User Information

Online Registration

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

| International | http://eservice.aten.com |

Telephone Support

For telephone support, call this number:

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

User Notice

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

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

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

Basic Package

The Video Session Recording Software package consists of:

1 Video Session Recording Software USB License Key
1 Software CD
1 User Instructions*

Check to make sure that all of the components are present and in good order. If anything is missing, or was damaged in shipping, contact your dealer.

Read this manual thoroughly and follow the installation and operation procedures carefully to prevent any damage to the switch or to any other devices on the Video Session Recording Software installation.

* Features may have been added to the Video Session Recording Software since this manual was published. Please visit our website to download the most up-to-date version.
Contents

User Information .................................................. ii
Online Registration ........................................ ii
Telephone Support ........................................ ii
User Notice ................................................ ii
Package Contents ........................................ iii
Basic Package ........................................ iii
Contents ................................................ iv
About This Manual ........................................ viii
Conventions ........................................ ix
Product Information ........................................ ix

Chapter 1. Introduction
Overview ......................................................... 1
Features ......................................................... 4
Requirements ................................................. 4
Computer ......................................................... 4
KVM over IP Switch ........................................ 4
Browsers ......................................................... 5
Bandwidth Requirement ..................................... 5
An Example of CCVSR Deployment ......................... 6
Primary Servers ............................................. 6
Secondary Servers .......................................... 6
Archive Servers ............................................. 7
Nodes ........................................................... 7
Licenses ........................................................ 8
License Options ............................................. 8
Node Options ............................................... 9
Archive Server Options .................................... 9

Chapter 2. CCVSR Installation
Overview ......................................................... 11
Installing the CCVSR Software .............................. 11
Starting the Installation ..................................... 11
Licenses ........................................................ 13

Chapter 3. The User Interface
Overview ......................................................... 15
Browser Login ............................................... 15
The Web Browser Main Page ............................... 16
Page Components .......................................... 16
Main Menu ................................................... 18
Personal Info / Configuration ............................ 18
Personal Configuration ................................... 19
Preference .................................................... 19
Change Password .......................................... 19
Password Policy ............................................. 47
Group .............................................................. 48
Creating Groups .............................................. 48
Modifying Groups ........................................... 49
Deleting Groups .............................................. 49
Authentication ............................................... 50
AD / LDAP Settings ......................................... 50
RADIUS Settings ............................................. 51

Chapter 8. System
Overview .................................................. 53
Server Info ................................................... 54
Server Information ......................................... 54
Server Port Settings ....................................... 55
Archive Server Settings ................................. 55
Server Type .................................................. 56
Misc .............................................................. 57
Notification ................................................... 58
SMTP .............................................................. 58
SNMP Server .................................................. 59
Syslog Server .................................................. 60
Advanced (Notification) ................................. 61
Security ......................................................... 62
Access Protection .......................................... 62
IP / MAC Filtering .......................................... 62
Lockout Policy .............................................. 63
Login String ................................................... 64
Certificate ..................................................... 65
Private Certificate .......................................... 65
Certificate Signing Request ............................. 67
License .......................................................... 69
Upgrading the License ..................................... 69
Backup & Restore ............................................ 71
Backup .......................................................... 71
Restore .......................................................... 71
Recording ....................................................... 73
Adding Secondary CCVSR Servers ...................... 74
Adding Shared Network Folder ......................... 75
Editing Secondary CCVSR Servers ...................... 76
Editing Shared Network Folder ......................... 77
Deleting Secondary CCVSR Servers/Shared Network Folder ......................... 77
Option - Retention Policy ............................... 77

Chapter 9. Logs
Overview ................................................... 79
Log Information ............................................. 80
Export Logs ................................................... 80
### Chapter 10. CCVSR Archive Server

