HIKVISION

iVMS-5200 Web Manager

User Manual

UD.6L0202D1465A01

Hikvision® Network Digital Video Recorder 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

1.1 Description

iVMS-5200 Web Manager is a B/S client for management of iVMS-5200 Professional Surveillance Platform. It provides multiple functionalities, including device management, record schedule settings, event configuration, user management, etc., for the iVMS-5200 platform to manage the connected devices.

This user manual describes the function, configuration and operation steps of iVMS-5200 Web Manager. To ensure the properness of usage and stability of the Web Manager, please refer to the contents below and read the manual carefully before installation and operation.

1.2 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 8.0 or above version, Firefox 3.5 or above version, Safari 5.02 or above version.

Notes:

- For high stability and good performance, these above system requirements must be met.
- The software does not currently support 64-bit operating system; the above mentioned 64-bit operating system refers to the system which supports 32-bit applications as well.

1.3 Login

Steps:

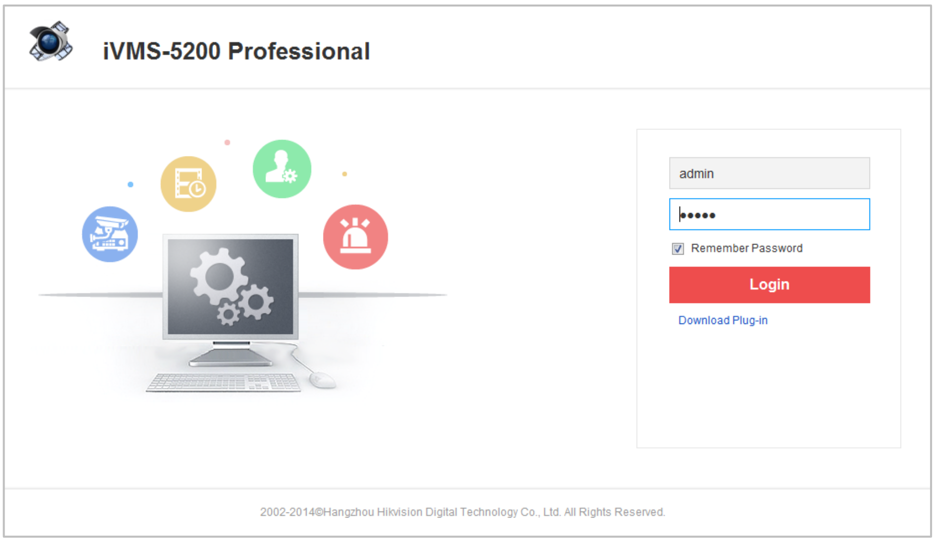
1. In the address bar of the web browser, input the IP address of the CMS (Central Management Server) and press the **Enter** key. A login window will pop up.

   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:

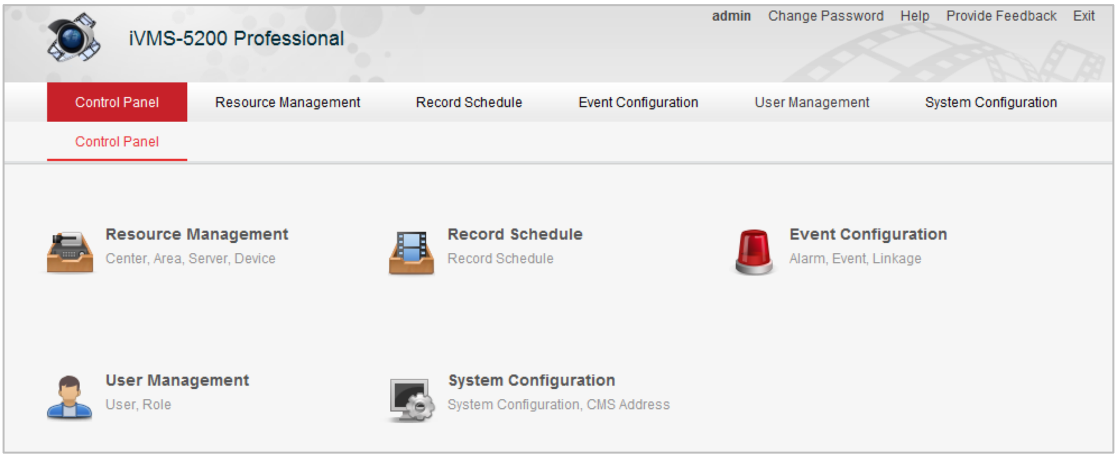
   - By default, the user name for login is ***admin*** and the password is ***12345***.
   - You are highly recommended to change the default password right after the first login to avoid safety problem.
3. For the first time to login, you should install the plug-in before you can access the functions. 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 platform.

4. Click **Login**.


iVMS-5200 Professional
admin
•••••
☑ Remember Password
Login
Download Plug-in
2002-2014©Hangzhou Hikvision Digital Technology Co., Ltd. All Rights Reserved.

1.4 Function Modules

After successfully login, 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-5200 platform.
- Send your problem or suggestion about the platform to us by clicking **Provide Feedback**. Our technical engineers will handle your problems and suggestions as soon as possible

Chapter 2 Resource Management

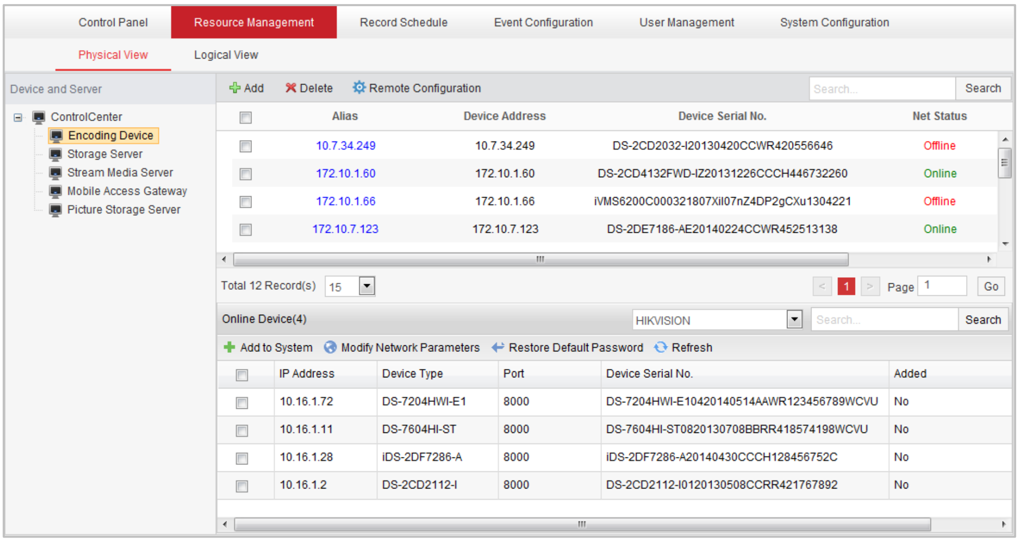
2.1 Adding the Encoding Device

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 platform 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.



□	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-IZ20131226CCCH446732260	Online
□	172.10.1.66	172.10.1.66	iVMS6200C000321807Xil07nZ4DP2gCXu1304221	Offline
□	172.10.7.123	172.10.7.123	DS-2DE7186-AE20140224CCWR452513138	Online

□	IP Address	Device Type	Port	Device Serial No.	Added
□	10.16.1.72	DS-7204HWI-E1	8000	DS-7204HWI-E10420140514AAWR123456789WCVU	No
□	10.16.1.11	DS-7604HI-ST	8000	DS-7604HI-ST0820130708BBRR418574198WCVU	No
□	10.16.1.28	iDS-2DF7286-A	8000	iDS-2DF7286-A20140430CCCH128456752C	No
□	10.16.1.2	DS-2CD2112-I	8000	DS-2CD2112-I0120130508CCRR421767892	No

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.

2.1.1 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.

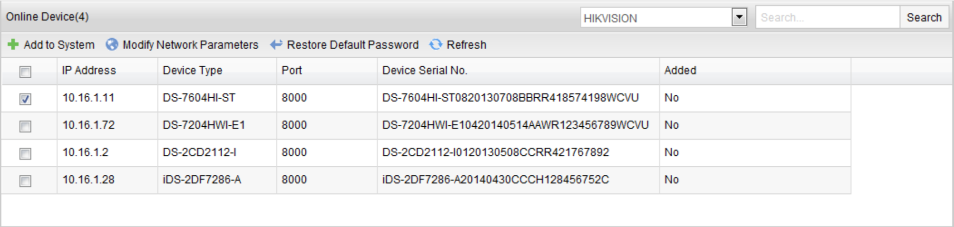
   Port: Input the device port No.. The default value is *8000*.

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.

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



□	IP Address	Device Type	Port	Device Serial No.	Added
☑	10.16.1.11	DS-7604HI-ST	8000	DS-7604HI-ST0820130708BBRR418574198WCVU	No
□	10.16.1.72	DS-7204HWI-E1	8000	DS-7204HWI-E10420140514AAWR123456789WCVU	No
□	10.16.1.2	DS-2CD2112-I	8000	DS-2CD2112-I0120130508CCRR421767892	No
□	10.16.1.28	iDS-2DF7286-A	8000	iDS-2DF7286-A20140430CCCH128456752C	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.

2.1.2 Adding Devices by IP Address

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.

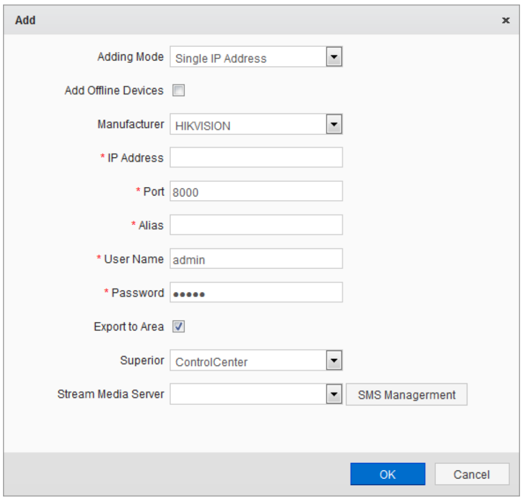
- **Add Offline Devices (Optional):** If you check this checkbox, when the offline device comes online, the software will connect it automatically. Input the analog camera number, alarm input number and alarm output number of the device.

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.
- **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 platform,

you can click **SMS Management** to add one. For details, please refer to *Chapter 2.2 Adding the Server*.

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



Add

Adding Mode: Single IP Address

Add Offline Devices □

Manufacturer: HIKVISION

* IP Address:

* Port: 8000

* Alias:

* User Name: admin

* Password: •••••

Export to Area ☑

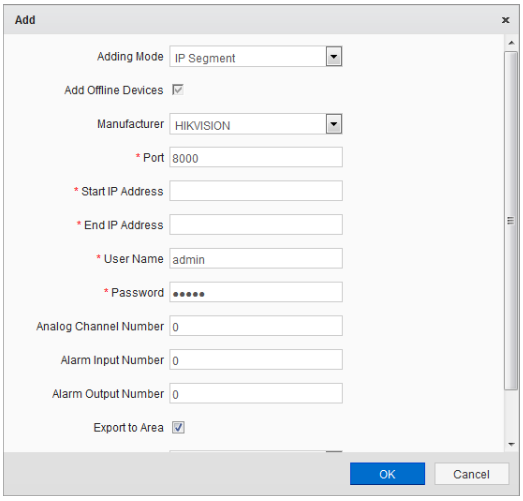
Superior: ControlCenter

Stream Media Server:

2.1.3 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 platform, you can click **SMS Management** to add one. For details, please refer to *Chapter 2.2 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.



Adding Mode: IP Segment

Add Offline Devices ☑

Manufacturer: HIKVISION

* Port: 8000

* Start IP Address:

* End IP Address:

* User Name: admin

* Password: ●●●●●

Analog Channel Number: 0

Alarm Input Number: 0

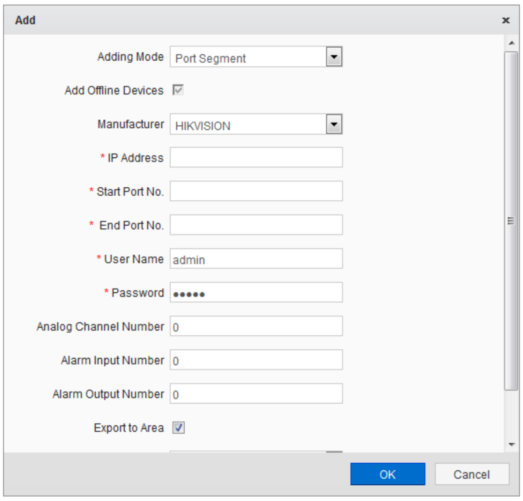
Alarm Output Number: 0

Export to Area ☑

2.1.4 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 platform, you can click **SMS Management** to add one. For details, please refer to *Chapter 2.2 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.



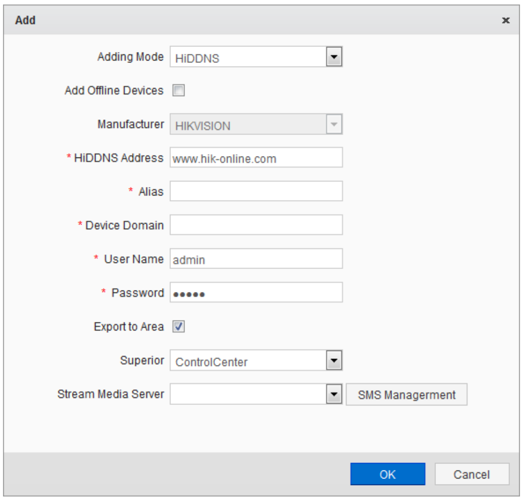
Adding Mode: Port Segment
Add Offline Devices: ☑
Manufacturer: HIKVISION
* IP Address:
* Start Port No.:
* End Port No.:
* User Name: admin
* Password: •••••
Analog Channel Number: 0
Alarm Input Number: 0
Alarm Output Number: 0
Export to Area: ☑

2.1.5 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 platform, you can click **SMS Management** to add one. For details, please refer to *Chapter 2.2 Adding the Server*.
5. Click **OK** to add the device.



Add

Adding Mode: HiDDNS

Add Offline Devices: □

Manufacturer: HIKVISION

* HiDDNS Address: www.hik-online.com

* Alias:

* Device Domain:

* User Name: admin

* Password: ●●●●●

Export to Area: ☑

Superior: ControlCenter

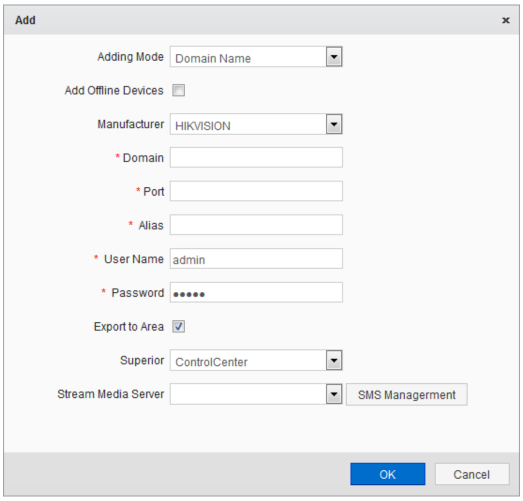
Stream Media Server:

2.1.6 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 platform, you can click **SMS Management** to add one. For details, please refer to *Chapter 2.2 Adding the Server*.
5. Click **OK** to add the device.



Add

Adding Mode: Domain Name

Add Offline Devices: □

Manufacturer: HIKVISION

* Domain:

* Port:

* Alias:

* User Name: admin

* Password: ●●●●●

Export to Area: ☑

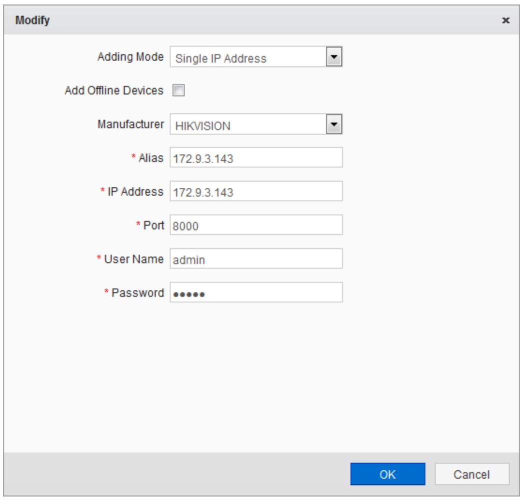
Superior: ControlCenter

Stream Media Server:

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.



Modify

Adding Mode: Single IP Address

Add Offline Devices: □

Manufacturer: HIKVISION

* Alias: 172.9.3.143

* IP Address: 172.9.3.143

* Port: 8000

* User Name: admin

* Password: ●●●●●

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.

2.2 Adding the Server

Purpose:

You can add the server to the platform, 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 *5.3.2 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).

2.3 Area Management

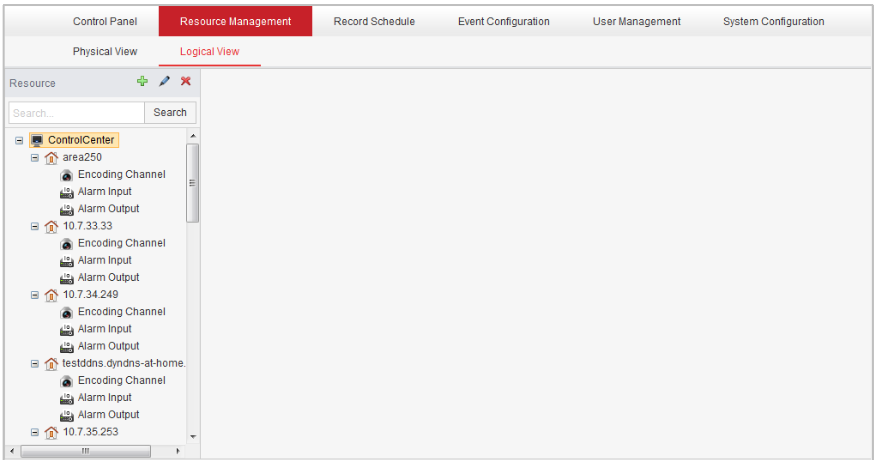
Purpose:

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-5200 platform for area management.

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

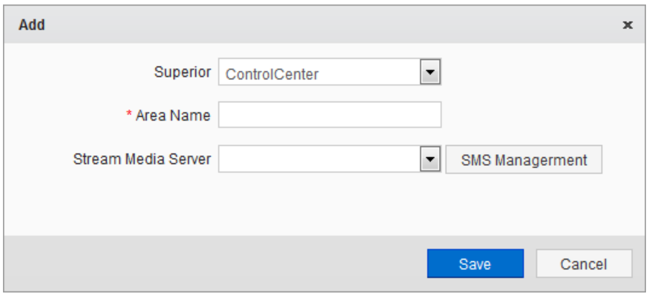


Adding the Area

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.



Add ×

Superior: ControlCenter

* Area Name:

Stream Media Server: SMS Management

Save Cancel

Adding Camera / Alarm Input / Alarm Output to Area

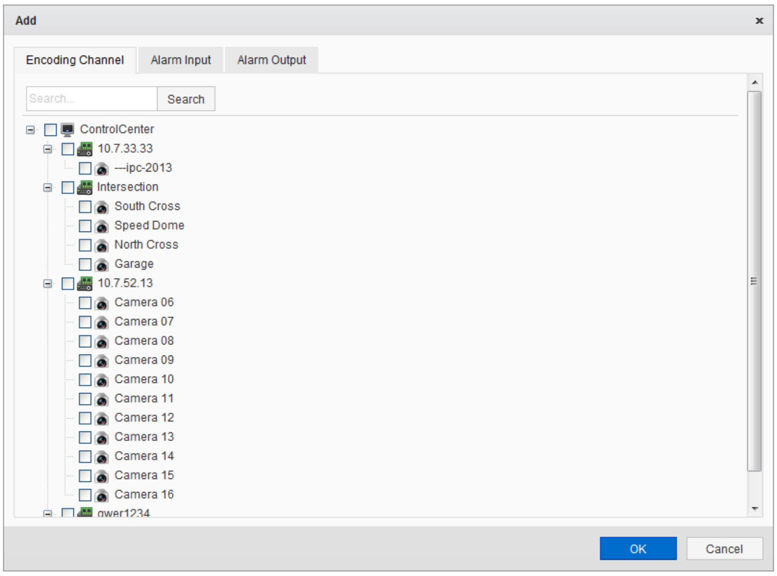
Steps:

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.



Add ×

Encoding Channel | Alarm Input | Alarm Output

Search... Search

```
⊟ □ ControlCenter
  ⊟ □ 10.7.33.33
      □ ---ipc-2013
  ⊟ □ Intersection
      □ South Cross
      □ Speed Dome
      □ North Cross
      □ Garage
  ⊟ □ 10.7.52.13
      □ Camera 06
      □ Camera 07
      □ Camera 08
      □ Camera 09
      □ Camera 10
      □ Camera 11
      □ Camera 12
      □ Camera 13
      □ Camera 14
      □ Camera 15
      □ Camera 16
  ⊟ □ qwer1234
```

OK Cancel

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).

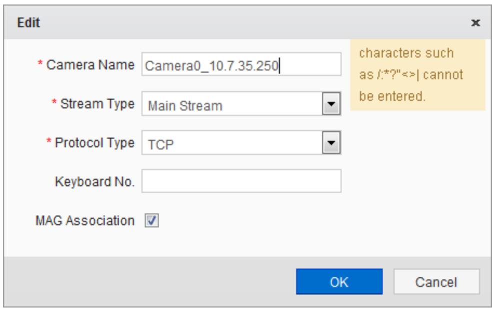
   - Keyboard No.: Set a unique number for corresponding to the keyboard.

- 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 platform 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.



* Camera Name: Camera0_10.7.35.250

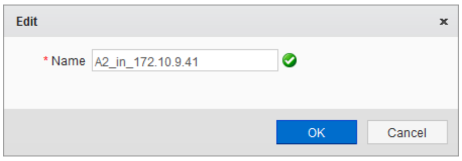
characters such as /:*?"<>| cannot be entered.

* Stream Type: Main Stream

* Protocol Type: TCP

Keyboard No.:

MAG Association ☑



* Name: A2_in_172.10.9.41 ✓

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:

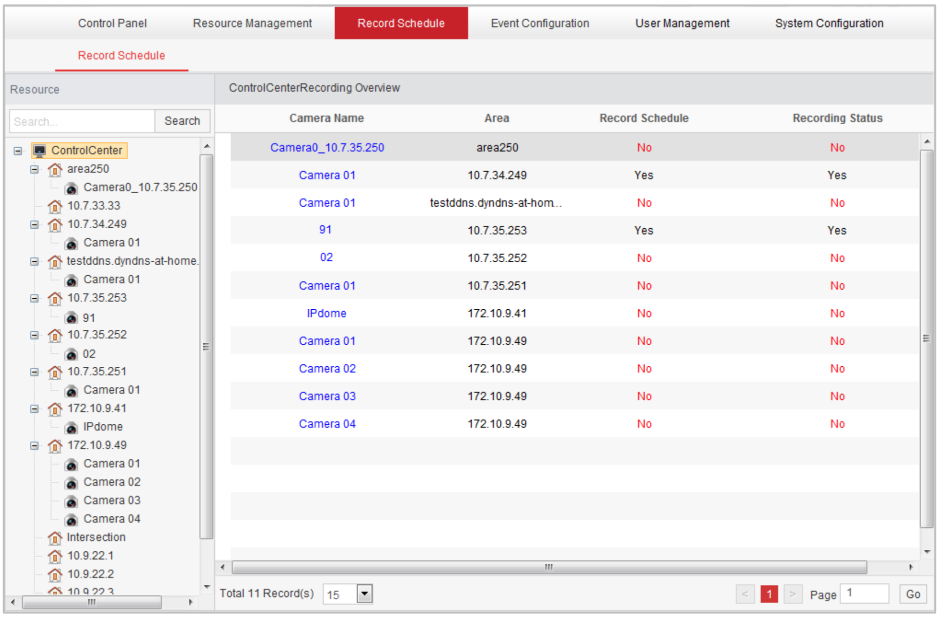
1. Select the area on the area tree panel.
2. Click ✖ and the selected area will be deleted.

Chapter 3 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.



ControlCenterRecording Overview

Camera Name	Area	Record Schedule	Recording Status
Camera0_10.7.35.250	area250	No	No
Camera 01	10.7.34.249	Yes	Yes
Camera 01	testddns.dyndns-at-hom...	No	No
91	10.7.35.253	Yes	Yes
02	10.7.35.252	No	No
Camera 01	10.7.35.251	No	No
IPdome	172.10.9.41	No	No
Camera 01	172.10.9.49	No	No
Camera 02	172.10.9.49	No	No
Camera 03	172.10.9.49	No	No
Camera 04	172.10.9.49	No	No

Total 11 Record(s) 15 ▾ < 1 > Page 1 Go

3.1 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 3.1.1 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.

3.1.1 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.

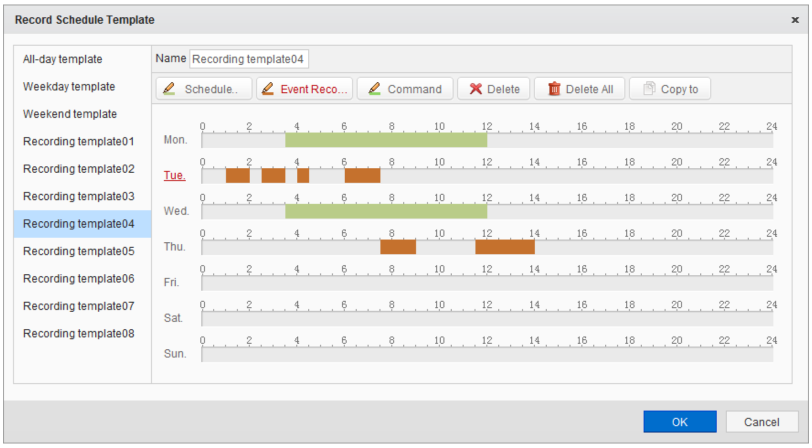
   Schedule.. refers to continuous recording. The schedule time bar is marked with 🟩.

   Event Reco... refers to the recording triggered by the alarm input or motion detection event. The schedule time bar is marked with 🟧.

   Command refers to the recording triggered by command. The schedule time bar is marked with 🟩.

   Note: Recording triggered by command is only available for the ATM transactions when the ATM DVR is added to iVMS-5200.
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.


Record Schedule Template

All-day template
Weekday template
Weekend template
Recording template01
Recording template02
Recording template03
Recording template04
Recording template05
Recording template06
Recording template07
Recording template08

Name Recording template04

3.2 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-5200 platform. When installing the iVMS-5200, check the checkbox **Storage Server** to enable the installation of storage server.

