해할 수 있도록 돕기 위해 제공됩니다. 장치, 설치, 환경 구성 및 동작을 포함한 전반적인 것을 다룹니다.

본 사용자 설명서에서 다루는 보안 서버 장치 모델은 다음과 같습니다.

모델	제품명
SN3001	1 포트 RS-232 보안 시리얼 장치 서버
SN3001P	1 포트 RS-232 보안 시리얼 장치 서버 with PoE
SN3002	2 포트 RS-232 보안 시리얼 장치 서버
SN3002P	2 포트 RS-232 보안 시리얼 장치 서버 with PoE
SN3401	1 포트 RS-232/RS-422/RS-485 보안 시리얼 장치 서버
SN3401P	1 포트 RS-232/RS-422/RS-485 보안 시리얼 장치 서버 with PoE
SN3402	2 포트 RS-232/RS-422/RS-485 보안 시리얼 장치 서버
SN3402P	2 포트 RS-232/RS-422/RS-485 보안 시리얼 장치 서버 with PoE

본 설명서에 있는 전체 정보 개요는 아래와 같이 제공합니다.

1장, 소개, 보안 시리얼 장치 서버를 소개합니다. 그 목적, 기능, 장점을 소개하고 전면 및 후면 패널 구성 요소를 설명합니다.

2장, 하드웨어 설치, 보안 시리얼 장치 서버 설정을 단계별로 제공합니다.

3장, 네트워크 환경 구성 및 로그인, 웹 브라우저에서 보안 시리얼 장치 서버에 로그인하는 방법을 설명합니다.

4장, 웹 콘솔, 보안 시리얼 장치 서버의 작업 환경을 구성하는 데 사용되는 관리 절차를 설명합니다.

5장, 사용자 관리, 로그인 계정 및 RADIUS와 같은 써드파티 인증 서비스 지원에 대해 자세히 설명합니다.

6장, 포트 동작 모드, 보안 시리얼 장치 서버의 동작 모드를 소개하고 각각의 목적을 설명합니다.

7장, 포트 접속, 보안 시리얼 장치 서버의 COM 포트에 접속하고 SNViewer를 시작하는 방법을 설명합니다.

8장, 원격 터미널 동작, Telnet, SSH, PuTTY와 같은 원격 터미널 세션을 통해 보안 시리얼 장치 서버에 접속하는 방법을 설명합니다.

9장, 버추얼 시리얼 포트 관리자, 버추얼 COM 포트 드라이버를 설치하고 버추얼 COM 포트를 설정 및 관리하는 방법을 보여줍니다.

부록, 설명서 끝에 기술 및 문제 해결 정보를 제공합니다.


주의:

- ◆ 이 설명서를 자세히 읽고 장치 또는 연결된 장치의 손상을 방지하기 위해 설치 및 동작 절차를 주의하여 따르십시오.
- ◆ 본 제품은 이 설명서 배포 이후에 기능이 추가, 개선 또는 제거되어 업데이트될 수 있습니다. 최신 사용자 설명서를 확인하려면 다음 사이트를 방문하십시오.

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

규정

본 설명서는 다음과 같은 규정을 따릅니다.

- | | |
|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Monospaced | 입력해야 하는 글자를 가리킵니다. |
| [] | 눌러야 하는 키들을 가리킵니다. 예를 들면 [Enter]는 키보드의 Enter 키를 누르라는 의미입니다. 키를 조합할 필요가 있는 경우 괄호 안에서 키 사이에 + 표시를 합니다: [Ctrl+Alt]. |
| 1. | 번호가 매겨진 목록은 순차적인 진행과정을 나타냅니다. |
| ◆ | 다이아몬드 표시 목록은 정보를 제공하지만 순차적인 과정과는 관련이 없습니다. |
| → | 메뉴나 대화 상자에서 다음에 선택하는 옵션을 말합니다. 예를 들어 시작 → 실행은 시작 메뉴를 고르고 나서 실행을 선택하라는 의미입니다. |
|  | 중요 정보를 가리킵니다. |

이 페이지는 빈 페이지 입니다.

1 장

소개

개요

SN시리즈 - 보안 시리얼 장치 서버는 시리얼 장치를 위한 보안을 보장하는 IP 기반 LAN 연결을 제공하고 광범위한 동작 모드를 지원합니다. 일반적인 시리얼 장치 (PLC, 계측기, 센서)를 네트워크에 연결하고 네트워크를 통해 어디서나 접속하고 관리할 수 있도록 합니다.

보안 Real COM, 보안 TCP 클라이언트 및 서버, 보안 시리얼 터널링 및 보안 콘솔 관리와 같은 광범위한 보안 기능을 갖춘 보안 시리얼 장치 서버는 보안에 민감한 다양한 분야에서 이상적인 시리얼 장치 관리를 해주는 솔루션입니다.

기존 시리얼 통신 소프트웨어와 완벽하게 호환되는 보안 시리얼 장치 서버는 소프트웨어 개발에 대한 비용을 절감하게 해줍니다. COM 또는 TTY 포트와 함께 동작하도록 설계된 소프트웨어는 보안 시리얼 장치 서버의 Real COM 또는 TTY 드라이버를 사용하여 TCP/IP 네트워크를 통해 연결된 시리얼 장치에 접속할 수 있습니다. 또한 이 기능은 PC 하드웨어에서 발생하는 포트 개수 및 거리 제한 장벽을 넘어설 수 있습니다.

SSL 및 SSH 프로토콜 지원 (데이터 전송 암호화용) - 보안 시리얼 장치 서버는 개인 및 공용 네트워크를 통해 안전한 데이터 전송을 보장합니다.

보안 시리얼 장치 서버를 설치하는 것은 빠르고 쉽습니다. 적절한 포트에 케이블을 연결하기만 하면 됩니다. 또한 브라우저 기반 GUI, Telnet/SSH 콘솔 세션, Windows 소프트웨어 유틸리티를 제공하여 환경 구성 및 동작이 빠르고 원활합니다.

SN3001P / SN3002P / SN3401P / SN3402P는 IEEE 802.3af를 준수하는 PoE 기능을 제공하므로 추가 전원 공급 장치 없이 PoE 스위치/아답터로 이더넷 케이블을 통해 전원을 공급받을 수 있습니다.

전체적으로 고급 기능과 동작 용이성을 갖춘 보안 시리얼 장치 서버는 시리얼 장치를 원격으로 관리하는 가장 편리하고 안정적이며 비용 효율적인 방법입니다.

기능

시리얼-이더넷 연결

- ◆ 이더넷 전송을 통한 보안 시리얼 데이터용 RS-232 시리얼 포트 1개 또는 2개 (SN3001/SN3001P/SN3002/SN3002만 해당)
- ◆ 이더넷 전송을 통한 보안 시리얼 데이터용 RS-232/RS-422/RS-485 시리얼 포트 1개 또는 2개 (SN3401/SN3401P/SN3402/SN3402P만 해당)
- ◆ Modbus TCP와 Modbus RTU/ASCII 프로토콜 간 변환을 위한 Modbus 게이트웨이 지원 (SN3401/SN3401P/SN3402/SN3402P만 해당)
- ◆ 보안 동작 모드 - 보안 Real COM, 보안 TCP 서버/클라이언트, 보안 시리얼 터널링, 콘솔 관리 (SSH) 및 콘솔 관리 다이렉트 (SSH)
- ◆ 표준 동작 모드 — Real COM, TCP 서버/클라이언트, 시리얼 터널링, UDP, 콘솔 관리 (Telnet) 및 콘솔 관리 다이렉트 (Telnet)
- ◆ 신호 반사를 피하기 위해 RS-485 모드에 통합된 소프트웨어 구성 가능한 종단 (120 Ω) 및 pull high/low 저항(1K Ω 또는 150K Ω) (SN3401/SN3401P/SN3402/SN3402P만 해당)
- ◆ Windows, Linux, UNIX용 Real COM, Real TTY, Fixed TTY 드라이버
- ◆ Java 뷰어 (SSH/Telnet) 또는 PuTTY와 같은 써드파티 클라이언트를 통한 편리한 콘솔 관리 접속
- ◆ Java 뷰어 및 Sun Solaris ready ("break-free")를 통한 간편한 콘솔 포트 접속
- ◆ 여러 사용자가 동시에 동일한 포트에 접속 가능 — 포트 당 최대 16개 연결

하드웨어

- ◆ 정전 시 보호를 위한 대체 전원 입력 (전원 잭 및 터미널 블록)
- ◆ IEEE 802.3af 준수 PoE 전원 장치 장비 (SN3001P/SN3002P/SN3401P/SN3402P만 해당)
- ◆ 시리얼, 이더넷, 전원을 위한 서지 보호
- ◆ 월 및 DIN 레일 마운팅, 랙 마운팅 (옵션 키트 VE-RMK1U 필요) 및 데스크탑 설치 가능
- ◆ baud rates (110, 134, 150, 300, 600, 1200, 1800, 2400, 4800, 7200, 9600, 19200, 38400, 57600, 115200, 230.4k, 460.8k, 921.6k bps) 지원

보안

- ◆ TLS 1.2 데이터 암호화 및 RSA 2048 bit 인증서로 브라우저에서 보안 로그인 지원
- ◆ 포트 접속 및 제어를 위한 구성 가능한 사용자 권한
- ◆ 로컬 및 원격 인증 및 로그인
- ◆ 써드파티 인증 (예: RADIUS)
- ◆ 보안 보호를 위한 IP 주소 필터

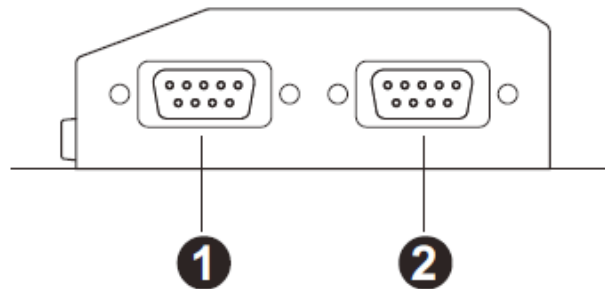
시스템 관리

- ◆ 직관적인 GUI를 통한 브라우저 접속
- ◆ 빠른 구성을 위한 웹 기반 빠른 설정 마법사
- ◆ Telnet/SSH를 통한 메뉴 기반 UI를 통한 터미널 기반 접속
- ◆ 연결된 시리얼 장치 (터미널 블록 포함)의 온라인/오프라인 감지 - 장치 상태 모니터링을 위해 장치가 오프라인 (예: 정전)일 때 이벤트 알림을 자동으로 전송
- ◆ 시스템 이벤트 로그는 내부 메모리 또는 시스템 로그 서버에 저장
- ◆ 포트 로그는 내부 메모리 또는 시스템 로그 서버에 저장
- ◆ SNMP 에이전트 (v1/v2c)
- ◆ 이벤트 알림 - SMTP 이메일 및 SNMP 트랩 알림 지원 (v1/v2c)
- ◆ 시스템 구성 및 업그레이드 가능한 펌웨어 백업/복원
- ◆ 64KB 포트 버퍼로 네트워크 다운 시 데이터 손실 방지
- ◆ 시간 서버 동기화를 위한 NTP
- ◆ 다국어 웹 기반 GUI

하드웨어 개요

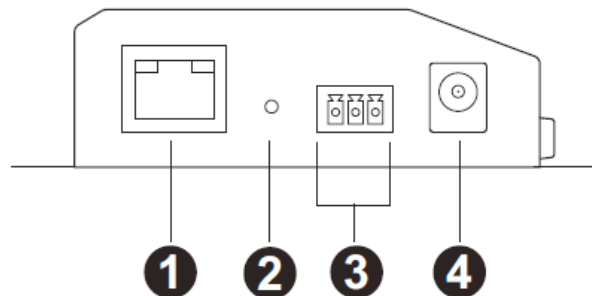
SN3001 / SN3001P / SN3002 / SN3002P

전면



번호	구성	설명
1	RS-232 시리얼 포트 1	RS-232 시리얼 장치에 연결합니다.
2	RS-232 시리얼 포트 2	2번째 RS-232 시리얼 장치에 연결합니다. (SN3002 / SN3002P만 해당)

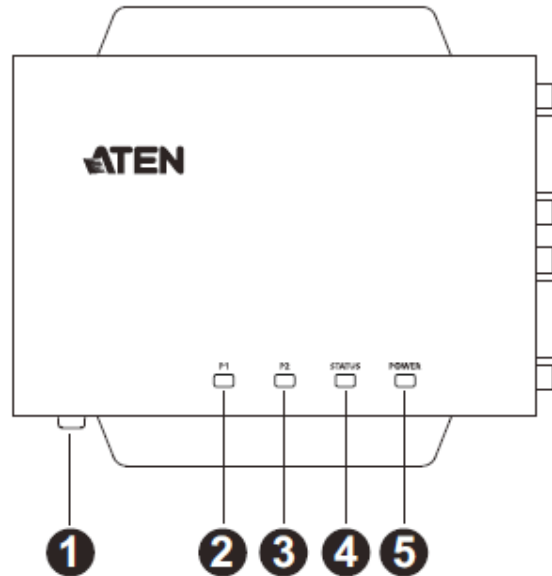
후면



번호	구성	설명
1	LAN 포트	LAN 포트 보안 시리얼 장치 서버를 네트워크에 연결합니다. SN3001P / SN3002P (PoE 802.3af 준수)의 경우, PoE 스위치를 통해 동시에 전원을 공급할 수 있습니다.
2	리셋 버튼	3초 미만으로 누르고 있으면 시스템이 다시 시작됩니다. 3초 이상 길게 누르면 설정(사용자 계정 설정 및 권한 제외)이 기본 상태로 돌아갑니다.
3	전원 터미널	제공된 DC 전기 리드와 터미널 블록을 통해 보안 시리얼 장치 서버를 전원에 연결합니다.

번호	구성	설명
4	전원 잭	전원 아답터를 사용하여 보안 시리얼 장치 서버를 전원에 연결합니다.

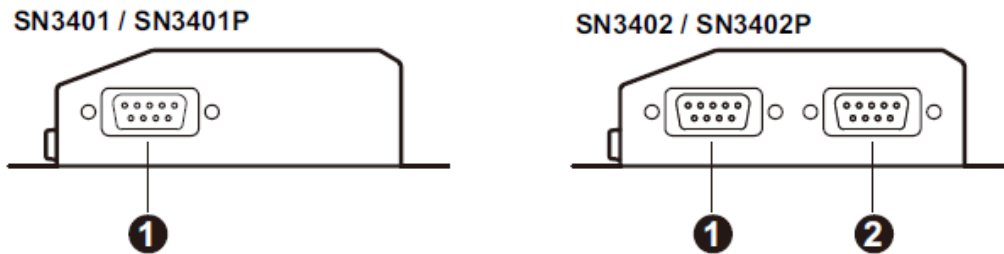
상단



번호	구성	설명
1	접지 터미널	접지선을 사용하여 적절한 접지 물체에 연결하여 장치를 접지합니다.
2	시리얼 포트 1 LED	장치의 RS-232 시리얼 포트 1을 통해 데이터를 송신 또는 수신 시 녹색 또는 주황색으로 켜집니다.
3	시리얼 포트 2 LED	장치의 RS-232 시리얼 포트 2를 통해 데이터를 송신 또는 수신 시 녹색 또는 주황색으로 켜집니다. (SN3002 / SN3002P만 해당)
4	상태 LED	정상 작동 또는 시작 시 각각 노란색/녹색으로 켜지거나 깜박이고 오류 (예: 하드웨어 오류 및 DHCP 이상)가 발생하면 빨간색으로 켜집니다.
5	전원 LED	보안 시리얼 장치 서버에 전원이 공급되고 준비되면 녹색으로 켜집니다.

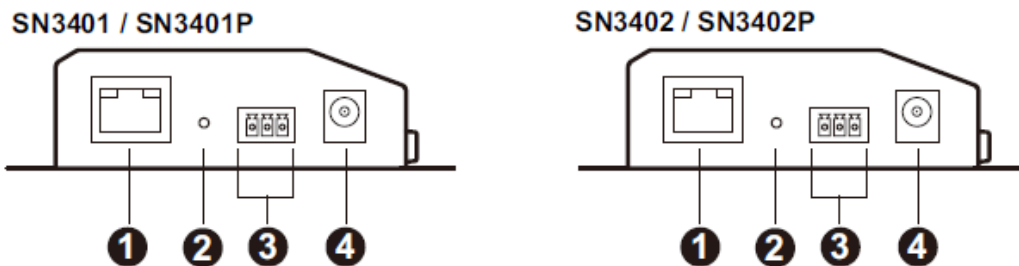
SN3401 / SN3401P / SN3402 / SN3402P

전면



번호	구성	설명
1	시리얼 포트 1	RS-232 / RS-422 / RS-485 시리얼 장치에 연결합니다.
2	시리얼 포트 2	2번째 RS-232 / RS-422 / RS-485 시리얼 장치에 연결합니다. (SN3402 / SN3402P만 해당)

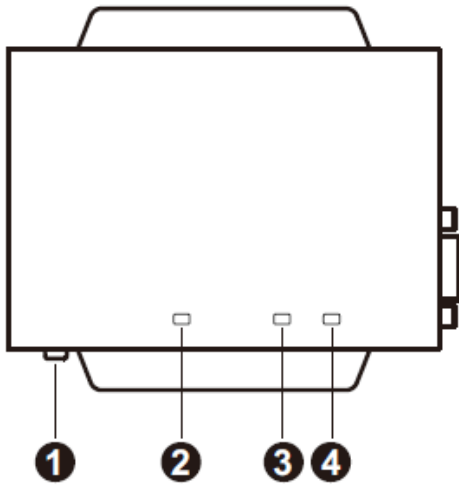
후면



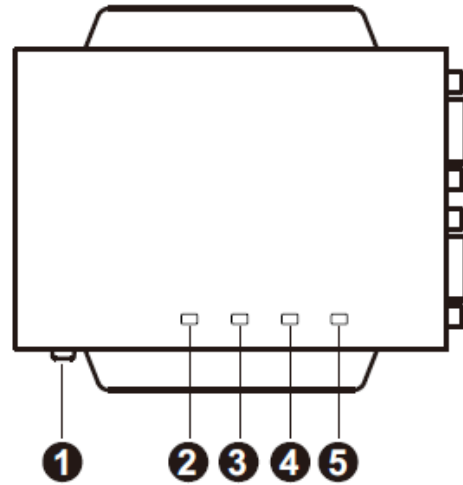
번호	구성	설명
1	LAN 포트	LAN 포트 보안 시리얼 장치 서버를 네트워크에 연결합니다. SN3402 / SN3402P (PoE 802.3af 준수)의 경우, PoE 스위치를 통해 동시에 전원을 공급할 수 있습니다.
2	리셋 버튼	3초 미만으로 누르고 있으면 시스템이 다시 시작됩니다. 3초 이상 길게 누르면 설정(사용자 계정 설정 및 권한 제외)이 기본 상태로 돌아갑니다.
3	전원 터미널	제공된 DC 전기 리드와 터미널 블록을 통해 보안 시리얼 장치 서버를 전원 에 연결합니다.

상단

SN3401 / SN3401P



SN3402 / SN3402P



번호	구성	설명
1	접지 터미널	접지선을 사용하여 적절한 접지 물체에 연결하여 장치를 접지합니다.
2	시리얼 포트 1 LED	장치의 시리얼 포트 1을 통해 데이터를 송신 또는 수신 시 녹색 또는 주황색으로 켜집니다.
3	시리얼 포트 2 LED	장치의 시리얼 포트 2를 통해 데이터를 송신 또는 수신 시 녹색 또는 주황색으로 켜집니다. (SN3402 / SN3402P만 해당)
4	상태 LED	정상 작동 또는 시작 시 각각 노란색/녹색으로 켜지거나 깜박이고 오류 (예: 하드웨어 오류 및 DHCP 이상)가 발생하면 빨간색으로 켜집니다.
5	전원 LED	보안 시리얼 장치 서버에 전원이 공급되고 준비되면 녹색으로 켜집니다.

이 페이지는 빈 페이지 입니다.

2 장

하드웨어 설치

시작하기 전에



1. 이 장치의 배치와 관련된 중요한 안전 정보는 87페이지에 있습니다. 진행하기 전에 검토하십시오.
2. 연결하려는 모든 장치의 전원이 꺼져 있는지 확인하십시오.

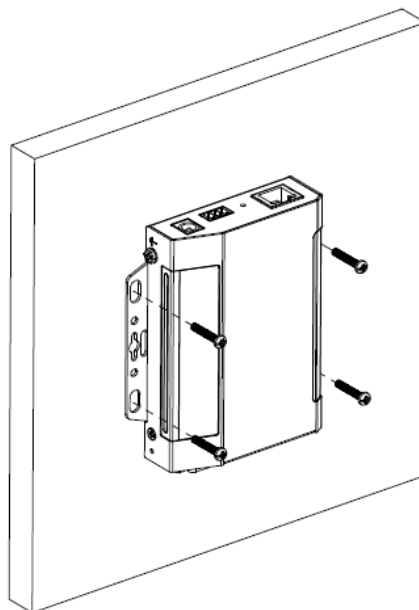
배치 옵션

유연성과 편의성을 위해 보안 시리얼 장치 서버는 아래 설명과 같이 벽이나 DIN 레일에 마운트 할 수 있습니다.

월 마운트

보안 시리얼 장치 서버를 벽에 마운트 하려면, 다음을 수행하십시오.

사용자는 4개의 자체 제공되는 나사를 사용하여 아래 그림과 같이 측면의 나사 구멍을 통해 장치를 벽에 마운트 할 수 있습니다.