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>85</td>
</tr>
<tr>
<td>Installing the CCVSR Archive Server</td>
<td>85</td>
</tr>
<tr>
<td>Starting the Installation</td>
<td>85</td>
</tr>
<tr>
<td>Archive Server GUI</td>
<td>89</td>
</tr>
<tr>
<td>Setup</td>
<td>89</td>
</tr>
<tr>
<td>Playback</td>
<td>90</td>
</tr>
<tr>
<td>Begin Time/End Time</td>
<td>90</td>
</tr>
<tr>
<td>Search Filter</td>
<td>90</td>
</tr>
<tr>
<td>Play Selected</td>
<td>91</td>
</tr>
<tr>
<td>Export/Import</td>
<td>92</td>
</tr>
<tr>
<td>Begin Time/End Time</td>
<td>92</td>
</tr>
<tr>
<td>Device Name</td>
<td>92</td>
</tr>
<tr>
<td>Search File</td>
<td>93</td>
</tr>
<tr>
<td>Export File</td>
<td>93</td>
</tr>
<tr>
<td>Export &amp; Delete</td>
<td>93</td>
</tr>
<tr>
<td>Delete File</td>
<td>93</td>
</tr>
<tr>
<td>Import File</td>
<td>93</td>
</tr>
<tr>
<td>Storage</td>
<td>94</td>
</tr>
<tr>
<td>Settings</td>
<td>95</td>
</tr>
<tr>
<td>License</td>
<td>96</td>
</tr>
</tbody>
</table>

### Appendix

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Support</td>
<td>97</td>
</tr>
<tr>
<td>International</td>
<td>97</td>
</tr>
<tr>
<td>North America</td>
<td>97</td>
</tr>
<tr>
<td>USB Authentication Key Specifications</td>
<td>98</td>
</tr>
<tr>
<td>Compatible Products</td>
<td>98</td>
</tr>
<tr>
<td>Linux Installation</td>
<td>99</td>
</tr>
<tr>
<td>Trusted Certificates</td>
<td>100</td>
</tr>
<tr>
<td>Overview</td>
<td>100</td>
</tr>
<tr>
<td>Self-Signed Private Certificates</td>
<td>101</td>
</tr>
<tr>
<td>Examples</td>
<td>101</td>
</tr>
<tr>
<td>Importing the Files</td>
<td>101</td>
</tr>
<tr>
<td>Limited Warranty</td>
<td>102</td>
</tr>
</tbody>
</table>
About This Manual

This User Manual is provided to help you get the most from your Video Log Server system. It covers all aspects of 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 application. Its purpose, features, benefits, and requirements are 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 login to the Video Session Recording Software using a web browser.

Chapter 4, Playback, explains how to use the features and functions of the Playback page, used to search and play video log files.

Chapter 5, Liveview explains the centralized liveview, including displaying only the favorite devices/ports, more playback options, single port mode, etc..

Chapter 6, Device Management, shows super administrators how to add KVM devices and configure ports on the Video Session Recording Software, in order to record video logs.

Chapter 7, User Accounts, shows super administrators and administrators how to create, modify, and delete users and groups, assign attributes to them and authentication settings.

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

Chapter 9, Logs, shows how to use the log file utilities to view the events that take place on the Video Session Recording Software.

Chapter 10, CCVSR Archive Server, describes how to use the CCVSR Archive Server, and explains it’s features and function.

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

This manual uses the following conventions:

Monospaced Indicates text that you should key in.

[ ] Indicates keys you should press. For example, [Enter] means to press the Enter key. If keys need to be chorded, they appear together in the same bracket with a plus sign between them: [Ctrl+Alt].

1. Numbered lists represent procedures with sequential steps.

• Bullet lists provide information, but do not involve sequential steps.

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

⚠ Indicates critical information.

Product Information

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

<table>
<thead>
<tr>
<th></th>
<th><a href="http://www.aten.com">http://www.aten.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>International</td>
<td></td>
</tr>
<tr>
<td>North America</td>
<td><a href="http://www.aten-usa.com">http://www.aten-usa.com</a></td>
</tr>
</tbody>
</table>
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 and remotely through KVM over IP switch and/or serial console servers. Whatever the target server’s operating status is, whether it’d be 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.

