



VioStor CMS

Central Management System

User Manual (Version: 1.0.1)

© 2013. QNAP Systems, Inc. All Rights Reserved.

Thank you for choosing the QNAP products! This user manual will introduce you how to use the VioStor Central Management System (CMS) server and client applications. Please follow the instructions in this user manual and start to enjoy the powerful VioStor CMS system.

Note:

- This user manual contains the instructions for using the QNAP CMS server and software. Some features are only available on specific models. The model you purchased may not support these features.
- The CMS hardware/server is hereafter referred to as the CMS Server, and the central management software is referred to as the CMS Client.
- This user manual (version 1.0.1) is only applicable for the CMS Client version 1.0.1.
- In order to support the full functions of CMS Client version 1.0.1, please use the VioStor NVR firmware version 4.1.0 or later versions.

Legal Notice

All the features, functionality, and other product specifications are subject to change without prior notice or obligation. Information contained herein is subject to change without notice.

QNAP and the QNAP logo are trademarks of QNAP Systems, Inc. All other brands and product names referred to are trademarks of their respective holders. Further, the ® or ™ symbols are not used in the text.

Limited Warranty

In no event shall the liability of QNAP Systems, Inc. (QNAP) exceed the price paid for the product from direct, indirect, special, incidental, or consequential damages resulting from the use of the product, its accompanying software, or its documentation. QNAP makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. QNAP reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity.

Note:

- Back up the system periodically to avoid any potential data loss. QNAP disclaims any responsibility of all sorts of data loss or recovery.
- Should you return any components of the product package for refund or maintenance, make sure they are carefully packed for shipping. Any form of damages due to improper packaging will not be compensated.
- Please read the safety warnings and user manual carefully before using this product.
- This product can only be used with the power supply provided by the manufacturer.
- Please contact qualified technicians for any technical enquires. Do not repair this product by yourself to avoid any voltage danger and other risks caused by opening this product cover.
- To avoid fire or electric shock, do not use this product in rain or humid environment. Do not place any objects on this product.

Regulatory Notice



FCC Notice

The QNAP products comply with different FCC compliance classes. Please refer the Appendix for details. Once the class of the device is determined, refer to the following corresponding statement.

=====

FCC Class B Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/television technician for help.

Modifications: Any modifications made to this device not approved by QNAP Systems, Inc.

may void the authority granted to the user by the FCC to operate this equipment.



Class B only.

Symbols in this document




 Warning	This icon indicates the instructions must be strictly followed. Failure to do so could result in injury to human body or death.
 Caution	This icon indicates the action may lead to disk clearance or loss OR failure to follow the instructions could result in data damage, disk damage, or product damage.
 Important	This icon indicates the information provided is important or related to legal regulations.

Table of Contents

TABLE OF CONTENTS.....	7
SAFETY WARNING.....	10
CHAPTER 1 INTRODUCTION.....	11
1.1 OVERVIEW	11
1.2 HARDWARE ILLUSTRATION	12
1.3 HARDWARE SPECIFICATION	14
CHAPTER 2 INSTALLING CMS SERVER.....	16
2.1 BROWSING CD-ROM	16
2.2 HARD DISK DRIVE COMPATIBILITY LIST	17
2.3 IP CAMERA COMPATIBILITY LIST	17
2.4 CHECKING SYSTEM STATUS.....	18
2.5 SYSTEM CONFIGURATION	20
CHAPTER 3 INSTALLING CMS CLIENT.....	25
3.1 SUGGESTED PC SPECIFICATION FOR CMS CLIENT	25
3.2 INSTALLING CMS CLIENT	26
3.3 CONNECTING CMS CLIENT TO CMS SERVER.....	28
3.4 QUICK CONFIGURATION WIZARD	30
3.5 CONFIGURING CMS CLIENT	37
3.6 LICENSE.....	40
3.7 ACTIVATING LICENSE ONLINE	41
3.7.1 ACTIVATING LICENSE OFFLINE.....	42
3.7.2 TRANSFERRING/DELETING AUTHORIZATION	46
3.8 SERVER.....	50
3.8.1 ADDING NVR	51
3.8.2 DELETING/EDITING NVR.....	55
3.8.3 ADDING/REMOVING CAMERA.....	56
3.8.4 FIRMWARE UPDATE.....	56
3.8.5 TCP/IP CONFIGURATION	58
3.8.6 SYSTEM TIME	63
3.8.7 ALERT NOTIFICATION	63
3.8.8 SMSC SETTINGS	64
3.9 CAMERA	66
3.10 EVENT MANAGEMENT.....	69
3.11 VIEW	71
3.12 E-MAP	77

3.12.1	ADDING E-MAP.....	80
3.12.2	EDITING AN E-MAP NAME	83
3.12.3	DELETING E-MAP.....	83
3.12.4	EDITING IP CAMERA ON E-MAP	84
3.13	USER MANAGEMENT	85
3.13.1	ROLE MANAGEMENT	86
3.13.2	GROUP MANAGEMENT.....	100
3.13.3	USER LIST.....	106
3.14	CMS SERVER SETTINGS	107
3.14.1	DOMAIN SECURITY	107
3.15	LIVE VIEW.....	111
3.15.1	LIVE VIEW PAGE.....	117
3.15.2	BOOKMARK.....	120
3.15.3	PTZ CAMERA CONTROL	123
3.15.4	AUTO CRUISING.....	124
3.15.5	ALARM MODE (ALARM LIST & EVENT LOGS)	128
3.15.6	E-MAP.....	130
3.15.7	MULTI-MONITOR MODE	133
3.16	PLAYBACK.....	135
3.16.1	VIDEO PLAYBACK PAGE.....	135
3.16.2	MULTI-VIEW PLAYBACK.....	143
3.16.3	EXPORTING VIDEO FILE.....	146
CHAPTER 4	SERVER LOG.....	149
4.1	EVENT LOG	149
4.2	SERVICE LOG.....	150
4.3	SYSTEM LOG	151
4.4	NVR EVENT LOG	152
4.5	ONLINE USER	153
CHAPTER 5	CMS SERVER MANAGEMENT.....	154
5.1	GENERAL SETTING	154
5.1.1	SYSTEM ADMINISTRATION.....	154
5.1.2	DATE AND TIME.....	154
5.1.3	DAYLIGHT SAVING TIME.....	156
5.1.4	LANGUAGE	157
5.1.5	PASSWORD STRENGTH.....	157
5.2	NETWORK SETTING	158
5.2.1	TCP/IP.....	158

5.2.2	DDNS	160
5.2.3	IPv6	162
5.3	POWER MANAGEMENT	164
5.4	BACKUP/RESTORE SETTINGS	165
5.5	SYSTEM LOG	166
5.5.1	SYSTEM EVENT LOG	166
5.5.2	SYSTEM CONNECTION LOG	166
5.5.3	ON-LINE USER	167
5.6	FIRMWARE UPDATE	167
5.6.1	UPDATE FIRMWARE BY WEB ADMINISTRATION PAGE	167
5.6.2	UPDATE FIRMWARE BY QNAP FINDER	169
5.7	RESTORING TO FACTORY DEFAULT	171
5.8	DISK MANAGEMENT	171
5.8.1	VOLUME MANAGEMENT	171
5.8.2	RAID MANAGEMENT	174
5.8.3	HDD SMART	176
5.8.4	ENCRYPTED FILE SYSTEM	176
5.9	SYSTEM STATUS	179
5.9.1	SYSTEM INFORMATION	179
5.9.2	RESOURCE MONITOR	179
CHAPTER 6	TROUBLESHOOTING	183
TECHNICAL SUPPORT		191
GNU - GENERAL PUBLIC LICENSE		192

Safety Warning

1. This product can operate normally in the temperature of 0°C–40°C and relative humidity of 0%–90%. Please make sure the environment is well-ventilated.
2. The power cord and devices connected to this product must provide correct supply voltage.
3. Do not place this product in direct sunlight or near chemicals. Make sure the temperature and humidity of the environment are in optimized level.
4. Unplug the power cord and all connected cables before cleaning. Wipe this product with a wet towel. Do not use chemical or aerosol to clean this product.
5. Do not place any objects on this product for the server's normal operation and to avoid overheat.
6. Use the flat head screws in the product package to lock the hard disks in this product when installing hard disks for proper operation.
7. Do not place this product near any liquid.
8. Do not place this product on any uneven surface to avoid falling off and damage.
9. Make sure the voltage is correct in your location when using this product. If you are not sure about the voltage, please contact the distributor or the local power supply company.
10. Do not place any object on the power cord.
11. Do not attempt to repair this product in any occasions. Improper disassembly of the product may expose you to electric shock or other risks. For any enquiries, please contact the distributor.
12. The chassis models should only be installed in the server room and maintained by the authorized server manager or IT administrator. The server room is locked by key or keycard access and only certified staff is allowed to enter the server room.



Warning:

- Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.
- Do NOT touch the fan inside the system to avoid serious injuries.

Chapter 1 Introduction

1.1 Overview

The QNAP Central Management System (CMS) is a high performance turnkey solution for large-scale and multiple-site surveillance projects. The CMS Client is a software utility designed to manage the QNAP VioStor network video recorders (NVR) and perform live video monitoring, recording, and playback. The CMS Server supports up to a maximum of 128 multi-server monitoring. Users can monitor up to a maximum of 1024 IP cameras, up to a maximum of 64 channels per screen. Concurrent independent playbacks and display controls in four screens are also supported. The CMS Server has the highest compatibility with the QNAP VioStor NVR series and also supports a variety of brand name IP cameras. For detailed compatibility list, please refer to:

http://www.qnapsecurity.com/pro_compatibility_camera.asp

1.2 Hardware Illustration

CMS-2000:



1. One Touch Copy button
2. USB 2.0 (reserved)
3. LED indicators: HDD1, HDD2, LAN, eSATA
4. Power button
5. Power connector
6. Gigabit LAN x 2
7. USB 2.0 x 2 (reserved)
8. Password & network settings reset button
9. K-Lock security slot
10. eSATA(reserved)
11. USB 3.0 x 2 (reserved)

CMS-4000U-RP:



1. USB 2.0 (reserved)
2. One Touch Copy button
3. LED indicators: HDD1-4, LAN, eSATA
4. Power button
5. Password & network settings reset button
6. Gigabit LAN x 2
7. USB 2.0 x 4 (reserved)
8. USB 3.0 x 2 (reserved)
9. eSATA (reserved)
10. Power Connector

1.3 Hardware Specification

CMS-2000:

Model Name	CMS-2000
Number of License	Base: 64, Maximum:1,024
HDD	2 x 3.5" or 2.5" SATA (Hot-swappable and lockable tray)
CPU	Intel 2.13GHz dual-core processor
RAM	1GB
Operating System	Linux Embedded
Ethernet Port	Gigabit Rj-45 Ethernet port x 2
Dimensions	150 (H) x 102 (W) x 216 (D) mm 5.91 (H) x 4.02 (W) x 8.5 (D) inch
Net Weight	1.74 Kg (3.84 lb)
Gross weight	2.92 Kg (6.44 lb)
Temperature	0-40 °C
Relative Humidity	0-95 % R.H.
Power Supply	Input: 100-240V AC, 50/60 Hz Output: 90W

CMS-4000U-RP:

Model Name	CMS-4000U-RP
Number of License	Base: 64, Maximum:1,024
HDD	4 x 3.5" or 2.5" SATA (Hot-swappable and lockable tray)
CPU	Intel 2.13GHz dual-core processor
RAM	1GB
Operating System	Linux Embedded
Ethernet Port	Gigabit Rj-45 Ethernet port x 2
Dimensions	44 (H) x 439 (W) x 499 (D) mm 1.73 (H) x 17.28 (W) x 19.65 (D) inch
Net Weight	7.63 Kg (16.82 lb)
Gross weight	9.55 Kg (21.05 lb)
Temperature	0-40 °C
Relative Humidity	0-95 % R.H.
Power Supply	Input: 100-240V AC, 50/60 Hz Output: Redundant 250W

Chapter 2 Installing CMS Server

For details on product hardware installation, please refer to the "Quick Installation Guide" (QIG) in the product package.

2.1 Browsing CD-ROM

The CMS installation CD-ROM contains the Quick Start Guide, CMS Client, QNAP Finder, and the user manual.



Browse the CD-ROM and access the following contents:

- Finder: The setup program of the QNAP Finder (for Windows OS).
- CMS Client: The main program of the central management and monitoring system.
- Manual: The user manual of the QNAP VioStor CMS.

The above contents can also be downloaded at the QNAP Security website (<http://www.qnapsecurity.com>).

2.2 Hard Disk Drive Compatibility List

This product works with popular brands of 2.5-inch and 3.5-inch SATA hard disk drives.

For hard disk compatibility list, please visit the QNAP Security website:

http://www.qnapsecurity.com/pro_compatibility.asp

Note: QNAP disclaims any responsibility for product damage/malfunction or data loss/recovery due to misuse or improper installation of hard disks in any occasions for any reasons.

2.3 IP Camera Compatibility List

For information on supported IP Camera models, please visit the QNAP Security website:

http://www.qnapsecurity.com/pro_compatibility_camera.asp

2.4 Checking System Status

LED Display & System Status Overview

LED	Color	LED Status	Description
System Status	Red/ Green	Flashes green and red alternately every 0.5 sec	1) A hard drive on the system is being formatted/initialized. 2) The system firmware is being updated. 3) RAID rebuilding is in process. 4) Online RAID Capacity Expansion is in process. 5) Online RAID Level Migration is in process.
		Red	1) A hard drive is invalid. 2) The disk volume has reached its full capacity. 3) The disk volume is going to be full. 4) The system fan is out of function. 5) An error occurs when accessing (read/write) the disk data. 6) A bad sector is detected on the hard drive 7) The system is in degraded read-only mode (2 member drives fail in a RAID 5 or RAID 6 configuration, the disk data can still be read). 8) (Hardware self-test error).
		Flashes red every 0.5 sec	The system is in degraded mode (one member drive fails in RAID 1, RAID 5 or RAID 6 configuration).
		Flashes green every 0.5 sec	1) The system is starting up. 2) The system is not configured. 3) A hard drive is not formatted.
		Green	The system is ready.
		Off	All the hard drives on the system are in standby mode.
LAN	Orange	Orange	The system is connected to the network.
		Flashes orange	The system is being accessed from the network.
HDD (Hard Drive)	Red/ Green	Flashes red	The hard drive data is being accessed and a read/write error occurs during the process.
		Red	A hard drive read/write error occurs.
		Flashes green	The hard drive data is being accessed.
		Green	The hard drive can be accessed.

USB	Blue	Flashes blue every 0.5 sec	1) A USB device is detected. 2) A USB device is being removed from the system. 3) The USB device connected to the front USB port of the system is being accessed. 4) The system data is being copied to the external USB device.
		Blue	The USB device connected to the front USB port of the system is ready.
		Off	1) No USB is detected. 2) The system has finished copying the data to the USB device connected to the front USB port of the system.
eSATA†	Orange	Flashes	The eSATA device is being accessed.

Beep Alarm (beep alarm can be disabled in "System Tools" > "Hardware Settings")

Beep sound	No. of Times	Description
Short beep (0.5 sec)	1	1) The system is starting up. 2) The system is being shut down (software shutdown). 3) The reset button is pressed. 4) The system firmware has been updated.
Short beep (0.5 sec)	3	The system data cannot be copied to the external device by pressing the auto-backup button.
Short beep (0.5 sec), long beep (1.5 sec)	3, every 5 min	The system fan is out of function.
Long beep (1.5 sec)	2	1) The disk volume is going to be full. 2) The disk volume has reached its full capacity. 3) The hard drives on the system are in degraded mode. 4) Hard disk rebuilding process starts.
	1	1) The system is turned off by force shutdown (hardware shutdown). 2) The system has been turned on successfully and is ready.

2.5 System Configuration

Setting up the CMS Server

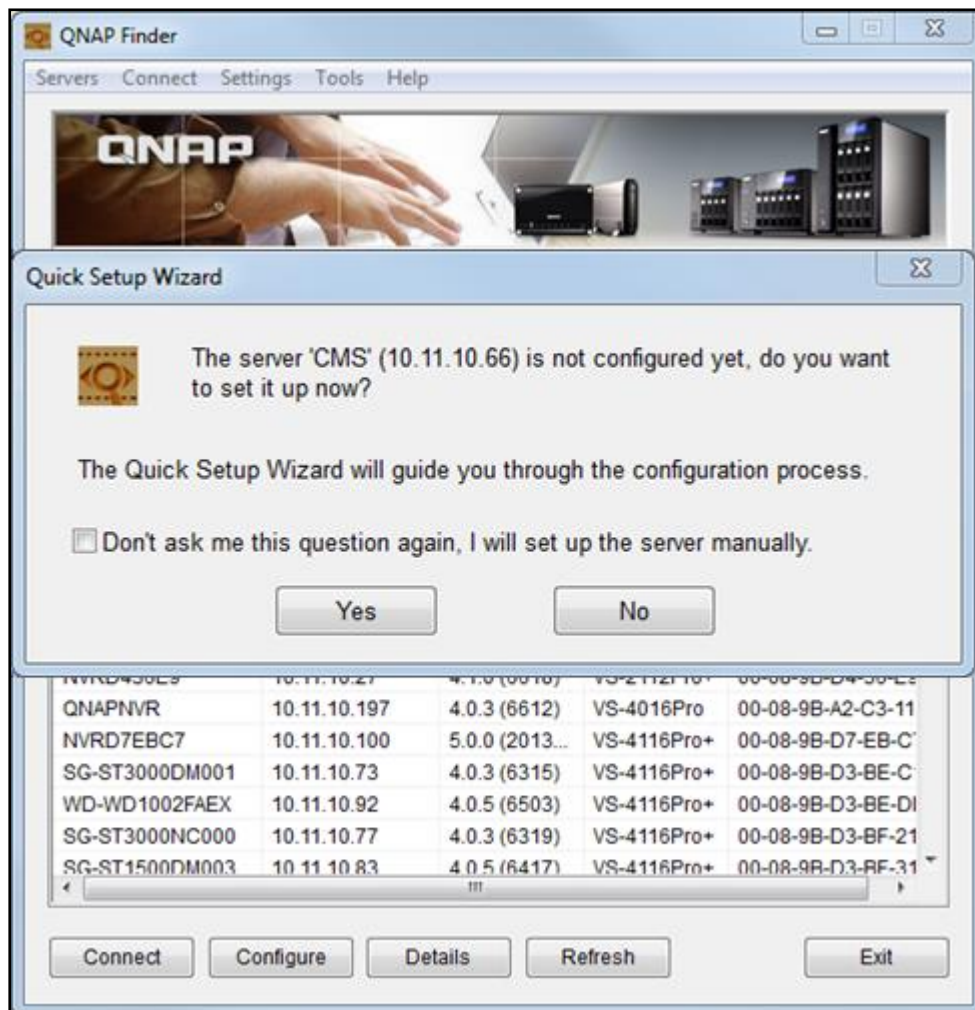
Follow the steps below to install the software of the CMS Server. The following example is based on the Windows OS.

1. Install the QNAP Finder from the product CD.

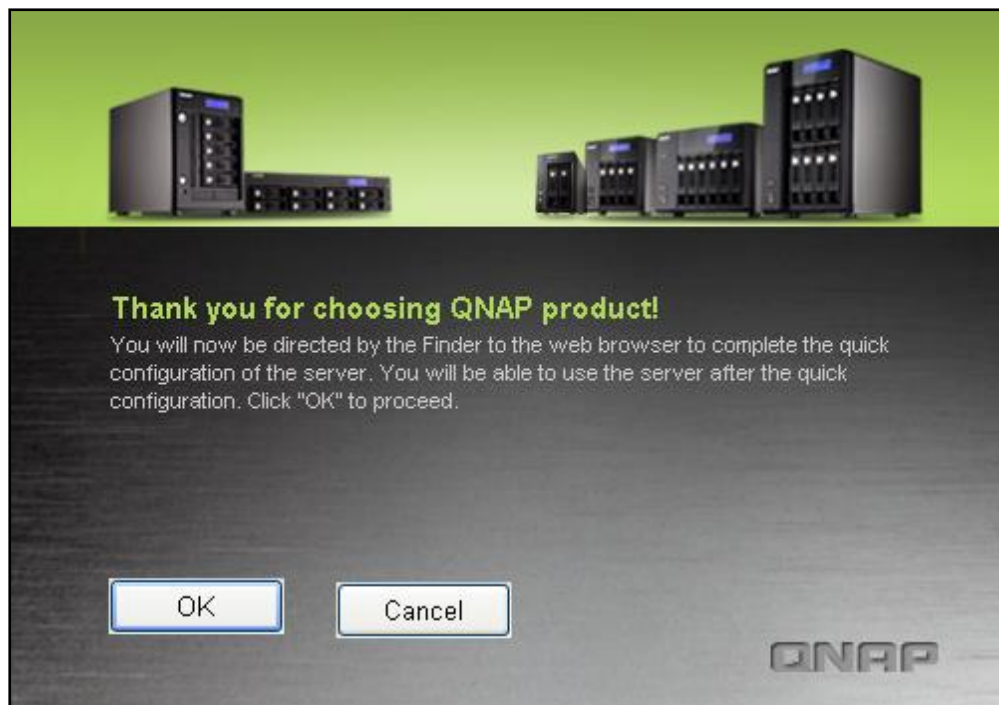


2. Run the QNAP Finder. If the QNAP Finder is blocked by the firewall or anti-virus software, unblock them.

3. The QNAP Finder will scan for CMS Server(s) that have not been configured on the local network. The CMS Server can be identified by the model number. Click "Yes" to start setting up the CMS Server.



4. Click "OK" to proceed.



5. The default web browser will be opened. Follow the onscreen instructions to configure the CMS Server.



6. Click "START INSTALLATION" in the last step.

Quick Configuration

WELCOME STEP 1 STEP 2 STEP 3 STEP 4 STEP 5 **FINISH**

Finish

The changes you have made to the server are as below. Click "Start installation" to begin the quick configuration, or click "Back" to return to the previous steps to modify the settings.

Server Name :	CMS-Demo
Password:	The password is unchanged.
Time Zone:	(GMT+08:00) Taipei
Time Setting:	Set the server time the same as your computer time.
Network:	Use the following settings
IP Address:	10.11.10.199
Subnet Mask:	255.255.254.0
Default Gateway:	10.11.10.1
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
Network services:	Microsoft Networking, FTP Service, Web Server
Disk configuration:	Raid 1
Encrypt disk volume:	No
File System:	EXT4
Drive 1:	Maxtor 6L200M0 BANC 189.92 GB
Drive 2:	Seagate ST3160318AS CC44 149.05 GB

BACK START INSTALLATION

7. All the installed hard disk drives will be formatted, and all the data will be cleared.
Click "OK" to proceed.



8. When finished, click "Return to system administration page" to complete the initialization process for the CMS Server.



Chapter 3 Installing CMS Client

After network settings of the CMS Server are configured, please connect the CMS Server to the network and set up the CMS Client.



Important: Before using the CMS Client, make sure the hard disk drives on the CMS Server have been properly installed and configured.

3.1 Suggested PC Specification for CMS Client

For optimal system performance, make sure the computer that the CMS Client runs on fulfills at least the following requirements:

CPU	Intel Sandy/Ivy bridge series (To display full HD videos or monitor multiple cameras, i5/i7 or above is recommended.)
Memory	4GB or above (To display HD videos or monitor multiple cameras, 6GB or above is recommended.)
Operating System	Windows 7 (64-bit is recommended)
Network Interface	Gigabit Ethernet
Screen Resolution	1920 x 1080
Graphics Card	NVIDIA GeForce GT430 or above ATI Radeon HD5700 or above (For multi-monitor mode, NVIDIA GeForce GT640 or above is recommended.)

Note: The CMS Client supports Windows 7 64-bit OS and can utilize up to 4GB of RAM.

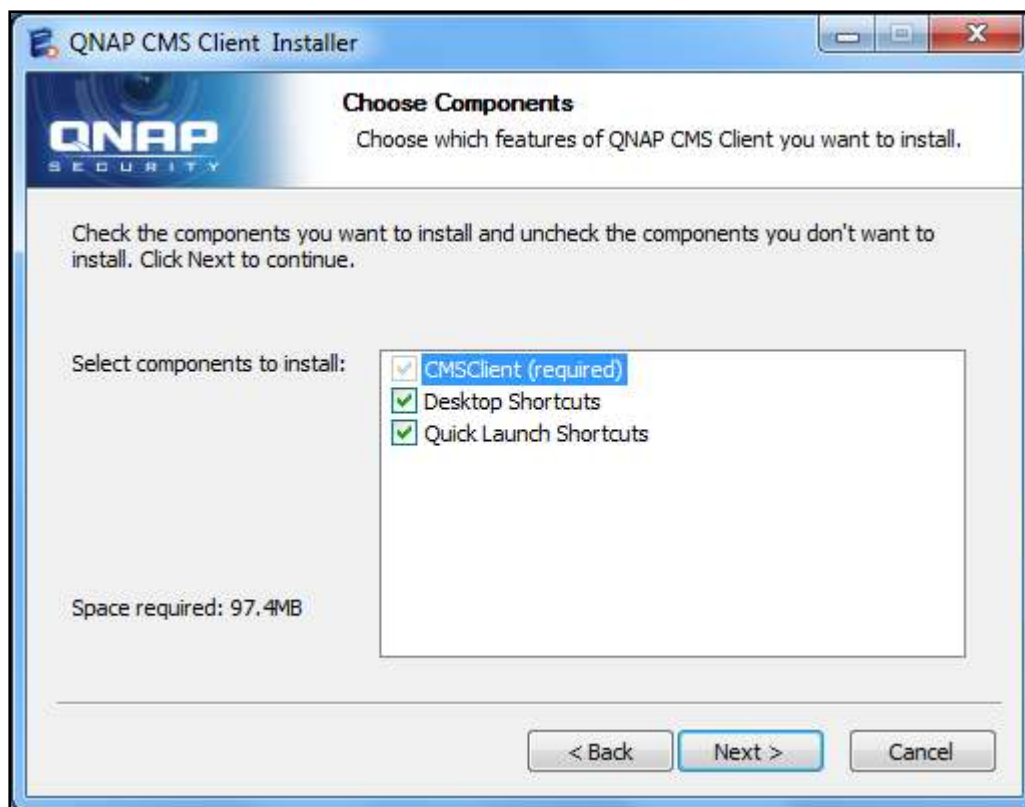
3.2 Installing CMS Client

Follow the steps below to install the CMS Client:

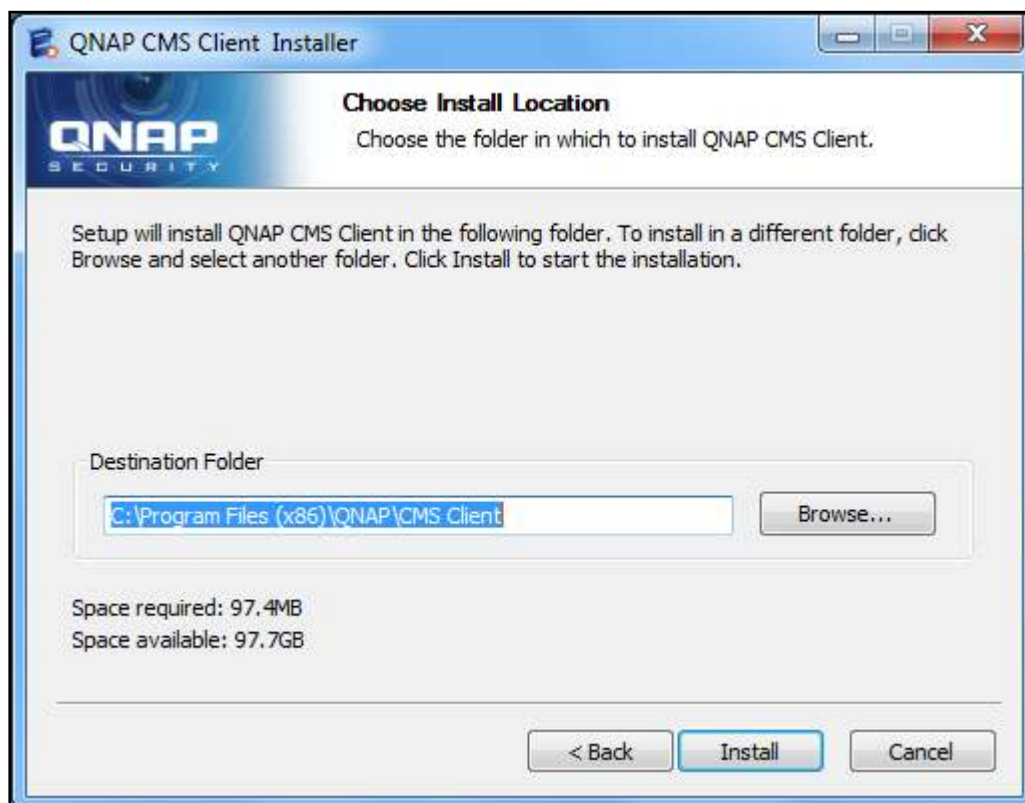
1. Run the CMS Client installer from the product CD and click "Next".



2. Choose the shortcuts to create and click "Next".



3. Select the installation directory and click "Install".



4. After finishing the installation process, click "Finish".



3.3 Connecting CMS Client to CMS Server

Follow the steps below to connect the CMS Client to the CMS Server:

1. Run the CMS Client. Enter the IP address of the CMS Server, the username, password and domain (please select the domain from the "Login to" field) and click "OK". Or, click "Auto Find" to search for CMS Servers on the local network. Double click a CMS Server from the list to connect to it or click "Connect" to connect the CMS Server.

The screenshot shows the 'Login' dialog box for the CMS (Central Management System) by QNAP. The dialog has a blue header with the QNAP logo. It contains the following fields and controls:

- Server Address:** A dropdown menu showing '10.11.16.52' and an 'Auto Find' button.
- Username:** A text field containing 'admin'.
- Password:** A text field with masked characters '*****'.
- Login to:** A dropdown menu showing 'Local'.
- ☐ Remember username and password
- ☐ Use enhanced security (SSL)
- Language:** A dropdown menu showing 'English'.
- At the bottom are 'OK' and 'Cancel' buttons.

Select the CMS Server and click "Connect".

The screenshot shows the 'CMS Finder' dialog box, which displays a list of discovered CMS servers. The list has the following columns: Name, IP Address, Version, Server Type, and MAC Address.

Name	IP Address	Version	Server Type	MAC Address
CMS-10-60	10.11.10.60	1.0.0(Build 20121203)	CMS-2000	00-08-96-D4-1D-15
CMS-QNAP	10.11.10.74	1.0.0(Build 20121203)	CMS-2000	00-08-96-D2-75-AC

At the bottom of the dialog are 'Refresh', 'Connect' (highlighted with a red box), and 'Cancel' buttons.

2. Enter the administrator username and password to login and start using the CMS Client.

Default administrator credentials:

username: admin

Password: admin

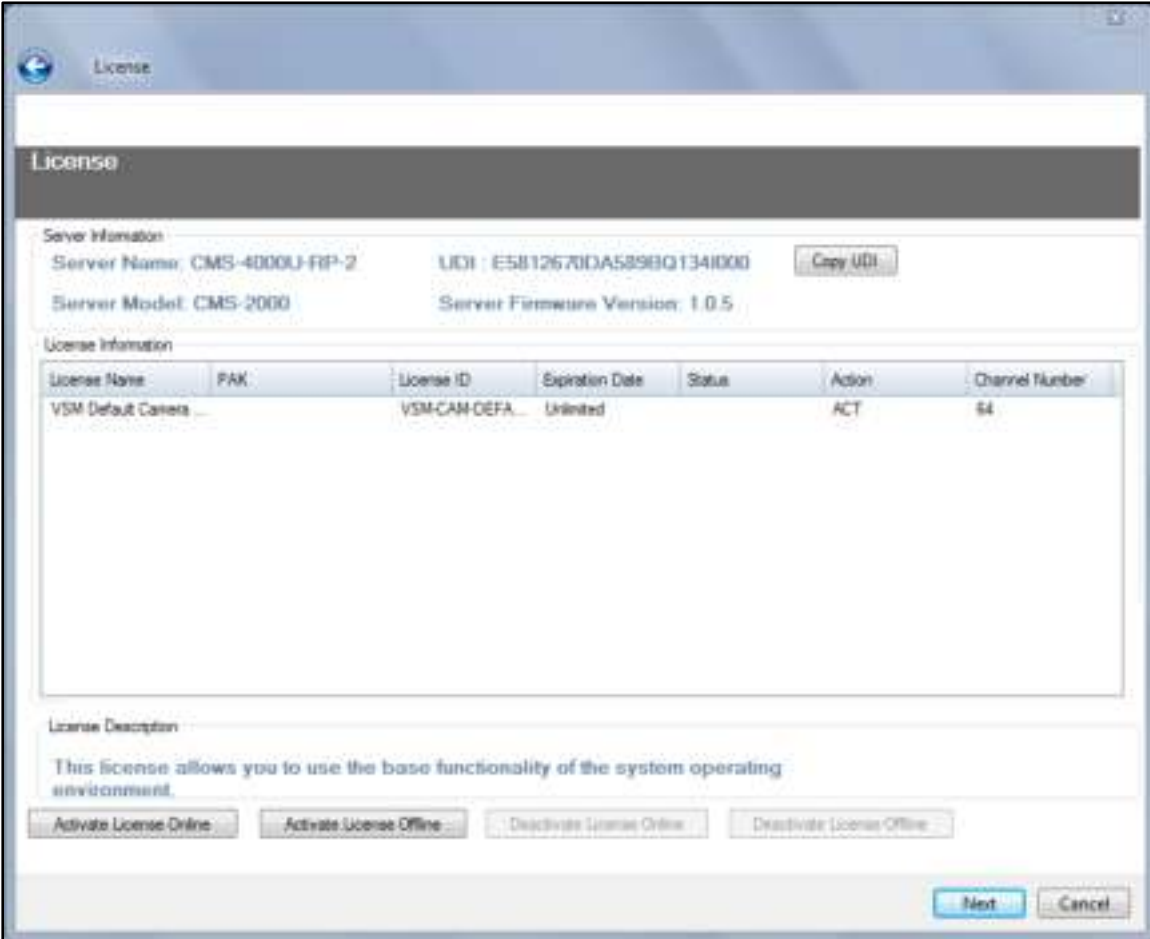
3.4 Quick Configuration Wizard

If this is the first time the CMS Client is configured, the Quick Configuration Wizard will start automatically. Please follow the instructions to set up the CMS system.



License Activation

Activate your license on this page. License activation is required before cameras can be added. For details, please refer to Chapter 3.6.



The image shows a software window titled "License" with a blue header bar. Below the header, there is a section titled "License" in a dark gray bar. The main content area is divided into several sections:

- Server Information:** This section contains two rows of information. The first row shows "Server Name: CMS-4000U-RP-2" and "UDI: E5812670DA589BQ1341000" with a "Copy UDI" button to the right. The second row shows "Server Model: CMS-2000" and "Server Firmware Version: 1.0.5".
- License Information:** This section contains a table with the following data:

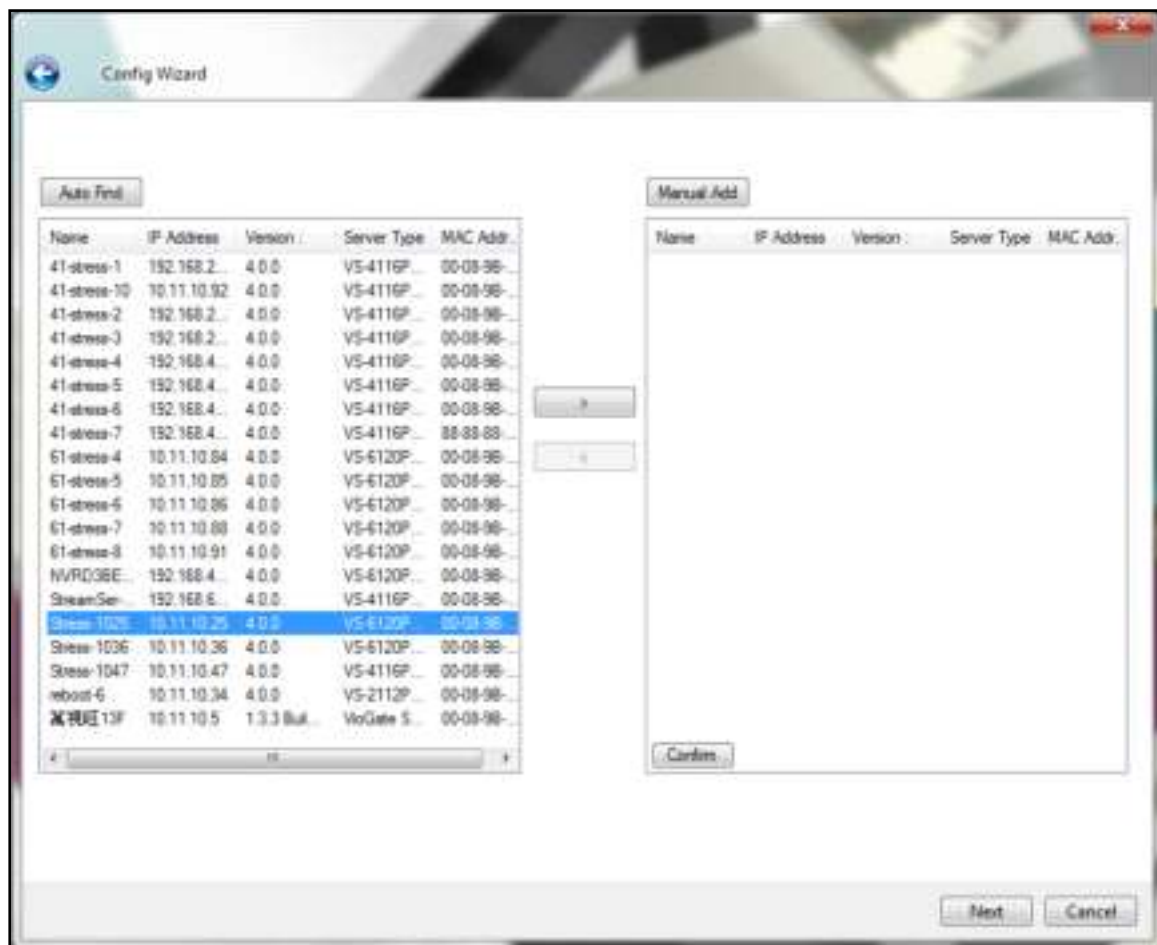
License Name	PAK	License ID	Expiration Date	Status	Action	Channel Number
VSM Default Camera		VSM-CAM-DEFA	Unlimited		ACT	64
- License Description:** This section contains the text: "This license allows you to use the base functionality of the system operating environment."
- Buttons:** At the bottom of the window, there are four buttons: "Activate License Online", "Activate License Offline", "Deactivate License Online", and "Deactivate License Offline". At the very bottom right, there are two buttons: "Next" and "Cancel".

Adding NVR(s)

Click "Auto Detect" to search for the NVR(s) on the LAN automatically, or enter the NVR IP address manually. Click > to move the NVR to be added to the box on the right and click "Confirm" to add the NVR.

Tip: Use the "Shift" or "Ctrl" + up or down keys on the keyboard to select multiple NVR servers.

For more details, please refer to Chapter 3.8.1.



Set up Display Mode

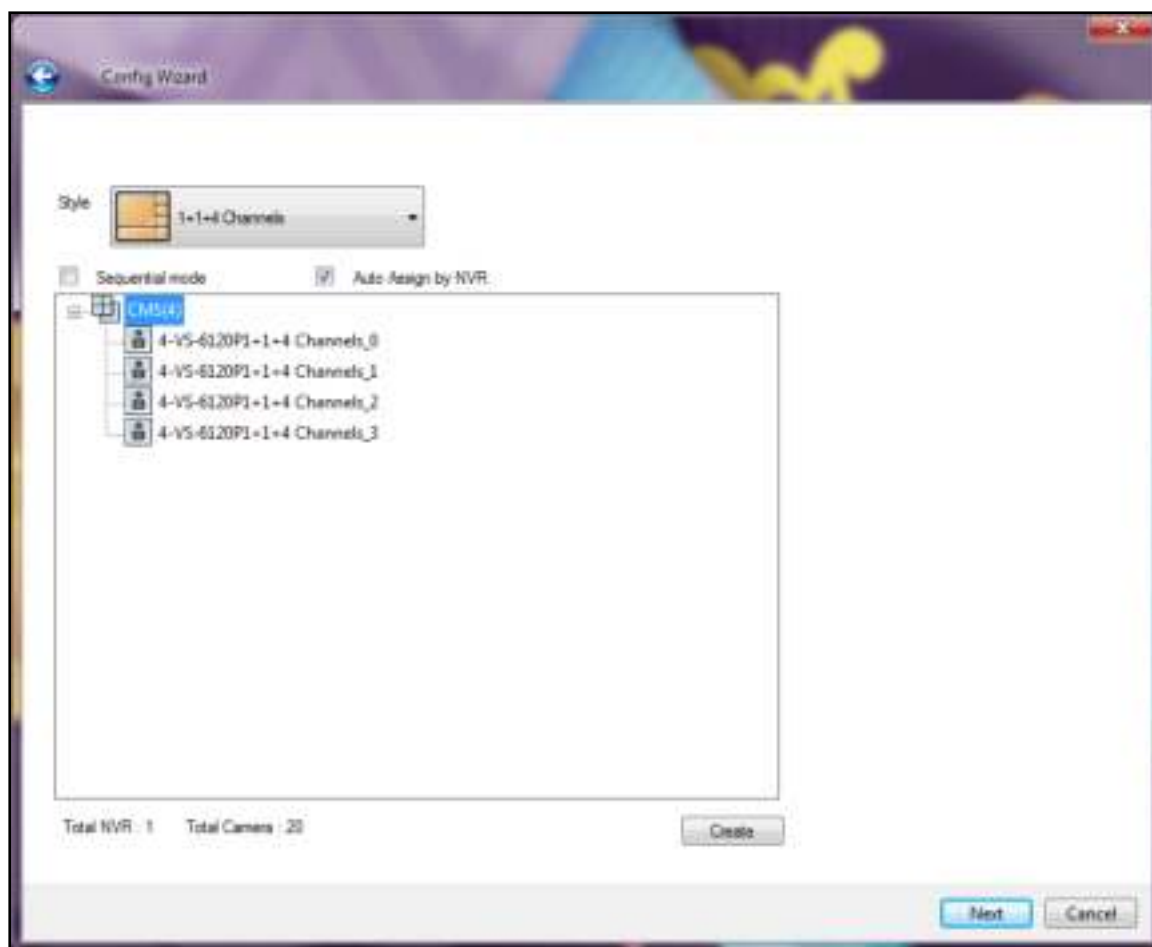
The administrator can select the display mode and assign the channels manually to use the sequential mode or have the all the channels assigned by the NVRs instead.

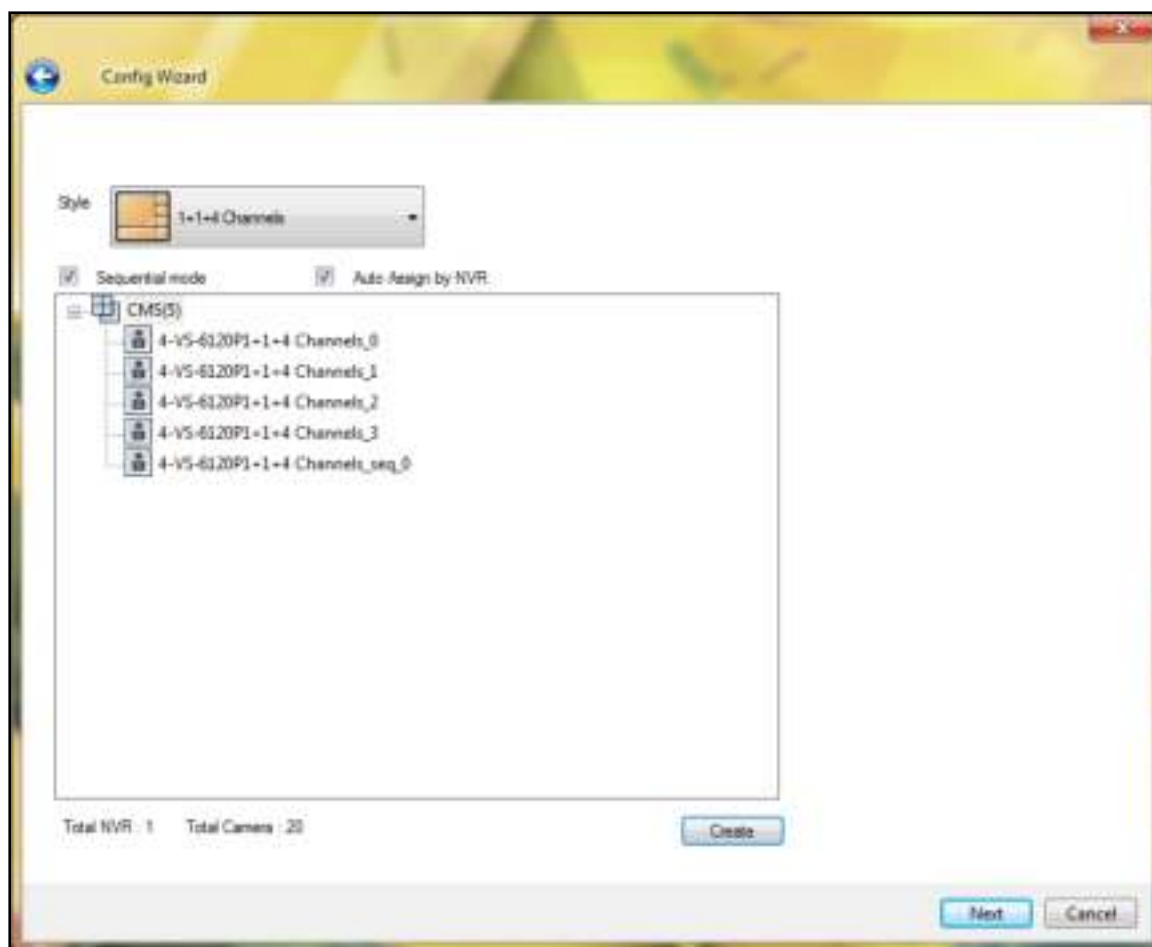
When "Sequential mode" is selected, cameras channels will be assigned sequentially to each channel window in the display mode. If the number of cameras used in the sequential mode is greater than the number of channels of the display mode, the extra channels will be assigned from Channel 1 again. For instance, if 64 channels are assigned to a 6-channel view, the seventh channel will be displayed on Channel 1 and the eighth channel will be displayed on Channel 2, and so on and so forth. Please note that since a maximum of 10 channels can be assigned to one channel, please always select a display mode with a maximum number of channels that is greater than the total number of selected channels (ex. for 64 channels, please select the 8-channel view.)

When "Auto Assign by NVR" is selected, camera channels will be assigned based on NVRs. For example, if 20 channels from NVR 1 and 32 channels from NVR 2 are selected for the 6-channel view, all 20 channels from NVR 1 will be first assigned from Channel 1 to Channel 6 sequentially (and the seventh channel from NVR 1 will be assigned to display on Channel 1 again and eighth on Channel 2.) All 32 channels from NVR 2 will then be assigned from Channel 1 to Channel 6 after all cameras from NVR 1 are assigned.

Please note that in "Sequential mode", channels assigned to a channel window will be displayed and switched sequentially and automatically, while in "Auto Assign by NVR", channels need to be switched manually.

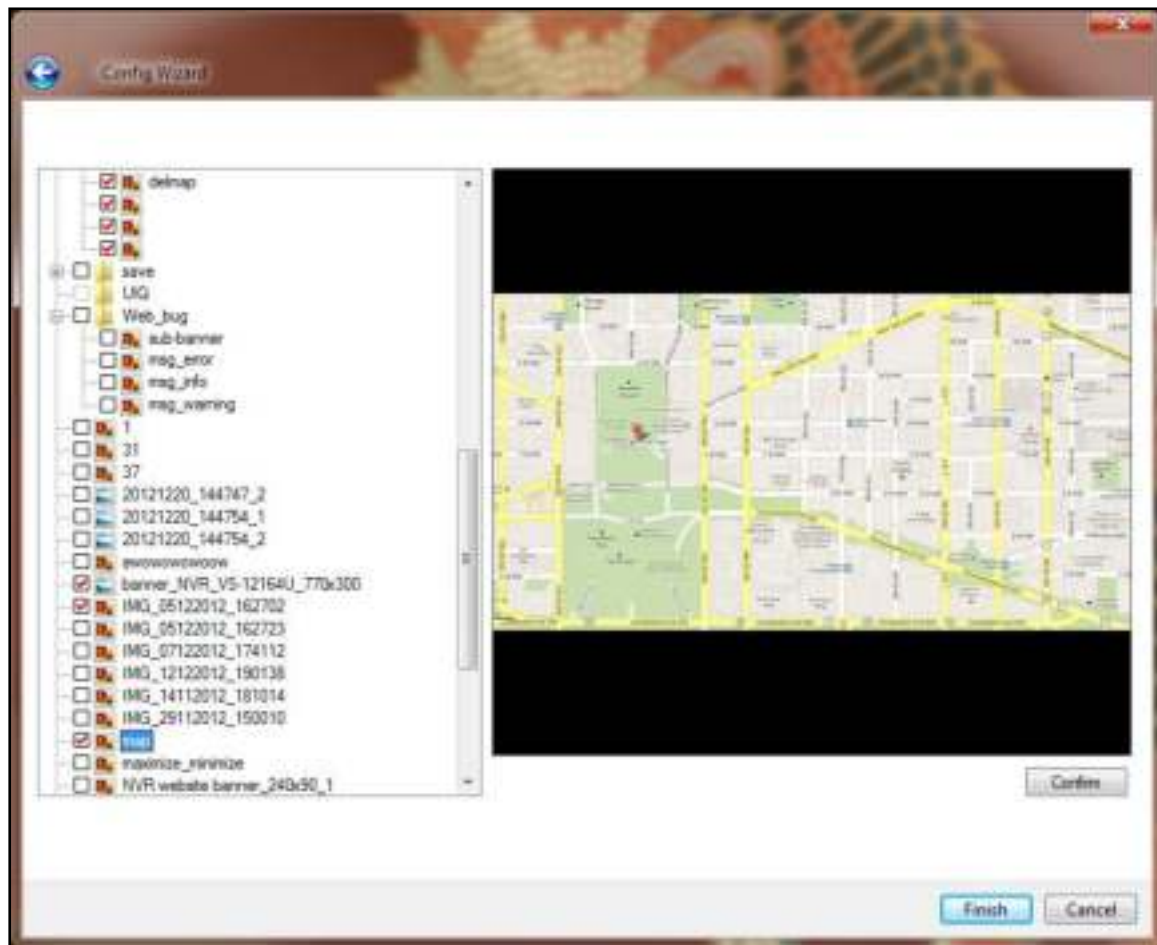
If both "Sequential mode" and "Auto Assign by NVR" are selected, all channels from the same NVR will be assigned to and displayed on the selected display mode sequentially and automatically. For instance, if 20 channels from NVR 1 and 32 channels from NVR 2 are selected for the 6-channel view, all channels from NVR 1 will be assigned to and displayed sequentially and automatically on the first page, and all 32 channels from NVR 2 will be assigned to and displayed sequentially and automatically on the second page. To view the channels from a different NVR, users are required to manually switch to the corresponding pages.






Uploading E-map(s)

Select the E-map files or directories on the right, click "Confirm" to upload the E-maps and then click "Finish" to finish the wizard.



3.5 Configuring CMS Client

To enter the system settings page on the CMS Client, login the live view page as an administrator and then click .



The system overview page will be opened. Select the overview period from the drop-down menu on the top right corner. The system can display system details for up to seven days. Click "Learn more" under each item to view the details.



