Simply Better Connections

ATEN Altusen™

CCVSR

Video Session Recording Software

User Manual

User Information

Online Registration

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

International	http://eservice.aten.com

Telephone Support

For telephone support, call this number:

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

User Notice

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

Product Information

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

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

Package Contents

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

The CCKM Video Session Recording Software package consists of:

1 CCKM USB License Key

1 software CD

1 user instructions*

Contents

Chapter 1.
Introduction

Chapter 2.
CCVSR Installation

Chapter 3.
The User Interface

Chapter 7.
User Accounts

Chapter 8.
System

Chapter 9.
Logs

Chapter 10.
CCVSR Archive Server

Appendix A

Authentication Key Utility

About This Manual

This manual is provided to help you get the most out of your CCVSR system. It covers all aspects of the software, including installation, configuration, and operation.

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

Chapter 1, ***Introduction*****,** introduces you to the Video Session Recording Software, with its purpose, features, benefits, and requirements presented.

Chapter 2, ***CCVSR Installation*****,** provides step-by-step instructions for installing the Video Session Recording Software software.

Chapter 3, ***The User Interface*****,** explains how to log in to the Video Session Recording Software using a web browser.

Chapter 4, ***Playback*****,** explains how to use the functions of the Playback page for searching for and playing back video log files.

Chapter 5, *Liveview*, explains the centralized live view, which includes the favorite devices / ports, more playback options, single port mode, etc..

Chapter 6, *Device Management***,** elaborates on how KVM devices can be added and their ports configured, using Video Session Recording Software.

Chapter 7, *User Accounts***,** explains how to create additional user accounts, modify and delete users and/or user groups, assigning attributes to them, as well as authentication settings.

Chapter 8, ***System*****,** explains how to use the System Management page to redefine the *Server Info* and configure *Notification, Security*, *License*, *Backup & Restore*, and *Recording* settings.

Chapter 9, ***Logs*****,** shows how to use the log file utilities to view the events that has occurred and been recorded on the Video Session Recording Software.

Chapter 10, ***CCVSR Archive Server*****,** describes how to use the CCVSR Archive Server, and explains its features and function.

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

Appendix B, Authentication Key Utility, describes how to access and update the information contained in the CCVSR Authentication Key.

Note:

- Read this manual thoroughly and follow the installation and operation procedures carefully to prevent any damage to the unit or connected devices.
- ATEN regularly updates its product documentation for new features and fixes. For an up-to-date CCVSR documentation, visit http://www.aten.com/global/en/

Conventions

This manual uses the following conventions:

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

Chapter 1
Introduction

Overview

ATEN's Control Center Video Session Recording (CCVSR) software is an innovative and effective solution designed for live monitoring and operation backtracking. Administrators can view live feed of operators currently operating on their systems and thus quickly resolve operational flaws, process discrepancies, etc. On the other hand, IT managers can go back to recorded operation videos to trace changes made for compliance control improvement and auditing efficiency.

Featuring the LiveView function, CCVSR provides live-video surveillance to allow administrators to monitor multiple KVM ports in real time. Various layout combinations and customizable layouts are available for selection by users to monitor multiple channels simultaneously. The LiveView function is especially suitable for industrial environments, such as production lines, which require real-time monitoring of continuous operations and system performance to facilitate timely responses to abnormalities or emergencies for administrators. Moreover, the LiveView page also implements the Playback function to allow users to quickly view older videos of the same channel for troubleshooting or problem solving.

The CCVSR automatically starts recording user sessions when users start accessing target servers locally or remotely through KVM over IP switch and/or serial console servers. Whatever the target server's operating status is, whether it is booting up the operating system, logging in, logging out, or in pre-boot BIOS mode, all activities and operations, such as video display, key strokes and mouse clicks are recorded. The CCVSR can also record continuously without keeping the WinClient and JavaClient running.

Without requiring agent software installation on target computers, the CCVSR is installed and operated independently as a server. It therefore does not require resource allocations from all target computers, including CPU, disk space, memory, and network bandwidth. Moreover, no agent software installation means that the CCVSR provides a non-intrusive method for user session recording. In IT-related environments, such as server rooms, data centers, and industrial settings like manufacturing plants, security is one of the first considerations on any administrator's mind. As a non-intrusive solution to provide reliable live-video surveillance and video session recording, implementing CCVSR minimizes both security concerns and accidents.

The CCVSR is enhanced with an HTML5 user interface, aiming to deliver a better user experience and advanced usability via its clear and concise interface, simplified structure, improved text readability, increased icon visibility, as well as ancillary functions such as system notifications. The UI's minimalist flat design aesthetic and two levels of typographic hierarchy, with the features grouped into self-explanatory handy sidebar, enable users to smoothly navigate and complete tasks intuitively.

The CCVSR system is scalable, supporting a single server and up to 3 secondary servers (to expand recording storage) setups. The system uses Primary-Secondary architecture to offer service redundancy. During standard operation, a Secondary server (max. 3 servers) acts as a storage server to store recorded videos. Moreover, if the Primary server fails, one of the Secondary servers can provide the required management and recording services for KVM over-IP Switches until the Primary server is back online. This feature ensures that the recording service is always on and uninterruptible. The CCVSR manages video recordings and allows all administrative activity to be controlled from a central CCVSR server (Primary server) through a single IP port, giving administrators access to all CCVSR data from one computer.

By integrating the CCVSR into your KVM installation, you can automate the security of your server room and make auditing an effective tool.

Features

- Automatically create complete recordings of a computer’s operations when remote users access a KVM port – which are saved to an indexed database for advanced searches
- Supports high quality video recordings – with a video resolution up to 1920 x 1200 with 24 bit color depth
- Supports recording on multiple KVM over IP Switches
- Simultaneously records and plays the operation of multiple KVM ports*
- Search functions with keyword filters for video recordings
- Special video player tools with format, video record exporting, and password protection for enhanced security
- IP Filter for enhanced protection
- System event notification via SMTP email; SNMP trap and Syslog support
- Configurable user and group permissions – for search, play, system management, record management, and save management
- Port level permissions – users can only view ports they have been authorized on
- Supports device level event logs
- Archive Server Support
- Multilanguage GUI Supports: English, Traditional Chinese, Simplified Chinese, Japanese, and Korean
- Automatically runs software as daemon service in the background
- Multi-browser support: Internet Explorer, Chrome, Firefox, Safari
- Supports TLS 1.2 data encryption and RSA 2048-bit certificates for secure web browser logins
- 3rd party remote authentication supports: RADIUS, LDAP, LDAPS, and MS AD Directory

Note: 1. Up to 20 KVM sessions (Resolution = 1920x1080, Text Mode = On, Bandwidth = 1G, Scenario = Surveillance) can be recorded and streamed at any time when the recommended hardware requirements of the CCVSR server are met.

2. Up to 64 KVM devices can be supported by one CCVSR server.

Requirements

Computer

Systems that the CCVSR will be installed on should meet the following requirements:

- Server Hardware Requirements
  - CPU: Intel Xeon D-1527 4 cores 2.2 GHz or equivalent
  - Memory: 8 GB or above
  - Hard drive (for CCVSR): 4 GB or above
  - Network: 1 Gbps
- Client Hardware Requirements
  - CPU: Intel Core i5-7600 4 cores 3.5 GHz or equivalent
  - Memory: 6 GB or above
  - Network: 1 Gbps
- Operating System Requirements:
  - Windows: 10, 8, 7 or the following versions of Linux

OS	Version	Type	Kernel
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 Viewer (Java-based application for video playback on a client computer) Requirements:
  - JRE 8 or Zulu OpenJDK 8 FX (Windows only)

KVM over IP Switch

Computers to be recorded by the Video Session Recorder must be connected to a port on a KVM over IP Switch* (refer to the *Specification* section on the CCVSR product page).

Note: Computers connected to cascaded KVM switches are not supported.

Browsers

Supported browsers for users that log into the CCVSR include the following:

Browser	Version
Microsoft Edge	44.18362.449 or later
Internet Explorer	11.0.9600 or later
Chrome	69.0.3497.100 or later
Firefox	62.0.3 or later

Bandwidth Requirement

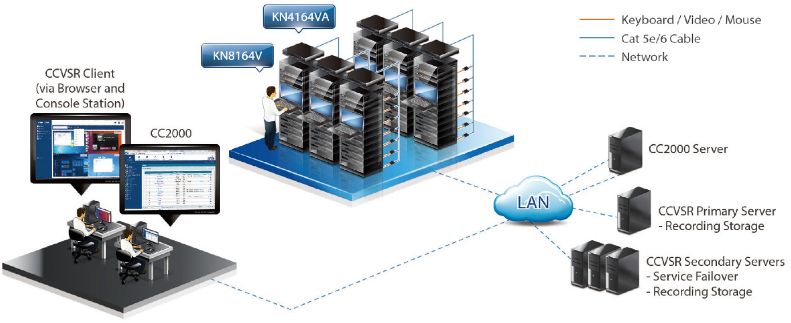
1920 x 1080, Text Mode = On, 1G Bandwidth

	General Operations (e.g. settings configuration, file editing, etc.)	Surveillance (e.g. NVR, playing videos, etc.)
KN8164V	3.37 Mbps / Channel 1 hour video size: 296 MB	44.6 Mbps / Channel 1 hour video size: 4 GB
CN8000A	12.40 Mbps/Channel 1 hour video size: 599 MB	32.4 Mbps / Channel 1 hour video size: 1.7 GB
CN9950 (4K)	17.2 Mbps / Channel 1 hour video size: 1.56 GB	189 Mbps / Channel 1 hour video size: 17.2 GB
CN9950 (1080P)	11.1 Mbps / Channel 1 hour video size: 0.93 GB	208 Mbps / Channel 1 hour video size: 17.5 GB

Note: 1. Numbers above are for reference only, actual bandwidth requirement may vary (e.g. resolution, KVM model, KVM settings, Operations from a remote server, etc.).

2. All videos recorded on the CCVSR are compressed prior to being stored.
3. Your computer's CPU resource is used when the system compresses the recorded videos. The CPU resource is released as soon as the compression is complete.
4. For CN9950, 4K's required bandwidth is lower than that of 1080P under surveillance scenario because its FPS is lowered when reaching the upper bound of its performance.

An Example of CCVSR Deployment



Primary Servers

Management - A Primary Server is the central management software used to record, view, and manage all aspects of a CCVSR installation. All Secondary Servers, Archive Servers, and Nodes work through the Primary Server.

Secondary Servers

Storage - Secondary Servers reduce the work load and provide extended storage for the Primary Server - with limited configuration functionality.

Redundancy - When the primary server fails to work, one of the secondary servers will work as primary server temporarily for service availability.

Refer to the following table for supported functions of primary, secondary, and archive servers.

Functions	Primary	Secondary (Storage)	Secondary (Redundancy)	Archive
System management	✓		view-only	
Device management	✓		view-only	
User management	✓		view-only	
Local management	✓	✓	✓	
Video & keystroke recording	✓	✓	✓	
Video search & playback	✓		✓	✓
Backup video & keystrokes				✓

Archive Servers

Archive - The Archive Server automatically archives all video log files created on the Primary Server into a separate organized database for extended backup and viewing. The Archive Server allow you to import, export, and allocate large databases separate from the CCVSR system.

Nodes

KVM Ports - A node is a physical port on a KVM over IP Switch. Each node you want to record video logs on requires a license.

Licenses

The CCVSR license controls the number of Primary Servers, Secondary Servers, Archive Servers, and nodes permitted on the CCVSR installation. License information is contained on the USB License Key that came with your CCVSR purchase. For a deployment example, see *Node Options*, page 9, for details.

Upon completion of the CCVSR software installation, the number of licenses that you purchased is automatically added. To add more, you must upgrade the license. See *License*, page 71, for more information.

License Options

License	Nodes	Primary Servers
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

Node Options

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

Archive Server Options

License	Servers
CCVSRAS1	1

This Page Intentionally Left Blank

Chapter 2
CCVSR Installation

Overview

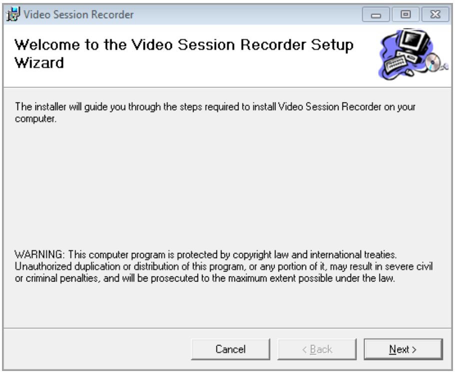
This chapter describes how to install the Video Session Recording Software (CCVSR) on a computer. The CCVSR application runs background services for the Video Session Recording Software to operate and is used to set basic server configurations. The CCVSR application must be running for the Video Session Recording Software's web browser features to work. To install the CCVSR software on a Linux server, see *Linux Installation*, page 100.

Installing the CCVSR Software

Starting the Installation

To install the CCVSR application on a Windows system, do the following:

1. Put the CD that came with your package into the computer's CD drive.
2. Go to the folder where the *setup.exe* file is located, and execute it. A screen, similar to the one below, appears:



Welcome to the Video Session Recorder Setup Wizard

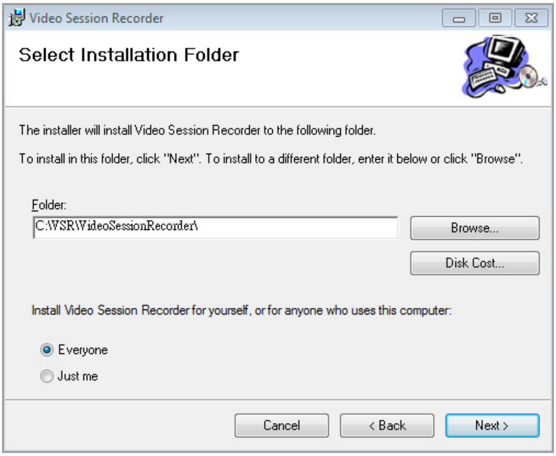
The installer will guide you through the steps required to install Video Session Recorder on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

   Click **Next** to continue.

3. On the *Select Installation Folder* page, specify the installation folder, or click **Browse** to choose the location where you want to install it. Then choose if you want to install it for yourself (**Just me**), or for anyone who

uses this computer (**Everyone**). Click **Disk Cost** to view available drives and disk space.



Video Session Recorder

Select Installation Folder

The installer will install Video Session Recorder to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\VSR\VideoSessionRecorder\

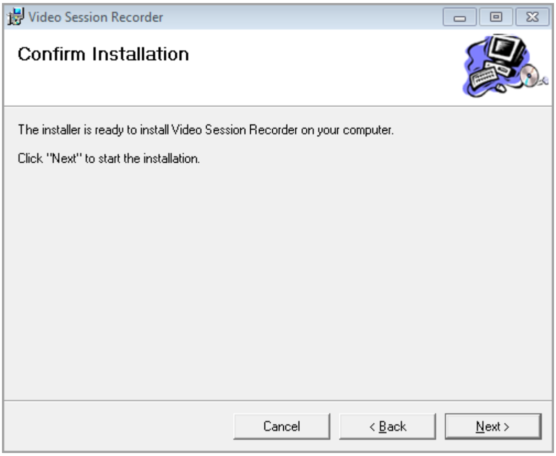
Install Video Session Recorder for yourself, or for anyone who uses this computer:

● Everyone

○ Just me

Click **Next** to continue.

4. The *Confirm Installation* window appears, click **Next** to continue:



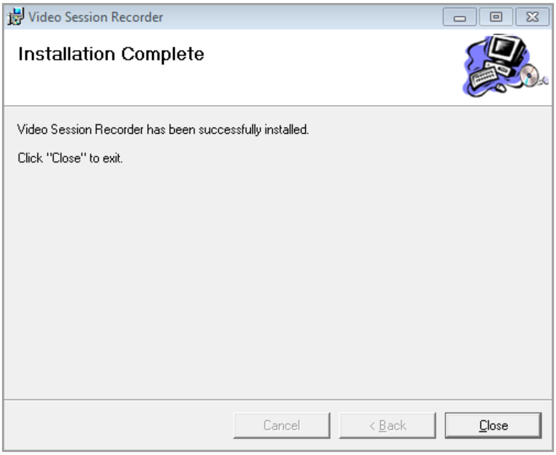
Video Session Recorder

Confirm Installation

The installer is ready to install Video Session Recorder on your computer.

Click "Next" to start the installation.

5. When the installation is complete the following message will appear:



Installation Complete

Video Session Recorder has been successfully installed.

Click "Close" to exit.

Licenses

Upon completion of the CCVSR software installation, a default license for one server is automatically provided. To add more Video Session Recording Softwares, you must upgrade the license. To upgrade the license, See *License*, page 71, for details. For License options See *Node Options*, page 9, for details.

This Page Intentionally Left Blank

Chapter 3
The User Interface

Overview

The Video Session Recording Software's user interface is accessed via web browser and contains the main features and functions. This chapter explains how to login to the Video Session Recording Software and highlights the browser components.

Browser Login

The Video Session Recording Software is accessed via an Internet browser running on any platform. To access the Video Session Recording Software's browser interface, the CCVSR application must be started.

To access the Video Session Recording Software, do the following:

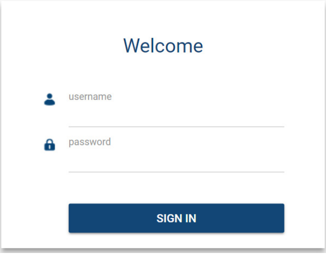
1. Open the browser and specify the IP address and service port of the Video Session Recording Software you want to access in the browser's location bar.

   For example: `https://192.168.0.100:9443`

   If you wish to log in locally, enter https://127.0.0.1:9443 instead.

2. When a Security *Alert* dialog box appears, accept the certificate – it can be trusted. If a second certificate appears, accept it as well (see *Trusted Certificates*, page 101).

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



Welcome

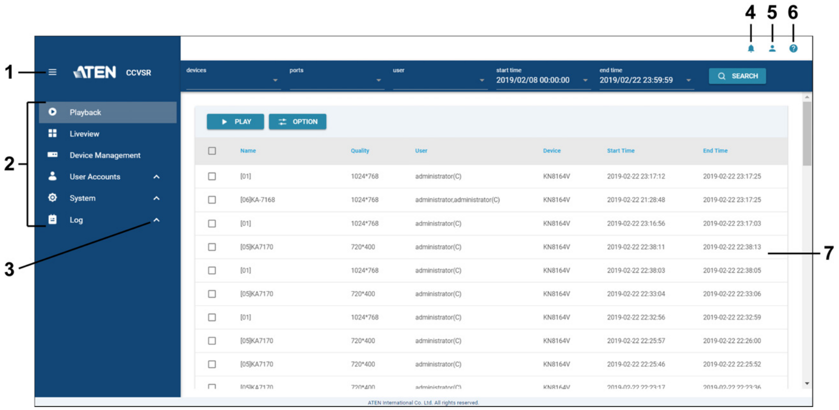
3. Provide your username and password, then click **Login** to bring up the Web Main Page.

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

4. If you are logging in for the first time, the system will prompt you to change the password.

The Web Browser Main Page

Once users login and are authenticated, the *Web Browser Main Page* comes up, with the *Playback* page displayed:



start time 2019/02/08 00:00:00

end time 2019/02/22 23:59:59

□	Name	Quality	User	Device	Start Time	End Time
□	[01]	1024*768	administrator(C)	KN8164V	2019-02-22 23:17:12	2019-02-22 23:17:25
□	[06]KA-7168	1024*768	administrator,administrator(C)	KN8164V	2019-02-22 21:28:48	2019-02-22 23:17:25
□	[01]	1024*768	administrator(C)	KN8164V	2019-02-22 23:16:56	2019-02-22 23:17:03
□	[05]KA7170	720*400	administrator(C)	KN8164V	2019-02-22 22:38:11	2019-02-22 22:38:13
□	[01]	1024*768	administrator(C)	KN8164V	2019-02-22 22:38:03	2019-02-22 22:38:05
□	[05]KA7170	720*400	administrator(C)	KN8164V	2019-02-22 22:33:04	2019-02-22 22:33:06
□	[01]	1024*768	administrator(C)	KN8164V	2019-02-22 22:32:56	2019-02-22 22:32:59
□	[05]KA7170	720*400	administrator(C)	KN8164V	2019-02-22 22:25:57	2019-02-22 22:26:00
□	[05]KA7170	720*400	administrator(C)	KN8164V	2019-02-22 22:25:46	2019-02-22 22:25:52
□	[05]KA7170	720*400	administrator(C)	KN8164V	2019-02-22 22:23:17	2019-02-22 22:23:36

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

Page Components

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

No.	Item	Description
1	Expand / Collapse Main Menu	Click this icon to expand or collapse main menu. The sub-menu can be accessed by clicking on their main operation categories.
2	Main Menu	Main Menu contains the Video Session Recording Software's main operation categories. The items that appear here are determined by the user's type, and the authorization options that were selected when the user's account was created.

No.	Item	Description
3	Expand / Collapse Sub-Menu	The up/down arrow indicates that the operation categories can be expanded or collapsed into sub menus. Click the operation categories to expand/collapse into sub menus, which contains operational sub-categories of the Main Menu. The items that appear here are determined by the user's type, and the authorization options that were selected when the user's account was created.
4	Notification / Message Center (Super Administrator only)	Click this icon for the notifications / messages of the system. Up to 50 notifications can be displayed here (use the scroll bar to scroll through the notifications). If there are unread notifications, a number will be shown above the notification icon. e.g. 🔔3 Click **CLEAR ALL** to clear the notifications / messages. Click **VIEW LOGS** to go to the system logs page.
5	Personal	Click this button for personal information and configurations. ◆ Displayed information include the user's username and when the user last logged into the system. ◆ Preferences: Click this to configure personal preference settings. ◆ Change password: Click this to change the password. ◆ Log out: Click this log out of the current session of this user. Refer to *Personal Configuration* on page 19 for more information.
6	Help	Click this button for **Online help** or **About**. Clicking **Online help** brings you to the online user manual. Clicking **About** displays the current firmware version.
7	Interactive Display Panel	This is your main work area. The screens that appears reflects your menu choices.

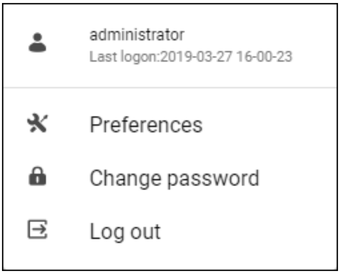
Main Menu

Main Menu is displayed differently for different user types (Super Administrator, Administrator, User) and permissions (assigned when the user account was created). The functions are explained in the table below:

Operation Item	Function
Playback	The Playback page is used to search and playback available video logs, and to monitor current browser sessions. Playback is discussed on page 21.
Liveview	The Liveview page allows the users to view live KVM ports feed. Liveview is discussed on page 31.
Device Management	The Device Management page is used to add KVM devices and configure the ports for recording video logs. This page is available to the Super Administrator, as well as administrators and users who have been given Device Management permission. The item does not appear for other administrators and users. The Device Management is discussed on page 37.
User Accounts	The User Accounts page is used to create and manage Users and Groups. It can also be used to assign devices to them. This item is available to the Super Administrator, as well as administrators and users who have been given User Management permission. The item doesn't appear for other administrators and users. User Accounts is discussed on page 43.
System	The Systems page is used to configure the Video Session Recording Software's system settings and to add secondary servers from the network. System is discussed on page 55.
Log	The Log page displays the contents of the log file. The Log page is discussed on page 81.

Personal Info / Configuration

On the top right-hand corner of the page, you can click the *Personal* icon (👤) for personal information and configurations:



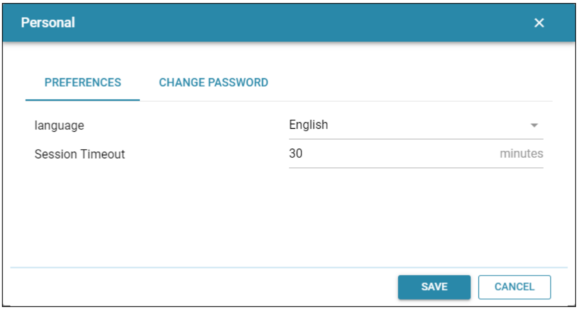
administrator
Last logon:2019-03-27 16-00-23

- The top section displays information including the user's username and when the user last logged into the system.
- Preferences: Click this to configure personal preference settings.
- Change password: Click this to change the password.
- Log out: Click this log out of the current session of this user.

Personal Configuration

Preference

Click *Preference* for the pop-up window shown below:



Personal

language: English

Session Timeout: 30 minutes

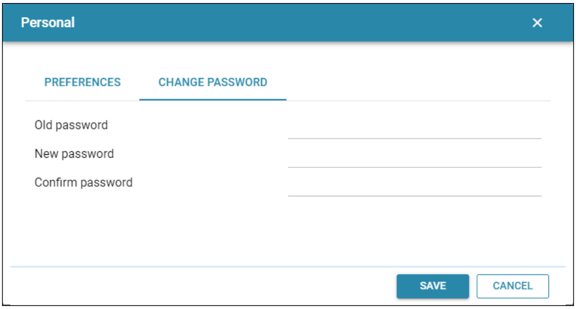
Language: Click the drop-down menu to select your preferred language.

Session Timeout: Enter a value for how long a user can stay logged into the system. Enter **0** if you wish to stay logged into the system until you manually log out.

Click *Save* to save the changes.

Change Password

Click *Change Password* for the pop-up window shown below:



Personal

Old password

New password

Confirm password

Enter the old password, new password and the new password again.

Click *Save* to save the changes.

Logout

Click *Log out* to logout of the system.

Chapter 4
Playback

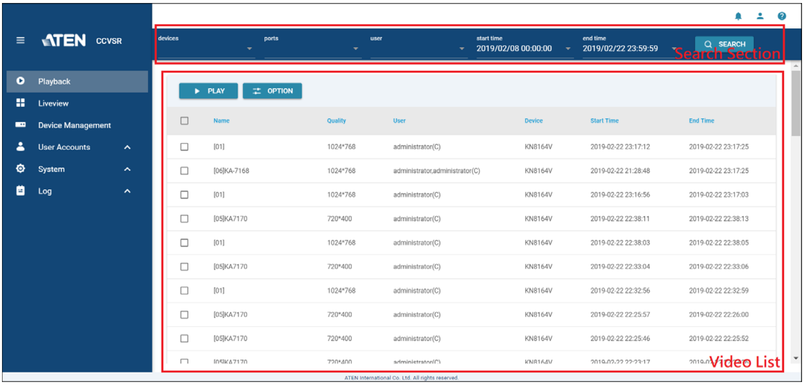
Overview

The *Playback* page is used to search and play video log files. Before using the Playback function, you must first add a KVM device, see *Recording KVM Ports*, page 38 for details.