No agent software installation required on target computers, the CCVSR is installed and operated independently as a server. It therefore does not require CPU resources, disk space, memory and network bandwidth of all target computers. 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 a brand new 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.
Chapter 1. Introduction

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 Video Session Recording Software will be installed on should meet the following requirements:

- **Server Hardware Requirements**
  - CPU: Intel Xeon D-1527 4 cores 2.2GHz or equivalent
  - Memory: 8GB or more
  - Hard drive (for CCVSR): 4GB or more
  - Network: 1Gbps

- **Client Hardware Requirements**
  - CPU: Intel Core i5-7600 4 cores 3.5GHz or equivalent
  - Memory: 6GB or more
  - Network: 1Gbps

- **Operating System Requirements:**
  - Windows: 10, 8, 7
  - Linux:

<table>
<thead>
<tr>
<th>OS</th>
<th>Version</th>
<th>Type</th>
<th>Kernel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ubuntu</td>
<td>16.04</td>
<td>X86</td>
<td>4.10.0-28</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>16.04</td>
<td>X64</td>
<td>4.8.0-36</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>18.04</td>
<td>X64</td>
<td>4.19</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux</td>
<td>7</td>
<td>X64</td>
<td>3.10.0</td>
</tr>
<tr>
<td>CentOS</td>
<td>7.4</td>
<td>X64</td>
<td>3.10.0-693</td>
</tr>
<tr>
<td>CentOS</td>
<td>7.5</td>
<td>X64</td>
<td>4.18.11-1</td>
</tr>
<tr>
<td>Debian</td>
<td>8.8</td>
<td>X64</td>
<td>3.16.0-4</td>
</tr>
<tr>
<td>Fedora</td>
<td>24</td>
<td>X32</td>
<td>4.5.5-200</td>
</tr>
<tr>
<td>Fedora</td>
<td>24</td>
<td>X64</td>
<td>4.5.5-200</td>
</tr>
<tr>
<td>OpenSUSE</td>
<td>13.2</td>
<td>X32</td>
<td>3.16.6</td>
</tr>
<tr>
<td>OpenSUSE</td>
<td>13.2</td>
<td>X64</td>
<td>3.16.6</td>
</tr>
</tbody>
</table>

**KVM over IP Switch**
Computers recorded by the Video Session Recorder must be connected to a port on a KVM over IP Switch* (refer to the “Specification” tab of the CCVSR page on the ATEN website).
Note: Computers connected to cascade-compatible KVM switches are not supported.

Browsers

Supported browsers for users that log into the Video Session Recording Software include the following:

<table>
<thead>
<tr>
<th>Browser</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Edge</td>
<td>44.18362.449 or later</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>11.0.9600 or later</td>
</tr>
<tr>
<td>Chrome</td>
<td>69.0.3497.100 or later</td>
</tr>
<tr>
<td>Firefox</td>
<td>62.0.3 or later</td>
</tr>
</tbody>
</table>

Bandwidth Requirement

1920x1080, Text Mode = On, 1G Bandwidth

<table>
<thead>
<tr>
<th></th>
<th>General Operations (e.g. settings configuration, file editing, etc.)</th>
<th>Surveillance (e.g. NVR, playing videos, etc.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>KN8164V</td>
<td>3.37 Mbps/Channel</td>
<td>44.6 Mbps/Channel</td>
</tr>
<tr>
<td></td>
<td>1 hour video size: 296MB</td>
<td>1 hour video size: 4GB</td>
</tr>
<tr>
<td>CN8000A</td>
<td>12.40 Mbps/Channel</td>
<td>32.4 Mbps/Channel</td>
</tr>
<tr>
<td></td>
<td>1 hour video size: 599MB</td>
<td>1 hour video size: 1.7GB</td>
</tr>
</tbody>
</table>

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. Your computer’s CPU resource will be used when the system further compresses the recorded videos. The CPU resource will be released when the compression is complete.
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.

<table>
<thead>
<tr>
<th>Functions</th>
<th>Primary</th>
<th>Secondary (Storage)</th>
<th>Secondary (Redundancy)</th>
<th>Archive</th>
</tr>
</thead>
<tbody>
<tr>
<td>System management</td>
<td>✓</td>
<td></td>
<td>view-only</td>
<td></td>
</tr>
<tr>
<td>Device management</td>
<td>✓</td>
<td></td>
<td>view-only</td>
<td></td>
</tr>
<tr>
<td>User management</td>
<td>✓</td>
<td></td>
<td>view-only</td>
<td></td>
</tr>
<tr>
<td>Local management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Video &amp; keystroke recording</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Video search &amp; playback</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Backup video &amp; keystrokes</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
Chapter 1. Introduction

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 allows 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 69, for more information.

<table>
<thead>
<tr>
<th>License</th>
<th>Nodes</th>
<th>Primary Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCVSR8</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>CCVSR16</td>
<td>16</td>
<td>1</td>
</tr>
<tr>
<td>CCVSR32</td>
<td>32</td>
<td>1</td>
</tr>
<tr>
<td>CCVSR64</td>
<td>64</td>
<td>1</td>
</tr>
<tr>
<td>CCVSR128</td>
<td>128</td>
<td>1</td>
</tr>
<tr>
<td>CCVSR256</td>
<td>256</td>
<td>1</td>
</tr>
<tr>
<td>CCVSR512</td>
<td>512</td>
<td>1</td>
</tr>
<tr>
<td>CCVSR1024</td>
<td>1024</td>
<td>1</td>
</tr>
<tr>
<td>CCVSR2048</td>
<td>2048</td>
<td>1</td>
</tr>
</tbody>
</table>
### Node Options

<table>
<thead>
<tr>
<th>License</th>
<th>Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCVSRN1</td>
<td>1</td>
</tr>
<tr>
<td>CCVSRN8</td>
<td>8</td>
</tr>
<tr>
<td>CCVSRN16</td>
<td>16</td>
</tr>
<tr>
<td>CCVSRN32</td>
<td>32</td>
</tr>
<tr>
<td>CCVSRN64</td>
<td>64</td>
</tr>
<tr>
<td>CCVSRN128</td>
<td>128</td>
</tr>
<tr>
<td>CCVSRN256</td>
<td>256</td>
</tr>
<tr>
<td>CCVSRN512</td>
<td>512</td>
</tr>
<tr>
<td>CCVSRN1024</td>
<td>1024</td>
</tr>
<tr>
<td>CCVSRN2048</td>
<td>2048</td>
</tr>
</tbody>
</table>

### Archive Server Options

<table>
<thead>
<tr>
<th>License</th>
<th>Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCVSRAS1</td>
<td>1</td>
</tr>
</tbody>
</table>
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 99.

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:

   ![Installer Screen](image)

   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.

![Select Installation Folder](image)

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

![Confirm Installation](image)
5. When the installation is complete the following message will appear:

![Image showing Installation Complete message]

**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 69, for details. For License options See *Node Options*, page 9, for details.
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 100).

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

   ![Login Page]

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:

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:

<table>
<thead>
<tr>
<th>No.</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Expand / Collapse Main Menu</td>
<td>Click this icon to expand or collapse main menu. The sub-menu can be accessed by clicking on their main operation categories.</td>
</tr>
<tr>
<td>2</td>
<td>Main Menu</td>
<td>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.</td>
</tr>
</tbody>
</table>
Chapter 3. The User Interface

<table>
<thead>
<tr>
<th>No.</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Expand / Collapse Sub-Menu</td>
<td>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.</td>
</tr>
<tr>
<td>4</td>
<td>Notification / Message Center (Super Administrator only)</td>
<td>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. 🔄 Click CLEAR ALL to clear the notifications / messages. Click VIEW LOGS to go to the system logs page.</td>
</tr>
</tbody>
</table>
| 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:

<table>
<thead>
<tr>
<th>Operation Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Playback</td>
<td>The Playback page is used to search and playback available video logs, and to monitor current browser sessions. Playback is discussed on page 21.</td>
</tr>
<tr>
<td>Liveview</td>
<td>The Liveview page allows the users to view live KVM ports feed. Liveview is discussed on page 29.</td>
</tr>
<tr>
<td>Device Management</td>
<td>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 35.</td>
</tr>
<tr>
<td>User Accounts</td>
<td>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 41.</td>
</tr>
<tr>
<td>System</td>
<td>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 53.</td>
</tr>
<tr>
<td>Log</td>
<td>The Log page displays the contents of the log file. The Log page is discussed on page 79.</td>
</tr>
</tbody>
</table>

Personal Info / Configuration

On the top right-hand corner of the page, you can click the Personal icon (👤) for personal information and configurations:
• 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 to log out of the current session of this user.

Personal Configuration

Preference

Click Preference for the pop-up window shown below:

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:
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 36 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.

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.

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:

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.

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:

![VSR Viewer screenshot](image)

Note:  
- The VSR Viewer is a Java-based application that requires JRE 8 or later 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.
Chapter 4. Playback

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:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Play" /></td>
<td><strong>Play:</strong> The Play button is used to resume playback of a video log that has been paused.</td>
</tr>
<tr>
<td><img src="image" alt="Pause" /></td>
<td><strong>Pause:</strong> The Pause button is used to stop playback of a video log that is being played.</td>
</tr>
<tr>
<td><img src="image" alt="Faster" /></td>
<td><strong>Faster:</strong> 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.</td>
</tr>
<tr>
<td><img src="image" alt="Slower" /></td>
<td><strong>Slower:</strong> 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.</td>
</tr>
<tr>
<td><img src="image" alt="Volume" /></td>
<td><strong>Volume:</strong> Use the volume bar to adjust the volume. Click the speaker icon to mute/unmute the video.</td>
</tr>
<tr>
<td><img src="image" alt="Progress Bar" /></td>
<td><strong>Progress Bar:</strong> 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.</td>
</tr>
<tr>
<td><img src="image" alt="Resize Window" /></td>
<td><strong>Resize Window:</strong> 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). <strong>Note:</strong> The entire window can be moved around the screen by holding a left click anywhere on the top window title bar.</td>
</tr>
</tbody>
</table>
Settings

Icon | Function
--- | ---

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.
Chapter 4. Playback

**Caption**

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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Full Screen Icon]</td>
<td><strong>Full Screen</strong>: This icon expands the Video Log Viewer window to fit the entire screen. To exit Full Screen mode, click the Full Screen icon again.</td>
</tr>
</tbody>
</table>

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

![Favorite Settings](image)

**Create Favorite**

1. To create a favorite, click the icon.

2. The system will ask you to change the name of the favorite:

![Create Favorite](image)

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:
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:

<table>
<thead>
<tr>
<th>No.</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Recorded time</td>
<td>This displays how long the port has been recorded for.</td>
</tr>
<tr>
<td>2</td>
<td>Resolution</td>
<td>This displays the resolution of the liveview.</td>
</tr>
<tr>
<td>3</td>
<td>Logged in Username</td>
<td>This displays the username of the user accessing the port. “Local console” is displayed when local console is accessed.</td>
</tr>
</tbody>
</table>
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:

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:
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.

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 the Log Server and enter the MAC Address and Service Port of the computer running the Video Session Recording Software, as shown below:

2. On the Device Management page, click the Add button. A pop-up window appears:

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 39.

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 the Log Server has been enabled and configured with the correct MAC Address.
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 button:

![KVM Device Editor](image)

Edit the options and click Save to save.

**Recording**

Click the Recording tab to edit recording options:

![Recording Options](image)

**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 and CN9600, enter a time 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 a 0 is entered here, CCVSR will record indefinitely.

**Delete KVM Devices**

To delete a KVM device, check the checkbox of the KVM device and click the 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:

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:

<table>
<thead>
<tr>
<th>User Type</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Access authorized ports and devices. Manage authorized ports and devices; configure personal working environment. <strong>Note:</strong> Users who have been given permission to do so, may also manage other users.</td>
</tr>
</tbody>
</table>

**Adding Users**

To add a user, and assign user permissions, 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>1 to 16 characters are allowed depending on the Account Policy settings. For security purposes, we recommend that you change this string occasionally., page 65.</td>
</tr>
<tr>
<td>Password</td>
<td>0 to 16 characters are allowed depending on the Account Policy settings (see Login &amp; Password Policy on page 47).</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>To make sure there is no mistake in the password. The two entries must match.</td>
</tr>
<tr>
<td>Description</td>
<td>Additional information about the user that you may wish to include.</td>
</tr>
<tr>
<td>User Type</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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 44) are automatically assigned by the system and cannot be altered.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Users who have been given User Account privileges cannot access or configure Groups.</td>
</tr>
</tbody>
</table>
3. If you selected the user to be a Super administrator, click a dd 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 48 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 29).
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 35).

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 79 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 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 42 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 .
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.

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.

<table>
<thead>
<tr>
<th>Login Policy</th>
<th>Entry</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Only one user may log into the same account at any given time</td>
<td>Check this to prevent users from logging in with the same account at the same time.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Password Policy</th>
<th>Entry</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Username Length</td>
<td>Sets the minimum number of characters required for a username. Acceptable values are from 1–16. The default is 6.</td>
<td></td>
</tr>
<tr>
<td>Minimum Password Length</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Password Must Contain At Least</td>
<td>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. <strong>Note:</strong> 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.</td>
<td></td>
</tr>
<tr>
<td>Enforce password history</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
**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 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A maximum of 16 characters is allowed.</td>
</tr>
<tr>
<td>Description</td>
<td>Additional information about the user that you may wish to include. A maximum of 63 characters is allowed.</td>
</tr>
</tbody>
</table>

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 29).
Chapter 7. User Accounts

- 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 35).
- 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 79 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 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 48 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 **Remove**.
Authentication

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

AD / LDAP Settings

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Check the Enable checkbox to allow AD / LDAP authentication and authorization.</td>
</tr>
<tr>
<td>LDAP Type</td>
<td>Click the drop-down menu to select Preferred or Alternate LDAP.</td>
</tr>
<tr>
<td>Server IP</td>
<td>Fill in the IP address, you can use the IPv4 address, the IPv6 address or the domain name in the LDAP Server field.</td>
</tr>
<tr>
<td>Port</td>
<td>Fill in the port number. Checking Server requires secure connection (SSL), the default port number is 636. Otherwise, the default port number is 389.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Set the time in seconds that the Video Log Server waits for a reply before it times out.</td>
</tr>
<tr>
<td>Admin DN</td>
<td>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</td>
</tr>
<tr>
<td>Admin Name</td>
<td>Key in the LDAP administrator’s username.</td>
</tr>
<tr>
<td>Password</td>
<td>Key in the LDAP administrator’s password.</td>
</tr>
<tr>
<td>Search DN</td>
<td>Set the distinguished name of the search base. This is the domain name where the search starts for user names.</td>
</tr>
</tbody>
</table>
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.
- 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**

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 42.)
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:

<table>
<thead>
<tr>
<th>Item</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the computer name of the server hosting the CCVSR application.</td>
</tr>
<tr>
<td>Description</td>
<td>Displays the description of the server. You may modify the information here.</td>
</tr>
<tr>
<td>Role</td>
<td>Displays the role of the server.</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>Displays the CCVSR’s IPv4 address.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>Displays the CCVSR’s IPv6 address.</td>
</tr>
<tr>
<td>Server MAC</td>
<td>Displays the MAC address of the computer hosting the CCVSR application.</td>
</tr>
</tbody>
</table>
Server Port Settings

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>The port number for a browser login. The default is 9080.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>The port number for a secure browser login. The default is 9443.</td>
</tr>
<tr>
<td>CCVSR</td>
<td>This is the port number for communication between a CCVSR Primary Server and Secondary Servers. The default is 9002.</td>
</tr>
</tbody>
</table>

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 85, 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 55.

The Secondary Server must be added to the Primary Server in order to work. See Recording, page 73, for details.

When you log in locally (http://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 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

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 61 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 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:

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.

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:
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 button. Configure as described in page 62.
To delete IP / MAC filtering, check an IP / IP range / MAC address and click the 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.

<table>
<thead>
<tr>
<th>Entry</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum login failures</td>
<td>Sets the number of consecutive failed login attempts that are permitted from a remote computer. The default is 5 times.</td>
</tr>
<tr>
<td>Timeout</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

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.

<table>
<thead>
<tr>
<th>Subject</th>
<th>DO NOT EDIT</th>
<th>Valid</th>
<th>Signature</th>
<th>Private Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issuer</td>
<td>DO NOT EDIT</td>
<td>Valid</td>
<td>Signature</td>
<td>Private Certificate</td>
</tr>
</tbody>
</table>

**Certificate Signing Request**

<table>
<thead>
<tr>
<th>Certificate</th>
<th>0 (0:0:0)</th>
</tr>
</thead>
</table>

**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 101 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:

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

<table>
<thead>
<tr>
<th>Information</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country (2 letter code)</td>
<td>TW</td>
</tr>
<tr>
<td>State or Province</td>
<td>Taiwan</td>
</tr>
<tr>
<td>Locality</td>
<td>Taipei</td>
</tr>
<tr>
<td>Organization</td>
<td>Your Company, Ltd.</td>
</tr>
<tr>
<td>Unit</td>
<td>Tech Department</td>
</tr>
<tr>
<td>Common Name</td>
<td>mycompany.com</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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 <a href="http://www.mycompany.com">www.mycompany.com</a>, and you only specify mycompany.com, the certificate will not be valid.</td>
</tr>
<tr>
<td>Email Address</td>
<td><a href="mailto:administrator@yourcompany.com">administrator@yourcompany.com</a></td>
</tr>
</tbody>
</table>

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 License tab is used to upgrade your software and add server licenses.

![License Key Image]

Upgrading the License

The license controls the total number of purchased Nodes, used and available Nodes permitted with your Video Session Recording Software installation. The license information is contained on the USB License Key that came with your purchase.

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

To upgrade the license:

1. Use the USB key that came with your package or contact your dealer to obtain a new license key for the number of primary and/or secondary servers you want to add.
2. Insert the license key into a USB port on your Video Session Recording Software.
3. Login to the CCVSR application, and from the License tab click Read License Key.

You can now install and use additional CCVSRs (per the number of licenses purchased), which will communicate and work in conjunction over a network.

Note: 1. Once the upgrade has completed, it is no longer necessary to keep the 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.
Chapter 8. System

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

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

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.
Chapter 8. System

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 56 for details. When you select Recording, the following screen appears:

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:

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

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:

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP/Name</td>
<td>Enter the IP address of the server sharing the network folder.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter a username with permission to access the shared network folder.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a password.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recording Path</td>
<td>Enter the folder location of the server where you want to save the video log files. Example: Share\Department2\Security\VideoLogs</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the network folder.</td>
</tr>
</tbody>
</table>
5. Click *Next* for the *Recording* tab:

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:

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.
Chapter 8. System

**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:

![Editing Shared Network Folder](image)

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.
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:
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:

Click Print for the print setup of your system or Close to leave this page.
Chapter 9. Logs

Option

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

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.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Keyword</strong></td>
<td>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<em>ds would return hands and hoods; h?nd would return hand and hind, but not hard; h</em>ds or h*ks would return hands and hooks.</td>
</tr>
</tbody>
</table>
| **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:  
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. |
This Page Intentionally Left Blank
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:

![Archive Server Setup Wizard](image)

---

85
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.

![Select Installation Folder](image)

Click **Next** to continue.

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

![Confirm Installation](image)
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**.

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**:

- **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:
Chapter 10. CCVSR Archive Server

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:

![Archive Server GUI Image]

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 55). Next, add a storage location from the Storage tab (see Storage, page 94). 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.

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* refer 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:

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 94).

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 92).
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.

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.

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 94). 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. 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 the following window appears:

2. Type in the Path or click Browse to select a storage location.

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:

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**.

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

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

<table>
<thead>
<tr>
<th>Email Support</th>
<th><a href="mailto:support@aten-usa.com">support@aten-usa.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Technical Support</td>
<td>Troubleshooting Documentation Software Updates</td>
</tr>
<tr>
<td>Telephone Support</td>
<td>1-888-999-ATEN ext 4988</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Function</th>
<th>Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environment</td>
<td></td>
</tr>
<tr>
<td>Operating Temp.</td>
<td>0–40(^\circ) C</td>
</tr>
<tr>
<td>Storage Temp.</td>
<td>-20–60(^\circ) C</td>
</tr>
<tr>
<td>Humidity</td>
<td>0–80% RH, Non-condensing</td>
</tr>
<tr>
<td>Physical Properties</td>
<td></td>
</tr>
<tr>
<td>Composition</td>
<td>Metal and Plastic</td>
</tr>
<tr>
<td>Weight</td>
<td>14 g</td>
</tr>
<tr>
<td>Dimensions</td>
<td>8.36 x 2.77 x 1.37 cm</td>
</tr>
</tbody>
</table>

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 install command: > 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.

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:
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=yourlocationorcity/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 62, and Certificate, page 65).
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 defective, 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:
