Video Manager 3.0

Quick Guide

Manual Version: P100-20140307
Zhejiang Uniview Technologies Co., Ltd.

Notice

The information in this manual is subject to change without notice. Every effort has been made in the preparation of this manual to ensure accuracy of the contents, but all statements, information, and recommendations in this manual do not constitute the warranty of any kind, express or implied.

Preface

Audience

This manual is intended for:

- Surveillance system planners
- Field technical support and servicing engineers
- Software installation, configuration, and servicing administrators
- Product users

Organization

The VM3.0 Video Manager Quick Start describes the features, software upgrade, software uninstallation, software reinstallation, and configuration of the VM3.0 Video Management Server (hereinafter referred to as VM3.0). Read this document carefully to help smoothly install VM3.0.

This manual is organized as follows:

1. **Overview.** Describes the functional characteristics and software specifications of VM3.0.
2. **VM3.0 Installation, Upgrade and Uninstallation.** Describes the software installation, upgrade and uninstallation of VM3.0.
3. **System Configuration.** Describes the basic configuration for VM3.0.

Contents

1 Overview

Video Manager 3.0 (VM3.0) is video management service software developed for a medium- and large-sized IP video surveillance system. It will be installed on hardware servers with the Linux operating system (OS).

VM3.0 is the core of service control and management for a video surveillance system. It implements service signaling exchange and scheduling, and manages information about devices and users in the entire system.

⚠ **WARNING!**

For details about the features and specifications of VM3.0, see the product brochure.

2 Installation, Upgrade and Uninstallation

⚠ **WARNING!**

Only professionals can install, upgrade, or uninstall VM3.0; otherwise, severe system faults or data loss may be caused. Contact authorized personnel of Uniview before you install, upgrade, or uninstall VM3.0.

System Requirements

Before installing VM3.0 on a server, ensure that Linux OS has been installed on the server.

Table 2-1 lists the system requirements of VM3.0 for the server.

Table 2-2 lists the system requirements of VM3.0 for the client.

Table 2-1 System requirements for the server

Item	System Requirements
OS	CentOS5.3, CentOS5.5, or CentOS6.X. For details, contact authorized personnel of Uniview.
CPU and operating frequency	4-core Intel Xeon, with dominant frequency no lower than 5410 2.33 GHz
Memory	2 * 2 GB, DDR2

Item	System Requirements
Network adapter	GE adapter card. One or multiple network adapters can be configured depending on actual requirements.
Hard disk	2 * 500 GB SATA or SAS hard disks Hard disk partitions of the OS: • Boot partition: at least 200 MB • Swap partition: at least the memory size • Dual-node hot standby partition: at least 40 GB • Root partition: remaining space
CD-ROM	DVD
Others	• A monitor and a keyboard are equipped to facilitate local maintenance. • There are various status LEDs, such as a power LED, an alarm LED, and a network adapter LED.

NOTE!

If the versions map to one another, VM3.0 can be installed together with DM3.0 and MS3.0 on a server. For details about version mapping, see the version mapping table released along with the version.

Table 2-2 System requirements for the client

Item	System Requirements
OS	Microsoft Windows XP SP2, Microsoft Windows XP SP3, or Microsoft Windows 7 Professional Edition. Microsoft Windows XP SP2 is recommended.
Software requirements	• Using Microsoft Internet Explorer 7.0 (or later versions) as the web browser is recommended, with a webpage zoom scale of 100%. • DirectX 9.0c (or later versions) has been installed.
CPU and operating frequency	Dual-Core Q9500 2.83GHz or higher is recommended. If the Pentium 4 CPU is used, the dominant frequency must be at least 2.8 GHz.
Memory	At least 1 GB. 2 GB or higher memory is recommended.
Hard disk	At least 40 GB. 160 GB or higher memory is recommended.
Display adapter	At least 128 MB. A mainstream NVIDIA GeForce 9800 GT 512 MB (or higher memory) is recommended. The hardware supports DirectX 9.0c. *Note: The display adapter must have the latest driver. A driver released after August 2009 is recommended.*
Audio adapter	Mandatory. *Note: The audio card must have the latest driver; otherwise, voice communication or broadcast may be unavailable.*

Item	System Requirements
Network adapter	100 Mbit/s (or higher) Ethernet adapter
Monitor resolution	1440 * 900 is recommended.

NOTE !

- A client meeting the above system requirement recommendation is able to simultaneously play 16 D1 video channels. To play more video channels, the client needs to have a CPU, memory, and display adapter with higher performance.
- Confirm that all acceleration functions are enabled on graphics hardware. Open the Control Panel on the client PC, and then view display attributes.

Preparations

Preconditions

- Before installing or upgrading the software, configure network parameters such as the IP address, subnet mask, and gateway address. For details, see section "Checking or Modifying the Configuration File".
- The server is well connected to the operating PC through the network.
- The SSH client has been installed on the client PC, and the client PC has logged into the server through the SSH client. For details, see section "Logging In to the Server Using the SSH Client". Do not close the SSH client during installation, upgrade, or uninstallation; otherwise, the operation might fail.
- Set the values of **Security Level** and **SELinux** to **Disabled** during firewall configuration. For details, see section "Configuring the Firewall".

Logging In to the Server Using the SSH Client

NOTE !

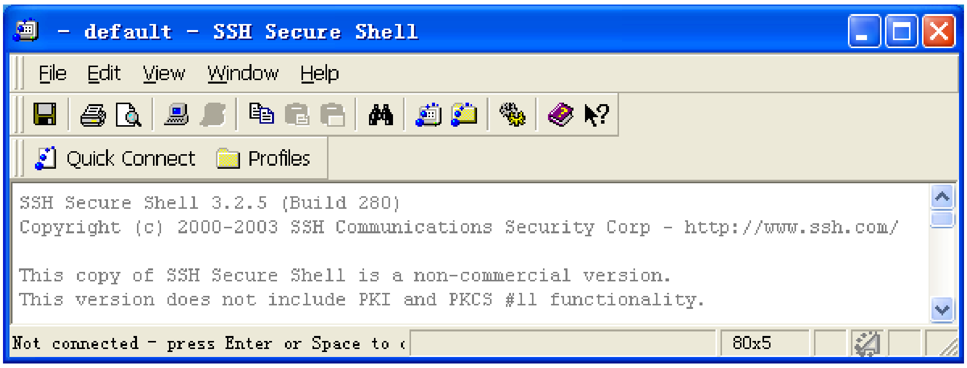
For the first login to the server using the SSH client, the username and password are those of the server OS. For details, contact server OS installation engineers. In this example, the username is root and the password is passwd.

After the SSH client is installed, shortcut icons SSH Secure Shell Client and SSH Secure File Transfer Client appear on the desktop.

To log in to the server through the SSH client, follow the steps below:

1. Double-click SSH Secure Shell Client to execute the application as shown in Figure 2-1.

Figure 2-1 SSH Secure Shell window

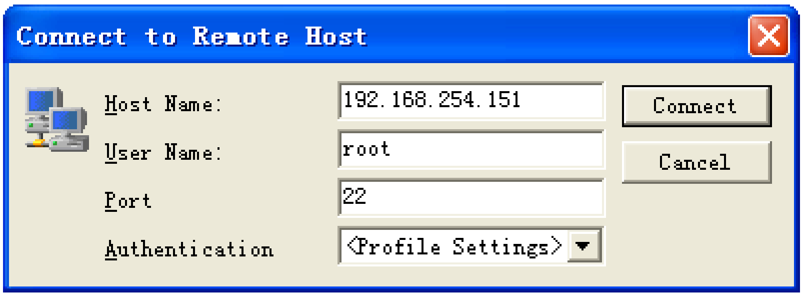


```
SSH Secure Shell 3.2.5 (Build 280)
Copyright (c) 2000-2003 SSH Communications Security Corp - http://www.ssh.com/

This copy of SSH Secure Shell is a non-commercial version.
This version does not include PKI and PKCS #11 functionality.
```

Not connected - press Enter or Space to c

2. Click Quick Connect. Input the IP address of VM3.0, login user name and port number, as shown in Figure 2-2. Then click Connect.

Figure 2-2 Connecting to the remote host



Host Name: 192.168.254.151

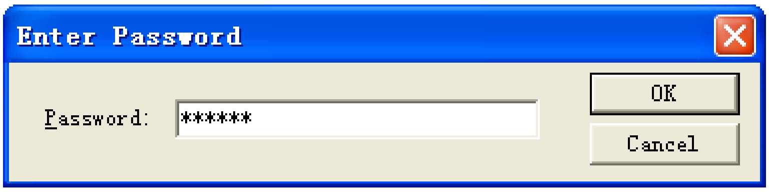
User Name: root

Port 22

Authentication <Profile Settings>

3. After connected, the server should require a password as shown in Figure 2-3. Input the password passwd, and then click OK to log in to the server where the software will be installed and access a command line interface (CLI).

Figure 2-3 Inputting your password



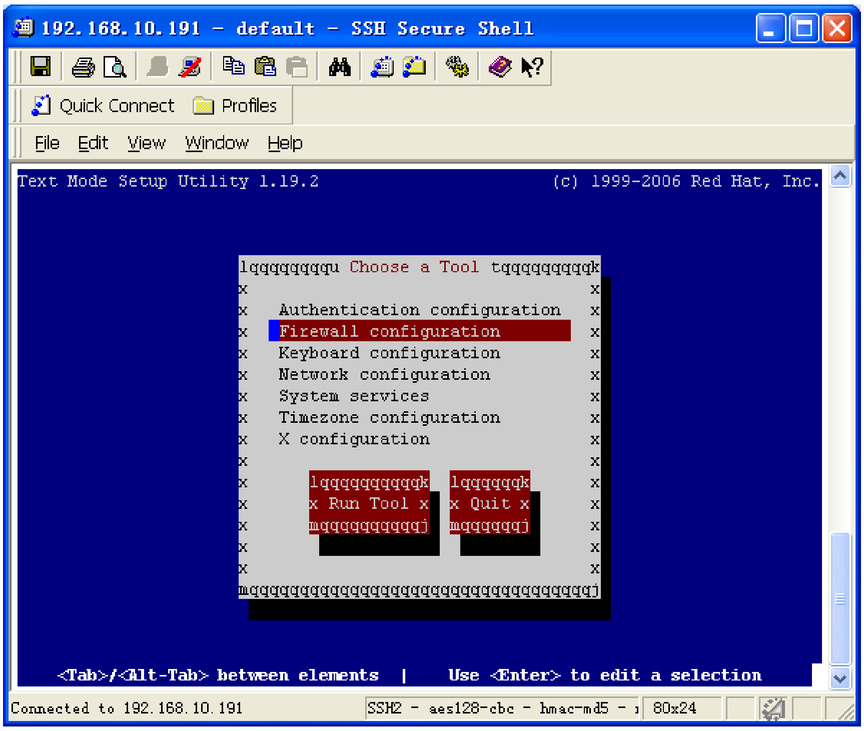
Password: ******

Configuring the Firewall

1. Log in to the server using the SSH client, and then input the setup command. A configuration window is displayed.

```
[root@vm ~]# setup
```

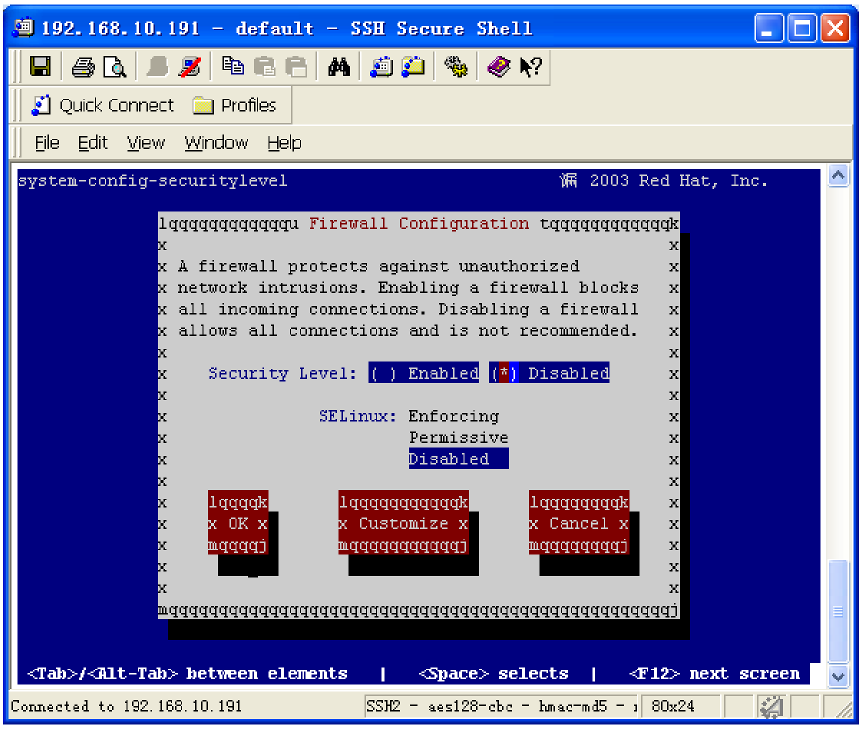
Figure 2-4 Configuration window


192.168.10.191 - default - SSH Secure Shell
Quick Connect
Profiles
File
Edit
View
Window
Help
Connected to 192.168.10.191
SSH2 - aes128-cbc - hmac-md5 - ı
80x24

```
Text Mode Setup Utility 1.19.2                     (c) 1999-2006 Red Hat, Inc.



                      lqqqqqqqqqu Choose a Tool tqqqqqqqqqk
                      x                                   x
                      x   Authentication configuration    x
                      x   Firewall configuration          x
                      x   Keyboard configuration          x
                      x   Network configuration           x
                      x   System services                 x
                      x   Timezone configuration          x
                      x   X configuration                 x
                      x                                   x
                      x      lqqqqqqqqqqk  lqqqqqqk       x
                      x      x Run Tool x  x Quit x       x
                      x      mqqqqqqqqqqj  mqqqqqqj       x
                      x                                   x
                      x                                   x
                      mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj




    <Tab>/<Alt-Tab> between elements   |   Use <Enter> to edit a selection
```

2. Select Firewall configuration, press Enter, and then set the values of Security Level and SELinux to Disabled.

Figure 2-5 Setting the values of Security Level and SELinux to Disabled


192.168.10.191 - default - SSH Secure Shell
Quick Connect
Profiles
File
Edit
View
Window
Help
Connected to 192.168.10.191
SSH2 - aes128-cbc - hmac-md5 - ı
80x24

```
system-config-securitylevel                      © 2003 Red Hat, Inc.

                    lqqqqqqqqqqqqqu Firewall Configuration tqqqqqqqqqqqqk
                    x                                                   x
                    x A firewall protects against unauthorized          x
                    x network intrusions. Enabling a firewall blocks    x
                    x all incoming connections. Disabling a firewall    x
                    x allows all connections and is not recommended.    x
                    x                                                   x
                    x     Security Level: ( ) Enabled (*) Disabled      x
                    x                                                   x
                    x                SELinux: Enforcing                 x
                    x                         Permissive                x
                    x                         Disabled                  x
                    x                                                   x
                    x     lqqqqk        lqqqqqqqqqqqqk     lqqqqqqqqqk  x
                    x     x OK x        x Customize x      x Cancel x   x
                    x     mqqqqj        mqqqqqqqqqqqqj     mqqqqqqqqqj  x
                    x                                                   x
                    x                                                   x
                    mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj

 <Tab>/<Alt-Tab> between elements   |   <Space> selects   |   <F12> next screen
```

3. Select OK, press Enter, and then select Quit to quit the configuration window.

Software Installation

To guarantee successful software installation, follow the steps below strictly:

1. Copy and decompress the software installation package.

2. Run the installation script.

Copying and Decompressing the Software Installation Package

Copy the software installation package to a directory such as **/root** in the current server OS by using the SSH client, and decompress the package. In this example, the IP address of the server is **192.168.254.151**, and the host name is **vm**.

The procedure is as follows:

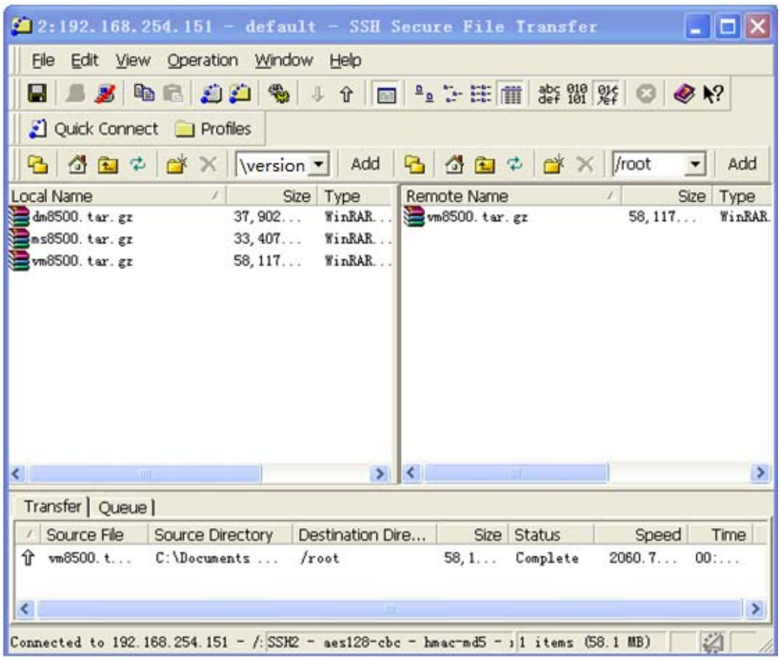
1. Log in to the server by using the SSH client, and then click . A window is displayed.

2. Select the directory where the software installation package resides on the left pane, and then drag the package to the /root directory on the right pane. The system copies the package to the server. Figure 2-6 shows the window after the package is successfully copied.

NOTE !

The work directory name must be in English.

Figure 2-6 Copying the software installation package to the server


2:192.168.254.151 - default - SSH Secure File Transfer
File Edit View Operation Window Help
Quick Connect
Profiles
\version
Add
/root
Add
Transfer
Queue

Local Name	Size	Type
dm8500.tar.gz	37,902...	WinRAR...
ms8500.tar.gz	33,407...	WinRAR...
vm8500.tar.gz	58,117...	WinRAR...

Remote Name	Size	Type
vm8500.tar.gz	58,117...	WinRAR.

Source File	Source Directory	Destination Dire...	Size	Status	Speed	Time
vm8500.t...	C:\Documents ...	/root	58,1...	Complete	2060.7...	00:...

Connected to 192.168.254.151 - /: SSH2 - aes128-cbc - hmac-md5 - ; 1 items (58.1 MB)

3. Access the directory where the software installation package resides, and run the tar command to decompress the package.

```
[root@vm ~]# tar zxvf vm8500.tar.gz
```

Files generated after decompression include installation, upgrade, and uninstallation scripts.

Running the Installation Script

NOTE !

- The standalone installation of VM3.0 is different from the HA installation of VM3.0. This section uses the standalone installation of VM3.0 as an example. For details about the HA installation of VM3.0, contact technical support engineers of Uniview.
- VM3.0 can be installed along with DM3.0, BM, and MS3.0 on a server. In that case, DM3.0, BM, and MS3.0 must register on the local VM3.0.
- If you want to install VM3.0 along with DM3.0, BM, and MS3.0 on a server, you must install VM3.0 first and then DM3.0/BM/MS3.0. In this case, some parameters of DM3.0/BM/MS3.0 will be automatically associated with the parameters of installed VM3.0. If DM3.0/BM/MS3.0 is already installed on the server, you must uninstall DM3.0/BM/MS3.0 before installing VM3.0.

Access the directory where the decompressed files are saved, and run the **source vminstall.sh** command to install the software. Below are related commands. The displayed information is an example only. The bold parts are parameter explanation.

```
[root@vm ~]# cd vm8500
[root@vm vm8500]# source vminstall.sh
2011-04-30 15:46:18 : Do not close the terminal during the installation; otherwise, unknown error might occur.
vm8500 installation begins...
Please choose the language of VM (default 0.Chinese): --- Select the language mode.
0.Chinese
1.English
Please input you choice:1
What version of VM do you want to install[default:1. stand-alone VM]: --- Select the standalone installation mode.
1. stand-alone
2. high ability (HA)
Please input your choice: 1
Please input Video Manager server port[default:5060]:  --- Set the VM3.0 port. Press Enter on the keyboard to select the default port.

Use default Server Port:5060
Please input SNMP port[default:162]: --- Set the SNMP service port. Press Enter on the keyboard to select the default port.

Use default Snmp Port:162
Please input Video Manager server IP address[such as 192.168.0.11]: --- Set the IP address of VM3.0. This IP address must be the IP address of a network adapter on this server.
192.168.254.151
start install database
Installing      pgsql
change installdir
change pgsqllog directory
change pgdata directory
Creating database
Creating table
Init database
Route initialization succeeded
Route initialization succeeded!
Flushing firewall rules:                                   [  OK  ]
Setting chains to policy ACCEPT: filter                    [  OK  ]
Unloading iptables modules:                                [  OK  ]
Begin to install vm8500 server ...
Begin to install rpm pdt_imos ...
Install rpm pdt_imos finished...
Install rpm pdt_imos succeeded
Begin to install rpm vm8500 ...
Install rpm vm8500 finished...
Install rpm vm8500 succeeded
lineofvmsys.conf:7 sedfileline:7
Install succeeded
Stopping crond:                                            [  OK  ]
Starting crond:                                            [  OK  ]
Creating mailbox file: File exists
Creating mailbox file: File exists
Shutting down vsftpd:                                      [  OK  ]
Starting vsftpd for vsftpd:                                [  OK  ]
Start vsftpd succeeded!!
setting ftp succeeded
Begin to start vm8500 server ...
Pgsql           already started
Starting IMGSERVER services: starting img
CImfLogTask: logNumber = IMFMaxLogNumber 2
CImfLogTask: logSize = IMFMaxLogSize 1048576
CImfLogTask: logPath = IMFLogPath /var/log
start ok 0

Start img succeeded
Starting MCSERVER services: starting mcserver
CImfLogTask: logNumber = IMFMaxLogNumber 2
CImfLogTask: logSize = IMFMaxLogSize 1048576
CImfLogTask: logPath = IMFLogPath /var/log
start ok 0

Start mcserver succeeded
Starting VMSERVER services: starting vmserver
start ok 0

CImfLogTask: logNumber = IMFMaxLogNumber 2
CImfLogTask: logSize = IMFMaxLogSize 1048576
CImfLogTask: logPath = IMFLogPath /var/log
Start vmserver succeeded
Starting ADAPTERSERVER services: starting adapter
/
start ok 0

CImfLogTask: logNumber = IMFMaxLogNumber 2
CImfLogTask: logSize = IMFMaxLogSize 1048576
CImfLogTask: logPath = IMFLogPath /var/log
Start adapter succeeded
Starting HTTPSERVER services: starting apachectl
/usr/local/vmwww/apache/bin/apachectl start: httpd started
start ok 0

Starting SGSERVER services: starting sgserver
```

```
start ok 0

CImfLogTask: logNumber = IMFMaxLogNumber 2
CImfLogTask: logSize = IMFMaxLogSize 1048576
CImfLogTask: logPath = IMFLogPath /var/log
Start sgserver succeeded
Start vmdaemon succeeded
Start servers succeeded
Install vm8500 succeeded
```

After the installation is complete, VM3.0 services automatically start. Run the **vmserver.sh status** command to check the service status. For details, see section "Operating VM3.0 Services".

Software Upgrade

NOTE !

- Only professionals can upgrade VM3.0; otherwise, severe system faults or data loss may be caused. Contact authorized personnel of UNIVIEW before you upgrade VM3.0.
- If VM3.0 is installed along with DM3.0/BM/MS3.0 on the same server, you must stop the services of DM3.0/BM/MS3.0 and then upgrade VM3.0 and DM3.0/BM/MS3.0 in sequence.

To upgrade VM3.0, follow the steps below:

1. Copy the upgrade package to a work directory in the current server OS. For details, see section "Copying and Decompressing the Software Installation Package".
2. Access the directory where decompressed files are saved, and then run the sh vmupdate.sh command. Finish the software upgrade according to system prompts. Below are related operation commands:

```
[root@vm ~]# cd vm8500
[root@vm vm8500~]# sh vmupdate.sh
```

Software Uninstallation

WARNING!

All data related to the software will be deleted after you uninstall the software. Therefore, back up data and contact authorized personnel of Uniview before uninstalling the software.

1. Log in to VM3.0 using the SSH client.
2. Access the directory where decompressed files are saved, and then run the sh vmuninstall.sh command. Finish VM3.0 software uninstallation according to system prompts.

```
[root@vm ~]# cd vm8500
[root@vm vm8500]# sh vmuninstall.sh
```

3 System Configuration

⚠ **WARNING!**

Only professionals can configure VM3.0; otherwise, severe system faults or data loss may be caused. Contact authorized personnel of Uniview before you configure VM3.0.

Configuration Tasks

Table 3-1 Configuration tasks

Configuration Task		Description
Command line configuration	Checking or Modifying the Configuration File	Check or modify the configuration file of VM3.0.
	Checking or Setting the System Time	Check or set the time zone, time, and date of VM3.0.
	Operating VM3.0 Services	Check the service status, and start, stop, or restart VM3.0 services.
	Checking System Logs	Check system logs.
	Checking the System Version	Check system version information.
	Configuring Automatic Database Backup	Start or stop automatic database backup.
Web configuration	Logging in to VM3.0 Through Web	Log in and log out through web.
	Patch Upgrade	Deploy and upgrade patches.
	License Management	Apply for and register a license.
	Logging In to the Customization Interface	Log in to the customization interface to perform system customization.

Checking or Modifying the Configuration File

Checking the configuration file

Run the following command to check parameter settings in the system:

```
[root@vm ~]# vmcfgtool.sh -q
```

```
DeviceID=iccsid
SnmpPort=162
SipPort=5060
ServerIP=192.168.254.151
DBBKUP_SWITCH=on
DBType=PostgreSQL
DBServerName=192.168.254.151:5432:imos
DBUserName=postgres
DBPassword=******
```

DBBKUP_SWITCH=on indicates that automatic database backup is enabled in the system. By default, automatic database backup is enabled.

Modifying the configuration file

When the network has changed or certain parameters need to be modified, run the corresponding script to modify parameter information. Below is the command for modifying the configuration file. The bold part indicates parameter explanation.

- Run the following command to modify the IP address of VM3.0:

```
[root@vm ~]# vmcfgtool.sh serverip 192.168.254.155 --- 192.168.254.155 is the new IP address of VM3.0.
```

CAUTION!

- The IP address of VM3.0 must be the IP address of a network adapter on VM3.0; otherwise, services will be unavailable.
- Do not modify the default device ID of VM3.0; otherwise, services may be affected.

- Modify Apache port numbers:

NOTE!

You need to modify the port number only when the default port number is already being used.

Run the following command to modify the Apache port number of VM3.0:

```
[root@vm ~]# vmcfgtool.sh namehost 890--- 890 is the new port number of VM3.0
```

You can also run the **vmcfgtool.sh –help** command to obtain more commands for modifying parameters. After modifying configuration information, you need to run the **vmserver.sh restart** command to restart the services for configuration changes to take effect.

Checking or Setting the System Time

Except for the VM3.0 client PC, the DM, MS, storage devices, and encoders/decoders will automatically synchronize their time zone and time to VM3.0. It is recommended that the time zone and time settings on the VM3.0 client PC be consistent with those on VM3.0.

Checking the Time and Date of the Local Time Zone

```
[root@vm ~]# date
Thu Aug 16 08:57:21 GMT-8 2009
```

NOTE!

In the Linux OS, GMT-N indicates an eastern time zone and GMT+N indicates a western time zone. In this example, GMT-8 indicates eastern time zone 8.

Setting the Time Zone

```
[root@vm ~]# timeconfig
```

After the command is executed, the system displays a window for selecting the time zone. Select a time zone (such as Asia/Shanghai), press the Tab key to select the OK button, and then press Enter to finish the setting.

Setting the System Time and Date

```
[root@vm ~]# date -s “2011-04-16 16:57:40”
Thu Apr 16 16:57:40 cst 2009
```

It is recommended that the RTC hardware time should be synchronized after you change the system time by using the date command. If you do not perform RTC hardware time synchronization, the clock may be asynchronous when the server obtains time upon restart following power interruption. You can run the hwclock–systohc command to synchronize the RTC hardware time with the system time.

```
[root@vm ~]# hwclock –-systohc
```

Run the following command to check whether the date and time after modification are correct:

```
[root@vm ~]# clock;date
```

Operating VM3.0 Services

Checking the Service Status

```
[root@vm ~]# vmserver.sh status
Pgsql           is      running
Img is running
Mcserver is running
Vmserver is running
Adapter is running
Sgserver is running
serversnmpd is running
DiskReadOnlyCheck is running
Vmdaemon is running
```

The service status is either **running** (indicating that the respective service is running) or **stopped** (indicating that the respective service has been stopped).

If the status of a process as shown above is **stopped**, you need to manually restart the service. For details, see section "Restarting the Services".

If an executable file on the server is deleted or its executable permission is modified, a message "does not exist" will be displayed, indicating that this service does not exist. In that case, you need to reinstall the software or contact authorized personnel of Uniview for a solution, so that services can be normally running.

Starting the Services

After the installation, VM3.0 services automatically start with the system startup. You can also manually start the services.

To start the services, run the following command:

```
[root@vm ~]# vmserver.sh start
```

Stopping the Services

You can manually stop the services as required.

To stop the services, run the following command:

```
[root@vm ~]# vmserver.sh stop
```

Restarting the Services

You can manually restart the services as required.

CAUTION!

Restarting the database service may cause system exceptions. If you want to restart the database service, contact authorized personnel of Uniview.

To restart the services, run the following command:

```
[root@vm ~]# vmserver.sh restart
```

Checking System Logs

System logs are saved in the /var/log directory. To view logs in a log file, run the ls command to find the log file and then run the tail command.

```
[root@vm ~]# cd /var/log
[root@vm log]# ls
abc                       imf_msserver_0.log      piranha
abc.cap                   imf_msserver_1.log      pm
acpid                     imf_ns_0.log            p.pcap
adapter_product00.log     imf_ns_1.log            ppp
adapter_product01.log     imf_SDK_0.log           prelink
```

```
...
[root@ vm ~]# tail adapter_product00.log
```

Checking the System Version

Run the following command to check system version information:

```
[root@vm ~]# vmcfgtool.sh –v
Interior version : VM8500V300R001B02D001SP25
Exterior version : VM8500-IMOS110-B3111P25
BUILDTIME        : 2011-04-25 05:46
The actual system version information may differ.
```

Configuring Automatic Database Backup

If you need to back up the system database, you can enable the automatic database backup function, so that the system will start to automatically back up the database at 03:00 every day.

Run the following command to enable the automatic database backup function:

```
[root@vm ~]# vmcfgtool.sh autodbbackup on
```

Run the following command to disable the automatic database backup function:

```
[root@vm ~]# vmcfgtool.sh autodbbackup off
```

NOTE !

- After the database backup is complete, a database backup file will be saved in the /var/autobackup/ directory and named in the format of database-Time.tar.gz. For example, database-2010-04-19_0300.tar.gz is a backup file generated in 03:00 on April 19, 2010.
- By default, the system keeps only the backup files of the last seven days. It is recommended that you copy the database backup file to a local disk each time you back up the database.

Logging in to VM3.0 Through Web

Before logging in to VM3.0 through web, ensure that the client PC satisfies system requirements described in Table 2-2.

Login

NOTE!

- To guarantee normal use of ActiveX, it is recommended that you add the IP address of VM3.0 to a list of trusted sites on the Internet Explorer (by choosing Tools > Internet Options > Security) before logging in to the webpage.
- There are two default users in the system: admin (the password is admin) and loadmin (the password is loadmin). For the first login to the webpage, use the admin or loadmin user as required. For details about differences between the two users, see Table 3-2.
- Before performing system configuration, you must apply for and register a license so that you obtain a permit to device management and the number of devices that can be managed. For details, see section "License Management".

Table 3-2 Differences between the admin user and the loadmin user

User Item	**admin**	**loadmin**
Organization	System super administrator, who has the highest permission in the system.	Local domain administrator, who has all permissions in the local domain.
Differences in permissions	• Only the **admin** user is entitled to upgrade and manage the system, manage other domains, and backup the system. • None of users in the system can modify or delete the **admin** user.	• The **loadmin** user is not entitled to upgrade and manage the system, manage other domains, and backup the system. • Users with related permissions can modify or delete the **loadmin** user.
Login from multiple points	Not supported	Supported

To log in to VM3.0 through web, follow the steps below:

1. Open the web browser on the client PC, and input the IP address of VM3.0 in the address box. If it is the first login, load all latest ActiveXs according to system prompts till no message appears on the login page asking you to load ActiveXs. When installing ActiveX, ensure as much as possible that ActiveXs is installed in the default installation directory.
2. Input the username and password in the login dialog box, and then click Login. A webpage is displayed.

NOTE !

- If you select Remember password, you do not need to input the password again upon next login. Instead, you will directly access the webpage after clicking Login.
- If you change to another OS user on the client to log in to the webpage again after ActiveXs are successfully installed, you can click Video play ActiveXs at the bottom of the page to manually load the installed ActiveXs. If you do not do it, you may fail to log in to the webpage.

After successfully logging in to the webpage, you can manage and operate the entire system. For details, see *VM3.0 Online Help*.

Exit

Click **Exit** at the upper right corner of the page, and then **Yes** to exit the webpage.

Patch Upgrade

Patch Overview

The client player, client ActiveX, and other modules must be periodically patched to expand functions or correct errors.

The administrator needs to deploy a patch package on the server in advance. Users can automatically download and install patches after logging in to VM3.0 through web.

Precautions

- Ensure that the server where the patch package resides and the client are normally connected through the network.
- It is recommended that the patch package be deployed on VM3.0.

Operation Steps

In this example, the patch package is deployed on VM3.0.

Deploying patches on the patch server

Log in to VM3.0 by using the SSH client, and upload the initial patch package to the root directory on VM3.0.

NOTE !

Select the correct patch package and upload it. This section uses the client_zhejiang.tar.gz package as an example.

```
[root@vm ~]# cd /root
[root@vm ~]# ll
-rw-r--r-- 1 root root  46724620 02-13 13:50 client_zhejiang.tar.gz
```

Decompress the patch package. The directory where decompressed files are saved will contain initial patch installation and uninstallation scripts.

```
[root@vm ~]# tar zxvf client_zhejiang.tar.gz
```

Access the directory where decompressed files are saved, and then run the **source clientinstall.sh** command to initially install the patches.

```
[root@vm ~]# cd client_zhejiang
[root@vm client_zhejiang]# source clientinstall.sh
```

If the patches are already deployed on the server during installation, a prompt is displayed, asking you whether to uninstall the existing patches before installation. Select **yes**, and then press **Enter**.

```
Client Patch has been installed ,do you want to uninstall it first?[yes/no]:yes
```

After the script is executed, patch deployment is finished on the server. If you log in to the webpage from a client PC, a prompt will be displayed, asking you whether to update patches.

Updating patches on the patch server

NOTE!

If a new patch exists, you need to upload it to the patch server.

Log in to VM3.0 by using the SSH client, and access the directory where patches are saved.

```
[root@vm ~]# cd /mnt/syncdata/imos/client_patchs/
[root@vm client_patchs]# ls
client_patch.zip  spversion.xml
```

Upload the patch package in zip format to the patch directory.

Edit the **spversion.xml** file. Add related settings for the new patches.

NOTE!

The spversion.xml file describes information about patches already existing on the current server. When adding a patch, you need to manually add settings for the new patch.

```
[root@ vm client_patchs]# vi spversion.xml
<?xml version='1.0'?>
<patchs count='1'>
<item>
<name>hik_decoder</name>
<filename>xp_hik_file.zip</filename>
<version>1.0</version>
<describe>hik</describe>
<order>1</order>
</item>
<item>---- Set parameters for the new patch.
<name>activeX</name>---- Set the patch name, which must be unique in the system.
<filename>activeX.zip</filename>---- Set the name of the patch package in zip format.
```

```
<version>1.1</version>---- Set the patch version number. If it is a new patch, setting the
patch version number to 1.0 is recommended. If it is not a new patch, set the patch version
number to an incremented number against the existing version number.
<describe>activeX patch.</describe>---- Set the patch description.
<order>2</order>---- Set the installation sequence to 2, so that this patch will be installed
after the last patch is installed.
</item>
</patchs>
```

Modifying or checking the IP address of the patch server

If the IP address of the patch server has changed, run the corresponding script to modify the IP address of the patch server. Below are related commands.

Run the following command to modify the IP address of the patch server:

```
[root@vm vm8500]# vmcfgtool.sh patchservip 192.168.90.245 ---- 192.168.90.245 is the new IP
address.
Run the following command to check modification results:
[root@vm vm8500]# cat /usr/local/svconfig/vmconf/patchserver.ini
[PatchServer]
PatchFtpServerAddr=192.168.90.245
PatchFtpServerPort=21
PatchFtpUserName=downloadusr
PatchFtpUserPasswd=h3ckey
```

Downloading and installing patches on the client

If there are new patches after you log in to VM3.0 through web, a dialog box is displayed, indicating that some patches need to be updated.

1. Click OK. A patch installation dialog box is displayed.

NOTE !

The patch installation dialog box shows the IP address of the patch server, the current VM version, and the installation path of ActiveXs.

2. Click Install to install the new patches.

License Management

A license file defines devices that can be managed in the system and resource authorization information.

According to factory settings, the system supports only eight cameras, one DM, one MS, and one storage device. To manage more devices and resources, you need to purchase a product license. Submit a license activation request to us by providing a license authorization code and detailed user information to activate the license. Then import the license file to the system to finish license registration. When the existing license expires, you also need to apply for a new license and register it again.

NOTE!

License management operations are subject to the online help of the latest software version.

Submitting a request to activate a standalone license

1. On the web login page, click License Management. The License Management page is displayed. If you have already logged in to the system through web, click System Configuration > License Management. The License Management page is displayed.
2. Input information about the license applicant and the contact person, and specify a local path where the license application file (host file) will be saved.
3. Click Generate Host File. A prompt is displayed, indicating that a license application file (hostid.id) has been successfully generated.
4. Log in to the official website of Uniview [Service /Product Licensing] to submit a request for license activation.

Step 1: On the **License Service** page, click **Initial License Activation Request** or **License Expansion Activation Request** according to system prompts. The **License Activation** page is displayed. In this example, you submit a request for initial license activation. The license activation request in the case of license expansion is similar.

Step 2: Select the product type. Upload the application file generated in (3).

Step 3: After you successfully upload the license application file, input the correct authorization code (obtained from the software authorization document) and customer information, and then click **Obtain Activation Code (File)**. For customer information, you need to input your email address if you hope to obtain the license activation file through an email.

Step 4: If the submitted information is correct, the system generates a license activation file and returns a page indicating that the operation is successful. You can click a license activation file link on this page to directly download the license activation file, or obtain the license activation file from your mailbox specified in the customer information as described above.

After decompressing the license activation file to obtain a license file (***.lic**), import the license file to the system to finish license registration.

Importing the license file

1. Open the License Management page.
2. Click Browse in the Import license file area, and import the obtained license file.
3. Click Import, and then confirm the import for the license file to take effect. It is recommended that you restart the system according to system prompts, so that system services are running normally under license control.

Logging In to the Customization Interface

The system supports customization, so that you can modify system information such as the system name, background color, and logos after logging in to the system customization page.

To log in to the system customization page, follow the steps below:

1. Open the web browser on the client PC, input the IP address (plus "/config.php") of VM3.0 such as http://192.168.20.16/config.php in the address box, and then press Enter.
2. Input the password (**admin** by default) in the login dialog box, and then click **OK**. The system customization page is displayed.