CDMS 6.0
User Manual

Centerm Information Co., Ltd.

Contents

Preface

Thanks for choosing our Centerm desktop management system software. This product is independently designed and developed by Centerm Information Co., Ltd. Please carefully read this manual before using this product.

If you have any doubt, please consult our local customer service office or call our headquarters: 86-591-28053888.

Copyright notice

Centerm Information Co., Ltd. has the right of final interpretation and revision of this manual. The content in this manual (including all pictures and words) is subject to change without further notice.

1. Product Introduction

1.1 Product overview

Centerm desktop management system is a desktop management system based on Browser/Server developed by Centerm Information Co., Ltd. and supports the remote management operation of clients and peripherals produced by Centerm Information Co., Ltd. The remote monitoring and management can save a lot of operation and maintenance costs for enterprises and finish the management operation with high efficiency.

Centerm desktop management system mainly has following five modules:

- Client management: the module is used for client management operation. The manageable clients include thin client, Mobile Terminal and PC;
- Peripheral management: manage the peripherals produced by Centerm;
- Task statistics: display the task statistics view executed by current system and distributed to clients or peripherals;
- Audit management: audit the operation logs of managed devices and the logs related to current system;
- System setting: configure some parameters of system.

1.2 Product characteristics

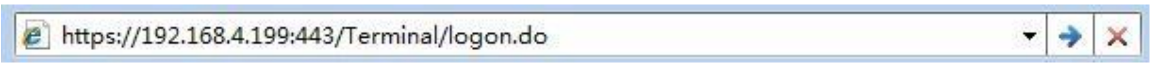
- Rapidly configure the device attributes;
- Install and update the application software by batch;
- Monitor the device operation situation in real time;
- Make the management plan and automatically and regularly execute the specific management operation without the need of manual intervention.

2. Quick Start

2.1 Enter system

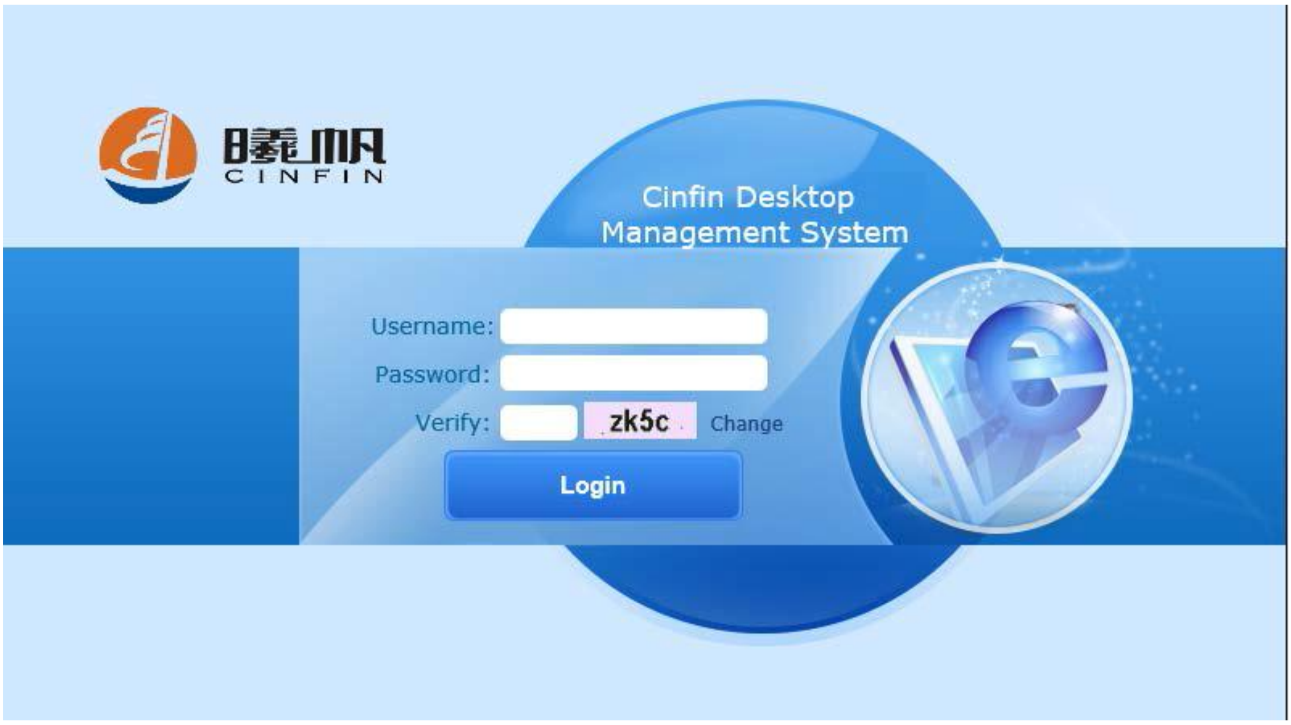
After installing Centerm desktop management system, log in system by following modes.

1. Open the browser and input the management server IP and the using port in address bar, as shown in following figure. Notice: the address prefix is “https://”.

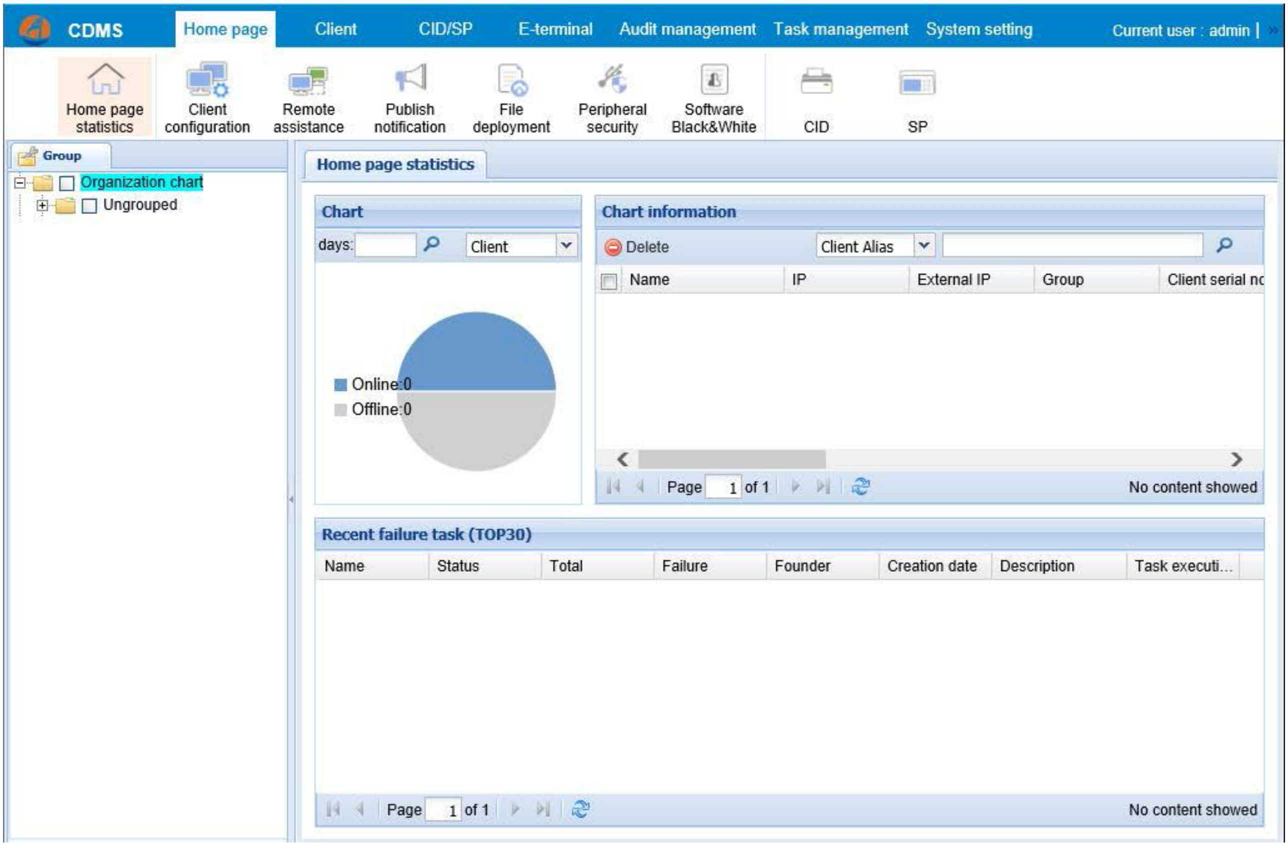


https://192.168.4.199:443/Terminal/logon.do

2. On the login interface, input the username and password. At the first time of login, log in with the default super administrator. The username and the password are admin and admin respectively.



3. At the first time of login, change the password to ensure security. After correct login, main interface of the system is shown in following figure:

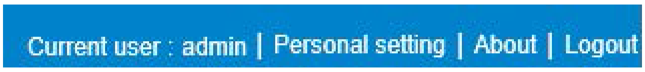


Name	IP	External IP	Group	Client serial nc

Name	Status	Total	Failure	Founder	Creation date	Description	Task executi...

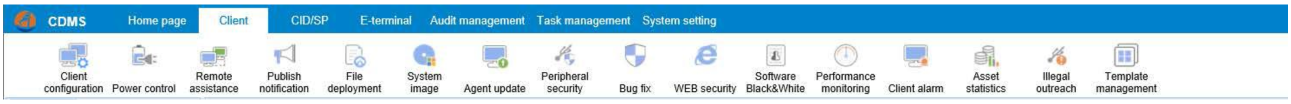
The main interface shows the statistical charts, the detailed information of chart and the last 30 failed tasks of system management device. On the interface, the statistics types include client, SP, CID and MTerminal. Client statistics includes general terminal and Mobile Terminal (because Mobile Terminal belongs to terminals). Select the sector graph module in the chart to screen the information displayed in the right list (online/offline).

4. The navigation bar is on the top of system interface. Upper right shortcuts provide user logout, authorization information view, personal settings and other functions.



Current user : admin | Personal setting | About | Logout

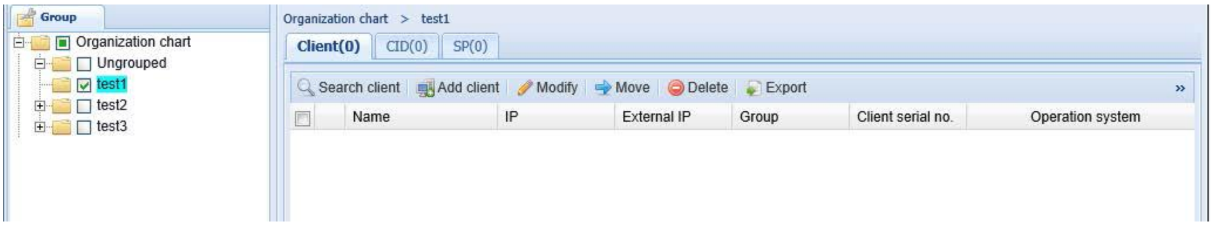
The icons on the navigation bar will classify all functions of the system. The administrator can enter the corresponding functional module for operation by selecting the menu option.



Note: CDMS6.0 management system supports the following browsers: IE7/8/9 (32bits), Chrome and Firefox.

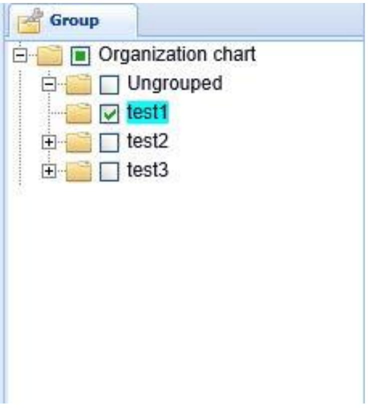
2.2 Device management

1. Enter the device management module.

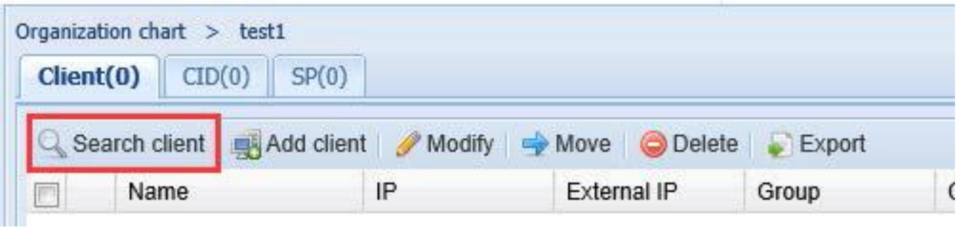


□	Name	IP	External IP	Group	Client serial no.	Operation system

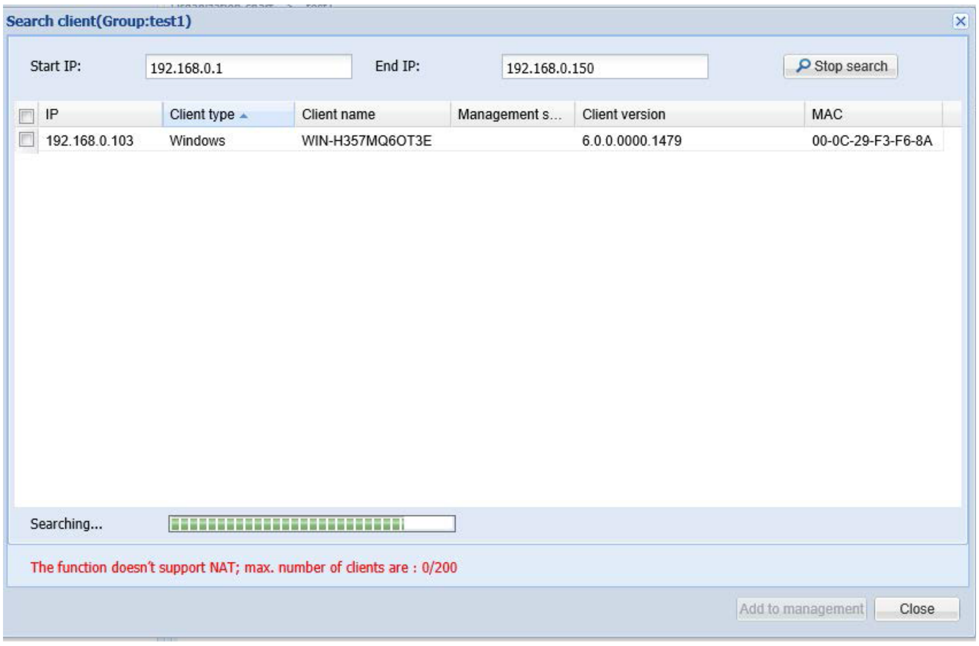
2. Create the organization structure of enterprise in the left grouping tree.



3. Select the grouping of device to be added and click the “search client” button on the right panel.



4. Fill in the searched IP range on the popup panel and click the “start search” button.


Search client(Group:test1)

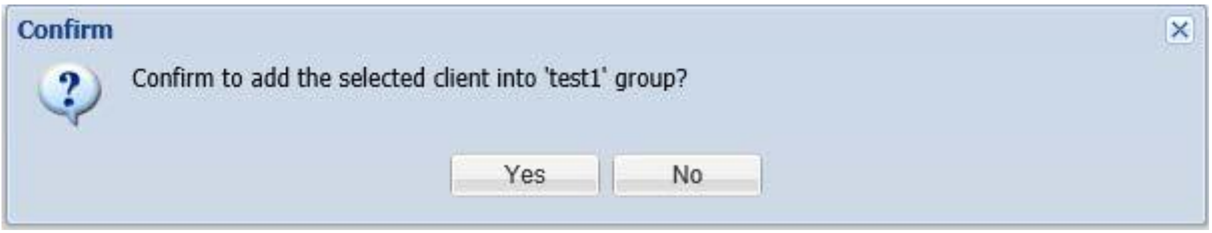
Start IP: 192.168.0.1 End IP: 192.168.0.150

□	IP	Client type	Client name	Management s...	Client version	MAC
□	192.168.0.103	Windows	WIN-H357MQ6OT3E		6.0.0.0000.1479	00-0C-29-F3-F6-8A

Searching...

The function doesn't support NAT; max. number of clients are : 0/200

5. Select the client to be added, click the “add to management” and click “Yes” to finish the adding operation.


Confirm

Confirm to add the selected client into 'test1' group?

6. The user will see the added client in the list for clients on the right panel, as shown in following figure; besides, the peripheral currently accessed to the client will be added in the corresponding classification list.

3. Device and Group

3.1 Group

The system provides management of client groups, can automatically create the client group, and classify the client groups for convenient management. The client group can avoid repeated and complicated operation of user. For example, in batch operation without grouping, the user shall manually select many clients. Many clients with the same type are included in one group to classify the clients more clearly and to facilitate the batch operation of clients.

3.1.1 Classification of groups

The system has 3 types of groups in total:

- No grouping

The client actively specifies the management server to make the management server receive the join request; the client and its peripherals are called non-grouped device. The non-grouped device cannot be modified or changed by user.

- Custom group

It refers to the group created by user. The device in the group can be moved or added by user; the custom group can only be created in the device management module.

- Search group

The user specifies search conditions and the system will automatically select the device which meets the conditions from the custom group to form the group. The search groups for different devices shall be created separately; the search group of clients can only be created in the client management module; the search group of peripherals can only be created in the peripheral management module.

3.1.2 Add custom group

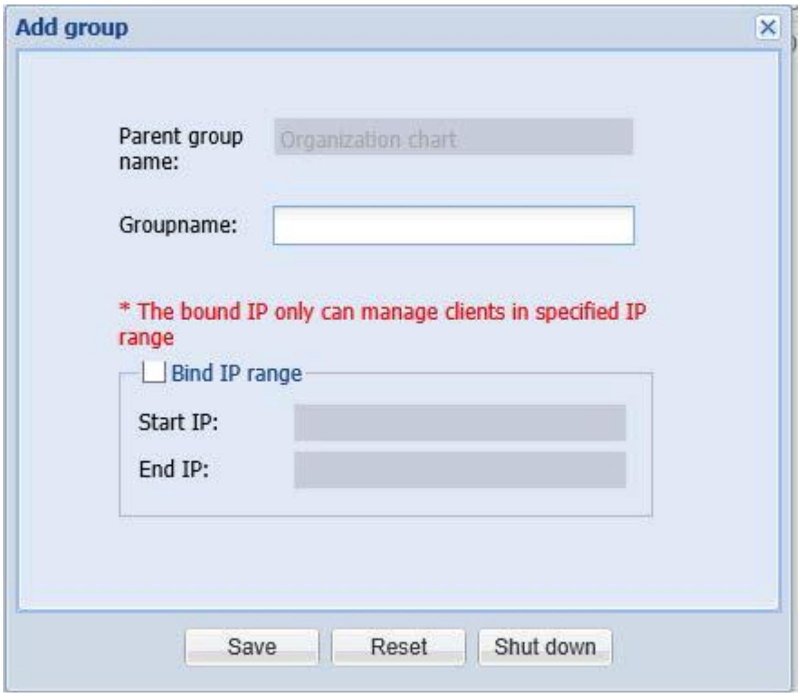
1. Enter the device management module;

2. Right click on client group on “client group” panel on the left side of interface;

3. Select “add group” to pop up the corresponding dialog box;

4. Input the group name in “group name” column;

5. If the IP range of client shall be bound, select “bind IP range”. After editing, click “save”.



Add group

Parent group name: Organization chart

Groupname:

* The bound IP only can manage clients in specified IP range

☐ Bind IP range

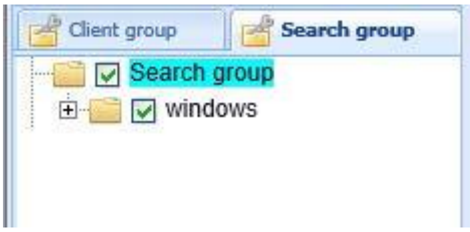
Start IP:

End IP:

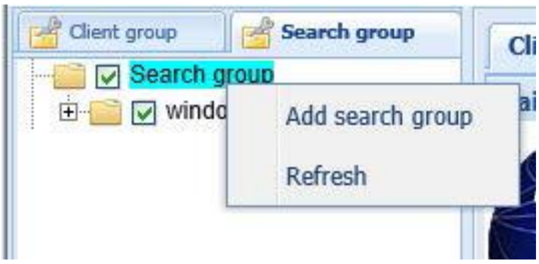
3.1.3 Add search group

Here is an example of adding a client search group. Its adding steps are same with that of adding the peripheral search group.

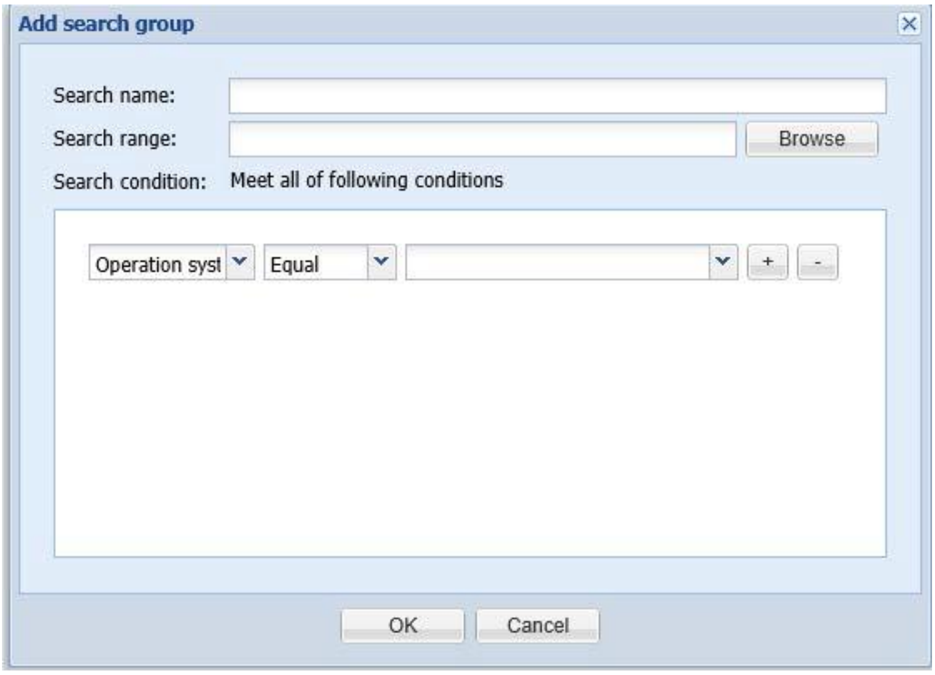
1. Enter any management module in “client management” submenu to display “search group” tab page on left panel;



2. Click to enter the “search group” tab page, right click on root node and select the “add search group”;



3. Select the corresponding search conditions in the popup dialog box;



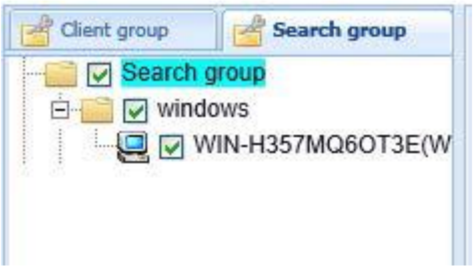
Search name:

Search range:

Search condition: Meet all of following conditions

Operation syst | Equal

4. Then, return to search group panel. The system will automatically display the client which meets conditions in the group;



Notice:

- The data of search group will not be refreshed in real time and only can be updated in manual refreshing.

3.2 Device management

The device management is specially used for creation of enterprise organization structures, management of clients and peripherals, etc.; therefore, clients and peripherals can only be added, deleted, changed and viewed in this module.

3.2.1 Search client

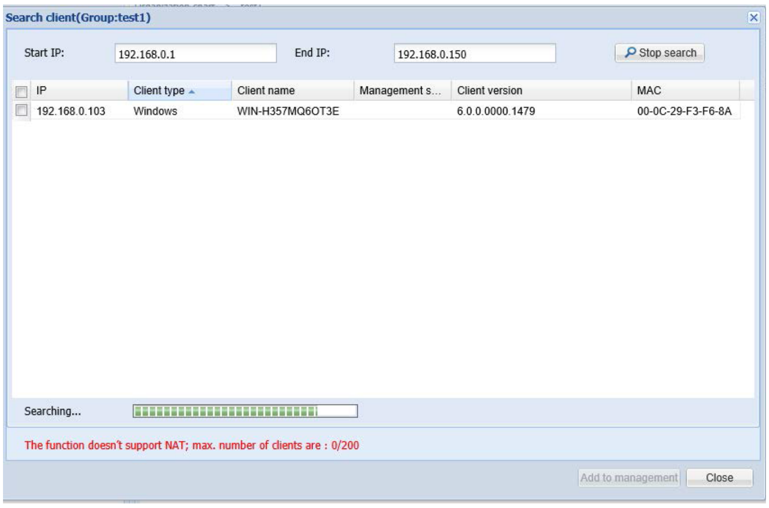
The "search client" function realizes search and adding the managed client and viewing the management situation of clients in the specified network without the need of check of each client (the client shall be installed with client Agent software).

When the client is added in management, the peripherals accessed to this client will also be added in management without the need of extra operation of adding peripherals.

1. Enter the "device management" module;

2. Select the "search client" on the right panel;

3. The search dialog box will pop up, as shown in following figure. Input the searched IP range (if the IP range isn't inputted, the system will directly search the network segment of the server);



Search client(Group:test1)

Start IP: 192.168.0.1

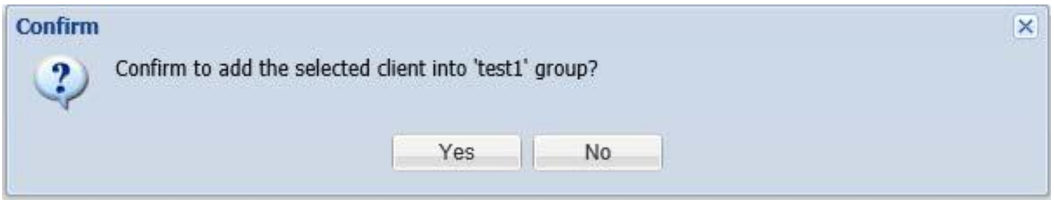
End IP: 192.168.0.150

□ IP	Client type	Client name	Management s...	Client version	MAC
□ 192.168.0.103	Windows	WIN-H357MQ6OT3E		6.0.0.0000.1479	00-0C-29-F3-F6-8A

Searching...

The function doesn't support NAT; max. number of clients are : 0/200

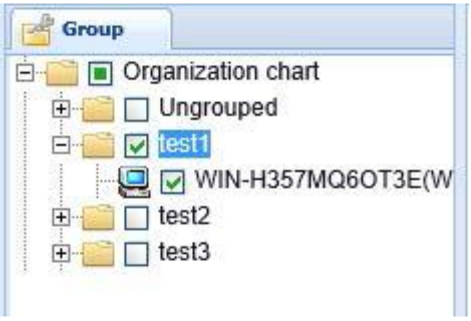
4. Select the client to be added, click "Add to management" and click "Yes" to finish the addition operation;



Confirm

Confirm to add the selected client into 'test1' group?

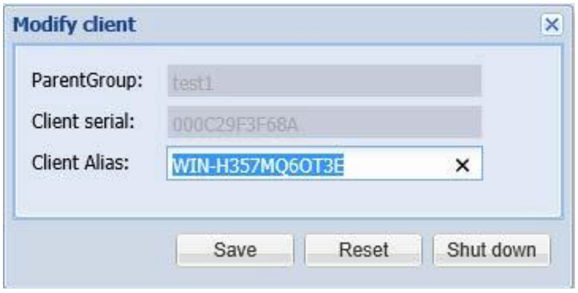
5. The user will add the client on the right panel to the client group, as shown in following figure:



3.2.2 Modify client

1. Select the client in the list and click “Modify” button;

2. In the popup window, modify the corresponding information and click “save”;


Modify client

ParentGroup: test1

Client serial: 000C29F3F68A

Client Alias: WIN-H357MQ6OT3E

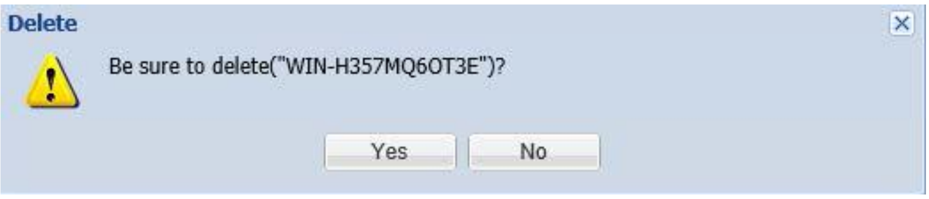
Notice:

- “Parent group” and “Client serial” are fixed and cannot be changed.

3.2.3 Delete client

1. Select the client to be deleted from the list and click “delete” button.

2. Click “Yes” on the popup “Delete” dialog box.


Delete

Be sure to delete("WIN-H357MQ6OT3E")?

There are different treatment modes in deletion of client according to the online situation of the client. The details are as follows:

- Client online: the management server of the client will be immediately empty and the client will be deleted from the list. This means that the client will not be managed by this server and can be added in other server for management.

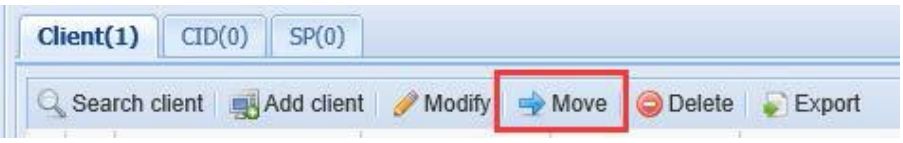
- Client offline: only when the client actively connects to the server in online mode, the address of local management server of the client can be deleted.

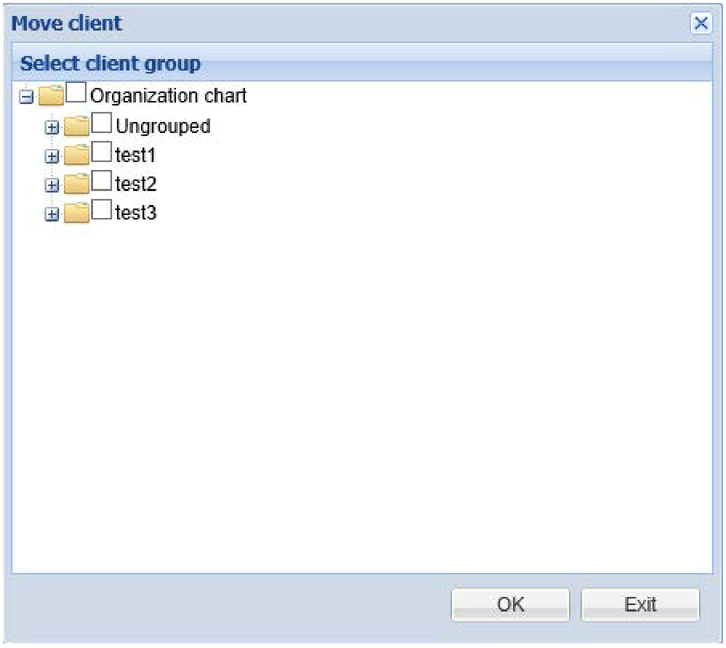
Notice:

- After the client is deleted, peripherals of the client will be deleted together.

3.2.4 Move client

1. Select the client in the list for client information, click “move” button and select the target group in the popup dialog box.





Move client

Select client group

Notice:

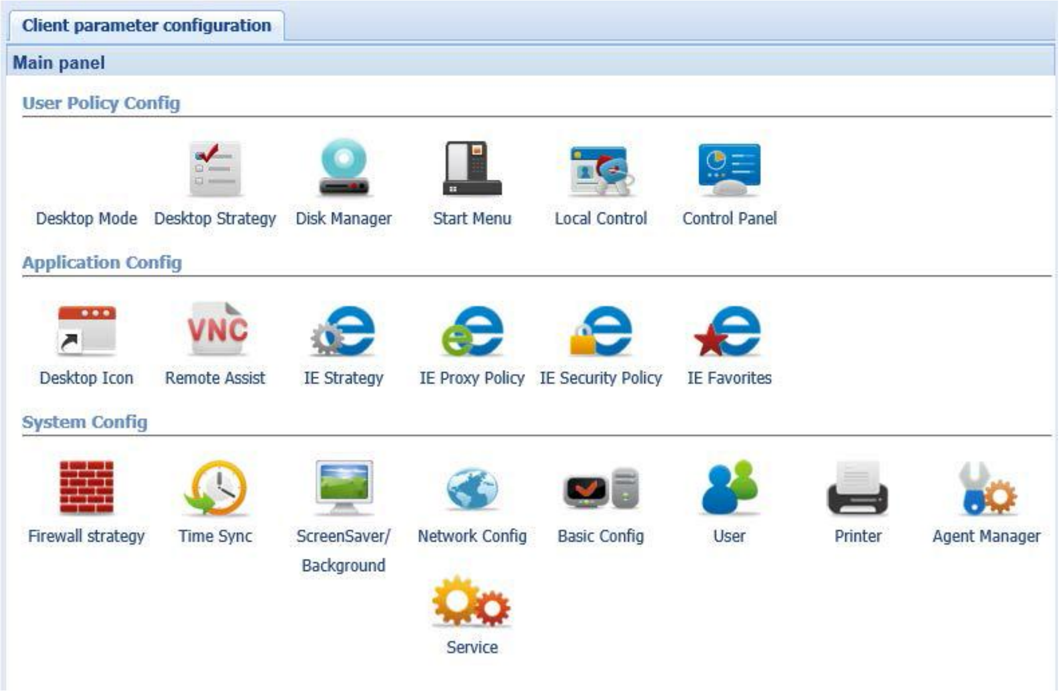
- After the client is moved, peripherals of the client will also be moved together.

4. Client Management

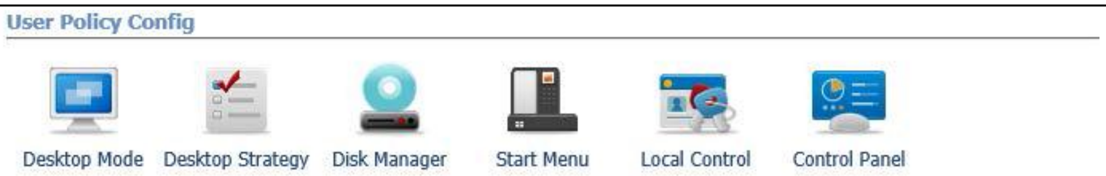
4.1 Client configuration

4.1.1 Client parameter configuration

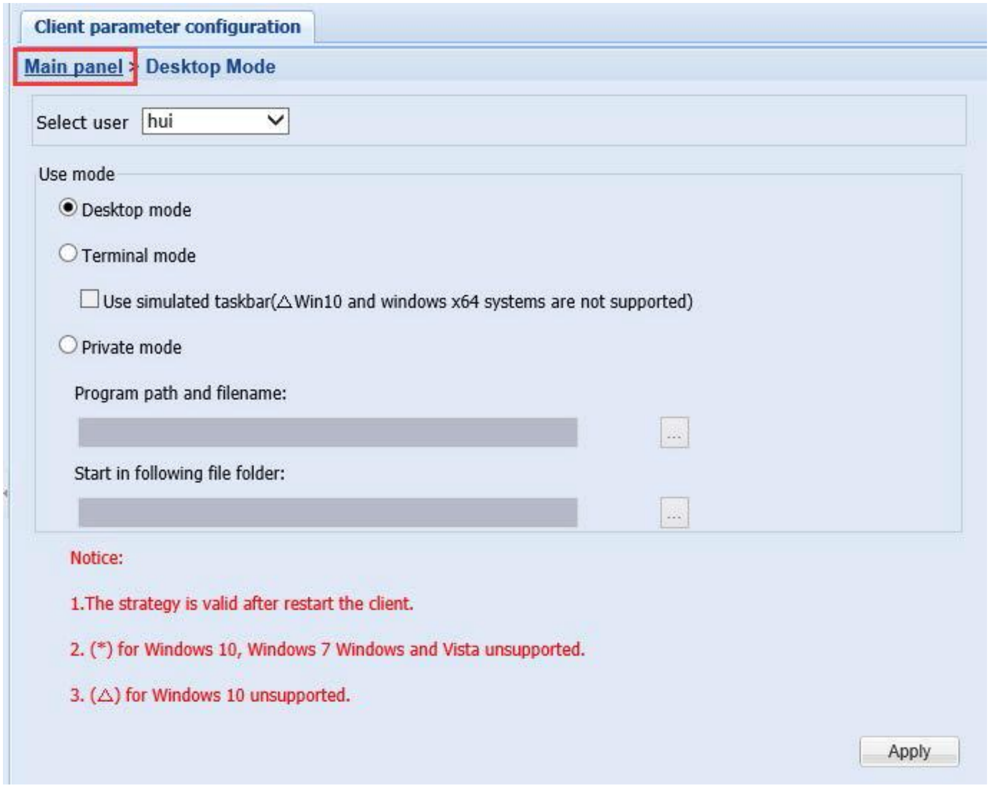
Enter 【client management—>basic management—>client configuration】 and select “client parameter configuration” tab page. The user shall select one client from the client group and can see the supported system configuration options on the right panel, as shown in following figure:



As for configuration of client parameters, click the corresponding option, such as the desktop mode in following figure:



After entering the configuration interface of desktop mode, click the link to return to previous interface, as shown in red frame in following figure:



Client parameter configuration

Main panel > Desktop Mode

Select user hui

Use mode

● Desktop mode

○ Terminal mode

□ Use simulated taskbar(△Win10 and windows x64 systems are not supported)

○ Private mode

Program path and filename:

Start in following file folder:

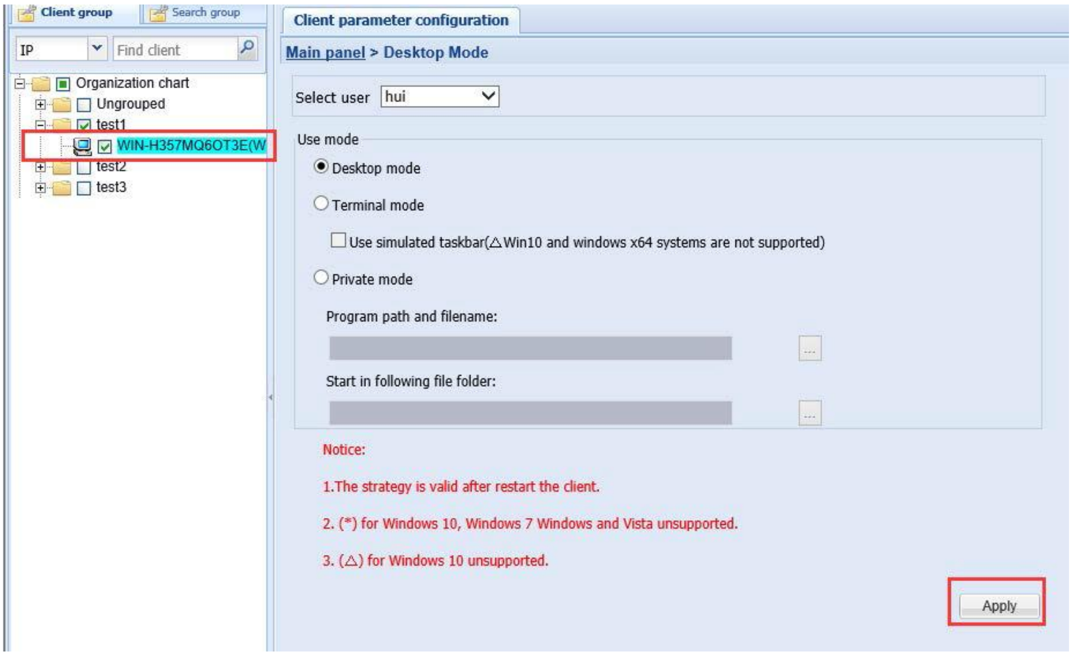
Notice:

1.The strategy is valid after restart the client.

2. (*) for Windows 10, Windows 7 Windows and Vista unsupported.

3. (△) for Windows 10 unsupported.

After configuration of desktop mode of client, click “apply” button to generate the configuration task. Notice: the user can select many clients at the same time and distribute the current strategy by batch.



Client parameter configuration

Main panel > Desktop Mode

Select user hui

Use mode

● Desktop mode

○ Terminal mode

□ Use simulated taskbar(△Win10 and windows x64 systems are not supported)

○ Private mode

Program path and filename:

Start in following file folder:

Notice:

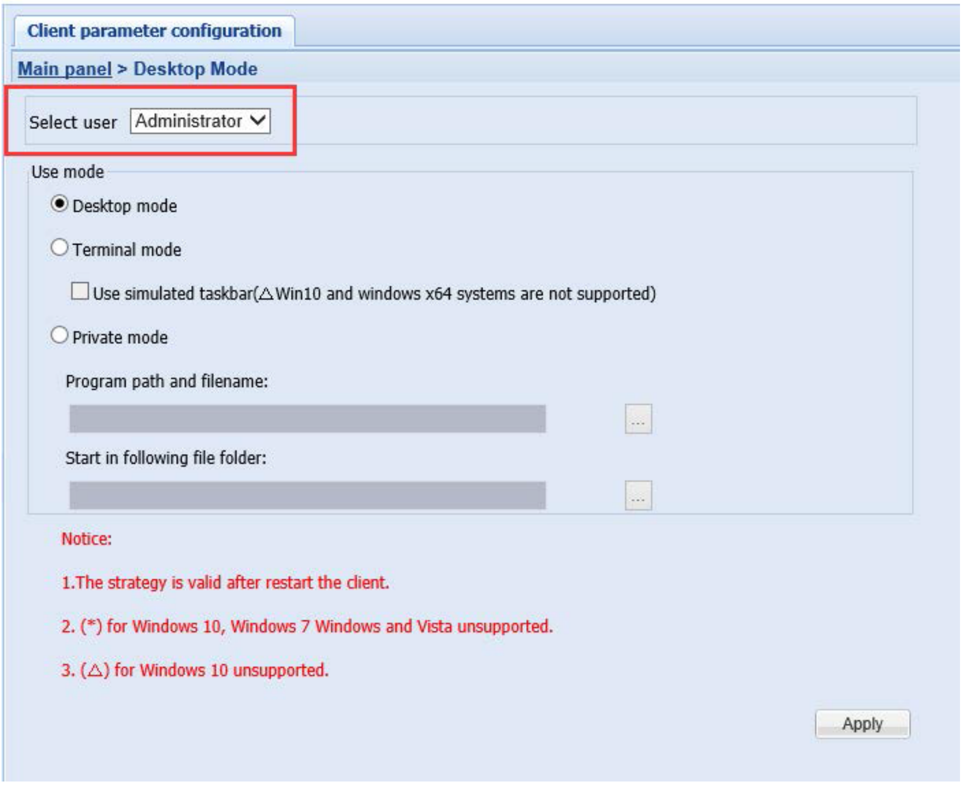
1.The strategy is valid after restart the client.

2. (*) for Windows 10, Windows 7 Windows and Vista unsupported.

3. (△) for Windows 10 unsupported.

4.1.1.1 Desktop mode

The desktop mode refers to the desktop display mode of client and can be customized and restricted according to the enterprise demand. The desktop mode is only valid to the user specified by the client and can be selected in the dropdown box.



Client parameter configuration

Main panel > Desktop Mode

Select user: Administrator

Use mode

● Desktop mode

○ Terminal mode

□ Use simulated taskbar(△Win10 and windows x64 systems are not supported)

○ Private mode

Program path and filename:

Start in following file folder:

Notice:

1.The strategy is valid after restart the client.

2. (*) for Windows 10, Windows 7 Windows and Vista unsupported.

3. (△) for Windows 10 unsupported.

At present, the following three desktop modes are supported:

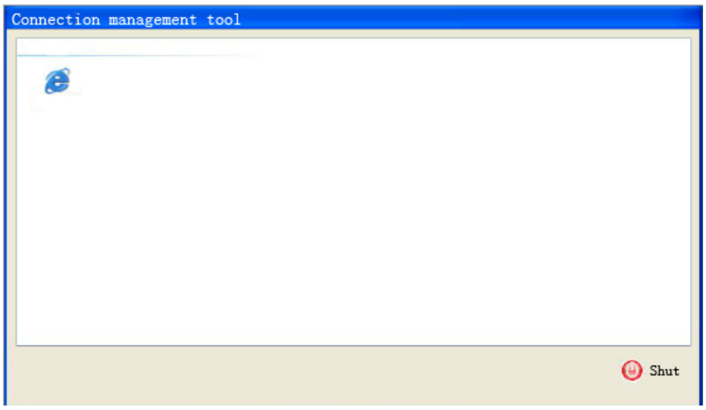
1. Desktop mode

It refers to the common desktop display mode. Desktop icon, taskbar, right key, start menu and other functions are available.

2. Terminal mode

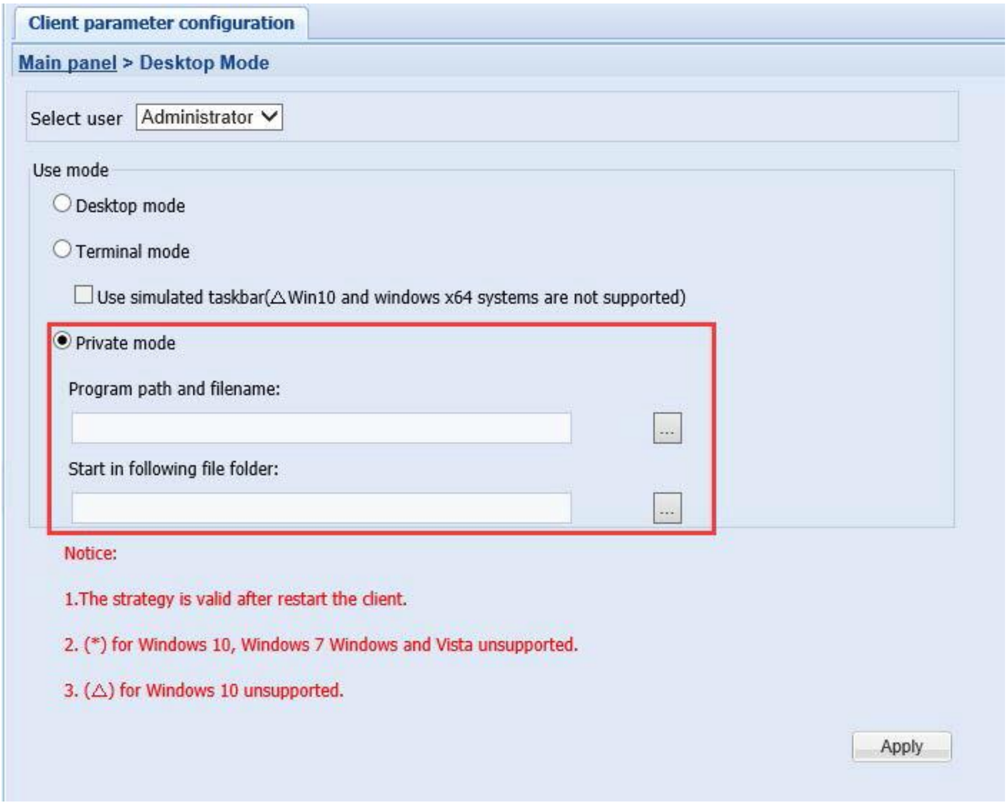
If working persons of enterprise or institution don’t use the local resources and only use OA system, remote connection and other simple functions, this mode is recommended.

In terminal mode, client desktop and taskbar are hidden by default, right click menu and other functions are disabled and only the local connection options of the client are displayed, as shown in following figure:



3. Special mode

After startup, the system only runs the programs specified by the user and doesn’t display desktop, taskbar, start menu, etc. As shown in following figure, at the server, set the client to only run IE. After the client strategy takes effect, only the IE browser is run.



Client parameter configuration

Main panel > Desktop Mode

Select user: Administrator

Use mode

○ Desktop mode

○ Terminal mode

□ Use simulated taskbar(△Win10 and windows x64 systems are not supported)

● Private mode

Program path and filename:

Start in following file folder:

Notice:

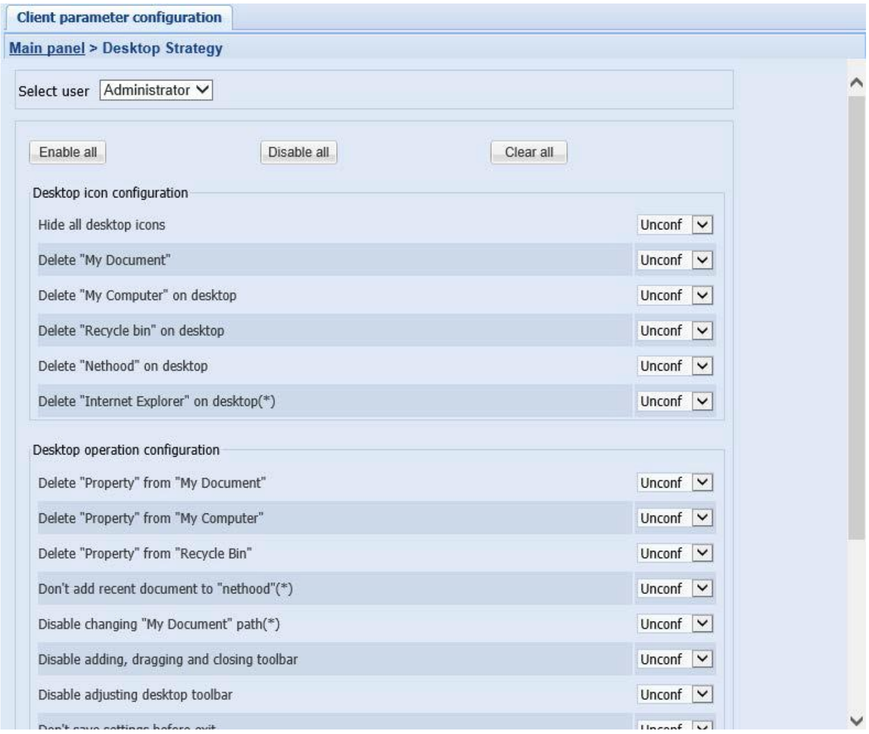
1.The strategy is valid after restart the client.

2. (*) for Windows 10, Windows 7 Windows and Vista unsupported.

3. (△) for Windows 10 unsupported.

4.1.1.2 Desktop strategy

The desktop strategy enables simple setting of icon display and operation of client desktop, is only valid to the user specified by the client and can be selected in the dropdown box.



Client parameter configuration

Main panel > Desktop Strategy

Select user: Administrator

Desktop icon configuration

Hide all desktop icons	Unconf
Delete "My Document"	Unconf
Delete "My Computer" on desktop	Unconf
Delete "Recycle bin" on desktop	Unconf
Delete "Nethood" on desktop	Unconf
Delete "Internet Explorer" on desktop(*)	Unconf

Desktop operation configuration

Delete "Property" from "My Document"	Unconf
Delete "Property" from "My Computer"	Unconf
Delete "Property" from "Recycle Bin"	Unconf
Don't add recent document to "nethood"(*)	Unconf
Disable changing "My Document" path(*)	Unconf
Disable adding, dragging and closing toolbar	Unconf
Disable adjusting desktop toolbar	Unconf
Don't save settings before exit	Unconf

4.1.1.3 Disk management

1. Shield disk

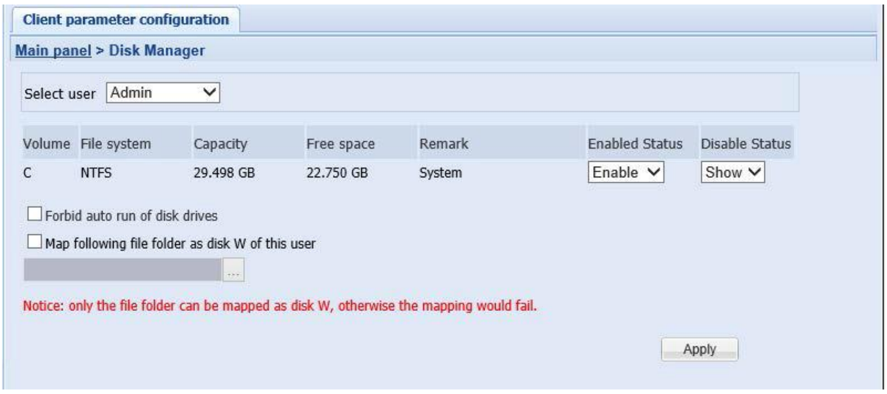
As for disk management, the disk displayed on client can be set. If “shield” is selected in the corresponding display state in partition, the partition will be hidden and disabled.

2. Disable automatic run of disk.

Prevent automatic run of U disk, mobile hard disk, CD driver and other external disks.

3. Map the folder

The folder specified by the client can be mapped as the W disk of user. Because it is not necessarily to hide or shield this type of disks to user, the mapped disk will not be displayed in the list as the system disk.



Select user: Admin

Volume	File system	Capacity	Free space	Remark	Enabled Status	Disable Status
C	NTFS	29.498 GB	22.750 GB	System	Enable	Show

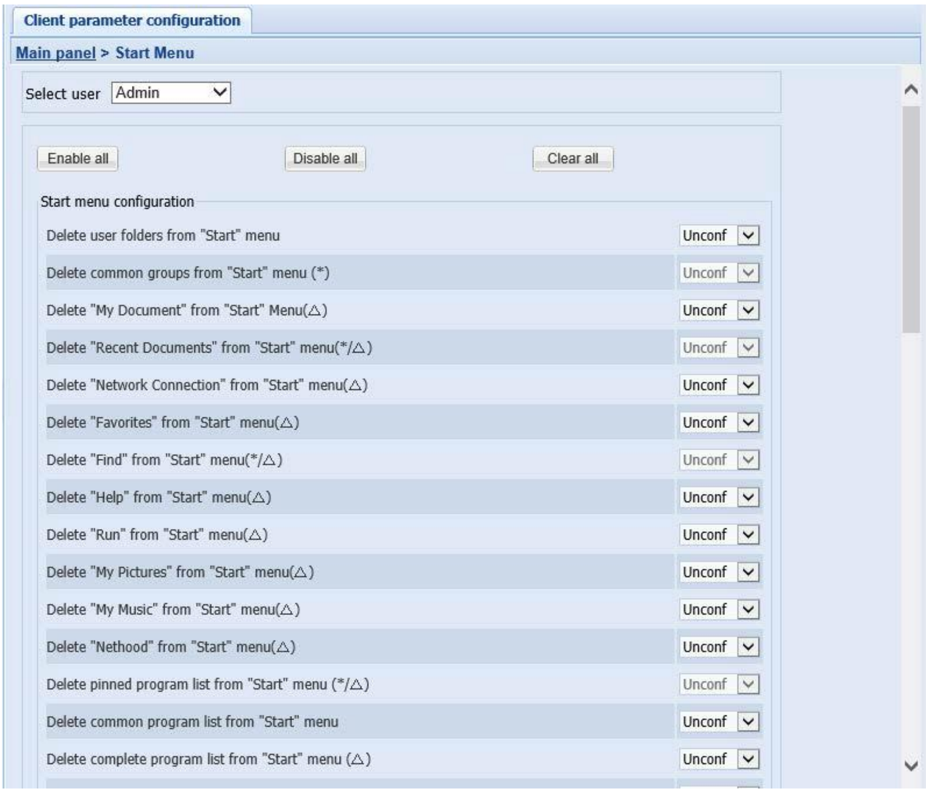
□ Forbid auto run of disk drives

□ Map following file folder as disk W of this user

Notice: only the file folder can be mapped as disk W, otherwise the mapping would fail.

4.1.1.4 Start menu taskbar

Set relevant configuration of start menu and task of the client. Notice: items marked with "*" don't support Vista and WIN7 clients.



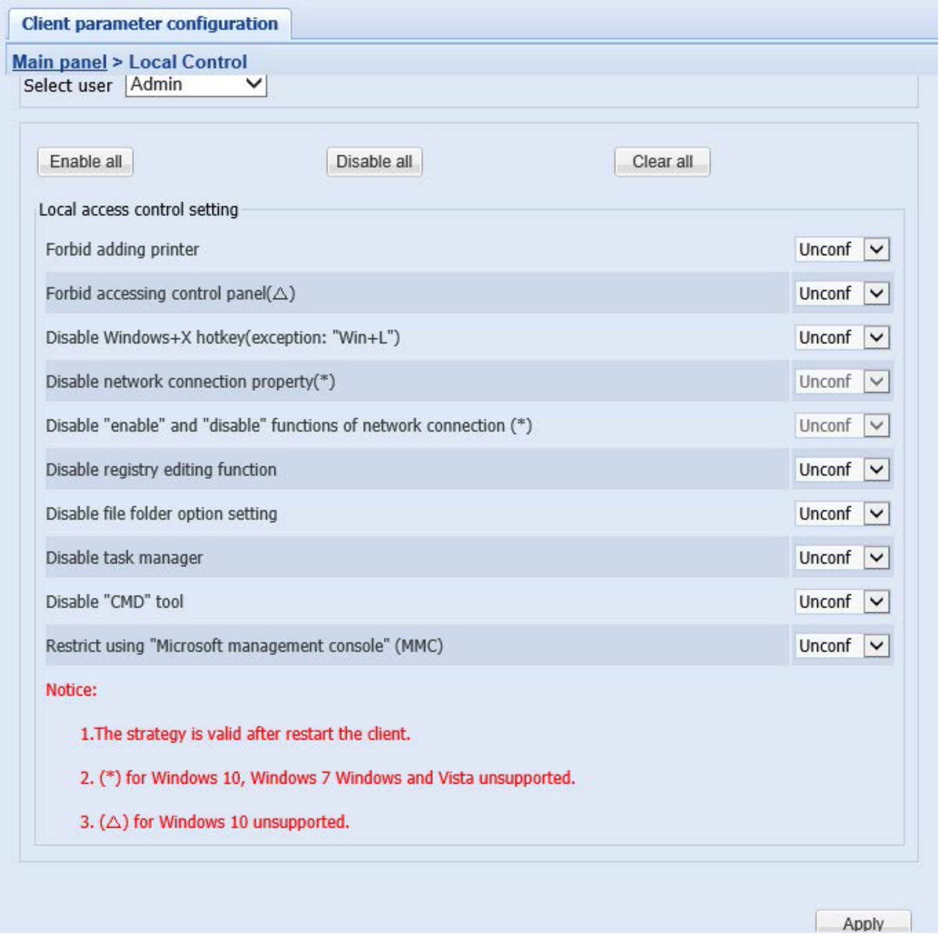
Select user: Admin

Start menu configuration

Delete user folders from "Start" menu	Unconf
Delete common groups from "Start" menu (*)	Unconf
Delete "My Document" from "Start" Menu(△)	Unconf
Delete "Recent Documents" from "Start" menu(*/△)	Unconf
Delete "Network Connection" from "Start" menu(△)	Unconf
Delete "Favorites" from "Start" menu(△)	Unconf
Delete "Find" from "Start" menu(*/△)	Unconf
Delete "Help" from "Start" menu(△)	Unconf
Delete "Run" from "Start" menu(△)	Unconf
Delete "My Pictures" from "Start" menu(△)	Unconf
Delete "My Music" from "Start" menu(△)	Unconf
Delete "Nethood" from "Start" menu(△)	Unconf
Delete pinned program list from "Start" menu (*/△)	Unconf
Delete common program list from "Start" menu	Unconf
Delete complete program list from "Start" menu (△)	Unconf

4.1.1.5 Local access control

The access authority of client to local resources is mainly set, such as restriction of using task manager, registry, command prompt and other system tools to ensure the local operation security of client. Notice: items marked with "*" don't support Vista and WIN7 clients.



