User Manual

Centerm Cloud Client Manager

CCCM 5.2.003.000

Issue: 01

Date: 2014-06-26

Centerm Information Co., Ltd.

Centerm™

Trademarks

Centerm and other Centerm trademarks are the registered trademarks of Centerm Information Co., Ltd.

All other trademarks or registered trademarks as mentioned in this document are owned their respective owners.

Disclaimer

The purchased products, services and features are stipulated by the contract made between Centerm and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, the information contained in this document is provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

Due to product upgrade or other reasons, the information in this document is subject to change without further notice.

Unless otherwise stated, this document is for reference only. All statements, information and recommendations in this document do not constitute the warranty of any kind, express or implied.

Centerm Information Co., Ltd.

Add:	2nd Floor, Building 22, Star-Net Sci. & Tech. Park, Juyuanzhou, 618 Jinshan Avenue, Fuzhou City, Fujian Province
Tel:	400-158-1515
Fax:	86-591-83057710
Postcode:	350002
Website:	http://www.centerm.com
Customer Service Email:	centermfw@centerm.com

Foreword

Thank you for choosing Centerm Cloud Client Manager, which was independently developed by Centerm Information Co., Ltd. Before using this product, please carefully read this Manual.

Reminder Description

Note

NOTE provides additional information (explanatory note, explanation or instruction) to emphasize or supplement the main text.

Caution

CAUTION indicates a potentially hazardous situation that, if not avoided, could result in the failure in installation/use/operation, equipment damage, data loss, performance deterioration, or other unanticipated results.

- The **Cloud Terminal**, **Terminal** or **Client** as mentioned in this document, unless otherwise stated, shall all indicate the computer equipment installed with CCCM Agent.
- Unless otherwise stated, the deletion of document or record by all functional modules is irrevocable.

Revision History

Revision History describes the cumulative changes to the document. The latest document version contains all changes made in previous versions.

Document Version 01 (2014-06-26)

This version is the first official release.

Contents

1 Product Introduction

1.1 Overview

Centerm Cloud Client Manager (CCCM) allows automated management of clients and covers client configuration, Windows system backup/recovery, Windows software distribution, Windows Agent upgrade, Centerm Linux system upgrade, Centerm Linux patch upgrade, Centerm Linux Agent upgrade, Centerm Linux multi-file upgrade, automatic configuration, automatic upgrade, remote maintenance, performance monitoring, alarm management and other stunning features. Through CCCM, you can carry out efficient maintenance and management, thoroughly address such challenges as client deployment, maintenance and configuration faced by IT administrators, and integrate IT resources and thus significantly improve the efficiency of IT management through centralized management.

CCCM consists of the following five modules:

- Basic management: This is the module for basic client management and operation. It supports desktop configuration, remote assistance, power control, etc.
- Deployment management: Enabling file copying and installation on the client.
- Policy management: Allowing the management and configuration of relevant policies during the process of intelligent management.
- Public management: Allowing administrator management, system log management and client upgrade.
- Task management: The task management center of the management allows viewing, analysis and maintenance operations.

1.2 Product Features

- Instant configuration of client attributes.
- Batch-mode installation of applications.
- Real-time monitoring of client operation.
- Creation of client management plans which can be automatically and periodically executed without the need for manual intervention.

2 Quick Start

2.1 Login

After completing the installation of CCCM, perform the following steps to log in the system.

1. Open system login interface
   - Single-server mode

     On the server, go to **"Start -> All Programs -> Centerm -> Login"** to open the login interface.

   - Distributed mode

     On any server, open the browser and type the IP address of load balancer and the port used at installation in the address bar (as shown below). Add "http://" before the IP address. If the default port of 443 is used during the installation of management server, the port number can be omitted.

     `https://192.168.1.10/Terminal/logon.do`

     If the default port has been changed during the installation of management server (such as 8443), you will need to enter the new port number.

     `https://192.168.1.11:8443/Terminal/logon.do`

2. On the login interface, enter username, password and captcha, and then click "**Login**" to enter system homepage.

   The system has a default super administrator, with username being **"admin"** and password being **"Admin123!@#"**.

   Note:

   Upon first time login, you must change the initial password before you can proceed.

   If you enter the wrong password for three successive times, your current IP address will be blocked for one hour before you can try again, or you can try on another computer.

2.2 Interface Layout
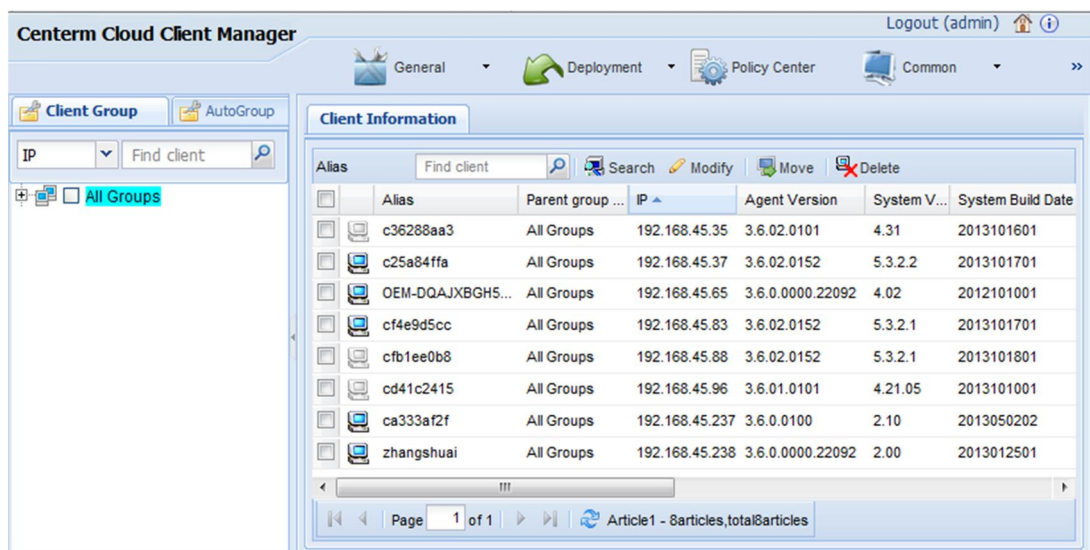
Quick links

The shortcuts in the top-right corner of system interface enable you to log out, return to system homepage and view license and version information.

- **Logout**: log out the current user and return to the login interface.
- (Home): return to system homepage.
- (About): show production version and license information.

Functional navigation

On the top navigation bar, click and select menu items to enter the corresponding operational interface.
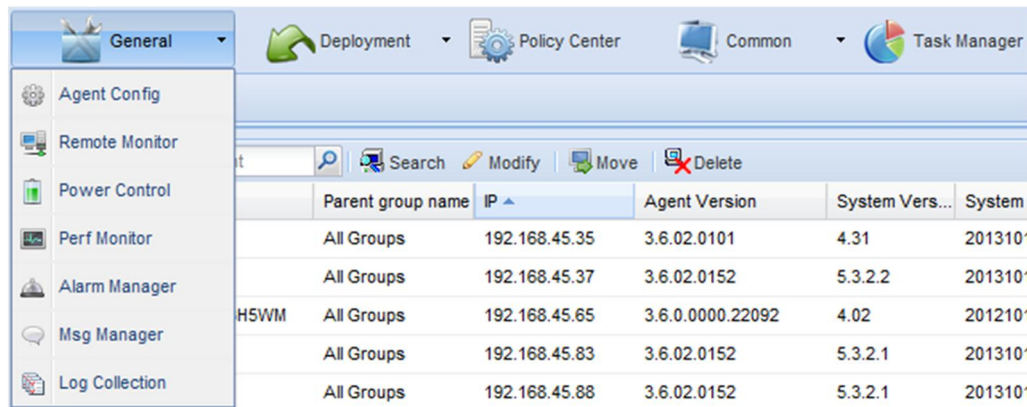
Client group

The **"Client Group"** panel on the left side shows the clients and groups managed by the current user. For details, please refer to "3 **Client Group Management**".
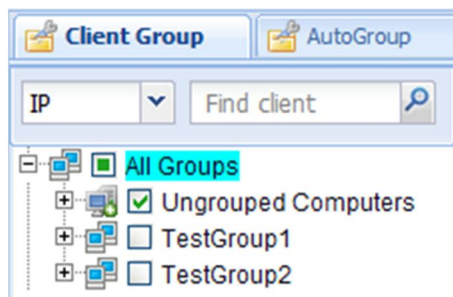
Client information

The **"Client Information"** panel shows the detailed information about clients managed. Click the name of client group or client in the left pane to view information about relevant clients.
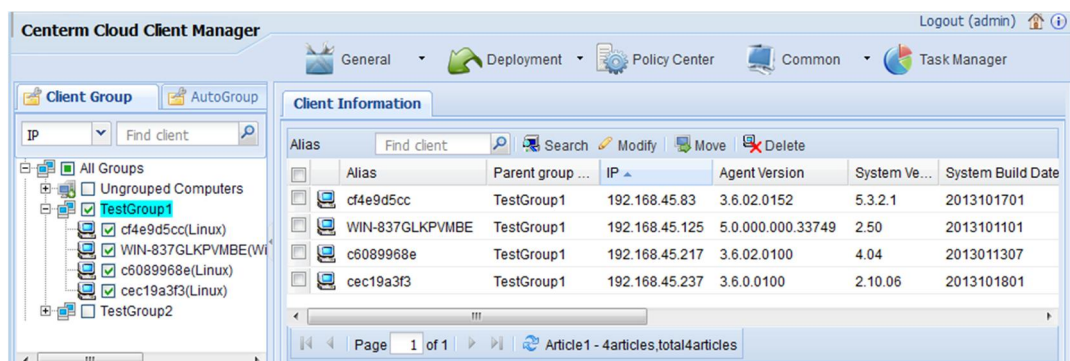
2.3 Search Client on the Server Side

Perform the following steps to manually search clients:

1. Right-click the name of any client group and select "**Search client**" from the context menu.

2. On the search interface, enter the IP range (if not entered, the Class-C network on which the server is located will be searched) and click "**Search**".

Search client(Group:All Groups)

Start IP Addr: 192.168.4.1   End IP Addr: 192.168.4.255   🔍 Search

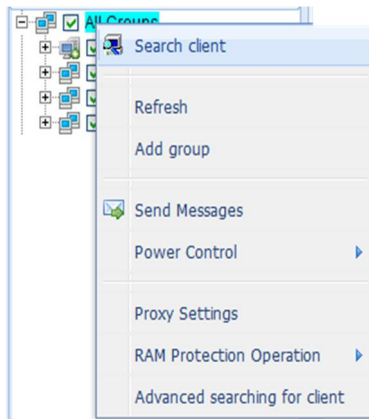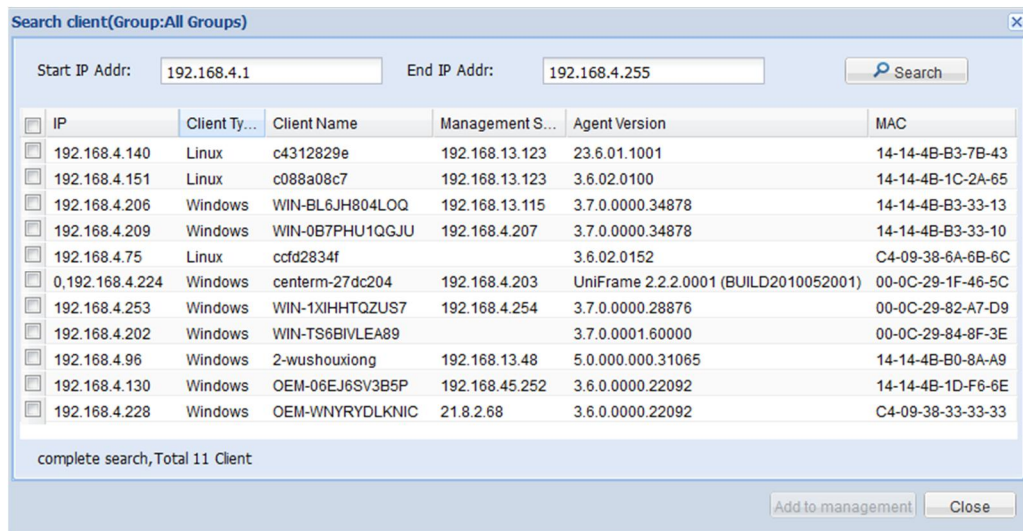|	IP	Client Ty...	Client Name	Management S...	Agent Version	MAC
☐	192.168.4.140	Linux	c4312829e	192.168.13.123	23.6.01.1001	14-14-4B-B3-7B-43
☐	192.168.4.151	Linux	c088a08c7	192.168.13.123	3.6.02.0100	14-14-4B-1C-2A-65
☐	192.168.4.206	Windows	WIN-BL6JH804LOQ	192.168.13.115	3.7.0.0000.34878	14-14-4B-B3-33-13
☐	192.168.4.209	Windows	WIN-0B7PHU1QGJU	192.168.4.207	3.7.0.0000.34878	14-14-4B-B3-33-10
☐	192.168.4.75	Linux	ccfd2834f		3.6.02.0152	C4-09-38-6A-6B-6C
☐	0,192.168.4.224	Windows	centerm-27dc204	192.168.4.203	UniFrame 2.2.2.0001 (BUILD2010052001)	00-0C-29-1F-46-5C
☐	192.168.4.253	Windows	WIN-1XIHHTQZUS7	192.168.4.254	3.7.0.0000.28876	00-0C-29-82-A7-D9
☐	192.168.4.202	Windows	WIN-TS6BIVLEA89		3.7.0.0001.60000	00-0C-29-84-8F-3E
☐	192.168.4.96	Windows	2-wushouxiong	192.168.13.48	5.0.000.000.31065	14-14-4B-B0-8A-A9
☐	192.168.4.130	Windows	OEM-06EJ6SV3B5P	192.168.45.252	3.6.0.0000.22092	14-14-4B-1D-F6-6E
☐	192.168.4.228	Windows	OEM-WNYRYDLKNIC	21.8.2.68	3.6.0.0000.22092	C4-09-38-33-33-33

complete search,Total 11 Client

Add to management   Close

3. Select the client to be managed and click "**Add to management**".
4. In the confirmation dialog box, click "**Yes**" to add the client(s).
5. In the "**Client Group**" pane, we can see that the clients have been added into the client group.

2.4   Send Message

To send a text message to the managed clients, perform the following steps:
1. In the "**Client Group**" pane, select the client group or at least one client.
2. On the navigation bar, click "**General > Msg Manager**".
3. Click "**Send Message**".
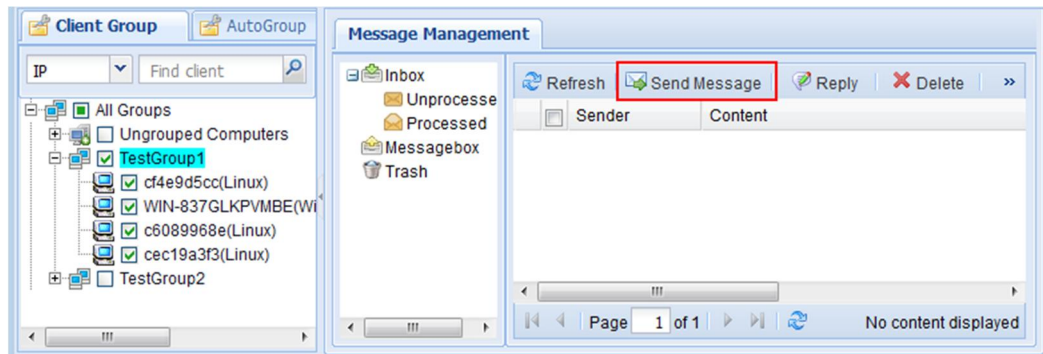
4. Type the message content and click "**OK**".
5. Select the corresponding OS version on the "**Plan Wizard**" interface and click "**Finish**".
6. Click "**Task Manager**" on the navigation bar to check task execution status.

3 Client Group Management

CCCM allows you to manage clients separately or in groups. There are two ways to group your clients:

- Manual grouping

  Use self-defined rules to manually group the clients (for example: by office or by department).

- Automatic grouping

  To group clients by operating system or software information.

3.1 Manual Grouping

On the client group panel, select "**Client Group**" to show manually grouped clients.
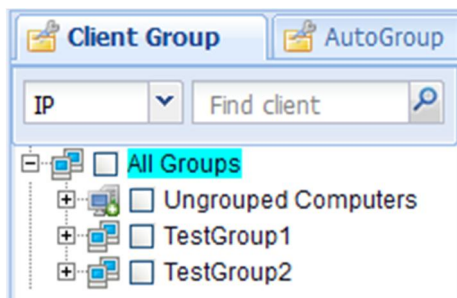
Classification of client groups

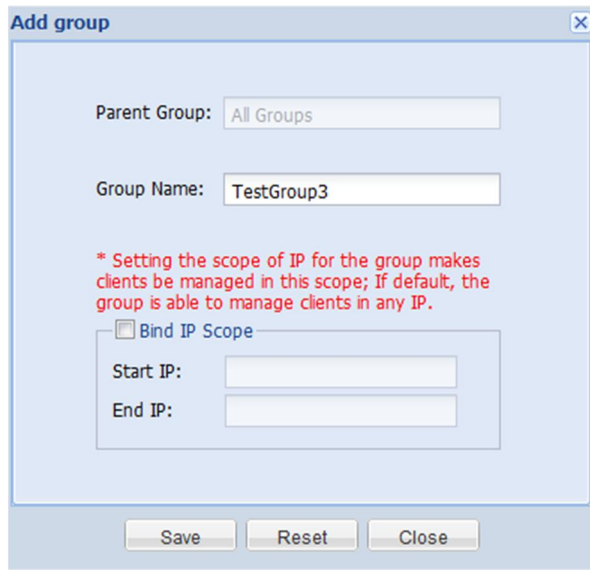There are two fixed groups in the **"Client Group"** pane:

- All Groups

  The parent group of all clients and groups. You can add clients and subgroups to this group, which cannot be modified or deleted by the user.

- Ungrouped Computers

  Ungrouped clients are under this group, and the user cannot modify or delete this group.

Add group

1. In the "**Client Group**" pane, right-click the name of client group to add a subgroup and select "**Add Group**" from the context menu.
2. Enter the group name.

Note:

> The group name must not contain /, \, :, *, ?, ", <, >, or |, and the length is limited to 32 characters.

Bind IP Scope

3. [Optional Step] Check "**Bind IP Scope**" and enter the IP scope.

   Note:

   > After binding the IP scope, the group can only manage clients falling within the specified IP scope.

4. Click "**Save**".

Delete group

1. In the "**Client Group**" pane, right-click the group to be deleted and select "**Delete**" from the context menu.

2.

   Caution:

   > All sub-groups and clients under this group will be deleted, and this operation is irrevocable.

   In the confirmation dialog box, click **"Yes"** to delete or **"No"** to cancel.

Modify group

1. In the **"Client Group"** pane, right-click the name of client group to add a subgroup and select **"Modify Group"** from the context menu.

2. Modify the information of client group.You can modify the group name and IP scope binding status.

3. Click **"Save"** to save the changes. Click **"Close"** to cancel or click **"Reset"** to restore to previous values.

Move group

1. In the "**Client Group**" pane, right-click the name of client group to add a subgroup and select "**Move**" from the context menu.

2. Select the new parent group and click "**OK**".

Refresh client group information

Client group information and the online status of clients will be refreshed periodically. To refresh immediately, right-click the name of **Client Group** to add a subgroup and select **"Refresh"** from the context menu.

3.2   Automatic Grouping

CCCM will group clients automatically according to the defined grouping rules, and the grouping results could be different if different rules are applied. Automatic groups cannot be edited.

On the client group panel, select **"AutoGroup"** to show automatically grouped clients.
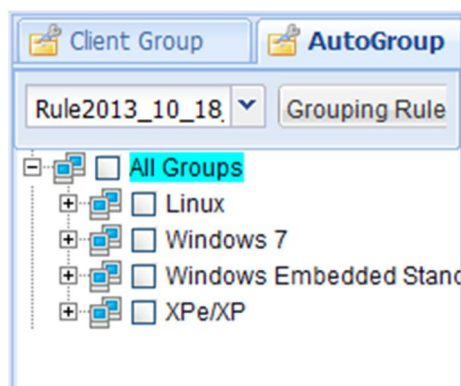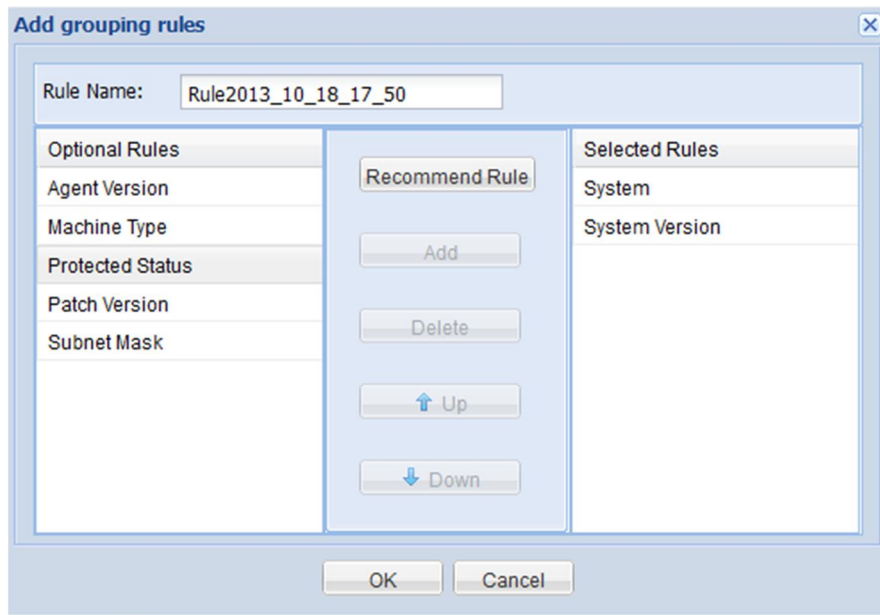

Grouping rule manager

Add grouping rules

1. In the "**AutoGroup**" pane, click "**Grouping Rule**".
2. In the "**Grouping Rule Manager**" window, click "**Add**".
3. Click "**Recommend Rule**" to create the grouping rule recommended by the system, or select the grouping conditions to create your own rules.

   You can repeatedly add or delete the grouping conditions, or change the sequence thereof. The sequence of grouping conditions corresponds to the results of automatic grouping.

Note:

- You can add up to 5 grouping conditions for each grouping rule.
- When grouping conditions contain "**Patch Version**", the patch version must be edited.

4. Click "**OK**" to save the grouping rule.

Modify rule

1. In the "**AutoGroup**" pane, click "**Grouping Rule**".
2. In the "**Grouping Rule Manager**" window, select the grouping rule and click "**Modify**".
3. Modify the grouping rule and click "**OK**" to save the grouping rule.

   Note:

   - You can add up to 5 grouping conditions for each grouping rule.
   - When grouping conditions contain "**Patch Version**", the patch version must be edited.

Delete rule

1. In the "**AutoGroup**" pane, click "**Grouping Rule**".
2. In the **"Grouping Rule Manager**" window, select the grouping rule and click "**Delete**".
3. Click "**Yes**" to delete the grouping rule.

Switch grouping rule

1. In the "**AutoGroup**" pane, click the drop-down arrow to expand the list of grouping rules and select the rule to be applied.
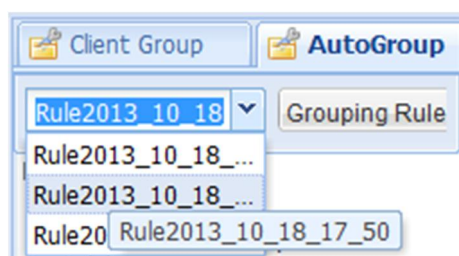


2. Click "**OK**" to apply the grouping rule.

3.3 Ungrouped Computers

For automatically registered clients whose IP addresses are not included the bound IP scope of any group, they will be added into **"Ungrouped Computers"**. All clients belonging to no group will also be added to **"Ungrouped Computers"**.

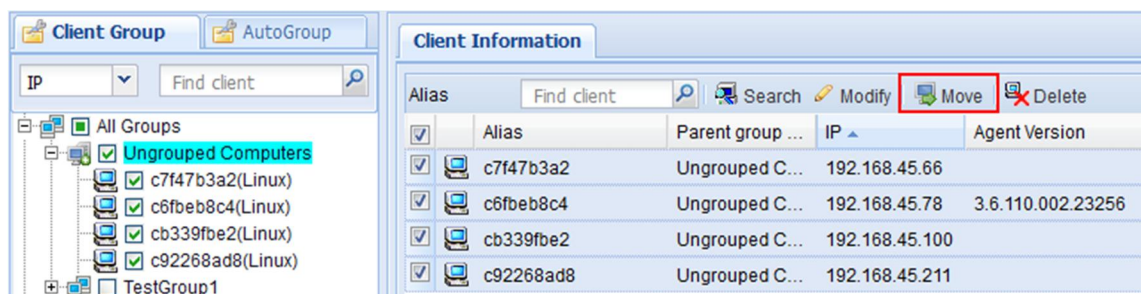Perform the following steps to add ungrouped computers to other groups.

Single-client dragging

You can drag any client in **"Ungrouped Computers"** to the target group.
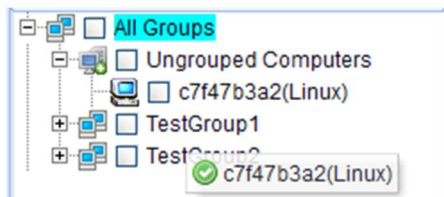
Batch-mode moving

1. Click quick link 🏠 to return to system homepage.
2. Click "**Ungrouped Computers**".
3. On the "**Client Information**" panel, select clients and click "**Move**".

4. Select target group and click "**OK**".

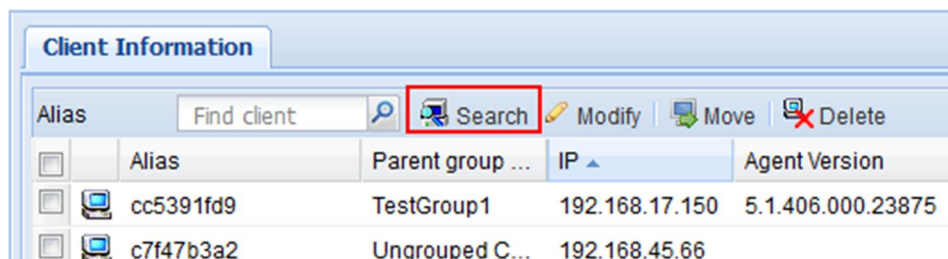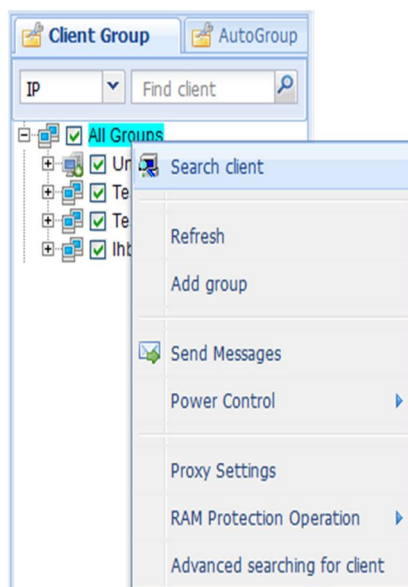# 4 Client Management

4.1 Search Client

Clients to be managed must be installed with CCCM Agent, or else CCCM cannot search and manage clients. There are three ways to search clients.

- Search client on the server side
- Automatic registration
- Manual configuration

Search client on the server side

The administrator can search clients falling within the specified network segment through manual search on the server side and add them to the client group.

1. Right-click the name of client group and select "**Search client**" from the context menu, or click "**Search**" on the "**Client Information**" panel to open the search interface.

2. On the search interface, enter the IP range (if not entered, the network segment on which the server is located will be searched) and click "**Search**".

3. Select the client to be managed and click "**Add to management**".
4. In the confirmation dialog box, click "**Yes**" to add the client(s).

   Note

   If the thin client had already managed by other server, in put correct client password can realize preemption and batch preemption.

5. View newly added client(s) in the "**Client Group**" pane.
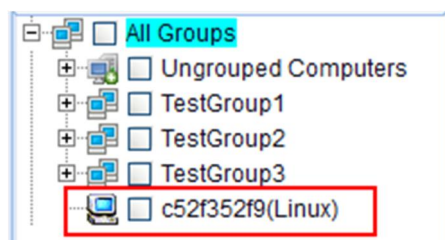
Automatic registration

On the network where clients get IP address via DHCP, the Agent on client will check DHCP lease file to check whether or not Option 232 has been defined. Option 232 carries the IP address and communication port of CCCM server. This extended option uses the prefix of CENTERM_CDMS_SERVER. The prefix, IP address, and port number are divided by colon (":"). For example, the following Option 232 is found in the DHCP lease file of the client.

```
CENTERM_CDMS_SERVER:192.168.1.10:8081
```

The client will try to connect to the server with IP address being 192.168.1.10 and will use the port number of 8081.

When the client gets the sever address from Option 232, it will send online commands to the server, which will add the client to **"Ungrouped Computers"**, or to the group with bound IP scope.

To configure Option 232 on the DHCP server, please refer to "**27.2 Configure DHCP Option**".

Manual configuration

You can directly configure the server address on the client, which will send online command to the server and then server will add the client to **"Ungrouped Computers"** or to the group with bound IP scope. To manually configure the server address on the client, please perform the following steps:

Windows thin client

1. On the taskbar of Windows thin client, right-click the tray icon and select "**CCCM > Preference**" to open the "**Preference**" dialog box.
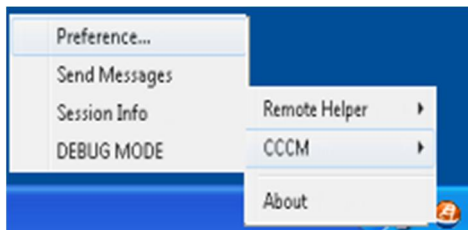
2. Select "**Config by yourself**" and enter the IP address of management server. In case of clustered deployment mode, enter the IP address of load balancing server. The default port number is 8081 (the same as the communication port set when installing the management server).
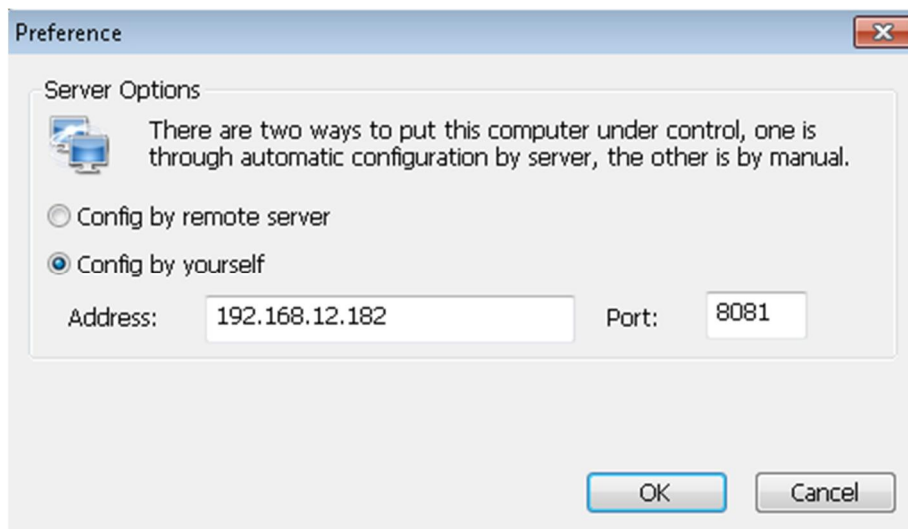
3. Click "**OK**" and enter the confirmation password to save. The default password is `centerm123!@#`.

Linux thin client

1. On the taskbar of Linux thin client, right-click the tray icon to open the settings interface.

2. Select "**Config by yourself**" and enter the IP address of management server. In case of clustered deployment mode, enter the IP address of load balancing server. The default port number is 8081 (the same as the communication port set when installing the management server).
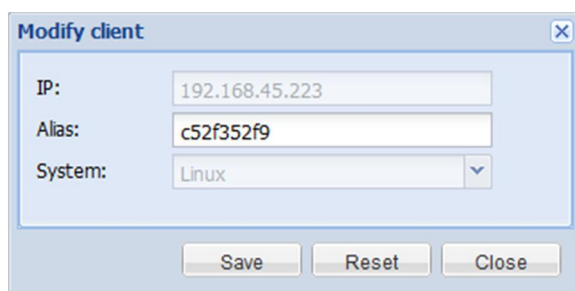
3. Click "**OK**" and enter the confirmation password to save. The default password is `centerm123!@#`.

4.2 Modify Client

1. Right-click the client and select "**Modify client**" from the context menu.

2. In the "**Modify client**" dialog box, change the alias of the client and click "**Save**".

Note:

● The alias must not contain /, \, :, *, ?, ", <, >, or |, and the length is limited to 32 characters.

● "**IP**" and "**System**" options cannot be modified.

4.3   Delete Client

1. Right-click the client to be deleted and select "**Delete**".
2. In the confirmation dialog box, click "**Yes**".

   While deleting the client, the operation will be proceeded differently according to the online status of client:

   - Client is online: The management server of the client will be set null immediately and the client will be removed from the list. This means the client will no longer be subject to the management of this server and can be added by another server.
   - Client is offline: After the client goes online, it will connect to the server and be added to "**Ungrouped Computers**" or to the group with bound IP scope.
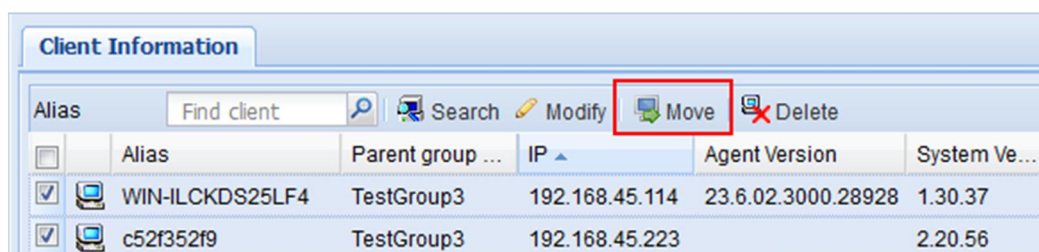
4.4   Move Client

There are two ways to move clients in the **"Client Group"**.

- Drag the client to the new group.
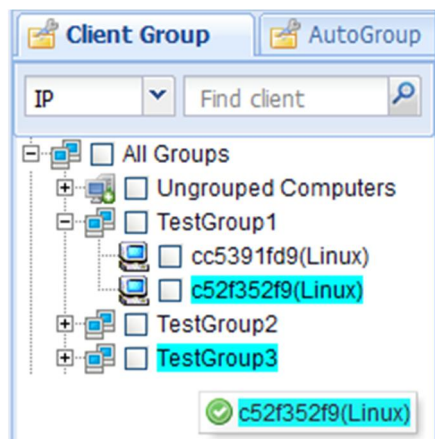
- Select the client(s) on the "**Client Information**" panel and click "**Move**". Select the target group in the pop-up dialog box and click "**OK**" to save.

4.5   Agent Configuration

Through Agent configuration, the administrator can change the server address and management password for managed clients. Perform the following steps to proceed with Agent configuration:

1. Right-click the client or client group, and then select "**Proxy Settings**".
2. Change relevant settings in the dialog box.
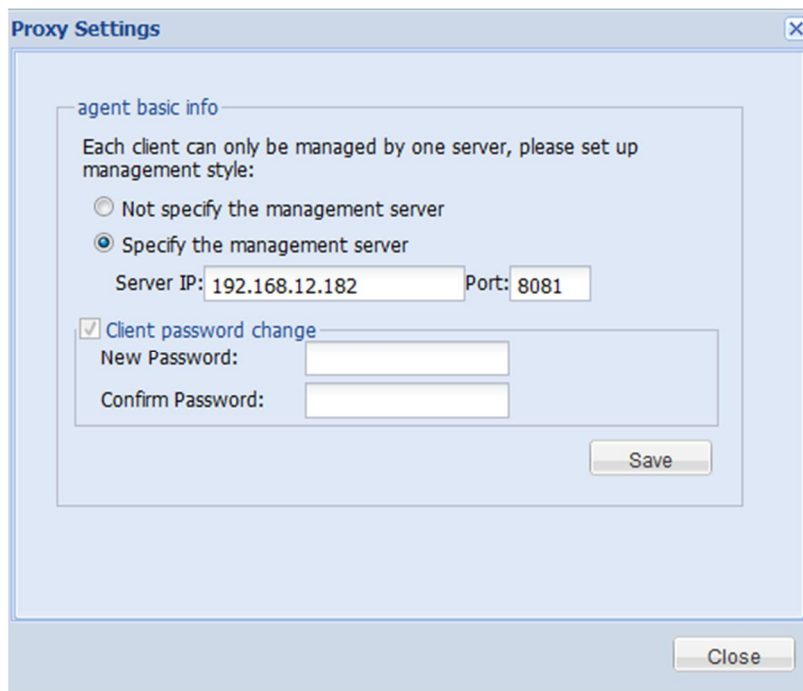
Management style:

- Not specify the management server

  The selected client won't be managed by any server, and must be added to management again.

- Specify the management server

  The selected client will be managed by the specified server, and the IP address and port of the server must be provided.

Client password change:

- To change the configuration password for client, so as to avoid unintended uninstallation of Agent. Initial password: `centerm123!@#`.

4.6 RAM Protection Operation

For Windows thin clients, the following types of RAM protection operations are supported:

- Enable protection: check RAM protection on the selected client.
- Disable protection: disable RAM protection on the selected client.
- Submit data: submit the current operations performed by the client.

To enable RAM protection for Windows thin clients, perform the following steps:

1. Right-click the client or client group and select "**RAM Protection Operation**".
2. Select the desired operation type from the secondary menu.

4.7 Search Client

Simple search

In the **"Client Group"** pane, you can set the conditions for searching clients. Matched client(s) will be highlighted in blue color.
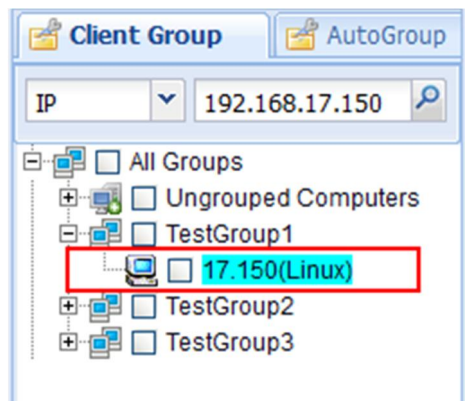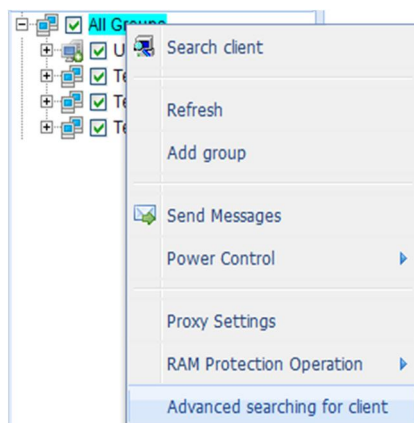
Advanced search

Advanced search allows you to find out clients meeting multiple conditions. By conducting advanced search in a specific group, all clients from this group and meeting search conditions will be listed.

To proceed with advanced search, perform the following steps:

1. Right-click the client group and select "**Advanced search for client**".

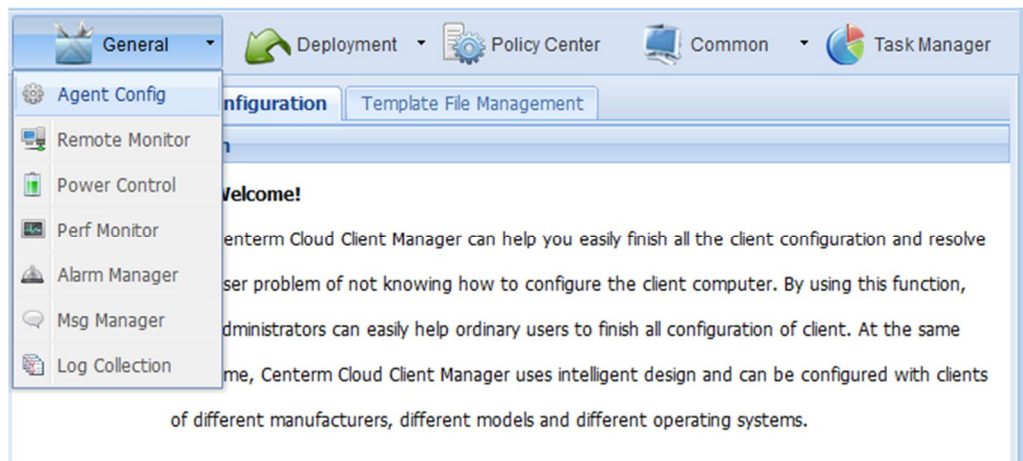2. Define at least one search condition and click "**Find**".

3. The search results will be listed in the "**Client Group**" pane. Click "**Back**" to return to the list of manually grouped clients.

5 Client Configuration

5.1 Client Parameters Configuration

Click **"General > Agent Config"** to enter the client configuration interface, as shown below:

5.1.1 Configuration of Windows client parameters

Click **"General > Agent Config"** to enter the client configuration interface. In the **"Client Group"** pane, click the Windows client to show the following configuration interface:
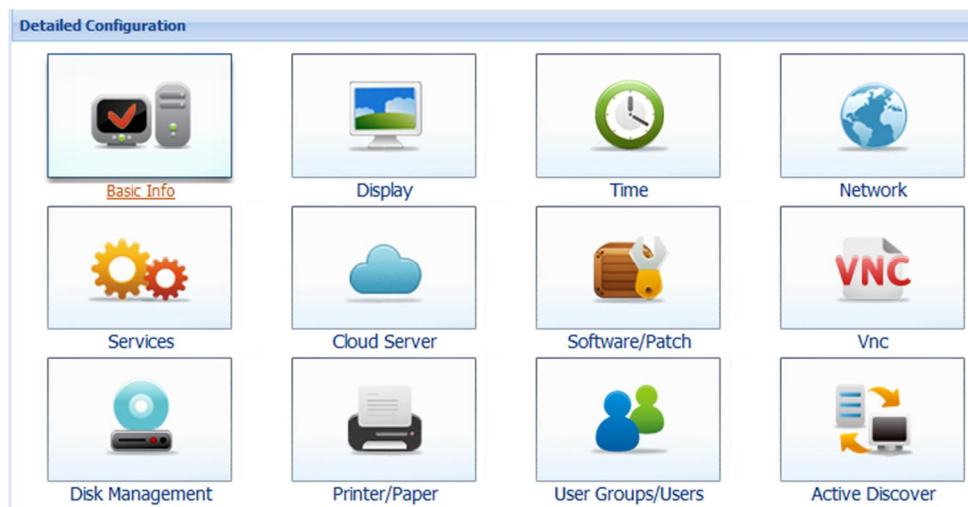

Note:

As the terminal version, this shows the functions and contents of screen will be slightly different.

VNC

VNC is used to set the options and parameters for client remote monitoring. As shown below, **"Share"** allows you to set the client control permission for the server. **"Security"** allows you to enable/disable password authentication, which targets the third-party VNC connection tools and is generally not required.
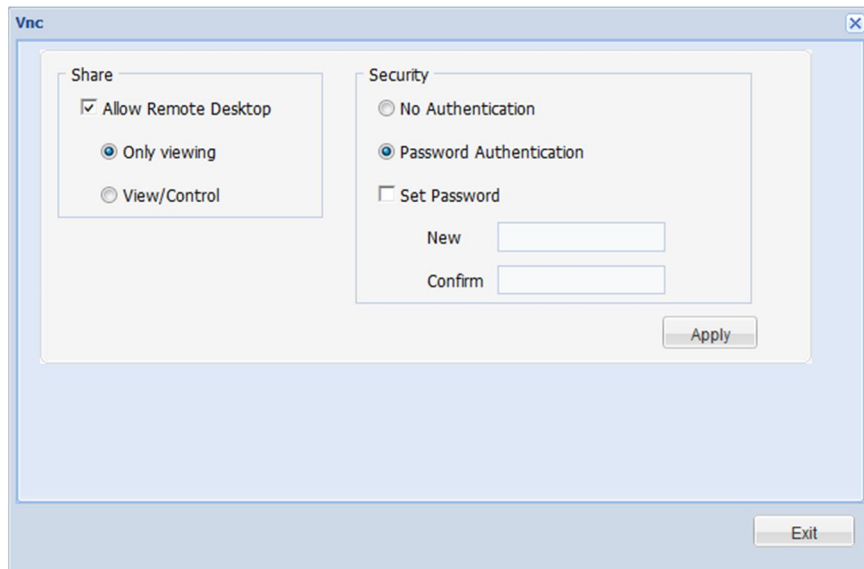
Time

"Time" window allows you to set time zone, time server and synchronization interval for the client.
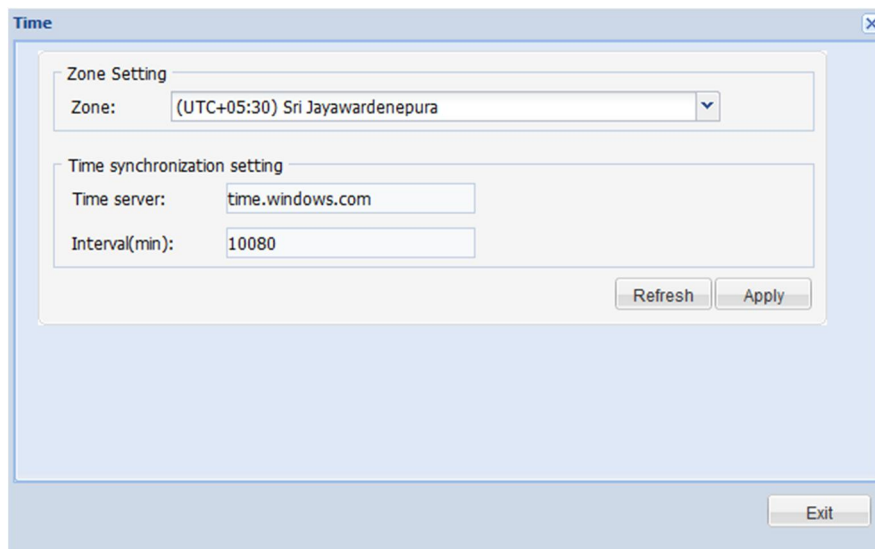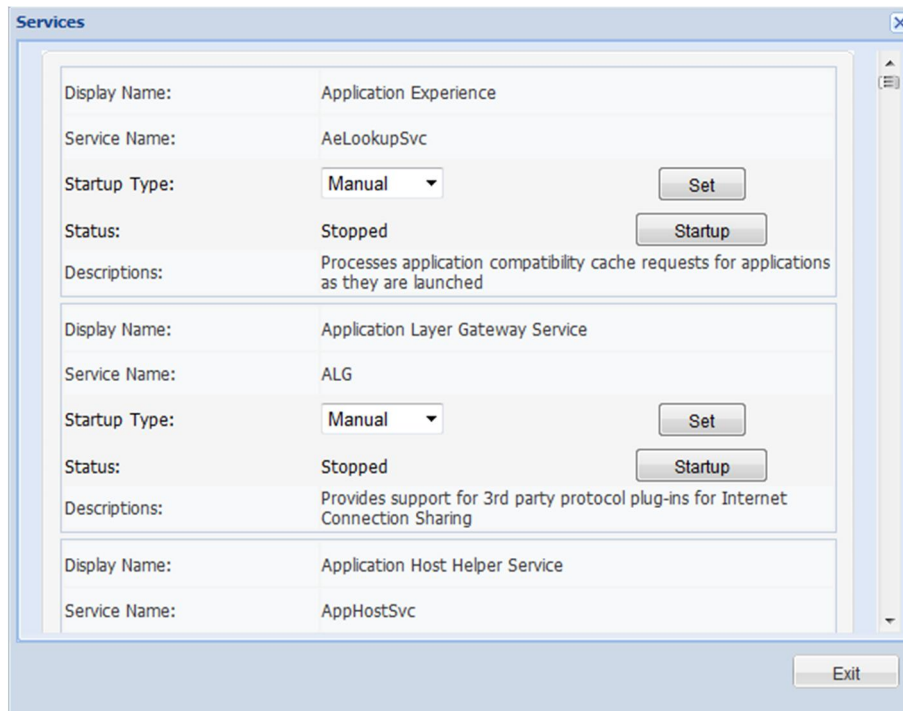

Services

"Services" window shows the status of all services running on the client.

Fields include "Service Name", "Startup Type" and "Status". You can click the corresponding **"Stop"** or **"Set"** button to control the service.
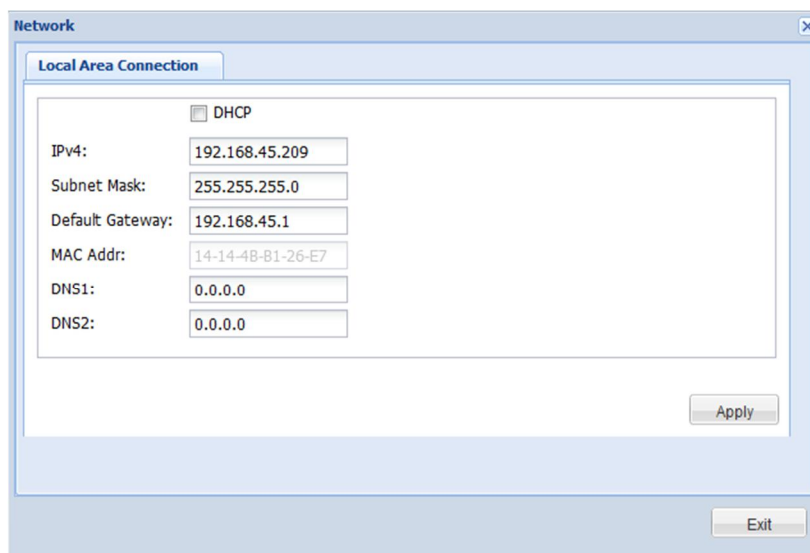
Network

"**Network**" window will display all configurations of the network adapter on the client, including "**IPv4**" address, "**Subnet Mask**", "**Default Gateway**" and "**DNS**".

If the network adapter is set to DHCP mode, those parameters will become unconfigurable (They are configured by the DHCP server on the same network as the client). Only by unchecking the DHCP checkbox can the user manually configure network parameters.

After completing the configuration, click "**Apply**" button and the configurations will take effect upon reboot.
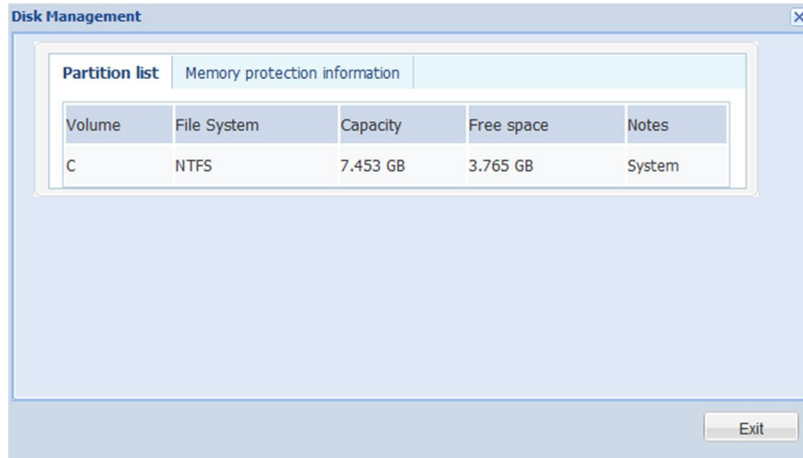

Note:

After network configuration, the client will be disconnected from network temporarily and the success message will only return after a while (a few seconds or dozens of seconds).
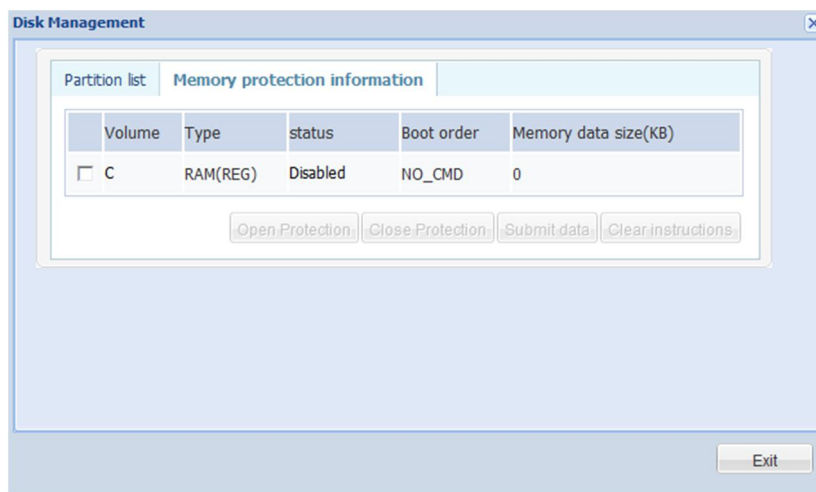
Disk Management

For client system with memory protection and hard disk protection, you can check **"Partition list"** and **"Memory protection information"**.

"Partition list" shows the disk information of selected client, as shown below:

"Memory protection information" shows the memory protection status of the client and allows the control thereof. However, the memory protection configuration will only take effect upon reboot of the client.


Note:

More memory protection operation detailed reference 22 RAM Protection Management

Basic information

Basic information can be divided into general information, version information and basic hardware information.

On the **"General"** panel, only **"Terminal name"** can be edited. Click **"Apply"** after editing and the configuration will take effect upon the reboot of client.
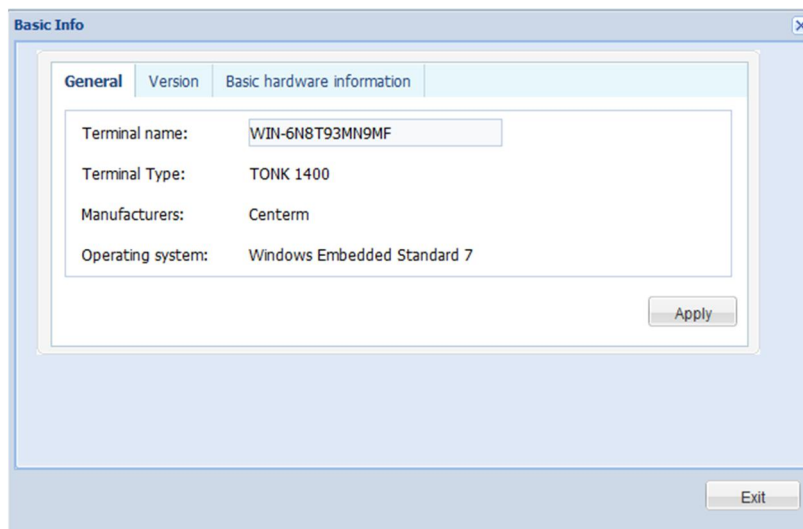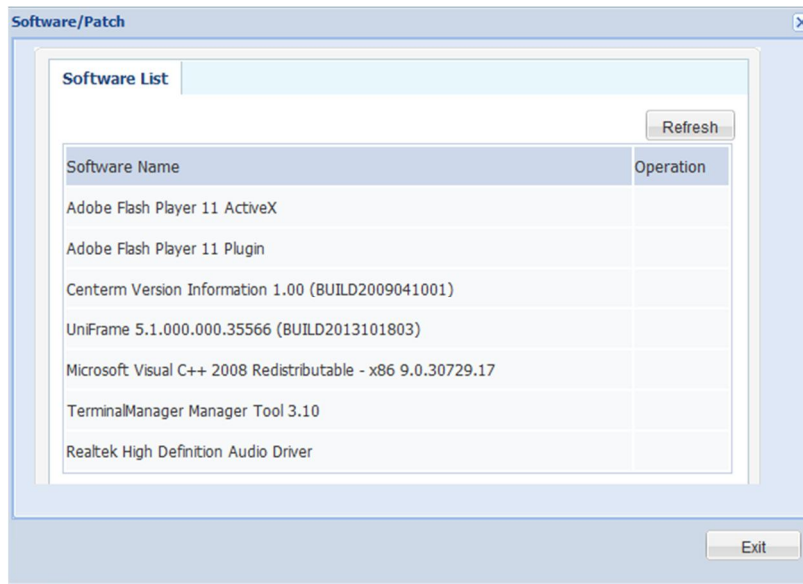
The version information only applies to XPE terminals manufactured by Centerm. Other terminals do not have such information.
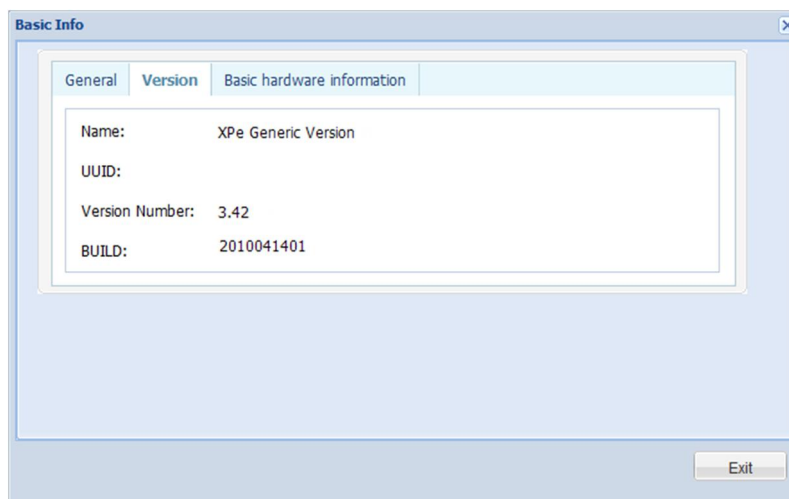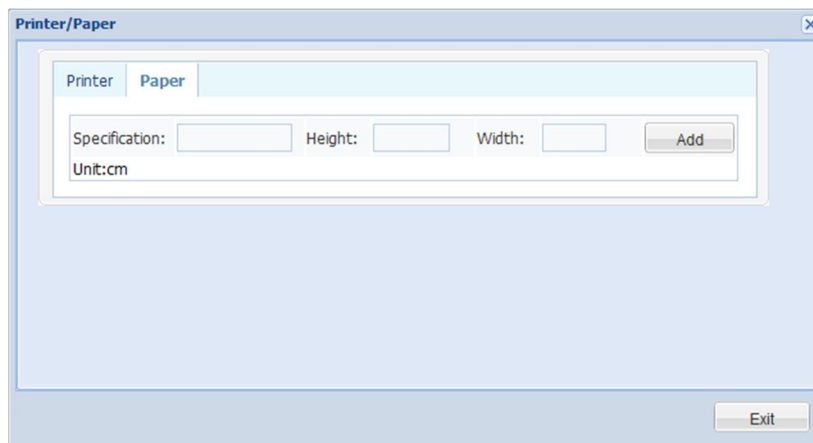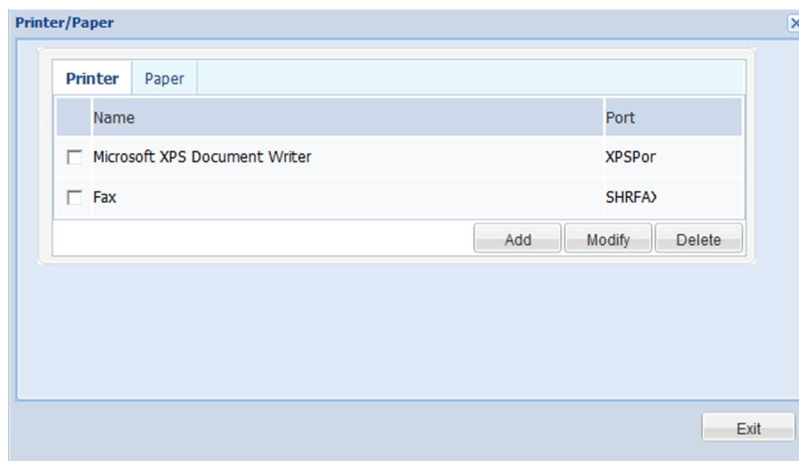

Software/Patch

This panel shows the software programs and patches installed on the client.

Printer/Paper

Before entering the printer configuration interface, the system will load the detailed information about all printers connected to the client. Meanwhile, the printer management interface allows user to **"Add"**, **"Modify"** and **"Delete"** printer(s).

Display

"**Display**" window contains: "**Screen resolution**", "**Color quality**", "**Screen refresh rate**", and "**Screen Saver**".

After modifying these parameters, click "**Apply**" button to take effect.
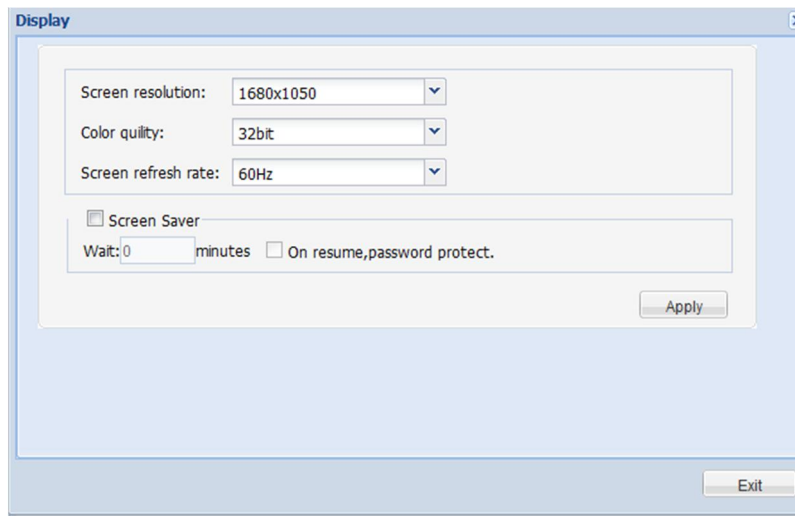

User Groups/Users

This module allows user to modify the user group/user information of the client and configure relevant policies for the specified user.

### Group

The group management interface shows the user groups on the client. Select any group to add, modify or delete.

While adding group or modifying group name, the group name to be saved cannot be the same as any existing group name, or else the system will prompt an error.
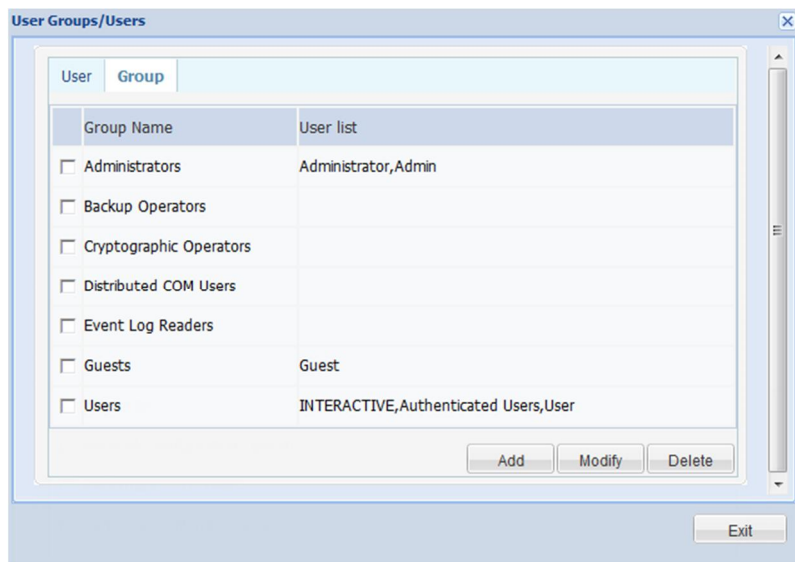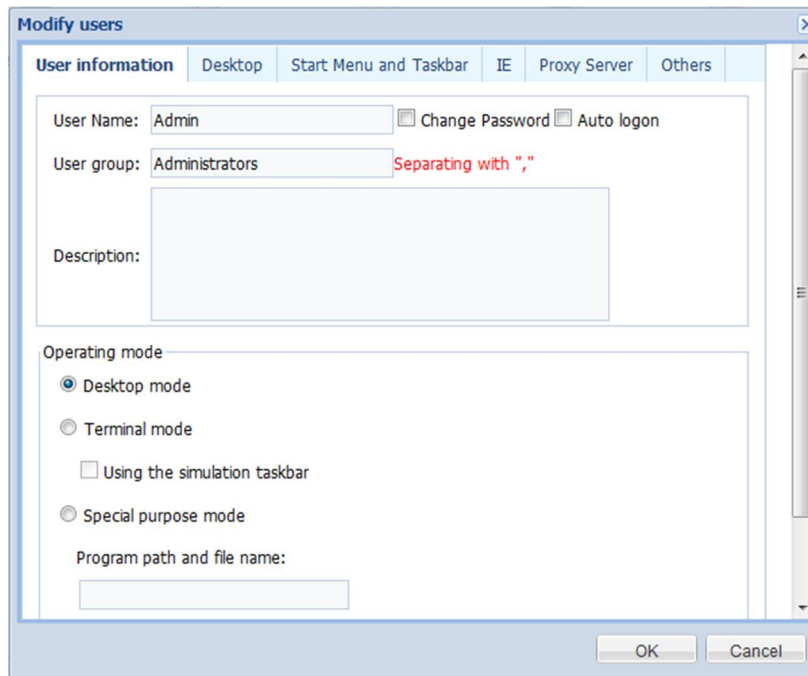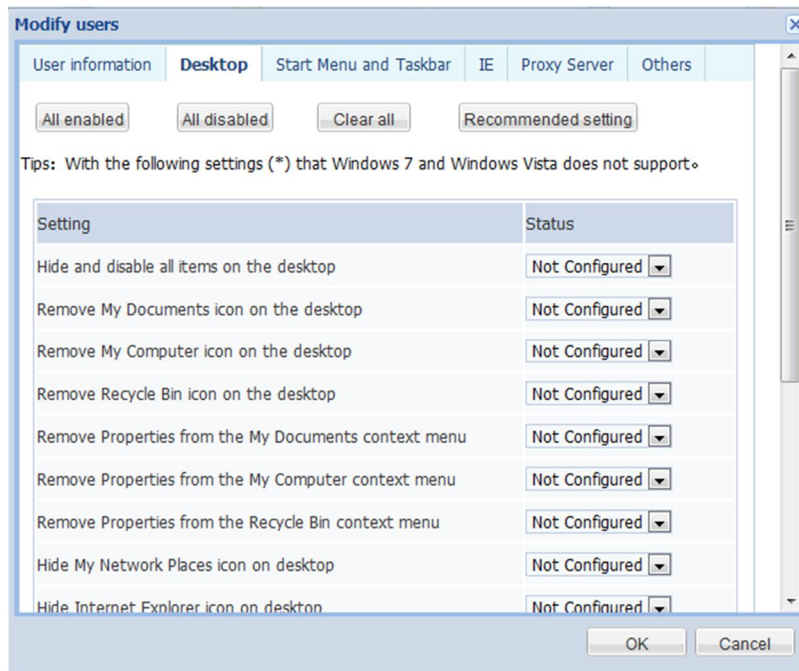

User

While adding or modifying the user, you can also configure the corresponding system policies for the user.
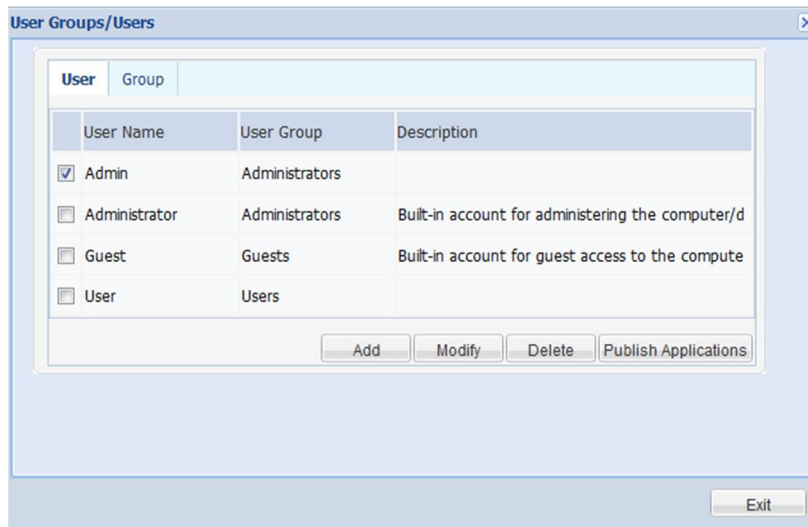
For example: Check **"Admin"** and click **"Modify"** button, the following interface will pop up:

Besides general parameters of the user, you can also configure the **"Desktop"** policy, **"IE"** policy and **"Others"** policy for the selected user.

As shown below, on the **"Others"** configuration interface, map a folder as a system drive. Since there is no need to hide or shield such a disk from the user, the mapped disk won't be shown in the list as a system drive.
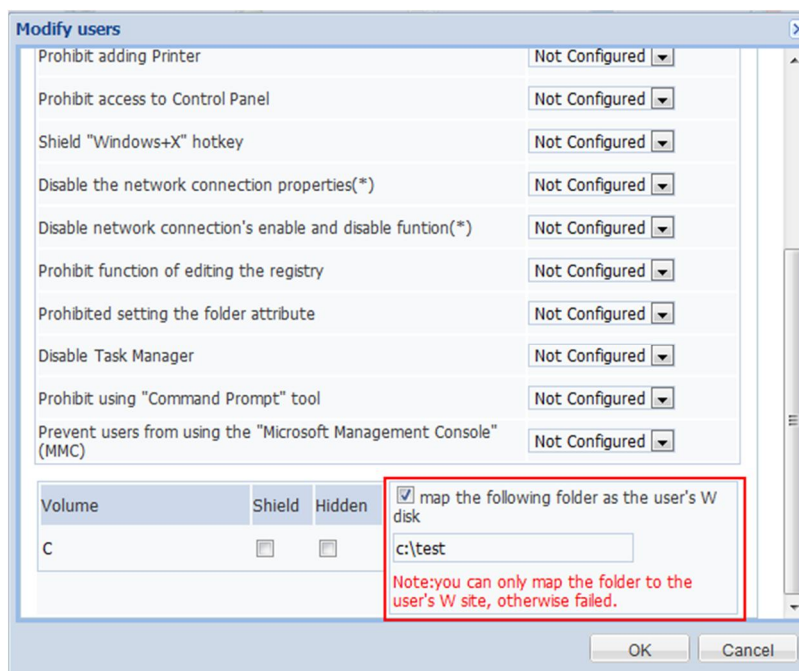
Meanwhile, you can also add commonly used shortcuts to the desktop of the specified user. Select the user from the user list and click **"Publish Applications"**.
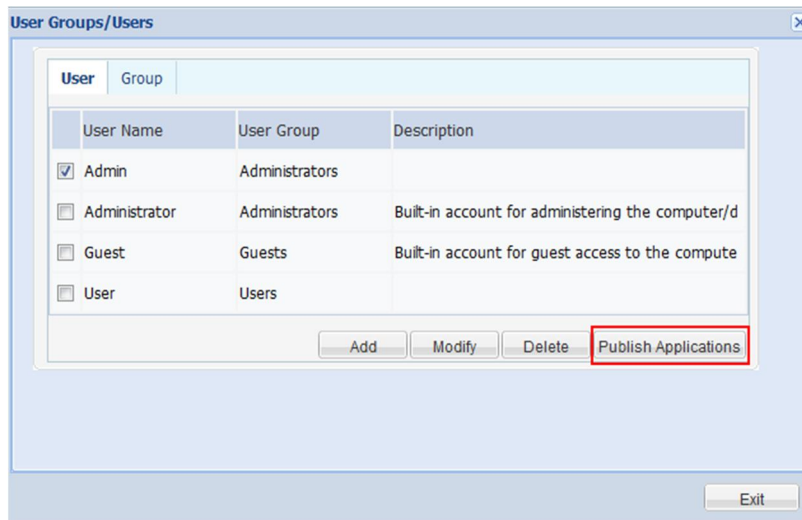
As shown below, select the link type in the pop-up dialog box.
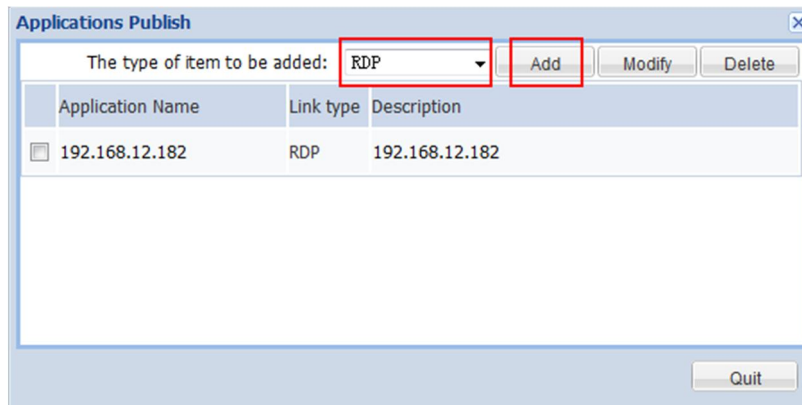
For example, to add a RDP connection, type the connection name, directory of the icon displayed and Login Settings. As for the icon, you only need to enter the path of icon on the client, or else the default icon will be used.
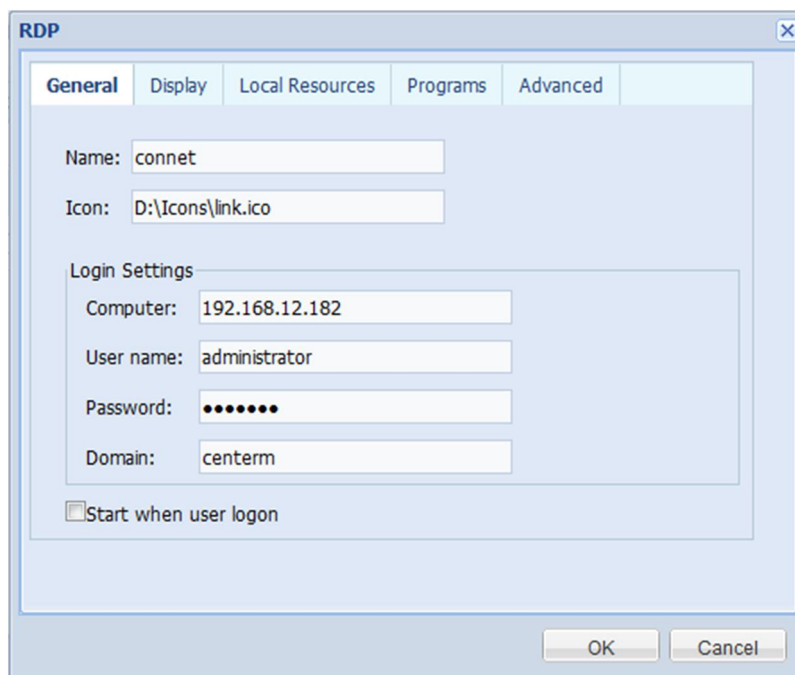
After clicking **"OK"**, the shortcut of connection will be displayed on the desktop of corresponding user (desktop contents have been hidden on the special desktop for Huawei), as shown below:
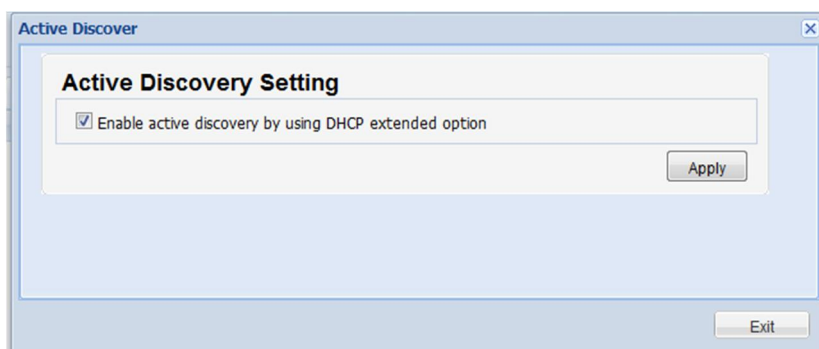

Active Discovery

By default, Active Discovery is enabled on the client. You can select to enable or disable active discovery and click **"Apply"** to take effect.

Cloud Server

The Cloud Server List on the remote management client.
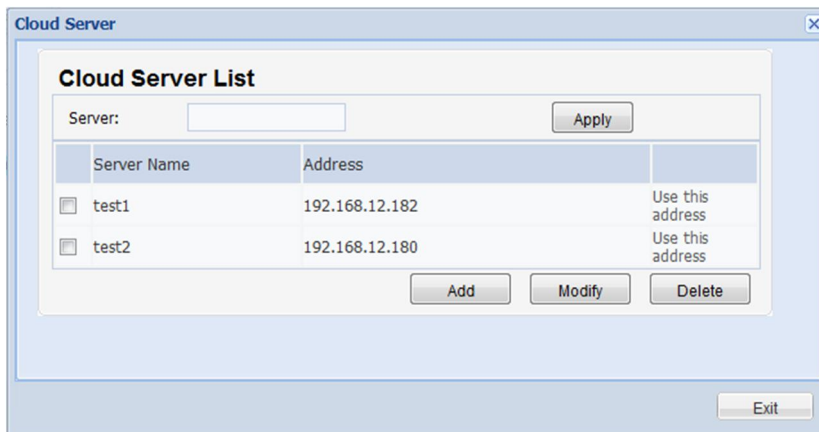
Edit Cloud Server List

Click the corresponding button to add, modify or delete cloud server entries.

Set address

Select the address to be set and click **"Use this address"** on the right side, and then click **"Apply"** button.

5.1.2 Configuration of Linux client parameters

Click **"General > Agent Config"** to enter the client configuration interface. In the **"Client Group"** pane, click the Linux client to open the configuration interface.

Note:

As the terminal version, this shows the functions and contents of screen will be slightly different.

Basic Info

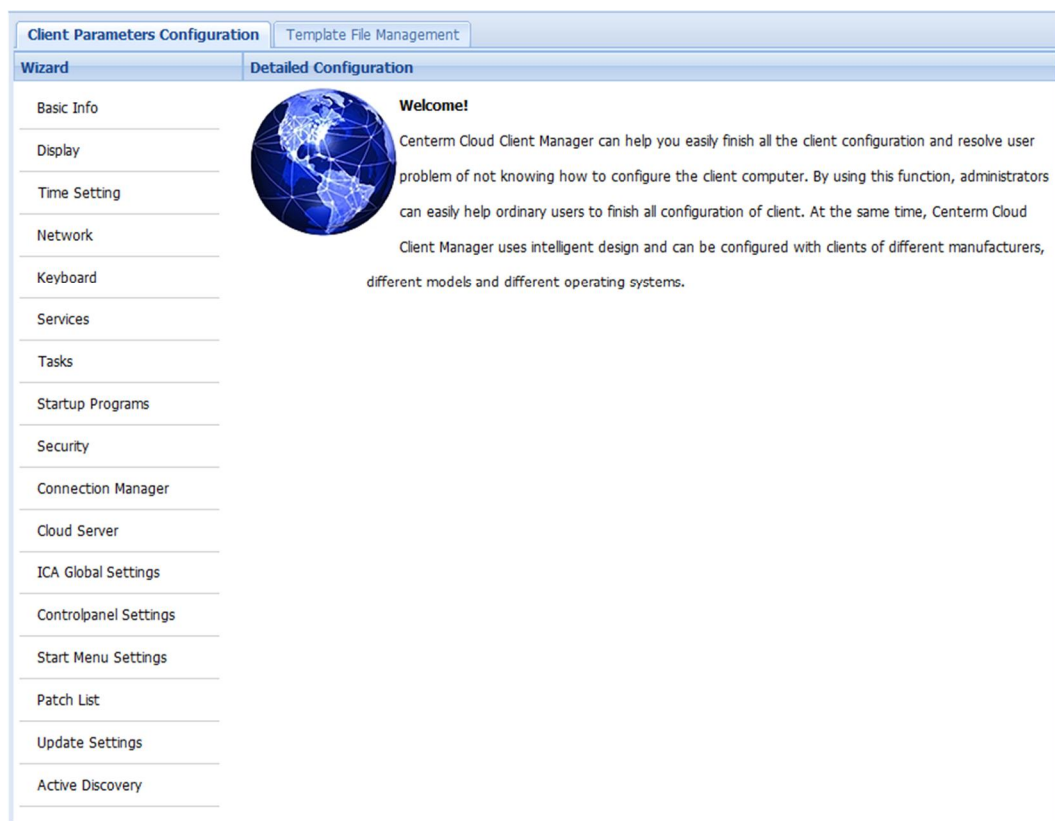Basic Information includes: Terminal Name, Terminal Type, Manufacturer, Operating System, Version, BIOS version number, BUILD No., Storage Capacity, IPv4 address and MAC address.

Only **"Terminal Name"** can be edited. Click **"Apply"** after editing and the configuration will take effect upon the reboot of client.

Display

Including such basic information as Resolution, Color, Language, Refresh Rate, etc.

User can configure these settings according to actual needs. Select the corresponding value from the drop-down list and then click the bottom-right **"Apply"** button to complete configuration.

The configuration will take effect upon the reboot of client.

If the user needs to apply Screen Saver, the user must check **"Screen Saver"** first before configuring the remaining settings.

The user can configure when the client will enter screen save mode, and whether or not to apply password protection. If password protection is enabled, the user must enter the correct password in order to quit screen saver mode and access desktop.

Click **"Apply"** to complete configuration, which will take effect upon the reboot of client.

Time Setting

The user may modify the settings according to actual needs. After modification, click **"Apply"** button to take effect.

- Time Zone: select the appropriate time zone from the drop-down list.
- You can select whether or not to enable time synchronization. After enabling time synchronization, you can configure the IP address of time server.

Network

On this panel, the user can see detailed configuration information about the Linux client, including: IP address of network adapter, routing, DNS, etc.

Network configuration

"Network" provides two ways for configuring the client, namely:

- Manually enter the IP address. The user shall know the IP address, subnet mask and default gateway, which are all required.

- Using DHCP service. To use DHCP, the user must check "**DHCP**" and the system will then assign an IP address to the client.

After modification, click **"Apply"** to complete the configuration of **"Network"**.

Note:

- You must uncheck "**DHCP**" first in order to manually enter the IP configuration information.

- The format of "**IPv4**" and "**Default Gateway**" is DDD:DDD:DDD:DDD. The first DDD shall fall within the range of 1-223, the last DDD shall fall within the range of 1-254, and the other two DDDs shall fall within 0-255.

- The format of "**Subnet Mask**" is DDD:DDD:DDD:DDD, which shall all fall within the range of 0-255. After the Subnet Mask is converted to binary, make sure the first DDD are all "1" and the last DDD are all "0" (i.e., 255.255.0.0).

Routing configuration

Click the **"Routing"** tab on the panel, where the user can view the current routing configuration information and add, delete or edit route.

During the configuration, please pay attention to the format of **"Target"** and **"Gateway"**. At the same time, the user also needs to configure the subnet mask and other options of the network adapter.

- Add route: If the user needs to add a route, click "**Add**" button to add a routing table and then edit the routing table.

- Delete route: If the user needs to delete a route, select the route(s) to be deleted and then click "**Delete**" button.

- Edit route: If the user needs to edit the routing table, edit directly in the routing table.

After editing, click the bottom-right **"Apply"** button to complete the configuration of routing table.

DNS configuration

In DNS configuration, the user can manually enter the IP address of DNS sever or select **"Obtain DNS server address automatically"**.
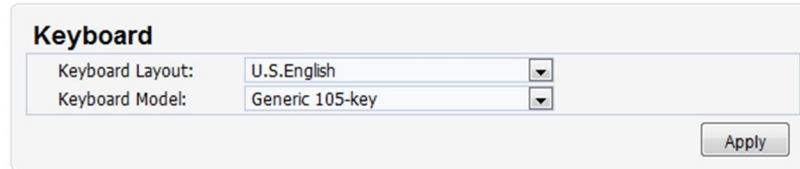
Caution:

Changing network configuration will cause the client to reinitialize network connection.

- During manual input, pay attention to the format of DNS server address.

- The user cannot type IP address in the edit box if "**Obtain DNS server address automatically**" has been selected.

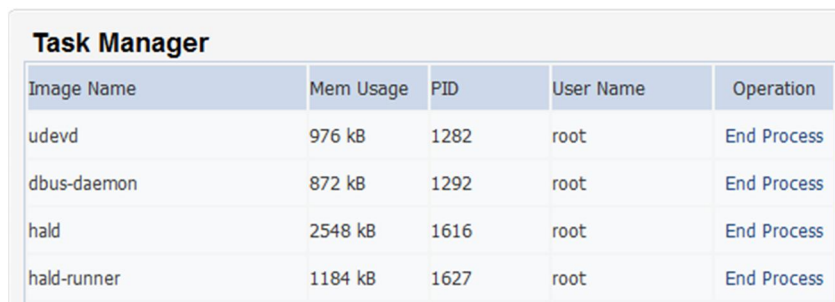After editing, click the bottom-right **"Apply"** button to complete the configuration of DNS.

Keyboard

"Keyboard" allows you to configure keyboard settings for the client, including Keyboard Layout and Keyboard Model.

Keyboard	
Keyboard Layout:	U.S.English
Keyboard Model:	Generic 105-key
	Apply

Task Manager

"Task Manager" allows the user to end certain tasks on the client by clicking **"End Process"** behind the corresponding task. At the same time, the user can also view the performance of client beneath the panel, including: CPU Usage, Mem Usage, Physical Memory, etc.

Task Manager				
Image Name	Mem Usage	PID	User Name	Operation
udevd	976 kB	1282	root	End Process
dbus-daemon	872 kB	1292	root	End Process
hald	2548 kB	1616	root	End Process
hald-runner	1184 kB	1627	root	End Process

Startup Management

In **"Startup Management"**, the user can configure whether or not to enable **"Connection Manager"** and **"Keypad"** at system startup.

To enable the above two features at startup, the user only needs to check the corresponding items and click **"Apply"** button to complete the configuration of **"Startup Management"**.

Startup Management	
Cloud Server	☑ Enable when system startup
Cloud Client	☑ Enable when system startup
Connection Manager	☐ Enable when system startup
	Apply

Security

In the **"Security"** dialog box, the user can configure the password needed to allow modifying system settings.

Check the item(s) to be configured and then enter the desired password in the edit box, and then click **"Apply"** button to complete the configuration.

Connector manager

In **"Connection Manager"**, the user can add such connection types as RDP, ICA, TELNET, XDMCP, etc, and is capable of configuring the varied attributes for the added connections and deleting connections.

Add connection

Click **"Connection Manager"**. Select the connection type to be added from the drop-down list on the **"Connection Manager"** panel and click **"Add"** to open the connection configuration interface.

The user can then configure the connection to be added according to the contents on the configuration interface.

Note:

The client can add up to 10 connections.

Edit connection

Click **"Connection Manager"**. Check the connection to be edited on the **"Connection Manager"** panel and click **"Edit"** to open the connection editing interface.

Caution:

Only one connection can be edited at a time.

Delete connection

Click **"Connection Manager"**. Check the connection(s) to be deleted on the **"Connection Manager"** panel and click **"Delete"** to delete the selected connection(s). You can delete multiple connections at a time.

In **"Connection Settings"**, the user can select the connection type:

● RDP connection manager
● ICA connection manager

- XDMCP connection manager

Cloud Server

In this module, the user can add the cloud server for the client as needed.

Edit Cloud Server List

Click the corresponding button to add, modify or delete cloud server entries.

Set address

Select the address to be set and click **"Use this address"** on the right side, and then click **"Apply"** button.

ICA Global Settings

Configure ICA global parameters.

Control Panel Settings

This module allows the user to configure those configurable items on the control panel of Linux client.

Start Menu

This module allows the user to hide Start Menu items. Check the checkbox on the right side of the item to be hidden and click **"Apply"** button.

Patch List

If upgrade patches have been installed on the selected client, you will see detailed information on this page.

Update Settings
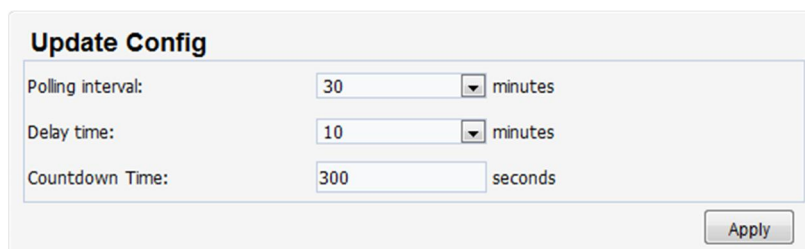
"Update Settings" allows you to configure the time to update clients, including:

- Polling interval: During client upgrade, if the client is shut down abnormally, it will query whether there is an upgrade command after the first polling interval.
- Delay time: the next time when the upgrade dialog box will pop up again after it is closed.
- Countdown time: the countdown time after which the upgrade dialog box will be closed automatically when it pops up.

Update Config

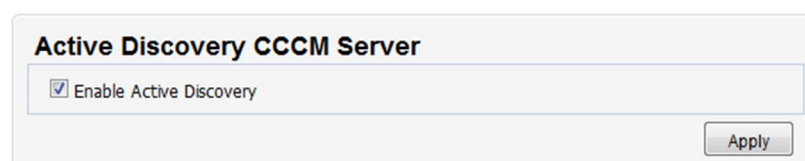|		
Polling interval:	30	minutes
Delay time:	10	minutes
Countdown Time:	300	seconds

Apply

Active Discovery

By default, Active Discovery is enabled on the client. You can select to enable or disable active discovery and click **"Apply"** to take effect.
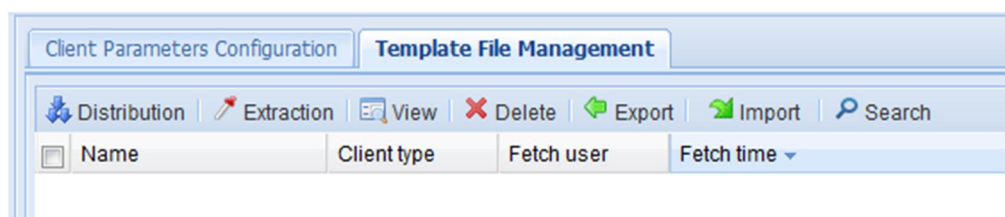
Active Discovery CCCM Server

☑ Enable Active Discovery

Apply

5.2 Template File Management

Template file allows you to extract the settings of a specific client and save on the server as a file. You can distribute the template file to multiple clients to synchronize the settings.

Client Parameters Configuration	**Template File Management**

🐜 Distribution	🖊 Extraction	🖹 View	✖ Delete	◀ Export	📤 Import	🔍 Search

☐ Name	Client type	Fetch user	Fetch time ▾

5.2.1 Extraction

To extract a template from client, perform the following steps:

Caution:

- The client to be operated must be online, or else the acquisition will fail.
- The template name must not contain *, |, /, :, ?, <, >, or ".
- The user can select items of the template file according to his/her needs.

1. Select one online client and configure necessary parameters (please refer to "**5.1Client Parameters Configuration**".
2. Click "**General > Agent Config > Template File Management**".
3. Select the client which was selected in Step 1 and click "**Extraction**" on the "**Template File Management**" panel.
4. Enter template file information, select the items to be extracted and click "**Save**".

The extracted template file will appear in the list.

5.2.2 Distribution

To distribute template file to one or multiple clients, perform the following steps:

1. Click "**General > Agent Config > Template File Management**".
2. Select the template file to be distributed. You can only select one file at a time.
3. In the "**Client Group**" pane, select the client or client group.
4. Click "**Distribution**" button.
5. Select the appropriate OS version on the "**Plan Wizard**" interface, configure the task plan and then click "**Finish**".

   Note:

   - The user may select one or more clients, or select the group.
   - The type of clients to which the template will be applied must be the same as the client type selected by the user.
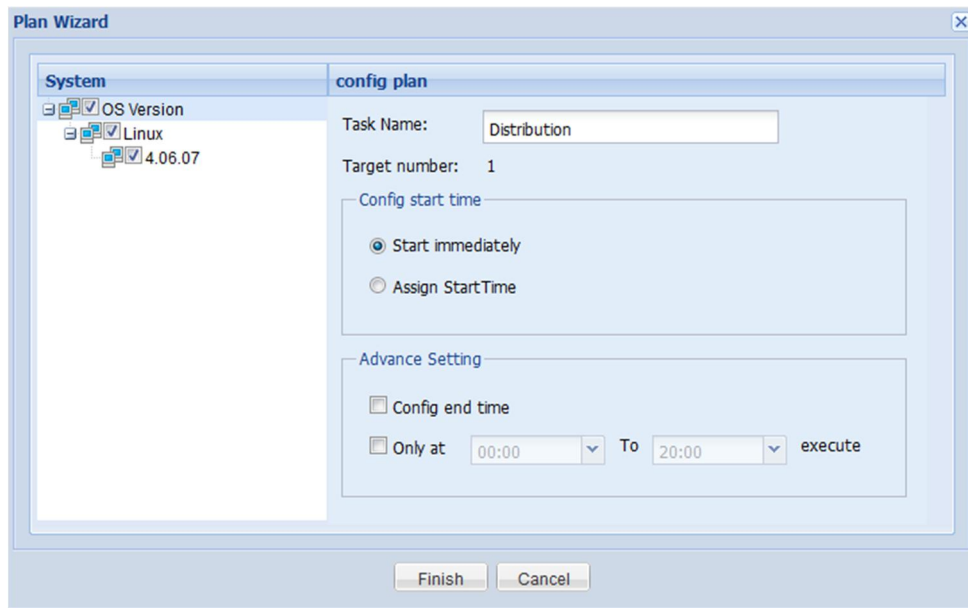
5.2.3 View

1. Click "**General > Agent Config > Template File Management**" to enter "**Template File Management**" interface.
2. Select the template file to be viewed and click "**View**".
3. Click the displayed configuration items to view detailed configuration information in the template.

5.2.4 Delete

1. Click "**General > Agent Config > Template File Management**" to enter "**Template File Management**" interface.
2. Select the template file to be deleted and click "**Delete**".
3. In the conformation dialog box, click "Yes" to delete the template file.

5.2.5 Export

1. Click "**General > Agent Config > Template File Management" to enter "Template File Management**" interface.
2. Select the template file to be exported and click "**Export**".
3. Save the template file according to browser's Save Wizard.

5.2.6 Import

1. Click "**General > Agent Config > Template File Management" to enter "Template File Management**" interface.
2. Click "**Import**".
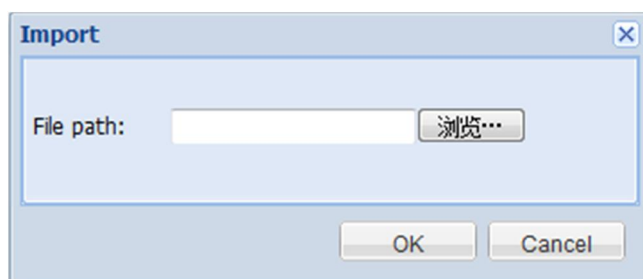
3. Click "**Select File**" to select the template file to be imported.
4. Click "**OK**" to import.

5.3 Firewall Settings

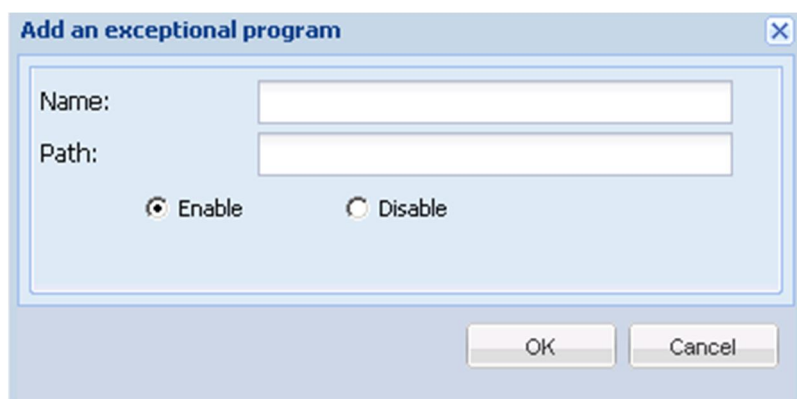Firewall Settings modular only support windows terminal.

5.3.1 Firewall settings

1. Click "**General** > **Agent Config** > **Firewall Settings**" to enter " **Firewall Settings** " interface。

2. Select" **Enable the firewall (recommended)**" means open firewall ;" **Disable the firewall(not recommended)**"means close firewall ;

3. Chose one or more terminal.

4. click " **Apply**" to enable or disable firewall.
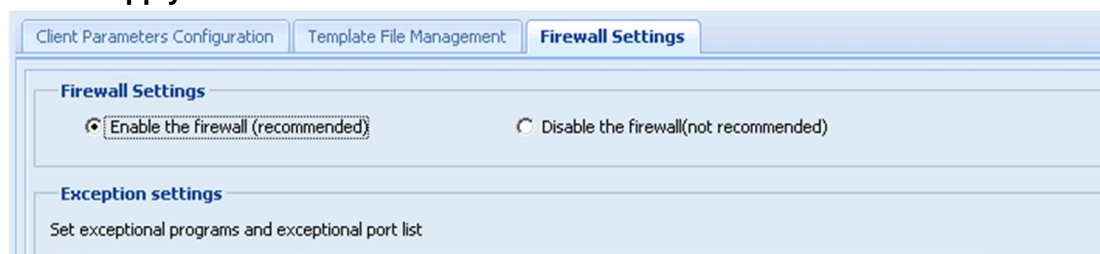
5.3.2 Exception settings

5.3.2.1 Add Program

1. Click "**General** > **Agent Config** > **Firewall Settings**" to enter " **Firewall Settings** " interface。

2. At Exception settings part , select" **Add Program** " ;

3. Fill in **Name** and **Path** information ;" **Enable**" means run exceptional program ; "**Disable**" means don't allow exceptional program ;

4. Click" **OK**" to confirm add ; click" **Cancle**" to cancle ;

5. Select exceptional program which have added , chose one or more terminals ;
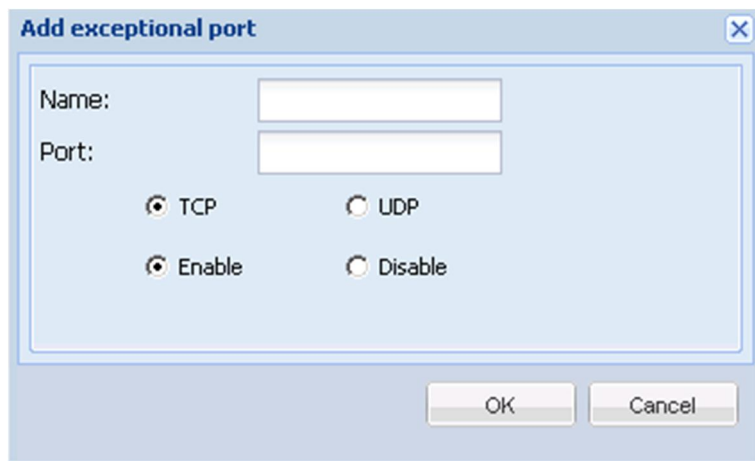
6. Click" **Apply**" to apply.

5.3.2.2 Add Port

1. Click "**General** > **Agent Config** > **Firewall Settings**" to enter " **Firewall Settings** " interface。

2. At Exception settings part，chose" **Add Port** "；

3. Fill in **Name** and **Port** information；select "**TCP"** or "**UDP";**" **Enable**" means open exceptional port；"**Disable**" means close port；

4. Click" **OK**" to confirm add exceptional port；Click" **Cancel**" to cancel；

5. Select exceptional ports which have added，chose one or more terminals；

6. Click" **Apply**" to apply.

5.3.2.3 Edit

1. Select Exception Program or Exception Port which had added，Click" **Edit**"；

2. Edit relate information；

3. Click" **OK**" to confirm edit；Click" **Cancel**" to cancel edit.

5.3.2.4 Delete

1. Select Exception Program or Exception Port which had added，Click" **Delete**"；

2. Then click" **Yes**" to confirm delete.

6 Remote Assistance

Remote assistance allows remote monitoring and control of clients. You can only monitor one client at a time. The remote desktop of the client will be displayed in 256-color mode, thus ensuring smooth operation under low bandwidth. This may result in color distortion, but the mouse and keyboard operations won't be affected.

Remote Assistance

To use remote assistance, perform the following steps:

1. On the navigation bar, click "**General > Remote Monitor**" to enter the operation interface.
2. Select the target client in the "**Client Group**" pane and click "**Monitor**".

   If Java Runtime Environment (JRE) is not installed or if the JRE version is too low, the browser may give you the following prompt. Please refer to "**27.1Install JRE**".
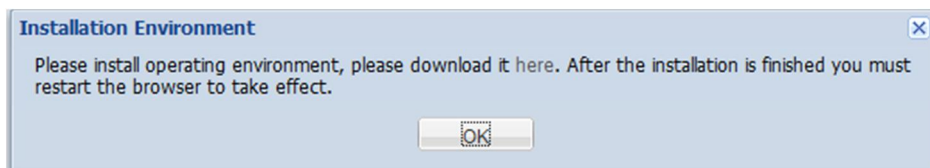
3. A confirmation dialog box may pop up on the client side (depending on the specific settings of client). Click "**Accept**".
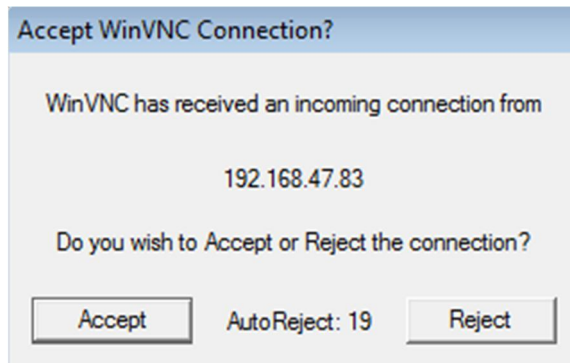
4. After the client user has accepted the connection, you will see the remote desktop on the browser page.
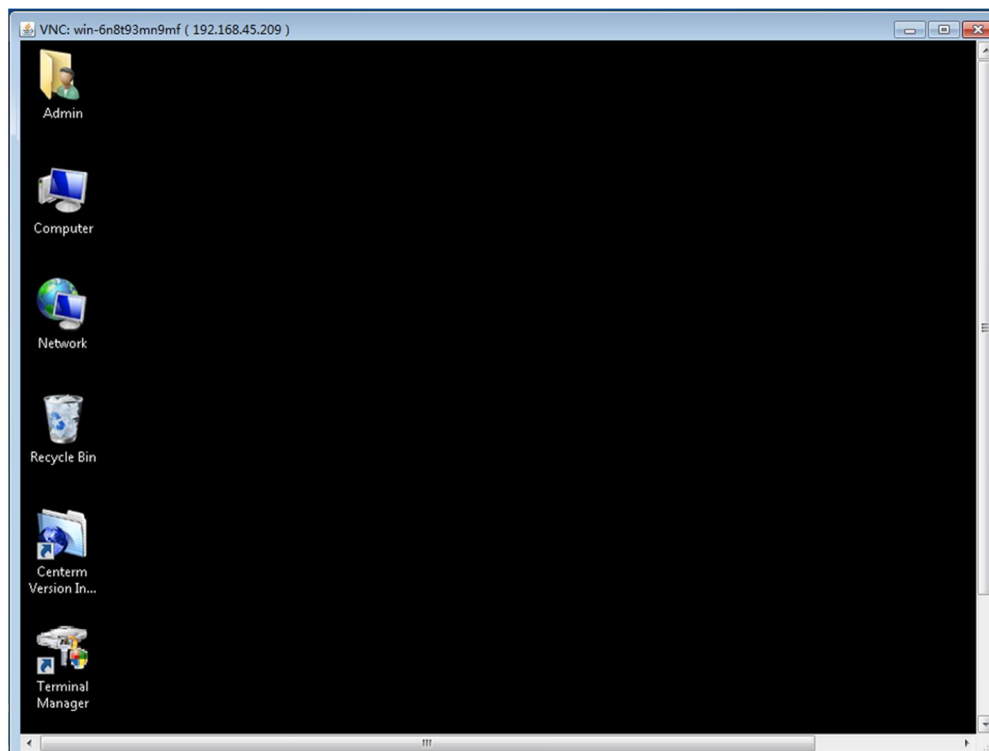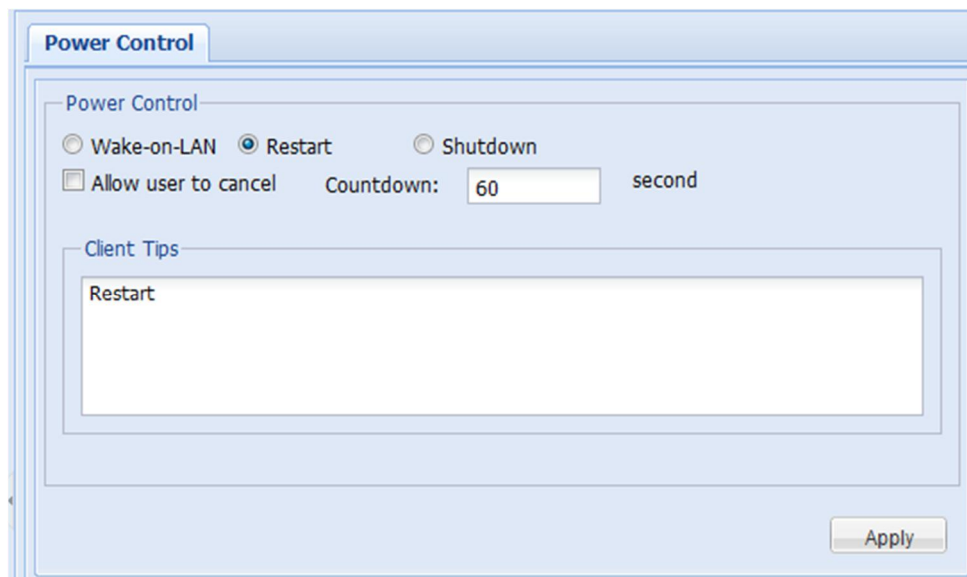
7 Power Control

Power Control allows you to shut down, restart or wake up the remote client. The operations supported by the client depend on its hardware platform and operation system. Shutdown and Restart are only applicable to online clients.

Remote wake-up is subject to the following constraint conditions:
- WOL is supported by the hardware (network adapter) and BIOS of the client.
- The server and the client to woken up must be on the same network segment and in the same VLAN.
- The network devices (such as switch) can transmit WOL command.
- The client cannot be woken up if it is not shut down normally.
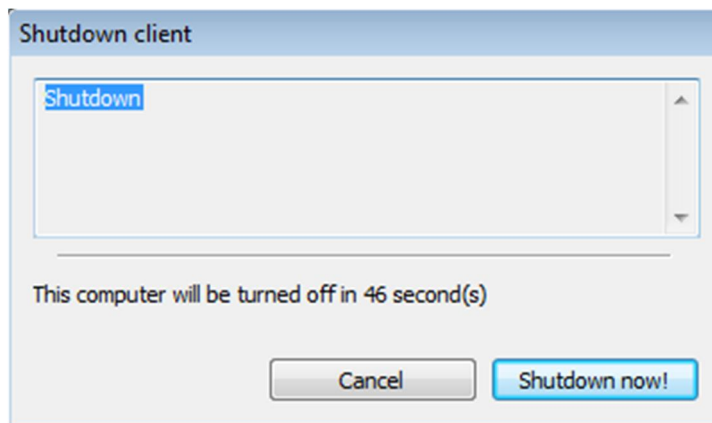
Control options

Allow user to cancel

After **"Allow user to cancel"** is checked, a cancel button will appear in the dialog box on the client side, so that the client user can cancel this power control operation.

Countdown

Enter the countdown time (default: 30 seconds) after which power control operations can be executed on the client.

Client Tips

The message entered in the input box of "Client Tips" will appear in dialog box on the client side.

Operation Steps

To apply power control on the remote client, perform the following steps:

1. On the navigation bar, click "**General > Power Control**".

2. In the "**Client Group**" pane, select at least one client or client group.

3. On the **"Power Control"** panel, select the type of power control (Shutdown, Restart, Wake-on-LAN).

4. Set control options and click "**Apply**".

   Note:

   Do not set any control option if Wake-on-LAN is selected.

5. Select the appropriate OS version of client on the "**Plan Wizard**" interface, configure the task plan and then click "**Finish**".

8 Performance Monitoring

Performance Monitoring is used to showcase the dynamic performance of client. By monitoring these performance items, you can analyze the operating status of the client. Performance Monitoring can also provide statistical reports which enable you to learn about the overall performance of the client. Memory monitoring and disk monitoring are not supported by Linux clients.

8.1 Real Time Performance

Real Time Performance is used to view the current operating status of a single client, including processes, CPU, memory, disk, network connections and network adapter.

To view the real-time performance of a specific client, perform the following steps:

1. On the navigation bar, click "**General > Perf Monitor**" to enter the performance monitoring

interface.

2. Click the desired client in the "**Client Group**" pane.

3. View the performance data of the client.

8.2   Performance Statistics

Performance monitoring allows scheduled collection of client's performance information for generating the statistical reports.

To take performance statistics on the client, perform the following steps:

Operation Steps

Create monitoring log

1. On the navigation bar, click "**General > Perf Monitor > Performance statics**" to enter the operation interface.
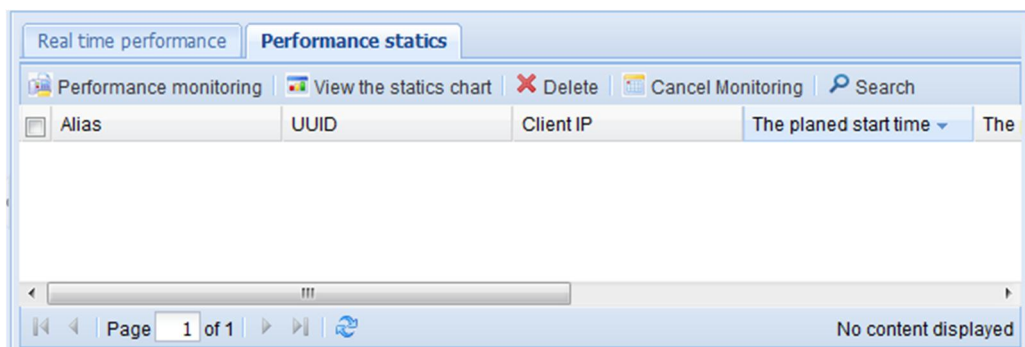
2. In the "**Client Group**" pane, select at least one client or client group and click "**Performance monitoring**" button.

3. Set the "**start monitoring time**", "**Frequency (Second)**" and "**Finish monitoring time**" and then click "**OK**".
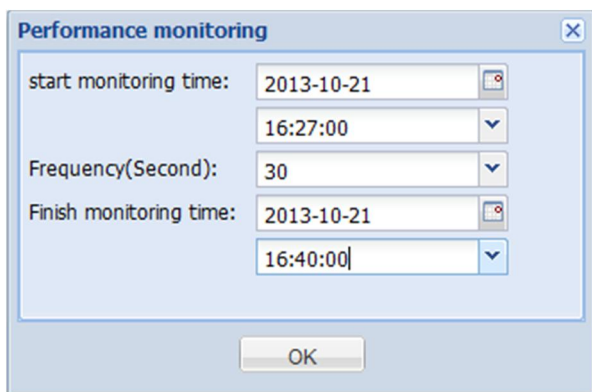
4. Select the appropriate OS version of client on the "**Plan Wizard**" interface, configure the task plan and then click "**Finish**".

5. View the monitoring task created.

View statistic data

6. Wait for a while or upon completion of monitoring, select one monitoring log and click "**View the statics chart**".

7. You can view the statistical graphs of CPU, memory and network.
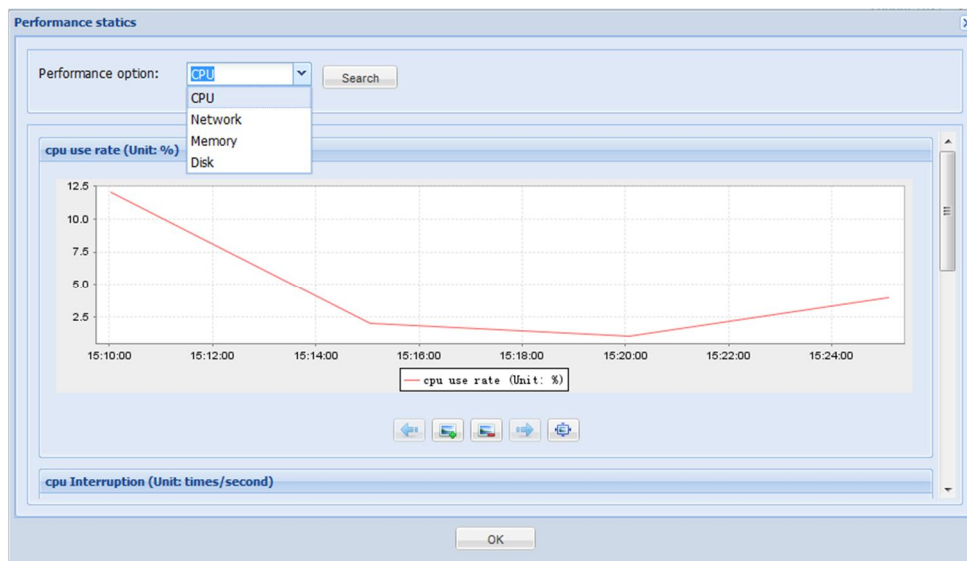
Stop and delete monitoring log

Select at least one monitoring log and click "**Cancel Monitoring**" to stop monitoring and keep the monitoring log, or click "**Delete**" to stop monitoring and delete the monitoring log.

9 Alarm Manager

You can enable performance alarm on the client the set the appropriate alarm thresholds. When an alarm threshold is reached, the client will send alarm log to the server, and such logs will be saved in the database. Meanwhile, you can also configure global effective time of alarms, alarm level, periodical email notification, etc.

By default, Performance Alarm is disabled, and the global parameters settings apply to all clients. You can configure different alarm thresholds for different clients.

To enable Performance Alarm, perform the following steps:

Configure global alarm parameters

Configure the effective time, alarm level and email notification for alarms. If not needed, please jump to Step 6.

1. On the navigation bar, click "**General > Alarm Manager > Alarm global parameters**" to enter the configuration interface.
2. Select the effective time of alarms.

   Note:

   Effective time is calculated from the last alarm. If no alarm policy is matched within the specified effective time, the alarm will be cleared.

   ---
   setting of time for the alarm to come into effect

   Effective time: Validate forev ▾

   Tips:The clients in alarm status display alarm status icon during the alarm time, allow the administrator to manually relieve the client alarm status.

   ---

3. Select the alarm level.

   Note:

   There are three alarm levels: information, Warning and Error (by order of severity).

   Alarm level setting

   Performance Alarm: Warning ▾

   ---

4. Enable mail inform.

   (Optional) When there is any alarm message, the server will send an email to the administrator.

   Caution:

   In "**Common > Global Setting > Global Parameters Setting**", the email server and email account shall be corrected configured, or else the server cannot send any email.

5. Click "**Apply**" to save and apply the settings.

Configure alarm thresholds

You can configure alarm thresholds for different clients or groups, including memory usage, network traffic, CPU usage and disk partition.

6. On the navigation bar, click "**General > Alarm Manager > Alarm Policy**" or click "**Alarm Policy**" tab directly to enter the configuration interface.

7. Check "**Enable Alarm**" to configure the times and thresholds, and then click "**Apply**".

8. Select the appropriate OS version of client on the "**Plan Wizard**" interface, configure the task plan and then click "**Finish**".

View alarm log

The alarm log will only be generated after a while. You can view alarm logs irregularly.

9. On the navigation bar, click "**General > Alarm Manager > Alarm Log**" or click "**Alarm log**" tab directly to enter the log interface.

You can delete alarm logs or clear the alarm(s) of the client.
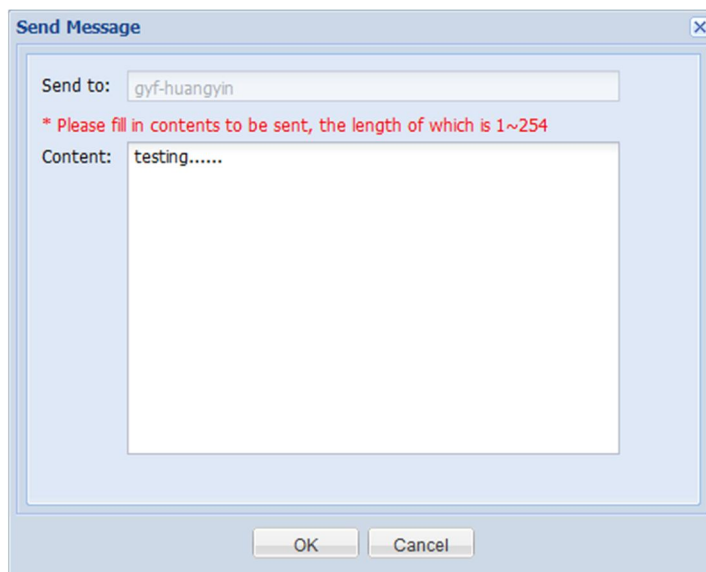
10 Message Manager

Message Manager offers a real-time messaging tool for the administrator and the client user, allowing convenient communication between system administrator and client user.

10.1 Send Message

1. On the navigation bar, click "**General > Msg Manager**" to enter the message management interface or right-click a client/group in the left pane and select "**Send Message**" from the context menu
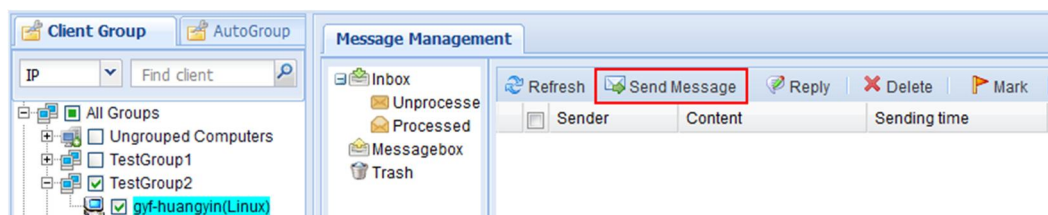
2. In the "**Client Group**" pane, select the client or group to send message(s).
3. Click "**Send Message**" button.
4. In the pop-up dialog box, edit the message to be sent and click "**OK**" button.

5. Select the client(s) on the "**Plan Wizard**" interface, configure the task plan or keep default settings and then click "**Finish**".
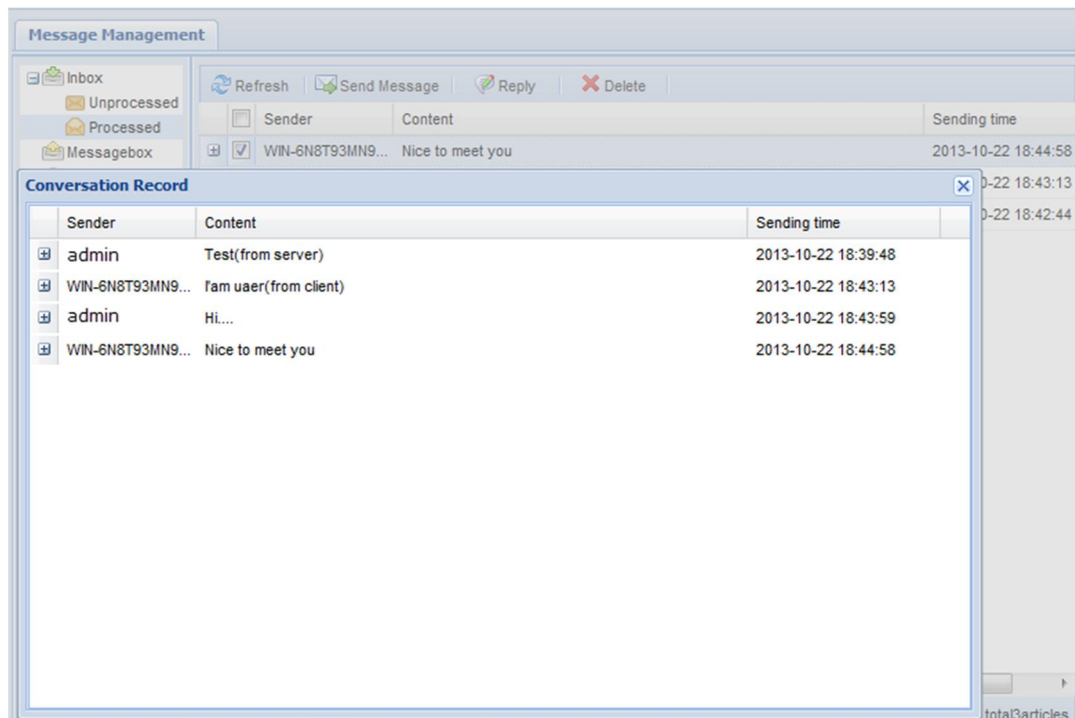
10.2 Inbox Management

In the **"Inbox"**, the user can refresh, view, reply and delete **"Processed"** and **"Unprocessed"** messages.

On the navigation bar, click **"General > Msg Manager"** to enter the message management interface.

View conversation record

Double-click a message to view the record of conversations with a client user.

Mark

"Mark" is used to change the state of unprocessed messages to the state of **"processed"**.

In the **"Unprocessed"** inbox, the user can select the messages to be marked and click **"Mark"**, and then click **"OK"** button to move these messages to the **"Processed"** inbox.

10.3 Messagebox Management

In the **"Messagebox"**, the user can refresh, send, resend and delete messages. In addition, the user can also view the latest reply from the client user in the **"Message Status"** pane.

On the navigation bar, click **"General > Msg Manager"** or right-click a client/group in the left pane and select **"Send Message"** from the context menu to enter the message management interface.

Resend

Select the message to be resent from the Messagebox and click **"Resend"** button to resend the message to the former one or more receivers.

Message Status

In the **"Message Status"** pane, the user will see the last reply received by each message from the corresponding client user. In the meantime, the user can also double click the content of last reply to view the record of conversations with this client user.

11 Device Security Management

Only windows terminal supports device security management

11.1 Limiting device type

" **Limiting device type**" used to limit part equipment of thin client，for example：" **Not configued** "、" **Read-write** "、" **Read**"、" **Allow**"" **Forbid** "；In the state of not configuration, access equipment is determined by the interface, part of the equipment need to restart.
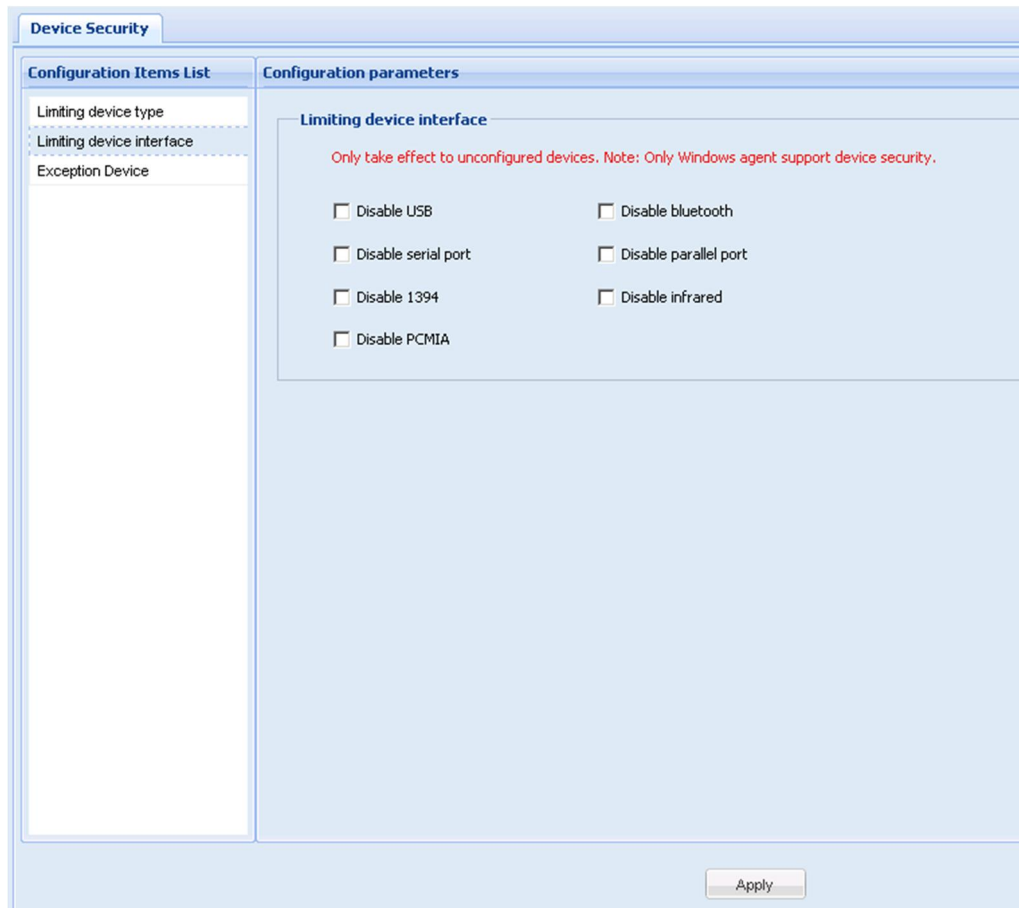
1. Click in turn at navigation-bar" **Divice Security**" >" **Limiting divice type**" go into Limiting divice type interface；

2. Limit configuration different types of equipment on the right side interface；

3. Chose the terminal，then click" **Apply**" to application.

11.2 Limiting device interface

1. Click in turn at navigation-bar " **Divice Security**" >" **Limiting device interface**" to go into Limiting divice interface；

2. Decide whether limiting device interface on the right side interface

3. Select terminal，click" **Apply**" then finish configuration.

11.3 Exception Device

1. Click in turn at navigation-bar" **Divice Security**" >" **Exception Device**" go into Exception Device interface;

2. Operation exception device on the right side interface " **Add** "、" **Change**" and" **Delete** " ；

   " **Add**" button is use to add exception device ,Click "**OK**" to confirm add，Click " **Cancel**" to cancel

"**Change**" button is used to edit exception device which have added；Click "**OK**" to confirm edit，click "**Cancel**" to cancel；

"**Delete**" button is used to delete exception device which have added，Click "**OK**" to confirm delete，click "**Cancel**" to cancel.

3. Select the terminal, then click "**Apply**" to finish configuration.

12 File Deployment Management

File Deployment is mainly used to deploy the system files, including file copying and software distribution. It is applicable to the batch-mode installation of application software on clients and the batch-mode distribution of files to clients. In the mean time, through file deployment, we can manage system files, including file uploading and deleting.

12.1 Linux File Deployment

On the navigation bar, click **"Deployment > File Deploy"** to enter the **"Linux File Deployment"** interface.

		File name	File Size	File Type	Version	For System Version
☐	1	AOSLinux_Agent_5.1.11X.000.zip	24M	Agent File	5.1.111.000.23877	1.11.06, 1.11.05, 1.10.
☐	2	uhisi_1M_130311.dat	1.1M	Patch File		1.10.*, 1.15.*, 1.11.*, 1
☐	3	uARM_xterm_depend_all_1305...	29.7K	Patch File		
☐	4	uhisi_5m_130311.dat	5.7M	Patch File		1.10.*, 1.15.*, 1.11.*, 1
☐	5	uCT2000test-125MB_1.10.8888...	123.7M	System File	1.10.8888	
☐	6	AOSLinuxSafe_1.11.06_201309...	164.7M	System File	1.11.06	

Upload file

Note:

You can only upload the dedicated upgrade files provided by Centerm for Linux clients.

Upgrade files for Linux clients can be divided into three types:

- System files: for upgrading the operating system of Linux clients.
- Patch files: upgrade patches or applications for Linux clients.
- Agent files: for upgrading the management agent installed on Linux clients.

1. On the navigation bar, click "**Deployment > File Deploy**" to enter the "**Linux File Deployment**" interface.
2. Click "**Upload**" button. According to the wizard to complete the upload. Please refer to 23.4Upload the Upgrade File.
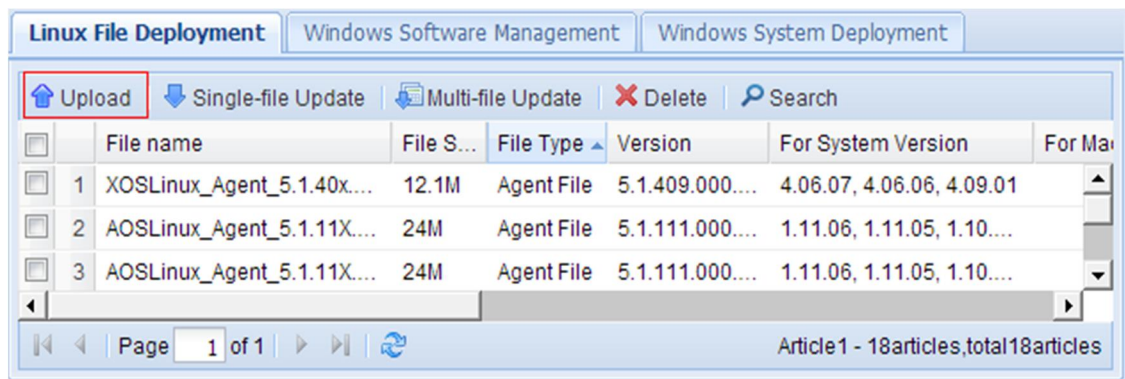
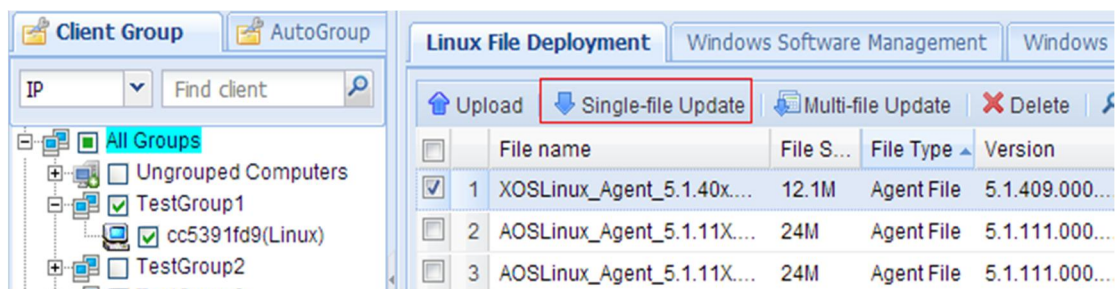Upon successful upload, exit the upload window, and the uploaded file will appear in the file list.

Single-file Update

1. On the navigation bar, click "**Deployment > File Deploy**" to enter the "**Linux File Deployment**" interface.

2. Select the client or client group to be upgraded, select the update file and click "**Single-file Update**" (update file must have been uploaded).

3. Set update conditions and click "**Apply**".
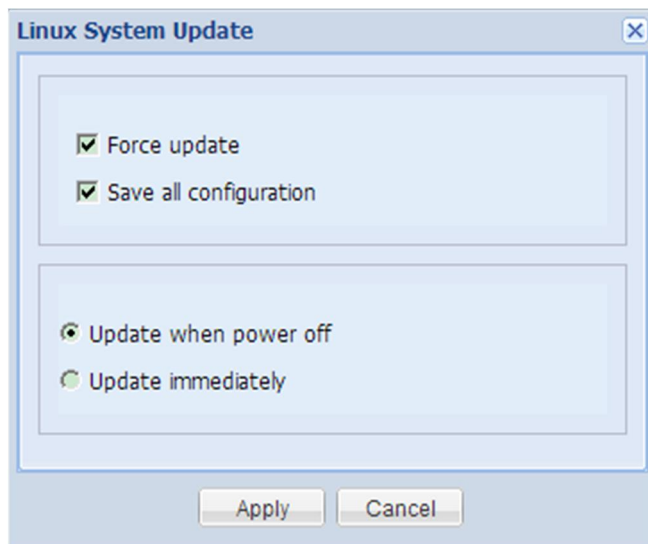
By default, "Force update" and "Save all configuration" have been enabled (applicable to operating system upgrade).

● Update when power off: to start update when the client is shut down normally and then shut down the client upon completion.

● Update immediately: to prompt the client user to update immediately after the client has downloaded the update file, yet client user can choose to postpone the update.

4. Select the OS version on the "**Plan Wizard**" interface, configure the task plan or keep default settings and then click "**Finish**".

5. On the navigation bar, click "**Task Manager**" to enter the task management interface to view update status and result.

Multi-file Update

1. On the navigation bar, click "**Deployment > File Deploy**" to enter the "**Linux File Deployment**" interface.

2. Select the client or client group to be upgraded, select one or multiple update files and click "**Multi-file Update**" (update files must have been uploaded).
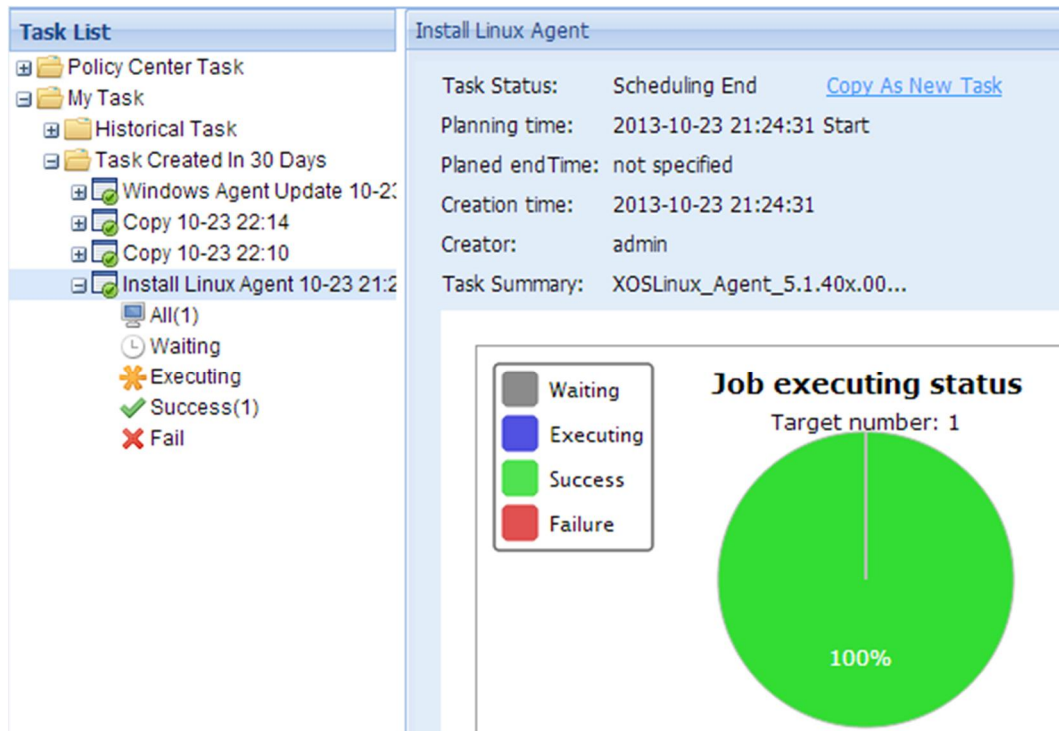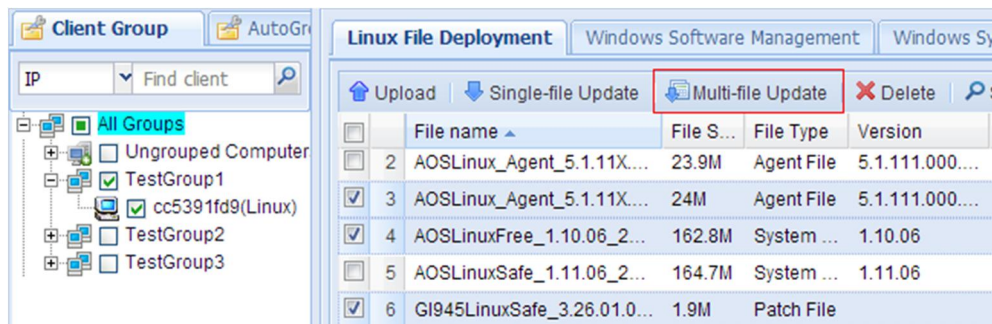

3. Set update conditions and click "**OK**".

Order of update files

You can add, delete or clear update files, or move up/down update files to change the order.
✔ indicates that the sequence of file update is correct, while ✘ indicates that the sequence is inappropriate, and you will need to change the update order or delete this file from the update list.

If the order of all update files is correct (all indicating ✔), then you can proceed to the next step.

Download method

To configure how the file will be downloaded when the local space for update is short.

● Segment will be taken: update process will be continued.

● Inform failure: terminate this update.

Upgrade Type

● Update when power off: to start update when the client is shut down normally and then shut down the client upon completion.

● Update immediately: to prompt the client user to update immediately after the client has downloaded the update file, yet client user can choose to postpone the update.

Updating system

● By default, "Force update" and "Save all configuration" have been enabled (applicable to operating system upgrade).

4. Select the OS version on the "**Plan Wizard**" interface, configure the task plan or keep default settings and then click "**Finish**".

5. On the navigation bar, click "**Task Manager**" to enter the task management interface to view update status and result.
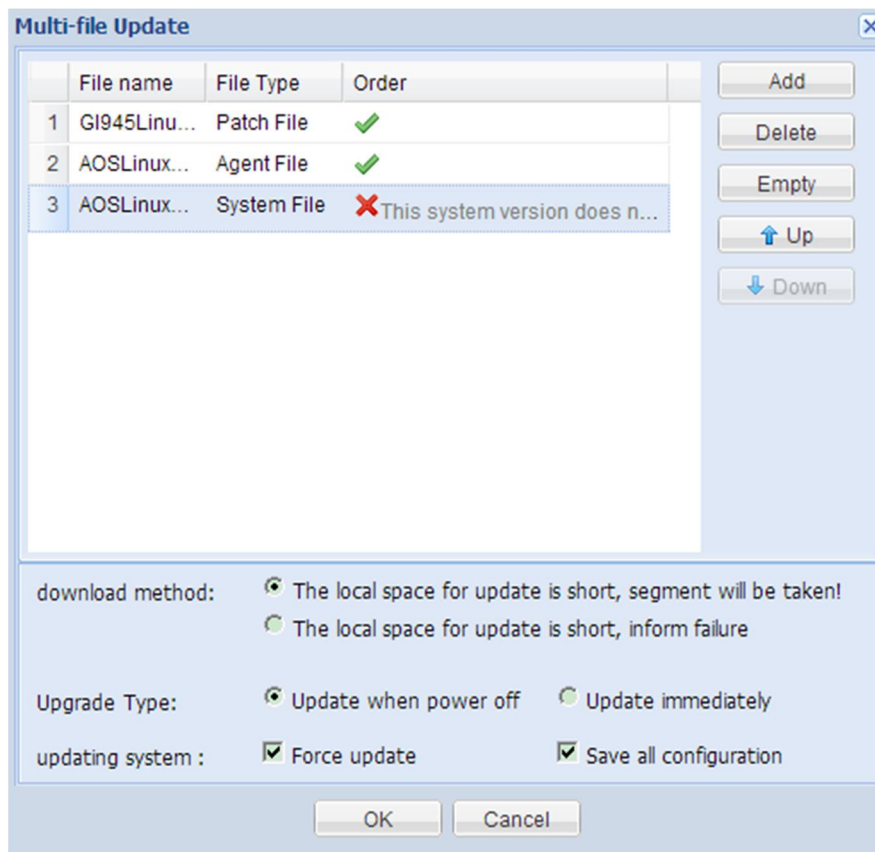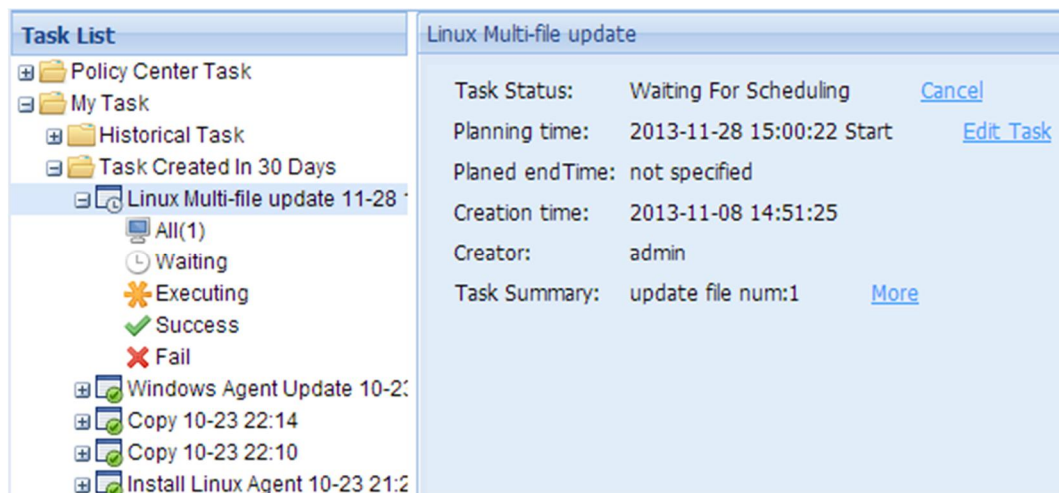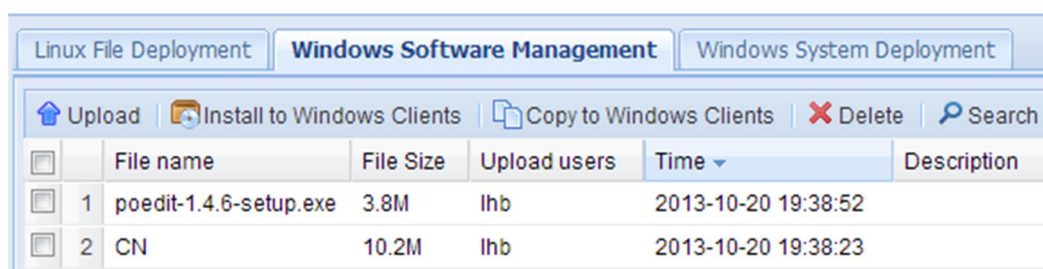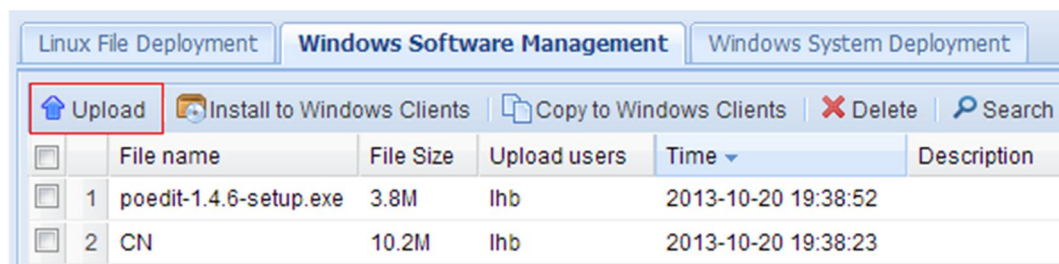
12.2 Windows Software Management

On the navigation bar, click "**Deployment > File Deploy > Windows Software Management**" to enter the "**Windows Software Management**" interface.

Upload file

1. On the navigation bar, click "**Deployment > File Deploy > Windows Software Management**" to enter the "**Windows Software Management**" interface.

2. Click **"Upload"** button. According to the wizard to complete the upload. Please refer to 23.4Upload the Upgrade File.


Upon successful upload, exit the upload window, and the uploaded file will appear in the file list.
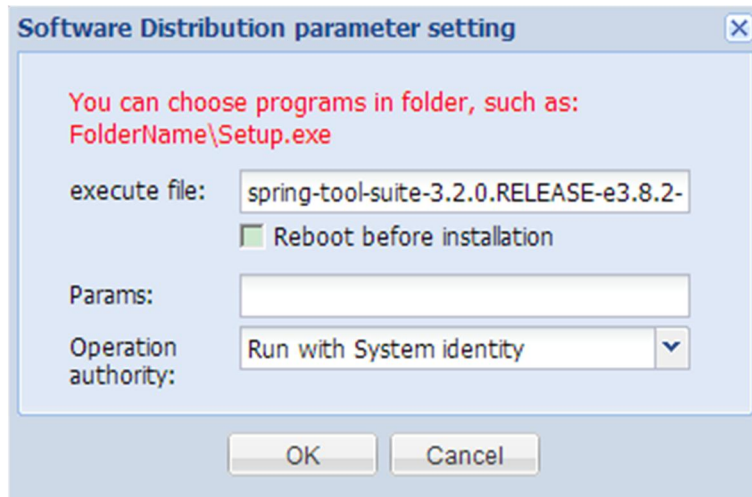
Install software

You can distribute the software stored on the server to clients and execute installation thereof.

1. On the navigation bar, click "**Deployment > File Deploy > Windows Software Management**" to enter the "**Windows Software Management**" interface.

2. Select the client or client group for software installation, select the software to be installed and then click **"Install to Windows Clients"**.
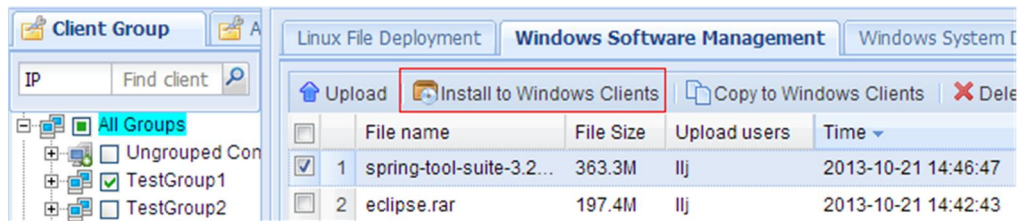
3. Edit the corresponding parameters and click **"OK"**.

Reboot before installation

Check "**Reboot before installation**" and the client will reboot first before installing the software.

Note to "Params":

1. This is an optional parameter used when installing software onto the client. It is by default left blank to indicate non-quite installation, and manual intervention may be needed. Different software applications use different parameters. For information about such parameters, please inquire the software provider;

2. Windows software package provided by CENTERM's default installation parameters is "/ VERYSILENT"

For example, JRE involves the following parameters:

- /quiet: quiet mode, no user interaction;
- /passive: no-participation mode, only displaying the process bar;
- /q[n|b|r|f]: to configure the level of user interface -- n: no user interface; b: basic interface; r: reduced interface; f: full interface.

Operation authority

- Current user: The currently active user permissions, when the software installation will create a shortcut on the desktop, suggested that choose the privileges for installation. If the current client no user login, software installation will fail;

- The specified user authority: That allows administrators to specify the user permissions to install. If the current login user privilege no software to install, it is suggested that choose the privileges for installation;

- System identity: System user permissions, if the current user does not have permissions to install the software, the System user permissions can be used for

installation, but using the System user permissions will vary in different operating System versions, and may arise session segregation phenomenon.

4. Select the OS version on the **"Plan Wizard"** interface, configure the task plan or keep default settings and then click **"Finish"**.

5. On the navigation bar, click **"Task Manager"** to enter the task management interface to view task status and result.

Copy file

File Copying is used to copy files to the client.

1. On the navigation bar, click "**Deployment > File Deploy > Windows Software Management**" to enter the "Windows Software Management" interface.

2. Select the client or client group for file copying, select the file(s) to be copied from the file list and then click **"Copy to Windows Clients"**.
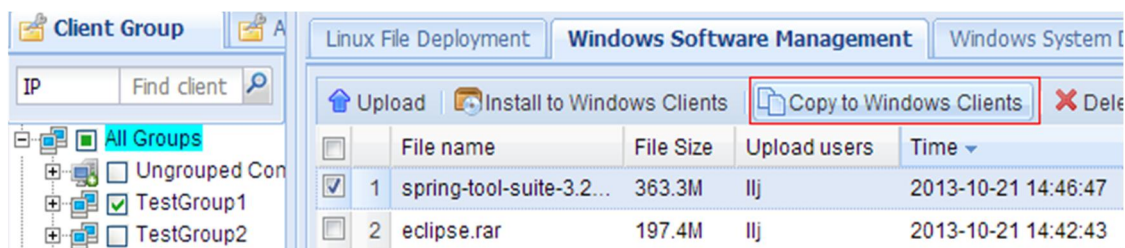

3. Enter the path of folder to which this file will be saved on the client and click **"OK"** button.
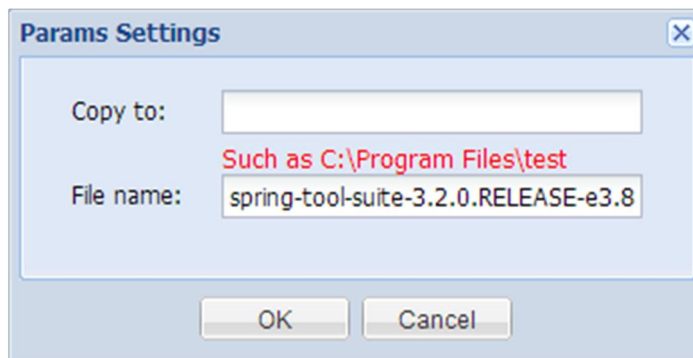
4. Select the OS version on the **"Plan Wizard"** interface, configure the task plan or keep default settings and then click **"Finish"**.

5. On the navigation bar, click **"Task Manager"** to enter the task management interface to view task status and result.
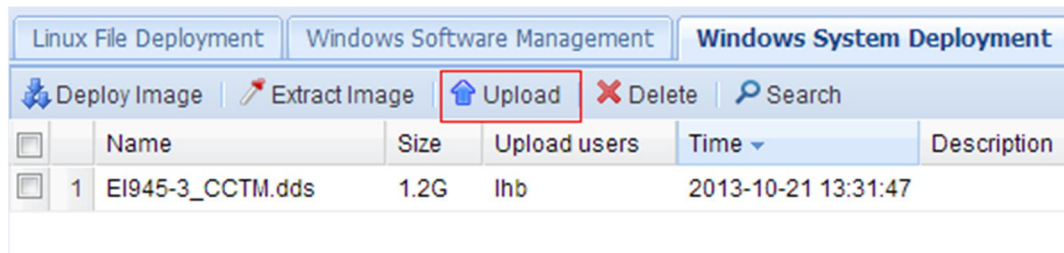
12.3 Windows System Deployment

On the navigation bar, click "**Deployment > File Deploy > Windows System Deployment**" to enter the **"Windows System Deployment"** interface.
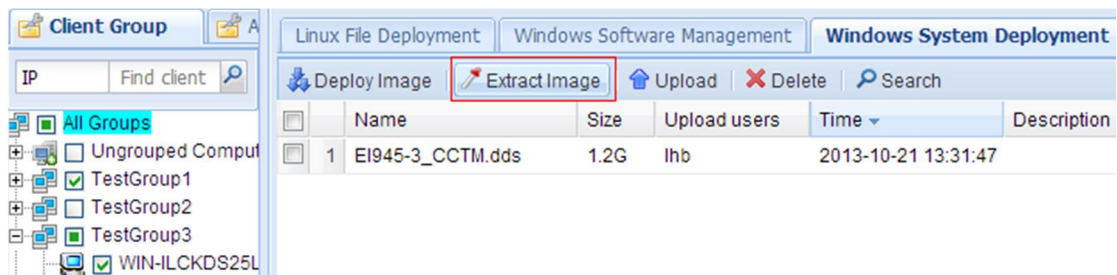
Upload image file

1. On the navigation bar, click "**Deployment > File Deploy > Windows System Deployment**".

2. Click "**Upload**" button. According to the wizard to complete the upload. Please refer to <u>23.4Upload the Upgrade File.</u>


Upon successful upload, exit the upload window, and the uploaded file will appear in the file list.

System backup

The administrator can back up the operating system of client to the server. When the client encounters system crash, we can use the backup system image to restore the client.

1. On the navigation bar, click "**Deployment > File Deploy > Windows System Deployment**".

2. Select one Windows client and click "**Extract Image**".

3. Configure backup parameters.
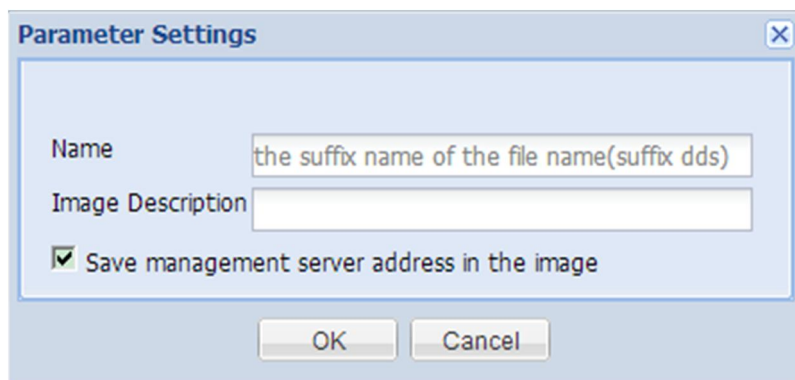
4. Select the client(s) on the "**Plan Wizard**" interface, configure the task plan or keep default settings and then click "**Finish**".

5. In the Task Manager module, view the progress of image extraction.

   Note:

   The client is offline during the process of image extraction, after which the client will need to reboot for several times. Therefore, you will observe that the client will go online and offline repeatedly.

6. View the extracted image file in the list.

System recovery

System recovery is to restore the system from the backup image stored on the server.

1. On the navigation bar, click "**Deployment > File Deploy > Windows System Deployment**".

2. Select the client or client group for deploying image, select the one image file and then click "**Deploy Image**".

3. Select the OS version on the "**Plan Wizard**" interface, configure the task plan or keep default settings and then click "**Finish**".

4. On the navigation bar, click "**Task Manager**" to enter the task management interface to view task status and result.

12.4 Upgrade Agent for Windows Clients

On the navigation bar, click **"Common > Agent Upgrade"** to enter Windows client Agent upgrade interface.

Note:

This feature can only upgrade Windows clients. Please refer to 12.1Linux File Deployment for the upgrade of Linux clients. By default, an upgrade file is embedded upon the installation of management server.

Upload upgrade file

To update or replace the upgrade file existing on the management server, perform the following steps:

1. On the navigation bar, click "**Common > Agent Upgrade"** to enter **"updating file management**" interface.
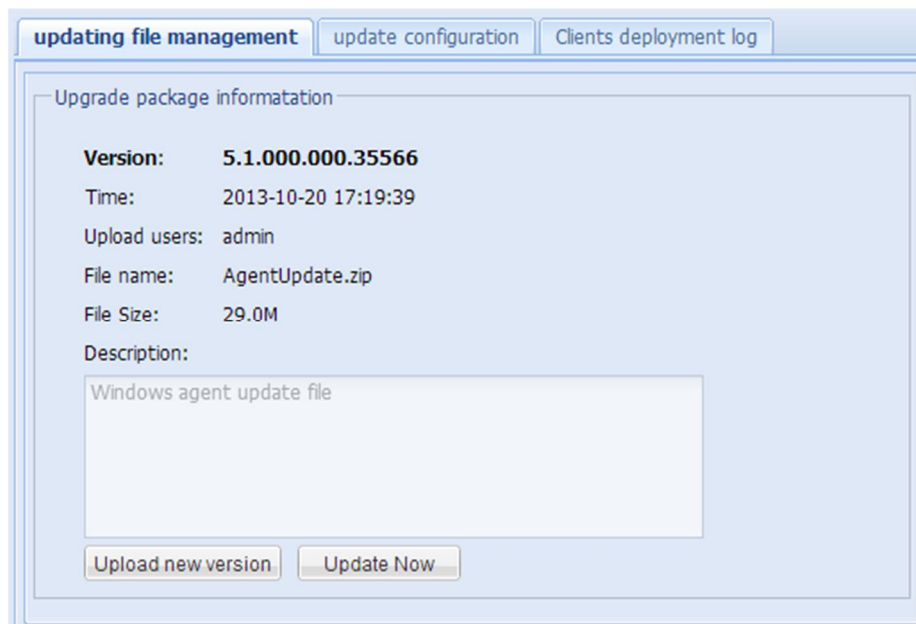
The version information of the existing upgrade file is displayed.

2. Click "**Upload new version**". According to the wizard to complete the upload. Please refer to 23.4Upload the Upgrade File.

Update Now

To immediately update the Agent software for Windows clients, perform the following steps:

1. On the navigation bar, click "**Common > Agent Upgrade**" to enter "**updating file management**" interface.

2. Select the client or client group to be upgraded, click "**Update Now**" and then click "**Yes**" in the confirmation dialog box.
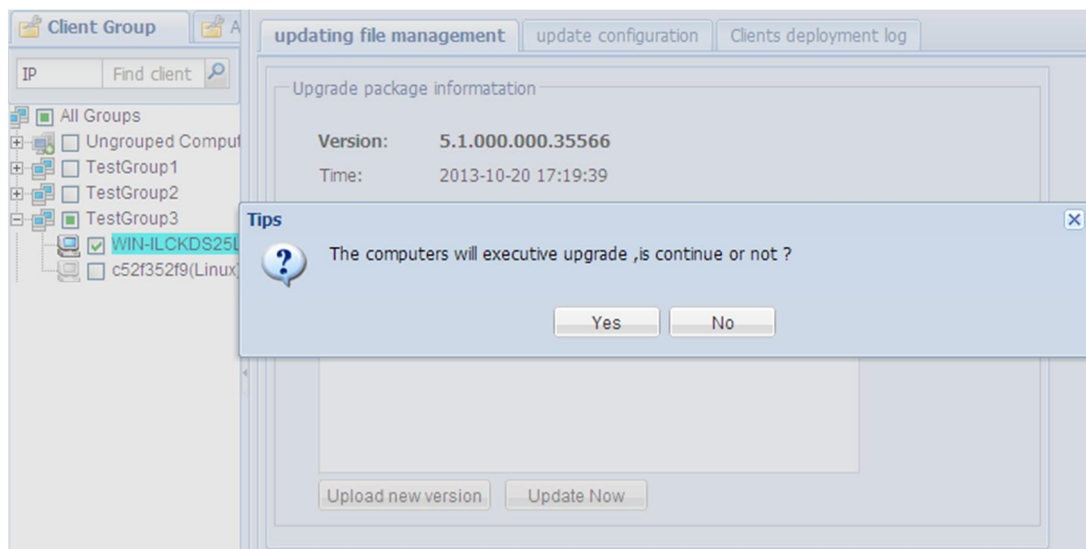
3. Select the client(s) on the **"Plan Wizard"** interface, configure the task plan or keep default settings and then click **"Finish"**.

4. On the navigation bar, click **"Task Manager"** to enter the task management interface to view task status and result.The duration of upgrade process depends on the size of upgrade file, number of clients and download speed.

5. Upon successful upgrade, click **"Common > Agent Upgrade > Clients deployment log"** to enter the upgrade log interface and view detailed upgrade logs.

Automatic upgrade

Automatic upgrade of the Agent software for Windows clients can be achieved through the scheduled update time and update parameters.

To configure automatic upgrade the Agent software for Windows clients, perform the following steps:

1. On the navigation bar, click "**Common > Agent Upgrade > Update Configuration**" to enter the automatic update configuration interface.

2. Configure upgrade parameters.

Memory protection setting

Clients with memory protection enabled must be configured to restart or not before upgrading. This setting also applies to "**Update Now**" clients.

● It will restart before upgrading, please clean up the dirty data: Before upgrading, the client will reboot first in order to clean up dirty data (recommended).

● It will not restart before the upgrade, ignore the dirty data: The client won't restart and will start upgrading directly. Upon completion of upgrade, the current startup operations will be proceeded and dirty data might be introduced.

Auto Update

1. Before enabling Auto Update, make sure the latest upgrade file has been uploaded.
2. During the automatic update, the client needs to keep on.

You can select to enable or disable Auto Update. When it's enabled, set the appropriate Update Time and the client will randomly select a time within the time range to update the Agent.

3. Select the client or client group to be upgraded, click "**Apply**".

4. Select the client(s) on the **"Plan Wizard"** interface, configure the task plan or keep default settings and then click **"Finish"**.

5. On the navigation bar, click **"Task Manager"** to enter the task management interface to view task status and result. Successful task execution only implies successful configuration. The client will execute upgrade within the set time range.

6. After the Update Time has lapsed, click **"Common > Agent Upgrade > Clients deployment log"** to enter the upgrade log interface and view detailed upgrade logs.

View upgrade log

On the navigation bar, click **"Common > Agent Upgrade > Clients deployment log"** to view detailed Agent upgrade logs. You can find out the versions before and after the update, detailed information, update result, etc.

	Alias	Client IP	Version	Pre-version	Time ▾	update result
☐	WIN-ILCKDS2...	192.168.45.114	5.1.000.000.3...	5.1.000.000.3...	2013-10-20 1...	Done
☐	WIN-ILCKDS2...	192.168.45.114	5.1.000.000.3...	5.1.000.000.3...	2013-10-20 1...	Done
☐	WIN-ILCKDS2...	192.168.45.114	5.1.000.000.3...	5.0.000.000.3...	2013-10-20 1...	Done
☐	WIN-ILCKDS2...	192.168.45.114	5.1.000.000.3...	5.1.000.000.3...	2013-10-20 1...	Done

Note:

- The client software can be degraded from higher version to a lower version. The client will first degrade from the higher version to the original version and then upgrade to the designed lower version. Therefore, the deployment log will contain two entries.

- If the upgrade fails, please try again or inform the technical support personnel of the failure prompting message to get help.

You can also switch to **"Client Information"** panel on the homepage to view the version information of the upgraded Agent.

		Alias	Parent group ...	IP ▲	Agent Version	System V...	System Build Date	MAC
☐	🖥	WIN-ILCKDS...	TestGroup3	192.168.45.114	23.6.02.3000.28928	1.30.37	2013040101	14-14-4B-B1-26-E

13 **Resource Center**

13.1 **Introduction**

What is resource center?

Resource center is used by the user for managing file resources, including the deployment and management of storage nodes. Relevant features of the system can only be used after the storage node has been added to the resource center. Therefore, the storage node must be added and bound before use.

What is storage node?

When user proceeds with client upgrade or deploys files, the system must reserve certain file resources for the user, while storage node serves as the carrier of such file resources. The storage node indicates the Centerm Data Server (CDS), which can only be used after being added to the resource center. During deployment, the system must properly deploy the storage nodes according to actual needs.

What is storage node binding?

Binding means to designate a storage node as the closest storage node to a specific client group. While carrying out file operations on this client group, files will only be uploaded to or downloaded from the bound storage node. If the current group is not bound to any storage node, the storage node bound to its parent group will serve as its closest storage node.

The significance of storage node binding is: the client can acquire resources from the closest storage node, thus shortening the duration of file transfer, allowing load balancing and avoid the network congestion caused by acquiring resources from only one storage node.

When one client group is bound to multiple storage nodes, it means this client group can acquire resources from multiple bound storage nodes, thus enhancing the transmission efficiency. When one storage node is bound to multiple client groups, it means multiple client groups will share the resources on the same storage node.

How to properly bind a storage node?

Proper storage node binding can expedite file resource transmission and avoid network congestion. It requires a good understanding of the current client distribution by the administrator. Generally, the storage node bound to the client group must be adjacent either geographically or within the network range. The user is suggested to deploy and bind storage nodes in each geographic area or network area.
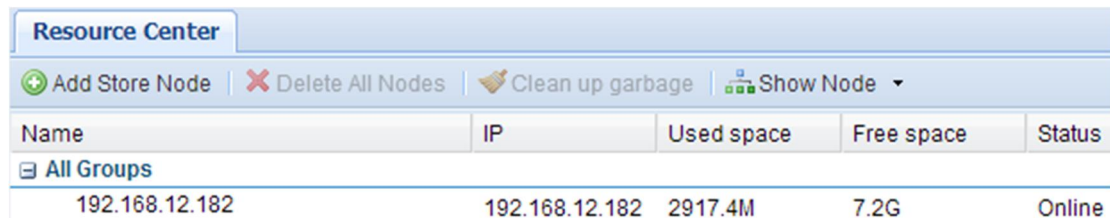
13.2 Add Storage Node

The administrator can only upload upgrade files, upgrade clients or extract files after adding the storage node.

To create a new storage node, please refer to the section relating to data server installation.

Perform the following steps to add a newly created storage node to CCCM.
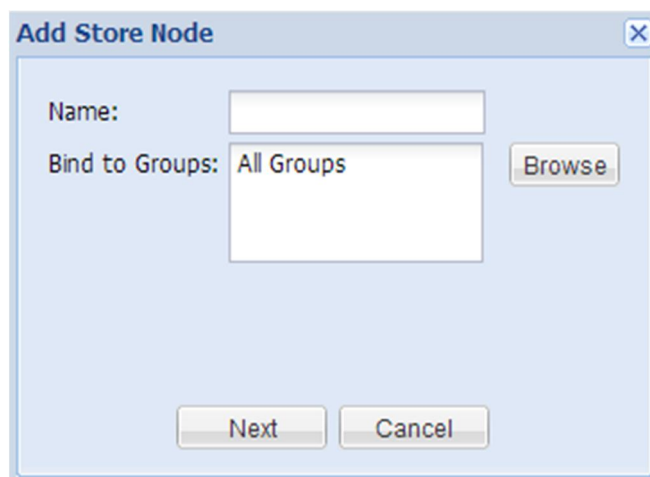
1. On the navigation bar, click "**Deployment > Resource Center**" to enter Resource Center interface.

2. Click "**Add Store Node**" button.

3. Enter node name and click "**Browse**" to select the client group to be bound or keep default settings and click "**Next**".

Bind to Groups:

(Optional) The node is by default bound to the root client group. Click "Browse" button to select other client groups to be bound to. A storage node can be bound to multiple client groups, but cannot be bound to the parent group and subgroup at the same time. As shown below, bind the node to two client groups.
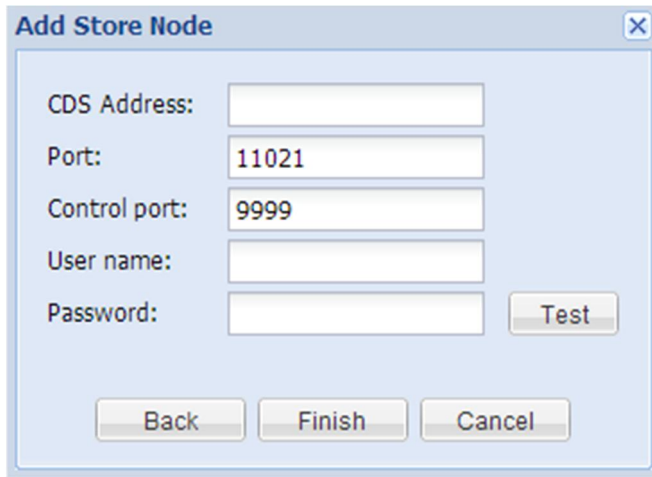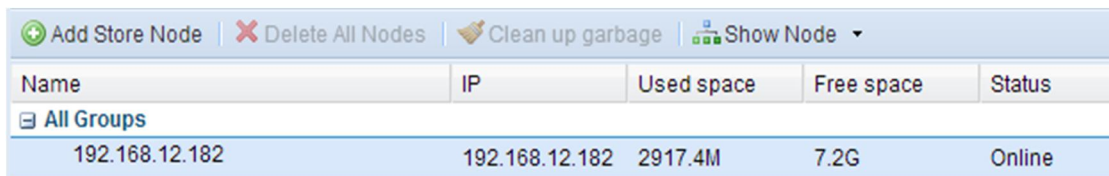
4. Enter the server address (IP address of data server), with default user name being "**admin**" and default password being "**Admin123!**". If the port number has been changed during the installation of database server, you shall enter the same port number here, or else please keep the default setting. Click "**Test**" to test if the data server can be reached.
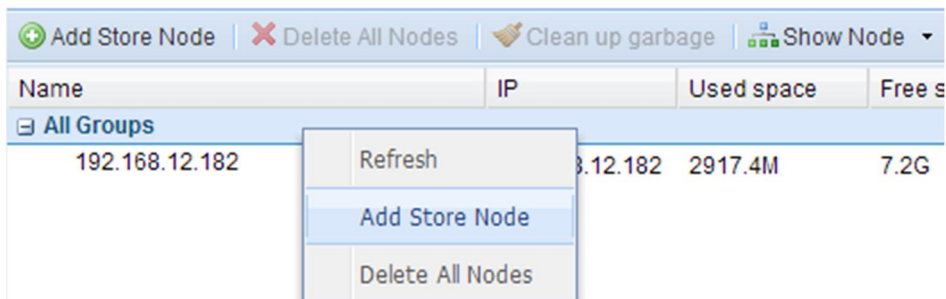
5. After the test, click "**OK**" to add the storage node. The successfully added storage node will appear in the list.

When the list has any binding entry, you can also bind the storage node to the group by right-click the group name to get a context menu, as shown below:

13.3 Modify or Delete Binding

When the storage node has changed or if the node has been abandoned, the binding of storage node must be modified or deleted.

Modify binding

To modify the binding relationship of a node, perform the following steps:

1. On the navigation bar, click "**Deployment > Resource Center**" to enter Resource Center interface.

2. You can modify only one storage node at a time. Right-click the storage node and select "**Attribute**".

Name	IP	Used space	Free space	Status
⊟ All Groups				
192.168.12.182	192.168.12.182	2917.4M	7.2G	Online

3. Click "**Browse**" to reselect the client group to be bound, enter the password again and click "**OK**" to save.

Delete binding

Caution

When delete storage node， all files uploaded will also be deleted.

To modify the binding relationship of a node, perform the following steps:

On the navigation bar, click **"Deployment > Resource Center"** to enter Resource Center interface.

● Delete the binding of a single storage node:

Right-click the storage node and select **"Delete node"** to delete the binding relationship between the current storage node and the client group.

● Delete the binding of all storage nodes under the client group:

Right-click the group name and select **"Delete All Nodes"** to delete the binding relationship between the current client group and all subordinate storage nodes.

- Delete the binding of all storage nodes:

Click **"Delete All Nodes"** on the toolbar.

Only "admin" administrator has this permission.

13.4 Quick Locating

When a storage node fails and thus compromises the normal running of file deployment or client upgrade, click **"Show All"** to expand the list and view all storage nodes, as shown below:

13.5 Clean Up Storage Node

After long-time use, extensive junk files will generate on the storage node, leading to the shortage in free space. The user can clean up the storage node through the following steps:

Clean up garbage

Garbage files are generally generated due to file transfer interruption and abnormal storage node. We can use the **"Clean up garbage"** button on the Resource Center toolbar to clear the garbage files on all storage nodes once for all, but only the **"admin"** administrator has such permission.

Caution:

If the system is executing file operations, do not use this feature, as it may cause abnormalities in operations.

Clean files

If you are certain that there is no important file on the storage node, you can use this feature to release space on the storage node. The clean command can only be executed on one node. Once it is executed, all files uploaded to the storage node will be deleted.

Caution:

If the system is executing file operations, do not use this feature, as it may cause abnormalities in operations.

14 Policy Center

The Policy Center allows to you create file update and template configuration polices to be bound to the client groups. Upon successful policy creation, the Policy Center Task will be generated and executed automatically, enabling automatic client upgrade and automatic template configuration.
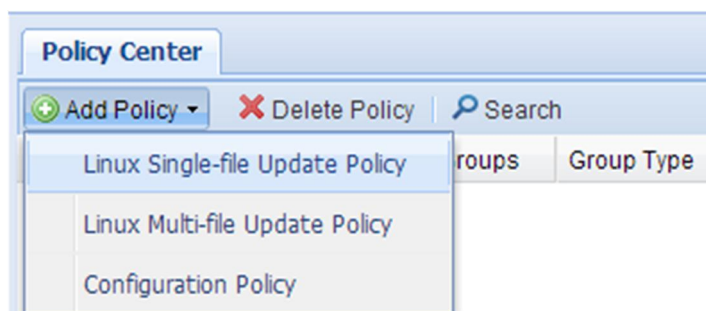
On the navigation bar, click **"Policy Center"** to enter the Policy Center management interface.
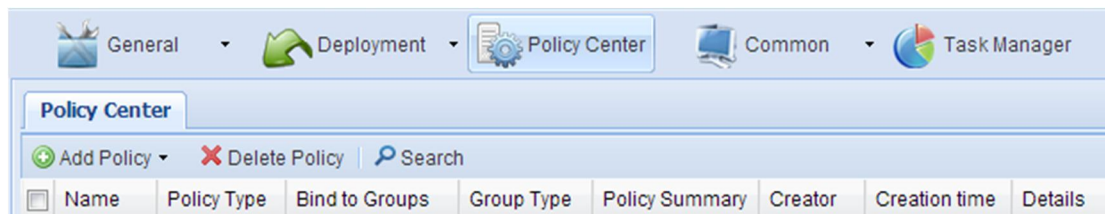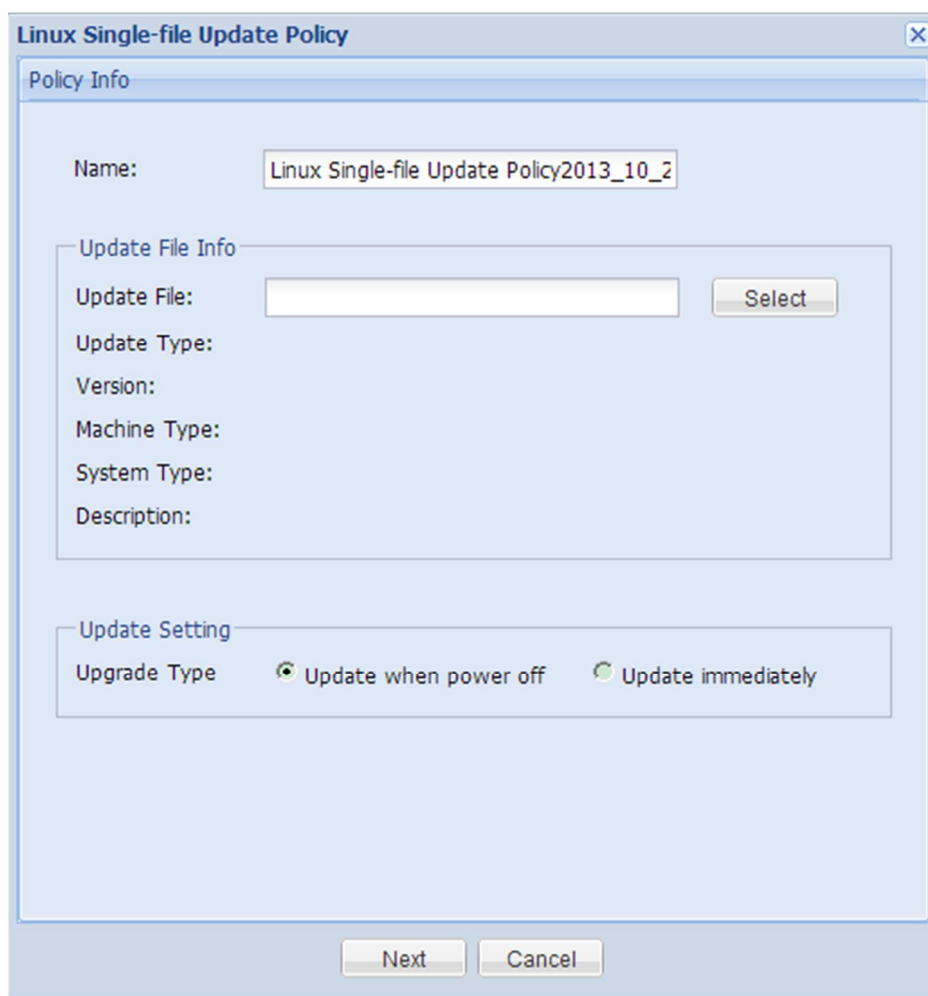

Linux Single-file Update Policy

To create Linux single-file update policy, perform the following steps:

1. On the navigation bar, click "**Policy Center**" to enter the Policy Center management interface.

2. Click "**Add Policy > Linux Single-file Update Policy**".

3. On "**Linux Single-file Update Policy**" configuration interface, edit policy name (optional) and click "**Select**".
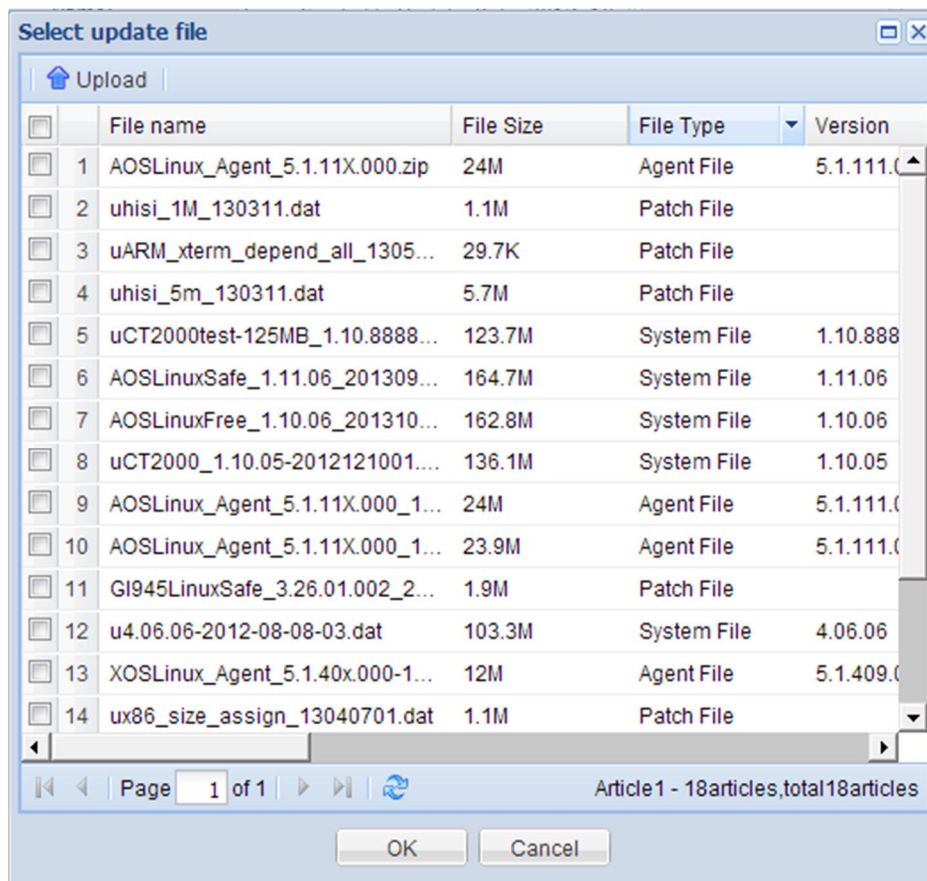
4. Select one target update file from the file list and click "**OK**".

   To upload a new file, click **"Upload"** and follow the instructions in the wizard. Please refer to 12.1Linux File Deployment for details.

Select update file

		File name	File Size	File Type	▼	Version
☐	1	AOSLinux_Agent_5.1.11X.000.zip	24M	Agent File		5.1.111.(
☐	2	uhisi_1M_130311.dat	1.1M	Patch File		
☐	3	uARM_xterm_depend_all_1305...	29.7K	Patch File		
☐	4	uhisi_5m_130311.dat	5.7M	Patch File		
☐	5	uCT2000test-125MB_1.10.8888...	123.7M	System File		1.10.888
☐	6	AOSLinuxSafe_1.11.06_201309...	164.7M	System File		1.11.06
☐	7	AOSLinuxFree_1.10.06_201310...	162.8M	System File		1.10.06
☐	8	uCT2000_1.10.05-2012121001....	136.1M	System File		1.10.05
☐	9	AOSLinux_Agent_5.1.11X.000_1...	24M	Agent File		5.1.111.(
☐	10	AOSLinux_Agent_5.1.11X.000_1...	23.9M	Agent File		5.1.111.(
☐	11	GI945LinuxSafe_3.26.01.002_2...	1.9M	Patch File		
☐	12	u4.06.06-2012-08-08-03.dat	103.3M	System File		4.06.06
☐	13	XOSLinux_Agent_5.1.40x.000-1...	12M	Agent File		5.1.409.(
☐	14	ux86_size_assign_13040701.dat	1.1M	Patch File		

◄◄ ◄ Page 1 of 1 ► ►► ⟳   Article1 - 18articles,total18articles

[OK] [Cancel]

5. Configure upgrade parameters and click "**Next**".
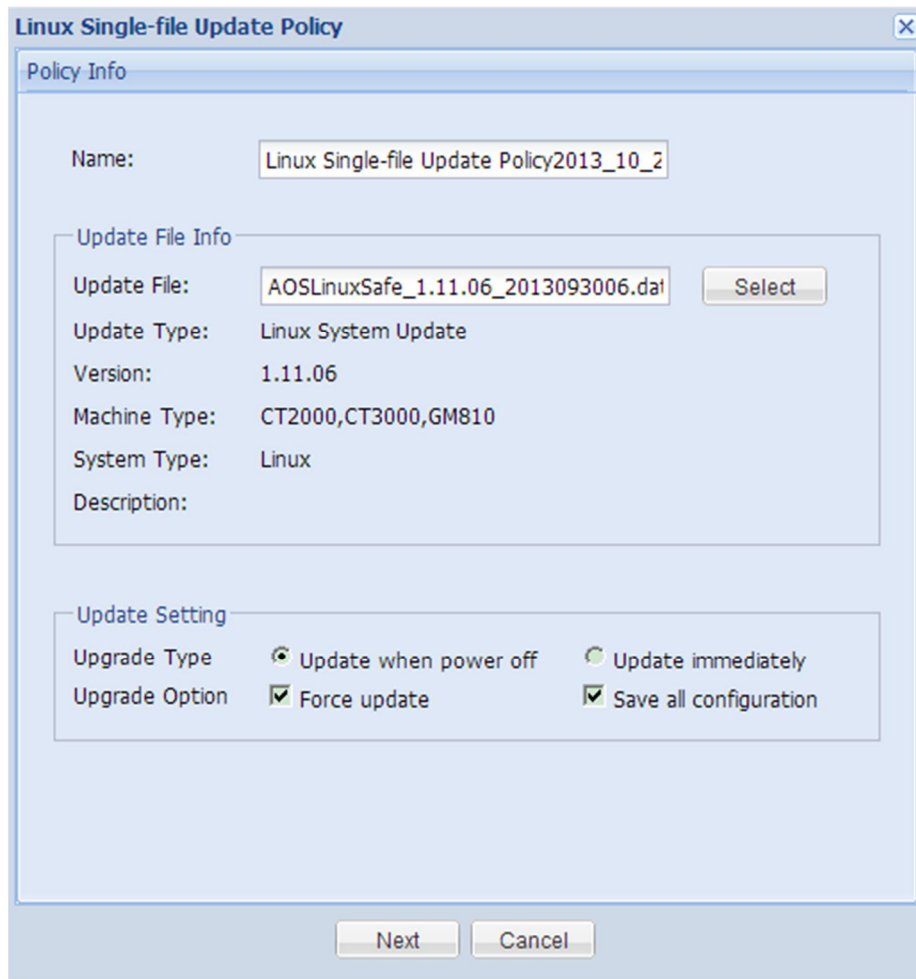
Update Setting

<mark>If the update file selected is a system file, system upgrade options will appear.</mark>

Upgrade Type

- Update when power off: to start update when the client is shut down normally and then shut down the client upon completion.
- Update immediately: to prompt the client user to update immediately after the client has downloaded the update file, yet client user can choose to postpone the update.

Update Setting

By default, **"Force update"** and **"Save all configuration"** have been enabled (applicable to operating system upgrade).

6. Select one client group to be bound and click "**Next**".

7. Select the OS version of clients on the **"Plan Wizard"** interface, configure the task plan or keep default settings and then click **"Finish"**.

8. On the navigation bar, click **"Task Manager"** to enter the task management interface and view upgrade status and result in the **"Policy Center Task"**.

The Policy Center tasks are always effective. You can periodically view the upgrade progress and result.

Linux Multi-file Update Policy

To create Linux multi-file update policy, perform the following steps:

1. On the navigation bar, click "**Policy Center**" to enter the Policy Center management interface.

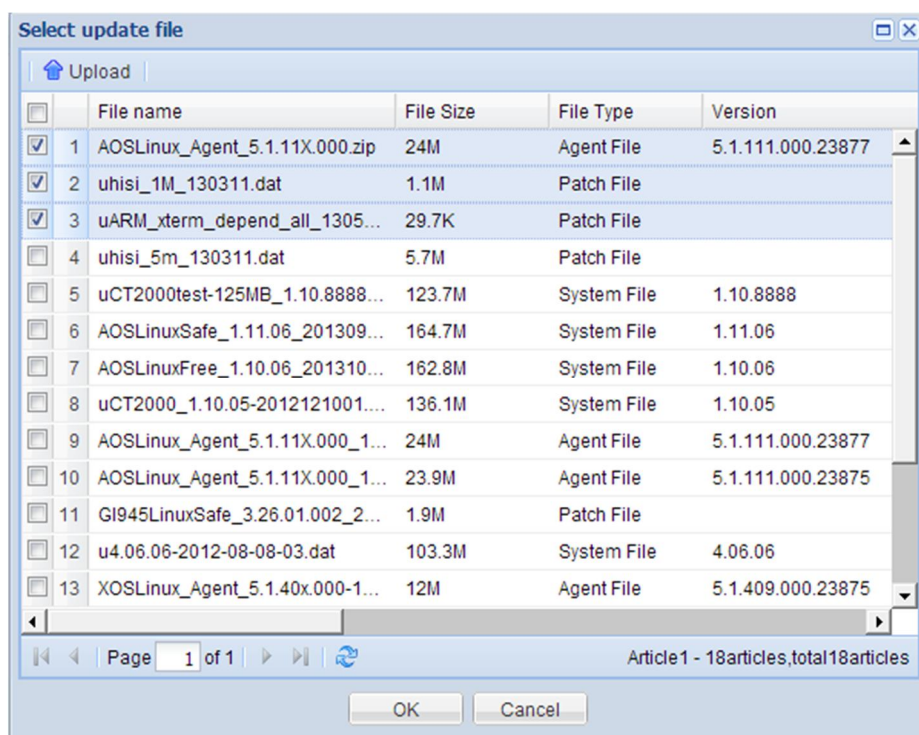2. Click "**Add Policy > Linux Multi-file Update Policy**".
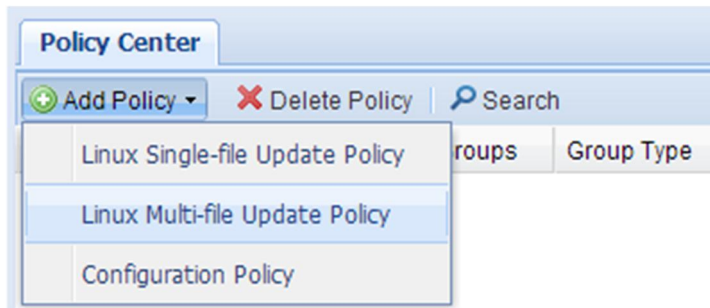
3. On "**Linux Multi-file Update Policy**" configuration interface, edit policy name (optional) and click "**Add**".
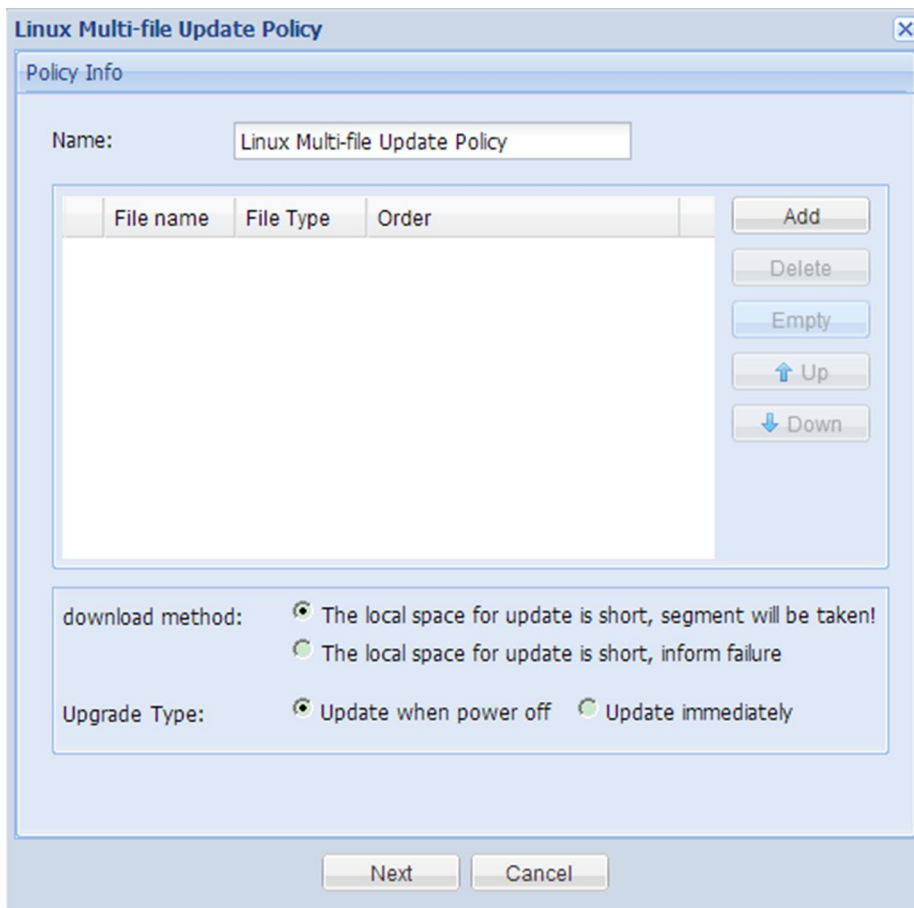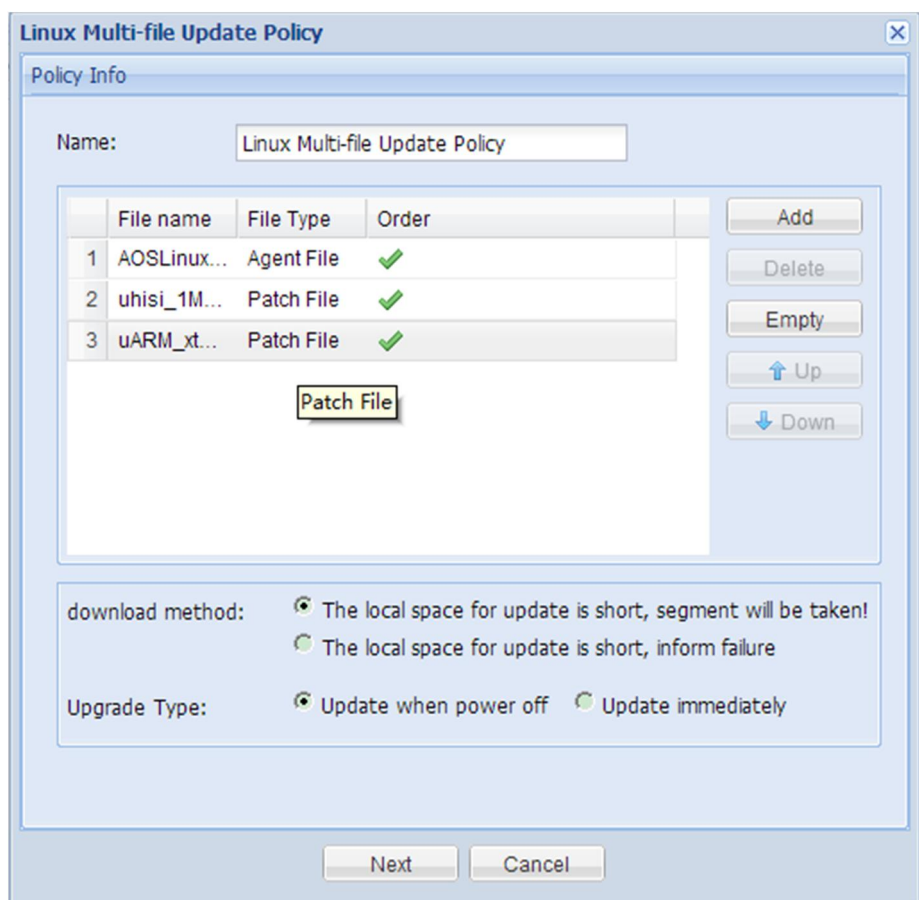

4. Select one or more target update files from the file list and click "**OK**".

To upload a new file, click **"Upload"** and follow the instructions in the wizard. Please refer to 12.1Linux File Deployment for details.

5. Edit policy conditions and click "**Next**".

Order of update files

You can add, delete or clear update files, or move up/down update files to change the order. ✔ indicates that the sequence of file update is correct, while ✖ indicates that the sequence is inappropriate, and you will need to change the update order or delete this file

from the update list.

If the order of all update files is correct (all indicating ✔), then you can proceed to the next step.

Download method

To configure how the file will be downloaded when the local space for update is short.

- Segment will be taken: update process will be continued.
- Inform failure: terminate this update.
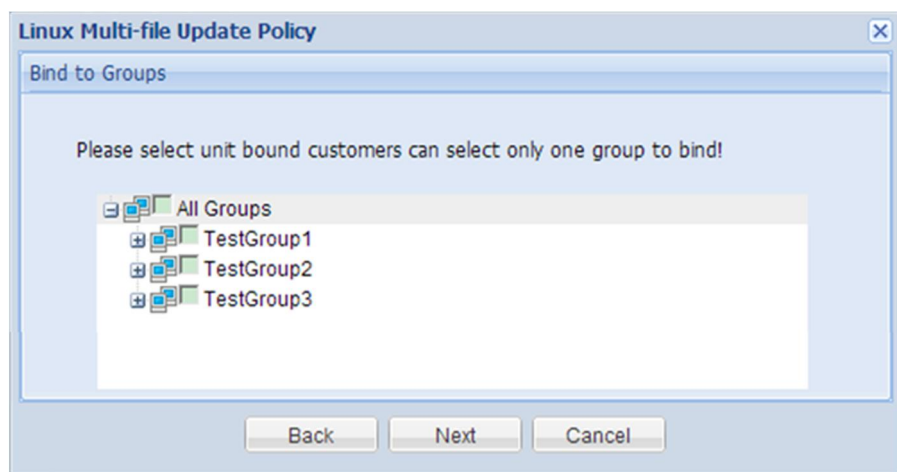
Upgrade Type

- Update when power off: to start update when the client is shut down normally and then shut down the client upon completion.
- Update immediately: to prompt the client user to update immediately after the client has downloaded the update file, yet client user can choose to postpone the update.

If the update file selected is a system file, system upgrade options will appear.

Update Setting

By default, **"Force update"** and **"Save all configuration"** have been enabled (applicable to operating system upgrade).

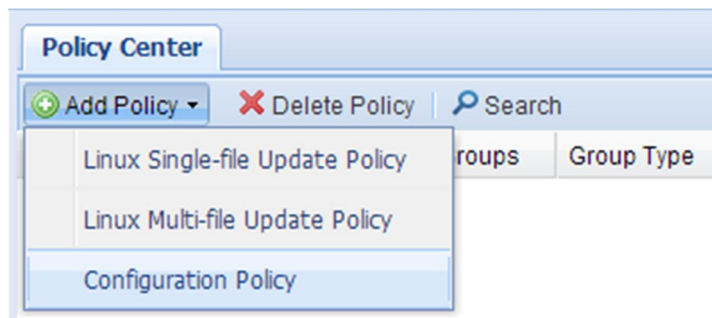6. Select one client group to be bound and click "**Next**".

7. Select the OS version of clients on the **"Plan Wizard"** interface, configure the task plan or keep default settings and then click **"Finish"**.

8. On the navigation bar, click **"Task Manager"** to enter the task management interface and view upgrade status and result in the **"Policy Center Task"**.

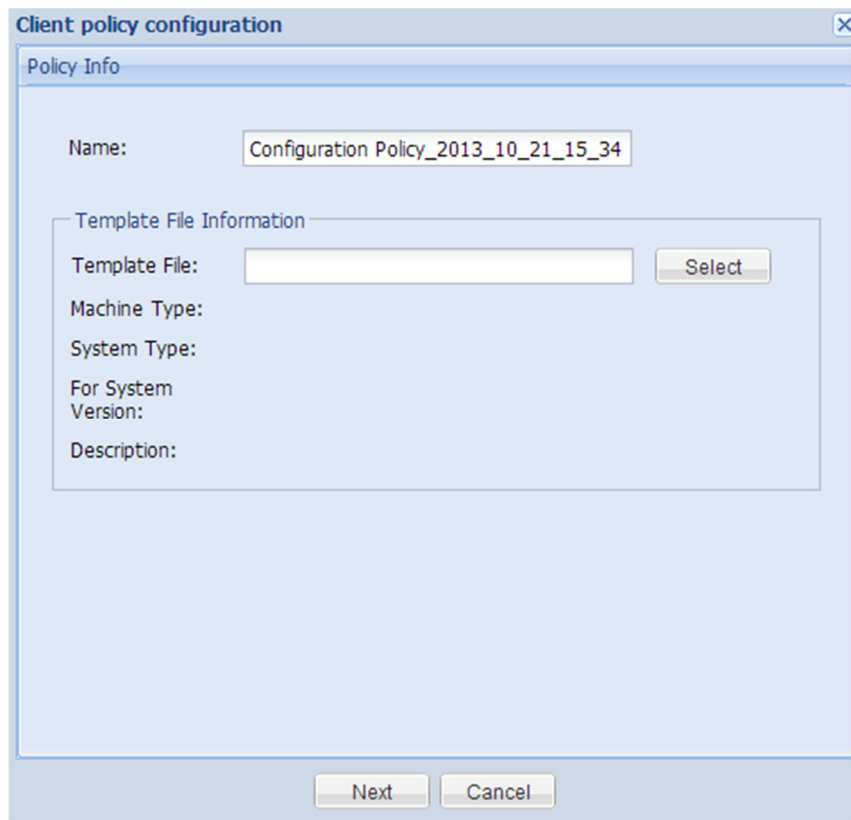   The Policy Center tasks are always effective. You can periodically view the upgrade progress and result.

Client Configuration Policy

To create client configuration policy, perform the following steps:

1. On the navigation bar, click **"Policy Center"** to enter the Policy Center management interface.

2. Click **"Add Policy > Configuration Policy"**.

3. On the "**Client policy configuration**" interface, edit policy name (optional) and click "**Select**".

4. Select one template file from the file list and click "**OK**".

   Click **"View"** to view the detailed configuration information of this template file.
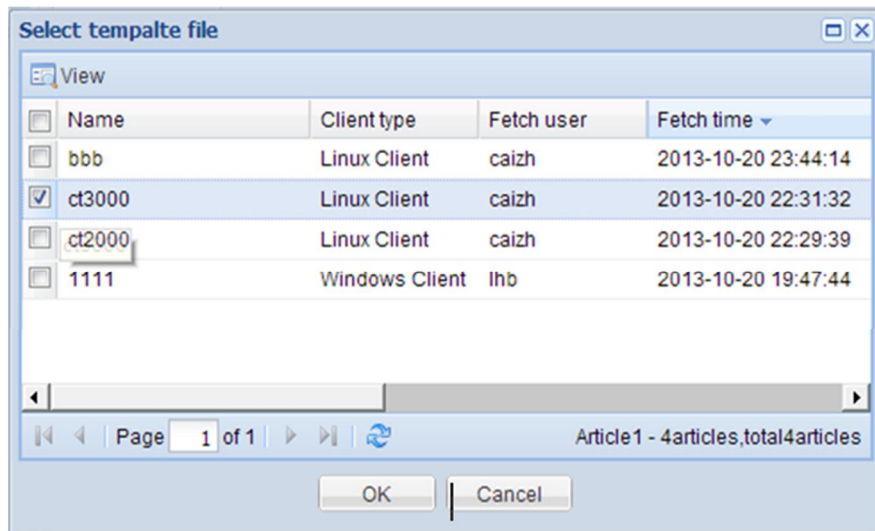
5. On the "**Client policy configuration**" interface, click "**Next**".

6. Select one client group to be bound and click "**Next**".
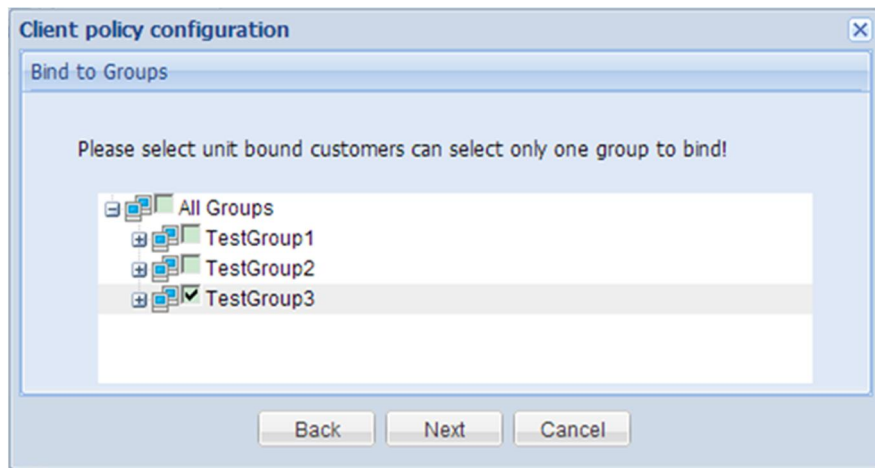
7. Select the OS version of clients on the **"Plan Wizard"** interface, configure the task plan or keep default settings and then click **"Finish"**.

8. On the navigation bar, click **"Task Manager"** to enter the task management interface and view upgrade status and result in the **"Policy Center Task"**.

   The Policy Center tasks are always effective. You can periodically view the upgrade progress and result.

15 User Management

Users indicates the system administrators of CCCM. According to the permissions granted, users can perform one or multiple operations shown below:

- Edit personal registration information and password;
- Create new users and user groups;
- Set user as the person in charge;
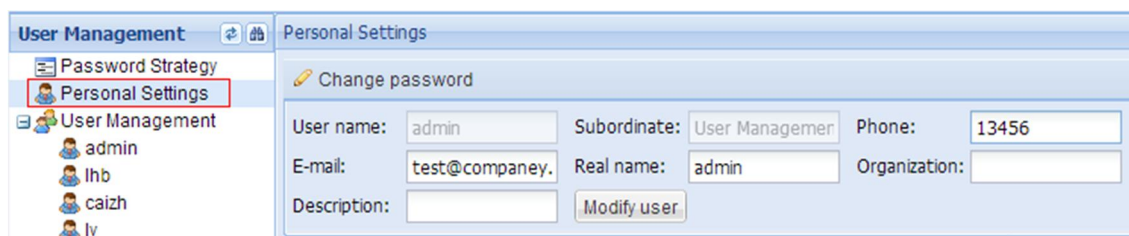- Create new roles assigned with one or multiple permissions.
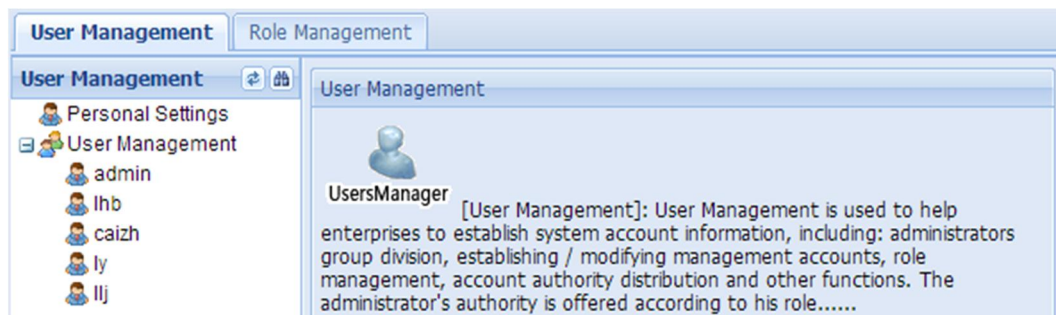
15.1 Personal Settings

Modify personal information

To modify personal information, perform the following steps:

1. On the navigation bar, click "**Common > User Control**" to enter the user management interface.

2. In the "**User Management**" pane, click "**Personal Settings**".

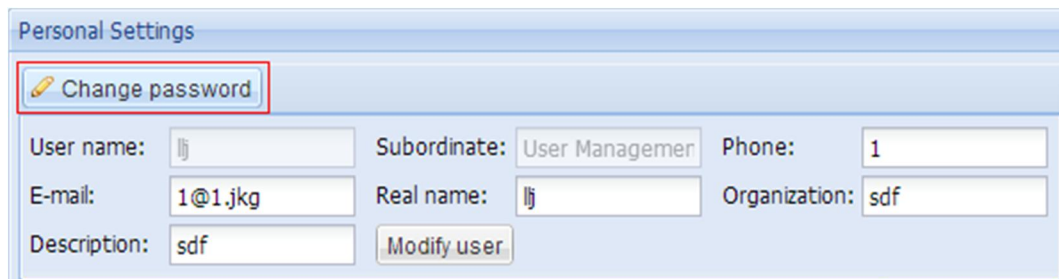3. Edit personal information and click "**Modify user**" to save.

The user can modify all personal information other than the resource information and role information (if this user is a **"person in charge"**, he/she can then modify the resource information).

Change password

To change password, perform the following steps:

1. On the navigation bar, click "**Common > User Control**" to enter the user management interface.
2. In the "**User Management**" pane, click "**Personal Settings**".
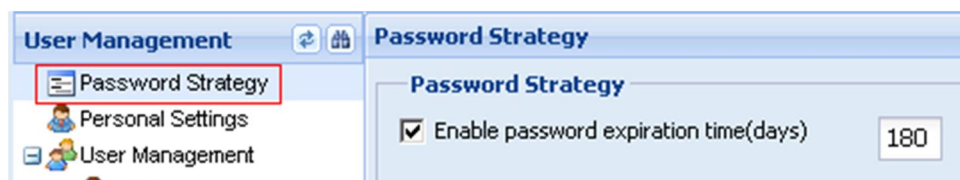3. On the "**Personal Settings**" panel, click "**Change password"**.

4. In the password dialog box, enter the original password and new password, confirm the new password and then click "**OK**" to save.

15.2 Password Strategy

Administrator **"admin"** can set the expiration time for the password. Upon password expiration, the user will be requested to change the password upon login.

To set the expiration time for password, perform the following steps:

1. Use "**admin**" account to log in the system.
2. On the navigation bar, click "**Common > User Control**" to enter the user management interface.
3. In the "**User Management"** pane, click "**Password Strategy".**
4. Check **"Enable password expiration time (days)**", enter the value in days and then click "**Save**".

15.3 Role Management

A role defines how the user will manage the system. Each role contains at least one permission. The administrator may have one or multiple roles.
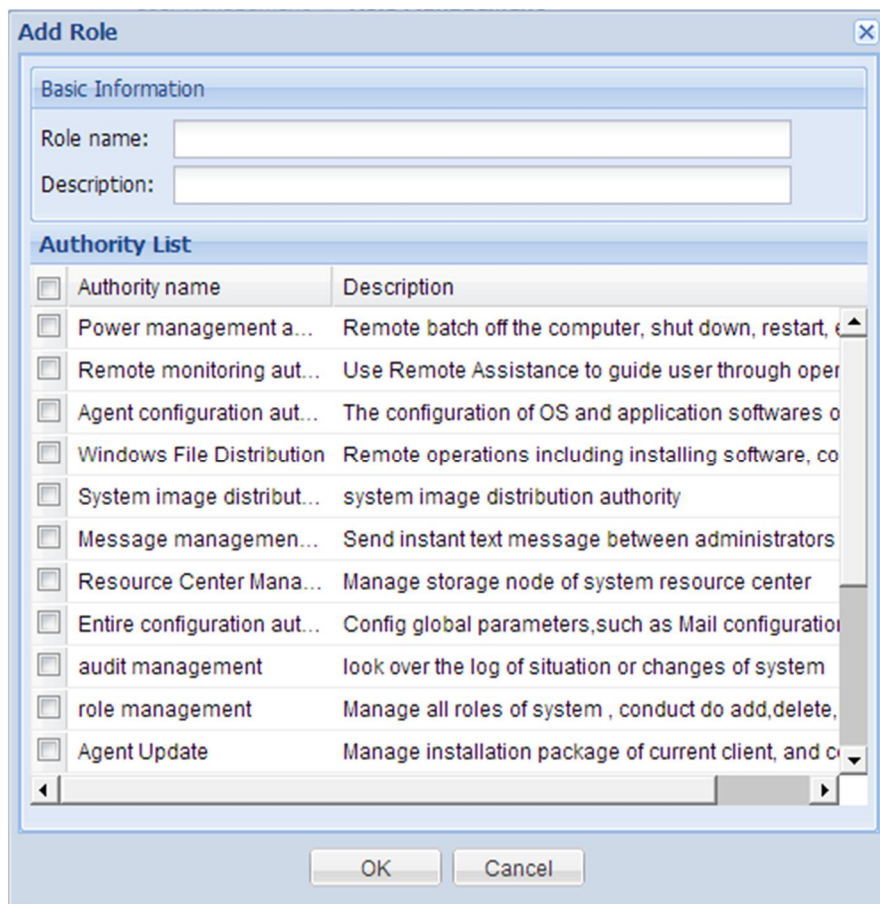
Add role

To add role, perform the following steps:

1. Use "**admin**" account or any account set as the person in charge to log in the system.
2. On the navigation bar, click "**Common > User Control > Role Management"** to enter the role management interface.
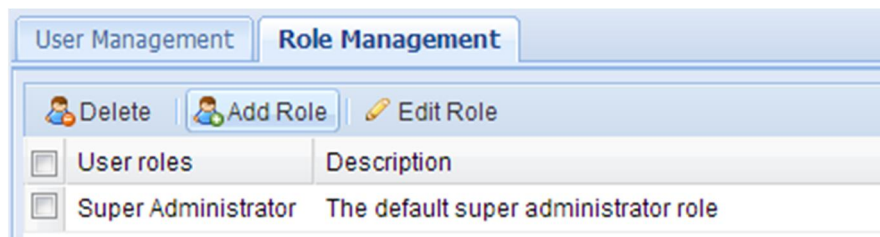
3. Click "**Add Role**" and enter role name and description in the new window. Select the required permissions and click "**OK**".

Edit role

To edit role, perform the following steps:

1. Use "**admin**" account or any account set as the person in charge to log in the system.

2. On the navigation bar, click "**Common > User Control > Role Management**" to enter the role management interface.

3. Click "**Edit Role**" and edit role name and description. Select the required permissions and click "**OK**".

Delete role

To delete role, perform the following steps:

1. Use "**admin**" account or any account set as the person in charge to log in the system.

2. On the navigation bar, click "**Common > User Control > Role Management**" to enter the role management interface.

3. Click "**Delete**".

4. In the confirmation dialog box, click "**OK**".

15.4 User Management

After CCCM installation is completed, the default username is **"admin"** and default password is **"Admin123!@#"**. During first-time login, **"admin"** user must change the initial password, and the new password must have at least 8 characters containing letters (case sensitive), digits and special symbols. The user can configure the user/group, role and the corresponding permissions. A user can be assigned with different roles. A role is the combination of one or multiple permissions, with each permission corresponding to different system privileges.

Create user group

To create user group, perform the following steps:

1. On the navigation bar, click "**Common > User Control"** to enter the user management interface.

2. In the "**User Management**" pane, right-click "**User Management"** or any existing user group and select **"Add user group"**.
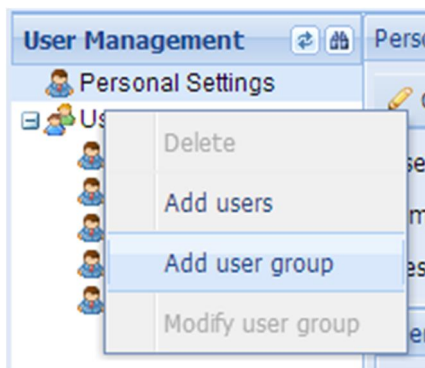
3. Enter group name and description and then click "**OK**".

Modify user group

To modify the name and description of user group, perform the following steps:

1. On the navigation bar, click **"Common > User Control"** to enter the user management interface.

2. In the **"User Management**" pane, right-click the user group to be modified and select **"Modify user group"**.

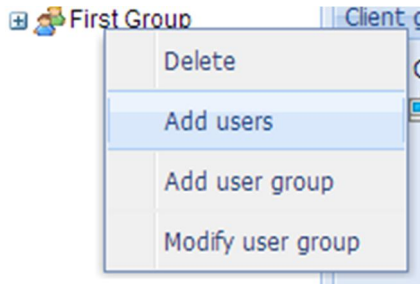3. Edit user group information and click "**OK**".

Delete user group

To delete user group, perform the following steps:

1. On the navigation bar, click "**Common > User Control**" to enter the user management interface.

2. In the "**User Management**" pane, right-click the user group to be deleted and select "**Delete user group**".

3. In the confirmation dialog box, click "**OK**".

Create user

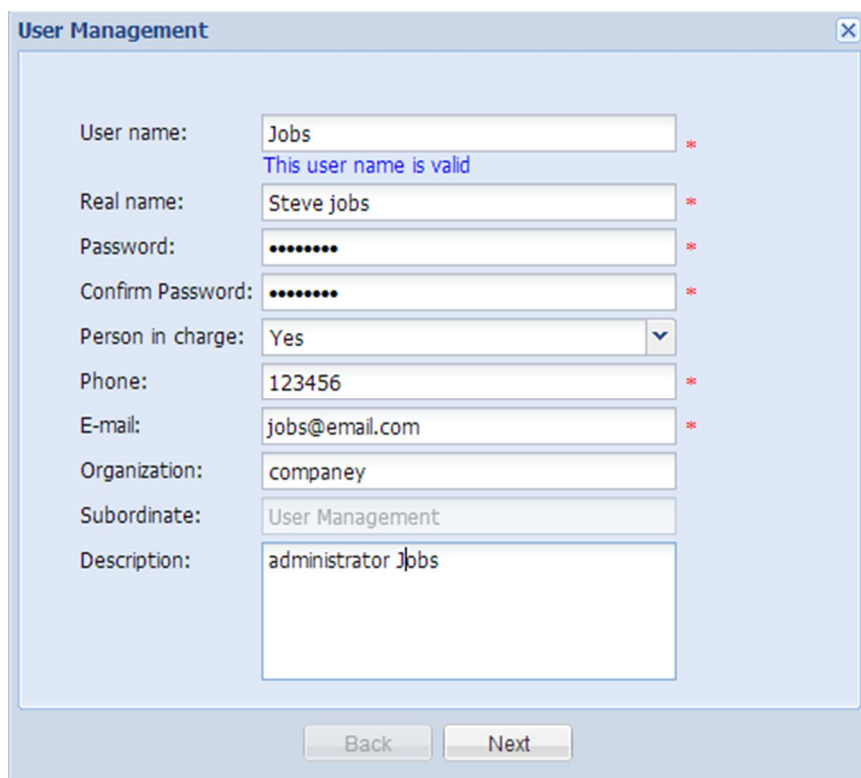To create user, perform the following steps:

1. Use "**admin**" account or any account set as the person in charge to log in the system.
2. On the navigation bar, click "**Common > User Control**" to enter the user management interface.
3. In the **"User Management**" pane, right-click "**User Management**" or any subordinate group node and select "**Add users**".
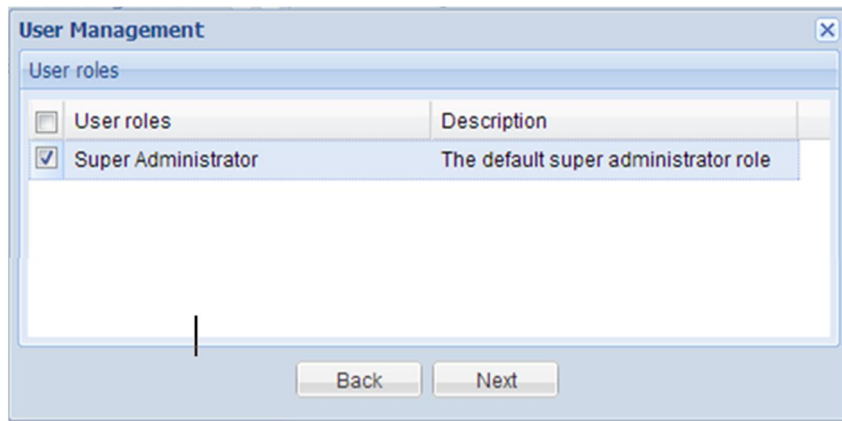

4. Enter user information and click "**Next**".

   Note:

   Person in charge: this user can govern all users in the same user group.

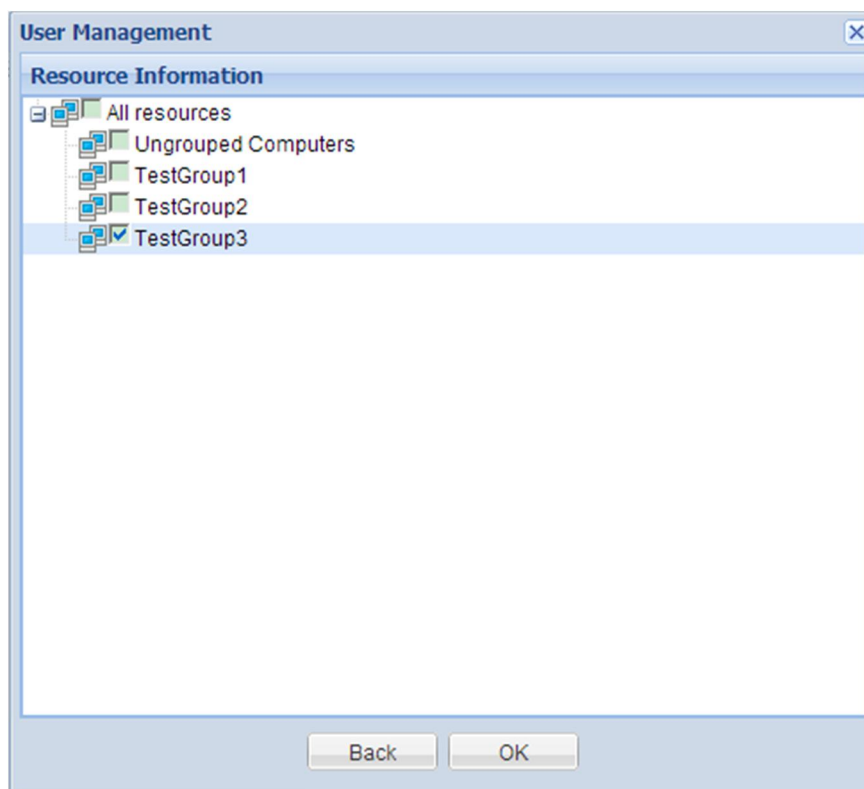5. Assign role(s) and click "**Next**".

6. Assign client resources.

    The resources imply the clients that can be managed by the user. Upon login, the user can only see the clients that can be managed by him/her.

    Note:

    If no client/group is assigned to this user, the "**Ungrouped Computers**" must be assigned to the user.

7. Click "**OK**" to complete user creation.

Modify user

To modify user, perform the following steps:

1. Use "**admin**" account or any account set as the person in charge to log in the system.
2. On the navigation bar, click "**Common > User Control**" to enter the user management interface.

3. In the "**User Management**" pane, right-click "**User Management**" or any subordinate group node and select "**Modify**".

4. Edit user information and click "**Next**".

5. Assign role(s) and click "**Next**".

6. Assign client resources and click "**OK**".

Delete user

To delete user, perform the following steps:

1. Use "**admin**" account or any account set as the person in charge to log in the system.

2. On the navigation bar, click "**Common > User Control**" to enter the user management interface.

3. In the **"User Management"** pane, right-click "**User Management**" or any subordinate group node and select "**Delete**".

4. Click "**OK**".

Set person in charge

The user set as person in charge can govern all users in the same user group. This user can view, modify and delete user(s) and set another user as (or clear) person in charge.

To set a user as person in charge, perform the following steps:

1. Use "**admin**" account or any account set as the person in charge to log in the system.

2. On the navigation bar, click "**Common > User Control**" to enter the user management interface.

3. In the "**User Management**" pane, right-click "**User Management"** or any subordinate group node.

4. In the list on the right side, manage the **"Person in charge"** of this group.

● Select the user and click "**Set person in charge**" to set the selected user as the person in charge.

● Select the user and click "**Clear person in charge**" to discharge the selected user from the role of "**person in charge**".
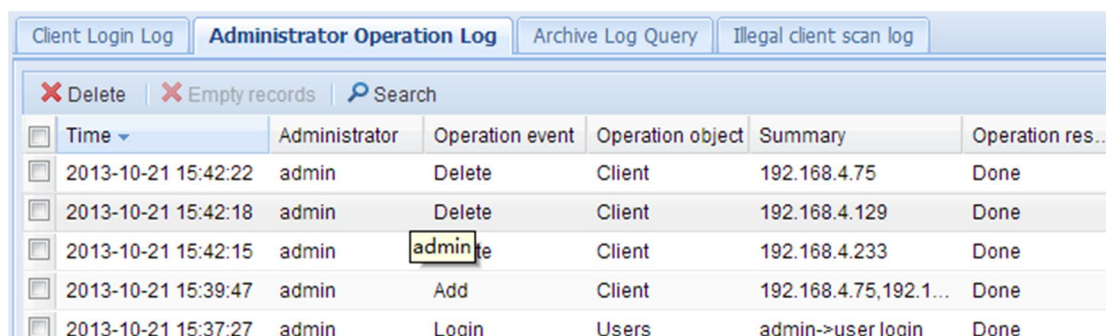
16 Audit Management

Audit Management provides **"Administrator Operation Log"**, **"Client Login Log"**, **"Archive Log Query"** and **"Illegal client scan log"**. The administrator can query and manage these logs as needed.

16.1 Administrator Operation Log

The Administrator Operation Log records the management operations done by the administrator, including operation event, operation object and operation result.

On the navigation bar, click **"Common > Audit Management > Administrator Operation Log"** to enter the operation interface.

The user can perform the following operations on the log:

- Search: Click "**Search**" button and type the keyword on the expanded search panel to search.
- Delete: Select one or more log entries and click "**Delete**" button.
- Empty records: Only administrator "**admin**" has such permission.

16.2 Client Login Log

"Client Login Log" is used to view the login records of clients, including login time, offline time, online time, etc.

On the navigation bar, click **"Common > Audit Management > Client Login Log"** to enter the operation interface.

The user can perform the following operations on the log:

- Search: Click "**Search**" button and type the keyword on the expanded search panel to search.
- Delete: Select one or more log entries and click "**Delete**" button.
- Empty records: Only administrator "**admin**" has such permission.

16.3 Archive Log Query

The archive log contains logs stored in the system.

On the navigation bar, click "**Common > Audit Management > Archive Log Query**" to enter the operation interface.

The user can perform the following operations on the log:

- Search: Click "**Search**" button and type the keyword on the expanded search panel to search.
- Empty records: Only administrator "**admin**" has such permission.

16.4 Illegal Client Scan Log

Illegal Client Scan Log records illegal clients found by the system. Clients which ought to be controlled by the server but are actually not controlled by the server are all called illegal clients.

On the navigation bar, click "**Common > Audit Management > Illegal Client Scan Log**" to enter the operation interface.

The user can perform the following operations on the log:

- Search: Enter IP address to search.
- Delete: Only "**admin**" administrator has this permission.
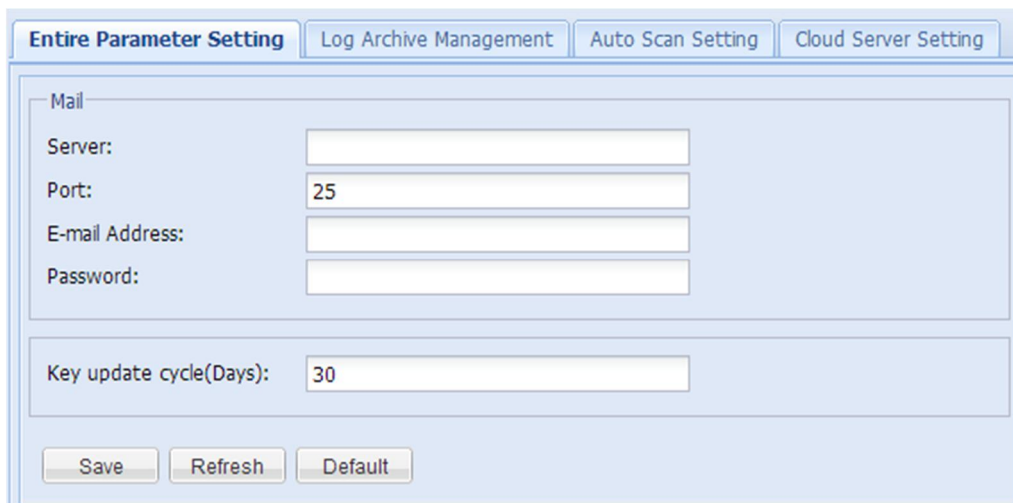
17 Global Settings

The Global Settings module allows you to configure such global settings as CCCM email, key update cycle, log archive management, cloud server address list, etc.

17.1 Entire Parameter Setting

On the **"Entire Parameter Setting"** page, the administrator can configure the mail server. System systems will be sent via this mail server.

In **"Key update cycle"**, the administrator can set the interval for updating AES communication key.

On the navigation bar, click **"Common > Global Setting > Entire Parameter Setting"** to enter the operation interface.

17.2 Log Archive Management

To set the archiving item(s) and the interval of automatic archiving.

On the navigation bar, click **"Common > Global Setting > Log Archive Management"** to enter the operation interface.

- Enable auto archive

  After checking **"Enable auto archive"**, the system will automatically archive logs pursuant to the set interval.

- Archive Now

  Click **"Archive Now"** and the system will immediately archive the logs.

17.3 Auto Scan Setting

By enabling auto-scan, CCCM will scan the designated IP ranges to find whether or not there are clients which haven't been added to management or clients being controlled by illegal servers. After checking **"Send Email to administrator"**, the system will send to scan results to the system email.
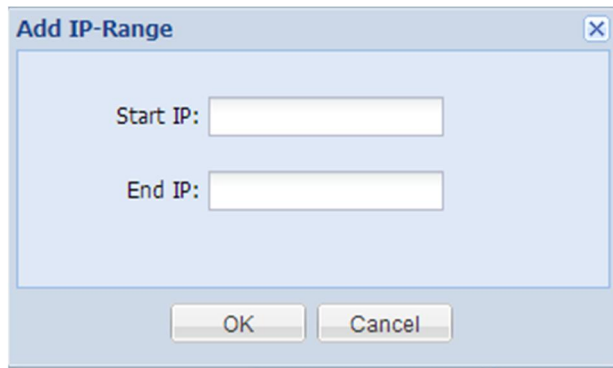
On the navigation bar, click **"Common > Global Setting > Auto Scan Setting"** to enter the operation interface.

Note:

Auto-scan is disabled by default.

When no IP range to be scanned has been configured, CCCM will not proceed with scanning.

To enable or configure auto-scan, perform the following steps:

1. Check **"Open auto-scan function"** to enable auto-scan.

2. Set start time or keep the default setting.

3. Set scan interval (in hours) or keep the default setting. Default: 24 hours; effective range: 1-360 hours.

4. Set to send email t administrator (enabled by default).

5. Click **"Add"** to add the IP ranges.

6. Edit IP range information and click **"OK"**.

   Note

   One IP range is suggested to include only four Class-C network segments, such as 192.168.1.0 - 192.168.4.255.
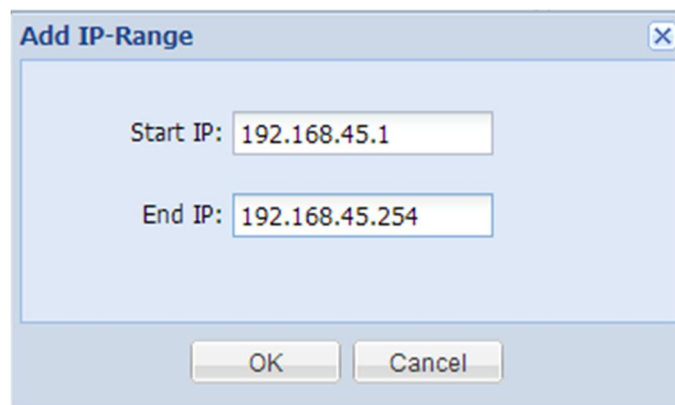
7. Click "**Apply**" to complete configuration.

Manage IP range information

After enabling auto-scan, perform the following steps to scan the IP range(s).

1. On the navigation bar, click "**Common > Global Setting > Auto Scan Setting**" to enter the operation interface.
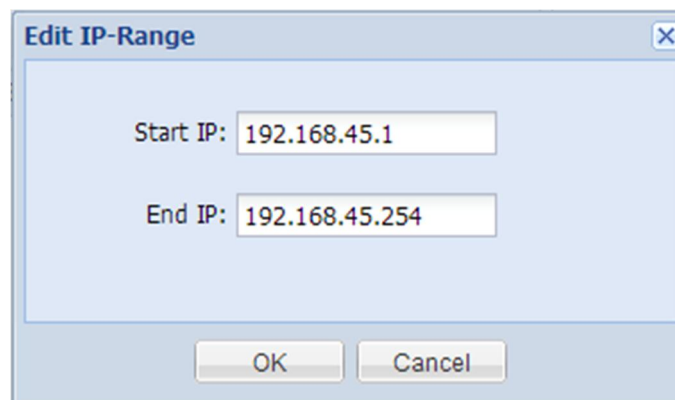2. Manage IP range(s).
   - Add

     Click **"Add"**, enter IP range information and click **"OK"**.

   - Edit

     Select an existing IP range and click **"Edit"**.

     After editing IP range, click **"OK"**.

   - Delete

     Select an existing IP range and click **"Delete"**.

17.4 Cloud Server Setting

You can create and maintain an list a cloud server addresses on CCCM for server-client synchronization.

To manage the list of cloud server addresses, perform the following steps:

On the navigation bar, click **"Common > Global Setting > Cloud Server Setting"** to enter the operation interface.

Edit server address list

- Add address

  Click **"Add"**, enter server name and address and click **"Save"**.

- Edit address

  Select an existing server address and click **"Edit"**. After editing server name and address, click **"Save"**.
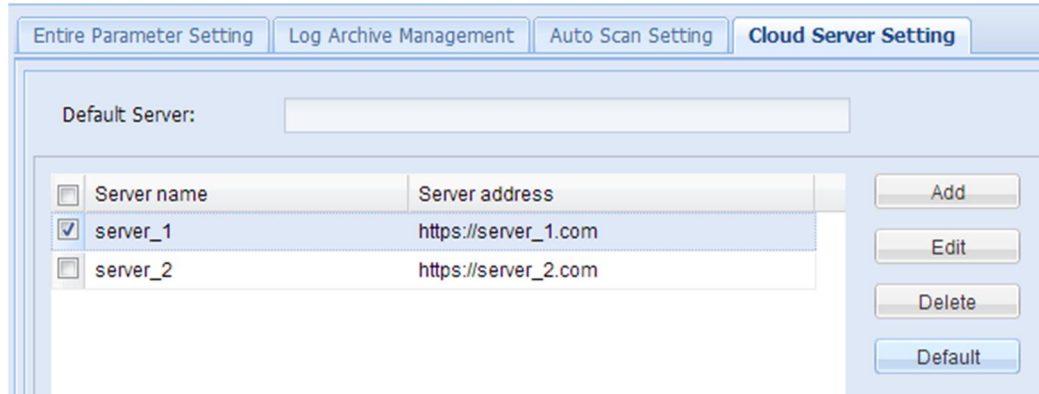

- Delete address

  Select an existing server address and click **"Delete"**.

Set the default server address

By setting the default address on the server, the client will use this default address as the current connection address after synchronizing the address list.
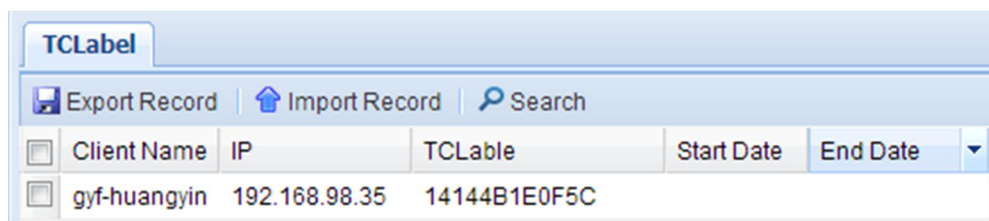
Select one server address and click **"Default"**.

18 Maintenance Management

Maintenance Management allows you to take statistics of the maintenance information of clients managed, import the existing maintenance information and import new maintenance information.

On the navigation bar, click **"Common > Maintenance"** to enter the operation interface.

Export Record

Click **"Export Record"** and save the file following the instructions in the wizard. The default file name is **"tclables.xls"**.

Import Record

On the operation interface, click **"Import Record"** to pop up the **"Import Record"** interface. Click **"Browse"** to select file and then click **"Import"** button.

The maintenance file to be imported will be provided by the client manufacturer or service provider.
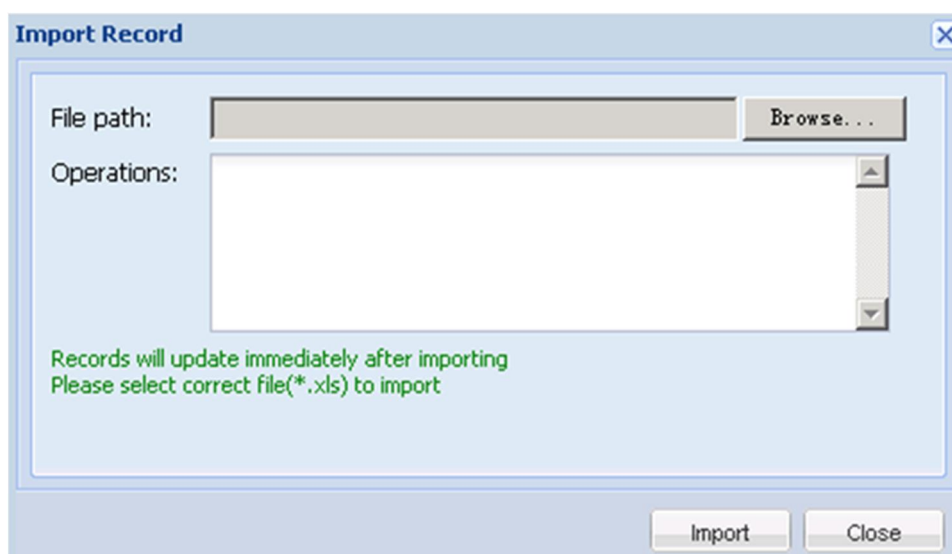
19 Task Management

19.1 Introduction

What is task?

A task can be considered as one or a series of commands assigned by the system to the client, which will execute such command(s) according to specific conditions, making this process a task. Currently, most of the management operations performed by the system on the client are done through tasks.

How to create task?

As the administrator performs certain management operations on the client, the corresponding tasks will be generated, and each operation will generate a task record. A task can be executed on one or multiple clients. In the system, such operations as software distribution, file copying, agent upgrade, power control and etc on the client will generate the corresponding task records.

For example, in the case of power control, clicking **"Apply"** button will open the following plan wizard panel:
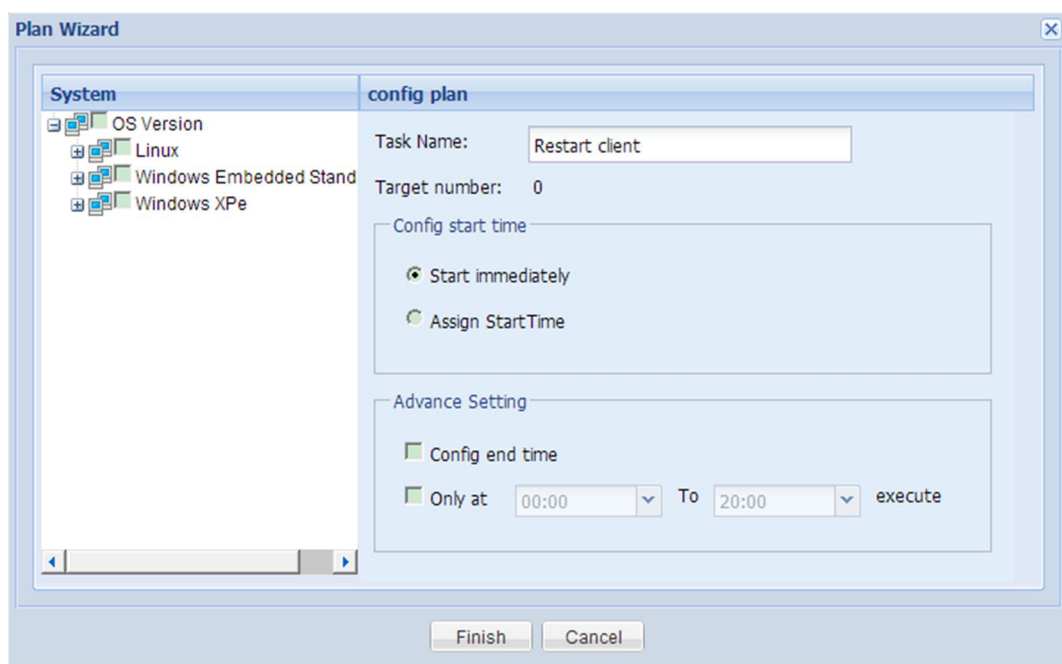
After clicking **"Finish"** button, you will find the corresponding task record in the **"Task Manager"** module on the navigation bar.
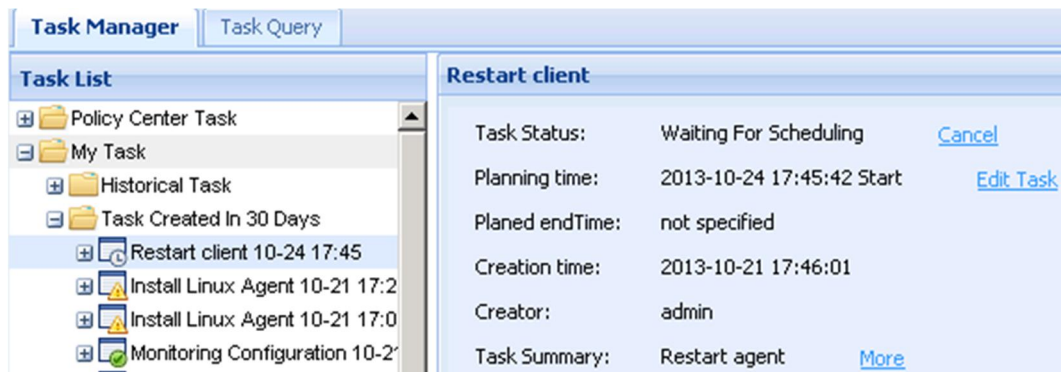
Task nodes

- Policy Center Task

  When a policy is created, a task will be created automatically and stored in the list of "**Policy Center Task**".

- My Task

  All tasks generated by the current administrator will be stored in the list of **My Task**. Tasks are divided into **"Historical Task"** and **"Task Created In 30 Days"**. When the task has been created for over 30 days, it will be automatically moved to **"Historical Task"**. Recently created tasks will be placed at the top of **"Task Created In 30 Days"** so that the administrator can check the tasks conveniently.

19.2 Task Attributes

The following attributes are provided when task is created:

Task name

Task name is the keyword used to identify the task. When the administrator creates one task, the system will automatically name the task according to task type, and the administrator can manually change the name. To allow easy identification of tasks, the task nodes in the task execution status panel will carry the scheduled start time of task.

Task target

Task target indicates the target client on which the task will be executed. There must be at least one client to create the task (except for policy center tasks). In the **"Task List"** module, each task node will generate **"All"**, **"Waiting"**, **"Executing"**, **"Success"** and **"Fail"** nodes according to execution status, as shown below:
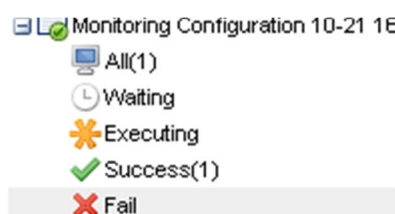
Click the node to link to the corresponding target list.
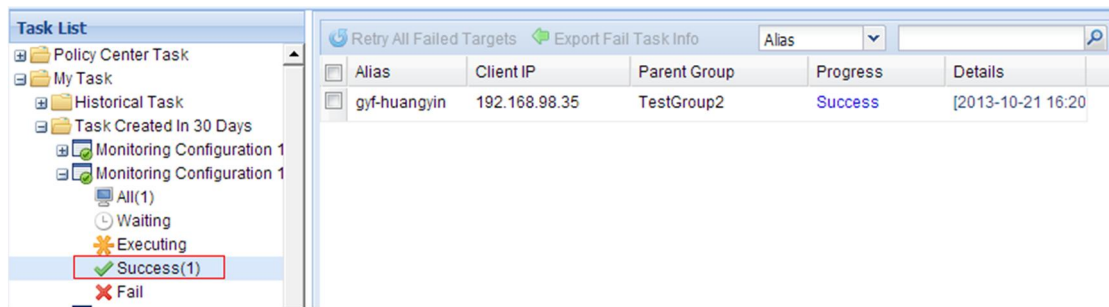
Task start time

Task start time indicates the time to start task execution. Before the arrival of start time, the task will remain in **"Waiting"** state.

- Start immediately: Execute the current task immediately.
- Assign Start Time: Specify the time to start executing the task. The time specified must be later than the present time of the server.

Task end time

Task end time indicates the time to end the task. It applies to the following two scenarios:

- The task will take a long time, such as file deployment task. If the administrator expects to distribute files to a lot of clients within two days, the actual time used may exceed two days as there may be too many clients. Configuring end time will timely end the task before the deadline, so as to ensure the normal running of business during office hours.
- The task is time-sensitive, such as sending a message or power control. If the client is offline when the task is assigned, the task will stay in "**Waiting**" state until the client is online. However, if the administrator only wishes to send a message or execute shutdown by the end of the day, this task will become meaningless beyond such time. In such a case, you can configure end time to control the end time of such tasks.

Task execution period

The task execution period will define the execution time period of the task.

For example, the administrator needs to upgrade a large number of clients after the office hours and ensure the normal running of clients during office hours. However, not all clients can be upgraded in one day. In such a case, the administrator can configure to upgrade the clients within the execution period, suspend execution beyond such period and then continue execution during the next period.

Task summary

Task summary contains descriptions about task execution, and can be viewed on the task information panel. For example, for the task of sending message, partial message contents will be displayed in **"Task Summary"**. Click **"More"** to jump to the detailed information panel of the task, as shown below:
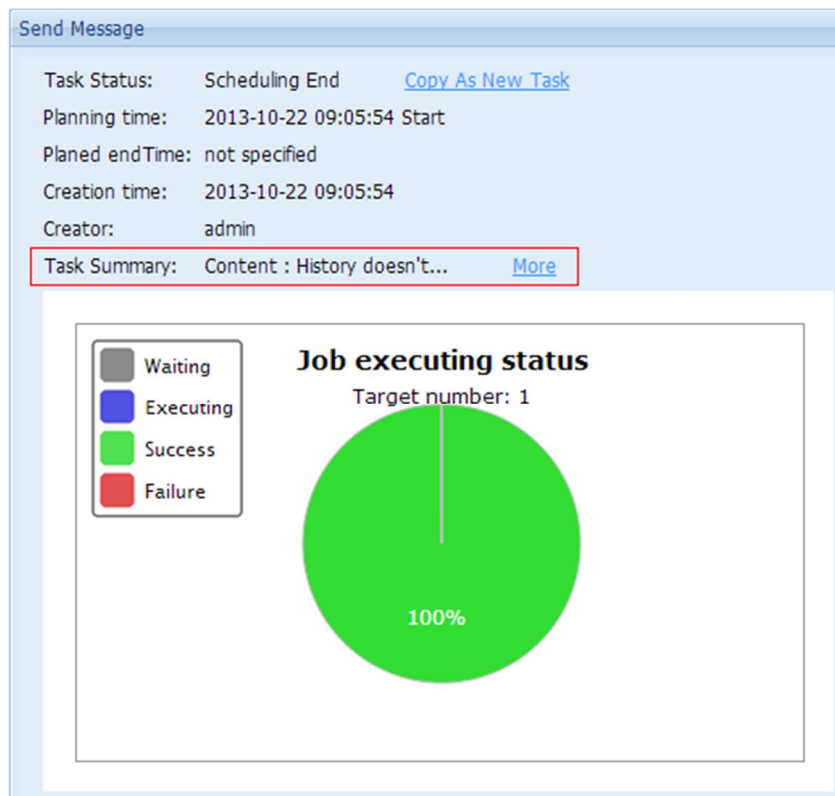
## 19.3 Task status

There are three types of status:

| Task status	Icon	Description
Waiting For Scheduling		Task will remain in this state until the arrival of start time.
Scheduling		The task is being scheduled.
Scheduling End		The task has been executed successfully on all targets.
		The task has been executed on all targets, but there are failed targets.

19.4 Copy Task

When the administrator copies a task, he creates a new task having the same contents and targets as the original task. During copying, the administrator can reschedule the time of task execution.

To copy a task, perform the following steps:

1. Right-click the task node and select "**Copy As New Task**" from the pop-up menu.
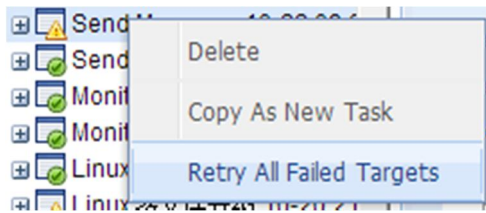
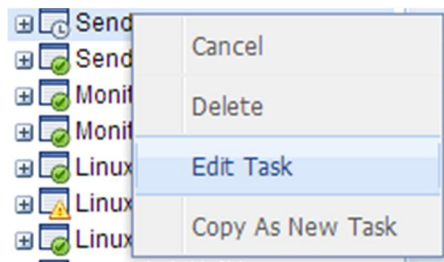2. On the plan wizard interface, reconfigure the planning time.
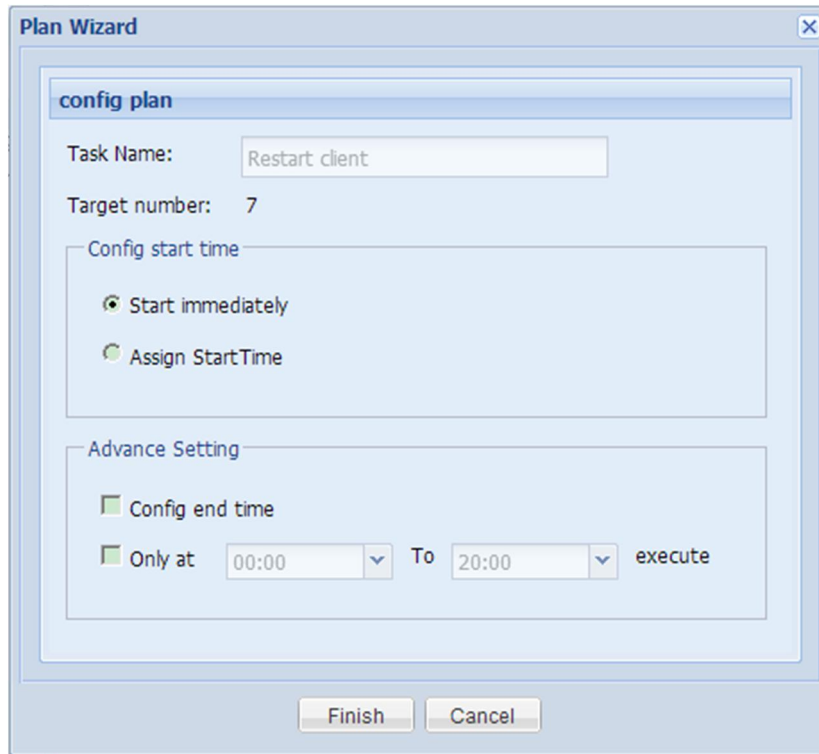

19.5 Edit Task

Note:

Editing task means to modify the planning time and task name of the task. Currently, the system can only support the editing of tasks indicating the status of **"Waiting For Scheduling"**.

Perform the following steps to edit the task:

- Right-click any task indicating the status of "**Waiting for Scheduling**" and select "**Edit Task**". On the plan wizard interface, reconfigure the planning time.

- Click the task node and, on the right side task information panel, click the "**Edit Task**" link. On the plan wizard interface, reconfigure the planning time.
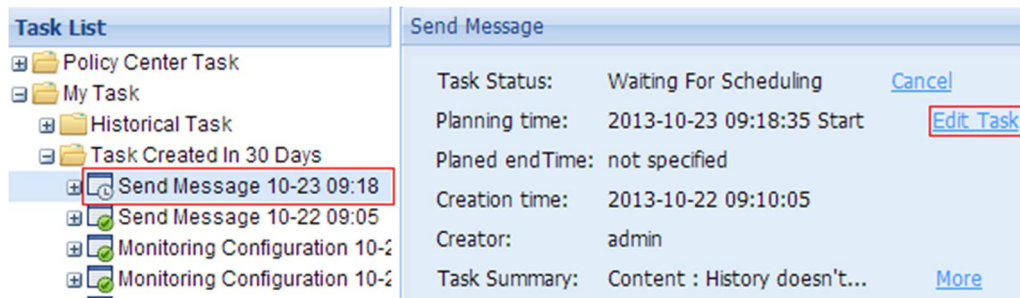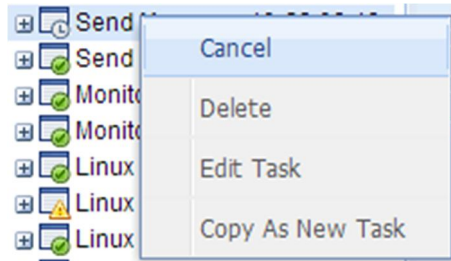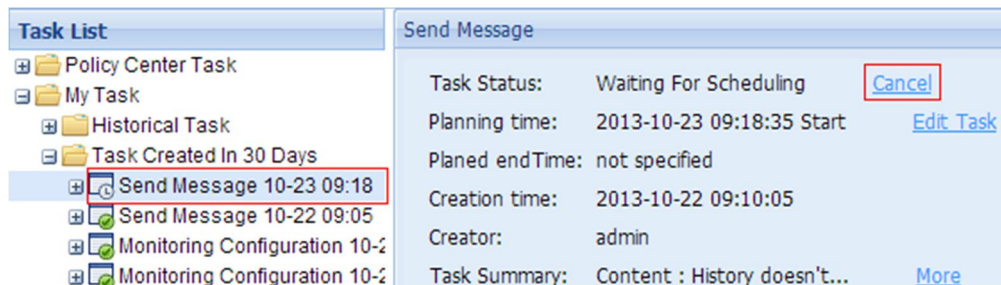
19.6 Cancel Task

In the event of any misoperation by the administrator, or if the administrator wishes to cancel the task created, he can use the **"Cancel"** feature provided by the system.

Cancel task

- Right-click any task indicating the status of "**Waiting For Scheduling**" or "**Scheduling**" and select "**Cancel**" from the pop-up menu.
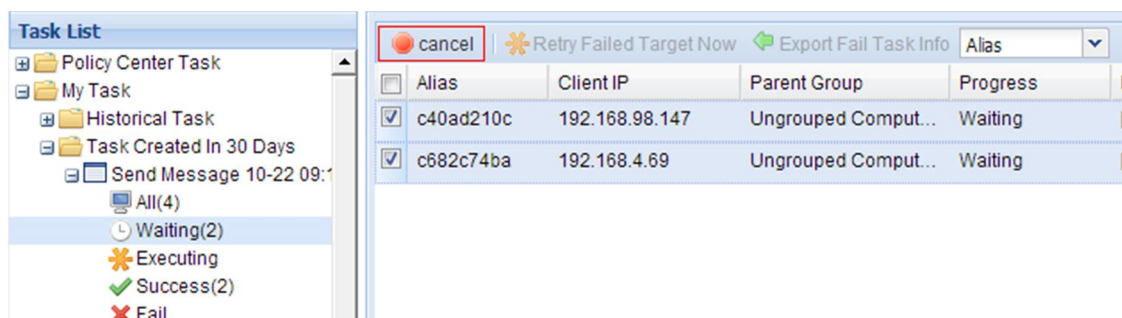

- Click the task node and, on the right side task information panel, click the "**Cancel**" link.

Cancel task execution

When the task is being scheduled and not all targets have been executed, you can cancel any **"Waiting"** target in the target list.


Note:

- Cancelling task is actually cancelling task execution on all targets.

- Only tasks indicating the status of "**Waiting For Scheduling**" or "**Scheduling**" can be cancelled.

- Only targets in "**Waiting**" and "**Executing**" state can be cancelled. Cancelled targets will indicate the state of "**Failure**".

- When a task indicates the status of "**Scheduling**", certain targets may have succeeded or failed, and the cancel operation won't apply to these targets. The execution result of all cancelled targets will indicate "**Failure**".

- When the administrator deletes the task, the task indicating the status of "**Waiting For Scheduling**" or "**Scheduling**" will be cancelled first before deletion.

19.7 Troubleshooting and Retry

The targets to which a task is assigned may encounter failure in task execution. The system allows troubleshooting and retry of failed targets.

Troubleshooting

Click the task node and, on the right side task information panel, you will see the execution status of the current task, including the execution status of target clients. Click the corresponding block on the pie chart to enter the corresponding target list.
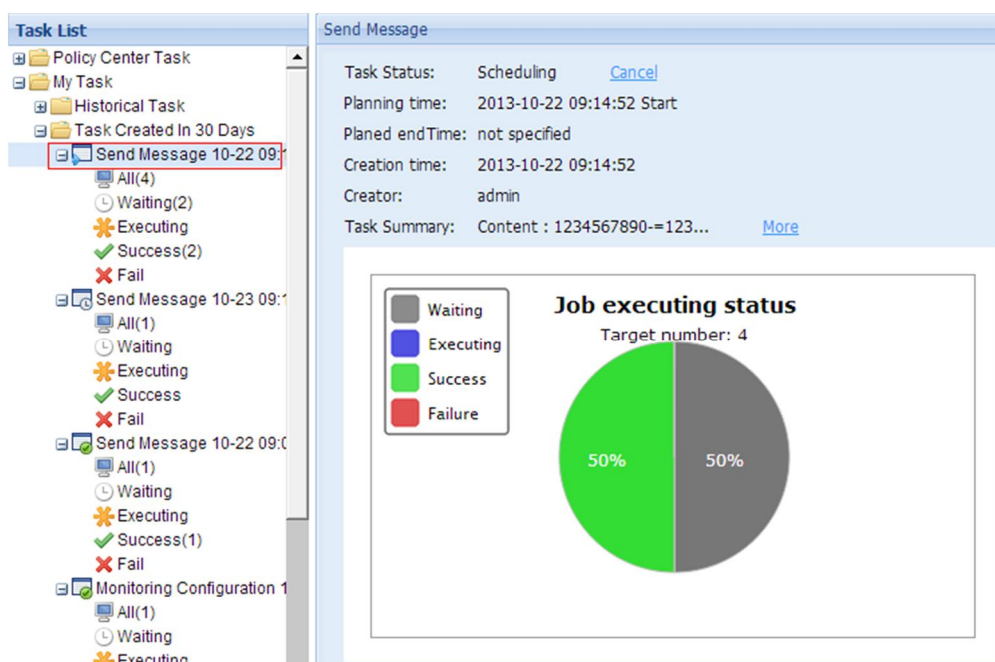
When the target client remains in **"Waiting"** state for an excessively long time, you can view the error report in the **"Details"** column of target list.

When the target client fails in task execution, you can also view the details.

Retry

Those failed targets can be retried.

Select failed targets and click **"Retry All Failed Targets"**.

If task execution has been completed, you can reschedule all failed targets. As shown below, right-click the finished task and select **"Retry All Failed Targets"**, and then reconfigure in the pop-up plan wizard configuration window.

Note:

Only those failed targets will be retried without creating a new task, and the former task information will be overwritten.
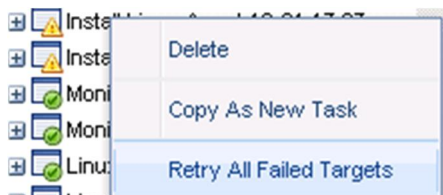
Export fail task info

If a task involves failed targets, you can export failed targets into a file.

1. On the navigation bar, click "**Task Manager**" to enter the task management interface and expand the task folder.

2. Select all targets and click "**Export Fail Task Info**" on the right side panel and save the file following the instructions in the wizard.

19.8 Task Query

On the navigation bar, click **"Task Manager > Task Query"** to enter the task query interface.

Enter search conditions and click **"Search"** to get matching tasks. If no search condition is entered, all tasks will be searched.
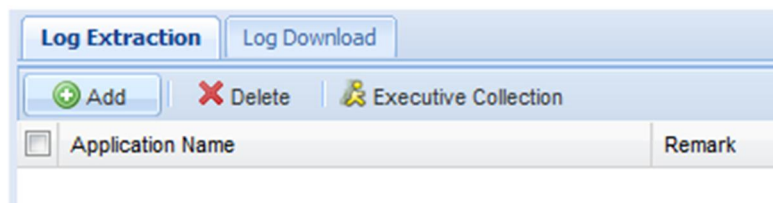
20 Log Collection

20.1 Log Extraction

Operation steps

1. On the navigation bar, click "**General > Log Collection**" to enter the log extraction interface.
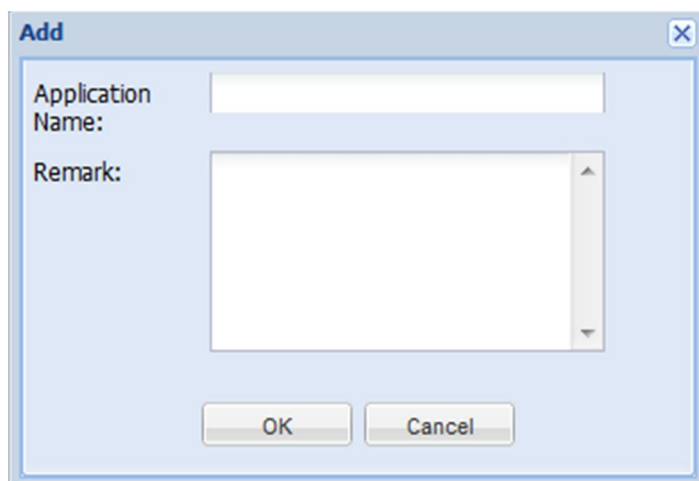

Add application

Note

If the application has been added, there is no need to add again. Please click "**Executive Collection**" directly.

2. Click "**Add**" button and enter the application name (i.e., colleting TC logs, type in **TC**) for collecting log on TC in the "**Add**" dialog box. Click "**OK"** to save the configuration information.

Collect log file

3. Select the client or client group for log extraction and select the application entry added, and then click "**Executive Collection**" button.
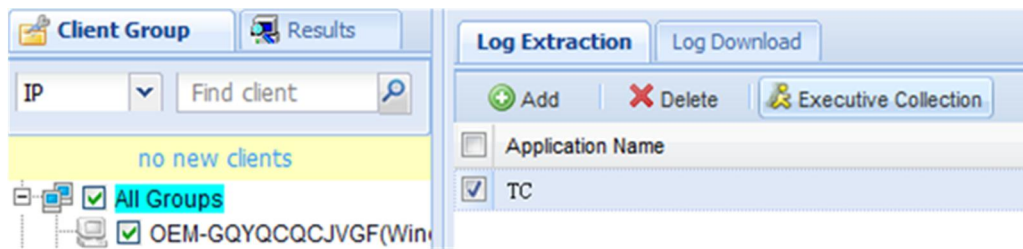
4. Configure the Plan Wizard and then click "Finish" (please refer to the section of "**Configure Plan Wizard**").

Note:

> After completing task plan configuration, you will be able to view the progress of log extraction in the "**Task Manager**" module. For offline clients, the log will be extracted after it goes online.
>
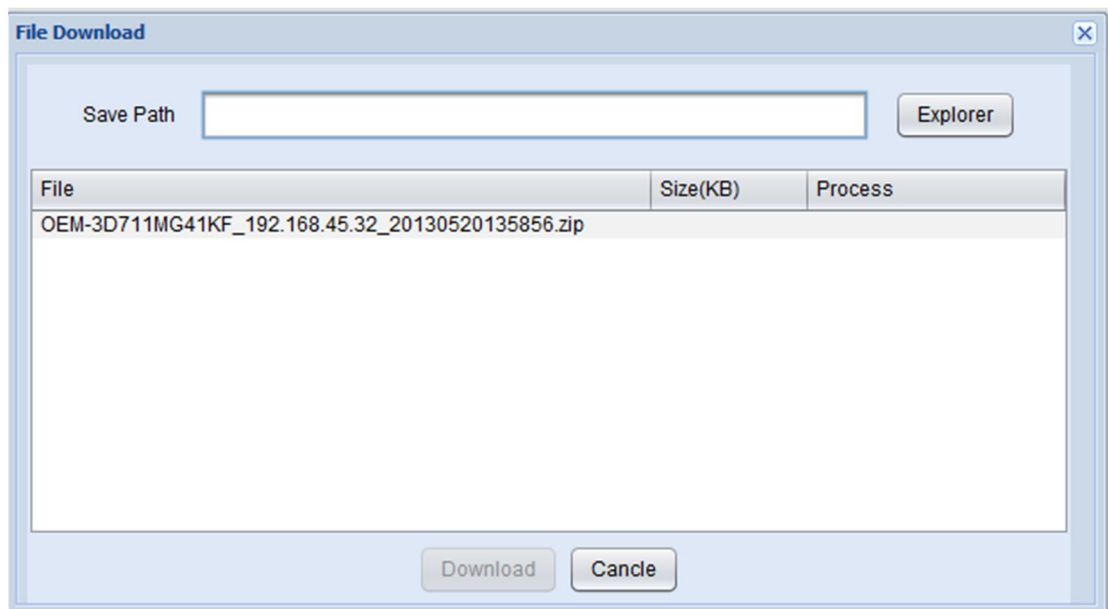> After extraction is completed, you can search the log files extracted in the "**Log Download**" list.

20.2 Log Download

1. On the navigation bar, click "**General > Log Collection**" and click the "**Log Download**" tab.
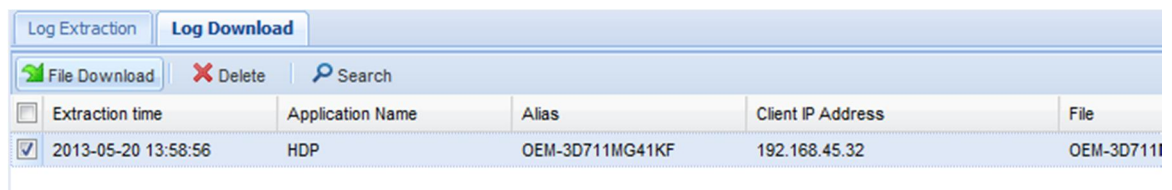
2. Select the log file(s) to be downloaded and click "**File Download**".
3. Select the "**Save Path**" for log file(s) and click "**Download**" button to start downloading.
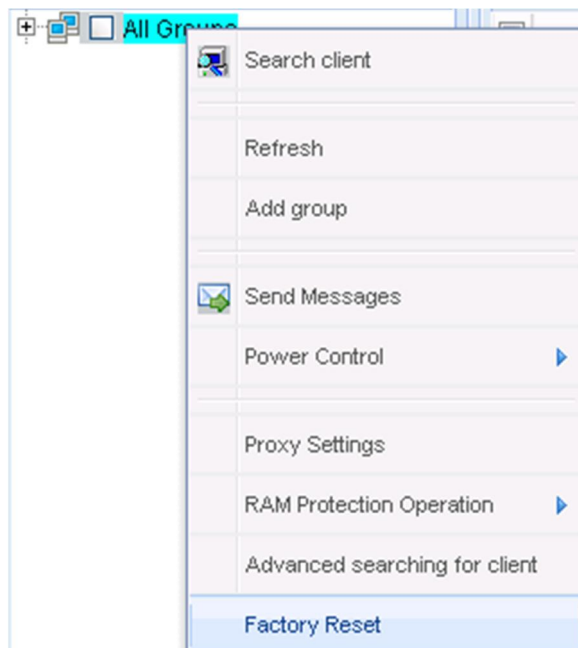
# 21 Linux Agent Factory Reset

Only Linux agent support factory reset。

1. Right-click a client/group in the left pane and select "**Factory Reset**" from the context menu；

2. Click"**Yes**" to confirm factory reset；click"**No**" to cancel；

3. Select the appropriate OS version on the "**Plan Wizard**" interface, configure the task plan and then click "**Finish**".

22 RAM Protection Management

RAM Protection Management can open or close operation for protection of terminal memory. Only windows terminal supports RAM Protection Management.
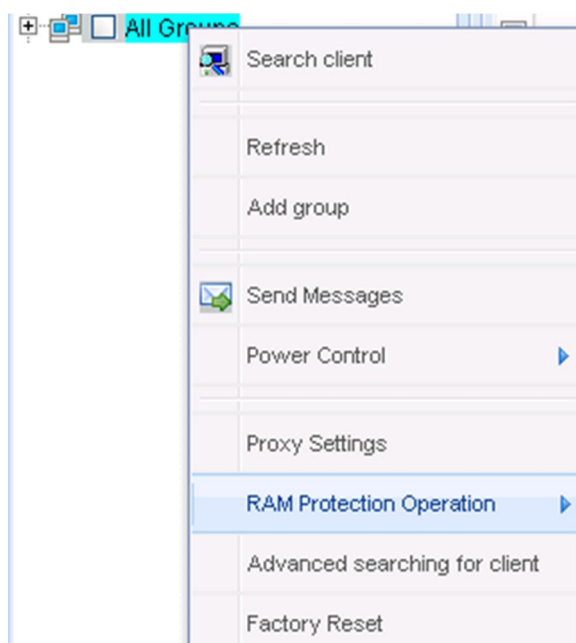
22.1 Enable the Protection

1. Right-click a client/group in the left pane and select "**RAM Protection Operation**" from the context menu；

2. Click"**Enable the Protection**"；

3. Jump out"**The function would be activated after the client restart(Only for Windows Embedded Version)**" Tips, Click"**OK**"；

4. Select the appropriate OS version on the "**Plan Wizard**" interface, configure the task plan and then click "**Finish**".

22.2 Disable the Protection

1. Right-click a client/group in the left pane and select "**RAM Protection Operation**" from the

context menu；

2. Click"**Disable the Protection**"；

3. Jump out"**The function would be activated after the client restart(Only for Windows Embedded Version)**"Tips, Click"**OK**"；

4. Select the appropriate OS version on the "**Plan Wizard**" interface, configure the task plan and then click "**Finish**".

22.3 Commit

1. Right-click a client/group in the left pane and select "**RAM Protection Operation**" from the context menu；

2. Click"**Commit**"；

3. Jump out"**The function would be activated after the client restart(Only for Windows Embedded Version)**"Tips, Click"**OK**"；

4. Select the appropriate OS version on the "**Plan Wizard**" interface, configure the task plan and then click "**Finish**".

22.4 Clear Instructions

1. Right-click a client/group in the left pane and select "**RAM Protection Operation**" from the context menu；

2. Click"**Clear Instructions**"；

3. Jump out"**The function would be activated after the client restart(Only for Windows Embedded Version)**"Tips, Click"**OK**"；

4. Select the appropriate OS version on the "**Plan Wizard**" interface, configure the task plan and then click "**Finish**".

22.5 Change Password

This password is password of local client terminal management tool

1. Right-click a client/group in the left pane and select "**RAM Protection Operation**" from the context menu；

2. Click"**Change Password**"；

3. After putting in the correct password then click "**OK**"；
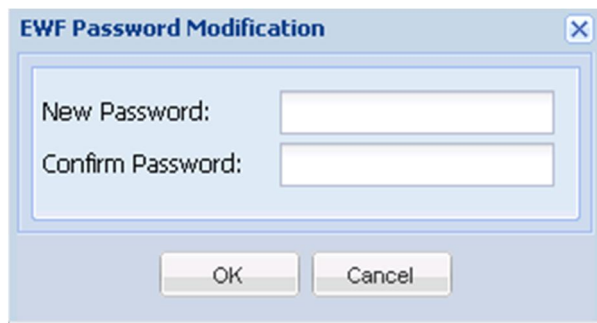
EWF Password Modification

New Password:

Confirm Password:

OK   Cancel

4. Select the appropriate OS version on the "**Plan Wizard**" interface, configure the task plan and then click "**Finish**".
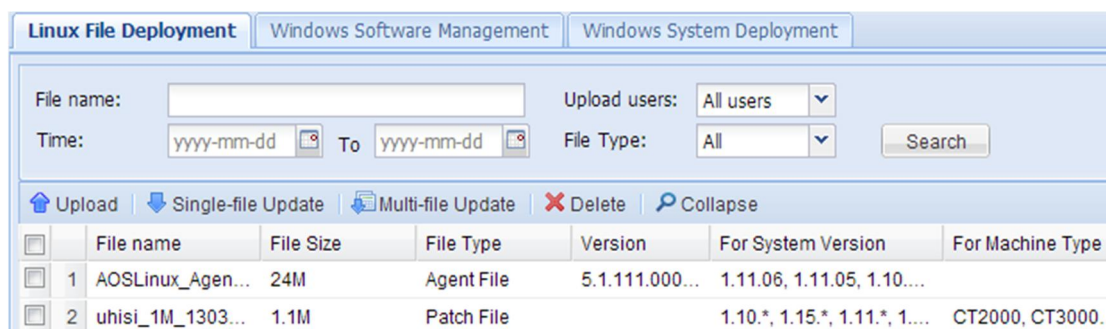
23 Common Operations

23.1 Search Record

Most of the functional modules provide a feature of record searching related to the existing module. The search panel is collapsed by default. Click **"Search"** button to expand the search panel. Enter the search conditions and click **"Search"** button to get the search results.

For example, in **"Linux File Deployment"**:

23.2 Delete Record

To delete a record, you must first select the record to be deleted and then click the **"Delete"** button on the interface. In the pop-up dialog box, click **"Yes"** or **"No"** to proceed.

23.3 Configure Plan Wizard

In CCCM, most of the management operations are done by means of tasks. During task creation, all tasks must be configured through the same Plan Wizard. The plan wizard for sending message is shown below.
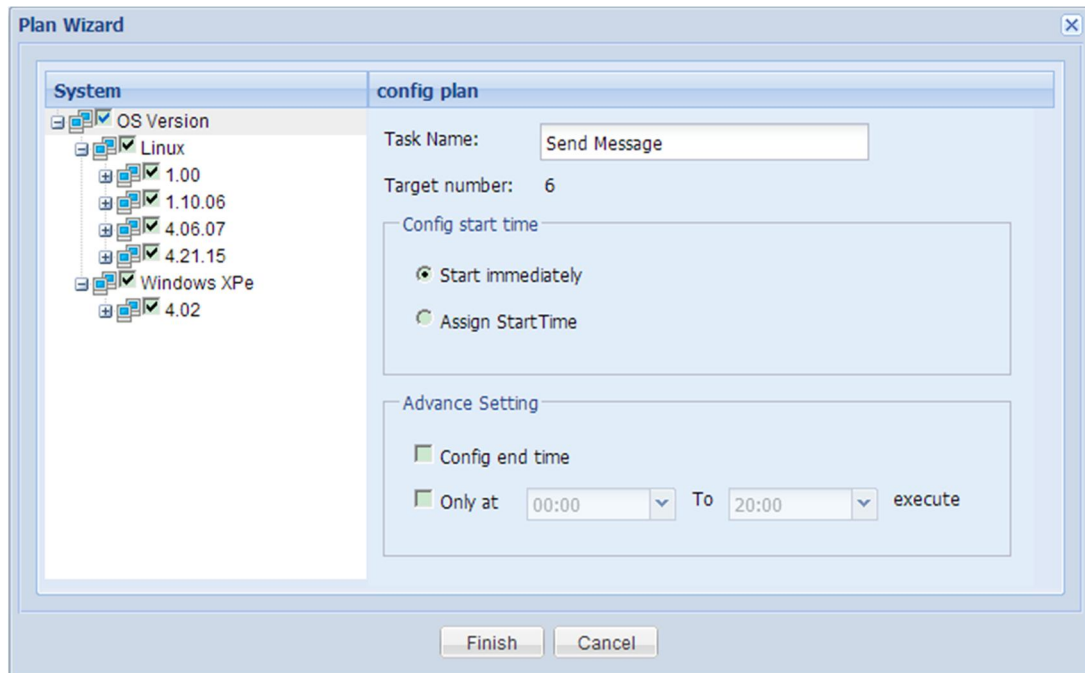
Required operation: select OS version

In the left pane of Plan Wizard, you need to select the appropriate OS version for the task being created. By default, no OS version is selected. For example: execute the task on Windows clients only.

Operational operation: configure task plan

- Task Name

  The task name has been given in the Plan Wizard. You can use the default name or enter a new name.

- Target number

  The number of targets to execute the task being created (i.e., the number of clients).

- Start time

  By default, the task created will be executed immediately. If needed, you can specify the start time. Please refer to "19.2Task Attributes" for details.

- Advanced Setting

  By default, the advanced settings are not required during task creation. If needed, you can configure the advanced settings by referring to "19.2Task Attributes".
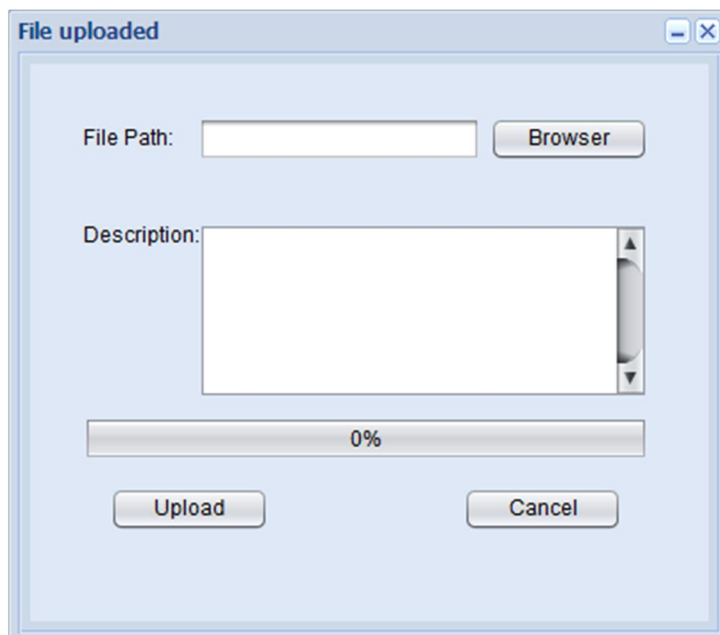
23.4 Upload the Upgrade File

Click the upload button to open the file upload interface.

If Java Runtime Environment (JRE) is not installed or if the JRE version is too low, the browser may give you the following prompt. Please refer to 27.1Install JRE.
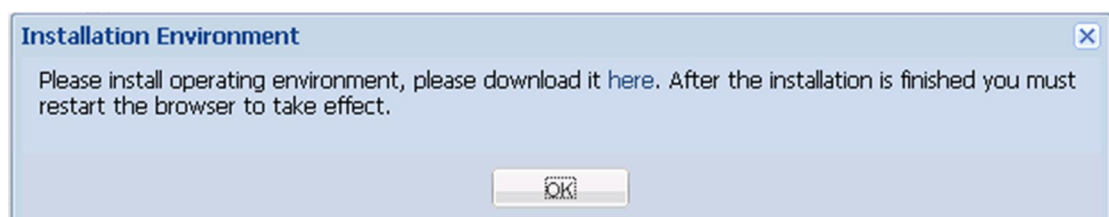
Click **"Browse"** to select the file or folder to be uploaded. Enter file description (optional) and then click **"Upload"**.
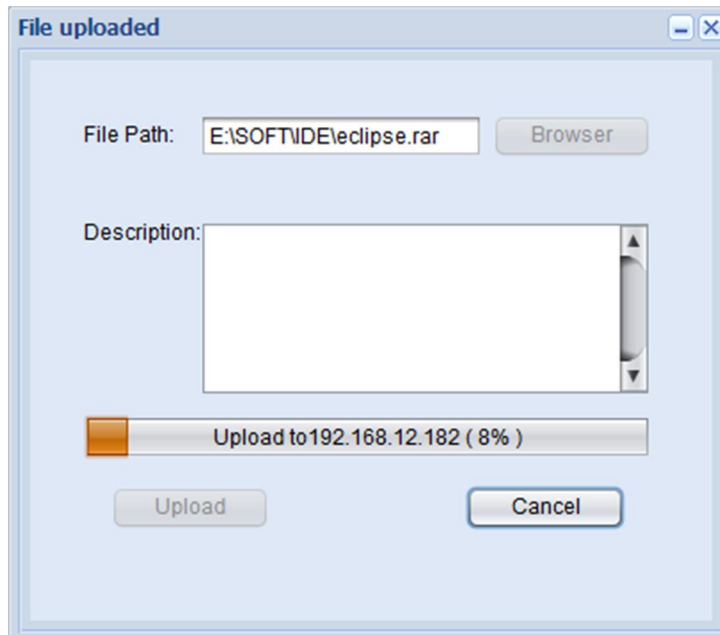

Upon successful upload, exit the upload window, and the uploaded file will appear in the file list.

Cancel uploading

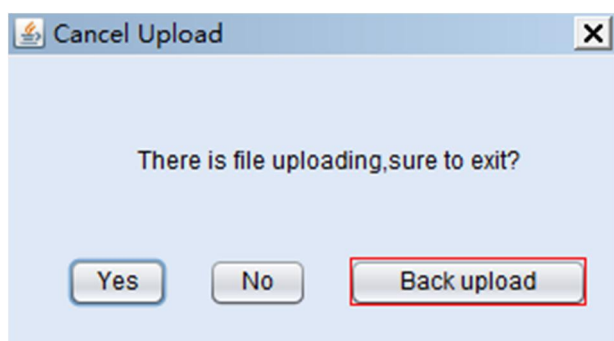You can cancel file uploading during file uploading by clicking the **"Cancel"** button:

Click **"Yes"** to cancel uploading or **"No"** to continue uploading.
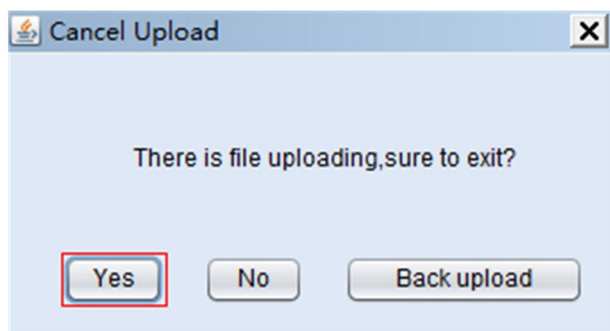
Background uploading

During file uploading, the upload window can be minimized to realize background upload, or you can click **"Cancel"** and then select background uploading.
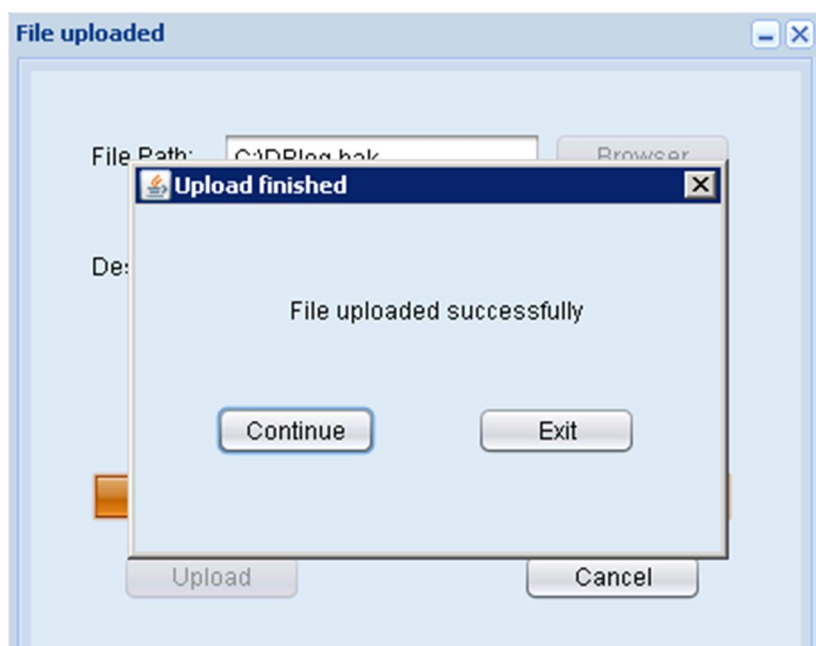

After minimizing the upload window, click the maximize button to restore the window.

Upload Multiple Files

Click **'Continue'** button to upload more files on the upload successful interface, or click **'Exit'** to stop uploading.

24 Server Configuration Tool

On the host computer running CCCM server, go to **"Start -> All Programs -> Centerm -> Server Configuration Tool"** to open the configuration interface.

Server

Change CCCM Language

Select the target language and click **"OK"** to restart service according to the prompting message.

Enable distributed deployment

Select **"Open Distributed"** and enter the IP address of load-balancing server. Click **"OK"** to restart service according to the prompting message.

> When the server is being used, do not change the communication port and management port.

System service

In **"System Service"**, you can start, stop and restart system services.
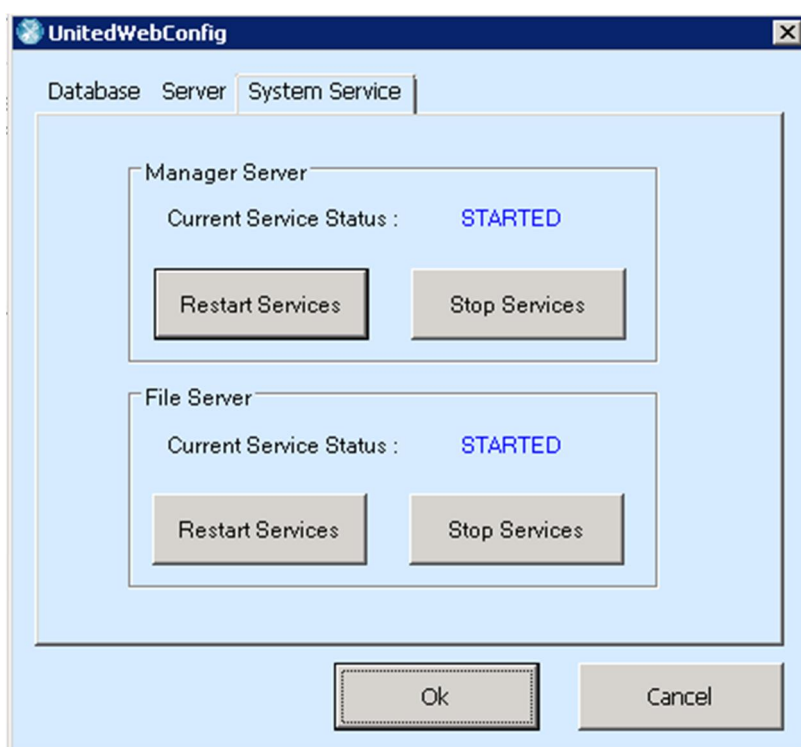
Database

In **"Database"**, you can view and update the database connection information. If you want to enable SQL Server mirroring, please configure the IP address of Mirror Server.

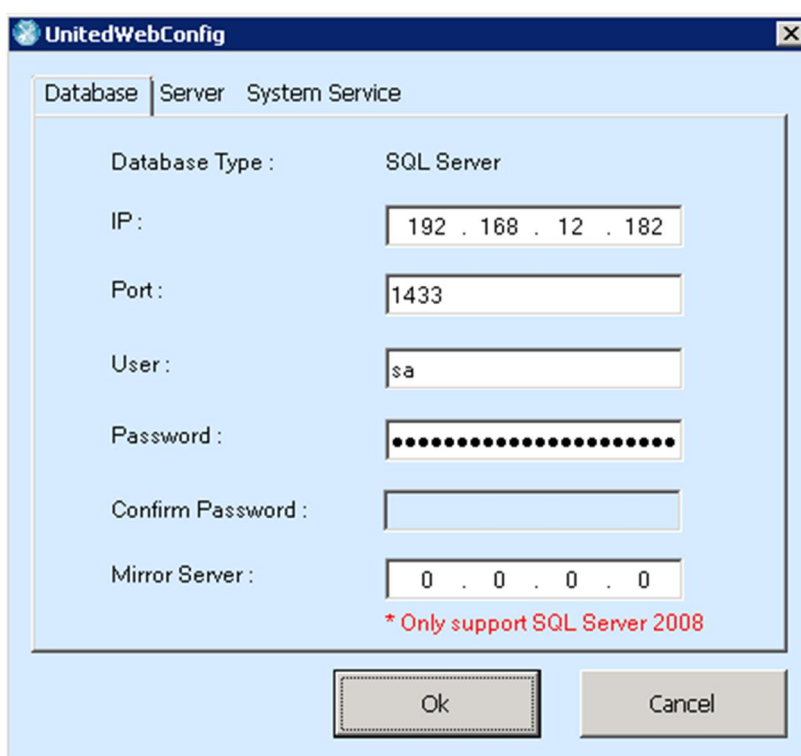# 25 System Hotkeys for Linux Clients

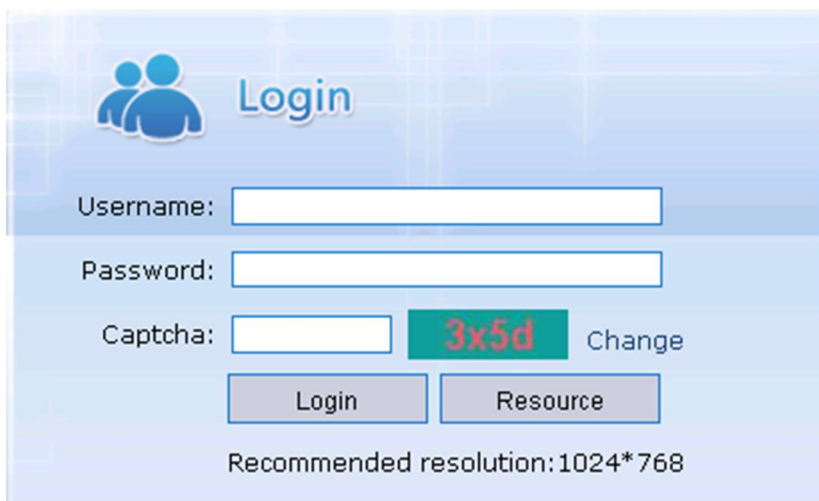| Hotkey	Function
Ctrl+Alt+A	To view version information
Ctrl+Alt+S	To restore to the default display parameters (not applicable to all-in-one computers)
Ctrl+Alt+Del	To lock the screen
Ctrl+Alt+U	To restore the system to default settings (supported by non-protection clients)
Shift+F2	To save system configuration
Alt+Tab	To switch between windows on the desktop
Ctrl+Alt+C	To call the Control Center
Ctrl+Shift+F3 (dual-monitor support)	To switch the display mode in the sequence of: VGA->DVI->TWIN->VGA
Ctrl+F1	To view the Help file (no this shortcut for the English edition)
Ctrl	To enter extended BIOS (press CTRL after the short beep at boot-up)

26 Default System Accounts for Windows Clients

Model	Version	Version Range	Account (Username/Password)
GI945	XPE Chinese	3.32.03-3.32.10	Administrator: Centerm User: User
GI945	XPE Chinese	3.32.10 and later versions	Administrator: Centerm123! User: User123!
GI945	XPE English	3.33-3.33.10	Administrator: Centerm User: User
GI945	XPE English	3.33.10 and later versions	Administrator: Centerm123! User: User123!
GA690-2(X2)/ HA690-2(2)	XPE Chinese	3.36.01, 3.36.02, 3.32.06	Administrator: Centerm User: User
EI945-3(X2)	WES7 Chinese	3.37.01	Admin: Centerm User: User
EI945-3(X2)	WES7 Chinese	3.37.02 and later versions	Admin: Centerm123! User: User123!
CT5000/CT6000	WES7 Chinese / English	3.38.01 and later versions	Admin: Centerm123! User: User123!

27 Installation and Configuration of Third-Party Products

27.1 Install JRE

Installation steps

1. On CCCM login interface, click "**Resource**" button to access the resource download page.


2. Click the "**Download**" hyperlink on the right side of "**JRE installation package**" and save the file following the instructions in the wizard.

3. Run the installation file after completing download and complete JRE installation following

the instructions in the setup wizard.

4. Restart the browser and log in CCCM system.

When you use such features as file uploading and remote monitoring which require to run Applet for the first time, the following warning message will pop up. Check "**Always trust content from this publisher**" and then click "**Run**".
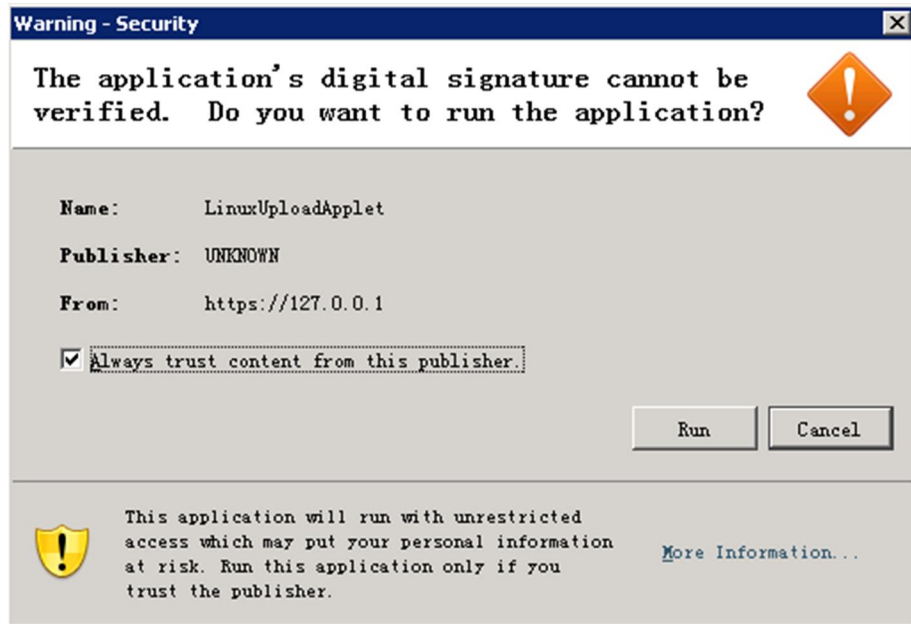
27.2 Configure DHCP Option

Client automatic registration only takes effect on the network where IP address is acquired via DHCP. To use this feature, we must set Option 232 on the DHCP server.

Option description

DHCP option code: 232

DHCP option type: string

DHCP option information: CENTERM_CDMS_SERVER : server address : communication port

- Option code of **232** cannot be changed; option type is character string (text).
- Option prefix of `CENTERM_CDMS_SERVER` is fixed and cannot be changed.
- When the deployment mode is simple mode and ordinary mode, the server address shall be the IP address of management server.
- When the deployment mode is cluster mode, the server address shall be the IP address of load-balancing server.
- The communication port shall be the same as the communication port set during management server installation (default: 8081).
- Option prefix, server address and communication port shall be divided by colon (":").

27.2.1 DHCP server for Windows server

You can install DHCP sever on the host computer running Windows server operating system and set DHCP options (Windows Server 2003/2008 supported).

Taking Windows Server 2008 as the example: perform the following steps to install and configure DHCP server.

Install Windows DHCP server

1. Go to "**Start -> All Programs -> Administrative Tools**" and select **"Server Manager"**.

2. Select "**Roles**" and click "**Add Roles**".
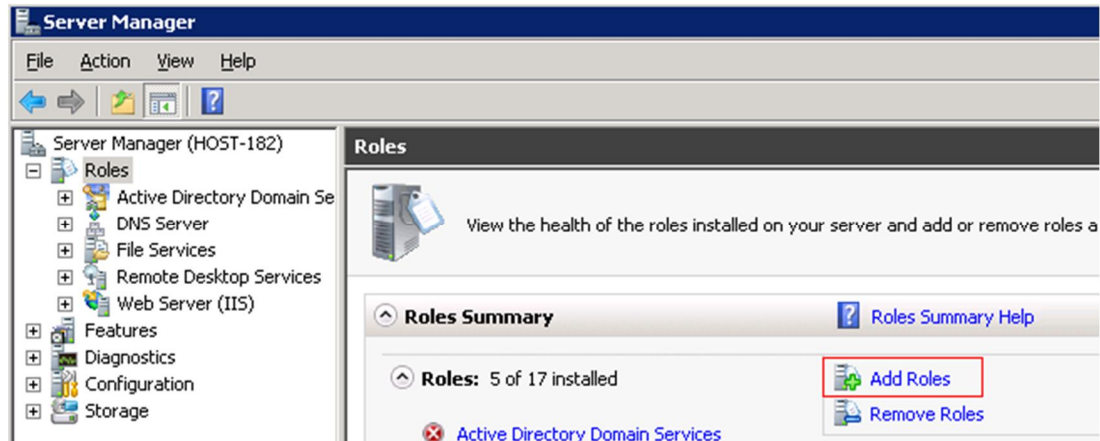
3. Select "**Server Roles**", check "**DHCP Server**" and click "**Next**".
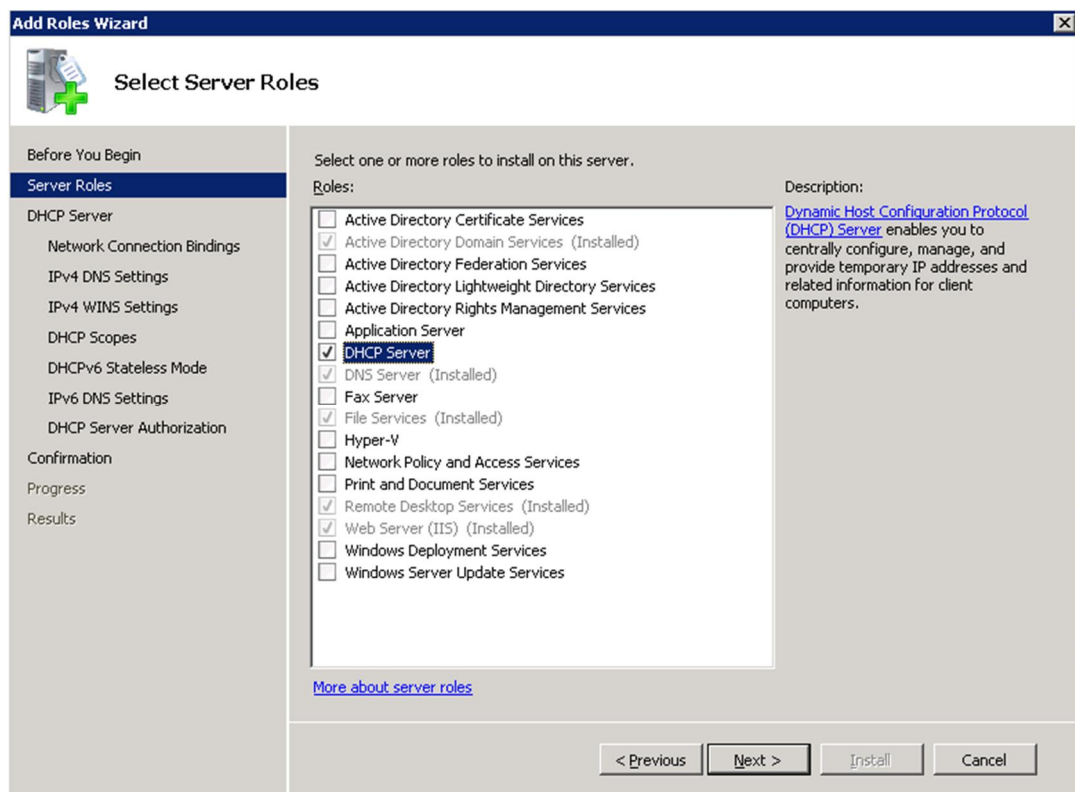
4. Under "**DHCP Server**", select "**IPv4 DNS Settings**" and enter DNS information or keep the default settings.

5. Under "**DHCP Server**", select "**DHCP Scopes**". Click "**Add**", enter scope information and click "**OK**".
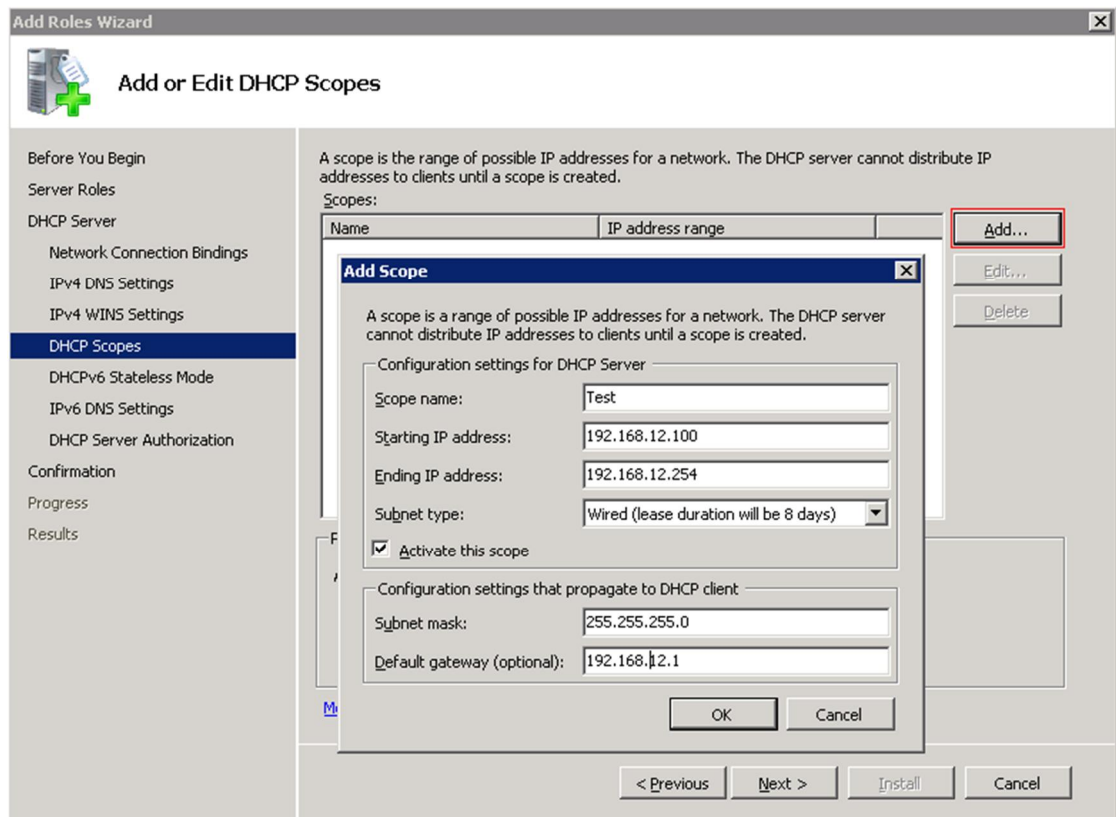
6. Under "**DHCP Server**", select "**DHCPv6 Stateless Mode**" and then select "**Enable DHCPv6 stateless mode for this server**".

7. Select "**Confirmation**", check the configuration information and then click "**Install**".
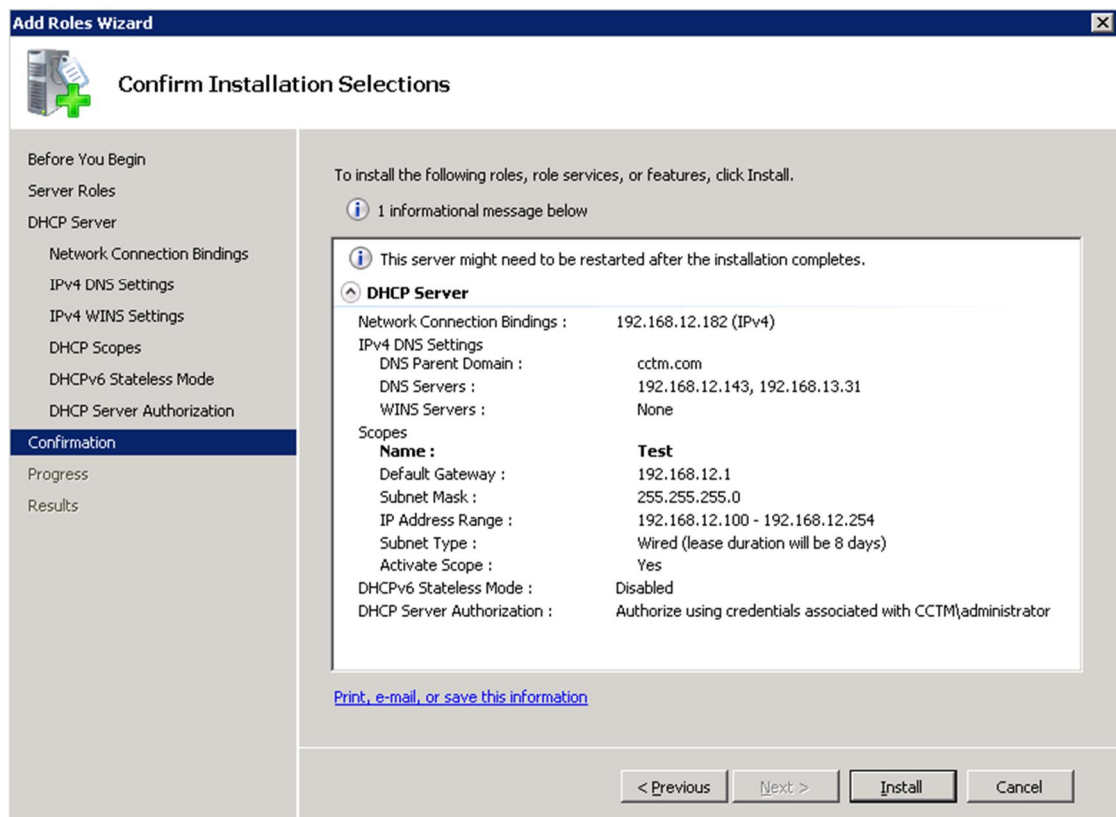
8. Close the window after successful installation.

Configure Windows DHCP server

9. Go to "**Start > All Programs > Administrative Tools > DHCP**" to open DHCP configuration interface.

10. Right-click the host and select "**Authorize**" from the context menu.

    Caution:

    To authorize DHCP server, "Active Directory Domain Services" must be installed first.
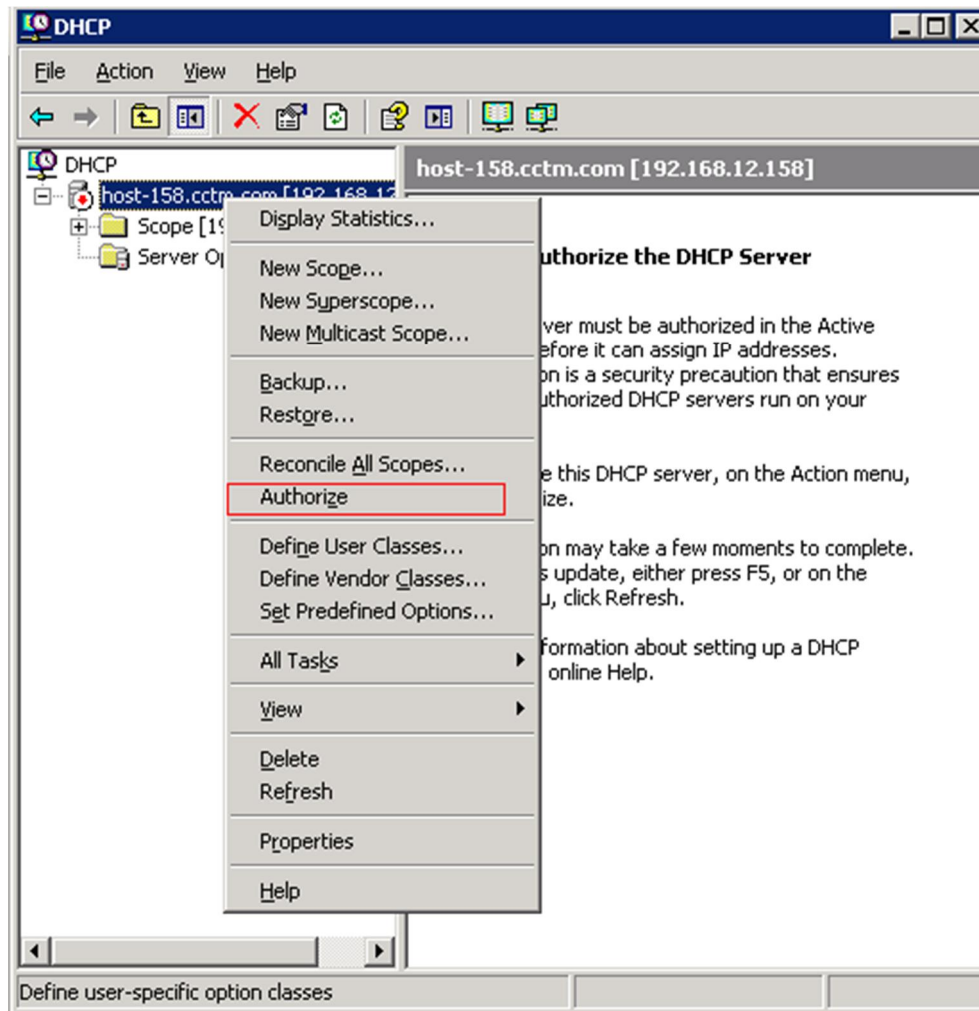
11. Reopen DHCP console and verify that the host has been successfully authorized. Right-click the server and select **"Set Predefined Options"**.
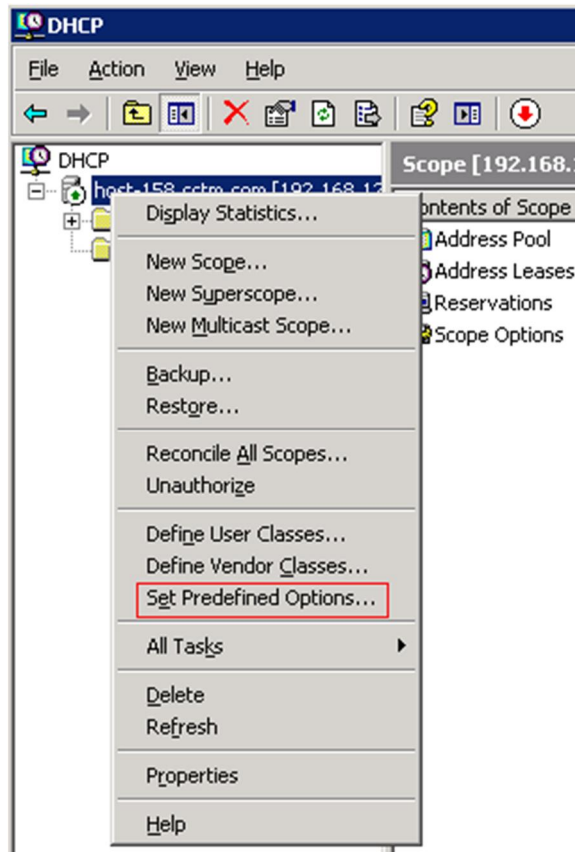
12. Click "**Add**", enter option information (as shown below) and then click "**OK**".

```
Name: CENTERM_CDMS_SERVER
Data type: String
Code: 232
```


13. To add DHCP option, click "**OK**".
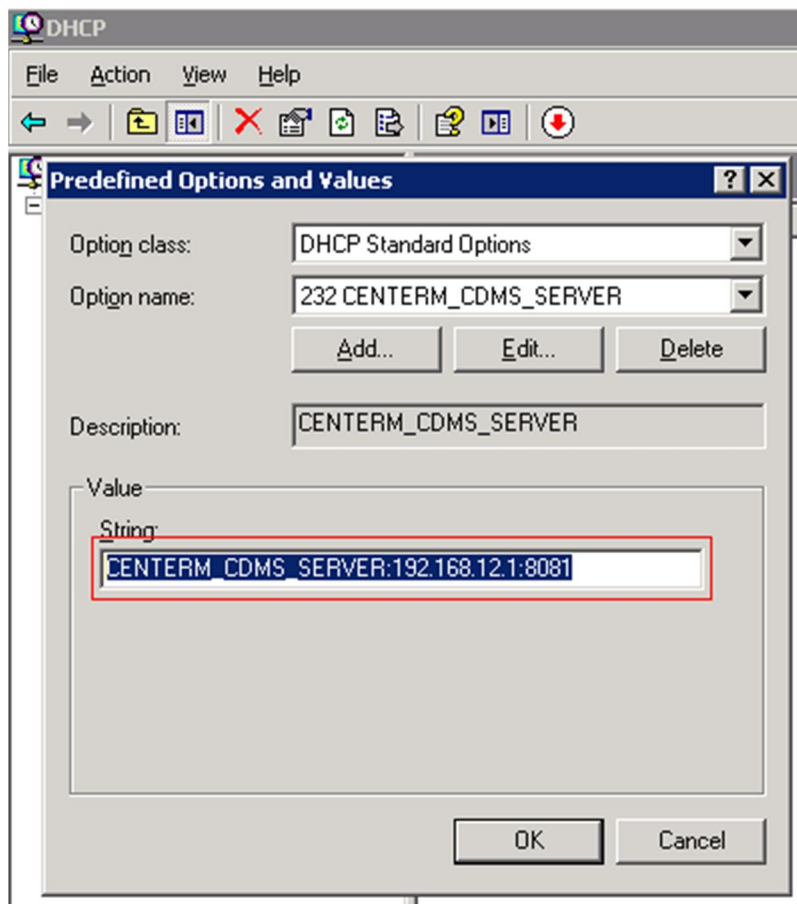
14. Right-click "**Scope Options**" and select "**Configure Options**".
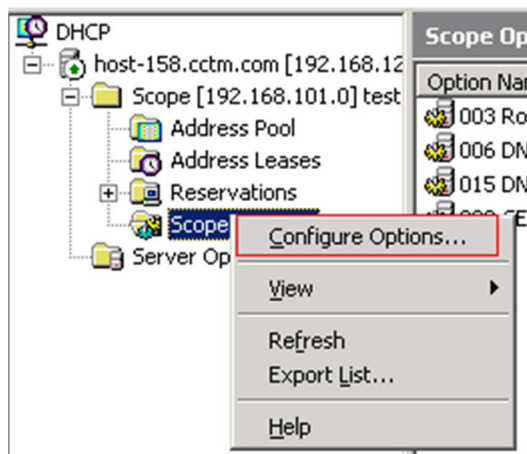
15. In the "**General**" tab of "**Server Options**", select Option 232 and click "**Apply**".
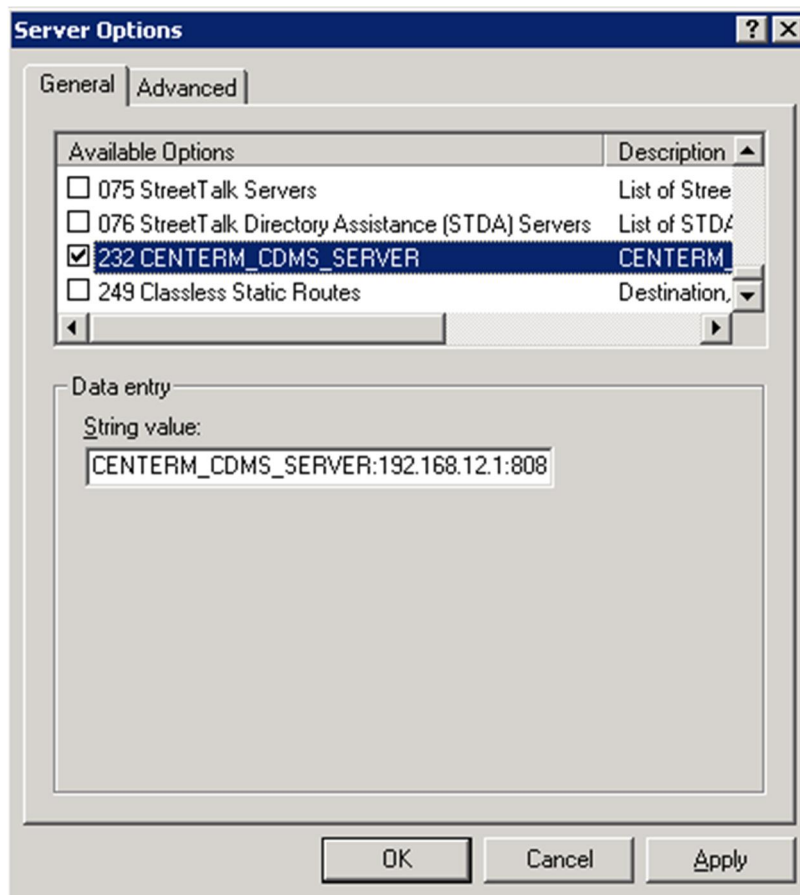
16. The option has been successfully configured.
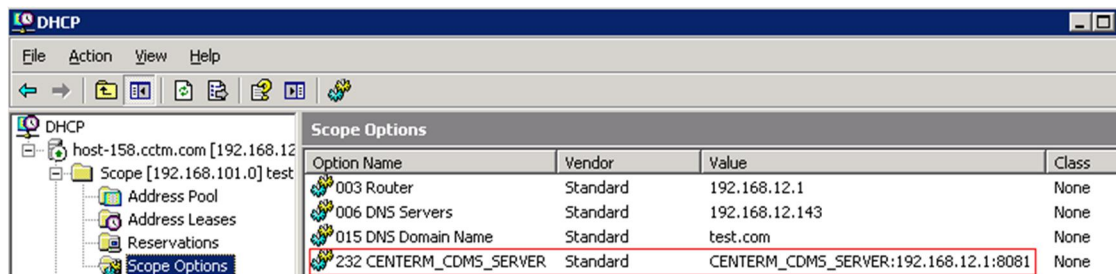
27.2.2 DHCP server for Linux Server
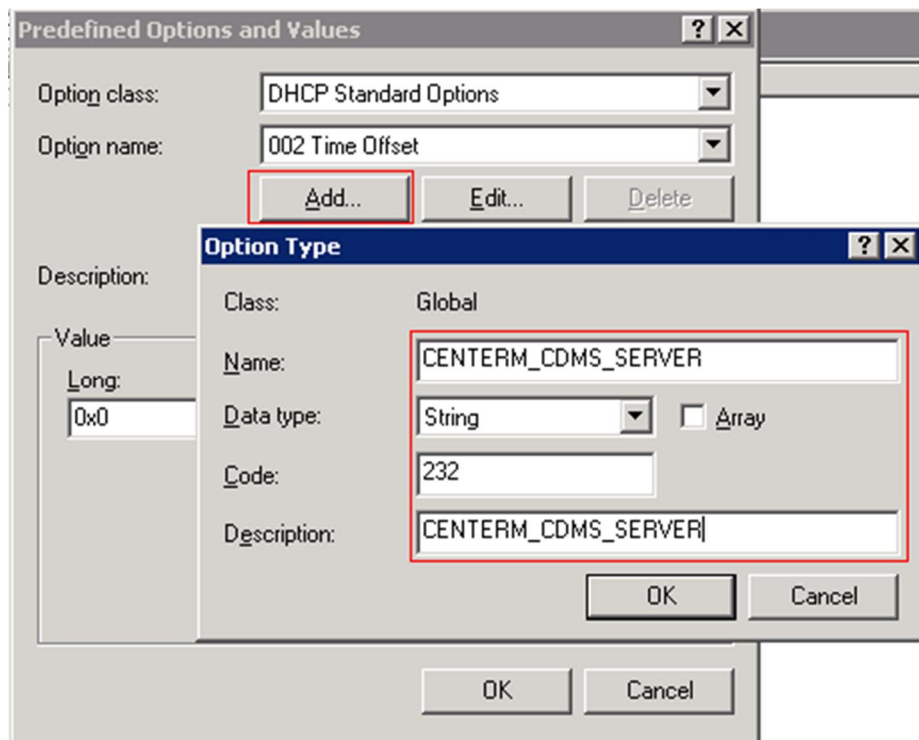
You can install DHCP sever on the host computer running Linux server operating system and set DHCP options.

Taking Ubuntu 9.10 as the example: perform the following steps to install and configure DHCP server.

1. Install DHCP server

```
sudo apt-get install dhcp3-server
```

2. Configure DHCP network adapter

```
emacs /etc/default/isc-dhcp-server
```

#Change to network adapter corresponding to the server, such as eth0, eth1, etc.

```
INTERFACES="eth0"
```

3. Back up the current configuration

```
sudo cp /etc/dhcp/dhcpd.conf /etc/dhcp3/dhcpd.conf.bak
```

4. Edit the current configuration file   /etc/dhcp/dhcpd.conf

```
sudo vi /etc/dhcp/dhcpd.conf

ddns-update-style none;

option domain-name "tagpt.mtn";

default-lease-time 14400;

# minimum least time is 14400 seconds = 4 hours

max-lease-time 36000;

# maximum lease time is 36000 seconds = 10 hours

subnet 192.168.2.0 netmask 255.255.255.0 {

# Range of IP addresses

range 192.168.2.77 192.168.2.240;

option subnet-mask 255.255.255.0;

# Subnet mask is 255.255.255.0

option routers 192.168.2.10;

# Default gateway is 192.168.2.10

option broadcast-address 192.168.2.255;

# Broadcast address is 192.168.2.255

}

authoritative

# Option

option cdms-server code 232 = text ;

option cdms-server  "CENTERM_CDMS_SERVER:192.168.12.2:8081";
```

5. Restart DHCP server

```
sudo /etc/init.d/dhcp3-server restart
```

A prompt message of OK means successful restart. If it failed, reinitialize the network and repeat the above steps.

27.2.3 DHCP server on the switch

You can configure DHCP option on the DHCP server of switch, which must support DHCP options and comply with RFC2131.

Taking Huawei S5700 switch as the example: perform the following steps to configure DHCP option.

Enable DHCP service

```
 [Quidway]dhcp enable
```

Configure DHCP address pool

```
[Quidway]ip dhcp pool A
```

Configure the assignable address range of the address pool

```
[Quidway-ip-pool-a]network 192.168.1.0 mask 255.255.255.0
```

Configure the least duration of addresses in the address pool

```
[Quidway-ip-pool-a]lease day 8
```

Configure default gateway for DHCP client

```
[Quidway-ip-pool-a] gateway-list 192.168.1.1
```

Configure DHCP option 232

```
[Quidway-ip-pool-a] option 232 ascii
CENTERM_CDMS_SERVER:192.168.1.1:8081
```

Check DHCP service and DHCP option to verify the configuration

```
[Quidway-ip-pool-a]display current-configuration
```

28 **Reset admin Password**

If the admin`s password is lost, it is necessary to reset to initial password, and then reset a new password.

Default password:

| Software Version	administrator	Initial Password	Encrypted Password
3.6.01	admin	admin	`21232f297a57a5a743894a0e4a801fc3`
3.6.02	admin	Admin123!@#	`A8D51FC6A058BFEACB77818D42D420AC` `1BF31529393A784EC60F7C2443047462`
5.0.000.000~	admin	Admin123!@#	`A8D51FC6A058BFEACB77818D42D420AC` `1BF31529393A784EC60F7C2443047462`

SQL Server

1. Click **Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio** , log in Microsoft SQL Server Management Studio。

2. Click **New Query** to open a new query window, choose correct *Encryted Password*. Execute below script.

```
use cdms_terminal
update sys_user set password='Encrypted Password' where name='admin'
```

Perform success as shown in the figure below:
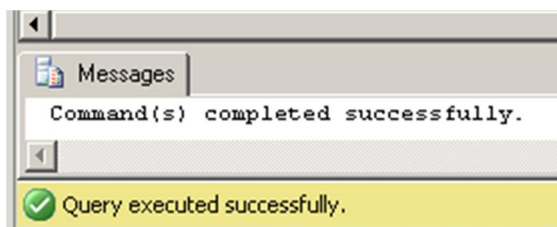
MySQL

1. Click **Start** > **Run** , type in `cmd` , open a command window.

2. Run MySQL program. You should use real program path and password(*mypassword*) for root user.

```
cd c:\Program Files\MySQL\MySQL Server 5.5\bin
```

```
mysql.exe -uroot –pmypassword
```

3. Execute below script, using correct **Encryted Password**.

```
use cdms_terminal
```

```
update sys_user set password=' Encrypted Password' where name='admin'
```

29 Update the Online User Manual

Copy the user manual to CCCM server installation directory:

%CCCM%\Cinfin\runtime\deploy\webapps\download\.

The file name fixed as follows:

- User manual in Chinese : *CN_User_Manual.pdf*
- User manual in English : *EN_User_Manual.pdf*