When you log into the Video Session Recording Software, you are automatically brought to this page.

On top of the page is a Search section, where it acts as a filter to help you quickly search for video logs.

Below the search section is the Video List section that shows the ports having recorded video logs.



devices
ports
user
start time 2019/02/08 00:00:00
end time 2019/02/22 23:59:59

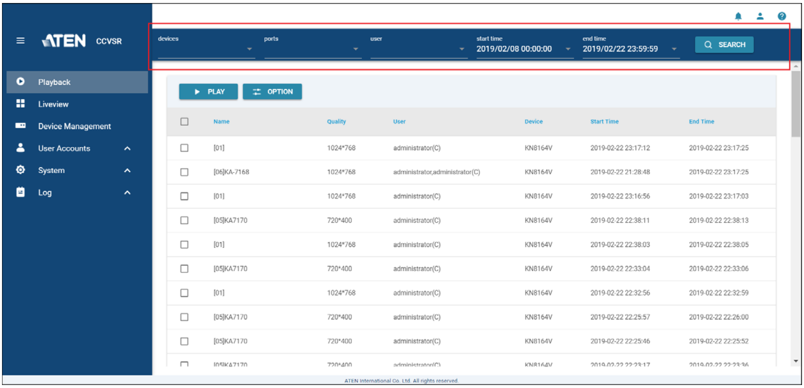
□	Name	Quality	User	Device	Start Time	End Time
□	[01]	1024*768	administrator(C)	KN8164V	2019-02-22 23:17:12	2019-02-22 23:17:25
□	[06]KA-7168	1024*768	administrator,administrator(C)	KN8164V	2019-02-22 21:28:48	2019-02-22 23:17:25
□	[01]	1024*768	administrator(C)	KN8164V	2019-02-22 23:16:56	2019-02-22 23:17:03
□	[05]KA7170	720*400	administrator(C)	KN8164V	2019-02-22 22:38:11	2019-02-22 22:38:13
□	[01]	1024*768	administrator(C)	KN8164V	2019-02-22 22:38:03	2019-02-22 22:38:05
□	[05]KA7170	720*400	administrator(C)	KN8164V	2019-02-22 22:33:04	2019-02-22 22:33:06
□	[01]	1024*768	administrator(C)	KN8164V	2019-02-22 22:32:56	2019-02-22 22:32:59
□	[05]KA7170	720*400	administrator(C)	KN8164V	2019-02-22 22:25:57	2019-02-22 22:26:00
□	[05]KA7170	720*400	administrator(C)	KN8164V	2019-02-22 22:25:46	2019-02-22 22:25:52
□	[05]KA7170	720*400	administrator(C)	KN8164V	2019-02-22 22:23:17	[illegible]

ATEN International Co. Ltd. All rights reserved.

Scroll through the list to find the desired video logs. You can also click the headings (port) name, (video) quality, user, device and time to sort the list into alphabetical order, quality from best to worst, etc. to help you find the desired video logs.

Search

On top of the page, a search section is displayed.

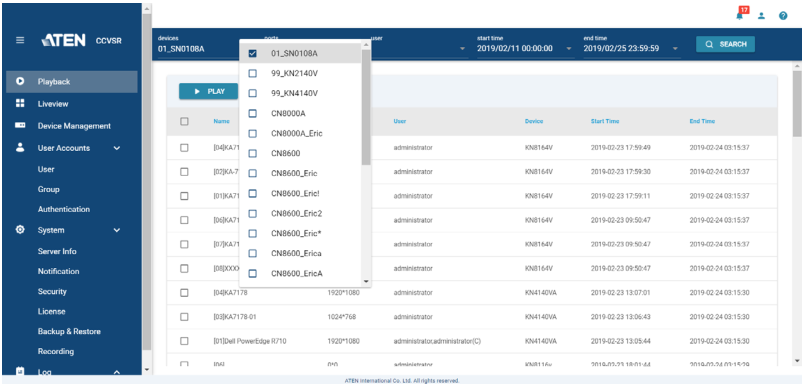


devices
ports
user
start time 2019/02/08 00:00:00
end time 2019/02/22 23:59:59

□	Name	Quality	User	Device	Start Time	End Time
□	[01]	1024*768	administrator(C)	KN8164V	2019-02-22 23:17:12	2019-02-22 23:17:25
□	[06]KA-7168	1024*768	administrator,administrator(C)	KN8164V	2019-02-22 21:28:48	2019-02-22 23:17:25
□	[01]	1024*768	administrator(C)	KN8164V	2019-02-22 23:16:56	2019-02-22 23:17:03
□	[05]KA7170	720*400	administrator(C)	KN8164V	2019-02-22 22:38:11	2019-02-22 22:38:13
□	[01]	1024*768	administrator(C)	KN8164V	2019-02-22 22:38:03	2019-02-22 22:38:05
□	[05]KA7170	720*400	administrator(C)	KN8164V	2019-02-22 22:33:04	2019-02-22 22:33:06
□	[01]	1024*768	administrator(C)	KN8164V	2019-02-22 22:32:56	2019-02-22 22:32:59
□	[05]KA7170	720*400	administrator(C)	KN8164V	2019-02-22 22:25:57	2019-02-22 22:26:00
□	[05]KA7170	720*400	administrator(C)	KN8164V	2019-02-22 22:25:46	2019-02-22 22:25:52
□	[05]KA7170	720*400	administrator(C)	KN8164V	2019-02-22 22:23:17	2019-02-22 22:23:36

The *Search* function is used to find video logs by filtering the categories *Device Name, Port Name, User, Begin Time,* or *End Time, Port Name*. The *Begin Time* and *End Time* refers to when the recording took place.

To filter the *Video List*, fill in the categories by either 1) typing to enter the information, or 2) clicking the drop-down menu and check the item(s), followed by clicking *Search*. An example of checking an item in the drop-down menu is shown:



devices 01_SN0108A
ports
user
start time 2019/02/11 00:00:00
end time 2019/02/25 23:59:59

□	Name		User	Device	Start Time	End Time
□	[04]KA71		administrator	KN8164V	2019-02-23 17:59:49	2019-02-24 03:15:37
□	[02]KA-7		administrator	KN8164V	2019-02-23 17:59:30	2019-02-24 03:15:37
□	[01]KA71		administrator	KN8164V	2019-02-23 17:59:11	2019-02-24 03:15:37
□	[06]KA71		administrator	KN8164V	2019-02-23 09:50:47	2019-02-24 03:15:37
□	[07]KA71		administrator	KN8164V	2019-02-23 09:50:47	2019-02-24 03:15:37
□	[08]XXX		administrator	KN8164V	2019-02-23 09:50:47	2019-02-24 03:15:37
□	[04]KA7178	1920*1080	administrator	KN4140VA	2019-02-23 13:07:01	2019-02-24 03:15:30
□	[03]KA7178-01	1024*768	administrator	KN4140VA	2019-02-23 13:06:43	2019-02-24 03:15:30
□	[01]Dell PowerEdge R710	1920*1080	administrator,administrator(C)	KN4140VA	2019-02-23 13:05:44	2019-02-24 03:15:30
□	[06]	0*0	administrator	KN8116v	2019-02-23 18:01:44	2019-02-24 03:15:29

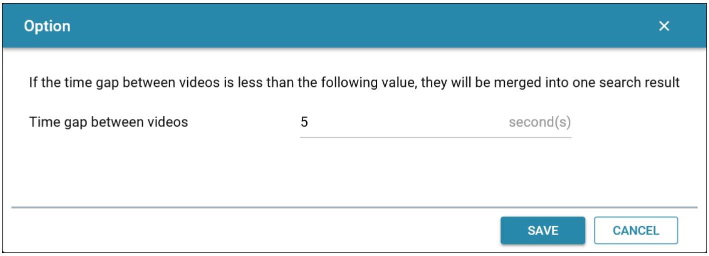
To remove the filters, uncheck the selected item and click **Search** again.

Play Video Log

To play a video log, select it from the *Video List*, then click the button *Play*. The video will open in a new window with the Video Log Viewer application. For information on the Video Log Viewer, see *VSR Viewer*, page 24.

Time Gap Option

Click *Option* for time gap setting.



If the time gap between videos is less than the following value, they will be merged into one search result

Time gap between videos: 5 second(s)

This setting helps narrow down the scope of video search results by merging video clips if the time interval between two videos is less than the configured value.

For example, if you have the following video clips, and the time interval is 2 minutes:

Video #1: 15:59:06 - 15:59:35

Video #2: 16:00:12 - 16:10:12

Video #3: 16:18:29 - 16:19:25

The search result will be:

Video #1: 15:59:06 - 16:10:12

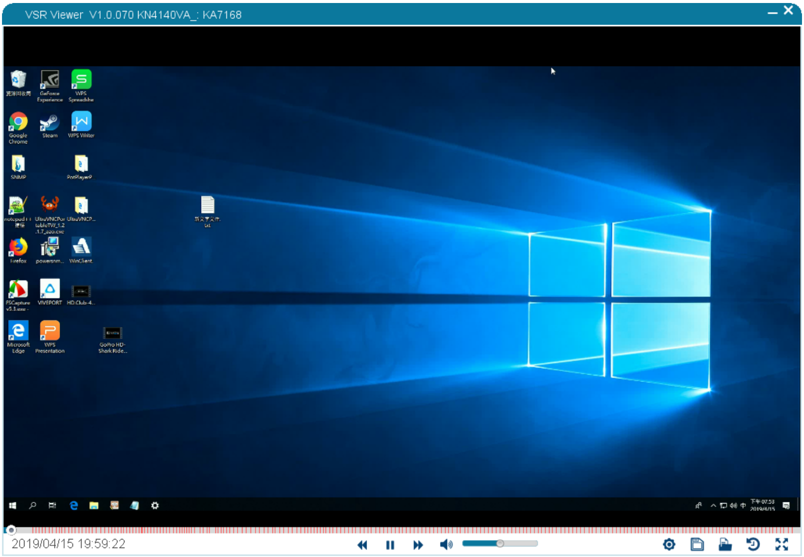
Video #2: 16:18:29 - 16:19:25

Enter a value between 0 and 3600 seconds. The default is 5 seconds.

VSR Viewer

The *VSR Viewer* is a built-in video player that pops-up when executing video log files (.vls) for playback*. The VSR Viewer is automatically used to view video logs from the Video Session Recording Software's web sessions or directly from the directory where it was saved. The VSR Viewer's playback tools are described below.

When you playback a video log, the *VSR Viewer* pops-up, and a screen similar to the one below appears:

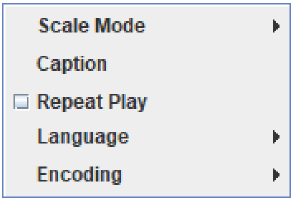


Note:
- The VSR Viewer is a Java-based application that requires JRE 8 or Zulu OpenJDK 8 FX (Windows only) to run.
- For 32-bit Java VM, the maximum viewer size support for full-screen mode is 3300*2048.
- For 64-bit Java VM, the maximum viewer size support for full-screen mode is 5130*2160.

Toolbar

The toolbar appears below the video and allows you to view information about the video and control playback features. The toolbar hides when no mouse movement is made for 3 seconds. To bring the toolbar into view simply move the mouse. The toolbar functions are described here:

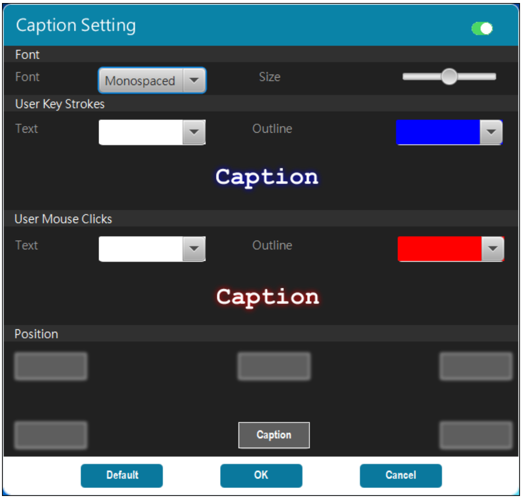
Icon	Function
▶	**Play:** The *Play* button is used to resume playback of a video log that has been paused.
❚❚	**Pause:** The *Pause* button is used to stop playback of a video log that is being played.
⏩	**Faster:** The *Faster* button is used to increase the playback speed of a video log. You can increase the speed X2, X4, or X8 of the normal playback rate.
⏪	**Slower:** The *Slower* button is used to decrease the playback speed of a video log. You can decrease the speed 1/2, 1/4, or 1/8 of the normal playback rate.
🔉 ━━━○──	**Volume:** Use the volume bar to adjust the volume. Click the speaker icon to mute/unmute the video.
━━━◉─	**Progress Bar:** The *Progress bar* shows how far along you are while viewing video logs. When viewing multiple video logs using the *Play All* feature, a solid red line on the progress bar represents the end of one video log, and the start of the next. Placing your mouse over any part of the Progress bar will produce a pop-up display of the time and date when the video log was captured, allowing you to quickly locate and go to reference points. You can click and drag the progress button forward or back to advance to any point of the video, or click anywhere on the progress bar to advance to a particular point.
⤡	**Resize Window:** Mouse over the edges of the viewer's window to see the resize mouse icon. Click and drag to resize the window. After doing so if the video doesn't fit within the resized window, you can scale the video using the *Scale Mode* feature (*see Scale Mode below).* **Note:** The entire window can be moved around the screen by holding a left click anywhere on the top window title bar.

Icon	Function
⚙	**Settings**  Scale Mode ▸ Caption ☐ Repeat Play Language ▸ Encoding ▸ **Scale Mode:** The *Scale Mode* icon allows you to change the video displays size in the Video Log Viewer's window. When you click the *Scale Mode* icon, three choices appear: ◆ *Keep Video Size:* Keeps the video display scaled at the original default size. ◆ *Keep Video Ratio*: Keeps the video display ratio scaled to fit within the resized window. ◆ *Scale Video to Window*: Scales the video display to the size of the entire window. **Caption:** Allows you to edit the captions settings. Refer to *Caption* on page 27 for more information. **Repeat Play:** Click to enable/disable playing this video log repeatedly. When the checkbox is checked, repeat play is enabled. **Language:** Allows you to select the preferred language. **Encoding:** Allows you to select the encoding method should there be any garbled content.
💾	**Save Video:** The *Save Video* icon allows you to save the current video log to a directory and encrypt it with a password. To save the video log, click **Save Video**, choose a directory, name the file, then click **Save**. After clicking *Save* the *Set Password* window will appear, enter a password for the video log file, or leave it blank for no password, then click **OK**. The video is saved as the .vls format. To open the video, please refer to *Open Video Log Files* on page 28. **Note:** Clicking *Cancel* at the *Set Password* prompt causes the save process to end and the file is not saved.
📂	**Open Video:** This icon is used to open previously saved video files. Click the icon, choose a video log file, then enter the password.
↺	**Control Panel:** When playing videos, in addition to the video image, the *Control Panel* shows the operations (mouse clicks and keystrokes), username, and IP address of the person logged into the computer, arranged in order of execution time. If multiple people are logged into the KVM port, the *Control Panel* will display the users, and who conducts each operation. Click the icon to bring up the *Control Panel* window, and use the Pin icon located at the top left corner to hold/release the open window. The *User List* displays the users logged into the KVM port at the time the video log was recorded.

Icon	Function
⛶	**Full Screen:** This icon expands the Video Log Viewer window to fit the the entire screen. To exit *Full Screen* mode, click the *Full Screen* icon again.

Caption

A settings menu will pop-up clicking this option as shown:



Caption Setting

Font

Font: Monospaced   Size

User Key Strokes

Text   Outline

Caption

User Mouse Clicks

Text   Outline

Caption

Position

Settings	Description
Caption Setting	Click the on/off switch (top-right of menu window) to turn on/off the caption function
Font	
Font	Choose the font of the caption.
Size	Drag the slider to adjust the size of the caption.
User Key Stroke	
Text	Click the drop-down menu to choose the font color for key strokes.
Outline	Click the drop-down menu to choose the color of the font outline for key strokes.
User Mouse Clicks	
Text	Click the drop-down menu to choose the font color for mouse clicks.
Outline	Click the drop-down menu to choose the color of the font outline for mouse clicks.

Settings	Description
Position	Select where you would like to have the captions positioned by clicking one of the six position boxes.
Default	Click this button to reset to the default settings.

Open Video Log Files

Follow the steps below if you wish to play video log files on a computer without CCVSR access:

1. Save the video log file.
2. Save `JavaVLS.jar` from a computer with CCVSR (usually in the `C:\VSR\VideoSessionRecorder\webroot_rls` folder).
3. Provide the video log file and `JavaVLS.jar` to the computer without CCVSR access.
4. On that computer, open `JavaVLS.jar` for the VSR Viewer.
5. Click the open video icon 📂 and select the video log file to play the video.

Import Video

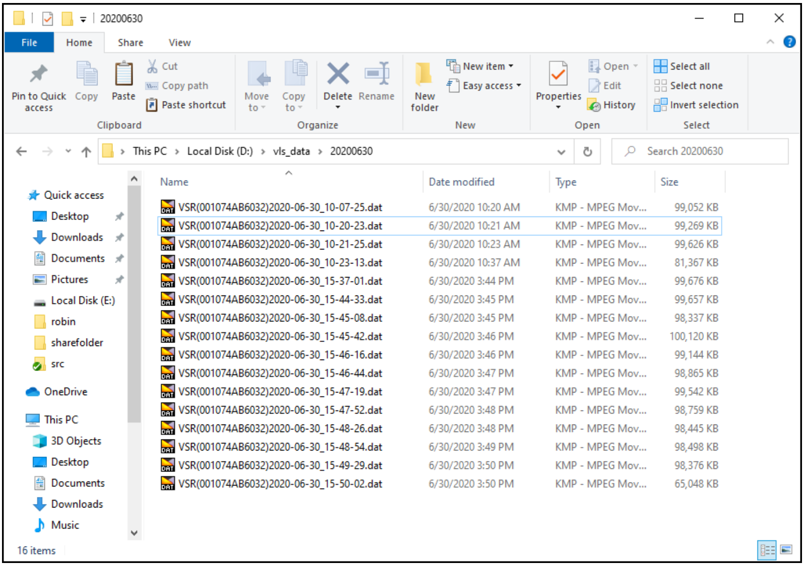
The VSR allows you to import video log files from different VSR servers. Recorded videos are typically saved in a directory named “vls_data” as *.dat files. This directory can be in a local drive or a network folder in your configurations in System > Recording (*Recording*, page 75).

A few examples are listed below:

C:\vls_data (local drive C:\)

D:\vls_data (local drive D:\)

\\10.0.8.168\sharerecording\vls_data (network folder)



Name	Date modified	Type	Size
VSR(001074AB6032)2020-06-30_10-07-25.dat	6/30/2020 10:20 AM	KMP - MPEG Mov...	99,052 KB
VSR(001074AB6032)2020-06-30_10-20-23.dat	6/30/2020 10:21 AM	KMP - MPEG Mov...	99,269 KB
VSR(001074AB6032)2020-06-30_10-21-25.dat	6/30/2020 10:23 AM	KMP - MPEG Mov...	99,626 KB
VSR(001074AB6032)2020-06-30_10-23-13.dat	6/30/2020 10:37 AM	KMP - MPEG Mov...	81,367 KB
VSR(001074AB6032)2020-06-30_15-37-01.dat	6/30/2020 3:44 PM	KMP - MPEG Mov...	99,676 KB
VSR(001074AB6032)2020-06-30_15-44-33.dat	6/30/2020 3:45 PM	KMP - MPEG Mov...	99,657 KB
VSR(001074AB6032)2020-06-30_15-45-08.dat	6/30/2020 3:45 PM	KMP - MPEG Mov...	98,337 KB
VSR(001074AB6032)2020-06-30_15-45-42.dat	6/30/2020 3:46 PM	KMP - MPEG Mov...	100,120 KB
VSR(001074AB6032)2020-06-30_15-46-16.dat	6/30/2020 3:46 PM	KMP - MPEG Mov...	99,144 KB
VSR(001074AB6032)2020-06-30_15-46-44.dat	6/30/2020 3:47 PM	KMP - MPEG Mov...	98,865 KB
VSR(001074AB6032)2020-06-30_15-47-19.dat	6/30/2020 3:47 PM	KMP - MPEG Mov...	99,542 KB
VSR(001074AB6032)2020-06-30_15-47-52.dat	6/30/2020 3:48 PM	KMP - MPEG Mov...	98,759 KB
VSR(001074AB6032)2020-06-30_15-48-26.dat	6/30/2020 3:48 PM	KMP - MPEG Mov...	98,445 KB
VSR(001074AB6032)2020-06-30_15-48-54.dat	6/30/2020 3:49 PM	KMP - MPEG Mov...	98,498 KB
VSR(001074AB6032)2020-06-30_15-49-29.dat	6/30/2020 3:50 PM	KMP - MPEG Mov...	98,376 KB
VSR(001074AB6032)2020-06-30_15-50-02.dat	6/30/2020 3:50 PM	KMP - MPEG Mov...	65,048 KB

To import saved files from any computer running as a VSR server, open a command prompt by clicking the Start Menu – Run, type *CMD* and click **OK**.

Use the following command line formula to import the video log files (.dat):

vsrImport <Destination DB file> <Source Path for VSR Data file> 0 <Destination path>

Examples:

Windows:

```
C:\VSR\VideoSessionRecorder>vsrImport VSR80.db d:\vls_data 0 c:\
```

Linux:

```
sudo /usr/local/bin/ccvsr/vsrImport /usr/local/bin/ccvsr/VSR.db /home/user1/vls_data 0 /var
```

After importing the files, the video logs will appear in the **Search Results** window on the *Playback* tab.

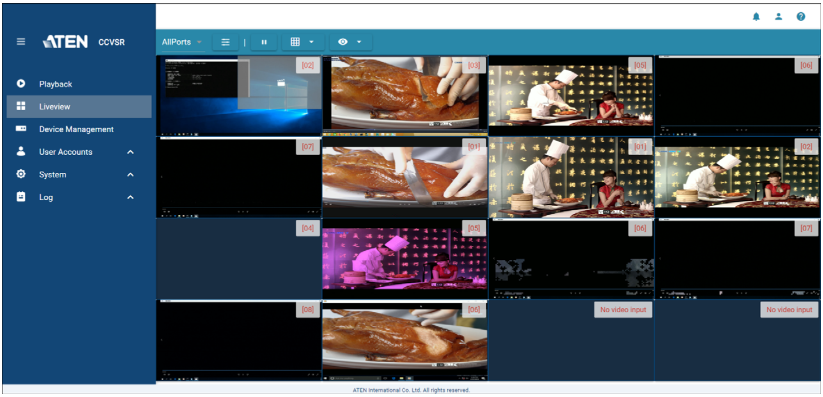
Chapter 5
Liveview

Overview

The *Liveview* page allows the user to have a centralized liveview of a specific group of ports or select a particular port for liveview display.

Centralized Liveview

Clicking the *Liveview* brings you to the page shown below:



The page provides a centralized liveview of the available ports.

If you have setup a favorite, you may choose to only display the ports within the favorite. You may also choose to only display *Recording Only* ports. Refer to the sections below for more details.

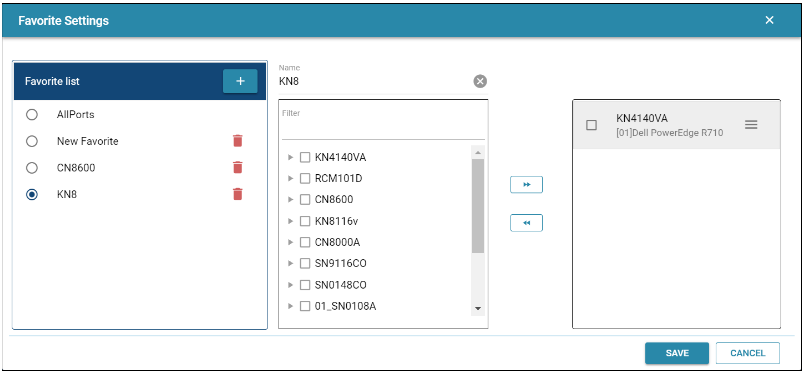
Display List

Clicking the display list drop-down menu will show the available lists. Initially, *AllPorts* is the only available option as all the ports will be shown in the centralized liveview.

If you have created favorite(s), the name of the favorite will also be shown in the drop-down menu.

Favorite Setting

Clicking the ≡ icon will bring you to *Favorite Settings*:



○ AllPorts
○ New Favorite
○ CN8600
● KN8

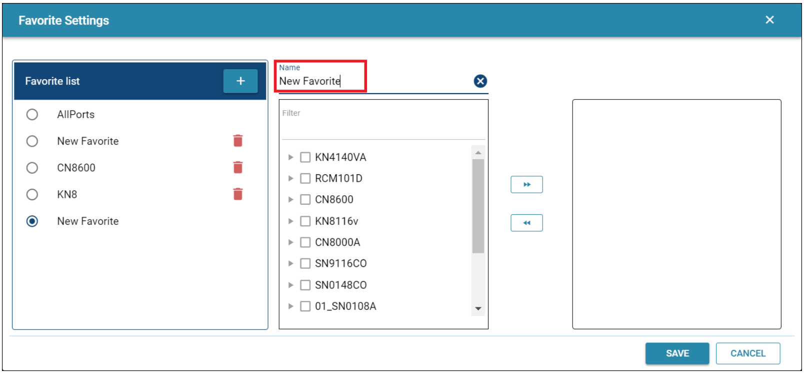
Name: KN8

□ KN4140VA
□ RCM101D
□ CN8600
□ KN8116v
□ CN8000A
□ SN9116CO
□ SN0148CO
□ 01_SN0108A

□ KN4140VA [01]Dell PowerEdge R710

Create Favorite

1. To create a favorite, click the + icon.
2. The system will ask you to change the name of the favorite:



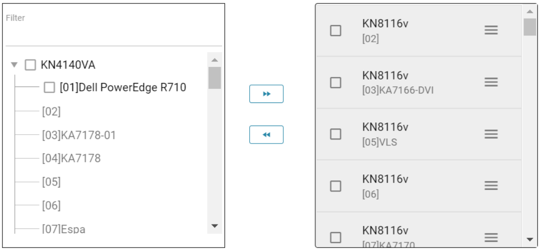
○ AllPorts
○ New Favorite
○ CN8600
○ KN8
● New Favorite

Name: New Favorite

□ KN4140VA
□ RCM101D
□ CN8600
□ KN8116v
□ CN8000A
□ SN9116CO
□ SN0148CO
□ 01_SN0108A

3. In the left panel, check the device checkbox that you wish to add to the favorite and click the ▸▸ button. The device will be shifted to the right panel.