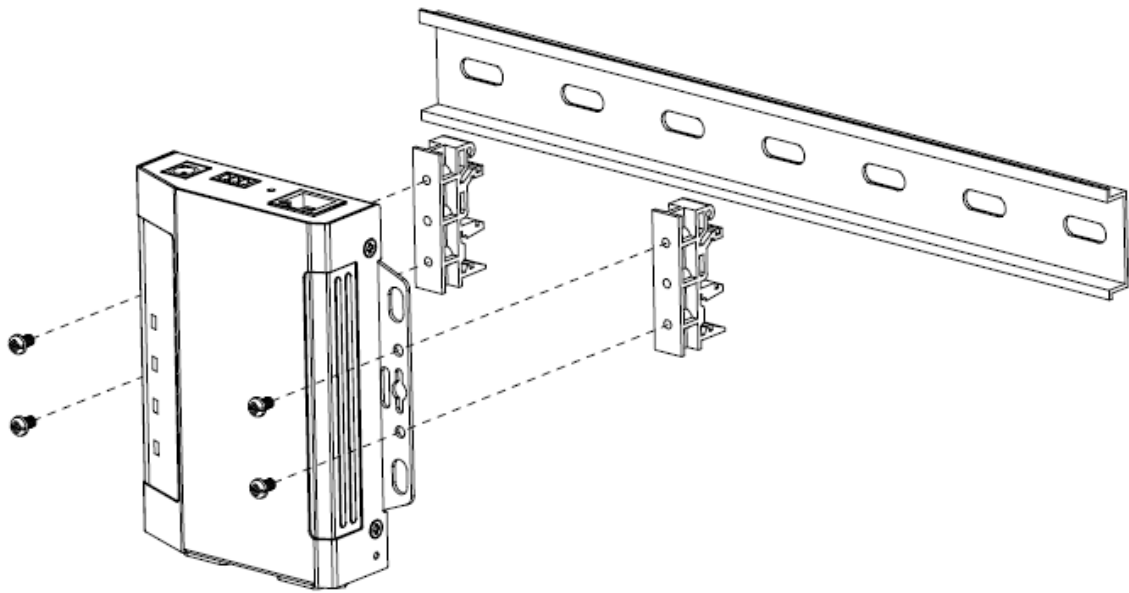


DIN 레일 마운트

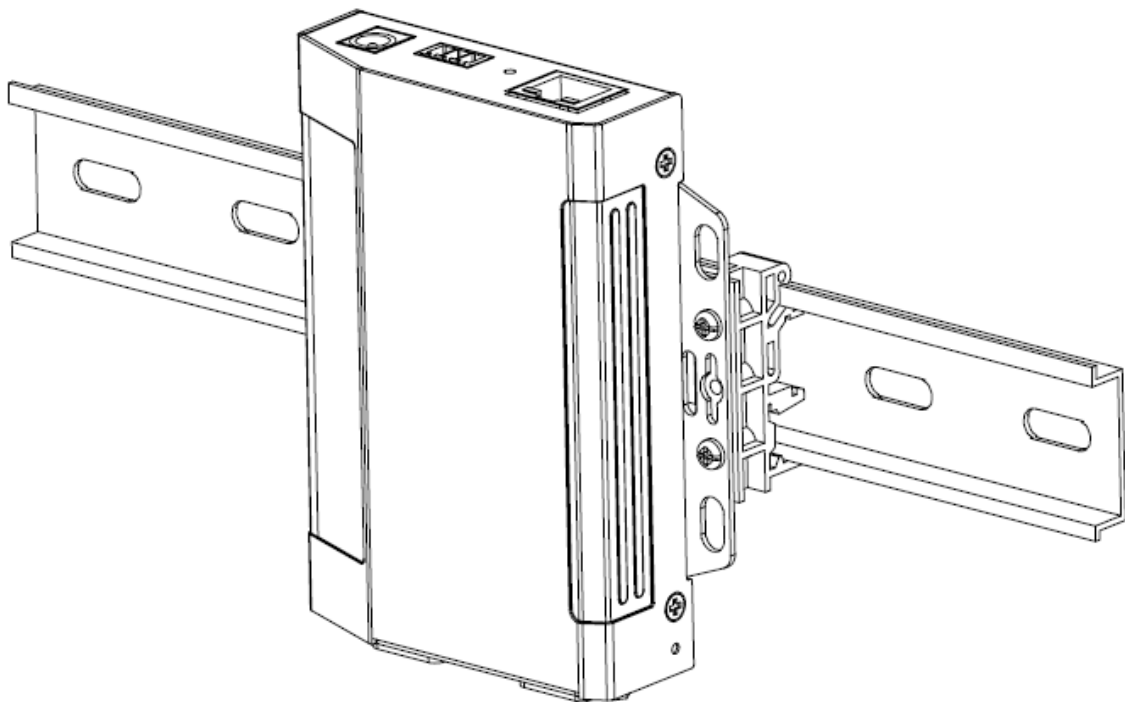
포함된 DIN 레일 마운트 키트를 사용하여 아래 지시 사항에 따라 DIN 레일에 보안 시리얼 장치 서버를 마운트 합니다.

병렬 DIN 레일 마운트

1. 장치를 DIN 레일에 병렬로 장착하려면 제공된 4개의 나사를 사용하여 중앙 나사 구멍을 통해 장치에 2개의 DIN 레일 장착 브라켓을 부착합니다.

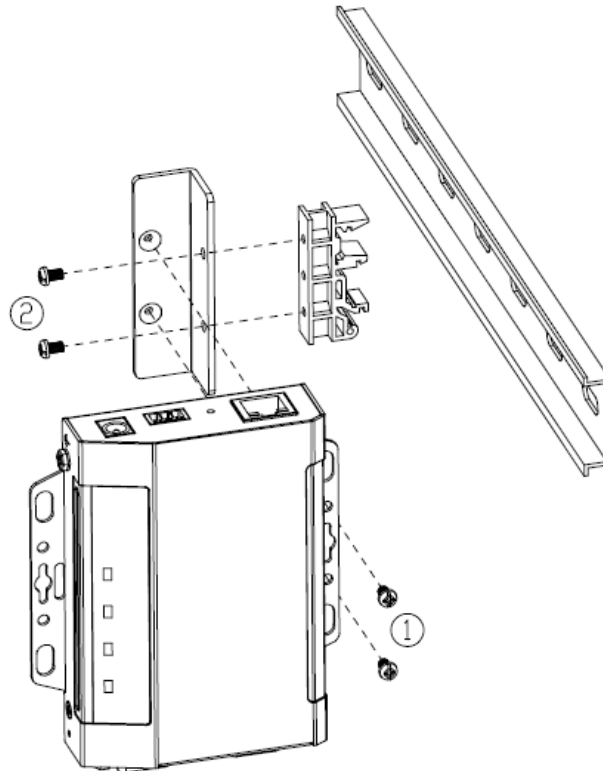


2. 장치를 DIN 레일에 겁니다.

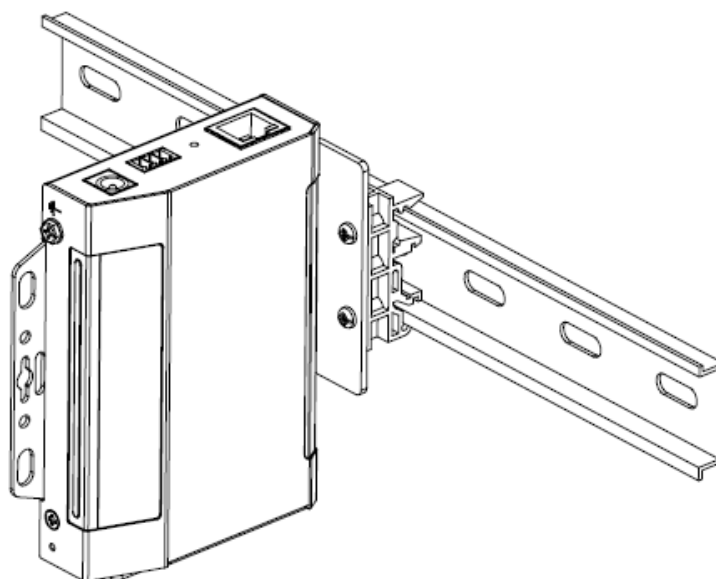


수직 DIN 레일 마운트

1. 접지 터미널 반대쪽에 있는 중앙 나사 구멍을 통해 M3x6 나사 2개를 사용하여 L자형 장착 브라켓을 장치에 부착합니다.
2. 동봉된 4개의 나사 중 2개를 사용하여 DIN 레일 장착 브라켓 1개를 L자형 장착 브라켓 측면에 부착합니다.



3. 장치를 DIN 레일에 겁니다.

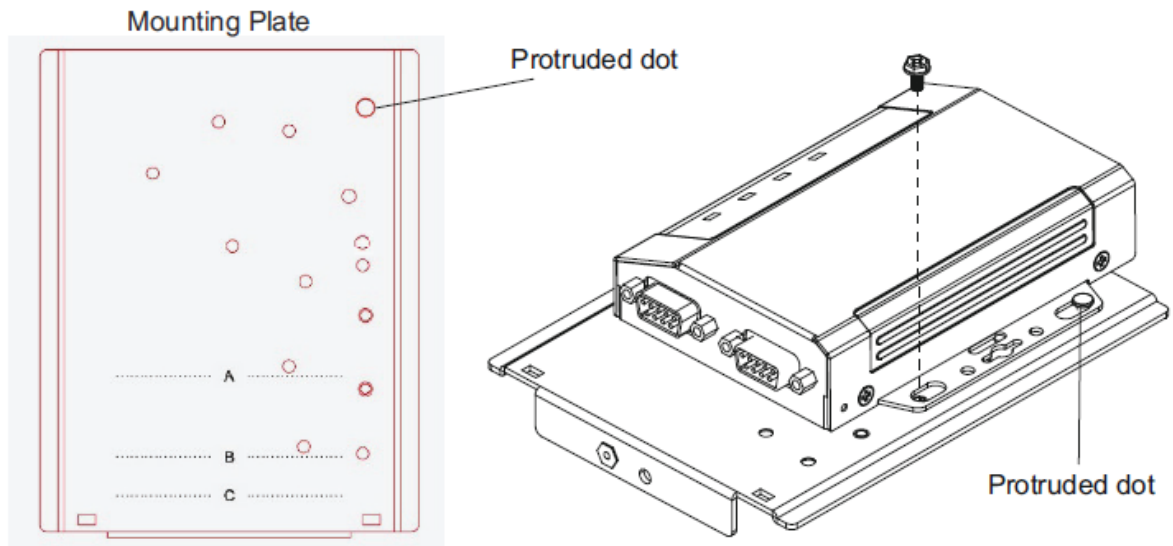


랙 마운트

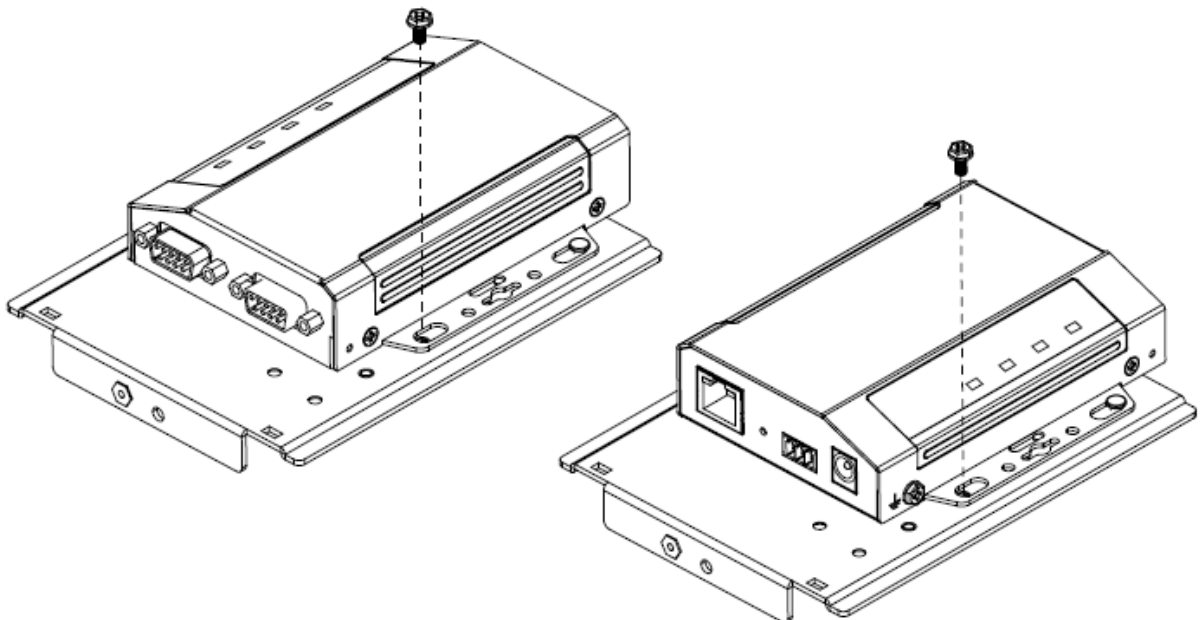
랙 마운트 키트 (VE-RMK1U)는 보안 시리얼 장치 서버를 마운트 하기 위해 필요합니다.

아래 지시 사항에 따라 랙에 장치 서버를 연결하십시오.

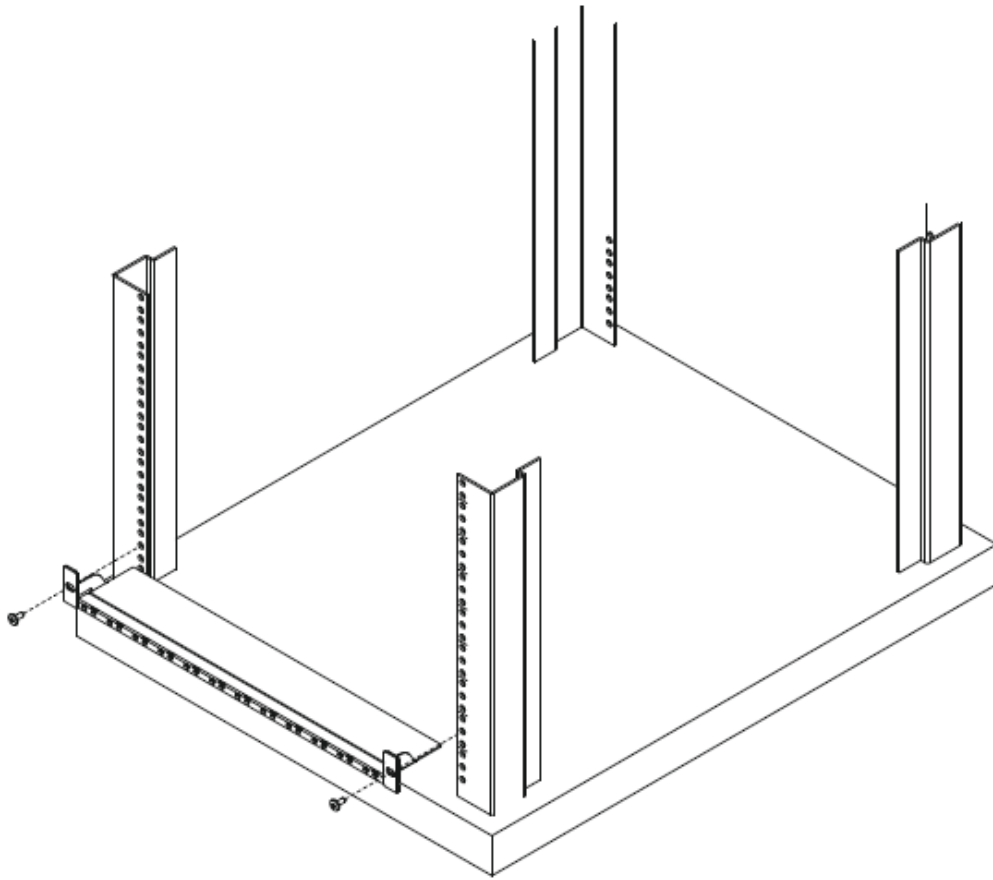
1. 아래 그림과 같이 랙 구멍 중 하나를 플레이트의 돌출된 점에 걸면서 장치를 마운팅 플레이트에 놓으십시오.



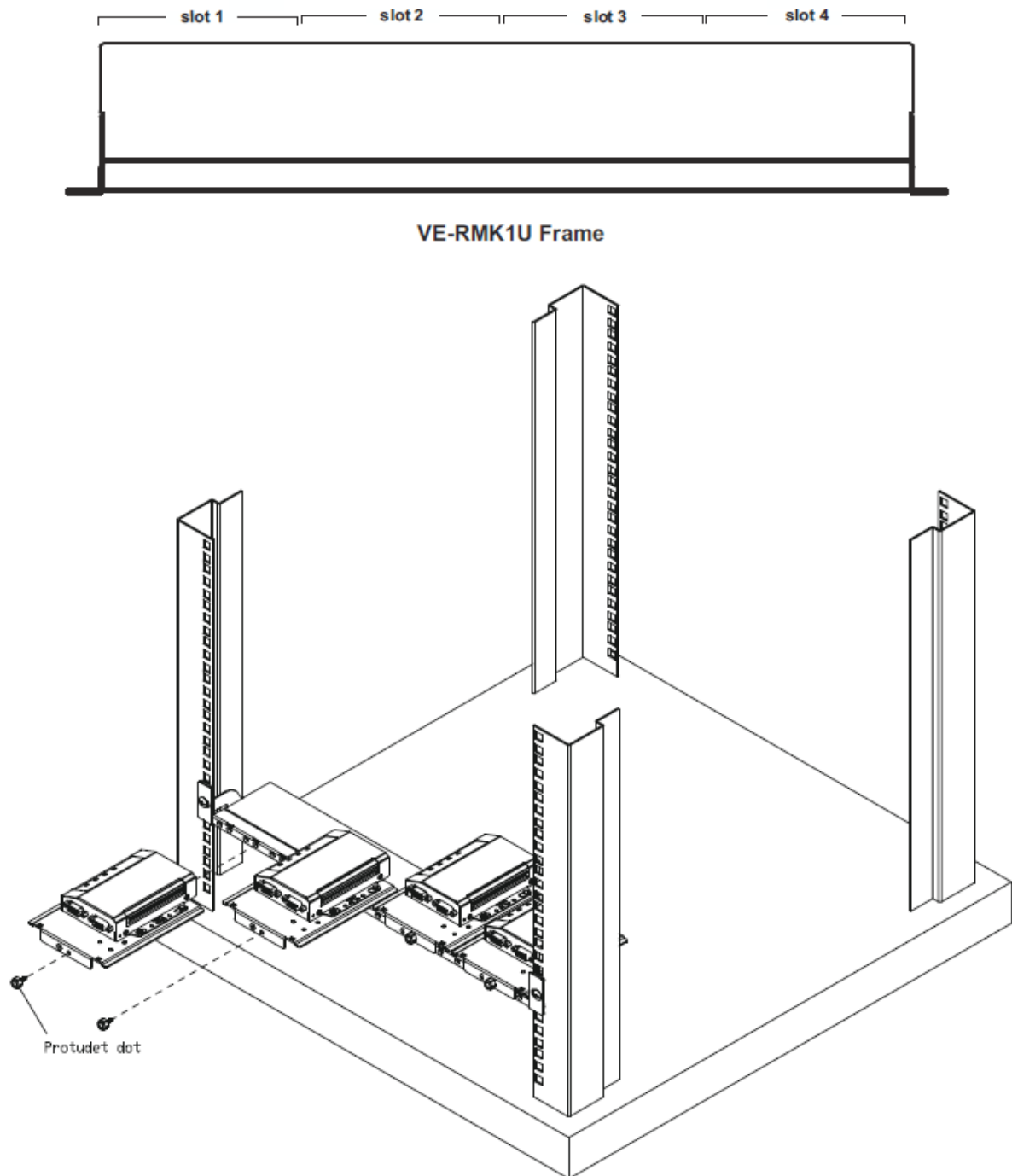
2. 제공된 육각 머리 나사를 사용하여 장치를 마운팅 플레이트에 고정하십시오. 사용자는 시리얼 포트가 안쪽 또는 바깥 쪽을 향하도록 보안 시리얼 장치 서버를 고정할 수 있습니다.



3. 아래 그림과 같이 VE-RMK1U 프레임의 구멍을 랙의 구멍에 정렬하고 자체 제공된 나사 2개를 사용하여 프레임을 랙에 고정하십시오.



4. 장치 및 마운팅 플레이트 어셈블리를 VE-RMK1U 프레임 상의 슬롯 중 하나에 정렬하십시오.
그 다음 제공된 플라스틱 나사를 사용하여 마운팅 플레이트를 프레임에 고정하십시오.

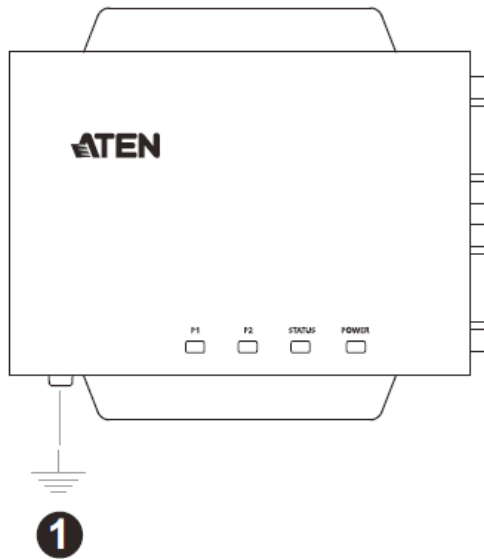


주의: 최대 4개의 보안 시리얼 장치 서버를 VE-RMK1U 프레임에 고정할 수 있습니다.

설치

보안 시리얼 장치 서버를 설치하려면, 아래 단계를 따르고 다음 페이지의 그림을 참조하십시오 (번호는 설치 단계에 해당)

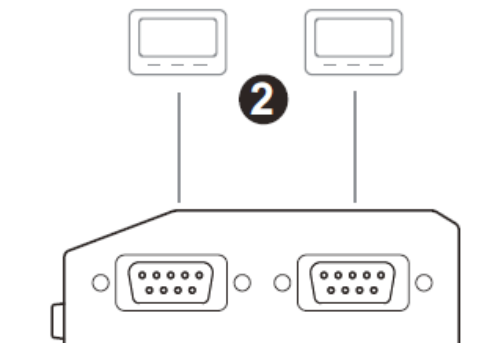
1. 접지 단자의 한쪽 끝과 다른 쪽 끝을 적절한 접지 물체에 연결하여 접지선을 사용하여 장치를 접지하십시오.



주의: 이 단계를 건너뛰지 마십시오. 적절한 접지는 전원 서지 및 정전기로 인한 장치 손상을 방지하는데 도움이 됩니다.

2. 장치의 시리얼 포트에 1개 또는 최대 2개의 시리얼 장치를 연결하십시오.

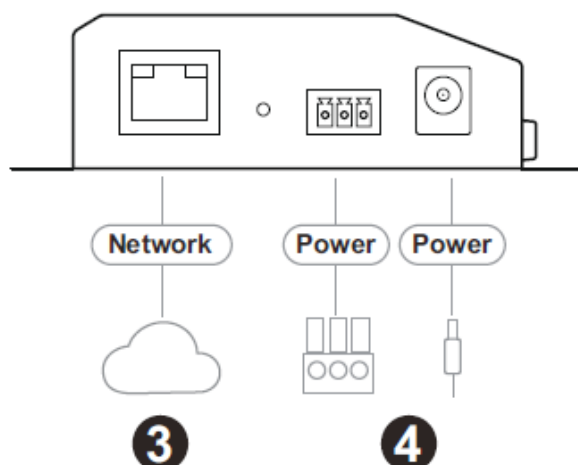
주의: SN3001 / SN3001P / SN3002 / SN3002P는 RS-232 연결을 지원하고 SN3401 / SN3401P / SN3402 / SN3402P는 RS-232 / RS-422 / RS-485 연결을 지원합니다.



