



iVMS-5200 Professional

User Manual (for Administrator)

UD.6L0202D1542A01

Hikvision® iVMS-5200 Professional User Manual

This manual, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. The content of this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Hangzhou Hikvision Digital Technology Co., Ltd. (Hikvision). Hikvision assumes no responsibility or liability for any errors or inaccuracies that may appear in the book.

Except as permitted by such license, no part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Hikvision.

HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE HIKVISION SOFTWARE. HIKVISION DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE HIKVISION SOFTWARE IN TERMS OF ITS CORRECTNESS, ACCURACY, RELIABILITY, CURRENTNESS, OR OTHERWISE. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE HIKVISION SOFTWARE IS ASSUMED BY YOU. THE EXCLUSION OF IMPLIED WARRANTIES IS NOT PERMITTED BY SOME STATES. THE ABOVE EXCLUSION MAY NOT APPLY TO YOU.

IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, AND THE LIKE) ARISING OUT OF THE USE OR INABILITY TO USE THE HIKVISION SOFTWARE EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

Contents

Chapter 1	Overview	4
1.1	About This Document.....	4
1.2	Introduction to iVMS-5200 Professional	4
1.3	Administrator Rights.....	5
Chapter 2	Getting Started	6
Chapter 3	Installation and Uninstallation	7
3.1	Installing the Server Modules.....	7
3.2	Uninstalling the Server Modules	12
3.2.1	Uninstall All the Server Modules	12
3.2.2	Uninstall the Specific Server Modules.....	12
3.3	Installing and Uninstalling the Control Client.....	13
Chapter 4	Activating CMS	16
4.1	Activating via Activation Code.....	16
4.1.1	Online Activation.....	16
4.1.2	Offline Activation.....	18
4.2	Activating via Dongle.....	21
Chapter 5	Accessing the iVMS-5200P	24
5.1	Open the Web Manager and Login	24
5.2	Function Modules	25
Chapter 6	Resource Management	26
6.1	Adding the Encoding Device.....	26
6.1.1	Adding Online Devices.....	26
6.1.2	Adding Devices by IP Address.....	27
6.1.3	Adding Devices by IP Segment	28
6.1.4	Adding Devices by Port Segment	29
6.1.5	Adding Devices by HiDDNS.....	30
6.1.6	Adding Devices by Domain Name	31
6.2	Adding the Server.....	32
6.3	Area Management	33
Chapter 7	Record Schedule Settings	36
7.1	Recording on Storage Devices of the Encoding Device	36
7.1.1	Configuring Record Schedule Template.....	37
7.2	Recording on Storage Server	38
Chapter 8	Event Configuration.....	39
8.1	Configuring Camera Exception Alarm	39
8.2	Configuring Alarm Input Linkage	41
8.3	Configuring Device Exception Linkage.....	43
8.4	Configuring Server Exception Linkage	45
Chapter 9	User and System Management	47
9.1	Role Management.....	47
9.2	User Management.....	47
9.3	System Configuration	49

9.3.1	System Settings	50
9.3.2	CMS IP Settings.....	50
Chapter 10	Appendix	51
10.1	Important Ports	51
10.2	FAQ.....	52
10.3	How to.....	52
10.3.1	How to Allocate Storage Space for Storage Server.....	52
10.3.2	How to Configure PSS Allocation and Upload Alarm Pictures to PSS.....	54

Chapter 1 Overview

1.1 About This Document

This user manual is intended for the administrator of the iVMS-5200 Professional V3.0 (hereafter simply as iVMS-5200P). It guides you to establish and configure the surveillance system. Follow this manual to perform the installation of the iVMS-5200P, activation of CMS, access of the iVMS-5200P and configuration of the surveillance task via the provided web manager, etc. To ensure the properness of usage and stability of the iVMS-5200P, please refer to the contents below and read the manual carefully before installation and operation.

1.2 Introduction to iVMS-5200 Professional

iVMS-5200P is developed by HIKVISION for central management of video monitoring system and features flexibility, scalability high reliability and powerful functions. Integrating with multiple surveillance systems, iVMS-5200P provides the central management, information sharing, convenient connection and multi-service cooperation. It is capable of adding devices for management, live view, storage and playback of record files, VCA search, alarm linkage, etc..

The complete iVMS-5200P contains the following modules:

Note: You can install the modules according to actual needs.

Module	Introduction
CMS (Central Management Server): For detailed installation, please refer to <i>Chapter 3.1 Installing the Server Modules</i> .	<ul style="list-style-type: none"> a) Provide the unified authentication service for connecting with the clients and servers. b) Provide the centralized management for the users, roles, permissions, surveillance devices, alarm device and servers. c) Provide the configuration interface for surveillance and management module, and sub-systems. d) Provide the log management and statistics function.
SMS (Stream Media Server) (Optional): For detailed installation, please refer to <i>Chapter 3.1 Installing the Server Modules</i> .	<ul style="list-style-type: none"> a) Forward and distribute the audio and video data of live view. b) Provide the function of live view via mobile control client.
SS (Storage Server) (Optional): For detailed installation, please refer to <i>Chapter 3.1 Installing the Server Modules</i> and <i>Chapter 10.3.1 How to Allocate Storage Space for Storage Server</i> .	<ul style="list-style-type: none"> a) Obtain the audio and video data stream via the SMS (Stream Media Server) or directly from the connected encoding device b) Extract the index information and dump the audio and video data to the storage device to realize the centralized management of the mass video files.

Module	Introduction
PSS (Picture Storage Server) (Optional): For detailed installation, please refer to <i>Chapter 3.1 Installing the Server Modules</i> .	a) Provide the efficient, secure, convenient storage service for pictures with storage efficiency of 10 pictures per second.
MAG (Mobile Access Gateway) (Optional): For detailed installation, please refer to <i>Chapter 3.1 Installing the Server Modules</i> .	When setting the image quality as Fluent in Mobile Client, the MAG can provide the following functions: a) Convert and distribute the low bitrate stream when live viewing the high-definition video via Mobile Client. b) Transcode and distribute up to 24-ch high-definition stream. c) Ensure the high-definition live view and playback without affecting the performance of the mobile phone.

The following table lists the provided clients for accessing or management the iVMS-5200P.

Client	Introduction
Control Client: For detailed installation, please refer to <i>Chapter 3.3 Installing and Uninstalling the Control Client</i> .	iVMS-5200 Control Client is a C/S software which provides multiple operating functionalities, including real-time live view, PTZ control, video playback and download, alarm receiving, log query, etc..
Web Client: For detailed introduction, please refer to the <i>User Manual of iVMS-5200 Control Client</i>	iVMS-5200 Web Client is a B/S software for accessing the iVMS-5200P through web browser. It provides the functionalities of live view, playback, and local configuration.
Web Manager: For detailed running environment for Web Manager, please refer to <i>Chapter 5.1 Open the Web Manager and Login</i> .	iVMS-5200 Web Manager is a B/S client for management of iVMS-5200P. It provides multiple functionalities, including device management, record schedule settings, event configuration, user management, etc., for the iVMS-5200P to manage the connected devices.
Mobile Client: For detailed installation, please refer to the <i>User Manual of iVMS-5260 Mobile Client</i> .	The iVMS-5260 Mobile Client is the mobile client software designed for getting access to the iVMS-5200P via Wi-Fi, 2G, 3G and 4G network with mobile device, it fulfills the functions of the devices connected to the iVMS-5200P, such as live view, remote playback, PTZ control and so on.

1.3 Administrator Rights

When you install the servers, clients and software, it is important that you have administrator rights on the PCs or servers that should run these modules.

Consult your IT system administrator if in doubt about your rights.

Chapter 2 Getting Started

The following content describes the tasks typically involved in setting a working iVMS-5200P.

Note: The contents below may not cover the exact needs of your organization.

- Verify Initial Configuration of Encoding Devices and other Servers

Before doing anything on iVMS-5200P, make sure the devices (cameras, DVR, storage server, etc.) you are going to use are correctly installed and connected to the network, etc. as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the iVMS-5200P via network.

- Install iVMS-5200P

Refer to *Chapter 3 Installation and Uninstallation* to for the detailed installation steps.

- Open the Web Manager

Refer to *Chapter 5.1 Open the Web Manager and Login*.

- Activate Your License

Refer to *Chapter 4 Activating CMS* for the operation of activating the license.

- Add Devices to iVMS-5200P and Configure Area

iVMS-5200P can quickly scan your network for relevant encoding devices (cameras, DVR, etc.), and add them to your system. Or you can add the devices by inputting the required information manually. The devices added should be organized into areas for convenient management. Refer to *Chapter 6 Resource Management*.

- Configure Record Schedule

The video files of the cameras to can be recorded on the storage device according to the configured record schedule. The schedule can be set as continuous, alarm triggered or command triggered as desired. Refer to *Chapter 7 Record Schedule Settings*.

- Configure Events

The camera exception, device exception, server exception and the alarm input can trigger linkage actions in iVMS-5200P. For example: when motion is detected, an audible warning appears or a notification email is sent to you. Refer to *Chapter 8 Event Configuration*.

- Configure Users

Now specify who should be able to access your iVMS-5200P, and how. You can set the different permissions for the users to limit the operation of the iVMS-5200P. Refer to *Chapter 9.1 Role Management* and *Chapter 9.2 User Management*.

Chapter 3 Installation and Uninstallation

The program file which is provided by HIKVISION contains 6 server modules and 1 client, including iVMS-5200 CMS (Central Management Server), iVMS-5200 Storage Server, iVMS-5200 Stream Media Server, iVMS-5200 Picture Storage Server, iVMS-5200 Mobile Access Gateway, iVMS-5200 Service Watchdog and iVMS-5200 Control Client. The server modules can be installed on different servers or PCs separately, or you can install them on the same server or PC as desired.

3.1 Installing the Server Modules

Before you start:

Please check the following items before you install the server modules of the iVMS-5200P.

- For installing CMS, please check that the port 80 of your PC or server to be installed the CMS is not occupied by other service. If it is occupied, please change the port of the service to other value since the port 80 should be used when running the CMS. You can also change the port of CMS to other available value after installation. For details, please refer to *Chapter 10.2 FAQ*.
- The SS must be installed on the 64-bit PC or server to work properly.

Running Environment

For CMS:

- **Operating System:** Windows Server 2008 R2 SP1 / Windows Server 2003 SP2 (64-bit)
- **Processor:** E5-2620 series processor with 6 cores (2.0 Ghz)
- **Memory:** 8GB
- **HDD:** Enterprise-level SATA disk with 600GB storage capacity
- **Network Controller:** RJ45 Gigabit self-adaptive Ethernet interfaces

Note: We also provide a dedicated product for installing and running the CMS. For details, please contact you dealer or our salesman.

For Other Servers

- **Operating System:** Windows Server 2008 R2 SP1 / Windows Server 2003 SP2 (64-bit)
- **Processor:** E3-1230 V2 series processor (3.3 GHz)
- **Memory:** 8GB
- **HDD:** Enterprise-level SATA disk with 500GB storage capacity
- **Network Controller:** RJ45 Gigabit self-adaptive Ethernet interfaces

Note: We also provide dedicated products for installing and running the servers. For details, please contact you dealer or our salesman.

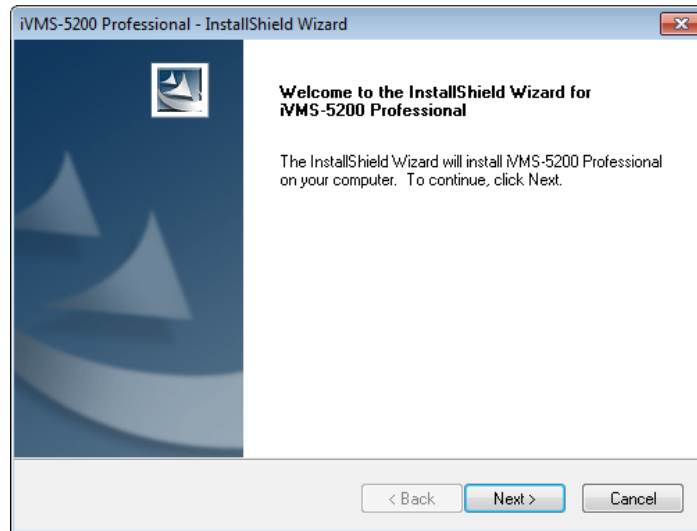
Installation

Perform the following steps to install the server modules.

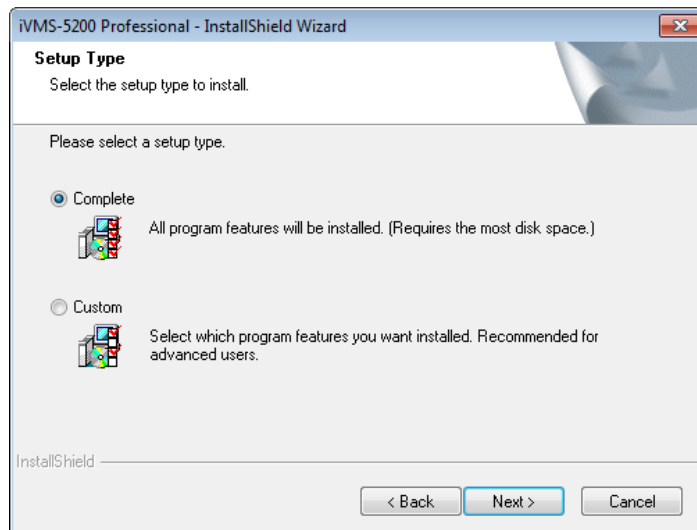
Steps:

1. Double-click the program file  to enter the welcome panel of the InstallShield Wizard. Click

Next to start the InstallShield Wizard.



2. On the next panel, you are prompted to select a setup type to install.

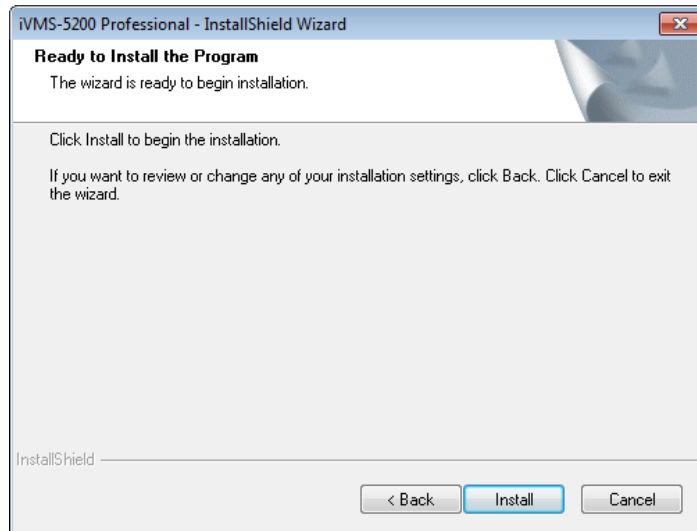


● **For Complete:** All the modules, including all the server modules and Control Client, will be installed and the installation directory cannot be modified.