The system overview page contains the following information:

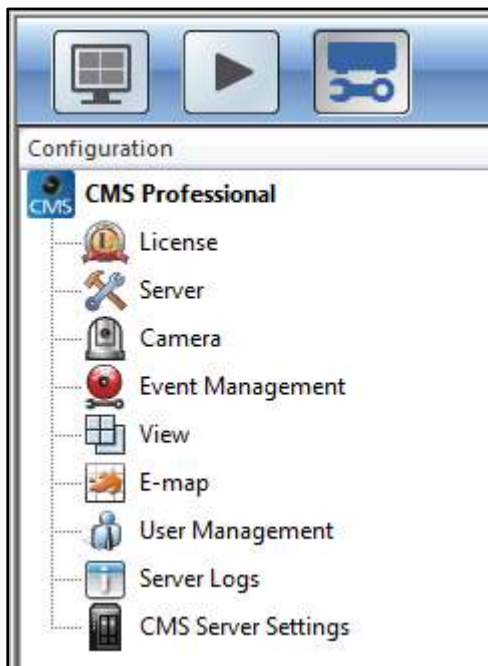
- Alarm: Alarm input, dynamic motion event information, and charts.
- User account: user account related information, such as login failed, never logged in, and the total number of user accounts.
- NVR connection status: Information about the number of NVRs that have never been disconnected and have been disconnected, and the total.
- IP camera connection status: Information about the number of cameras that have never been disconnected and have been disconnected, connection failure, and the total.
- NVR system status: Information about the number of hard disk failure, fan failure, and the total.
- Real-time status: Online users/total users, online NVRs/total NVRs, and online cameras/total cameras.

Note:

- Besides the real-time information, all other information provided is the records from the previous seven days.
- If a NVR is deleted, its records will also be permanently deleted and its logs will no longer be available.

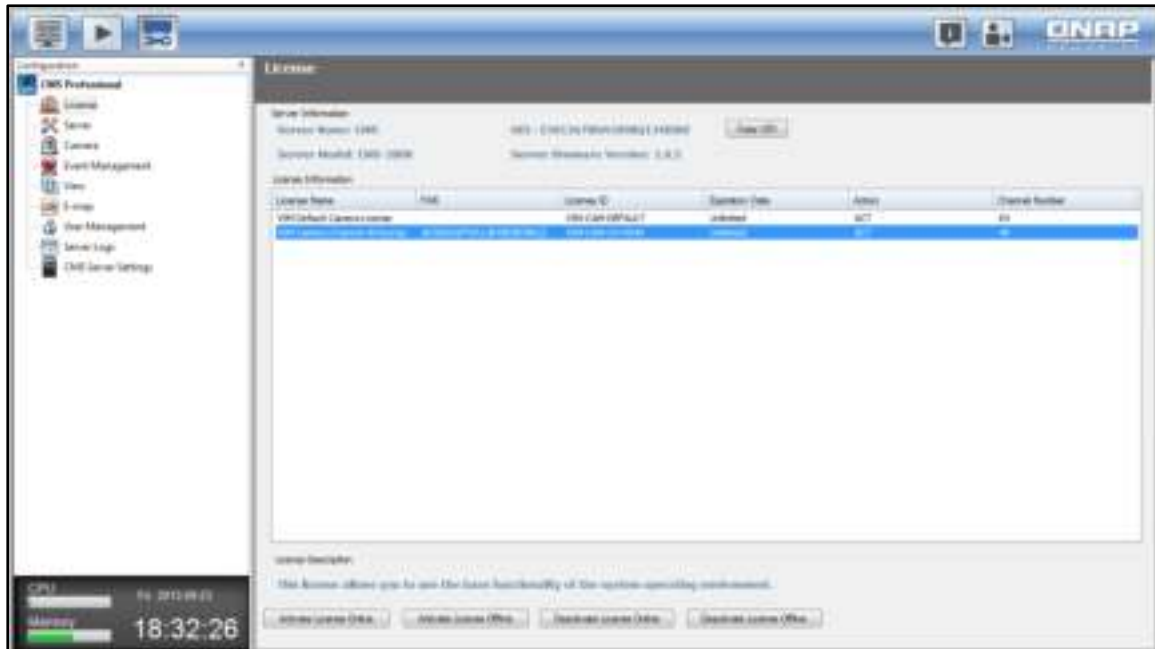
The configuration settings are available on the left:

- License
- Server
- Camera
- Event management
- View
- E-map
- User management
- Server logs
- CMS Server Settings



3.6 License

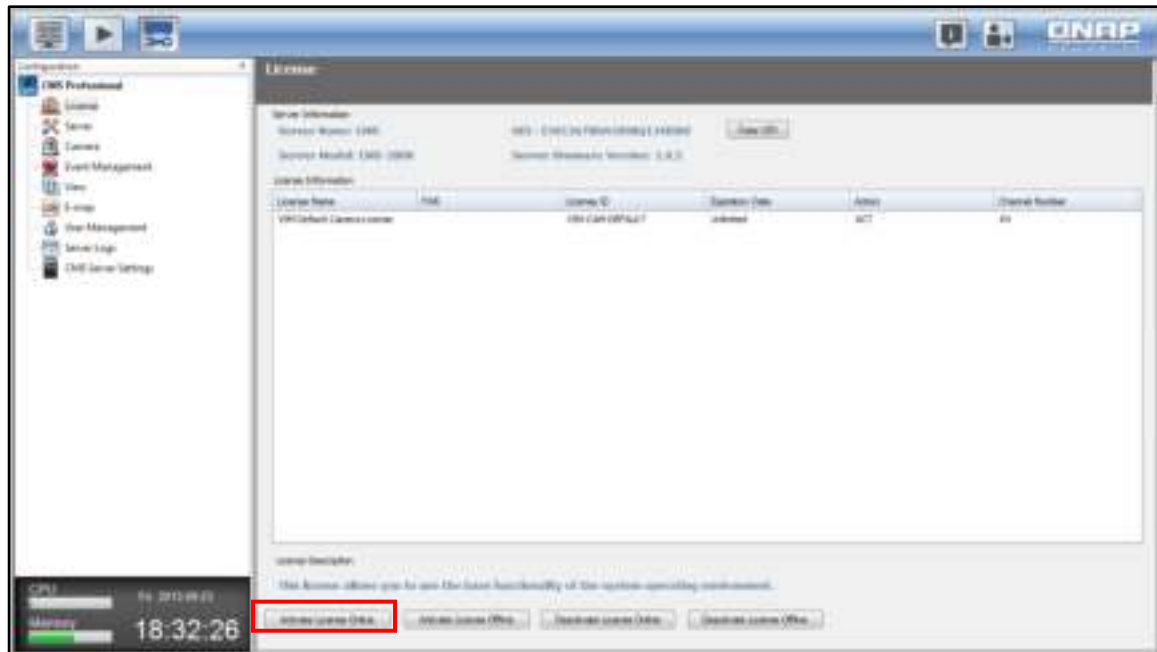
Please activate your license on this page if you have not already done so using the Quick Configuration Wizard. License activation is required before cameras can be added. A 64-channel license is provided for each CMS Server and you can choose to activate or deactivate your license online or offline.



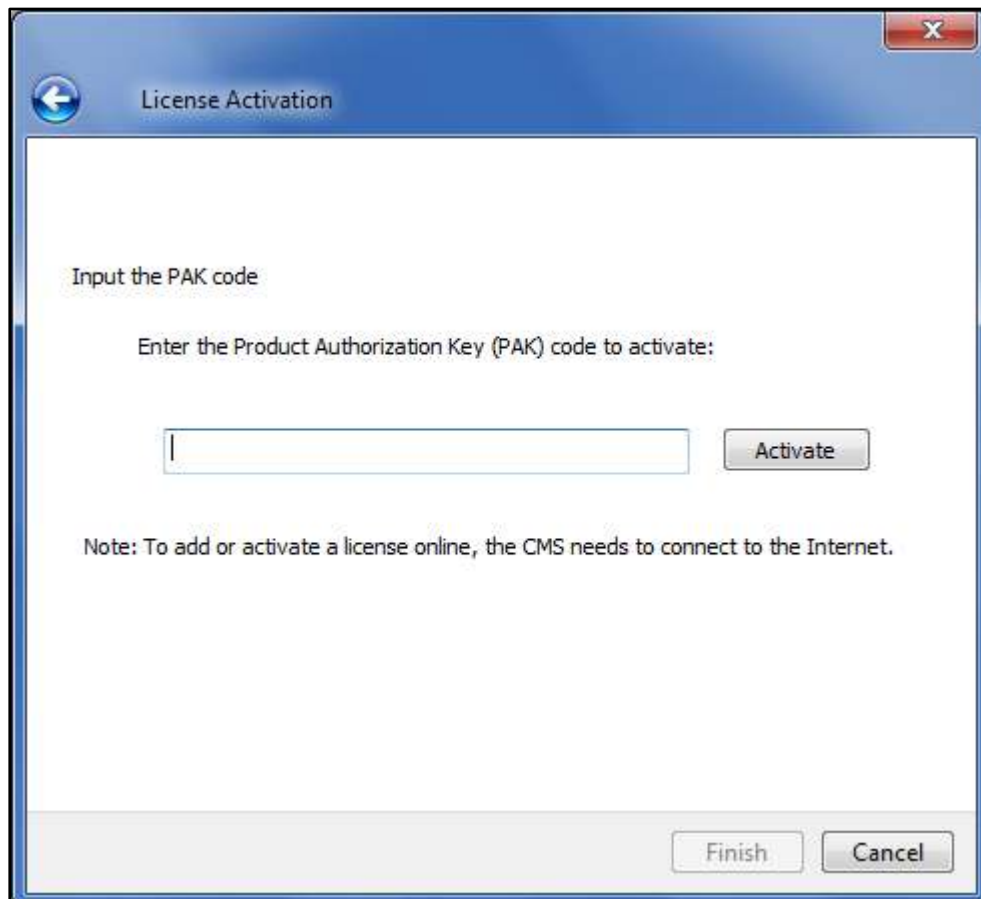
3.7 Activating License Online

Please follow the steps below to activate your license online:

1. Click "Activate License Online"



2. Enter the product authorization key and click "Activate" and "Finish".

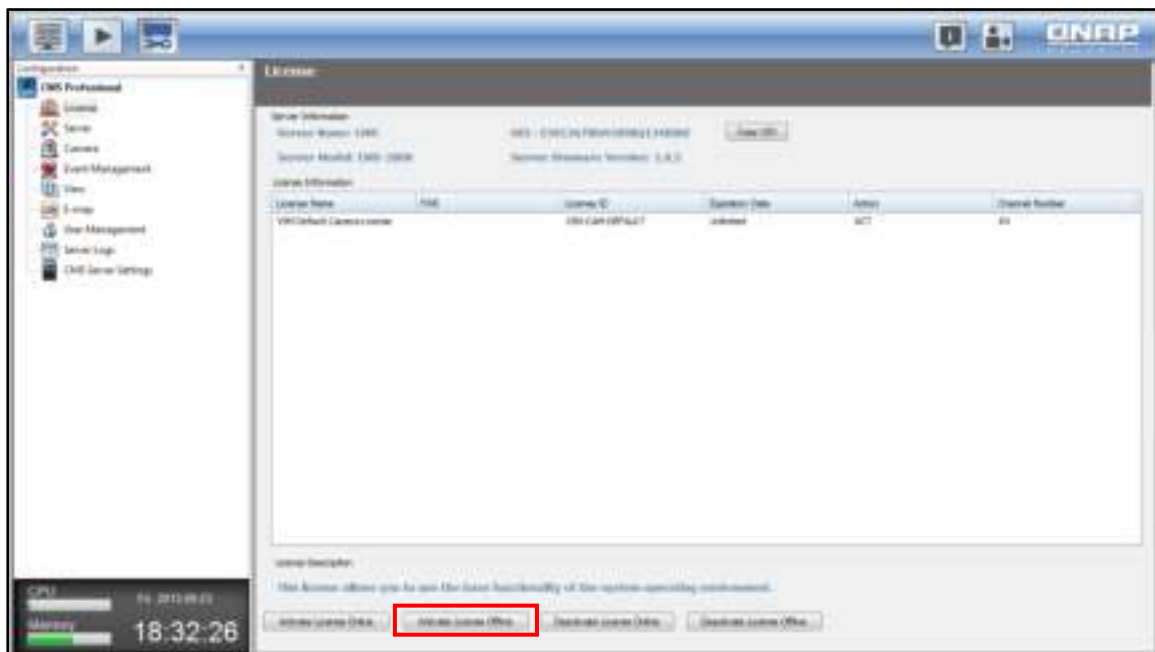


3. After the license is activated online, the license detail will appear.

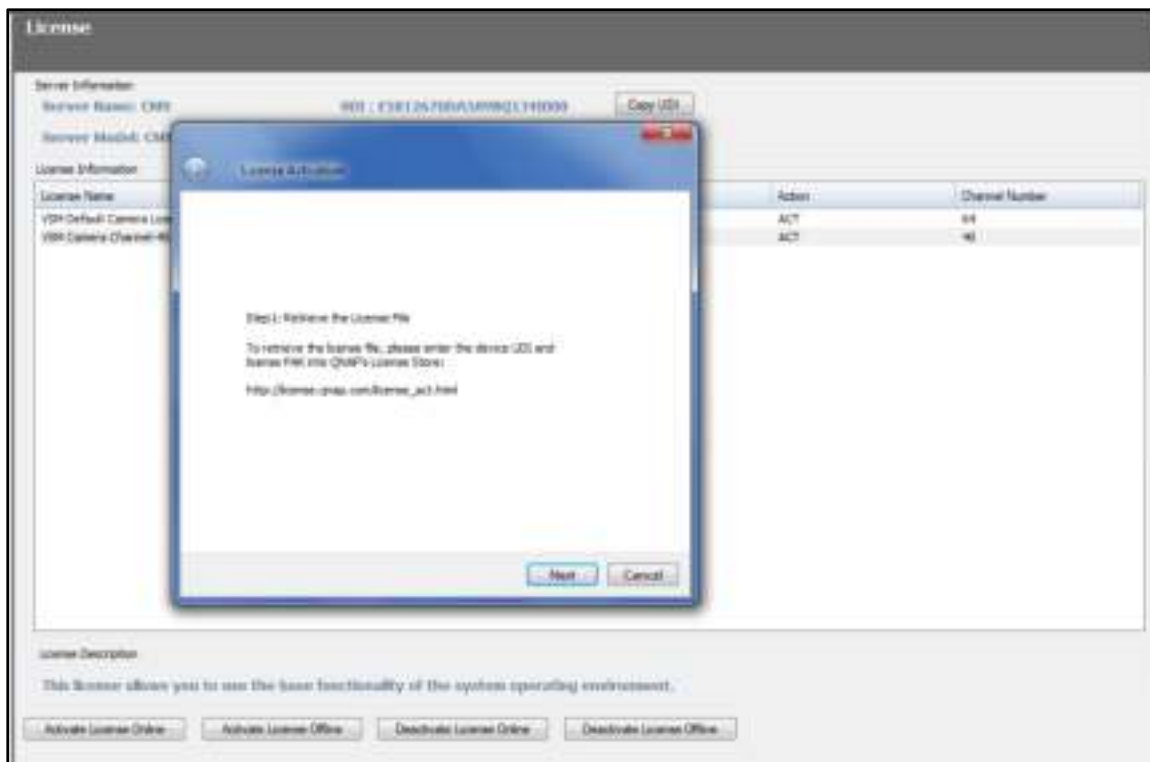


3.7.1 Activating License Offline

If the Internet is unavailable, please follow the steps below to activate your license offline.



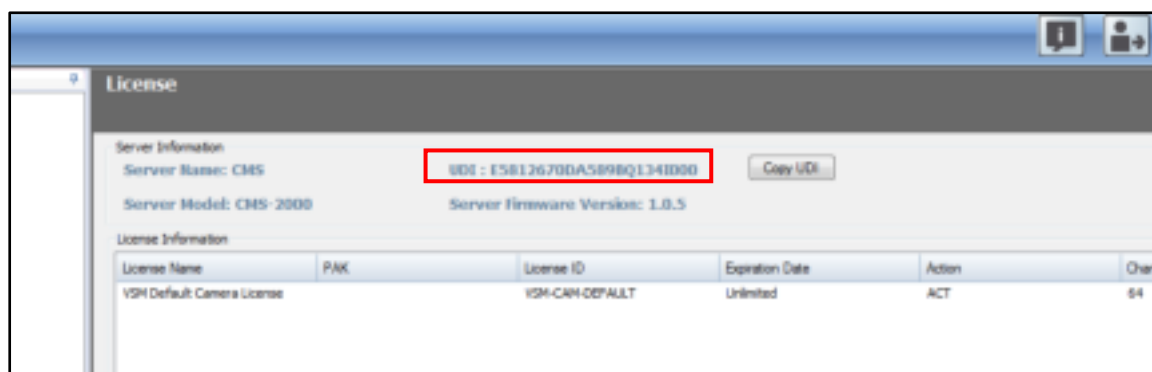
1. Click the "Activate License Offline" button. A prompt window will appear to remind you to use another PC that can go online to bind the PAK and UDI. So, a physical permission file can be generated to activate the CMS Client.



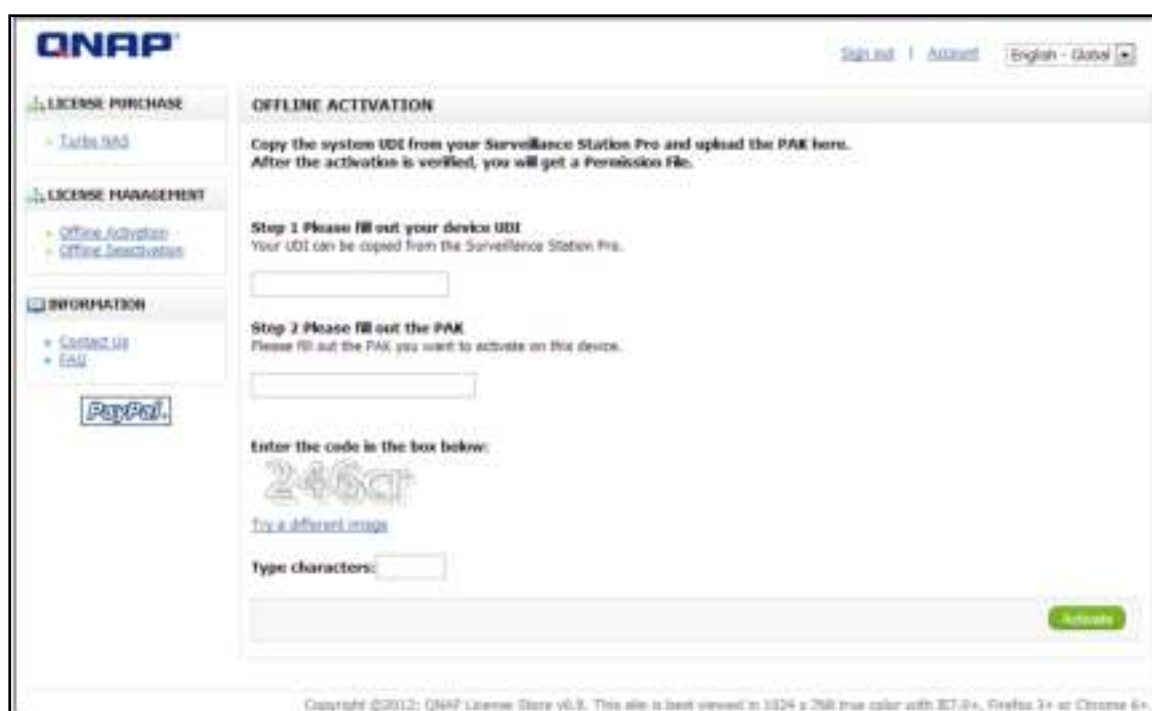
2. Click "Offline Activation" after entering the License Store (<http://license.qnap.com>).



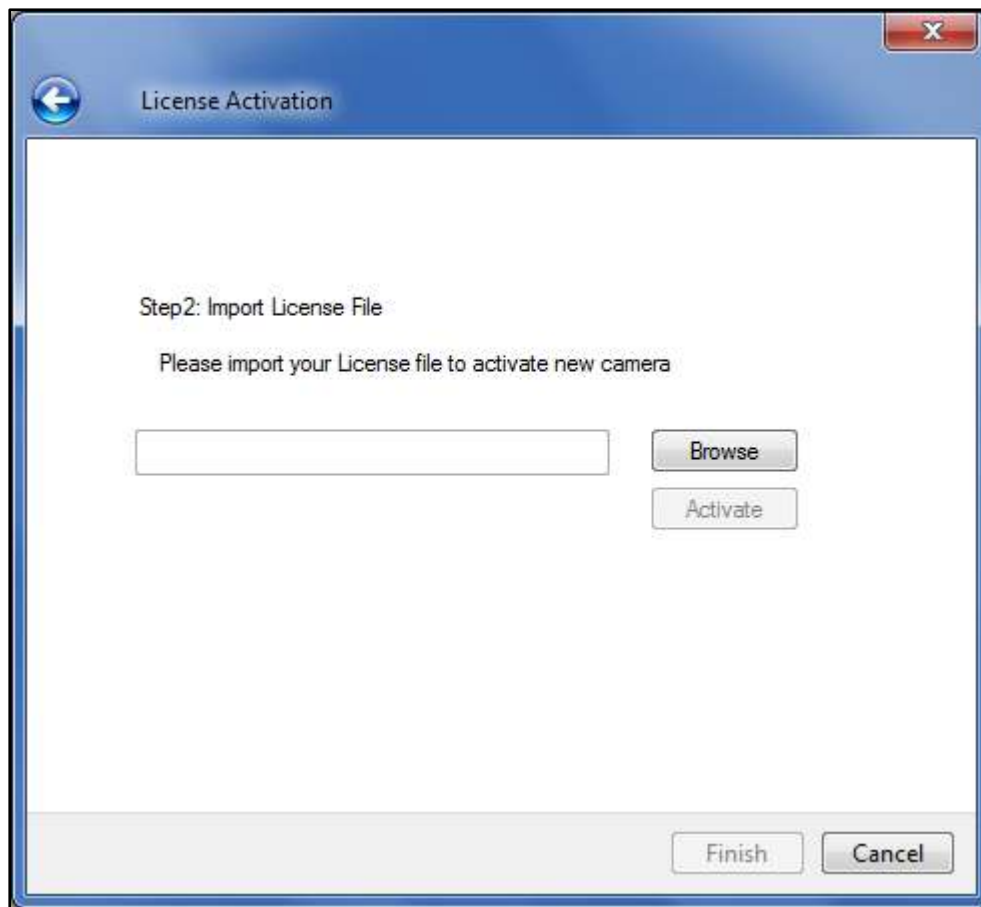
3. After membership registration, please fill out the PAK provided, the device UDI and verification code from the license activation page to download the physical permission file.



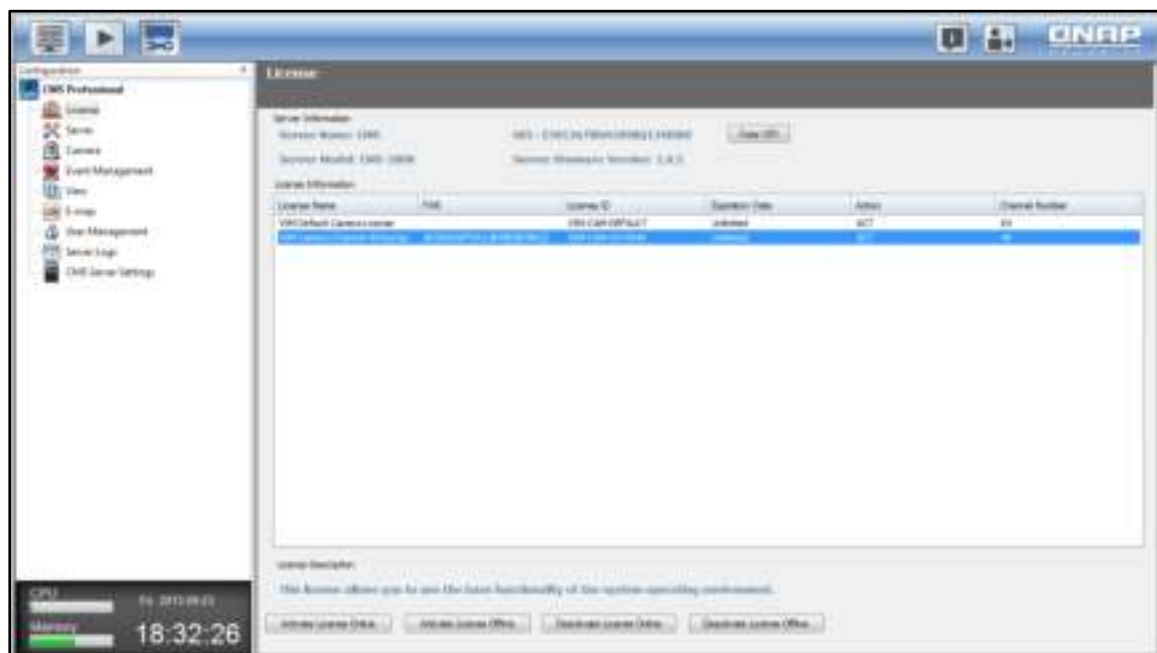
Tip: Use the "Copy UDI" function to copy UDI and paste in the field of QNAP license store.



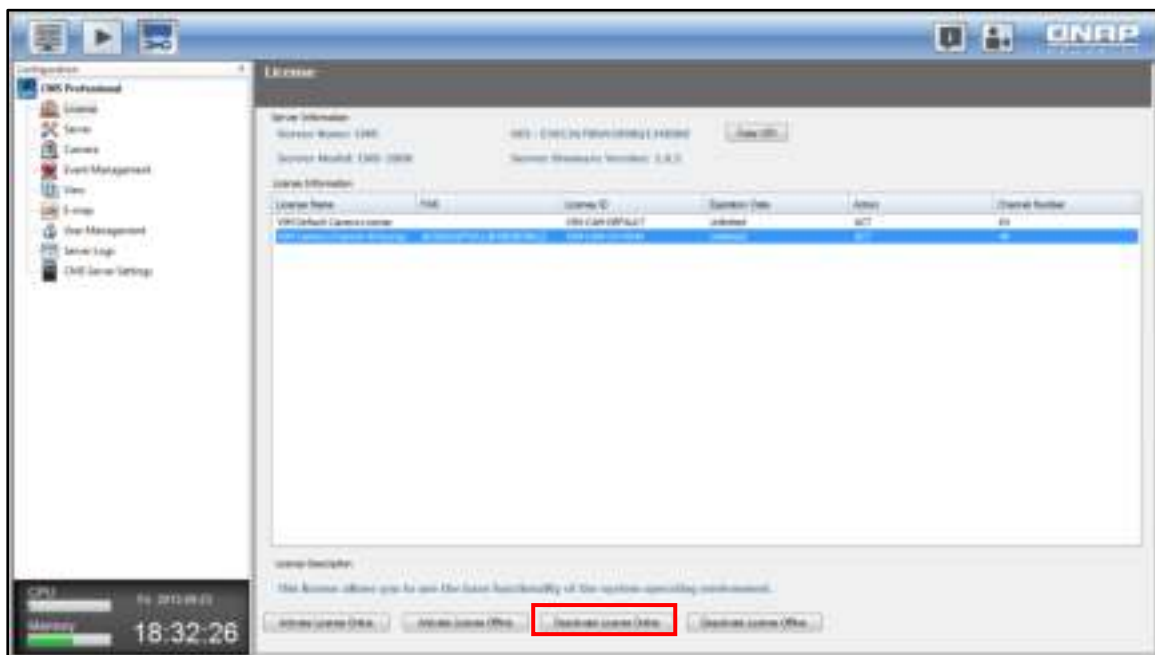
4. Upload the license file.



After the license is activated, its details will appear.

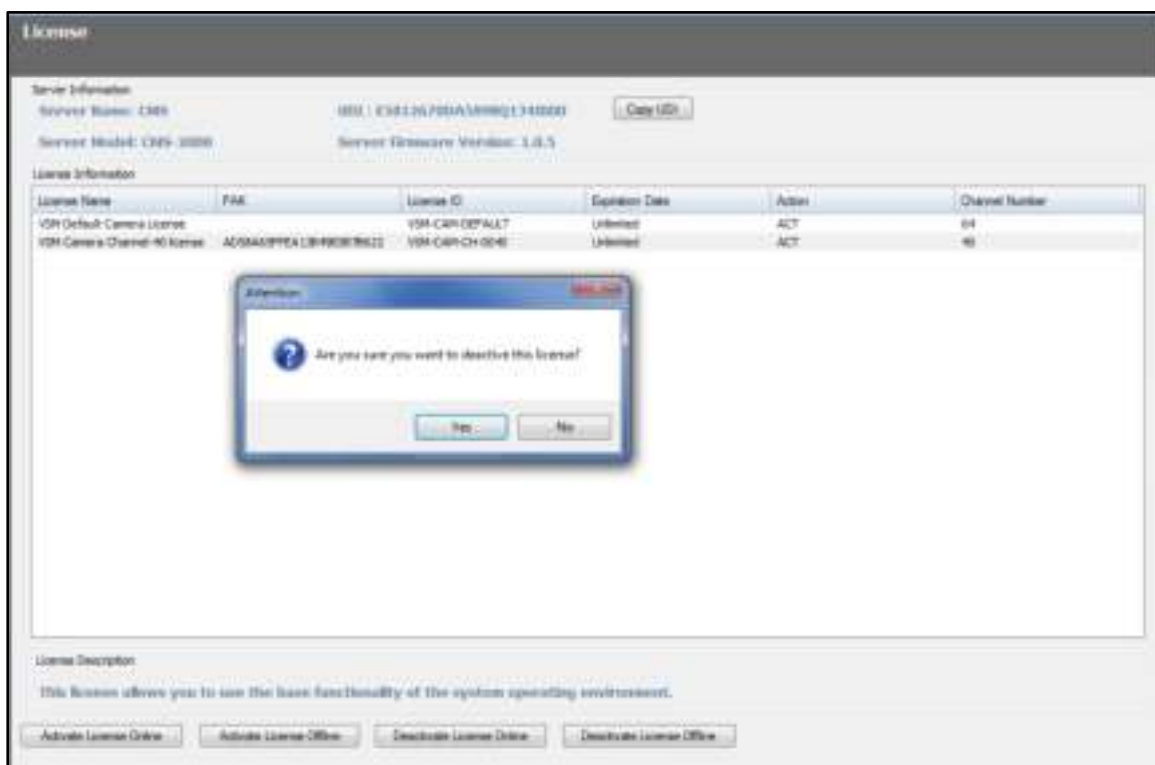


3.7.2 Transferring/Deleting Authorization

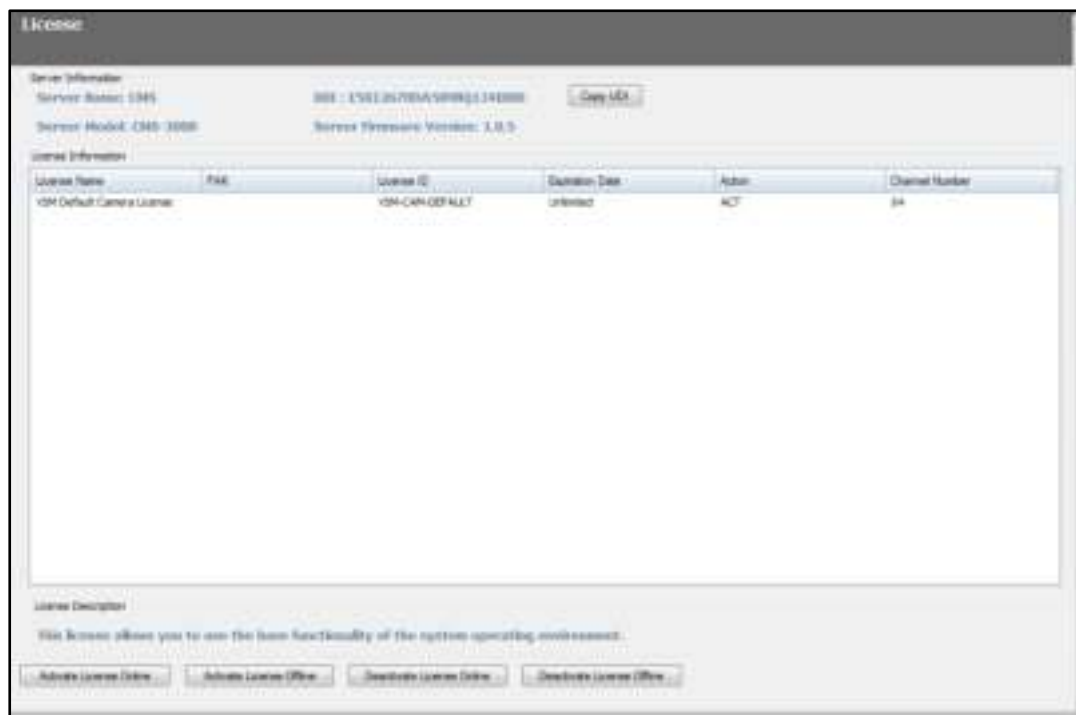


To transfer and delete your license, please deactivate it first either online or offline.

- Online License Deactivation: If Internet access is available for the CMS Server, please click the license to be deactivated and then "Deactivate License Online". The CMS Server will connect to the License Store to deactivate the selected license. The system will confirm with you about license deactivation. Please click "Yes".

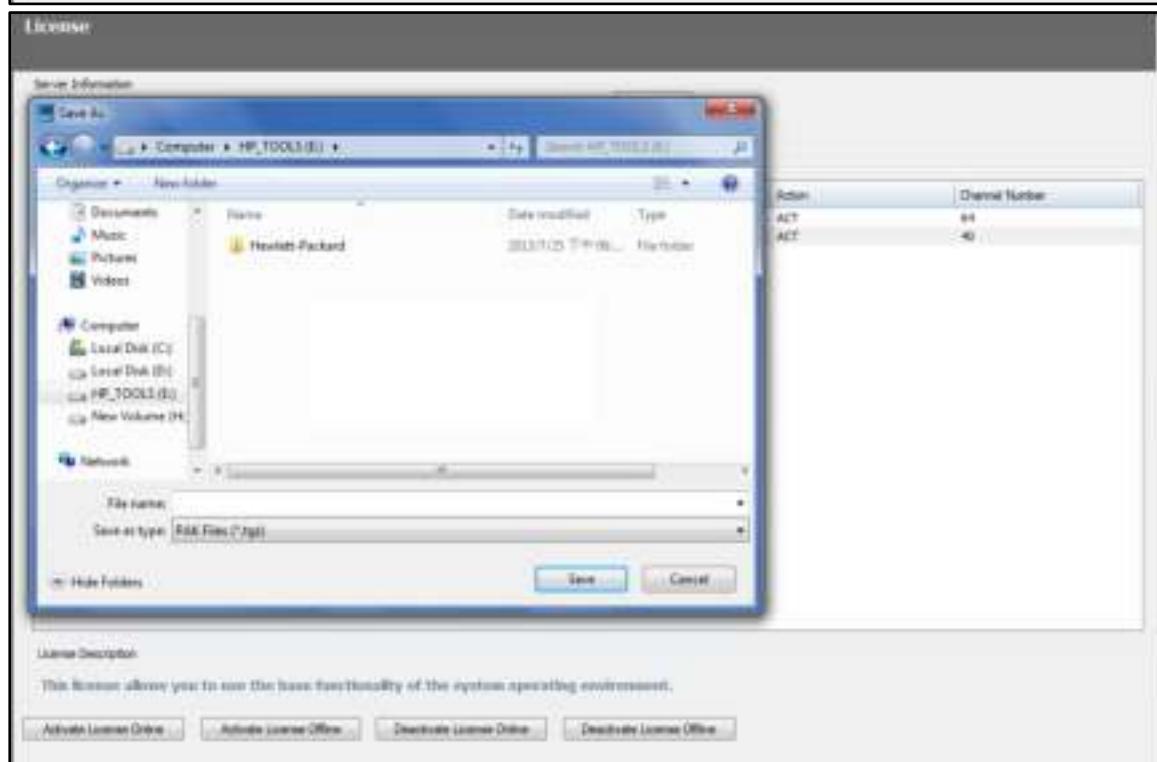
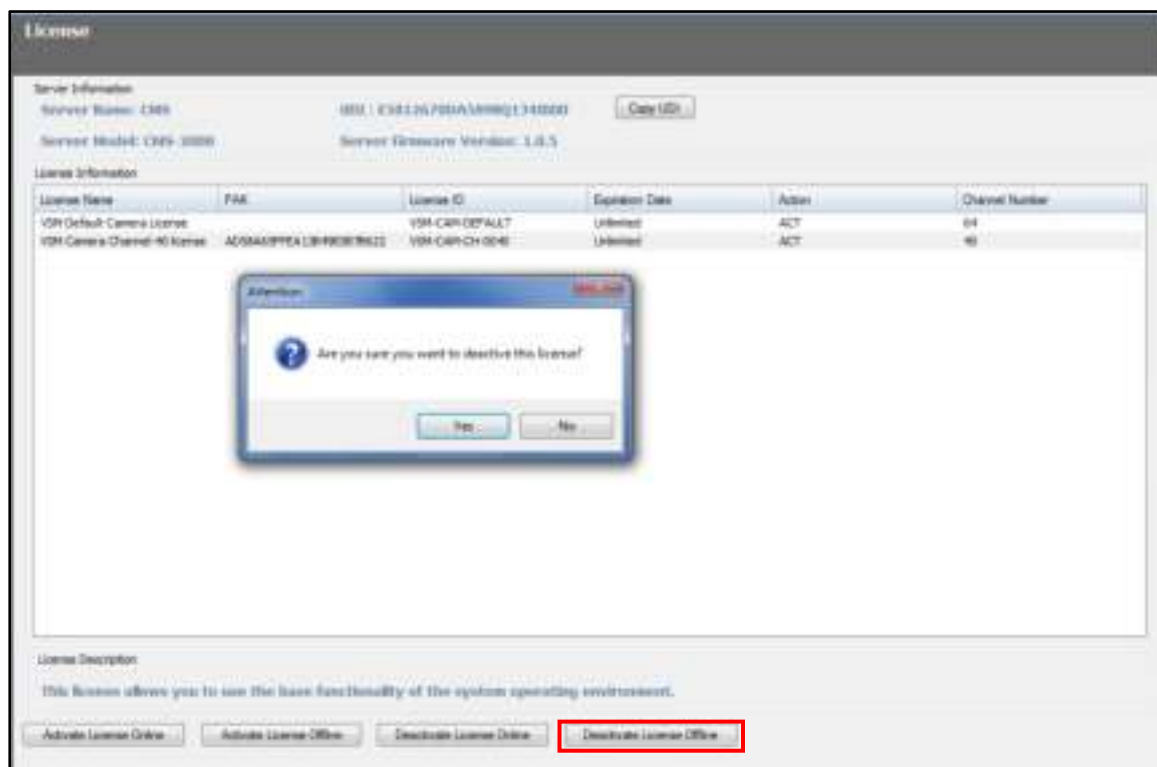


The license will be deactivated and removed from the list.




Offline License Deactivation: If Internet connection is unavailable for the CMS Server, please click "Deactivate License Offline". The CMS Client will generate a deactivation ticket (a physical file). Please upload this ticket to the License Store using another device that can connect to the Internet. To deactivate the license offline, please follow the steps below:

1. Select a license to be deactivated, click "Yes" and a ticket will be generated.



2. Go to the License Store using another computer that can connect to the Internet and click "Offline Deactivation".





[Sign out](#) | [Account](#) | [English](#) - Global

LICENSE PURCHASE


[Turbo NAS](#)

LICENSE MANAGEMENT

[Offline Activation](#)
[Offline Deactivation](#)

INFORMATION

[Contact Us](#)
[FAQ](#)



OFFLINE DEACTIVATION


QNAP License Deactivation Service allow you to apply license deactivation.

Step 1 Please upload your deactivation ticket

選擇檔案

上傳檔案

Enter the code in the box below:


[Try a different image](#)

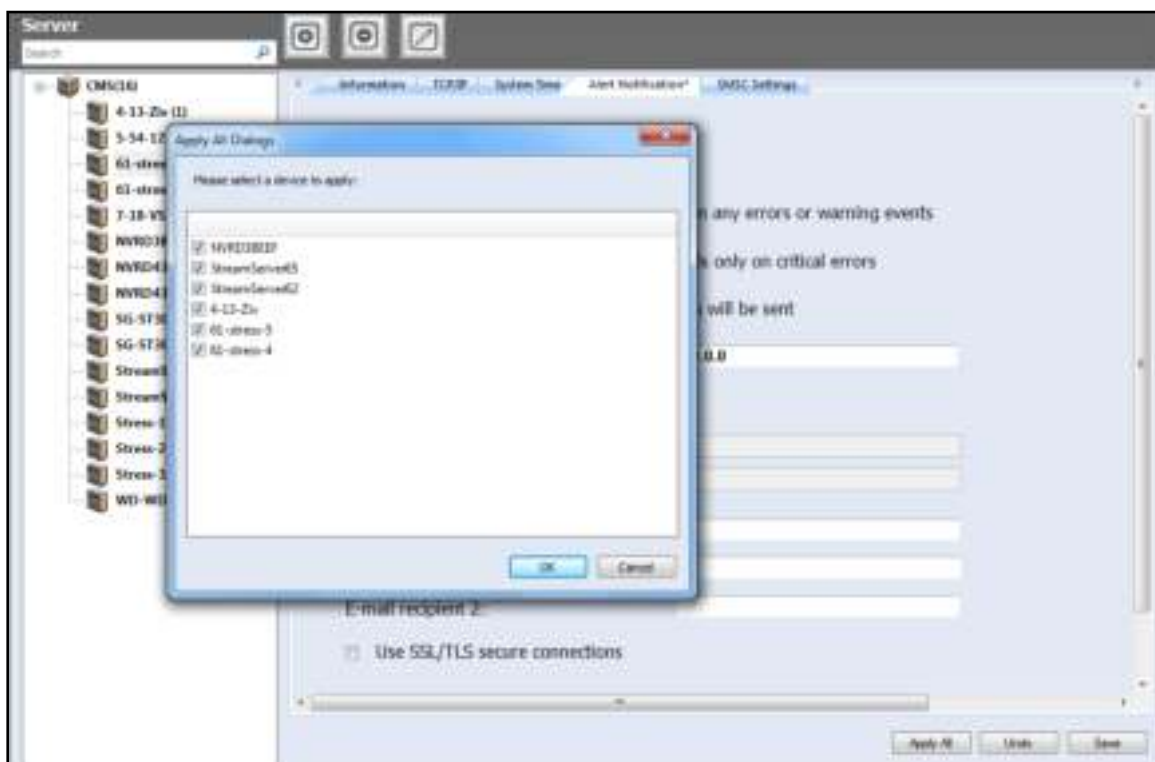
Type characters:

Copyright ©2012: QNAP License Store v0.9. This site is best viewed in 1024 x 768 true color with IE7.0+, Firefox 3+ or Chrome 6+.

After license management (activation and deactivation), the next step is to add NVR servers and cameras.



The CMS client can apply the same system time, alert notification and SMSC settings to a number of NVRs (only limited to the same models) to save the system setup time.



3.8.1 Adding NVR

To add one or more NVR servers, click .



You can use the auto-find function to search for the NVR server(s) on the LAN, or enter the NVR IP address manually.



When adding more than one server, you can enter a pair of username and password and apply to all of them. When the "Add all the cameras" option is checked, all the cameras configured on the NVR will be added.

Note: When any pair of username and password for the multiple NVRs to be added is incorrect, the server(s) will not be added and no warning message will appear.

If the subnet of an NVR is different from that of the CMS Client, use "Manual Add" and enter the IP and port number of that NVR. Click "OK" to connect.

Manual Add ✕

IP Address:

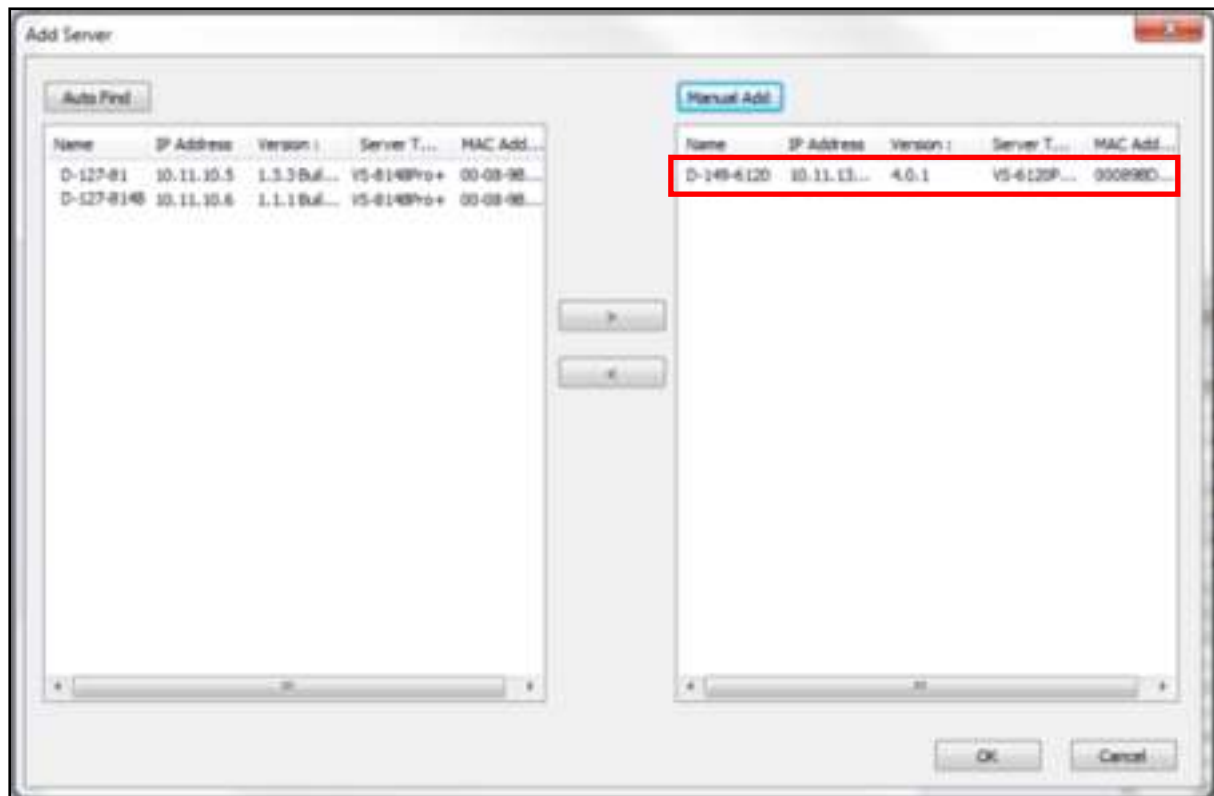
Port Number:

Username:

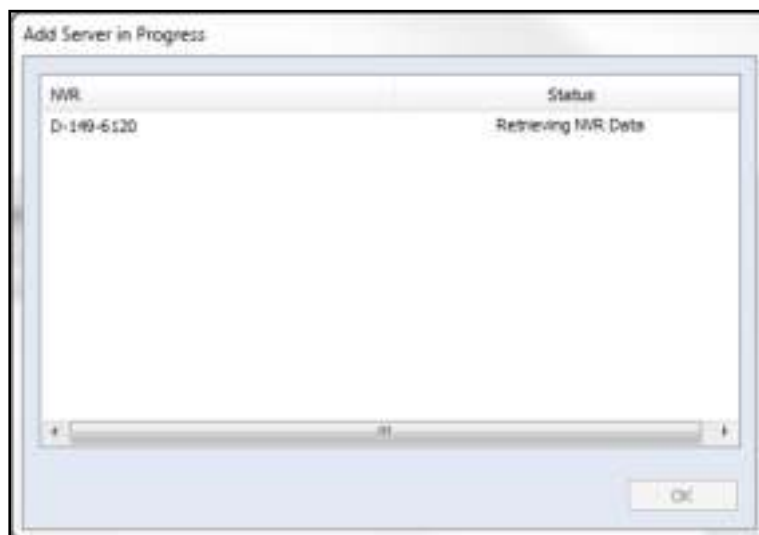
Password:

☒ Add all Cameras

The NVR in another subnet will be added.





After adding all required NVR(s), click "OK" and the "Add Server in Progress" message box will appear and the status will be shown in the box.

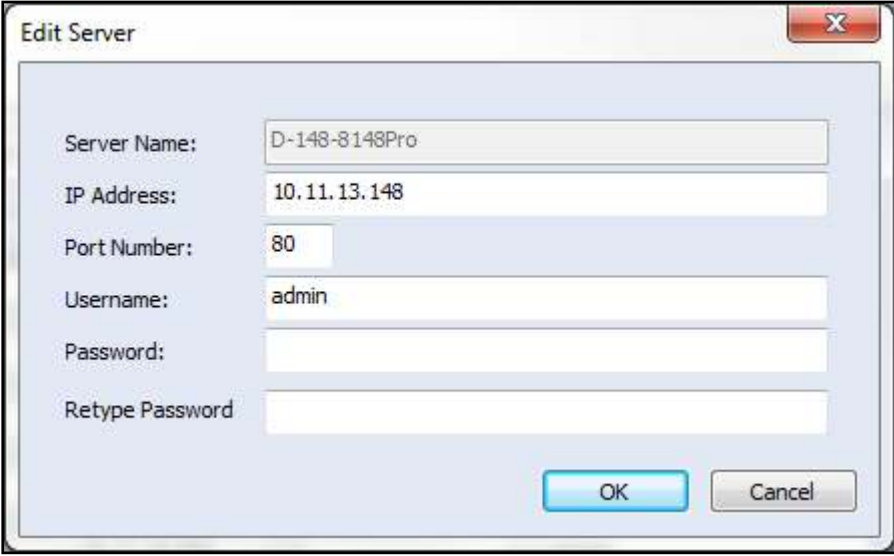


Click "Confirmation". The system will add the servers one by one. There are four kinds of status: Retrieving NVR Data, Add Channel (channel number) to CMS, Done and Connection Error.

Note: For the “Connection Error” error message, please check your user ID/password, firewall and network settings.

3.8.2 Deleting/Editing NVR

To delete an NVR, select the NVR on the list and click . To edit the NVR details (server name, IP address, port, user name, or password), select the NVR and click . Click “OK” after all fields are completed.



The image shows a dialog box titled "Edit Server" with a close button (X) in the top right corner. The dialog contains several input fields for server configuration:

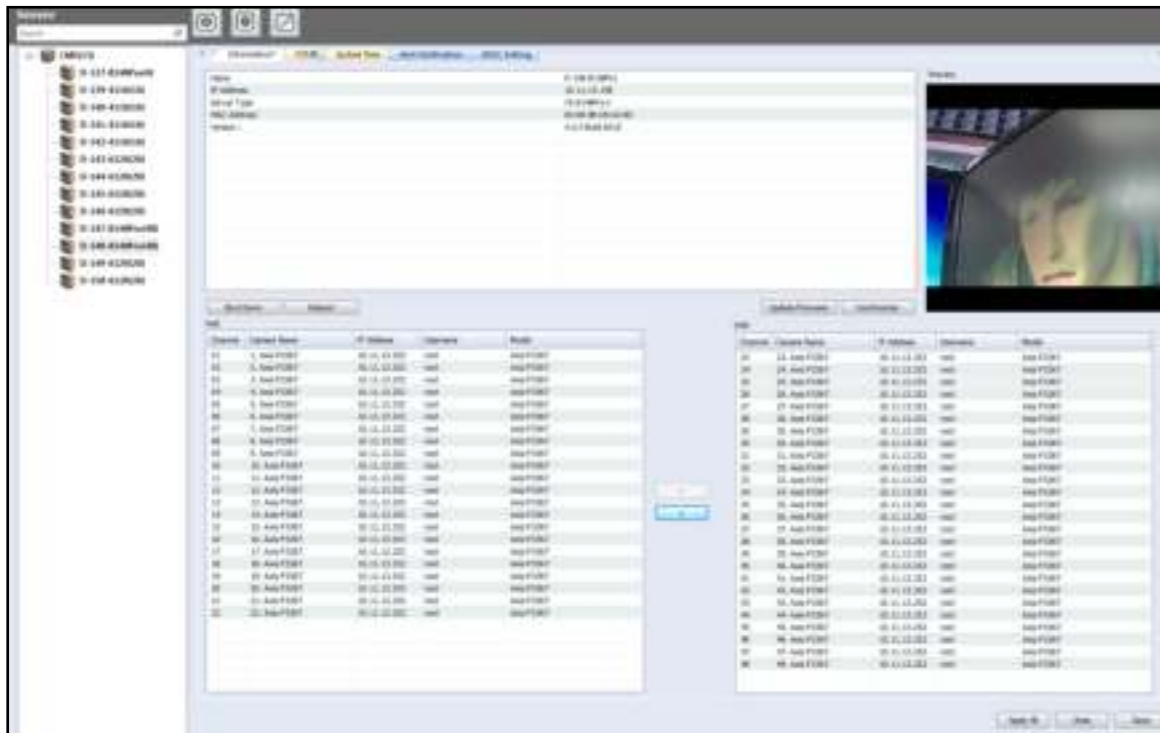
- Server Name: D-148-8148Pro
- IP Address: 10.11.13.148
- Port Number: 80
- Username: admin
- Password: (empty field)
- Retype Password: (empty field)

At the bottom right of the dialog are two buttons: "OK" and "Cancel".