For adding the storage server, please refer to *Chapter 2.2 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 3.1.1 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 2.2 Adding the Server*.
6. Select the stream type for recording from the drop-down list and select the disk grouping of the storage server.
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 4 Event Configuration

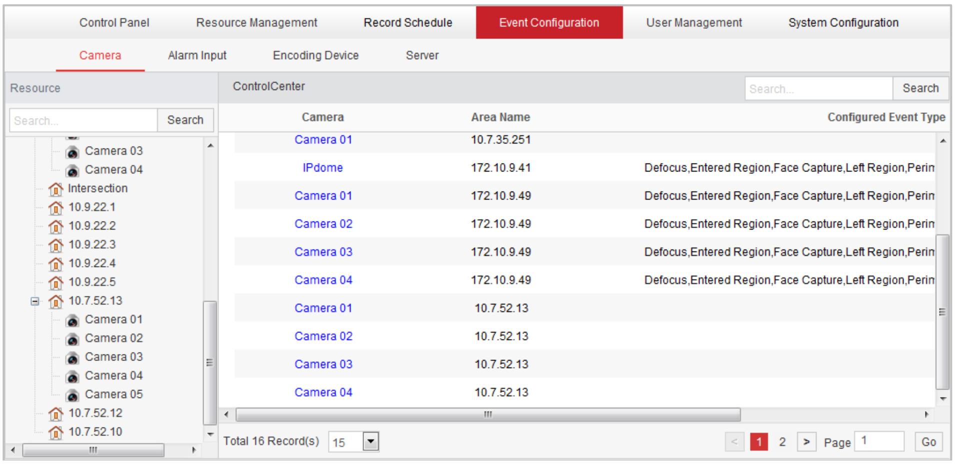
Purpose:

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.



Camera	Area Name	Configured Event Type
Camera 01	10.7.35.251	
IPdome	172.10.9.41	Defocus,Entered Region,Face Capture,Left Region,Perim
Camera 01	172.10.9.49	Defocus,Entered Region,Face Capture,Left Region,Perim
Camera 02	172.10.9.49	Defocus,Entered Region,Face Capture,Left Region,Perim
Camera 03	172.10.9.49	Defocus,Entered Region,Face Capture,Left Region,Perim
Camera 04	172.10.9.49	Defocus,Entered Region,Face Capture,Left Region,Perim
Camera 01	10.7.52.13	
Camera 02	10.7.52.13	
Camera 03	10.7.52.13	
Camera 04	10.7.52.13	

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.

4.1 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:

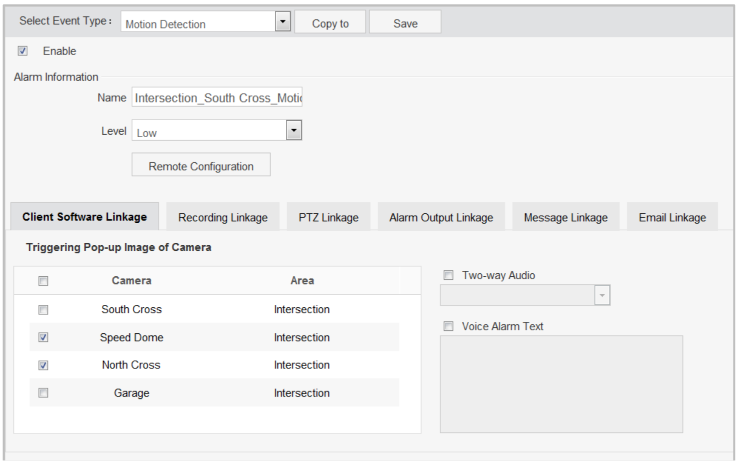
A motion detection alarm is triggered when the camera detects motion within its defined area. The linkage actions, such as Control Client linkage, recording linkage and alarm output linkage, can be set.

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.



Select Event Type: Motion Detection

☑ Enable

Alarm Information

Name: Intersection_South Cross_Motic

Level: Low

Triggering Pop-up Image of Camera

□	Camera	Area
□	South Cross	Intersection
☑	Speed Dome	Intersection
☑	North Cross	Intersection
□	Garage	Intersection

□ Two-way Audio

□ Voice Alarm Text

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 *Chapter 3 Record Schedule Settings*.
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. **Note:** 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 *Chapter 5.1 User Management*.
Email Linkage	**Email Linkage**	Send an Email notification of the alarm information to one or more receivers. **Notes:** ● 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 *Chapter 5.1 User Management*. ● You should configure the email settings for the system in System Configuration page. For details, please refer to *Chapter 5.3.1 System Settings*.

4.2 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.

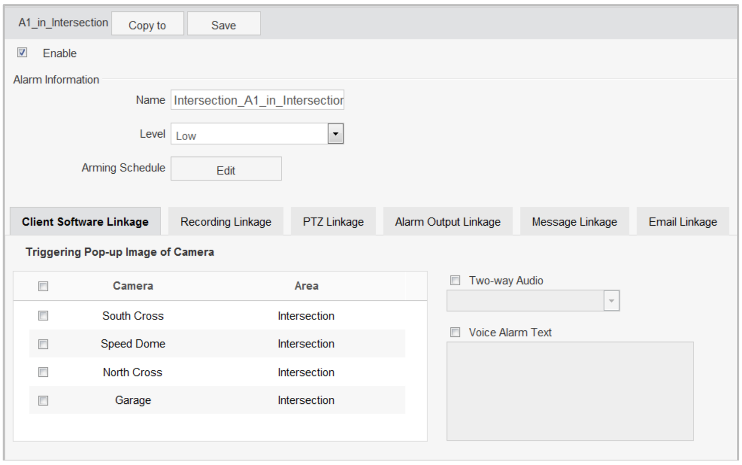
Note: The alarm input should be supported by the device.

Before you start:

Add the alarm inputs to the areas for management. For details, please refer to *Chapter 2.3 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.



☑ Enable

Alarm Information

Name: Intersection_A1_in_Intersectior

Level: Low

Arming Schedule

Triggering Pop-up Image of Camera

□	Camera	Area
□	South Cross	Intersection
□	Speed Dome	Intersection
□	North Cross	Intersection
□	Garage	Intersection

□ Two-way Audio

□ Voice Alarm Text

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 *Chapter 3 Record Schedule Settings*.
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. ***Note:*** 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 *Chapter 5.1 User Management*.
Email Linkage	**Email Linkage**	Send an Email notification of the alarm information to one or more receivers. ***Notes:*** ● 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 *Chapter 5.1 User Management*. ● You should configure the email settings for the system in System Configuration page. For details, please refer to *Chapter 5.3.1 System Settings*.

4.3 Configuring Device Exception Linkage

Steps:

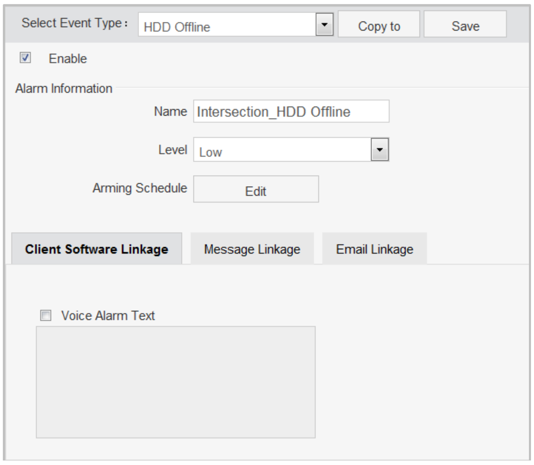
1. Open the Event Configuration page and click the **Encoding Device** tab.
2. Select the device to be configured.
3. Select the device exception type, including Device offline, HDD full, HDD exception, illegal login, etc.
4. Check the checkbox **Enable**.
5. Edit the name for the event and select the alarm level.
6. 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*.
7. Check the checkboxes to activate the linkage actions. For details, see *Table 4.3 Linkage Actions for Device Exception*.
8. Optionally, click **Copy to...** to copy the event parameters to other devices.
9. Click **Save** to save the settings.



Select Event Type: HDD Offline

☑ Enable

Alarm Information

Name: Intersection_HDD Offline

Level: Low

Arming Schedule: Edit

□ Voice Alarm Text

Table 4.3 Linkage Actions for Device 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

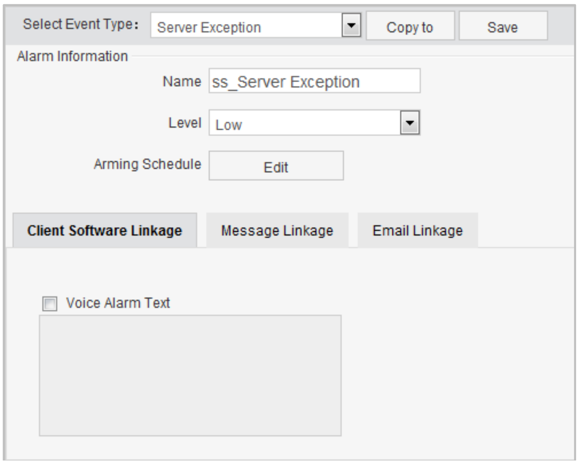
		Local Configuration page of Control Client.
Message Linkage	**Message Linkage**	Send a message of the alarm information to one or more mobile phones. ***Note:*** Only the users that are configured with mobile phone number are available in the pop-up window when you click **Receiver**. For configuring users, please refer to *Chapter 5.1 User Management*.
Email Linkage	**Email Linkage**	Send an Email notification of the alarm information to one or more receivers. ***Notes:*** ● 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 *Chapter 5.1 User Management*. ● You should configure the email settings for the system in System Configuration page. For details, please refer to *Chapter 5.3.1 System Settings*.

4.4 Server Exception

Purpose:

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.



Select Event Type: Server Exception

Alarm Information

Name: ss_Server Exception

Level: Low

Arming Schedule: Edit

☐ Voice Alarm Text

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. ***Note:*** 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 *Chapter 5.1 User Management*.
Email Linkage	**Email Linkage**	Send an Email notification of the alarm information to one or more receivers. ***Notes:*** ● 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 *Chapter 5.1 User Management*. ● You should configure the email settings for the system in System Configuration page. For details, please refer to *Chapter 5.3.1 System Settings*.

Chapter 5 User and System Management

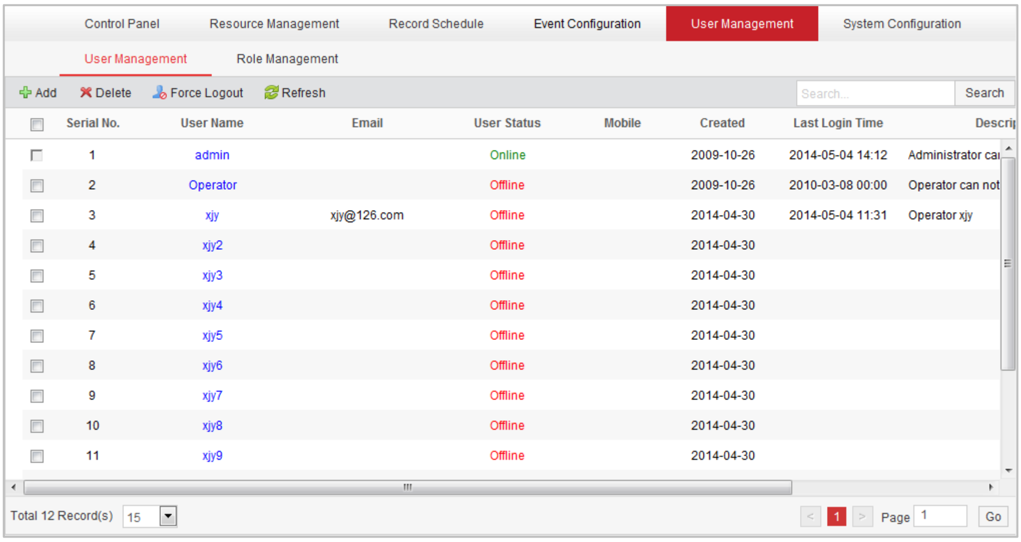
5.1 User Management

Purpose:

Multiple user accounts can be added to the iVMS-5200 platform, and you are allowed to assign different roles for different users. The roles are assigned with different permissions.

Click the 👤 icon on the control panel,

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



□	Serial No.	User Name	Email	User Status	Mobile	Created	Last Login Time	Descri
□	1	admin		Online		2009-10-26	2014-05-04 14:12	Administrator ca
□	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		

Total 12 Record(s) 15

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.

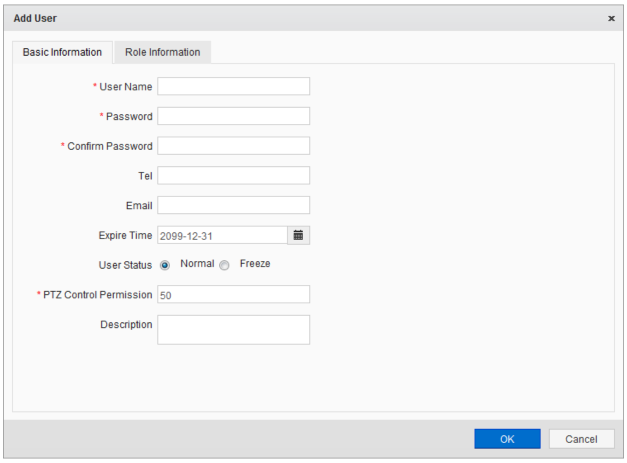
   Note: If no role has been added, two default roles are selectable: system administrator and system operator. System administrator is the role that owns all the permission of the iVMS-5200 platform, and system operator is the role that owns the all the permission of the iVMS-5200

Control Client. For creating other roles as desired, please refer to *Chapter 5.2 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.



* User Name
* Password
* Confirm Password
Tel
Email
Expire Time 2099-12-31
User Status ● Normal ○ Freeze
* PTZ Control Permission 50
Description

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.

5.2 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-5200 platform.
   - **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.

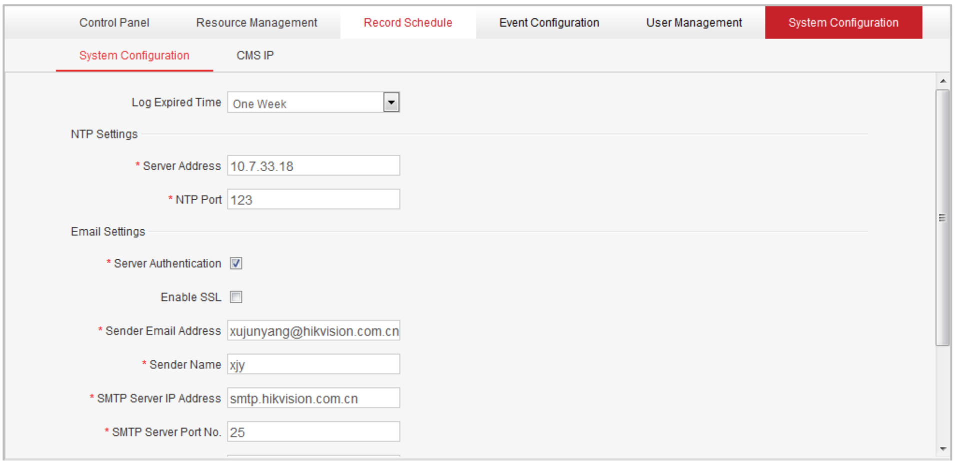
5.3 System Configuration

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.



Log Expired Time: One Week

NTP Settings

* Server Address: 10.7.33.18

* NTP Port: 123

Email Settings

* Server Authentication: ☑

Enable SSL: □

* Sender Email Address: xujunyang@hikvision.com.cn

* Sender Name: xjy

* SMTP Server IP Address: smtp.hikvision.com.cn

* SMTP Server Port No.: 25

5.3.1 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.

5.3.2 CMS IP Settings

Purpose:

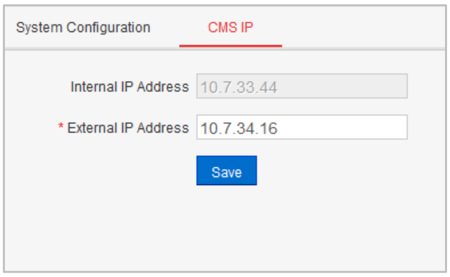
Two IP addresses can be set for CMS to meet the requirements of accessing via both LAN and WAN.

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.



Internal IP Address 10.7.33.44

* External IP Address 10.7.34.16

First Choice for Security Professionals