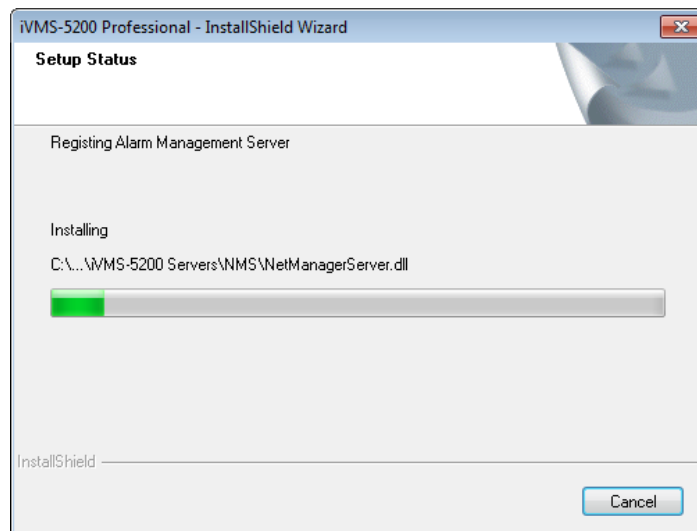
Note: The default directory is *C:\Program Files\iVMS-5200 Professional* or *C:\Program Files (x86)\iVMS-5200 Professional*.

Click **Next** to continue.

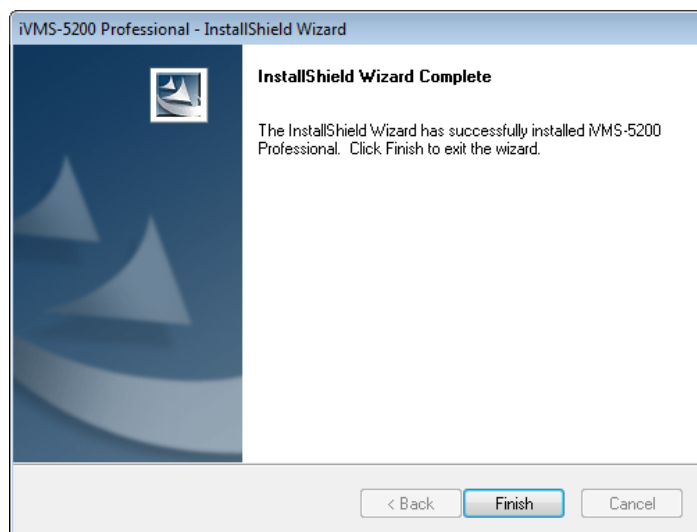
1) Read the pre-install information and click **Install** to begin the installation.



- 2) A panel indicating progress of the installation is displayed.



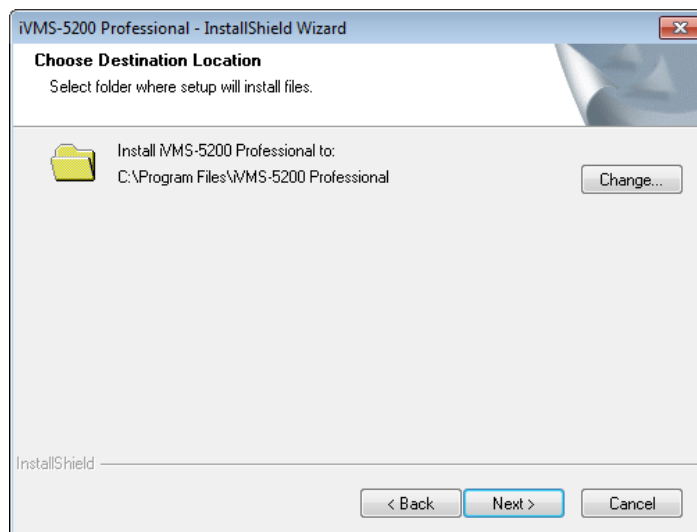
- 3) Read the post-install information and click **Finish** to complete the installation.



- **For Custom:** You can select the installation directory and server modules to be installed as desired.

Click **Next** to continue.

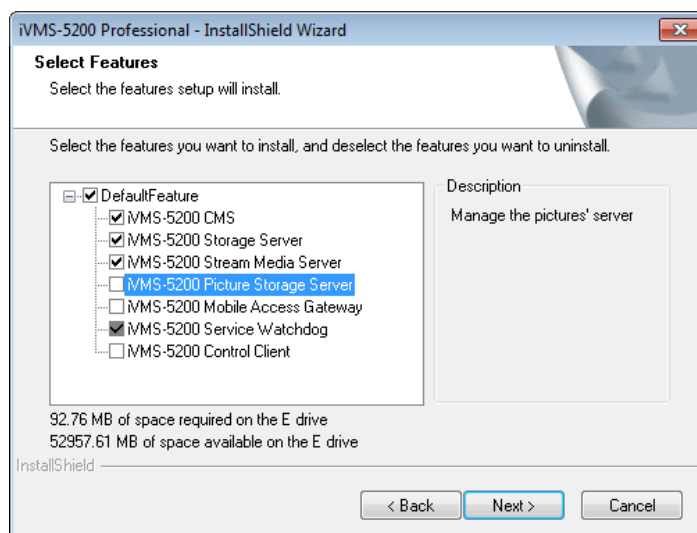
- 1) Click **Change** and select a proper directory as desired to install the module(s). Click **Next** to continue.



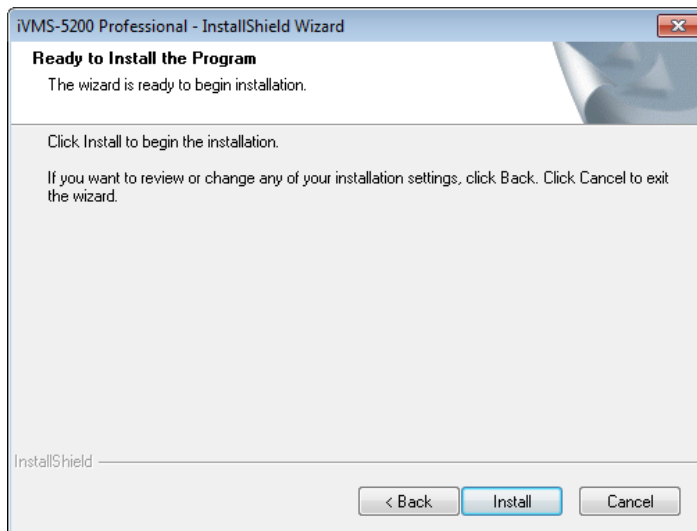
- 2) Select the module(s) you want to install and click **Next** to start installation. In this way, you can install the server modules to different PCs or servers as desired.

Notes:

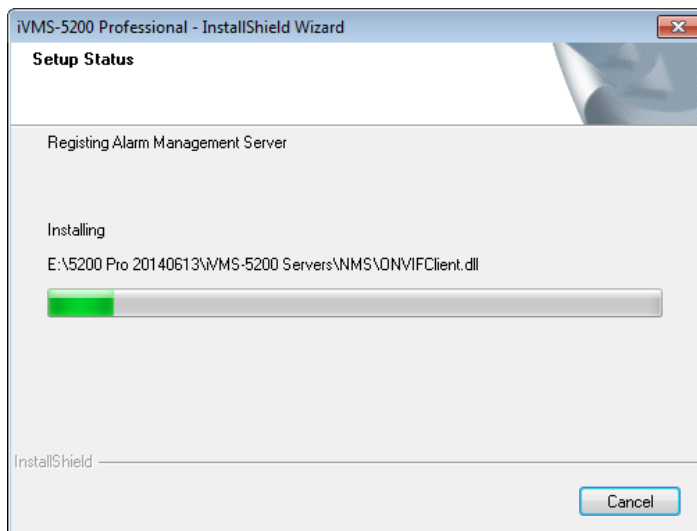
- To build the surveillance system, the iVMS-5200 CMS must be installed on ones of your PCs or servers. For other modules, you can install them according to actual needs. Refer to *Chapter 1.2 Introduction to iVMS-5200 Professional* for the description of the modules.
- If you select server module(s) (iVMS-5200 CMS, iVMS-5200 Storage Server, iVMS-5200 Stream Media Server, iVMS-5200 Picture Storage Server or iVMS-5200 Mobile Access Gateway), the iVMS-5200 Service Watchdog will be selected as well.



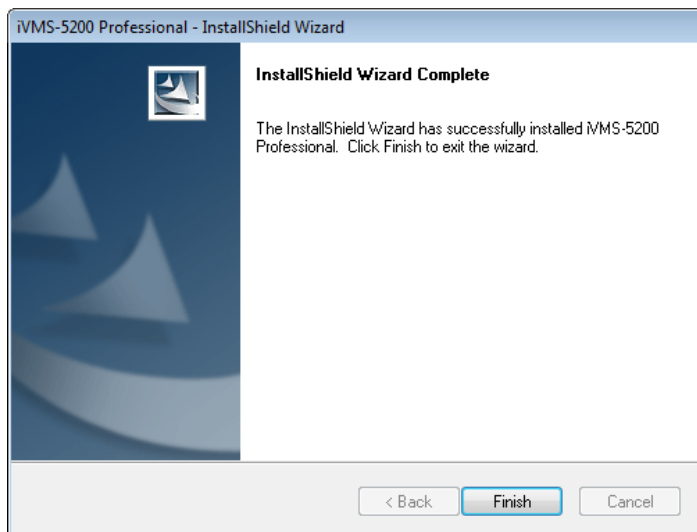
- 3) Read the pre-install information and click **Install** to begin the installation.



4) A panel indicating progress of the installation is displayed.



5) Read the post-install information and click **Finish** to complete the installation.



After successfully installing the server module(s), the Watchdog runs automatically.

Note: The Watchdog should be run as administrator. If not, please exit the Watchdog and then run it as administrator. Consult your IT system administrator if in doubt about your rights.

3.2 Uninstalling the Server Modules

3.2.1 Uninstall All the Server Modules

To remove the entire iVMS-5200P (that is the surveillance server software and related installation files, and the Control Client) from your PC or server, perform the following steps:

Note: Before removing the CMS, you should logout the License or Dongle if you have activated the CMS so that the License or Dongle can be used for activating another CMS. For details, please refer to *Chapter 4 Activating CMS*.

Steps:

1. Shut down all iVMS-5200P modules and exit the iVMS-5200 Service Watchdog.
Note: The following procedure of standard system module removal may be slightly different according to the different OS versions.
2. In Windows' Start menu, select Control Panel.
 - If using Category view, find the Programs category, and click **Uninstall a program**.
 - If using Small icons or Large icons view, select **Programs and Features**.
3. In the list of currently installed programs, right-click the iVMS-5200 Professional.
4. Select **Uninstall** and follow the removal instructions.

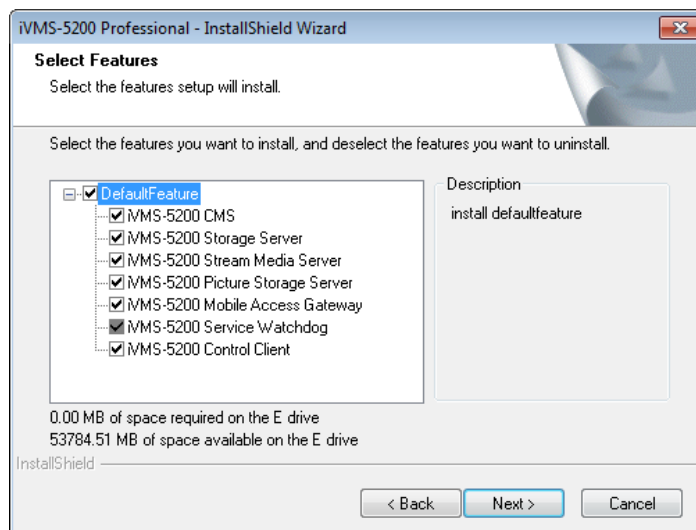
3.2.2 Uninstall the Specific Server Modules

To remove the specific module(s) of the iVMS-5200P (e.g., CMS, SS or the Control Client) from your PC or server, perform the following steps:

Note: Before removing the CMS, you should logout the License or Dongle if you have activated the CMS so that the License or Dongle can be used for activating another CMS. For details, please refer to *Chapter 4 Activating CMS*.

Steps:

1. Shut down all iVMS-5200P modules and exit the iVMS-5200 Service Watchdog.
Note: The following procedure of standard system module removal may be slightly different according to the different OS versions.
2. In Windows' Start menu, select Control Panel.
 - If using Category view, find the Programs category, and click **Uninstall a program**.
 - If using Small icons or Large icons view, select **Programs and Features**.
3. In the list of currently installed programs, right-click the iVMS-5200 Professional.
4. Select **Change** and the InstallShield Wizard pops up.
5. Select the Modify radio button and click **Next** to continue.



- Uncheck the checkbox of the module(s) that you want to uninstall, click **Next** and follow the removal instructions.


3.3 Installing and Uninstalling the Control Client

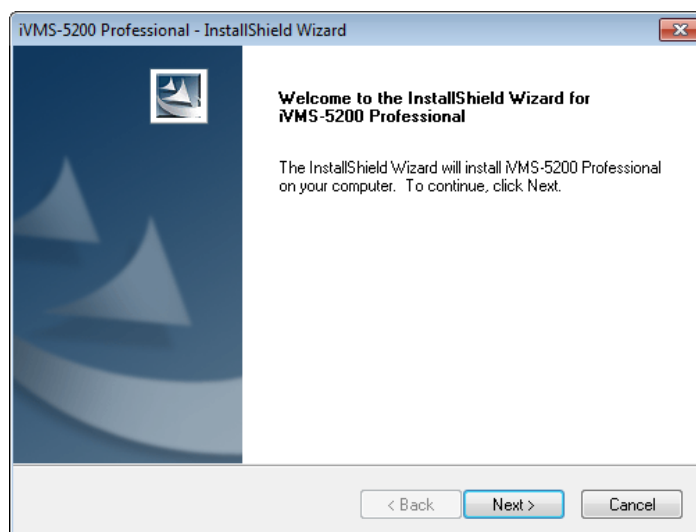
Running Environment

- **Operating System:** Windows 7 / Windows 8 (32/64-bit)
- **CPU:** Intel Core i5 750 and above
- **Memory:** 4GB
- **Video Card:** Geforce GTX 460 and above

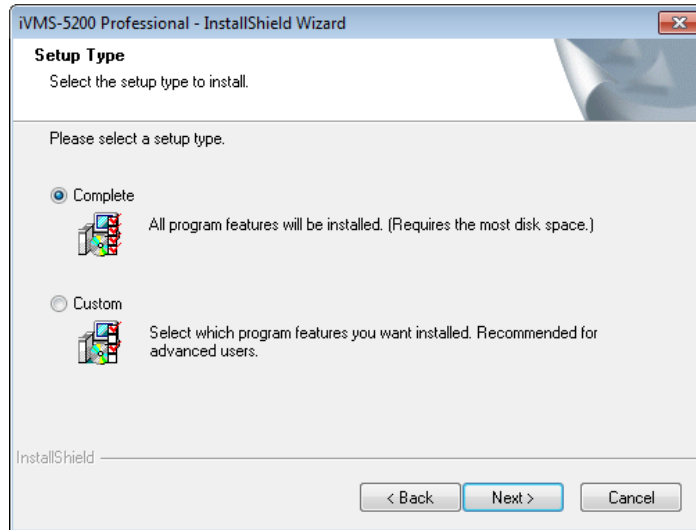
Perform the following steps to install the iVMS-5200 Control Client.

