Dräger

Installation Instructions

Vista CMS

WARNING
To properly use this medical device, read and comply with these instructions for use.

Vista CMS
Software 2.n

Contents

This page intentionally left blank

Terms and definitions

Terms	Definitions	Descriptions
Vista CMS 2.0	Central Monitoring System V2.0	**Vista CMS** includes two components, **Central Server** and **CMSClient**.
Vista CMS 1.0	Central Monitoring System V1.0	/
Central Server	Server side of Vista CMS 2.0	/
CMSClient	Client side of Vista CMS 2.0	/
PostgreSQL	The database management software used by Vista CMS 2.0	**1** After installation of Central Server component, two databases cmsdb_common and cmsdb_reality will be created in PostgreSQL. **2** Due to the differences in the installation environment, after the software is installed, there may be two names displayed, **postgresql-x64-10** and **postgresql-10**. Both are the same software.
Common Library	Database cmsdb_common	**1** Common library stores the non-monitoring data. When using the distributed mode of Vista CMS 2.0, all Central Servers need to use the Common library under the same IP. The Common library under this IP is **Main Common library**. **2** **Configuration database** in this installation instruction is **Common library**. **3** Monitoring data are stored in cmsdb_reality which named **reality library** in this installation instruction.
Distributed CMS	Distributed central monitoring system that Multiple Central Servers are networked to each other	**1** If each Central Server connects to Common Library on its own computer, it is called standalone version. **2** If multiple Central Servers connect to the same Common library, those Central Servers are called Distributed CMS.

CMP	Communication protocol between Vista CMS 2.0 and monitoring device	For older version of protocol, it is more common in V1.0 or V1.1.
Main Central Server	Main Central Server in Common library that connects all Central Servers	/
Public network	It is used to connect with local or metropolitan area networks in different area, and is a remote network for computer communication.	Alias: WAN, outside net.
The gateway software	Vista gateway software	/

Setup of your computer

Overview

Vista CMS 2.0 includes following applications:

- Stand-alone. This application is the same as Vista CMS 1.0 as shown in Figure 1.1.

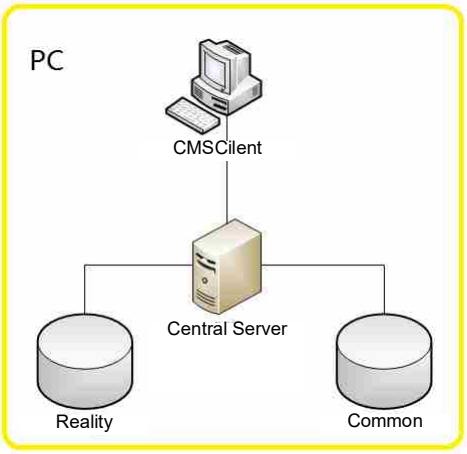


Figure 1.1

- Single Central Server - multiple clients. This application is basically consistent with Vista CMS 2.0 as shown in Figure 1.2. Multiple clients are supported based on Vista CMS 2.0. In the deployment, Central Server and CMSClient should be deployed on one computer, and other CMSClients can be separately deployed on other computers.

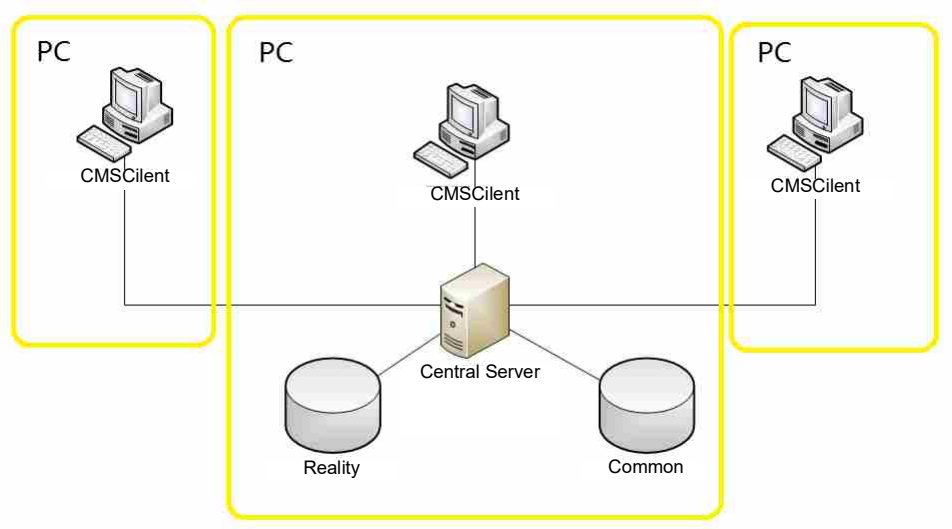


Figure 1.2

- Multiple Central Servers - multiple clients. This application is the Distributed CMS as shown in Figure 1.3. The Central Server and CMSClient should be deployed on multiple computers, and the configuration database for all Central Servers should be set to the IP address of the computer where Main Common is installed. Refer to Figure 2.8 for settings. If needed, refer to Chapter *Environment Deployment Inspection of Distributed CMS* for inspection.

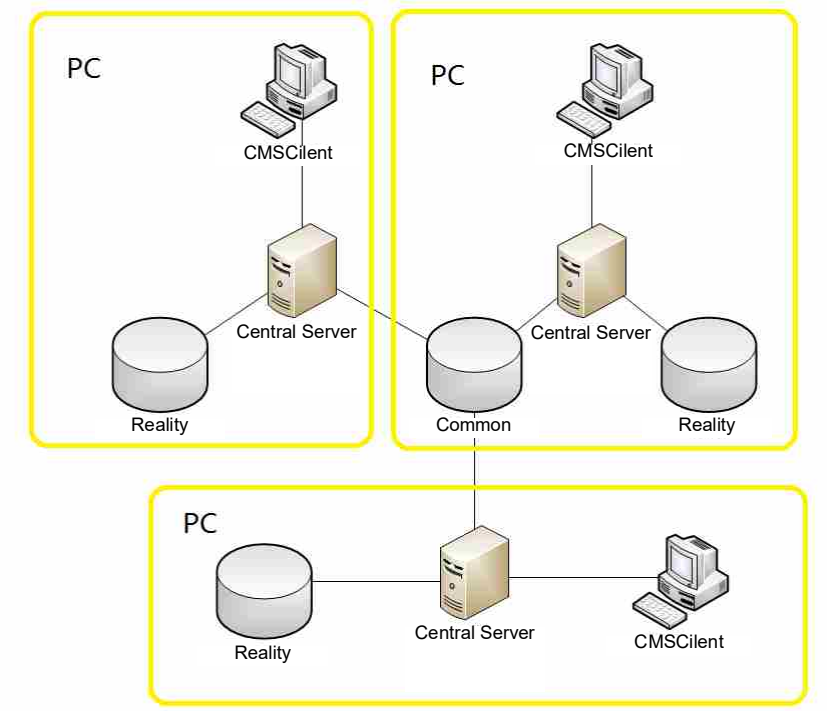


Figure 1.3

Server performance requirements	Maximum number of networked monitors	128
	Maximum number of clients	When admitting 128 patients online, the Vista CMS can connect up to 5 clients simultaneously. When admitting 64 patients online, the Vista CMS can connect up to 10 clients simultaneously.
	Maximum number of networked server	10

Hardware requirements

The hardware specifications of CMS (that is, Vista CMS 2.0) vary depending on the type of deployment. Vista CMS 2.0 deployment currently supports two types:

- Separately deploy CMSClient
- Deploy Central Server and CMSClient on one computer

Select the hardware that meets the deployment requirements based on the following actual conditions:

1 Vista CMS 2.0 deployment method.

2 Quantity of monitoring devices connected.

3 Vista CMS 2.0 application environment.

Deploying CMSClient separately

To separately deploy CMSClient on one computer, the basic hardware specifications are as follows:

- CPU: Intel Core i5, Duo 3.1 GHz or above
- Memory: 4 G or above
- Hard disk: 120 GB or above
- Display interface: 2 or above
- LAN port: 2 or above
- USB port: 4 or above
- OS: Windows 10 Pro 64 bit, Windows 11
- Display: 1 or more, up to 4

CMSClient mainly includes Monitoring Station (with dongle) and Viewer Station (without dongle).

- Monitoring Station: refers to the PC client with larger scope of permission for software functions. It is mainly used for the central monitoring system which needs real-time monitoring, viewing and remote control in the nurse workstation.
- Viewer Station: refers to the PC client with smaller scope of permission for software functions. It focuses on real-time monitoring and viewing.

In addition, USB dongle must be inserted for the normal working of Monitoring Station.

The recommended CMS display specifications:

- 19-inch (widescreen): 1440 x 900
- 19-inch (regular-screen): 1280 x 1024
- 22-inch (widescreen): 1920 x 1080
- 24-inch (widescreen): 1920 x 1200

NOTE

The 64-bit operating system with 8 GB (or above) of memory is recommended in any of following cases:

- Connect with more than 64 monitoring devices.
- Use 2 or more displays.

Deploying Central Server

To deploy Central Server on one computer, the basic hardware specifications are as follows:

- CPU: Intel Core i5, Duo 3.1 GHz or above
- Memory: 8 G or above
- Hard disk: 1 T or above
- Display interface: 2 or above
- LAN port: 2 or above
- USB port: 2 or above
- OS: Windows 10 Pro 32/64 bit, Windows 11 Pro 64 bit, Server 2012, Server 2016, Server 2019, Server 2022, virtual machine
- Display: 1 or more, up to 4

It is recommended that the computer on which Central Server is deployed shall be configured with two ports for network adapter. One is for communication with the monitoring device and the other is for communication with CMSClient to ensure data isolation.

NOTE

The 64-bit operating system with 16 GB of memory is recommended in any of following cases:

- Connect with more than 64 monitoring devices.
- Use 2 or more displays.

To support 2 or more displays, note the following:

1. The 32-bit version of Vista CMS 2.0 software supports double-screen at most. If more than 2 displays are needed, install the 64-bit version of the Vista CMS 2.0 software.
2. If 2 or more displays are needed, it is recommended to use an independent graphics card.
3. If more than 2 displays are needed, use the CPU which has the equivalent or higher performance with I7-7700.
   - i7 processor, 7th generation or above;
   - i5 processor, 8th generation or above;

Installing the operating system

Install the corresponding Windows operating system on your computer as required.

NOTE

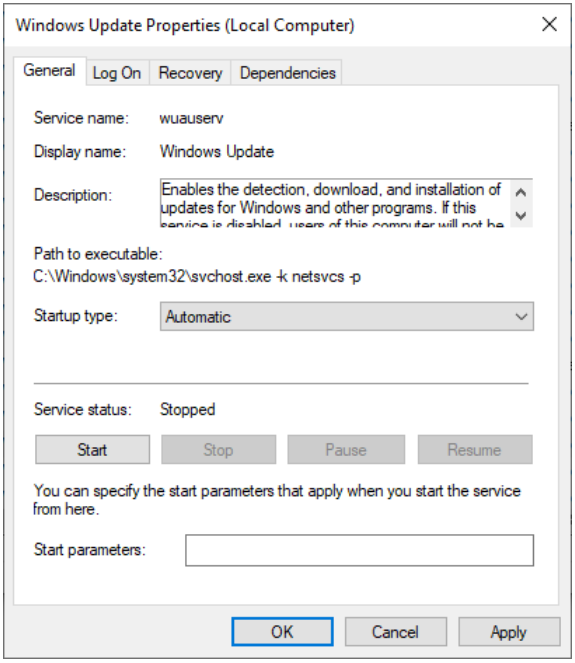
It is recommended to enable Windows password strategy to improve security.

NOTE

Install anti-virus software of Microsoft Security Essentials and carry out the anti-virus measures regularly.

NOTE

It is recommended to allow security updates from third-party manufacturers (e.g. Microsoft) to be installed after validation by the manufacturer.



NOTE

Set Vista CMS 2.0 to white list in Microsoft Security Essentials.

- In Windows Security, select Virus & threat protection > Manage settings.
- Select Add or remove exclusions.
- Click Add exclusions and select the CMS installation folder to add the whitelist.

Region and language settings

Region and Language should be set to be consistent.

Hard disk partition

The hard disk should be partitioned during or after the installation of the operating system. It is recommended to format hard disk as NTFS for file recovery and auditing purposes.

Divide the hard disk into 3 partitions: For example (C :), (D :) and (E :).

- Partition C: 100 GB, for OS installation.
- Partition D: 800 GB, for Vista CMS 2.0 installation and database storage. The memory portion to this partition is based on the total volume of the hard disk. The default installation path of Vista CMS 2.0 is Disk D, and it is recommended to reserve sufficient space for this partition.
- Partition E: 100 GB, for backing up the data of the OS.

Hardware drive

To ensure that the Vista CMS 2.0 can run normally, the user should install the network adapter, video adapter, audio adapter as well as their respective drives on the computer before installing the software. Otherwise, some functional failures may be found even though the system can be normally started.

WARNING

If the drive for the network adapter is not installed, the system cannot be connected to the bedside monitors. Thereby, the system cannot play the part of monitoring.

WARNING

If the driver for the video adapter is not installed, the system display is abnormal and the refreshing of the data is delayed.

WARNING

If the driver for the audio adapter is not installed, the system cannot play the alarm sound and thus fails to indicate an alarm in the audio way.

NOTE

CMSClient includes Monitoring Station (with dongle) and Viewer Station. Audio adapter is optional for Viewer Station.

After OS installation, install the drives in the following order.

1. Motherboard chipset (drive)
2. Video adapter (drive)
3. Audio adapter (drive)
4. Network adapter (drive)

Installing the printer

To perform the printing function of the Vista CMS software, the user has to install a printer before use. HP LaserJet Series printers are recommended.

NOTE
If no printer is installed, the function of printing or preview is disabled.

NOTE
Use the recommended HP M104A LaserJet printer to avoid incompatibility.

NOTE
If the printer used is a double-sided printer, install the printer drive correctly, otherwise you may not be able to use the double-sided printing function.

Multiple displays

Display setup

After video adapter installation, install corresponding drive > right-click the desktop > **Display** > **Multiple displays** > **Extend desktop to this display** as shown in Figure 1.4.

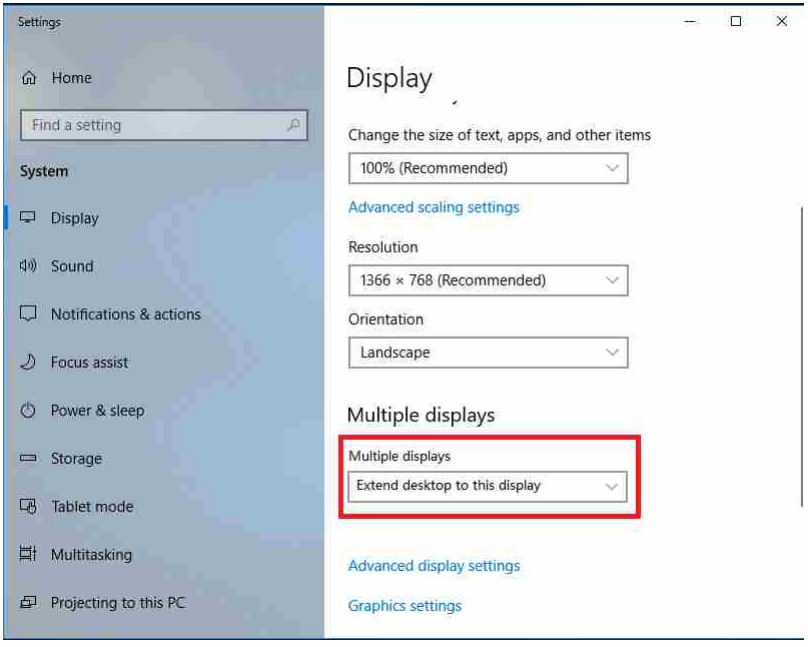


Figure 1.4

NOTE
The example used here is ATI video adapter setting. If a video adapter of another brand/type is used, make similar setting when installing the video adapter drive.

NOTE
If the selected mode is incorrect, Vista CMS 2.0 may fail to tboot up, or only a single display is available.

Display setup of multiple displays

Up to 4 displays is supported. To achieve the multiple displays, make sure that the displays are of the same brand, the same type and set with the same resolution. The video adapter should support multi-display as well. The number of displays and corresponding layout are shown in table below:

Number of displays	Layout
1	1
2	1x2
3	1x3
4	2x2, 1x4

The default layout for 4 displays is 1*4. If 2*2 is required, right-click on the desktop > **Display** as shown in Figure 1.5.

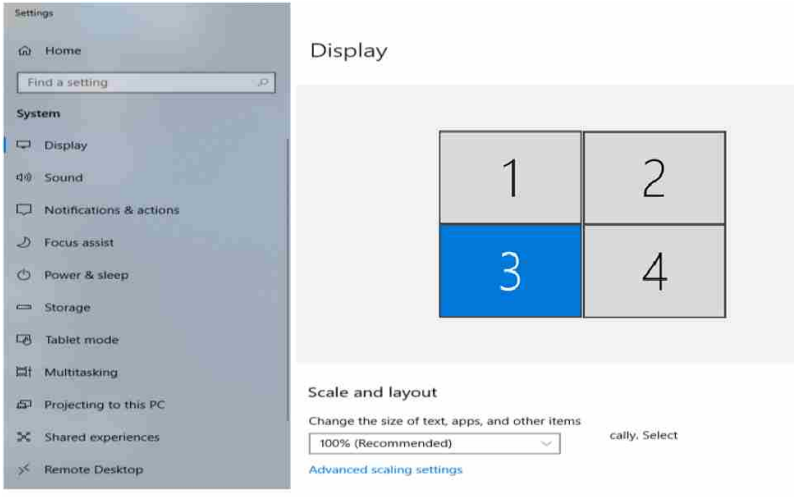


Figure 1.5

NOTE
The operation path in the figure above is available for Windows 10.

NOTE
After completing the setup, restart the software to use Vista CMS 2.0 in multiple displays.

NOTE
If one of the displays is plugged in/out or powered off during the operation, restart the software to ensure the proper running.

NOTE
The sequence of Display 1, Display 2, Display 3 and Display 4 should be in the order of left to right and top to bottom, otherwise Vista CMS 2.0 cannot run normally.

Scale and layout setup

Right-click on the desktop > **Display** > set scale and layout to **100%** as shown in Figure 1.6.

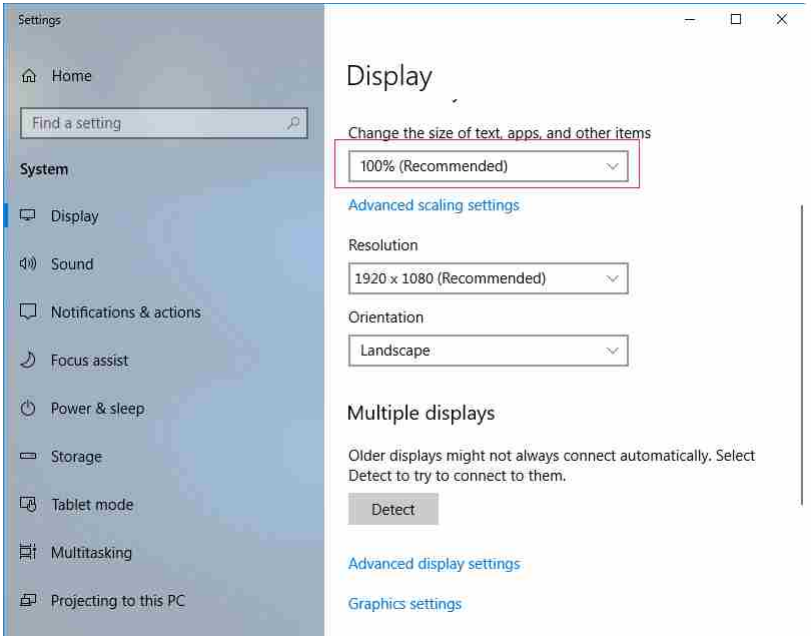


Figure 1.6

Network setup

NOTE
Make sure the network adapter as well as the corresponding drive has been installed in the computer prior to network setup. Otherwise the following steps cannot be proceeded.

Network IP setup

NOTE

The default network segment 202.114.4.x/24 used by the monitoring device is not recommended to be used in the public network environment. Network segment 202 is the public network IP. Under condition of cross-network segment, the router and switch will send data to the public network.

1 Click **Control Panel** > **Network and Internet** > **Network and Sharing Center** as shown in Figure 1.7.

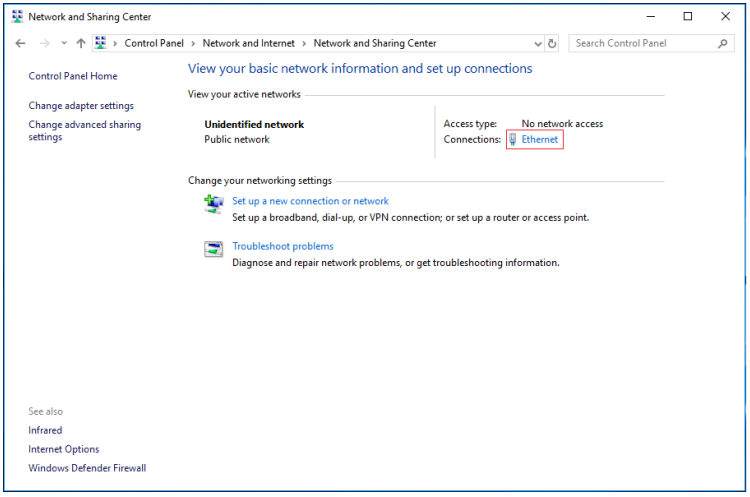


Figure 1.7 Network and Sharing Center

Click **Ethernet** in Figure 1.7 to pop up the left window as shown in Figure 1.8 > click **Properties** to pop up right window as shown in Figure 1.8 > select **TCP/IPV4** > click **Properties** to pop up Figure 1.9.

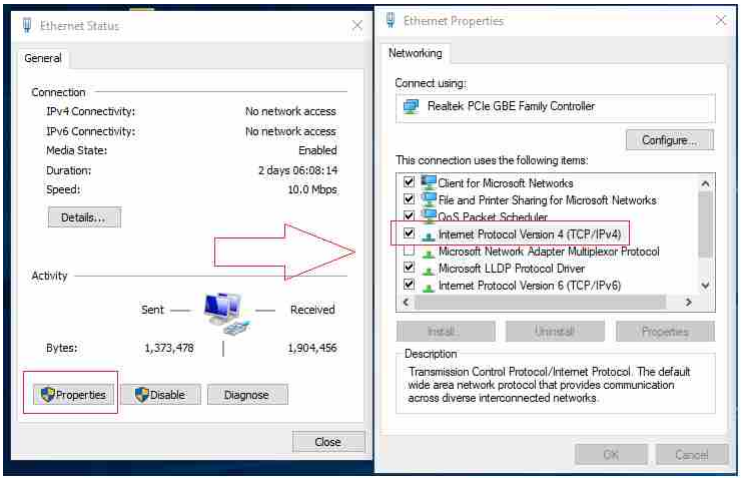


Figure 1.8 Ethernet

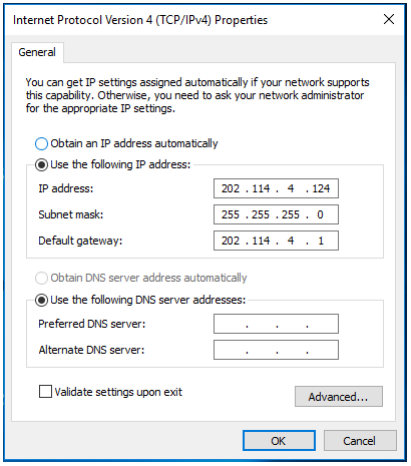


Figure 1.9 Set IP Address

2 Set the server IP address of the monitoring device. For example, in Figure 1.9, set IP address of the computer where Vista CMS 2.0 is installed to 192.168.46.235, accordingly, set server IP address of the monitoring device to 192.168.46.235.

NOTE

If multiple monitors are simultaneously connected to one Vista CMS 2.0 system, make sure all these monitors share the same server. Different monitors cannot share the same IP address, otherwise some monitors cannot be connected to the Vista CMS 2.0 system.

The supported monitoring devices		
Devices	Software Version	Note
Vista 120 V2	V2.2 and above	/
Vista 120 V3	V3.0 and above	/
Vista 120S	V3.0 and above	/
Vista 120 SC	V1.0 and above	/
Vista 300	V1.0 and above	/

Dual network adapters configuration

Dual network adapters are recommended to be used for the computer that Central Server is deployed. One is for CMSClient communication, and the other is for communication with monitoring device to ensure data isolation.

NOTE

When setting the IP of dual network adapters, these two IP should be set in different network segments to ensure communication isolation. Refer to Section *How to Increase the Static Routing Table Configuration* for further information.

Installing Vista CMS 2.0 software

Overview

NOTE
The system shall be installed by trained and qualified personnel.

If reinstallation is required, ensure the following steps before installation.

1 Turn off all CMSClient.

2 Uninstall Vista CMS 2.0.

3 Turn off the antivirus software.

NOTE
A dedicated computer is required. It is not allowed to install any software other than Vista CMS 2.0 component and the antivirus software.

NOTE
If Vista CMS 2.0 and gateway software are deployed on one computer, please block the function of connecting monitoring device to gateway, and change gateway port number. Monitoring device should connect to Vista CMS 2.0, and Vista CMS 2.0 should connect to gateway.

NOTE
Incompatibility between the Client side and the Server side may cause incorrect monitoring data reading and display. To avoid the potential patient injury, update the client and the service-side software simultaneously.

Installation steps

NOTE
All images in this installation instruction are based on Windows 10. Different operating systems may vary in the display content.

After finishing the Vista CMS 2.0 installation, login to the administrator account (username: service, password: 111111) for authorization activation. Refer to Section *Authorization* for the activation steps.

1 Double-click the file Setup.exe in the installation package in CD. Click **Vista CMS** and install the software step by step.

Figure 2.1

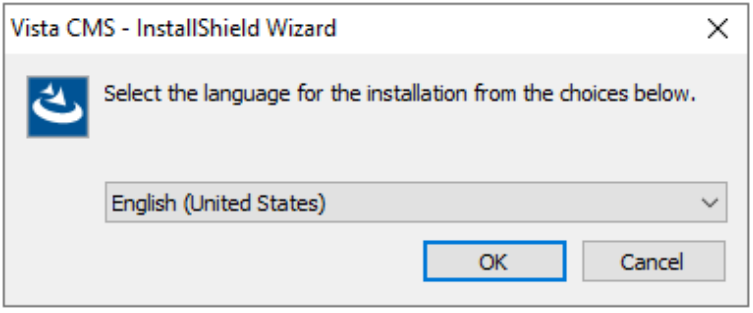


Figure 2.2

Figure 2.3

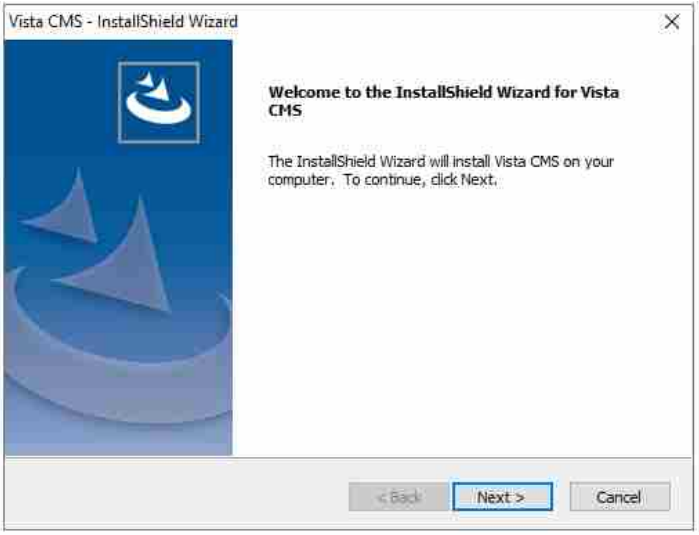


Figure 2.4

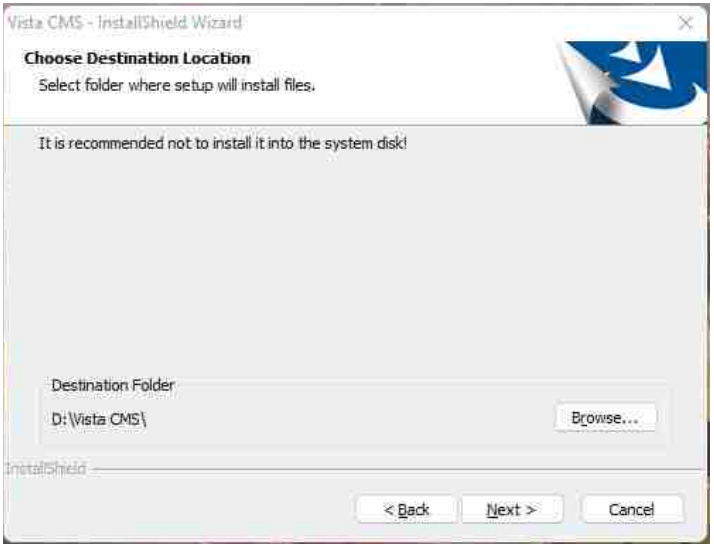


Figure 2.5

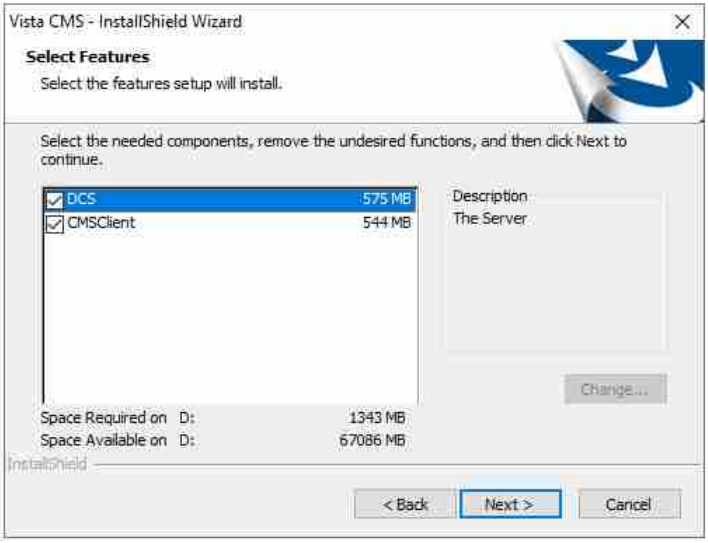


Figure 2.6

NOTE

DCS is for server side and CMSClient is for client side. Select the components to install based on the target deployment type.

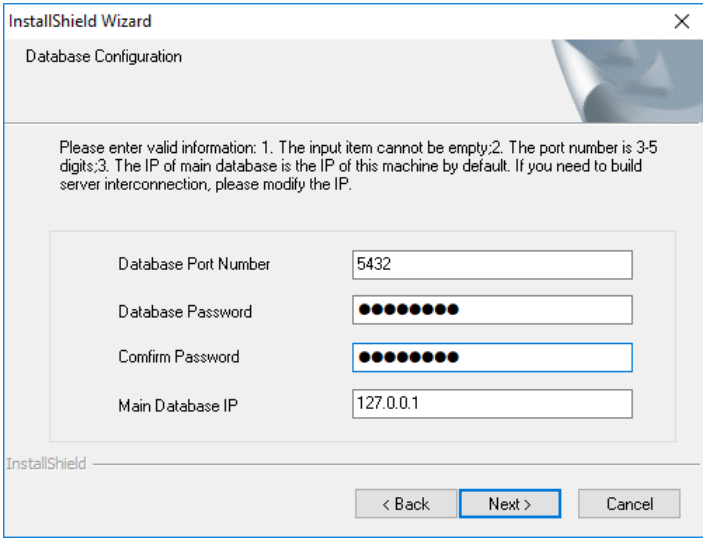


Figure 2.7

The default IP address of main database is 127.0.0.1.

The key steps for the distributed environment deployment:

1 For standalone Central Server-CMSClient, just keep the default IP address: 127.0.0.1. Click **Next** for subsequent installation steps.

2 For distributed Central Server environment, in multiple Central Server environments, one must be selected as the main Central Server. The **Main Database IP** is the IP of the computer where the main Central Server is installed.

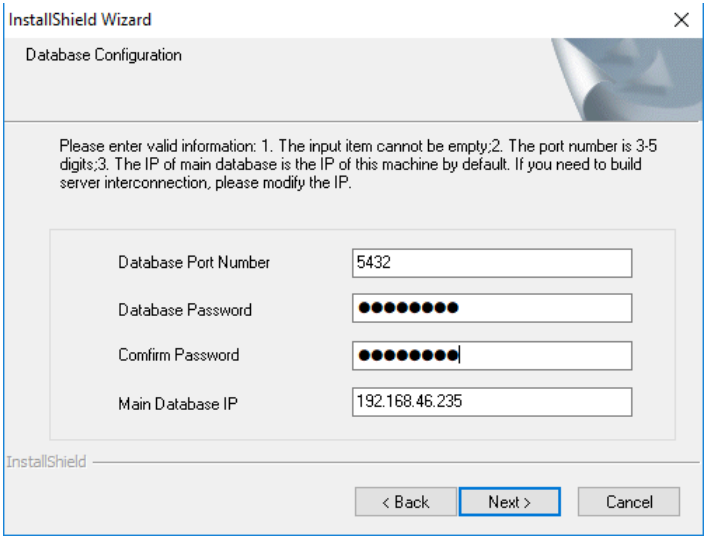


Figure 2.8

Default password for database is ACE007jh. Change the default password during the installation.

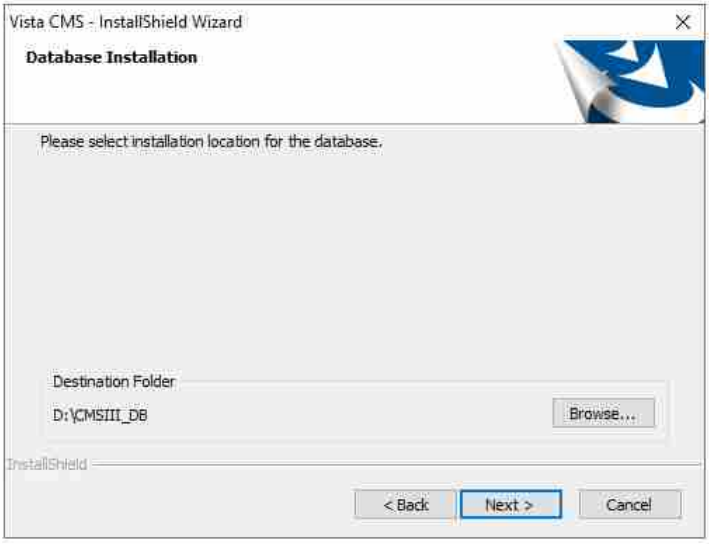


Figure 2.9

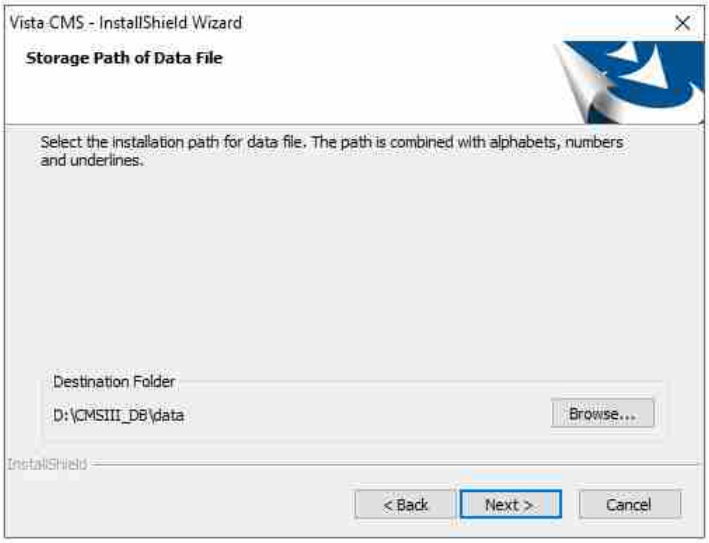


Figure 2.10

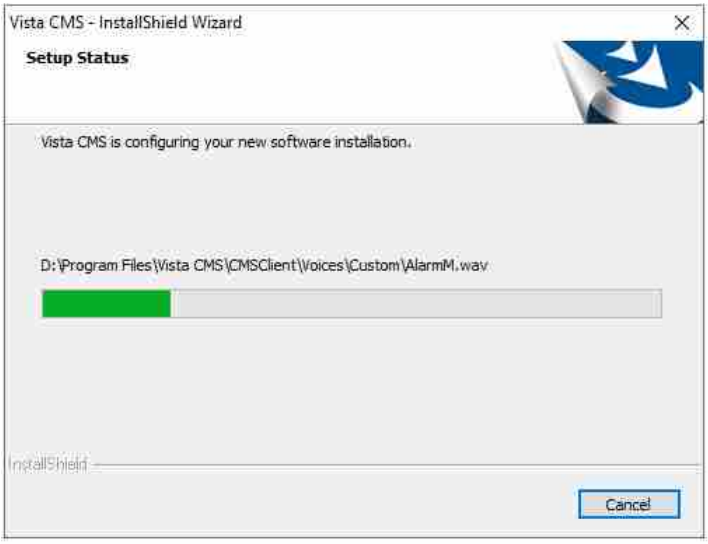


Figure 2.11

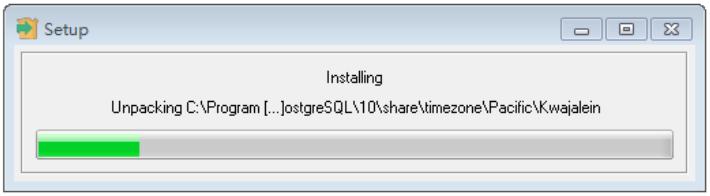


Figure 2.12

Installation Tips:

If the computer already has a database installed, the Setup can detect the database, so you can skip the database installation.

Click **Next** in the interface as shown in Figure 2.6 to enter the **Select Features** interface as shown in Figure 2.13, indicating that the database already exists, and the user only needs to confirm the configuration information of the database.

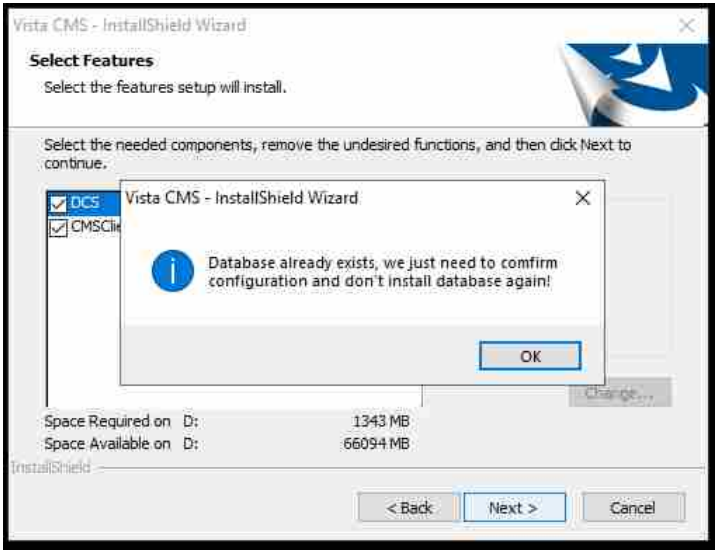


Figure 2.13

Refer to Figure 2.8 to configure the database information.

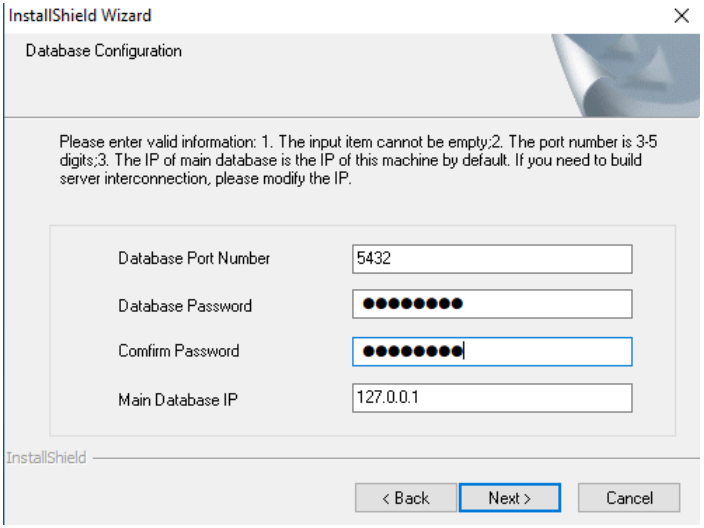


Figure 2.14

Install Net Framework 4.8

Net Framework 4.8 is the dependent environment for running Vista CMS 2.0. If Net Framework 4.8 is not installed in the current operating system, it will enter the installation program at the end of installation. Users only need to click on **Next** to complete the installation. After installing Net Framework 4.8, the system will prompt the user to restart the computer. After restarting the computer, the user must reinstall Vista CMS 2.0.

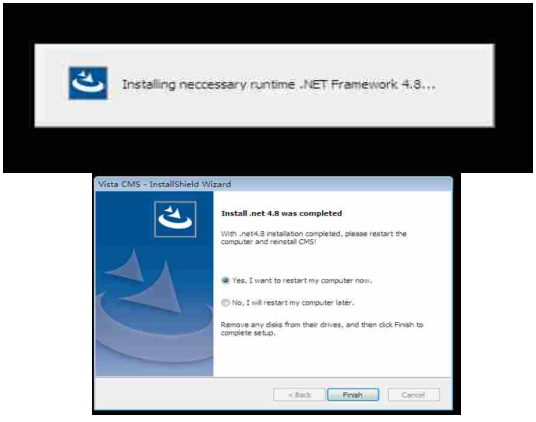


Figure 2.15

NOTE

The system prompts to restart the computer after the installation. If no other hardware drives or software (such as printers, etc.) need to be installed, restart the computer. The Vista CMS 2.0 software will automatically run after the restart.

NOTE

Restart the computer to make the hardware drive take effect. If you directly run the Vista CMS 2.0 program without restarting the computer, the video adapter, audio adapter, network adapter, main board, dongle or other hardware may not be identified, and the Vista CMS 2.0 software will therefore fail to boot up.

NOTE

If the antivirus software or defensive software is installed on your computer, a dialog box about Windows Security Alert may pop up when you run the Vista CMS 2.0 software at the first time. Click on Unblock.

NOTE

After the installation, do not modify or delete any file in the directory where the Vista CMS 2.0 software and the database are installed, otherwise unanticipated mistakes may occur.

Configuring the broadcast address of central server

Configure the broadcast address in the following situations:

1 If dual network adapters are configured and the two IP are not in the same network segment, set broadcast address to the IP address of the same network segment as the monitoring device. If not configured, monitoring device may not connect to Vista CMS 2.0. Refer to Section *Network IP* setup for further information about IP setting.

2 If CMP protocol version is V1.0 or V1.1, the broadcast address should be set, otherwise, the monitoring device may not be connected to Vista CMS 2.0 for long time. If CMP protocol version is uncertain, it is recommended to set the broadcast address.

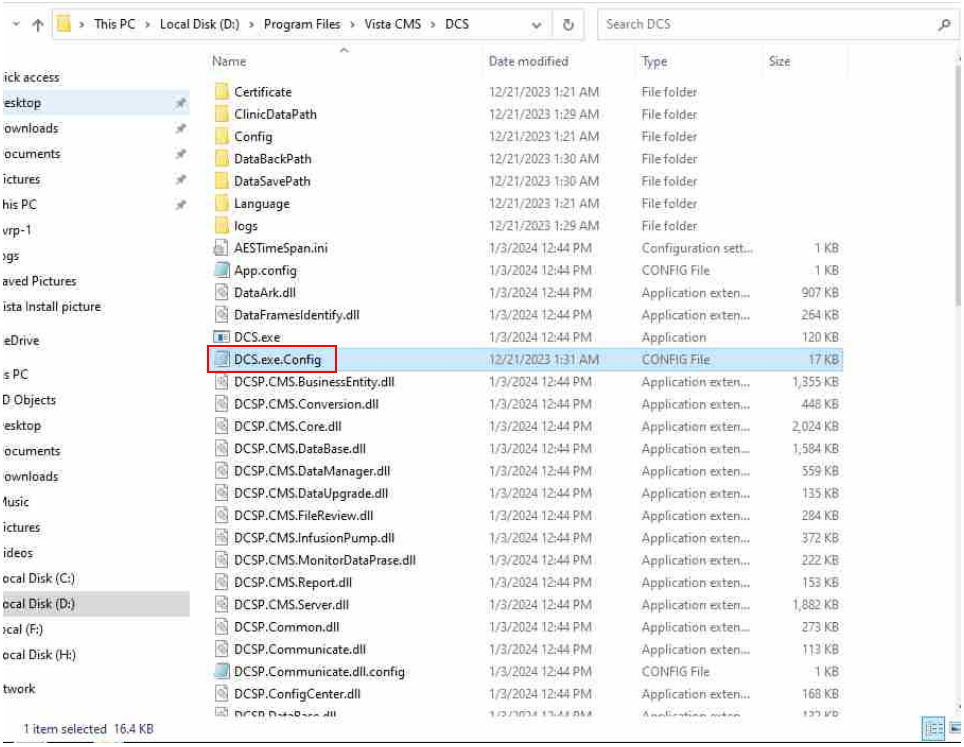


Figure 2.16

In Vista CMS 2.0 installation path, find Central Server installation path as shown in Figure 2.16. Open DCS.exe.config, and find the configuration items of broadcast IP (UdpIplist) and broadcast subnet mask (UdpSubnetMask) as shown in Figure 2.17.

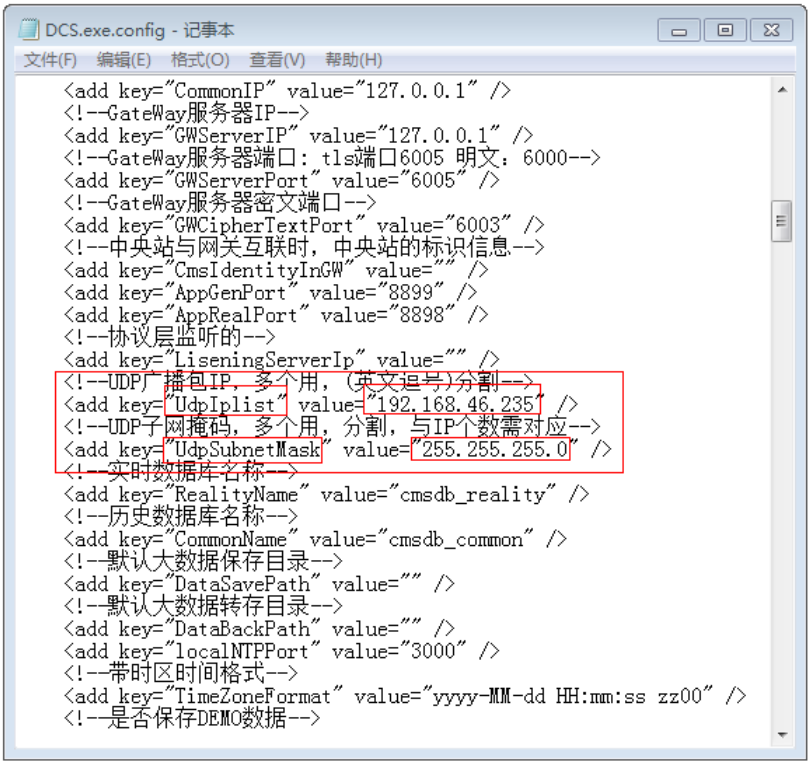


Figure 2.17

NOTE

The subnet mask must also be filled in together with the broadcast IP.

NOTE

If there’re multiple broadcast IP addresses, the subnet mask must be filled in the same order as the IP address.

NOTE

If multiple Broadcast IP or UDP subnet mask needs to be filled, use English comma between them.

Configuring Vista CMS 2.0 identification information when interaction with gateway is required

If there are two independent Vista CMS 2.0 systems (they have separate common databases that are not shared) and common database IP is 127.0.0.1 and also these two systems need to connect to the same gateway, then, different 'Vista CMS 2.0 Identification' should be set for each Vista CMS 2.0, and the same 'Vista CMS 2.0 Identification' should be set for multiple Central Servers of one Vista CMS 2.0. Make the settings as below:

1 In Vista CMS 2.0 installation path, find Central Server installation path. Open DCS.exe.config, and find the configuration item (CmsIdentityInGW) of Vista CMS 2.0 identification information as shown in Figure 2.18.

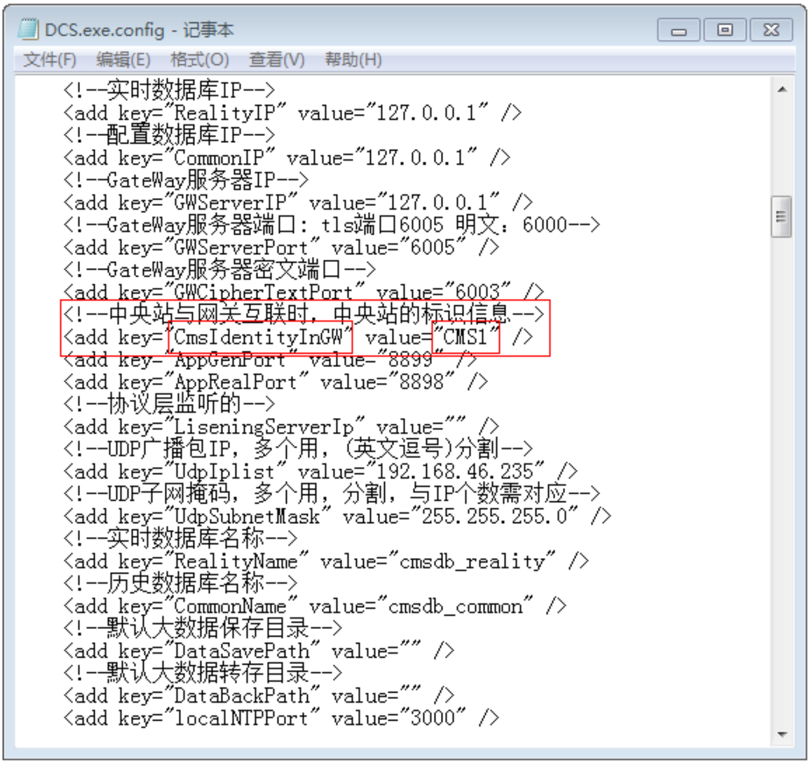
2 When setting Vista CMS 2.0 identification, notice that: use strings, such as 'CMS1' or 'CMS2', etc, or use an identification easy to record, but the configuration identification of multiple Vista CMS 2.0 systems must be different, thus the gateway can correctly identify different Vista CMS 2.0.

NOTE

In the deployment, one Vista CMS 2.0 system can connect to an independent gateway without any special configuration. If this configuration item is not configured, Vista CMS 2.0 sends IP of Common database to gateway by default.

NOTE

In the deployment, two separate Vista CMS 2.0 systems have their own Common databases that are not shared. The common database IP is not 127.0.0.1, and IP of two common databases are set differently. If this configuration item is not configured, Vista CMS 2.0 sends Common database IP to gateway by default.




```
<!--实时数据库IP-->
<add key="RealityIP" value="127.0.0.1" />
<!--配置数据库IP-->
<add key="CommonIP" value="127.0.0.1" />
<!--GateWay服务器IP-->
<add key="GWServerIP" value="127.0.0.1" />
<!--GateWay服务器端口: tls端口6005 明文: 6000-->
<add key="GWServerPort" value="6005" />
<!--GateWay服务器密文端口-->
<add key="GWCipherTextPort" value="6003" />
<!--中央站与网关互联时, 中央站的标识信息-->
<add key="CmsIdentityInGW" value="CMS1" />
<add key="AppGenPort" value="8899" />
<add key="AppRealPort" value="8898" />
<!--协议层监听的-->
<add key="LiseningServerIp" value="" />
<!--UDP广播包IP, 多个用, (英文逗号)分割-->
<add key="UdpIplist" value="192.168.46.235" />
<!--UDP子网掩码, 多个用, 分割, 与IP个数需对应-->
<add key="UdpSubnetMask" value="255.255.255.0" />
<!--实时数据库名称-->
<add key="RealityName" value="cmsdb_reality" />
<!--历史数据库名称-->
<add key="CommonName" value="cmsdb_common" />
<!--默认大数据保存目录-->
<add key="DataSavePath" value="" />
<!--默认大数据转存目录-->
<add key="DataBackPath" value="" />
<add key="localNTPPort" value="3000" />
```

Figure 2.18

Restarting services after installation

NOTE
If configuration items in the above two sections have been modified, restart services to make them effective.

Right-click **Computer** on the desktop > **Management** > **Service and Applications** > **Services** to find related services for verification. Find and restart **CMSWindowsService**, **CMSCommonService**. After the restart, find **CMSWindowsService**, **CMSCommonService**, **postgresql-x64-10** and ensure that they have been started.

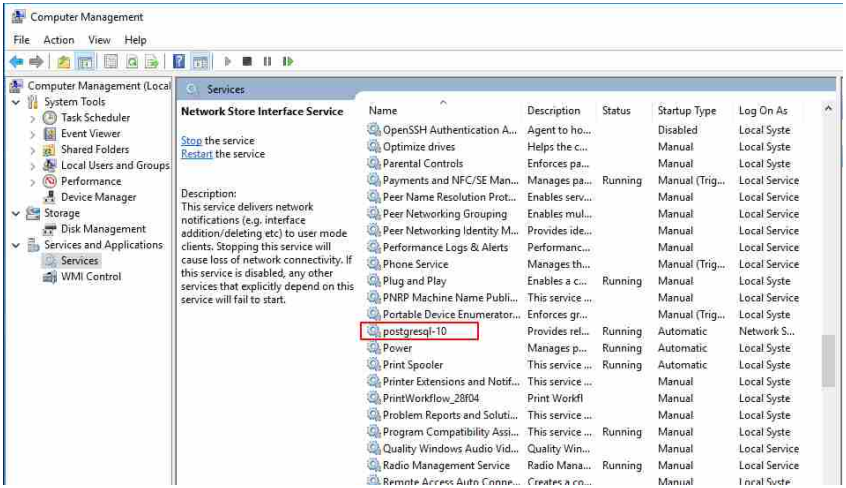


Figure 2.19

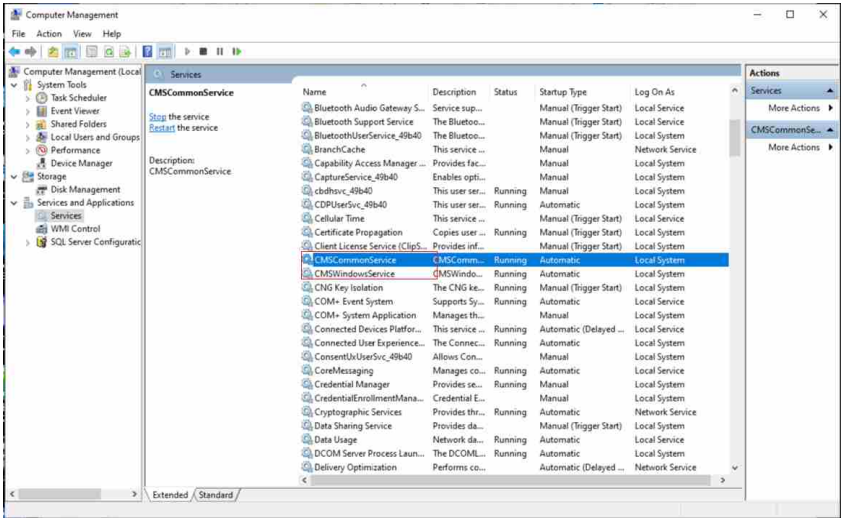


Figure 2.20

Uninstalling Vista CMS 2.0 software

Preparation for uninstallation

Before uninstalling Vista CMS 2.0, ensure that:

- Below configuration file for Central Server has been backed up.
  - Vista CMS\DCS\ConfigBack
- Below disk data files have been backed up.
  - ClinicDataPath
  - DataBackPath
  - DataSaveData

Find the Central Server installation directory as shown in Figure 3.1. Backup the files.

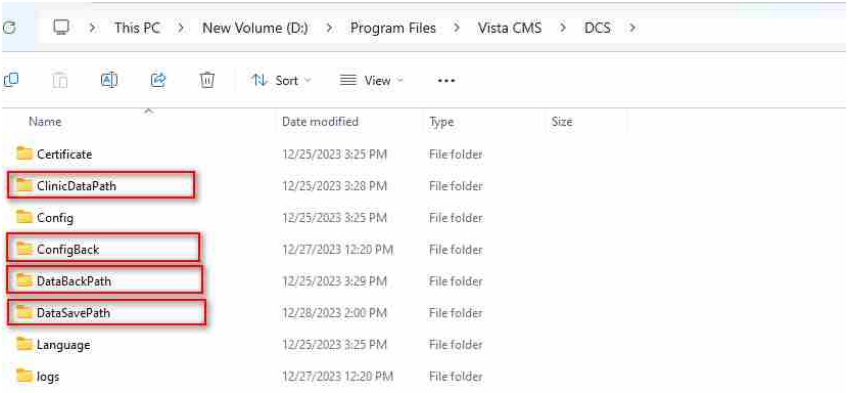


Figure 3.1

- To restore the Central server configuration file and the disk data (Patient data), put above 4 files back to the same directory after CMS reinstallation or update.

NOTE

The backup of Central server configuration file and the disk data (Patient data) only works for CMS reinstallation or update without reinstalling the Database (PostgreSQL).

Uninstalling

Uninstalling Vista CMS 2.0

Two alternatives are available for uninstalling the Vista CMS 2.0 software.

Method 1: Click **Start** > **All Programs** > **Vista CMS** > **Uninstall** to uninstall the software.

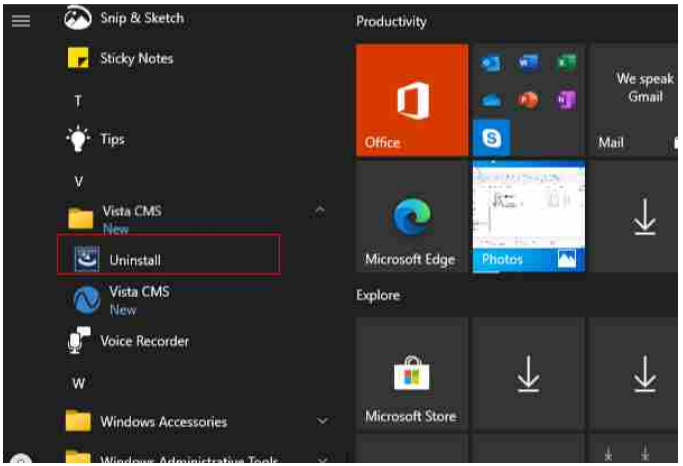


Figure 3.2

Method 2: Click **Start** > **Control Panel** > **Programs** > **Programs and Features** and select the Vista CMS program > right-click it to uninstall it.

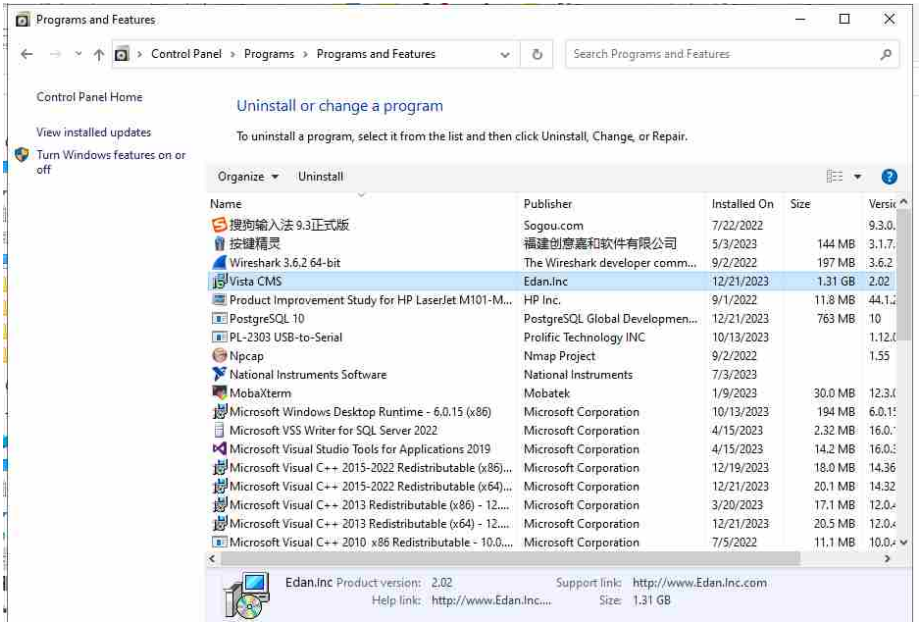
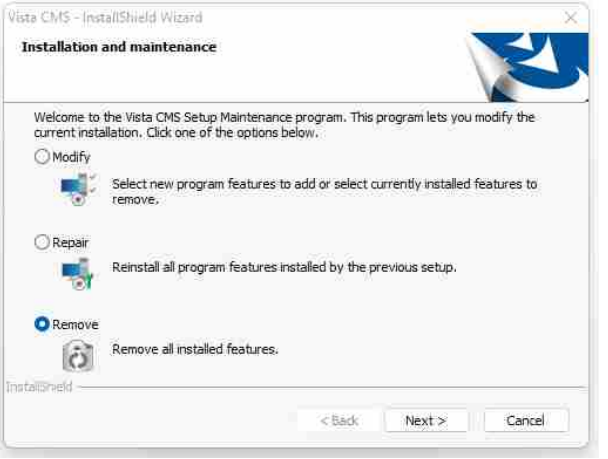


Figure 3.3

Installation Maintenance

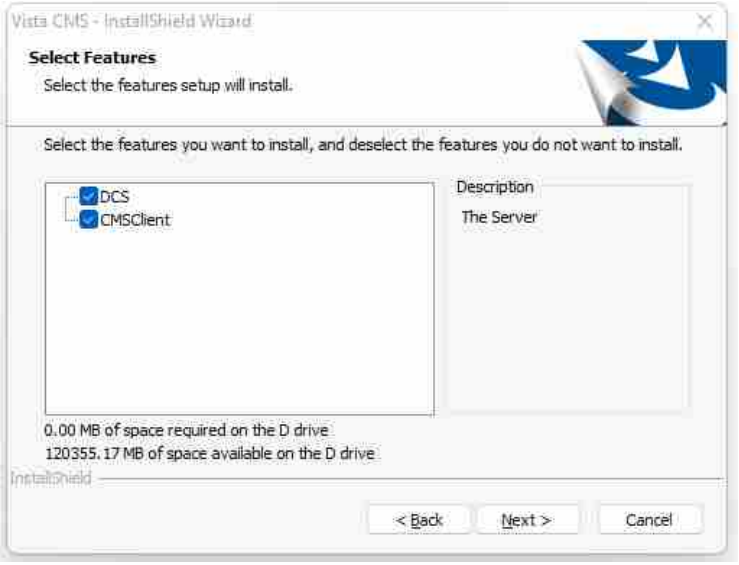
When users uninstall Vista CMS, the system enters the installation and maintenance interface.



In this interface, users can perform three operations: modify, repair, and remove.

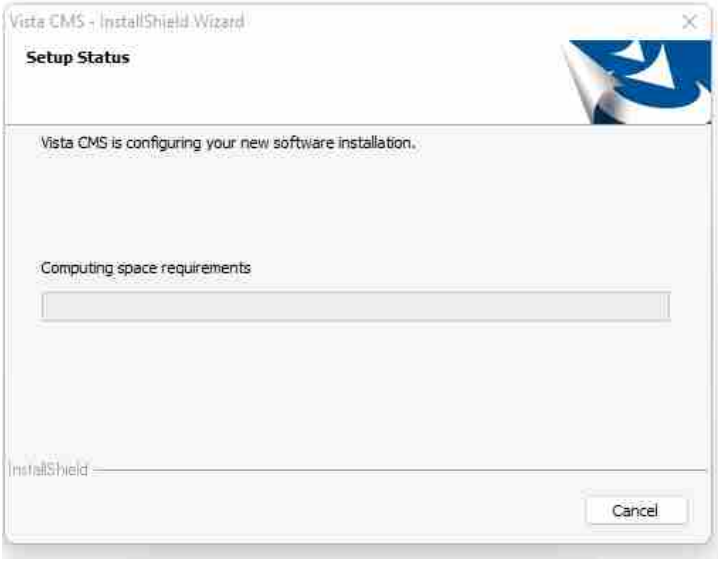
1) Modify

If you need to install or uninstall the client or server separately, select the Modify option and click Next to proceed to the selection screen. Select the features you want to install, and deselect the features you do not want to install.

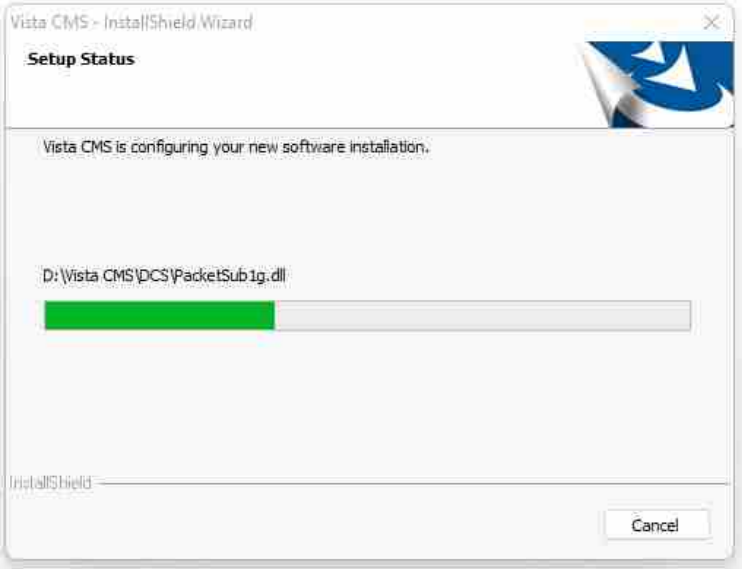


2) Repair

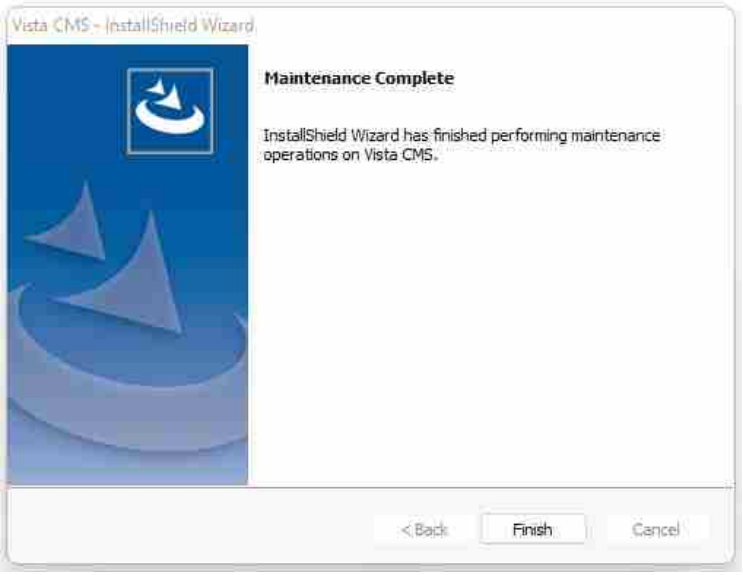
You can perform this operation if the configuration file is lost or damaged. This operation restores all files in the installation directory to their original state.



3) Remove Uninstall the client and server.



After performing any of the above, the maintenance completion screen appears and maintenance is complete.



Uninstalling database

Click **Start** > **Control Panel** > **Programs** > **Programs and Features** and select PostgreSQL > right-click it to uninstall it.

NOTE

Uninstalling the database will invalidate the previous authorization. To restore the previous authorization, properly keep the License file authorization.

NOTE

Uninstalling the database will cause the monitoring data loss. The backup data of DataBackPath and DataSavePath folder can only be viewed via backup data loading function.

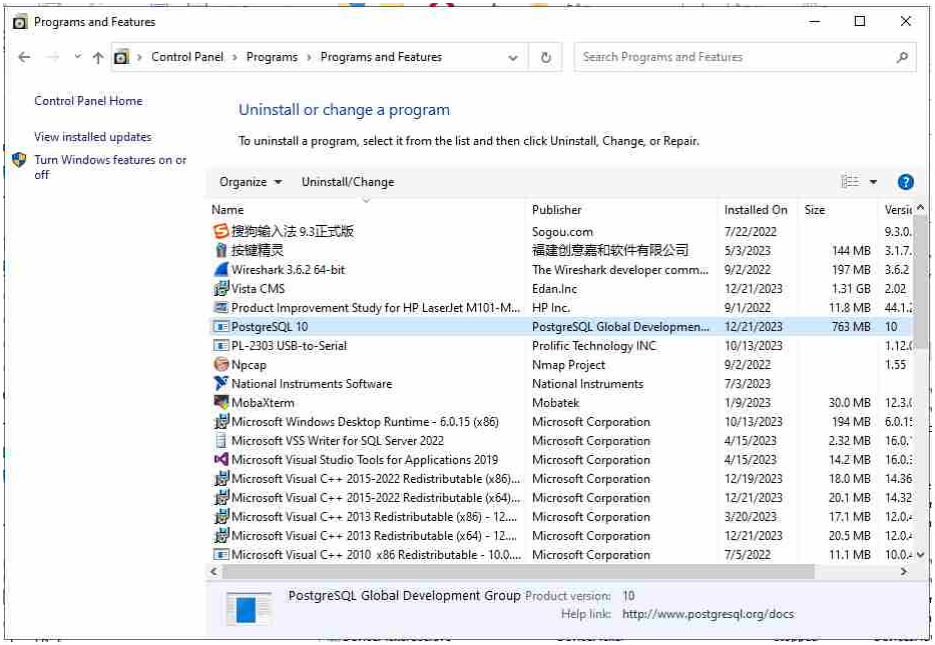

Programs and Features
Control Panel › Programs › Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Uninstall or change a program
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.
Organize
Uninstall/Change
Name
Publisher
Installed On
Size
搜狗输入法 9.3正式版
Sogou.com
7/22/2022
按键精灵
福建创意嘉和软件有限公司
5/3/2023
144 MB
Wireshark 3.6.2 64-bit
The Wireshark developer comm...
9/2/2022
197 MB
Vista CMS
Edan.Inc
12/21/2023
1.31 GB
Product Improvement Study for HP LaserJet M101-M...
HP Inc.
9/1/2022
11.8 MB
PostgreSQL 10
PostgreSQL Global Developmen...
12/21/2023
763 MB
PL-2303 USB-to-Serial
Prolific Technology INC
10/13/2023
Npcap
Nmap Project
9/2/2022
National Instruments Software
National Instruments
7/3/2023
MobaXterm
Mobatek
1/9/2023
30.0 MB
Microsoft Windows Desktop Runtime - 6.0.15 (x86)
Microsoft Corporation
10/13/2023
194 MB
Microsoft VSS Writer for SQL Server 2022
Microsoft Corporation
4/15/2023
2.32 MB
Microsoft Visual Studio Tools for Applications 2019
Microsoft Corporation
4/15/2023
14.2 MB
Microsoft Visual C++ 2015-2022 Redistributable (x86)...
Microsoft Corporation
12/19/2023
18.0 MB
Microsoft Visual C++ 2015-2022 Redistributable (x64)...
Microsoft Corporation
12/21/2023
20.1 MB
Microsoft Visual C++ 2013 Redistributable (x86) - 12....
Microsoft Corporation
3/20/2023
17.1 MB
Microsoft Visual C++ 2013 Redistributable (x64) - 12....
Microsoft Corporation
12/21/2023
20.5 MB
Microsoft Visual C++ 2010 x86 Redistributable - 10.0....
Microsoft Corporation
7/5/2022
11.1 MB
PostgreSQL Global Development Group
Product version: 10
Help link: http://www.postgresql.org/docs

Figure 3.4

Updating Vista CMS 2.0 software

Overview

The software update of Vista CMS 2.0 is implemented by uninstalling the old version of Vista CMS 2.0 and then installing the new version of Vista CMS 2.0, referring to ‘Uninstalling Vista CMS 2.0 software’ and ‘Installing Vista CMS 2.0 software’.

NOTE: Database (PostgreSQL) is not required to be uninstalled/reinstalled when doing Vista CMS software update. If the database (PostgreSQL) is uninstalled/reinstalled, the Historical Patient data will be lost. Please back up the patient data via Data Dump before uninstalling the database (PostgreSQL).

Configuring the Windows Firewall

Overview

NOTE

It is recommended to configure a hardware firewall. For details about how to configure a hardware firewall, consult the hardware firewall vendor.

NOTE

For security, disable all unused USB and network ports. A registry is recommended to disable task managers and Windows key.

The Windows Firewall must be configured after installing the Vista CMS 2.0. Otherwise data sent by the Vista CMS 2.0 is blocked by the firewall.

Enable the firewall. Add CMS and DCSHost to the whitelist.

1 CMS application path: in the Vista CMS 2.0 installation directory, Vista CMS > CMSClient > WTC.exe.

2 DCSHost application path: in the Vista CMS 2.0 installation directory, Vista CMS > DCS > DCS.exe.

The **Inbound Rules** should be set for following **Name**:

TCP port:

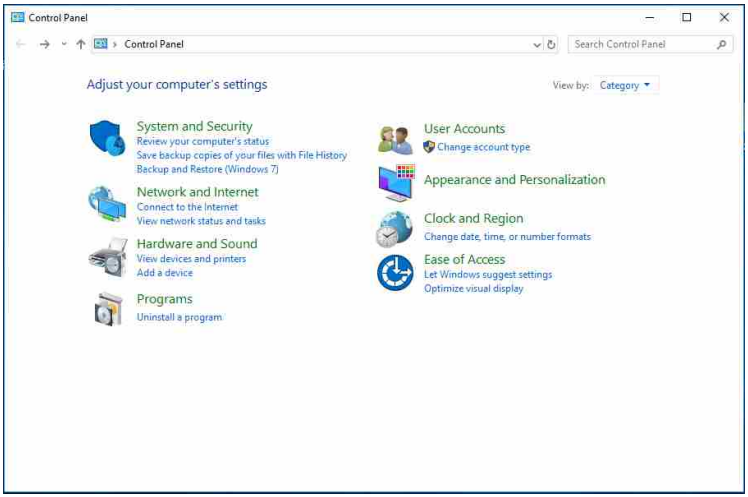
- Name: WCF-TCP-RealTime, Port: 4501
- Name: WCF-TCP-GeneralBusiness, Port: 4502
- Name: ComuicationService, Port: 4507
- Name: DataBase, Port: 5432
- Name: GW-TLS, Port: 6005
- Name: GW-TLS-Trans, Port: 6000
- Name: GW-Cipher, Port: 6003
- Name: ServiceAccess, Port: 8183
- Name: HardWareInfoService, Port: 4505
- Service detection, Port: 8186
- Name: Communication ports with monitoring devices: 9901, 9500, 9600, 6000-6005, 5510-5519, 5594, 5595, 9907, 9908

UDP port:

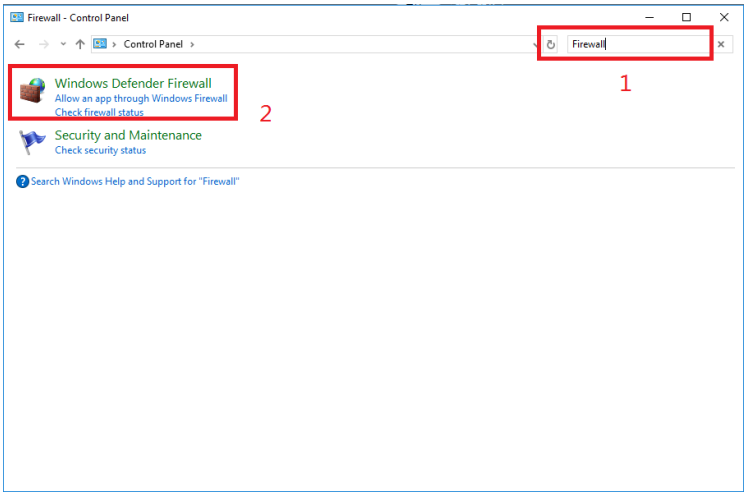
- Name: SYS-TIME, Port: 123

Below steps are the configuration for WCF-TCP-RealTime, Port: 4501. Refer to below steps for configuring other TPC port and UPD port.

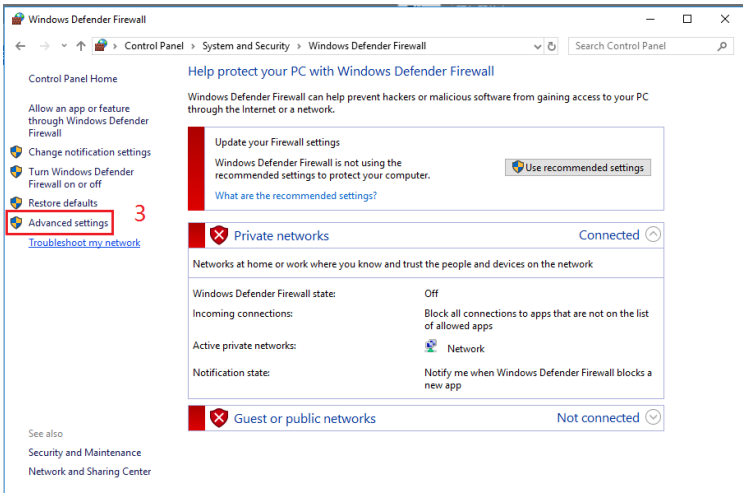
1 Enter the **Control Panel** interface.

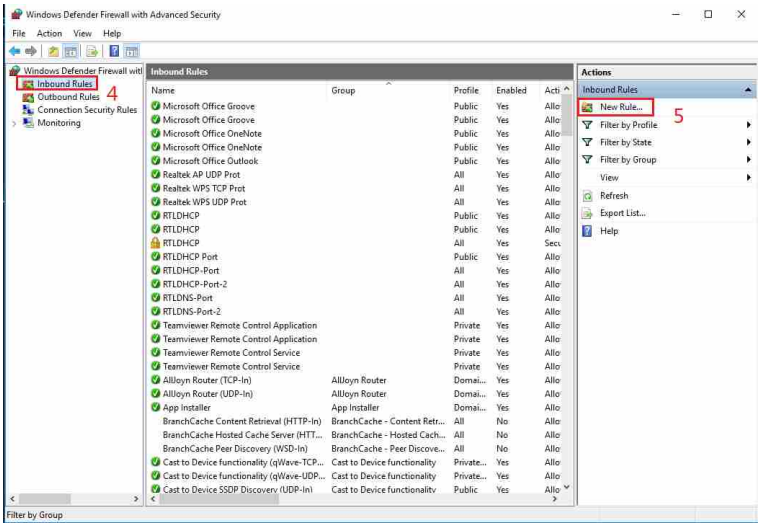


2 Search Firewall to enter firewall setting window.

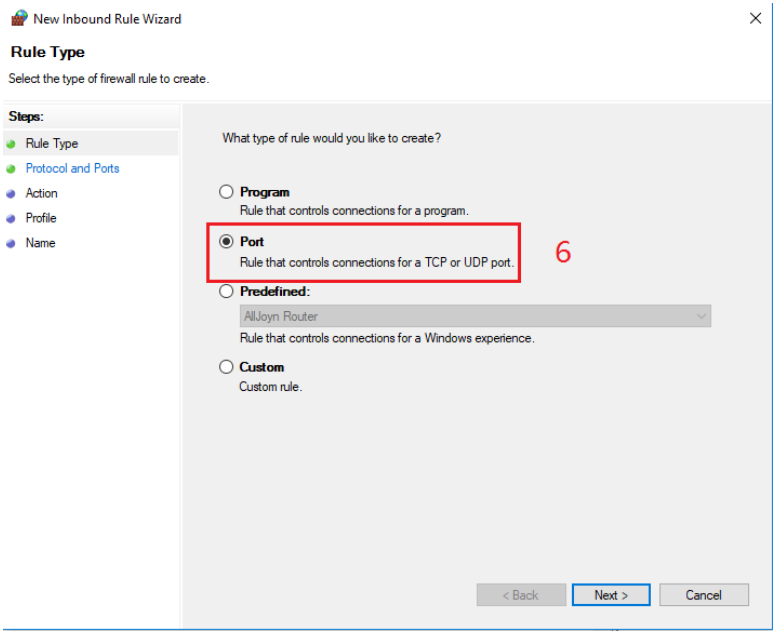


3 Click **Advanced Settings** > **Inbound Rules** > **New Rule**.

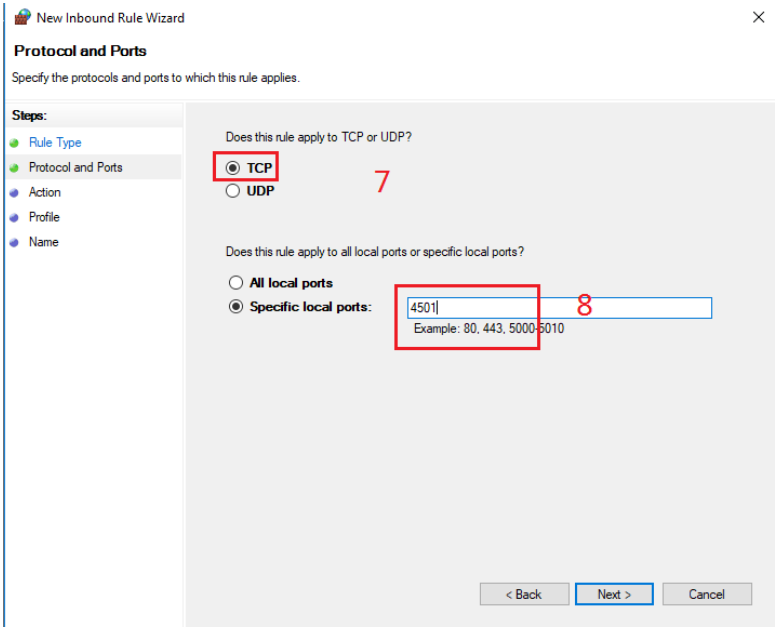




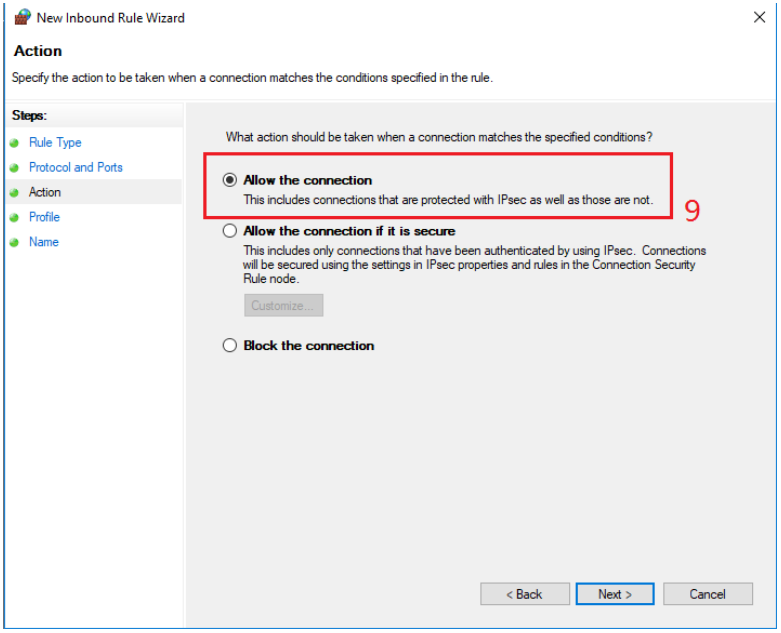
4 Click **Rule Type** > **Port**.



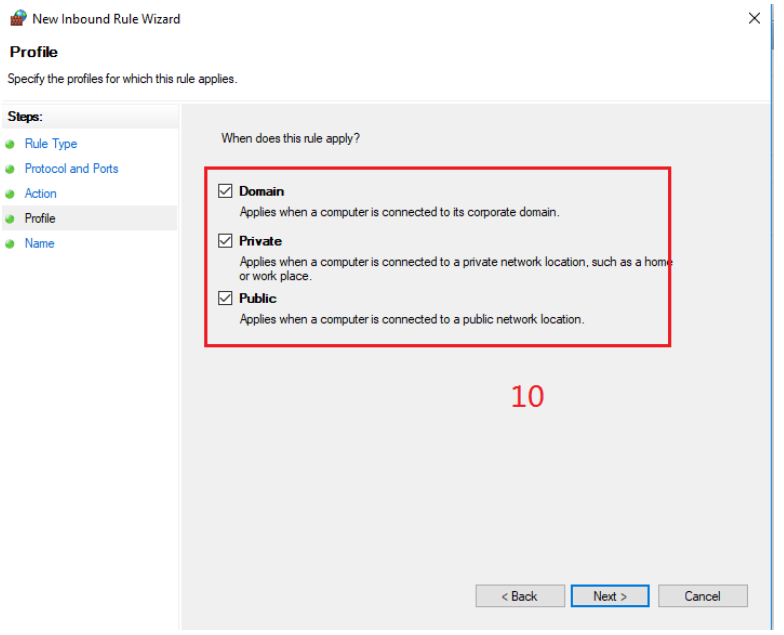
5 Click **Protocol and Ports** > **TCP** > **Set Specific local ports** (e.g. **80**).



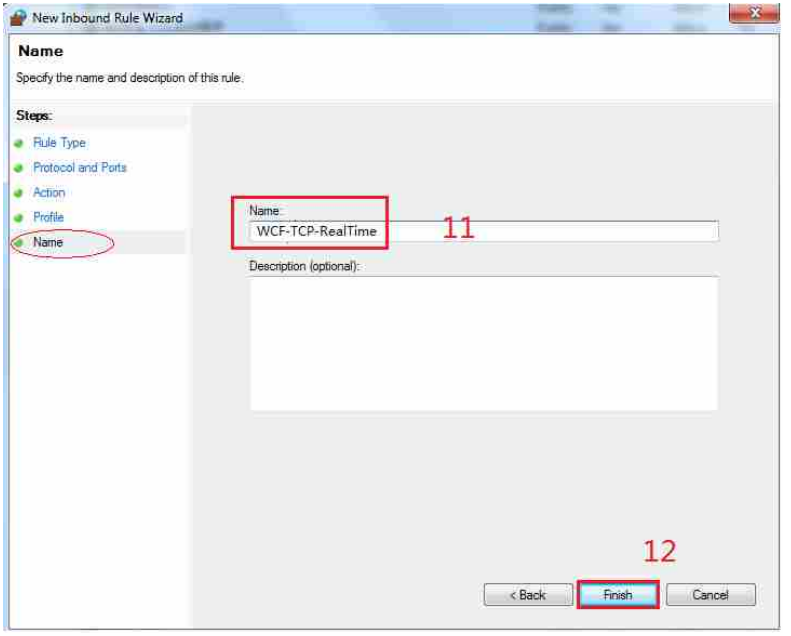
6 Click **Action** > **Allow the connection**.



7 Click **Profile** > tick all options.



8 Set **Name** and click **Finish**.



Key operation of administrator

Authorization

After the successful installation, open CMSClient, login to the service account and select the Authority Management menu to access the interface as shown in Figure 5.1.

1 Add server. Click **Add Server**, input Server IP and add the server. Skip this step if it is not a distributed multi-server environment.

NOTE
Modify the server IP address before the server is activated.

To change the IP address of the server during use, follow the steps below (for example, change the IP from 202.114.4.119 to 202.114.4.223):

- Log in CMSClient of the service, find server whose IP is 202.114.4.119 in authorization list, and change it to new IP 202.114.4.223.
- Change the IP of PC to 202.114.4.223, and restart the Central Server program and CMSClient program.
- In CMSClient login interface, change the CMSClient connection setting to 202.114.4.223.
- Login to the service account, change IP of time server to 202.114.4.223, or keep the default 'IP of Common database' (IP of Common database for the stand-alone version is generally 127.0.0.1).

2 Obtain the authorization files. In the Authority Management interface, as shown in step 2 in Figure 5.1, click **Hardware ID** key to view hardware ID. After accessing the authorized website, input the customer identification code on the customer identification code certificate and the hardware ID to obtain the License file.

NOTE
http://183.47.44.185/HomePage.aspx

The authorized website shall be subject to the customer identification code certificate.

3 Activate the server. After obtaining the authorization file, click **Server Activation**, select the License file, and then click **Activation** key.

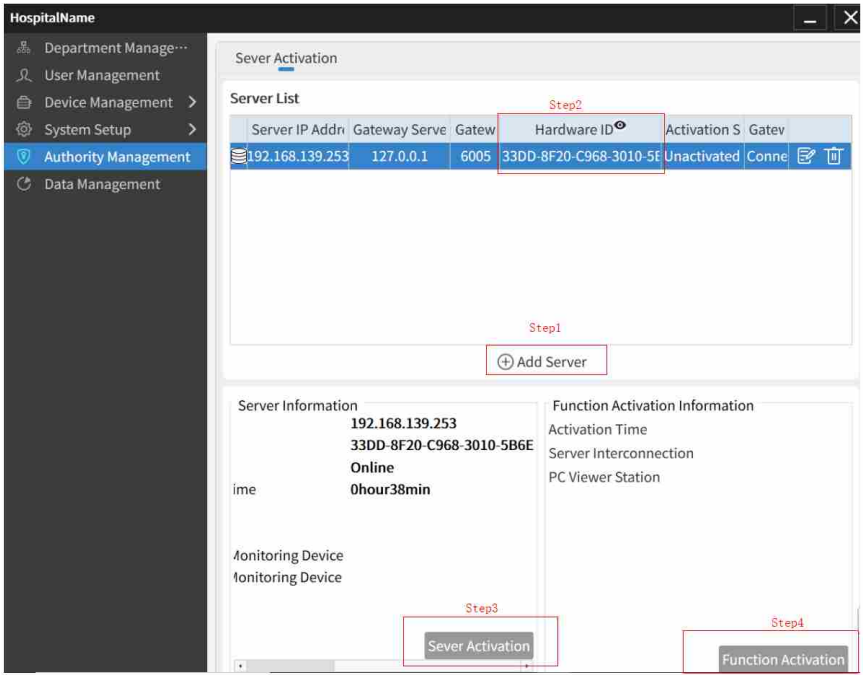


Figure 5.1

Figure 5.2

4 Activate the function. After obtaining the authorization file, click **Function Activation**, select the License file, and then click **Activation** key.

Figure 5.3

For Licence from trial version to official version, if the distributed switch status is from On to Off, strictly follow the steps below:

1 Uninstall Vista CMS 2.0;

2 Uninstall postgresql database;

3 Install Vista CMS 2.0 (including postgresql database).

For other cases of License from trial version to official version, import the License as normal.

Server configuration

Refer to Section *Server configuration* in *Vista CMS Central Monitoring System Instruction for Use*.

Device management

Refer to Section *Device management* in *Vista CMS Central Monitoring System Instruction for Use*.

Department management

Refer to Section *Department management* in *Vista CMS Central Monitoring System Instruction for Use*.

User management

Refer to Section *User management* in *Vista CMS Central Monitoring System Instruction for Use*.

Data management

Refer to Section *Data management* in *Vista CMS Central Monitoring System Instruction for Use*.

This page intentionally left blank

Environment deployment inspection of distributed CMS

Overview

To deploy the distributed CMS environment, perform the following inspections.

Inspecting central server configuration

All configuration items for Central Server in the distributed environment should be inspected. During the inspection, if the configuration is inconsistent as described in this installation instruction, modify it manually and restart service **CMSWindowsService**, **CMSCommonService** as described in Section *Restarting services after installation*.

1 Check Vista CMS installation directory > DCS directory and then find the file DCS.exe.Config.

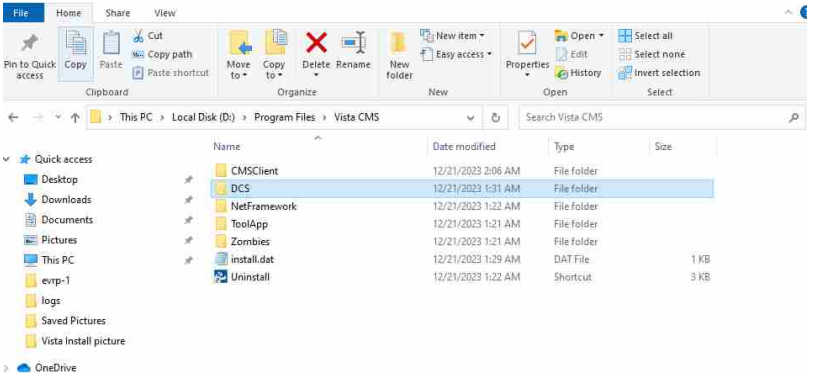


Figure 6.1

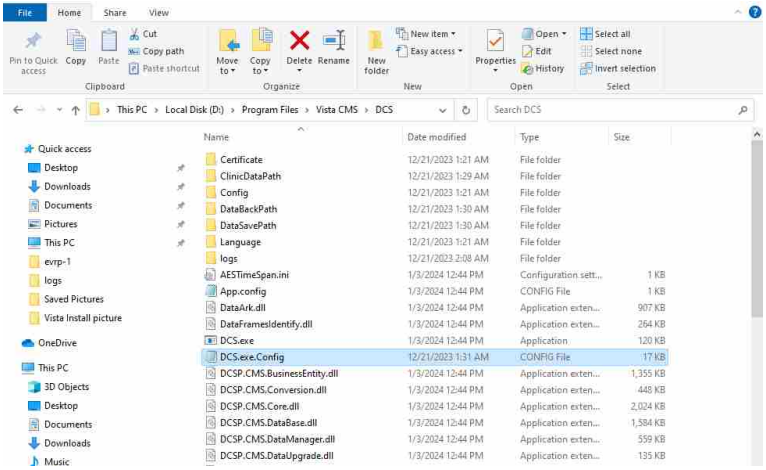


Figure 6.2

2 Inspect configuration file DCS.exe.config.
Check whether the value of the database IP is consistent with the database IP connected with the main Central Server.

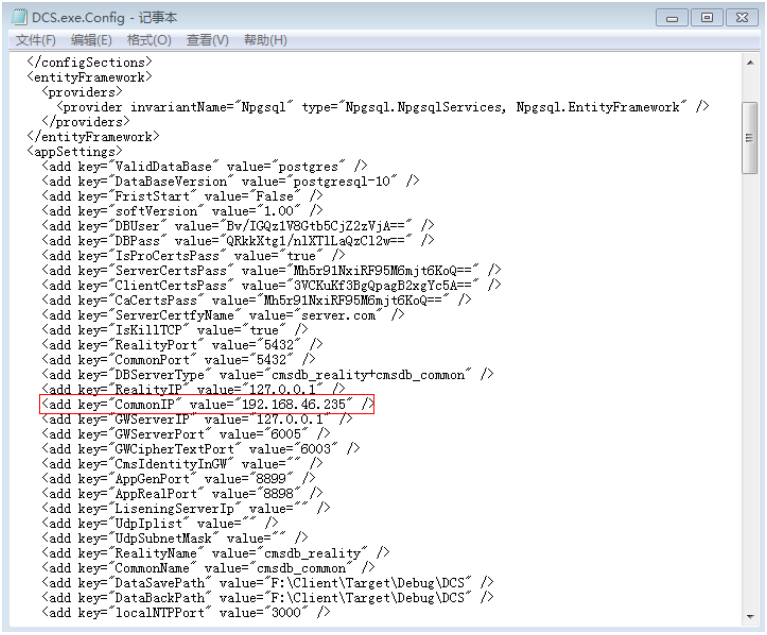


Figure 6.3

Inspecting main database configuration

Only inspect the configuration items for the database to which the main Central Server is connected. During the inspection, if the configuration is inconsistent as described in this installation instruction, modify it manually and restart service **CMSWindowsService**, **CMSCommonService** as described in Section *Restarting services after installation*.

1 Find the computer where main database is installed via the main database IP, and then find the installation directory for database to get the **data** folder.

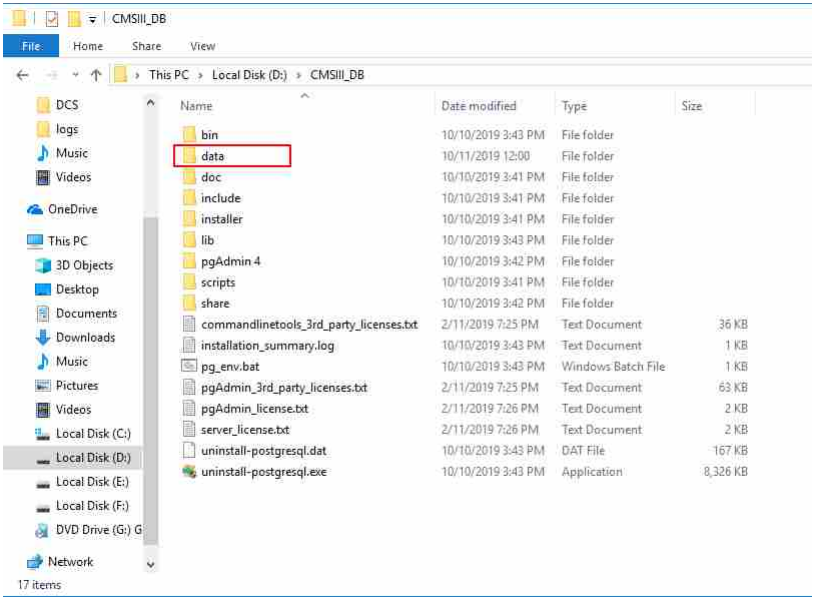


Figure 6.4

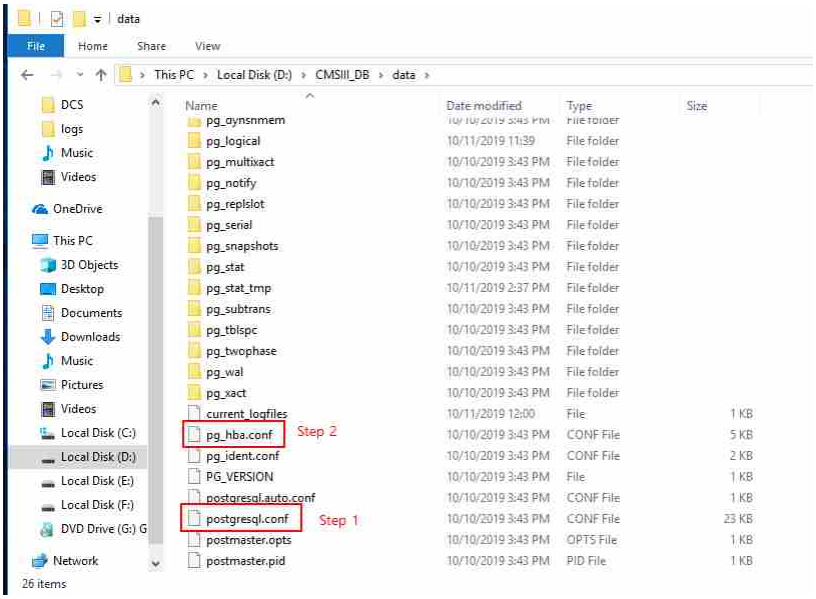


Figure 6.5

2 Inspect file postgresql.conf. In **data** folder, find **postgresql.conf**, open it with text editor, change listen_addresses = 'localhost' to listen_addresses = '*'.