Main panel > Local Control

Select user: Admin

Local access control setting

Forbid adding printer	Unconf
Forbid accessing control panel(△)	Unconf
Disable Windows+X hotkey(exception: "Win+L")	Unconf
Disable network connection property(*)	Unconf
Disable "enable" and "disable" functions of network connection (*)	Unconf
Disable registry editing function	Unconf
Disable file folder option setting	Unconf
Disable task manager	Unconf
Disable "CMD" tool	Unconf
Restrict using "Microsoft management console" (MMC)	Unconf

Notice:

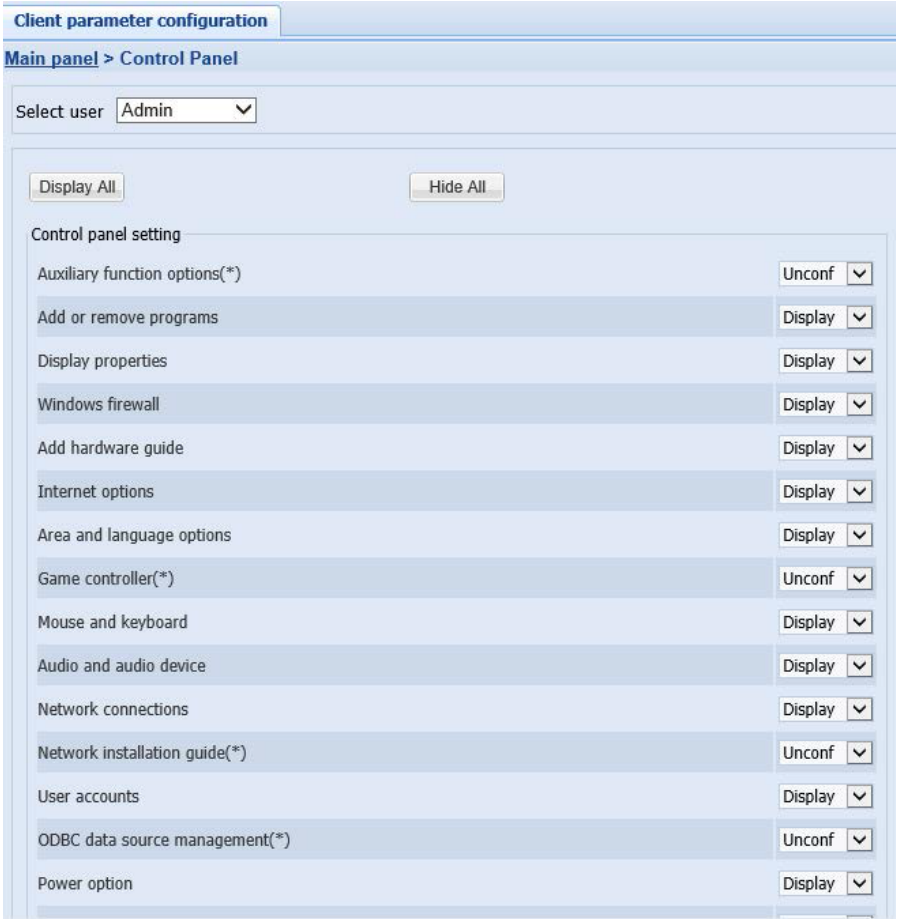
1.The strategy is valid after restart the client.

2. (*) for Windows 10, Windows 7 Windows and Vista unsupported.

3. (△) for Windows 10 unsupported.

4.1.1.6 Control panel

Configure the control panel display item of user specified by client. Notice: items marked with "*" don't support Vista and WIN7 clients.



Client parameter configuration

Main panel > Control Panel

Select user: Admin

Display All   Hide All

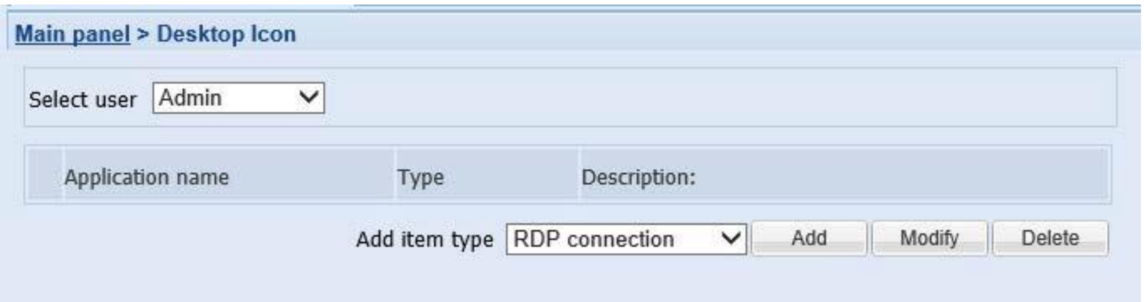
Control panel setting

Auxiliary function options(*)	Unconf
Add or remove programs	Display
Display properties	Display
Windows firewall	Display
Add hardware guide	Display
Internet options	Display
Area and language options	Display
Game controller(*)	Unconf
Mouse and keyboard	Display
Audio and audio device	Display
Network connections	Display
Network installation guide(*)	Unconf
User accounts	Display
ODBC data source management(*)	Unconf
Power option	Display

4.1.1.7 Publish desktop icons

Create a shortcut on client desktop so as to rapidly connect to the target address or software to be used by user. At present, it supports to create RDP connection, IE connection and application program connection.

In order to add the item, select from the dropdown menu of type box and click “add” button.



Main panel > Desktop Icon

Select user: Admin

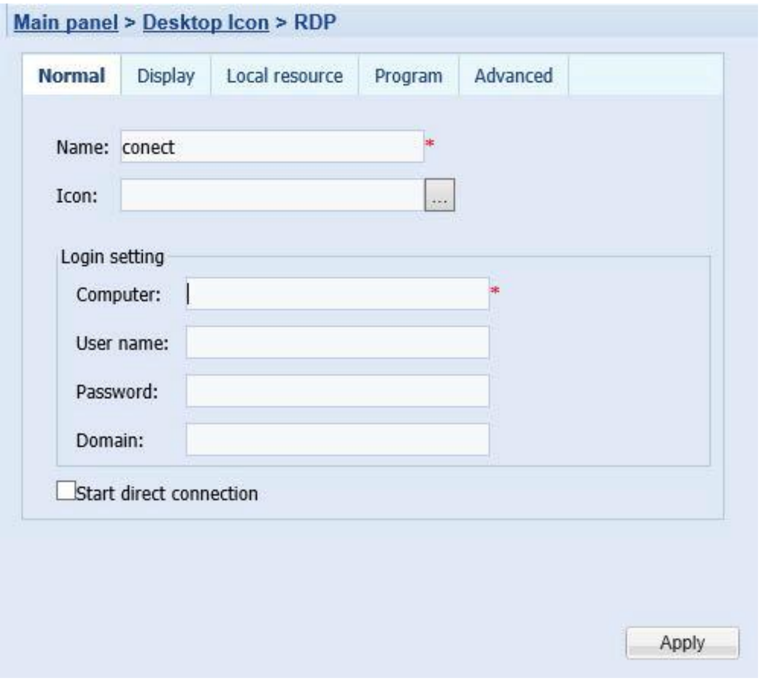
Application name	Type	Description:

Add item type: RDP connection   Add   Modify   Delete

1. RDP connection

In order to add a RDP connection item, fill in the connection name, displayed icon path, login setting and other relevant information. After successful creation of RDP item, the user can click the client to log in the computer with specified IP.

Notice: the icon path in connection item is the local path of client. If the icon file isn’t found on the path specified by client or the icon path is empty, directly use the default icon. Setting of icons of other connection items is same with the setting.



Main panel > Desktop Icon > RDP

Name: conect *

Icon: ...

Login setting

Computer: *

User name:

Password:

Domain:

□Start direct connection

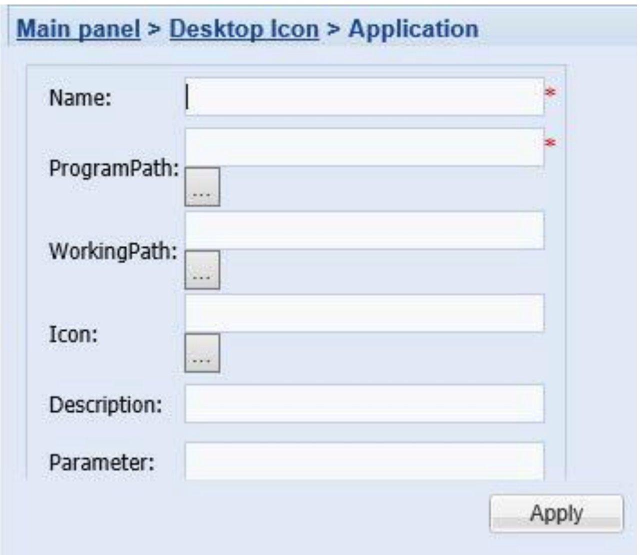
Click "apply" to finish addition. The desktop of user corresponding to client will display the shortcut of connection item, as shown in following figure:

2. Application program

The application program is connected to create a desktop shortcut for local application program of the client. Click the shortcut to automatically open the program or file specified on client. In following example, a start D:\ProgramFiles\test\setup.exe desktop shortcut is established for the client.

Program path: path where the program exists.

Work path: default path during program running (in general, it is the directory of program. As for special software, refer to its instructions)



Main panel > Desktop Icon > Application

Name: *

ProgramPath: * ...

WorkingPath: ...

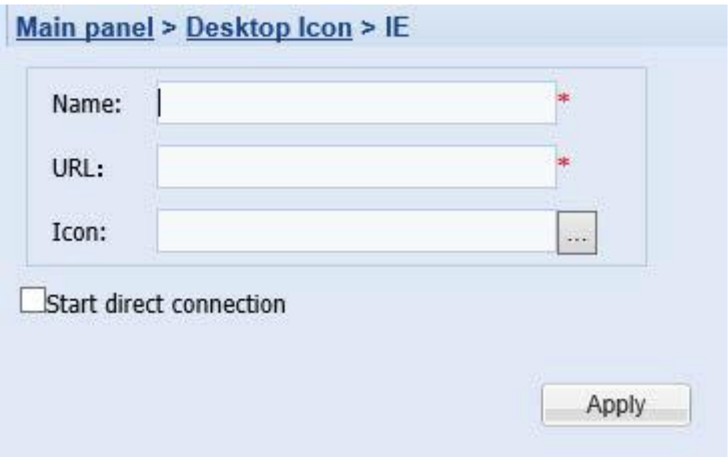
Icon: ...

Description:

Parameter:

3. IE

IE connection item is equal to shortcut connected to the specified web page. Click the shortcut to directly open the specified web page in IE.



Main panel > Desktop Icon > IE

Name: *

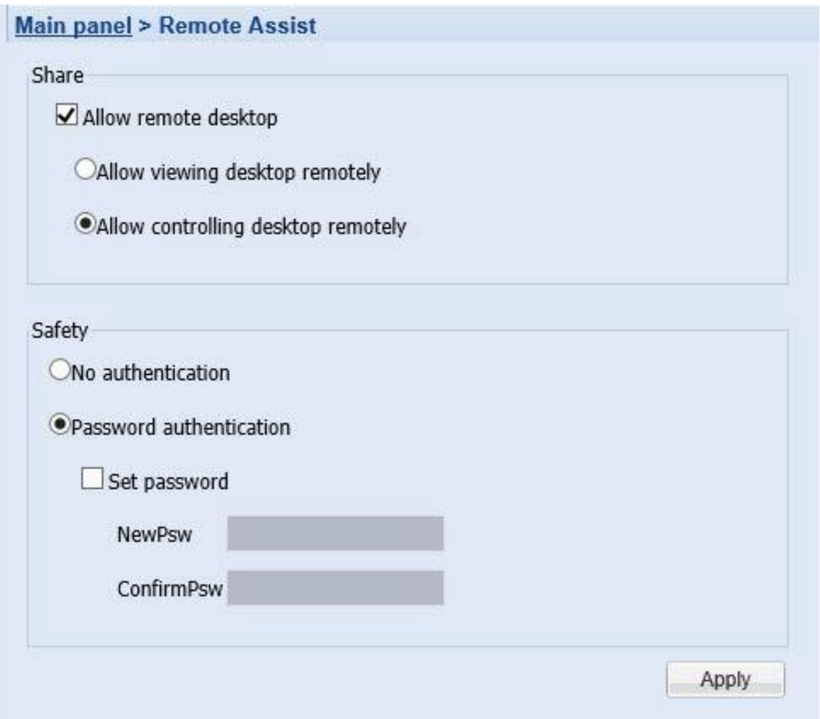
URL: *

Icon: ...

□ Start direct connection

4.1.1.8 Remote assistance

The remote assistance is used for setting the remote monitoring options and parameters of client, as shown in following figure. The share item can be used to set the control authority of server to client. The security item can be used to configure whether password authentication is required for remote assistance. The item is to support the extension of connection tool of the third party remote assistance. In general situation, it is unnecessary to configure.



Main panel > Remote Assist

Share

☑ Allow remote desktop

○ Allow viewing desktop remotely

● Allow controlling desktop remotely

Safety

○ No authentication

● Password authentication

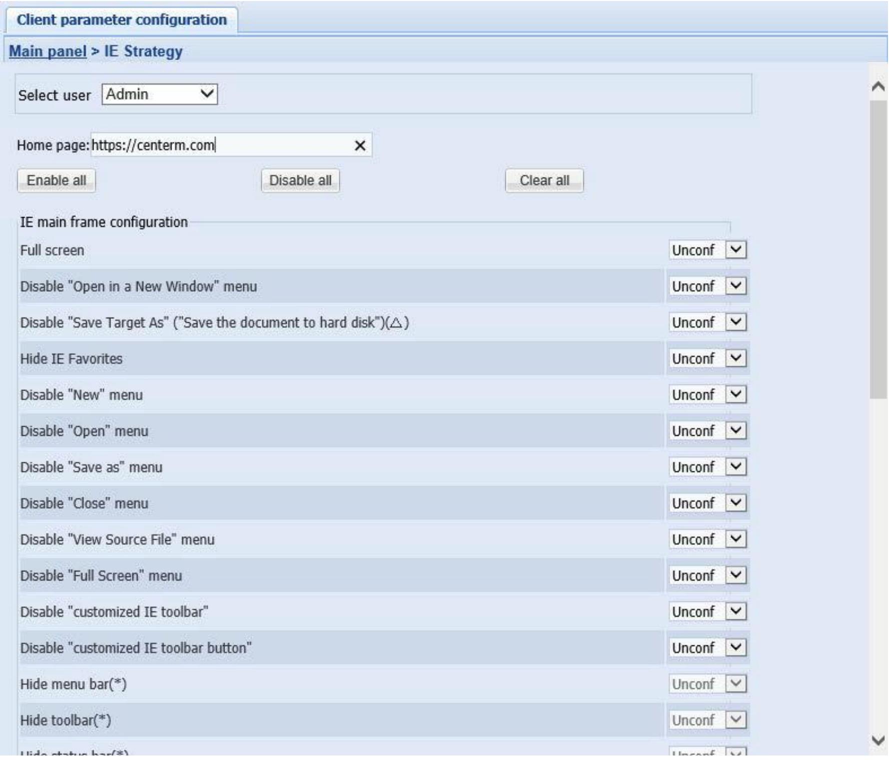
□ Set password

NewPsw

ConfirmPsw

4.1.1.9 IE strategy

Set the IE basic strategy of user specified by the client. Notice: items marked with "*" don't support Vista and WIN7 clients.



Client parameter configuration

Main panel > IE Strategy

Select user: Admin

Home page: https://centerm.com

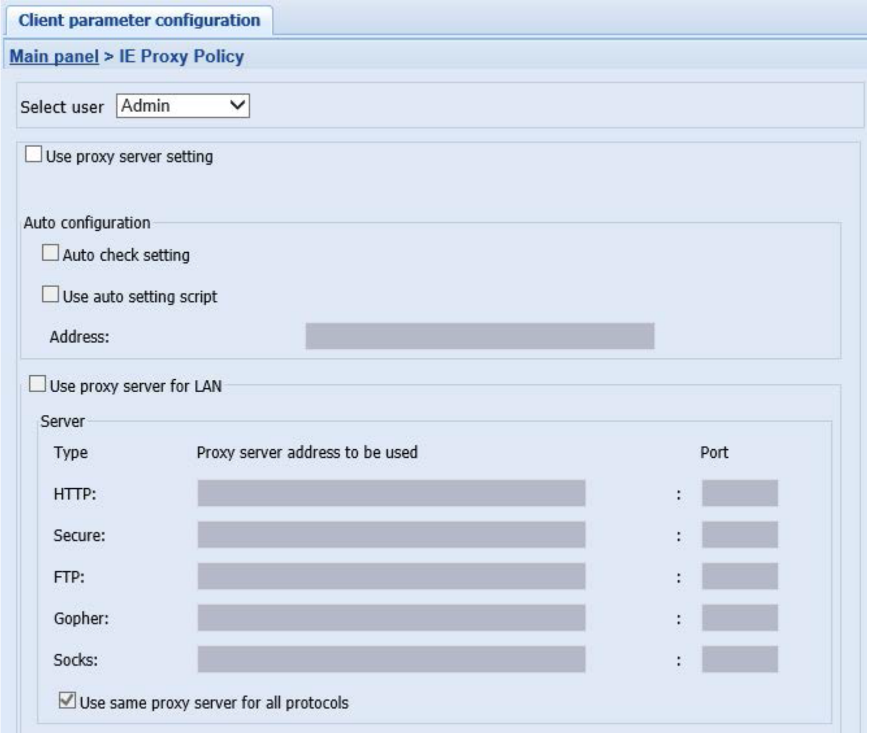
Enable all | Disable all | Clear all

IE main frame configuration

Full screen	Unconf
Disable "Open in a New Window" menu	Unconf
Disable "Save Target As" ("Save the document to hard disk")(△)	Unconf
Hide IE Favorites	Unconf
Disable "New" menu	Unconf
Disable "Open" menu	Unconf
Disable "Save as" menu	Unconf
Disable "Close" menu	Unconf
Disable "View Source File" menu	Unconf
Disable "Full Screen" menu	Unconf
Disable "customized IE toolbar"	Unconf
Disable "customized IE toolbar button"	Unconf
Hide menu bar(*)	Unconf
Hide toolbar(*)	Unconf
Hide status bar(*)	Unconf

4.1.1.10 IE agent strategy

Set the local IE agent item of the client.



Client parameter configuration

Main panel > IE Proxy Policy

Select user: Admin

□ Use proxy server setting

Auto configuration

□ Auto check setting

□ Use auto setting script

Address:

□ Use proxy server for LAN

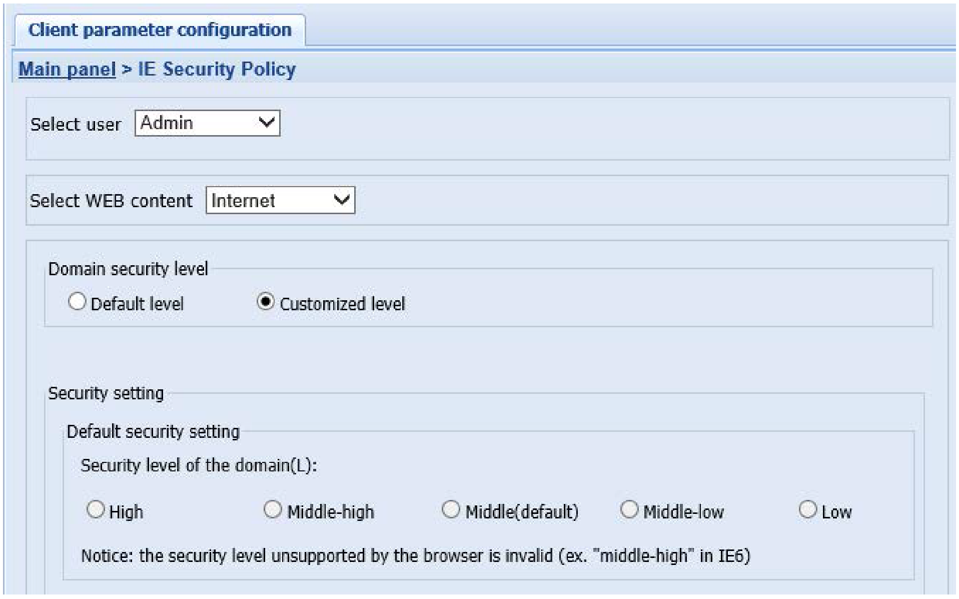
Server

Type	Proxy server address to be used		Port
HTTP:		:	
Secure:		:	
FTP:		:	
Gopher:		:	
Socks:		:	

☑ Use same proxy server for all protocols

4.1.1.11 IE security strategy

Set the local IE security strategy of the client.



Client parameter configuration

Main panel > IE Security Policy

Select user: Admin

Select WEB content: Internet

Domain security level

○ Default level ● Customized level

Security setting

Default security setting

Security level of the domain(L):

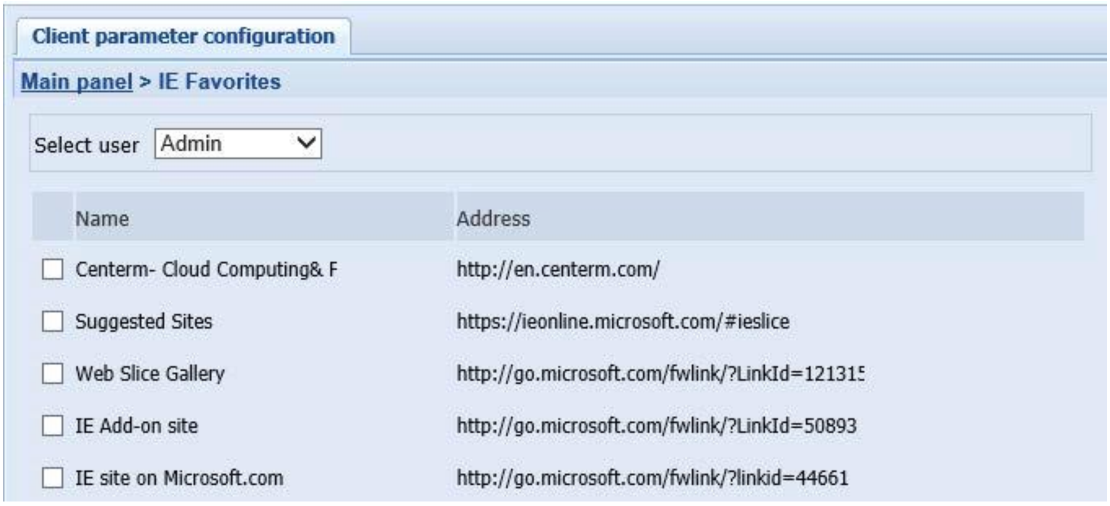
○ High ○ Middle-high ○ Middle(default) ○ Middle-low ○ Low

Notice: the security level unsupported by the browser is invalid (ex. "middle-high" in IE6)

Notice: the trusted site strategy sent from the server will cover the existing strategy of the user.

4.1.1.12 IE favorites

Set the local IE favorites of the client.

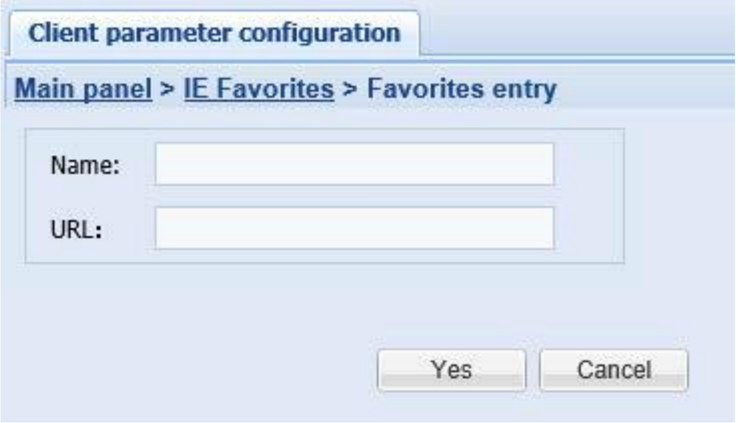


Client parameter configuration

Main panel > IE Favorites

Select user: Admin

	Name	Address
□	Centerm- Cloud Computing& F	http://en.centerm.com/
□	Suggested Sites	https://ieonline.microsoft.com/#ieslice
□	Web Slice Gallery	http://go.microsoft.com/fwlink/?LinkId=12131ᵹ
□	IE Add-on site	http://go.microsoft.com/fwlink/?LinkId=50893
□	IE site on Microsoft.com	http://go.microsoft.com/fwlink/?linkid=44661



Client parameter configuration

Main panel > IE Favorites > Favorites entry

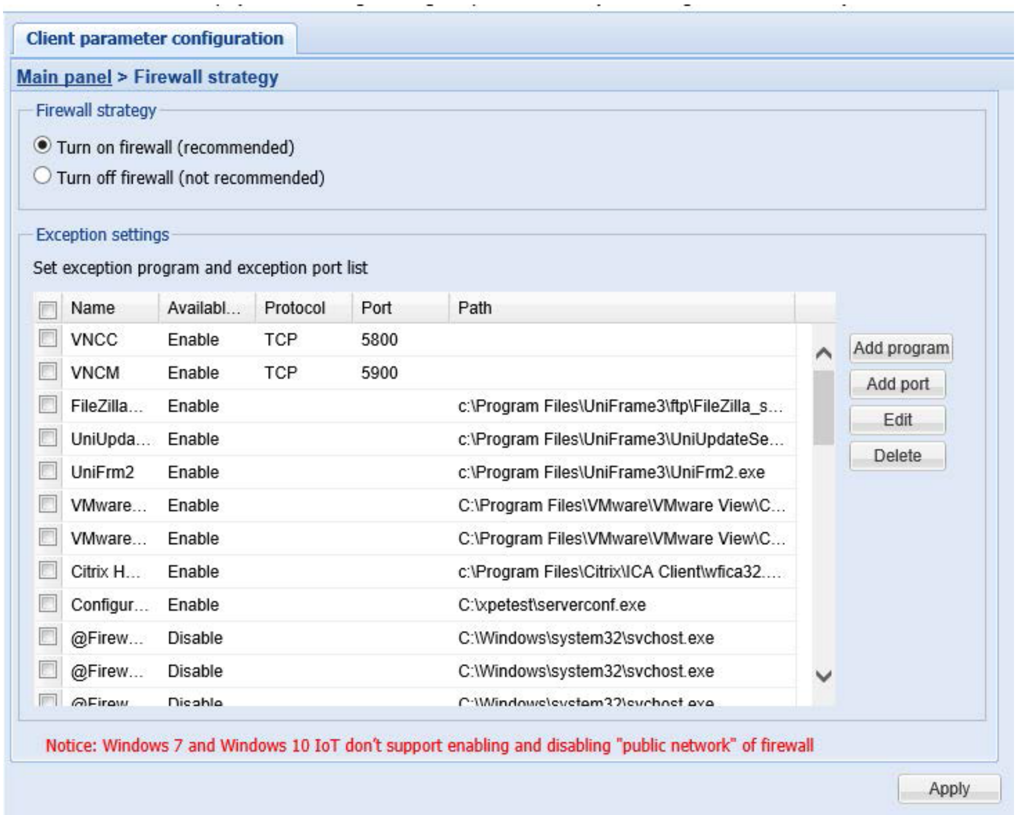
Name:

URL:

4.1.1.13 Firewall strategy

The firewall refers to the firewall function in the terminal system. In the firewall setting, the user can configure the firewall according to the actual demand. In order to ensure the security of user's information, it is suggested opening the firewall of client.

Select single client in high light to obtain the current firewall configuration of client from the list. Same with the setting of windows firewall, the exceptional program and exceptional port can be configured on the interface.



Client parameter configuration
Main panel > Firewall strategy

Firewall strategy

● Turn on firewall (recommended)
○ Turn off firewall (not recommended)

Exception settings

Set exception program and exception port list

□	Name	Availabl...	Protocol	Port	Path
□	VNCC	Enable	TCP	5800	
□	VNCM	Enable	TCP	5900	
□	FileZilla...	Enable			c:\Program Files\UniFrame3\ftp\FileZilla_s...
□	UniUpda...	Enable			c:\Program Files\UniFrame3\UniUpdateSe...
□	UniFrm2	Enable			c:\Program Files\UniFrame3\UniFrm2.exe
□	VMware...	Enable			C:\Program Files\VMware\VMware View\C...
□	VMware...	Enable			C:\Program Files\VMware\VMware View\C...
□	Citrix H...	Enable			c:\Program Files\Citrix\ICA Client\wfica32....
□	Configur...	Enable			C:\xpetest\serverconf.exe
□	@Firew...	Disable			C:\Windows\system32\svchost.exe
□	@Firew...	Disable			C:\Windows\system32\svchost.exe
□	@Firew...	Disable			C:\Windows\system32\svchost.exe

Notice: Windows 7 and Windows 10 IoT don't support enabling and disabling "public network" of firewall

After configuration, click “apply” button in lower position of the interface. Plan the firewall configuration tasks on the popup panel and apply the strategy in the client.

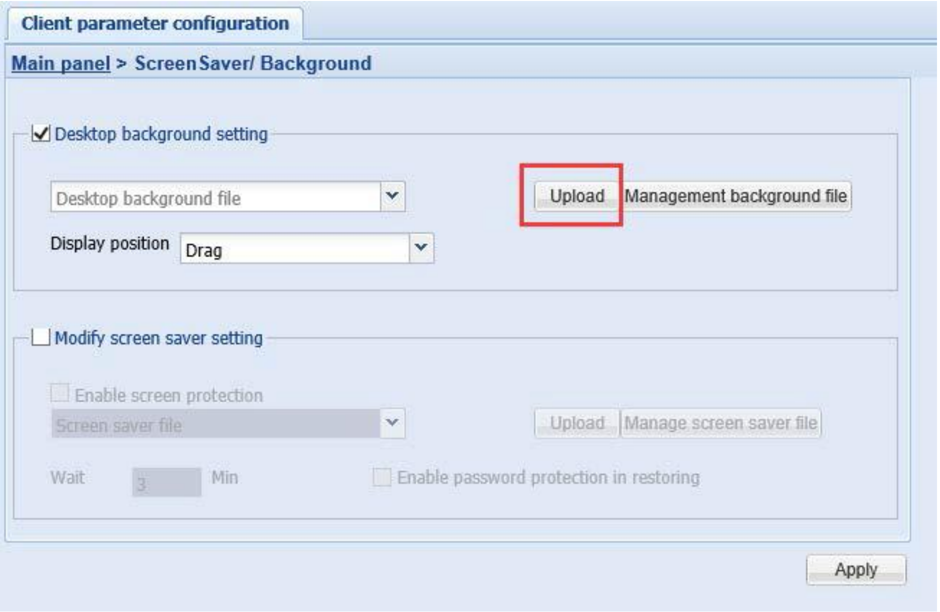
Notice: when the user selects application strategy of many clients, the current strategy can be configured into the client by batch.

4.1.1.14 Screensaver/desktop background

Screensaver/desktop background can help administrator to configure desktop background and screensaver program of client by batch and to simply configure relevant parameters. This function only supports background files and screensaver files with bmp format. The special picture format conversion tool can be used to generate bmp file rather than directly change the suffix.

The desktop background change function is taken as an example to briefly introduce:

1. Select “change desktop background setting”. If the user uses this function at the first time, the user shall upload the desktop background images to the system.



Client parameter configuration
Main panel > ScreenSaver/ Background
Upload
Management background file
Upload
Manage screen saver file
Apply

☑ Desktop background setting

Desktop background file

Display position: Drag

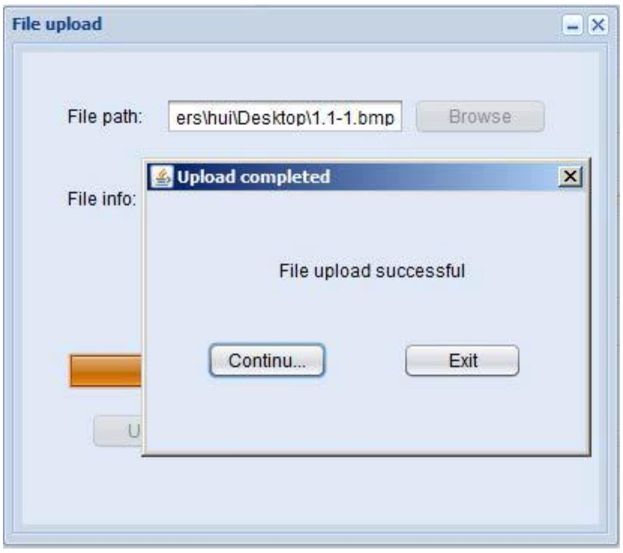
□ Modify screen saver setting

□ Enable screen protection

Screen saver file

Wait 3 Min

□ Enable password protection in restoring

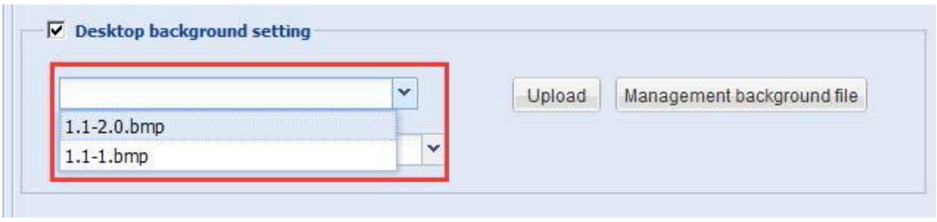


File path: ers\hui\Desktop\1.1-1.bmp

File info:

File upload successful

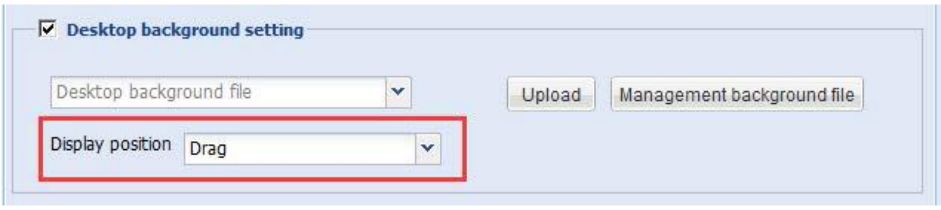
2. After uploading, select the file in the dropdown list, set the display position and click “apply” button.



☑ Desktop background setting

1.1-2.0.bmp

1.1-1.bmp

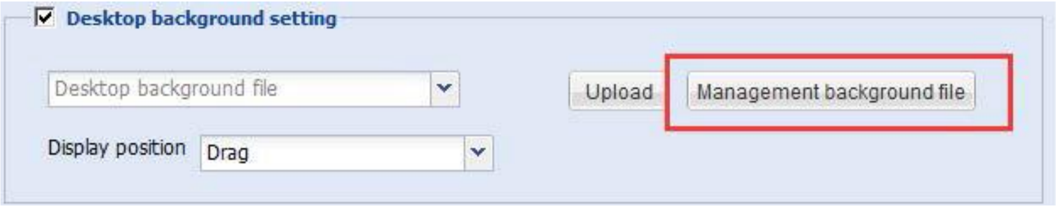


☑ Desktop background setting

Desktop background file

Display position: Drag

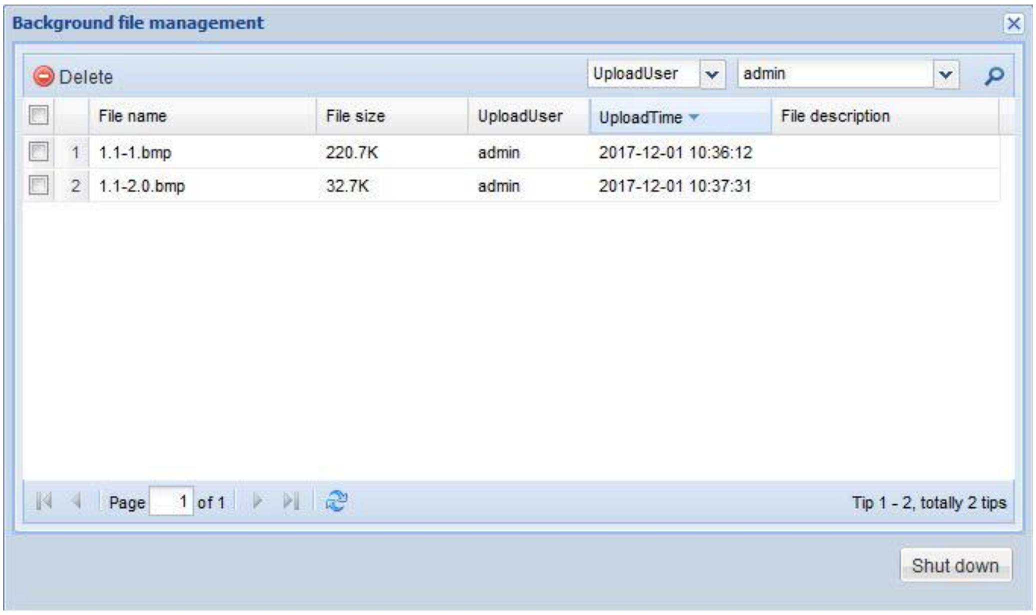
3. If the desktop wallpaper files are too many and shall be cleaned up, click “manage background file” button to view all uploaded wallpaper files.



☑ Desktop background setting

Desktop background file

Display position: Drag



Background file management

UploadUser: admin

		File name	File size	UploadUser	UploadTime	File description
□	1	1.1-1.bmp	220.7K	admin	2017-12-01 10:36:12	
□	2	1.1-2.0.bmp	32.7K	admin	2017-12-01 10:37:31	

Page 1 of 1

Tip 1 - 2, totally 2 tips

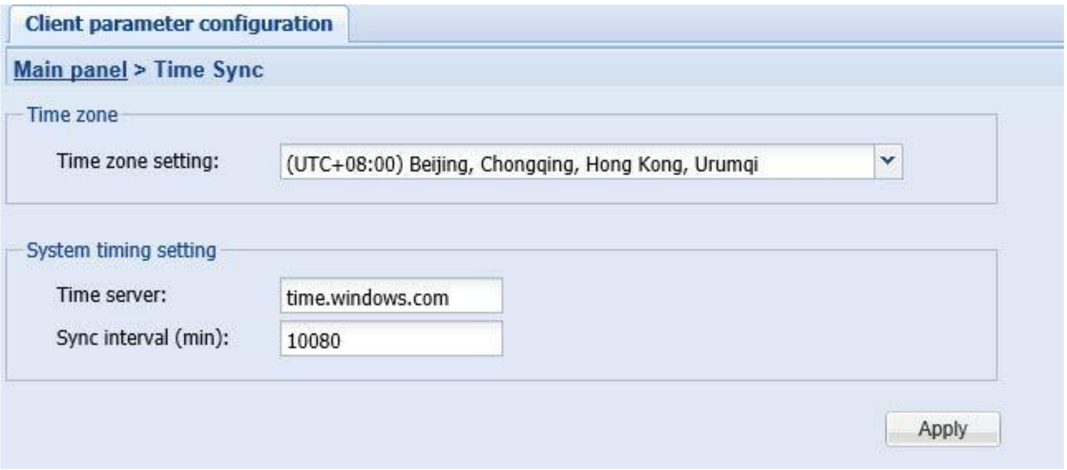
The setting method of screensaver is same with that of desktop background. No more details are given here.

4.1.1.15 Time synchronization

If the client time is inconsistent with the server time, some software may not run normally. The time synchronization function can automatically synchronize the time of all clients with the time of specified server.

The configuration method of time synchronization is simple. Select one or more clients. Input “time server” and “synchronization interval (min)” on the following interface and click “apply” button to execute the task.

Notice: the “time server” column can be filled with domain name or IP.



Client parameter configuration

Main panel > Time Sync

Time zone

Time zone setting: (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

System timing setting

Time server: time.windows.com

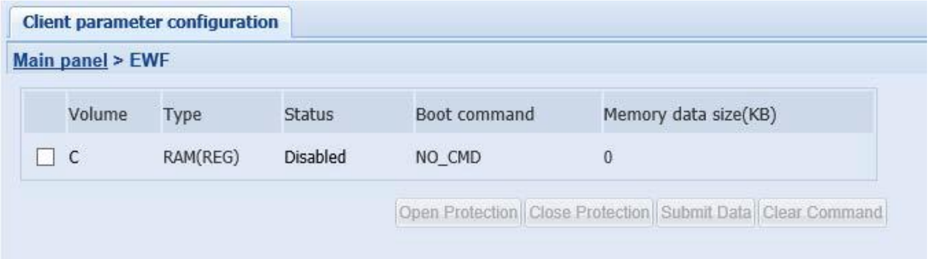
Sync interval (min): 10080

4.1.1.16 EWF protection control

EWF protection control is only valid in the client with memory protection or hard disk protection function.

As for the memory protection client, firstly select the partition and then, carry out corresponding operation. The server can be configured with following four operations:

- Enable protection: enable the memory protection function of the selected client.
- Disable protection: disable the memory protection function of the selected client.
- Submit date: submit the current operation of the client.
- Cleaning command: clean all commands currently submitted by the client.

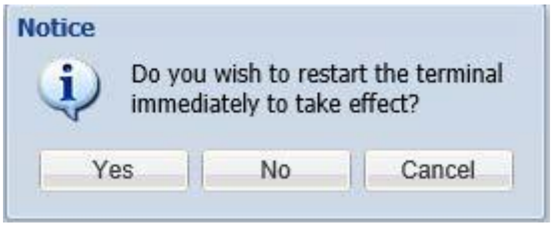


Client parameter configuration

Main panel > EWF

	Volume	Type	Status	Boot command	Memory data size(KB)
□	C	RAM(REG)	Disabled	NO_CMD	0

After executing the operation, the system will prompt the user whether to immediately restart for validating. If “Yes” is selected, the client will be immediately restarted and the strategy application will be validated. If “No” is selected, the client will not be immediately restarted and the strategy will be validated after restart of the client next time. “Cancel” refers to give up the current settings and return to configuration page.



Notice

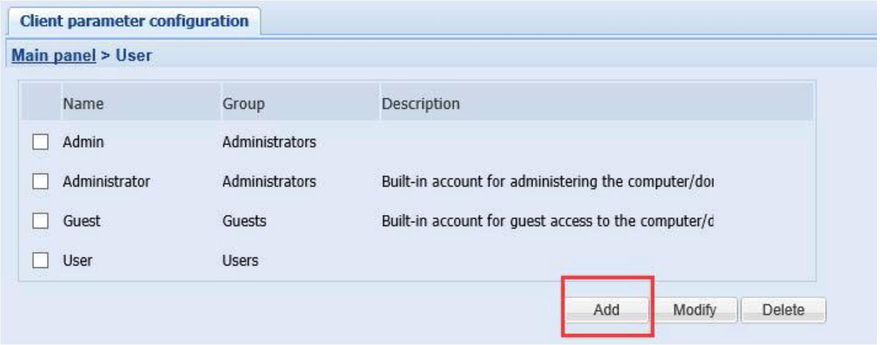
Do you wish to restart the terminal immediately to take effect?

The configuration interface of hard disk protection client is similar to that of memory protection client. No more details are given here.

4.1.1.17 User

In user configuration, a user can be changed or deleted or new user can be added to the client. The user configuration function is introduced in following content with the addition of a new user as an example.

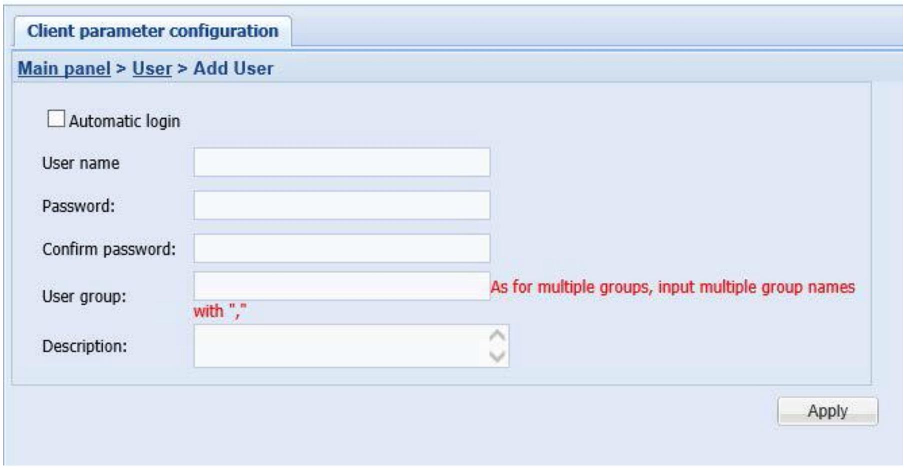
Click “add” button to switch to “add user” page, as shown in following figure:



Client parameter configuration

Main panel > User

	Name	Group	Description
□	Admin	Administrators	
□	Administrator	Administrators	Built-in account for administering the computer/do
□	Guest	Guests	Built-in account for guest access to the computer/d
□	User	Users	



Client parameter configuration

Main panel > User > Add User

☐ Automatic login

User name

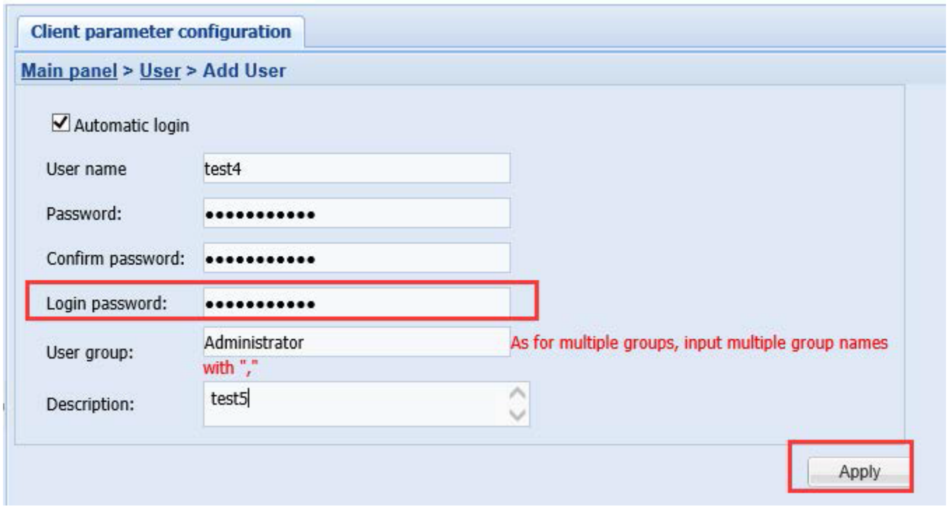
Password:

Confirm password:

User group: As for multiple groups, input multiple group names with ","

Description:

If current user will be set as the automatic login user, the automatic login password shall be inputted. Then, click “apply” button.



Client parameter configuration

Main panel > User > Add User

☑ Automatic login

User name: test4

Password: ●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●

Login password: ●●●●●●●●●●●

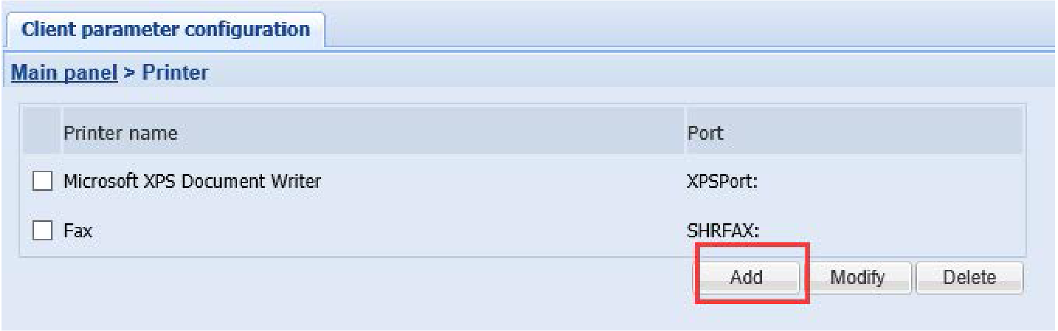
User group: Administrator As for multiple groups, input multiple group names with ","

Description: test5

4.1.1.18 Printer

The printer page supports the user to add, change and delete the local printer of client. Take the addition of printer as an example as follows.

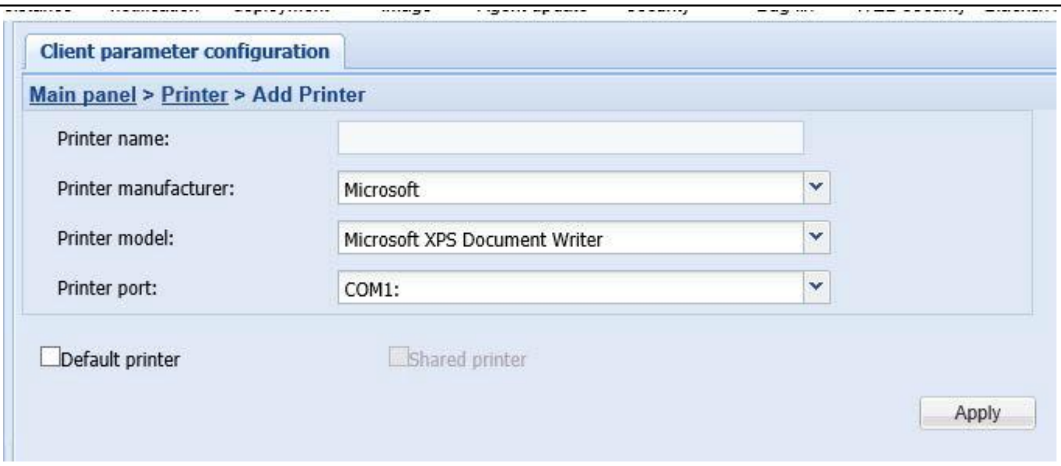
Click “add” button to enter the “add printer” page.



Client parameter configuration

Main panel > Printer

	Printer name	Port
☐	Microsoft XPS Document Writer	XPSPort:
☐	Fax	SHRFAX:



Client parameter configuration

Main panel > Printer > Add Printer

Printer name:

Printer manufacturer: Microsoft

Printer model: Microsoft XPS Document Writer

Printer port: COM1:

□ Default printer   □ Shared printer

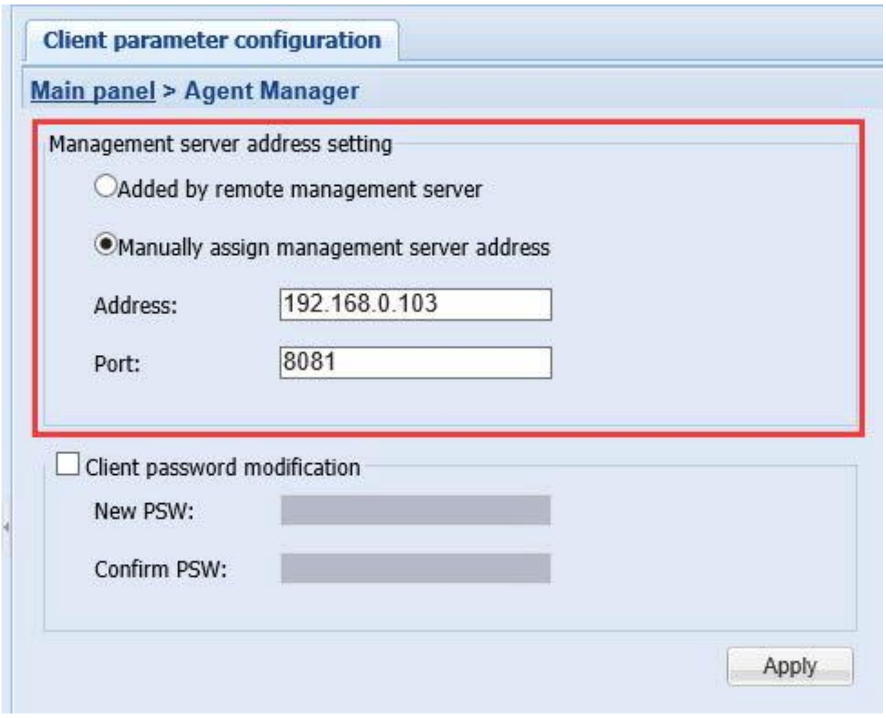
The administrator can set the printer as the default printer or shared printer.

4.1.1.19 Client management

In Agent configuration of client, the user can carry out basic setting in the client, including address and password of management server of the client.

Address of management server:

- Actively add by remote management server: if this mode is selected, the selected client shall be added through search of server.
- Manually specify the management server address: if this mode is selected, the selected client will actively target at the specified management server. This function can be used for migration of server with large number of clients. In new server, the user can view the manually specified client in the ungrouped column.



Client parameter configuration

Main panel > Agent Manager

Management server address setting

○ Added by remote management server

● Manually assign management server address

Address: 192.168.0.103

Port: 8081

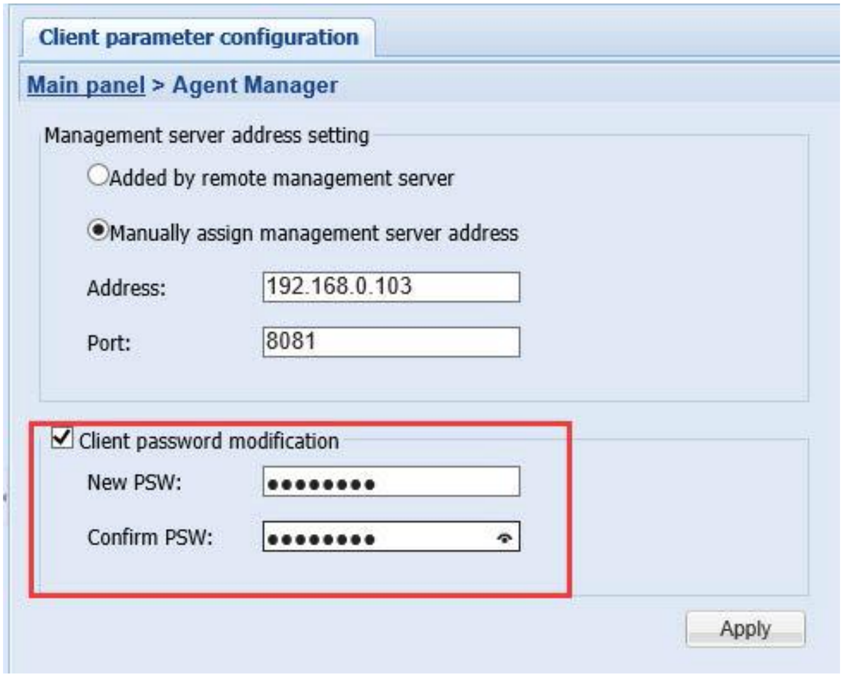
□ Client password modification

New PSW:

Confirm PSW:

Change of client password:

- Change the configuration password of client to prevent client from uninstalling the client software without authorization.



Main panel > Agent Manager

Management server address setting

○Added by remote management server

●Manually assign management server address

Address: 192.168.0.103

Port: 8081

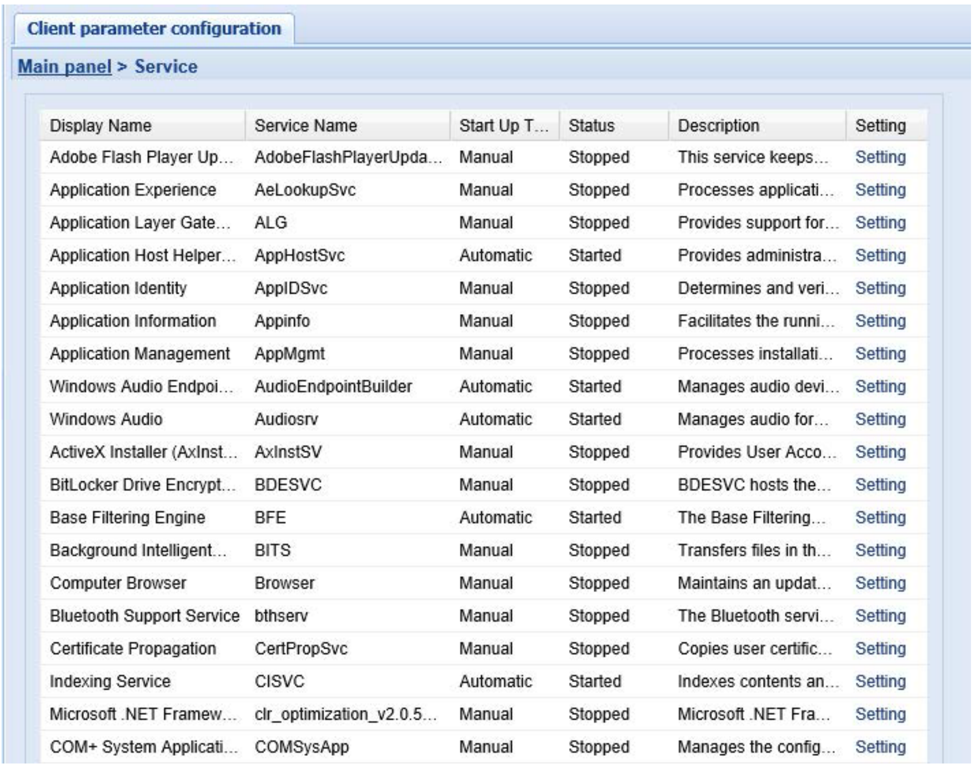
☑ Client password modification

New PSW: ●●●●●●●●●

Confirm PSW: ●●●●●●●●●

4.1.1.20 Service

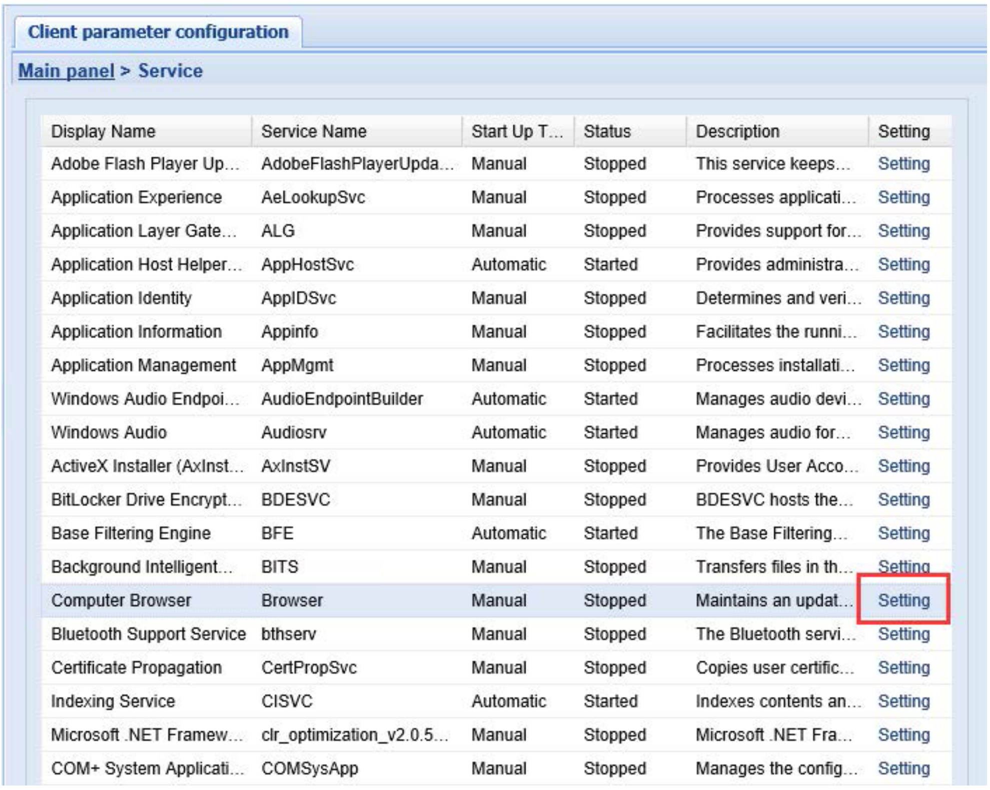
It shows running situation of all current service programs to administrator. The administrator can configure local service of the client.