Steps:

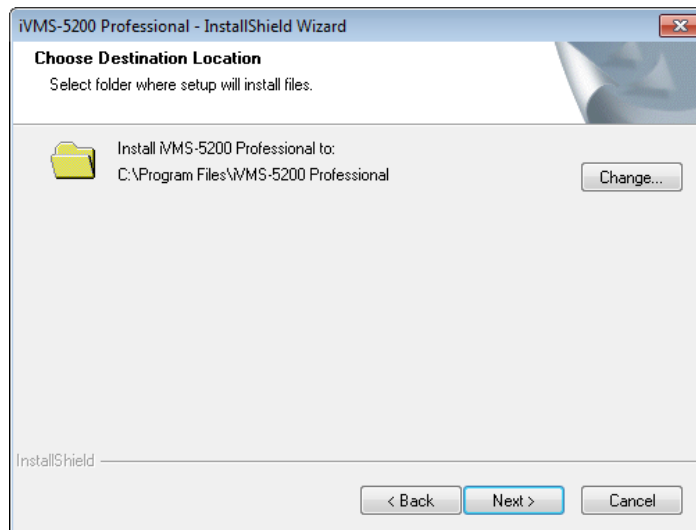
- Double-click the program file  to enter the welcome panel of the InstallShield Wizard. Click **Next** to start the InstallShield Wizard.



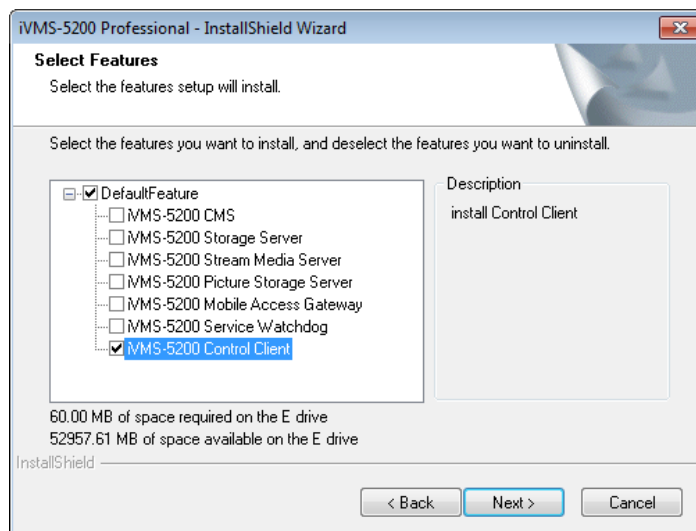
- On the next panel, you are prompted to select a setup type to install. Select **Custom** radio button and click **Next** to continue.



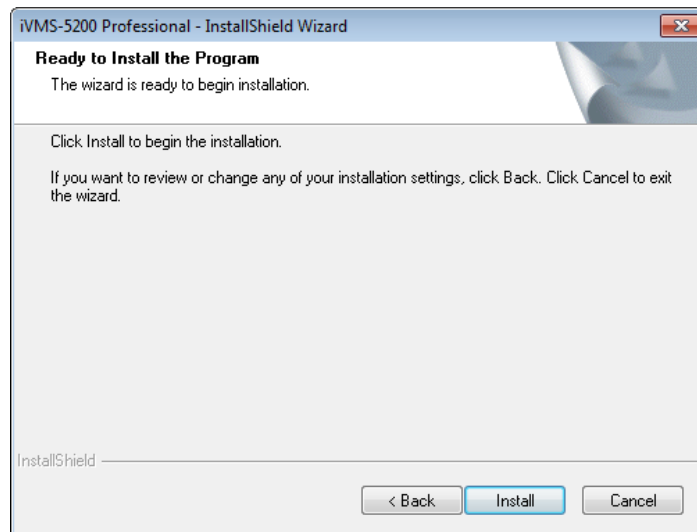
- Click **Change** and select a proper directory as desired to install the Control Client. Click **Next** to continue.



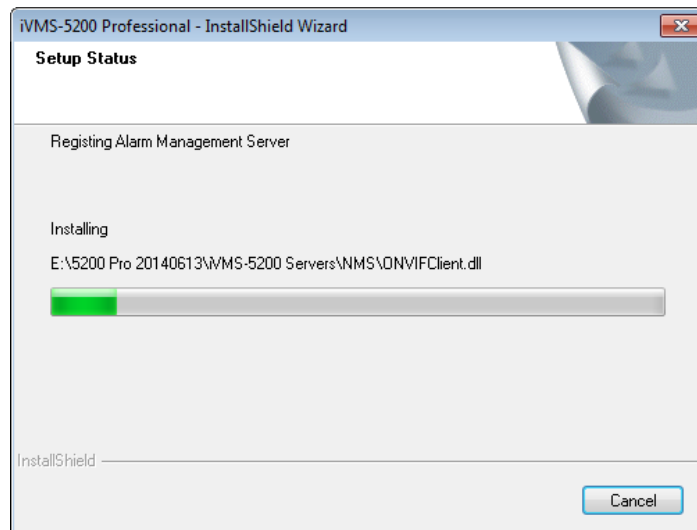
- Select the iVMS-5200 Control Client and click **Next** to start installation.



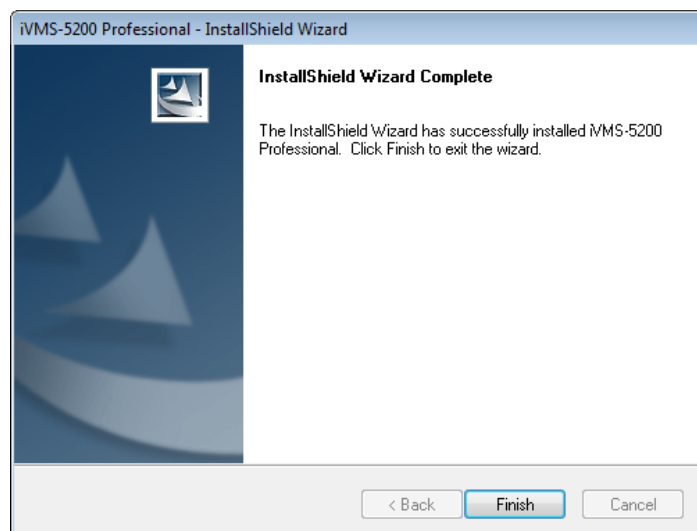
5. Read the pre-install information and click **Install** to begin the installation.



6. A panel indicating progress of the installation is displayed.



7. Read the post-install information and click **Finish** to complete the installation.



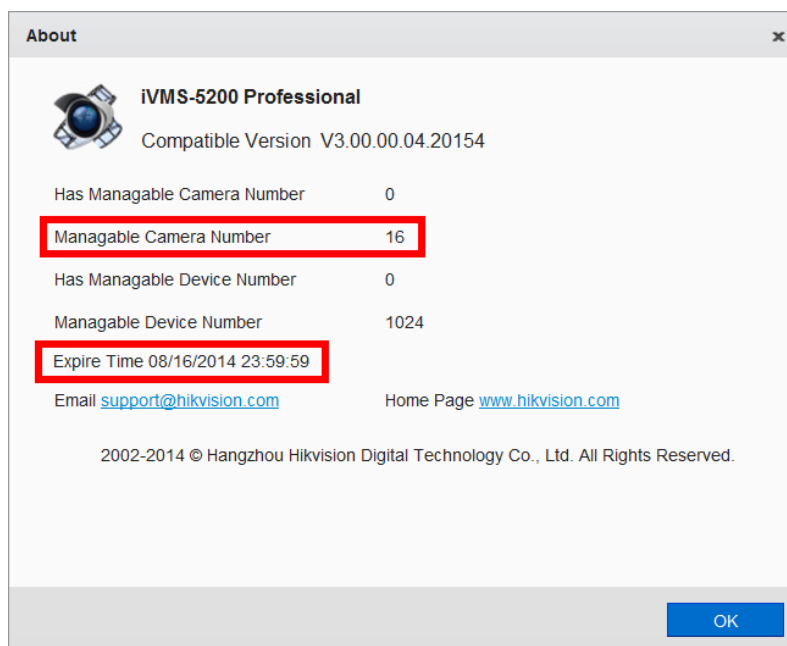
To uninstall the Control Client, you can refer to *Chapter 3.2 Uninstalling the Server Modules* for detailed steps.

Chapter 4 Activating CMS

After you install the iVMS-5200P, you get a temporary License for certain number of connected cameras within a certain time period. This is called the trial period. If trial period have expired and the CMS has not been activated, the iVMS-5200P will stop working.

To ensure the proper use of the iVMS-5200P, you should activate the CMS before the trial period ends.

Note: Please log into the iVMS-5200P via Web Manager (refer to *Chapter 5.1 Open the Web Manager and Login.*), click **Help** at the top right corner and click **About** to check the trial period and the manageable camera number of your iVMS-5200P.



Two activation modes are available: Dongle and License. We introduce the configuration of these two modes separately here.

If you purchase Dongle, please refer to *Chapter 4.2 Activating via Dongle* for detailed configuration about activating the CMS via Dongle.

If you purchase License, please refer to *Chapter 4.1 Activating via Activation Code* for details.

4.1 Activating via Activation Code

If you purchase the License, you will get an activation code from HIKVISION.

Two ways are selectable according to your network condition.

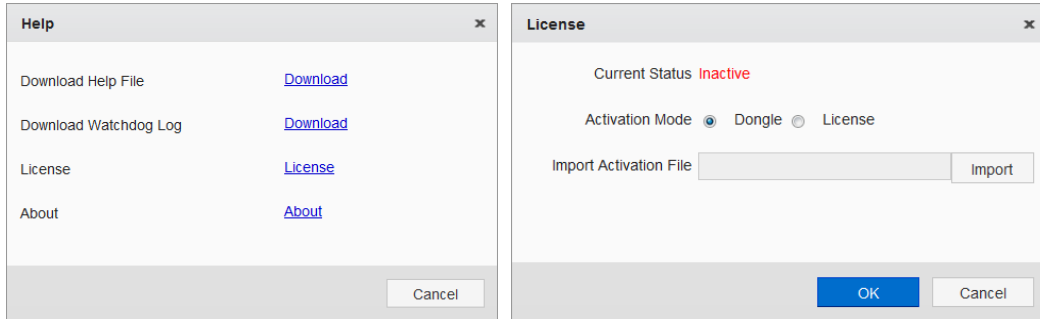
4.1.1 Online Activation

Purpose:

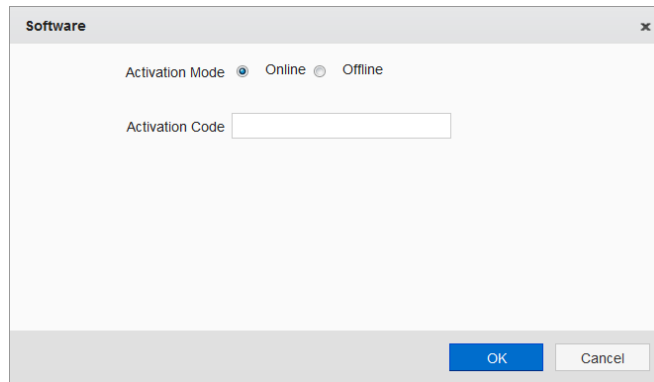
If the CMS to be activated can properly connect to the Internet, you can perform the following steps to activate the License.

Steps:

1. Log into the iVMS-5200P via Web Manager. Please refer to *Chapter 5.1 Open the Web Manager and Login*.
2. After successfully logging in, you enter the control panel of iVMS-5200 Web Manager. Click **Help** at the top right corner and click **License** to pop up the License configuration window.



3. Select the **License** radio button and click **OK**.
4. On the pop-up window, select the **Online** radio button and enter the activation code received when you purchase your License.



5. Click **OK** and the prompt "Activated" will pop up when the CMS is successfully activated.

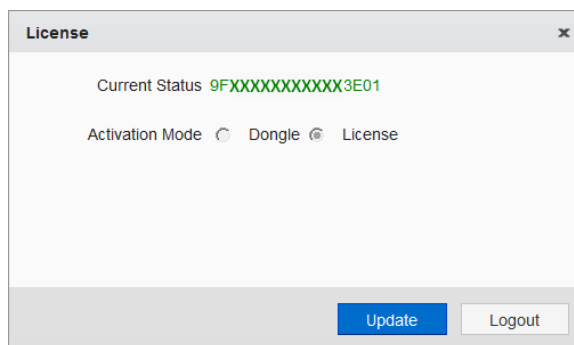
Update

Purpose:

As your project grows, you may need to enlarge the connectable number of cameras for your iVMS-5200P. You can contact your dealer or our salesman to purchase additional features and then perform the following steps to update your License.

Steps

1. Log into the iVMS-5200P via Web Manager. Please refer to *Chapter 5.1 Open the Web Manager and Login*.
2. After successfully logging in, you enter the control panel of iVMS-5200 Web Manager. Click **Help** at the top right corner and click **License** to pop up the License configuration window.



- Click **Update** and enter the activation code received when you purchase your License.
Note: After you have contacted your dealer or our salesman to purchase additional features, you can use the same activation code received when you purchase your License to update the CMS.
- Click **OK** and the prompt “Activated” will pop up when the CMS is successfully updated.

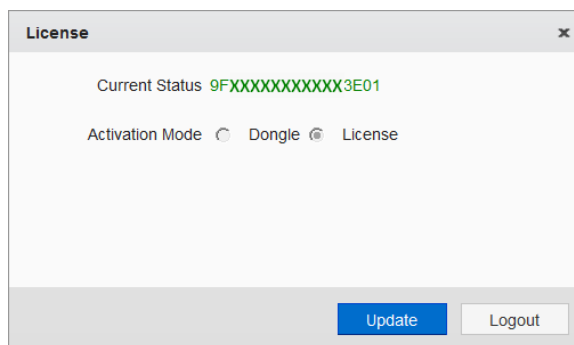
Logout

Purpose:

If you want to run the CMS on another PC or server, you should logout the License first and then activate the CMS again. You can also use the License to activate other CMS after you logout the License.