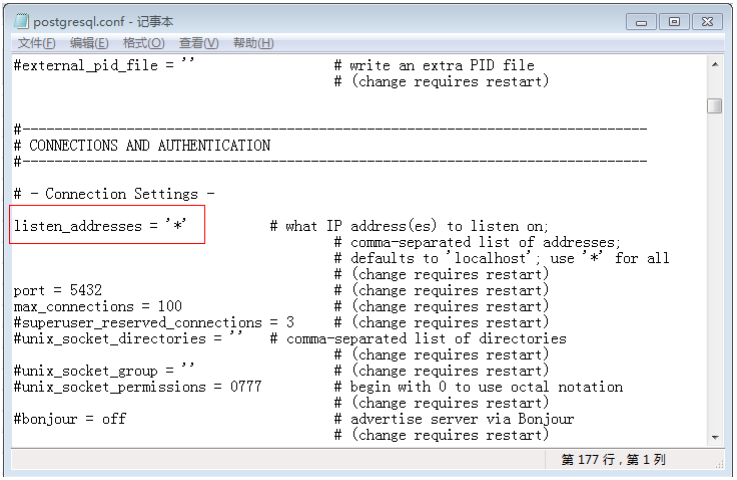


Figure 6.6

3 Inspect configuration of pg_hba.conf. Ensure the value in red box is 0.0.0.0/0.

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD

# IPv4 local connections:
host    all             all             0.0.0.0/0               md5
# IPv6 local connections:
host    all             all             ::1/128                 md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
host    replication     all             127.0.0.1/32            md5
host    replication     all             ::1/128                 md5
```

Figure 6.7

Importing Vista CMS 1.0 database into Vista CMS 2.0

Overview

NOTE
To import data successfully, ensure Vista CMS 1.0 (V1.73&V1.74) databases are not deleted, otherwise, the importing will be failed.

Data preparation

1 In this document, Vista CMS 1.0 (V1.73&V1.74) database is called older database, and 'OldDB_Import.exe' is called data import tool. Find \ToolApp\OldDB_Import in Vista CMS 2.0 installation directory.

2 Backup the older database into a directory, such as 'D:\Psql_Data', and the database file directory is as shown below.

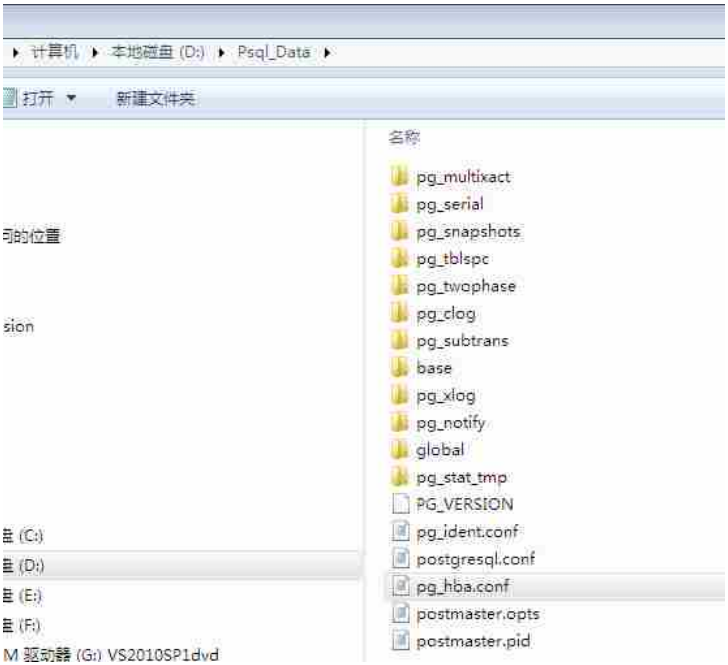


Figure 7.1

3 Open file ‘PG_VERSION’ and record the version of the older database.

- For the older database (V8.3)

  Open configuration file ‘OldDB_Import.exe.config’ for the data import tool, set value for ‘Db83Path’, and configuration path is the directory where Postgres8.3 is installed, such as ‘C:\Program Files\DB_8.3\bin’.

- For the older database (V9.2)

  Open configuration file ‘OldDB_Import.exe.config’ for the data import tool, set value for ‘Db92Path’, and configuration path is the directory where Postgres9.2 is installed, such as ‘C:\Program Files\psql\bin’.

4 Manually set the items in configuration file ‘OldDB_Import.exe.config’.

‘Real-time database process port (RealityPort)’ and ‘configuration database process port (CommonPort)’ should be respectively set as the real-time database (cmsdb_reality) port and common database (cmsdb_common) port on the server side of the computer in the current environment.

5 Items automatically configured by the program: ‘Real-time database IP (RealityIP)’ and ‘configuration database IP (CommonIP)’ are automatically obtained from the configuration file of server side when the tool is running.

‘DataSavePath’ is set as: the configuration item ‘DataSavePath’ in configuration file ‘DCS.exe.config’ of the server side program.

‘DataBackPath’ is set as: the configuration item ‘DataBackPath’ in configuration file ‘DCS.exe.config’ of the server side program.

Search for file DCS.exe.Config in the DCS folder under Vista CMS 2.0 installation directory.

Operating the data import tool

1 Open the data import tool. When importing multiple older databases, the databases must be stored in different file paths; otherwise, the patient information will be lost.

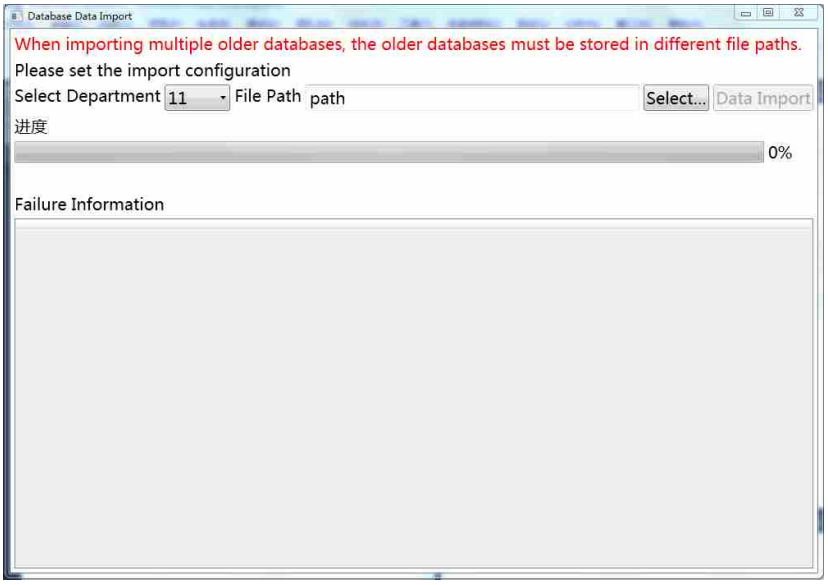


Figure 7.2

2 Click ***Data Import*** to start the importing.

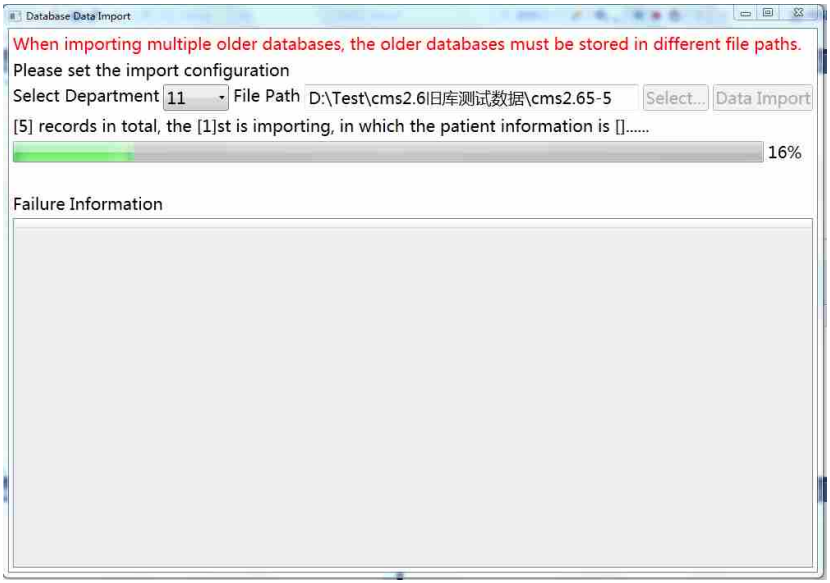


Figure 7.3

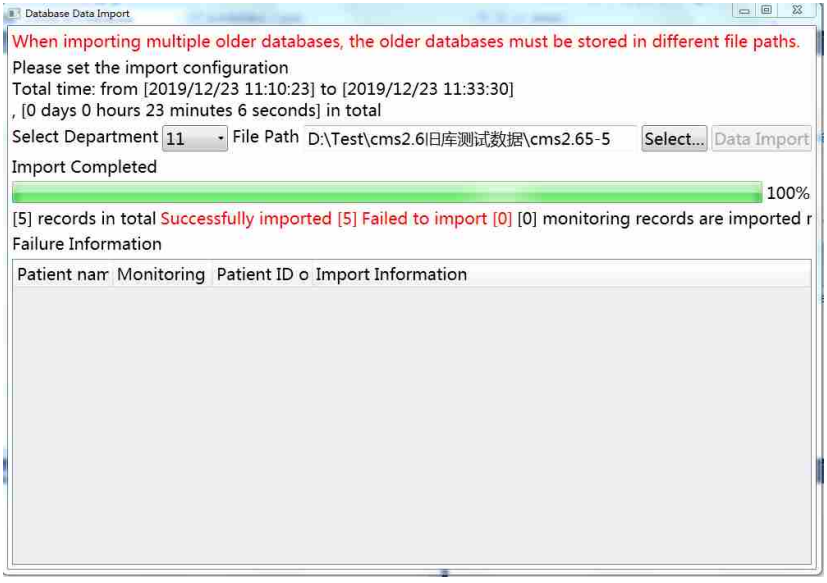


Figure 7.4

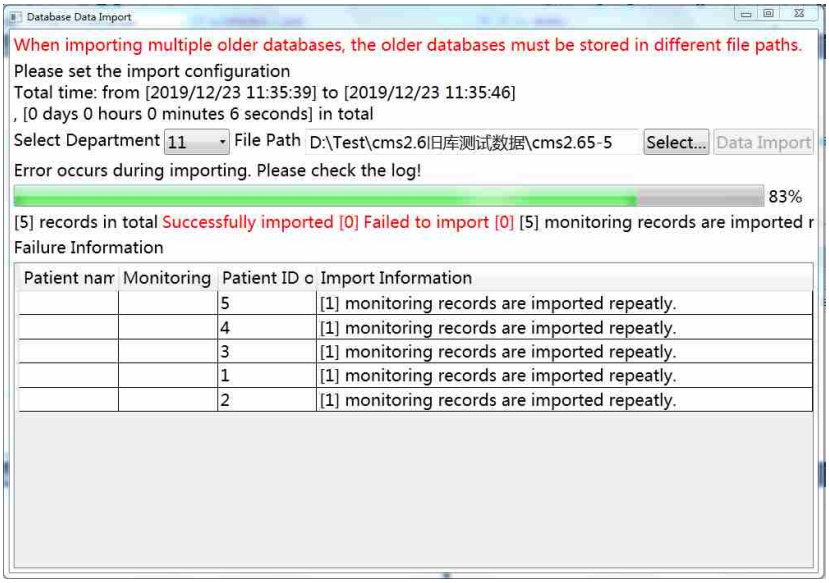

Database Data Import
When importing multiple older databases, the older databases must be stored in different file paths.
Please set the import configuration
Total time: from [2019/12/23 11:35:39] to [2019/12/23 11:35:46]
, [0 days 0 hours 0 minutes 6 seconds] in total
Select Department 11
File Path D:\Test\cms2.6旧库测试数据\cms2.65-5
Select...
Data Import
Error occurs during importing. Please check the log!
83%
[5] records in total Successfully imported [0] Failed to import [0] [5] monitoring records are imported r
Failure Information
Patient nam
Monitoring
Patient ID o
Import Information
5 [1] monitoring records are imported repeatly.
4 [1] monitoring records are imported repeatly.
3 [1] monitoring records are imported repeatly.
1 [1] monitoring records are imported repeatly.
2 [1] monitoring records are imported repeatly.

Figure 7.5

Network deployment of distributed CMS

Terms and definitions

Terms	Definitions	Descriptions
NAS	Network Attached Storage	Network memory, a dedicated data storage server
NIC	Network Interface Card	Network card or network adapter, the hardware for network communication
Central Server	Data Center Server	Data Center Server, the subsystem of Vista CMS 2.0 server side
VLAN	Virtual Local Area Network	Virtual Local Area Network makes the group of devices and users logically in one network segment regardless of physical location restriction.
DHCP	Dynamic Host Configuration Protocol	Protocol of local area network. The server controls a range of IP addresses, and once the client logs in to the server, it automatically gets the IP address and subnet mask assigned by the server.

Network structure

Vista CMS 2.0 is a clinical information system for the patient monitoring and operates within the internal network of the hospital. To ensure network security and stability of the whole system, the network of whole system mainly includes three sub-networks: device access network, clinical information network and external network. The whole network structure is shown as below.

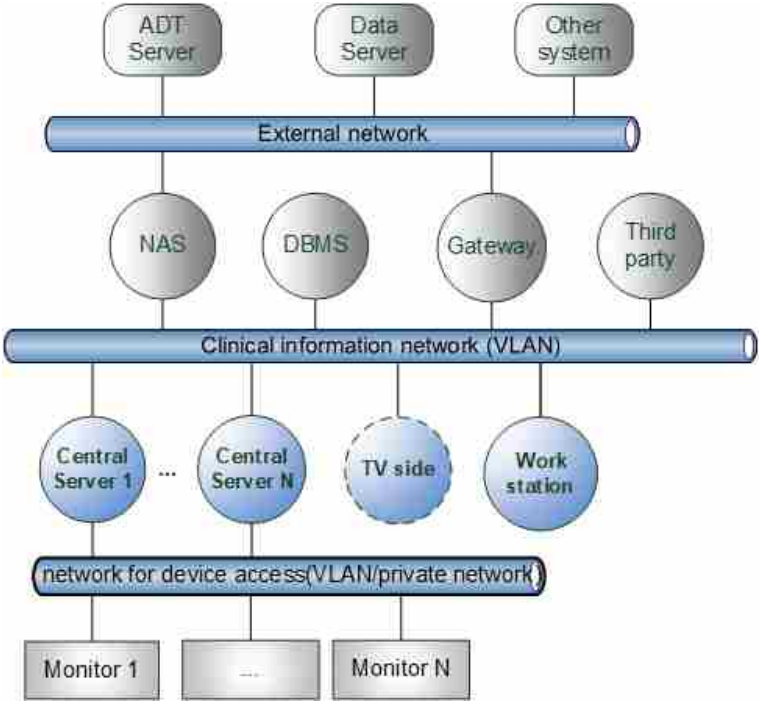


Figure 8.1

Each subnet can be realized by dividing the VLAN on the three-layer switch or by the router. The device access network, clinical information network and external network are separated from each other and cannot exchange visits.

Typical deployment

Stand-alone deployment

The stand-alone network structure is the same as the existing Vista CMS 1.0. Refer to the installation instructions of Vista CMS 1.0 for further information.

Deploying central server in the department

When Central Server is deployed in the department, the whole network topology is shown as below.

- The hospital network, the clinical information network and the device subnet are separated from each other to ensure the data security and network performance of the relevant subnet. They can be separated by independent switches or by VLAN.
- The server where Central Server is located is connected to the monitor through NIC2, and the communication method between Central Server and the monitor is the same as that of Vista CMS 1.0. You can either build your own network or use VLAN provided by hospital to access the device. NIC1 is connected to the VLAN allocated by the hospital for the clinical information network, and uses the IP allocated by the hospital to realize the communication between Central Server and each CMSClient or Gateway.
- Hospital workstations, nurse stations, etc. are deployed in the clinical information network VLAN provided by the hospital. It is recommended to use static IP for system audit of network problems.
- When the client configures Vista 120 Gateway, the corresponding host is connected to the clinical information network through NIC2 to realize data interaction with Central Server, and the internal network of the hospital is connected through NIC1 to realize data exchange between the whole central station network and HIS.

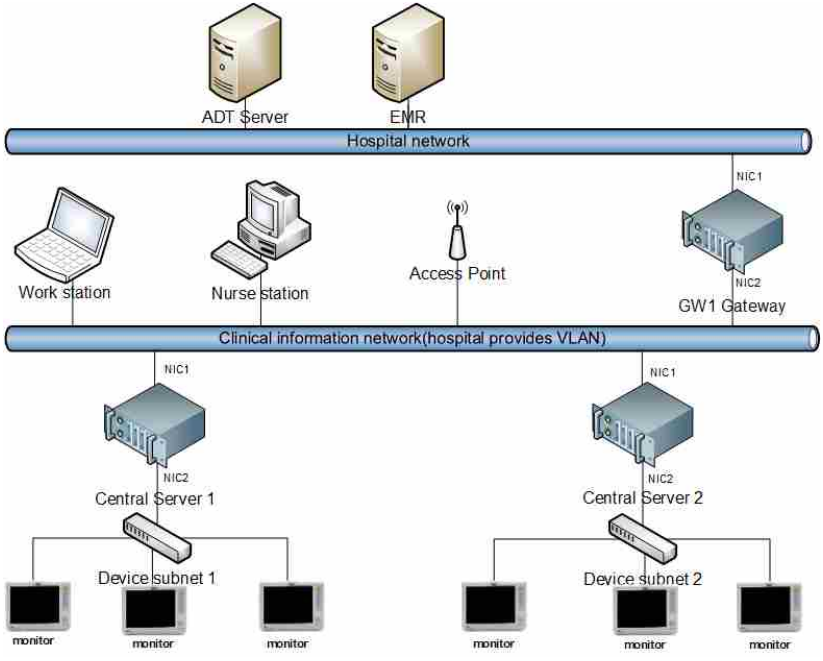


Figure 8.2

NOTE

When Central Server connects to the monitor with the software version that does not support cross-network transmission, it is recommended to use the self-built network. NIC2 can use the default address 202.114.4.119.

NOTE

The number of device subnets shall be controlled according to the number of monitors, which shall not exceed the maximum number of devices allowed by Central Server. If the hospital requires higher stability for Central Server, and the monitor supports automatic switchover of Central Server connection, multiple Central Servers can be accessed in the same device sub-gateway.

Deploying central server centrally within hospital

After Central Server is deployed in the data center, it is basically similar to the network topology deployed in the department, and its features and precautions are basically the same. The main difference is that devices need to access the network with the help of the VLAN provided by the hospital. As shown in the Figure below, on the Central Server, NIC2 connected to the monitor needs to be connected to the device network VLAN provided by the hospital, and all monitors can communicate with Central Server through the VLAN provided by the hospital.

NOTE

Due to the complexity of the hospital network environment, when using the VLAN to realize the communication between the device and the monitor, the monitor is required to support the function of data transmission across network segments (the main feature is that gateway addresses can be configured on network devices). Therefore, the monitor that does not support data transmission across network segments may not be able to access Central Server.

NOTE

Since the VLAN for device access to the network is provided by the hospital, NICe2 address in Central Server and the IP address the monitor used are allocated by the hospital. If the hospital adopts DHCP to assign the address, it is recommended to assign the static address for NIC2 of Central Server.

NOTE

When the NIC2 of the monitor is not in the same subnet as the computer where the Central Server is located, it is recommended to check the Windows routing table to confirm that the communication between the monitor and Central Server is normal, and static routing information may need to be added (refer to Section *How to Verify Network Connection Status* for details).

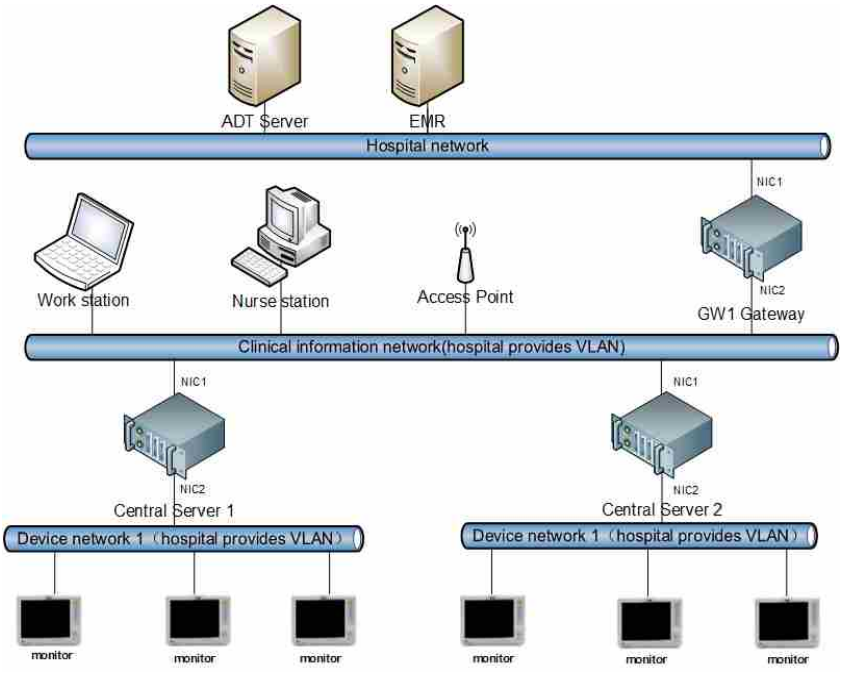


Figure 8.3

Accessing device via self-built Wi-Fi

This method is mainly suitable for hospitals that do not provide wireless network environment. The connection methods of clinical information network and hospital network are the same as the former two connection methods. The main difference is that the communication method between Central Server and the monitor is changed from wired switch to AP (Access Point). For data stability, it is recommended to adopt AC+AP scheme to realize zero roaming coverage of wireless network.

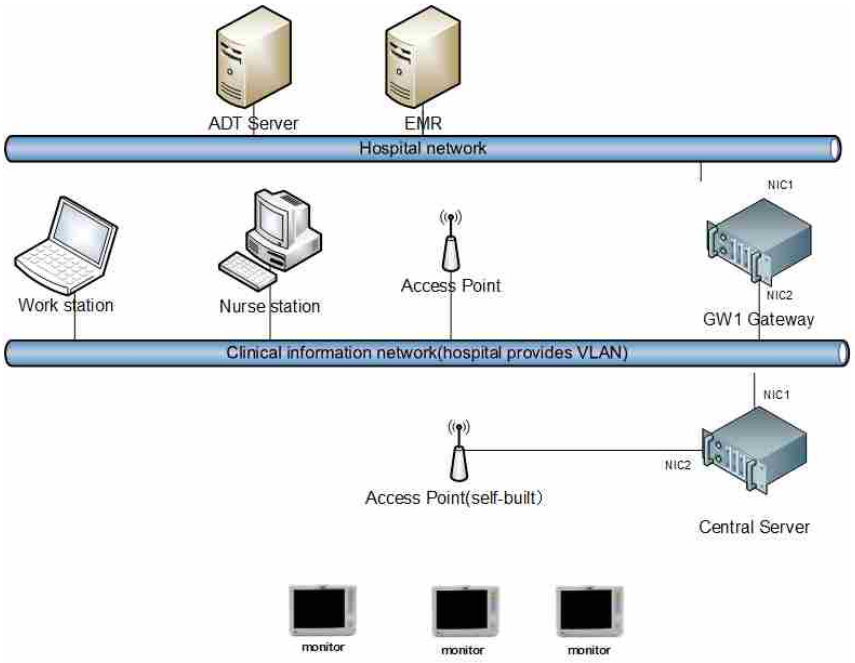


Figure 8.4

Accessing device via hospital Wi-Fi

When accessing the monitor through the wireless network provided by the hospital, it is recommended to configure an independent SSID for monitor access, and isolate the network from other wireless networks to ensure network security and prevent attackers from directly attacking Central Server or the monitor through the wireless network, resulting in data loss or system crash. In this mode, the NIC2 of Central Server shall be connected to the VLAN corresponding to the wireless network of the device.

NOTE

It is recommended to assign a fixed IP address to NIC2, otherwise, the monitor cannot obtain the Central Server address if it is not in the same network segment as Central Server.

NOTE

When the monitor is not in the same network segment as Central Server, the Central Server system may need to configure the static routing table (refer to Section *How to Verify Network Connection Status* for details).

NOTE

Monitors that do not support data transfer across network segments may not be able to access the network environment.

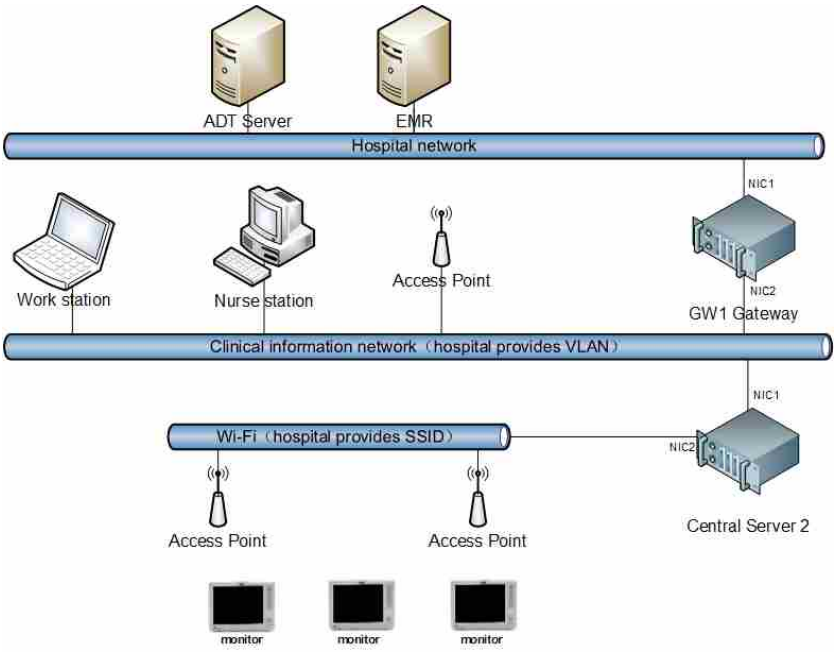


Figure 8.5 Currently Existing Wi-Fi

NOTE
Do not set the wired and wireless IP of the monitor to the same network segment.

Network requirement

Overall system

Basic requirement

- Support 100 Mbps (802.3u), and 1000 Mbps (802.3ab/802.3z) Ethernet.
- The monitoring device should be isolated in a separate VLAN or dedicated network to ensure the stability and security of the network, which should allow ICMP requests.
- The delay between two-layer network nodes tested by ping command is less than 50 ms.
- The delay between three-layer network nodes tested by ping command is less than 100 ms.
- The average RTT is less than jitter 5%.

NOTE
Gigabit switches are recommended for Central Server.

NOTE
It is recommended to use laptop to verify the network environment.

8.4.1.2 Switch

- Support Port Fast, RPVST+, MSTP/RSTP or other equivalent network loopback avoidance, network device redundancy and VLAN protocols.
- The switch that supports 1000 M Ethernet should support Jumbo Frames.
- Each port in the switch can be manually configured or automatically negotiated to have a separate connection rate and duplex state.

Wi-Fi device requirement

Suggested selection

- Cisco or H3C network equipment is recommended to ensure network stability.
- Three-layer switch H3C S5500 or other products with higher performance and stability.
- Wireless controller (Access controllers) AIR-CT2504 or other products with higher performance. Software version should be above 7.6.130.
- The wireless controller turns off the function of IP-MAC matching.
- Layer 2 switches connected to AP support Ethernet for power supply (PoE), avoiding massive power demand, such as using WS-C2960-24PC-S.

FAQ

How to verify network connection status

The ping command can be used to test network connection. During the test, the ping delay between the current computer and the target node should be less than 50 ms.

Although the monitor does not support network bandwidth test, two laptops instead of monitors can be used to perform network bandwidth test. One laptop turns on file-sharing mock dump server, and the other laptop shares directory to upload files via the network. Peak traffic of 100 M on the Ethernet can reach 70-80 Mbps, which shows that the network is in good condition.

How to increase the static routing table configuration

When Central Server uses dual network adapters, and if Central Server, monitor and third party system are in the different network segments, Windows may not be able to recommend a normal routing table, resulting in network communication failure. In this case, you need to manually add static routing information to Windows to solve the network communication problem. Here is a dual network adapter configuration scenario for Central Server to illustrate how to add static routing information.

Central Server network adapter configuration information:

NIC 1 IP: 192.168.51.130/24, gateway: 192.168.51.1

NIC 2 IP: 192.168.50.20/24, gateway: 192.168.50.1

IP address segment of the monitor: 192.168.0.1/24

IP address of Vista 120 Gateway: 192.168.202.20/24

Since Central Server has two network adapters and two gateway addresses configured at the same time, static routing information needs to be added to determine which network adapter the different network addresses interact with:

Open the command prompt (CMD) as an administrator and first check the routing information that Central Server is added to the monitor.

route add -p 192.168.0.0 mask 255.255.255.0 192.168.50.1

and then, add Central Server - Vista 120 Gateway route

route add -p 192.168.202.0 mask 255.255.255.0 192.168.51.1

The route print command can be used to verify that the static routing information has been configured successfully.

To verify the validity of the configuration, check the network routing information by the tracert command.

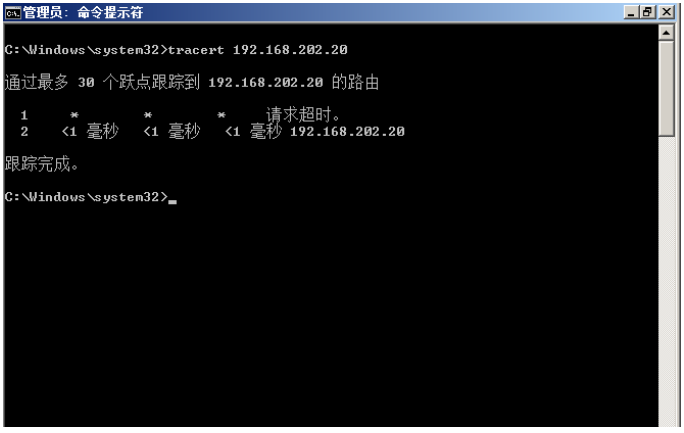


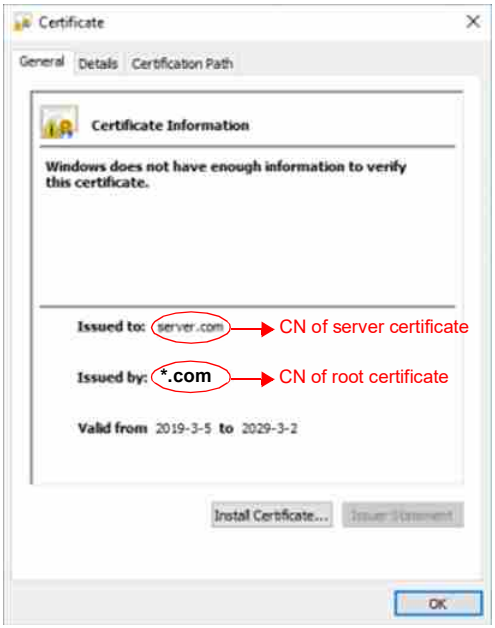
Figure 8.6

Replacing digital certificate

NOTE
The certificates issued by Certificate Authority (CA) is recommended and self-signed certificate should be avoided.

Server

1. Copy the new certificate to Vista CMS\DCS\Certificate in the running directory and Vista CMS\ToolApp\CMSCommonService\Certificate folder. Modify the certificate name, root certificate to ca.crt, server certificate to server.p12, client certificate to client.p12, client verification certificate to client.crt, and server verification certificate to server.crt. Client.key and server.key are the key files that need to be associated with the crt files.
2. If the server certificate CN (CommonName) is the same as the old certificate, manually delete the old certificate in the digital certificate console, refer to Section *Manually deleting digital certificate*. The CN of the certificate is the common name in the subject (Subject) of the digital certificate, which can be viewed in the general or detailed information tab of the digital certificate. For instance, the server certificate server.crt is under the Certificates folder of the server's running directory, open this directory and double-click server.crt, as shown below:



server.com is the CN of server certificate. *.com is the CN of the root certificate (CA), which is the certificate that needs to be deleted.

3 Update dcs.exe.config file in the DCS directory and CMSCommonService.exe.config file in the CMSCommonService directory:

```
  <!--证书密码是否加密-->
<add key="IsProCertsPass" value="true" />
<!--服务端证书密码-->
<add key="ServerCertsPass" value="Mh5r91NxiRF95M6mjt6KoQ==" />
<!--客户端证书密码-->
<add key="ClientCertsPass" value="3VCKuKf3BgQpagB2xgYc5A==" />
<!--CA证书密码-->
<add key="CaCertsPass" value="Mh5r91NxiRF95M6mjt6KoQ==" />
<!--服务端证书认证的名称-->
<add key="ServerCertfyName" value="server.com" />
```

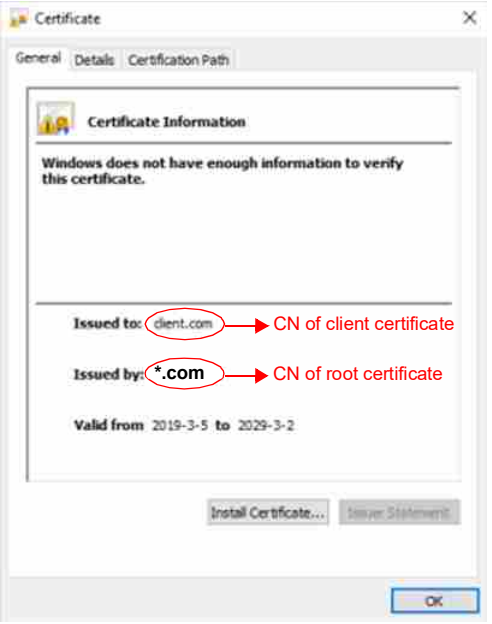
- Check if the IsProCertsPass node is encrypted by the certificate password. If true, the following two certificate passwords fill in the encrypted password string, otherwise fill in the plaintext password.
- If the CN of the certificate changes, the ServerCertfyName and ClientCertfyName nodes are updated to the CN of the new certificate, the ServerCertfyName is changed to the CN of the server, and the ClientCertfyName is changed to the CN of the client.

4 Restart the DCS server.

Client

1 Copy the new certificate to Certificate folder (Vista CMS\CMSClient\Certificates) in the running directory. Modify the root certificate to ca.crt, server verification certificate to server.crt, client certificate to client.p12.

2 If the server certificate CN (CommonName) is the same as the old certificate, manually delete the old certificate in the digital certificate console, refer to Section *Manually deleting digital dertificate*. Meanwhile, modify AppSettings ServerCN and ClientCN values. Likewise, view client certificate CN by opening client.crt file. The client.crt file is under the Certificates folder of the client's running directory, double-click server.crt, as shown below:



3 Update AppSettings file:

```
<!--服务端证书认证的名称-->
<add key="ServerCN" value="server.com"/>
<!--客户端证书认证的名称-->
<add key="ClientCN" value="client.com"/>
<!--是否双向认证-->
<add key="ClientCertRequired"  value="true"/>
<!--证书密码是否加密-->
<add key="IsProCertsPass" value="false" />
<!--客户端证书密码-->
<add key="ClientCertsPass" value="r62rMSc3vU8XtS2I6TNn+Q=="/>
<!--CA证书密码-->
<add key="CaCertsPass" value="EsuV8/xjyPGjEMW4koW88Q=="/>
```

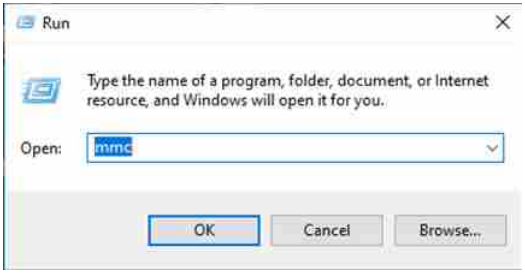
- If the CN of the certificate changes, update the ServerCN and ClientCN nodes.
- Generally, there is no need to modify the ClientCertRequired node, default to bidirectional authentication.
- Check if the IsProCertsPass node is encrypted by the certificate password. If true, the following two certificate passwords fill in the encrypted password string, otherwise fill in the plaintext password.

4 Restart the client.

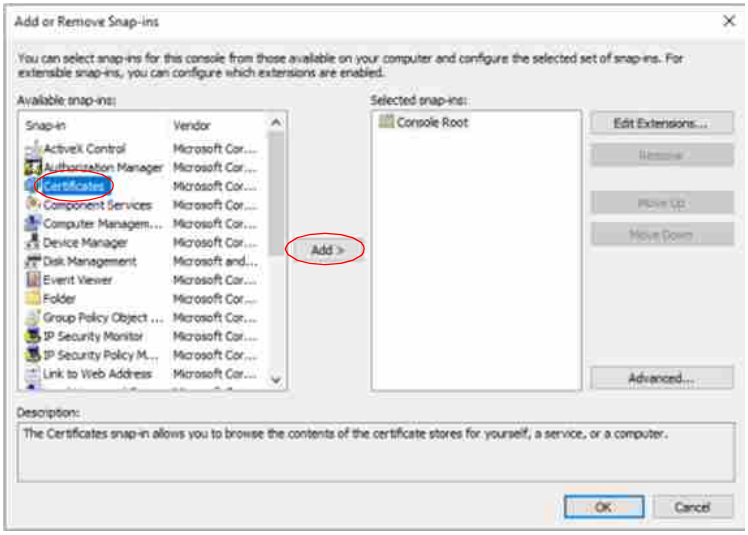
Manually installing digital certificate

The software will read the certificate under the Certificates for automatic installation by default, but in some cases (for instance, automatic installation is forbidden by the anti-virus software), the installation will fail, thus the user can try to install the certificate manually.

Open the digital certificate console: Start > Run > MMC > Enter, open Microsoft console.



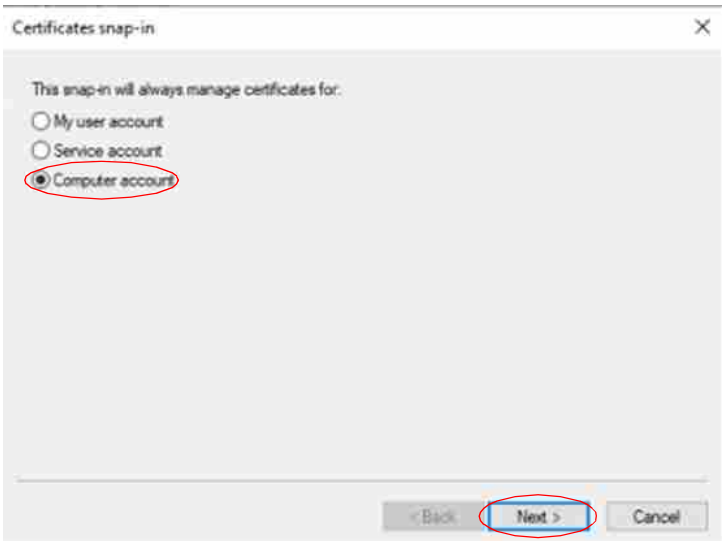
File > Add/Remove Snap-ins, select Certificate under Available Snap-ins, click Add:



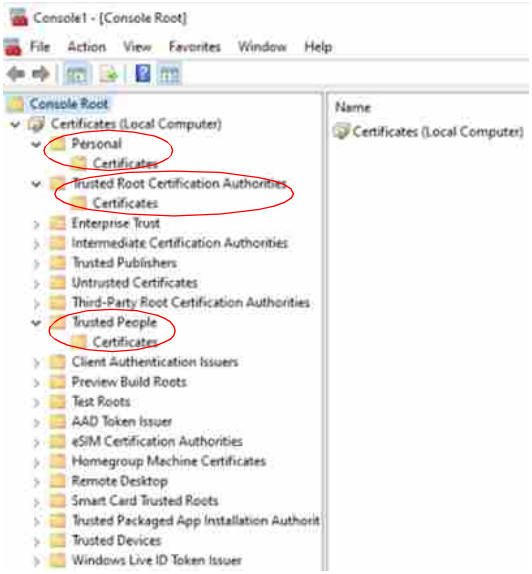
The certificate here is stored in the local, so select Computer Account and click Next.

To manage a certificate for a local computer, click Local Computer and then click Finish.

To manage a certificate for a remote computer, click Another Computer, then type the name of that computer, or click Browse to select the computer name, and then click Finish.



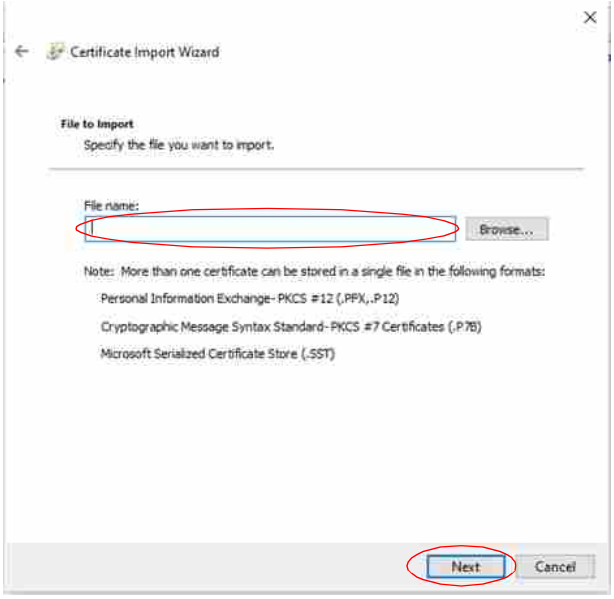
Unfold the certificate node, as shown below:

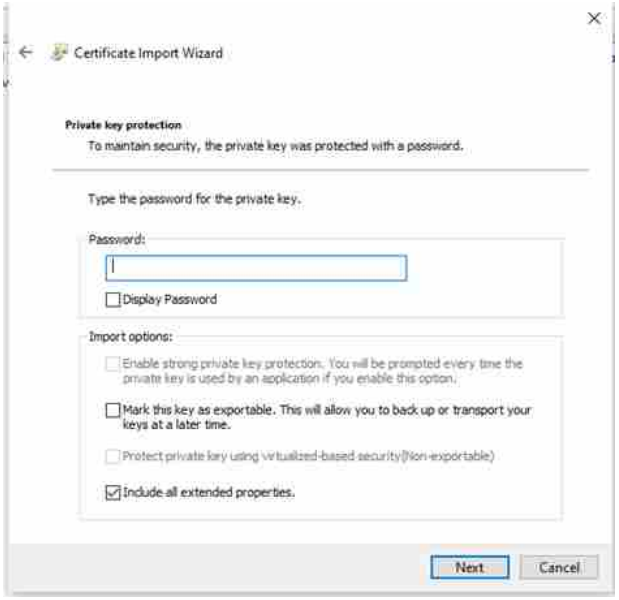


- Select Personal > Certificate directory, right click > All Tasks > Import, open the certificate import wizard dialog box and install the server.p12 and client.p12 certificates according to the certificate import steps.
- Select Trusted Root Certification Authorities > Certificate directory, right click > All Tasks > Import, open the certificate import wizard dialog box and install the ca.p12 certificate or ca.crt certificate according to the certificate import steps.
- Select Trusted People > Certificate directory, right click > All Tasks > Import, open the certificate import wizard dialog box and install the server.crt and client.crt certificates according to the certificate import steps.

The certificate import steps are as shown below:

Click Next to select the path of the certificate:



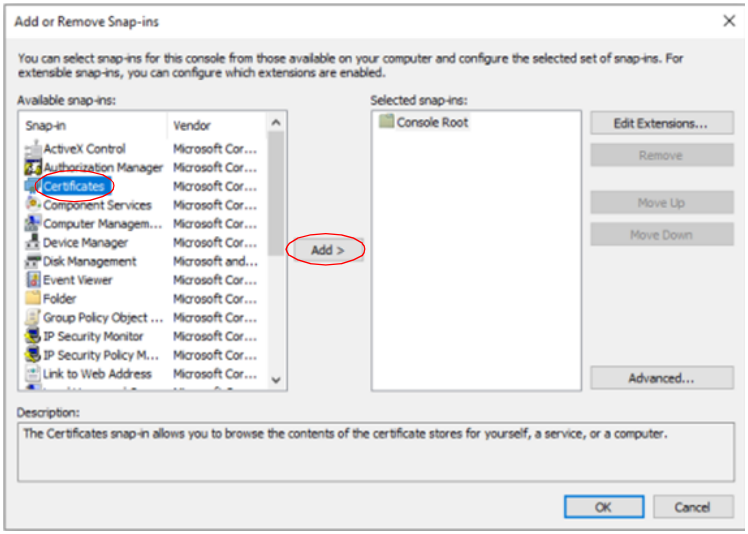


Click Next. If it is p12 certificate, you need to enter the password of the private key and click Next until the installation is completed.

Manually deleting digital certificate

Open the digital certificate console: Start > Run > MMC > Enter, open Microsoft console.

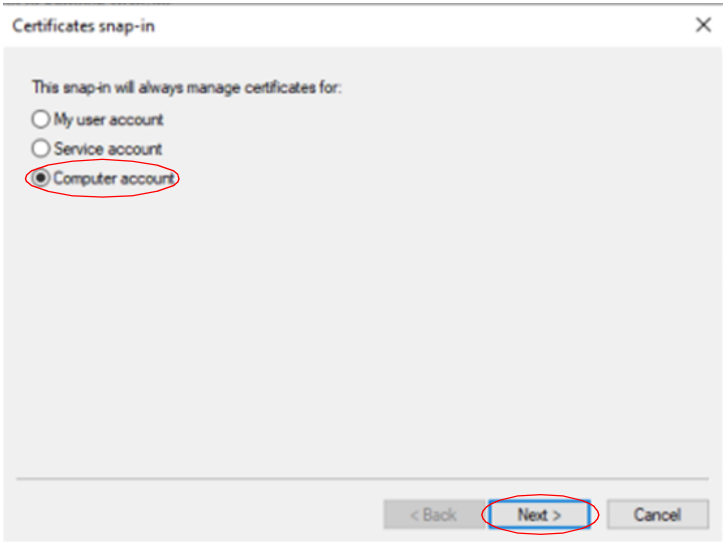
File > Add/Remove Snap-ins, select Certificate under Available Snap-ins, click Add:



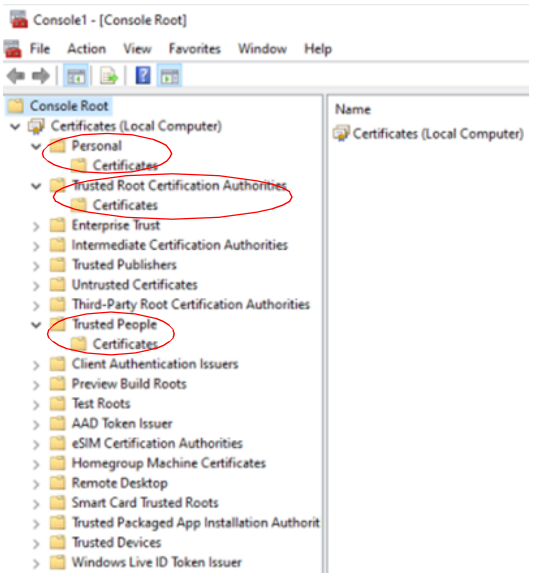
The certificate here is stored in the local, so select Computer Account and click Next.

To manage a certificate for a local computer, click Local Computer and then click Finish.

To manage a certificate for a remote computer, click Another Computer, then type the name of that computer, or click Browse to select the computer name, and then click Finish.

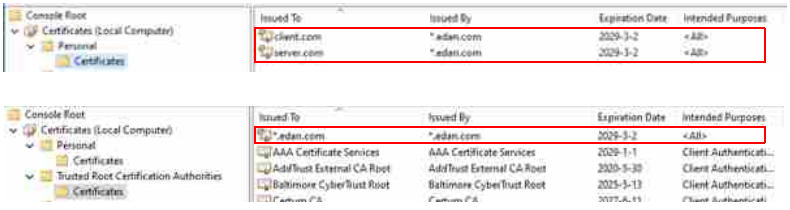


Unfold the certificate node, as shown below:



Open the personal, trusted root certification authorities, trusted people directory in turn, delete the old certificate. The name of the old certificate is as follows:

The certificate in the directory of the trusted root certificate issuer is the CA certificate. The name of the CA certificate is the issuer of the client and server certificate. If the name is the same as the current version of the certificate, delete the following five certificates as shown below:



NOTE

If the server certificate is replaced, consider replacing the mobile and monitor digital certificate synchronously.

This page intentionally left blank

Manufacturer:

Shanghai Dräger Medical Instrument Co., Ltd.
3#, No. 229, HuPo Road, Shanghai International Medical Zone
Pudong New Area, 201321 Shanghai
PEOPLE'S REPUBLIC OF CHINA
+86 21 3108 6000
FAX +86 21 3108 6001
http://www.draeger.com

EC REP

Drägerwerk AG & Co. KGaA
Moislinger Allee 53-55
23542 Lübeck
Germany

+49 451 8 82-0
FAX +49 451 8 82-20 80
http://www.draeger.com

2680250 – GA 6498.020 en

Edition: 3 – 2024-09

2 6 8 0 2 5 0