3. Cat 5e/6 케이블을 사용하여 장치의 LAN 포트를 네트워크에 연결하십시오. SN3001P / SN3002P / SN3401P / SN3402P (PoE 802.3af 준수)의 경우, 사용자는 PoE 스위치를 통해 장치에 전원을 동시에 공급할 수 있으며 4번 단계를 건너뛸 수 있습니다.
4. 보조 전원을 위해 다음 중 하나 또는 두가지 모두를 수행하여 장치를 전원에 연결하고 전원을 켜십시오.
 - ◆ 제공된 전원 아답터 (SN3001P / SN3002P / SN3401P / SN3402P에는 포함되지 않음)를 AC 전원에 연결하고 케이블을 기기의 전원 잭에 연결합니다.

주의: 전원 아답터의 온도 허용 범위는 0 – 40°C입니다. 환경 온도가 40 – 60°C 인 경우 전원 터미널을 통해서만 장치에 전원을 공급할 수 있습니다.

- ◆ 제공된 터미널 블록을 사용하여 DC +/- 전선 (DC 9 – 48 V)를 장치의 전원 터미널에 연결합니다.



5. 전원을 공급한 후 보안 시리얼 장치 서버가 준비되고 상태 LED가 녹색으로 계속 켜질 때까지 약 50초 동안 기다리십시오.

주의: 1개 이상의 전원 공급 장치가 연결된 경우, 다른 전원 공급 장치가 중단되어도 대체 전원 연결이 계속 동작합니다. 예를 들어 장치가 전원 잭과 전원 터미널을 통해 전원에 연결되어 있는 경우, 전원 잭의 전원이 차단될 때 전원 터미널은 동작을 유지하고 그 반대의 경우도 마찬가지입니다.

시리얼 포트 핀 할당

보안 시리얼 장치 서버의 시리얼 포트의 핀 할당은 다음과 같습니다.

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

이 페이지는 빈 페이지 입니다.

3 장

네트워크 환경 구성 및 로그인

IP 주소 결정

시작하기 전에 사용중인 PC가 보안 시리얼 장치 서버와 동일한 LAN 내에 있는지 확인하십시오. 보안 시리얼 장치 서버의 IP 주소를 결정/설정하는 2가지 방법이 있습니다. 아래에 설명된 대로, 하나는 Windows PC의 IP 설치 유틸리티를 통해, 다른 하나는 PC만 사용하는 장치 서버 (non-DHCP 네트워크에만 적용 가능)

IP 설치 유틸리티

사용자는 Windows PC를 사용하여 IP 설치 유틸리티 (**IP Installer Utility**)로 보안 시리얼 장치 서버의 IP 주소를 검색하거나 IP를 사용하여 DHCP 또는 non-DHCP 네트워크에서 IP 주소를 할당할 수 있습니다.

1. 제품 웹 페이지의 지원 및 다운로드 탭에서 **IP Installer** zip 파일을 다운로드하십시오.
2. IPInstaller.exe 압축을 풀고 실행합니다. 아래와 비슷한 대화 상자가 나타납니다.

Network Device IP Installer

Device list:

Device Name	Model Name	MAC Address	IP Address
SN300X	SN3002P	00-10-74-24-04-21	10.3.41.138

Exit About Enumerate Set IP

Protocol: IPv4 Network adapter: MAC: 94-c6-91-9b-2f-4d, IP: 10.3.41.174

IPv4 settings

☒ Obtain an IP address automatically

☐ Use the following IP address:

IP address: 10 . 3 . 41 . 138

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 3 . 41 . 254

☒ Obtain DNS server address automatically

☐ Use the following DNS server addresses:

Preferred DNS server: 10 . 0 . 1 . 7

Alternate DNS server: 10 . 0 . 1 . 6

IPv6 settings

☐ Obtain an IPv6 address automatically (DHCP)

☐ Use the following IPv6 address:

IPv6 address:

Subnet prefix length:

Default gateway:

☒ Obtain DNS server address automatically

☐ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

3. 장치 목록에서 보안 시리얼 장치 서버를 선택하십시오.

주의: 1. 목록이 비어 있거나 장치가 나타나지 않으면 올바른 네트워크 아답터를 선택했는지 다시 확인하고 **Enumerate**를 클릭하여 장치 목록을 새로 고침 하십시오.

2. 목록에 2개 이상의 장치가 있는 경우 MAC 주소를 사용하여 장치를 구분합니다. 보안 시리얼 장치 서버의 MAC 주소는 하단 패널에 있습니다.

4. 보안 시리얼 장치 서버의 IP 주소를 확인하거나 IP 주소를 설정하려면 각각 **Obtain an IP address automatically** (자동으로 IP 주소 받기) 또는 **Use the following IP address** (다음 IP 주소 사용)을 선택하십시오.
 - ◆ IP 주소를 설정하려면 네트워크 환경에 따라 필요한 IP 주소, 서브넷 마스크, 게이트웨이 정보를 입력합니다.
5. **Set IP**를 클릭하십시오. 보안 시리얼 장치 서버의 IP 주소가 장치 목록에 표시됩니다.
6. **Exit**를 클릭하여 프로그램을 닫습니다.

IP 인스톨러 미사용 (non-DHCP 전용)

Windows가 아닌 시스템에서 DHCP가 아닌 네트워크에서 사용자는 아래 단계를 따라 기본 값인 192.168.0.60과는 다른 정적 IP 주소를 보안 시리얼 장치 서버에 할당할 수 있습니다.

1. PC의 IP 주소를 192.168.0.XXX로 설정하십시오. 여기서 XXX는 10을 제외한 모든 숫자입니다.
2. 브라우저의 URL 위치 바에 장치의 기본 IP 주소 (192.168.0.60)를 입력하십시오.
3. 유효한 사용자 이름과 암호로 로그인하십시오. (21페이지 참조)
4. 보안 시리얼 장치 서버의 웹 인터페이스에서 네트워크 환경에 따라 고정 IP 주소를 할당하십시오.
5. 설정을 저장하고 로그아웃 하십시오. 로그아웃 한 후에는 PC의 IP 주소를 원래 값으로 리셋했는지 확인하십시오.

로그인

웹 브라우저에서 보안 시리얼 장치 서버에 접속하려면 다음을 수행하십시오.

1. 브라우저를 열고 브라우저의 URL 위치 바에 접속하려는 보안 시리얼 장치 서버의 IP 주소를 입력하십시오.

주의: 관리자이고 처음 로그인하는 경우 보안 시리얼 장치 서버의 IP 주소를 결정하는 다양한 방법이 IP 주소 결정 (19페이지 참조)에 설명되어 있습니다.

2. 보안 경고 대화 상자가 나타나면 인증서를 수락하십시오. 이것은 신뢰할 수 있습니다. (세부 사항은 48페이지 보안 인증서 참조) 2 번째 인증서가 나타나면 이를 수락하십시오.
3. 표시되는 로그인 페이지에서 유효한 사용자 이름과 암호를 입력하여 로그인하십시오. 기본 **Username**과 **Password**는 각각 administrator와 password입니다.

The image shows a login interface. At the top, the word "Welcome" is displayed in a blue, sans-serif font. Below it, there are two input fields. The first field is labeled "Username" with a small blue person icon to its left. The second field is labeled "Password" with a small blue padlock icon to its left. Both fields have horizontal lines indicating where to enter text. Below these fields is a dark blue rectangular button with the text "SIGN IN" in white, uppercase letters.

4. 성공적으로 로그인하면 보안 시리얼 장치 서버의 메인 화면이 나타납니다. 처음 로그인 할 때 사용자는 보안 시리얼 장치 서버의 로그인 암호를 변경해야 합니다.
5. 처음 로그인 할 때 사용자는 보안 시리얼 장치 서버의 로그인 암호를 변경해야 합니다.
6. 로그인하면 보안 시리얼 장치 서버의 기본 설정을 안내하는 빠른 설정 마법사가 표시됩니다.

빠른 설정 마법사

Quick Setup Wizard는 보안 시리얼 장치 서버의 기본 설정을 시작합니다.

일반

Quick Setup Wizard

GENERAL

NETWORK

SERIAL

General settings

Device name

SN300X

☐ Display device name in login page

Time settings

Current time

2089-02-21 11:38:23

Time zone

(GMT) Casablanca, Monrovia

☐ Synchronize with computer time

☐ Set manually

☒ Synchronize with NTP Server (Recommended)

Sync Now

2089-02-21 11:37:44

Using default NTP servers

Primary NTP server

pool.ntp.org

Alternate NTP server

north-america.pool.ntp.org

☐ Don't show this again

PREVIOUS

NEXT

CANCEL

항목	설명
Device name	보안 시리얼 장치 서버의 이름을 표시합니다. 필요한 경우 장치 이름을 변경합니다.
Current time	장치의 현재 시간을 표시합니다.
Time settings	장치의 시간 설정을 설정합니다. 세부 사항은 41페이지 시간을 참조하십시오.

네트워크

Quick Setup Wizard

X

GENERAL NETWORK SERIAL

IPV4

Configuration

DHCP

IP address

10.3.41.161

Subnet mask

255.255.255.0

Default gateway

10.3.41.254

DNS

Set manually

Preferred DNS server

10.0.1.7

Alternate DNS server

10.0.1.6

☐ Don't show this again

PREVIOUS

NEXT

CANCEL

네트워크 탭은 보안 시리얼 장치 서버의 네트워크 설정을 지정합니다. 세부 사항은 37페이지 네트워크를 참조하십시오.

시리얼

주의: **Serial** 탭의 설정은 보안 시리얼 장치 서버의 모든 시리얼 포트에 적용됩니다.

The image shows a 'Quick Setup Wizard' window with the 'SERIAL' tab selected. The window has three tabs: GENERAL, NETWORK, and SERIAL. Under 'Operating mode', there is a 'Mode' dropdown menu set to 'TCP Server' and an unchecked checkbox for 'Secure transfer'. Under 'Serial properties', there are five dropdown menus: 'Baud rate' (9600), 'Parity' (None), 'Data bits' (8 bits), and 'Stop bits' (1 bit). At the bottom, there is a checkbox for 'Don't show this again' and three buttons: 'PREVIOUS', 'SAVE', and 'CANCEL'.

항목	설명
Mode	보안 시리얼 장치 서버의 시리얼 포트에 대한 작동 모드를 선택합니다. 포트 작동 모드를 참조하십시오.
Secure transfer	보안 데이터 전송하려면 체크합니다.
Baud rate	시리얼 포트의 데이터 전송 속도를 선택합니다.
Parity	연결된 시리얼 장치의 패리티 설정과 일치하는 전송된 데이터의 무결성을 체크하여 선택합니다.
Data bits	데이터 비트 데이터의 한 문자를 전송하고 연결된 시리얼 장치의 데이터 비트 설정과 일치하는데 사용되는 비트 수를 선택합니다.
Stop bits	정지 비트 문자가 전송되었음을 나타내며 연결된 시리얼 장치의 정지 비트 설정과 일치하는 정지 비트를 선택합니다.

설정을 적용하려면 **Save**를 클릭하십시오. 보안 시리얼 장치 서버의 웹 콘솔 메인 화면이 표시됩니다. 자세한 내용은 웹 콘솔을 참조하십시오.

4 장

웹 콘솔

웹 인터페이스



보안 시리얼 장치 서버 및 해당 구성 요소의 웹 인터페이스를 아래에 표시하고 설명합니다.





번호	항목	설명
A	사이드바 메뉴	메뉴 구성 페이지 선택을 제공합니다. 클릭하면 환경 구성 페이지를 선택하거나 하위 메뉴를 확장합니다.
B	작업 표시줄	빠른 설정 마법사, 사용자 설정 (로그아웃 포함), 장치 정보에 대한 접속을 포함합니다.
C	대화형 디스플레이 패널	현재 선택된 환경 구성 페이지를 표시합니다.
1	빠른 설치 마법사	사용자에게 보안 시리얼 장치 서버의 기본 설정을 안내합니다. 22페이지를 참조하십시오.
2	개인 설정	클릭하면 현재 로그인한 사용자, 로그인 시간, 사용자 기본 설정 옵션, 암호 변경 및 로그 아웃 옵션을 표시합니다. Preferences를 클릭하면 인터페이스의 언어를 변경합니다. Change password를 클릭하면 현재 사용자 계정의 암호를 변경합니다.
3	정보	클릭하면 장치의 모델 번호와 펌웨어 버전이 표시됩니다.

시리얼 포트

Serial Ports 페이지는 설정 및 연결된 시리얼 장치를 포함하여 보안 시리얼 장치 서버의 시리얼 COM 포트에 대한 개요를 제공합니다.

	Port Name	Operating Mode	Ethernet Port	Baud Rate	Online	In Use	Action
	[01] Port 1	TCP Server	5301	9600	Online	No	<button>EDIT</button> <button>DUMP BUFFER</button>
	[02] Port 2	RealCOM	5200	9600	Online	No	<button>EDIT</button> <button>DUMP BUFFER</button>

항목	설명
 	RS-232 시리얼 포트가 온라인인지 오프라인인지를 나타냅니다. 주의: 이 기능은 RS-232 연결에만 적용됩니다. RS-422 또는 RS485 연결의 경우 이 필드에 회색 아이콘이 표시됩니다.
Port Name	시리얼 포트의 이름을 표시합니다.
Operating Mode	시리얼 포트의 현재 동작 모드를 표시합니다. 30페이지 동작 모드를 참조하십시오.
Ethernet Port	시리얼 포트의 네트워크 포트 값을 표시합니다.
Baud Rate	시리얼 포트의 Baud Rate를 표시합니다.
Online	RS-232 시리얼 포트가 온라인인지 오프라인인지를 나타냅니다. 주의: 이 기능은 RS-232 연결에만 적용됩니다. RS-422 또는 RS485 연결의 경우 이 필드에 회색 아이콘이 표시됩니다.
In Use	시리얼 포트에 활성화된 데이터 전송이 있는지 여부를 나타냅니다.
Action	<ul style="list-style-type: none"> ◆ Edit: 클릭하면 시리얼 포트의 설정을 편집합니다. ◆ Dump Buffer: 클릭하면 장치에서 시리얼 포트의 포트 활동 로그를 .txt 파일로 다운로드합니다. 이 기능은 포트 활동 로그가 장치의 메모리에 저장된 경우에만 사용할 수 있습니다. 28페이지 포트 버퍼링을 참조하십시오. ◆ Telnet / SSH: 클릭하면 보안 시리얼 장치 서버를 구성하거나 Telnet/SSH 프로토콜을 통해 연결된 시리얼 장치에 접속하고 제어합니다. 이 기능은 포트의 동작 모드가 Console Management (콘솔 관리)로 설정된 경우에만 사용할 수 있습니다. 30페이지 동작 모드 및 70페이지 Telnet/SSH를 참조하십시오. <p>주의: 하나의 시리얼 포트에 대한 최대 동시 연결 수는 16개입니다.</p>

시리얼 포트 편집

시리얼 COM 포트의 설정을 편집하려면 **EDIT** 버튼을 클릭합니다. Properties (속성), Operating Mode (동작 모드), Port Buffering (포트 버퍼링) 탭이 있는 편집 윈도우가 나타납니다.

속성

Edit

PROPERTIES

OPERATING MODE

PORT BUFFERING

Port number

1

Port name

Port 1

Baud rate

9600

Parity

None

Data bits

8 bits

Stop bits

1 bit

Flow control

None

Interface

RS-485 2-wire

Terminator

off (default)

Pull high/low resistor

150 kOhms(default)

SAVE & APPLY ALL

SAVE

CANCEL

항목	설명
Port number	시리얼 포트의 번호를 표시합니다.
Port Name	시리얼 포트의 이름을 설정합니다.
Baud Rate	시리얼 포트의 데이터 전송 속도를 선택합니다. 기본 값 = "9600"
Parity	선택하면 연결된 시리얼 장치의 패리티 설정과 일치하는 전송된 데이터의 무결성을 체크합니다. 기본값 = "None"
Data bits	데이터의 한 문자를 전송하고 연결된 시리얼 장치의 데이터 비트 설정과 일치하는 데 사용되는 비트 수를 선택합니다. 기본값 = "8"
Stop bits	문자가 전송되었음을 나타내며 연결된 시리얼 장치의 정지 비트 설정과 일치하는 정지 비트를 선택합니다. 기본값 = "1"
Flow control	데이터 흐름이 제어되는 방식을 선택하고 연결된 시리얼 장치의 흐름 제어 설정과 일치합니다. 기본값 = "None"
Interface	COM 포트의 시리얼 인터페이스 유형을 설정합니다.

항목	설명
Terminator	RS-485 신호 반사 및 데이터 손상을 방지하려면 이 설정을 활성화합니다.
Pull high/low resistor	RS-485 연결을 위해 Pull high/low resistor 저항을 올바르게 구성하십시오.

변경 사항을 적용하려면 **Save**를 클릭하십시오.

보안 시리얼 장치 서버의 모든 시리얼 포트에 같은 설정을 적용하려면 **Save & Apply All**을 클릭하십시오.

포트 버퍼링

포트 버퍼링은 포트에 접속할 때 수행된 활동의 로그를 생성합니다. 로그를 보안 시리얼 장치 서버의 내부 메모리 (최대 128KB) 또는 Syslog 서버에 저장할 수 있습니다.

포트 버퍼링을 활성화하려면 포트 버퍼링 탭의 드롭 다운 목록에서 **Memory** 또는 **Syslog Server**를 선택합니다. Time Stamps에 체크하면 생성된 로그에 타임 스탬프를 추가합니다.

Edit

PROPERTIES

OPERATING MODE

PORT BUFFERING

Port buffering

Syslog

☐ Time stamps

SAVE & APPLY ALL

SAVE

CANCEL

변경 사항을 적용하려면 **Save**를 클릭하십시오.

주의: Syslog를 선택하기 전에 Syslog 서버를 활성화했는지 확인하십시오. 44페이지 Syslog를 참조하십시오.

보안 시리얼 장치 서버의 모든 시리얼 포트에 같은 설정을 적용하려면 **Save & Apply All**을 클릭하십시오.

동작 모드

동작 모드 탭은 보안 시리얼 장치 서버의 시리얼 COM 포트에 접속하는 방법을 결정합니다.

주의: 하나의 시리얼 포트에 대한 최대 동시 연결 수는 16개입니다.

다양한 포트 동작 모드에 대한 자세한 내용은 6장 포트 동작 모드를 참조하십시오.

■ Real COM

Mode RealCOM ▼

☐ Secure transfer

Secure transfer을 체크하면 시리얼 COM 포트를 통해 SSL을 사용하여 전송되는 모든 데이터를 암호화합니다.

주의: Real COM 동작 모드는 반드시 ATEN의 버추얼 COM 포트 유틸리티와 함께 사용해야 합니다. 79페이지 버추얼 시리얼 포트 관리자를 참조하십시오.

■ TCP 서버

Mode TCP Server ▼

☐ Secure transfer

항목	설명
Secure transfer	체크하면 SSL을 사용하여 TCP 클라이언트-서버 모드를 통해 보안 시리얼 장치 서버의 시리얼 COM 포트 사이에 전송되는 모든 데이터를 암호화합니다.

■ TCP 클라이언트

Mode TCP Client ▼

☐ Secure transfer

Destination host 1	IP / Domain	Port 0
Destination host 2	IP / Domain	Port 0
Destination host 3	IP / Domain	Port 0
Destination host 4	IP / Domain	Port 0
Destination host 5	IP / Domain	Port 0
Destination host 6	IP / Domain	Port 0
Destination host 7	IP / Domain	Port 0
Destination host 8	IP / Domain	Port 0
Destination host 9	IP / Domain	Port 0
Destination host 10	IP / Domain	Port 0
Destination host 11	IP / Domain	Port 0
Destination host 12	IP / Domain	Port 0
Destination host 13	IP / Domain	Port 0

항목	설명
Secure transfer	체크하면 SSL을 사용하여 TCP 클라이언트-서버 모드를 통해 보안 시리얼 장치 서버의 시리얼 COM 포트 사이에 전송되는 모든 데이터를 암호화합니다.
Destination host	데이터 전송을 위한 대상 호스트의 IP 주소와 서비스 포트를 입력합니다. 장치는 최대 16개의 대상 호스트에 동시에 데이터를 보낼 수 있습니다.

■ UDP

Mode	UDP ▼	
	Start IP	End IP
Destination host 1	Port 0	
	Start IP	End IP
Destination host 2	Port 0	
	Start IP	End IP
Destination host 3	Port 0	
	Start IP	End IP
Destination host 4	Port 0	
	Start IP	End IP
Destination host 5	Port 0	

항목	설명
Destination host	UDP 프로토콜을 통해 대상 호스트에 연결하기 위한 IP 주소 범위 및 포트 값을 입력합니다. 보안 시리얼 장치 서버는 최대 16개의 대상 호스트에 동시에 연결할 수 있습니다.

■ 시리얼 터널링 서버

Mode Serial Tunneling Server ▼

TCP port 5301

☐ Secure transfer

항목	설명
TCP port	시리얼 터널링 서버로 동작하는 시리얼 포트의 TCP/IP 포트 값을 설정합니다.
Secure transfer	체크하면 SSL을 사용하여 시리얼 터널링 서버-클라이언트를 통해 2대의 보안 시리얼 장치 서버 사이에서 시리얼 COM 포트를 통해 전송되는 모든 데이터를 암호화합니다.

■ 시리얼 터널링 클라이언트

Mode Serial Tunneling Client ▼

Destination IP Port

☐ Secure transfer

항목	설명
Destination	데이터를 보낼 시리얼 터널링 서버의 IP 주소와 포트 값을 입력합니다.
Secure transfer	체크하면 SSL을 사용하여 시리얼 터널링 클라이언트-서버를 통해 2대의 보안 시리얼 장치 서버 사이에서 시리얼 COM 포트를 통해 전송되는 모든 데이터를 암호화합니다.