   Click ▸ for a device’s ports if you wish to select the ports individually.



To remove a device or a port from the list, check the checkbox in the right panel and click the ◂◂ button.

You may use the filter to refine your search.

On the right panel, you may also click and drag the devices/ports to rearrange the order of the added devices/ports.

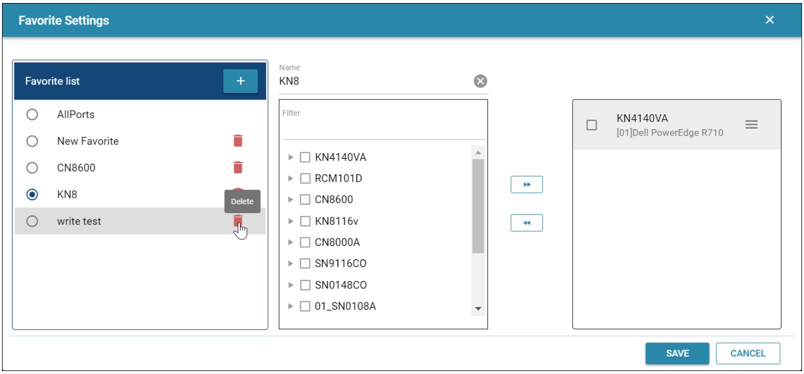
4. When completed, click the *Save* button. Click the *Cancel* button to cancel the modification. The added favorite will be displayed in the *Favorite List* panel.

Modify Favorite

To modify the favorite, click the name of the favorite and modify as described in *Create Favorite* above.

Delete Favorite

To delete a favorite, click the 🗑 icon and click the *Save* button:



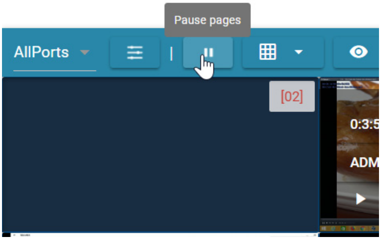
Name: KN8

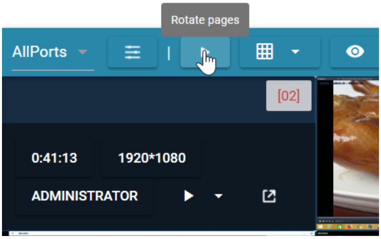
After setting up your favorite, clicking the display list drop-down menu will show the favorites in the list.

Select a favorite to only view ports in the favorite on the centralized view.

Rotate / Pause Pages

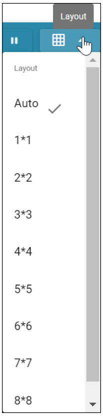
If the source ports exceed the number of display for a layout, CCVSR will automatically rotate through the displayed ports page by page. Click the ▶ or ⏸ icons to respectively begin or pause the rotation.





Layout

You can change the layout of the centralized view by clicking the layout button ⊞ ▾ and select a desired layout choice.

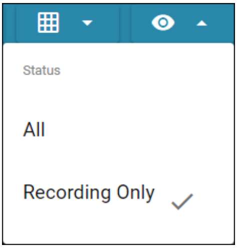


By default, Auto is selected. A range of options can be selected as shown in the diagram above.

Status

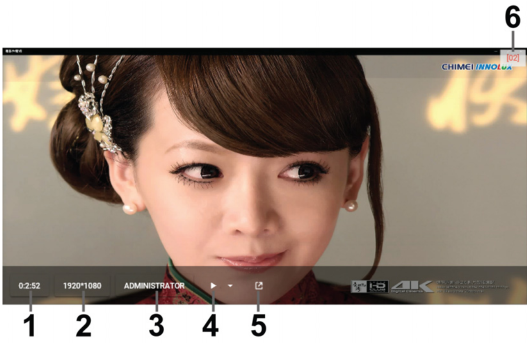
The status button is another filter that allows you to select whether to view all the ports or only the ports that are recording on the centralized view.

Click 👁 ▾ for a drop-down menu and select between *All* or *Recording Only*:



Port Info / Playback / Liveview Function

Port information, playback and liveview function will appear when moving your mouse cursor over a port on the centralized view.



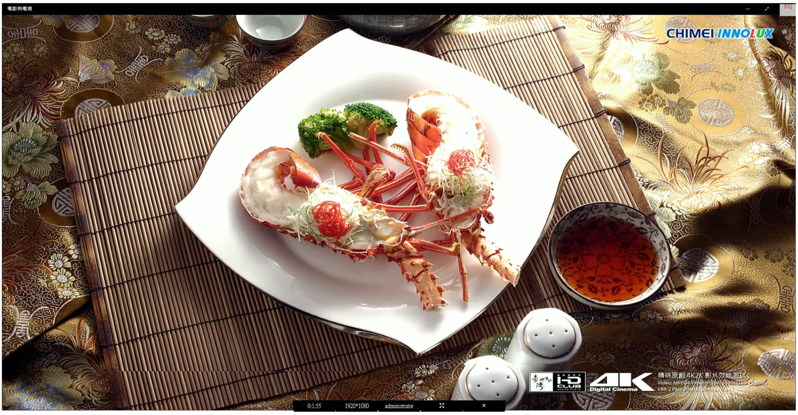
The labeled components are explained in the table below:

No.	Item	Description
1	Recorded time	This displays how long the port has been recorded for.
2	Resolution	This displays the resolution of the liveview.
3	Logged in Username	This displays the username of the user accessing the port. “Local console” is displayed when local console is accessed.

No.	Item	Description
4	Playback from	Click this for a drop-down menu. The option allows you to choose when you wish to play the video log from.
5	Open in new window	Click this if you wish to view this port in a new window. Refer to *Single Port Mode* on page 36.
6	Port No.	This displays the port number of the liveview.

Single Port Mode

Click the *Open in new window* icon to enter Single Port Mode.



The window also displays the *Recorded Time*, *Resolution*, *Logged in Username*.

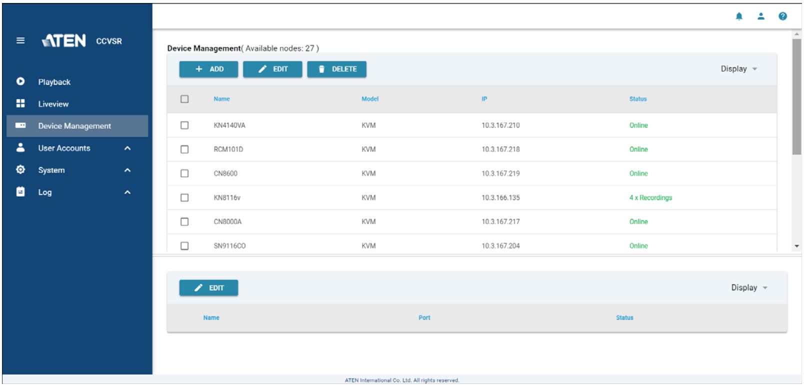
Click ⛶ for full-screen mode. Press Esc to quit full-screen mode.

Click ☒ to exit *Single Port Mode*.

Chapter 6
Device Management

Overview

The purpose of the *Device Management* page is to add KVM devices and configure ports through which the Video Session Recording Software can record video logs. The Device Management page opens the main page showing a list of KVM devices that have been added:



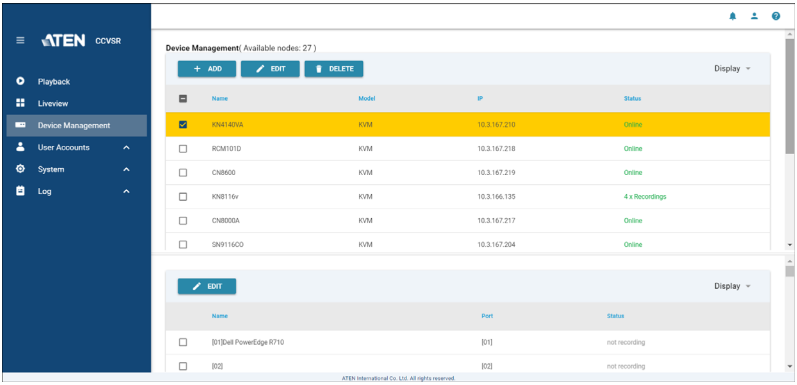
Device Management(Available nodes: 27)

	Name	Model	IP	Status
□	KN4140VA	KVM	10.3.167.210	Online
□	RCM101D	KVM	10.3.167.218	Online
□	CN8600	KVM	10.3.167.219	Online
□	KN8116v	KVM	10.3.166.135	4 x Recordings
□	CN8000A	KVM	10.3.167.217	Online
□	SN9116CO	KVM	10.3.167.204	Online

Name	Port	Status

Port List

A port list is available on the lower half of the *Device Management* page. Checking a KVM device will display all the device’s ports in the port list as shown:



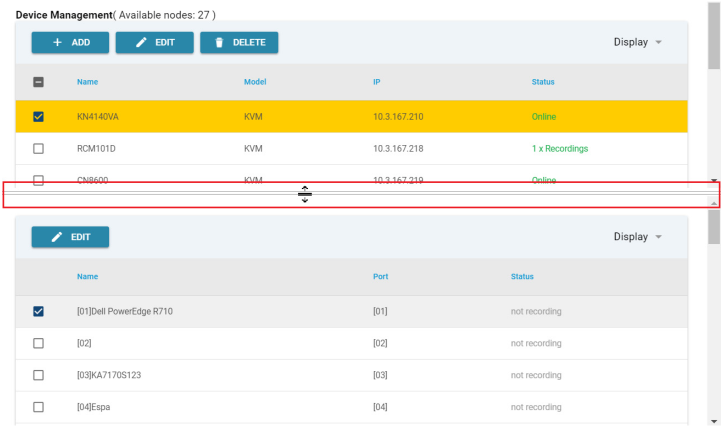
Device Management(Available nodes: 27)

	Name	Model	IP	Status
☑	KN4140VA	KVM	10.3.167.210	Online
□	RCM101D	KVM	10.3.167.218	Online
□	CN8600	KVM	10.3.167.219	Online
□	KN8116v	KVM	10.3.166.135	4 x Recordings
□	CN8000A	KVM	10.3.167.217	Online
□	SN9116CO	KVM	10.3.167.204	Online

	Name	Port	Status
□	[01]Dell PowerEdge R710	[01]	not recording
□	[02]	[02]	not recording

Note: The port list will only display the ports of the highlighted checked device. From the example above, the port list will only display the ports of KN4140VA.

You can drag the window splitter up or down to show more ports in the list or you can use the scroll bar on the right.



	Name	Model	IP	Status
☑	KN4140VA	KVM	10.3.167.210	Online
□	RCM101D	KVM	10.3.167.218	1 x Recordings
□	CN8600	KVM	10.3.167.219	Online

	Name	Port	Status
☑	[01]Dell PowerEdge R710	[01]	not recording
□	[02]	[02]	not recording
□	[03]KA7170S123	[03]	not recording
□	[04]Espa	[04]	not recording

Recording KVM Ports

To record video logs you must add a KVM switch and configure its recording settings (in the *Recording* tab). Enabled ports are recorded by the Video Session Recording Software every time they are accessed through the KVM switch, and are saved as a video log file. Logs can be viewed from the *Playback* tab. As long as you are licensed (see *Licenses* on page 8) to do so, there is no limit to the number of KVM devices that you can add or ports you can enable. The Video Session Recording Software can simultaneously record a maximum of 20 ports at one time, across multiple KVM devices.

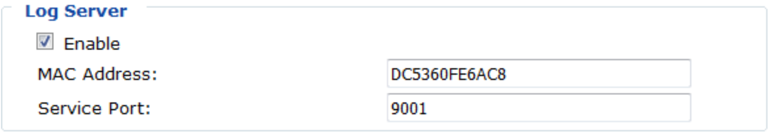
Display

Click *Display* (top right-hand corner) to select what information is shown in the list.

Adding KVM Devices

To add a KVM device to the *KVM Device* list, do the following:

1. On the KVM device, go to *Device Management* to enable **Log Server** and enter the **MAC Address** and **Service Port** of the computer running the Video Session Recording Software, as shown below:



Log Server

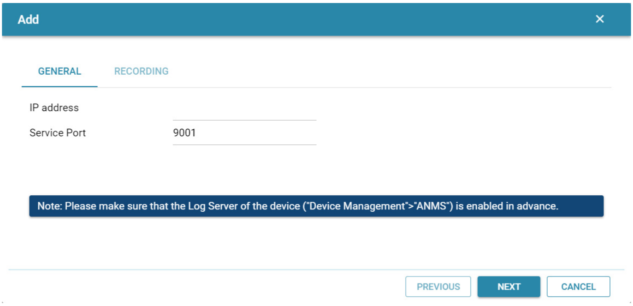
☑ Enable

MAC Address: DC5360FE6AC8

Service Port: 9001

2. On the *Device Management* page, click the + ADD button.

   A pop-up window appears:



IP address

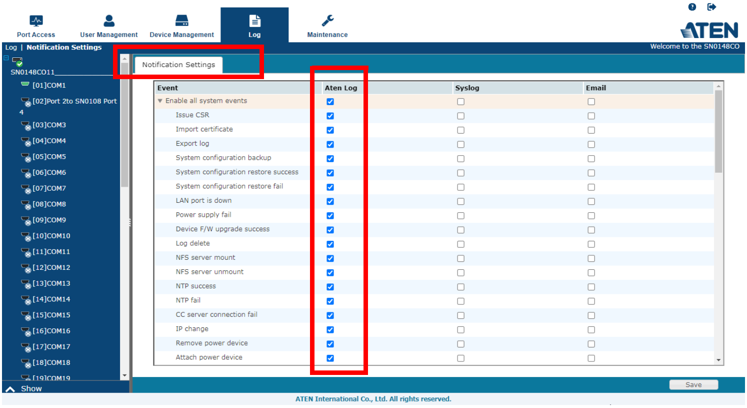
Service Port 9001

Note: Please make sure that the Log Server of the device ("Device Management">"ANMS") is enabled in advance.

3. Fill in the IP address and Service Port number of the KVM device you are adding, and click **Next**. The system will bring you to the *Recording* tab.
4. If you wish to enable recording of a port on the KVM device, click the drop-down menu and select "Enable (Video + Audio)" or "Enable (Video)". For more information, please refer to *Enabling Video/Audio Recording* on page 41.
5. If you wish to enable recording on local console, check the checkbox and enter a time delay value in seconds (0-999) in the entry field.
6. Click *Add* to add the KVM device.
7. The KVM device will appear in the device list, and on the *Device Management* main page.

Note:

1. After adding a KVM device, check the *Status* column. If *Online* is shown, you have successfully added the device.
2. An *Offline* status indicates the KVM device can't be reached over the network. Check that the KVM device's IP address and Service Port numbers are correct, the KVM device is online and its Log Server has been enabled and configured with the correct MAC Address.
3. If you wish to receive logs of an added serial console server, make sure you have enabled notification settings on the serial console server's own notification page. An example (SN0148CO device interface) is shown below:

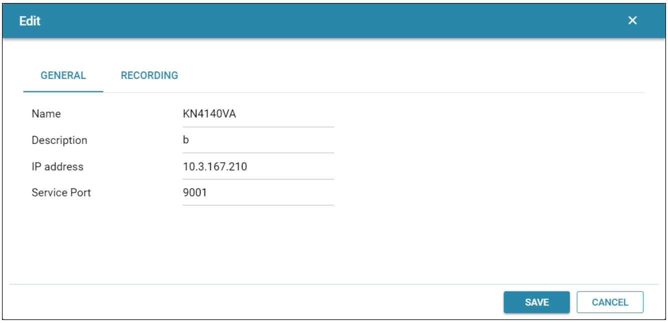


Event	Aten Log	Syslog	Email
▼ Enable all system events	☑	□	□
Issue CSR	☑	□	□
Import certificate	☑	□	□
Export log	☑	□	□
System configuration backup	☑	□	□
System configuration restore success	☑	□	□
System configuration restore fail	☑	□	□
LAN port is down	☑	□	□
Power supply fail	☑	□	□
Device F/W upgrade success	☑	□	□
Log delete	☑	□	□
NFS server mount	☑	□	□
NFS server unmount	☑	□	□
NTP success	☑	□	□
NTP fail	☑	□	□
CC server connection fail	☑	□	□
IP change	☑	□	□
Remove power device	☑	□	□
Attach power device	☑	□	□

4. For sessions recorded via the ports of KE6900AiT, KE6940AiT, please note the following:
   1. Audio is not supported.
   2. Users must *Enable recording on local console port* to record sessions that are accessed by their local console ports or KE Receivers, see page 41 for details.
   3. Keystroke & mouse click recording is only supported for remote sessions captured from the ports of KE6900AiT, KE6940AiT.

Edit KVM Devices

To edit the name, description, IP address, service port and recording options, check the checkbox of the KVM device and click the EDIT button:

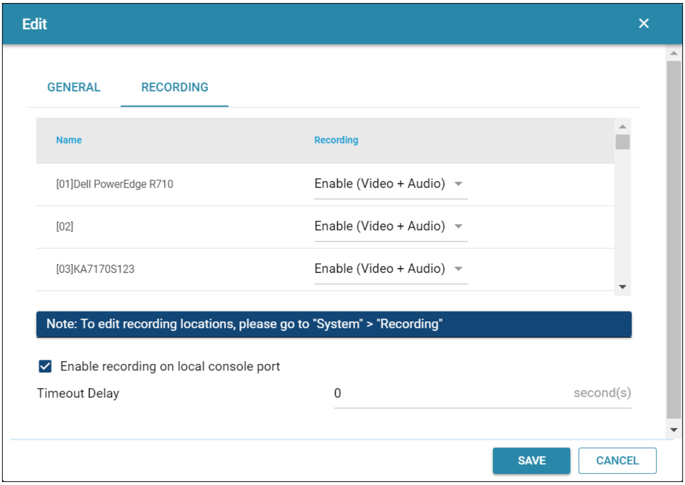


Name	KN4140VA
Description	b
IP address	10.3.167.210
Service Port	9001

Edit the options and click *Save* to save.

Recording

Click the *Recording* tab to edit recording options:



Name	Recording
[01]Dell PowerEdge R710	Enable (Video + Audio)
[02]	Enable (Video + Audio)
[03]KA7170S123	Enable (Video + Audio)

Note: To edit recording locations, please go to "System" > "Recording"

☑ Enable recording on local console port

Timeout Delay 0 second(s)

Enabling Video/Audio Recording

To enable the ports of a KVM device to record video + audio or video only sessions, do the following:

1. Check the KVM device’s checkbox.

2. Click the button for the edit pop-up menu.
3. Click the *Recording* tab.
4. Click the drop-down menu under the *Recording* column.
5. Select “Enable (Video + Audio)”, “Enable (Video)” or “Disable”.
6. Click *Save* to save.
7. The enabled ports will now record anytime they are accessed.

Enable Recording on Local Console Port

Devices added to the CCVSR may be access via local console ports. Check the checkbox to enable recording on the local console whenever they are accessed.

For CN8000A, CN8600, CN9000, CN9600, CN9950, RCM101A, RCM101D, RCMVGA101, RCMDVI101, and RCMDP101U, enter a Timeout Delay value in seconds (0 - 180) in the entry field. CCVSR will stop recording if there are no key stroke or mouse movement after the set time. If **‘0’** is entered, CCVSR will record indefinitely.

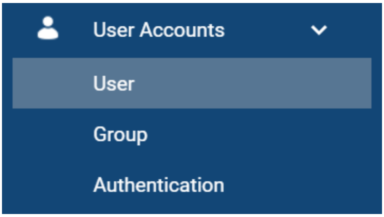
Delete KVM Devices

To delete a KVM device, check the checkbox of the KVM device and click the DELETE button.

Chapter 7
User Accounts

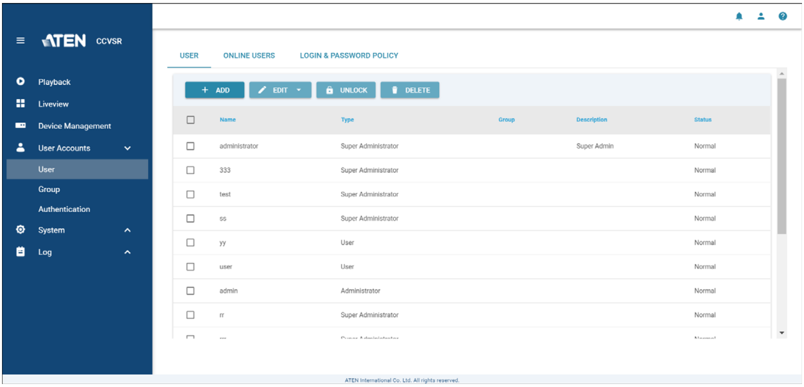
Overview

The User Account in the main menu expands into 3 sub-menus.



User

Below is the User sub-menu:



□	Name	Type	Group	Description	Status
□	administrator	Super Administrator		Super Admin	Normal
□	333	Super Administrator			Normal
□	test	Super Administrator			Normal
□	ss	Super Administrator			Normal
□	yy	User			Normal
□	user	User			Normal
□	admin	Administrator			Normal
□	rr	Super Administrator			Normal
□	[illegible]	Super Administrator			Normal

The main panel provides a more detailed user information at-a-glance.

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

The buttons on top of the main panel are used to manage users.

User Type

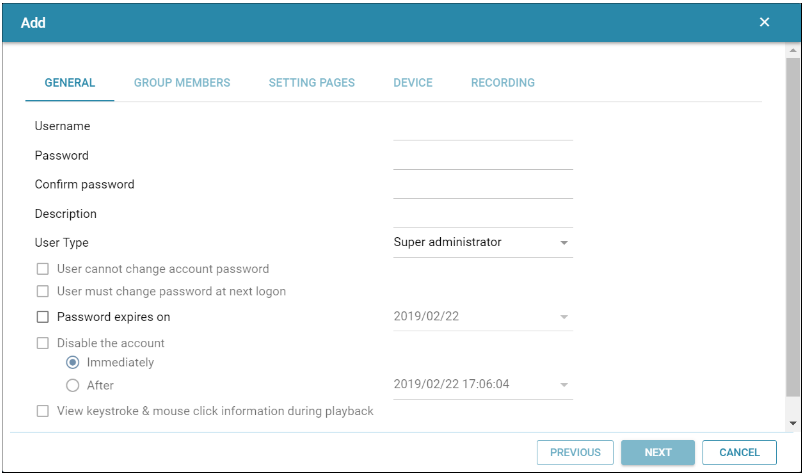
The Video Session Recording Software supports three types of users, as shown in the table, below:

User Type	Role
Super Administrator	Access and manage ports and devices. Manage Users, and Groups. Configure the overall installation. Configure personal working environment.
Administrator	Access and manage authorized ports and devices. Manage Users and Groups. Configure personal working environment.
User	Access authorized ports and devices. Manage authorized ports and devices; configure personal working environment. **Note:** Users who have been given permission to do so, may also manage other users.

Adding Users

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

1. Click the + ADD button for the pop-up window below:



Username

Password

Confirm password

Description

User Type: Super administrator

□ User cannot change account password

□ User must change password at next logon

□ Password expires on 2019/02/22

□ Disable the account

● Immediately

○ After 2019/02/22 17:06:04

□ View keystroke & mouse click information during playback

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

Field	Description
Username	1 to16 characters are allowed depending on the Account Policy settings. see *For security purposes, we recommend that you change this string occasionally.*, page 67.
Password	0 to 16 characters are allowed depending on the Account Policy settings (see *Login & Password Policy* on page 49).
Confirm Password	To make sure there is no mistake in the password. The two entries must match.
Description	Additional information about the user that you may wish to include.
User Type	There are three categories: Super Administrator, Administrator and User. There is no limitation on the number of accounts that can be created in each category. ◆ The Super Administrator are granted the highest permissions, where you can view/configure Liveview, Playback, Device Management, User Accounts, System and Log. The Super Administrator's permissions (see page 46) are automatically assigned by the system and cannot be altered. ◆ The default permissions for Administrators include everything except User Accounts, but the permissions can be altered for each Administrator by checking or unchecking any of the permissions checkboxes. ◆ The default permissions for Users include Playback, but the permissions can be altered for each User by checking or unchecking any of the permissions checkboxes. **Note:** Users who have been given User Account privileges cannot access or configure Groups.

Field	Description
Account Condition	Condition allows you to control the user's account and access to the system. Check the checkbox to add the conditions described below: ◆ **User cannot change account password:** To make a password permanent, so that the user cannot change it to something else. Checking this will disable the next two conditions. ◆ **User must change password at next logon:** Checking this will disable the above condition. When this user changes the password, this option will be unchecked. ◆ **Password expires on:** Select a date for the condition. ◆ **Disable the Account:** lets you suspend a user's account without actually deleting it, so that it can be easily reinstated in the future. ◆ Immediately ◆ After: Select a date and time to disable the account. ◆ **View Keystroke & mouse click information during playback**.

3. If you selected the user to be a Super administrator, click add to add the user.

   If you selected the user to be an Administrator or a User, the tabs *Group Member*, *Setting Pages*, *Device* and *Recording* may light up for you to configure. Continue configuring the user by clicking the lit tabs or *Next*.

4. **Group Members:** You can assign the new user to a group by selecting the *Group Members* tab, check the group you wish the user to be in and click *Next*.

   Note: If the group you wish to assign to has not been created, refer to *Creating Groups* on page 50 to create a new group.

5. **Setting Pages:** You can assign permissions in this tab by checking the options and click *Next*.

   Note: For ordinary users, in addition to enabling Device Management, the user must also be given those rights for each device that he will be allowed to manage.

   - Enabling *Liveview* allows a user to use the liveview function (see *Liveview*, page 31).

- Enabling *Playback* allows a user to use the playback function (see *Playback*, page 21).
- Enabling *Device Management* allows a user to view the settings and devices on the Device Management tab (see *Device Management*, page 37).
- Enabling *User Accounts* allows a user to create, modify, and delete user and group accounts.
- Enabling *Log* allows a user to access the system log (see *Logs*, page 81 for details)
- Enabling *System* allows a user to access and configure settings in the System tab.

6. **Device:** You can assign the user's device access rights by selecting the *Device* tab, check the devices you wish to have access rights to and click *Next*.
7. **Recording:** You can assign CCVSR configuration rights by selecting the *Recording* tab, check the CCVSR you wish the user to be able to configure and click Next.
8. When your selections have been made click **Add**.

Modifying User

To modify a user account, do the following:

1. Check the checkbox of the user.
2. Click the ✎ EDIT ▾ button and choose *Properties* or *Access right*.
3. **Properties:** Choosing Properties allows you to configure the general tab and group members tab.

   Access right: Choosing Access right allows you to configure the setting pages tab, device tab and recording tab.

   Refer to *Adding Users* on page 44 for more information.
4. Click *Save* when the modification is complete.

Deleting User

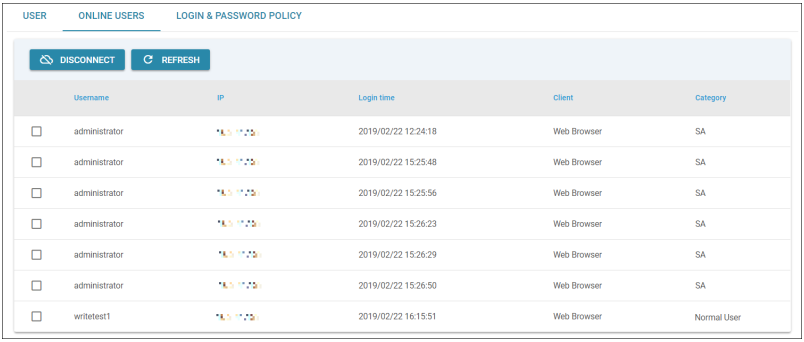
To delete a user account, do the following:

1. Check the checkbox of the user.
2. Click DELETE.

Note: If all users are deleted, the system will automatically generate the original administrator account and password (name: administrator, password: password).

Online Users

The *Online Users* tab lets super administrators see at a glance which super users are currently logged into the Video Session Recording Software, and provides information about each of their sessions.



	Username	IP	Login time	Client	Category
□	administrator	[redacted]	2019/02/22 12:24:18	Web Browser	SA
□	administrator	[redacted]	2019/02/22 15:25:48	Web Browser	SA
□	administrator	[redacted]	2019/02/22 15:25:56	Web Browser	SA
□	administrator	[redacted]	2019/02/22 15:26:23	Web Browser	SA
□	administrator	[redacted]	2019/02/22 15:26:29	Web Browser	SA
□	administrator	[redacted]	2019/02/22 15:26:50	Web Browser	SA
□	writetest1	[redacted]	2019/02/22 16:15:51	Web Browser	Normal User

Note:
1. The Online User page is not available for Administrator or User user types.
2. The *Category* heading lists the type of user who has logged in: SA (Super Administrator); Admin (Administrator); Normal user (User).

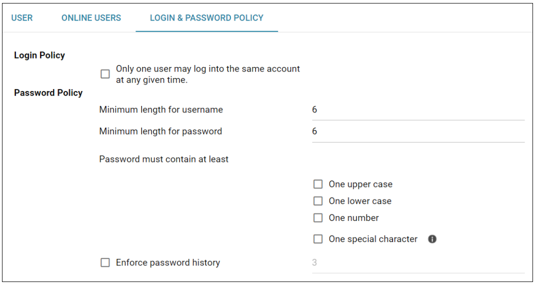
The meanings of the headings at the top of the page are fairly straightforward. The *IP* heading refers to the IP address that the user has logged in from; the *Login Time* refers to the time the user logged into the Video Session Recording Software, and the *Client* heading refers to the client the user used to access the system.

- This page also gives the super administrator the option to disconnect a user from the system by selecting the user and clicking *DISCONNECT*.
- Click *Refresh* to refresh the list.

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

Login & Password Policy

In the Login & Password Policy tab, system administrators can set policies governing login, usernames and passwords.



Login Policy

□ Only one user may log into the same account at any given time.

Password Policy

Minimum length for username 6

Minimum length for password 6

Password must contain at least

□ One upper case
□ One lower case
□ One number
□ One special character

□ Enforce password history 3

Login Policy

Entry	Explanation
Only one user may log into the same account at any given time	Check this to prevent users from logging in with the same account at the same time.

Password Policy

Entry	Explanation
Minimum Username Length	Sets the minimum number of characters required for a username. Acceptable values are from 1–16. The default is 6.
Minimum Password Length	Sets the minimum number of characters required for a password. Acceptable values are from 0–16. A setting of 0 means that no password is required. The default is 6.
Password Must Contain At Least	Checking any of these items requires users to include at least one uppercase letter, one lowercase letter, one number in their password, or one special character. **Note:** This policy only affects user accounts created after this policy has been enabled, and password changes to existing user accounts. Users accounts created before this policy was enabled, with no change to the existing password, are not affected.
Enforce password history	When checked, you cannot use the same password when attempting to change the password. The number entered here is how many password changes the system will remember. The system will not let you change to the passwords it remembers.

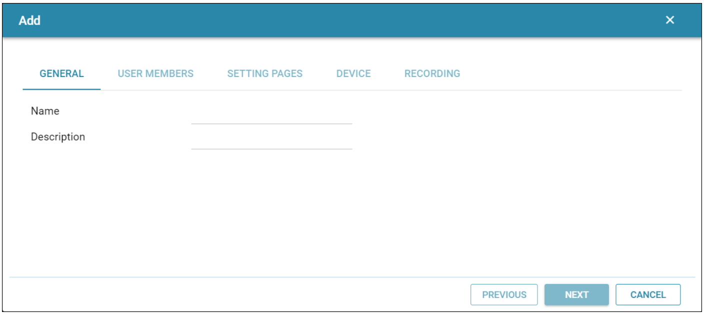
Group

Groups allow administrators to easily and efficiently manage users and devices. Since device access rights apply to anyone who is a member of the group, administrators need only set them once for the group, instead of having to set them for each user individually. Multiple groups can be defined to allow some users access to specific devices, while restricting other users from accessing them.

Creating Groups

To create a group, do the following:

1. Click the + ADD button for the pop-up window below:



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

Field	Description
Name	A maximum of 16 characters is allowed.
Description	Additional information about the user that you may wish to include. A maximum of 63 characters is allowed.

   Click *Next* for the *User Members* tab.

3. **User Members:** You can assign users to the group by checking the members, check the members you wish the group to include and click *Next*.

4. **Setting Pages:** You can assign permissions in this tab by checking the options and click *Next*.

   - Enabling *Liveview* allows a user to use the liveview function (see *Liveview*, page 31).

- Enabling *Playback* allows users in the group to use the playback function (see *Playback*, page 21).
- Enabling *Device Management* allows users in the group to view the settings and devices on the Device Management tab (see *Device Management*, page 37).
- Enabling *User Accounts* allows users in the group to create, modify, and delete user and group accounts.
- Enabling *Log* allows users in the group to access the system log (see *Logs*, page 81 for details).
- Enabling *System* allows users in the group to access and configure settings in the System tab.

5. **Device:** You can assign the group's device access rights by selecting the *Device* tab, check the devices you wish to have access rights to and click *Next*.

6. **Recording:** You can assign CCVSR configuration rights by selecting the *Recording* tab, check the CCVSR you wish the group to be able to configure and click Next.

7. When your selections have been made click **Add**.

Modifying Groups

To modify a group, do the following:

1. Check the checkbox of the group.

2. Click the ✎ EDIT ▾ button and choose *Properties* or *Access right*.

3. **Properties:** Choosing Properties allows you to configure the general tab and group members tab.

   Access right: Choosing Access right allows you to configure the setting pages tab, device tab and recording tab.

   Refer to *Creating Groups* on page 50 for more information.

4. Click *Save* when the modification is complete.

Deleting Groups

To delete a group, do the following:

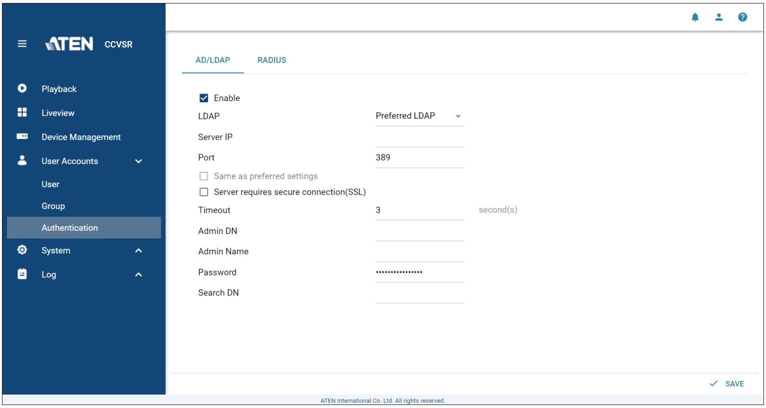
1. Check the checkbox of the group.

2. Click 🗑 DELETE.

Authentication

The Authentication sub-menu includes settings of AD/LDAP and RADIUS.

AD / LDAP Settings



☑ Enable

LDAP: Preferred LDAP

Server IP:

Port: 389

□ Same as preferred settings

□ Server requires secure connection(SSL)

Timeout: 3 second(s)

Admin DN:

Admin Name:

Password: ••••••••••••••••

Search DN:

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

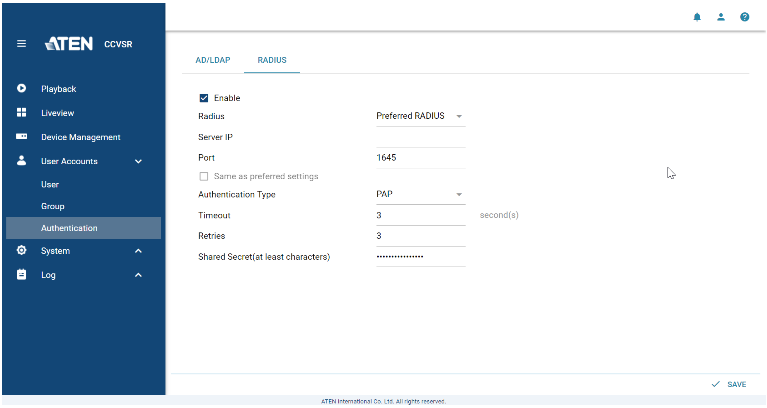
Item	Action
Enable	Check the Enable checkbox to allow AD / LDAP authentication and authorization.
LDAP Type	Click the drop-down menu to select Preferred or Alternate LDAP.
Server IP	Fill in the IP address, you can use the IPv4 address, the IPv6 address or the domain name in the LDAP Server field.
Port	Fill in the port number. Checking *Server requires secure connection (SSL)*, the default port number is 636. Otherwise, the default port number is 389.
Timeout	Set the time in seconds that the Video Log Server waits for a reply before it times out.
Admin DN	Consult the AD / LDAP administrator to ascertain the appropriate entry for this field. For example, the entry might look like this: ou=kn4132,dc=aten,dc=com
Admin Name	Key in the LDAP administrator’s username.
Password	Key in the LDAP administrator’s password.
Search DN	Set the distinguished name of the search base. This is the domain name where the search starts for user names.

Click *Save* on the bottom right-hand corner of the window to save the configuration.

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

- With MS Active Directory Schema.
  - To allow authentication via LDAP, the AD LDAP Schema must be extended with an attribute name for the CCVSR — *iVlog-userProfile* — as an optional attribute to the person class.
- Without Schema – Only the Usernames used on the Video Log Server are matched to the names on the LDAP / LDAPS server. User privileges are the same as the ones configured on the switch.
- Without Schema – Only Groups in AD are matched. User privileges are the ones configured for the groups he belongs to on the switch.
- Without Schema – Usernames and Groups in AD are matched. User privileges are the ones configured for the User and the Groups he belongs to on the switch.

RADIUS Settings



☑ Enable

Radius	Preferred RADIUS
Server IP	
Port	1645
□ Same as preferred settings	
Authentication Type	PAP
Timeout	3 second(s)
Retries	3
Shared Secret(at least characters)	••••••••••••••••

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

1. Check **Enable**.
2. Select *Preferred RADIUS* or *Alternate RADIUS* from the drop-down menu.

3. Fill in the IP addresses and service port numbers. You can use the IPv4 address, the IPv6 address or the domain name in the IP fields.
4. Select *PAP* or *CHAP* from the drop-down menu for Authentication Type.
5. In the *Timeout* field, set the time in seconds that the Video Log Server waits for a RADIUS server reply before it times out.
6. In the *Retries* field, set the number of allowed RADIUS retries.
7. In the *Shared Secret* field, key in the character string that you want to use for authentication between the Video Log Server and the RADIUS Server. A minimum of 6 characters is required.
8. Click *Save* on the bottom right-hand corner of the window to save the configuration.

On the RADIUS server, Users can be authenticated with any of the following methods:

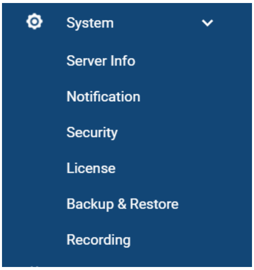
- Set the entry for the user as **su/xxxx**
- Where *xxxx* represents the Username given to the user when the account was created on the Video Log Server.
- Use the same Username on both the RADIUS server and the Video Log Server.
- Use the same Group name on both the RADIUS server and the Video Log Server.
- Use the same Username/Group name on both the RADIUS server and the Video Log Server.

In each case, the user’s access rights are the ones assigned that were assigned when the User of Group was created on the Video Log Server. (See *Adding Users*, page 44.)

Chapter 8
System

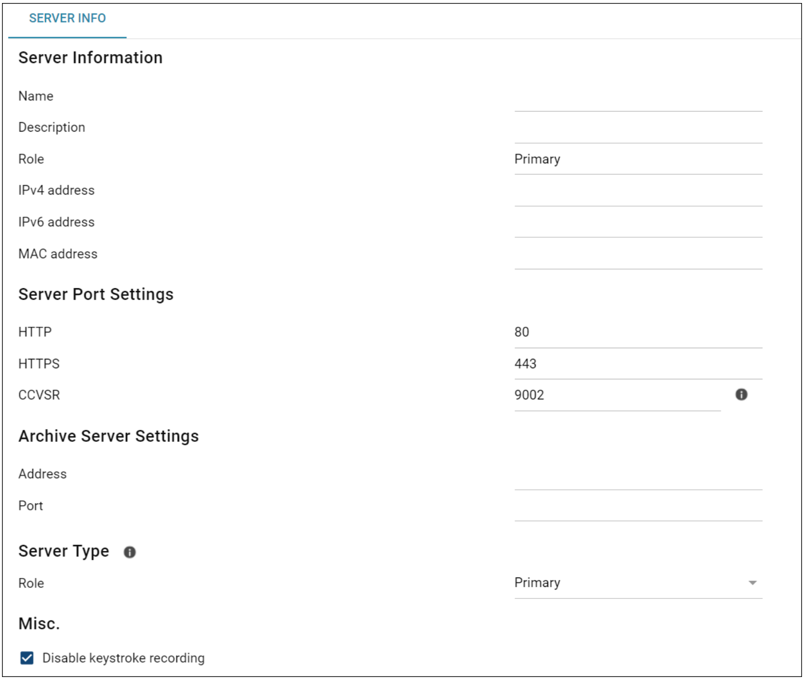
Overview

The System page is used to view and manage the CCVSR’s system settings. Clicking *System* will expand/collapse its sub-menu:



Server Info

Clicking *Server Info* sub-menu will bring you to the page below:



SERVER INFO

Server Information

Name

Description

Role: Primary

IPv4 address

IPv6 address

MAC address

Server Port Settings

HTTP: 80

HTTPS: 443

CCVSR: 9002

Archive Server Settings

Address

Port

Server Type

Role: Primary

Misc.

☑ Disable keystroke recording

Server Information

Item	Meaning
Name	Displays the computer name of the server hosting the CCVSR application.
Description	Displays the description of the server. You may modify the information here.
Role	Displays the role of the server.
IPv4 Address	Displays the CCVSR's IPv4 address.
IPV6 Address	Displays the CCVSR's IPV6 address.
Server MAC	Displays the MAC address of the computer hosting the CCVSR application.

Server Port Settings

This is used to specify the service ports used to access the CCVSR:

Item	Meaning
HTTP	The port number for a browser login. The default is 9080.
HTTPS	The port number for a secure browser login. The default is 9443.
CCVSR	This is the port number for communication between a CCVSR Primary Server and Secondary Servers. The default is 9002.

As a security measure, if a firewall is being used, the Administrator can specify the port numbers that the firewall will allow. If a port other than the default is used, users must specify the port number as part of the IP address when they log in. If an invalid port number (or no port number) is specified, the CCVSR will not be found.

For Example: To access the CCVSR with an IP address of 192.168.0.100, using a secure browser login (https), enter:

https://192.168.0.100:9443

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

2. Service ports cannot have the same value. You must set a different value for each one.
3. If there is no firewall (on an Intranet, for example), it does not matter what these numbers are set to since they have no effect.

Archive Server Settings

If you have installed a CCVSR Archive Server, input the IP Address and Port number of the computer hosting the software. For more information on configuring the Archive Server see *CCVSR Archive Server*, page 87, for details.

Server Type

You can change the role of the server here. Select *Primary* or *Secondary* using the drop-down menu.Primary Server

Select *Primary Server* for a computer that is running as the main Video Session Recording Software. This computer will host and manage all aspects of the Video Session Recording Software, and can add computers running as *Secondary Servers* for extended storage of video log files.

Secondary Server

Select *Secondary Server* if the computer is being used as a storage for video log files from the *Primary Server* and they do not support any system management functions such as settings configuration, device management, and user management.

As a *Secondary Server*, one of its functions is to store video log files for the *Primary Server.* If you choose this option, provide the following information:

> *Sever Address:* enter the IP address of a computer running the *Primary* Video Session Recording Software.
>
> *Service Ports:* in the *Server Port Settings* above, enter the CCVSR / HTTP / HTTPS service port numbers of the *Primary Server.* The default service ports are 9002 / 9080 / 9443. Additional information about service ports is provided in *Server Port Settings* on page 57.

The Secondary Server must be added to the *Primary Server* in order to work. *See Recording*, page 75, for details.

When you log in locally (httsp://127.0.0.1:9443) after changing the server to a secondary server, only the *Server Info* sub-menu is shown.

When the primary server fails, one of the secondary servers will act as a redundant server to make sure that the service is always available. In this case, this secondary server will have access to viewing the management settings. The other secondary servers in your setup will still act as storages. Once the primary server is back online, the redundant server will resume to its original role as a storage server. If the primary server is broken down permanently, administrators can change a secondary server to a primary server from the local management webpage (https://127.0.0.1:9443).

Note: If you try to enter the secondary server using its IP address (e.g. https:\\192.168.0.100:9443), the system will automatically direct you to the primary server.

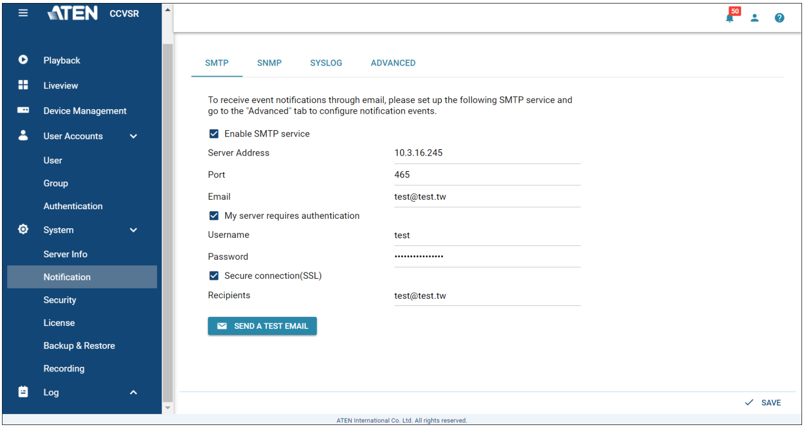
Misc

Check the checkbox to disable keystroke recording.

Notification

The notification page allows you to setup notification methods.

SMTP



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

☑ Enable SMTP service

Server Address	10.3.16.245
Port	465
Email	test@test.tw

☑ My server requires authentication

Username	test
Password	················

☑ Secure connection(SSL)

Recipients	test@test.tw

To have the CCVSR email reports from the SMTP server to you, do the following:

1. Enable the *Enable SMTP service*, and key in either the IPv4 address, IPv6 address, or domain name of the SMTP server.
2. Key in the SMTP port.
3. Key in the email address of where the report is being sent from in the *Email* field.

Note:

1. Only one email address is allowed in the *Email* field, and it cannot exceed 64 Bytes.
2. 1 Byte = 1 English alphanumeric character.

4. If your server requires authentication, check the *My server requires authentication* checkbox, and key in the appropriate account information in the *Username* and *Password* fields.
5. If your server requires a secure SSL connection, check the *Secure connection (SSL)* checkbox.

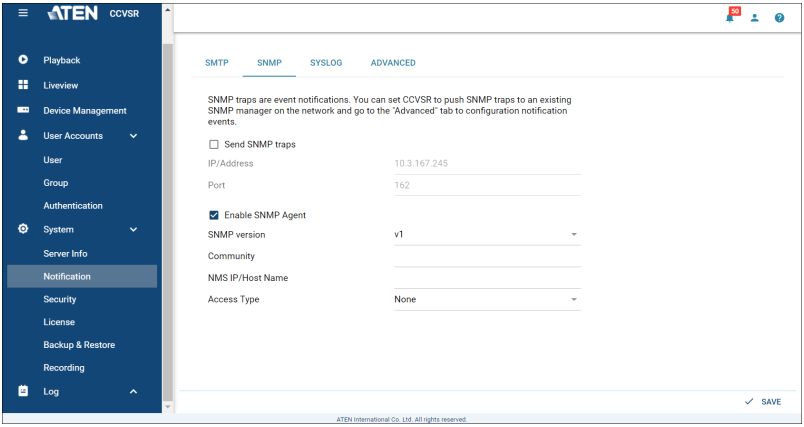
6. Key in the email address of where the report is being sent to in the *Recipients* field.

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

---

7. Click *Save* on the bottom right-hand corner of the window to save the configuration.

SNMP Server



SNMP traps are event notifications. You can set CCVSR to push SNMP traps to an existing SNMP manager on the network and go to the "Advanced" tab to configuration notification events.

☐ Send SNMP traps

IP/Address 10.3.167.245

Port 162

☑ Enable SNMP Agent

SNMP version v1

Community

NMS IP/Host Name

Access Type None

To be notified of SNMP trap events, do the following:

1. Check *Send SNMP traps*.
2. Key in either the IPv4 address, IPv6 address, or domain name of the computer to be notified of SNMP trap events.
3. Key in the port number. The valid port range is 1–65535.

Note: The logs that are notified of SNMP trap events are configured on the Notification Settings page under the *Log* tab. See *Advanced (Notification)*, page 63 for details.

---

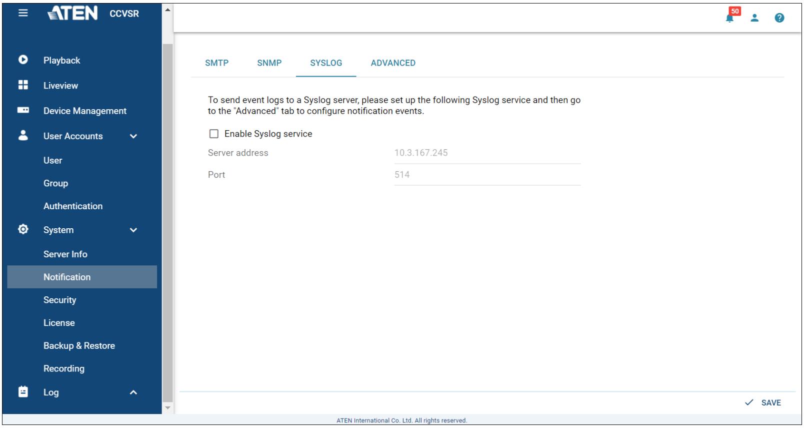
4. Check *Enable SNMP Agent*.
5. Select SNMP version by clicking the drop-down menu.
6. Key in the community value(s) if required for the SNMP version.

7. Enter the NMS IP/Host Name.

8. Select Access Type by clicking the drop-down menu.

9. Click *Save* on the bottom right-hand corner of the window to save the configuration.

Syslog Server



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

☐ Enable Syslog service

Server address 10.3.167.245

Port 514

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

1. Check *Enable Syslog service*.

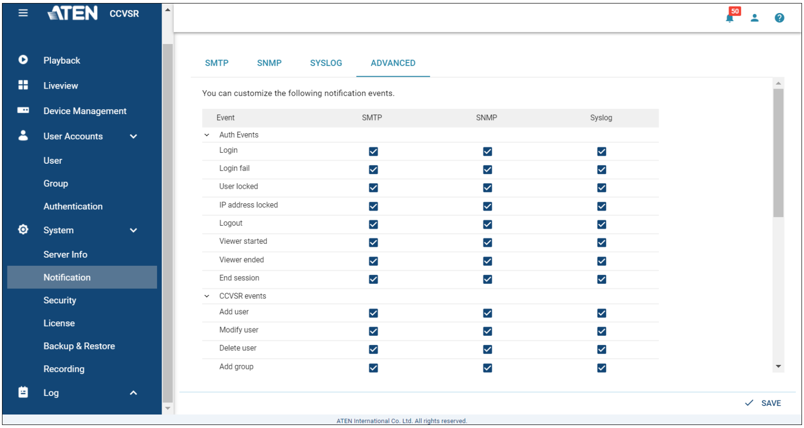
2. Key in either the IPv4 address, IPv6 address, or domain name of the Syslog server.

3. Key in the port number. The valid port range is 1-65535.

4. Click *Save* on the bottom right-hand corner of the window to save the configuration.

Advanced (Notification)

The *Advanced (Notification)* page lets you decide which events trigger a notification, and how the notifications are sent out:



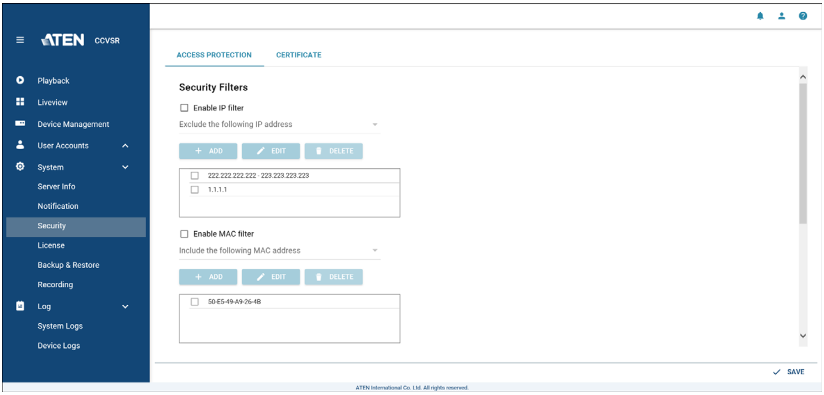
You can customize the following notification events.

Event	SMTP	SNMP	Syslog
Auth Events			
Login	☑	☑	☑
Login fail	☑	☑	☑
User locked	☑	☑	☑
IP address locked	☑	☑	☑
Logout	☑	☑	☑
Viewer started	☑	☑	☑
Viewer ended	☑	☑	☑
End session	☑	☑	☑
CCVSR events			
Add user	☑	☑	☑
Modify user	☑	☑	☑
Delete user	☑	☑	☑
Add group	☑	☑	☑

Notifications can be sent via SNMP trap, SMTP email, written to the SysLog file, or any combination of the three. A check mark indicates that notification of the event is permitted for the method specified in the column heading. An empty box indicates that notification is not restricted.

Security

The Security sub-menu includes 2 tabs.



Security Filters

□ Enable IP filter

Exclude the following IP address

□ 222.222.222.222 - 223.223.223.223
□ 1.1.1.1

□ Enable MAC filter

Include the following MAC address

□ 50-E5-49-A9-26-4B

Access Protection

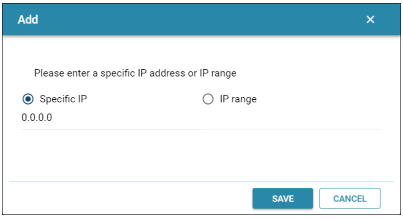
IP / MAC Filtering

IP / MAC filters control access to the Video Session Recording Software based on the IP / MAC addresses of the client computers attempting to connect. A maximum of 100 IP or MAC filters are allowed. If any filters have been configured, they appear in the IP Filter list box.

To enable and add IP / MAC filtering,

1. Check the *Enable IP Filter* or *Enable MAC Filter* checkbox.
2. Select between *Exclude the following IP/MAC address* or *Include the following IP/MAC address* from the drop-down menu.
3. Click the + ADD button.

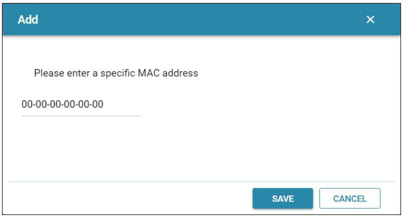
   A pop-up window appears:



Please enter a specific IP address or IP range

● Specific IP ○ IP range

0.0.0.0



Please enter a specific MAC address

00-00-00-00-00-00

4. For IP filter, select between *Specific IP* and *IP range*.

   For MAC filter, enter the MAC address.

5. For specific IP, enter the IP. For IP range, enter the first IP of the IP range in the first field and the second IP in the second field.

6. Repeat these steps for any additional IP / MAC addresses you want to filter.

7. Click *Save*.

To edit IP / MAC filtering, check an IP / IP range / MAC address and click the ✎ EDIT button. Configure as described in page 64.

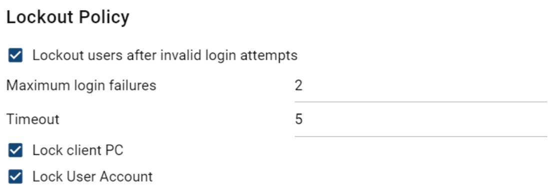
To delete IP / MAC filtering, check an IP / IP range / MAC address and click the 🗑 DELETE button..

- IP Filter / MAC Filter Conflict

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

Lockout Policy

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



Lockout Policy

☑ Lockout users after invalid login attempts

Maximum login failures 2

Timeout 5

☑ Lock client PC

☑ Lock User Account

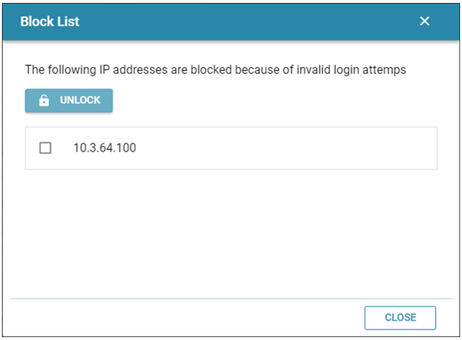
To set the lockout policy, check *Lockout users after invalid login attempts* (the default is for Login Failures to be enabled). The meanings of the entries are explained below.

Entry	Explanation
Maximum login failures	Sets the number of consecutive failed login attempts that are permitted from a remote computer. The default is 5 times.
Timeout	Sets the amount of time a remote computer must wait before attempting to login again after it has exceeded the number of allowed failures. The default is 3 minutes.

Entry	Explanation
Lock Client PC	If this is enabled (checked), after the allowed number of failures have been exceeded, the computer attempting to log in is automatically locked out. No logins from that computer will be accepted. The default is enabled. **Note:** This function relates to the client computer's IP. If the IP is changed, the computer will no longer be locked out.
Lock Account	If this is enabled (checked), after the allowed number of failures have been exceeded, the user attempting to log in is automatically locked out. No logins from the username and password that have failed will be accepted. The default is enabled.

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

Block List: Clicking this button will bring out a window. The window includes the locked accounts.



The following IP addresses are blocked because of invalid login attemps

□ 10.3.64.100

To unlock the accounts, check the IP address and click the *Unlock* button.

Login String

The *Login String* entry field lets the administrator specify a login string (in addition to the IP address) that users must add to the IP address when they access the Video Session Recorder with a browser.

For example, if *192.168.0.126* were the IP address, and *atenccvsr* were the login string, then the user would have to key in:

```
192.168.0.126:9443/atenccvsr
```

Note: 1. Users must place a forward slash between the IP address and the string.

2. If no login string is specified here, anyone will be able to access the Video Session Recorder login page using the IP address alone. This makes your installation less secure.

The following characters are allowed in the string:

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

The following characters are not allowed:

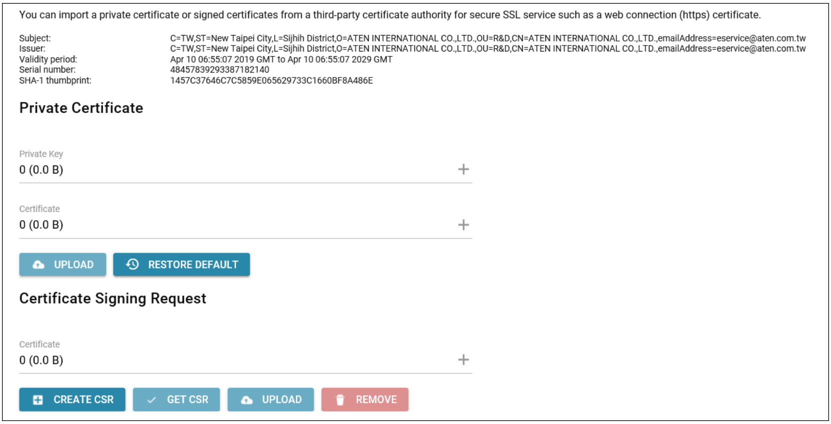
% ^ ” : / ? # \ ‘ { } ; ’ < > [Space]

Compound characters (É Ç ñ ... etc.)

For security purposes, we recommend that you change this string occasionally.

Click *Save* on the bottom right-hand corner of the window to save the configuration.

Certificate



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

Subject:	C=TW,ST=New Taipei City,L=Sijhih District,O=ATEN INTERNATIONAL CO.,LTD.,OU=R&D,CN=ATEN INTERNATIONAL CO.,LTD.,emailAddress=eservice@aten.com.tw
Issuer:	C=TW,ST=New Taipei City,L=Sijhih District,O=ATEN INTERNATIONAL CO.,LTD.,OU=R&D,CN=ATEN INTERNATIONAL CO.,LTD.,emailAddress=eservice@aten.com.tw
Validity period:	Apr 10 06:55:07 2019 GMT to Apr 10 06:55:07 2029 GMT
Serial number:	48457839293387182140
SHA-1 thumbprint:	1457C37646C7C5859E065629733C1660BF8A486E

Private Certificate

Private Key: 0 (0.0 B)

Certificate: 0 (0.0 B)

Certificate Signing Request

Certificate: 0 (0.0 B)

Private Certificate

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

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

- Generating a Self-Signed Certificate

  If you wish to create your own self-signed certificate, a free utility – openssl.exe – is available for download over the web. See *Self-Signed Private Certificates*, page 102 for details about using OpenSSL to generate your own private key and SSL certificate.

- Obtaining a CA Signed SSL Server Certificate

  For the greatest security, we recommend using a third party certificate authority (CA) signed certificate. To obtain a third party signed certificate, go to a CA (Certificate Authority) website to apply for an SSL certificate. After the CA sends you the certificate and private encryption key, save them to a convenient location on your computer.

- Importing the Private Certificate

  To import the private certificate, do the following:

1. Click + to the right of *Private Key*; browse to where your private encryption key file is located; and select it.
2. Click + to the right of *Certificate*; browse to where your certificate file is located; and select it.
3. Click **Upload** to complete the procedure.

Note: 1. Clicking **Restore Default** returns the device to using the default ATEN certificate.

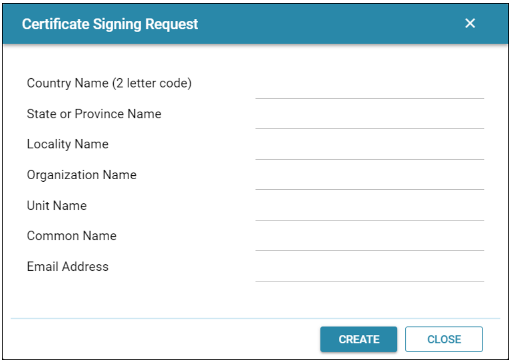
2. Both the private encryption key and the signed certificate must be imported at the same time.

Certificate Signing Request

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

To perform this operation do the following:

1. Click **Create CSR**. The following dialog box appears:



Certificate Signing Request

Country Name (2 letter code)	
State or Province Name	
Locality Name	
Organization Name	
Unit Name	
Common Name	
Email Address	

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

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

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

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

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

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

5. After the CA sends you the certificate, save it to a convenient location on your computer. Click + to locate the file; then click **Upload** to store it on the CCVSR.

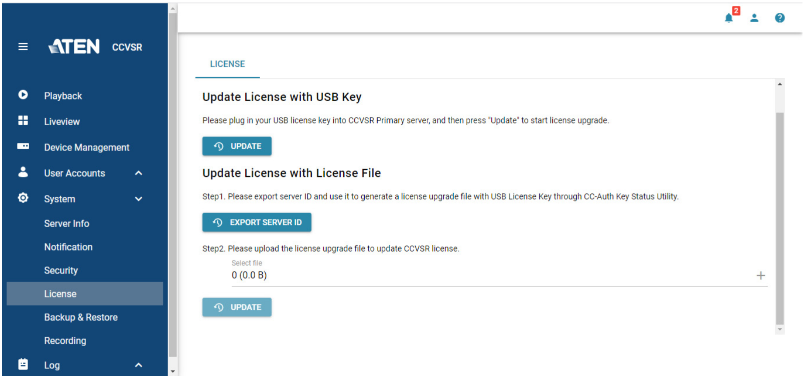
Note: When you upload the file, the CCVSR checks the file to make sure the specified information still matches. If it does, the file is accepted; if not, it is rejected.

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

License

The CCVSR license controls the total number of secondary servers and nodes permitted, including used and available, on your CCVSR installation.

Upon completion of the CCVSR software installation, a default license for one primary server is automatically provided. To add more CCVSR nodes and/or secondary servers, you must upgrade the license.



Update License with USB Key

Please plug in your USB license key into CCVSR Primary server, and then press "Update" to start license upgrade.

Update License with License File

Step1. Please export server ID and use it to generate a license upgrade file with USB License Key through CC-Auth Key Status Utility.

Step2. Please upload the license upgrade file to update CCVSR license.

Select file: 0 (0.0 B)

To upgrade the license, contact your dealer to purchase a license key for the number of nodes and secondary servers desired.

After receiving your purchased USB license key, you can upgrade your CCVSR license using one of the two following methods:

- Upgrade by directing inserting the USB license key into the primary server.
- Upgrade without directly inserting the USB license key.

Upgrade License with USB Key

1. Insert the license key into a USB port on your CCVSR server.
2. Log into the CCVSR application, go to **License**, and click **Update** under *Update License with USB Key*.

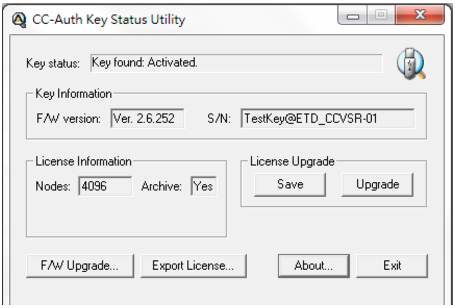
Note: 1. Once the upgrade has completed, it is no longer necessary to keep the license key plugged into the USB port. Remove the key and place it somewhere safe, since you will need it for future upgrades.

2. If you lose the USB license key, contact your dealer to obtain another one. If you supply the key's serial number the new key will contain all of the information that was stored on the lost key.

Upgrade License with License File

This method is useful when it is inconvenient to directly insert the USB license key into your CCVSR primary server, such as in a restricted area where USB connection is prohibited.

1. On the CCVSR primary server, go to **License**, and click **Export Server ID** to generate a **.sid* server ID file, containing information about the server and its installation details. Export and save the file onto a separate PC.
2. On the separate PC, insert the USB license key.
3. Open *CC-Auth Key Status Utility* and click **Export License**, as illustrated below. You're asked to locate and select the server ID file generate from step 1. Once finished, a **.lic* license upgrade file is generated.



CC-Auth Key Status Utility

Key status: Key found: Activated.

Key Information

F/W version: Ver. 2.6.252 S/N: TestKey@ETD_CCVSR-01

License Information

Nodes: 4096 Archive: Yes

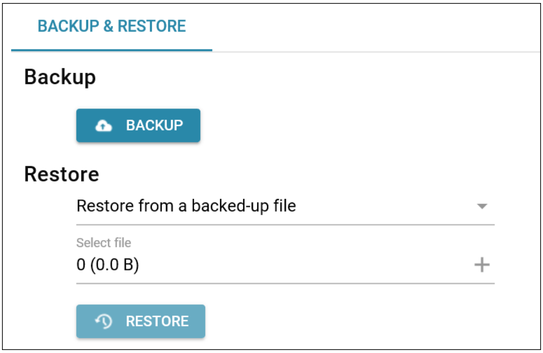
4. Import and save the **.lic* file into the CCVSR primary server, and click + under *Update License with License File* to locate it.
5. Click **Update** to initiate the license upgrade.

Note: The license upgrade file can only be used to upgrade the license of the CCVSR server from which the server id file was generated.

Once the license has been upgraded, you can install and use additional CCVSRs and/or nodes (per the number of licenses purchased), which will communicate and work in conjunction over a network.

Backup & Restore

The *Backup & Restore* page is used to *Backup* and *Restore* system configuration settings and user account information to/from a file or system created *Checkpoint*. There are two sections:



BACKUP & RESTORE

Backup

BACKUP

Restore

Restore from a backed-up file

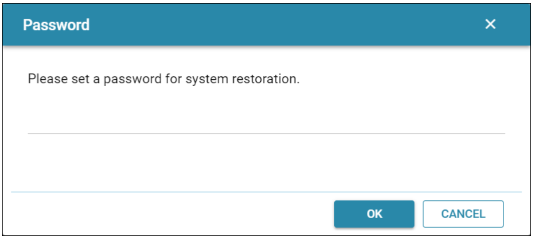
Select file

0 (0.0 B)

RESTORE

Backup

To create a backup file, click *Backup* to save the file. A window will pop-up to ask you to enter a password.



Password

Please set a password for system restoration.

OK CANCEL

Leave the *Password* field blank if you do not want to use a password. Press *OK* to backup the system configuration. The saved data file contains the current system configuration and all user account information.

Restore

To restore data,

1. Select where you are restoring the configurations from by selecting from the drop-down menu. Select between *Restore from a backed-up file* or *Restore from a checkpoint*.

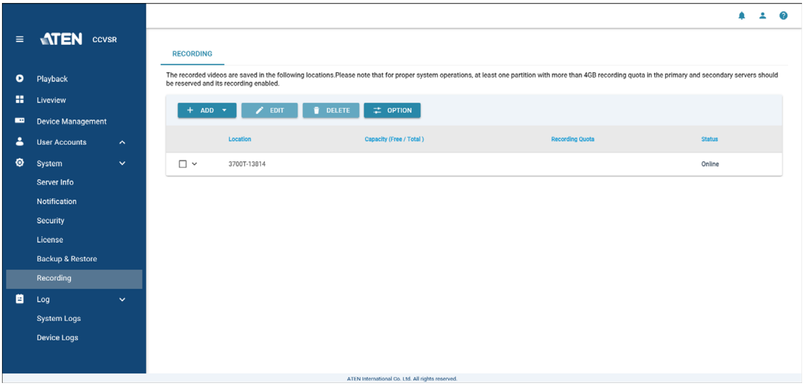
2. For back-up file, click + and select a file.

For checkpoint, select the checkpoint from the checkpoint list.

3. Click Restore.

Recording

This page allows you to select the destinations (Primary Server, Secondary Servers, or shared network folder) and you wish to store the video log files. *Secondary CCVSR Servers* are also used to save video log files on alternative computers in order to consolidate disk space across different computers. To configure a secondary computer to work as a *Secondary CCVSR Server*, see *Server Type*, page 58 for details. When you select *Recording*, the following screen appears:



The recorded videos are saved in the following locations.Please note that for proper system operations, at least one partition with more than 4GB recording quota in the primary and secondary servers should be reserved and its recording enabled.

	Location	Capacity (Free / Total)	Recording Quota	Status
□	3700T-13814			Online

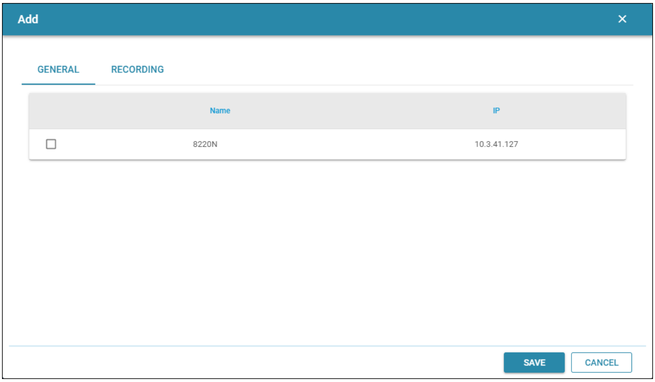
From the *Recording* menu page you can:

- *Add* or *Delete* CCVSR Servers
- *Add* or *Delete* Network shared folder
- *Enable* or *Disable* recording locations
- Set retention policy for video log files

Adding Secondary CCVSR Servers

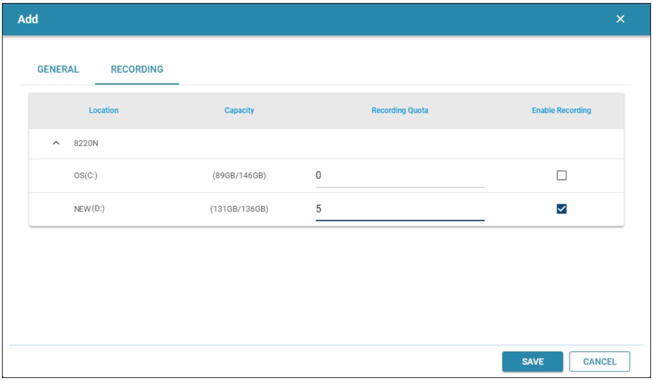
The Secondary CCVSR Server you are adding must be on a computer available over the network. To add a CCVSR Server, do the following:

1. Click *Add*.
2. A pop-up screen appears to bring you to the *General* tab:



	Name	IP
□	8220N	10.3.41.127

3. Select a CCVSR Server from the list (in the same LAN as the primary server) and click **Next** for the *Recording* tab:



Location	Capacity	Recording Quota	Enable Recording
^ 8220N			
OS(C:)	(89GB/146GB)	0	□
NEW(D:)	(131GB/136GB)	5	☑

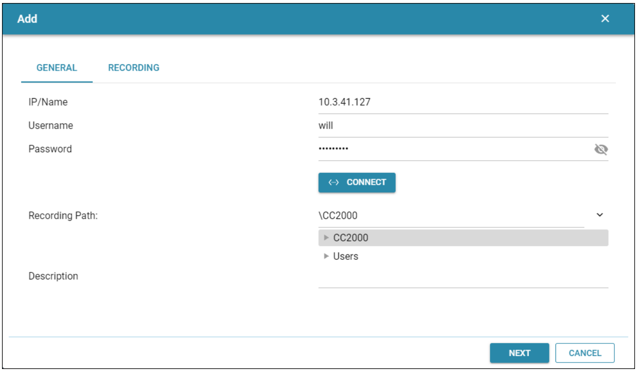
4. Select the recording location by checking the checkbox of the *Enable Recording* column. Enter a value in the corresponding field of the *Recording Quota* column.
5. Click *Save* to save the configuration and the CCVSR Server will now appear on the Recording main page.

Adding Shared Network Folder

To add a Shared Network Folder, do the following

1. Click *Add*.

2. A pop-up screen appears to bring you to the *General* tab:



Add

IP/Name: 10.3.41.127
Username: will
Password: •••••••••
Recording Path: \CC2000
Description

3. Fill in the information of the top three entries that are valid for your network folder location using the following table:

Item	Description
IP/Name	Enter the IP address of the server sharing the network folder.
Username	Enter a username with permission to access the shared network folder.
Password	Enter a password.

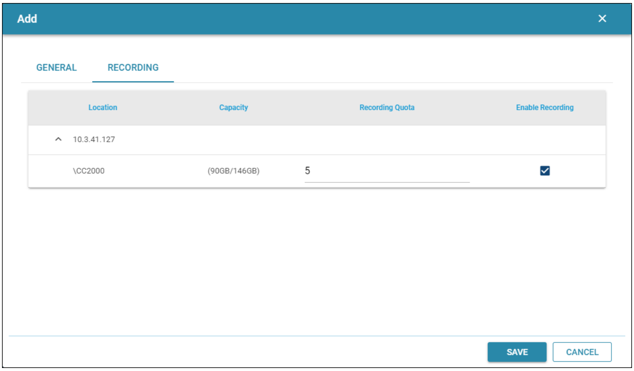
4. Click *Connect* to retrieve path information automatically. If retrieved correctly, you can select the recording path from the drop-down menu. You may also enter a description in the description entry.

Note: Please make sure that SMBv2 & v3 are supported.

Alternatively, you can enter the rest of the information using the table below:

Item	Description
Recording Path	Enter the folder location of the server where you want to save the video log files. Example: Share\Department2\Security\VideoLogs
Description	Enter a description for the network folder.

5. Click *Next* for the *Recording* tab:



Location	Capacity	Recording Quota	Enable Recording
^ 10.3.41.127			
\CC2000	(90GB/146GB)	5	☑

6. Select the recording location by checking the checkbox of the *Enable Recording* column. Enter a value in the corresponding field of the *Recording Quota* column.

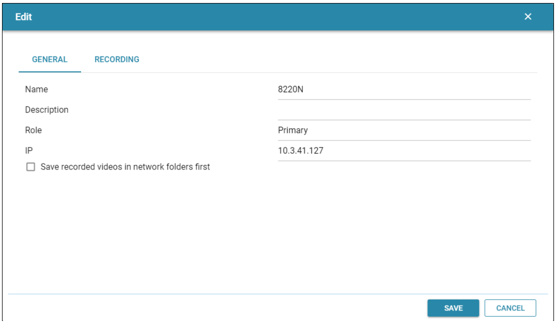
7. Click *Save* to save the configuration and the Shared Network Folder will now appear on the Recording main page.

Editing Secondary CCVSR Servers

To edit a CCVSR server, do the following:

1. On the *Recording* page, check the checkbox of the CCVSR server.

2. Click *Edit* for the pop-up page below:



Name 8220N

Description

Role Primary

IP 10.3.41.127

□ Save recorded videos in network folders first

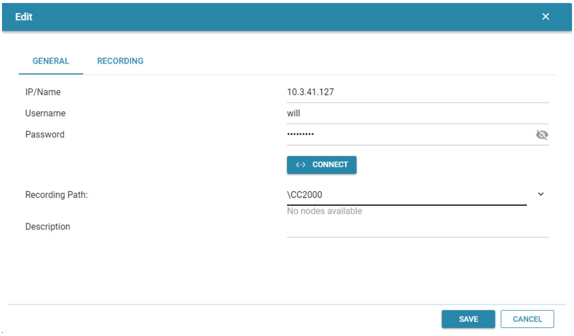
3. You can edit the name and description of the CCVSR server and enable (check)/disable (uncheck) *Save recorded videos in network folders first* here. Click the *Recording* tab to edit the options there (e.g. disable recording).

4. After making the changes, click *Save* to save the configuration.

Editing Shared Network Folder

To edit a Shared network folder, do the following:

1. On the *Recording* page, check the checkbox of the Shared network folder.
2. Click *Edit* for the pop-up page below:



IP/Name: 10.3.41.127
Username: will
Password: ••••••••
Recording Path: \CC2000
No nodes available
Description:

3. You can edit the username and password and click *Connect* again to retrieve path information and re-select the recording path from the drop-down menu. Click the *Recording* tab to edit the options there (e.g. disable recording).
4. After making the changes, click *Save* to save the configuration.

Deleting Secondary CCVSR Servers/Shared Network Folder

To delete a CCVSR server/Shared network folder, do the following:

1. On the *Recording* page, check the checkbox of the entry you wish to delete.
2. Click *Delete*.

Option - Retention Policy

If *Continue recording without overwriting any video* is selected, CCVSR will continue recording until the recording quota is reached.

If *Keep the videos within (days)* and a number (1-365) is entered, the videos older than the entered number will be deleted.

For example, if you entered 7 days, the Video Session Recording Software will delete recordings that are older than 7 days and leaves all video files created in the past 7 days untouched.

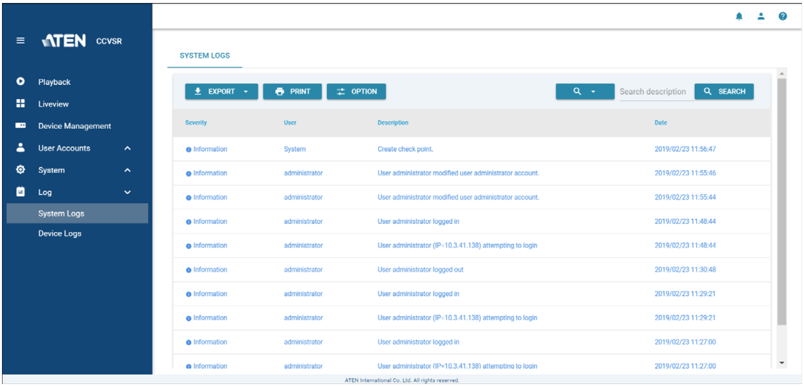
The retention policy is refreshed at 00:00 everyday.

This Page Intentionally Left Blank

Chapter 9
Logs

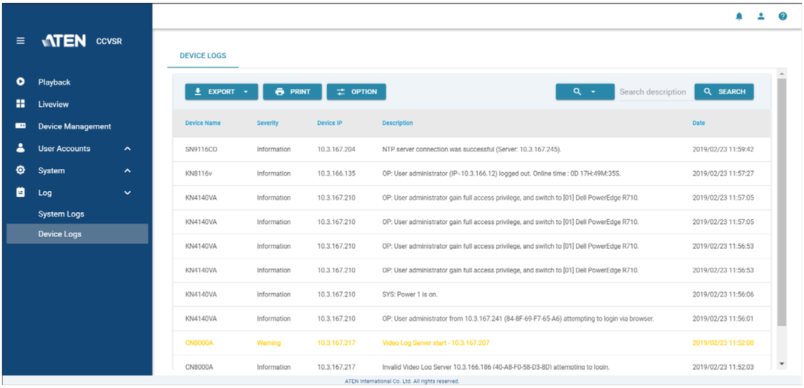
Overview

The Video Session Recording Software logs all the events that take place on it. To view the contents of the log, click *Log* to expand the Log main menu and click to select the type of log you wish to see. The System Logs and Device Logs are respectively shown below:



Severity	User	Description	Date
Information	System	Create check point.	2019/02/23 11:56:47
Information	administrator	User administrator modified user administrator account.	2019/02/23 11:55:46
Information	administrator	User administrator modified user administrator account.	2019/02/23 11:55:44
Information	administrator	User administrator logged in	2019/02/23 11:48:44
Information	administrator	User administrator (IP=10.3.41.138) attempting to login	2019/02/23 11:48:44
Information	administrator	User administrator logged out	2019/02/23 11:30:48
Information	administrator	User administrator logged in	2019/02/23 11:29:21
Information	administrator	User administrator (IP=10.3.41.138) attempting to login	2019/02/23 11:29:21
Information	administrator	User administrator logged in	2019/02/23 11:27:00
Information	administrator	User administrator (IP=10.3.41.138) attempting to login	2019/02/23 11:27:00

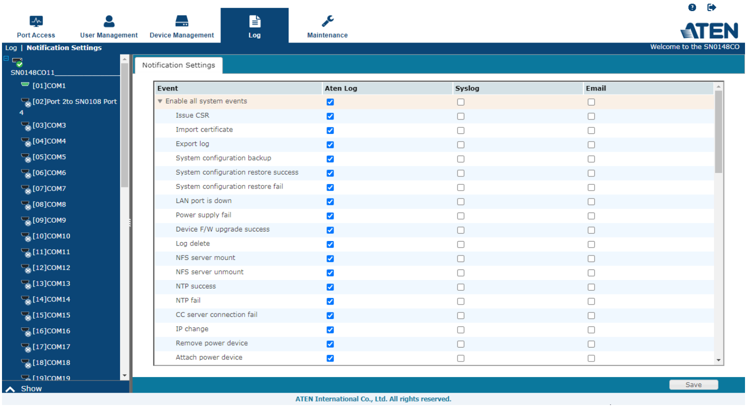
ATEN International Co. Ltd. All rights reserved.



Device Name	Severity	Device IP	Description	Date
SN9116CO	Information	10.3.167.204	NTP server connection was successful (Server: 10.3.167.245).	2019/02/23 11:59:42
KN8116v	Information	10.3.166.135	OP: User administrator (IP=10.3.166.12) logged out. Online time : 0D 17H:49M:35S.	2019/02/23 11:57:27
KN4140VA	Information	10.3.167.210	OP: User administrator gain full access privilege, and switch to [01] Dell PowerEdge R710.	2019/02/23 11:57:05
KN4140VA	Information	10.3.167.210	OP: User administrator gain full access privilege, and switch to [01] Dell PowerEdge R710.	2019/02/23 11:57:05
KN4140VA	Information	10.3.167.210	OP: User administrator gain full access privilege, and switch to [01] Dell PowerEdge R710.	2019/02/23 11:56:53
KN4140VA	Information	10.3.167.210	OP: User administrator gain full access privilege, and switch to [01] Dell PowerEdge R710.	2019/02/23 11:56:53
KN4140VA	Information	10.3.167.210	SYS: Power 1 is on.	2019/02/23 11:56:06
KN4140VA	Information	10.3.167.210	OP: User administrator from 10.3.167.241 (84-8F-69-F7-65-A6) attempting to login via browser.	2019/02/23 11:56:01
CN8000A	Warning	10.3.167.217	Video Log Server start - 10.3.167.207	2019/02/23 11:52:08
CN8000A	Information	10.3.167.217	Invalid Video Log Server 10.3.166.186 (40-A8-F0-58-D3-8D) attempting to login.	2019/02/23 11:52:03

ATEN International Co. Ltd. All rights reserved.

Note: If you wish to receive logs of an added serial console server, make sure you have enabled notification settings on the serial console server's own notification page. An example (SN0148CO device interface) is shown below:

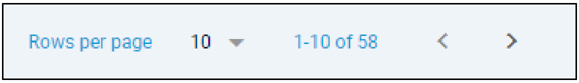


Event	Aten Log	Syslog	Email
▾ Enable all system events	☑	□	□
Issue CSR	☑	□	□
Import certificate	☑	□	□
Export log	☑	□	□
System configuration backup	☑	□	□
System configuration restore success	☑	□	□
System configuration restore fail	☑	□	□
LAN port is down	☑	□	□
Power supply fail	☑	□	□
Device F/W upgrade success	☑	□	□
Log delete	☑	□	□
NFS server mount	☑	□	□
NFS server unmount	☑	□	□
NTP success	☑	□	□
NTP fail	☑	□	□
CC server connection fail	☑	□	□
IP change	☑	□	□
Remove power device	☑	□	□
Attach power device	☑	□	□

Log Information

The System and Device log tables display events that take place on the Video Session Recording Software, and provide sorting columns with headings of time, severity, user, and a description. Click any of the headings to sort the order of the events.

At the bottom right-hand corner of the tables, you can select the number of displayed entries (rows), and go to previous/next page of entries.



To select the number of displayed entries, click the drop-down menu and select from the menu.

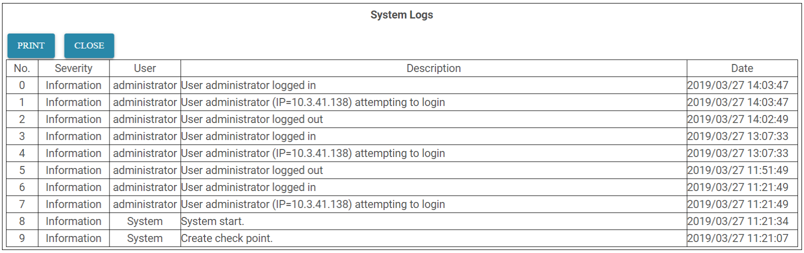
Click the < or > to go to previous or next page of entries.

Export Logs

You can export *Logs in current page* or *All logs* using the export button. Click for a drop-down menu and select either of the options. The log file is saved in the .dat format.

Print Logs

You can print logs using the *Print* button. When clicked, the system will bring you to a printable log page as shown:

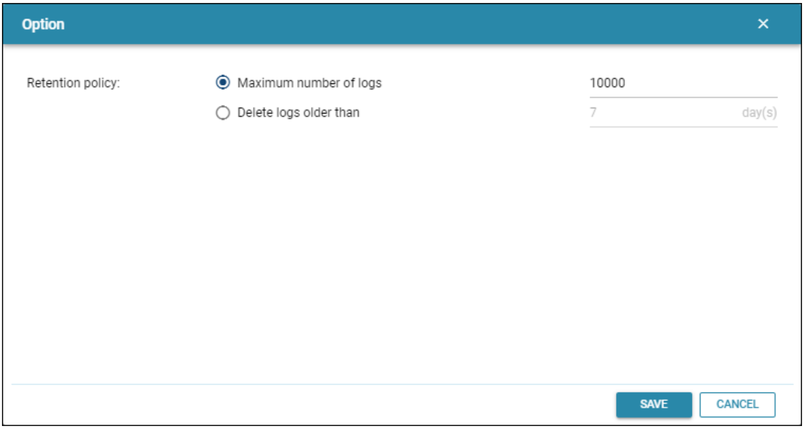


No.	Severity	User	Description	Date
0	Information	administrator	User administrator logged in	2019/03/27 14:03:47
1	Information	administrator	User administrator (IP=10.3.41.138) attempting to login	2019/03/27 14:03:47
2	Information	administrator	User administrator logged out	2019/03/27 14:02:49
3	Information	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

Click *Print* for the print setup of your system or *Close* to leave this page.

Option

You can set the retention policy of the logs by clicking the *Option* button:



Option ✕

Retention policy: ● Maximum number of logs 10000

○ Delete logs older than 7 day(s)

The system is set to keep a maximum of 10,000 log events by default. The system will overwrite the oldest entries. You can enter a different number here.

If you wish to keep the log events within a number of days, select *Delete logs older than* and enter a value (in days). Log entries older than the entered value will be discarded automatically.

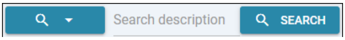
Search Logs

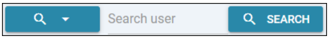
The *Search* function allows you to do a general search or an advanced search. and *Advanced Search*.

General Search

For a general search, you can search according to the *Description* or *User*:

1. Click the 🔍 ▾ button for a drop-down menu.
2. Select *Description* or *User*. The search field will display the selection.



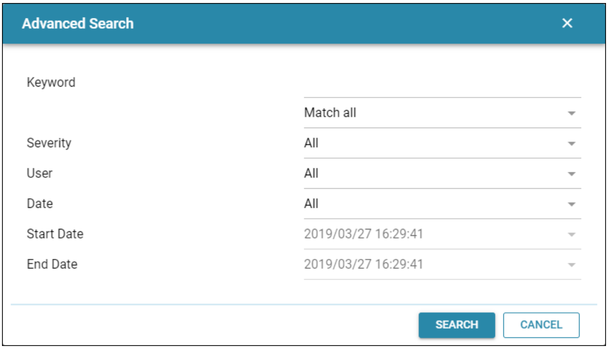


3. Enter the information you wish to search for in the entry field and click the 🔍 SEARCH button.

Advanced Search

For an advanced search:

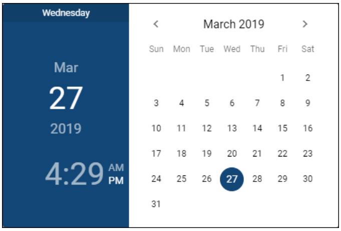
1. Click the 🔍 ▾ button for a drop-down menu.
2. Select *Advanced Search* for the pop-up window below:



Advanced Search ✕

Keyword	
	Match all ▾
Severity	All ▾
User	All ▾
Date	All ▾
Start Date	2019/03/27 16:29:41 ▾
End Date	2019/03/27 16:29:41 ▾

Refer to the table below on how to use the advanced search:

Field	Explanation
Keyword	Searches for a particular word or string. Key the word or string into the entry. Only events containing that word or string are displayed. Wildcards (? for single characters; * for multiple characters) and the keyword **or** are supported. E.g., h*ds would return hands and hoods; h?nd would return hand and hind, but not hard; h*ds or h*ks would return hands and hooks.
Match all / Match any	Click the drop-down menu to select between *Match all* and *Match any*. **Match all**: The search has to meet all specified information. **Match any**: The search only has to meet any of the specified information.
Severity	Click the drop-down menu to search by the severity level. Available entries include *Information*, *Warning* and *Critical*.
User	Click the drop-down menu to search according to the user type. Available entries include *All*, *System* and *administrator*.
Date	Click the drop-down menu to search according to the date range. Available entries include *All* and *Range*. If *Range* is selected, the next two entries (*Start Date* and *End Date*) will light up and can be used. **Start Date**: From the drop-down menu, select a specific date and time. Clicking the drop-down menu will bring up date and time selection as shown:  Wednesday Mar 27 2019 4:29 AM PM March 2019 Sun Mon Tue Wed Thu Fri Sat 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 As shown on the left of the diagram above, the day of the month is lit, indicating we are selecting the day as reflected on the left of the diagram. For other selections (month, year, hour, minute, am/pm), click the dimmed section you wish to change. **End Date**: Follow the selection method as in *Start Date*.
Search	Click to search according to the filter choices.
Cancel	Click this to cancel advanced search.

Chapter 10
CCVSR Archive Server

Overview

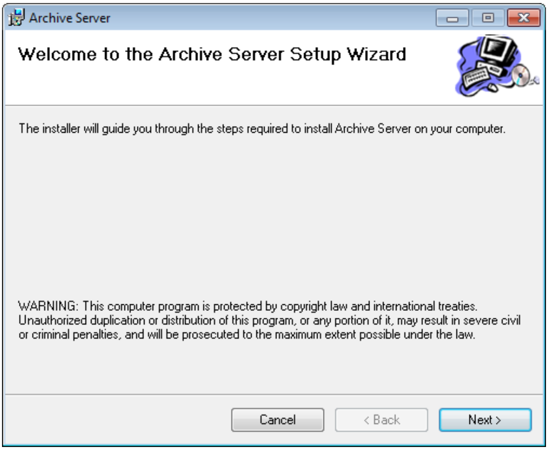
The CCVSR Archive Server allows you to store, playback, import, and export data created on CCVSR servers. The software automatically transfers a copy of the video log files from the Primary CCVSR server into an organized archive separate from the main system. This gives you the ability to purge older files from the main system but keep a safe archive of all videos for future use. The Archive Server runs in the background and updates the archive automatically every 15 minutes. To purchase this software, please see *Licenses*, page 8, for details.

Installing the CCVSR Archive Server

Starting the Installation

To install the Archive Server on a Windows system, insert the USB License Key into your computer, and do the following:

1. Put the software CD that came with your package into the computer's CD drive, or open the folder with the installation file.
2. Go to the folder where the *setup.exe* is located and double click it. A screen similar, to the one below, appears:



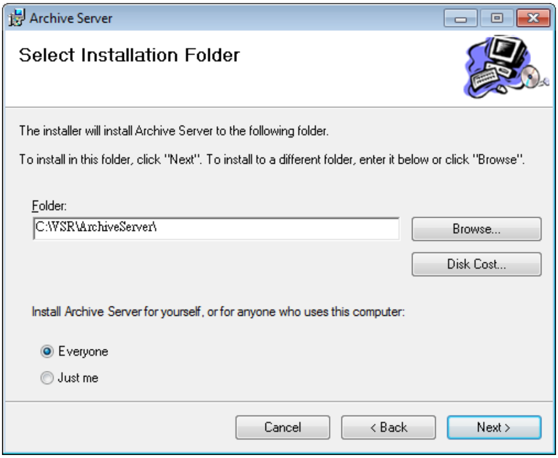
Welcome to the Archive Server Setup Wizard

The installer will guide you through the steps required to install Archive Server on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Click **Next** to continue.

3. On the *Select Installation Folder* page, specify the installation folder, or click **Browse** to choose the location where you want to install it. Then choose if you want to install it for yourself (**Just me**), or for anyone who uses this computer (**Everyone**). Click **Disk Cost** to view available drives and disk space.



The installer will install Archive Server to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

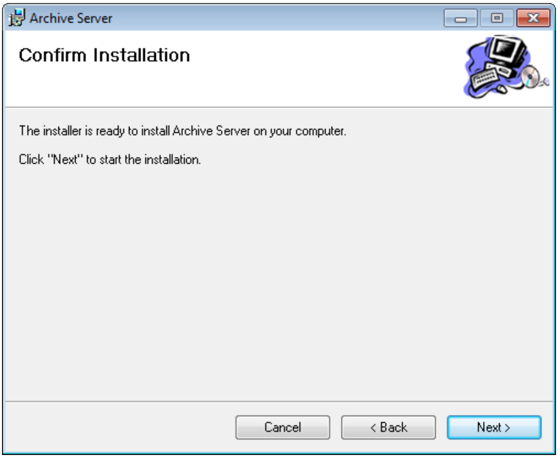
Folder: C:\VSR\ArchiveServer\

Install Archive Server for yourself, or for anyone who uses this computer:

● Everyone
○ Just me

Click **Next** to continue.

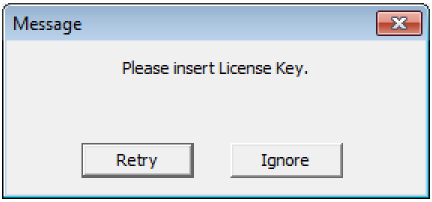
4. The *Confirm Installation* window appears, click **Next** to continue:



The installer is ready to install Archive Server on your computer.

Click "Next" to start the installation.

5. If a message appears to insert the License Key, re-plug the USB License Key into your computer or try a different USB port, then click **Retry**.

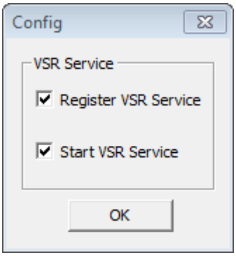


Message

Please insert License Key.

Clicking **Ignore** will install the software but you will not be able to use it until the USB License Key has been made available.

6. The **Config** dialog box appears, select the options and click **OK**:



Config

VSR Service

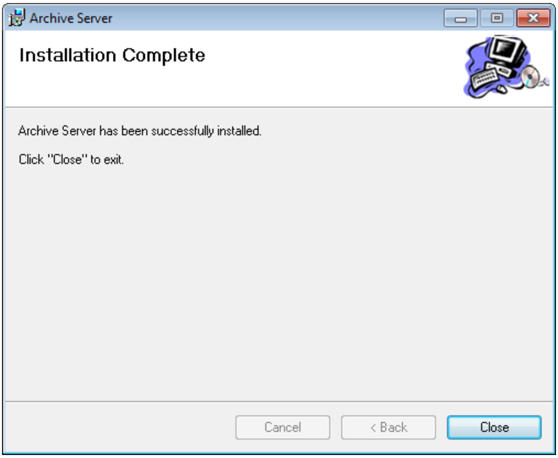
☑ Register VSR Service

☑ Start VSR Service

Register CCVSR Service: This option registers the CCVSR Service with the Windows operating system so that it can run the software in the background.

Start CCVSR Service: This option will start the CCVSR Service automatically after the installation is complete. It is recommend to select both options.

7. When the installation is complete the following message will appear:

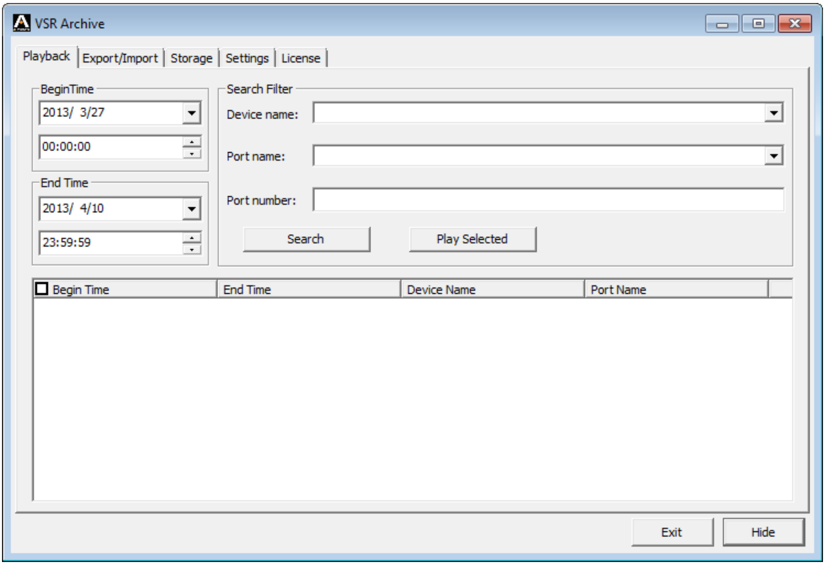


Archive Server has been successfully installed.

Click "Close" to exit.

Archive Server GUI

The Archive Server's interface has 5 tabs: *Playback*, *Export/Import*, *Storage*, *Settings*, and *License*; all described below. Once the software has been installed, double click the *Archive GUI* icon located on the desktop, and the *Playback* page appears:



BeginTime
2013/ 3/27
00:00:00

End Time
2013/ 4/10
23:59:59

Search Filter
Device name:
Port name:
Port number:

□ Begin Time	End Time	Device Name	Port Name

Use the **Exit** button to shutdown the Archive Server, or **Hide** button to minimize the window to the task bar.

Setup

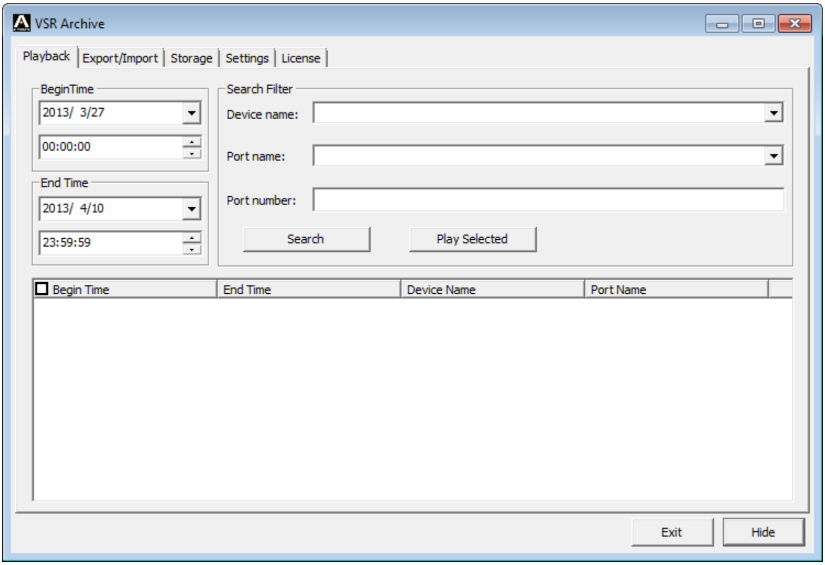
There are two steps to setup the Archive Server- set the Archive Server's IP address on the Primary CCVSR server, and add a storage location from the Archive Server's **Storage** tab.

First, configure the Archive Server's IP Address on the Primary CCVSR Server (see *Archive Server Settings*, page 57). Next, add a storage location from the **Storage** tab (see *Storage*, page 96). The storage location is where the archived video log files are saved.

After the IP address is configured and a storage location is added, the Archive Server will begin to automatically archive all video log files created after the installation. The archive is updated every 15 minutes. To check for new video log files, go to the **Playback** tab and click *Search*. All new video log files will appear in the search window.

Playback

The *Playback* tab is used to search and playback video log files which have been archived or manually imported. To see a list of all video log files that have been archived, simply click the *Search* button.



BeginTime: 2013/ 3/27 00:00:00

End Time: 2013/ 4/10 23:59:59

Device name:

Port name:

Port number:

□ Begin Time	End Time	Device Name	Port Name

The *Playback* tab has 3 sections used to search and playback archived video log files.

Begin Time/End Time

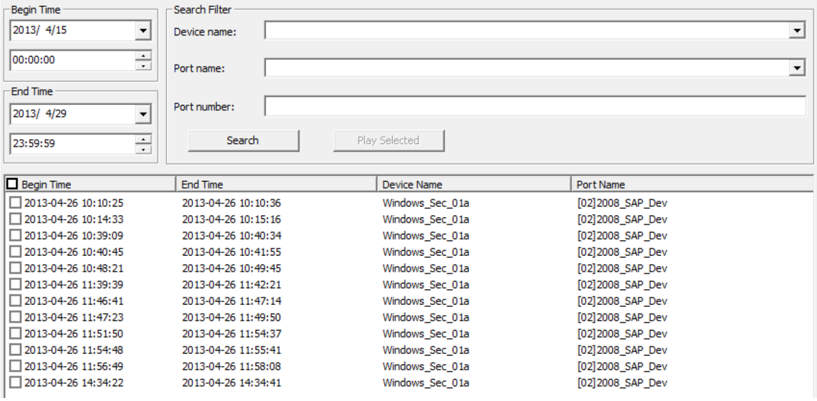
This section allows you to filter the search results by the begin and end time. The *Begin Time* and *End Time* refers to the time when the actual video log recording took place on the KVM switch.

Search Filter

The *Search Filter* is used to search for archived video log files by the *Port Name, Device Name*, or *Port Number* of the KVM switch they were recorded on. After inputting the search data, click **Search**. Your search results* will appear at the bottom of the page, and you can sort your results using the columns provided. If you would like to view all archived video logs, simply leave the fields blank and click **Search**.

Play Selected

To playback video logs, click **Search*** for a list of the archived video log to appear:



Begin Time
2013/ 4/15
00:00:00

End Time
2013/ 4/29
23:59:59

Search Filter
Device name:
Port name:
Port number:

□ Begin Time	End Time	Device Name	Port Name
□ 2013-04-26 10:10:25	2013-04-26 10:10:36	Windows_Sec_01a	[02]2008_SAP_Dev
□ 2013-04-26 10:14:33	2013-04-26 10:15:16	Windows_Sec_01a	[02]2008_SAP_Dev
□ 2013-04-26 10:39:09	2013-04-26 10:40:34	Windows_Sec_01a	[02]2008_SAP_Dev
□ 2013-04-26 10:40:45	2013-04-26 10:41:55	Windows_Sec_01a	[02]2008_SAP_Dev
□ 2013-04-26 10:48:21	2013-04-26 10:49:45	Windows_Sec_01a	[02]2008_SAP_Dev
□ 2013-04-26 11:39:39	2013-04-26 11:42:21	Windows_Sec_01a	[02]2008_SAP_Dev
□ 2013-04-26 11:46:41	2013-04-26 11:47:14	Windows_Sec_01a	[02]2008_SAP_Dev
□ 2013-04-26 11:47:23	2013-04-26 11:49:50	Windows_Sec_01a	[02]2008_SAP_Dev
□ 2013-04-26 11:51:50	2013-04-26 11:54:37	Windows_Sec_01a	[02]2008_SAP_Dev
□ 2013-04-26 11:54:48	2013-04-26 11:55:41	Windows_Sec_01a	[02]2008_SAP_Dev
□ 2013-04-26 11:56:49	2013-04-26 11:58:08	Windows_Sec_01a	[02]2008_SAP_Dev
□ 2013-04-26 14:34:22	2013-04-26 14:34:41	Windows_Sec_01a	[02]2008_SAP_Dev

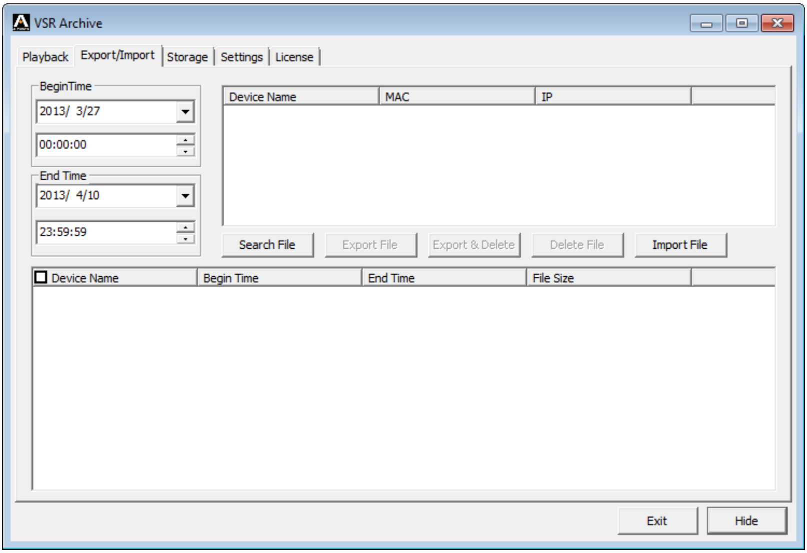
Select the checkboxes of the video(s) you want to playback, then click **Play Selected**. The video will open in a new window with the Video Log Viewer application. For information on the Video Log Viewer, see *VSR Viewer*, page 24.

Note: 1. If no video log files appear after clicking *Search*, either the archive hasn't updated, in which case you should wait 15 minutes; or a storage location needs to be added on the **Storage** tab (see *Storage*, page 96).

2. Only video logs created after the Archive Server was installed are automatically archived from the Primary CCVSR server. Video logs created before the installation must be manually imported from the **Export/Import** tab (see *Export/Import*, page 94).

Export/Import

The *Export/Import* tab is used to export and import video log files in a single database (.vse) file format. The database (.vse) files can combine a large number of individual video logs into a single compressed file to reduce disk space, which can be exported for storage and imported for use. The Export/Import tab also allows you to import individual video log files (.dat) created on the CCVSR Primary Server.



BeginTime: 2013/ 3/27, 00:00:00

End Time: 2013/ 4/10, 23:59:59

You can search for files to export (which are already archived) by selecting a **Device Name** and clicking **Search File**; or manually import .vse or .dat files into the Archive Server by clicking **Import File**. For more information on imported files see *Import File* below.

Begin Time/End Time

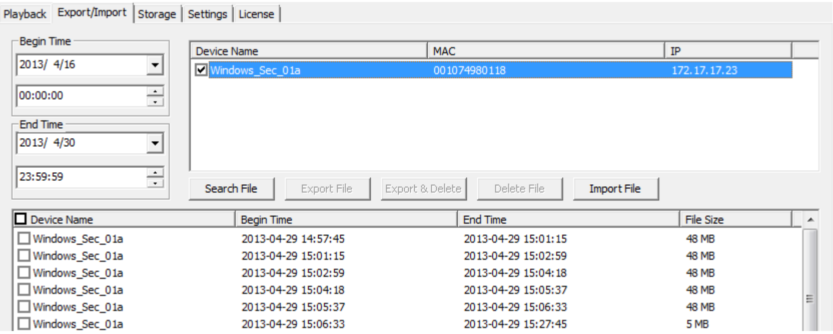
This section allows you to filter the search results by the begin and end time. The *Begin Time* and *End Time* refers to the time when the actual video recording took place on the KVM switch.

Device Name

This section lists the name(s) of the KVM switches which have been added to the Primary CCVSR server. You can select a device(s) and click Search for a list of individual video log files which have been archived from that KVM switch. After doing so you can select video logs to export into a .vse database file.

Search File

The *Search File* button is used to search for video log files on the **Device Name** you have selected. The results will appear in the lower section of the window, as shown below. After doing so you can select video logs to export into a .vse database file.



Begin Time: 2013/ 4/16 00:00:00

End Time: 2013/ 4/30 23:59:59

Device Name	MAC	IP
☑ Windows_Sec_01a	001074980118	172.17.17.23

□ Device Name	Begin Time	End Time	File Size
□ Windows_Sec_01a	2013-04-29 14:57:45	2013-04-29 15:01:15	48 MB
□ Windows_Sec_01a	2013-04-29 15:01:15	2013-04-29 15:02:59	48 MB
□ Windows_Sec_01a	2013-04-29 15:02:59	2013-04-29 15:04:18	48 MB
□ Windows_Sec_01a	2013-04-29 15:04:18	2013-04-29 15:05:37	48 MB
□ Windows_Sec_01a	2013-04-29 15:05:37	2013-04-29 15:06:33	48 MB
□ Windows_Sec_01a	2013-04-29 15:06:33	2013-04-29 15:27:45	5 MB

Export File

When you export logs they are saved in a single compressed .vse database file. Select the video log file(s) displayed in the lower window that you want to export, click **Export File** and provide a name to save the .vse file as.

Export & Delete

The *Export & Delete* button exports the selected files into a .vse database file and deletes the individual video log files that you are exporting from the Archive Server. This is a fast way to purge the individual files you are archiving into a single database.

Delete File

The *Delete File* button deletes the selected video log file from the Archive Server.

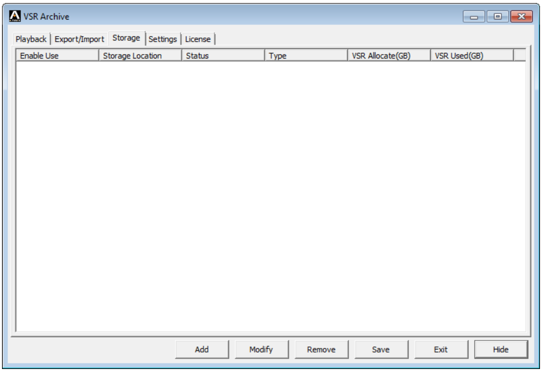
Import File

The *Import File* button is used to import database files (.vse) and individual video log files for viewing, archiving, or creating a new database- for export.

Click **Import File,** to browse and select the (.dat or .vse) file(s) to import, click **Open.** If you open a .vse database file: select the files from the list and click **Import**. Importing files will copy them into the Archive Server, therefore before you can import files, a storage location needs to be added from the **Storage** tab (see *Storage*, page 96). The storage location is where the archived files are saved, by the date they were created.

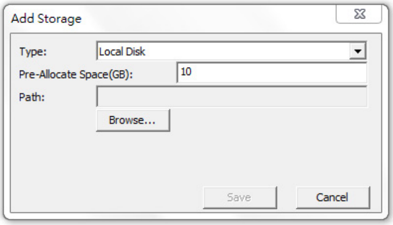
Storage

The *Storage* tab is used to add storage locations, locally or in a shared network folder. This is where archived video logs are saved. You can add multiple storage locations for video logs. When the first location becomes full, the second will be used, and so on. Video logs are archived into folders according to the date they were created. The Archive Server cannot archive video logs until a storage location is **added** and **enabled**.



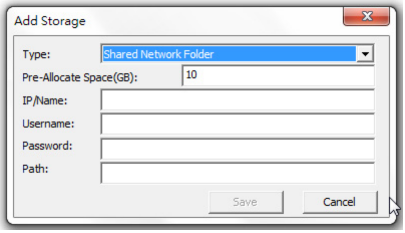
To add and enable a storage location, do the following:

1. Click **Add** and select **Local Disk** or **Shared Network Folder** for their respective settings, as shown below:



Type: Local Disk

Pre-Allocate Space(GB): 10



Type: Shared Network Folder

Pre-Allocate Space(GB): 10

2. For *Local Disk*, type in the *Path* or click **Browse** to select a storage location. For *Shared Network Folder*, fill in the required fields *IP/Name*, *Username*, *Password*, and *Path*.

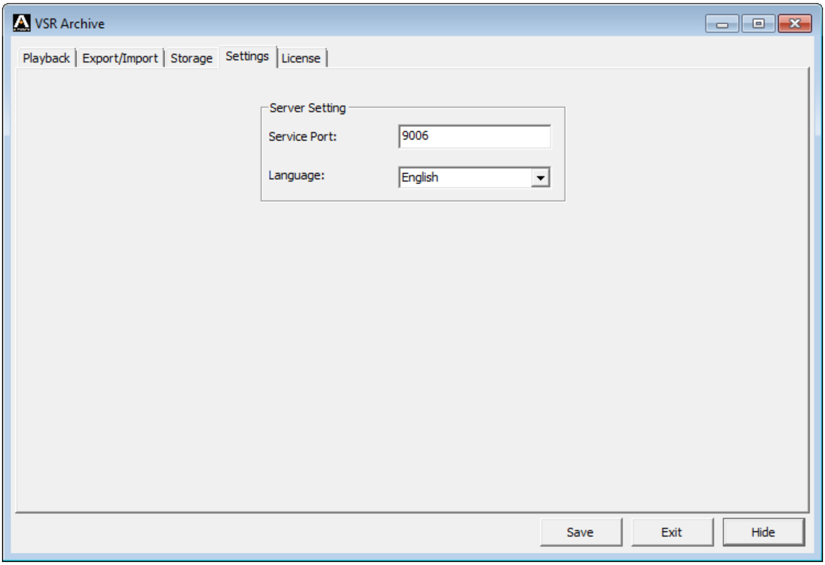
Note: Before a shared network folder can be used, users must first add a local disk with at least 10 GB of space, for saving temporary transfer files, to prevent video loss in the event of unstable network.

3. In the *Pre-Allocate Space(GB)* field enter the maximum amount of disk space to use, then click **Save**. The storage location appears in the lower window.
4. Next, check the **Enable Use** box and click **Save**.

Select a Storage Location and click **Modify** to modify it, or **Remove** to remove it. Click **Save** to save the changes.

Settings

The Settings tab is used to set the Server Settings:



Server Setting

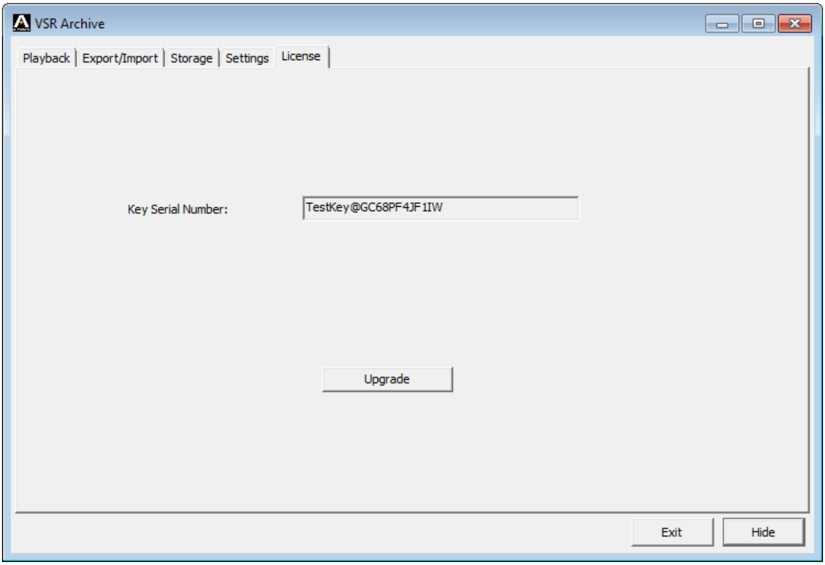
Service Port: 9006

Language: English

On this tab you can set the *Service Port* and *Language*. The default Service Port is **9006**.

License

Use the License tab to upgrade your license key. Insert the USB License Key into your computer, then click **Upgrade**.



Key Serial Number: TestKey@GC68PF4JF1IW

If the upgrade fails, re-insert the USB License Key, or try a different USB port on your computer.

Appendix A

Technical Support

International

- For online technical support – including troubleshooting, documentation, and software updates: **http://support.aten.com**
- For telephone support, see *Telephone Support*, page ii.

North America

Email Support		support@aten-usa.com
Online Technical Support	Troubleshooting Documentation Software Updates	http://support.aten.com
Telephone Support		1-888-999-ATEN ext 4988

When you contact us, please have the following information ready beforehand:

- Product model number, serial number, and date of purchase.
- Your computer configuration, including operating system, revision level, expansion cards, and software.
- Any error messages displayed at the time the error occurred.
- The sequence of operations that led up to the error.
- Any other information you feel may be of help.

USB Authentication Key Specifications

Function		Key
Environment	Operating Temp.	0–40^{o} C
	Storage Temp.	-20–60^{o} C
	Humidity	0–80% RH, Non-condensing
Physical Properties	Composition	Metal and Plastic
	Weight	14 g
	Dimensions	8.36 x 2.77 x 1.37cm

Compatible Products

For a list of compatible products, refer to the “Specification” tab of the CCVSR page on the ATEN website.

Linux Installation

When installing or uninstalling the CCVSR software on a computer running Linux, use the following commands:

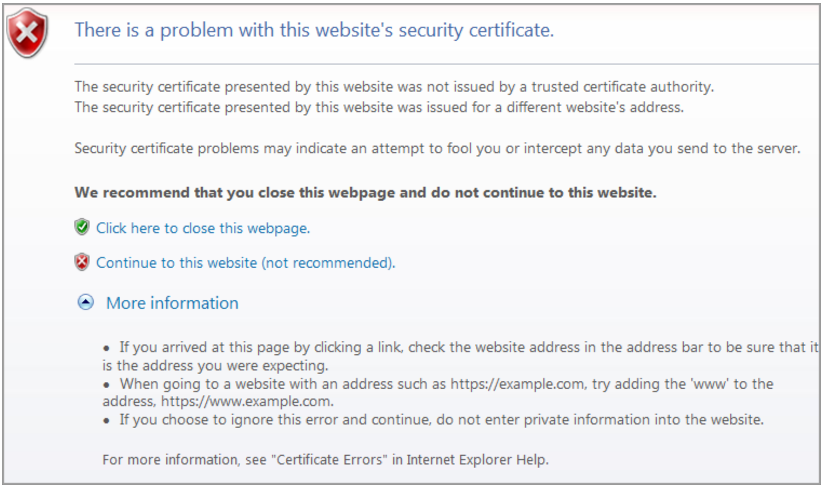
Linux installcommand:> sudo ./vlsman.run

Linux uninstall command:> sudo /usr/local/bin/ccvsr/uninstallvlsmon

Trusted Certificates

Overview

When you try to log in to the device from your browser, a Security Alert message appears to inform you that the device's certificate is not trusted, and asks if you want to proceed.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

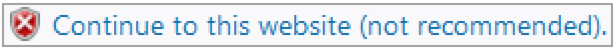
Continue to this website (not recommended).

More information

- If you arrived at this page by clicking a link, check the website address in the address bar to be sure that it is the address you were expecting.
- When going to a website with an address such as https://example.com, try adding the 'www' to the address, https://www.example.com.
- If you choose to ignore this error and continue, do not enter private information into the website.

For more information, see "Certificate Errors" in Internet Explorer Help.

The certificate can be trusted, but the alert is triggered because the certificate's name is not found on the Microsoft list of Trusted Authorities. You can ignore the warning and click:



Continue to this website (not recommended).

Self-Signed Private Certificates

If you wish to create your own self-signed encryption key and certificate, a free utility – openssl.exe – is available for download over the web at www.openssl.org. To create your private key and certificate do the following:

1. Go to the directory where you downloaded and extracted *openssl.exe* to.
2. Run openssl.exe with the following parameters:

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

Note: 1. The command should be entered all on one line (i.e., do not press [Enter] until all the parameters have been keyed in).

2. If there are spaces in the input, surround the entry in quotes (e.g. ”ATEN International”).

To avoid having to input information during key generation the following additional parameters can be used:

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

Examples

```
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
```

Importing the Files

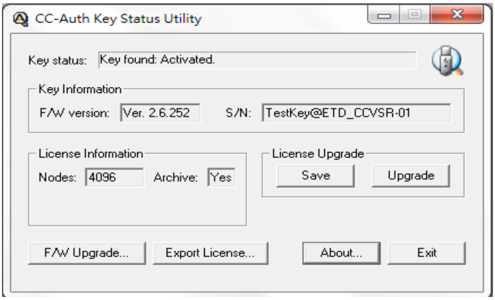
After the openssl.exe program completes, two files – CA.key (the private key) and CA.cer (the self-signed SSL certificate) – are created in the directory that you ran the program from. These are the files that you upload in the *Private Certificate* panel of the Security page (See *Security*, page 64, and *Certificate*, page 67).

Appendix B
Authentication Key Utility

Overview

The Authentication Key Utility (*CCAuthKeyStatus.exe*), is a Windows-based utility for accessing and updating the information and data contained in the CCVSR Authentication Key. *CCAuthKeyStatus.exe*, can be found on the CCVSR website.

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



CC-Auth Key Status Utility

Key status: Key found: Activated.

Key Information

F/W version: Ver. 2.6.252 S/N: TestKey@ETD_CCVSR-01

License Information

Nodes: 4096 Archive: Yes

Key Status Information

The layout of the dialog box is described in the table below:

Section	Purpose
Key Status	Indicates whether the key has been recognized and accepted as valid or not.
Key Information	Displays the key's current firmware version and serial number.
License Information	Displays the number of servers (Primary and Secondaries), and the number of nodes the key is licensed for.
License Upgrade	These buttons are used when performing an Offline license upgrade.
F/W Upgrade	This button is used to upgrade the authentication key's firmware.

Key Utilities

The License Upgrade and F/W Upgrade sections offer utilities that allow you to upgrade the key's firmware (F/W Upgrade), and to upgrade the number of servers and nodes authorized by the license (License Upgrade).

Key Firmware Upgrade

The CCVSR Authentication Key's firmware is upgradable. As new revisions of the firmware become released, upgrade file are posted on our web site. Check the web site regularly to find the latest files and information relating to them.

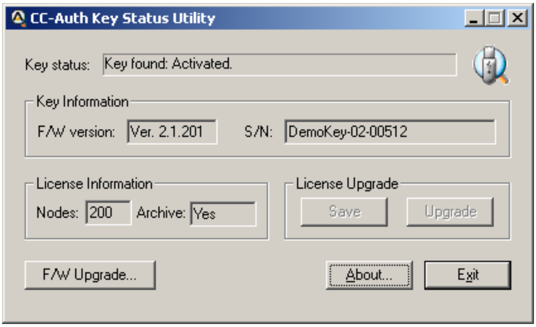
Starting the Upgrade

To upgrade your firmware, do the following:

1. Go to our website and download the new firmware file to a convenient location on your computer.
2. With the authentication key plugged in, run the *Key Status Utility* (CCAuthKeyStatus.exe).

Note: *CCAuthKeyStatus.exe* only runs under Windows and can be found on the CCVSR website.

3. In the screen that appears, click **F/W Upgrade...**



CC-Auth Key Status Utility

Key status: Key found: Activated.

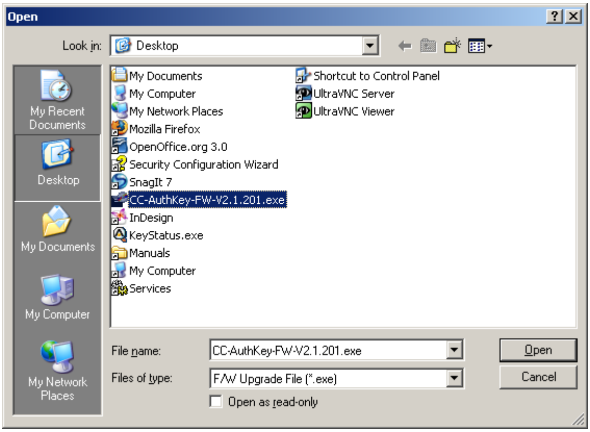
Key Information

F/W version: Ver. 2.1.201 S/N: DemoKey-02-00512

License Information

Nodes: 200 Archive: Yes

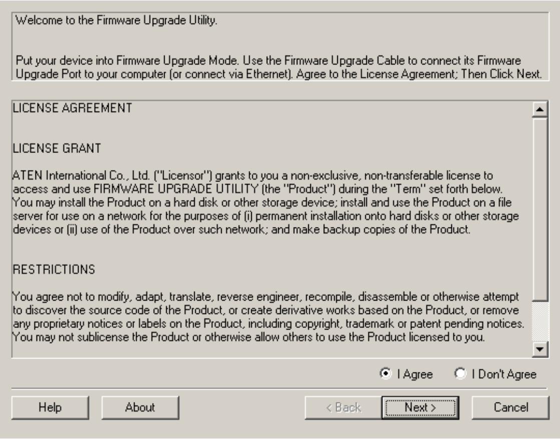
4. In the *File Open* dialog box that appears, select the firmware upgrade file, then click **Open**.



File name: CC-AuthKey-FW-V2.1.201.exe

Files of type: F/W Upgrade File (*.exe)

5. Read and *Agree* to the License Agreement (enable the *I Agree* radio button).



Welcome to the Firmware Upgrade Utility.

Put your device into Firmware Upgrade Mode. Use the Firmware Upgrade Cable to connect its Firmware Upgrade Port to your computer (or connect via Ethernet). Agree to the License Agreement; Then Click Next.

LICENSE AGREEMENT

LICENSE GRANT

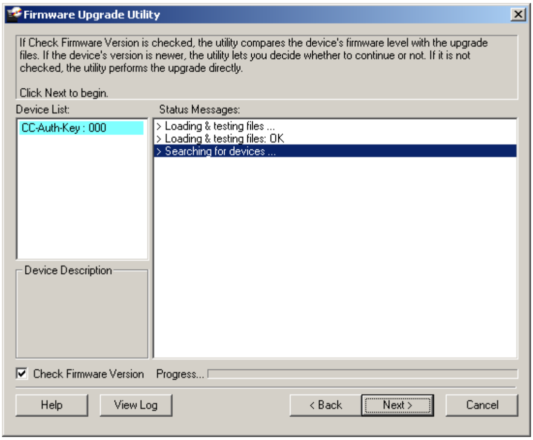
ATEN International Co., Ltd. ("Licensor") grants to you a non-exclusive, non-transferable license to access and use FIRMWARE UPGRADE UTILITY (the "Product") during the "Term" set forth below. You may install the Product on a hard disk or other storage device; install and use the Product on a file server for use on a network for the purposes of (i) permanent installation onto hard disks or other storage devices or (ii) use of the Product over such network; and make backup copies of the Product.

RESTRICTIONS

You agree not to modify, adapt, translate, reverse engineer, recompile, disassemble or otherwise attempt to discover the source code of the Product, or create derivative works based on the Product, or remove any proprietary notices or labels on the Product, including copyright, trademark or patent pending notices. You may not sublicense the Product or otherwise allow others to use the Product licensed to you.

● I Agree ○ I Don't Agree

6. The utility searches your installation. When it finds your device, it lists it in the *Device List* panel.



If Check Firmware Version is checked, the utility compares the device's firmware level with the upgrade files. If the device's version is newer, the utility lets you decide whether to continue or not. If it is not checked, the utility performs the upgrade directly.

Click Next to begin.

Device List:

CC-Auth-Key : 000

Status Messages:

```
> Loading & testing files ...
> Loading & testing files: OK
> Searching for devices ...
```

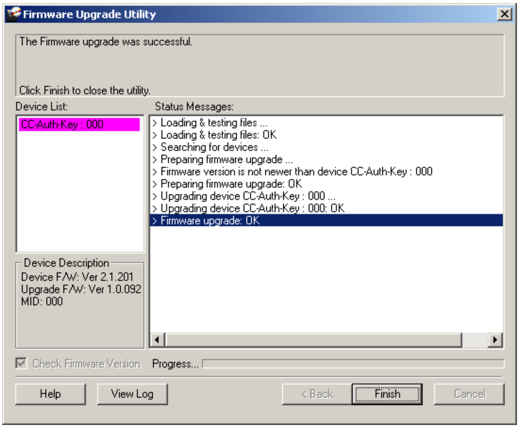
Note: If you enable *Check Firmware Version*, the Utility compares the device’s firmware level with that of the upgrade files. If it finds that the device’s version is higher than the upgrade version, it brings up a dialog box informing you of the situation and gives you the option to Continue or Cancel.

If you don’t enable *Check Firmware Version*, the Utility installs the upgrade files without checking if they are a higher level.

Click **Next** to continue.

Upgrade Succeeded

After the upgrade has completed, a screen appears to inform you that the procedure was successful:



The Firmware upgrade was successful.

Click Finish to close the utility.

Device List:

CC-Auth-Key : 000

Status Messages:

```
> Loading & testing files ...
> Loading & testing files: OK
> Searching for devices ...
> Preparing firmware upgrade ...
> Firmware version is not newer than device CC-Auth-Key : 000
> Preparing firmware upgrade: OK
> Upgrading device CC-Auth-Key : 000 ...
> Upgrading device CC-Auth-Key : 000: OK
> Firmware upgrade: OK
```

Device Description
Device F/W: Ver 2.1.201
Upgrade F/W: Ver 1.0.092
MID: 000

☑ Check Firmware Version

Click **Finish** to close the Firmware Upgrade Utility.

Key License Upgrade

Overview

The CC series has a feature that allows end users (clients) to update their authentication keys to reflect an increase to their number of licenses. The key license upgrade can be performed either by the clients or by the dealers/ distributors, and can take place either in a browser session over the Internet (an Online upgrade), or via a stand-alone utility program (an Offline upgrade).

Clients first inform their dealers/distributors of the number of licenses to be upgraded. The dealers/distributors then place an order with an Altusen sales representative, specifying the number of licenses to be added. After processing the order, Altusen then sends a confirmation and authorization email to the dealer/distributor with the necessary details for performing the upgrade.

Note: A separate order must be processed for each key.

There are two ways to upgrade the key:

- **On Line:** To perform the upgrade the key is inserted in the computer's USB port and a browser session is opened to directly upgrade the key. If the client performs the upgrade, the dealer/distributor provides him with the email authorization details; if the dealer/distributor performs the upgrade, the client provides him with the Authentication Key.

- **Off Line:** A Windows-based *Key Status Utility* is used to extract the key's information and write it to a Key Information Data File. The key information data file is then used in a a browser session to generate a license upgrade file. After the license upgrade file has been generated, the Key Status Utility is used again to write the upgrade file's information to the license key.
  - If the client is the one who updates the CC license database, the dealer/ distributor provides him with the email authorization details – allowing the client to generate his key license upgrade file. The client then uses the Key Status Utility and the key license upgrade file to upgrade the Authentication Key's license information.
  - If the dealer/distributor is the one who updates the CC license database, the client provides him with the key information data file (extracted with the Key Status Utility) which the dealer/distributor uses to generate the client's key license upgrade file. The dealer/distributor then returns the key license upgrade file to the client which the client uses with the Key Status Utility to upgrade the Authentication Key's license information.

Online Upgrade

Clients contact their dealers/distributors to place their upgrade order(s). A separate order must be processed for each key. After the dealers/distributors place the upgrade orders with an Altusen sales representative, they receive a confirmation and authorization email, similar to the example below:

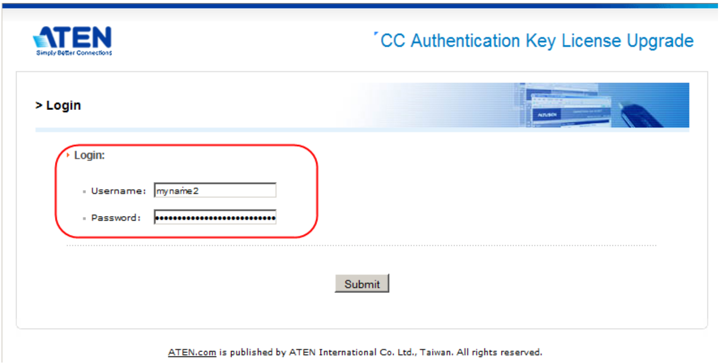
> Your order is ready to be processed. Please go to http://xxx.xxx.x.xxx to upgrade your key's license.
>
> Login Information:
>
> - Username: myname2
> - Password: mypassword5678
>
> Order Information:
>
> - Order ID: 1017000700 (authorized number: 2068919892). This order requests 1 more node(s)

Either the client or the dealers/distributors can perform the upgrade. If the dealer does it, the client provides the dealer with his license key; if the client does it, the dealer forwards the confirmation email to him.

Follow the steps below to perform online upgrade.

1. Plug the authentication key into a USB port on your computer.
2. Open a browser, go to the website CC Authentication Key License Upgrade page:

   https://cc.aten.com.tw/
3. When the upgrade Login screen comes up, log in with the Username and Password provided in the authorization email.

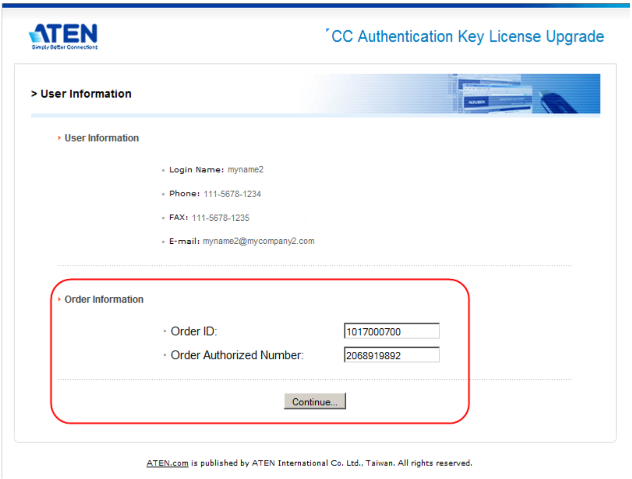


Username: myname2

Password: ••••••••••••••••••••••••••

ATEN.com is published by ATEN International Co. Ltd., Taiwan. All rights reserved.

4. In the screen that comes up, key in the Order ID number and Order Authorization number that applies to the upgrade, then click **Continue**.



ATEN Simply Better Connections

CC Authentication Key License Upgrade

> User Information

User Information

- Login Name: myname2
- Phone: 111-5678-1234
- FAX: 111-5678-1235
- E-mail: myname2@mycompany2.com

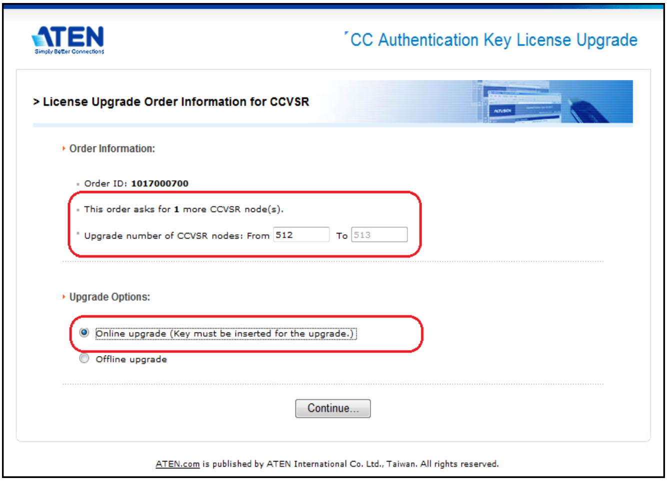
Order Information

- Order ID: 1017000700
- Order Authorized Number: 2068919892

Continue...

ATEN.com is published by ATEN International Co. Ltd., Taiwan. All rights reserved.

5. In the License Upgrade Order Information screen, key in the current number of licenses in the From fields (the To fields are automatically filled in), and select **Online upgrade**.



ATEN Simply Better Connections

CC Authentication Key License Upgrade

> License Upgrade Order Information for CCVSR

Order Information:

- Order ID: **1017000700**
- This order asks for **1** more CCVSR node(s).
- Upgrade number of CCVSR nodes: From 512 To 513

Upgrade Options:

● Online upgrade (Key must be inserted for the upgrade.)

○ Offline upgrade

Continue...

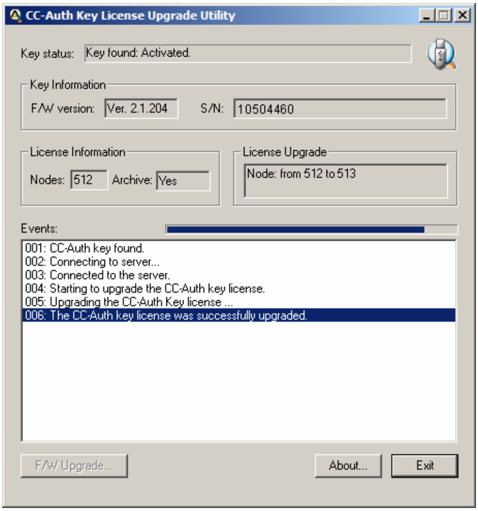
ATEN.com is published by ATEN International Co. Ltd., Taiwan. All rights reserved.

Note: You can use the Key status utility (e.g. ccauthkeystatus_utility.exe) to see the current number of licenses.

6. Click **Continue**.
7. When the Authentication Key License Upgrade by Distributor screen comes up, click **Download**.
8. When the browser asks what to do with the file (KeyUpgrade.exe), select *Save to disk*.
9. Leave the browser open, exactly as it is; go to where you downloaded the file and execute it.

Note: This step must be done in the same web session that you downloaded the KeyUpgrade.exe file in. Otherwise the upgrade will not succeed.

The upgrade utility comes up and starts the upgrade. The actions it performs are reported in the main panel:



CC-Auth Key License Upgrade Utility

Key status: Key found: Activated.

Key Information

F/W version: Ver. 2.1.204 S/N: 10504460

License Information

Nodes: 512 Archive: Yes

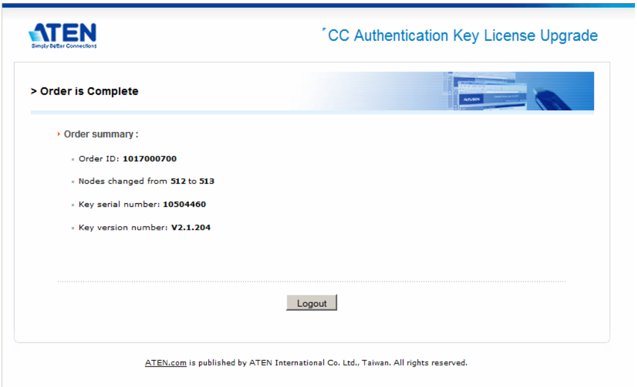
License Upgrade

Node: from 512 to 513

Events:

```
001: CC-Auth key found.
002: Connecting to server...
003: Connected to the server.
004: Starting to upgrade the CC-Auth key license.
005: Upgrading the CC-Auth Key license ...
006: The CC-Auth key license was successfully upgraded.
```

10. When the upgrade is finished, a window pops up to inform you that the upgrade was successful. Click **OK** to close the popup.The browser screen provides a summary of the upgrade:


ATEN
Simply Better Connections
CC Authentication Key License Upgrade

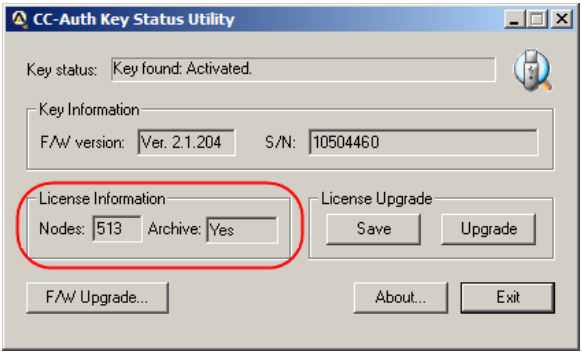
> Order is Complete

- Order summary :
  - Order ID: **1017000700**
  - Nodes changed from **512** to **513**
  - Key serial number: **10504460**
  - Key version number: **V2.1.204**

ATEN.com is published by ATEN International Co. Ltd., Taiwan. All rights reserved.

11. Click **Logout** to exit.

You can use the Key status utility (CCAuthKeyStatus.exe) to confirm that the number of licenses on the key has been changed to reflect the successful upgrade:



Key status: Key found: Activated.

Key Information

F/W version: Ver. 2.1.204 S/N: 10504460

License Information

Nodes: 513 Archive: Yes

Upgrade Succeeded

After the upgrade has succeeded, the dealer/distributor receives an email from Altusen informing him that the upgrade has been completed online. For example:

> 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.

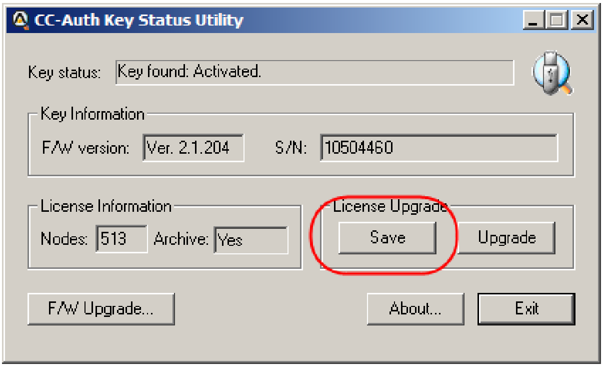
Offline Upgrade

An Offline upgrade can be performed either by the dealer/distributor, or the end user client. The advantage of this type of upgrade is that the client doesn't give up the use of his key. All he needs to do is email a key information data file to the dealer/distributor and receive a key upgrade file in return.

Preliminary Steps

To perform the upgrade, the first step that the client must perform is to create a *Key Information Data File*, as follows:

1. With the authentication key plugged in, run the *Key Status Utility* (CCAuthKeyStatus.exe).
2. In the *License Upgrade* panel of the dialog box that comes up, click **Save** to create a *Key Information Data File* (KeyUpload.dat).



Key status: Key found: Activated.

F/W version: Ver. 2.1.204

S/N: 10504460

Nodes: 513

Archive: Yes

Note: The Key Information Data File is created in the same directory that the Key Status Utility resides in.

After the Key Information Data File is created, the client sends it to the dealer/distributor.

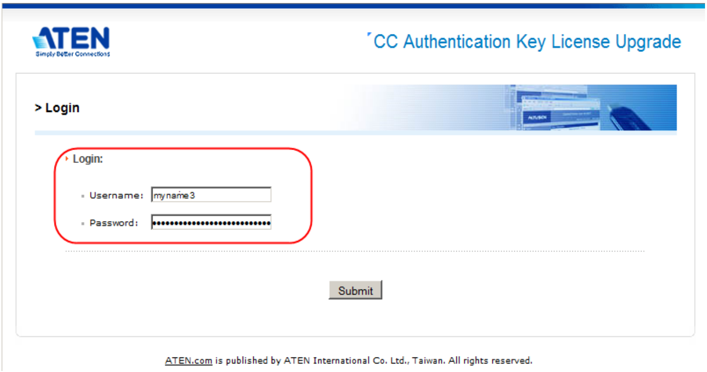
Performing the Upgrade

After the dealers/distributors place the upgrade orders with an Altusen sales representative, they receive a confirmation and authorization email from ALTUSEN, for example:

> 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)

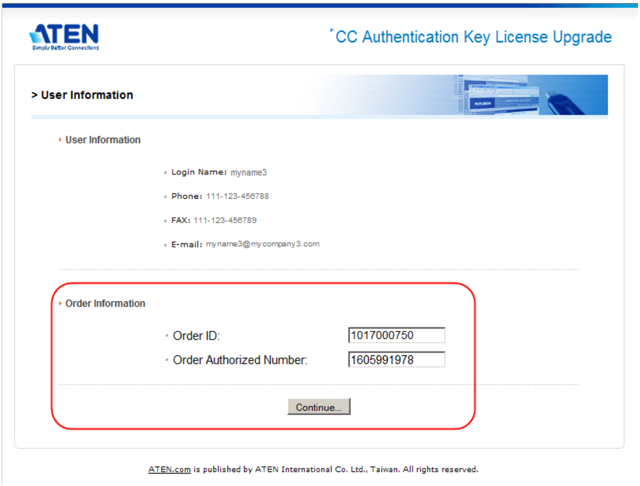
To perform the upgrade, do the following:

1. Follow steps 1 – 3 given for the Online Upgrade (see page 109).
2. When the upgrade Login screen comes up, log in with the Username and Password provided in the authorization email.


ATEN
Simply Better Connections
CC Authentication Key License Upgrade
> Login
Login:
Username:
Password:
Submit
ATEN.com is published by ATEN International Co. Ltd., Taiwan. All rights reserved.

Username: myname3
Password: ••••••••••••••••••••••••••

3. In the screen that comes up, key in the Order ID number and Order Authorization number that applies to the upgrade, then click **Continue**.



CC Authentication Key License Upgrade

> User Information

User Information

- Login Name: myname3
- Phone: 111-123-456788
- FAX: 111-123-456789
- E-mail: myname3@mycompany3.com

Order Information

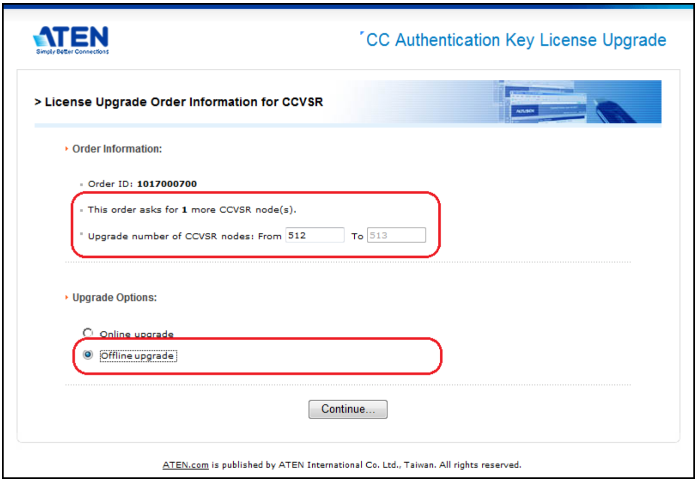
- Order ID: 1017000750
- Order Authorized Number: 1605991978

ATEN.com is published by ATEN International Co. Ltd., Taiwan. All rights reserved.

4. When the License Upgrade Order Information screen comes up, key in the number of current licenses in the *From* fields. The *To* fields are automatically filled in.

Note: If necessary, you can use the Key Status Utility (CCAuthKeyStatus.exe) to see the number of current licenses.

5. Select that this is to be an Offline upgrade, then click **Continue**.



CC Authentication Key License Upgrade

> License Upgrade Order Information for CCVSR

Order Information:

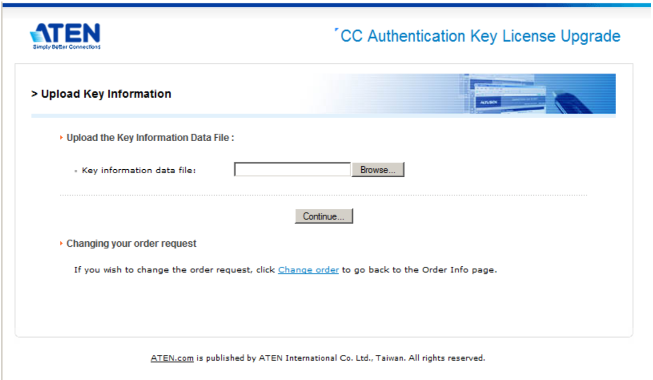
- Order ID: **1017000700**
- This order asks for **1** more CCVSR node(s).
- Upgrade number of CCVSR nodes: From 512 To 513

Upgrade Options:

○ Online upgrade
● Offline upgrade

ATEN.com is published by ATEN International Co. Ltd., Taiwan. All rights reserved.

6. When the Upload Key Information screen comes up, click **Browse**; load the **KeyUpload.dat** file that was generated in the *Preliminary Steps* section; then click **Continue**.



ATEN Simply Better Connections

CC Authentication Key License Upgrade

> Upload Key Information

- Upload the Key Information Data File :
  - Key information data file: [ ] Browse...

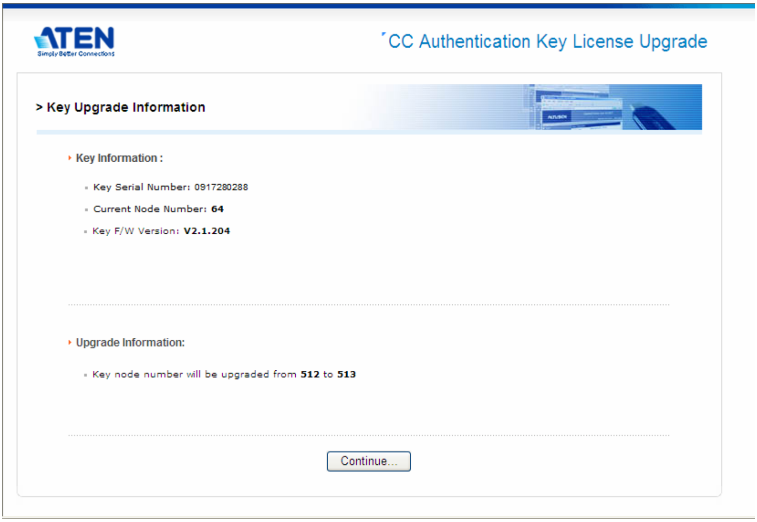
Continue...

- Changing your order request

If you wish to change the order request, click Change order to go back to the Order Info page.

ATEN.com is published by ATEN International Co. Ltd., Taiwan. All rights reserved.

7. The next screen that comes up summarizes the transaction up to this point.



ATEN Simply Better Connections

CC Authentication Key License Upgrade

> Key Upgrade Information

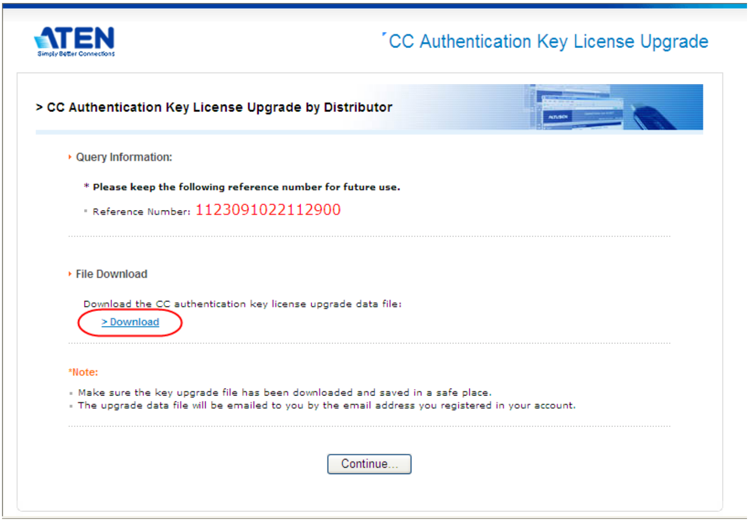
- Key Information :
  - Key Serial Number: 0917280288
  - Current Node Number: **64**
  - Key F/W Version: **V2.1.204**

- Upgrade Information:
  - Key node number will be upgraded from **512** to **513**

Continue...

Click **Continue** to move on.

8. In the screen that appears next, click **Download** to download the key license upgrade data file (KeyUpgrade.dat).



ATEN
Simply Better Connections
CC Authentication Key License Upgrade

> CC Authentication Key License Upgrade by Distributor

Query Information:

* Please keep the following reference number for future use.

Reference Number: 1123091022112900

File Download

Download the CC authentication key license upgrade data file:

> Download

*Note:

- Make sure the key upgrade file has been downloaded and saved in a safe place.
- The upgrade data file will be emailed to you by the email address you registered in your account.

9. When the browser asks what to do with the key upgrade file, select *Save to disk*. After the file is saved to disk, click **Continue** to go on.

10. In the confirmation popup that appears click **Yes**. A summary page confirming the order appears.

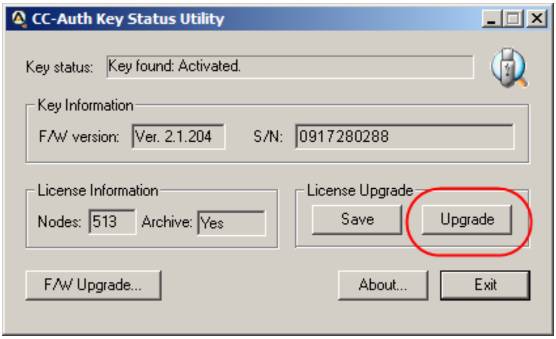
11. Click **Logout** to exit.

Note: 1. If you are upgrading more than one key, you can rename the KeyUpgrade.dat files to separately recognizable names (keeping the *dat* extension).

2. If the client is performing the upgrade, the dealer/distributor provides the KeyUpgrade.dat file to the client.

12. Run the *Key Status Utility* again.

13. In the License Upgrade panel, click **Upgrade**.



Key status: Key found: Activated.

F/W version: Ver. 2.1.204

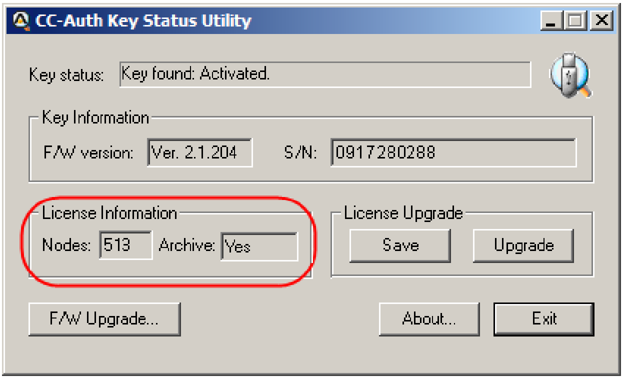
S/N: 0917280288

Nodes: 513

Archive: Yes

14. In the dialog box that comes up, navigate to the upgrade file (KeyUpgrade.dat) and select it.

- Once you click **Open**, a window pops up stating that the upgrade was successful.
- The figure for the number of licenses in the License Information panel changes to reflect the upgrade.



Key status: Key found: Activated.

F/W version: Ver. 2.1.204

S/N: 0917280288

Nodes: 513

Archive: Yes

Offline Upgrade Failure

If the offline upgrade fails, it may be due to the key upgrade file (KeyUpgrade.dat), having become corrupted during the file transfer process. There are two ways to proceed:

- When the key upgrade file is downloaded, an email is sent to the dealer/distributor containing the particulars, along with a copy of the upgrade file in case there was a problem with the original file transfer – as shown in the example below:

```
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 CC-
Authentication key's license, please confirm it online
at http://xxx.xxx.x.xxx using the username and
password above.
```

  You can repeat steps 11 (Run the Key Status Utility) and 12 (Click Upgrade) – this time using the copy of the key upgrade file (KeyUpgrade.dat) that was attached in the dealer/distributor email.

- If the above fails to resolve the problem, information contained in the *Offline email upgrade response* can be used to try an online upgrade. Either the dealer/distributor can provide the end user with the authorization details, or the end user can give his key to the dealer/distributor.

Order Expiration

Once Altusen sends the dealer/distributor the confirmation/authorization email informing him that the order is ready to be processed, he has a total of two weeks to process the order. If during that time the order is not processed, two more emails reminding him that order has not been processed are sent:

1. Your order will expire in one week...
2. Your order will expire in one day...

If the order still has not been processed by the end of the deadline, a final email is sent, informing the dealer/distributor that the order has expired, as follows:

> Your order has expired and has been canceled...
> If you still wish to add licenses, you must place a new order.

Limited Warranty

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

What is covered by the Limited Hardware Warranty

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

To learn more about our warranty policies, please visit our website:

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

Released: 2022-01-13