Main panel > Service

Display Name	Service Name	Start Up T...	Status	Description	Setting
Adobe Flash Player Up...	AdobeFlashPlayerUpda...	Manual	Stopped	This service keeps...	Setting
Application Experience	AeLookupSvc	Manual	Stopped	Processes applicati...	Setting
Application Layer Gate...	ALG	Manual	Stopped	Provides support for...	Setting
Application Host Helper...	AppHostSvc	Automatic	Started	Provides administra...	Setting
Application Identity	AppIDSvc	Manual	Stopped	Determines and veri...	Setting
Application Information	Appinfo	Manual	Stopped	Facilitates the runni...	Setting
Application Management	AppMgmt	Manual	Stopped	Processes installati...	Setting
Windows Audio Endpoi...	AudioEndpointBuilder	Automatic	Started	Manages audio devi...	Setting
Windows Audio	Audiosrv	Automatic	Started	Manages audio for...	Setting
ActiveX Installer (AxInst...	AxInstSV	Manual	Stopped	Provides User Acco...	Setting
BitLocker Drive Encrypt...	BDESVC	Manual	Stopped	BDESVC hosts the...	Setting
Base Filtering Engine	BFE	Automatic	Started	The Base Filtering...	Setting
Background Intelligent...	BITS	Manual	Stopped	Transfers files in th...	Setting
Computer Browser	Browser	Manual	Stopped	Maintains an updat...	Setting
Bluetooth Support Service	bthserv	Manual	Stopped	The Bluetooth servi...	Setting
Certificate Propagation	CertPropSvc	Manual	Stopped	Copies user certific...	Setting
Indexing Service	CISVC	Automatic	Started	Indexes contents an...	Setting
Microsoft .NET Framew...	clr_optimization_v2.0.5...	Manual	Stopped	Microsoft .NET Fra...	Setting
COM+ System Applicati...	COMSysApp	Manual	Stopped	Manages the config...	Setting

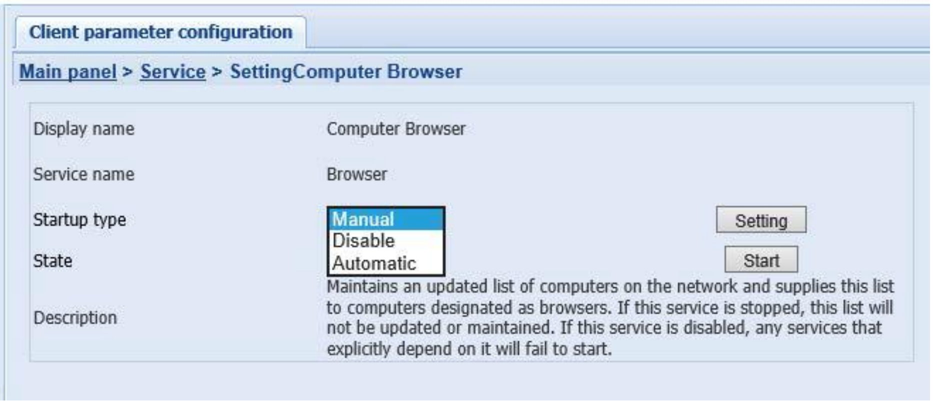
Click the “setting” corresponding to service to enter the configuration interface of specified server, as shown in following figure:



Client parameter configuration

Main panel > Service

Display Name	Service Name	Start Up T...	Status	Description	Setting
Adobe Flash Player Up...	AdobeFlashPlayerUpda...	Manual	Stopped	This service keeps...	Setting
Application Experience	AeLookupSvc	Manual	Stopped	Processes applicati...	Setting
Application Layer Gate...	ALG	Manual	Stopped	Provides support for...	Setting
Application Host Helper...	AppHostSvc	Automatic	Started	Provides administra...	Setting
Application Identity	AppIDSvc	Manual	Stopped	Determines and veri...	Setting
Application Information	Appinfo	Manual	Stopped	Facilitates the runni...	Setting
Application Management	AppMgmt	Manual	Stopped	Processes installati...	Setting
Windows Audio Endpoi...	AudioEndpointBuilder	Automatic	Started	Manages audio devi...	Setting
Windows Audio	Audiosrv	Automatic	Started	Manages audio for...	Setting
ActiveX Installer (AxInst...	AxInstSV	Manual	Stopped	Provides User Acco...	Setting
BitLocker Drive Encrypt...	BDESVC	Manual	Stopped	BDESVC hosts the...	Setting
Base Filtering Engine	BFE	Automatic	Started	The Base Filtering...	Setting
Background Intelligent...	BITS	Manual	Stopped	Transfers files in th...	Setting
Computer Browser	Browser	Manual	Stopped	Maintains an updat...	Setting
Bluetooth Support Service	bthserv	Manual	Stopped	The Bluetooth servi...	Setting
Certificate Propagation	CertPropSvc	Manual	Stopped	Copies user certific...	Setting
Indexing Service	CISVC	Automatic	Started	Indexes contents an...	Setting
Microsoft .NET Framew...	clr_optimization_v2.0.5...	Manual	Stopped	Microsoft .NET Fra...	Setting
COM+ System Applicati...	COMSysApp	Manual	Stopped	Manages the config...	Setting



Client parameter configuration

Main panel > Service > SettingComputer Browser

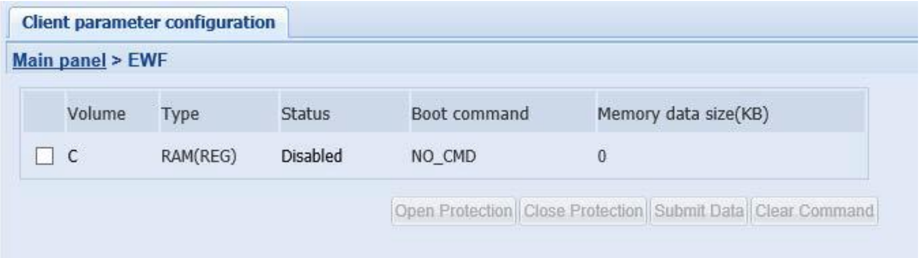
Display name	Computer Browser
Service name	Browser
Startup type	Manual Disable Automatic
State	
Description	Maintains an updated list of computers on the network and supplies this list to computers designated as browsers. If this service is stopped, this list will not be updated or maintained. If this service is disabled, any services that explicitly depend on it will fail to start.

If an administrator wants to immediately start or stop the service, the administrator can directly click “start/stop” button. If an administrator wants to set the start type of service, the administrator can select the start type in the dropdown box and then click “set” button.

4.1.1.21 UWF protection control

UWF protection control is only valid for the client with UWF module. The server can be configured with following four operations:

- Enable protection: enable the UWF protection function of the selected client.
- Disable protection: disable the UWF protection function of the selected client.

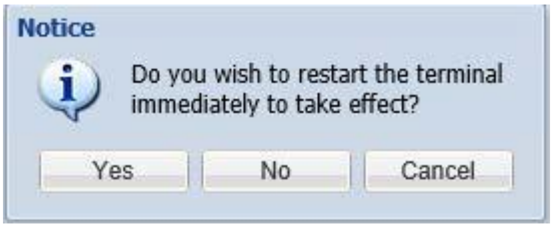


Client parameter configuration

Main panel > EWF

	Volume	Type	Status	Boot command	Memory data size(KB)
□	C	RAM(REG)	Disabled	NO_CMD	0

After executing the operation, the system will prompt the user whether to immediately restart for validating. If “Yes” is selected, the client will be immediately restarted and the strategy application will be validated. If “No” is selected, the client will not be immediately restarted and the strategy will be validated after restart of the client next time. “Cancel” refers to give up the current settings and return to configuration page.



Notice

Do you wish to restart the terminal immediately to take effect?

4.2 Power control

The module provides power control function for remote client, including restart, shutdown and WoL.

4.2.1 Control type

There are three power control types, i.e. WoL, restart and shutdown. Before operation of client, the user shall at least select one or more clients. Restart and shutdown are only valid for the online client. If the client is offline, the task will be in failure.

Restart and shutdown are simple and aren’t explained any more. Pay attention to following content for WoL:

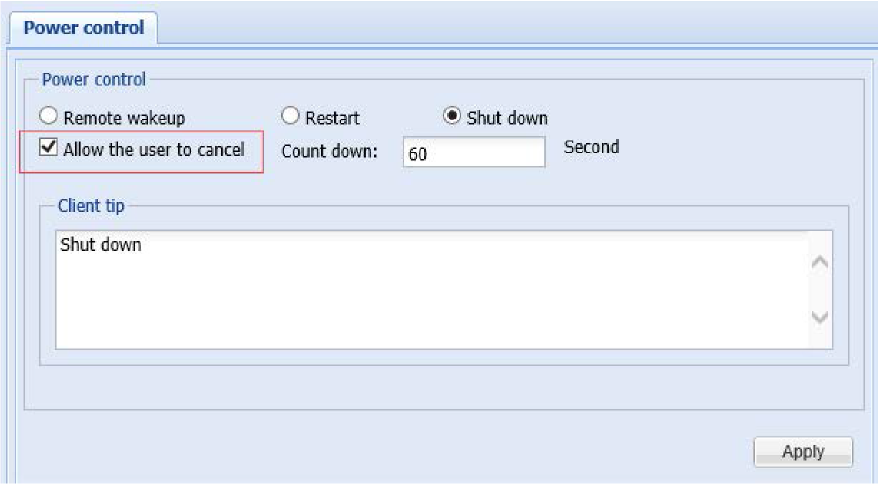
- The server and the wakened client cannot cross network segment and shall be in the same VLAN;
- Special settings of switch and other network device may cause failure of WoL function;
- If the client is in abnormal shutdown state, the client cannot be wakened.

4.2.2 Control options

The following options are available for restart and shutdown operation:

1. Allow user to cancel

After selecting this option, the command can be manually cancelled after the client receives the command. Otherwise, the client will forcibly execute the command. As shown in following figure, select “allow user to cancel” during sending the command.



Power control

Power control

○ Remote wakeup ○ Restart ● Shut down

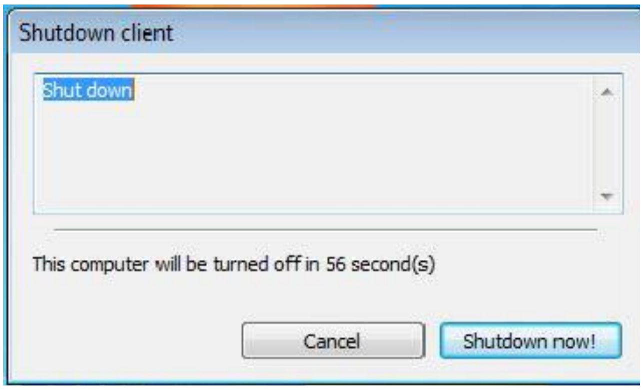
☑ Allow the user to cancel

Count down: 60 Second

Client tip

Shut down

After the client receives the command, “cancel” button will be displayed.



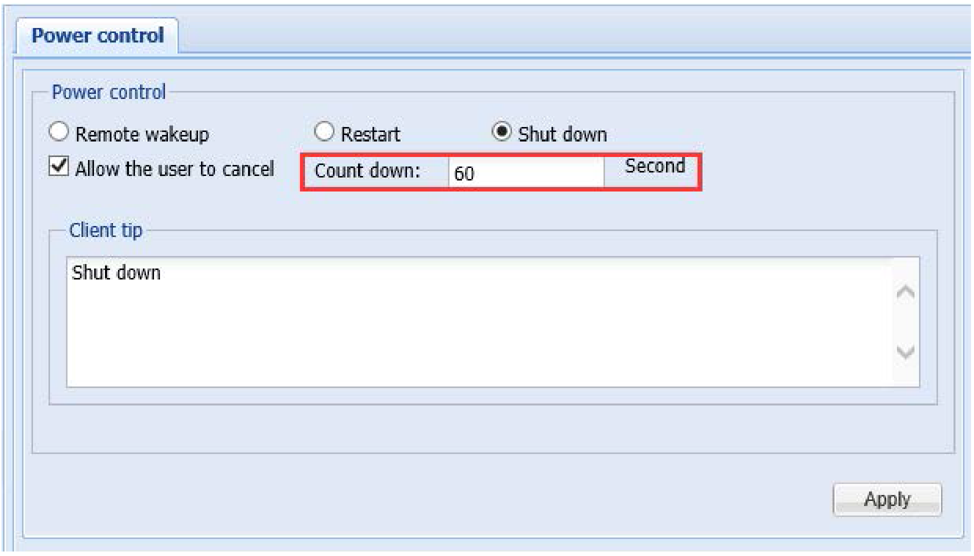
Shutdown client

Shut down

This computer will be turned off in 56 second(s)

2. Set the countdown time:

User can select this option to make the client execute command in specified time. As shown in following figure, the set time is 60s, so the client will shut down at 60s after sending the command.



Power control

Power control

○ Remote wakeup ○ Restart ● Shut down

☑ Allow the user to cancel

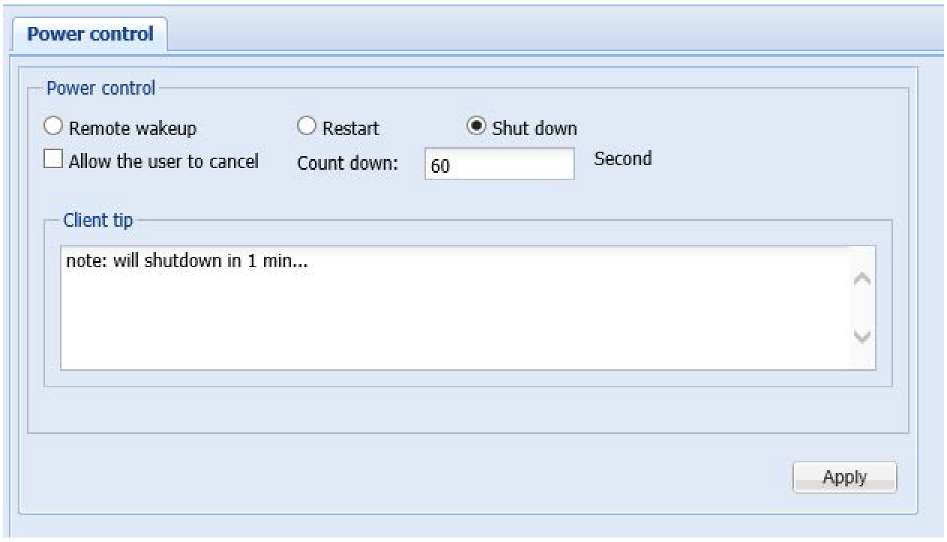
Count down: 60 Second

Client tip

Shut down

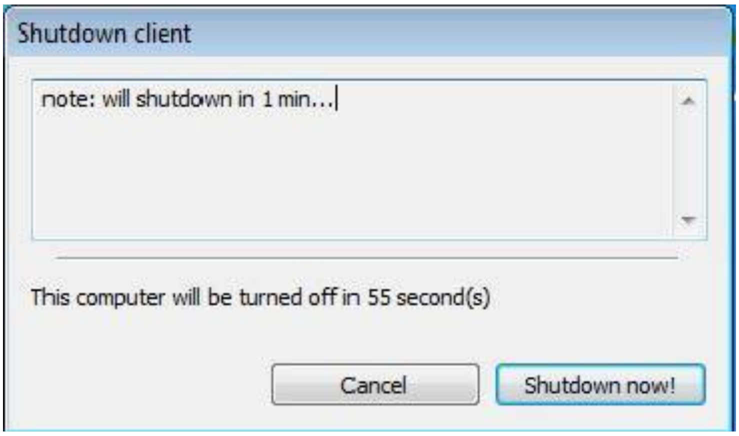
3. Add the prompt information

If the prompt is added, when the client receives the command, the prompt sent by server will be displayed. As shown in following figure, during sending the command, the client prompt will be added.



note: will shutdown in 1 min...

The commands received by the client include the prompt information sent by the server.



note: will shutdown in 1 min...

This computer will be turned off in 55 second(s)

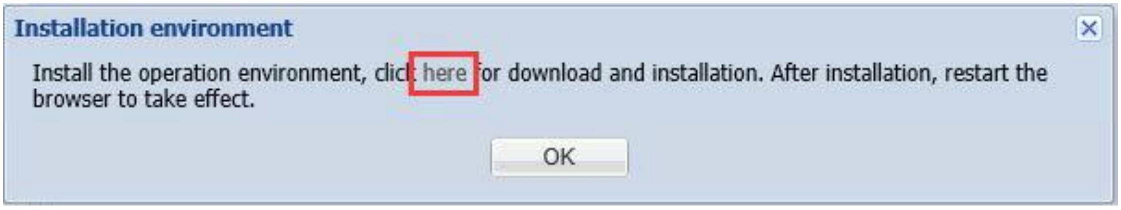
4.3 Remote assistance

The remote assistance realizes the remote monitoring of client and direct control of the client. Only one client can be monitored at the same time. In order to optimize the efficiency of network transmission, the client screen is displayed by 256 colors, so the screen may be distorted, but the control operation of mouse and keyboard will not be influenced.

4.3.1 Install JRE

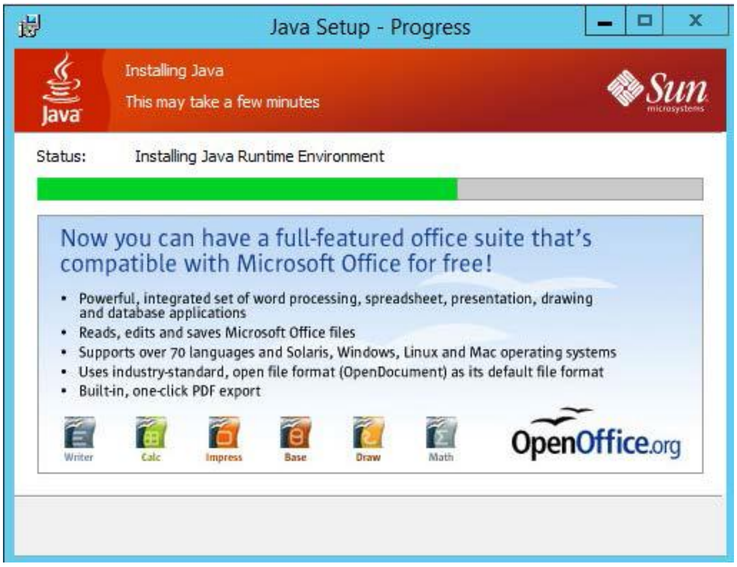
The installation step of JRE will be briefly introduced as follows:

1. Enter 【client management—>basic management—>remote assistance】, and switch to "remote assistance" tab page; select one client and click "start to view" or "start to assist"; if the current system isn't installed with JRE, the following prompt box will be popped up.



Install the operation environment, click here for download and installation. After installation, restart the browser to take effect.

2. Click to finish the installation of jre environment according to the prompt.



Java Setup - Progress

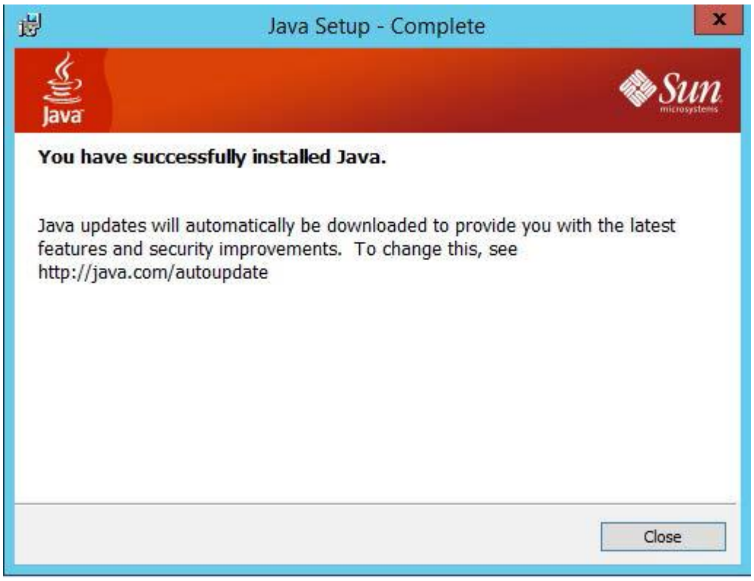
Installing Java

This may take a few minutes

Status: Installing Java Runtime Environment

Now you can have a full-featured office suite that's compatible with Microsoft Office for free!

- Powerful, integrated set of word processing, spreadsheet, presentation, drawing and database applications
- Reads, edits and saves Microsoft Office files
- Supports over 70 languages and Solaris, Windows, Linux and Mac operating systems
- Uses industry-standard, open file format (OpenDocument) as its default file format
- Built-in, one-click PDF export

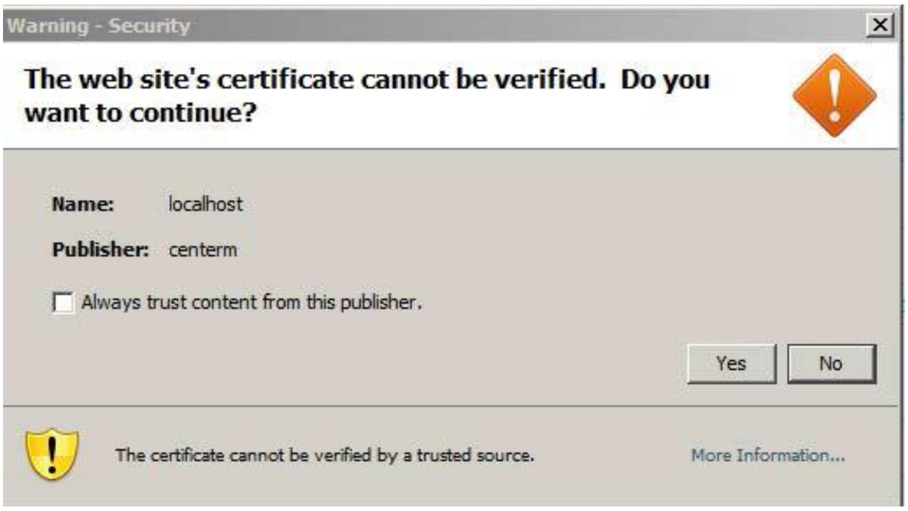


Java Setup - Complete

You have successfully installed Java.

Java updates will automatically be downloaded to provide you with the latest features and security improvements. To change this, see http://java.com/autoupdate

3. Restart the browser. If the monitoring function is executed again, the security alert box will be popped up. Select “Yes”.



Warning - Security

The web site's certificate cannot be verified. Do you want to continue?

Name: localhost

Publisher: centerm

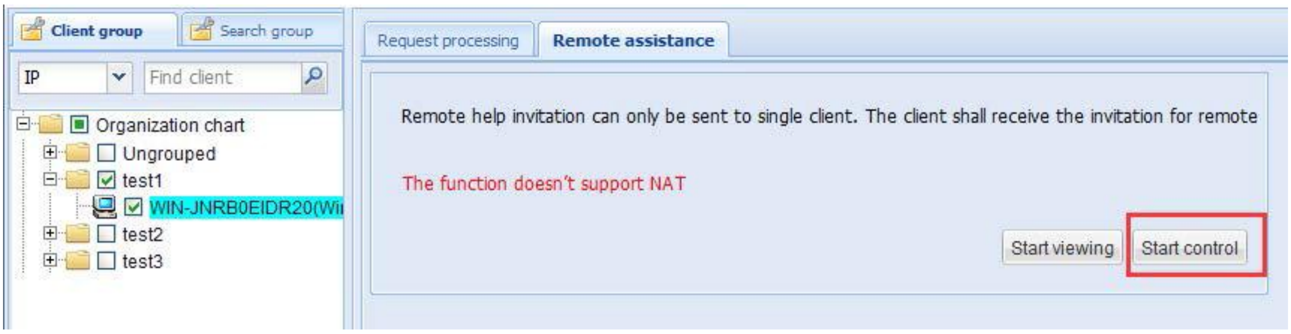
□ Always trust content from this publisher.

The certificate cannot be verified by a trusted source.

4.3.2 Remote assistance

1. After installing the JRE environment, select a client and click “start viewing” or “start control”; the

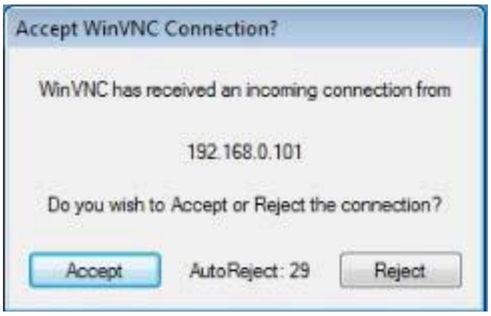
difference between view and control is that the view operation only enables view and disables any operation of the client;



Remote help invitation can only be sent to single client. The client shall receive the invitation for remote

The function doesn't support NAT

2. By default, the precondition of remote assistance of client is that the client accepts the request. The following screen will be popped up in the client:



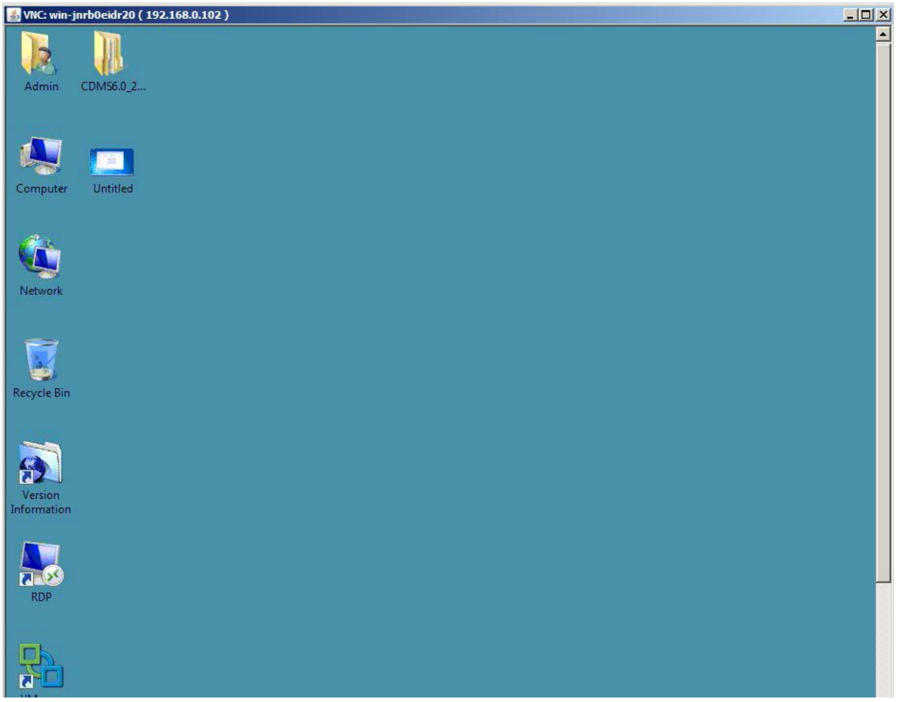
Accept WinVNC Connection?

WinVNC has received an incoming connection from

192.168.0.101

Do you wish to Accept or Reject the connection?

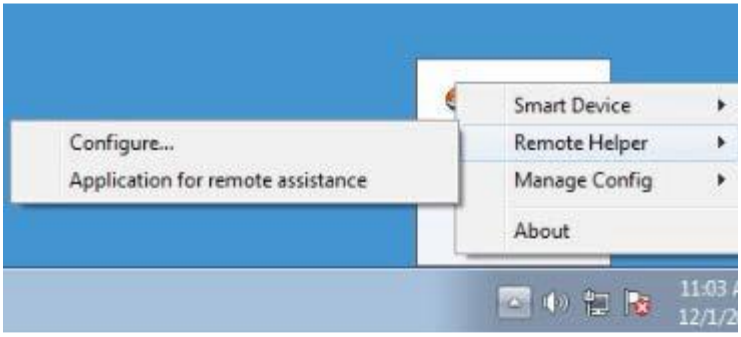
3. After the client accepts the monitoring, the server will display the monitoring screen.



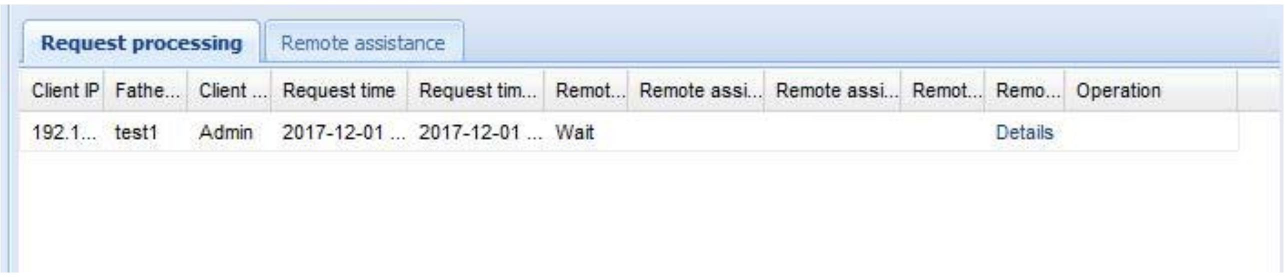
4.3.3 Request processing

The system supports the client to actively send the remote assistance invitation. The administrator judges whether to carry out assistance and selects corresponding operation on the system interface.

1. The method of request initiating from client is as shown in following figure. Select “apply for remote assistance” on the right click menu of client icon.



2. When the remote assistance request is sent from client, corresponding request item will be displayed in the list on “request processing” tab page; the administrator can select to accept or refuse the request.



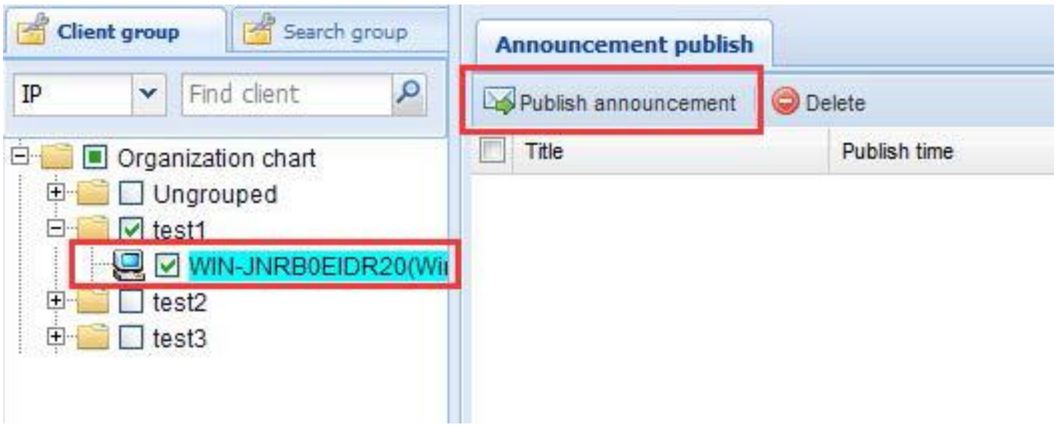
Client IP	Fathe...	Client ...	Request time	Request tim...	Remot...	Remote assi...	Remote assi...	Remot...	Remo...	Operation
192.1...	test1	Admin	2017-12-01 ...	2017-12-01 ...	Wait				Details	

4.4 Notice publish

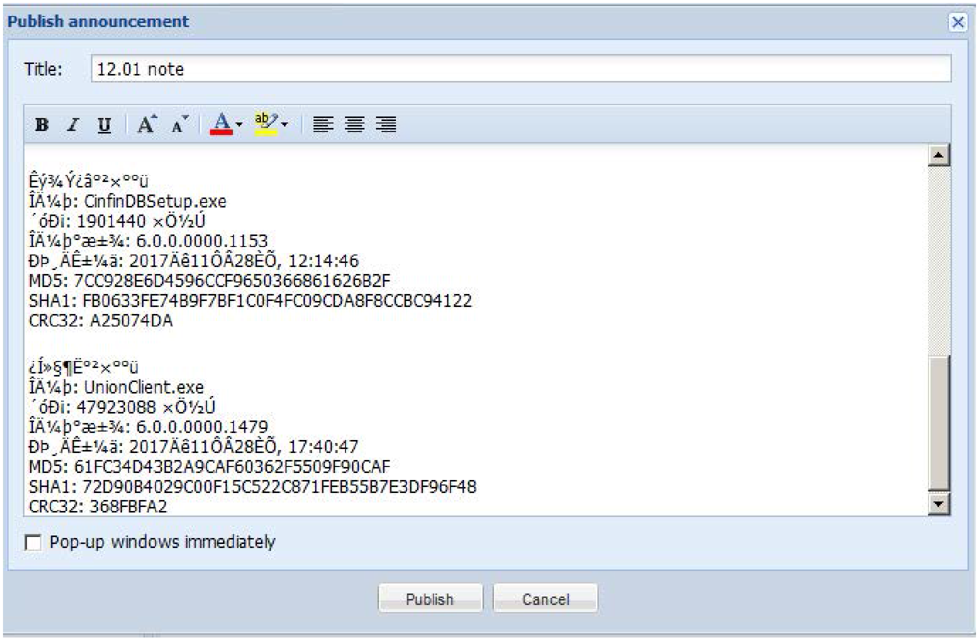
The administrator can use “notice publish” function to publish the notices by batch to the client. The function supports many text types and formats. Besides, the administrator can make statistics and query for notice sending and confirming situation.

4.4.1 Publish notice

1. Select the client or client group and click “publish notice” button.



2. In the popup dialog box, fill in a title less than 50 words and content less than 2000 words, and finally click “publish” button, as shown in following figure:



Title: 12.01 note

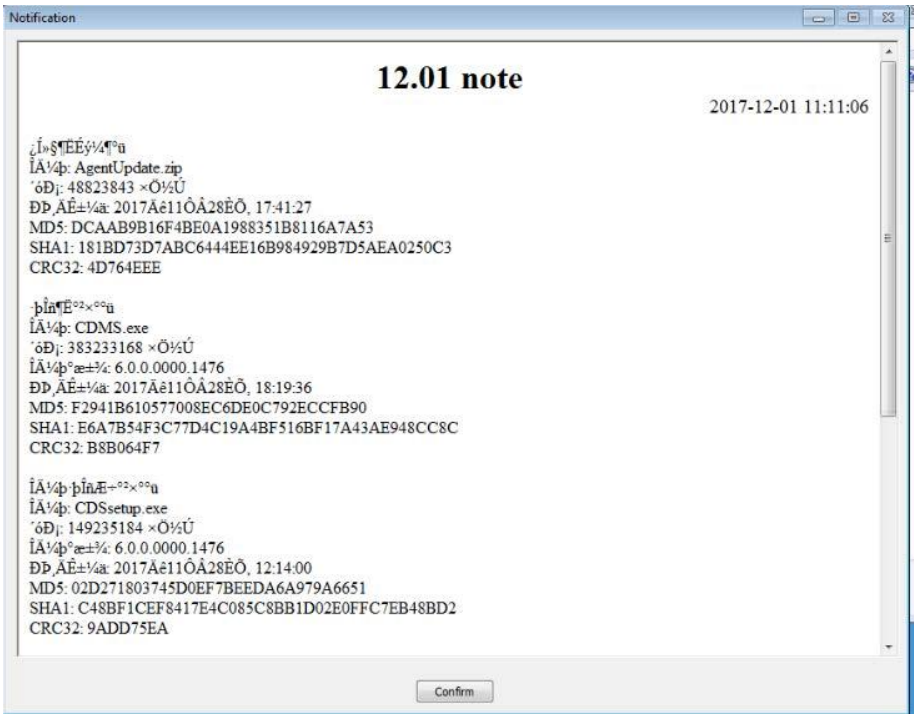
```
Êý¾Ý¿â°²×°°ü
ÎÄ¼þ: CinfinDBSetup.exe
´óÐ¡: 1901440 ×Ö½Ú
ÎÄ¼þ°æ±¾: 6.0.0.0000.1153
Ðþ¸ÄÊ±¼ä: 2017Äê11ÔÂ28ÈÕ, 12:14:46
MD5: 7CC928E6D4596CCF9650366861626B2F
SHA1: FB0633FE74B9F7BF1C0F4FC09CDA8F8CCBC94122
CRC32: A25074DA

¿Í»§¶Ë°²×°°ü
ÎÄ¼þ: UnionClient.exe
´óÐ¡: 47923088 ×Ö½Ú
ÎÄ¼þ°æ±¾: 6.0.0.0000.1479
Ðþ¸ÄÊ±¼ä: 2017Äê11ÔÂ28ÈÕ, 17:40:47
MD5: 61FC34D43B2A9CAF60362F5509F90CAF
SHA1: 72D90B4029C00F15C522C871FEB55B7E3DF96F48
CRC32: 368FBFA2
```

☐ Pop-up windows immediately

The administrator can select whether to forcibly pop up the notice on the client.

- Not forcibly pop up the notice: inform the user in notice bar of client in icon flashing mode. The notice will be popped up by double-click of user.
- Forcibly pop up the notice: directly pop up the notice in client. It is applicable to important message.

3. After the client receives the message, as for the notice not forcibly popped up, the icon in notice bar will flash. Double click on the icon to pop up the notice box. Click “already read” button to close the notice box.

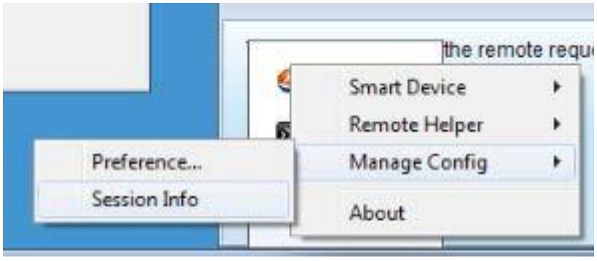


12.01 note

2017-12-01 11:11:06

```
¿Í»§¶ËÉý¼¶°ü
ÎÄ¼þ: AgentUpdate.zip
´óÐ¡: 48823843 ×Ö½Ú
ÐÞ¸ÄÊ±¼ä: 2017Äê11ÔÂ28ÈÕ, 17:41:27
MD5: DCAAB9B16F4BE0A1988351B8116A7A53
SHA1: 181BD73D7ABC6444EE16B984929B7D5AEA0250C3
CRC32: 4D764EEE

·þÎñ¶Ë°²×°°ü
ÎÄ¼þ: CDMS.exe
´óÐ¡: 383233168 ×Ö½Ú
ÎÄ¼þ°æ±¾: 6.0.0.0000.1476
ÐÞ¸ÄÊ±¼ä: 2017Äê11ÔÂ28ÈÕ, 18:19:36
MD5: F2941B610577008EC6DE0C792ECCFB90
SHA1: E6A7B54F3C77D4C19A4BF516BF17A43AE948CC8C
CRC32: B8B064F7

ÎÄ¼þ·þÎñÆ÷°²×°°ü
ÎÄ¼þ: CDSsetup.exe
´óÐ¡: 149235184 ×Ö½Ú
ÎÄ¼þ°æ±¾: 6.0.0.0000.1476
ÐÞ¸ÄÊ±¼ä: 2017Äê11ÔÂ28ÈÕ, 12:14:00
MD5: 02D271803745D0EF7BEEDA6A979A6651
SHA1: C48BF1CEF8417E4C085C8BB1D02E0FFC7EB48BD2
CRC32: 9ADD75EA
```

All notices received by the client can be viewed in the historic notices in right click of tray icon of the client.

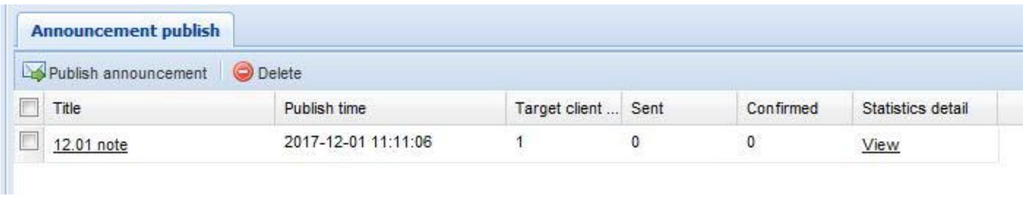


4.4.2 View publish result

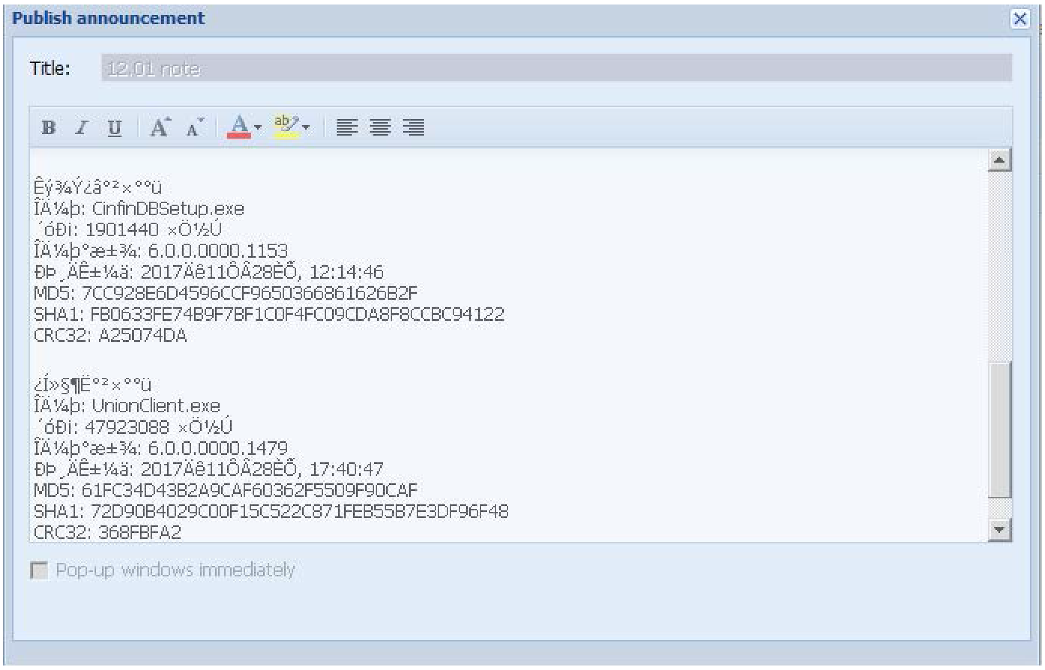
After successfully publishing the notice, the notice record will be generated in the list to display the publish result of corresponding notice.

1. View the notice content

Click the corresponding link of the title to view the detailed content of notice. However, the content cannot be edited.



□	Title	Publish time	Target client ...	Sent	Confirmed	Statistics detail
□	12.01 note	2017-12-01 11:11:06	1	0	0	View



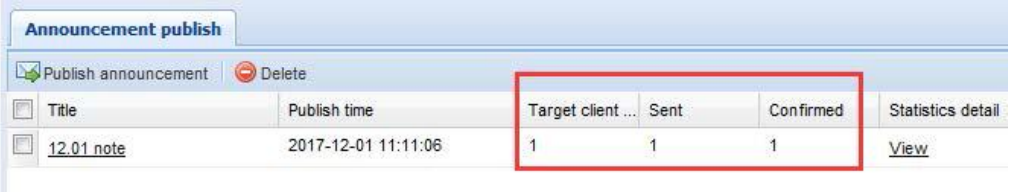
Title: 12.01 note

```
Êý¾Ý¿â°²×°°ü
ÎÄ¼þ: CinfinDBSetup.exe
´óÐ¡: 1901440 ×Ö½Ú
ÎÄ¼þ°æ±¾: 6.0.0.0000.1153
Ðþ¸ÄÊ±¼ä: 2017Äê11ÔÂ28ÈÕ, 12:14:46
MD5: 7CC928E6D4596CCF9650366861626B2F
SHA1: FB0633FE74B9F7BF1C0F4FC09CDA8F8CCBC94122
CRC32: A25074DA

¿Í»§¶Ë°²×°°ü
ÎÄ¼þ: UnionClient.exe
´óÐ¡: 47923088 ×Ö½Ú
ÎÄ¼þ°æ±¾: 6.0.0.0000.1479
Ðþ¸ÄÊ±¼ä: 2017Äê11ÔÂ28ÈÕ, 17:40:47
MD5: 61FC34D43B2A9CAF60362F5509F90CAF
SHA1: 72D90B4029C00F15C522C871FEB55B7E3DF96F48
CRC32: 368FBFA2
```

□ Pop-up windows immediately

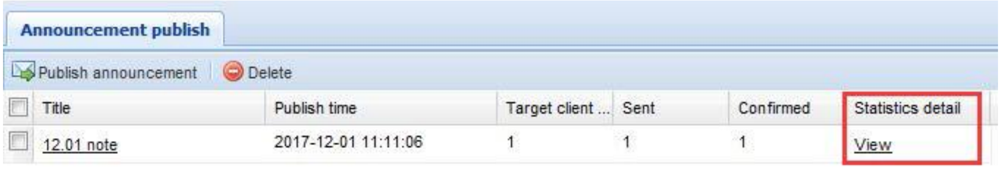
2. View the publish result

Each notice record will include corresponding publish situation, including total number of target clients to which the notice is published, the number of clients to which the notice has been published and the number of clients which have confirmed. The client to which the notice has been published refers to the client which receives the notice, but not confirms by clicking "already read" button.

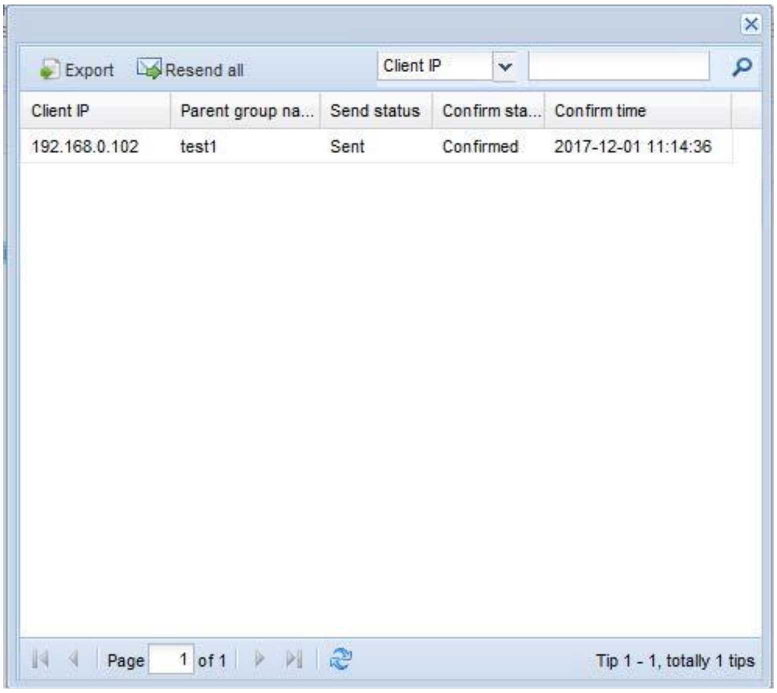


□	Title	Publish time	Target client ...	Sent	Confirmed	Statistics detail
□	12.01 note	2017-12-01 11:11:06	1	1	1	View

If the user wants to know the receiving and confirming situation of all clients further, the user can click “view” button to view the publish situation of all clients in the popup dialog box.



	Title	Publish time	Target client ...	Sent	Confirmed	Statistics detail
□	12.01 note	2017-12-01 11:11:06	1	1	1	View



Client IP	Parent group na...	Send status	Confirm sta...	Confirm time
192.168.0.102	test1	Sent	Confirmed	2017-12-01 11:14:36

4.5 File deployment

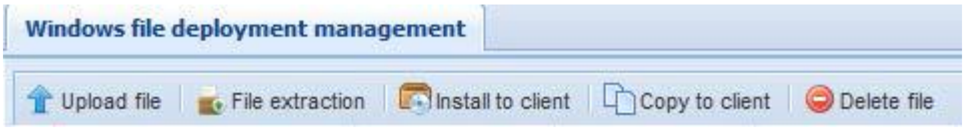
The file deployment is mainly used for deploying files in the system, including copy of file and distribution of software. It is mainly applicable to batch installation of application software of client and batch distribution of files. Besides, the file deployment can realize the management of files in the system, including the upload and deletion of files, etc.

4.5.1 Windows file deployment management

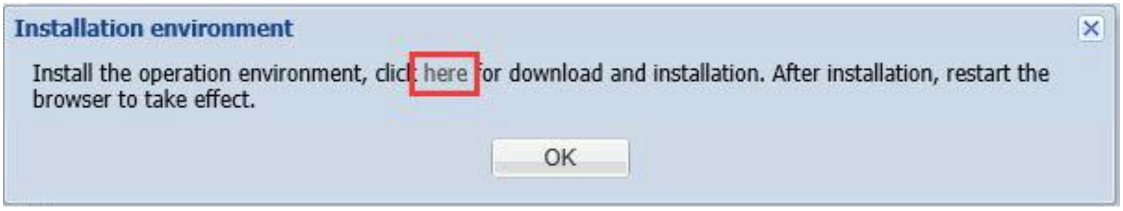
4.5.1.1 Upload file

1. Initialize the upload environment

Click “upload file” button, as follows:



If the system of browser isn’t installed with JRE run environment or JRE version is too low, the system will prompt to install JRE, as shown in following figure:

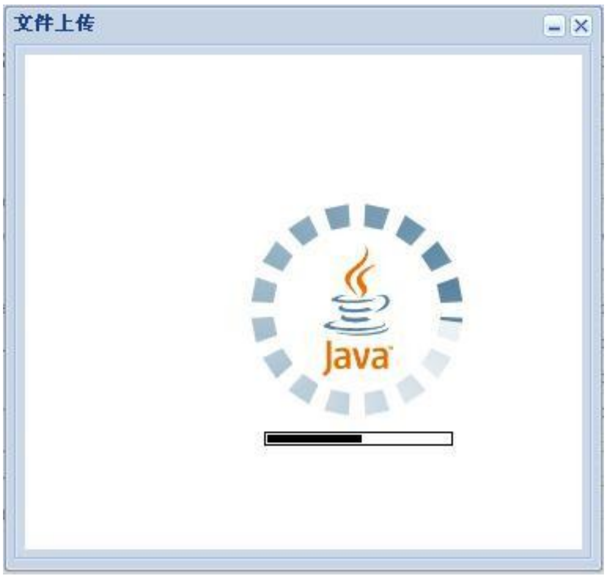


Install the operation environment, click here for download and installation. After installation, restart the browser to take effect.

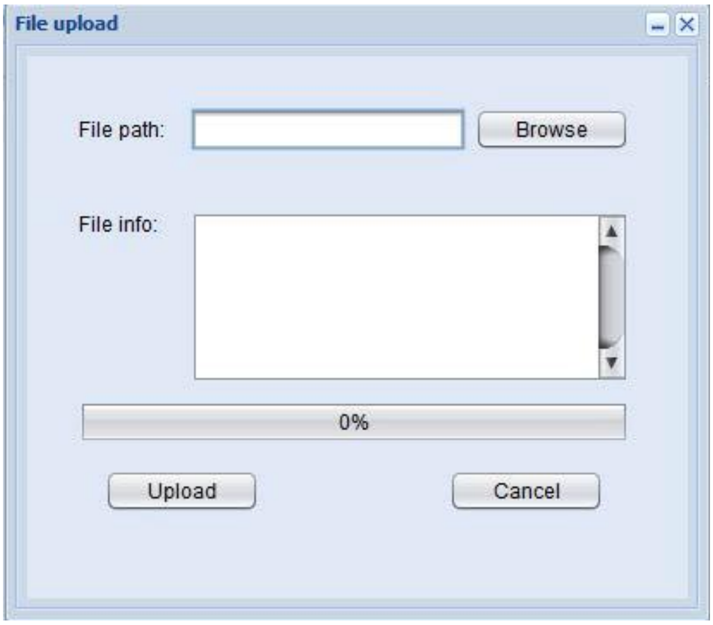
Click download and install JRE. Then, restart the browser.

2. Initialize the upload component

After installing JRE, restart the browser and click “upload file” button again to initialize applet, as follows:

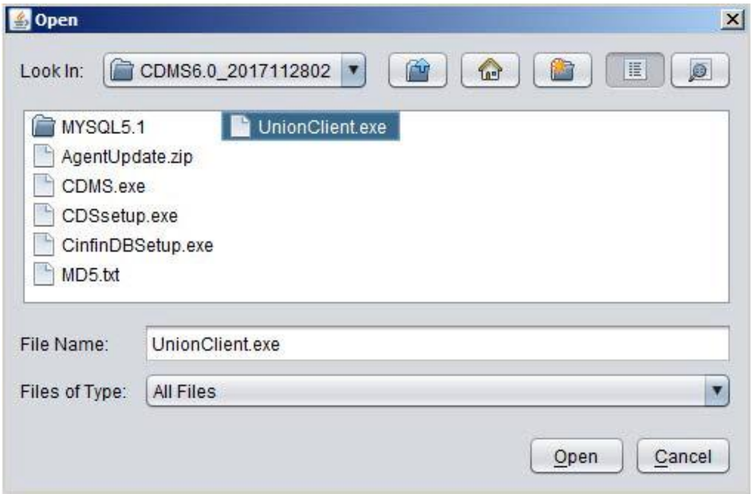


The upload interface after initialization is as follows:



3. Select the file to be uploaded

Click “browse” button, select the file or folder to be uploaded, select corresponding file in the popup file selection window, and click “open”.



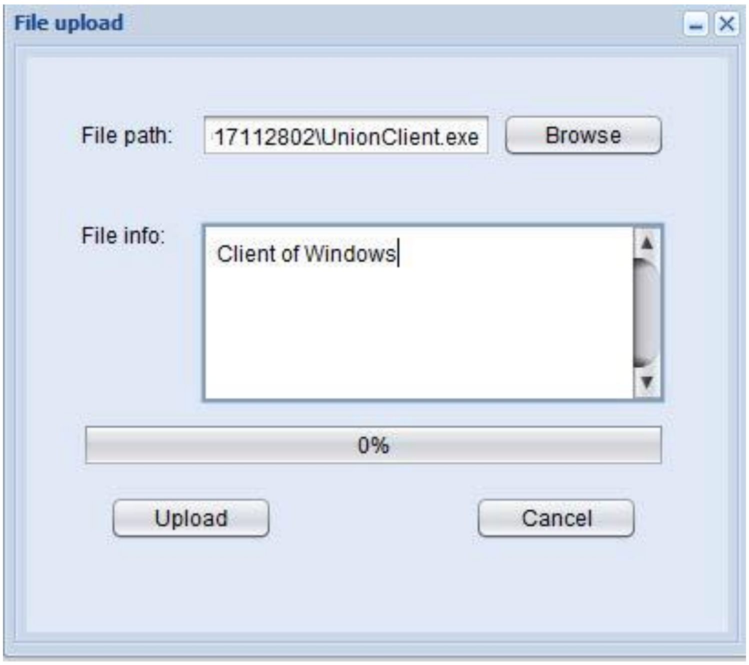
Look In: CDMS6.0_2017112802

MYSQL5.1
AgentUpdate.zip
CDMS.exe
CDSsetup.exe
CinfinDBSetup.exe
MD5.txt
UnionClient.exe

File Name: UnionClient.exe

Files of Type: All Files

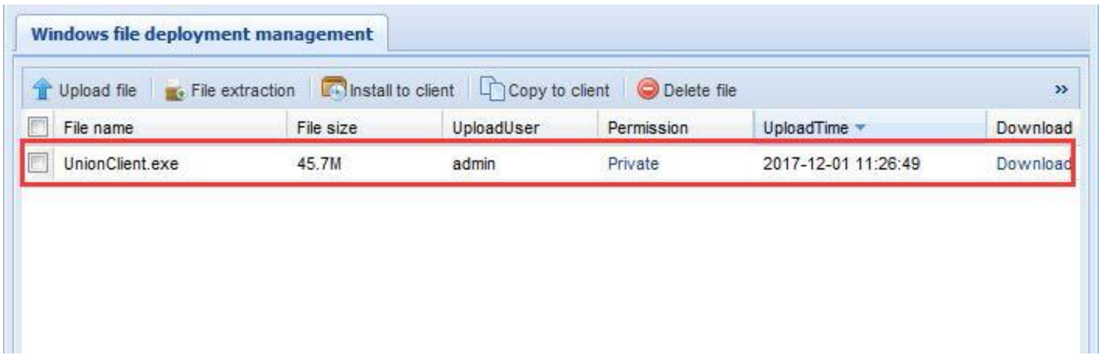
Fill in the file description and click “upload” to start uploading the file;



File path: 17112802\UnionClient.exe

File info: Client of Windows

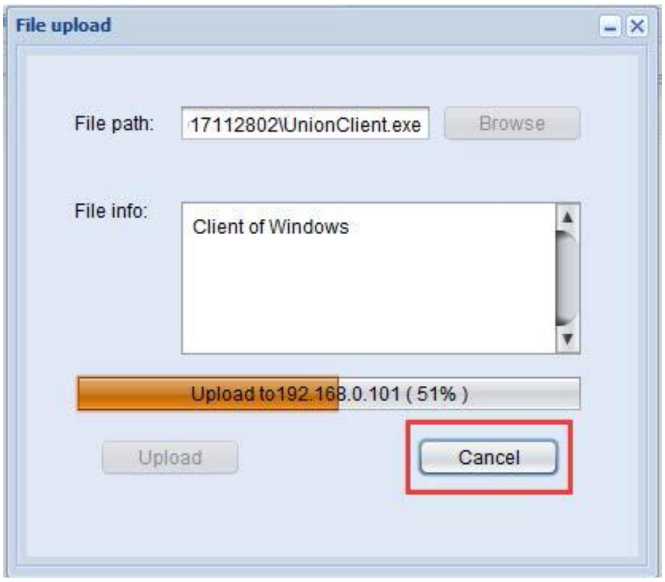
4. After successful uploading, the uploaded file will be added in the file list, as shown in following figure:



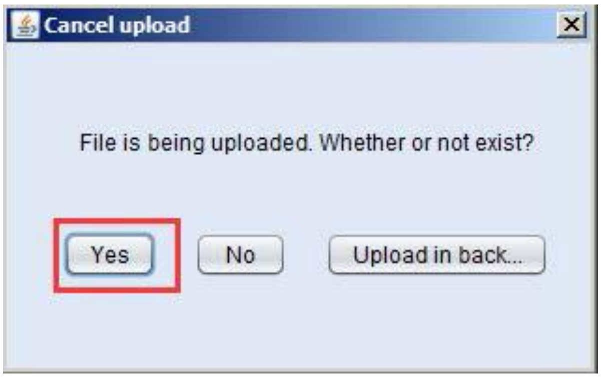
□	File name	File size	UploadUser	Permission	UploadTime	Download
□	UnionClient.exe	45.7M	admin	Private	2017-12-01 11:26:49	Download

5. Cancel upload

During uploading of file, the upload can be cancelled by click “cancel” button:

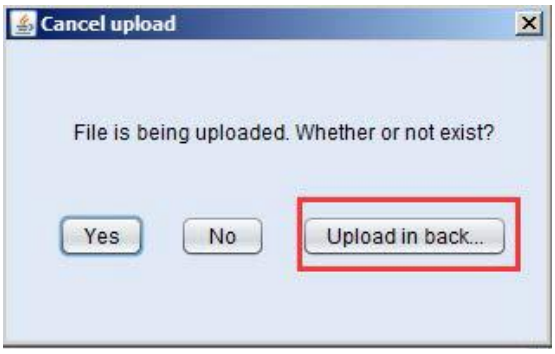


Select “Yes” to exit the upload.

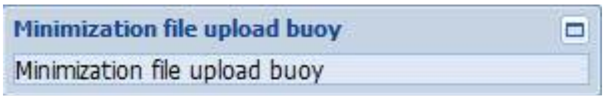


6. Background upload

During uploading of file, minimize the upload window to realize the background upload or select the background upload in the cancellation window.



After minimizing the upload window, click the maximization button to restore the window.

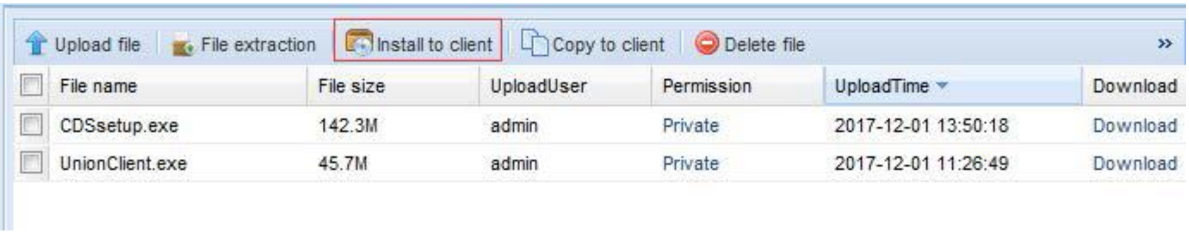


4.5.1.2 Install software

Software installation refers to distribution of software stored in the server to the client as well as installation operation. The traditional software distribution, as for system administrator, is distribution of the updated software to many work stations, which is undoubtedly the most tedious task. Software distribution function of Centerm desktop management system facilitates the batch distribution of software and also helps the network administrator to prevent from virus source or potential safety hazard caused by software installation without authorization.

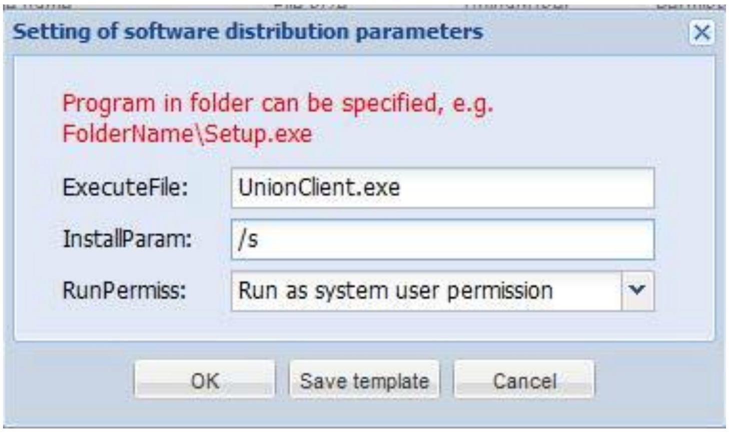
The specific operation steps are as follows:

1. Select the client to be installed with software from the client tree, select the software to be installed from the file list and click “install to client” button:



□	File name	File size	UploadUser	Permission	UploadTime ▾	Download
□	CDSsetup.exe	142.3M	admin	Private	2017-12-01 13:50:18	Download
□	UnionClient.exe	45.7M	admin	Private	2017-12-01 11:26:49	Download

2. Fill in the silent installation parameters (ensure silent installation of software in the client), and click OK:


Setting of software distribution parameters

Program in folder can be specified, e.g. FolderName\Setup.exe

ExecuteFile: UnionClient.exe

InstallParam: /s

RunPermiss: Run as system user permission

The description of installation parameters is as follows:

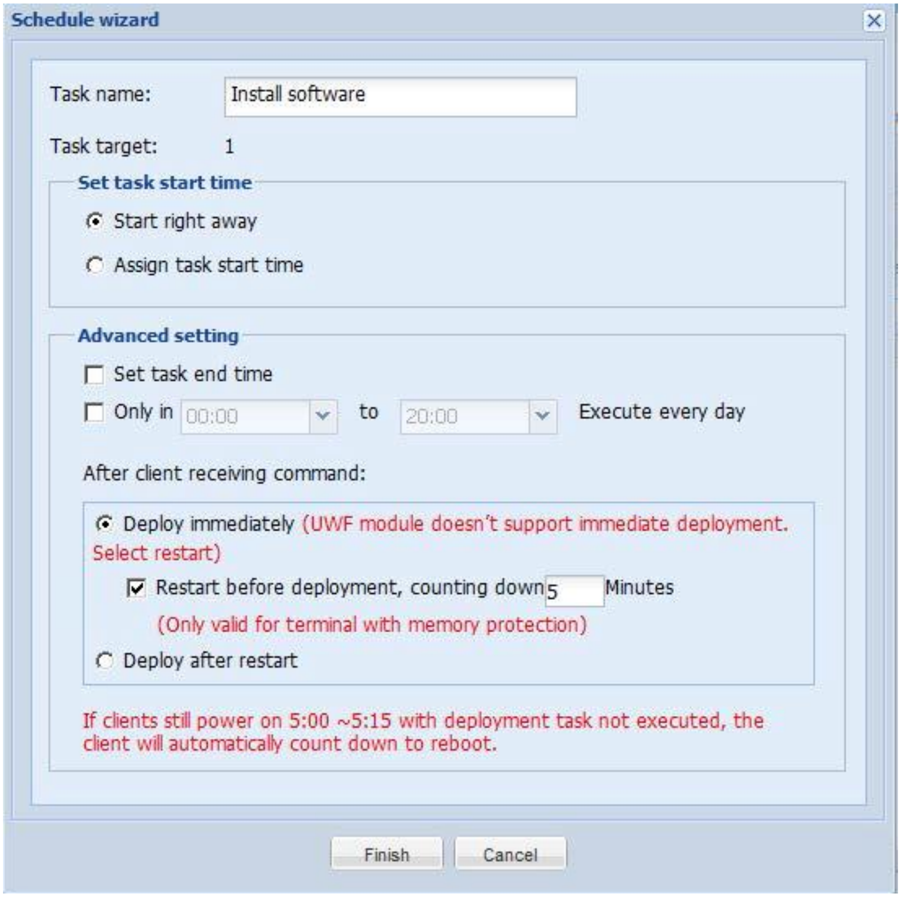
This item is option and is the parameters used during installation of software in client. It is empty by default, which refers to the non-silent installation and may require manual intervention. The parameters of different software are different (in general situation, the parameters aren’t used). If the parameters are used, please contact the software provider for support;

Take jre as an example. The following parameters are available:

- /quiet quiet mode without user interaction
- /passive no participation mode-only display the process bar
- /q[n|b|r|f] set the user interface class n －no user interface; b －basic interface r －refined interface f –finished interface (default)

3. Configure the plan wizard and execute the task

Notice: if select “immediately prompt and execute after countdown restart” in execution setting of the client, the client will pop up the restart prompt. The client user will select whether to restart immediately for installation; if “no prompt, execute in restart next time” is selected, it is defaulted that the client carries out file deployment in start next time.



Schedule wizard

Task name: Install software

Task target: 1

Set task start time

● Start right away

○ Assign task start time

Advanced setting

□ Set task end time

□ Only in 00:00 to 20:00 Execute every day

After client receiving command:

● Deploy immediately (UWF module doesn't support immediate deployment. Select restart)

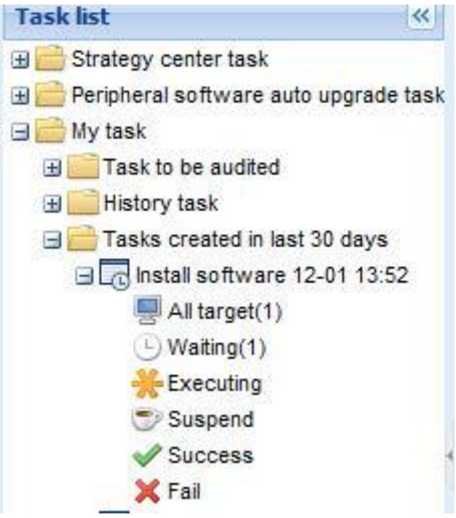
☑ Restart before deployment, counting down 5 Minutes

(Only valid for terminal with memory protection)

○ Deploy after restart

If clients still power on 5:00 ~5:15 with deployment task not executed, the client will automatically count down to reboot.

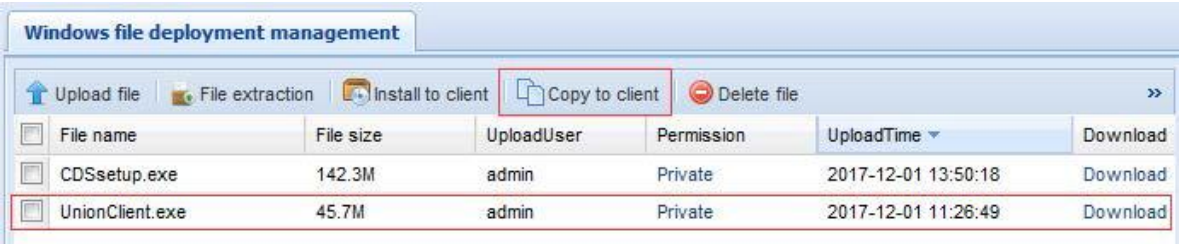
4. The results and process information of software distribution are displayed on the task execution state panel, as shown in the following figure:



4.5.1.3 Copy file

The file copy function is used for copying the prepared file to the specified client. Its operation steps are similar to software installation steps and are briefly introduced as follows:

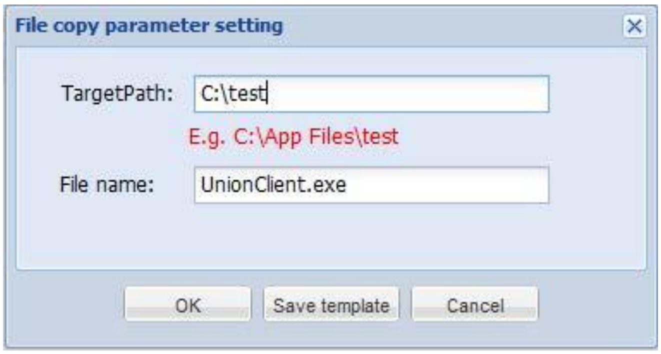
1. Select the client to copy file from the client tree, select the file to be copied from the file list and click "Copy to client" button.



Windows file deployment management

□	File name	File size	UploadUser	Permission	UploadTime	Download
□	CDSsetup.exe	142.3M	admin	Private	2017-12-01 13:50:18	Download
□	UnionClient.exe	45.7M	admin	Private	2017-12-01 11:26:49	Download

2. Fill in the saving path of file in the client and click OK:



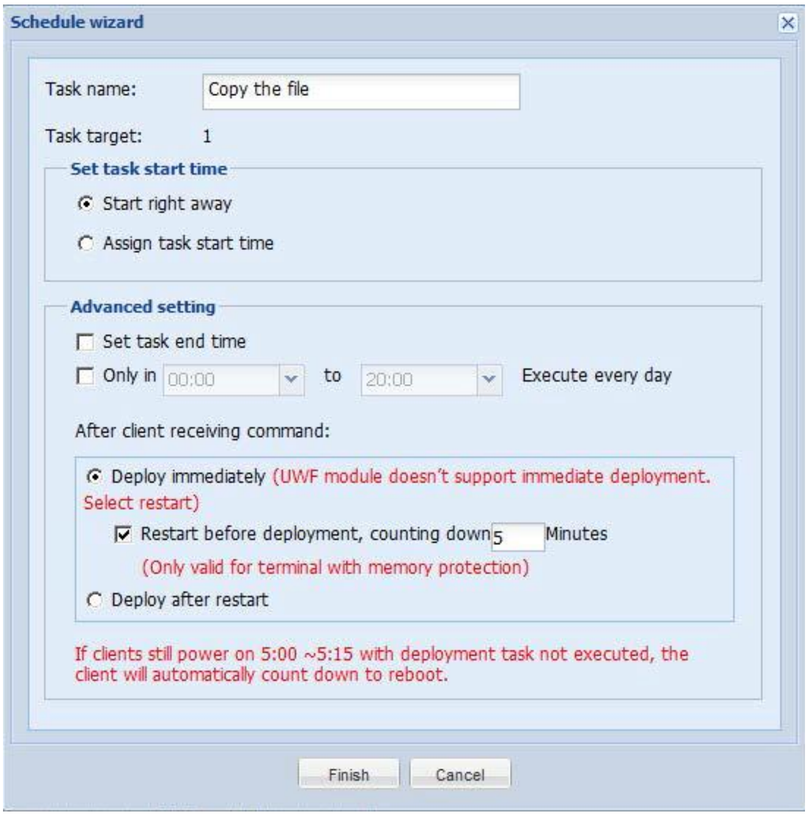
File copy parameter setting

TargetPath: C:\test

E.g. C:\App Files\test

File name: UnionClient.exe

3. Configure the plan wizard and execute the task



Schedule wizard

Task name: Copy the file

Task target: 1

Set task start time

● Start right away

○ Assign task start time

Advanced setting

□ Set task end time

□ Only in 00:00 to 20:00 Execute every day

After client receiving command:

● Deploy immediately (UWF module doesn't support immediate deployment. Select restart)

☑ Restart before deployment, counting down 5 Minutes

(Only valid for terminal with memory protection)

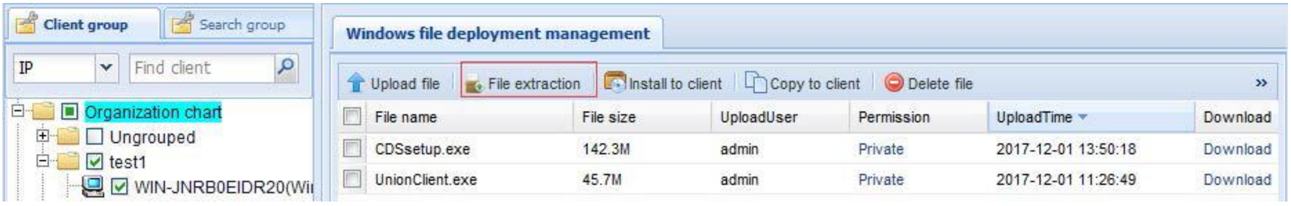
○ Deploy after restart

If clients still power on 5:00 ~5:15 with deployment task not executed, the client will automatically count down to reboot.

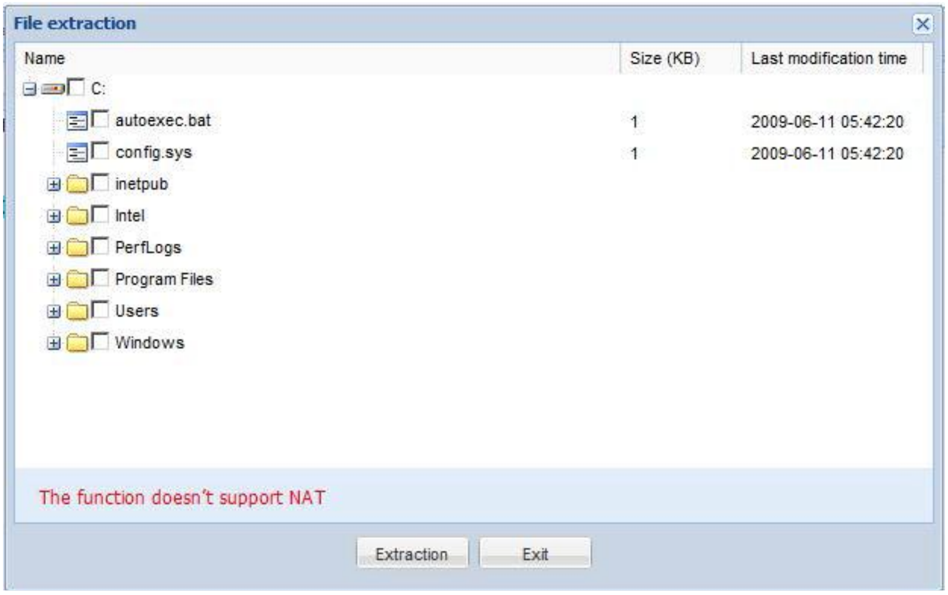
4.5.1.4 Extract file

If the administrator needs to acquire file from local client, this function can be used to directly extract. This function is only valid for Windows client.

Operation steps: select the single client, click “extract file” button and browse and select the file or folder to be extracted from the list.



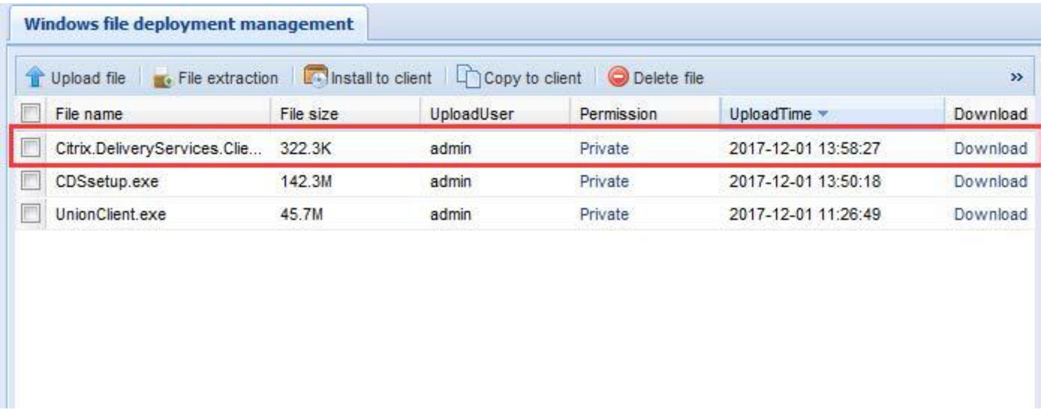
□	File name	File size	UploadUser	Permission	UploadTime	Download
□	CDSsetup.exe	142.3M	admin	Private	2017-12-01 13:50:18	Download
□	UnionClient.exe	45.7M	admin	Private	2017-12-01 11:26:49	Download



Name	Size (KB)	Last modification time
□ C:		
□ autoexec.bat	1	2009-06-11 05:42:20
□ config.sys	1	2009-06-11 05:42:20
□ inetpub		
□ Intel		
□ PerfLogs		
□ Program Files		
□ Users		
□ Windows		

The function doesn't support NAT

The file list shows the extracted file.



□	File name	File size	UploadUser	Permission	UploadTime	Download
□	Citrix.DeliveryServices.Clie...	322.3K	admin	Private	2017-12-01 13:58:27	Download
□	CDSsetup.exe	142.3M	admin	Private	2017-12-01 13:50:18	Download
□	UnionClient.exe	45.7M	admin	Private	2017-12-01 11:26:49	Download

4.6 System image

OS often has virus, crash, system crash and other problems during running. Reinstallation of operation system and business system of client device is very complicated, spends a lot of time and influences the normal business flow of an enterprise. The system image function module can help the enterprise to rapidly install, restore and backup the client device system.

4.6.1 Notices of use

4.6.1.1 Anti-virus software installed in client

If the client is installed with anti-virus software, the function of system image may be influenced at certain degree. Therefore, during extracting image, disable the anti-virus software or add relevant processes of system image into the exception list of anti-virus software according to the following mode.

As for WIN7\WES7 system, the exceptional processes to be added are:

A. Client installation directory

--UniFrm2.exe, C:\ProgramFiles\UniFrame3\UniFrm2.exe by default

--grubinst.exe, C:\ProgramFiles\UniFrame3\DDS\grub\grubinst.exe by default

--grubinstutil.exe, C:\ProgramFiles\UniFrame3\DDS\grub\grubinstutil.exe by default

B. System directory, C:\Windows\System32 in most cases

--XPeDDSInit.exe, C:\Windows\System32\XPeDDSInit.exe

--sysprep_back.exe, C:\Windows\System32\sysprep_back.exe

--sysprep.exe, C:\Windows\System32\sysprep.exe

--CentermWin7deploy.exe, C:\Windows\System32\CentermWin7deploy.exe

--oobe directory, C:\Windows\System32\oobe directory

4.6.1.2 Different installation disk identifiers of client

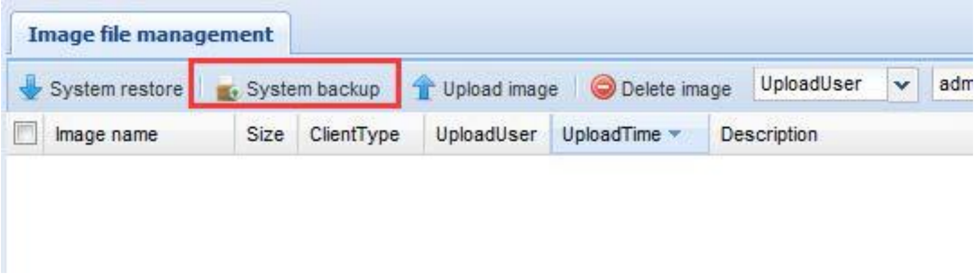
The installation disk identifiers of backed up client and the restored client shall be the same. The reason is that the system image function only can back up the information of system disk and if the client is installed in non-system disk, the extracted image will not include the client software.

Therefore, if the administrator backs up image from client A, the installation disk identifier of client which is restored by image A shall be consistent with A. They shall be installed in system disk together or in non-system disk together. If they are installed in cross way, they cannot be restored normally.

4.6.2 System backup

The administrator can back up OS of client to the server. If the client system is crashed, the client can be restored by the backed up image. Notice: "system backup" can only back up the system disk.

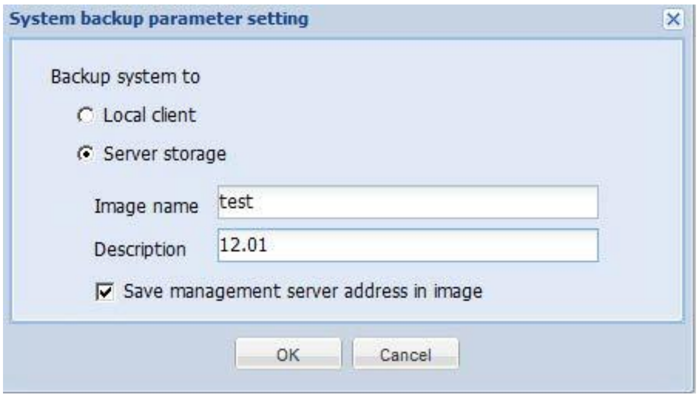
1. Select the client and click "system backup" button.



2. Select the backup mode in the popup dialog box. The system has the following two backup modes:

- Back up to local client: the backed up image file is saved in the local non-system disk with the largest residual space of client. The image file will be hidden in local partition of client.
- Back up to server: the backed up image file will be stored in the storage node added in the management server. This mode is influenced by network environment. Enough network bandwidth shall be ensured.

Besides, the administrator can select whether to keep the management server address in image. If the address isn't kept, when the image is restored to other client, the management server address is empty.


System backup parameter setting

Backup system to

○ Local client

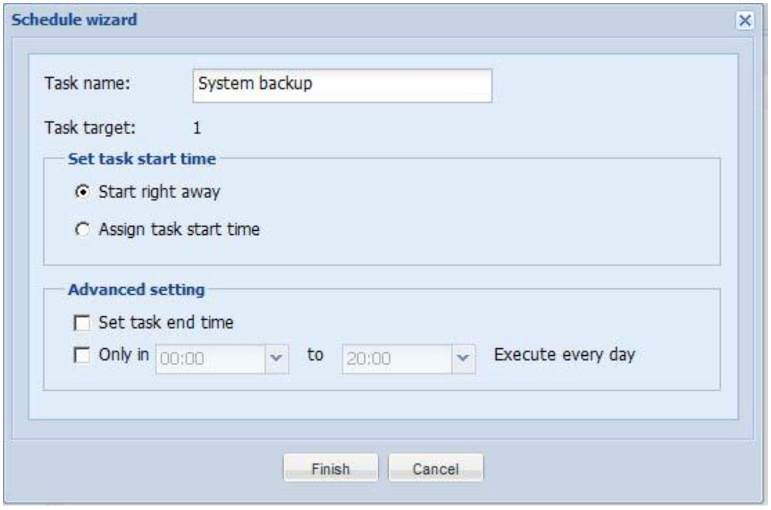
● Server storage

Image name: test

Description: 12.01

☑ Save management server address in image

3. Click "OK" button and configure the plan wizard.



Schedule wizard

Task name: System backup

Task target: 1

Set task start time

● Start right away

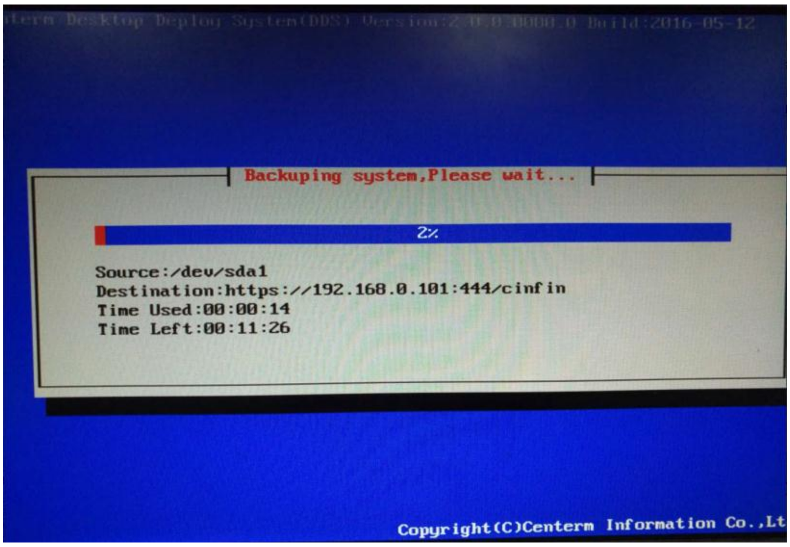
○ Assign task start time

Advanced setting

□ Set task end time

□ Only in 00:00 to 20:00 Execute every day

4. After the local partition of client receives the command, the client will firstly restart to clean the dirty data; after entering the desktop, the desktop will display “image backup preparing”; next, the client will restart second time to enter the backup interface:

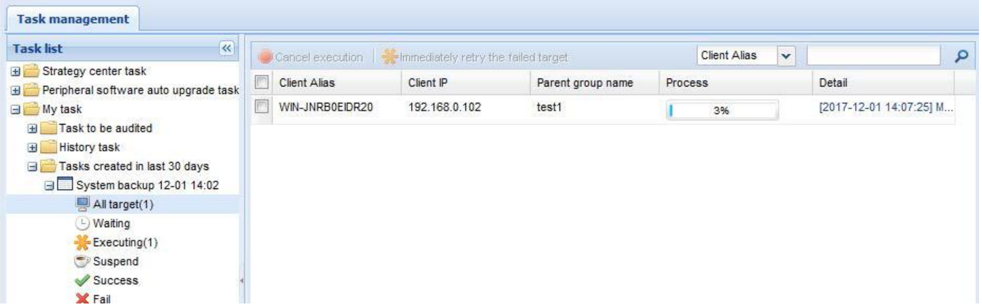


```
tERM Desktop Deploy System(DDS) Version:2.0.0.0000.0 Build:2016-05-12

Backuping system,Please wait...

2%

Source:/dev/sda1
Destination:https://192.168.0.101:444/cinfin
Time Used:00:00:14
Time Left:00:11:26

Copyright(C)Centerm Information Co.,Lt
```

Notice:

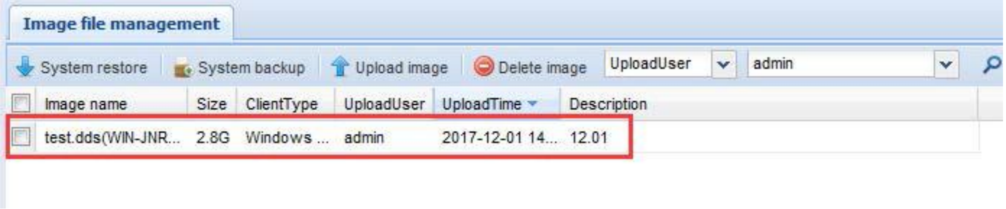
- During extracting image, the client is offline; after extracting image, the client will restart many times. Therefore, the client will be online and offline repeatedly.
- Above description is for backup to server. The interface of backup to local client is basically the same with the above mentioned interface and will not be described any more.

5. The server can display the system backup progress in task management module.



□	Client Alias	Client IP	Parent group name	Process	Detail
□	WIN-JNRB0EIDR20	192.168.0.102	test1	3%	[2017-12-01 14:07:25] M...

After backup, the backed up image file is shown in image list:

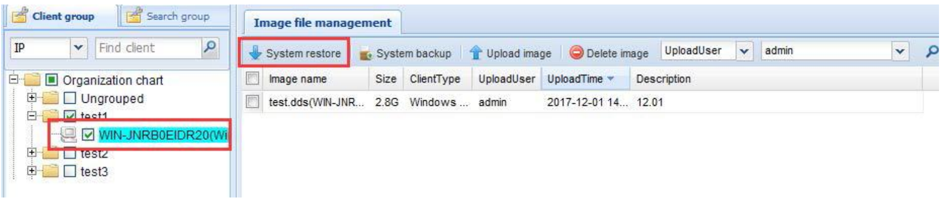


☐	Image name	Size	ClientType	UploadUser	UploadTime	Description
☐	test.dds(WIN-JNR...	2.8G	Windows ...	admin	2017-12-01 14...	12.01

4.6.3 System restore

If the client executed the system backup, the system can restore OS of client by system restore function. Notice: “system restore” only can restore the system disk.

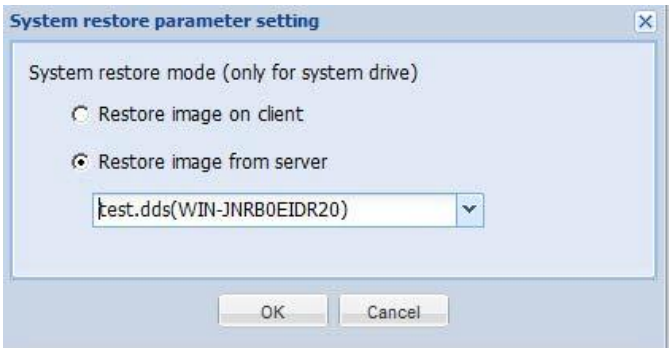
1. In system backup, there are two backup modes, i.e. back up to local client and back up to server. Therefore, there are two restore modes, as shown in following figure. Select one or more terminals. Click “system restore” button.



☐	Image name	Size	ClientType	UploadUser	UploadTime	Description
☐	test.dds(WIN-JNR...	2.8G	Windows ...	admin	2017-12-01 14...	12.01

2. In the popup dialog box, select the restore mode. Local image restore of client shall ensure the existence of backed up image in local client. Otherwise, the restore will be in failure.

The following figure demonstrates the restore by server image. Select the image file to be used from the list.



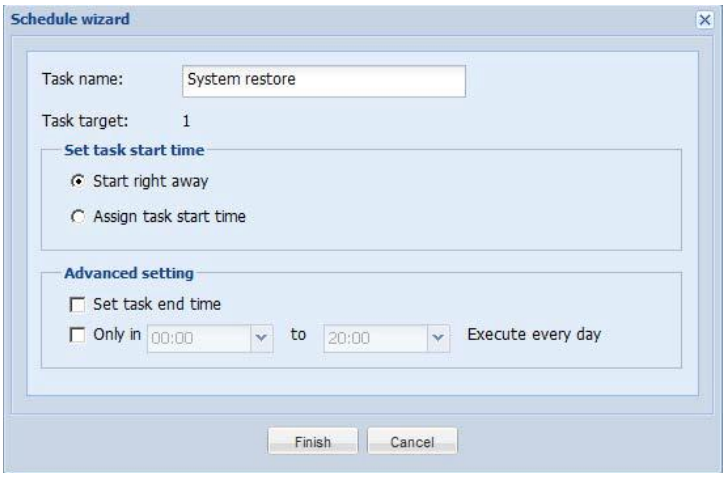
System restore mode (only for system drive)

○ Restore image on client

● Restore image from server

test.dds(WIN-JNRB0EIDR20)

3. Click “OK” and configure the plan to enter the task management module to view the restore progress.



Task name: System restore

Task target: 1

Set task start time

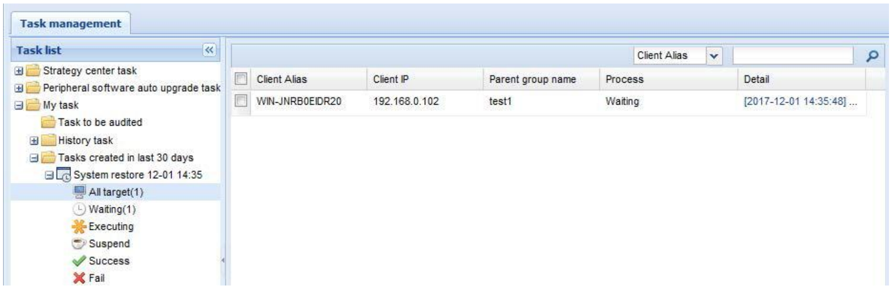
● Start right away

○ Assign task start time

Advanced setting

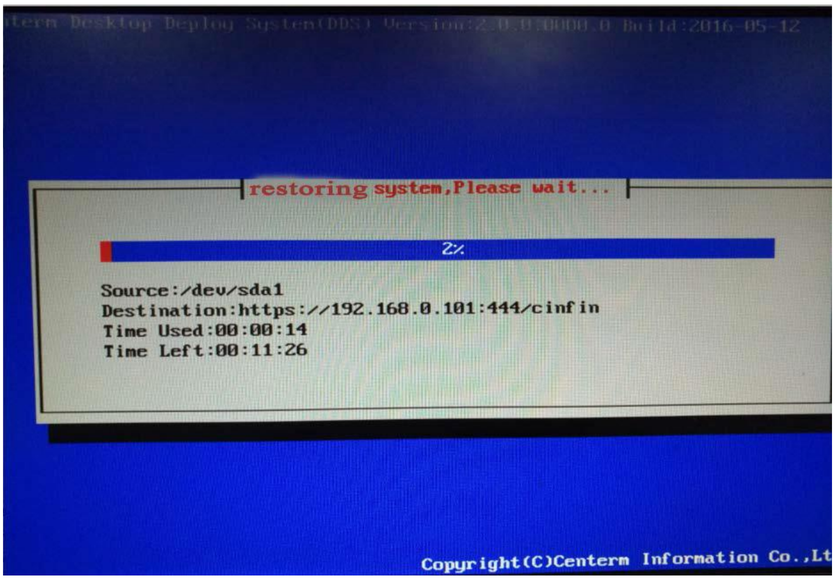
☐ Set task end time

☐ Only in 00:00 to 20:00 Execute every day



□	Client Alias	Client IP	Parent group name	Process	Detail
□	WIN-JNRB0EIDR20	192.168.0.102	test1	Waiting	[2017-12-01 14:35:48] ...

4. If the desktop of OS of client before restore can be normally used, the desktop will prompt “image restore preparing”; in restoring, the client interface is as follows:



```
term Desktop Deploy System(DDS) Version:2.0.0.0000.0 Build:2016-05-12

restoring system,Please wait...

2%

Source:/dev/sda1
Destination:https://192.168.0.101:444/cinfin
Time Used:00:00:14
Time Left:00:11:26

Copyright(C)Centerm Information Co.,Lt
```

4.7 Client upgrade

Due to increase and improvement of functions of system version, the batch version upgrade of clients within the system management range is often required. This module is only valid for upgrade of Windows clients.

The general client upgrade mode of system is: upload the upgrade files to server—>set the upgrade mode of client—>obtain upgrade files from server and upgrade—>finish upgrade of client and feed the result information back.

4.7.1 Description of upgrade files

The upgrade files are the packaged files which are stored in server and used for updating software of all clients. In the system, the upgrade files are divided into two types: main version files and patch files.

- Main version files: the complete client installation package. The server shall have these files. Otherwise, the upgrade function cannot be used;
- Patch files: the patch of client software and the non-complete installation package. The files are not necessarily uploaded to the server.

After installing the management server, the server will have complete client installation package with the same version. The client upgrade function can ensure that all managed clients are upgraded to the latest version. During uploading the patch files, the patch files shall be matched with the main version. Otherwise, the upload will be in failure.

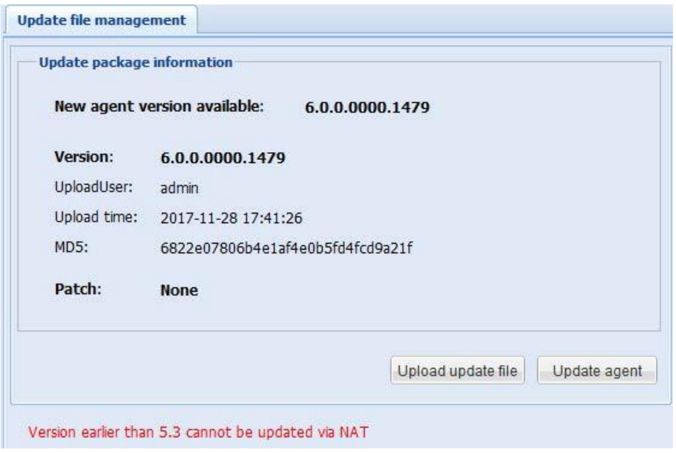
4.7.2 Upload upgrade files

1. The client version can only be upgraded by upgrade files of Centerm Information Co., Ltd.

2. Confirm that the client group to be upgraded has bound the available storage node. Refer to the chapter of resource center for the binding method.

3. Enter [public management—>client upgrade] module of the system.

4. The “upgrade file management” tab page shows the version information of upgrade files of current server. As shown in following figure, the current system has client with 6.0.0.0000.775 version and has no patch package.



New agent version available: 6.0.0.0000.1479

Version: 6.0.0.0000.1479

UploadUser: admin

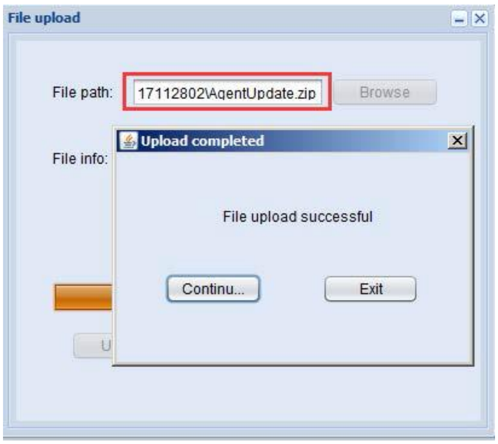
Upload time: 2017-11-28 17:41:26

MD5: 6822e07806b4e1af4e0b5fd4fcd9a21f

Patch: None

Version earlier than 5.3 cannot be updated via NAT

5. Click “upload the upgrade file” button, and select the patch package or main version files to upload, as shown in following figure:

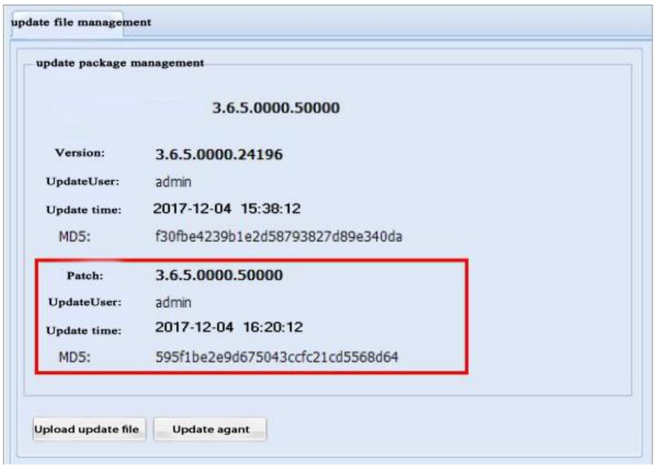


File path: 17112802\AgentUpdate.zip

File info:

File upload successful

6. After uploading, the upgrade file information has changed into the latest version, as shown in following figure:



3.6.5.0000.50000

Version: 3.6.5.0000.24196

UpdateUser: admin

Update time: 2017-12-04 15:38:12

MD5: f30fbe4239b1e2d58793827d89e340da

Patch: 3.6.5.0000.50000

UpdateUser: admin

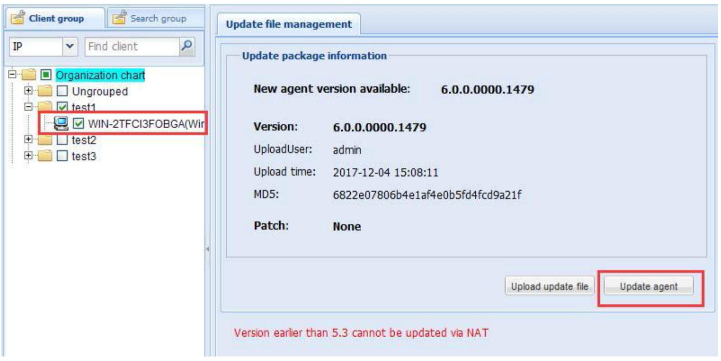
Update time: 2017-12-04 16:20:12

MD5: 595f1be2e9d675043ccfc21cd5568d64

7. Above figure shows the upload of patch files. The upload method of main version files is same with above mentioned method. However, if the uploaded main version files aren’t consistent with current main version No., all original main version and patch documents will be deleted and replaced.

4.7.3 Upgrade client

1. After uploading the patch files, execute the “upgrade the client” operation. Select the client group or client to be upgraded in the left interface, and click “immediately upgrade” button to immediately upgrade the selected client, as shown in following figure:



Update package information

New agent version available: 6.0.0.0000.1479

Version: 6.0.0.0000.1479

UploadUser: admin

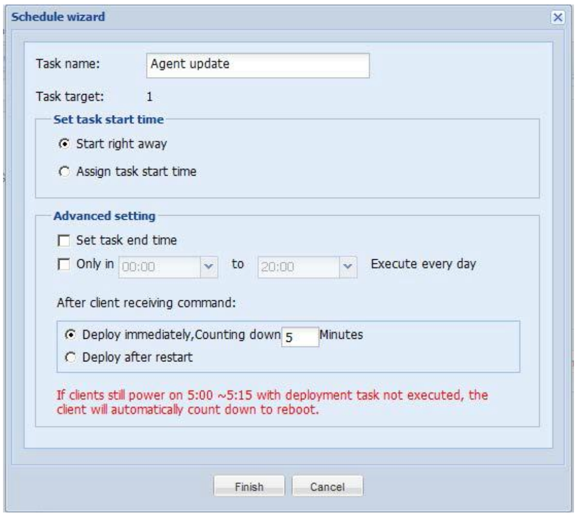
Upload time: 2017-12-04 15:08:11

MD5: 6822e07806b4e1af4e0b5fd4fcd9a21f

Patch: None

Version earlier than 5.3 cannot be updated via NAT

2. In the popup plan wizard configuration window, set the execution conditions of the task.



Task name: Agent update

Task target: 1

Set task start time

● Start right away

○ Assign task start time

Advanced setting

□ Set task end time

□ Only in 00:00 to 20:00 Execute every day

After client receiving command:

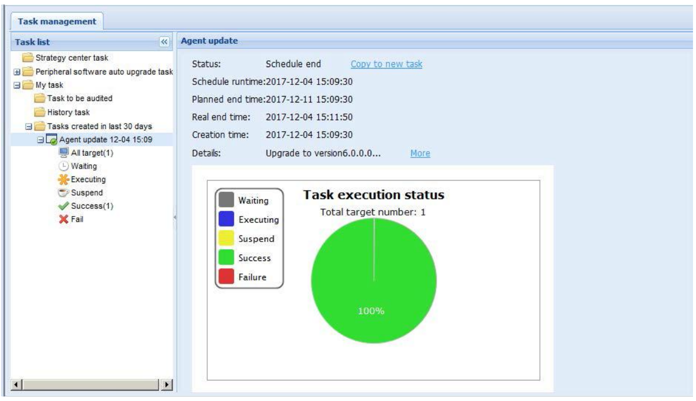
● Deploy immediately,Counting down 5 Minutes

○ Deploy after restart

If clients still power on 5:00 ~5:15 with deployment task not executed, the client will automatically count down to reboot.

4.7.4 View upgrade result

1. Enter 【task management】 module to view whether the client upgrade task is in “success” state.



Status: Schedule end

Schedule runtime:2017-12-04 15:09:30

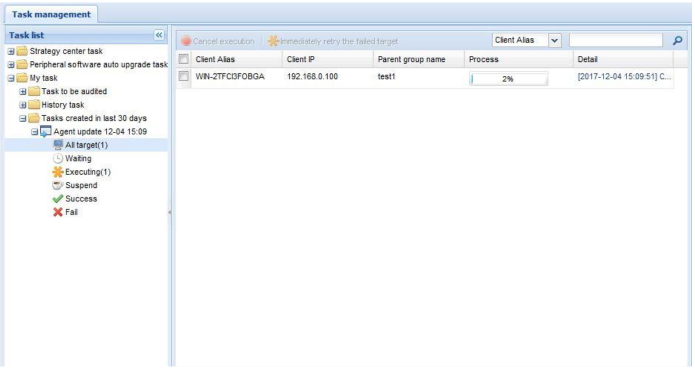
Planned end time:2017-12-11 15:09:30

Real end time: 2017-12-04 15:11:50

Creation time: 2017-12-04 15:09:30

Details: Upgrade to version6.0.0.0...

2. Unfold the task nodes and select all targets to view the upgrade situation of all clients.

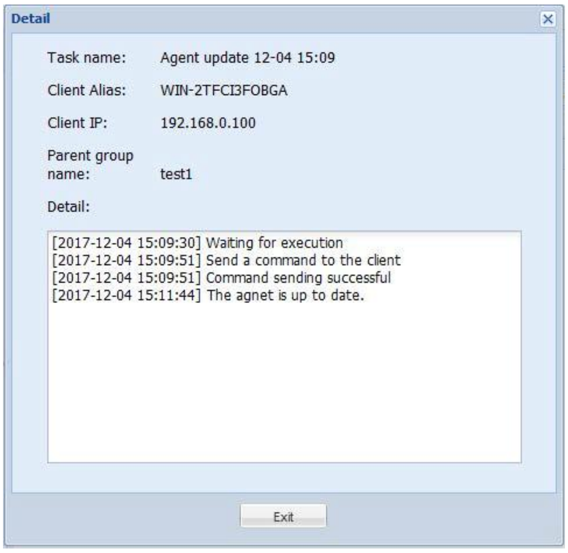


□	Client Alias	Client IP	Parent group name	Process	Detail
□	WIN-2TFCI3FOBGA	192.168.0.100	test1	2%	[2017-12-04 15:09:51] C...

3. Click the link shown in following figure for more details.

Notice:

- Allow change of higher client software version to lower version.
- If the upgrade is in failure, notify the technical support persons of prompt information about failure for help.



Task name: Agent update 12-04 15:09

Client Alias: WIN-2TFCI3FOBGA

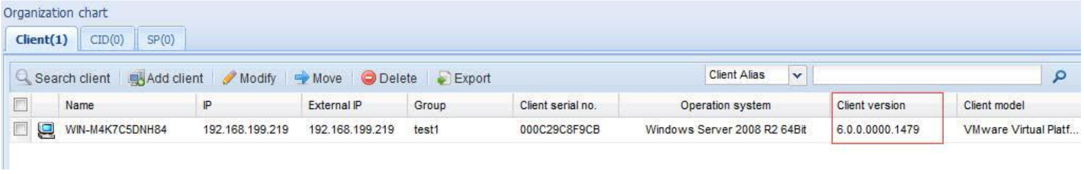
Client IP: 192.168.0.100

Parent group name: test1

Detail:

```
[2017-12-04 15:09:30] Waiting for execution
[2017-12-04 15:09:51] Send a command to the client
[2017-12-04 15:09:51] Command sending successful
[2017-12-04 15:11:44] The agnet is up to date.
```

4. After successfully displaying all upgrade records, the administrator can switch to the device management page. Select the client unit and view whether the client version information is consistent with the upgrade information on the right “client information” panel. Confirm whether the upgrade is successful.



□		Name	IP	External IP	Group	Client serial no.	Operation system	Client version	Client model
□		WIN-M4K7C5DNH84	192.168.199.219	192.168.199.219	test1	000C29C8F9CB	Windows Server 2008 R2 64Bit	6.0.0.0000.1479	VMware Virtual Platf...

4.8 Outer operation registration

The outer operation registration is the registration and strategy configuration behavior of business persons when carrying mobile terminals outside for business. At present, the outer operation registration function is only valid for Centerm Mobile Terminal and is invalid for thin client and PC. The using mode is as follows:

1. Enter “client management—>outer operation management—>outer operation registration” module. Select the outer Mobile Terminal from the left client tree. The right list will show the registration information of this client.

2. Click “lend” to pop up information edit box. Fill in the lender and set the locking strategy after lending.

3. After lending the Mobile Terminal, the locking strategy can be changed. If the Mobile Terminal is returned, the terminal can be set as non-locking state.

4.9 3G account

When the business person uses the Mobile Terminal to work outside, the 3G wireless network card shall be inserted for connecting the network. Therefore, similar to the outer operation registration function, 3G account is only valid for Centerm Mobile Terminal and is invalid for thin client and PC. The using mode is as follows:

1. Enter “client management—>outer operation management—>3G account” module. Click “add 3G account” button in the right list.

2. In the popup dialog box, fill in the correct 3G card information and select whether to bind with the Mobile Terminal. If the 3G card is bound with the Mobile Terminal, the 3G card can only be used in the corresponding Mobile Terminal and the Mobile Terminal can only use the bound 3G card.

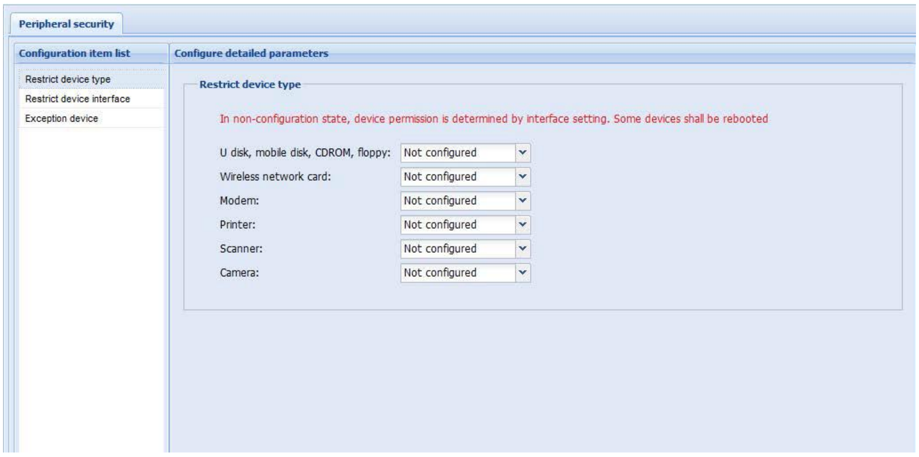
3. After adding the 3G account, the information or binding strategy can be changed.

4.10 Peripheral security

Peripherals on the client often generate unsafe factors, such as infecting virus, information leak and other risks in using USB, wireless network card, etc. Security management of peripherals enables the user to disable or enable any peripheral to reduce the risk caused by above unsafe factors.

4.10.1 Limit device type

The administrator can limit the using of client peripherals according to the device types. The system supports the peripherals in following figure.



In non-configuration state, device permission is determined by interface setting. Some devices shall be rebooted

U disk, mobile disk, CDROM, floppy: Not configured

Wireless network card: Not configured

Modem: Not configured

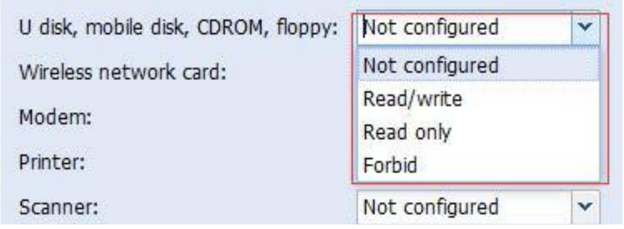
Printer: Not configured

Scanner: Not configured

Camera: Not configured

U disk, mobile hard disk, CD drive and floppy disk drive have four following states:

- Not configured: not limit the device;
- Read/write: normally read and write in the device;
- Read only: only read the data in the device rather than write;
- Forbid: prohibit any using operation of the device;



U disk, mobile disk, CDROM, floppy: Not configured

Wireless network card:

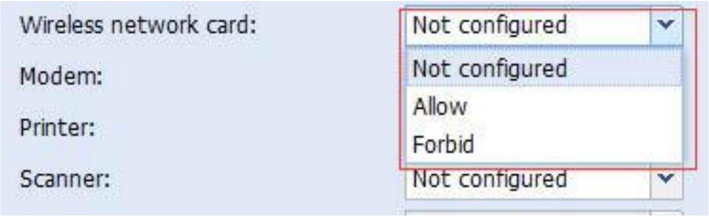
Modem:

Printer:

Scanner: Not configured

Other device has three following states:

- Not configure: not limit the device;
- Allow: allow all using operations of the device;
- Forbid: prohibit any using operation of the device;



Wireless network card: Not configured

Not configured

Allow

Forbid

Modem:

Printer:

Scanner: Not configured

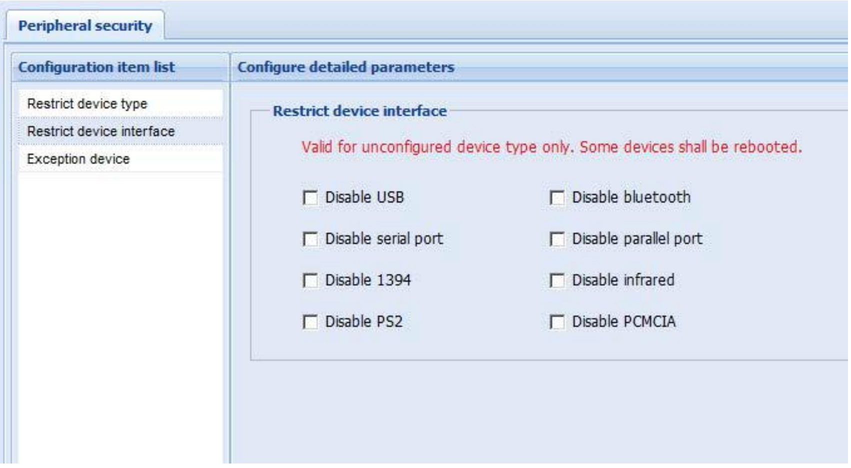
Notice:

- The device which is connected before applying the strategy will not be limited by the strategy. The device shall be plugged out and then connected again.
- Priority of device type is higher than the priority of device interface. If in setting of device interface, the USB interface is disabled, but in setting of device type, U disk and other storage device are allowed, the strategy will allow the using of U disk and other storage device, but prohibit other USB device.

4.10.2 Limit device interface

The administrator can limit the using of peripherals of client through the device interface. If the client device type to be limited isn't within the system configuration options, the limitation can be realized by limiting the device interface.

The types of interfaces which can be configured are shown as follows:



Peripheral security

Configuration item list

Restrict device type

Restrict device interface

Exception device

Configure detailed parameters

Restrict device interface

Valid for unconfigured device type only. Some devices shall be rebooted.

☐ Disable USB ☐ Disable bluetooth

☐ Disable serial port ☐ Disable parallel port

☐ Disable 1394 ☐ Disable infrared

☐ Disable PS2 ☐ Disable PCMCIA

Notice:

- The device which is connected before applying the strategy will not be limited by the strategy. The device shall be plugged out and then connected again.
- Priority of device type is higher than the priority of device interface. If in setting of device interface, the USB interface is disabled, but in setting of device type, U disk and other storage device are allowed, the strategy will allow the using of U disk and other storage device, but prohibit other USB device.

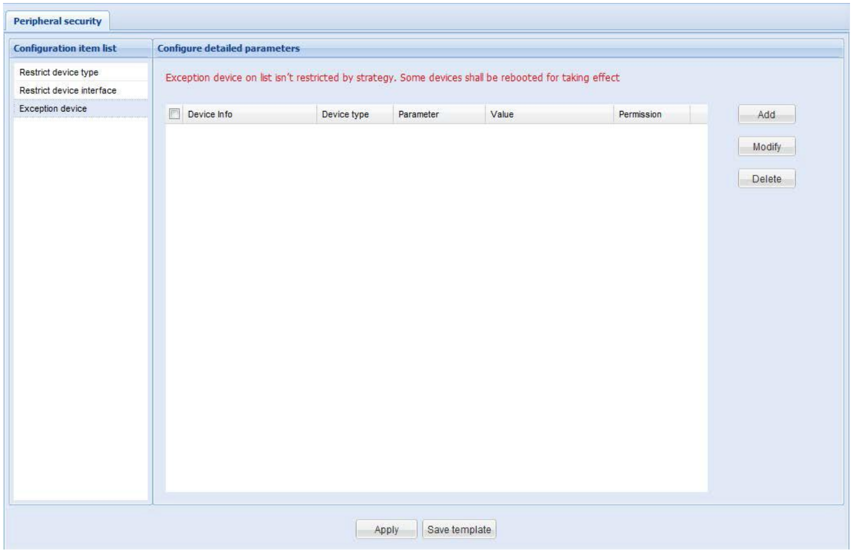
4.10.3 Exceptional device

4.10.3.1 Operation steps

The exceptional device refers to the special device which can be connected in the client, but isn't limited by the strategy. The method of adding the exceptional device is as follows:

1. Select the client to be set by user.

2. Click "add" button in "exceptional device" page.



Exception device on list isn't restricted by strategy. Some devices shall be rebooted for taking effect

3. Fill in the detailed information of exceptional device in the popup box, including following information:

- Device description: simple description of device. Any content can be filled in;
- Device type: storage type and non-storage type;
- Parameters: fill in any item of hardware ID, supplier ID, device ID and serial No. for storage device; fill in any item of hardware ID, supplier ID, device ID, type and service for non-storage device; refer to following two chapters for obtaining the parameters.
- Value: value of selected parameter;
- Authority: specify the using authority of device.

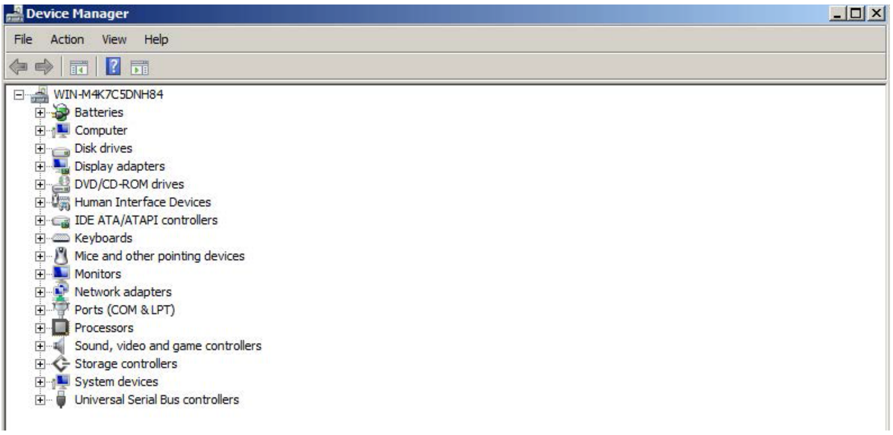
Notice:

The device which is connected before applying the strategy will not be limited by the strategy. The device shall be plugged out and then connected again.

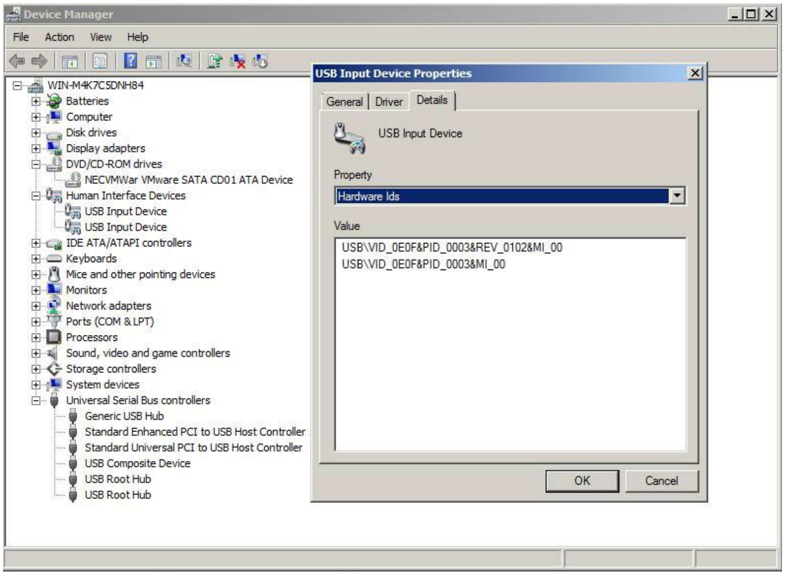
4.10.3.2 Directly view device parameters

1. View the hardware ID

Open the device manager



View the information of device to be set as exceptional device, such as USB input device



Property: Hardware Ids

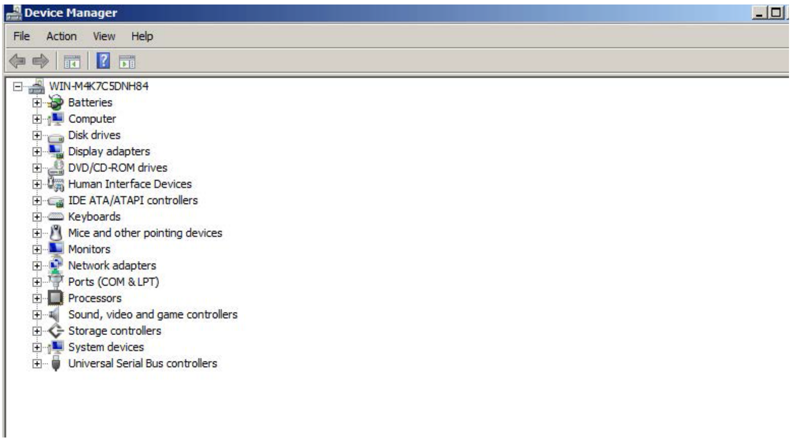
Value:

USB\VID_0E0F&PID_0003&REV_0102&MI_00
USB\VID_0E0F&PID_0003&MI_00

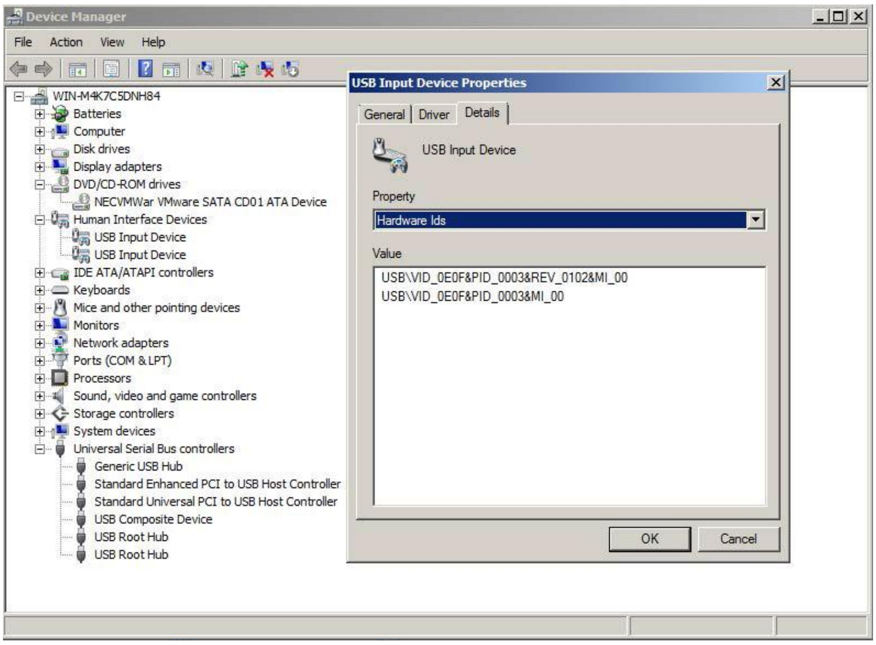
USB\VID_0627&PID_0001&REV_0000 in the figure is the hardware ID.

2. View the supplier ID

Open the device manager



View the information of device to be set as exceptional device, such as USB input device



Property: Hardware Ids

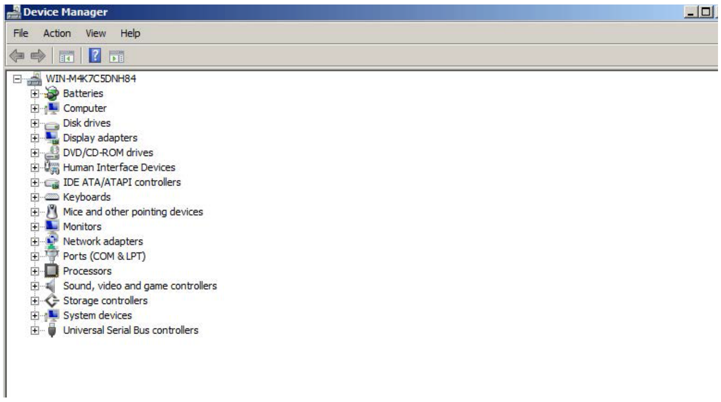
Value:

USB\VID_0E0F&PID_0003&REV_0102&MI_00
USB\VID_0E0F&PID_0003&MI_00

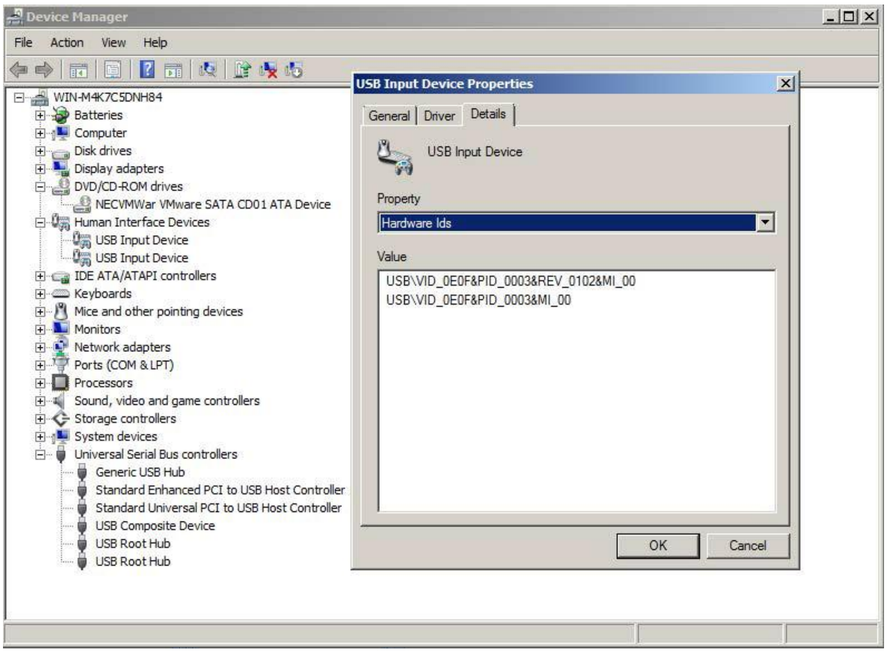
VID_0627 in the figure is the supplier ID.

3. View the device ID

Open the device manager



View the information of device to be set as exceptional device, such as USB input device



Property: Hardware Ids

Value:

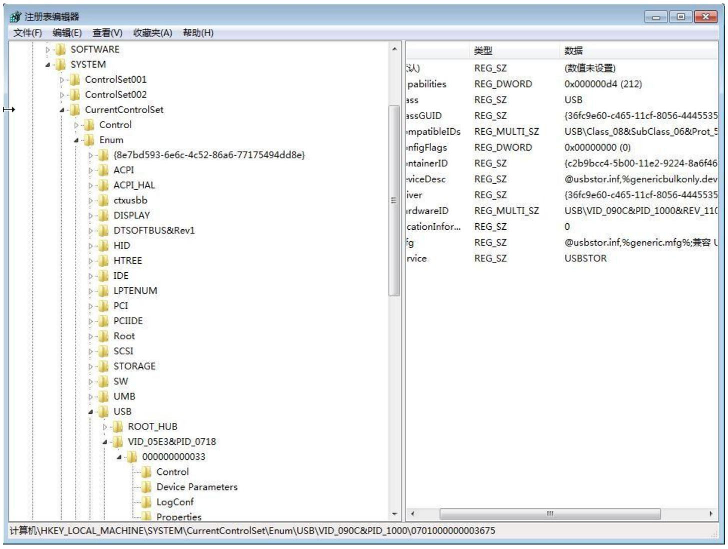
```
USB\VID_0E0F&PID_0003&REV_0102&MI_00
USB\VID_0E0F&PID_0003&MI_00
```

PID_0001 in the figure is the device ID.

4. View the serial No.

Open the registry and enter HKEY_LOCAL_MACHINE->SYSTEM->Enum

View the corresponding registry entry based on the device type, such as the serial No. of USB peripheral with supplier ID 05E3 and device ID 0718 is 000000000033.



	类型	数据
认)	REG_SZ	(数值未设置)
pabilities	REG_DWORD	0x000000d4 (212)
ass	REG_SZ	USB
assGUID	REG_SZ	{36fc9e60-c465-11cf-8056-4445535
mpatibleIDs	REG_MULTI_SZ	USB\Class_08&SubClass_06&Prot_5
nfigFlags	REG_DWORD	0x00000000 (0)
ntainerID	REG_SZ	{c2b9bcc4-5b00-11e2-9224-8a6f46
viceDesc	REG_SZ	@usbstor.inf,%genericbulkonly.dev
iver	REG_SZ	{36fc9e60-c465-11cf-8056-4445535
rdwareID	REG_MULTI_SZ	USB\VID_090C&PID_1000&REV_110
cationInfor...	REG_SZ	0
fg	REG_SZ	@usbstor.inf,%generic.mfg%;兼容 U
rvice	REG_SZ	USBSTOR

计算机\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB\VID_090C&PID_1000\0701000000003675

Notice: some composite device may have no serial No.

4.10.3.3 View device parameters by tools

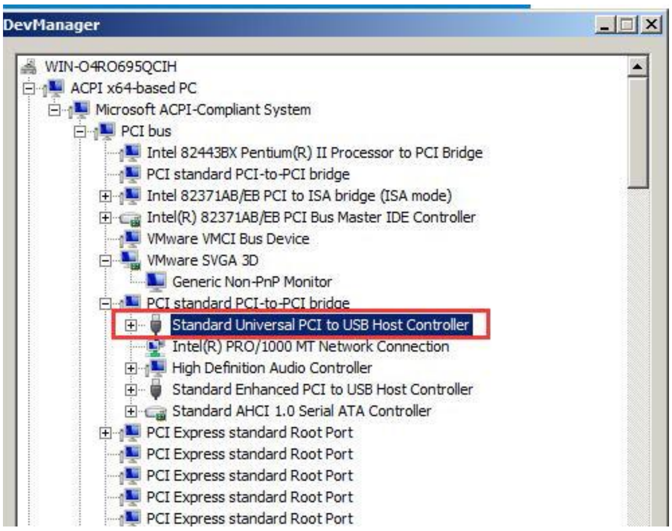
Double click on the application program. The device tree on the window arranges the device in accordance with connection mode and lists all devices including hidden device. The device is listed below the connected hardware.

1. Storage peripherals

Storage peripherals often refer to U disk, mobile hard disk and other devices for storing information. The storage peripheral can be set as exceptional device by any of following information:

- Hardware ID: uniquely identify one device. One device can have many hardware IDs.
- Supplier ID: PID, manufacturer No.
- Device ID: VID, product ID, PID+VID uniquely identify one device.
- Serial No.: uniquely identify one device.

The information of storage peripheral is generally connected with the USB bus controller of computer PCI bus, as shown in following figure.


DevManager
WIN-O4RO695QCIH
ACPI x64-based PC
Microsoft ACPI-Compliant System
PCI bus
Intel 82443BX Pentium(R) II Processor to PCI Bridge
PCI standard PCI-to-PCI bridge
Intel 82371AB/EB PCI to ISA bridge (ISA mode)
Intel(R) 82371AB/EB PCI Bus Master IDE Controller
VMware VMCI Bus Device
VMware SVGA 3D
Generic Non-PnP Monitor
PCI standard PCI-to-PCI bridge
Standard Universal PCI to USB Host Controller
Intel(R) PRO/1000 MT Network Connection
High Definition Audio Controller
Standard Enhanced PCI to USB Host Controller
Standard AHCI 1.0 Serial ATA Controller
PCI Express standard Root Port
PCI Express standard Root Port
PCI Express standard Root Port
PCI Express standard Root Port
PCI Express standard Root Port

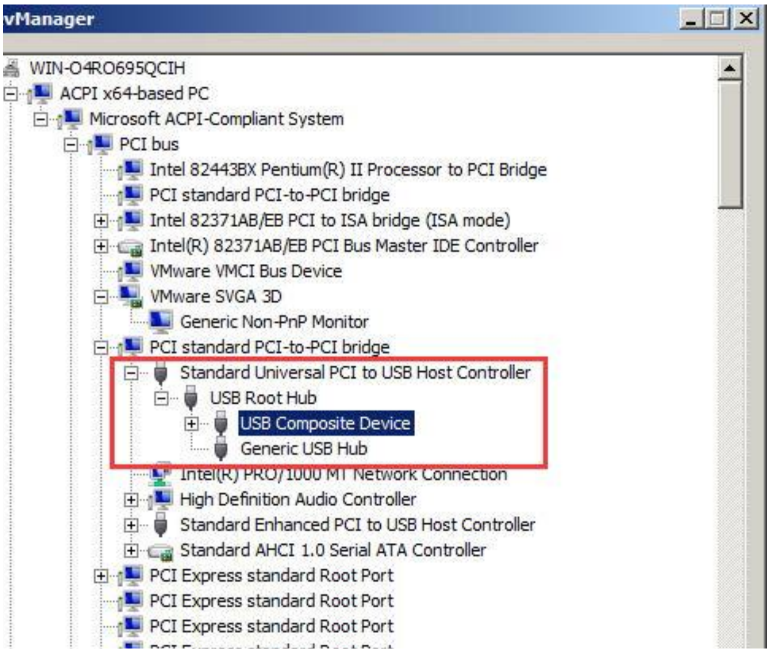
2. Non-storage peripherals

The non-storage peripherals generally refer to keyboard, mouse, wireless network card etc. The non-storage peripherals can be set as exceptional device by any of following information:

- Hardwire ID: uniquely identify one device. One device may have many hardware IDs. Some virtual devices have no ID.
- Supplier ID: VEN, manufacturer No.
- Device ID: DEV, product ID, DEV+VEN uniquely identify one device.
- Type: represent device type, not uniquely identify one device.
- Service: represent device service type, not uniquely identify one device.

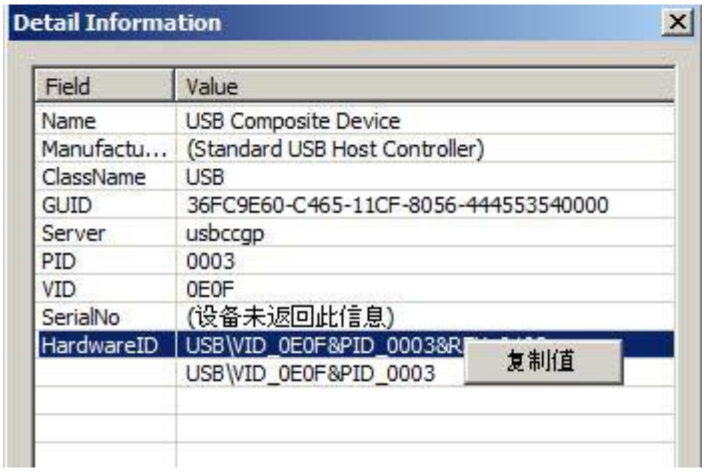
3. View and copy the device information

Click the left key to select the device and click “detailed information” button to pop up the corresponding window.



```
WIN-O4RO695QCIH
⊟ ACPI x64-based PC
  ⊟ Microsoft ACPI-Compliant System
    ⊟ PCI bus
        Intel 82443BX Pentium(R) II Processor to PCI Bridge
        PCI standard PCI-to-PCI bridge
      ⊞ Intel 82371AB/EB PCI to ISA bridge (ISA mode)
      ⊞ Intel(R) 82371AB/EB PCI Bus Master IDE Controller
        VMware VMCI Bus Device
      ⊟ VMware SVGA 3D
          Generic Non-PnP Monitor
      ⊟ PCI standard PCI-to-PCI bridge
        ⊟ Standard Universal PCI to USB Host Controller
          ⊟ USB Root Hub
            ⊞ USB Composite Device
              Generic USB Hub
          Intel(R) PRO/1000 MT Network Connection
        ⊞ High Definition Audio Controller
        ⊞ Standard Enhanced PCI to USB Host Controller
        ⊞ Standard AHCI 1.0 Serial ATA Controller
      ⊞ PCI Express standard Root Port
        PCI Express standard Root Port
        PCI Express standard Root Port
```

Click the left key to select one line in the list and then click the right key to select “copy value” in the popup menu to copy.



Field	Value
Name	USB Composite Device
Manufactu...	(Standard USB Host Controller)
ClassName	USB
GUID	36FC9E60-C465-11CF-8056-444553540000
Server	usbccgp
PID	0003
VID	0E0F
SerialNo	(设备未返回此信息)
HardwareID	USB\VID_0E0F&PID_0003&R
	USB\VID_0E0F&PID_0003

4.10.3.4 Other description

- If the device with many hardware IDs is set as the exceptional device. Any ID can uniquely identify the device.
- Some devices only have one sub-device, so the security strategy of exceptional of sub-device is applicable to parent device.
- As for composite device, the security strategy of exceptional of one sub-device isn’t applicable

to other sub-devices.

- Serial No., device ID and supplier ID of sub-device of composite device are same with that of parent device.

4.11 Vulnerability fixing

Attack on system vulnerabilities is a common method of virus attack. Therefore, vulnerability fixing in time is the effective means to prevent the client from virus attack. However, there are many difficulties and risks in fixing the client vulnerabilities by batch; besides, due to lack of statistics and maintenance, in later period, the vulnerabilities will be fixed repeatedly, which will spend a lot of time and need a lot of workload.

The vulnerability fixing module can solve above mentioned problem better and assist the IT administrator to fix vulnerabilities in any unified way. Besides, the automatic fixing function of client can be set and relevant fixing situation will be displayed.

4.11.1 Patch library management

The patch library includes information of all current patches for fixing the client vulnerabilities. The mentioned patches are **Microsoft patches** and **Centerm patches**. The Microsoft patches are directly provided by Microsoft and the Centerm patches are customized for Centerm XPE and WES7 clients.

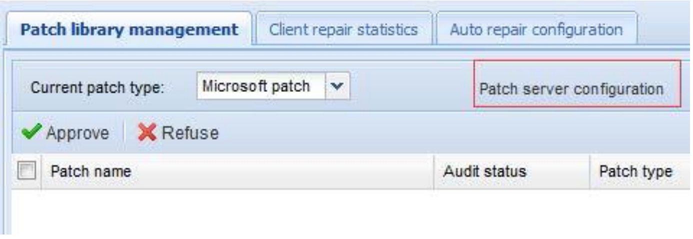
If the administrator needs to fix the vulnerabilities of XP and WIN7 clients, only the Microsoft patches are enough. If the administrator needs to fix the vulnerabilities of Centerm XPE and WES7 clients, we suggest using Centerm patch server to fix.

4.11.1.1 Patch server setting

1. Set up patch server

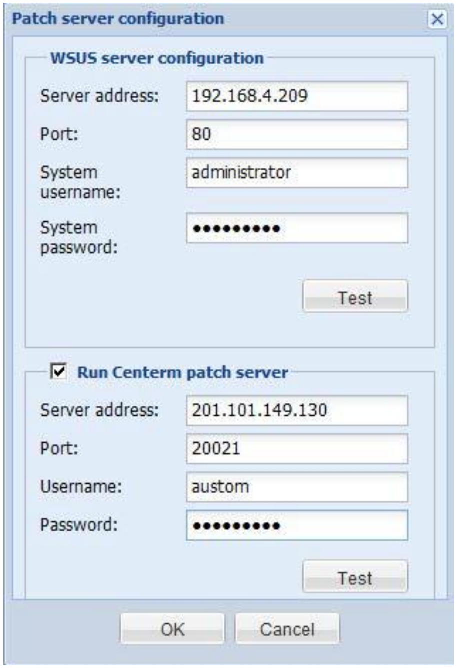
If Microsoft patches are used, only WSUS server shall be set up; if Centerm patches are used, both the WSUS server and Centerm patch server shall be set up. Refer to deployment file for setup method.

2. Click “patch server configuration” link



3. Fill in patch server information

If Microsoft patch server is used, only fill in the WSUS server; if Centerm patch server is used, fill in both the WSUS server and Centerm patch server, as shown in following figure:



Patch server configuration

WSUS server configuration

Server address: 192.168.4.209

Port: 80

System username: administrator

System password: •••••••••

☑ Run Centerm patch server

Server address: 201.101.149.130

Port: 20021

Username: austom

Password: •••••••••

After filling in, click “connect to test” button to test. Only if the filled patch server is available, the patch server information can be saved.

4. After setting the patch server, exit and refresh the patch list to view information of all patches.

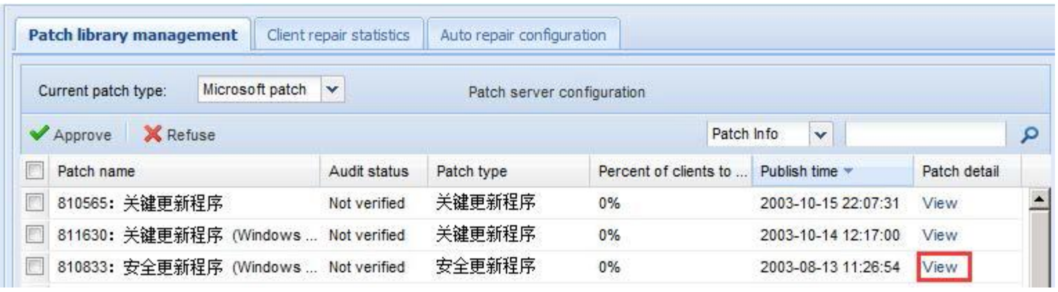
4.11.1.2 Patch review

The initial patches in the patch library cannot be directly downloaded by the client because some patches aren’t matched with the system or the patch isn’t necessary. Therefore, the administrator shall review the patch. Only the approved patch can be installed in the client.

Review the patch according to following steps:

1. Locate the patch to be reviewed

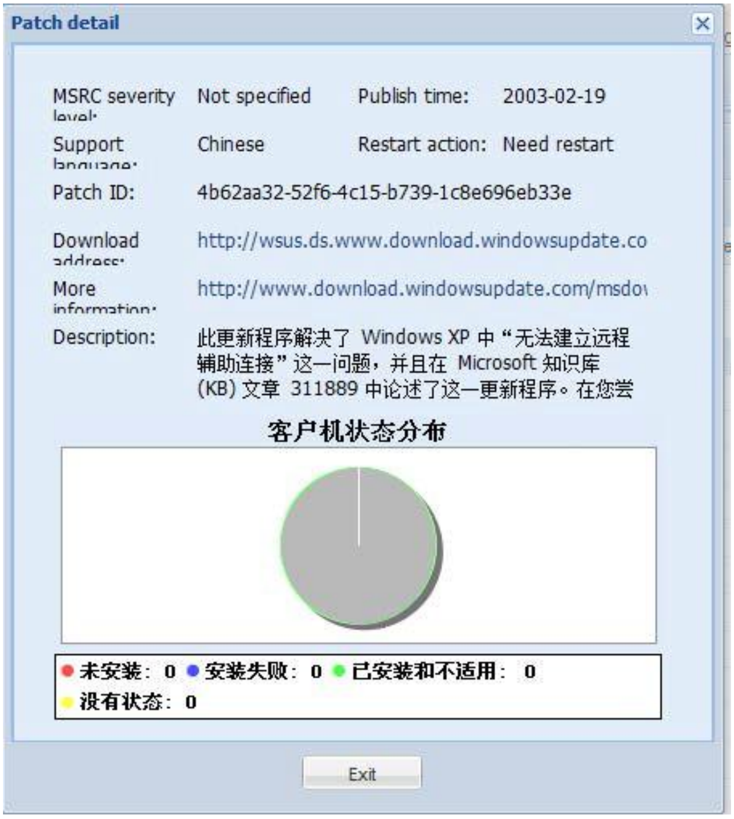
The list shows the name, review state and type of patch, proportion of clients to be updated. Click “view” link for more detailed information of patch.



Current patch type: Microsoft patch

□	Patch name	Audit status	Patch type	Percent of clients to ...	Publish time	Patch detail
□	810565：关键更新程序	Not verified	关键更新程序	0%	2003-10-15 22:07:31	View
□	811630：关键更新程序 (Windows ...	Not verified	关键更新程序	0%	2003-10-14 12:17:00	View
□	810833：安全更新程序 (Windows ...	Not verified	安全更新程序	0%	2003-08-13 11:26:54	View

The popup box shows the detailed information of patch and has the pie graph for statistics of installation situation of this patch in clients of WSUS server.



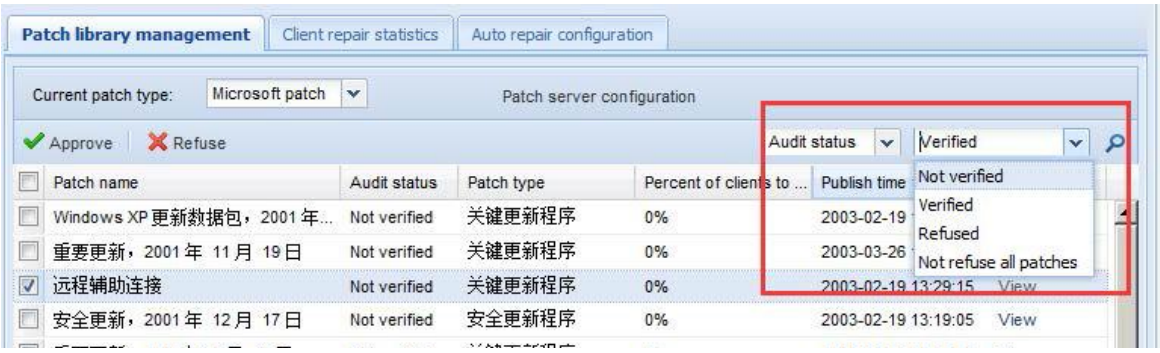
Patch detail

MSRC severity level:	Not specified	Publish time:	2003-02-19
Support language:	Chinese	Restart action:	Need restart
Patch ID:	4b62aa32-52f6-4c15-b739-1c8e696eb33e		
Download address:	http://wsus.ds.www.download.windowsupdate.co		
More information:	http://www.download.windowsupdate.com/msdo		
Description:	此更新程序解决了 Windows XP 中“无法建立远程辅助连接”这一问题，并且在 Microsoft 知识库 (KB) 文章 311889 中论述了这一更新程序。在您尝		

客户机状态分布

● 未安装：0 ● 安装失败：0 ● 已安装和不适用：0
● 没有状态：0

Screen and filter the patches by query function.



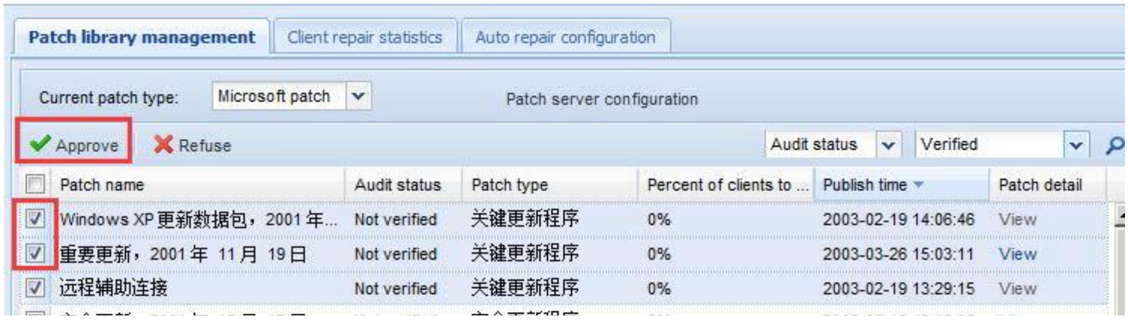
Current patch type: Microsoft patch

Audit status: Verified

Not verified
Verified
Refused
Not refuse all patches

☐	Patch name	Audit status	Patch type	Percent of clients to ...	Publish time
☐	Windows XP 更新数据包，2001 年...	Not verified	关键更新程序	0%	2003-02-19
☐	重要更新，2001 年 11 月 19 日	Not verified	关键更新程序	0%	2003-03-26
☑	远程辅助连接	Not verified	关键更新程序	0%	2003-02-19 13:29:15 View
☐	安全更新，2001 年 12 月 17 日	Not verified	安全更新程序	0%	2003-02-19 13:19:05 View

2. Select the patch and click “review” button



Current patch type: Microsoft patch

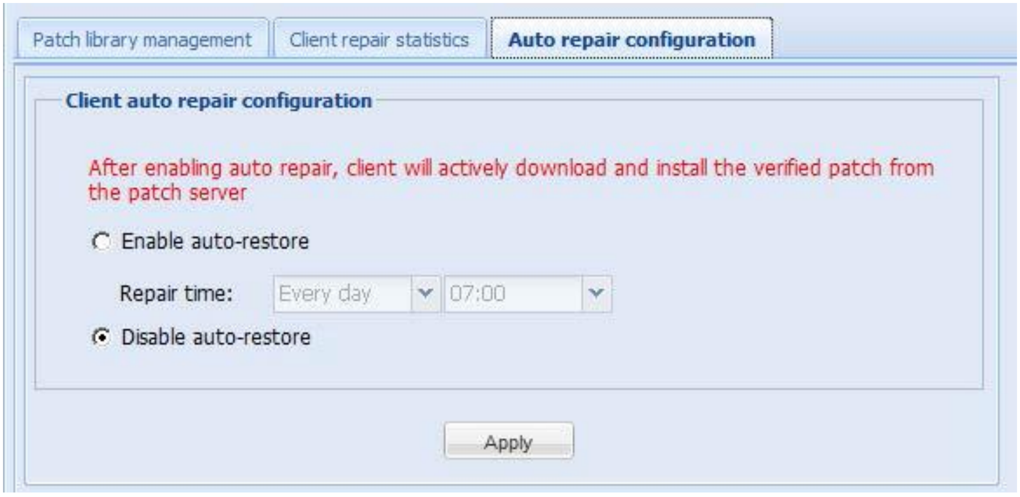
Audit status: Verified

☐	Patch name	Audit status	Patch type	Percent of clients to ...	Publish time	Patch detail
☑	Windows XP 更新数据包，2001 年...	Not verified	关键更新程序	0%	2003-02-19 14:06:46	View
☑	重要更新，2001 年 11 月 19 日	Not verified	关键更新程序	0%	2003-03-26 15:03:11	View
☑	远程辅助连接	Not verified	关键更新程序	0%	2003-02-19 13:29:15	View

4.11.2 Automatic fixing configuration

After reviewing the patch, the client can be set to automatically download and install the patch. The setting steps are:

Select one or more clients to be set from the client tree, enter “automatic fixing configuration” page, start the automatic fixing, set the fixing time and apply to the client.



Patch library management | Client repair statistics | **Auto repair configuration**

Client auto repair configuration

After enabling auto repair, client will actively download and install the verified patch from the patch server

○ Enable auto-restore

Repair time: Every day 07:00

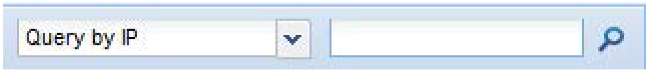
● Disable auto-restore

Apply

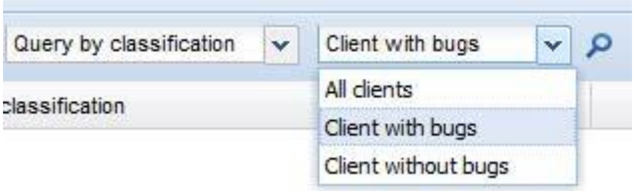
4.11.3 Client fixing statistics

The client repair statistics centrally shows the client fixing situation. The administrator can know the vulnerability fixing situation of current client from the statistics information.

The user can query according to IP or type:



Query by IP



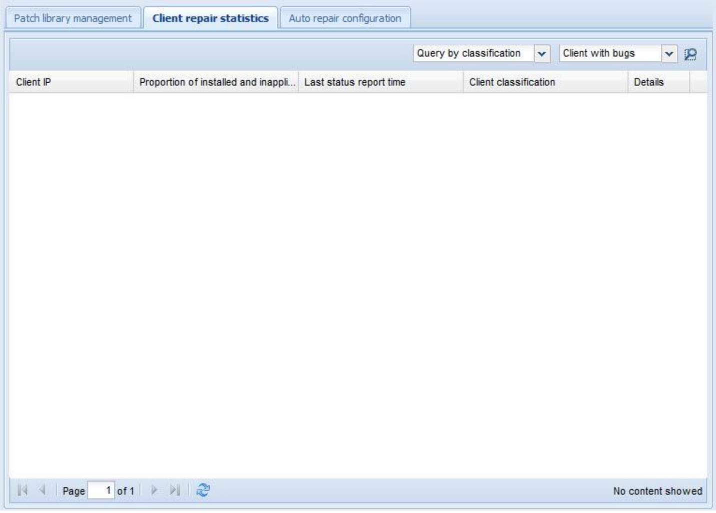
Query by classification | Client with bugs

All clients

Client with bugs

Client without bugs

Notice: only the client which enables the automatic fixing is included in the statistics list.



Patch library management | **Client repair statistics** | Auto repair configuration

Query by classification | Client with bugs

Client IP	Proportion of installed and inappli...	Last status report time	Client classification	Details

Page 1 of 1

No content showed

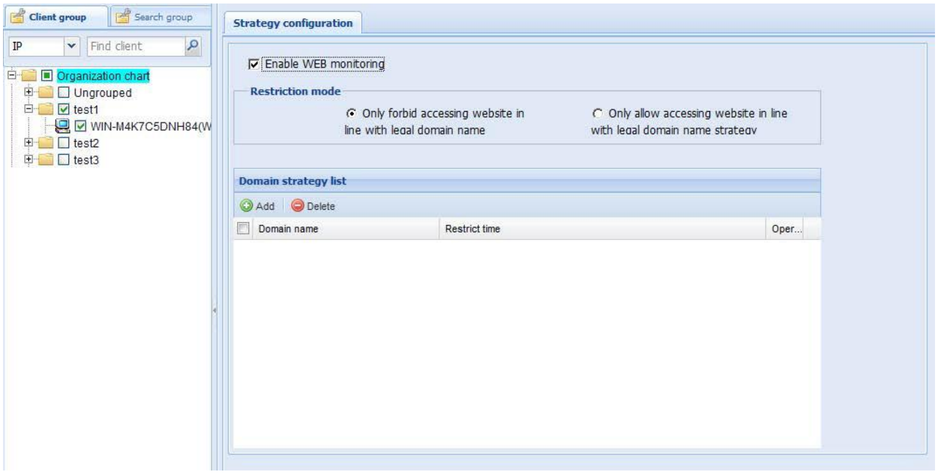
4.12 WEB security

WEB security management is used for monitoring WEB browsing behavior of client user and preventing the WEB behavior which isn’t in line with the browsing strategy.

4.12.1 Strategy configuration

In the strategy configuration, the user can enable and disable WEB monitoring function and set the domain name access strategy.

1. Select the client to be set with web monitoring, and select “enable WEB monitoring”.



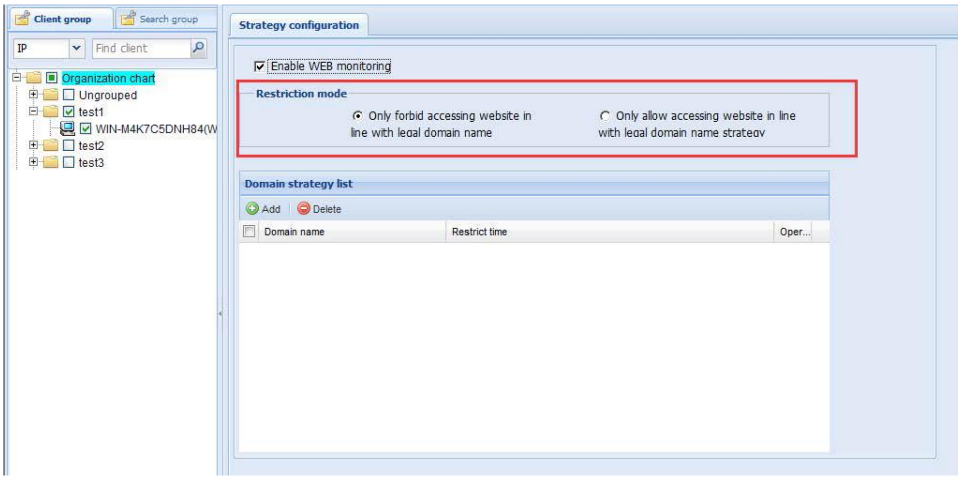
☑ Enable WEB monitoring

● Only forbid accessing website in line with legal domain name

○ Only allow accessing website in line with legal domain name strategy

2. Select the restriction mode.

- Only prohibit accessing website in line with domain name strategy: the strategy limits that the monitored client cannot access to the domain name in the list.
- Only allow to access website in line with domain name strategy: the strategy limits that the monitored client can only access to the domain name in the list.

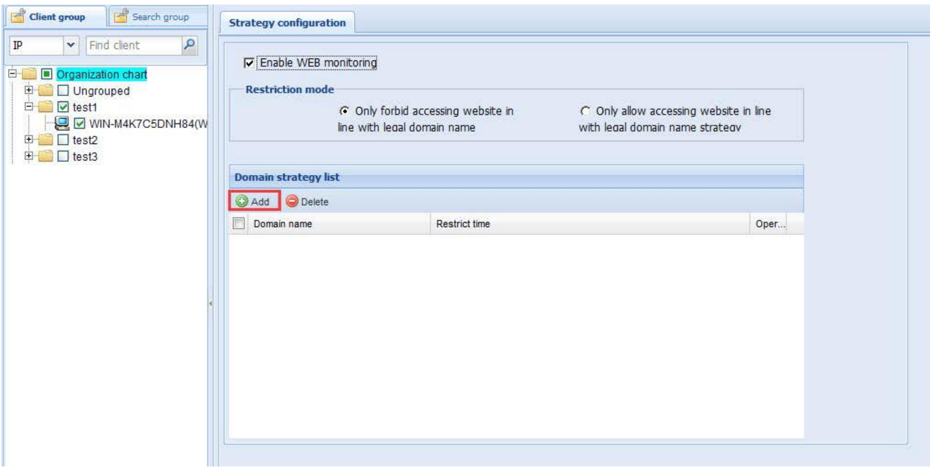


☑ Enable WEB monitoring

● Only forbid accessing website in line with legal domain name

○ Only allow accessing website in line with legal domain name strategy

3. After selecting the limitation mode, click “add” button to add in the list for domain names.



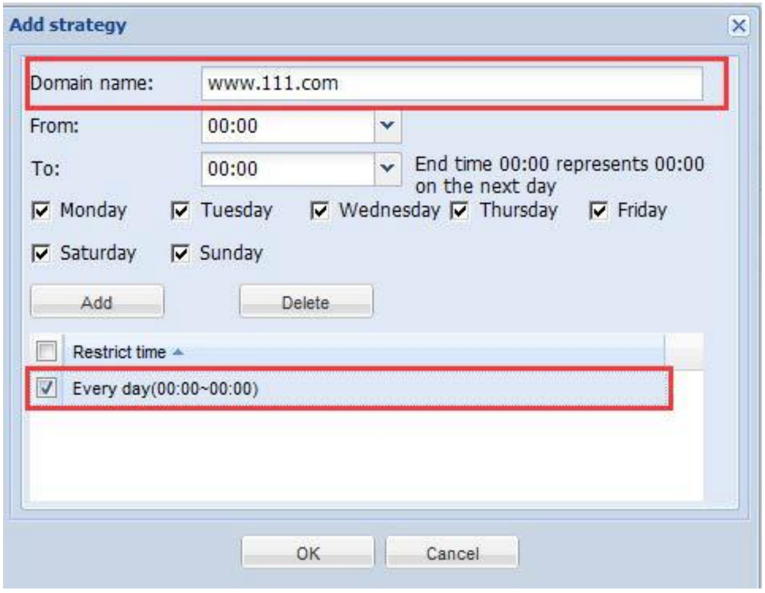
☑ Enable WEB monitoring

● Only forbid accessing website in line with legal domain name

○ Only allow accessing website in line with legal domain name strategy

4. In the popup dialog box, fill in the process name and limit time.

Notice: after selecting the time and date, click “add” button to add the time in the list for “Restrict time”, as shown in following figure:



Add strategy

Domain name: www.111.com

From: 00:00

To: 00:00

End time 00:00 represents 00:00 on the next day

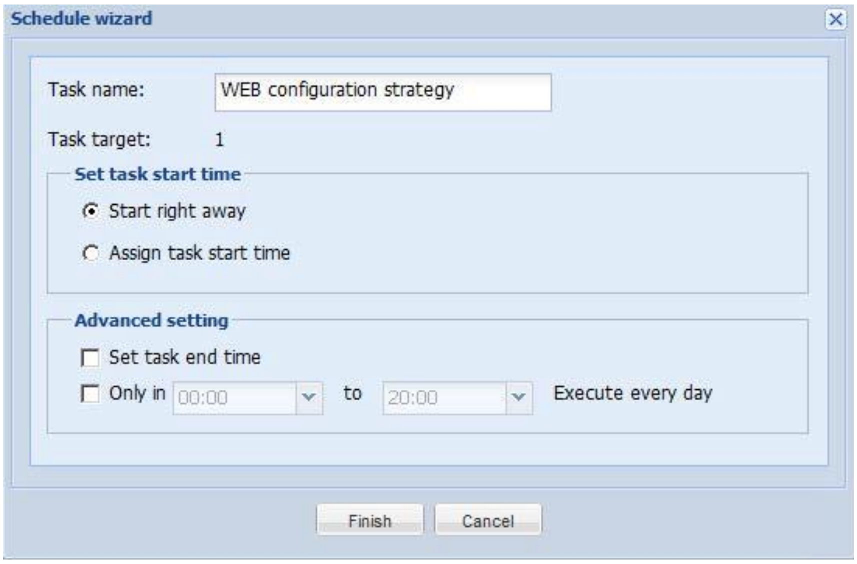
☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday

☑ Saturday ☑ Sunday

□	Restrict time
☑	Every day(00:00~00:00)

5. After adding in the list for domain names, click “apply” button to make the configuration valid. In working day, the client is limited to access www.126.com.

6. Configure “plan wizard” and execute operation.



Schedule wizard

Task name: WEB configuration strategy

Task target: 1

Set task start time

● Start right away

○ Assign task start time

Advanced setting

□ Set task end time

□ Only in 00:00 to 20:00 Execute every day

4.13 Software blacklist and whitelist

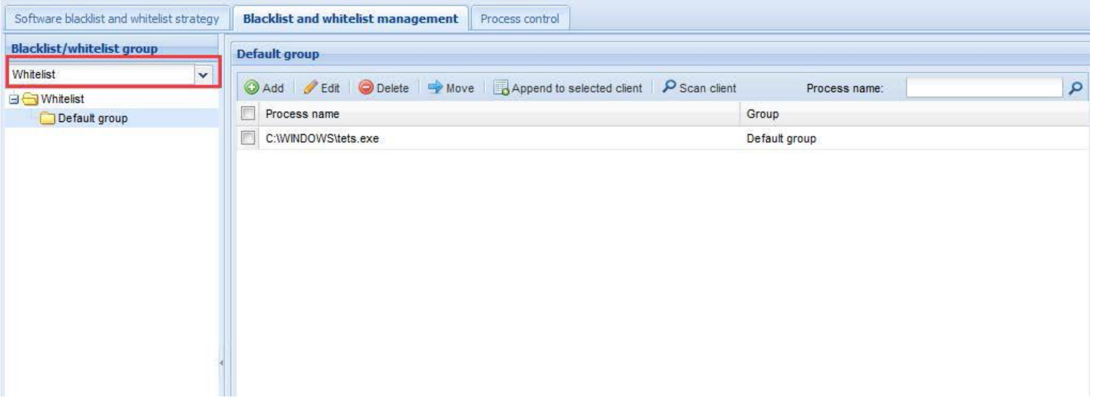
Software blacklist and whitelist control and limit the software progress on the client so as to standardize software application of local running of client and to ensure the safety of program running of client.

- The whitelist function only allows processes in the whitelist and basic system processes of client to run and prohibits other processes.
- The blacklist function only prohibits processes in the blacklist and allows other processes to run.

4.13.1 Blacklist and whitelist management

This module is used for maintaining the common processes in blacklist and whitelist in the system and facilitating the addition and change of processes in blacklist and whitelist by the administrator. In setting the process strategy, the administrator can directly select the needed process, which simplifies the input of user. Therefore, blacklist and whitelist library is only a process library in server and has no necessary connection with the client.

In the dropdown box of following figure, switch the page of blacklist and whitelist.


Software blacklist and whitelist strategy
Blacklist and whitelist management
Process control
Blacklist/whitelist group
Whitelist
Whitelist
Default group
Default group
Add
Edit
Delete
Move
Append to selected client
Scan client
Process name:

Process name	Group
C:\WINDOWS\tets.exe	Default group

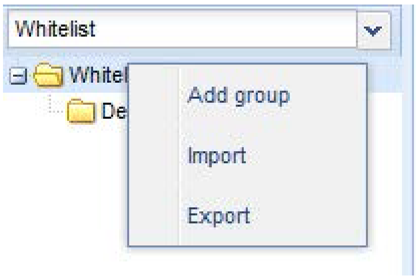
Because the addition method of whitelist is same with that of blacklist, the whitelist is taken as an example to introduce.

4.13.1.1 Add process group

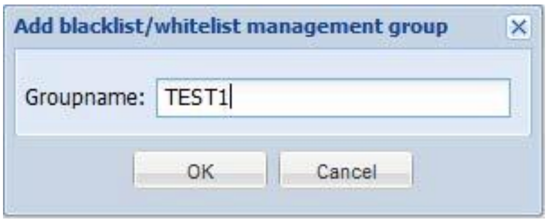
The group is used for classifying and distinguishing processes. We suggest the administrator to make the group based on software.

Both whitelist and blacklist only support the one layer group. The root groups have "default group" respectively which shall not be renamed or deleted. Adding method of group is as follows:

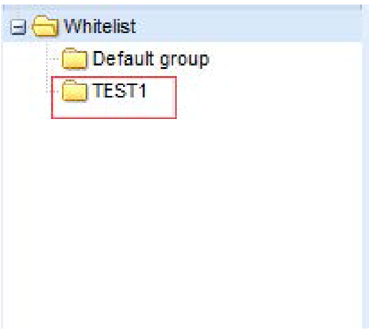
1. Right click on the whitelist node and select the "add group".



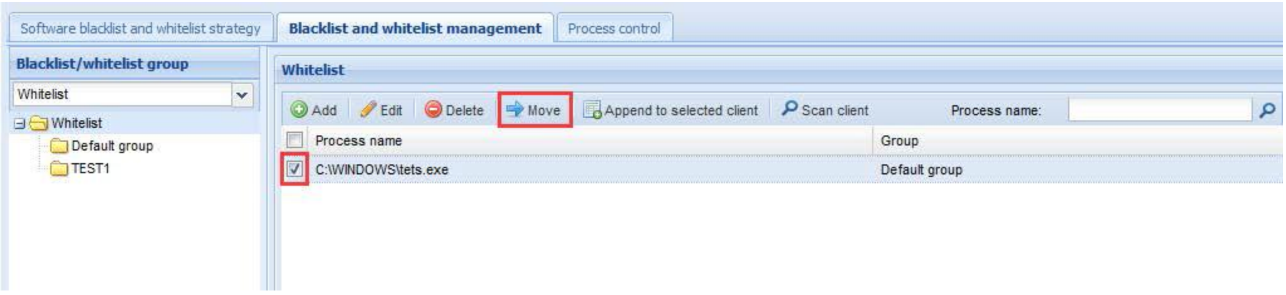
2. Fill in the group name and finish adding.



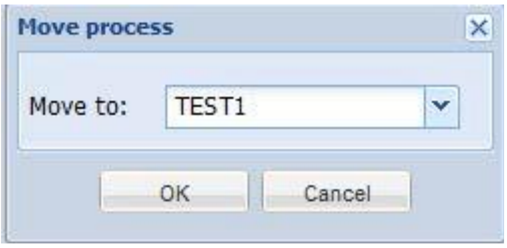
Groupname: TEST1



3. The grouped process can be transferred to other groups by "move" function.


Software blacklist and whitelist strategy
Blacklist and whitelist management
Process control
Blacklist/whitelist group
Whitelist
Whitelist
Default group
TEST1
Whitelist
Add
Edit
Delete
Move
Append to selected client
Scan client
Process name:

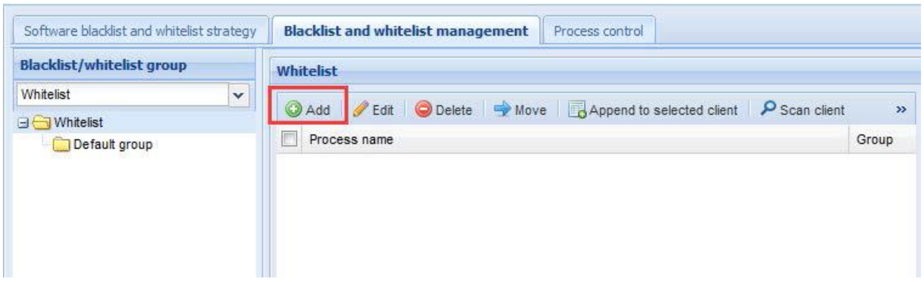
	Process name	Group
☑	C:\WINDOWS\tets.exe	Default group



Move to: TEST1

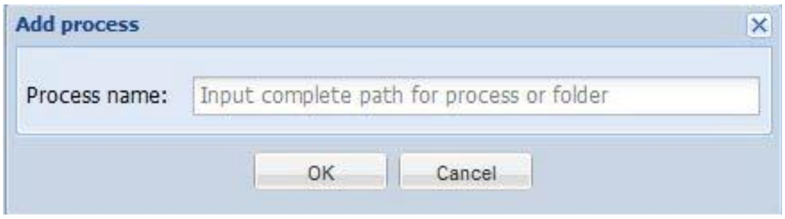
4.13.1.2 Manually adding

1. Click “add” button.


Software blacklist and whitelist strategy
Blacklist and whitelist management
Process control
Blacklist/whitelist group
Whitelist
Whitelist
Default group
Whitelist
Add
Edit
Delete
Move
Append to selected client
Scan client
»
Process name
Group

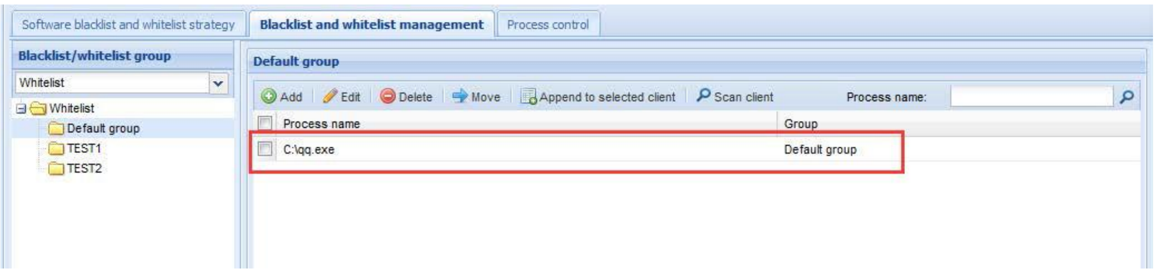
2. In the popup dialog box, fill in the process name. If only one process is added, fill in the complete path of the process, such as “C:\Windows\system32\notepad.exe”; if a directory is added, fill in the complete path of the directory, such as D:\ProgramFiles\NewCommi.

If the process in blacklist is added, as for single process, only fill in the process name, such as “notepad.exe”; as for directory, fill in the complete path.



Process name: Input complete path for process or folder

3. Click “OK”. The list will show the added process. Processes added in the root group will be automatically included in the default group.

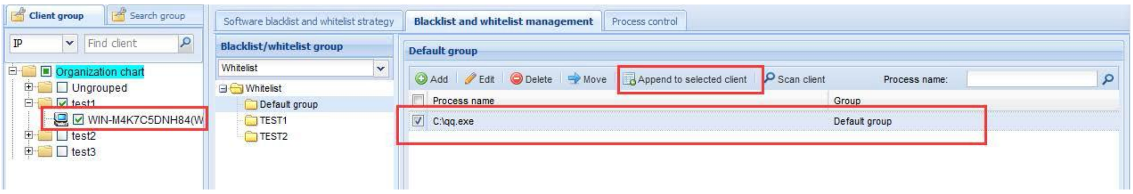

Software blacklist and whitelist strategy
Blacklist and whitelist management
Process control
Blacklist/whitelist group
Whitelist
Whitelist
Default group
TEST1
TEST2
Default group
Add
Edit
Delete
Move
Append to selected client
Scan client
Process name:

	Process name	Group
□	C:\qq.exe	Default group

4.13.1.3 Add to selected client

Adding to selected client refers to add the selected whitelist strategy to the specified strategy list in the client without covering original record, including following two situations:

- If the client enables the whitelist strategy, the added whitelist will take effect immediately;
- If the client disables the whitelist strategy, the added whitelist can only be added in the list and cannot take effect.



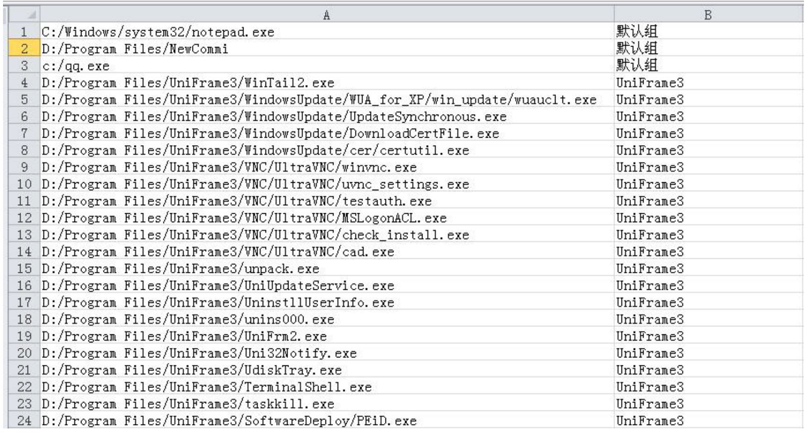
☐ Process name	Group
☑ C:\qq.exe	Default group

4.13.1.4 Import list

When the administrator needs to add more processes or directories or transfer the process list, the administrator can use the import function of process list.

1. Description of importing files

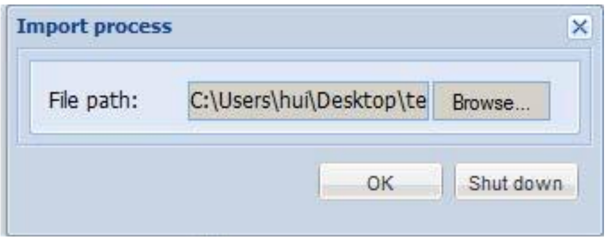
The imported file shall be CSV file. Firstly, create a new file in excel. Fill in the process name in the first column and the process group in the second column, as follows. After editing, save the file as csv format.



	A	B
1	C:/Windows/system32/notepad.exe	默认组
2	D:/Program Files/NewCommi	默认组
3	c:/qq.exe	默认组
4	D:/Program Files/UniFrame3/WinTail2.exe	UniFrame3
5	D:/Program Files/UniFrame3/WindowsUpdate/WUA_for_XP/win_update/wuauclt.exe	UniFrame3
6	D:/Program Files/UniFrame3/WindowsUpdate/UpdateSynchronous.exe	UniFrame3
7	D:/Program Files/UniFrame3/WindowsUpdate/DownloadCertFile.exe	UniFrame3
8	D:/Program Files/UniFrame3/WindowsUpdate/cer/certutil.exe	UniFrame3
9	D:/Program Files/UniFrame3/VNC/UltraVNC/winvnc.exe	UniFrame3
10	D:/Program Files/UniFrame3/VNC/UltraVNC/uvnc_settings.exe	UniFrame3
11	D:/Program Files/UniFrame3/VNC/UltraVNC/testauth.exe	UniFrame3
12	D:/Program Files/UniFrame3/VNC/UltraVNC/MSLogonACL.exe	UniFrame3
13	D:/Program Files/UniFrame3/VNC/UltraVNC/check_install.exe	UniFrame3
14	D:/Program Files/UniFrame3/VNC/UltraVNC/cad.exe	UniFrame3
15	D:/Program Files/UniFrame3/unpack.exe	UniFrame3
16	D:/Program Files/UniFrame3/UniUpdateService.exe	UniFrame3
17	D:/Program Files/UniFrame3/UninstllUserInfo.exe	UniFrame3
18	D:/Program Files/UniFrame3/unins000.exe	UniFrame3
19	D:/Program Files/UniFrame3/UniFrm2.exe	UniFrame3
20	D:/Program Files/UniFrame3/Uni32Notify.exe	UniFrame3
21	D:/Program Files/UniFrame3/UdiskTray.exe	UniFrame3
22	D:/Program Files/UniFrame3/TerminalShell.exe	UniFrame3
23	D:/Program Files/UniFrame3/taskkill.exe	UniFrame3
24	D:/Program Files/UniFrame3/SoftwareDeploy/PEiD.exe	UniFrame3

2. Import steps

In the right click menu of whitelist node, select “import” to import the process in the system.

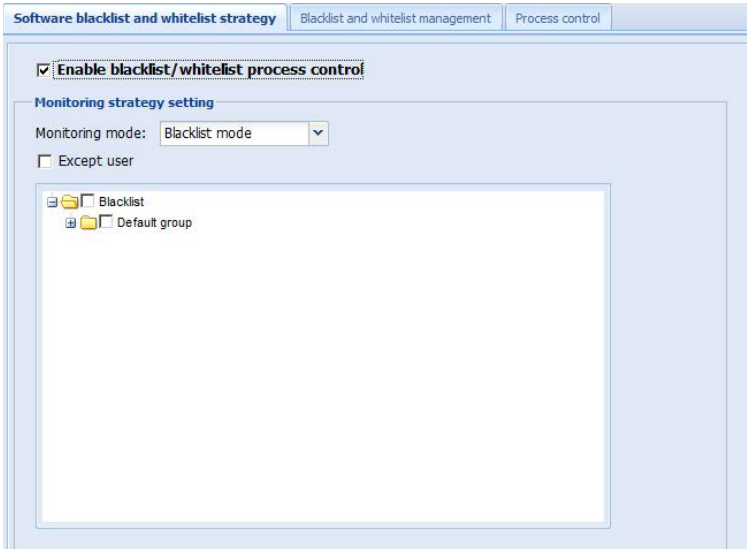


File path: C:\Users\hui\Desktop\te

4.13.2 Blacklist and whitelist strategy

In the blacklist and whitelist strategy, the administrator can set relevant strategy of monitoring processes of the client. The steps are as follows.

1. Select one or more clients to be configured with strategy. Select “enable blacklist/whitelist control function” on the right panel, as follows.


Software blacklist and whitelist strategy
Blacklist and whitelist management
Process control
Monitoring strategy setting
Blacklist
Default group

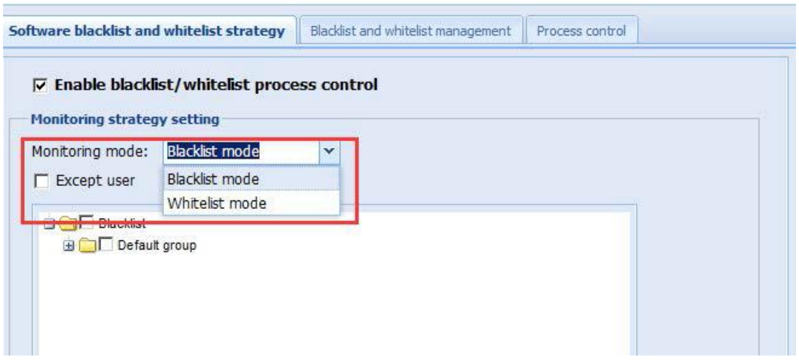
☑ Enable blacklist/whitelist process control

Monitoring mode: Blacklist mode

□ Except user

2. Select the monitoring mode

At a moment, the client only can use one mode and cannot use the blacklist and whitelist mode simultaneously.


Software blacklist and whitelist strategy
Blacklist and whitelist management
Process control
Monitoring strategy setting
Blacklist mode
Whitelist mode
Blacklist
Default group

☑ Enable blacklist/whitelist process control

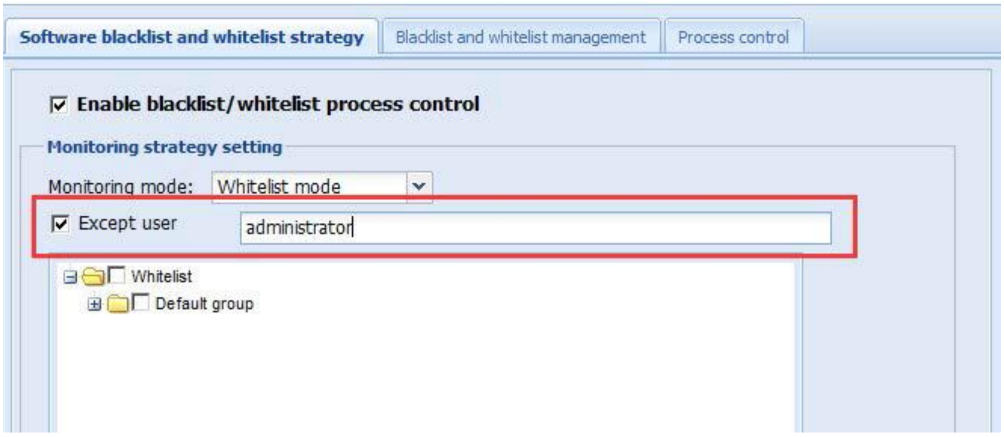
Monitoring mode: Blacklist mode

□ Except user

3. Fill in the exceptional user

The exceptional user function realizes that the user in exceptional user list isn’t controlled by the process strategy. For example, if the administrator is filled in the list as the exceptional user, all users except for the administrator in the whitelist will take effect.

In order to use this function, select the option in red frame in following figure, fill in corresponding username and use English “,” to separate.


Software blacklist and whitelist strategy
Blacklist and whitelist management
Process control
Monitoring strategy setting
Whitelist
Default group

☑ Enable blacklist/whitelist process control

Monitoring mode: Whitelist mode

☑ Except user administrator

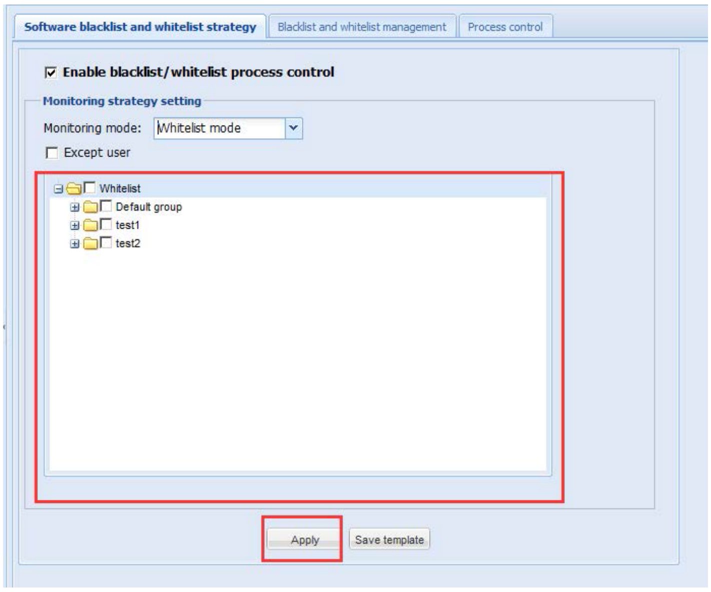
4. Select process

When the administrator selects the monitoring mode, the list will automatically load the corresponding blacklist and whitelist library. Select the process to be valid in the client and then apply to client.

Description of unknown group:

When a process in the client doesn’t belong to blacklist or whitelist library, the process will be automatically included in the unknown group. Once the monitoring is cancelled, the process will not be acquired. The unknown process may occur in following three situations.

- The client applies the blacklist and whitelist strategy with too early version;
- The client runs other software during installation of client which adds these software processes in blacklist and whitelist by default;
- The administrator deletes or edits some processes in blacklist and whitelist library, but the client has configured with these processes.


Software blacklist and whitelist strategy
Blacklist and whitelist management
Process control
Apply
Save template

☑ Enable blacklist/whitelist process control

Monitoring strategy setting

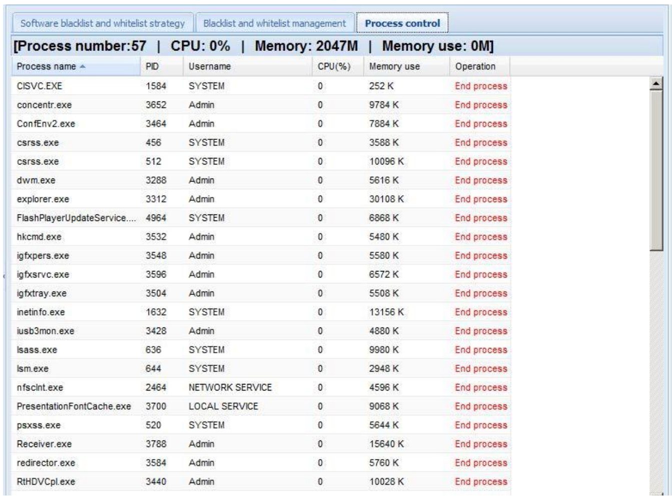
Monitoring mode: Whitelist mode

☐ Except user

- ☐ Whitelist
  - ☐ Default group
  - ☐ test1
  - ☐ test2

4.13.3 Process control

The process control function is similar to the task manager of windows OS; after selecting one client, the administrator can view current processes run in the client and can click “end the process” to end the process in the client.


Software blacklist and whitelist strategy
Blacklist and whitelist management
Process control

[Process number:57 | CPU: 0% | Memory: 2047M | Memory use: 0M]

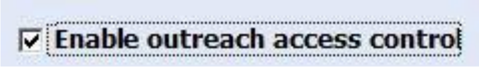
Process name	PID	Username	CPU(%)	Memory use	Operation
CISVC.EXE	1584	SYSTEM	0	252 K	End process
concentr.exe	3652	Admin	0	9784 K	End process
ConfEnv2.exe	3464	Admin	0	7884 K	End process
csrss.exe	456	SYSTEM	0	3588 K	End process
csrss.exe	512	SYSTEM	0	10096 K	End process
dwm.exe	3288	Admin	0	5616 K	End process
explorer.exe	3312	Admin	0	30108 K	End process
FlashPlayerUpdateService....	4964	SYSTEM	0	6868 K	End process
hkcmd.exe	3532	Admin	0	5480 K	End process
igfxpers.exe	3548	Admin	0	5580 K	End process
igfxsrvc.exe	3596	Admin	0	6572 K	End process
igfxtray.exe	3504	Admin	0	5508 K	End process
inetinfo.exe	1632	SYSTEM	0	13156 K	End process
iusb3mon.exe	3428	Admin	0	4880 K	End process
lsass.exe	636	SYSTEM	0	9980 K	End process
lsm.exe	644	SYSTEM	0	2948 K	End process
nfsclnt.exe	2464	NETWORK SERVICE	0	4596 K	End process
PresentationFontCache.exe	3700	LOCAL SERVICE	0	9068 K	End process
psxss.exe	520	SYSTEM	0	5644 K	End process
Receiver.exe	3788	Admin	0	15640 K	End process
redirector.exe	3584	Admin	0	5760 K	End process
RtHDVCpl.exe	3440	Admin	0	10028 K	End process

4.14 Illegal outreach management

The outreach control is limitation to outreach state of client. When the client will be disconnected with the management of internal network and connected with external network to access by other methods, detect the specified URL address in specified time to obtain the outreach state of client; if any illegal behavior is found, take corresponding isolation or screen locking operation.

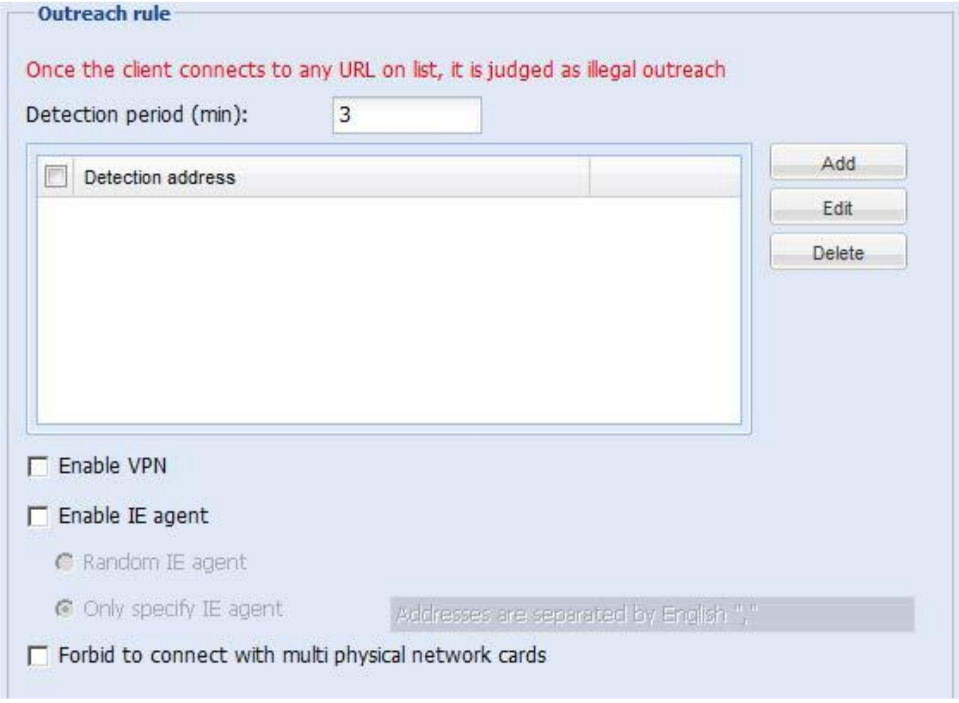
4.14.1 Illegal outreach access control

1. Select the client to be configured from client tree in the left and select “start the outreach access control” on the right panel;



☑ Enable outreach access control

2. Set the outreach rule



Outreach rule

Once the client connects to any URL on list, it is judged as illegal outreach

Detection period (min): 3

□ Detection address

□ Enable VPN

□ Enable IE agent

○ Random IE agent

● Only specify IE agent Addresses are separated by English “,”

□ Forbid to connect with multi physical network cards

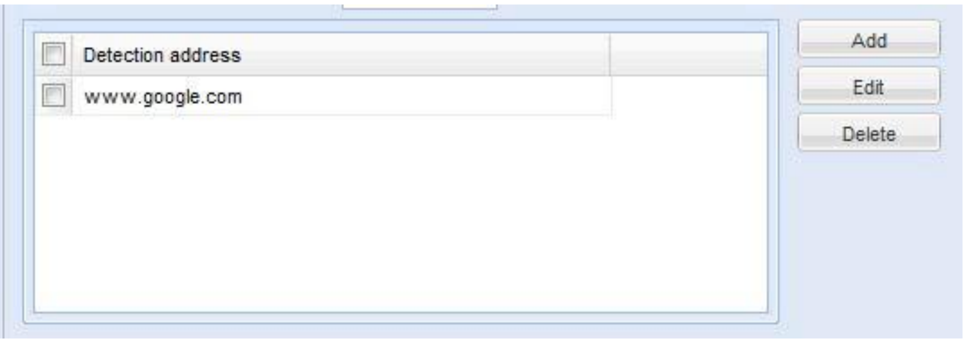
- Detection cycle

At the interval of one cycle, the client will detect whether the local client connects with address in the list.

Detection period (min): 3

- Detect the address list

The address list is the key reference to judge whether the client is outreached. Once the client can connect with any URL in the list, it is determined as illegal outreach.



□ Detection address
□ www.google.com

- Whether allow to use VPN

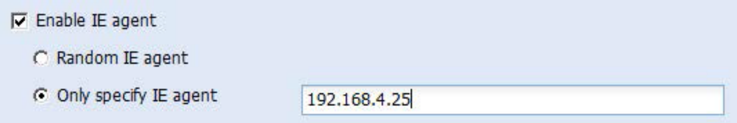
If this option is selected, it represents that the client is allowed to connect with external network by VPN mode. When the client is connected with detection address by VPN mode, the connection will also be reported as the illegal outreach;

□ Enable VPN

- Whether allow to use IE agent

If this option is selected, it represents that the client is allowed to connect with external network by IE agent mode. When the client is connected with detection address by IE agent mode, the connection will also be reported as the illegal outreach;

The administrator can specify to allow all IE agents, or specify one agent or many agents.



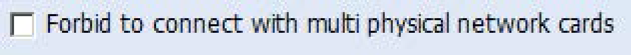
☑ Enable IE agent

○ Random IE agent

● Only specify IE agent 192.168.4.25

- Whether allow to connect many physical network cards at the same time

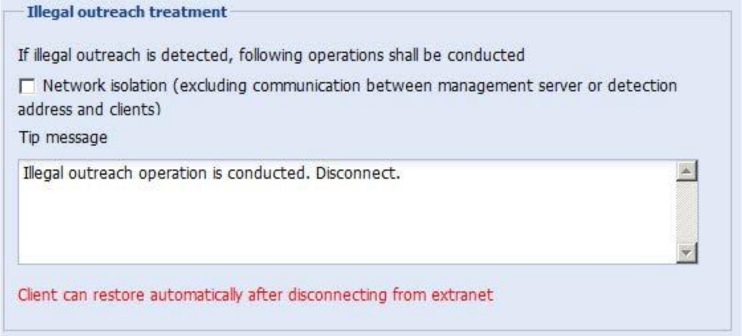
After selecting, the client is prohibited connecting with many physical network cards. The function is mainly used for limiting the client connecting with many LANs and is unrelated to the detection address.



□ Forbid to connect with multi physical network cards

3. Set the illegal outreach treatment

When the illegal outreach of client is found, the system will automatically prompt to the client. Besides, the administrator can select network isolation of client without influence of management of client by management server.



Illegal outreach treatment

If illegal outreach is detected, following operations shall be conducted

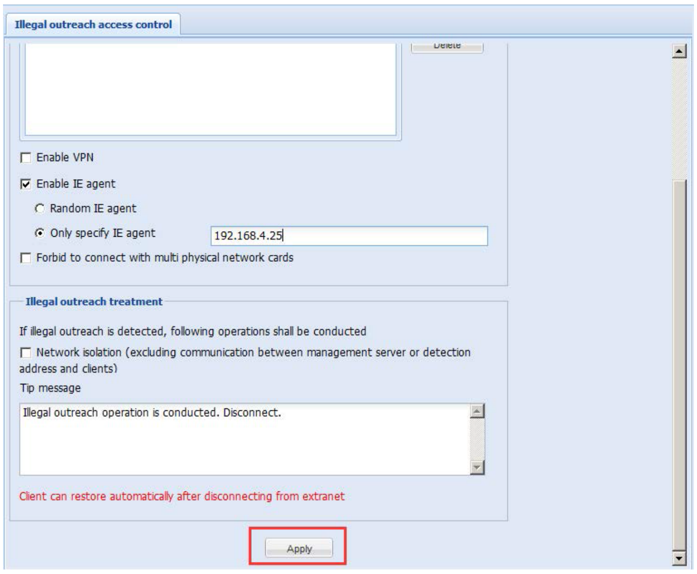
□ Network isolation (excluding communication between management server or detection address and clients)

Tip message

Illegal outreach operation is conducted. Disconnect.

Client can restore automatically after disconnecting from extranet

4. Click “apply” button to apply the strategy in the client.



□ Enable VPN

☑ Enable IE agent

○ Random IE agent

● Only specify IE agent 192.168.4.25

□ Forbid to connect with multi physical network cards

Illegal outreach treatment

If illegal outreach is detected, following operations shall be conducted

□ Network isolation (excluding communication between management server or detection address and clients)

Tip message

Illegal outreach operation is conducted. Disconnect.

Client can restore automatically after disconnecting from extranet

5. The outreach log generated in client can be viewed in audit management module.

4.15 Performance monitoring

The performance monitoring is the dynamic overview of client performance. All performances of the client are monitored to trace the running situation of client and to treat the emergency immediately. Besides, the user can comprehensively know the client performance based on analysis and statistics of statements.

4.15.1 Real-time performance

It is similar to “performance” option in Windows task manager to display the current system performance of the selected client, including six performances, i.e. process running state, CPU, memory, disk, network connection and network card.

1. Enter 【basic management—>client monitoring—>performance monitoring】 and switch to “real-time performance” tab page, as shown in following figure:

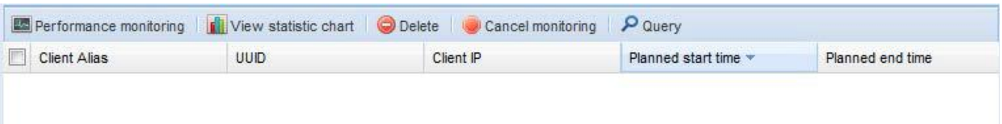
2. Among the real-time performances, user can view following information:

- Process running state: detailed information and occupied resource of running process of selected client;
- CPU, memory and disk: CPU, memory and disk using situation of selected client;
- Network connection: all listening ports of network connection of selected client;
- Network card: network card using situation of selected client;

4.15.2 Performance statistics

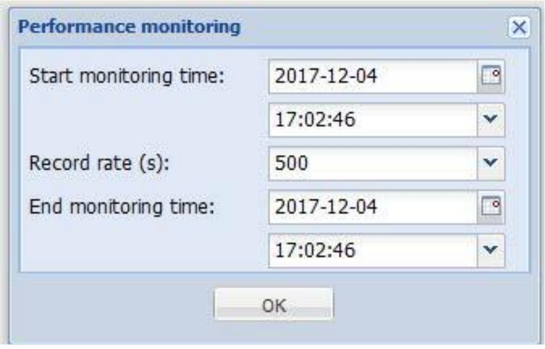
In performance statistics, the user sets the performance monitoring and acquires the performance information of client in specified time. The system will generate the statistical statements according to the acquired sample point for analysis and view.

1. Enter 【client management—>client monitoring—>performance monitoring】 and switch to “performance statistics” tab page, as shown in following figure:



□	Client Alias	UUID	Client IP	Planned start time	Planned end time

2. Click “performance monitoring” button. In the popup dialog box, set the starting and ending time of monitoring and sampling interval.

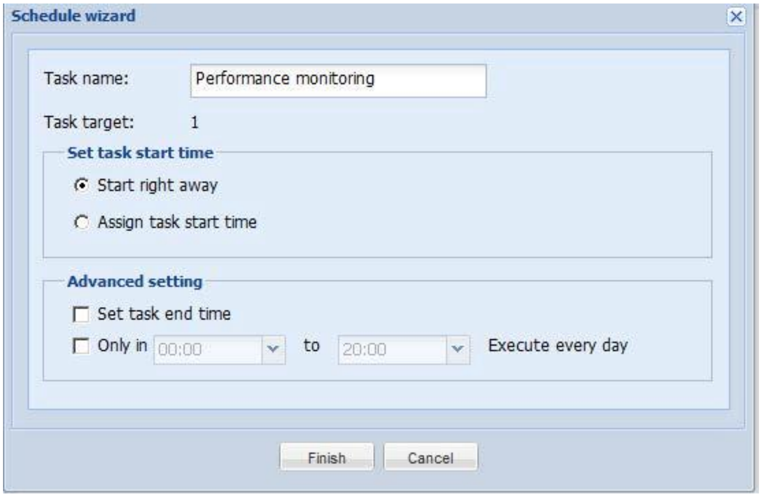

Performance monitoring

Start monitoring time: 2017-12-04 17:02:46

Record rate (s): 500

End monitoring time: 2017-12-04 17:02:46

3. Click “OK” button, configure plan wizard and execute operation.



Schedule wizard

Task name: Performance monitoring

Task target: 1

Set task start time

● Start right away

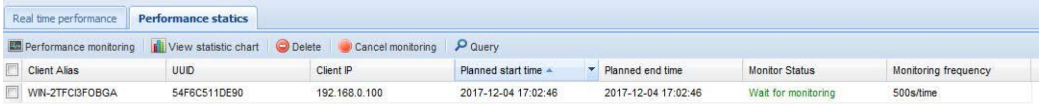
○ Assign task start time

Advanced setting

□ Set task end time

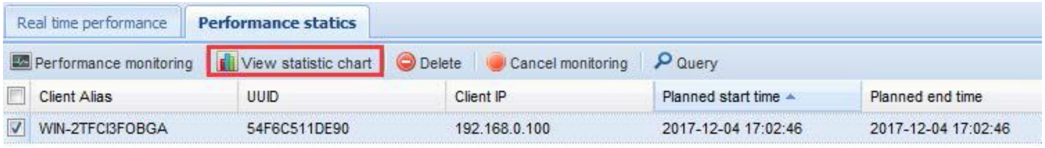
□ Only in 00:00 to 20:00 Execute every day

4. After execution, the monitoring record will be generated, as follows:



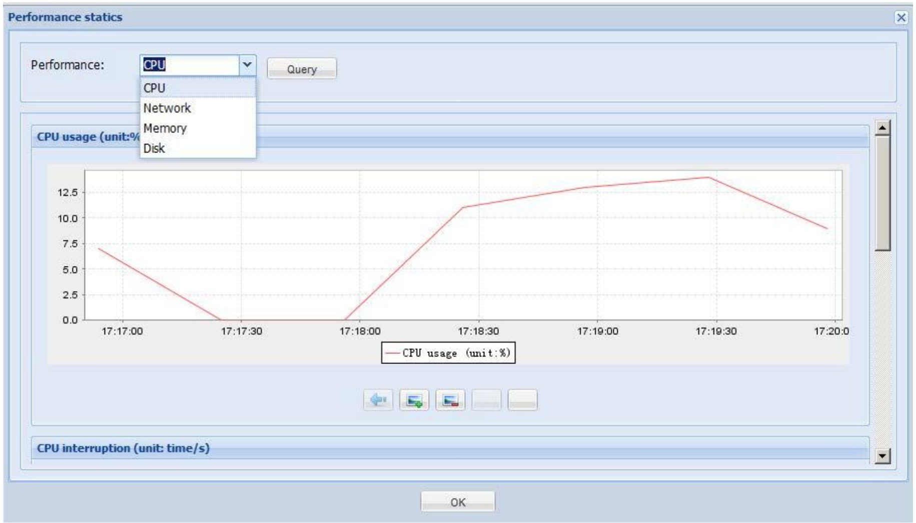
□	Client Alias	UUID	Client IP	Planned start time	Planned end time	Monitor Status	Monitoring frequency
□	WIN-2TFCI3FOBGA	54F6C511DE90	192.168.0.100	2017-12-04 17:02:46	2017-12-04 17:02:46	Wait for monitoring	500s/time

5. Select the monitoring record and click “view the statistical chart”.



□	Client Alias	UUID	Client IP	Planned start time	Planned end time
☑	WIN-2TFCI3FOBGA	54F6C511DE90	192.168.0.100	2017-12-04 17:02:46	2017-12-04 17:02:46

6. The popup performance statistics dialog box will show statistical statements of CPU, memory and network IO.



Performance statics

Performance: CPU

The interface has moving, zooming and other buttons to provide convenient conditions to user.

4.16 Client alarm

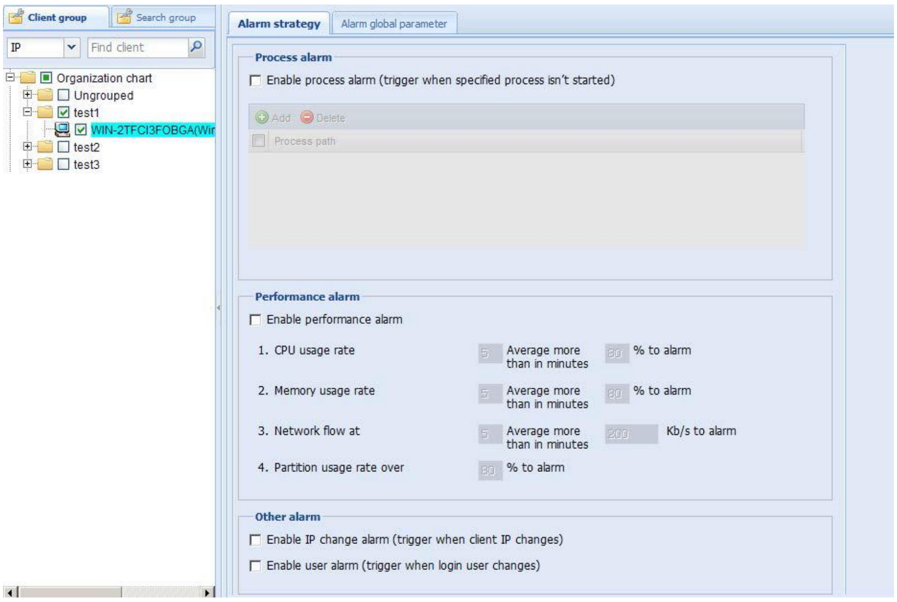
The client alarm is used for alarming the abnormality of client. The administrator can set the item to be alarmed in this module and can set the alarm threshold. When the client sends alarm, the administrator can view the log in the server in time.

4.16.1 Alarm strategy

The alarm strategy is mainly for detailed configuration of alarm threshold of client, including process alarm, performance alarm, etc. The start mode of alarm strategy is as follows:

1. Enter 【client management—>client monitor—>client alarm】 and select “alarm strategy” tab page;

2. Select the client to enable the alarm strategy from the client tree in the left side;



Process alarm

□ Enable process alarm (trigger when specified process isn’t started)

□ Process path

Performance alarm

□ Enable performance alarm

1. CPU usage rate 5 Average more than in minutes 80 % to alarm

2. Memory usage rate 5 Average more than in minutes 80 % to alarm

3. Network flow at 5 Average more than in minutes 200 Kb/s to alarm

4. Partition usage rate over 80 % to alarm

Other alarm

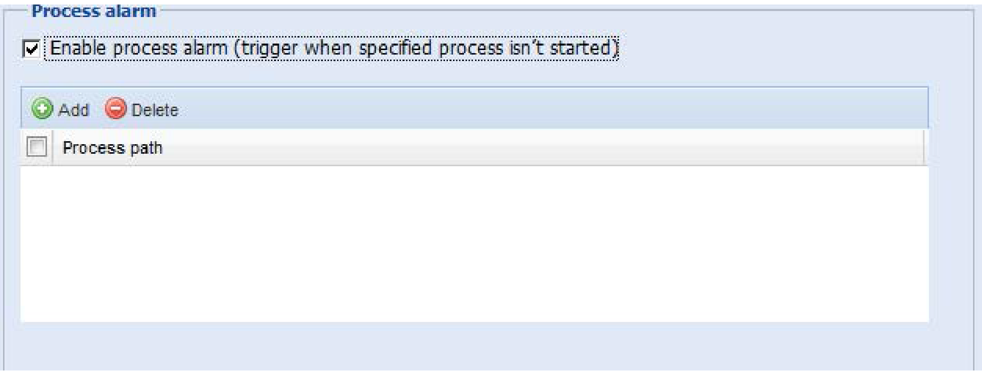
□ Enable IP change alarm (trigger when client IP changes)

□ Enable user alarm (trigger when login user changes)

3. Select the alarm item to be enabled on the right panel. The system provides many available alarm items, i.e. process alarm, performance alarm, IP change alarm and user change alarm.

- Process alarm

If this item is selected, the process list shall be added in the list in following figure. When the client doesn’t enable the process in the list, the system will send alarm.

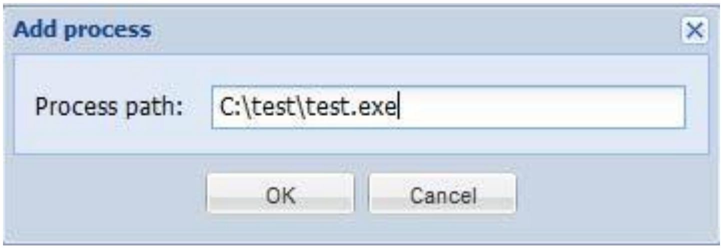


Process alarm

☑ Enable process alarm (trigger when specified process isn’t started)

□ Process path

Click “add” button and fill in the process to be added in the popup whitelist.

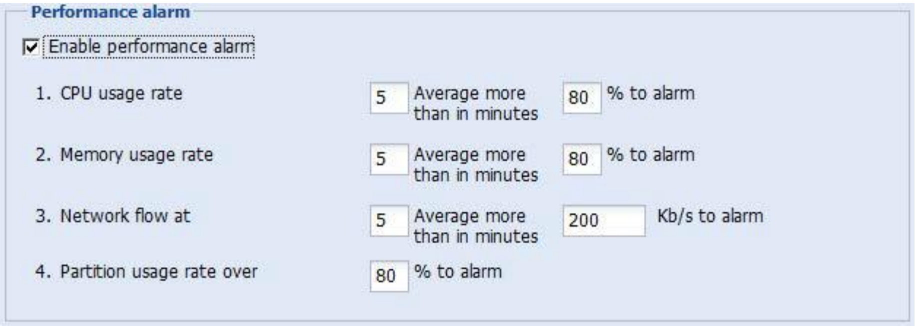


Add process

Process path: C:\test\test.exe

- Performance alarm

The performance alarm is mainly used for alarm of performance situation of client. The available alarm items are CPU, memory, network IO and disk using.



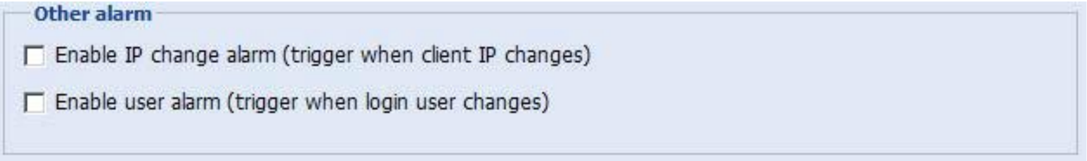
Performance alarm

☑ Enable performance alarm

1. CPU usage rate 5 Average more than in minutes 80 % to alarm
2. Memory usage rate 5 Average more than in minutes 80 % to alarm
3. Network flow at 5 Average more than in minutes 200 Kb/s to alarm
4. Partition usage rate over 80 % to alarm

- Other alarm items

Refer to other common alarm items, including IP alarm and user alarm.



Other alarm

□ Enable IP change alarm (trigger when client IP changes)

□ Enable user alarm (trigger when login user changes)

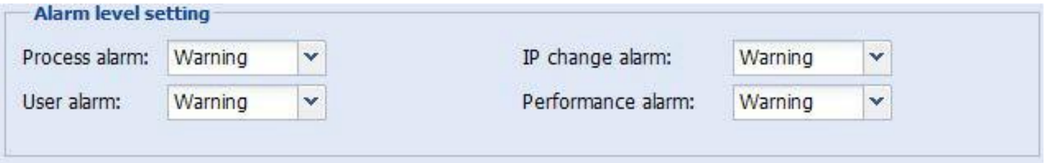
4. Finally, click “apply” button and execute plan wizard to make it valid. After successful execution of strategy, the “audit management” module will show the alarm logs.

4.16.2 Global alarm parameters

The alarm global parameters refer to the set parameters of alarm levels and alarm triggering events of the system. These settings will influence the alarm feedback information of all clients which enable alarm strategy.

2. Set the alarm level

The system divides alarms into three levels, i.e. information, warning and error from low severity to high severity. The user can set the alarm level according to demand, such as set the IP alarm level as “error”. In this case, when the system sends IP alarm, the alarm information shall be marked as “error”.



Alarm level setting

Process alarm: Warning

IP change alarm: Warning

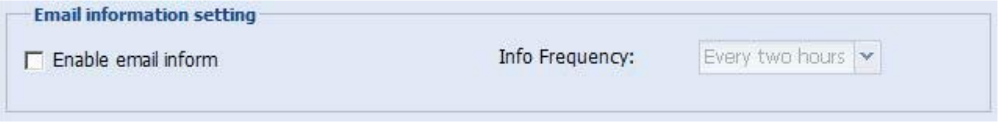
User alarm: Warning

Performance alarm: Warning

3. Set the mail notice

When the system sends the alarm information, the system will send the alarm mail to the administrator’s email in specified time.

Notice: the user shall set the system email in 【other management—>global parameter setting】, otherwise, the mail cannot be sent.



Email information setting

□ Enable email inform

Info Frequency: Every two hours

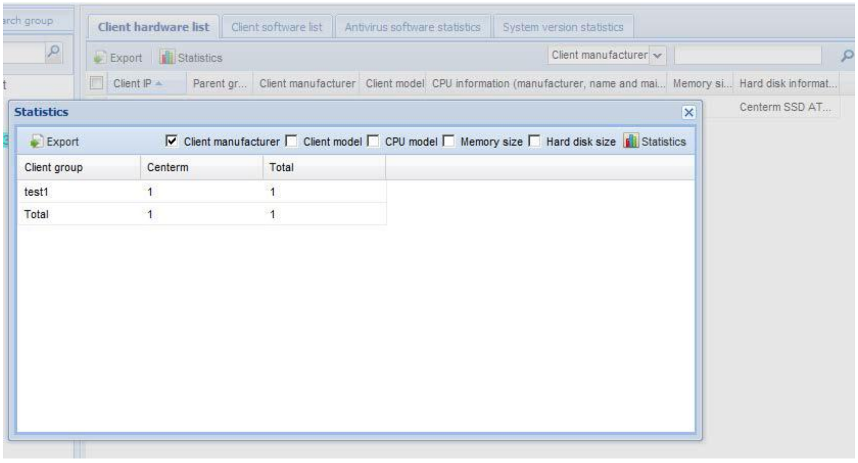
4. Finally, click “apply” button to make it valid.

4.17 Asset management

Asset management is the statistics and analysis of clients currently managed by the system, including hardware, software and other asset information. It can be regarded as the basis data for knowing the client overview and further making statistics by administrator.

4.17.1 Client hardware list

The system will list the corresponding hardware information, including client manufacturer, model and CPU information for the group or client selected by the administrator. Click “statistics” button on the upper left side of the interface. The system will automatically generate the statistics statement according to the selected conditions.



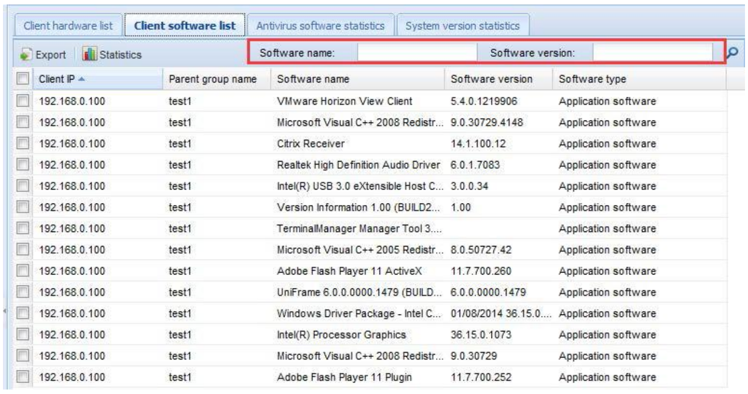
☑ Client manufacturer □ Client model □ CPU model □ Memory size □ Hard disk size Statistics

Client group	Centerm	Total
test1	1	1
Total	1	1

4.17.2 Client software list

The client software list shows all software installed in the currently selected client.

If the administrator needs to obtain the software information of single client, the administrator can select this client from the client tree. If the administrator needs to obtain the installation situation of specified version of certain software. Input the query conditions in the query box in following figure. Click "statistics" button on the upper left of interface. The system will automatically generate the statistics list according to the selected conditions.

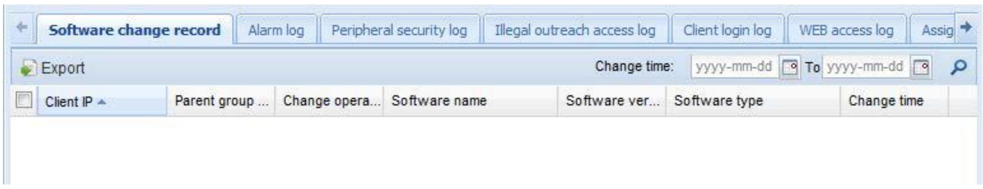


Software name: Software version:

□	Client IP	Parent group name	Software name	Software version	Software type
□	192.168.0.100	test1	VMware Horizon View Client	5.4.0.1219906	Application software
□	192.168.0.100	test1	Microsoft Visual C++ 2008 Redistr...	9.0.30729.4148	Application software
□	192.168.0.100	test1	Citrix Receiver	14.1.100.12	Application software
□	192.168.0.100	test1	Realtek High Definition Audio Driver	6.0.1.7083	Application software
□	192.168.0.100	test1	Intel(R) USB 3.0 eXtensible Host C...	3.0.0.34	Application software
□	192.168.0.100	test1	Version Information 1.00 (BUILD2...	1.00	Application software
□	192.168.0.100	test1	TerminalManager Manager Tool 3....		Application software
□	192.168.0.100	test1	Microsoft Visual C++ 2005 Redistr...	8.0.50727.42	Application software
□	192.168.0.100	test1	Adobe Flash Player 11 ActiveX	11.7.700.260	Application software
□	192.168.0.100	test1	UniFrame 6.0.0.0000.1479 (BUILD...	6.0.0.0000.1479	Application software
□	192.168.0.100	test1	Windows Driver Package - Intel C...	01/08/2014 36.15.0....	Application software
□	192.168.0.100	test1	Intel(R) Processor Graphics	36.15.0.1073	Application software
□	192.168.0.100	test1	Microsoft Visual C++ 2008 Redistr...	9.0.30729	Application software
□	192.168.0.100	test1	Adobe Flash Player 11 Plugin	11.7.700.252	Application software

4.17.3 Software change record

In order to monitor whether the client user installs or uninstalls software without authorization, the management system will provide the operation record of client software change.



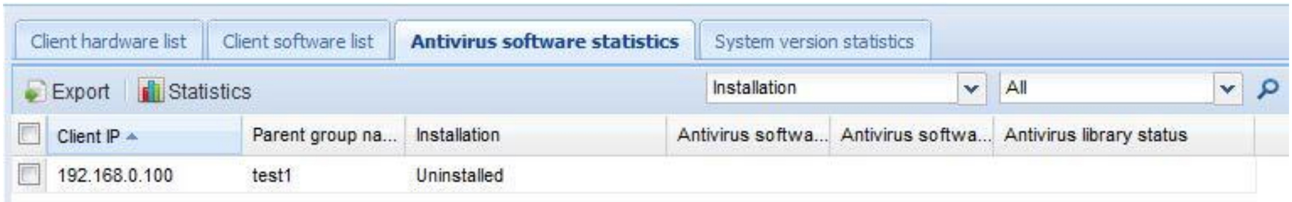
Change time: yyyy-mm-dd To yyyy-mm-dd

□	Client IP	Parent group ...	Change opera...	Software name	Software ver...	Software type	Change time

4.17.4 Antivirus software statistics

The antivirus software statistics shows the using situation of antivirus software in the currently selected client, including whether the antivirus software is installed, enabled, and expired. This function can assist the administrator to know the antivirus situation of the client.

Click "statistics" button to generate the statistical statements of antivirus software, as shown in following figure:

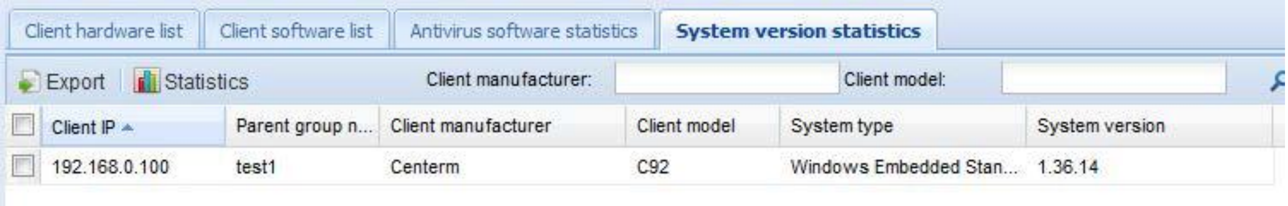


Installation | All

☐	Client IP ▲	Parent group na...	Installation	Antivirus softwa...	Antivirus softwa...	Antivirus library status
☐	192.168.0.100	test1	Uninstalled			

4.17.5 System version statistics

The system version statistics is the statistics for system versions of managed clients and can be regarded as the reference data of system version upgrade of client. Click “statistics” button on the upper left of the interface to automatically generate the statistical list according to selected conditions.



Client manufacturer: | Client model:

☐	Client IP ▲	Parent group n...	Client manufacturer	Client model	System type	System version
☐	192.168.0.100	test1	Centerm	C92	Windows Embedded Stan...	1.36.14

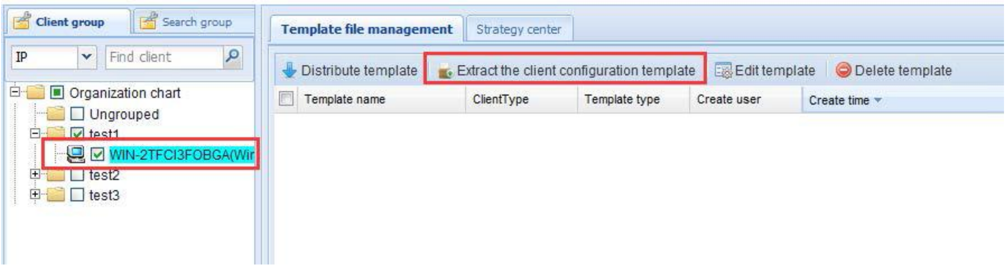
4.18 Template management

4.18.1 Template file management

The template file management can extract and keep the parameter configuration of clients as template in the server or save templates of some tasks (file copy, software installation, peripheral security and software blacklist and whitelist) so as to rapidly set the clients by batch.

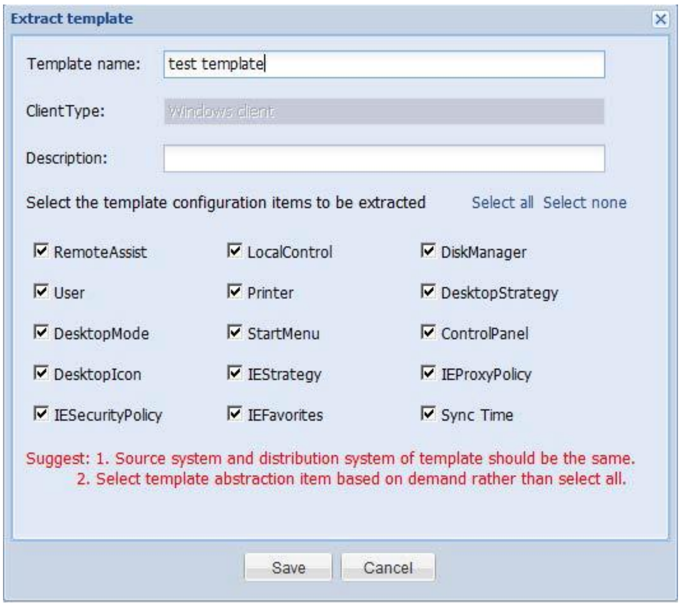
4.18.1.1 Extract client configuration template

1. Select one client and click “extract client configuration template” button.



☐	Template name	ClientType	Template type	Create user	Create time ▾

2. Fill in the text information of template and select the item to be extracted. In the following figure, remote assistance, desktop mode, IE strategy and IE favorites are selected.



Template name: test template

ClientType: Windows client

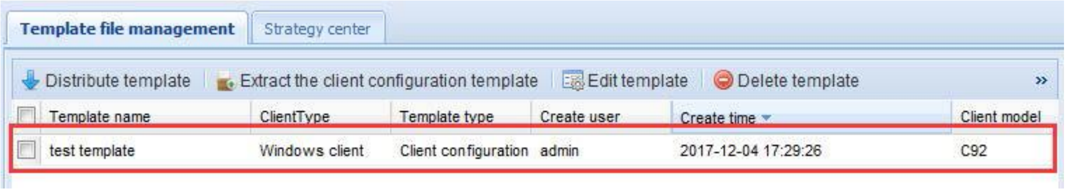
Description:

Select the template configuration items to be extracted

☑ RemoteAssist ☑ LocalControl ☑ DiskManager
☑ User ☑ Printer ☑ DesktopStrategy
☑ DesktopMode ☑ StartMenu ☑ ControlPanel
☑ DesktopIcon ☑ IEStrategy ☑ IEProxyPolicy
☑ IESecurityPolicy ☑ IEFavorites ☑ Sync Time

Suggest: 1. Source system and distribution system of template should be the same.
2. Select template abstraction item based on demand rather than select all.

3. After saving, the list will show the template extracted just now.



□	Template name	ClientType	Template type	Create user	Create time	Client model
□	test template	Windows client	Client configuration	admin	2017-12-04 17:29:26	C92

Notice:

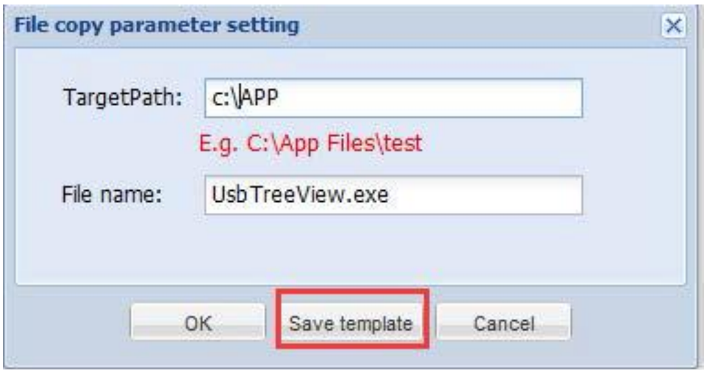
- The client for extraction shall be online. Otherwise, the extraction will be in failure.
- The user can select the item of template files on the panel according to his/her demand.

4.18.1.2 Save task template

File copy, software installation, peripheral security and software blacklist and whitelist template can be saved.

1) File copy

Enter the file deployment page to copy the file. In the configuration page, click “save template”.



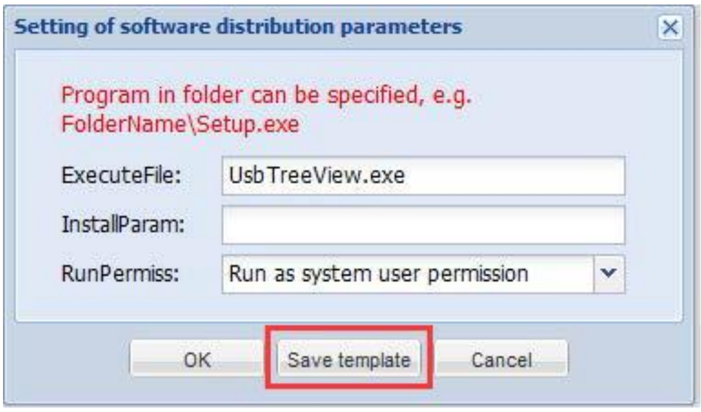
TargetPath: c:\APP

E.g. C:\App Files\test

File name: UsbTreeView.exe

2) Software installation

After entering the file deployment page, install the software. In the configuration page, click “save template”.



Program in folder can be specified, e.g. FolderName\Setup.exe

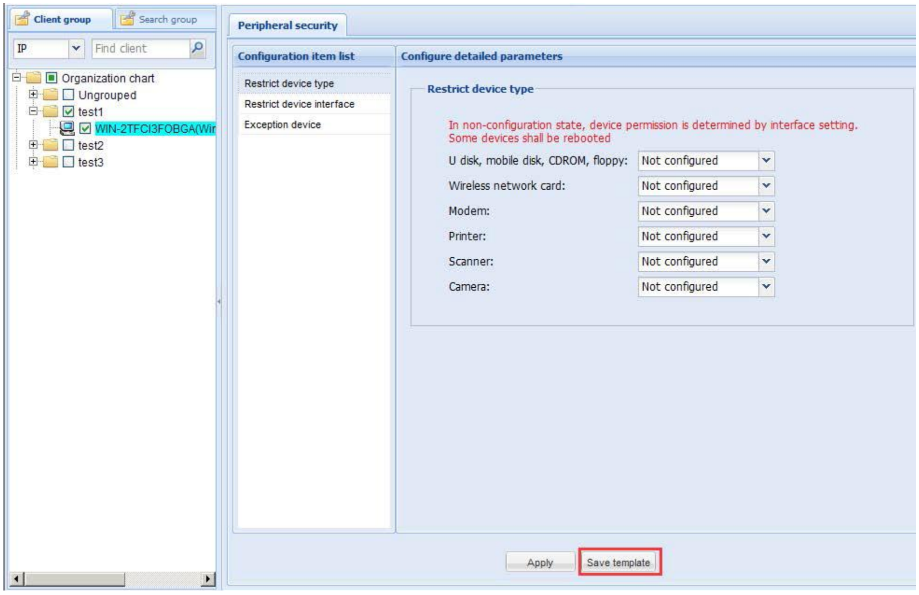
ExecuteFile: UsbTreeView.exe

InstallParam:

RunPermiss: Run as system user permission

3) Peripheral security

Enter the peripheral security page, configure the peripheral security and click “save template”.

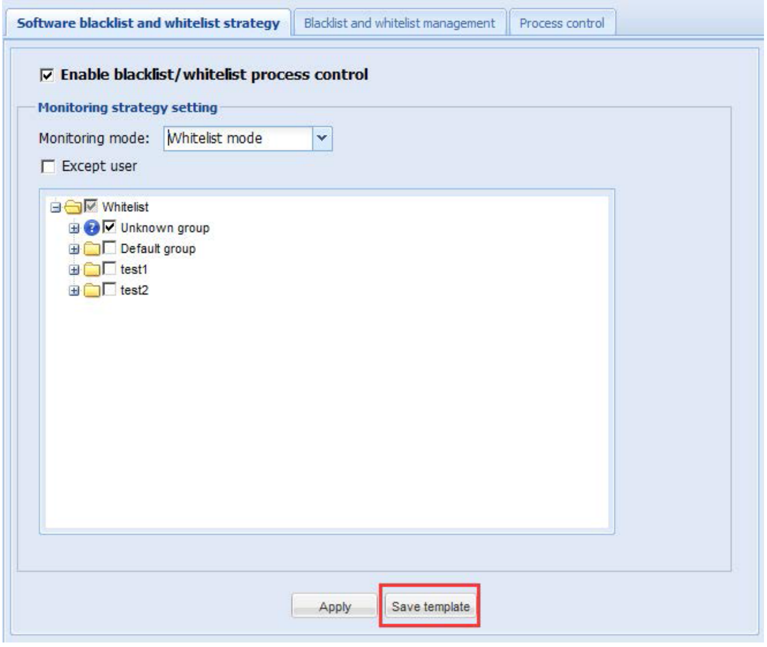


In non-configuration state, device permission is determined by interface setting. Some devices shall be rebooted

U disk, mobile disk, CDROM, floppy:	Not configured
Wireless network card:	Not configured
Modem:	Not configured
Printer:	Not configured
Scanner:	Not configured
Camera:	Not configured

4) Software blacklist and whitelist

Enter the software blacklist and whitelist page, configure the software blacklist and whitelist and save the template.

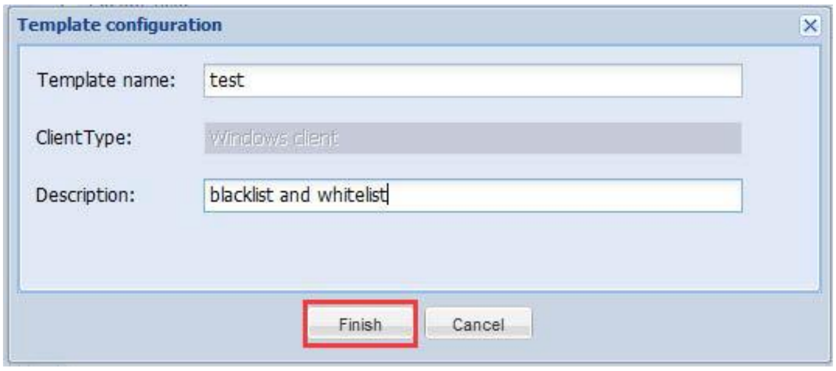

Software blacklist and whitelist strategy
Blacklist and whitelist management
Process control
Monitoring strategy setting
Whitelist
Unknown group
Default group
test1
test2
Apply
Save template

☑ Enable blacklist/whitelist process control

Monitoring mode: Whitelist mode

□ Except user

After clicking “save template”, the system will pop up template information windows.

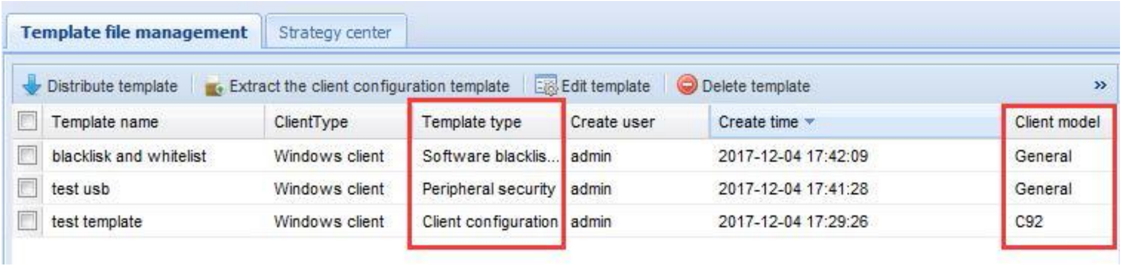


Template name: test

ClientType: Windows client

Description: blacklist and whitelist

The template management page will show the following template information:

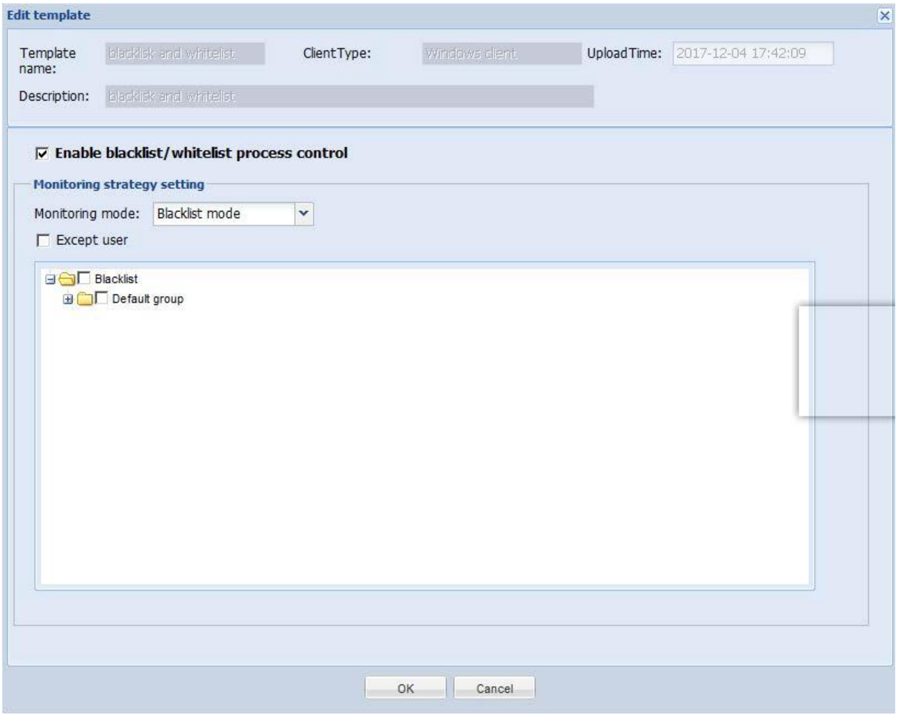


□	Template name	ClientType	Template type	Create user	Create time	Client model
□	blacklisk and whitelist	Windows client	Software blacklis...	admin	2017-12-04 17:42:09	General
□	test usb	Windows client	Peripheral security	admin	2017-12-04 17:41:28	General
□	test template	Windows client	Client configuration	admin	2017-12-04 17:29:26	C92

The list shows types of template and applicable modes of clients.

4.18.1.3 Edit template

After selecting the template, click “edit the template” button to edit the saved template.



Edit template

Template name: blacklisk and whitelist

ClientType: Windows client

UploadTime: 2017-12-04 17:42:09

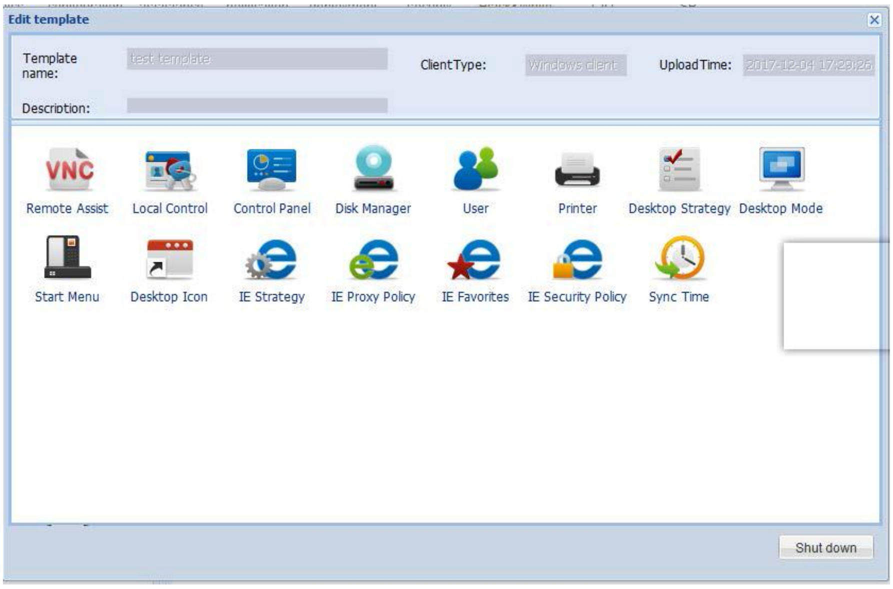
Description: blacklisk and whitelist

☑ Enable blacklist/whitelist process control

Monitoring strategy setting

Monitoring mode: Blacklist mode

□ Except user



Edit template

Template name: test template

ClientType: Windows client

UploadTime: 2017-12-04 17:29:26

Description:

After changing the template content, click “OK” or “save” to save the edited template.

4.18.1.4 Distribute template

1. Select the client which receives the distributed template and template files.

2. Click “distribute the template” button.

3. Configure “plan wizard” and execute the task.

Notice:

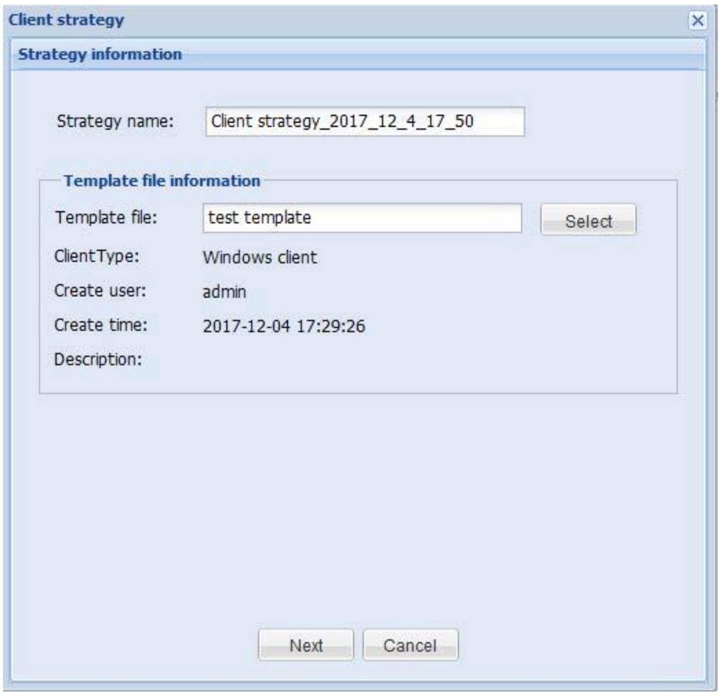
- The client selected by user may be one or more and can be selected based on group.
- The template file to be selected by user shall be only one. If the client configuration template is selected, the client types to which the template is applicable shall be consistent with the type of client selected by user.

4.18.2 Strategy center

In order to apply the unified strategy in a certain group or automatically apply the strategy to new clients in the group, the template binding function of strategy center can be used. The operation steps are as follows:

1. Click “add the strategy” button;

2. Select the template file to be bound and click “next” in the popup dialog box;



Client strategy

Strategy information

Strategy name: Client strategy_2017_12_4_17_50

Template file information

Template file: test template

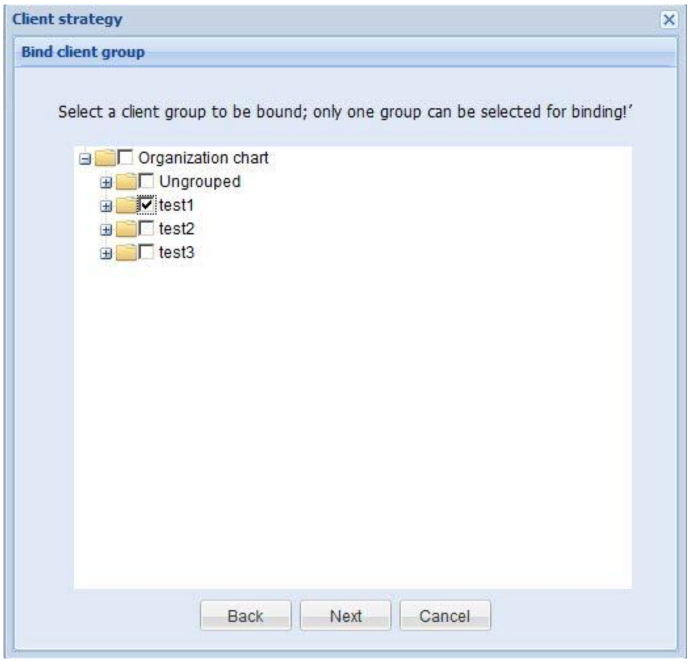
ClientType: Windows client

Create user: admin

Create time: 2017-12-04 17:29:26

Description:

3. Select the group to be bound and click “next”.



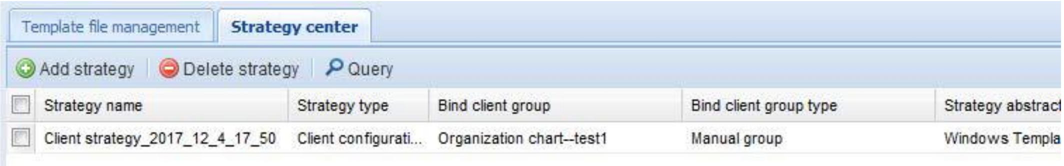
Client strategy

Bind client group

Select a client group to be bound; only one group can be selected for binding!’

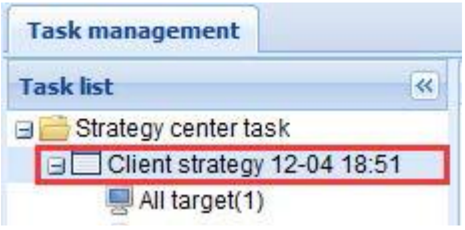
- □ Organization chart
  - □ Ungrouped
  - ☑ test1
  - □ test2
  - □ test3

4. Configure plan wizard and finish the creation of strategy;



□	Strategy name	Strategy type	Bind client group	Bind client group type	Strategy abstract
□	Client strategy_2017_12_4_17_50	Client configurati...	Organization chart--test1	Manual group	Windows Templa

5. The execution situation of strategy can be viewed in “strategy center task” node in “task statistics” module.



5. Peripheral Management

5.1 CID management

This function shows the CID in different groups according to organization structures of client connected with CID. At present, the management function supports software upgrade of CID device.

5.1.1 Software upgrade

1. Click “upload the upgrade file” button;

2. Select the local upgrade file in the popup dialog box to finish upload;

3. Select CID to be upgraded. Select the upgrade file in the list. Click “distribute” button;

4. Configure the distribution parameters and select whether to confirm before upgrade.

5.2 SP management

5.2.1 Software upgrade

1. Click “upload the upgrade file” button;

2. Select the local upgrade file in the popup dialog box to finish upload;

3. Select SP to be upgraded. Select the upgrade file in the list. Click “distribute” button;

4. Configure the distribution parameters and select whether to confirm before upgrade.

5.2.2 Resource publish

1. Click “upload the resource file” button;

2. Select the local upgrade file in the popup dialog box to finish upload; the following three resource files are supported:

- **Picture**

Support jpg, bmp and png format

- **Video**

Only support mp4 format with mpeg4, h264 and aac coding format

- **Audio**

Only support mp3 format

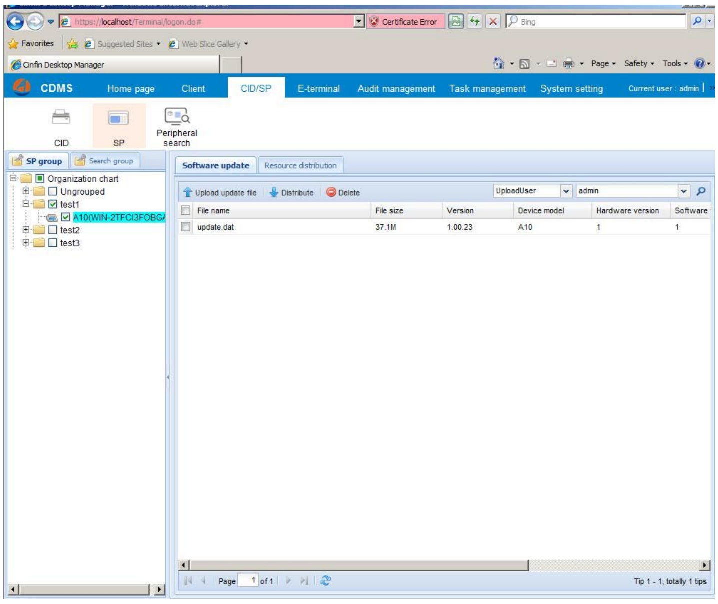
- **Folder**

Support the folder which contains above files.

Notice: if the distributed resource of SP is folder, the function only supports the same resource in one folder (picture or video) and doesn't support picture and video in one distributed folder.

3. Select SP to be upgraded. Select the upgrade file in the list. Click "distribute" button;

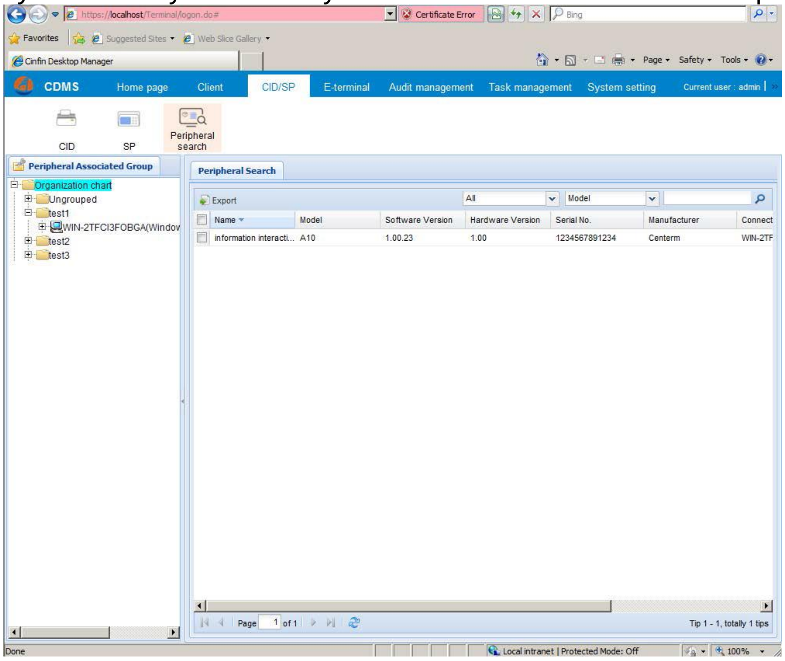
4. Configure the distribution parameters and select whether to confirm before upgrade and the addition form of resource file in SP.



□	File name	File size	Version	Device model	Hardware version	Software
□	update.dat	37.1M	1.00.23	A10	1	1

5.3 Peripheral query

The peripheral query function has a unified query page, can realize the query of all peripherals synchronously and visually shows the association relationship between peripherals and client by picture.



□	Name	Model	Software Version	Hardware Version	Serial No.	Manufacturer	Connect
□	information interacti...	A10	1.00.23	1.00	1234567891234	Centerm	WIN-2TF

6. Task Statistics

6.1 Brief introduction to task

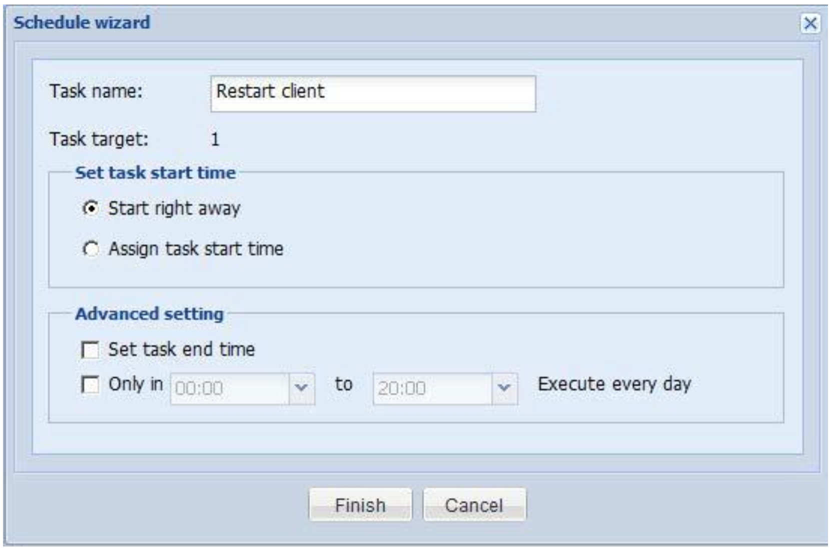
1. What is task?

The task refers to one command or a series of commands distributed by a system to client to be treated by client according to the specific situation. At present, most management operations of system for client are realized by task.

2. How to generate a task?

Execution of some operation commands in client by an administrator will generate the corresponding task. Each operation will form a task record. One task is applicable to one client or more clients. In the system, the software distribution, file copy, strategy configuration (such as software blacklist and whitelist and peripheral security) and power control of client will form the corresponding task record.

For example, in power control, after clicking “apply” button, the following plan wizard panel will generate:



Task name: Restart client

Task target: 1

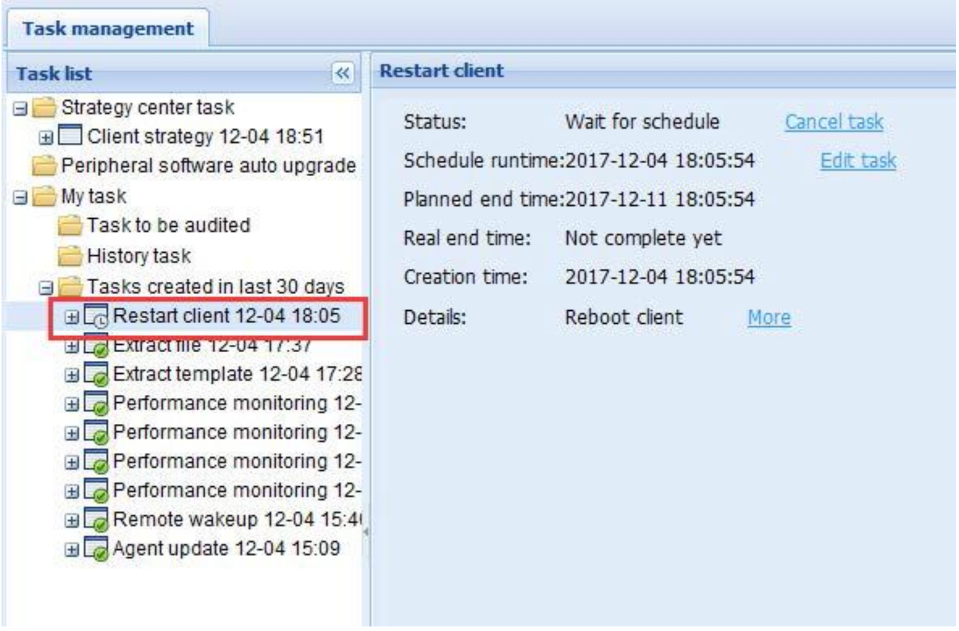
● Start right away

○ Assign task start time

□ Set task end time

□ Only in 00:00 to 20:00 Execute every day

Click “end” button and view corresponding task record in 【task management】 module.


Task management
Task list
Strategy center task
Client strategy 12-04 18:51
Peripheral software auto upgrade
My task
Task to be audited
History task
Tasks created in last 30 days
Restart client 12-04 18:05
Extract file 12-04 17:37
Extract template 12-04 17:28
Performance monitoring 12-
Performance monitoring 12-
Performance monitoring 12-
Performance monitoring 12-
Remote wakeup 12-04 15:4
Agent update 12-04 15:09
Restart client
Cancel task
Edit task
More

Status: Wait for schedule

Schedule runtime:2017-12-04 18:05:54

Planned end time:2017-12-11 18:05:54

Real end time: Not complete yet

Creation time: 2017-12-04 18:05:54

Details: Reboot client

3. Display of task node

The task tree has two folders, i.e. “historic tasks” and “tasks in recent 30 days”. When a task has been created for more than 30 days, the task will be automatically transferred to “historic task”. The latest task will be at the top of “tasks in recent 30 days” for viewing of the administrator.

6.2 Task properties

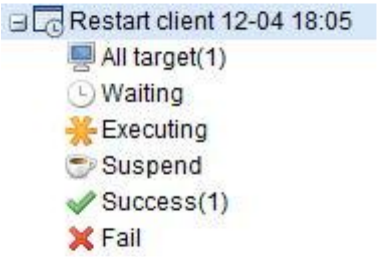
The task has following properties during generation:

1. Task name

The task name is a key word for identifying the task. When an administrator creates a task, the system will automatically name the task according to its type. The name can be manually changed by the administrator. In order to distinguish the task, the planned starting time of a task will be added behind the task name in task node on task execution state panel.

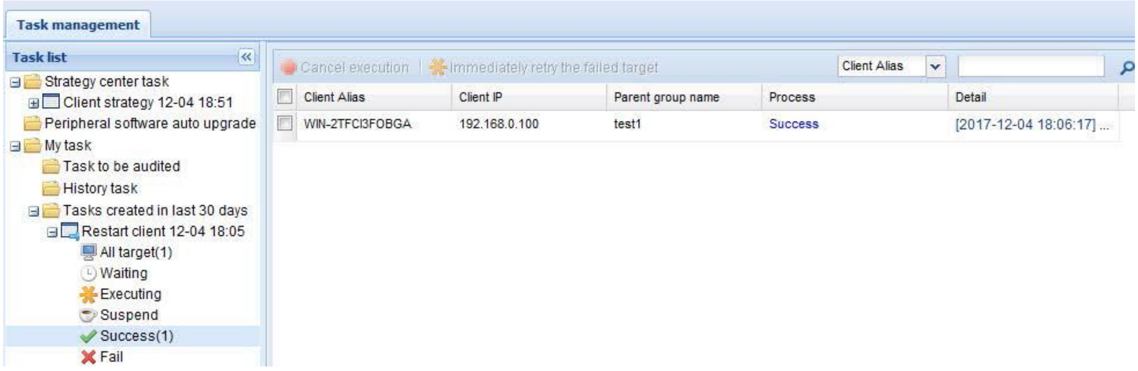
2. Task object

The task object refers to the target client of current task. The task can be generated by at least one client. The task nodes in task management module includes all objects, wait for executing, executing, hanging, success and failure nodes based on different execution states, as follows:



- Restart client 12-04 18:05
  - All target(1)
  - Waiting
  - Executing
  - Suspend
  - Success(1)
  - Fail

Click the node to link with corresponding object list.



□	Client Alias	Client IP	Parent group name	Process	Detail
□	WIN-2TFCI3FOBGA	192.168.0.100	test1	Success	[2017-12-04 18:06:17] ...

3. Task starting time

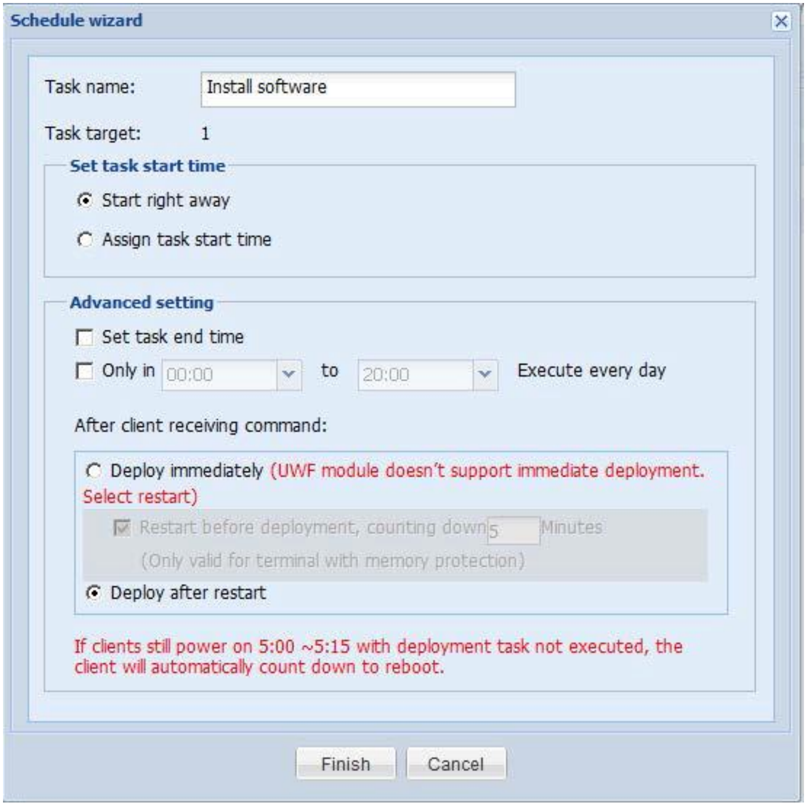
The task starting time refers to the task scheduling starting time. Before starting time, the task is in the state of waiting for scheduling.

① Immediately start: immediately schedule the current task;

② Specify the task starting time: specify the task scheduling starting time. The specified time shall be later than the current time.

4. Whether to prompt the user to restart

In the system, the configuration or update of some modules shall be valid after restart of client, such as client configuration, file deployment and client upgrade. The plan panel of such task will display the execution setting option of client.



Schedule wizard

Task name: Install software

Task target: 1

Set task start time

● Start right away

○ Assign task start time

Advanced setting

□ Set task end time

□ Only in 00:00 to 20:00 Execute every day

After client receiving command:

○ Deploy immediately (UWF module doesn't support immediate deployment. Select restart)

☑ Restart before deployment, counting down 5 Minutes

(Only valid for terminal with memory protection)

● Deploy after restart

If clients still power on 5:00 ~5:15 with deployment task not executed, the client will automatically count down to reboot.

5. Task ending time

The task ending time is the time of forcible ending of task. It is applicable to following two situations:

① The task lasts for long time, such as file deployment task. If the administrator wants to send the files to many clients within two days, the sending time may be longer than 2 days because of too many clients. If the ending time is set, the task will stop before the ending time to avoid influence on business in normal work time.

② The task has timeliness, such as message and power control task. If the client is offline when the task is distributed, the task will be always in the scheduling state and waiting for online of client. However, if the administrator only wants to send the message to client or power off before going off work, the task significance will be lost after this time. At this time, the task ending time can be set to control the timeliness of the task.

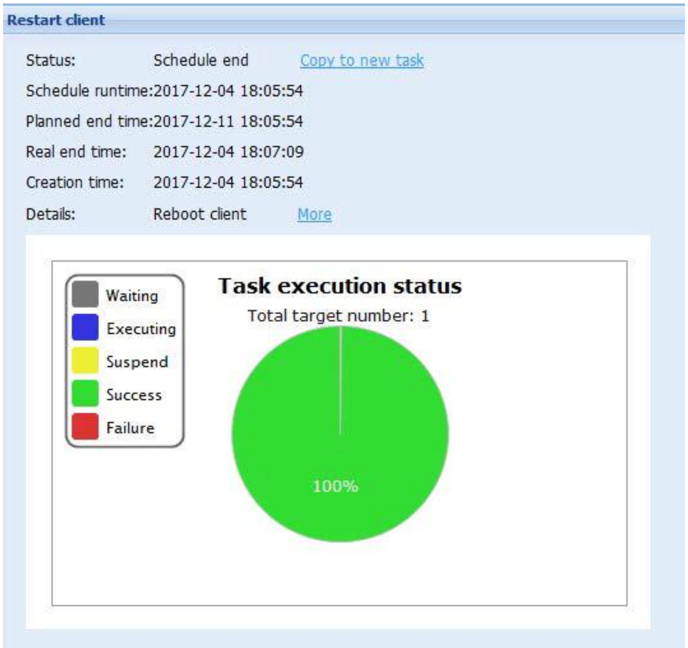
6. Task execution time

The task execution time is the execution time of object client of limited task.

For example, the administrator wants to upgrade many clients in non-working hours and the clients shall normally operate in working hours. However, the off-working hours in one day may be insufficient to upgrade all clients. In this circumstance, the administrator can set that the objects are only upgraded in the execution time, are suspended in non-execution time and then are upgraded in the next execution time.

7. Task abstract

The task abstract is the abstract of task content and can be viewed on the information panel of task. For example, if the message task is sent, partial content of the message will be displayed in the abstract. Click “more” to link to the detailed information penal of task, as shown in following figure.



Restart client

Status: Schedule end Copy to new task

Schedule runtime:2017-12-04 18:05:54

Planned end time:2017-12-11 18:05:54

Real end time: 2017-12-04 18:07:09

Creation time: 2017-12-04 18:05:54

Details: Reboot client More

6.3 Task state

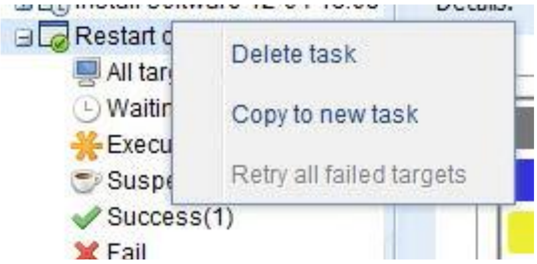
The tasks have three states:

Task state	State icon	State description
Wait for scheduling	🕒	Before the starting time, tasks are in this state
Scheduling	↻	The task is in scheduling
After finishing	✓	All task objects are successfully executed
	⚠	All task objects are executed, but some objects are failed.

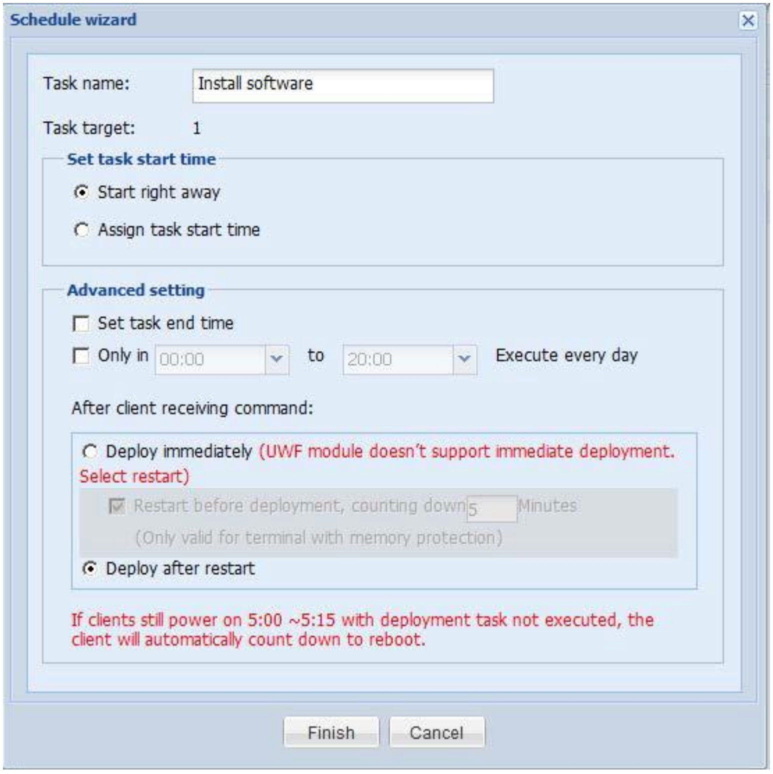
6.4 Task copy

Task copy is equals to creation of a new task with the same content and object of original task. During copying, the administrator can plan the task execution time.

Right click on task node and select “copy as new task”



The task name can be changed and the plan time can be configured in the popup panel.



Schedule wizard

Task name: Install software

Task target: 1

Set task start time

● Start right away

○ Assign task start time

Advanced setting

□ Set task end time

□ Only in 00:00 to 20:00 Execute every day

After client receiving command:

○ Deploy immediately (UWF module doesn't support immediate deployment. Select restart)

☑ Restart before deployment, counting down 5 Minutes

(Only valid for terminal with memory protection)

● Deploy after restart

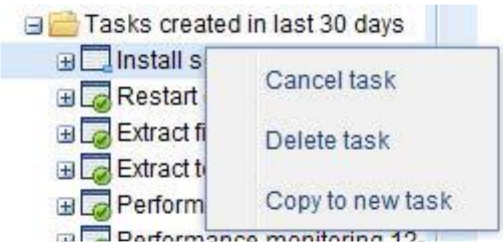
If clients still power on 5:00 ~5:15 with deployment task not executed, the client will automatically count down to reboot.

6.5 Task editing

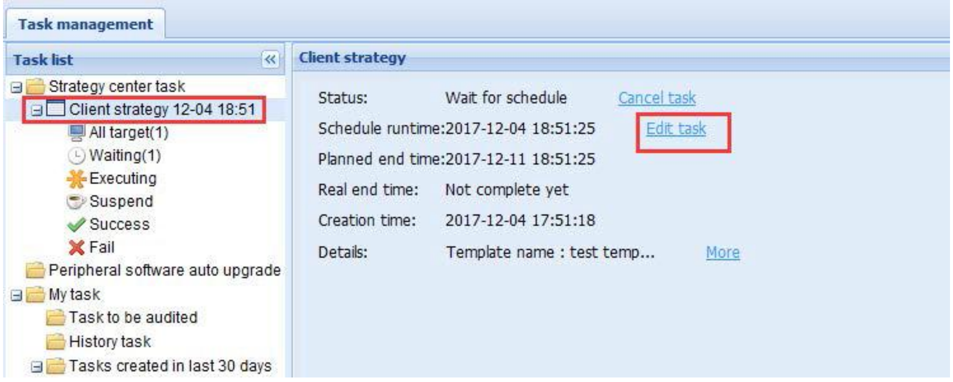
Task information editing refers to change of plan time and name of the task. At present, the system only supports editing the task in "waiting for scheduling" state.

The task can be edited by following two modes:

Right click on the task in waiting for scheduling state and select "edit task". Change on the popup panel.



Alternatively, click the task node. On the task information panel in right side, select "edit task" link in right side of the plan time. Change on the popup panel.



Status: Wait for schedule

Schedule runtime:2017-12-04 18:51:25

Planned end time:2017-12-11 18:51:25

Real end time: Not complete yet

Creation time: 2017-12-04 17:51:18

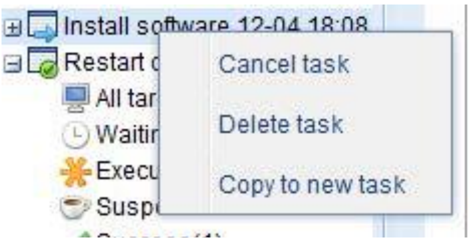
Details: Template name : test temp...

6.6 Task cancellation

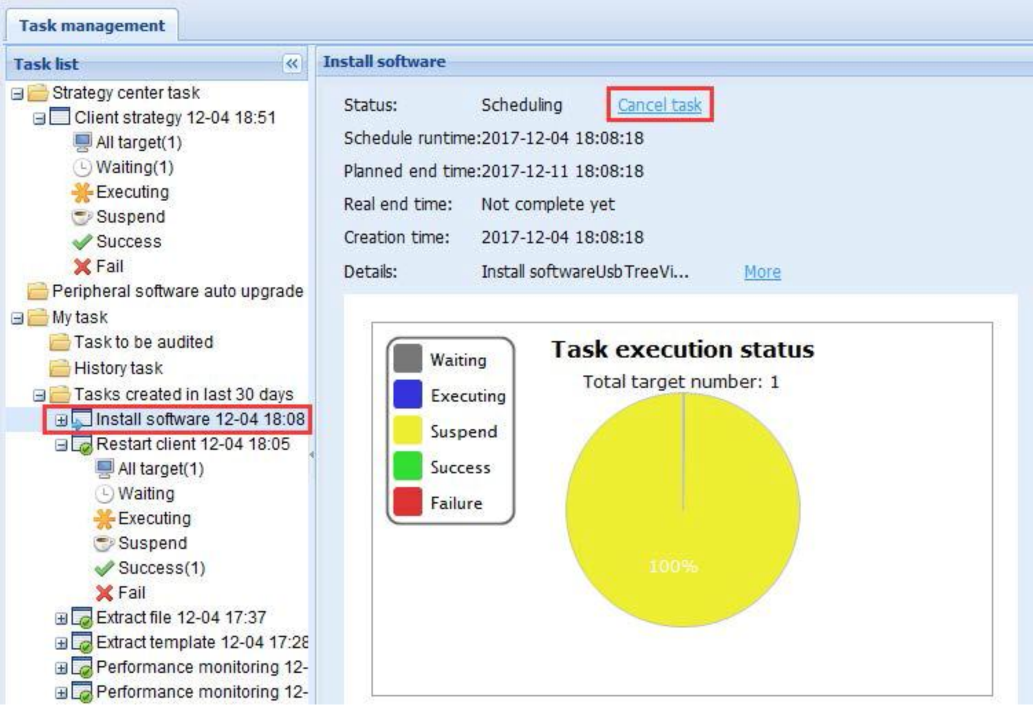
When the administrator executes the wrong operation or wants to cancel the generated task, the administrator can use this function.

1. Cancel task

Right click on the task in waiting for scheduling or in scheduling state and select “cancel task”.



Or click the task node and click “cancel task” link on the task information panel in right side.



Status: Scheduling

Schedule runtime:2017-12-04 18:08:18

Planned end time:2017-12-11 18:08:18

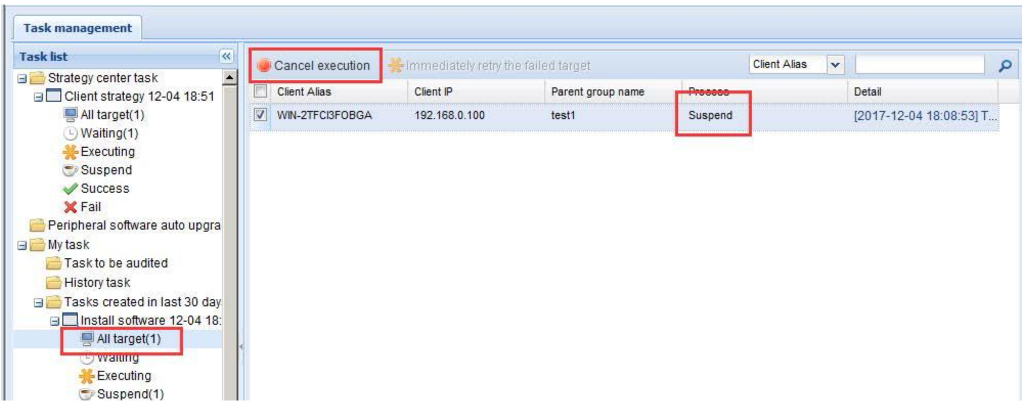
Real end time: Not complete yet

Creation time: 2017-12-04 18:08:18

Details: Install softwareUsbTreeVi...

2. Cancel execution object

When the task is in scheduling state and its objects aren’t fully executed, the administrator can cancel the object in “wait for executing” state in the object list.



☐	Client Alias	Client IP	Parent group name	Process	Detail
☑	WIN-2TFCI3FOBGA	192.168.0.100	test1	Suspend	[2017-12-04 18:08:53] T...

Pay attention to following content in calculation:

- Task calculation actually refers to cancellation of execution of all objects.
- Only the task in “wait for scheduling” and “scheduling” state can be cancelled.
- Only the object in the “wait for executing” and “executing” state can be cancelled. The cancelled object will be included in failure state.

- When the task is in “scheduling” state, some objects may be executed in success or failure. At this time, the cancelation operation will be invalid for this part of task. The cancelled object will be included in failure state.
- When the administrator deletes the task, the task in “wait for scheduling” and “scheduling” state will be automatically cancelled and then be deleted.

6.7 Task scheduling in order

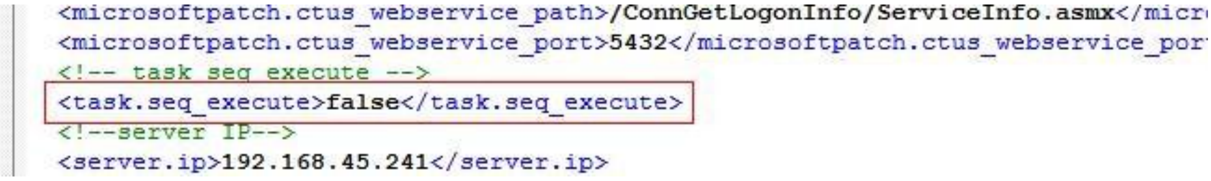
In a specific application demand scenario, the tasks can be scheduled by changing the configuration in the order of creation time.

Change steps:

1. Enter the directory C:\ProgramFiles(x86)\Centerm\runtime\conf

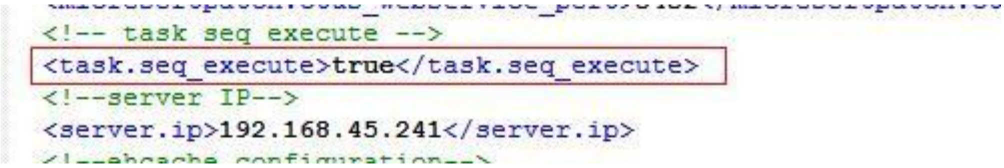
2. Open system.xml file

3. Find the following configuration nodes



```
<microsoftpatch.ctus_webservice_path>/ConnGetLogonInfo/ServiceInfo.asmx</micr
<microsoftpatch.ctus_webservice_port>5432</microsoftpatch.ctus_webservice_por
<!-- task seq execute -->
<task.seq_execute>false</task.seq_execute>
<!--server IP-->
<server.ip>192.168.45.241</server.ip>
```

The default value is false. Change it to true.



```
<microsoftpatch.ctus_webservice_port>5432</microsoftpatch.ct
<!-- task seq execute -->
<task.seq_execute>true</task.seq_execute>
<!--server IP-->
<server.ip>192.168.45.241</server.ip>
<!--ehcache configuration-->
```

4. After changing the configuration, “UnitedWeb” will take effect after restart of server

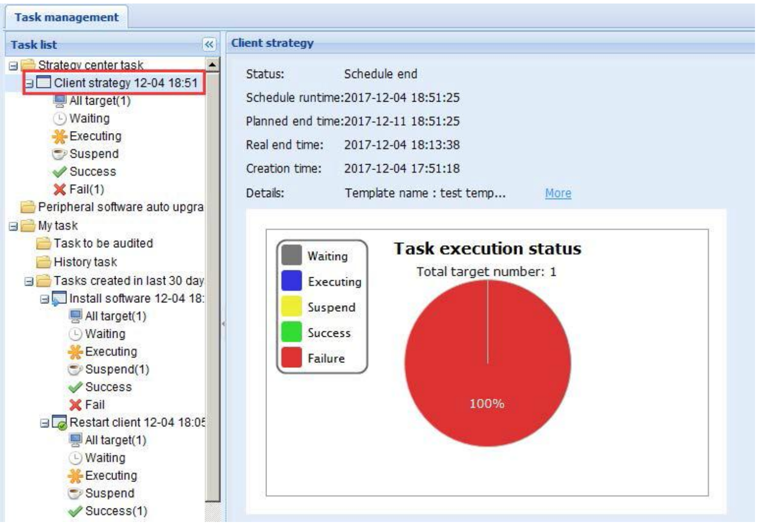
Remark: the enabling and disabling task sequence scheduling only can take effect after restart of server.

6.8 Error troubleshooting and retrying

The object of a task may be in failure. The system has the function of error troubleshooting and retrying for failed objects.

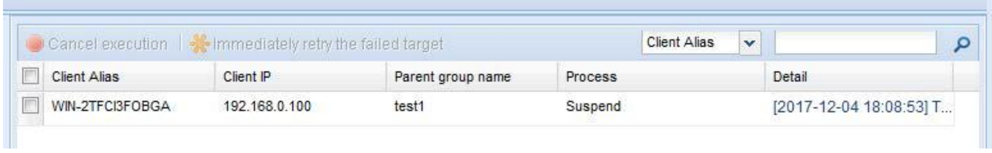
1. Error troubleshooting

Click the task node. The information panel in right side will display the scheduling situation of current task, including the execution situation of object clients. Click corresponding part on the pie graph to enter the corresponding object list.



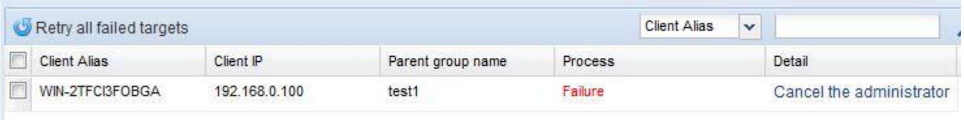
Status: Schedule end
Schedule runtime:2017-12-04 18:51:25
Planned end time:2017-12-11 18:51:25
Real end time: 2017-12-04 18:13:38
Creation time: 2017-12-04 17:51:18
Details: Template name : test temp... More

When the object client is in “wait for executing” state for a long period, the administrator can view the error report abstract in the detailed information column in the object list.



□	Client Alias	Client IP	Parent group name	Process	Detail
□	WIN-2TFCI3FOBGA	192.168.0.100	test1	Suspend	[2017-12-04 18:08:53] T...

When the object client executes in failure, the administrator also can view the detailed information.



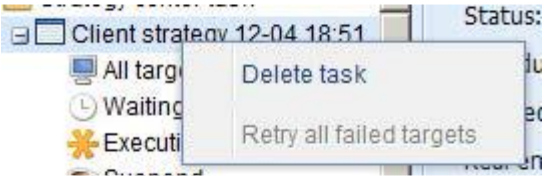
□	Client Alias	Client IP	Parent group name	Process	Detail
□	WIN-2TFCI3FOBGA	192.168.0.100	test1	Failure	Cancel the administrator

2. Retry the object

If the task is still in scheduling, the failed object can be immediately retried.

If the task has been scheduled, all failed objects can be rescheduled. As shown in following figure, right click on the finished task, select “retry failed object” and reschedule in the popup plan wizard.

Notice: as for retrying of failed object, only the failed object will be executed again, and no new task can be generated. The original task information will be covered.



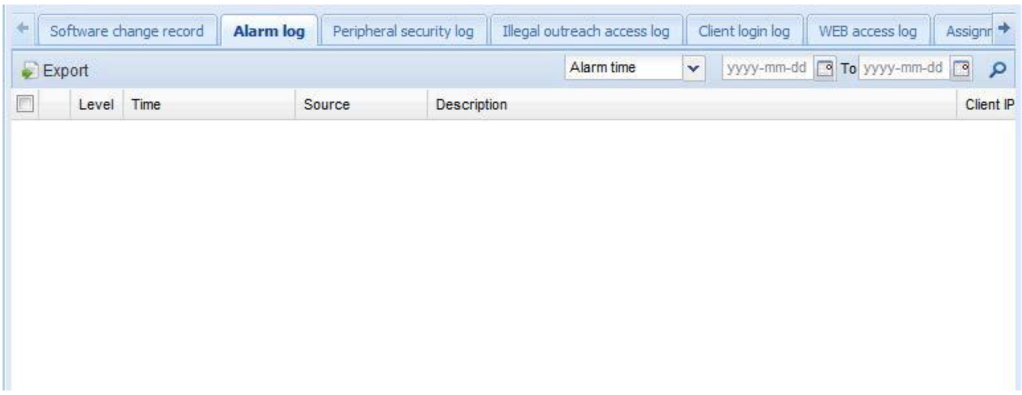
7. Audit Management

The “audit management” function generates administrator's operation logs, client login logs and the related logs of some functional modules. The administrator can query the information according to practical demand.

7.1 Client audit

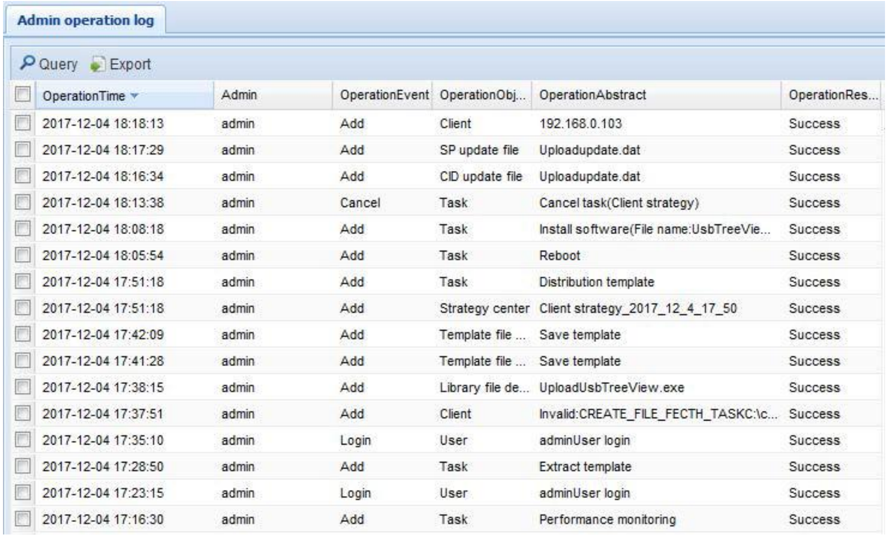
“Client audit” module audits the client’s behaviors, including client login logs, alarm logs, peripherals security logs, illegal outreach logs, software change records, Web security logs and outer operation logs.

- To view the log, user can use the query function to filter according to demand;
- When the user selects one client or one group from the client tree in the left side, the right side will display the audit logs of the selected object.



7.2 System log

“System log” mainly refers to the operation and change logs of system to realize the traceability of system operation.



	OperationTime	Admin	OperationEvent	OperationObj...	OperationAbstract	OperationRes...
□	2017-12-04 18:18:13	admin	Add	Client	192.168.0.103	Success
□	2017-12-04 18:17:29	admin	Add	SP update file	Uploadupdate.dat	Success
□	2017-12-04 18:16:34	admin	Add	CID update file	Uploadupdate.dat	Success
□	2017-12-04 18:13:38	admin	Cancel	Task	Cancel task(Client strategy)	Success
□	2017-12-04 18:08:18	admin	Add	Task	Install software(File name:UsbTreeVie...	Success
□	2017-12-04 18:05:54	admin	Add	Task	Reboot	Success
□	2017-12-04 17:51:18	admin	Add	Task	Distribution template	Success
□	2017-12-04 17:51:18	admin	Add	Strategy center	Client strategy_2017_12_4_17_50	Success
□	2017-12-04 17:42:09	admin	Add	Template file ...	Save template	Success
□	2017-12-04 17:41:28	admin	Add	Template file ...	Save template	Success
□	2017-12-04 17:38:15	admin	Add	Library file de...	UploadUsbTreeView.exe	Success
□	2017-12-04 17:37:51	admin	Add	Client	Invalid:CREATE_FILE_FECTH_TASKC:\c...	Success
□	2017-12-04 17:35:10	admin	Login	User	adminUser login	Success
□	2017-12-04 17:28:50	admin	Add	Task	Extract template	Success
□	2017-12-04 17:23:15	admin	Login	User	adminUser login	Success
□	2017-12-04 17:16:30	admin	Add	Task	Performance monitoring	Success

8. System Setting

8.1 User management

8.1.1 User management

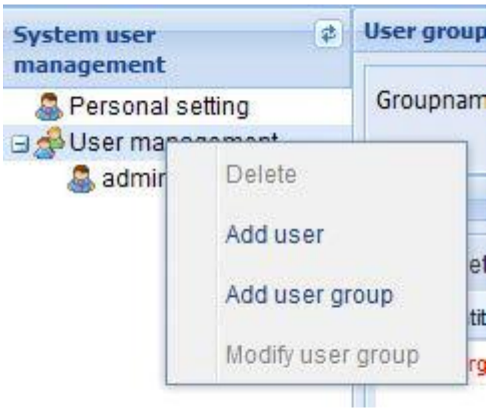
After installation of system, default username and password are admin and admin respectively. The administrator can configure the user/group, role and authority of role. Description about authority: the user authority can restrict the user to access to system functions. The user authority is the role authority.

Click “user management” to view the information of current group. The user in this group can be deleted. However, the super admin cannot be deleted.

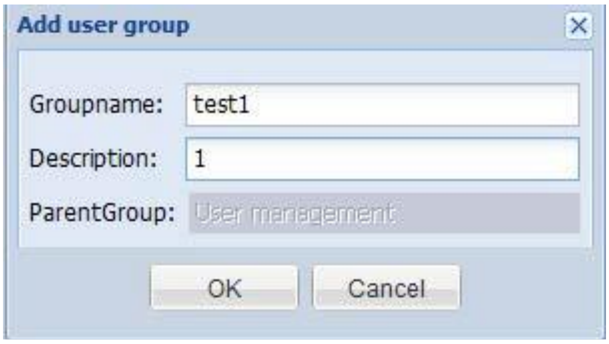
8.1.1.1 Add user group

The system doesn’t limit the number of groups. User can add infinite groups in cascade connection mode.

1. Right click on a group node in “user management” and select “add the user group” in the popup menu.



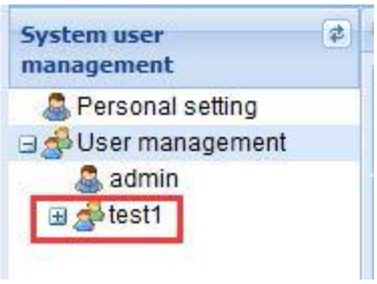
2. After editing, click “OK” button to finish the addition of user group.


Add user group

Groupname: test1

Description: 1

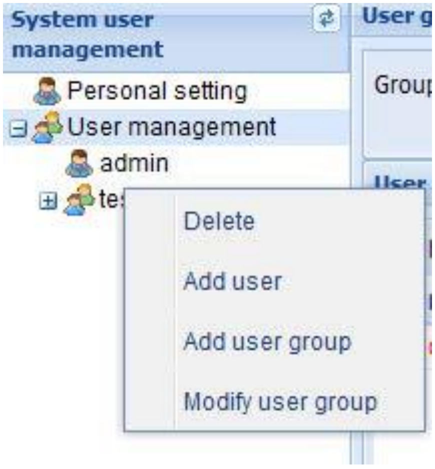
ParentGroup: User management



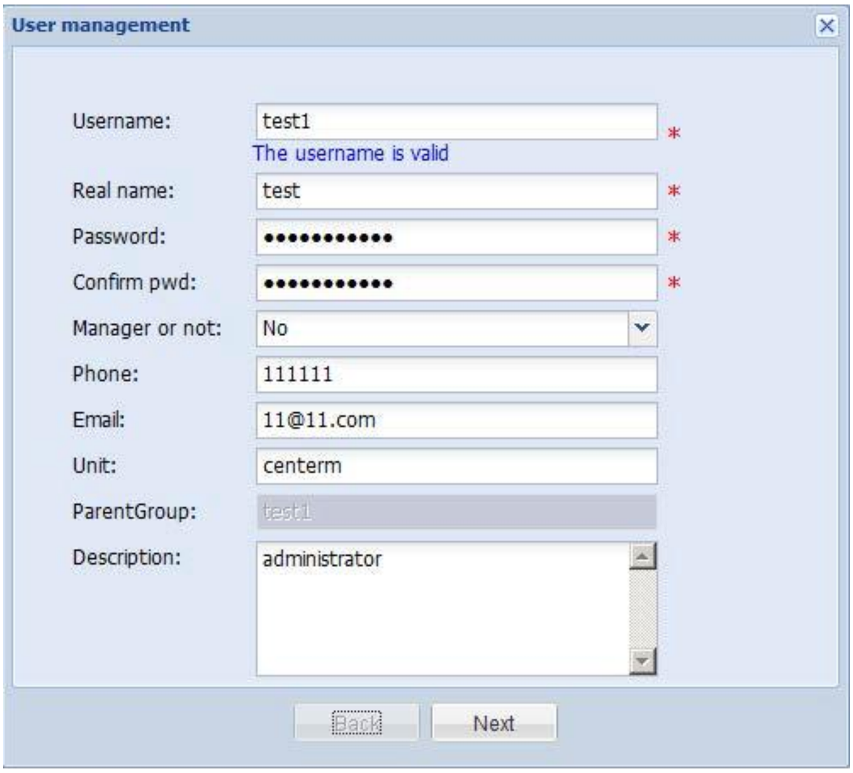
8.1.1.2 Add user

The system doesn’t limit the number of users. User can add infinite users.

1. Right click on a group node in “user management” and select “add the user” in the popup menu.



2. Fill in the basic information.



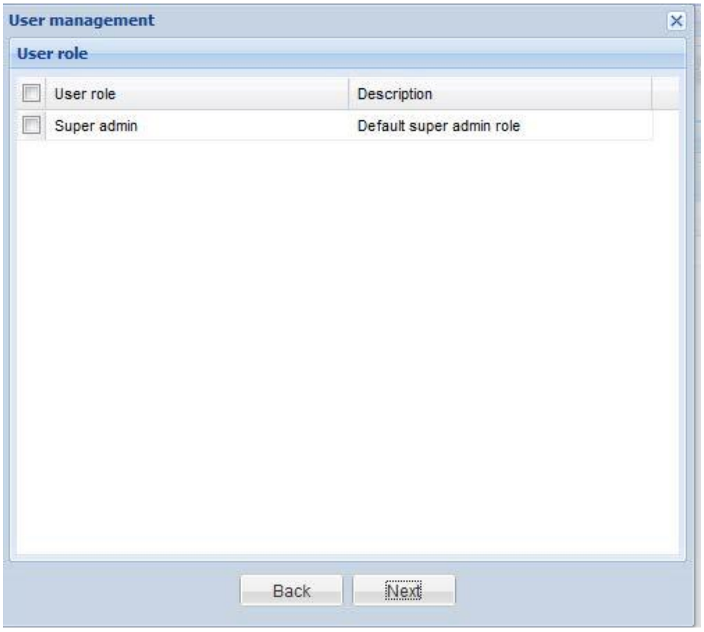
Username: test1 *
The username is valid
Real name: test *
Password: ●●●●●●●●●●● *
Confirm pwd: ●●●●●●●●●●● *
Manager or not: No
Phone: 111111
Email: 11@11.com
Unit: centerm
ParentGroup: test1
Description: administrator

Notice:

The principal refers to the administrator who has administration authority of the user group and can manage all users in the user group.

3. Distribute role

The user role is a set of authorities to restrict the user to access some functions of the system and to carry out some operations. See “role management” for details.



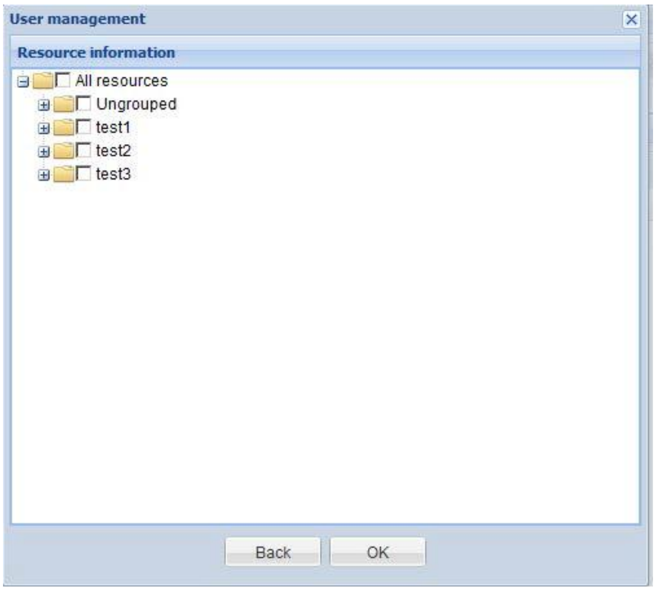
User management

User role

□ User role	Description
□ Super admin	Default super admin role

4. Distribute the client resources

Resources refer to the client resources which can be managed by user. After login, the user can only see the clients under his/her management.

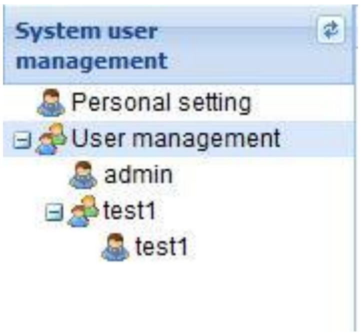


User management

Resource information

- □ All resources
  - □ Ungrouped
  - □ test1
  - □ test2
  - □ test3

Finally, click “OK” button, as shown in following figure.



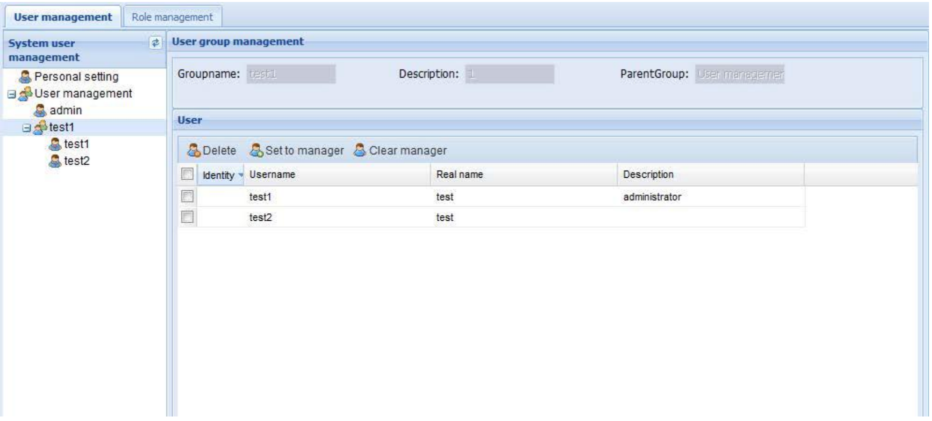
8.1.1.3 Principal

The principal refers to the administrator who has administration authority of the user group and can manage all users in the user group.

Only the principal can add, delete and change the group and users and can view and change all user information. Other persons only have the user authority for “individual setting”.

The administrator who is the principal can set or cancel the principal identity of other users.

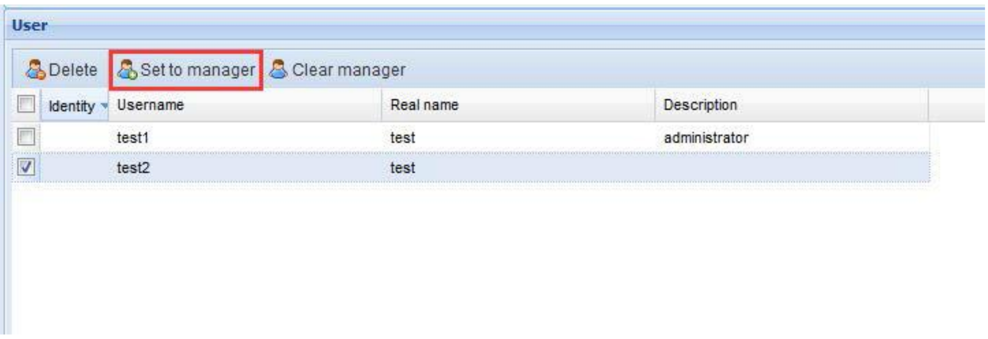
Select the user group and manage the principals of this group in the right list.



Groupname: test1 Description: 1 ParentGroup: User managemer

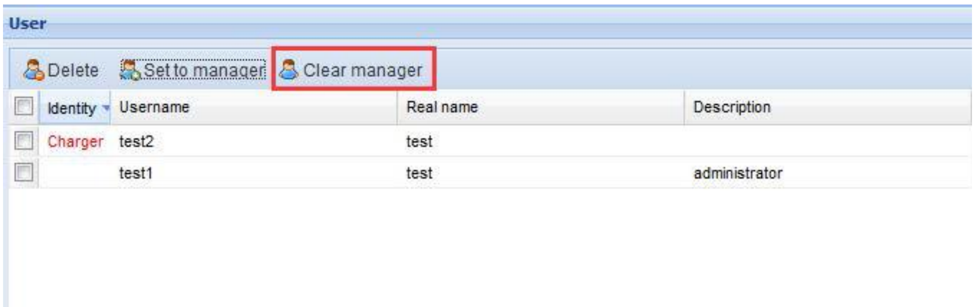
□	Identity	Username	Real name	Description
□		test1	test	administrator
□		test2	test	

Select the user and click “set as principal” to set the selected user as the principal.



□	Identity	Username	Real name	Description
□		test1	test	administrator
☑		test2	test	

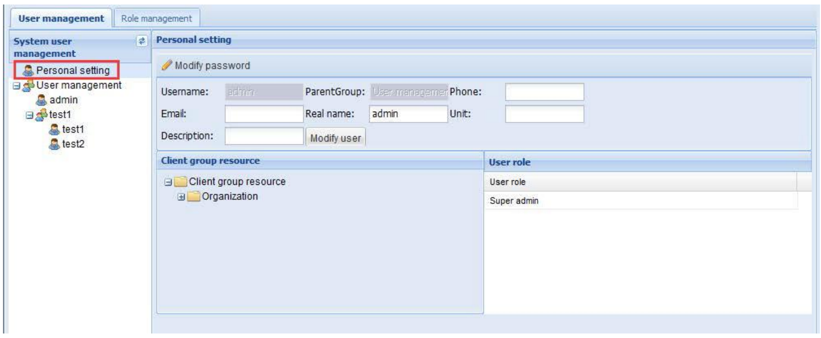
Select the user and click “remove the principal” to cancel the principal identity of the selected user.



□	Identity	Username	Real name	Description
□	Charger	test2	test	
□		test1	test	administrator

8.1.1.4 Individual setting

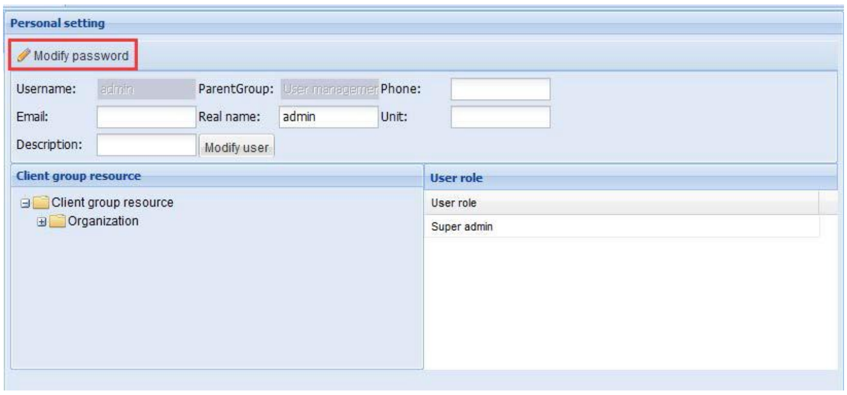
On “individual setting” panel, user can change his/her basic information, but cannot change the resource and role information (if the user is the principal, the user can change the resource information in management group).



Username: admin ParentGroup: User managemer Phone:
Email: Real name: admin Unit:
Description:

User role
Super admin

Change the individual password according to the following figure.



Username: admin ParentGroup: User manageme Phone:

Email: Real name: admin Unit:

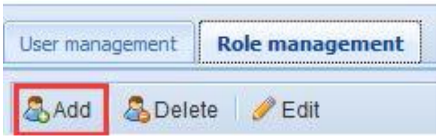
Description:

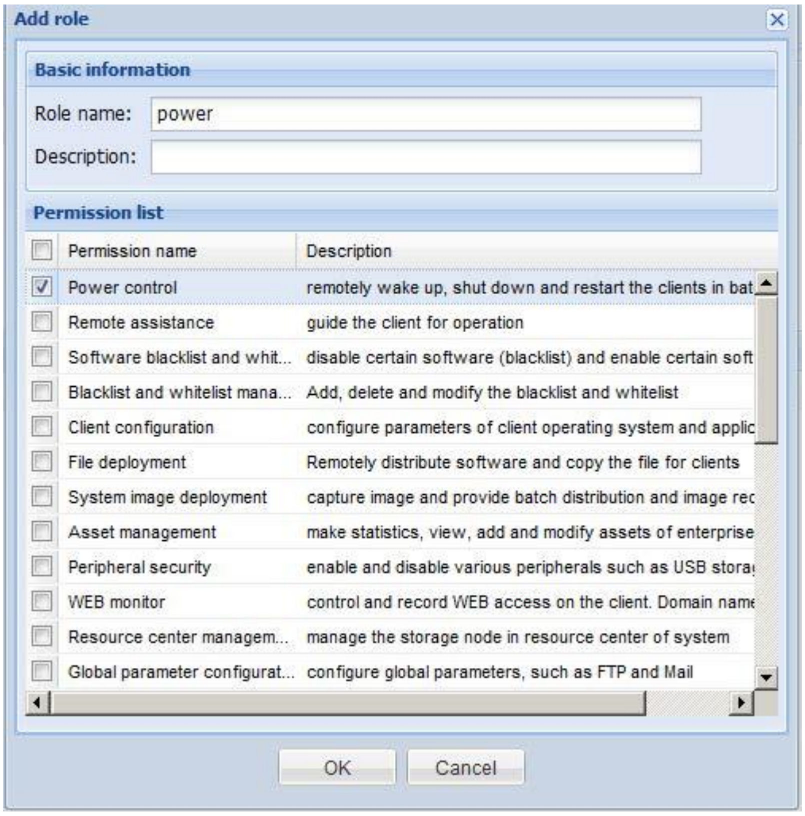
User role
Super admin

8.1.2 Role management

Role is the authority of user management system. The corresponding role can be set for an administrator based on the authority. The administrator can be assigned with one or more roles to facilitate the management division and authority division of the system. The adding method of role is as follows:

1. Click "add" button. Input "role name" and "description" in the popup window and select the corresponding "authority".



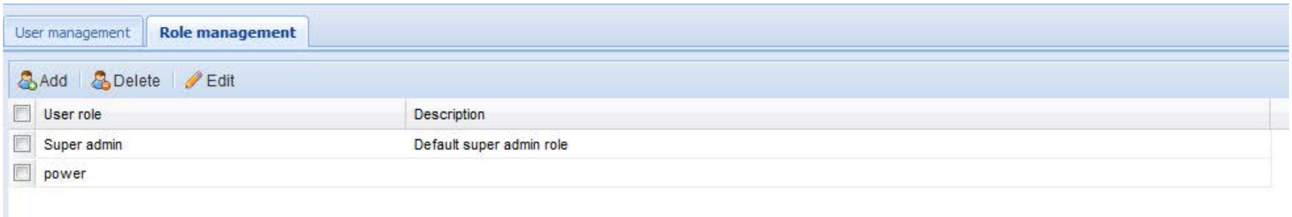


Role name: power

Description:

□	Permission name	Description
☑	Power control	remotely wake up, shut down and restart the clients in bat
□	Remote assistance	guide the client for operation
□	Software blacklist and whit...	disable certain software (blacklist) and enable certain soft
□	Blacklist and whitelist mana...	Add, delete and modify the blacklist and whitelist
□	Client configuration	configure parameters of client operating system and applic
□	File deployment	Remotely distribute software and copy the file for clients
□	System image deployment	capture image and provide batch distribution and image rec
□	Asset management	make statistics, view, add and modify assets of enterprise
□	Peripheral security	enable and disable various peripherals such as USB stora
□	WEB monitor	control and record WEB access on the client. Domain name
□	Resource center managem...	manage the storage node in resource center of system
□	Global parameter configurat...	configure global parameters, such as FTP and Mail

2. Then, the list will display the added role, as shown in following figure.



User role	Description
Super admin	Default super admin role
power	

8.2 Resource center

8.2.1 Brief introduction to resource center

1. What is a resource center?

A resource center is a gathering center of user management file resources, including deployment and management of storage nodes. Only the storage node is added in the resource center, relevant function of the system can be enabled. Therefore, it is necessary to add and bind the storage nodes before using.

2. What is a storage node?

When a user uses the client upgrade, file deployment and other functions, the system shall reserve some file resources for the user, so the storage node is the carrier for storing these file resources. At present, the storage node only supports CDS server (Centerm data server). The storage node can be managed and used only after being added in the resource center. In the deployment stage, the system shall rationally deploy the storage nodes according to the practical situation.

3. What is a bound storage node?

Binding refers to specifying the storage node as the nearest storage node of a client group. During executing file operation of this client group, the files can only be uploaded to or downloaded from the bound storage node. If the current group has no bound storage node, the bound storage node of the parent group shall be regarded as the nearest storage node.

The meaning of bound storage node is that the client can acquire the resource from the nearest storage node, which shortens the file transmission time and rationally divides the resources to avoid possible network congestion caused by acquiring resources from one storage node.

If one client group is bound with many storage nodes, it represents that the client group can acquire resources from these bound storage nodes to improve the transmission efficiency. If one storage node is bound with many client groups, it represents that many client groups share resources in one storage node.

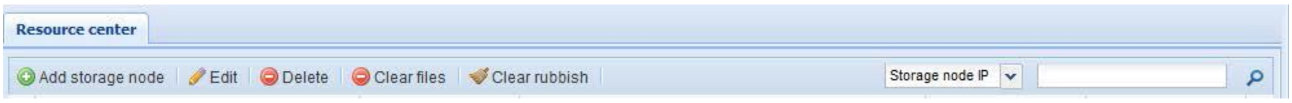
4. How to rationally bind the storage node?

Rational binding of storage node can accelerate the transmission speed of file resources and avoid the network congestion. In order to rationally bind the storage node, the administrator shall clearly know the distribution of current clients. Generally, the storage node bound with the client shall be closest in the geographic or network scope. We suggest the user setting up and binding the storage node in each geographic area and network area.

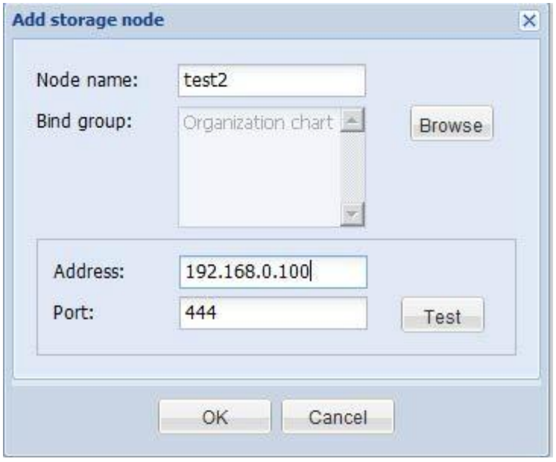
8.2.2 Add storage node

1. Firstly, set up CDS server in the host with large hard disk space and fast reading and writing speed.

2. Enter 【deployment management—>resource center】 module. In adding at the first time, click “add the storage node” button, as shown in following figure:



3. In the popup dialog box, fill in the name of storage node, bound client group and IP address. After filling, test whether the storage node can be normally communicated.



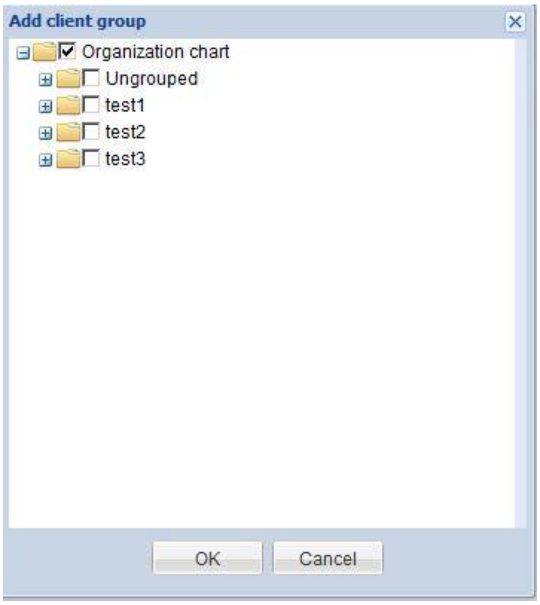
Node name: test2

Bind group: Organization chart

Address: 192.168.0.100

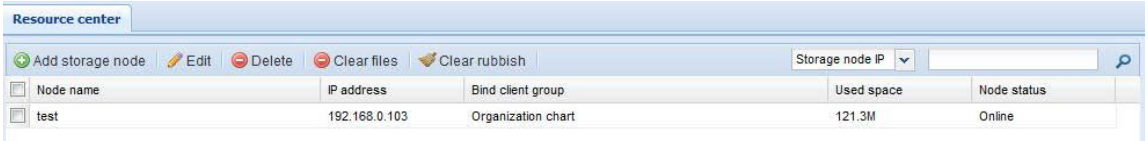
Port: 444

- Type of storage node: at present, only support CDS server;
- Bound client group: bind with client root group by default. Click “browse” button. Select other bound groups from the client group tree. The storage node can be bound with many groups, but cannot be bound with parent group and sub-group simultaneously. As shown in following figure, the storage node is bound with two groups.



- ☑ Organization chart
  - □ Ungrouped
  - □ test1
  - □ test2
  - □ test3

4. Click “OK” button. The list will display the added storage node.



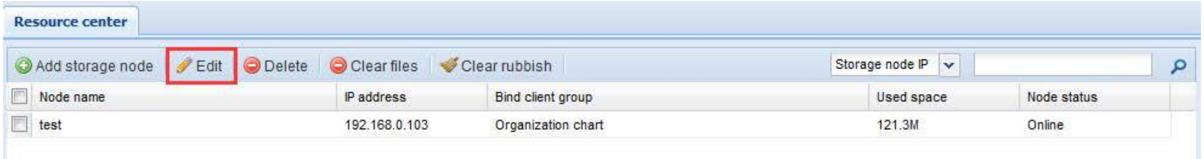
□	Node name	IP address	Bind client group	Used space	Node status
□	test	192.168.0.103	Organization chart	121.3M	Online

8.2.3 Change binding

When the location of storage node changes or the storage node is discarded, it is necessary to release or change the binding of storage node. Refer to following method:

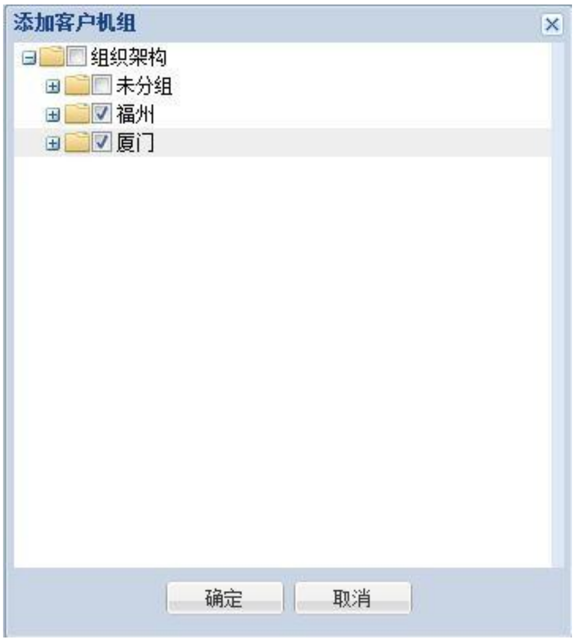
1. Change binding

The change binding is only applicable to single storage node. Click “edit storage node” button.



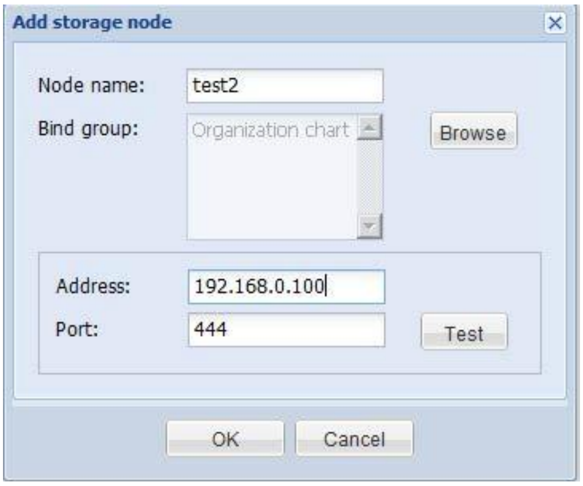
□	Node name	IP address	Bind client group	Used space	Node status
□	test	192.168.0.103	Organization chart	121.3M	Online

In the popup property dialog box, reselect the client group to be bound with the storage node.



添加客户机组

- ⊟ □ 组织架构
  - ⊞ □ 未分组
  - ⊞ ☑ 福州
  - ⊞ ☑ 厦门



Add storage node

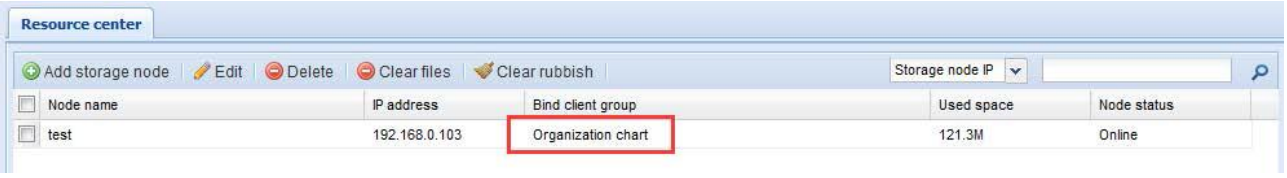
Node name: test2

Bind group: Organization chart

Address: 192.168.0.100

Port: 444

Click "OK". The interface displays that the group bound with the storage node has been changed.

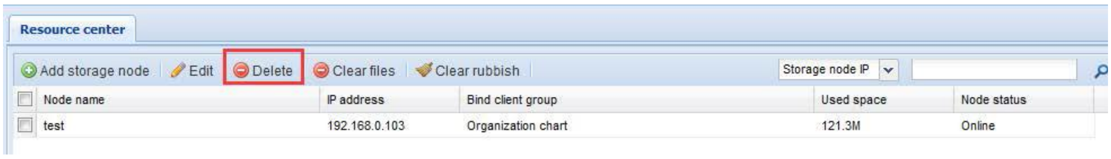


□	Node name	IP address	Bind client group	Used space	Node status
□	test	192.168.0.103	Organization chart	121.3M	Online

2. Delete node

After deleting a node, the binding relationship between the storage node and all client groups will be released, i.e. release of all using of the storage node by management server.

Operation step: select the storage node and click “delete” button.



☐	Node name	IP address	Bind client group	Used space	Node status
☐	test	192.168.0.103	Organization chart	121.3M	Online

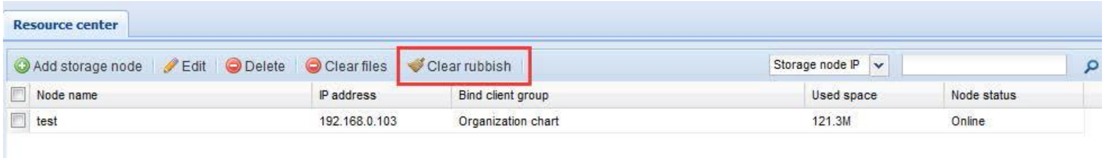
8.2.4 Clean storage node

After long term using of storage node, a lot of junk files will generate and the hard disk space will become small. User can clean the storage node by following method.

1. Clean junk files

Junk files are usually caused by file transfer interruption, storage node abnormality and other reasons. The “clean junk file” button in toolbar of the resource center can be clicked to clean the junk files of all storage nodes at one time. However, only administrator has such authority.

Notice: if the system is executing the file operation, don’t use this function. Otherwise, abnormality may occur.

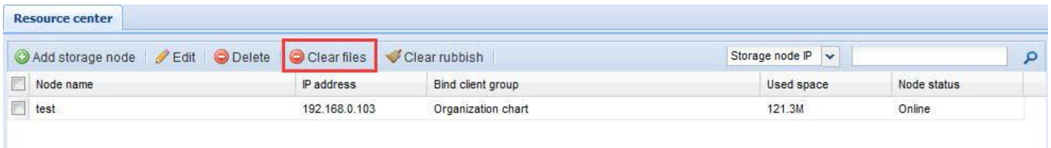


☐	Node name	IP address	Bind client group	Used space	Node status
☐	test	192.168.0.103	Organization chart	121.3M	Online

2. Empty files of storage node

If it is confirmed that the storage node has no important files, the storage node can be emptied to release space of the storage node. After emptying, all files in the storage node will be deleted. However, files saved by other users in FTP server will not be deleted.

Notice: if the system is executing the file operation, don’t use this function. Otherwise, abnormality may occur.



☐	Node name	IP address	Bind client group	Used space	Node status
☐	test	192.168.0.103	Organization chart	121.3M	Online

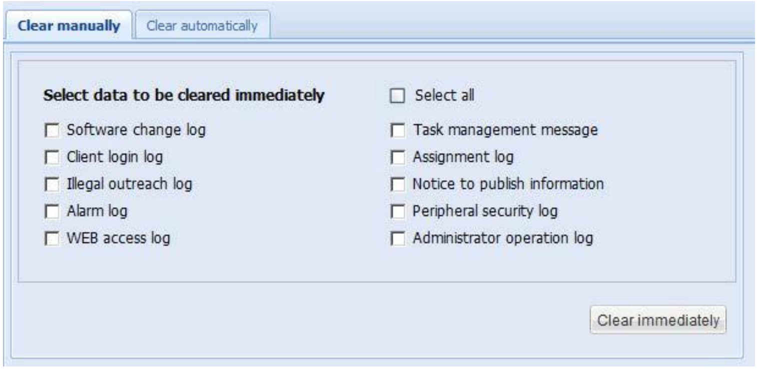
8.3 Data cleaning

After management system running for a certain period, the system will generate a lot of logs related to clients or system. The logs will occupy the storage space of server and may cause slow running of system. In order to solve this problem, the system has the data cleaning module. Therefore, the administrator can clean the running logs of the system conveniently.

8.3.1 Manual cleaning

The manual cleaning refers to that the administrator manually cleans data in the system.

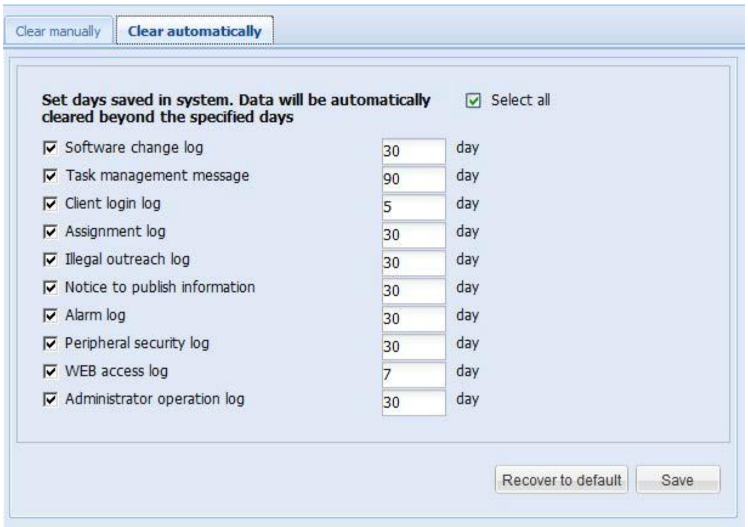
On the manual cleaning interface, select the type of data to be cleaned, and click “immediately clean” to clean all data with same type in the current system.



Select data to be cleared immediately

☐ Software change log
☐ Client login log
☐ Illegal outreach log
☐ Alarm log
☐ WEB access log

☐ Select all
☐ Task management message
☐ Assignment log
☐ Notice to publish information
☐ Peripheral security log
☐ Administrator operation log



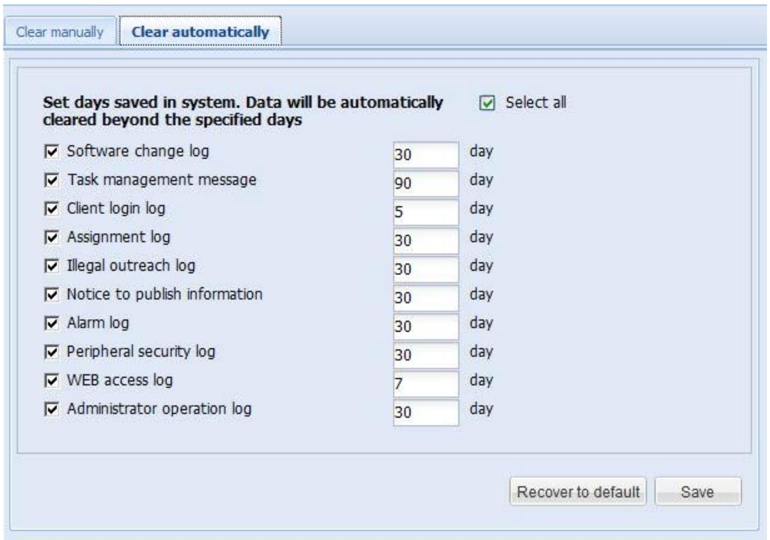
Set days saved in system. Data will be automatically cleared beyond the specified days ☑ Select all

☑ Software change log	30	day
☑ Task management message	90	day
☑ Client login log	5	day
☑ Assignment log	30	day
☑ Illegal outreach log	30	day
☑ Notice to publish information	30	day
☑ Alarm log	30	day
☑ Peripheral security log	30	day
☑ WEB access log	7	day
☑ Administrator operation log	30	day

8.3.2 Automatic cleaning

The automatic cleaning refers to automatic cleaning of data by system. By default, the automatic cleaning function is enabled to all types of data to automatically clean the operation data which are stored longer than the specified days.

If the administrator doesn’t want to automatically clean operation data with certain type, the administrator can cancel the corresponding check box. The system will not automatically clean the data with this type.



Set days saved in system. Data will be automatically cleared beyond the specified days ☑ Select all

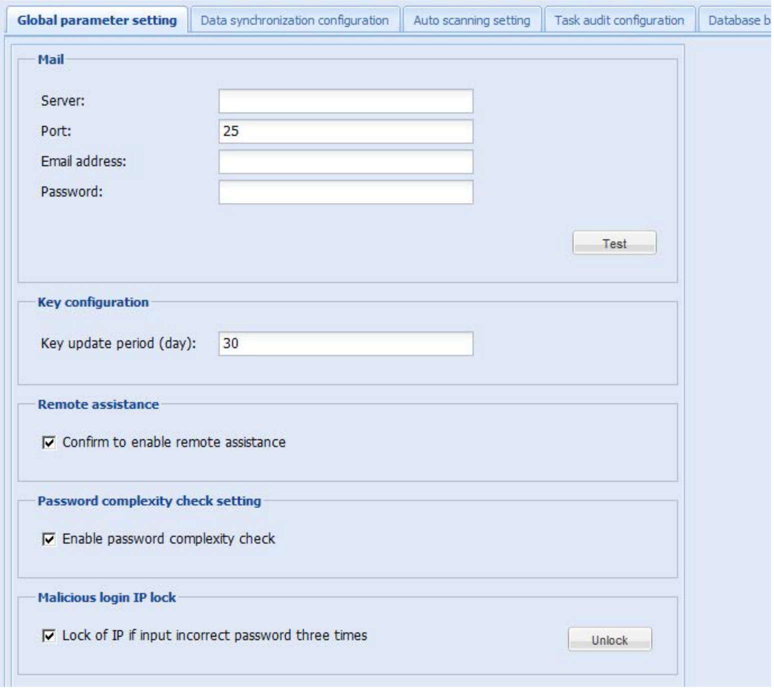
☑ Software change log	30	day
☑ Task management message	90	day
☑ Client login log	5	day
☑ Assignment log	30	day
☑ Illegal outreach log	30	day
☑ Notice to publish information	30	day
☑ Alarm log	30	day
☑ Peripheral security log	30	day
☑ WEB access log	7	day
☑ Administrator operation log	30	day

8.4 Global parameters

8.4.1 Global parameter setting

1. Mail parameter setting

On the global parameter page, the administrator can set the mail server for the system. When the system sends alarm information, the server will send the mail.



Mail

Server:

Port: 25

Email address:

Password:

Key configuration

Key update period (day): 30

Remote assistance

☑ Confirm to enable remote assistance

Password complexity check setting

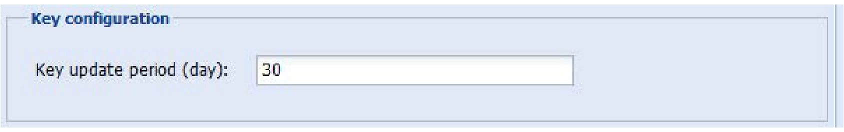
☑ Enable password complexity check

Malicious login IP lock

☑ Lock of IP if input incorrect password three times

2. Key update cycle

The key refers to the communication key between the server and the clients. The default update cycle is 30 days. The administrator can change the cycle according to demands.



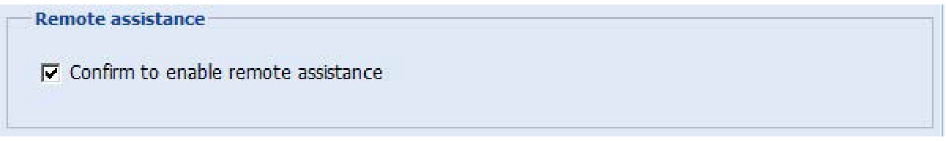
Key configuration

Key update period (day): 30

3. Remote assistance

The confirmation of remote assistance refers to the popup confirmation box in client when the server sends the remote assistance to the client. In other words, the server can realize the remote assistance only after confirming and accepting by the client.

The system enables the remote assistance confirmation by default. If the user selects cancel, the server can directly realize the remote assistance without confirmation by client.



Remote assistance

☑ Confirm to enable remote assistance

4. Password complexity check

The password complexity check refers to the limitation of complexity of administrator’s password. By default, the password complexity check is disabled. If the user enables the check, the password of system administrator shall include uppercase and lowercase letters, numbers and special symbols.

Password complexity check setting

☑ Enable password complexity check

5. Malicious login IP locking

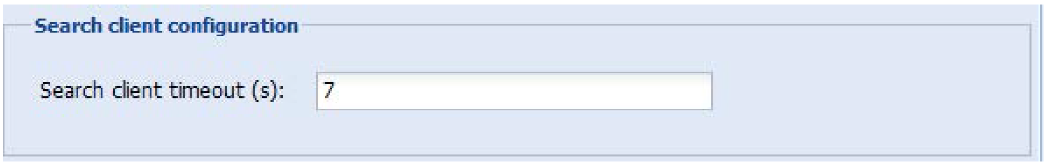
In order to prevent from cracking of system account, the system supports locking of IP which fails in login successively. Within one hour, the IP cannot log in. The function is enabled by default.

Malicious login IP lock

☑ Lock of IP if input incorrect password three times

6. Client search configuration

Configuration of client search timeout is for configuring the timeout of waiting for feedback information after the client sends the search command.


Search client configuration

Search client timeout (s): 7

7. Task configuration

Configure the default deadline of task. The task beyond the deadline will be terminated.

task configuration

Task default time(days): 7

8. File deployment configuration

Configure whether to refresh the file list after copying of distributed files for deployment and after software installation task.

file deployment configuration

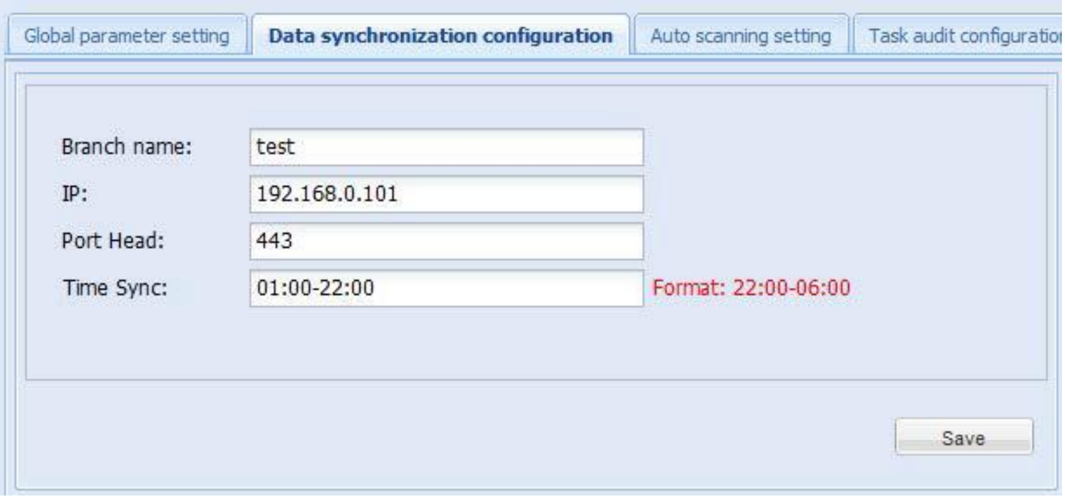
□ file deployment refresh check item

8.4.2 Data synchronization configuration

If an enterprise has the multi-level management structure, when the upper level wants to view the data of management structure at lower level, the enterprise can use the data synchronization configuration function of the management system.

During deploying the management system, the branch shall set up the complete Centerm desktop management system and the headquarters only needs to set up the management system of headquarters.

- Data synchronization interface of management system of branch:



Branch name: test

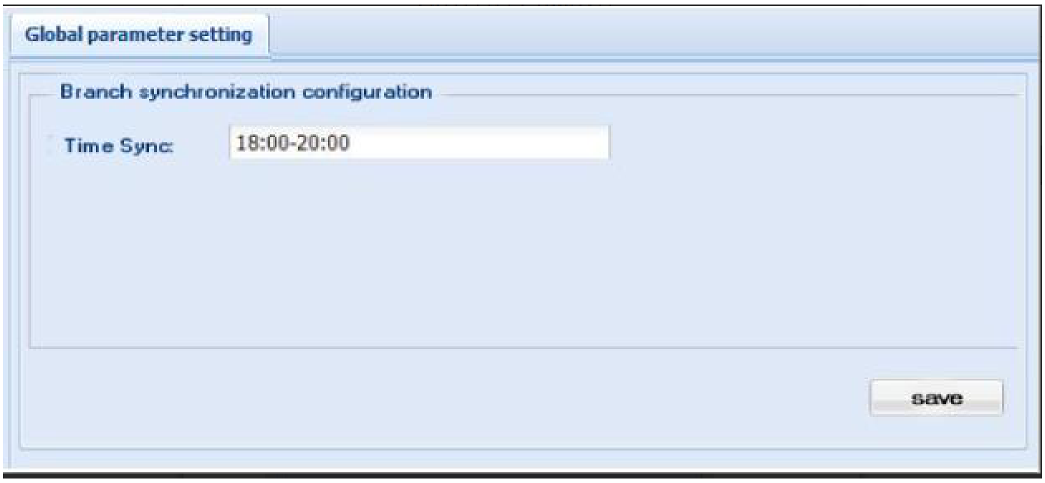
IP: 192.168.0.101

Port Head: 443

Time Sync: 01:00-22:00 Format: 22:00-06:00

The port No. is the WEB port No. of management system of headquarters.

- Data synchronization interface of management system of headquarters:



Time Sync 18:00-20:00

If the time of headquarters and branch isn't consistent, synchronization time of the headquarters shall prevail.

8.4.3 Automatic scan setting

Automatic scanning refers to that the system automatically scans the specified IP range. Within the range, if the management client has been installed and there is the unmanaged client, the client will be automatically added in the management.

Configured parameters are as follows:

- Next scanning time

Refer to the time of scanning the specified IP range next time;

- Scanning start time

Refer to the initial scanning time set by administrator. After setting the time, the scanning time will change to the set scanning start time;

- Scanning interval

Refer to the interval between two scanning behaviors;

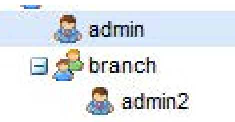
- Scanning IP range

Refer to the IP range scanned by the system. The system allows to setting many IP segments which shall not be overlapped.

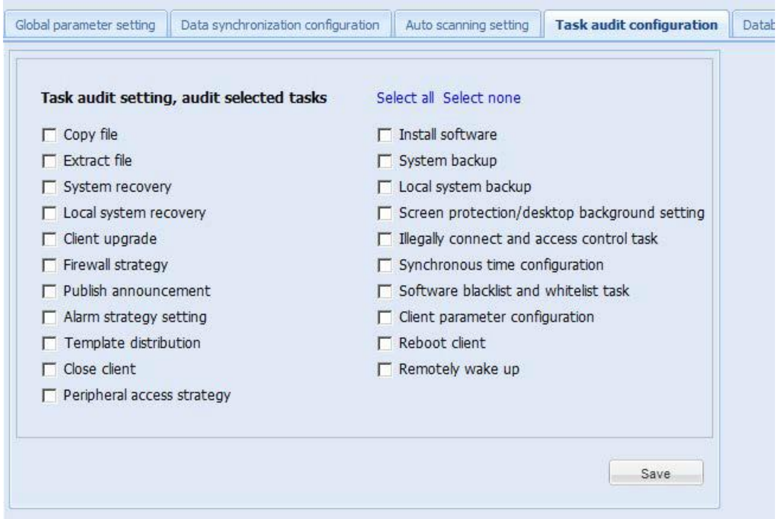
8.4.4 Task review configuration

When an enterprise needs to carry out leveled authority control for task execution, the enterprise can use the task review configuration function. The using steps are as follows:

1. In “system setting—>user management” module, the authorities can be divided by setting up the user group; as shown in following figure, admin1 is the superior administrator of admin2.



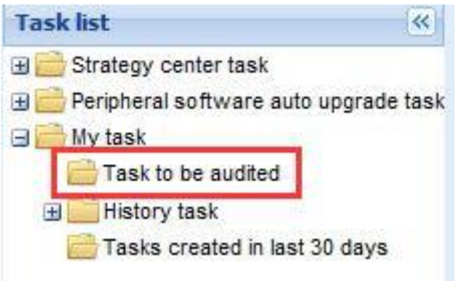
2. Log in system as the administrator. Enter “system setting—>global parameters”. Switch to “task review configuration” tab page. Select the task types to be reviewed. Click “save”.



Task audit setting, audit selected tasks

□ Copy file
□ Extract file
□ System recovery
□ Local system recovery
□ Client upgrade
□ Firewall strategy
□ Publish announcement
□ Alarm strategy setting
□ Template distribution
□ Close client
□ Peripheral access strategy
□ Install software
□ System backup
□ Local system backup
□ Screen protection/desktop background setting
□ Illegally connect and access control task
□ Synchronous time configuration
□ Software blacklist and whitelist task
□ Client parameter configuration
□ Reboot client
□ Remotely wake up

3. After setting, when the inferior administrator creates the notice publish task, only after approval of the superior administrator, the task can be executed; the superior administrator can view the tasks to be reviewed in “tasks to be reviewed” node in “task management” module.

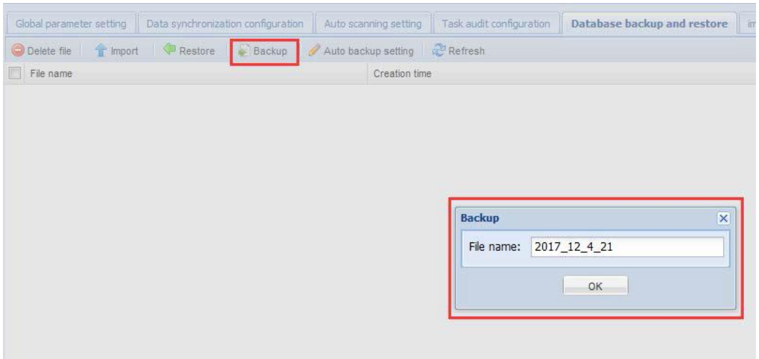

Task list
Strategy center task
Peripheral software auto upgrade task
My task
Task to be audited
History task
Tasks created in last 30 days

8.4.5 Database backup and restore

The database backup and restore page provides the database backup and restore function of server. Automatic backup is supported.

8.4.5.1 Backup

Click “backup” button to backup the server database.



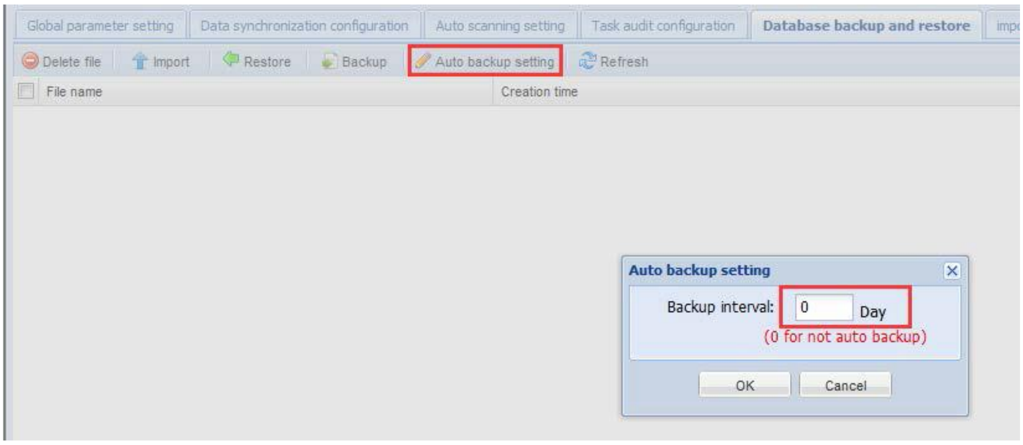
File name: 2017_12_4_21

8.4.5.2 Restore

Select the database record which has been backed up and click “restore” to restore the server database.

8.4.5.3 Automatic backup

If the interval of automatic backup is configured, the system will automatically backup the database.

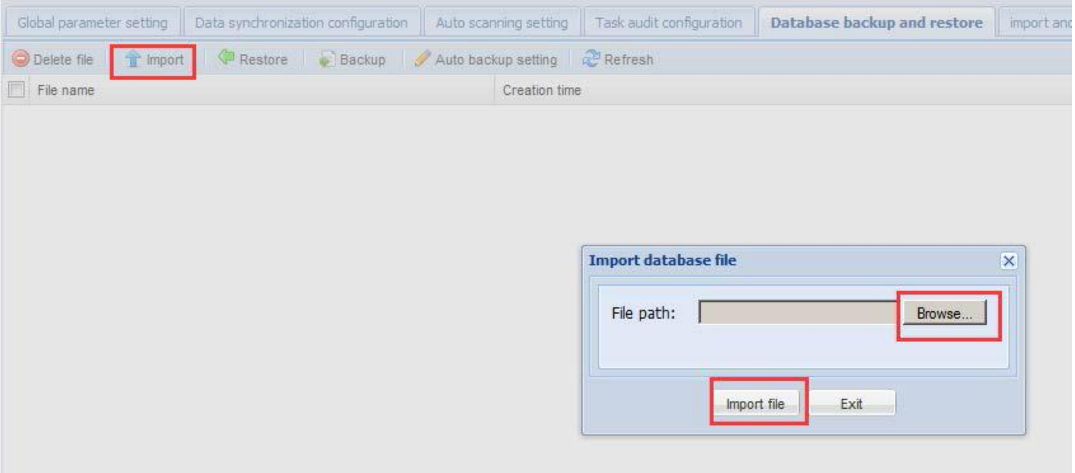


Backup interval: 0 Day

(0 for not auto backup)

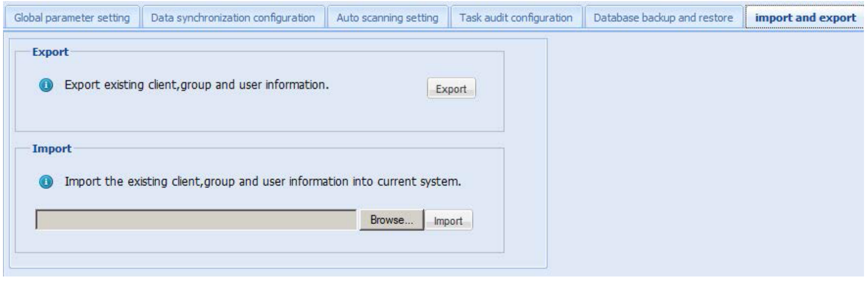
8.4.5.4 Import

Import the local database backup files



8.4.6 Import and export of organization structure

The system has the function to import and export client, group and user information managed by the system to facilitate the migration of organizational structure.



Export

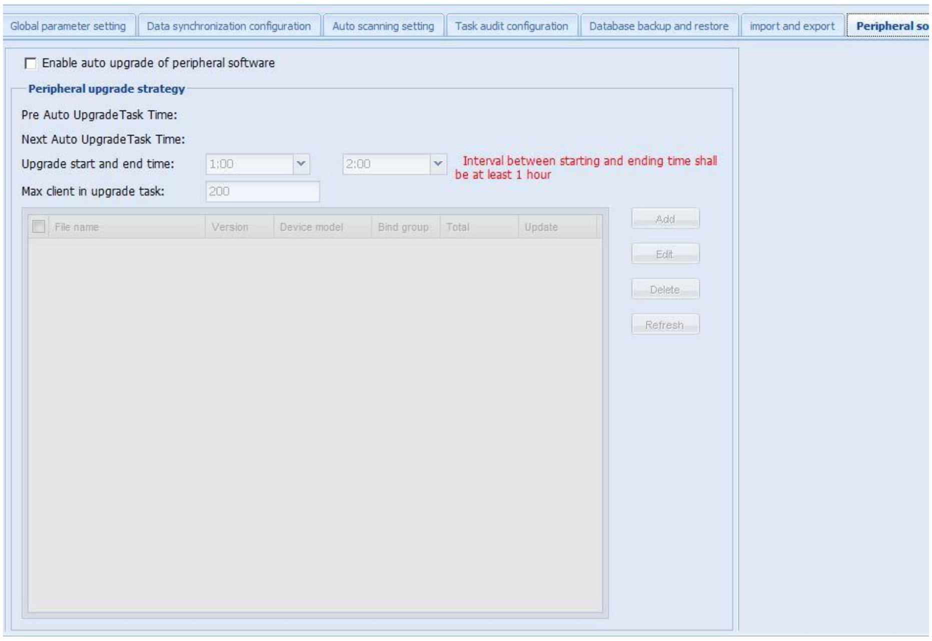
Export existing client,group and user information.

Import

Import the existing client,group and user information into current system.

8.4.7 Automatic upgrade of peripheral software

The system has the strategy configuration of automatic upgrade of software version of peripherals managed by the system to facilitate the deployment and upgrade operation of user.



☐ Enable auto upgrade of peripheral software

Peripheral upgrade strategy

Pre Auto UpgradeTask Time:

Next Auto UpgradeTask Time:

Upgrade start and end time: 1:00 2:00 Interval between starting and ending time shall be at least 1 hour

Max client in upgrade task: 200

☐	File name	Version	Device model	Bind group	Total	Update

9. Frequently Asked Questions

If you want more help, please visit http://www.centerm.com, call our headquarters: 86-591-28053888 or send email to strjzc@centerm.com.cn to contact our technical support department. Furthermore, you can consult our regional business person who will satisfy your demand by utilizing our resources.

FAQ

1. Why the default group of client tree is messy code after installation?

Reason: it is caused by manually adding the environment variableLANG=POSIX after installation of OS. Delete the variable and reestablish the database to solve the problem.

2. Why the storage node (file server) cannot be added?

Possible reasons:

- The firewall shields the service port.
- The data server isn't installed.
- The default port 9999 is occupied by other program, so the service cannot start.

3. Why no client is found?

- Firstly, please confirm whether the network between computer which will is installed with server software and the client is disconnected (detect whether the TCP8000 port and UDP8000 port of client are open by the port detection tool, such as nmap).
- Secondly, confirm whether the IP address of network card in client conflicts with IP address of other clients. If the network card of client is DHCP, please confirm whether the DHCP server assigns non-conflicted and normal IP address to the client (whether ping can respond gateway of ICMPprotocol instruction or IP address or domain name of server).
- Check whether the service program named as “UniFrame” is in “running” state. If not, start the service and set the running mode of the service as “automatic running”. If the UniFrame service cannot be started, please check whether these services are set as “disabled” state by the system or the third party antivirus software: DNSclient, RemoteProcedureCall (RPC), DHCPclient and TerminalServices.

4. Why the searched client cannot be managed?

- Firstly, check whether the searched client is managed by other servers (check whether the “management server” on search interface is blank). Only the unmanaged client can be managed.

- Secondly, confirm whether your management system is beyond the deadline. When software is beyond the authorization deadline, the system cannot add the new client for management.

5. Why the remote assistance function fails?

- When the monitoring system starts first time, the monitoring system will detect whether JRE is installed based on browser environment of the user. If not, the system will pop up a prompt box, please manually download and install JRE and then restart the browser.
- If Firefox browser is used and the agent server is ISA2000, during monitoring, the Firefox browser may be halted, resulting in failure of monitoring. Please download and install JRE1.5 or use IE browser for monitoring.
- If the monitoring function is normal previously and at present, the screen is white or black, please close the remote assistance window and click "remote assistance" again. If the monitoring is still in failure, close the browser and retry.
- If the client with high resolution enables the remote desktop service, one user connects with the client by RDP and the management tool is used for remote assistance, VNC crash may be caused. Please restart the VNC service.

6. Why a file isn't in the client when the file copy task is successful?

- Please confirm whether the whole path is correctly filled in during adding task, including both the target directory and the file name.

7. Why a task is always in "wait for executing" state?

- Whether the specified plan time expires?
- Whether the client starts?
- Whether the client is managed by the server?
- Whether the client displayed on the client management interface is online?
- Whether the data source is valid? View the system data source in ODBC. Whether it is valid during attempted configuration test?

8. Why the task plan information panel displays that the task is failed, but in fact, the task is successfully executed?

- The IP address of server is changed, but UnitedWeb service isn't restarted. Solution: restart UnitedWeb service or directly restart the server.

9. Why the file tasks always fail?

- The firewall or anti-virus software blocks download of file. Solution: disable the firewall or anti-virus software.
- The target client doesn't support the task. The task management interface displays the detailed execution results. If the result shows that the target client doesn't support the task, the task is be doomed to failure.

10. Why the client isn't wakened when the WoL task is successful?

- Because when the client is shut down and client agent doesn't start, the system regards that the WoL task is successful once the WoL message is sent.

The possible reasons are:

- The client doesn't support WoL (the hardware doesn't support).
- The management server and the client to be wakened aren't in the same network segment.
- The network of client has virtual subnet.

11. Whether the user is logged out during logging in system?

- Whether there is the administrator with the same name?
- Whether the Cookie is allowed in FireFox? If the Cookieisn't allowed, the user cannot log in the system.
- After logging in the system, if the period without operation is more than 10 minutes, the system will automatically execute the logout operation.

12. Why the browserdoesn't act during uploading the file?

- The jre version shall be jre-6u16 or higher version.

13. Why it is failed to add printer in XPe/XP?

- If the printer name includes the symbol @ and the printer is added first time, the addition will be failed. Delete @. Alternatively add the printer with this type and without @ firstly and then add the printer with @.

14. How the user can change the default printer settings in terminal mode?

In the terminal mode, the user cannot change the printer settings. If the user needs to change the default printer, adopt the following method:

Add a publish application program for the user:

Program path C:\windows\rundll32.exe

Parameter: SHELL32.DLL,SHHelpShortcuts_RunDLLPrintersFolder

If the management server is available, add a publish application program for the user in basic management->system configuration->client parameter configuration->user and group.

If the management server isn't available, import the following registry entry:

```
Windows Registry Editor Version5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Centerm\CSC100\Users\User\Applications\APP_printer and fax]

"Name"="printer and fax"

"FullPath"="C:\\WINDOWS\\system32\\rundll32.exe"

"AppType"=dword:00000001

"Description"=""

"Startup"=dword:00000000
```

```
"IconPath"=""
"WorkingPath"=""
"Parameter"="SHELL32.DLL,SHHelpShortcuts_RunDLLPrintersFolder"
"DesktopLink"="C:\\Documents andSettings\\User\\desktop\\printer and fax.lnk"
```

15. Whether the offline upgrade of client is supported?

The system adopts the task scheduling mechanism. As for offline client, the upgrade will be automatically deployed after start next time.

16. Why the configuration can take effect only after clicking “apply” button?

The command sent by the system is executed as the task. The configuration process only realizes the selection of option and will not apply on the client. Clicking “apply” button refers to that the user wants to execute the configured tasks. So, the system will apply the configuration in the client.

17. If the client is installed with anti-virus software, which ports and processes of client shall be added in the trust exceptions of anti-virus software?

Port list: 8000(UDP and TCP) and 8001(TCP)

Process list:

UniFrm2.exe,	C:\ProgramFiles\UniFrame3\UniFrm2.exe by default
UniUpdateService.exe,	C:\ProgramFiles\UniFrame3\UniUpdateService.exe by default
ConfEnv2.exe,	C:\ProgramFiles\UniFrame3\ConfEnv2.exe by default
UdiskTray.exe,	C:\ProgramFiles\UniFrame3\UdiskTray.exe by default