Simply Better Connections

CCVSR

비디오 세션 녹화 소프트웨어

사용자 설명서

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
한국	82-2-467-6789
중국	86-400-810-0-810
일본	81-3-5615-5811
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 라이센스가 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.

제품 정보

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

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

패키지 구성

패키지 내에 모든 구성품이 있는지, 구성품 상태가 정상인지 확인하십시오. 배송 중에 누락되거나 손상된 것이 있으면 대리점에 문의하십시오.

CCKM 비디오 세션 녹화 소프트웨어 패키지는 다음과 같이 구성되어 있습니다.

- CCKM USB 라이센스 키 1개
- 소프트웨어 CD 1개
- 사용자 설명서 1개

목차

사용자 정보. ii
온라인 등록. ii
전화 연결 지원. ii
사용자 공지. ii
제품 정보. iii
패키지 구성. iii
목차 iv
설명서에 관하여. ix
규정. x

1장. 소개

개요. 1
기능. 3
요구 사양. 5
컴퓨터. 5
KVM Over IP 스위치. 6
브라우저. 6
대역폭 요구 사양. 6
CCVSR 배치 예제. 8
프라이머리 서버. 8
세컨더리 서버. 8
아카이브 서버. 8
노드. 9
라이센스. 10
라이센스 옵션. 10
노드 옵션. 10

2장. CCVSR 설치

개요. 11
CCVSR 소프트웨어 설치. 11
설치 시작. 11
라이센스. 13

3장. 사용자 인터페이스

개요. 14
브라우저 로그인. 14
웹 브라우저 메인 페이지. 15
페이지 구성. 15
메인 메뉴. 17
개인 정보 / 환경 구성. 17
개인 환경 구성. 18

기본 설정. 18
암호 변경. 18
로그아웃. 19

4장. 재생

개요. 20
비디오 기록 검색 기준. 21
비디오 기록 재생 22
비디오 기록 내보내기 22
비디오 기록 내보내기 22
내보낸 비디오 기록 재생 23
시간 간격 옵션 23
VSR 뷰어. 24
툴바. 25
자막. 27
비디오 기록 파일 열기. 28
비디오 가져오기. 29

5장. 라이브뷰

개요. 32
라이브뷰 페이지 접속. 32
목록 표시. 33
즐겨 찾기 설정. 33
즐겨 찾기 생성. 33
즐겨 찾기 수정. 34
즐겨 찾기 삭제. 34
페이지 회전 / 정지. 35
레이아웃. 35
상태. 36
포트 정보 / 재생 / 라이브뷰 기능 36
싱글 포트 모드. 37

6장. 장치 관리

개요. 38
포트 목록. 38
KVM 포트 녹화. 39
디스플레이. 39
KVM 장치 추가. 40
KVM 장치 편집. 42
녹화. 42
비디오/오디오 녹화 활성화. 42
로컬 콘솔 포트에서 녹화 활성화. 43
KVM 장치 삭제. 43

7장. 사용자 관리

사용자 . . . 44
사용자 유형 . . . 45
사용자 추가 . . . 45
사용자 수정 . . . 48
사용자 삭제 . . . 48
온라인 사용자 . . . 49
로그인 및 암호 정책 . . . 50
로그인 정책 . . . 50
암호 정책 . . . 50
그룹 . . . 51
그룹 생성 . . . 51
그룹 수정 . . . 52
그룹 삭제 . . . 52
인증 . . . 53
AD/LDAP 설정 . . . 53
RADIUS 설정 . . . 54

8장. 시스템

개요 . . . 56
서버 정보 . . . 57
서버 정보 . . . 57
서버 포트 설정 . . . 58
아카이브 서버 설정 . . . 58
서버 유형 . . . 59
기타 . . . 60
알림 . . . 61
SMTP . . . 61
SNMP 서버 . . . 62
시스템로그 서버 . . . 63
고급 (알림) . . . 64
보안 . . . 65
접속 보안 . . . 65
IP/MAC 필터 . . . 65
락아웃 정책 . . . 66
로그인 문자열 . . . 67
인증서 . . . 68
개인 인증서 . . . 68
인증서 서명 요청 . . . 70
라이센스 . . . 72
USB 키로 라이센스 업그레이드 . . . 72
라이센스 파일로 라이센스 업그레이드 . . . 73
백업 및 복구 . . . 74
백업 . . . 74
복구 . . . 74

녹화 76
세컨더리 CCVSR 서버 추가. 77
네트워크 공유 폴더 추가. 78
세컨더리 CCVSR 서버 편집. 79
네트워크 공유 폴더 편집. 80
세컨더리 CCVSR/네트워크 공유 폴더 삭제. 80
옵션 – 보관 정책 80

9장. 로그

개요. 81
로그 정보. 83
로그 내보내기. 83
로그 출력. 83
옵션. 84
로그 검색. 85
일반 검색. 85
고급 로그. 85

10장. CCVSR 아카이브 서버

개요. 87
VSR 아카이브 서버 설치. 87
설치 시작. 87
아카이브 서버 GUI. 91
설정. 91
재생. 92
시작 시간/종료 시간 92
필터 검색 92
재생 선택 93
내보내기/가져오기. 94
시작 시간/종료 시간 94
장치 이름. 94
파일 검색. 95
파일 내보내기. 95
내보내기 및 삭제. 95
파일 삭제. 95
파일 가져오기. 95
저장. 96
설정. 97
라이센스. 98

부록 A

기술 지원. 99
국제. 99
북미. 99

USB 인증 키 사양. 100
호환 제품. 100
Linux 설치. 100
신뢰 인증서. 101
개요. 101
자기 서명 개인 인증서. 102
예제. 102
파일 가져오기. 102
호스트 헤더 공격에 대한 보안 강화 103
아카이브 서버에서 TLS1.0 / 1.1 비활성화 104

부록 B. 인증 키 유틸리티

개요. 105
키 상태 정보. 105
키 유틸리티. 106
키 펌웨어 업그레이드. 106
업그레이드 시작. 106
업그레이드 성공. 109
키 라이센스 업그레이드. 110
개요. 110
온라인 업그레이드. 111
업그레이드 성공. 114
오프라인 업그레이드. 115
예비 단계. 115
업그레이드 수행. 116
오프라인 업그레이드 실패. 121
요청 만료. 122

부록 C. 고급 네트워크 설정

HTTP 포트 활성화 / 비활성화 123
TLS1.0 또는 TLS1.1 비활성화 123

부록 D. CCVSR MIB 참조

개요 124
MIB 트리 구조 124
MIB 파일 다운로드 125
OID 형식 125
객체 유형 및 인덱싱 126
CCVSR 트랩 객체 128
ATEN 표준 보증 정책 144

설명서에 관하여

본 사용자 설명서는 CCVSR 시스템 시스템을 이해할 수 있도록 돕기 위해 제공됩니다. 설치, 환경 구성 및 동작을 포함한 소프트웨어의 전반적인 것을 다룹니다. 본 설명서의 개요는 다음과 같습니다.

1장, 소개, 비디오 세션 녹화 소프트웨어의 목적, 특징, 장점 및 요구 사양을 소개합니다.

2장, CCVSR 설치, 비디오 세션 녹화 소프트웨어 설치 과정을 단계별로 제공합니다.

3장, 사용자 인터페이스, 웹 브라우저를 통해 비디오 세션 녹화 소프트웨어에 로그인 하는 방법에 대해 설명합니다.

4장, 재생, 비디오 로그 파일 검색 및 재생을 위한 재생 페이지의 기능을 사용하는 방법에 대해 설명합니다.

5장, 라이브뷰, 즐겨 찾는 장치/포트, 더 많은 재생 옵션, 싱글 포트 모드 등을 포함하는 중앙 집중 라이브뷰를 설명합니다.

6장, 장치 관리, 비디오 세션 녹화 소프트웨어를 사용하여 KVM 장치를 추가하고 포트를 설정하는 방법에 대해 설명합니다.

7장, 사용자 계정, 추가 사용자 계정을 만드는 방법을 설명합니다. 사용자 또는 사용자 그룹을 수정 및 삭제하고 속성과 인증 설정을 할당합니다.

8장, 시스템, 시스템 관리 페이지를 사용하여 서버 정보를 재정의하고 알림, 보안, 라이센스, 백업 및 복구, 녹화 설정을 구성하는 방법에 대해 설명합니다.

9장, 로그, 로그 파일 유틸리티를 사용하여 비디오 세션 녹화 소프트웨어에서 발생하고 기록된 이벤트를 보는 방법을 설명합니다.

10장, CCVSR 아카이브 서버, CCVSR 아카이브 서버를 사용하는 방법과 특징 및 기능에 대해 설명합니다.

부록 A, 설명서 끝에 기술 및 문제 해결 정보를 제공합니다.

부록 B, 인증 키 유틸리티는 CCVSR 인증 키에 포함된 정보에 접근하여 업데이트하는 방법을 설명합니다.

부록 C, HTTP 포트 및 TLS 설정의 활성화 또는 비활성화 방법에 대해 설명합니다.

부록 D, 네트워크 관리 시스템과의 통합, 자동 모니터링 및 이벤트 처리에 필요한 상세 정보를

제공합니다.

주의:

- 이 설명서를 자세히 읽고 장치 또는 연결된 장치의 손상을 방지하려면 설치 및 동작 절차를 주의하여 따르십시오.
- 이 설명서가 인쇄된 이후 제품의 새로운 기능이 추가되었거나 기존 기능이 변경 또는 삭제되었을 가능성이 있습니다. 최신 사용자 설명서는 다음 사이트를 방문하여 확인하십시오. 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.

1 장

소개

개요

ATEN의 비디오 세션 녹화 소프트웨어 CCVSR은 실시간 모니터링 및 작업 역추적을 위해 설계된 혁신적이고 효과적인 솔루션입니다. 관리자는 현재 시스템에서 운영중인 운영자의 실시간 반응을 볼 수 있으므로 운영 결함, 프로세스 불일치 등을 신속하게 해결할 수 있습니다. 반면 관리자는 녹화된 운영 비디오로 규정 준수 제어 개선 및 감사 효율성에 대한 변경 사항을 추적할 수 있습니다.

라이브뷰 기능을 갖춘 CCVSR은 관리자가 여러 KVM 포트를 실시간으로 모니터링 할 수 있도록 실시간 비디오 감시를 제공합니다. 사용자가 여러 채널을 동시에 모니터링 할 수 있도록 다양한 레이아웃 조합과 사용자 지정 가능한 레이아웃을 선택할 수 있습니다. 라이브뷰 기능은 관리자가 이상 또는 긴급 상황에 적시에 대응할 수 있도록 지속적인 운영 및 시스템 성능을 실시간으로 모니터링 해야 하는 생산 라인과 같은 산업 환경에 특히 적합합니다. 또한 라이브뷰 페이지는 사용자가 문제 해결을 위해 동일한 채널의 이전 비디오를 빠르게 볼 수 있도록 재생 기능을 구현합니다.

CCVSR은 사용자가 KVM over IP 스위치 또는 시리얼 콘솔 서버를 통해 로컬 또는 원격으로 대상 서버에 접속하기 시작할 때 사용자 세션 녹화를 자동으로 시작합니다. 대상 서버의 동작 상태, 운영 체제 부팅, 로그인, 로그아웃 또는 사전 부팅 BIOS 모드에 관계없이 비디오 디스플레이, 키 입력, 마우스 클릭과 같은 모든 활동 및 작업이 기록됩니다. 또한 윈도우 클라이언트 및 자바 클라이언트를 실행하지 않고 지속적으로 녹화할 수 있습니다.

대상 컴퓨터에 에이전트 소프트웨어를 설치할 필요 없이, CCVSR은 서버로 독립적으로 설치 및 운영됩니다. 따라서 CPU, 디스크 공간, 메모리 및 네트워크 대역폭을 포함하여 모든 대상 컴퓨터에서 리소스를 할당할 필요가 없습니다. 또한 에이전트 소프트웨어를 설치하지 않는다는 것은 CCVSR이 사용자 세션 녹화를 위한 비간섭적인 방법을 제공한다는 것을 의미합니다. 서버 룸, 데이터 센터와 같은 IT 관련 환경 및 제조 공장과 같은 산업 환경에서 보안은 관리자가 가장 먼저 고려해야 할 사항 중 하나입니다. 안정적인 실시간 비디오 감시 및 비디오 세션 녹화를 제공하는 비 간섭 솔루션인 CCVSR을 구현하면 보안 문제와 사고를 모두 최소화합니다.

CCVSR은 명확하고 간결한 인터페이스, 단순화된 구조, 개선된 텍스트 가독성, 향상된 아이콘 가시성 및 시스템 알림과 같은 보조 기능을 통해 더 나은 사용자 경험과 고급 사용성을 제공하는 것을 목표로 하는 HTML5 사용자 인터페이스로 향상되었습니다. UI의 소형화한 평면 디자인 미학과 2단계의 시각적 계층 구조를 갖추고 있으며, 기능을 쉽게 설명할 수 있는 사이드 바로 그룹화하여 사용자가 작업을 원활하게 탐색하고 직관적으로 완료할 수 있습니다.

CCVSR 시스템은 확장 가능하며 단일 서버와 최대 3대의 세컨더리 서버 (녹화 저장 확장용) 설정을 지원합니다. 시스템은 서비스 중복성을 제공하기 위해 프라이머리-세컨더리 (Primary-Secondary) 아키텍처를 사용합니다. 일반 동작 중에는 세컨더리 서버 (최대 3대의 서버)가 녹화된 비디오를 저장하는 저장 서버 역할을 합니다. 또한 프라이머리 서버에 장애가 발생하면 세컨더리 서버 중 하나가 프라이머리 서버가 다시 온라인 상태가 될 때까지 KVM over-IP 스위치에 필요한 관리 및 녹화 서비스를 제공할 수 있습니다. 이 기능은 녹화 서비스가 항상 켜져 있고 중단되지 않도록 합니다. CCVSR은 비디오 녹화를 관리하고 단일 IP 포트를 통해 중앙 CCVSR 서버 (프라이머리 서버)에서 모든 관리 활동을 제어할 수 있도록 하여 관리자가 한 컴퓨터에서 모든 CCVSR 데이터에 접속할 수 있도록 합니다.

CCVSR을 KVM 설치에 통합하면 서버 룸의 보안을 자동화하고 감사에 효과적인 도구로 만들 수 있습니다.

특징

- BIOS 레벨에서 사용자가 로컬[1] 또는 원격으로 ATEN KVM over IP 스위치 및 시리얼 콘솔 서버에 접속할 때 사용자 세션을 녹화
- 다수의 KVM over IP 스위치 동작을 동시에 녹화, 스트리밍, 재생
- 고품질 비디오 녹화 지원 – 최대 4096 x 2160 해상도 지원[2]
- 비디오 녹화 세션 동안의 키 입력, 마우스 클릭, 오디오 작업 기록
- 강화된 보안을 위해 비디오 내보내기 형식 지정 및 암호 보호 기능이 포함된 전용 비디오 플레이어 제공
- 서버 또는 연결된 장치에서 수행된 작업 및 변경 사항을 직접 모니터링할 수 있도록 실시간 비디오 감시를 제공하는 라이브뷰 기능 지원[3]
- 사용자 친화적인 경험을 제공하는 HTML5 기반의 직관적인 사용자 인터페이스
- WinClient/JavaClient를 열지 않고도 지속적인 녹화 가능[4]
- IP 및 MAC 주소 필터링, 구성 가능한 로그인 실패 시도 횟수 및 계정 잠금 기능을 통해 사용자 접속 제어
- 사용자 및 그룹 권한을 구성 가능
- 브라우저를 통한 사용자 로그인을 보호하기 위해 TLS v1.2 데이터 암호화 (AES-256 bit 지원) 및 RSA 2048-bit 인증서 지원
- 포트 레벨 권한 – 사용자는 승인된 포트만 보기 가능
- 사고 조사를 위해 캡처된 세션을 쉽게 검색 가능
- 정확한 결과를 위해 시간, 포트 이름 및 사용자 이름을 사용한 고급 검색 기능 제공
- 녹화된 비디오를 로컬 하드 드라이브, 세컨더리 CCVSR 서버, 네트워크 연결 저장 장치 (NAS)에 저장하거나 아카이브 서버에 보관할 수 있는 유연성 제공
- 저장 공간 확장, 부하 분산, 서비스 장애 조치를 위해 최대 3대의 세컨더리 CCVSR 서버 지원
- 자기 서명 인증서 및 써드파티 인증 기관(CA)에서 서명한 인증서 지원
- 써드파티 원격 인증 지원: RADIUS, LDAP, LDAPS, Active Directory 지원

- ◆ 사용자 접속 권한 제어를 위한 중앙 집중식 역할 기반 (통합 관리자 및 사용자) 정책 지원
- ◆ SMTP 이메일, SNMP 트랩 및 Syslog를 통한 시스템 이벤트 알림 지원
- ◆ 장치 레벨 이벤트 기록 지원

주의: 1. 특정 모델에서만 사용 가능하므로 사양을 확인해 주십시오.

2. 4K를 지원하는 호환 가능한 KVM이 필요합니다.

3. CCVSR 서버의 권장 하드웨어 요구 사항이 충족되면 언제든지 최대 20개의 KVM 세션 (Resolution = 1920x1080, Text Mode= On, Bandwidth = 1G, Scenario = Surveillance)을 녹화 및 스트리밍 할 수 있습니다. 1대의 CCVSR로 최대 64대의 KVM 장치가 지원됩니다.

4. CN9950, CN9600, CN9000, CN8600, CN8000A, RCMDP101U, RCMDVI101, RCMVGA101, RCM101D, RCM101A만 해당됩니다.

요구 사양

컴퓨터

CCVSR이 설치될 시스템은 다음 요구 사양을 만족해야 합니다.

- 하드웨어 요구 사양
  - CPU: Intel Xeon D-1527 4 cores 2.2 GHz 또는 동급
  - 메모리: 8 GB 이상
  - 하드 드라이브 (CCVSR 용): 4 GB 이상
  - 네트워크: 1 Gbps
- 클라이언트 하드웨어 요구 사양
  - CPU: Intel Core i5-7600 4 cores 3.5 GHz 또는 동급
  - 메모리: 6 GB 이상
  - 네트워크: 1 Gbps
- 운영 체제 요구 사항
  - Windows: 10, 8, 7 또는 다음 Linux 버전

운영 체제	버전	유형	커널
Ubuntu	16.04	X86	4.10.0-28
Ubuntu	16.04	X64	4.8.0-36
Ubuntu	18.04	X64	4.19
Red Hat Enterprise Linux	7	X64	3.10.0
CentOS	7.4	X64	3.10.0-693
CentOS	7.5	X64	4.18.11-1
Debian	8.8	X64	3.16.0.4
Fedora	24	X32	4.5.5-200
Fedora	24	X64	4.5.5-200
OpenSUSE	13.2	X32	3.16.6
OpenSUSE	13.2	X64	3.16.6

- VSR 뷰어 (클라이언트 컴퓨터에서 비디오 재생을 위한 자바 기반 어플리케이션) 요구 사양:
  - JRE 8 또는 Zulu OpenJDK 8 FX (Windows 전용)

KVM over IP 스위치

비디오 세션 레코더로 저장되는 컴퓨터는 반드시 KVM over IP 스위치*의 포트에 연결되어 있어야 합니다. (CCVSR 제품 페이지에 사양 섹션 참조)

주의: 캐스케이드 연결된 KVM 스위치에 연결된 컴퓨터는 지원되지 않습니다.

브라우저

CCVSR에 로그인 하는 사용자를 위해 지원되는 브라우저는 다음과 같습니다.

브라우저	버전
Microsoft Edge	44.18362.449 이상
Internet Explorer	11.0.9600 이상
Chrome	69.0.3497.100 이상
Firefox	62.0.3 이상

대역폭 요구 사양

1920x1080, Text Mode = On, 1G 대역폭

	일반 동작 (예: 설정 환경 구성, 파일 편집 등)	감시 (예: NVR, 비디오 재생 등)
CN8000A	12.40 Mbps / Channel 1시간 비디오 크기: 599MB	32.4 Mbps / Channel 1시간 비디오 크기: 1.7GB
CN9950 (1080P)	11.1 Mbps / Channel 1시간 비디오 크기: 0.93 GB	208 Mbps / Channel 1시간 비디오 크기: 17.5 GB
CN9950 (4K)	17.2 Mbps / Channel 1시간 비디오 크기: 1.56 GB	189 Mbps / Channel 1시간 비디오 크기: 17.2 GB
KN8164V	3.37 Mbps/Channel 1시간 비디오 크기: 296MB	44.6Mbps/Channel 1시간 비디오 크기: 4GB
KG0032 (1080p)	2.2 Mbps / Channel 1시간 비디오 크기: 0.3 GB	181.4 Mbps / Channel 1시간 비디오 크기: 9.5 GB

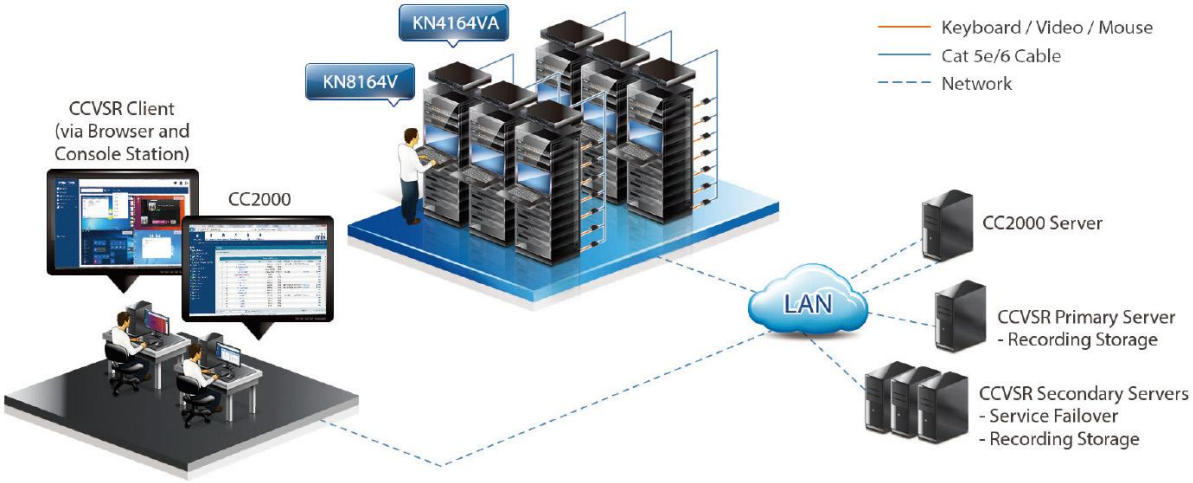
주의: 1. 위의 숫자는 참조용으로 실재 대역폭 요구 사양은 다를 수 있습니다. (예: 해상도, KVM 모델, KVM 설정, 원격 서버에서 동작 등)

2. CCVSR에서 녹화된 모든 비디오는 저장되기 전에 압축됩니다.

3. 시스템이 녹화된 비디오를 압축할 때 컴퓨터의 CPU 리소스가 사용됩니다. 압축이 완료되는 즉시 CPU 리소스는 해제됩니다.

4. CN9950의 경우, 성능 상한치에 도달하면 FPS가 낮아지기 때문에 감시 시나리오에서 4K에 필요한 대역폭이 1080P보다 낮습니다.

CCVSR 배치 예제



프라이머리 서버

관리 – 프라이머리 서버는 녹화, 보기 및 CCVSR 설비의 모든 영역을 관리하기 위해 사용되는 관리 소프트웨어입니다. 모든 세컨더리 서버, 아카이브 서버, 노드는 프라이머리 서버를 통해 동작합니다.

세컨더리 서버

저장 – 세컨더리 서버는 프라이머리 서버의 작업 부하를 줄이고 확장된 저장 공간을 제공하며, 제한된 환경 구성 기능을 가지고 있습니다.

대체 – 프라이머리 서버가 동작하지 않으면 세컨더리 서버 중 하나가 서비스 가용성을 위해 일시적으로 프라이머리 서버로 동작합니다.

아카이브 서버

보관 – 아카이브 서버는 백업 및 보기를 위해 프라이머리 서버에서 제작된 모든 비디오 로그 파일을 따로 정리된 데이터베이스에 자동으로 보관합니다. 아카이브 서버는 VSR 시스템으로부터 분리된 대형 데이터베이스에 불러오기, 내보내기, 할당을 수행하도록 합니다.

프라이머리, 세컨더리 및 아카이브 서버에서 지원되는 기능은 다음 테이블을 참조하십시오.

기능	프라이머리	세컨더리 (저장)	세컨더리 (대체)	아카이브
시스템 관리	✓		보기만 허용	
장치 관리	✓		보기만 허용	
사용자 관리	✓		보기만 허용	
로컬 관리	✓	✓	✓	
비디오 및 키 입력 녹화	✓	✓	✓	
비디오 검색 및 재생	✓		✓	✓
비디오 및 키 입력 백업				✓

노드

KVM 포트 – 노드는 KVM Over IP 스위치에 있는 물리적 포트입니다. 비디오 로그를 저장하려는 각 노드는 라이센스가 필요합니다.

라이센스

CCVSR 라이센스는 CCVSR 서버 설비에 사용하도록 허용된 수많은 프라이머리, 세컨더리 서버, 아카이브 서버 및 노드를 제어합니다. 라이센스 정보는 CCVSR 패키지에 있는 USB 라이센스 키에 포함되어 있습니다. 배치 예제에 대한 세부 사항은 10페이지 노드 옵션을 참조하십시오.
CCVSR 소프트웨어 설치가 완료된 후, 사용자가 구매한 숫자의 라이센스가 자동으로 추가됩니다. 더 많은 라이센스를 추가하려면, 라이센스를 업그레이드해야 합니다. 세부 정보는 72페이지 라이센스를 참조하십시오.

라이센스 옵션

라이센스	노드	프라이머리 서버
CCVSR8	8	1
CCVSR16	16	1
CCVSR32	32	1
CCVSR64	64	1
CCVSR128	128	1
CCVSR256	256	1
CCVSR512	512	1
CCVSR1024	1024	1
CCVSR2048	2048	1

노드 옵션

라이센스	노드
CCVSRN1	1
CCVSRN8	8
CCVSRN16	16
CCVSRN32	32
CCVSRN64	64
CCVSRN128	128
CCVSRN256	256
CCVSRN512	512
CCVSRN1024	1024
CCVSRN2048	2048

아카이브 서버 옵션

라이센스	서버
CCVSRAS1	1

2 장

CCVSR 설치

개요

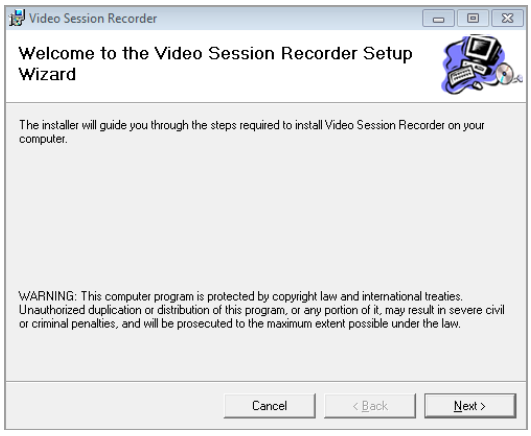
이 장은 비디오 세션 녹화 소프트웨어 (CCVSR)를 설치하는 방법을 설명합니다. CCVSR 어플리케이션은 비디오 세션 녹화 소프트웨어가 동작하기 위해 백그라운드 서비스를 운영하며 기본 서버 환경 구성을 위해 사용됩니다. CCVSR 어플리케이션은 비디오 세션 녹화 소프트웨어의 웹 브라우저 기능을 수행하기 위해 반드시 동작 중이어야 합니다. Linux에 CCVSR 소프트웨어를 설치하려면 100페이지 Linux 설치를 참조하십시오.

CCVSR 소프트웨어 설치

설치 시작

Windows 시스템에 CCVSR 어플리케이션을 설치하려면, 다음을 수행하십시오.

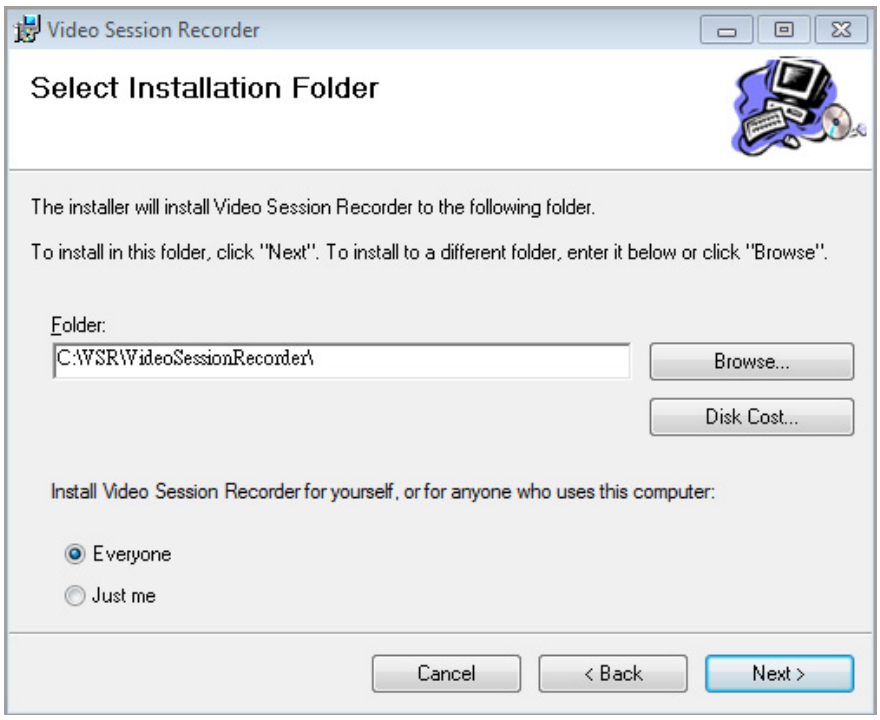
1. 패키지에 포함된 소프트웨어 CD를 컴퓨터의 CD ROM 드라이브에 삽입하십시오.
2. setup.exe 파일이 위치한 폴더로 가서, 파일을 실행하십시오. 아래와 비슷한 화면이 나타납니다.



Next를 클릭하여 다음으로 진행하십시오.

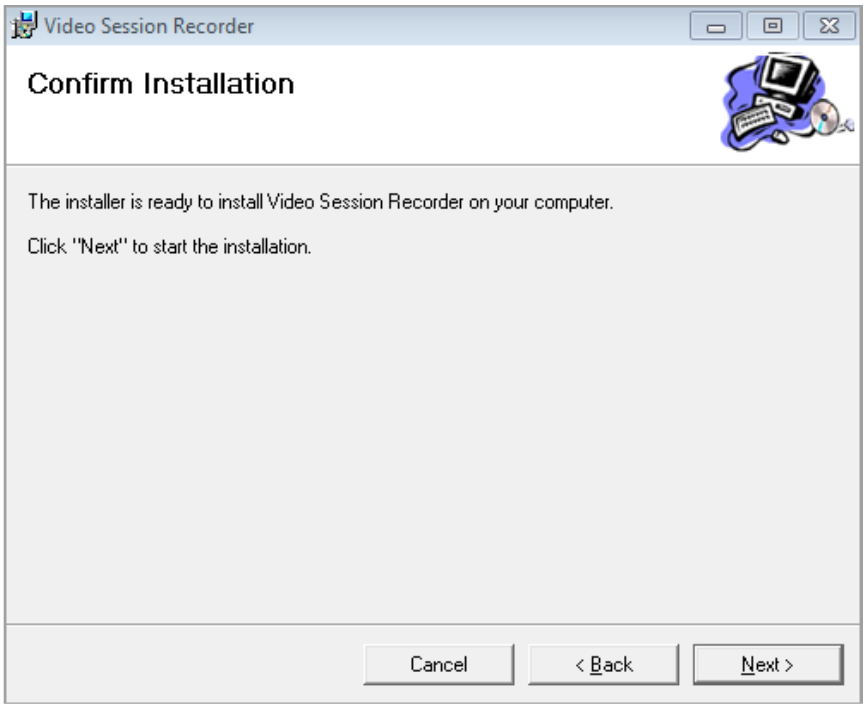
3. Select Installation Folder 페이지에서, 설치 폴더를 설정하거나 혹은 **Browse**를 클릭하여 설치하려는 위치를 선택하십시오. 그 후 사용자 본인만을 위해 사용할 것인지(**Just me**) 혹은

이 컴퓨터를 사용하는 모두를 위해 사용할 것인지 (**Everyone**) 선택하십시오. **Disk Cost**를 클릭하면 설치 가능한 드라이브와 사용 가능 용량이 표시됩니다.

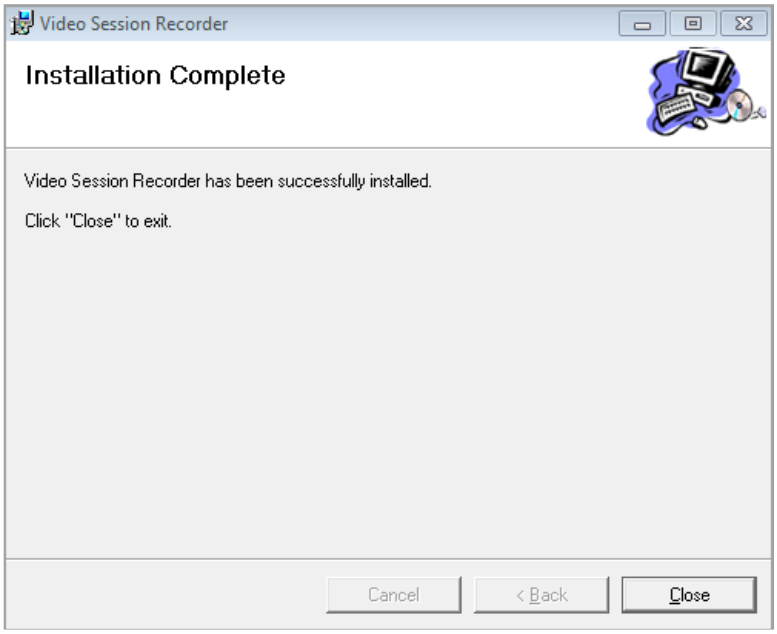


Next를 클릭하여 계속 진행하십시오.

4. Confirm Installation 윈도우가 나타나면, **Next**를 클릭하여 다음으로 진행하십시오.



5. 설치가 완료되면 다음 메시지가 나타납니다.



라이센스

CCVSR 소프트웨어 설치가 완료되면, 1대의 서버를 위한 기본 라이센스가 자동으로 제공됩니다. 더 많은 비디오 세션 레코더를 추가하려면, 라이센스를 업그레이드해야 합니다. 라이센스를 업그레이드하기 위한 세부 사항은 72페이지 라이센스를 참조하십시오. 라이센스 옵션을 위한 세부 사항은 10페이지 노드 옵션을 참조하십시오.

3 장

사용자 인터페이스

개요

비디오 세션 녹화 소프트웨어의 사용자 인터페이스는 웹 브라우저에 의해 접근할 수 있으며 주요 기능들을 포함하고 있습니다. 이 장은 비디오 세션 녹화 소프트웨어에 로그인 하는 방법 및 브라우저 구성 요소를 설명합니다.

브라우저 로그인

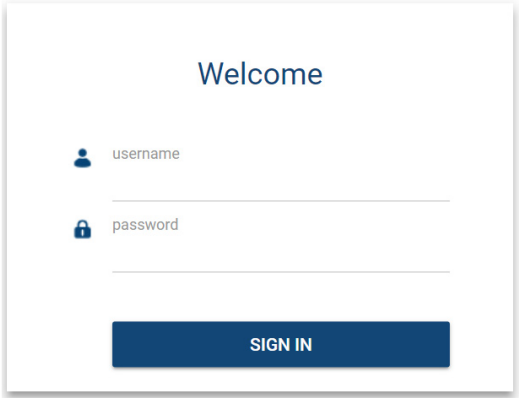
비디오 세션 녹화 소프트웨어는 모든 플랫폼에서 동작하는 인터넷 브라우저를 통해 접근할 수 있습니다. 비디오 세션 녹화 소프트웨어의 브라우저 인터페이스에 접근하려면, 반드시 CCVSR 어플리케이션이 실행되어야 합니다.

비디오 세션 레코더에 접근하려면 다음을 수행하십시오.

1. 브라우저를 열고 브라우저의 위치 바에 접근하려는 비디오 세션 레코더의 IP 주소 및 서비스 포트를 입력하십시오.

   예제: https:₩₩192.168.0.100:9443

2. 보안 경고 대화 상자가 나타나면 인증서를 수락하십시오 - 이것은 신뢰될 수 있습니다. 두 번째 인증서가 나타나면 그것도 수락하십시오. (101페이지 신뢰 인증서 참조)
   일단 인증서를 수락하면 로그인 페이지가 나타납니다.



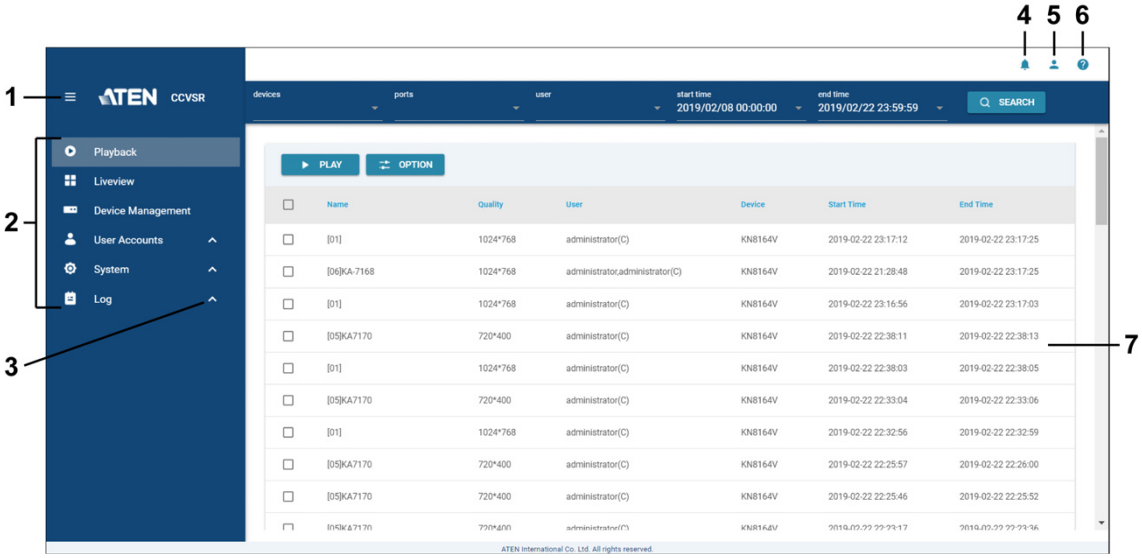
3. 사용자 이름과 암호를 입력하고 **Login**을 클릭하면 웹 메인 페이지를 불러옵니다.

주의: 처음 로그인한 경우, 기본 사용자 이름 (administrator) 및 기본 암호 (password)를 사용하십시오.

4. 처음 로그인하는 경우 시스템에서 암호를 변경하라는 메시지를 표시합니다.

웹 브라우저 메인 페이지

사용자가 로그인 및 인증을 받았으면, Playback (재생) 페이지와 함께 웹 브라우저 메인 페이지가 나타납니다.



주의: 이 화면은 통합 관리자의 페이지입니다. 사용자의 타입 및 권한에 따라 모든 아이템이 나타나지 않을 수 있습니다.

페이지 구성

웹 페이지 화면 구성 요소는 아래 테이블에 있습니다.

번호	항목	설명
1	메인 메뉴 확장/축소	이 아이콘을 클릭하여 기본 메뉴를 확장하거나 축소합니다. 하위 메뉴는 주요 작업 범주를 클릭하여 접속할 수 있습니다.

번호	항목	설명
2	메인 메뉴	메인 메뉴에는 비디오 세션 녹화 소프트웨어의 주요 작업 범주가 있습니다. 여기에 표시되는 항목은 사용자 유형 및 사용자 계정을 만들 때 선택한 인증 옵션에 따라 결정됩니다.
3	서브 메뉴 확장/축소	위/아래 화살표는 작업 범주를 하위 메뉴로 확장하거나 축소할 수 있음을 나타냅니다. 작업 범주를 클릭하여 주 메뉴의 작업 하위 범주를 포함하는 하위 메뉴로 확장/축소합니다. 여기에 표시되는 항목은 사용자 유형 및 사용자 계정을 만들 때 선택한 인증 옵션에 따라 결정됩니다.
4	알림/메시지 센터 (통합 관리자 전용)	시스템의 알림/메시지를 위해 이 아이콘을 클릭합니다. 최대 50개의 알림이 표시될 수 있습니다. (스크롤 바를 사용하여 알림을 스크롤) 읽지 않은 알림이 있으면, 알림 아이콘 위에 숫자가 표시됩니다. 예:  **CLEAR ALL**을 클릭하면 알림/메시지를 삭제합니다. **VIEW LOGS**를 클릭하면 시스템 로그 페이지로 이동합니다.
5	개인	개인 정보 및 환경 구성을 위해 이 아이콘을 클릭합니다. ◆ 표시되는 정보에는 사용자의 사용자 이름과 사용자가 마지막으로 시스템에 로그인 한 시간이 포함됩니다. ◆ 기본 설정: 클릭하면 개인 기본 설정을 구성합니다. ◆ 비밀번호 변경: 클릭하면 비밀번호를 변경합니다. 클릭합니다. ◆ 로그아웃: 클릭하면 현재 세션에서 사용자가 로그아웃 됩니다. 자세한 내용은 18페이지 개인 환경 구성을 참조하십시오.
6	도움말	온라인 도움말 (**Online help**) 또는 정보 (**About**)용 버튼을 클릭합니다. **Online help**을 클릭하면 온라인 사용 설명서로 이동합니다. **About**를 클릭하면 현재 펌웨어 버전이 표시됩니다.
7	대화형 디스플레이 패널	주요 작업 공간입니다. 나타나 있는 화면은 사용자의 메뉴 선택을 반영합니다.

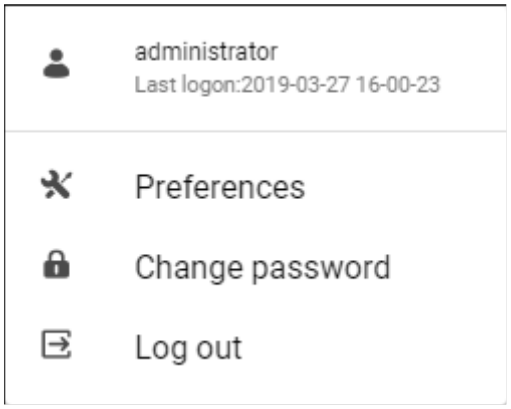
메인 메뉴

메인 메뉴는 사용자 유형 (통합 관리자, 관리자, 사용자) 및 권한 (사용자 계정이 생성될 때 할당됨)에 따라 다르게 표시됩니다. 기능은 아래 테이블에서 설명합니다.

동작 아이템	기능
Playback (재생)	재생 페이지는 이용 가능한 비디오 로그를 검색 및 재생하고 현재 브라우저 세션을 모니터링 하는데 사용됩니다. 재생은 20페이지에서 설명합니다.
Liveview (라이브뷰)	라이브뷰 페이지는 사용자가 실시간 KVM 포트 반응을 볼 수 있도록 합니다. 라이브뷰는 32페이지에서 설명합니다.
Device Management (장치 관리)	장치 관리 페이지는 비디오 로그를 녹화하기 위해 KVM 장치를 추가하거나 포트를 설정하는데 사용됩니다. 이 페이지는 통합 관리자 및 장치 관리 권한을 가진 관리자가 사용할 수 있습니다. 다른 관리자와 사용자에게는 나타나지 않습니다. 장치 관리는 38페이지에서 설명합니다.
User Accounts (사용자 계정)	사용자 계정 페이지는 사용자와 그룹을 생성하고 관리하는데 사용됩니다. 또한 장치들을 사용자와 그룹에 할당할 수 있습니다. 이 페이지는 통합 관리자 및 사용자 관리 권한을 가진 관리자가 사용할 수 있습니다. 다른 관리자와 사용자에게는 나타나지 않습니다. 사용자 관리는 44페이지에서 설명합니다.
System (시스템)	시스템 페이지는 비디오 세션 녹화 소프트웨어의 시스템 설정을 구성하고 네트워크에 세컨더리 서버를 추가하기 위해 사용됩니다. 시스템 관리는 56페이지에서 설명합니다.
Log (로그)	로그 페이지는 로그 파일 내용을 표시합니다. 로그 페이지는 81페이지에서 설명합니다.