■ 콘솔 관리

Mode Console Management ▼

General settings

Connection protocol ☒ SSH ☐ Telnet

☐ Direct connection

Logout timeout (0~180min) 1

Suspend character D

Exit Macro

Map <CR-LF> CRLF ▼

항목	설명
Connection protocol	체크/해제하여 SSH 및 Telnet 연결 프로토콜을 활성화/비활성화합니다.
Direct connection	콘솔 관리 다이렉트 동작 모드를 선택합니다. 사용 가능한 다양한 동작 모드에 대한 자세한 내용은 6장 포트 동작 모드를 참조하십시오.
Logout timeout (0 ~ 180 min)	설정된 시간 동안 사용자가 입력하지 않으면 접속 중인 사용자를 자동으로 로그아웃 합니다. "0"은 사용자가 자동으로 로그아웃 되지 않음을 의미합니다.
Suspend character	일시 중지 문자는 Telnet 세션에서 일시 중지 메뉴를 불러오는데 사용됩니다. 유효한 문자는 A - Z (H, I, J, M 제외)입니다.
Exit Macro	시리얼 장치를 종료할 때 실행될 매크로 종료를 설정합니다.
Map <CR-LF>	선택하면 Carriage Return (CR) 또는 Line Feed (LF) 신호를 전송합니다.

■ Modbus RTU/ASCII 마스터

보안 시리얼 장치 서버를 RTU/ASCII 마스터 장치로 설정하려면 이 옵션을 선택합니다.

RTU/ASCII 마스터 장치는 동시에 최대 16개의 슬레이브 장치와 통신을 시작할 수 있습니다.

선택적으로 TCP 슬레이브 장치에 대해 최대 16개의 설정 세트를 입력합니다.

주의:

- ◆ 이 모드는 SN3401 / SN3401P / SN3402 / SN3402P에만 적용됩니다.
- ◆ SN3402 / SN3402P의 경우 선택한 동작 모드가 장치의 양쪽 시리얼 포트에 모두 적용됩니다.

PROPERTIES **OPERATING MODE** PORT BUFFERING

Mode

Modbus RTU Master

Modbus TCP Slave 1

IP/Domain
 TCP port 502
 ID Start 0
 ID End 0

Modbus TCP Slave 2

IP/Domain
 TCP port 502
 ID Start 0
 ID End 0

Modbus TCP Slave 3

IP/Domain
 TCP port 502
 ID Start 0
 ID End 0

Modbus TCP Slave 4

IP/Domain
 TCP port 502
 ID Start 0
 ID End 0

Modbus TCP Slave 5

IP/Domain
 TCP port 502
 ID Start 0
 ID End 0

Modbus TCP Slave 6

IP/Domain
 TCP port 502
 ID Start 0
 ID End 0

항목	설명
IP/Domain	슬레이브 장치의 IP 주소를 입력합니다.
TCP port	슬레이브 장치의 TCP 포트를 입력합니다.
ID Start	슬레이브 장치의 시작 및 끝 ID를 입력합니다. 유효한 범위는 1~247입니다.
ID End	

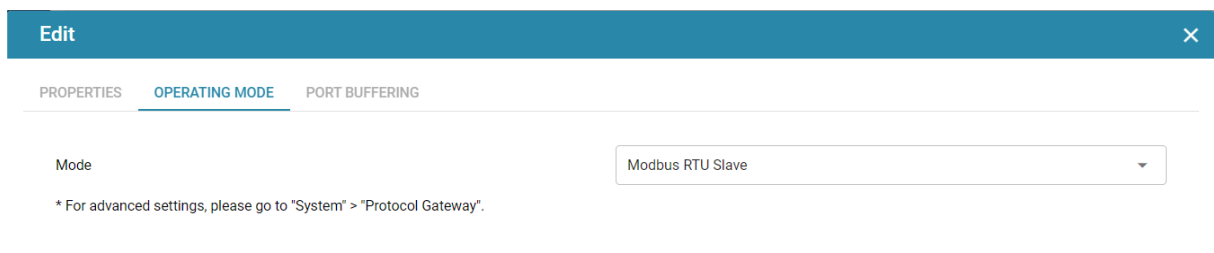
■ Modbus RTU/ASCII 슬레이브

보안 시리얼 장치 서버를 RTU/ASCII 슬레이브 장치로 설정하려면 이 옵션을 선택합니다.

RTU/ASCII 슬레이브 장치는 동시에 최대 16개의 마스터 장치와 통신을 시작할 수 있습니다.

주의:

- ◆ 이 모드는 SN3401 / SN3401P / SN3402 / SN3402P에만 적용됩니다.
- ◆ SN3402 / SN3402P의 경우 선택한 동작 모드가 장치의 양쪽 시리얼 포트에 모두 적용됩니다.



The screenshot shows a software interface for configuring a device. At the top is a blue header bar with the word 'Edit' and a close button (X). Below the header are three tabs: 'PROPERTIES', 'OPERATING MODE' (which is selected and highlighted in blue), and 'PORT BUFFERING'. In the 'OPERATING MODE' tab, there is a label 'Mode' followed by a dropdown menu that currently displays 'Modbus RTU Slave'. At the bottom of the window, there is a small note: '* For advanced settings, please go to "System" > "Protocol Gateway".'

■ 비활성화

선택하면 시리얼 포트 사용을 비활성화합니다.

네트워크

Network 페이지는 아래 테이블에서 설명하는 것처럼 보안 시리얼 장치 서버의 네트워크 설정이 포함되어 있습니다.

LAN1

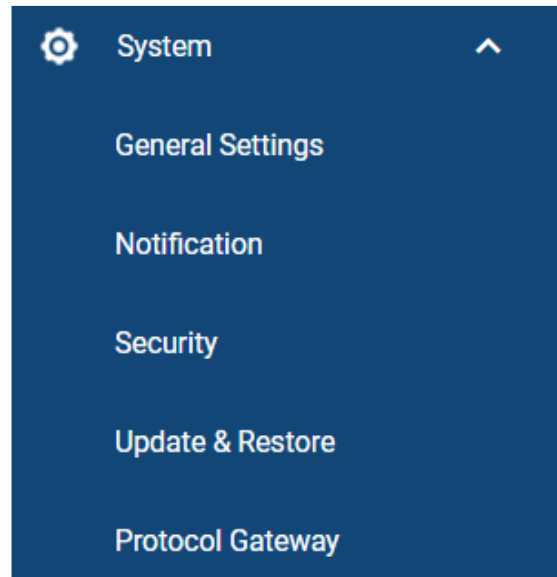
IPv4

Configuration	DHCP ▼
IP address	10.3.41.138
Subnet mask	255.255.255.0
Default gateway	10.3.41.254
DNS	Obtain automatically ▼
Preferred DNS server	10.0.1.7
Alternate DNS server	10.0.1.6

항목	설명
Configuration	DHCP 또는 고정 IP에서 보안 시리얼 장치 서버의 IP 주소 설정을 위한 환경 구성 유형을 선택합니다.
IP address Subnet mask Default gateway	고정 IP의 경우 네트워크 환경에 따라 장치의 IP 주소, 서브넷 마스크, 게이트웨이를 설정합니다.
DNS	Obtain automatically (자동 설정) 또는 Set manually (수동 설정)에서 DNS 서버를 얻는 방법을 선택합니다.
Preferred DNS server Alternate DNS server	DNS 서버를 수동으로 설정하는 경우, 장치에 대한 기본 및 대체 DNS 서버 주소를 입력합니다.

시스템

클릭하면 **General settings (일반 설정)**, **Notification (알림)**, **Security (보안)**, **Update & Restore (업데이트 및 복원)**을 포함하여 보안 시리얼 장치 서버의 모든 시스템 관련 설정에 대한 시스템 하위 메뉴를 확장합니다.



일반 설정

일반 설정은 General (일반) 및 Time (시간) 2개의 탭으로 구성됩니다.

일반

GENERAL
TIME

Device name
☐ Display device name in login page

Description

MFG
-

MAC
001074240421

Uptime
00:23:47:49 (DD:HH:MM:SS)

Power source
DC

Login session timeout(0-180 min)

Reboot System

Service ports

HTTP

HTTPS

SSH

Telnet

Base socket

IP Installer

Configuration

✓ SAVE

항목	설명
Device name	보안 시리얼 장치 서버의 장치 이름을 설정합니다.
Description	필요한 경우 장치에 대한 설명을 입력합니다.
MFG	장치의 MFG (제조 번호)를 표시합니다. 주의: 제조 번호는 ATEN의 공장 및 기술 지원 직원이 제품을 식별하는데 사용하는 내부 일련 번호입니다.
MAC	보안 시리얼 장치 서버의 MAC 주소를 표시합니다.
Uptime	장치가 실행된 시간을 표시합니다.
Power source	장치의 현재 전원 소스를 표시합니다.

항목	설명
Login session timeout (0 ~ 180 min)	설정된 시간 동안 보안 시리얼 장치 서버의 웹 인터페이스에서 수행한 작업이 없으면 사용자를 자동으로 로그아웃 합니다. "0"은 사용자가 자동으로 로그아웃 되지 않음을 의미합니다.
Reboot System	보안 시리얼 장치 서버를 재부팅합니다.
Service ports	<p>다음과 같이 서비스 포트 값을 설정합니다.</p> <ul style="list-style-type: none"> ◆ HTTP: 브라우저 접속에 사용 (기본값 = 80) ◆ HTTPS: 보안 브라우저 접속에 사용 (기본값 = 443) ◆ SSH: SSH 접속에 사용 (기본값 = 22) ◆ Telnet: Telnet 접속에 사용 (기본값 = 23) ◆ Base socket: TCP 연결을 수신하고 수락하는데 사용 (기본값 = 5001) 예를 들어, 기본 소켓 값이 5001인 경우 Telnet 및 SSH를 통한 포트 1/2에 대한 장치의 TCP 포트 값은 각각 5001/5002 및 5101/5102입니다. <p>주의:</p> <ol style="list-style-type: none"> 1. 모든 서비스 포트에 대한 유효한 항목은 1 – 65535입니다. 2. 모든 서비스 포트 설정이 변경될 때 시스템을 다시 시작해야 합니다.
IP Installer Configuration	<p>선택하면 IP 설치 유틸리티가 보안 시리얼 장치 서버의 IP 주소를 감지 또는 변경할 수 있는지 결정합니다.</p> <ul style="list-style-type: none"> ◆ Enabled: IP 인스톨러는 장치의 IP 주소를 감지하고 변경할 수 있습니다. ◆ View Only: IP 인스톨러는 장치의 IP 주소를 감지만 하고 변경할 수는 없습니다. ◆ Disabled: IP 인스톨러는 장치의 IP 주소를 감지하고 변경할 수 없습니다.

변경 사항을 적용하려면 **Save**를 클릭하십시오.

시간

Time 탭에는 아래 테이블에서 설명한 것처럼 보안 시리얼 장치 서버의 시간 설정이 포함되어 있습니다.

GENERAL

TIME

Current time

2089-04-03 08:44:55

Time zone

(GMT) Casablanca, Monrovia

☐ Synchronize with computer time

Sync Now

☐ Set manually

2089-04-03 08:44:33

☒ Synchronize with NTP Server
(Recommended)

Using default NTP servers

Primary NTP server

pool.ntp.org

Alternate NTP server

north-america.pool.ntp.org

Update Now

항목	설명
Time zone	<p>다음 중 하나를 선택하여 보안 장치의 시간을 설정합니다.</p> <ul style="list-style-type: none"> ◆ Synchronize with computer time: 클라이언트 PC의 시간과 동기화합니다. ◆ Set manually: 장치에 원하는 시간을 수동으로 설정합니다. ◆ Synchronize with NTP Server: NTP 서버와 사용하는 장치의 시간을 동기화합니다. <p>주의:</p> <ul style="list-style-type: none"> ◆ Synchronize with computer time 또는 Set manually를 사용하는 경우, 시간 설정은 보안 시리얼 장치 서버가 재시작될 때마다 반드시 재설정되어야 합니다. ◆ 특히 보안 시리얼 장치 서버가 잠시 동안 동작하는 경우 시간 불일치를 피하기 위해 Synchronize with NTP Server을 사용하는 것이 좋습니다.

알림

Notification 페이지는 SMTP, SNMP, Syslog, Advanced 4개의 탭으로 구성됩니다.

SMTP

SMTP
SNMP
SYSLOG
ADVANCED

To receive event notifications through email, please set up the following SMTP service and go to the 'Advanced' tab to configure notification events.

☒ Enable SMTP service

Server Address

Port

Email

☐ My server requires authentication

Recipient

항목	설명
Enable SMTP service	선택하면 Advanced 탭에서 지정한대로 이메일을 통해 이벤트 알림을 보내기 위해 SMTP 서비스를 활성화합니다. (45페이지 참조)
Server Address / Port	SMTP 서버의 주소와 서비스 포트 값을 입력합니다.
Email	발신자의 이메일 주소를 입력합니다.
My server requires authentication	체크하면 SMTP 서버에 인증이 필요한지 확인하고 유효한 사용자 이름과 암호를 입력합니다.
Recipient	수신자 수신자의 이메일 주소를 입력합니다.

SNMP

주의: SNMP를 사용하기 전에 System > Security > Security Level에서 **Enable SNMP Agent service**를 확인하십시오.

SMTP
SNMP
SYSLOG
ADVANCED

SNMP Traps

You can set the system to push SNMP traps, which are event notifications, to an existing SNMP manager on the network.

☒ Send SNMP traps

IP/Server Address

Port

Community

SNMP Agent

You can manage the access control of SNMP agent for SNMP manager to query.

Port

Community

항목	설명
Send SNMP traps	체크하면 Advanced 탭에서 지정한대로 SNMP 트랩 이벤트 알림을 전송하기 위해 SNMP 서비스를 활성화합니다. (45페이지 참조) SNMP v1 및 v2c가 지원됩니다.
IP/Server Address	SNMP 트랩 이벤트를 수신할 IP/서버 주소를 입력합니다.
Port	포트 SNMP 트랩 이벤트를 수신할 서버의 서비스 포트를 입력합니다.
Community	SNMP 커뮤니티를 입력합니다.
SNMP Agent	SNMP 에이전트의 서비스 포트 및 커뮤니티를 입력합니다.

Syslog

SMTP SNMP **SYSLOG** ADVANCED

To send event logs to a Syslog server, please set up the following Syslog service and then go to the "Advanced" tab to configure notification events.

☒ Enable Syslog service

Server Address

10.3.167.235

Port

514

항목	설명
Enable Syslog service	체크하면 Advanced 탭에서 지정한대로 이벤트 알림을 Syslog 서버로 보내기 위해 Syslog 서비스를 활성화합니다. (45페이지 참조)
Server Address / Port	Syslog 서버의 주소와 포트 값을 입력합니다.

고급

Advanced 탭은 SMTP, SNMP 또는 Syslog 서버를 통해 보낼 이벤트 알림 유형을 설정합니다. 옵션에는 아래 제공된 예가 포함되지만 이에 국한되지는 않습니다.

SMTP
SNMP
SYSLOG
ADVANCED

You can customize the following notification events.

Event	SMTP	SNMP	Syslog
Serial ports events			
Port online	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port offline	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Serial connection started	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Serial connection stopped	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Network events			
LAN port was down	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IP changed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IP address retrieved from a DHCP server	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
General settings events			
System rebooted	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Notification events			
SMTP settings enabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SMTP settings disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SNMP Trap settings enabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SNMP Trap settings disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SNMP Agent settings enabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SNMP Agent settings disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Syslog settings enabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Syslog settings disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security events			
IP filter settings enabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IP filter settings disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

SAVE

해당 이벤트가 발생할 때 SMTP / SNMP / Syslog 알림을 전송하려면 각 이벤트 유형 옆에 있는 SMTP / SNMP / Syslog에 체크합니다.

주의: 지정된 알림을 보내려면, 필요한 SMTP / SNMP / Syslog 서비스가 올바르게 구성되었는지 확인하십시오.

보안

Security 페이지는 보안 시리얼 장치 서버의 보안 설정 및 인증서 정보가 포함되어 있으며 Access Protection, Security Level, Account Policy, Certificate 4개의 탭으로 구성됩니다.

접속 보호 (IP 필터)

접속 보호 기능은 추가된 IP 주소에서만 원격 접속을 허용하고 다른 모든 원격 접속을 거부하도록 IP 필터를 설정합니다.

ACCESS PROTECTION

SECURITY LEVEL

ACCOUNT POLICY

CERTIFICATE

Security Filters

☒ Enable IP filter

Include the following IP address

+ ADD

DELETE

✓ SAVE

특정 IP 주소에 대해서만 독점 접속을 활성화하려면 **Enable IP filter**에 체크하고, 원하는 IP 주소를 추가하려면 **ADD** 버튼을 클릭하십시오.

변경 사항을 적용하려면 **Save**를 클릭하십시오.

보안 레벨

ACCESS PROTECTION SECURITY LEVEL ACCOUNT POLICY CERTIFICATE

- ☐ Enable Telnet service
- ☒ Enable SNMP Agent service
- ☒ Enable ICMP service
- ☒ Enable SSH service
- ☒ Enable HTTP and redirect to HTTPS

항목	설명
Enable Telnet / SNMP Agent / ICMP / SSH service	체크/해제하여 Telnet / SNMP 에이전트 / ICMP / SSH 서비스를 활성화/비활성화합니다. 주의: SNMP 에이전트 설정이 변경된 경우 시스템을 다시 시작해야합니다.
Enable HTTP and redirect to HTTPS	체크하면 보안 웹 브라우저 접속을 위해 HTTP를 활성화하고 모든 HTTP 접속을 HTTPS로 자동 리디렉션합니다. 주의: 이 설정이 변경되면 시스템을 다시 시작해야합니다.

계정 정책

ACCESS PROTECTION SECURITY LEVEL ACCOUNT POLICY CERTIFICATE

Password Policy

Minimum length for username

Minimum length for password

Password must contain at least

☐ One uppercase

☐ One lowercase

☐ One number

☐ One special character ⓘ

항목	설명
Minimum length for username / password	새로 설정된 모든 로그인 사용자 이름/암호에 필요한 최소 문자 수를 설정합니다. 기본 값 = "6"
Password must contain at least	체크하면 새로 설정된 모든 암호에 최소 하나 이상의 대문자/소문자/숫자/특수 문자를 요구합니다.

보안 인증서

Security Certificate 탭에는 사용된 보안 인증서의 정보가 표시됩니다.

ACCESS PROTECTION
SECURITY LEVEL
ACCOUNT POLICY
CERTIFICATE

You can import a private certificate or signed certificates from a third-part certificate authority for secure SSL service such as a web connection (https) certificate.

Issued To	
Common Name(CN)	ATEN INTERNATIONAL CO.,LTD
Organization(O)	ATEN INTERNATIONAL CO.,LTD
Organization Unit (OU)	R&D
Country(C)	TW
State or Province (ST)	New Taipei City
Locality (L)	Sijhih District
Email Address (E)	eservice@aten.com.tw
Serial Number	00C915DC9CC9CACA65
Issued By	
Common Name(CN)	ATEN INTERNATIONAL CO.,LTD
Organization(O)	ATEN INTERNATIONAL CO.,LTD
Organization Unit (OU)	R&D
Validity	
Issued On	Mon, 18 Jan 2021 08:04:07 GMT
Expires On	Sun, 19 Jan 2031 08:04:07 GMT
Fingerprints	
SHA1 Fingerprint	A0:0B:DE:A8:18:A0:81:9B:E2:E3:80:F1:80:70:F2:3E:0E:2A:C8:FD
MD5 Fingerprint	9F:F8:29:9E:B5:DF:02:60:EF:89:68:6C:52:D6:A8:B1

Import Certificate
Restore Defaults

보안 강화를 위해 사용자는 기본 ATEN 인증서 대신 자신의 개인 암호화 키와 서명된 인증서를 사용할 수 있습니다.

개인 인증서를 설정하는 방법에는 두 가지가 있습니다.

◆ 자체 서명 인증서 생성

자체 서명 인증서를 만들려면 무료 유틸리티인 openssl.exe를 웹에서 다운로드 할 수 있습니다.

◆ CA 서명 SSL 서버 인증서 얻기

보안을 위해 CA (인증 기관) 웹 사이트에서 얻은 타사 CA 서명 SSL 인증서를 사용하는 것이 좋습니다. 획득한 인증서와 개인 암호화 키를 PC에 저장하십시오.

항목	설명
Import Certificate	PC에서 개인 또는 CA 서명 보안 인증서를 가져옵니다.
Restore Defaults	기본 ATEN 인증서 사용으로 복구합니다.

업데이트 및 복원

Update & Restore 페이지는 보안 시리얼 장치 서버의 펌웨어를 업그레이드하고 장치 설정을 백업 또는 복원할 수 있습니다.

펌웨어 업데이트

FIRMWARE UPDATE

CONFIG. BACKUP & RESTORE

Firmware version: V1.0.072

☒ Upgrade with newer firmware version only

No file chosen

항목	설명
Firmware version	현재 펌웨어 버전을 표시합니다.
Upgrade with newer firmware version only	최신 펌웨어 버전으로만 펌웨어 업그레이드를 허용하려면 선택하십시오.
Choose File	업그레이드에 사용할 펌웨어 업데이트 파일을 선택합니다.
UPGRADE	선택한 펌웨어 파일로 장치 펌웨어를 업그레이드합니다.

백업 및 복원

Backup & Restore 페이지에서는 사용자가 보안 시리얼 장치 서버의 시스템 설정을 백업하거나 복원할 수 있습니다.

The screenshot shows a web interface for system configuration. At the top, there are two tabs: 'FIRMWARE UPDATE' and 'CONFIG. BACKUP & RESTORE'. The 'CONFIG. BACKUP & RESTORE' tab is selected. Below the tabs, there are two main sections: 'Backup' and 'Restore'. In the 'Backup' section, there is a 'Password' label and an empty input field, and a blue button labeled 'BACKUP'. In the 'Restore' section, there is a 'Password' label and an empty input field, a 'Choose File' button, and the text 'No file chosen', and a blue button labeled 'RESTORE'.

◆ 시스템 설정 백업

보안 시리얼 장치 서버의 시스템 설정을 백업하려면 복원에 사용할 암호를 입력하고 **Backup**을 클릭하여 시스템 설정 백업 파일인 System.conf를 PC에 저장합니다. 여기에는 암호 및 사용자 권한과 같은 계정 관련 설정도 포함됩니다.

◆ 시스템 설정 복원

이전에 백업한 시스템 설정 파일을 복원하려면 해당 암호를 입력하고 Choose File를 클릭하여 PC에서 파일을 찾은 다음 **Restore**를 클릭합니다.

프로토콜 게이트웨이

이 페이지를 사용하여 Modbus 통신 설정을 구성합니다.

MODBUS

General

Initial delay (0~30000ms)

Modbus TCP exception

Response timeout (10~65535ms)

Inter-character timeout (0~500ms)

Routing Policy

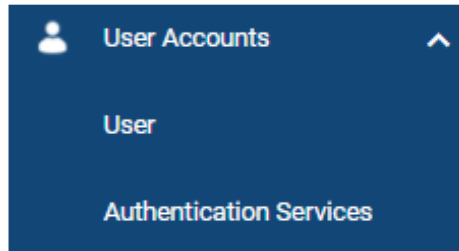
Received requests will be routed to the connected modbus RTU/ASCII Slave devices according to the following routing table.