Note: A NVR can only be edited and deleted by administrators of that NVR. Please be sure to type in the administrator username and password in the Edit Server dialog window, or details of cameras and their live view may not be displayed correctly.

3.8.3 Adding/Removing Camera

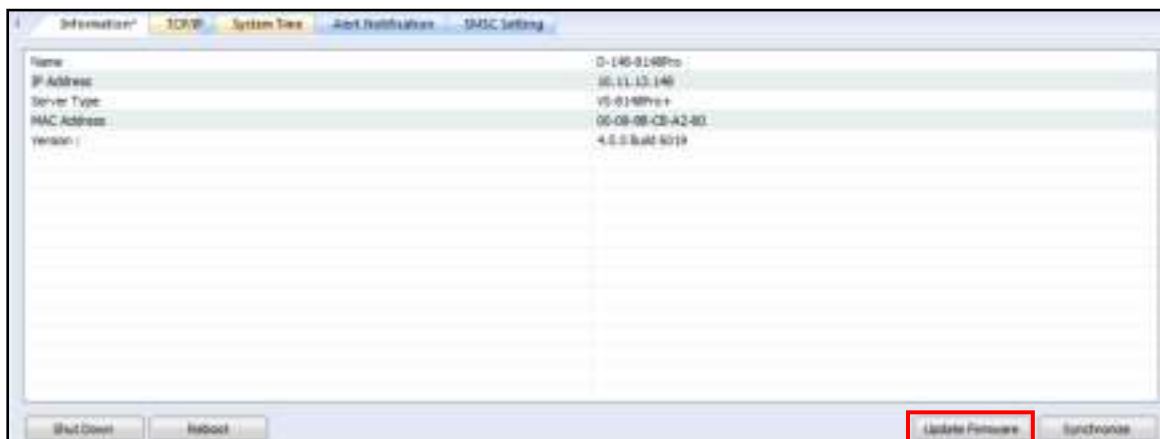
Select an NVR from the list and a list of available cameras will be shown below. Use the left and right arrows to add or remove the cameras to be controlled and monitored by the CMS Client. After applying the settings, the number of cameras connected to the NVR will appear next to the NVR name on the left list.



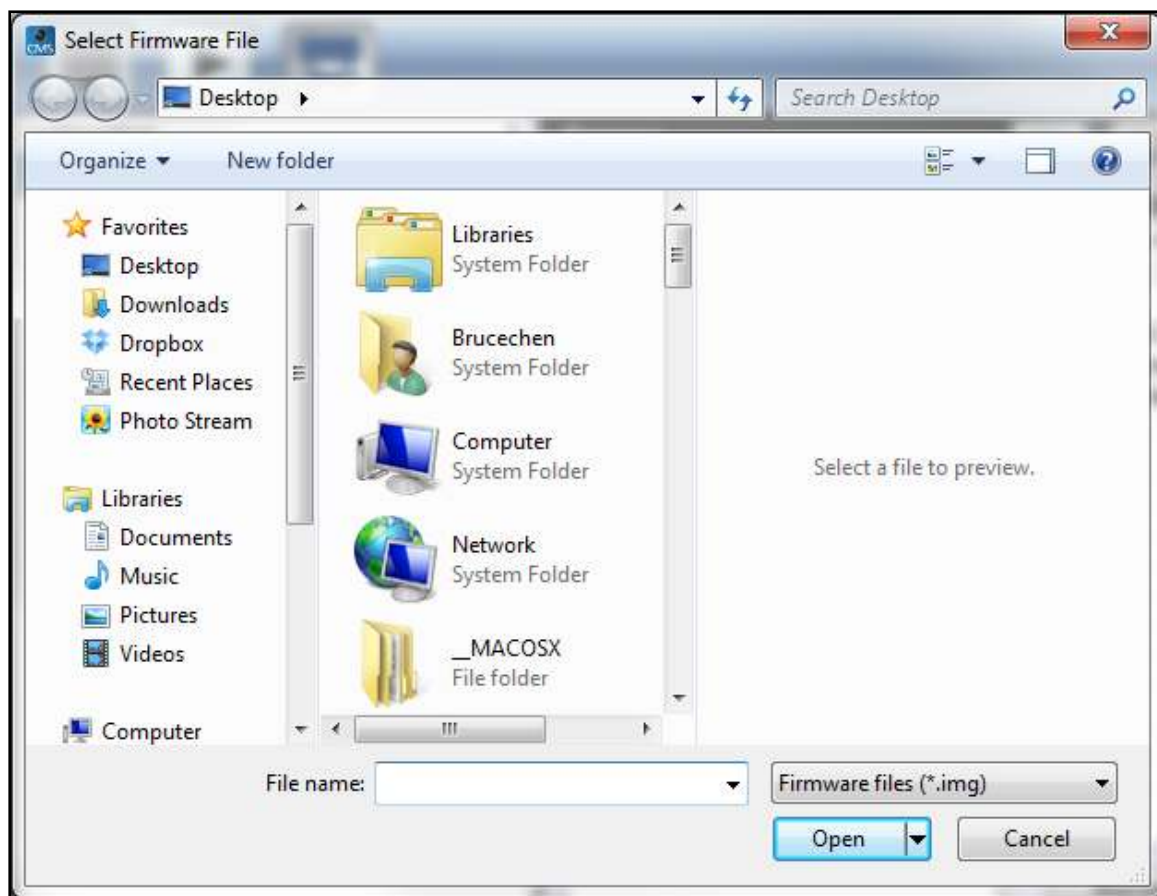
3.8.4 Firmware Update

Follow the steps below to update firmware:

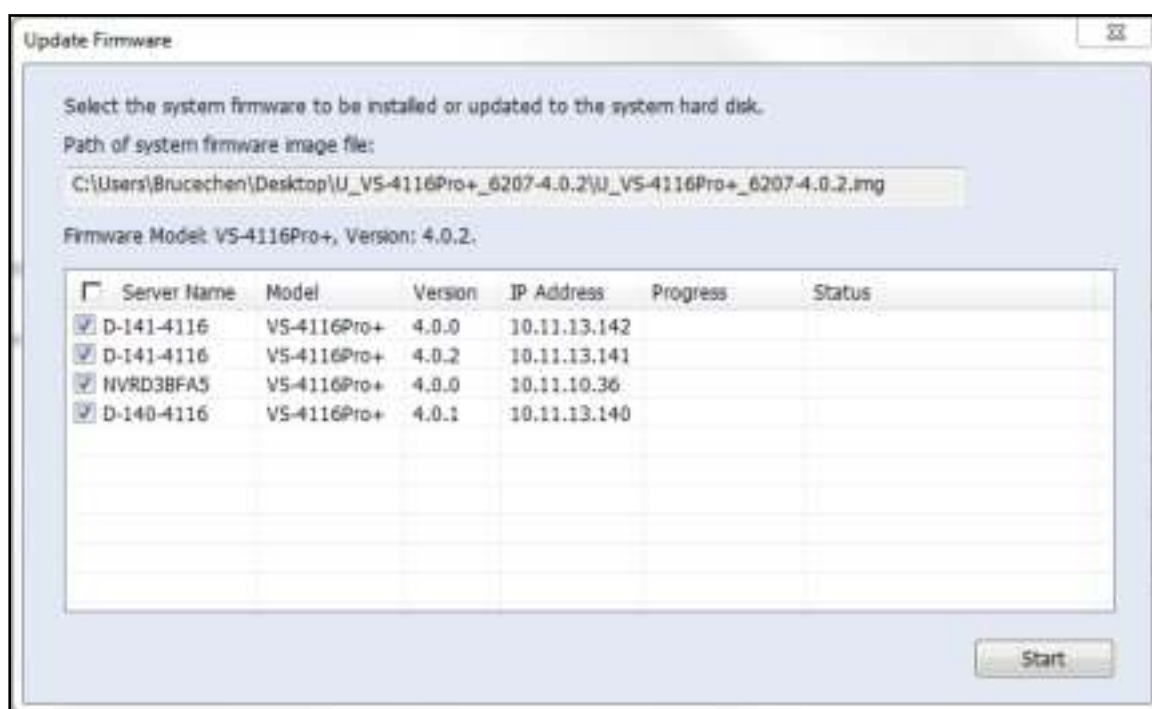
1. Select the NVR for which to update the firmware and click "Update Firmware".



2. Browse and select the firmware image file (*.img) from the local computer.



Tip: You can select to update the firmware of multiple NVR servers at the same time if they are the same model.

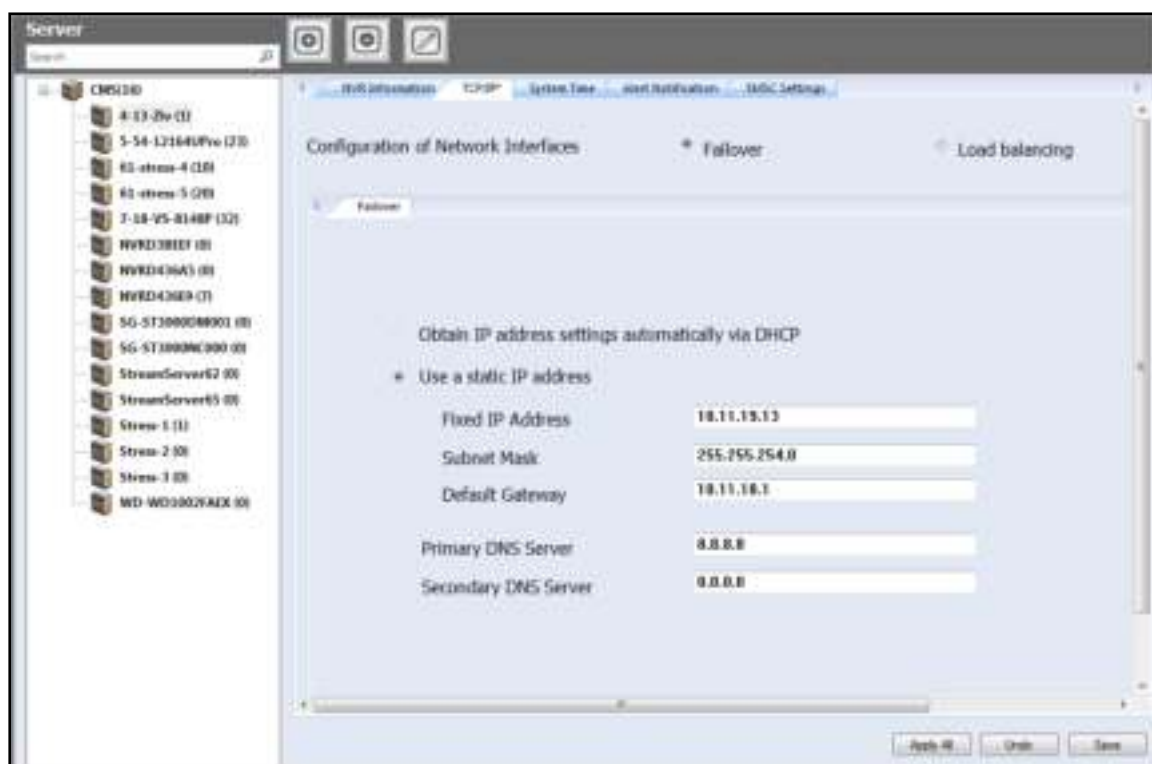


3.8.5 TCP/IP Configuration

The CMS Server supports static IP assignment for all NVRs, and for each NVR, the number of LAN ports can be different. Please note that DHCP is not supported.

Configuring NVR with a Single LAN Port

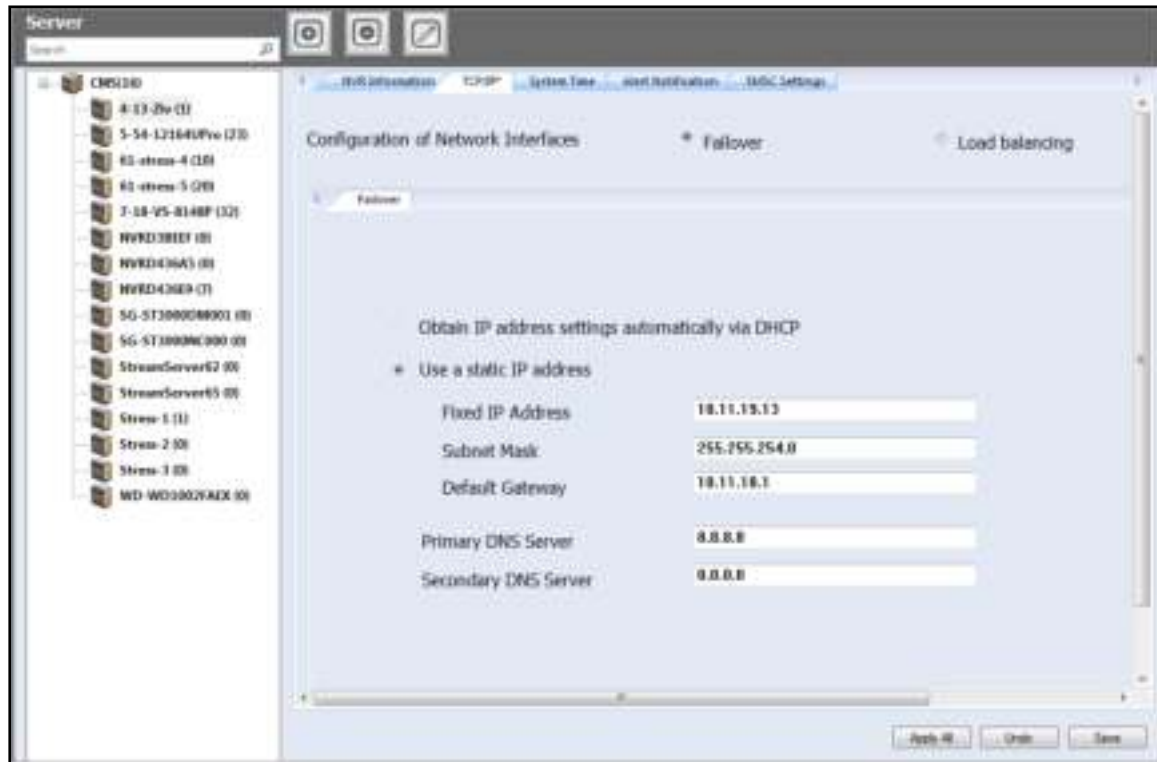
If the NVR supports a single LAN port, select one of the following options to configure the TCP/IP settings of the NVR.



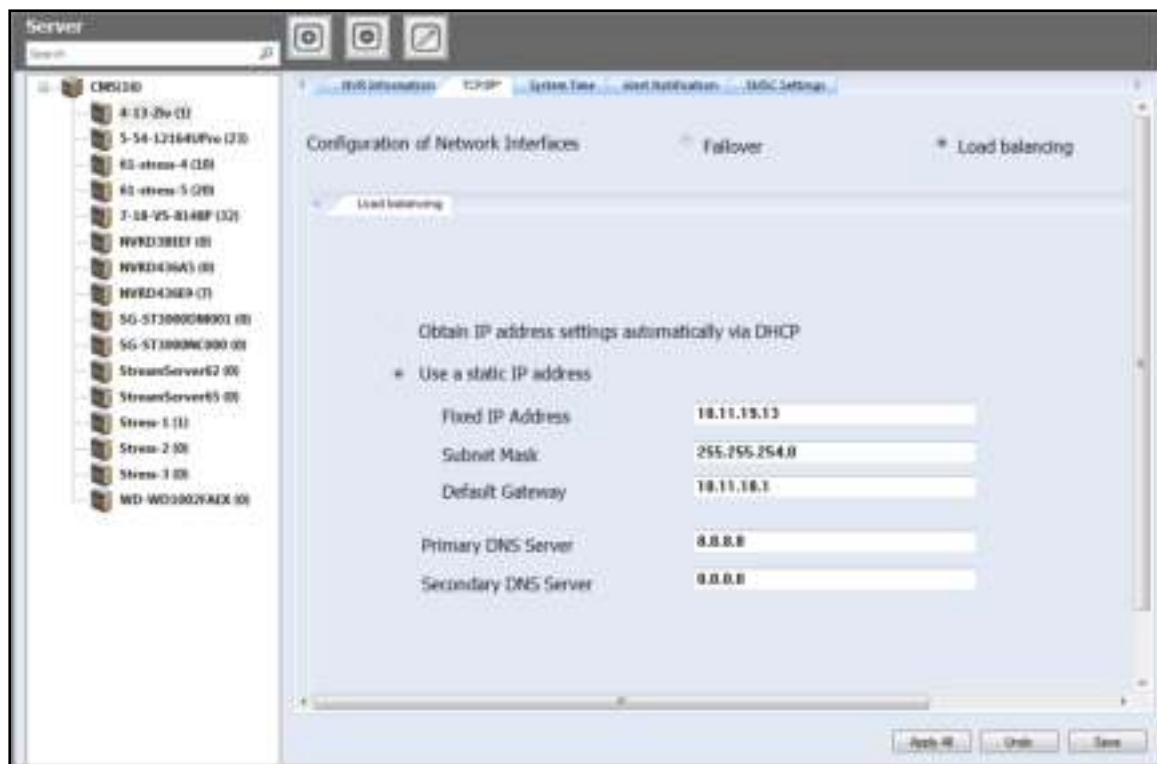
- Use static IP address: To assign a fixed IP to the NVR, enter the IP address, the subnet mask, and the default gateway.
- Primary DNS Server: Enter the IP address of the primary DNS server that provides the DNS service for the NVR on the external network.
- Secondary DNS Server: Enter the IP address of the secondary DNS server that provides the DNS service for the NVR on the external network.

Configuring NVR with Dual LAN Ports

If the NVR supports two LAN ports, select to use failover, load balancing, or standalone setting. To use these features, make sure both LAN ports are connected to the network.

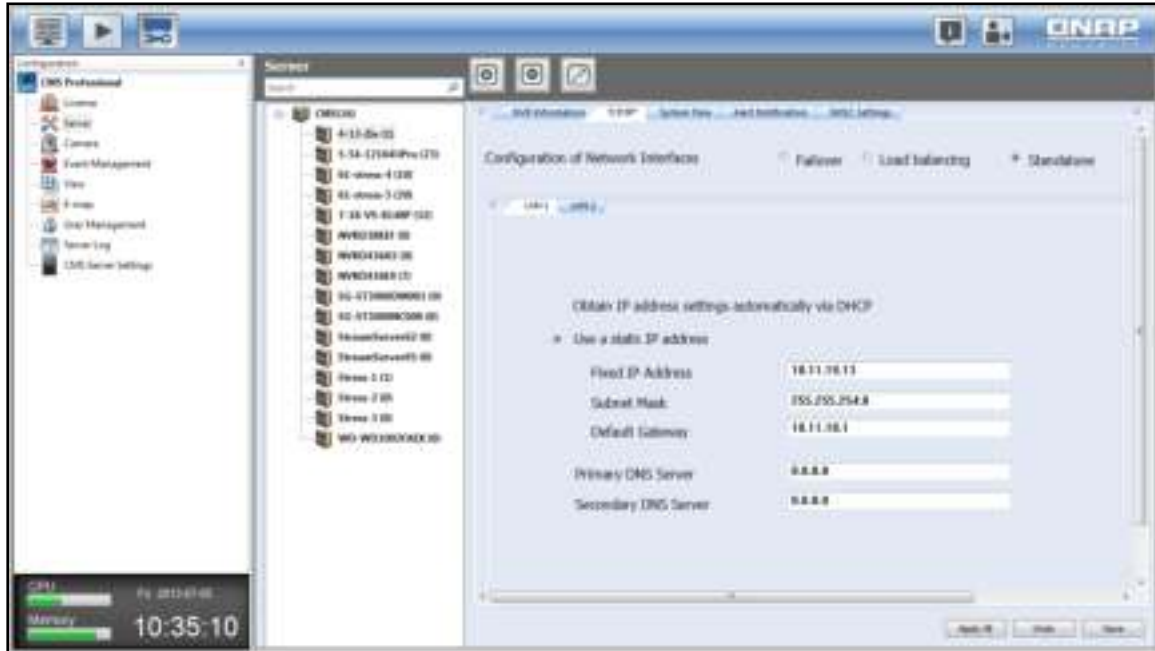


- Failover (Default settings for dual LAN NVR models): Failover refers to the capability of switching over the network transfer port to the redundant port automatically when the primary one fails to avoid network disconnection. When the connection is resumed on the primary network port, the network transfer will be switched over to that port automatically.
- Load balancing: Load balancing refers to the ability to spread network traffic between two or more network interfaces to optimize the network transfer and enhance the system performance.



Note: To optimize the network transfer speed of the NVR in the load balancing mode, use an Ethernet switch and enable 802.3ad (or link aggregation) on the switch ports that the NVR's Gigabit LAN ports are connected to.

- Standalone: Assign different IP settings for each network port. The NVR can be accessed by different workgroups on two subnets. When load balancing is enabled, failover will not work. The DHCP server can only be enabled for the primary network port (LAN 1).



- Use static IP address: To assign a fixed IP to the NVR, enter the IP address, the subnet mask, and the default gateway.
- Primary DNS Server: Enter the IP address of the primary DNS server that provides the DNS service for the NVR on the external network.
- Secondary DNS Server: Enter the IP address of the secondary DNS server that provides the DNS service for the NVR on the external network.

3.8.6 System Time

Set the date, time, and time zone. If the settings are incorrect, the following problems may occur:

- Incorrect time stamps on the video files.
- Incorrect time stamps on the event logs.



Synchronize with an Internet time server automatically

Enable this option to update the date and time of the NVR automatically with an NTP (Network Time Protocol) server. Enter the IP address or the domain name of the NTP server (for example, time.nist.gov or time.windows.com.)

3.8.7 Alert Notification

When a problem occurs (e.g. power outage or a hard disk drive is unplugged,) an alert email will be sent to the specified recipients automatically.

To configure this feature, please set the alert level and specify SMTP server address, SMTP authorization credentials and email addresses of the recipients. To view the details of all the errors and warnings, go to "Logs & Statistics" > "System Event Logs".



Note: It is recommended to send a test email to make sure the mail server settings are configured correctly.

3.8.8 SMSC Settings

Configure the SMSC (Short message service centre) settings to send the SMS text messages to the particular mobile phone numbers when an event is detected by the NVR. The default SMS service provider is Clickatell. Add an SMS service provider by selecting "Add SMS Provider" from the drop-down menu.

After "Add SMS service provider" is selected, enter the name of the SMS provider and the URL template text.

Server

Search

CMSC161

- 4-13-Ziv (1)
- 5-54-12164UPro (2)
- 61-stress-4 (10)
- 61-stress-5 (20)
- 7-18-VS-8148P (12)
- NVRD3888F (0)
- NVRD436A5 (0)
- NVRD436B8 (7)
- SG-ST3000CM001 (0)
- SG-ST3000CM000 (0)
- StreamServer62 (0)
- StreamServer63 (0)
- Stream-1 (1)
- Stream-2 (0)
- Stream-3 (0)
- WD-WD1002AER (0)

Information | TCP/IP | System Time | Start Notifications | **SMS Settings**

SMS Service Provider: Clickatell

[SMS Server Settings]

☐ Enable SSL Connection

SSL Port: 443

SMS Server Login Name: clickatell

SMS Server Login Password: test

SMS Server API_ID:

[SMS Notification Settings]

Country Code: Albania (+355)

Cell Phone No. 1: +355 98885473532 (Do n

Cell Phone No. 2: +355 23532535325 (Do n

☐ Send a test SMS message (If the SMSC settings are incorrect, you will not be able to receive it)

Send SMS text messages when the following events take place:

☐ Motion is detected on an IP camera

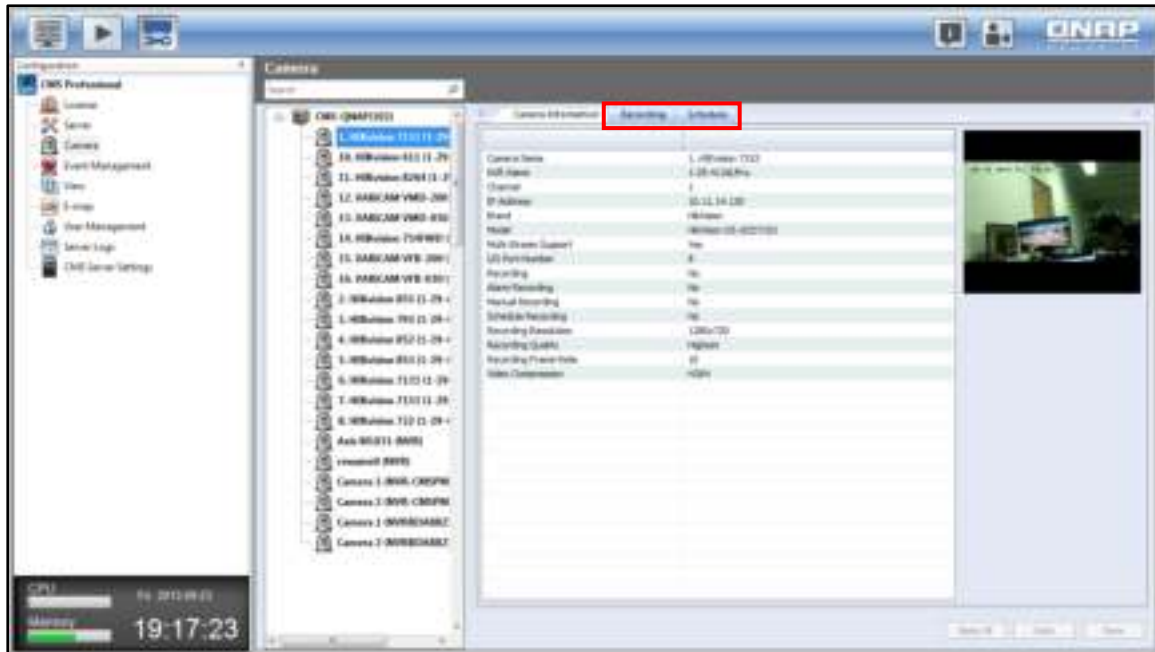
Apply All Cancel Save

Note:

- Please always follow the standard published by the SMS service provider to configure the SMS settings.
- Please send a test SMS to verify that the settings are correct.
- Go to "Camera Settings" > "Alarm Settings" > "Advanced Mode" to edit the SMS settings, or select to use the "Traditional Mode" and configure the SMS settings on this page.
- It is recommended to send a test email to make sure the mail server settings are configured correctly.

3.9 Camera

Information of the cameras being controlled by the CMS is shown on this page. The information shown on this page includes the camera name, the NVR that the camera belongs to, IP address, model, and the live video. Recording settings and schedules of the cameras can also be managed on this page.



Under the "Recording" tab, you can configure the video compression format, screen resolution, frame rate, and video quality, and select to enable or disable audio recording and manual recording for the configured channel.

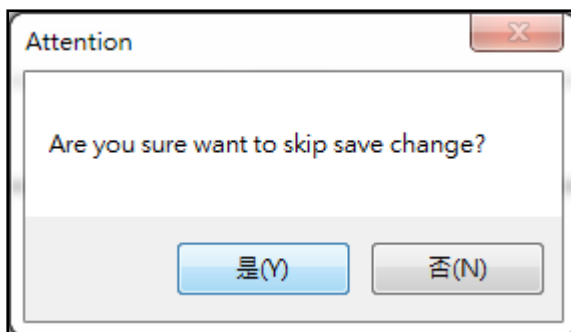
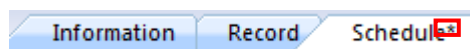


- Video compression: Select the compression format of the recording files.
- Resolution: Select the recording resolution of the camera. The higher the resolution, the clearer the video will be, but the larger the hard disk space will be used.
- Frame rate: Select the number of recording images per second. Please note that the actual frame rate may vary according to traffic conditions.
- Video quality: Select the video recording quality used by the camera. The higher the resolution, the more clear the video will be, but the larger the hard disk space will be used
- Enable audio recording (optional): Check this option to enable audio recording.
- Enable manual recording: After this option is checked, you can choose to start or stop the recording manually on the live view page.

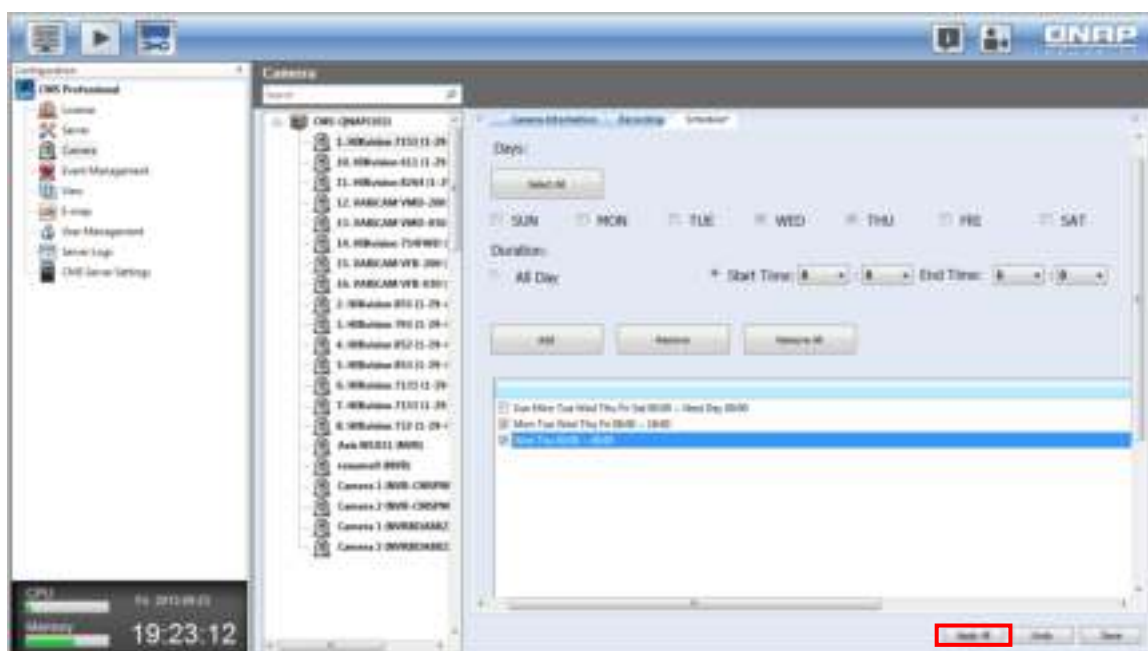
To create a recording schedule under the "Schedule" tab, specify the days and duration for recording and click "Add".



Note: When any changes have been made, an asterisk will appear on the tab. You will be prompted to save the changes when switching to a different tab.

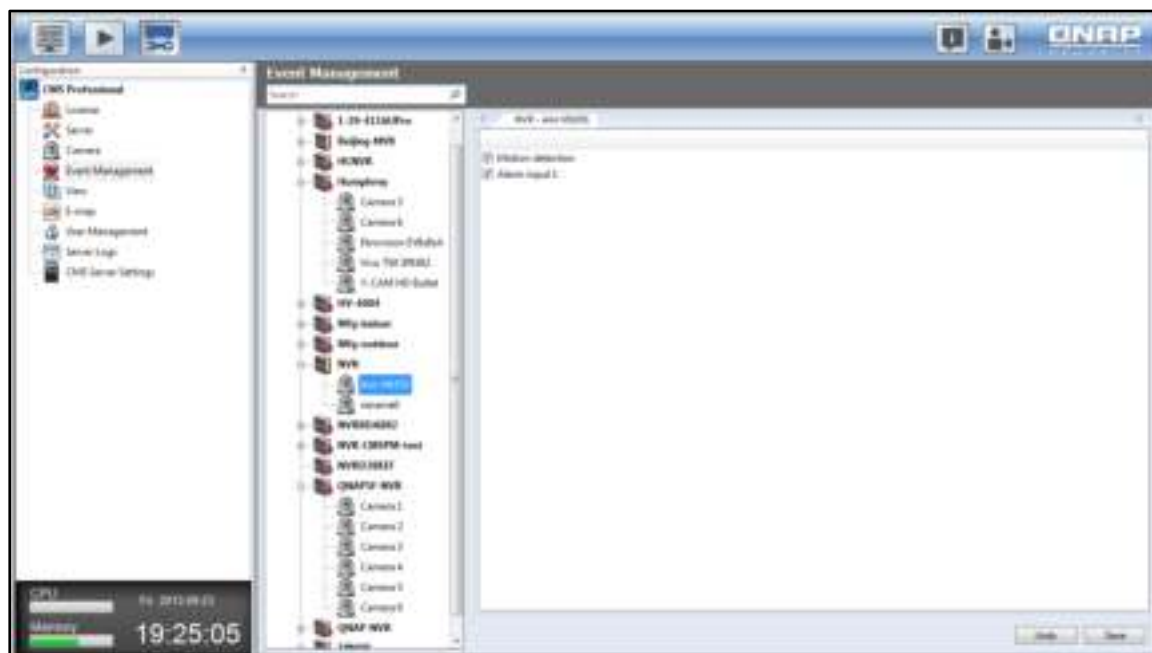


Note: By clicking "Apply to all", the changes made will be applied to all cameras. For cameras that do not support the selected functions, the changes made will not apply to them even if "Apply to all" is clicked.



3.10 Event Management

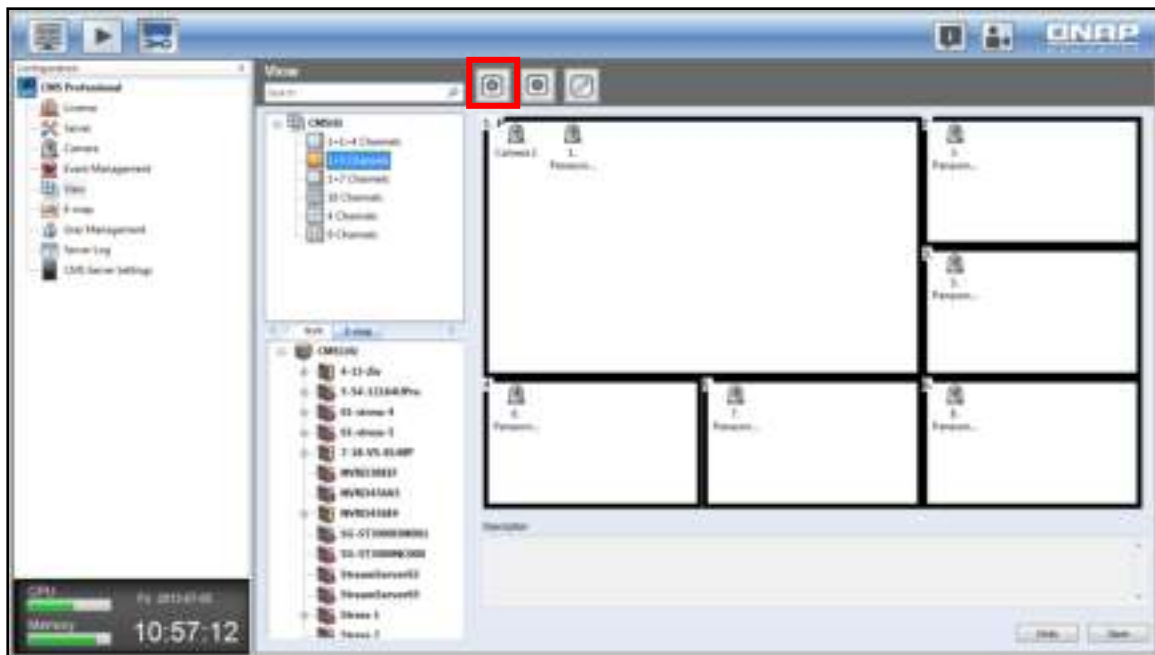
The CMS Server can be set to receive NVR alerts (such as motion detection events or events triggered by alarm inputs). After checking these options, click “Save” to save the settings or “Undo” to go back to the previous step.



Note: The alarm settings must be configured on the NVR first. Then, go to Event Management of the CMS system to enable the alarm input of the camera. So, the CMS system can receive the alarms from the NVR. Please refer to [Chapter 7-10 \(FAQ\)](#) for details.

3.11 View


The administrator can define the view layout in view configuration.



After choosing a view layout, enter the name and description of the view. Click "OK" to confirm.



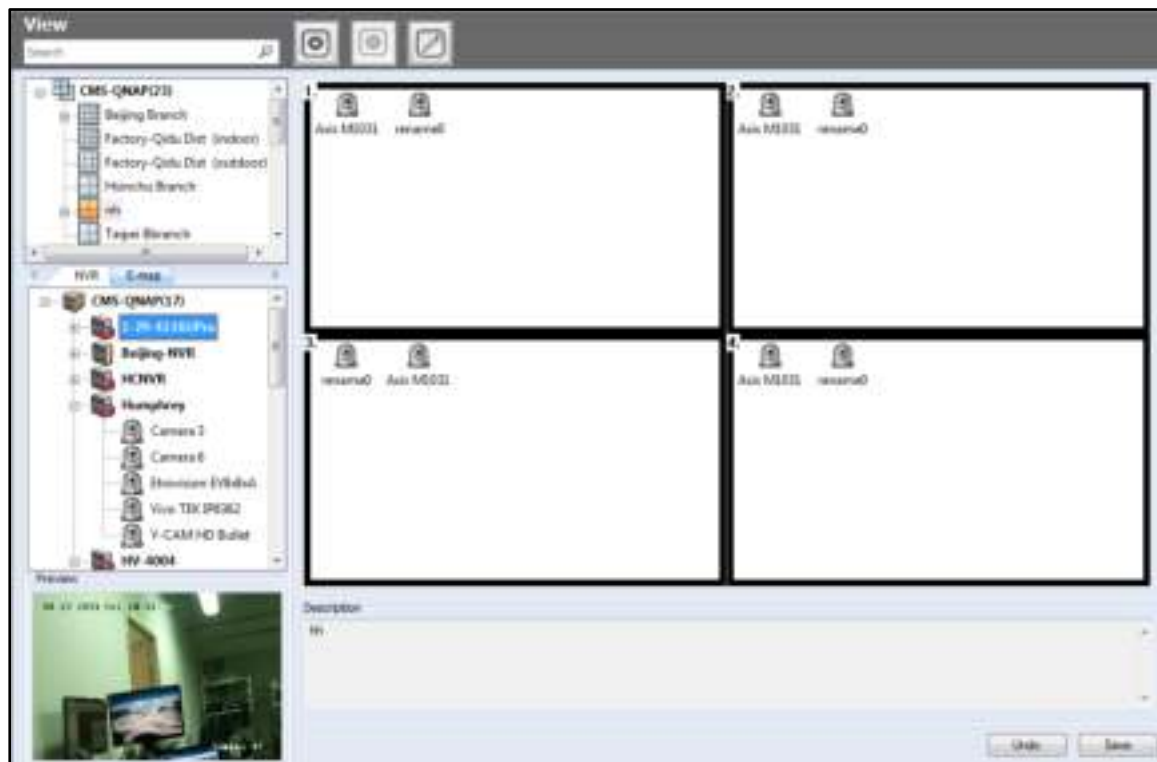
Add View ✕

Style:  4 Channels ▼

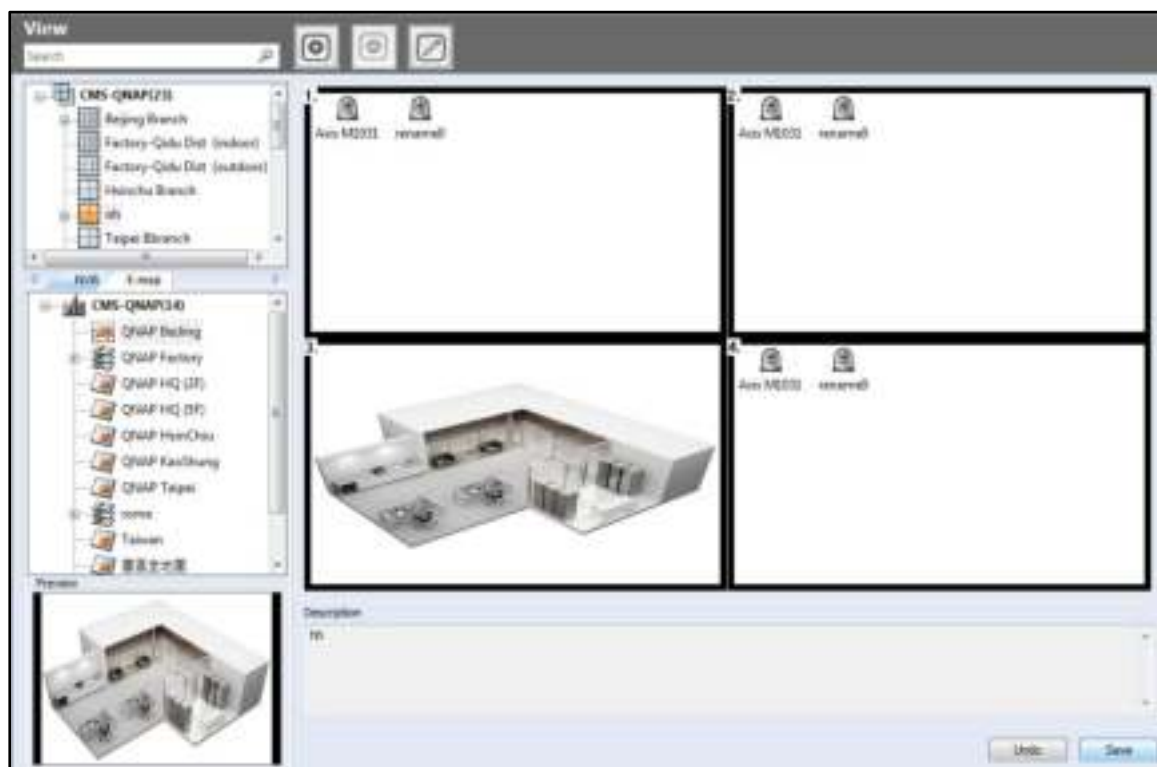
View Name:

Description:

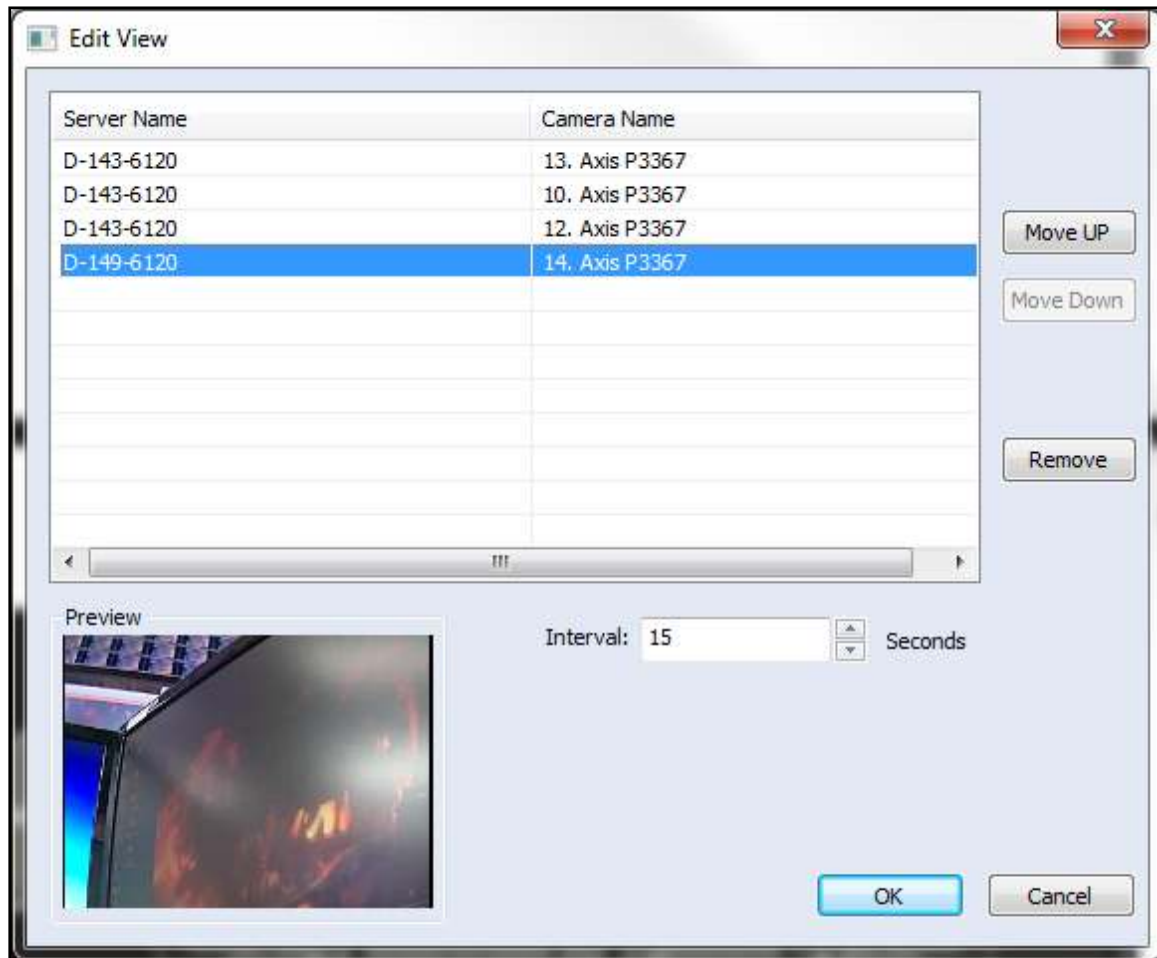
Then, drag the cameras in the NVR list on the left to the channel window on the right.



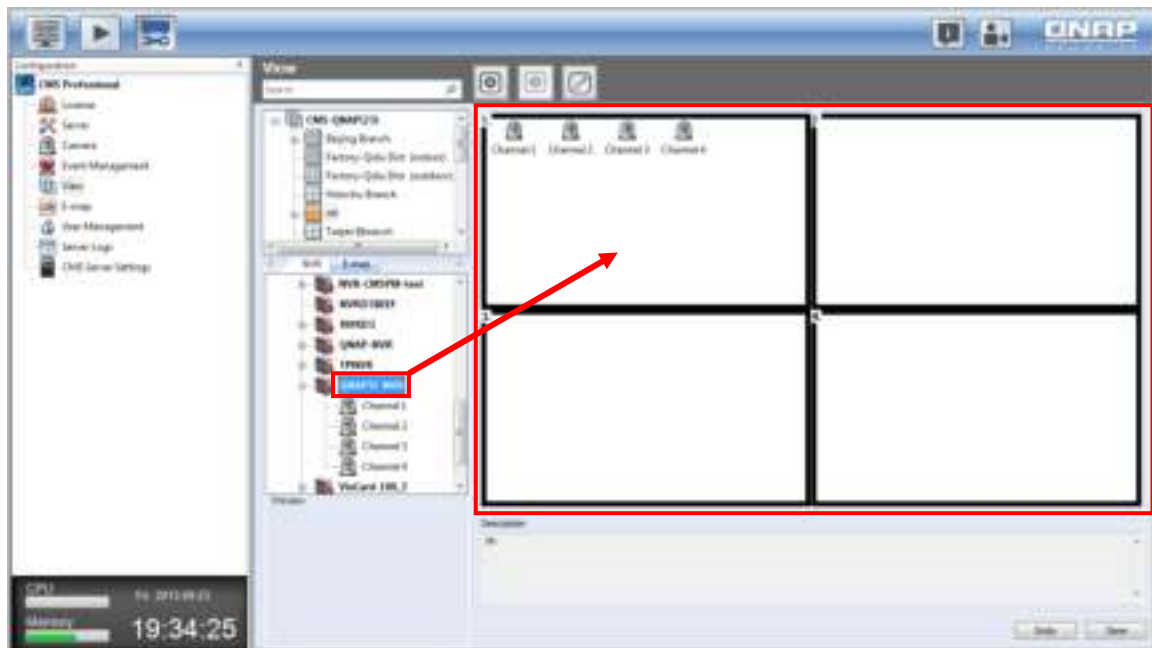
The E-map(s) can also be inserted.



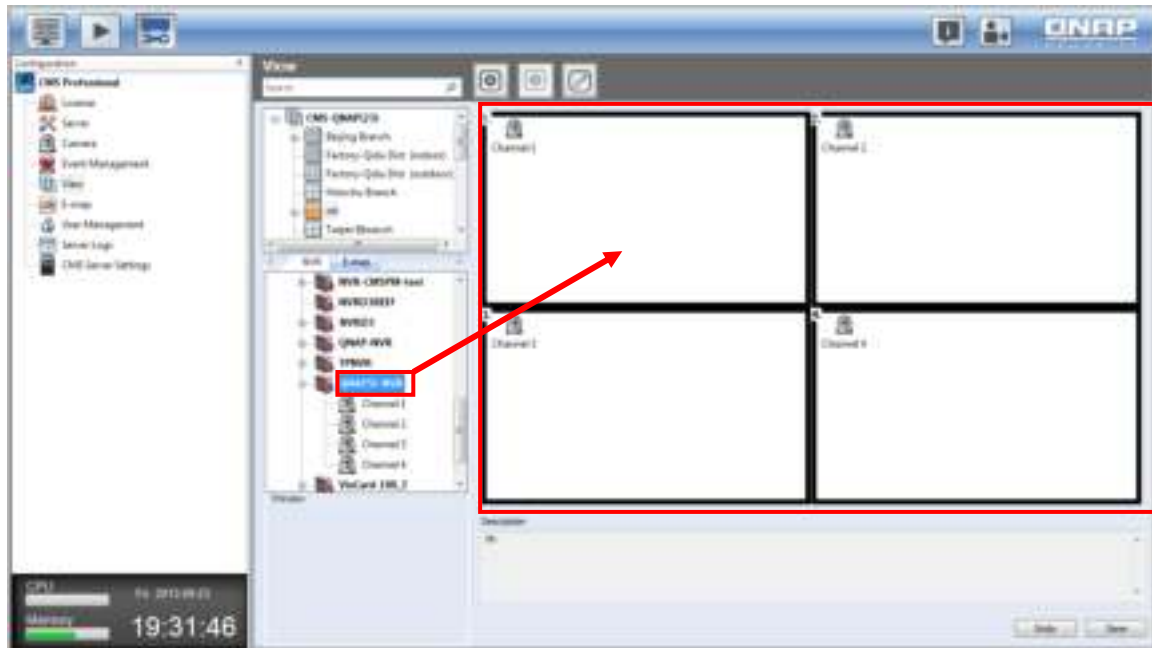
Double click the window to adjust the carousel order and interval, and edit the camera to be viewed. The live view supports the carousel function. In the description field of each layout, Server name and the order of each placed camera will be listed. Adjust the carousel order and interval, and preview the live video.