Steps:

- Log into the iVMS-5200P via Web Manager. Please refer to *Chapter 5.1 Open the Web Manager and Login*.
- After successfully logging in, you enter the control panel of iVMS-5200 Web Manager. Click **Help** at the top right corner and click **License** to pop up the License configuration window.



- Click **Logout** and enter the activation code received when you purchase your License in the pop-up window.
- Click **OK** to confirm logging out. After successfully logging out, the “Logout Succeeded” will pop up. You can activate other CMS with the License.

4.1.2 Offline Activation

Purpose:

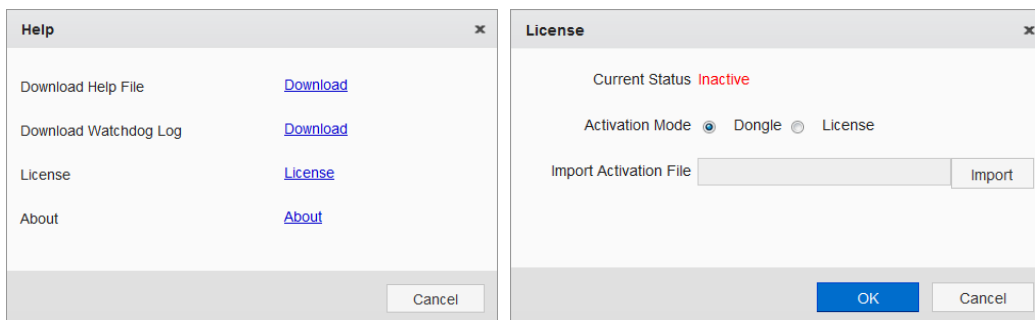
If the CMS to be activated cannot connect to the Internet, you can perform the following steps to

activate the License.

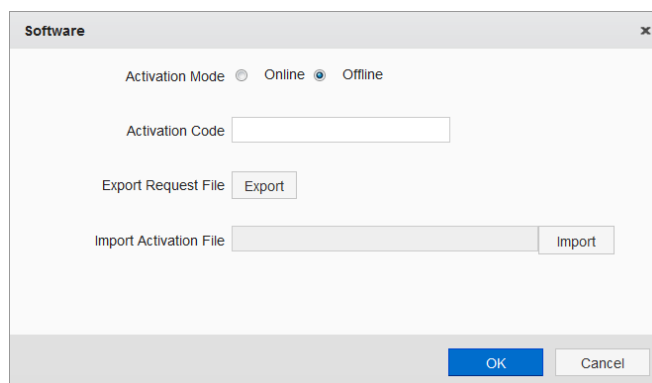
Note: Offline License Activation Utility will also be provided by HIKVISION for offline activation.

Steps:

1. Log into the iVMS-5200P via Web Manager. Please refer to *Chapter 5.1 Open the Web Manager and Login*.
2. After successfully logging in, you enter the control panel of iVMS-5200 Web Manager. Click **Help** at the top right corner and click **License** to pop up the License configuration window.



3. Select the **License** radio button and click **OK**.
4. On the pop-up window, select the **Offline** radio button and enter the activation code received when you purchase your License.



5. Click **Export** and save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).
6. Copy the request file and the Offline License Activation Utility to the PC that can connect to the Internet.

Note: If the PC accessing the iVMS-5200P via Web Manager can connect to the Internet, you can skip step 6.

7. Run the Offline License Activation Utility, click **Browse** to select the License Request Binary File and click **Browse** to set the name and saving path for the License Response Binary File.
8. Click **Send Request to Server** to generate the response file.
9. Save the response file to the proper directory of the PC that accesses the iVMS-5200P via Web Manager. In the License configuration window, click **Import** to import the response file.
10. Click **OK** and the prompt "Activated" will pop up when the CMS is successfully activated.

Update

Purpose:

As your project grows, you may need to enlarge the connectable number of cameras for your iVMS-5200P. You can contact your dealer or our salesman to purchase additional features and then perform the following steps to update your License.

Steps

1. Log into the iVMS-5200P via Web Manager. Please refer to *Chapter 5.1 Open the Web Manager and Login*.
2. After successfully logging in, you enter the control panel of iVMS-5200 Web Manager. Click **Help** at the top right corner and click **License** to pop up the License configuration window.
3. Click **Update** and enter the activation code received when you purchase your License.
Note: After you contact your dealer or our salesman to purchase additional features, you can use the activation code received when you purchase your License to update the CMS.
4. Click **Export** and save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).
5. Copy the request file and the Offline License Activation Utility to the PC that can connect to the Internet.
Note: If the PC accessing the iVMS-5200P via Web Manager can connect to the Internet, you can skip step 5.
6. Run the Offline License Activation Utility, click **Browse** to select the License Request Binary File and click **Browse** to set the name and saving path for the License Response Binary File.
7. Click **Send Request to Server** to generate the response file.
8. Save the response file to the proper directory of the PC that accesses the iVMS-5200P via Web Manager. In the License configuration window, click **Import** to import the response file.
9. Click **OK** and the prompt “Activated” will pop up when the CMS is successfully updated.

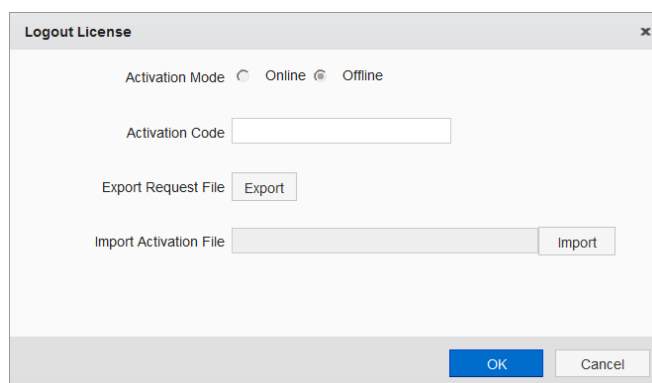
Logout

Purpose:

If you want to run the CMS on another PC or server, you should logout the License first and then activate the CMS again. You can also use the License to activate other CMS after you logout the License.

Steps:

1. Log into the iVMS-5200P via Web Manager. Please refer to *Chapter 5.1 Open the Web Manager and Login*.
2. After successfully logging in, you enter the control panel of iVMS-5200 Web Manager. Click **Help** at the top right corner and click **License** to pop up the License configuration window.
3. Click **Logout** and on the pop-up window, select the **Offline** radio button and enter the activation code received when you purchase your License.



4. Click **Export** and save the request file to the proper directory or the removable storage medium (e.g., USB flash disk).
5. Copy the request file and the Offline License Activation Utility to the PC that can connect to the Internet.

Note: If the PC accessing the iVMS-5200P via Web Manager can connect to the Internet, you can skip step 5.
6. Run the Offline License Activation Utility, click **Browse** to select the License Request Binary File and click **Browse** to set the name and saving path for the License Response Binary File.
7. Click **Send Request to Server** to generate the response file.
8. Save the response file to the proper directory of the PC that accesses the iVMS-5200P via Web Manager. In the License configuration window, click **Import** to import the response file.
9. Click **OK** to confirm logging out.
10. Click **Help** at the top right corner and click **License** to pop up the License configuration window again.
11. Enter the activation code and perform the step 4-9 to logout again to complete the logout operation. After successfully logging out, the "Logout Succeeded" will pop up. You can activate other CMS with the License.

4.2 Activating via Dongle

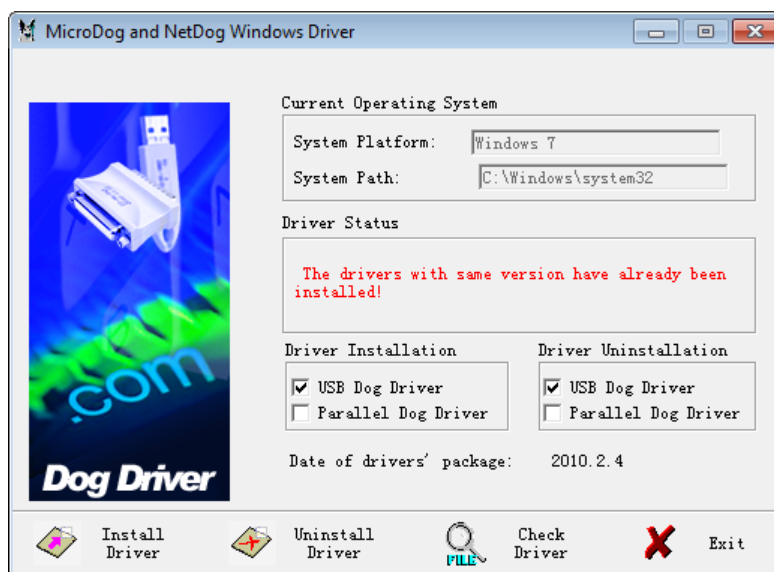
If you purchase the Dongle, you will get a USB Dongle Key and an activation file from HIKVISION. Please perform the following steps to activate the CMS.

Note: You will also get a USB Dongle Key driver from HIKVISION for installing the driver for the Dongle Key.

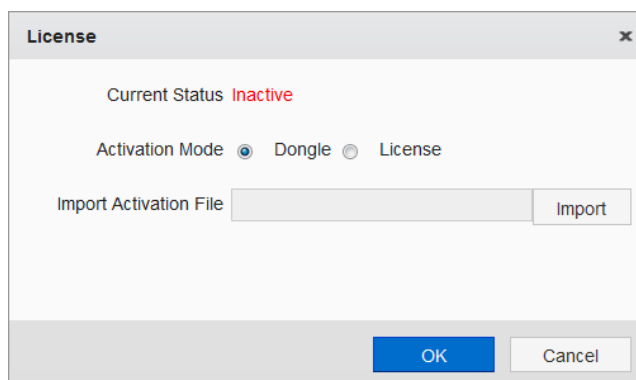
Steps:

1. Decompress the USB Dongle Key driver file and run **MicroDogInstdrv.exe** in the folder as administrator, select the installation type (USB Dog Driver or Parallel Dog Driver) and click **Install Driver** in the pop-up window to install the driver of the Dongle Key.

Note: It is recommended to select USB Dog Driver as the installation type.



2. Insert the Dongle Key into the USB interface of your PC.
3. Log into the iVMS-5200P via Web Manager. Please refer to *Chapter 5.1 Open the Web Manager and Login*.
4. After successfully logging in, you enter the control panel of iVMS-5200 Web Manager. Click **Help** at the top right corner and click **License** to pop up the License configuration window.
5. Select the **Dongle** radio button and click **Import**.



6. On the pop-up window, select the activation file received when you purchase your License and click **Open**.
7. Click **OK** and the prompt "Activated" will pop up when the CMS is successfully activated.

Update

Purpose:

As your project grows, you may need to enlarge the connectable number of cameras for your iVMS-5200P. You can contact your dealer or our salesman to purchase additional features and then perform the following steps to update your CMS.

Steps:

1. Log into the iVMS-5200P via Web Manager. Please refer to *Chapter 5.1 Open the Web Manager and Login*.
2. After successfully logging in, you enter the control panel of iVMS-5200 Web Manager. Click **Help** at the top right corner and click **License** to pop up the License configuration window.

3. Click **Import** and on the pop-up window, select the new activation file received after you purchase additional features and click **Open**.
4. Click **OK** and the prompt "*Activated*" will pop up when the CMS is successfully updated.

Logout

Purpose:

If you want to run the CMS on another PC or server, you should logout the License first and then activate the CMS again. You can also use the License to activate other CMS after you logout the License.

Steps:

1. Log into the iVMS-5200P via Web Manager. Please refer to *Chapter 5.1 Open the Web Manager and Login*.
2. After successfully logging in, you enter the control panel of iVMS-5200 Web Manager. Click **Help** at the top right corner and click **License** to pop up the License configuration window.
3. Click **Logout**. After successfully logging out, the "*Logout Succeeded*" will pop up. You can activate other CMS with the License.

Chapter 5 Accessing the iVMS-5200P

5.1 Open the Web Manager and Login

Running Environment

- **Operating System:** Microsoft Windows 7 / Windows 8 (32 / 64-bit)
- **CPU:** Intel Pentium IV 3.0 GHz or above
- **Memory:** 1G or above
- **Video Card:** RADEON X700 Series
- **Web Browser:** IE 8.0 or above version, Chrome 34.0, Firefox 28.0.

Steps:

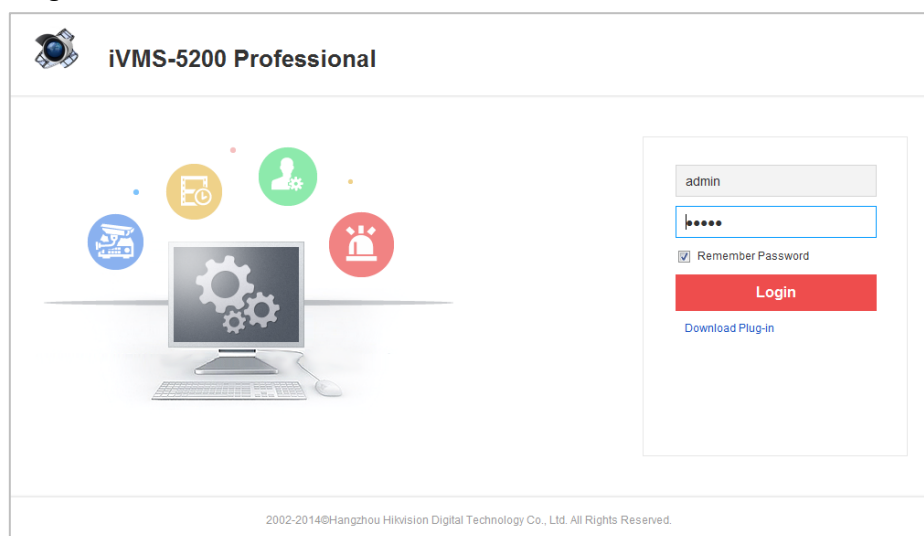
1. In the address bar of the web browser, input the IP address of the CMS (Central Management Server) and press the **Enter** key. A login window will pop up.

Example: If the IP address of CMS is 172.6.21.96, and you should enter **http://172.6.21.96** in the address bar.

2. Input the user name and password of CMS. Optionally, check the checkbox of **Remember Password** to save the password.