☒ Auto routing for slave devices

항목	설명
Initial delay	Modbus 마스터가 슬레이브 장치에 첫 번째 요청을 보내기 전에 기다려야 하는 기간을 설정합니다. 이것은 특히 일부 슬레이브 장치가 환경의 다른 장치보다 부팅하는 데 더 많은 시간이 걸리는 경우 초기 부팅 중에 반복되는 예외를 줄이는데 사용됩니다.
Modbus TCP exception	슬레이브가 요청을 인식할 수 없거나 요청을 보내는 동안 오류가 발생한 경우 보안 시리얼 장치 서버가 Modbus 슬레이브에서 예외 응답을 반환할 수 있도록 이 설정을 활성화합니다.
Response timeout	상위 장치가 요청을 포기하고 다음 요청을 보내기 시작하기 전에 Modbus 슬레이브 장치로부터 응답을 수신하는 시간 제한을 설정합니다.
Inter-character timeout	요청의 각 문자 사이의 시간 제한을 설정합니다. 요청의 모든 문자가 수신되기 전에 시간이 초과되면 요청이 삭제됩니다.
Auto-routing	보안 시리얼 장치 서버가 수신된 모든 요청을 연결된 RTU/ASCII 슬레이브 장치로 자동 라우팅하려면 이 설정을 선택합니다. 비활성화된 경우 수신된 요청은 지정된 슬레이브 장치(ID)로만 전달됩니다.

사용자 계정

사용자 계정 하위 메뉴는 **User** 및 **Authentication Services** 페이지로 구성되며, 사용자는 각각 로그인 계정을 추가/편집하거나 보안 시리얼 장치 서버의 사용자 계정을 관리하기 위해 써드파티 인증 서비스를 활용할 수 있습니다.



사용자 계정 및 써드파티 인증 서비스 구성에 대한 자세한 내용은 5장 사용자 관리를 참조하십시오.

로그

Logs 페이지는 보안 시리얼 장치 서버의 모든 시스템 로그 정보가 나열됩니다.

SYSTEM LOGS

<div> <div>EXPORT</div> <div>CLEAR ALL</div> </div>			
Severity	User	Description	Date/Time
Information	-	NTP get new time:2089-02-23 12:51:22	2089-02-23 12:51:22
Information	administrator	HTTPS ,Login succeeded at 10.3.41.174:54530	2089-02-23 12:51:16
Information	-	NTP get new time:2089-02-23 12:41:36	2002-07-01 01:01:13
Information	-	LAN port was up.	2002-07-01 01:01:13
Information	-	IP address retrieved from a DHCP server	2002-07-01 01:01:07
Information	-	Port 2 online.	2002-07-01 01:01:07
Information	-	Port 1 online.	2002-07-01 01:01:07
Information	-	NTP get new time:2021-02-05 08:57:48	2021-02-05 08:57:48
Information	-	NTP get new time:2021-02-05 08:27:48	2021-02-05 08:27:48
Information	-	NTP get new time:2021-02-05 07:57:48	2089-02-23 11:11:54
Information	-	NTP get new time:2089-02-23 10:41:54	2021-02-05 07:27:47
Information	-	NTP get new time:2021-02-05 06:57:48	2021-02-05 06:57:49
Information	administrator	HTTPS ,Timeout at 10.3.41.112	2021-02-05 06:51:38

항목	설명
Export	로그를 log.txt 파일로 PC에 내보내고 다운로드합니다.
Clear All	모든 로그 정보를 삭제합니다.

이 페이지에는 최대 2048개의 로그를 저장하고 표시할 수 있습니다.

이 페이지는 빈 페이지입니다.

5 장

사용자 관리

개요

이 장에서는 써드파티 인증 서비스 사용과 함께 관리자를 포함한 보안 시리얼 장치 서버의 로그인 계정을 추가하거나 편집하는 방법에 대해 설명합니다.

사용자


보안 시리얼 장치 서버는 아래에 설명한 것처럼 2가지 유형의 사용자로 최대 16개의 사용자 계정을 지원합니다.


사용자 유형	역할
Administrator	모든 시리얼 포트에 접속 및 구성하고 다른 로그인 계정을 관리할 수 있습니다.
User	관리자가 허용한대로 승인된 시리얼 포트에만 접속 또는 구성할 수 있으며, 모든 장치의 시스템 설정을 구성할 수 없습니다.

USERS

ONLINE USERS

+ ADD

 EDIT

 DELETE

<input type="checkbox"/>	Name	Type	Description	Status
<input type="checkbox"/>	administrator	Administrator		Normal
<input type="checkbox"/>	user-01	User		Normal

항목	설명
Name	사용자 계정의 사용자 이름을 표시합니다.
Type	계정 유형을 Administrator 또는 User로 표시합니다.
Description	사용자 계정을 설명하는데 사용되는 추가 정보입니다.
Status	다음에 포함하는 사용자 계정의 상태를 표시합니다. <ul style="list-style-type: none">◆ Normal: 계정이 정상적으로 작동합니다.◆ Password Expired: 계정의 암호가 만료되었으며 변경해야 합니다.

사용자 추가

1. 보안 시리얼 장치 서버의 웹 인터페이스에서 **User Accounts > User > Users**를 클릭하십시오.
2. **Add**를 클릭하십시오. **Add User window**의 General 탭이 나타납니다. 아래 테이블과 같이 필요한 필드를 입력하십시오.

항목	설명
Username	계정 정책 설정에 따라 1 ~ 32자까지 허용됩니다. 47페이지 계정 정책을 참조하십시오.
Password	계정 정책 설정에 따라 1 ~ 16자까지 허용됩니다. 47페이지 계정 정책을 참조하십시오.
Confirm Password	Password 필드를 일치시켜 암호 입력을 확인합니다.
Description	사용자가 포함하고 싶어하는 추가 정보입니다.
User type	Administrator를 선택하면 전체 접속 및 환경 구성 권한을 허용하며, User를 선택하면 설정된 대로 시리얼 포트의 접속 및 환경 구성 권한만 허용합니다.
User cannot change account password	선택하면 사용자가 계정 암호를 변경하지 못하도록 제한합니다.
User must change password at next login	체크하면 사용자가 다음에 로그인 할 때 비밀번호를 변경하도록 요구합니다.

항목	설명
Password expires on	로그인 계정의 암호가 만료되고 다시 정의되는 날짜를 지정합니다. 주의: 사용자의 암호가 만료된 후에도 이전 암호로 로그인 할 수 있지만 로그인 시 암호를 변경해야 합니다.

3. User 사용자 유형에만 해당 - 아래 테이블에서 설명하는 것처럼 각 시리얼 포트에 대한 접속을 허용하거나 권한을 구성하려면 **Device** 탭을 클릭하십시오.

Serial Port	No Access	View Only	Full Access	Configuration
[01]Port1	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
[02]Port2	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>

SAVE CANCEL

항목	설명
No Access	선택하면 시리얼 포트에 대한 접속을 제한합니다.
View Only	선택하면 시리얼 포트에 대한 보기 접속만 허용하고 Telnet 및 SSH 세션을 제한합니다.
Full Access	선택하면 시리얼 포트에 대한 전체 접속을 허용합니다.
Configuration	체크하면 속성, 동작 모드 및 포트 버퍼링 설정을 포함한 시리얼 포트에 대한 환경 구성을 허용합니다. 27페이지 시리얼 포트 편집을 참조하십시오.

4. **Save**를 클릭하여 완료합니다.
5. Operation Succeeded 메시지가 나타나면 **OK**을 클릭하십시오.

사용자 편집

사용자 계정을 편집하려면, 해당 계정을 선택하고 **Edit**를 클릭하십시오.

사용자 편집 윈도우에서 56페이지 사용자 추가를 참조하여 변경한 다음 **Save**를 클릭하십시오.

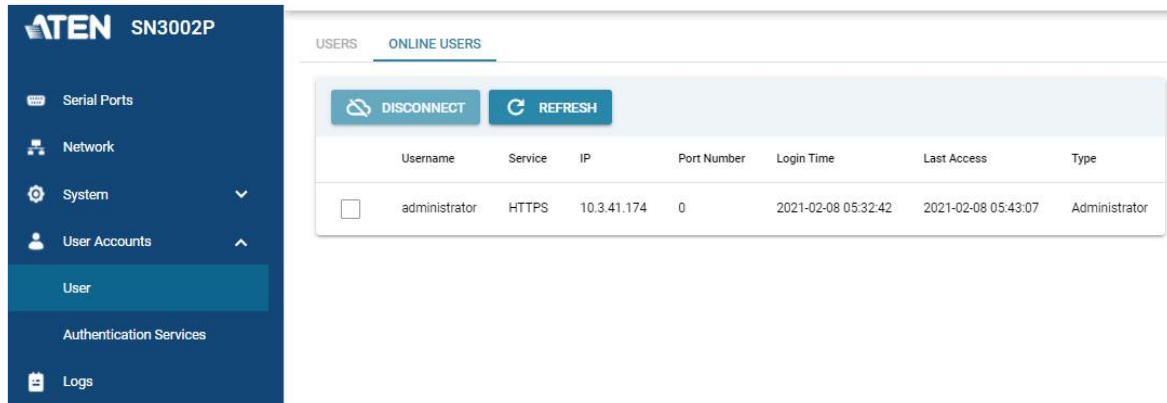
사용자 삭제

사용자 계정을 삭제하려면 해당 계정을 선택하고 **Delete**를 클릭하십시오.

Are you sure to delete? 라는 메시지가 표시되면 확인을 위해 **OK**을 클릭하십시오.

온라인 사용자

Online Users 탭에는 현재 보안 시리얼 장치 서버에 접속 중인 사용자 계정이 표시됩니다.



	Username	Service	IP	Port Number	Login Time	Last Access	Type
<input type="checkbox"/>	administrator	HTTPS	10.3.41.174	0	2021-02-08 05:32:42	2021-02-08 05:43:07	Administrator

관리자는 현재 로그인된 다른 사용자 계정을 선택하고 **Disconnect**를 클릭하여 해당 사용자의 접속 세션을 종료할 수 있습니다.

인증 서비스

보안 시리얼 장치 서버는 외부의 써드파티 인증 서비스, 즉 RADIUS를 통해 사용자 계정을 관리하고 인증할 수 있습니다.

주의: 인증에 RADIUS를 사용하는 경우 PAP만 지원됩니다.

이러한 서비스를 사용하려면 웹 인터페이스에서 **User Accounts > Authentication Services**를 클릭하십시오.

RADIUS

RADIUS

☒ Enable RADIUS

Preferred server IP/address

Preferred server port

Alternate server IP/address

Alternate server port

Timeout

Retries

Shared Secret (at least 6 characters)

1812

1645

3 second(s)

3

Secret

1. RADIUS를 통한 인증을 사용하려면, 아래 테이블을 참조하여 보안 시리얼 장치 서버의 서비스를 활성화하십시오.

항목	설명
Preferred server IP/ address and server port	기본 (선택) RADIUS 서버의 IP 주소와 서비스 포트를 입력하십시오.
Alternate server IP/ address and server port	대체 RADIUS 서버의 IP 주소와 서비스 포트를 입력하십시오.
Timeout	보안 시리얼 장치 서버가 RADIUS 서버를 기다리는 시간 (초)을 설정합니다.
Retries	허용되는 RADIUS 재시도 횟수를 설정합니다.
Shared Secret (at least 6 characters)	보안 시리얼 장치 서버와 RADIUS 서버 간의 인증에 사용할 문자열을 입력하십시오.

2. RADIUS 서버에서 다음 테이블에 제공된 속성 정보에 따라 각 접속 권한을 설정합니다.

속성	설명
U	(User) 사용자는 일부 포트에 접속 및 구성할 권한을 가집니다. 이 속성은 장치에 접속하는 모든 사용자에게 대해 지정되어야 합니다.
T	(True) 사용자는 지정된 포트에 접속하고 구성할 수 있는 권한을 가집니다.
F	(False) 사용자는 어떤 포트도 구성할 수 없습니다.
A	(All) 사용자는 모든 포트에 접속하고 구성할 수 있는 권한을 가집니다.

예제:

U, T, 1

사용자는 포트 1에 접속하고 구성할 수 있습니다.

-
- 주의:** 1. 문자는 대소문자를 구분하지 않습니다. 즉, 대문자와 소문자가 똑같이 잘 작동하며
임의로 구분됩니다.
2. 문자열에 잘못된 문자가 있으면 보안 시리얼 장치 서버에 접속을 제한합니다.
-

6 장

포트 동작 모드

개요

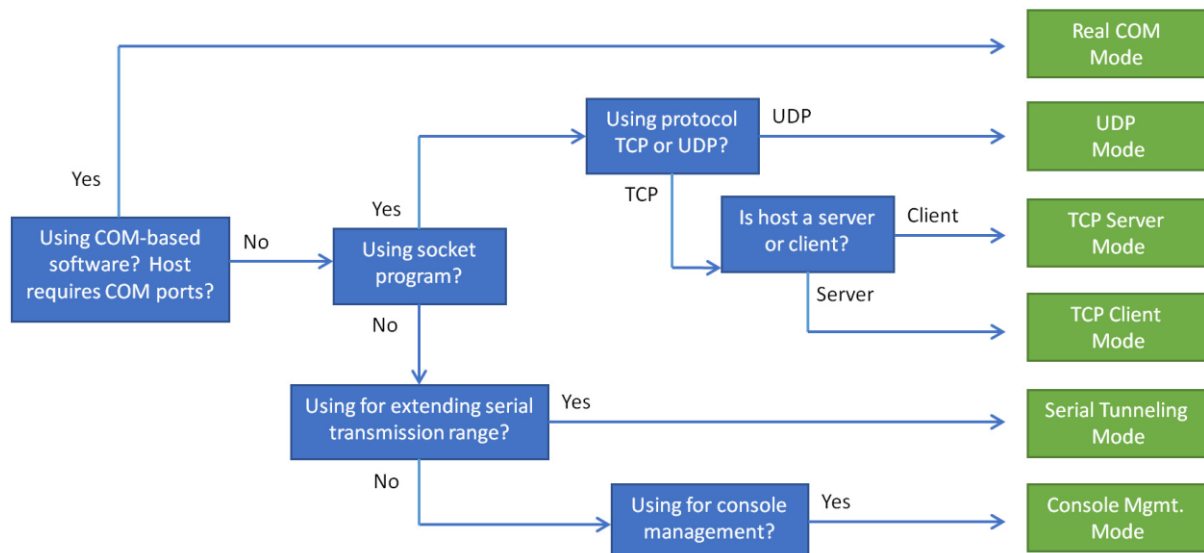
광범위한 시리얼 애플리케이션에 대응하기 위해 보안 시리얼 장치 서버의 COM 포트는 여러 포트 동작 모드를 지원합니다.

여기에는 시리얼-이더넷 연결을 위한 Real COM, TCP 서버 및 클라이언트, UDP 및 시리얼 터널링 서버 및 클라이언트 모드, 콘솔 관리, 장치 제어를 위한 콘솔 관리 다이렉트 및 COM 포트, 시리얼 터널링, 또는 TCP/UDP 소켓 기능이 필요한 분야를 포함합니다.

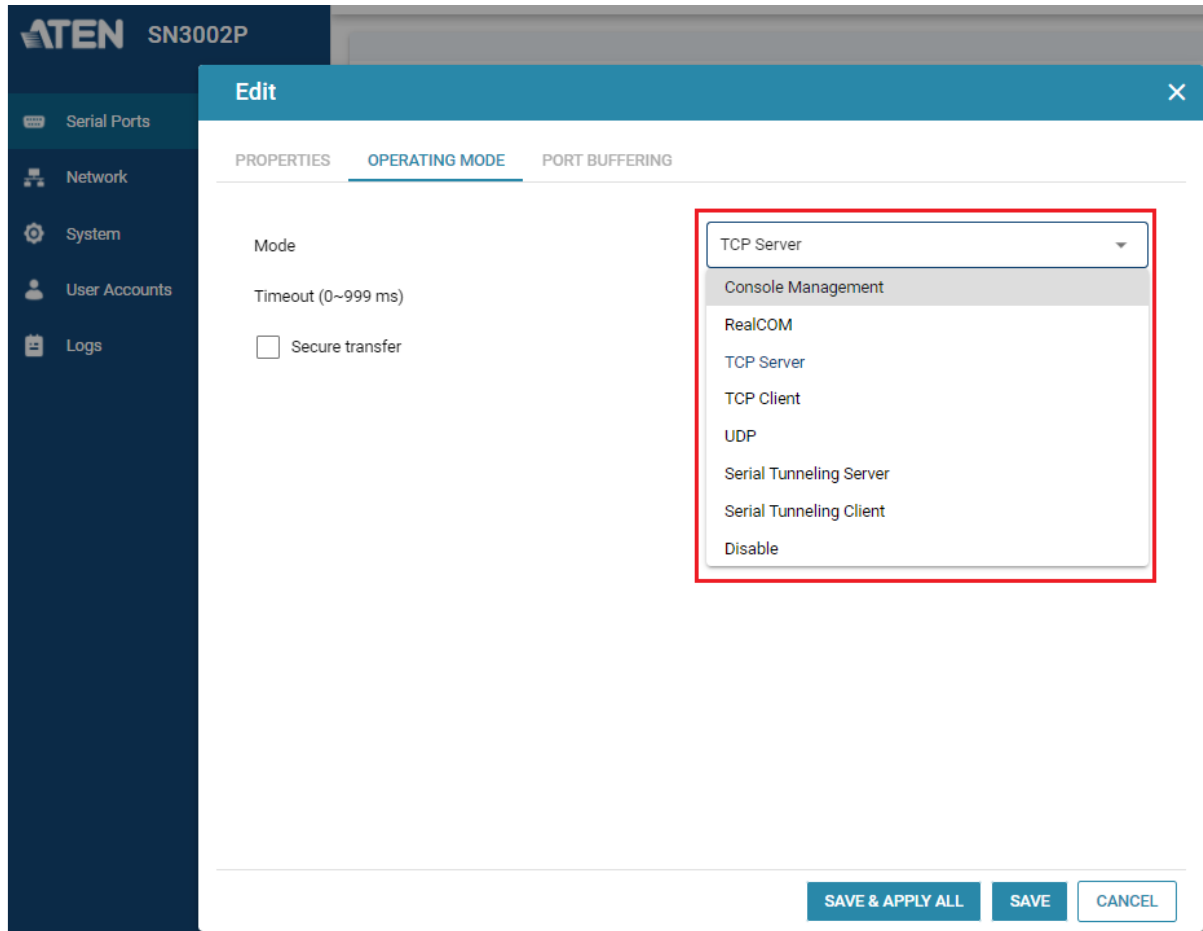
주의: 하나의 시리얼 포트에 대한 최대 동시 연결 수는 16개입니다.

동작 모드 선택

다음은 작동 모드를 선택할 때 고려해야 할 몇 가지 질문입니다.



아래 그림과 같이 Serial Ports > Edit > Operating Mode에서 **Operating Mode**를 선택가능 합니다.



이 페이지에서 사용자는 보안 시리얼 장치 서버의 시리얼 포트를 아래 설명과 같이 사용 가능한 다양한 포트 동작 모드로 설정할 수 있습니다.

동작 모드

시리얼 포트의 동작 모드를 구성하려면 30페이지 동작 모드를 참조하십시오.

Real COM

이 모드는 원격 PC에 설치된 버추얼 COM 포트 드라이버와 함께 사용됩니다. (9장, 버추얼 시리얼 포트 관리자 참조) 보안 시리얼 장치 서버의 COM 포트를 이 모드로 설정하면 연결된 장치가 원격 PC의 COM 포트에 직접 연결된 것처럼 보입니다.



이 모드는 사용자가 순수 시리얼 통신 응용 프로그램 용으로 작성된 소프트웨어를 사용할 수 있도록 하기 때문에, POS 터미널, 바코드 판독기, 시리얼 프린터 등과 같은 장치에 유용합니다. 보안 시리얼 장치 서버는 Windows 시스템용 Real COM 드라이버 (버추얼 시리얼 포트 유틸리티)와 및 Linux 시스템용 TTY 드라이버와 함께 제공됩니다.

TCP 서버 및 클라이언트

TCP (Transmission Control Protocol)는 소켓 프로그래밍을 통해 TCP 프로토콜로 시리얼 데이터를 전송하기 위한 안정적인 전송 계층을 제공합니다.



TCP 서버

TCP 서버 모드에서 데이터 전송은 양방향입니다. 이 모드에서 호스트 컴퓨터는 보안 시리얼 장치 서버와의 연결을 시작하고 시리얼 포트에 대한 연결을 요청합니다.

연결이 설정되면 호스트는 시리얼 장치에서 데이터를 수신합니다. 이 시점부터 호스트와 장치 간에 양방향으로 데이터를 전송할 수 있습니다. 이 작동 모드에서는 SSL 데이터 암호화가 지원됩니다.

보안 시리얼 장치 서버는 이 모드에서 최대 16대의 호스트 컴퓨터에서 동시 연결을 지원하므로 여러 대의 컴퓨터가 동시에 시리얼 장치와 통신할 수 있습니다.

주의: General Settings (일반 설정) 페이지에 지정된 Base socket (기본 소켓) 항목이 장치가 수신하는 포트와 일치하는지 확인하십시오. 5001은 보안 시리얼 장치 서버의 기본 설정입니다. (39페이지 일반 참조)

TCP 클라이언트

TCP 클라이언트 모드에서 시리얼 데이터가 시리얼 포트에 들어오면 보안 시리얼 장치 서버는 호스트 컴퓨터와의 연결을 시작하고 시리얼 데이터를 호스트로 보내기 시작합니다. 보안 시리얼 장치 서버는 데이터를 최대 16대의 호스트 컴퓨터를 동시에 지원하며 이 동작 모드에서 SSL 데이터 암호화를 지원합니다.

시리얼 포트의 동작 모드를 구성하려면 30페이지 동작 모드를 참조하십시오.

시리얼 터널링 서버 및 클라이언트

Serial Tunneling (시리얼 터널링) 이더넷을 통해 2개의 보안 시리얼 장치 서버 간에 직접 연결 설정을 구성하며, 클라이언트-서버 관계에서 동작합니다. 한 장치는 시리얼 터널링 클라이언트로 지정되고 다른 장치는 시리얼 터널링 서버로 지정됩니다.



주의: 이 환경 구성에서, 어느 쪽이 클라이언트 또는 서버로 지정되는 것은 중요하지 않습니다.

두 장치 중 하나의 COM 포트는 컴퓨터의 COM 포트에 연결되고 다른 장치의 COM 포트는 접속할 시리얼 장치에 연결됩니다.

그런 다음 두 장치는 IP 및 포트 주소를 통해 서로 통신하고 SSL 데이터 암호화를 지원합니다. 포트 주소는 일반 설정 페이지의 기본 소켓 항목에 의해 설정됩니다. 세부 사항은 34페이지 일반을 참조하십시오.

UDP 모드

UDP (User Datagram Protocol) 모드는 TCP보다 통신에서 더 빠르고 효율적입니다. UDP 모드에서 통신은 양방향입니다. 시리얼 장치는 보안 시리얼 장치 서버의 COM 포트를 통해 최대 16대의 호스트 컴퓨터와 데이터를 주고받을 수 있습니다.



TCP와 같은 방식으로 오류 검사를 수행하지 않기 때문에 UDP는 데이터 정확도에 최적화된 느린 TCP보다 실시간 애플리케이션 (예: 메시지 표시)에 더 적합합니다.

콘솔 관리

Console Management를 통해 사용자는 연결된 시리얼 장치를 관리하고 제어하기 위해 보안 시리얼 장치 서버에 대한 Telnet 또는 SSH 세션을 설정할 수 있습니다. 사용자는 Telnet 또는 SSH를 통해 Java SNViwer 애플리케이션을 사용하거나 Telnet, SSH 또는 PuTTY를 통해 원격으로 로그인 할 수 있습니다.



- 주의:** 1. General Settings (일반 설정) 페이지에 지정된 Base socket (기본 소켓) 항목이 장치가 수신하는 포트와 일치하는지 확인하십시오. 5001은 보안 시리얼 장치 서버의 기본 설정입니다. (39페이지 일반 참조)
2. 이 모드에서는 Cisco 콘솔 케이블 (DB-9 to RJ-45)을 사용하여 보안 시리얼 장치 서버를 Cisco 네트워크 스위치에 연결할 수도 있습니다.
-

콘솔 관리 다이렉트

콘솔 관리 모드에서 **Direct** 옵션이 활성화되면 사용자는 웹 브라우저를 통해 로그인 할 필요없이 PC에서 보안 시리얼 장치 서버에 연결된 시리얼 장치로 직접 Telnet 또는 SSH 세션을 설정할 수 있습니다. 사용자는 PC에서 직접 Telnet, SSH 또는 PuTTY를 사용하여 연결된 시리얼 장치에 로그인 할 수 있습니다. 시리얼 포트의 동작 모드를 구성하려면 30페이지 동작 모드를 참조하십시오.

비활성화

이 모드에서는 보안 시리얼 장치 서버의 시리얼 포트가 비활성화됩니다.
시리얼 포트의 동작 모드를 구성하려면, 30페이지 동작 모드를 참조하십시오.

Modbus 게이트웨이

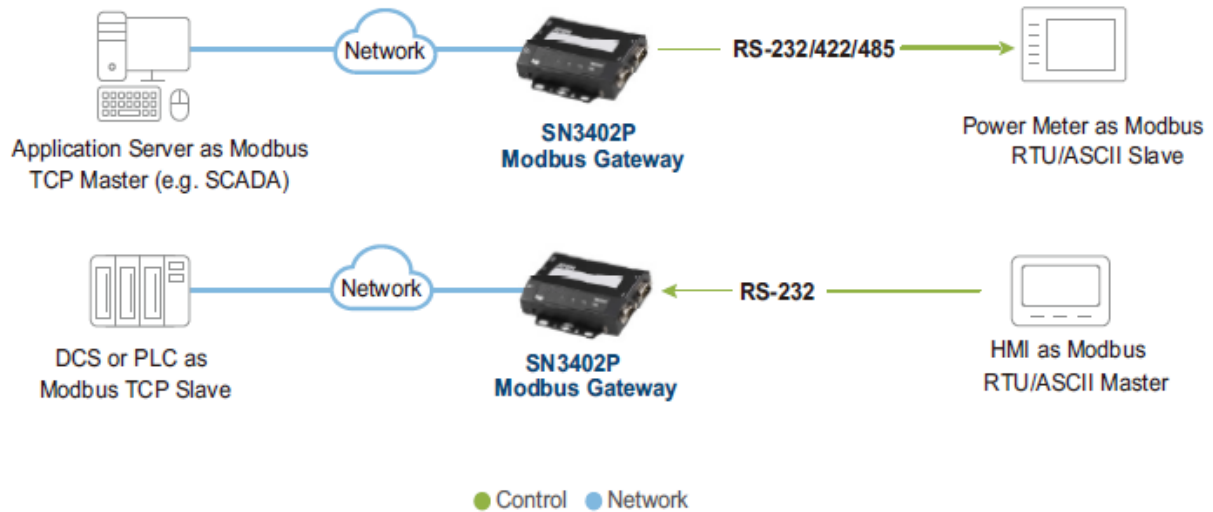
SN3401 / SN3401P / SN3402 / SN3402P가 Modbus TCP와 Modbus RTU/ASCII 프로토콜 간의 데이터를 변환하는 게이트웨이 역할을 수행하려면, 동작 모드를 Modbus 마스터 또는 Modbus 슬레이브로 구성하십시오.

일반적인 애플리케이션

- ◆ 여러 시리얼 슬레이브가 있는 이더넷 클라이언트
여러 시리얼 슬레이브가 있는 TCP 클라이언트 (예: SCADA 시스템)가 있는 경우 SN3401 / SN3401P / SN3402 / SN3402P를 동시에 최대 31대의 슬레이브 장치에서 통신을 지원하는 Modbus 슬레이브로 설정할 수 있습니다.

◆ 여러 이더넷 서버가 있는 시리얼 마스터

여러 TCP 서버가 있는 HMI (Human Machine Interface) 시스템과 같은 시리얼 마스터 장치가 있는 경우, SN3401 / SN3401P / SN3402 / SN3402P를 동시에 최대 32대의 서버에서 통신을 지원하는 Modbus 마스터로 설정할 수 있습니다.




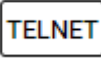

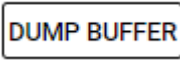
이 페이지는 빈 페이지 입니다.

7 장

포트 접속

개요

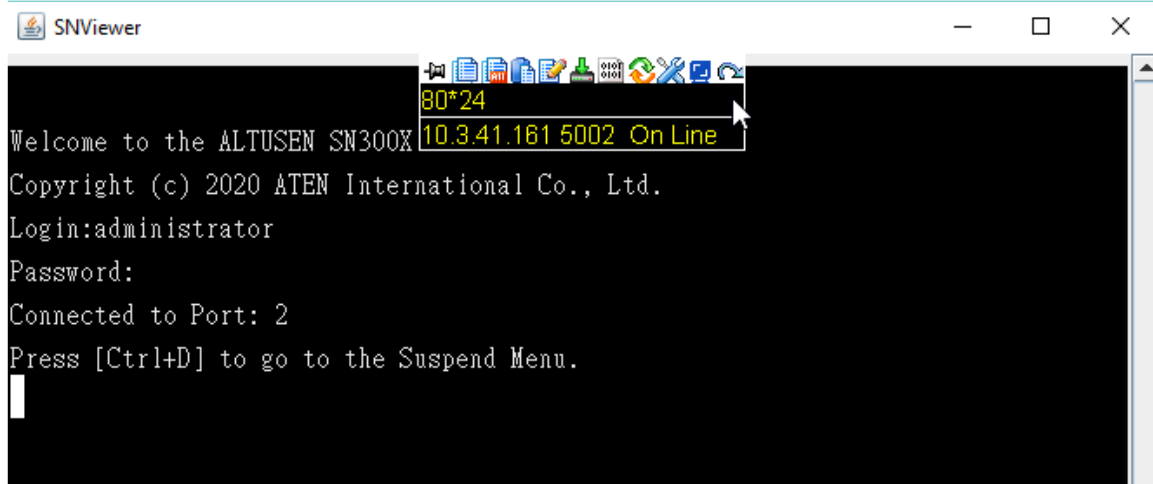
보안 시리얼 장치 서버의 웹 인터페이스에 로그인하면 **Serial Ports** 페이지가 나타납니다. 아래 설명된 버튼을 사용하여 장치의 시리얼 COM 포트에 접속하고 제어합니다.

버튼	기능
	시리얼 포트의 설정을 편집합니다. 27페이지 시리얼 포트 편집을 참조하십시오.
	SNViewer을 사용하여 보안 시리얼 장치 서버로 Telnet 세션을 열고 환경 구성 메뉴에 접속하거나, 시리얼 장치를 COM 포트에 연결합니다. 세부 사항은 70페이지 Telnet/SSH를 참조하십시오.
	SNViewer을 사용하여 보안 시리얼 장치 서버로 SSH 세션을 열고 환경 구성 메뉴에 접속하거나, 시리얼 장치를 COM 포트에 연결합니다. 세부 사항은 70페이지 Telnet/SSH를 참조하십시오.
	시리얼 포트의 포트 활동 로그 (최대 128KB)를 log.txt 파일로 다운로드합니다. 28페이지 포트 버퍼링을 참조하십시오.

주의: 버튼은 사용자가 수행할 권한이 있는 기능에 대해서만 활성화됩니다.

Telnet / SSH

Telnet 또는 SSH를 통해 보안 시리얼 장치 서버의 환경 구성 메뉴에 접속하거나, COM 포트에 연결된 시리얼 장치에 접속하려면 Serial Ports 페이지에서 **Telnet** 또는 **SSH** 버튼을 클릭합니다. Java 애플리케이션 (SNViewer)이 나타나고 아래 예시와 같이 Telnet / SSH 세션을 엽니다.

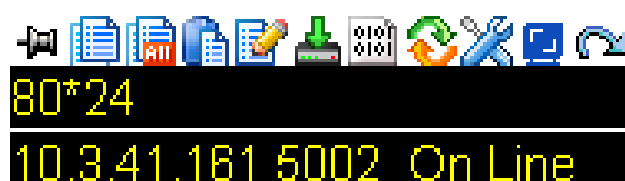


- 주의:** 1. SNViewer를 실행하려면 JRE 8이 설치되어 있어야 합니다.
2. Telnet / SSH 버튼이 나타나기 위해서는 보안 시리얼 장치 서버의 COM 포트는 콘솔 관리 모드로 설정해야 합니다 (30페이지 동작 모드 참조)

SNViewer

SNViewer는 Telnet/SSH 프로토콜을 통해 웹에서 보안 시리얼 장치 서버에 연결된 시리얼 장치에 액세스하는 데 사용되는 Java 애플리케이션입니다.












SNViewer 위로 마우스 커서를 이동하면 컨트롤 패널이 나타납니다. 컨트롤 패널은 1개의 아이콘 행과 2개의 텍스트 행인 총 3개의 행으로 구성됩니다.



- ◆ 기본적으로 상단 텍스트 행에는 윈도우의 너비와 높이가 표시됩니다. 마우스 커서를 컨트롤 패널의 아이콘 위로 이동하면 상단 텍스트 행의 정보가 변경되어 아이콘의 기능을 나타냅니다.
- ◆ 하단 행에는 현재 연결 상태와 함께 접속중인 장치의 IP 주소와 포트가 표시됩니다.

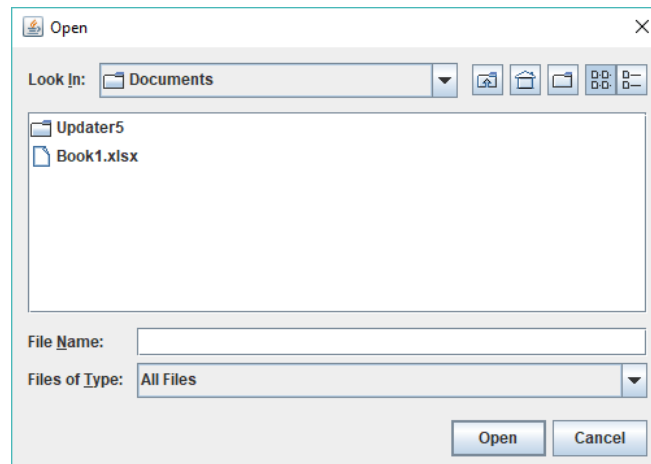
컨트롤 패널 기능

컨트롤 패널 기능은 아래 테이블에 설명되어 있습니다.

아이콘	기능
	컨트롤 패널이 Always On Top (항상 위) 또는 Auto Hide (자동 숨김) 모드로 나타나도록 합니다.
	화면에 있는 선택된 문자를 복사합니다.
	화면에 있는 전체 문자를 복사합니다.
	복사된 문자를 붙여 넣기 합니다.
	로그인/로그오프를 토글합니다. 시리얼 장치에서 SNViewer로 보내지는 문자들의 로그 파일을 전송 시작합니다. 사용자는 반드시 텍스트 기반 로그 파일을 생성하고 가져오기 해야합니다. (53페이지 로그 참조)
	가져오기 할 데이터 파일을 탐색합니다. (72페이지 데이터 가져오기 참조)
	페이지 인코딩을 변경합니다. (72페이지 인코딩 참조)
	터미널 설정을 기본 설정으로 리셋합니다.
	SNViewer의 폰트, 색상, 및 다른 표시 설정을 변경합니다. (72페이지 터미널 설정 참조)
	SNViewer 윈도우의 폭을 조절합니다.
	SNViewer을 종료합니다.

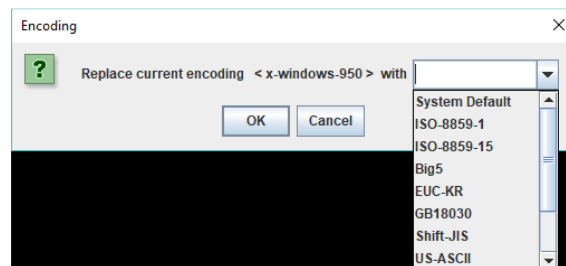
데이터 가져오기

Data Import 페이지는 표준 브라우저 메뉴를 열고 아래 그림처럼 데이터 파일을 가져옵니다.



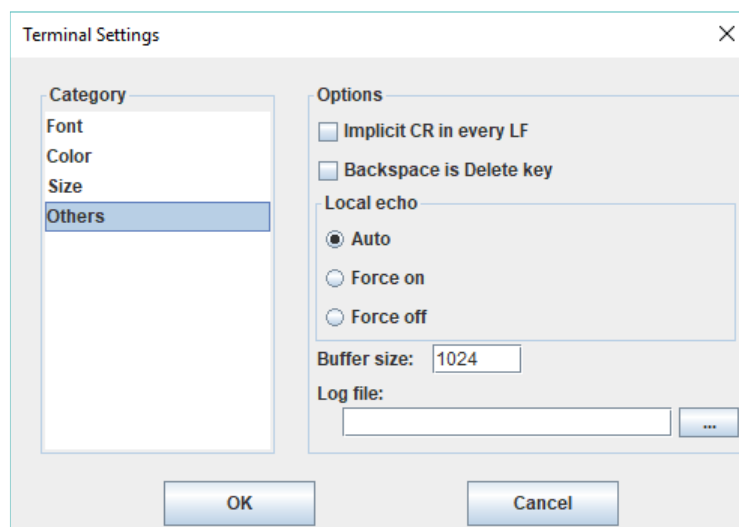
인코딩

Encode 옵션은 아래와 같이 사용될 인코딩 유형을 선택합니다.



터미널 설정

Terminal Settings 옵션을 사용하면 아래와 같이 터미널 세션의 디스플레이 파라미터 및 설정을 변경할 수 있습니다.



분류	사용
Font	폰트 유형, 크기, 스타일을 포함한 SNViewer의 폰트를 설정합니다. 설정 예제는 오른쪽에 표시됩니다.
Color	<p>앞 배경 색상(Foreground color), 뒤 배경 색상(Background Color0) 커서 문자 색상(Cursor Text color), 커서 색상(Cursor Color)을 변경합니다.</p> <p>HSL, Swatches, HSV 탭을 사용하여 세밀하게 조절하고 색상을 선택합니다.</p> <p>탭 아래 Preview 부분에서 변경된 색상을 미리 볼 수 있습니다.</p> <p>OK를 클릭하여 변경 사항을 저장합니다. Cancel을 클릭하면 변경사항을 제거하고 종료하거나, Reset를 누르면 기본 색상 설정으로 돌아갑니다.</p>
Size	창 크기에 따라 표시되는 정보의 양이 결정됩니다. Column (열) 및 Row (행) 크기를 구성하여 SNViewer의 윈도우 크기를 변경합니다.
Others	<p>이 섹션을 사용하여 다음을 설정합니다.</p> <ul style="list-style-type: none"> ◆ Implicit CR in every LF – 이 박스를 체크하면 [Enter]키가 눌릴 때 되돌림 문자가 추가되어, 커서는 왼쪽 여백에 정렬되어 복귀합니다. [Enter] 입력 후에 문자가 왼쪽 여백에 정렬되지 않는 경우 이 기능을 사용합니다. ◆ Backspace는 Delete 키입니다. ◆ Local echo: 에코는 입력된 문자의 시리얼 장치에서 오는 응답입니다. <ul style="list-style-type: none"> ◆ Auto: 입력된 문자는 에코 응답을 받았지만 화면에 표시되지 않습니다. ◆ Force On: 입력된 문자는 에코 응답을 받았고 입력된 대로 화면에 표시됩니다. 이 모드가 사용된 경우 암호가 화면에 표시됩니다. ◆ Force Off: 입력된 문자는 시리얼 장치로부터 에코 응답을 받지 않았습니다. ◆ Buffer size – 이것은 로그 파일의 최대 크기입니다. ◆ Log file – 로그 파일은 SNViewer에 연결된 시리얼 장치로부터 보내진 문자들의 로그를 생성합니다. 로그는 우선 노트 혹은 워드를 사용하여 외부 편집기를 사용하여 텍스트 파일로 생성되어야 하며, 그 후 여기에서 열어야 합니다. 그 다음 사용자는 SNViewer 컨트롤 패널로부터 Logging on을 활성화해야 합니다. (71페이지 컨트롤 패널 기능 참조)

이 페이지는 빈 페이지입니다.

8 장

원격 터미널 옵션

개요

보안 시리얼 장치 서버는 다음 섹션에서 설명하는 것처럼 Telnet, SSH 또는 PuTTY를 포함한 다양한 방법을 통해 원격 터미널 세션을 통해 접속할 수 있습니다.

터미널 로그인

웹 브라우저를 사용하는 것 외에도 사용자는 Telnet, SSH 또는 PuTTY와 같은 텍스트 기반 터미널 애플리케이션을 사용하여 원격으로 로그인 할 수도 있습니다.

Telnet 로그인

터미널 (명령어 라인) 세션을 시작하고 다음과 같은 포맷으로 보안 시리얼 장치 서버의 IP 주소를 입력하십시오.

```
telnet [IP Address]
```

[Enter]를 누르십시오.

주의: 기본 Telnet 포트는 23입니다. 보안 시리얼 장치 서버의 COM 포트에 연결된 장치를 제어하려면 (메인 메뉴를 열지 않고), General 설정 (39페이지 일반 설정 참조)에서 Base socket 항목에 설정된 대로 포트 번호를 입력하십시오.

예: **telnet 192.168.0.60 5001**

로그인 프롬프트가 나타납니다.



처음 로그인하는 경우, 기본 사용자 이름 (administrator)을 입력하고 [Enter]를 누른 후, 기본 암호 (password)를 입력하고 [Enter]를 다시 눌러 로그인 합니다.

SSH 로그인 (Linux)

터미널 (명령어 라인) 세션을 시작하고 다음과 같은 포맷으로 보안 시리얼 장치 서버의 IP 주소를 입력하십시오.

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

[Enter]를 누른 다음 보안 시리얼 장치 서버의 암호를 입력하면 로그인 합니다.

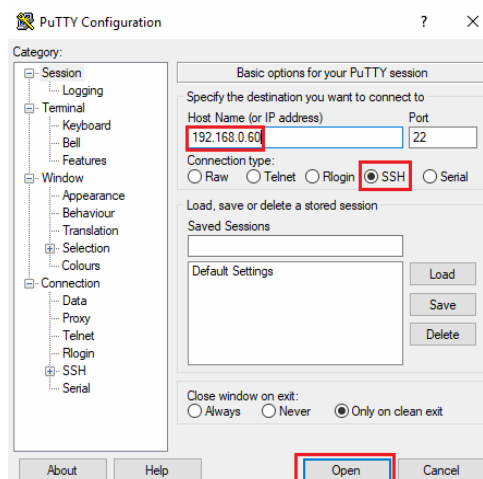
주의: 기본 SSH 포트는 22입니다. 보안 시리얼 장치 서버의 COM 포트에 연결된 장치를 제어하려면 (메인 메뉴를 열지 않고), General 설정 (39페이지 일반 설정 참조)에서 Base socket 항목에 설정된 대로 포트 번호를 입력하십시오.

예: **ssh administrator@192.168.0.60-P5001.**

써드파티 유틸리티 (Windows)

SSH 세션은 Win32 및 Unix 플랫폼용 무료 Telnet 및 SSH인 PuTTY와 같은 써드파티 유틸리티를 사용하여 Windows에서 접속할 수 있습니다. PuTTY를 통해 SSH 연결을 설정하려면 다음을 수행하십시오.

1. Host Name 아래에서, 보안 시리얼 장치 서버의 IP 주소를 입력하십시오.



2. Protocol 아래에서 **SSH**를 선택하고 **Open**을 클릭하십시오.
3. 연결이 이루어지면, 유효한 사용자 이름과 암호를 입력하여 보안 시리얼 장치 서버에 로그인 합니다.

주의: 로그인에 실패하면 SSH 프로토콜을 통해 다시 시도할 수 없습니다. PuTTY를 닫고 다시 시작해야 합니다.

터미널 메인 메뉴

로그인이 되면 다음 텍스트 기반 메인 메뉴가 나타납니다.

```

SN3001   Main Menu
=====
 1. General Settings
 2. User Settings
 3. Port Settings
 4. Device Access
 5. Network Settings
 6. Date/Time Settings
 7. Service Settings
 8. System
 9. History Buffer
10. Network Management Service
 Q. Logout

Select one:

```

터미널 세션 메인 메뉴에는 이전에 설명한 웹 브라우저와 유사한 텍스트 기반 환경 구성이 포함되어 있지만, 펌웨어 업그레이드와 백업 및 복원을 설정하는 등을 할 수 없는 몇 가지 제한 사항이 있습니다.

사용자는 하위 메뉴를 통해 작업하는 동안 브라우저 버전에 제공된 정보를 참조할 수 있습니다. (25페이지 웹 콘솔 참조)

주의: 브라우저 버전과 마찬가지로 이러한 하위 메뉴의 대부분에 대한 접속은 관리자 또는 COM 포트 접속 권한이 있는 사용자로 제한됩니다. 권한이 없는 하위 메뉴를 선택하면 아무 일도 일어나지 않습니다.

사용자는 4. Device Access 메뉴를 통해 보안 시리얼 장치 서버에 연결된 시리얼 장치에 접속할 수 있습니다.

주의: 연결된 시리얼 장치에 접근하려면 시리얼 포트의 작동 모드를 콘솔 관리로 설정해야 합니다. (30페이지 동작 모드 참조)

터미널 세션을 닫으려면 메인 메뉴를 불러와 **[Q]**를 눌러 로그 아웃합니다. 그 다음 창을 닫습니다.

이 페이지는 빈 페이지입니다.

9 장

버추얼 시리얼 포트 관리자

개요

보안 시리얼 장치 서버는 Windows용 버추얼 COM 드라이버, Linux용 Real TTY 드라이버, OpenServer, Solaris, FreeBSD, AIX, Mac용 Fixed TTY 드라이버를 제공합니다.

보안 시리얼 장치 서버의 COM 포트에 연결된 장치는 PC에서 드라이버를 실행함으로써 해당 COM 포트에 직접 연결된 것처럼 나타납니다.

주의: 시리얼 포트의 동작 모드를 버추얼 포트로 설정하려면 Real COM으로 설정되어야 합니다.
(30페이지 동작 모드 참조)

데이터 전송은 PC의 버추얼 COM 포트와 보안 시리얼 장치 서버의 COM 포트에 연결된 장치 간에 이더넷을 통해 이루어집니다.

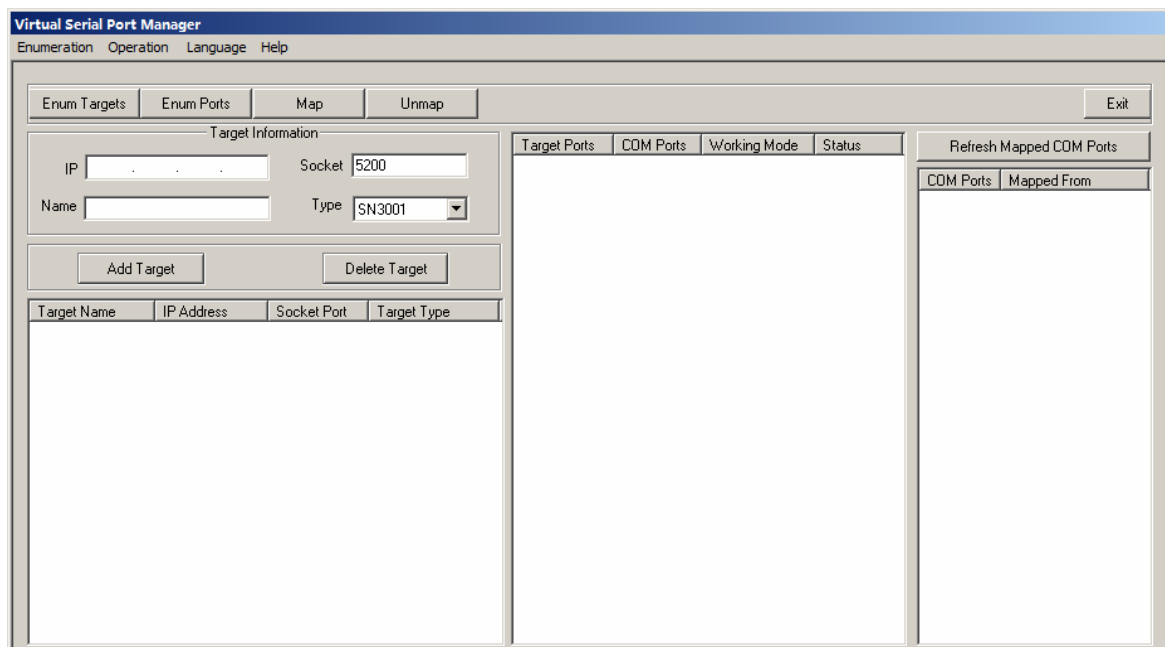
사용자는 보안 시리얼 장치 서버의 제품 웹 페이지에서 PC OS에 해당하는 드라이버를 다운로드하여 설치할 수 있습니다.

Real COM 포트 관리 – 버추얼 시리얼 포트 관리자

버추얼 시리얼 포트 관리자는 COM 포트 매핑을 위한 편리한 인터페이스를 제공하는 유틸리티입니다.

주의: 버추얼 시리얼 포트 관리자는 Windows 및 Linux (Kernel 4.15.0-43 and 4.2.0-27)만 지원합니다. 다른 버전의 Linux 시스템에 대해서는 86페이지 Real COM 포트 관리 — Linux 명령어를 참조하십시오.

Virtual Serial Port Manager (Start > Virtual Port Management Utility > Virtual Serial Port Manager)를 시작합니다. 다음 대화 상자가 나타납니다.



유틸리티 인터페이스

버추얼 시리얼 포트 관리자의 인터페이스는 다음과 같이 구성됩니다.

- ◆ 메뉴 및 버튼 바는 장치 및 포트를 자동으로 열거하고 표시할 수 있습니다.
- ◆ 메뉴 및 버튼 바 아래에 대상 장치가 자동 열거 방법을 사용하여 나타나지 않는 경우 장치를 수동으로 표시하는데 필요한 정보를 입력할 수 있는 영역이 있습니다.
- ◆ 열거를 통해 찾거나 수동으로 입력한 모든 장치가 왼쪽 패널에 표시됩니다.
- ◆ 선택한 장치에서 찾은 모든 포트가 중앙 패널에 표시됩니다.
- ◆ 오른쪽 패널에는 생성된 버추얼 COM 포트 매핑이 표시됩니다.

메뉴 및 툴바

버추얼 시리얼 포트 관리자 메뉴와 툴바는 동일한 기능으로 구성됩니다. 사용자는 아래 테이블에 설명과 같이 메뉴 항목이나 버튼을 클릭하여 원하는 기능을 실행할 수 있습니다.

항목	동작
Enum Targets	이 기능은 LAN 내 보안 시리얼 장치 서버와 ATEN 시리얼 콘솔 서버를 포함한 모든 SN 장치를 검색하고 표시합니다. 결과는 대상 목록 패널에 표시됩니다. (세부 사항은 82페이지 대상 목록 참조) 삭제 기능이 호출되면 대상 목록에 표시된 모든 장치가 삭제됩니다. 삭제 기능을 호출하기 전에 삭제하지 않으려는 장치를 목록에서 제거하십시오.
Enum Ports	이 기능은 대상 목록에서 현재 선택된 대상 장치의 기존 포트를 표시합니다. 결과는 포트 목록 패널에 표시됩니다.
Map	Port List 패널에서 포트를 선택한 후 이 기능을 선택하면 장치의 COM 포트가 사용자 PC의 버추얼 COM 포트에 매핑됩니다.
Unmap	Mapped Ports 목록에서 포트를 선택한 후 이 기능을 선택하면 PC와 장치의 COM 포트 간의 매핑이 해제됩니다.

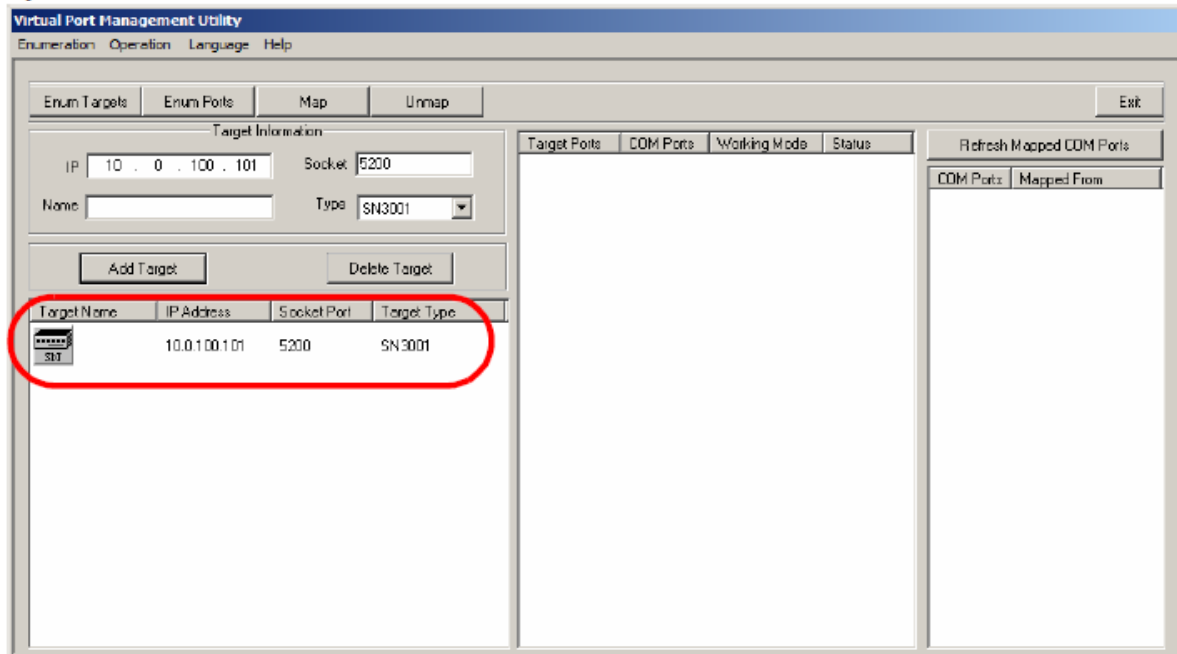
대상 정보

대상 정보 필드를 사용하면 아래에 설명과 같이 오프라인 대상 장치에 포트를 설치 (매핑) 할 수 있습니다.

필드	동작
Target IP Address	COM 포트를 매핑할 대상의 IP 주소를 입력합니다.
Base Socket Port	대상 장치의 기본 소켓 포트입니다. Real COM 포트 동작 경우, 기본 기본 소켓 포트는 5200입니다.
Target Name	대상의 이름입니다. 대상의 실명과 다른 경우 실명으로 대체됩니다. 이름은 매핑/매핑 해제 절차와 관련이 없다는 것에 주의하십시오. IP 주소, 소켓 포트, 대상 유형만 관련됩니다.
Target Type	매핑할 대상의 유형입니다. SN3001 / SN3002 및 ATEN 시리얼 콘솔 서버는 유효한 대상 유형입니다. 주의: SN3001는 SN3001P를 포함하며, SN3002는 SN3002P를 포함합니다.
Add Target	위의 정보를 기반으로 대상 목록에 항목을 생성합니다.
Delete Target	대상 목록에서 현재 선택된 대상을 삭제합니다.

대상 목록

왼쪽 패널에는 Enumeration 기능으로 찾은 모든 장치 및 Target Information 필드에 수동으로 추가된 모든 장치가 표시됩니다.

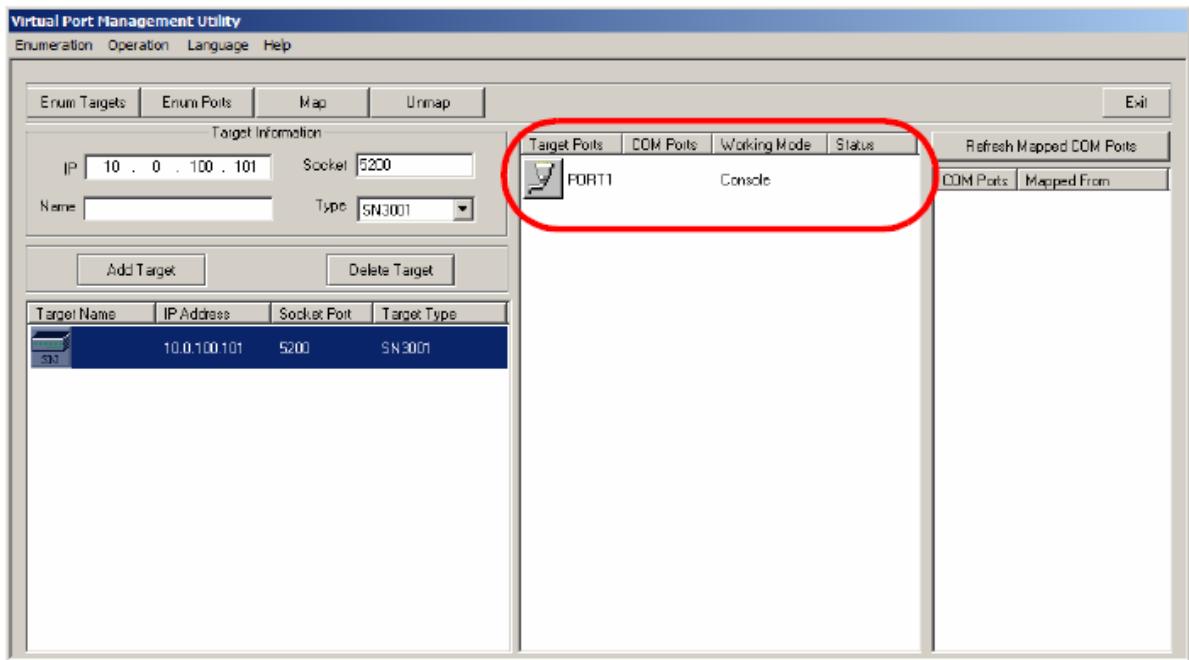


주의: 목록에서 항목을 더블 클릭하면 **Enum Ports**를 선택하는 것과 동일한 기능이 호출되어 Port List 옆에 선택한 대상 포트의 번호와 작업 모드가 표시됩니다.

- ◆ Enumeration 절차의 결과로 장치가 자동으로 표시되면 왼쪽의 아이콘에 녹색 점과 선이 그려져 대상이 온라인 상태이고 매핑할 준비가 되었음을 나타냅니다.
- ◆ 장치가 수동으로 목록에 추가되고 오프라인 상태인 경우 왼쪽의 아이콘에 검은색 점과 선이 그려집니다. 수동으로 추가한 항목을 더블 클릭하면 해당 정보가 Port List에 표시되지만 작업 모드 정보는 정확하지 않으며 모든 장치의 포트가 Real COM 모드에 있다고 가정해야 합니다. 포트 모드에 대한 세부 사항은 30페이지 동작 모드를 참조하십시오.
- ◆ 대상이 오프라인이거나 온라인 상태이지만 포트 열거를 요청한 후 2초 이내에 응답하지 않으면 작업 모드 정보가 정확하지 않으며 모든 장치의 포트가 Real COM 모드에 있다고 가정해야 합니다. 포트 모드에 대한 세부 사항은 30페이지 동작 모드를 참조하십시오.

포트 목록

이 목록은 선택한 대상의 포트 정보를 표시합니다. (한 번에 하나의 대상만 선택 가능)



- ◆ 왼쪽 열에는 대상의 포트 번호가 표시되고, 2번째 열에는 매핑된 COM 포트 (있는 경우), 3번째 열에는 동작 모드, 오른쪽 열에는 상태가 표시됩니다.

주의: 동작 모드는 시리얼 포트가 설정된 동작 모드를 나타냅니다. 세부 사항은 30페이지 동작 모드를 참조하십시오.

- ◆ 포트 목록에서 포트를 더블 클릭하면 포트 매핑 대화 상자가 나타납니다. 매핑 세부 사항은 84페이지 포트 매핑을 참조하십시오.

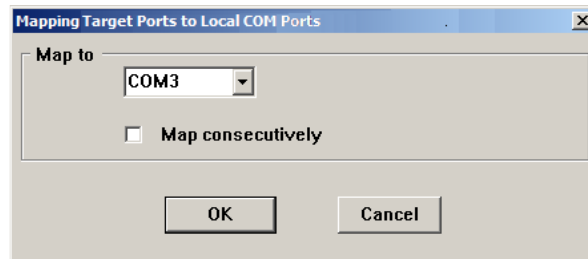
주의: 포트 매핑 대화 상자는 툴바에서 MapTo...를 클릭하거나 메뉴에서 MapTo...를 선택하여 호출할 수도 있습니다.

포트 매핑 및 매핑 해제

포트 매핑

버추얼 COM 포트를 매핑하려면

1. 포트 목록에서 대상 항목을 더블 클릭하여 포트 매핑 상자를 불러옵니다.

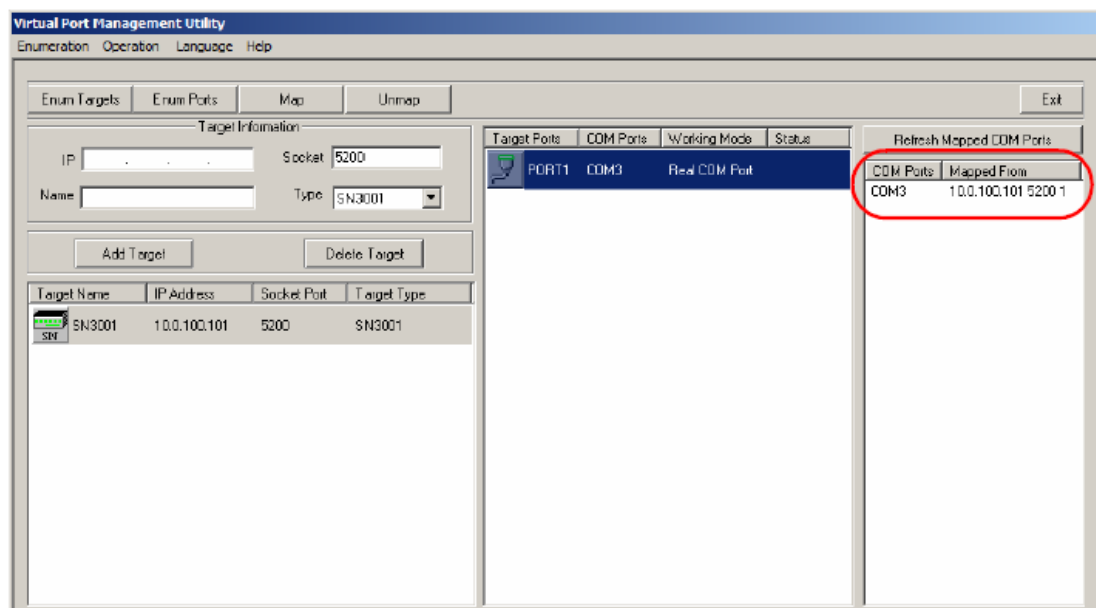


2. 드롭 다운 목록에서 대상 포트를 매핑할 COM 포트를 선택하십시오.
3. **OK**를 클릭합니다.

주의: 경고 대화 상자가 나타나면 무시해도 됩니다. 작업을 완료하려면 **Continue Anyway**를 클릭하십시오.

매핑된 COM 포트

버추얼 포트 관리의 가장 오른쪽 패널에는 매핑된 COM 포트가 표시됩니다. 항목은 애플리케이션이 시작되는 즉시 생성되며 설치 및 제거 결과 매핑된 COM 포트 구성이 변경될 때마다 업데이트됩니다.

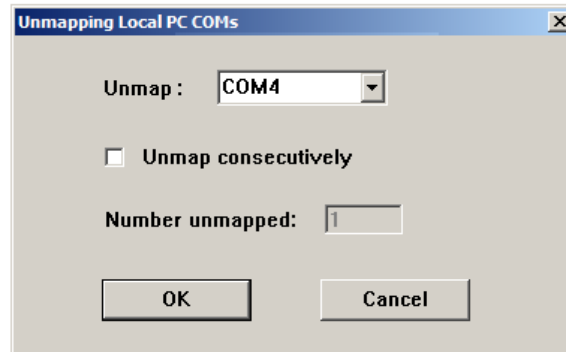


Windows 시스템에서 최대 256개의 포트를 매핑할 수 있습니다.

포트 매핑 해제

버추얼 COM 포트 매핑을 해제하려면 다음을 수행하십시오.

1. 매핑된 COM 포트 (맨 오른쪽 패널에서)를 선택하여 포트 매핑 해제 상자를 불러옵니다.



주의: 대화 상자가 나타나지 않으면 버튼 모음에서 **Unmap...**를 클릭하거나 메뉴에서 Unmap...를 선택합니다.

2. **OK**를 클릭하여 작업을 완료하십시오.

Real COM 포트 관리 – Linux 명령어

버추얼 포트 매핑/매핑 해제

가상 포트를 매핑하거나 매핑을 해제하려면 다음을 수행하십시오.

1. 루트에서, /usr/lib/AtenVPort 디렉토리로 이동하십시오.
2. 다음 명령어를 실행하십시오.

```
/AtenVPMapping
```

이 절차는 Interactive 모드 또는 Fast 모드에서 실행할 수 있습니다. Interactive 모드에서는 사용자가 명령어 라인에서 파라미터를 지정할 필요가 없습니다.

프로그램이 실행될 때 생성된 질문을 기반으로 매핑/매핑 해제를 선택합니다.

Fast 모드를 사용하는 경우, 사용자는 다음 예제와 같이 매핑/매핑 해제 선택 사항을 나타내기 위해 명령어 라인에 파라미터를 입력해야 합니다.

1. 매핑 (입력은 모두 한 라인 내에 있어야 함):

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

```
TargetPort(1-48) NumberofMapping(1-48)
```

1. 매핑 해제 (입력은 모두 한 라인 내에 있어야 함):

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

Linux 시스템에서 최대 256개의 포트를 매핑할 수 있습니다.

버추얼 포트 이름 설정 규칙

Linux 내에 모든 ATEN SN 버추얼 포트에는 접두사 ttya가 있습니다.

매핑된 버추얼 포트는 /dev 디렉토리에서 찾을 수 있습니다. 그들은 모두 ttya 접두사 (ttya000, ttya001 등)를 가지고 있습니다. 범위는 ttya000 – ttya255입니다.


안전 지시 사항

일반

- ◆ 본 제품은 실내에서만 사용 가능합니다.
- ◆ 아래 지시사항들을 전부 읽기를 권장합니다. 참고 사항으로 알아 두십시오.
- ◆ 장비에 관한 모든 경고와 지시사항을 따르십시오.
- ◆ 불안정한 위치(카트, 스탠드, 테이블 등)에 장비를 놓지 마십시오. 만약 장비가 떨어지면 심각한 피해가 발생할 수 있습니다.
- ◆ 물 근처에서 장비를 사용하지 마십시오.
- ◆ 난방기나 열기구 근처 혹은 위에 장비를 놓지 마십시오.
- ◆ 장비 캐비닛은 통풍이 잘 이루어지도록 하기 위한 틈과 구멍이 있습니다. 이러한 통풍구는 절대 막거나 덮어서는 안됩니다.
- ◆ 부드러운 표면(침대, 소파, 융단 등) 위에 절대 장비를 놓아서는 안됩니다. 왜냐하면 통풍구를 막을 수 있기 때문입니다. 마찬가지로 장비는 적절히 통풍이 이루어지지 않는 막힌 공간에 놓아서도 안됩니다.
- ◆ 절대 장비 위에 어떤 액체도 흘려서는 안됩니다.
- ◆ 청소하기 전에 벽 콘센트에 있는 플러그를 빼십시오. 액체나 분무기를 사용하지 마십시오. 젖은 수건을 이용하십시오.
- ◆ 장비는 라벨에 쓰여진 전원의 종류에 따라 동작해야 합니다. 만약 이용 가능한 전원의 종류에 대해 확인할 수 없다면, 판매자에게 문의하십시오.
- ◆ 설비에 손상을 입히지 않으려면 모든 장비를 적절하게 접지해야 합니다.
- ◆ 전원코드나 케이블 위에 어떤 것도 올려놓지 마십시오. 전원 코드나 케이블이 밟히거나 걸리지 않도록 정리하십시오.
- ◆ 시스템 케이블과 전원 케이블을 주의해서 배치하십시오. 케이블 위에 아무것도 올려 놓지 마십시오.
- ◆ 절대 캐비닛 틈 사이로 어떤 것이든 넣지 마십시오. 위험한 전압이 있는 위치를 건드릴 수 있고 출력 부분이 합선되면 화재나 전기 충격을 일으킬 수 있습니다.
- ◆ 절대 스스로 장비를 수리하려고 하지 마십시오. 공인된 엔지니어에게 모든 수리를 맡기십시오.

- ◆ 핫 플러그용 전원 공급기에 전원을 연결하거나 제거할 때, 다음 가이드라인을 준수하십시오.
 - ◆ 전원 공급기에 전원 케이블을 연결하기 전에 전원 공급기를 먼저 설치하십시오.
 - ◆ 전원 공급기를 제거하기 전에 전원 케이블을 분리하십시오.
 - ◆ 시스템이 여러 개의 전원을 사용할 경우, 전원 공급기로부터 모든 전원 케이블을 분리하여 시스템의 전원 연결을 제거하십시오.
- ◆ 만약 다음 상황들이 발생하면 벽 콘센트에서 장비를 분리하고 수리를 위해 공인된 엔지니어에게 가져가십시오.
 - ◆ 전원 코드나 플러그가 손상되었거나 벗겨진 경우
 - ◆ 액체가 장비 안으로 흘러 들어간 경우
 - ◆ 비나 물에 장비가 노출된 경우
 - ◆ 높은 곳에서 떨어졌거나 캐비닛이 손상된 경우
 - ◆ 장비의 성능이 수리를 요할 정도로 눈에 띄게 변화한 경우
 - ◆ 동작 지시사항을 따랐을 때 정상적으로 동작하지 않는 경우
- ◆ 오직 동작 지시사항에 포함되는 컨트롤들만 조절하십시오. 다른 컨트롤들을 적절하지 않게 조절하는 경우 숙련된 엔지니어가 광범위하게 수리 작업을 할 정도의 손상을 장비에 입힐 수 있습니다.
- ◆ 소켓-아웃렛은 장비 근처에 설치해야 하며 쉽게 접근할 수 있어야 합니다.

DC 전원

- ◆ 이 시스템은 단락, 과전류 및 접지 오류로부터 보호하기 위해 건물 설비의 보호 장치에 의존합니다. 건물 설비의 보호 장치가 시스템을 보호할 수 있는 적절한 등급을 받았는지, 국가 및 지역 규정을 준수하는지 확인하십시오.
- ◆ 건물의 설비 배선에 쉽게 접근할 수 있는 분리된 장치가 있는지 확인하십시오.
- ◆ 제품에는 별도의 보호 접지 단자가 제공되며 영구적으로 접지되어야 합니다.
- ◆ DC 공급 회로의 경우, UL, AWM VW-1 Style 1015, 최소 16 AWG, 최소 105° C, 최소 300V 인증을 받은 DC 공급 케이블을 선택합니다.
- ◆  **경고:** 이 장비는 DC 공급 회로의 접지된 컨덕터를 장비의 접지 컨덕터에 연결할 수 있도록 설계되었습니다. 이 연결이 이루어지면 다음 조건이 모두 충족되어야 합니다.
 - ◆ 이 장비는 DC 공급 시스템 접지 전극 도체 또는 DC 공급 시스템 접지 전극 컨덕터가 연결된 접지 단자 막대 또는 버스의 본딩 점퍼에 직접 연결되어야 합니다.
 - ◆ 이 장비는 동일한 DC 공급 회로의 접지된 컨덕터와 접지 컨덕터 사이에 연결된 다른 장비와 같은 인접 영역 (예: 인접한 캐비닛)에 위치해야 하며 DC 시스템의 접지 지점도 있어야 합니다. DC 시스템은 다른 곳에서 접지해서는 안 됩니다.
 - ◆ DC 공급원은 이 장비와 같은 건물 내에 있어야 합니다.
 - ◆ 스위칭 또는 분리 장치는 DC 소스와 접지 전극 컨덕터의 연결 지점 사이의 접지 회로 컨덕터에 있어서는 안 됩니다.
- ◆ **경고:** 이 장치는 접근이 제한된 지역에 설치하기 위한 것입니다. 접근 제한 지역 (서버룸, 데이터 센터 등)은 특수 도구, 잠금 및 키 또는 기타 보안 수단을 사용하여 서비스 직원만 접근할 수 있는 곳이며, 해당 권한이 있는 기관에 의해 제어됩니다.

랙 마운팅

- ◆ 랙 위에 작업하기 전에 stabilizer가 랙에서 바닥까지 안전하게 설치되었는지 확인하시고, 바닥에 기댄 랙의 총 중량을 확인하십시오. 앞면과 옆면 stabilizer를 랙 하나에 설치하거나, 랙 위에 작업하기 전에 여러 개의 랙이 겹친 곳에 앞면 stabilizer를 설치하십시오.
- ◆ 항상 랙 아래에서 위로 물건을 놓으십시오. 그리고 맨 처음 랙에 가장 무거운 물건을 올려 놓으십시오.
- ◆ 랙에 장비를 설치하기 전에 랙이 평평하고 안정적인지 확인하십시오.
- ◆ 장비 레일을 눌렀을 때, 빗장을 풀고 랙에 장비를 밀어 넣거나 뺄 때 주의하십시오. 슬라이드 레일에 손가락을 다칠 수 있습니다.
- ◆ 장비를 랙에 삽입한 후에 조심스럽게 레일을 고정 위치까지 늘립니다. 그리고 나서 장비를 랙에 밀어 넣습니다.
- ◆ 랙에 전원을 제공하는 AC 전원 분류 회로에 과부하를 일으키지 마십시오. 총 랙 부하는 분류 회로 용량의 80%를 초과해서는 안됩니다.
- ◆ 전원 스트립이나 다른 전기 관련 커넥터들을 포함하여 랙에 있는 모든 장비들이 적절하게 접지되어 있는지 확인하십시오.
- ◆ 랙에 있는 장치들 사이에 적절하게 통풍을 하고 있는지 확인하십시오.
- ◆ 랙 환경의 동작 주변 온도가 제조업체에서 제공하는 장비의 최대 주변 온도를 초과하지 않도록 주의하십시오.
- ◆ 랙 안에 다른 장비들이 수리 중일 때 어떤 장비이든지 밟거나 기대지 마십시오.

기술 지원

국제 지역

- ◆ 온라인 기술 지원 – 문제 해결, 문서 및 소프트웨어 업그레이드 <http://support.aten.com>
- ◆ 전화 연결 지원은 iv페이지 전화 연결 지원을 참조하십시오.

북미 지역

E- 메일 지원		support@aten-usa.com
온라인 지원	문제 해결	http://support.aten.com
	문서	
	소프트웨어 업그레이드	
전화 지원		1-888-999-ATEN 내선 4988 1-949-428-1111

본사와 연락할 때 사전에 다음과 같은 정보를 준비하십시오.

- ◆ 제품 모델 번호, 시리얼 번호, 구입 날짜
- ◆ 컴퓨터 환경, 운영체제, 개조 정도, 확장 카드, 소프트웨어
- ◆ 에러가 발생했을 때 나타나는 에러 메시지
- ◆ 에러가 발생하는 동작 과정
- ◆ 문제 해결에 도움이 될 만한 다른 정보들

사양

SN3001 / SN3001P / SN3002 / SN3002P

기능		사양
커넥터	시리얼	1 x DB-9 Male (Black) 1 x DB-9 Male (Black; SN3002 / SN3002P only)
	네트워크	1 x RJ-45 Female (Black)
	전원	PWR1 1 x DC Jack (Black)
		PWR2 1 x 3-pole Terminal (Green)
		PWR3 1 x RJ-45 PoE, IEEE 802.3af (SN3001P / SN3002P only)
스위치	리셋	1 x Semi-recessed button
LED	전원	1 x Green
	상태	1 x Yellow Green / Red
	Port 1 / Port 2	1 x Green / Orange 1 x Green / Orange (SN3002 / SN3002P only)
	10 / 100 Mbps	1 x Green 1 x Orange
전원 입력	전원 잭	9 V DC
	전원 터미널	9 - 48 V DC
	PoE	48 V DC (SN3001P / SN3002P only)
소비 전력	SN3001	DC9V:0.634W:3BTU/h DC48V:0.804W:4BTU/h
	SN3002	DC9V:0.769W:4BTU/h DC48V:0.939W:4BTU/h
	SN3001P	DC48V:0.975W:5BTU/h PoE:1.22W:6BTU/h
	SN3002P	DC48V:1.11W:5BTU/h PoE:1.39W:7BTU/h
		주의: <ul style="list-style-type: none"> ◆ 와트 단위의 측정은 외부 부하가 없는 경우 장치의 일반적인 전력 소비량을 나타냅니다. ◆ BTU/h 단위의 측정은 장치가 완전히 부하가 연결된 때의 전력 소비량을 나타냅니다.

기능			사양
인터페이스	시리얼	표준	RS-232
		Baud Rate	110, 134, 150, 300, 600, 1200, 1800, 2400, 4800, 7200, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600
		RS-232 신호	TxD, RxD, RTS, CTS, DTR, DSR, DCD, GND
		Parity	None, Even, Odd, Mark, Space
		Data Bits	5, 6, 7, 8
		Stop Bits	1, 1.5, 2
		Flow Control	RTS/CTS, DTR/DSR, XON/XOFF, None
	네트워크	표준	10/100BaseTX; Autosensing
		보호	1.5 KV Magnetic Isolation
		프로토콜	ARP, DHCP, DNS, HTTP, HTTPS, ICMP, IP, TCP, UDP, NTP, PPP, RADIUS, Telnet, SNMP, SNMP Trap, SMTP, SSH
표준 및 지원버전		EMC	EN55032/35
		EMI	CISPR 32, FCC Part 15B Class A
		EMS	IEC 61000-4-2 ESD: Contact: 4 kV; Air: 8 kV IEC 61000-4-3 RS: 80 MHz to 1 GHz: 3 V/m IEC 61000-4-4 EFT: Power: 1 kV; Signal: 0.5 kV IEC 61000-4-5 Surge: Power: 2 kV (Power Adapter), 1 kV (Terminal Block); Signal: 1 kV IEC 61000-4-6 CS: 150 kHz to 10 MHz: 3 V/m; 10 kHz to 30 MHz: 3 to 1 V/m; 30 kHz to 80 MHz: 1 V/m IEC 61000-4-8 PFMF IEC 61000-4-11 DIPs
		안전	UL 60950-1 and UL 62368-1 standards compliant
		RoHS	
사용 환경	동작 온도		0 – 60 °C
	보관 온도		-40 – 75 °C
	습도		비응축 상태에서 5 – 95% RH
제품 외관	재질		금속
	무게	SN3001	0.20 kg (0.44 lb)
		SN3002	0.21 kg (0.46 lb)
		SN3001P	0.21 kg (0.46 lb)
		SN3002P	0.22 kg (0.48 lb)
크기 (L x W x H)		9.80 x 11.7 x 2.60 cm (3.86 x 4.61 x 1.02 in)	

SN3401 / SN3401P / SN3402 / SN3402P

	SN3401	SN3402	SN3401P	SN3402P
커넥터				
시리얼	1 x DB-9 Male	2 x DB-9 Male	1 x DB-9 Male	2 x DB-9 Male
네트워크	1 x RJ-45 Female			
전원	◆ 1 x DC Jack ◆ 1 x 3-pole Terminal Block		◆ 1 x DC Jack ◆ 1 x 3-pole Terminal Block ◆ 1 x RJ-45 (PoE, IEEE 802.3af)	
스위치				
리셋	1 x semi-recessed pushbutton			
LED				
전원	1 (Green)			
상태	1 (Yellow Green / Red)			
10/100 Mbps	2 (Green / Orange)			
포트	1 (Green / Orange)	2 (Green / Orange)	1 (Green / Orange)	2 (Green / Orange)
입력 전압				
DC 잭	9 V DC (Power Adapter: 9 V DC 100-240 V AC 50~60 Hz)		DC Jack: 9 V DC 주의: 전원 아답터는 패키지에 포함되어 있지 않지만 구매할 수 있습니다.	
터미널 블록	9-48 V DC		9-48 V DC	
PoE	N/A		48 V DC	
소비 전력				
DC	DC9V:1.18W:6BTU/h DC48V:1.30W:6BTU/h	DC9V:1.19W:6BTU/h DC48V:1.30W:6BTU/h	DC48V:1.30W:6BTU/h	DC48V:1.30W:6BTU/h
PoE	N/A	N/A	PoE:1.475W:7BTU/h	PoE:1.48W:7BTU/h
	주의: ◆ 와트 단위의 측정은 외부 부하가 없는 경우 장치의 일반적인 전력 소비량을 나타냅니다. ◆ BTU/h 단위의 측정은 장치가 완전히 부하가 연결된 때의 전력 소비량을 나타냅니다.			

	SN3401	SN3402	SN3401P	SN3402P
인터페이스				
시리얼	<ul style="list-style-type: none">◆ RS-232: TxD, RxD, RTS, CTS, DTR, DSR, DCD, GND◆ RS-422: Tx+, Tx-, Rx+, Rx-, GND◆ RS-485 (4-wire): Tx+, Tx-, Rx+, Rx-, GND◆ RS-485 (2-wire): Data+, Data-, GND◆ Pull High/Low Resistor for RS-485: 1 kilo-ohm, 150 kilo-ohms◆ Baud Rate: 110, 134, 150, 300, 600, 1200, 1800, 2400, 4800, 7200, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600 bps◆ Data Bits: 5, 6, 7, 8◆ Parity: None, Even, Odd, Space, Mark◆ Stop Bits: 1, 1.5, 2◆ Flow Control: RTS/CTS, DTR/DSR, XON/XOFF			
네트워크	10 / 100 Base TX; Built-in 1.5 kV Magnetic Isolation Protection			
산업 프로토콜	<ul style="list-style-type: none">◆ 이더넷: Modbus TCP 클라이언트 (마스터), Modbus TCP 서버 (슬레이브)◆ 시리얼: Modbus RTU/ASCII 마스터, Modbus RTU/ASCII 슬레이브◆ 최대 Modbus 마스터 모드에서 16개 연결 및 Modbus 슬레이브 모드에서 32개 연결			
지원버전	<ul style="list-style-type: none">◆ EMC: EN 55032/35◆ EMI: CISPR 32, FCC Part 15B Class A◆ EMS: IEC 61000-4-2 ESD: Contact: 4 kV; Air: 8 kV◆ IEC 61000-4-3 RS: 80 MHz to 1 GHz: 3 V/m◆ IEC 61000-4-4 EFT: Power: 1 kV; Signal: 0.5 kV◆ IEC 61000-4-5 Surge: Power: 2 kV (Power Adapter), 1kV (Terminal Block); Signal: 1 kV◆ IEC 61000-4-6 CS: 150 kHz to 10 MHz: 3 V/m; 10 kHz to 30 MHz: 3 to 1V/m; 30 kHz to 80 MHz: 1 V/m◆ IEC 61000-4-8 PFMF◆ IEC 61000-4-11 DIPs◆ Safety: UL 60950-1 and UL 62368-1 standards compliant◆ RoHS			
사용 환경				
동작 온도	0 – 60 °C			
보관 온도	-40 – 75 °C			
습도	비응축 상태에서 5 – 95% RH			
제품 외관				
재질	금속			
무게	0.20 kg (0.44 lb)	0.21 kg (0.46 lb)	0.21 kg (0.46 lb)	0.22 kg (0.48 lb)

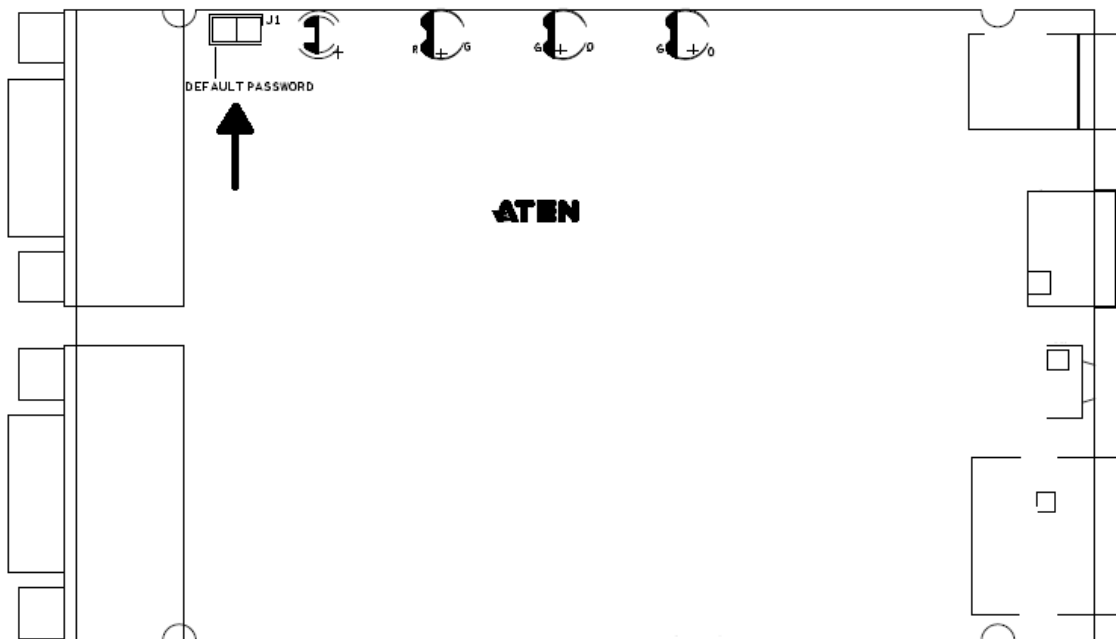
	SN3401	SN3402	SN3401P	SN3402P
크기 (L x W x H)	9.80 x 11.70 x 2.60 cm (3.86 x 4.61 x 1.02 in)			
설치	<ul style="list-style-type: none"> ◆ 데스크탑 ◆ 월 마운팅 ◆ Din 레일 마운팅 ◆ VE-RMK1U를 사용한 랙 마운팅 <p>주의: 랙 마운팅 키트 (VE-RMK1U)는 따로 구매가능합니다.</p>			

로그인 정보 삭제

관리자 로그인을 수행할 수 없는 경우 (예: 로그인 자격 증명이 손상되거나 분실되어) 다음을 수행하여 로그인 정보를 삭제할 수 있습니다.

주의: 이 절차를 수행하면 모든 설정이 공장 기본 값으로 되돌아갑니다.

1. 보안 시리얼 장치 서버의 전원을 끄고 커버를 제거합니다.
2. 점퍼 캡을 사용하여 **J1** (DEFAULT PASSWORD)이라고 표시된 점퍼를 단락 시킵니다.



3. 보안 시리얼 장치 서버의 전원을 켭니다.
4. 상태 LED가 깜박이면 장치의 전원을 끕니다.
5. **J1**에서 점퍼 캡을 제거합니다.
6. 커버를 닫고 장치를 시작합니다.

전원을 켜 후 기본 관리자 사용자 이름과 암호를 사용하여 로그인 할 수 있습니다. 21페이지 로그인을 참조하십시오.

이 절차를 수행한 후 처음 로그인 할 때 암호를 변경하라는 메시지가 표시됩니다.

문제 해결

동작 문제는 다양한 원인으로 인해 발생할 수 있습니다. 문제를 해결하는 첫 번째 단계는 모든 케이블이 소켓에 단단히 연결되어 있는지 확인하는 것입니다.

또한 제품의 펌웨어를 업데이트하면 이전 버전이 출시된 이후 발견되고 해결된 문제를 해결할 수 있습니다. 제품이 최신 펌웨어 버전으로 실행되지 않는 경우 업그레이드할 것을 권장합니다.

업그레이드 세부 사항은 49페이지 펌웨어 업데이트를 참조하십시오.

ATEN 표준 보증 정책

하드웨어 보증 제한

ATEN은 구입 국가에서 최초 구입 일자일로부터 보증 기간 [2]년 동안 부품이나 기술상 결함에 대해서 하드웨어를 보증합니다(보증 기간은 특정 지역/국가별로 상이할 수 있습니다). 이 보증 기간은 ATEN LCD KVM 스위치의 LCD 패널을 포함합니다. UPS 제품은 장치 보증 기간이 [2]년이지만, 일부 제품은 추가로 [1]년 동안 보증됩니다. (세부 사항은 A+ 보증을 참조하십시오) 케이블이나 부속품은 표준 보증이 적용되지 않습니다.

하드웨어 제한 보증 보상 대상

ATEN은 보증 기간 동안 무상 수리 서비스를 제공합니다. 제품에 결함이 있으면 ATEN의 재량권으로 (1) 해당 제품을 새 부품이나 수리된 부품으로 수리하거나 (2) 전체 제품을 동일 제품 또는 결함 제품과 동일한 기능을 수행하는 유사 제품으로 교체하는 옵션을 수행할 수 있습니다. ATEN KOREA에서는 교체된 제품의 보증 기간은 최초 구매한 제품의 보증 기간을 승계 받아 적용합니다. 상품이나 부품이 교체되면, 교체 품목은 고객의 소유가 되며 교체된 품목은 ATEN 소유가 됩니다.

보증 정책에 관한 추가사항은 당사의 웹페이지를 방문하십시오:

<http://www.aten.com/global/en/legal/policies/warranty-policy>

Copyright © 2024 ATEN® International Co., Ltd.
Released: 2024-07-22

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.