Note: Drag an NVR to the blank channel window, and all the cameras of the chosen NVR will be played in the sequential mode in that channel window.



Tip: Press and hold the “Shift” key and drag an NVR to a channel window, and its cameras will be inserted to each channel window one by one. If the number of the remaining channel window is less than the total number of cameras from the NVR, those additional cameras will not be added.



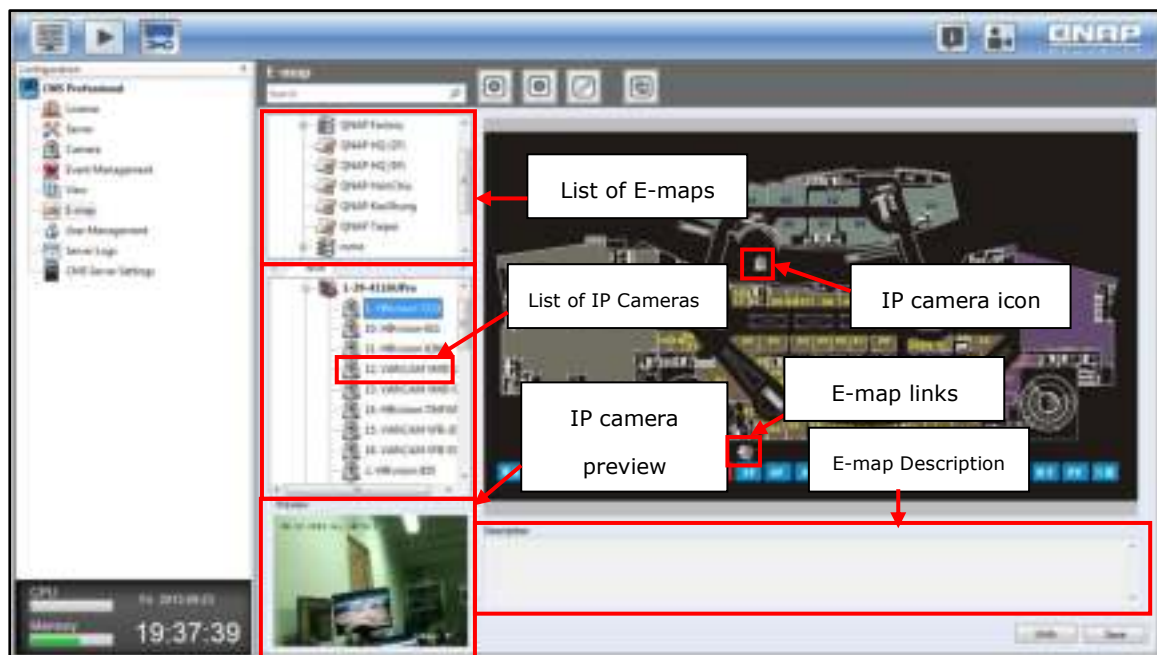
3.12 E-map

The E-map feature of the NVR is provided for users to upload electronic maps to the system to indicate the locations of the IP cameras. Users can drag and drop the camera icons* to the E-map and enable event alert to receive instant notification when an event occurs to the IP camera.













* To set up an IP camera on the E-map, please complete the IP camera settings on the Alarm Settings page on the NVR first.

An E-map example is shown below. The NVR provides a default E-map. Add or remove the E-maps whenever necessary.

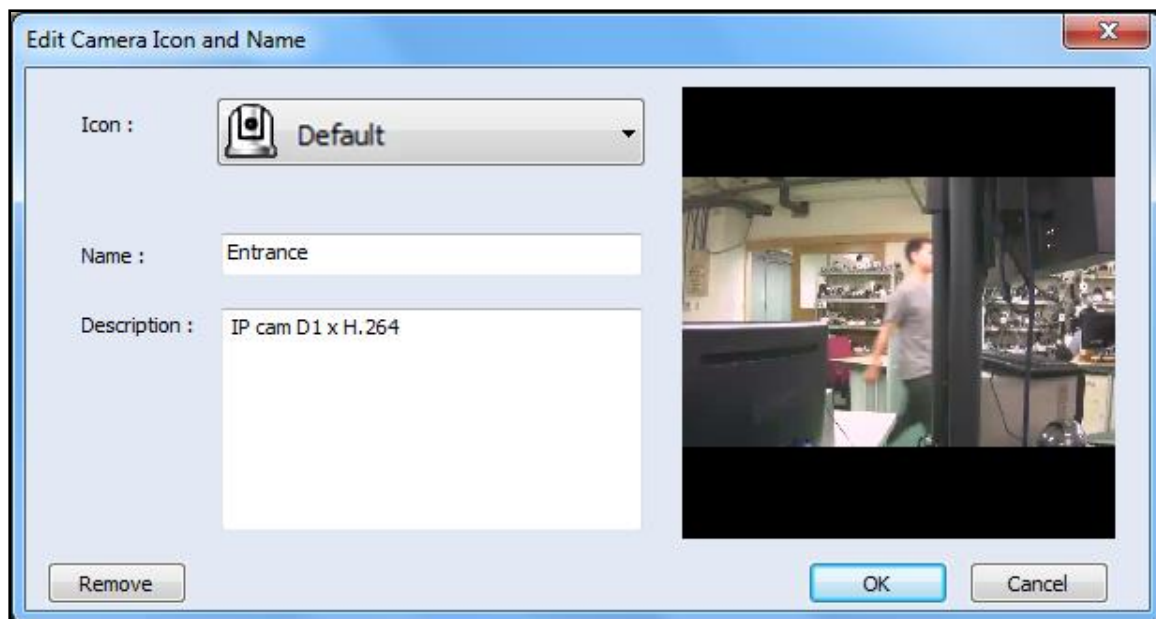
Note: Please login the CMS Client as an administrator to edit and view the E-maps.




Icons and Description

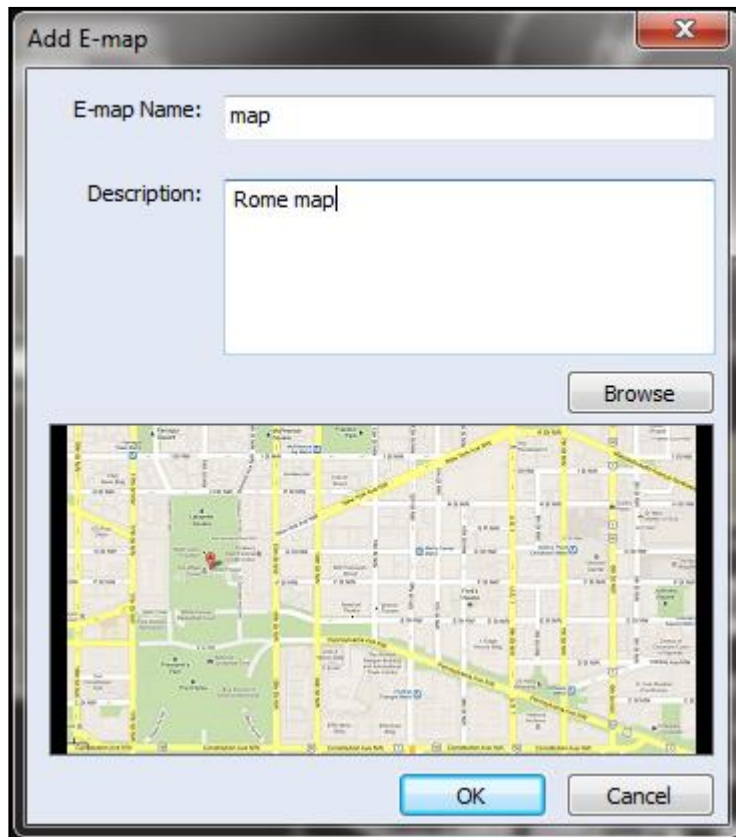
Icon	Description
	Add an E-map.
	Remove an E-map.
	Edit the name of an E-map.
	Batch-upload E-maps.
	Icon for a set of E-maps.
	Single-layer E-map: Click  to select a single-layer E-map. When an E-map is selected, the icon will become  .
	An E-map symbol on the E-map. This symbol on the E-map serves as a link to another E-map. This is particularly convenient for users to switch between E-maps.
	An NVR icon used to indicate the location of an NVR. The NVR icon is only provided for users to pinpoint a NVR location on the map.
	Icon for a PTZ IP camera.
	Icon for a fixed body or fixed dome IP camera. After dragging the icon to an E-map, right click the camera icon to change the icon direction or delete the icon from the E-map.



Tip: Double click a camera icon on the E-map to change its icon, name, or description. For the NVR, double click a NVR icon on the E-map to change its name or description, but not its icon.

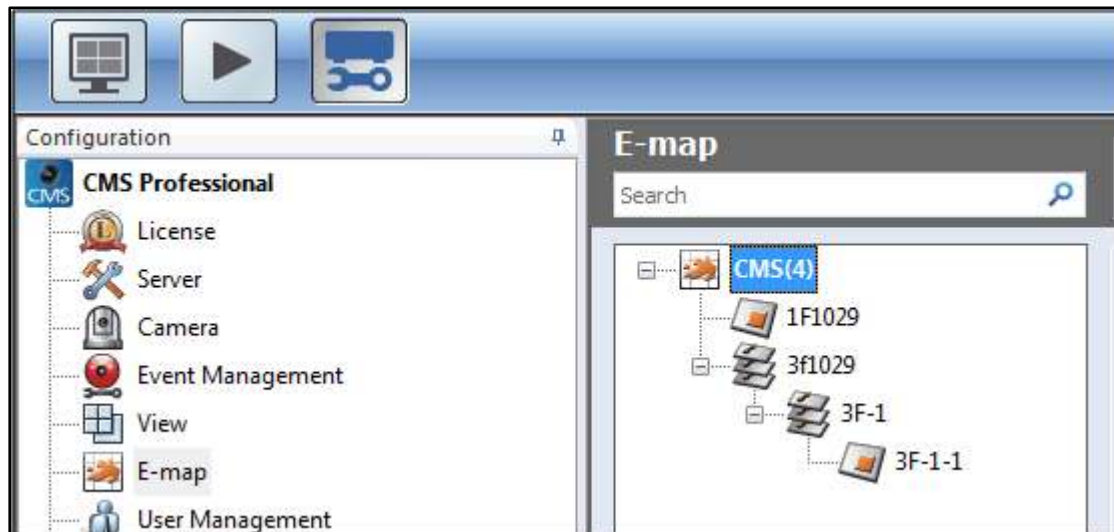


3.12.1 Adding E-map

To add an E-map to indicate the location of an IP camera, click  to enable the Edit mode and enter the map name and description. Browse and select the image file for the map and click "OK".




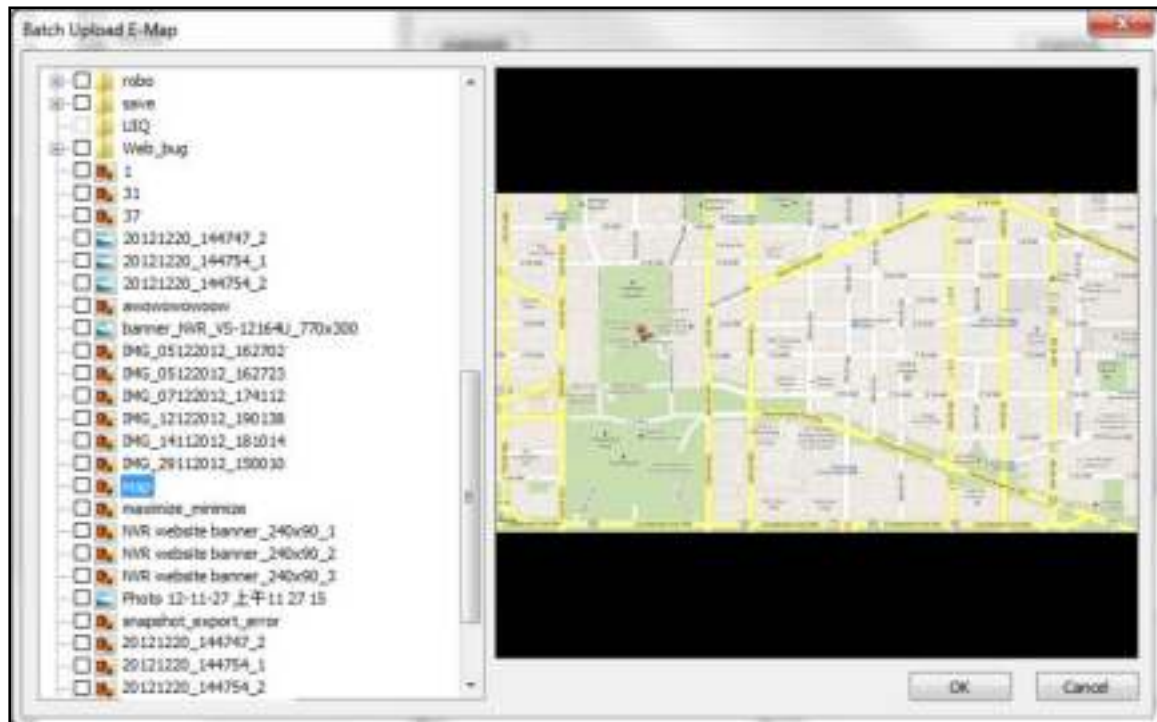
To add an E-map under another E-map, e.g. 1F-1, click the E-map icon at the upper layer, e.g. 1F1029, and click . After adding a lower layer E-map, the E-map icon at the upper layer will change to .




Note: After a lower layer E-map is added, you will be automatically directed back to the upper layer E-map icon to add multiple E-maps for the same upper layer.

Batch-uploading E-maps





Click  to batch-upload multiple E-maps to the CMS Server. Select the image files or directory on the left and click "OK" to upload the E-maps.



3.12.2 Editing an E-map Name

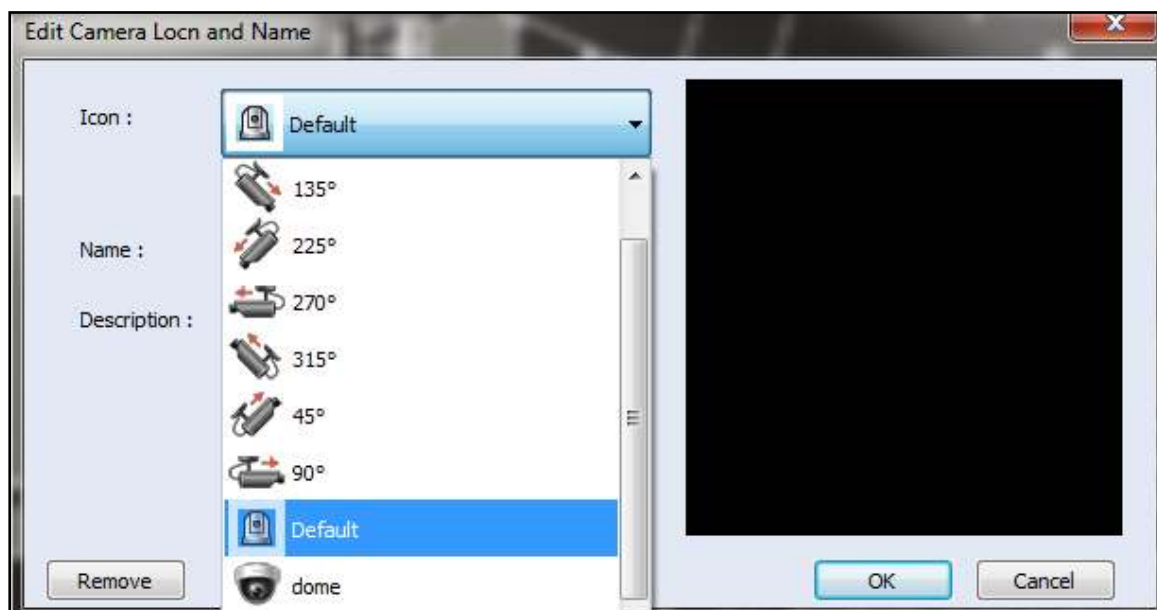
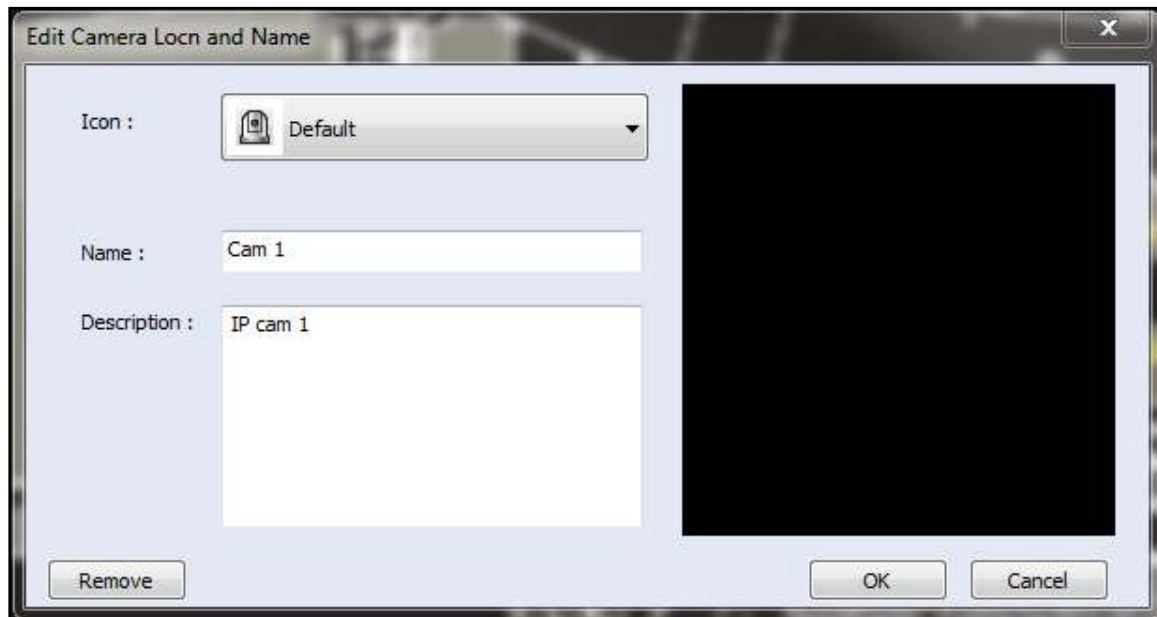
To edit an E-map name, select the E-map and click . Enter the new name and description, and click "OK". To change the picture of the E-map, re-upload the picture and then click "OK".

3.12.3 Deleting E-map

To delete an E-map, select the map icon , and click . To delete a set of E-maps under the same level, select the map set icon , and click .


3.12.4 Editing IP Camera on E-map

After uploading the E-map and adding the cameras to the map, double click the IP camera icon to configure the cameras.



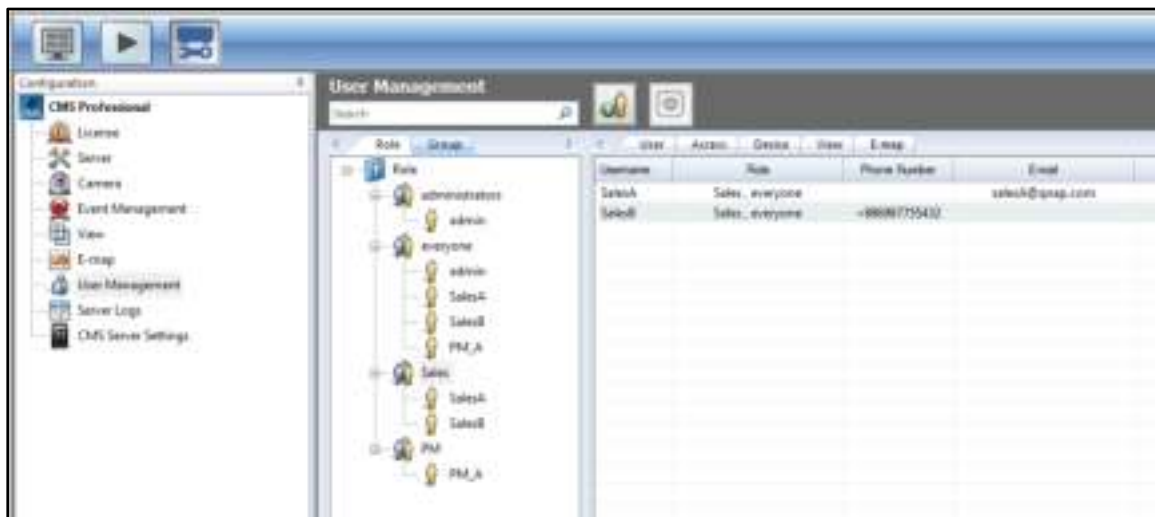
The icon style and name, font color, background color, description, etc. can be set. Please use the "Remove" button at the lower left corner to remove cameras.

The following is the icon and description of the camera alert icon displayed on the E-map:

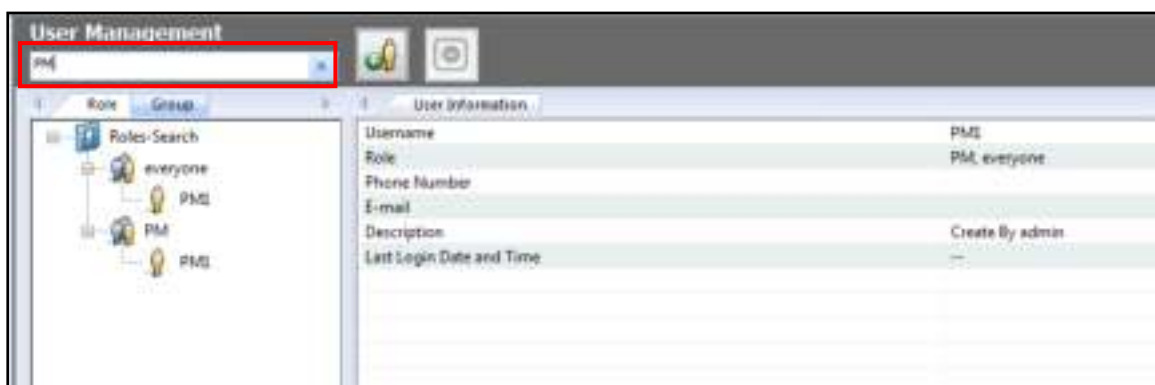
Icon	Description
	Camera alert.

3.13 User Management

The CMS system provides secure user permission management. Two user categories are supported for this feature: role and group. For the role, appropriate permissions can be assigned for monitoring, playback, and system management functions, based on its positions and responsibilities. For the group, all the users are simply categorized for better classification and identification.



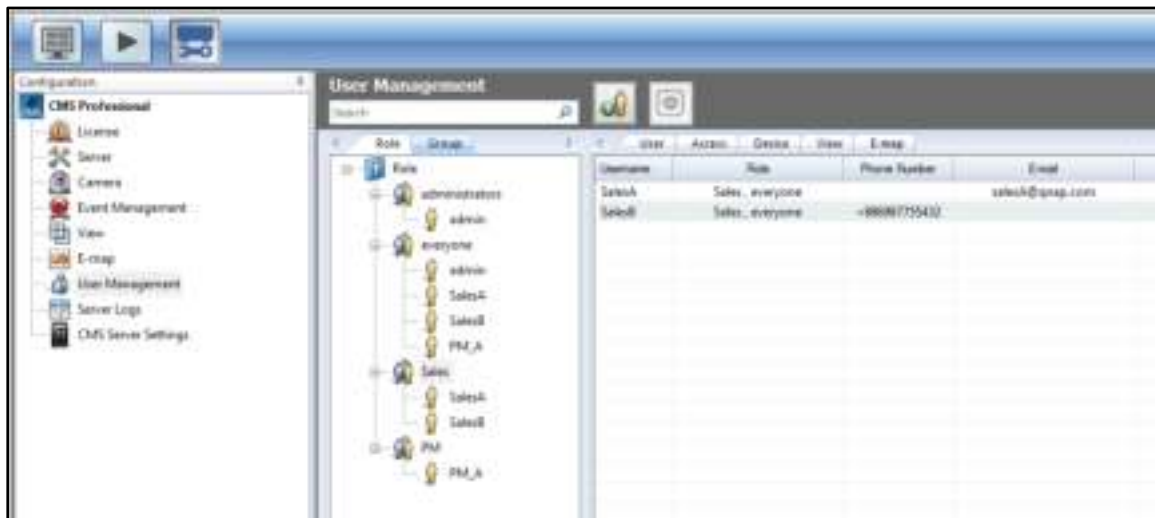
Note: The keywords entered in the search box on top left side of the page are case-sensitive.



Note: To delete a user under Role/Group, please do so in the user list under each role/group and not on the user information page.

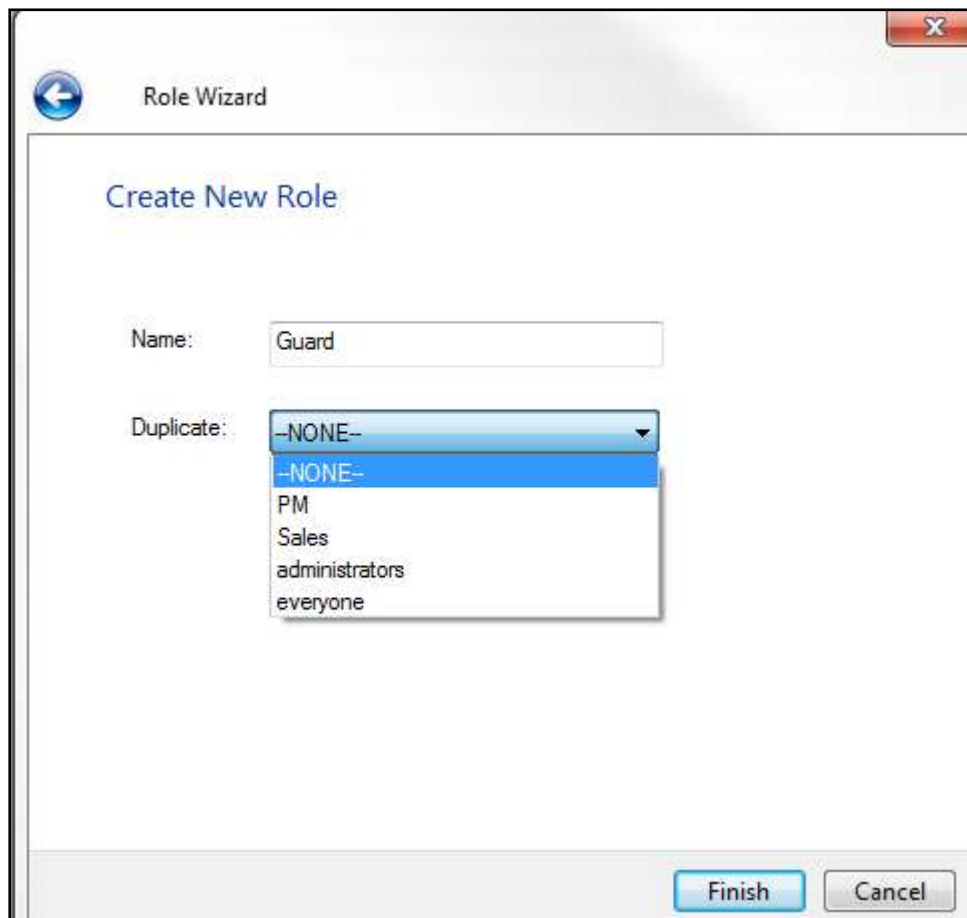
3.13.1 Role Management

Assign users to their role based on their responsibility and specify permissions for their role on this page.



Creating a new role

To create a new role, click

The screenshot shows a 'Role Wizard' dialog box with a title bar containing a back arrow and a close button. The main content area is titled 'Create New Role'. It features a 'Name:' label followed by a text input field containing the word 'Guard'. Below this is a 'Duplicate:' label followed by a dropdown menu. The dropdown menu is open, showing a list of options: '-NONE-' (highlighted in blue), '-NONE-', 'PM', 'Sales', 'administrators', and 'everyone'. At the bottom right of the dialog are two buttons: 'Finish' and 'Cancel'.

Enter a name for the role and copy the permission attributes, such as accessing/editing the NVR, camera, display mode and E-map permissions, of the existing roles. Click "Finish" to save the changes.

Deleting a role

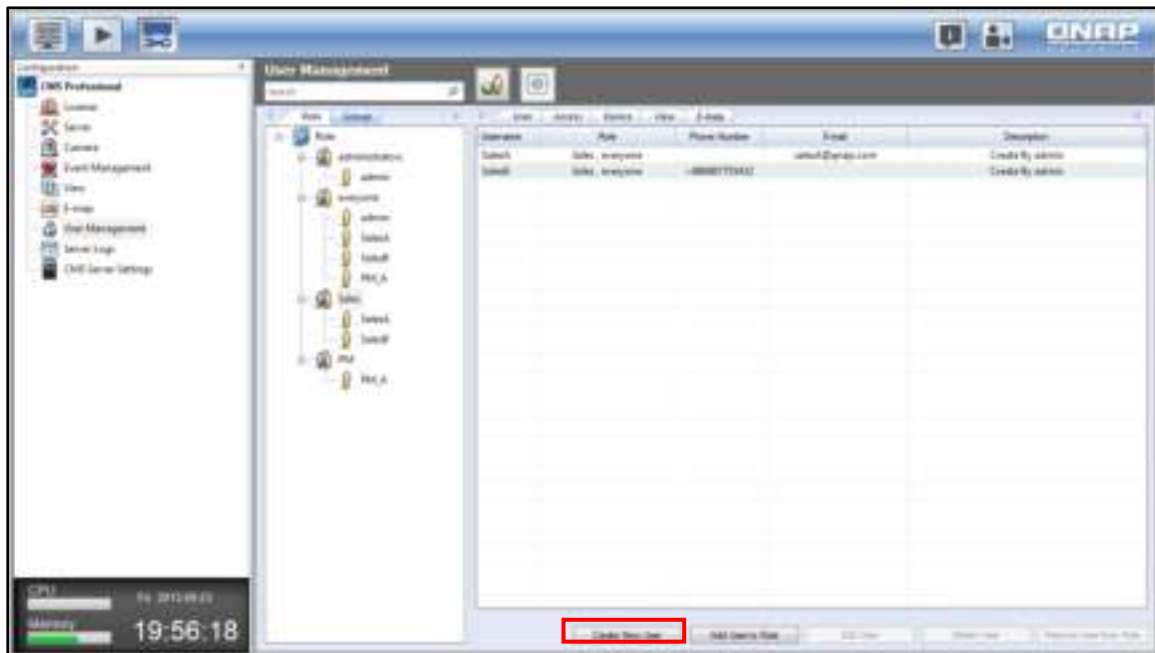
To delete a role, select the role on the list to the left and click



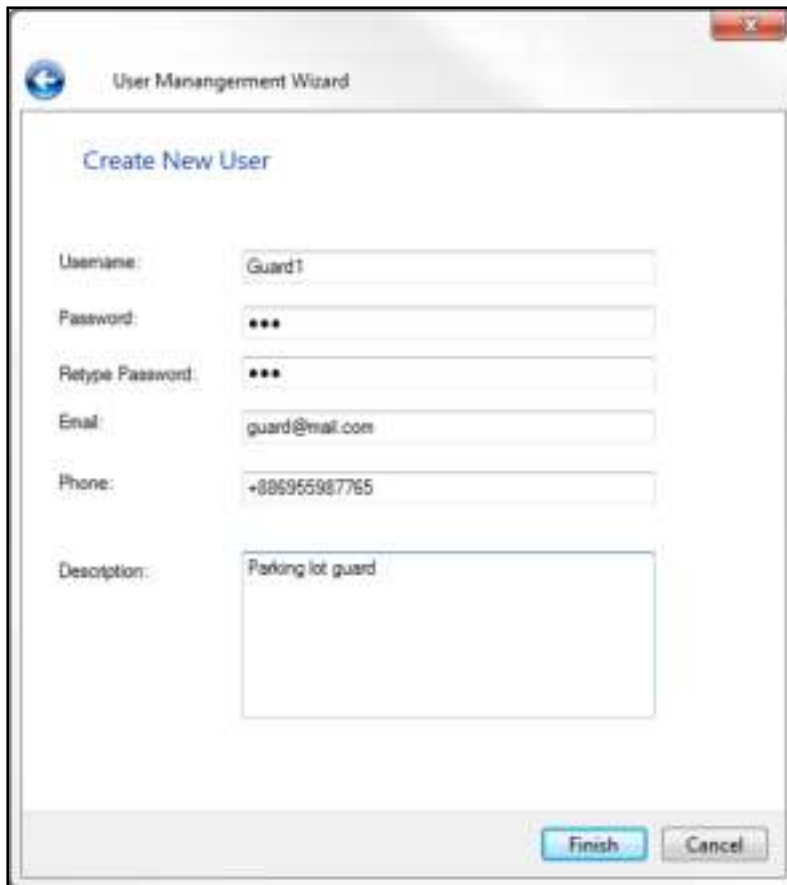
Note: A role cannot be deleted unless all users under that role are deleted. Please be sure to delete all users under a role before deleting that role.

Creating new user(s) under the role

Select a role and click "Add User".



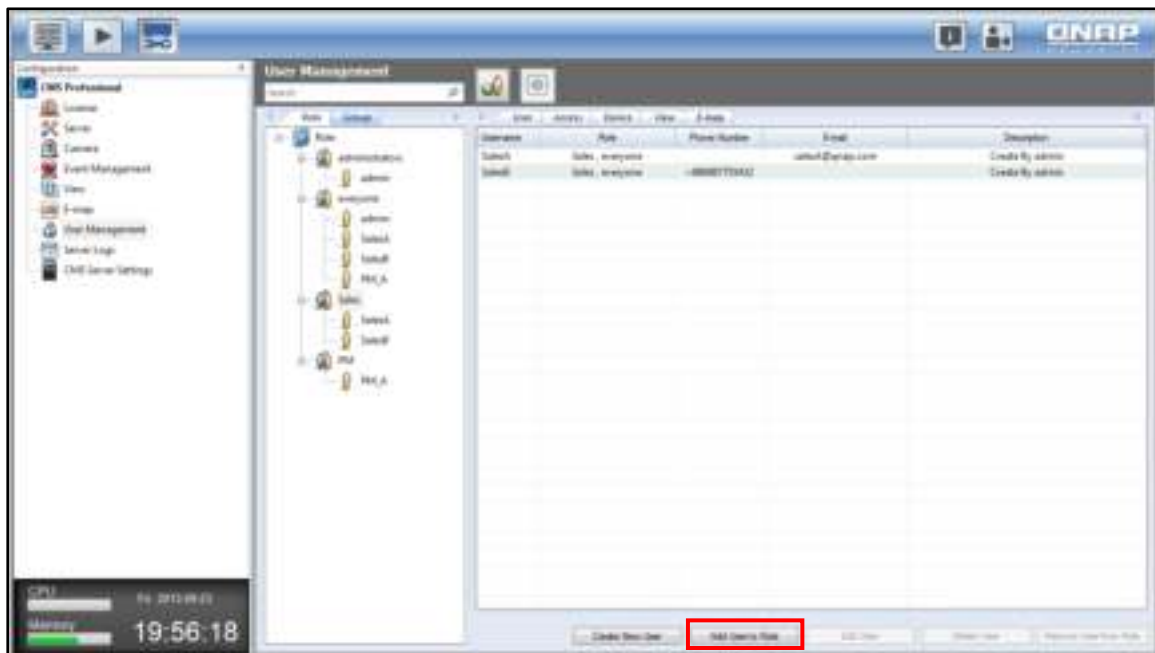
Enter all the fields in the User Management Wizard and the new user will appear under its perspective role.

The image shows a screenshot of a software window titled "User Management Wizard". Inside the window, there is a section titled "Create New User". Below this title, there are several input fields with labels to their left: "Username:" with the value "Guard1", "Password:" with three asterisks, "Retype Password:" with three asterisks, "Email:" with the value "guard@mail.com", "Phone:" with the value "+886955987765", and "Description:" with the value "Parking lot guard". At the bottom right of the window, there are two buttons: "Finish" and "Cancel".

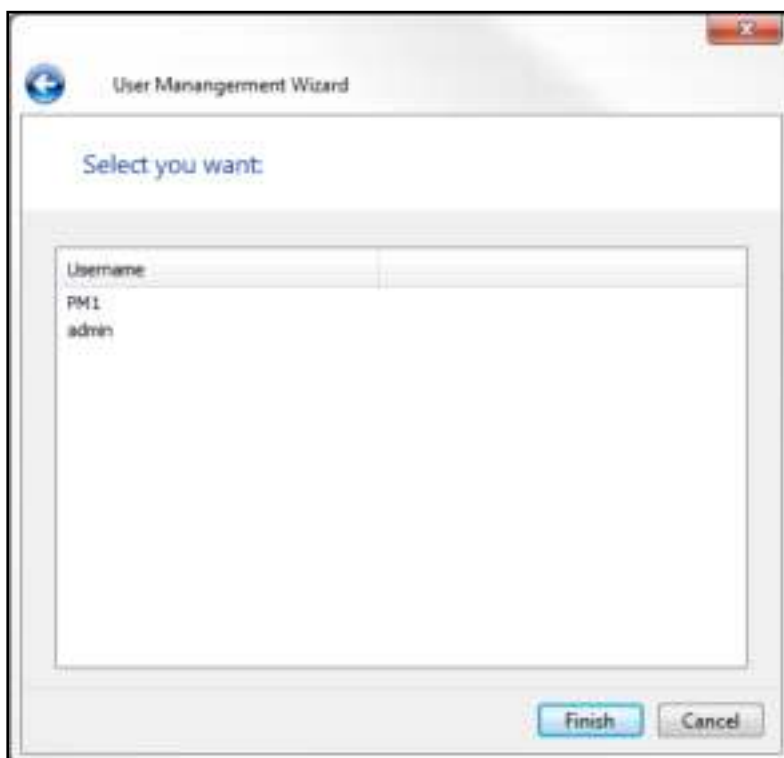
- Username: The user name must be 1 to 32 characters in length. It supports alphabets (A-Z), numbers (0-9), and underscores (_). It is case-insensitive and supports double-byte characters, such as Chinese, Japanese, and Korean but cannot be a pure number or contain the following characters:
"/ \ [] : ; | = , + * ? < > ` ' "
- Password: The password is case-sensitive and the maximum length is 16 characters. It is recommended to use a password of at least 6 characters.
- Other fields: Please finish the remaining fields, such as email, phone number and description.

Adding an existing user to the role

To quickly add existing users to a different role, simply choose a role, click "Add User to Role" and click "OK".



Newly added users will be listed in the User Management Wizard. Click "Finish" to save the changes.

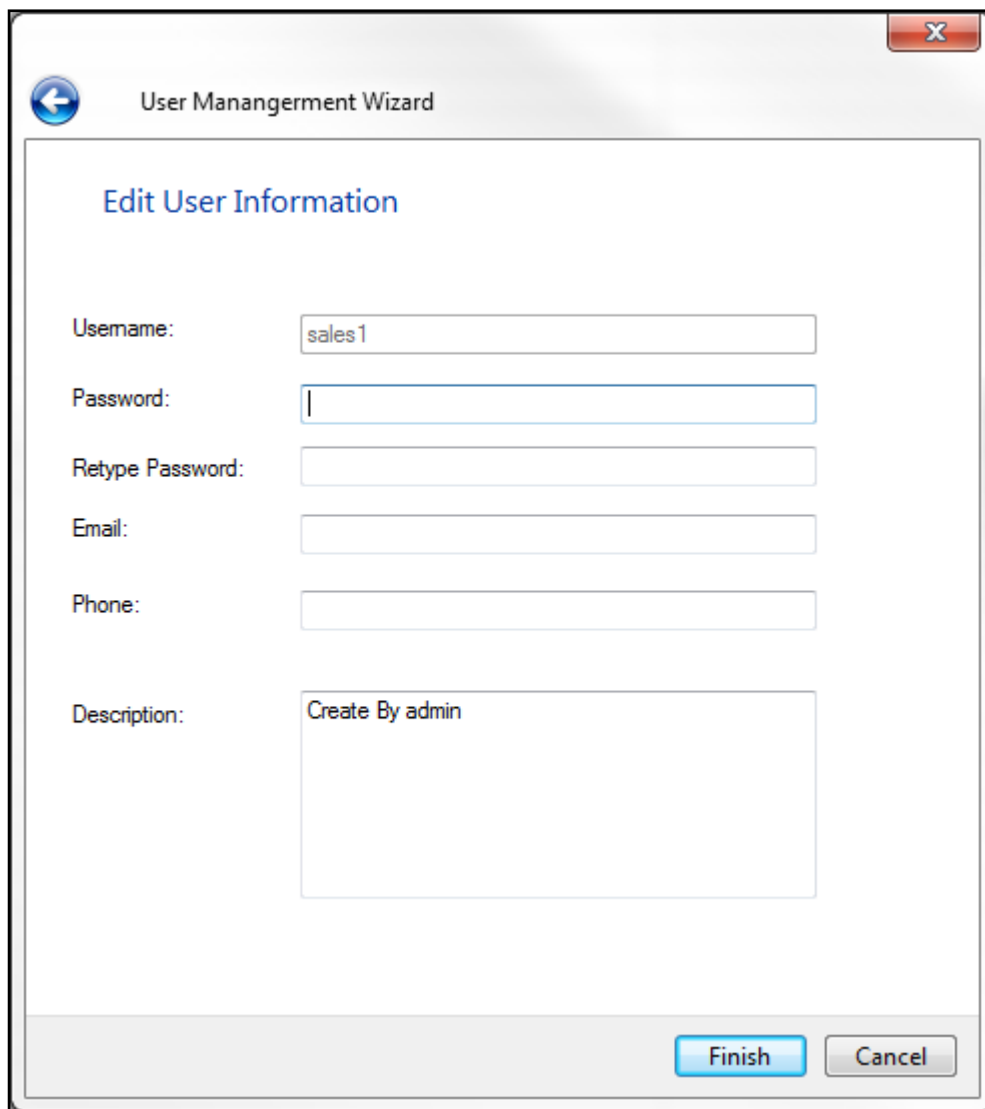


Editing an user

Select a user and click "Edit User".



Edit user information and click "Finish".



The image shows a 'User Management Wizard' dialog box with the title 'Edit User Information'. It contains several input fields: 'Username' (containing 'sales1'), 'Password' (empty), 'Retype Password' (empty), 'Email' (empty), 'Phone' (empty), and 'Description' (containing 'Create By admin'). At the bottom right, there are 'Finish' and 'Cancel' buttons. The dialog box has a standard Windows-style title bar with a close button (X) in the top right corner.

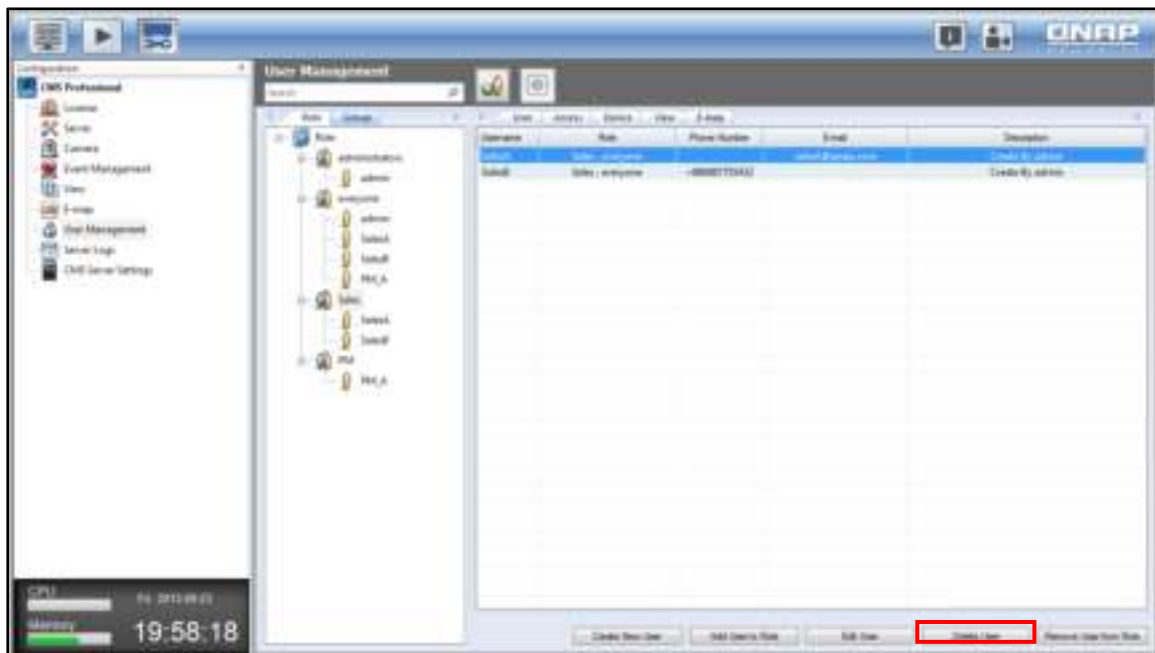
Username:	sales1
Password:	
Retype Password:	
Email:	
Phone:	
Description:	Create By admin

Finish Cancel

Note: Due to security and safety concerns, the Password and Retype Password fields will be cleared each time the user password is edited.

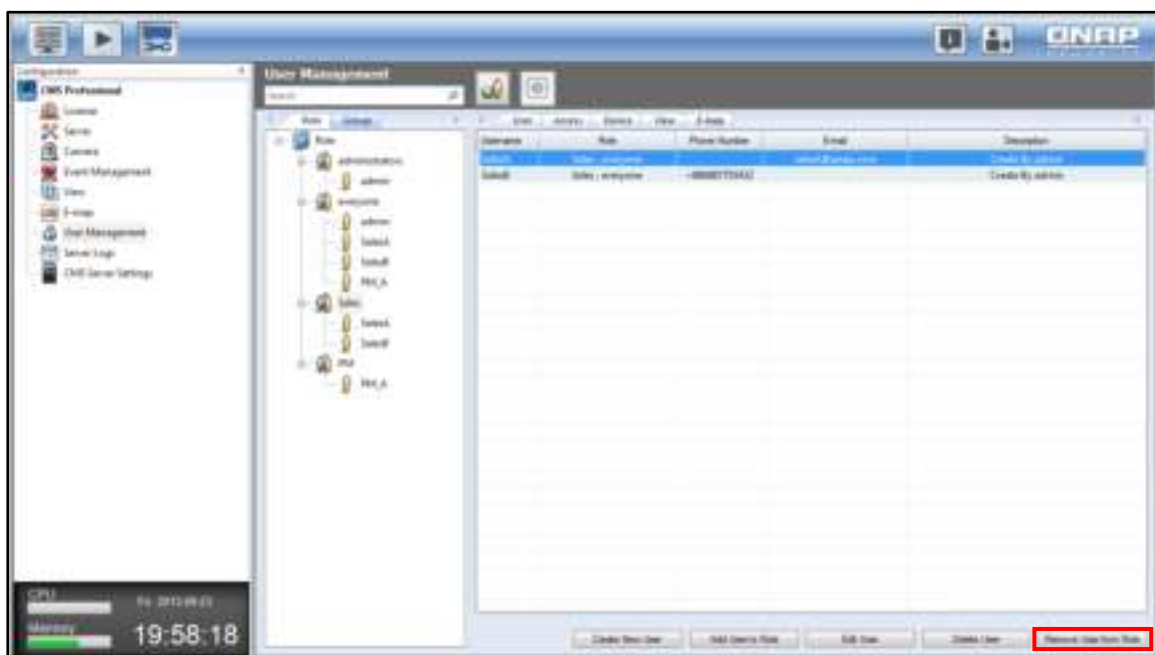
Deleting an user/remove an user from a role

To delete a user, please select the role first. Select the user from the list to the right and click "Delete User".



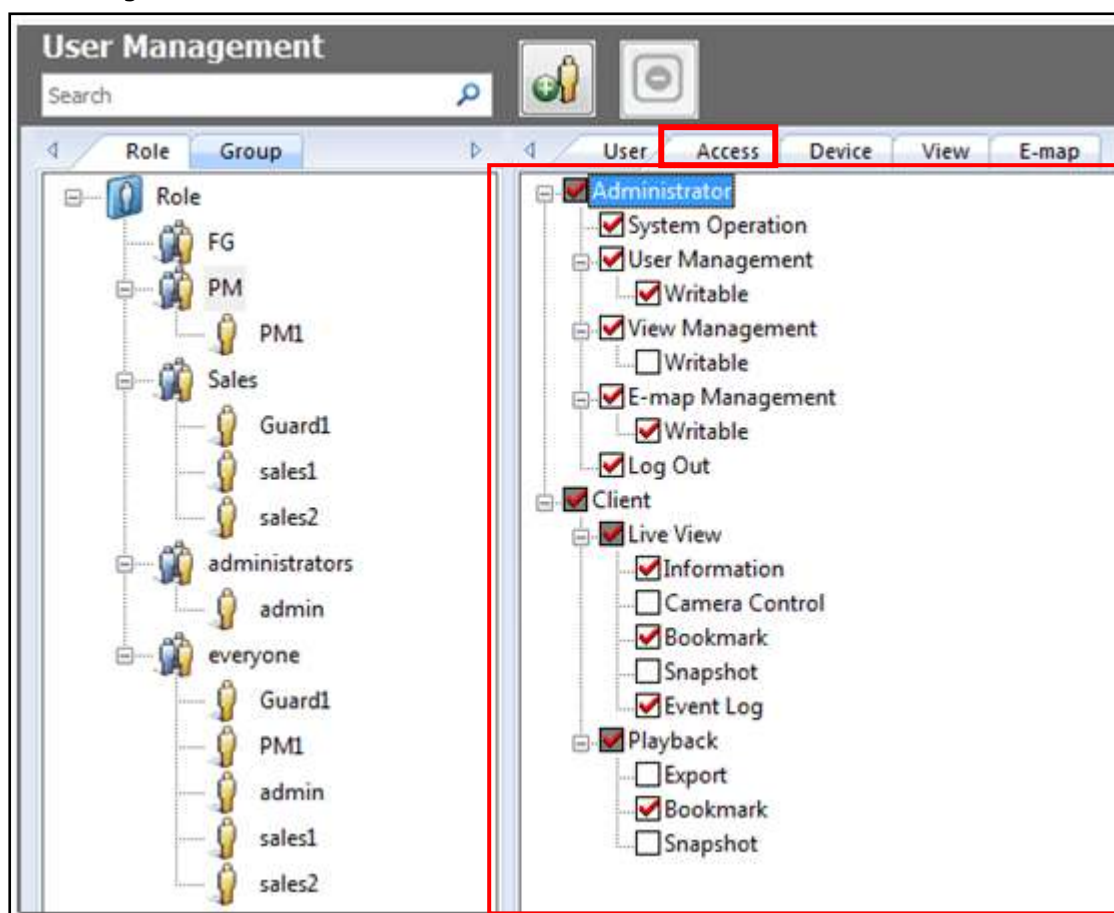
The chosen user account under the role will be deleted permanently from the system.

Please note that the "Remove User from Role" button is used to only remove the user account from the role, and the account will still exist in the system after the account is removed.



Configuring role permissions

Select "Role" and the information of all users under that role will be shown. You can set the access rights of the role under the "Access" tab.

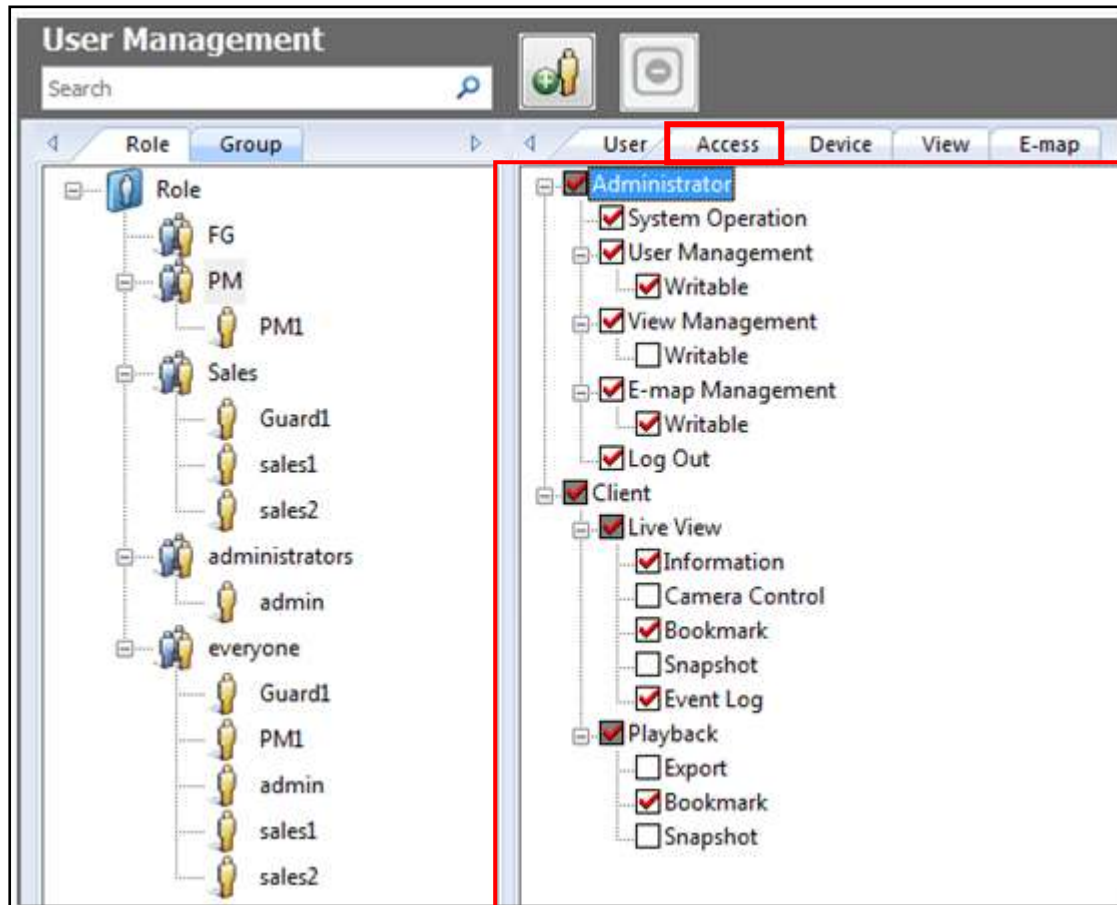


Access right (Administrator)	Description
System Operation	Ability to configure License, Server, Camera, Event Management.
User Management (Writable)	Ability to configure or only read User configuration.
View Management (Writable)	Ability to configure or only read View configuration.
E-map Management (Writable)	Ability to configure or only read E-map configuration.
Log Out	Ability to log out.

Access right (Client)	Description
Live View/Information	Ability to see the camera live view and Input Device list.
Live View/Camera Control	Ability to control camera panels.
Live View/Bookmark	Ability to use quick/detail bookmarks on the live view page.
Live View/Event Log	Ability to watch view and control event logs on live view page.
Playback/Export	Ability to export video or playback.
Playback/Bookmark	Ability to use quick/detail bookmark during playback.
Playback/Snapshot	Ability to take a snapshot during camera playback.

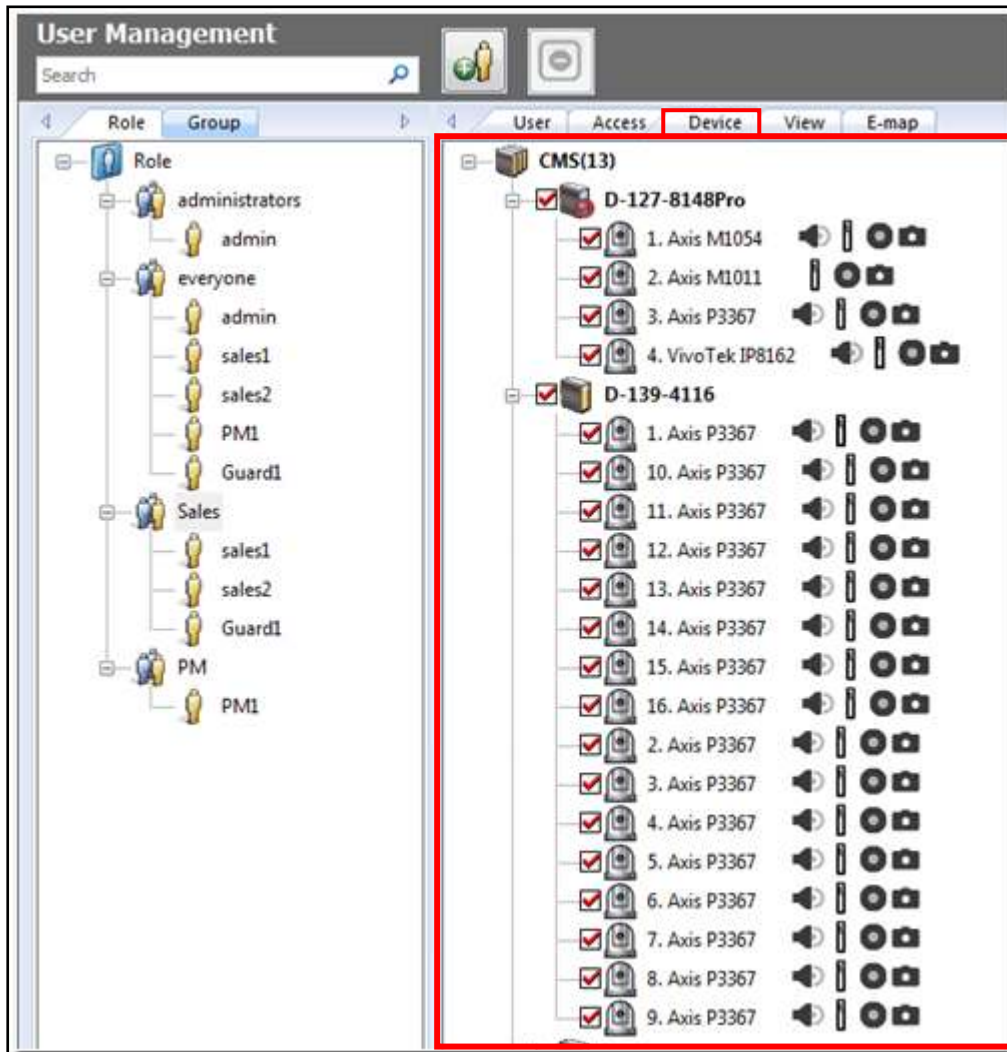
Access

This page includes two categories: administrator and client access. Each category is organized and presented in a treeview (click the "+" sign or "-" sign before an item to collapse or expand for more items.) Also, the access right for each application can be configured for the role.. Click "Save" after confirmation, or "Undo" to go back to the last step.



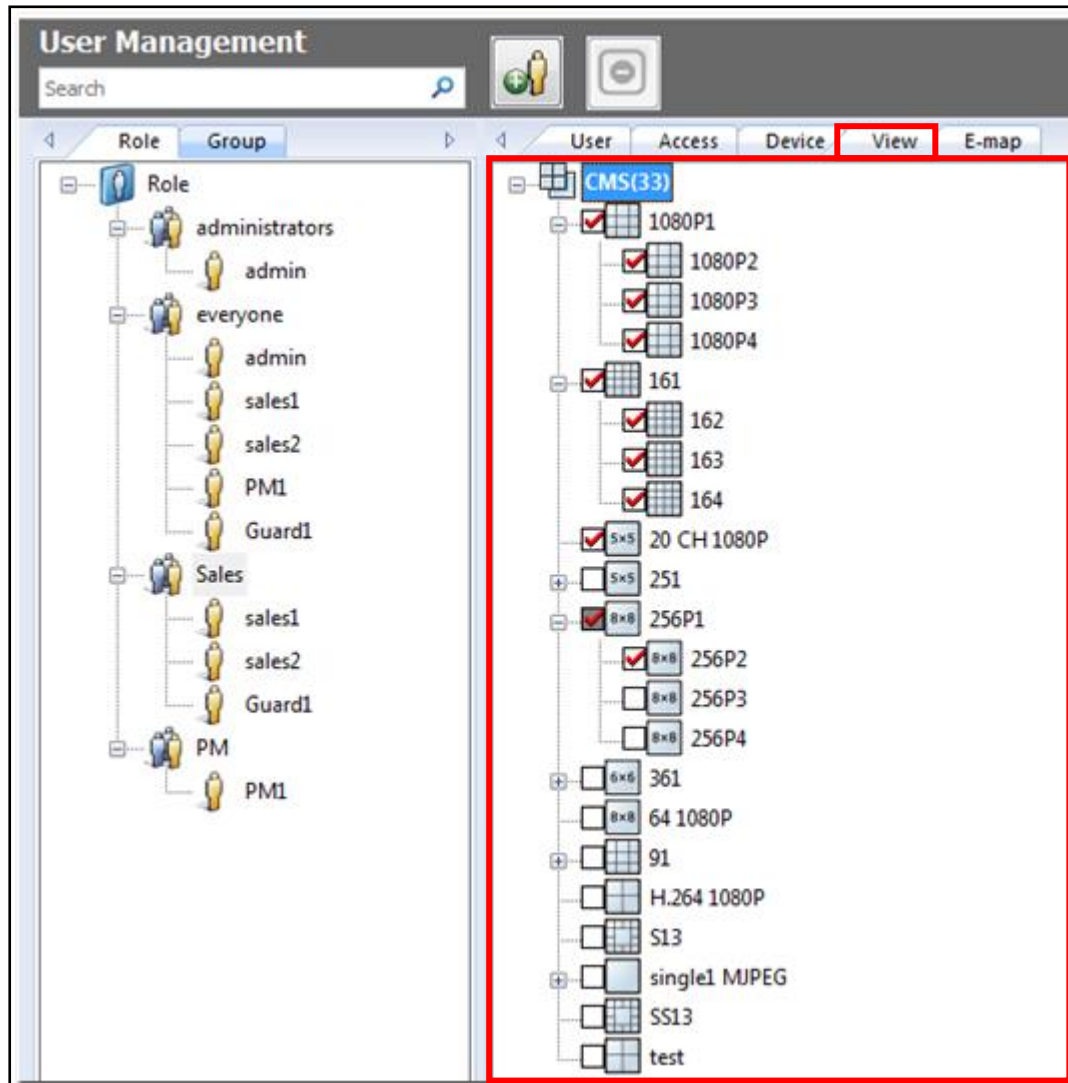
Device

Configure the access rights of the NVRs or the cameras for each role on this page. The available options include sound output/input, recording, PTZ control, manual recording and snapshot. Click "Save" to apply the changes or select "Undo" to return to the previous step.



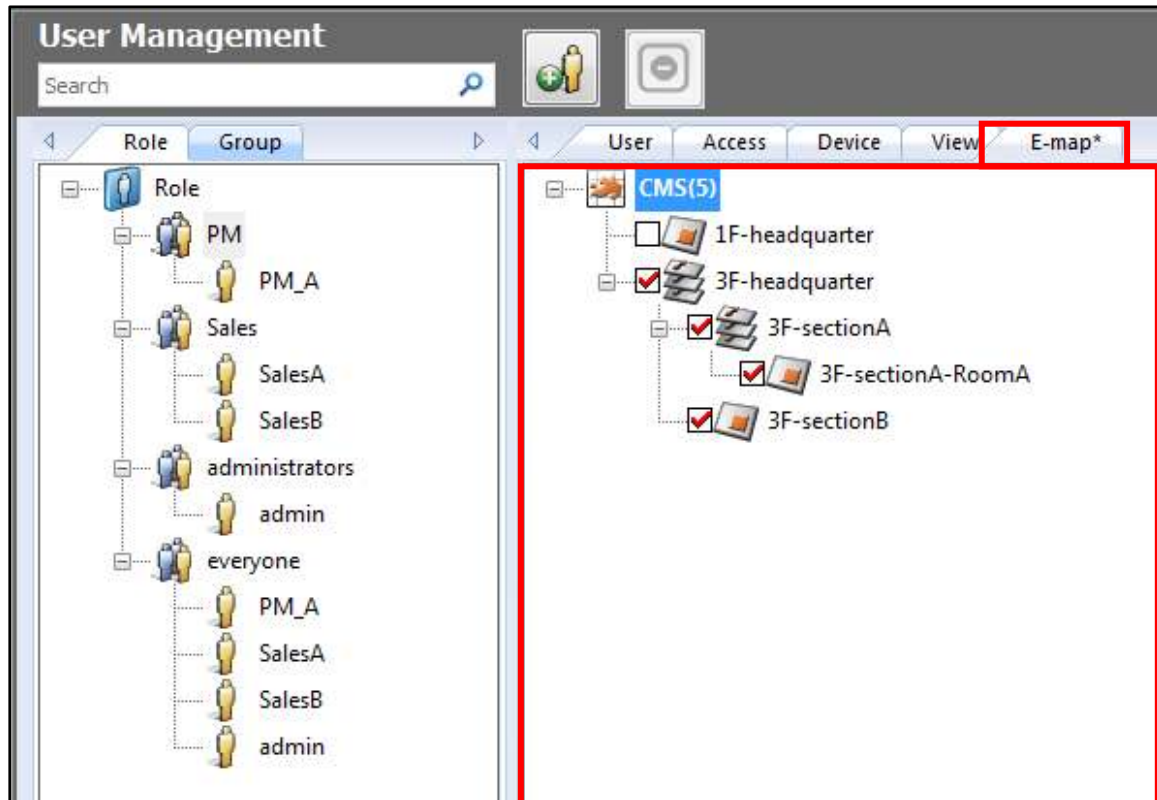
View

Configure the view layouts for each role on this page (this feature is for administrators only.)
Click "Save" to apply the changes made on this page or select "Undo" to return to the previous step.



E-map

Assign the rights of each right to edit and use E-maps on this page (this feature is for administrators only). Click "Save" to save the changes made on this page or select "Undo" to return to the previous step.




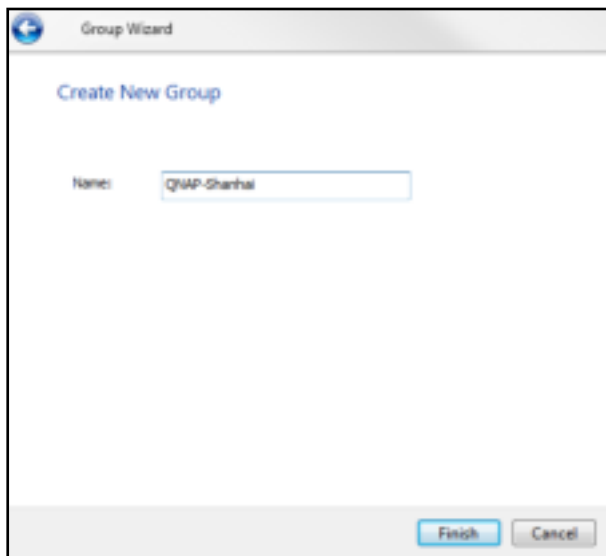
3.13.2 Group Management

This feature is used to classify the users for efficient user management.

Note: The same CMS users can be assigned both to a Role and Group. Therefore, one user can have both role and group properties.

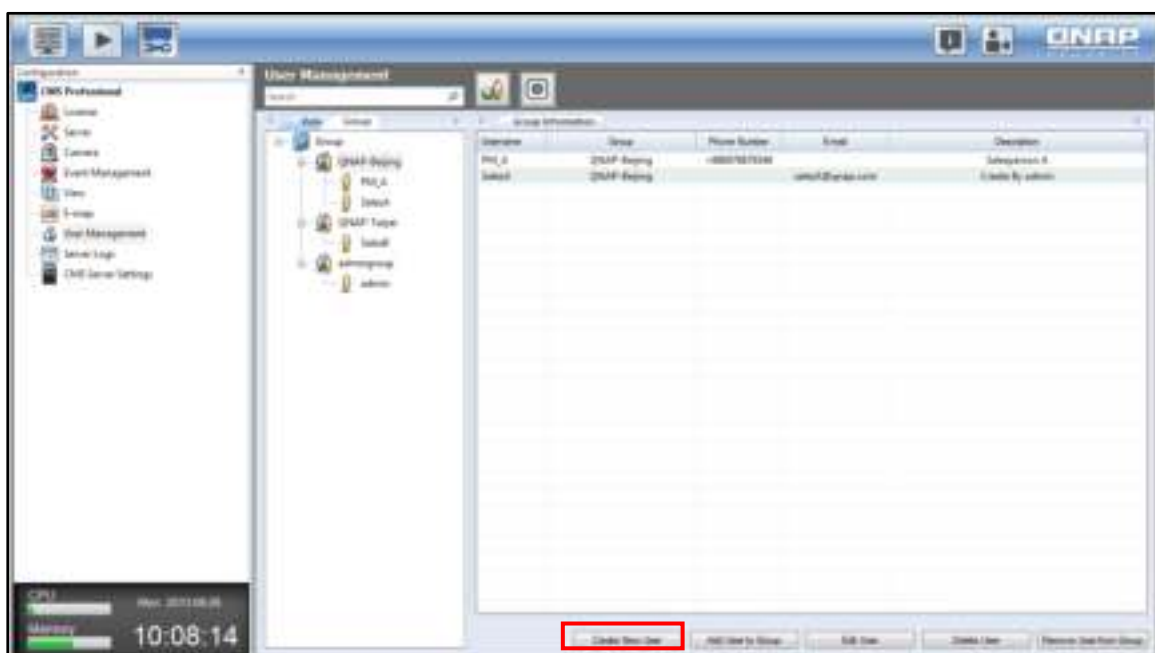
Adding a group

To create a new group, click . Enter the name of the group and click "Finish".

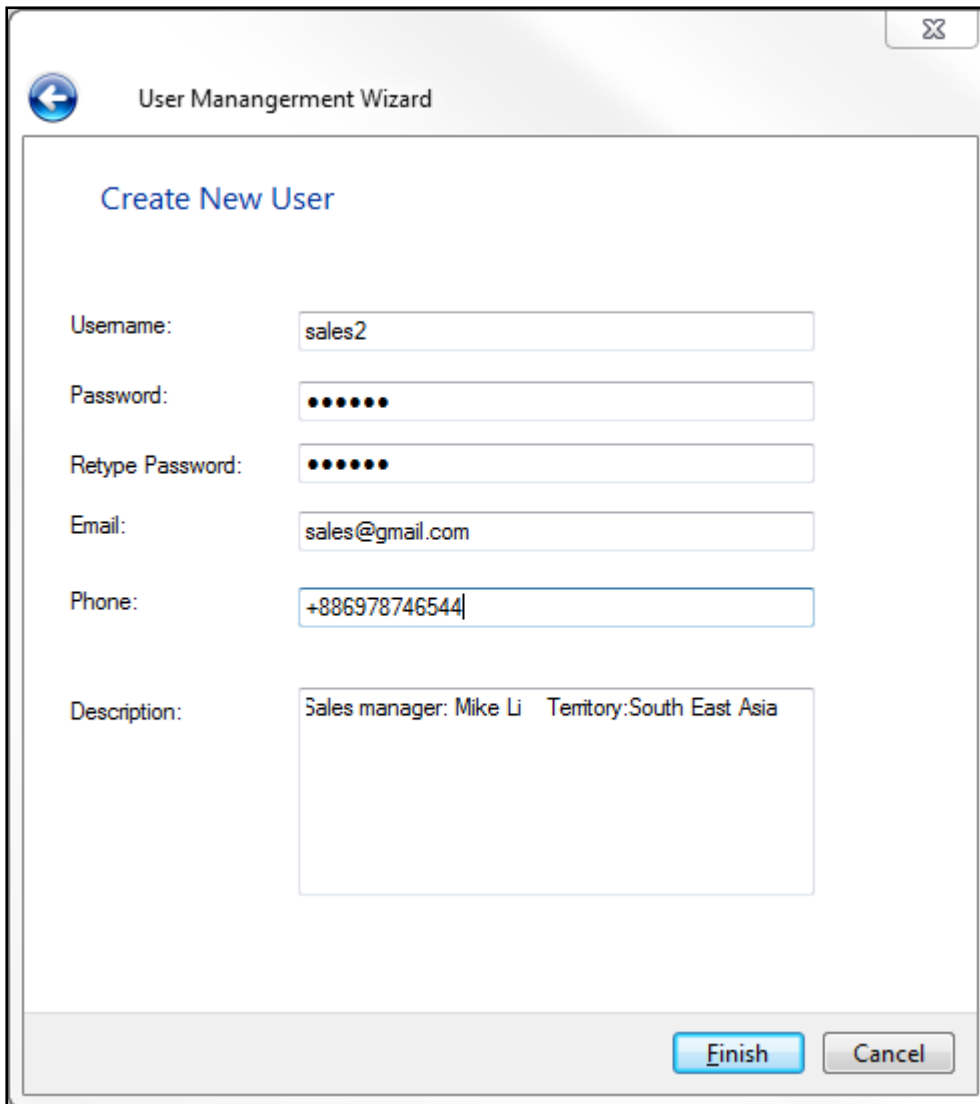


Adding an user to a group

Select a group and click "Create New User".




After all the fields in the User Management Wizard are complete, the newly created user will be listed under its perspective group under the "Group" tab.



The screenshot shows a 'User Management Wizard' window with a 'Create New User' section. It contains several input fields: 'Username' with the value 'sales2', 'Password' and 'Retype Password' both masked with dots, 'Email' with 'sales@gmail.com', and 'Phone' with '+886978746544'. The 'Description' field contains the text 'Sales manager: Mike Li Territory:South East Asia'. At the bottom right are 'Finish' and 'Cancel' buttons.

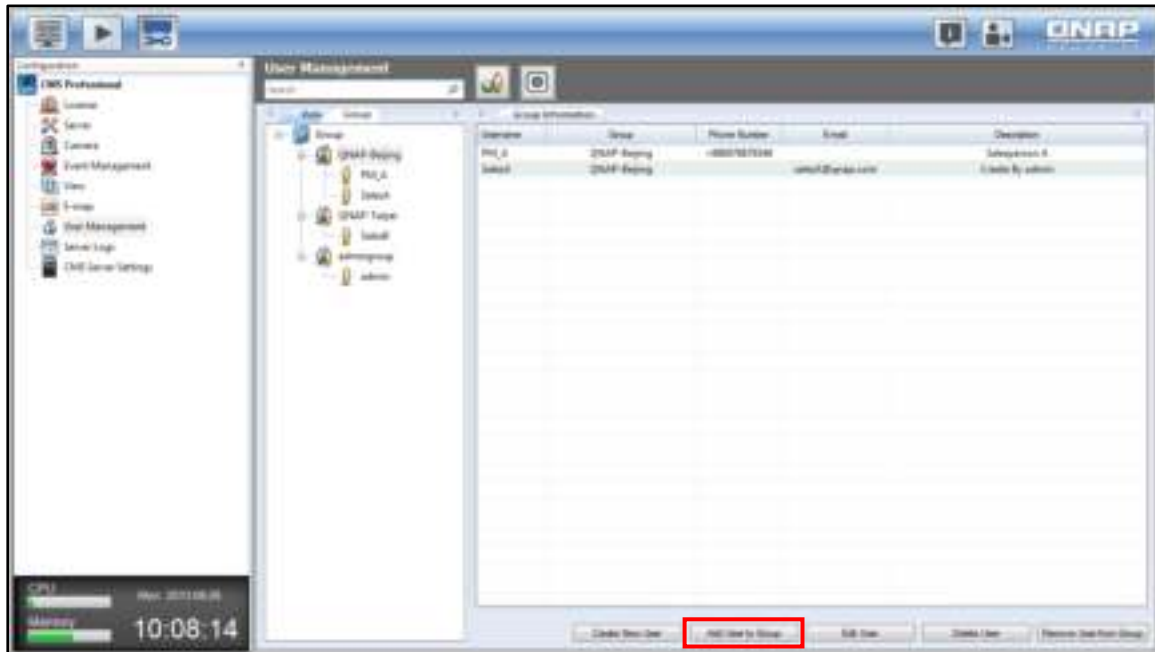
- Username: The user name must be 1 to 32 characters in length. It supports alphabets (A-Z), numbers (0-9), and underscores (_). It is case-insensitive and supports double-byte characters, such as Chinese, Japanese, and Korean but cannot be a pure number or contain the following characters:
"/ \ [] : ; | = , + * ? < > ` ' "
- Password: The password is case-sensitive and the maximum length is 16. It is recommended to use a password of at least 6 characters.
- Other fields: fields such E-mail, phone number and description can be left blank.

Deleting a group

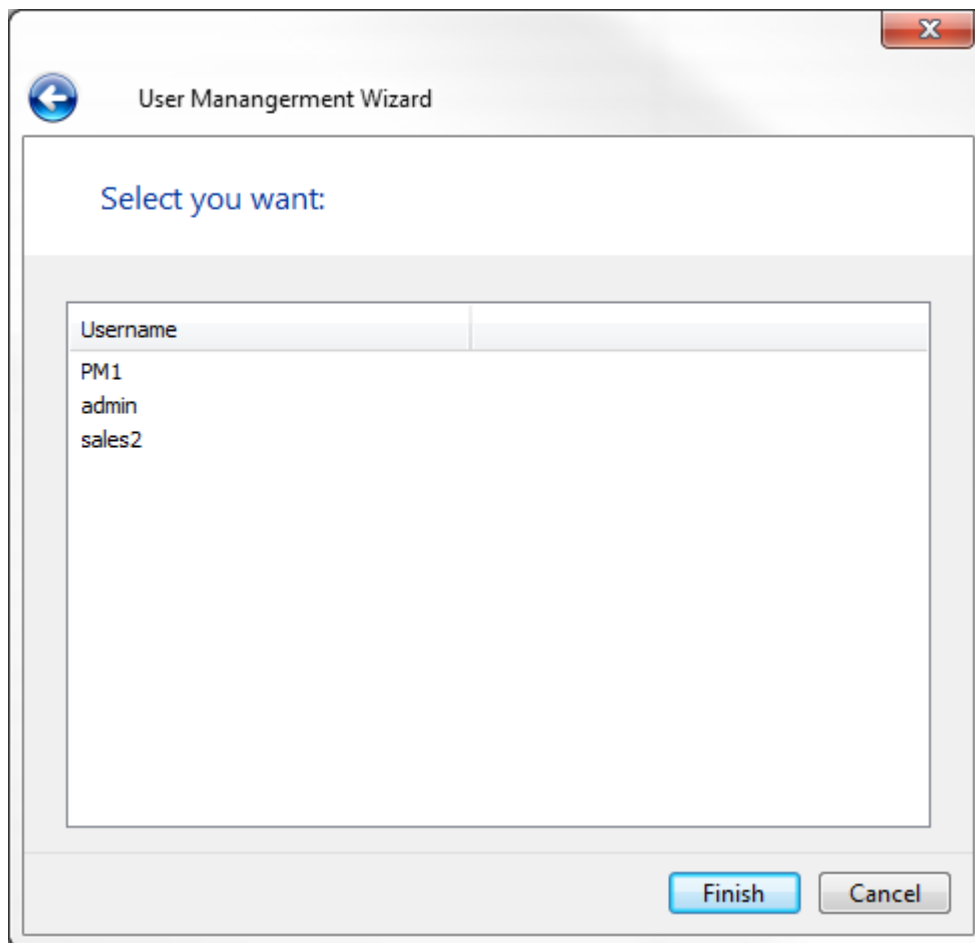
To delete a group, select the group on the left, and click .

Adding the existing user(s) to a group

To quickly add the existing users to the different groups, click "Add User to group".

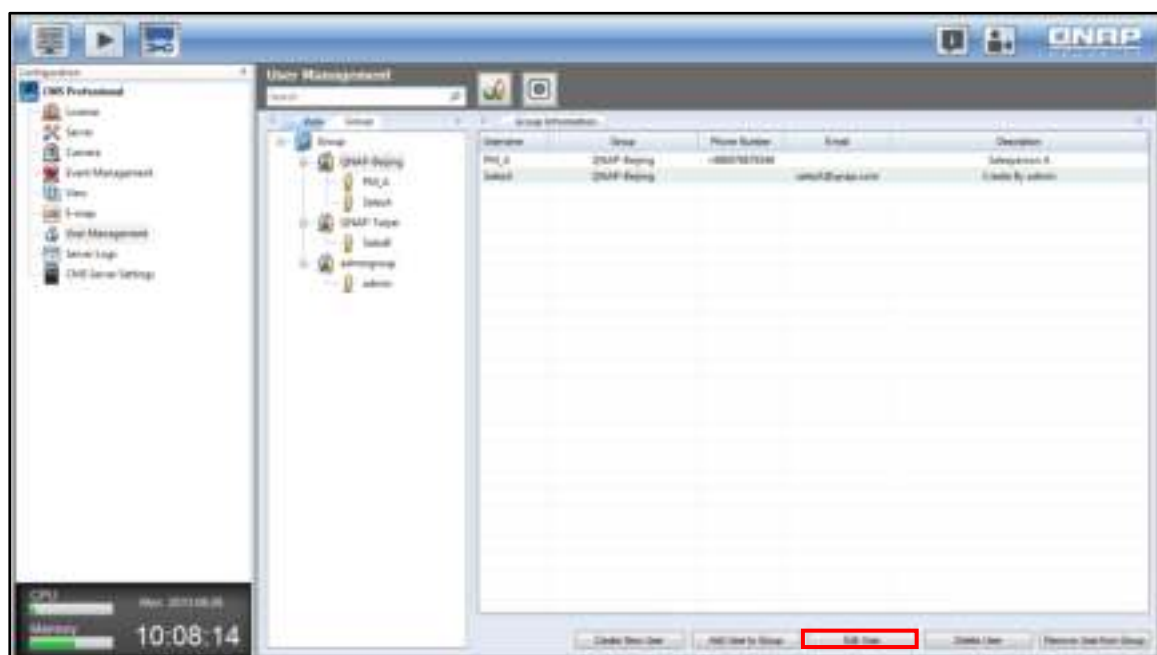


Users already created for the group will be listed. Click "Finish" after making your selection.

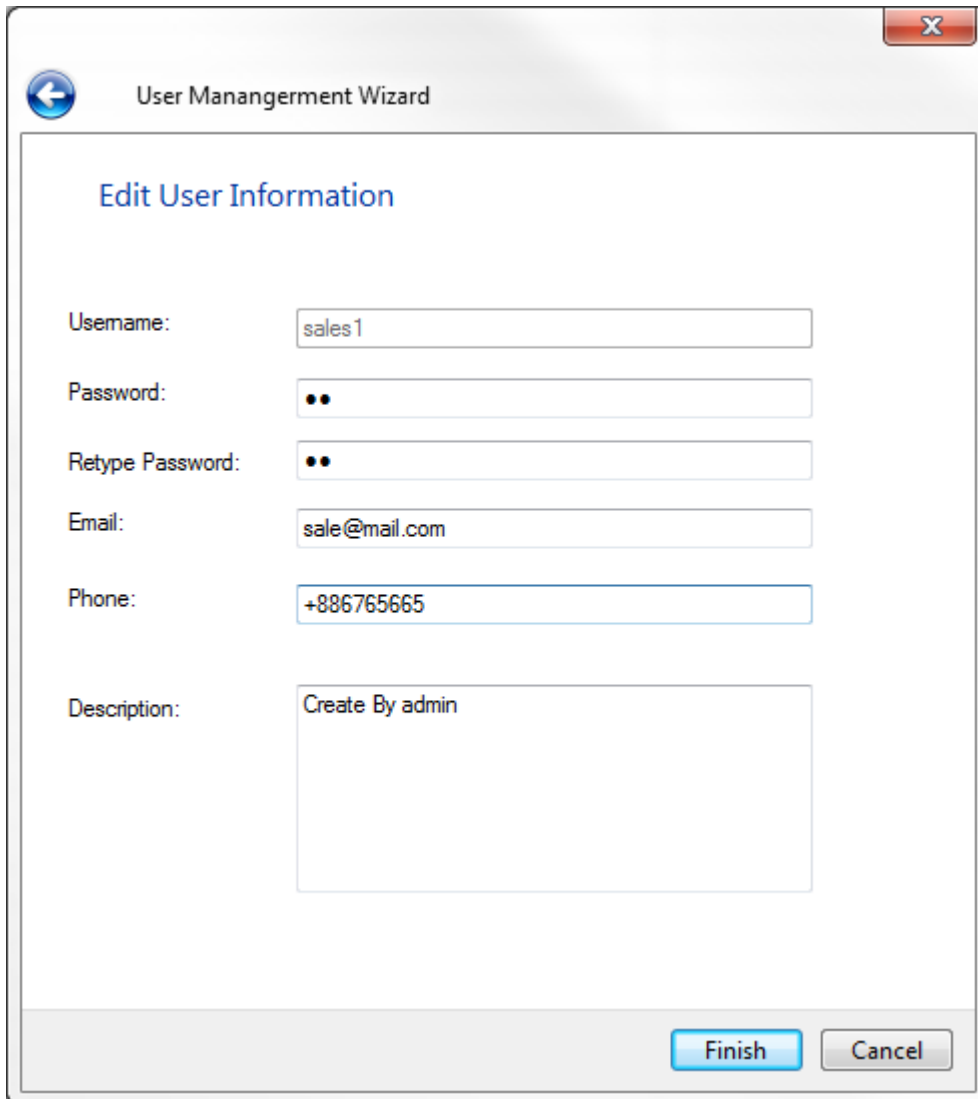


Editing an user

Select a user and click "Edit User".



Modify user information and click "Finish".



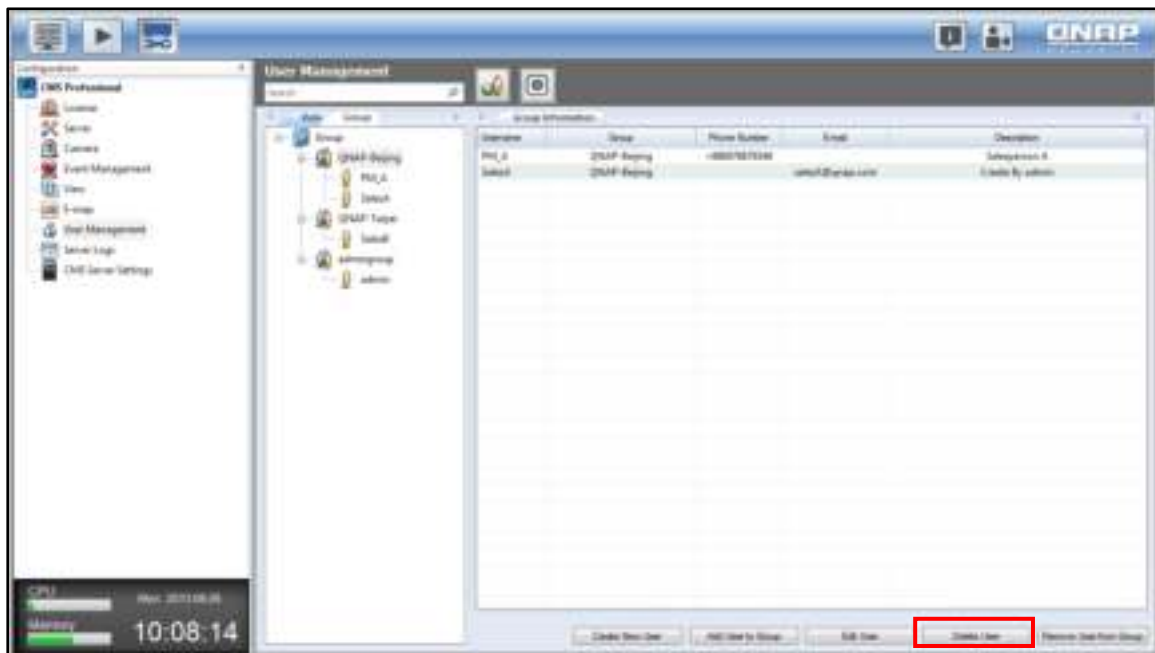
The image shows a 'User Management Wizard' dialog box with the title 'Edit User Information'. It contains several input fields for user details. The 'Username' field is filled with 'sales1'. The 'Password' and 'Retype Password' fields are masked with two black dots each. The 'Email' field is filled with 'sale@mail.com'. The 'Phone' field is filled with '+886765665'. The 'Description' field is a larger text area containing the text 'Create By admin'. At the bottom right, there are two buttons: 'Finish' (highlighted in blue) and 'Cancel' (disabled).

Username:	sales1
Password:	••
Retype Password:	••
Email:	sale@mail.com
Phone:	+886765665
Description:	Create By admin

Note: Due to security and safety concerns, the Password and Retype Password fields will be cleared each time the user password is edited.

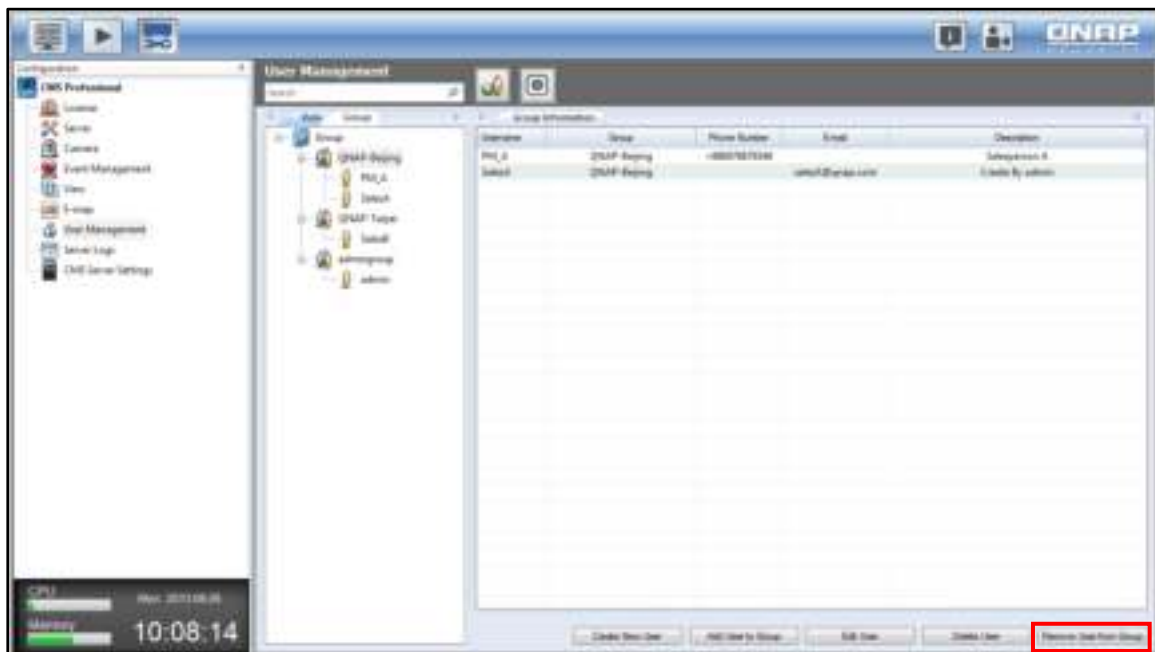
Deleting an user

To delete a user, select the role and the user, then click "Delete User". The account will be permanently deleted from the system after the user is deleted.



Removing an user from a group

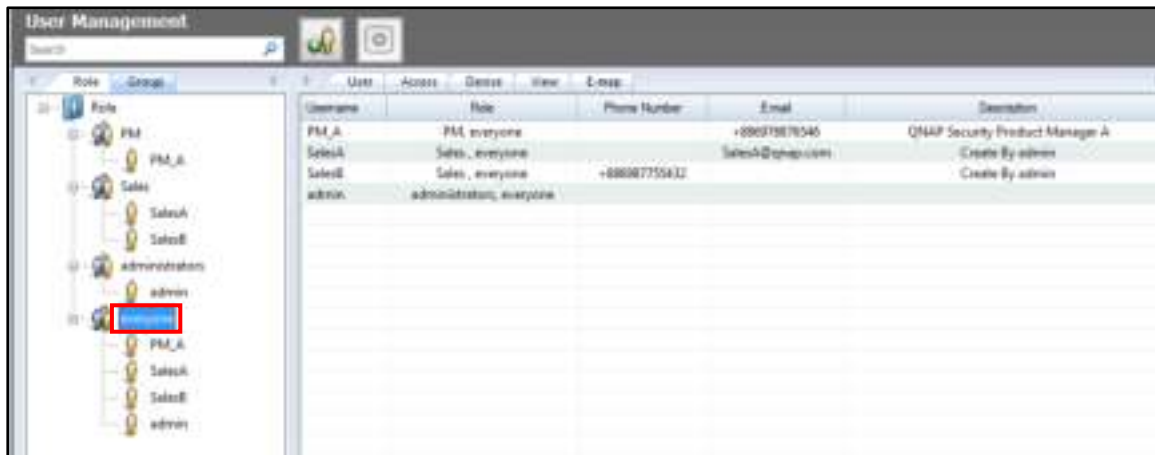
To remove a user from a group, select the user and click "Remove User from Group".



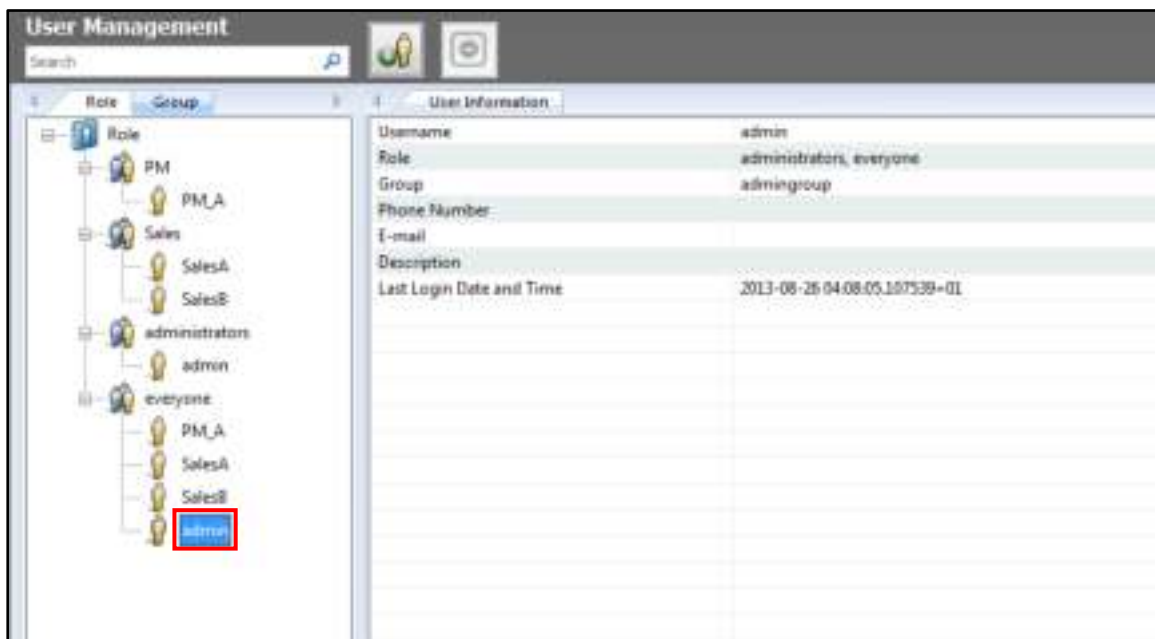
Note: The "Removing User from Group" button will only remove users from a role, but the user account will still remain in the system.

3.13.3 User List

To check the users within a group or role, please click the role or group under the “Role” or “Group” tab and all user accounts and their details, including the name, role/group that it belongs to, phone number, email, and description, will be listed on the right side of the page.



To further check on the details of a particular user account, please click on the user account on the left box and all its account details, including the Last Login Date and Time will be shown on the right side of the page.



3.14 CMS Server Settings

3.14.1 Domain Security

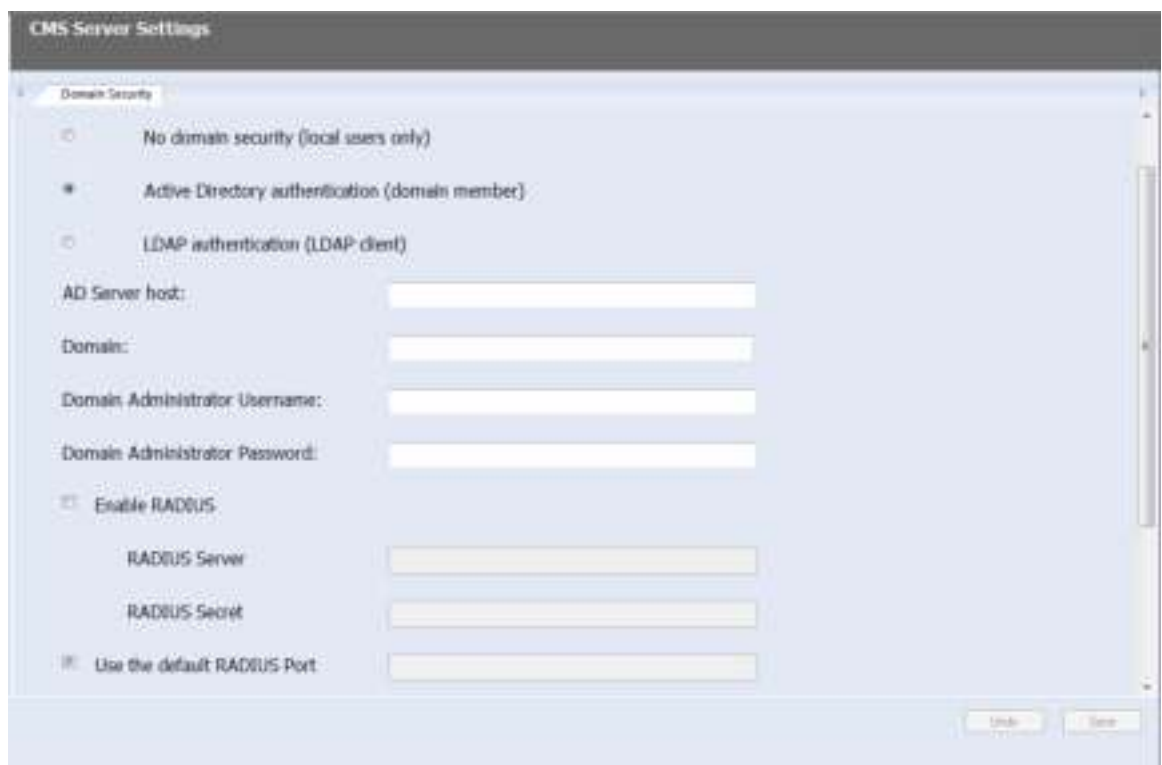
The domain security feature is designed for the CMS Server to join the Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) directory and for AD and LDAP users to access the CMS Server. Go to the “CMS Server Settings” page to set up the domain security. There are three options available:



- No domain security (local users only): Select this option, and only local users can access the CMS Server.



- Active Directory authentication (domain member): Select this option to join the CMS Server to an AD domain. Enter all fields and choose to enable the RADIUS service. After joining the CMS Server to an AD domain, the AD users can log into the CMS Server.



CMS Server Settings

Domain Security*

☒ Use the default LDAP Port

LDAP Security: **None**

LDAP BASE DN:

LDAP Bind DN:

LDAP Bind Password:

Users Base DN:

☒ Enable RADIUS

RADIUS Server: **myRADIUS.gnap.com**

RADIUS Secret: **xxxxxxxx**

☒ Use the default RADIUS Port

Undo Save

CMS Server Settings

Domain Security*

☒ Use the default LDAP Port

LDAP Security: **None**

LDAP BASE DN:

LDAP Bind DN:

LDAP Bind Password:

Users Base DN:

☒ Enable RADIUS

RADIUS Server: **myRADIUS.gnap.com**

RADIUS Secret: **xxxxxxxx**

☒ Use the default RADIUS Port

Undo Save

- LDAP authentication (LDAP client): Select this option to connect the CMS Server to an LDAP directory. Enter all fields (refer to the following table for explanations on each field) and choose to enable the RADIUS service. After the CMS Server is connected to the LDAP directory, either the local users or the LDAP users can be authenticated to access the CMS Server. After the LDAP directory settings are

applied, users will be prompted to choose between “Local” and “LDAP Domain Name” in the “login to” field on the of login screen.

CMS Server Settings

Domain Security

- ☐ No domain security (local users only)
- ☐ Active Directory authentication (domain member)
- ☒ LDAP authentication (LDAP client)

Select the type of LDAP server: **LDAP Server**

LDAP Server Host:

☒ Use the default LDAP Port:

LDAP Security: **None**

LDAP BASE DN:

LDAP Bind DN:

LDAP Bind Password:

Users Base DN:

CMS Server Settings

Domain Security

☒ Use the default LDAP Port:

LDAP Security: **None**

LDAP BASE DN:

LDAP Bind DN:

LDAP Bind Password:

Users Base DN:

☒ **Enable RADIUS**

RADIUS Server:

RADIUS Secret:

☒ Use the default RADIUS Port:

Field	Description
Select the type of	Choose the LDAP server domain you want to access.

LDAP Server	
LDAP Server Host	The LDAP server host or IP.
LDAP Security	Specify how the NAS will communicate with the LDAP server: - ldap:// = Use a standard LDAP connection (default port: 389). - ldap:// (ldap + SSL) = Use an encrypted connection with SSL (default port: 686). - ldap:// (ldap + TLS) = Use an encrypted connection with TLS (default port: 389).
BASE DN	The LDAP domain. For example, dc=mydomain,dc=local
Root DN	The LDAP root user. For example, cn=admin, dc=mydomain,dc=local
Password	The root user password.
Users Base DN	The organization unit (OU) in which users are stored. For example, ou=people,dc=mydomain,dc=local

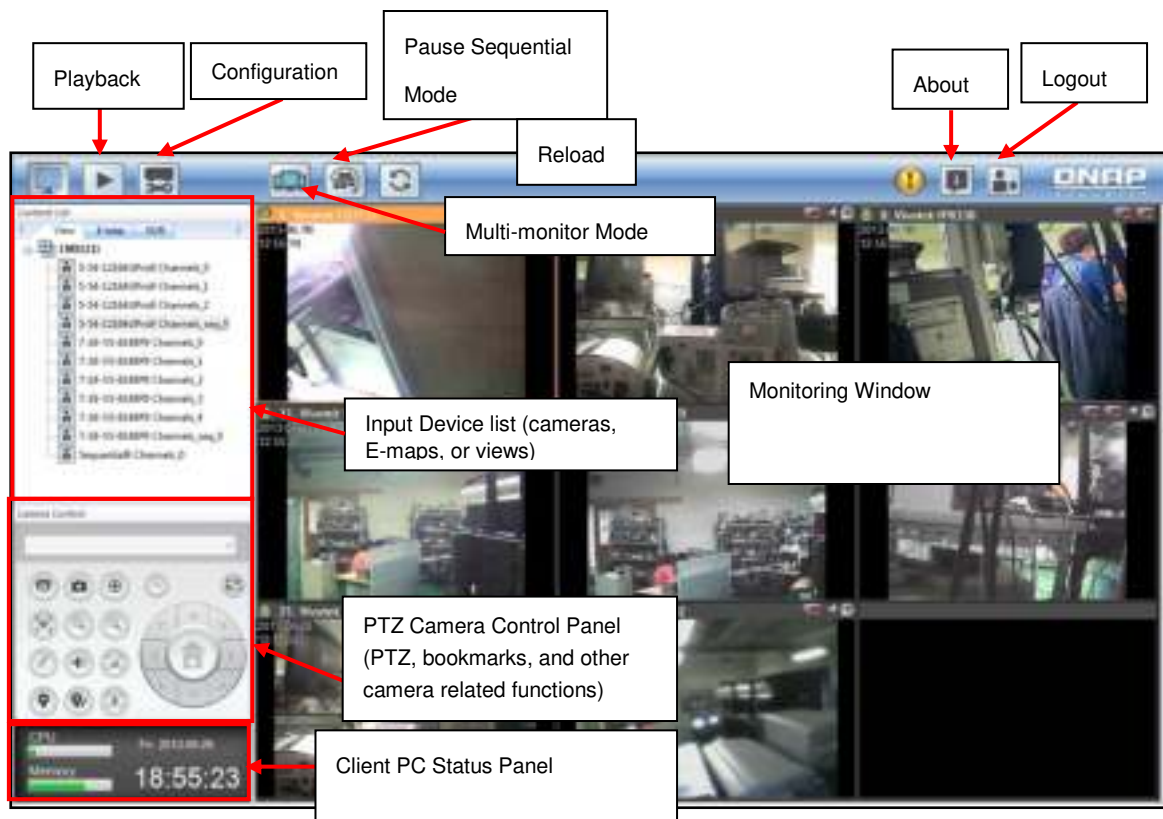
Note:

- To avoid account conflicts, please do not create CMS user accounts that already exist in the AD and LDAP directory.
- After the domain security feature is configured, please be sure to select the correct domain to log in on the login screen.


3.15 Live View

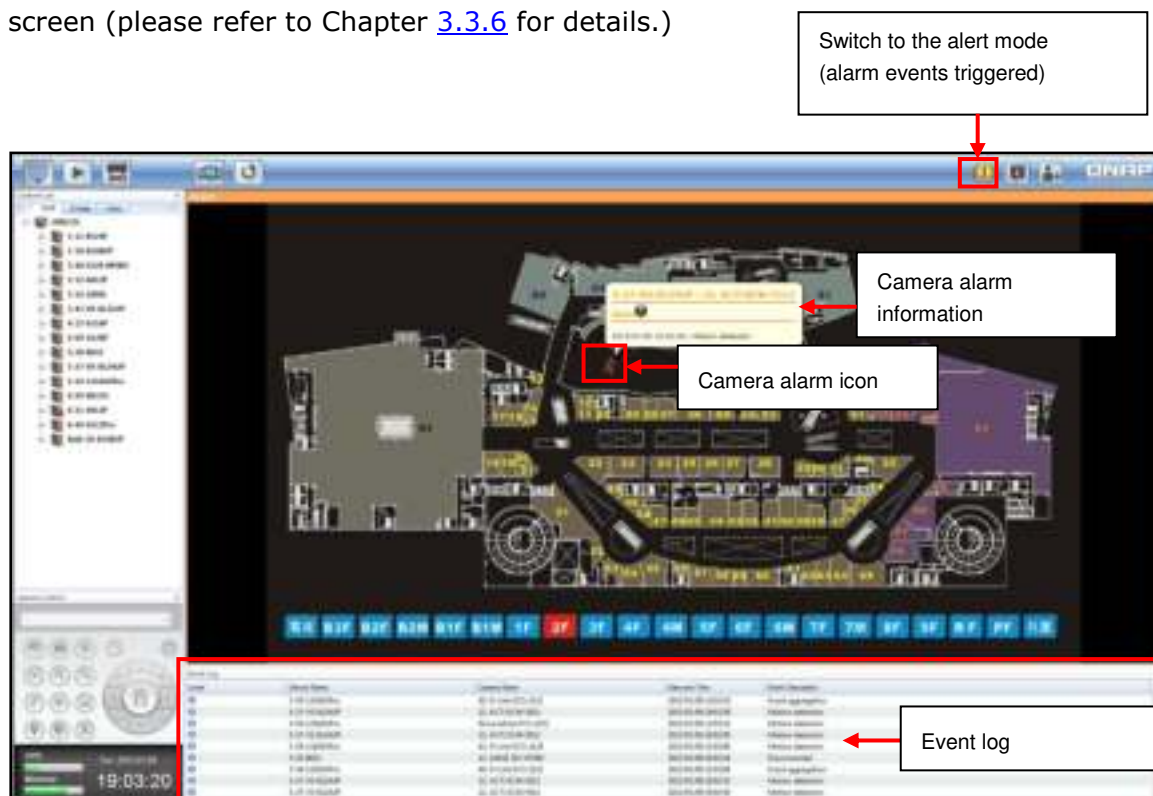
Upon successful login to the CMS Server, the live view console will appear. System administrators can view all the configured IP cameras and E-maps, switch between the display modes, enable or disable manual recording, or take a snapshot, etc. The borders and sizes of the left toolbar, the main screen in the middle, and the system logs window below are all adjustable. To set up the monitoring page, please first add NVR servers to the CMS Server, add camera channels, and then go to live view page (please refer to Chapter [5.4](#) and [5.7](#) for details.) The camera channels will be available on the page.

The live view page and all its features are described in the following figure:



Note: The Client PC Status Panel at the bottom left shows the date and time, and the memory and CPU usage of the client PC.










When an alarm is triggered by a camera and the CMS will enter the alert mode. There are two kinds of alert presentations in the alert mode: 1) if the live view is displayed on the Monitoring Window, the alarm button on the top right corner of the screen will start to flash. When this happens, users can click this alarm button to view the system logs; and 2) if the E-map is displayed on the Monitoring Window, the camera icon will change to . Users can choose to handle the alarm by moving the mouse cursor to the event logs at bottom of the screen (please refer to Chapter [3.3.6](#) for details.)









Note: Users can press F11 to turn the full screen mode on or off.



Icons and description of the main toolbar:

Icon	Description
	Open the live view page.
	Open the video playback page.
	Open the system configuration page (administrator username and password are required).
	The multi-monitor mode is supported. The icon will appear if the client PC has multiple monitors.
	Pause all cameras running in the sequential mode at any time in order not to miss any event.
	Reload the page.
	Shows the CMS Client version and website address of QNAP Security.
	Logout the CMS Client.
	When an alarm is triggered, this icon will flash, and users can click this button to enter the alarm mode.

Icons and description of the Input Device List:

Icon	Description
	NVRs that have been added to the system.
	IP cameras that have been added to the system.
	This icon shows that there are several layers in the E-map. Click the icon to enter the next layer in the E-map group.
	Click  to select a single-layer E-map. When an E-map is selected, the icon will become  .

Note:

- Enabling or disabling manual recording will not affect scheduled or alarm recording. They are independent processes.
- By default, the snapshots are saved in "My Documents" or "Documents"> "Snapshots" (in Windows.)
- If the snapshot time is inconsistent with the actual time that the snapshot is taken, it is caused by the network environment and not a system error.
- The event alarm settings can only be configured on the NVR. Users can only enable or disable the CMS to receive alarms.
- When the digital zoom function is enabled on multiple IP cameras, the zooming performance will be affected if the computer performance decreases.

When right clicking a camera channel on the live view page, the following functions may not be available depending on the IP camera model:

- Connect to camera homepage.
- Camera Settings: Open the configuration page of the IP camera (Please refer to the camera settings in the NVR user manual for details.)
- Preset Positions: Select the preset positions of a PTZ camera.
- Auto Cruising: Configure the PTZ cameras to cruise according to the preset positions and the staying time set for each preset position.
- PTZ Control: Pan, tilt, or zoom camera control.
- Digital Zoom: Enable or disable digital zoom.
- Keep Aspect Ratio.
- Adjust Live Stream: Auto/Quality priority/Performance priority/Recording stream.
- Carousel: Manually switch to the next or last camera in the sequential mode.







3.15.1 Live View Page

After correctly setting the channel layout, the live videos of the IP camera will be shown on the live view page. Click the monitoring page to use the features supported. Please note that the PTZ camera control panel at bottom left side of the screen can only be used after a channel is selected from the monitoring page (The frame of the channel will turn into the orange color, and the channel selected will become an active channel.)

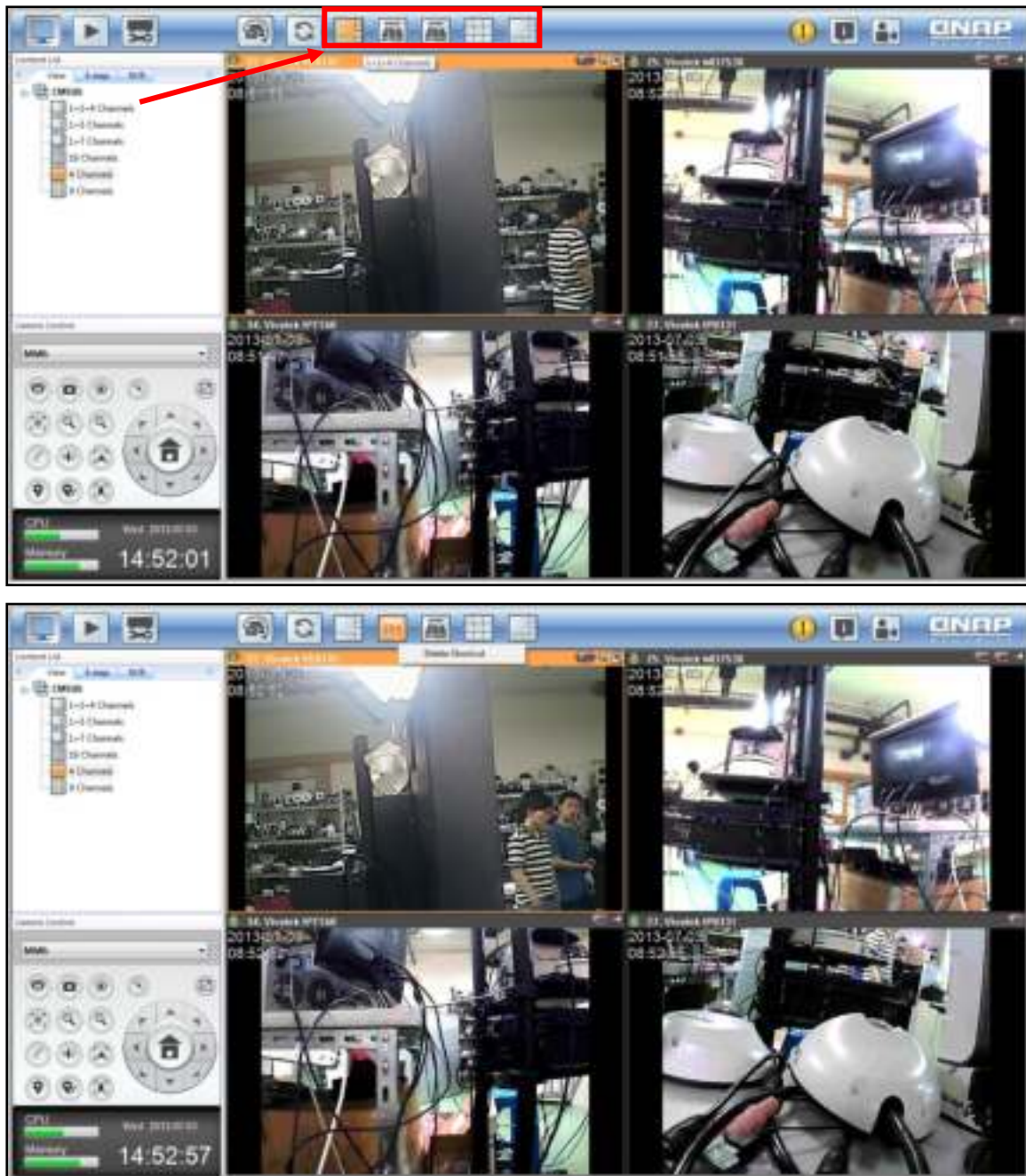


Camera Status

The camera status is indicated by the icons shown below:















Icon	Camera Status
	Indicates that the camera is in the scheduled or continuous recording mode.
	Indicates that manual recording mode is enabled for the camera.
	Indicates that the camera is currently being triggered to record by the advanced NVR Event Management ("Camera Settings" > "Alarm Settings" > "Advanced Mode").
	Indicates that this IP camera supports the audio function.
	Indicates that this IP camera supports PTZ control.
	Indicates that digital zoom is enabled.

The frequently viewed channels can be dragged to the main toolbar as shortcuts. To delete a shortcut, right click the shortcut and select "Delete Shortcut".



Note: A maximum of five shortcuts are supported on the main toolbar (including camera live view and E-maps.)



Icons and description of main toolbar:

ICON	Description
	Single-channel view
	4-channel view (2x2)
	6-channel view (1+1+4)
	6 channel view (1+5)
	8-channel view (1+7)
	9-channel view (3x3)
	10-channel view (2+8)
	12 channel view
	13-channel view (1+12)
	16-channel view (4x4)
	25-channels view (5x5)
	36-channels view (6x6)
	49-channels view (7x7)
	64-channels view (8x8)



3.15.2 Bookmark

The CMS Client provides quick and detailed bookmarks to review the snapshot of a channel on the live video page.




- Quick bookmark  : Select a live view channel and click .



- Detailed bookmark  : To edit the content of a bookmark, select a live view channel and click  . Enter the title and description.



To review bookmarks, follow the steps below:

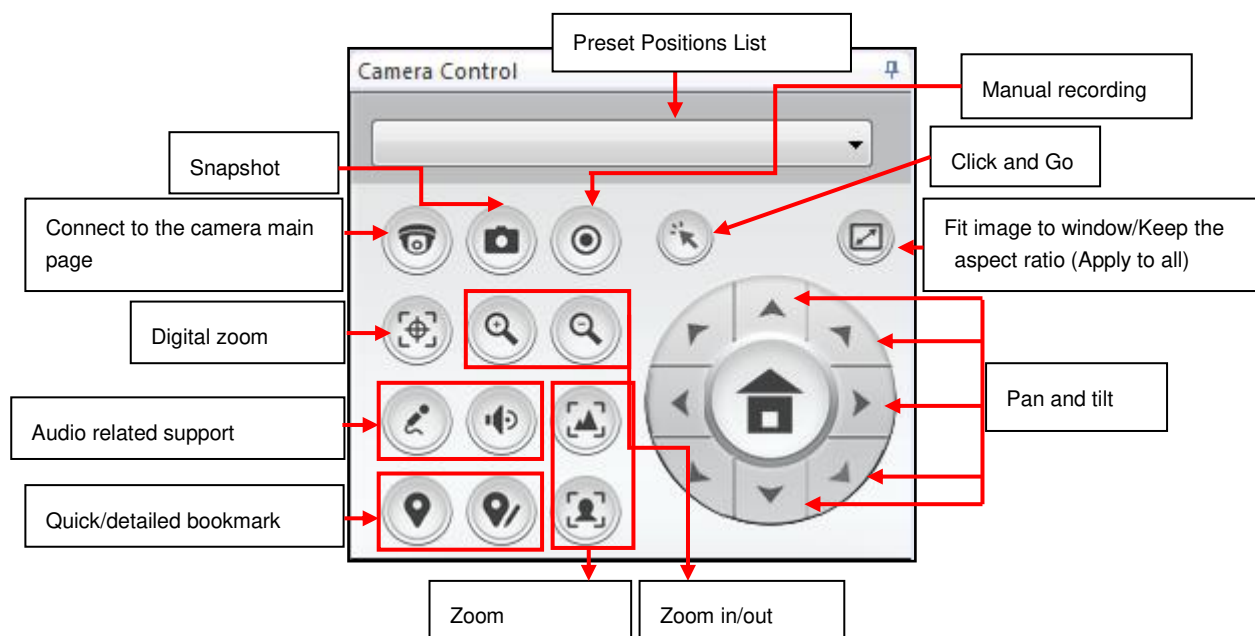
- Click the playback button  on the monitoring or management page.
- Click the bookmark to view the content. You can also save the snapshot, print or delete the bookmark.








Note: When several bookmarks are set in less than two minutes, they will be grouped and sorted by time for easy search.










3.15.3 PTZ Camera Control

The term “PTZ” stands for “Pan/Tilt/Zoom”. Use the PTZ Camera Control Panel in the CMS to adjust the viewing angle of an IP camera that supports PTZ controls. Support for PTZ controls vary depending on the camera models. Please refer to the user manual of your IP cameras for more information. Please note that the digital zoom function will be disabled when the PTZ function is in use.



Icons and descriptions of the PTZ Camera Control Panel:

Icon	Description
	Preset Positions List: Connect to the web page of the IP camera to customize the preset positions and conveniently and quickly point the camera to the present point.
	Login the main page of the specified IP camera: Select an IP camera and click this button to connect to the web page of that IP camera.
	Snapshot: Take a snapshot of the currently selected camera channel. After the snapshot appears, you can right click the snapshot to save it to the local computer.
	Manual Recording: Start or cancel the recording (for system administrators only.)
	Enable “Click and Go”: Click the camera channel at any point to align it to the center of the screen.

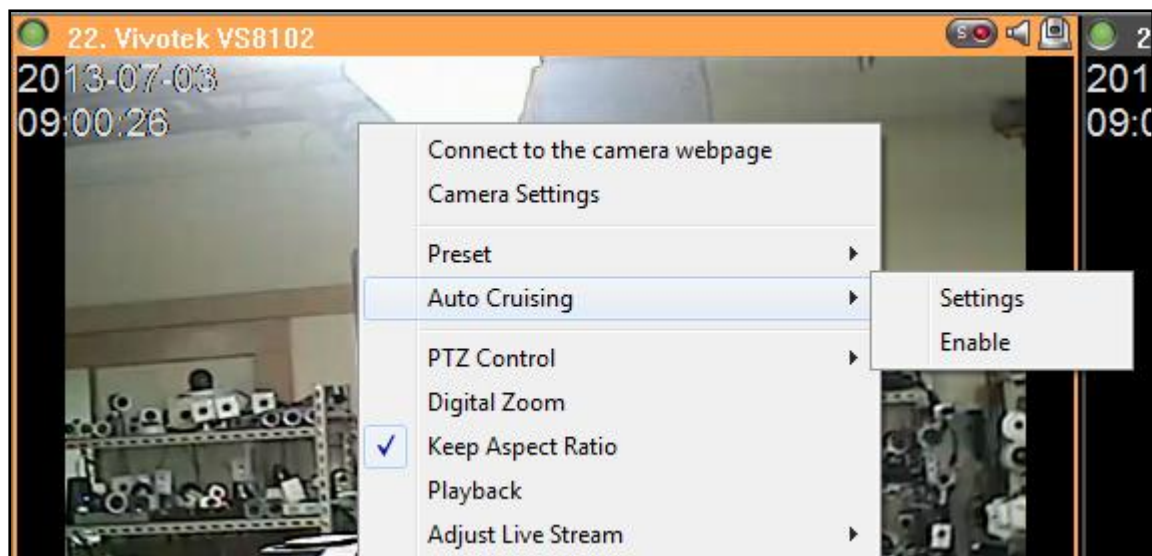
	<p>Fit image to window/Keep the aspect ratio (Apply to all):</p> <p>Fit the live view channel to its window or keep the aspect ratio for all channels on the Live View Screen.</p>
	<p>Digital Zoom:</p> <p>Select an IP camera and click this button to enable digital zoom. This function can also be enabled by right clicking the Monitoring Window.</p>
	<p>Zoom in/out:</p> <p>Click these buttons to zoom in/zoom out a PTZ camera if that camera supports digital zoom. With digital zoom enabled, the buttons can be used to zoom in/zoom out the camera digitally.</p>
	<p>Audio in:</p> <p>Enable/disable the camera's audio input.</p>
	<p>Audio Support (optional):</p> <p>Turn on or off the audio support for the live view page.</p>
	<p>Focus Control:</p> <p>Adjust the focus of the camera (if this feature is supported by that camera.)</p>
	<p>Quick Bookmark:</p> <p>Bookmark an instant video image for live view.</p>
	<p>Detailed Bookmark:</p> <p>Enter the details of a bookmarked image.</p>
	<p>Pan and Tilt:</p> <p>Click these buttons to pan or tilt the camera (If the pan and tilt control is supported by the camera.)</p>

3.15.4 Auto Cruising

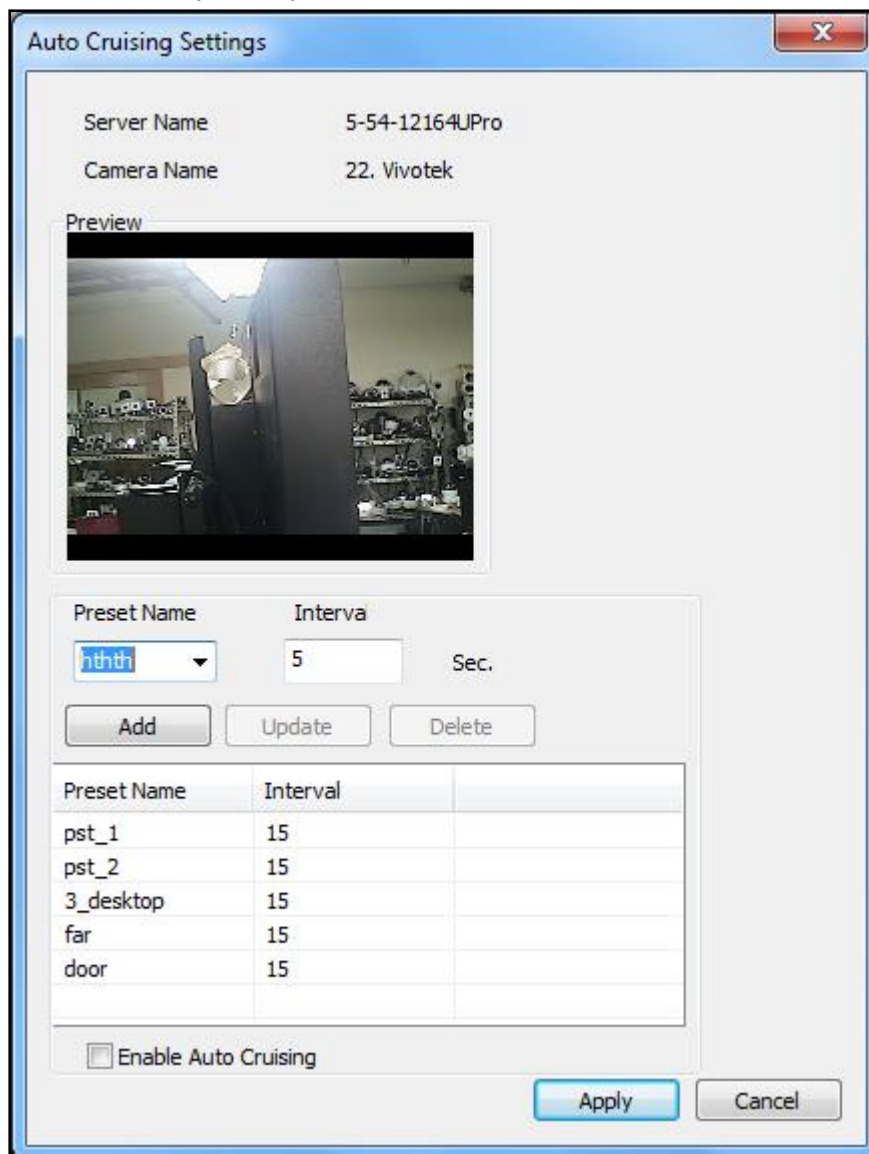
The auto cruising feature is used to configure the PTZ cameras to cruise according to the preset positions and the staying time set for each position.

To use the auto cruising feature, follow the steps below:

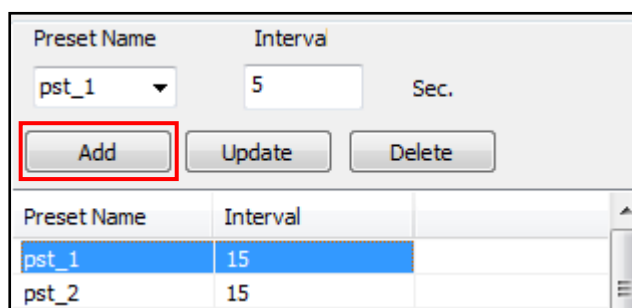
1. Right click the PTZ camera channel on the live view page. Select "Auto Cruising" > "Settings".



2. View the preset position of a camera:



3. Add a preset point: To add a preset position for auto cruising, select a "Preset Name" from the drop-down menu and enter the staying time (interval, in seconds). Click "Add".



4. Update a preset position: To change a setting on the list, highlight the selection. Select another preset position from the drop-down menu and change the staying time (interval). Click "Update".

The screenshot shows the PTZ camera settings interface. At the top, there is a 'Preset Name' dropdown menu with '3_desktop' selected, an 'Interval' input field with '5' entered, and a 'Sec.' label. Below these are three buttons: 'Add', 'Update' (highlighted with a red box), and 'Delete'. A table below the buttons lists preset positions:

Preset Name	Interval
pst_1	15
pst_2	15
3_desktop	15

Two red arrows point from the '3_desktop' row in the table to the 'Update' button and the 'Interval' input field in the second screenshot.

5. Delete: To delete a setting, highlight a selection on the list and click "Delete". To delete more than one settings, press and hold the Ctrl key on your keyboard and select the settings. Click "Delete".

The screenshot shows the PTZ camera settings interface. At the top, there is a 'Preset Name' dropdown menu with '3_desktop' selected, an 'Interval' input field with '5' entered, and a 'Sec.' label. Below these are three buttons: 'Add', 'Update', and 'Delete' (highlighted with a red box). A table below the buttons lists preset positions:

Preset Name	Interval
3_desktop	5
pst_2	15
3_desktop	15

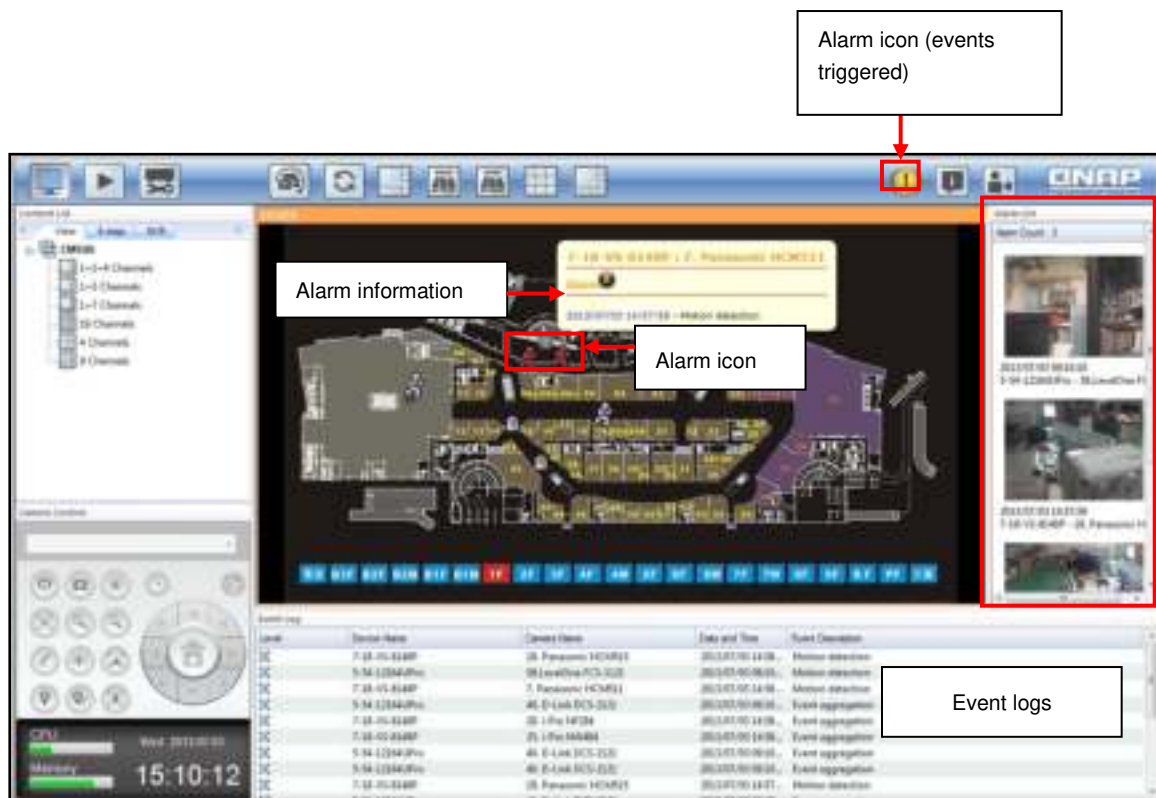
6. After configuring the auto cruising settings, select "Enable auto cruising" and click "OK". The PTZ camera will start auto cruising according to the settings.

Note:

- The default staying time (interval) of the preset position is 5 seconds. Enter 5–9999 seconds for this setting.
- The system supports up to 10 preset positions (the first 10) configured on the PTZ cameras. Up to 20 auto cruising settings can be configured. In other words, a maximum of 10 selections on the drop-down menu and 20 settings on the auto cruising list are supported.
- The name of a preset position can only be specified in languages other than English if it is supported by the camera.

3.15.5 Alarm Mode (Alarm List & Event Logs)

When an alarm is shown, click the icon to view the alarm information. The event logs will be shown at the bottom of the screen. If the E-map of the alarm camera is loaded, the Instant Popup Viewing window and the event logs can be displayed. Please refer to Chapter 3.3.7 for details.



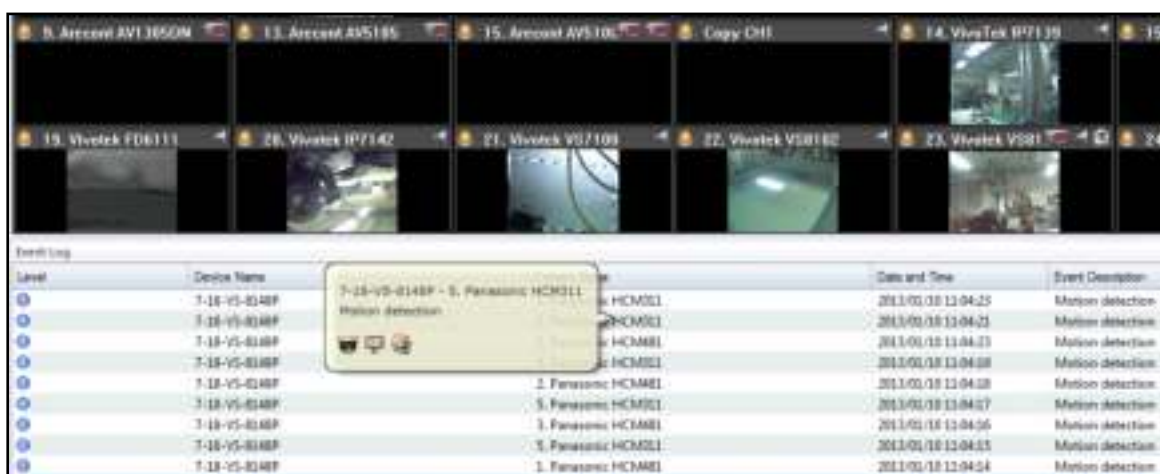
Note: The alarm settings must be configured on the NVR first. Then, go to Event Management settings in the CMS to enable the alarm input of the camera, so that the CMS can receive the alarms from the NVR. Please refer to [Chapter 7-10 \(FAQ\)](#) for details.

When an alarm is triggered, move the mouse cursor to the icon and the alarm information will be displayed. Double click the camera symbol to open the Instant Camera Viewing Popup Window and click the stop symbol to clear the alarm record. Double click the camera icon and a live window for the camera will pop up. If you further click the maximize button on the top right of the window, the video will occupy the single channel view for you to immediately monitor the camera where the alarm occurred. Click the close or restore down button to return to the E-map.








When moving the mouse cursor to the alarm snapshot in the alarm list to the right, the camera information and alarm content will both be shown.

Note: Only the first 150 records can be saved in the event logs.



The content of an event log includes the alarm event level, device (NVR) name, camera name, date and time an event occurs, and alarm details.

Note: The alarm list can be turned off, and so, to review an event, it is advised to check its recording files for more details...

Icon	Description
	Open the E-map of the alarm-triggered camera.
	Open the live view of the alarm-triggered camera.
	Show the pop-up window of the live view for the alarm-triggered camera.
	Immediately play back the video 15 seconds before or after the alarm is triggered.
	Turn off the camera alarm on the list. Please note that if a new alarm is triggered by a camera, the corresponding alarm will show up again.

3.15.6 E-map

Select the E-map tab on the left, double click or drag the E-map to the main screen to monitor.



Note: For more information on uploading E-maps, E-map related settings, and the camera icon settings on the E-map, please refer to Chapter 5.8.

An E-map provides the tooltip on camera information. Double click the camera icon to open the live view popup window, drag and move the window, or adjust the screen size.

Note: A maximum of 5 live view popup windows can be opened on the E-map at the same time.



Click the maximize button on top right side of the live view popup window to expand it. Click the close or restore down button to return to the original E-map.



In addition to the live view popup window feature, multiple E-maps can be linked and grouped together. Double click an E-map icon on the E-map to open another E-map. Please note that the E-map icon serves as a link. So, users can inter-link different E-maps to quickly switch between them.









The E-map provides a variety of features and relevant E-map settings are covered in Chapter [5.8](#).




After a camera alarm is triggered on the NVR, the alarm information will be shown.

E-map icons and description:

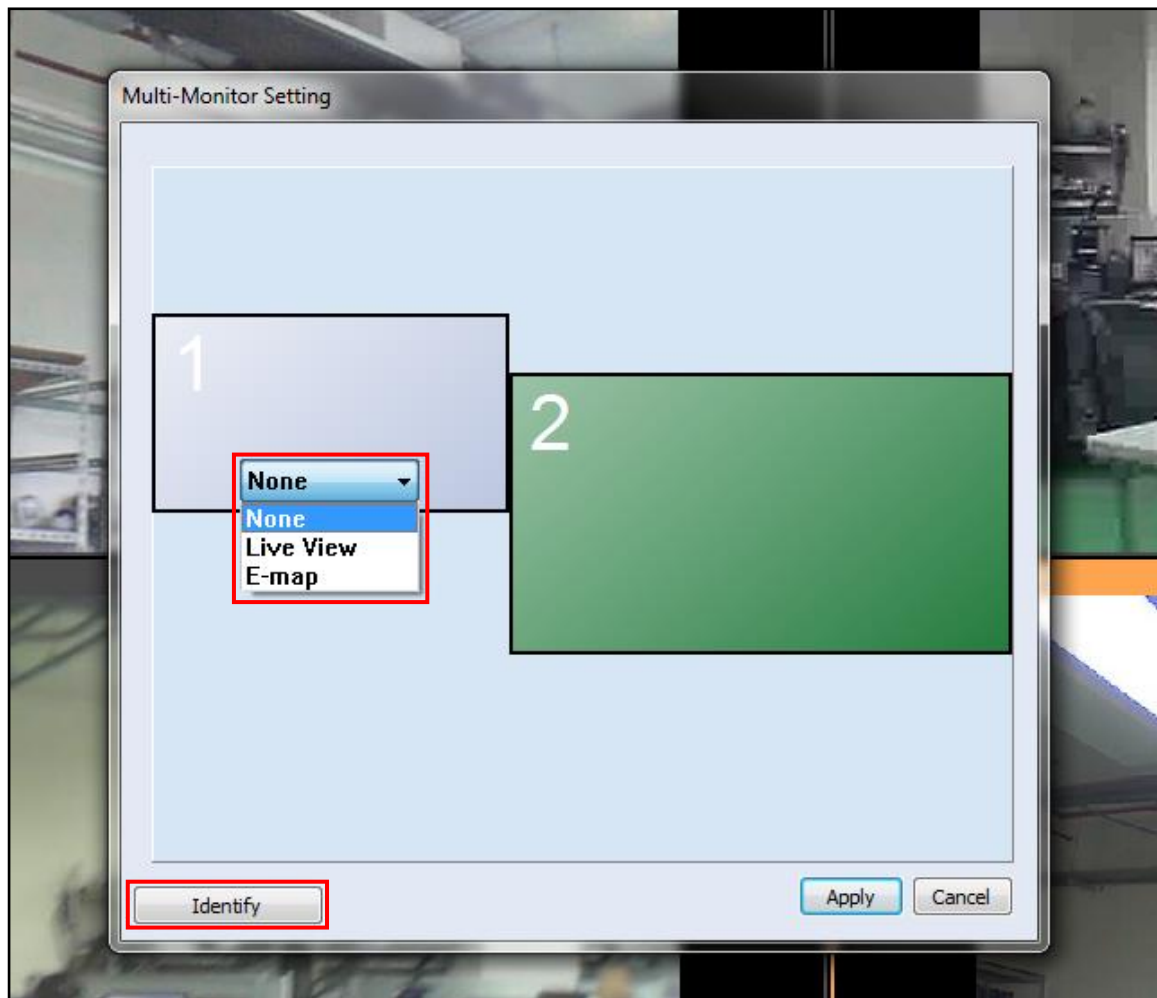
Icon	Description
	Multi-layer E-map: This icon shows that there are several layers in the E-map. Click the icon to enter the next layer in the E-map group.
	Single-layer E-map: Click  to select a single-layer E-map. When an E-map is selected, the icon will become  .
	E-map link: Double click this icon to link other E-maps.
	NVR: The NVR icon is only provided for users to pinpoint a NVR location on the map.

3.15.7 Multi-monitor Mode

Click the icon  in the Live View screen to configure the multi-monitor settings if multiple monitors (two to four) are connected to the client PC



The system will automatically retrieve the screen settings of the operating system. To identify the screen, click "Identify". Next, specify the screen function from the drop-down menu and the options include: None (do not display), Live view, and E-map.






The following shows an example of the Multi-monitor mode (Live View screen on the first monitor and E-map on the second monitor.)

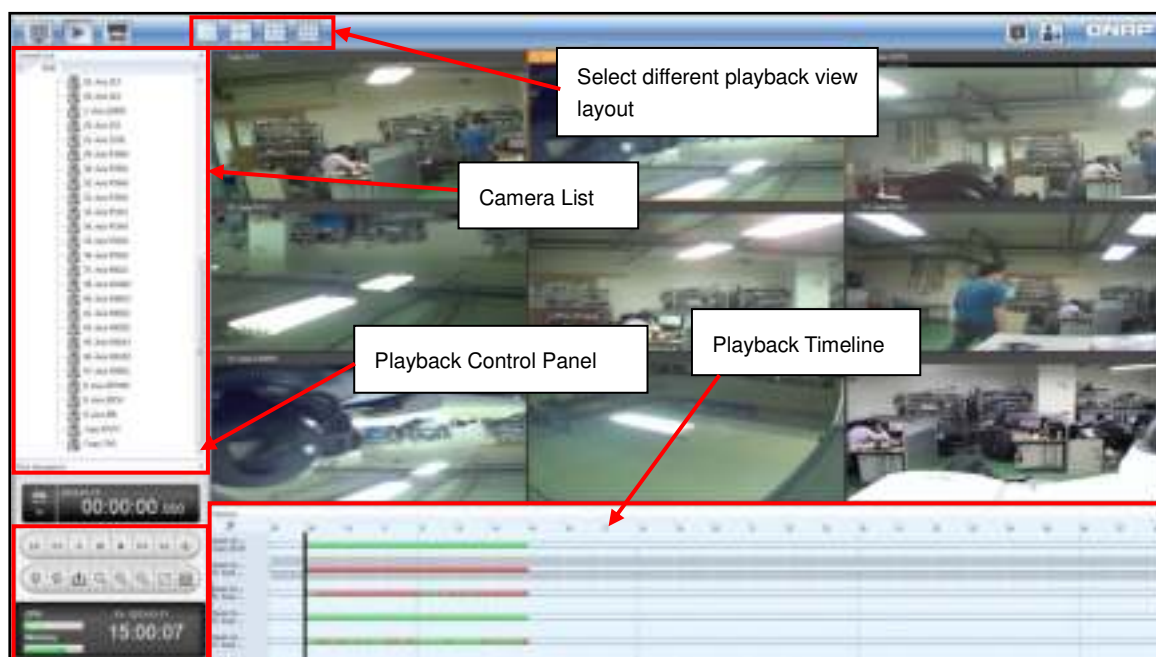


3.16 Playback

Using the CMS Client, you can playback recording files of a NVR on the playback page.













3.16.1 Video Playback Page







To switch to the Video Playback page, click the playback button  on the monitoring or management page. You can search and play the recording files on multiple NVR servers. To return to the live view page, click . To enter the system management page, click .



Note: The playback access right is required to play video files. For access right configuration, please refer to Chapter 5.9.1.

The icons and description of the video playback page are shown as below:

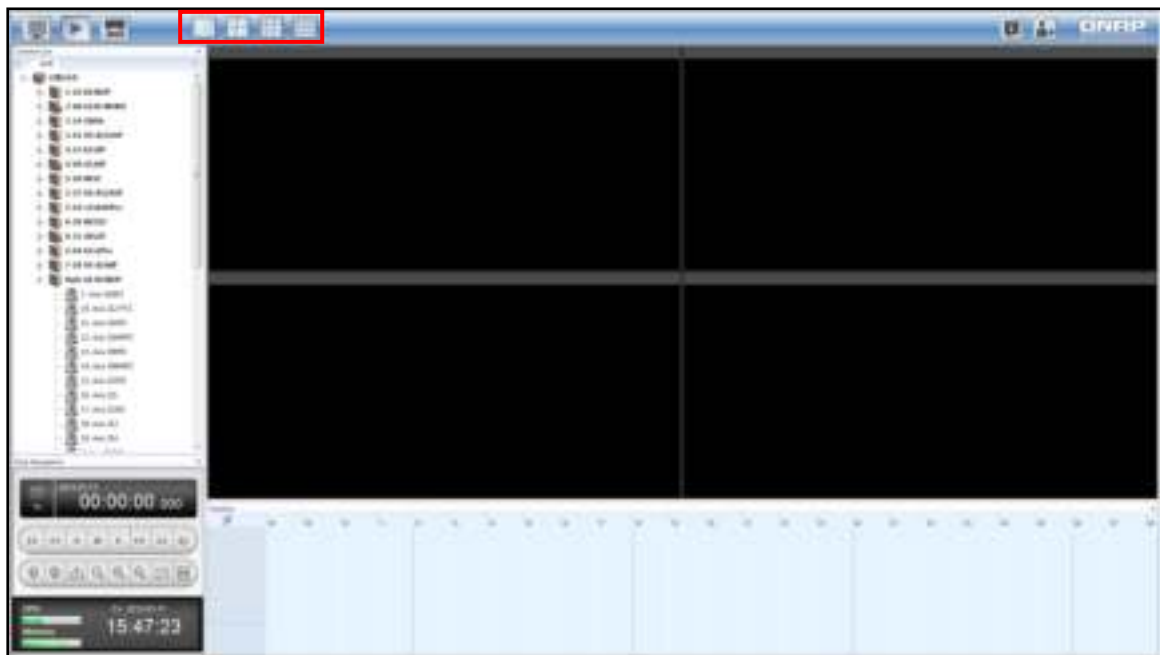
Icon	Description
	Single channel playback view.
	4-channel playback view.
	9-channel playback view.
	16-channel playback view.
	Export video: Export a video clip by entering the time interval of the playback.
	Audio (optional): Enable or disable the audio function.
	Digital zoom: Enable or disable the digital zoom function.
	Zoom in/out: Click these buttons to zoom in/zoom out a PTZ camera if that camera supports digital zoom. With digital zoom enabled, the buttons can be used to zoom in/zoom out the camera digitally.
	Set the playback interval: Set the time interval between the start and end points of a clip for playback. This interval cannot exceed 24 hours.
	Fit image to window/Keep aspect ratio: Adjust the proportions of all or only the current video depending on synchronous or asynchronous playback mode.
	Asynchronous/synchronous playback mode in the multi-view layout: Set the playback mode to be with the same playing time or with independent playing time for each channel, but all in the same interval.
	Quick bookmark: Bookmark an instant image of the camera.

	<p>Detailed bookmark: Enter the bookmark details of an instant image of the camera.</p>
	<p>Play/pause a video.</p>
	<p>Stop.</p>
	<p>Reverse playback.</p>
	<p>Decelerate/Accelerate.</p>
	<p>Previous frame/Next frame.</p>

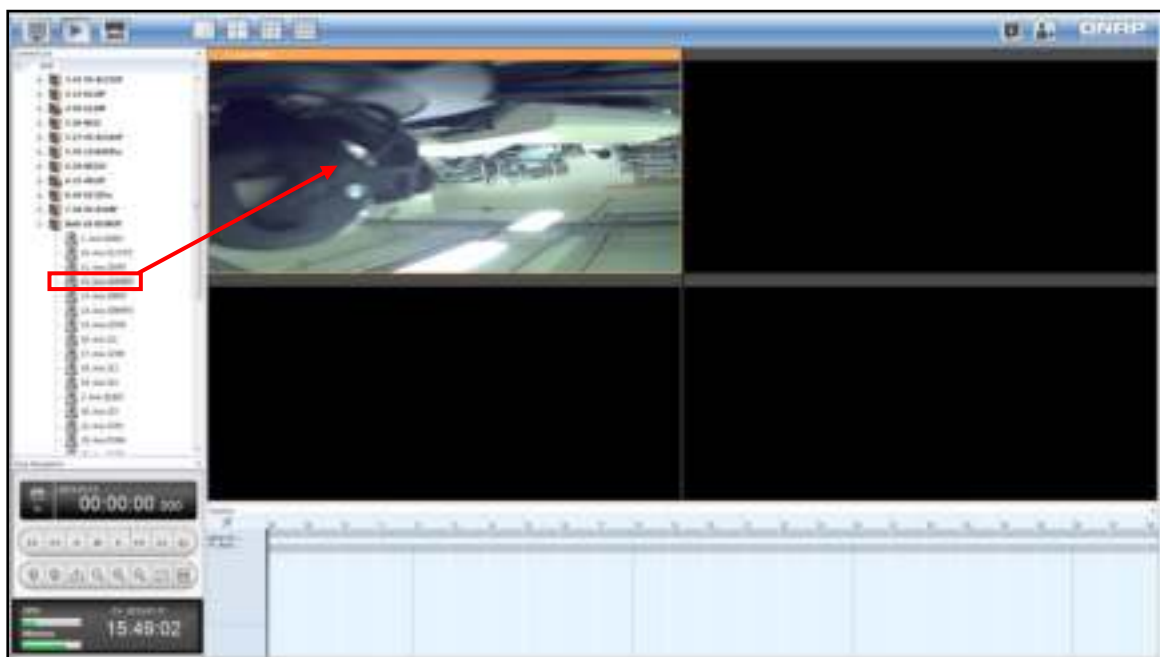
Playing recording files:

Follow the steps below to play the recording files on a remote NVR server:

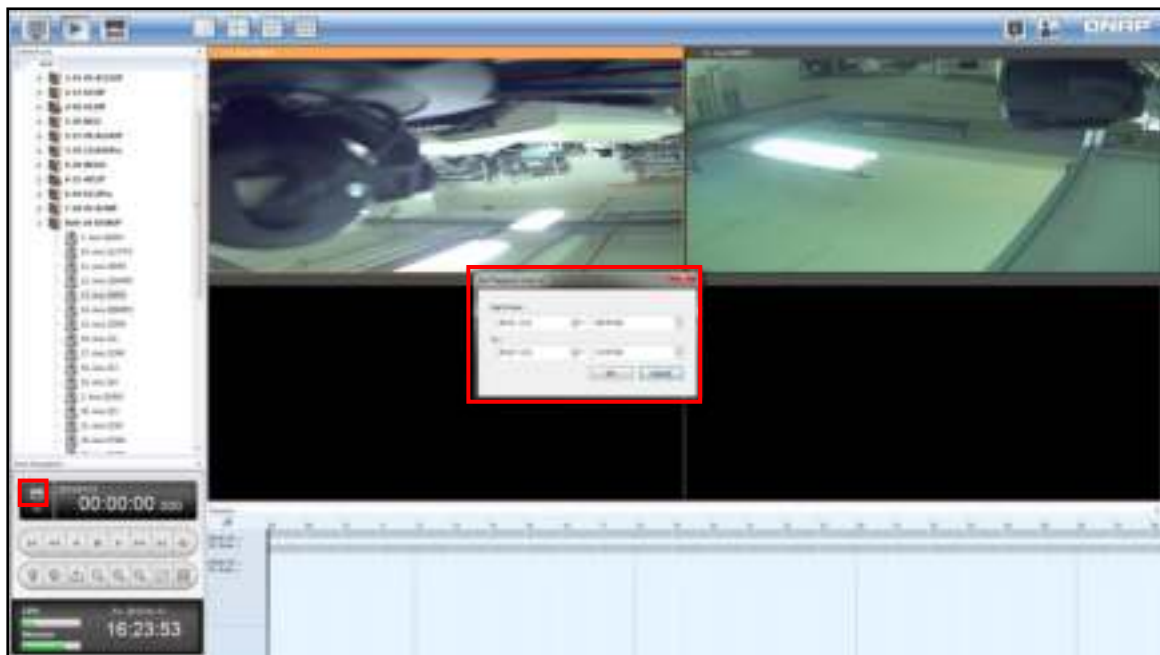
1. Select single-view or multi-view playback from the top.



2. Drag and drop a camera to the playback window.




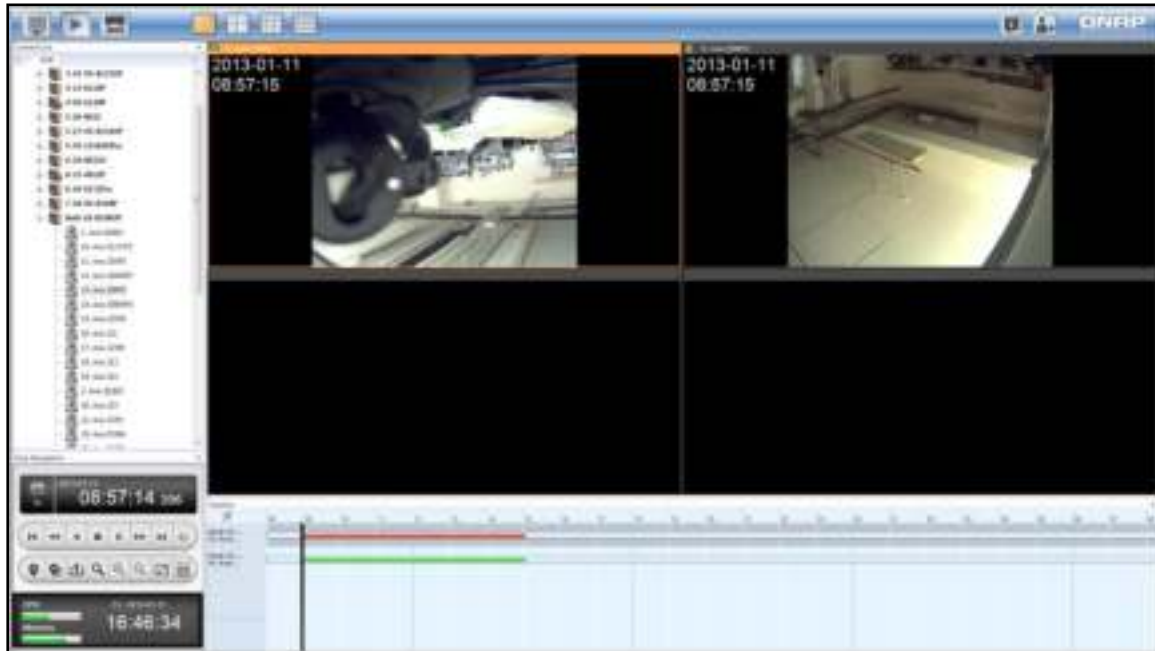
3. Set the playback interval. The interval cannot exceed 24 hours.