개인 정보 / 환경 구성

Personal 아이콘 ( )을 클릭하면 페이지 오른쪽 상단에서 개인 정보 및 구성을 볼 수 있습니다.

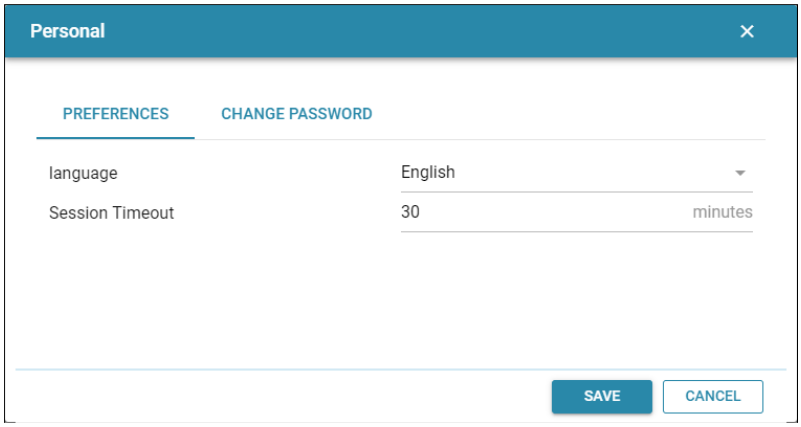


- 상단 섹션에는 사용자의 사용자 이름과 사용자가 마지막으로 시스템에 로그인한 시간을 포함한 정보가 표시됩니다.
- Preferences: 클릭하면 개인 기본 설정을 구성합니다.
- Change password: 클릭하면 비밀번호를 변경합니다.
- Log out: 클릭하면 이 사용자의 현재 세션에서 로그아웃합니다.

개인 환경 구성

기본 설정

Preference를 클릭하면 아래와 같은 팝업 윈도우가 나타납니다.



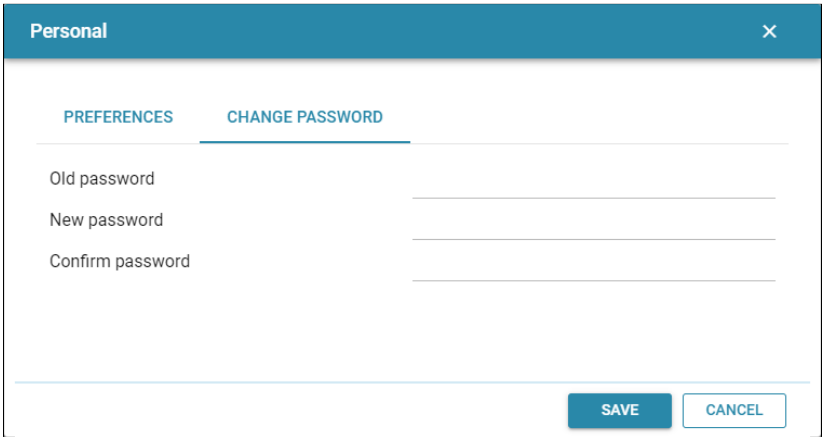
Language: 드롭 다운 메뉴를 클릭하여 원하는 언어를 선택합니다.

Session Timeout: 사용자가 시스템에 로그인 상태를 유지할 수 있는 시간 값을 입력합니다. 수동으로 로그아웃 할 때까지 시스템 로그인 상태를 유지하려면 **0**을 입력하십시오.

Save를 클릭하면 변경 사항이 저장됩니다.

암호 변경

Change Password를 클릭하면 아래와 같은 팝업 윈도우가 나타납니다.



이전 암호, 새 암호 및 새 암호를 다시 입력합니다.
Save를 클릭하면 변경 사항이 저장됩니다.

로그아웃

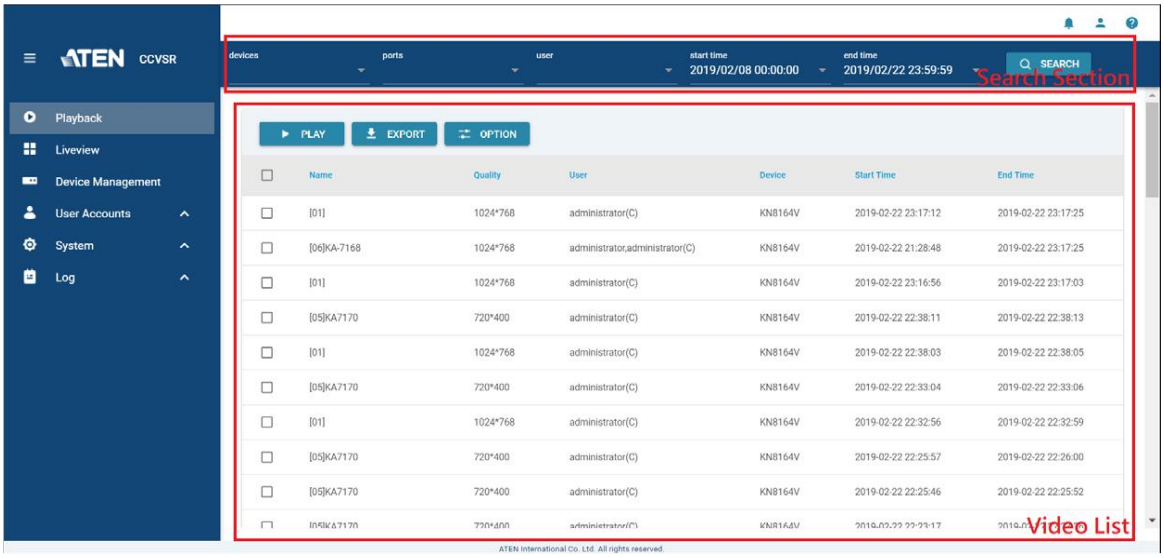
Log out을 클릭하면 시스템에서 로그아웃 합니다.

4 장

재생

개요

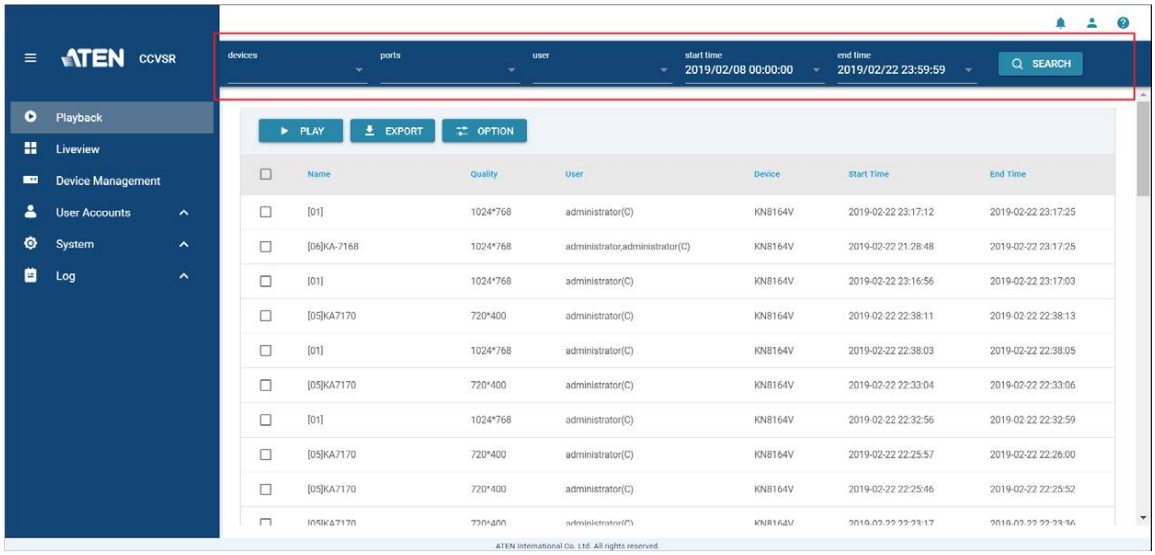
Playback 페이지는 비디오 로그 파일을 검색 및 재생하는데 사용됩니다. 재생 기능을 사용하기 전에 먼저 KVM 장치를 추가해야 합니다. 세부 사항은 39페이지 KVM 포트 녹화를 참조하십시오.
비디오 세션 녹화 소프트웨어에 로그인 하면 자동으로 이 페이지를 불러옵니다.
이 페이지 상단에 검색 섹션은 비디오 로그를 빠르게 검색하는 필터 역할을 합니다.
검색 섹션 아래에는 녹화된 비디오 로그를 가진 포트를 표시하는 비디오 목록 섹션이 있습니다.



목록을 스크롤하여 원하는 비디오 로그를 검색합니다. 또한 항목 (포트) 이름, (비디오) 품질, 사용자, 장치 및 시간을 클릭하여 목록을 알파벳 순서, 최고에서 최저로 품질 등으로 정렬하여 원하는 비디오 로그를 찾을 수 있습니다.

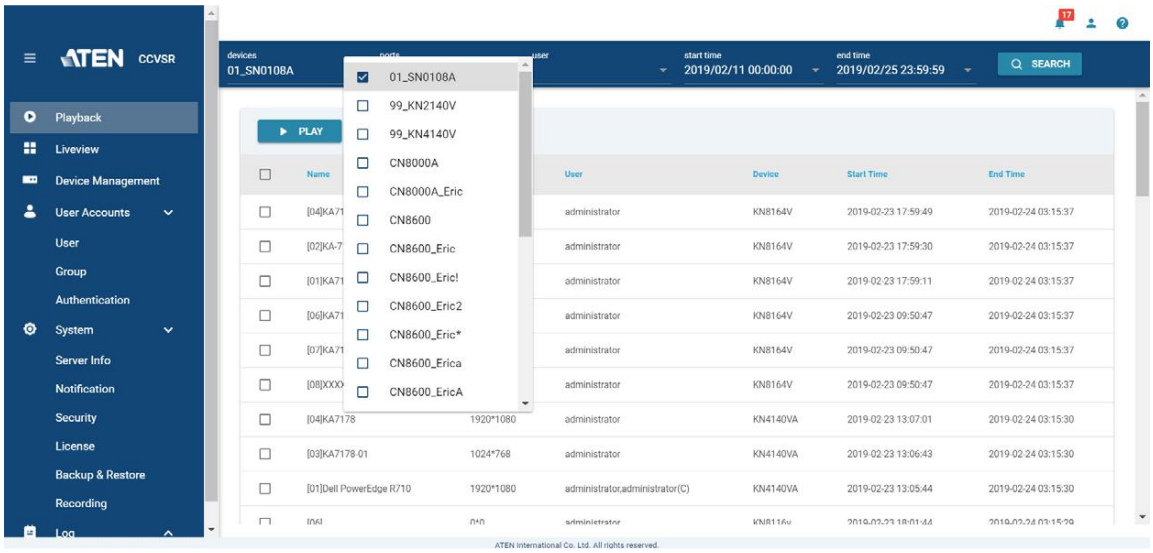
비디오 기록 검색 기준

이 페이지 상단에 검색 섹션이 표시됩니다.



검색 기능은 장치 이름, 포트 이름, 사용자, 시작 시간 또는 종료 시간, 포트 이름 범주를 필터링하여 비디오 로그를 찾는데 사용됩니다. 시작 시간 및 종료 시간은 녹화가 발생한 시간을 나타냅니다.

비디오 목록을 필터링하려면 1) 정보를 입력하여 입력하거나 2) 드롭 다운 메뉴를 클릭하고 항목을 확인한 다음 검색을 클릭하여 범주를 채우십시오. 드롭 다운 메뉴에서 항목을 확인하는 예가 표시됩니다.



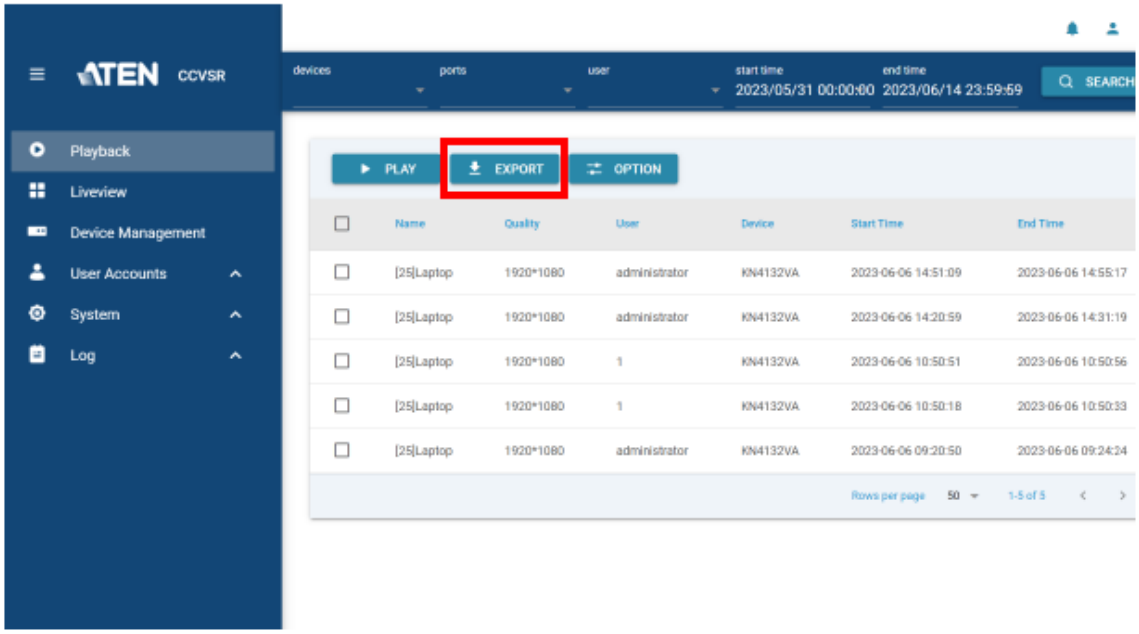
필터를 제거하려면 선택한 항목을 선택 취소하고 **Search**을 다시 클릭하십시오.

비디오 기록 재생

비디오 로그를 재생하려면, Video List에서 비디오 로그를 선택한 후, Play 버튼을 클릭합니다. 비디오는 비디오 로그 뷰어 어플리케이션에서 새로운 윈도우로 열립니다. 비디오 로그 뷰어에 대한 정보는 24페이지 VSR 뷰어를 참조하십시오.

비디오 기록 내보내기

비디오 로그를 .264 포맷으로 내보내면 VLC와 같은 지원되는 플레이어로 재생할 수 있습니다. 단, 이 기능은 CCVSR Windows 버전에서만 사용 가능하며, 내보낸 비디오에는 오디오, 키 입력 및 마우스 클릭 작업이 포함되지 않습니다.



비디오 기록 내보내기

1. **Playback** 페이지로 이동하십시오.
2. 비디오 로그 목록에서 내보내고자 하는 비디오를 클릭해 선택하십시오. 특정 비디오 로그를 검색하려면 검색 기능을 사용하십시오.
3. **EXPORT**를 클릭하십시오.

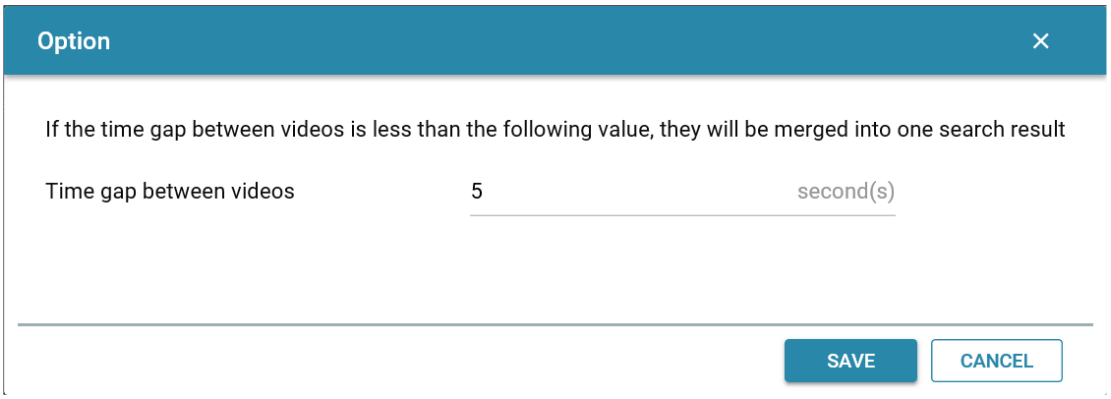
주의: 파일 크기에 따라 비디오 내보내기 완료에 시간이 걸릴 수 있습니다.

내보낸 비디오 기록 재생

내보낸 비디오 파일이 2개 이상의 파일로 분할될 수 있으므로, 모든 비디오를 선택하여 VLC 미디어 플레이어에 추가하면 자동으로 재생됩니다.

시간 간격 옵션

시간 간격 설정을 위해 Option을 클릭합니다.



이 설정은 두 비디오 간의 시간 간격이 구성된 값보다 작을 경우 비디오 클립을 병합하여 비디오 검색 결과의 범위를 좁히는데 도움이 됩니다.

예를 들어, 다음 비디오 클립이 있고 시간 간격이 2분인 경우:

비디오 #1: 15:59:06 - 15:59:35

비디오 #2: 16:00:12 - 16:10:12

비디오 #3: 16:18:29 - 16:19:25

검색 결과는 다음과 같습니다.

비디오 #1: 15:59:06 - 16:10:12

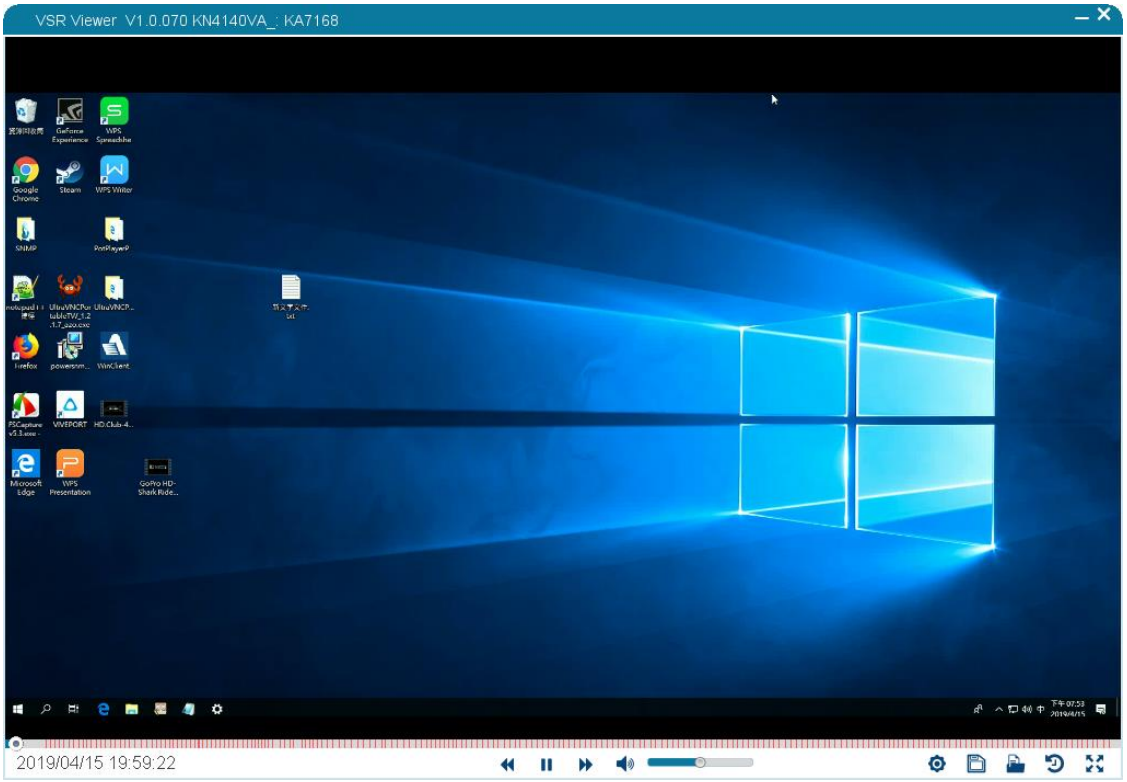
비디오 #2: 16:18:29 - 16:19:25

0 ~ 3600초 사이의 값을 입력합니다. 기본값은 5초입니다.

VSR 뷰어

VSR 뷰어는 재생을 위해 비디오 로그 파일 (.vls)을 실행할 때 팝업 되는 내장 비디오 플레이어입니다. * VSR 뷰어는 비디오 세션 녹화 소프트웨어의 웹 세션에서 또는 저장된 디렉토리에서 직접 비디오 로그를 보기 위해 자동으로 사용됩니다. VSR 뷰어의 재생 도구는 아래에서 설명합니다.

비디오 로그를 재생하면 VSR 뷰어가 팝업 되고 아래와 유사한 화면이 나타납니다.



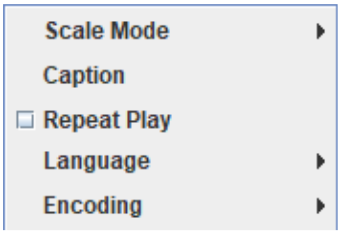
주의:

- VSR Viewer는 JRE 8 또는 Zulu OpenJDK 8 FX (Windows 전용)를 실행해야 하는 Java 기반 응용 프로그램입니다.
- 32bit Java VM의 경우 전체 화면 모드에 대한 최대 뷰어 크기 지원은 3300 * 2048입니다.
- 64bit Java VM의 경우 전체 화면 모드에 대한 최대 뷰어 크기 지원은 5130 * 2160입니다.

툴바

툴바는 비디오 아래에 나타나며 비디오에 관한 정보를 제공하고 재생 기능을 제어합니다. 툴바는 3초간 마우스 동작이 없으면 사라집니다. 다시 툴바를 보려면 마우스를 움직이기만 하면 됩니다. 툴바 기능은 아래에서 설명합니다.

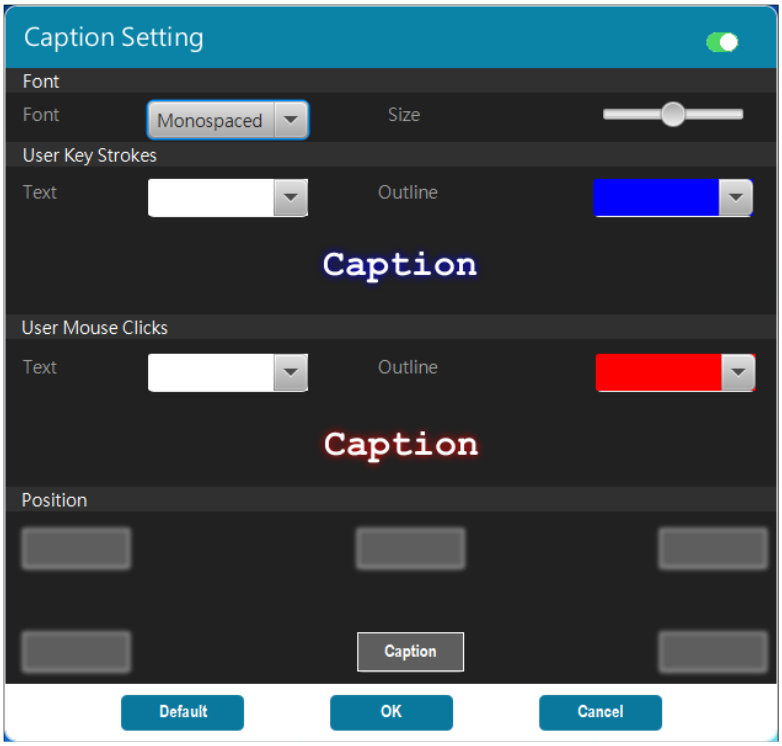
아이콘	기능
	**재생**: Play 버튼은 정지된 비디오 로그를 다시 재생하기 위해 사용됩니다.
	**정지**: Pause 버튼은 재생중인 비디오 로그를 정지하기 위해 사용됩니다.
	**빠르게**: Faster 버튼은 비디오 로그 재생 속도를 빠르게 하는데 사용됩니다. 기본 재생 속도의 2배, 4배, 8배로 속도를 변경할 수 있습니다.
	**느리게**: Slower 버튼은 비디오 로그 재생 속도를 느리게 하는데 사용됩니다. 기본 재생 속도의 1/2배, 1/4배, 1/8배로 속도를 변경할 수 있습니다.
	**볼륨**: 볼륨 막대를 사용하여 볼륨을 조정합니다. 스피커 아이콘을 클릭하면 비디오를 음소거 / 음소거 해제 합니다.
	**진행 바**: Progress bar는 비디오 로그를 얼마만큼 보고 있는지 알려줍니다. 모두 보기 기능을 사용하여 다수의 비디오 로그를 볼 때, 진행 바의 빨간색 라인은 비디오 로그의 끝을 의미하고 다음 비디오 로그의 시작을 의미합니다. 진행 바의 아무 곳이나 마우스로 이동하면 언제 비디오 로그가 생성되었는지 시간 및 날짜 팝업이 나타나 알려줍니다. 이는 빠르게 원하는 위치로 이동할 수 있도록 합니다. 진행 버튼을 클릭하고 드래그 하여 앞뒤로 이동하거나, 특정 위치의 진행 바를 클릭하여 원하는 비디오 위치로 갈 수 있습니다.
	**윈도우 크기 조절**: 오른쪽 아래 구석에 클릭 후 드래그하여 윈도우 크기를 조절할 수 있습니다. 윈도우 크기 조절 후 비디오 화면이 맞지 않는 경우, Scale Mode 기능을 사용하여 비디오 크기를 조절할 수 있습니다. (아래 스케일 모드 참조) **주의:** 크기 조절된 윈도우 영역 바깥에 회색 윈도우 프레임에 아무 곳이나 마우스 왼쪽 버튼을 클릭한 상태로 마우스를 움직여 전체 윈도우를 화면 내에서 이동할 수 있습니다.

아이콘	기능
	**설정**  **스케일 모드**: Scale Mode 아이콘은 비디오 로그 뷰어의 윈도우에 비디오 디스플레이 크기를 변경하도록 합니다. 스케일 모드 아이콘을 클릭할 때 3가지 선택 사항이 나타납니다. ◆ Keep Video Size: 기본 크기대로 비디오 화면을 유지합니다. ◆ Keep Video Ratio: 크기 조절된 윈도우에 맞게 비디오 화면을 조절합니다. ◆ Scale Video to Window: 전체 윈도우 크기로 비디오 화면을 조절합니다. **Caption**: 자막 설정을 편집할 수 있습니다. 자세한 내용은 27페이지의 자막을 참조하십시오. **Repeat Play**: 클릭하면 이 비디오 로그의 반복 재생을 활성화/비활성화합니다. 체크하면 반복 재생이 활성화됩니다. **Language**: 선호하는 언어를 선택할 수 있습니다. **Encoding**: 컨텐츠가 깨질 경우 인코딩 방법을 선택할 수 있습니다.
	**비디오 저장**: Save Video 아이콘은 폴더로 현재 비디오 로그를 저장하고 암호로 보호합니다. 비디오 로그를 저장하려면, **Save Video**를 클릭하고, 폴더를 선택하고, 파일 이름을 설정한 후 **Save**를 클릭합니다. Save 클릭 후 Set Password 윈도우가 나타나면, 비디오 로그 파일에 대한 암호를 입력하거나, 암호가 필요하지 않은 경우 입력하지 않고 **OK**를 클릭합니다. 비디오는 .vls 포맷으로 저장됩니다. 비디오를 열려면 28페이지의 비디오 로그 파일 열기를 참조하십시오. **주의:** Set Password에서 Cancel을 클릭하면 저장 과정을 중지하고 파일이 저장되지 않습니다.
	**비디오 열기**: 이 아이콘은 이전에 저장된 비디오 파일을 여는데 사용됩니다. 아이콘을 클릭하여 비디오 로그 파일을 선택하고 암호를 입력합니다.
	**컨트롤 패널**: Control Panel은 비디오 이미지 외에 비디오를 재생할 때 동작(마우스 클릭 및 키 입력), 사용자 이름, 컴퓨터에 로그인한 사람의 IP 주소를 실행한 시간에 맞게 정렬하여 보여줍니다. KVM 포트에 여러 사용자가 로그인 한 경우, 제어 패널은 사용자들을 표시하며 누가 각 동작을 실행했는지 보여줍니다. 아이콘을 클릭하면 제어 패널 윈도우를 불러오며, 왼쪽 위 구석에 있는 핀 아이콘을 사용하여 열려 있는 윈도우를 고정/이동할 수 있습니다. User List는 비디오 로그가 저장될 때 KVM 포트에 로그인한 사용자를 표시합니다.

아이콘	기능
	**전체 화면**: 이 아이콘은 비디오 로그 뷰어 윈도우를 전체 화면에 맞게 확장합니다. 전체 화면 모드를 종료하려면, Full Screen 아이콘을 다시 한번 클릭합니다.

자막

이 옵션을 클릭하면 아래와 같은 설정 메뉴가 나타납니다.



설정	설명
Caption Setting	on/off 스위치 (메뉴 윈도우 우측 상단)을 클릭하여 자막 기능을 켜기/끄기 합니다.
Font	
Font	자막 폰트를 선택합니다.
Size	자막 크기를 슬라이더를 드래그하여 조절합니다.
User Key Stroke	
Text	드롭다운 메뉴를 클릭하여 키 입력의 폰트 색상을 선택합니다.
Outline	드롭다운 메뉴를 클릭하여 키 입력의 폰트 아웃라인 색상을 선택합니다.
User Mouse Clicks	
Text	드롭다운 메뉴를 클릭하여 마우스 클릭의 폰트 색상을 선택합니다.
Outline	드롭다운 메뉴를 클릭하여 마우스 클릭의 폰트 아웃라인 색상을 선택합니다.

설정	설명
Position	6개의 위치 박스 중 하나를 클릭하여 자막을 배치할 위치를 선택합니다.
Default	이 버튼을 클릭하여 기본 설정으로 리셋합니다.

비디오 기록 파일 열기

CCVSR 접속 권한이 없는 컴퓨터에서 비디오 로그 파일을 재생하려면 아래 단계를 수행하십시오.

1. 비디오 로그 파일을 저장하십시오.
2. CCVSR이있는 컴퓨터에서 JavaVLS.jar를 저장하십시오. (일반적으로 C:₩VSR₩VideoSessionRecorder₩webroot_rls 폴더)
3. CCVSR 접속 권한이 없는 컴퓨터에 비디오 로그 파일과 JavaVLS.jar를 제공합니다.
4. 해당 컴퓨터에서 VSR 뷰어용 JavaVLS.jar을 여십시오.
5. 비디오 열기 아이콘  을 클릭하고 비디오를 재생할 비디오 로그 파일을 선택하십시오.

비디오 가져오기

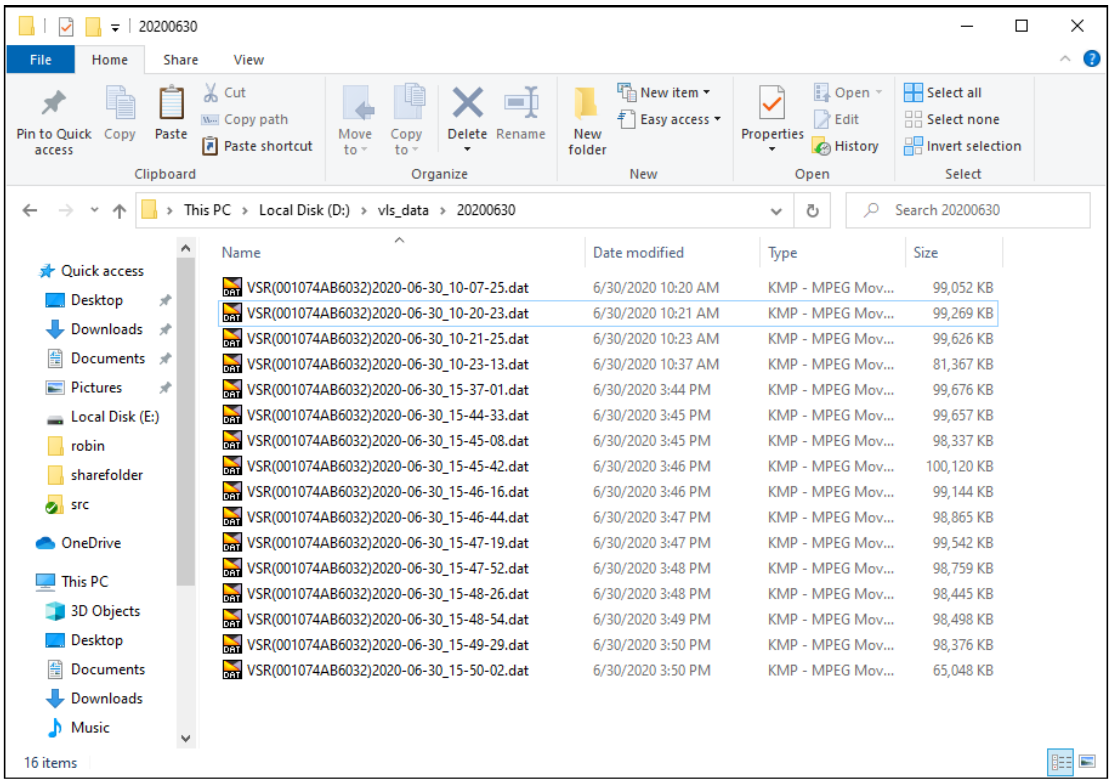
VSR을 사용하면 다른 VSR 서버에서 비디오 로그 파일을 가져올 수 있습니다. 녹화된 비디오는 일반적으로 "vls_data"라는 디렉토리에 * .dat 파일로 저장됩니다. 이 디렉토리는 System > Recording (76페이지 녹화 참조)의 환경 구성에서 로컬 드라이브 또는 네트워크 폴더에 있을 수 있습니다.

다음은 몇 가지 예입니다.

C:₩vls_data (로컬 드라이브 C:₩)

D:₩vls_data (로컬 드라이브 D:₩)

₩₩10.0.8.168₩sharerecording₩vls_data (네트워크 폴더)



VSR 서버로 작동중인 컴퓨터에서 저장된 파일을 불러오려면 다음을 따라하십시오:

1. CCVSR 서비스를 중지하십시오.
2. CCVSR 서버에서 명령어 라인 인터페이스를 실행하십시오.
3. 불러오는 소스에 맞게 비디오 로그 파일 (.dat)을 불러오는 관련 명령어를 사용하십시오.

플랫폼	명령어 구문 & 예시
로컬 하드 디스크에서 불러오기	
Windows	**명령어 구문:** vsrImport <DB Destination> <Source Path for VSR Data file> <OP Code> [Destination path] **예시:** vsrImport C:₩VSR₩videosessionrecorder₩VSR80.db E:₩backup₩vls_data 0 D:₩
Linux	**명령어 구문:** sudo <DB Destination> <Source Path for VSR Data file> <OP Code> [Destination path] Example: **예시:** sudo /usr/local/bin/ccvsr/vsrImport /usr/local/bin/ ccvsr/VSR80.db /home/user1/backup/vls_data 0 /var
NAS 서버에서 불러오기	
Windows	**명령어 구문:** vsrImport <DB Destination> <NAS Path> <OP Code> <username> <password> **예시:** vsrImport C:₩VSR₩videosessionrecorder₩VSR80.db ₩₩10.0.90.123₩Volume1/NASROOT 2 nasuser1 password
Linux	**명령어 구문:** sudo <DB Destination> <NAS Path> <OP Code> <username> <password> **예시:** sudo /usr/local/bin/ccvsr/vsrImport /usr/local/bin/ ccvsr/VSR80.db //10.0.90.123/Volume1/NASROOT 2 nasuser1 password

각 매개변수에 대한 자세한 내용은 아래 표를 참조하십시오.

매개변수	설명
DB Destination	CCVSR 데이터베이스 파일이 저장되는 위치입니다.
Source Path for VSR Data file	VSR 파일 (녹화 파일)을 가져올 경로입니다.
Operation Code (OP Code)	로컬 디스크에서 파일을 가져오려면 **0**을 사용하고, NAS 서버에서 파일을 가져오려면 **2**를 사용합니다.
Destination Path	이 매개변수를 사용하여 VSR 파일(녹화 파일)의 복사본을 지정된 경로에 저장할 수 있습니다. 이 매개변수는 이동식 디스크와 같이 소스에 CCVSR이 일시적으로만 접근할 수 있는 경우에 유용합니다.

4. CCVSR 서비스를 시작하십시오.

   파일을 가져온 후, 비디오 로그가 재생 탭의 **Search Results (검색 결과)** 윈도우에 나타납니다.

5 장

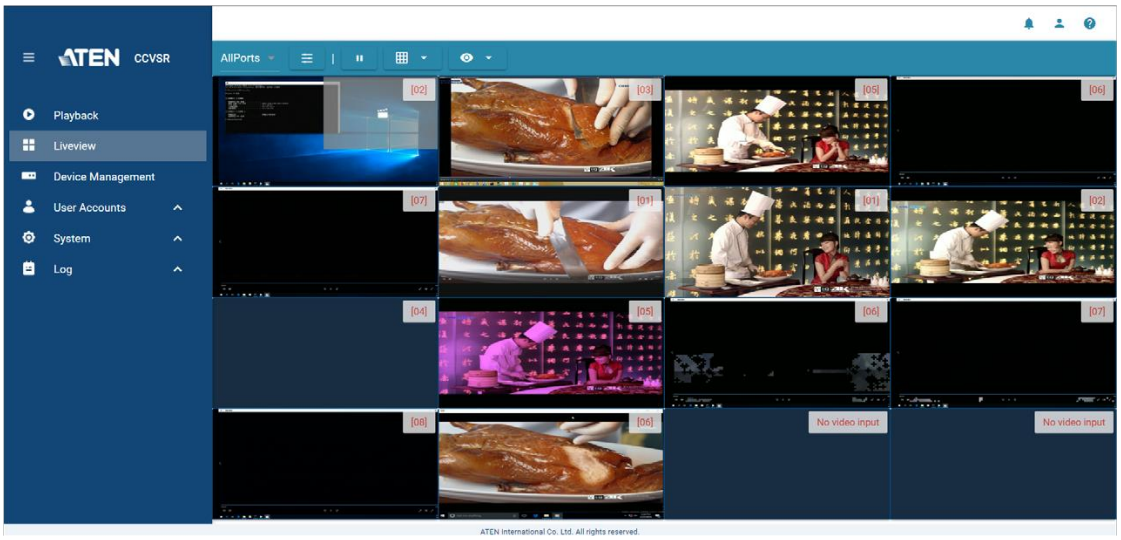
라이브뷰

개요

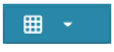
Liveview 페이지는 사용자가 특정 포트 그룹의 중앙 집중 라이브뷰를 갖거나 라이브뷰 디스플레이용 특정 포트를 선택할 수 있도록 합니다.

라이브뷰 페이지 접속

1. CCVSR GUI에 로그인 하십시오.
2. 왼쪽 패널에서 **Liveview**를 클릭하십시오. 아래 페이지가 나타납니다.



3. 표시되는 포트를 변경하려면 

을 클릭하고 드롭다운 목록에서 선택하십시오. 즐겨찾기를 생성하여 여기에 더 많은 옵션을 추가할 수 있습니다. 자세한 내용은 33페이지의 표시 목록을 참조하십시오.
4. 라이브뷰 레이아웃을 변경하려면 
을 크릭하고 드롭다운 목록에서 클릭하여 선택하십시오.
5. 녹화 중인 포트만 표시하거나 연결된 모든 포트를 표시하도록 전환하려면, 
을 클릭하십시오.
   - **All:** 선택한 그룹 (즐겨찾기)에 대해 연결된 모든 포트를 표시하려면 이 옵션을 선택하십시오.

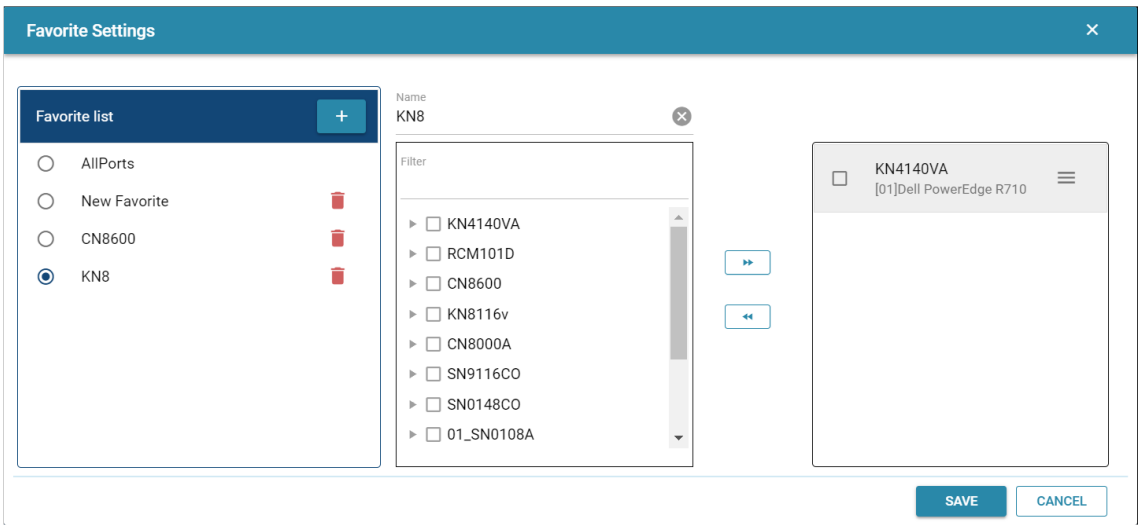
- **Recording Only**: 선택한 그룹 (즐겨찾기)에 대해 녹화 중인 포트만 표시하려면 이 옵션을 선택하십시오.

디스플레이 목록

디스플레이 목록 드롭 다운 메뉴를 클릭하면 사용 가능한 목록이 표시됩니다.
처음에 AllPorts는 사용 가능한 유일한 옵션으로 모든 포트가 중앙 집중 라이브뷰에 표시됩니다.
즐겨 찾기를 생성한 경우 즐겨 찾기 이름도 드롭 다운 메뉴에 표시됩니다.

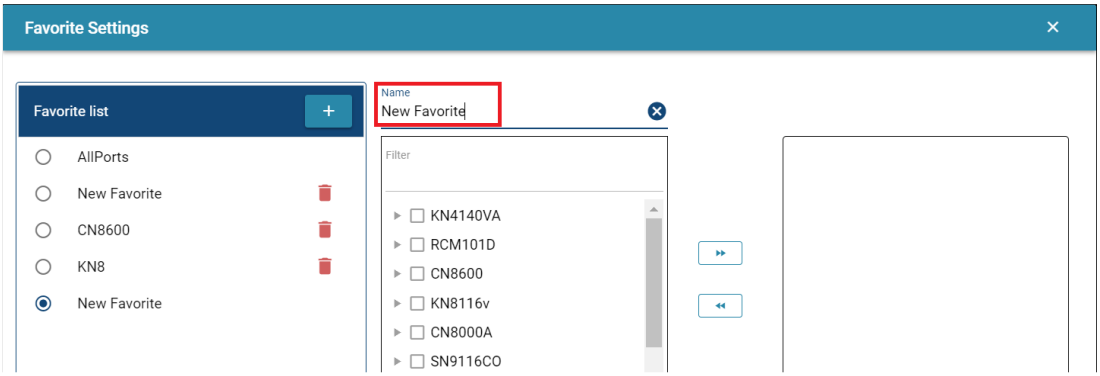
즐겨 찾기 설정

아이콘을 클릭하면 즐겨 찾기 설정을 불러옵니다.

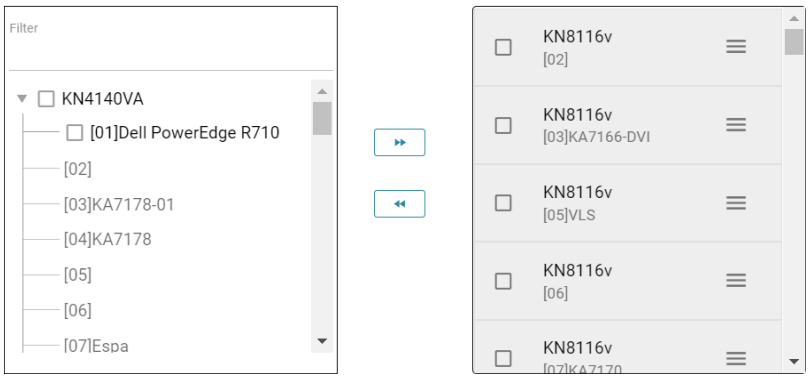


즐겨 찾기 생성

1. 즐겨 찾기를 생성하려면, + 아이콘을 클릭하십시오.
2. 시스템이 즐겨 찾기의 이름을 변경할 것인지 요청합니다.



3. 왼쪽 패널에서, 즐겨 찾기에 추가할 장치 체크박스에 체크하고 ▸▸ 버튼을 클릭하십시오.
   장치의 이용 가능한 포트가 오른쪽 패널에 표시됩니다.
   이 그룹에 추가할 포트를 선택하십시오.



   목록에서 장치 또는 포트를 삭제하려면, 오른쪽 패널에서 체크박스를 체크하고 ◂◂ 버튼을 클릭하십시오.
   필터를 사용하여 검색을 재정의할 수 있습니다.
   오른쪽 패널에서, 장치/포트를 클릭하고 드래그하여 추가된 장치/포트의 순서를 재정렬 할 수도 있습니다.

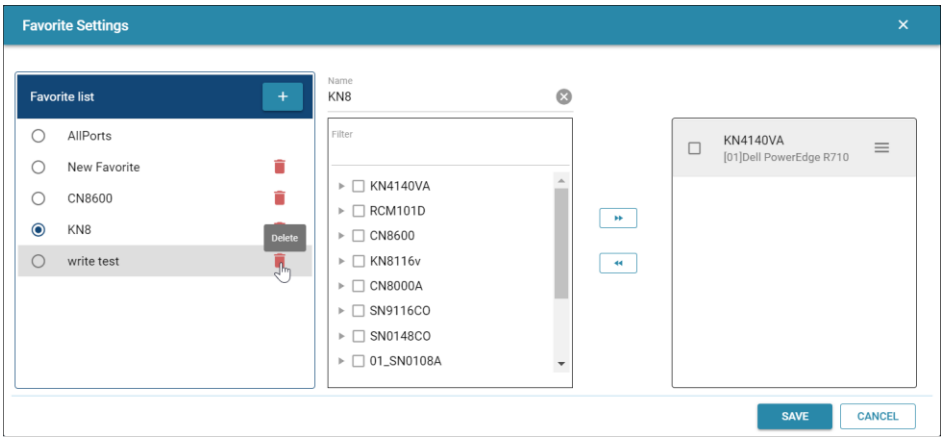
4. 완료되면 Save 버튼을 클릭하십시오. 변경 사항을 취소하려면 Cancel 버튼을 클릭하십시오.
   추가된 즐겨 찾기가 Favorite List 패널에 표시됩니다.

즐겨 찾기 수정

즐겨 찾기를 수정하려면, 즐겨 찾기의 이름을 클릭하고 위의 즐겨 찾기 생성에서 설명한 대로 수정하십시오.

즐겨 찾기 삭제

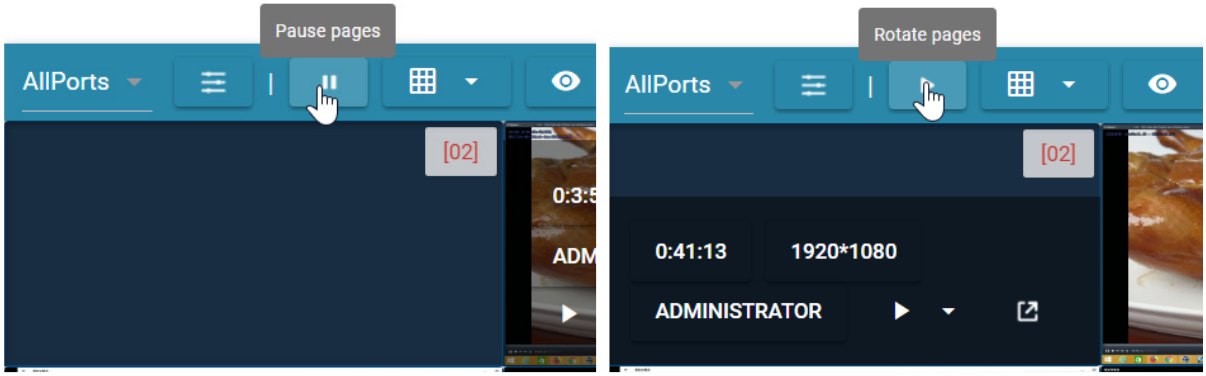
즐겨 찾기를 삭제하려면 🗑 아이콘을 클릭하고 Save 버튼을 클릭하십시오.



즐겨 찾기를 설정한 후 표시 목록 드롭 다운 메뉴를 클릭하면 목록에 즐겨 찾기가 표시됩니다.
중앙 뷰에서 즐겨 찾기의 포트만 보려면 즐겨 찾기를 선택하십시오.

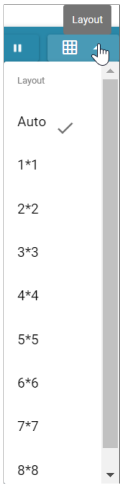
페이지 회전 / 정지

소스 포트가 레이아웃의 디스플레이 수를 초과하면 CCVSR은 페이지 별로 표시된 포트를 자동으로 회전합니다. ▶ 또는 ⏸ 아이콘을 클릭하여 각각 회전을 시작하거나 일시 중지합니다.



레이아웃

레이아웃 버튼 ▦ 을 클릭하고 원하는 레이아웃을 선택하여 중앙 집중 뷰의 레이아웃을 변경할 수 있습니다.



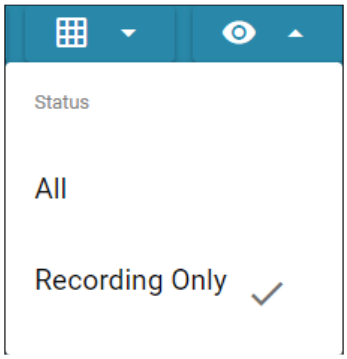
기본적으로, 자동 (Auto)이 선택됩니다. 옵션 범위는 위의 그림에 표시한대로 선택 가능합니다.

상태

상태 버튼은 모든 포트를 볼 것인지 아니면 중앙 집중 뷰에서 녹화 중인 포트만 볼 것인지 선택할 수 있는 또 다른 필터입니다.

드롭 다운 메뉴  클릭한 후

- **All:** 선택한 그룹 (즐겨찾기)에 대해 연결된 모든 포트를 표시하려면 이 옵션을 선택하십시오.
- **Recording Only**: 선택한 그룹 (즐겨찾기)에 대해 녹화 중인 포트만 표시하려면 이 옵션을 선택하십시오.



포트 정보 / 재생 / 라이브뷰 기능

마우스를 중앙 집중 뷰의 포트 위로 움직일 때 포트 정보, 재생, 라이브뷰 기능이 나타납니다.

표시된 구성 요소는 아래 테이블에서 설명합니다.

번호	항목	설명
1	녹화 시간	포트가 녹화되고 있는 시간을 표시합니다.
2	해상도	라이브뷰의 해상도를 표시합니다.

번호	항목	설명
3	로그인된 사용자 이름	포트에 접속 중인 사용자 이름을 표시합니다. 로컬 콘솔이 접속 중일 때 "Local console"이 표시됩니다.
4	재생 위치	클릭하면 드롭다운 메뉴가 나타납니다. 이 옵션은 사용자가 비디오 로그를 재생할 위치를 선택할 수 있도록 합니다.
5	새로운 윈도우로 열기	클릭하면 새로운 윈도우로 포트를 볼 수 있습니다. 37페이지 싱글 포트 모드를 참조하십시오.
6	포트 번호	라이브뷰의 포트 번호를 표시합니다.

싱글 포트 모드

새로운 윈도우로 열기 (Open in new window) 아이콘을 클릭하면 싱글 포트 모드 (Single Port Mode)로 들어갑니다.

이 윈도우 또한 녹화 시간, 해상도, 로그인된 사용자 이름을 표시합니다.

을 클릭하면 전체 화면 모드가 됩니다. Esc를 클릭하면 전체 화면 모드를 종료합니다.

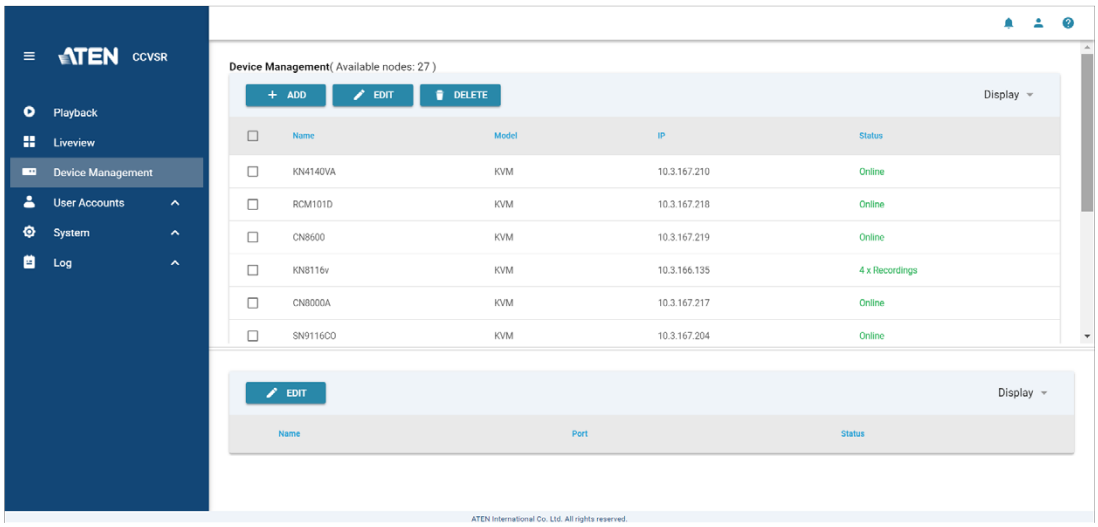
을 클릭하면 싱글 포트 모드를 종료합니다.

6 장

장치 관리

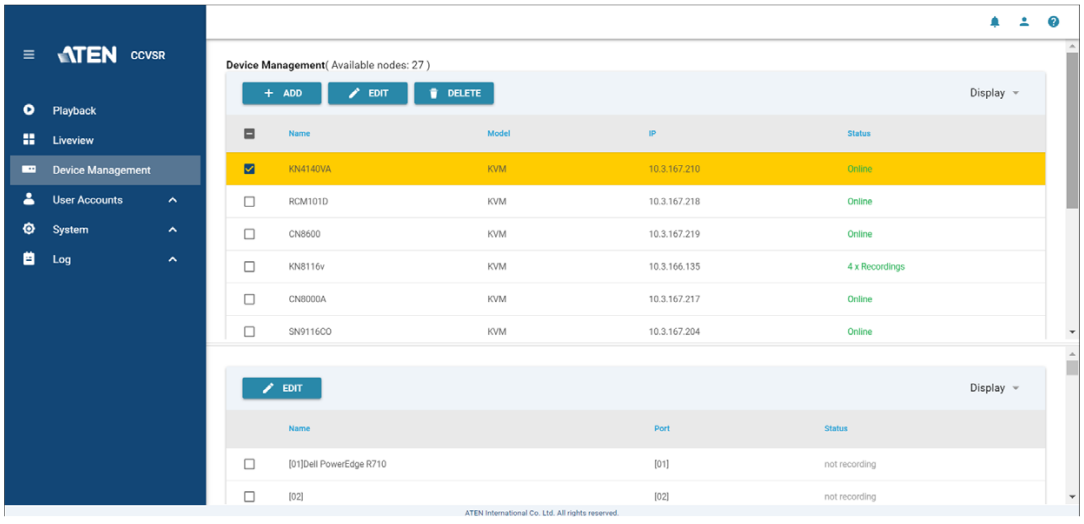
개요

Device Management 페이지는 KVM 장치를 추가하고 비디오 세션 녹화 소프트웨어가 비디오 로그를 녹화할 수 있는 포트를 구성하는 것입니다. 장치 관리 페이지는 추가된 KVM 장치 목록을 보여주는 메인 페이지를 엽니다.



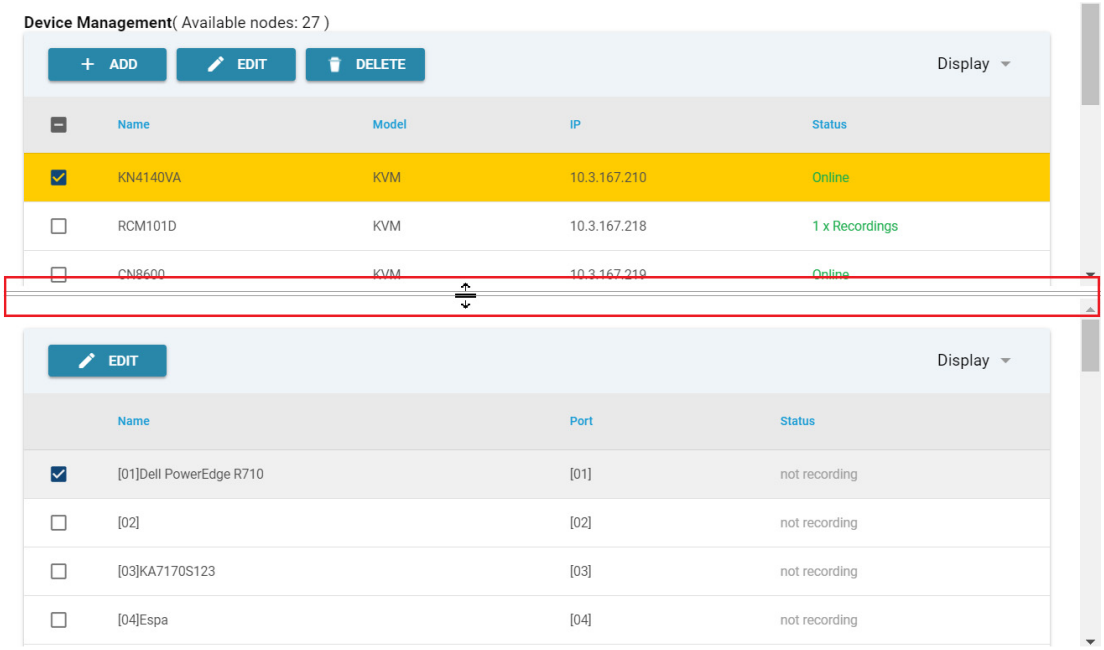
포트 목록

포트 목록은 장치 관리 페이지의 하단에 있습니다. KVM 장치를 확인하면 다음과 같이 포트 목록에 있는 모든 장치의 포트가 표시됩니다.



주의: 포트 목록은 강조 표시된 선택된 장치의 포트만 표시합니다. 위의 예에서 포트 목록은 KN4140VA의 포트만 표시합니다.

윈도우 분할을 위 또는 아래로 끌어 목록에 더 많은 포트를 표시하거나 오른쪽의 스크롤 막대를 사용할 수 있습니다.



KVM 포트 녹화

비디오 로그를 녹화하려면 KVM 스위치를 추가하고 녹화 설정 (녹화 탭)을 구성해야 합니다. 활성화된 포트는 KVM 스위치를 통해 접속할 때마다 비디오 세션 녹화 소프트웨어에 의해 기록되며 비디오 로그 파일로 저장됩니다. 로그는 재생 탭에서 볼 수 있습니다. 라이센스가 있는 한 (10페이지 라이센스 참조) 추가할 수 있는 KVM 장치 또는 활성화할 수 있는 포트의 수에는 제한이 없습니다. 비디오 세션 녹화 소프트웨어는 여러 KVM 장치에서 동시에 최대 20개의 포트를 동시에 녹화할 수 있습니다.

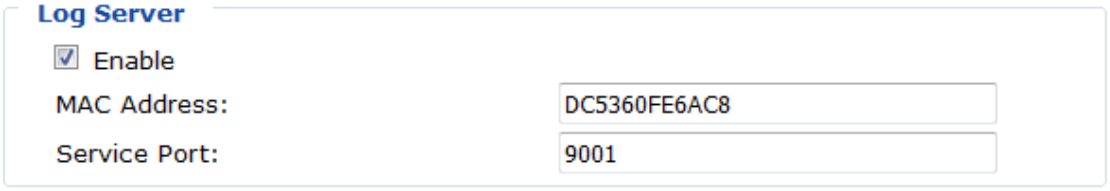
디스플레이

Display (우측 상단 구석)를 클릭하여 목록에 표시되는 정보를 선택합니다.

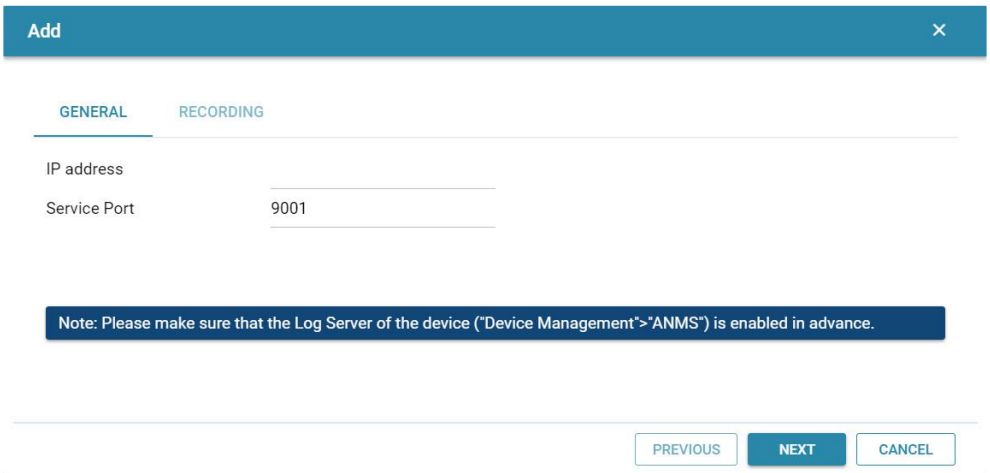
KVM 장치 추가

KVM 장치 목록에 KVM 장치를 추가하려면 다음을 수행하십시오.

1. KVM 장치에서 장치 관리로 이동하여 **로그 서버**를 활성화하고 아래와 같이 비디오 세션 녹화 소프트웨어를 실행하는 컴퓨터의 **MAC 주소 (MAC Address)** 및 **서비스 포트 (Service Port)**를 입력하십시오.



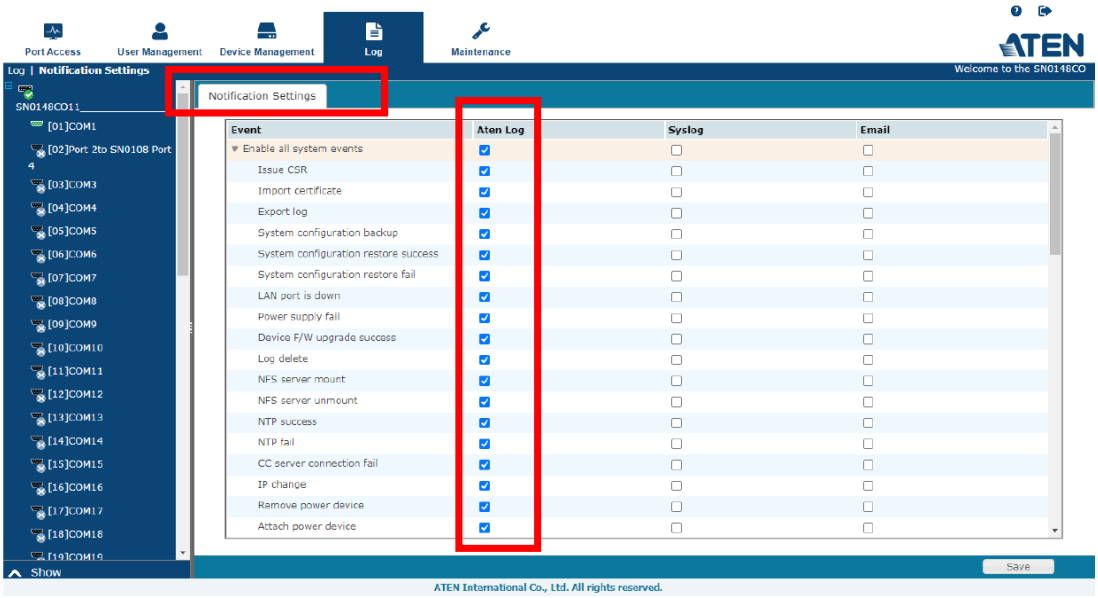
2. 장치 관리 페이지에서 + ADD 버튼을 클릭하십시오.
   팝업 창이 나타납니다.



3. 추가하려는 KVM 장치의 IP 주소와 서비스 포트 번호를 입력하고 **Next**를 클릭하십시오. 시스템이 자동으로 Recording 탭으로 이동합니다.
4. KVM 장치에서 포트 녹화를 활성화하려면 드롭 다운 메뉴를 클릭하고 "Enable (Video + Audio)" 또는 "Enable (Video)"를 선택하십시오. 자세한 내용은 42페이지의 비디오/오디오 녹화 활성화를 참조하십시오.
5. 로컬 콘솔에서 녹화를 활성화하려면 체크박스에 체크하고 입력 필드에 시간 지연 값 (0-999)을 입력하십시오.
6. Add를 클릭하여 KVM 장치를 추가하십시오.
7. KVM 장치가 장치 목록과 장치 관리 메인 페이지에 나타납니다.

주의:

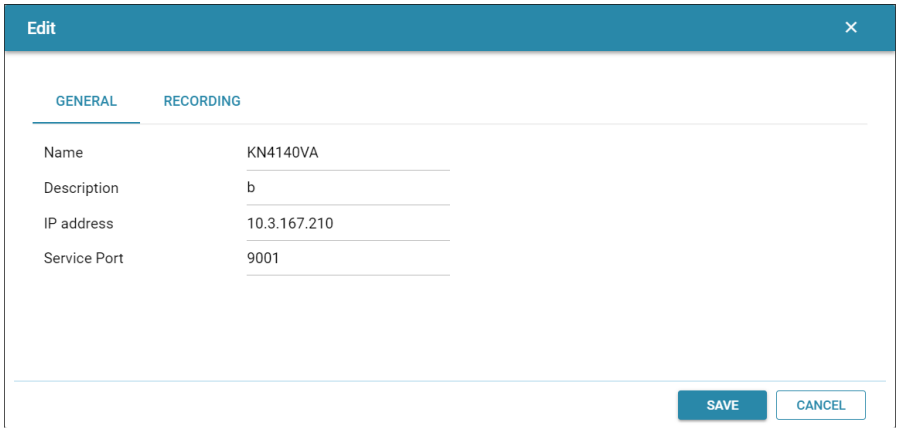
- KVM 장치를 추가한 후 Status 열을 체크하십시오. Online이 표시되면 장치를 성공적으로 추가한 것입니다.
- Offline 상태는 KVM 장치가 네트워크를 통해 연결할 수 없음을 나타냅니다. KVM 장치의 IP 주소 및 서비스 포트 번호가 정확한지, KVM 장치가 온라인 상태이며 로그 서버가 활성화되고 올바른 MAC 주소로 구성되어 있는지 확인하십시오.
- 추가된 시리얼 콘솔 서버의 로그를 수신하려면 시리얼 콘솔 서버의 자체 알림 페이지에서 알림 설정을 활성화했는지 확인하십시오. 아래에 예제 (SN0148CO 장치 인터페이스)가 있습니다.



- KE6900AiT, KE6940AiT, RCMDVI00AT, RCMDVI40AT, RCMDVI00BT, RCMDVI40BT, RCMDV150BT의 포트를 통해 녹화된 세션의 경우 다음 사항에 유의하십시오.
  - 오디오는 지원되지 않습니다.
  - **로컬 콘솔 포트 녹화 활성화** 설정은 **Extender Mode**로 설정된 RCMDVI00BT, RCMDVI40BT, RCMDVI50BT에서 지원됩니다.
  - **로컬 콘솔 포트 녹화 활성화** 설정은 KE6900AiT, KE6940AiT, RCMDVI00AT, RCMDVI40AT에서 지원되지 않습니다.
  - 키 입력 및 마우스 클릭 녹화는 KE6900AiT, KE6940AiT의 포트에서 캡처된 원격 세션에 대해서만 지원됩니다.

KVM 장치 편집

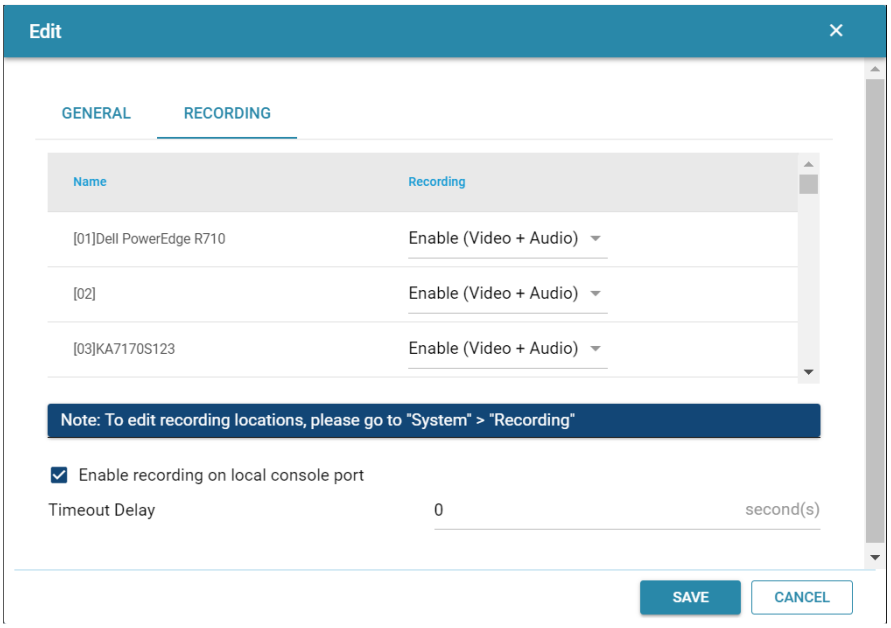
이름, 설명, IP 주소, 서비스 포트 및 녹화 옵션을 편집하려면 KVM 장치의 체크박스에 체크하고 EDIT 버튼을 클릭하십시오.



옵션을 편집하고 Save을 클릭하여 저장합니다.

녹화

녹화 옵션을 편집하려면 Recording 탭을 클릭하십시오.



비디오/오디오 녹화 활성화

KVM 장치의 포트가 비디오 + 오디오 또는 비디오 전용 세션을 녹화하도록 하려면 다음을 수행하십시오.

1. KVM 장치의 체크박스에 체크하십시오.

2. 편집 팝업 메뉴 버튼을 클릭하십시오.
3. Recording 탭을 클릭하십시오.
4. Recording 열 아래의 드롭 다운 메뉴를 클릭하십시오.
5. "Enable (Video + Audio)" (활성화 (비디오+오디오)), "Enable (Video)" (활성화 (비디오)), 또는 "Disable" (비활성화)을 선택하십시오.
6. Save을 클릭하여 저장하십시오.
7. 활성화된 포트는 이제 접속할 때마다 녹화됩니다.

로컬 콘솔 포트에서 녹화 활성화

CCVSR에 추가된 포트 장치는 로컬 콘솔 포트를 통해 접속할 수 있습니다. 접속할 때마다 로컬 콘솔에서 녹화를 활성화하려면 체크박스에 체크하십시오.

CN8000A, CN8600, CN9000, CN9600, CN9950, RCM101A, RCM101D, RCMVGA101, RCMDVI101, RCMDP101U의 경우 입력 필드에 시간 초과 지연 값을 초 단위 (0-180)로 입력하십시오.

CCVSR은 설정된 시간 이후에 키 입력이나 마우스 움직임이 없으면 녹화를 중지합니다. 여기에 '**0**'을 입력하면 CCVSR은 무기한으로 녹화합니다.

KVM 장치 삭제

KVM 장치를 삭제하려면 KVM 장치의 체크박스에 체크하고 

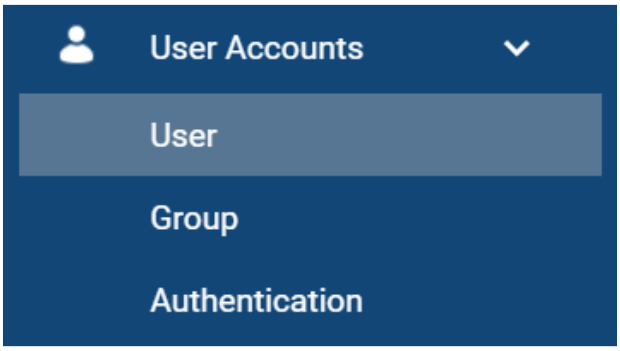
버튼을 클릭하십시오.

7 장

사용자 계정

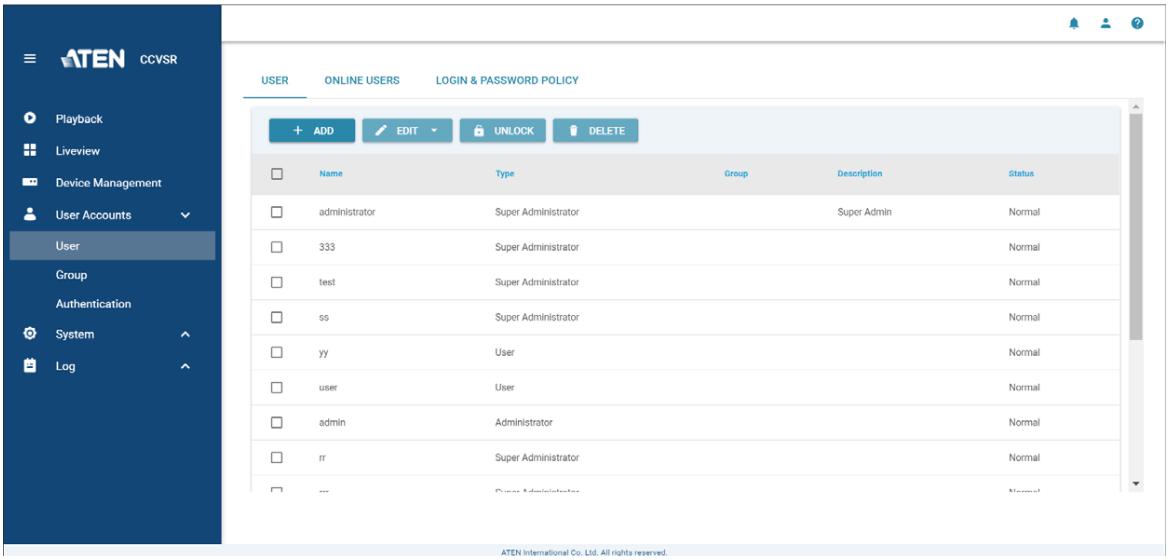
개요

메인 메뉴의 사용자 계정은 3가지 하위 메뉴로 확장됩니다.



사용자

User 하위 메뉴는 아래와 같습니다.



메인 패널은 한눈에 볼 수 있도록 더 자세한 사용자 정보를 제공합니다.

표시되는 정보의 정렬 순서는 열 항목을 클릭하여 변경할 수 있습니다.

메인 패널 상단의 버튼은 사용자를 관리하는데 사용됩니다.

사용자 유형

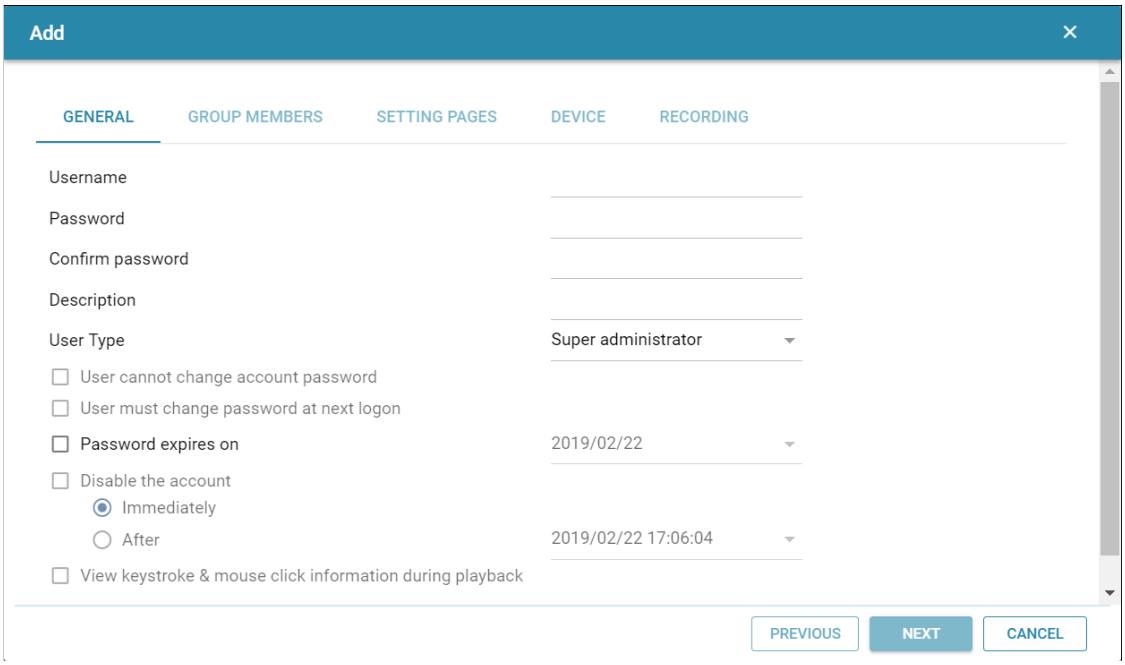
비디오 세션 녹화 소프트웨어는 아래 테이블의 3가지 유형의 사용자를 지원합니다.

사용자 유형	역할
Super Administrator (통합 관리자)	포트 및 장치에 접속 및 관리합니다. 사용자 및 그룹을 관리합니다. 전체 설비를 구성합니다. 개인 작업 환경을 구성합니다.
Administrator (관리자)	승인된 포트 및 장치에 접근 및 관리합니다. 사용자 및 그룹을 관리합니다. 개인 작업 환경을 구성합니다.
User (사용자)	승인된 포트 및 장치에 접근합니다. 승인된 포트 및 장치를 관리합니다. 개인 작업 환경을 구성합니다. **주의:** 권한이 주어진 사용자는 다른 사용자를 관리할 수 있습니다.

사용자 추가

사용자를 추가하고, 사용자 권한을 할당하려면 다음을 수행하십시오.

1. + ADD 버튼을 클릭하면 아래와 같은 팝업 윈도우가 나타납니다.



2. 해당 필드에 필수 정보를 입력하십시오. 각 필드에 대한 설명은 아래 테이블에 있습니다.

필드	설명
Username	계정 정책 설정에 따라 1~16 자를 입력할 수 있습니다. 보안을 위해 68 페이지의 내용과 같이 주기적으로 이 문자열을 변경할 것을 권장합니다.
Password	계정 정책 설정에 따라 0~16자를 입력할 수 있습니다. (50페이지 로그인 & 암호 정책 참조)
Confirm Password	암호를 정확히 입력했는지 확인하기 위해, 다시 한번 입력합니다. 2개의 목록이 정확히 일치해야 합니다.
Description	포함하고 싶은 사용자에 대한 추가 정보입니다.
User Type	통합 관리자, 관리자. 사용자 3가지 카테고리가 있습니다. 각 카테고리에 생성할 수 있는 계정의 수는 제한이 없습니다. ◆ 통합 관리자는 전체 설비 환경 구성 및 유지보수, 사용자 관리, 장치 및 포트 할당을 관장합니다. 통합 관리자의 권한 (46페이지 참조)는 시스템에 의해 자동으로 할당되며 변경될 수 없습니다. ◆ 관리자의 기본 권한은 키보드/마우스 보기를 제외한 모든 것이 포함되나, 각 권한의 체크 박스를 체크 혹은 해제함으로써 각 관리자의 권한을 변경할 수 있습니다. ◆ 사용자는 기본적으로 권한이 없습니다. 그러나 권한 체크 박스에 체크 혹은 해제함으로써 각 관리자의 권한을 변경할 수 있습니다. **주의:** 사용자 관리 권한을 가진 사용자는 그룹에 접근 및 설정할 수 없습니다.

필드	설명
Account Condition	조건을 통해 사용자의 계정과 시스템 접속을 제어할 수 있습니다. 아래 설명된 조건을 추가하려면 체크박스에 체크하십시오. ◆ **User cannot change account password:** 암호를 영구적으로 만들어 사용자가 다른 것으로 변경할 수 없도록 합니다. 이것을 체크하면 다음 2가지 조건이 비활성화됩니다. ◆ **User must change password at next logon:** 이것을 체크하면 위의 조건을 비활성화합니다. 이 사용자가 암호를 변경하면 이 옵션의 체크는 해제됩니다. ◆ **Password expires on:** 조건에 대한 날짜를 선택합니다. ◆ **Disable the Account:** 사용자 계정을 실제로 삭제하지 않고 일시 중지하여 나중에 쉽게 복원할 수 있습니다. ◆ Immediately (즉시 비활성화) ◆ After: 계정을 비활성화할 날짜와 시간을 선택합니다. ◆ **재생 중에 키 입력 및 마우스 클릭 정보 보기**

3. 사용자를 통합 관리자로 선택한 경우 add를 클릭하여 사용자를 추가하십시오. 사용자를 관리자 또는 사용자로 선택한 경우 Group Member, Setting Pages, Device, Recording (그룹 멤버, 설정 페이지, 장치, 녹화) 탭이 활성화되어 구성할 수 있습니다. 활성화된 탭 또는 Next를 클릭하여 사용자 구성을 계속합니다.
4. **Group Members:** 그룹 멤버 탭을 선택하여 새 사용자를 그룹에 할당하고 사용자가 속할 그룹을 선택한 후 Next를 클릭하십시오.

주의: 할당하려는 그룹이 생성되지 않은 경우 51페이지의 그룹 생성을 참조하여 새 그룹을 생성하십시오.

---

5. **Setting Pages:** 이 탭에서 옵션을 체크하고 Next를 클릭하여 권한을 할당할 수 있습니다.

주의: 일반 사용자의 경우 장치 관리를 활성화하는 것 외에도 사용자가 관리할 수 있는 각 장치에 대한 권한을 부여 받아야합니다.

◆ Liveview를 활성화하면 사용자가 라이브뷰 기능을 사용할 수 있습니다. (32페이지 라이브뷰 참조)

- ◆ Playback을 활성화하면 사용자가 재생 기능을 사용할 수 있습니다. (20페이지 재생 참조)
- ◆ Device Management를 활성화하면 사용자가 장치 관리 탭에서 설정 및 장치를 볼 수 있습니다. (38페이지 장치 관리 참조)
- ◆ User Accounts을 활성화하면 사용자가 사용자 및 그룹 계정을 생성, 수정 및 삭제할 수 있습니다.
- ◆ Log를 활성화하면 사용자가 시스템 로그에 접속할 수 있습니다. (세부 사항은 81페이지 로그 참조)
- ◆ 시스템을 활성화하면 사용자가 시스템 탭에서 설정에 접속하고 구성할 수 있습니다.

6. **Device:** 장치 탭을 선택하여 사용자의 장치 접속 권한을 할당하고 접속 권한을 부여할 장치를 선택한 후 Next를 클릭하십시오.
7. **Recording:** 녹화 탭을 선택하여 CCVSR 구성 권한을 할당하고 사용자가 구성할 수 있는 CCVSR을 선택한 후 Next를 클릭하십시오.
8. 선택이 완료되면 **Add**를 클릭하십시오.

사용자 수정

사용자 계정을 수정하려면 다음을 수행하십시오.

1. 사용자의 체크박스에 체크하십시오.
2. EDIT 버튼을 클릭하고 속성 (Properties) 또는 접속 권한 (Access right)을 선택하십시오.
3. **Properties:** 속성을 선택하면 일반 탭과 그룹 멤버 탭을 구성할 수 있습니다.
   Access right: 접속 권한을 선택하면 설정 페이지 탭, 장치 탭 및 녹화 탭을 구성할 수 있습니다.
   자세한 내용은 45페이지의 사용자 추가를 참조하십시오.
4. 수정이 완료되면 Save를 클릭하십시오.

사용자 삭제

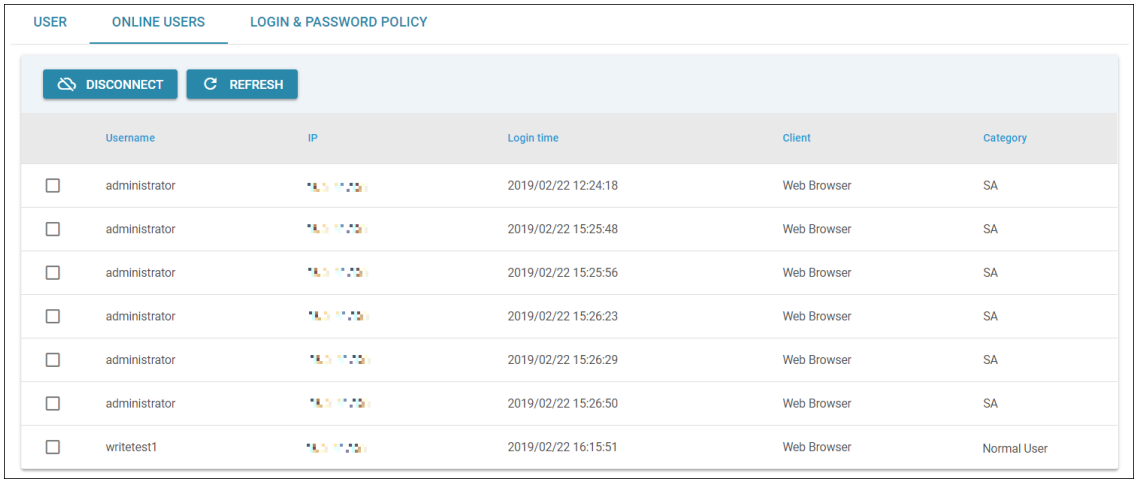
사용자 계정을 삭제하려면 다음을 수행하십시오.

1. 사용자의 체크박스에 체크하십시오.
2. DELETE 를 클릭하십시오.

주의: 모든 사용자가 삭제되면 시스템은 기본 관리자 계정과 암호 (이름: administrator, 암호: password)를 자동으로 생성합니다.

온라인 사용자

Online Users 탭을 통해 통합 관리자는 현재 비디오 세션 녹화 소프트웨어에 로그인한 사용자를 한 눈에 볼 수 있으며, 각 세션에 대한 정보를 제공합니다.



주의: 1. Online User 페이지는 Administrator 또는 User 사용자 유형은 사용할 수 없습니다.
2. Category 항목에는 로그인한 사용자 유형이 나열됩니다. SA (통합 관리자); Admin (관리자); Normal user (사용자)

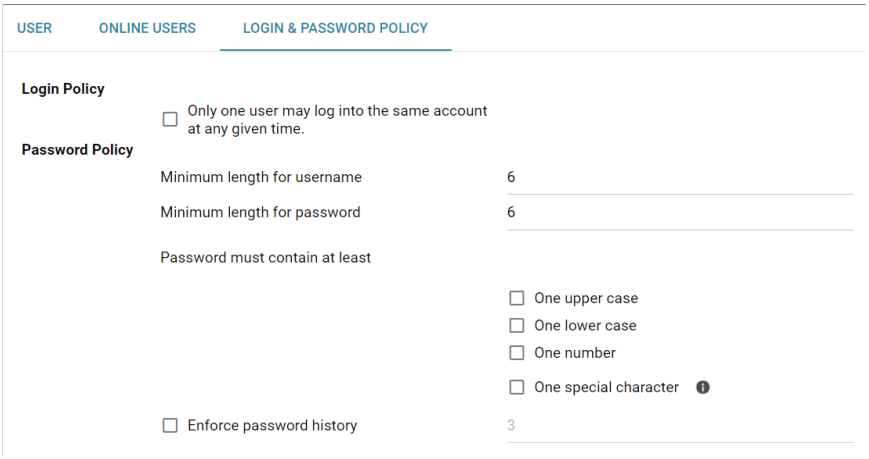
페이지 상단에 있는 항목의 의미는 매우 간단합니다. IP는 사용자가 로그인한 IP 주소를 나타냅니다. Login Time은 사용자가 비디오 세션 녹화 소프트웨어에 로그인한 시간을 의미하고 Client는 사용자가 시스템에 접속하는데 사용한 클라이언트를 의미합니다.

- 이 페이지는 또한 통합 관리자에게 사용자를 선택하고 DISCONNECT를 클릭하여 시스템에서 사용자 연결을 해제할 수 있는 옵션을 제공합니다.
- Refresh을 클릭하여 목록을 새로 고침 합니다.

표시되는 정보의 정렬 순서는 열 항목을 클릭하여 변경할 수 있습니다.

로그인 및 암호 정책

Login & Password Policy 탭에서 시스템 관리자는 로그인, 사용자 이름 및 암호를 관리하는 정책을 설정할 수 있습니다.



로그인 정책

항목	설명
Only one user may log into the same account at any given time	이것을 체크하면 동시에 같은 계정으로 로그인하는 것을 방지할 수 있습니다.

암호 정책

항목	설명
Minimum Username Length	사용자 이름에 필요한 최소 글자수를 설정합니다. 가능한 글자 수는 1-16 입니다. 기본 설정은 6 입니다.
Minimum Password Length	암호에 필요한 최소 글자수를 설정합니다. 가능한 글자 수는 0-16 입니다. 0 은 암호가 필요하지 않다는 의미입니다. 기본 설정은 6 입니다. 사용자는 사용자 이름만으로 로그인 할 수 있습니다. 기본 설정은 6 입니다.
Password Must Contain At Least	암호를 입력할 때 사용자에게 최소한 1개의 대문자, 소문자 혹은 숫자, 또는 1개의 특수문자를 요구할 것인지 체크합니다. **주의:** 이 정책은이 정책이 활성화된 후 생성된 사용자 계정과 기존 사용자 계정의 암호 변경에만 영향을 줍니다. 이 정책이 활성화되기 전에 기존 암호를 변경하지 않고 생성된 사용자 계정은 영향을 받지 않습니다.
Enforce password history	체크하면 암호를 변경하려고 할 때 동일한 암호를 사용할 수 없습니다. 여기에 입력한 숫자는 시스템이 기억할 암호 변경 횟수입니다. 시스템은 기억하는 암호를 변경할 수 없습니다.

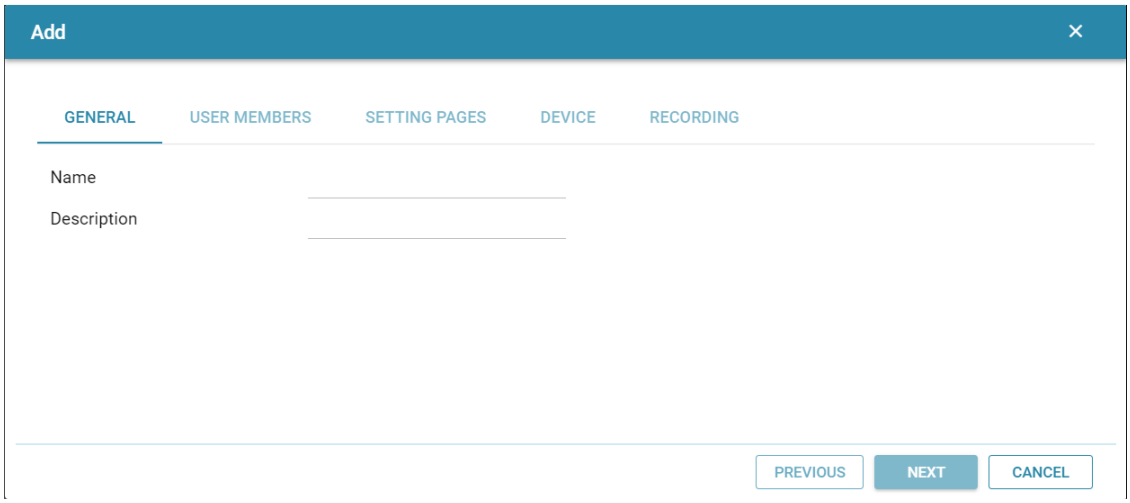
그룹

그룹을 통해 관리자는 사용자와 장치를 쉽고 효율적으로 관리할 수 있습니다. 장치 접속 권한은 그룹의 멤버인 모든 사용자에게 적용되므로 관리자는 각 사용자에 대해 개별적으로 설정하는 대신 그룹에 대해 한 번만 설정하면됩니다. 여러 그룹을 정의하여 일부 사용자는 특정 장치에 접속하고 다른 사용자는 접속하지 못하도록 제한할 수 있습니다.

그룹 생성

그룹을 생성하려면 다음을 수행하십시오.

1. + ADD 버튼을 클릭하면 아래와 같은 팝업 윈도우가 나타납니다.



2. 해당 필드에 필수 정보를 입력하십시오. 각 필드에 대한 설명은 아래 테이블에서 설명합니다.

필드	설명
Name	최대 16 자의 글자를 사용할 수 있습니다.
Description	사용자가 추가하려는 사용자에 관한 추가 정보입니다. 최대 63자의 글자를 사용할 수 있습니다.

Next를 클릭하면 사용자 멤버 탭이 나타납니다.

3. **User Members:** 멤버 탭을 선택하여 사용자를 그룹에 할당하고 사용자가 속할 그룹을 선택한 후 Next를 클릭하십시오.
4. **Setting Pages:** 이 탭에서 옵션을 체크하고 Next를 클릭하여 권한을 할당할 수 있습니다.
   - ◆ Liveview를 활성화하면 사용자가 라이브뷰 기능을 사용할 수 있습니다. (32페이지 라이브뷰 참조)

- ◆ Playback을 활성화하면 그룹에 있는 사용자가 재생 기능을 사용할 수 있습니다. (20페이지 재생 참조)
- ◆ Device Management를 활성화하면 그룹에 있는 사용자가 장치 관리 탭에서 설정 및 장치를 볼 수 있습니다. (38페이지 장치 관리 참조)
- ◆ User Accounts을 활성화하면 그룹에 있는 사용자가 사용자 및 그룹 계정을 생성, 수정 및 삭제할 수 있습니다.
- ◆ Log를 활성화하면 그룹에 있는 사용자가 시스템 로그에 접속할 수 있습니다. (세부 사항은 81페이지 로그 참조)
- ◆ 시스템을 활성화하면 그룹에 있는 사용자가 시스템 탭에서 설정에 접속하고 구성할 수 있습니다.

5. **Device:** 장치 탭을 선택하여 그룹의 장치 접속 권한을 할당하고 접속 권한을 부여할 장치를 선택한 후 Next를 클릭하십시오.
6. **Recording:** 녹화 탭을 선택하여 CCVSR 구성 권한을 할당하고 그룹이 구성할 수 있는 CCVSR을 선택한 후 Next를 클릭하십시오.
7. 선택이 완료되면 **Add**를 클릭하십시오.

그룹 수정

그룹을 수정하려면 다음을 수행하십시오.

1. 그룹의 체크박스에 체크하십시오.
2. EDIT 버튼을 클릭하고 속성 (Properties) 또는 접속 권한 (Access right)을 선택하십시오.
3. **Properties:** 속성을 선택하면 일반 탭과 그룹 멤버 탭을 구성할 수 있습니다.
   Access right: 접속 권한을 선택하면 설정 페이지 탭, 장치 탭 및 녹화 탭을 구성할 수 있습니다.
   자세한 내용은 51페이지의 그룹 생성을 참조하십시오.
4. 수정이 완료되면 Save를 클릭하십시오.

그룹 삭제

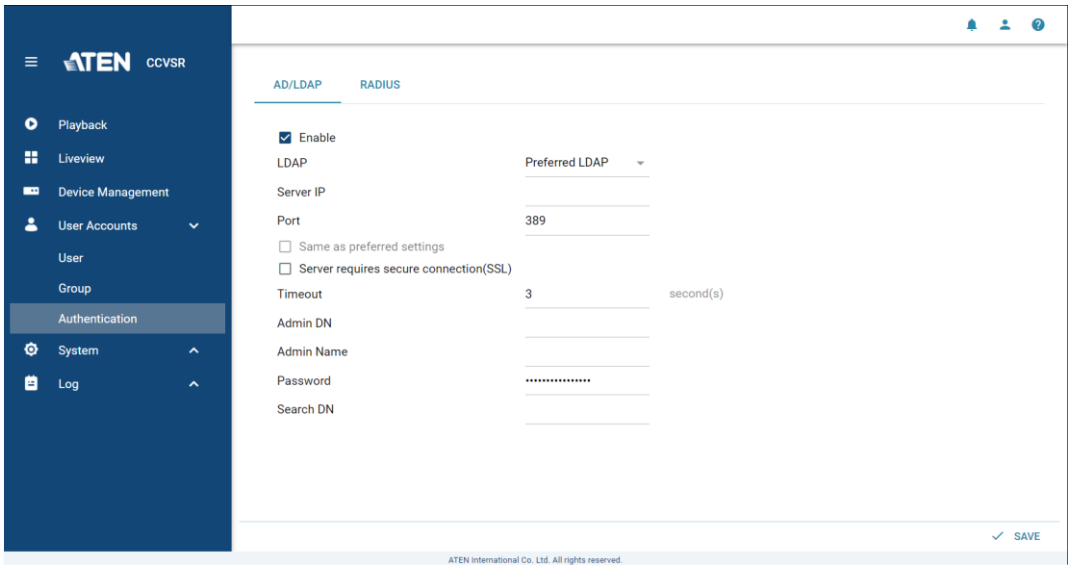
그룹을 삭제하려면 다음을 수행하십시오.

1. 사용자의 체크박스에 체크하십시오.
2. DELETE 를 클릭하십시오.

인증

Authentication 하위 메뉴는 AD/LDAP 및 RADIUS 설정을 포함합니다.

AD/LDAP 설정



AD/LDAP를 통해 비디오 로그 서버의 인증 및 승인을 허용하려면, 아래 테이블에 있는 정보를 참조하십시오.

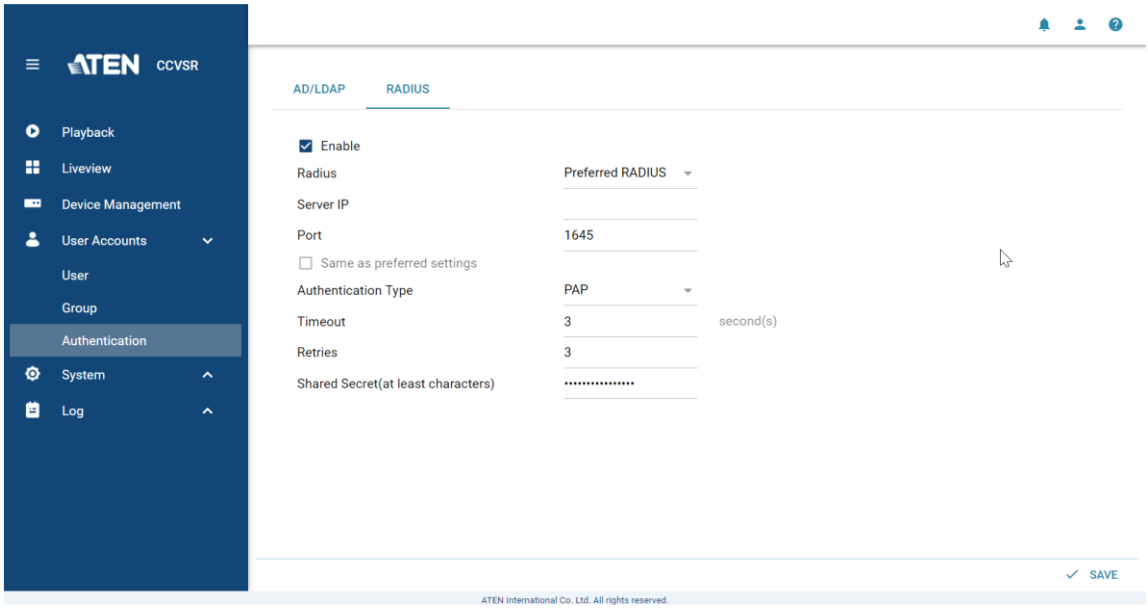
항목	효과
Enable	Enable 체크 박스에 체크하여 AD/LDAP 인증 및 승인을 허용합니다.
LDAP Type	드롭다운 메뉴를 클릭하여 Preferred 또는 Alternate LDAP 를 선택합니다.
Server IP	IP 주소를 입력합니다. LDAP 서버 필드에서 IPv4 주소, IPv6 주소 또는 도메인 네임을 사용할 수 있습니다.
Port	포트 번호를 입력합니다. Server requires secure connection (SSL)를 체크하면, 기본 포트 번호는 636 입니다. 그렇지 않으면 기본 포트 번호는 389입니다.
Timeout	타임아웃이 되기 전에 비디오 로그 서버가 응답하는 것을 기다리는 시간을 초 단위로 설정합니다.
Admin DN	AD/LDAP 관리자와 상의하여 이 필드에 적절한 목록을 확인합니다. 예를 들어 목록은 다음과 같습니다. ou=kn4132,dc=aten,dc=com
Admin Name	LDAP 관리자의 사용자 이름을 입력합니다.
Password	LDAP 관리자의 암호를 입력합니다.
Search DN	검색이 가능한 구분되는 이름을 설정합니다. 이 아이템은 사용자 이름으로 검색이 시작되는 도메인 이름입니다.

윈도우의 우측 하단 구석에 있는 Save를 클릭하여 환경 구성을 저장합니다.

AD/LDAP 서버에서, 사용자는 다음과 같은 방법으로 인증 받을 수 있습니다.

- MS Active Directory 스키마
  - LDAP를 통한 인증을 허용하려면, AD LDAP 스키마를 CCVSR (iVlog-userProfile)의 속성 이름을 개인 클래스에 대한 선택적 속성으로 확장해야 합니다.
- 스키마를 통하지 않고 – 비디오 로그 서버에서 사용되는 사용자 이름만 LDAP/LDAPS 서버의 이름과 일치합니다. 사용자 권한은 스위치에 구성된 권한과 동일합니다.
- 스키마를 통하지 않고 – AD의 그룹만 일치합니다. 사용자 권한은 스위치에서 그가 속한 그룹에 대해 구성된 권한입니다.
- 스키마를 통하지 않고 – AD의 사용자 이름과 그룹이 일치합니다. 사용자 권한은 스위치에서 사용자 및 그가 속한 그룹에 대해 구성된 권한입니다.

RADIUS 설정



RADIUS 서버를 통해 비디오 로그 서버에 대한 인증 및 승인을 허용하려면 다음을 수행하십시오.

1. **Enable**를 체크하십시오.
2. 드롭 다운 메뉴에서 Preferred (기본) RADIUS 또는 Alternate (대체) RADIUS를 선택하십시오.

3. IP 주소와 서비스 포트 번호를 입력합니다. IP 필드에 IPv4 주소, IPv6 주소 또는 도메인 이름을 사용할 수 있습니다.
4. 인증 유형 드롭 다운 메뉴에서 PAP 또는 CHAP를 선택하십시오.
5. Timeout 필드에서 시간이 초과되기 전에 비디오 로그 서버가 RADIUS 서버 응답을 기다리는 시간 (초)을 설정합니다.
6. Retries 필드에서 RADIUS 재시도 허용 횟수를 설정합니다.
7. Shared Secret 필드에 비디오 로그 서버와 RADIUS 서버 사이의 인증에 사용할 문자열을 입력하십시오. 최소 6자가 필요합니다.
8. 창의 우측 하단에 있는 Save를 클릭하여 환경 구성을 저장하십시오

RADIUS 서버에서 사용자는 다음 방법 중 하나로 인증될 수 있습니다.

- 사용자 항목을 **su/xxxx**로 설정합니다.
- 여기서 xxxx는 비디오 로그 서버에서 계정을 만들 때 사용자에게 부여된 사용자 이름을 나타냅니다.
- RADIUS 서버와 비디오 로그 서버에서 동일한 사용자 이름을 사용합니다.
- RADIUS 서버와 비디오 로그 서버에서 동일한 그룹 이름을 사용하십시오.
- RADIUS 서버와 비디오 로그 서버에서 동일한 사용자 이름/그룹 이름을 사용합니다.

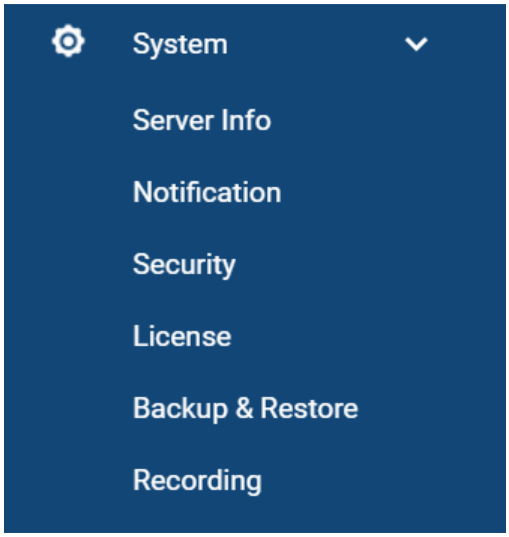
각각의 경우 사용자의 접근 권한은 비디오 로그 서버에 그룹의 사용자가 생성될 때 할당된 권한입니다. (45페이지 사용자 추가 참조)

8 장

시스템

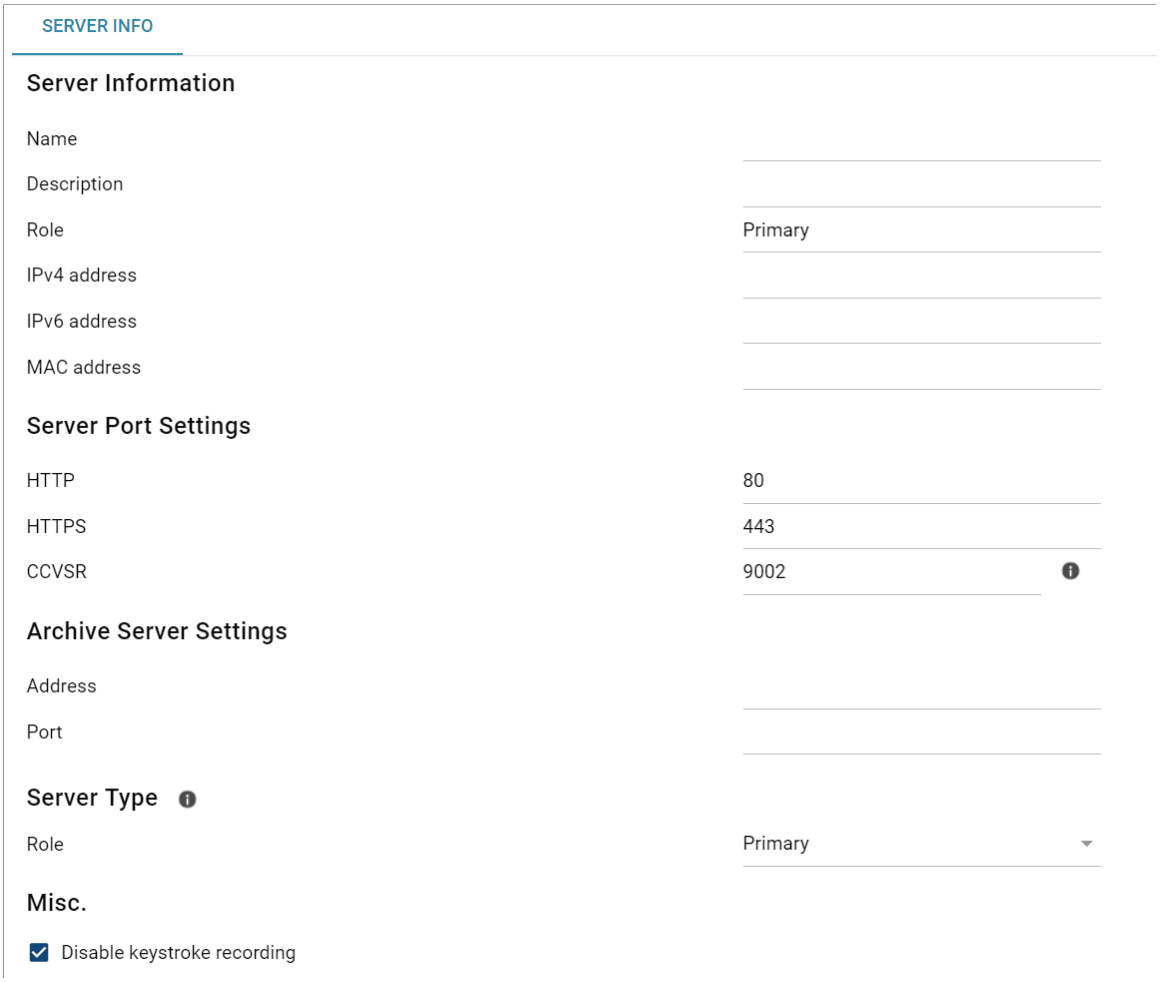
개요

System 페이지는 CCVSR의 시스템 설정을 보고 관리하는데 사용됩니다. System을 클릭하면 하위 메뉴가 확장/축소됩니다.



시스템 정보

Server Info 하위 메뉴를 클릭하면 아래 페이지를 불러옵니다.



서버 정보

항목	의미
Name	CCVSR 애플리케이션을 호스팅하는 서버의 컴퓨터 이름을 표시합니다.
Description	서버 설명을 표시합니다. 여기에서 정보를 수정할 수 있습니다.
Role	서버의 역할을 표시합니다.
IPv4 Address	CCVSR의 IPv4 주소를 표시합니다.
IPV6 Address	CCVSR의 IPV6 주소를 표시합니다.
Server MAC	CCVSR 애플리케이션을 호스팅하는 컴퓨터의 MAC 주소를 표시합니다.

서버 포트 설정

이것은 CCVSR에 접속하는데 사용되는 서비스 포트를 지정하는 데 사용됩니다.

항목	의미
HTTP	브라우저 로그인한 포트 번호입니다. 기본 값은 9080 입니다.
HTTPS	보안 브라우저 로그인한 포트 번호입니다. 기본 값은 9443 입니다.
CCVSR	CCVSR 프라이머리 서버 및 세컨더리 서버 사이의 통신을 위한 포트 번호입니다. 기본 값은 9002 입니다.

보안 조치로 방화벽을 사용하는 경우 관리자는 방화벽이 허용할 포트 번호를 지정할 수 있습니다. 기본 값 이외의 포트를 사용하는 경우 사용자는 로그인 할 때 IP 주소의 일부로 포트 번호를 지정해야 합니다. 유효하지 않은 포트 번호 (또는 포트 번호 없음)를 지정하면 CCVSR을 찾을 수 없게 됩니다.

예제: 보안 브라우저 로그인 (https)을 사용하여 IP 주소가 192.168.0.100인 CCVSR에 접속하려면 다음 주소를 입력하십시오.

https://192.168.0.100:9443

주의: 1. 모든 서비스 포트의 유효한 목록은 1-65535입니다.

2. 서비스 포트는 같은 값을 가질 수 없습니다. 각 포트마다 다른 값을 설정해야 합니다.
3. 방화벽이 없는 경우(예를 들어 인트라넷), 효과가 없기 때문에 설정된 번호 값은 상관없습니다.

아카이브 서버 설정

CCVSR 보관 서버를 설치한 경우 소프트웨어를 호스팅하는 컴퓨터의 IP 주소와 포트 번호를 입력합니다. 아카이브 서버 환경 구성에 대한 자세한 내용은 87페이지 CCVSR 아카이브 서버를 참조하십시오.

서버 유형

여기에서 서버의 역할을 변경할 수 있습니다. 드롭 다운 메뉴를 사용하여 프라이머리 또는 세컨더리를 선택합니다.

- 프라이머리 서버

  주요 비디오 세션 녹화 소프트웨어로 운영 중인 컴퓨터에 대해 Primary Server (프라이머리 서버)를 선택합니다. 이 컴퓨터는 비디오 세션 녹화 소프트웨어의 모든 측면을 호스팅하고 관리하며 비디오 로그 파일의 확장된 저장을 위해 Secondary Servers (세컨더리 서버)로 실행되는 컴퓨터를 추가할 수 있습니다.

- 세컨더리 서버
  - 프라이머리 서버의 비디오 로그 파일을 저장할 용도로 컴퓨터를 사용하려면 세컨더리 서버를 선택하십시오.
  - 이 옵션을 선택하시는 경우 다음 사항을 꼭 확인하십시오.
    - 세컨더리 서버를 프라이머리 서버에 추가합니다. 자세한 내용은 77페이지의 "세컨더리 CCVSR 서버 추가"를 참조하십시오.
    - 다음 설정을 구성하십시오.

      Sever Address: 프라이머리 비디오 세션 녹화 소프트웨어를 실행하는 컴퓨터의 IP 주소를 입력합니다.

      Service Ports: 위의 서버 포트 설정에서 프라이머리 서버의 CCVSR/HTTP/HTTPS 서비스 포트 번호를 입력합니다. 기본 서비스 포트는 9002/9080/9443입니다. 서비스 포트에 대한 추가 정보는 58페이지 서버 포트 설정에서 제공됩니다.

주의: 세컨더리 서버를 구성하려면 기본 서버에 로그인하십시오. 세컨더리 서버의 IP 주소 (예: https:₩₩192.168.0.100:9443)를 사용하여 접속하려고 하면 시스템에서 자동으로 기본 서버로 리디렉션됩니다.

- 서버 이중화
  - 프라이머리 서버에 장애가 발생하면 세컨더리 서버 중 하나가 대체 서버 역할을 하여 서비스를 항상 사용할 수 있도록 합니다. 이 경우 이 세컨더리 서버는 관리 설정 보기에 접속할 수 있습니다. 설정의 다른 세컨더리 서버는 여전히 스토리지 역할을 수행합니다. 프라이머리 서버가 다시 온라인 상태가 되면 대체 서버는 스토리지 서버로의 원래 역할로 재개됩니다.

- 프라이머리 서버가 영구적으로 고장난 경우 관리자는 세컨더리 서버의 웹 브라우저에 **https://127.0.0.1:9443**을 입력하고 서버 유형 (역할) 설정을 기본으로 변경하여 세컨더리 서버를 **프라이머리** 서버로 변경할 수 있습니다.

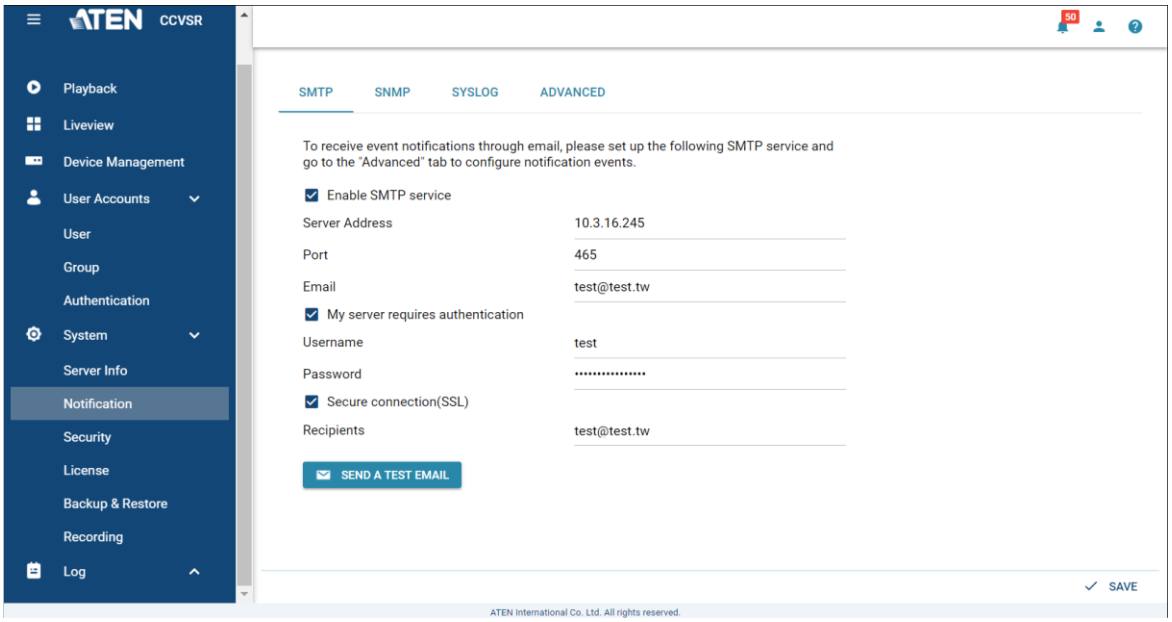
기타

체크박스에 체크하면 키 입력 녹화를 비활성화 합니다.

알림

알림 페이지는 알림 방식을 설정합니다.

SMTP



SMTP 서버에서 사용자에게 CCVSR 이메일 리포트를 받으려면 다음을 수행하십시오.

1. Enable SMTP service를 활성화하고, SMTP 서버의 IPv4 주소, IPv6 주소, 혹은 도메인 이름을 입력하십시오.
2. SMTP 포트를 입력하십시오.
3. Email 필드에 리포트가 전송되는 이메일 주소를 입력하십시오.

주의:

1. 필드에는 하나의 이메일 주소만 입력가능 하며 64 Byte를 초과할 수 없습니다.
2. 1 Byte = 영문자 1자

---

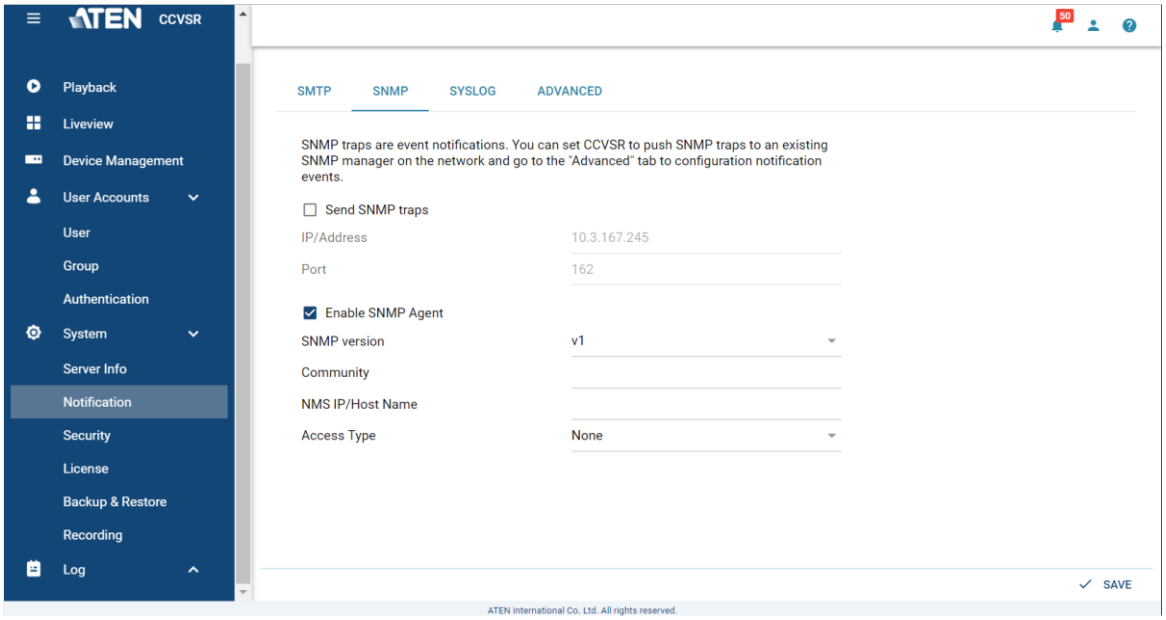
4. 서버가 인증을 요청하는 경우, My server requires authentication 체크 박스에 체크하고, Account Name, Password 필드에 적절한 정보를 입력하십시오.
5. 서버가 보안 SSL 연결을 요청하는 경우, My server requires secure connection (SSL) 체크 박스에 체크하십시오.

6. Recipients 필드에 리포트가 전송될 메일 주소를 입력하십시오.

주의: 사용자가 1개 이상의 이메일 주소로 리포트를 보내는 경우, 세미콜론 (;)으로 주소를 분리하십시오. 전체는 256 Byte를 초과할 수 없습니다.

7. 윈도우의 우측 하단 구석에 있는 Save를 클릭하여 환경 구성을 저장하십시오.

SNMP 서버



SNMP 트랩 알림을 사용하기를 원한다면 다음을 수행하십시오.

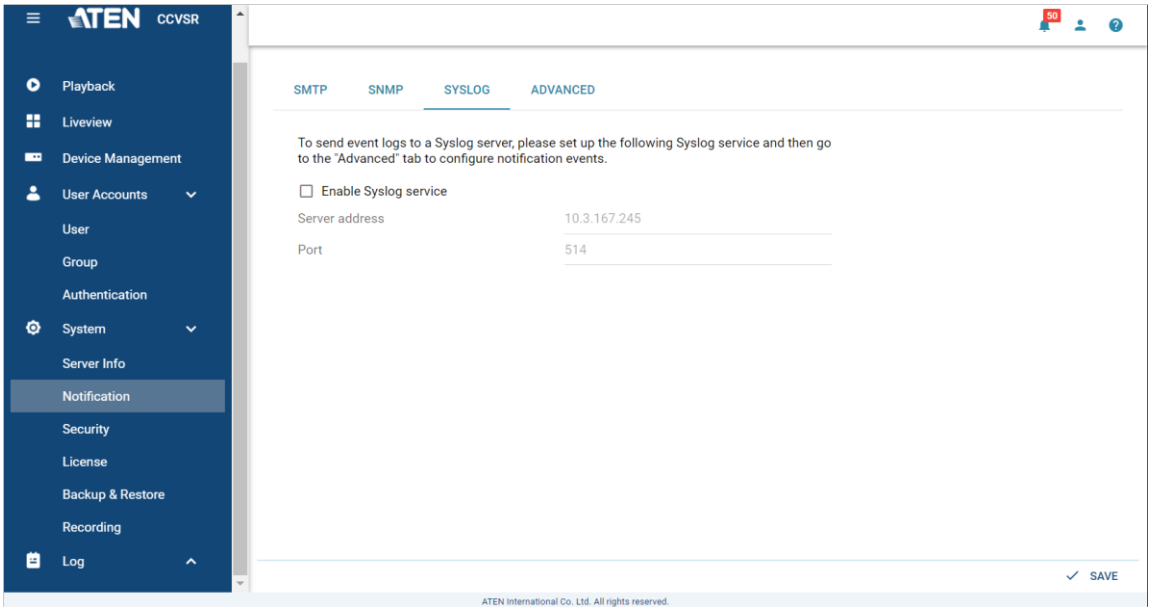
1. Send SNMP traps를 체크하십시오.
2. SNMP 트랩 이벤트를 알리기 위한 컴퓨터의 IPv4 주소, IPv6 주소 혹은 도메인 이름을 입력하십시오.
3. 포트 번호를 입력하십시오. 유효한 포트 범위는 1–65535 입니다.

주의: Log 탭 아래 알림 설정 페이지에서 SNMP 트랩 이벤트를 알리는 로그가 설정됩니다. 세부 사항은 64페이지 고급 (알림)을 참조하십시오.

4. Enable SNMP Agent를 체크하십시오.
5. 드롭 다운 메뉴를 클릭하여 SNMP 버전을 선택하십시오.
6. SNMP 버전에 필요한 경우 community 값을 입력하십시오.

7. NMS IP/Host Name.을 입력하십시오.
8. 드롭 다운 메뉴를 클릭하여 Access Type (접속 유형)을 선택하십시오.
9. 윈도우의 우측 하단 구석에 있는 Save를 클릭하여 환경 구성을 저장하십시오.

시스템로그 서버

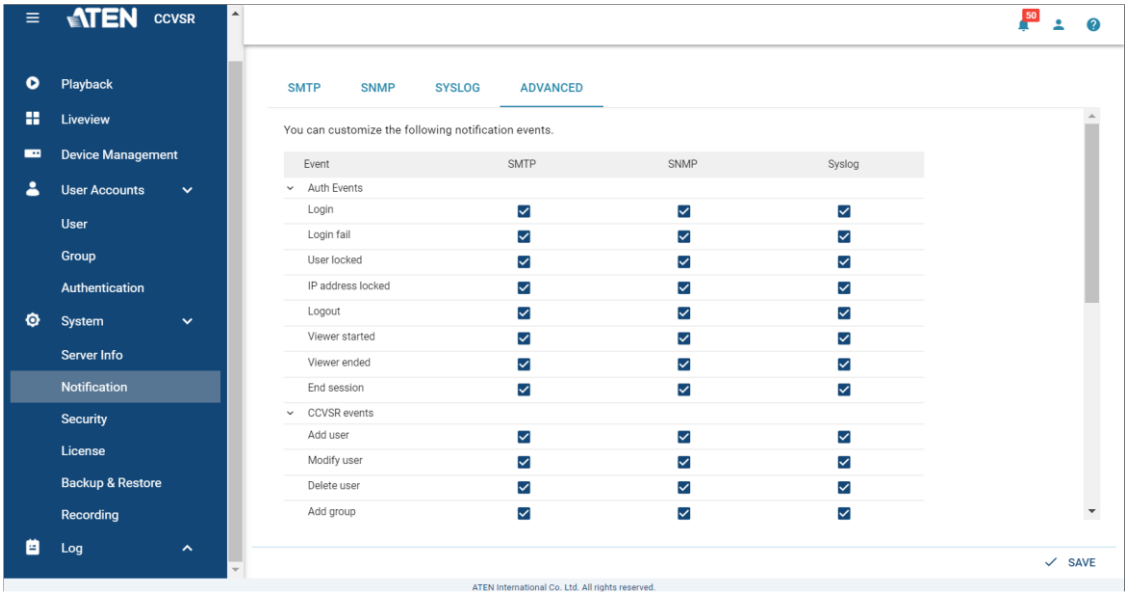


CCVSR에서 발생한 모든 이벤트를 기록하면 모든 이벤트를 저장하고 시스템로그 서버에 기록하려면 다음을 수행하십시오.

1. Enable Syslog service을 체크하십시오.
2. 시스템 서버의 IPv4 주소, IPv6 주소 혹은 도메인 이름을 입력하십시오.
3. 포트 번호를 입력하십시오. 유효한 포트 범위는 1–65535 입니다.
4. 윈도우의 우측 하단 구석에 있는 Save를 클릭하여 환경 구성을 저장하십시오.

고급 (알림)

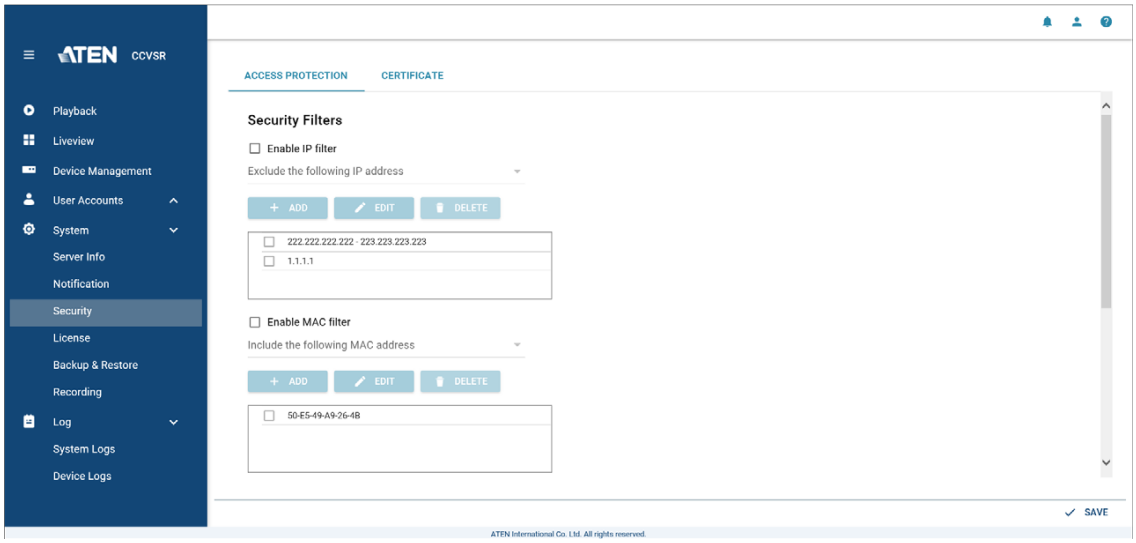
Advanced (Notification) 페이지는 알림을 트리거하는 이벤트와 알림을 보내는 방법을 결정할 수 있습니다.



알림은 SNMP 트랩, SMTP 이메일, SysLog 파일에 기록 또는 이 3가지 조합을 통해 보낼 수 있습니다. 체크 표시는 해당 열 제목에 지정된 방법으로 이벤트 알림이 허용됨을 나타냅니다. 빈 칸은 알림에 제한이 없음을 나타냅니다.

보안

보안 하위 메뉴는 2가지 탭이 있습니다.



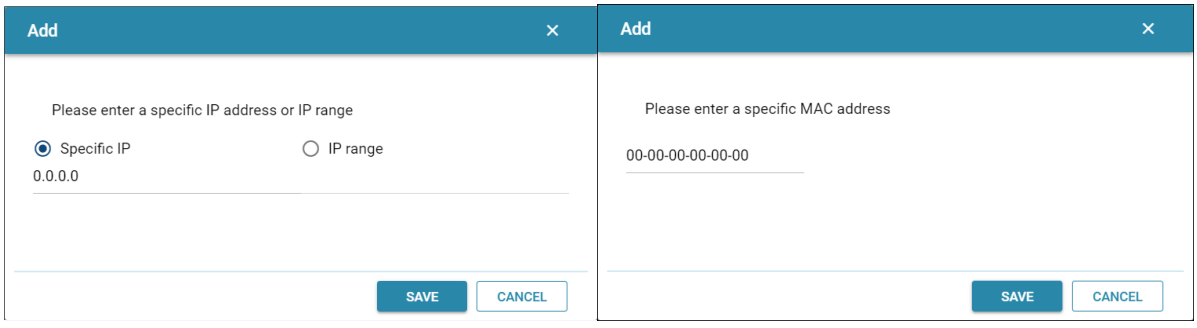
접속 보안

IP/MAC 필터링

IP/MAC 필터는 연결을 시도하는 클라이언트 컴퓨터의 IP/MAC 주소를 기반으로 비디오 세션 녹화 소프트웨어에 대한 접속을 제어합니다. 최대 100개의 IP 또는 MAC 필터가 허용됩니다. 필터가 구성되면, IP 필터 목록 박스에 나타납니다.

IP/MAC 필터링을 활성화하고 추가하려면

1. Enable IP Filter or Enable MAC Filter 체크박스에 체크하십시오.
2. 드롭 다운 메뉴에서 Exclude the following IP/MAC address (다음 IP/MAC 주소 제외) 또는 Include the following IP/MAC address (다음 IP/MAC 주소 포함) 중에서 선택하십시오.
3. + ADD 버튼을 클릭하십시오.
   팝업 윈도우가 나타납니다.



4. IP 필터의 경우 Specific IP (특정 IP)와 IP range (IP 범위) 중에서 선택하십시오.
   MAC 필터의 경우 MAC 주소를 입력하십시오.
5. 특정 IP의 경우 IP를 입력하십시오. IP 범위의 경우 첫 번째 필드에 IP 범위의 첫 번째 IP를 입력하고 두 번째 필드에 두 번째 IP를 입력하십시오.
6. 필터링하려는 추가 IP/MAC 주소에 대해이 단계를 반복하십시오.
7. Save를 클릭하십시오.

IP/MAC 필터링을 편집하려면, IP / IP range / MAC address를 체크하고 

버튼을 클릭하십시오. 65페이지에서 설명한대로 구성하십시오.

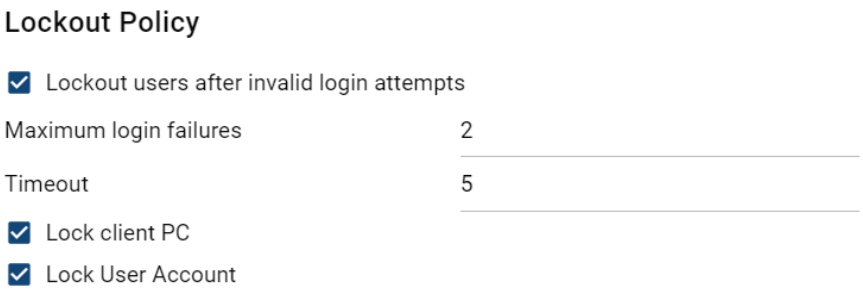
IP/MAC 필터링을 삭제하려면, IP / IP range / MAC address를 체크하고 

버튼을 클릭하십시오.

◆ IP 필터/MAC 필터 충돌
   IP 필터와 MAC 필터 사이에 충돌이 있는 경우 (즉, 컴퓨터의 주소가 한 필터에 의해 허용되지만 다른 필터에 의해 차단되는 경우) 차단 필터가 우선합니다. (컴퓨터의 접속이 차단됨)

락아웃 정책

보안 강화를 위해 관리자는 잠금 정책 섹션을 사용하여 사용자가 성공적으로 로그인하지 못할 때 발생하는 상황을 관리하는 정책을 설정할 수 있습니다.



락아웃 정책을 설정하려면 Lockout users after invalid login attempts (유효하지 않은 로그인 시도 후 사용자 락아웃)을 체크합니다. (기본값은 로그인 실패 활성화) 항목의 의미는 아래 테이블에서 설명합니다.

항목	설명
Maximum login failures	사용자를 락아웃 하기 전에 허용 가능한 로그인 실패 횟수를 입력합니다. 기본 값은 5 입니다.
Timeout	허용된 실패 횟수를 초과한 후 다시 로그인을 시도하기 전에 원격 컴퓨터가 기다려야하는 시간을 설정합니다. 기본값은 3 분입니다.

항목	설명
Lock Client PC	이 기능을 활성화 (선택)하면 허용된 실패 횟수를 초과한 후 로그인을 시도하는 컴퓨터가 자동으로 잠깁니다. 해당 컴퓨터의 로그인은 허용되지 않습니다. 기본값은 활성화입니다. **주의**: 이 기능은 클라이언트 컴퓨터의 IP 와 관련이 있습니다. IP 가 변경되면 컴퓨터가 더 이상 잠기지 않습니다.
Lock Account	이것이 활성화 (체크)되면 허용된 실패 횟수를 초과한 후 로그인을 시도하는 사용자가 자동으로 잠깁니다. 실패한 사용자 이름 및 비밀번호의 로그인은 허용되지 않습니다. 기본값은 활성화입니다.

주의: 잠금 정책이 활성화되지 않은 경우 사용자는 제한없이 무제한 로그인을 시도할 수 있습니다. 보안을 위해 이 기능을 활성화하고 락아웃 정책을 활성화하는 것이 좋습니다.

Block List: 이 버튼을 클릭하면 윈도우가 열립니다. 이 윈도우에는 잠긴 계정이 포함됩니다.

계정 잠금을 해제하려면 IP 주소를 확인하고 Unlock 버튼을 클릭합니다.

로그인 문자열

Login String 항목 필드를 통해 관리자는 사용자가 브라우저를 사용하여 비디오 세션 레코더에 접속할 때 IP 주소에 추가해야 하는 로그인 문자열 (IP 주소 외에)을 지정할 수 있습니다.
예를 들어 192.168.0.126이 IP 주소이고 atenccvsr이 로그인 문자열 인 경우 사용자는 다음을 입력해야 합니다.

192.168.0.126:9443/atenccvsr

주의: 1. 사용자는 IP 주소와 문자열 사이에 (/)를 넣어야 합니다.
2. 여기에 로그인 문자열을 지정하지 않으면 누구나 IP 주소만 사용하여 비디오 세션 레코더 로그인 페이지에 접속할 수 있습니다. 이로 인해 설치가 덜 안전해질 수 있습니다.

문자열에는 다음 문자가 허용됩니다.

0–9 a–z A–Z ~ ! @ $ & * ( ) _ - = + [ ].

다음 문자는 허용되지 않습니다.

% ^ " : / ? # ₩ ' { } ; ' < > [Space]

복합 문자 (É Ç ñ ... 등)

보안을 위해이 문자열을 가끔 변경하는 것이 좋습니다.

윈도우 우측 하단에 있는 Save을 클릭하여 환경 구성을 저장합니다.

증명서

개인 인증서

보안 (SSL) 연결을 통해 로그인 할 때 서명된 인증서를 사용하여 사용자가 의도한 사이트에 로그인하고 있는지 확인합니다. 보안 강화를 위해 인증서 섹션에서는 기본 ATEN 인증서가 아닌 개인 암호화 키와 서명된 인증서를 사용할 수 있습니다.

개인 인증서를 생성하는 방법에는 2가지 있습니다. 자기 서명 인증서 생성 및 서드 파트 인증 기관(CA) 서명 인증서 가져오기가 있습니다.

- 자기 서명 인증서 생성

  사용자만의 자기 서명 인증서를 생성하려는 경우, 무료 유틸리티 - openssl.exe – 를 웹에서 다운로드 받아 사용할 수 있습니다. 사용자 개인 키 및 SSL 인증서를 생성하기 위해 OpenSSL을 사용하는 것에 관련된 세부 사항은 102페이지 자기 서명 개인 인증서를 참조하십시오.

- CA 서명 SSL 서버 인증서 획득

  최고의 보안을 위해, 서드 파트 인증 기관(CA) 서명 인증서를 사용할 것을 권장합니다. 써드 파티 서명 인증서를 얻으려면, CA(인증 기관) 웹사이트로 가서 SSL 인증서를 지원하십시오. CA가 사용자에게 인증서를 보낸 후에, 사용자 컴퓨터에 저장하십시오.

- 개인 인증서 불러오기

  개인 인증서를 불러오려면 다음을 수행하십시오.

  1. Private Key의 오른쪽에 있는 ＋를 클릭하고, 개인 암호 키 파일이 있는 위치를 탐색하고 선택하십시오.
  2. Certificate의 오른쪽에 있는 ＋를 클릭하고, 사용자의 인증서 파일이 있는 위치를 탐색하고 선택하십시오.
  3. **Upload**를 클릭하고 과정을 끝마칩니다.

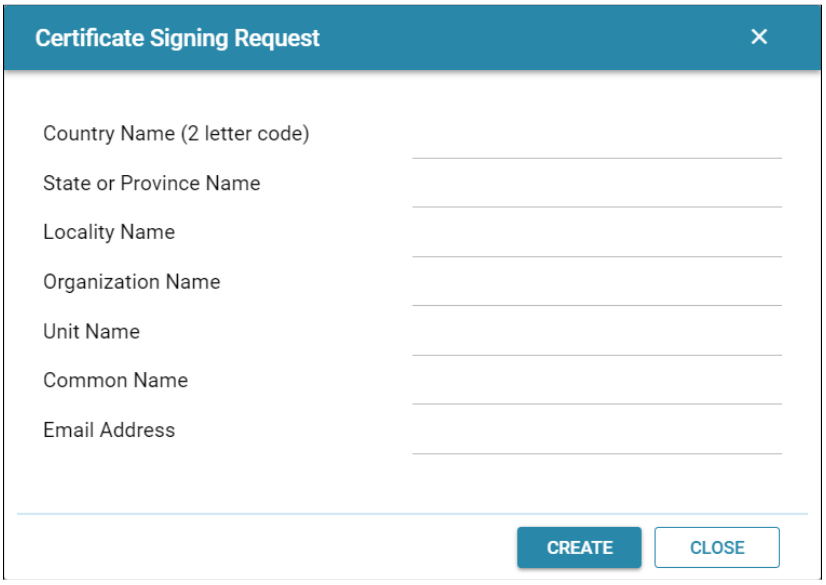
주의: 1. **Restore Default**를 클릭하면 기본 ATEN 인증서를 사용하는 방식으로 복구합니다.
2. 개인 암호 키 및 서명 인증서는 반드시 동시에 불러와야 합니다.

인증서 서명 요청

인증서 서명 요청(CSR) 섹션은 CA 및 서명 SSL 서버의 자동화된 인증 획득 및 설치를 제공합니다.

이 작업을 수행하려면 다음을 수행하십시오.

1. **Create CSR**를 클릭하십시오. 다음 대화 상자가 나타납니다.



2. 아래 테이블에 있는 예제 정보에 따라 이 양식(사용자 지역에 유효한 목록)을 채우십시오.

아이템	설명
Country (2 letter code)	TW
State or Province	대만
Locality	타이페이
Organization	회사명
Unit	부서명
Common Name	mycompany.com **주의**: 인증서가 유효하도록 하기 원하는 사이트의 정확한 도메인 이름을 입력해야 합니다. 사이트의 도메인 이름이 www.mycompany.com 인 경우, mycompany.com 만 입력하면 인증서가 유효하지 않습니다.
Email Address	administrator@yourcompany.com

3. 양식(모든 필드에 채워 넣어야 함) 작성이 완료된 후, **Create**를 클릭하십시오.
   사용자가 제공한 정보에 따른 자기 서명 인증서는 지금 CCVSR에 저장됩니다.
4. Get CSR을 클릭하고, 서명서 파일(csr.cer)을 사용자 컴퓨터의 편리한 위치에 저장하십시오.

이 파일은 사용자가 외부 인증 기관에게 서명 SSL 인증서에 적용하도록 합니다.

5. 인증 기관이 인증서를 보낸 후에, 사용자 컴퓨터의 편리한 위치에 저장하십시오. + 를 클릭하여 파일을 찾은 후, **Upload**를 클릭하여 파일을 CCVSR에 저장하십시오.

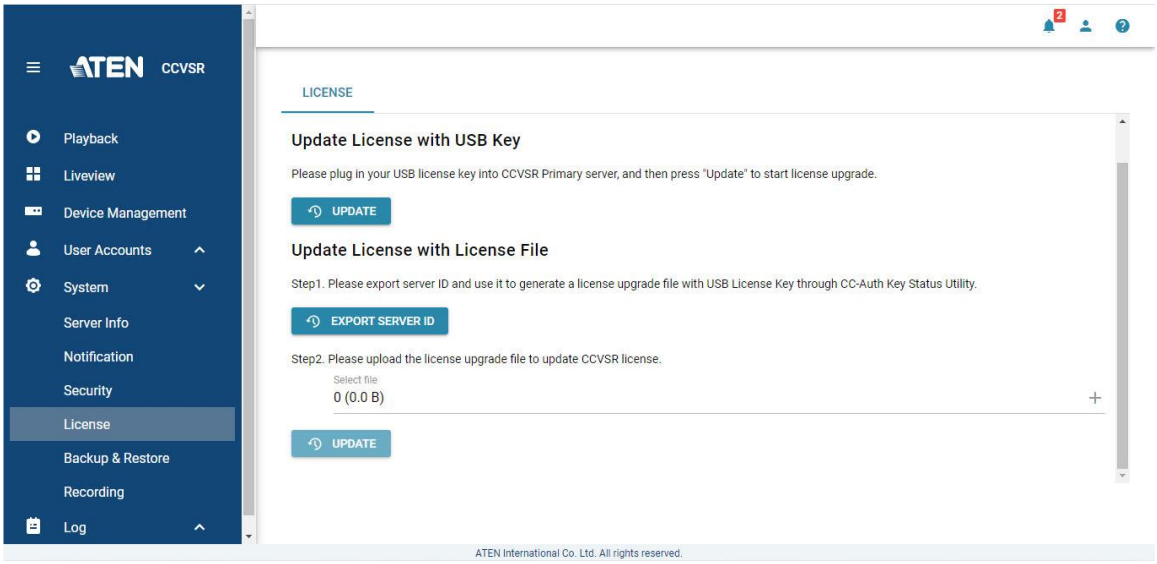
주의: 파일을 업로드 할 때, CCVSR는 특정 정보가 여전히 일치하는지 확인하기 위해 파일을 체크합니다. 일치하는 경우, 파일은 수락되고, 그렇지 않으면 거절됩니다.

인증서를 제거하려면 (혹은 예를 들어 도메인 이름이 변경되어 새로운 것으로 대체하려면) 간단히 **Remove**를 클릭하십시오.

라이센스

CCVSR 라이센스는 사용 중인 노드와 가용 노드를 포함하여, 해당 CCVSR 설치 환경에서 허용되는 세컨더리 서버 및 노드의 총 수량을 제어합니다.

CCVSR 소프트웨어 설치가 완료되면 기본 서버 1대에 대한 기본 라이센스가 자동으로 제공됩니다. 더 많은 CCVSR 노드 및 세컨더리 서버를 추가하려면 라이센스를 업그레이드해야 합니다.



라이센스를 업그레이드하려면 대리점에 문의하여 원하는 노드 및 세컨더리 서버 수량에 맞는 라이센스 키를 구입하십시오.

구입한 USB 라이센스 키를 수령한 후, 다음 두 가지 방법 중 하나를 사용하여 CCVSR 라이센스를 업그레이드할 수 있습니다:

- USB 라이센스 키를 기본 서버에 직접 삽입하여 업그레이드합니다.
- USB 라이센스 키를 직접 삽입하지 않고 업그레이드합니다.

USB 키로 라이센스 업그레이드

1. CCVSR 서버의 USB 포트에 라이센스 키를 삽입하십시오.
2. CCVSR 애플리케이션에 로그인한 후 **License**로 이동하고 Update License with USB Key 아래의 **Update**를 클릭하십시오.

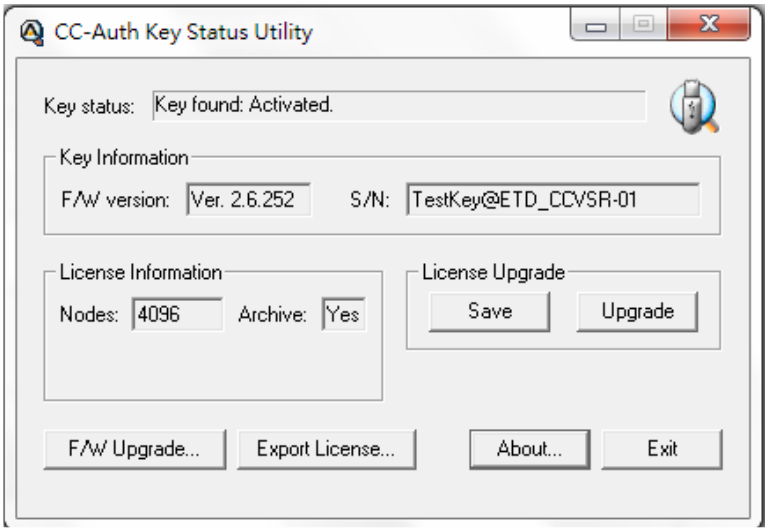
주의: 1. 업그레이드를 완료하면 SB 포트에 라이센스 키를 연결해 둘 필요가 없습니다. 차후 업그레이드가 필요할 수 있으므로 키를 안전한 장소에 보관하십시오.

2. USB 라이센스 키를 잃어버린 경우, 판매자에게 연락해 새로 받으십시오. 키의 시리얼 번호를 제공하면 새 키에 분실한 키에 저장된 모든 정보가 담깁니다.

라이센스 파일로 라이센스 업그레이드

이 방법은 USB 연결이 금지된 제한 구역과 같이 CCVSR 프라이머리 서버에 USB 라이센스 키를 직접 삽입하기 불편한 경우에 유용합니다.

1. CCVSR 프라이머리 서버에서 **License**로 이동하여 **Export Server ID** (서버 ID 내보내기)를 클릭해 서버 및 설치 세부 정보가 포함된 *.sid 서버 ID 파일을 생성합니다. 해당 파일을 내보내 별도의 PC에 저장하십시오.
2. 별도의 PC에 USB 라이센스 키를 삽입하십시오.
3. CC-Auth Key Status Utility를 열고 아래 그림과 같이 **Export License**를 클릭하십시오. 1단계에서 생성한 서버 ID 파일을 찾아 선택하라는 메시지가 표시됩니다. 완료되면 *.lic 라이센스 업그레이드 파일이 생성됩니다.



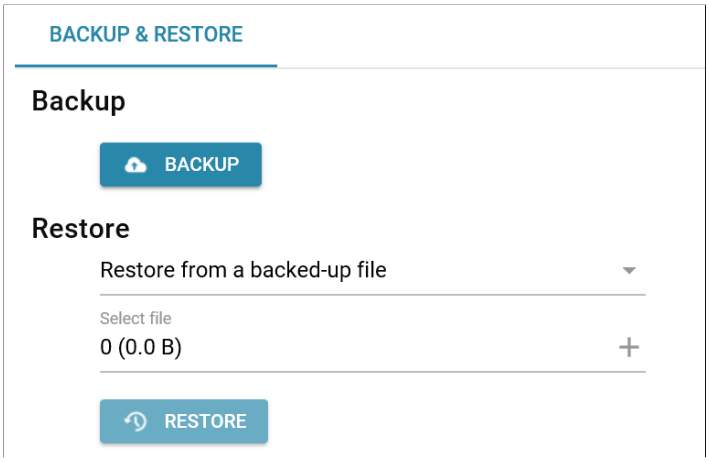
4. *.lic 파일을 CCVSR 프라이머리 서버로 가져와 저장한 다음, 라이센스 파일을 사용하여 라이센스 업데이트 아래의 +를 클릭하여 해당 파일을 찾으십시오.
5. **Update**를 클릭하여 라이센스 업그레이드를 시작하십시오.

주의: 라이센스 업그레이드 파일은 서버 ID 파일이 생성된 해당 CCVSR 서버의 라이센스를 업그레이드하는 데만 사용할 수 있습니다.

라이센스가 업그레이드되면 (구매한 라이센스 수에 따라) 추가 CCVSR 및/또는 노드를 설치하여 사용할 수 있으며, 이들은 네트워크를 통해 서로 통신하고 연동하여 작동합니다.

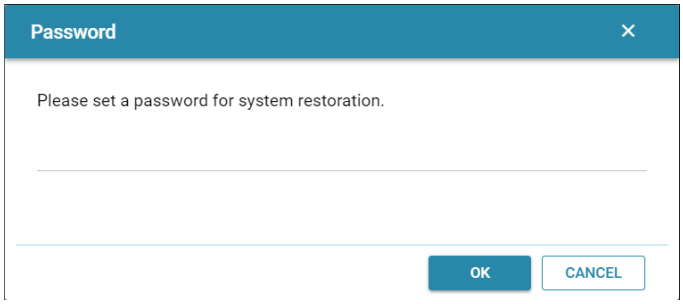
백업 및 복구

Backup & Restore 페이지는 시스템 구성 설정 및 사용자 계정 정보를 파일 또는 시스템에서 생성한 체크 포인트에 (또는 체크 포인트로부터) 백업 및 복원하는 데 사용됩니다. 2가지 섹션이 있습니다.



백업

백업 파일을 생성하려면 백업을 클릭하여 파일을 저장합니다. 암호를 입력하라는 창이 나타납니다.



암호를 사용하지 않으려면 Password 필드를 비워 둡니다. OK을 누르면 시스템 환경 구성을 백업합니다. 저장된 데이터 파일에는 현재 시스템 환경 구성과 모든 사용자 계정 정보가 포함됩니다.

복원

데이터를 복원하려면

1. 드롭 다운 메뉴에서 선택하여 구성을 복원할 위치를 선택하십시오. Restore from a backed-up file (백업된 파일에서 복원) 또는 Restore from a checkpoint (체크 포인트에서 복원) 중에서 선택하십시오.
2. 백업 파일의 경우, ＋ 을 클릭하고 파일을 선택하십시오.

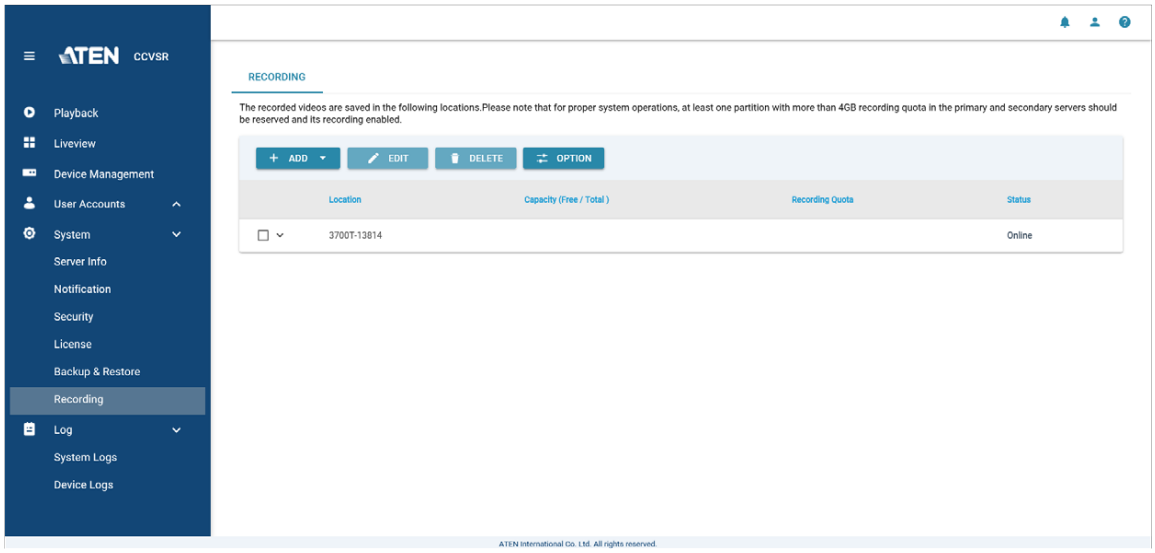
체크 포인트의 경우, 체크 포인트 목록에서 선택하십시오.

3. Restore를 클릭하십시오.

녹화

이 페이지에서는 대상 (프라이머리 서버, 세컨더리 서버 또는 네트워크 공유 폴더)을 선택하고 비디오 로그 파일을 저장할 수 있습니다. 세컨더리 CCVSR 서버는 다른 컴퓨터의 디스크 공간을 통합하기 위해 대체 컴퓨터에 비디오 로그 파일을 저장하는데도 사용됩니다. 세컨더리 CCVSR 서버로 동작하도록 세컨더리 컴퓨터를 설정하려면 59페이지 서버 유형을 참조하십시오.

Recording를 선택하면 다음 화면이 나타납니다.



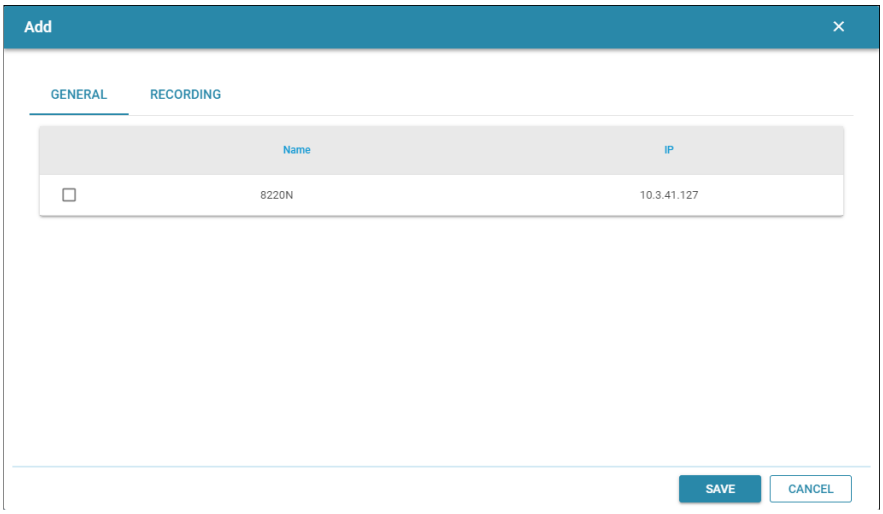
Recording 메뉴 페이지에서 다음을 수행할 수 있습니다.

- CCVSR 서버 추가 또는 삭제
- 네트워크 공유 폴더 추가 또는 삭제
- 녹화 위치 활성화 또는 비활성화
- 비디오 로그 파일에 대한 보관 정책 설정

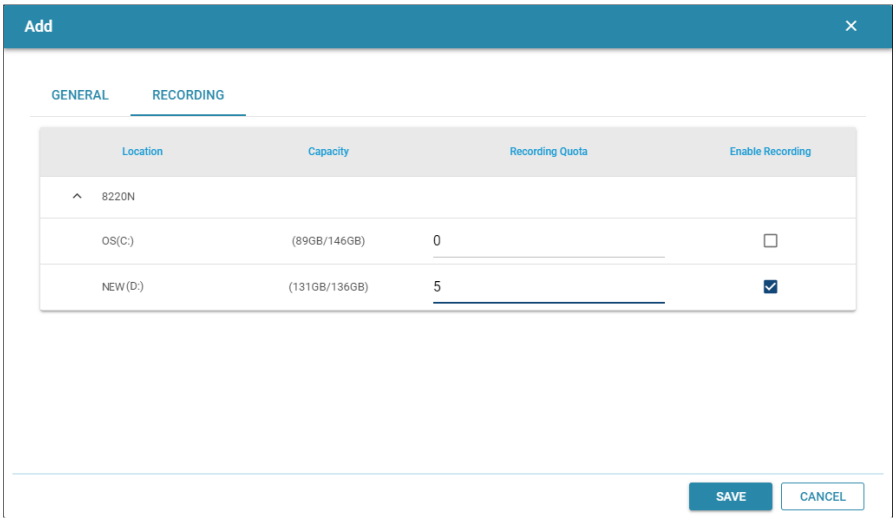
세컨더리 CCVSR 서버 추가

추가하려는 세컨더리 CCVSR 서버는 네트워크를 통해 사용할 수 있는 컴퓨터에 있어야합니다. CCVSR 서버를 추가하려면 다음을 수행하십시오.

1. Add를 클릭하십시오.
2. General 탭으로 이동하는 팝업 화면이 나타납니다.



3. 목록에서 CCVSR 서버 (프라이머리 서버와 동일한 LAN에 있음)를 선택하고 Recording 탭에서 **Next**를 클릭하십시오.

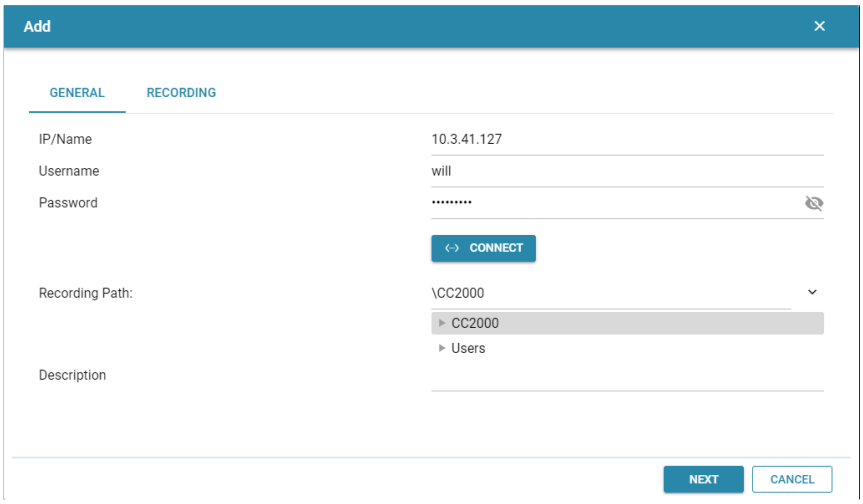


4. Enable Recording 열의 체크박스에 체크하여 녹화 위치를 선택하십시오. 녹화 할당량 열의 해당 필드에 값을 입력하십시오.
5. Save를 클릭하여 환경 구성을 저장하면 CCVSR 서버가 녹화 기본 페이지에 나타납니다.

네트워크 공유 폴더 추가

네트워크 공유 폴더를 추가하려면, 다음을 수행하십시오.

1. Add를 클릭하십시오.
2. General 탭으로 이동하는 팝업 화면이 나타납니다.



3. 다음 테이블을 사용하여 네트워크 폴더 위치에 유효한 상위 3개 항목의 정보를 입력합니다.

아이템	설명
IP/Name	네트워크 폴더를 공유하는 서버의 IP 주소를 입력합니다.
Username	공유 네트워크 폴더에 대한 접속 권한이 있는 사용자 이름을 입력합니다.
Password	암호를 입력합니다.

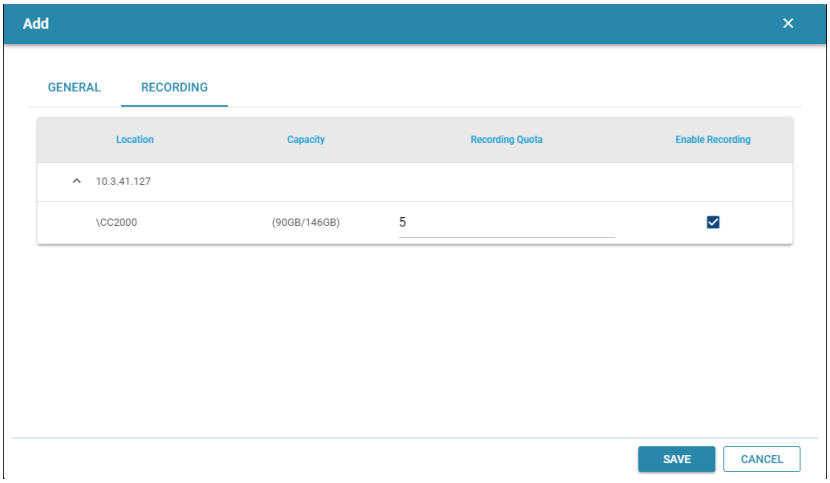
4. Connect을 클릭하여 경로 정보를 자동으로 검색합니다. 올바르게 검색되면 드롭 다운 메뉴에서 녹화 경로를 선택할 수 있습니다. 설명 항목에 설명을 입력할 수도 있습니다.

주의: SMBv2 및 v3가 지원되는지 확인하십시오.

또는 아래 테이블을 사용하여 나머지 정보를 입력할 수 있습니다.

아이템	설명
Recording Path	비디오 로그 파일을 저장할 서버의 폴더 위치를 입력합니다. 예: Share₩Department2₩Security₩VideoLogs
Description	네트워크 폴더에 대한 설명을 입력합니다.

5. Recording 탭에서 Next를 클릭하십시오.

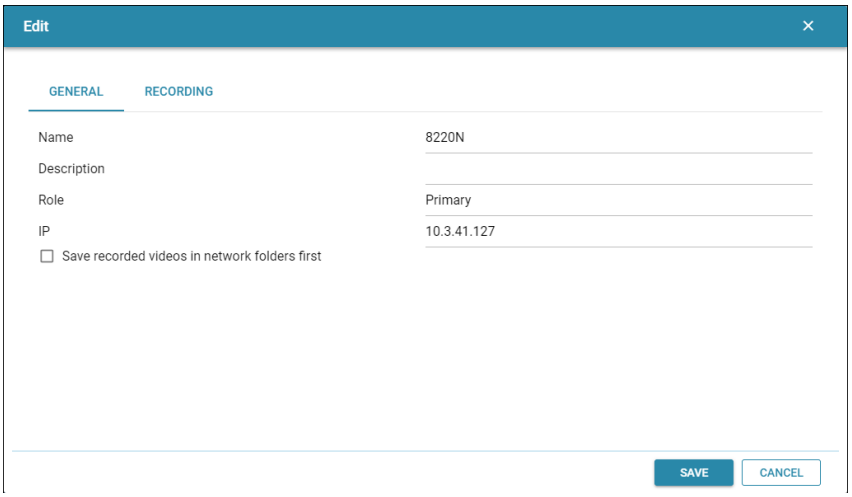


6. Enable Recording 열의 체크박스에 체크하여 기록 위치를 선택하십시오. 기록 할당량 열의 해당 필드에 값을 입력하십시오.
7. Save를 클릭하여 환경 구성을 저장하면 네트워크 공유 폴더가 녹화 기본 페이지에 나타납니다.

세컨더리 CCVSR 서버 편집

CCVSR 서버를 편집하려면 다음을 수행하십시오.

1. Recording 페이지에서 CCVSR 서버의 체크박스에 체크하십시오.
2. 아래 팝업 페이지에서 Edit를 클릭하십시오.

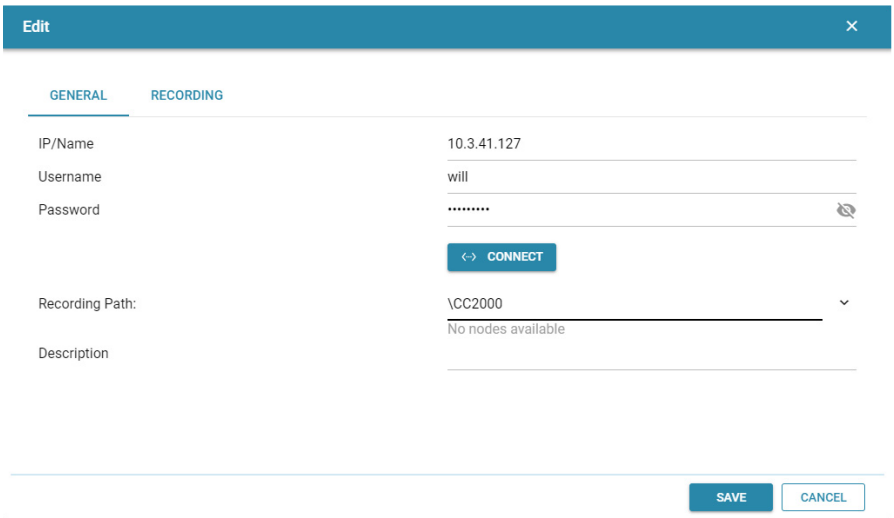


3. CCVSR 서버의 이름과 설명을 편집하고 여기에서 Save recorded videos in network folders first (먼저 네트워크 폴더에 녹화된 비디오 저장을 활성화 (체크) / 비활성화 (체크해제) 할 수 있습니다. Recording 탭을 클릭하여 옵션을 편집하십시오. (예: 녹화 비활성화)
4. 변경한 후 Save를 클릭하여 환경 구성을 저장하십시오.

네트워크 공유 폴더 편집

네트워크 공유 폴더를 편집하려면 다음을 수행하십시오.

1. Recording 페이지에서 공유 네트워크 폴더의 체크박스에 체크하십시오.
2. 아래 팝업 페이지에서 Edit를 클릭하십시오.



3. 사용자 이름과 암호를 편집하고 Connect을 다시 클릭하여 경로 정보를 검색하고 드롭 다운 메뉴에서 녹화 경로를 다시 선택할 수 있습니다. Recording 탭을 클릭하여 옵션을 편집하십시오. (예: 녹화 비활성화)
4. 변경한 후 Save를 클릭하여 환경 구성을 저장하십시오.

세컨더리 CCVSR 서버/네트워크 공유 폴더 삭제

CCVSR 서버/네트워크 공유 폴더를 삭제하려면 다음을 수행하십시오.

1. Recording 페이지에서 CCVSR 서버/공유 네트워크 폴더의 체크박스에 체크하십시오.
2. Delete를 클릭하십시오.

옵션 - 보관 정책

Continue recording without overwriting any video (비디오를 덮어쓰지 않고 계속 녹화)를 선택한 경우, CCVSR은 녹화 할당량에 도달할 때까지 녹화를 계속합니다.

Keep the videos within (days) ((일) 이내의 동영상 보관)과 숫자 (1-1825)를 입력하면 입력한 숫자보다 오래된 동영상이 삭제됩니다.

예를 들어, 7일을 입력한 경우 비디오 세션 녹화 소프트웨어는 7일이 지난 녹화분을 삭제하고 지난 7일 동안 생성된 모든 비디오 파일은 그대로 둡니다.

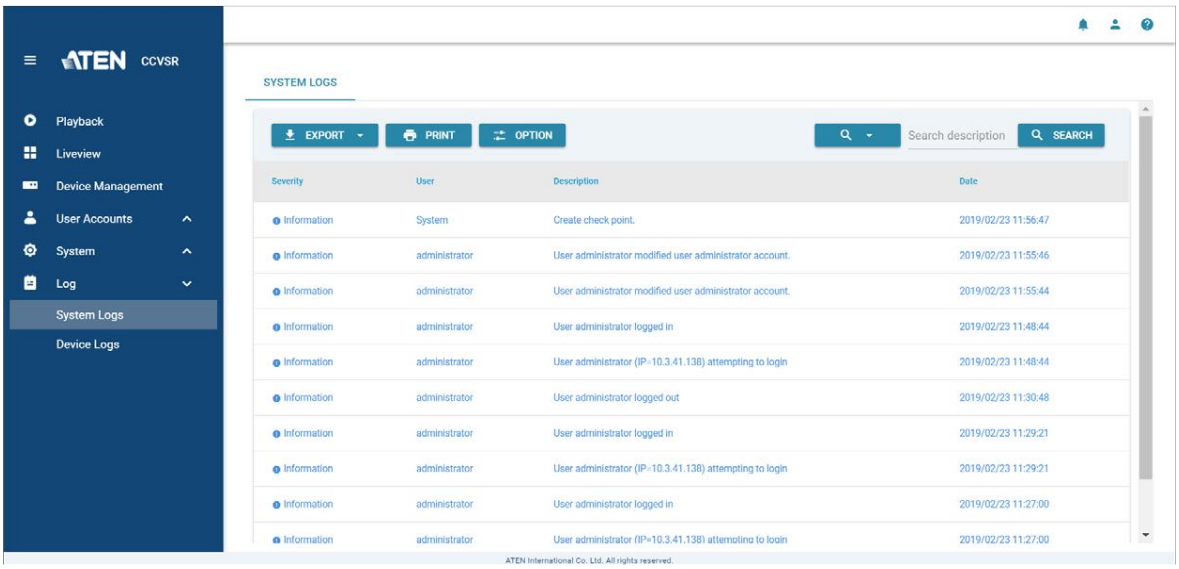
보관 정책은 매일 00:00에 새로 갱신합니다.

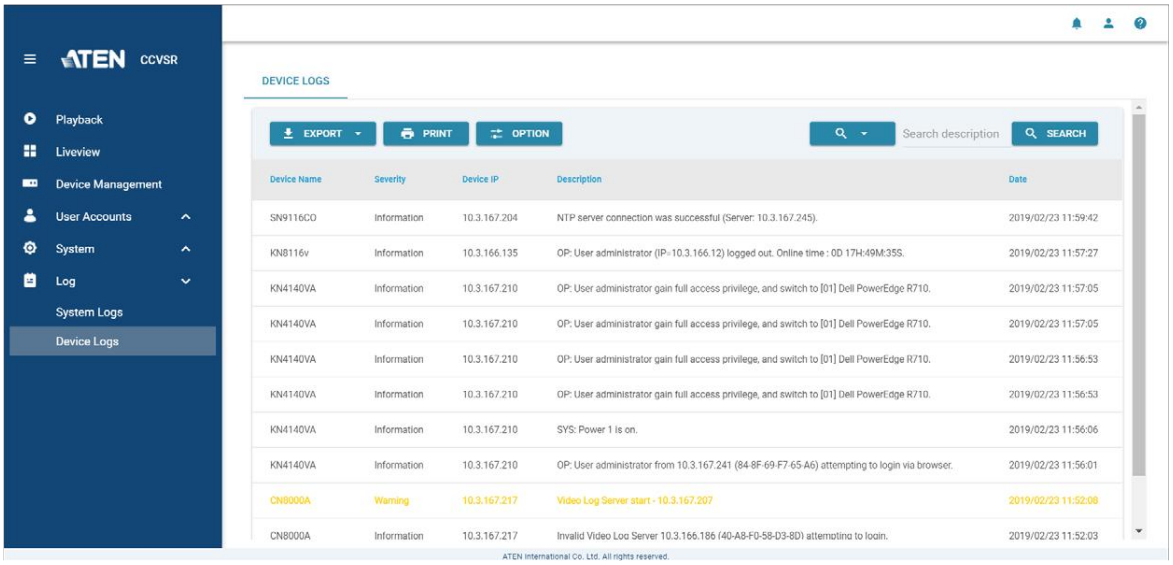
9 장

로그

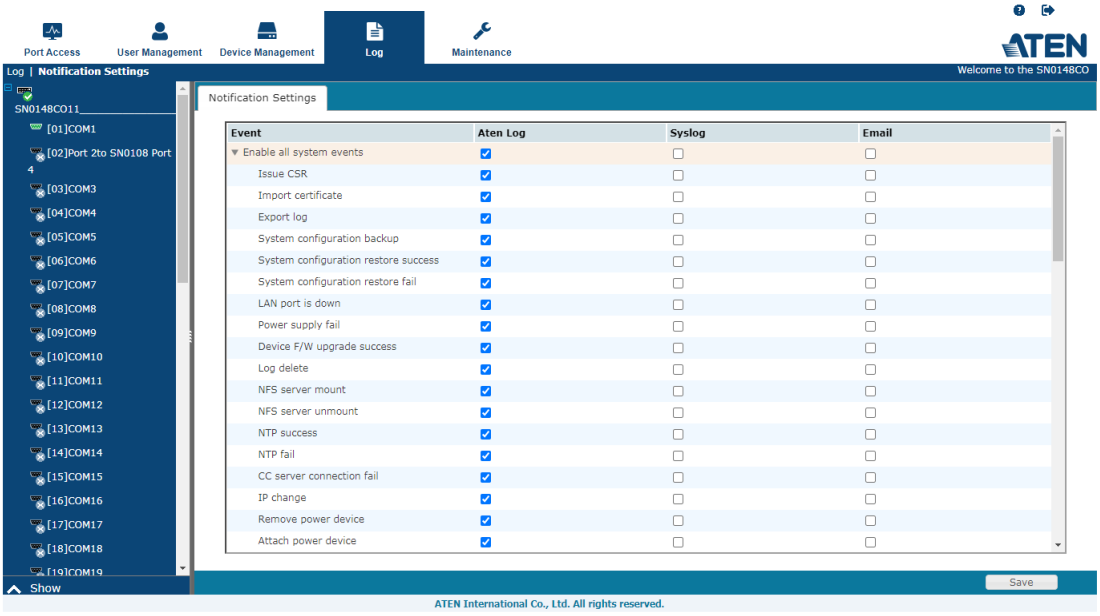
개요

비디오 세션 녹화 소프트웨어는 발생하는 모든 이벤트를 기록합니다. 로그의 내용을 보려면 로그를 클릭하여 로그 기본 메뉴를 확장하고 보려는 로그 유형을 클릭하여 선택하십시오. 시스템 로그 및 장치 로그는 각각 아래와 같습니다.





주의: 추가된 시리얼 콘솔 서버의 로그를 수신하려면 시리얼 콘솔 서버의 자신의 알림 페이지에서 알림 설정을 활성화했는지 확인하십시오. 예 (SN0148CO 장치 인터페이스)는 다음과 같습니다.



로그 정보

시스템 및 장치 로그 테이블은 비디오 세션 녹화 소프트웨어에서 발생하는 이벤트를 표시하고 시간, 심각성, 사용자, 설명의 항목이 있는 정렬 열을 제공합니다. 항목을 클릭하여 이벤트 순서를 정렬합니다.

테이블의 오른쪽 하단에서 표시된 항목 (행) 수를 선택하고 항목의 이전/다음 페이지로 이동할 수 있습니다.

표시된 항목 수를 선택하려면 드롭 다운 메뉴를 클릭하고 메뉴에서 선택합니다.

항목의 이전 또는 다음 페이지로 이동하려면 < 또 는 >를 클릭하십시오.

로그 내보내기

내보내기 버튼을 사용하여 현재 페이지의 로그 또는 모든 로그를 내보낼 수 있습니다. 드롭 다운 메뉴를 클릭하고 옵션 중 하나를 선택합니다. 로그 파일은 .dat 형식으로 저장됩니다.

로그 출력

출력 버튼을 사용하여 로그를 출력할 수 있습니다. 클릭하면 다음과 같이 출력 가능한 로그 페이지가 표시됩니다.

System Logs

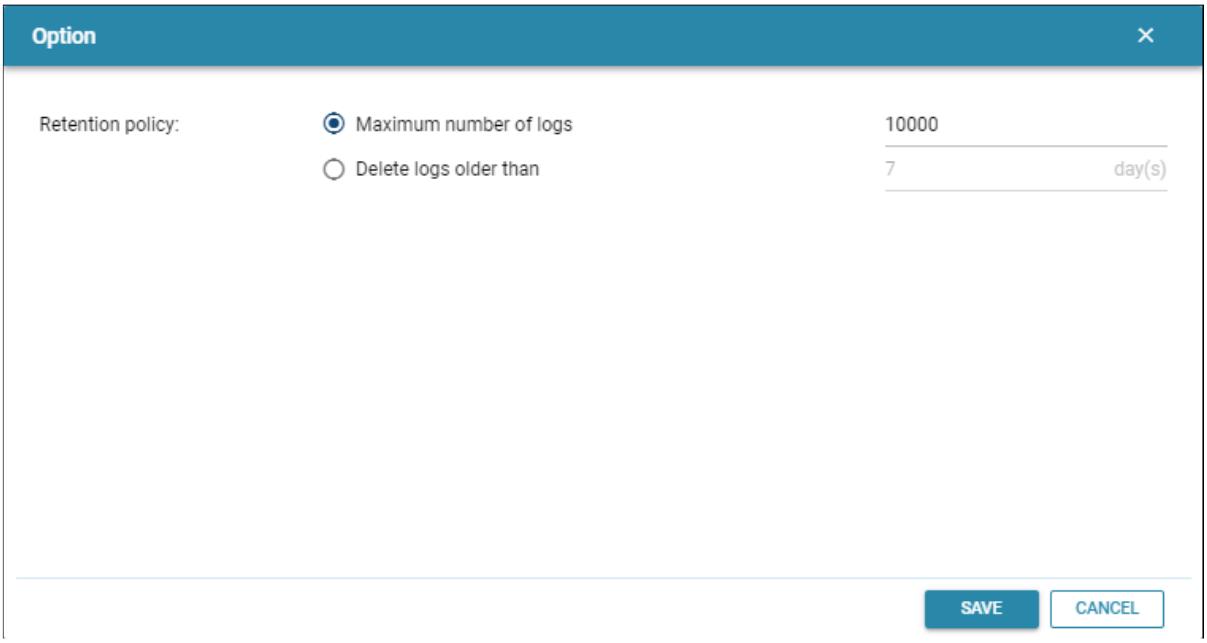
PRINT CLOSE

No.	Severity	User	Description	Date
0	Information	administrator	User administrator logged in	2019/03/27 14:03:47
1	Information	administrator	User administrator (IP=10.3.41.138) attempting to login	2019/03/27 14:03:47
2	Information	administrator	User administrator logged out	2019/03/27 14:02:49
3	Information	administrator	User administrator logged in	2019/03/27 13:07:33
4	Information	administrator	User administrator (IP=10.3.41.138) attempting to login	2019/03/27 13:07:33
5	Information	administrator	User administrator logged out	2019/03/27 11:51:49
6	Information	administrator	User administrator logged in	2019/03/27 11:21:49
7	Information	administrator	User administrator (IP=10.3.41.138) attempting to login	2019/03/27 11:21:49
8	Information	System	System start.	2019/03/27 11:21:34
9	Information	System	Create check point.	2019/03/27 11:21:07

시스템의 출력 설정을 위해 Print를 클릭하거나 이 페이지를 종료하려면 Close를 클릭하십시오.

옵션

옵션 버튼을 클릭하여 로그의 보관 정책을 설정할 수 있습니다.



시스템은 기본적으로 최대 10,000개의 로그 이벤트를 유지하도록 설정되어 있습니다. 시스템은 가장 오래된 항목을 덮어 씁니다. 여기에 다른 번호를 입력 할 수 있습니다.
일 수 내에 로그 이벤트를 유지하려면 다음보다 오래된 로그 삭제를 선택하고 값 (일)을 입력합니다. 입력한 값보다 오래된 로그 항목은 자동으로 삭제됩니다.

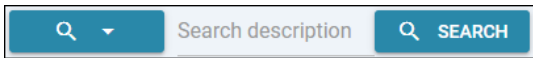
로그 검색

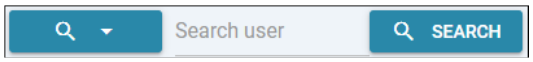
Search 기능을 사용하면 일반 검색 또는 고급 검색을 수행할 수 있습니다.

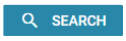
일반 검색

일반 검색의 경우 설명 또는 사용자에 따라 검색할 수 있습니다.

1. 드롭 다운 메뉴 버튼  을 클릭하십시오.
2. 설명 (Description) 또는 사용자 (User)를 선택하십시오. 검색 필드에 선택 항목이 표시됩니다.





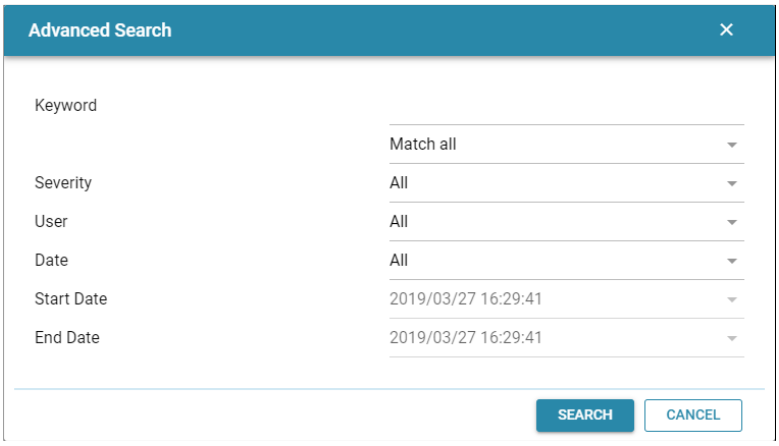
3. 검색하려는 정보를 입력 필드에 입력하고 

버튼을 클릭합니다.

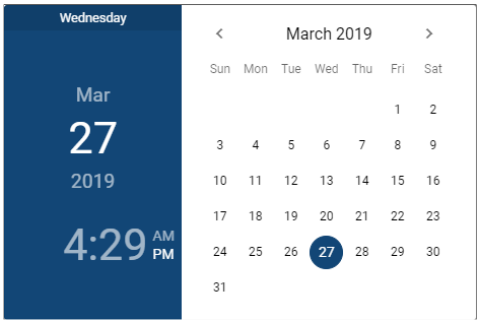
고급 검색

고급 검색의 경우:

1. 드롭 다운 메뉴 버튼  을 클릭하십시오.
2. 아래 팝업 창에 대해 Advanced Search을 선택하십시오.



고급 검색 사용 방법은 아래 테이블을 참조하십시오.

필드	설명
Keyword	특정 단어 혹은 문자열을 필터링 합니다. Information 텍스트 박스에 단어 혹은 문자열을 입력하십시오. 오로지 단어 혹은 문자열을 포함하고 있는 이벤트만이 표시됩니다. 와일드 카드(1개 글자인 경우 ?, 여러 글자인 경우 *)만 허용되므로 1개 이상의 포트가 목록에 나타날 수 있습니다. 예를 들어, h*ds 를 입력하면 hands와 hoods와 매치됩니다. h?nd 를 입력하면 hand 및 hind를 보여주지만 hard는 아닙니다. h*ds 혹은 h*ks는 hands 및 hooks를 리턴합니다.
Match all / Match any	드롭 다운 메뉴를 클릭하여 Match all와 Match any 중에서 선택합니다. **Match all**: 검색은 지정된 모든 정보를 충족해야 합니다. **Match any**: 검색은 지정된 정보 중 하나만 충족하면 됩니다.
Severity	드롭 다운 메뉴를 클릭하여 심각도 레벨로 검색합니다. 사용 가능한 항목에는 정보 (Information), 경고 (Warning) 및 위험 (Critical)이 포함됩니다.
User	드롭 다운 메뉴를 클릭하여 사용자 유형에 따라 검색합니다. 사용 가능한 항목에는 모두 (All), 시스템 (System) 및 관리자 (administrator)가 포함됩니다.
Date	드롭 다운 메뉴를 클릭하여 날짜 범위에 따라 검색합니다. 사용 가능한 항목은 모두 (All) 및 범위 (Range)입니다. Range를 선택하면 다음 두 항목 (시작일 (Start Date) 및 종료일 (End Date))이 켜지고 사용할 수 있습니다. **Start Date**: 드롭 다운 메뉴에서 특정 날짜와 시간을 선택합니다. 드롭 다운 메뉴를 클릭하면 다음과 같이 날짜 및 시간 선택이 표시됩니다.  위 그림의 왼쪽에 표시된 것처럼 월의 날짜가 켜져 그림 왼쪽에 반영된 대로 날짜를 선택하고 있음을 나타냅니다. 다른 선택 사항 (월, 년, 시, 분, 오전/오후)의 경우 변경하려는 흐리게 표시된 섹션을 클릭합니다. **End Date**: Start Date와 같은 선택 방법을 따릅니다.
Search	클릭하면 검색에 필터 선택을 적용합니다.
Cancel	클릭하면 고급 검색을 취소합니다.

10 장

CCVSR 아카이브 서버

개요

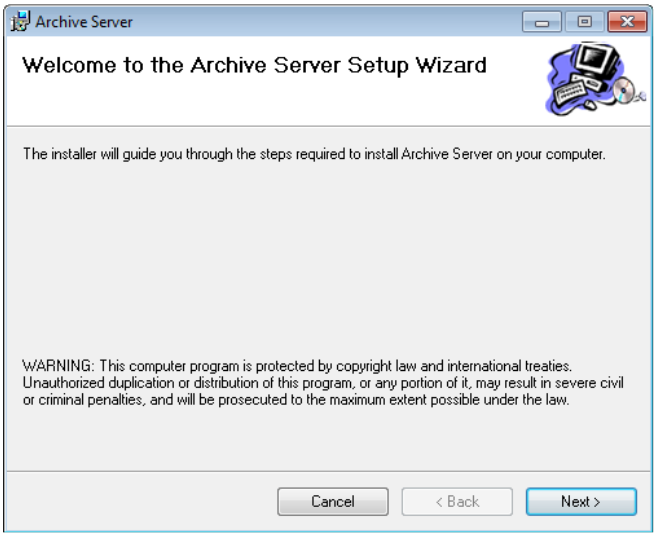
CCVSR 아카이브 서버를 사용하면 CCVSR 서버에서 생성된 데이터를 저장, 재생, 가져오기, 내보내기를 수행할 있습니다. 소프트웨어는 기본 CCVSR 서버의 비디오 로그 파일 사본을 기본 시스템과 별도로 구성된 아카이브로 자동 전송합니다. 이렇게 하면 기본 시스템에서 오래된 파일을 제거할 수 있지만 나중에 사용할 수 있도록 모든 비디오를 안전하게 보관할 수 있습니다. 아카이브 서버는 백그라운드에서 실행되며 15분마다 아카이브를 자동으로 업데이트합니다. 이 소프트웨어를 구입하려면 10페이지 라이센스를 참조하십시오.

CCVSR 아카이브 서버 설치

설치 시작

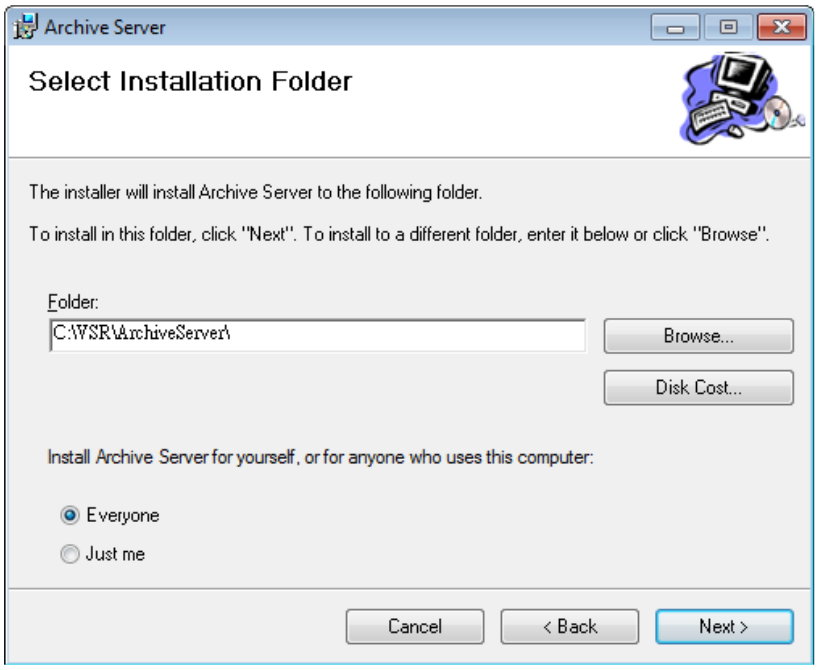
Windows 시스템에 아카이브 서버를 설치하려면, 컴퓨터에 USB 라이센스 키를 삽입하고 다음을 수행하십시오.

1. 패키지에 포함된 소프트웨어 CD를 컴퓨터의 CD ROM 드라이브에 삽입하십시오.
2. setup.exe 파일이 위치한 폴더로 가서, 파일을 실행하십시오. 아래와 비슷한 화면이 나타납니다.



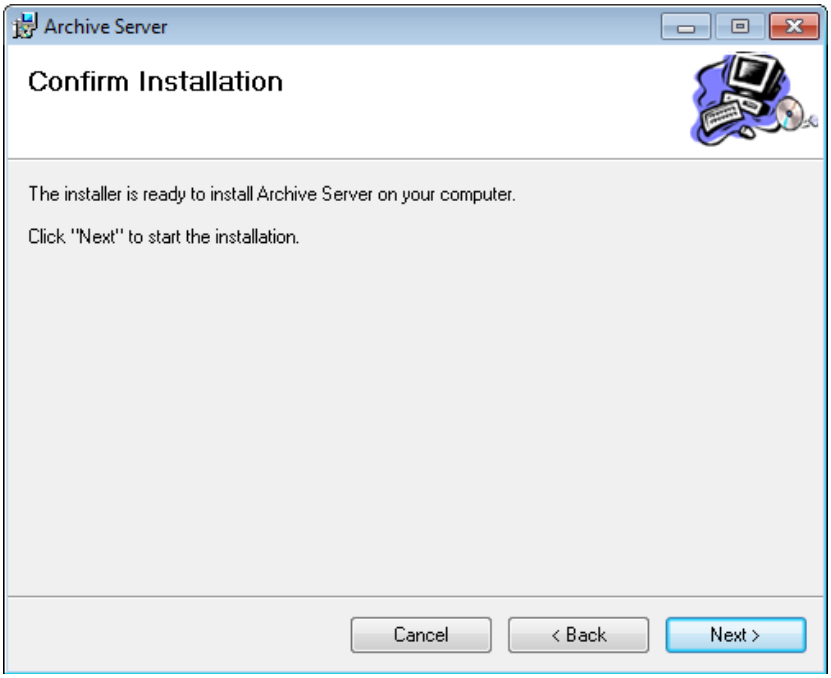
Next를 클릭하여 다음으로 진행하십시오.

3. Select Installation Folder 페이지에서, 설치 폴더를 설정하거나 혹은 **Browse**를 클릭하여 설치하려는 위치를 선택하십시오. 그 후 사용자 본인만을 위해 사용할 것인지(**Just me**) 혹은 이 컴퓨터를 사용하는 모두를 위해 사용할 것인지 (**Everyone**) 선택하십시오. **Disk Cost**를 클릭하면 설치 가능한 드라이브와 사용 가능 용량이 표시됩니다.

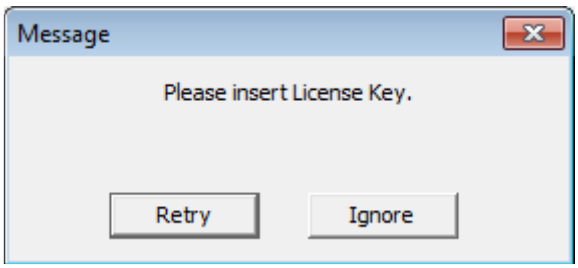


Next를 클릭하여 다음으로 진행하십시오.

4. Confirm Installation 윈도우가 나타나면, **Next**를 클릭하여 다음으로 진행하십시오.

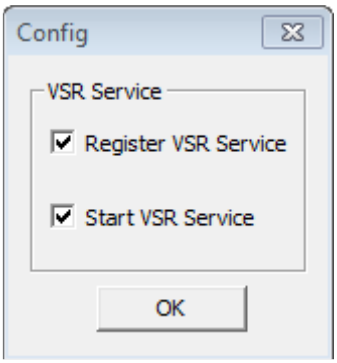


5. 라이센스 키를 삽입하라는 메시지가 나타난 경우, 다시 한번 USB 라이센스 키를 삽입하거나 혹은 다른 USB 포트에 삽입해 본 후 **Retry**를 클릭하십시오.



Ignore를 클릭하면 소프트웨어를 설치하지만 USB 라이센스 키를 사용하기 전까지는 소프트웨어를 사용할 수 없습니다.

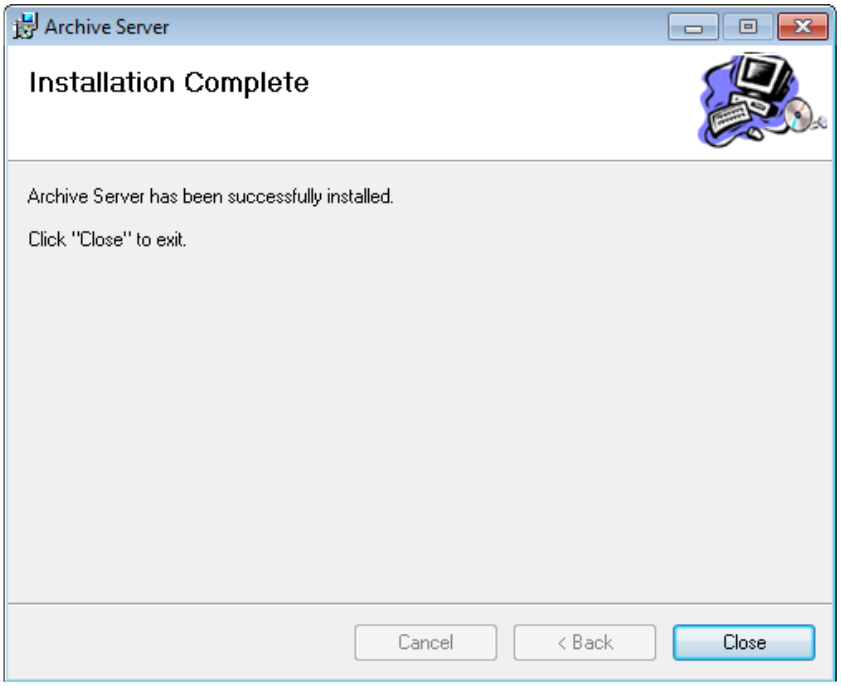
6. **Config** 대화 상자가 나타나면, 옵션을 선택하고 **OK**를 클릭하십시오.



Register VSR Service: 이 옵션을 설정하면 Windows 운영 체제에 CCVSR 서비스를 설치 및 등록하여 소프트웨어를 백그라운드에서 운영합니다.

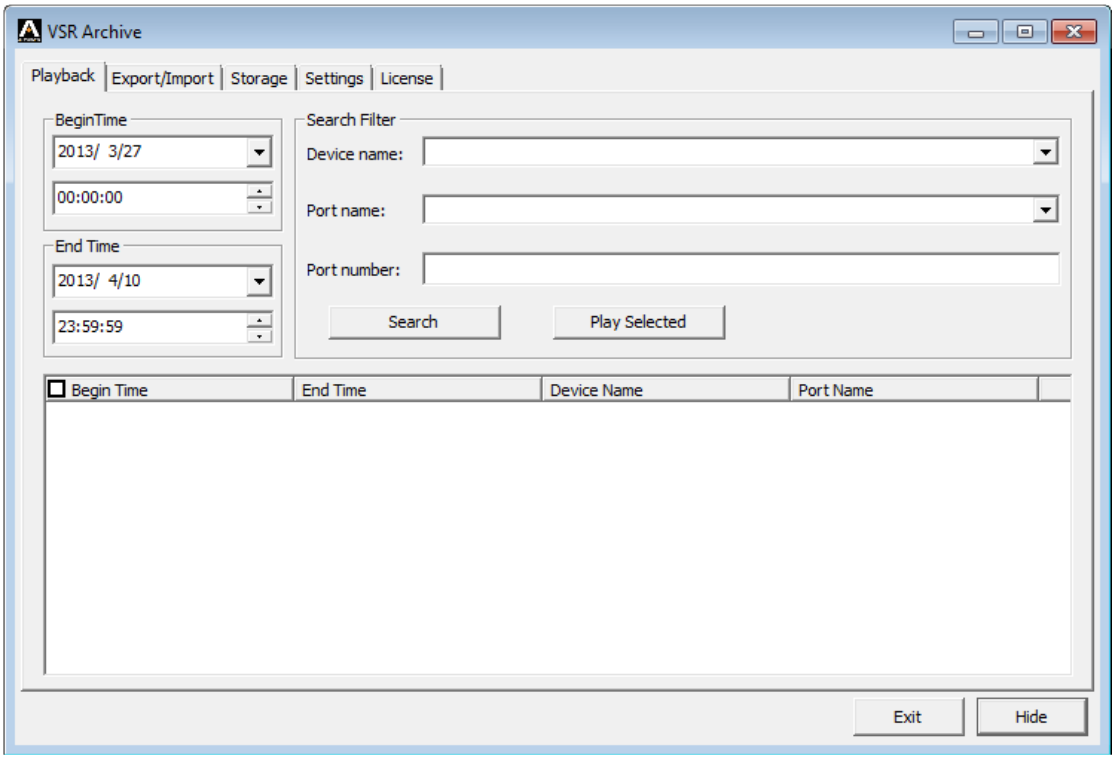
Start VSR Service: 이 옵션을 설정하면 설치 완료 후 CCVSR 서비스가 자동으로 시작합니다. 두 옵션 모두 설정할 것을 권장합니다.

7. 설치가 완료되면 다음 메시지가 나타납니다.



아카이브 서버 GUI

아카이브 서버의 인터페이스는 재생 (playback), 내보내기/가져오기 (Export/Import), 저장(Storage), 설정 (Setting), 라이센스 (License) 5개의 탭으로 이루어져 있습니다. 소프트웨어가 설치된 후, 바탕화면에 있는 Archive GUI 아이콘을 더블클릭 하면 playback 페이지가 나타납니다.



Exit 버튼을 클릭하면 아카이브 서버를 정지하며, 혹은 **Hide** 버튼을 누르면 작업 표시줄에 윈도우를 최소화합니다.

설정

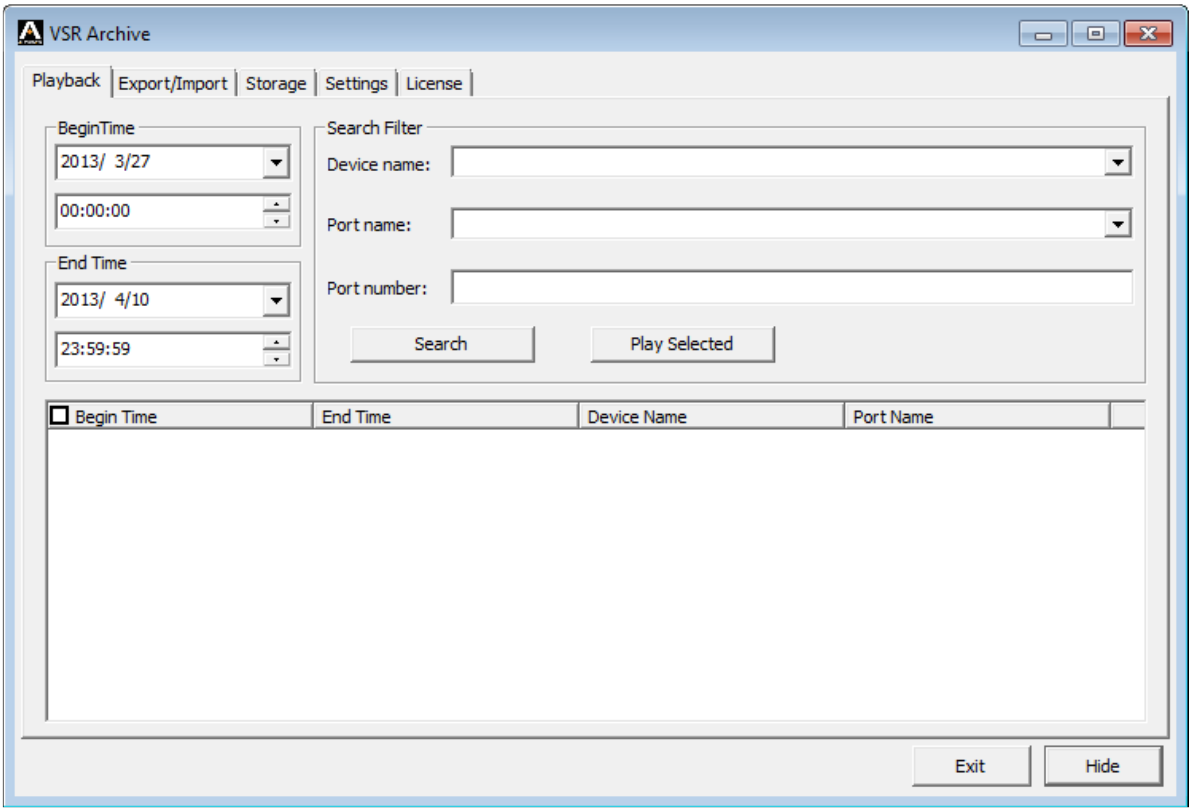
아카이브 서버를 설정하는 2가지 단계가 있습니다. 프라이머리 CCVSR 서버에서 아카이브 서버의 IP 주소를 설정하고, 아카이브 서버의 **Storage** 탭으로부터 저장 위치를 추가하는 것입니다.

먼저 프라이머리 CCVSR 서버에 아카이브 서버의 IP 주소를 설정합니다. (58페이지 참조) 다음 **Storage** 탭에서 저장 위치를 추가합니다. (96페이지 저장 참조) 저장 위치는 비디오 로그 파일이 저장될 위치를 의미합니다.

IP 주소가 설정되고 저장 위치가 추가된 후, 아카이브 서버는 설치 이후 생성되는 모든 비디오 로그 파일을 자동으로 보관합니다. 아카이브는 매 15분마다 업데이트 됩니다. 새로운 비디오 로그 파일에 대해 점검하려면, **Playback** 탭으로 가서 Search를 클릭합니다. 모든 새로운 비디오 로그 파일이 검색 윈도우에 나타납니다.

재생

Playback 탭은 보관된 혹은 수동으로 가져온 비디오 로그 파일들을 검색 및 재생하는데 사용됩니다. 보관된 모든 비디오 로그 파일 목록을 보려면, Search 버튼을 클릭합니다.



Playback 탭은 저장된 비디오 로그 파일을 검색 및 재생하기 위해 3가지 섹션으로 구분되어 있습니다.

시작 시간/종료 시간

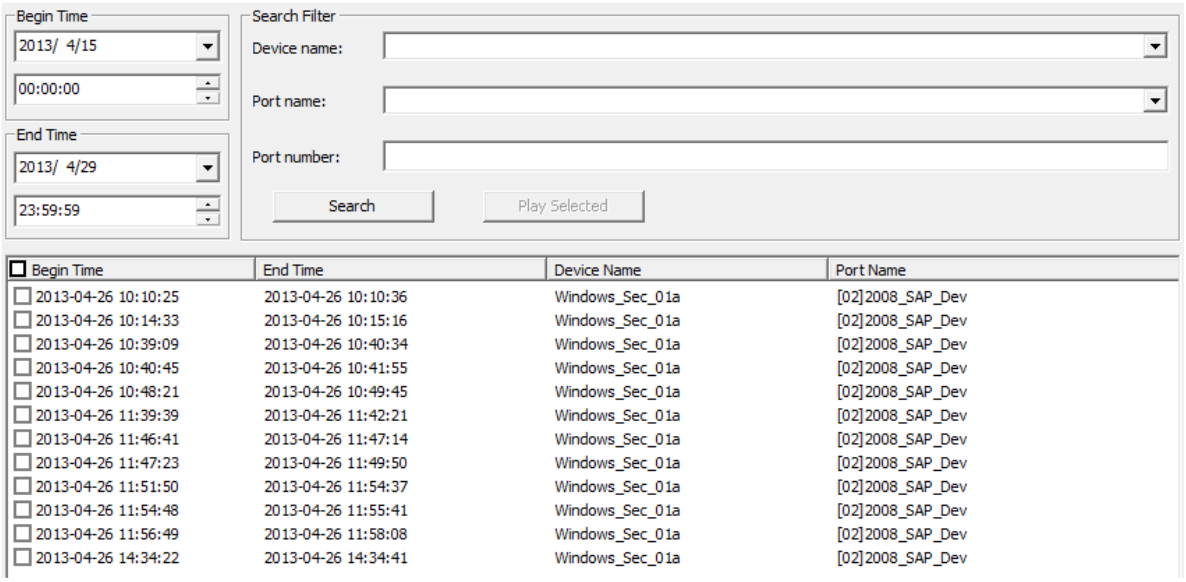
이 섹션은 사용자가 시간 및 종료 시간에 의해 검색 결과를 필터링 하도록 합니다. Begin Time 및 End Time은 KVM 스위치에서 발생했던 실제 비디오 로그 저장 시간을 참조합니다.

검색 필터

Search Filter는 KVM 스위치의 포트 이름 (Port Name), 장치 이름 (Device Name), 포트 번호 (Port Number)에 의해 비디오 로그 파일을 검색하는데 사용됩니다. 검색 데이터를 입력한 후, **Search**를 클릭합니다. 검색 결과*는 페이지의 아래에 나타나며, 제공되는 열을 사용하여 정렬할 수 있습니다. 모든 보관된 비디오 로그를 보려면, 간단히 이 필드에 아무것도 입력하지 않고 **Search**를 클릭합니다.

재생 선택

비디오 로그를 재생하려면, **Search***를 클릭합니다. 보관된 비디오 로그 목록이 나타납니다:



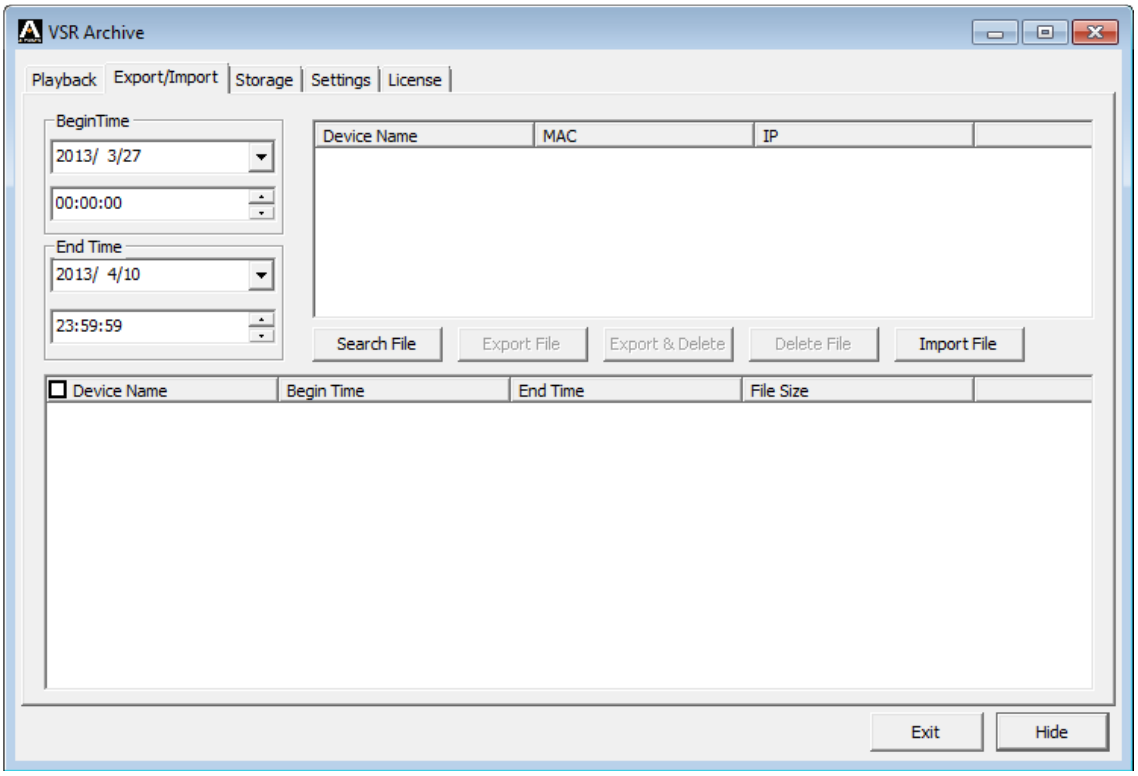
재생하려는 비디오의 체크 박스에 체크하고, **Play Selected**를 클릭합니다. 비디오는 비디오 로그 뷰어 프로그램에서 새로운 윈도우로 열립니다. 비디오 로그 뷰어에 관한 정보는 24페이지 VSR 뷰어를 참조하십시오.

주의: 1. 비디오 로그 파일이 Search를 클릭한 후 나타나지 않는 경우, 아직 아카이브가 업데이트되지 않았습니다. 이 경우 15분을 기다리거나 혹은 저장 위치가 **Storage** 탭에 추가되어야 합니다. (96페이지 저장 참조)

2. 아카이브 서버가 설치된 후 생성된 비디오 로그만 자동으로 프라이머리 CCVSR 서버에 보관됩니다. 설치 전 생성된 비디오 로그는 **Export/Import** 탭에서 반드시 수동으로 가져와야 합니다. (94페이지 내보내기/가져오기 참조)

내보내기/가져오기

Export/Import 탭은 비디오 로그 파일들을 단일 데이터베이스(.vse)에 내보내기 및 가져오기를 수행하는데 사용됩니다. 데이터베이스(.vse) 파일은 수많은 개별 비디오 로그를 단일 압축 파일로 통합하여 디스크 공간을 절약하고, 쉽게 내보내기 및 가져오기를 수행할 수 있습니다. Export/Import 탭은 또한 VSR 프라이머리 서버에서 생성된 개별 비디오 로그 파일 (.dat)을 가져올 수 있습니다.



Device Name을 선택하고 **파일 검색 Search File**을 클릭하여 내보낼 파일 (이미 아카이브에 저장된)을 검색할 수 있습니다. 아니면 **Import File**을 클릭하여 아카이브 서버에 .vse 혹은 .dat 파일을 수동으로 가져올 수 있습니다. 파일 가져오기에 관한 세부 사항은 아래 파일 가져오기를 참조하십시오.

시작 시간/종료 시간

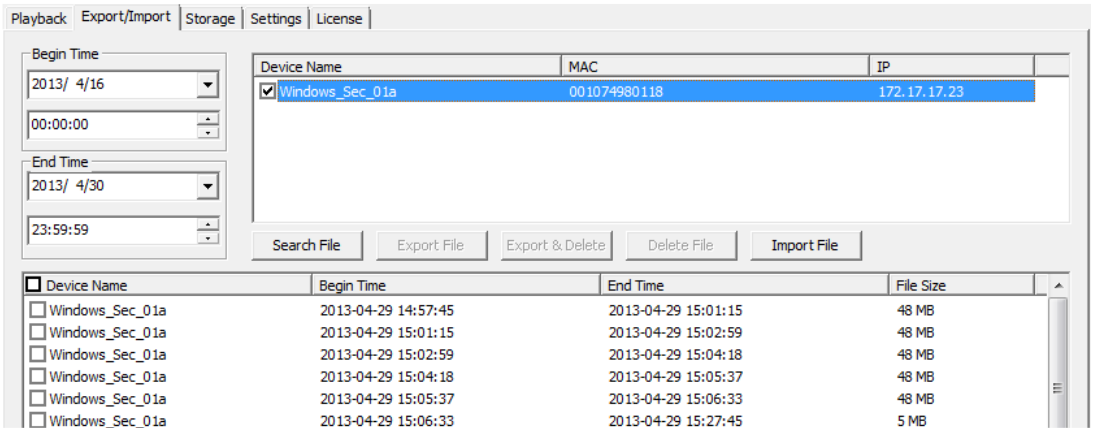
이 섹션은 사용자가 시간 및 종료 시간에 의해 검색 결과를 필터링 하도록 합니다. Begin Time 및 End Time은 KVM 스위치에서 발생했던 실제 비디오 로그 저장 시간을 참조합니다.

장치 이름

이 섹션은 1차 VSR 서버에 추가된 KVM 스위치의 이름을 목록으로 표시합니다. 장치를 선택하고 KVM 스위치로부터 보관된 개별 비디오 로그 파일의 목록을 검색합니다. 그 다음 비디오 로그를 선택하고 .vse 데이터베이스 파일로 내보낼 수 있습니다.

파일 검색

Search File 버튼은 사용자가 선택한 **Device Name**에 있는 비디오 로그 파일을 검색하는데 사용됩니다. 이 결과는 아래와 같이 윈도우 아래 섹션에 나타납니다. 그 다음 비디오 로그를 선택하고 .vse 데이터베이스 파일로 내보낼 수 있습니다.



파일 내보내기

로그를 내보내기 할 때 단일 압축 .vse 데이터베이스 파일로 저장됩니다. 아래 윈도우에 표시된 비디오 로그 파일 중 내보내기 할 파일을 선택한 후, **Export File**을 클릭하고 저장할 .vse 파일 이름을 입력하십시오.

내보내기 및 삭제

Export & Delete 버튼은 선택한 파일들을 .vse 데이터베이스 파일로 내보내고 아카이브 서버로부터 내보내려는 개별 비디오 로그 파일을 삭제합니다. 이것은 단일 데이터베이스로 개별 파일을 정리하는 가장 빠른 방법입니다.

파일 삭제

Delete File 버튼은 아카이브 서버로부터 선택된 비디오 로그 파일을 삭제합니다.

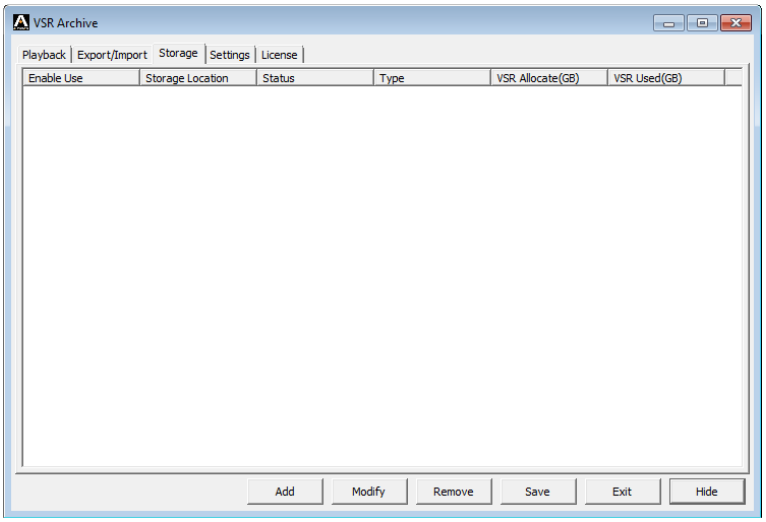
파일 가져오기

Import File 버튼은 보기, 보관, 혹은 새로운 데이터베이스 생성을 위해 데이터베이스 파일 (.vse) 및 개별 비디오 로그 파일을 가져오는데 사용됩니다.

Import File을 클릭하면 가져올 파일(.dat 혹은 .vse)를 찾아서 선택하고, **Open**을 클릭합니다. .vse 파일을 열었을 경우, 목록에서 파일을 선택하고 **Import** 를 클릭합니다. 가져오는 파일은 아카이브 서버로 복사되며, 따라서 파일을 가져오기 전에 Storage 탭에 저장 위치가 추가되어야 합니다. (96페이지 저장 참조) 저장 위치는 생성된 날짜 별로 저장되는 위치입니다.

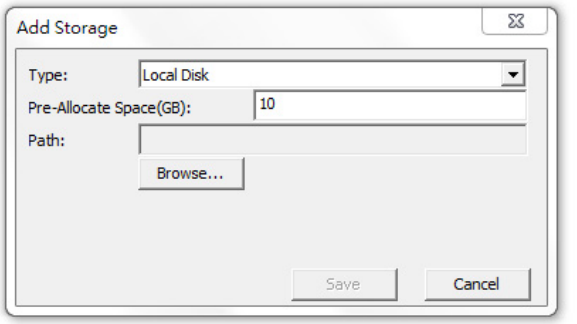
저장

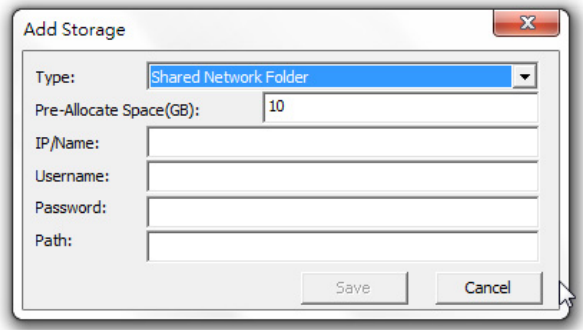
Storage 탭은 저장 위치를 추가하는데 사용됩니다. 이것은 보관된 비디오 로그가 저장되는 위치입니다. 여러 저장 위치를 추가할 수 있습니다. 처음 위치가 가득 차면 다음 위치가 사용되는 구조입니다. 비디오 로그는 생성된 날짜에 따라 폴더로 저장됩니다. 아카이브 서버는 저장 위치가 **추가**되거나 **활성화**될 때까지 비디오 로그를 보관할 수 없습니다.



저장 위치를 추가하거나 활성화하려면 다음을 수행하십시오.

1. **Add**를 클릭하고 아래와 같이 각 설정에 대한 **Local Disk** 또는 **Shared Network Folder**를 선택하십시오.





2. Local Disk의 경우, Path에 저장 위치를 입력하거나 **Browse**를 클릭하여 저장 위치를 선택하십시오. Shared Network Folder의 경우, 필수 필드인 IP/Name, Username, Password, Path를 입력하십시오.

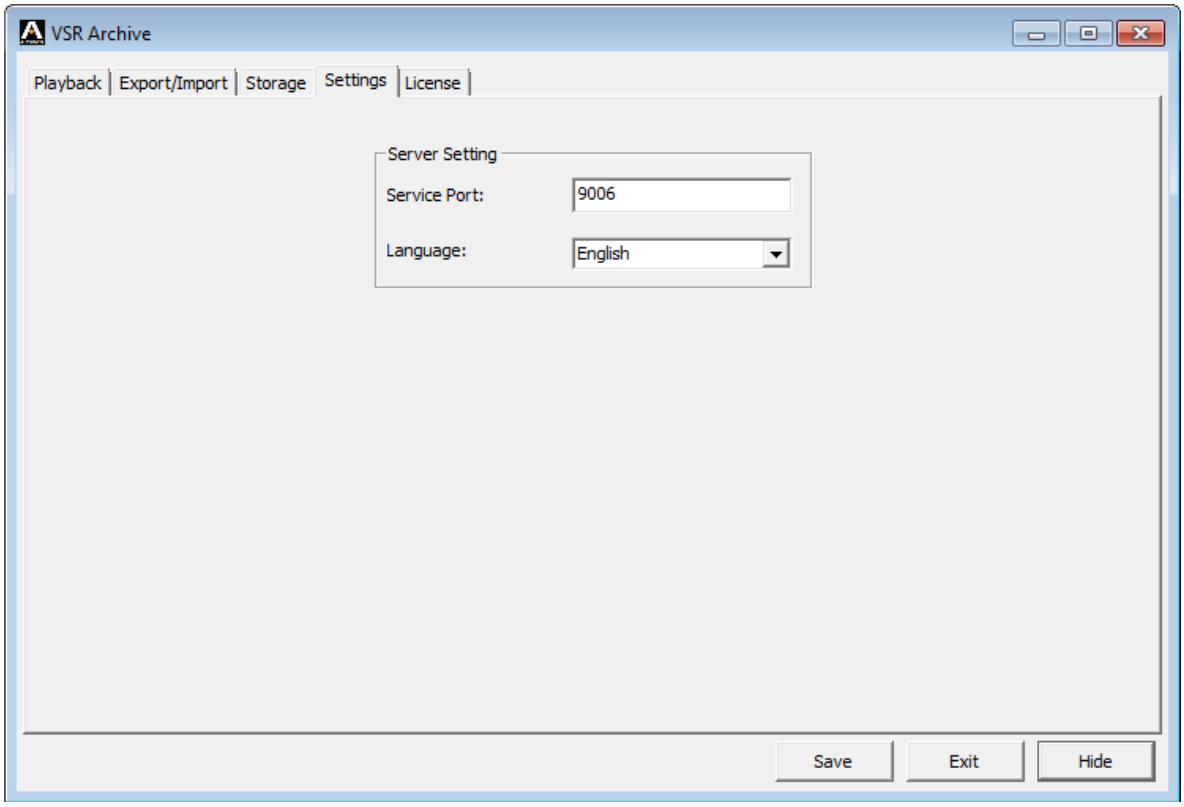
주의: 네트워크 공유 폴더를 사용하려면 먼저 네트워크가 불안정한 경우 비디오 손실을 방지하기 위한 임시 전송 파일을 저장하기 위해 최소 10GB의 공간이 있는 로컬 디스크를 추가해야 합니다.

3. Pre-Allocate Space(GB) 필드에 사용할 디스크 최대 용량을 입력하고, **Save**를 클릭하십시오. 저장 위치가 아래 윈도우에 나타납니다.
4. 다음, **Enable Use** 상자에 체크하고 **Save**를 클릭하십시오.

저장 위치를 선택하고 **Modify**를 클릭하여 설정하거나, **Remove**를 클릭하여 삭제하십시오. **Save**를 클릭하여 변경 사항을 저장하십시오.

설정

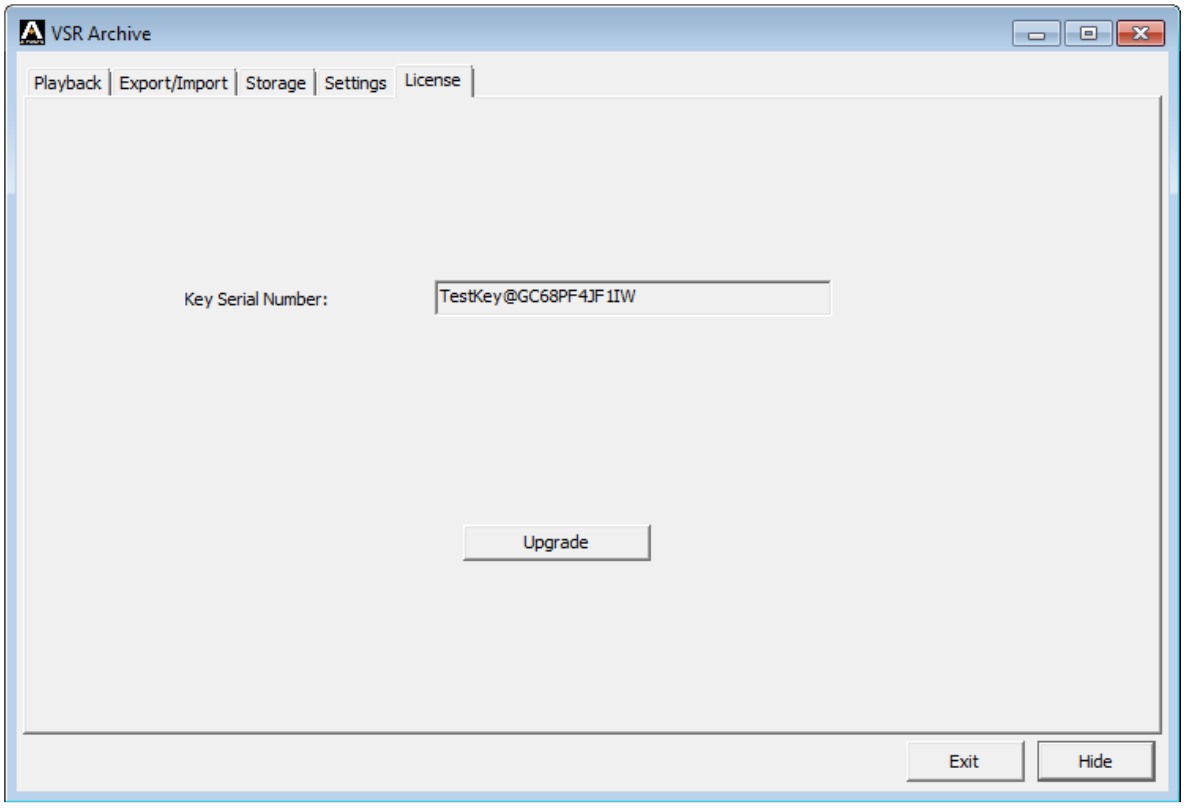
Settings 탭은 서버 설정을 위해 사용됩니다.



이 탭에서 Service Port 및 Language를 설정할 수 있습니다. 기본 서비스 포트는 **9006**입니다.

라이센스

License 탭을 사용하여 라이센스 키를 업그레이드합니다. 컴퓨터에 USB 라이센스 키를 삽입하고 **Upgrade**를 클릭하십시오.



업그레이드가 실패한 경우, USB 라이센스 키를 다시 삽입하거나 다른 USB 포트에 삽입해보십시오.

부록 A

기술 지원

국제 지역

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

북미 지역

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

본사와 연락할 때 사전에 다음과 같은 정보를 준비해주십시오.

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

USB 인증 키 사양

기능		키
사용 환경	동작 온도	0–40 ℃
	보관 온도	-20–60 ℃
	습도	비응축 상태에서 0–80% RH
제품 외관	재질	금속 및 플라스틱
	무게	14 g
	크기	8.36 x 2.77 x 1.37 cm

호환 제품

호환 제품 목록은 ATEN 웹 사이트 CCVSR 페이지의 "사양" 탭을 참조하십시오.

Linux 설치

Linux를 실행하는 컴퓨터에서 CCVSR 소프트웨어를 설치하거나 제거할 때 다음 명령을 사용하십시오.

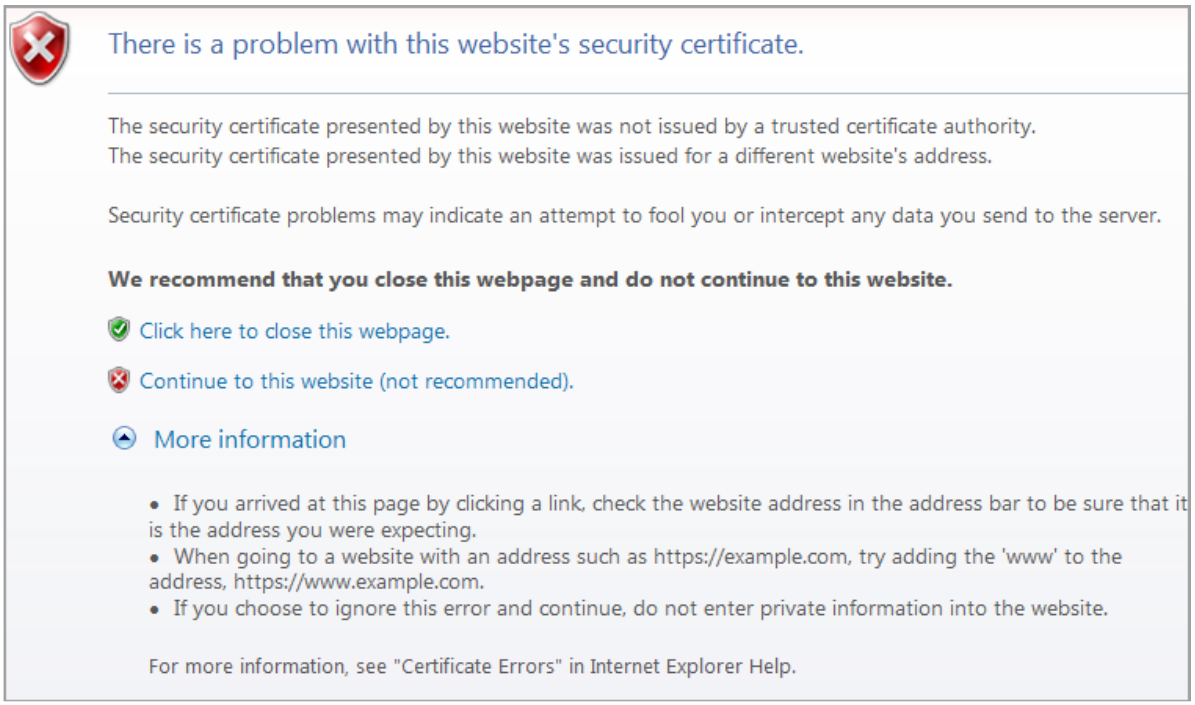
Linux 설치 명령 :> sudo ./vlsman.run

Linux 제거 명령 :> sudo /usr/local/bin/ccvsr/uninstallvlsmon

신뢰 인증서

개요

사용자의 브라우저를 통해 장치에 로그인을 시도할 때, 보안 경고 메시지 창이 나타나 장치의 인증서를 신뢰할 수 없다고 알리고, 계속 진행할 것인지를 묻습니다.



인증서는 신뢰될 수 있지만, 인증서의 이름이 Microsoft에서 신뢰된 승인 기관이 아니기 때문에 경고가 발생합니다. 경고를 무시하고 클릭하십시오.

자기 서명 개인 인증서

사용자가 자기 서명 암호 키와 인증서를 생성하려면, 무료 유틸리티 - openssl.exe –를 **www.openssl.org** 에서 다운로드 하여 사용할 수 있습니다. 개인 키와 인증서를 생성하려면 다음을 수행하십시오.

1. 다운로드한 폴더에 가서 압축을 풀어 openssl.exe 파일을 찾으십시오.
2. 다음 매개변수로 openssl.exe를 실행하십시오.

   openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509
   keyout CA.key -out CA.cer -config openssl.cnf.

주의: 1. 명령어는 1개의 라인으로 입력되어야 합니다. (매개변수 입력이 끝날 때까지 [Enter]를 누르지 마십시오.)
2. 입력에 띄어쓰기가 있는 경우, 따옴표를 붙여주십시오. (예: "ATEN International")

키 생성 동안 정보 입력하지 않으려면 다음 추가 매개변수를 사용할 수 있습니다.

/C /ST /L /O /OU /CN /emailAddress.

예제

openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509
-keyout CA.key -out CA.cer -config openssl.cnf -subj
/C=yourcountry/ST=yourstateorprovince/L=yourlocationor
city/O=yourorganiztion/OU=yourorganizationalunit/
CN=yourcommonname/emailAddress=name@yourcompany.com
openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509
-keyout CA.key -out CA.cer -config openssl.cnf -subj
/C=CA/ST=BC/L=Richmond/O="ATEN International"/OU=ATEN
/CN=ATEN/emailAddress=eservice@aten.com.tw

파일 가져오기

openssl.exe 프로그램이 완료된 후에, 2개의 파일 CA.key (개인 키) 및 CA.cer (자기 서명 SSL 인증서)가 프로그램을 실행했던 폴더에 생성됩니다. 이 파일들을 보안 페이지의 개인 인증서 패널에 업로드 합니다. (65페이지 보안 및 68페이지 인증서 참조)

호스트 헤더 공격에 대한 보안 강화

허용 리스트를 생성하려면 아래 단계를 따르십시오.

1. 텍스트 파일에 허용된 호스트 이름을 세미콜론으로 구분하여 추가하십시오.
   예시: www.aten.com;www.abcd.com;noname.com;

주의: 허용 리스트의 길이는 768자를 초과하지 않아야 하며, 내용은 줄 바꿈 없이 하나의 연속된 줄로 유지되어야 합니다.

---

2. 파일을 'vlshost.dat'로 저장하십시오.
3. 'vlshost.dat' 파일을 CCVSR 작업 디렉토리에 복사하십시오.
   - Windows: C:₩VSR₩VideoSessionRecorder
   - Linux: /usr/local/bin/ccvsr
4. 설정을 적용하려면 CCVSR 서비스를 재시작하거나 CCVSR 서버를 재시작하십시오.

아카이브 서버에서 TLS1.0 / 1.1 비활성화

1. Archive 서비스를 중단하십시오.
2. Archive 서버 디렉토리에서 'vlssys.ini' 파일을 찾아 '[Comm]' 아래에 'SecurityLevel=4'를 추가하십시오.

   [Comm]

   SecurityLevel=4
3. Archive 서비스를 재시작하거나 PC를 재시작하십시오.

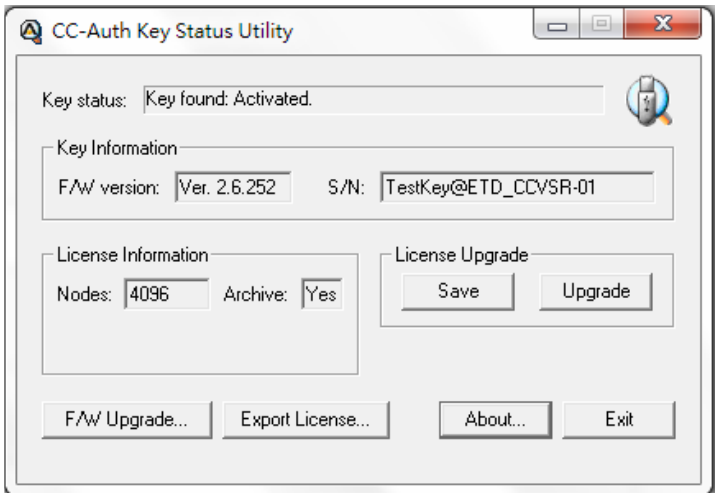
부록 B

인증 키 유틸리티

개요

인증 키 유틸리티 (CCAuthKeyStatus.exe)는 CCVSR 인증 키에 포함된 정보 및 데이터에 접속하고 업데이트하기 위한 Windows 기반 유틸리티입니다. CCAuthKeyStatus.exe는 CCVSR 웹 사이트에서 다운로드할 수 있습니다.

프로그램을 실행하면 아래와 비슷한 화면이 나타납니다.



키 상태 정보

대화 박스의 레이아웃은 아래 테이블에서 설명합니다.

섹션	목적
Key Status	키가 발견되었는지, 키가 활성화되었는지 알립니다. 키가 발견되지 않은 경우, 또는 키가 활성화되지 않은 경우 판매자에게 문의하십시오.
Key Information	키의 현재 펌웨어 버전 및 시리얼 번호를 표시합니다.
License Information	서버 숫자 (프라이머리 및 세컨더리) 및 키가 제공하는 라이센스의 노드 수를 표시합니다.
License Upgrade	이 버튼들은 오프라인 라이센스 업그레이드를 수행할 때 사용됩니다.
F/W Upgrade	이 버튼은 인증 키의 펌웨어를 업그레이드할 때 사용됩니다.

키 유틸리티

라이센스 업그레이드 및 F/W 업그레이드 섹션은 사용자가 키의 펌웨어 (F/W 업그레이드)를 업그레이드하도록 하며, 라이센스에 의해 승인된 서버 및 노드 수를 업그레이드 (라이센스 업그레이드)하기 위한 유틸리티를 제공합니다.

키 펌웨어 업그레이드

CCVSR 인증 키 펌웨어는 업그레이드 가능합니다. 새로운 펌웨어 버전이 나오면, 업그레이드 파일이 웹 사이트에 올려집니다. 본사의 웹 사이트를 주기적으로 방문하여 최신 파일 및 관련 정보가 있는지 확인하십시오.

업그레이드 시작

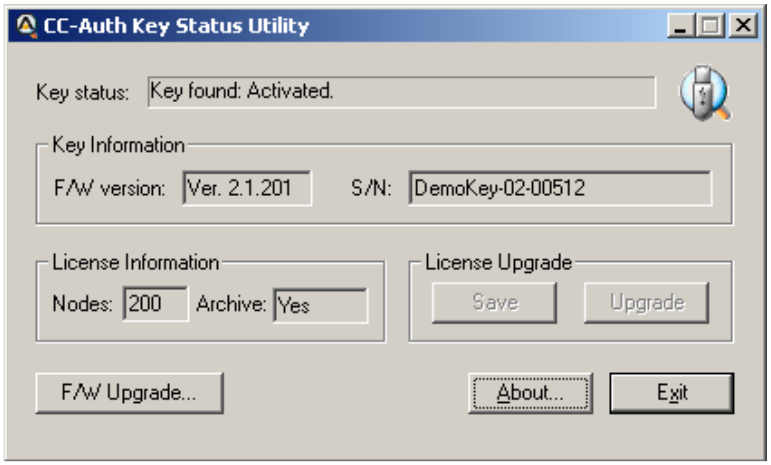
펌웨어를 업그레이드하려면 다음을 수행하십시오.

1. 웹사이트로 가서 새로운 펌웨어 파일을 컴퓨터의 편리한 곳에 다운로드 하십시오.
2. 인증 키를 연결하고 키 상태 유틸리티 (CCAuthKeyStatus.exe)를 실행하십시오.

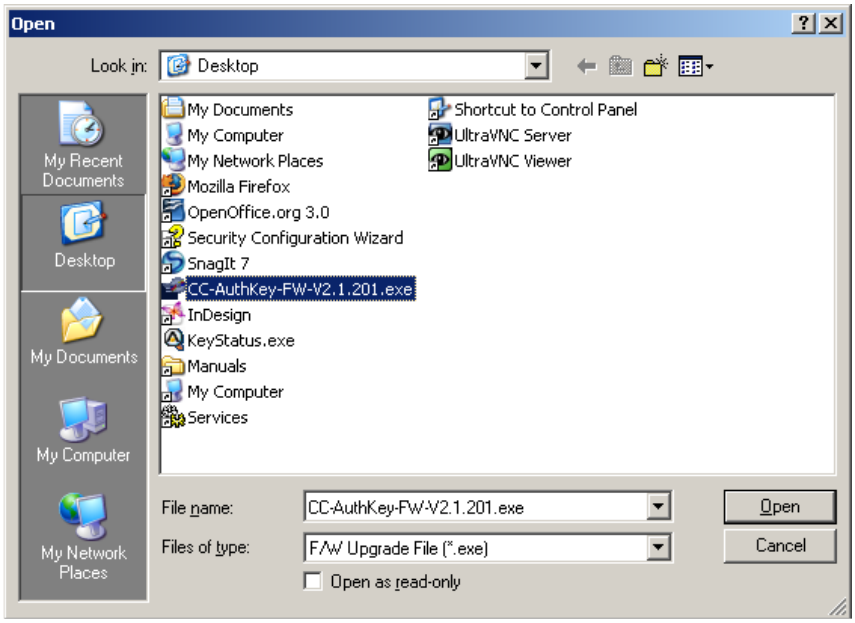
주의: CCAuthKeyStatus.exe는 Windows에서만 실행가능 하며 CCVSR 웹사이트에서 다운로드 할 수 있습니다.

---

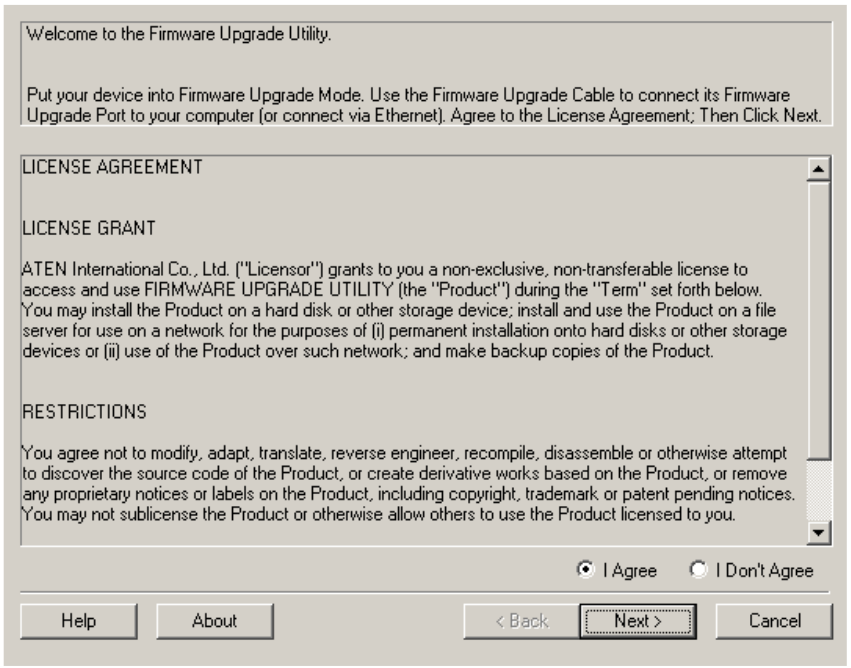
3. 아래와 같은 화면이 나타나면, **F/W Upgrade...**를 클릭하십시오.



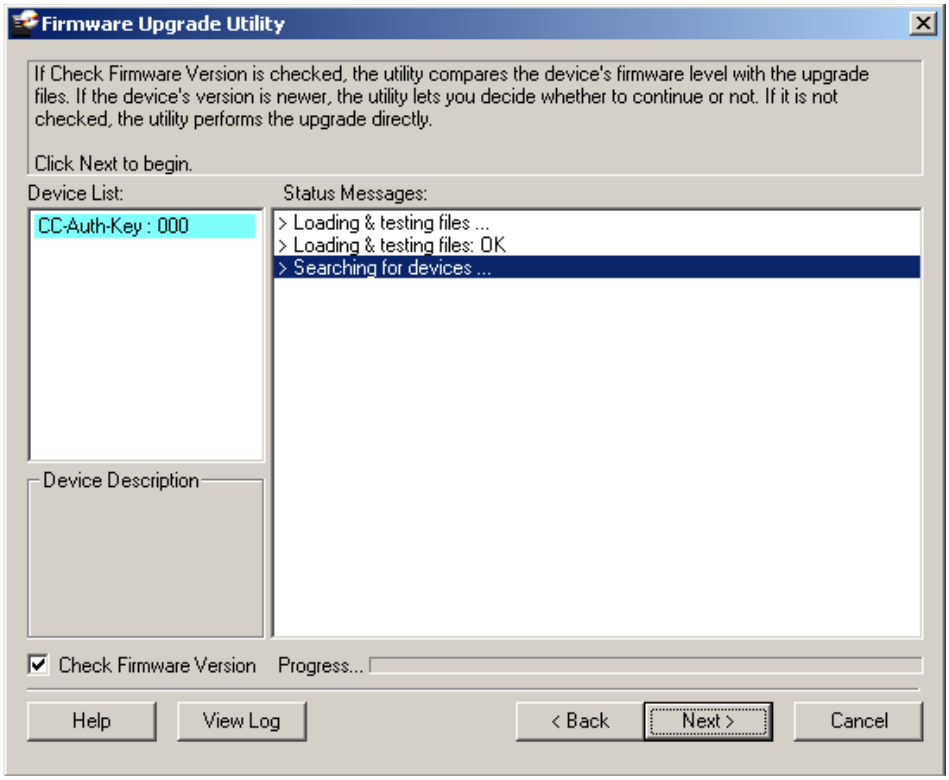
4. 파일 열기 대화 상자가 나타나면, 펌웨어 업그레이드 파일을 선택하고 **Open**을 클릭하십시오.



5. 라이센스 동의 내용을 읽고 수락하십시오. (I Agree 라디오 버튼 클릭)



6. 유틸리티는 사용자의 설비를 검색합니다. 장치를 찾게 되면, 장치 목록 패널에 표시됩니다.

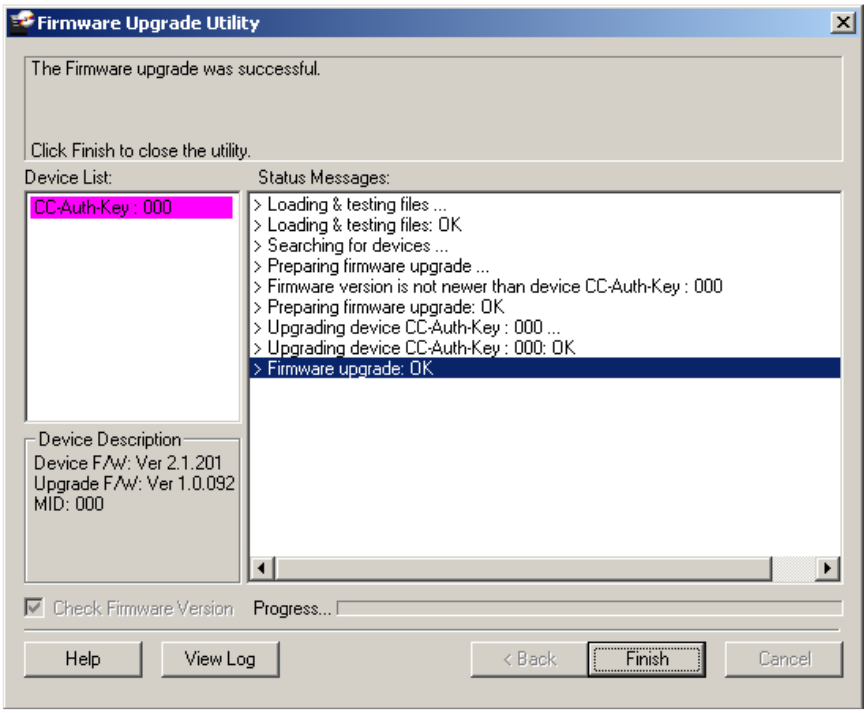


주의: Check Firmware Version을 사용하도록 설정한 경우, 유틸리티는 업그레이드 파일과 장치의 펌웨어 버전을 비교합니다. 장치의 버전이 업그레이드 버전보다 높은 경우 대화 상자가 나타나 계속 진행할 것인지 취소할 것인지 선택하도록 합니다.
Check Firmware Version를 사용하지 않도록 설정한 경우, 유틸리티는 버전 체크를 하지 않고 업그레이드를 수행합니다.

Next를 클릭하여 계속 진행합니다.

업그레이드 성공

업그레이드가 완료되면, 아래와 같은 화면이 나타나 업그레이드 과정이 완료되었음을 알립니다.



Finish를 클릭하면 펌웨어 업그레이드 유틸리티를 닫습니다.

키 라이센스 업그레이드

개요

CC 시리즈는 최종 사용자 (클라이언트)가 라이센스 수를 증가하는 것을 반영하기 위한 인증 키를 업데이트 하도록 합니다. 키 라이센스 업그레이드는 클라이언트나 판매자/대리점에 의해 수행될 수 있으며, 인터넷을 통한 브라우저 세션 (온라인 업그레이드) 또는 독립 실행 유틸리티 프로그램 (오프라인 업그레이드)를 통해서도 가능합니다.
클라이언트는 먼저 판매자/대리점에게 업그레이드될 라이센스 개수를 알리면, 판매자/대리점은 ALTUSEN 판매 대리점에게 요청하여 추가될 라이센스 개수를 설정합니다. 주문 과정 후에 ALTUSEN은 업그레이드를 수행하기 위해 필요한 세부 사항들과 함께 확인 및 인증 메일을 판매자/대리점으로 전송합니다.

주의: 여러 주문들은 각 키마다 과정을 거쳐야 합니다.

키를 업그레이드하는 2가지 방식이 있습니다.

- **On Line**: 컴퓨터의 USB 포트와 브라우저 세션에 삽입된 키를 업그레이드하기 위해 키를 직접 업그레이드합니다. 클라이언트가 업그레이드를 수행하는 경우, 판매자/대리점은 자세한 메일 인증을 제공합니다. 판매자/대리점이 업그레이드를 수행하는 경우, 클라이언트는 그들에게 인증 키를 제공합니다.
- **Off Line**: 윈도우 기반의 Key Status Utility (키 상태 유틸리티)는 키의 정보를 빼내기 위해 사용되고, 키 정보 데이터 파일에 키 정보를 작성합니다. 키 정보 데이터 파일은 라이센스 업그레이드 파일을 생성하기 위해 브라우저 세션에서 사용됩니다. 라이센스 업그레이드 파일이 생성된 후, 키 상태 유틸리티는 업그레이드 파일의 정보를 라이센스 키에 기록하기 위해 다시 사용됩니다.
  - 클라이언트가 CC 라이센스 데이터베이스를 업데이트하는 경우, 판매자/대리점은 클라이언트에게 메일 인증을 제공하여 클라이언트가 키 라이센스 업그레이드 파일을 생성하도록 합니다. 클라이언트는 키 상태 유틸리티 및 키 라이센스 업그레이드 파일을 사용하여 인증 키의 라이센스 정보를 업그레이드합니다.
  - 판매자/대리점이 CC 라이센스 데이터베이스를 업데이트 하는 경우, 클라이언트는 판매자/대리점에게 키 정보 데이터 파일(키 상태 유틸리티에서 나온)을 제공하며, 이 파일은 판매자/대리점이 클라이언트의 키 라이센스 업그레이드 파일을 생성하기 위해 사용됩니다. 판매자/대리점은 키 라이센스 업그레이드 파일을 클라이언트에게 반납하고 클라이언트는 키 상태 유틸리티를 사용하여 인증 키의 라이센스 정보를 업데이트 합니다.

온라인 업그레이드

클라이언트는 판매자/대리점에 연락하여 업그레이드를 요청합니다. 여러 주문은 각 키마다 과정이 필요합니다. 판매자/대리점은 업그레이드 주문을 ALTUSEN 판매 대리점에 요청하면, 아래와 같은 확인 및 인증 메일을 받습니다.

Your order is ready to be processed. Please go to http://xxx.xxx.x.xxx to upgrade your key's license.

Login Information:

- **Username: myname2**
- **Password: mypassword5678**

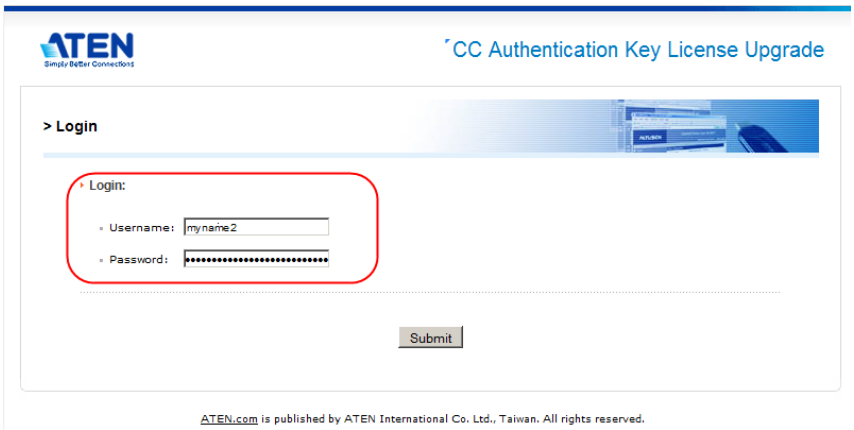
Order Information:

- **Order ID: 1017000700 (authorized number: 2068919892). This order requests 7 more server(s) and 20500 more node(s)**

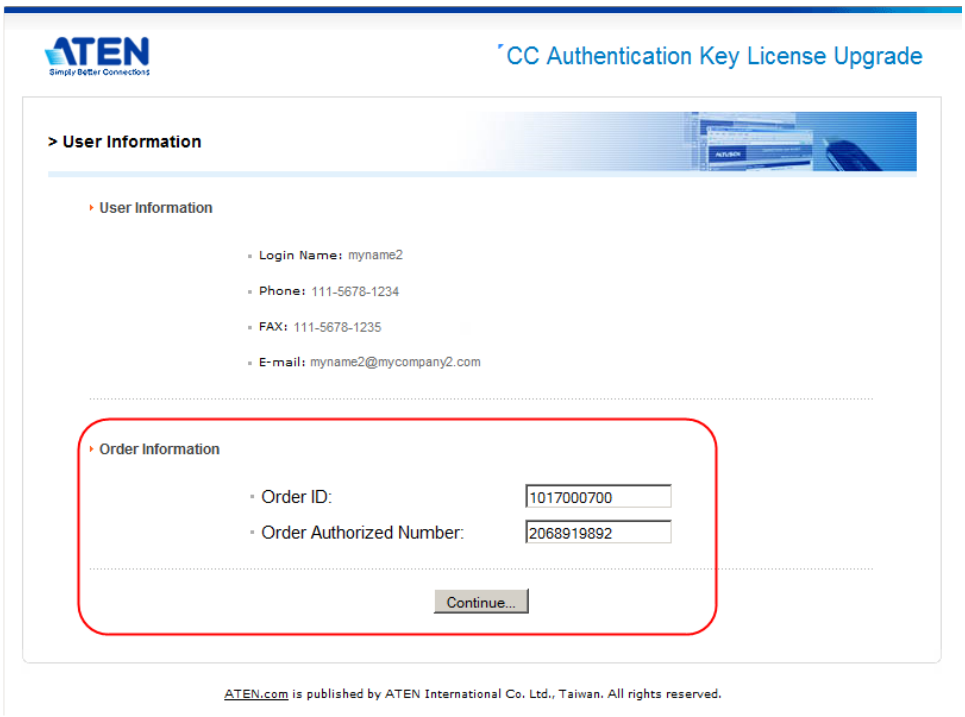
클라이언트 또는 판매자/대리점은 업그레이드를 수행할 수 있습니다. 판매자가 하는 경우, 클라이언트는 라이센스 키를 판매자에게 제공하고, 클라이언트가 하는 경우, 판매자는 확인 메일을 클라이언트에게 전송합니다.

온라인 업그레이드를 하려면 다음을 수행하십시오.

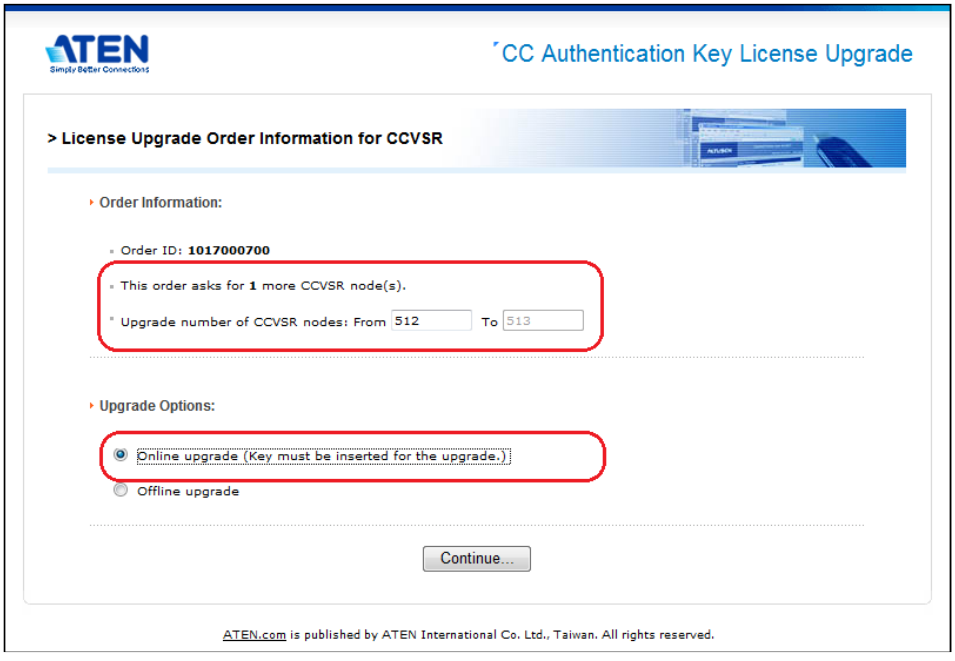
1. 인증 키를 사용자의 컴퓨터의 USB 포트에 연결하십시오.
2. 브라우저를 열고, 웹 사이트 CC 인증 키 라이센스 업그레이드 페이지로 이동하십시오. https://cc.aten.com.tw/
3. 업그레이드 로그인 화면이 나타나면 인증 이메일에 제공된 사용자 이름과 비밀번호로 로그인하십시오.



4. 표시되는 화면에서 업그레이드에 적용되는 주문 ID 번호와 주문 승인 번호를 입력한 다음 **Continue**를 클릭하십시오.



5. 라이센스 업그레이드 주문 정보 화면에서 From 필드에 현재 라이센스 수를 입력하고 (To 필드는 자동으로 채워짐) **Online upgrade**를 선택하십시오.

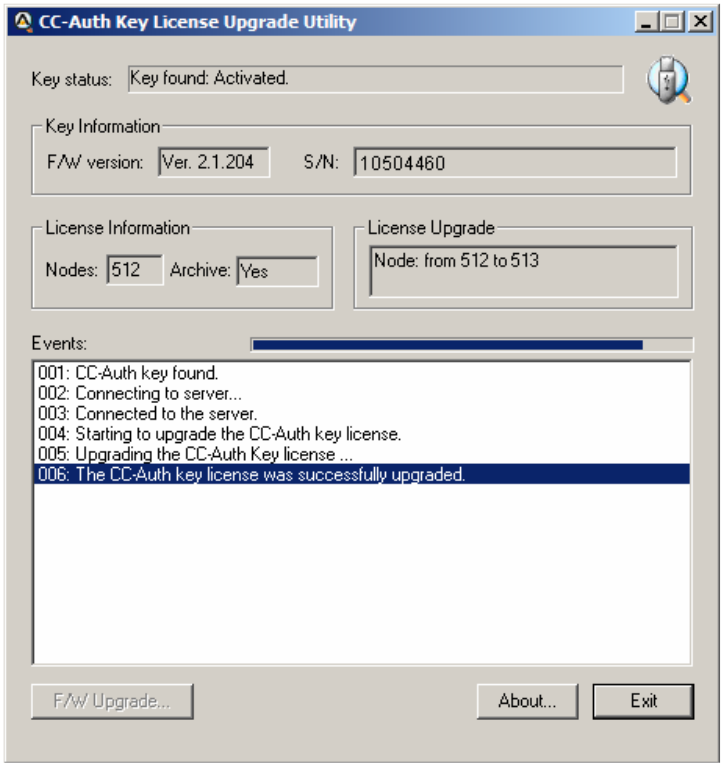


주의: 키 상태 유틸리티 (ccauthkeystatus_utility.exe)를 사용하여 현재 라이센스 수를 확인할 수 있습니다.

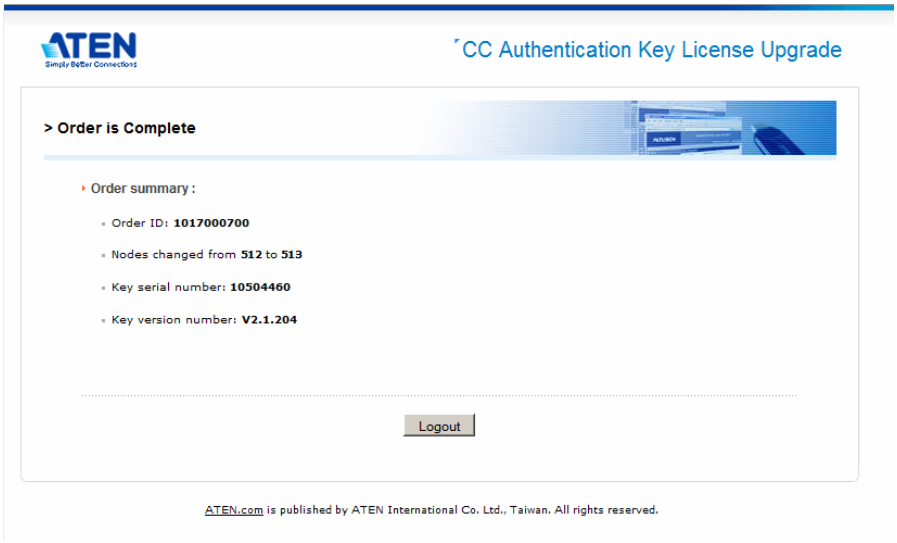
6. **Continue**를 클릭하십시오.
7. 대리점에서 제공한 CC 인증 키 라이센스 업그레이드 화면이 나타나면, **Download**를 클릭하십시오.
8. 브라우저가 이 파일 (KeyUpgrade.exe)로 무엇을 할 것인지 물으면, Save to disk를 선택하십시오.
9. 브라우저에서 벗어나서, 파일을 다운로드 한 곳으로 가서 실행하십시오.

주의: 이 단계는 반드시 KeyUpgrade.exe를 다운로드 한 같은 웹 세션에서 실행되어야 합니다. 그렇지 않으면 업그레이드가 되지 않습니다.

업그레이드 유틸리티가 나타나 업그레이드를 시작합니다. 업그레이드가 실행되면 메인 패널에서 과정이 나타납니다.

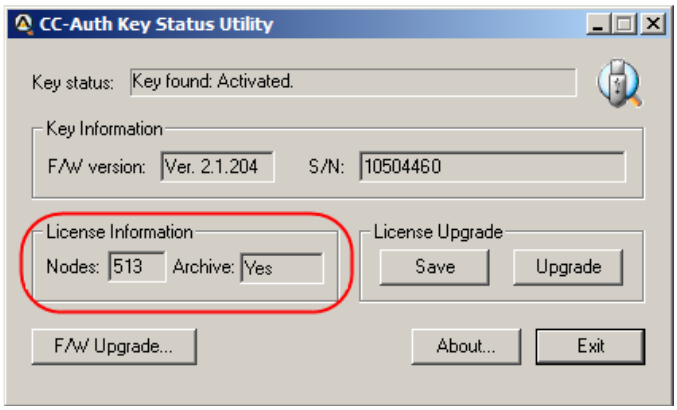


10. 업그레이드가 완료되면, 윈도우가 나타나 업그레이드가 성공하였음을 알립니다. **OK**를 클릭하여 팝업 창을 닫으십시오. 브라우저 화면은 업그레이드 요약 정보를 제공합니다.



11. **Logout**를 클릭하여 종료하십시오.

키 상태 유틸리티 (CCAuthKeyStatus.exe)를 사용하여 업그레이드에 반영될 키의 변경된 라이센스 개수를 확인합니다.



업그레이드 성공

펌웨어 업그레이드가 완료된 후, 판매자/대리점은 ALTUSEN에서 온라인 업그레이드가 완료되었음을 메일로 받습니다. 예를 들면

Your order (Order ID: 1017000700) has been completed successfully by the online utility.

The key (PSN: 10504460) server number has been upgraded from 512 to 513.

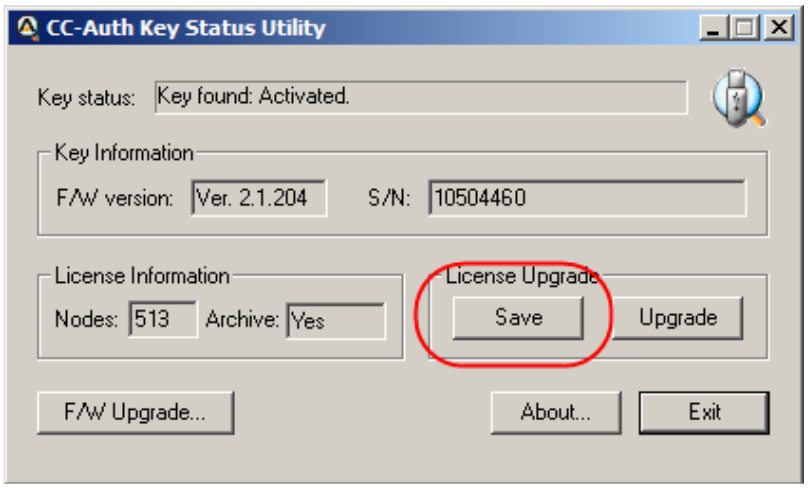
오프라인 업그레이드

오프라인 업그레이드는 판매자/대리점이나 최종 사용자인 클라이언트에 의해 수행될 수 있습니다. 이 업그레이드의 장점은 클라이언트는 키를 사용하지 않아도 된다는 것입니다. 필요한 것은 키 정보 데이터 파일을 판매자/대리점에 메일로 전송하고 키 업그레이드 파일을 받는 것입니다.

예비 단계

업그레이드를 수행하기 위해 클라이언트가 수행해야 할 처음 단계는 아래와 같이 Key Information Data File를 생성하는 것입니다.

1. 인증 키를 연결하고, Key Status Utility (CCAuthKeyStatus.exe)를 실행하십시오.
2. 대화 상자의 License Upgrade 패널이 나타나면, **Save**를 클릭하여 Key Information Data File (KeyUpload.dat)를 생성합니다.



주의: 키 정보 데이터 파일은 키 상태 유틸리티가 있는 같은 폴더에서 생성됩니다.

키 정보 데이터 파일이 생성된 후, 클라이언트는 이것을 판매자/대리점으로 보냅니다.

업그레이드 수행

판매자/대리점에서 ALTUSEN 판매 대리점에 업그레이드 요청을 하면, ALTUSEN으로부터 확인 및 인증 메일을 받습니다. 예를 들면

Your order is ready to be processed. Please go to http://xxx.xxx.x.xxx to upgrade your key's license.

Login Information:

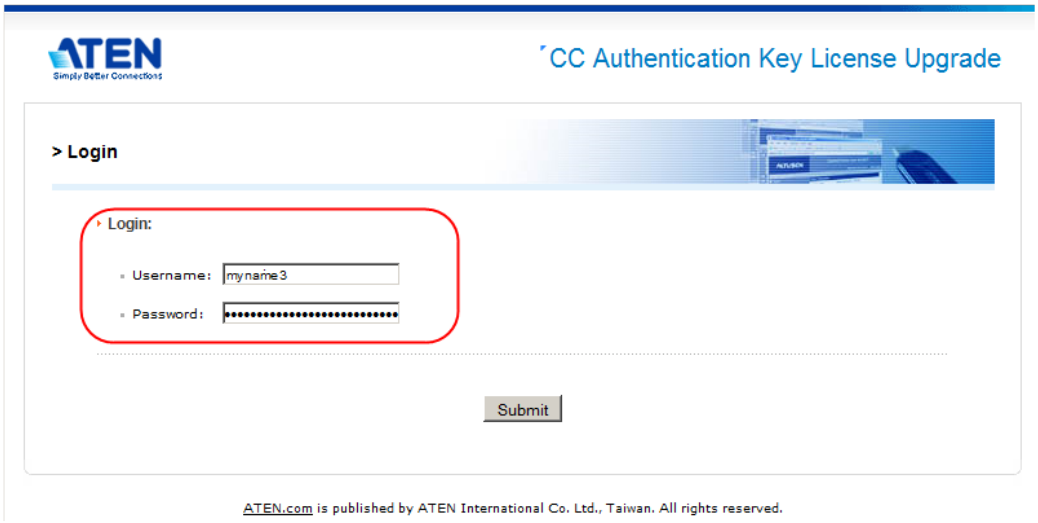
- **Username: myname3**
- **Password: mypassword3**

Order Information:

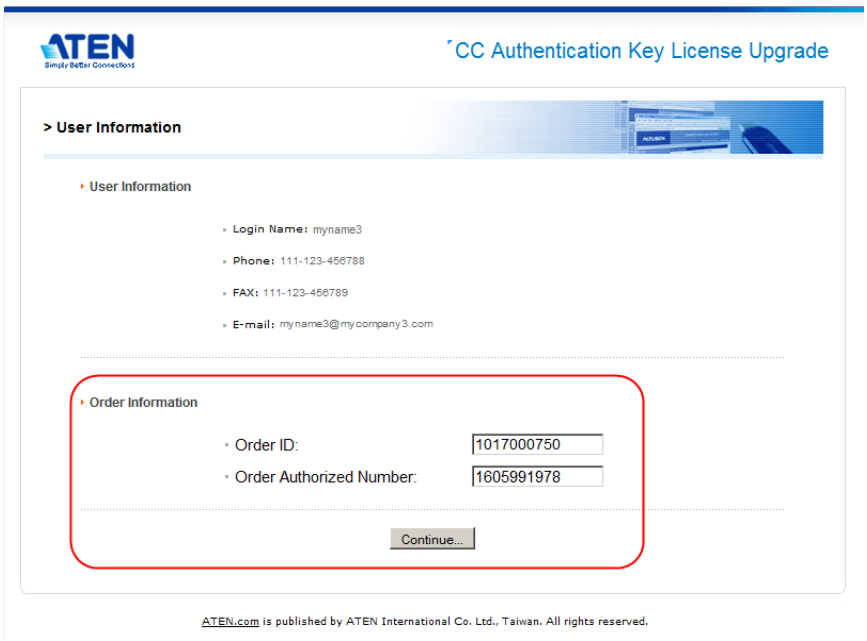
Order ID: 1017000750 (authorized number: 1605991978). This order requests 1 more node(s)

업그레이드를 하려면 다음을 수행하십시오.

1. 온라인 업그레이드 1-3단계를 따르십시오 (111페이지 참조)
2. 업그레이드 로그인 화면이 나타나면, 인증 메일에서 제공하는 사용자 이름 및 암호를 사용하여 로그인 하십시오.



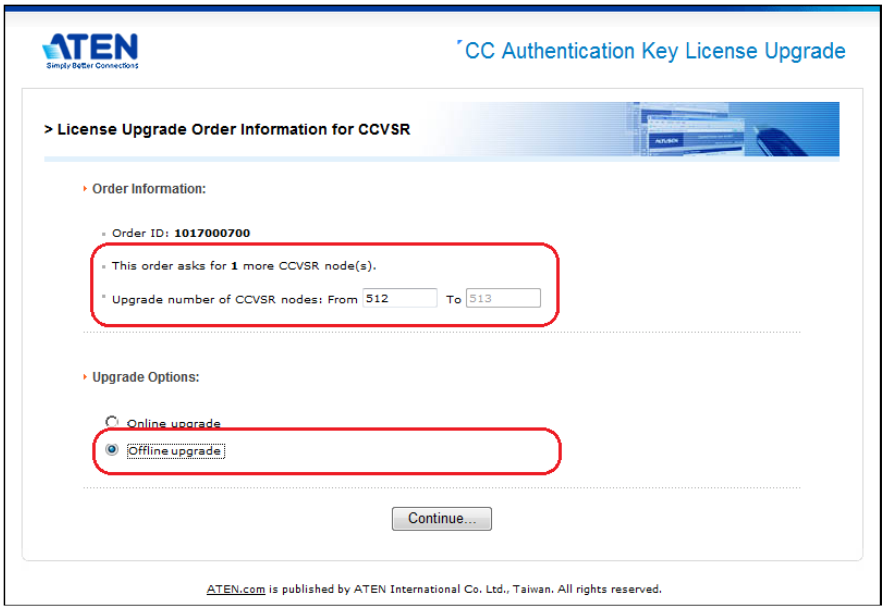
3. 다음 나타난 화면에서 업그레이드에 적용되는 요청 ID 번호와 요청 인증 번호를 입력하고, **Continue**를 클릭하십시오.



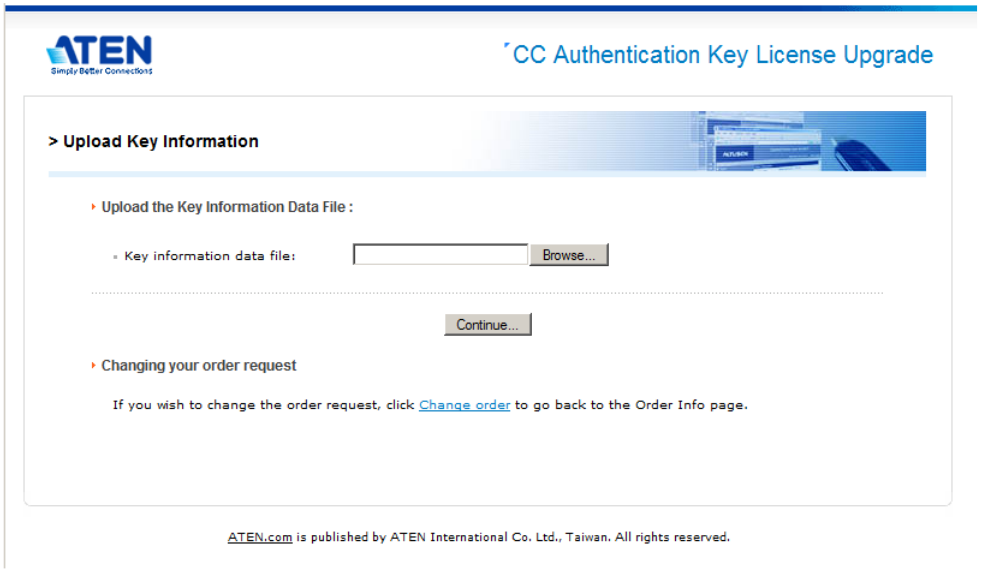
4. 라이센스 업그레이드 요청 정보 화면에서, From 필드에 현재 라이센스 개수를 입력하십시오. To 필드는 자동으로 입력됩니다.

주의: 필요한 경우, 현재 라이센스 키를 보려면 키 상태 유틸리티 (CCAuthKeyStatus.exe)를 사용할 수 있습니다.

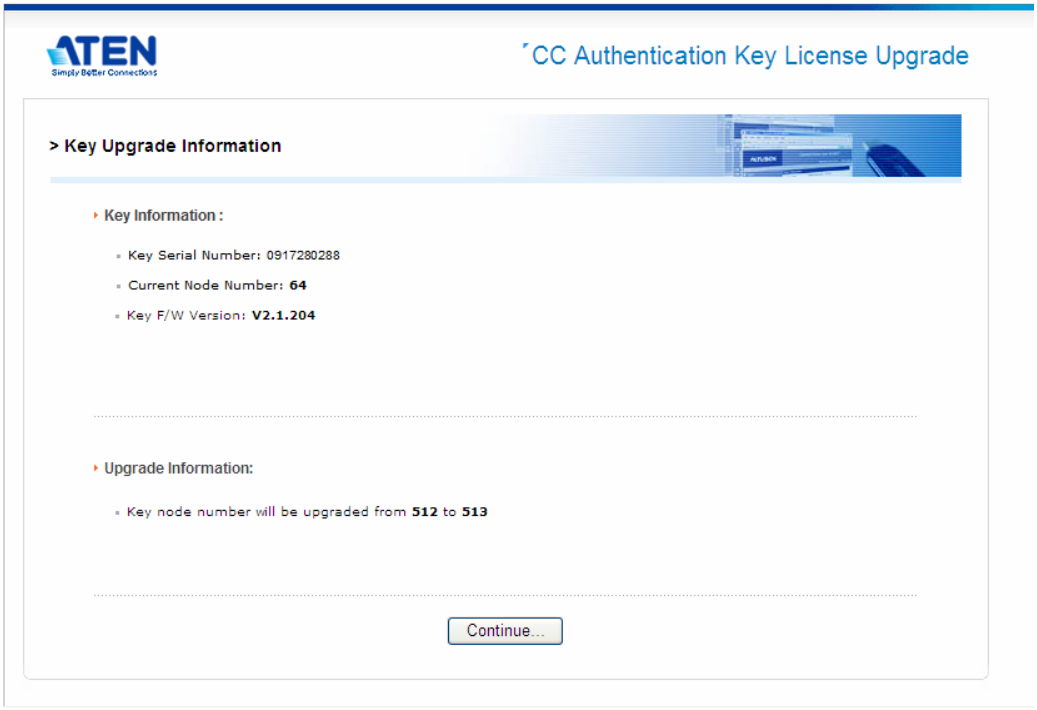
5. 오프라인 페이지를 선택하고 **Continue**를 클릭하십시오.



6. 키 정보 업로드 화면이 나타나면, **Browse**를 클릭하십시오. 예비 단계에서 생성된 **KeyUpload.dat** 파일을 로드하고, **Continue**를 클릭하십시오.

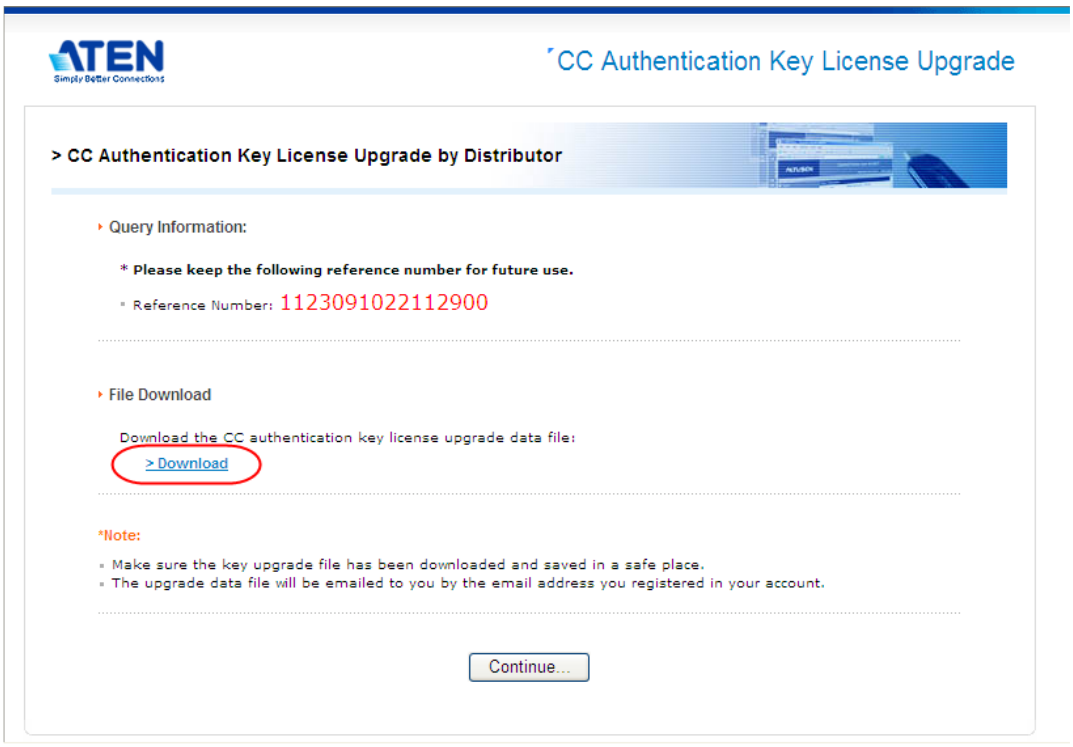


7. 다음 화면이 나타나고 변경 사항을 요약합니다.



Continue를 클릭하면 다음으로 이동합니다.

8. 다음 화면이 나타나면 **Download**를 클릭하여 키 라이센스 업그레이드 데이터 파일 (KeyUpgrade.dat)을 다운로드하십시오.



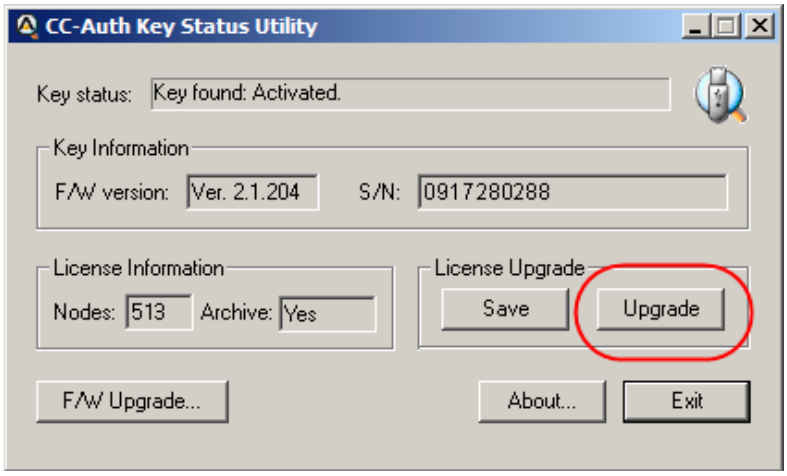
9. 브라우저가 키 업그레이드 파일로 무엇을 할 것인지 물을 때, Save to disk를 선택하십시오. 파일이 디스크에 저장된 후, **Continue**를 클릭하여 계속 진행하십시오.
10. 확인 팝업이 나타나면 **Yes**를 클릭하십시오. 요청 확인 요약 페이지가 나타납니다.
11. **Logout**를 클릭하여 종료하십시오.

주의: 1. 사용자가 1개 이상의 키를 업그레이드하는 경우, 따로 이름을 인식할 수 있도록 KeyUpgrade.dat 파일의 이름을 변경할 수 있습니다. (확장자 dat는 유지)
2. 클라이언트가 업그레이드를 수행하는 경우, 판매자/대리점은 KeyUpgrade.dat 파일을 클라이언트에게 제공합니다.

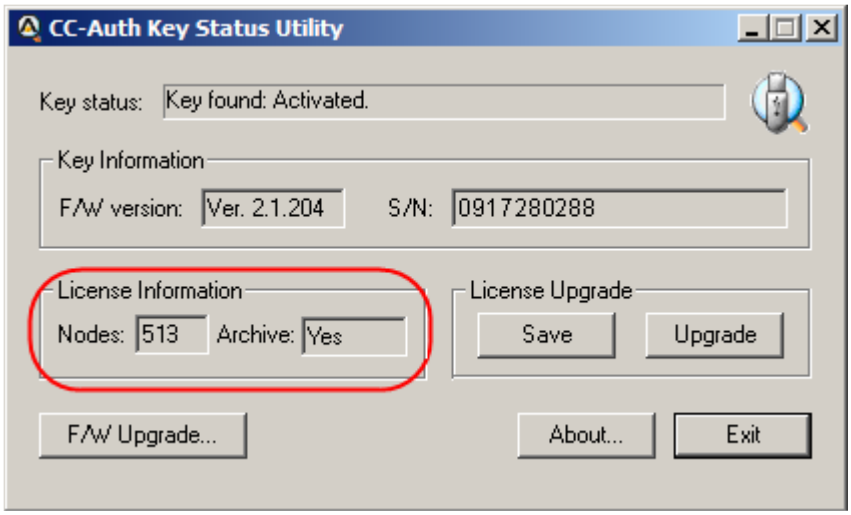
---

12. Key Status Utility를 다시 실행하십시오.

13. 라이센스 업그레이드 패널에서 **Upgrade**를 클릭하십시오.



14. 대화 상자가 나타나면 업그레이드 파일 (KeyUpgrade.dat)을 탐색하여 선택하십시오.
    - **Open**을 클릭하면, 윈도우가 나타나 업그레이드가 성공적으로 완료되었음을 알립니다,
    - 라이센스 정보 패널에서 라이센스 개수는 업그레이드를 반영하기 위해 변경됩니다.



오프라인 업그레이드 실패

오프라인 업그레이드가 실패한 경우, 파일 전송 과정에서 망가진 키 업그레이드 파일 (KeyUpgrade.dat) 때문인 경우가 있습니다. 다음과 같은 2가지 해결 방식이 있습니다.

◆ 키 업그레이드 파일을 다운로드 할 때, 아래와 같이 원본 파일 전송에 문제가 생긴 경우에 업그레이드 파일의 복사본과 함께 자세한 내용이 메일이 판매자/대리점에게 전송됩니다.

Offline upgrade email response:
Your CC-Authentication key's upgrade data file is
attached. Please upgrade your CC-Auth key with the
attached file.
Key Info:
* F/W Version: 2.1.204
* Serial number: 0917280288
License Upgrade Info:
* From 512 to 513 concurrent nodes
Confirmation Info:
* Username: newname
* Password: 1123091022112900
If you have any problem with upgrading your CCAuthentication
key's license, please confirm it online
at http://xxx.xxx.x.xxx using the username and
password above.

사용자는 11단계 (키 상태 유틸리티 실행) 및 12단계 (Upgrade 클릭)을 반복할 수 있습니다. 이 때 판매자/대리점 메일에 첨부된 키 업그레이드 파일 (KeyUpgrade.dat)의 복사본을 사용합니다.

◆ 위 방법으로도 문제가 해결되지 않는 경우, Offline email upgrade response에 있는 정보가 온라인 업그레이드를 시도하는데 사용될 수 있습니다. 판매자/대리점 둘 다 최종 사용자에게 인증에 관한 자세한 사항을 제공할 수 있고, 또는 최종 사용자가 가지고 있는 키를 판매자/대리점에 줄 수도 있습니다.

요청 만료

ALTUSEN에서 판매자/대리점으로 요청이 진행될 준비가 되었음을 알리는 확인/인증 메일을 보내면, 요청이 진행되는데 전체 2주가 소요됩니다. 이 시간 동안 요청사항이 진행되지 않으면 2개 이상의 메일이 전달되어 진행이 되지 않는다고 알려줍니다.

1. 사용자의 요청이 1주일 내에 만료됩니다.
2. 사용자의 요청이 1일 내에 만료됩니다.

요청이 마지막 날까지 처리되지 않은 경우, 아래와 같이 마지막 메일이 전송되어 판매자/대리점에 요청이 만료되었음을 알립니다.

Your order has expired and has been cancelled...

If you still wish to add licenses, you must place a new order.

부록 C

고급 네트워크 설정

HTTP 포트 활성화 / 비활성화

1. CCVSR 서비스를 중지하십시오.
2. CCVSR 디렉토리에서 cmdapi 툴을 사용해 사용자의 플랫폼 타입에 맞는 다음의 명령어를 입력하십시오:

   Windows:

   C:₩VSR₩VideoSessionRecorder>cmdapi -h 1

   Linux:

   /usr/local/bin/ccvsr$ sudo cmdapi -h 1
3. CCVSR 서비스를 시작하십시오.

TLS 1.0 또는 TLS 1.1 비활성화

1. CCVSR 서비스를 중지하십시오.
2. CCVSR 디렉토리에서 cmdapi 툴을 사용해 보안 레벨을 4로 변경하십시오.

   cmdapi -g 4
3. CCVSR 서비스를 시작하십시오.

부록 D

CCVSR MIB 참조

개요

이 섹션에서는 CCVSR v2.2.211 이상 (MIB v2.0.196)에서 지원되는 MIB에 대한 정보를 제공합니다. 여기에는 네트워크 관리 시스템과의 통합, 자동 모니터링 및 이벤트 처리에 필요한 상세 정보가 포함되어 있습니다.

이 섹션에는 다음 정보가 포함됩니다:

- 객체 그룹화 및 탐색을 위한 하위 트리 구조 및 조직
- 트랩 OID, 트리거 조건(설명) 및 관련 매개변수를 포함한 SNMP 트랩 정의

MIB 트리 구조

- **products** (.1.3.6.1.4.1.21317.1)

모든 ATEN 제품의 루트 노드입니다.

- **overip** (.1.3.6.1.4.1.21317.1.3)

ATEN 소프트웨어 제품을 위한 하위 트리입니다.

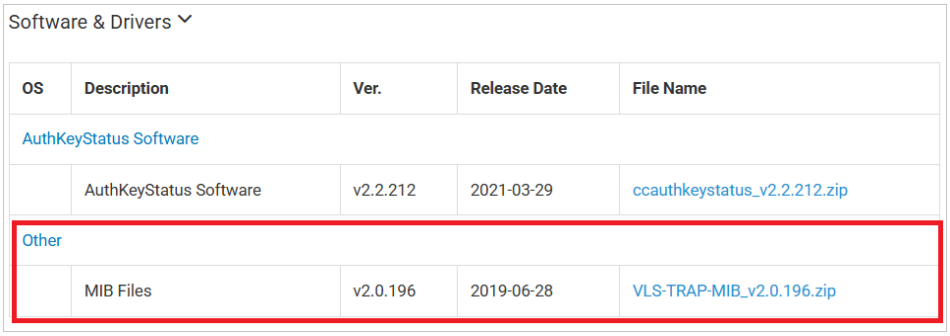
- **VLS** (.1.3.6.1.4.1.21317.1.3.8)

ATEN CCVSR에 대한 MIB 객체 및 트랩을 정의합니다.

MIB 파일 다운로드

최신 MIB 파일을 다운로드하려면:

1. 이 링크를 클릭하여 CCVSR 제품 페이지를 방문하십시오.
2. 아래로 스크롤하여 **MIB File** 섹션을 찾으십시오.



3. 클릭하여 MIB 파일을 다운로드하십시오.

OID 형식

이 문서에서 모든 객체 식별자 (OID)는 앞에 마침표가 없는 숫자 형식으로 표시됩니다.

예를 들어, 일부 SNMP 도구에서는 OID가 다음과 같이 표시될 수 있습니다:

.1.3.6.1.4.1.21317.1.2.1.1.1.1.0

이 문서에서는 다음과 같이 표기합니다:

1.3.6.1.4.1.21317.1.2.1.1.1.1.0

두 표기법은 동일합니다. 일관성과 가독성을 위해 앞의 마침표는 생략되었습니다.

객체 유형 및 인덱싱

SNMP 객체는 스칼라 (scalar) 또는 테이블 기반일 수 있습니다. GET 요청을 보낼 때 스칼라 객체와 인스턴스 객체를 구분하고, 올바른 OID 사용법을 확인하십시오.

◆ 스칼라 객체

스칼라 객체는 이산적인 데이터 조각을 포함하는 객체입니다. 스칼라 객체는 항상 하나의 인스턴스만 갖는 것으로 정의되므로, 인스턴스 객체와 구분하기 위해 GET 요청에서 스칼라 객체를 참조할 때 OID 뒤에 ".0"을 추가합니다.

예시:

DeviceName 객체가 다음과 같이 정의된 경우:

객체 이름	OID
DeviceName	1.3.6.1.4.1.21317.1.3.3.3.7.1

SNMP 버전 2c와 커뮤니티 문자열 'public'을 사용하여 IP 192.168.1.10에 있는 SNMP 에이전트로부터 스칼라 객체 DeviceName.0의 값을 가져오려면, GET 요청은 다음과 같습니다:

snmpget -v2c -c public 192.168.1.10 DeviceName.0

또는

snmpget -v2c -c public 192.168.1.10 1.3.6.1.4.1.21317.1.3.3.3.7.1.0

결과:

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

주의: ".0"이 생략되면, SNMP 에이전트는 인스턴스를 찾을 수 없으며 오류 또는 유효하지 않음 메시지를 반환합니다.

◆ 인스턴스 객체

스칼라 객체와 반대로, 일부 객체는 장치의 네트워크 인터페이스와 같이 여러 인스턴스를 포함할 수 있습니다. 인스턴스 객체는 SNMP 테이블에 존재하는 여러 데이터 조각 중 하나입니다. GET 요청에서 이러한 데이터 조각을 올바르게 참조하려면 인덱스 번호가 추가된 OID를 사용하십시오.

예시:

MIB에서 인터페이스 카드의 열(column) OID를 1.3.6.1.2.1.2.2.1.2로 정의하고 장치에 2개의 인터페이스가 있는 경우:

인터페이스 인덱스	설명
1	Ethernet 0
2	Ethernet 1

SNMP 버전 2c와 커뮤니티 문자열 'public'을 사용하여 IP 192.168.1.10에 있는 SNMP 에이전트로부터 인스턴스 2의 값을 가져오려면, SNMP 명령은 다음과 같습니다:

snmpget -v2c -c public 192.168.1.10 1.3.6.1.2.1.2.2.1.2.2

CCVSR 트랩 객체

이 섹션은 VLS-TRAP-MIB 파일에 정의된 SNMP 트랩에 대한 상세 정보를 제공합니다. 다음 항목들은 SNMP 지원 네트워크 환경 내에서 모니터링, 알림 및 문제 해결을 지원하기 위해 트랩 유형, 의미 및 예상 매개변수를 설명합니다.

◆ sysTrapLogin

OID	1.3.6.1.4.1.21317.1.3.8.3.1
상태	활성 (current)
설명	사용자가 로컬 콘솔, 인터넷 브라우저, Windows 애플리케이션 프로그램 또는 Java 애플리케이션 프로그램을 통해 로그인했습니다.

◆ sysTrapLoginFailed

OID	1.3.6.1.4.1.21317.1.3.8.3.2
상태	활성 (current)
설명	잘못된 로그인 시도 횟수가 지정된 양을 초과하면 이 사용자 계정은 잠깁니다. 이 사용자는 시간 초과 기간이 만료될 때까지 기다린 후 다시 로그인해야 합니다.

◆ sysTrapUserLocked

OID	1.3.6.1.4.1.21317.1.3.8.3.3
상태	활성 (current)
설명	잘못된 로그인 시도 횟수가 지정된 양을 초과하면 원격 컴퓨터의 IP 주소가 잠깁니다. 시간 초과 기간이 만료될 때까지 해당 컴퓨터에서의 로그인은 허용되지 않습니다.

◆ sysTrapIPAddressLocked

OID	1.3.6.1.4.1.21317.1.3.8.3.4
상태	활성 (current)
설명	유효하지 않은 로그인 시도 횟수가 지정된 양을 초과하면 원격 컴퓨터의 IP 주소가 잠깁니다. 타임아웃 기간이 만료될 때까지 해당 컴퓨터에서의 로그인은 허용되지 않습니다.

◆ sysTrapLogout

OID	1.3.6.1.4.1.21317.1.3.8.3.5
상태	활성 (current)
설명	사용자가 시스템에서 로그아웃하였습니다.

◆ sysTrapBViewerStart

OID	1.3.6.1.4.1.21317.1.3.8.3.6
상태	활성 (current)
설명	브라우저에서 뷰어용 세션이 생성되었습니다.

◆ sysTrapBViewerEnd

OID	1.3.6.1.4.1.21317.1.3.8.3.7
상태	활성 (current)
설명	브라우저 뷰어 세션이 종료되었습니다.

◆ sysTrapSwitchPort

OID	1.3.6.1.4.1.21317.1.3.8.3.8
상태	활성 (current)
설명	사용자가 포트를 전환했습니다.

◆ sysTrapRemoteVMStart

OID	1.3.6.1.4.1.21317.1.3.8.3.9
상태	활성 (current)
설명	원격 사용자가 원격 버추얼 미디어를 실행했습니다.

◆ sysTrapRemoteVMStop

OID	1.3.6.1.4.1.21317.1.3.8.3.10
상태	활성 (current)
설명	원격 사용자가 원격 버추얼 미디어 마운트를 해제했습니다.

◆ sysTrapLocalVMStart

OID	1.3.6.1.4.1.21317.1.3.8.3.11
상태	활성 (current)
설명	사용자가 로컬 버추얼 미디어를 실행했습니다.

◆ sysTrapLocalVMStop

OID	1.3.6.1.4.1.21317.1.3.8.3.12
상태	활성 (current)
설명	사용자가 로컬 버추얼 미디어 마운트를 해제했습니다.

◆ sysTrapRemoteCRStart

OID	1.3.6.1.4.1.21317.1.3.8.3.13
상태	활성 (current)
설명	원격 사용자가 원격 스마트 카드 리더기를 실행했습니다.

◆ sysTrapRemoteCRStop

OID	1.3.6.1.4.1.21317.1.3.8.3.14
상태	활성 (current)
설명	원격 사용자가 원격 스마트 카드 리더기의 마운트를 해제했습니다.

◆ sysTrapLocalCRStart

OID	1.3.6.1.4.1.21317.1.3.8.3.15
상태	활성 (current)
설명	사용자가 로컬 스마트 카드 리더기를 호출했습니다.

◆ sysTrapLocalCRStop

OID	1.3.6.1.4.1.21317.1.3.8.3.16
상태	활성 (current)
설명	사용자가 로컬 스마트 카드 리더기를 마운트 해제했습니다.

◆ sysTrapOutletON

OID	1.3.6.1.4.1.21317.1.3.8.3.17
상태	활성 (current)
설명	선택한 아웃렛에 전원 켜기 신호를 전송합니다.

◆ sysTrapOutletOFF

OID	1.3.6.1.4.1.21317.1.3.8.3.18
상태	활성 (current)
설명	선택한 아웃렛에 전원 끄기 신호를 전송합니다.

◆ sysTrapOutletCycle

OID	1.3.6.1.4.1.21317.1.3.8.3.19
상태	활성 (current)
설명	선택한 아웃렛에 재시작 신호를 전송합니다.

◆ sysTrapModemdailin

OID	1.3.6.1.4.1.21317.1.3.8.3.20
상태	활성 (current)
설명	모뎀 다이얼인이 성공했습니다.

◆ sysTrapModemdailinFailed

OID	1.3.6.1.4.1.21317.1.3.8.3.21
상태	활성 (current)
설명	모뎀 다이얼인이 실패했습니다.

◆ sysTrapModemdailout

OID	1.3.6.1.4.1.21317.1.3.8.3.22
상태	활성 (current)
설명	모뎀 다이얼아웃이 성공했습니다.

◆ sysTrapModemdailoutFailed

OID	1.3.6.1.4.1.21317.1.3.8.3.23
상태	활성 (current)
설명	모뎀 다이얼아웃이 실패했습니다.

◆ sysTrapModemdailback

OID	1.3.6.1.4.1.21317.1.3.8.3.24
상태	활성 (current)
설명	모뎀 다이얼백이 성공했습니다.

◆ sysTrapModemdailbackFailed

OID	1.3.6.1.4.1.21317.1.3.8.3.25
상태	활성 (current)
설명	모뎀 다이얼백이 실패했습니다.

◆ sysTrapModifyPortCfg

OID	1.3.6.1.4.1.21317.1.3.8.3.26
상태	활성 (current)
설명	사용자가 포트 구성을 수정했습니다.

◆ sysTrapAddUser

OID	1.3.6.1.4.1.21317.1.3.8.3.27
상태	활성 (current)
설명	새 사용자 계정을 생성합니다.

◆ sysTrapModifyUser

OID	1.3.6.1.4.1.21317.1.3.8.3.28
상태	활성 (current)
설명	사용자 관리 권한을 가진 사용자가 사용자 계정을 수정했습니다.

◆ sysTrapDeleteUser

OID	1.3.6.1.4.1.21317.1.3.8.3.29
상태	활성 (current)
설명	사용자 관리 권한을 가진 사용자가 사용자 계정을 제거했습니다.

◆ sysTrapAddGroup

OID	1.3.6.1.4.1.21317.1.3.8.3.30
상태	활성 (current)
설명	새 그룹을 생성합니다.

◆ sysTrapModifyGroup

OID	1.3.6.1.4.1.21317.1.3.8.3.31
상태	활성 (current)
설명	관리자가 그룹 설정을 수정했습니다.

◆ sysTrapDeleteGroup

OID	1.3.6.1.4.1.21317.1.3.8.3.32
상태	활성 (current)
설명	관리자가 그룹을 제거했습니다.

◆ sysTrapModifyDevInfo

OID	1.3.6.1.4.1.21317.1.3.8.3.33
상태	활성 (current)
설명	장치 정보 설정이 수정되었습니다.

◆ sysTrapModifyOperationSetting

OID	1.3.6.1.4.1.21317.1.3.8.3.34
상태	활성 (current)
설명	작업 설정이 수정되었습니다.

◆ sysTrapModifyNetworkSetting

OID	1.3.6.1.4.1.21317.1.3.8.3.35
상태	활성 (current)
설명	네트워크 설정이 수정되었습니다.

◆ sysTrapModifyANMSSetting

OID	1.3.6.1.4.1.21317.1.3.8.3.36
상태	활성 (current)
설명	ANMS 설정이 수정되었습니다.

◆ sysTrapModifyNotificationSetting

OID	1.3.6.1.4.1.21317.1.3.8.3.38
상태	활성 (current)
설명	알림 설정이 수정되었습니다.

◆ sysTrapModifyOOBCSetting

OID	1.3.6.1.4.1.21317.1.3.8.3.39
상태	활성 (current)
설명	OOBC (대역 외 제어) 설정이 수정되었습니다.

◆ sysTrapModifySecuritySetting

OID	1.3.6.1.4.1.21317.1.3.8.3.40
상태	활성 (current)
설명	보안 설정이 수정되었습니다.

◆ sysTrapModifyDateTimeSetting

OID	1.3.6.1.4.1.21317.1.3.8.3.41
상태	활성 (current)
설명	시간 설정이 수정되었습니다.

◆ sysTrapModifyIPAddress

OID	1.3.6.1.4.1.21317.1.3.8.3.42
상태	활성 (current)
설명	장치 IP 주소가 변경되었습니다.

◆ sysTrapLogServerConnectionFailed

OID	1.3.6.1.4.1.21317.1.3.8.3.43
상태	활성 (current)
설명	ATEN 로그 서버 연결에 실패했습니다.

◆ sysTrapUploadCertificate

OID	1.3.6.1.4.1.21317.1.3.8.3.44
상태	활성 (current)
설명	사용자가 인증서를 업로드했습니다.

◆ sysTrapRestoreDefaultCertificate

OID	1.3.6.1.4.1.21317.1.3.8.3.45
상태	활성 (current)
설명	사용자가 기본 ATEN 인증서를 사용하기 위해 기본값 복원을 호출했습니다.

◆ sysTrapUploadCSR

OID	1.3.6.1.4.1.21317.1.3.8.3.48
상태	활성 (current)
설명	사용자가 CSR을 업로드했습니다.

◆ sysTrapInvalidIPAccess

OID	1.3.6.1.4.1.21317.1.3.8.3.49
상태	활성 (current)
설명	유효하지 않은 IP 접근입니다.

◆ sysTrapInvalidMACAccess

OID	1.3.6.1.4.1.21317.1.3.8.3.50
상태	활성 (current)
설명	유효하지 않은 MAC 접근입니다.

◆ sysTrapNTP

OID	1.3.6.1.4.1.21317.1.3.8.3.51
상태	활성 (current)
설명	사용자 NTP 작업이 성공했습니다.

◆ sysTrapNTPFailed

OID	1.3.6.1.4.1.21317.1.3.8.3.52
상태	활성 (current)
설명	사용자 NTP 작업이 실패했습니다.

◆ sysTrapDeleteLog

OID	1.3.6.1.4.1.21317.1.3.8.3.53
상태	활성 (current)
설명	사용자가 로그 삭제 작업을 수행했습니다.

◆ sysTrapUpgradeFW

OID	1.3.6.1.4.1.21317.1.3.8.3.54
상태	활성 (current)
설명	사용자가 시스템 펌웨어를 업그레이드했습니다.

◆ sysTrapUpgradeFWFailed

OID	1.3.6.1.4.1.21317.1.3.8.3.55
상태	활성 (current)
설명	사용자가 시스템 펌웨어 업그레이드를 시도했으나 실패했습니다.

◆ sysTrapUpgradeAdapter

OID	1.3.6.1.4.1.21317.1.3.8.3.56
상태	활성 (current)
설명	사용자가 어댑터 펌웨어를 업그레이드했습니다.

◆ sysTrapUpgradeAdapterFailed

OID	1.3.6.1.4.1.21317.1.3.8.3.57
상태	활성 (current)
설명	사용자가 어댑터 펌웨어 업그레이드를 시도했으나 실패했습니다.

◆ sysTrapUpgradePDU

OID	1.3.6.1.4.1.21317.1.3.8.3.58
상태	활성 (current)
설명	사용자가 PDU 펌웨어를 업그레이드했습니다.

◆ sysTrapUpgradePDUFailed

OID	1.3.6.1.4.1.21317.1.3.8.3.59
상태	활성 (current)
설명	사용자가 PDU 펌웨어 업그레이드를 시도했으나 실패했습니다.

◆ sysTrapBackupSystemConfiguration

OID	1.3.6.1.4.1.21317.1.3.8.3.60
상태	활성 (current)
설명	사용자가 시스템 구성을 백업했습니다.

◆ sysTrapRestoreSystemConfiguration

OID	1.3.6.1.4.1.21317.1.3.8.3.61
상태	활성 (current)
설명	사용자가 시스템 구성을 복원했습니다.

◆ sysTrapRestoreSystemConfigurationFailed

OID	1.3.6.1.4.1.21317.1.3.8.3.62
상태	활성 (current)
설명	사용자가 시스템 구성을 복원하려고 시도했으나 실패했습니다.

◆ sysTrapClearPortName

OID	1.3.6.1.4.1.21317.1.3.8.3.63
상태	활성 (current)
설명	사용자가 포트 이름을 삭제했습니다.

◆ sysTrapRestoreDefaultSetting

OID	1.3.6.1.4.1.21317.1.3.8.3.64
상태	활성 (current)
설명	사용자가 시스템 구성을 기본값으로 재설정했습니다.

◆ sysTrapResetSystem

OID	1.3.6.1.4.1.21317.1.3.8.3.65
상태	활성 (current)
설명	사용자가 시스템을 리셋했습니다.

◆ sysTrapSystemPowerOn

OID	1.3.6.1.4.1.21317.1.3.8.3.66
상태	활성 (current)
설명	전원이 켜졌습니다.

◆ sysTrapSystemPowerOff

OID	1.3.6.1.4.1.21317.1.3.8.3.67
상태	활성 (current)
설명	전원이 꺼졌습니다.

◆ sysTrapTemperatureWarning

OID	1.3.6.1.4.1.21317.1.3.8.3.69
상태	활성 (current)
설명	온도가 센서 임계값을 초과했습니다.

◆ sysTrapFanSpeedWarning

OID	1.3.6.1.4.1.21317.1.3.8.3.70
상태	활성 (current)
설명	비정상적인 팬 속도입니다.

◆ sysTrapEndSession

OID	1.3.6.1.4.1.21317.1.3.8.3.71
상태	활성 (current)
설명	관리자가 강제로 사용자를 시스템에서 로그아웃 했습니다.

◆ sysTrapAddDevice

OID	1.3.6.1.4.1.21317.1.3.8.3.72
상태	활성 (current)
설명	장치를 추가합니다.

◆ sysTrapDeleteDevice

OID	1.3.6.1.4.1.21317.1.3.8.3.73
상태	활성 (current)
설명	장치를 제거합니다.

◆ sysTrapAddLogServer

OID	1.3.6.1.4.1.21317.1.3.8.3.74
상태	활성 (current)
설명	로그서버를 추가합니다.

◆ sysTrapModifyLogServerSetting

OID	1.3.6.1.4.1.21317.1.3.8.3.75
상태	활성 (current)
설명	로그서버 설정을 수정합니다.

◆ sysTrapDeleteLogServer

OID	1.3.6.1.4.1.21317.1.3.8.3.76
상태	활성 (current)
설명	로그서버를 삭제합니다.

◆ sysTrapCreateCheckPoint

OID	1.3.6.1.4.1.21317.1.3.8.3.77
상태	활성 (current)
설명	체크 포인트를 생성합니다.

◆ sysTrapSystemStart

OID	1.3.6.1.4.1.21317.1.3.8.3.78
상태	활성 (current)
설명	시스템을 시작합니다.

◆ sysTrapSystemStop

OID	1.3.6.1.4.1.21317.1.3.8.3.79
상태	활성 (current)
설명	시스템을 중지합니다.

◆ sysTrapSystemDiskFull

OID	1.3.6.1.4.1.21317.1.3.8.3.80
상태	활성 (current)
설명	디스크가 가득 찼습니다.

ATEN 표준 보증 정책

보증 정책은 제품 카테고리 및 구매 지역에 따라 다를 수 있습니다. 자세한 내용은 ATEN의 공식 웹사이트를 방문하여 구매 국가/지역을 선택한 후 지원 센터로 이동하거나 현지 ATEN 영업 담당자에게 연락하여 추가 지원을 받으십시오.

© Copyright 2025 ATEN® International Co., Ltd.
Released: 2025-10-28

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.