
CDMS 7.0 User Manual

Centerm Information Co., Ltd.

CentermTM

Index

Index.....	1
1. Quick start.....	2
1.1 Enter to system.....	2
1.2 Device Management.....	4
2. Device and group.....	6
2.1 Group.....	6
2.1.1 Group classification.....	6
2.1.2 Add customized group.....	7
2.1.3 Add search Group.....	7
2.1.4 Add personal group.....	9
2.1 Device management.....	10
2.2 Search client.....	10
2.2.1 Modify client.....	11
2.2.2 Delete client.....	12
2.2.3 Move lclient.....	12
3Client Management.....	13
3.1 Windows client configuration.....	13
3.1.1 Windows client parameter configuration.....	13
3.2 Linux client settings.....	41
3.2.1 Linux client specification settings.....	41
3.3 Power control.....	50
3.3.1 Control type.....	50
3.3.2 Control option.....	50
3.4 Remote assistance.....	53
3.4.1 Request processing.....	56
3.5 Notice publishing.....	57
3.5.1 Publish notice.....	57
3.5.2 View the publishing result.....	59
3.6 File deployment.....	62
3.6.1 Windows file deployment management.....	62
3.6.2 Linux Patch Update.....	68
3.6.3 Linux System update.....	72
3.6.4 Linux log.....	74
3.7 Client upgrade.....	75
3.7.2 System backup.....	77
3.7.3 System restore.....	79
3.8 Peripheral Security.....	82
3.8.1 Restriction to device type.....	82
3.8.2 Restriction to device interface.....	83
3.9 Windows vulnerability fixing.....	84
3.9.1 Patch library management.....	84
3.10 Software blacklist and whitelist.....	86
3.10.1 Blacklist and whitelist management.....	86
3.10.2 Blacklist and whitelist strategy.....	91
3.10.3 Process control.....	94
3.11 Template management.....	95
3.11.1 Windows/Linux.....	95
3.11.2 Strategy center.....	105
3.12 Printer whitelist.....	106
3.13 Terminal IP trace.....	107
3.14 Directory security.....	108
3.14.1 Add the directory security.....	109
3.14.2 Folder secure policy edit.....	109

3.14.3	Delete folder secure policy	110
3.14.4	Folder secure policy distribution	111
3.15	Log on by IC card.....	112
3.15.1	User management for logon.....	112
3.15.2	User enable/disable.....	113
4.	System settings.....	114
4.1	User management.....	114
4.1.1	User management.....	114
4.1.2	Role management	125
4.2	Resource center	126
4.2.1	Introduction	126
4.2.2	Add storage node	127
4.2.3	Binding changes	129
4.2.4	Clean storage node	130
4.3	Data cleaning.....	131
4.3.1	Manual cleaning	131
4.3.2	Automatic cleaning	131
4.4	Global parameters.....	133
4.4.1	Global parameter settings	133
4.4.2	Database backup and restore.....	138
4.4.3	Organization structure import and export.....	139
4.4.4	Peripheral firmware upgrade.....	139

1. Quick start

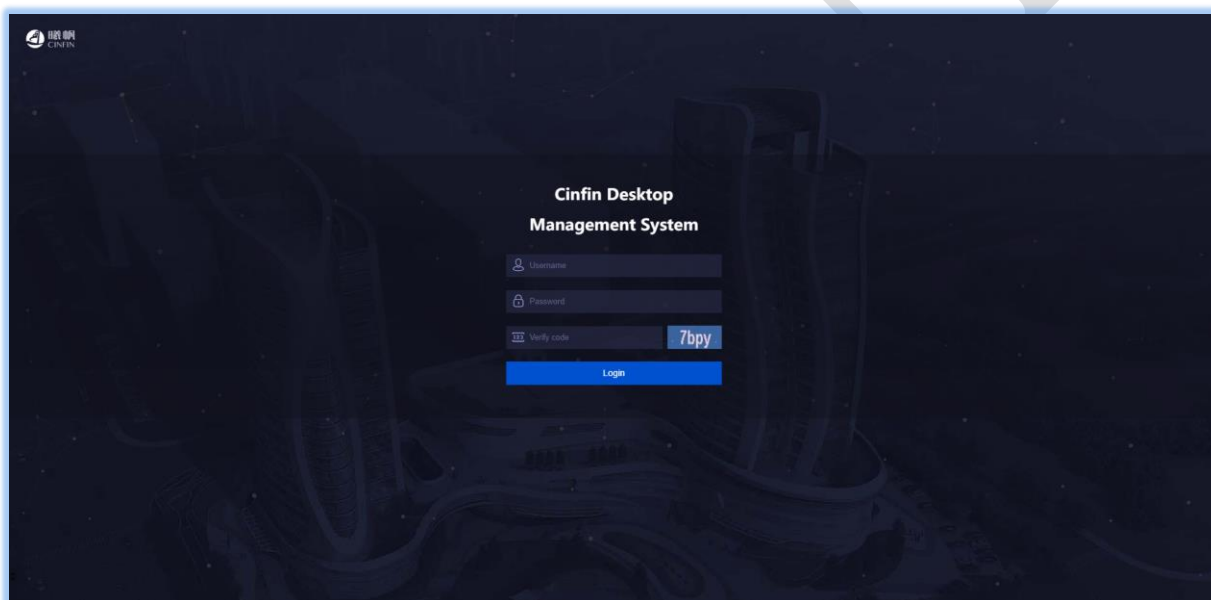
1.1 Enter to system

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

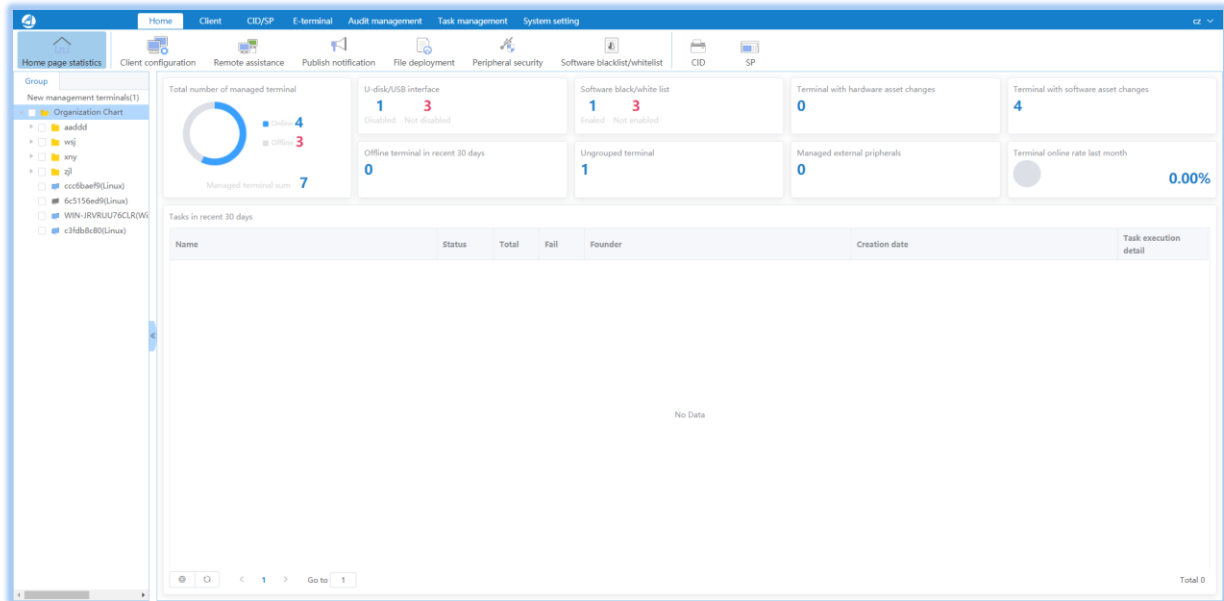
1. Open the browser and input the management server IP and the using port in address bar, as shown in following figure. Notice: the address prefix is “https://”.

`https://192.168.106.181/terminal/login`

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.

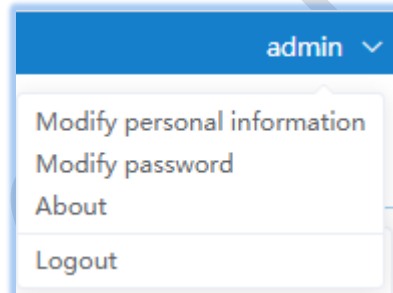


3. At the first time of login, change the password to ensure security. After correct login, main interface of the system is shown in following figure:

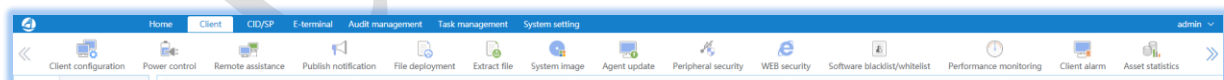


The main interface shows the statistical charts, the detailed information of chart and the last 30 failed tasks of system management device. On the interface, the statistics types include client, SP, CID and MTerminal. Client statistics includes general terminal and Mobile Terminal (because Mobile Terminal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

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



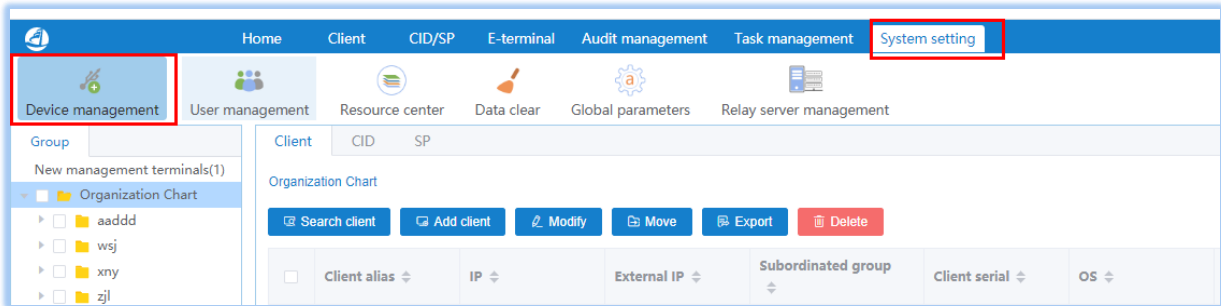
The icons on the navigation bar will classify all functions of the system. The administrator can enter the corresponding functional module for operation by selecting the menu option.



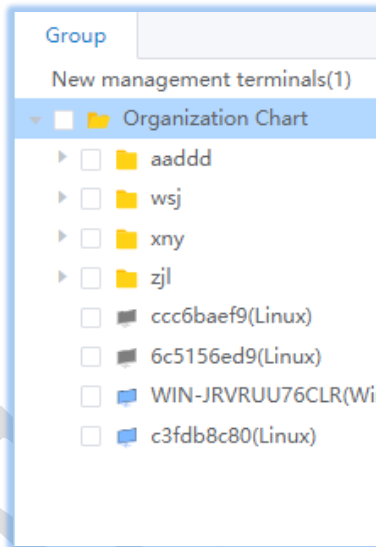
Memo: CDMS supports browser including IE10, 11, Chrome (later than v66 preferred), Firefox (later than v68 preferred)

1.2 Device Management

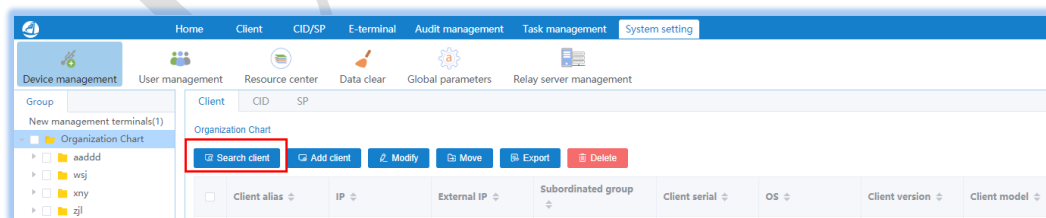
1. Enter the device management module.



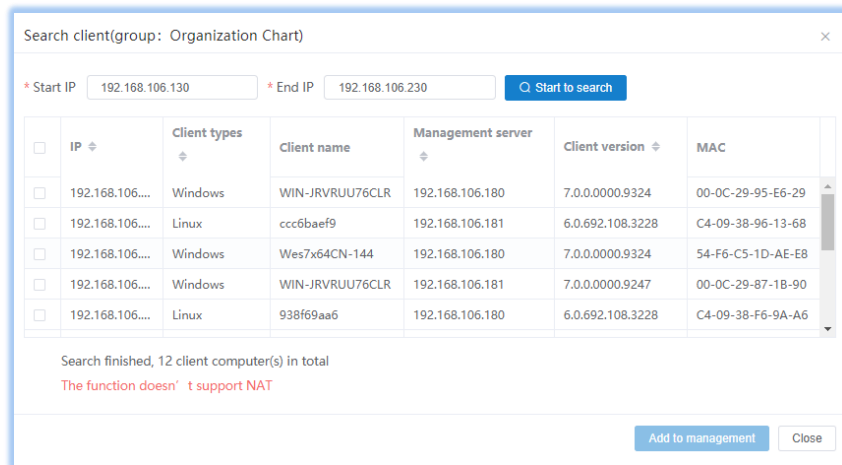
2. Create the organization structure of enterprise in the left grouping tree.



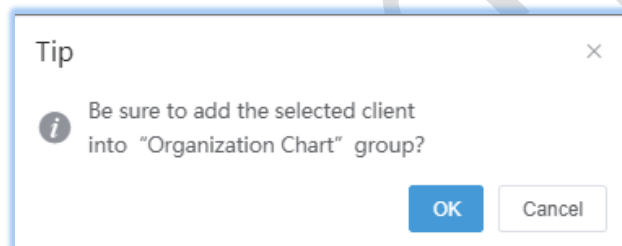
3. Select the grouping of device to be added and click the "search client" button on the right panel.



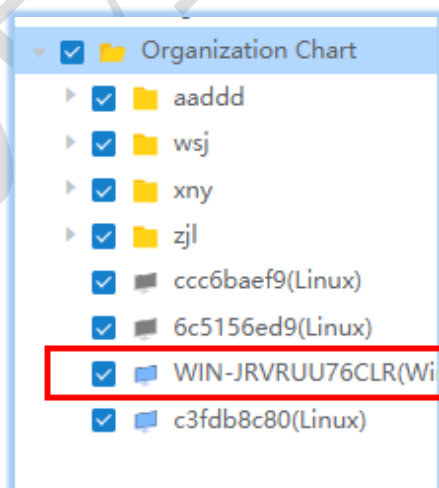
4.Fill in the searched IP range on the popup panel and click the “start search” button.



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



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.



2. Device and group

2.1 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.

2.1.1 Group classification

The system has 3 types of groups in total:

- New group

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.

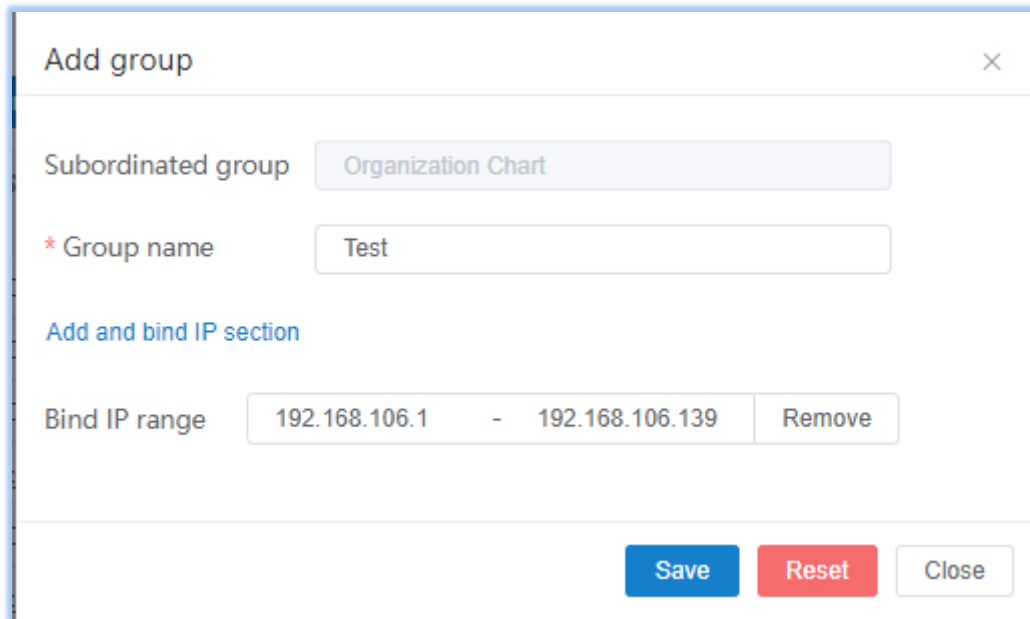
- Search group

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.

2.1.2 Add customized 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”.

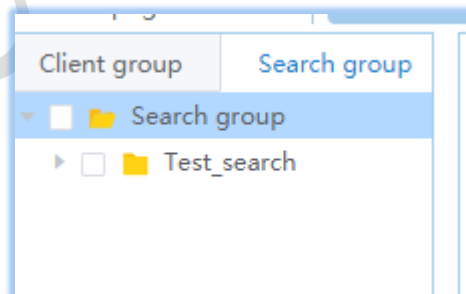
(The bound IP only can be managed clients in specified IP)



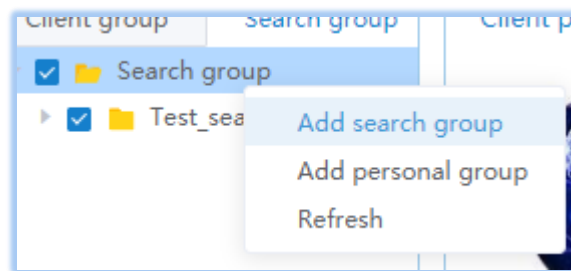
2.1.3 Add search Group

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

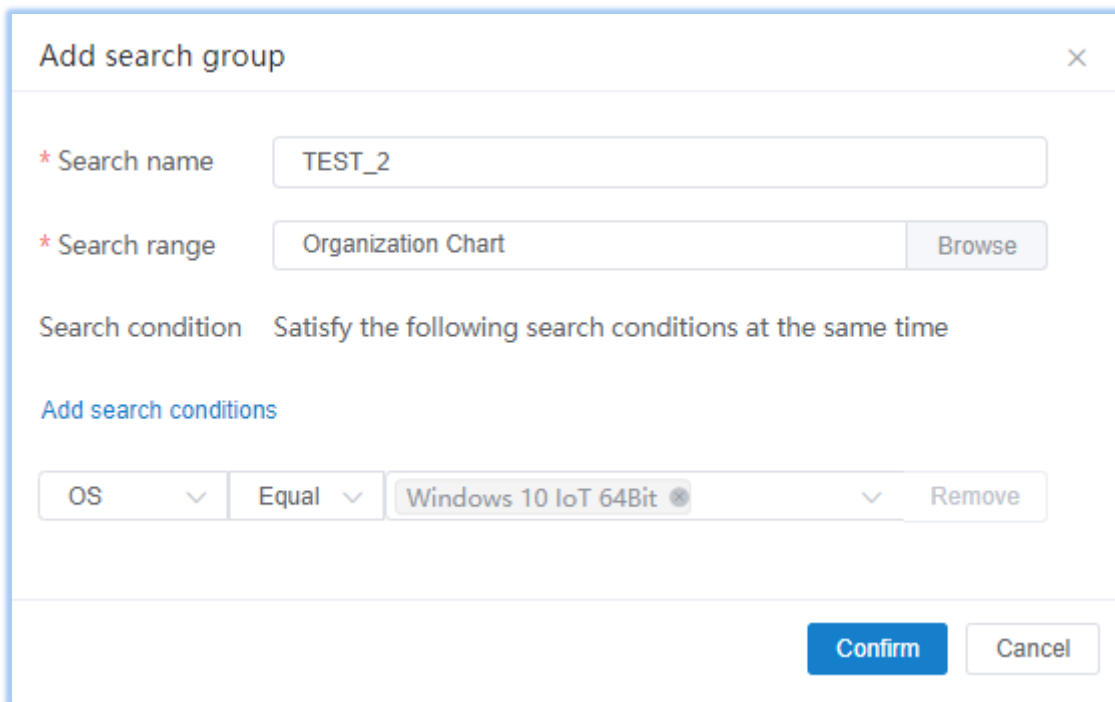
1. Enter any management module in “client management” submenu to display “search group” tab page on left panel;



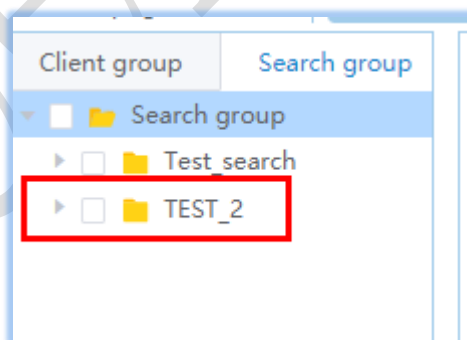
2. Click to enter the “search group” tab page, right click on root node and select the “add search group”;



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



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

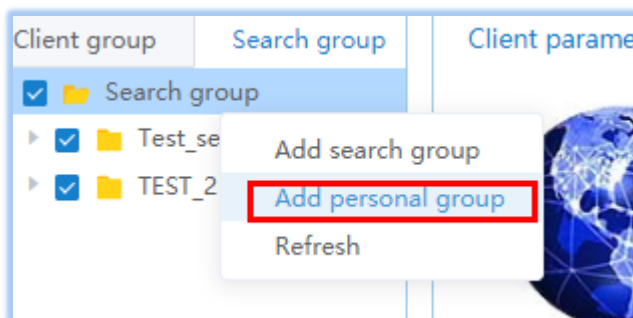


Notice:

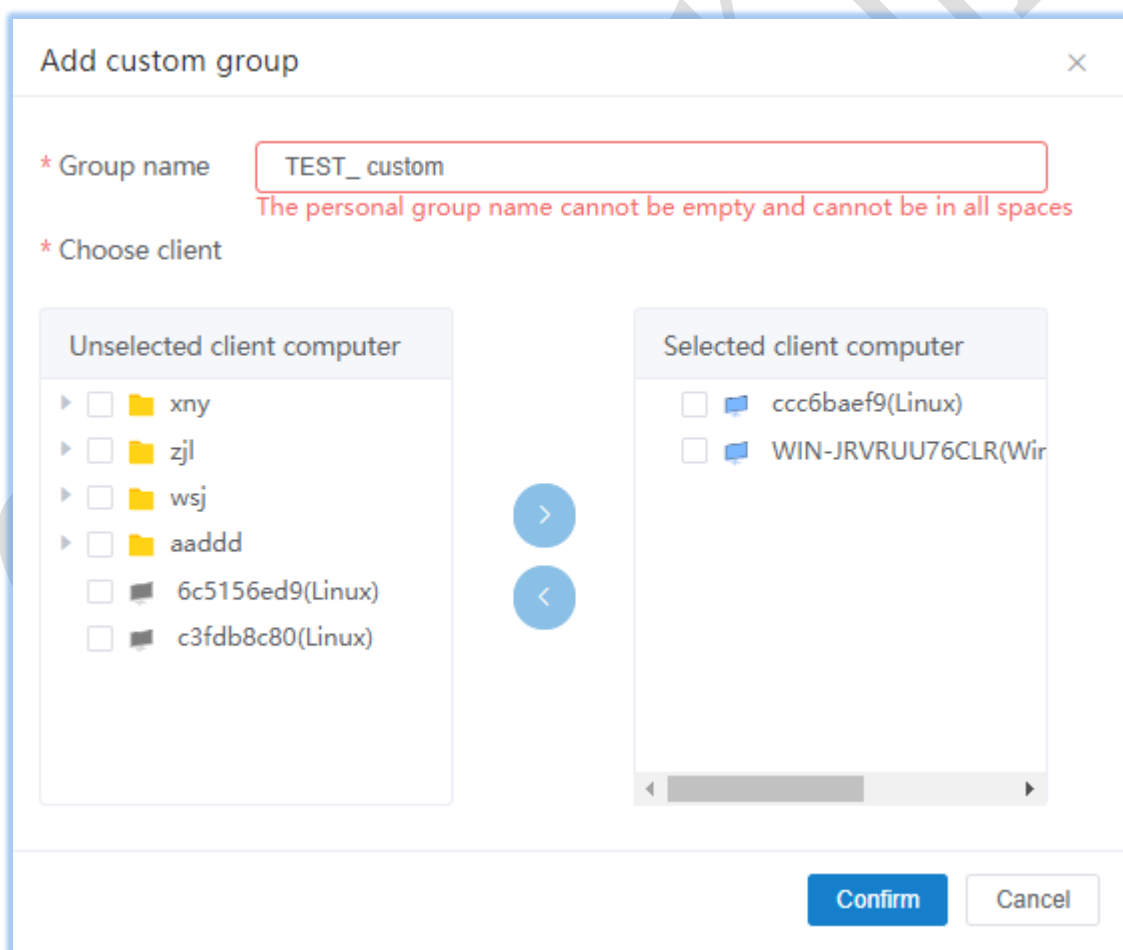
- The data of search group will not be refreshed in real time and only can be updated in manual refreshing.

2.1.4 Add personal group

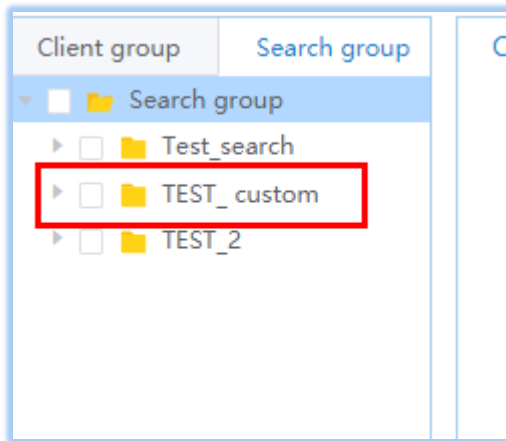
1. Enter to Client management-> Client group -> Add personal group



2. Fill the group and client in the blank index;



3. Client met with the conditions would be shown in the group after search complete;



Notice:

- Sometime, data will not be shown without refresh manually

2.1 Device management

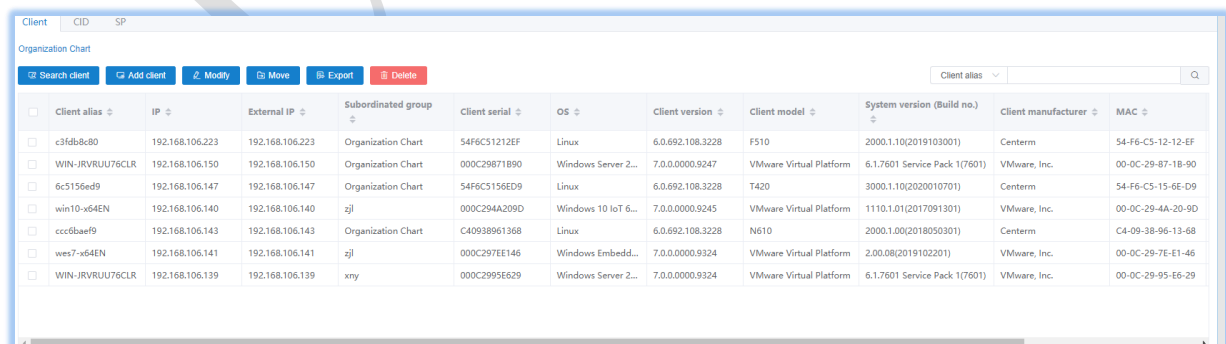
The device management is specially used for creation of enterprise organization structures, management of clients and peripherals, etc.; therefore, clients and peripherals can only be added, deleted, changed and viewed in this module.

2.2 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).

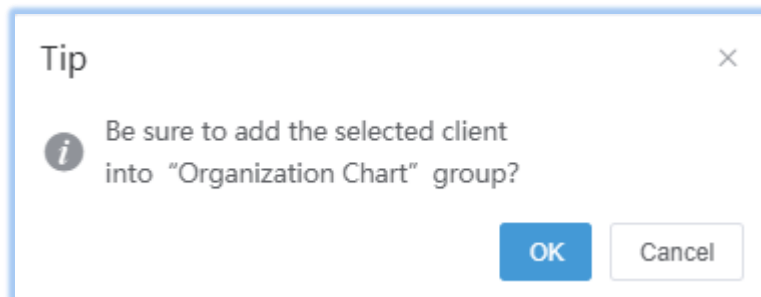
When the client is added in management, the peripherals accessed to this client will also be added in management without the need of extra operation of adding peripherals.

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);

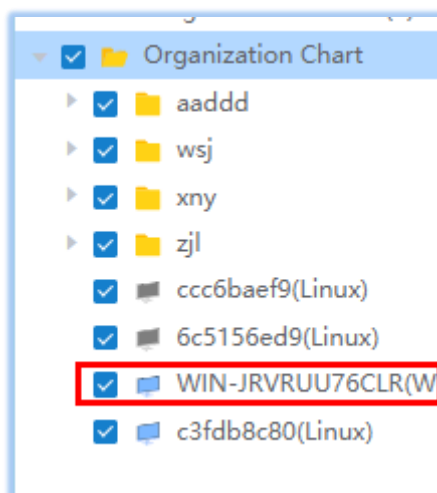


Client alias	IP	External IP	Subordinated group	Client serial	OS	Client version	Client model	System version (Build no.)	Client manufacturer	MAC
c3fdb8b0	192.168.106.223	192.168.106.223	Organization Chart	54F6C51212EF	Linux	6.0.692.108.3228	F510	2000.1.10(2019103001)	Centerm	54-F6-C5-12-12-EF
WIN-JRVBUU76CLR	192.168.106.150	192.168.106.150	Organization Chart	000C29871B90	Windows Server 2...	7.0.0.0000.9247	VMware Virtual Platform	6.1.7601 Service Pack 1(7601)	VMware, Inc.	00-0C-29-87-1B-90
6c5156ed9	192.168.106.147	192.168.106.147	Organization Chart	54F6C5156ED9	Linux	6.0.692.108.3228	T420	3000.1.10(2020010701)	Centerm	54-F6-C5-15-6E-D9
win10-x64EN	192.168.106.140	192.168.106.140	zjl	000C294A209D	Windows 10 IoT 6...	7.0.0.0000.9245	VMware Virtual Platform	1110.1.01(2017091301)	VMware, Inc.	00-0C-29-4A-20-9D
ccc6baef9	192.168.106.143	192.168.106.143	Organization Chart	C40938961368	Linux	6.0.692.108.3228	N610	2000.1.00(2018050301)	Centerm	C4-09-38-96-13-68
wes7-x64EN	192.168.106.141	192.168.106.141	zjl	000C297EE146	Windows Embedd...	7.0.0.0000.9324	VMware Virtual Platform	2.00.08(2019102201)	VMware, Inc.	00-0C-29-7E-E1-46
WIN-JRVBUU76CLR	192.168.106.139	192.168.106.139	xny	000C29956629	Windows Server 2...	7.0.0.0000.9324	VMware Virtual Platform	6.1.7601 Service Pack 1(7601)	VMware, Inc.	00-0C-29-95-E6-29

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

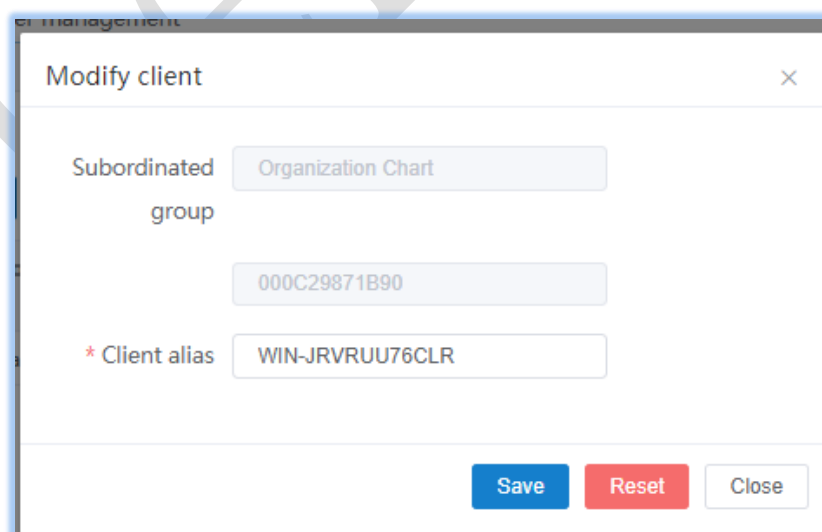


5. The user will add the client on the right panel to the client group, as shown in following figure:



2.2.1 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";

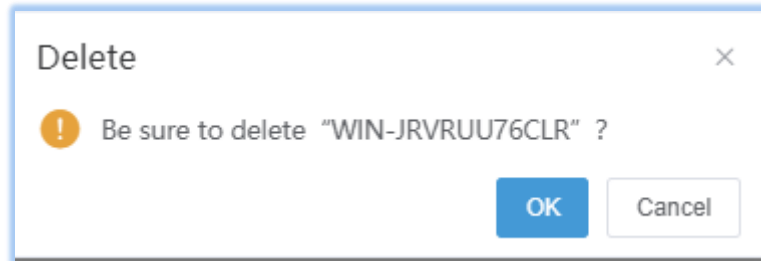


Notice:

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

2.2.2 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.



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.

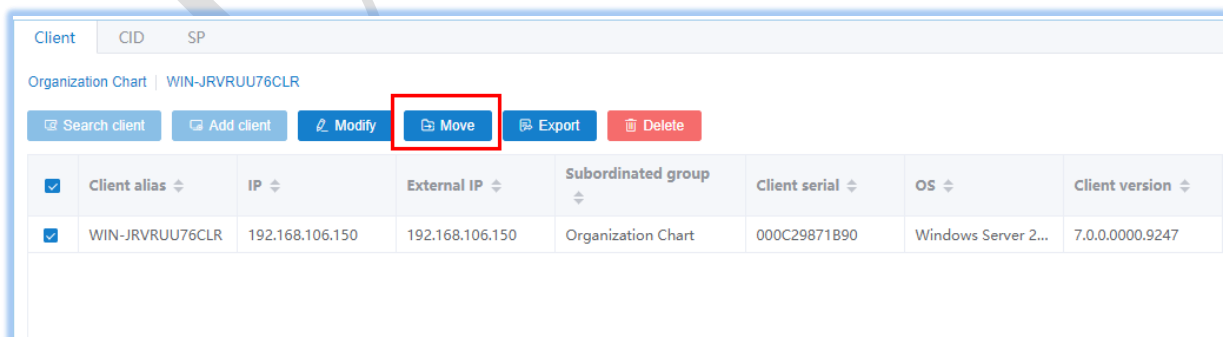
Notice:

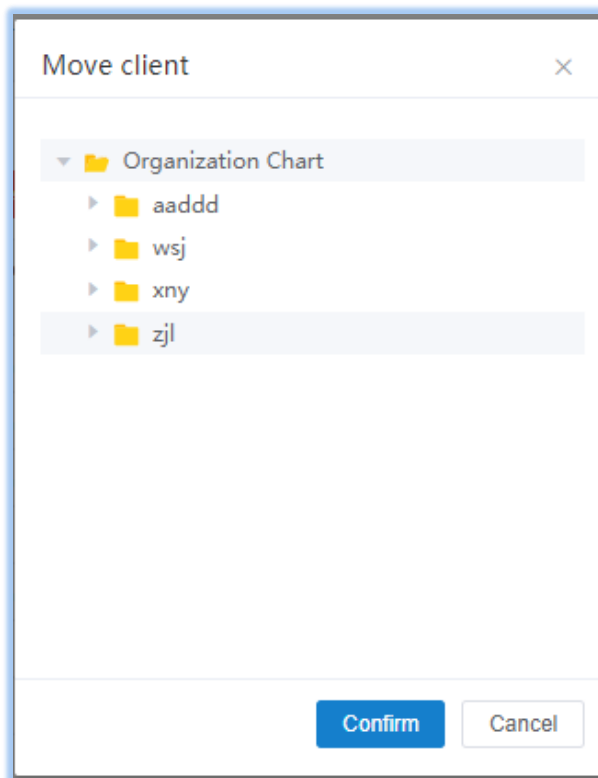
- After the client is deleted, peripherals of the client will be deleted together.

Please research thin client for re-managing thin client after 5 minutes when the same client is deleted.

2.2.3 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.





Notice:

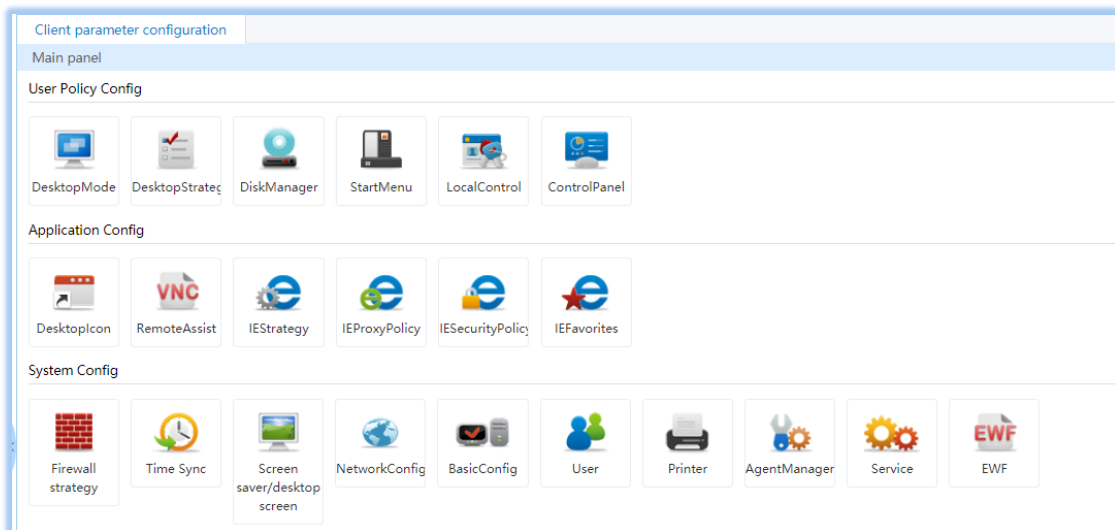
- After the client is moved, peripherals of the client will also be moved together.

3 Client Management

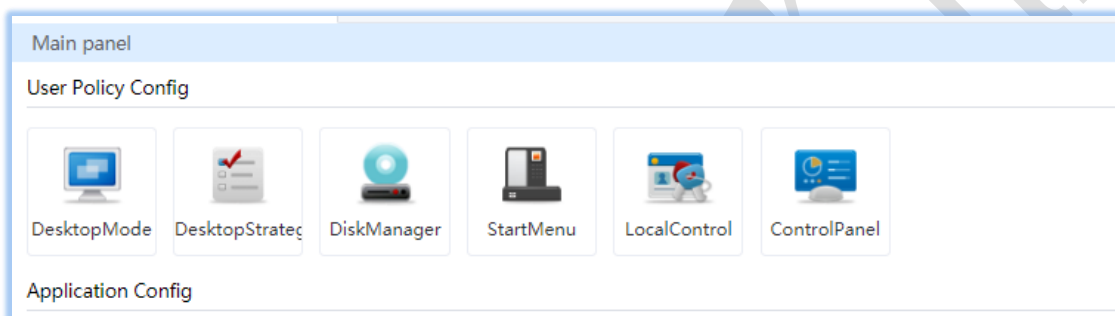
3.1 Windows client configuration

3.1.1 Windows client parameter configuration

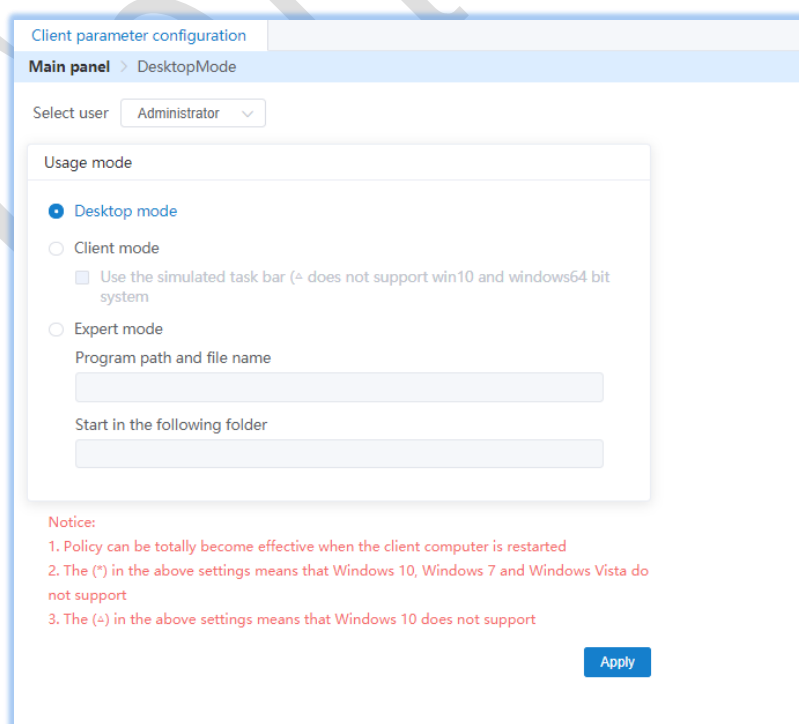
Enter **【client management—>basic management—>client configuration】** and select “client parameter configuration” tab page. The user shall select one client from the client group and can see the supported system configuration options on the right panel, as shown in following figure:



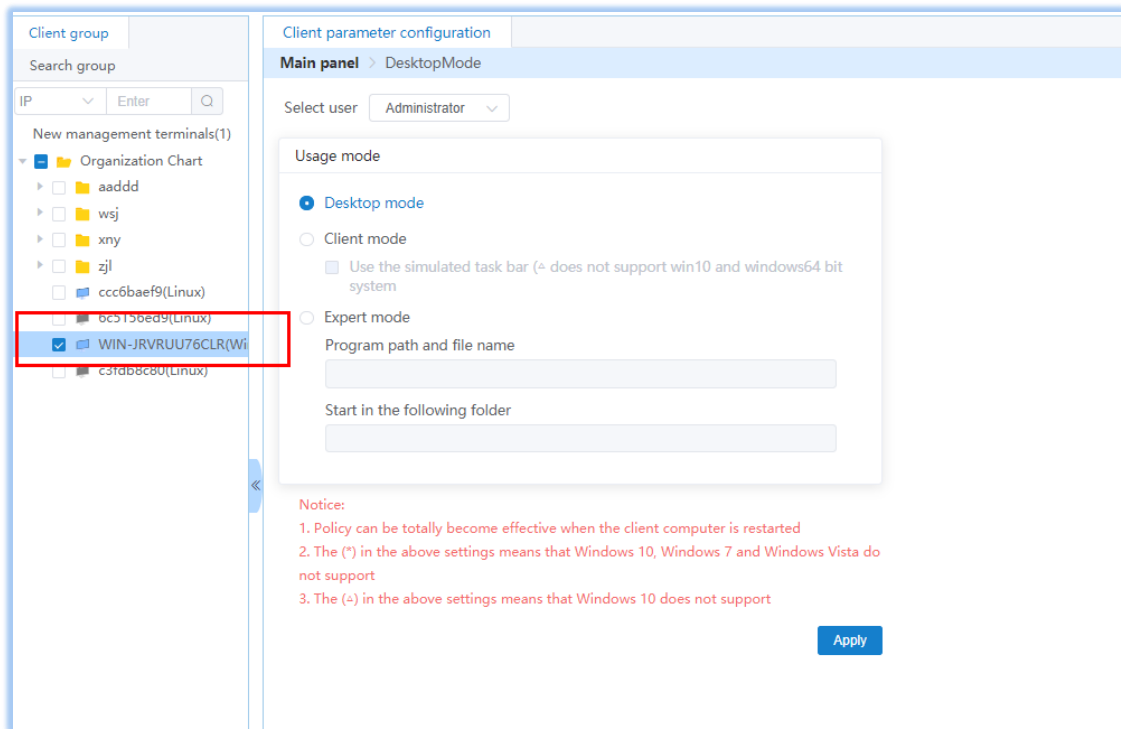
As for configuration of client parameters, click the corresponding option, such as the desktop mode in following figure:



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



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.



3.1.1.1 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 > DesktopMode

Select user Administrator

Usage mode

☒ Desktop mode

☐ Client mode

☐ Use the simulated task bar (* does not support win10 and windows64 bit system)

☐ Expert mode

Program path and file name

Start in the following folder

Notice:

1. Policy can be totally become effective when the client computer is restarted
2. The (*) in the above settings means that Windows 10, Windows 7 and Windows Vista do not support
3. The (+) in the above settings means that Windows 10 does not support

Apply

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.

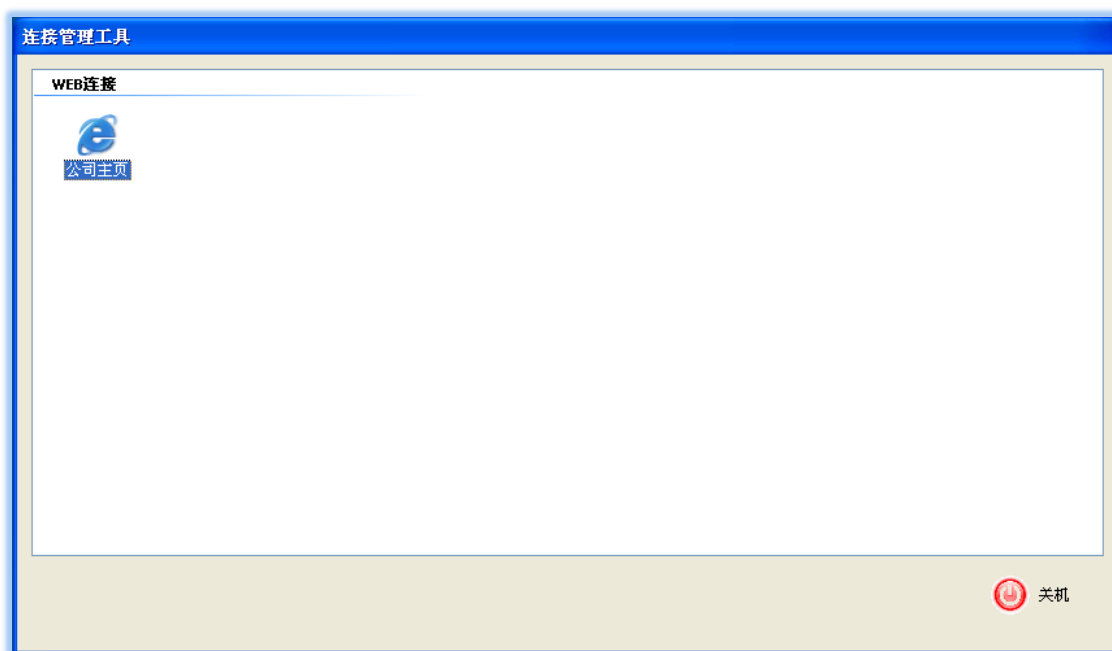
2. Terminal mode

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:

1

地址：福建省福州市金山大道 618 号橘园洲星网锐捷科技园 22#2 层 邮编：350002
 总机：400-158-1515 传真：0591-83057710 投诉电话：0591-83057123 网址：<http://www.centerm.com>
 Email：centermfw@centerm.com



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 > DesktopMode

Select user Administrator

Usage mode

☐ Desktop mode
 ☐ Client mode
 ☐ Use the simulated task bar (^ does not support win10 and windows64 bit system)

☒ Expert mode
 Program path and file name

 Start in the following folder

Notice:

1. Policy can be totally become effective when the client computer is restarted
2. The (*) in the above settings means that Windows 10, Windows 7 and Windows Vista do not support
3. The (^) in the above settings means that Windows 10 does not support

Apply

3.1.1.2 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 > DesktopStrategy

Select user Administrator

Enable all

Disable all

Clear all

Desktop Icon Configuration

Hide all desktop Icons	Not configurec
Delete "My Document" Icon on desktop	Not configurec
Delete "My Computer" Icon on desktop	Not configurec
Delete "Recycle bin" Icon on desktop	Not configurec
Delete "Nethood" Icon on desktop	Not configurec
Delete "Internet Explorer" Icon on desktop (*)	Not configurec

Desktop Operation Configuration

Delete "Property" from the context menu of "My Document"	Not configurec
Delete "Property" from the context menu of "My Computer"	Not configurec
Delete "Property" from the context menu of "Recycle Bin"	Not configurec
Don't add the sharing of recently opened document to "nethood"(*)	Not configurec
Disable users to change "My Document" route(*)	Not configurec
Disable the toolbar of adding, dragging and closing task bar	Not configurec
Disable adjustment of desktop toolbar	Not configurec
Don't save the settings when logging out	Not configurec
Delete desktop clearance guide (*)	Not configurec
Disable right click on desktop	Not configurec

3.1.1.3 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.

Client parameter configuration

Main panel > DiskManager

Select user Administrator

Disk setting

Volu...	File system	Capacity	Free space	Remark	Enabled	Show status
A		0 B	0 B	DRIVE_RE...	Enable	Show
C	NTFS	30 GB	51 %	System	Enable	Show
D		0 B	0 B	DRIVE_C...	Enable	Show

☐ Disable disk automatic running
 ☐ Map the following folder as W disk of the user

Notice: Only the selected folder can be mapped as W disk of the user, otherwise the mapping will fail

Apply

3.1.1.4 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.

Client parameter configuration

Main panel > StartMenu

Select user Administrator

Enable all

Disable all

Clear all

Start Menu Configuration

Delete user folders form "Start" menu	Not configurec
Delete common groups from "Start" menu (*)	Not configurec
Delete "My Document" icon from "Start" Menu(^)	Not configurec
Delete "Recently used documents" menu from "Start" menu(*/^)	Not configurec
Delete "Network Connection" from "Start" menu(^)	Not configurec
Delete "Favorites" menu from "Start" menu(^)	Not configurec
Delete "Find" menu from "Start" menu(*/^)	Not configurec
Delete "Help" command from "Start" menu(^)	Not configurec
Delete "Run" menu from "Start" menu(^)	Not configurec
Delete "My Pictures" icon from "Start" menu(^)	Not configurec
Delete "My Music" icon from "Start" menu(^)	Not configurec
Delete "Nethood" icon from "Start" menu(^)	Not configurec
Delete the additional program list from "Start" menu (*/^)	Not configurec
Delete the commonly used program list from "Start" menu	Not configurec
Delete complete program list from "Start" menu (^)	Not configurec
Delete "Remove PC" button from "Start" menu(^)	Not configurec
Delete user name from "Start" menu(*/^)	Not configurec
Disable the shortcut of unusable Windows Installer from "Start" menu(^)	Not configurec

3.1.1.5 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.

Client parameter configuration

Main panel > LocalControl

Select user
Administrator
Enable all
Disable all
Clear all

Local access control setting

Forbid adding printer	Not configurec
Forbid accessing control panel(^)	Not configurec
Disable Windows+X hotkey(exception: "Win+L")	Not configurec
Disable network connection property (*)	Not configurec
Disable "enable" and "disable" functions of network connection (*)	Not configurec
Disable registry editing function	Not configurec
Disable file folder option setting	Not configurec
Disable task manager	Not configurec
Disable "CMD" tool	Not configurec
Forbid users to use "Microsoft management console" (MMC)	Not configurec

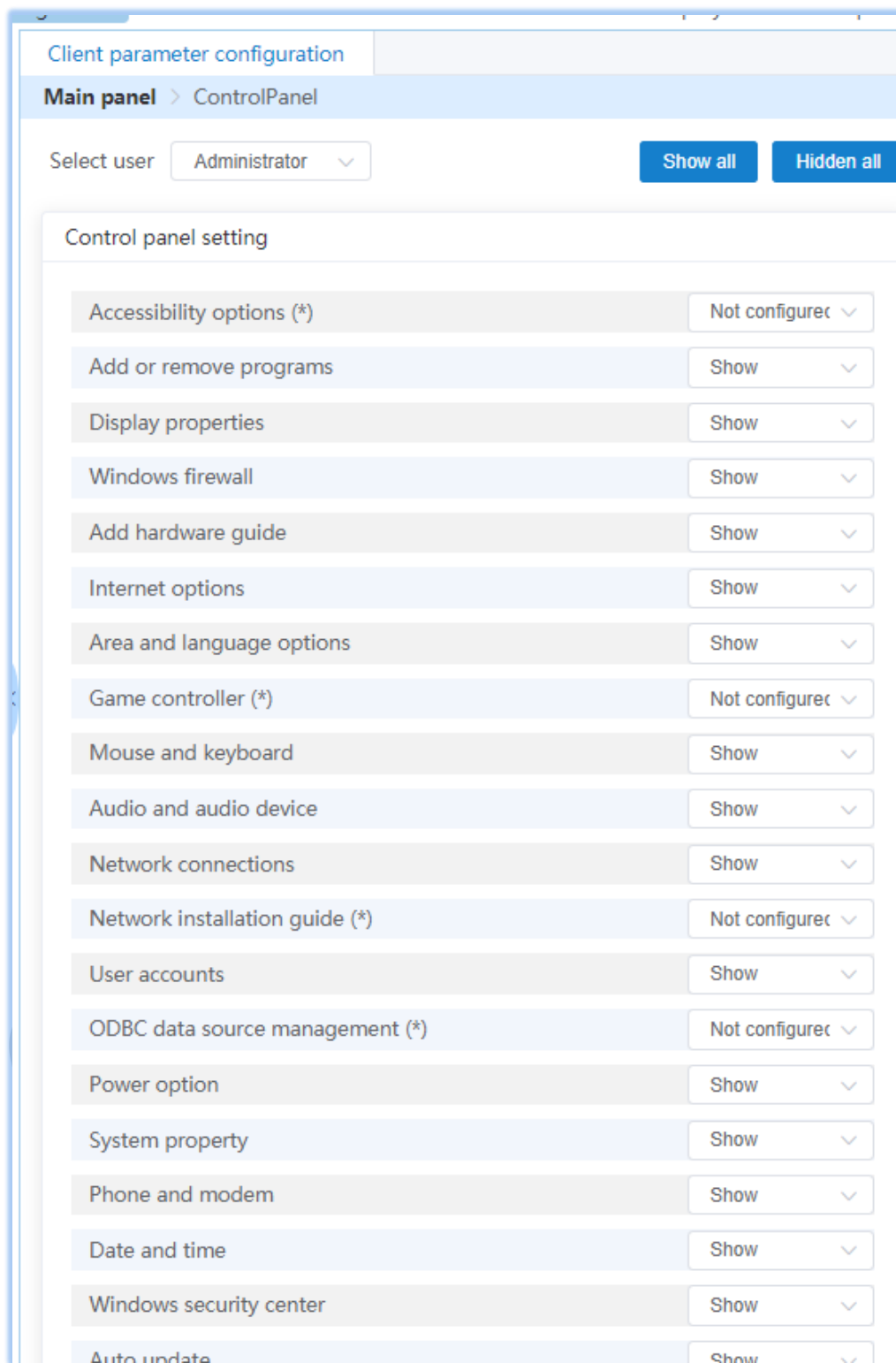
Notice:

- 1.The strategy needs restart of clients to take full effect.
2. In above configurations, (*) means Windows 10, Windows 7 and Windows Vista are not supported.
3. In above configurations, (^) means Windows 10 is not supported.

Apply

3.1.1.6 Control panel

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



3.1.1.7 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.

Client parameter configuration

Main panel > DesktopIcon

Select user

Administrator

Application configuration

☐	App	Type	Description	Operation
No Data				

Add item type

RDP connection

Add

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.

Add

Convention

Display

Local resource

App

Advanced

* Name

connet

Icon

D:\link.ioc

Login setting

* Client

192.168.106.191

Username

admin

Password

Field

☐

Enable the direct connection

Apply

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

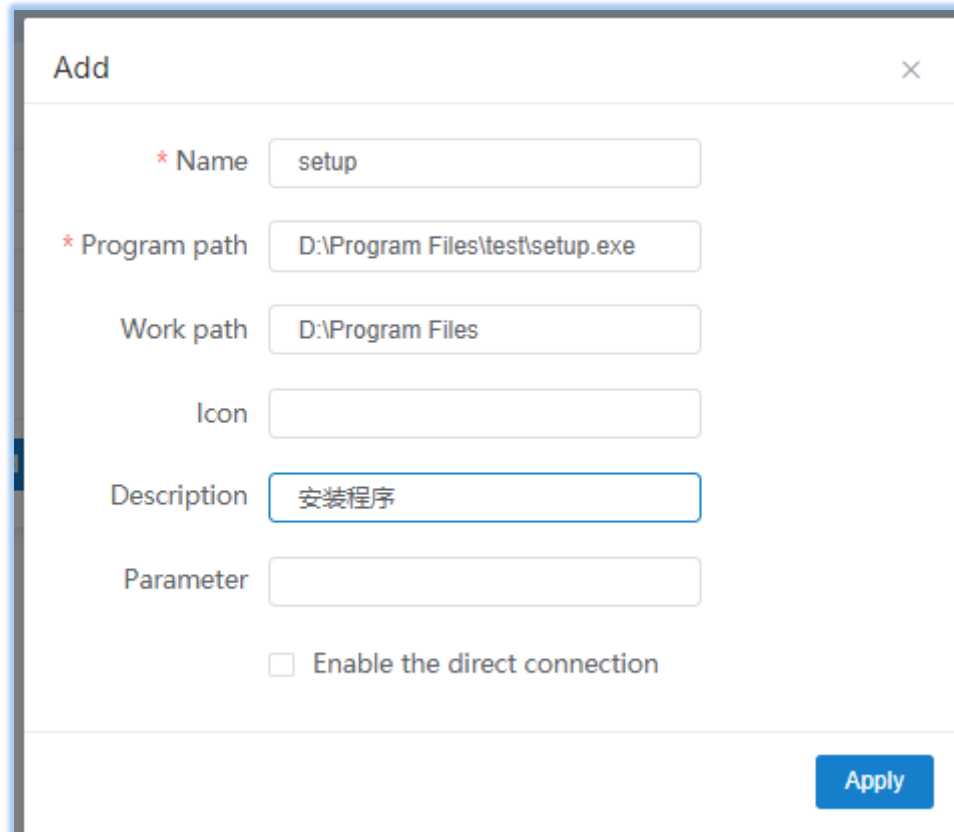


2. Application program

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)



Add [X]

* Name: setup

* Program path: D:\Program Files\test\setup.exe

Work path: D:\Program Files

Icon:

Description: 安装程序

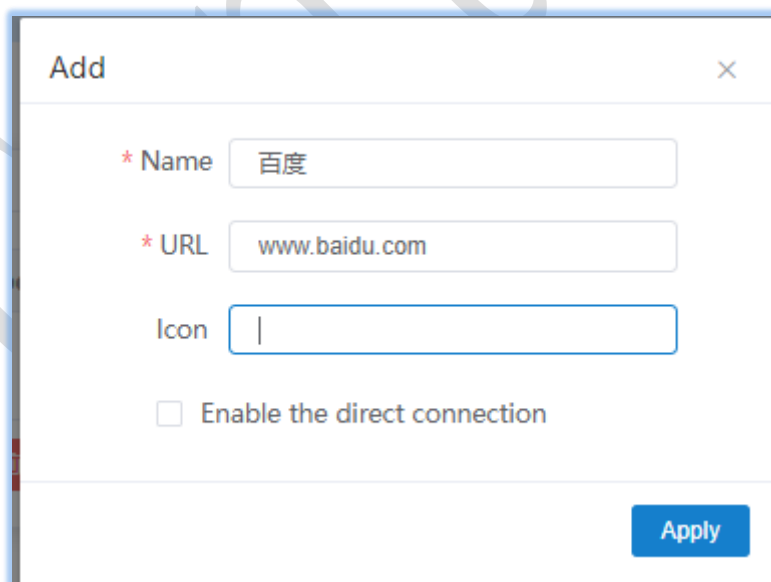
Parameter:

☐ Enable the direct connection

Apply

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.



Add [X]

* Name: 百度

* URL: www.baidu.com

Icon: |

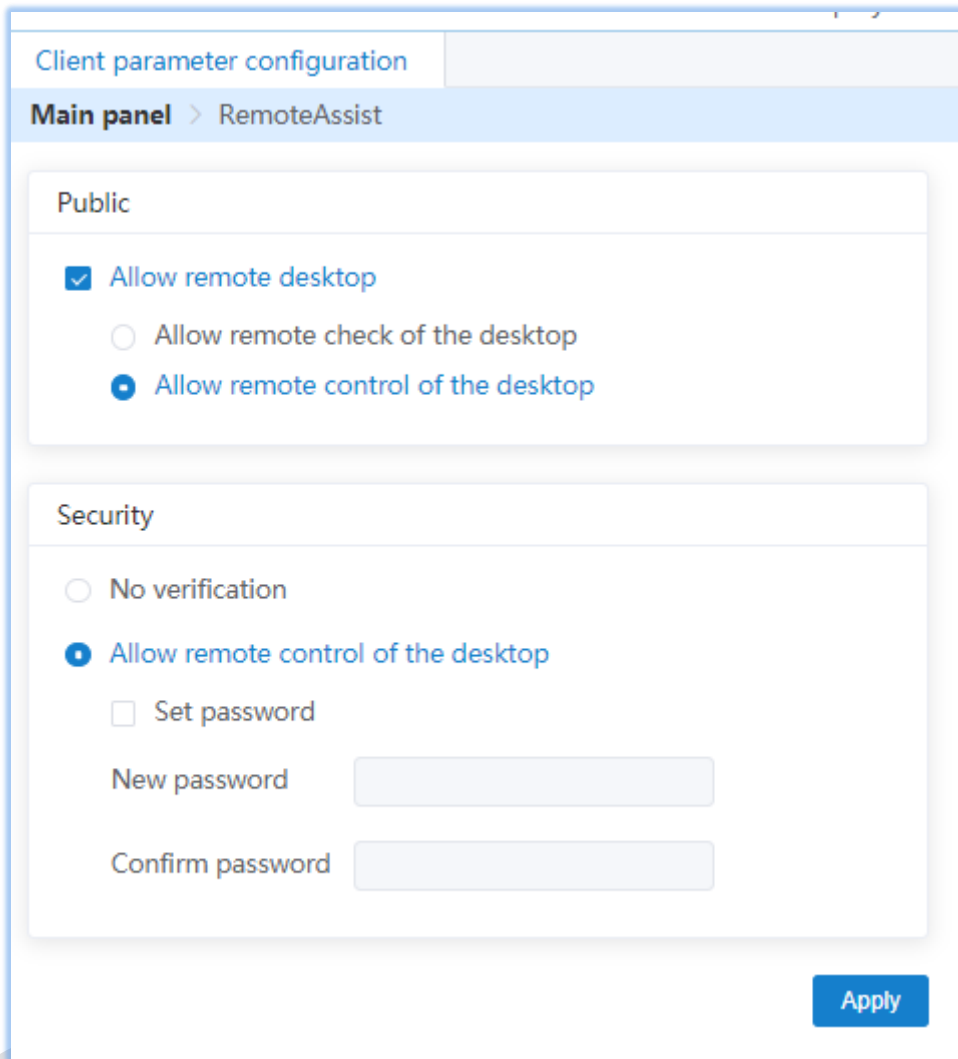
☐ Enable the direct connection

Apply

3.1.1.8 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.



Client parameter configuration

Main panel > RemoteAssist

Public

☒ Allow remote desktop

☐ Allow remote check of the desktop

☒ Allow remote control of the desktop

Security

☐ No verification

☒ Allow remote control of the desktop

☐ Set password

New password

Confirm password

Apply

3.1.1.9 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 > IEStrategy

Select user Administrator

Home page res://iesetup.dll/HardAdmin.htm

Enable all

Disable all

Clear all

IE main frame configuration

Full Screen	Not configured
Disable "Open in a new window" menu	Not configured
Disable "Save Target As" option(±Win10 and windows x64 systems are not supported)	Not configured
Hide IE Favorites	Not configured
Disable "New windows" menu	Not configured
Disable "Open" menu	Not configured
Disable "Save as" menu	Not configured
Disable "Close" menu	Not configured
Disable "View Source File" menu	Not configured
Disable "Full Screen" menu	Not configured
Disable "customized IE toolbar"	Not configured
Disable "customized IE toolbar button"	Not configured
Hide menu bar(*)	Not configured
Hide tool bar(*)	Not configured
Hide status bar(*)	Disabled

Internet option setting

3.1.1.10 IE agent strategy

Set the local IE agent item of the client.

Client parameter configuration

Main panel > IEProxyPolicy

Select user

Administrator

☐ Use proxy server configuration

Automatic configuration

☐ Use proxy server configuration
 ☐ Use automatic configuration script

IP

☐ Use proxy server for LAN

Server

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

☒ Use the same proxy server for all protocols

Exceptions

No proxy server is used for addresses that start with:

3.1.1.11 IE Security strategy

Set the local IE security strategy of the client.

Client parameter configuration

Main panel > IESecurityPolicy

Select user Administrator

Select WEB Internet

content

Regional

☐ Default level
 ☒ Custom level

security level

Safe setting

Default safe setting

Safe level of the region (L)

☐ High
 ☐ Medium-high
 ☐ Medium (default)
 ☐ Medium-low
 ☒ Low

Notice:The safe level not supported by the browser cannot become valid (such as "Medium-high" of IE6)

.Net Framework

XAML browser application setting Forbidd

XPS document Forbidd

Relax XAML Forbidd

.Net Framework related module

Module with list permission Forbidd

Run module that has not used Authenticode signature Forbidd

Run module that has used Authenticode signature Forbidd

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

3.1.1.12 IE favorites

Set the local IE favorites of the client.

Client parameter configuration

Main panel > IEFavorites

Select user

Administrator

Favorites setting

⊕ Add

🗑 Delete

☐	Name	IP	Operation
☐	建议网站	https://ieonline.microsoft.com/#ieslice	Edit
☐	网页快讯库	http://go.microsoft.com/fwlink/?LinkId=...	Edit
☐	自定义链接	http://go.microsoft.com/fwlink/?linkid=5...	Edit

Add

×

* Name

* URL

Confirm

Cancel

3.1.1.13 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

+ Add program

+ Add port

🗑 Delete

☐	Name ↕	Available or not ↕	Protocol ↕	Port ↕	Path ↕	Operation
☐	VNCC	Enable	TCP	5800		Edit
☐	VNCM	Enable	TCP	5900		Edit
☐	UnitedComminut...	Enable	TCP	8081		Edit
☐	UnitedComminut...	Enable	UDP	8081		Edit
☐	UnitedWebPortTCP	Enable	TCP	443		Edit
☐	UnitedWebPort	Enable	UDP	443		Edit
☐	UnitedHttpPortTCP	Enable	TCP	8443		Edit
☐	SDNS	Enable	TCP	65529		Edit

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

Apply

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.

3.1.1.14 Screen saver/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 > Screen saver/desktop screen

☒ Desktop background setting

Select picture Desktop background file Upload Management background file

Display position Drag

☐ Modify screen saver setting

☐ Enable screen protection

Select Screen saver file Upload Manage screen saver file

file

Wait 3 Min

time

☐ Enable password protection in restoring

File Path 片_20200114190808.bmp Scan

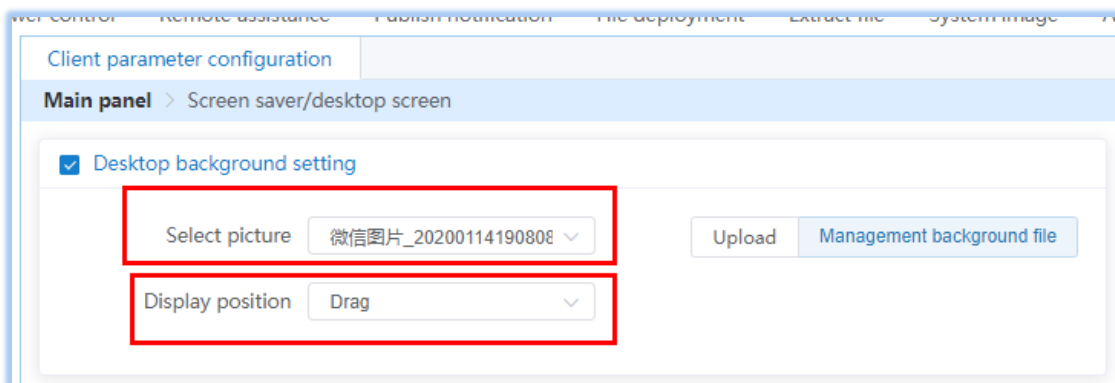
File

Upload Completed

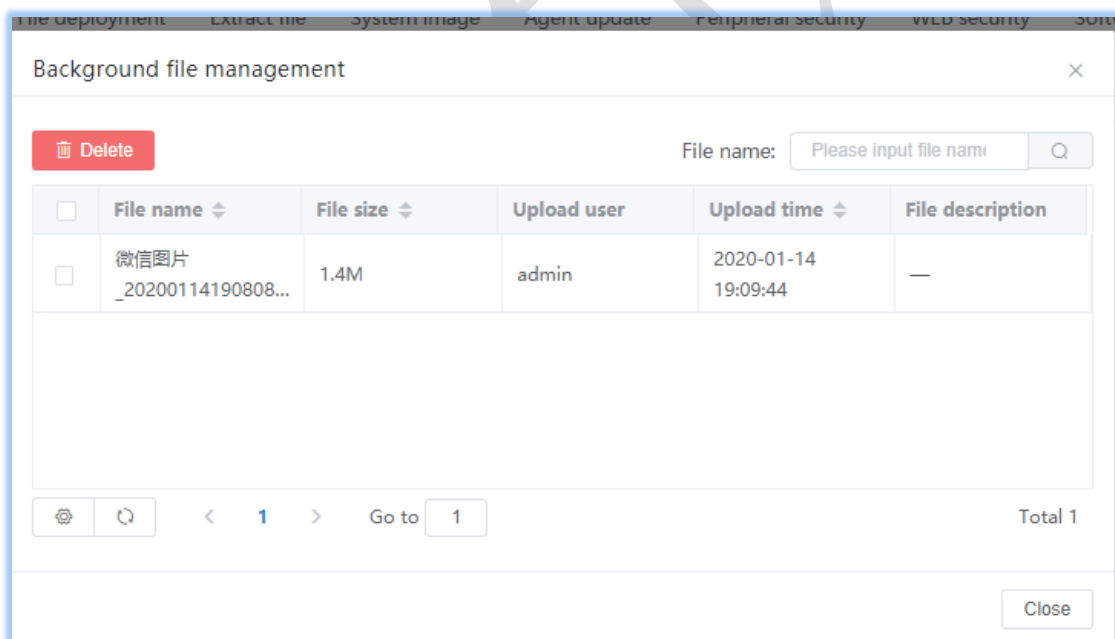
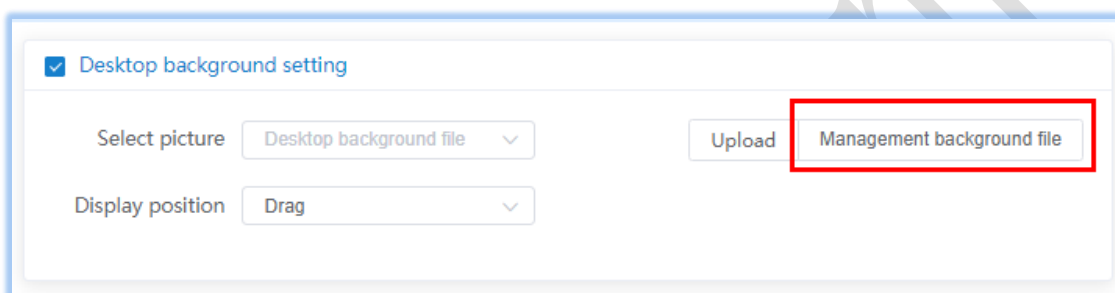
File Upload Successful

Continue Uploading Exit

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



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.



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

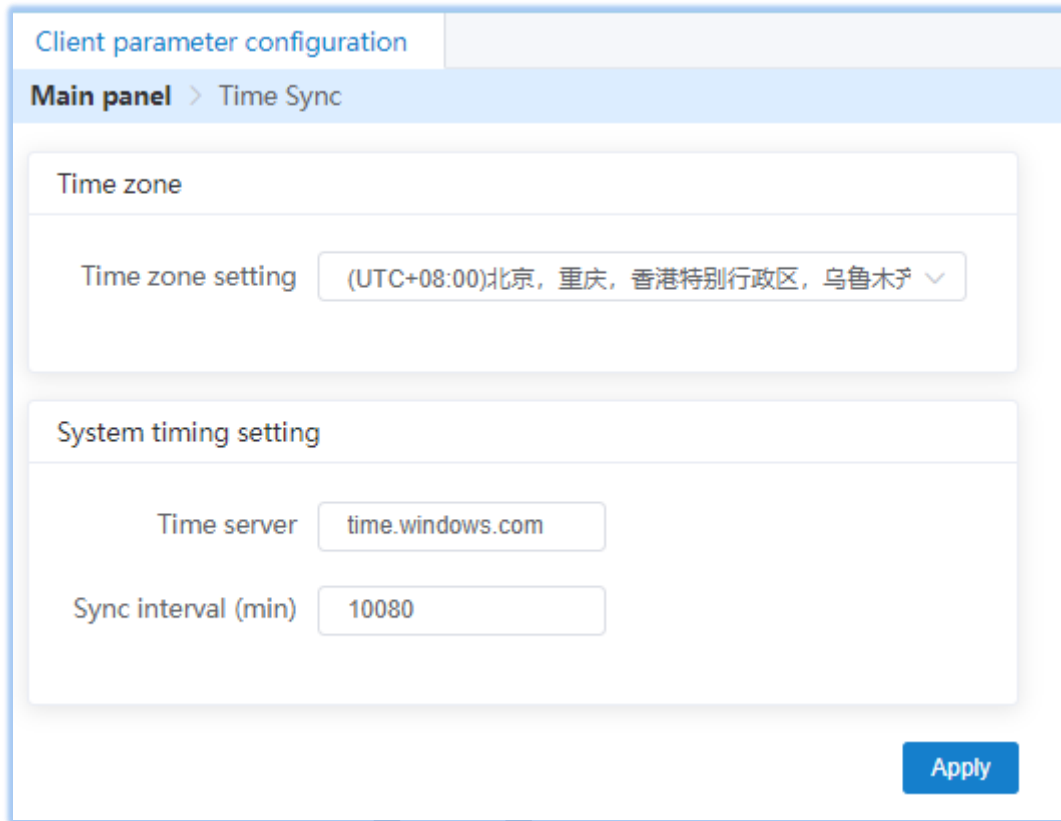
3.1.1.15 Time synchronization

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.

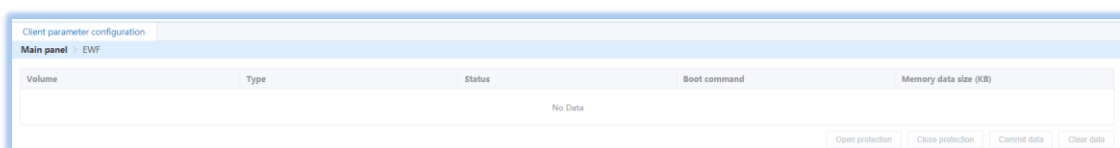


3.1.1.16 EWF protection control

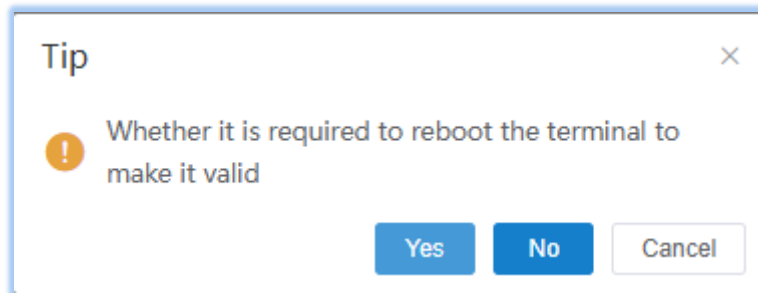
EWF protection control is only valid in the client with memory protection or hard disk protection function.

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.



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.



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

3.1.1.17 User management

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:



Edit

☐ Modify password
 ☒ Auto login

* Username

Administrator

Login password

.....

* User group

Administrators,Users

Description

管理计算机(域)的内置帐户

Confirm

Cancel

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

Add

☒ Auto login

* Username

NewUser

Password

.....

Confirm password

.....

Login password

•

* User group

administrator

Description

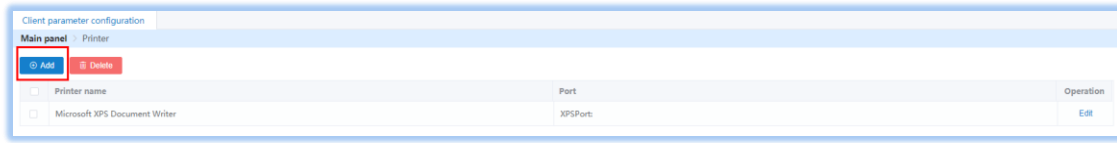
test

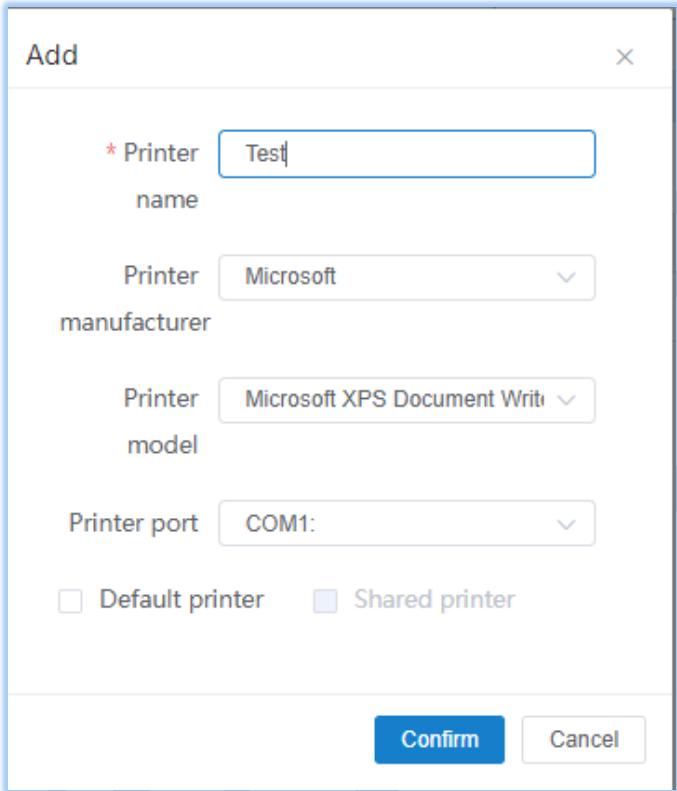
Confirm

Cancel

3.1.1.18 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





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

3.1.1.19 Agent 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 > AgentManager

Manage the server address configuration

☐ Actively add by remote management server

☒ Manually specify the address of management server

IP

Port

☐ Client password modification

New password

Confirm password

Apply

Change of client password:

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

Client parameter configuration

Main panel > AgentManager

Manage the server address configuration

☐ Actively add by remote management server

☒ Manually specify the address of management server

IP

Port

☒ Client password modification

New password

Confirm password

Apply

3.1.1.20 Service

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

Client parameter configuration					
Main panel Service					
Show name	Service name	Startup type	Status	Description	Set
☐ Application Experience	AeLookupSvc	Automatic	Stopped	在应用程序启动时为应用程序处理应用程序兼容性请求	Set
☐ Application Layer Gateway Service	ALG	Manual	Stopped	为 Internet 连接共享提供第三方协议插件的支持	Set
☐ Application Identity	AppIDSvc	Manual	Stopped	确定并验证应用程序的标识。禁用此服务将阻止强制执行 AppLocker。	Set
☐ Application Information	Appinfo	Manual	Stopped	使用辅助管理权限便于交互式应用程序的运行。如果停止此服务，用户将无法使用辅助管理权限启动应用程序。	Set
☐ Application Management	AppMgmt	Manual	Stopped	为通过设备部署的软件处理安装、删除以及效率请求。如果该服务被禁用，则用户将无法安装、删除或效率。	Set
☐ Windows Audio Endpoint Builder	AudioEndpointBuilder	Manual	Stopped	管理 Windows 音频服务的音频设备。如果此服务被停止，音频设备和效果将不能正常工作。如果此服务被禁...	Set
☐ Windows Audio	AudioSrv	Manual	Stopped	管理基于 Windows 的程序的音频。如果该服务被停止，音频设备和效果将不能正常工作。如果此服务被禁...	Set
☐ Base Filtering Engine	BFE	Automatic	Started	基本筛选引擎(BFE)是一种管理防火墙和 Internet 协议安全(IPsec)策略以及实施用户模式策略的服务。停止或...	Set
☐ Background Intelligent Transfer Service	BITS	Manual	Stopped	使用空闲网络带宽在后台传送文件。如果该服务被禁用，则依赖于 BITS 的任何应用程序如 Windows Updat...	Set
☐ Computer Browser	Browser	Prohibit	Stopped	维护网络上计算机的更新列表，并将列表提供给计算机指定浏览。如果服务停止，列表不会被更新或维护。如...	Set

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					
Show name	Service name	Startup type	Status	Description	Set
☐ Application Experience	AeLookupSvc	Automatic	Stopped	在应用程序启动时为应用程序处理应用程序兼容性请求	Set
☐ Application Layer Gateway Service	ALG	Manual	Stopped	为 Internet 连接共享提供第三方协议插件的支持	Set
☐ Application Identity	AppIDSvc	Manual	Stopped	确定并验证应用程序的标识。禁用此服务将阻止强制执行 AppLocker。	Set
☐ Application Information	Appinfo	Manual	Stopped	使用辅助管理权限便于交互式应用程序的运行。如果停止此服务，用户将无法使用辅助管理权限启动应用程序。	Set
☐ Application Management	AppMgmt	Manual	Stopped	为通过设备部署的软件处理安装、删除以及效率请求。如果该服务被禁用，则用户将无法安装、删除或效率。	Set
☐ Windows Audio Endpoint Builder	AudioEndpointBuilder	Manual	Stopped	管理 Windows 音频服务的音频设备。如果此服务被停止，音频设备和效果将不能正常工作。如果此服务被禁...	Set
☐ Windows Audio	AudioSrv	Manual	Stopped	管理基于 Windows 的程序的音频。如果该服务被停止，音频设备和效果将不能正常工作。如果此服务被禁...	Set
☐ Base Filtering Engine	BFE	Automatic	Started	基本筛选引擎(BFE)是一种管理防火墙和 Internet 协议安全(IPsec)策略以及实施用户模式策略的服务。停止或...	Set
☐ Background Intelligent Transfer Service	BITS	Manual	Stopped	使用空闲网络带宽在后台传送文件。如果该服务被禁用，则依赖于 BITS 的任何应用程序如 Windows Updat...	Set
☐ Computer Browser	Browser	Prohibit	Stopped	维护网络上计算机的更新列表，并将列表提供给计算机指定浏览。如果服务停止，列表不会被更新或维护。如...	Set

Set

Show name

Application Information

Service name

Appinfo

Startup type

Manual

Set

Status

Stopped

Start

Description

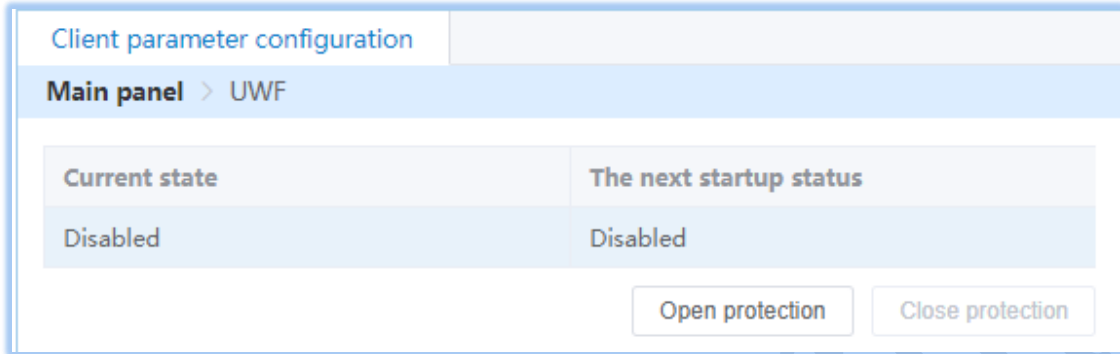
使用辅助管理权限便于交互式应用程序的运行。如果停止此服务，用户将无法使用辅助管理权限启动应用程序，而执行所需用户任务可能需要这些权限。

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.

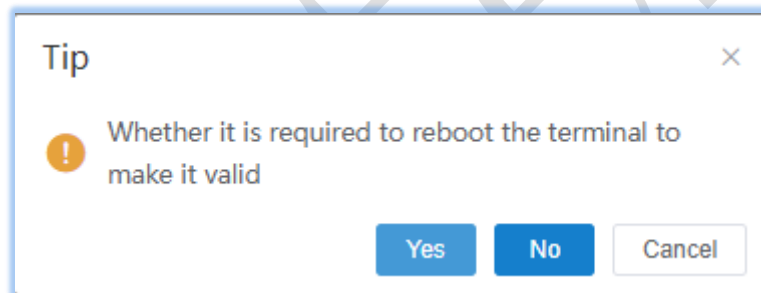
3.1.1.21 UWF protection

UWF protection control is only valid for the client with UWF module. The server can be configured with following four operations: (only available for UWF supported client, such as Windows client)

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



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.



3.2 Linux client settings

3.2.1 Linux client specification settings

Enter to Client Management -> Basic Info, then choose one of client, all clients settings can be viewed and configured on the right, the figure is shown as below

Client parameter configuration

Basic Info

Display

Time Setting

Network

Language And Keyboard

Security

Cloud Service

ICA Global Settings

DeviceManager

Patch List

Power Manager

* Terminal Name:

ccc6baef9

Terminal Type:

N610

Manufacturer:

Centerm

Operating System:

Linux

Version:

2000.1.00

BIOS:

2.52

BUILD No.:

2018050301

Storage Capacity:

15104M

Network Card1-IPv4:

192.168.106.143

MAC Address:

C4-09-38-96-13-68

Citrix Receiver:

13.3.0.344519

VMware Horizon View:

4.1.0

RDP:

8.1

Flash Player:

27.0

Apply

Enter to relevant settings for modification to its parameter, the figure is shown as below:

Client parameter configuration

Basic Info

Display

Time Setting

Network

Language And Keyboard

Security

Cloud Service

ICA Global Settings

DeviceManager

Patch List

Power Manager

Display

Main Display

VGA

Mode

Single

☒ Auto check

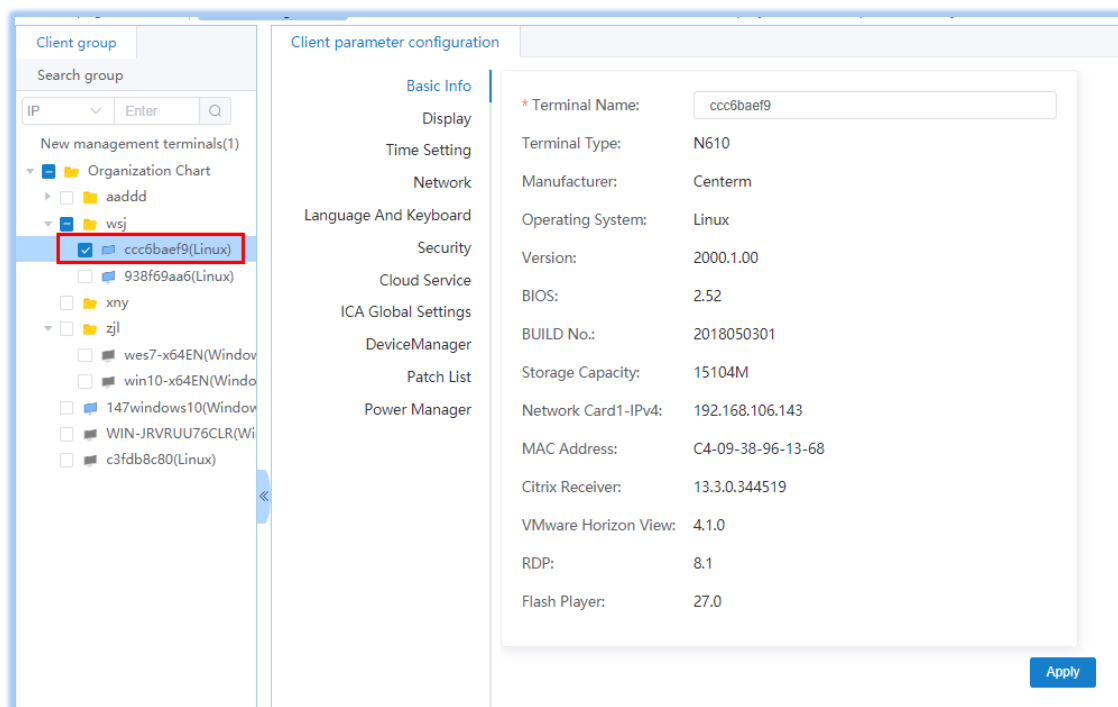
VGA

Resolution

1024x768

Apply

After configuration done, click “Apply” to take settings effected. Notice: settings can be made into policy for deployment to multiple clients



3.2.1.1 Basic info

Basic info includes the client type, OS, BIOS version, storage size, IP address, MAC, cloud service version, flash player version, manufacturer, build NO. the figure is shown as below:

* Terminal Name:	ccc6baef9
Terminal Type:	N610
Manufacturer:	Centerm
Operating System:	Linux
Version:	2000.1.00
BIOS:	2.52
BUILD No.:	2018050301
Storage Capacity:	15104M
Network Card1-IPv4:	192.168.106.143
MAC Address:	C4-09-38-96-13-68
Citrix Receiver:	13.3.0.344519
VMware Horizon View:	4.1.0
RDP:	8.1
Flash Player:	27.0

Apply

3.2.1.2 Display

Display would take effects to the resolution rate for the monitor connected with client, setting should be allowed to be modified after Auto check option is unticked

Display

Main Display

VGA

Mode

Single

☐ Auto check

VGA

Resolution

1024x768

Apply

3.2.1.3 Time

This is above time settings for client

Time Zone

(UTC+08:00) Beijing, Chongqing, Hong Kong, Urum

Time synchronization settings

☐ Synchronize with an internet time server

* Time Server

0.0.0.0

* Query time interval(day)

7

Apply

3.2.1.4 Network

IP, Gateway, subnet mask and DNS can be set in Network

Network

Routing

DNS

☐ DHCP

MAC

C4-09-38-96-13-68

Net port

1

* IPv4

192.168.106.143

* Subnet mask

255.255.255.0

Default gateway

192.168.106.1

Apply

3.2.1.5 Language and keyboard

Language and keyboard layout can be set

Display language:

English

▼

Keyboard Layout:

United States (English)

▼

Keyboard Model:

Generic 105-key

▼

Apply

3.2.1.6 Security

Password can be set in Security, to allow or deny connection to local

System Setting

☒ Use Password

Password

Re-Password

VNC Settings

☒ Allow Remote Desktop

When a user attempt to view or control your desktop:

☒ Ask user to enter this password

Password

Apply

3.2.1.7 Cloud service

Session can be add, edit and delete in Cloud service

Default

Add

Edit

Type: RDP

	Type	Default Connection
☐	RDP	
☐	Citrix Receiver	Enabled
☐	VMware Horizon View	

3.2.1.8 ICA Global settings

ICA global settings is settings about USB port ,printer mobile storage, sound redirection, connection

bar hidden in session.

Device Redirection

☐ Serial ports
 ☒ USB device
 ☒ Printer
 ☐ Storage
 ☒ Smart card
 ☒ Sound

Options

☒ Display the connection bar
 ☒ Video HDX
 ☒ Audio HDX
 ☐ Flash HDX
 ☐ WebCam HDX
 ☐ H.264

Apply

Notice: Webcam HDX herewith will not be effected without Video HDX ticked first

3.2.1.9 Device management

Peripheral availability can be set in Device manager

☒ Serial Port
 ☒ Parallel Port
 ☒ Storage
 ☒ USB Printer

Apply

3.2.1.10 Patch list

Patch version can be check in below list

Patch Name	Patch Version
flashplayer	27.0.0.187

3.2.1.11 Power management

Power management is the settings about time to shut down monitor

Idle Policy

☒ Enable Close Monitor Policy

When system idle, wait minutes

Schedule Policy

☐ Enable Schedule Policy

Everyday :

Apply

3.3 Power control

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

3.3.1 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:

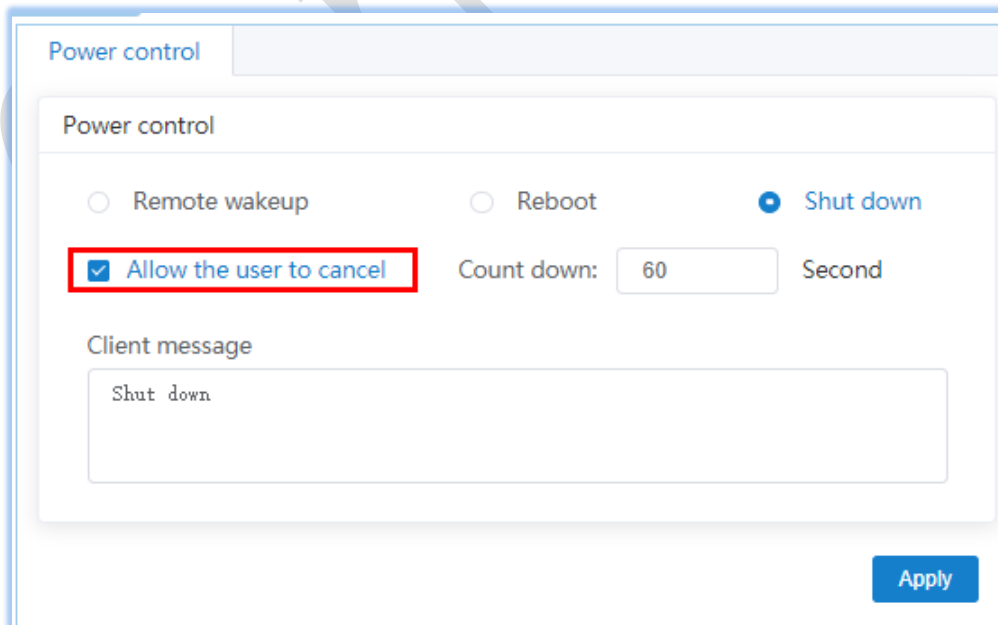
- The server and the wakened client cannot cross network segment and shall be in the same VLAN;
- Special settings of switch and other network device may cause failure of WoL function;
- If the client is in abnormal shutdown state, the client cannot be wakened.

3.3.2 Control option

The following options are available for restart and shutdown operation:

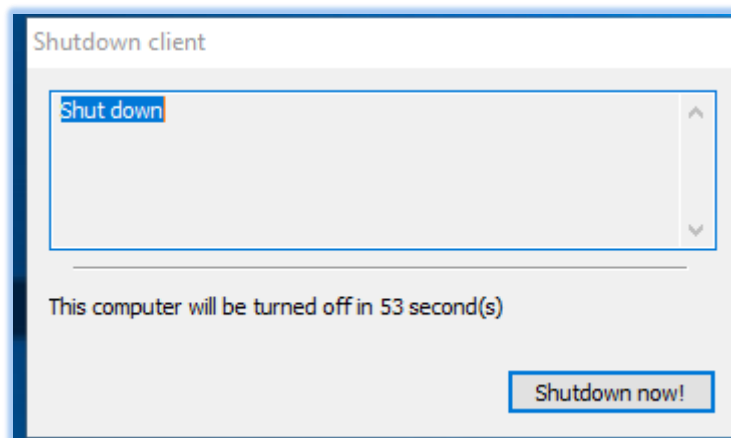
1. Allow user to cancel

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.



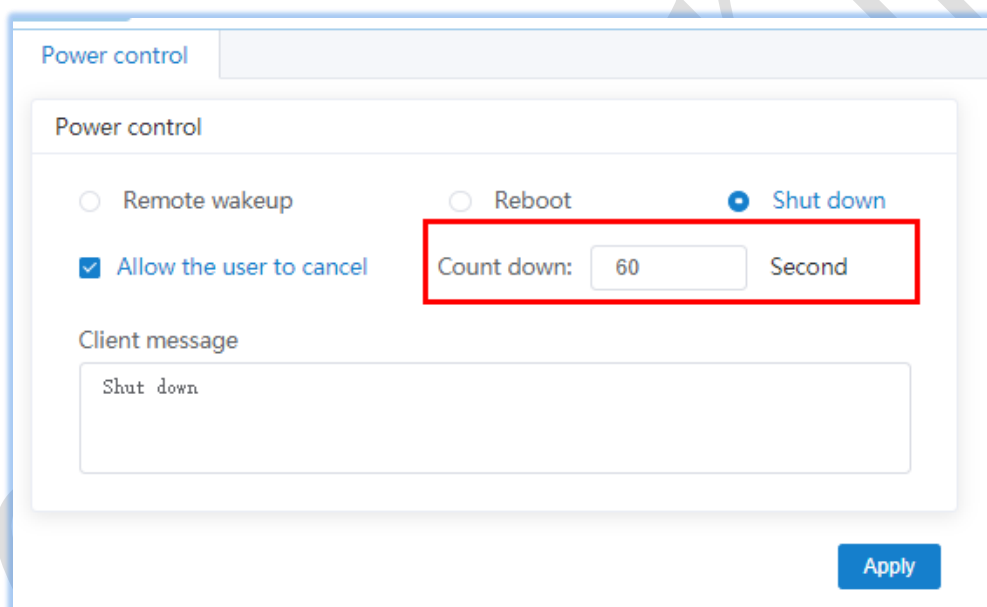
The screenshot shows a web interface for power control. At the top, there's a tab labeled 'Power control'. Below it, the main heading is 'Power control'. There are three radio buttons: 'Remote wakeup', 'Reboot', and 'Shut down'. The 'Shut down' button is selected. Below these, there's a checkbox labeled 'Allow the user to cancel' which is checked and highlighted with a red box. To the right of this checkbox is a 'Count down:' field with the value '60' and the unit 'Second'. Below this is a text area labeled 'Client message' containing the text 'Shut down'. At the bottom right, there is an 'Apply' button.

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



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.



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.

Power control

Power control

☐ Remote wakeup
 ☒ Reboot
 ☐ Shut down

☒ Allow the user to cancel
 Count down: Second

Client message

Reboot

Apply

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

Restart client

Reboot

This computer will restart in 48 second(s)

Restart now!

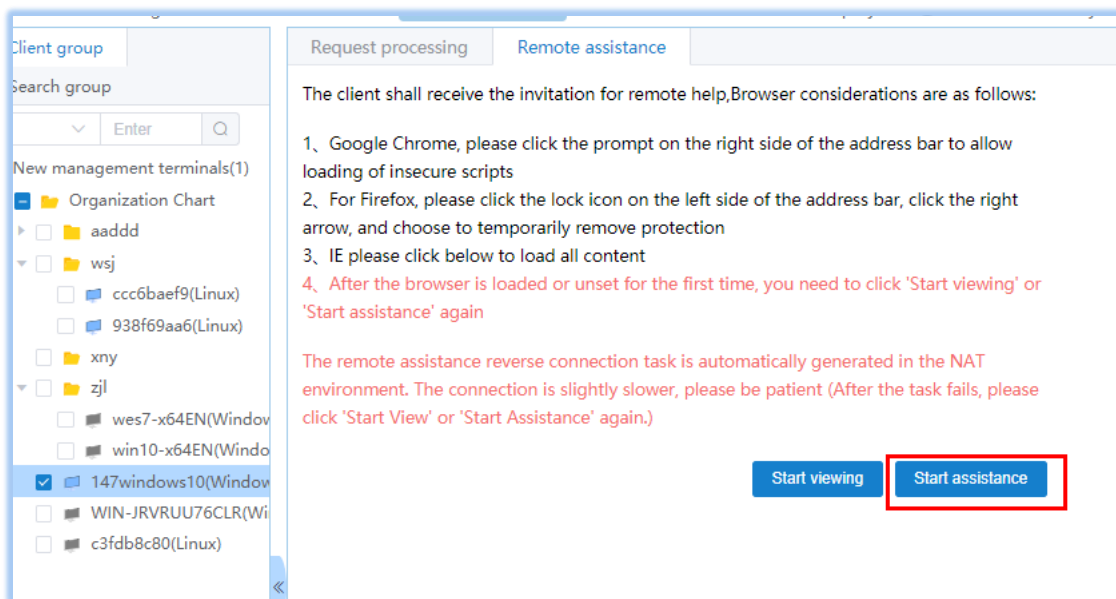
3.4 Remote assistance

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.

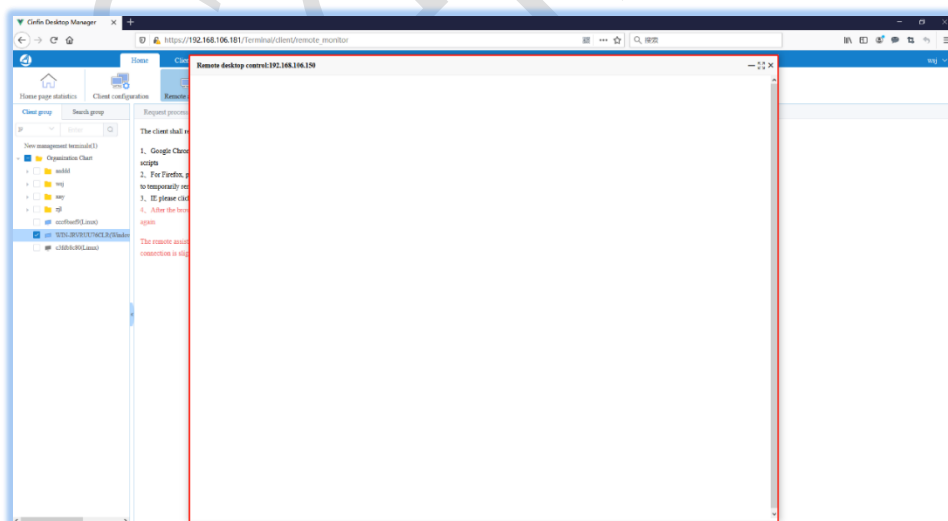
4.3.1 Install JRE

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.

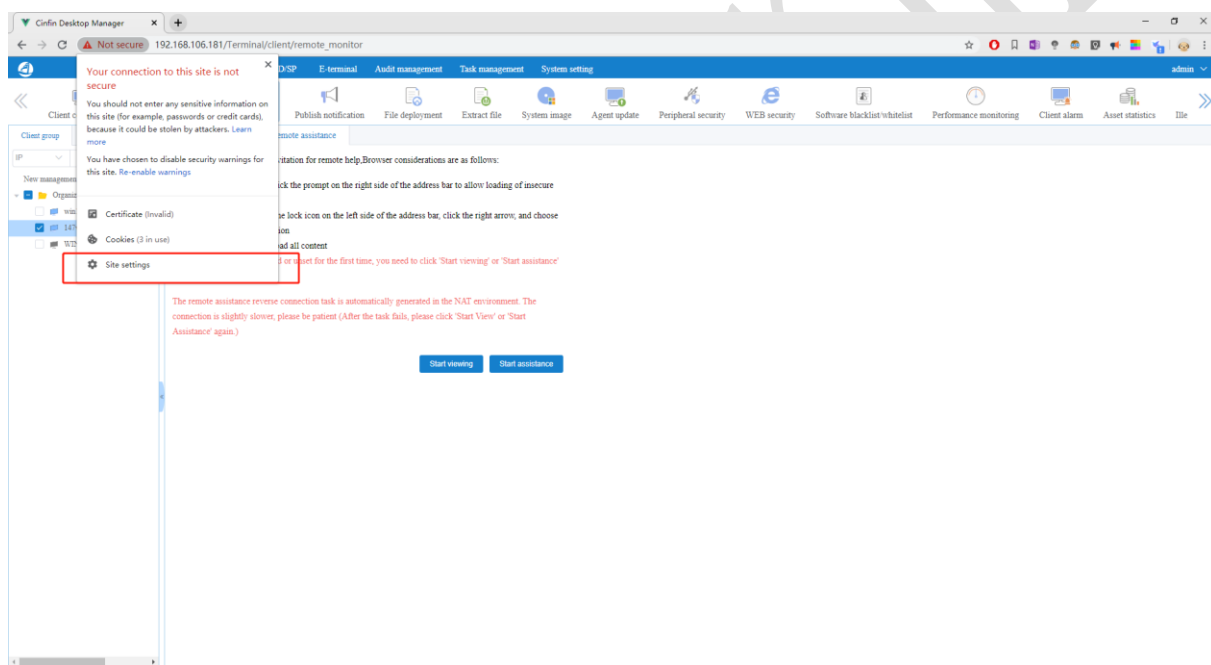
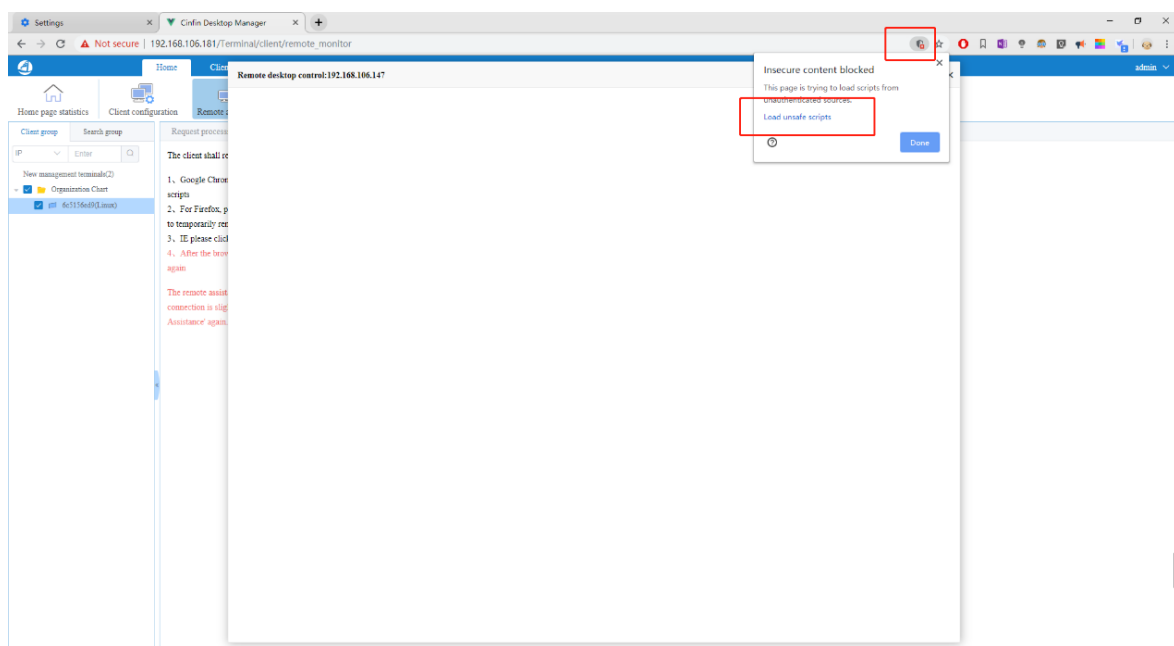


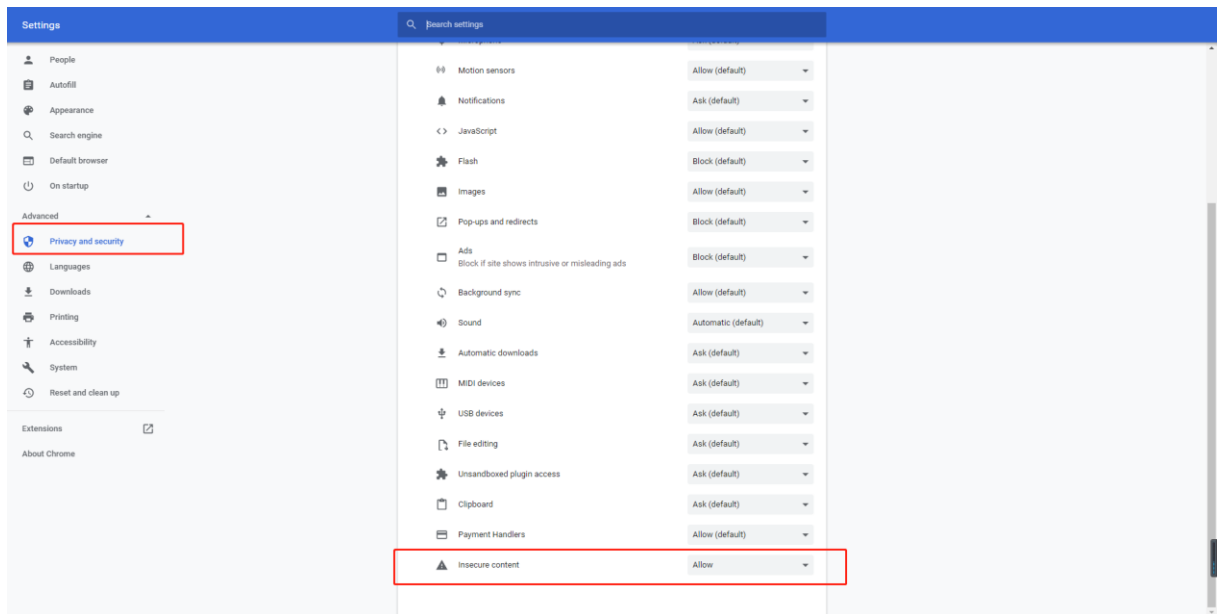
2. Click to finish the installation of jre environment according to the prompt.



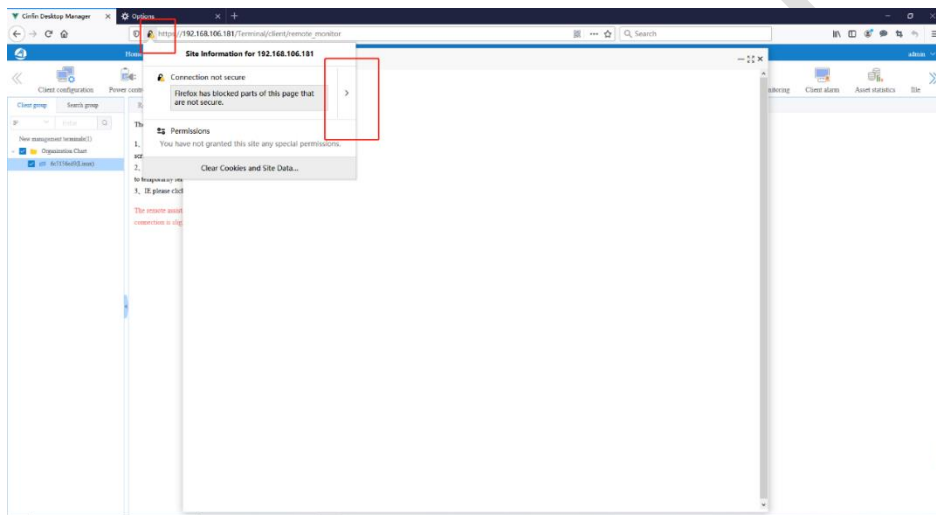
The following methods are provided for solution to different browser when VNC function is not working

- Chrome browser: click the shield icon on the right, choose ‘Load unsafe scripts’ then allow browser to run ‘Insecure content’

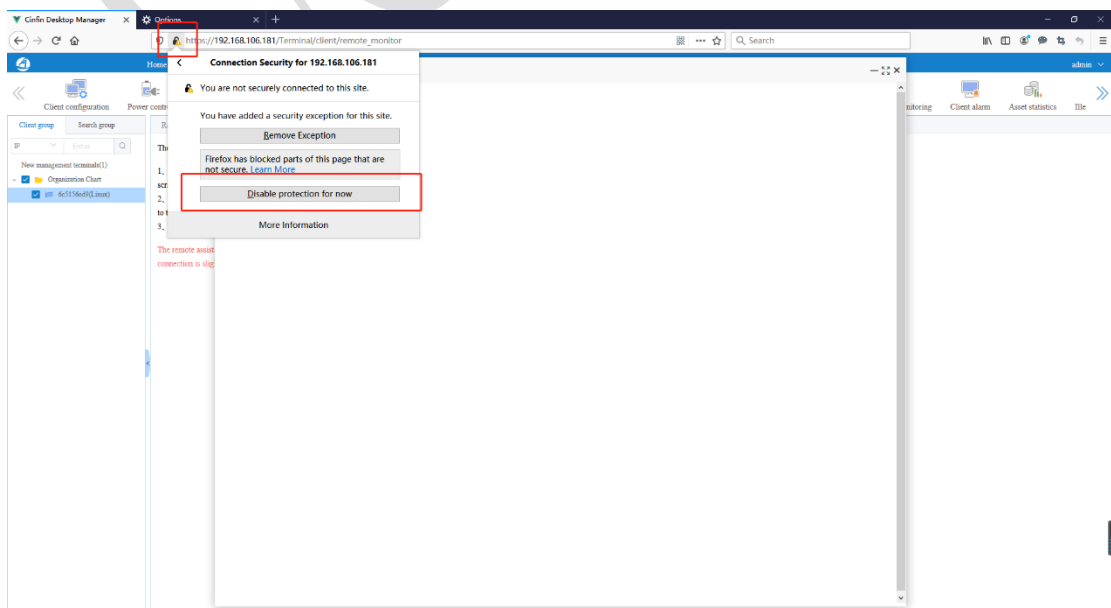




- Firefox: Click the below lock icon in URL, then choose 'Firefox has blocked parts of this page that are not secure'

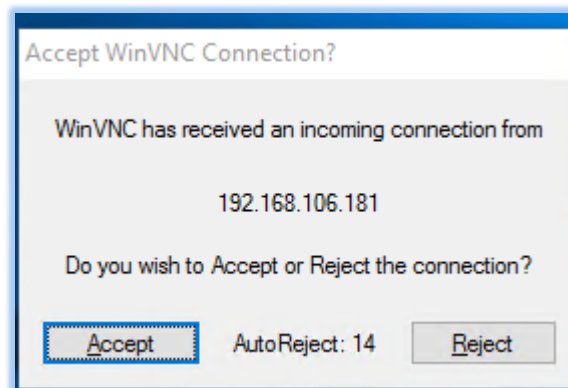


After that, click 'Disable the protection for now'

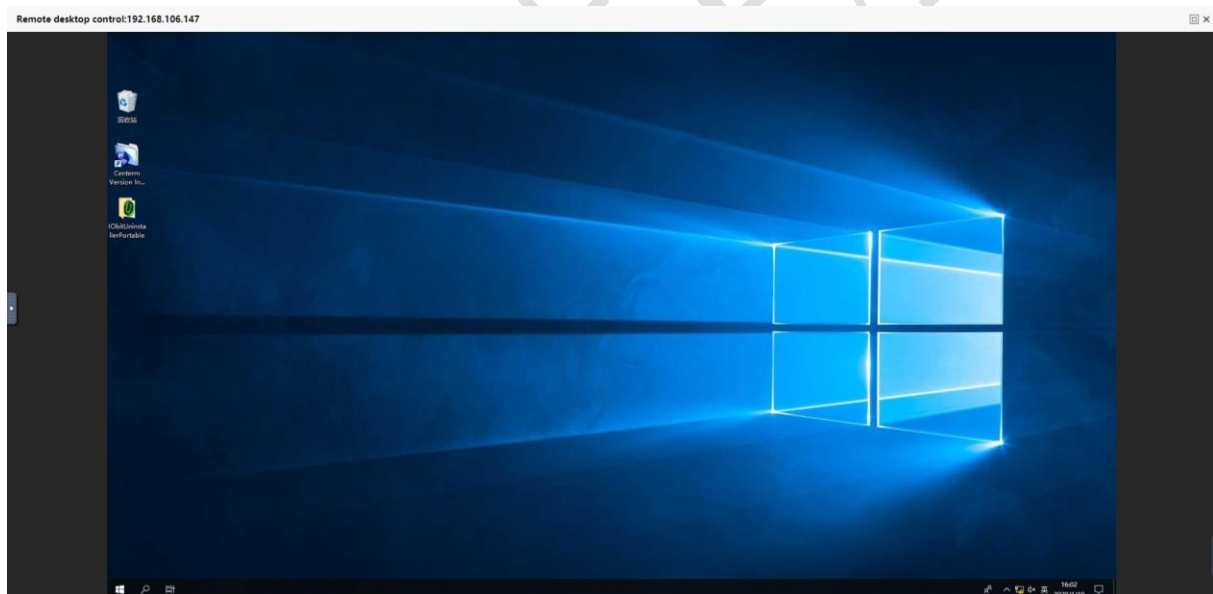


Moreover, input 'about:config' in Firefox URL, then setup security.mixed_content.block_active_content to false; after that, save settings to reboot browser for taking effect.

1. The following prompt would be shown on in client if remote assistance starts working



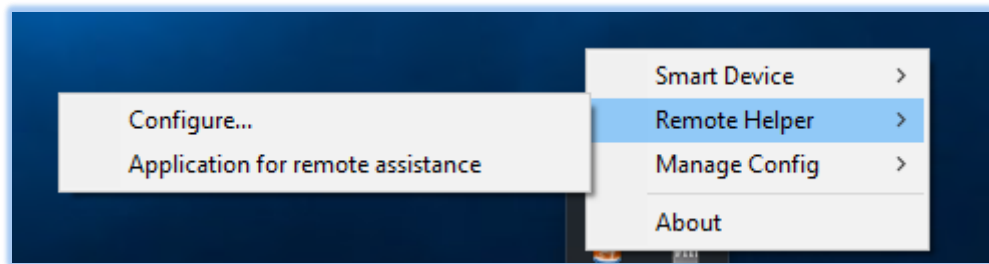
2. After click 'Accept' monitoring to client can work, the view is shown as be below



3.4.1 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.



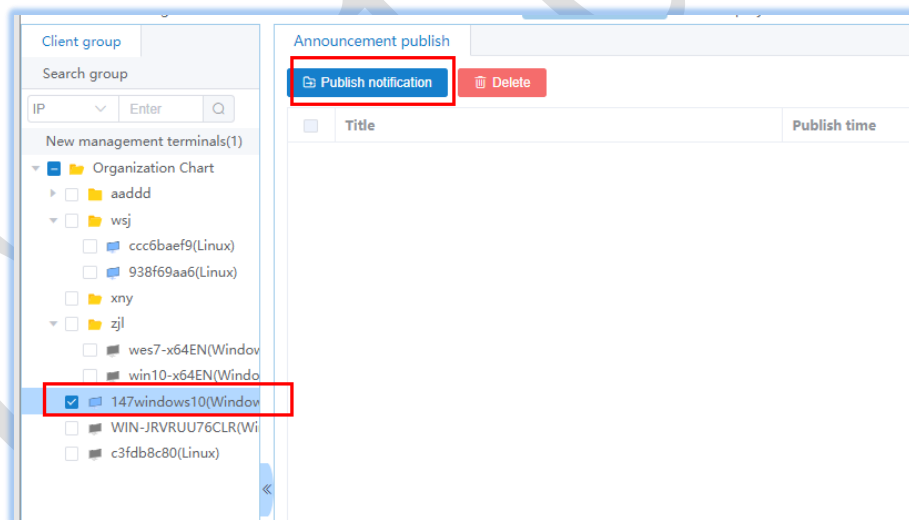
When the remote assistance request is sent from client, corresponding request item will be displayed in the list on “request processing” tab page; the administrator can select to accept or refuse the request.

3.5 Notice publishing

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.

3.5.1 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:

Publish notification

* Title

Xi gathers with non-Communist party leaders, perso

Title cannot be empty

B

T

I

U

S

ClieChinese President Xi Jinping on Tuesday gathered with leaders from non-Communist parties and the All-China Federation of Industry and Commerce (ACFIC), as well as personages without party affiliation ahead of the Spring Festival.

☐ Pop-up windows immediately

Publish

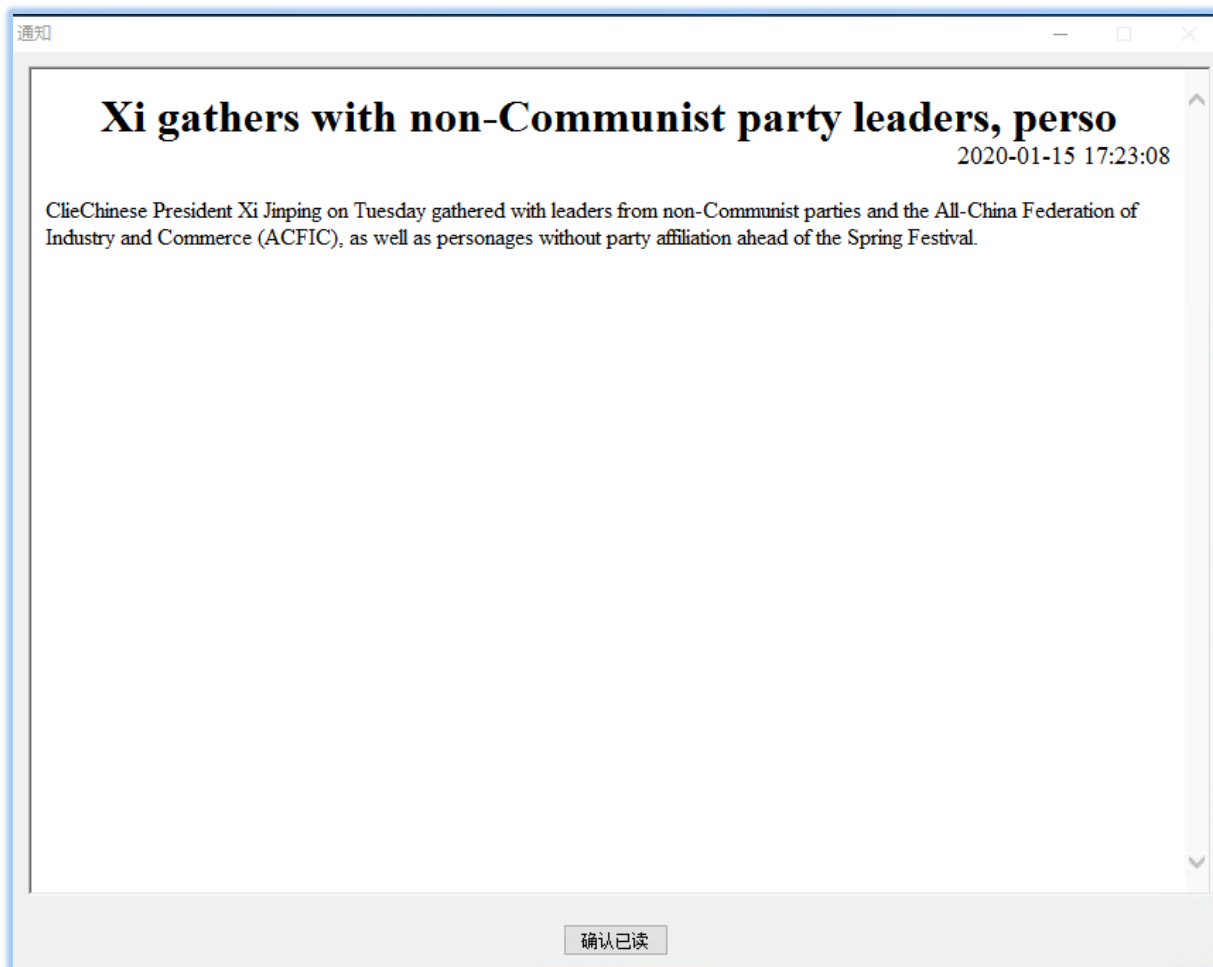
Cancel

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

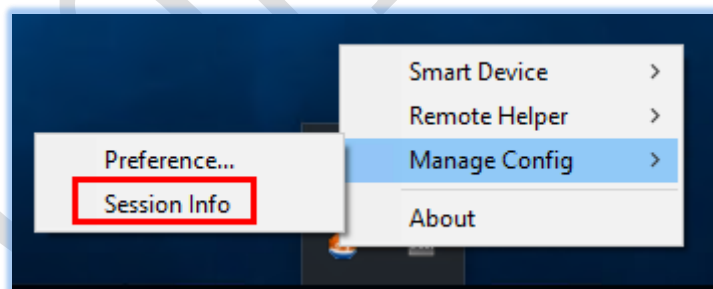
- Not forcibly pop up the notice: inform the user in notice bar of client in icon flashing mode. The notice will be popped up by double-click of user.
- Forcibly pop up the notice: directly pop up the notice in client. It is applicable to important message.

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.





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



3.5.2 View the publishing 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

Announcement publish						
Publish notification		Delete				
☐ Title	Publish time	Target client amount	Sent	Confirmed	Statistics detail	
☐ Xi gathers with non-Communist party leaders, perso	2020-01-15 17:23:09	1	1	0	View	

Publish notification

* Title

B **T** *I* U ~~S~~    

ClieChinese President Xi Jinping on Tuesday gathered with leaders from non-Communist parties and the All-China Federation of Industry and Commerce (ACFIC), as well as personages without party affiliation ahead of the Spring Festival.

☐ Pop-up windows immediately

[Confirm](#)

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.

Announcement publish						
Publish notification		Delete				
☐ Title	Publish time	Target client amount	Sent	Confirmed	Statistics detail	
☐ Xi gathers with non-Communist party leaders, perso	2020-01-15 17:23:09	1	1	0	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.

Announcement publish						
Publish notification		Delete				
☐ Title	Publish time	Target client amount	Sent	Confirmed	Statistics detail	
☐ Xi gathers with non-Communist party leaders, perso	2020-01-15 17:23:09	1	1	0	View	

View ×

Export

Resend all

Client IP

▼

Enter

Q

Client IP	Subordinated group	Send status	Confirm status	Confirm time
192.168.106.147	Organization Chart	Sent	Confirmed	2020-01-15 17:27:06

3.6 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.

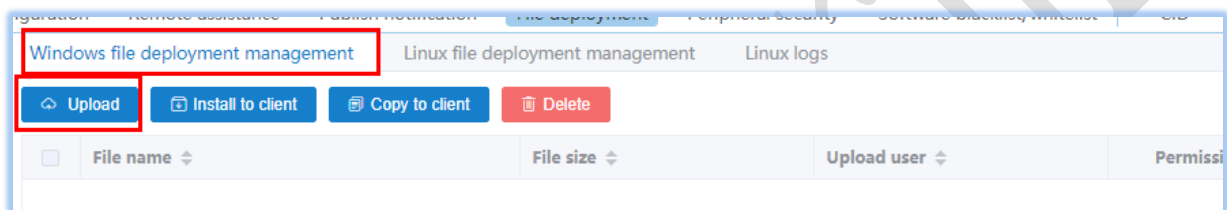
3.6.1 Windows file deployment management

3.6.1.1 Upload file

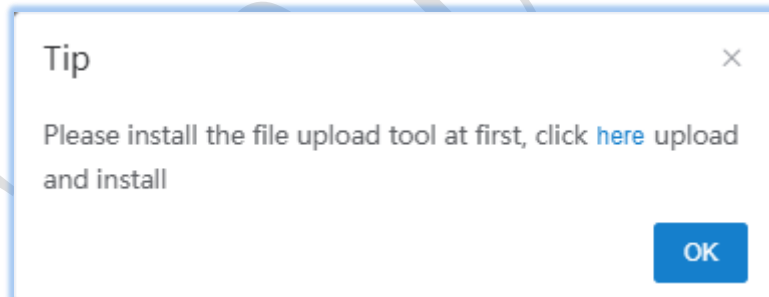
1. Initialize the upload environment

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:



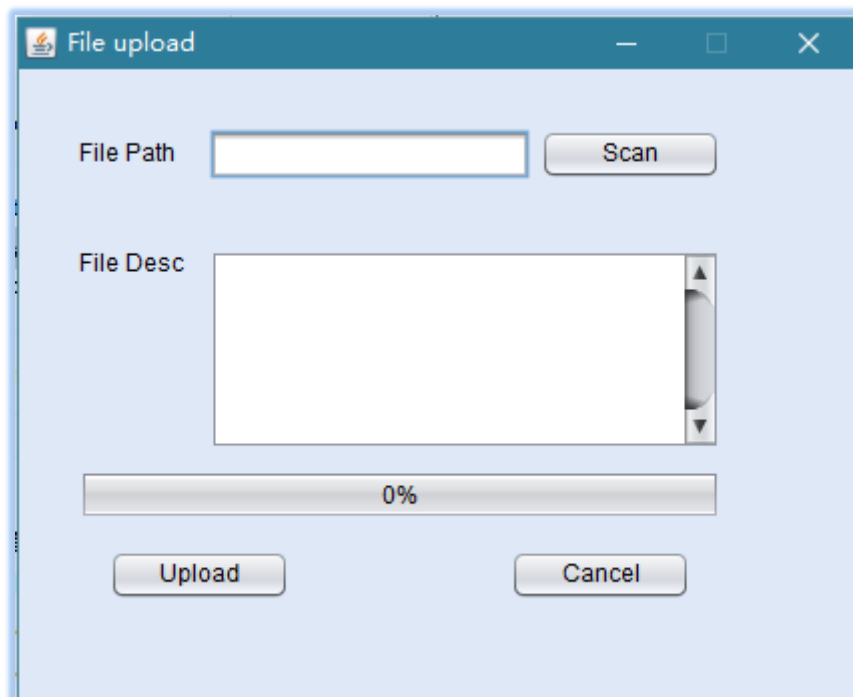
Click download and install JRE. Then, restart the browser.

2. Initialize the upload component

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

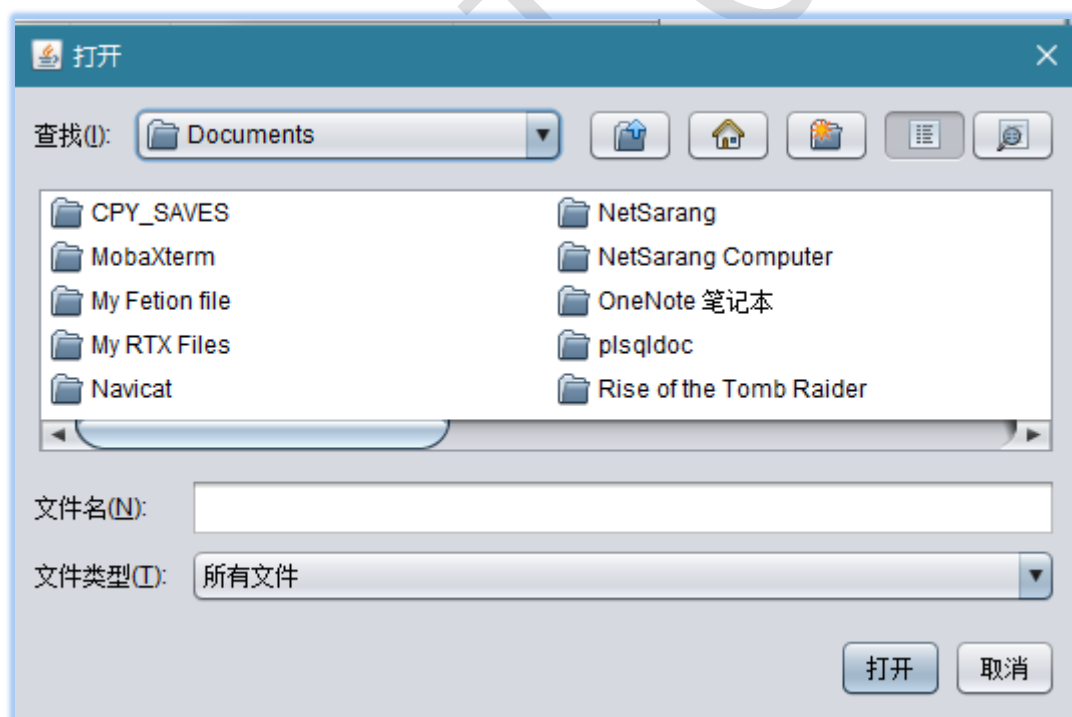


The upload interface after initialization is as follows:

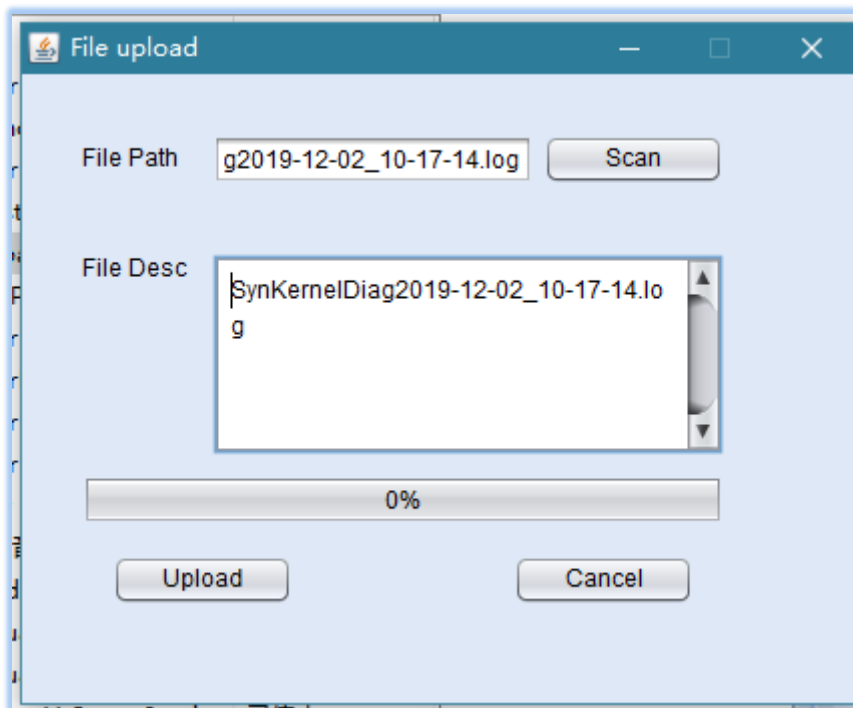


Select the file to be uploaded

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



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



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

Windows file deployment management

Linux file deployment management

Linux logs

Upload

Install to client

Copy to client

Delete

Only the shared file can be searched by others

Upload u

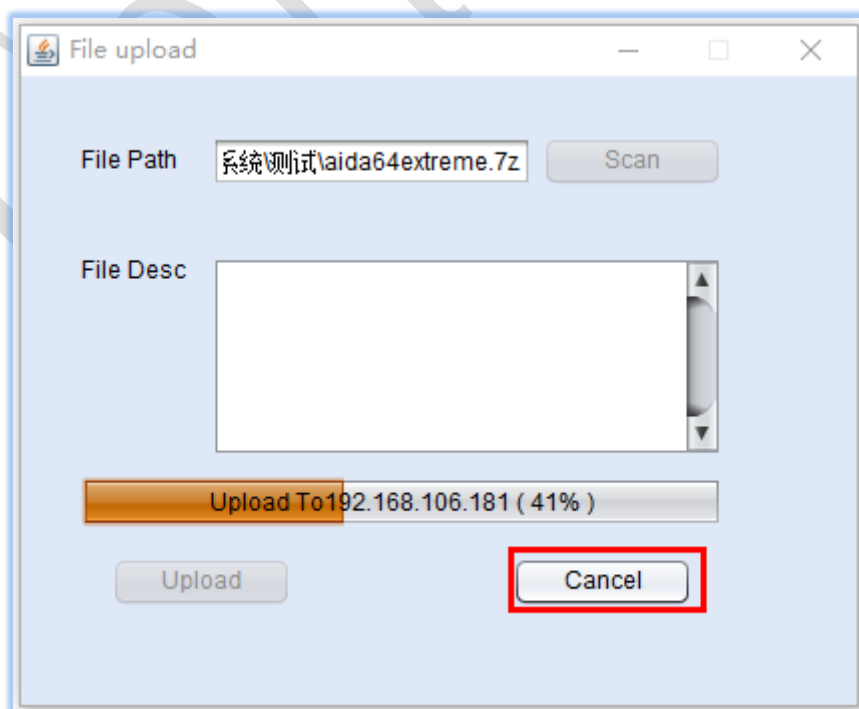
cz

Q

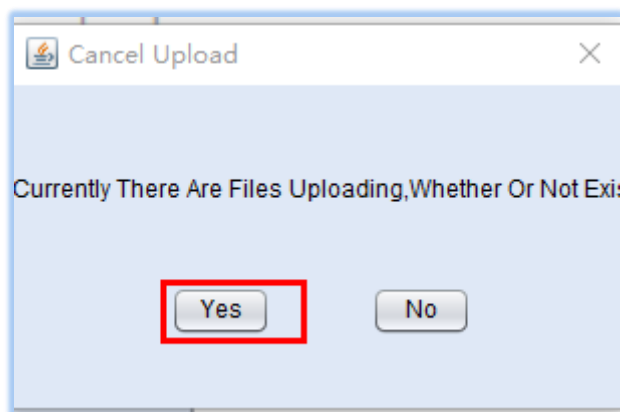
☐	File name	File size	Upload user	Permission	Upload time	Download	File description
☐	SynKernelDiag2019-12-02_10-19-14.log	636.1K	cz	Private	2020-01-15 17:34:31	Download	SynKernelDiag2019-12-02_10-19-14.log

Cancel upload

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



Select "Yes" to exit the upload.

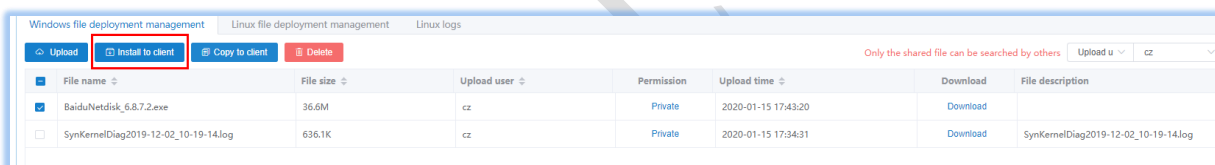


3.6.1.2 Software installation

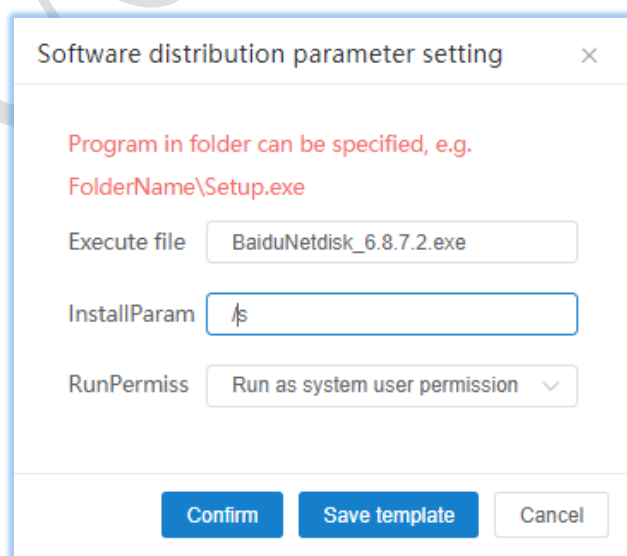
Software installation refers to distribution of software stored in the server to the client as well as installation operation. The traditional software distribution, as for system administrator, is distribution of the updated software to many work stations, which is undoubtedly the most tedious task. 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:



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



The description of installation parameters is as follows:

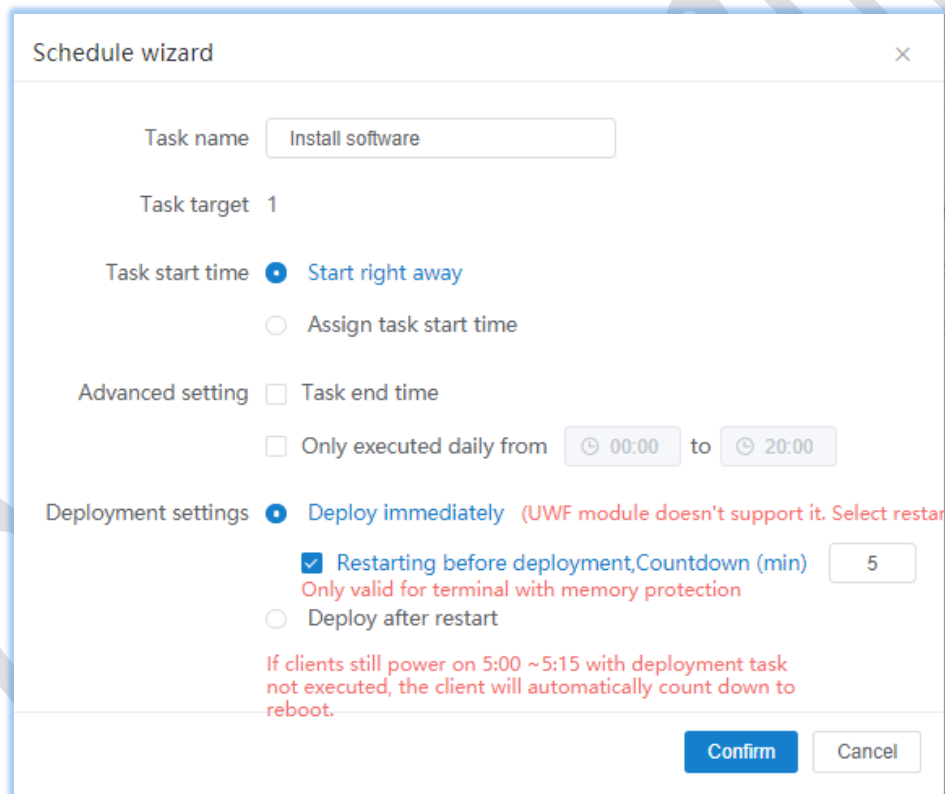
This item is option and is the parameters used during installation of software in client. It is empty by default, which refers to the non-silent installation and may require manual intervention. The parameters of different software are different (in general situation, the parameters aren't used). If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

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

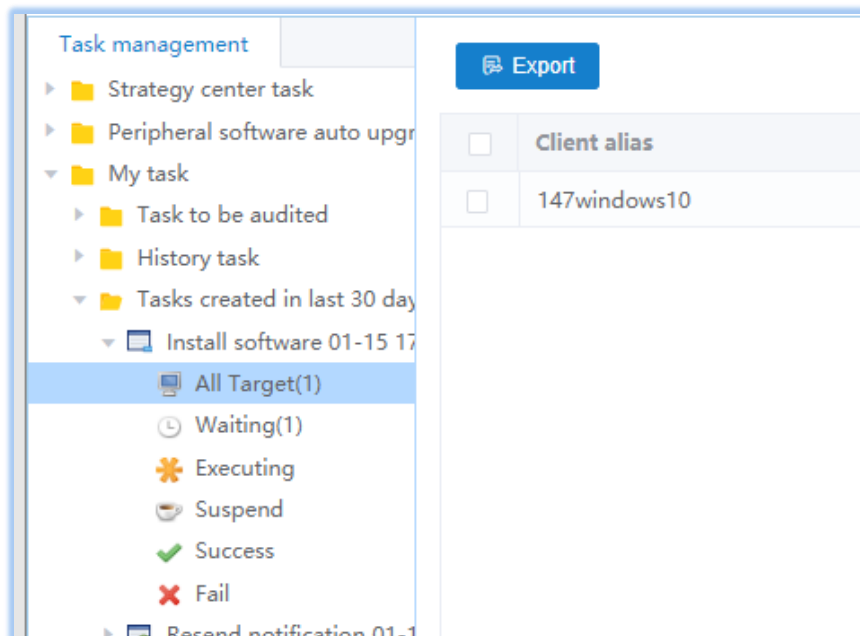
- /quiet quiet mode without user interaction
- /passive no participation mode-only display the process bar
- /q[n|b|r|f] set the user interface class n –no user interface; b –basic interface r –refined interface f –finished interface (default)

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.



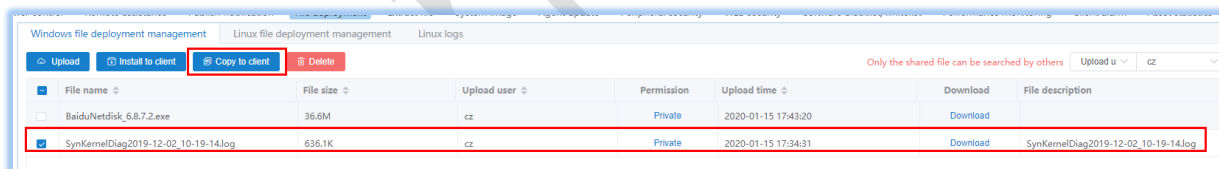
The results and process information of software distribution are displayed on the task execution state panel, as shown in the following figure:



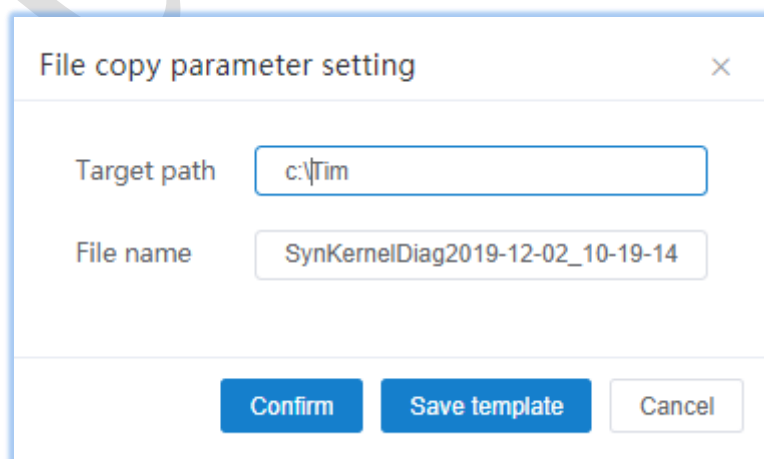
3.6.1.3 Copy file

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.



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



3. Configure the plan wizard and execute the task

Schedule wizard

×

Task name

Copy file

Task target

1

Task start time

☒ Start right away
 ☐ Assign task start time

Advanced setting

☐ Task end time
 ☐ Only executed daily from

00:00

 to

20:00

Deployment settings

☒ Deploy immediately (UWF module doesn't support it. Select restart)

☒ Restarting before deployment, Countdown (min)

5

 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.

Confirm

Cancel

3.6.2 Linux Patch Update

3.6.2.1 Upload patch

1. When the terminal needs to update to a new version, you must use the update file provided by Centerm Information.
2. You need to check first whether the terminal has bind a usable storage node
3. Enter the "file deployment->Linux file management" module
4. Click the "Upload file" button, as below shows:

Windows file deployment management

Linux file deployment management

Linux logs

File name

Upload user

cz

Upload time

Start Date

to

End Date

Query

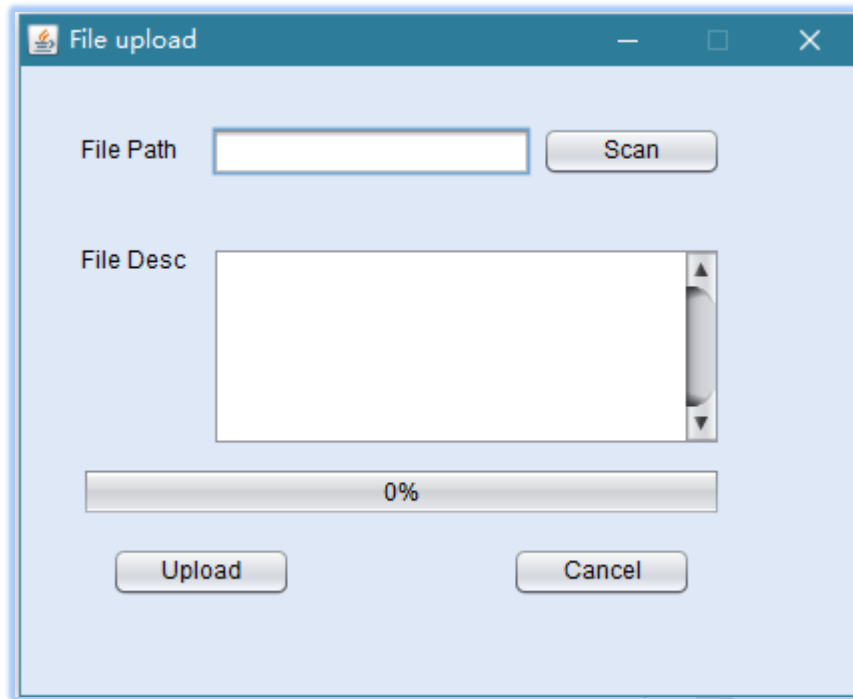
Upload

Update patch

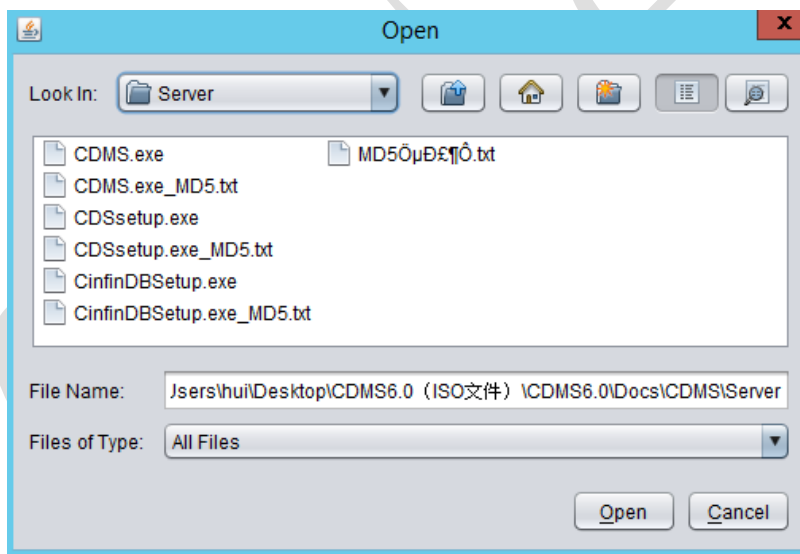
Update system

Delete file

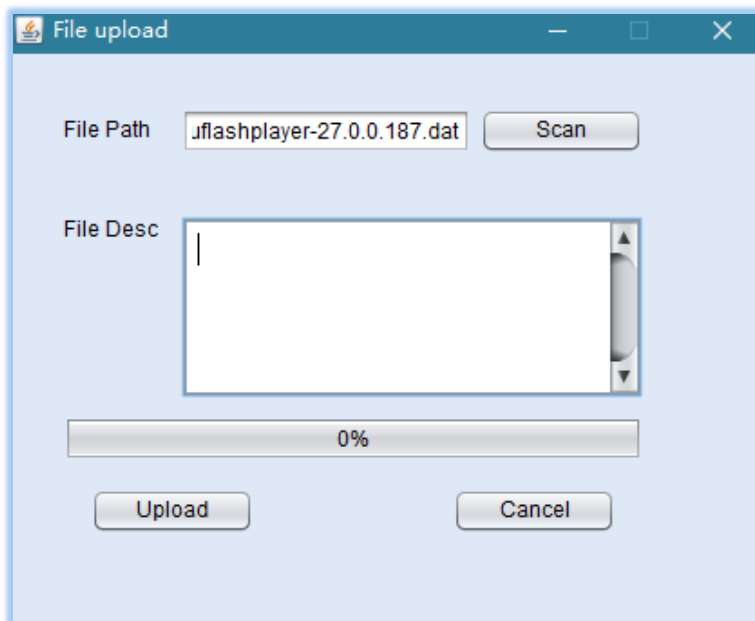
File name	File type	Version information	Suitable system version	Applicable model	File size	Upload user	Upload time	File description	Status
-----------	-----------	---------------------	-------------------------	------------------	-----------	-------------	-------------	------------------	--------



Click the “Browse” button and select the patch file to upload. The patch file must be .dat format file.



5. Fill the file description in the “File Desc” box and click “upload”, then the file will begin upload.

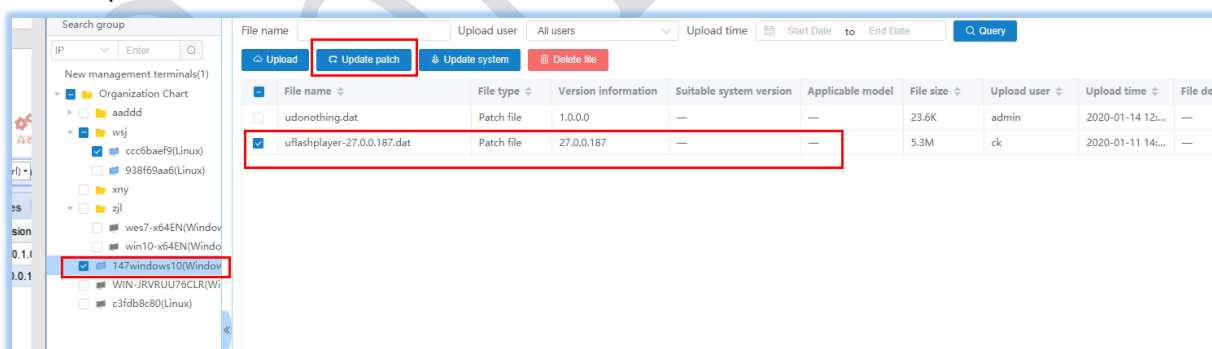


6. After the successful upload, the file list would add the uploaded file, as below shows:

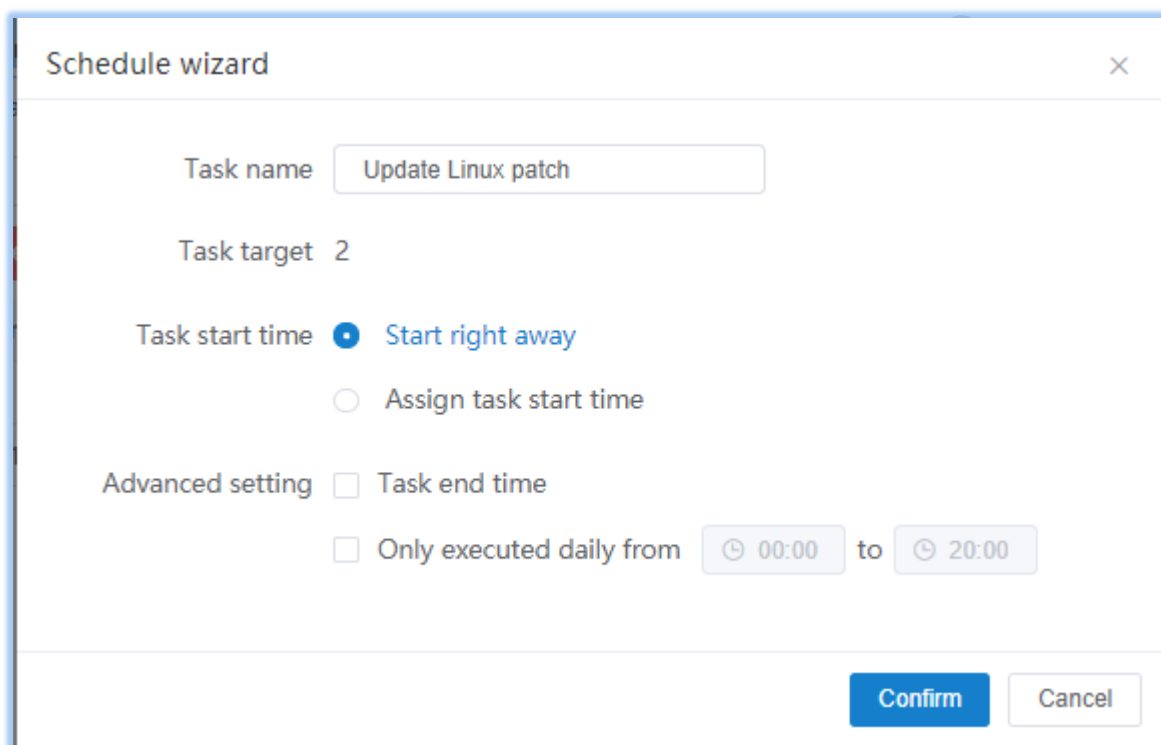
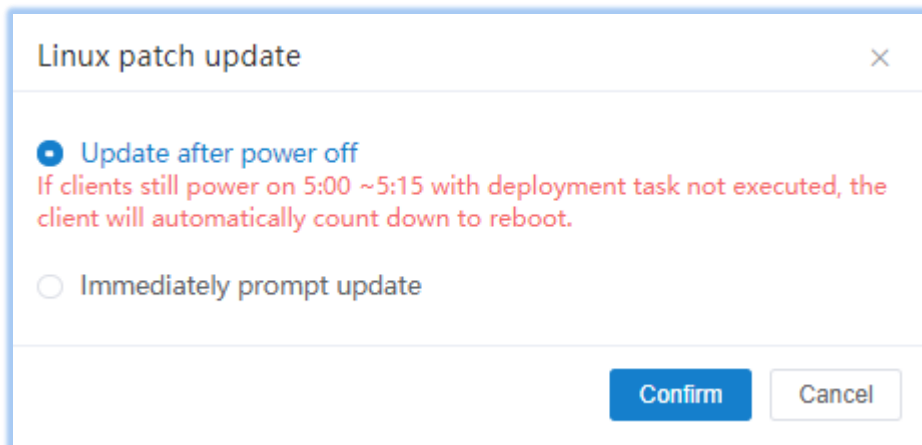
File name	File type	Version information	Suitable system version	Applicable model	File size	Upload user	Upload time	File description	Status
udonothing.dat	Patch file	1.0.0.0	—	—	23.6K	admin	2020-01-14 12:...	—	Unzip complete
uflashplayer-27.0.0.187.dat	Patch file	27.0.0.187	—	—	5.3M	ck	2020-01-11 14:...	—	Unzip complete

3.6.2.2 Distribute the patch

1. Select the uploaded patch file, select the terminal to update and click “update patch”.

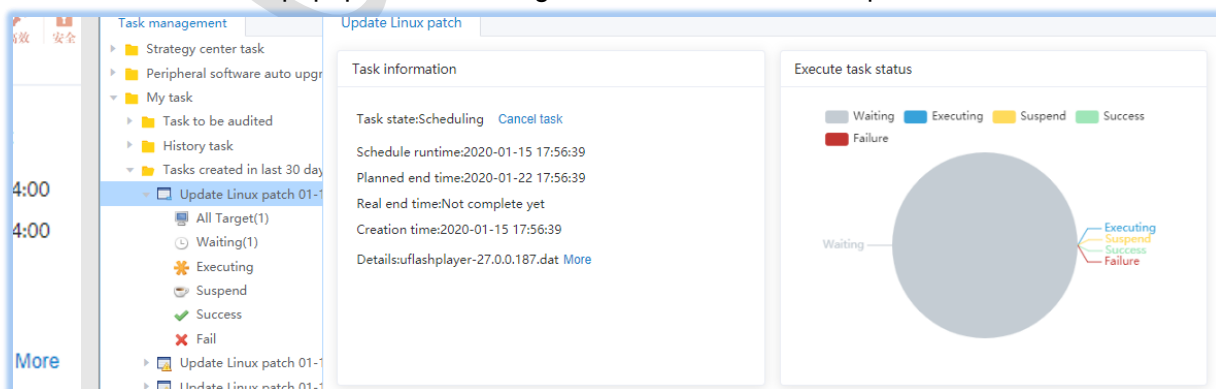


2. In the popup window, configure the task's execution option.



3.6.2.3 Check the result

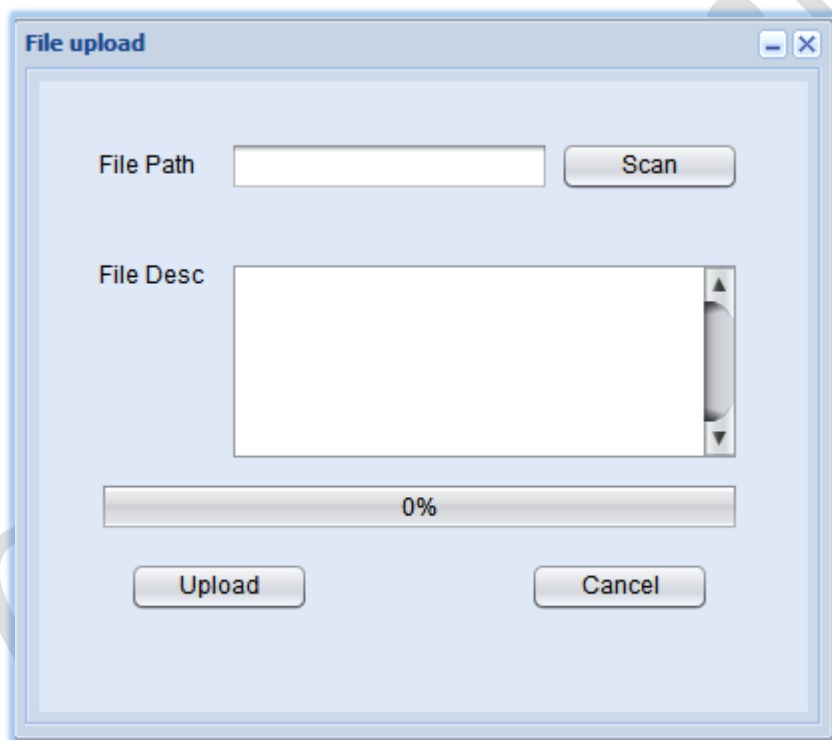
1. In the popup window, configure the task's execution option.



3.6.3 Linux System update

3.6.3.1 Upload update file

1. When the terminal needs to update to a new version, you must use the update file provided by Centerm Information.
2. You need to check first whether the terminal has bind a usable storage node
3. Enter the “file deployment->Linux file management” module
4. Click the “Upload file” button, as below shows:

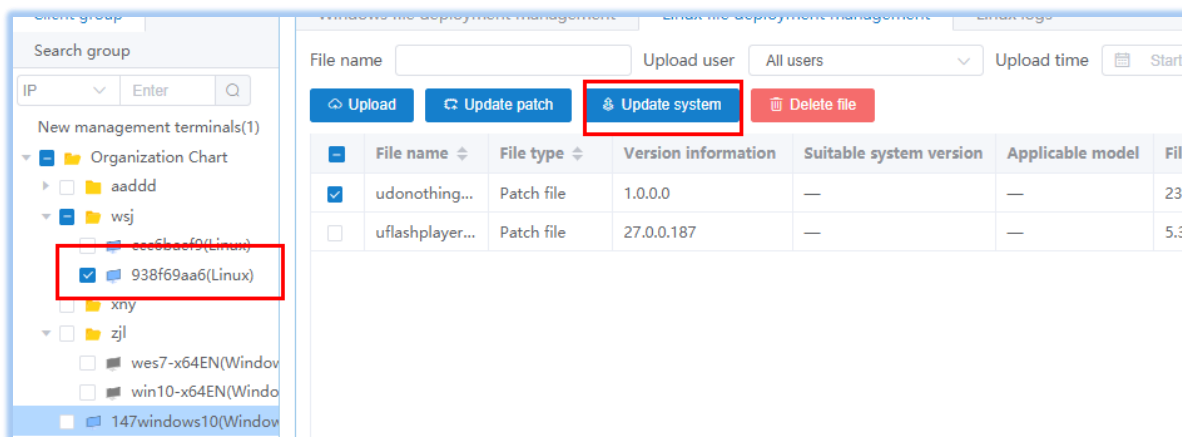


5. Click the “Browse” button and select the patch file to upload. The patch file must be .dat format file. After the successful upload, the file list would add the uploaded file, as below shows:

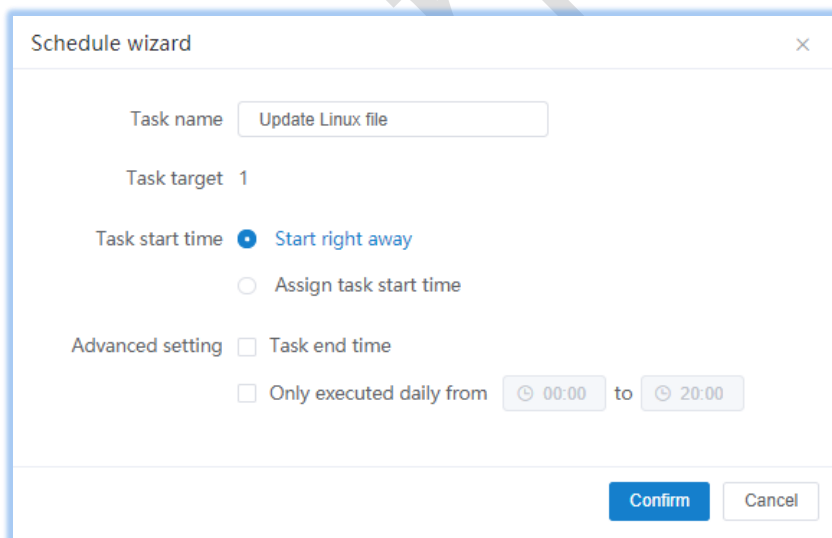
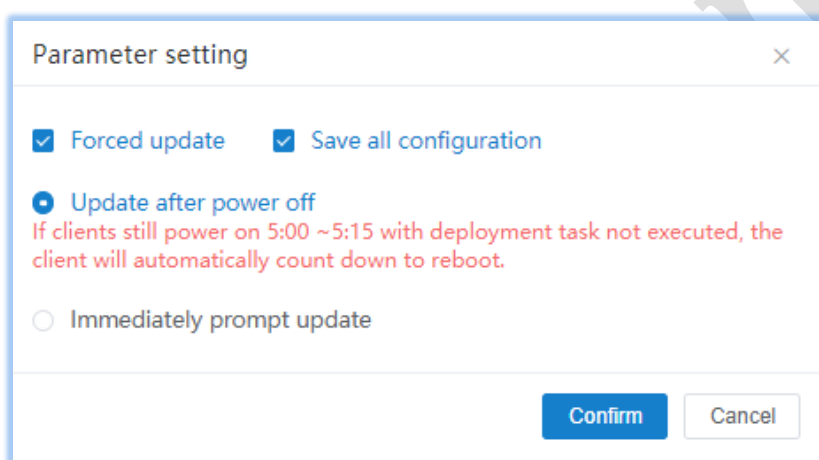
Upload file Update patch Update system Delete Files Search									
	File name	File type	Version	OS version	Model	File size	Uploaduser	Uploadtime	File description
☒	1 uflashplayer-27.0.0.187.dat	Patch file	27.0.0.187			5.3M	admin	2018-06-13 11:22:06	升级补丁

3.6.3.2 System update

1. Select the uploaded patch file, select the terminal to update and click “update system”.



2. In the popup window, configure the task's execution option.



3.6.3.3 Check result

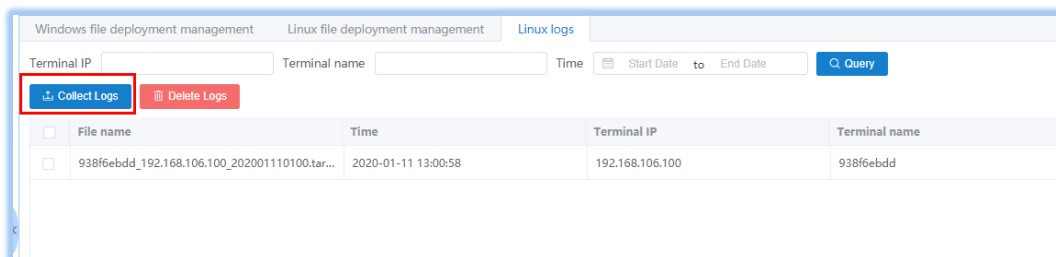
Enter "Task Management" module and check whether the client update task is successful.

3.6.4 Linux log

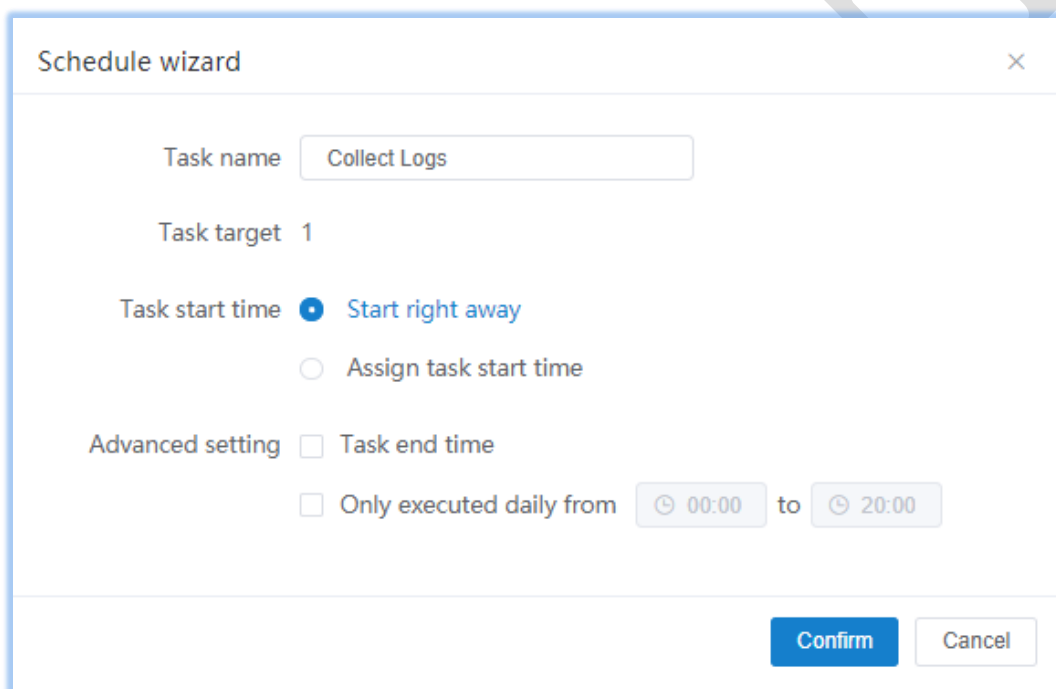
This feature can be used to extract the running logs directly when the administrator needs to obtain them locally from the client. This feature is only available for Linux clients. Operation steps:

3.6.4.1 Log extraction

1. Select one terminal and click “Collect Logs” button, then browse and select the file or file folder to be extracted.

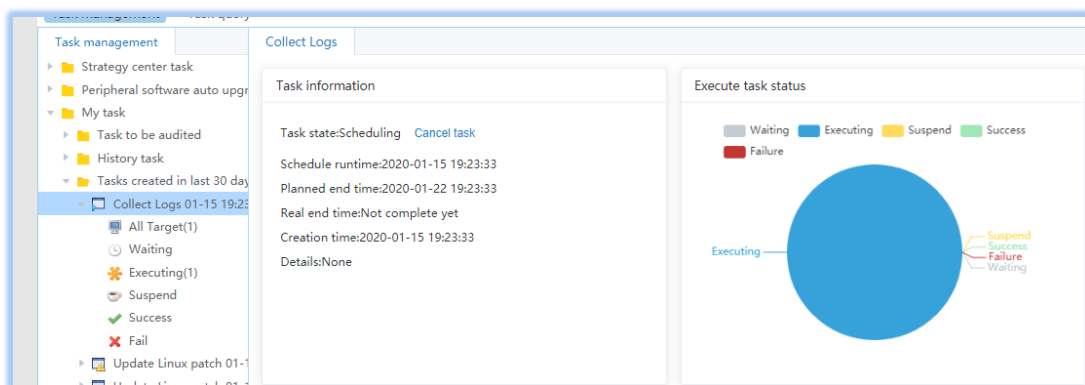


2. Click “finished” to finish the task creation.



3.6.4.2 Check result

Enter “Task Management” module and check whether “Collect Logs ” task is successful.



2. Enter File deployment->Linux Log module and check whether there is extracted log files.

Terminal IP

Terminal name

Time

Start Date to End Date

Q Query

Collect Logs

Delete Logs

☐	File name	Time	Terminal IP	Terminal name	App	Operation
☐	938f6ebdd_192.168.106.100_2020011110100.tar...	2020-01-11 13:00:58	192.168.106.100	938f6ebdd	TC	Download

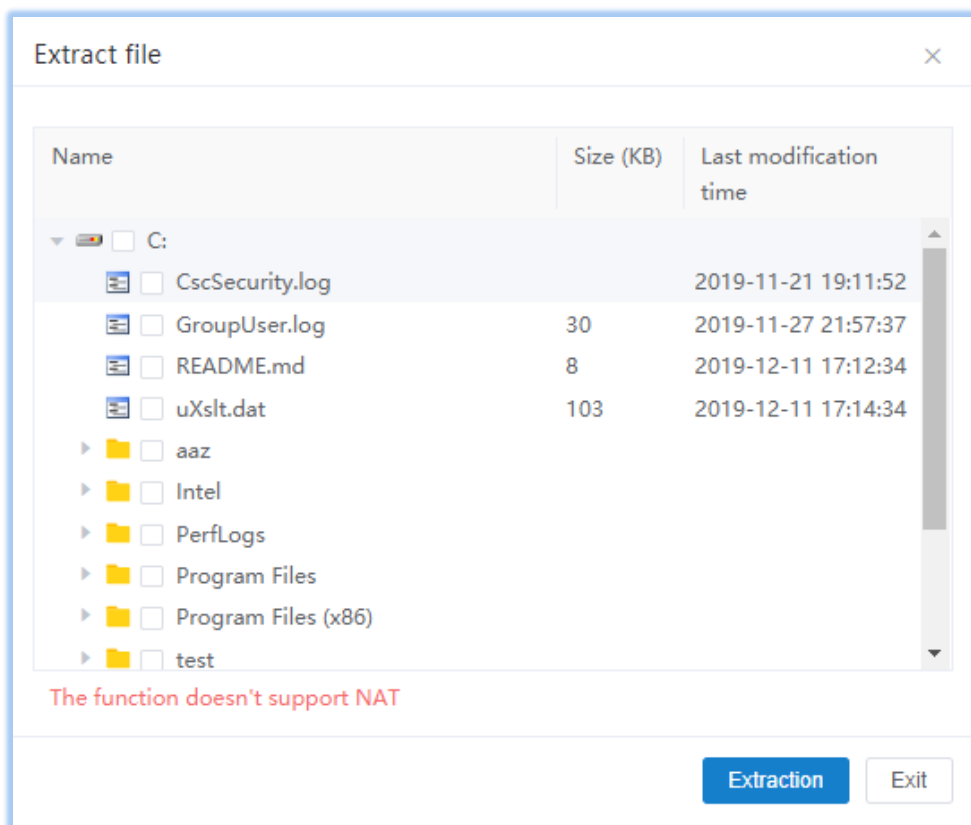
3.6.4.3 Log check

Click "download" to download the log to local system and you can check the log.

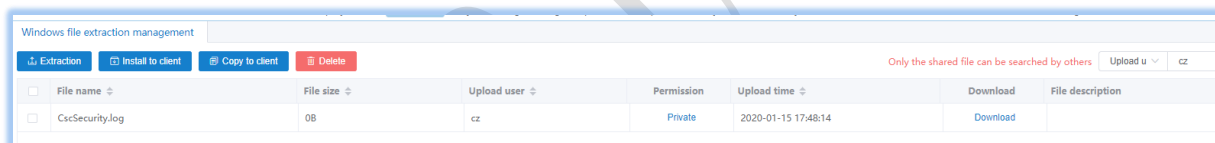
3.7 Client upgrade

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.**

Windows file extraction management						
Extraction Install to client Copy to client Delete						
Only the shared file can be searched by others						
Upload us	cz					
File name	File size	Upload user	Permission	Upload time	Download	File description



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.



3.7.1.1 Description on 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.

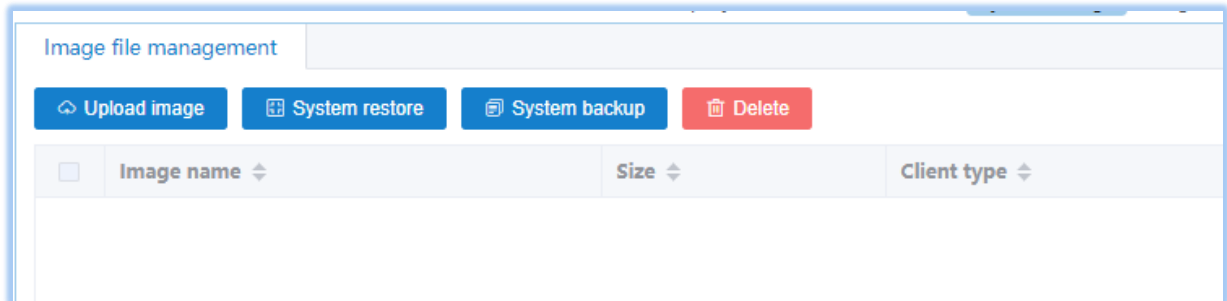
- Main version files: the complete client installation package. The server shall have these files. Otherwise, the upgrade function cannot be used;
- Patch files: the patch of client software and the non-complete installation package. The files are not necessarily uploaded to the server.

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.

3.7.2 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.**

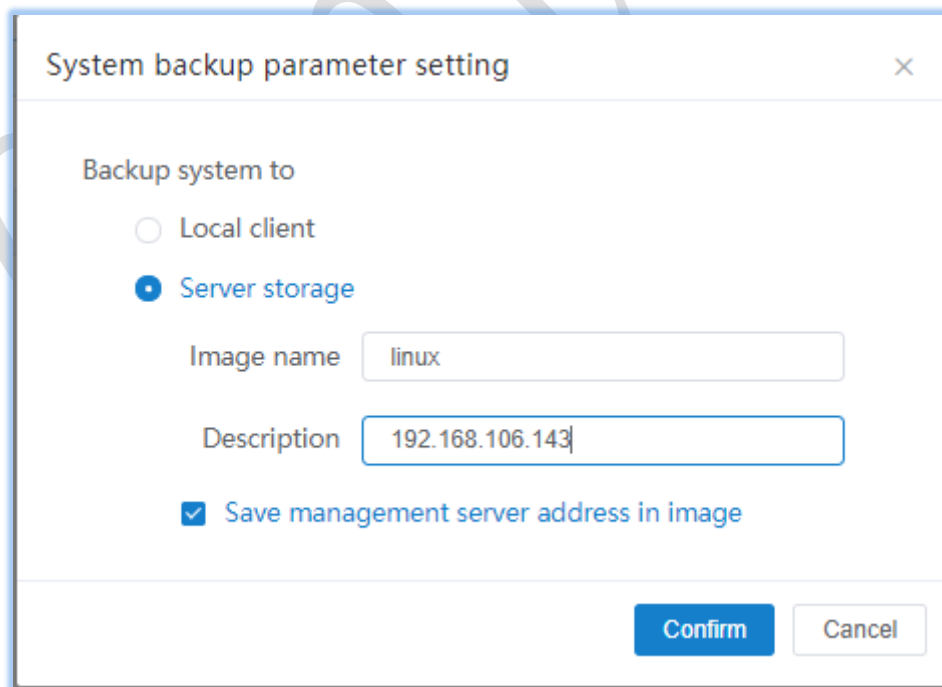
1. Select the client and click "system backup" button.



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.



Click "OK" button and configure the plan wizard.

Schedule wizard

Task name

System backup

Task target

1

Task start time

☒ Start right away
 ☐ Assign task start time

Advanced setting

☐ Task end time
 ☐ Only executed daily from

00:00

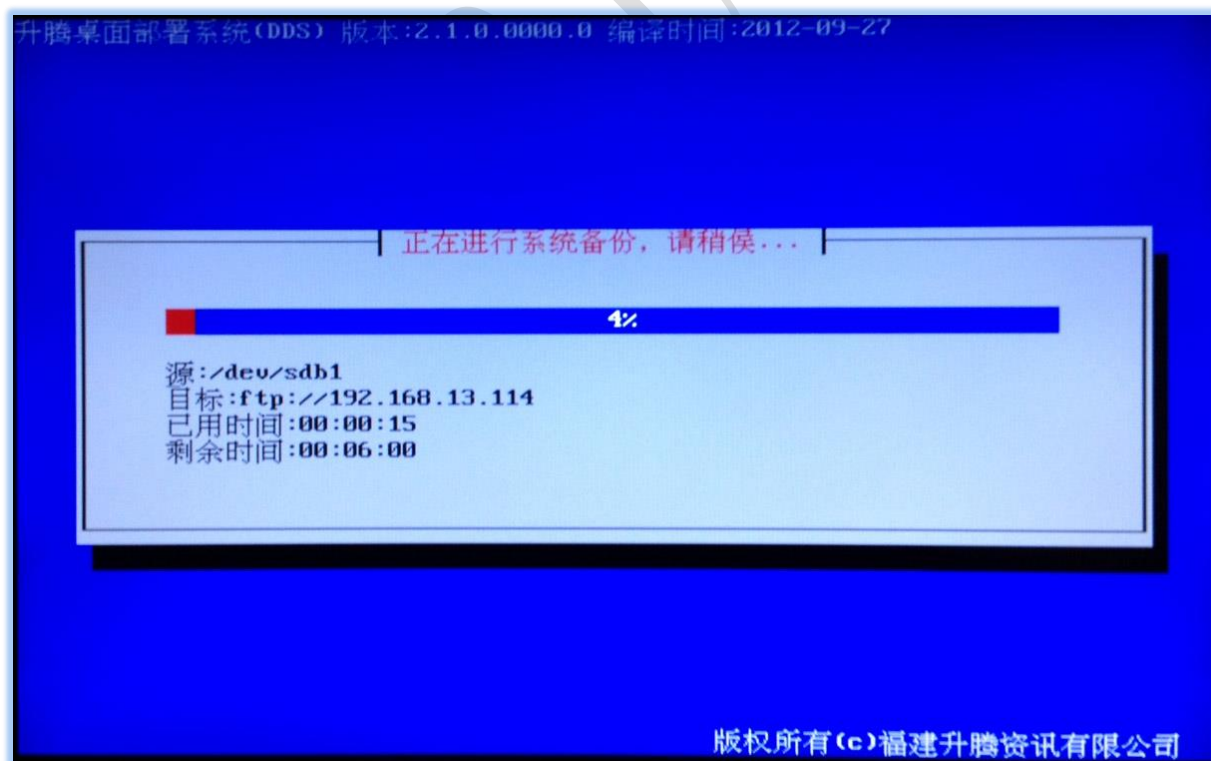
 to

20:00

Confirm

Cancel

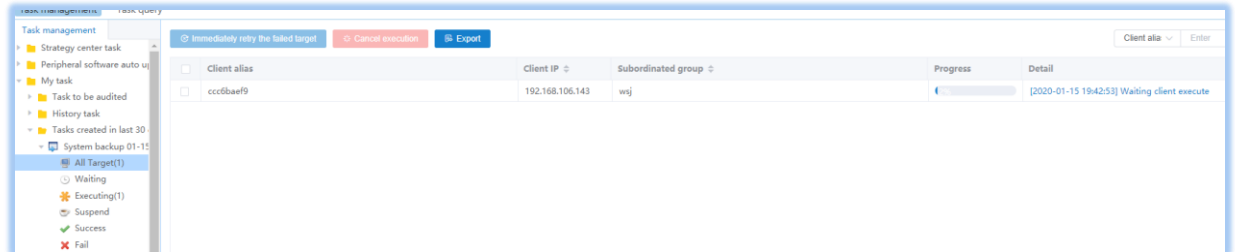
After the local partition of client receives the command, the client will firstly restart to clean the dirty data; after entering the desktop, the desktop will display "image backup preparing"; next, the client will restart second time to enter the backup interface:



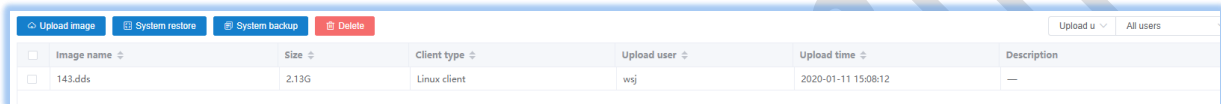
Notice:

- 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.

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



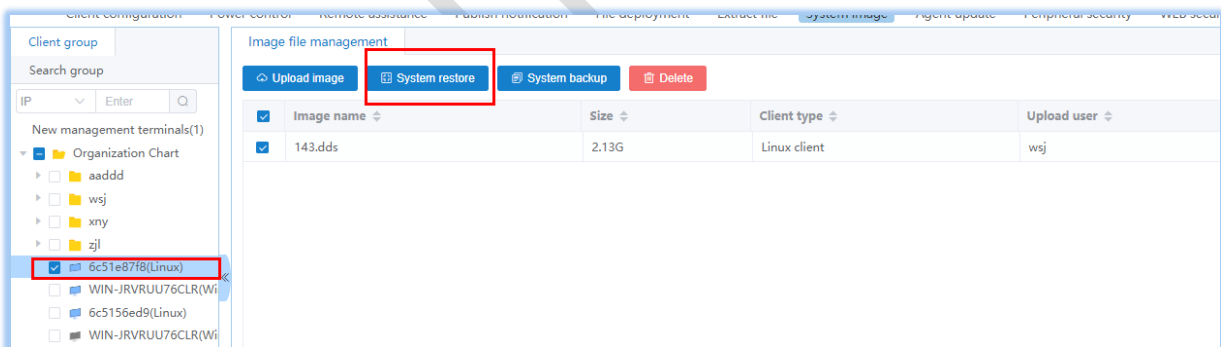
After backup, the backed up image file is shown in image list:



3.7.3 System restore

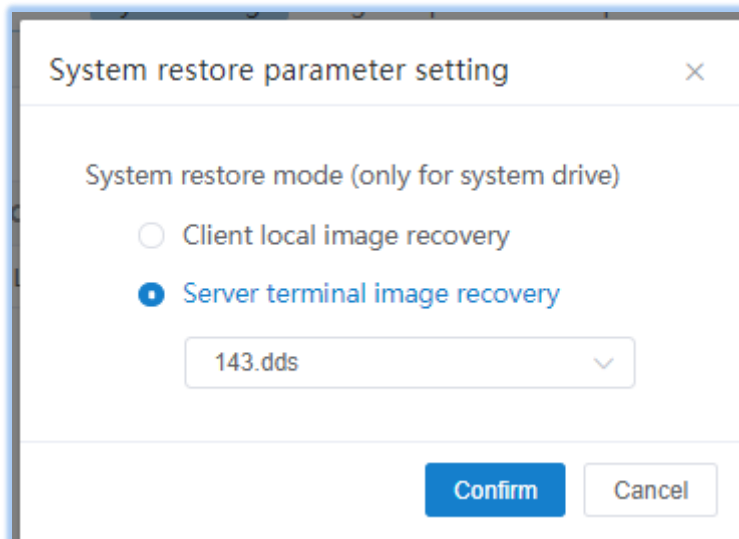
If the client executed the system backup, the system can restore OS of client by system restore function. **Notice: "system restore" only can restore the system disk.**

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.

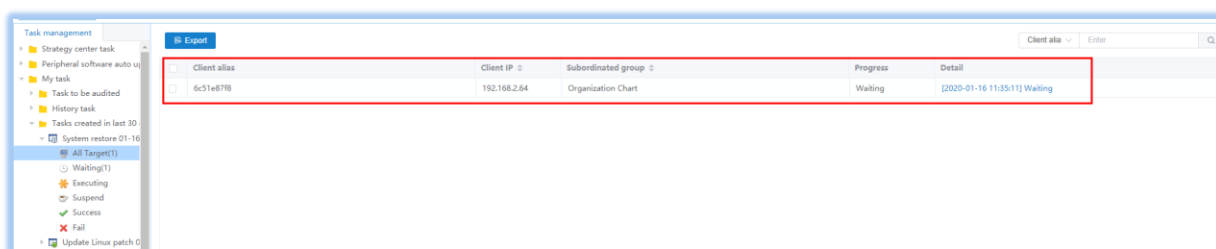
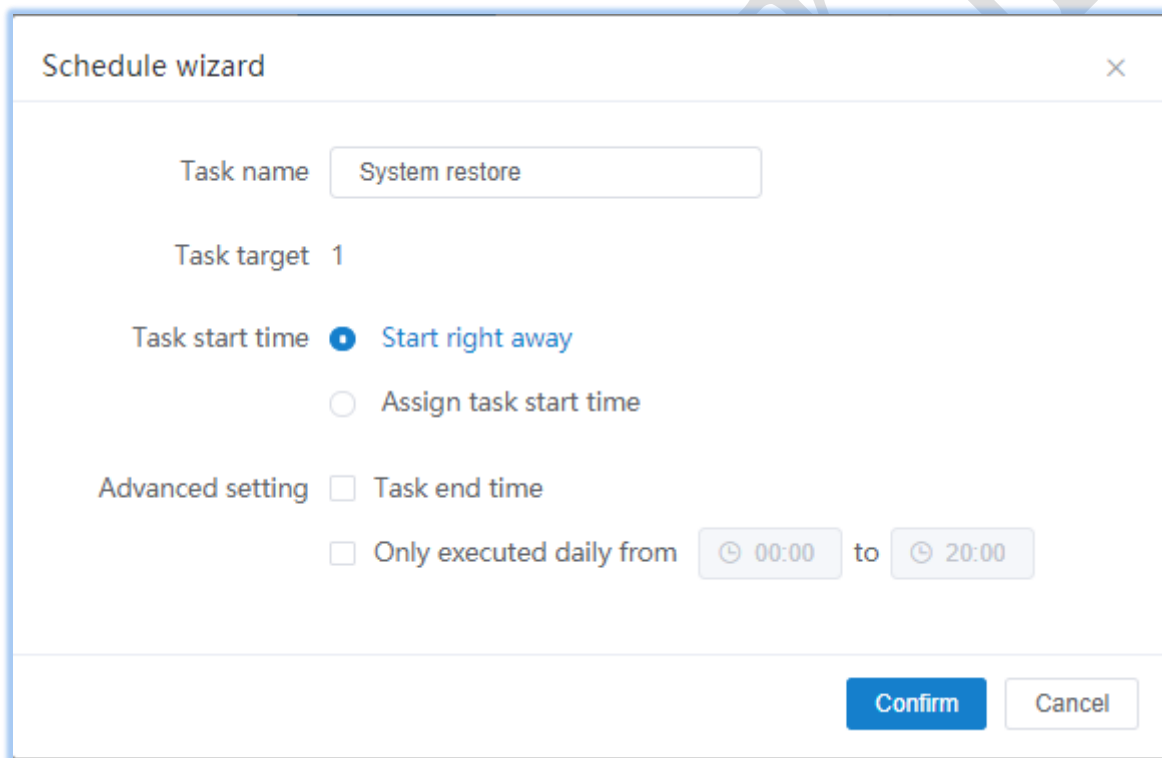


2. In the popup dialog box, select the restore mode. Local image restore of client shall ensure the existence of backed up image in local client. Otherwise, the restore will be in failure.

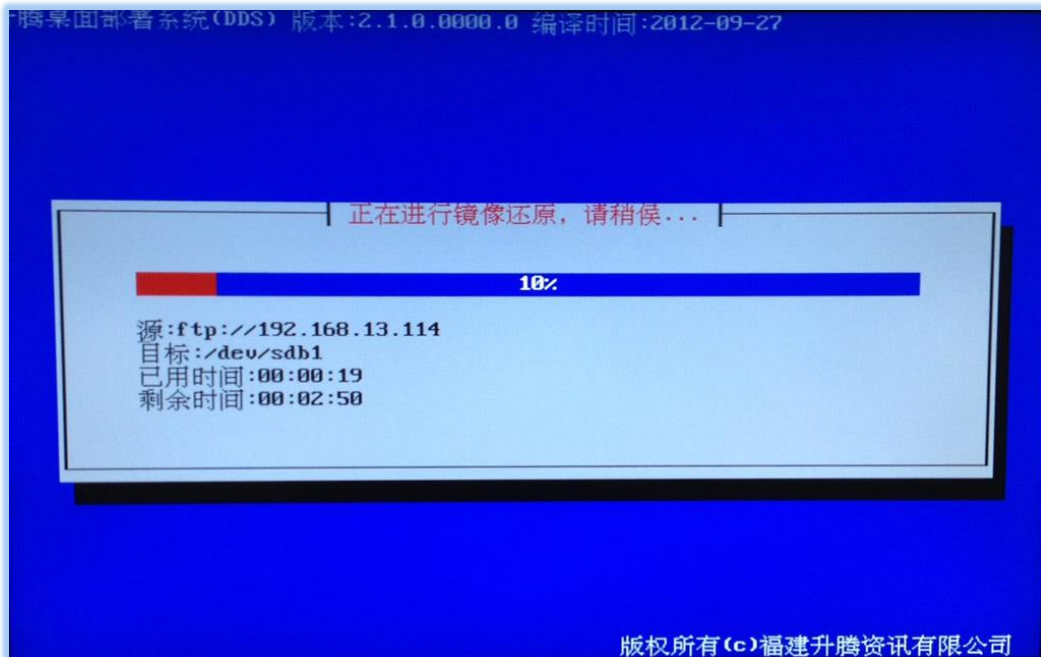
The following figure demonstrates the restore by server image. Select the image file to be used from the list.



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



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:

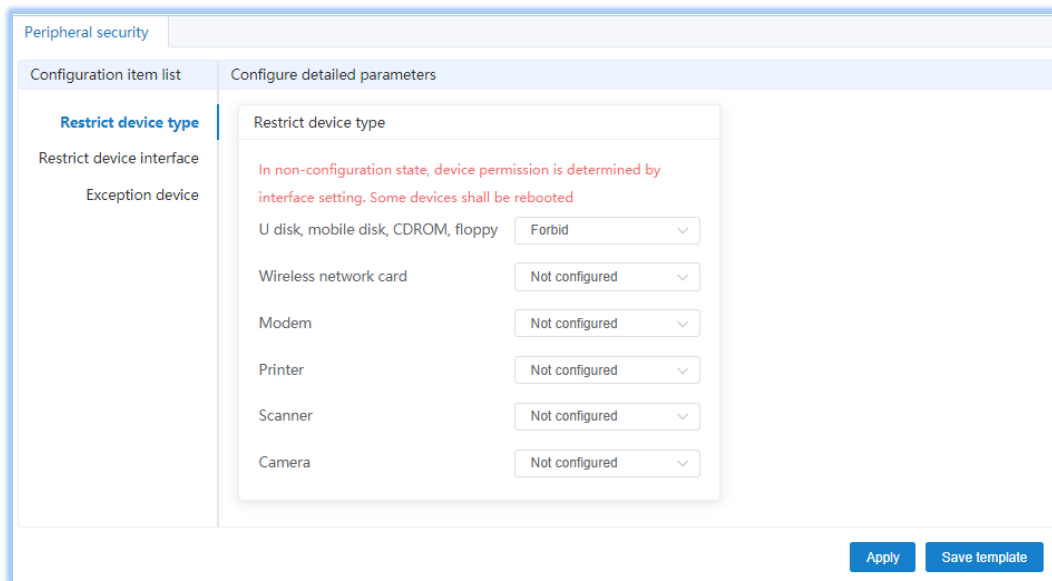


3.8 Peripheral Security

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.

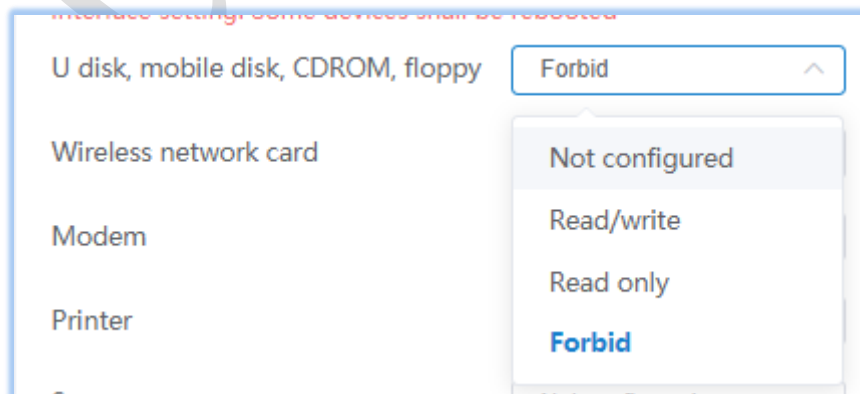
3.8.1 Restriction to device type

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



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

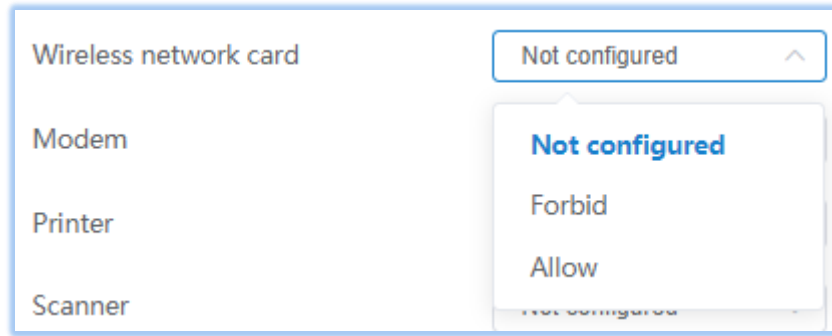
- Not configured: not limit the device;
- Read/write: normally read and write in the device;
- Read only: only read the data in the device rather than write;
- Forbid: prohibit any using operation of the device;



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;



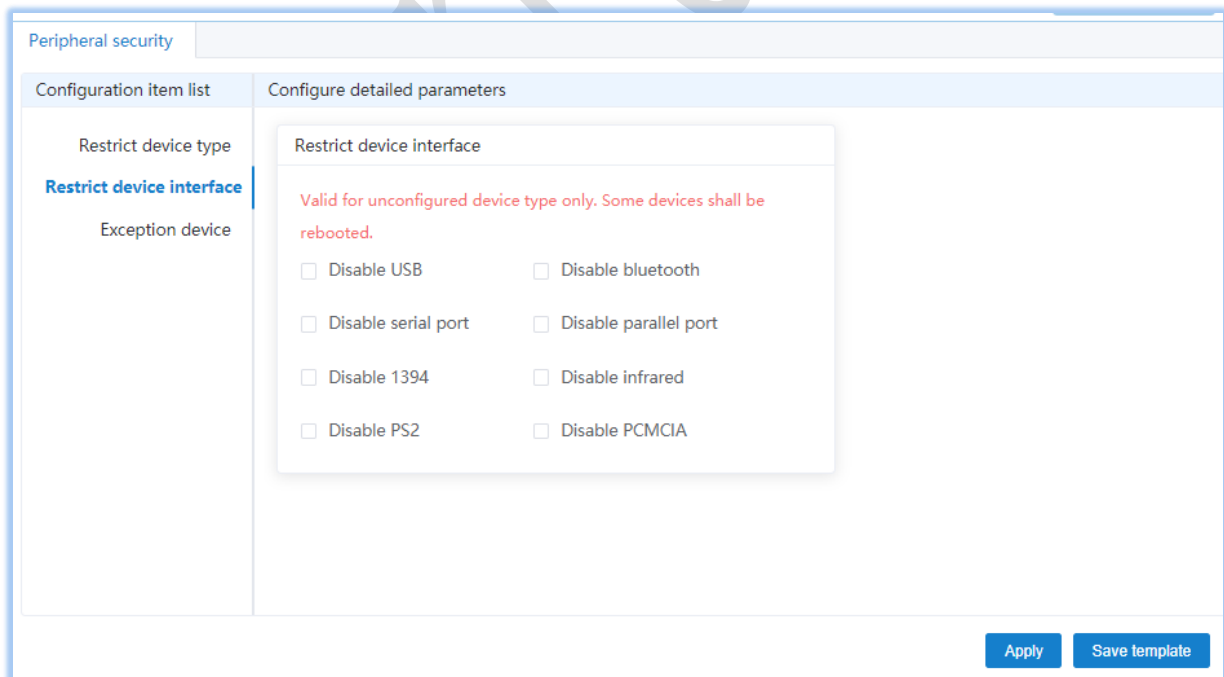
Notice:

- 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.

3.8.2 Restriction to 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:



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.

3.9 Windows 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.

3.9.1 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.

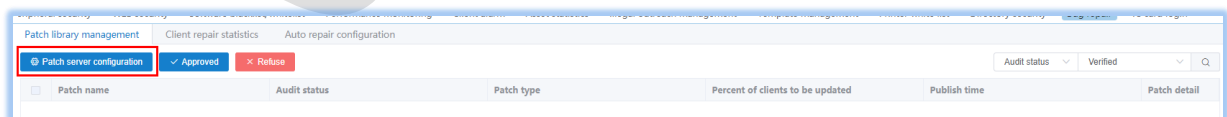
If the administrator needs to fix the vulnerabilities of XP and WIN7 clients, only the Microsoft patches are enough. If the administrator needs to fix the vulnerabilities of Centerm XPE and WES7 clients, we suggest using Centerm patch server to fix.

3.9.1.1 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

Server address

192.168.4.209

Port

80

System username

administrator

System password

.....

Test

Confirm

Cancel

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.

Patch library management

Client repair statistics

Auto repair configuration

Patch server configuration

✓

Approved

✗

Refuse

Audit status

Verified

Q

☐	Patch name	Audit status	Patch type	Percent of clients to be updated	Publish time	Patch detail
☐	系统恢复增强功能更新	Verified	关键更新程序	0%	2003-02-19 12:02:38	View
☐	Q311967: 安全更新	Verified	安全更新程序	0%	2003-02-19 12:30:33	View
☐	Q320174: 关键更新	Verified	关键更新程序	0%	2003-02-20 19:16:48	View
☐	安全更新, 2002 年 2 月 13 日 (MSXML 4.0)	Verified	安全更新程序	0%	2003-10-01 10:02:49	View
☐	Q318138: 安全更新程序	Verified	安全更新程序	0%	2003-08-06 11:02:20	View
☐	Q329048: 安全更新程序	Verified	安全更新程序	0%	2003-10-14 10:52:16	View
☐	Q320920: 安全更新程序	Verified	安全更新程序	0%	2003-06-19 05:56:39	View
☐	用于后台智能传送服务 (BITS) 2.0 和 WinHTTP 5.1 的更新程序 (KB842773)	Verified	关键更新程序	0%	2004-10-05 16:24:56	View
☐	Windows XP 安全更新程序 (KB871250)	Verified	安全更新程序	0%	2005-01-12 11:20:18	View
☐	Microsoft Windows 安装程序 3.1	Verified	关键更新程序	0%	2005-05-18 15:27:22	View

3.9.1.2 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.

Patch server configuration						
Approved Refuse						
Patch name	Audit status	Patch type	Percent of clients to be updated	Publish time	Patch detail	
系统恢复消息更新	Verified	关键更新程序	0%	2003-02-19 12:02:38	View	
Q311967: 安全更新	Verified	安全更新程序	0%	2003-02-19 12:30:33	View	
Q320174: 关键更新	Verified	关键更新程序	0%	2003-02-20 19:16:48	View	
安全更新, 2002 年 2 月 13 日 (MSXML 4.0)	Verified	安全更新程序	0%	2003-10-01 10:02:49	View	
Q318138: 安全更新程序	Verified	安全更新程序	0%	2003-08-06 11:02:20	View	
Q329048: 安全更新程序	Verified	安全更新程序	0%	2003-10-14 10:52:16	View	
Q320920: 安全更新程序	Verified	安全更新程序	0%	2003-06-19 05:56:39	View	
用于后台智能传送服务 (BITS) 2.0 和 WinHTTP 5.1 的更新程序 (KB842773)	Verified	关键更新程序	0%	2004-10-05 16:24:56	View	
Windows XP 安全更新程序 (KB871250)	Verified	安全更新程序	0%	2005-01-12 11:20:18	View	
Microsoft Windows 安装程序 3.1	Verified	关键更新程序	0%	2005-05-18 15:27:22	View	

Or search from filter for review

Patch library management						
Client repair statistics Auto repair configuration						
Patch server configuration Approved Refuse						
Patch name	Audit status	Patch type	Percent of clients to be updated	Publish time	Patch detail	
系统恢复消息更新	Verified	关键更新程序	0%	2003-02-19 12:02:38	Audit status Verified Not verified Verified Refused Not refuse all patches	
Q311967: 安全更新	Verified	安全更新程序	0%	2003-02-19 12:30:33	View	
Q320174: 关键更新	Verified	关键更新程序	0%	2003-02-20 19:16:48	View	
安全更新, 2002 年 2 月 13 日 (MSXML 4.0)	Verified	安全更新程序	0%	2003-10-01 10:02:49	View	
Q318138: 安全更新程序	Verified	安全更新程序	0%	2003-08-06 11:02:20	View	
Q329048: 安全更新程序	Verified	安全更新程序	0%	2003-10-14 10:52:16	View	
Q320920: 安全更新程序	Verified	安全更新程序	0%	2003-06-19 05:56:39	View	
用于后台智能传送服务 (BITS) 2.0 和 WinHTTP 5.1 的更新程序 (KB842773)	Verified	关键更新程序	0%	2004-10-05 16:24:56	View	
Windows XP 安全更新程序 (KB871250)	Verified	安全更新程序	0%	2005-01-12 11:20:18	View	
Microsoft Windows 安装程序 3.1	Verified	关键更新程序	0%	2005-05-18 15:27:22	View	

3.10 Software blacklist and white-list

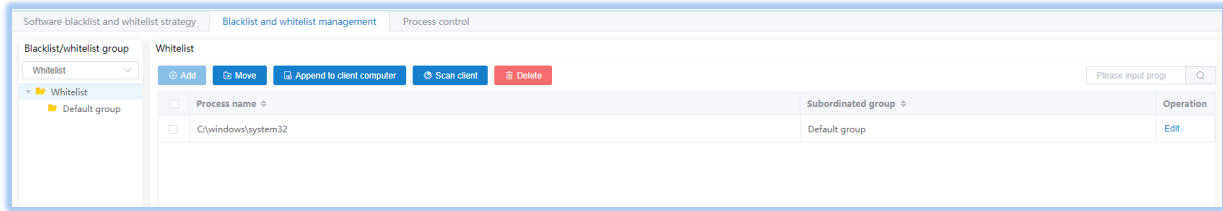
Software blacklist and whitelist control and limit the software progress on the client so as to standardize software application of local running of client and to ensure the safety of program running of client.

- 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.

3.10.1 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.



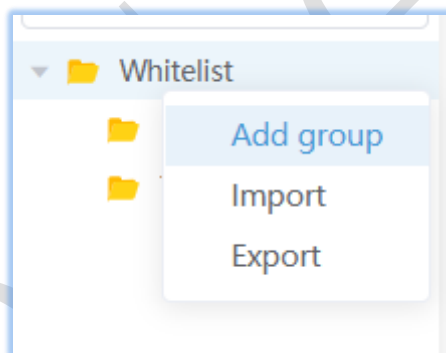
Because the addition method of whitelist is same with that of blacklist, the whitelist is taken as an example to introduce.

3.10.1.1 Add process group

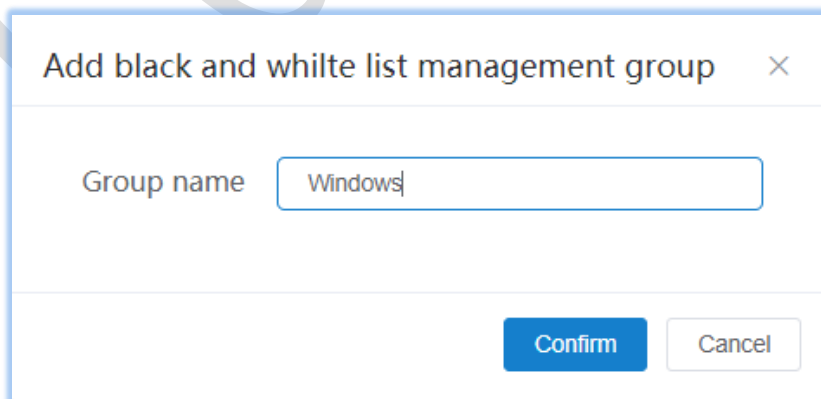
The group is used for classifying and distinguishing processes. We suggest the administrator to make the group based on software.

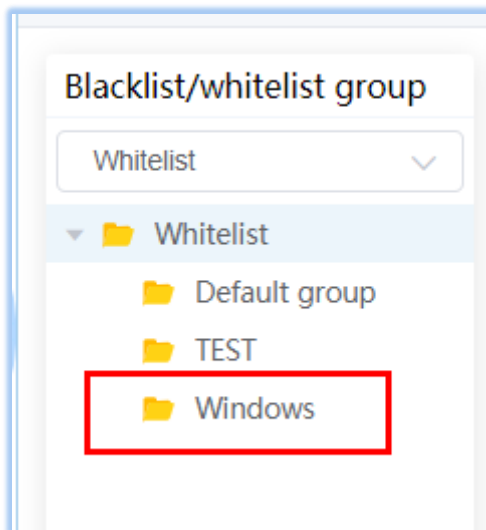
Both whitelist and blacklist only support the one layer group. The root groups have “default group” respectively which shall not be renamed or deleted. Adding method of group is as follows:

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

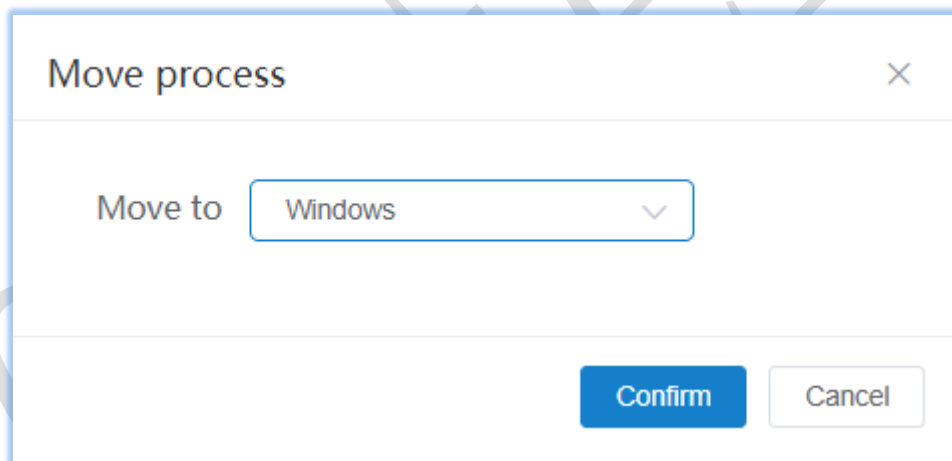
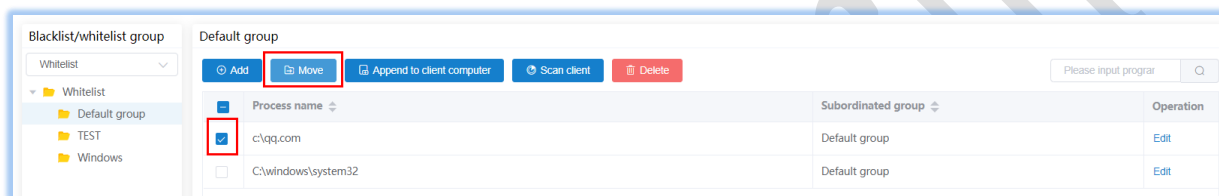


2. Fill in the group name and finish adding.



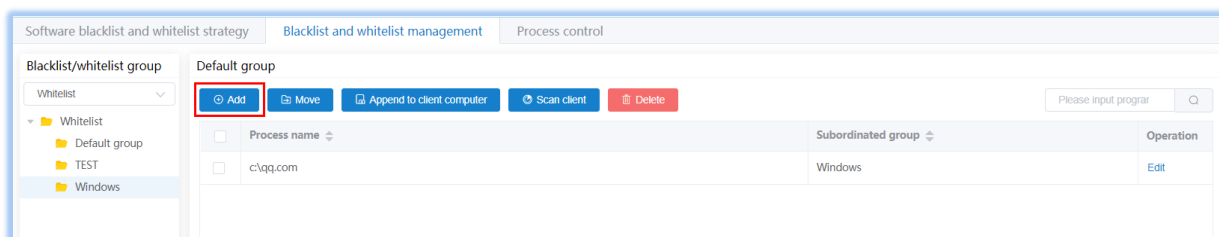


3.The grouped process can be transferred to other groups by “move” function.



3.10.1.2 Manually adding

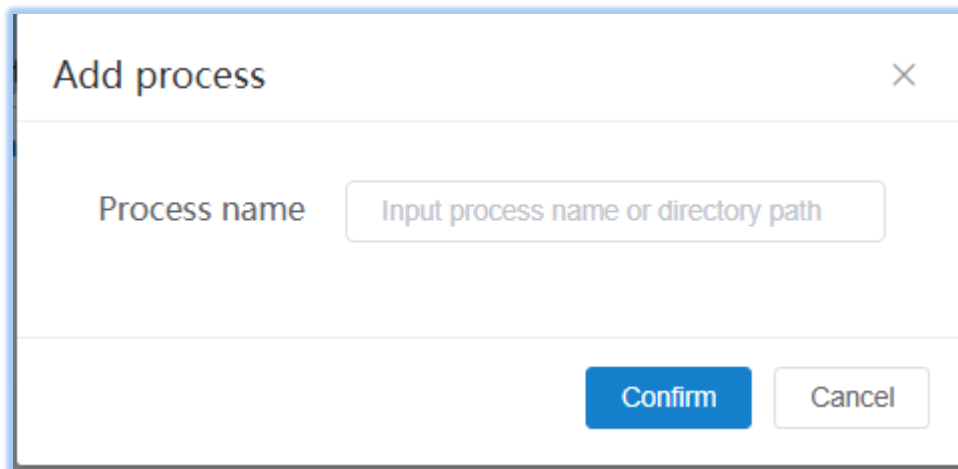
1. Click “add” button.



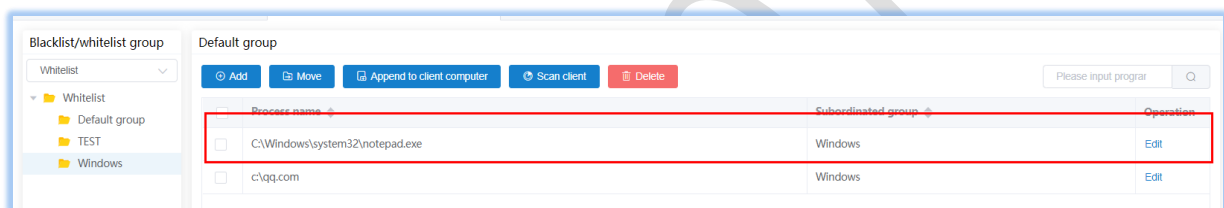
2. In the popup dialog box, fill in the process name. If only one process is added, fill in the complete

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.



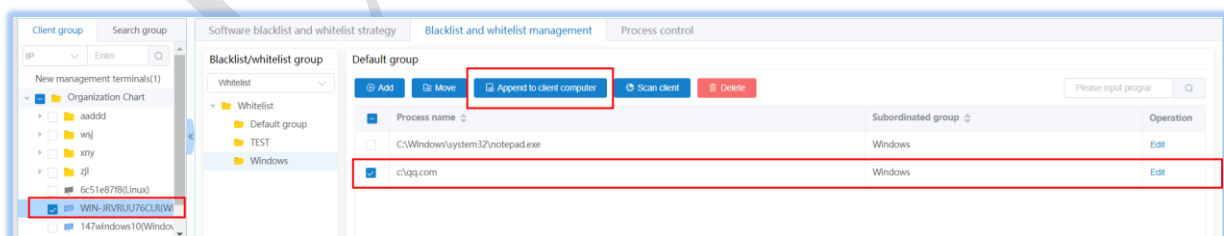
3. Click “OK”. The list will show the added process. Processes added in the root group will be automatically included in the default group.



3.10.1.3 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.



3.10.1.4 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 ormat.

	A	B
1	C:/Windows/system32/notepad.exe	默认组
2	D:/Program Files/NewComm	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/UninstallUserInfo.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.

Import process

File path:

Select file

WhiteProcess.csv

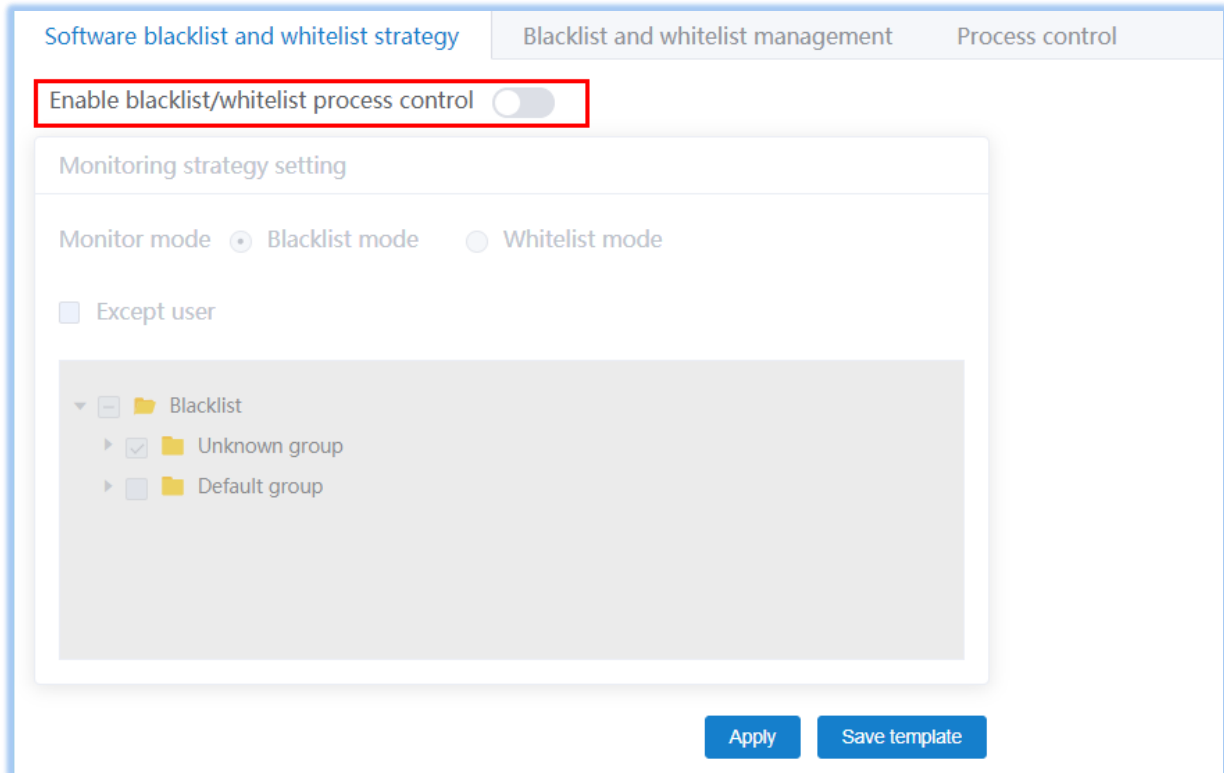
Confirm

Cancel

3.10.2 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

Enable blacklist/whitelist process control ☐

Monitoring strategy setting

Monitor mode ☒ Blacklist mode ☐ Whitelist mode

☐ Except user

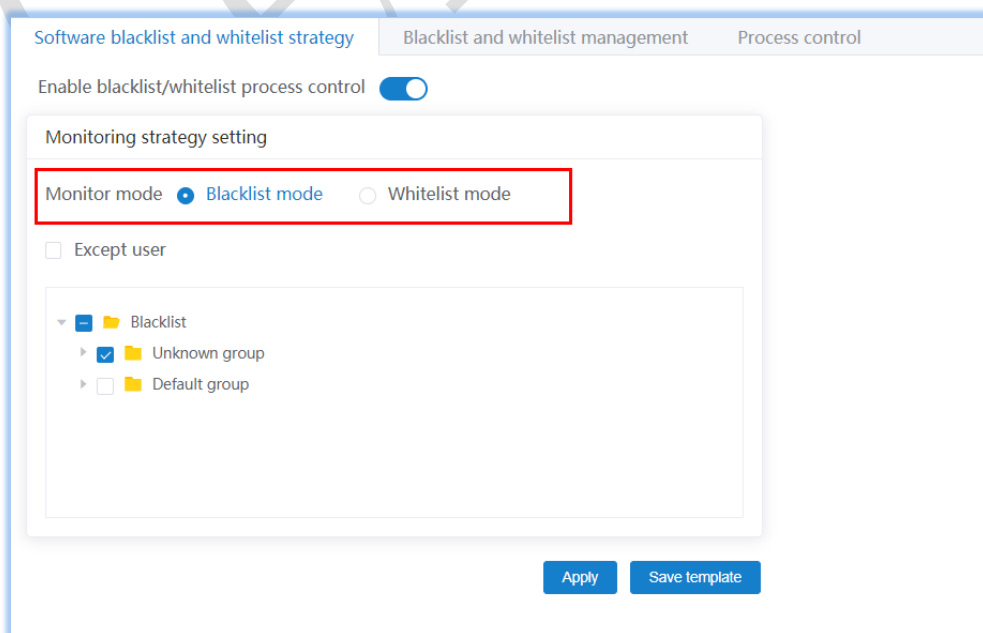
☒ Blacklist

- ☒ Unknown group
- ☐ Default group

Apply Save template

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

Enable blacklist/whitelist process control ☒

Monitoring strategy setting

Monitor mode ☐ Blacklist mode ☒ Whitelist mode

☐ Except user

☒ Blacklist

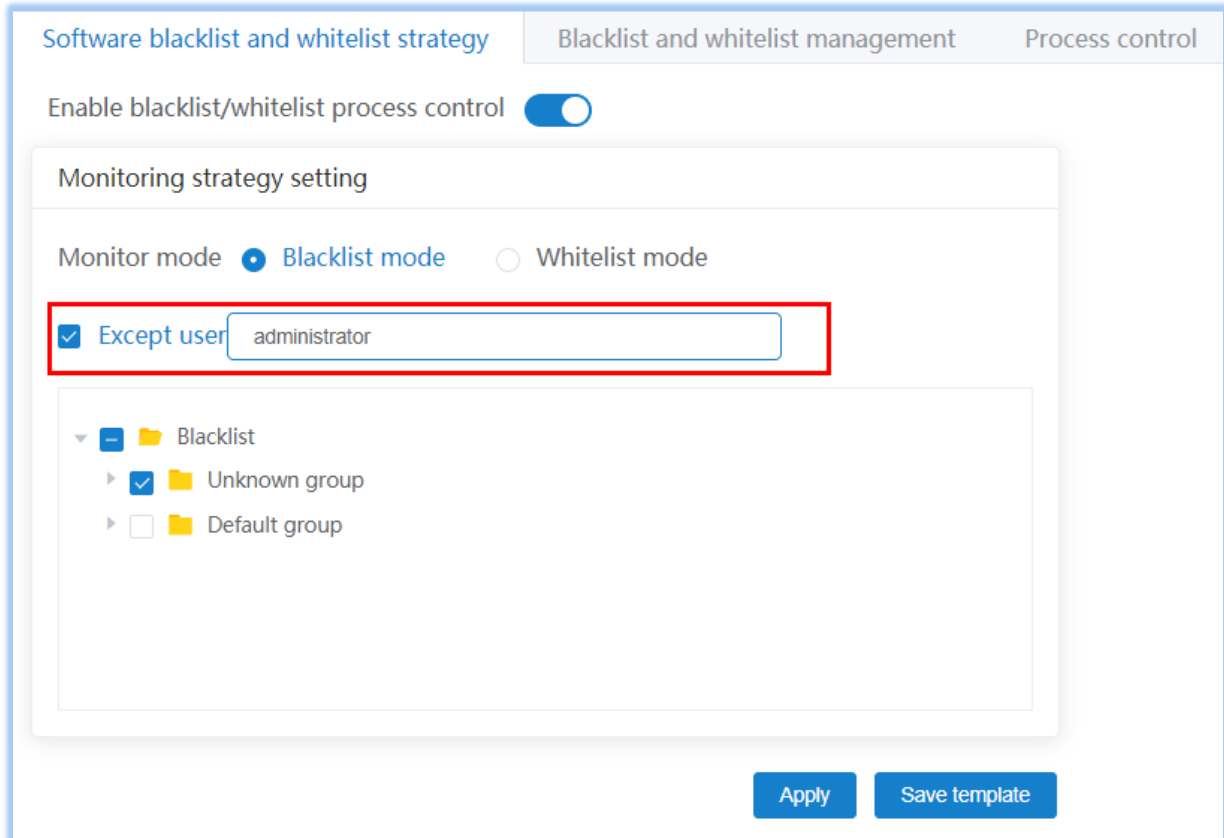
- ☒ Unknown group
- ☐ Default group

Apply Save template

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

Enable blacklist/whitelist process control ☒

Monitoring strategy setting

Monitor mode ☒ Blacklist mode ☐ Whitelist mode

☒ Except user administrator

- Blacklist
 - ☒ Unknown group
 - ☐ Default group

Apply Save template

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

Enable blacklist/whitelist process control ☒

Monitoring strategy setting

Monitor mode ☐ Blacklist mode ☒ Whitelist mode

☐ Except user

Whitelist

☒ Unknown group
 ☒ Default group
 ☒ C:\windows\system32
 ☐ TEST
 ☐ Windows

Apply

Save template

3.10.3 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: 5% | Memory: 8191M | Memory use: 1549M]

Process name	PID	Username	CPU(%)	Memory use	Operation
ConfEmv2.exe	82740	Administrator	0	7196 K	End process
JavaService.exe	1164	SYSTEM	0	111536 K	End process
LicenseServer.exe	2524	SYSTEM	0	11104 K	End process
LogonUI.exe	808	SYSTEM	0	18048 K	End process
Oobe.exe	82080	Administrator	0	8376 K	End process
System	4	SYSTEM	0	368 K	End process
System Idle Process	0	SYSTEM	94	16 K	End process
TPAutoConnSvc.exe	3664	SYSTEM	0	6840 K	End process
UnlFrm2.exe	2612	SYSTEM	0	39944 K	End process
UnlUpdateService.exe	2752	SYSTEM	0	9436 K	End process
UnlitedWeb.exe	2700	SYSTEM	0	6784 K	End process
cmd.exe	2804	SYSTEM	0	3596 K	End process
cmd.exe	31824	SYSTEM	0	2680 K	End process
conhost.exe	2832	SYSTEM	0	2976 K	End process

The function doesn't support NAT

3.11 Template management

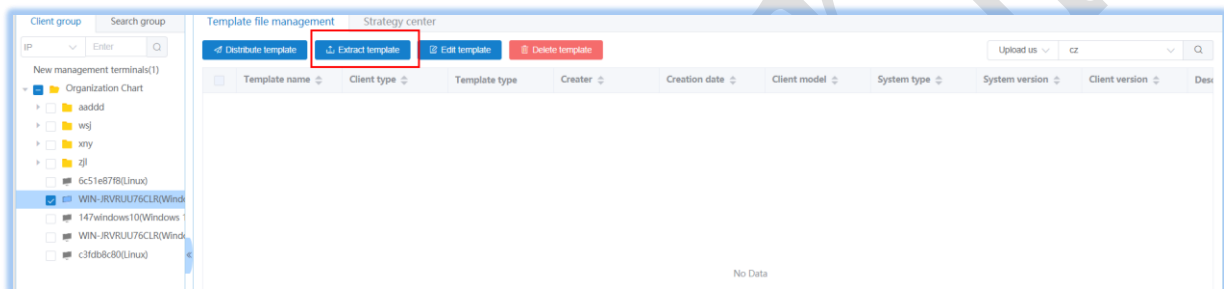
3.11.1 Windows/Linux

Windows OS 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.

3.11.1.1 Extract client configuration template

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



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.

Extract template

* Template name

Client type

Windows client

Description

Select the template configuration items to be extracted

☐ Select all

☐ Remote assistance

☐ Local access control

☐ Disk management

☐ Printer

☐ Desktop strategy

☐ Desktop mode

☐ Star menu taskbar

☐ Control panel

☐ Desktop icon publish

☐ IE strategy

☐ IE proxy configuration

☐ IE security

☐ IE favorites

☐ Time Sync

Confirm

Cancel

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

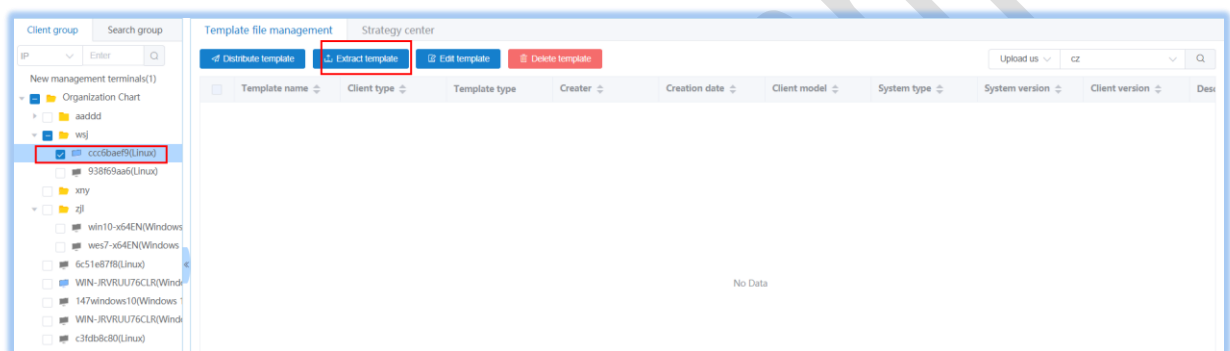
Template file management									
Strategy center									
⬅️ Distribute template ⬇️ Extract template ✎ Edit template 🗑 Delete template Upload us cz Q									
☐	Template name	Client type	Template type	Creator	Creation date	Client model	System type	System version	Client version
☐	template	Windows client	Client configuration	cz	2020-01-16 15:52:39	VMware Virtual Platform	Windows Server 2008 R2 64位	6.1.7601 Service Pack 1	7.0.0.0000.9388

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.

3.11.1.2 Extract configured template for Linux client

1. Choose a client, click "Extract the terminal configuration template" button.



2. Fill in name, type and description, then tick on options about to be added to template for extraction

Extract template

×

* Template name

Linux

Client type

Linux client

Description

Linux

Select the template configuration items to be extracted

☒ Select all

☒ Time
 ☒ Network
 ☒ Language And Keyboard

☒ Security
 ☒ Cloud Service
 ☒ ICA Global Settings

☒ Device Manager
 ☒ Power Manager

1. Source system and distribution system of template should be the same.

2. Select template abstraction item based on demand rather than select all.

Confirm

Cancel

5. After template extraction done, it can be seen in below list

Template file management

Strategy center

Distribute template

Extract template

Edit template

Delete template

Upload us

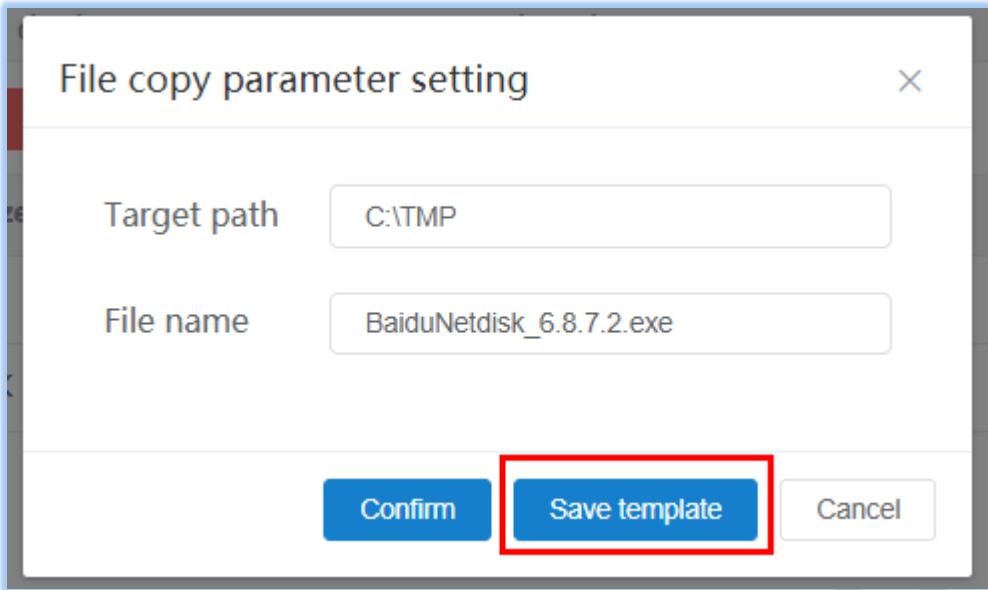
cz

☐	Template name	Client type	Template type	Creator	Creation date	Client model	System type	System version	Client version	Description
☐	Linux	Linux client	Client configuration	cz	2020-01-16 15:54:43	N610	Linux	2000.1.00	6.0.692.108.3228	Linux
☐	template	Windows client	Client configuration	cz	2020-01-16 15:52:39	VMware Virtual Platform	Windows Server 2008 R2 64位	6.1.7601 Service Pack 1	7.0.0.0000.9388	terminal

3.11.1.3 Save task template

1) File copy

Enter to file deployment, save settings for copy parameter , then save the template



File copy parameter setting

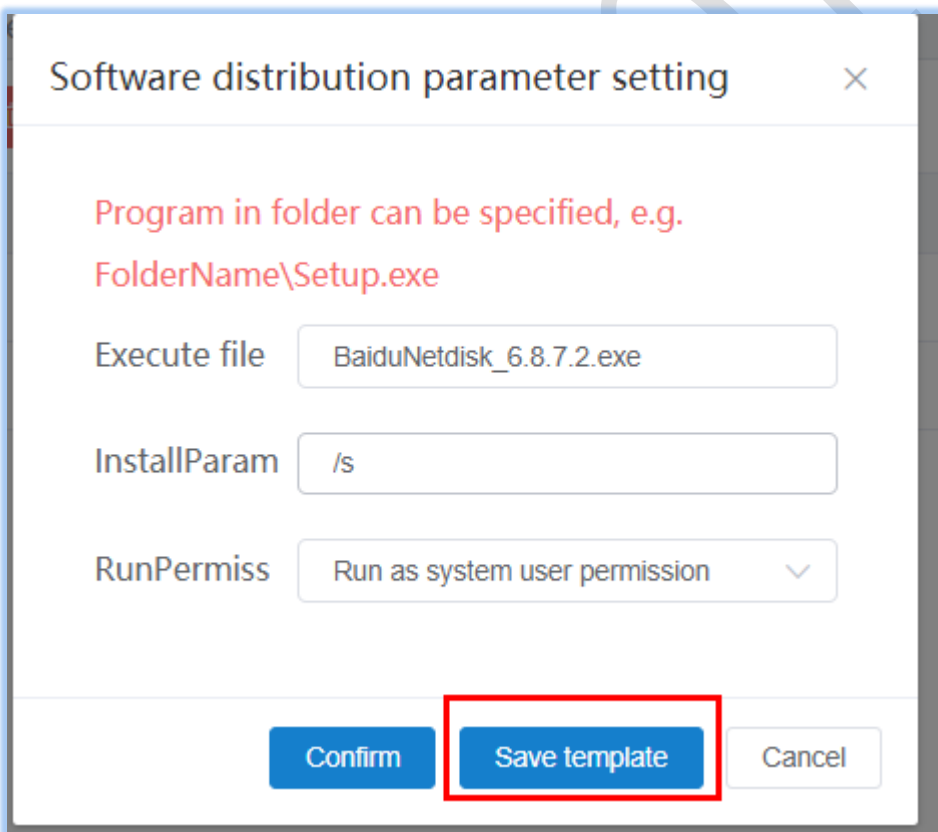
Target path: C:\TMP

File name: BaiduNetdisk_6.8.7.2.exe

Buttons: Confirm, Save template (highlighted with a red box), Cancel

2) Software installation

Setup parameter settings for software installation, then save settings; the figure shown as below,



Software distribution parameter setting

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

Execute file: BaiduNetdisk_6.8.7.2.exe

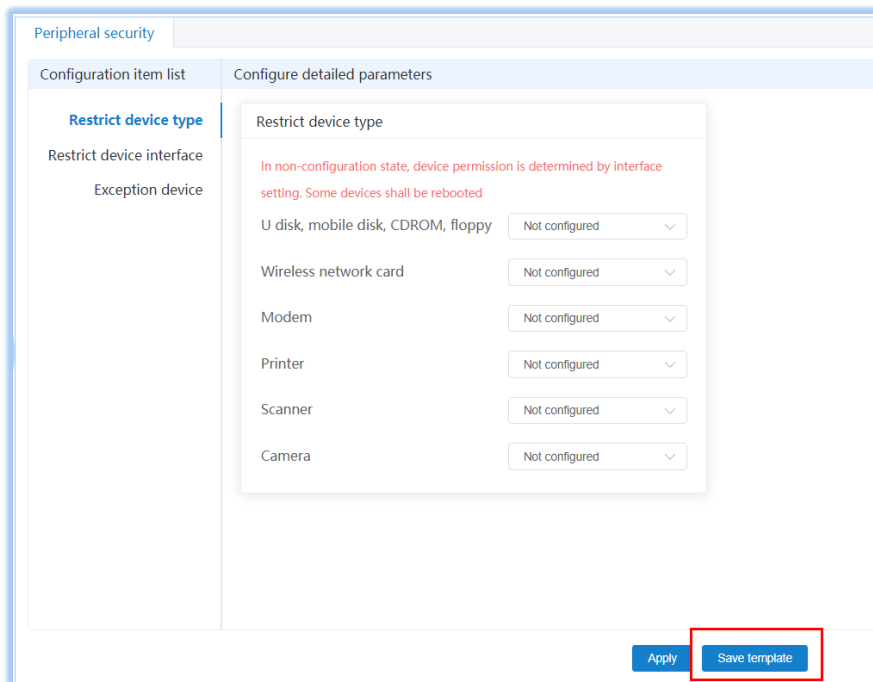
InstallParam: /s

RunPermiss: Run as system user permission

Buttons: Confirm, Save template (highlighted with a red box), Cancel

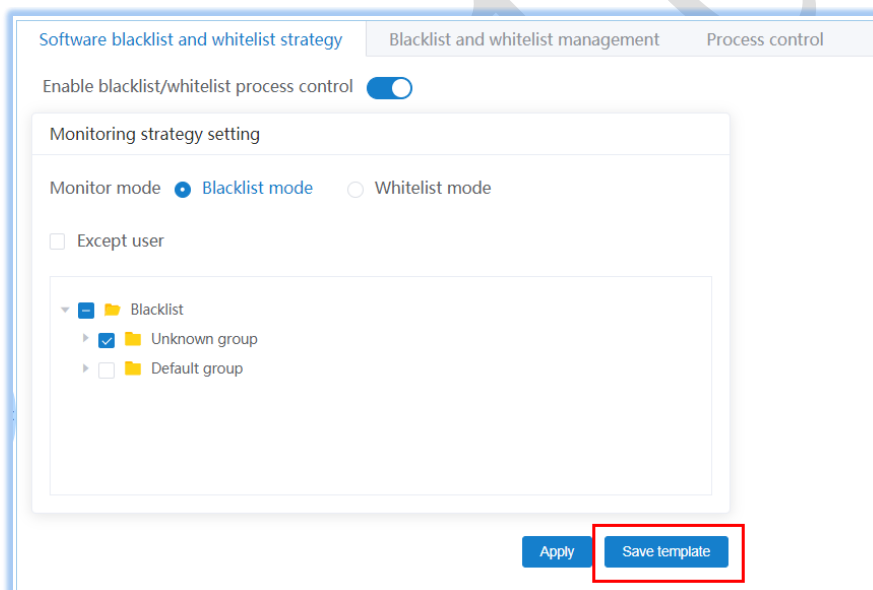
3) Peripheral security

Setup parameter settings for peripheral security, then save settings; the figure shown as below,



4) Software black-list & white-list

Setup parameter settings for software black & white list, then save settings; the figure shown as below,



After saving template, prompt would be shown up for reminding

Template configuration

Template name

blacklistAndWhitelistStrategy

Client type

Windows client

Description

Software blacklist and whitelist strategy

Confirm

Cancel

5) WEB security

Go to WEB security: configure the WEB security list, then save the template

Strategy configuration

Start WEB monitoring ☒

Restriction mode

- ☒ Only forbid accessing website in line with legal domain name strategy
☐ Only allow accessing website in line with legal domain name strategy

Domain strategy list

+ Add

Delete

☐	Domain name	Restrict time	Operation
☐	www.baidu.com	Every day(00:00~24:00)	Edit

Apply

Save template

After click 'Save template'; a prompt would be shown up for reminding

6) Printer white-list

Go to printing white-list, configure the white-list for printing, then save the template.

White list strategy

Enable the print of white list ☒

⊕ Add
🗑 Delete

☐	Program name	Operation
☐	wps.exe	Edit

[Apply](#)

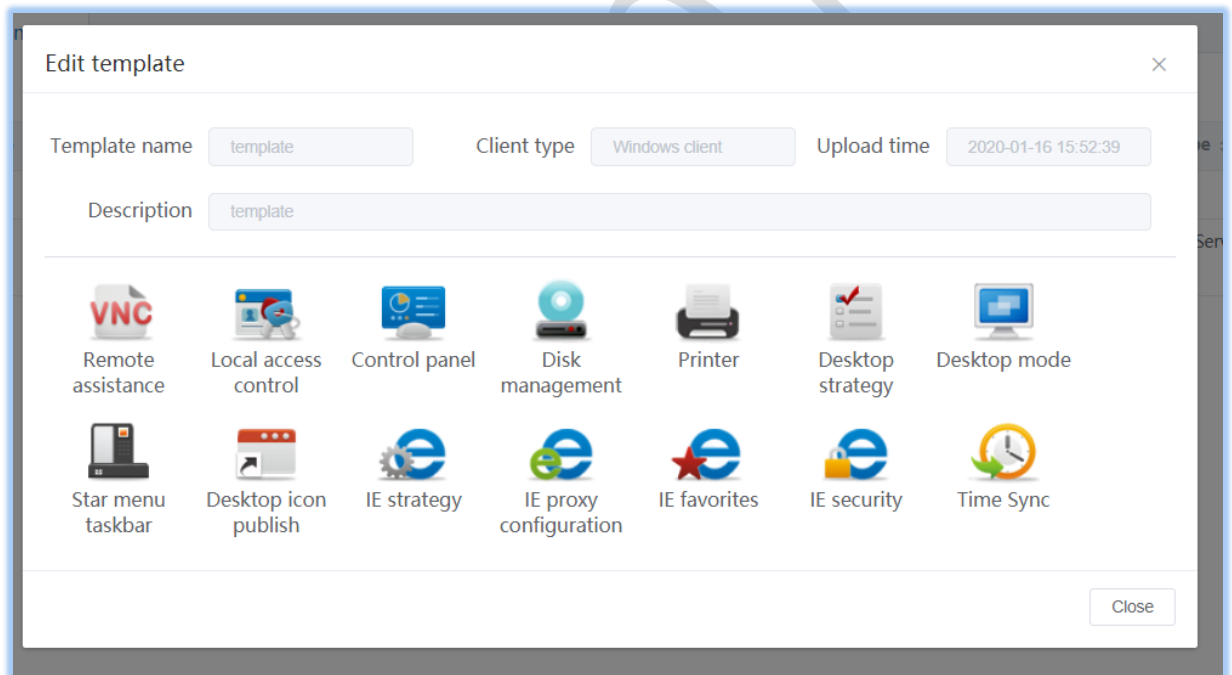
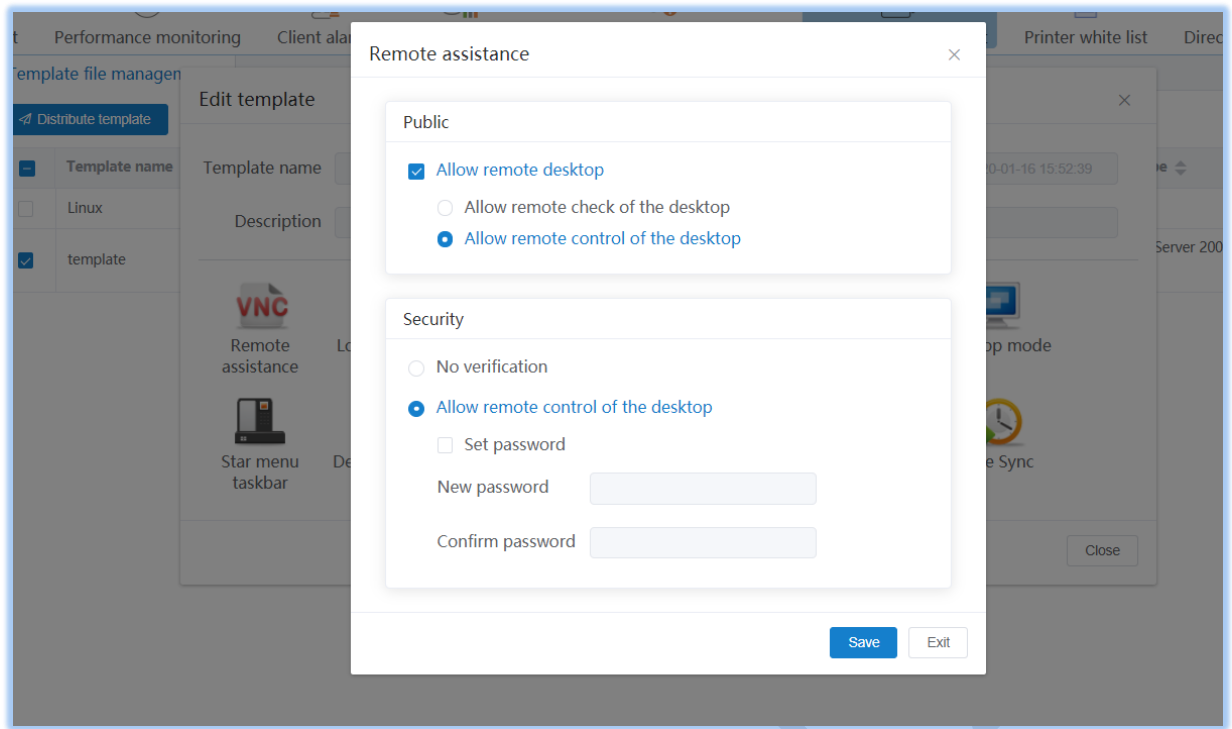
[Save template](#)

A prompt would be shown up for reminding; which display the template type and matched terminal model

Template file management									
Strategy center									
Distribute template	Extract template	Edit template	Delete template						
☐	Template name	Client type	Template type	Creator	Creation date	Client model	System type	System version	Client version
☐	Linux	Linux client	Client configuration	cz	2020-01-16 15:54:43	N610	Linux	2000.1.00	6.0.692.108.3228
☐	template	Windows client	Client configuration	cz	2020-01-16 15:52:39	VMware Virtual Platform	Windows Server 2008 R2 64位	6.1.7601 Service Pack 1	7.0.0.0000.9388

3.11.1.4 Edit to template

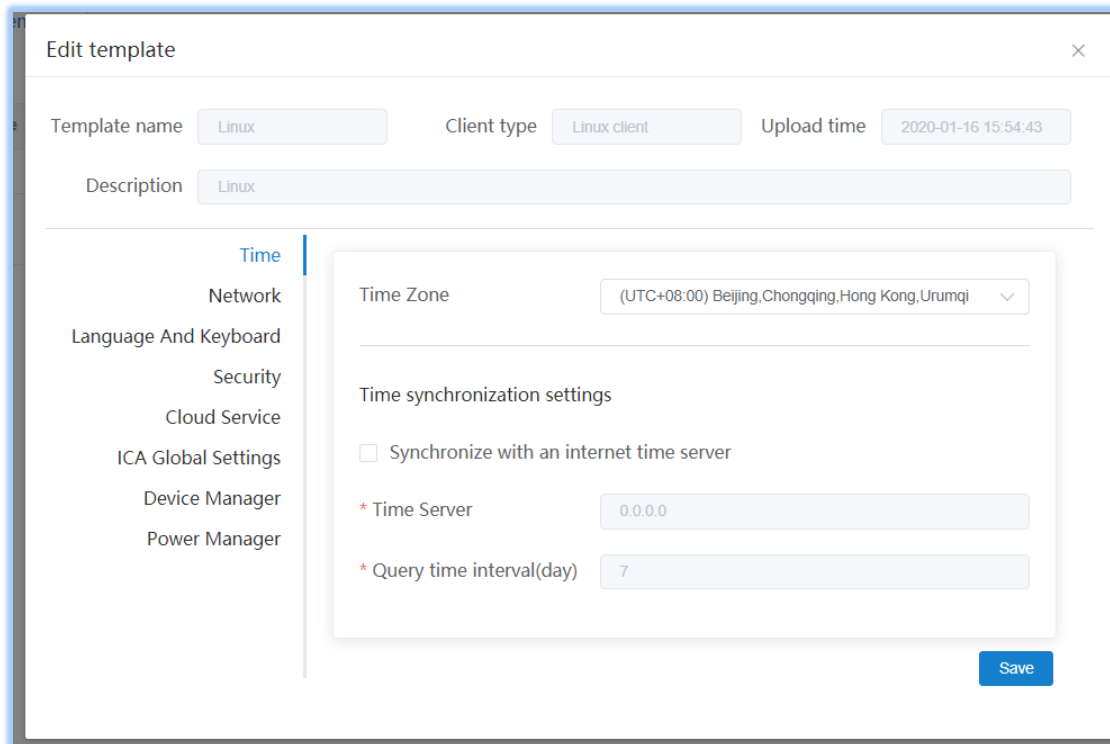
Select the template, then click 'Edit' to start editing



After template modified, click 'Save' to save settings

3.11.1.5 Linux template edit

Click 'Edit template' to edit the template just saved before



Edit template

Template name: Linux Client type: Linux client Upload time: 2020-01-16 15:54:43

Description: Linux

Time

Network

Language And Keyboard

Security

Cloud Service

ICA Global Settings

Device Manager

Power Manager

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

Time synchronization settings

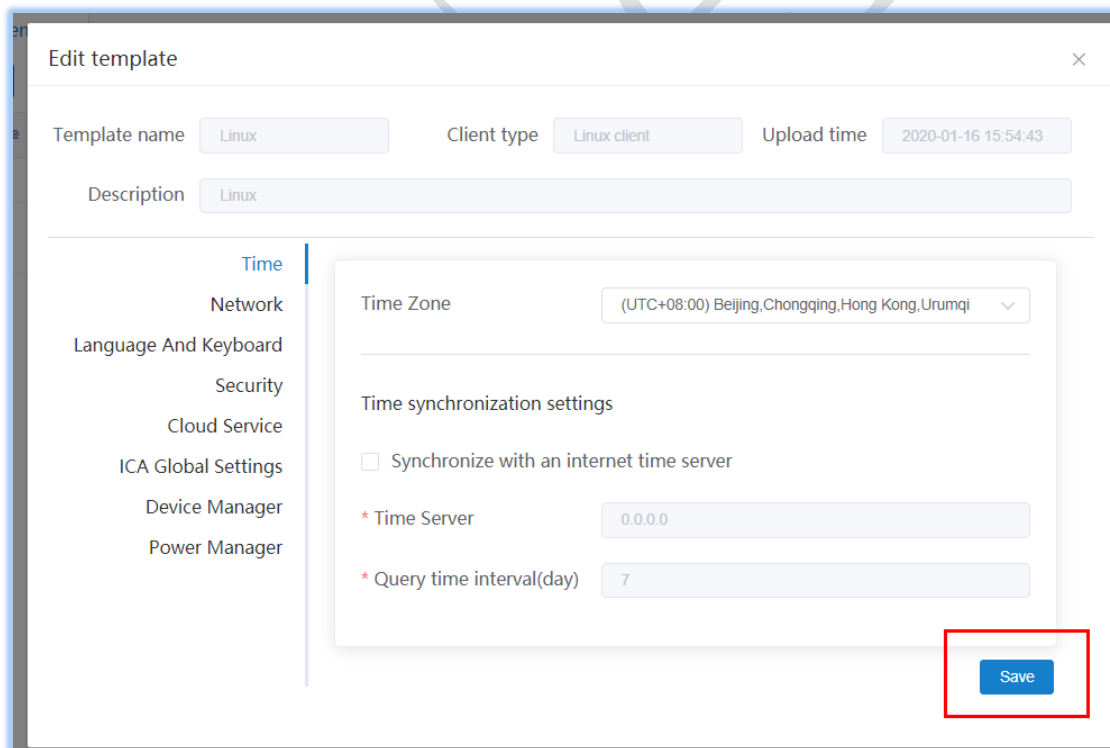
☐ Synchronize with an internet time server

* Time Server: 0.0.0.0

* Query time interval(day): 7

Save

Click option to start editing, then click 'save' to complete.



Edit template

Template name: Linux Client type: Linux client Upload time: 2020-01-16 15:54:43

Description: Linux

Time

Network

Language And Keyboard

Security

Cloud Service

ICA Global Settings

Device Manager

Power Manager

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

Time synchronization settings

☐ Synchronize with an internet time server

* Time Server: 0.0.0.0

* Query time interval(day): 7

Save

3.11.1.6 Template distribution

1. Select the template file and the client for distribution
2. Click 'Template distribution'
3. Execute the task in Plan

Memo:

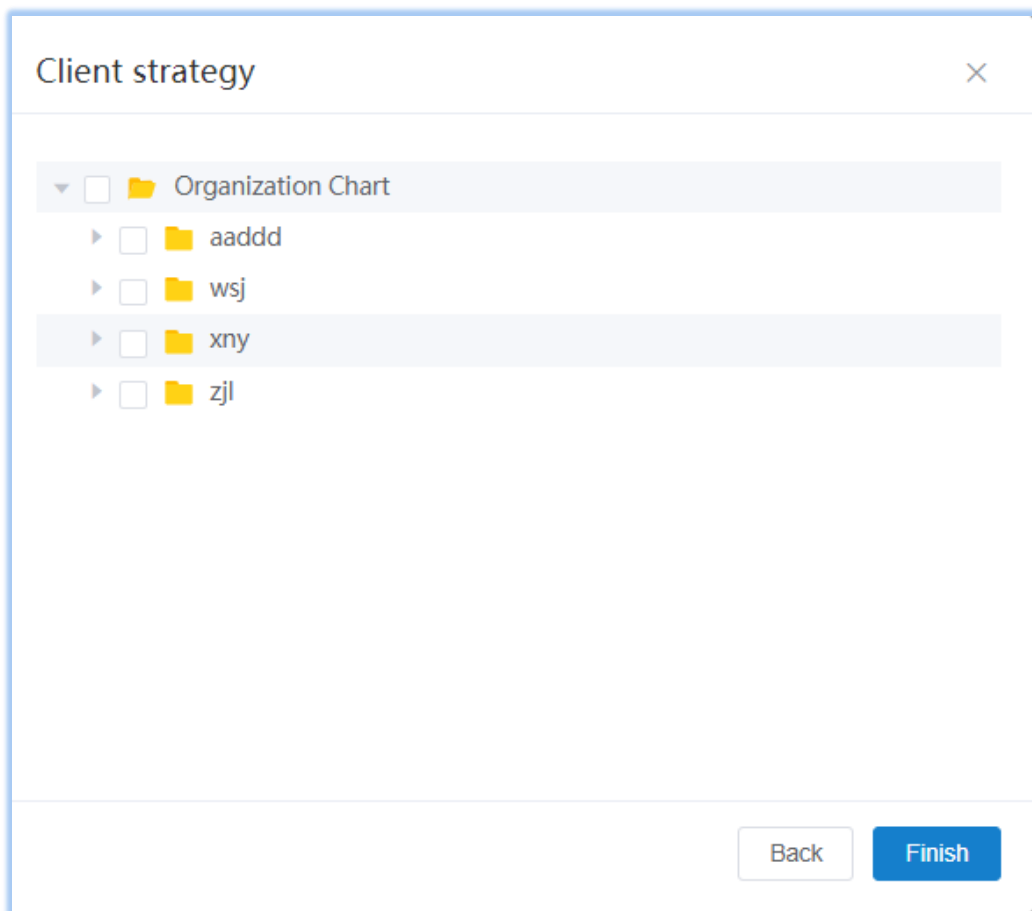
- Clients for template distribution can be one or many, as well as in group
- Template for client type should be matched with client OS; such as Windows template for Windows client, and Linux template for Linux

Centerm

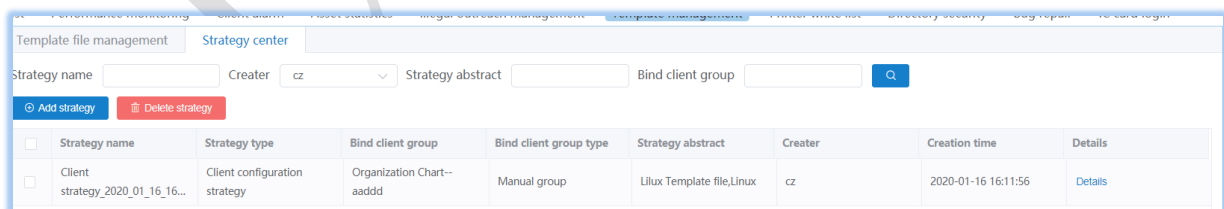
3.11.2 Strategy center

When a group require a united strategy for deployment, and wish new added client could adapt the same strategy, the template binding with strategy would be highly recommended.

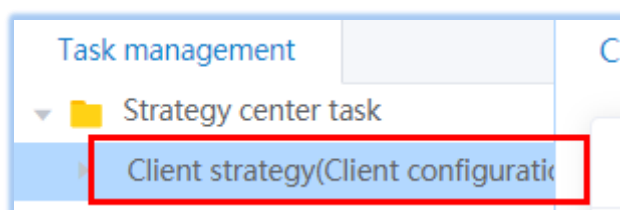
1. Click 'Add strategy'
2. Select the template file for binding with strategy, then click 'Next'
3. Choose the group, click 'Next';



4. Complete the strategy create

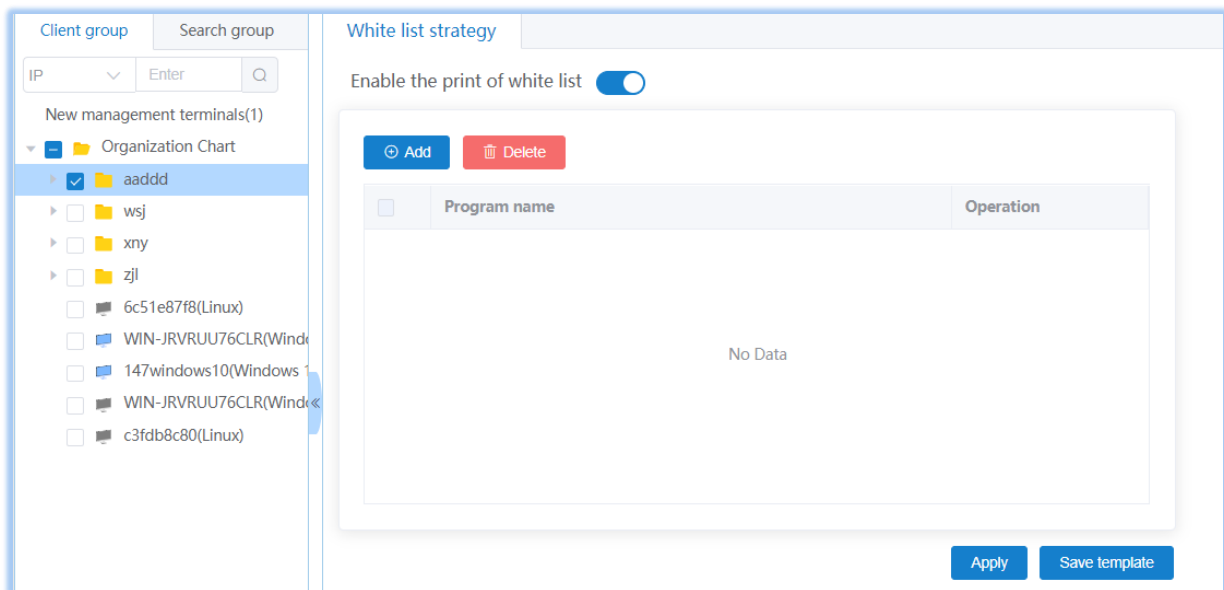


5. Strategy executed status and result can be checked in 'Task management'

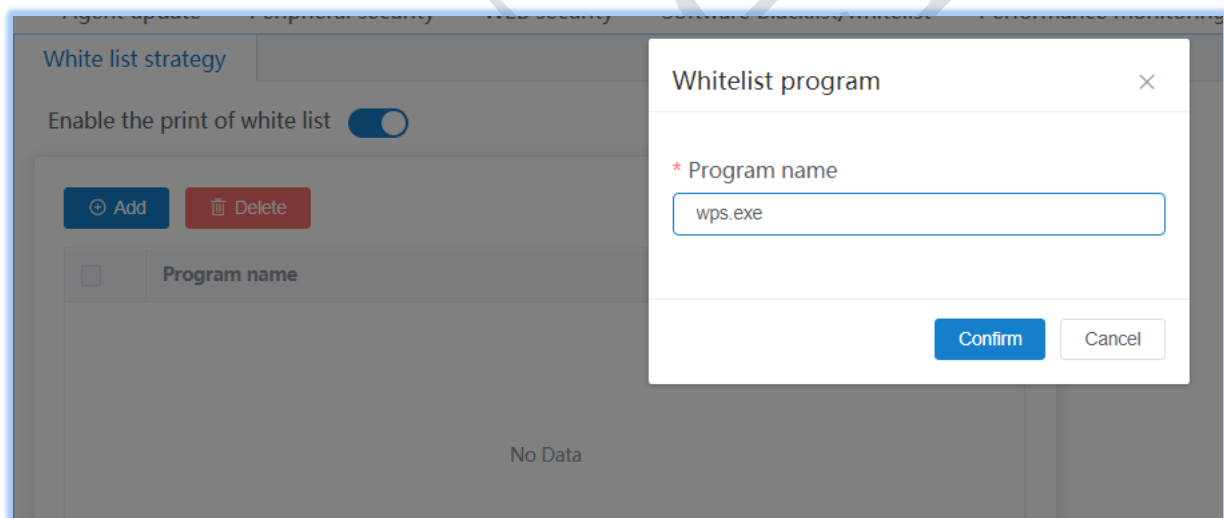


3.12 Printer white-list

Allow printer to work with certain client for document printing in the particular programs only



1 Add the programs into white-list for document printing.



2 Click 'Confirm' to complete settings

White list strategy

Enable the print of white list ☒

⊕ Add

🗑 Delete

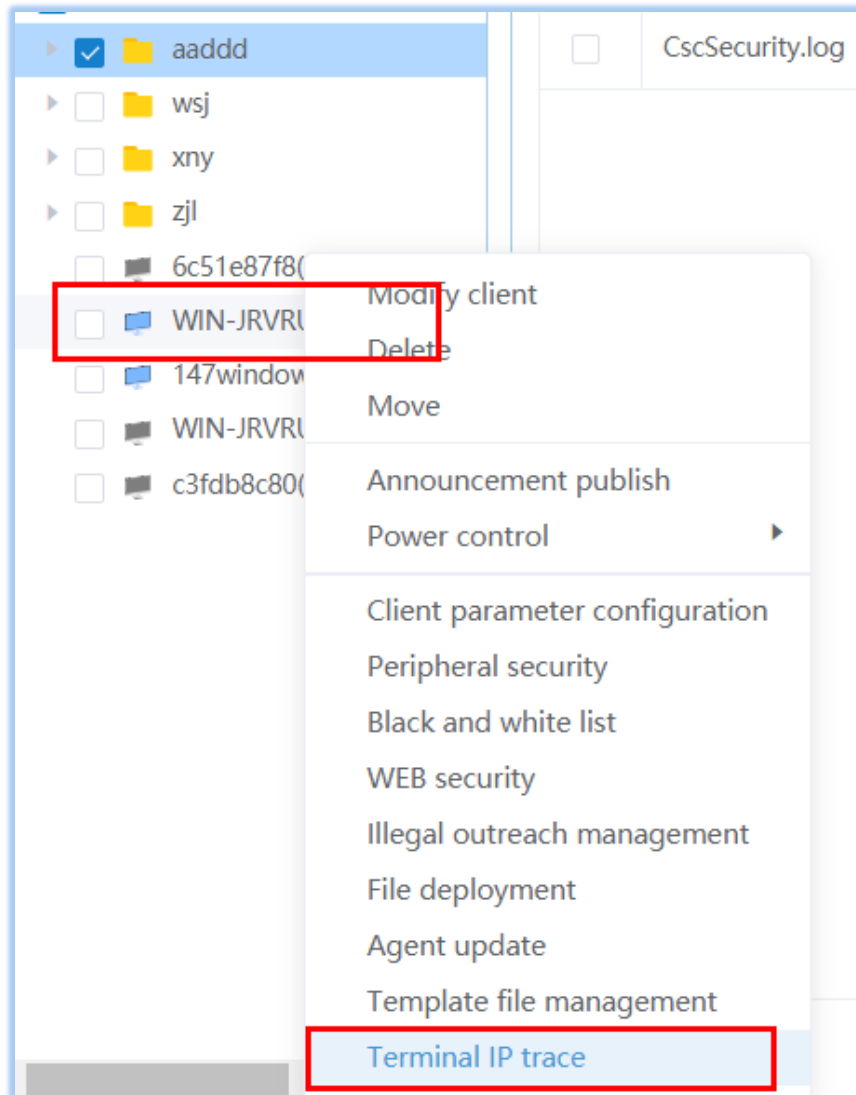
☐	Program name	Operation
☐	wps.exe	Edit

Apply

Save template

3.13 Terminal IP trace

1. Right click a terminal, then select "Terminal IP trace"



2. After that, altering status of the terminal IP, group can be seemed; the figure shown as below

Peripheral security log Illegal outreach access log Client login log WEB access log Assignment log Automatic update log for internal and external clearing Terminal IP trace				
Export				
Change time Start Date to End Date Q				
Subordinated group	Client alias	Client IP	MAC	Change time
zjl	win10-x64EN	192.168.44.168	00-0C-29-4A-20-9D	2020-01-15 13:24:31
zjl	win10-x64EN	192.168.106.140	00-0C-29-4A-20-9D	2020-01-11 14:04:11

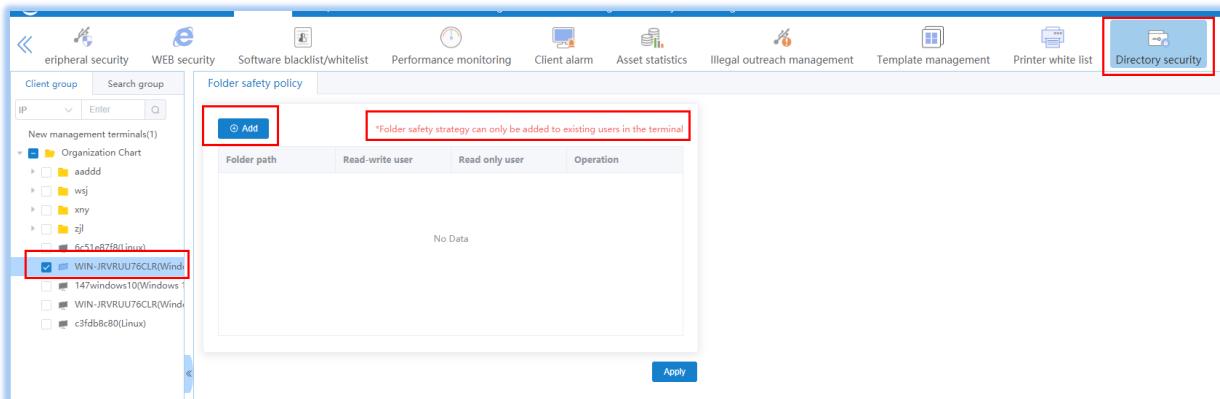
3. IP change tracing can be executed and traced by checking changed time of MAC address
4. The result can be imported to excel file

3.14 Directory security

Directory security can be set by changing the read/write permission for different users to certain folders

3.14.1 Add the directory security

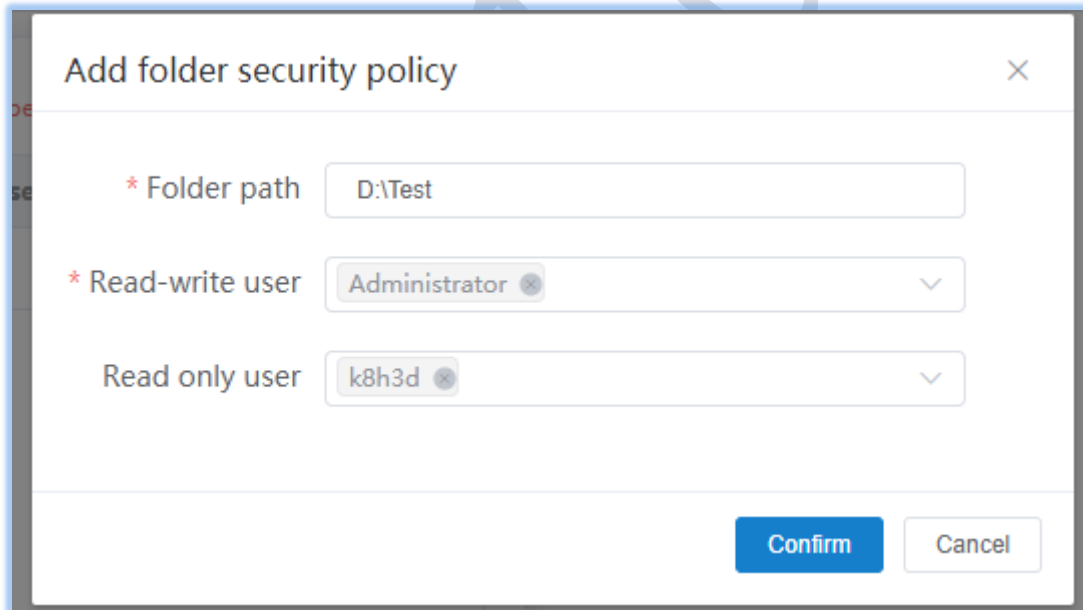
- 1、Enter to 'Directory security' ; select a terminal, then click 'Add' in folder safety policy



- 2、Fill in folder security patch and user given different permission, then click 'Confirm'

Notice:

- 1) Folder patch should be met with Windows folder rule, given the max 240-character length without &
- 2) Read-write user should be filled, is compulsory
- 3) User status should be enable and existed for terminal. Otherwise, task may go fails.



3.14.2 Folder secure policy edit

- 1、Click 'Edit' to one of policies, the start editing

[+ Add](#)

*Folder safety strategy can only be added to existing users in the terminal

Folder path	Read-write user	Read only user	Operation
D:\Test	Administrator	k8h3d	Edit Delete

2、Editing does not have folder patch modified, click 'Confirm' after done

Edit folder security policy
×

* Folder path

D:\Test

* Read-write user

Administrator ✕

Read only user

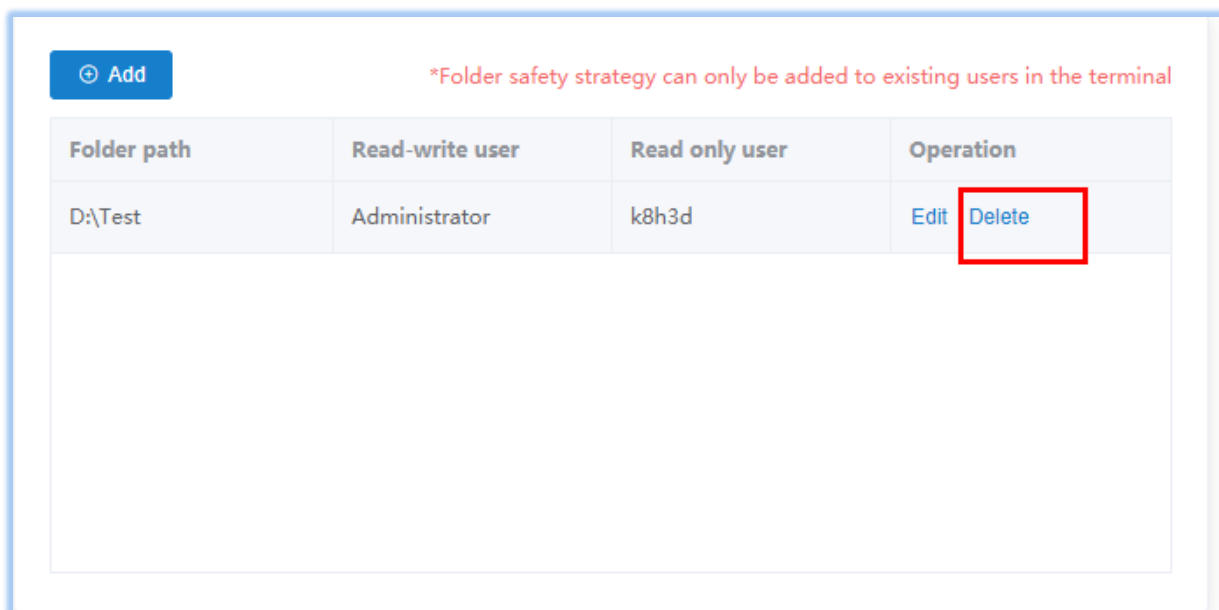
k8h3d ✕

Confirm

Cancel

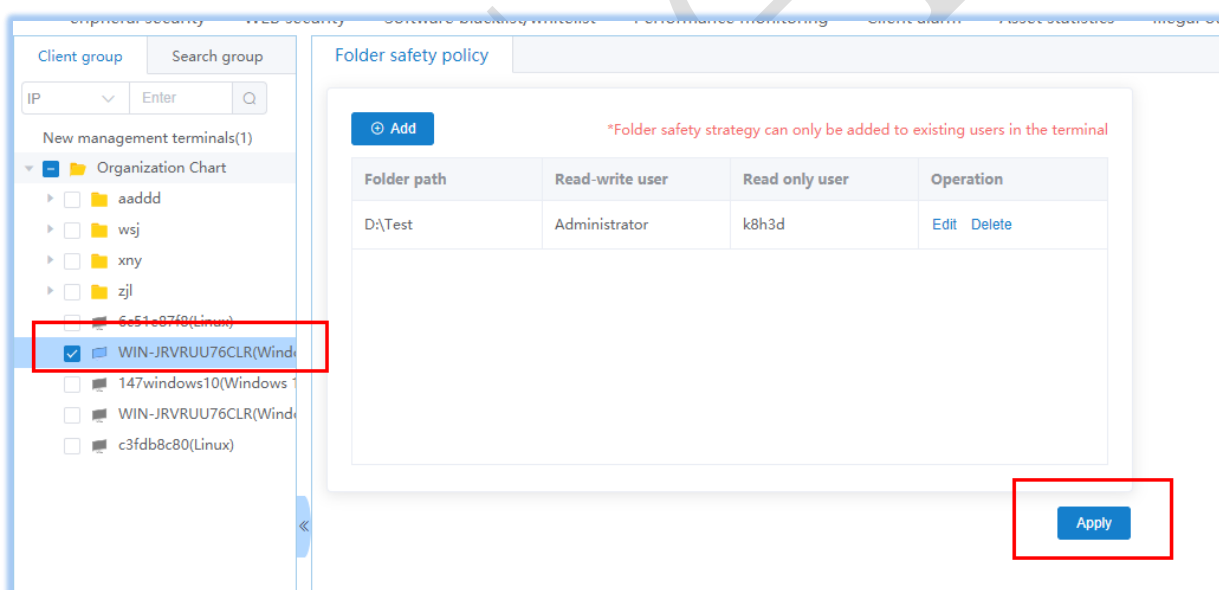
3.14.3 Delete folder secure policy

Select the relevant policies, then click 'Delete'; folder secure policy would be back to previous one after its secure policy removed



3.14.4 Folder secure policy distribution

Click on relevant policy and distribute it to selected terminal



Schedule wizard

Task name

Folder security policy configuration

Task target

1

Task start time

☒ Start right away
 ☐ Assign task start time

Advanced setting

☐ Task end time
 ☐ Only executed daily from

00:00

 to

20:00

Deployment settings

☒ Deploy immediately (UWF module doesn't support it. Select restart)

☒ Restarting before deployment, Countdown (min)

5

 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.

Confirm

Cancel

注意：

- 1) 添加的策略、编辑和删除策略的操作结果只会保存在当前会话中，如果没有成功应用到终端，下次进入到文件夹安全模块时记录将不会存在。
- 2) 下发文件夹策略到终端，若终端中无此文件夹则会新建。

3.15 Log on by IC card

User can login to session by swapping a card after first register to clients

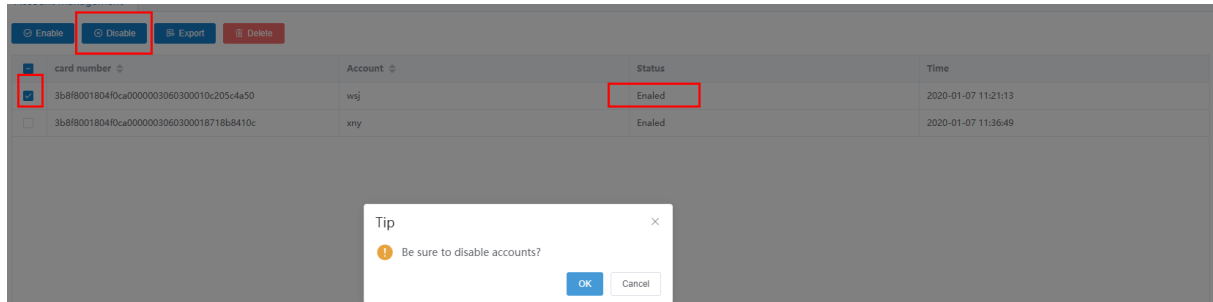
3.15.1 User management for logon

The interface for user account to logon by card, is shown as below

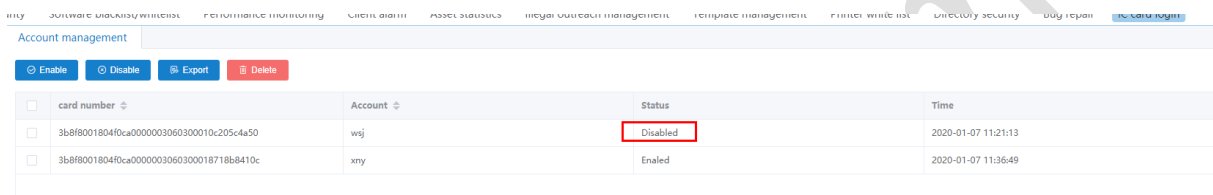
Account management			
Enable Disable Export Delete			
☐ card number	Account	Status	Time
☐ 3b8f8001804f0ca0000003060300010c205c4a50	wsj	Enaled	2020-01-07 11:21:13
☐ 3b8f8001804f0ca0000003060300018718b8410c	xny	Enaled	2020-01-07 11:36:49

3.15.2 User enable/disable

Choose the user first, then make user enable or disable



After click 'ok', the status change



4. System settings

4.1 User management

4.1.1 User management

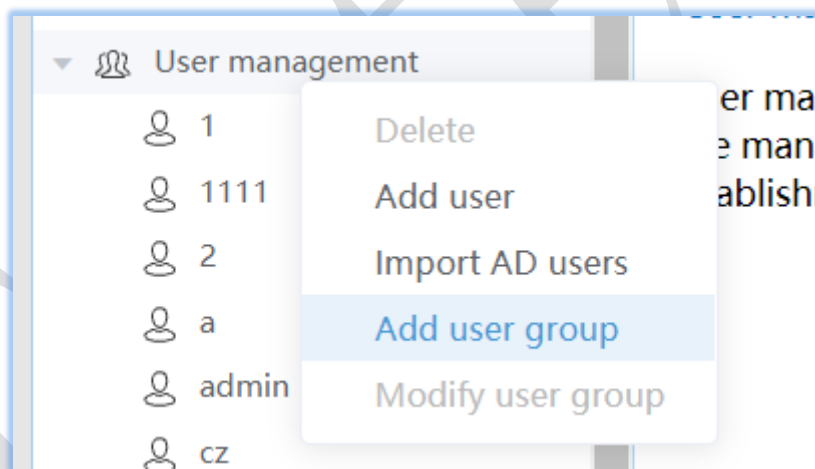
After installation of system, default username and password are admin and admin respectively. The administrator can configure the user/group, role and authority of role. Description about authority: the user authority can restrict the user to access to system functions. The user authority is the role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

4.1.1.1 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 “Confirm” button to finish the addition of user group.

Add user group

* Group name

TEST

Description

TEST

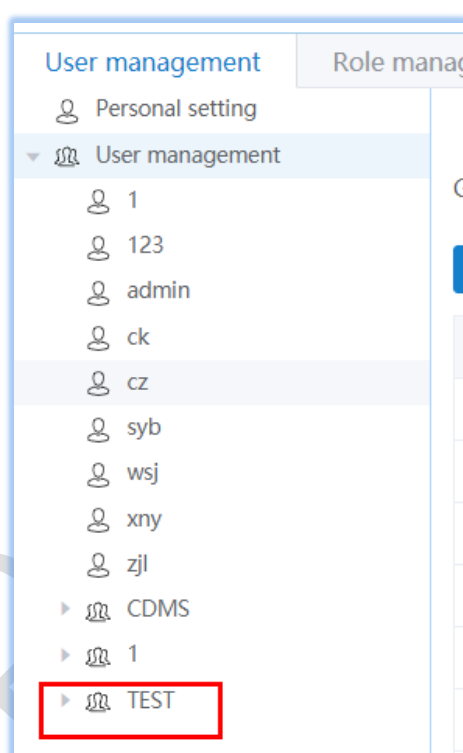
Subordinated group

User management

	User role	Description
☐	Super admin	Super admin
☐	Universal	Universal
☐	1111	—

Confirm

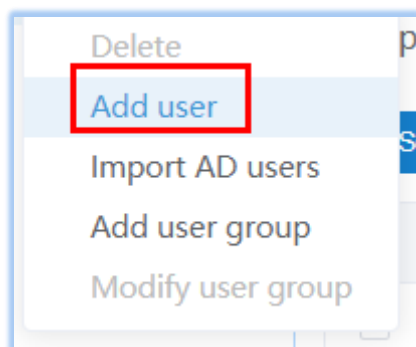
Cancel



4.1.1.2 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. 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 ▾	Description ▾
☒	Super admin	Super admin
☐	Universal	Universal
☐	1111	—

Back

Next

3. Fill in the basic information.

User management

* Confirm pwd

•

Manager or not

Yes

Phone

12345678901

Email

123@qq.com

Unit

Subordinated group

User management

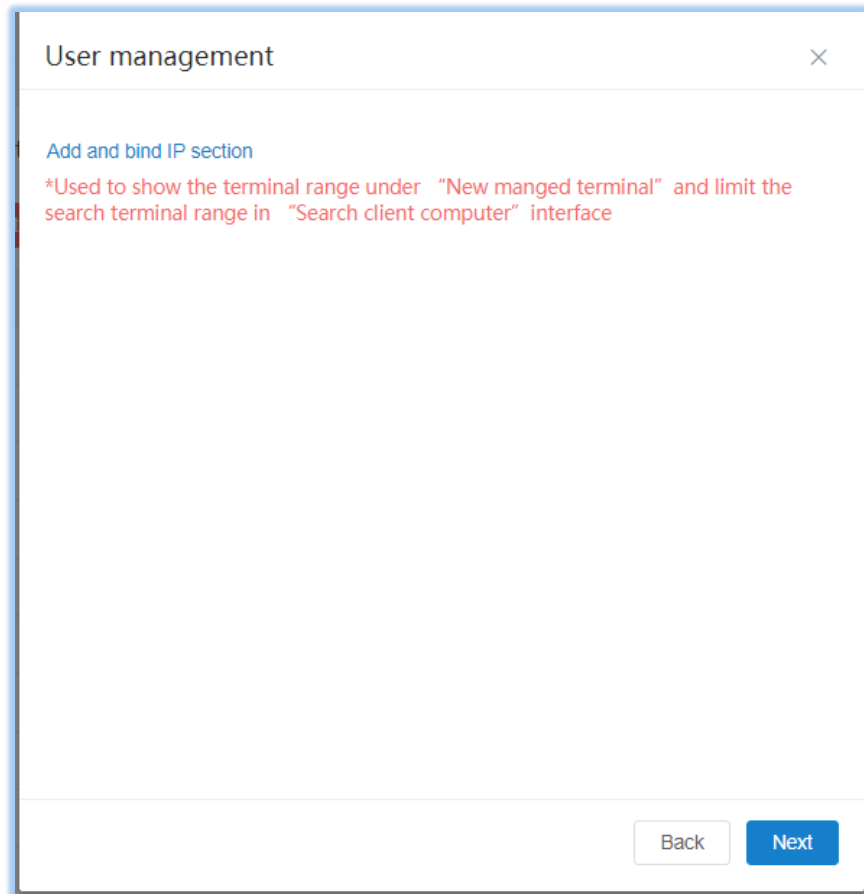
Description

Back

Next

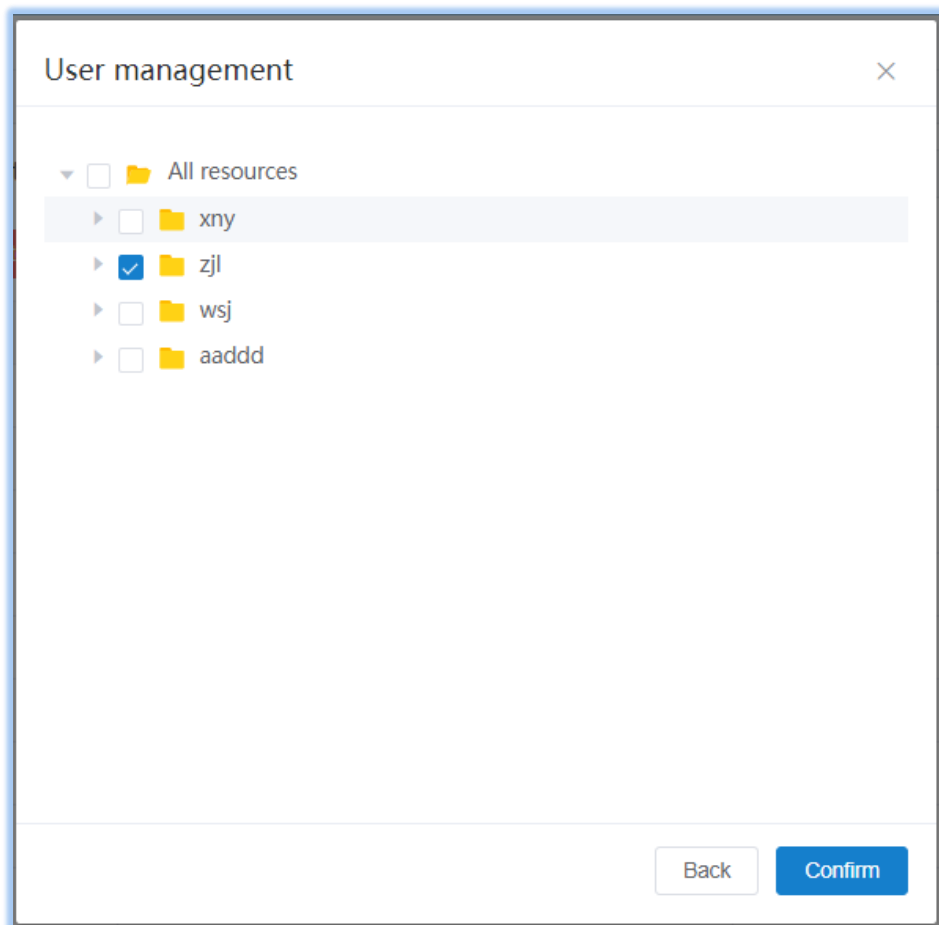
Notice:

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

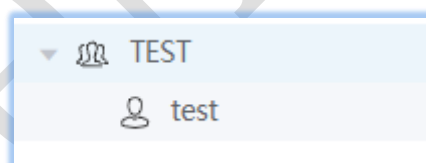


4. Distribute the client resources

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.



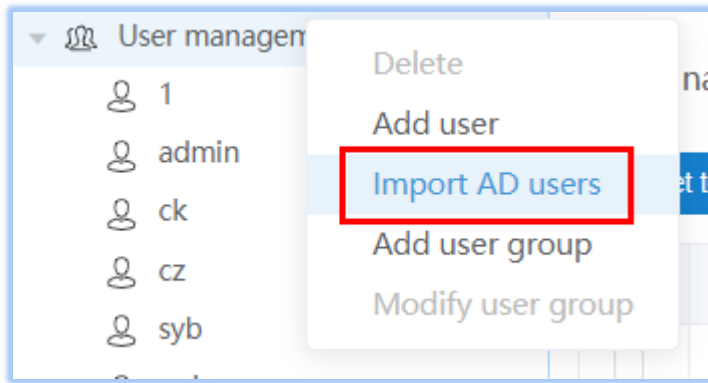
Finally, click "OK" button, as shown in following figure.



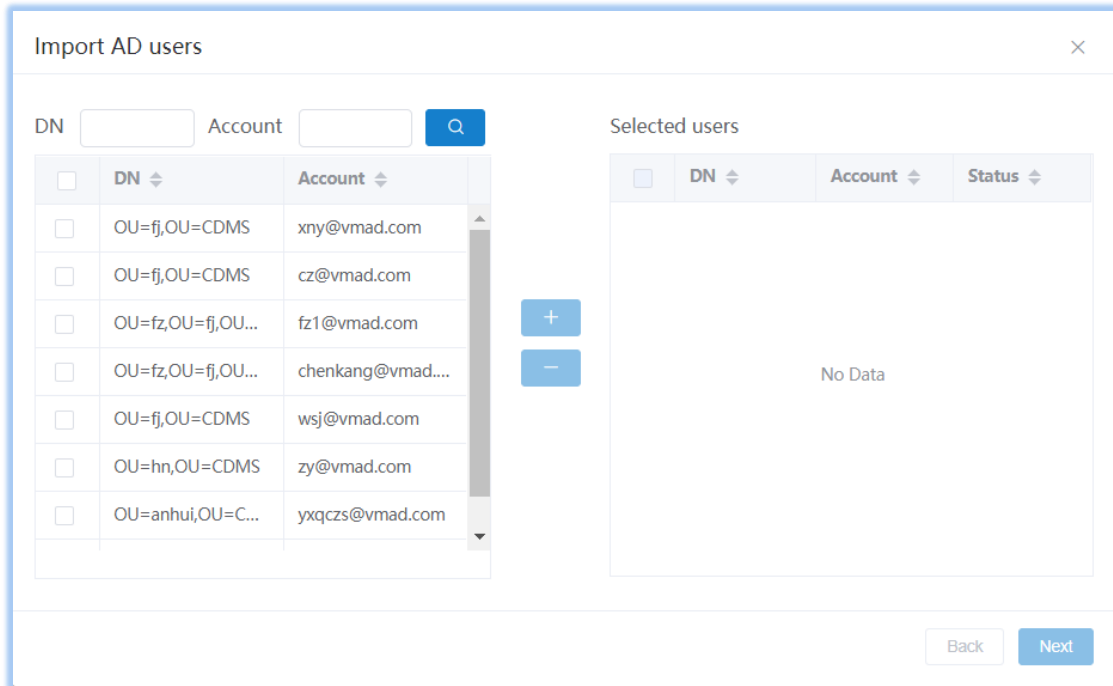
4.1.1.3 Import AD user

There is no restriction to user importing

Right click 'User management' then select 'Import AD users'



AD user is detected, the LDAP connection should be configured before import AD user



Select the users about to be imported, status should be existed for user who has imported. Otherwise, the status would be 'Not used'

Import AD users

DN

Account

Q

☐	DN	Account
☐	OU=fj,OU=CDMS	xny@vmad.com
☐	OU=fj,OU=CDMS	cz@vmad.com
☐	OU=fz,OU=fj,OU=...	fz1@vmad.com
☐	OU=fz,OU=fj,OU=...	chenkang@vmad.com
☐	OU=fj,OU=CDMS	wsj@vmad.com
☐	OU=hn,OU=CDMS	zy@vmad.com
☐	OU=anhui,OU=C...	yxqczs@vmad.com

+

-

Selected users

☐	DN	Account	Status
☐	OU=fj,OU=...	xny@vmad...	Existed
☐	OU=fj,OU=...	cz@vmad.c...	Existed
☐	OU=fz,OU=f...	fz1@vmad.c...	Not used

Back

Next

Click 'Next' to import the users for basic information and group resource editing status should be 'Universal' when user is not existed in CDMS

Selected users

Basic information

User role

Client group resource

xny@vmad.com(OU=fj,OU=...

cz@vmad.com(OU=fj,OU=...

fz1@vmad.com(OU=fz,OU=...

Username

xny@vmad.com

* Real name

xienengyanxny

Manager or not

No

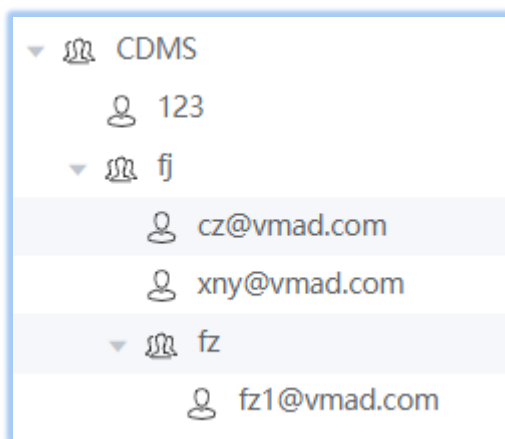
Phone

Email

Unit

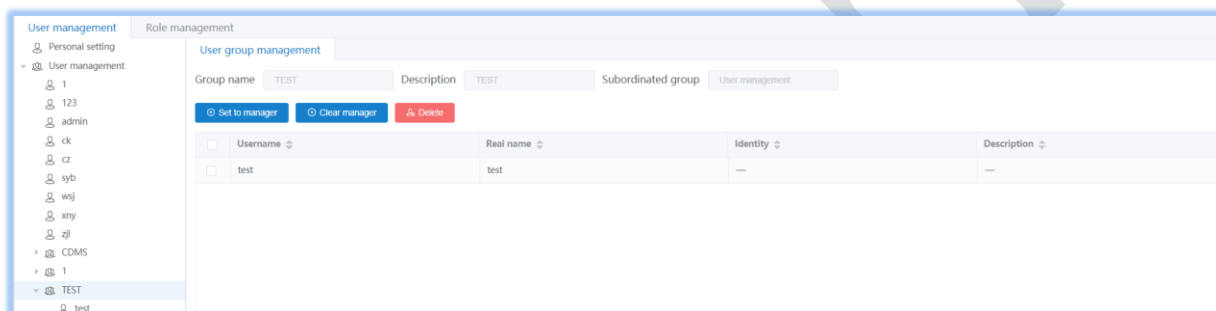
Description

If importing AD user success, a tree structure would be shown on the basis of AD structure, the figure shown as below;

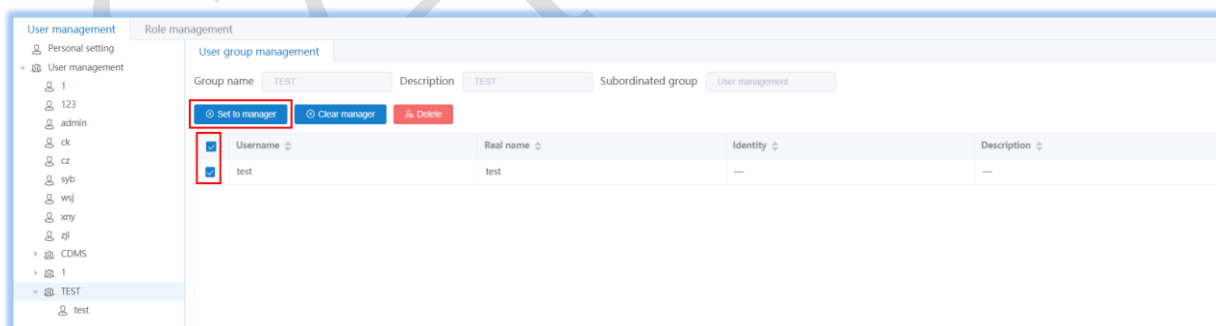


4.1.1.4 Manager

Manager can handle all permissions in the group; who also have permission to add, remove, edit the all AD user info



Select one of user, then click 'Set to manager', to give user the permission of manager



Likewise, the manager role also can be removed

User management

Personal setting

User management

Role management

User group management

Group name

TEST

Description

TEST

Subordinated group

User management

Set to manager

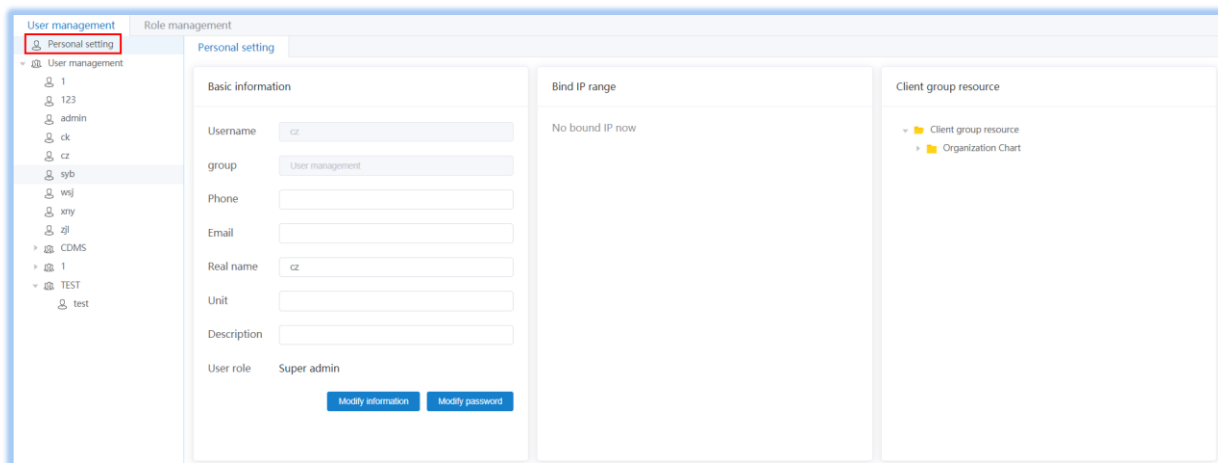
Clear manager

Delete

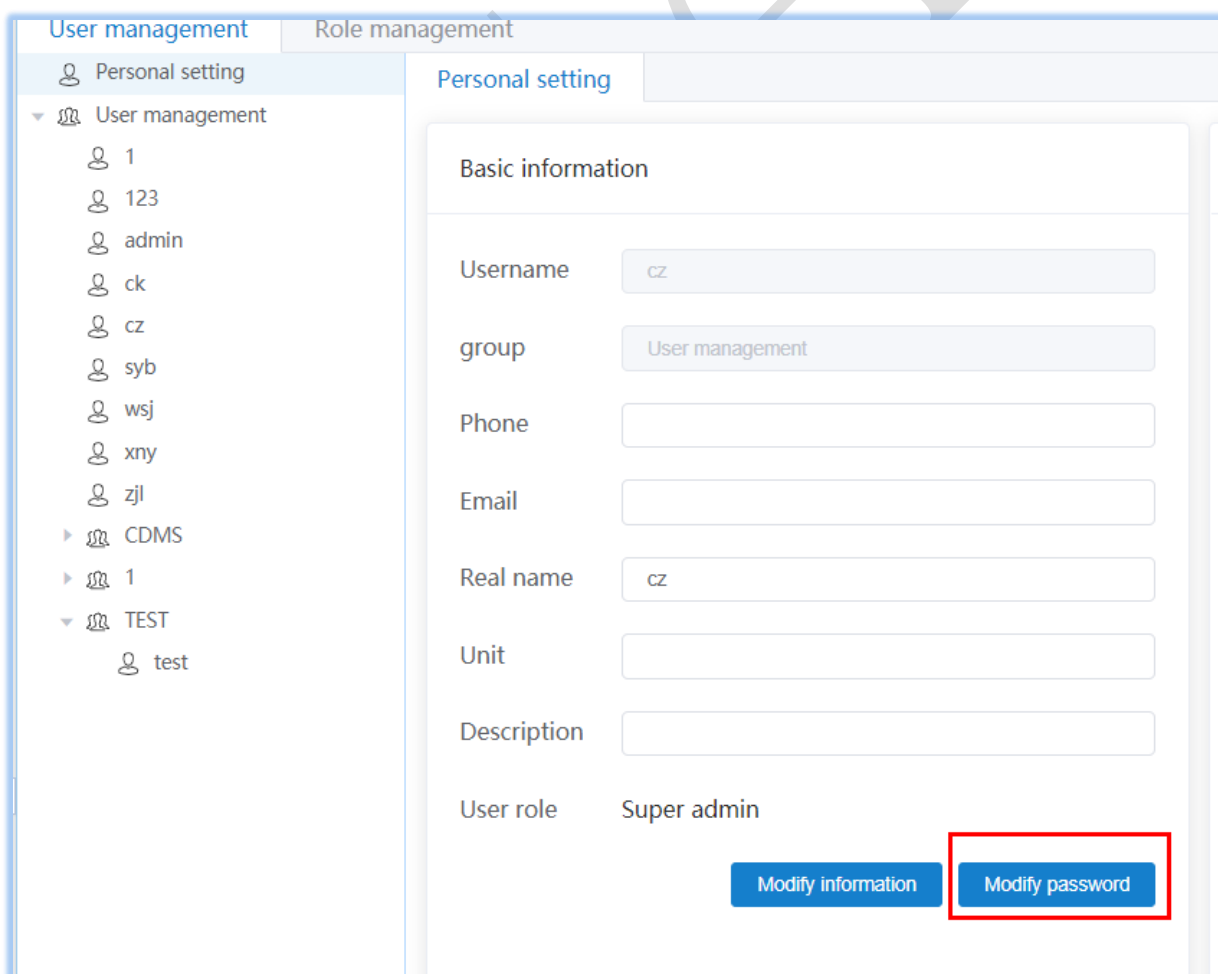
☒	Username	Real name	Identity	Description
☒	test	test	Charger	—

4.1.1.5 Individual settings

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).



Change the individual password according to the following figure.



4.1.2 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”.

User management

Role management

Role information

⊕ Add

✎ Edit

🗑 Delete

☐	User role ⇅	Description ⇅
☐	Super admin	Super admin
☐	Universal	Universal
☐	1111	—

Add role

* Role name

TestRole

Description

TestRole

☐	Permission name	Description
☒	Power control	remotely wake up, shut down ...
☐	Remote assistance	guide the client for operation
☐	Software blacklist and whitelist...	disable certain software (blackl...
☐	Blacklist and whitelist manage...	Add, delete and modify the bl...
☐	Client configuration	configure parameters of client ...
☐	File deployment	Remotely distribute software a...

Confirm

Cancel

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

Role information

Add

Edit

Delete

☐	User role	Description
☐	Super admin	Super admin
☐	Universal	Universal
☐	1111	—
☐	TestRole	TestRole

4.2 Resource center

4.2.1 Introduction

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.

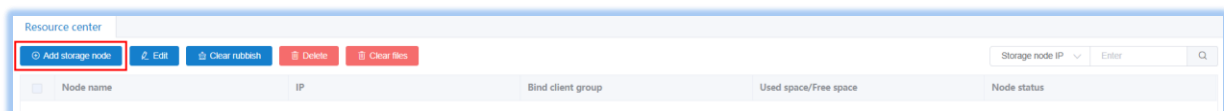
If one client group is bound with many storage nodes, it represents that the client group can acquire resources from these bound storage nodes to improve the transmission efficiency. If one storage node is bound with many client groups, it represents that many client groups share resources in one storage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

4.2.2 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.

Add storage node
×

* Node name

* Bind client group

Organization Chart

Browse

* IP

* Port

444

Connected

Confirm

Cancel

- 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.

Add client group
×

☒ Organization Chart

☐ xny
 ☐ zjl
 ☐ wsj
 ☐ aadd

Confirm

Cancel

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

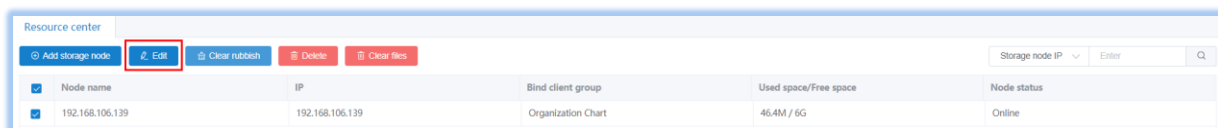
Resource center					
Add storage node Edit Clear rubbish Delete Clear files Storage node IP Enter Q					
☒	Node name	IP	Bind client group	Used space/Free space	Node status
☒	192.168.106.139	192.168.106.139	Organization Chart	46.4M / 6G	Online

4.2.3 Binding changes

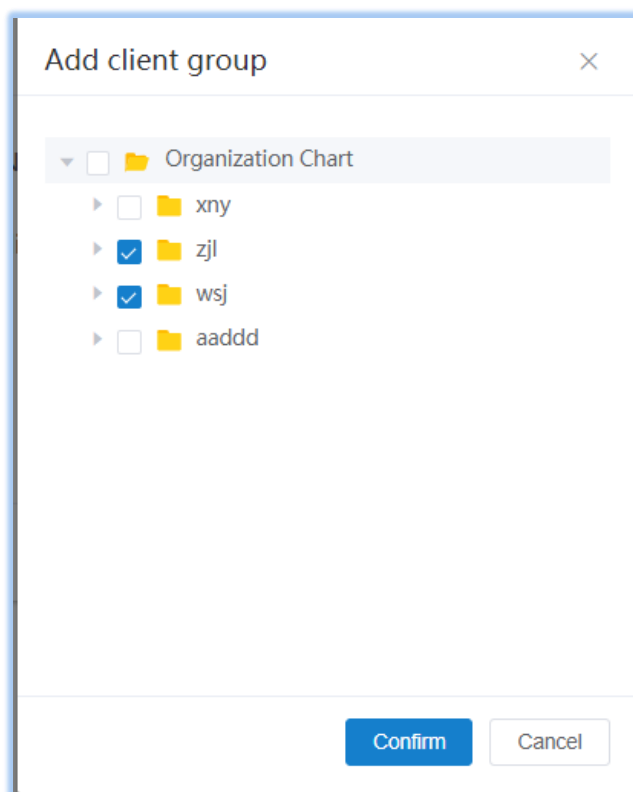
When the location of storage node changes or the storage node is discarded, it is necessary to release or change the binding of storage node. Refer to following method:

1. Change binding

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



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



Edit

*

Node name

192.168.106.139

*

Bind client group

zjl,wsj

Browse

*

IP

192.168.106.139

*

Port

444

Connected

Confirm

Cancel

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

Resource center					
Add storage node Edit Clear rubbish Delete Clear files Storage node IP Enter Q					
☐	Node name	IP	Bind client group	Used space/Free space	Node status
☐	192.168.106.139	192.168.106.139	zjl,wsj	46.4M / 6G	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.

Resource center					
Add storage node Edit Clear rubbish Delete Clear files Storage node IP Enter Q					
☒	Node name	IP	Bind client group	Used space/Free space	Node status
☒	192.168.106.139	192.168.106.139	zjl,wsj	46.4M / 6G	Online

4.2.4 Clean storage node

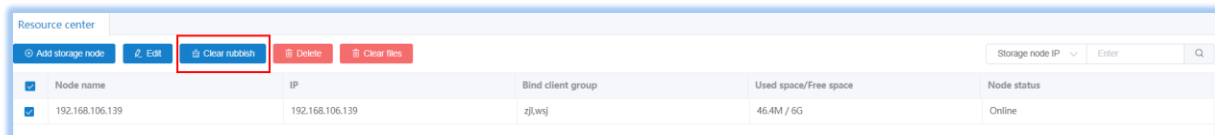
After long term using of storage node, a lot of junk files will generate and the hard disk space will become small. User can clean the storage node by following method.

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

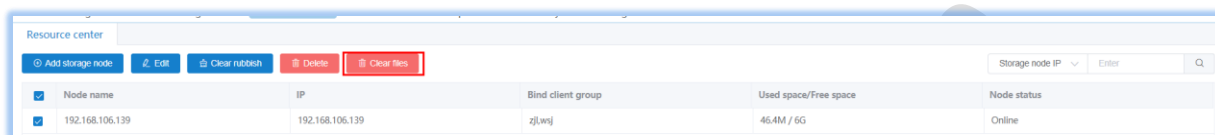
may occur.



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.



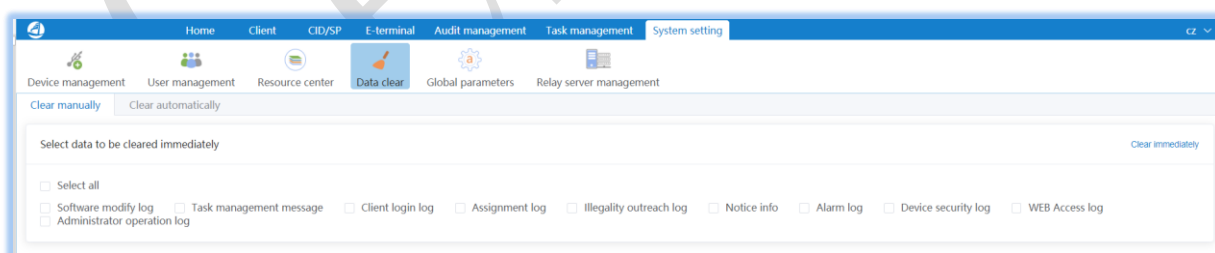
4.3 Data cleaning

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.

4.3.1 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.



4.3.2 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.

Clear manually

Clear automatically

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

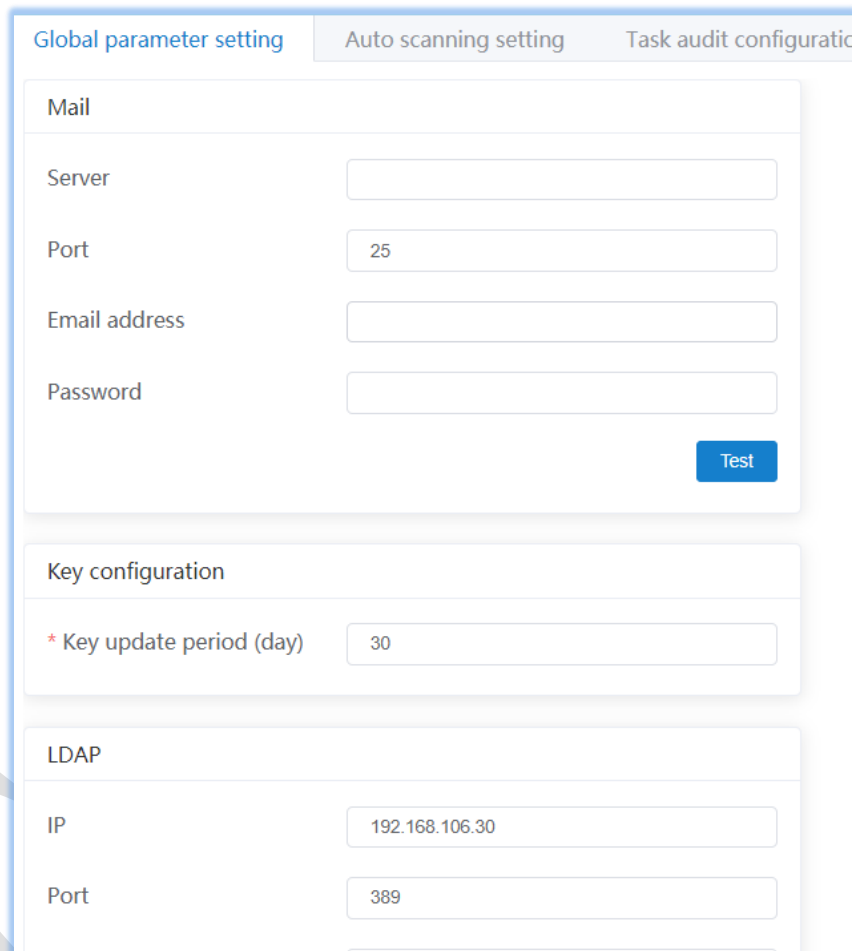
☒ Select all		
☒ Software modify log	30	Day
☒ Task management message	90	Day
☒ Client login log	5	Day
☒ Assignment log	30	Day
☒ Illegality outreach log	30	Day
☒ Notice info	30	Day
☒ Alarm log	30	Day
☒ Device security log	30	Day
☒ WEB Access log	7	Day
☒ Administrator operation log	30	Day

4.4 Global parameters

4.4.1 Global parameter settings

1. Mail settings

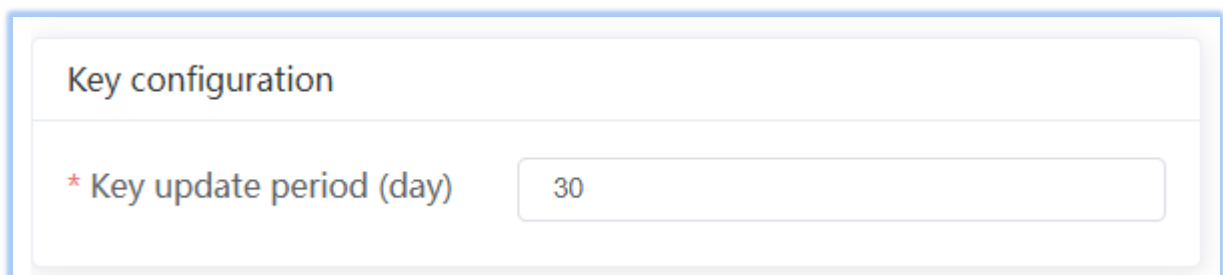
On the global parameter page, the administrator can set the mail server for the system. When the system sends alarm information, the server will send the mail.



The screenshot shows the 'Global parameter setting' tab selected. It contains three main sections: 'Mail', 'Key configuration', and 'LDAP'. The 'Mail' section has fields for 'Server', 'Port' (set to 25), 'Email address', and 'Password', with a 'Test' button. The 'Key configuration' section has a field for '* Key update period (day)' set to 30. The 'LDAP' section has fields for 'IP' (set to 192.168.106.30) and 'Port' (set to 389).

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.



This is a close-up of the 'Key configuration' section from the previous screenshot. It shows the label 'Key configuration' and a single input field for '* Key update period (day)' with the value '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

Be sure to enable remote assistance ☐

Only Windows is valid, please set in the client parameters for Linux

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 ☐

Unlock

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. Task configuration

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

task configuration

* Task default time(days)

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 ☐

9. LDAP Settings

LDAP settings could allow domain users to join to CDMS, then login to CDMS by domain user account

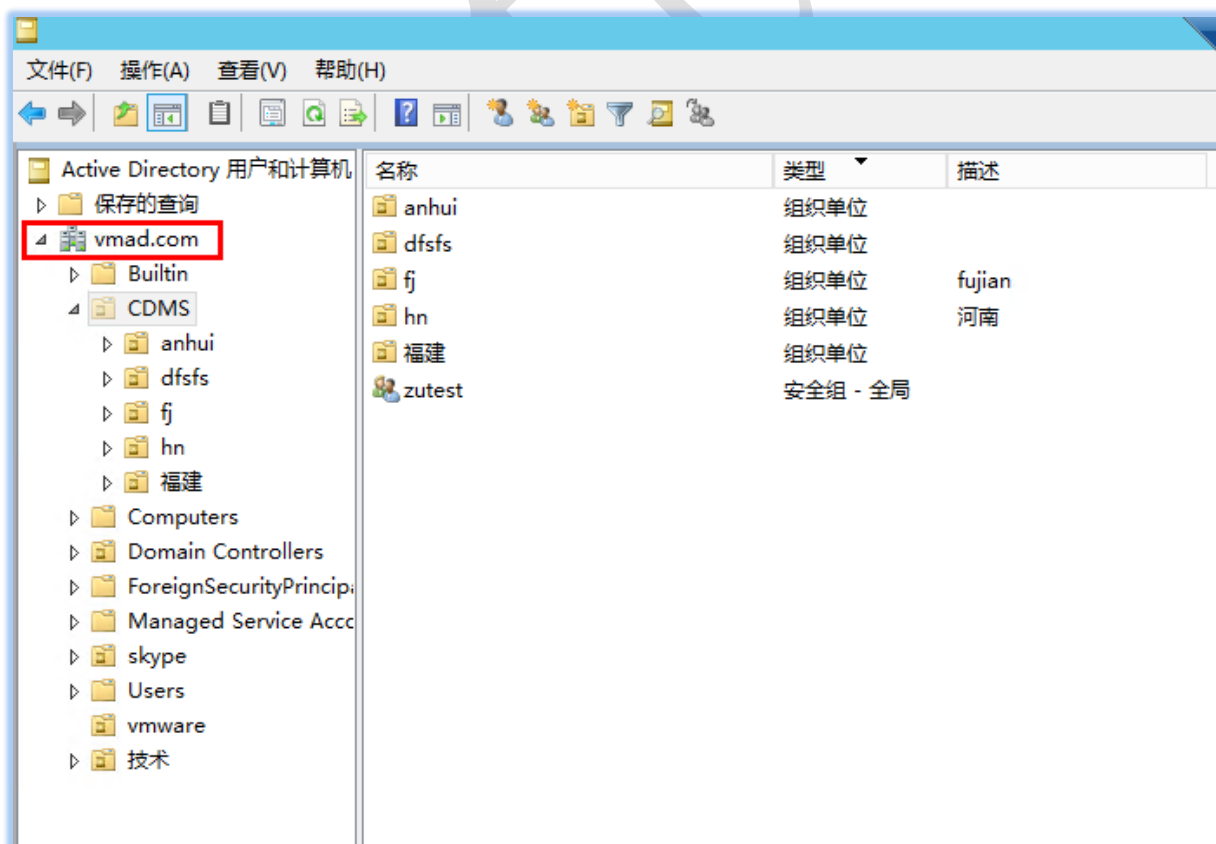
LDAP

IP	192.168.106.30
Port	389
Basic path	dc=vmad,dc=com
Account DN	cn=Administrator,cn=Users,dc=vmad,dc=com
Password	
Search path	OU=CDMS

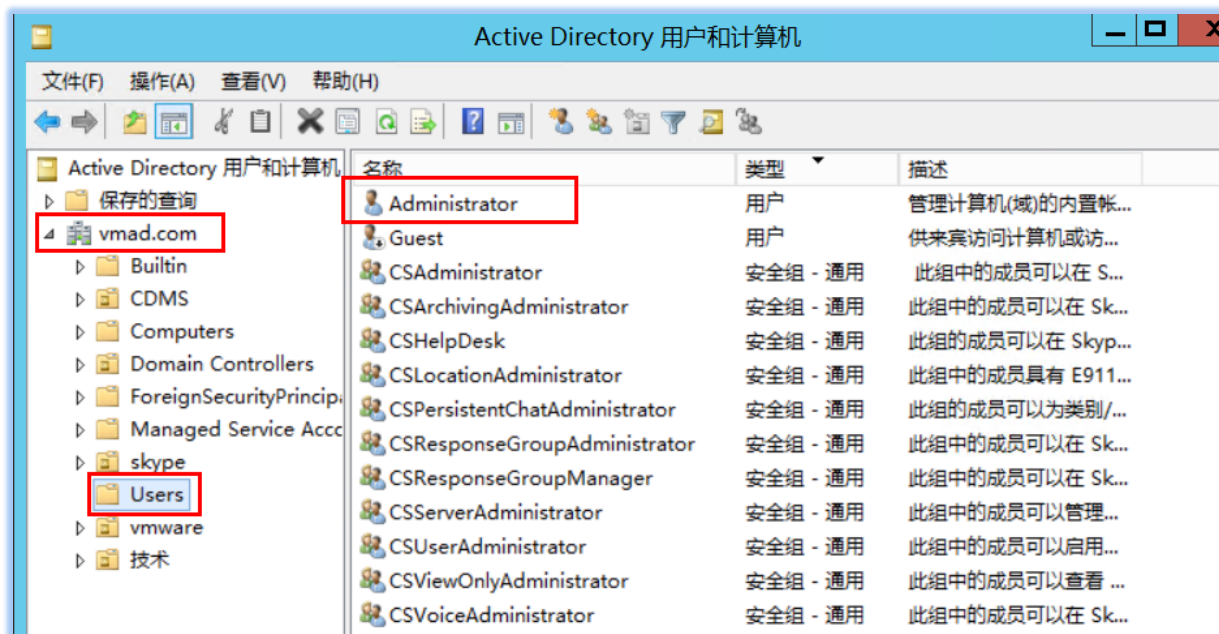
Test

PS:

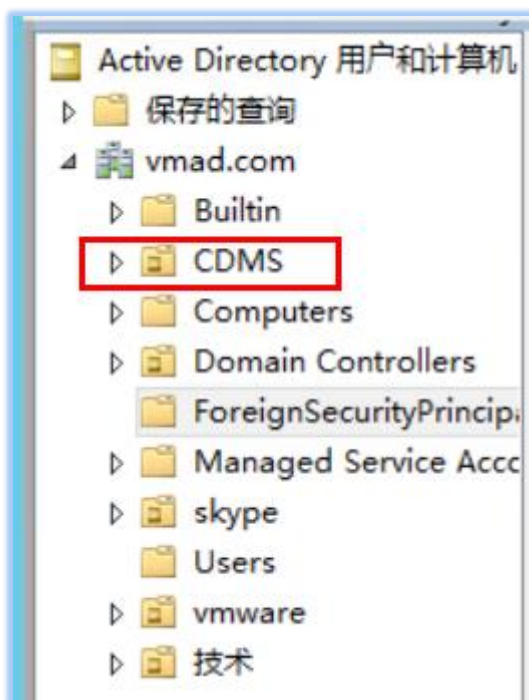
1. Basic path is the server address of Domain controller



2. Account DN shows the role of user in DC



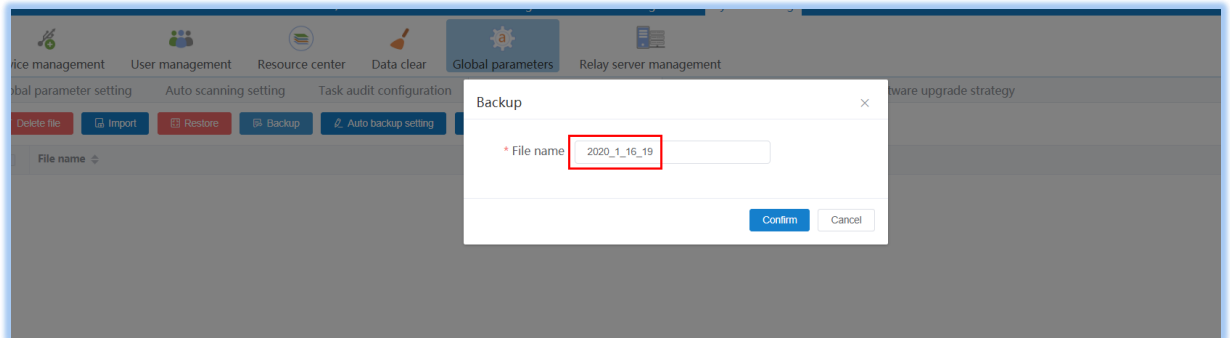
3. Search path is a filter for research



4.4.2 Database backup and restore

4.4.2.1 Backup

Click 'Backup' to start backup the database

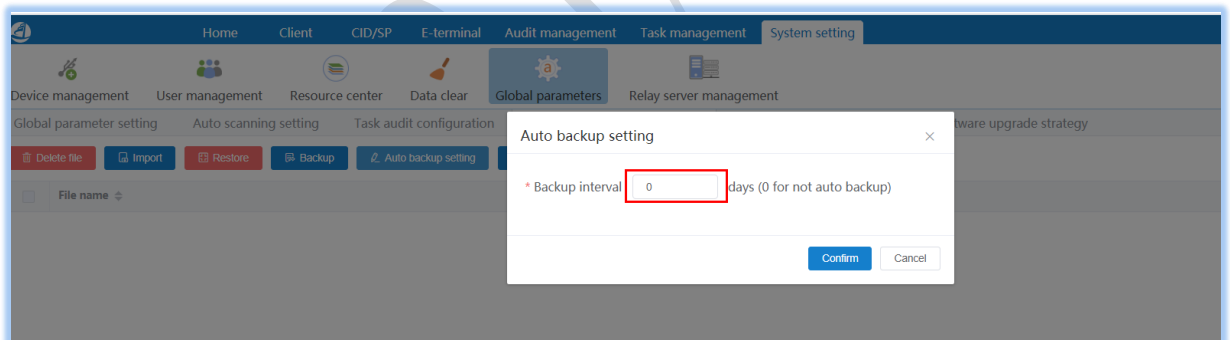


4.4.2.2 Restore

Select the database record, click 'Restore' to recovery

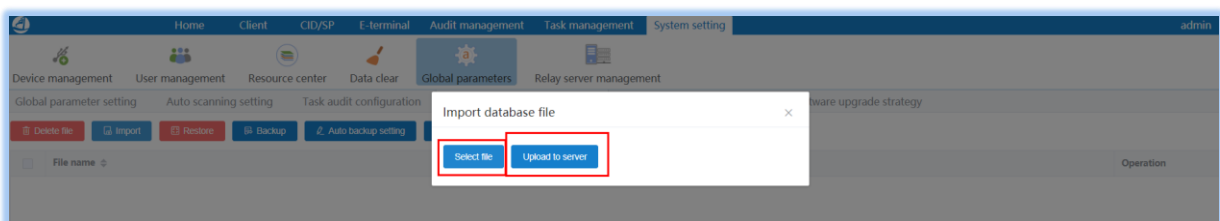
4.4.2.3 Backup automatically

Backup interval can be set for task execution automatically.



4.4.2.4 Import

Database in local host is allowed to be imported



4.4.3 Organization structure import and export

Enable to import and export info of client, group and user info for moving organization structure more efficient

4.4.4 Peripheral firmware upgrade

Enable to upgrade the peripheral firmware or software for user to deploy more convenient