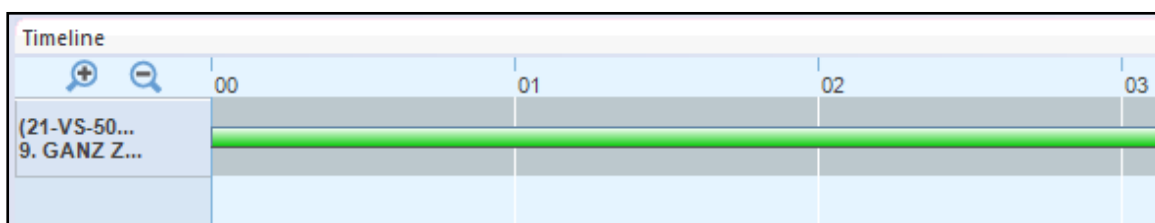
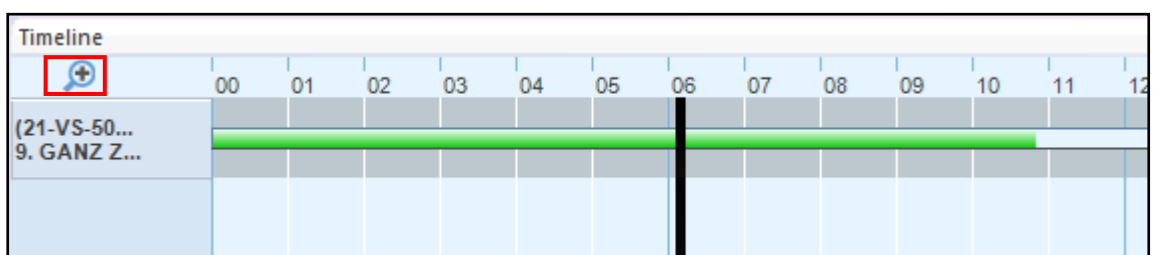
4. After setting the start and end time, the green bar(s), representing normal recording files, and the red bar(s), representing alarm recording files, will be shown on the timeline.

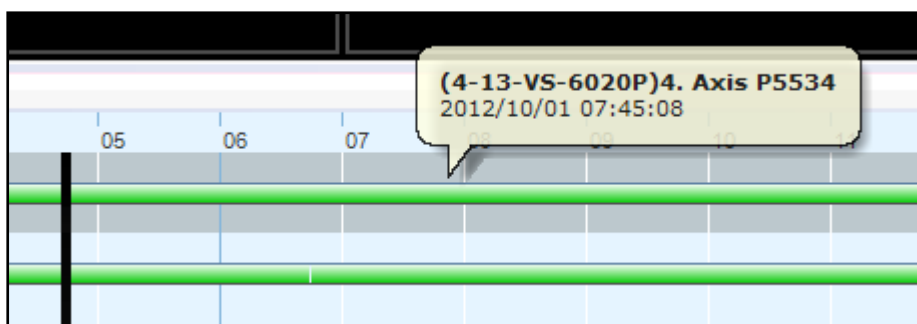


5. Click  or directly click on the timeline to playback the video. The NVR time for each channel is displayed on its respective screen. By default, the aspect ratio is kept for each camera.



6. Click the green parts of a timeline to view the camera image at the corresponding time point. Use the magnifying glass  to zoom in or out on the timeline. A tooltip with the time information will appear when moving the mouse cursor to a corresponding time point on the timeline.





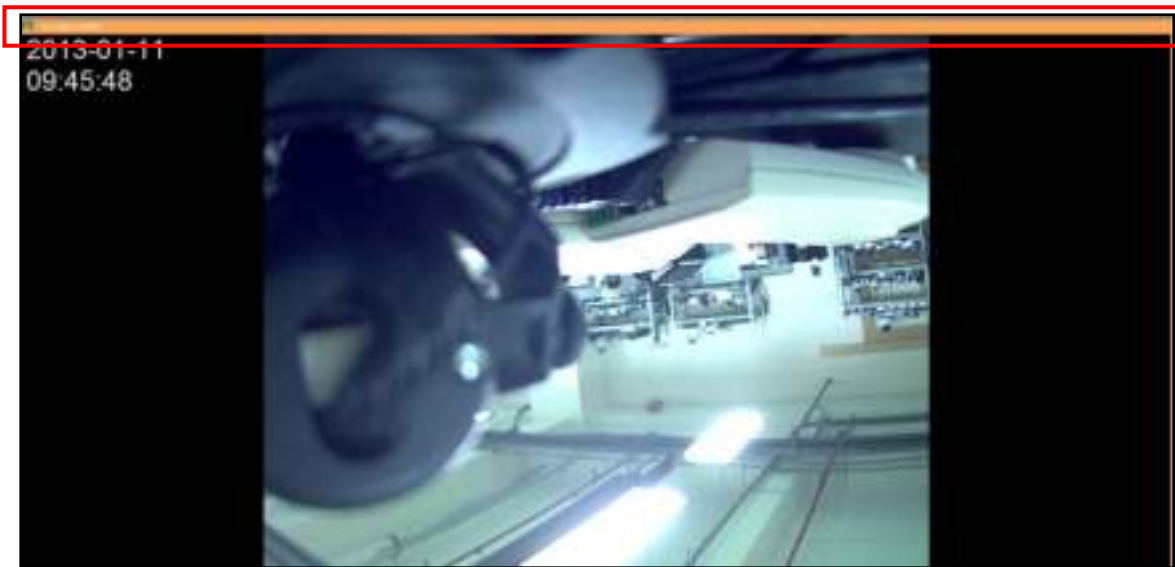
Note:

- The green parts on the timeline represent the intervals for round-the-clock recording files.
- After a camera is dragged to the screen and its recording files are being played, that channel window is reserved only for that camera until the current playback process is stopped and the camera status light turns red.
- The red parts on the green bars of the timeline represent the intervals for alarm recordings files. To use this feature, please configure the settings in "Camera settings" > "Alarm settings" on the NVR.

Double click the title of a camera to view its recording files in the single channel mode.
Double click the title again to return to the original viewing mode.

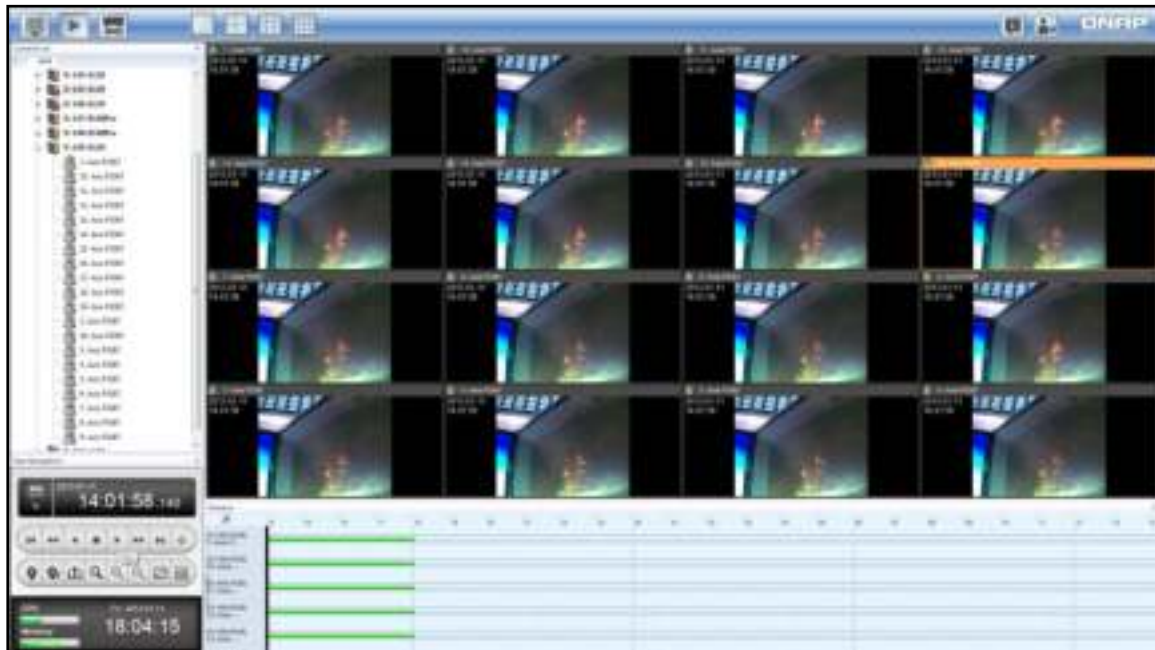
- In the 1 or 4-channel layout, you can right click each camera playback window to enable support for Intel hardware decoding (disabled by default).



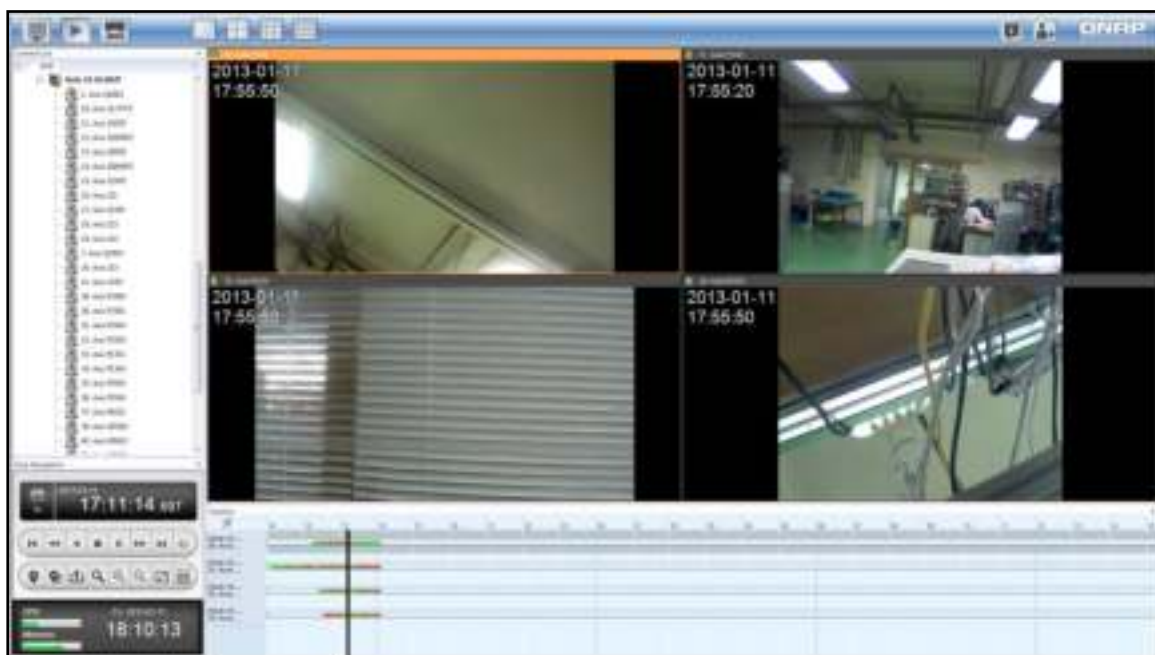


3.16.2 Multi-view Playback


Playback recording files of a maximum of 16 IP cameras concurrently.



By default, the multi-view playback time is synchronized.



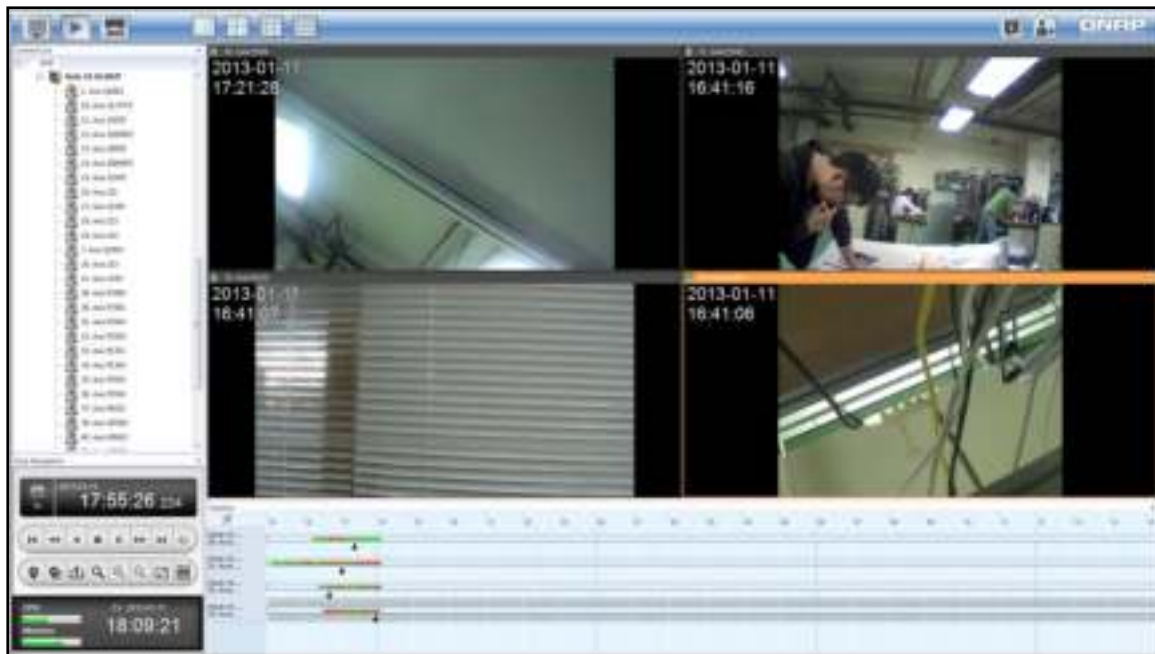
To playback each channel independently using the multi-view mode, click the synchronize

button  to cancel synchronization first.



In asynchronous playback, the timeline can be adjusted to playback at different time for each channel respectively.

Note: While switching to the asynchronous mode, you can independently playback each channel, but only within the same time interval.



Note: Click to align the time stamps of all channels according to that of the active channel (the channel that is being selected). For instance, the time stamps of all channels




played back are different in the figure above. After is clicked, the time stamps of all channels in the figure below will be aligned and played based on the channel four (the active channel.)




3.16.3 Exporting Video File

Follow the instructions below to convert the NVR recording files to the AVI format and save them to the local computer.

Note: The playback access rights of the IP camera need to be set before this feature can be used.

1. Select a NVR from the content list on the left, and drag and drop a channel (a camera icon) to be played to the playback window on the right.
2. Click  (Set Playback Interval) to select the interval.

3. Select the channel that you would like to export video files for and click  (Export video file) on the panel.



Note: Only green and red parts on the timeline can be selected to export video files.

4. Enter the storage path and file name of the video file and click "Export". You can watch the video in the preview window. The time it takes to export the files varies depending on computer performance.



Chapter 4 Server Log

The CMS logs are divided into event logs, service logs, and system logs. Among them, the event logs are shown on the main monitoring page, and the remaining two types of logs are in the server logs/ configuration. Besides the logs on the main monitoring page, you can switch to the previous or next page and refresh the page to check other available logs.

Note: Currently, only English event logs are supported by the CMS system.

4.1 Event Log

After the alarm mode is enabled, the following camera event logs will be recorded and listed at bottom of the page: IP camera connection, motion detection, or IP camera permission authentication failure.

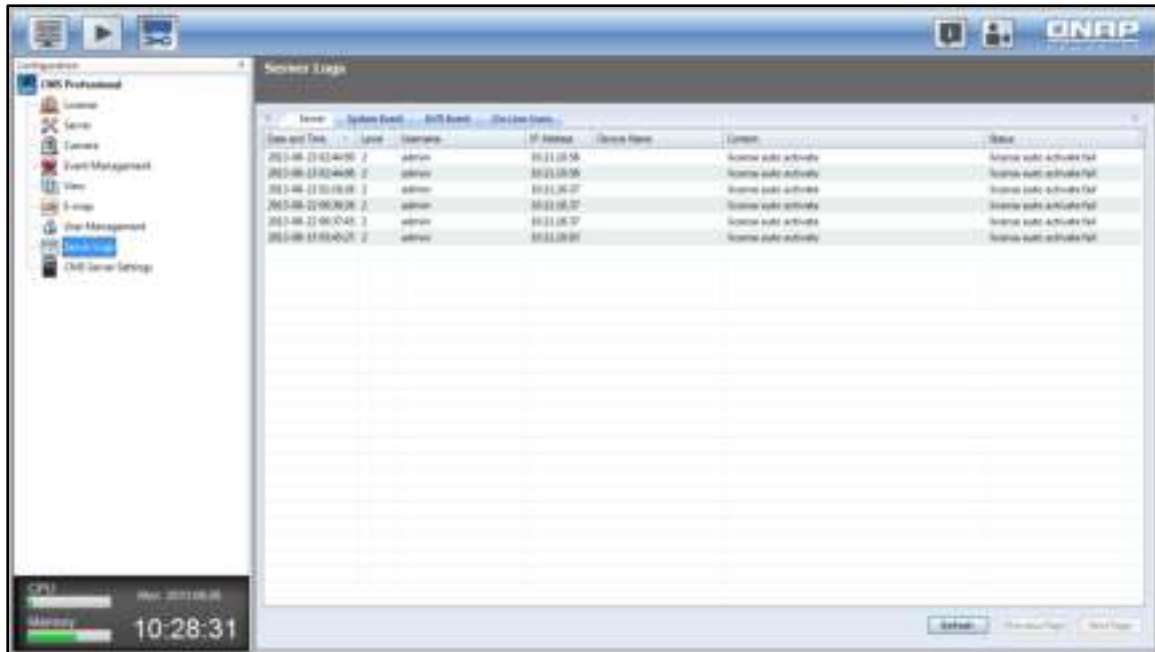


Level	Device Name	Camera Name	Date and Time	Event Description
③	7-28-VS-R148P	7. Panasonic HCM13	2013/05/13 19:30:43	Motion detection
③	7-28-VS-R148P	1. Panasonic HCM12	2013/05/13 19:30:42	Motion detection
③	7-27-VS-R124P	22. ACT-R124P-M23	2013/05/13 19:40:24	Motion detection

For each record, its priority level, device name, camera name, data and time and event description are displayed from left to right, and older logs (the first and oldest 150 records) will be overwritten automatically.

4.2 Service Log

Click "Server Log" on the configuration page and then the "System Event" tab to list all service logs. Each record listed is recorded from the last login to the current login. The log content is the communications, including messages, warnings, and errors, between the CMS system applications and the PC, CMS Server, or other NVR devices

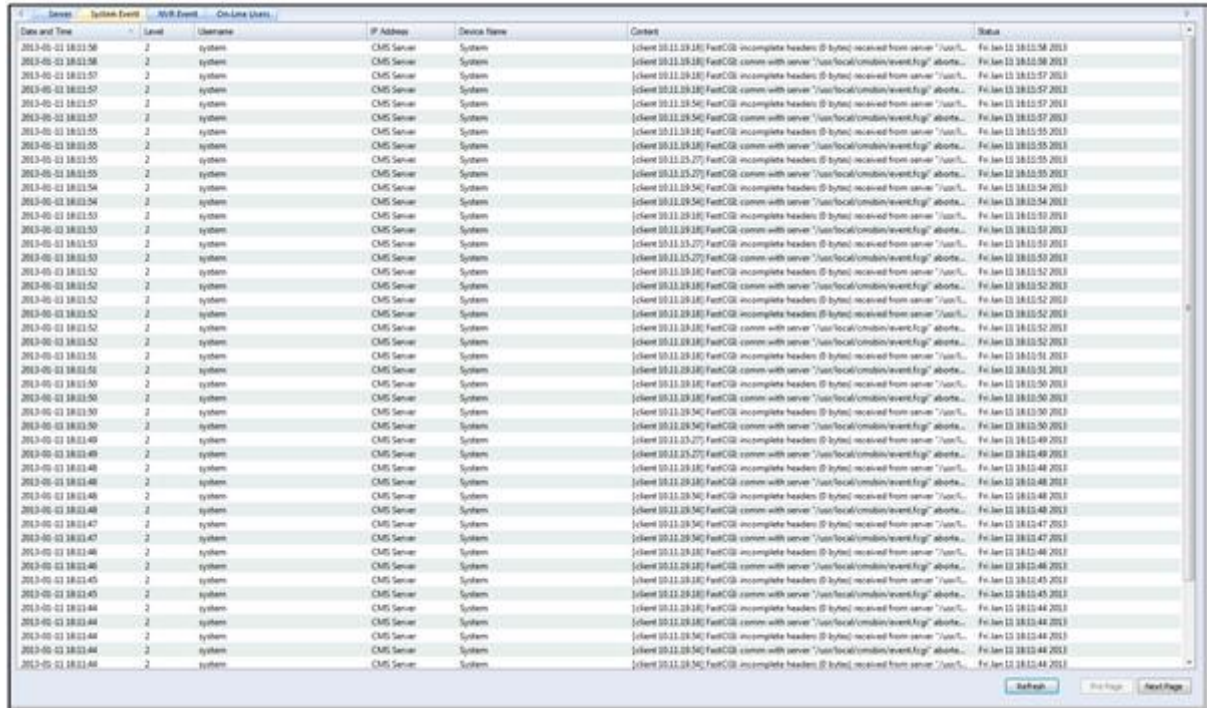


Date and Time	Level	Username	IP Address	Device Name	Content	Status
2013-08-23 01:44:50	2	admin	10.11.18.56		License auto activate fail	License auto activate fail
2013-08-23 01:44:50	2	admin	10.11.18.56		License auto activate fail	License auto activate fail
2013-08-23 01:45:00	2	admin	10.11.18.57		License auto activate fail	License auto activate fail
2013-08-23 01:45:00	2	admin	10.11.18.57		License auto activate fail	License auto activate fail
2013-08-23 01:45:00	2	admin	10.11.18.57		License auto activate fail	License auto activate fail
2013-08-23 01:45:01	2	admin	10.11.18.57		License auto activate fail	License auto activate fail

For each record, its date and time, event level, username, IP address, device name, the log content and status are displayed from left the right.

4.3 System Log

The second item of the system configuration is system logs. The recording range is the interval from the last login to the current login. The content is the content of the events occurring at the bottom level of the CMS system, or the problems occurring between the underlying system and other devices, such as system malfunctions. You can view the event logs as the basis of diagnosing system problems.



The screenshot displays a web-based interface for viewing system logs. At the top, there are tabs for 'Server', 'System Event', 'All Event', and 'On-Line Users', with 'System Event' currently selected. Below the tabs is a table with the following columns: 'Date and Time', 'Level', 'Username', 'IP Address', 'Device Name', 'Content', and 'Status'. The table contains multiple rows of log entries, all showing a level of '2' and a username of 'system'. The 'Content' column provides detailed descriptions of events, such as 'FastCGI: incomplete headers (0 bytes) received from server' and 'FastCGI: cannot with server'. The 'Status' column shows the time of the event, for example, 'Fri Jan 10 18:11:58 2013'. At the bottom right of the table, there are buttons for 'Refresh', 'Prev Page', and 'Next Page'.

Date and Time	Level	Username	IP Address	Device Name	Content	Status
2013-01-10 18:11:58	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:58 2013
2013-01-10 18:11:58	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:58 2013
2013-01-10 18:11:57	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:57 2013
2013-01-10 18:11:57	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:57 2013
2013-01-10 18:11:57	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:57 2013
2013-01-10 18:11:57	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:57 2013
2013-01-10 18:11:55	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:55 2013
2013-01-10 18:11:55	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:55 2013
2013-01-10 18:11:55	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:55 2013
2013-01-10 18:11:55	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:55 2013
2013-01-10 18:11:54	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:54 2013
2013-01-10 18:11:54	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:54 2013
2013-01-10 18:11:53	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:53 2013
2013-01-10 18:11:53	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:53 2013
2013-01-10 18:11:53	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:53 2013
2013-01-10 18:11:53	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:53 2013
2013-01-10 18:11:53	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:53 2013
2013-01-10 18:11:53	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:53 2013
2013-01-10 18:11:52	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:52 2013
2013-01-10 18:11:52	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:52 2013
2013-01-10 18:11:52	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:52 2013
2013-01-10 18:11:52	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:52 2013
2013-01-10 18:11:52	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:52 2013
2013-01-10 18:11:52	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:52 2013
2013-01-10 18:11:51	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:51 2013
2013-01-10 18:11:51	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:51 2013
2013-01-10 18:11:50	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:50 2013
2013-01-10 18:11:50	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:50 2013
2013-01-10 18:11:50	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:50 2013
2013-01-10 18:11:50	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:50 2013
2013-01-10 18:11:50	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:50 2013
2013-01-10 18:11:50	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:50 2013
2013-01-10 18:11:49	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:49 2013
2013-01-10 18:11:49	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:49 2013
2013-01-10 18:11:49	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:49 2013
2013-01-10 18:11:49	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:49 2013
2013-01-10 18:11:48	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:48 2013
2013-01-10 18:11:48	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:48 2013
2013-01-10 18:11:48	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:48 2013
2013-01-10 18:11:48	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:48 2013
2013-01-10 18:11:47	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:47 2013
2013-01-10 18:11:47	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:47 2013
2013-01-10 18:11:46	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:46 2013
2013-01-10 18:11:46	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:46 2013
2013-01-10 18:11:45	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:45 2013
2013-01-10 18:11:45	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:45 2013
2013-01-10 18:11:44	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:44 2013
2013-01-10 18:11:44	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:44 2013
2013-01-10 18:11:44	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:44 2013
2013-01-10 18:11:44	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: cannot with server "/usr/local/condom/event/cgi" abort...	Fri Jan 10 18:11:44 2013
2013-01-10 18:11:44	2	system	CMS Server	System	[event 10.11.10.181] FastCGI: incomplete headers (0 bytes) received from server "/usr/L...	Fri Jan 10 18:11:44 2013

From left to right, the following log details are displayed: time, event level, username, IP address, device name (all names listed here will be shown as "System"), the event summary and status.

4.4 NVR Event Log

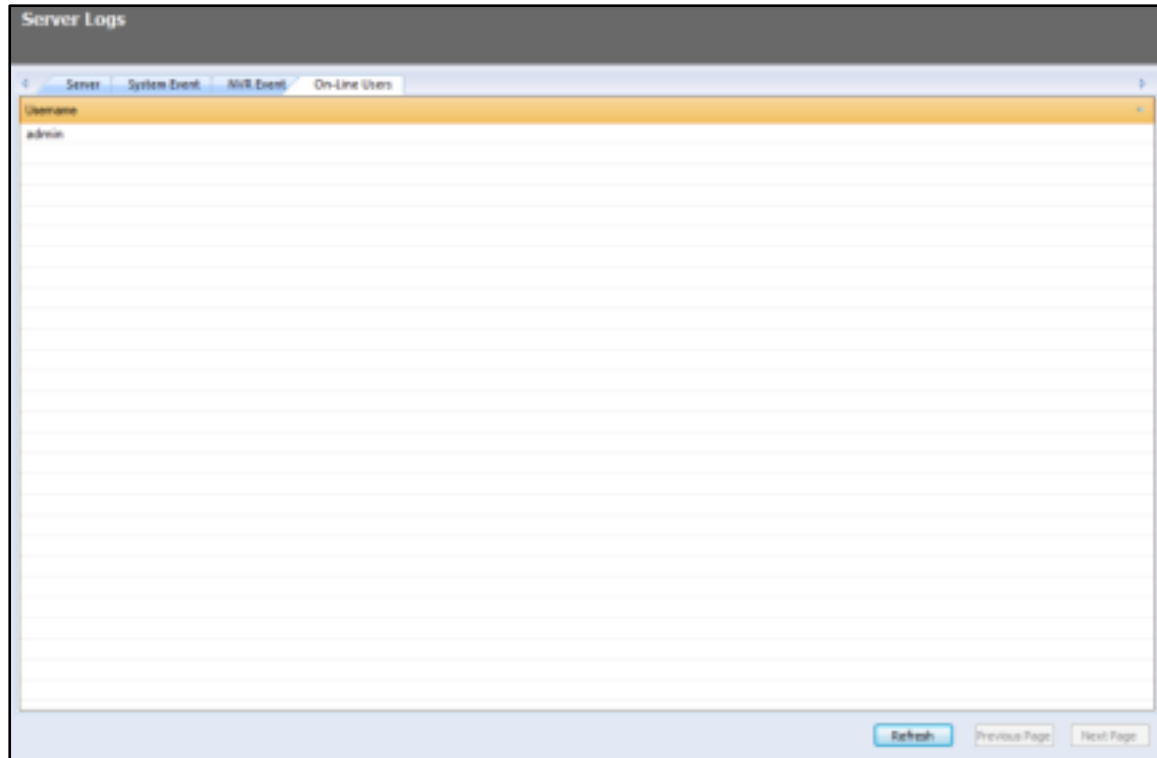
As the name implies, NVR event logs are event logs associated with an NVR or IP cameras. Click "Server Log" on the configuration page and then the "NVR Event" tab to list all NVR event logs. Each record listed is recorded from the last login to the current login.

[illegible]

For each record, its date and time, event level, username, IP address, device name (for now, the name will only be NVR or camera), the content of the event and status are displayed from left the right.

4.5 Online User

To check on current online users, click "Server Log" on the configuration page and then the "ON-Line Users" tab. Click the "Previous", "Next" and "Refresh" buttons at bottom right side of the screen to list other online users.



Chapter 5 CMS Server Management

5.1 General Setting

5.1.1 System Administration

Enter the name of the CMS server. The system name supports a maximum of 14 characters and can be a combination of alphabets (a-z, A-Z), numbers (0-9), and dash (-). Space (), period (.), or pure number are not allowed.



The screenshot shows the 'General Settings' interface with the 'SYSTEM ADMINISTRATION' tab selected. The 'System Administration' section contains the following fields and options:

- Server Name:** A text input field containing 'CMS'.
- System Port:** A text input field containing '8080'.
- Enable Secure Connection (SSL):** A checked checkbox.
- Port Number:** A text input field containing '8081'.
- Force secure connection (SSL) only:** An unchecked checkbox.
- Note:** After enabling the "Force secure connection (SSL) only" option, the Web Administration can only be connected via https.
- APPLY:** A button at the bottom right.

Specify the port number used for system connection and the default value is 8080.

Enable Secure Connection (SSL)

To allow the users to connect the CMS Server, turn on secure connection (SSL) and enter the port number. If the "Force secure connection (SSL) only" option is enabled, the users can only connect to the CMS Server by HTTPS connection.

5.1.2 Date and Time

Adjust the date, time, and time zone according to your current location.

If the settings are incorrect, the timestamps (the event occurring time) on the recording files will be inaccurate.

General Settings

SYSTEM ADMINISTRATION **DATE AND TIME** DAYLIGHT SAVING TIME LANGUAGE PASSWORD STRENGTH

Current date and time

2013/3/7 14:36:17 Thursday

Date and Time

Time Zone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London ▼

Date Format: yyyy/MM/DD ▼

Time Setting: 24HR ▼

☒ Manual Setting

Date/Time: 2013/3/7 / 14 : 33 : 52

☐ Synchronize with an internet time server automatically

Server: pool.ntp.org

Time Interval: 1 day(s) =

Set the server time the same as your computer time **UPDATE NOW**

APPLY

Synchronize with the time of your computer

To synchronize the time of the CMS Server with the time of your computer, click "Update Now".

Synchronize with an Internet time server automatically

Turn on this option to synchronize the date and time of the NAS automatically with an NTP (Network Time Protocol) server. Enter the IP address or domain name of the NTP server, for example, time.nist.gov, time.windows.com. Then enter the time interval for synchronization.

Note: The first time synchronization may take several minutes to complete.

5.1.3 Daylight Saving Time

If your region adopts daylight saving time (DST), turn on the option “Adjust system clock automatically for daylight saving time” and click “Apply”. The latest DST schedule of the time zone specified in the “Date and Time” section will be shown. The system time will be adjusted automatically according to the DST.

If your region does not adopt DST, the options on this page will not be available.

The screenshot shows the 'General Settings' page with the 'DAYLIGHT SAVING TIME' tab selected. The 'Daylight Saving Time' section displays the following information:

- Time Zone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London
- Recent daylight saving time: Start time: 2013/03/31, 01:00; End time: 2013/10/27, 02:00
- Offset: +50 minutes
- ☒ Adjust system clock automatically for daylight saving time.
- ☐ Enable customized daylight saving time table.
- APPLY button

To enter the daylight saving time table manually, select the option “Enable customized daylight saving time table”. Click “Add Daylight Saving Time Data” and enter the daylight saving time schedule. Then, click “Apply” to save the settings.

This screenshot shows the 'General Settings' page with the 'DAYLIGHT SAVING TIME' tab selected. The 'Daylight Saving Time' section displays the following information:

- ☒ Adjust system clock automatically for daylight saving time.
- ☒ Enable customized daylight saving time table.
- APPLY button

Below the 'Daylight Saving Time' section, the 'Customized Daylight Saving Time Tables' section is visible. It contains a table with columns: Start Time, End Time, Offset, and Action. A red box highlights the 'Add Daylight Saving Time Data' button in the Action column.

Start Time	End Time	Offset	Action
			Add Daylight Saving Time Data

5.1.4 Language

Select the language the CMS uses to display the files and directories.

Note: All the files and directories on the CMS will be created using Unicode encoding. If your PC does not support Unicode, select the language which is the same as the OS language of your PC in order to view the files and directories on the system properly.



5.1.5 Password Strength


Specify the password rules. After applying the settings, the system will automatically check the validity of the new password.

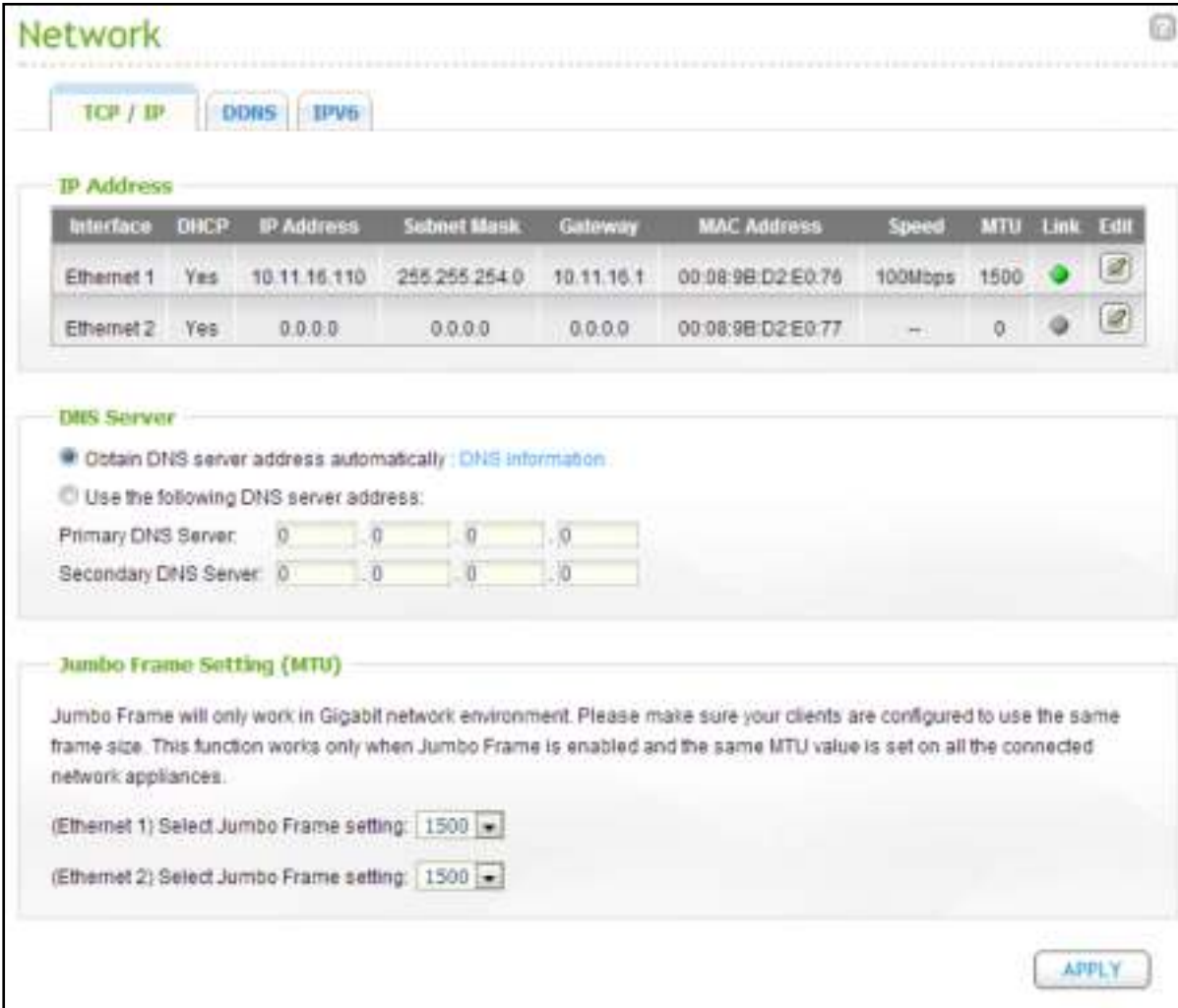


5.2 Network Setting





5.2.1 TCP/IP

(i) IP Address

Configure the TCP/IP settings of the CMS Server on this page. Click the Edit button () to edit the network settings (TCP/IP Property, as described in the following paragraphs). For the CMS Server with two LAN ports, users can connect both network interfaces to two different switches and configure the TCP/IP settings. The CMS Server will acquire two IP addresses which allow access from two different subnets. This is known as multi-IP settings. When using the QNAP Finder to detect the CMS IP, the IP of the Ethernet 1 will be shown in LAN 1 only and the IP of the Ethernet 2 will be shown in LAN 2 only.




The screenshot shows the 'Network' configuration page with tabs for 'TCP / IP', 'DDNS', and 'IPv6'. The 'IP Address' section contains a table with the following data:

Interface	DHCP	IP Address	Subnet Mask	Gateway	MAC Address	Speed	MTU	Link	Edit
Ethernet 1	Yes	10.11.16.110	255.255.254.0	10.11.16.1	00:08:9B:D2:E0:76	100Mbps	1500		
Ethernet 2	Yes	0.0.0.0	0.0.0.0	0.0.0.0	00:08:9B:D2:E0:77	--	0		

Below the table is the 'DNS Server' section with two options: 'Obtain DNS server address automatically' (selected) and 'Use the following DNS server address'. The latter has input fields for Primary and Secondary DNS Servers, both set to 0.0.0.0.

The 'Jumbo Frame Setting (MTU)' section includes a warning about Gigabit network environments and two dropdown menus for Ethernet 1 and Ethernet 2, both set to 1500.

An 'APPLY' button is located at the bottom right of the page.

Click the Edit button () as described above to open the "TCP/IP Property" page and configure the following settings:

TCP/IP - Property

Network Speed: Auto-negotiation

☒ Obtain IP address settings automatically via DHCP

☐ Use static IP address

Fixed IP Address: 169 . 254 . 100 . 100

Subnet Mask: 255 . 255 . 0 . 0

Default Gateway: 169 . 254 . 100 . 100

☐ Enable DHCP Server

Start IP Address: 10 . 11 . 1 . 100

End IP Address: 10 . 11 . 1 . 200

Lease Time: 1 Day 0 Hour

Step 1 of 1

APPLY CANCEL

Network Speed

Select the network transfer rate according to the network environment to which the CMS Server is connected. Select auto negotiation and the system will adjust the transfer rate automatically.

Obtain the IP address settings automatically via DHCP

If the network supports DHCP, select this option and the CMS Server will obtain the IP address and network settings automatically.

Use static IP address

To use a static IP address for network connection, enter the IP address, subnet mask, and default gateway.

Enable DHCP Server

A DHCP (Dynamic Host Configuration Protocol) server assigns IP addresses to the clients on a network. Select "Enable DHCP Server" to set the CMS Server a DHCP server if there is none on the local network where the CMS Server locates.

Note:

- Do not enable DHCP server if there is already one on the local network to avoid IP address conflicts or network access errors.
- The DHCP server option is available to Ethernet 1 only when both LAN ports of a dual LAN CMS Server are connected to the network and configured as standalone IP settings.

Start IP, End IP, and Lease Time: Set the range of IP addresses allocated by the CMS Server to the DHCP clients and the lease time. The lease time refers to the time that an IP address is leased to the clients. During that time, the IP will be reserved to the assigned client. When the lease time expires, the IP can be assigned to another client.

(ii) **Default Gateway**

Select the gateway settings. Please be reminded to select the first LAN port for the default gateway if both LAN ports are connected to the network.

(iii) **DNS Server**

Primary DNS Server: Enter the IP address of the primary DNS server. This server will provide the DNS service to dissolve domain names of the external network for the CMS Server.

Secondary DNS Server: Enter the IP address of the secondary DNS server. This server will be the second server to provide the DNS service for the CMS Server.

Note:

- Please contact the ISP or network administrator for the IP address of the primary and the secondary DNS servers. When the CMS Client needs the domain name to connect to the CMS Server, the client needs at least one DNS server IP for proper URL connection. Otherwise, the function may not work properly.
- If you select to obtain the IP address by DHCP, there is no need to configure the primary and the secondary DNS servers. In this case, enter "0.0.0.0".

5.2.2 **DDNS**

To allow remote access to the CMS Server using a domain name instead of a dynamic IP address, enable the DDNS service.

Network

TCP / IP

DDNS

IPv6

DDNS Service

After enabling DDNS Service, you can connect to this server by domain name.

☐ Enable Dynamic DNS Service

Select DDNS server:

www.dyndns.com

Enter the account information you registered with the DDNS provider

User Name:

Password:

Host Name:

☐ Check the External IP Address Automatically

10 minutes

Current WAN IP: 118.166.234.178

Recent DDNS Update Result

Connection IP Last Checked:

Next Check for Connection IP:

Last DDNS Update Time:

Update Server Response:

APPLY

The CMS supports the following DDNS providers:

<http://www.dyndns.com>, <http://update.ods.org>, <http://www.dhs.org>, <http://www.dyns.cx>, <http://www.3322.org>, <http://www.no-ip.com> °

5.2.3 IPv6


The CMS supports IPv6 connectivity with “stateless” address configurations and RADVD (Router Advertisement Daemon) for IPv6, RFC 2461 to allow the hosts on the same subnet to acquire IPv6 addresses from the CMS automatically.

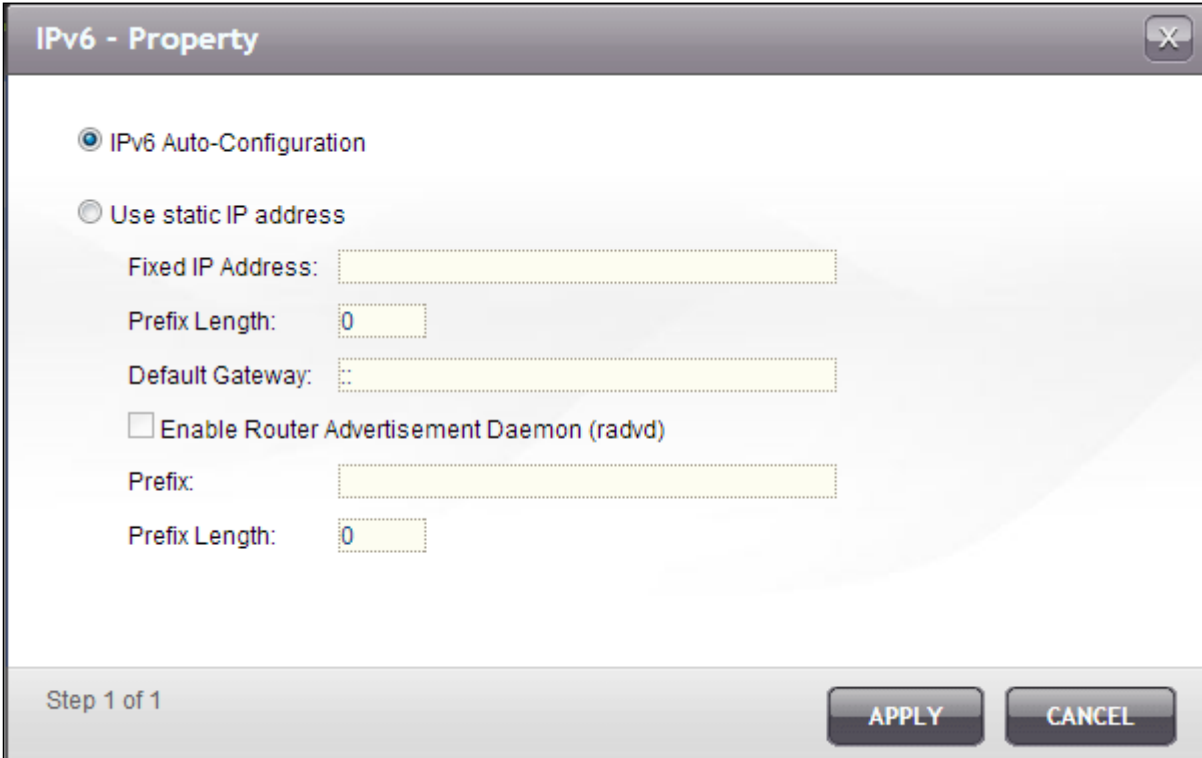


The screenshot shows a 'Network' configuration window with tabs for 'TCP / IP', 'DDNS', and 'IPv6'. The 'IPv6' tab is active. Under the 'IPv6 Address' section, the 'Enable IPv6' checkbox is checked. Below this is a table with the following data:

Interface	Auto Configuration	IPv6 Address	Prefix Length	Gateway	Link	Edit
Ethernet 1	Yes	fe80::208:9bff:fed2:e076	64	...		

Below the table is a 'DNS Server' section with two empty text input fields. An 'APPLY' button is located at the bottom right of the window.

To use this function, select the option “Enable IPv6” and click “Apply”. The CMS will restart. After the system restarts, login the IPv6 page again. The settings of the IPv6 interface will be shown. Click the Edit button  to edit the settings.



The screenshot shows the 'IPv6 - Property' dialog box. It has two radio button options: 'IPv6 Auto-Configuration' (selected) and 'Use static IP address'. Under 'Use static IP address', there are input fields for 'Fixed IP Address:', 'Prefix Length:' (set to 0), and 'Default Gateway:'. There is also an unchecked checkbox for 'Enable Router Advertisement Daemon (radvd)'. Below this are input fields for 'Prefix:' and 'Prefix Length:' (set to 0). At the bottom, it says 'Step 1 of 1' and has 'APPLY' and 'CANCEL' buttons.

IPv6 Auto Configuration

If an IPv6 enabled router is available on the network, select this option to allow the CMS Server to acquire the IPv6 address and the configurations automatically.

Use static IP address

To use a static IP address, enter the IP address (e.g. 2001:bc95:1234:5678), prefix length (e.g. 64), and the gateway address for the CMS. You may contact your ISP for the information of the prefix and the prefix length.

- Enable Router Advertisement Daemon (radvd)

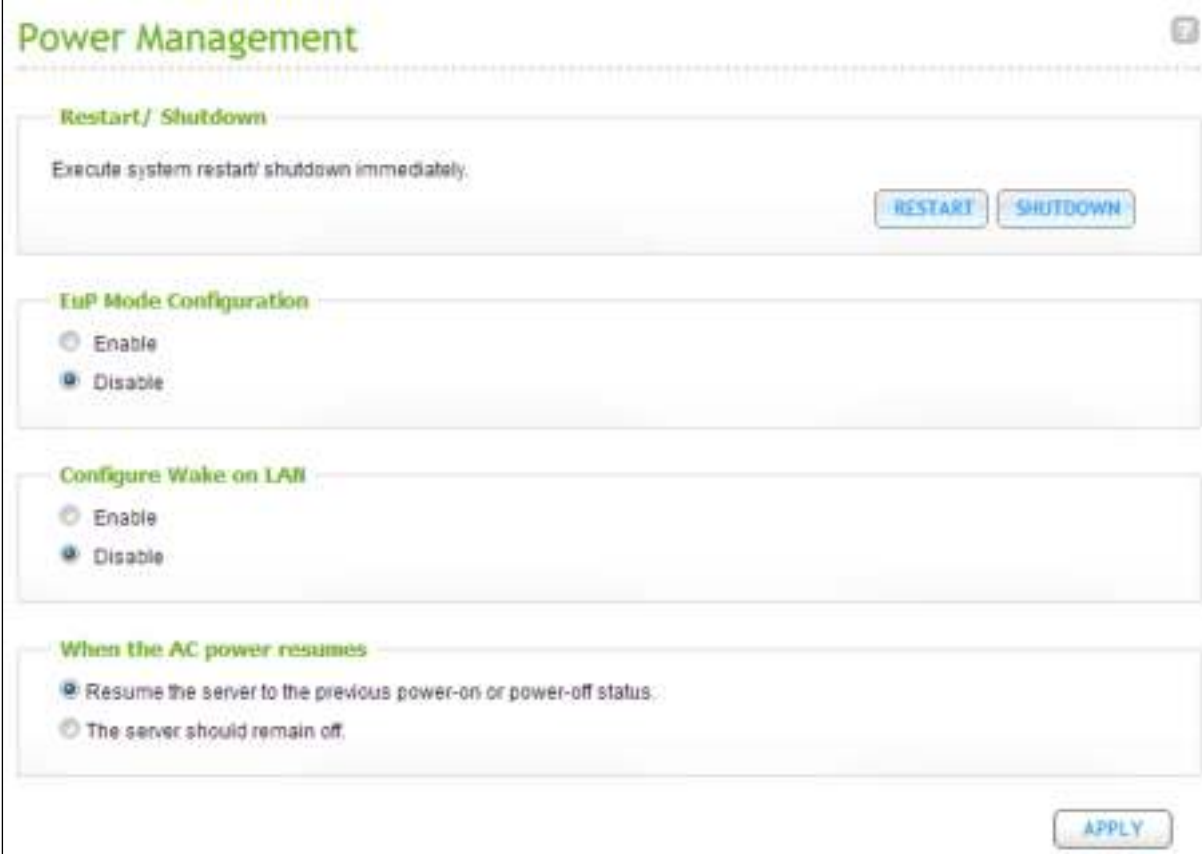
To configure the CMS Server as an IPv6 host and distribute IPv6 addresses to the local clients which support IPv6, enable this option and enter the prefix and prefix length.

IPv6 DNS server

Enter the preferred DNS server in the upper field and the alternate DNS server in the lower field. Contact the ISP or network administrator for the information. If IPv6 auto configuration is selected, leave the fields as "::".

5.3 Power Management

You can restart or shut down the CMS Server and specify the behavior of the CMS Server after a power recovery.



The screenshot shows a web interface titled "Power Management" with a help icon in the top right corner. It contains four main configuration sections:

- Restart/ Shutdown**: A section with the instruction "Execute system restart/ shutdown immediately." and two buttons, "RESTART" and "SHUTDOWN", on the right.
- EuP Mode Configuration**: A section with two radio buttons: "Enable" and "Disable". The "Disable" option is selected.
- Configure Wake on LAN**: A section with two radio buttons: "Enable" and "Disable". The "Disable" option is selected.
- When the AC power resumes**: A section with two radio buttons: "Resume the server to the previous power-on or power-off status." (selected) and "The server should remain off."

An "APPLY" button is located at the bottom right of the interface.

Restart/Shutdown

Restart or shut down the CMS Server immediately.

If you try to restart or turn off the CMS Server from the web-based interface or the LCD panel (if available) when a remote replication job is in process, the CMS Server will prompt you to ignore the running replication job or not.

EuP Mode Configuration

EuP (also Energy-using Products) is a European Union (EU) directive designed to improve the energy efficiency of electrical devices, reduce use of hazardous substances, increase ease of product recycling, and improve environment-friendliness of the product.

When EuP is enabled, the following settings will be affected so that the CMS Server maintains low power consumption (less than 1W) when the CMS Server is powered off:

- Wake on LAN: Disabled.
- AC power resumption: The CMS will remain off after the power restores from an outage.

When EuP is disabled, the power consumption of the CMS Server is slightly higher than 1W when the CMS Server is powered off. EuP is disabled by default so that you can use the functions Wake on LAN, AC power resumption settings properly.

This feature is only supported by certain CMS Server models, please visit http://www.qnapsecurity.com/pro_detail_featurecms.asp?p_id=273 for details

Configure Wake on LAN

Turn on this option to allow the users to power on the CMS Server remotely by Wake on LAN. Note that if the power connection is physically removed (in other words, the power cable is unplugged) when the CMS Server is turned off, Wake on LAN will not function whether or not the power supply is reconnected afterwards.

When the AC Power resumes

Configure the CMS Server to resume to the previous power-on or power-off status, turn on, or remain off when the AC power resumes after a power outage.

5.4 Backup/Restore Settings



Backup System Settings

To back up all the settings, including the user accounts, server name, network configuration, and so on, click "BACKUP". If the system asks whether to open or save the backup image file, select "Save".

Restore System Settings

To restore all the settings, click "Browse" to select a previously saved setting file and click

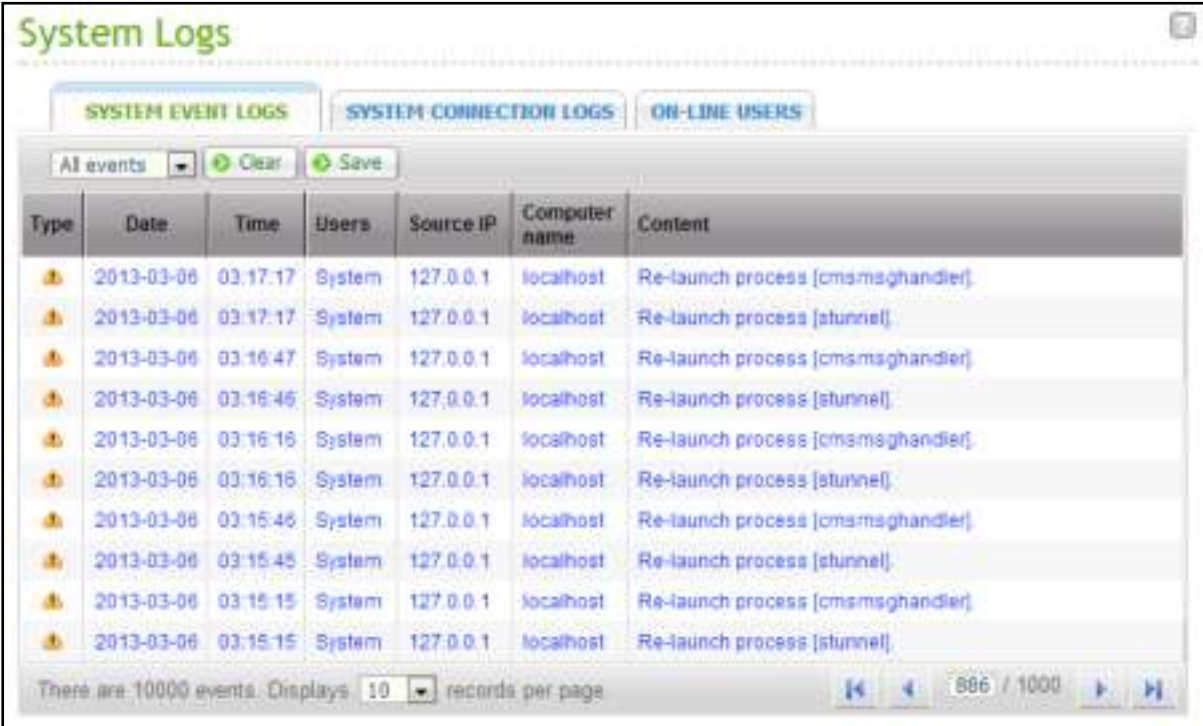
“Restore”.

5.5 System Log

5.5.1 System Event Log

The CMS Server can store 32,768 recent event logs, including warnings, errors, and information messages. If the CMS Server does not function correctly, refer to the event logs for troubleshooting.

Tip: Right click a log to delete the record. To clear all the logs, click “Clear”.



The screenshot shows a web interface titled "System Logs". It has three tabs: "SYSTEM EVENT LOGS" (selected), "SYSTEM CONNECTION LOGS", and "ON-LINE USERS". Below the tabs, there are buttons for "All events" (a dropdown menu), "Clear", and "Save". The main area contains a table with the following columns: Type, Date, Time, Users, Source IP, Computer name, and Content. The table lists several log entries, all from "System" users at "localhost" on "2013-03-06", describing "Re-launch process" for various components. At the bottom, it states "There are 10000 events. Displays 10 records per page" and includes pagination controls showing "886 / 1000".

Type	Date	Time	Users	Source IP	Computer name	Content
⚠	2013-03-06	03:17:17	System	127.0.0.1	localhost	Re-launch process [cmsmsgHandler].
⚠	2013-03-06	03:17:17	System	127.0.0.1	localhost	Re-launch process [stunnel].
⚠	2013-03-06	03:16:47	System	127.0.0.1	localhost	Re-launch process [cmsmsgHandler].
⚠	2013-03-06	03:16:46	System	127.0.0.1	localhost	Re-launch process [stunnel].
⚠	2013-03-06	03:16:16	System	127.0.0.1	localhost	Re-launch process [cmsmsgHandler].
⚠	2013-03-06	03:16:16	System	127.0.0.1	localhost	Re-launch process [stunnel].
⚠	2013-03-06	03:15:46	System	127.0.0.1	localhost	Re-launch process [cmsmsgHandler].
⚠	2013-03-06	03:15:45	System	127.0.0.1	localhost	Re-launch process [stunnel].
⚠	2013-03-06	03:15:15	System	127.0.0.1	localhost	Re-launch process [cmsmsgHandler].
⚠	2013-03-06	03:15:15	System	127.0.0.1	localhost	Re-launch process [stunnel].

5.5.2 System Connection Log

The CMS Server can store 32,768 recent event logs, including warnings, errors, and information messages. If the CMS cannot be logged in normally, refer to the system connection logs for troubleshooting.

Click “Save” to save the log data as a CSV file and “Clear” to clear all the logs.

Note: Only English event logs are supported in this system.



5.5.3 On-line User

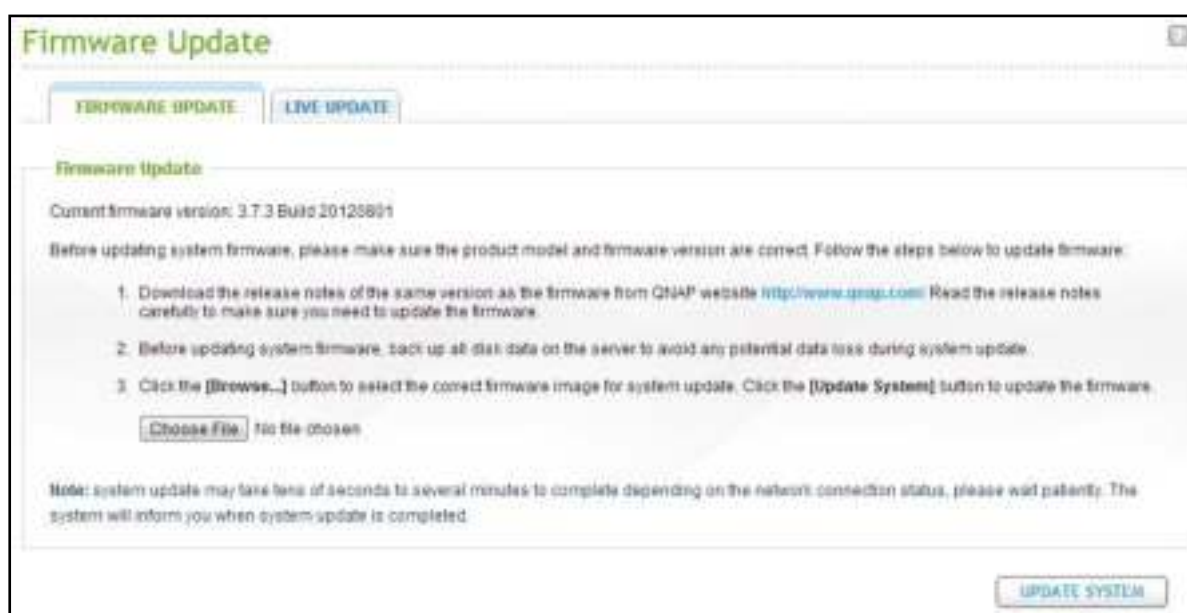
The information of the on-line users connecting to the CMS Server by networking services is shown on this page.

Tip: Right click a log to disconnect the IP connection and block the IP.



5.6 Firmware Update

5.6.1 Update Firmware by Web Administration Page



Note: If the system is running properly, there is no need to update the firmware.

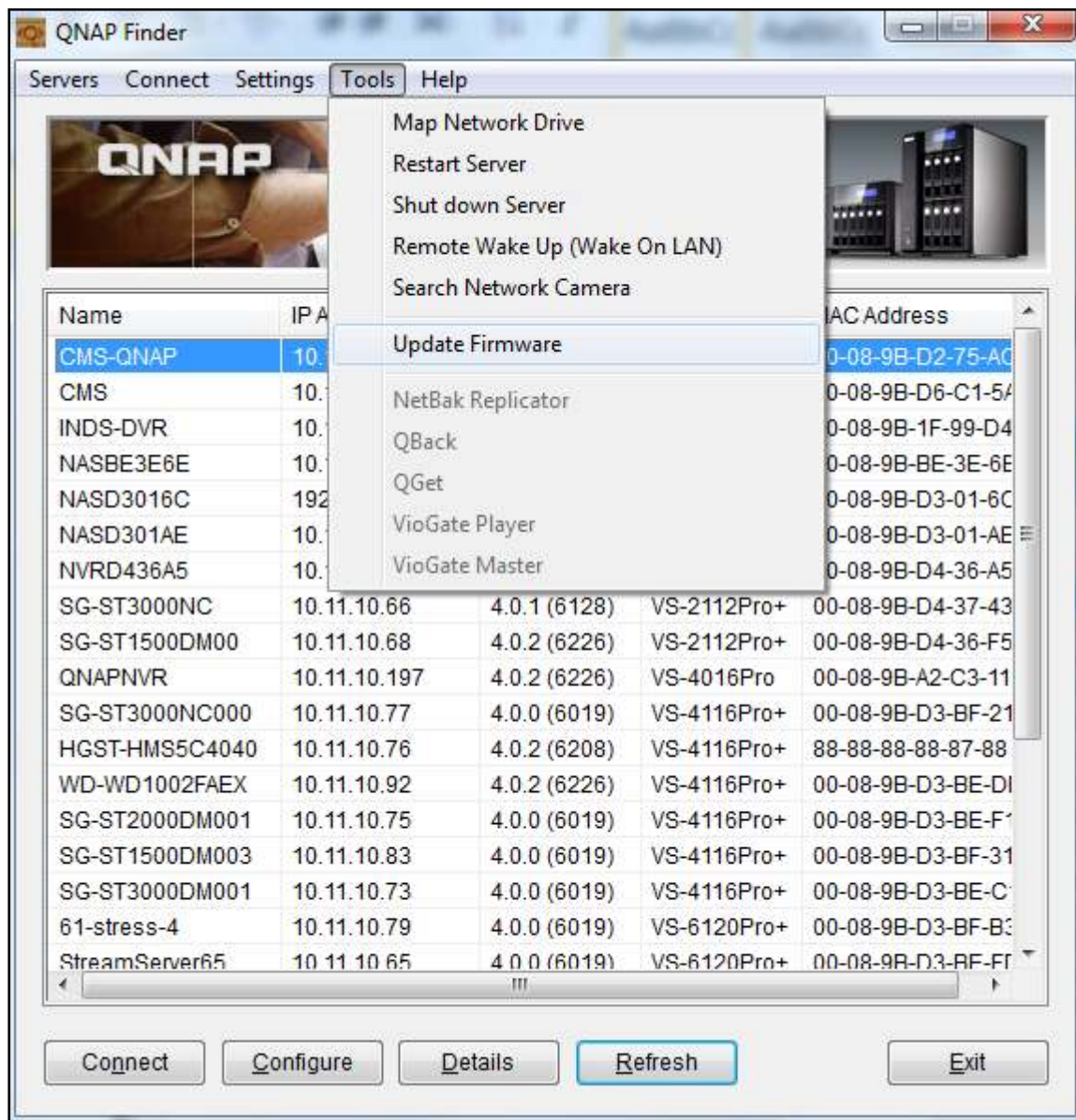
Before updating the system firmware, make sure the product model and firmware version are correct. Follow the steps below to update firmware:

1. Download the release notes of the firmware from the QNAP Security website <http://www.qnapsecurity.com>. Read the release notes carefully to make sure it is required to update the firmware.
2. Download the CMS Server firmware and unzip the IMG file to the computer.
3. Before updating the system firmware, back up all the disk data on the CMS Server to avoid any potential data loss during the system update.
4. Click "Choose File" to select the correct firmware image for the system update. Click "UPDATE SYSTEM" to update the firmware.

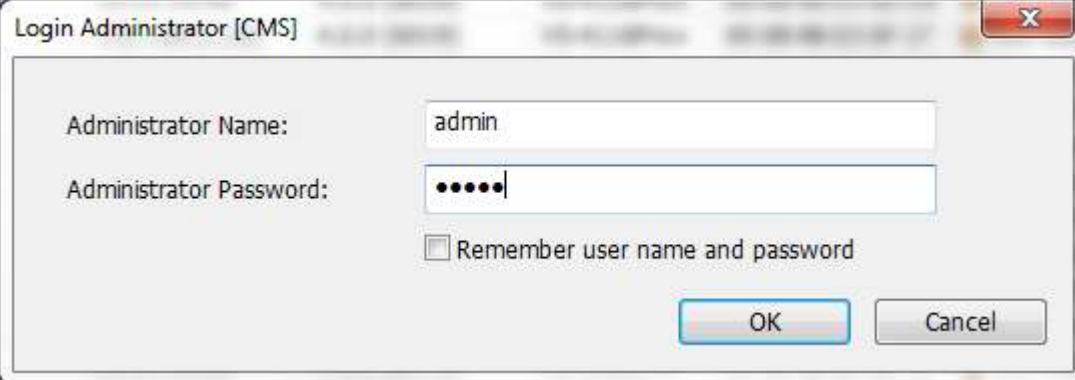
The system update may take up to several minutes to complete depending on the network connection status. Please wait patiently. The CMS Server will inform you when the system update has completed.

5.6.2 Update Firmware by QNAP Finder

The CMS Server firmware can be updated by the QNAP Finder. Select a CMS Server model and choose "Update Firmware" from the "Tools" menu.

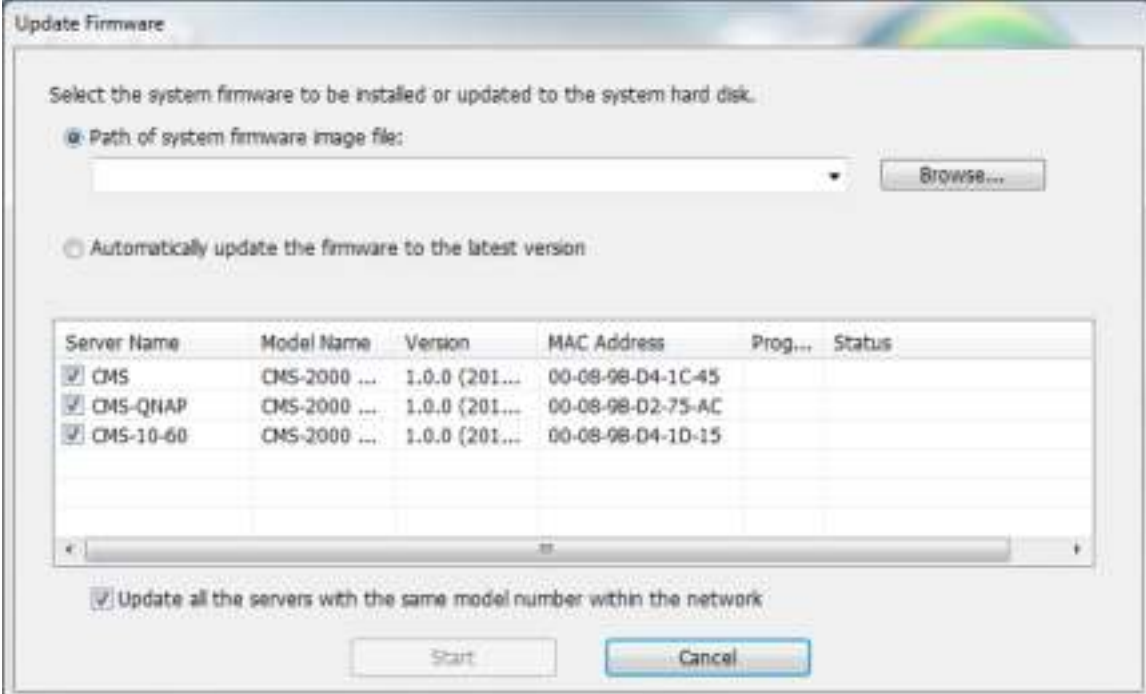


Login the CMS Server as an administrator.



A dialog box titled "Login Administrator [CMS]" with a close button (X) in the top right corner. It contains two input fields: "Administrator Name:" with the text "admin" and "Administrator Password:" with masked characters "•••••". Below the password field is a checkbox labeled "Remember user name and password" which is currently unchecked. At the bottom right are "OK" and "Cancel" buttons.

Browse and select the firmware for the CMS Server. Click "Start" to update the system.



A dialog box titled "Update Firmware" with a close button (X) in the top right corner. It contains a text label "Select the system firmware to be installed or updated to the system hard disk." Below this are two radio buttons: "Path of system firmware image file:" (selected) and "Automatically update the firmware to the latest version". The selected option has a text field and a "Browse..." button. Below the radio buttons is a table with columns: "Server Name", "Model Name", "Version", "MAC Address", "Prog...", and "Status". The table contains three rows of data, each with a checked checkbox in the first column. At the bottom of the table is a checkbox labeled "Update all the servers with the same model number within the network" which is checked. At the bottom of the dialog are "Start" and "Cancel" buttons.

Server Name	Model Name	Version	MAC Address	Prog...	Status
<input checked="" type="checkbox"/> CMS	CMS-2000 ...	1.0.0 (201...	00-08-98-D4-1C-45		
<input checked="" type="checkbox"/> CMS-QNAP	CMS-2000 ...	1.0.0 (201...	00-08-98-D2-75-AC		
<input checked="" type="checkbox"/> CMS-10-60	CMS-2000 ...	1.0.0 (201...	00-08-98-D4-1D-15		

Note: The CMS servers of the same model on the same LAN can be updated by the QNAP Finder at the same time. Administrator access is required for system update.

5.7 Restoring to Factory Default

To reset all the system settings to default, click “RESET” and then click “OK”.



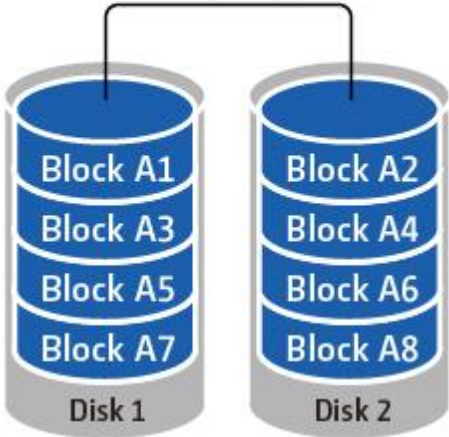
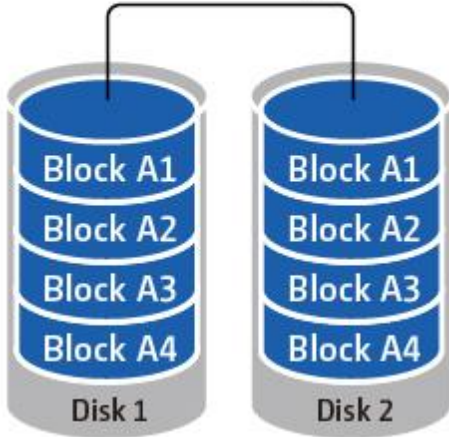
Caution: When “RESET” is pressed on this page, all the disk data, user accounts, network shares, and system settings will be cleared and restored to default. Always back up all the important data and system settings before resetting the CMS Server.

5.8 Disk Management

This page shows the model, size, and current status of the hard drives on the CMS Server. You can format and check the hard drives, and scan the bad blocks on the hard drives.

5.8.1 Volume Management

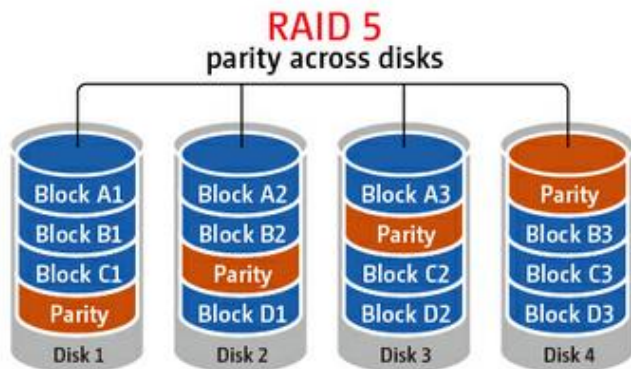


Disk Configuration	
<p>Single Disk Volume</p> <p>Each hard drive is used as a standalone disk. If a hard drive is damaged, all the data will be lost.</p>	
<p>RAID 0 Striping Disk Volume</p> <p>RAID 0 (striping disk) combines 2 or more hard drives into one larger volume. The data is written to the hard drive without any parity information and no redundancy is offered. The total storage capacity of a RAID 0 disk volume is equal to the sum of the capacity of all member hard drives.</p>	<p style="text-align: center;">RAID 0 striping</p> 
<p>RAID 1 Mirroring Disk Volume</p> <p>RAID 1 duplicates the data between two hard drives to provide disk mirroring. To create a RAID 1 array, a minimum of 2 hard drives are required. The storage capacity of a RAID 1 disk volume is equal to the size of the smallest hard drive.</p>	<p style="text-align: center;">RAID 1 mirroring</p> 

RAID 5 Disk Volume

The data are striped across all the hard drives in a RAID 5 array. The parity information is distributed and stored across each hard drive. If a member hard drive fails, the array enters degraded mode. After installing a new hard drive to replace the failed one, the data can be rebuilt from other member drives that contain the parity information.

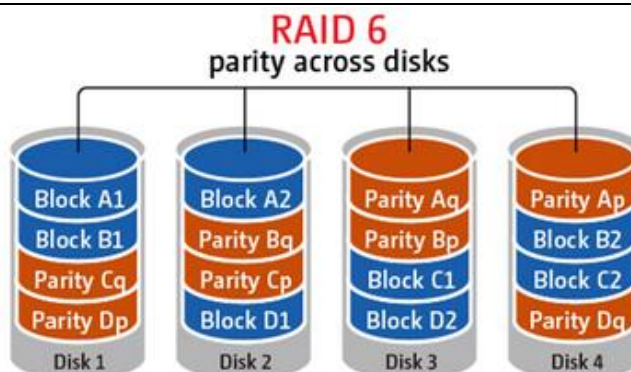
To create a RAID 5 disk volume, a minimum of 3 hard drives are required. The storage capacity of a RAID 5 array is equal to $(N-1) * (\text{size of smallest hard drive})$. N is the number of hard drives in the array.



RAID 6 Disk Volume

The data are striped across all the hard drives in a RAID 6 array. RAID 6 differs from RAID 5 that a second set of parity information is stored across the member drives in the array. It tolerates failure of two hard drives.

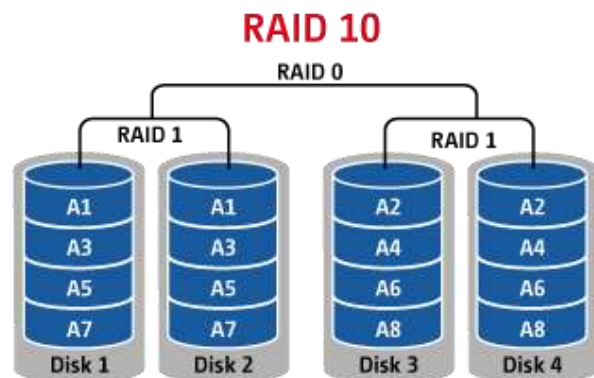
To create a RAID 6 disk volume, a minimum of 4 hard drives are required. The storage capacity of a RAID 6 array is equal to $(N-2) * (\text{size of smallest hard drive})$. N is the number of hard drives in the array.



RAID 10 Disk Volume

RAID 10 combines four or more disks in a way that protects data against loss of non-adjacent disks. It provides security by mirroring all data on a secondary set of disks while using striping across each set of disks to speed up data transfers.

RAID 10 requires an even number of hard drives (minimum 4 hard drives). The storage capacity of RAID 10 disk volume is equal to (size of the smallest capacity disk in the array) * N/2. N is the number of hard drives in the volume.



5.8.2 RAID Management

You can perform online RAID level migration and recover a RAID configuration on this page. You can perform online RAID capacity expansion (RAID 1, 5, 6, 10) and online RAID level migration (single disk, RAID 1, 5, 10), add a hard drive member to a RAID 5, 6, or 10 configuration, configure a spare hard drive (RAID 5, 6, 10) recover a RAID configuration on this page.

RAID Management

This function enables capacity expansion, RAID configuration migration or spare drive configuration with the original drive data reserved. Note: Make sure you have read the instructions carefully and you fully understand the correct operation procedure before using this function.

Volume	Total Size	Bitmap	Status	Description
Single Disk: Drive 1	294.28 GB	—	Ready	No operation can be executed for this drive configuration.

EXPAND CAPACITYADD HARD DRIVEMIGRATECONFIGURE SPARE DRIVEBITMAPRECOVER

For detailed instructions, please [click here](#).



Caution: When the hard drive synchronization is in process, do NOT turn off the CMS Server or plug in or unplug the hard disk drives

HDD Hot Swapping in RAID Configuration

The CMS Server supports HDD hot swapping. When a hard drive of a RAID configuration fails, the failed hard drive can be replaced by a new one immediately without shutting down the server, and the recording data can still be retained. However, if the hard drives are working properly and the recording is in process, do not swap the hard drives to avoid damages to the hard drives or the recording files.



Warning: It is strongly recommended to turn OFF the server before replacing the hard drives to reduce the risk of electric shock. The system should only be managed and maintained by authorized system administrators.

5.8.3 HDD SMART

Monitor the hard disk drives (HDD) health, temperature, and the usage status by HDD S.M.A.R.T. (Self-Monitoring Analysis and Reporting Technology).



The following information of each hard drive on the CMS Server is available.

Field	Description
Summary	Display the hard drive S.M.A.R.T. summary and the latest test result.
Hard disk information	Display the hard drive details, for example, model, serial number, HDD capacity.
SMART information	Display the hard drive S.M.A.R.T. information. Any items that the values are lower than the threshold are regarded as abnormal.
Test	Perform quick or complete hard drive S.M.A.R.T. test.
Settings	Configure temperature alarm. When the hard drive temperature is over the preset values, the NAS records the error logs. You can also set the quick and complete test schedule. The latest test result is shown on the Summary page.

5.8.4 Encrypted File System

You can manage the encrypted disk volumes on the CMS Server on this page. Each encrypted disk volume is locked by a particular key. The encrypted volume can be unlocked by the following methods:

- Encryption Password: Enter the encryption password to unlock the disk volume. The default password is "admin". The password must be 8-16 characters long. Symbols (! @ # \$ % ^ & * () _ + = ?) are supported.

- Encryption Key File: Upload the encryption file to the CMS Server to unlock the disk volume. The key can be downloaded from "Encryption Key Management" page after the disk volume has been unlocked successfully.

Please note that the data encryption functions may not be available in accordance to the legislative restrictions of some countries.

Click "ENCRYPTION KEY MANAGEMENT" on the "Action" column of an unlocked disk volume.



You can perform the following actions:

- Change the encryption key: Input your old encryption password and input the new password. (Note that after the password is changed, any previously exported keys will not be working anymore. You have to download the new encryption key if necessary, see below).
- Save the encryption key: Save the encryption key on the CMS Server for automatic unlocking and mounting the encrypted disk volume when the CMS Server restarts.
- Download the encryption key file: Input the encryption password to download the encryption key file. Downloading the encryption key file will allow you to save the encryption key in a file. The file is also encrypted and can be used to unlock a volume, without knowing the real password (see "unlock a disk volume manually" below). Please save the encryption key file in a secure place!

Create a new encrypted disk volume with new hard drives

To create a new encrypted disk volume and install new hard drives on the CMS Server after its installation, follow the steps below:

1. Install the new hard drive(s) to the CMS Server.
2. Log into the CMS Server as an administrator. Go to "Disk Management" > "Volume Management".
3. Select the disk volume you want to configure according to the number of new hard drives installed.



4. Select the hard drive(s) for creating the disk volume. In this example, we select to create a single drive. The procedure applies also to a RAID configuration.
5. Select "Yes" for the "Encryption" option and enter the encryption settings.
6. Then click "CREATE" to create the newly encrypted volume. Note that all the data on the selected drives will be DELETED! Please back up the data before creating the encrypted volume.
7. You have created an encrypted disk volume on the CMS Server.

Verify that disk volume is encrypted

To verify the disk volume is encrypted, log into the CMS Server as an administrator. Go to "Disk Management" > "Volume Management".

You will be able to see the encrypted disk volume, with a lock icon in the Status column. The lock will be open if the encrypted volume has been unlocked. A disk volume without the lock icon in the Status column is not encrypted.

5.9 System Status

5.9.1 System Information

You can view the system information such as CPU usage and memory on this page

System Information

System Information

Server Name

CMS

Firmware Version

1.0.4 Build 20138701

System Up Time

2 Day 1 Hour 21 Minutes

Serial Number

Q12102981

Port Status

Port No.	Port Status	IP Address	MAC Address	Packets Received	Packets Sent	Error Packets
Ethernet 1	Up	192.254.100.100	00:08:36:a5:5c:76	16747	3028	0
Ethernet 2	Up	192.11.10.100	00:08:36:a5:5c:71	101344	93976	0

Hardware Information

CPU Usage

8.4 %

Total Memory

395.4 MB

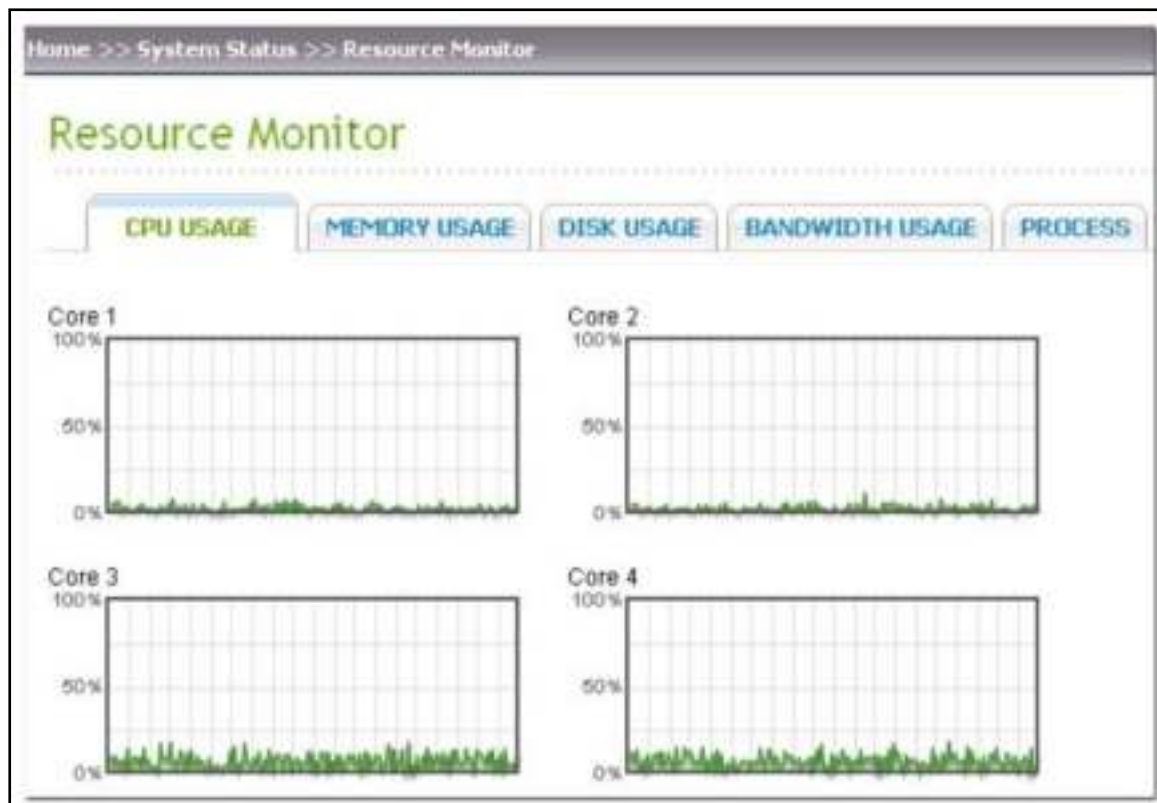
Free Memory

736.4 MB

5.9.2 Resource Monitor

You can view the CPU usage, disk usage, and bandwidth transfer statistics of the CMS Server on this page.

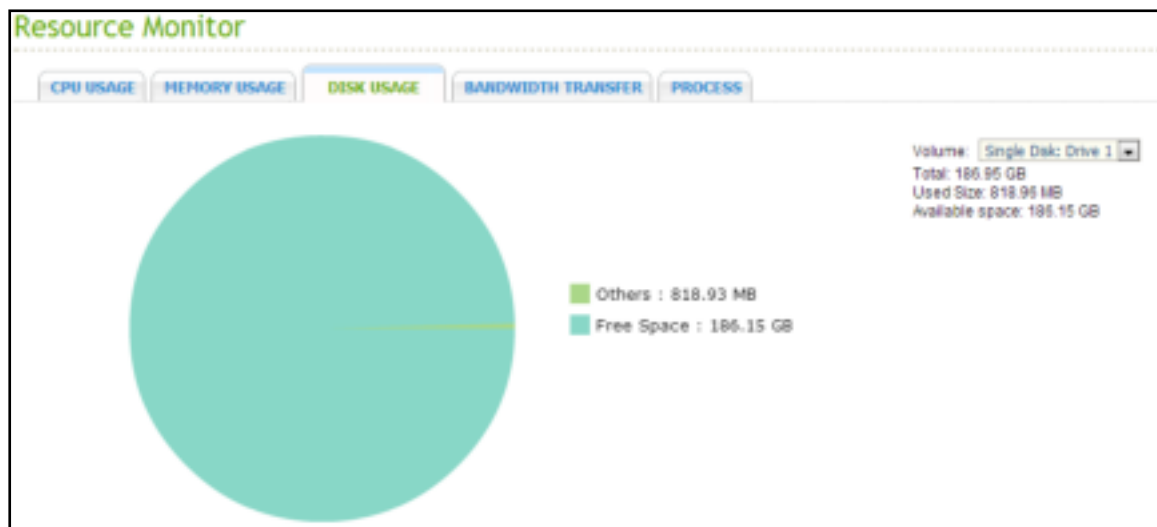
CPU Usage: This tab shows the CPU usage of the CMS Server.



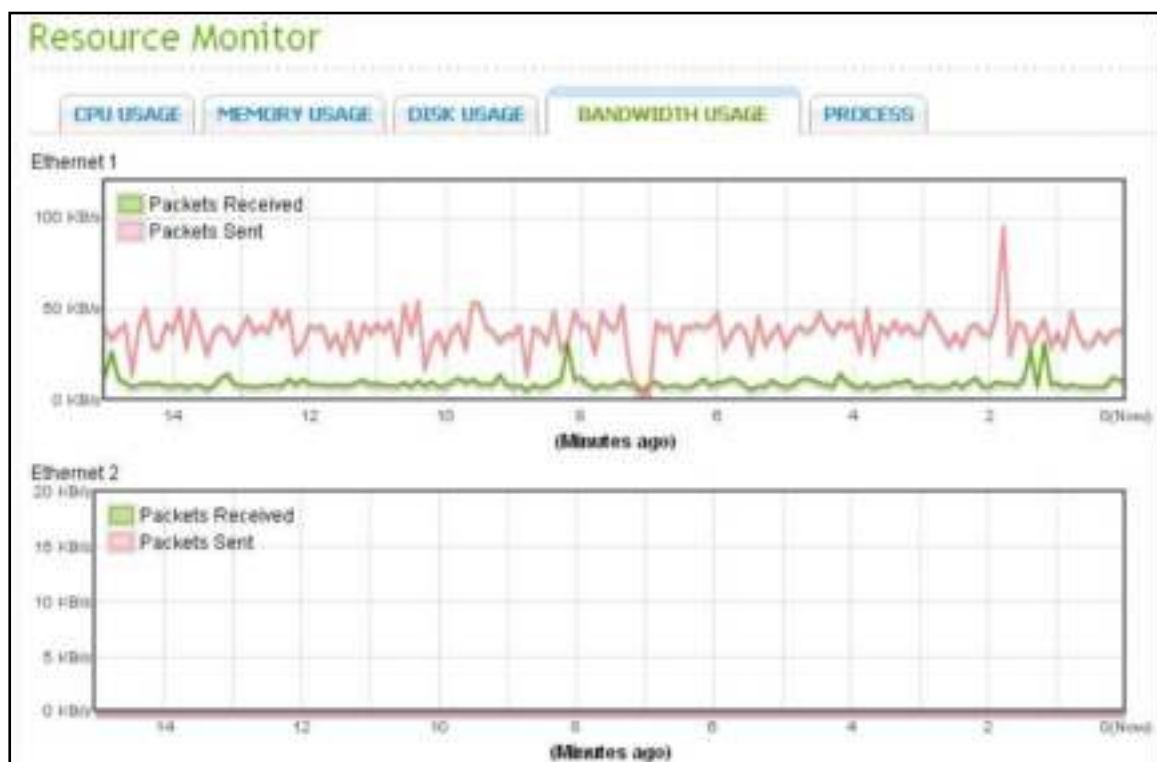
Memory Usage: This tab shows the memory usage of the CMS Server by real-time dynamic graph.



Disk Usage: This tab shows the disk space usage of each disk volume and its network shares.



Bandwidth Usage: This tab provides information about bandwidth transfer of each available LAN port of the CMS Server.



Process: This tab shows information about the processes running on the CMS Server.

Resource Monitor				
CPU USAGE	MEMORY USAGE	DISK USAGE	BANDWIDTH TRANSFER	PROCESS
Process Name	Users	PID	CPU Usage	Memory
top	admin	21016	2.8%	376 K
postgres: wal writer proc...	postgres	4899	0.0%	1996 K
top	admin	21021	0.9%	888 K
qLogEngine: Write log i...	admin	6747	0	1284 K
modagent	admin	2371	0	552 K
hotswap	admin	3062	0	1384 K
gsmand	admin	2067	0	992 K
dhcpd	admin	3386	0	408 K
dhcpd	admin	3701	0	262 K
httpd	admin	4259	0	1868 K
cuped	admin	4331	0	2052 K
smtd	admin	4437	0	2960 K
crond	admin	4579	0	720 K
smtd	admin	4606	0	1120 K
ntpd	admin	4648	0	728 K

Chapter 6 Troubleshooting

1. After quick installation of the CMS-2000 (CMS Server) and having entered the correct user name and password, the system showed the warning message "Network Failure: the server is not found on the network. Please check the server status."



Solution

Please check the following:

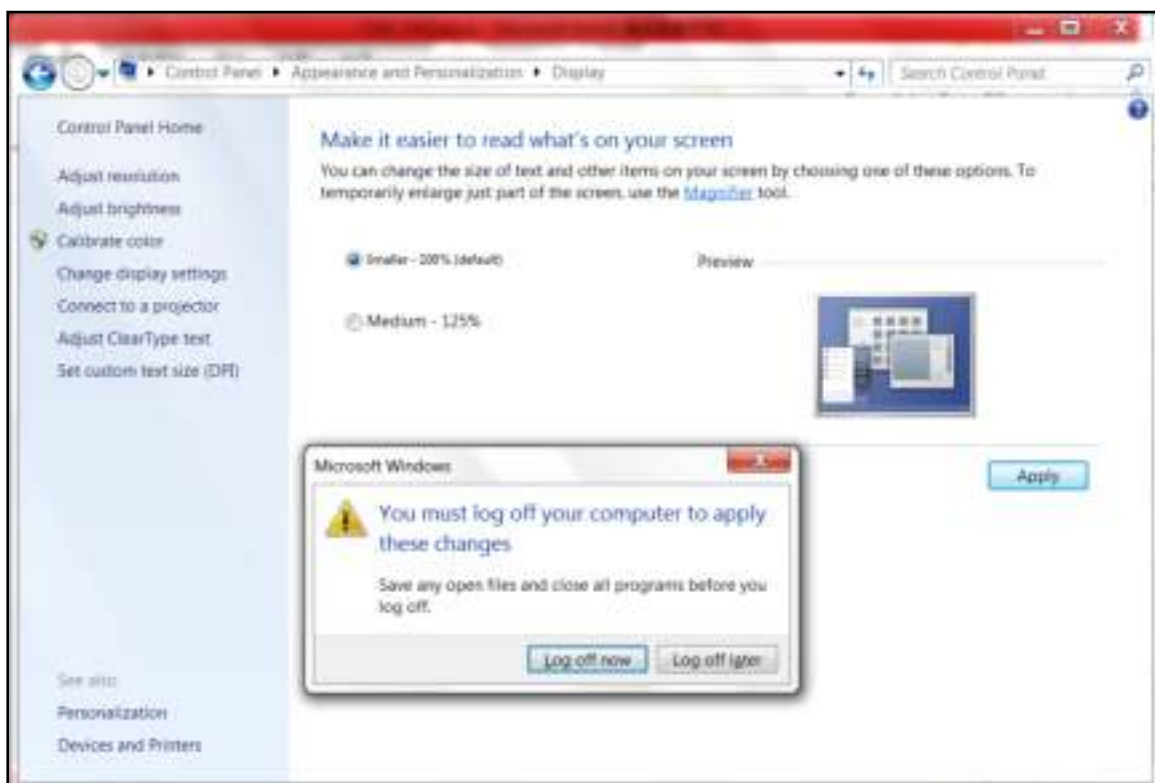
- a) The hard drives are empty and do not contain any data. You can clean all the data on the hard drives in Windows Disk Management, and install the CMS-2000 again.
- b) If a hard drive has been used in a NAS or an NVR, it may be determined abnormal and unavailable by CMS.

2. The CMS Client interface displays abnormally and does not show complete contents.



Solution

Please go to "Display" on Windows ("Control Panel" > "Appearance and Personalization" > "Display" > "Make it easier to read what's on your screen") and change the setting from "Medium - 125 %" to default.

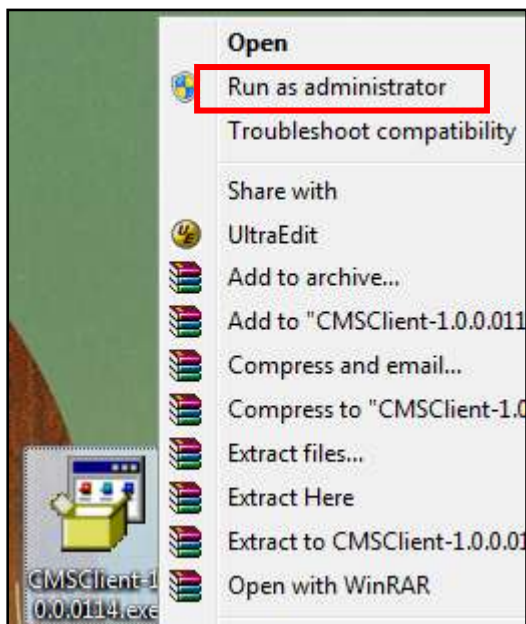


3. The live view page did not display.

Solution

Please check the following:

- a) The NVR and the IP camera are turned on and correctly connected to the network.
- b) The IP addresses of the CMS Server and NVR do not conflict with other devices on the same subnet.
- c) Check if the CMS Server, NVR, and IP camera is connected to each other.
- d) Please use a user account with administrator privilege to install the CMS Client, if not, please run the CMS Client installer as administrator.



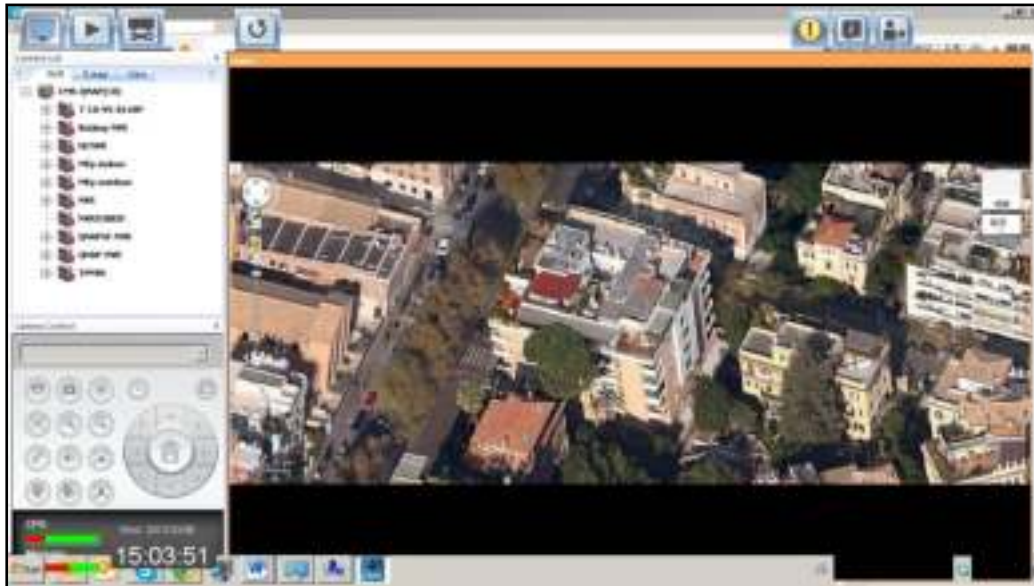
- e) Update the latest driver of your Intel onboard graphics chip or graphic card, please download in Intel download center: <http://downloadcenter.intel.com/>

4. The live video is not clear or smooth sometimes.

Solution

The image quality may be restricted or interfered by the network traffic. Please use independent connections or avoid sharing the same connection with other network devices.

5. After login, the GUI (Graphic User Interface) looks abnormal in crushed shape (as the figure below). Is this a system compatibility problem? How do I solve this?



Solution

Please select the Aero Theme of the operating system (Control Panel > All Control Panel Items > Personalization), please note that CMS doesn't support Basic and High Contrast Themes of Windows OS.



6. The E-map cannot be displayed correctly.

Solution

Please check the format of the uploading image files. Currently the CMS supports E-maps in JPEG, BMP, and PNG (not including translucent images) only.

7. Unable to find the CMS Server by the "Auto Search" after logging into the CMS Client.
Or, cannot find the NVR by the "Auto Search" at the "Add Server" of the CMS Client configuration.

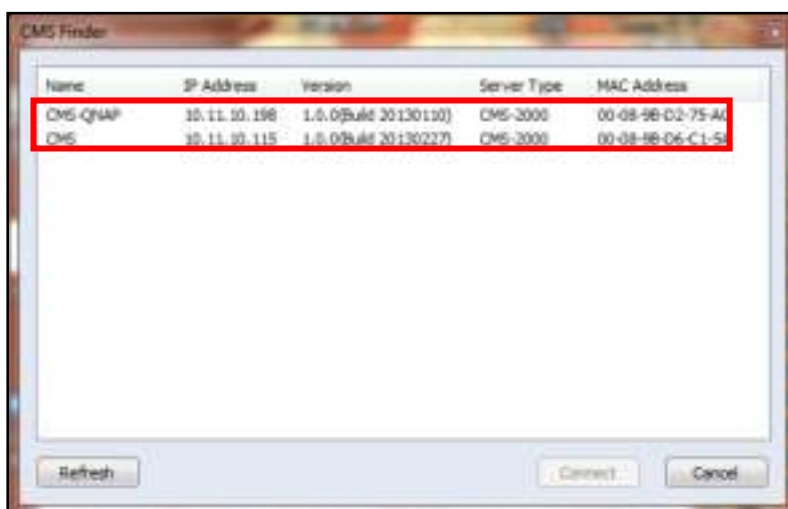
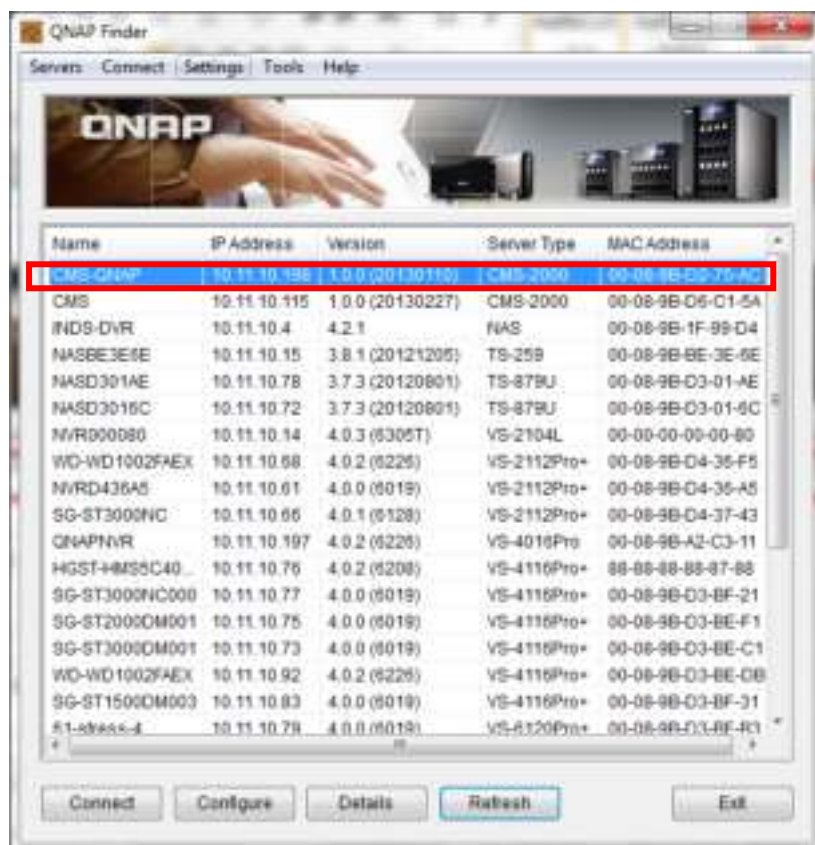
Solution

- Check that the CMS Server and the NVR have been turned on.
- Connect the local PC and the CMS Server/NVR to the same subnet.
- Install the latest version of CMS Client from www.qnapsecurity.com.
- Run the CMS Client to search for the CMS Server. Make sure all the firewall software on the computer have been turned off; or add the CMS Client to the list of allowed programs in the firewall.
- Please check if the QNAP Finder program is closed.
- If the CMS Server and NVR are not found, click the "Auto Search" button to try again.
- If the problem persists, contact the technical support.

8. Unable to find the CMS Server or any NVR by the CMS Client, but able to find by QNAP Finder.

Solution

Please close the QNAP Finder and run the CMS Client. The search function of the QNAP Finder is mutually exclusive with that of the CMS Client.



9. The changes to the system configuration did not take effect.

Solution

After changing the settings on the configuration page, click "Apply" to save the changes; otherwise the settings will not be saved and will not take effect.

10. The CMS Client does not show the alarm information.

Solution

You have to configure the alarm settings in the NVR, and check the event management page in the CMS Client. After that, you can find the alarms in the Live View user interface.

11. After power outage and improper server shutdown, the server does not function properly after the restart. What should I do?

Solution

Please try the following:

- a) If the system configuration were lost, configure the system again.
- b) If the problem persists, contact the technical support.

Technical Support

QNAP Security provides dedicated online support and customer service via instant messenger. Please contact us by the following means:

Online Support: <http://www.qnapsecurity.com/onlinesupport.asp>

Forum: <http://forum.qnapsecurity.com>

Technical Support in the USA and Canada:

Email: q_supportus@qnap.com

TEL: 909-595-2819

Address: 168 University Parkway Pomona, CA 91768-4300

Service Hours: 08:00–17:00 (GMT- 08:00 Pacific Time, Monday to Friday)

GNU - GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <<http://fsf.org/>>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the

work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights from Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

- a) The work must carry prominent notices stating that you modified it, and giving a relevant date.
- b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".
- c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.
- d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an

“aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

- a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.
- b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.
- c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.
- d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.
- e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object

code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation

available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

“Additional permissions” are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

- a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
- b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
- c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
- d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
- e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
- f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice

stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using

peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license

was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version

permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS