

KEDACOM

VMS Advanced Configuration Guide

Version 02

March 2016

Kedacom™ and **KEDACOM**™ are registered trademarks of Suzhou Keda Technology Co., Ltd. in China and various other countries. All other trademarks mentioned in this document are the property of their respective holders.

Suzhou Keda Technology Co., Ltd.

131 Jinshan Road

New District, Suzhou, 215011

People's Republic of China

<http://www.kedacom.com/en>

Tel: +86-512-68418188

Fax: +86-512-68412699

© 2016 Suzhou Keda Technology Co., Ltd. All rights reserved.

Without the prior written permission of Suzhou Keda Technology Co., Ltd., any reproduction, translation or retransmission of all or any part of this document for any purpose in either electronic or mechanical form is not allowed.

Notice

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. Suzhou Keda Technology Co., Ltd. is not responsible for printing or clerical errors.

Contents

1	Configuring a Google Map	3
1.1	Mounting a Disk Array.....	3
1.2	Configuring the Partition	3
1.3	Adding the Support for Google Maps	4
1.4	Configuring an Offline Google Map.....	4
1.5	Storing History GPS Tracks	7
1.6	Using the Google Map	8
2	N+1 Hot Backup	10
2.1	Introduction.....	10
2.2	Configuration.....	10
2.3	Enabling/Disabling the Heartbeat Service	13
2.4	Upgrading Main and Standby VMSs.....	14
3	Restoration Using a USB Flash Drive	16
4	Authorized Inter-Domain Operation	17
4.1	Single Device	17
4.2	Multiple Devices	17
4.3	Cancelling Authorization	18
5	External MSS Being Master VMS	19
6	Keyboard Controlled Video Wall	20
6.1	Keyboard Configuration	20
6.2	Keyboard Operations	21
7	Database Recording Recovery	23
8	Disable Punch and Anti-crossing Streams	25
9	Abbreviations and Acronyms	26

Intended Audience

This document is intended for the personnel who:

- Configure the advanced settings of the Video Management System (VMS)
- Know video surveillance basics

Document Versions

Version 02 (2016-03-15)

Compared with Version 01 (2015-09-30), Version 02 (2016-03-15) includes the changes described in the following table.

Change Type	Description
Feature change	Added "External MSS Being Master VMS"; Added "Keyboard Controlled Video Wall"; Added "Database Recording Recovery"; Added "Disable Punch and Anti-crossing Streams".
Editorial change	Updated screenshots and revised the document.

Version 01 (2015-09-30)

Compared with Version 00 (2014-11-20), Version 01 (2015-09-30) includes the changes described in the following table.

Change Type	Description
Feature change	Added authorized inter-domain operations. For details, see chapter 4 "Authorized Inter-Domain Operation."
Editorial change	Updated screenshots and revised the document.

Version 00 (2014-11-20)

This is a draft.

Compatibility

The following table provides the products and VMS software version to which this document applies.

Product	KDM2801H-G2
VMS Software Version	V2R2B3SP1

1 Configuring a Google Map

1.1 Mounting a Disk Array

By default, VMS 2.0 provides only 8 GB of storage space using an mSATA card. You need to mount disk arrays to enable the VMS to support more services, such as using a Google map and storing history GPS tracks.

For details on how to mount a disk array and create one partition, see *VMS Configuration Guide*.



Create only one partition for the disk array.

After one partition is created for the disk array, run the following command to format the partition.

```
mkfs.ext4/dev/sdd1
```

1.2 Configuring the Partition

To configure the partition:

1. Mark the partition as an application data partition using the following command.

```
# e2label/dev/sdd1/kdmappdata
```

2. Write the mount path of the Google map into the SCS configuration file using the following command.

```
# cd/opt/kdm/scs/conf (This is to enter the conf directory.)  
# vi scscfg.ini (This is to make changes to the SCS configuration file.)  
[STORAGE]  
DISABLE_STORAGE_MANAGE = 0  
USE_DISK_WITHOUT_FDISK = 0  
APPDATA_DISK_MOUNT_PATH = /opt/mysql/kdmdb (This is to write the mount path into the SCS  
configuration file.)
```

To verify the configuration:

1. Reboot the VMS using the following command.

```
# reboot
```

2. Check whether the partition is marked as an application data partition using the following command.

```
# telnet.sh rcs
```

```
rcs->nrulist (This is to display the disk list.)
```

```
mLevel
1 /dev/sda1 / 896 312 0 0 MOUNTED ext4
2 /dev/sda2 /opt 2296 1524 0 0 MOUNTED ext4
3 /dev/sda3 635 0 0 0 FORMATTED Linux
4 /dev/sda4 /var/lib/iscsi 56 37 0 0 MOUNTED ext4
-----
diskID[3] diskName[/dev/sdc] diskSize[7388MB] diskAbnNum[0] diskState[ONLINE] CHS[7388,0,0] Usage[BACKUP]
diskSource:[DataTraveler 2.0] usbno: 0
partID partName mountPath totalSize freeSize preAllocSize lockSize partState partTy
mLevel
1 /dev/sdc1 /opt/kdm/cpconf 7370 5283 0 0 MOUNTED vfat
-----
diskID[4] diskName[/dev/sdd] diskSize[4000MB] diskAbnNum[1] diskState[ONLINE] CHS[4000,0,0] Usage[APPDATA]
diskSource:[VIRTUAL-DISK] IP: 10.20.20.207:3260,0 (HostID:5,BusID:0,TargetID:5,LunID:0)
partID partName mountPath totalSize freeSize preAllocSize lockSize partState partTy
mLevel
1 /dev/sdd1 /opt/mysql/kdmdb 39371 39195 0 0 MOUNTED ext4
```

As shown in the preceding figure, the partition is already marked as an application data partition.

3. Check whether the mount path of the Google map is written into the SCS configuration file using the following command.

```
# mount -l
```

```
/dev/sdd1 on /opt/mysql/kdmdb type ext4(rw) [/kdmappdata]
```

As shown in the preceding figure, the mount path of the Google map is already written into the SCS configuration file.

1.3 Adding the Support for Google Maps

Make changes to the **mps.ini** file to add the support for Google maps using the following command.

```
# cd /opt/kdm/mps/conf (This is to enter the conf directory.)
```

```
# vi mps.ini (This is to make changes to the mps.ini file.)
```

```
[mps]
```

```
SupportMapsTypes=google (This is to add the support for google maps.)
```

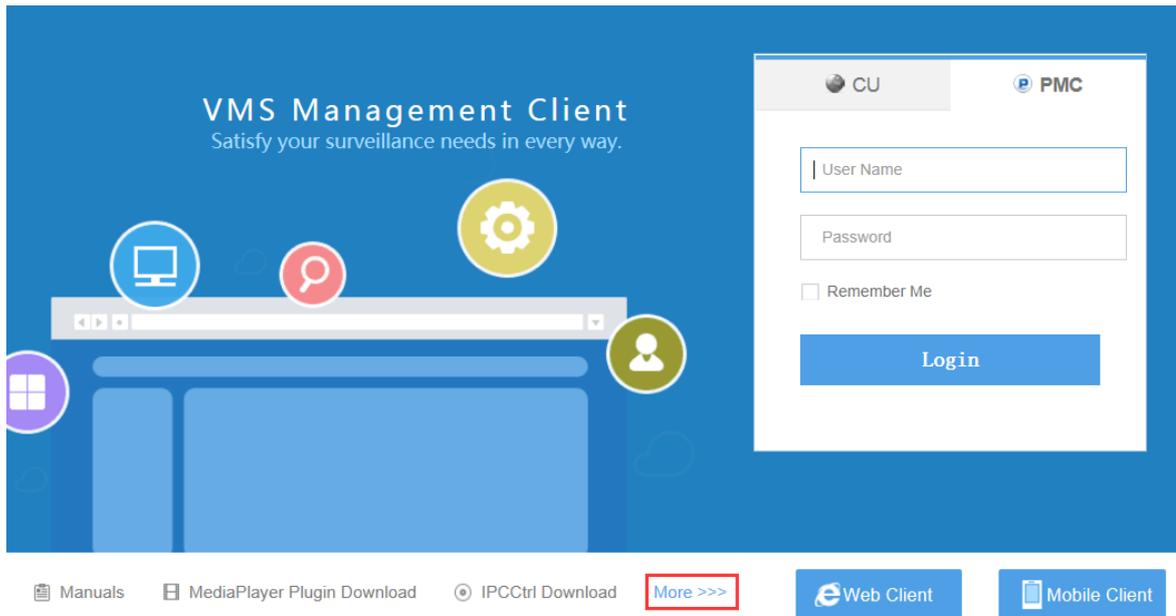
1.4 Configuring an Offline Google Map

1.4.1 Downloading an Offline Google Map

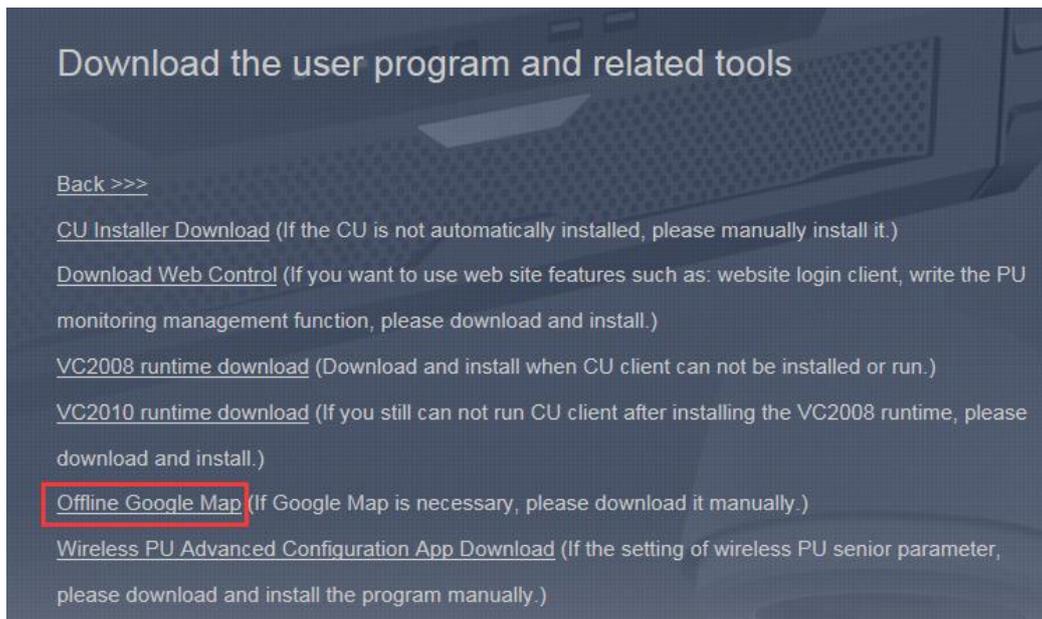
To download an offline Google map:

1. Download the Google map download tool (**KdGoogleMapDown.exe**).

- 1) Click **More** on the PMC login interface, as shown in the following figure.



- 2) Click **Offline Google Map**, as shown in the following figure.



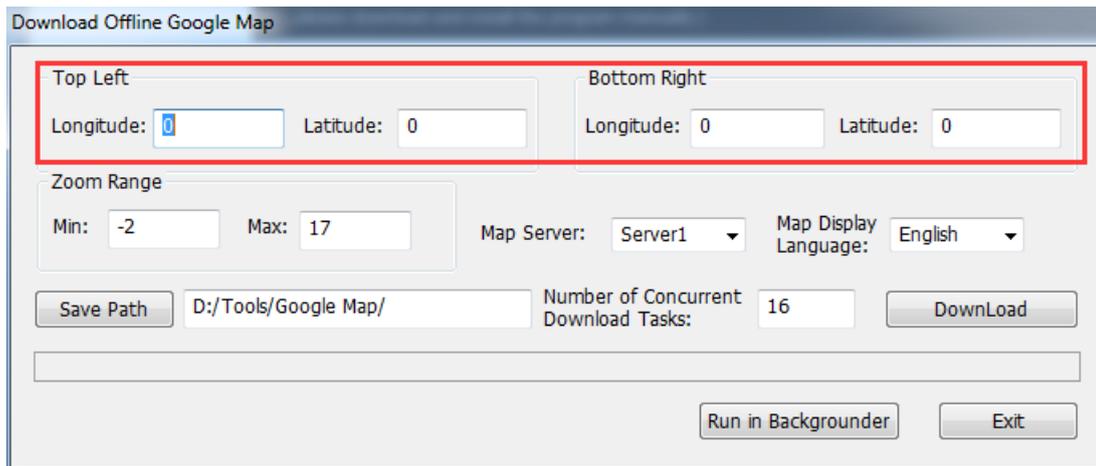
- 3) Save the **KdGoogleMapDown.exe** to your personal computer (PC), as shown in the following figure.



2. Run the **KdGoogleMapDown.exe**.

3. Create a download task.

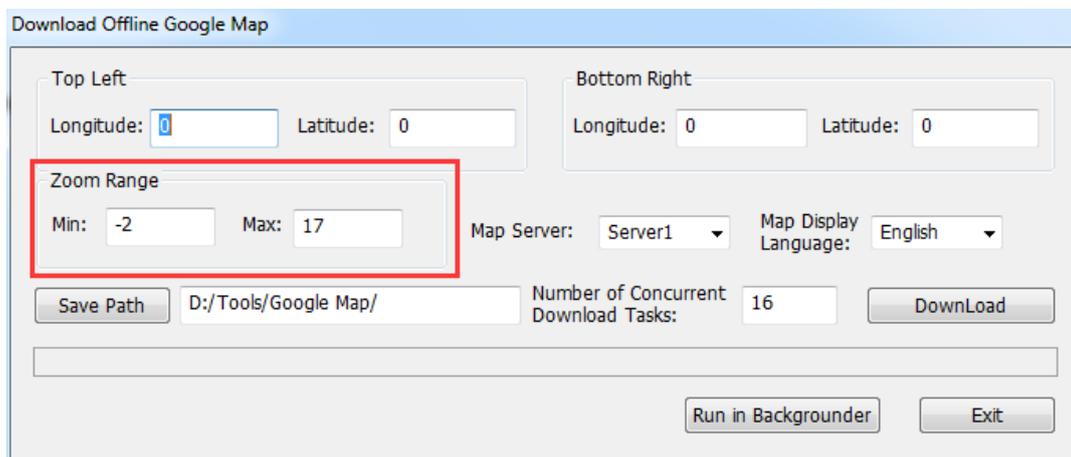
- 1) Configure the longitudes and latitudes.



When configuring these parameters, you can visit <http://www.gpsspg.com/maps.htm> for help.

Note that a large map will take a long period of time to be downloaded.

- 2) Configure the zoom range.



Note that if the minimum zoom range is very low, it will take a long period of time to download a map. You are advised to use a level of 6-17 to download a panoramic map and a level of -2-5 to download a detailed map.

- 3) Configure the other parameters.

For the **Map Server** parameter, you are advised to use the default value. If the default value does not work, try other values.

For the **Number of Concurrent Download Tasks** parameter, the value range is from 4 to 16.

4. Click **Download**.

5. Find the **tiles** file in the save path and compress the file into **tiles.tar** using 7-Zip.

1.4.2 Uploading an Offline Google Map

You need to save the **tiles.tar** file into a directory of a HTTP server and enable the apache server of the VMS to access the directory before you can use an offline Google map.

To achieve the preceding:

1. Create a web folder in the application data partition configured in section 1.2 and upload the **tiles.tar** file to the folder using the following command.

```
#cd /opt/mysql/kdmdb/  
#mkdir web  
#cd web  
# rz (This is to upload the tiles.tar file.)
```

2. Uncompress the **tiles.tar** file using the following command.

```
# tar xvf tiles.tar.
```

3. Enable the apache server of the VMS to access the directory using the following command.

```
#ln-s/opt/mysql/kdmdb/web/tiles/opt/kdm/uls/apache/htdocs/emap/googlemap/tiles
```

1.5 Storing History GPS Tracks

When the GPS function is enabled, a camera will periodically report its location to the VMS. However, due to the limited VMS space, you need to mount disk arrays to save history GPS tracks.

To

1. Create a GPS track save path.

```
#mkdir /opt/mysql/kdmdb/db
```

2. Configure the preceding save path as the path for saving history GPS tracks and enable the **mps.ini** to use this save path.

```
# cd /opt/kdm/mps/conf  
# vi mps.ini (This is to modify the mps.ini file.)  
  
[gps]  
  
enable = 1 (This is to enable the function of saving GPS data.)  
  
DBIP = 127.0.0.1 (For local configuration, set DBIP to 127.0.0.1. Currently, remote database  
configuration is not supported.)  
  
DBPort = 3306 (This port is the open port of mysql.)
```

```
DBType = 2 (The value 1 indicates the database type sybase, 2 mysql, and 3 oracle.)
DBName = mps (The mps file saves GPS data. Before running this command, ensure that the mps
file is already created.)
DBUserName = root (A user name of the mps file.)
DBUserPassword = kdc (The password of the root user.)
DBConnMaxNum = 10
DBThreadNum = 8
DBStorePath = /opt/mysql/kdmdb/db (This is the GPS track save path.)
max_days = 30 (This is to clear excess GPS data. When over 30 days of GPS data is saved, the
system will clear excess GPS data.)
contraction_factor = 10 (The greater the contraction factor, the better the contraction performance.
You are advised to keep the value 10.)
```

3. Add the cleaning script (/opt/kdm/mps/daily_clean_data.sh) of the mps file to the daily task list of the system.

```
#vi /etc/crontab
0 0 *** root /opt/kdm/mps/daily_clean_data.sh (This is to enable the systme to clean data at 0:0
every day.)
```

4. Restart the mps file and enable the configuration to take effect.

```
# killall -9 mps (This is to forcibly stop the mps progress.)
```

1.6 Using the Google Map

Log in to the CU, choose **E-map > Google map >** , and configure the following.

Map Name: china

Source Get from platform
 Get from google map server

Zoom level: 12

Center longitude East Longitude ▼ 104.062500°

Center latitude North Latitude ▼ 34.741612°

Map Desc:

✓ OK ⓧ Cancel

After the preceding, you can use the Google map. For details, see *VMS User Guide*.

2.1 Introduction

When a main VMS fails to work properly or disconnects from the Internet, the N+1 hot backup feature allows the standby VMS of the main VMS to do the following:

- Import the backup files of the main VMS
- Apply the network configurations of the main VMS
- Process the services of the main VMS

When the main VMS restores or connects to the Internet again, this feature enables the main VMS to take its services back from the standby VMS. Then, the standby VMS no longer applies the network configurations of the main VMS or process the services of the main VMS.

Note that one standby VMS can work with 32 main VMSs.

For the KDM2801H-G2, when a main VMS uses its G-LAN0 as its service port:

- If the G-LAN0 port is working properly but the other network ports fail, the main VMS will continue work.
- If the G-LAN0 port fails but the other network ports are working properly, the standby VMS of the main VMS will take over the services of the service port and the services associated with the other functional network ports will be stopped.

For example, the G-LAN0 port (service port) of a main VMS fails and the G-LAN1 port (storage port) is working properly, the standby VMS will take over the services of the G-LAN0 port and storage services of the G-LAN1 port will be stopped.

2.2 Configuration

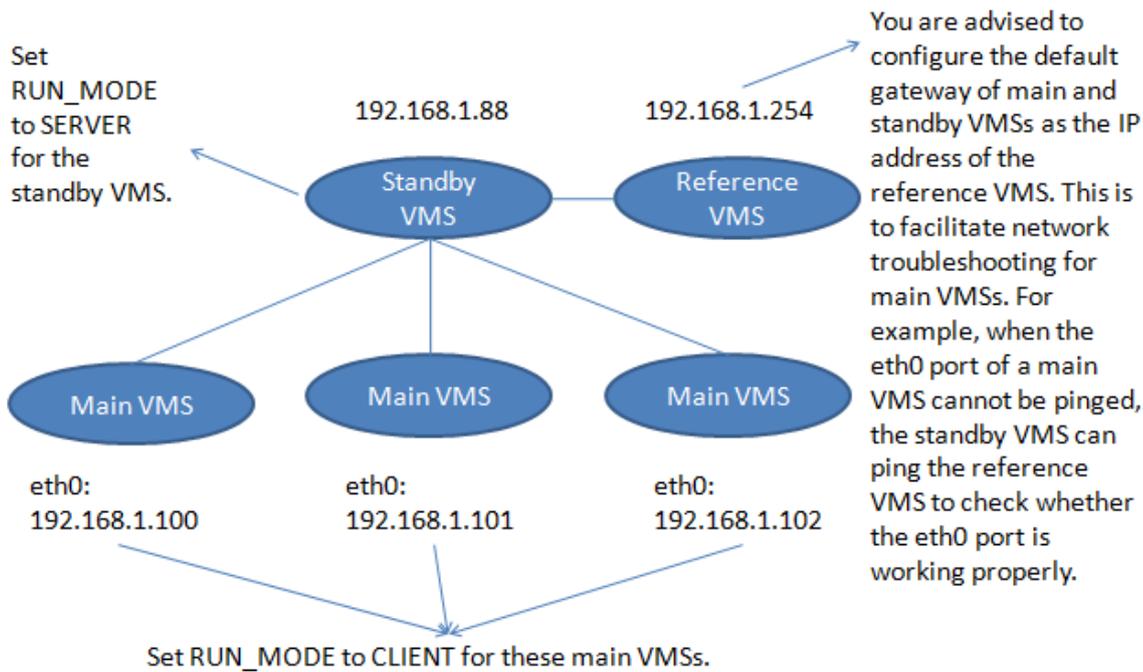


Note

If the storage directory of a main VMS is `/opt/kdm/cpconf` or its subdirectory, a USB flash drive must be inserted to the main VMS.

You must configure main VMSs and then standby VMSs and then verify configurations on the standby VMSs.

This section will configure main and standby VMSs in the way showed in the following figure.



2.2.1 Configuring a Main VMS

To configure a main VMS:

1. Log in to the main VMS using a Secure Shell (SSH) tool with a port of 2222.
2. Go to the `/opt/kdm/heartbeat/conf` directory and modify the `hbcfg.ini` file.

```
[common]
RUN_MODE = CLIENT (This is to set this VMS as a main VMS.)

[CLIENT]
HEARTBEAT_SERVER_IP=192.168.1.88 (This is the IP address of the standby VMS.)
```

3. Enable the heartbeat service.

For details, see section 2.3 "Enabling/Disabling the Heartbeat Service."

2.2.2 Configuring a Standby VMS

To configure a standby VMS:

1. Restore the factory defaults for the standby VMS.
2. Log in to the standby VMS using an SSH tool with a port of 2222.
3. Go to the `/opt/kdm/heartbeat/conf` directory and modify the `hbcfg.ini` file.

```
[common]
```

```
RUN_MODE = SERVER (This is to set this VMS as a standby VMS.)
```

```
[SERVER]
```

```
#Before the standby VMS processes the services of a main VMS, you must ensure that the standby VMS can ping the reference VMS.
```

```
REFERENCE _MACHINE_IP=192.168.1.254 (This is the default gateway of standby and main VMSs.)
```

```
#Assign an IP address to a main VMS as its idle IP address which will be used as a temporary IP address when the main VMS restores. (The idle IP address can be obtained after the main/standby relationship is established between the main and standby VMSs.)
```

```
(Assign an idle IP address to the main VMS and this IP address will be used as a temporary IP address for the service port when the main VMS restores. Configure the subnet mask and default gateway. Note that the default gateway should not be in use and complies with the network settings of the main VMS.)
```

```
HOST_IDLE_IP=192.168.1.99
```

```
HOST_IDLE_IP_MASK=255.255.255.0
```

```
HOST_IDLE_IP_GATEWAY=192.168.1.254
```

```
#Identify main VMSs in the form of " hostXip=<IP> " where X is a variable ranging from 0 to 31 and IP indicates the IP address of the eth0 port of each main VMS.
```

```
host0ip=192.168.1.100
```

```
host1ip=192.168.1.101
```

```
host2ip=192.168.1.102
```

```
#Assign a unique directory to each of the following paths and ensure that enough space is available in each directory. If SATA disks are installed, you can assign another directory, for example, /var/log/cpconf.
```

```
EXPORT_MIRROR_PATH=/opt/kdm/cpconf/export_dir (This is the directory to which mirror files are exported.)
```

```
IMPORT_MIRROR_PATH=/opt/kdm/cpconf/import_dir (This is the directory to which mirror files are imported.)
```

```
RECV_MIRROR_PATH=/opt/kdm/cpconf/recv_dir (This is the directory to which received mirror files are saved.)
```

```
MIRROR_SHORT_NAME=DevCfg.kcf
```

4. Enable the heartbeat service.

For details, see section 2.3 "Enabling/Disabling the Heartbeat Service."

5. Create a default mirror file.

A default mirror file must be created to ensure that a standby VMS can start running. The following is the command for creating such a mirror file using SecureCRT.

```
/opt/kdm/pms/exportdata.sh -f /(mirror file importing directory on the standby VMS)/(mirror file name) -with_snapshot
```

The following is an example.

```
/opt/kdm/pms/exportdata.sh -f /opt/kdm/cpconf/import_dir/DevCfg.kcf -with_snapshot
```



Note

Before running the preceding command, ensure that a mirror file importing directory is already created on the standby VMS.

2.2.3 Verifying Configurations

Verify the preceding configurations on the standby VMS using the following command.

```
telnet.sh hbs ✓ (Telnet to hbs and leave the user name and password blank.)  
heartbeat->hbstat  
InstID:1 --- State:backup, the HostID:192.168.1.100 (When the state is backup, the main/standby configuration is successful. When the state is not backup, you need to check host IP addresses configured in section 2.2.2. If these IP addresses are correct, check whether the value for HEARTBEAT_SERVER_IP of the main VMS is appropriate.)  
InstID:2 --- State:backup, the HostID:192.168.1.101  
...
```

2.3 Enabling/Disabling the Heartbeat Service

To enable the heartbeat service:

1. Log in to a main VMS from the port 2222 using an SSH tool.
2. Run the following command.

```
/bin/cp /opt/kdm/heartbeat/heartbeat.conf /etc/init/kedacom;/mount -n --move /etc/  
/var/lib/stateless/state/etc;/mount -oremount,rw /;/bin/cp -f -a  
/var/lib/stateless/state/etc/init/kedacom/heartbeat.conf /etc/init/kedacom/heartbeat.conf;/mount  
-oremount,ro /;/mount -n --move /var/lib/stateless/state/etc/ /etc;/initctl start kedacom/heartbeat
```

To disable the heartbeat service:

1. Log in to the main VMS from the port 2222 using an SSH tool.
2. Run the following command.

```
initctl stop kedacom/heartbeat;/bin/rm -rf /etc/init/kedacom/heartbeat.conf;mount -n --move /etc/  
/var/lib/stateless/state/etc/;mount -oremount,rw /;/bin/rm -rf /etc/init/kedacom/heartbeat.conf;mount  
-oremount,ro /;mount -n --move /var/lib/stateless/state/etc/ /etc/
```



Note

The heartbeat service is disabled by default.

2.4 Upgrading Main and Standby VMSs



Note

During an upgrade, do not make any changes to configurations of main and standby VMSs, for example, adding devices and deleting users.

To upgrade main VMSs and their standby VMS:

1. Log in to the PMC of the standby VMS.
2. On the **Status** tab page, check whether the value of **Main/Standby** is **Standby (not switched over)**.

If yes, go to the next step.

If not, enable the main VMS to start working.

3. Disable the heartbeat service.
4. Upgrade all main VMSs.
5. Upgrade the standby VMS.
 - 1) Log out from the PMC of the standby VMS.
 - 2) Go to **/opt/kdm/heartbeat/conf** and make changes to the **hbcfg.ini** file.

```
[COMMON]
```

```
RUN_MODE=CLIENT (This is to configure the VMS in operation to a main VMS.)
```

- 3) Log in to the PMC of the standby VMS to upgrade the standby VMS.

- 4) Go to **/opt/kdm/heartbeat/conf** and make changes to the **hbcfg.ini** file.

```
[COMMON]
```

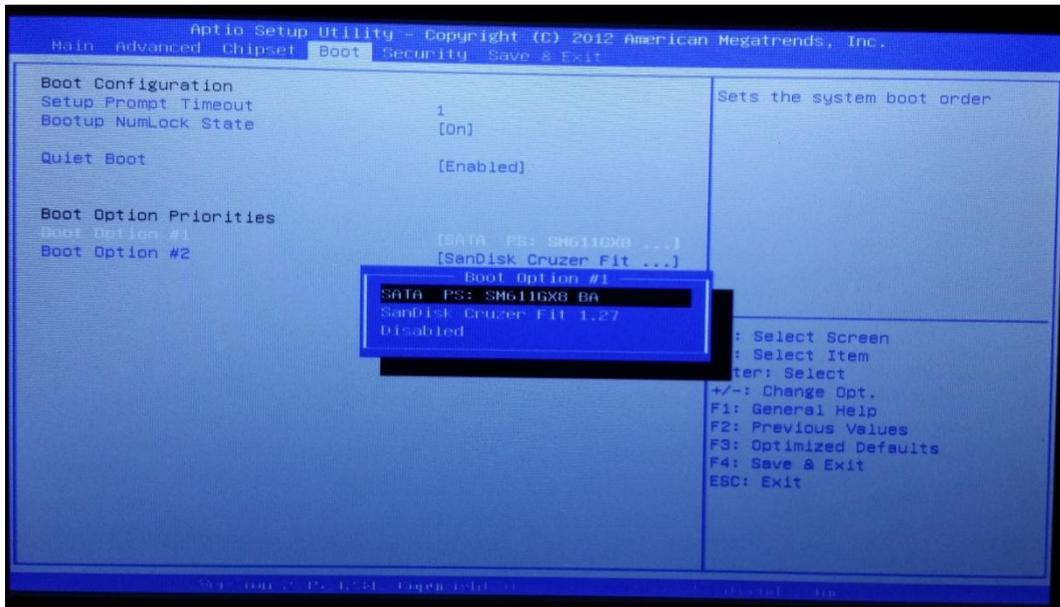
```
RUN_MODE=SERVER (This is to configure the VMS in operation to a standby VMS.)
```

- 5) Delete the previously received mirror file of the main VMS in the **/opt/kdm/cpconf/import_dir**.
- 6) Create a default mirror file again.
- 7) Enable the heartbeat service.

3 Restoration Using a USB Flash Drive

To restore a faulty VMS using a USB flash drive:

1. Connect a display and a keyboard to the faulty VMS.
2. Start the VMS and press the Home button.
3. In the BIOS Setup interface, set **SanDisk Cruzer...** to the first system boot order.
4. Log in to the system with the user name and password being root and kedacom.
5. Execute the restore command and following the instructions.
6. Press the Home button when a reboot notice is displayed.
7. In the BIOS Setup interface, set **SATA PS...** to the first system boot order.



8. Log in to the PMC to configure the following.
 - 1) Change the IP address of network ports.
 - 2) If software license files are used, reload these files. (Note that this step applies to only the KDM201-CMS-L1E.)

4 Authorized Inter-Domain Operation

When VMSs are cascaded, an upper-level VMS can give a lower- or same-level VMS authorization to perform specific operations on specific devices.

4.1 Single Device

To give a lower- or same-level VMS authorization to perform specific operations on a single device:

1. Check whether the upper-level VMS in operation supports authorized inter-domain operations.

```
[root@KEDACOM ~]# cd /opt/kdm/tas/dbscript/mysql/authorize
[root@KEDACOM authorize]# ll
-rw-r--r-- 1 root root 99 12月 9 15:05 1
-rwxr-xr-x 1 root root 3341 11月 28 16:57 authorize.sh
-rwxr-xr-x 1 root root 9251 12月 2 10:00 cancel.sh
drwxrwxrwx 2 root root 4096 12月 9 15:00 export-2014-12-09-150032
drwxrwxrwx 2 root root 4096 12月 9 15:04 export-2014-12-09-150415
-rwxr-xr-x 1 root root 5307 11月 25 16:28 export.sh
[root@KEDACOM authorize]#
```

2. Obtain the UUID of the device from the PMC or cmu.
3. Run the export.sh command on the upper-level VMS to export information about the device.

```
./ export.sh UUID (This is to export information about the device.)
sz /opt/kdm/tas/dbscript/mysql/authorize/export-2014-12-09-153243/data.tar (This is
to download the information.)
```

4. Upload the exported information (**data.tar**) to the lower- or same-level VMS.
5. Run the authorize.sh command on the lower- or same-level VMS to import the **data.tar**.

```
./authorize.sh data.tar
```

4.2 Multiple Devices

To give a lower- or same-level VMS authorization to perform specific operations on multiple devices:

1. Obtain the UUID of these devices from the PMC or cmu.

```
[root@KEDACOM authorize]# cat 1
f1a53291b5b8437d95128c6cee910005
f1a53291b5b8437d95128c6cee910006
f1a53291b5b8437d95128c6cee910007
[root@KEDACOM authorize]#
```

2. Run the `export.sh` command on the upper-level VMS to export information about these devices.

```
./ export.sh 1
```

3. Upload the exported information (**data.tar**) to the lower- or same-level VMS.
4. Run the `authorize.sh` command on the lower- or same-level VMS to import the **data.tar**.

```
./ authorize.sh data.tar
```

4.3 Cancelling Authorization

Run the following command on a lower- or same-level VMS to cancel authorization of a single device:

```
./cancle.sh UUID
```

Run the following command on a lower- or same-level VMS to cancel authorization of multiple devices:

```
./cancle.sh 1
```

5 External MSS Being Master VMS

- On the basis of built-in MSS, change it as external master VMS. Operation steps:
 1. Disable MSS module in PMC interface;
 2. Modify parameters;

```
vi /etc/httpd/conf.d/g900.conf
```

This is the built-in config file:

```
<IfModule rewrite_module>
    RewriteEngine on
    RewriteCond %{REQUEST_URI} ^.*bin/mssurl\.fcgi$ [NC]
    RewriteRule
^?(.*)$ http://%{SERVER_ADDR}:90/$1?server=%{SERVER_ADDR} [P]
</IfModule>
```

Modify it as follows:

```
<IfModule rewrite_module>
    RewriteEngine on
    RewriteCond %{REQUEST_URI} ^.*bin/mssurl\.fcgi$ [NC]
    RewriteRule ^?(.*)$ http://172.16.65.168/$1?server=%{SERVER_ADDR} [P]
</IfModule>
```

--172.16.65.168 is the IP of external MSS

3. Network with VMS 2.0. Please refer to *MSS User Manual* for detailed operations.

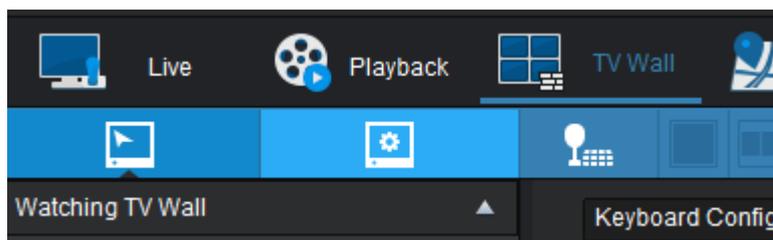
6 Keyboard Controlled Video Wall

The VMS can network with keyboard KB10 and can perform video wall control by the keyboard.

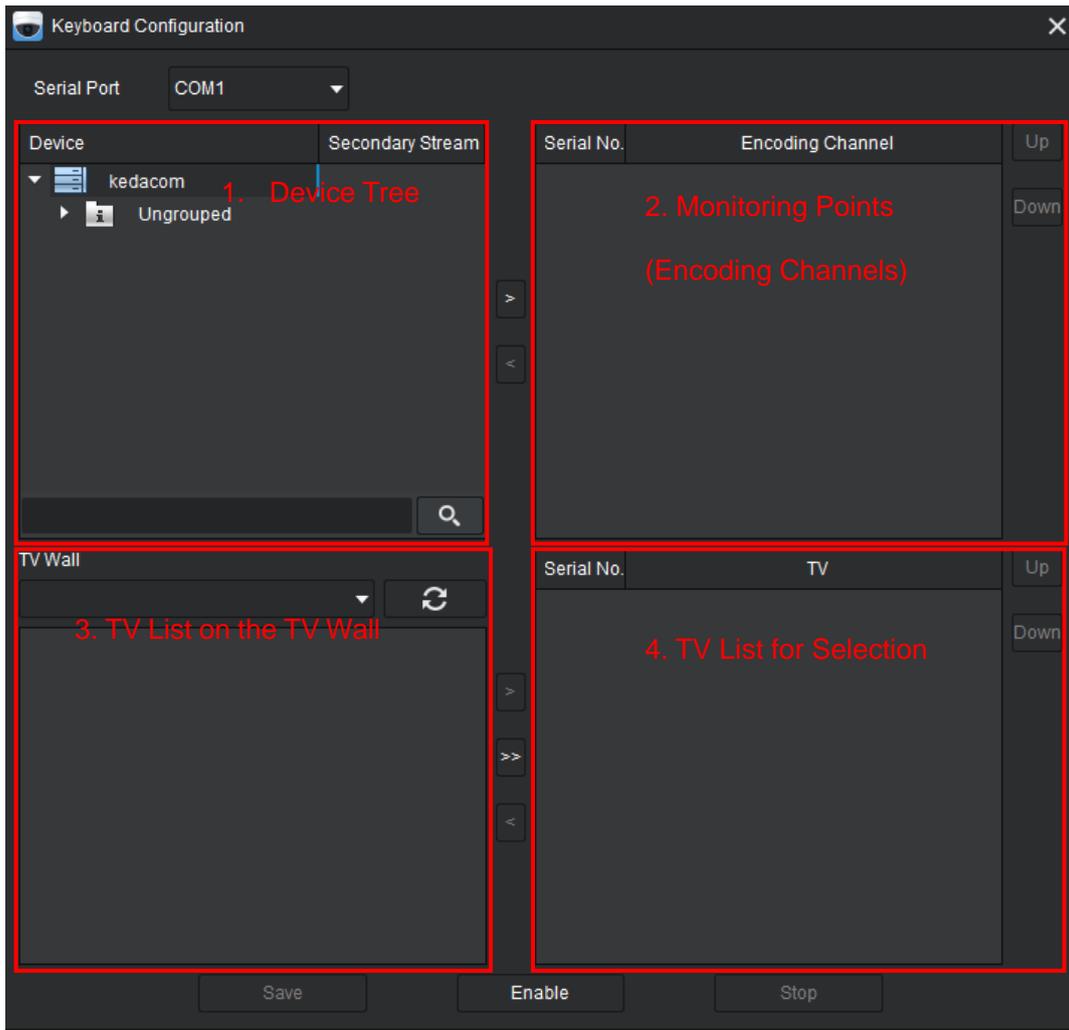
- Plugin install: put “kedasdk.dll” under CU installation menu (cu.exe file’s menu).
- Keyboard wiring: please refer to *KB10 Keyboard User Manual*.

6.1 Keyboard Configuration

1. Go to TV Wall interface in CU and click “**Keyboard Config**”;



2. Pop up a window of “**Keyboard Configuration**”:



Area 1 is Device Tree, Area 2 the monitoring points to be displayed on TV wall (encoding channel), Area 3 the TV list on the TV wall and Area 4 the TV list for selection.

3. According to actual serial port connection, select “**Serial Port**”;

 **Note:** The baud rate of KB10 is 9600 by default and can't be modified.

4. Click “**Save**”.

6.2 Keyboard Operations

6.2.1 Display on TV Wall

For example, display the image of channel 1 to TV 0 on the TV wall:

1. After configuring “**Keyboard Config**”, click “**Enable**” to enable keyboard functions and “**Stop**” to disable keyboard functions;
2. Press “**MODE**” on keyboard to switch to “TV Wall Control” mode;
3. Press “**MON**” > “**0**” > “**OK**” > “**CAM**”, “**1**” > “**OK**” on the keyboard to finish displaying on TV wall.

If the monitor need not be changed and the camera should be changed into 3, press “**CAM**” > “**3**” > “**OK**”.

Finally, the encoding channel “**CAM**” chooses is the current encoding channel and keyboard will perform PTZ operations on this encoding channel.

6.2.2 PTZ Operation by Keyboard

Keyboard functions:

Name	Function
MODE	Switch between NVR control mode and TV wall control mode
MON	In TV wall control mode, set TV No.
CAM	In TV wall control mode, set camera No.
FOCUS+	Focus in
FOCUS-	Focus out
ZOOM+	Zoom in
ZOOM-	Zoom out
BRIGHT+	Open aperture
BRIGHT-	Close aperture

Joystick functions:

Name	Function
UP	PTZ holder moves upward
DOWN	PTZ holder moves downward
LEFT	PTZ holder moves leftward
RIGHT	PTZ holder moves rightward
Turn Clockwise	Zoom in
Turn Anticlockwise	Zoom out
Turn Speed	Move speed of PTZ holder

7 Database Recording Recovery

When the database of VMS and disk array damages, use recrecover command to recover recordings. When the database of disk array damages, recrecover can run automatically and recover recordings. When the VMS database damages, need to configure manually and recover recordings. Operation steps:

1. Go to “/opt/kdm/nru”;
2. Run recrecover command, command format:

```
./startrecrecover.sh runMode recoverDb nruCfgPath [startTime endTime [initPath] ]
```

Rules for modifying parameters:

- runMode parameters and description

Parameter	Description	Remark
1	PartPlatRecover	Partial recover of VMS (need to specify period; the default is to recover recordings of specified period of all partitions. If only recover recordings of some partitions or menu, need to input initial menu.)
2	AllPlatRecover	Full recover of VMS (recover recordings of all partitions)
3	PartDiskAryRecover	Partial recover of array data (same as partial recover of VMS)
4	AllDiskAryRecover	Full recover of array data (same as full recover of VMS)
5	PartCloudRecover	Partial recover of cloud storage data (not supported currently)
6	AllCloudRecover	Full recover of cloud storage data (not supported currently)

 **Note:** Parameter “1” and “2”: mainly for iSCSI mode, recrecover runs on VMS;

parameter “3” and “4”: mainly for recrecover to run on array; parameter “5” and “6”: mainly for recrecover to run on cloud storage (not supported currently).

- recoverDb parameters and description

Parameter	Description	Remark
1	AllDb	All database
2	RmsDb	VMS database
3	NruDb	Array database

 **Note:** Select parameter according to actual database. “All database” is applicable only when recrecover runs on array and the array has database.

- Items in [] are optional:

If runMode is 2, 4 or 6, startTime, endTime and initPath need not to fill;

If runMode is 1, 3 or 5, startTime and endTime are compulsory but initPath is optional.

Example:

- recrecover recovers all disks database and VMS database on VMS:

```
./startrecrecover.sh 2 2 /opt/kdm/nru/conf
```

- recrecover recovers specific period recordings of all disks database and VMS database on VMS:

```
./startrecrecover.sh 1 2 /opt/kdm/nru/conf 20150314 20150316
```

8 Disable Punch and Anti-crossing Streams

Disable Punch function: when CU, VMS, array and front-end devices are in the same LAN and the videos need not to playback or view lively on internet, disable Punch.

Disable Anti-crossing Streams: after disabling this function, user can also view live videos (i.e. no crossing streams appear); if user cannot view live video after disabling this function, please contact the engineer. It doesn't have to be disabled by default.

Configuring method:

Go to the public configuration file “vi /etc/kdm/commonconfig.ini”, and add the following in the file:

```
--disable punch  
  
<punch>  
    <enable>0</enable>  
</punch>  
  
--disable anti-crossing streams  
  
<switch>  
    <enable>0</enable>  
</switch>
```

9 Abbreviations and Acronyms

PC	personal computer
SSL	Secure Shell
VMS	Video Management System