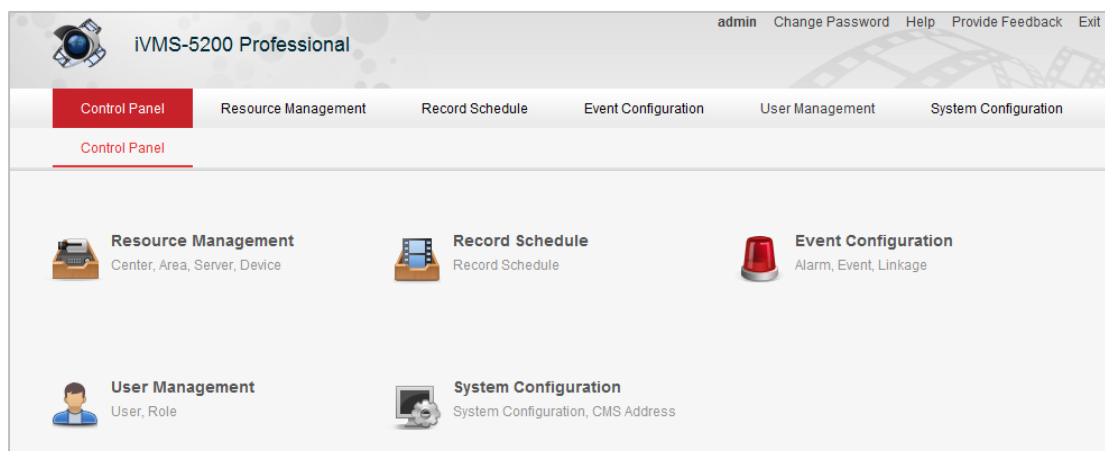
Notes:

- By default, the user name for login is **admin** and the password is **12345**.
 - You are highly recommended to change the default password right after the first login to avoid safety problem.
3. For the first time to login, you should install the plug-in before you can access the functions. Optionally, you can click **Download Plug-in**, run and install the plug-in according to the prompt. After the installation of plug-in, re-open the web browser and log into the iVMS-5200P.
 4. Click **Login**.



5.2 Function Modules

After successfully logging in, you enter the control panel of iVMS-5200 Web Manager.



The iVMS-5200 Web Manager is composed of the following function modules:



The Resource Management module provides the adding, modifying and deleting of areas and different devices, and the devices can be assigned to areas for management.



The Record Schedule module provides the schedule settings for recording.



The Event Configuration module provides the settings of arming schedule, alarm linkage actions and other parameters for different events of the camera, alarm inputs, encoding devices and servers.



The User Management module provides the adding, modifying and deleting of user and roles, and you are allowed to assign different roles for different users. The roles are assigned with different permissions.



The System Configuration module provides the configuration of NTP settings, email settings, IP address settings, etc.

The function modules are easily accessed by clicking the navigation buttons on the control panel or by clicking the corresponding tab.

You can achieve the following functions in the upper-right corner of the main page:

- Change password of the current login user.
- Click **Help** to download the help file and the log files of Watchdog, configure your license and check the information of iVMS-5200P.
- Send your problem or suggestion about the iVMS-5200P to us by clicking **Provide Feedback**. Our technical engineers will handle your problems and suggestions as soon as possible


Chapter 6 Resource Management

6.1 Adding the Encoding Device

Purpose:

Before you can live view, playback via the Control Client or set recording schedule, event configuration via Web Manager, you need to add devices to the iVMS-5200P and manage them by areas.



Click the  icon on the control panel,

or click **Physical View** under **Resource Management** tab to open the Resource Management page.

The screenshot shows the 'Resource Management' page in 'Physical View'. The left sidebar contains a tree view with 'Encoding Device' selected. The main area displays a table of devices with columns for Alias, Device Address, Device Serial No., and Net Status. Below the table, there are options to 'Add to System', 'Modify Network Parameters', 'Restore Default Password', and 'Refresh'. A search bar is also present.

Alias	Device Address	Device Serial No.	Net Status
10.7.34.249	10.7.34.249	DS-2CD2032-I20130420CCWR420556646	Offline
172.10.1.60	172.10.1.60	DS-2CD4132FWD-I220131226CCCH446732260	Online
172.10.1.66	172.10.1.66	iVMS6200C000321807Xl07nZ4DP2gCXu1304221	Offline
172.10.7.123	172.10.7.123	DS-2DE7186-AE20140224CCWR452513138	Online

Two kinds of view are available for management: the Physical View provides the management of devices and servers; the Logical View provides the management of areas.

6.1.1 Adding Online Devices

Purpose:

The active online encoding devices in the same local subnet with the Web Manager will be displayed on a list. You can click the **Refresh** button to get the latest information of the online devices. You can also select protocol in the drop-down list, or input key word of the IP address and click **Search** to show the corresponding devices.

Steps:

1. Click the **Physical View** tab.
2. Click **Encoding Device** and check the checkbox of the device(s) to be added from the list.
3. Click **Add to System** to open the device adding dialog box.
4. Input the required information.

IP Address: Input the IP address of the device. The IP address of the device is obtained automatically in this adding mode.

Port: Input the device port No.. The default value is **8000**.

User Name: Input the user name of the device. By default, the user name is *admin*.

Password: Input the password of the device. By default, the password is *12345*.

Note: If multiple devices are selected, only user name and password are available in the pop-up dialog box.

- Click **Save** to add the device(s).

Online Device(4)					
Add to System Modify Network Parameters Restore Default Password Refresh					
IP Address	Device Type	Port	Device Serial No.	Added	
<input checked="" type="checkbox"/> 10.16.1.11	DS-7604HI-ST	8000	DS-7604HI-ST0820130708BBRR418574198WCVU	No	
<input type="checkbox"/> 10.16.1.72	DS-7204HWI-E1	8000	DS-7204HWI-E10420140514AAWR123456789WCVU	No	
<input type="checkbox"/> 10.16.1.2	DS-2CD2112-I	8000	DS-2CD2112-I0120130508CCRR421767892	No	
<input type="checkbox"/> 10.16.1.28	IDS-2DF7286-A	8000	IDS-2DF7286-A20140430CCH128456752C	No	

Modify Network Information

Select a device from the list, and click **Modify Network Parameters** to edit the network information of the selected device.

Restore Default Password

Select the device from the list, click **Restore Default Password**, input the security code, and then you can restore the default password of the selected device.

Note: The default admin password of the device is 12345, and the security code is returned after you send the date and serial No. of the device to the manufacturer.

6.1.2 Adding Devices by IP Address

Steps:

- Click the **Physical View** tab.
 - Click **Encoding Device** and click **Add** to activate the device adding dialog box.
 - Select **Single IP Address** as the adding mode.
 - Input the required information.
 - Add Offline Devices (Optional):** If you check this checkbox, when the offline device comes online, the software will connect it automatically. Input the analog camera number, alarm input number and alarm output number of the device.
- Note:** When the checkbox of **Add Offline Devices** is checked, the analog camera number, alarm input number and alarm output number items are available.
- Manufacturer (Optional):** Select the manufacturer of the device. If you select third-party device, only adding offline devices is available.
 - IP Address:** Input the IP address of the device.
 - Port:** Input the port No. of the device. By default, it's 8000.
 - Alias:** Edit a name for the device as desired.
 - User Name:** Input the user name of the device.
 - Password:** Input the password of the device.
 - Export to Area (Optional):** Check the checkbox to create an area by the device alias. All the cameras, alarm inputs and alarm outputs of the device will be added to the area by default.
 - Superior:** Select the parent area for the newly created area.
 - Stream Media Server:** Input the IP address of the stream media server to get the video stream of a camera via the server. (Optional) If no server has been added to the iVMS-5200P,

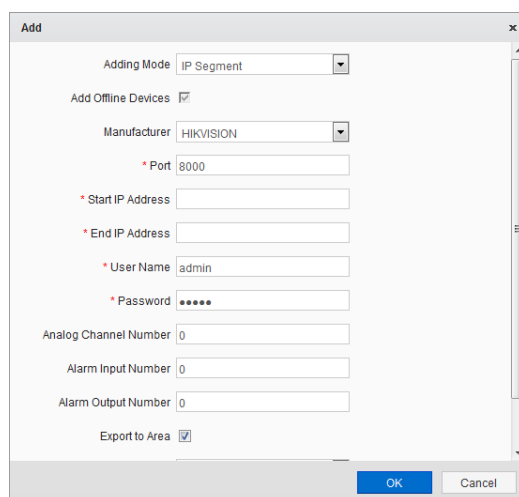
you can click **SMS Management** to add one. For details, please refer to *Chapter 6.2 Adding the Server*.

5. Click **OK** to add the device.

6.1.3 Adding Devices by IP Segment

Steps:

1. Click the **Physical View** tab.
2. Click **Encoding Device** and click **Add** to activate the device adding dialog box.
3. Select **IP Segment** as the adding mode.
4. Input the required information.
 - **Manufacturer (Optional):** Select the manufacturer of the devices.
 - **Port:** Input the port No. of the devices. By default, it's 8000.
 - **Start IP Address:** Input the start address of the IP segment.
 - **End IP Address:** Input the end address of the IP segment.
 - **User Name:** Input the user name of the device.
 - **Password:** Input the password of the device.
 - **Analog Channel Number / Alarm Input Number / Alarm Output Number (Optional):** Input the analog camera number, alarm input number and alarm output number of the device.
 - **Export to Area (Optional):** Check the checkbox to create an area by the device alias. All the cameras, alarm inputs and alarm outputs of the device will be added to the area by default.
 - **Superior:** Select the parent area for the newly created area.
 - **Stream Media Server:** Input the IP address of the stream media server to get the video stream of a camera via the server. (Optional) If no server has been added to the iVMS-5200P, you can click **SMS Management** to add one. For details, please refer to *Chapter 6.2 Adding the Server*.
5. Click **OK**, and the device of which the IP address is between the start IP address and end IP address will be added to the device list.



6.1.4 Adding Devices by Port Segment

Steps:

1. Click the **Physical View** tab.
2. Click **Encoding Device** and click **Add** to activate the device adding dialog box.
3. Select **Port Segment** as the adding mode.
4. Input the required information.
 - **Manufacturer (Optional):** Select the manufacturer of the devices.
 - **IP Address:** Input the IP address of the device.
 - **Start Port No.:** Input the start port No. of the port segment.
 - **End Port No.:** Input the end port No. of the port segment.
 - **User Name:** Input the user name of the device.
 - **Password:** Input the password of the device.
 - **Analog Channel Number / Alarm Input Number / Alarm Output Number (Optional):** Input the analog camera number, alarm input number and alarm output number of the device.
 - **Export to Area (Optional):** Check the checkbox to create an area by the device alias. All the cameras, alarm inputs and alarm outputs of the device will be added to the area by default.
 - **Superior:** Select the parent area for the newly created area.
 - **Stream Media Server:** Input the IP address of the stream media server to get the video stream of a camera via the server. (Optional) If no server has been added to the iVMS-5200P, you can click **SMS Management** to add one. For details, please refer to *Chapter 6.2 Adding the Server*.
5. Click **OK**, and the device of which the port No. is between the start port No. and end port No. will be added to the device list.

6.1.5 Adding Devices by HiDDNS

Steps:

1. Click the **Physical View** tab.
2. Click **Encoding Device** and click **Add** to activate the device adding dialog box.
3. Select **HiDDNS** as the adding mode.
4. Input the required information.
 - **Add Offline Devices (Optional):** If you check this checkbox, when the offline device comes online, the software will connect it automatically. Input the analog camera number, alarm input number and alarm output number of the device.

Note: When the checkbox of **Add Offline Devices** is checked, the analog camera number, alarm input number and alarm output number items are available.

 - **HiDDNS Address:** Input the HiDDNS server address.
 - **Alias:** Edit a name for the device as desired.
 - **Device Domain:** Input the device domain name registered on HiDDNS server.
 - **User Name:** Input the user name of the device.
 - **Password:** Input the password of the device.
 - **Export to Area (Optional):** Check the checkbox to create an area by the device alias. All the cameras, alarm inputs and alarm outputs of the device will be added to the area by default.
 - **Superior:** Select the parent area for the newly created area.
 - **Stream Media Server:** Input the IP address of the stream media server to get the video stream of a camera via the server. (Optional) If no server has been added to the iVMS-5200P, you can click **SMS Management** to add one. For details, please refer to *Chapter 6.2 Adding the Server*.
5. Click **OK** to add the device.

6.1.6 Adding Devices by Domain Name

Steps:

1. Click the **Physical View** tab.
2. Click **Encoding Device** and click **Add** to activate the device adding dialog box.
3. Select **Single IP Address** as the adding mode.
4. Input the required information.
 - **Add Offline Devices (Optional):** If you check this checkbox, when the offline device comes online, the software will connect it automatically. Input the analog camera number, alarm input number and alarm output number of the device.

Note: When the checkbox of **Add Offline Devices** is checked, the analog camera number, alarm input number and alarm output number items are available.
 - **Manufacturer (Optional):** Select the manufacturer of the device. If you select third-party device, only adding offline devices is available.
 - **Domain:** Input the domain name of the device.
 - **Port:** Input the port No. of the device. By default, it's 8000.
 - **Alias:** Edit a name for the device as desired.
 - **User Name:** Input the user name of the device.
 - **Password:** Input the password of the device.
 - **Export to Area (Optional):** Check the checkbox to create an area by the device alias. All the cameras, alarm inputs and alarm outputs of the device will be added to the area by default.
 - **Superior:** Select the parent area for the newly created area.
 - **Stream Media Server:** Input the IP address of the stream media server to get the video stream of a camera via the server. (Optional) If no server has been added to the iVMS-5200P, you can click **SMS Management** to add one. For details, please refer to *Chapter 6.2 Adding the Server*.
5. Click **OK** to add the device.

The devices will be displayed on the device list for management after added successfully. You can check the network status, camera number, and other information of the added devices on the list.

You can also input the device name in the filter field for search.

Click the **Alias** field of the device and you can edit the information of the device.

Select the device(s) from the list and click **Delete** to remove the selected device(s).

Select a device from the list, click **Remote Configuration**, and then you can perform some remote configurations of the selected device if needed.

6.2 Adding the Server

Purpose:

You can add the server to the iVMS-5200P, including SS (Storage Server), SMS (Stream Media Server), MAG (Mobile Access Gateway) and PSS (Picture Storage Server).

Steps:

1. Click the **Physical View** tab.
2. Click a server type on the left panel and click **Add** to activate the server adding dialog box.
3. Input the required information.
 - **Alias:** Edit a name for the device as desired.

- **IP Address:** Input the IP address of the server.
- **CMS IP:** Select the IP address of CMS (Central Management Server). The CMS may have two IP addresses. If the server is in the same subnet with the CMS, select the internal IP address of CMS. If not, please select the external IP address. For detailed information, please refer to *Chapter 9.3.2 CMS IP Settings*.

Note: The ports of different servers have default value entered. If the port No. is changed, you can enter the new value.

4. Click **OK** to add the server.

The servers will be displayed on the server list for management after added successfully. You can check the related information of the added servers on the list.

You can also input the server name in the filter field for search.

Click the **Alias** field of the server and you can edit the information of the server.

Select the server(s) from the list, and click **Delete** to remove the selected server(s).

6.3 Area Management

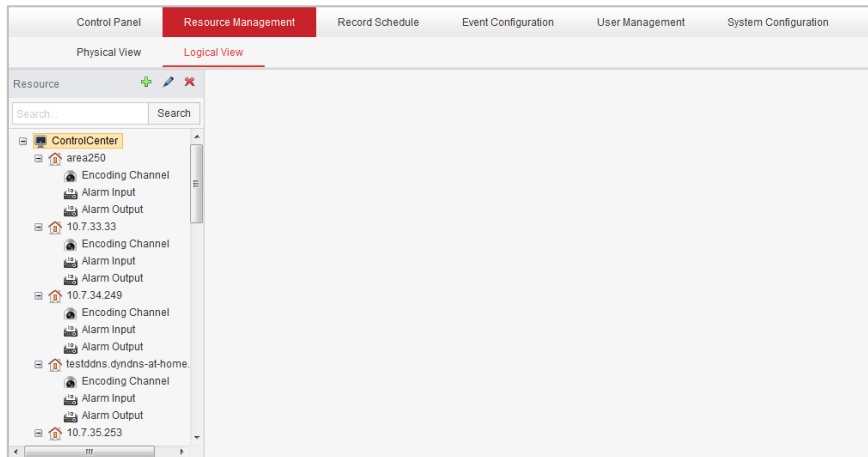
Purpose:

The devices added should be organized into areas for convenient management. You can get the live view, play back the record files, and do some other operations of the devices after managing devices by areas.

Before you start:


Devices need to be added to the iVMS-5200P for area management.


Click the **Logical View** tab to enter the Area Management interface.

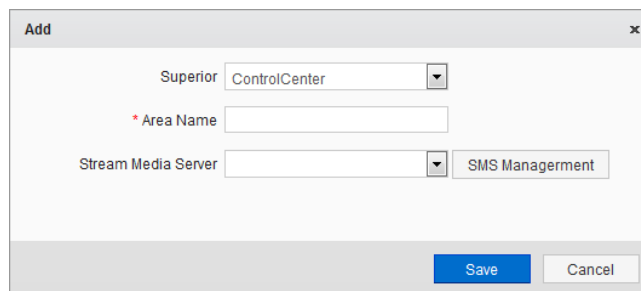


Adding the Area

Steps:

1. Click  to open the Add Area dialog box.
2. Select the parent area in the **Superior** drop-down list.
3. Input an area name as you want. Optionally, you can select a stream media server for the area to get the the video stream of the cameras belonging to this area via the server.
4. Click **Save** to add the new area.

You can also select an area and click  to edit the area.



Adding Camera / Alarm Input / Alarm Output to Area

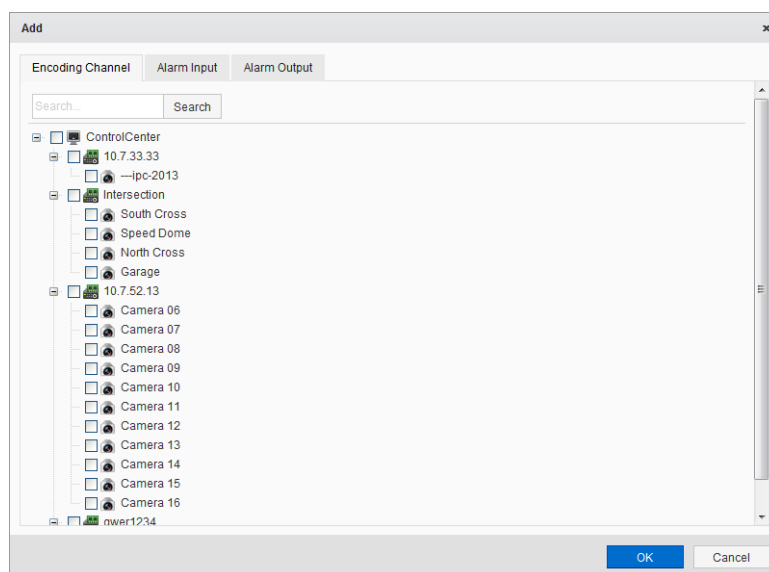
Steps:

1. In the area tree panel, click to select an area.
2. Click **Add** and a dialog box pops up.
3. Click the corresponding tab to add the camera(s), alarm input(s) or alarm output(s) to the area.

Note: You can input the key word in the text filed and click **Search** to find the required device, camera, alarm input or alarm output.
4. Click **OK** to confirm the settings.

Notes:

- Up to 64 cameras can be added to one area.
- A camera, alarm input or alarm output can only be added to one area.



Editing the Camera / Alarm Input / Alarm Output

Steps:

1. Click the field of the Name column to activate the Edit dialog box.
2. Edit the corresponding information.

For camera: You can edit the name, stream type, protocol type, keyboard No. (optional) and MAG association (optional).

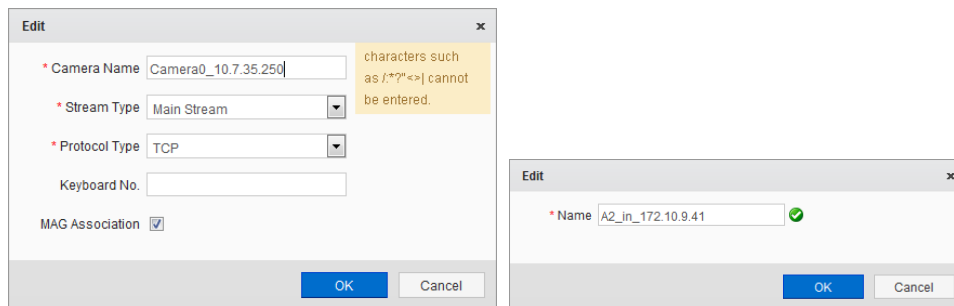
- Keyboard No.: Set a unique number for corresponding to the keyboard.

- **MAG Association:** The iVMS-5260 Mobile Client gets the stream from the camera via the MAG (Mobile Access Gateway) server. A SMS (Stream Media Server) should be added to the iVMS-5200P to activate this function.

For alarm input and alarm output: You can edit the name of the alarm input / output.

3. Click **OK** to save the new settings.

You can also click the field of Encoding Device column to check the details of the device.




Removing Camera / Alarm Input / Alarm Output from the Area

Steps:

1. Select an area, and the cameras, alarm inputs and alarm outputs belonging to the area display.
2. Select the item(s) and click **Delete** to remove the item(s) from the area.


Deleting the Area

Steps:

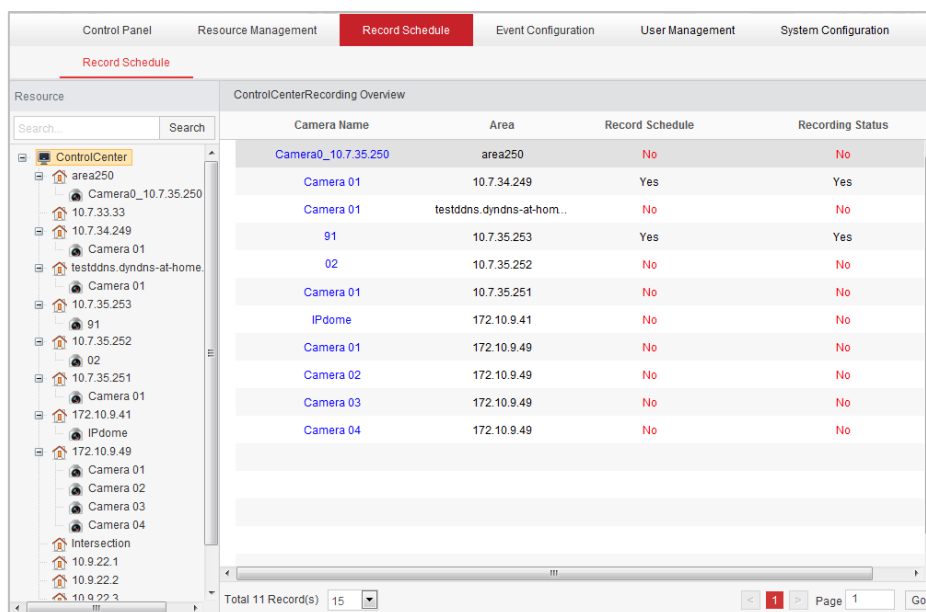
1. Select the area on the area tree panel.
2. Click  and the selected area will be deleted.

Chapter 7 Record Schedule Settings

When there are video storage devices (e.g., HDDs, Net HDDs, SD/SDHC cards) on the local device, or the storage server is available, you can set the record schedule of the cameras for the continuous, alarm triggered or command triggered recording.

Click the  icon on the control panel,

or click **Record Schedule** tab to open the Record Schedule page.



7.1 Recording on Storage Devices of the Encoding Device

Purpose:

Some local devices, including the DVRs, NVRs, and Network Cameras, provide storage devices such as the HDDs, Net HDDs and SD/SDHC cards for record files. You can set a record schedule for the cameras of the local devices.

Before you start:

The newly installed storage devices need to be formatted. Go to the remote configuration page (**Resource Management -> Physical View -> Remote Configuration**) of the device, click **Storage->General**, select the HDD, Net HDD or SD/SDHC card, and click **Format** to initialize the selected storage device.

Steps:

1. Open the Record Schedule page.
2. Select the camera in the camera list or in the area tree panel.

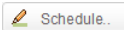


3. Check the checkbox **Enable Record Schedule** under Local Record Schedule to enable device local recording.
4. Select the record schedule template from the drop-down list.
 - All-day Template:** All-day continuous recording whole week.
 - Weekday Template:** All-day continuous recording from Monday to Friday.
 - Weekend Template:** All-day continuous recording from Saturday to Sunday.
 - Recording Template 01-08:** You can edit the templates as desired.

If you need to edit or customize the template, see *Chapter 7.1.1 Configuring Record Schedule Template*.
5. Optionally, click **Copy to** to copy the record schedule settings to other cameras.
6. Click **Save** to save the settings.

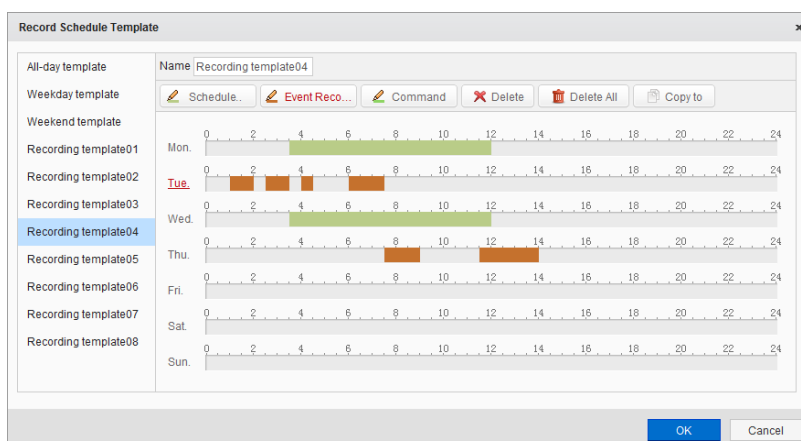
7.1.1 Configuring Record Schedule Template

Perform the following steps to configure the record schedule template:

Steps:

1. Click **Edit Template** to enter the Record Schedule Templates interface. Select the template (Recording Template 01-08) to be set and you can edit the template name.
2. Click the recording type button and then click-and-drag on the time bar to set the time schedule.
 -  refers to continuous recording. The schedule time bar is marked with ■.
 -  refers to the recording triggered by the alarm input or motion detection event. The schedule time bar is marked with ■.
 -  refers to the recording triggered by command. The schedule time bar is marked with ■.
3. Optionally, you can select the schedule time period, and then click **Delete** to delete the selected time period, or click the **Delete All** to delete all the time periods. You can click **Copy to** to copy the time bar settings to other dates.
4. Click **OK** to save the settings.

Note: Up to 4 time periods can be set for each day in the record schedule.



7.2 Recording on Storage Server

Purpose:

The storage server performs as a NVR installed on the server. The record files can be stored in the storage server.

Before you start:

At least one available storage server has been added to the iVMS-5200P. When installing the iVMS-5200P, check the checkbox **Storage Server** to enable the installation of Storage Server.

For adding the Storage Server, please refer to *Chapter 6.2 Adding the Server*.

Steps:

1. Open the Record Schedule page.
2. Select the camera in the camera list or in the area tree panel.
3. Check the checkbox **Enable Record Schedule** under Storage Server Record Schedule to enable recording on storage server.
4. Select the record schedule template from the drop-down list.
If you need to edit the template, see *Chapter 7.1.1 Configuring Record Schedule Template*.
5. Select the storage server from the drop-down list. If you want to add / delete the storage server, click **SS Management**. For detailed configuration, please refer to *Chapter 6.2 Adding the Server*.
6. Select the stream type for recording from the drop-down list and select the disk grouping of the storage server.

Note: For configuration of Storage Server, please refer to *Chapter 10.3.1 How to Allocate Storage Space for Storage Server*.

7. Optionally, you can check the checkbox Obtain Video Stream via Stream Media Server to get the video stream of the camera via stream media server for recording.

Note: A stream media server should be added properly.


8. Optionally, click **Copy to** to copy the record schedule settings to other cameras.
9. Click **Save** to save the settings.

Chapter 8 Event Configuration

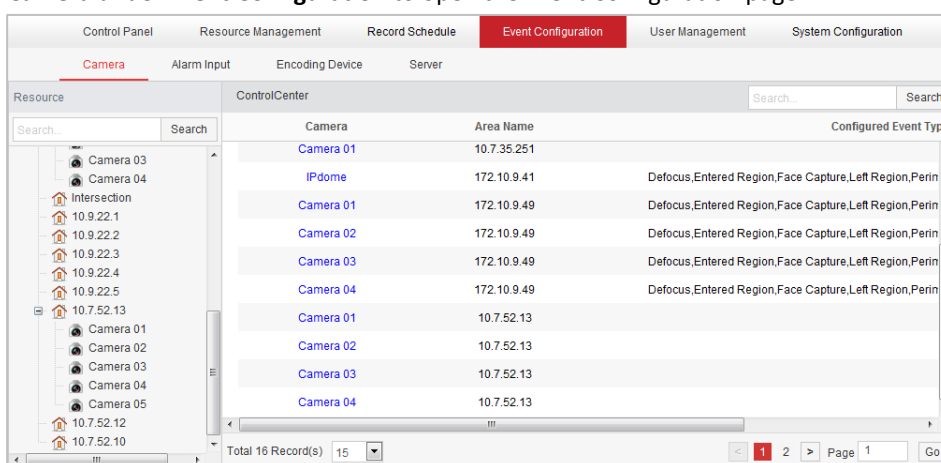
Purpose:

In iVMS-5200 Web Manager, you can assign linkage actions to the event by setting up a rule. For example, when motion is detected, an audible warning appears or other linkage actions happen. The alarm information of the events can be received by the iVMS-5200 Control Client. For detailed information about checking the alarm information, please refer to the *User Manual of iVMS-5200 Control Client*.



Click the  icon on the control panel,

or click **Camera** under **Event Configuration** to open the Event Configuration page.



You can set different linkage actions for the following events:

- Camera Exception
- Alarm Input
- Encoding Device Exception
- Server Exception

Note: Camera exception refers to the video exception or the events detected in the monitoring area of the camera, such as motion detection, video loss, line crossing, etc.

8.1 Configuring Camera Exception Alarm

Note: The camera exception types vary according to the connected device. Here we take the introduction of motion detection settings as an example. For the settings of other exception types, please refer to the *User Manual* of the connected devices.

Purpose:

A motion detection alarm is triggered when the camera detects motion within its defined area. The linkage actions, such as Control Client linkage, recording linkage and alarm output linkage, can be set.

Steps:

1. Select **Camera** under the Event Configuration tab.

2. In the area tree panel, select the camera to be configured and select **Motion Detection** as the event type.
 3. Check the checkbox **Enable** to enable the function of motion detection.
 4. Edit the name for the event, and select the alarm level according to actual needs.
 5. Click **Remote Configuration** and set the parameters for motion detection (Event>Motion Detection) in the pop-up interface.
- Note:** For detailed configuration, please refer to the *User Manual* of the device.
6. Check the checkboxes to enable the linkage actions. For details, see *Table 4.1 Linkage Actions for Motion Detection Alarm*.
 7. Optionally, click **Copy to...** to copy the event parameters to other cameras.
 8. Click **Save** to save the settings.

Table 4.1 Linkage Actions for Motion Detection Alarm

Linkage Type	Linkage Actions	Descriptions
Control Client Linkage	Triggering Pop-up Image of Camera	The image of the selected camera(s) pops up when alarm is triggered.
	Two-way Audio	Enable two-way audio between the Control Client and the selected camera when alarm is triggered.
	Voice Alarm Text	Set the voice text for playing on the PC when alarm is triggered. Note: You should set voice engine as the alarm sound on Local Configuration page of Control Client.
Recording Linkage	Camera Record	Start the recording of the selected camera(s) on the chosen storage location when alarm is triggered. Note: Before you can select the camera(s), you must configure the record schedule for the camera(s) on Record Schedule page. For details, please refer to <i>Chapter 7 Record Schedule Settings</i> .
PTZ Linkage	PTZ Linkage	Trigger to call the preset, patrol or pattern of the selected camera(s) when alarm is triggered.
Alarm Output Linkage	Alarm Output Linkage	Select the alarm output and the external device connected can be activated when alarm is triggered.

Message Linkage	Message Linkage	<p>Send a message of the alarm information to one or more mobile phones.</p> <p>Notes:</p> <ul style="list-style-type: none"> • Before using the message linkage, you should install and configure the SMS (Short Message Service) Modem. For details, please contact our technical engineer. • Only the users that are configured with mobile phone number are available in the pop-up window when you click Receiver. For configuring users, please refer to <i>Chapter 9.2 User Management</i>.
Email Linkage	Email Linkage	<p>Send an Email notification of the alarm information to one or more receivers.</p> <p>Notes:</p> <ul style="list-style-type: none"> • Only the users that are configured with email are available in the pop-up window when you click Receiver. For configuring users, please refer to <i>Chapter 9.2 User Management</i>. • You should configure the email settings for the system in System Configuration page. For details, please refer to <i>Chapter 9.3.1 System Settings</i>.

8.2 Configuring Alarm Input Linkage

Purpose:

When a device's alarm input port receives a signal from an external alarm device, such as smoke detector, doorbell, etc., the alarm input linkage actions are triggered for notification.

Note: The alarm input should be supported by the device.

Before you start:

Add the alarm inputs to the areas for management. For details, please refer to *Chapter 6.3 Area Management*.

Steps:

1. Open the Event Configuration page and click the **Alarm Input** tab.
2. Select the alarm input channel to be configured and check the checkbox **Enable**.
3. Edit the name for the alarm input and select the alarm level for it.
4. Click **Edit** to select or edit the arming schedule. Click **OK** to confirm the settings.

All-day Template: All-day continuous recording whole week.

Weekday Template: All-day continuous recording from Monday to Friday.

Weekend Template: All-day continuous recording from Saturday to Sunday.

Alarm Template 01-08: You can edit the templates as desired. If you need to edit the template, see *Configuring Arming Schedule Template*.

5. Check the checkboxes to activate the linkage actions. For details, see *Table 4.2 Linkage Actions for Alarm Input*.
6. Optionally, click **Copy to...** to copy the event parameters to other alarm inputs.
7. Click **Save** to save the settings.

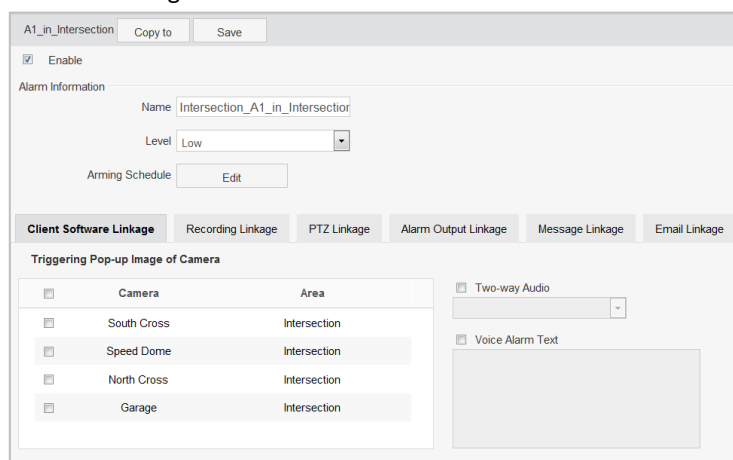


Table 4.2 Linkage Actions for Alarm Input

Linkage Type	Linkage Actions	Descriptions
Control Client Linkage	Triggering Pop-up Image of Camera	The image of the selected camera(s) pops up when alarm is triggered.
	Two-way Audio	Enable two-way audio between the Control Client and the selected camera when alarm is triggered.
	Voice Alarm Text	Set the voice text for playing on the PC when alarm is triggered. Note: You should set voice engine as the alarm sound on Local Configuration page of Control Client.
Recording Linkage	Camera Record	Start the recording of the selected camera(s) on the chosen storage location when alarm is triggered. Note: Before you can select the camera(s), you must configure the record schedule for the camera(s) on Record Schedule page. For details, please refer to <i>Chapter 7 Record Schedule Settings</i> .
PTZ Linkage	PTZ Linkage	Trigger to call the preset, patrol or pattern of the selected camera(s) when alarm is triggered.
Alarm Output Linkage	Alarm Output Linkage	Select the alarm output and the external device connected can be activated when alarm is triggered.
Message Linkage	Message Linkage	Send a message of the alarm information to one or more mobile phones. Notes: <ul style="list-style-type: none"> ● Before using the message linkage, you should install and configure the SMS (Short Message Service) Modem. For details, please contact our technical engineer.

		<ul style="list-style-type: none"> Only the users that are configured with mobile phone number are available in the pop-up window when you click Receiver. For configuring users, please refer to <i>Chapter 9.2 User Management</i>.
Email Linkage	Email Linkage	<p>Send an Email notification of the alarm information to one or more receivers.</p> <p>Notes:</p> <ul style="list-style-type: none"> Only the users that are configured with email are available in the pop-up window when you click Receiver. For configuring users, please refer to <i>Chapter 9.2 User Management</i>. You should configure the email settings for the system in System Configuration page. For details, please refer to <i>Chapter 9.3.1 System Settings</i>.

8.3 Configuring Device Exception Linkage

Steps:

- Open the Event Configuration page and click the **Encoding Device** tab.
- Select the device to be configured.
- Select the device exception type, including Device offline, HDD full, HDD exception, illegal login, etc.
- Check the checkbox **Enable**.
- Edit the name for the event and select the alarm level.
- Click **Edit** to select or edit the arming schedule. Click **OK** to confirm the settings.
 - All-day Template:** All-day continuous recording whole week.
 - Weekday Template:** All-day continuous recording from Monday to Friday.
 - Weekend Template:** All-day continuous recording from Saturday to Sunday.
 - Alarm Template 01-08:** You can edit the templates as desired. If you need to edit the template, see *Configuring Arming Schedule Template*.
- Check the checkboxes to activate the linkage actions. For details, see *Table 4.3 Linkage Actions for Device Exception*.
- Optionally, click **Copy to...** to copy the event parameters to other devices.
- Click **Save** to save the settings.

Table 4.3 Linkage Actions for Device Exception

Linkage Type	Linkage Actions	Descriptions
Control Client Linkage	Voice Alarm Text	<p>Set the voice text for playing on the PC when alarm is triggered.</p> <p>Note: You should set voice engine as the alarm sound on Local Configuration page of Control Client.</p>
Message Linkage	Message Linkage	<p>Send a message of the alarm information to one or more mobile phones.</p> <p>Notes:</p> <ul style="list-style-type: none"> • Before using the message linkage, you should install and configure the SMS (Short Message Service) Modem. For details, please contact our technical engineer. • Only the users that are configured with mobile phone number are available in the pop-up window when you click Receiver. For configuring users, please refer to <i>Chapter 9.2 User Management</i>.
Email Linkage	Email Linkage	<p>Send an Email notification of the alarm information to one or more receivers.</p> <p>Notes:</p> <ul style="list-style-type: none"> • Only the users that are configured with email are available in the pop-up window when you click Receiver. For configuring users, please refer to <i>Chapter 9.2 User Management</i>. • You should configure the email settings for the system in System Configuration page. For details, please refer to <i>Chapter 9.3.1 System Settings</i>.

8.4 Configuring Server Exception Linkage

Purpose:

The linkage actions can be triggered when the server is in exceptional status..

Steps:

1. Open the Event Configuration page and click the **Server** tab.
2. Select the server to be configured.
3. Edit the name for the event and select the alarm level.
4. Click **Edit** to select or edit the arming schedule. Click **OK** to confirm the settings.

All-day Template: All-day continuous recording whole week.

Weekday Template: All-day continuous recording from Monday to Friday.

Weekend Template: All-day continuous recording from Saturday to Sunday.

Alarm Template 01-08: You can edit the templates as desired. If you need to edit the template, see *Configuring Arming Schedule Template*.

5. Check the checkboxes to activate the linkage actions. For details, see *Table 4.4 Linkage Actions for Device Exception*.
6. Optionally, click **Copy to...** to copy the event parameters to other servers.
7. Click **Save** to save the settings.

Table 4.4 Linkage Actions for Server Exception

Linkage Type	Linkage Actions	Descriptions
Control Client Linkage	Voice Alarm Text	Set the voice text for playing on the PC when alarm is triggered. Note: You should set voice engine as the alarm sound on Local Configuration page of Control Client.
Message Linkage	Message Linkage	Send a message of the alarm information to one or more mobile phones. Notes: <ul style="list-style-type: none"> • Before using the message linkage, you should install and configure the SMS (Short Message Service) Modem. For details, please contact our technical engineer.

		<ul style="list-style-type: none"> Only the users that are configured with mobile phone number are available in the pop-up window when you click Receiver. For configuring users, please refer to <i>Chapter 9.2 User Management</i>.
<p>Email Linkage</p>	<p>Email Linkage</p>	<p>Send an Email notification of the alarm information to one or more receivers.</p> <p>Notes:</p> <ul style="list-style-type: none"> Only the users that are configured with email are available in the pop-up window when you click Receiver. For configuring users, please refer to <i>Chapter 9.2 User Management</i>. You should configure the email settings for the system in System Configuration page. For details, please refer to <i>Chapter 9.3.1 System Settings</i>.

Chapter 9 User and System Management

Purpose:

Multiple user accounts can be added to the iVMS-5200P for accessing the system through Web Manager, Control Client or Web Client, and you are allowed to assign different roles for different users. The roles can be specified with different permissions.

9.1 Role Management

Purpose:

You can assign the permissions to the roles as required, and the user can link to the role to obtain different permissions.

Steps:

1. Select **Role Management** under User Management tab. If no role has been added, two roles are listed by default, including system administrator and system operator.
 - **System Administrator:** Have all the permission of the iVMS-5200P.
 - **System Operator:** Have the all the permission for operating the iVMS-5200 Control Client.
2. Click **Add** to open the Add Role dialog box.
3. Input the role name as desired. Optionally, you can also set the expiry time and description for the role.
4. (Optional) Check the checkbox **Copy from** and select the default or pre-defined role to copy the permission settings of it. If not, please perform step 5 to assign the permissions to the role.
5. In the permission area, select the permission type in the left panel and check the checkboxes to select the corresponding devices or functions.
6. Click **OK** to save the settings.

Managing the Role

Purpose:

After created successfully, the role is added to the role list on the Role Management page. You can edit or delete the information of the roles.


Click the field in the Name column and you can edit the settings of the role.

To delete the information of the role, select the role from the list, and click **Delete**.

Note: The system administrator and system operator roles cannot be edited or deleted.

9.2 User Management



Click the  icon on the control panel,

or click **User Management** under **User Management** to open the User Management page.

Control Panel		Resource Management		Record Schedule		Event Configuration		User Management		System Configuration	
User Management						Role Management					
Add		Delete		Force Logout		Refresh		Search		Search	
Serial No.	User Name	Email	User Status	Mobile	Created	Last Login Time	Description				
1	admin		Online		2009-10-26	2014-05-04 14:12	Administrator can not				
2	Operator		Offline		2009-10-26	2010-03-08 00:00	Operator can not				
3	xjy	xjy@126.com	Offline		2014-04-30	2014-05-04 11:31	Operator xjy				
4	xjy2		Offline		2014-04-30						
5	xjy3		Offline		2014-04-30						
6	xjy4		Offline		2014-04-30						
7	xjy5		Offline		2014-04-30						
8	xjy6		Offline		2014-04-30						
9	xjy7		Offline		2014-04-30						
10	xjy8		Offline		2014-04-30						
11	xjy9		Offline		2014-04-30						

Adding the User

Steps:

1. Select **User Management** under User Management tab.
2. Click **Add** to open the Add User dialog box.
3. Input the user name, password, confirm password, and PTZ control permission as desired. Optionally, you can set the telephone number, email, expire time, user status and description.
 - **Expire Time:** The date that this user account becomes invalid.
 - **User Status:** Two kinds of status are available. If you select freeze, the user account is inactive until you set the user status as normal.
 - **PTZ Control Permission:** Set the permission level (1~100) for PTZ control and the larger the value is, the higher permission the user has. E.g., when user1 and user2 control the PTZ unit at the same time, the user who has the larger PTZ control permission will take the control of the PTZ movement.
4. Click Role Information tab and check the checkboxes to assign the roles for the created user.

Note: If no role has been added, two default roles are selectable: system administrator and system operator. System administrator is the role that owns all the permission of the iVMS-5200P, and system operator is the role that owns the all the permission of the iVMS-5200 Control Client. For creating other roles as desired, please refer to *Chapter 9.1 Role Management*.
5. Click **OK** to save the settings.

Notes:

- A user name cannot contain any of the following characters: / \ : * ? " < > |.
- Up to 64 user accounts can be added.

Managing the User

Purpose:

After created successfully, the user account is added to the user list on the User Management page. The following operations are available for managing the user.

Edit: Click the **User Name** field of the user to edit the information of the device.

Delete: To delete the information of the user, select the user from the list, and click **Delete**.


Force Logout: You can also select the online user and click **Force Logout** to log out the online user.

Change Password: Click **Change Password** of the user and enter the required information to change the password of the user as desired.

9.3 System Configuration

Purpose:

The log expiry time, NTP settings, email settings and CMS (Central Management Server) IP can be configured.

Click the  icon on the control panel,

or click **System Configuration** under **System Configuration** to open the System Configuration page.

9.3.1 System Settings

Purpose:

The log expiry time, NTP settings and email setting can be set.

Steps:

1. Open the System Configuration page.
2. Click the **System Configuration** tab to enter the System Settings interface.
3. Configure the parameters according to actual needs.

Log Expired Time: The time for keeping the log files, once exceeded, the files will be deleted.

NTP Settings: Set the NTP server address and NTP port for time synchronization.

Email Settings:

- **Enable Server Authentication:** If your mail server requires authentication, check this checkbox to use authentication to log in to this server and enter the login User Name and Password.
 - **Enable SSL (optional):** Check the checkbox to enable SSL if required by the SMTP server.
 - **Sender Email Address:** The email address of sender.
 - **Sender Name:** The name of sender.
 - **SMTP Server IP Address:** The SMTP Server IP address or host name (e.g., smtp.263xmail.com).
 - **SMTP Server Port No.:** The SMTP port. The default TCP/IP port used for SMTP is 25.
 - **User Name:** The user account of sender's email.
 - **Password:** The password of sender's email.
 - **Email Test:** Click it to test whether the email settings work. The corresponding attention message box will pop up.
4. Click **Save** to save the settings.

9.3.2 CMS IP Settings

Purpose:

Two IP addresses can be set for CMS to meet the requirements of accessing via both LAN and WAN.

Internal IP Address: The IP address used for LAN access.

External IP Address (Optional): The IP address used for WAN access.

Steps:

1. Open the System Configuration page.
2. Click the **CMS IP** tab to enter the CMS IP Settings interface. The internal IP address cannot be edited.
3. If a static IP address is available for WAN access, enter it in the **External IP address** field.
4. Click **Save** to save the settings.

The screenshot shows the 'CMS IP' configuration window. It has two input fields: 'Internal IP Address' with the value '10.7.33.44' and 'External IP Address' with the value '10.7.34.16'. A blue 'Save' button is located at the bottom center of the form.

Chapter 10 Appendix

10.1 Important Ports

iVMS-5200P uses particular ports when communication with other servers, devices, etc.

Make sure that the following ports are not occupied for data traffic on your network and you should open these ports in the firewall in case you may need to access the system via other networks.

CMS Port	
80	Used for web browser access.
5800	The port of MQ (message queue). Used for receiving the alarm information by the Control Client.
6300	The port for record query. Used for receiving the query conditions.
6502	The monitoring port of manual alarm.
7200	Used for receiving the alarm of HIKVISION devices in listening mode.
7000	Used for receiving the PTZ control command from the Control Client.
7002	Used for receiving the PTZ control command from the Mobile Client.
SMS Port	
6678	The communication port between the CMS and the SMS.
6001	The port of the network management agent.
554	Used for accepting the request of RTSP.
10000-12000	The value range for the getting-stream port pair (RTP/UDP) via UDP transmission and the value range for the getting-stream port pair (RTP/RTSP) via TCP transmission.
SS Port	
6400	The communication port between the CMS and the SS, and the port for searching the video files of the SS.
6401	The port of the network management agent. Used for inspecting the status of the Network Management Server.
6304	Used for accepting the request of RTSP.
20000-22000	The value range for the getting-stream port pair (RTP/RTCP) via UDP transmission.
MAG Port	
7071	The port of the network management agent. Used for inspecting the status of the Network Management Server.
7072	The communication port between the CMS and the MAG.
556	Used for accepting the request of RTSP.
12000-14000	The value range for the getting-stream port pair (RTP/UDP) via UDP transmission.
PSS Port	
8008	The port for uploading and downloading the pictures.
7512	The port of the network management agent. Used for inspecting the status of the Network Management Server.

10.2 FAQ

Q: Why does the CMS fail to start?

A: Please check that the port 80 (you can input `netstat -ano|findstr "80"` in the console) of your PC installing the CMS is not occupied by other service. If it is occupied:

- Please change the port of the service to other value since the port 80 should be used when running the CMS. Please consult your IT system administrator if in doubt about how to changing the port No..
- Or please perform the following steps to change the port of CMS to other available value.

Steps:

1. Shut down all iVMS-5200P modules and exit the iVMS-5200 Service Watchdog.
2. Go to the installation directory of the CMS, and open the server.xml file (by default, the directory is: `C:\Program Files\iVMS-5200 Professional\iVMS-5200 CMS\webserver\Tomcat\conf`).
3. Find the content `Connector port="80" protocol="HTTP/1.1"` in the file and change the 80 to other value (e.g., 85) that is not occupied by other service.
4. Run the Watchdog as administrator and check the status of CMS. The status changes to *Running* which means the CMS is working properly.
5. Then you can log into the iVMS-5200P via Web Manager by inputting `http://IP address of CMS:new port` in the address bar of your web browser.

Example: Input `http://172.6.21.55:85` in the address bar to access the iVMS-5200P.

Q: Why does the status of the services on the Watchdog show as Unusable?

A: You may not run the Watchdog as administrator. Please exit the Watchdog and then right-click to run it as administrator.

Note: Consult your IT system administrator if in doubt about your rights.

Q: Why does the status of the Storage Server on the Watchdog show as Unusable after successfully allocating the storage space for the Storage Server?

A: The Storage Server should be installed on the 64-bit PC or server. Please make sure that the PC or server that running the Storage Server is 64-bit operating system.

10.3 How to


10.3.1 How to Allocate Storage Space for Storage Server

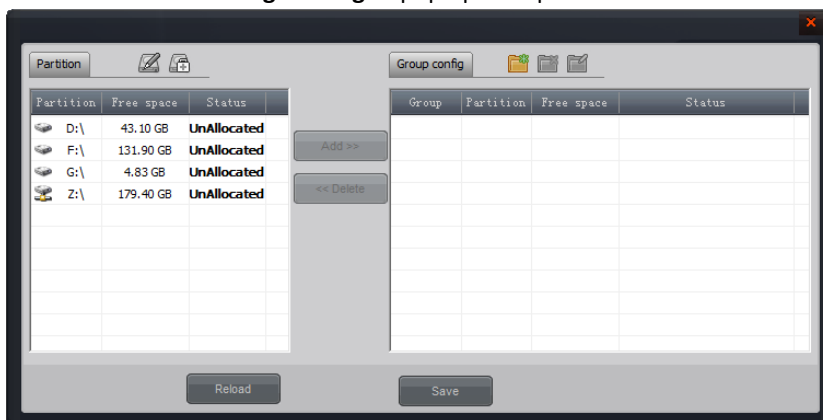
Purpose:


After you install the SS (Storage Server), you should allocate the storage space for it before you can store the record files on it.

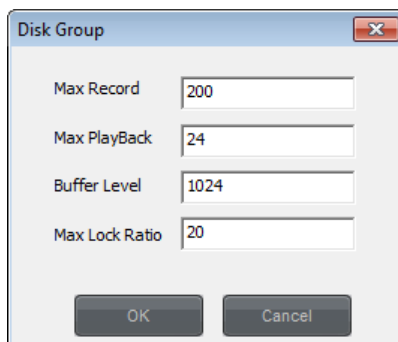
Note: The SS must be installed on the 64-bit PC or server to work properly.




Steps:

1. Double-click  on the desktop or click **Start->All Programs->iVMS-5200 Professional->iVMS-5200 Storage Config** to pop up the Space Allocation window.

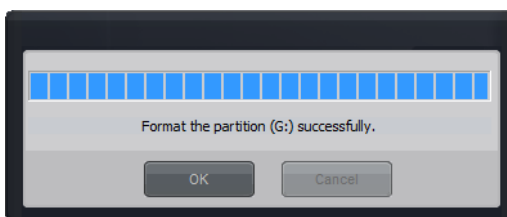


2. In the Group Config panel, click  to create a disk group and configure the parameters in the pop-up window. It is recommended to use the default settings.
 - Max Record:** The maximum number of cameras that can record on this Storage Server
 - Max Playback:** The maximum number of cameras that can play back from this Storage Server via Control Client.
 - Buffer Level:** The size of memory buffer each camera occupies for recording.
 - Max Lock Ratio:** The maximum percentage of HDD space that could be locked. Locked record files won't be overwritten when HDD is full.



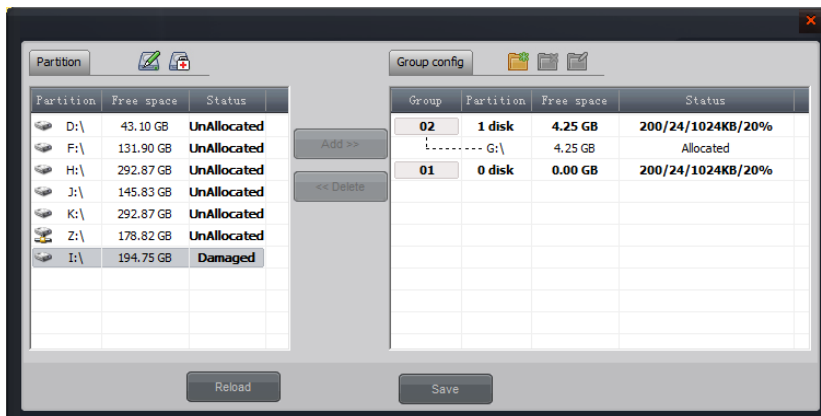
3. Click **OK** to create the disk group. You can also click  to delete the group or click  to edit the parameters of the group.
4. In the Partition panel, click to select an available disk and click  to pre-allocate the disk.

Note: The pre-allocation will format the disk and all the data on the disk will be erased. Please back up and remove all the data on the disk before pre-allocating it.
5. After successfully pre-allocating, the following dialog box pops up. Click **OK** to confirm.



Note: If the status of the pre-allocated disk becomes *Damaged*, you can click  to repair the

disk.



- Click to select a disk group, select a pre-allocated disk and click **Add>>** to add the disk to the group. You can add multiple disks to a group.
Note: You can also select the disk and click **<<Delete** to remove the disk from the group.
- Click **Save** to save the allocation for the Storage Server. You can repeat step 2-6 to create more disk groups for the Storage Server.


10.3.2 How to Configure PSS Allocation and Upload Alarm Pictures to PSS

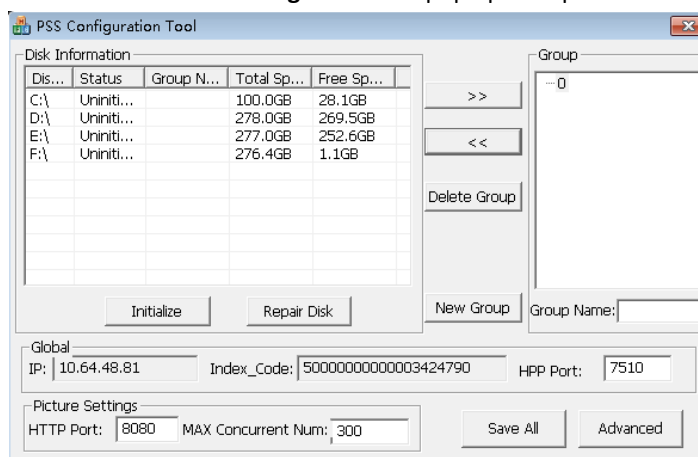
Purpose:

After you install the PSS (Picture Storage Server), you should allocate the storage space for it before you can use it.

Note: The function of uploading alarm pictures to PSS should be supported by the device. Please contact your dealer or our salesman to get the list of the supported devices.

Steps:

- Double-click  on the desktop or click **Start->All Programs->iVMS-5200 Professional->iVMS-5200 Picture Storage Server** to pop up the Space Allocation window.

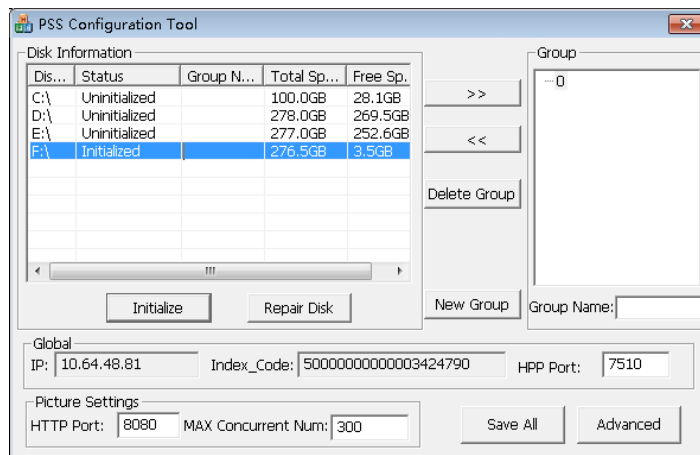


- In the Group panel, edit a name in the Group Name field and click **New Group** to create a new group. There is a group 0 created by default.
- In the Disk Information panel, click to select an available disk and click **Initialize** to pre-allocate

the disk. After successfully pre-allocating, the status of the disk changes to *Initialized*.

Notes:

- The pre-allocation will format the disk and all the data on the disk will be erased. Please back up and remove all the data on the disk before pre-allocating it.
- If the status of the disk changes to *Damaged* after pre-allocating, you can click **Repair Disk** to repair the disk.



4. Click to select a group, select a pre-allocated disk and click >> to add the disk to the group. You can add multiple disks to a group.

Notes:

- You can also select the disk and click << to remove the disk from the group.
 - If you click **Delete Group**, the selected group and the disks under it will be deleted.
5. You can repeat step 2-4 to create more groups. Click **Save All** to save the allocation for the Picture Storage Server.
 6. After configuring the PSS, you can configure to upload the alarm pictures of the device to the PSS. Please perform the following steps:
 - 1) Set the event configuration via the Web Manager. Please refer to *Chapter 8.1 Configuring Camera Exception Alarm*. The **Upload Image to Center** and **Notify Surveillance Center** should be enabled when configuring the alarm settings to enable uploading the alarm pictures to PSS.
 - 2) View the alarm pictures. Please enter the Alarm Center interface of the Control Client to check the alarm pictures that are uploaded to the PSS. For details, please refer to the *User Manual of iVMS-5200 Control Client*.

The graphic consists of two overlapping rectangles. The front rectangle is red and is tilted slightly counter-clockwise. The back rectangle is light grey and is tilted slightly clockwise, creating a layered effect.

First Choice for Security Professionals