SSL M7.6.6R1 User Manual



Dec 2018

Table of Contents

Table of Contents....1
Declaration....7
Preface....8
About This Manual....8
Document Conventions....10
Graphic Interface Conventions....10
Symbol Conventions....11
CLI Conventions....11
Technical Support....12
Acknowledgments....12
Chapter 1 Knowing Your Sangfor Device....13
Operating Environment....13
Product Appearance....13
Connecting Sangfor Device....14
Chapter 2 Initial Login to Admin Console....17
Logging in to Admin Console....17
Modifying Administrator Password....18
Chapter 3 System and Network Settings....20
Viewing Status....21
Viewing SSL VPN Status....21
Viewing Online Users....23
Certificate Status....25
Viewing Alarm Logs....25
Viewing Remote Application....27
System Settings....31
Configuring System Related Settings....31
Configuring License of Device and Function Modules....31
Modifying System Date and Time....33
Configuring Console Options....34
Configuring External Report Center....34
Generating Certificate for Sangfor Device....35
Configuring SMTP Server....38
Configuring Syslog Server....39
Logs Output....40
Configuring SNMP....40
Network Settings....42
Device Deployment....42
Setting Multiline Options....47
Configuring Route....51
Configuring Host Mapping Rule (HOSTS)....55
Configuring IP Assignment Options (DHCP)....56

Configuring Local Subnet....59
Schedules....62
Administrator....66
Adding Administrator Group....66
Adding Administrator....68
SSL VPN Options....70
General Settings....70
Configuring User Login Options....70
Configuring Client Related Options....74
Configuring Virtual IP Pool....77
Configuring Local DNS Server....78
Configuring SSO Options....81
Configuring Resource Options....85
Web App Resource Options....85
TCP App Resource Options....89
Background Knowledge: What is Smart Recursion?....91
L3VPN Resource Options....93
Other Resource Options....94
Network Optimization Related Settings....96
Application Access Optimization....96
Data Transfer Optimization....97
Webpage Access Optimization....100
Web Cache....103
User Logging in....104
Configuring Login Policy....104
Configuring Login Page....106
Uploading Icon to Device....110
Clustering....112
Terminology....112
Main Features of Cluster....112
Deploying Clustered Sangfor Devices....115
Deploying Clustered Device in Single-Arm Mode....115
Deploying Clustered Device in Gateway Mode....116
Deploying Clustered Device with Multiple Lines....118
Viewing Clustered Node Status....122
Viewing Cluster Online Users....122
Distributed Nodes....124
Distributed Deployment....124
Viewing Status of Distributed Nodes....125
Chapter 4 SSL VPN....126
SSL VPN Users....126
Adding User Group....127
Adding User....133
Searching for Users....140

Managing Hardware IDs....141
Importing User to Device....143
Importing Users from File....144
Importing Users from LDAP Server....146
Moving Users to Another Group....148
Exporting Users....149
Associating Roles with User....150
Configuring SSO User Account....151
Generating Multiple Certificates for Users....152
Configuring Multiple Users Assigned To CA....153
Creating Multiple USB Keys for Users....154
Viewing Associated Resources of User....156
Resources....157
Adding/Editing Resource Group....158
Background Knowledge: Load-Balanced Resource Access....160
Adding/Editing Web Application....161
Adding/Editing TCP Application....167
Adding/Editing L3VPN....173
Adding/Editing Remote Application....178
More Operations....182
Exporting Resources....182
Importing Resources....183
Sorting Resources....183
Roles....186
Adding Role....187
Getting Privilege Report....189
Authentication Options....192
Primary Authentication Methods....193
Local Password Based Authentication....193
LDAP Authentication....194
Configuring LDAP Server....194
RADIUS Authentication....202
Configuring RADIUS Server....202
Certificate/USB Key Based Authentication....205
Configuring Local CA....206
Configuring External CA....208
Configuring USB Key Model....213
Client-Side Domain SSO....214
Secondary Authentication Methods....216
SMS Authentication....216
Using Built-in SMS Module to Send SMS Message....218
Using External SMS Module to Send SMS Message....220
Using SMS Gateway of ISP to Send SMS Message....223
Using Webservice Based SMS Platform to Send SMS Message....223

Using Jasson MAS to Send SMS Message....224
Hardware ID Based Authentication....225
Dynamic Token Based Authentication....226
Other Authentication Options....226
Priority of LDAP and RADIUS Servers....226
Password Security Options....227
Anonymous Login....229
Policy Sets....231
Adding Policy Set....232
Remote Servers....242
Adding Remote Application Server....244
Adding Remote Storage Server....247
EMM....252
MDM Policy....252
Adding Android MDM Policy....252
Adding iOS MDM Policy....255
Mobile Devices....257
Published Apps....259
App Wrapping....263
Endpoint Security....268
Security Rules....268
Predefining Basic Rule....269
Predefining Combined Rule....278
Configuring Security Rule....280
Policies....281
Adding User-Level Policy....283
Adding Role-level Policy....285
Configuring Advanced Policy Settings....289
Built-in Rules Update....290
Chapter 5 Firewall....293
Defining Firewall Service....293
Defining IP Group....294
Configuring Filter Rule....295
Rules on Access to Local Device....296
Rules on Access among Sangfor Device's Interfaces....296
Configuring NAT Rule....297
Configuring SNAT Rule....297
Configuring DNAT Rule....298
Configuring IP/MAC Binding....299
Configuring HTTP Port....301
Defining URL Group....301
Defining WAN Service....303
Configuring Access Right of Local Users....304
Real-time Monitoring....308

Viewing Real-time Traffic....308
Viewing URL Access Logs....308
Configuring Anti-DoS....309
Chapter 6 System Maintenance....311
System Update....311
System Upgrade....311
Proxy Options....311
Viewing Logs....312
Viewing System Logs....312
Viewing Operating Logs....313
Backing Up/Restoring Configurations....314
Restarting/Shutting Down Device or Services....316
System Automatic Update....318
Chapter 7 Scenarios....320
Device Deployment....320
Deploying Device in Gateway Mode with Single Line....320
Deploying Device in Gateway Mode with Multiple Lines....322
Deploying Device in Single-Arm Mode With Single Line....326
Deploying Device in Single-Arm Mode With Multiple Lines....328
Configuring System Route....331
Deploying Clustered Sangfor Devices....332
Deploying Clustered Device in Gateway Mode....332
Deploying Clustered Device in Single-Arm Mode....333
Deploying Clustered Device with Multiple Lines....334
Gateway-mode Sangfor Device with Multiple Lines....335
Single-Arm Sangfor Device with Multiple Lines....335
Adding User....336
Adding User Logging in with Local Password....336
Adding User Logging in with Certificate....336
Configuring VPN Resource....338
Adding Web Application....338
Masquerading Resource Address....341
Adding FileShare Type of Web Application....342
Adding Web Application Enabling Site Mapping....345
Configuring TCP Application....347
Configuring URL Access Control Feature....349
Adding L3VPN Application....350
Adding Remote Application....352
Configuring Authentication with External CA....361
Using External CA Root Certificate to Generate Device Certificate....361
Mapping User to Local Group Based on External Certificate....365
Configuring Resource Enabling SSO....367
Adding TCP Application Enabling SSO....367
Adding Remote Application Enabling SSO....371

Mobile Users Accessing SSL VPN....388
Application for IOS MDM Certificate....394
EMM Configuration Case....397
Configuring Firewall Rule....399
Configuring LAN<->VPN Filter Rules....399
Adding SNAT Rule....402
Adding DNAT Rule....404
Typical Case Study....406
Required Environment....406
Configuring Sangfor Device....406
Appendix A: End Users Accessing SSL VPN....413
Required Environment....413
Configuring Browser and Accessing SSL VPN....413
Configuring Browser....413
Using Account to Log In to SSL VPN....417
Using USB Key to Log In to SSL VPN....419
Using VPN Client to Log In SSL VPN....420
Appendix B: Sangfor Firmware Updater 6.0....426
Updating Your Sangfor Device....426
Appendix C: Restore Network Configuration and Password using USB drive....433
Restore network configuration by using USB....433
Check the ETH port configuration by using USB....433
Restore Web UI admin login password by using USB....434
Precautions....434

Declaration

Copyright © 2016 Sangfor Inc. All rights reserved.

No part of the contents of this document shall be extracted, reproduced or transmitted in any form or by any means without prior written permission of SANGFOR.

SINFOR, SANGFOR and the Sangfor logo  are the trademarks or registered trademarks of Sangfor Inc. All other trademarks used or mentioned herein belong to their respective owners.

This manual shall only be used as usage guide, and no statement, information, or suggestion in it shall be considered as implied or express warranty of any kind, unless otherwise stated. This manual is subject to change without notice. To obtain the latest version of this manual, please contact the Customer Service of Sangfor.

Preface

About This Manual

SSL VPN M7.6.6R1 EN user manual includes the following chapters:

Chapter	Describe…
Chapter 1 Knowing Your Sangfor Device	The product appearance, function features and performance parameters of SSL VPN M7.6.6R1 EN, wiring and cautions before installation.
Chapter 2 Initial Login to Admin Console	How administrator logs in to SSL VPN M7.6.6R1 EN administrator console for the first time and change initial administrator password.
Chapter 3 System and Network Settings	How administrator configures each function module. The settings include system and network related settings, global settings of SSL VPN, as well as other system objects such as schedule and administrator.
Chapter 4 SSL VPN	How administrator configures SSL VPN related setting, including users, resources, roles, user authentication methods, policy sets, remote servers, endpoint security.
Chapter 5 Firewall	How administrator configures firewall related settings.
Chapter 6 System Maintenance	Maintenance options of this SSL VPN hardware device.
Chapter 7 Scenarios	How administrator configures Sangfor device in different deployment mode, and how to configure the device according to different requirements.
Appendix A: End Users Accessing SSL VPN	How end users configure browser and log in to SSL VPN.

Appendix B: Sangfor Firmware Updater 6.0	How administrator uses Sangfor Firmware Updater 6.0 to update the current Sangfor device.

Document Conventions

Graphic Interface Conventions

This manual uses the following typographical conventions for special terms and instructions:

Convention	Meaning	Example
boldface	Page title, parameter, menu/submenu, button, key press, link, other highlighted keyword or item	Page/tab name example: Navigate to **System** > **Administrator** to enter the **Administrator Management** page. Parameter example: **IP Address:** Specifies the IP address that you want to reserve for certain computer Menus/submenus example: The basic (SSL VPN related) settings are under **System** > **SSL VPN Options > General**. Button example: Click the **Save** button to save the settings. Key press example: Press **Enter** key to enter the administrator console of the Sangfor device. Link example: Once the certificate signing request is generated, click the **Download** link to download the request. Highlighted keyword/item example: The user name and password are **Admin** by default.
italics	Directory, URL	Enter the following address in the IE address bar: *http://10.254.254.254:1000*
>	Multilevel menu and submenu	Navigate to **System** > **Network Interface** to configure the network interfaces.
“ ”	Prompt	The browser may pop up the prompt “Install ActiveX control”.

Symbol Conventions

This manual also adopts the following symbols to indicate the parts which need special attention to be paid during the operation:

Convention	Meaning	Description
	Caution	Indicates actions that could cause setting error, loss of data or damage to the device
	Warning	Indicates actions that could cause injury to human body
	Note	Indicates helpful suggestion or supplementary information

CLI Conventions

Command syntax on Command Line Interface (CLI) applies the following conventions:

- Content in brackets ([ ]) is optional
- Content in {} is necessary
- If there is more than one option, use vertical bar (|) to separate each option, for example,

  ip wccp *60* **redirect** { *in* | *out* }
- CLI command appears in bold, for example:

  configure terminal
- Variables appear in italic, for example:

  interface *e0/1*

Technical Support

For technical support, please contact us through the following:

- **Website:** *http://www.sangfor.com*
- **Community:** *http://community.sangfor.com*
- **Email:** *tech.support@sangfor.com*
- **Tel:** + 60 12711 7129(7511)

Acknowledgments

Thanks for using our product and user manual. If you have any suggestion about our product or user manual, please provide feedback to us through phone call or email. Your suggestion will be much appreciated.

Chapter 1 Knowing Your Sangfor Device

This chapter introduces the Sangfor device and the way of connecting Sangfor device. After proper hardware installation, you can configure and debug the system.

Operating Environment

- Voltage input: 110V/230V (AC, alternating current)
- Temperature: 0-45°C
- Humidity: 5%-90%

To ensure endurance and stability of the Sangfor device, please ensure the following:

- The power supply is well grounded
- Dustproof measures are taken
- Working environment is well ventilated
- Indoor temperature is kept stable

This product conforms to the requirements on environment protection. The placement, usage and discard of the product should comply with the relevant national laws and regulations of the country where it is applied.

Product Appearance



Above is the front panel of a SSL VPN hardware device (M5100). The interfaces from left to right are described in the table followed:

Interface	Description
CONSOLE	Network interface used for high availability (HA) feature or used by device supplier to debug system.
USB	Standard USB port, connecting to peripheral device
ETH0	LAN interface, connecting to the LAN network segment; orange LED on the left

	side indicates link status, while green LED on the right side indicates data flow.
ETH1	DMZ interface, connecting to the DMZ network segment; orange LED on the left side indicates link status, while green LED on right side indicates data flow.
ETH2	WAN1 interface, connecting to the first Internet line; orange LED on the left side indicates link status, while green LED on the right side indicates data flow.
ETH3	WAN2 interface, connecting to the second Internet line; orange LED on the left side indicates link status, while green LED on the right side indicates data flow.
POWER	Power LED
ALARM	Alarm LED



The picture above (M5100) is just for reference. The actual product you purchased and received may vary.

Connecting Sangfor Device

1. Deploy the Sangfor device in your network. Sangfor device can be deployed in either **Single-arm** mode or **Gateway** mode. For details, please refer to the Device Deployment section in Chapter 3.
2. Plug the power cable into the power interface on the rear panel of the device. Attach and turn on power supply, and then watch the LEDs on the front panel of the Sangfor device.

   When the device starts up, **ALARM** LED will turn on and keep on for 1 to 2 minutes, then turn off; **POWER** LED (in green) will turn on; **ETH2/3** and **ETH0** connection status LEDs (in orange) will also turn on.

   After successful bootup, **POWER** LED (in green), **ETH2/3** and **ETH0** connection status LEDs (in orange) will stay on. If data are being transferred through a port, the data flow LED (in green, beside connection status LED) will blink.



If **ALARM** LED stays on always, please switch off the power supply and reboot the device. If **ALARM** LED still keeps on after reboot, please contact SANGFOR Customer Service.

If the corresponding LED indicates normal working status, turn off and unplug the power supply, and perform the following steps.

3. Use RJ-45 straight-through Ethernet cable to connect the **LAN** interface (**ETH0**) to the internal network (LAN).

4. Use RJ-45 Ethernet crossover cable to connect the **WAN** interface (**ETH2)** to the external network, (i.e., router, optical fiber transceiver or ADSL Modem for external network).

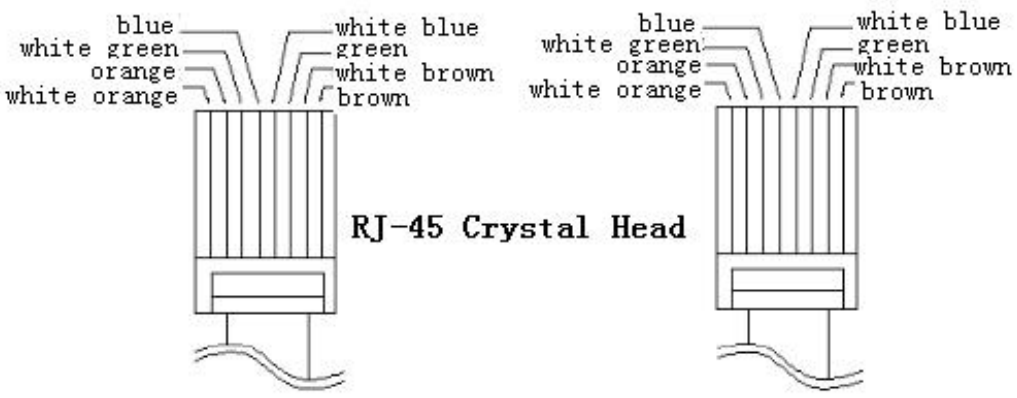
Multi-line function allows multiple Internet lines to be connected to Sangfor device. When deploy multiple lines, please connect the second Internet line to **WAN2** interface (**ETH3**) and the third Internet line to **WAN3** interface (**ETH4**), and so on.

5. If you want the Sangfor device to provide secure protection for DMZ (Demilitarized Zone), use RJ-45 Ethernet cable to connect **ETH1** interface to the devices such as Web server, SNMP Server that provides services to external networks.

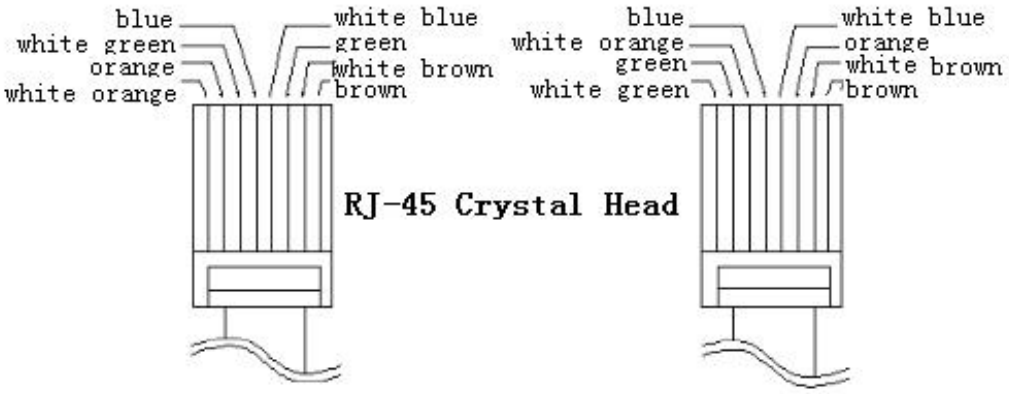
- Use crossover cable to connect **WAN** interface **(ETH2/3)** to the external network.
- Use straight-through cable to connect **LAN** interface **(ETH0)** to the internal network.
- For direct access to administrator Web console, use crossover cable to connect **LAN (ETH0)** interface to the computer.

In case session cannot be established but the corresponding LED indicates normal working status, please check whether the right type of cables are being used. The differences between straight-through cable and crossover cable are shown in the figures below:

1. Wire Sequence of Straight-through Cable



2. Wire Sequence of Crossover Cable



Chapter 2 Initial Login to Admin Console

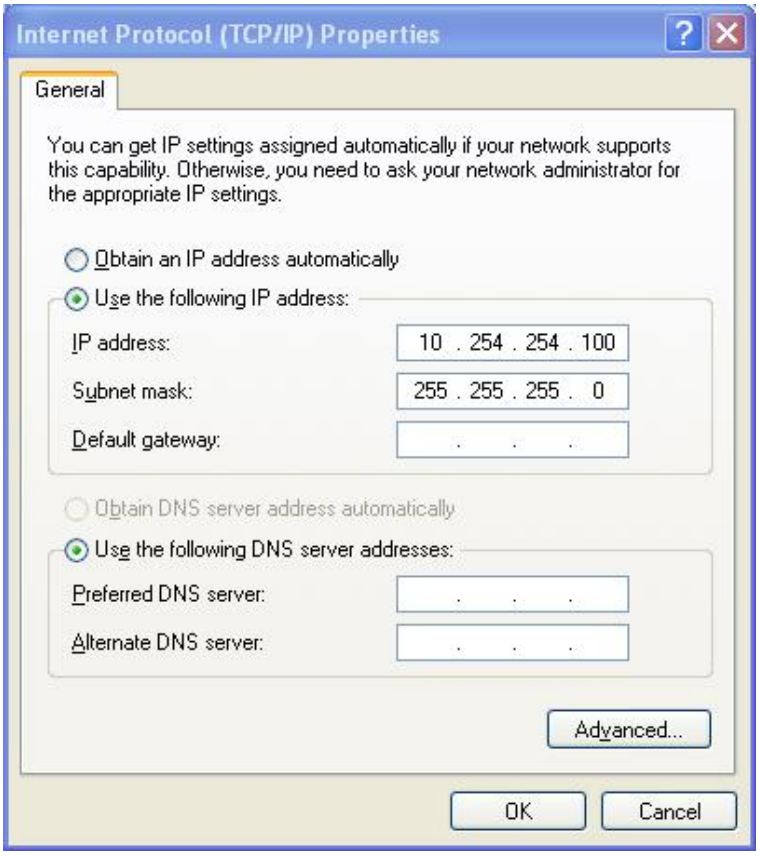
SANGFOR SSL VPN system provides Web-based administration through HTTPS port 4430. The initial URL for administrator console access is https://10.254.254.254:4430.

Before logging in to administrator console of SSL VPN, please ensure the following:

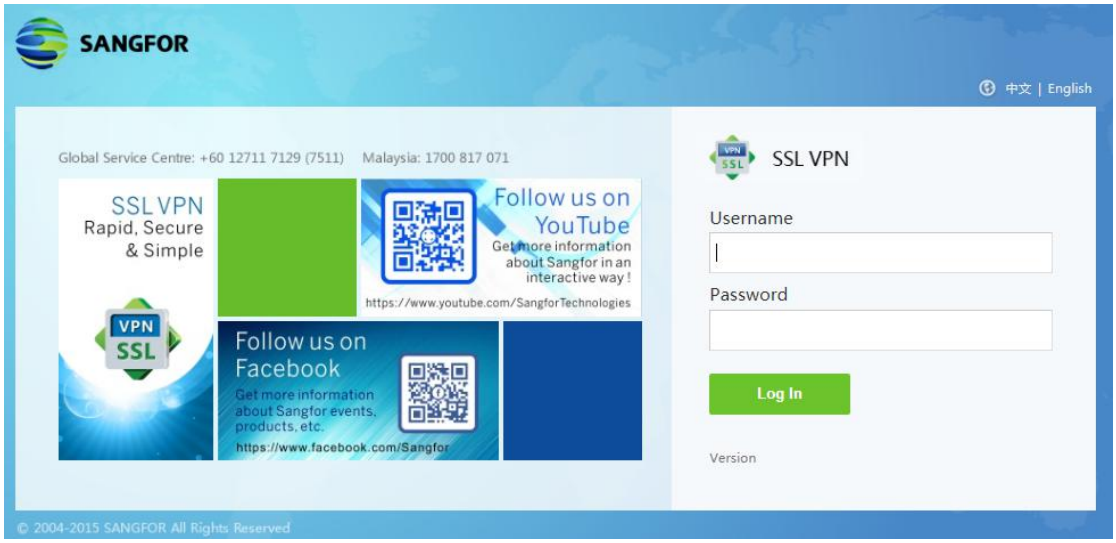
- Deploy a computer in the subnet where the Sangfor device resides.
- Connect the PC's network interface card (NIC) and the Sangfor device's **ETH0** interface to a same layer-2 switch, or connect the PC's NIC to Sangfor device's **ETH0** interface directly with a network cable.
- Ensure any IE browser is installed on the PC. Non-IE browsers Opera, Firefox, Safari and Chrome are not supported.

Logging in to Admin Console

1. Turn on the PC and Sangfor device.
2. Add an IP address on the PC, an IP address that resides in the network segment **10.254.254.X** (for instance, 10.254.254.100) with subnet mask **255.255.255.0**, as shown below:



3. Open the IE browser and enter the SSL VPN address and HTTPS port (https://10.254.254.254:4430) into the address bar. Press **Enter** key to visit the login page to SSL VPN administrator Web console, as shown below:



You also can scan the QR code on above page to follow SANGFOR.

4. Enter the administrator username and password and click the **Log In** button. The default administrator username and password are a**dmin** (case-sensitive). You can also choose page language at the upper right corner of the login page as per your need .

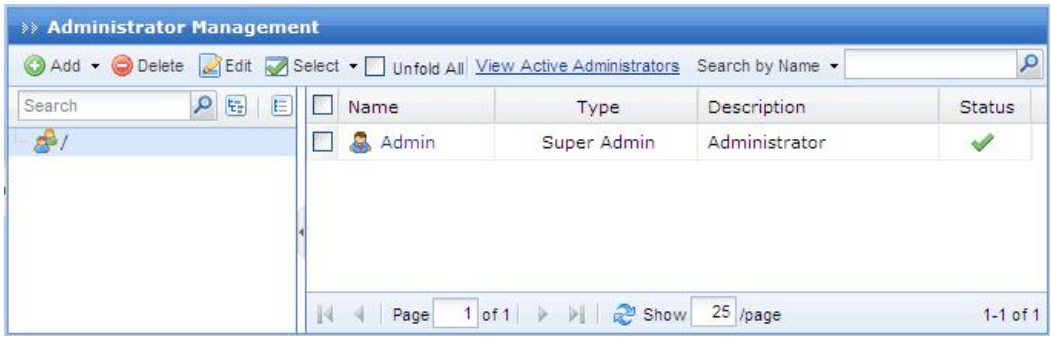
5. For version information of the software package, click on **Version** below the textboxes.

Modifying Administrator Password

We strongly recommend you to change the administrator password after initial login, so as to prevent others from logging in to the administrator Web console and using default Admin credentials to make unauthorized changes on the administrator account and initial configurations.

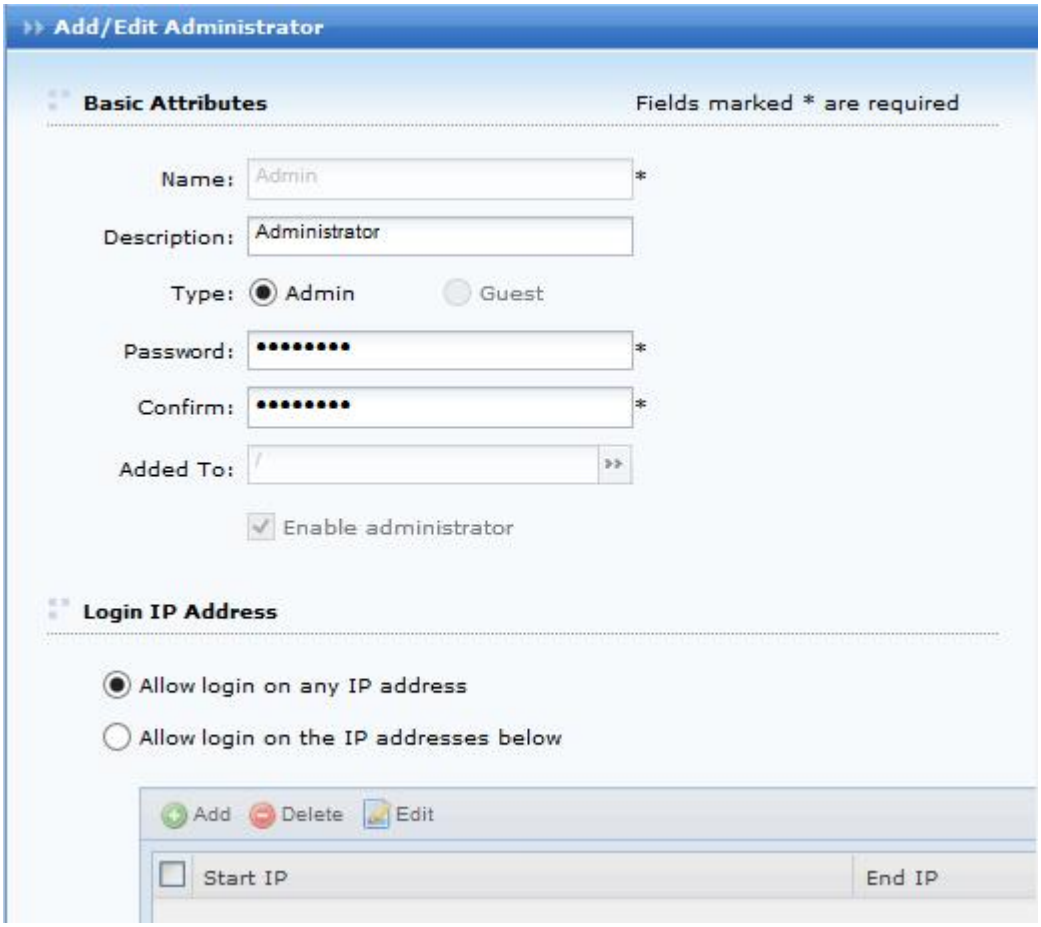
To modify default administrator password, perform the following steps:

1. Navigate to **System** > **Administrator** to enter the **Administrator Management** page. The default administrator account (super administrator) is as seen in the figure below:



2. Click the account name **Admin** to enter the **Add/Edit Administrator** page (as shown

below):



3. Modify the password and click the **Save** button on the above page.

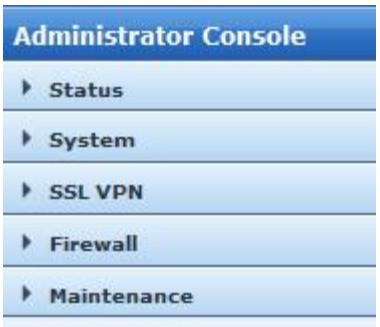


- Password of the account **Admin** should not be shared with anyone.
- If the Sangfor device is to be maintained by several administrators, create multiple administrator accounts for segregation of duty.

Chapter 3 System and Network Settings

After logging in to the administrator console, status of this SSL VPN and some function modules are seen at the right side of the page, and a tree of configuration modules are seen at the left side of the page.

There are five configuration modules in all:

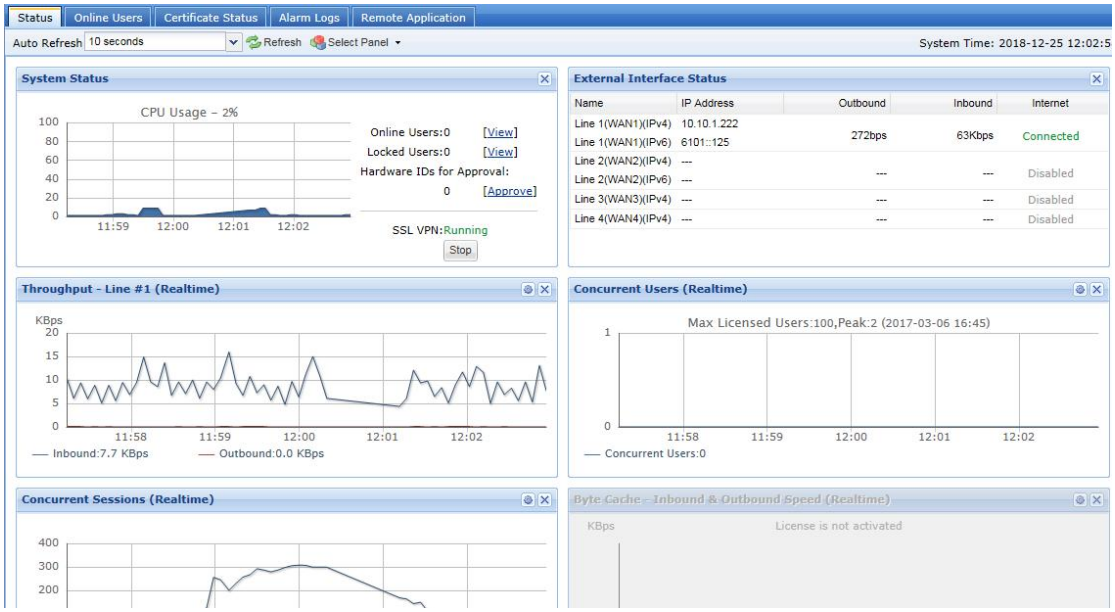


- **Status:** Shows the running status of the Sangfor device and the related modules.
- **System:** Configures the related licenses of the device, network settings and other global settings such as schedule, administrator, SSL VPN options, etc.
- **SSL VPN:** Configures the SSL VPN related settings, such as SSL VPN account, resources, roles, policy sets, remote servers and endpoint security rules and policies.
- **Firewall:** Configures the internal firewall rule or policy of the Sangfor device.
- **Maintenance:** Shows the logs, backups. It also enables administrator to restore configuration, restart service, reboot or shut down device.

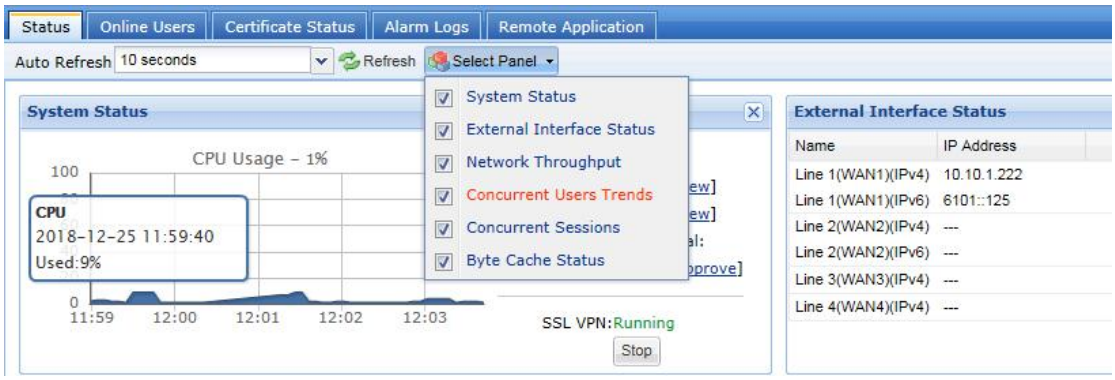
Viewing Status

Viewing SSL VPN Status

There are six panels showing status of SSL VPN, including **System Status, External Interface Status**, **Throughput**, **Trends of Concurrent Users**, **Concurrent Sessions** and **Byte Cache**.



Each panel is selective and display criteria are configurable. To show or hide certain panel, click **Select Panel** and then select or clear the checkbox next to the panel name, as shown below:

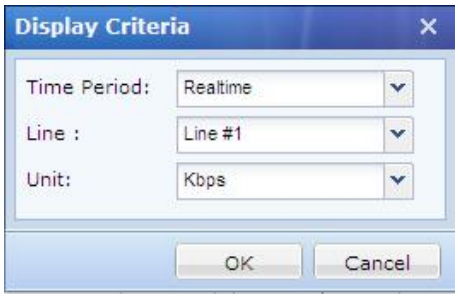


The other contents on the **Status** page are described as follows:

- **Auto Refresh:** Specifies the time interval for refreshing the status automatically, or click **Refresh** to refresh the page manually and immediately.
- **System Status:** This panel shows the CPU utilization of the SSL VPN system, number of online users and locked users as well as status of SSL VPN service. **View** is a link to the **Online User** page or **Hardware ID** page.
- **Stop Service:** Click this button to stop the SSL VPN service.

- **External Interface Status:** This panel shows the status of the external interfaces and Internet, including information of the outbound and inbound speed, Internet connection.
- **Throughput:** This panel shows the overall outbound and inbound speed in graph.

  Click the **Settings** icon (at the upper right of the panel) to specify display criteria, such as time period (realtime, last 24 hours or last 7 days), Internet line and the unit of traffic speed, as shown below:

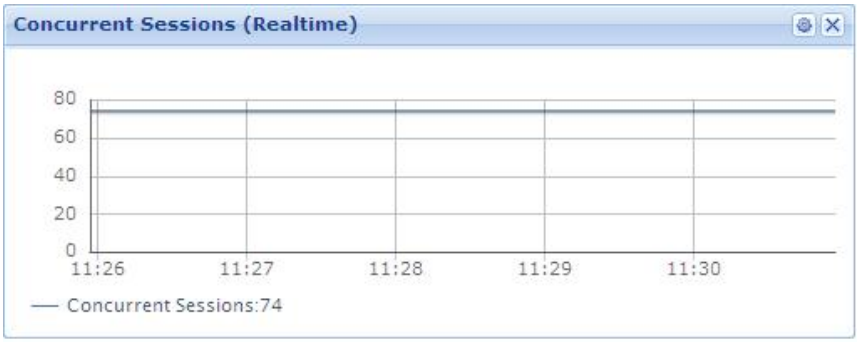


- **Trends of Concurrent Users:** This panel shows the number of users that are using SSL VPN concurrently during certain period of time, as shown below:



  Click the **Settings** icon (at the upper right of the panel) to specify time period (realtime, last 24 hours or last 7 days), as shown below:

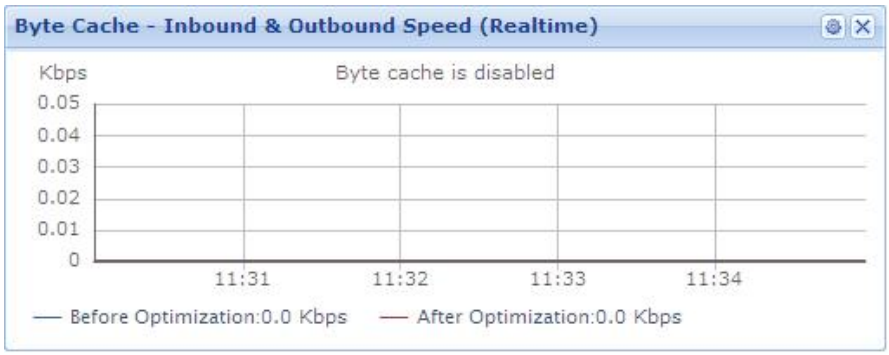
- **Concurrent Sessions:** This panel shows the concurrent sessions initiated by users currently or during certain period of time, as shown below:



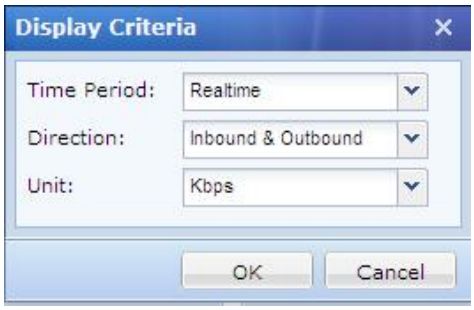
  Click the **Settings** icon (at the upper right of the panel) to specify time period (realtime, last 24 hours or last 7 days).

- **Byte Cache:** This panel shows the byte cache status and optimization effect brought by byte

caching, as shown below:



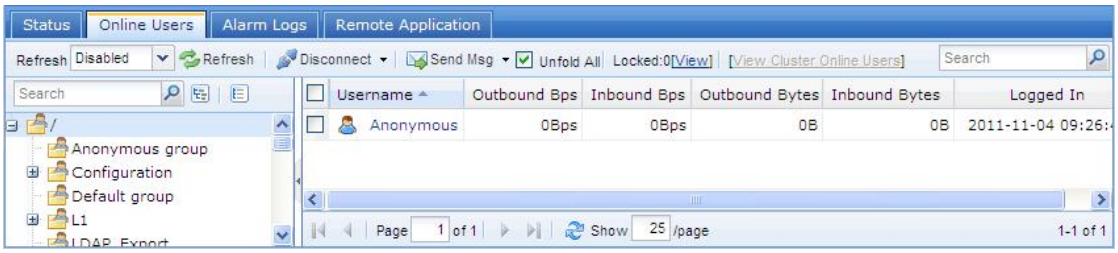
Click the **Settings** icon  (at the upper right of the panel) to specify display criteria, such as time period (realtime, last 24 hours or last 7 days) and direction of traffic speed (inbound&outbound, outbound or inbound), as shown below:



Viewing Online Users

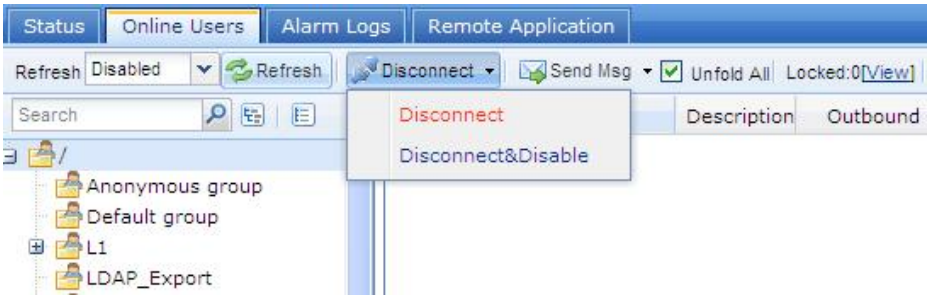
Navigate to **Status** > **SSL VPN** > **Online User** to view information of the online users, such as number of users connecting to the SSL VPN, the time when these online users connected, the mount of received/sent bytes, as well as the outbound and inbound speed. Administrator can disconnect or disable any of these online users.

The **Online Users** page is as shown below:



The following are the contents included on **Online Users** page:

- **Auto Refresh:** Specifies the time interval for refreshing this page, or click **Refresh** to refresh the page manually and immediately.
- **Disconnect:** Click it and select an option to disconnect, or disconnect and disable the selected user(s), as shown below:



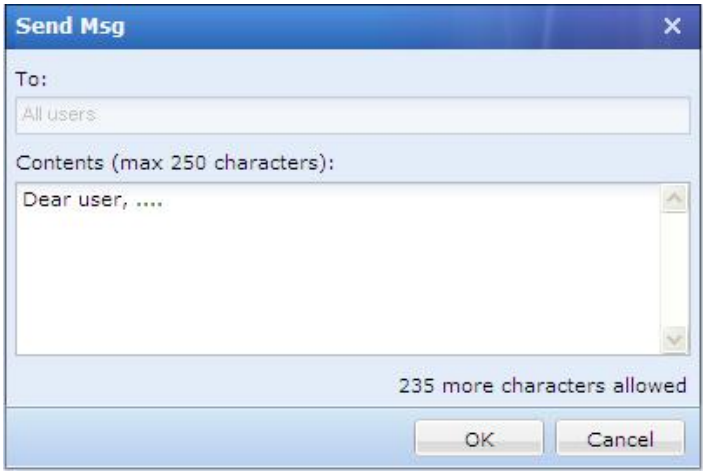
If **Disconnect** is selected, the selected user will be forced to disconnect from the SSL VPN.

If **Disconnect&Disable** is selected and **Apply** button is clicked (on the pop-up bar at the top of the page), the selected user will be forced to disconnect with SSL VPN after are clicked and be prohibited from logging in again until it is unlocked.

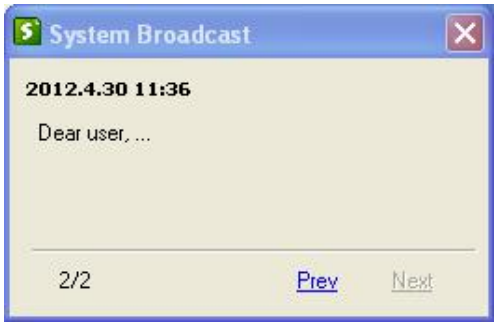
- **Send Msg:** Click it to write and send a message to the selected or all SSL VPN user(s), as shown below:



After receiver is selected, write the message, as shown below:

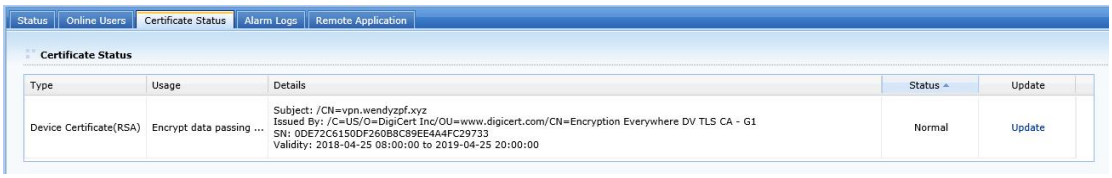


Click the **OK** button and the online end user(s) will see the system broadcasting prompt, as shown below:



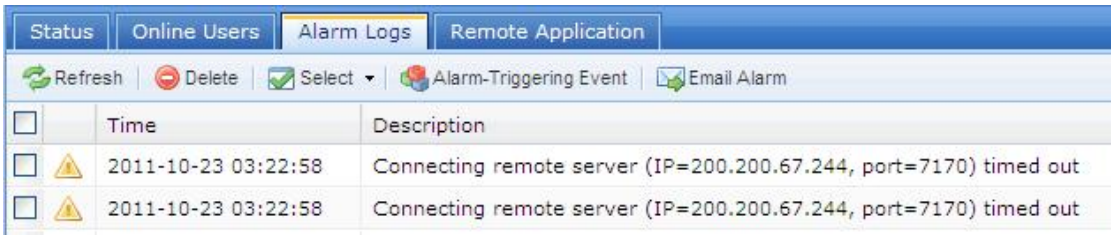
Certificate Status

Navigate to **Status** > **SSL VPN** > **Certificate Status** to view the status information of the device certificate, as shown below:



Viewing Alarm Logs

Navigate to **Status** > **SSL VPN** > **Alarm Logs** to view the alarm-related logs on the Sangfor device, as shown below:



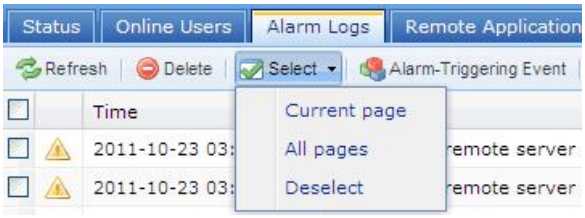
The following are the contents included on **Alarm Logs** page:

- **Delete:** Click it and the selected alarm log(s) will be removed from the log list.
- **Select:** Click it and three options appear, namely, **Current page, All pages** and **Deselect**.

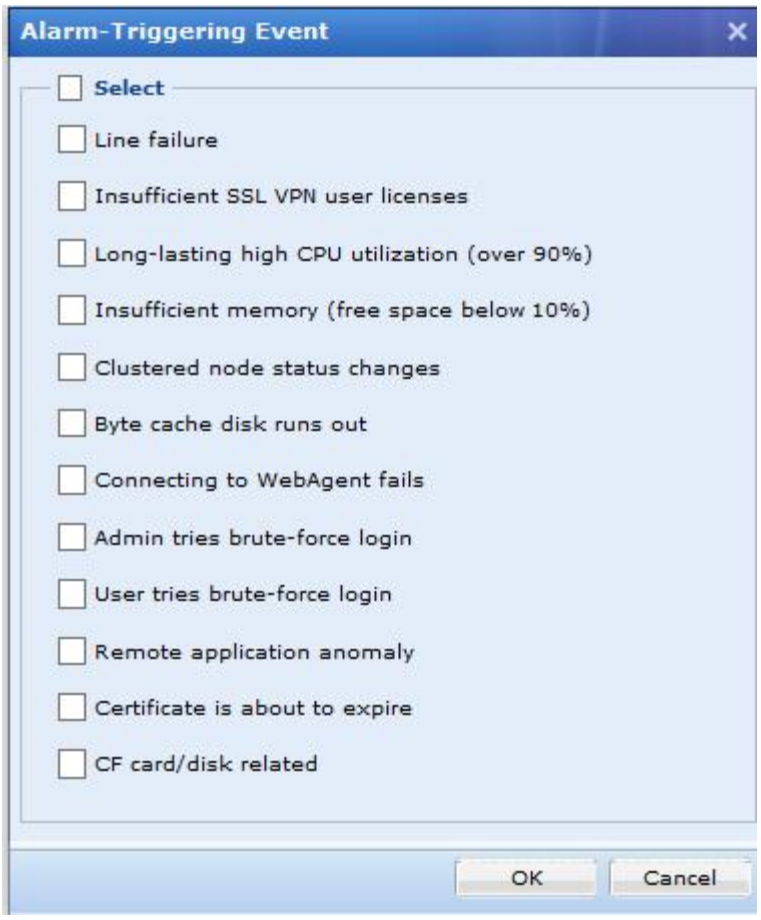
  If **Current page** option is selected, all the logs displayed on this page will be selected.

  If **All pages** option is selected, all the logs (including those on all other pages that are not displayed) will be selected.

  If **Deselect** is selected, all the selected logs will be deselected, as shown in the figure below:



- **Alarm-Triggering Event:** Click it to enter the **Alarm-Triggering Event** page to specify the event(s) that can trigger email alarm.

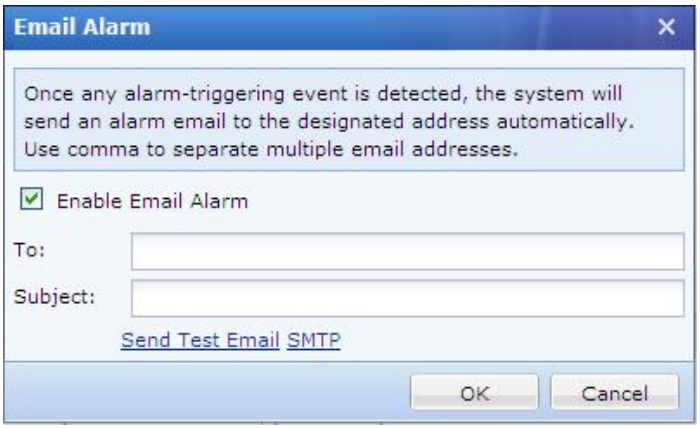


The following are the contents included on the **Alarm-Triggering Event** page:

- **Line failure:** Indicates that there is something wrong with Internet line.
- **Insufficient SSL VPN user licenses:** Indicates the number of concurrent users that are connecting to SSL VPN reaches the maximum number of licenses.
- **Long-lasting high CPU utilization (over 90%):** Indicates that the CPU utilization is too high (above 90%) during 120 seconds. Once it reaches the threshold, the system will send an email to the specified email address to notify the administrator of that, and do so when the CPU utilization of the system returns to normal.
- **Insufficient memory (free space below 10%):** Once system memory keeps insufficient (below 10%) for 4 minutes, the system will send an email to the specified email address to notify the administrator of that, and do so when the system memory returns to normal.
- **Clustered node status changes:** Once any node of the cluster changes status, the system will send an email to the specified email address to notify the administrator of that.
- **Byte cache disk runs out:** When the byte cache runs out of the assigned disk space, the system will email an alarm event to the specified email address to notify the administrator of that.
- **Connecting to WebAgent fails:** If the WebAgent is inaccessible, the system will email an alarm event to the specified email address to notify the administrator of that.

- **Admin tries brute-force login:** If an administrator successively fails to log in to the SSL VPN administrator console too many times, the system will email an alarm event to the specified email address to notify the administrator of that.
- **User tries brute-force login:** If a VPN user successively fails to log in to SSL VPN too many times, the system will email an alarm event to the specified email address to notify the administrator of that.
- **Remote application anomaly:** Indicates that the system will generate remote application related alarm once error arises from remote application, and will email an alarm event to the specified email address to notify the administrator of that.
- **Certificate is about to expire:** Indicates that system will generate related alarm once certificate is about to expire, and will email an alarm event to the specified email address to notify the administrator of that.
- **CF card/disk related:** Indicates that the system will generate CF card/disk related alarm once error arises from CF card/disk, and will email an alarm event to the specified email address to notify the administrator of that.

- **Email Alarm:** Click it to enter **Email Alarm** page. Select the checkbox next to **Enable Email Alarm** and configure email recipient and subject. An email notification will be sent to the email address once alarm is triggered by any of the specified alarm-triggering event(s).

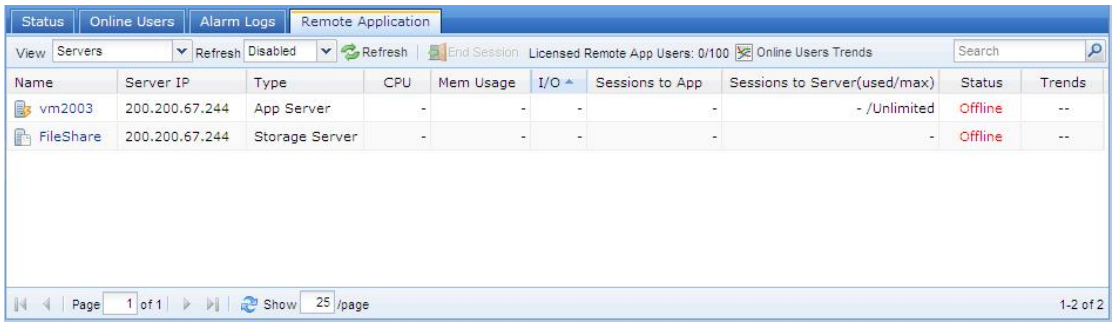


Click **Send Test Email**, and system will send a test email to specified email address automatically.

Click **SMTP**, and you will be redirected to **Status > SSL VPN > SMTP** page. For more, refer to **Configuring SMTP Server** section in Chapter 3.

Viewing Remote Application

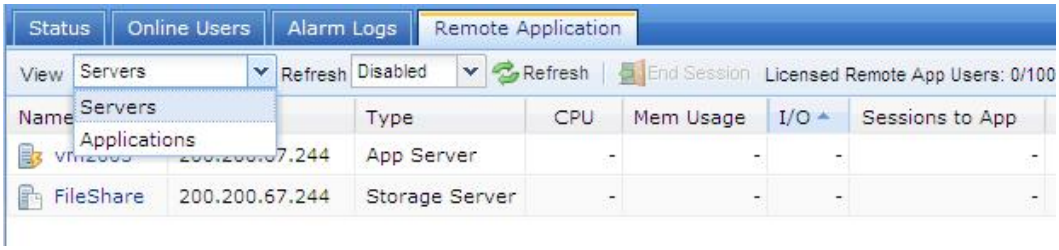
Navigate to **Status** > **SSL VPN** > **Remote Application** to view the information and status of the remote application servers that provide services to users over SSL VPN, as shown below:



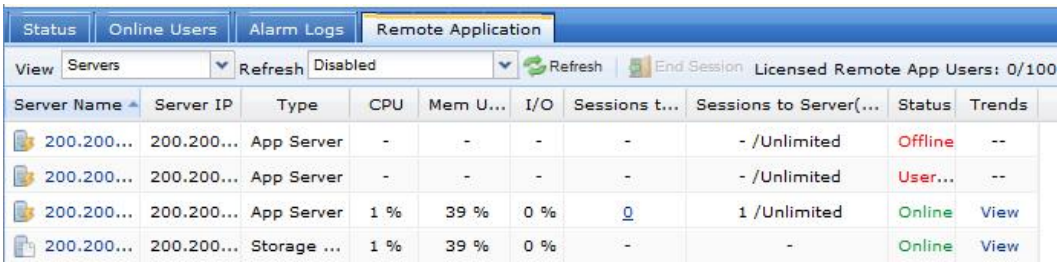
The above page shows information of the remote servers, including name, address, sessions and status of the remote application server, maximum number of concurrent sessions.

The following are the contents included on **Remote Application** page:

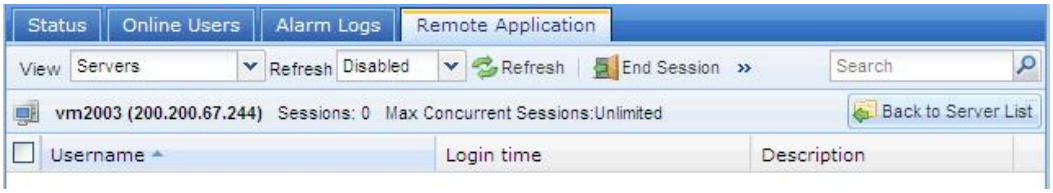
- **View:** Indicates the object showing up on this page. Options are **Servers** and **Applications**, as shown below:



- **Servers:** Mainly offers the information of the involved servers that are providing services to VPN users. They are the servers configured in **SSL VPN** > **Remote Servers.** The page is as shown below:

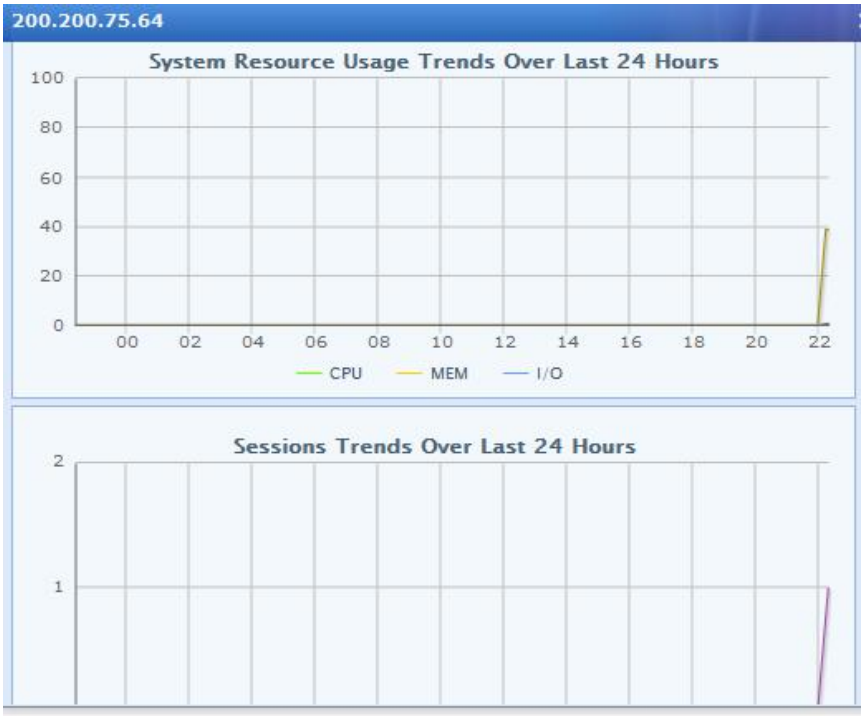


To view users that are currently connecting to a server, click on server name and the user detailed information of the user is seen, as shown in the figure below:

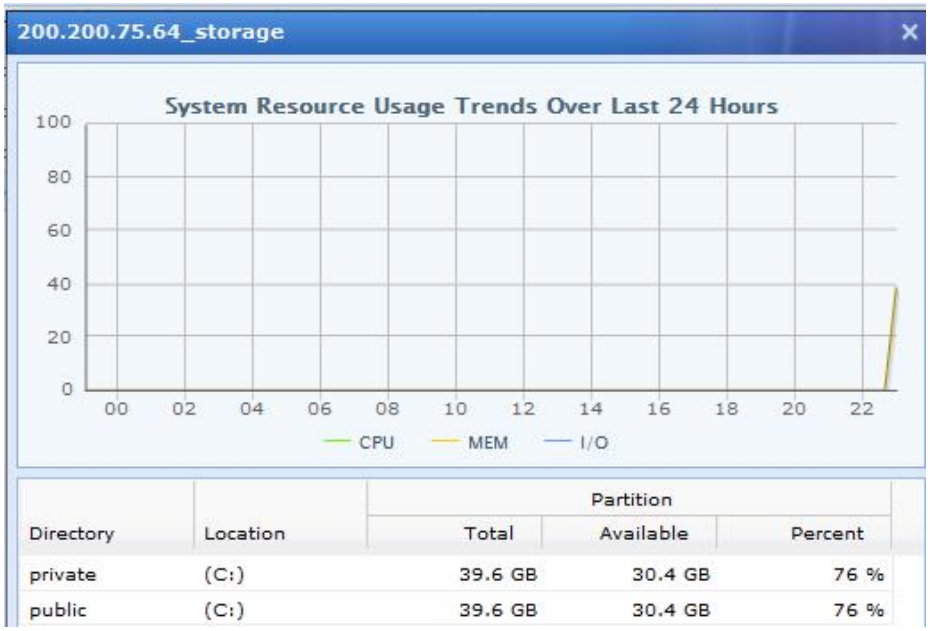


End Session: Select a desired user and then click it, and the session(s) established between the selected user and that server will be ended.

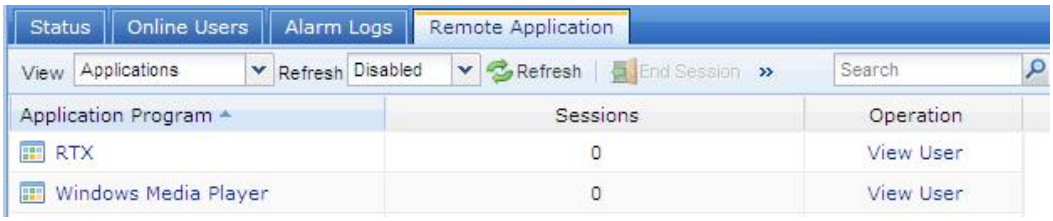
To view resource usage of a app server, click **View** in **Trends** column, as shown below:



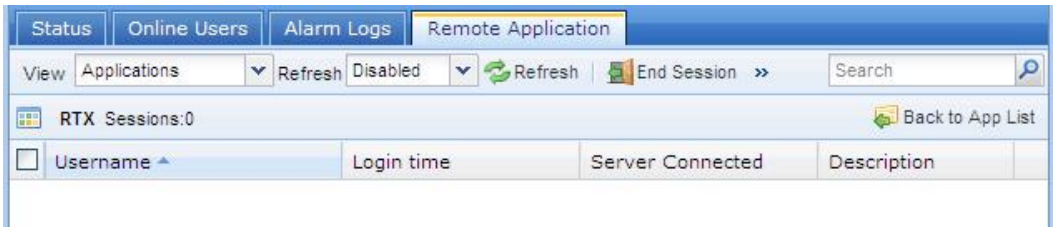
To view system resource usage of storage server over the last 24 hours, click **View** in **Trends** column, as shown below:



- **Applications:** Mainly offers the information of the involved services that are being accessed by SSL VPN users and presents the use of these services since they have been invoked by the requested resource. They are the application programs configured in **SSL VPN** > **Remote Servers,** as shown below:



To view the users accessing an application, click the application name or **View User**, information of the users involved are as shown in the figure below:



End Session: Select a desired user and then click it, and the session(s) established between the selected user and that application will be ended.

System Settings

System settings refer to the settings under **System** module, including **System**, **Network**, **Schedule**, **Administrator** and **SSL VPN Options**.

Configuring System Related Settings

Navigate to **System** > **System** and the seven pages are seen, namely, **Licensing**, **Date/Time**, **Console Options**, **External Report Center**, **Device Certificate, SMTP**, **Syslog** and **SNMP**, as shown below:



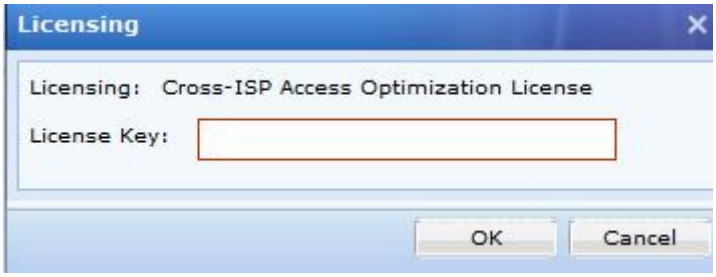
Configuring License of Device and Function Modules

Navigate to **System** > **System** > **Licensing** to activate the license or modify the license key related to this device and each function module.

Under **License of Device** are the license of this Sangfor device and other authorization you have bought from SANGFOR. Under **License of Each Module** are licenses that are optional for Sangfor device. Once license of a function module is activated and that feature is enabled, the corresponding module will work.

The following are the contents included on **Licensing** page:

- **Cross-ISP Access Optimization:** Cross-ISP access optimization function is an optional function offered by SANGFOR SSL VPN, which helps to facilitate and optimize the data transmission among links provided by different Internet Service Operators (ISP, in China, for example, there are China Telecom, China Netcom, etc). Click **Activate** to enter license key for Cross-ISP access optimization feature, as shown below:

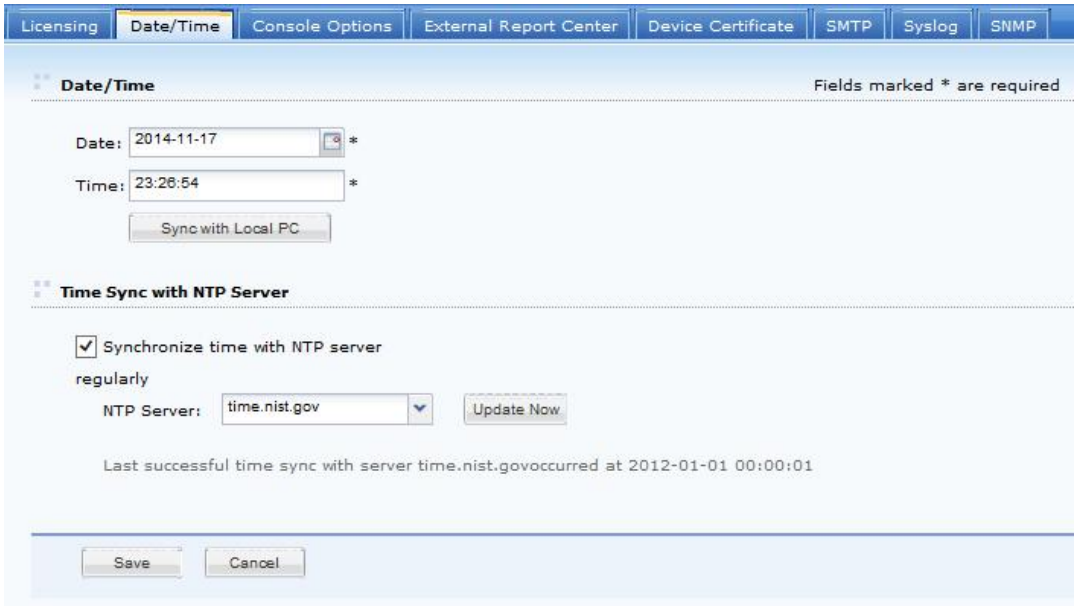


- **Upgrade License:** The license is used to update the current SANGFOR SSL VPN system with Sangfor Firmware Updater 6.0 (for more details, refer to Appendix B: Sangfor Firmware Updater 6.0). Every upgrade license has an expiry date, which means prior to this date you can update this device to keep the software version up-to-date.
- **License Key:** Indicates the license of this Sangfor device. The device license determines some other authorization, more specifically, the maximum number of Internet lines and maximum number of connecting VPN users.
- **Lines:** Indicates the maximum number of Internet lines that this Sangfor device can be connected to.
- **SSL VPN Users:** Indicates the maximum number of SSL VPN users that are allowed to access the SSL VPN concurrently.
- **SSO:** With this license, Single Sign-On (SSO) feature can apply to users' access to the SSL VPN.
- **SMS Authentication:** With this license, SMS authentication could be enabled to add variety to the authentication methods applying to users' secure access to the SSL VPN. This type of authentication requires the connecting users to enter SMS password that has been sent to their mobile phones.
- **Byte Cache:** Byte cache is an additional but optional network optimization function offered by the SANGFOR SSL VPN. With byte cache being enabled, time for data transmission and bandwidth consumption will be dramatically reduced.
- **One-Way Acceleration:** This license allows you to enable one-way acceleration to optimize transmission rate in high-latency network.
- **Cluster:** This license allows you to enable cluster to couple some scattered Sangfor devices. It is known that cluster can achieve unified management and greatly improve the performance, availability, reliability of the "network" of Sangfor devices.
- **Remote Application:** With this license, applications launched by remote server can be accessed remotely through SSL VPN by end users from any location, as if they are running on the end user's local computer.
- **Max Remote App Users:** Indicates the maximum number of users that can access the remote application resources.
- **Application Wrapping License:** This license allows you to wrap application before it is published to users.

- **Activate:** Click this button and then enter the corresponding license key to activate the license.
- **Modify:** Click this button and enter the new license key (or value) to modify the license key (or number of mobile Sangfor VPN users).

Modifying System Date and Time

1. Navigate to **System** > **System** > **Date/Time** to enter **Date/Time** page, as shown below:

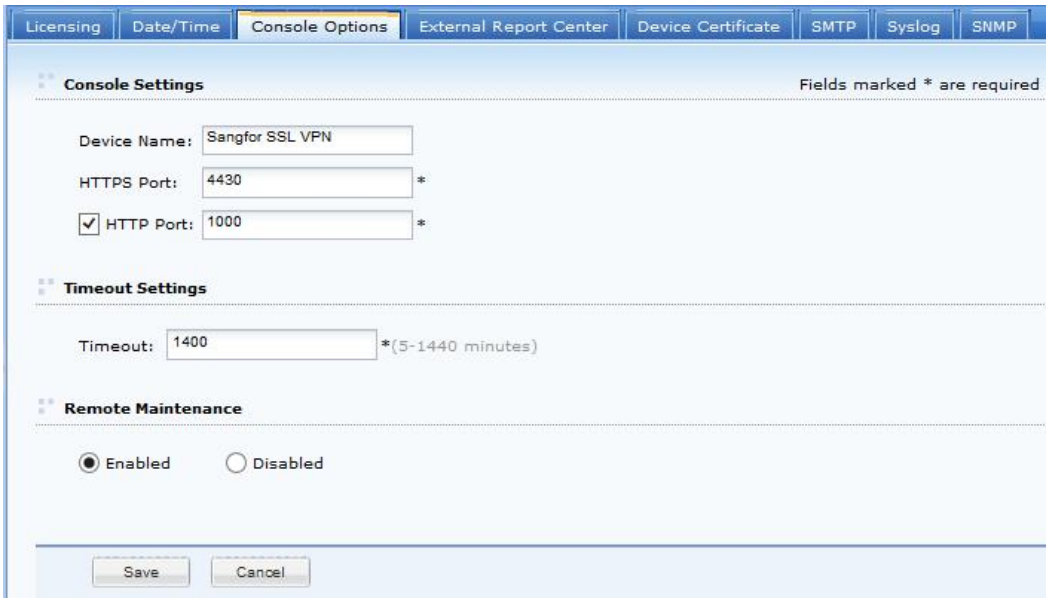


2. Configure the following:
   - **Date:** Specifies the date. To select date, click the icon .
   - **Time:** Specifies the time. Enter the time into this field and set it as the current time of this Sangfor device. Date format should be **hh: mm: ss**.
   - **Sync with Local PC:** Click this button to synchronize the date and time of the Sangfor device with your computer.
   - **Synchronize time with NTP server regularly:** Select it to specify NTP server.
   - **Update Now:** Click on it to synchronize time of Sangfor device with NTP server.
3. Click the **Save** button to save the settings, or click the **Cancel** button not to save the changes.

Modifying system date or time requires all services to restart.

Configuring Console Options

1. Navigate to **System** > **System** > **Console Options** to enter **Console Options** page, as shown below:



2. Configure the following:

   - **Device Name:** Specifies the name of the Sangfor device, which helps to distinguish it from other clustered nodes if this device joins cluster.
   - **HTTPS Port:** Specifies the HTTPS port used for logging in to this Sangfor device. The default is 4430.
   - **HTTP Port:** Specifies the HTTP port used for logging in to this Sangfor device. The default is 1000.
   - **Timeout:** Specifies the period of time before administrator is forced to log out of the administrator console if no operation is performed.
   - **Remote Maintenance:** Indicates whether to enable or disable administrator to manage this Sangfor device via the WAN interface.

3. Click the **Save** button to save the settings on this page; otherwise, click the **Cancel** button.

Configuring External Report Center

Logs generated by Sangfor device can be sent to external report center, such as system logs, user logs, operation logs, alarm logs, etc. Navigate to **System** > **System** > **External Report Center** to enter the **External Report Center** page, as shown below:



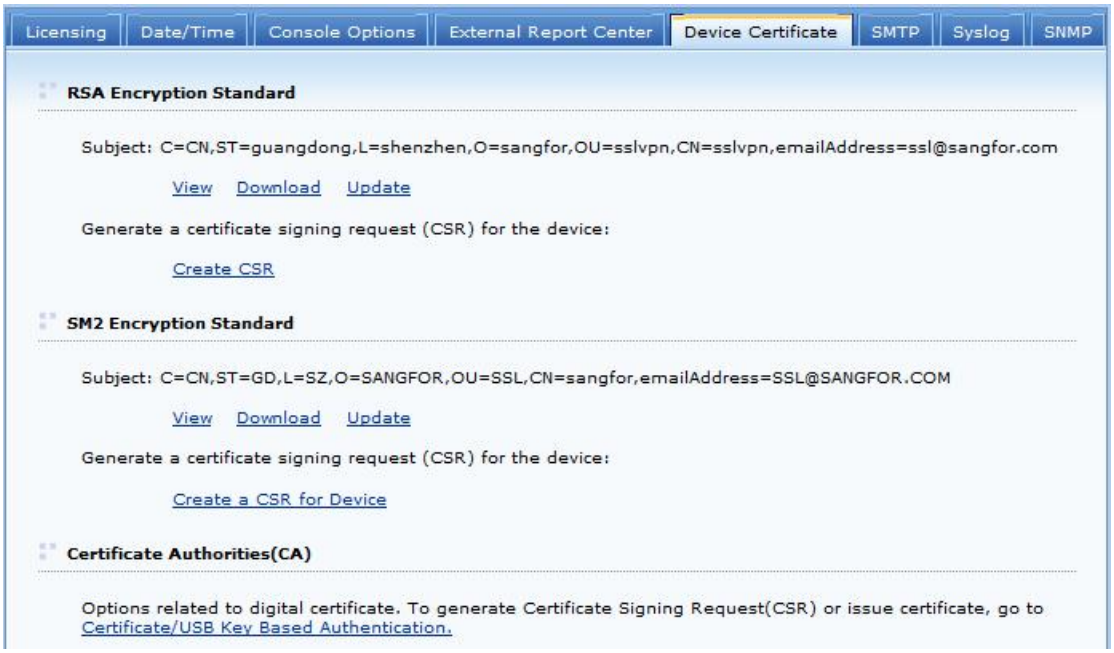
The following are the contents included on this page:

- **Send logs to external report Center:** If it is selected, logs will be sent to external report center.
- **Server IP:** Specifies the IP address of external report center server.
- **Port:** Specifies a port used to communicate with external report center server. Default is 9501.
- **Sync Password, Confirm:** Specifies and confirms sync password for device synchronizing with external report center server. It must be the same as that configured on external report center server.
- **Test Connectivity:** Click it to test the connectivity between the device and external report center server.

Click **Save** to save the changes; otherwise, click **Cancel** button.

Generating Certificate for Sangfor Device

Device certificate is intended for establishing sessions between the Sangfor device and client. Sangfor device supports RSA and SM2 encryption protocol standards. To view current certificate of or to generate certificate for the Sangfor device, navigate to **System** > **System** > **Device Certificate**, as shown in the figure below:



The following are the contents included on the **Device Certificate** page:

- **View:** Click it to view the detailed information of the current certificate.
- **Download:** Click it to download the current device certificate.
- **Update:** Click it to import a new certificate to take the place of the current one.
- **Certificate/USB Key Based Authentication:** Click it to configure Certificate/USB key based authentication (for more details, refer to the Certificate/USB Key Based Authentication section in Chapter 4).
- **Create a CSR for device:** Click this button to generate a certificate signing request (CSR) which should be sent to the external CA to generate the device certificate, and configure the required fields, as shown below:



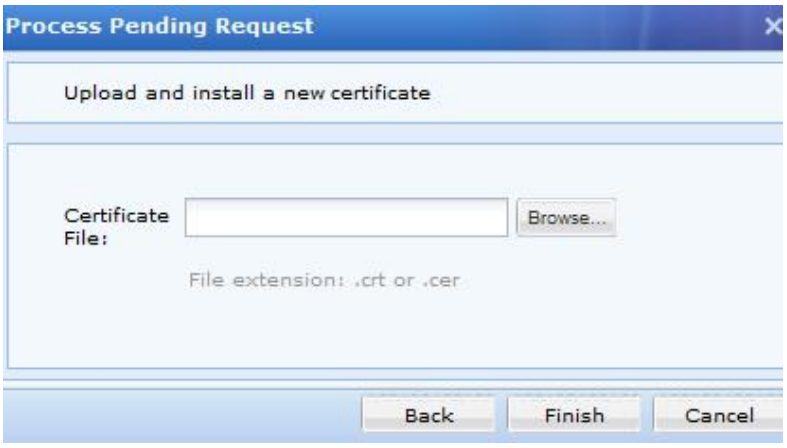
Then click the **OK** button.

Once the certificate signing request is generated, click the **Download** link to download the request.

- **Update:** Click it to import the new external-CA-issued device certificate into the Sangfor device to replace the old one.
- **Process Pending Request:** Click it enter the following page:



If you select **Process pending request and install certificate** and click **Next**, you need to select a certificate you want to install, as show below:

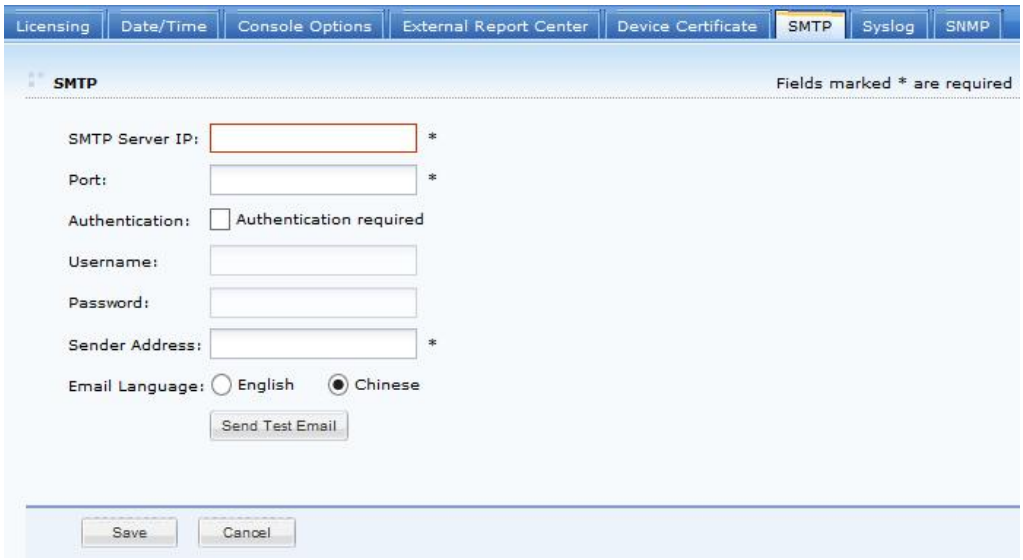


Click **Browse** to select a certificate from your local PC, and click **Finish** to save the settings.

The certificate you want to import must be .crt or .cer.

Configuring SMTP Server

1. Navigate to **System** > **System** > **SMTP** to enter the **SMTP** page, as shown below:



2. Configure the following:

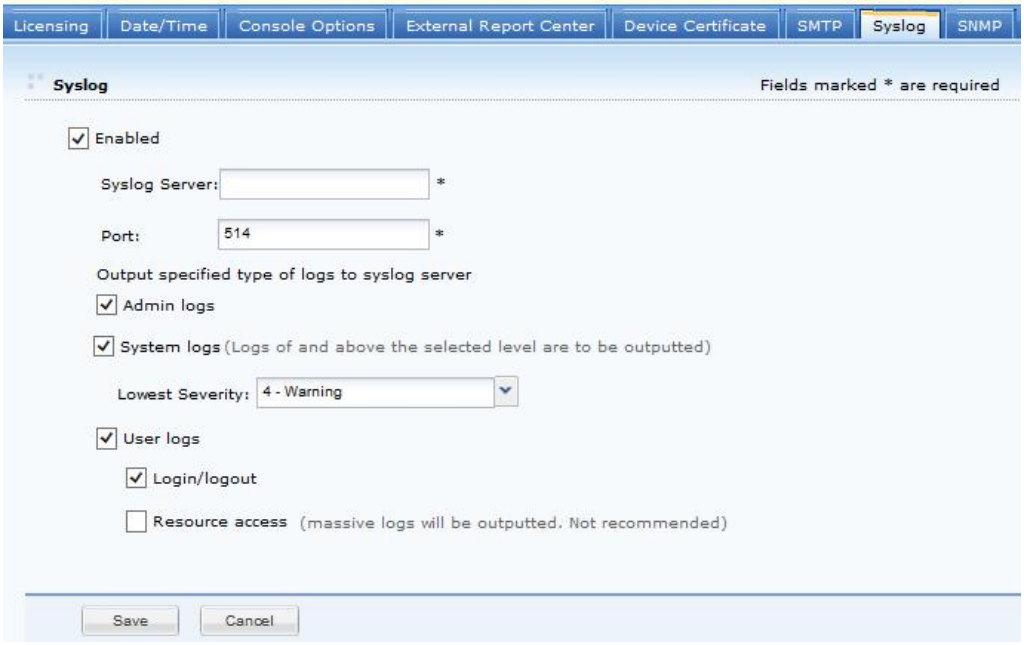
   - **SMTP Server IP:** Specifies the IP address of the SMTP server.
   - **Port:** Specifies the port number used by this SMTP server to provide email delivery related services.

- **Authentication:** Select **Authentication required** and then configure **Username** and **Password**, if this SMTP server requires identity verification.
- **Sender Address:**Specifies email address of sender.
- **Email Language:** Specifies language of email sent by server.
- **Send Test Email:** Click this button to send an email to the specified recipient (configured under **Status** > **Alarm Logs** > **Email Alarm**) to check whether this SMTP server works normally.

3. Click **Save** to save the settings on this page; otherwise, click **Cancel**.

Configuring Syslog Server

1. Navigate to **System** > **System** > **Syslog** to enter the **Syslog** page, as shown below:



2. Configure the following contents on Syslog page:

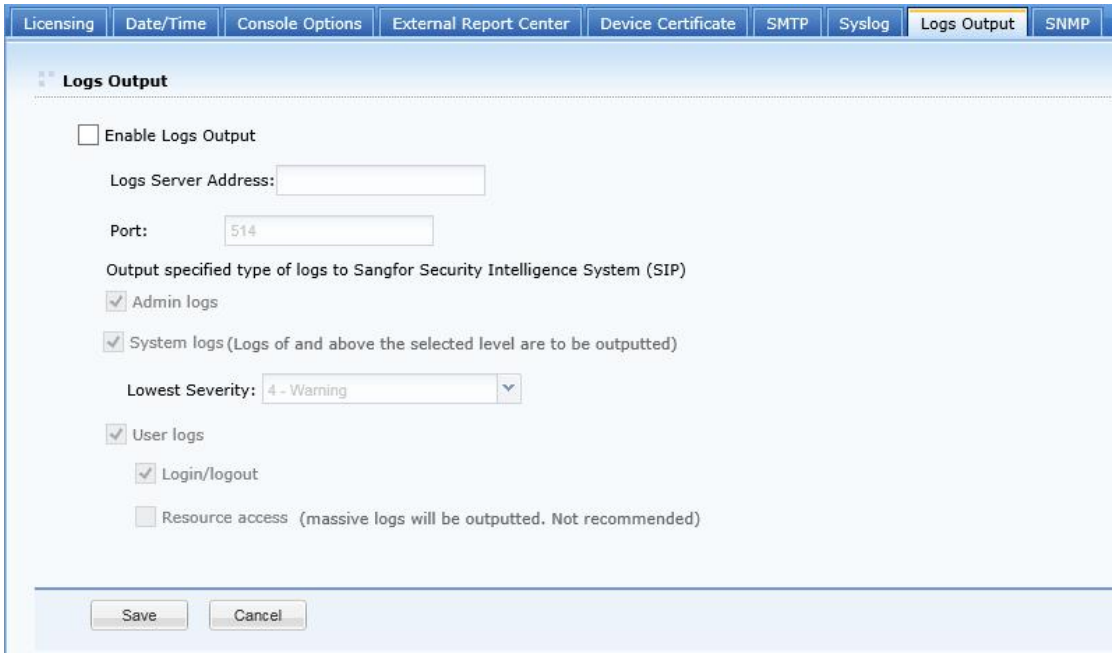
- **Enabled**: Select it to enable logs to be sent to Syslog server.
- **Syslog Server:** Specifies IP address of Syslog server.
- **Port:** Specifies the port number used by the device to communicate with Syslog server.
- **Admin logs:** Select it to allow the admin logs to be outputted to Syslog server.
- **System Logs:** If it is selected, system logs of and above the specified level will be outputted.
- **Lowest Severity:** Specifies the severity level of system logs.
- **User logs：** If it is selected, user logs can be sent to Syslog server.

- **Login/logout:** Select it and system will generate logs when user logs in or log out of device, and the logs can be sent to syslog server.
- **Resource access:** If it is selected, massive logs will be outputted. It is not recommended .

3. Click **Save** to save the changes; otherwise, click **Cancel**.

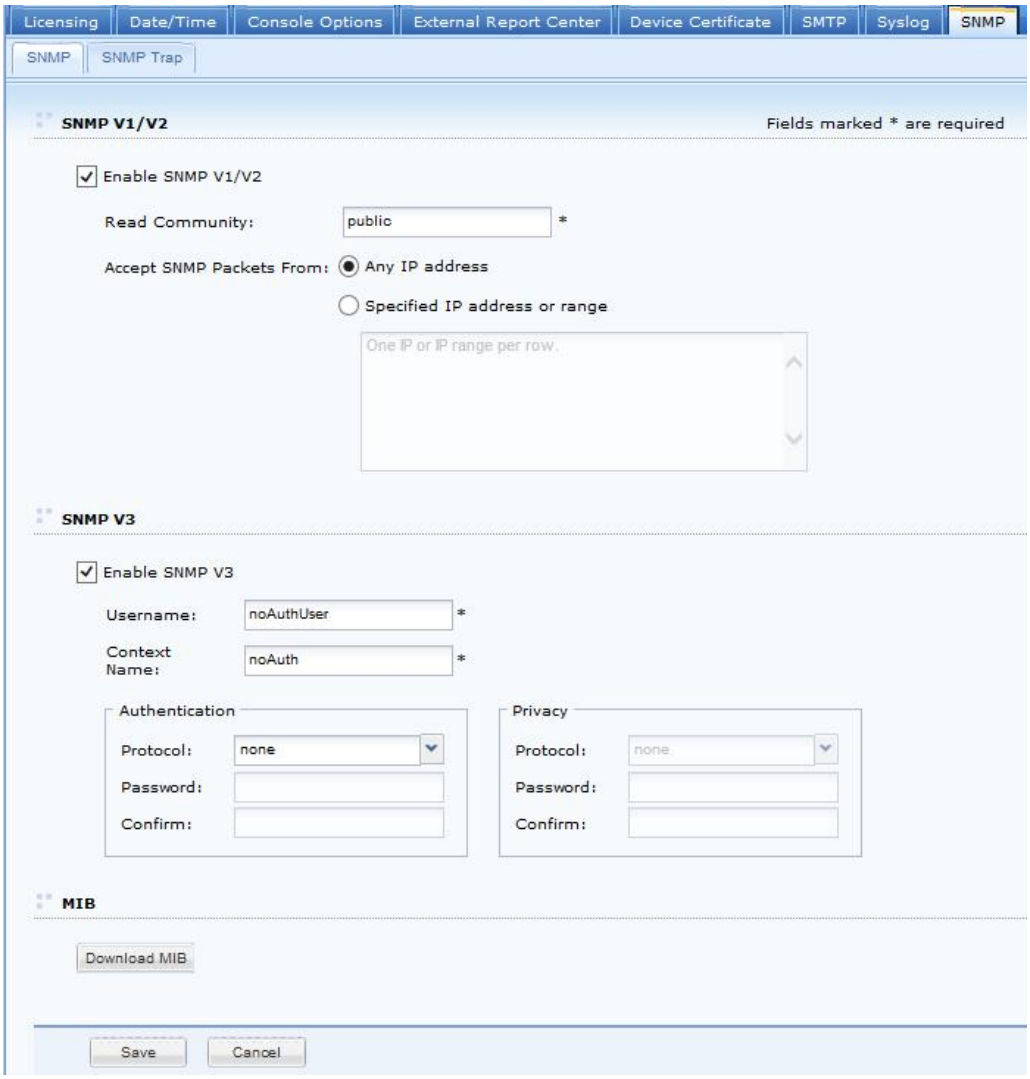
Logs Output

Logs Output is used to synchronize log information to Sangfor Security Intelligence System (SIP).



Configuring SNMP

SNMP(Simple Network Management Protocol) is used to communicate with SNMP management software or SNMP server in customer network.

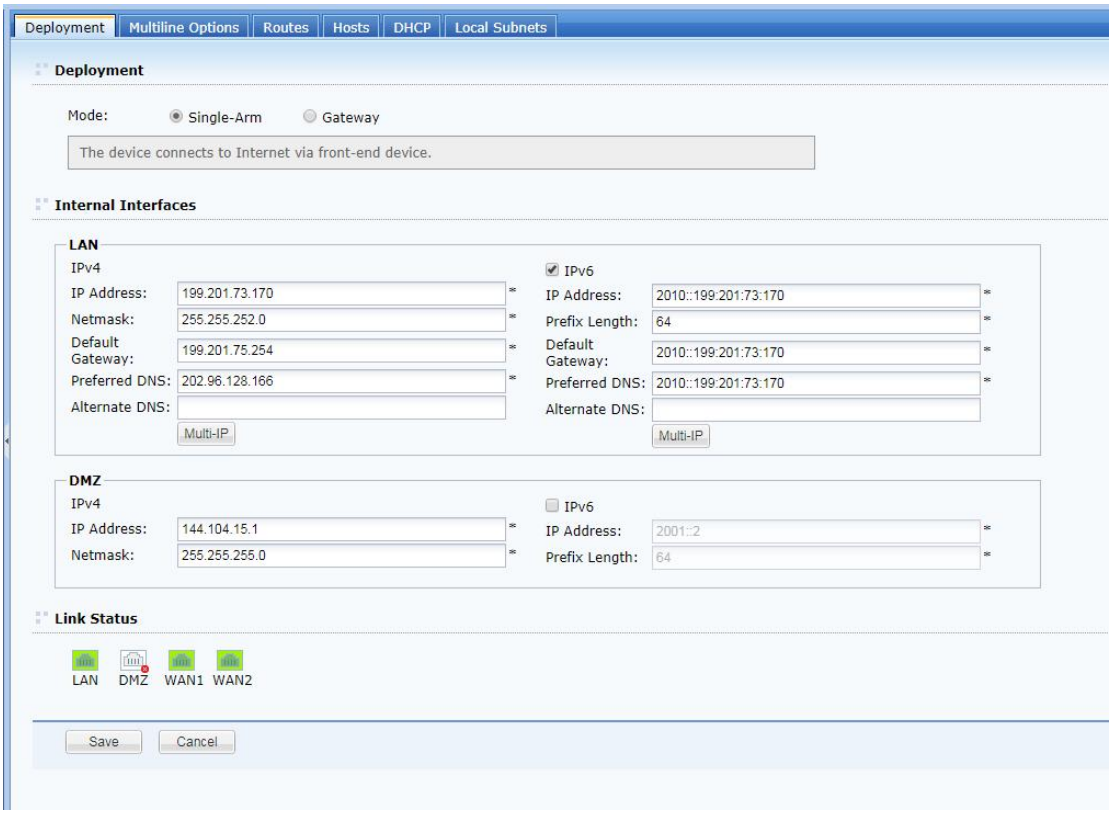

Licensing
Date/Time
Console Options
External Report Center
Device Certificate
SMTP
Syslog
SNMP
SNMP
SNMP Trap
SNMP V1/V2
Fields marked * are required
Enable SNMP V1/V2
Read Community:
public
*
Accept SNMP Packets From:
Any IP address
Specified IP address or range
One IP or IP range per row.
SNMP V3
Enable SNMP V3
Username:
noAuthUser
*
Context Name:
noAuth
*
Authentication
Protocol:
none
Password:
Confirm:
Privacy
Protocol:
none
Password:
Confirm:
MIB
Download MIB
Save
Cancel

Network Settings

Device Deployment

Sangfor device can work in two modes, **Single-Arm** mode and **Gateway** mode. Deployment mode is configured in **System** > **Network** > **Deployment**.

If **Single-arm** mode is selected, the **Deployment** page is as shown in the figure below:



Note: For deployment in Single-Arm mode, IPv4 is mandatory, and IPv6 is optional.

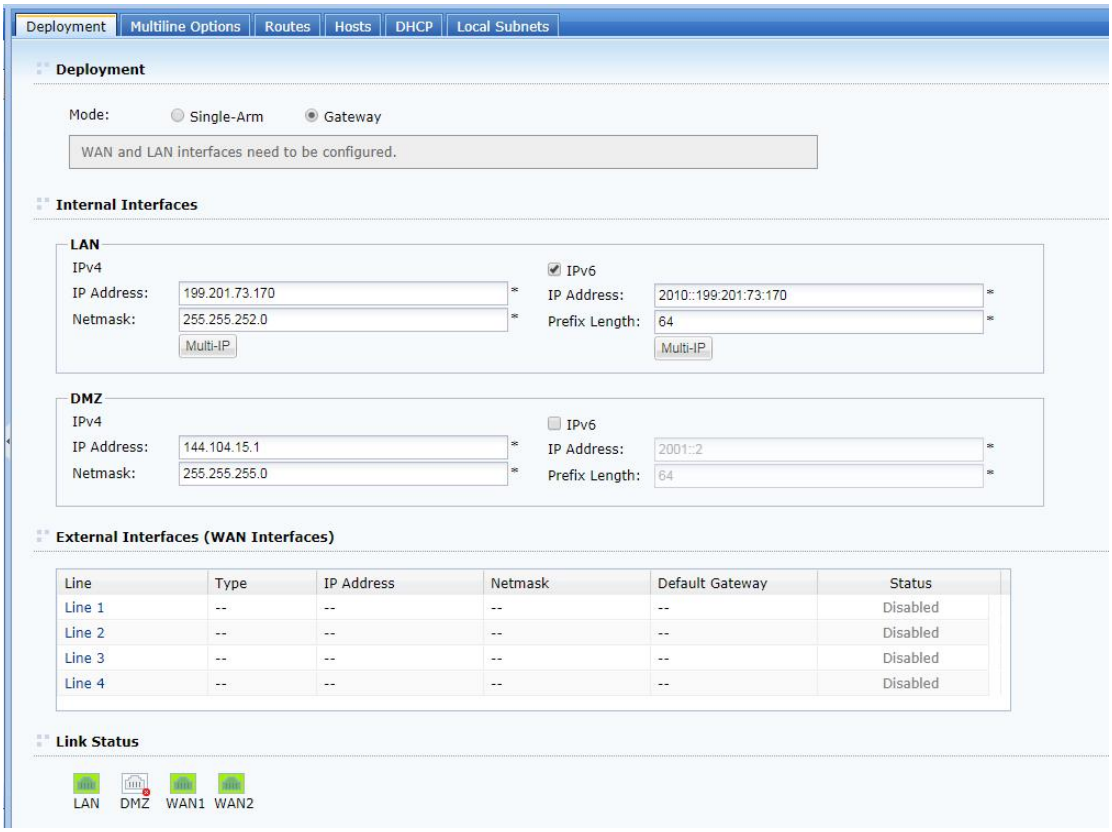
The following are the contents included on the **Deployment** page when **Single-arm** is selected:

- **(LAN) IP Address:** Configures the IP address of the internal interface, **LAN**. This IP address must be identical as the physical LAN interface IP of the Sangfor device.
- **Netmask:** Configures the netmask of the LAN interface IP.
- **Default Gateway:** Configures the default gateway of the LAN interface.
- **(DMZ) IP Address:** Configures the IP address of the internal interface, **DMZ**.
- **Netmask:** Configures the netmask of the DMZ interface IP.
- **Link Status:** Indicates the connection status of internal and external interfaces of the Sangfor

device, whether the network cables are plugged in.

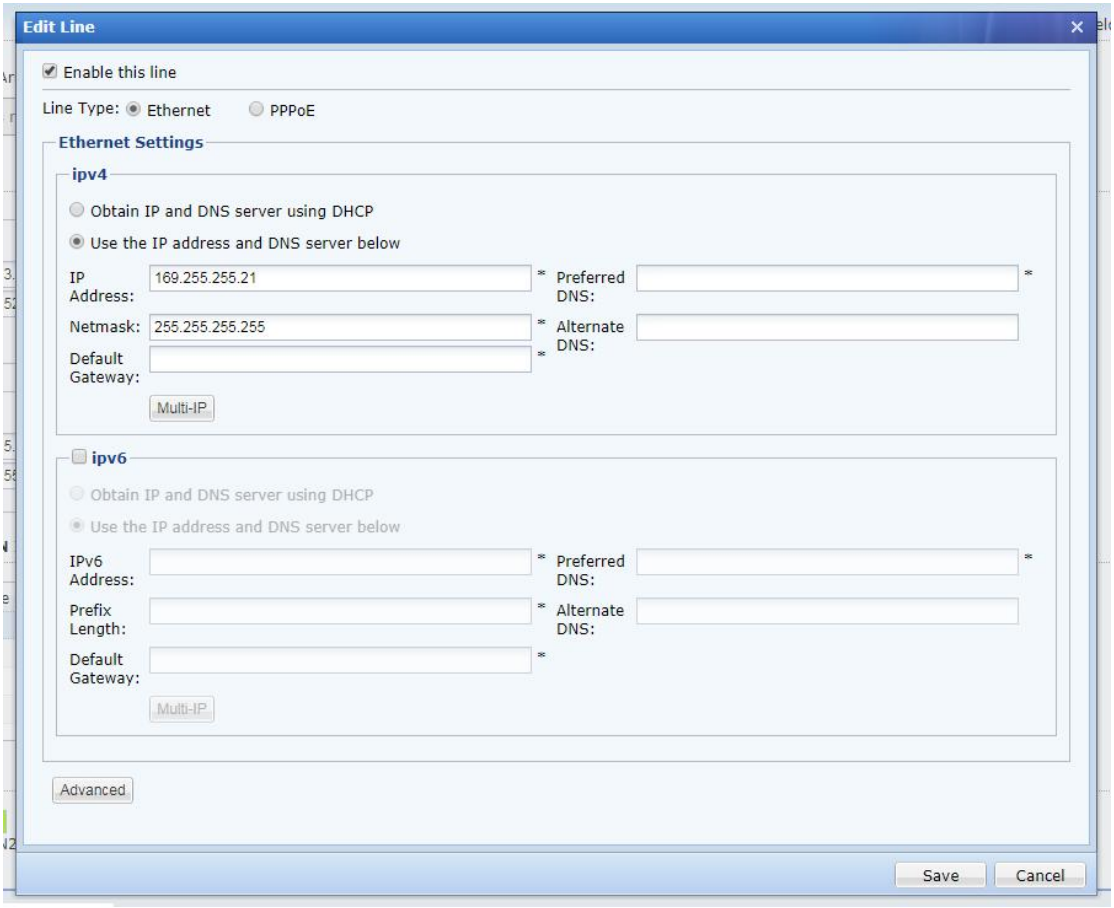
- **Preferred DNS:** Configures the primary DNS server.
- **Alternate DNS:** Configures the secondary DNS server.

If **Gateway** mode is selected, the **Deployment** page is as shown in the figure below:



The following are the contents included on the **Deployment** page when **Gateway** is selected:

- **(LAN) IP Address:** Configures the IP address of the internal interface, **LAN**. This IP address must be identical as the physical LAN interface IP of the Sangfor device.
- **Netmask:** Configures the netmask of the LAN interface IP.
- **(DMZ) IP Address:** Configures the IP address of the internal interface, **DMZ**.
- **Netmask:** Configures the netmask of the DMZ interface IP.
- **Link Status:** Indicates the connection status of internal and external interfaces of the Sangfor device, whether the network cables are plugged in.
- **External Interfaces:** External interfaces are WAN interfaces of the Sangfor device. To set a WAN interface, click on the name and the attributes of the corresponding Internet line appears, as shown in the figure below:

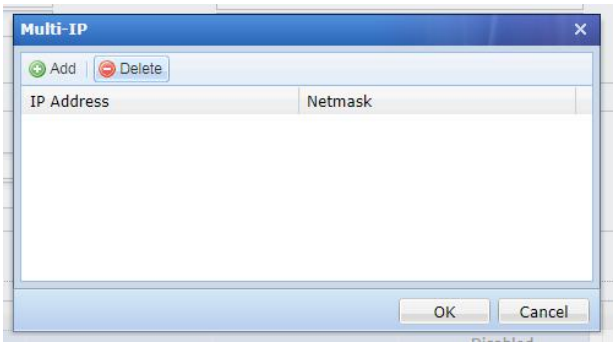


The following are the contents included on the **Edit Line** page, when line type is **Ethernet**:

- **Enable this line:** Select this option and this line will be enabled.
- **Line Type:** Options are **Ethernet** or **PPPoE**.

  If line type **Ethernet** is selected, the fields under **Ethernet Settings** should be configured, so that the Internet line would be assigned IP address and DNS server.

  IP address and DNS server could be assigned automatically or configured manually. The former is achieved by selecting the option **Obtain IP and DNS server using DHCP**, and the latter means that administrator needs to select the option **Use the IP and DNS server below** and configure the IP address, default gateway and DNS servers.
- **Multi-IP:** This button is only available for **Ethernet** type of Internet line, which means multiple IP addresses can be set on WAN interface. Click this button and the following dialog pops up, as shown below:

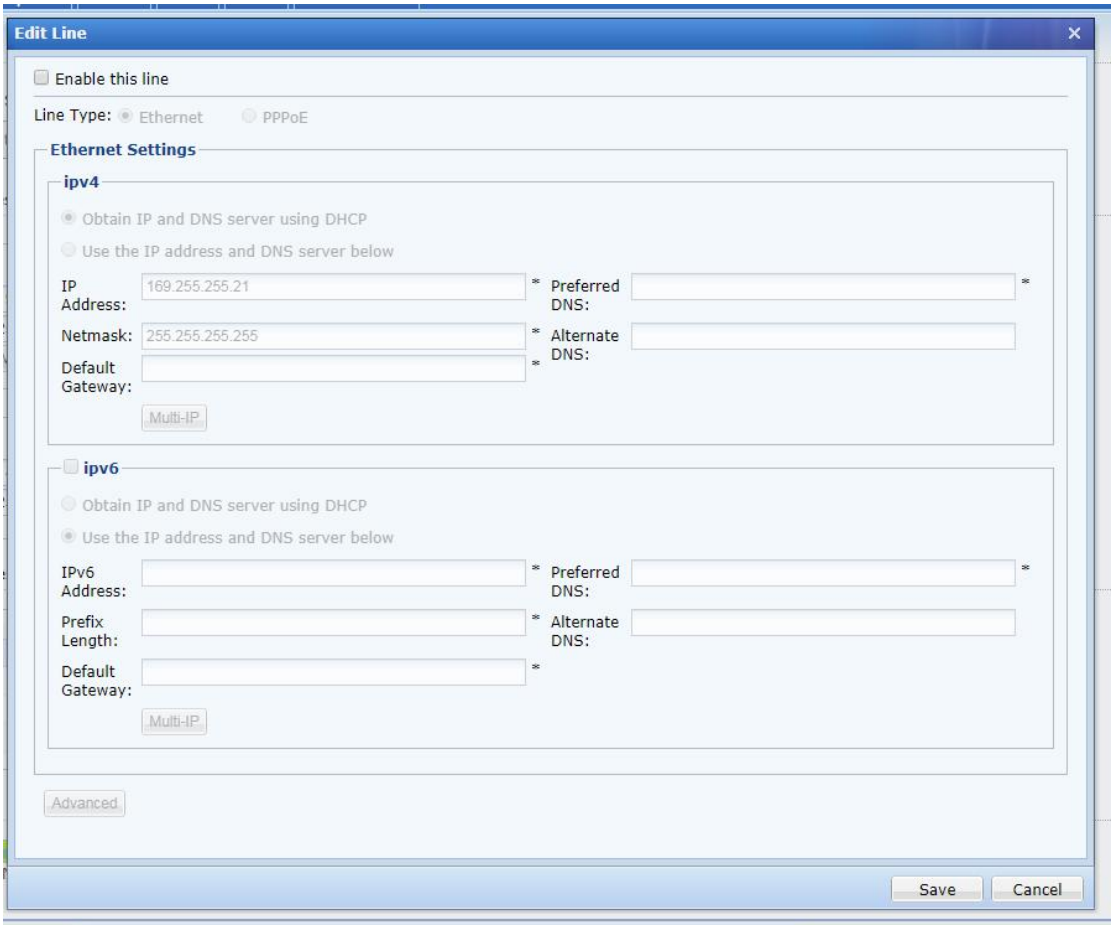


To add a new IP address entry, click **Add**.

To remove an IP address from the list, select the desired entry and click **Delete**.

In gateway mode, LAN, DMZ, and WAN interfaces cannot be configured on the same subnet. For the LAN interface in gateway mode, IPv4 is mandatory, and IPv6 is optional.

If line type **PPPoE** is selected, the fields under **PPPoE Settings** should be configured, as shown in the figure below:



- **Username, Password:** Configure the ADSL account to get dialup access.
- **Automatically connect:** Select the checkbox next to this option if Sangfor device automatically dials up when Internet connection is dropped.

  The changes apply after settings are saved (click the **Save** button) and services restart. Once the changes have applied, go to this page again to and click the **Connect** button to dial up immediately.

  For detailed information of dialup, click **Details**.
- **Options:** Click this button to enter the **PPPoE Properties** page and configure the parameters for dialup, such as handshake time, timeout, and max tries. Defaults are recommended to be adopted.

Note: ADSL dial-up does not support obtaining IPv6 addresses.

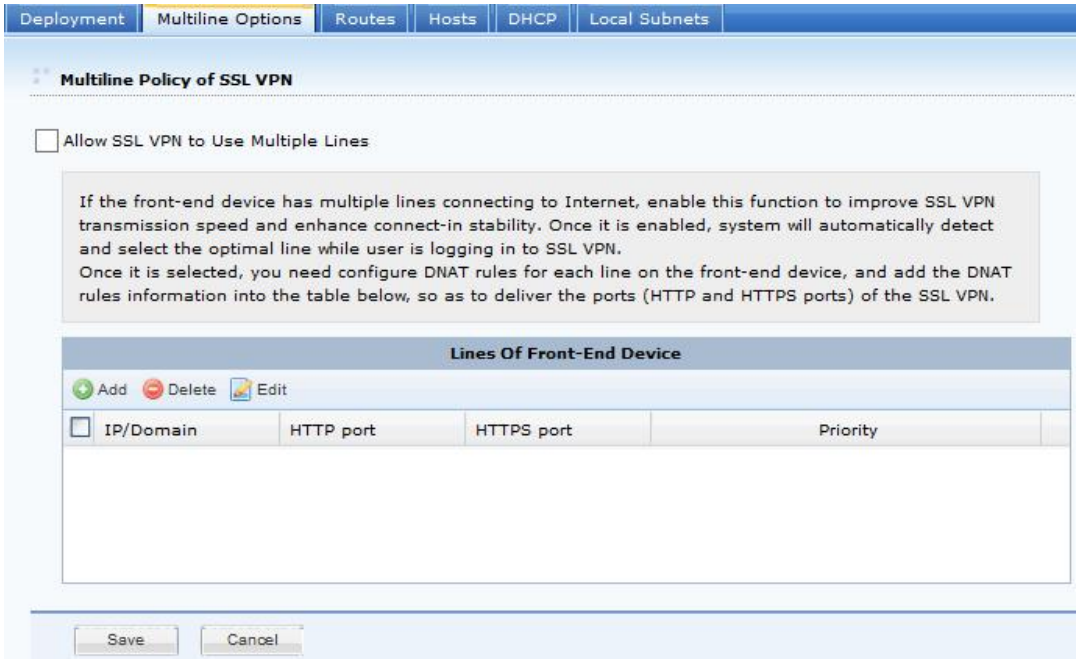
Note: DHCP automatically obtaining IP supports obtaining IPv4 address and IPv6 address.

Setting Multiline Options

If the Sangfor device needs more than one lines to connect to its WAN interfaces (including the case that Sangfor device is deployed in **Single-arm** mode), multiline policies should be enabled and configured, more exactly, all the internet lines should be configured.

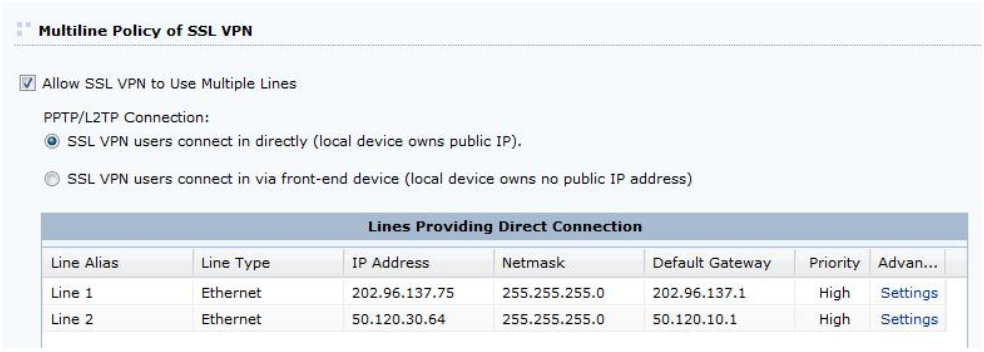
1. Navigate to **System** > **Network** > **Multiline Options** to configure the multiline options.

   The **Multiline Options** page is as shown below, when deployment mode is **Single-arm**:



   The **Multiline Options** page is as shown below, when deployment mode is **Gateway**:

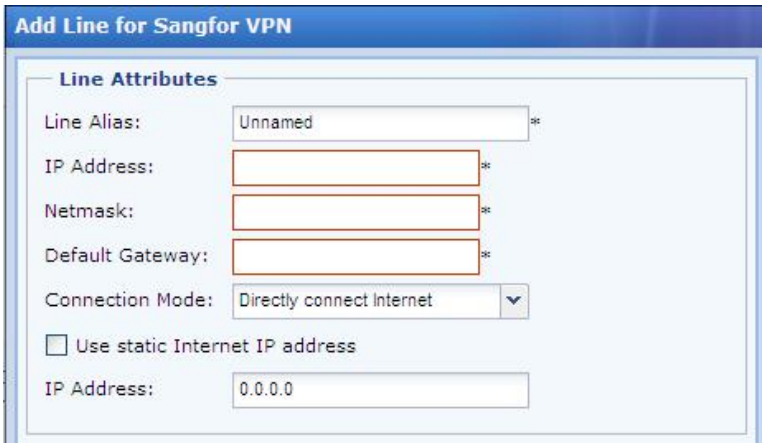




2. Configure **Multiline Policy of Sangfor VPN**.

   - **Allow Sangfor VPN to Use Multiple Lines:** Select this option to enable the multiline policy of Sangfor VPN, the configured Internet lines will be available for users' access to Sangfor VPN.

     To add a line, click **Add**. The following figure shows the **Add Line for Sangfor VPN** page while the deployment mode is **Gateway**:



     Name the line, enter the IP address and gateway and specify whether or not this line uses a static IP address. If the line is to use a static Internet IP address, configure **IP Address** field.

   - **Enable extranet connection detection:** Select this option and configure **Interval**, and connection status of this line will be detected periodically.

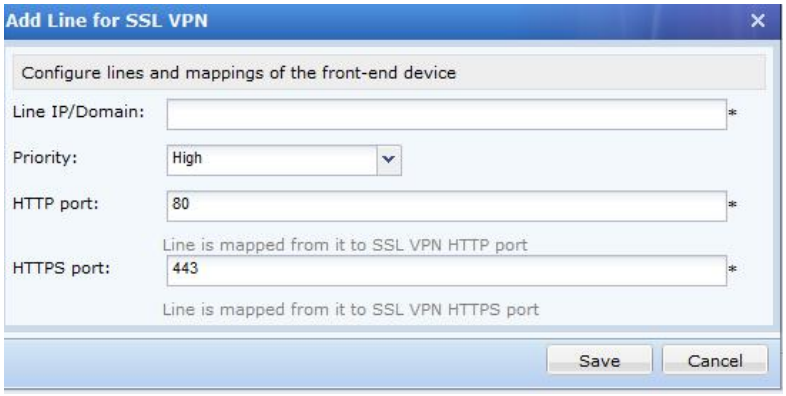
3. Configure **Multiline Policy of SSL VPN**.

   - **Allow SSL VPN to Use Multiple Lines:** Select this option to enable the multiline policy of SSL VPN, if the SSL VPN is to use multiple lines. Then add the lines into the line list, as shown below:



Once multiline policy of SSL VPN is enabled, the line selection policy will help the system automatically detect the lines and choose the optimal one to let the user connect in faster when it accesses the SSL VPN, improving the data transfer and stability of SSL VPN connections.

- **SSL VPN users connect in directly(local device owns public IP):** If Sangfor device is deployed in gateway mode, and owns public IP, then VPN user can connect it directly.
- **SSL VPN users connect in via front-end device(local device owns no public IP address):** If Sangfor device is deployed on Intranet and does not own public IP, then VPN users connect in via front-end device.
- If the Sangfor device is deployed in gateway mode and **SSL VPN users connect in via front-end device(local device owns no public IP address)** option is selected, and needs to use multiple Internet lines, map front-end network device's public addresses to the Sangfor device and launch the ports, simply by configuring port mapping rules under **Lines Of Front-End Device**. To do that, click **Add** to enter the **Edit Line for SSL VPN** page, as shown below



Configure the fields included on the **Add Line for SSL VPN** page:

- **Line IP/Domain:** Specifies the IP address or domain name of the Internet line.
- **Priority:** Specifies the priority of this line. The higher the priority is, this line is more likely to be used.
- **HTTP Port:** Specifies the HTTP port of the front-end device that is to be mapped

to the Sangfor device.

- **HTTPS Port:** Specifies the HTTPS port of the front-end device that is to be mapped to the Sangfor device.

- Click **Settings** to specify line priority and select whether to eliminate security certificate alert, as shown below:



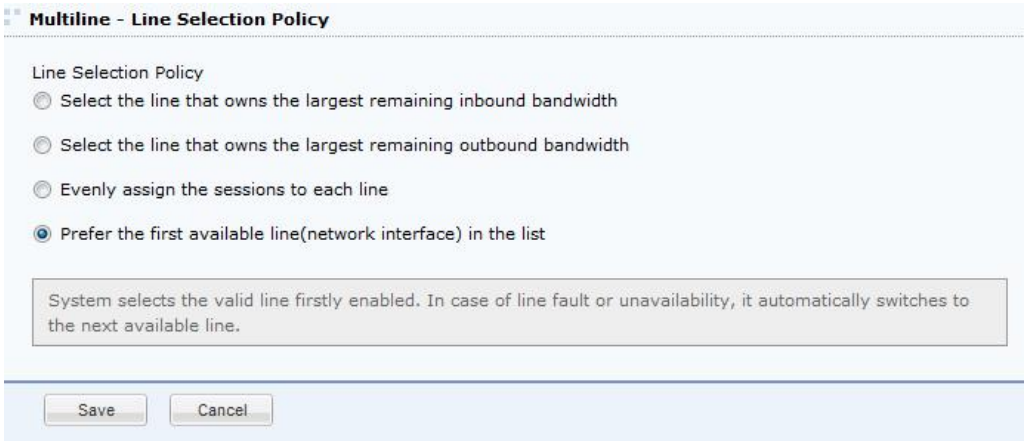
If **Eliminate security certificate alert** is selected, you need to specify domain name of the line, browser will not prompt certificate security alert any more when user visits SSL VPN login page.



If the login policy selected is **Users use different login pages** (under **System** > **SSL VPN Options** > **Logging in** > **Login Policy**), multiline policy of SSL VPN is disabled by default and unavailable, which means SSL VPN cannot use multiple lines.

4. Configure the **Line Selection Policy** which will apply to the Internet access data sent from/to computers in the local area network and handled by the Sangfor device.

   This is available when Sangfor device is deployed in **Gateway** mode, as shown below:



The following are the four line selection methods:

- **Select the line that owns the largest remaining inbound bandwidth:** Indicates that the system will automatically select the line that owns the largest remaining inbound bandwidth, to make full use of the remaining bandwidth.
- **Select the line that owns the largest remaining outbound bandwidth:** Indicates that the system will automatically select the line that owns the largest remaining outbound bandwidth, to make full use of the remaining bandwidth.
- **Evenly assign the sessions to each line:** Indicates that the system will evenly assign the sessions to each line automatically, without considering the remaining bandwidth.
- **Prefer the first available line(network interface) in the list:** Indicates that the system will select the valid line that has been firstly enabled. In case that line fault or unavailability appears, it automatically switches to the next available line.

5. Click the **Save** button and that **Apply** button to save and apply the settings.

For more detail about configuring multiple lines, refer to Device Deployment in Chapter 7.

Note: Multiline only supports IPv4 addresses and do not support IPv6 addresses.

Configuring Route

Route can route data of the Sangfor device itself, and route the data (either VPN data or VPN irrelevant data) to the Sangfor device, which then will forward the data to destination. To add a new route, perform the steps below:

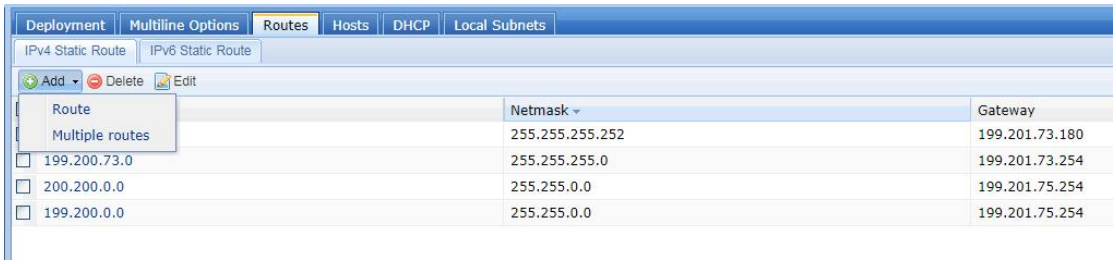
1. Navigate to **System** > **Network** > **Routes** to enter **Routes** page, as shown below:



Routes include IPv4 static routes and IPv6 static routes.

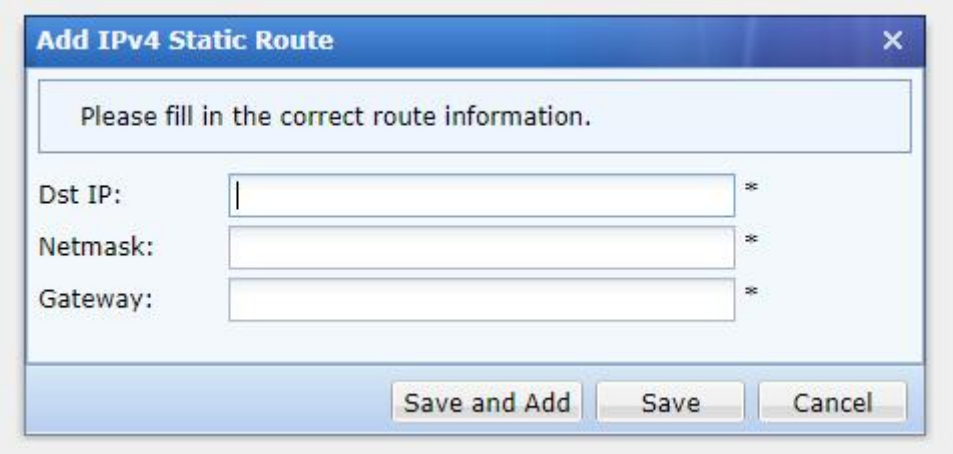
On the IPv4 static route module, click **Add** and select **[Routes]** and **[Multiple routes]**, as shown in the following figure:

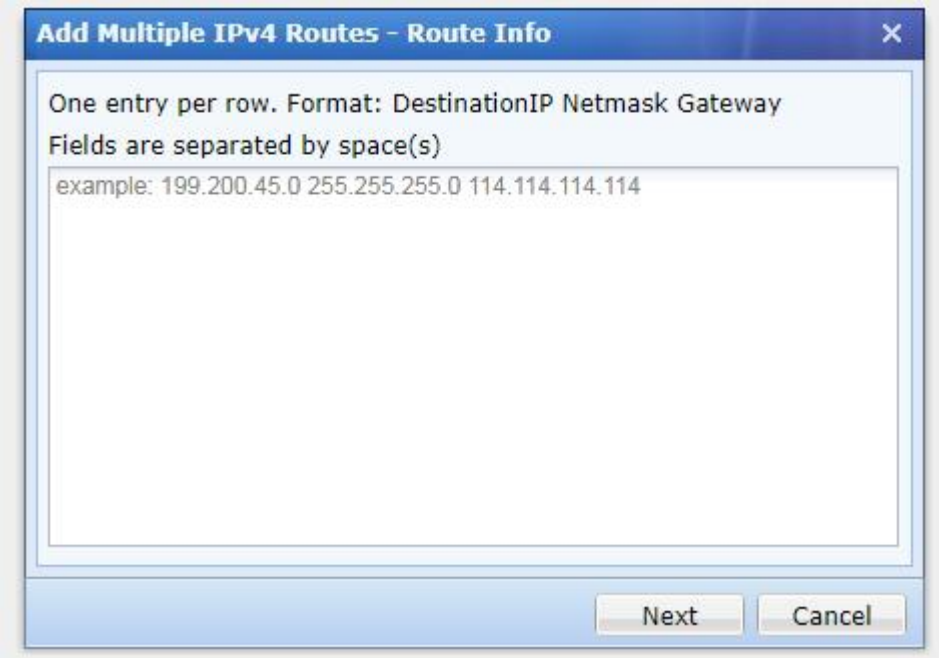
2. Click **Add** > **Routes** or **Multiple routes** to add a single route or a batch of routes, as shown below:



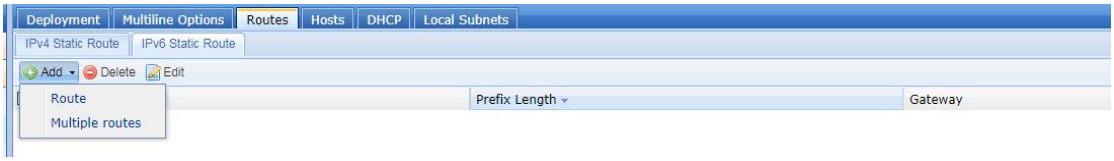
3. Enter the destination subnet, network mask and gateway. The following two figures show the two cases of adding a single route and a batch of routes.

Select **[Add route]** to add a route, as shown in the following figure:

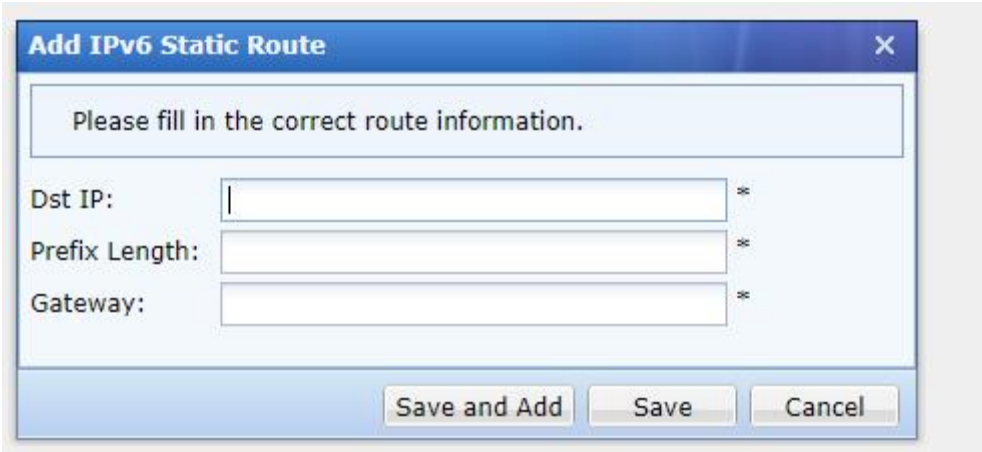




On the IPv6 static route module, click Add and select [Route] and [Multiple routes], as shown in the following figure:



Select [Add route] to add a route, as shown in the following figure:



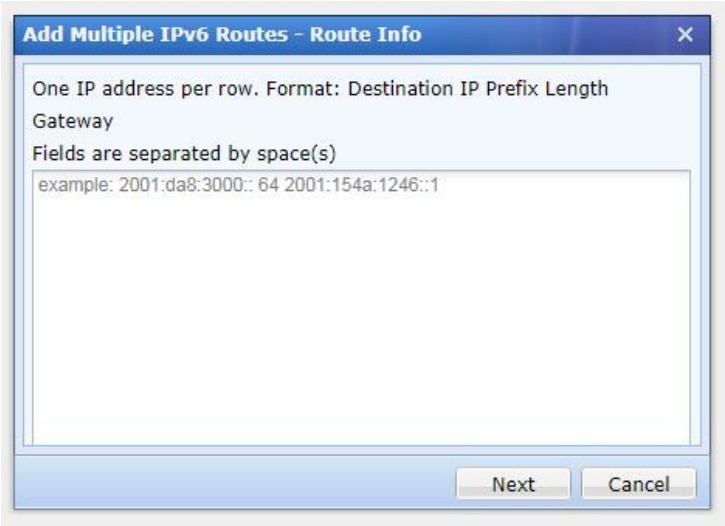
[Dst IP] is the destination address segment to which the route points.

[Prefix Length] is subnet mask of the destination address segment.

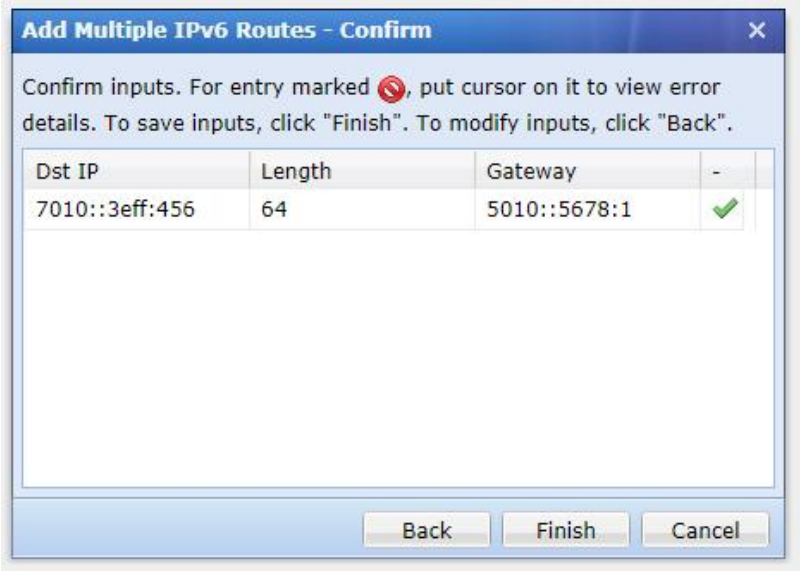
[Gateway] is the next hop of address to the destination address segment.

Click Save and Add to add more routes.

Click Save to save the configuration.



Click Next to confirm whether the route information is correct. If yes, click Finish to save the configuration. As shown in the following figure:

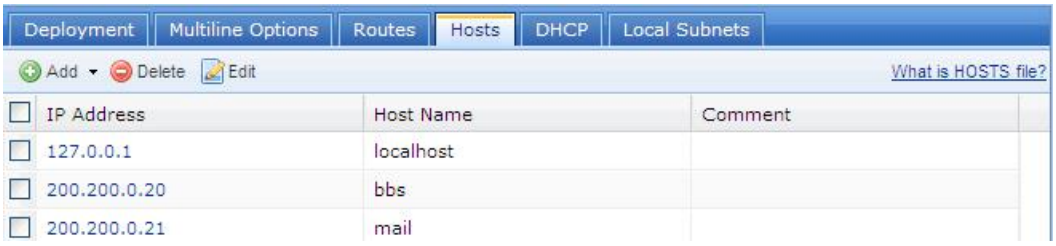


Configuring Host Mapping Rule (HOSTS)

HOSTS file is the built-in host file (more specifically, the mapping information of the IP addresses and domain name/hostnames) on the Sangfor device. This file works when SSL VPN users need to access Web resources using domain name or host name, generally in the situation that the internal network (where the Sangfor device resides) is using MS Active Directory.

To add a new Host entry or a batch of Host entries:

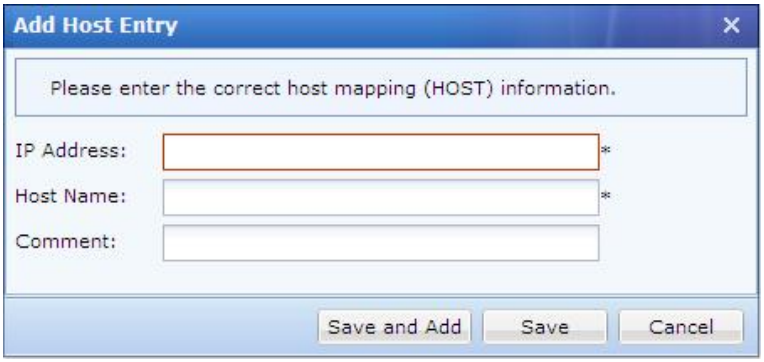
1. Navigate to **System** > **Network** > **Hosts** to enter **Hosts** page, as shown below:



2. Click **Add** > **Host entry** or **Multiple host entries**, as shown below:



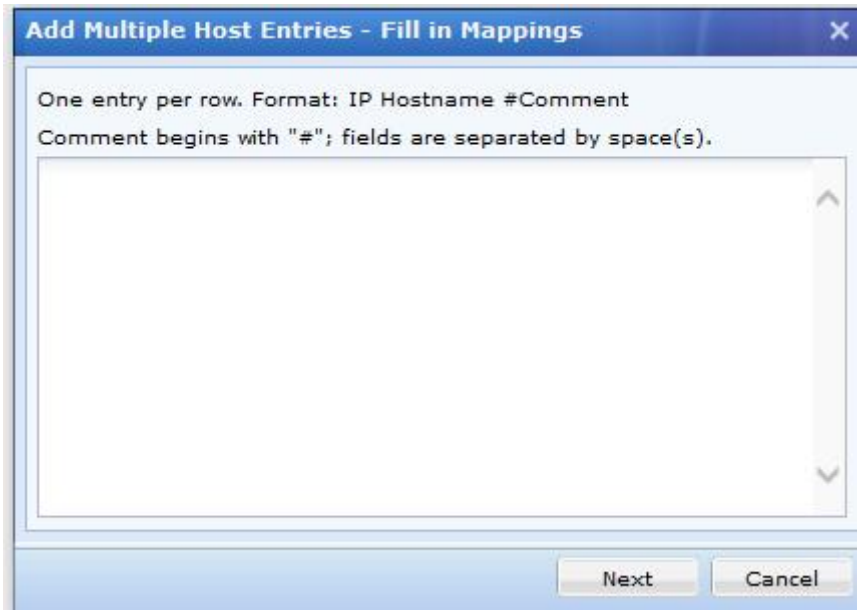
If **Host entry** is selected, the page pops up as follows. Specify the fields on this page.



The following are the contents included on the **Add Host Entry** page:

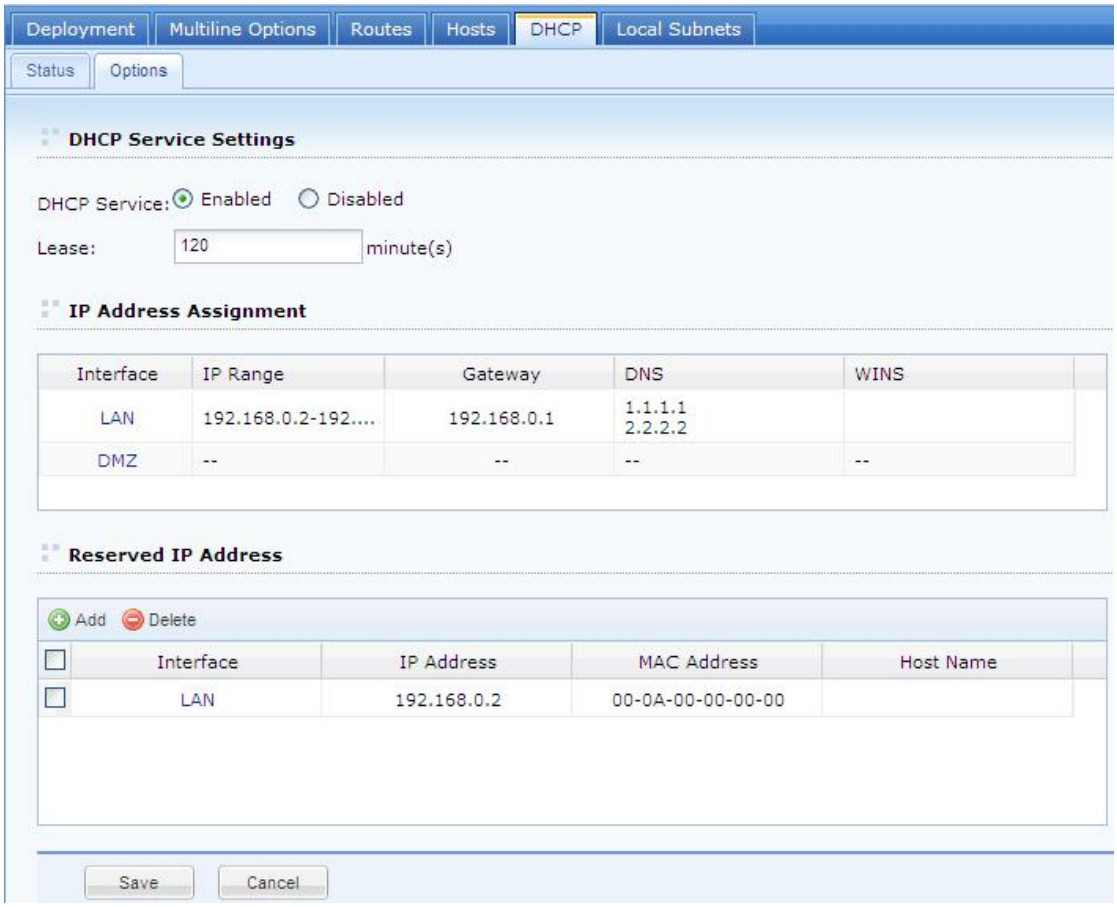
- **IP Address:** Indicates the IP address of the server providing resources.
- **Host Name:** Indicates the host name of the server providing resources.
- **Comment:** Description to this host mapping rule.

If **Multiple host entries** is selected, the pop-up page is as shown below. Enter the IP address and domain into the text box in the format as required.



Configuring IP Assignment Options (DHCP)

Navigate to **System** > **Network** > **DHCP** > **Options** to view **Status** of DHCP service and configure the **Options**. **Status** tab shows the running status of the DHCP service, the IP addresses that are assigned through each network interface, the related hostname, MAC address, and lease time left; while **Options** tab contains the DHCP related settings, as shown below:

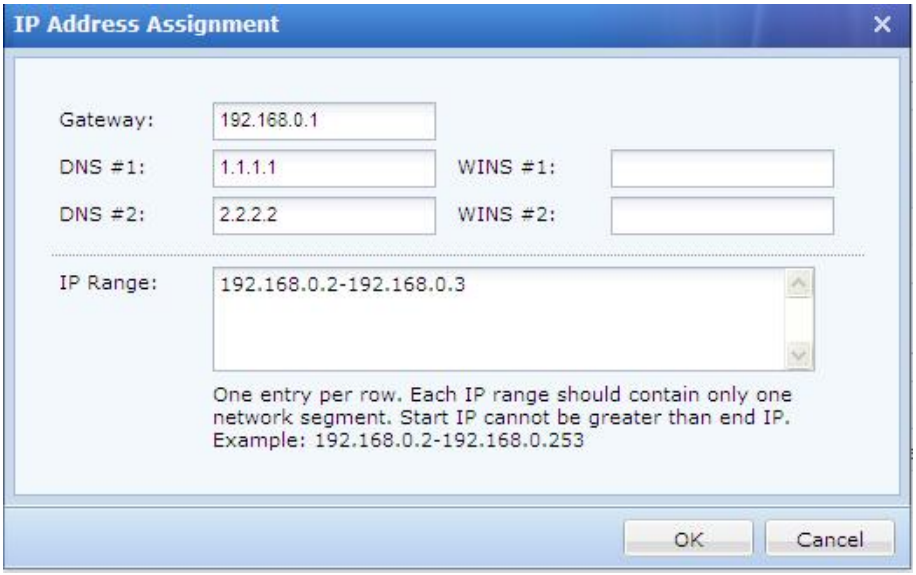


The following are the contents included on **Options** tab:

- **DHCP Service:** Click **Enabled** or **Disabled** to enable or disable the DHCP service.
- **Lease:** Indicates the DHCP IP address lease, the life cycle that an assigned IP address will be used by the corresponding user.
- **IP Address Assignment:** Configure the IP address range that can be assigned to the SSL VPN users by each interface.

  To view and assign IP address to a network interface, perform the steps below:

  1. Click on the name of a network interface to enter the **IP Address Assignment** page;
  2. Configure the IP range, gateway and DNS server address, as shown below:

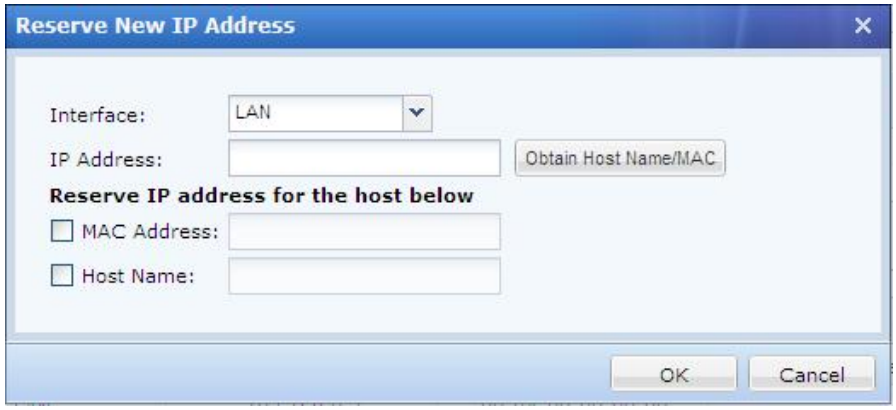


3. Click the **OK** button to save the settings.

- In case that some LAN computers are using static private IP addresses, the IP address range configured above should not cover any of those static IP addresses, otherwise, IP address conflict will occur after those IP addresses are assigned to VPN users automatically.
- Generally, the IP address range configured above should not cover the first and the last IP address of a network segment, for these two IP addresses are network address and broadcast address of a network segment. The correct input is like 192.168.1.1 -192.168.1.254.

Note: It only supports setting up the IPv4 DHCP server to assign IPv4 addresses to users, and does not support IPv6.

- **Reserved IP Address:** The address is reserved IP address (range) for specific host. To reserve IP address for a user, click **Add** to enter the **Reserve New IP Address** page, as shown below:



The fields on this page are described as follows:

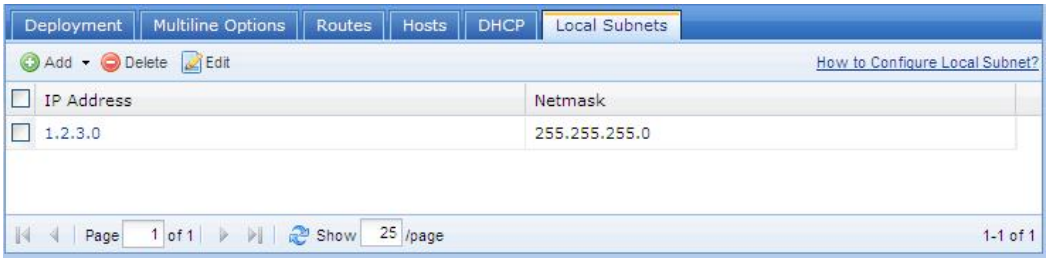
- **Interface:** Specifies the network interface of this DHCP rule.
- **IP Address:** Specifies the IP address that to be reserved for certain computer. The reserved IP address will not be assigned to VPN users.
- **Obtain Host Name/MAC:** Click this button to obtain the MAC address and host name of the host for which this IP address is reserved.
- **MAC Address:** Specifies MAC address of the host which the IP address is reserved for.
- **Host Name:** Specifies the name of the host which the IP address is reserved for.

Configuring Local Subnet

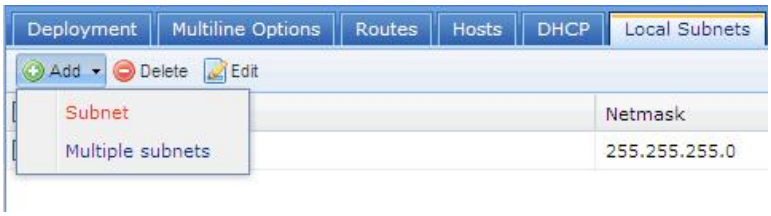
Local subnets are subnets thought in the LAN where this Sangfor device resides. Configuring local subnet is intended for the case that the VPN users want to communicate with the other subnets of the headquarters (HQ) network.

Assume that the HQ has two subnets (192.200.200.x and 192.200.254.x); the subnet 192.200.200.x is a network segment that is directly connected to the Sangfor device, while the subnet 192.200.254.x is indirectly connected to the Sangfor device. To add a local subnet entry,

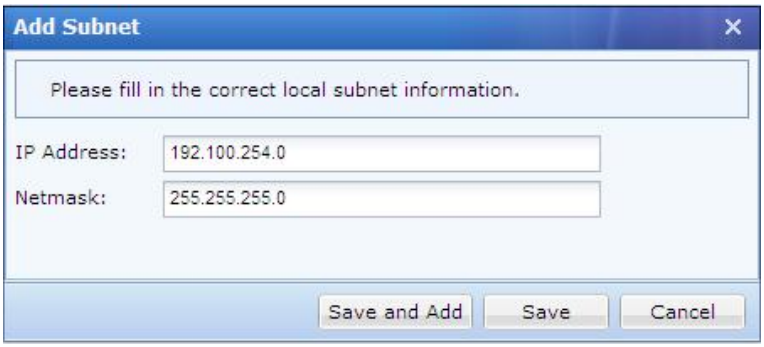
1. Navigate to **System** > **Network** > **Local Subnets** to enter **Local Subnets** page, as shown below:



2. Click **Add** > **Subnet** or **Multiple subnets**, as shown below:

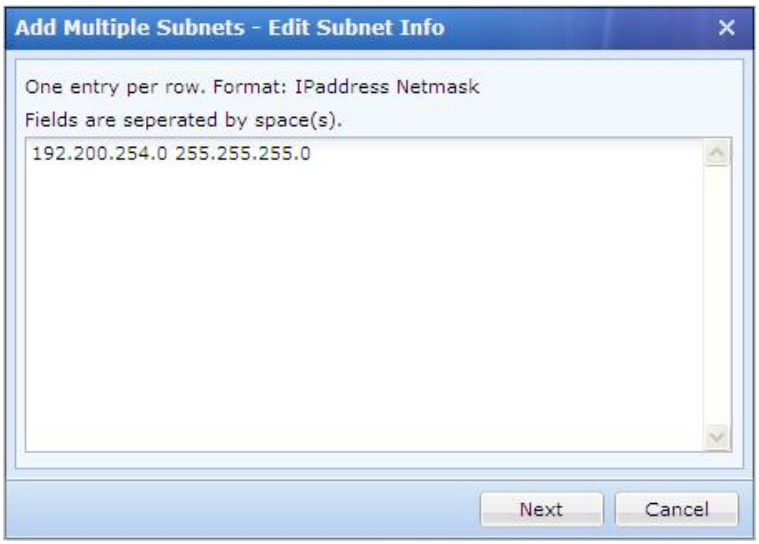


If **Subnet** is selected, the **Add Subnet** page appears. Configure the subnet, as shown below:



Since the subnet 192.200.254.x indirectly connects to the Sangfor device (which resides in a different network segment), enter the IP address and netmask into the corresponding fields and then click the **Save** button.

If **Multiple subnets** is selected, one subnet or multiple subnets can be added at one step. The **Add Multiple Subnet – Edit Subnet Info** page is as shown in the figure below:



Note: The local subnet only supports adding IPv4 addresses and does not support adding IPv6 addresses.

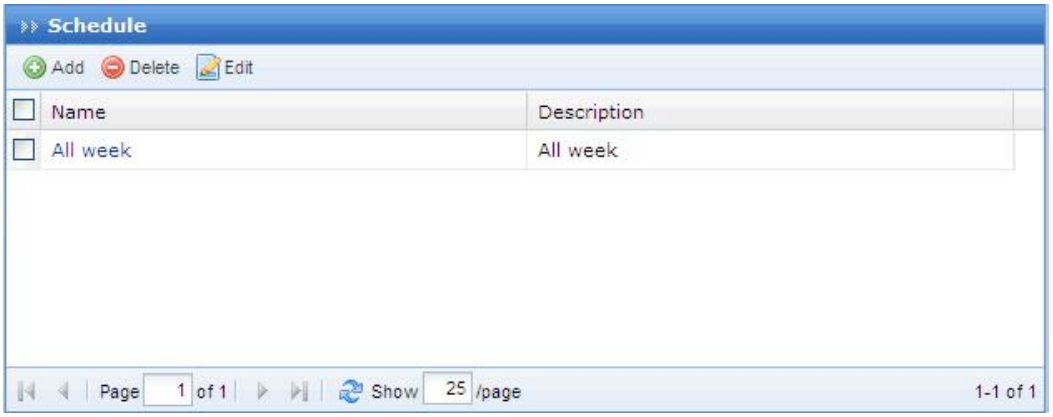
- The local subnets are deemed as network segments of VPN by the Sangfor device and the client software, which means all the data sent from (or to) these network segments through the Sangfor device or software will be encapsulated into and transmitted through the VPN tunnels. For this reason, if you want to allow the VPN users to access certain subnet, add the related subnet into the list on the **Local Subnets** page and then go to the **Routes** page to configure a corresponding route.
- When adding subnet, you can add the network segment overlapping with that in which the LAN interface of Sangfor device resides. When corresponding policy is distributed, the overlapped network segment will be discarded, in order to ensure normal communication.

Schedules

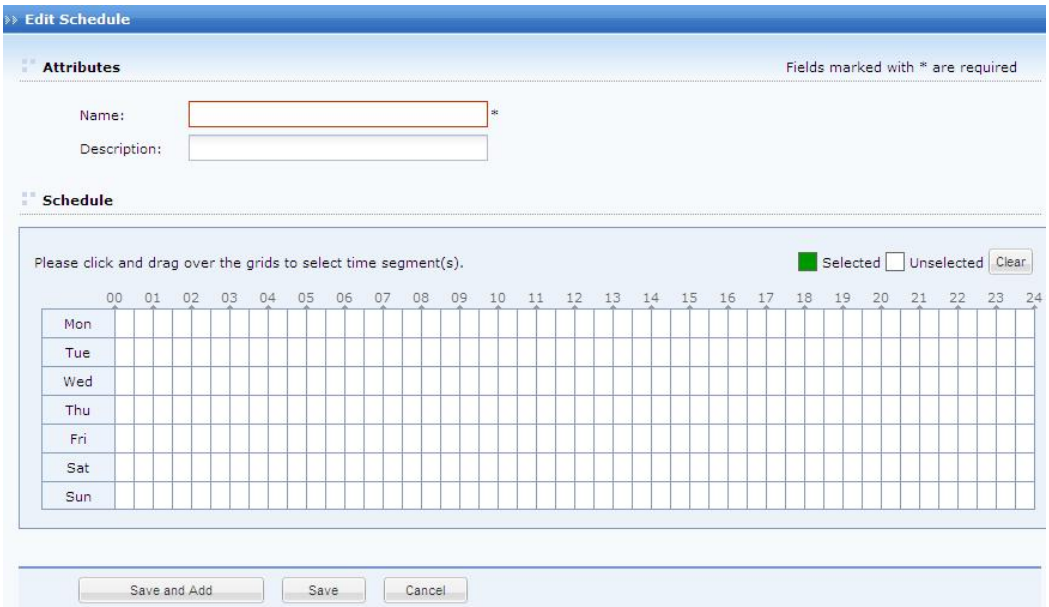
A schedule is a combination of time segments, which can be referenced by SSL VPN account settings, firewall filter rules, user privilege settings and endpoint security rules. The date and time are based on the system time of the Sangfor device.

To create a schedule, for example, named **Office hours** that consists of time segments 8: 00-12: 00 and 14: 00-18: 00, from Monday to Friday:

1. Navigate to **System** > **Schedule**, as shown in the figure below:

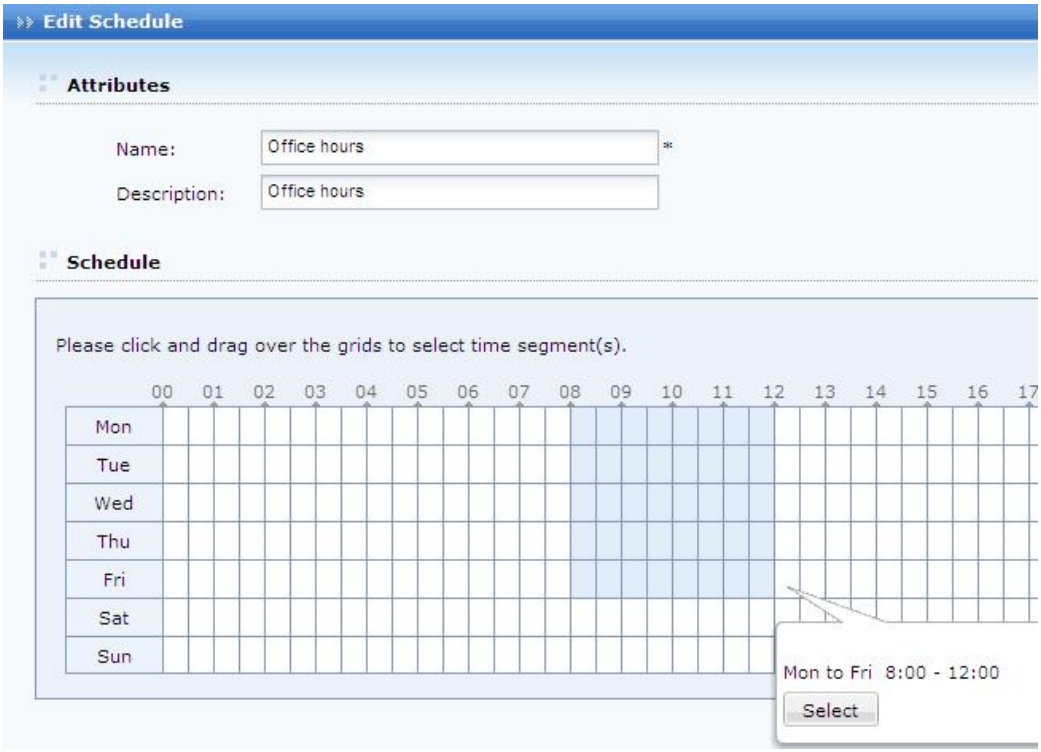


2. Click **Add** to add a new schedule, as shown below:

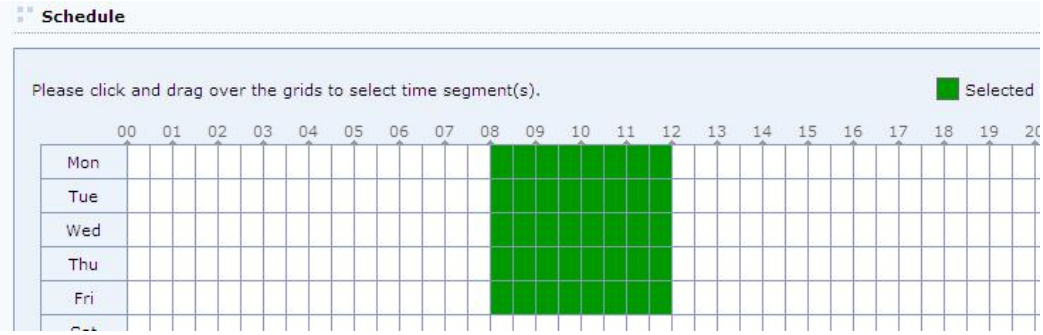


3. Enter the name into the **Name** field (in this scenario, it is **Office hours**). Description is optional.

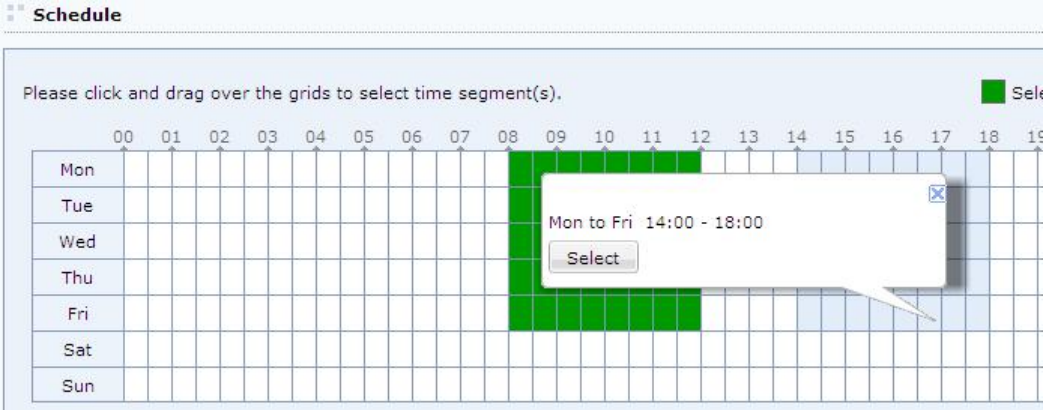
4. Click and drag over the grids to select the desired time segment (8: 00-12: 00, from Monday to Friday). A prompt dialog will display the exact time segment selected, as shown below:



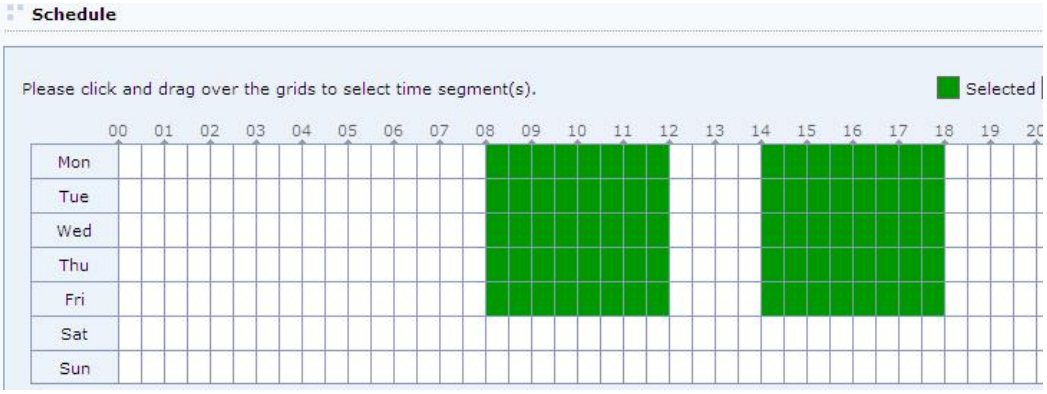
5. Click the **Select** button to select the time segment, as shown below:



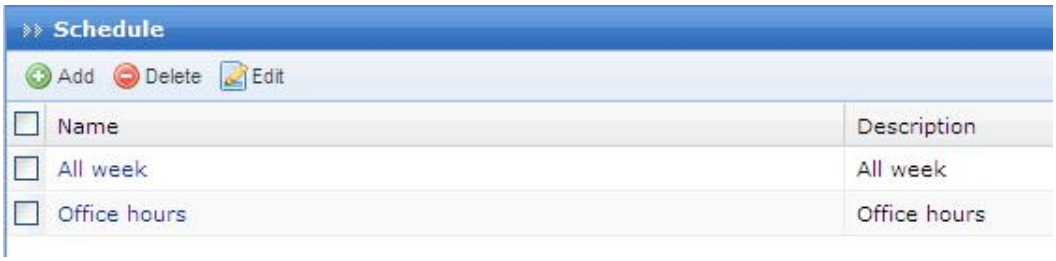
6. Go on to select the other time segment (14: 00-18: 00, from Monday to Friday) in the same way, as shown below:



7. Click the **Select** button to select the time segment, as shown below:

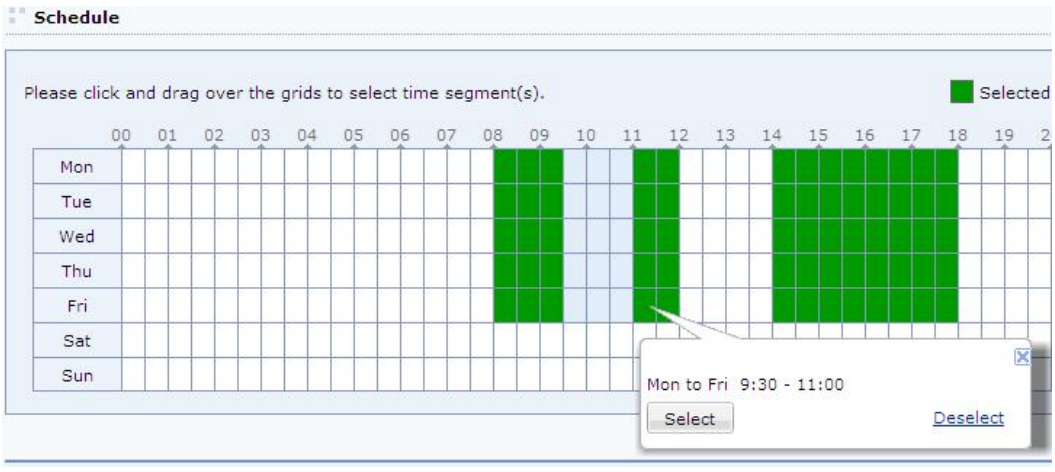


8. Click **Save** to save the settings on this page. The newly-created schedule will show in the schedule list, as shown below:



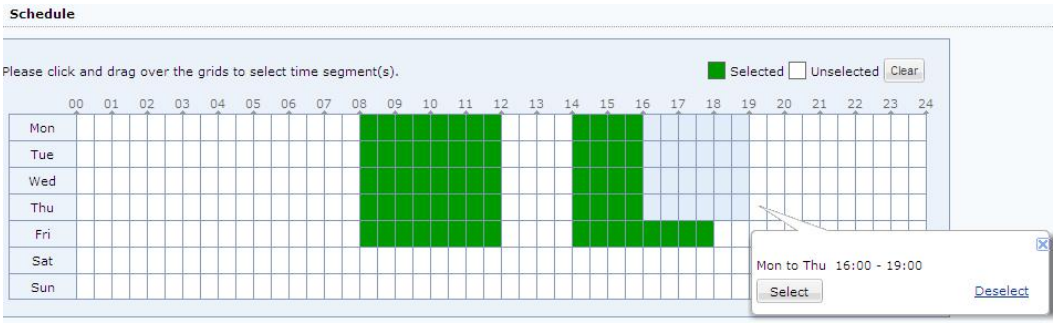
To deselect and remove a time segment from the schedule, perform the steps below:

1. Click on and drag over the green grids (selected time segments) to select the time segment that you want to deselect. A prompt dialog will display the exact time segment selected, as shown below:

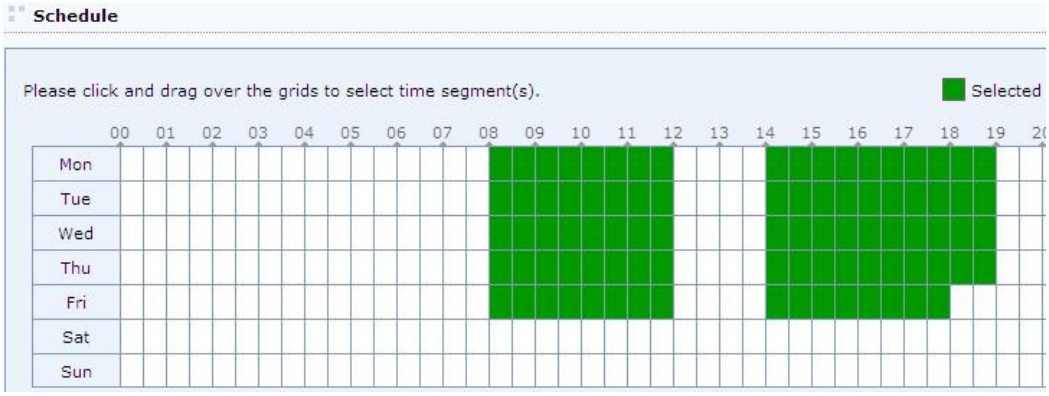


2. Click **Deselect** to deselect the time segment that has turned to light blue (while green grid indicates that the time segments are selected, and white grid indicates that the time segments are unselected).

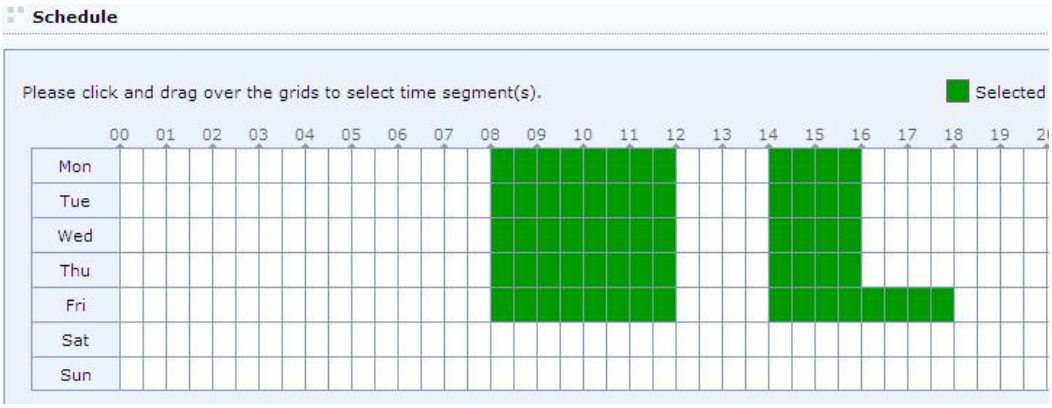
3. In case that the selected time segment (in green) and the desired time segment (in light blue) lap, as shown below:



- To select this part, click the **Select** button, and the grids in light blue (including the overlapped part) will turn to green, being selected, as shown below:



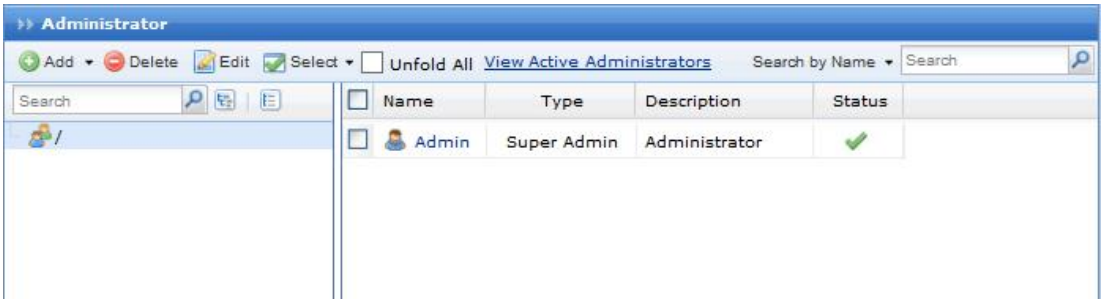
- Or click **Deselect**, the grids in light blue (including the overlapped part) will turn to white, being removed, as shown below:



Administrator

Through administrator management feature, super administrator of the Sangfor device can create administrators for others to maintain the SSL VPN server.

An administrator can be put into certain group and so be granted with restricted administrative privileges. The **Administrator** page is shown in the figure below:



The following are some contents included on **Administrator** page:

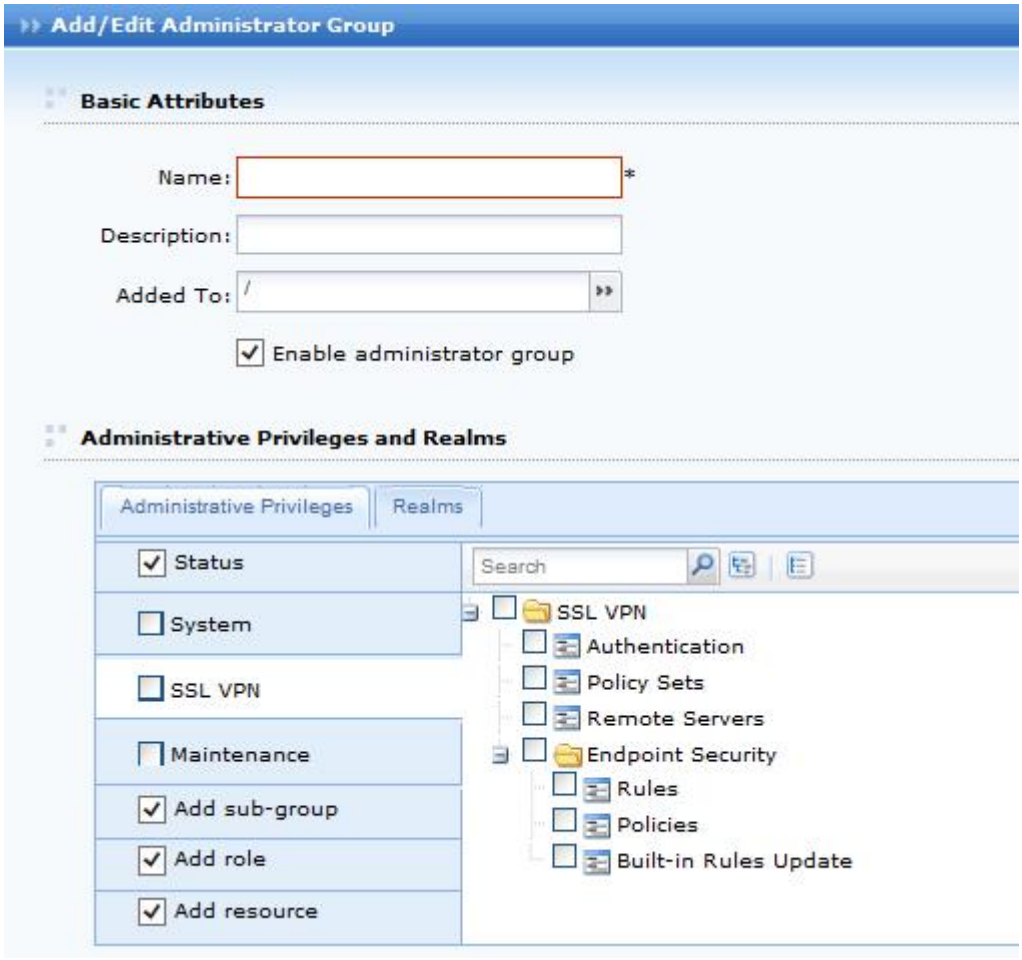
- **Unfold All:** Select the checkbox next to it and the subgroups and individual administrators of the selected administrator group (in the left pane) will be seen on the right pane.
- **Edit**, **Delete:** To edit or delete an administrator or administrator group, select that administrator or administrator group and click **Edit** or **Delete**.
- **View Active Administrators:** Click this link to view the administrators that are accessing the administrator Web console currently.

Adding Administrator Group

1. Click **Add** > **Admin group** to enter **Add/Edit Administrator Group** page, as shown below:



2. Configure **Basic Attributes** and **Administrative Privileges and Realms** of the administrator group, as shown below:



The following are the information of administrator group:

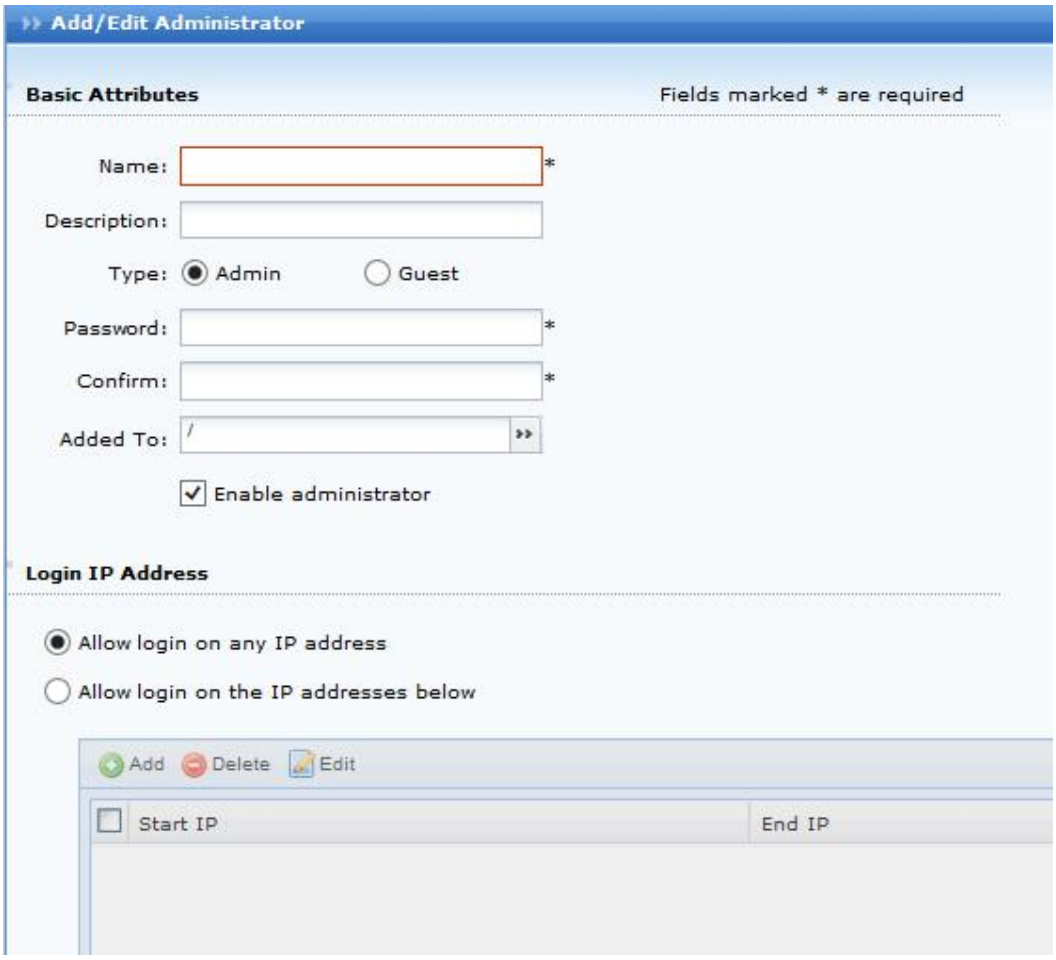
- **Name:** Specifies the username of the administrator group.
- **Description:** Descriptive information of the administrator group.
- **Added To:** Specifies the administrator group to which this administrator group will be added. This group determines the administrative privileges and realms of this administrator group.
- **Administrative Privileges:** Specifies the configuration modules that the administrator in this group could maintain. Select the checkbox next to each module name and the administrators in this administrator group will be authorized to configure that module.
- **Realms:** Specifies the administrative realms (users, resources and roles) for the administrators in this administrator group, as shown below:



3. Click the **Save** button to save the settings.

Adding Administrator

1. Click **Add** > **Admin** to enter **Add/Edit Administrator** page, as shown below:
2. Configure **Basic Attributes** and **Login IP Address** of the administrator, as shown below:



The following are the information of administrator:

- **Name:** Specifies the username of the administrator account that can used to log in to the administrator console of SSL VPN.
- **Description:** Descriptive information of the administrator account.
- **Type:** Specifies the account type. Options are **Admin** and **Guest**. Administrators of **Admin** type have the specified administrative privileges to configure some modules through the administrator console; while the administrators of **Guest** type only have read-only privilege to view the configurations of modules that are specified for that administrator group.
- **Password**, **Confirm:** Respectively specifies and confirms password of the account that is used by administrator to log in to SSL VPN administrator console.
- **Added To:** Specifies the administrator group to which this administrator account will be added. This group determines the administrative privileges and realms of this

administrator.

- **Login IP Address:** Specifies the IP address on which this account can be used by the administrator to log in to the SSL VPN administrator console.

3. Click the **Save** button to save the settings.



The administrator password is valid if it matches all the following:

- It must contain at least 8 characters.
- It cannot contain username of administrator.
- It must contain any two of the following: upper-case letters, lower-case letters, digits, special characters.



The administrative privilege of an administrator group will never be higher than its parent administrator group. That is to say, administrators' privilege of maintaining SSL VPN users, resources and roles is authorized by the parent group and will not be more or higher than that.

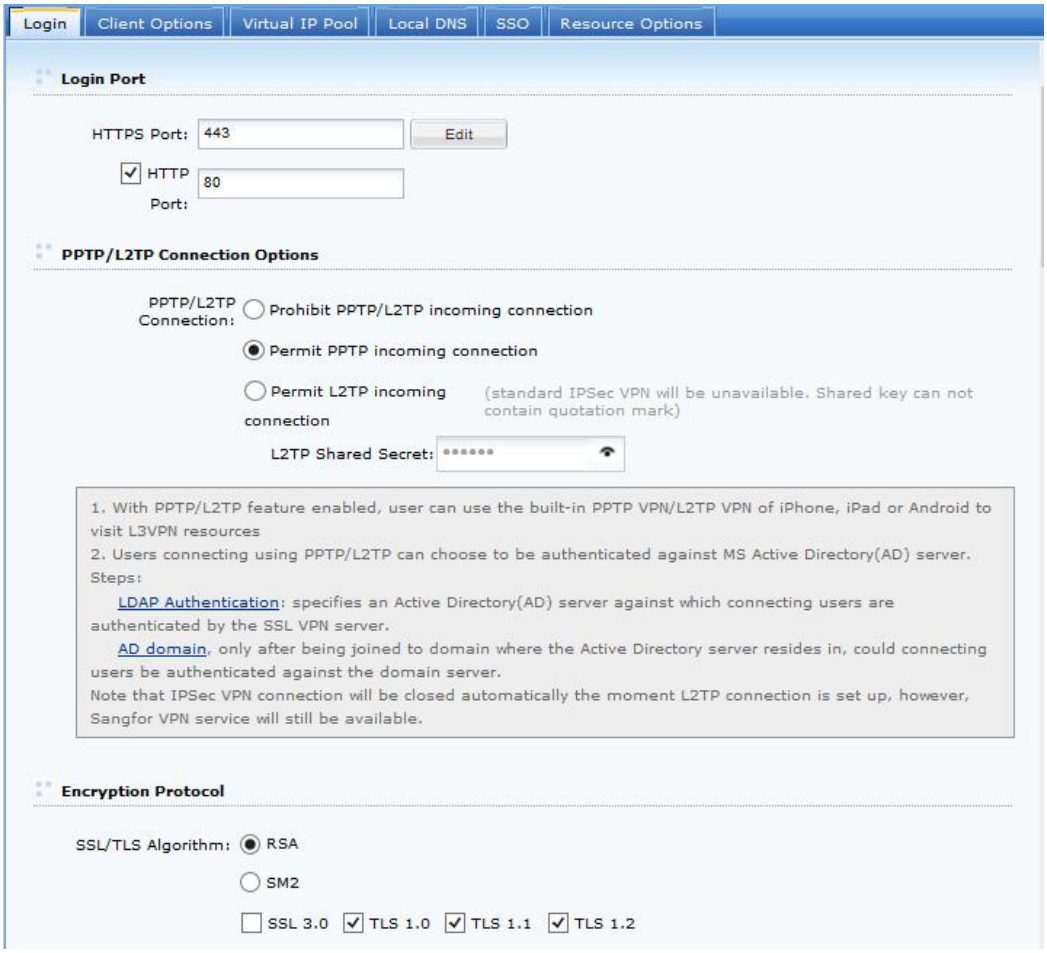
SSL VPN Options

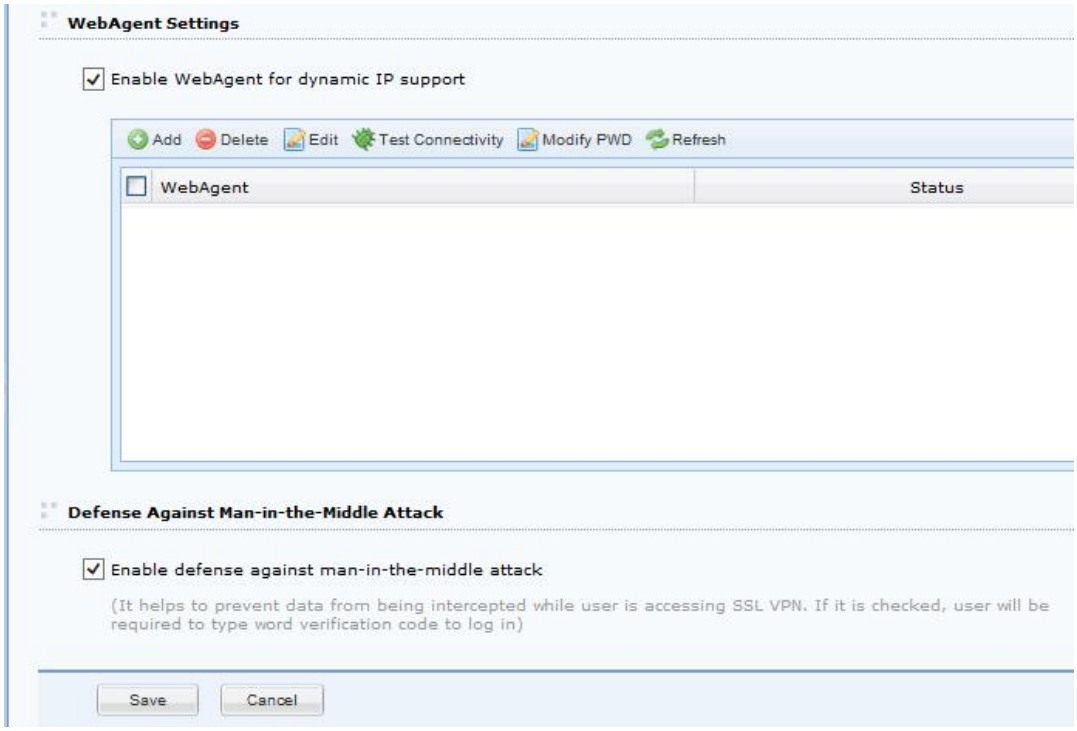
General Settings

The basic (SSL VPN related) settings under **System** > **SSL VPN Options > General** are global settings, including user login options, client options, virtual IP address pool, Single Sign-On (SSO) and resource options.

Configuring User Login Options

1. Navigate to **System** > **SSL VPN Options > General** > **Login**, as shown in the figure below:





2. Configure the following fields under **Login Port**.

   - **Login Port:** Specifies the HTTPS and HTTP port on which the SSL VPN service is being listened.
   - **HTTPS Port:** Specifies the HTTPS listening port. It is TCP 443 by default. Enter the port(s) into the field (ports should be separated by comma) or click the **Configure** button.
   - **HTTP Port:** Select this option and enter the HTTP listening port. It is TCP 80 by default.

3. Configure the following fields under **Login PPTP/L2TP Connection Options**.

   - **Prohibit PPTP/L2TP incoming connection:** If it is selected, PPTP/L2TP connection will be denied.
   - **Permit PPTP incoming connection:** Select it to allow PPTP incoming connection, and user can access L3VPN resources on mobile phone via VPN.
   - **Permit L2TP incoming connection:** Select it to allow L2TP incoming connection. If it is selected, you need to specify L2TP shared secret.
   - **L2TP Shared Secret:** Specifies L2TP shared secret, then user can access L3VPN resources on mobile phone via built-in L2TP VPN.

For users accessing VPN though PPTP/L2TP, they can be authenticated on MS Active Directory. To do that, you need to configure as follows:

a. Click **LDAP Authentication** to enter **Add/Edit LDAP Server** page, and configure LDAP server to make Sangfor device connect to this server.

b. Click **AD domain** to enter the **Client-side Domain SSO** page, enable SSO and configure required fields on that page.



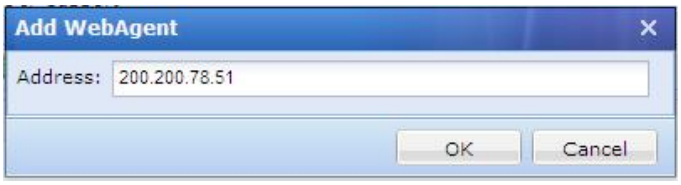
- Do not modify the ports unless it is absolutely necessary. Once the port is altered, the new port number should be entered to the end of the URL address when endpoint user enters the address to connect SSL VPN.
- If the checkbox next to **HTTP Port** is selected, user can use HTTP protocol to communicate with the SSL VPN. Access to SSL VPN is achieved by redirecting HTTP to HTTPS, for instance, ***http://202.96.137.75*** is redirected to ***https://202.96.137.75***. If **HTTP Port** is selected and configured, user can only use HTTPS protocol, in which case, he/she needs to visit ***https://202.96.137.75***.
- If **Permit L2TP incoming connection** is selected, user will be denied to connect to VPN through standard IPSec VPN, while users will be allowed to connect to VPN through Sangfor IPSec VPN.

4. Select encryption protocol for encrypting data. Options are **RSA**, **SM2**, **SSL3.0**, **SSL1.0**, **SSL1.1**, **SSL1.2**, as shown below:



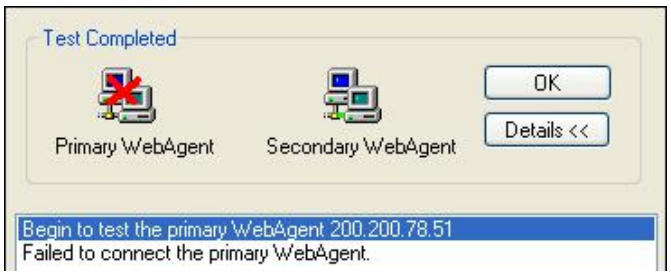
5. Configure **WebAgent Settings**. Select **Enable WebAgent for dynamic IP support** to enable this feature, and the Sangfor device will be able to get an IP using WebAgent dynamic addressing if it is not using a static Internet IP address. To add a Webagent entry:

   a. Click **Add** to enter the **Add WebAgent** page, as shown below:

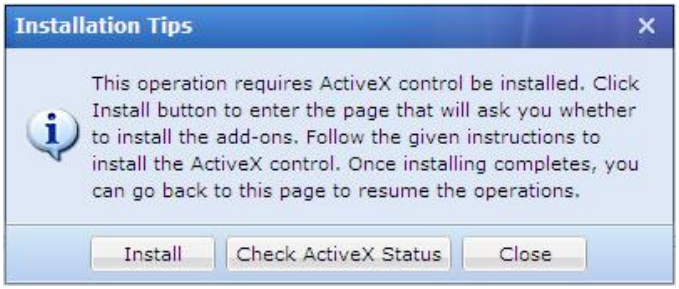


   b. Enter the WebAgent address into the **Address** field and click the **OK** button.

   c. To check connectivity of a WebAgent, select a WebAgent and click **Test**. If the address is correct, the Sangfor device can connect to this WebAgent; otherwise, connecting will fail, as shown in the figure below:



Before test begins, certain ActiveX control should be installed (as shown below).



Click the Check ActiveX Status button to check whether ActiveX control has been installed. If not, click the Install button and follow the instructions to install the ActiveX control.

d. To remove or edit a WebAgent entry, select the desired entry and click **Delete** or **Edit**.

e. To modify password of a WebAgent select the desire entry and click **Modify PWD**. Modifying password can prevent unauthorized user from using and updating a false IP address into the WebAgent page,

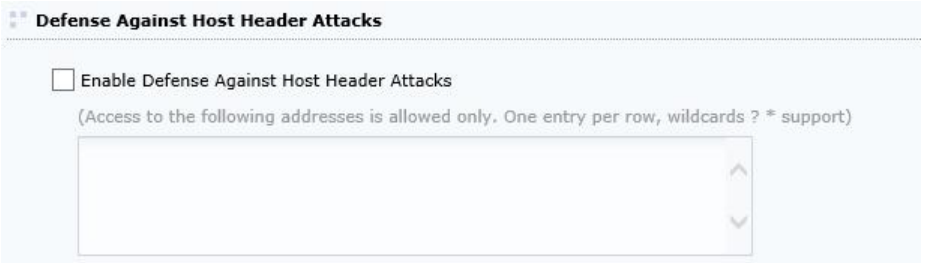
f. To refresh the status of the WebAgent, click **Refresh**.

6. Configure **Defense Against Man-in-the-Middle Attack** option.



Select **Enable defense against man-in-the-middle attack** option and the user will be required to enter the word verification code and be forced to install the related controls. This feature protects the transmitted data from being altered or intercepted by unauthorized user.

7. Configure **Defense Against Host Header Attacks** option.



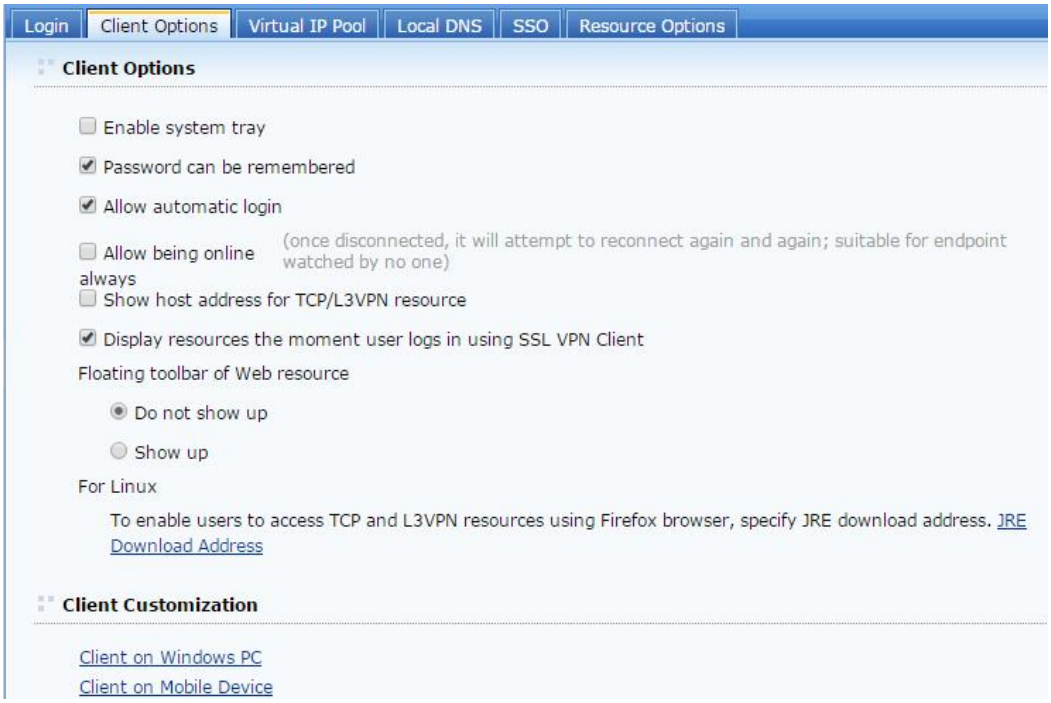
Select **Enable Defense Against Host Header Attacks** option and the user can prevent from the host header attacks, and the device is only allowed to access through the address that matches the rule.

8. Click the **Save** button to save the settings.

Configuring Client Related Options

Client related options are settings related to the SSL VPN Client software and end users' access to SSL VPN at the endpoint.

1. Navigate to **System** > **SSL VPN Options** > **General** > **Client Options** to **Client Options** page, as shown in the figure below:



2. Configure the contents under **Client Options**:

- **Enable system try:** System tray is a taskbar status area showing status of and configure SSL VPN on the client end. Select this option and the browser window can minimize to a system tray when **Resource** page is closed.



Put the cursor on the **System Tray** icon and the brief information of SSL VPN connection status is seen, as shown in the figure below:



- **Password can be remembered:** Select the checkbox next to this option and the SSL VPN Client will remember the SSL VPN login account (username and password) user entered if user selects the option **Remember me** when he/she uses SSL VPN Client program to connect SSL VPN, as shown in the figure below:



- **Allow automatic login:** Select this option to allow connecting users to use automatic login feature when they connect to SSL VPN. This option depends on **Password can be remembered** option, which means that if you select this option, and **Password can be remembered** option will be selected together.



- **Allow being online always:** If selected, client will try reconnecting to VPN again and

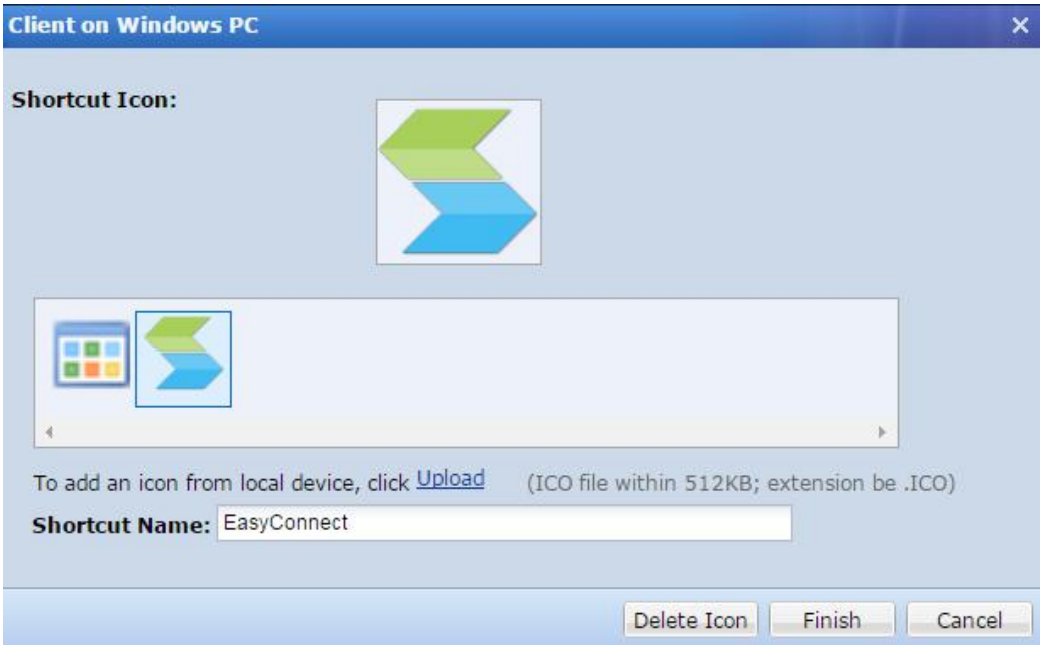
again after disconnected from VPN. It is used for the unattended endpoint.

- **Show host address for TCP/L3VPN resource:** If selected, host address for TCP/L3VPN resource will be displayed on **Resources** page; otherwise, only resource name will be displayed after user logs in to SSL VPN.
- **Display resources the moment user logs in using SSL VPN client:** If selected, associated resources list will be displayed after user logs in using SSL VPN client successfully.
- **Do not show up:** If selected, floating toolbar of Web resource will not show up.
- **Show up:** If selected, floating toolbar of Web resource will show up.
- **JRE Download Address:** Click this link and specify JRE download address. Connecting users must download and install JRE installation package before accessing TCP and L3VPN resources with Firefox browser on Linux. The **JRE Download Address** page is as shown in the figure below:



3. Customize shortcut icon of VPN client on Windows PC or mobile phone:

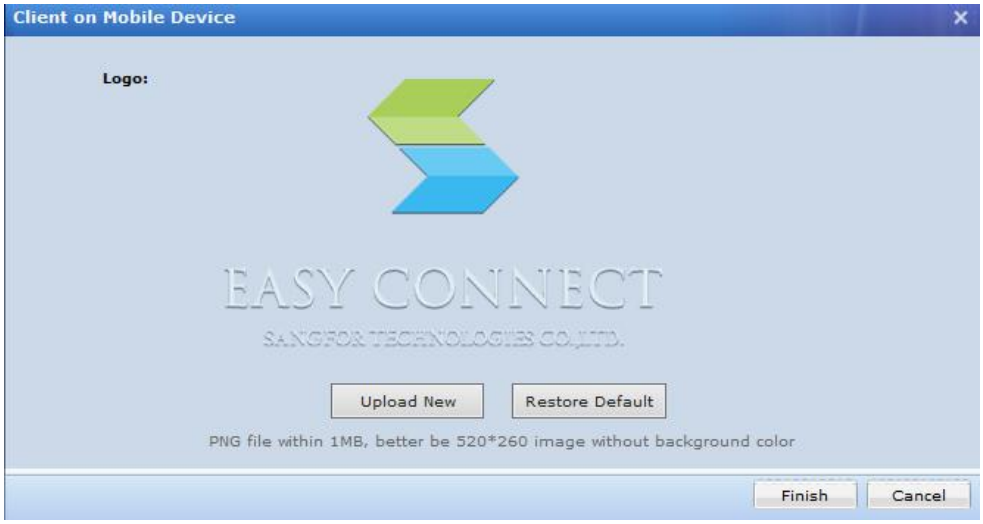
- **Client on Windows PC:** Click it to enter the following page:



Shortcut icon will be created automatically after user logs in to SSL VPN. If you want

to change shortcut icon of system tray, click **Upload** to upload a new icon from local PC to take place of the old one. And you can edit the name of shortcut icon in **Shortcut Name** field.

- **Client on Mobile Device:** It is used for the user logs in SSL VPN using EasyConnect on mobile device, such as mobile phone, tablet, etc. Click it to enter the following page:

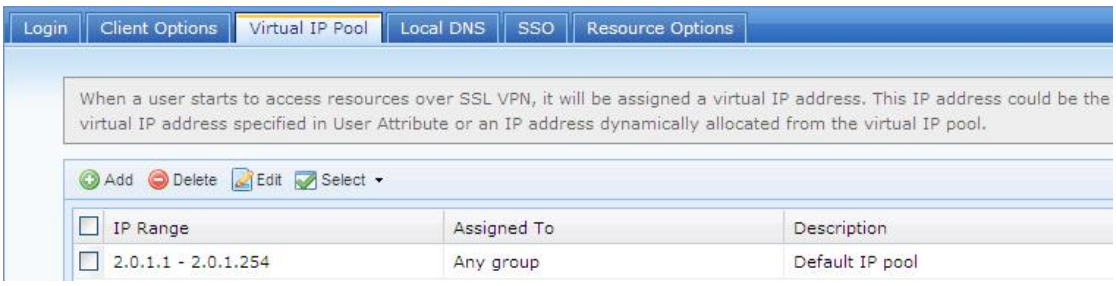


Click **Upload New** to upload a new icon file from local device, or click **Restore Default** to use default logo of VPN client on mobile device.

Configuring Virtual IP Pool

Virtual IP addresses are assigned to users who are to access L3VPN, Web and TCP applications over SSL VPN.

Navigate to **System** > **SSL VPN Options** > **General** > **Virtual IP Pool** and the **Virtual IP Pool** page appears, as shown in the figure below:

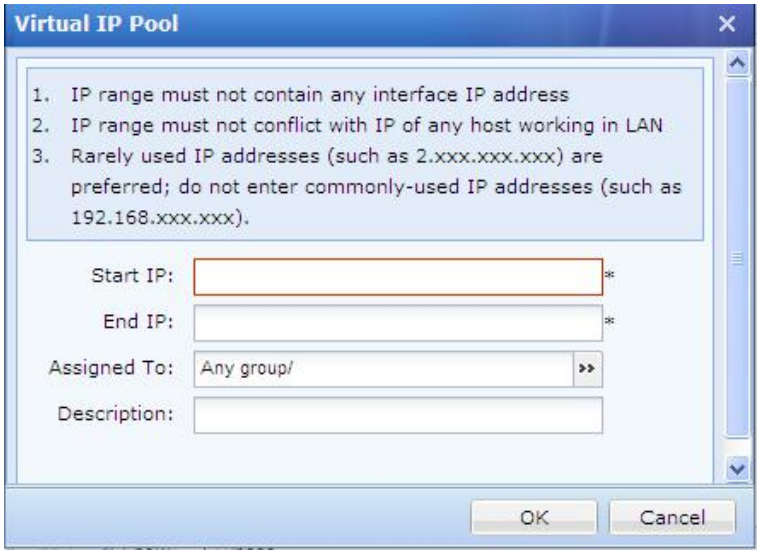


The following are the contents included on the **Virtual IP Pool** page:

- **IP Range:** Range of IP addresses included in the virtual IP pool. The IP addresses should be rarely used IP address, such as 2.0.1.1 - 2.0.1.254.
- **Assigned To:** Indicates the user group whose users will be assigned IP addresses from this IP

address pool.

- **Description:** Description of the IP address pool.
- **Select:** Click it and then click **All** or **Deselect** to select all the IP address pools or deselect all the selected ones.
- **Delete**, **Edit:** Select the desired IP range and click it to delete or edit the IP pool.
- **Add:** Click it to create a IP address pool and enter **Virtual IP Pool** page, as shown below:



When configuration is completed, apply the settings by clicking the **Apply** button that appears after any change is made.

The IP ranges should not cover IP address of any network interface of the Sangfor device, or conflict with IP address of any running machine in the local area network.

Note: Virtual IP pool addresses only support IPv4 addresses and do not support IPv6 addresses.

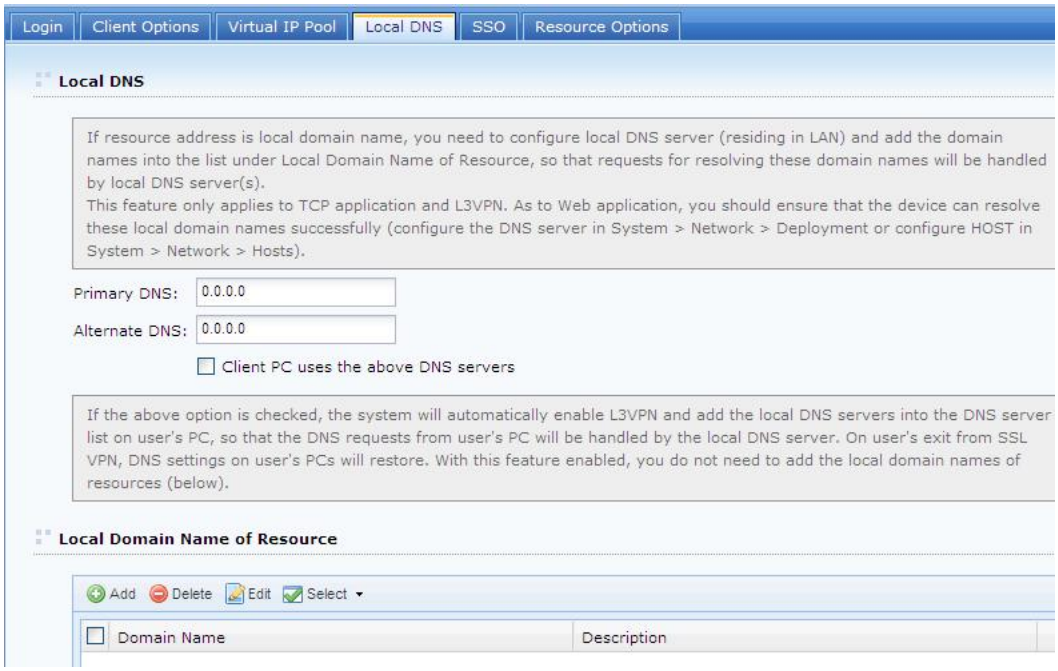
Configuring Local DNS Server

In an enterprise network, local DNS server works well if some internal resources are only accessible to users who request resources by domain names, for local DNS server can provide domain name resolving services when users request resources by domain name.

That is the same with such kind of resource access over SSL VPN. If this type of resources exists

in local area network, local DNS servers could provide domain name resolving services to the connecting users.

1. Navigate to **System** > **SSL VPN Options** > **General** > **Local DNS** to enter the **Local DNS** page, as shown in the figure below:



2. Configure the following under **Local DNS**:

   - **Primary DNS:** This is the primary local DNS server that is preferred to solve domain names.
   - **Alternate DNS:** This is the secondary local DNS server that is used to solve domain names when the primary DNS is unavailable.



   If there is only one local DNS server, enter the server address into the **Primary DNS** field.

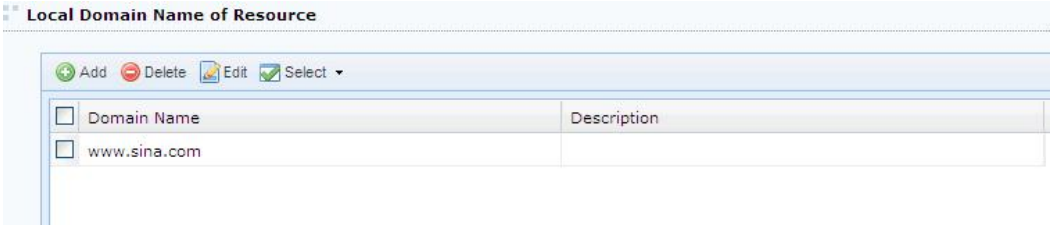
3. Configure **Client PC uses the above DNS servers** option.

   With this option selected, address of primary and secondary local DNS servers will be distributed to the network adapter of the SSL VPN client end. The reason to prefer using the local DNS servers is to avoid such conflict when the domain controller also works as a local DNS server but the local DNS server needs to be authenticated by the domain controller after the user connects to SSL VPN.

   If this option is not selected and many application resources are using domain name as their addresses, administrator needs to add the address (in form of domain name) of resource into the list followed after specifying the local DNS servers. Later on, once a user accesses any of these resources by domain name, the local DNS server will resolve the requested domain

name first, according to the local DNS server and domain names configured on this tab.

4. Configure **Local Domain Name of Resource**. This table is available when **Client PC uses the above DNS servers** option is not selected.



To select all or deselect the selected the entries, click **Select** > **All** or **Deselect**.

To delete or edit the domain name, select a domain name and click **Delete** or **Edit**.

To add an entry, click **Add** and add enter the domain name of a resource, as shown below:



Make sure that the address is in form of IP address when configuring the address of the resource (refer to the Resource section in Chapter 4).

5. Click the **Save** button and **Apply** button to save and apply the settings.

Once the local DNS server is configured and domain name of resources are added, the configuration will work and provide DNS service to the connecting users who request for the resource by domain name.

Beyond local DNS, the internal HOSTS file will also help to resolve the matching domain name and return the resolving result to user (refer to the Configuring Host Mapping Rule

(HOSTS) section in Chapter 3).



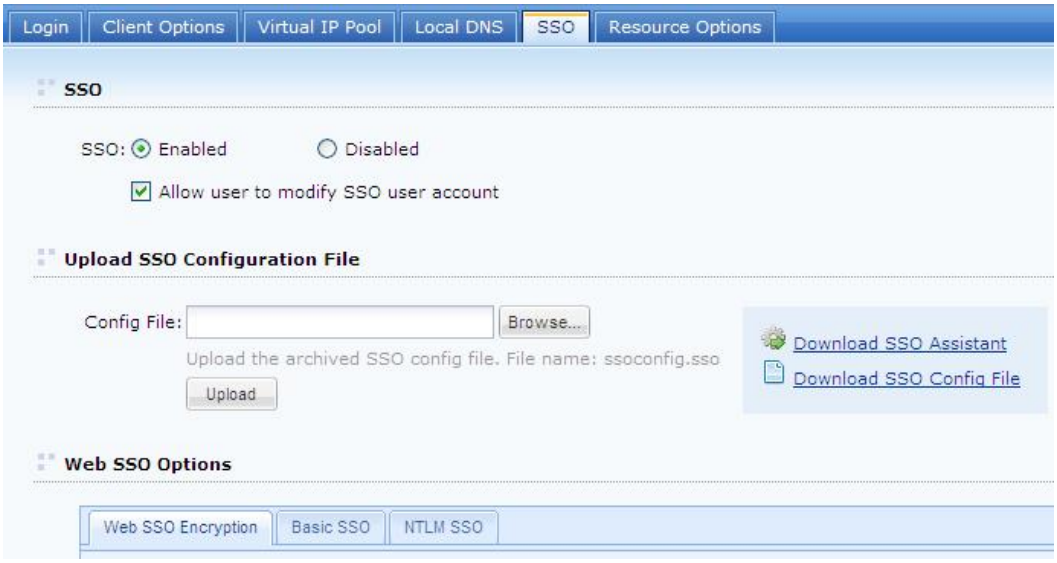
- If address of some resources are domain names and there is a specific DNS server in the local area network providing domain name resolving services, the domain name of that resource is recommended to be added to the list. That will have the requests of DNS handled preferentially by the local DNS server. In other cases, do not add any domain name into the list.
- Domain supports wildcards * and ?. * indicates any character string, while ? indicates any character. For example, ***.com** stands for any domain name ending with **.com**. **b?s.SANGFOR.com** indicates that the second character of that domain name can be any character, such as **bbs.SANGFOR.com**.
- Maximum 100 entries support.

 **Note: For intranet domain name parse, preferred and standby DNS server addresses only support IPv4 addresses, and do not support IPv6 addresses.**

Configuring SSO Options

SSO (Single Sign-On) is a one-off authentication method. It means that once a user successfully logs in to the SSL VPN and is authorized the right to access certain resource, system or application software, that user does not need to enter the required usernames and passwords ever after when accessing that resource, system or application software over the SSL VPN. That is because the system will automatically fill in the usernames and passwords for that user every time.

1. Navigate to **System** > **SSL VPN Options** > **General** > **SSO** and the **SSO** page appears, as shown below:

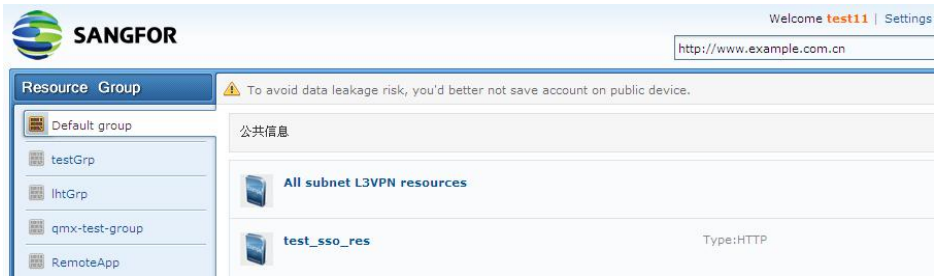


2. Configure the fields under **SSO** and **Upload SSO Configuration File**.

- **SSO:** To enable user to access the corporate resources over SSL VPN without entering username/password, select the option **Enabled**; or else, select **Disabled** to disable SSO.
- **Download SSO Assistant:** Click this link to download the SSO Assistant program. This assistant will help the administrator to record the SSO file if user uses the login method **Auto fill in form** (specified on the **SSO** tab when creating the resource) to access the SSL VPN resources.
- **Download SSL Config File:** Click this link to download the configuration file of SSO. This file should be downloaded after the **SSO** page has been configured. The SSO information of a user can be recorded into the downloaded configuration file, with the help of SSO Assistant.
- **Upload:** It is used to upload the SSO configuration file into the Sangfor device. Browse and upload the configuration file (containing the recorded SSO information) to the device.
- **Allow user to modify SSO user account:** To allow user to modify the SSO user account (username and password) after successful access to SSL VPN, select this option.

  Then connecting users can modify the SSO user account by performing the steps below:

  a. Log in to the SSL VPN and enter the **Resource** page, as shown below:



b. Click **Settings** to enter **Personal Setup** page and select **SSO Options** in the left pane. The right pane shows the SSO resources and user accounts, as shown below:



c. Click **Edit** to edit the SSO user account, as shown below:



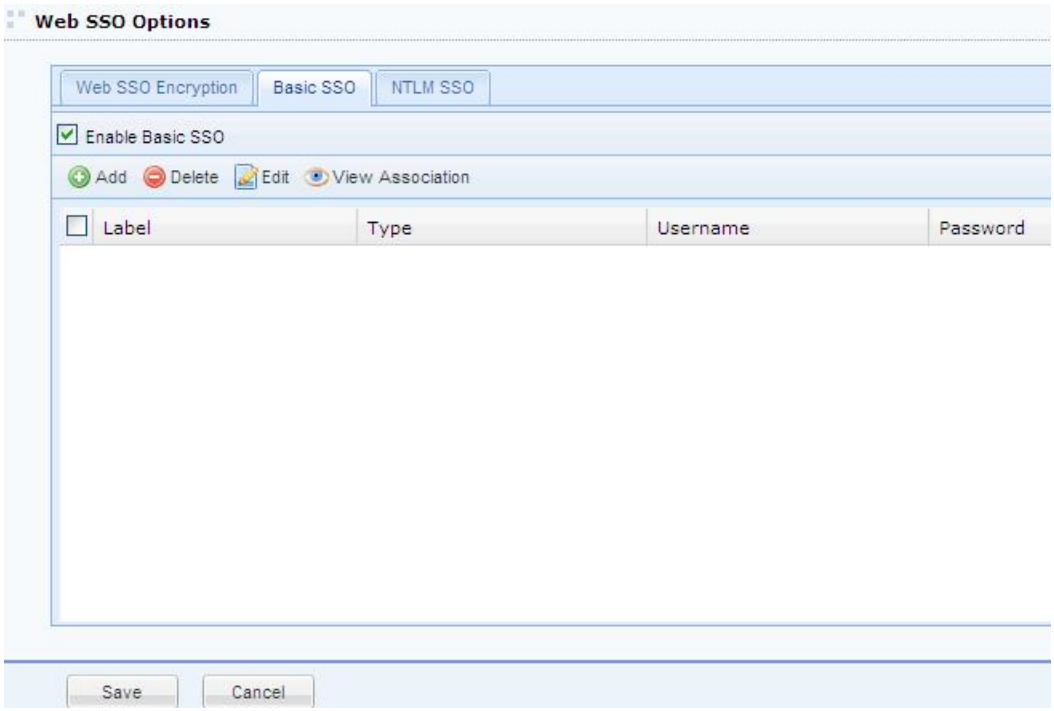
d. Enter the new username and password into **Username**, **Password** and **Confirm** fields.

e. Click **Save** to save the changes.



- Only one type of users can configure **SSO** page on the **Resource** page, that is, the private users who have associated with the resources that have applied SSO.
- To change SSO user account, you need to select **Same with VPN Username** and **Same with VPN Password** in **Input Value** field when recording the SSO file with SSO Assistant.

3. Configure **Web SSO Options**.



There are three tabs under **Web SSO Options**, namely, **Web SSO Encryption**, **Basic SSO** and **NTLM SSO**.

- **Web SSO Encryption:** Configures the options applied to some B/S applications. To add security to SSO to internal resources, the transmitted data (username or password) is better encrypted first when they are submitted from the client side and then be decrypted by the server using the corresponding algorithm. To achieve that, configure the correct JavaScript function on this tab.
- **Basic SSO:** Configures the Basic SSO policy. The policies could be referenced as SSO policy when administrator configures **SSO** options of a **Web** resource and chooses **Basic SSO** as the **Login Method**. Click **Add** to add a basic SSO policy, as shown below:



- **NTLM SSO:** Configures the NTLM SSO policy. The policies could be referenced as SSO policy when administrator configures **SSO** options of a **Web** resource and chooses **NTLM SSO** as the **Login Method**. Click **Add** to add a NTLM SSO policy, as shown below:



4. Click the **Save** button and **Apply** button to save and apply the settings.

Configuring Resource Options

Resource options include access mode for each application (Web, TCP and L3VPNs) and allow administrator to customize access-denied prompt page to inform user of the access failure.

Web App Resource Options

Web App is used to set parameters for Web App resources type and to modify Web service objects.

Navigate to **System** > **SSL VPN Options** > **General** > **Resource Options** > **Web App,** as shown in the figure below:



1. Configure the following fields under **Web Resouce Access Settings**.

- **Access Mode:** This determines the source IP address that connecting users will use to access the server resources. The source IP address could be the interface IP address of the Sangfor device or an assigned virtual IP address (to configure virtual IP address, refer to the Configuring Virtual IP section in Chapter 3).

  To have the connecting users take the IP address of the Sangfor device as the source address to visit the server resources, select **Take device IP address as source**.

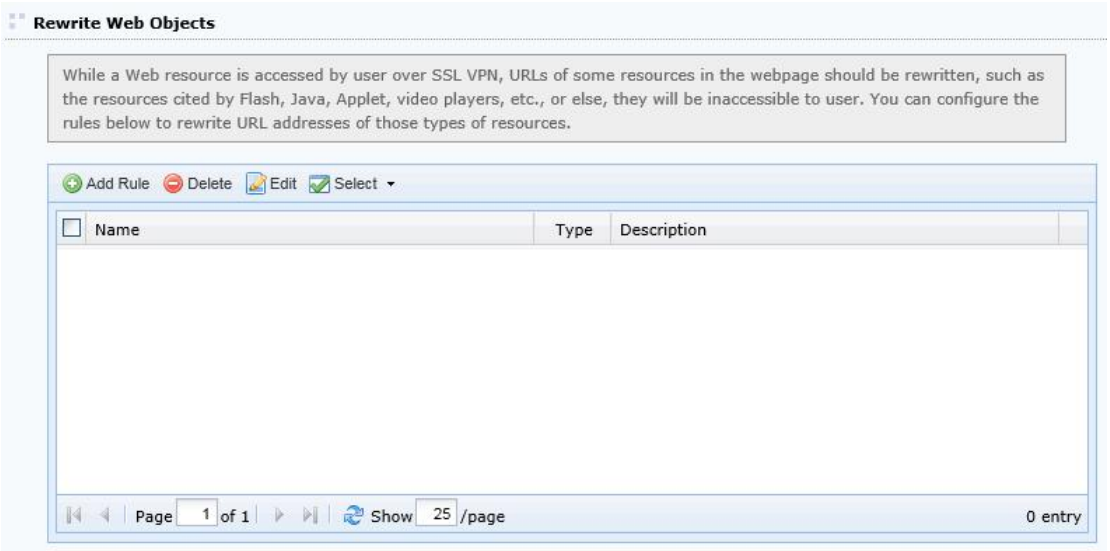
To have the connecting users take the assigned virtual IP address as the source to visit the server resources, select **Take virtual IP address as source** (to configure virtual IP address, refer to the Configuring Virtual IP section in Chapter 3).

- **Pan-Domain Name:**To use the Pan-Domain Name scenario to fill in the Pan-Domain Name.

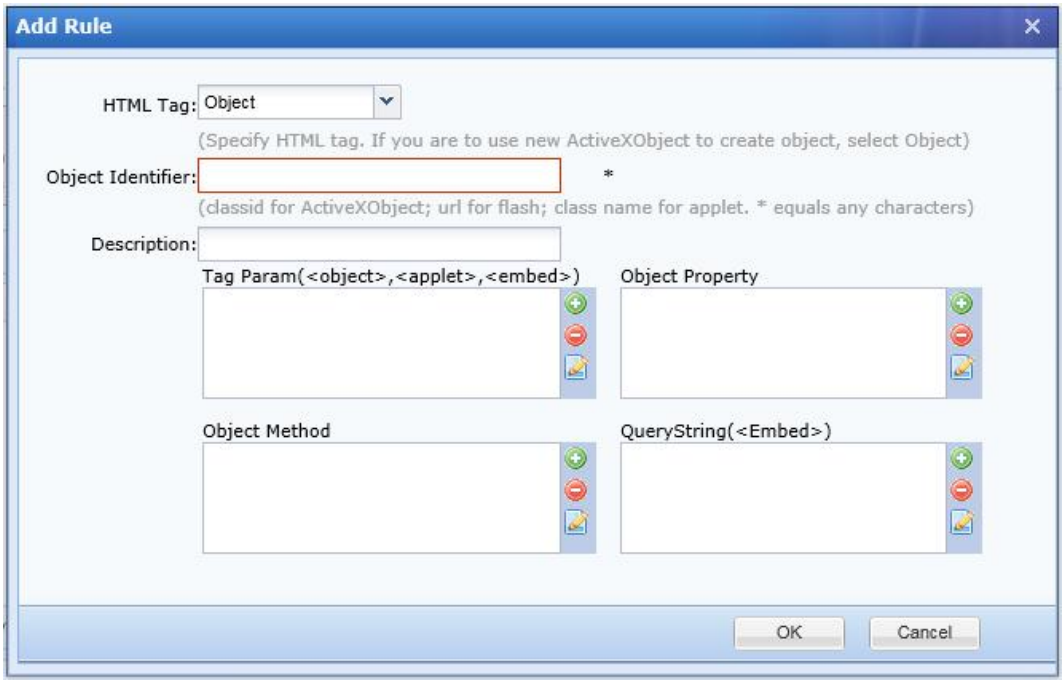
  Selecting Enable HTTP transparent proxy access requires enabling HTTP ports under System > SSL VPN Options > General > Login.

2. Configure the following fields under **Rewrite Web Objects**.

Rewrite Web Objects: Fix the path in which a control references a resource in a WEB application service, such as Flash, Java Applet, or video player, so that it can execute properly. As shown in the figure below:



- **Add Rule:** Add a rule and some paths of resources being cited by controls (Flash, Java, Applet, video players) of the Web application will be rewritten so that these resources can be accessed. Click **Add Rule** and the **Add Rule** page appears, as shown below:



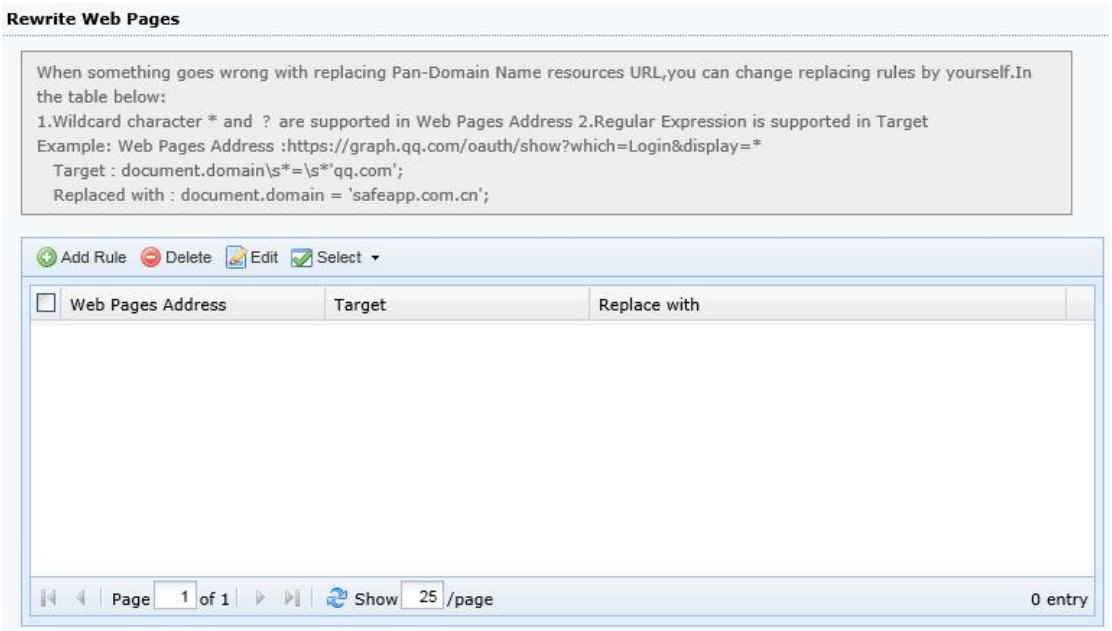
The following are the contents included on **Add Rule** page:

- **HTML Tag:** Specifies the HTML tag used for rewriting webpage objects. Options are **Object**, **Applet** and **Embed**.
- **Object Identifier:** Specifies the identifier (name) of this rule.
- **Description:** Brief description of this rule.
- **Tag Param:** Specifies the parameters in the codes that should be rewritten to revise the webpage.
- **Object Property:** Specifies the object properties in the codes that should be rewritten to revise the webpage.
- **Object Method:** Specifies the object method in the codes that should be rewritten to revise the webpage.
- **QueryString (<Embed>):** Specifies the Querystrings in the codes that should be rewritten to revise the webpage.

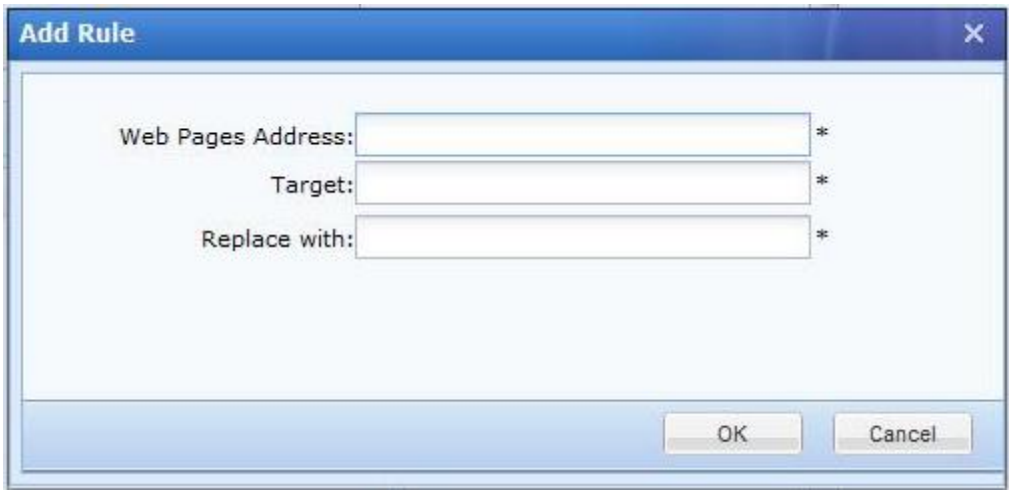
- **Delete**, **Edit:** Select a rule and click **Delete** or **Edit** to remove or modify an entry.
- **Select:** Click **Select** > **All** or **Deselect** to select all rules or deselect the selected rules.
- **Save:** Click this button to save the settings.

3. Configure the following fields under **Rewrite Web Pages**.

Rewrite Web Pages: Used to modify the replacement rule manually when a URL replacement error occurs in a Pan-Domain Name resource, as shown in the figure below:



- **Add Rule:** Click Add Rule, and the rule edit box will appear, as shown in the figure below:



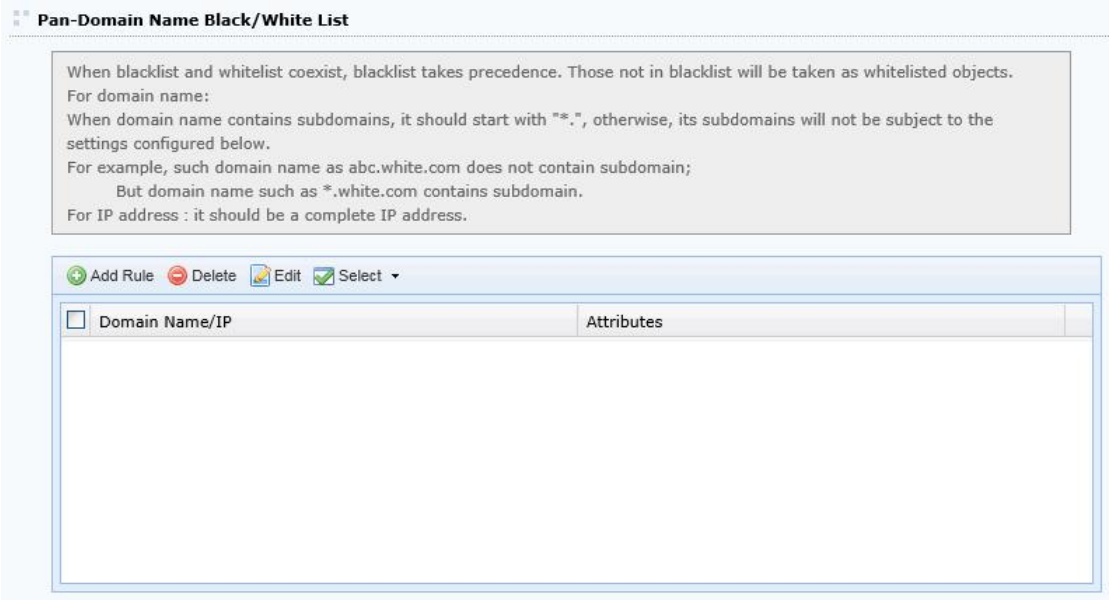
The following are the contents included on **Add Rule** page:

- **Web Pages Address:** Fill in the corresponding URL link based on the Web Pages Address to be modified.
- **Target:** Fill in the URL that needs to be modified.
- **Replace with:** Fill in the URL that needs to be replaced.

- **Delete**, **Edit:** Select a rule and click **Delete** or **Edit** to remove or modify an entry.
- **Select:** Click **Select** > **All** or **Deselect** to select all rules or deselect the selected rules.
- **Save:** Click this button to save the settings.

4. Configure the following fields under **Pan-Domain Name Black/White List**.

Pan-Domain Name Black/White List: Configure the Pan-Domain Name resource with access and non-access permissions. As shown in the figure below:



- **Add Rule:** Click Add Rule, and the rule edit box will appear, as shown in the figure below:

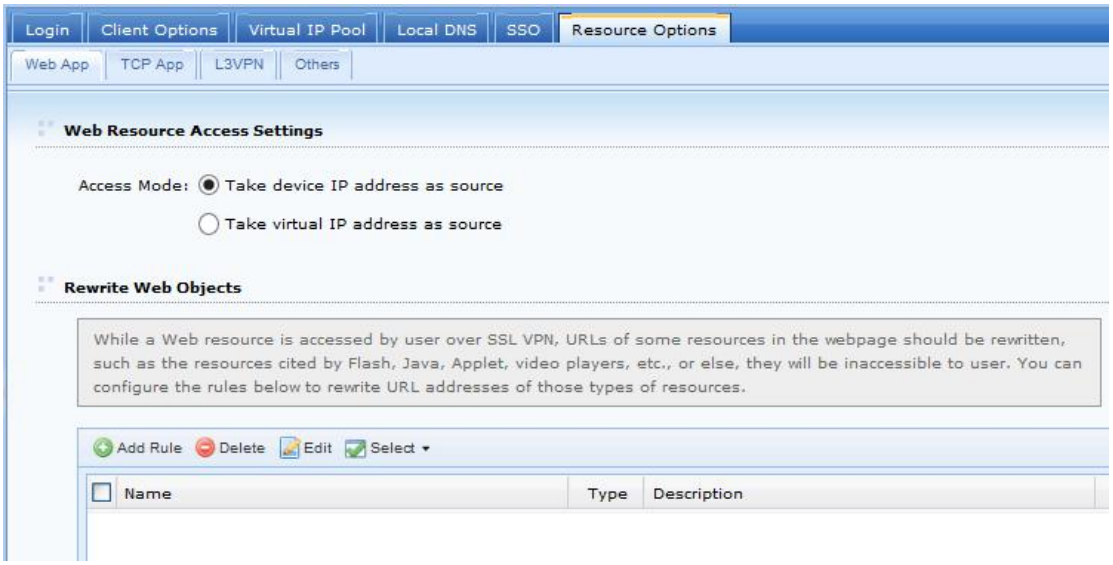


  Add the corresponding domain name or IP select as a white list that is allowed to access or a blacklist that is not allowed to access, and click ok to save.

- **Delete**, **Edit:** Select a rule and click **Delete** or **Edit** to remove or modify an entry.
- **Select:** Click **Select** > **All** or **Deselect** to select all rules or deselect the selected rules.
- **Save:** Click this button to save the settings.

TCP App Resource Options

Navigate to **System** > **SSL VPN Option** > **System** > **Resource Options** > **TCP App** to configure the parameters related to TCP resource access and smart recursion feature, as shown below:



The following are the contents included on **TCP App** tab:

- **Access Mode:** Specifies the source IP address that connecting users will use to access the server resources, whether it is the interface IP address of the Sangfor device or an assigned virtual IP address (to configure virtual IP address, refer to the Configuring Virtual IP section in Chapter 3).

  To have the connecting users take the IP address of the Sangfor device as the source address to visit the server resources, select **Take device IP address as source**.

  To have the connecting users take the assigned virtual IP address as the source address to visit the server resources, select **Take virtual IP address as source** (to configure virtual IP address, refer to the Configuring Virtual IP section in Chapter 3).

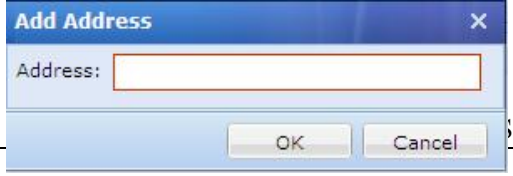
- **Max Sessions Per User:** Specifies a maximum of sessions that one user can establish to access TCP resources concurrently.

- **Enable:** Select this option to enable smart recursion feature for access to TCP resources.

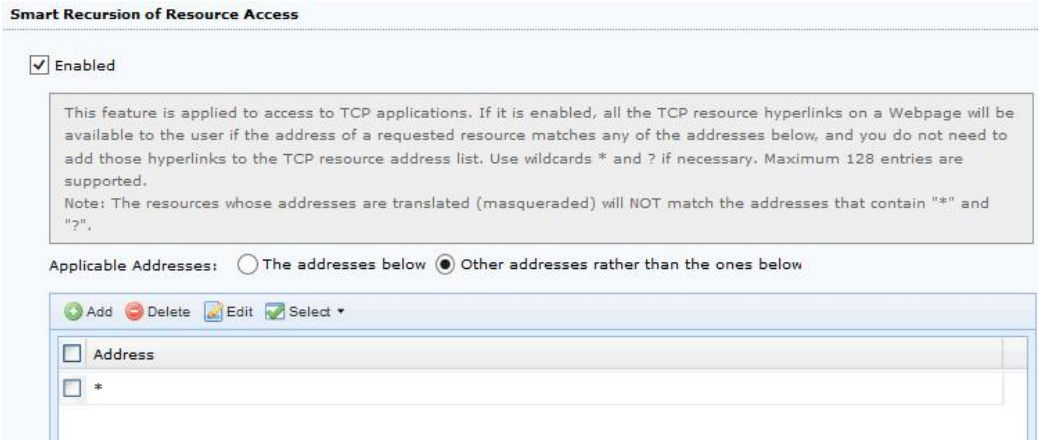


Please note that, to have smart recursion feature take effect, **Enabled** option should be selected, and option **Apply smart recursion** on **Others** tab should also be selected when editing the TCP resource.

- **Applicable Address:** The addresses to which the smart recursion feature will apply. If **The addresses below** is selected, smart recursion will apply to all the URL addresses in the list; if **Other addresses rather than the ones below** is selected, smart recursion will apply to all



other URL addresses except those in the list.



To add a URL address, click **Add**. The **Add Address** page is as shown below:

To remove or modify the rule**, s**elect a rule and click **Delete** or **Edit**.

To select all rules or deselect the selected rules, click **Select** > **All** or **Deselect**.

- **Save:** Click this button to save the settings.

Background Knowledge: What is Smart Recursion?

It is common that on the homepage of some websites there are many links. If a user wants to visit those link and therefore access the corresponding servers over the SSL VPN, the addresses of those servers must be available on **Resource** page; otherwise, those server resources will be inaccessible to the user.

However, it is an immense task and tedious work for the administrator to add all those addresses one by one in to the resource address list by hand when editing a resource, and most likely, some of the addresses may be left outside the list. Without a complete list of link resources, connecting user still cannot visit some resources.

Smart recursion functionality is intended for solving the aforementioned troubles. With the help smart recursion, administrator needs only to,

1. Navigate to **SSL VPN** > **Resources** page to add a TCP resource. Add the homepage address of a website to the **Address** field, and select the option **Apply smart recursion** on **Others** tab.
2. Navigate to the **System** > **SSL VPN Options** > **General** > **Resource Options** > **TCP App**, Select **The addresses below** as the applicable addresses and add the URL addresses of the links to the list.

Without taking the links as TCP resources and adding their URL addresses to the resource address

list, all the link resources on that homepage will be available for connecting users.

Scenario 4: Configuring and Applying Smart Recursion

Background:

The homepage of a library website is *www.library.com*. The website contains a great many links to other servers and databases.

Purpose:

Enable users to remotely and securely access the homepage of the library and the links to other servers and databases.

Analysis and Solution:

To meet the requirements, firstly create TCP resource (address of the resource is homepage of the library, *www.library.com*) and enable smart recursion, secondly configure smart recursion on **Resource Options** page.

Below is the configuration procedure:

1. Navigate to **SSL VPN** > **Resources**, and click **Add** > **TCP app** to add the TCP resource of library homepage.
2. Configure the required fields and add library homepage (*www.library.com*) into the textbox next to the **Address** field.
3. Click **Others** tab and select the option **Apply smart recursion**.
4. Navigate to **System** > **SSL VPN Options** > **General** > **Resource Options** > **TCP App** and select **Enabled**.
5. Specify the applicable addresses by selecting **The addresses below**.
6. Add the URL address of the library website into list (***.library.***). If the homepage library contains other URL links, add them into this list.
7. Click **Save** to save the settings and then click the **Apply** button on the next page.
8. Edit the user and associate this library resource with the user.



- Currently, smart recursion is applied only to TCP-supported HTTP and HTTPS.
- While user is visiting the resource that applies smart recursion, to access the links, he/she must click on the links on the “root” resource page; however, if the “root” resource page is closed, it can still click the link on the links on the “links” page.

L3VPN Resource Options

Navigate to **System** > **SSL VPN Option** > **System** > **Resource Options** > **L3VPN** to configure the parameters related to L3VPN resource, as shown in the figure below:



The following are the contents included on **L3VPN** tab:

- **Access Mode:** Specifies the source IP address that connecting users will use to access the server resources, whether it is the interface IP address of the Sangfor device or an assigned virtual IP address (refer to the Configuring Virtual IP section in Chapter 3).

  To have the connecting user take the IP address of the Sangfor device as the source address to visit the server resources, select **Take device IP address as source**.

  To have the connecting user take the assigned IP address as the source address to visit the server resources, select **Take virtual IP address as source** (refer to the Configuring Virtual IP section in Chapter 3).

- **Transfer Protocol:** Specifies the transfer protocol used while L3VPN resource is accessed.

  Select **TCP** and only TCP will be used to transfer data while user is using L3VPN resources; while **Auto select** makes it apt to start UDP to transfer data.

- **UDP Port:** Indicates the UDP port used for transferring data. It is 442 by default. Assume that the Sangfor device is in **Single-arm** mode, this port should be mapped from the front-end firewall to the Sangfor device.

- **Advanced:** Click this button and optional advanced options appears, **Max Concurrent Users** and **IP of Local Virtual NIC**. The latter specifies the server-end IP address range to which the virtual NIC is applied.

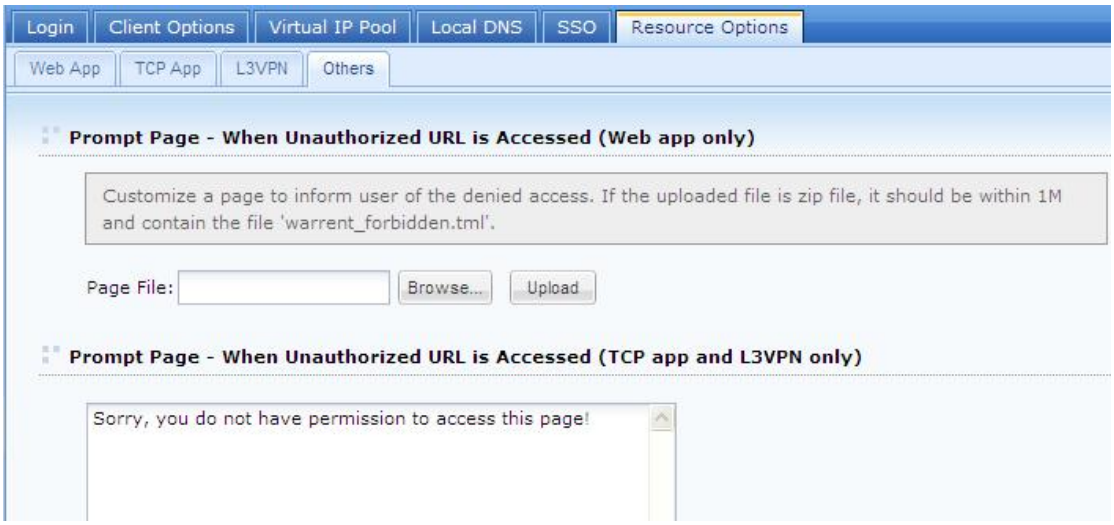


Changing advanced options may severely affect the performance of the system, therefore, it is recommended to adopt the defaults.

Note: If the user modifies parameters in Advanced Settings, it may have a serious impact on SSL VPN performance. Generally, it is proper to keep the default values. Furthermore, IPv4 addresses instead of IPv6 addresses can be filled here.

Other Resource Options

Navigate to **System** > **SSL VPN Option** > **System** > **Resource Options** > **Others** tab. This tab configures access-denied prompt page that will appear in front of the users when they visit an unauthorized URL address (resource), as shown in the figure below:



The following are the contents included on **Others** tab:

- **Page File:** For users accessing unauthorized URL of Web application resource, upload a prompt page through **Page File** field. When any user accesses authorized URL, he/she will be notified that access is denied.

- For the users accessing unauthorized URL address of TCP or L3VPN resource, enter the words into the textbox to inform user that access is denied because they are visiting unauthorized page.



The compressed file should be in format of .zip, smaller than 1M and contain the file **warrant_forbidden.tml**.



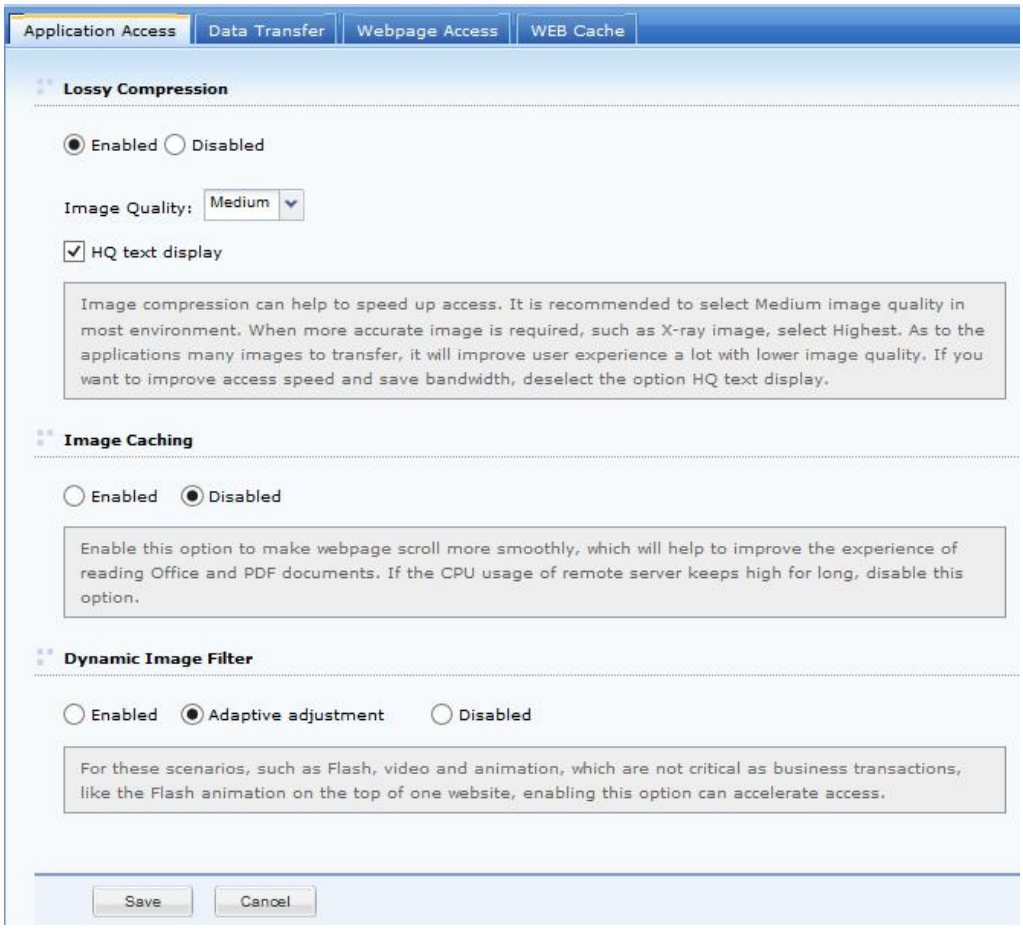
Unauthorized or authorized URL addresses are configured on **URL Access Control** tab while editing a Web/TCP/L3VPN resource (refer to the Resource section in Chapter 4).

Network Optimization Related Settings

Navigate to **System** > **SSL VPN Options** > **Network Optimization** and four pages are seen, namely, **Application Access**, **Data Transfer**, **Webpage Access** and **Web Cache**, which configure the optimization options in terms of application access, data transfer, webpage access and Web cache.

Application Access Optimization

1. Navigate to **System > SSL Options > Network Optimization > Application Access** to enter **Application Access** page, as shown in the figure below:



2. The following contents are under **Lossy Compression**:
   - **Enabled**, **Disabled**:If enabled, image displayed in remote application will be compressed according to specified image quality so as to speed up transmission.
   - **HQ text display:** Select it to keep text displayed clearly when image quality is decreased.
3. Configure image caching: If **Enabled** is selected, image will be cached in order to make

image scroll more smoothly, but it will also increase CPU usage of remote server.

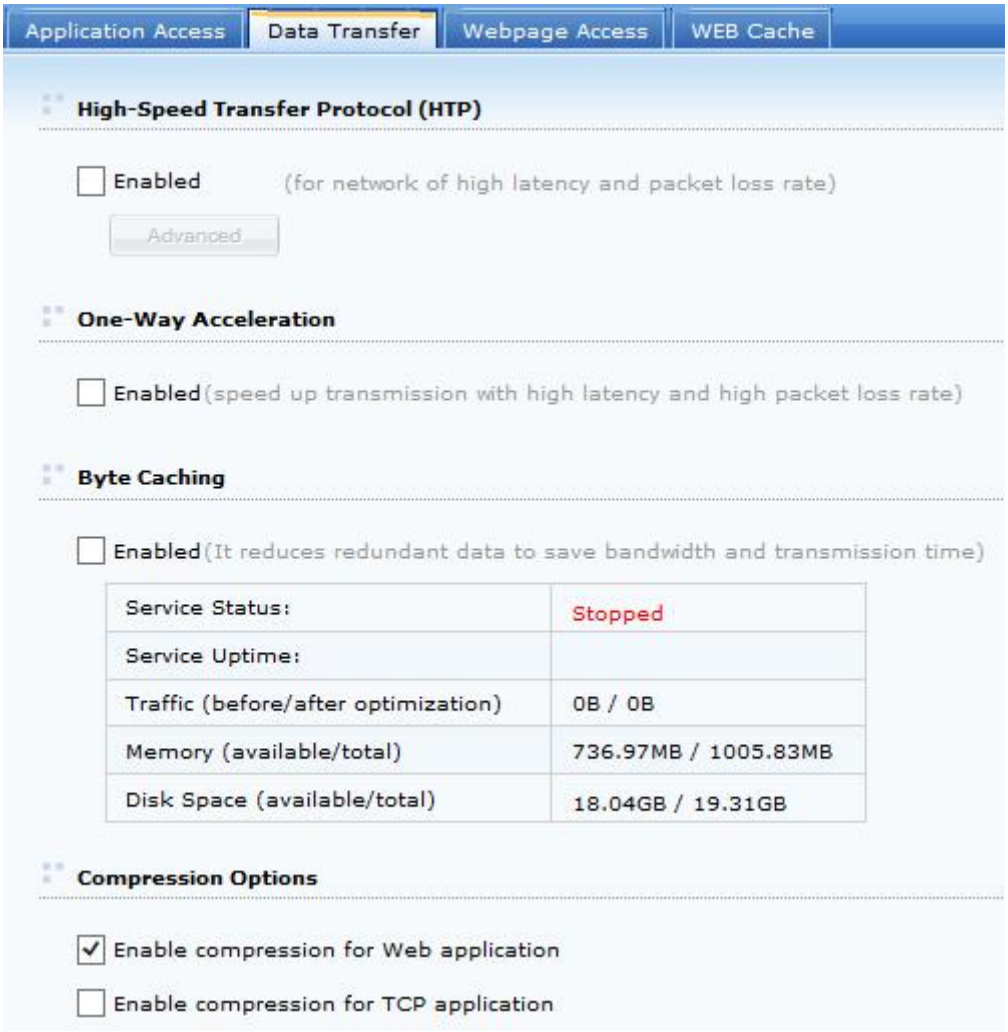
4. The following information are included under **Dynamic Image Filter**:

   - **Enabled**, **Disabled:** If enabled, dynamic image, like Flash animation, will be filtered so as to save bandwidth and speed up access.
   - **Adaptive adjustment:** Select it to make dynamic images filtered adaptively.

5. Click **Save** to save the changes; or click **Cancel** to give up.

Data Transfer Optimization

1. Navigate to **System > SSL Options > Network Optimization > Data Transfer** to enter **Data Transfer** page, as shown in the figure below:



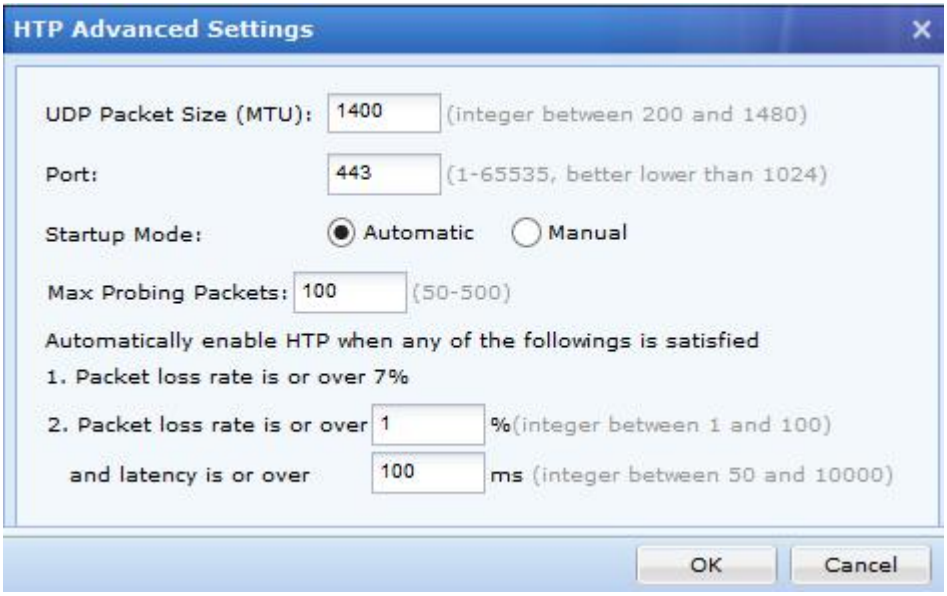
2. Configure the following contents on **Data Transfer** page:

   - **High-Speed Transfer Protocol(HTP):** Enable it to speed up access in a wireless network or in poor network environment.



- HTP is the short name of High-Speed Transfer Protocol, which can optimize data transfer over the involved networks.
- At the client end, after user logs in to SSL VPN, he/she needs to enable HTP on **Optimization** page.

- **Advanced:** Click this button to enter the **HTP Advanced Settings** page, as shown below:



Startup Mode indicates the way that HTP is to start up, automatically or manually.

If **Manual** is selected, HTP needs to be started by hand. If **Automatic** is selected, HTP will start up automatically according the network state (good, wireless or poor) of the endpoint detected by SSL VPN client software when users connect to SSL VPN.

Network state detection is based on the two conditions: a). **Packet loss rate is or over 7%**; b). **Packet loss rate is or over _ % and latency is or over _ ms**. Either condition may trigger start up of HTP. Generally, defaults are recommended to be adopted.

- **Enable HTP** option only takes effect when users access TCP resources over SSL VPN via IE browser (other kinds of browsers are not supported).
- Applying HTP needs the support of UDP port 443. If the Sangfor device is deployed in

Single-arm mode, do remember to configure the front-end firewall to map this UDP port to the Sangfor device.

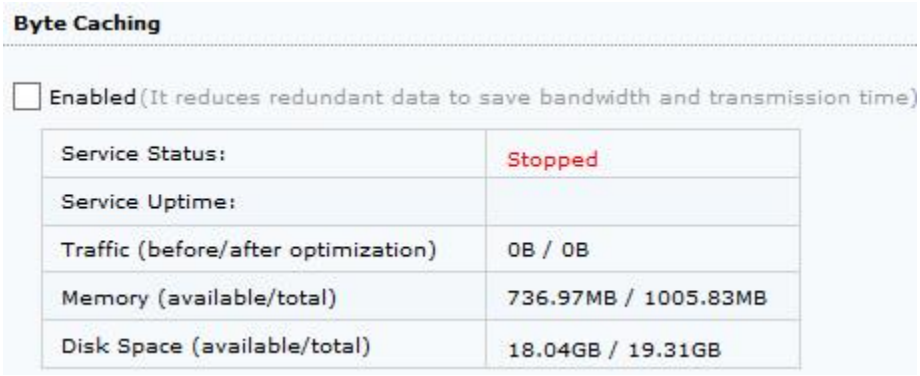
- **One-Way Acceleration:** Enable it to speed up TCP-based tunnel service.





To enable one-way acceleration feature, you need to activate corresponding license first; otherwise, **Enabled** option turns gray, and you cannot select it.

- **Enabled:** Select this option so that redundant data will be compressed and that data transmission time and bandwidth consumption could be minimized.



- **Compression Options:** Select **Enable compression for Web application** and/or **Enable compression for TCP application** according. The former mean data related to Web applications will be compressed, while the latter means data related to TCP applications will be compressed.



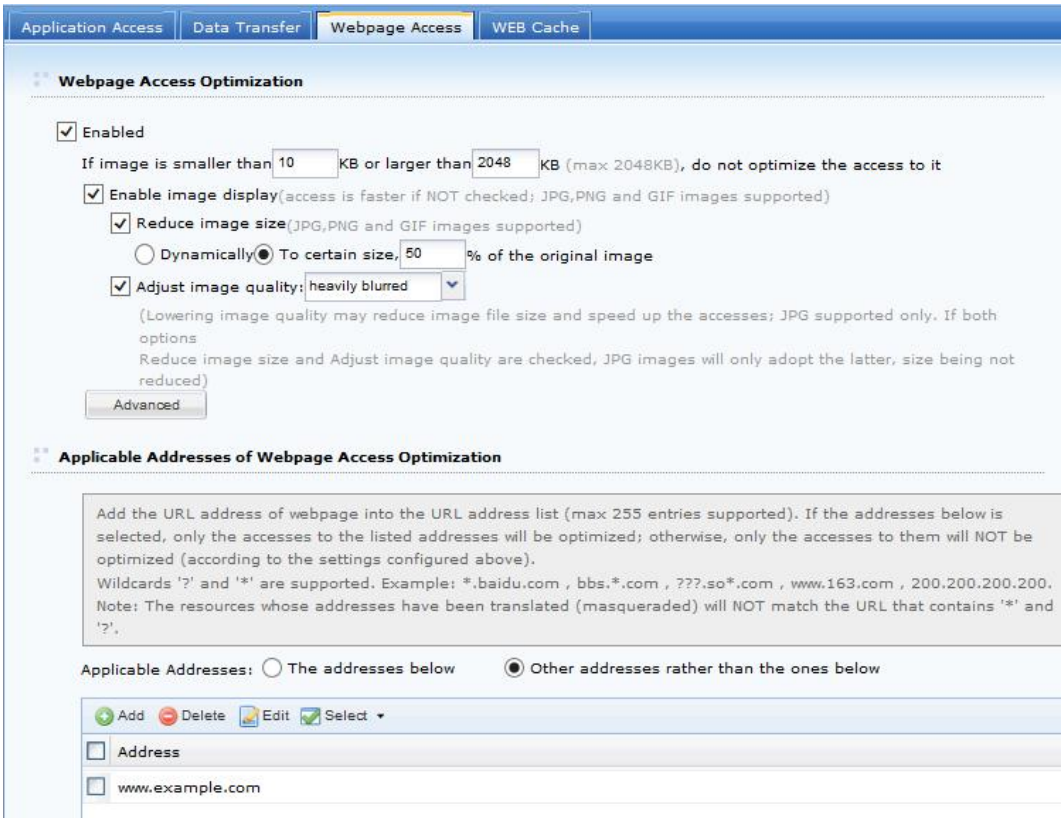
- **Advanced:** Click this button to specify the compression algorithm for TCP application access, **LZO** or **GZIP/ZLIB**, as shown in the figure below:



Webpage Access Optimization

This kind of optimization utilizes system resources of the Sangfor device to handle images and therefore reduce data stream from/to public networks. It is an ideal feature for the users who are using PDA (Personal Digital Assistant) to access SSL VPN or the user's computer is in poor network. This feature should not be enabled for users in good network environment.

Navigate to **System** > **SSL VPN Options** > **Network Optimization** > **Webpage Access** and the **Webpage Access** page is as shown in the figure below:



The following are the contents included on **Webpage Access** page:

- **Enabled:** It is a global switch for webpage access optimization. Select this option and webpage access optimization feature will be enabled.
- To optimized access to webpage, set the image size limit, that is, configure **If images is smaller than _ KB** and **or larger than _ KB**.
- **Enable image display:** Uncheck this option to disable image display and therefore enhance

the access speed.



- **Enable image display** only applies to the images with any of the following extensions: .jpg, .png and .gif.
- **Enable image display** achieves the opposite optimization effect, comparing with the effect that **Adjust image quality** achieves.

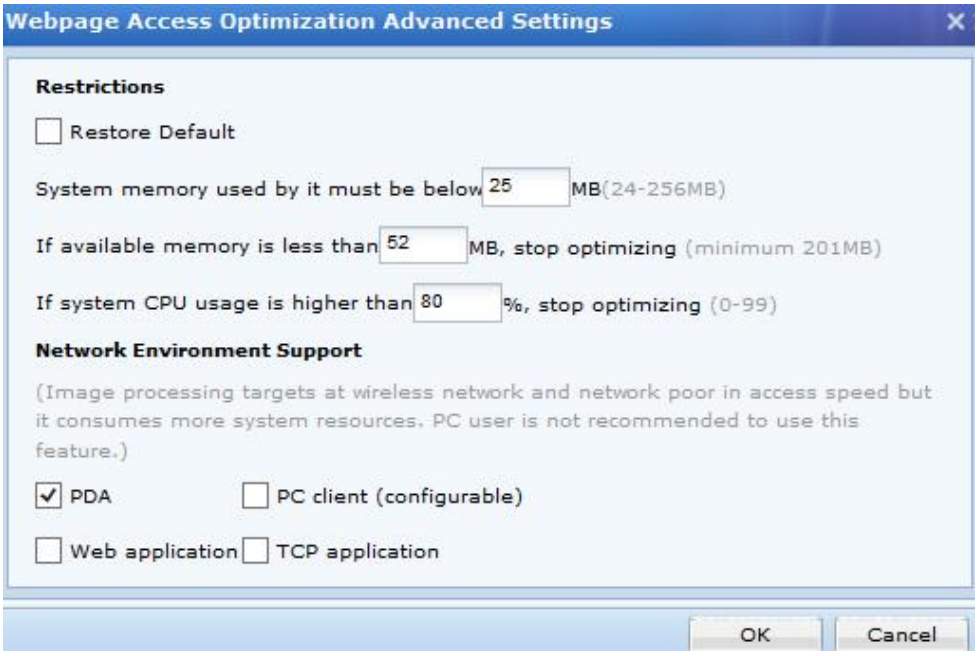
- **Reduce image size:** Select it and then select **Dynamically** or **To certain size _% of the original image** to reduce the image size and data. This feature applies to the images with any of the following extensions: .jpg, .png and .gif.

  Dynamically indicates that the system will dynamically adjust the image size in accordance with the original size.

  To certain size, _ % of the original image indicates that image will shrink based on the original image and the proportion configured.

- **Adjust image quality:** This option leads to quality deterioration of image (jpg image supported only), though it helps to reduce the image data. Four options are available, namely, **Smartly blurred**, **Slightly blurred**, **Blurred** and **Heavily blurred**. This feature applies to .jpg images only.

- **Advanced:** Click this button and the **Webpage Access Optimization Advanced Settings** page appears, as shown in the figure below:



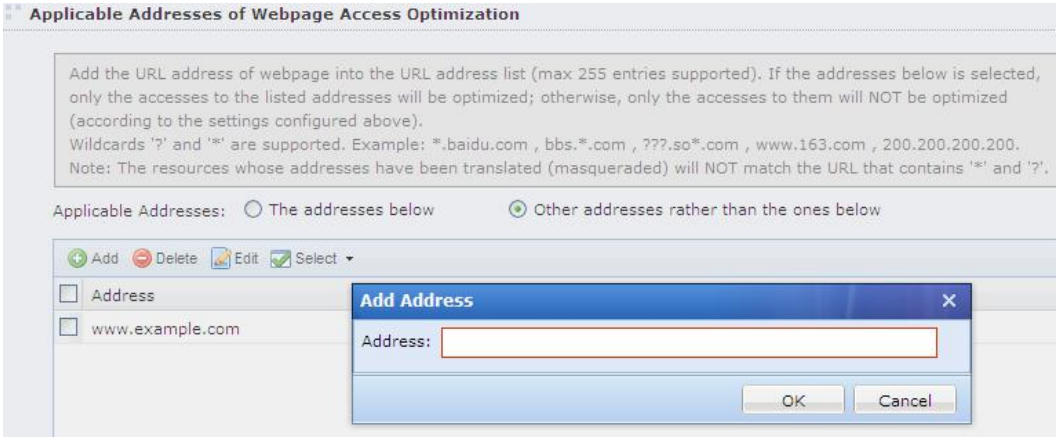
- **Restrictions:** Indicates the thresholds determining when webpage access optimization functionality will start up. These thresholds could minimize the impact that webpage access optimization poses on the running and performance of other modules. The restrictions include those on **system memory** usage and **CPU** usage. Each threshold has a default. Select the option **Restore Default** if you want to.



In no case will any of the thresholds be disabled.

- **Network Environment Support:** This part specifies the types of services and client-end network environment (PDA, PC client, Web app access and/or TCP app access) that can support webpage access optimization.

- **Applicable Address of Webpage Access Optimization:** Configure the URL addresses to have the access to them optimized or not optimized.



The following are contents under **Applicable Address of Webpage Access Optimization**:

- **Applicable addresses:** If **The addresses below** is selected, only the access to the added URL addresses will be optimized. If **Other addresses rather than the ones below** is selected, access to any other URL addresses (except the added addresses) will be optimized. ttones listed below] incied below] inci
- **Add:** Click it to add address into the list.
- **Select:** Click it and then select **All** or **Deselect** to select all the addresses or deselect the selected address.
- **Delete**, **Edit:** Select an entry and click it to remove or modify the address.



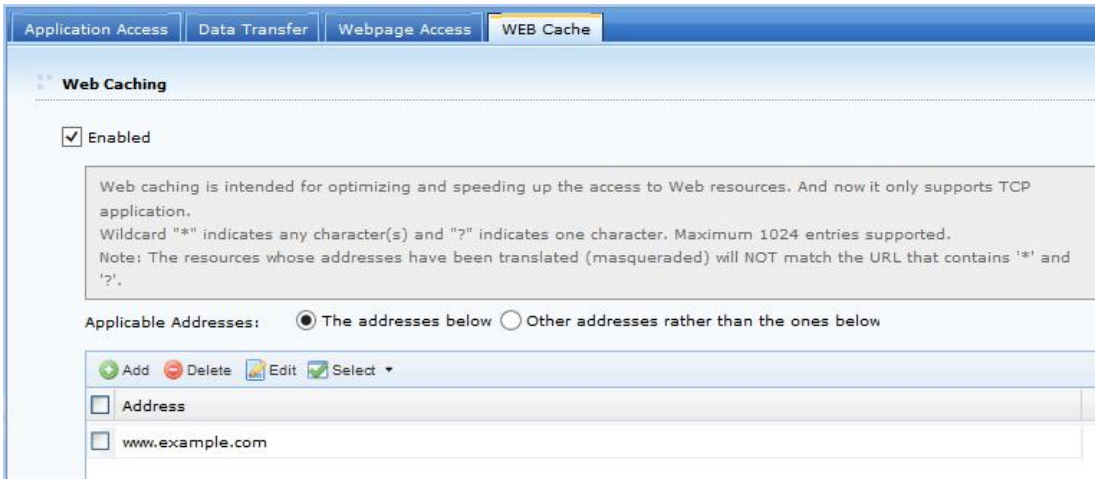
- The two types of applicable address are alternative.

- Wildcards "?" and "*", and a maximum of 255 entries are supported.

Web Cache

Web Cache is a feature based on IE caching mechanism. The contents that can be cached by Internet Explorer are cacheable for the Web Cache. With the Web Cache optimization function caching images, .js scripts, css (compression is not applied to transferring webpage data), response time of user's access request for the Webpage will be reduced.

Navigate to **System** > **SSL VPN Options** > **General** > **Network Optimization** > **Web Cache** and the **Web Cache** page is as shown in the figure below:



The following are the contents included on the **Web Cache** page:

- **Enabled:** Select it to enable Web Cache.
- **Applicable Addresses:** If **The addresses below** is selected, only the access to the added URL addresses will be optimized. If **Other addresses rather than the ones** is selected, access to any other URL addresses (except the added ones) will be optimized.
- **Add:** Click it to enter the **Add Address** page to add an entry, as shown below:



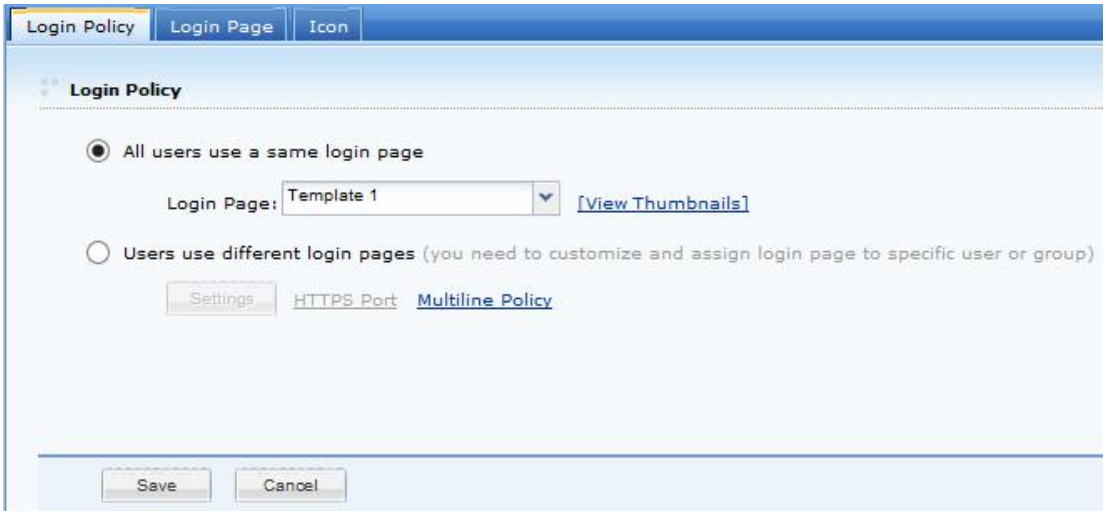
- **Select:** Click it and then select **All** or **Deselect** to select all the addresses or deselect the selected address.
- **Delete**, **Edit:** Select an entry and click it to remove or modify the address.

User Logging in

This section covers configuration on three pages, **Login Policy**, **Login Page** and **Icon**.

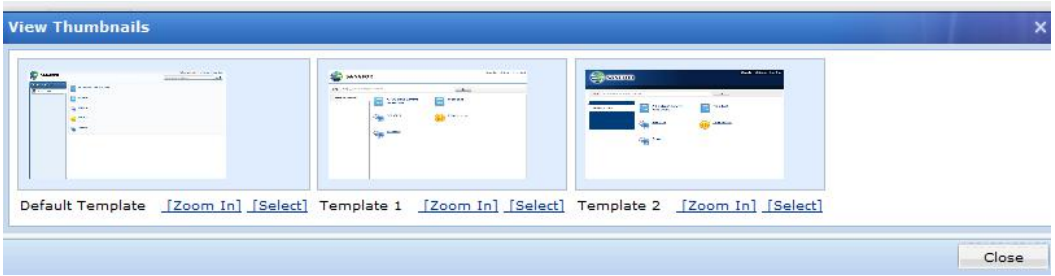
Configuring Login Policy

Login policy is a kind of policy that not only sets the login page for connecting users at the client end but also specifies the default login method.



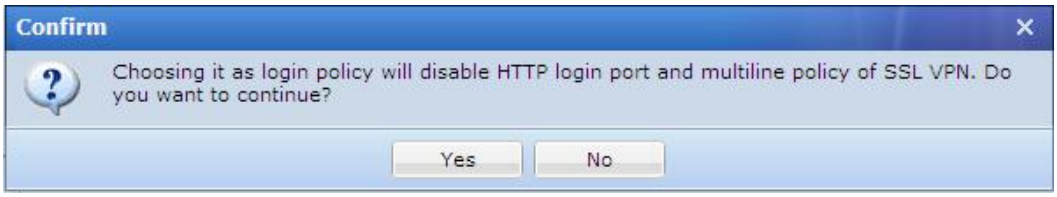
If **All users use a same login page** is selected, configure the following:

- **All users use a same login page:** A global setting indicates that all the users will use the specified login page.
- **Login Page:** Specifies the login page that users use to log in to SSL VPN. It could be a built-in page or a custom login page.
- **View Thumbnails:** Click to view thumbnails of the built-in page template, as shown below:

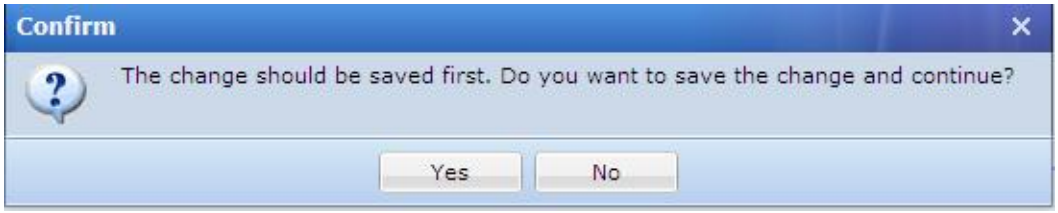


If **Users use different login pages** is selected, a user/group can only use the designated login page to access SSL VPN. Please do the following:

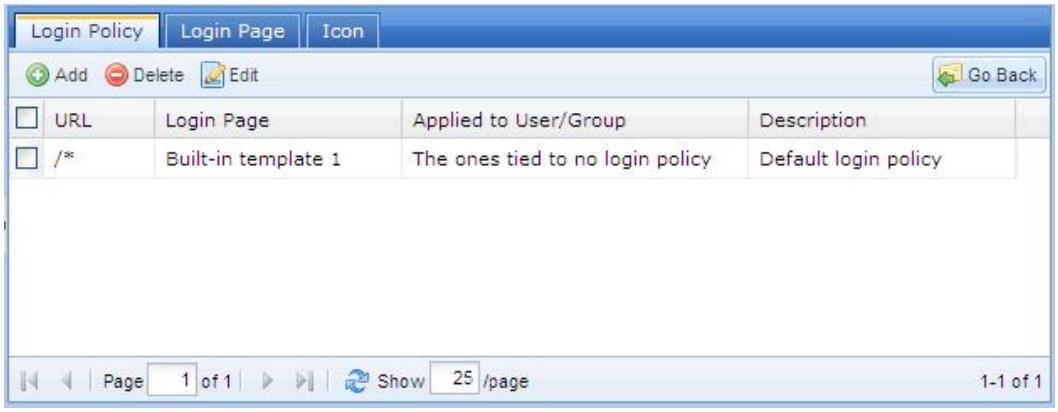
1. Click the **Yes** button to confirm choosing **Users use different login pages** as the policy selected. As shown in the following prompt, the HTTP login port and multiline policy of SSL VPN will be disabled.



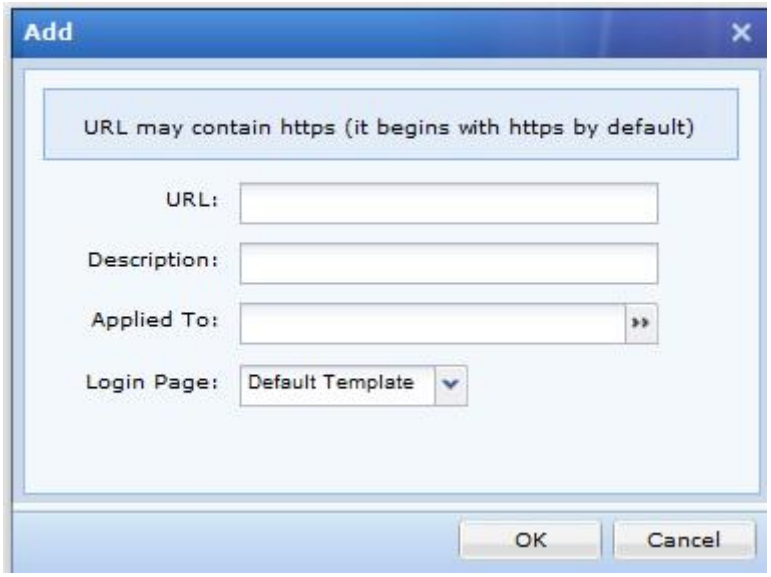
2. Click the **Configure** button on the **Login Policy** page to customize login pages and assign them to specific users/groups. If change is not saved, the following prompt will pop up:



3. Click the **Yes** button to save the change and enter the next page, as shown below:



4. Click **Add** and enter the **Add Login Policy** page to add a login policy, as shown below:

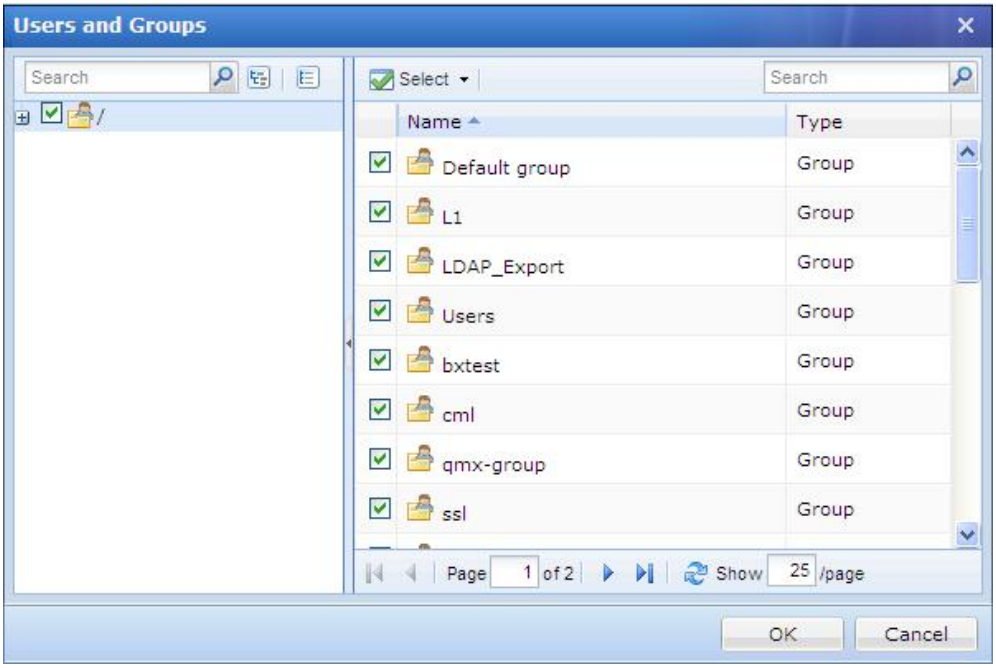


5. Configure the following fields on the **Add Login Policy** page:

   - **URL:** Specifies the URL address of the homepage of SSL VPN. URL may contain **https**.

By default, it contains **https**.

- **Description:** Brief description of the user or group.
- **Applied To:** Specifies the users or groups that are associated with this login policy. Click this field and **Users and Groups** page appears, as shown below:



Select the desired users or groups to associate them with this login policy and click **OK**.

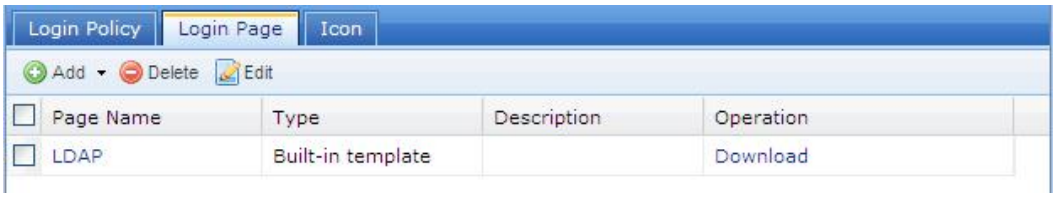
- **Login Page:** Specifies the login page that the specified users or groups will use to log in to SSL VPN. It could be a built-in page or a custom login page.

If **Users use different login pages** is the login policy, HTTPS port and multiline policy will be disabled. You can click the **HTTPS Port** and **Multiline Policy** links to enter the **Login** page to view HTTPS port settings and **Multiline Options** page to view the multiline settings respectively.

Note: Both IPv4 address and IPv6 address are supported for the access address.

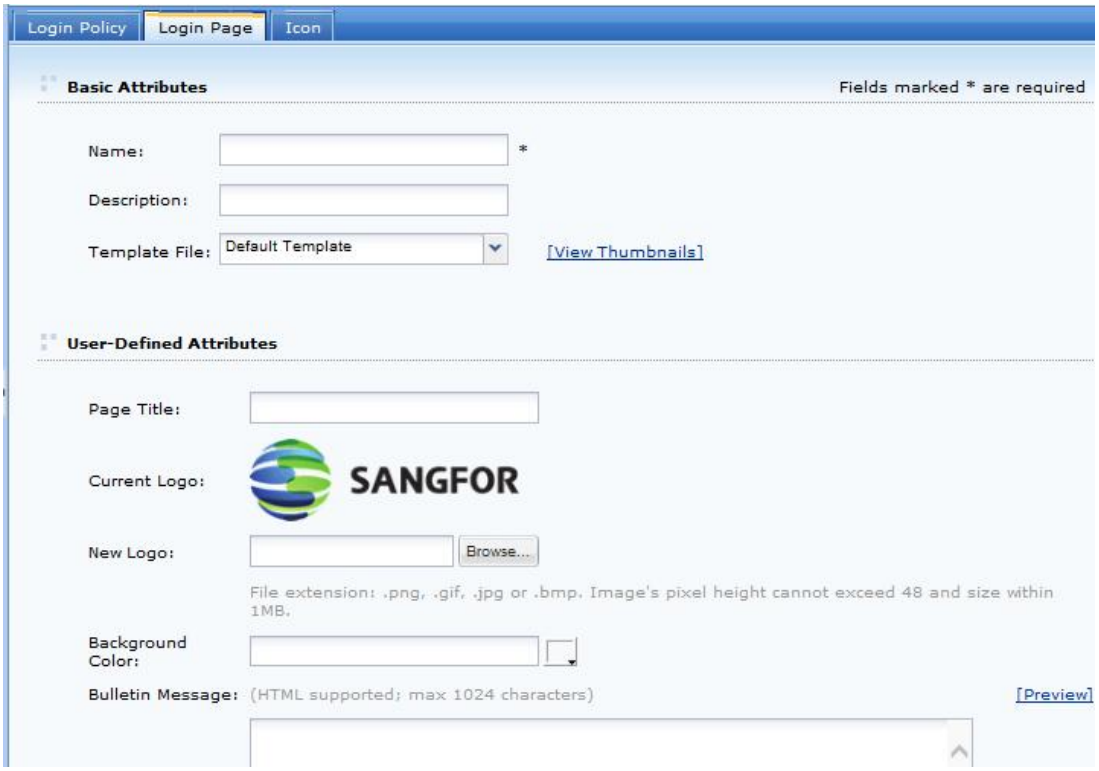
Configuring Login Page

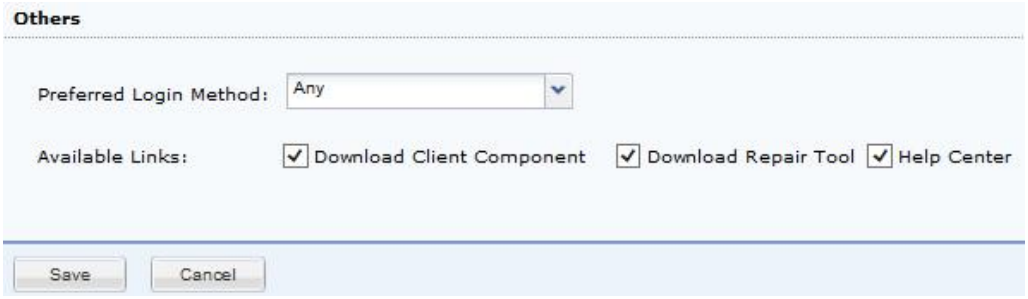
1. Navigate to **System** > **SSL VPN Options** > **Login Policy** > **Login Page**. The **Login Page** is as shown in the figure below:



2. Click **Add** > **By using built-in template** to use built-in template as template or select **By uploading custom page** to upload a custom page as template to configure login page.

   If **By using built-in template** is selected, the contents are as shown in the figure below:





The following are the contents included in the above page:

- **Name:** Indicates the name of this login page.
- **Description:** Indicates the brief description of this login page.
- **Template File:** Specifies the system template based on which the login policy will be configured. To view the thumbnail of the built-in page template, click **View Thumbnails**.

- **Page Title:** Specifies the caption of the login page.
- **Current Logo:** Indicates the logo currently showing on the login page.
- **New Logo:** Upload a new logo to replace the current logo.
- **Background Color:** Indicates the background color of the login page.
- **Bulletin Message:** Enter the message into the textbox. This bulletin message will be seen on the portal after users log in to the SSL VPN. Maximum 1024 characters are allowed and HTML is supported. To preview the bulletin message, click **Preview**.
- **Preferred Login Method:** Specifies the default login method. Options are **Any**, **Use password**, **Use certificate** and **Use USB key.**

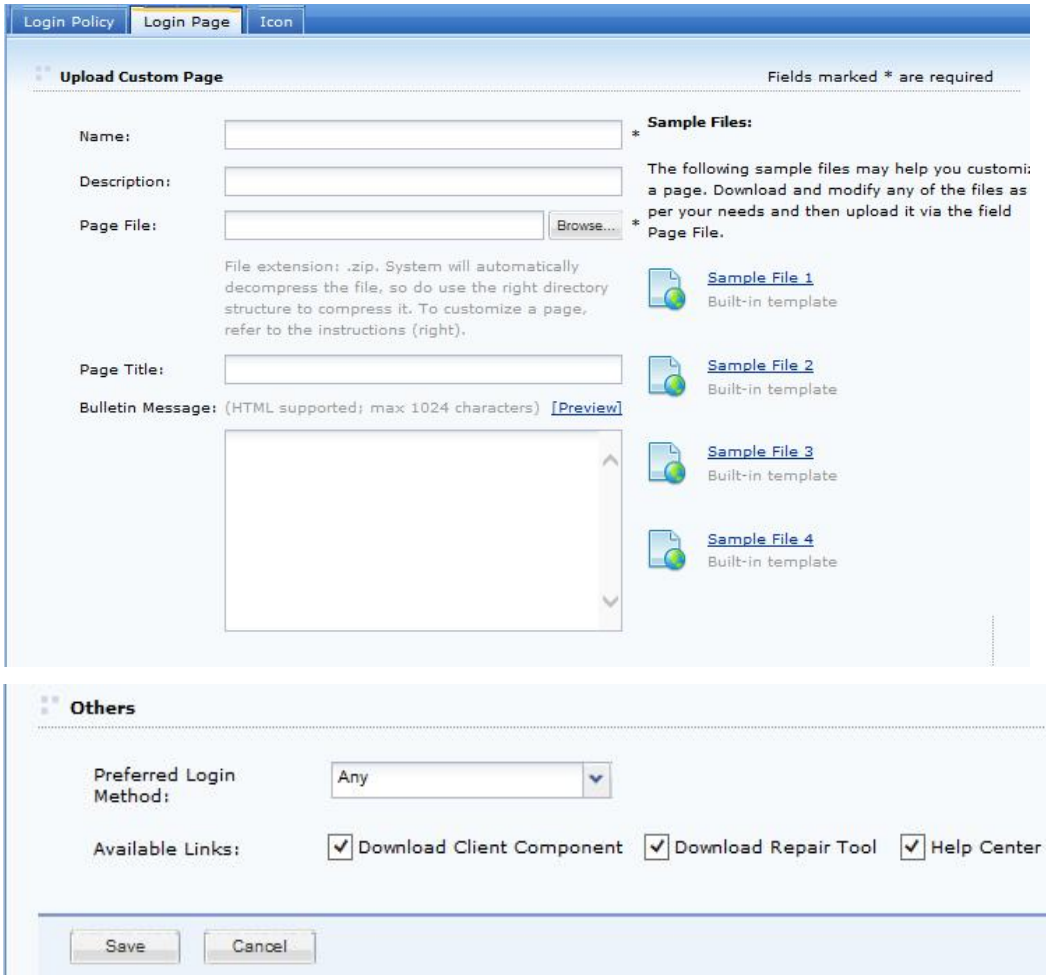


- **Available Links:** Indicates the links displayed on login page. It include **Download Client Component**, **Download Repair Tool** and **Help Center**.



If **Anonymous Login** is enabled on **SSL VPN > Authentication >Anonymous Login Options** page, **Preferred Login Method** option becomes unavailable.

If **By uploading custom page** is selected, the contents are as shown in the figure below:



The following are the contents included in the above page:

- **Name:** Indicates the name of this login page.
- **Description:** Indicates the brief description of this login page.
- **Page File:** Upload a page file though this field. The file extension must be **.zip**. At the right side of the page, there are instructions on how to upload a page file and three sample page files available.
- **Page Title:** Specifies the caption of the login page.
- **Bulletin Message:** Enter the message into the textbox. This bulletin message will be seen on the portal after users log in to the SSL VPN. Maximum 1024 characters are allowed and HTML is supported. To preview the bulletin message, click **Preview**.
- **Preferred Login Method:** Specifies the default login method. Options are **Any**, **Use password**, **Use certificate** and **Use USB Key.**



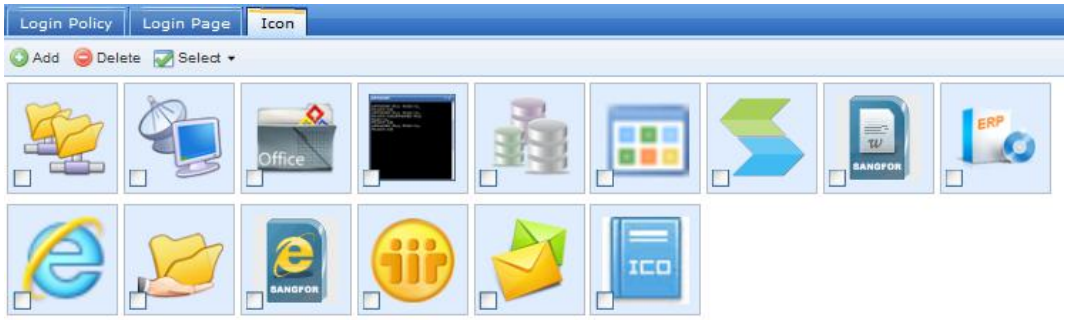
- **Available Links:** Indicates the links displayed on login page. Options are **Download Client Component**, **Download Repair Tool** and **Help Center**

3. Click the **Save** button to save the settings on this page.

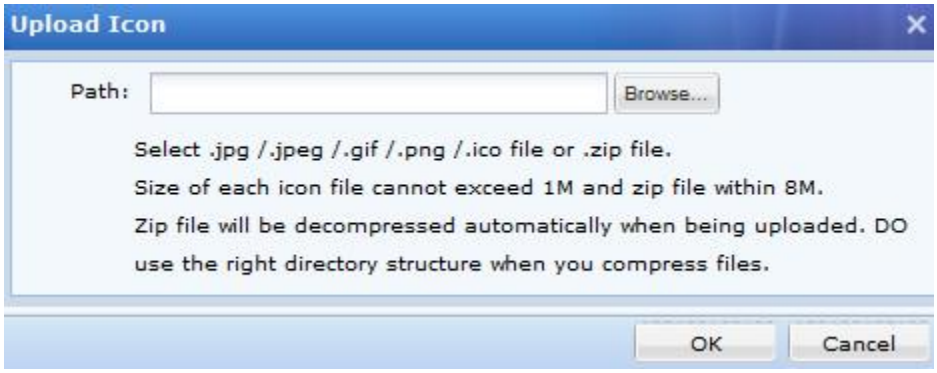
Uploading Icon to Device

Recalling from the above section on configuring the login page, we know that when defining a login page, there is a field requiring logo. Except that configuration, images or icons are also needed in some other places. Such kinds of images used by Sangfor device could be uploaded to and managed on Sangfor device.

1. Navigate to **System** > **SSL VPN Options** > **Login Policy**> **Icon** to enter the **Icon** page, as shown in the figure below:



2. Click **Add** to enter **Upload Icon** page, as shown in the figure below:



3. Browse an image file and click the **OK** button.

Clustering

Cluster enables multiple independent servers (nodes) to work as single system and be managed as a single system. A node (in fact, a Sangfor device) in a cluster may be a real server being managed by one node master, or the dispatcher (a real server by nature).

While an Internet user accesses SSL VPN, the dispatcher will do scheduling and assign this session to a reasonable (most idle) real server to have this real server provide services to this user. In this way, the cluster can achieve the goal of enhancing system capacity and performance, and providing users with the best and most reliable services.

Terminology

Cluster: A cluster is a multi-processor system that is loosely coupled with a group of independent computers. It can achieve the goal of coordinating the communication and data synchronization among the scattered computers.

Dispatcher: It works as the load-balancing device of a cluster. Dispatcher itself is a real server.

Real server: A single Sangfor device that works as real server in a cluster.

Node: A general name for dispatcher and real server.

Cluster IP address: The IP address that the cluster communicates with the networks outside the cluster. This IP address is also used by user to access the SSL VPN if cluster is enabled.

Cluster key: It is the key intended for communication among the clustered nodes, which helps to encrypt the relevant data.

Weight: Performance metric of a cluster node. 0 indicates that node is not reachable.

Dynamical Weighted Least-Connection Scheduling: Or DWLC in short, is the weight reported by each server of the processing ability. It is playing such a role that the number of established sessions to a server could be in certain proportion with the weight while new session is about to assigned to clustered nodes.

Cluster IP: refers to the external IPv4 address and IPv6 address of the cluster, through which external users access SSLVPN.

Main Features of Cluster

- **High performance**

- A new connection will be scheduled to an optimal node based on Dynamical Weighted Least-Connection Scheduling.
- The consequent connections initiated by a same IP address will not be assigned to a different node, unless that IP address disconnects with the SSL VPN.
- Once the dispatcher receives a request, it assigns that request to a real server so that the real server will respond to the user.

- **High availability**
  - If a node gets into fault, this node will be removed from the available node list by the dispatcher when heartbeat detecting (a signal sent from LAN interface) timed out. The removal of this node from the available node list will only pose impact on the users that are being served by that node.
  - When a new node joins in the cluster, the dispatcher will add it to the available node list.
  - Once the dispatcher gets into fault, another node will be elected as the new dispatcher after two heartbeats in accordance with the priority (the higher priority a node has, the more likely it will be elected as dispatcher; if two nodes are of the same priority, the one that is higher in performance will take the place). Reelection of dispatcher will only pose impact on the users that are being served by the bad dispatcher.
- **Consistency of services**
  - If a new node joins in the cluster, it will download all the configurations and data from the dispatcher to keep consistent with it.
  - Administrator is allowed to make configuration changes after it logs in the console of the dispatcher. Logging in to any other node, the administrator has the privilege to configure basic settings related to cluster, but can only view other SSL VPN configurations.
  - Changes on any user or user information (such as password, hardware ID and mobile number) will be synchronized to all the other nodes in the cluster.
  - Changes on database of any node will trigger data checking which is based on that of the dispatcher. If database of a node is found inconsistent with that of the dispatcher, all the nodes will download the configurations and database from the dispatcher and then restart the related services.

    Some configurations and data will not be synchronized among the clustered nodes, but take effect on an individual node if operation is performed. These configurations and state information include network settings, logs, license, SSL VPN running status, restart device, configuration backup and restore, DHCP status, etc.
  - No data checking will be performed if there is no change made on database; however, if database of any node changes, database of any other node will be checked.
  - System time of the cluster group is synchronized from the dispatcher, keeping consistent with each other.
- **System monitoring**

- On the dispatcher, administrator can view the resource utilization of each clustered node, or restart SSL VPN service, all services or devices.
- Cluster online user list is also available on the dispatcher, including the information of which node each user is being served and the operation of disconnect the connecting user.

- **Hot plug of dispatcher**
  - **Single node:** A node can be elected as dispatcher in an interval of two heartbeats.
  - **Dispatcher re-election:** If the dispatcher gets into fault, another node that has the highest priority will be elected as the new dispatcher in an interval of two heartbeats.
  - **Dispatcher re-election mechanism:** If a newly-joining node is configured with the highest priority (the only one in a cluster that has such highest priority), then this node will first become a real server of this cluster group, and in an interval of two heartbeats, become the dispatcher, while the original dispatcher will be degraded and become a real server.
- **Hot plug of node**
  - **Node joining cluster:** During the interval of the first heartbeat, the newly-joining node will download data from the dispatcher, decompress the data and replace the original ones, restart the services and check data. After the above series of operations, it will become a real server officially.
  - **Node getting into fault:** During the interval of two heartbeats, the bad node will be removed from the available node list by the dispatcher.
- **Reliability**

  With cluster being enabled, user can use any service provided by SSL VPN as long as at least one clustered Sangfor device keeps running. If user is using a static cluster IP address to access the services but that node gets into fault, the online users related to that node will be disconnected and required to re-login.

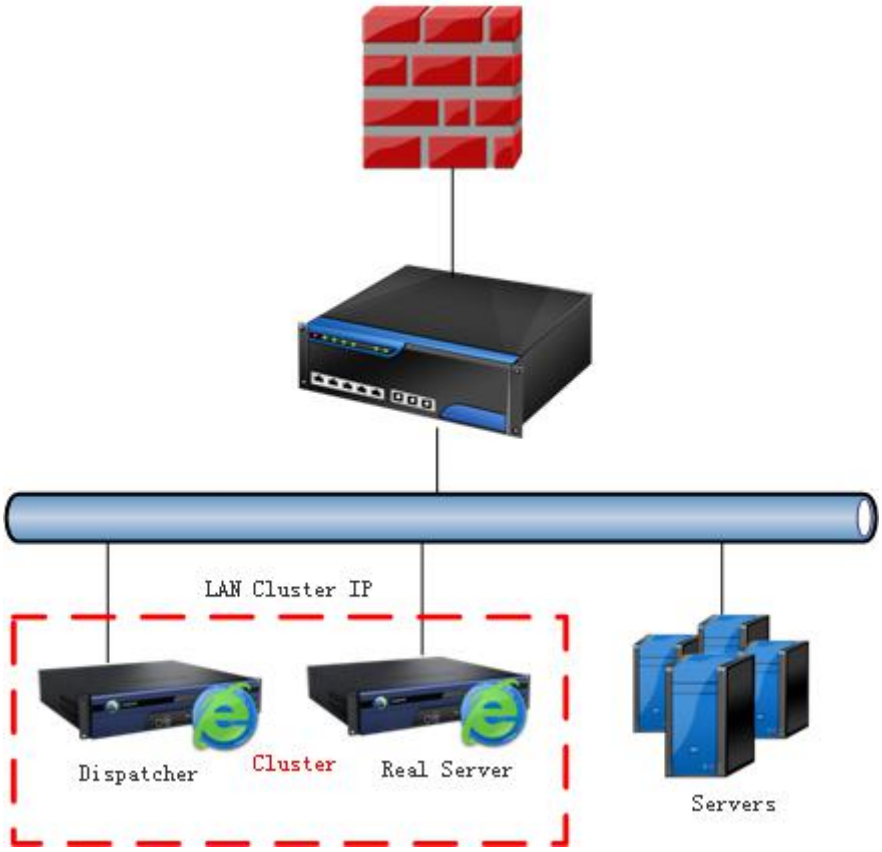
Deploying Clustered Sangfor Devices

Deploying Clustered Device in Single-Arm Mode

For clustered nodes deployed in **Single-arm** mode, the configurations of internal and external interfaces are the same as those on an individual Single-arm Sangfor device (please refer to the Device Deployment section in Chapter 3). One additional configuration is **Cluster IP Address** of **LAN** interface (under **System** > **SSL VPN Options** > **Clustering** > **Cluster Deployment**).

In addition, you need to configure the same cluster IPv4 address and cluster IPv6 address in **Cluster Deployment** > **Cluster IP Address** for each SSL device.

Typical network topology of cluster in **Single-arm** mode is as shown in the figure below:



- **LAN Cluster IP** address on every clustered device should be identical.
- **LAN interface IP** address (configured in **System** > **Network** > **Deployment**) and the **LAN Cluster IP** (configured in **System** > **SSL VPN Options** > **Clustering** > **Cluster**

Deployment) must be of a same network segment.

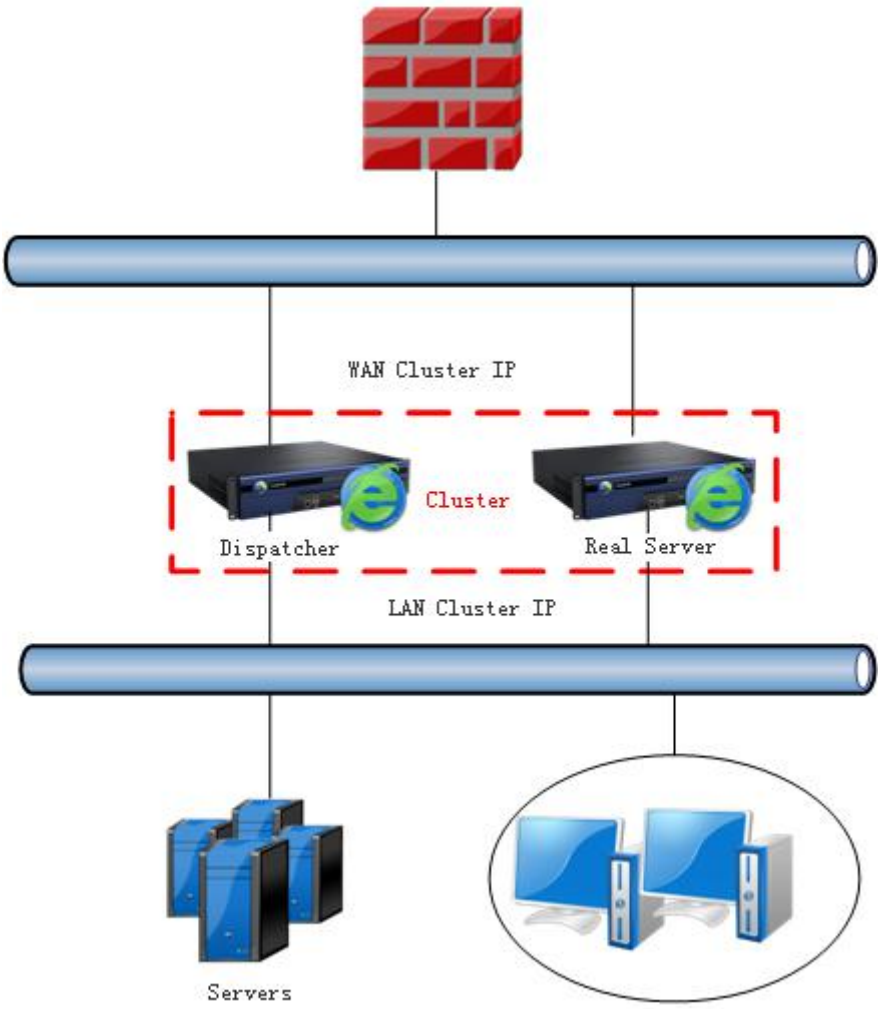
**Note: For Single-Arm deployment, the LAN interface IP addresses set in [LAN Interface Configuration] for all SSL devices in the cluster must be of the same network segment with the LAN interface cluster IPv4 address and cluster IPv6 address set in [Cluster Deployment]>[Cluster IP Address].**

▪

Deploying Clustered Device in Gateway Mode

For clustered nodes deployed in **Gateway** mode, the configurations of internal and external interfaces are the same as those on an individual Gateway-mode Sangfor device (please refer to the Device Deployment section in Chapter 3). One additional configuration is Cluster IP Address of LAN interface and WAN interface (under System > SSL VPN Options > Clustering > Deployment). In addition, you need to configure the same LAN interface cluster IPv4 address and cluster IPv6 address, as well as WAN interface cluster IPv4 address and cluster IPv6 address, in [Cluster Deployment]>[Cluster IP Address] for each SSL device.

Typical network topology of cluster in **Gateway** mode is as shown in the figure below:



- **LAN Cluster IP** address on every clustered device should be identical; so is the **WAN Cluster IP** address.
- WAN interface IP address on every clustered device should be of a same network segment; whereas **WAN Cluster IP** address and **WAN Interface IP** address configured on a Sangfor device **must NOT** be a same network segment.
- Cluster will not work if the Sangfor device works as gateway and dials up to Internet.

Note: For gateway deployment, the WAN interface IPv4 addresses or IPv6 addresses set in [WAN Interface Configuration] for all SSL devices in the cluster need to be of the same network segment, but of different network segment with the WAN interface cluster IPv4 address and cluster IPv6 address set in [Cluster Deployment]>[Basic Configuration]. When an SSL device servers as the gateway, the cluster is not supported if

the device is for dial-up access.

▪

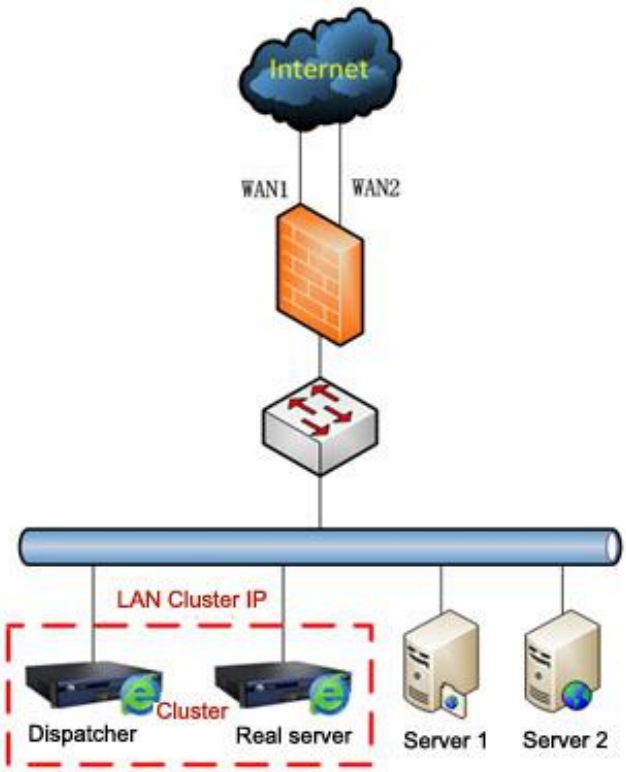
Deploying Clustered Device with Multiple Lines

For clustered nodes deployed with multiple lines, the configurations of internal and external interfaces are the same as those on an individual Sangfor device that has multiple lines (please refer to the Device Deployment section in Chapter 3). One additional configuration is **Cluster IP Address** of **LAN** interface and **WAN** interface (under **System** > **SSL VPN Options** > **Clustering** > **Deployment**).

LAN Cluster IP address on every clustered device should be identical; so is the **WAN Cluster IP address**. As a Sangfor device has more than one line, the **WAN Cluster IP** addresses on every clustered device must be consistent.

Single-Arm Sangfor Device with Multiple Lines

Typical network topology of cluster of **Single-arm** devices is as shown in the figure below:



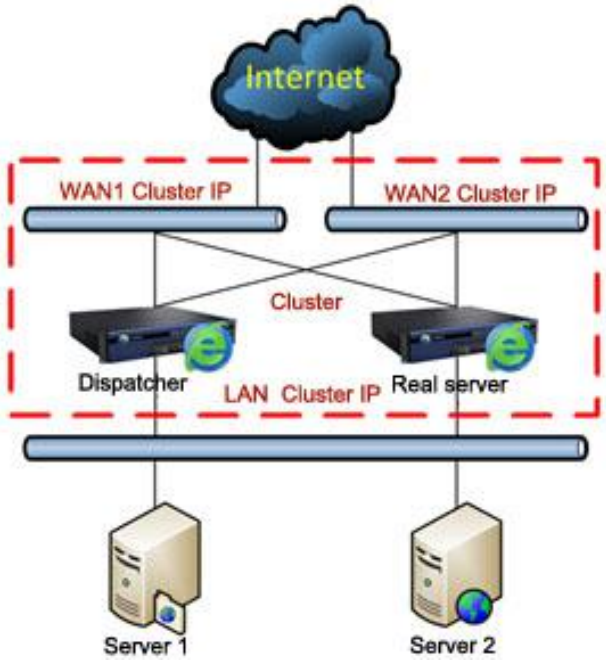
The cluster IP addresses configured on each clustered node (Sangfor device) should be consistent.

Note: You must enter the same cluster IPv4 address and cluster IPv6 address for each node in the cluster.

Gateway-mode Sangfor Device with Multiple Lines

Typical network topology of cluster of **Gateway-mode** devices is as shown in the figure below:

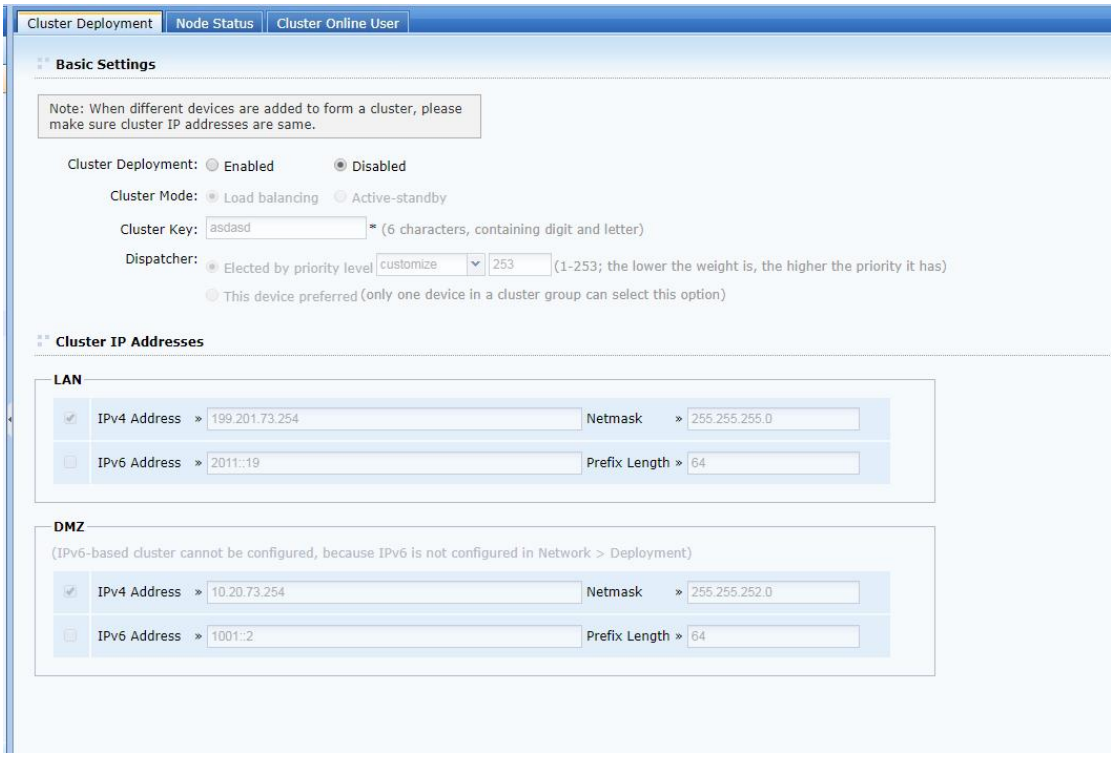
You need to configure the same LAN interface cluster IPv4 address and cluster IPv6 address, as well as WAN interface cluster IPv4 address and cluster IPv6 address (one WAN interface requiring one WAN interface cluster IPv4 address and cluster IPv6 address), in **Cluster Deployment** > **Cluster IP Address** for each SSL device.



Configuring Newly-Joining Clustered Device

Recalling from the above section, we know that cluster IP address for a newly-joining cluster needs to be configured. This section introduces how to configure the cluster IP address and other cluster related options for a device joining cluster.

1. Go to **System** > **SSL VPN Options** > **General** > **Clustering** > **Cluster Deployment**, as shown in the figure below:



2. Configure the following basic settings of the cluster:

- **Cluster:** It is a global switch to enable or disable the cluster functionality of the SSL VPN system. Select **Enabled** to enable cluster functionality and proceed to configure the related options.
- **Cluster Key:** Specifies the secret key to be used by the cluster. This field configured on every clustered node should be identical. If not the same, the secret key configured on the dispatcher will be taken as the ultimate key.
- **Dispatcher:** Specifies the way that dispatcher of the cluster is to be elected or specified. Select **Local device preferred** to specify this Sangfor device as the dispatcher; or select **Elected by priority level** to have the dispatcher be elected in accordance with the priority level that may be high, medium, low or user-defined value.

  High means that the node is more likely to be elected as the dispatcher; **medium** indicates that the node is less likely to be elected as the dispatcher, while **low** indicates that node is least likely to be elected as the dispatcher.

  The value of priority level, however, will be compared with those values configured on other clustered nodes. Opposed to what is indicated by the concept **High** or **Low**, the lower the value, the higher priority that node has, and the more likely it will be elected as the dispatcher. The node will be elected as the dispatcher that has the highest priority (with the lowest value).

  For the option **This device preferred**, only one Sangfor device in a cluster group can

use this option.

3. Specify the cluster IP address of LAN interface, DMZ interface and WAN interface.

   Any Sangfor device that joins in a cluster should be configured with the same cluster IP addresses as those on other clustered nodes.

   LAN Cluster IP: Cluster IP address of LAN interface, being launched to external networks.

   DMZ Cluster IP: Cluster IP address of DMZ interface, being launched to external networks.

   WAN1 Cluster IP: Cluster IP address of WAN1 interface, being launched to external networks.

   Netmask: Indicates the network mask of the corresponding cluster IP address.

   WAN1 Interface Gateway: Specifies the gateway of the WAN1 interface.

   Cluster IP address is a group of IP addresses of a cluster formed by more than one Sangfor devices, and will be launched to the external networks. These IP addresses configured on each clustered node must be consistent.

4. Click **Save** to save the settings.

[Cluster IP Address] is used to set the cluster IPv4 address and cluster IPv6 address for each network port. You must enter the same cluster IPv4 address and cluster IPv6 address for each SSL device added to the cluster.

[LAN Configuration] is used to set the LAN interface cluster IPv4 address and cluster IPv6 address to be released.

[DMZ Configuration] is used to set the DMZ interface cluster IPv4 address and IPv6 address to be released.

[WAN Configuration] is used to set the WAN interface cluster IPv4 address and cluster IPv6 address to be released.

[WAN Interface Mask] is used to set the mask and prefix of the WAN interface.

[WAN Interface Gateway] is used to set the gateway information for the WAN interface.

Note: Cluster IP refers to released IP addresses of the cluster system composed of a group of SSL devices. The settings of each device in the cluster must be consistent in [Cluster IP Address].

Note: In Cluster IP, the IPv4 address is mandatory and IPv6 address is optional.

Click Save to validate the configuration.

5.

Viewing Clustered Node Status

Clustered node information includes IP address of clustered node, node type (dispatcher or real server), CPU utilization of node, number of licenses each node can grant, connecting users of each node, as well as total licenses and total online users.

Navigate to **System** > **SSL VPN Options** > **Clustering** > **Node Status** and the **Node Status** page appears, as shown in the figure below:



To enter the administrator console of a clustered node, click the **Login to Node** link.

Viewing Cluster Online Users

Cluster online users information includes the number of users connecting to SSL VPN, username, IP address of user's host, IP address of the node that is providing services to connecting user and the time when the user connects in.

Navigate to **System** > **SSL VPN Options** > **Clustering** > **Cluster Online User** and the **Cluster Online User** page appears, as shown in the figure below:



The following are the contents included on **Cluster Online User** page:

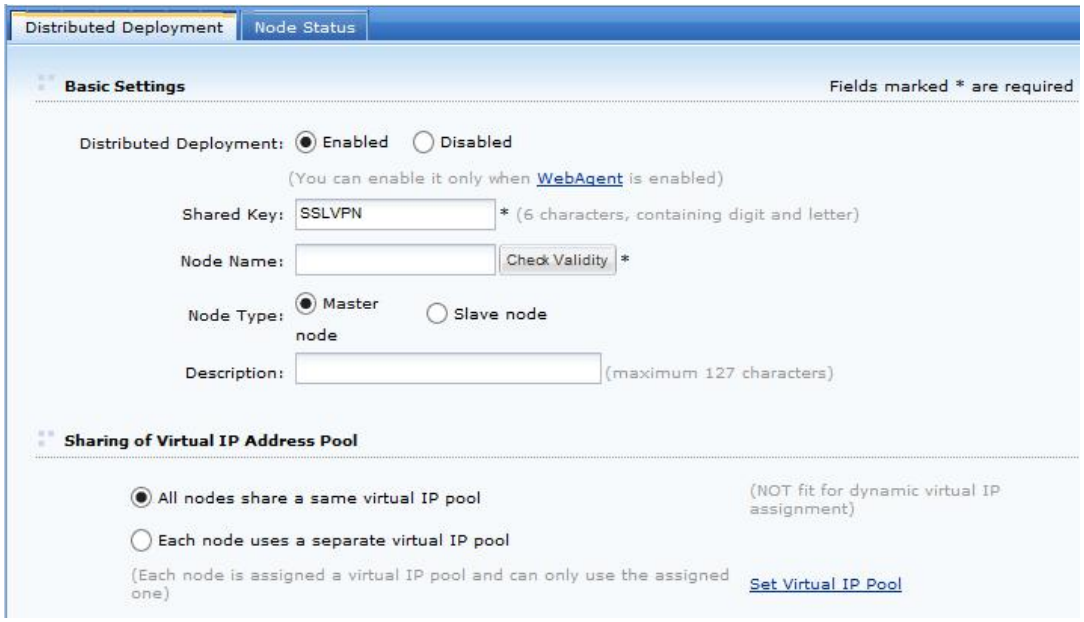
- **View:** Select an option to view a specific type of clustered nodes to show. It is **All nodes** by default.
- **Refresh:** Click it to refresh the status information on the **Cluster Online User** page.
- **Disconnect:** Click it to disconnect the selected user from the SSL VPN.
- **View Locked Users:** Click it to view the locked users. Administrator can unlock them when viewing the locked users.
- **Search:** To search for a specific user, enter the keyword into **Search** field and then click the magnifier icon or press **Enter** key.

Distributed Nodes

Distributed Deployment

With distributed deployment enabled and configured properly, the Sangfor devices scattered over the Internet could keep load-balanced.

Navigate to **System** > **SSL VPN Options** > **Distributed Nodes** to enter the **Distributed Deployment** page, as shown in the figure below:



The following are the contents included on **Distributed Deployment** page:

- **Distributed Deployment:** A global switch intended for enabling or disabling distributed deployment of SSL VPN system. To enable the distributed deployment, select **Enabled**.
- **Shared Key:** Specifies shared key, no more than 6 characters. It is used for distributed deployment.
- **Node Name:** Specifies the name of the node (Sangfor device). After entering node name, click the **Check Validity** button to check on the WebAgent whether this name is valid.
- **Node Type:** Specifies the type of node. **Master node** indicates that the current node is a master node, while **Slave Node** indicates that the current node is a slave node.
- **Description:** Enter brief description for the node.
- **All nodes share a same virtual IP pool:** Indicates that all nodes share the settings of a virtual IP pool. This option is applicable to the case that administrator specifies a virtual IP address to the user when creating the user account. Users use their own specified virtual IP address to log in to distributed node. Please note that this option is not suitable for dynamic virtual IP assignment, because assignment of virtual IP addresses to connecting users of

different nodes may cause IP address conflict.

- **Each node uses a separate virtual IP pool:** Indicates that each node is assigned a different virtual IP range and its connecting users use those IP addresses in that pool only. The user who logs in to a distributed node will use an IP address assigned from its specific IP address pool, which can eliminate the possibility that the IP addresses assigned to users of different nodes conflict.
- **Set Virtual IP Pool:** Click this link to enter the **Virtual IP Pool** page and configure the virtual IP pools. Virtual IP addresses are to be used by the users while they are accessing the distributed nodes (please refer to the Configuring Virtual IP section in Chapter 3).
- **Save:** Click it to save the settings.

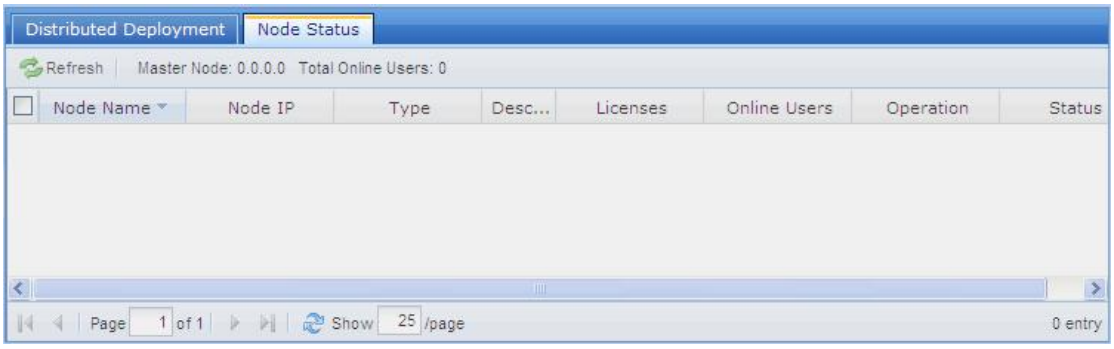


- Distributed deployment requires that WebAgent is enabled and configured properly.
- If **Users user different login page** option is enable on **System > SSL VPN Options > Login Policy** page, distributed deployment cannot be enabled.

Viewing Status of Distributed Nodes

Status of distributed nodes include real-time status of the master node and slave nodes, such as name, IP address, type, description, status, number of licenses and online users of each distributed node.

Navigate to **System** > **SSL VPN Options** > **Distributed Nodes** > **Node Status** and the **Node Status** page is seen, as shown in the figure below:



To enter the administrator console of a node, click the **Login to Node** link in the column **Operation**.

Chapter 4 SSL VPN

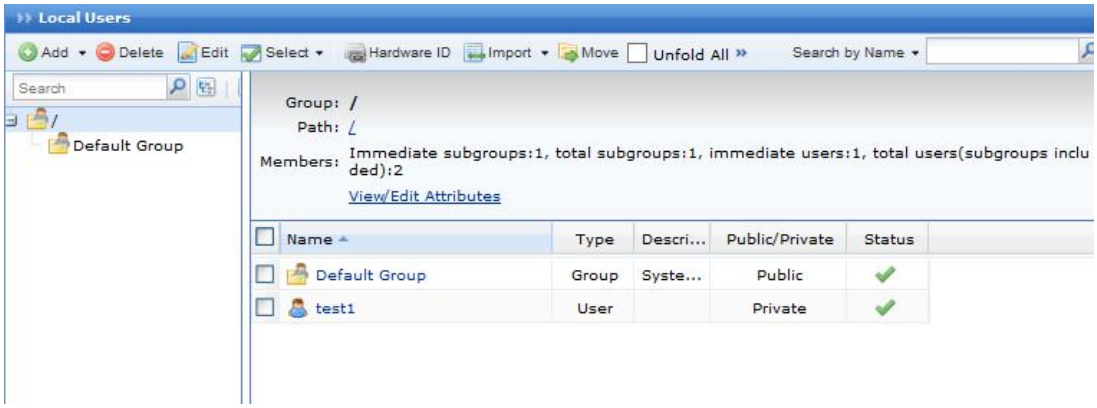
SSL VPN covers configurations of **Users**, **Resources**, **Roles**, **Authentication**, **Policy Sets, Remote Servers** and **Endpoint Security**.

SSL VPN options are crucial, because they are the core of the entire SSL VPN system, in particular those in **Users**, **Resources** and **Roles**. The relationships among the three factors are: **role** is the joint where the **user (group)** and **resource** are associated; **user** in certain group can acquire the right to access certain **resource** as per the privileges and realms granted to that **user group**.

SSL VPN Users

Users and groups are managed in a hierarchic structure. The users with similar attributes could be classified into a group which is further included in another higher-level user group. This kind of management is similar to and compatible with the interior organization structure of an enterprise, facilitating management of VPN users.

Navigate to **SSL VPN** > **Users** to enter **Local Users** page, as shown below:



In the left pane, there is a tree of user groups. Click on a group name, and the subgroups and direct users of that group will be seen in the right pane, with group information (**Group**, **Location**, number of **member**s) displaying above right pane.

To search for a group, enter keyword of the group name into the **Search** field in the left pane and click the magnifier icon. The group will be highlighted in bold if found.

To see all direct and indirect users of the selected group, click **Unfold All**.

To delete the selected user or group, click **Delete**.

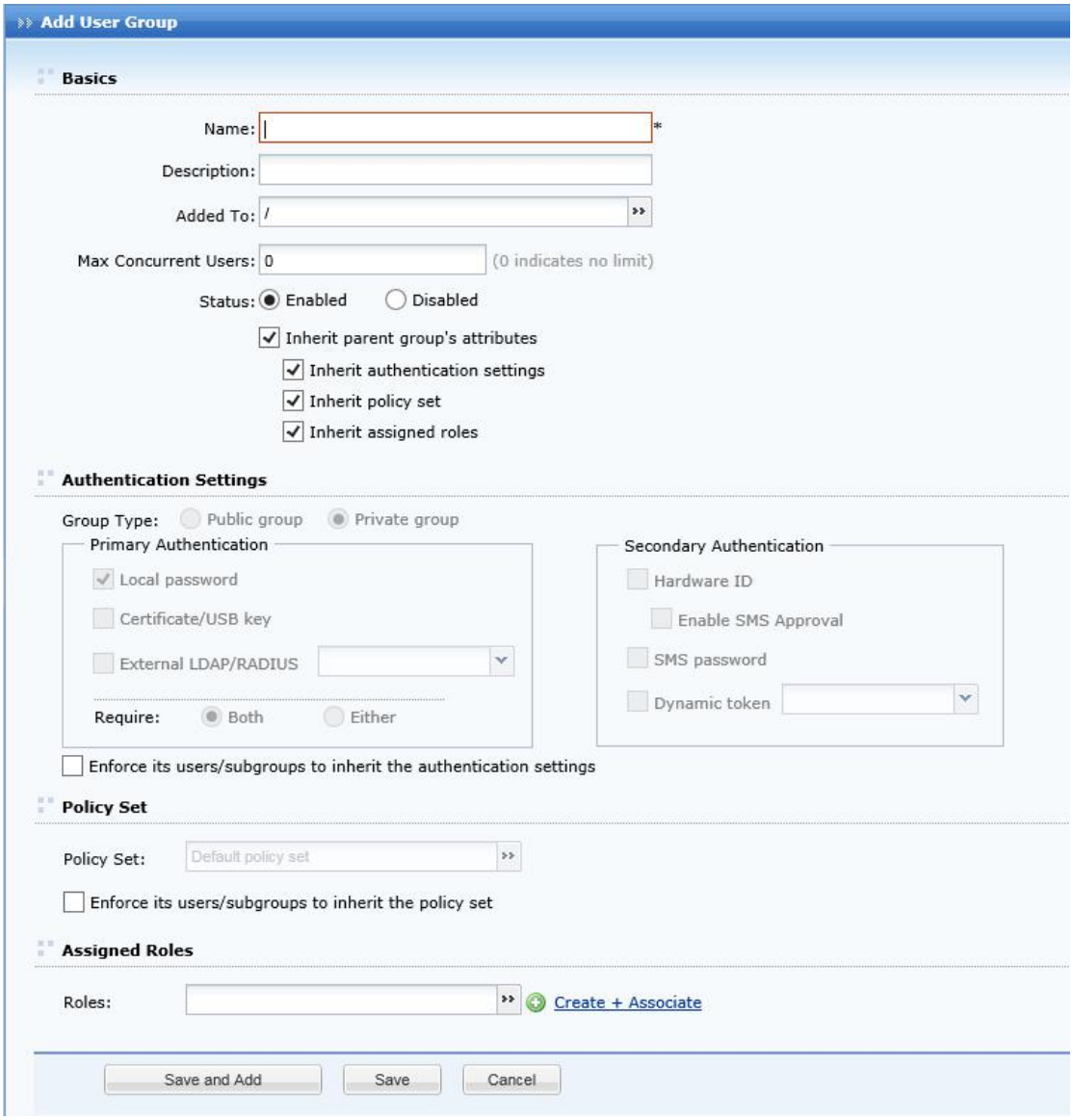
To choose the desired entries, click **Select** > **Current page** or **All pages**.

To deselect entries, click **Select** > **Deselect**.

To edit the attributes of a user or group, select the user or group and click **Edit** to enter the **Edit User** or **Edit User Group** page.

Adding User Group

1. Navigate to **SSL VPN** > **Users** > **Local Users** page. Click **Add** > **User Group** to enter **Add User Group** page, as shown in the figure below:

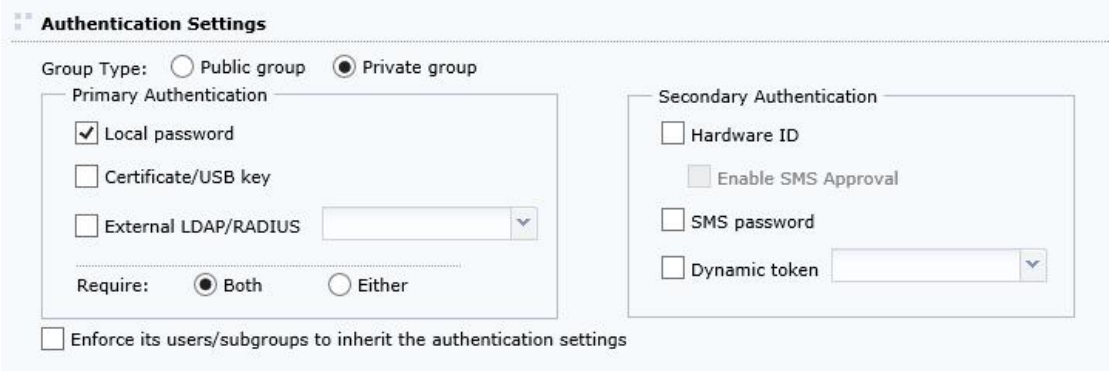


2. Configure **Basic Attributes** of the user group. The following are basic attributes:

   - **Name:** Enter a name for this user group. This field is required.
   - **Description:** Enter brief description for this user group.
   - **Added To:** Select the user group to which this user group is added. / indicates root group.

- **Max Concurrent Users:** Indicates the maximum number of users in this group that can concurrently access SSL VPN.
- **Status:** Indicates whether this user group is enabled or not. Select **Enabled** to enable this group; otherwise, select **Disabled**.
- **Inherit parent group's attributes:** Select the checkbox next to it and this user group will inherit the attributes of its parent group, such as the roles, authentication settings and the policy set.
  - **Inherit authentication settings:** Select the checkbox next to it and this user group will inherit the authentication settings of its parent group.
  - **Inherit policy set:** Select the checkbox next to it and this user group will inherit the policy set of its parent group.
  - **Inherit assigned roles:** Select the checkbox next to it and the current user group will inherit the assigned roles of its parent group.

3. Configure **Authentication Settings**.



- **Group Type:** Specifies the type of this user group, **Public group** or **Private group**.
  - **Public group:** Indicates that any user account in this group can be used by multiple users to log in to the SSL VPN concurrently.
  - **Private group:** Indicates that none of the user accounts in this group can be used by multiple users to log in to the SSL VPN concurrently. If a second user uses a user account to connect SSL VPN, the previous user will be forced to log out.
- **Primary Authentication:** Indicates the authentication method(s) that is (are) firstly applied to verify user when he or she logs in to the SSL VPN. If any secondary authentication method is selected, primary authentication will be followed by secondary authentication when the users log in to the SSL VPN.

  At least one primary authentication method should be selected, **Local password**, **Certificate/USB key** or **External LDAP/RADIUS**. However, two of them can form a combination.
  - **Local password:** If this option is selected, the connecting users need to pass local password based authentication, using the SSL VPN account in this user group.
  - **Certificate/USB key:** If this option is selected, all the user accounts in this group

must own digital certificate or USB key (ordinary or driver-free USB key).

- **External LDAP/RADIUS:** If this option is selected, an external authentication server (LDAP or RADIUS server) should be specified, which means, the account user used to connect the SSL VPN must exist on the selected external authentication server (to configure external authentication server, refer to the LDAP Authentication section and RADIUS Authentication section in Chapter 4).
- **Require:** It helps to achieve combination of two primary authentication methods. Options are **Both** and **Either**.

  Both means that the selected primary authentication methods (if two authentication methods are selected), and the user has to pass both the selected primary authentications.

  Either means that the selected primary authentication methods (if two authentication methods are selected), and the user has to pass either of the selected primary authentications.



- The available authentication servers are predefined. If there is no authentication server available in the drop-down list, navigate to **SSL VPN** > **Authentication** > **Authentication Options** page and configure the LDAP server or RADIUS server accordingly.
- **Local password** and **External LDAP/RADIUS** are alternative.

- **Secondary Authentication:** Secondary authentication is optional and supplementary authentication methods. Select any or all of them to require the connecting users to submit the corresponding credentials after he or she has passed the primary authentication(s), adding security to SSL VPN access.
- When the user logs in for the first time, the hardware ID is automatically approved by SMS approval. After the hardware ID is approved, the user logs in to the terminal again and directly verifies the hardware ID. If the hardware ID verification failed, it will proceed to SMS approval verification.
- Enable hardware ID and SMS approval. After the hardware ID is approved, if you replace new SSL VPN device, you need to verify again with SMS approval verification.
  - **Hardware ID:** This is the unique identifier of a client-end computer. Each computer is composed of some hardware components, such as NIC, hard disk, etc., which are unquestionably identified by their own features that cannot be forged. SSL VPN client software can extract the features of some hardware components of the terminal and generate the hardware ID consequently.

    This hardware ID should be submitted to the Sangfor device and bind to the corresponding user account. Once administrator approves the submitted hardware

ID, the user will be able to pass hardware ID based authentication when accessing SSL VPN through specified terminal(s). This authentication method helps to eliminate potential unauthorized access.

As mentioned above that multiple users could use a same user account (public user account) to access SSL VPN concurrently, it is reasonable that a user account may bind to more than one hardware IDs. That also means, an end user can use one account to log in to SSL VPN through different endpoints, as long as the user account is binding to the hardware IDs submitted by the user from those endpoints.

- **SMS password:** Implementation of this authentication requires that user's mobile number is available. Administrator configures the mobile number while adding or editing user account(for more, refer to **Adding User** section in chapter 4). If this option is selected, connecting user must enter the received SMS password after he or she passes the primary authentication and is going through SMS authentication, as shown in the figure below:



If the user fails to receive any text message containing SMS password, he or she can click **get again** to get a new SMS password.





- By default, SMS authentication will not be enabled if mobile number is not configured. SMS authentication comes into use only after, a). mobile number has been configured; b). **SMS password** has been selected; c). the required options on **SMS Authentication** page have been configured properly.
- Each user account supports only one mobile number. By default, the mobile number starts with China's international code **86**. If necessary, change this number to the international code of your own country (refer to the instructions on **SMS Authentication** page to configure SMS message delivery module).

- **Dynamic token:** If this option is selected, a RADIUS authentication server must be specified, which means, the account that user is using to connect SSL VPN must

exist on the selected RADIUS authentication server (to configure RADIUS server, refer to the RADIUS Authentication section in Chapter 4).

- **Enforce its users/subgroups to inherit the authentication settings:** If this option is selected, the subgroups and users included in this group will inherit the authentication settings configured above. However, its subgroups and sub-users could still use the other unselected authentication methods or use a different external authentication server, in addition to the inherited ones.

The combinations of authentication methods are as follows:

a. Local password + SMS password/Hardware ID/Dynamic token

b. Certificate/USB key + SMS password/ Hardware ID/Dynamic token

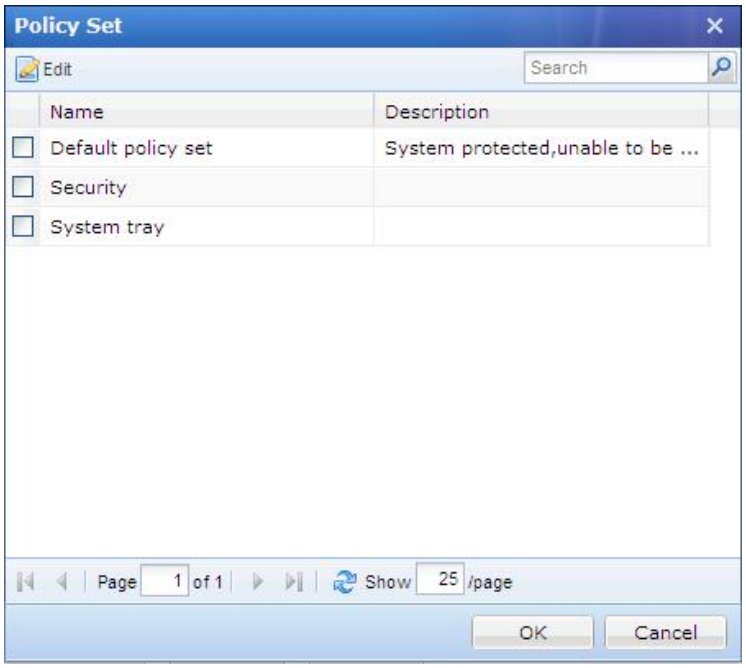
c. External LDAP/RADIUS + SMS password/Hardware ID/Dynamic token

d. Local password + Certificate/USB key + SMS password/Hardware ID /Dynamic token

e. External LDAP/RADIUS + Certificate/USB key + SMS password/Hardware ID /Dynamic token

4. Associate policy set with user. A policy set is a collection of various access policies, which should be associated with user or group to control access to and use of SSL VPN (for details, refer to the Adding Policy Set section in Chapter 4).

Click on **Policy Set** field to enter **Policy Set** page and select a policy set, as shown below:



To edit a policy set, select a policy and click **Edit**.

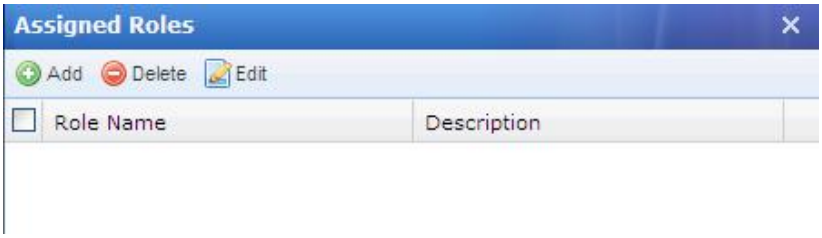
To confirm the selection, click the **OK** button and the selected policy set will be filled in **Policy Set** field.

If the desired policy set is not found in the list, click **Create + Associate** to create a new policy set and associate it with the user group. The procedures of adding a policy set is the same as that in Adding Policy Set section.

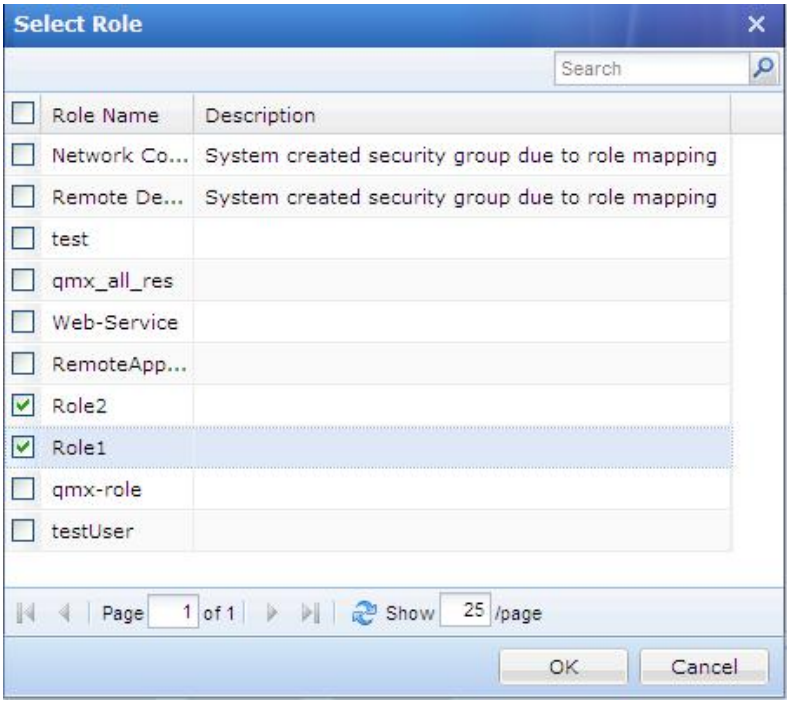
Enforce its users/subgroups to inherit the policy set: If this option is selected, the subgroups and users in this user group will also use this policy.

5. Assign roles to user group. For the procedures of configuring role, refer to the Adding Role section in Chapter 4.

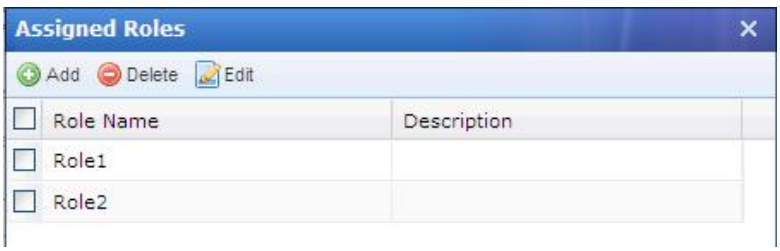
   a. Click on **Roles** field to enter the **Assigned Roles** page, as shown below:



   b. Click **Add** to enter the **Select Role** page, as shown below:



   c. Select the checkbox next to the desired roles and click the **OK** button. The roles are added in to the **Assigned Roles** page, as shown below:



   d. Click the **OK** button and name of the assigned role is filled in the **Roles** field.

e. If the desired role is not found in the list, click **Create + Associate** to create a new role and associate with the user group. The procedures of creating a role is the same as that in Adding Role section).

f. To remove a role from the list, select the role and click **Delete**.

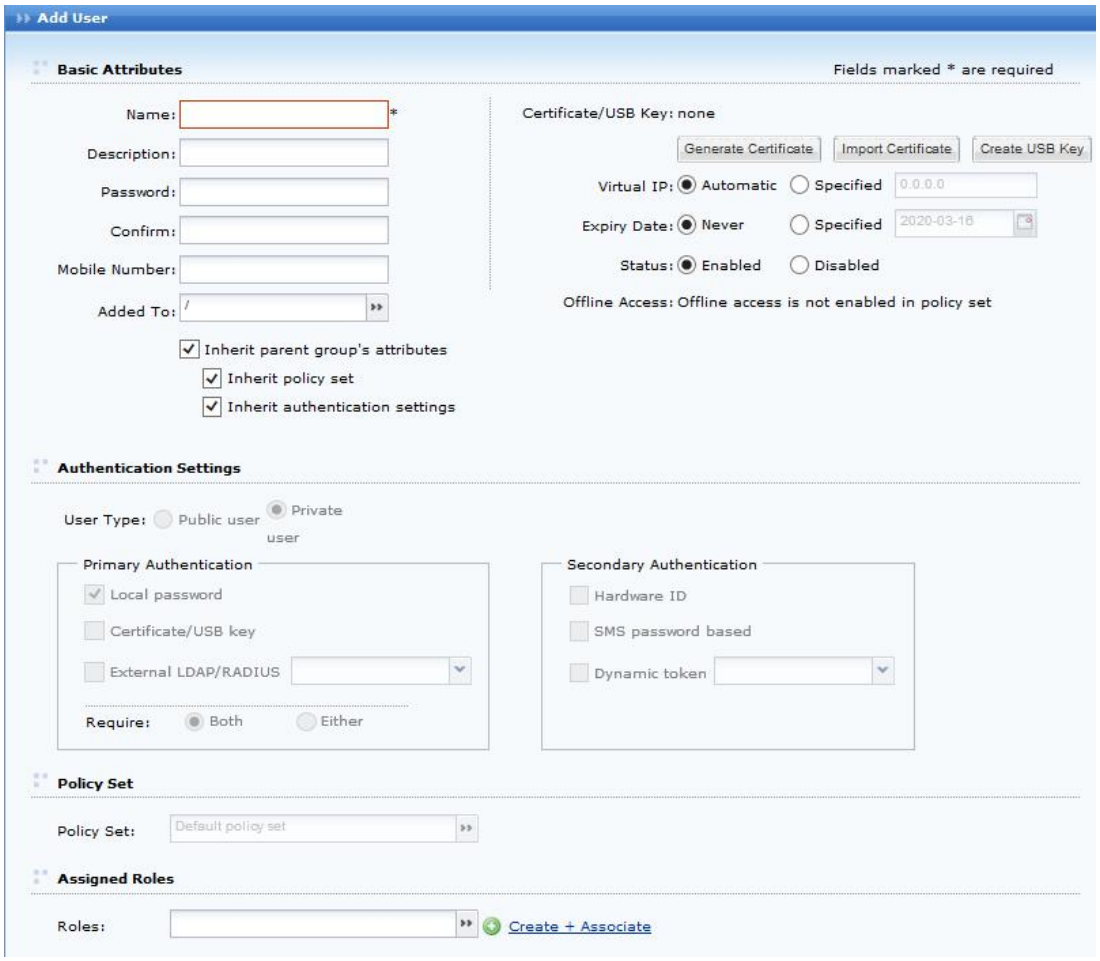
g. To edit a role, select the role and click **Edit**.



No user group can be added to **Default Group** or **Anonymous Group**.

Adding User

1. Navigate to **SSL VPN** > **Users** > **Local Users** page. Click **Add** and select **User** to enter the **Add User** page, as shown in the figure below:



2. Configure **Basis Attributes** of user. The following are the basic attributes:

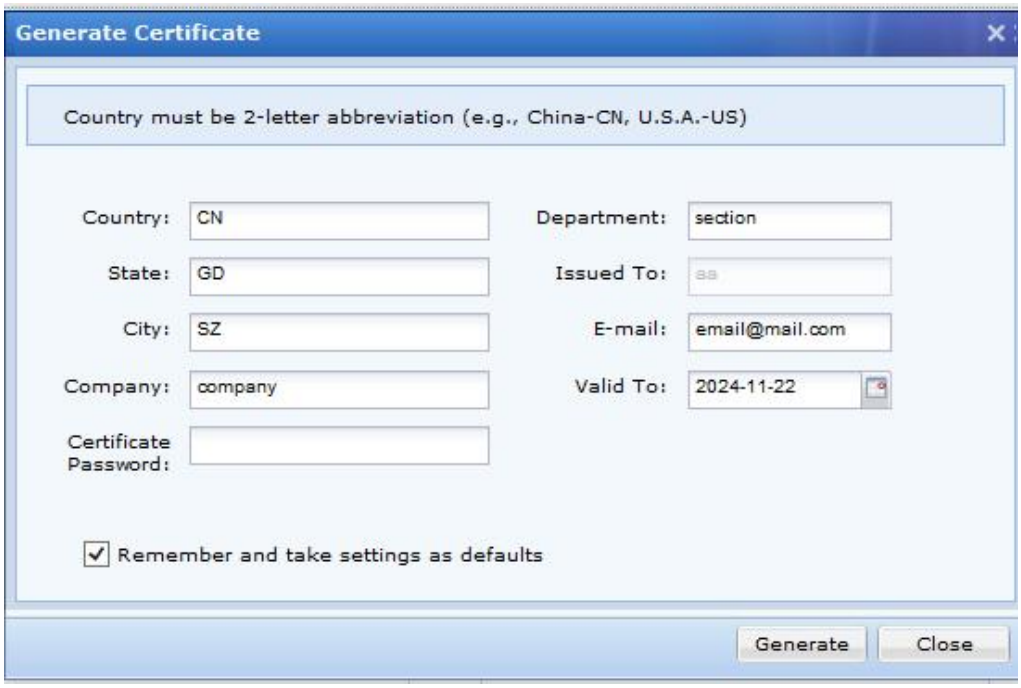
   - **Name:** Enter a name for this user. This field is required.
   - **Description:** Enter brief description for this user.
   - **Added To:** Select the user group to which this user is added.
   - **Password**, **Confirm:** Enter the password of this user account.
   - **Mobile Number:** Enter the mobile phone number of the user. If SMS authentication is applied to this user, mobile phone number must be specified so that user can get SMS password through text message.
   - **Added To:** Specifies to which user group this user is added.
   - **Inherit parent group's attributes:** If selected, the current user will inherit its parent group's policy set and authentication settings. If not selected, the authentication settings and policy set could be different from those of its parent group.
     - **Inherit policy set:** Indicates that the policy set of this user is the same with its parent group.
     - **Inherit authentication settings:** Indicates that the authentication settings of this user are the same with its parent group.

3. Create and generate digital certificate for this user.

   a. To generate a certificate, local CA should be enabled on **SSL VPN > Authentication > Certificate/USB Key Based Authentication** page. If it is not enabled, click the **Generate Certificate** button and a prompt dialog will pop up, as shown below:



   If local CA is enabled, click the **Generate Certificate** button to enter the **Generate Certificate** page, as shown below:



b. Configure the fields on the above page. Since these fields are known by their name, we only introduce the following:

- **Issued To:** Indicates the username of the SSL VPN account. This field is read-only.
- **Certificate Password:** This password is required while user imports or installs the digital certificate on his or her computer. Please inform the corresponding user of this password after configuration is completed.

c. Select the checkbox next to **Remember and take settings as defaults** and the settings in all the fields will be remembered (exclusive of **Certificate Password** and **Issued To**) and be re-used when generating certificate for users next time.

d. Click the **Generate** button to start generating the certificate. When it completes, the following prompt appears:

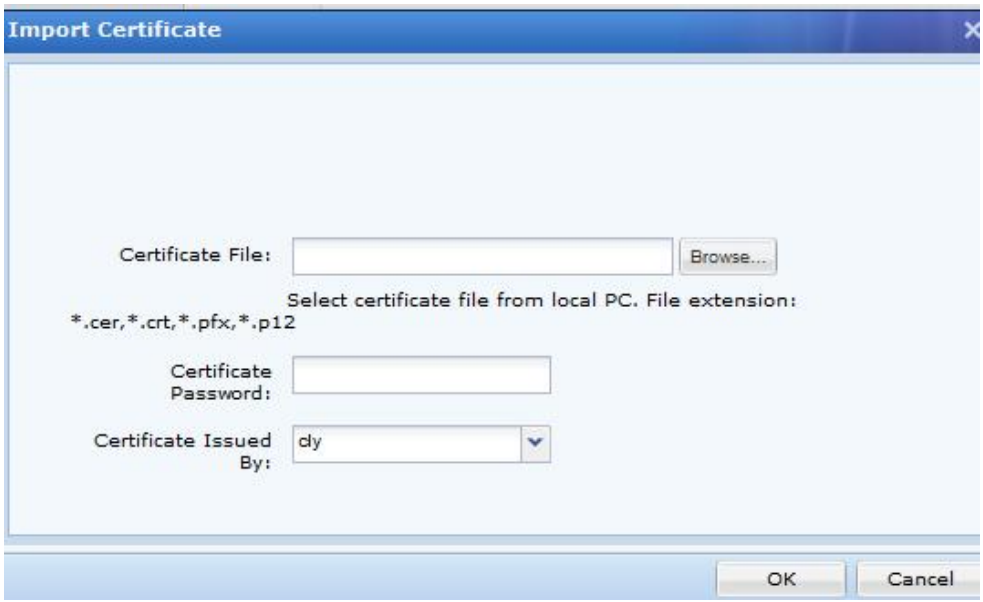


e. Click the **Download Certificate** button and select a path to save the certificate to the computer. File extension of the certificate is .p12. Then certificate key will be shown in **Certificate/USK Key** field, as shown in the figure below:



f. **Import Certificate** option is used to import user certificate for the user being authenticated with third-party digital certificate. Click **Import Certificate** to enter the

Import Certificate page, as shown below:



Select certificate file from local PC and specify certificate password and certificate issuer. Click **OK** to save the settings. Then you will see the certificate key, as shown below:



Put the cursor on "External CA", you will see an editing icon . Click on it and you can change user binding field and the external CA to which the certificate belongs.



4. Generate USB key for the current user. The USB key can be with driver or no driver-free.

   a. Navigate to **SSL VPN** > **Authentication** > **Authentication Options** and click the **USB Key Driver** link and **USB Key Tool** link to download and install USB key driver (file name is **dkeydrv.cab**) and USB key tool (file name is **DKeyImport.exe**) respectively, as shown in the figure below:

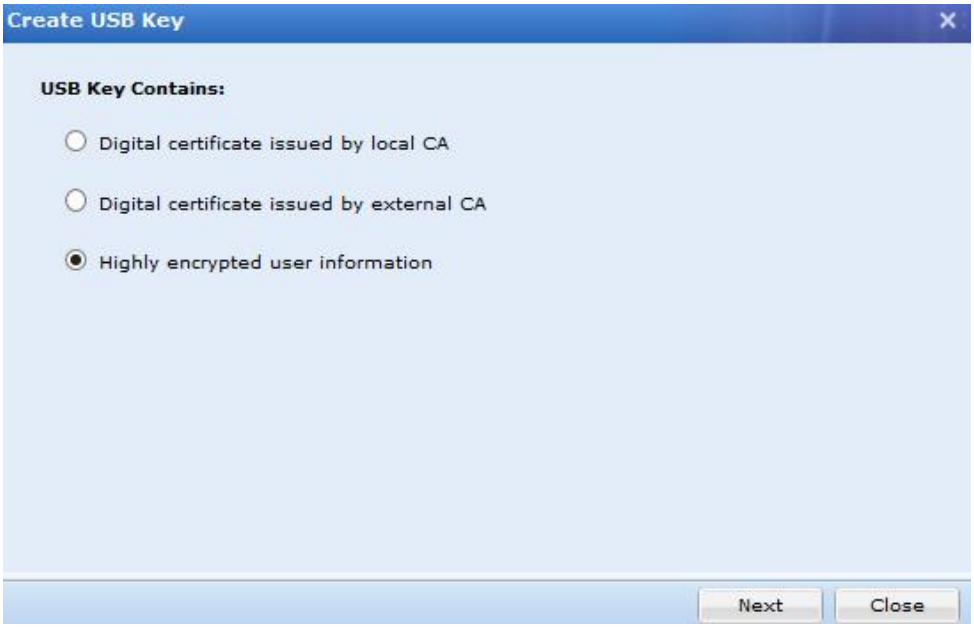


   b. Install the USB key driver as instructed.

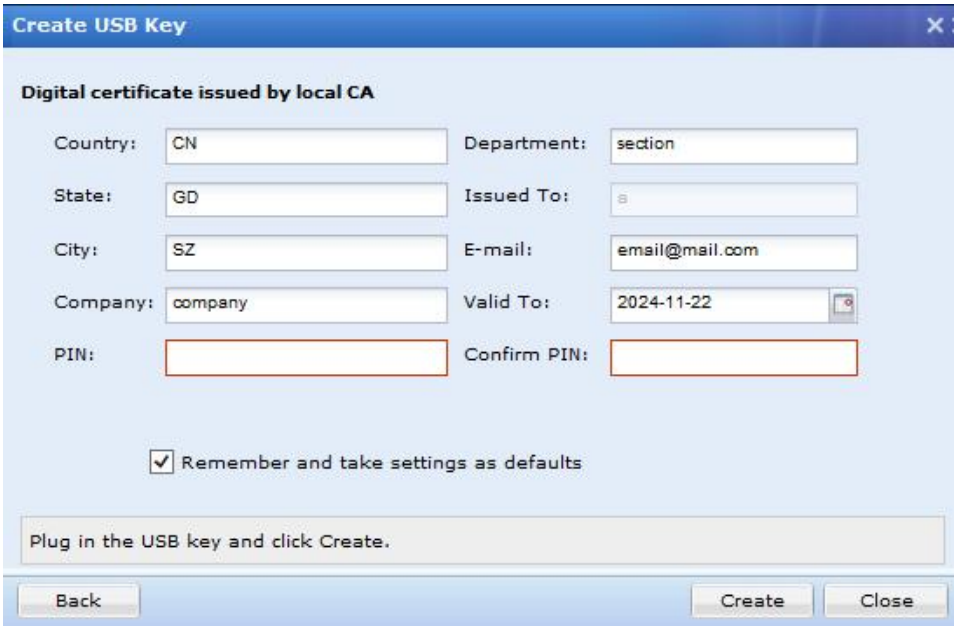
   c. Run USB Key Tool and install the tool on the computer.

Installing USB Key Tool requires “administrator” privilege on the computer. Otherwise, installation will not be complete.

d. Click the **Create USB Key** to enter Create USB Key page, as shown below:

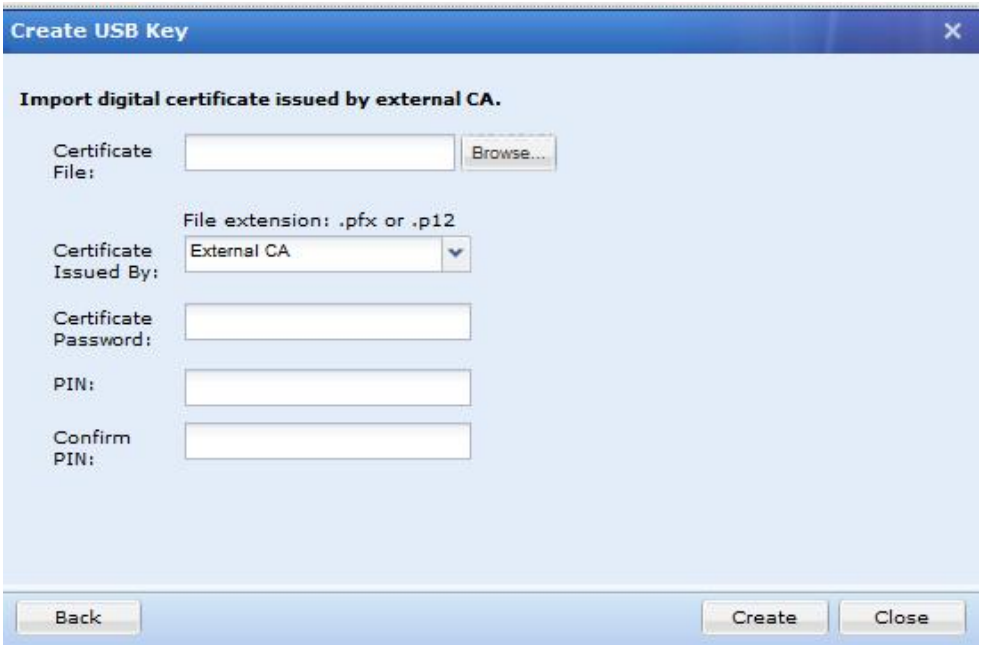


If **Digital certificate issued by local CA** is selected, the USB key should contain a digital certificate issued by the internal CA of the device (local CA) and user information, USB key PIN acting as password. Every time the user logs in to SSL VPN with USB key, he or she has to enter the PIN.



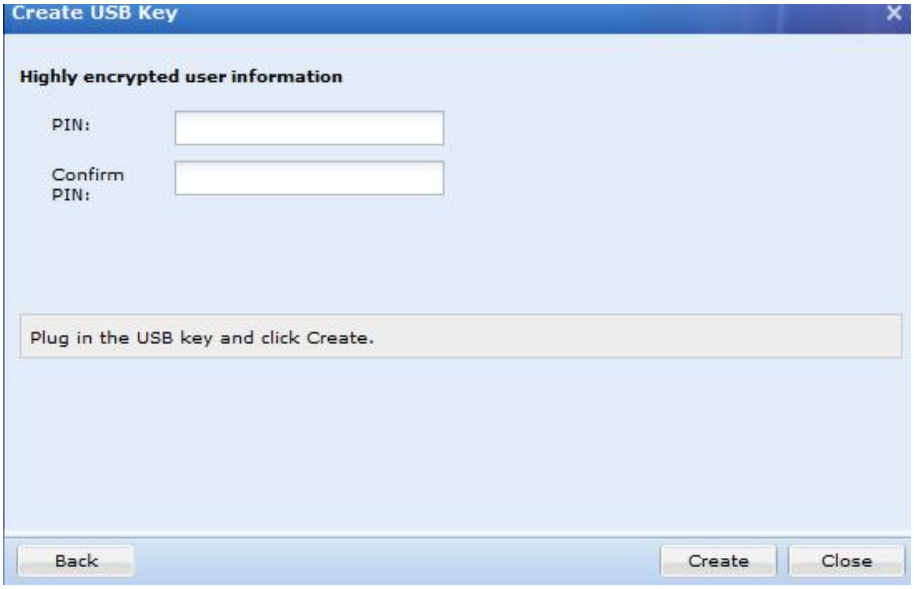
If **Digital certificate issued by external CA** is selected, the USB key should contain a digital certificate issued by the external CA and user information, USB key PIN acting

as password. Every time the user logs in to SSL VPN with USB key, he or she has to enter the PIN.



Above are two of the solutions, using ordinary USB key, which records the digital certificate and writes it into the USB key. The other solution is to use driver-free USB key, which means that the connecting user can directly use the USB key without installing the USB key driver.

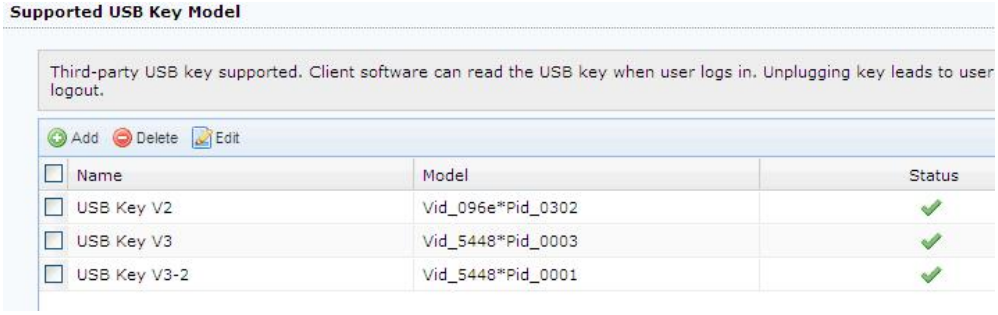
If **Highly encrypted user information** is selected, the USB key will store user's strictly-encrypted features (unique identifier) based on which the connecting user will be verified, as shown in the figure below:



Enter and Confirm the PIN. Insert USB key into computer and click **Create** to create USB key.

To create USB key containing **Highly encrypted user information**, you could go to

Certificate/USB Key Based Authentication page and configure the USB key models whose plugging in or unplugging can lead to user login or logout (for more details, refer to the Configuring USB Key Model section in Chapter 4), as shown in the figure below:



5. Assign virtual IP address to user. Virtual IP address will be assigned to connecting user automatically or manually when he or she connects to the SSL VPN.

   Select either **Automatic** or **Specified** to have the system assign an available virtual IP address to the connecting user randomly or specify a virtual IP address to the user.

   If **Specified** is selected, click **Get Idle IP** to obtain an available IP address or fill in a virtual IP address into the textbox by hand. This IP address will be assigned to the user in due course. However, if the entered IP address is not included in the virtual IP pool (that has been assigned to its parent group) or is being used by another user, a prompt of IP conflict will appear, as shown below:





- Automatic virtual IP address assignment applies only to private user.
- By default, user inherits the attributes of its parent group, such as authentication options, policy set, etc. However, you could uncheck the option **Inherit parent group's attributes** and specify an authentication solution for a specific user.

6. Configure valid time of the user account. **Expiry Date** indicates the date on which this user account will get invalid. If **Never** is selected, the user account will be valid always. If **Specified** is selected, select a date as expiry date.
7. Configure status of the user account. This user account will be enabled (valid) if **Enabled** is selected or disabled (invalid) if **Disabled** is selected.
8. Configure **Authentication Settings**. For details, please refer to the **Adding User Group**

section in Chapter 4.

- **Public user:** Indicates that multiple users can use the user account to access SSL VPN concurrently.
- **Private user:** Indicates that only one user can use the user account to log in to the SSL VPN at a time. If a second user uses this user account to connect SSL VPN, the previous user will be forced to log out.

9. Associate user with policy set. For detailed guide, please refer to the Adding User Group section in Chapter 4.
10. Assign roles to user group. For detailed guide, please refer to the **Adding User Group** section in Chapter 4.
11. Click the **Save** button and the **Apply** button to save and apply the settings.

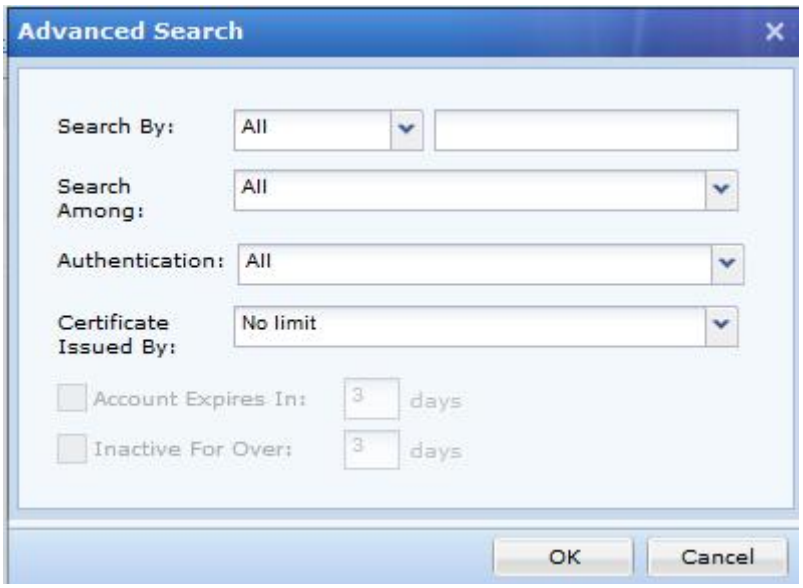
Searching for Users

At the upper right of **Local Users** page, there is a **Search** tool intended for searching for user or group, as shown below:



To search for user or group by username, description, virtual IP or mobile number, click and select **Search by xxx**, enter the keyword and click the magnifier icon or press **Enter** key.

To search for a specific user or category of users with specific criteria, click **Advanced Search**. The criteria for advanced search are as shown in the figure below:

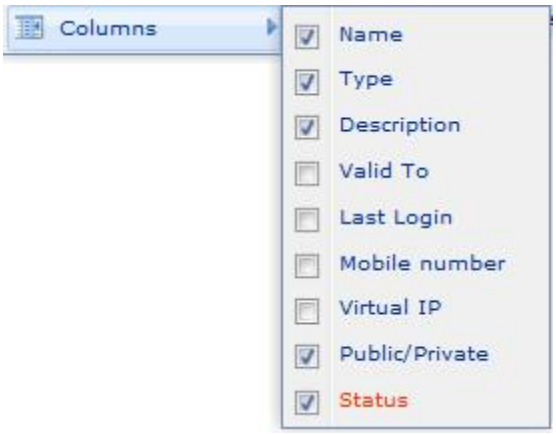


Search criteria are type of keyword, keyword, type of users, authentication method, certificate

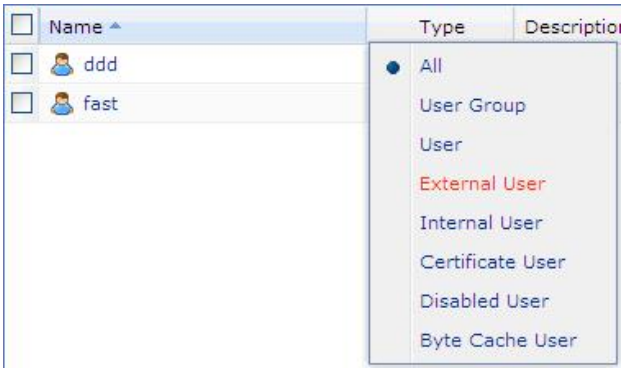
issuer, expiry date and idleness of the user account.

To sort users by name or description, in ascending or descending order, click column header **Name** or **Description**.

To specified columns to display on this page, click the downwards arrow icon and select the desired **Column** item in the drop-down list, as shown in the figure below:

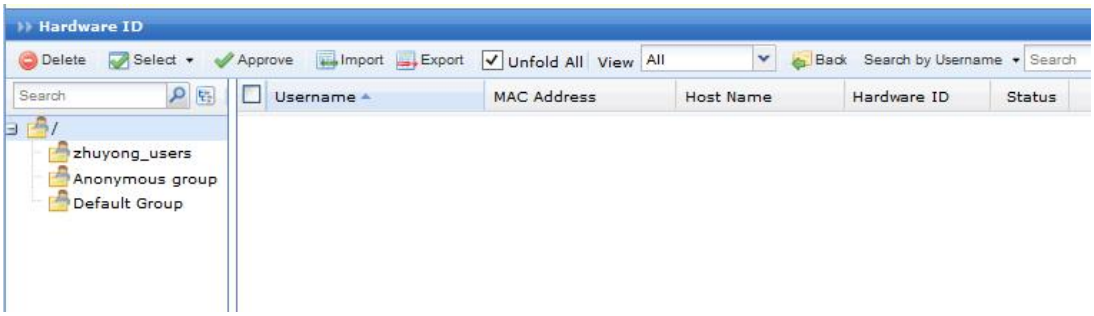


To filter users and view only one category of users, click column header **Type**, as shown below:



Managing Hardware IDs

Among the tools on **Local Users** page, there is an item **Hardware ID**. Click it to enter the **Hardware ID** page, as shown below:



The following are some optional operations on **Hardware ID** page:

- **Delete:** Click it to remove the selected user and/or group.
- **Select:** Click **Select** > **All pages** or **Current page** to select all the hardware IDs or only those showing on the present page; or click **Select** > **Deselect** to deselect users.
- **Approve:** Click it and the selected hardware ID(s) will be approved and the corresponding user will be able to pass hardware ID based authentication.
- **View:** Filter the hardware IDs. Choose certain type of hardware IDs to show on the page, **All**, **The approved** or **Not approved** hardware IDs.
- **Search:** Use the search tool on the upper right of the page, to search for hardware ID based on username or hostname.
- **Import:** Click it to import hardware IDs by hand, as shown below:



For the file format and the way of maintaining the file that contains hardware IDs, click the **Download Example File** link to download a copy to the local computer and main the hardware ID as instructed.

Overwrite the user owning a same name: If it happens that any imported user owns the name of an existing user, selection of this option would have that user imported and overwrite the existing user, including hardware ID and other information.

Click the **Browse** button to select a file and then **Upload** button to upload it.

- **Export:** Click it to export the desired hardware IDs and save them into the computer, as shown in the figure below:

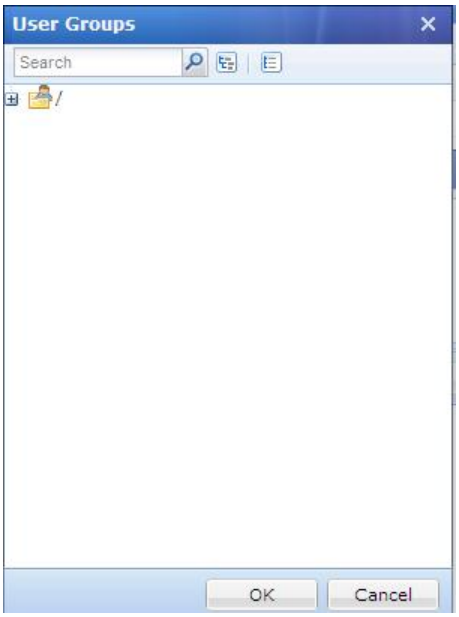


a. Specify the hardware IDs that you want to export.

To export all the hardware IDs, select the option **All hardware IDs** and then click the **OK** button. All the hardware IDs will be written into a file that will then be saved on the computer.

To export the desired hardware IDs of a specific user group, select **Hardware IDs of**

specified group and click the textbox to specify a user group, as shown below:



b. Click the **OK** button and the name of the selected user group is filled in the textbox, as shown in the figure below:

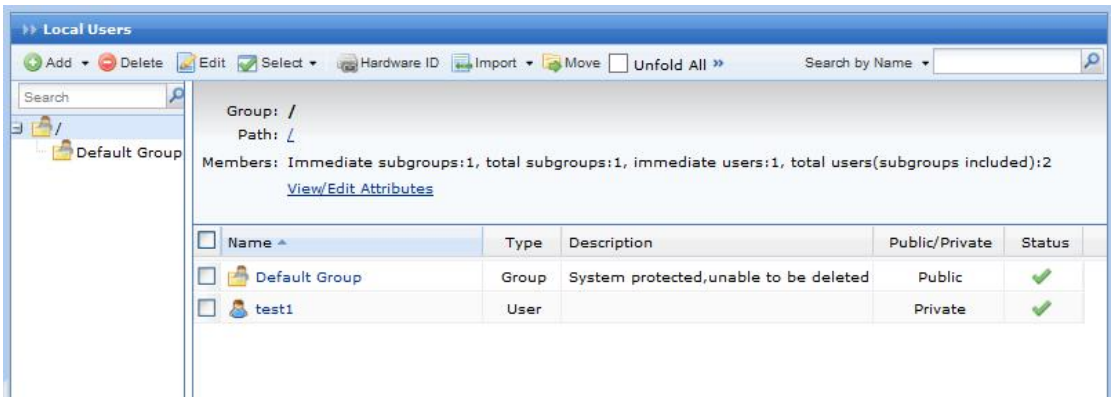


c. To also export the hardware IDs of the users that are included in the subgroups of the specified user group, select the checkbox next to **Subgroup included**. If this option is not selected, only the hardware IDs of the direct users in the selected group will be exported.

d. Click the **OK** button to write the hardware IDs into a file and download the file into the computer.

Importing User to Device

Ways of importing users fall into two types: one is **Import users from file** and the other is **Import users from LDAP server**, as shown in the figure below:



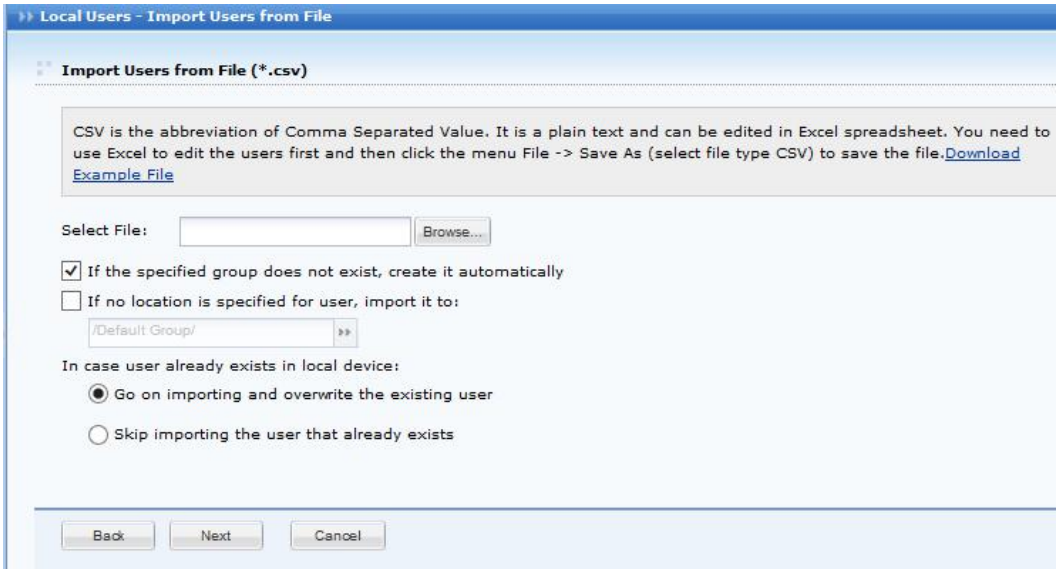
Importing Users from File

1. On the **Local Users** page, select **Import users from file** to enter the **Local Users - Import Users from File** page, as shown in the figure below:



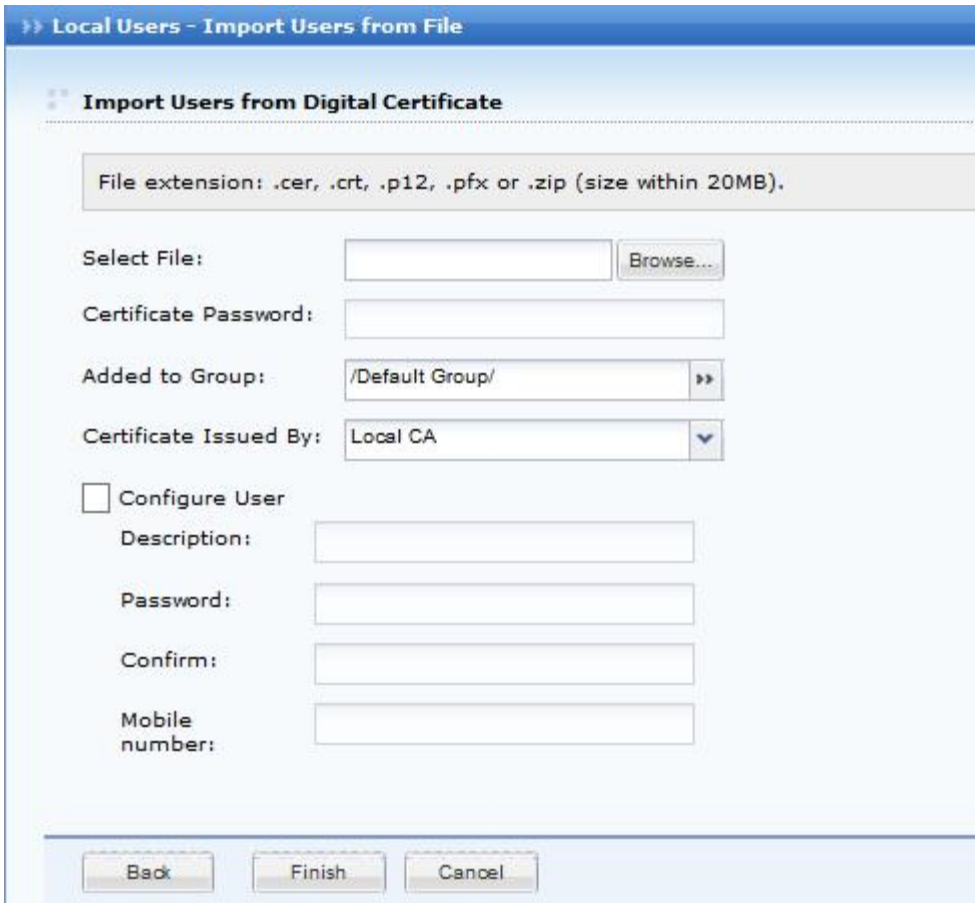
2. Select a way of importing.

   If **Import Users from File (*.csv)** is selected, the contents included are as follows:



- **Select File:** Browse a CSV file that contains user information, such as username, path, description, password, mobile number, virtual IP address, etc., among which the username is required, and others are optional. For more details on how to maintain and edit the CSV file, click the **Download Example File** link to download a copy and refer to the instructions in it.
- **If no location is specified for user, import it to:** This specifies the user group to which these users will be added if the **Added to Group** column is not filled in for some users in the CSV file.
- **If the specified group does not exist, create it automatically:** This happens if the **Added to Group** of some users in the CSV file does not match any of the user groups existing on this Sangfor device.
- **In case user already exists in local device:** This means the imported user's name conflicts with an existing user's name. Select **Go on importing and overwrite the existing user** to overwrite the existing one, or select **Skip importing the user that already exist**s not to overwrite the existing one.
- **Next:** Click it to import the users and add them into the specified user group.

If **Import Users from Digital Certificate** is selected, the contents included are as follows:



- **Select File:** Browse a certificate file with the .cer, .crt, .p12, or .pfx extension; or browse a ZIP file with certificates to import the user accounts of these certificate users.
- **Certificate Password:** If certificate owns a password, fill in the certificate password.
- **Added to Group:** This specifies the user group to which this certificate user is to be added.
- **Custom attributes:** If this option is selected, configure the following fields, namely, **Description**, **Password**, **Confirm** and **Mobile Number**. These certificate users will inherit the attributes specified here after they are imported into the specified user group on this Sangfor device; otherwise, these certificate users will inherit the attributes of its parent group (specified by **Added to Group**), with description, password and mobile number being null by default.

If **Import Group Tree From File (*.xml)** is selected, the contents included are as follows:

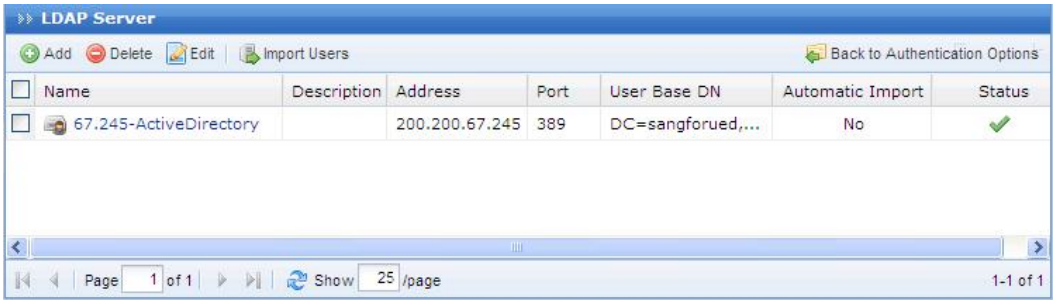


- **Select File:** Browse the XML file that you have edited. For more details of how to maintain the file, click the **Download Example File** link to download a copy and refer to the instructions in it.
- **Added to Group:** This specifies the user group to which the group tree will be added.

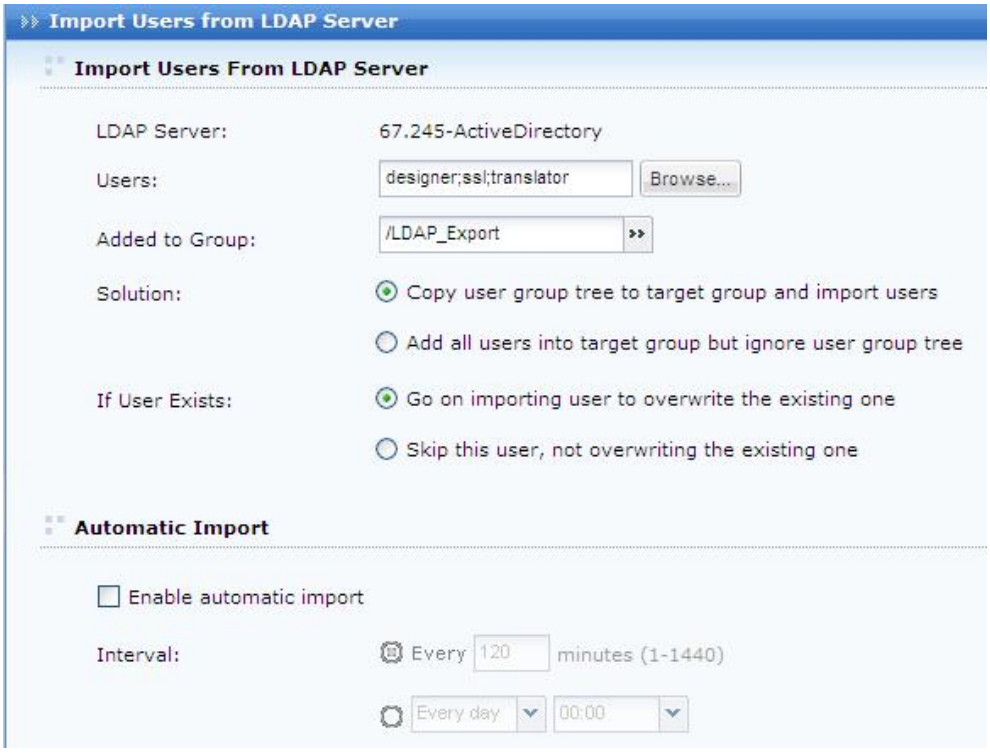
3. Configure the corresponding options on the above pages.
4. Click the **Finish** button to import the users.

Importing Users from LDAP Server

1. On the **Local Users** page, select **Import users from LDAP server**, and the **LDAP Server** page appears, as shown in the figure below:

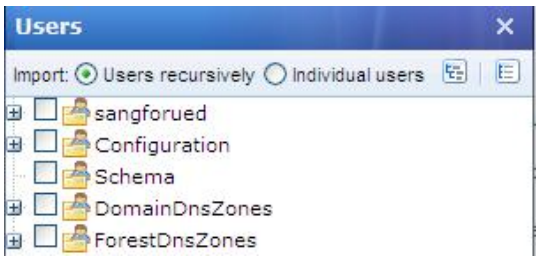


2. Click **Import Users** to enter **Import Users from LDAP Server** page, as shown below:



3. Configure the **Import Users from LDAP Server** page.

- **LDAP Server:** This shows the name of the current LDAP server.
- **Users:** Click it to enter the **Users** page and select the users that you want to export from the LDAP server and add into the list on **Local Users** page, as shown below:



You could either import user recursively or import individual users. If **Importing user recursively** is selected, and the users and groups on the LDAP server will be added into this Sangfor device as a whole, without altering its OU structure. If **Importing individual users** is selected, the users to be imported are the selected users.

- **Added To Group:** This specifies the user group to which these users will be added after they are imported into this Sangfor device.
- **Import:** Indicates the solution of importing users. One is **Copy user group tree to target group and import users** and the other is **Add all users into target group but ignore user group tree**. The former option indicates that the organizational unit (OU) on the LDAP server together with the users will be synchronized to this Sangfor device, while the latter option means that only the users will be added to the specified group.
- **If User Exists:** This means name of LDAP user is the same as that of local user (on the Sangfor device). Select **Go on importing user to overwrite the existing one** to replace the existing user with the one that are being imported from the LDAP server, or select **Skip this user, not overwriting the existing one** to skip importing the user and go on importing the others without replacing the existing user with a new one.
- **Automatic Import:** This indicates whether the users will be automatically imported into this Sangfor device and added to the specified group in due course. If **Enable automatic import** is selected, configure interval to have the users in specified group imported into the Sangfor device periodically. What worth being mentioned is that the auto-importing result could be referred to in **Maintenance** > **Logs**.



The objects imported automatically include users and groups.

4. Click the **Save and Import Now** button to save the changes and import the users. When user import completes, the result will show up at the top of page.

Moving Users to Another Group

1. On the **Local Users** page, select the desired user/group(s) and click **Move** (on the toolbar) to enter **User Groups** page, as shown below:

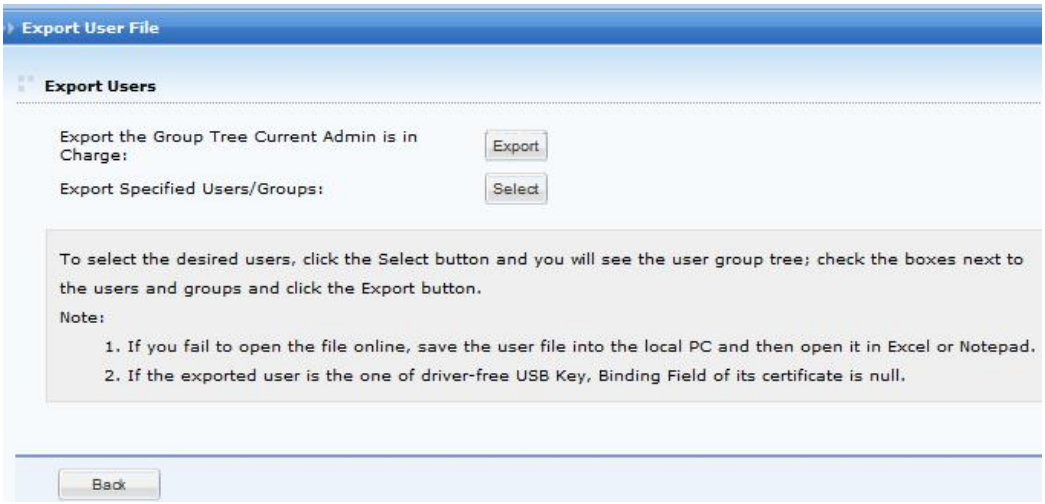


2. Select a user group to which the user/group(s) is added.

3. Click the **OK** button.

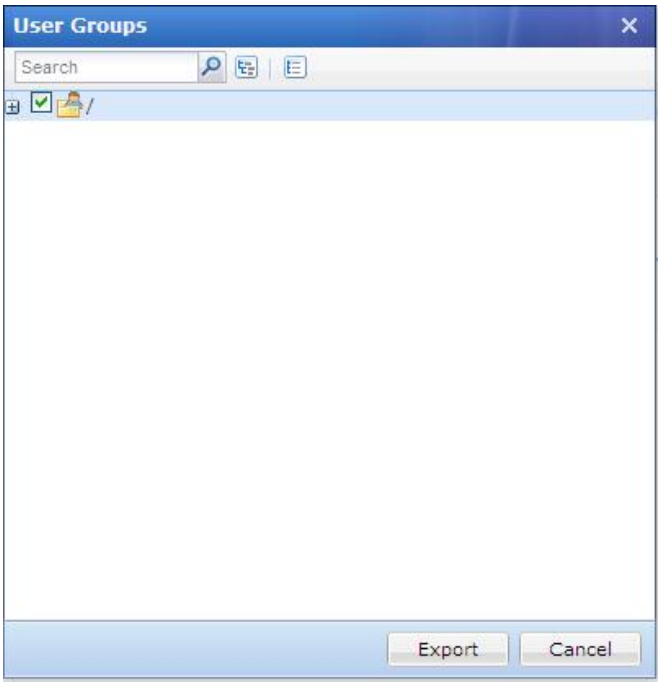
Exporting Users

1. Navigate to **SSL VPN** > **Users** > **Local Users** page and click **More** > **Export** to enter the **Export User File** page, as shown in the figure below:



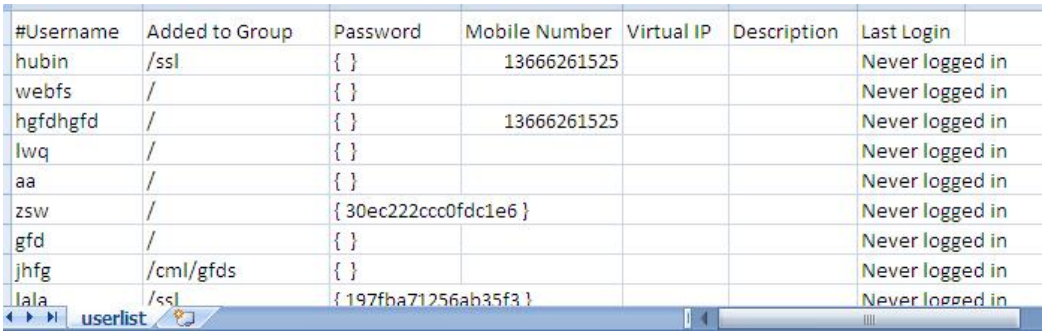
2. Select the objects that you want to export.

   Two solutions are available, **Export the Group Tree Current Admin is in Charge** and **Export Specified Users/Groups.** If the former is selected, the organization structure in the current administrator's administrative realms will be exported. If the latter is selected, users on specified groups will be exported, as shown below:



3. Select the desired user group and then click the **Export** button. The selected user will be written into a CSV file and saved on the local computer.

   The exported user information includes username, group path, password (encrypted by an algorithm developed by SANGFOR), mobile number, virtual IP address, description and the time user logged in last time, as shown below:

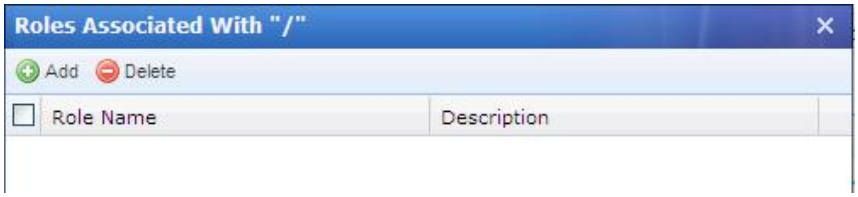


#Username	Added to Group	Password	Mobile Number	Virtual IP	Description	Last Login
hubin	/ssl	{ }	13666261525			Never logged in
webfs	/	{ }				Never logged in
hgfdhgfd	/	{ }	13666261525			Never logged in
lwq	/	{ }				Never logged in
aa	/	{ }				Never logged in
zsw	/	{ 30ec222ccc0fdc1e6 }				Never logged in
gfd	/	{ }				Never logged in
jhfg	/cml/gfds	{ }				Never logged in
lala	/ssl	{ 197fba71256ab35f3 }				Never logged in

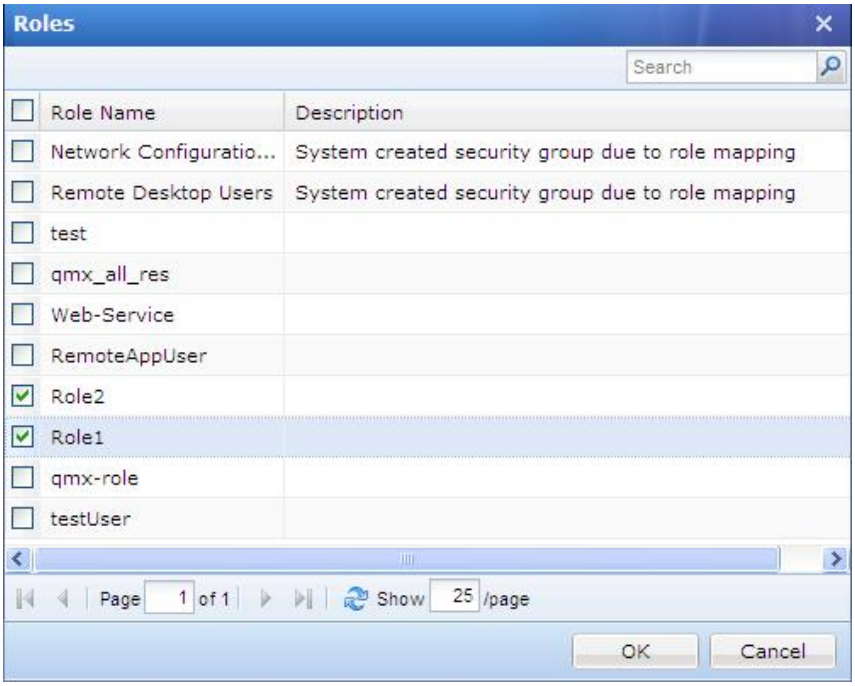
userlist

Associating Roles with User

1. Navigate to **SSL VPN** > **Users** > **Local Users** page and click **More** > **Associate with role** to enter the **Roles Associated With xxx** page, as shown below:



2. Click **Add** to enter the **Roles** page, as shown in the figure below.



The roles on **Roles** page are all the roles predefined under **SSL VPN** > **Roles** > **Role Management**.

3. Select the checkboxes next to the roles that you want to associate with the selected user or group.
4. Click the **OK** button and then the **Submit** button to save the settings.

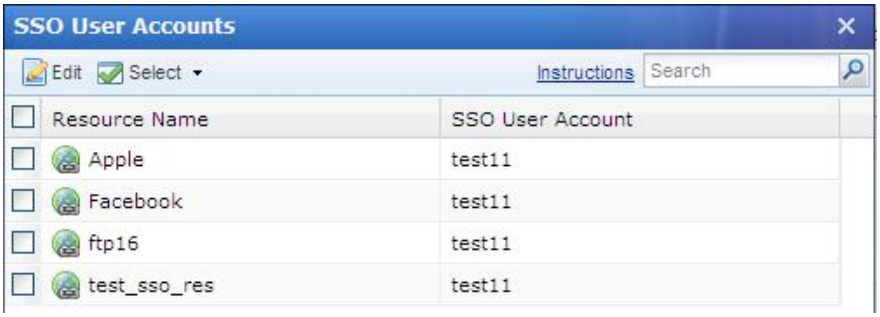
Configuring SSO User Account

SSO feature facilitates user to perform one-stop access to the resource that has enabled SSO. When the connecting user clicks on the resource name on the **Resource** page, he or she will directly visit that resource with the Sangfor device helping him or her submit the required credentials (username and password of the user account).

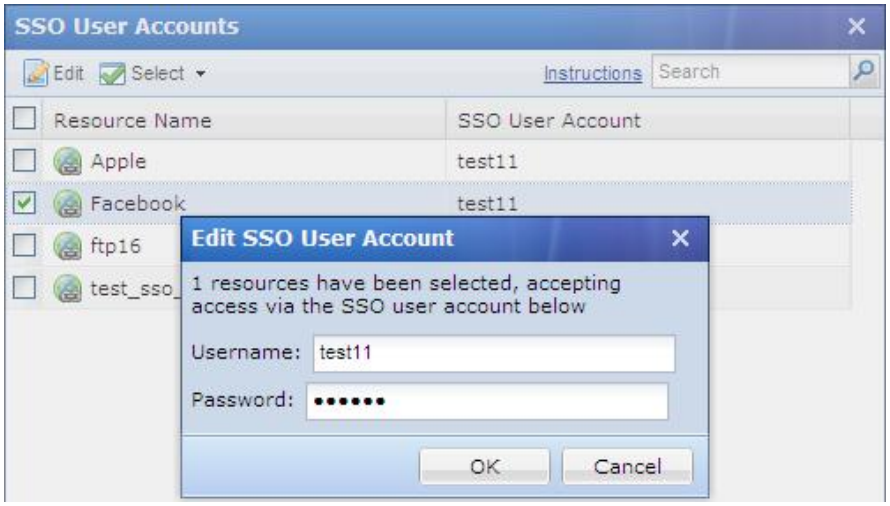
SSO user account should be configured if SSL VPN user account has associated with any resource that allows SSO.

To configure SSO user account for a user, perform the following steps:

1. Navigate to **SSL VPN** > **Users** > **Local Users**, select a desired user and click **More** > **Configure SSO user account** to enter the **SSO User Accounts** page, as shown below:



2. Select the desired resource(s) to edit the SSO user account, as shown below:



3. Enter the username and password of the SSO user account into the corresponding fields, and

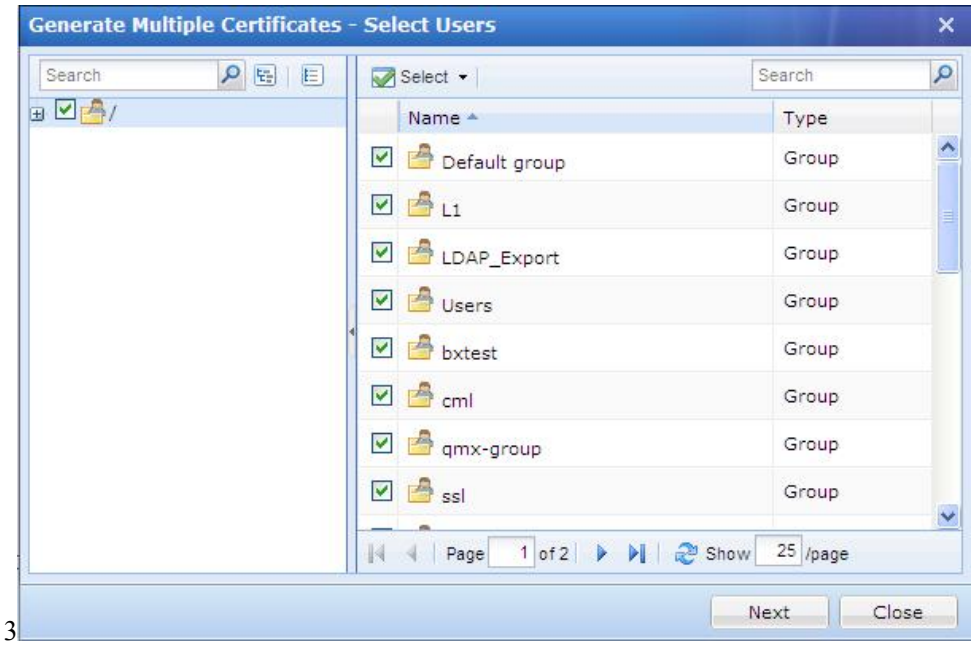
click the **OK** button. The newly created SSO user account is configured.

4. Click the **Close** button and the **Apply** button on the next page to save and apply the changes.

Generating Multiple Certificates for Users

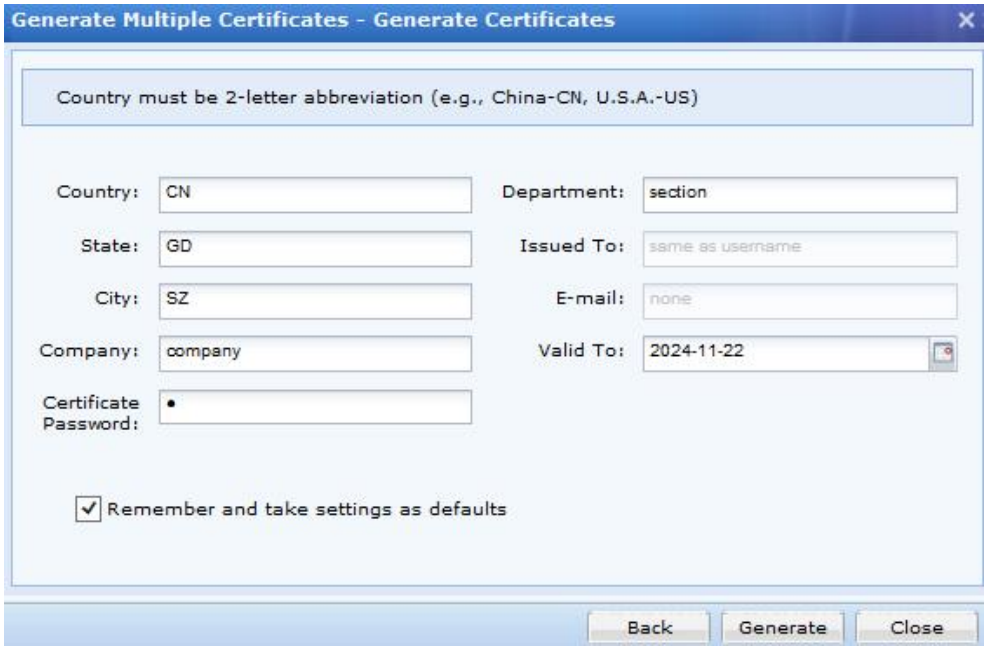
To save time and trouble, generating certificates for a bunch of users is a good choice.

1. Navigate to **SSL VPN** > **Users** > **Local Users** page and click **More** > **Generate multiple certificates**, as shown below:



3

2. Select the desired users and click the **Next** button to create and generate multiple certificates, as shown below:



Configure the fields on the page. The following are the contents:

- Configure the required fields, such as **Country**, **State**, **City**, **Company**, **Department**, **Valid To** and **Certificate Password**. **E-Mail** is not configurable. **Issued To** shows the username and is not configurable.
- **Remember and take settings as defaults:** If it is selected, the settings in all the fields will be remembered (exclusive of **Certificate Password** and **Issued To**), so that they could be reused when generating certificate for a bunch of similar users next time.

3. Click **Generate** to generate certificates for the specified users one by one, as shown below:

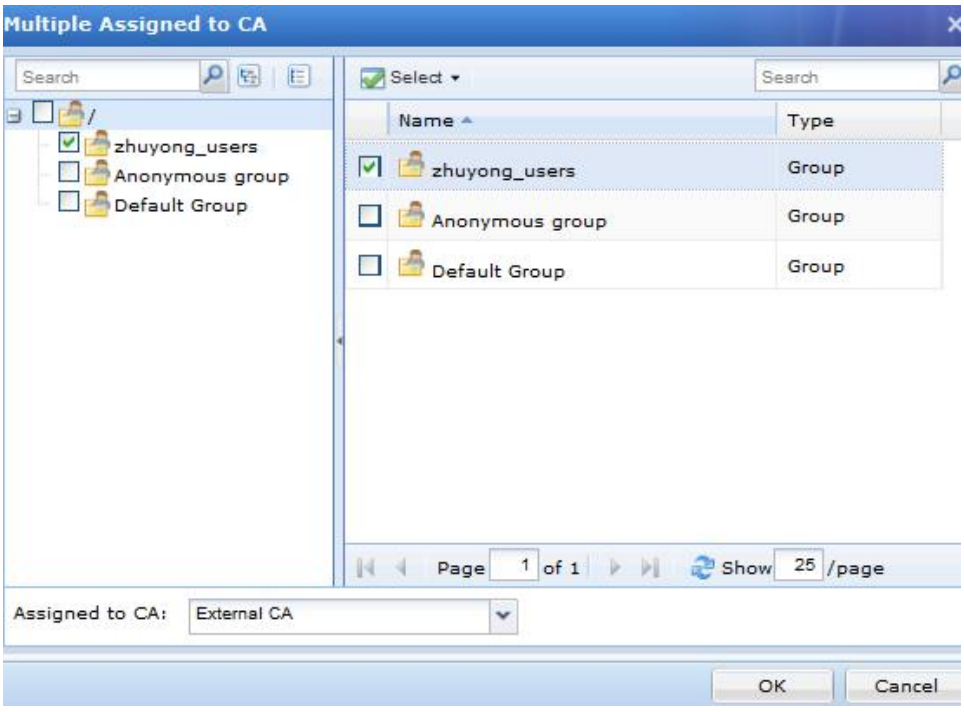


4. To save the certificate to the computer, click the **Download Certificate** button.

Configuring Multiple Users Assigned To CA

If you want to assign multiple users to one third-party CA, perform the following steps:

1. Navigate to **SSL VPN** > **Users** > **Local Users** page, and click **More** > **Multiple Assigned To CA**, as shown below:



2. Select the desired users and/or group, then specify the CA to which you want to assign these users.
3. Click **OK** to save the settings.

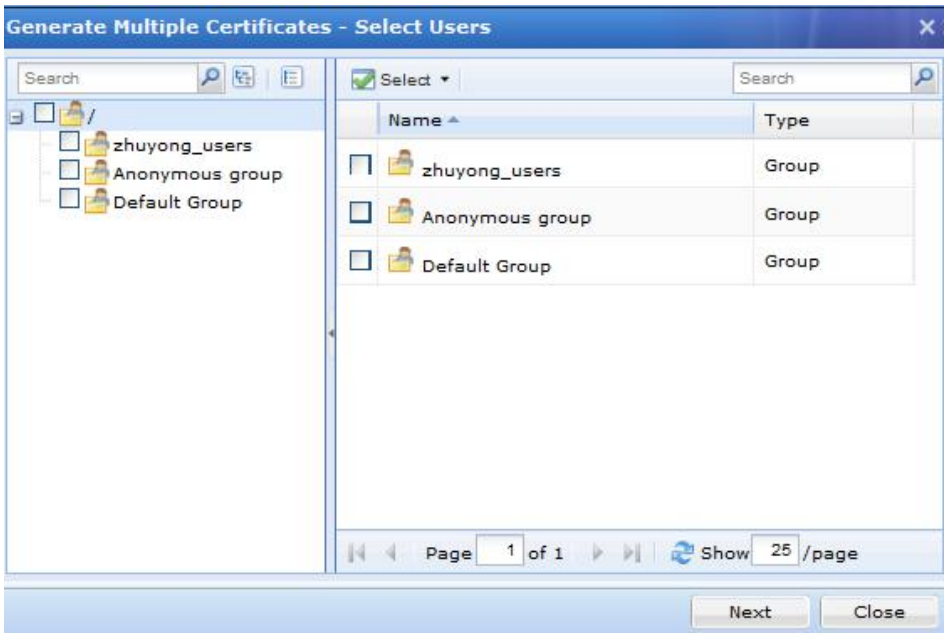
Creating Multiple USB Keys for Users

To save time and trouble, creating USB keys for a bunch of users is a good choice.

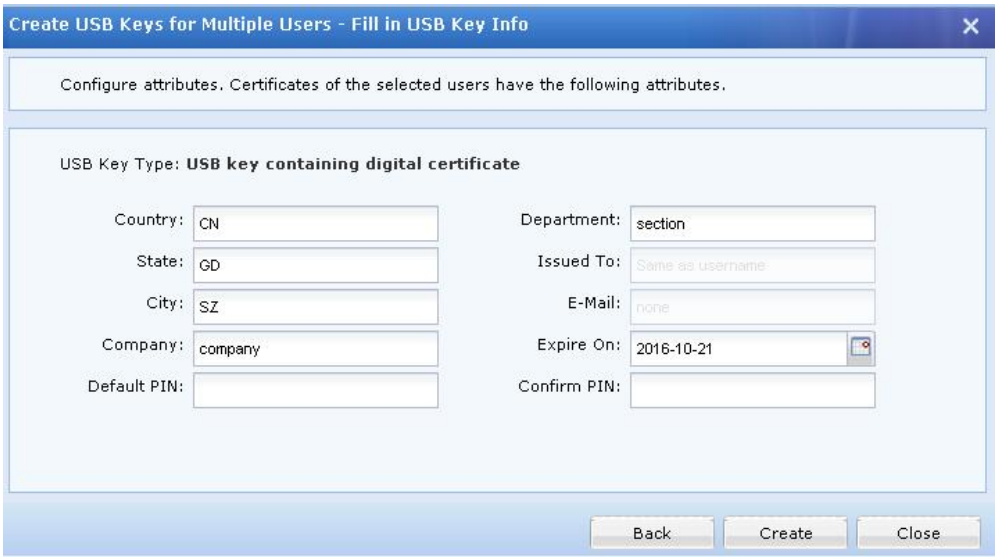
1. Navigate to **SSL VPN** > **Users** > **Local Users** page and click **More** > **Generate multiple USB keys** to enter the following page:



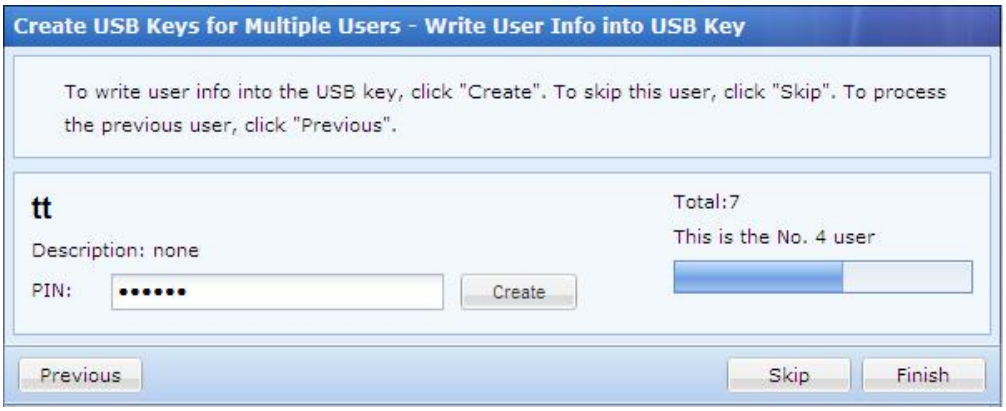
2. Select USB key type (take **USB key containing digital certificate** for example) and click the **Next** button, the next step is as shown below:



3. Select the desired users and/or groups and click the **Next** button to proceed, as shown below:



4. Configure the required fields. Click the **Create** button and the process is as shown below:



5. Every time when the process stops here, insert a physical USB key into the USB port of the computer, enter PIN and click the **Create** button to write information of the current user into the USB key.

   To give up creating USB key for a user, click the **Skip** button to skip that user.

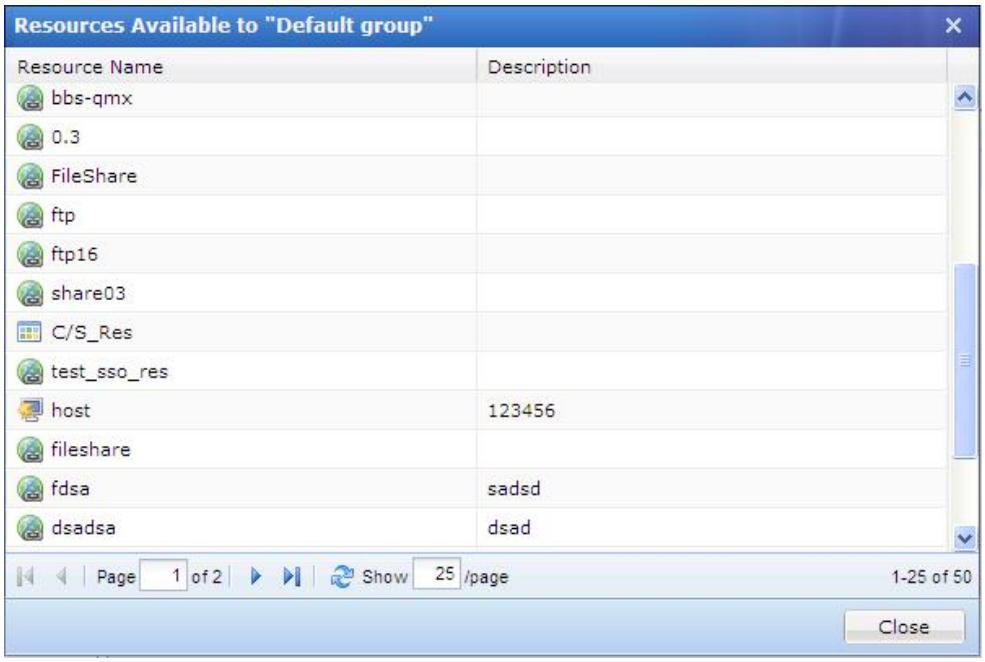
   To rewrite information into the USB key of the previous user, click the **Previous** button.

   To stop writing user information into and generating USB key, click the **Finish** button.

6. After creating USB key, give the USB key to the corresponding user and the user could use the USB key to log in to SSL VPN.

Viewing Associated Resources of User

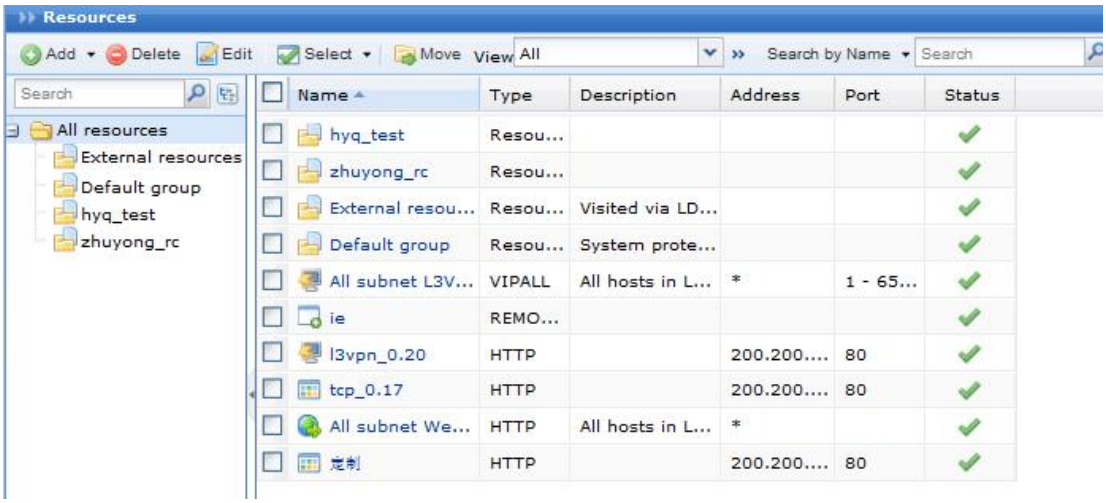
To see what resources are available to certain user or group, select that user or group and click **Associated Resource**. The resources available to the selected user or group are as shown below:



Resources

The resources we are talking about in this user manual are the resources that can be accessed by specified users over SSL VPN.

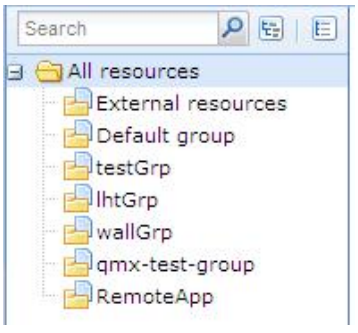
Resource type falls into **Web** application, **TCP** application, **L3VPN** and **Remote Application**. Navigate to **SSL VPN** > **Resources** page appears, as shown below:



A resource group could contain a number of resources entries. Similar to user management, resources could be grouped according to categories and associated user or group, etc. This kind of management is welcomed by majority of administrators because it makes resources more distinguishable.

Note: The resource management module only supports IPv4 addresses and does not support IPv6 addresses.

Navigate to **SSL VPN** > **Resources** and click on the resource group, and the resources included in the group are displayed on the right pane. The resource group tree is as shown in the figure on the right.



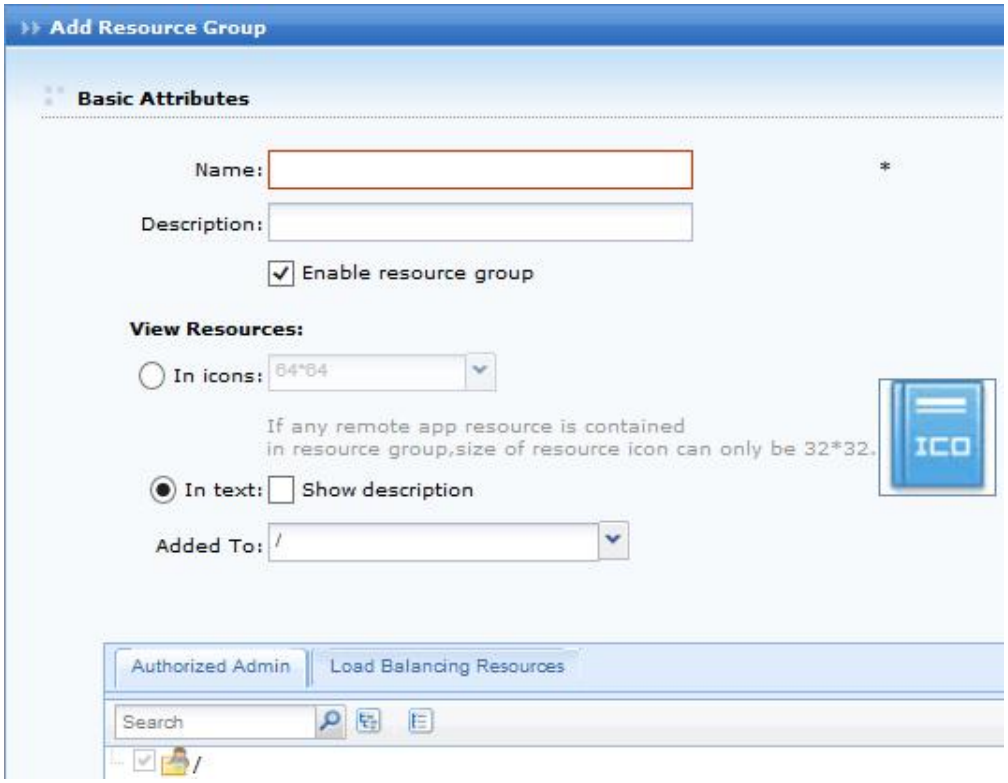
External resources is a group protected by system and cannot be deleted; however, its attributes

could be modified. All the resources contained in this resource group are the resources associated with LDAP users.

Default group is also a group protected by system and cannot be deleted, but its attributes could be modified.

Adding/Editing Resource Group

1. Click **Add** > **Resource Group** to enter **Edit Resource Group**, as shown in the figure below:



2. Configure **Basic Attributes** of the resource group. The following are the basic attributes:

   - **Name, Description:** Indicates the name and description of the resource group respectively. This name will be seen on **Resource** page after user logs in to the SSL VPN successfully.
   - **View resource:** Indicates the way resources are displayed on **Resource** page, in icon or in text. If **In Icons** is selected, define the icon size, **48*48**, **64*64** or **128*128**, so that the resources will be displayed in icon as wanted. If **In Text** is selected, you may select **Show description** of the resource. To manage icons, refer to the Uploading Icon to Device section in Chapter 3.
   - **Added To:** Indicates the resource group to which this group is added. This also means that the administrative privilege over this resource group is moved from the creator (who created this resource group) to its high-level administrator, while the creator has no right to edit this resource group and the resources in it.

It is normal that the creator is unable to see the resource group and its resources on the administrator console, if the administrative privilege over a resource has been moved from the creator to its high-level administrator.

3. Specify **Authorized Admin** who will have the right to manage this resource group and the right to grant other administrators the right to manage this resource group.

4. Configure **Load Balancing Resources** feature when a resource group has multiple resources of the same type, but with different IP addresses. Sangfor device will distribute the resource, elected by corresponding weight, to client. The resources contained in **Load Balancing Resources** tab are attached with weight that ranges from 1 to 9 (by default, it is 5), as shown below:

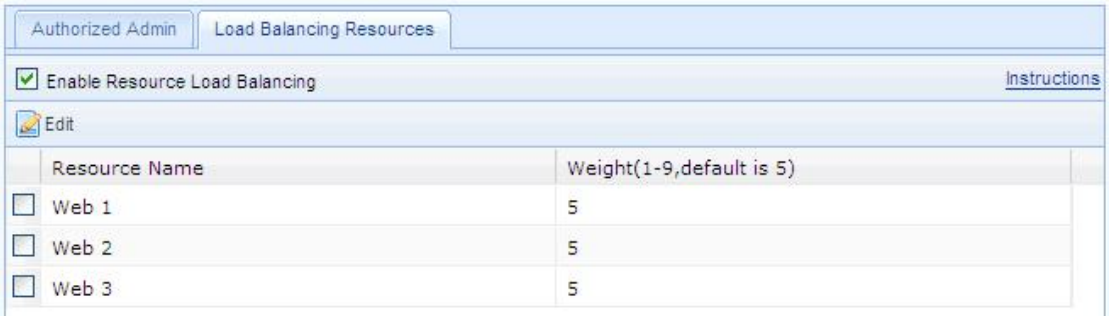


- A resource could be included in only one resource group.
- Maximum 100 resource groups are supported.

5. Click the **Save** button to save the settings.

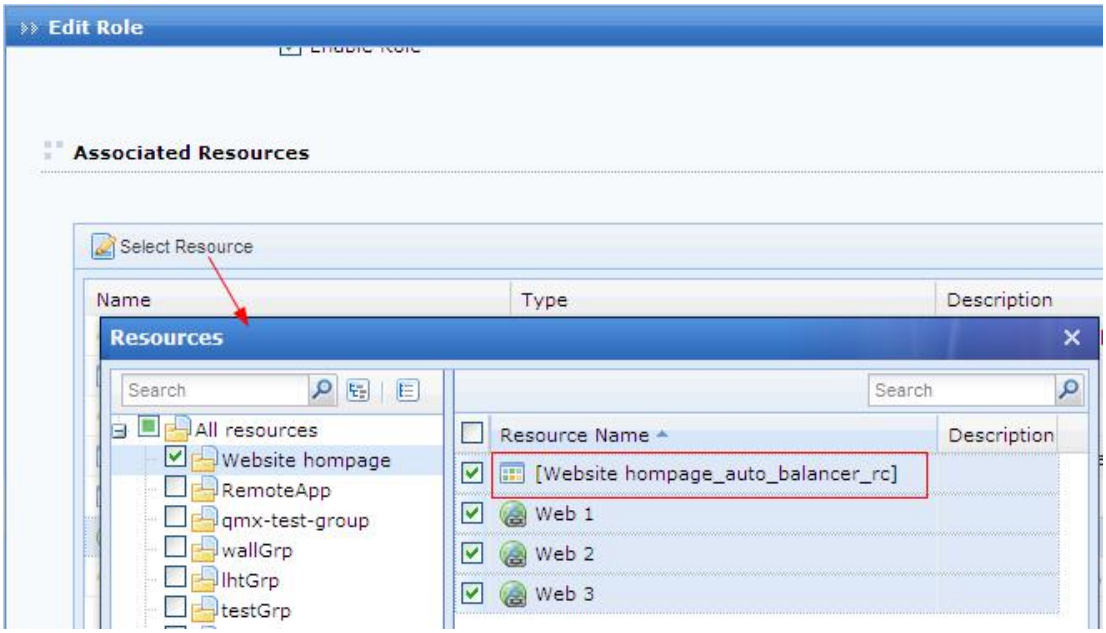
Background Knowledge: Load-Balanced Resource Access

Assume that three resources named **Web1**, **Web2** and **Web3** are created based on three servers providing services, and are added into a new group **Website homepage**. The three resources have the same settings but different IP addresses; weights for load balancing are **5**, as shown below:



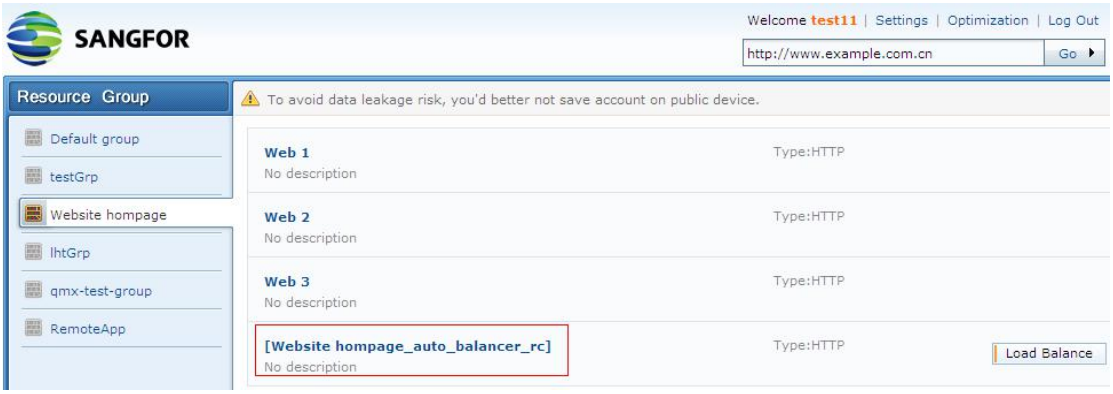
Working Principle

The background actually ensures that a load-balancing resource has been generated already. Administrator can see that resource while editing a role to associate user with resources (under **SSL VPN** > **Roles > Edit Role)**, as shown in the figure below:



If the associated resource **Website hompage_auto_balancer_rc** of the role is assigned to users or groups, the first five connecting users will access the resource launched by **Web 1**, the second five users access the resource launched by **Web 2** and the third five connecting users access the resource launched by **Web 3**. Through this way, load of the three servers is kept balanced (to associate resources with user or group, refer to the Adding Role section in Chapter 4).

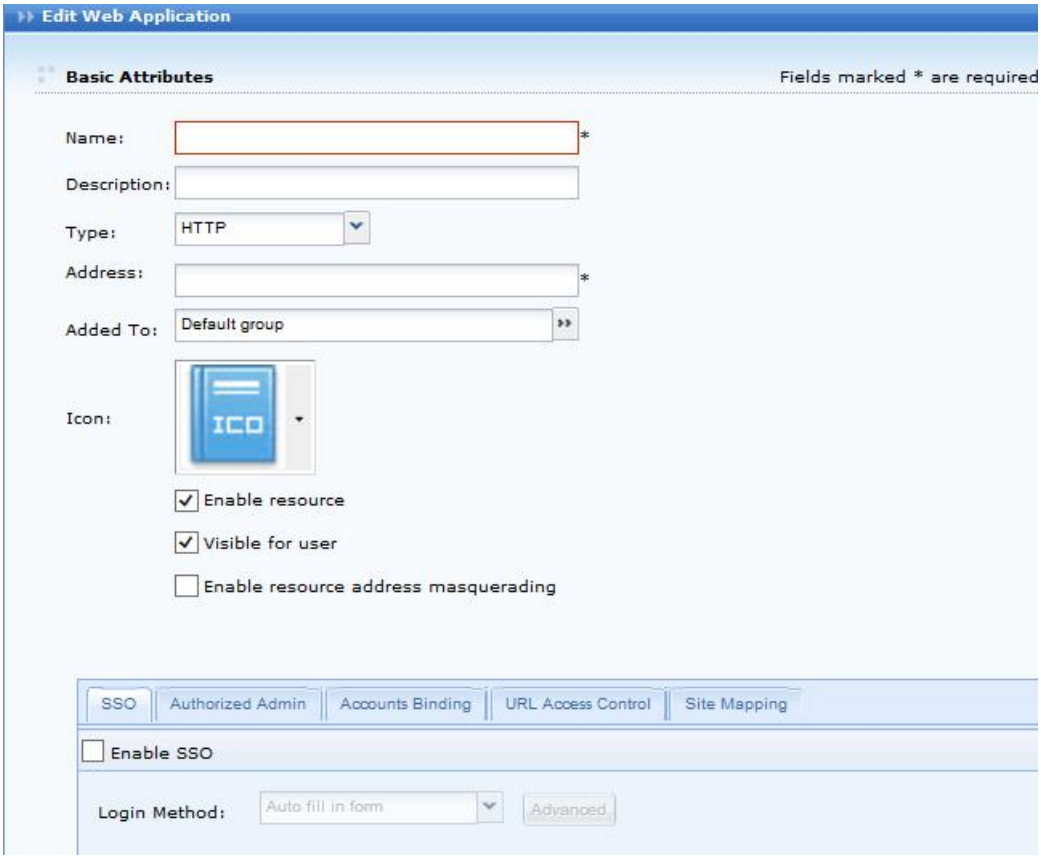
The load balancing resources available to the designated user will show as follows after the user logs in to the SSL VPN:



To access the same resource provided by a different server, connecting user needs only to click the **Load Balance** button.

Adding/Editing Web Application

1. Navigate to **SSL VPN** > **Resources** page and click **Add** > **Web app** to enter **Edit Web Application** page, as shown below:



2. Configure **Basic Attributes** of the Web application. The following are the basic attributes:

   - **Name, Description:** Indicates the name and description of the Web resource. This name may be seen on the **Resource** page after user logs in to the SSL VPN successfully.

- **Type:** Options are **HTTP**, **HTTPS**, **MAIL**, **FileShare** and **FTP**.
- **Address:** Indicates the address of the resource. Enter the IP address or domain name of the Web server that is to be visited by user while this resource is requested.

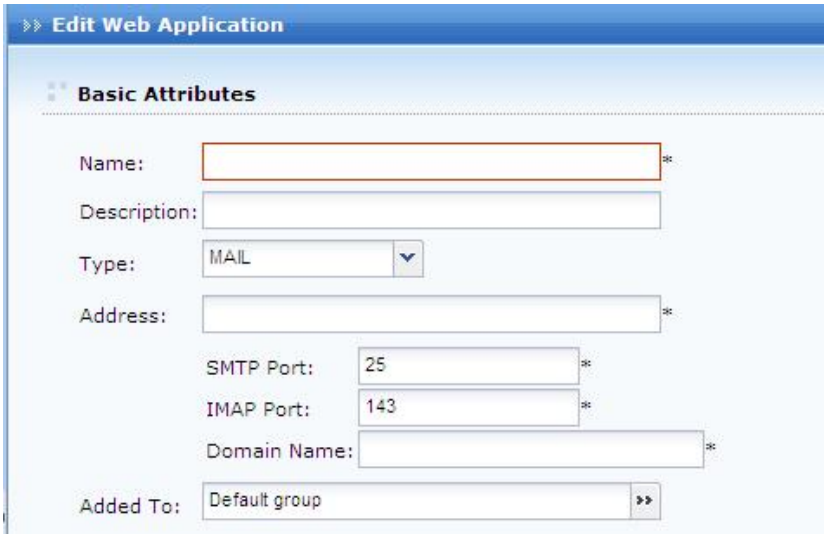
If the selected Web application type is **HTTP** or **HTTPS**, the fields are as shown below:





- Address field is required. The address must begin with **http://** or **https://**, for example, *http://200.200.0.66* and *https://200.200.0.66*.
- If resource address is domain name or hostname, add a host entry to map the domain name/hostname to the actual IP address (in **System** > **Network** > **Hosts**, refer to the Configuring Host Mapping Rule (HOSTS) section in Chapter 3), or configure the DNS server of the Sangfor device and ensure it can resolve the local domain names (in **System** > **Network** > **Deployment**).

If the selected Web application type is **MAIL**, enter the IP address of the SMTP server in the **Address** field and configure **SMTP Port**, **IMAP Port** (defaults are recommended) and **Domain Name** (of the mailbox) the fields, as shown below:



To enable users to use this type of email receiving and sending, the mail server must support protocol **IMAP**.

If the selected Web application type is **FTP**, enter IP address or domain name of the FTP server into the **Address** field, and configure **FTP Port** of the FTP server that users are going to connect to (default is recommended), as shown below:



After entering domain name into the **Address** field and completing the configuration, go to **System** > **Network** > **Hosts** and add a Host entry to map the domain name or host name to the IP address of the FTP server.

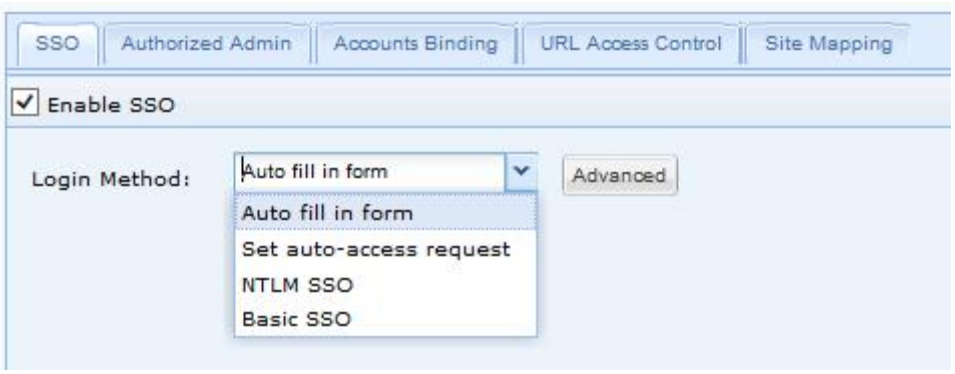
- **Added To:** Indicates the resource group to which this resource is added. By default, the selected resource group is **Default group** (to configure resource group, refer to the Adding/Editing Resource Group section in Chapter 4).
- **Icon:** Indicates the icon for this resource, which could be seen on the **Resource** page if this resource is added to a group that has its resources shown in icons. Select an icon, or click on the icon to upload a new one.

  To browse an image and upload it from the local PC to the device, click **Upload** (for detailed guide, refer to the Uploading Icon to Device section in Chapter 3).
- **Visible for user:** To have connecting users see this resource on the **Resource** page, select this option. Invisibility here only means that the resource will not be seen on the **Resource** page; in fact, it is still accessible to the user.
- **Enable resource address masquerading:** To conceal the true IP address of the resource,

select this option.

3. Configure **SSO** tab.

To enable user to access corporate resources over SSL VPN using SSO, select **Enable SSO** option and configure the **SSO** page (under **System** > **SSL VPN Options** > **General**. For more details, refer to the Configuring SSO Options section in Chapter 3). Enable SSO on SSO tab and specify login method, as shown below:



4. Configure **Authorized Admin** tab.

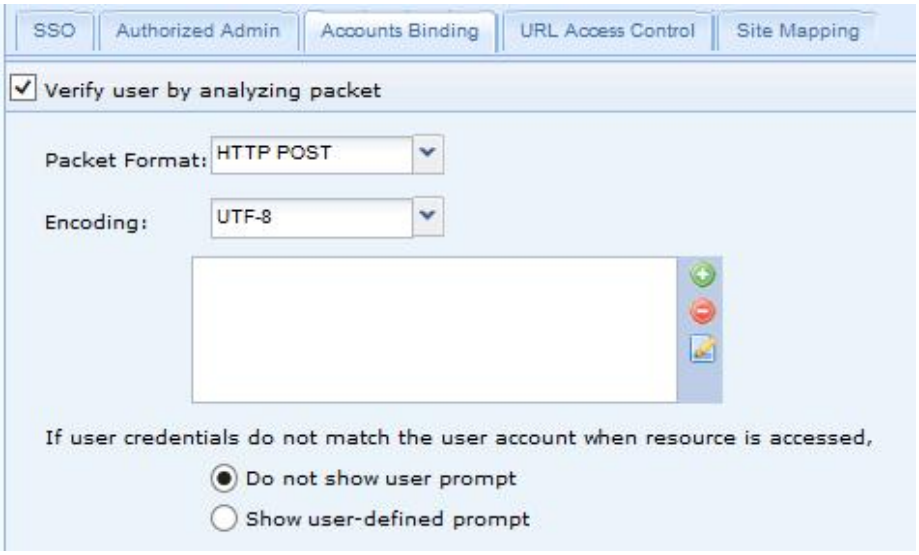
Specify the administrators who will have the right to manage this resource and the right to grant other administrator the privilege to manage this resource.





- The authorized administrators cannot edit the resource. They only have the right to assign this resource to users (in other words, to associate resources with the role under **SSL VPN** > **Roles** > **Edit Role**) and to grant other administrators (in its permitted realm) the privilege to manage this resource, rather than the privilege of editing the resource.
- Please it keep in mind that the privilege of editing a resource always belongs to the creator who has created this resource as well as the administrator with higher privilege. The authorized administrators cannot see those resources in **Resources** page, but can see and associate them with users on the **Add Role** or **Edit Role** page.

5. Configure **Accounts Binding** tab, as shown in the figure below.

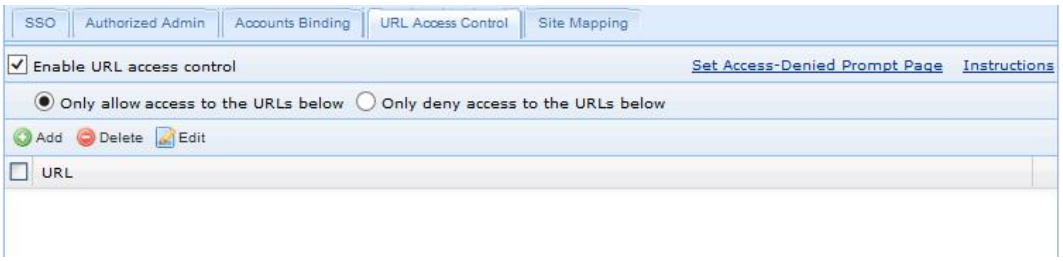


If **Verify user by analyzing packet** is selected, the SSL VPN account will bind to the account for resource access, in the way that packet is obtained as specified according to **Packet Format** and the others settings. For end user, he or she needs to use the corresponding SSL VPN account and resource access account to access the resource over SSL VPN, other user accounts being unable to match the credential.

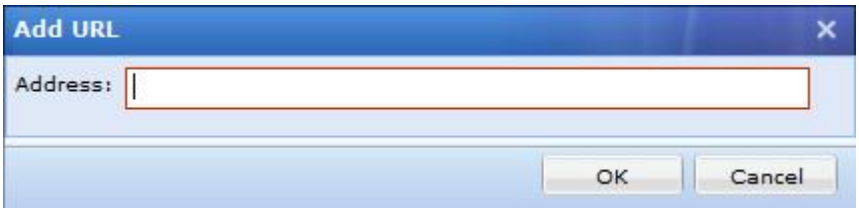
Web application, TCP application and L3VPN support accounts binding.

Applying **Verify user by analyzing packet** does not need SSO to be enabled.

6. Configure **URL Access Control** tab. This achieves the control over users' access to certain directory of a server, user being able or unable to access the specified directory.

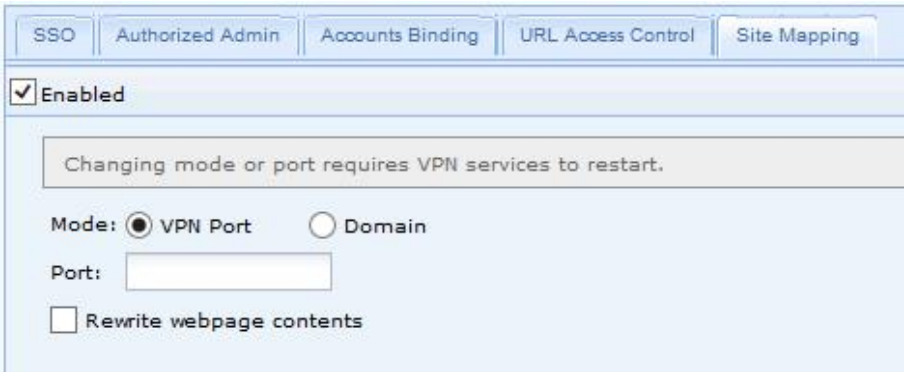


Select **Only allow access to the URLs below** to allow user to access the specified ULR in the list, or select **Only deny access to the URLs below** to forbid user from accessing the specified ULR in the list. To add a new URL, click **Add** to enter the **Add URL** page, as shown below:



Please note that the URL access control feature is only available while Web application type is **HTTP**, **HTTPS** or **FileShare**. The other two types of Web application (**MAIL** and **FTP**) do not support this feature.

7. Configure **Site Mapping** tab.



Select **Enabled** to enable site mapping feature. Administrator can specify a VPN port or domain name mapping to this Web resource. VPN User accesses this Web resource via the specified VPN port or domain name.

If **VPN Port** is selected, you need to enter VPN port number in **Port** field, which cannot conflict with other ports in use; if **Domain** is selected, the domain name is required, and it should be a public URL of SSL VPN. To ensure the domain name can be resolved on client PC, add a Host entry on client PC. User cannot connect to SSL VPN though the specified domain name if **Domain** is selected.

To rewrite webpage on client, select **Rewrite webpage contents**. Checking this option is recommended.

- Site mapping and resource address masquerading features cannot be enabled together.
- Site mapping feature is only available while Web application type is HTTP, HTTPS. The other types of Web application (FileShare, MAIL and FTP) do not support this feature.
- For the resource enabling site mapping feature, it can be accessed only through clicking resource link. It is not accessible through typing resource address into the **URL** field.

8. Click the **Save** button and the **Apply** button to save and apply the settings.

After the user logs in to the SSL VPN, he or she will see the available resources on the **Resource** page, as shown below:



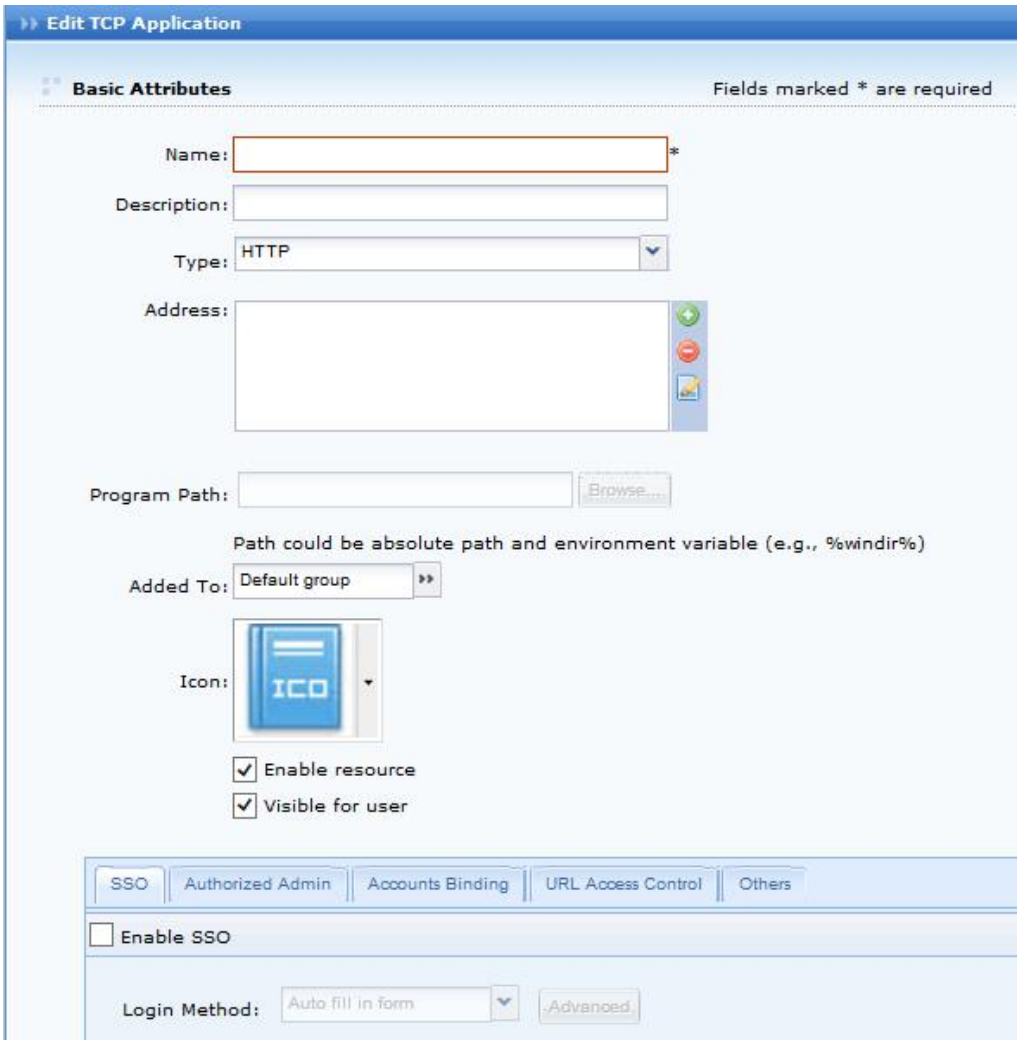
To access an available Web resource, the user needs only to click the resource link, or enter resource address into the **URL** field and click the **Go** button.

Web resources could be accessed via all types of browsers including non-IE browsers.

Adding/Editing TCP Application

TCP application is a type of resource that allows end users to use TCP-based applicationon their local computer to access corporate resources and servers over SSL VPN.

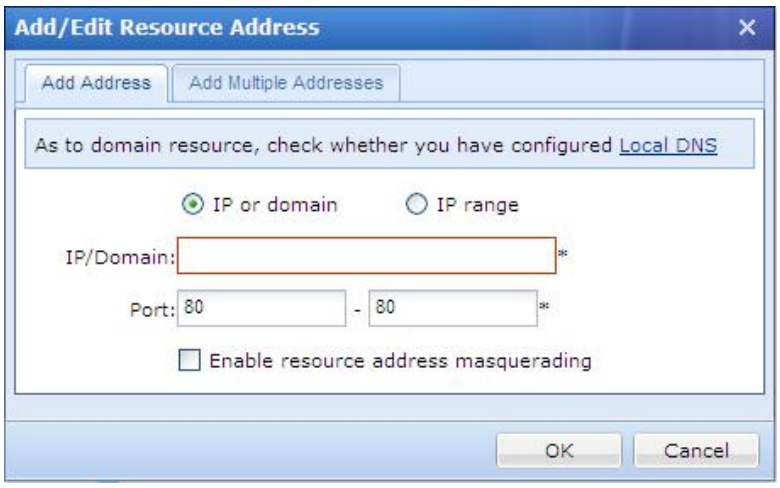
1. Navigate to **SSL VPN** > **Resources** and click **Add** > **TCP app** to enter the **Edit TCP Application** page, as shown in the figure below:

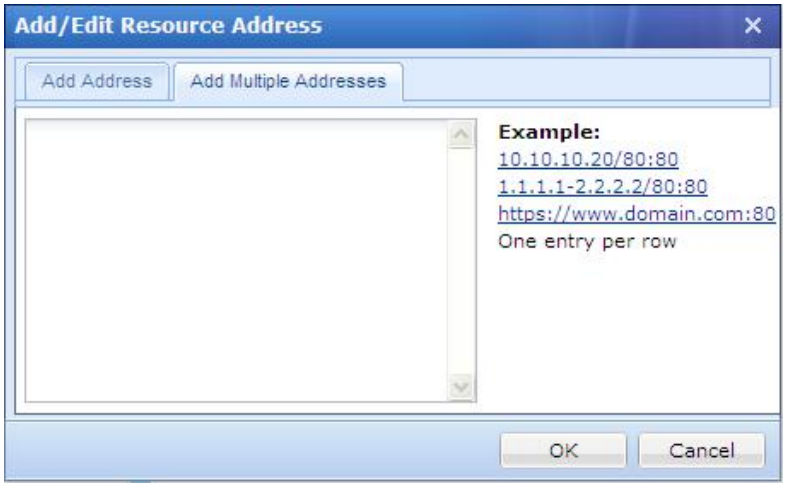


2. Configure **Basic Attributes** of the TCP application. The following are the basic attributes:

   - **Name, Description:** Indicates the name and description of the TCP resource. This name may be seen on the **Resource** page after user logs in to the SSL VPN.
   - **Type:** Indicates the type of the TCP application. Some common types are built in the Sangfor device.

     This selection determines the port number entered in the **Port** field automatically. If the TCP application is not any of the built-in types, select **Other** and configure the port manually.
   - **Address:** Indicates the address of the TCP resource. To add one entry of address (IP address, domain name or IP range), click the **Add Address** tab. To add multiple entries of addresses, click the **Add Multiple Addresses** tab, as shown in the figures below:







- **Port** indicates the port used by this TCP application to provide services. For built-in types of TCP applications, this port is predefined. For **Other** type of TCP application, enter the corresponding port number.
- If resource address is domain name, navigate to **System** > **SSL VPN Options** > **General > Local DNS** to configure local DNS server (for detailed guide, refer to the Configuring Local DNS Server section in Chapter 3).

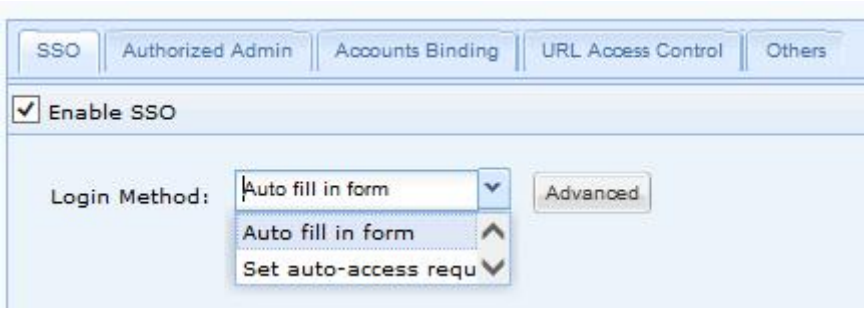
- **Program Path:** Indicates path of the client software program that may be used by C/S (client/server) application.
- **Added To:** Indicates the resource group to which this resource is added. By default, the selected resource group is **Default group** (to configure resource group, refer to the Adding/Editing Resource Group section in Chapter 4).
- **Visible for user:** To have connecting users see this resource on the **Resource** page, select this option. Invisibility here only means that the resource is not seen on the

Resource page, in fact, it is still accessible to the user.

- **Enable resource address masquerading:** To conceal the true IP address of the resource, select this option.

3. Configure **SSO** tab.

   To enable connecting users to use SSO feature to access corporate resources over SSL VPN, select **Enable SSO** option and configure the **SSO** page (under **System** > **SSL VPN Options** > **General > SSO**. For more details, refer to the Configuring SSO Options section in Chapter 3).



4. Configure **Authorized Admin** tab.

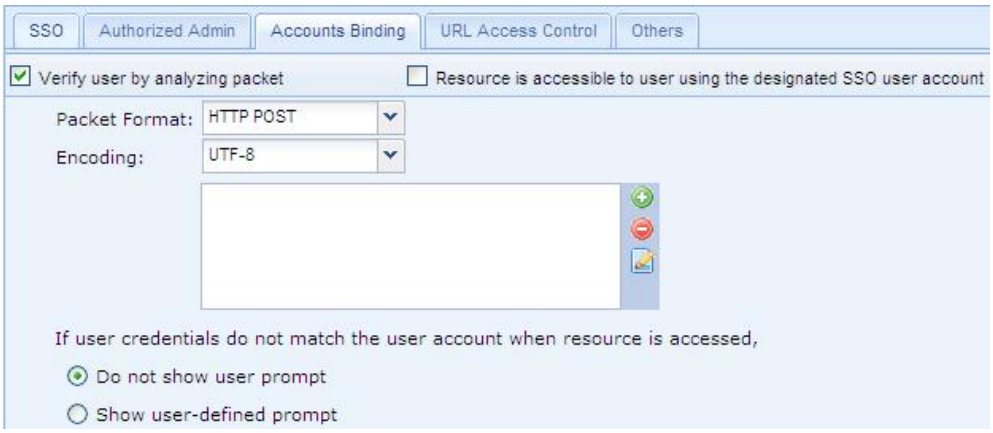
   Specify the administrators who will have the right to manage this resource and the right to grant other administrator the privilege to manage this resource.





- The authorized administrators cannot edit the resource. They only have the right to assign this resource to users (in other words, the right to associate resources with the role under **SSL VPN** > **Roles** > **Edit Role**) and to grant other administrators (in its permitted realm) the privilege to manage this resource, rather than the privilege of editing resource.
- Please it keep in mind that the privilege of editing a resource always belongs to the creator who has created this resource as well as the administrator with higher privilege. The authorized administrators cannot see those resources in the **Resources** page, but can see and associate them with users on the **Add Role** or **Edit Role** page.

5. Configure **Accounts Binding** tab, as shown in the figure below.



If **Verify user by analyzing packet** is selected, the SSL VPN account will bind to the account for resource access, in the way that packet is obtained as specified according to **Packet Format** and the others settings.

If **Resource is accessible to user using the designated SSO user account** is selected, end user has to use the corresponding SSL VPN account and designated SSO user account to access this TCP resource over SSL VPN, other user accounts being unable to match the credential.

Web application, TCP application and L3VPN support accounts binding.



- To enable end users to single sign in to a resource, enable SSO for that resource (under **SSL VPN** > **Resources** > **Edit TCP Application** > **SSO** tab) and bind the SSL VPN account to the SSO user account (to configure SSO user account, refer to the Configuring SSO User Account section in Chapter 4).
- Applying **Verify user by analyzing packet** does not required SSO to be enabled.

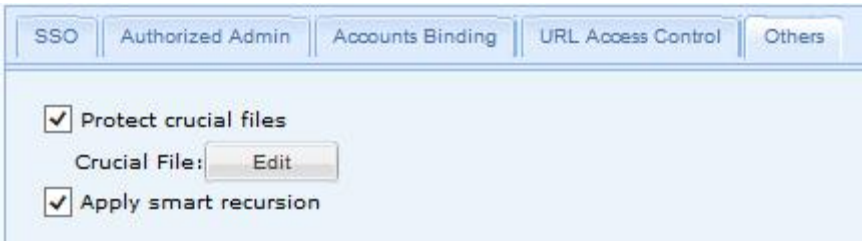
6. Configure **URL Access Control** tab.

   This achieves the control over users' access to certain directory of a server, user being able or unable to access the specified directory.



Please note that URL access control feature is only available while the selected TCP application type is **HTTP**. The other types of TCP applications do not support this feature.

7. Configure **Others** tab. This tab covers two options, **Protect crucial files** and **Apply smart recursion**, as shown in the figure below:



- **Apply smart recursion:** Select this option to apply smart recursion to this resource. Before doing so, go to **System** > **SSL VPN** > **General** > **Resource Options** > **TCP App** to enable and configure smart recursion. For more details, please refer to the Background Knowledge: What is Smart Recursion? in Chapter 3 and Scenario 4: Configuring and Applying Smart Recursion in Chapter 3.
- **Protect crucial file:** This feature is intended to lock some crucial files that might be invoked by the process while user is accessing the Internet by using **Socket** connection, so that these crucial files will not be altered during SSL VPN access. If any of these protected processes and crucial files is altered, the corresponding resource would not be accessible to the user.

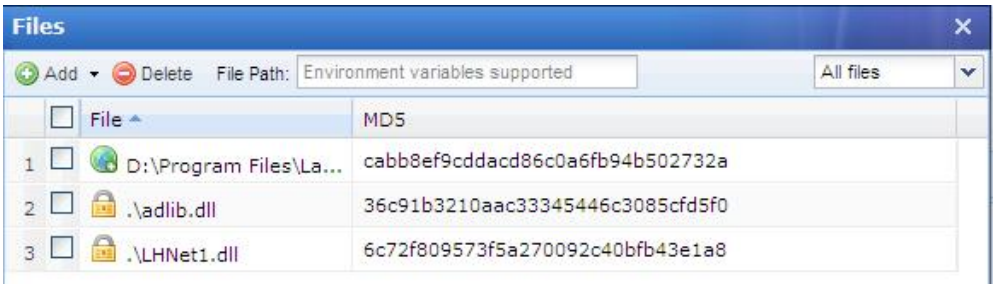
  To add crucial files, perform the following steps:

  a. Click the **Edit** button next to **Crucial File** to enter the **Files** page, as shown below:



  b. Click **Add** > **Process related file** to select the process (file extension is .exe).

  c. The selected file and all the involved DLL files are added to the **Files** page, with the information of file directory and MD5, as shown in the figure below:



  d. To view a specific type of file, dll, exe or pdb, specify the file type in the textbox at the upper right of the page. By default, all files are displayed.

  e. To remove an entry, select the checkbox next to the entry and click **Delete**.

  f. Click the **OK** button to save the settings.



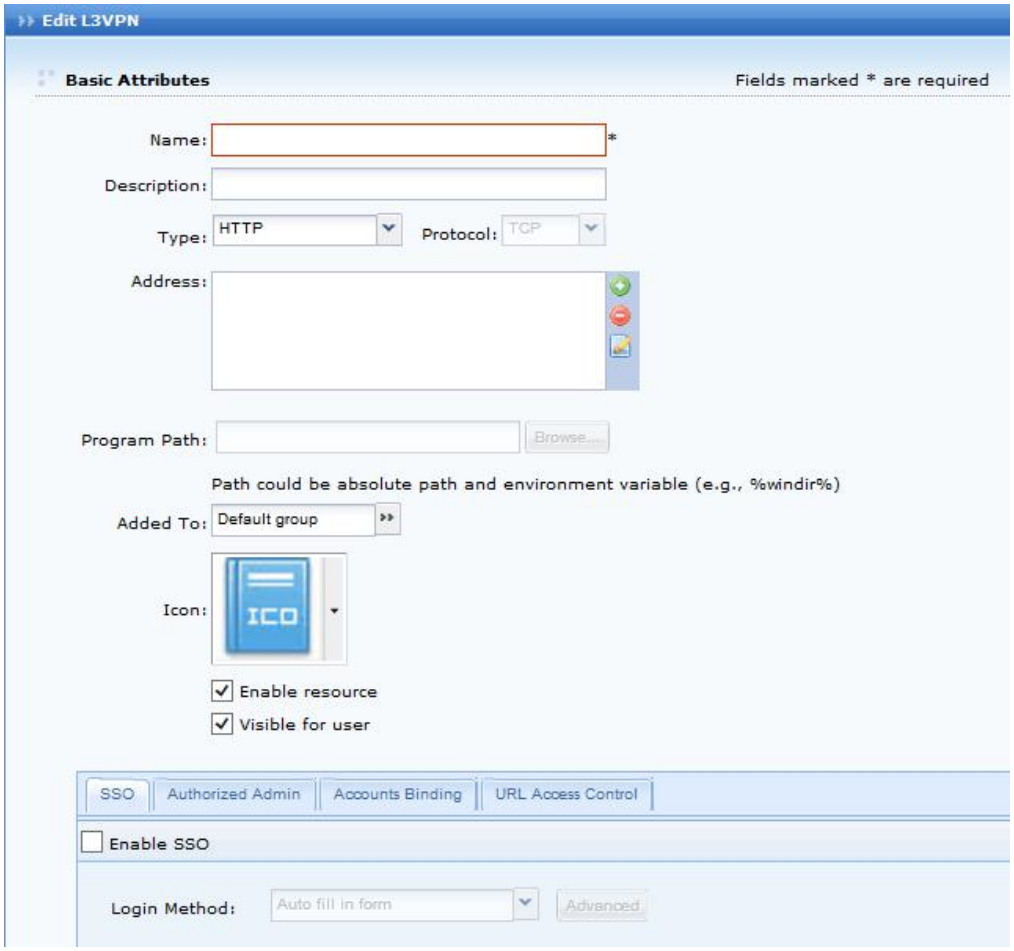
- While any user is accessing the resource, none of the protected files can be altered.
- The first time TCP resource is accessed by end user over SSL VPN, the TCP component may be installed on the computer automatically. However, installation of TCP component requires administrator privilege on the computer. If any firewall or anti-virus software is installed and runs on the client PC, it will block installation process. To ensure the component installed successfully, terminate the firewall or anti-virus software first.

8. Click the **Save** button and then the **Apply** button to save and apply the settings.

Adding/Editing L3VPN

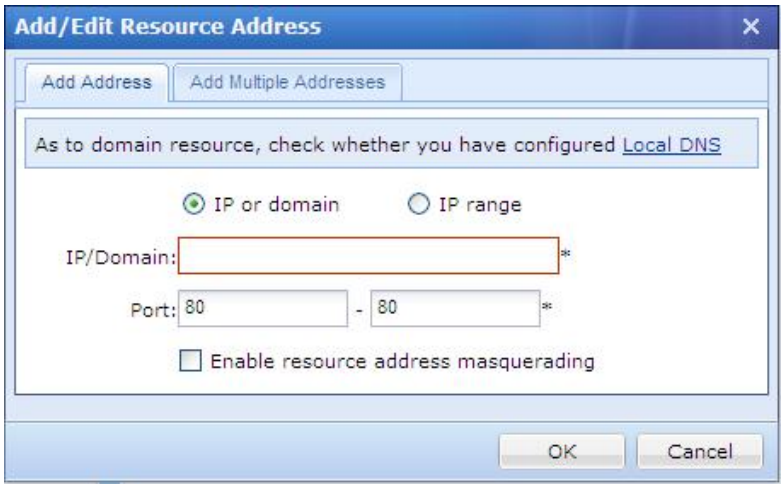
L3VPN is a type of resource based on IP protocol, allowing end users to use TCP/UDP/ICMP based application on their computer to remotely access corporate resources and servers over SSL VPN.

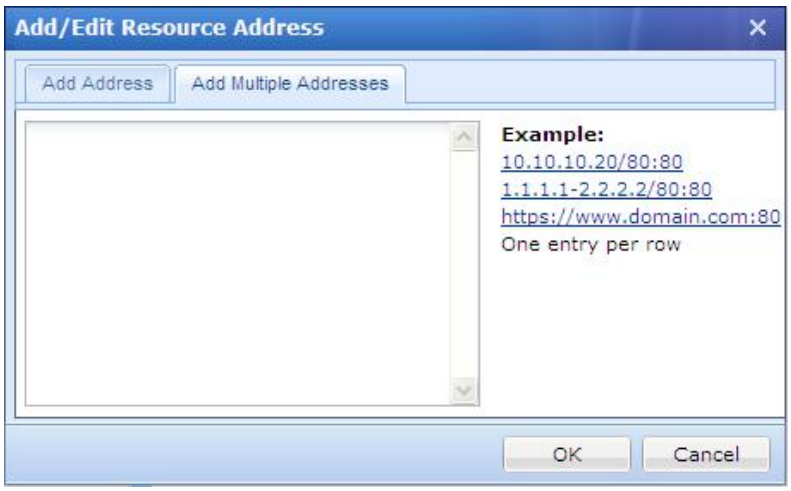
1. Navigate to **SSL VPN** > **Resources** page and click **Add** > **L3VPN** to enter the **Edit L3VPN** page, as shown in the figure below:



2. Configure **Basic Attributes** of the L3VPN. The following are the basic attributes:

- **Name, Description:** Indicates the name and description of the L3VPN. This name may be seen on the **Resource** page after user logs in to the SSL VPN successfully.
- **Type:** Indicates type of the L3VPN. Some common types are built in the Sangfor device. This selection determines the port number entered in the **Port** field automatically. If the L3VPN is not any of the built-in types, select **Other** and configure the port by hand.
- **Protocol:** When the selected L3VPN type is **Other**, **Protocol** is selectable. Options are **All**, **TCP**, **UDP** and **ICMP**. Select the protocol according to the L3VPN you are defining.
- **Address:** Indicates address of the L3VPN. To add one entry of address (IP address, domain name or IP range), click the **Add Address** tab. To add multiple entries of addresses, click the **Add Multiple Addresses** tab, as shown in the figures below:







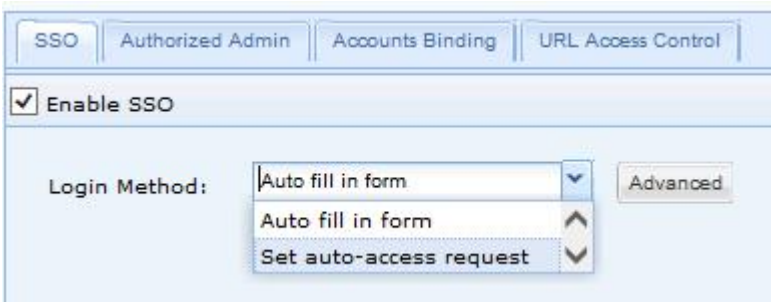
- **Port** indicates the port used by this L3VPN to provide services. For the built-in types, this port is predefined. For **Other** type of L3VPN, enter the port number that is to be used by the L3VPN you are defining.
- If resource address is domain name, navigate to **System** > **SSL VPN Options** > **General > Local DNS** to configure local DNS server (for detailed guide, refer to the Configuring Local DNS Server section in Chapter 3).

- **Program Path:** Indicates path of the client software program that may be used by some C/S application.
- **Added To:** Indicates the resource group to which this resource is added. By default, the selected resource group is **Default group** (to configure resource group, refer to the Adding/Editing Resource Group section in Chapter 4).
- **Visible for user:** To have connecting users see this resource on the **Resource** page, select this option. Invisibility here only means that the resource is not seen on the

Resource page, in fact, it is still accessible to the user.

3. Configure **SSO** tab.

   To enable connecting users to use SSO feature to access corporate resources over SSL VPN, select **Enable SSO** option and configure the **SSO** page (under **System** > **SSL VPN Options** > **General**. For more details, refer to the Configuring SSO Options section in Chapter 3).



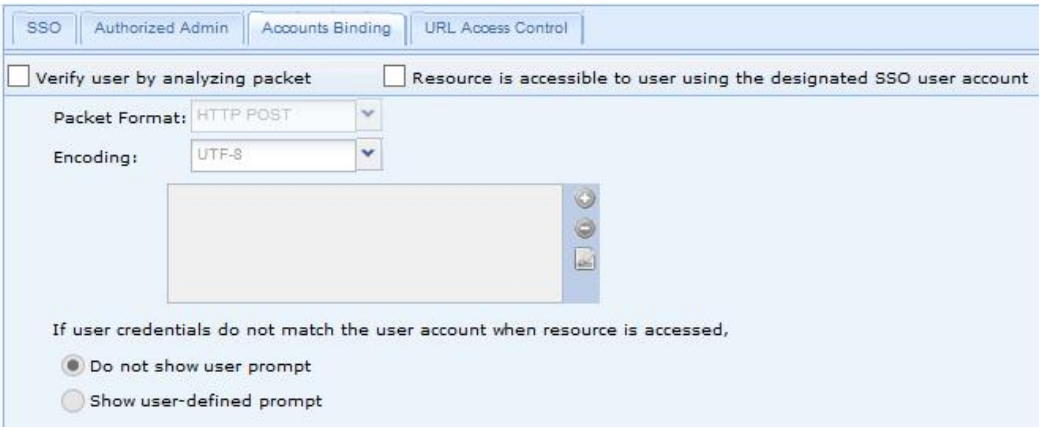
4. Configure **Authorized Admin** tab.

   Specify the administrators that will have the right to manage this resource and the right to grant other administrator the privilege to manage this resource.



- The authorized administrators cannot edit the resource. They only have the right to assign this resource to users (in other words, the right to associate resources with the role under **SSL VPN** > **Roles** > **Edit Role**) and to grant other administrators (in its permitted realm) the privilege to manage this resource, rather than the privilege of editing resource.
- Please it keep in mind that the privilege of editing a resource always belongs to the creator who has created this resource as well as the administrator with higher privilege. The authorized administrators cannot see those resources in the **Resource Management** page, but can see and associate them with users on the **Add Role** or **Edit Role** page.

5. Configure **Accounts Binding** tab, as shown in the figure below.



If **Verify user by analyzing packet** is selected, the SSL VPN account will bind to the account for resource access, in the way that packet is obtained as specified according to **Packet Format** and the others settings.

If **Resource is accessible to user using the designated SSO user account** is selected, end user have to use the corresponding SSL VPN account and designated SSO user account to access this L3VPN resource, other user accounts being unable to match the credential.

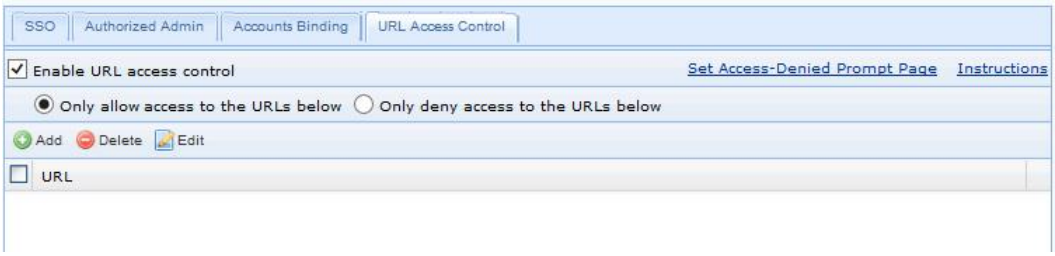
Web application, TCP application and L3VPN support accounts binding.



- To enable end users to single sign in to a resource, enable SSO for that resource (under **SSL VPN** > **Resources** > **Edit L3VPN** > **SSO** tab) and bind the SSL VPN account to the SSO user account (to configure SSO user account, refer to the Configuring SSO User Account section in Chapter 4).
- Applying **Verify user by analyzing packet** does not require SSO to be enabled.

6. Configure **URL Access Control** tab.

This achieves the control over users' access to certain directory of a server, user being able or unable to access the specified directory.





URL access control feature is only available while the selected L3VPN type is **HTTP**. The other types of L3VPN do not support this feature.

7. Click the **Save** button and **Apply** button to save and apply the settings.

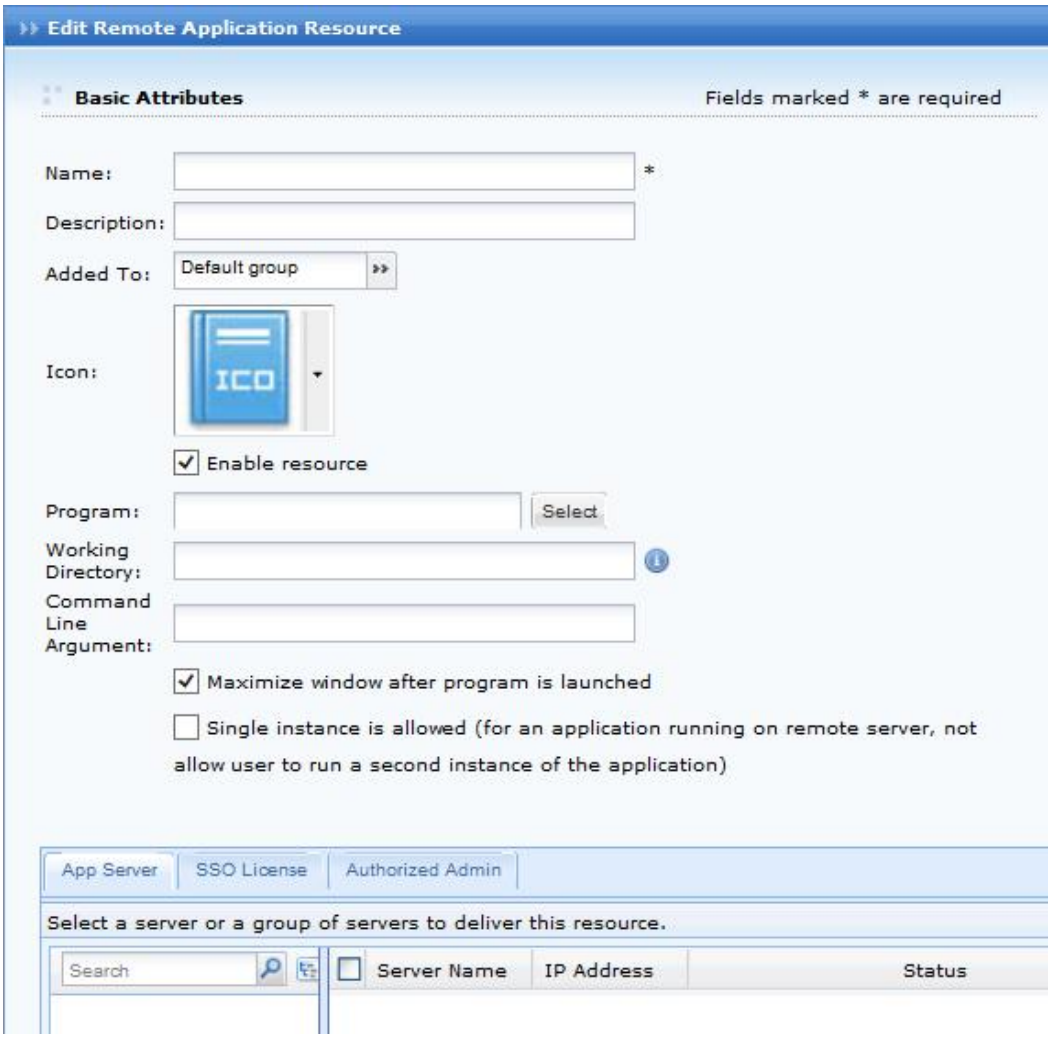


- The first time L3VPN resource is accessed over SSL VPN, L3VPN component may be installed on the user's PC automatically. However, installation of L3VPN component requires administrator privilege on the computer. If any firewall or anti-virus software is installed and runs on the computer, it will block installation process. To ensure the component installed successfully, terminate the firewall or anti-virus software first.
- Among the L3VPN resources, there is a system-protected L3VPN resource named **All Subnet L3VPN resources**. This resource stands for all L3VPN resources with the addresses on the subnets where LAN and DMZ interfaces reside and those resources on the subnets where LAN and DMZ interfaces reside, using the protocol TCP, UDP or ICMP (port: 1-65535). Like other L3VPN resource, it can be associated with users; however, no attribute of it can be modified except for the name, description and visibility. If the subnet resources do not reside in the same network segment as the LAN and DMZ interface of the Sangfor device, which means, there is layer-3 router or switch on the way, add the subnet on the **Local Subnets** page (under **System** > **Network**) and a corresponding route on **Routes** page (under **System** > **Network**) to make that subnet "local". That will enable the machines on the two subnets to communicate directly.

Adding/Editing Remote Application

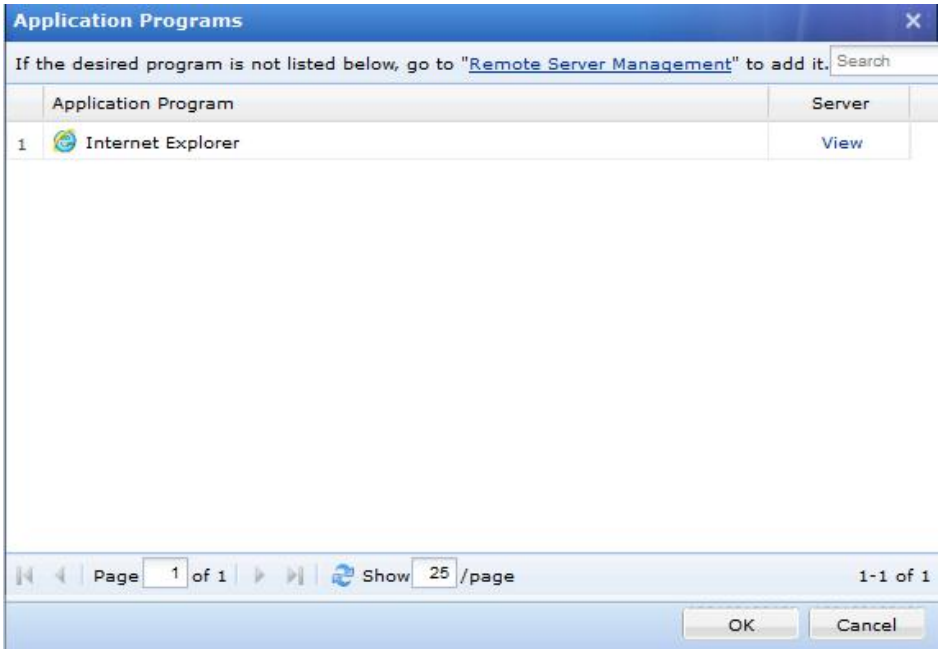
Remote applications are applications launched by remote servers and accessed by end users over SSL VPN. User runs the program on the local computers but access the data on the remote server in the remote application session.

1. Navigate to **SSL VPN** > **Resources** and click **Add** > **Remote Application** to enter the **Edit Remote Application Resource** page, as shown below:



2. Configure **Basic Attributes** of the remote application. The following are the basic attributes:

   - **Name, Description:** Indicates the name and description of the remote application. This name may not be seen on the **Resource** page after user logs in to the SSL VPN successfully.
   - **Added To:** Indicates the group to which this resource is added. By default, the selected resource group is **Default group** (to configure resource group, refer to the Adding/Editing Resource Group section in Chapter 4).
   - **Icon:** Icon specified for this resource, which could be seen on the **Resource** page if this resource is added to a group that has its resources show in icons.
   - **Program:** Specifies the applications provided by remote application server. Click on **Select** to select the desired application, as shown in the below figure:



- **Working Directory：** Indicates the path of the application on remote application server.
- **Command Line Argument:** Specifies the parameters that may be used when some application program starts.

If **Maximize window after program is launched** is selected, program window will be maximized once program is launched.

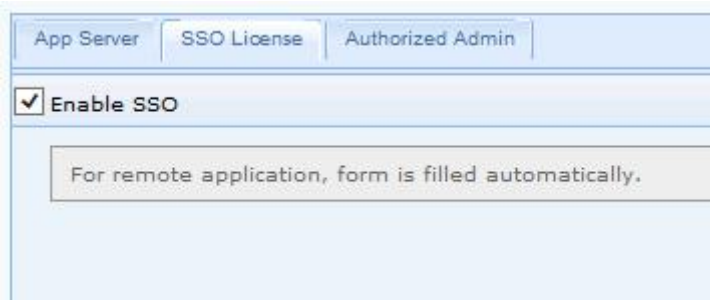
In case that **Single instance is allowed** is selected and user has launched an application, user will be redirected to the previously-launched application if user clicks on the resource link again, instead of launching a new instance. If command line argument is configured, this options is not recommended to enable.

3. Click the **App Server** tab and select remote application servers, so that they can provide the application (to configure remote server, refer to the Adding Remote Application Server section in Chapter 4).



4. Configure **SSO License** tab.

If SSO feature is enabled and SSO information is recorded, SSO will be performed automatically when user accesses specific remote application over SSL VPN.



- As to remote application, SSO feature only supports the method of auto fill in form.
- If you want to deliver a browser allowing SSO, only IE-cored browser can be delivered.
- When recording SSO information for remote application, only IE is taken as B/S-based resource, all the other resources are taken as C/S-based resource.

5. Configure **Authorized Admin** tab.

   Specify the administrators who will have the right to manage this resource and the right to grant other administrator the privilege to manage this resource.



   - The authorized administrators cannot edit the resource. They only have the right to assign this resource to users (in other words, the right to associate resources with the role under **SSL VPN** > **Roles** > **Edit Role**) and to grant other administrators (in its permitted realm) the privilege to manage this resource, rather than the privilege of editing resource.
   - Please it keep in mind that the privilege of editing a resource always belongs to the creator who has created this resource as well as the administrators with higher privilege. The authorized administrators cannot see those resources in the **Resources** page, but can see and associate them with users on the **Add Role** or **Edit Role** page.

More Operations

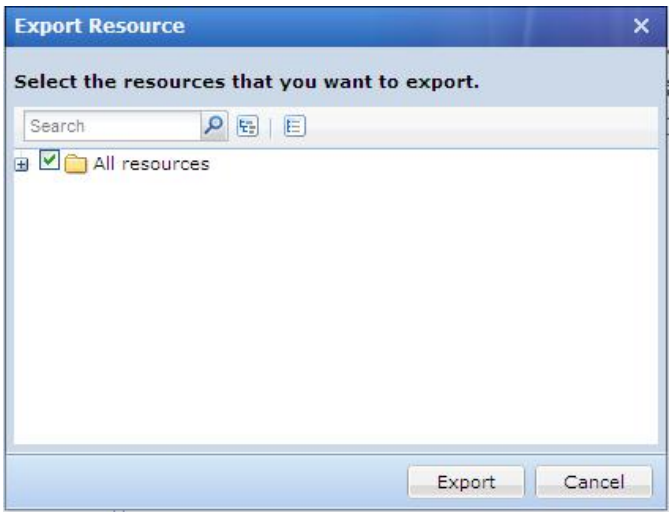
More operations include **Export resource**, **Import resource** and **Resource Sorting**. Click **More** on **Resources** page, you will see the following figure:



Exporting Resources

This feature helps export the existing resources from the current Sangfor device to the computer.

1. Navigate to **SSL VPN** > **Resources** and click **More** > **Export resource** to enter the **Export Resource** page, as shown the figure below:

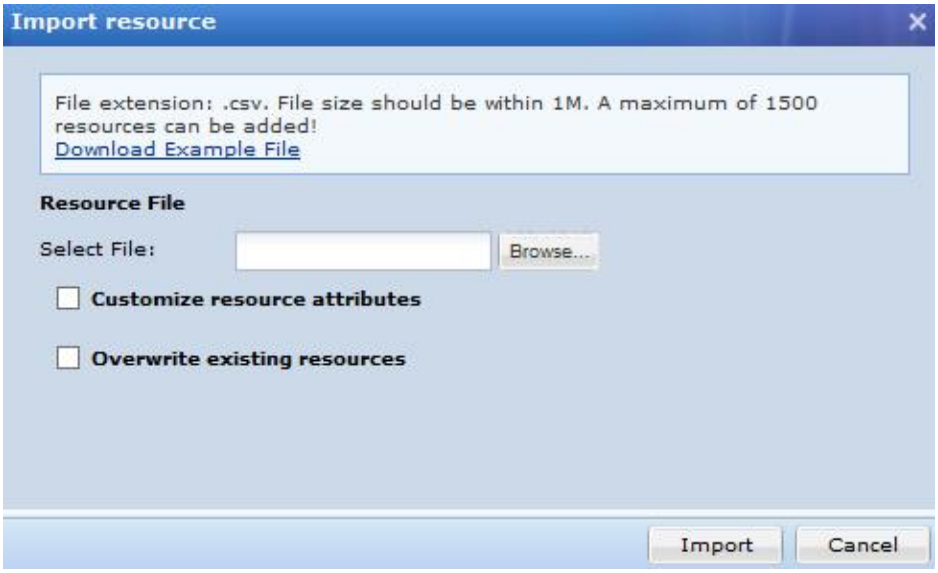


2. Select the checkboxes next to the resources or resource groups that you want to export.
3. Click the **Export** button. By default, the exported resource will be saved in a csv file named **rclist.csv**.

Importing Resources

This feature helps import resources from the computer to the Sangfor device.

1. Navigate to **SSL VPN** > **Resources** and click **More** > **Import resource** to enter the **Import Resource** page, as shown in the figure below:



2. Configure the following included on **Import Resource** page:

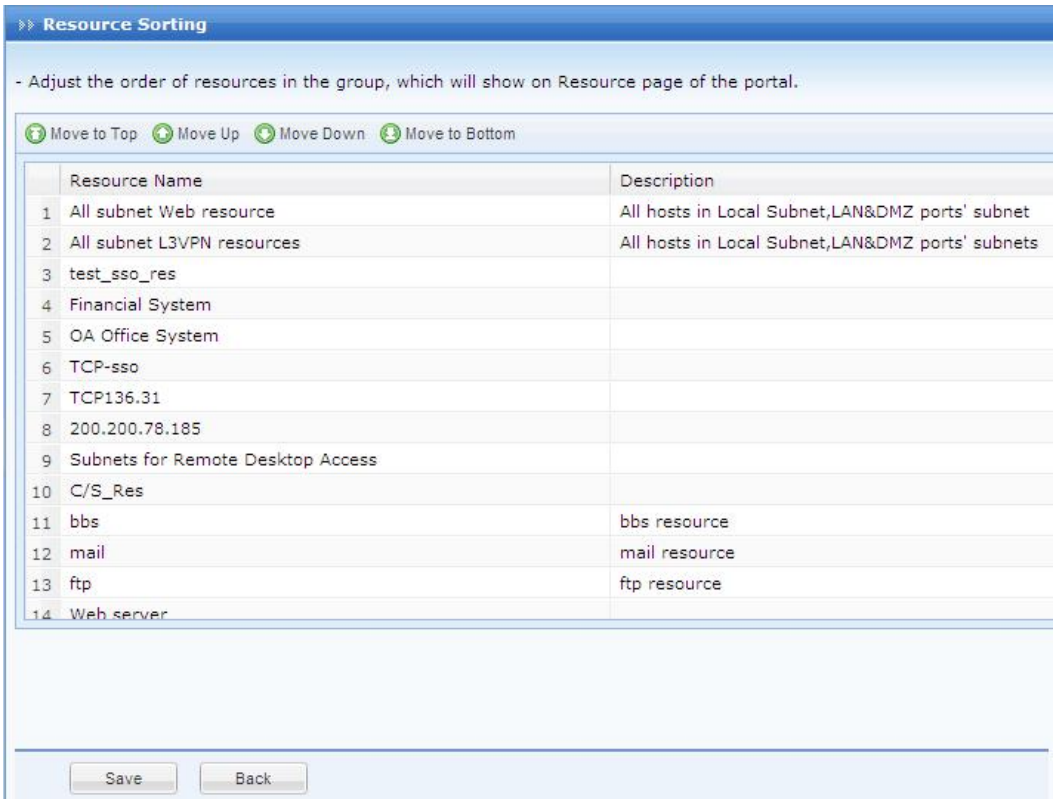
   - **Download Example File:** Before uploading the csv file, make sure that format of each resource entry in it is proper. It is recommended to download the example file and edit the resources based on the example file. After editing the csv file, upload it through the above page.
   - **Customize resource attributes:** The two fields below it define the attributes of the imported resources, the description and the target group to which they are to be added.
   - **Overwrite existing resources:** If this option is checked, the existing resource will be replaced by the imported resource that owns a same name.

3. Click the **Import** button.

Sorting Resources

Sorting resource is a feature applying to resource group. You can change the resource order by clicking **Move to Top**, **Move Up**, **Move Down** or **Move to Bottom** button. The resource order in the group determines the order of the resources that end users see on the **Resource** page.

1. Navigate to **SSL VPN** > **Resources** and click **More** > **Import resource** to enter the **Import Resource** page, as shown in the figure below:



2. To move an entry to top of the list, click the entry and click **Move to Top**.
3. To move an entry to bottom of the list, click the entry and click **Move to Bottom**.
4. To move an entry up and exchange order with the upper entry, click the entry and click **Move Up**.
5. To move an entry down and exchange order with the lower entry, click the entry and click **Move Down**.
6. To edit the selected resource, click **Edit**; to remove the selected resource, click **Delete** on **Resources** page, as shown below:



7. To select the resources on current page, click **Select > Resource > Current page,** or click **Select > Resource > All pages** to select the resources on all pages, as shown below**:**



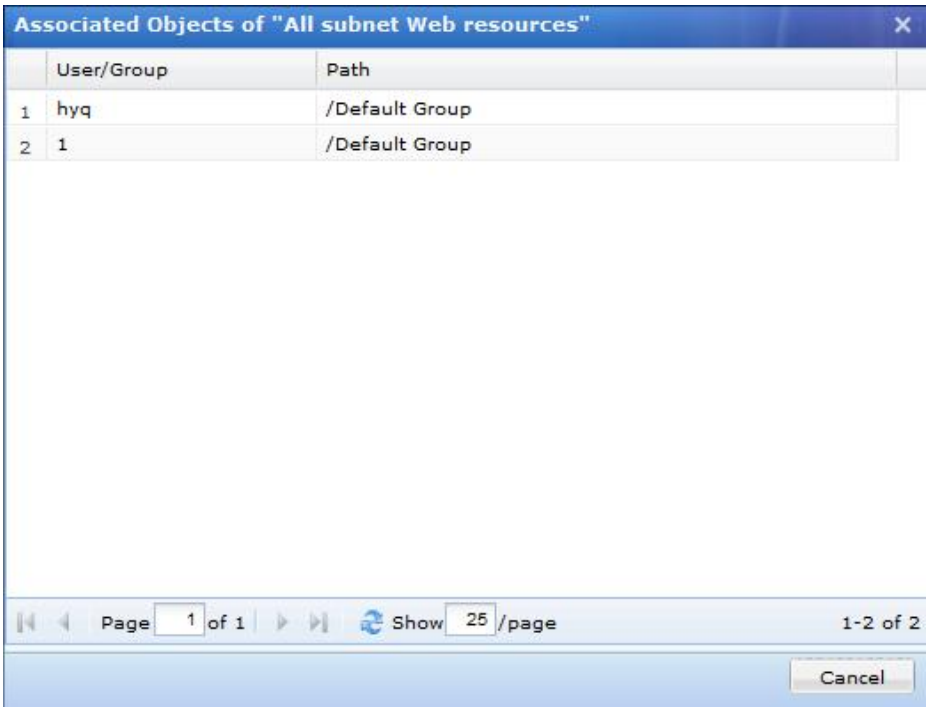
8. To deselect the selected resource, click **Deselect**.

9. To move a resource to other resource group, select the resource and click **Move**.

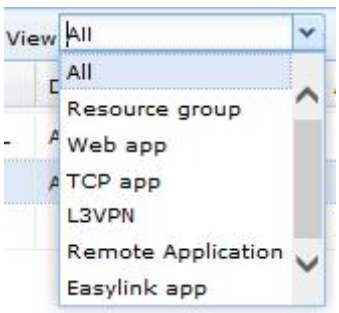


Please note that resource group cannot be moved.

10. To view associated user of a selected resource, click **View Association**, as shown below:



11. To view resource of specific type, you can specify the desired resource type in **View** field on **Resources** page. Options are **All**, **Resource group**, **Web app**, **TCP app**, **L3VPN**, **Remote Application** and **Easylink app**.

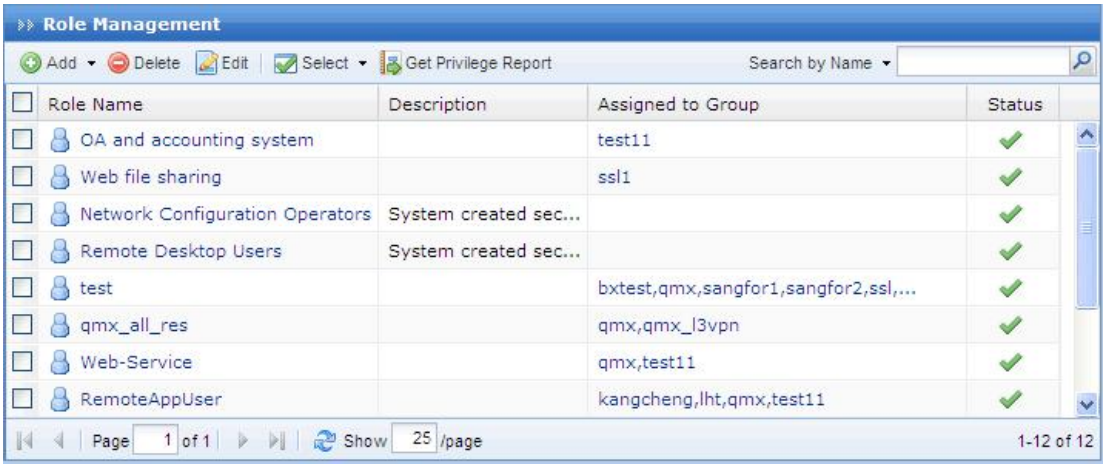


Roles

A role is an intermediate that builds a connection between user/group and resource, more specifically, designates internal resources to user or group. Users can only access the designated internal resources over SSL VPN.

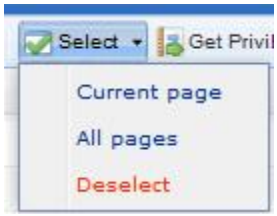
This kind of association enables one or multiple users or groups to associate with one or multiple resources, facilitating control over users' access to corporate resources.

Navigate to **SSL VPN** > **Roles** and the **Role Management** page appears, as shown below:



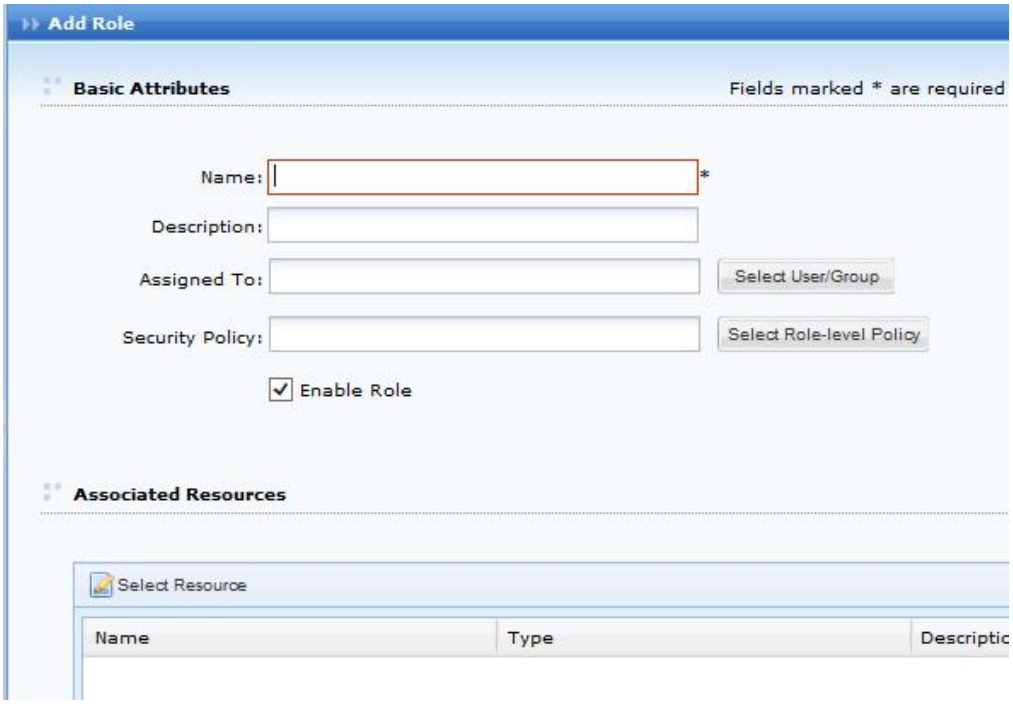
The following are some contents included on **Role Management** page:

- **Search By Name/Description/User(Group):** To search for specific role or type of roles, select an option, enter the keyword into the textbox and click the magnifier icon. Name/description indicates the name/description of the role. User/group indicates the user and/or group that the role is assigned to.
- **Role Name:** Indicates name of the role.
- **Description:** Indicates description of the role.
- **Add:** Click it to add new role directly or using an existing role as template.
- **Edit:** Click it to edit a selected role.
- **Delete:** Click it to remove the selected role(s).
- **Select:** To select roles on all pages, click **Select > All pages**; click **Select > Current page** to select roles on current page. To deselect entries, click **Select > Deselect**.



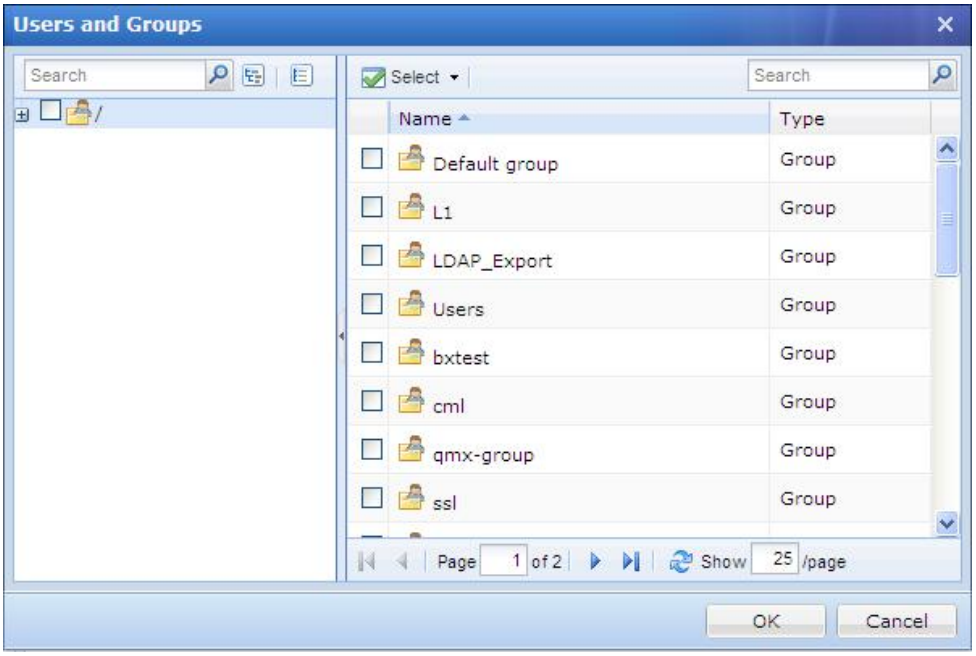
Adding Role

1. Navigate to **SSL VPN** > **Roles** and click **Add** > **Role** to enter the **Add Role** page, as shown in the figure below:



2. Configure the **Basic Attributes** of the role. The following are basic attributes:

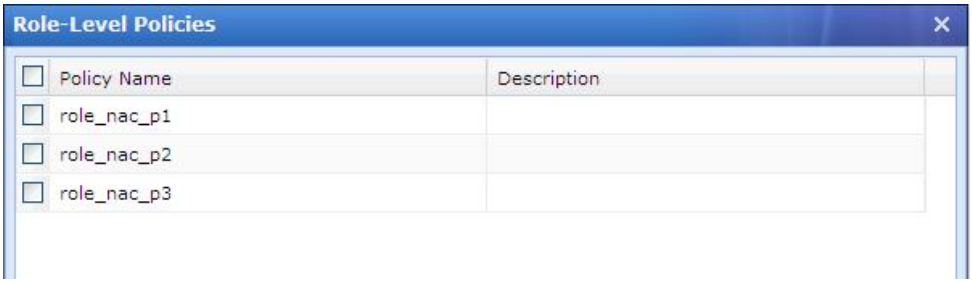
   - **Name:** Configures name of the role.
   - **Description:** Configures description of the role.
   - **Assigned To:** Configures the user and/or group that can access the associated resources. To specify user and group, click the **Select User/Group** button, and all the predefined users and groups on **Local Users** page are seen in the list, as shown below:



Select the user or group to which the role is to be assigned and click the **OK** button.

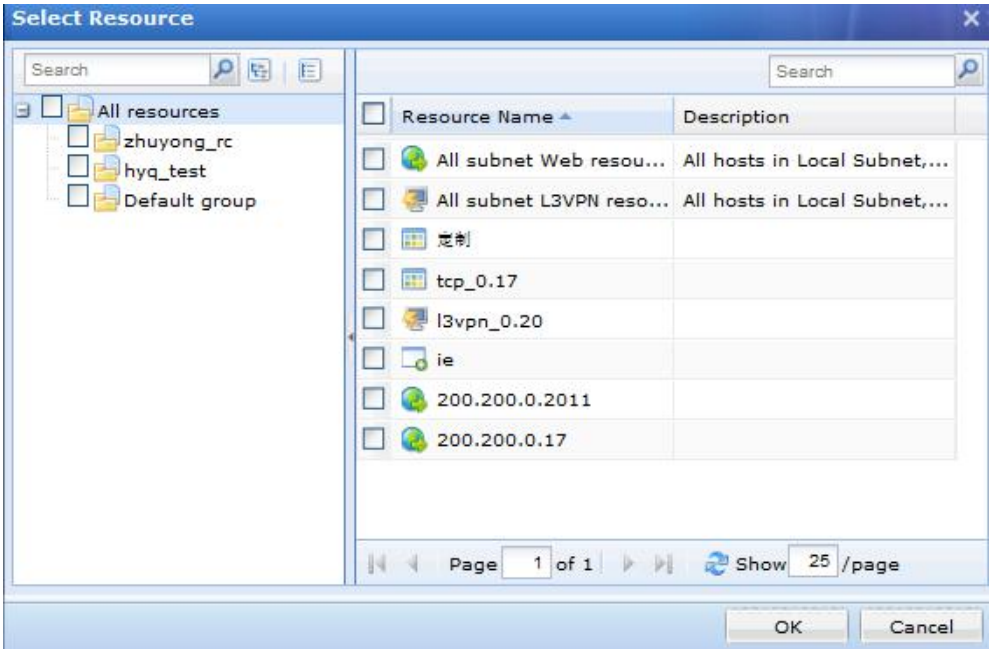
- **Security Policy:** This policy enforces host checking when user logs in to the SSL VPN. If user fails any security check, he or she cannot access the associated resources.

  To specify a role-level policy, click the **Select Role-level Policy** button and all the predefined role-level policies are seen (to configure role-level policy, refer to the Adding Role-level Policy section in chapter 4), as shown in the figure below:



If no role-level policy is configured, you do not need to configure security policy.

3. Configure associated resources. Click **Select Resources** to enter the **Select Resource** page and select resources that the associated users of this role can access, as shown below:

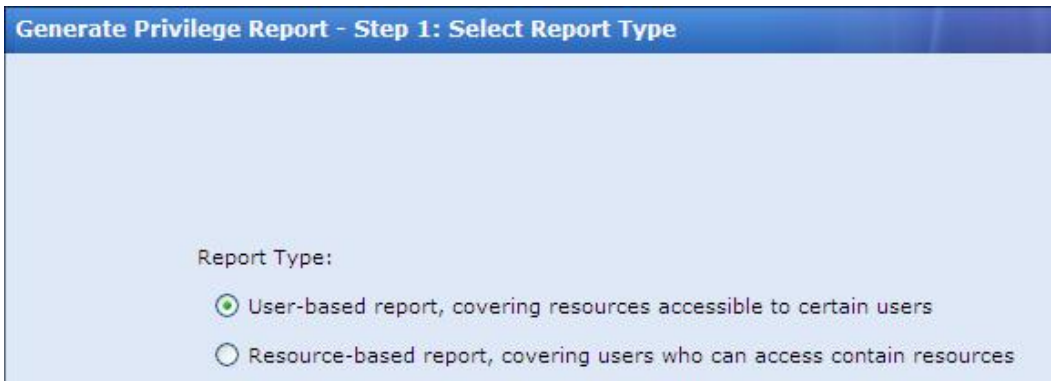


4. Click the **Save** button on the **Add Role** page to save the settings.

Getting Privilege Report

Privilege report is a kind of report telling what resources the specified users can access, or what users can access the specified resources.

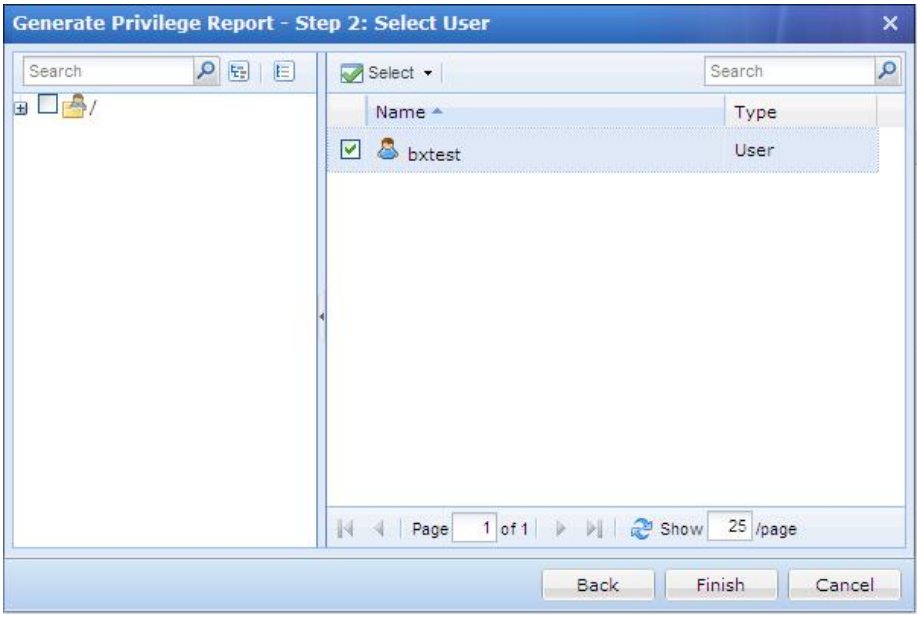
1. Click **Get Privilege Report** to get started, as shown below:



2. Select the type of report you want to generate. There are two types of privilege reports, **User-based report** and **Resource-based report**. The former type of report presents what internal resources the selected users can access, while the latter type of report presents what users can access the selected resources

   To generate **user-based privilege report**, perform the following two steps:

   a. Select **User-based report…** and click the **Next** button, as shown below:

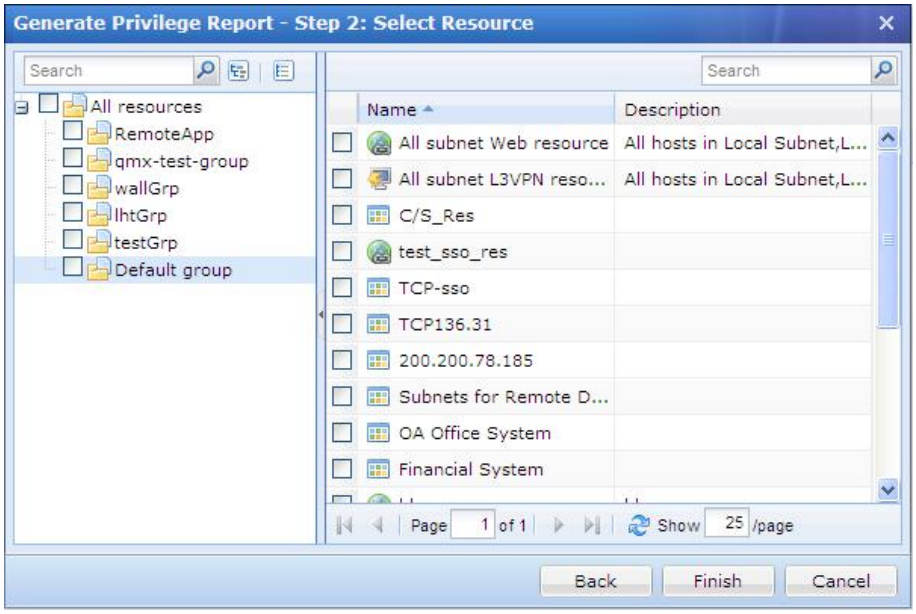


b. Select the desired user(s) and click the **Finish** button to download the .csv file. The download user-based privilege report file is as shown below:

	A	B	C	D	E	F
1	Privilege Report - On User Groups					
2	Generated at: 2011-10-10 5:32:59 ; total user groups: 2					
3						
4	Group	Location	Descriptic	Associated Resources		
5	gfds	/cml				
6	cml	/				
7						
8	Privilege Report - On Users					
9	Generated at: 2011-10-10 5:32:59 ; total users: 3					
10						
11	Username	Location	Descriptic	Associated Resources		
12	jhfg	/cml/gfds				

To generate **resource-based privilege** report, perform the following two steps:

a. Select **Resource-based report…** and click the **Next** button, as shown below:



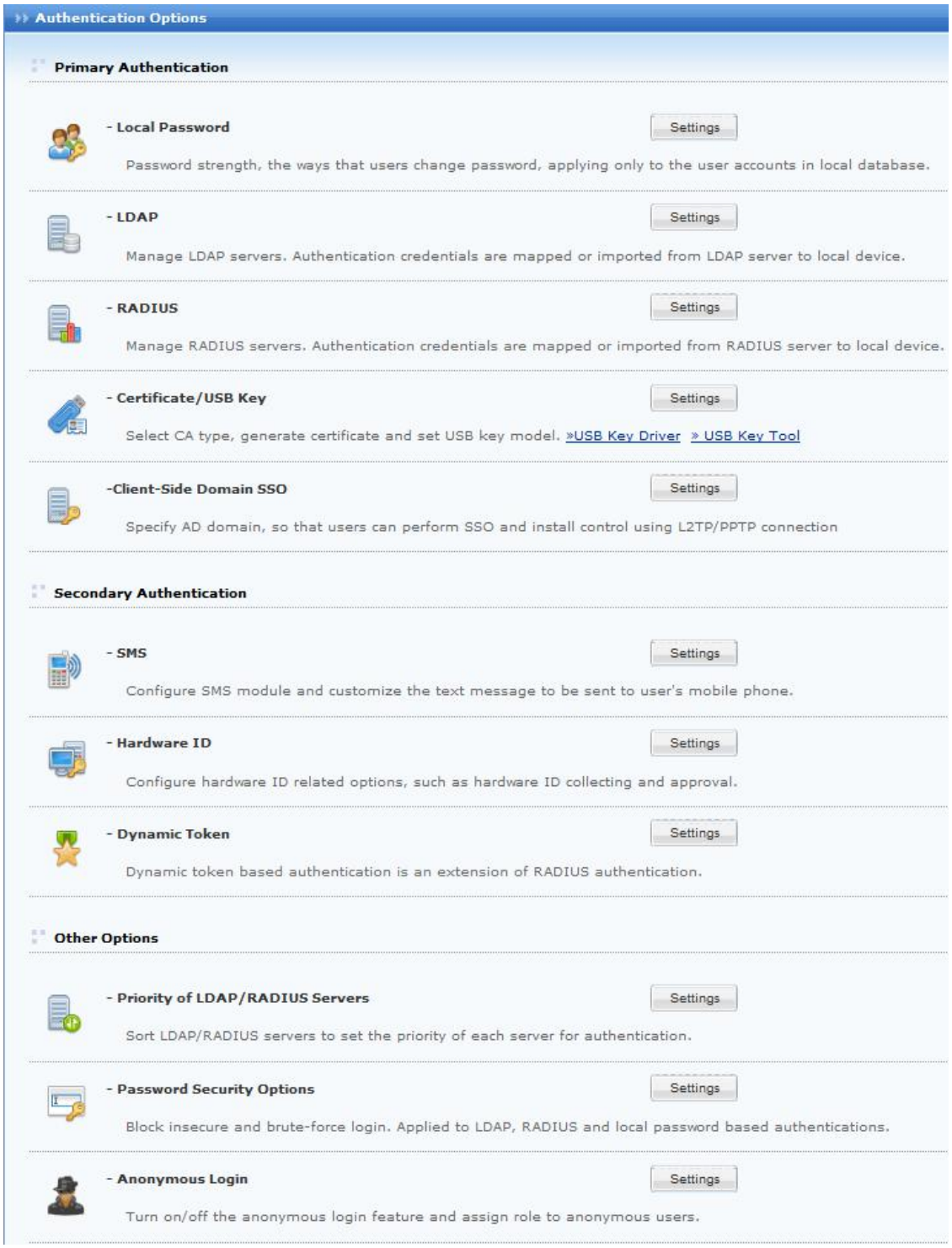
b. Select the desired resource(s) and click the **Finish** button to download the .csv file. The download resource-based privilege report file is as shown below:

A	B	C	D	E	F
Privilege Report - On Resources					
Generated at:2011-10-10 8:07:05; total resources:1					
Resource	In Group	Description	Type	Address	Assigned to User
All subnet	Default group	All hosts in Local Subnet,LAN&DMZ ports' subnets	WEB app	*	/Default group/,

Authentication Options

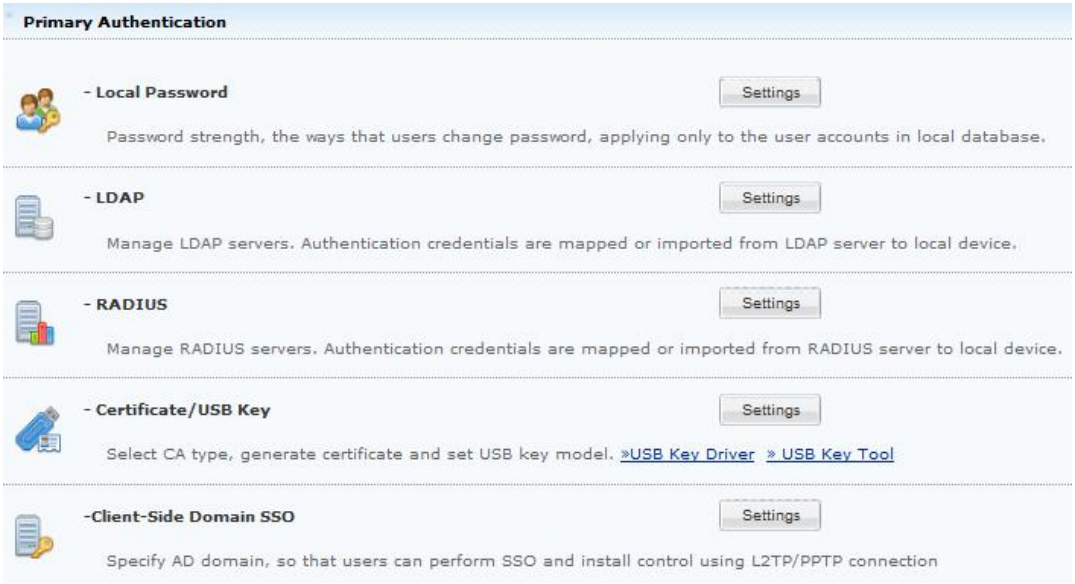
Authentication Options covers settings related to primary and secondary authentication methods.

Navigate to **SSL VPN** > **Authentication** and the **Authentication Options** page appears, as shown in the figure below:



Primary Authentication Methods

There are five primary authentication methods, namely, **local password** based authentication, **LDAP** authentication, **RADIUS** authentication, **certificate/USB key** based authentication and **client-side domain SSO** authentication.



Local Password Based Authentication

The settings related to local password based authentication include password security options and username options.

Navigate to **SSL VPN** > **Authentication** to enter the **Authentication Options** page (as shown in the figure above). Click the **Settings** button following **Local Password**, and the **Local Password Based Authentication** page appears, as shown in the figure below:



The following are some contents included on the **Local Password Based Authentication** page:

- **Password Security Options:** Configures the password strength, the ways that users change password. If enabled is selected, password security check will be performed when user logs in to SSL VPN. If user password fails to match the password security policy configured in this field, user will be asked to change password.
- **Username Options:** If the option **Ignore case of username** is selected, case of username would be ignored when users enter credentials to log in to SSL VPN. If any same usernames in different case already exist in user organization structure before this option is enabled, such as "HSw", "hsw", this user will fail to modify personal information after **Ignore case of username** is selected, he/she needs to modify its username first. Then enable this option.



Password Security Options and **Username Options** only apply to the user accounts in local Sangfor device.

LDAP Authentication

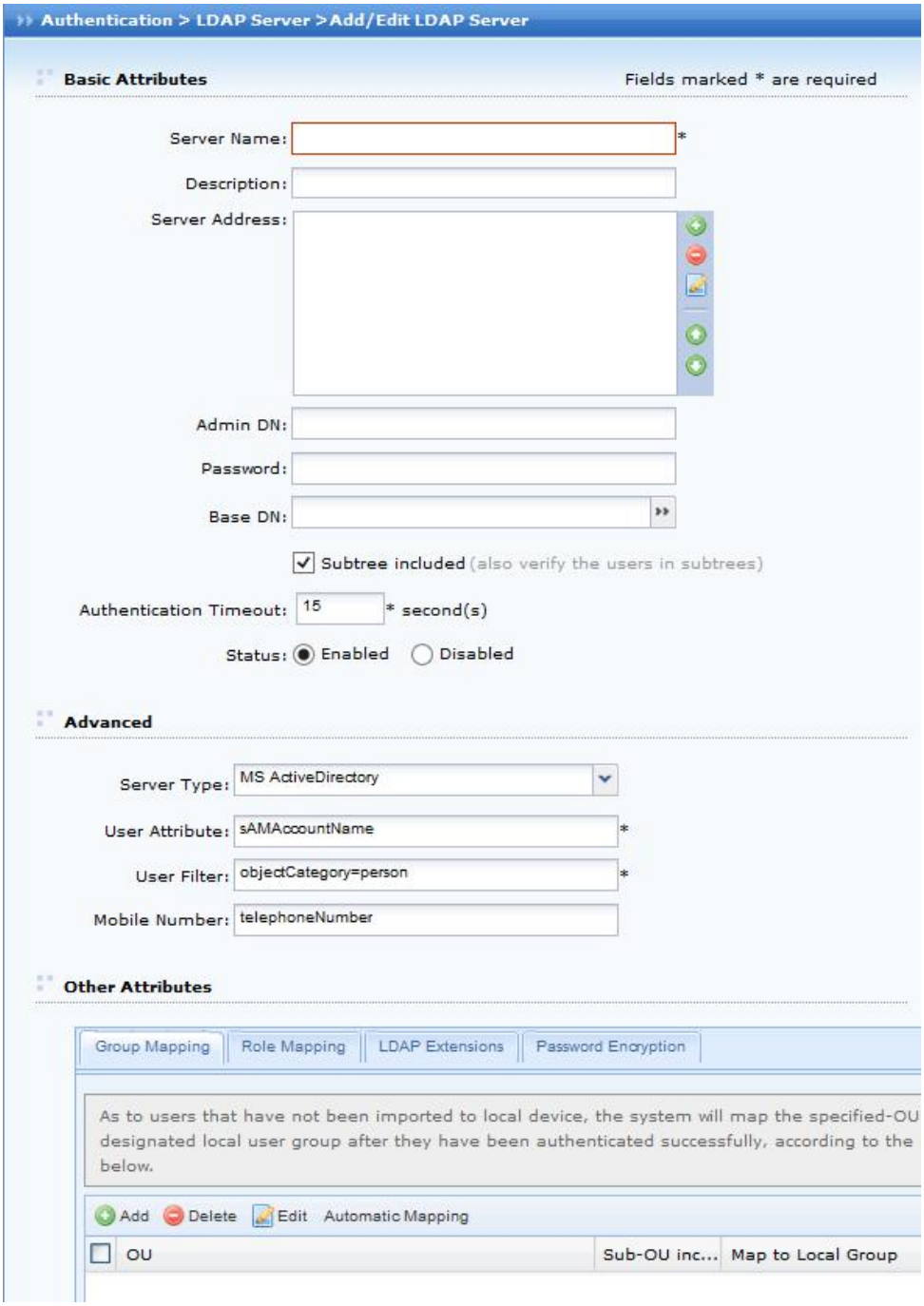
Sangfor device supports third-party LDAP server to verify the users connecting the SSL VPN.

Configuring LDAP Server

1. Navigate to **SSL VPN** > **Authentication** to enter the **Authentication Options** page. Click the **Settings** button following **LDAP** and the **LDAP Server** page appears, as shown below:



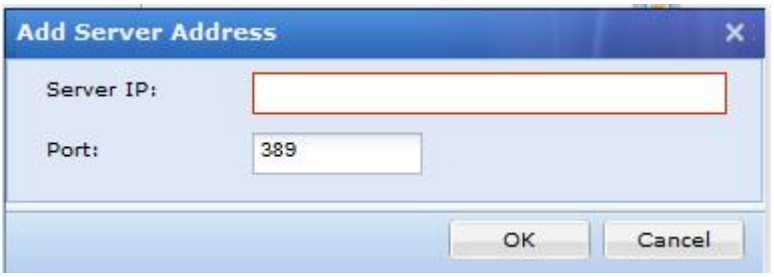
2. Click **Add** to enter the **Add/Edit LDAP Server** page, as shown below:



3. Configure the **Basic Attributes** of the LDAP server. The following are basic attributes:

   - **Server Name, Description:** Configures the name and description of the LDAP server.
   - **Server Address:** Configures the usable IP address and port of the LDAP server. You can add multiple IP addresses and ports. Generally, only the first IP address/port is active and the others are standby. If the first IP address/port is unavailable, the second IP address/port will take the place; if the second IP address/port is unavailable, the third IP address/port will take the place, and so on; if none of the configured server IP addresses/ports is available, the server will be disconnected.

     To add an entry of server address and port, click the **Add** icon  next to the **Server Address** field. The **Add Server Address** page is as shown in the figure below:



To remove an entry, click the entry and click **Delete** icon next to **Server Address**.

To edit an entry, click the entry and click **Edit** icon next to **Server Address**.

To adjust order of an entry, click the entry and click **Move Up** icon or **Move Down** icon .

- **Admin DN**, **Password:** Configure the administrator account to read the organizational units (OU) and security groups on the LDAP server. The administrator account should be in DN format.

This administrator must have privilege to read path of users on the LDAP server.

- **Base DN:** Configures the location of the LDAP users that are to be verified.
- **Subtree included:** Select this option so that the users contained in the sub-OU of the OU specified in **Base DN** field are included in. Otherwise, only the direct users in the specified OU level will be verified.
- **Authentication Timeout:** Configures the time period that user authentication gets timed out if LDAP server gives no response.
- **Status:** Indicates whether the LDAP server is enabled.

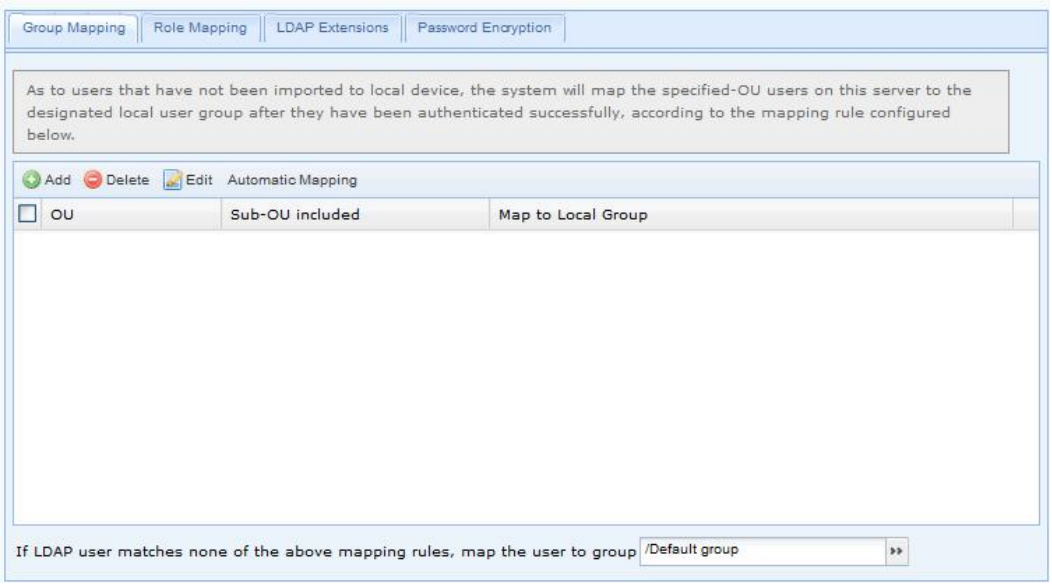
4. Configure the **Advanced** options. The values in these fields must be consistent with those on the LDAP server



Protocols supported are LDAP and MS Active Directory (AD). For MS AD, user authentication is achieved using attribute **sAMAccountName** and filter **objectCategory=person**. For LDAP, user authentication is achieved using attribute **uid** and filter **objectclass=person**. However, the attribute names could be modified.

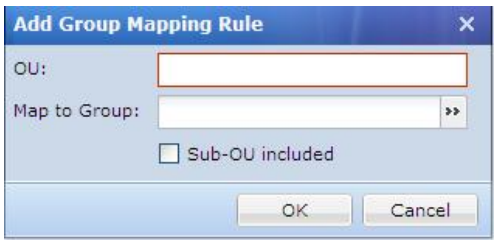
5. Configure **Group Mapping** tab.

Group mapping only applies to the LDAP users that have not been imported to the Sangfor device. The users in specified OU on the LDAP server will be mapped to a local group after successful login, and therefore have the same privilege as the users that they are mapped to.



The following are contents included on the **Group Mapping** tab:

- **Add:** To add a group mapping rule to map specified LDAP users to the local group, click it to enter the **Add Group Mapping Rule** page, as shown in the figure below:

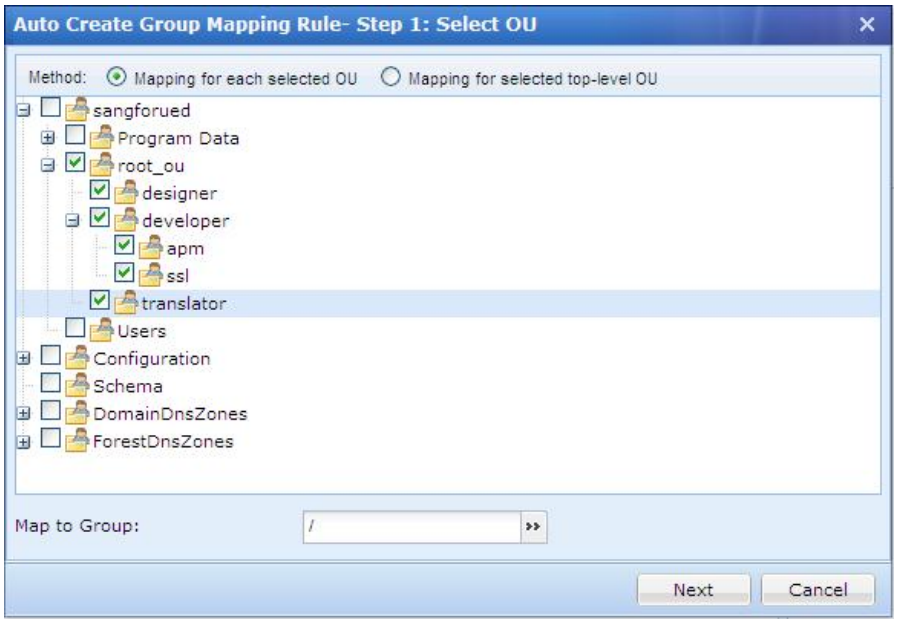


  - **OU:** Configures the OU that will be mapped to a local group, in format of DN.
  - **Map to Group:** Configures the local group to which users of the specified OU will be mapped.
  - **Sub-OU included:** If this option is selected, users in the sub-OU will also be included and mapped to the local group. If not selected, only the users in the

specified OU level will be mapped to the local group.

- **If LDAP user matches none of the above mapping rules, map the user to group:** For the users that match none of the group mapping rules, select this option and specify a local group, so that those LDAP users will be mapped to that group automatically.
- **Delete:** To delete a group mapping rule, select the rule and click **Delete**.
- **Edit:** To edit a group mapping rule, select the rule and click **Edit**.
- **Automatic Mapping:** This feature simplifies the process of adding a batch of mapping rules. Administrator needs only to select the LDAP user and/or group on the **Auto Create Group Mapping Rule – Step 1: Select OU** page (as shown in the figure below) and configure **Map to Group** field, without adding mapping rule one by one, and the involved mappings will be added to the group mapping rule list automatically. To configure automatic mapping, please perform the following steps:

  a. Click **Automatic Mapping** to enter the **Auto Create Group Mapping Rule – Step 1: Select OU** page, as shown below:



  b. Select a mapping method, **Mapping for each selected OU** or **Mapping for selected top-level OU**, and then select the organizational units (OU).

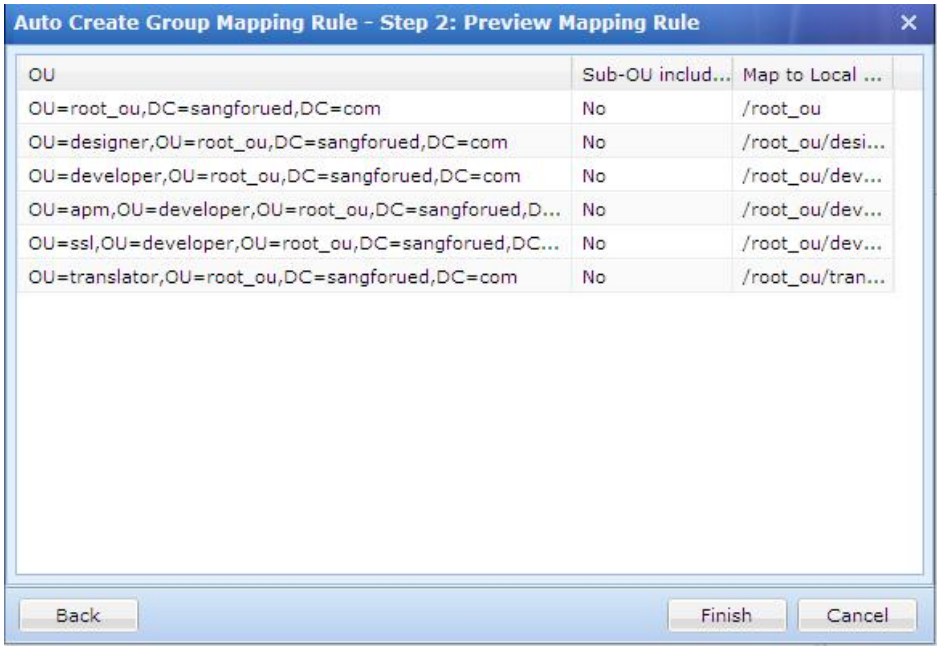
  If the selected method is **Mapping for each selected OU**, every selected LDAP user group will be mapped to the respective local group (name of target group is the same as the OU name) specified in **Map to Group** field, organizational units (OU) not being changed.

  If the selected method is **Mapping for selected top-level OU**, only one group will be created on the Sangfor device, name of the target group being the same as the top-OU name. All the users under the top-OU and/or the sub-OUs will be mapped to that group.

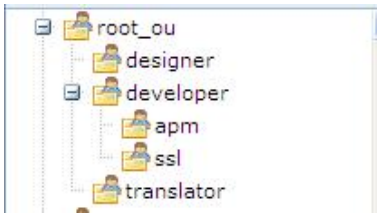
  c. Configure **Map to Group**. The specified group is a local user group to which the

specified LDAP users will be mapped.

d. Click the **Next** button and the automatically added mapping rules are as shown below:

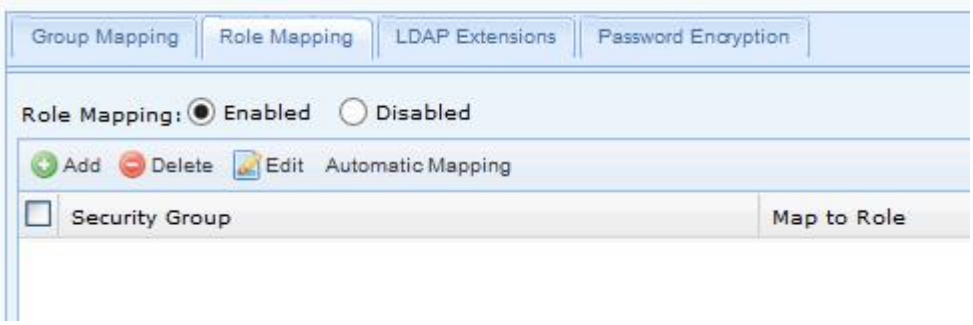


e. Click the **Finish** and **Save** buttons and go back to **Local Users** page. Check whether the groups created through automatic mapping are in user group list, as shown below:



6. Configure **Role Mapping** tab (if you are adding an MS Active Directory server).

Role Mapping helps map the security groups from the MS Active Directory server to the roles on this Sangfor device. Once a user matches certain role mapping rule and is mapped to the role on the Sangfor device, the associated user will be permitted to access the resources that are associated with that role. The **Role Mapping** tab is as shown in the figure below:



The following are the contents included on the **Role Mapping** tab:

- **Add:** Click it to add a role mapping rule, mapping the security groups on MS Active Directory server to the local groups. To configure role mapping, please perform the following steps:

  a. Select **Enabled** to enable role mapping feature.

  b. Click **Add** to enter the **Add Role Mapping Rule** page, and configure the **Security Group** and **Map to Role** fields, as shown below:

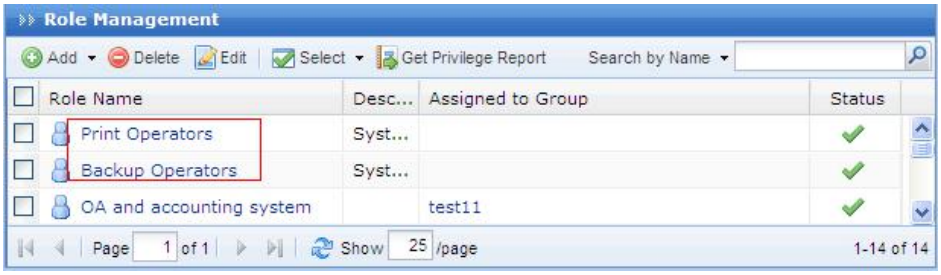


- **Delete:** To delete a role mapping rule, select the rule and click **Delete**.
- **Edit:** To edit a role mapping rule, select the rule and click **Edit**.
- **Automatic Mapping:** Click it and some role mapping rules will be generated automatically according to the security groups on the MS Active Directory server. To configure automatic mapping, please perform the following steps:

  a. Click **Automatic Mapping** and the following page pops up, as shown below:



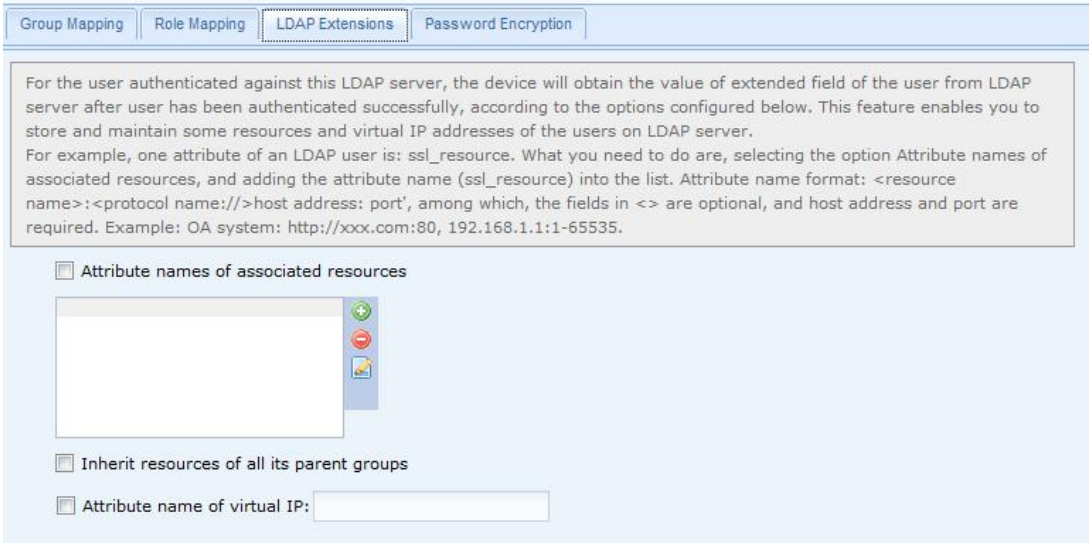
  b. Select the desired role mapping rules and click the **OK** and **Save** buttons. The two selected roles are then added to **Role Management** page, as shown below:



7. Configure **LDAP Extensions**.

LDAP Extensions are extended attributes of the users on LDAP server. This feature enables

some resources and virtual IP addresses of the users to be stored and maintained on the LDAP server.



The following are the contents included on the **LDAP Extensions** tab:

- **Attribute names of associated resources:** These are resource attributes according to which the LDAP users will be assigned some resources, after these LDAP users are authenticated successfully.

  To add a new attribute name of resource, click the **Add** icon . Then enter **Attribute Name** of the associated resource.

- **Inherit resources of all its parent groups:** Besides the resources with the specified attributes, all other resources (available to users in the specified OU and parent OUs of certain LDAP user) with the configured attributes will be displayed on **Resource** page and seen by the LDAP user once he or she logs in to the SSL VPN.

- **Attribute name of virtual IP:** Select this option and configure the attribute name of the virtual IP address of the users stored on the LDAP server. When an LDAP user logs in to the SSL VPN, the LDAP server returns the virtual IP address of this user to the Sangfor device.

  The option **Attribute names of associated resources** only applies to the LDAP users who do not have a corresponding account on the Sangfor device. For the LDAP users that already exist on the **User Management** page (under **SSL VPN** > **Users**), this option is invalid.

8. Configure **Password Encryption** tab.

   This feature enables user password to be encrypted before it is forwarded to LDAP server.



The following contents are included on above page:

- **Enabled:** Select it to enable password encryption feature.
- **Encryption Protocol:** Specifies encryption protocol. Options are **MD5** and **SHA1**.
- **Size:** Specifies the size of encryption key. It can be 32-bit or 16-bit.
- **Character Case:** Specifies character case of password.

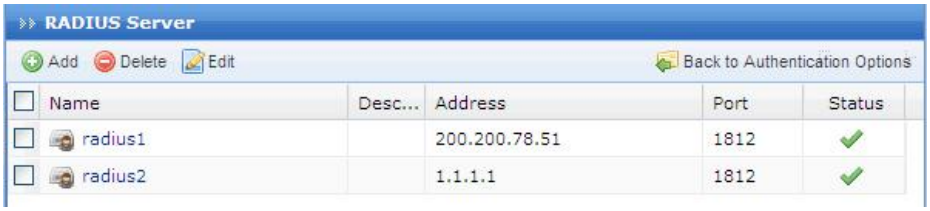
9. Click the **Save** button and then the **Apply** button to save and apply the settings.

RADIUS Authentication

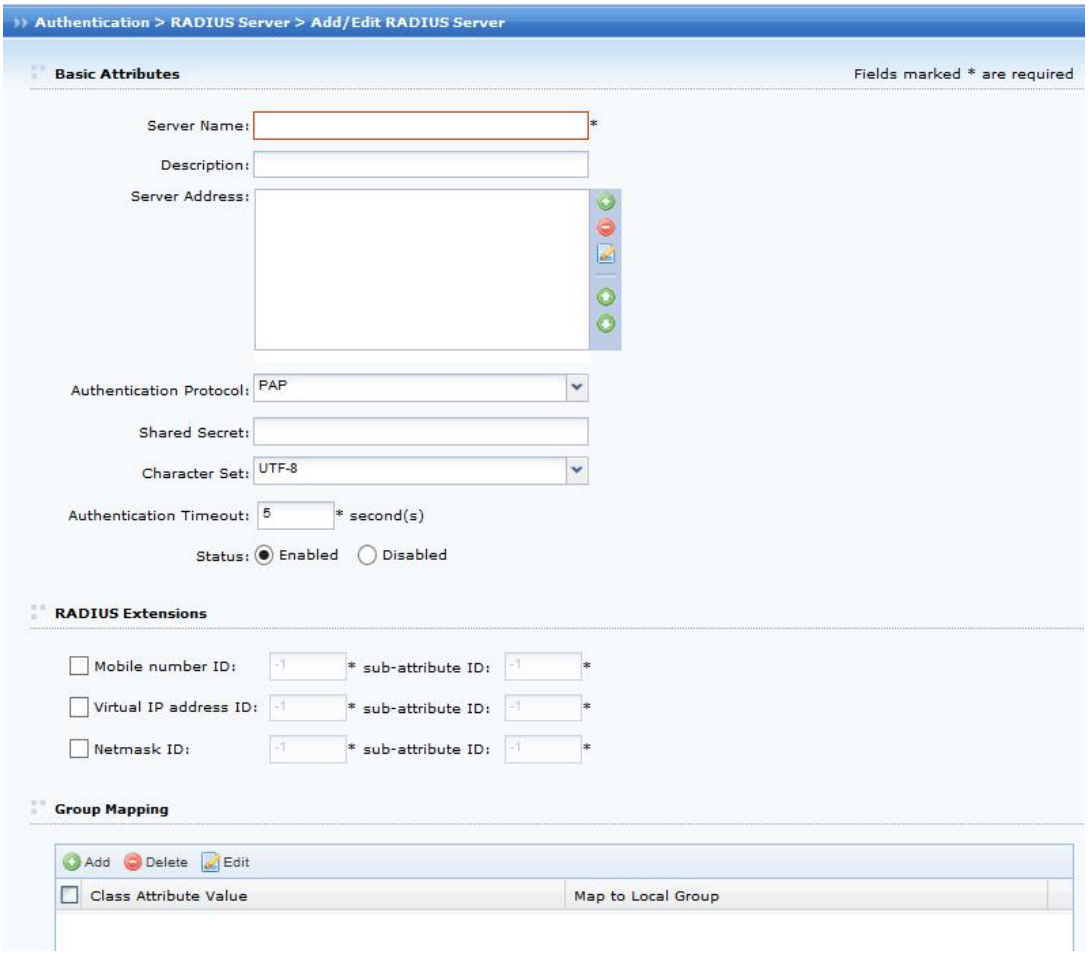
Sangfor device supports third-party RADIUS server to verify the users connecting the SSL VPN.

Configuring RADIUS Server

1. Navigate to **SSL VPN** > **Authentication** to enter **Authentication Options** page. Click the **Settings** button following **RADIUS** and **RADIUS Server** page appears, as shown below:



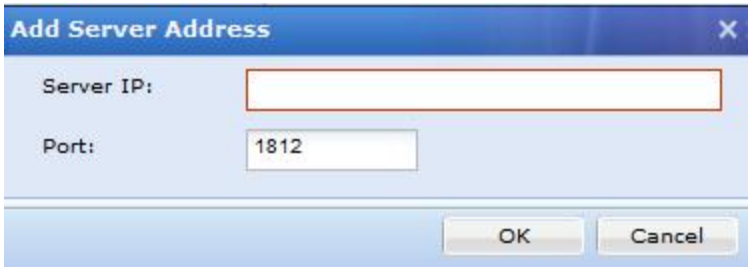
2. Click **Add** to enter the **Add/Edit RADIUS Server** page, as shown below:



3. Configure the **Basic Attributes** of the RADIUS server. The following are basic attributes:

   - **Server Name, Description:** Configures name and description of the RADIUS server.
   - **Server Address:** Configures the usable IP address and port of the RADIUS server. You can add multiple IP addresses and ports. Generally, only the first IP address/port is active and others are standby. If the first IP address/port is unavailable, the second IP address/port will take the place; if the second IP address/port is unavailable, the third IP address/port will take the place, and so on; if none of the configured server IP address/port is available, the server will be disconnected.

     To add a server address/port, click the **Add** icon next to **Server Address** field. The **Add Server Address** page is as shown in the figure below:



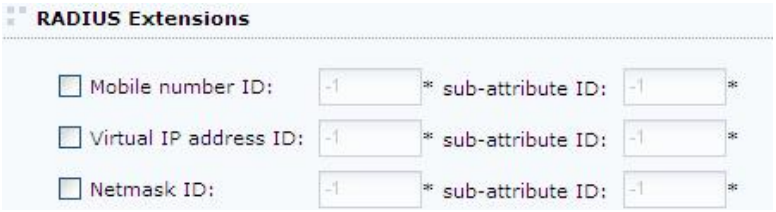
     To remove an entry, click the entry and click **Delete** icon next to **Server Address**.

     To edit an entry, click the entry and click **Edit** icon next to **Server Address**.

To adjust order of an entry, click the entry and click **Move Up** icon or **Move Down** icon .

- **Authentication Protocol:** Options are **PAP, CHAP, Microsoft CHAP, Microsoft CHAP2 and EAP-MD5.** Select the protocol as needed.
- **Shared Secret:** Configures the shared key used for RADIUS authentication.
- **Character Set:** Configures the character set used for RADIUS authentication.
- **Authentication Timeout:** Configures the time period that user authentication times out if RADIUS server gives no response.
- **Status:** Indicates whether the external RADIUS server is enabled.

4. Configure **RADIUS Extensions**, as shown below:



- **Mobile number ID:** Configures attribute ID and sub-attribute ID of the RADIUS user mobile number attribute. Once a RADIUS user logs in to the SSL VPN, the RADIUS server will return the attribute value to the Sangfor device.
- **Virtual IP address ID:** Configures the attribute ID and sub-attribute ID of RADIUS user's virtual IP address. When a RADIUS user logs in to the SSL VPN, the RADIUS server will return the attribute value to the Sangfor device.



- Mobile number ID only works in association with SMS authentication.

5. Configure **Group Mapping** rule.

The users with specified class attribute will be mapped to the corresponding group on the Sangfor device after successful login, and therefore have the same privilege as the users under the group to which they are mapped.



The following are the contents:

- **Add:** Click it to enter the **Add Group Mapping Rule** page and configure the two fields **Class** and **Map to Group**. The specified class attribute value on the RADIUS server will be mapped to the specified local group, as shown in the figure below:



- **Delete:** To delete a group mapping rule, select that rule and then click **Delete**.
- **Edit:** To edit a group mapping rule, select that rule and then click **Edit**.
- **If RADIUS user matches none of the above mapping rules, map the user to group:** For the users that match none of the group mapping rules, select this option and specify the local group to which the RADIUS users will be mapped automatically.

6. Click the **Save** button and then the **Apply** button to save and apply the settings.

Certificate/USB Key Based Authentication

Sangfor device not only supports built-in CA, but also supports external CA or more than one external CA, and can offer some certificate information. If Sangfor device is deployed in HQ, branch users can use certificate issued by different third-party CA for authentication when logging into SSL VPN. It increases flexibility of SSL VPN deployment. Certificates could be generated and configured through the **Certificate/USB Key Based Authentication** page.

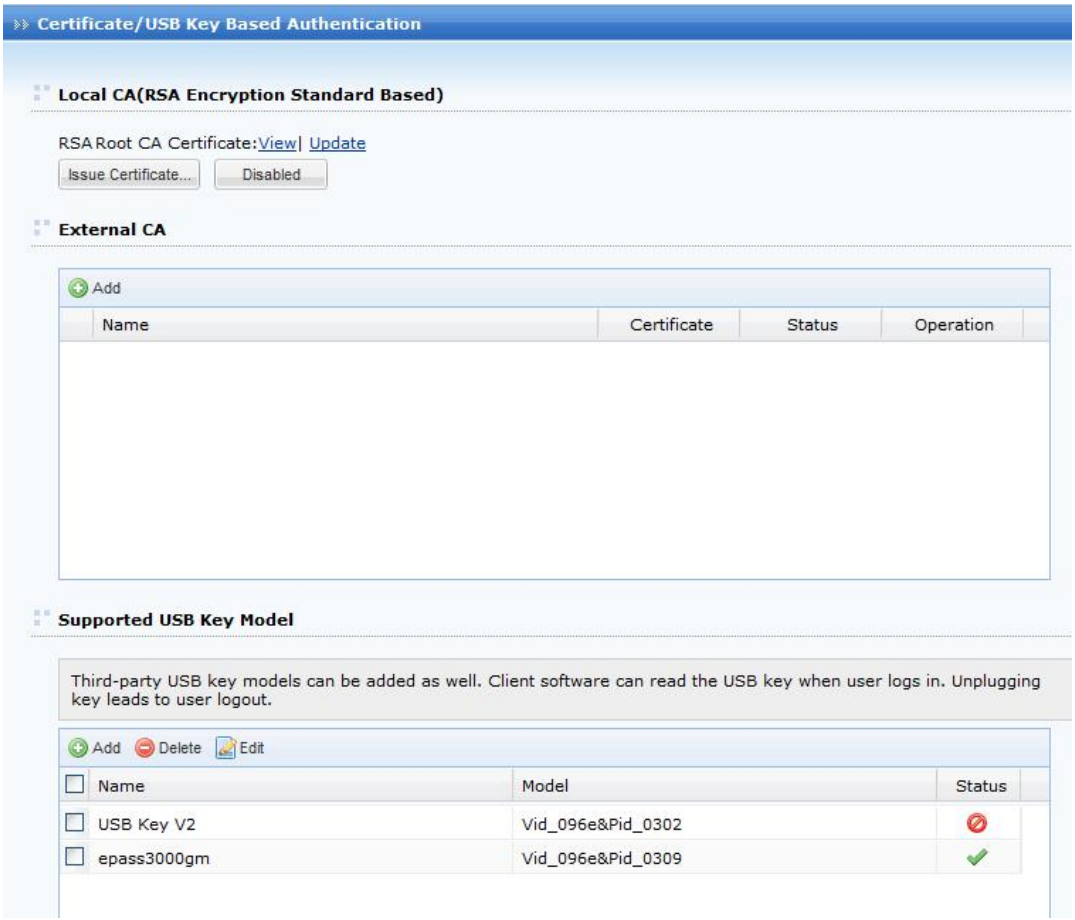
Navigate to **SSL VPN** > **Authentication** to enter the **Authentication Options** page.



To download and install USB key driver manually, click **USB Key Driver**.

To download and install USB key tool manually, click **USB Key Tool.**

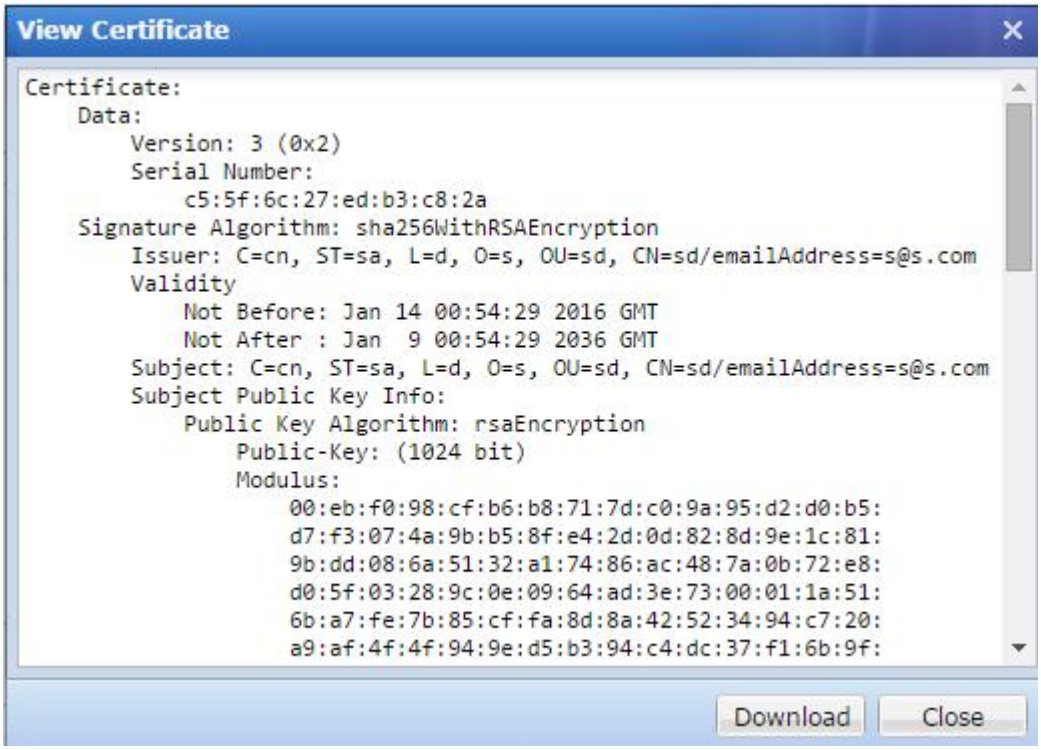
Click the **Settings** button following **Certificate/USB Key** and the **Certificate/USB Key Based Authentication** page appears, as shown in the figure below:



Configuring Local CA

The following contents are under **Local CA** section:

- **View:** Click it to view root certificate of local CA, as shown below:



- **Update**: Click it to update root certificate, as shown in the figure below:



When **RSA Encryption Standard** is selected in Key Encryption field, key size can be 1024, 2048 or 4096, while **SM2 Encryption Standard** is selected, key size can be 256 only. Configure all the required fields above and then click **Finish** to save the setting, and then a root certificate will be created, and it will be also taken as device certificate.

- Country must be a two-letter abbreviation of country, for example, CN indicates China.
- Email address should not contain any full-angle characters.

- **Issue Certificate:** Click it to enter the **Issue a Certificate** page. The issued certificate can be used as user certificate or a server certificate.

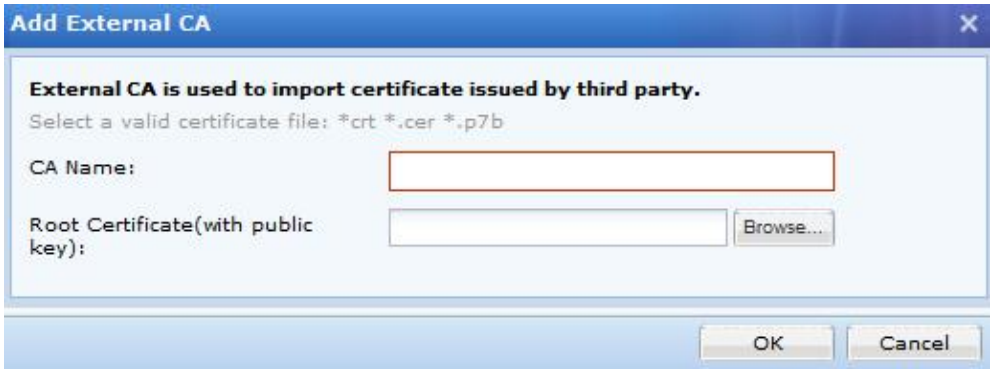


To generate the certificate, configure all the fields and click **OK** to save the changes.

Configuring External CA

The following contents are under **External CA** section.

- **Add:** Click it to enter the **Add External CA** page, as shown below:

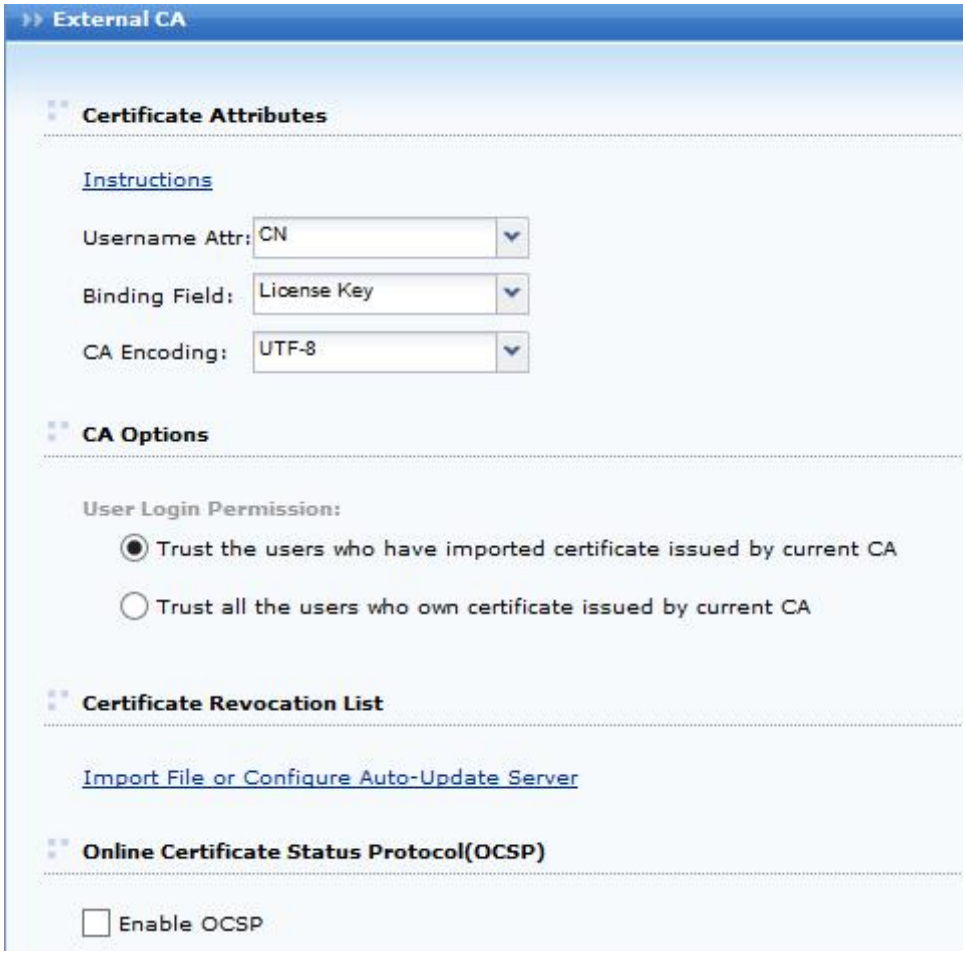


Specify the CA name and select a root certificate from local PC. Click **OK** to save the changes. Then you will see the newly-imported external CA, as shown in the figure below:



A maximum of seven external CA is supported.

Click on the **External CA** in **Name** column. You will see the following page:



The following information are included on above page:

- **Username Attr:** Indicates the field used to store username in certificate issued by this CA. The username will be displayed on the homepage of client. Options are **CN**, **Email Prefix** and **OID**.
- **Binding Field:** Indicates the certificate field binding to a user. It takes effect when current certificate is imported into Sangfor device.
  - **License Key:** If it is selected, CA will issue a new certificate when the certificate gets expired. As the license key of new certificate has changed, user needs to imports this new certificate on **Local Users** page.
  - **CN:** If it is selected, user does not need to import new certificate when user certificate is updated. Before selecting this option, user needs to make sure the DN of each certificate is different.
  - **OID:** It is similar with DN. Generally, user also needs to specify OID attribute for storing username.
  - **CA Encoding**: Indicates the encoding used by this certificate.
  - **CA Options:** It determines whether the users are trusted if they own certificate issued by the current external CA, that is to say, whether they are allowed to log in to the SSL VPN.

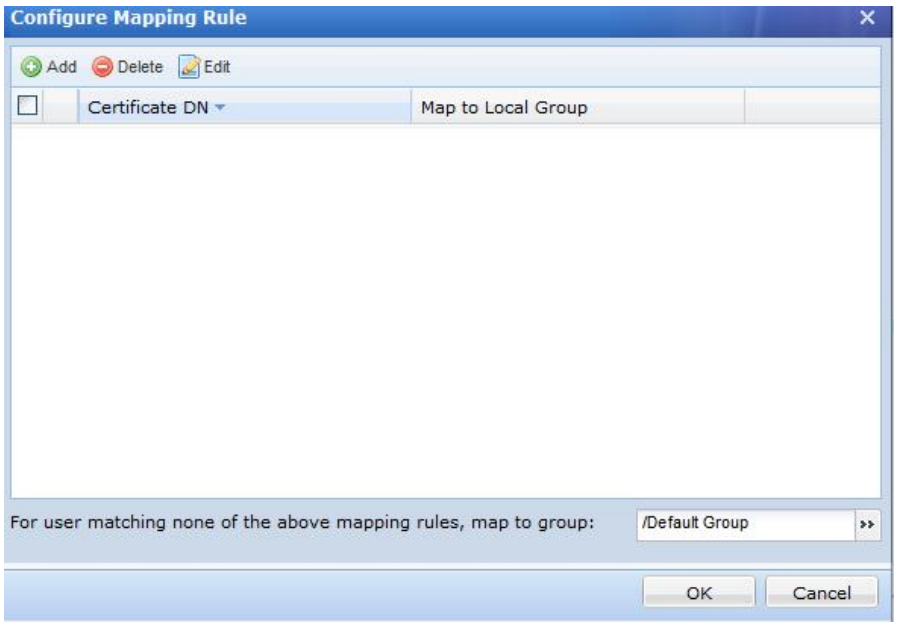


If **Trust the users who have imported certificate issued by current** is selected, only after the users certificates have been imported to the Sangfor device can they use their own certificates to log in to the SSL VPN.

If **Trust all the users who own certificate issued by current CA** is selected, all the users who own valid certificates issued the current external CA will be able to log in to the SSL VPN with their own certificates.



Click on the link **Configure Mapping Rule** to enter the **Configure Mapping Rule** page, as shown in the figure below:

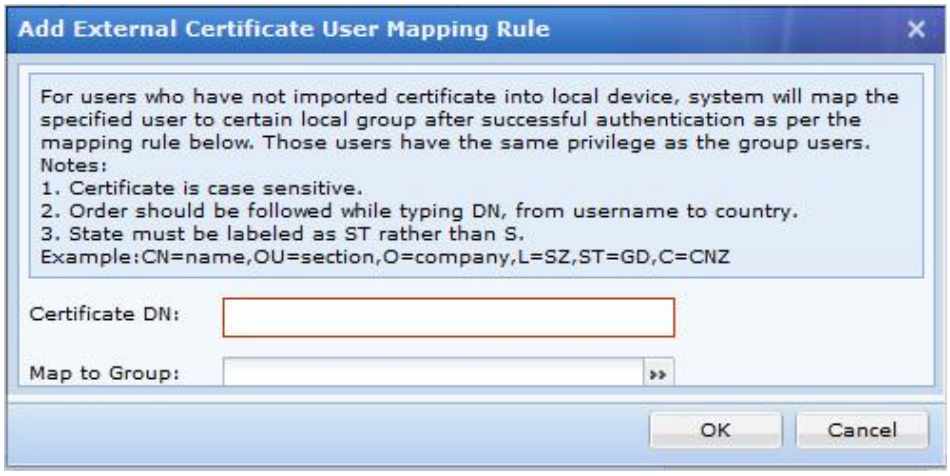


Configure the **Mapping Rule** that can map the certificate users of certain certificate DN to a group on the Sangfor device, so that they will have the same privilege as others under the target group.

To delete a mapping rule, select the rule and click **Delete**.

To edit a mapping rule, select the rule and click **Edit**.

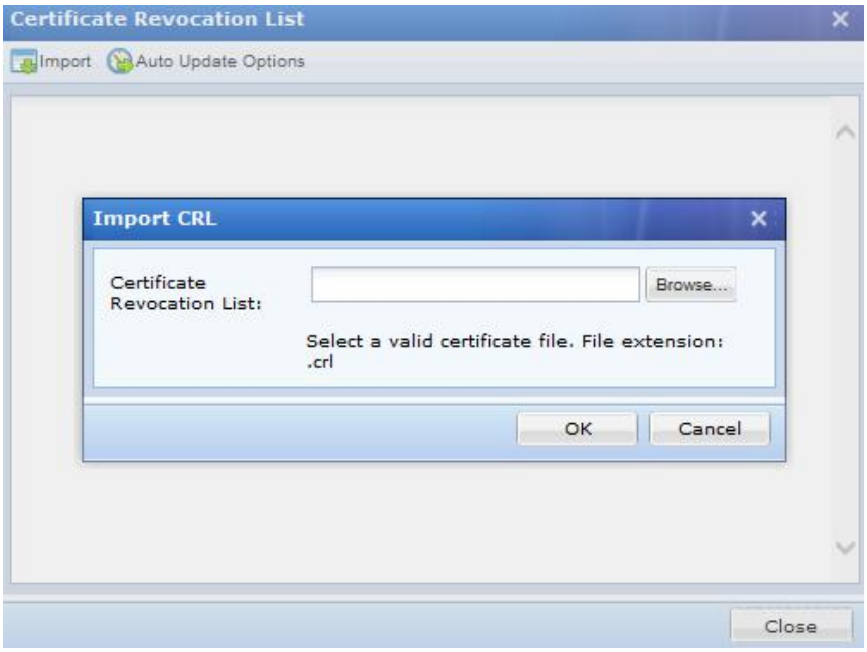
To add a new mapping rule, click **Add** and the **Add External Certificate User Mapping Rule** page appears, as shown below:



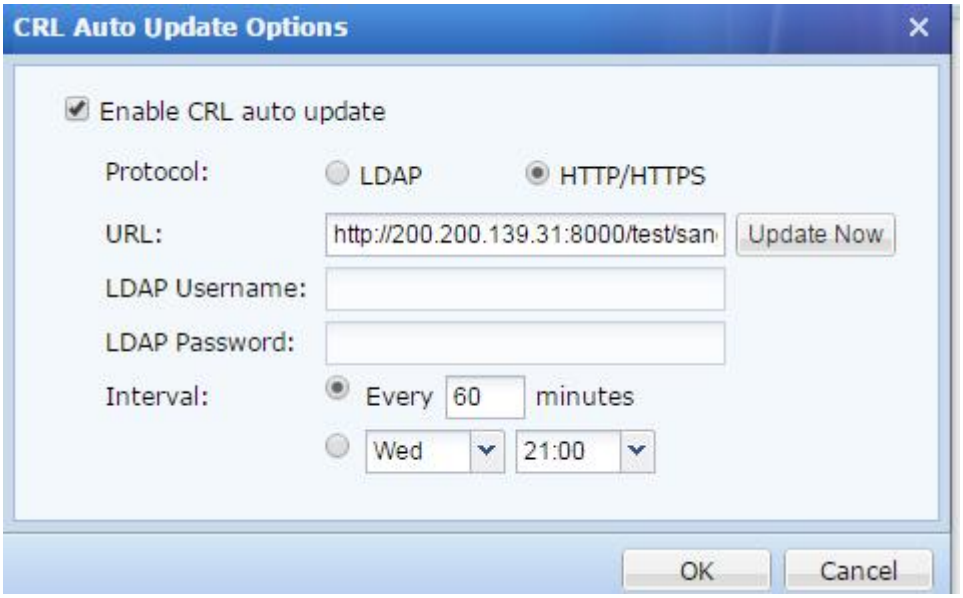
- **Certificate DN:** Configures DN of certificate, which can be referred to in certificate subject.
- **Map to Group:** Configures the local group to which the certificate users will be mapped if their certificates have the configured DN.
- **For user matching none of the above group mapping rules, map the user to group:** Configures the local group to which the certificate users will be mapped automatically if they match none of the mapping rules.



- **Certificate Revocation List (CRL):** Click the link **Import File or Configure Auto-Update Server** to import certificate or enable auto-update, as shown below:



To have the CRL updated automatically and regularly, click the **Auto Update Options** link and configure the fields on the **Auto Update Options** page, as shown in the figure below:



Configure **Online Certificate Status Protocol(OCSP)**. This part includes options related to OCSP that supports online check of certificate validity, as shown in the figure below:



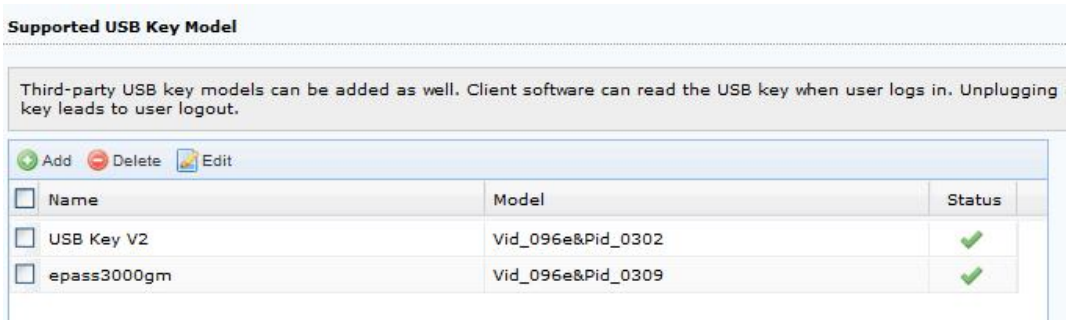
The contents under **Online Certificate Status Protocol(OCSP)** are as follows:

- **Enable OCSP:** Select this option and OCSP will be enabled and related options will appear.
- **Server Address, Server Port:** Configure the address and port of OCSP server that provides OCSP service.
- **Authentication required:** Select this option and the OCSP server will verify identity of the Sangfor device.
- **Test Connectivity:** Click it to check whether the Sangfor device can connect to the OCSP server.

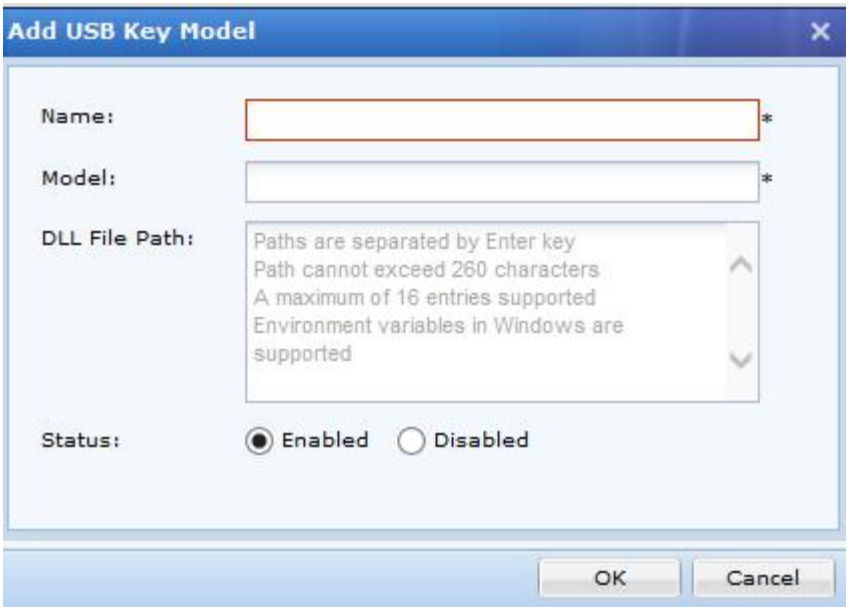
Configuring USB Key Model

Under **Supported USB Key Model**, configure the model of third-party USB keys that can be identified by the Sangfor device while USB key of this model is plugged in to the end user's PC. Unplugging key will lead to automatic logout.

The contents under this part are as shown below:



To add a new USB key model, click **Add** to enter **Add USB Key** page, as shown below:



The following are the contents included on **Add USB Key** page:

- **Name:** Specifies name of this USB key model.
- **Model:** Specifies the model of USB key that supports automatic logout while end user unplugs the USB key.
- **DLL File Path:** Specifies the path of DLL file that is used to provide interface for SM2 encryption function. It is required when adding third-party USB key supporting SM2 encryption algorithm.
- **Status:** Configures whether this model of USB key is enabled or not, that is, whether to enable the feature of automatic logout while end user unplugs the USB key of this model.

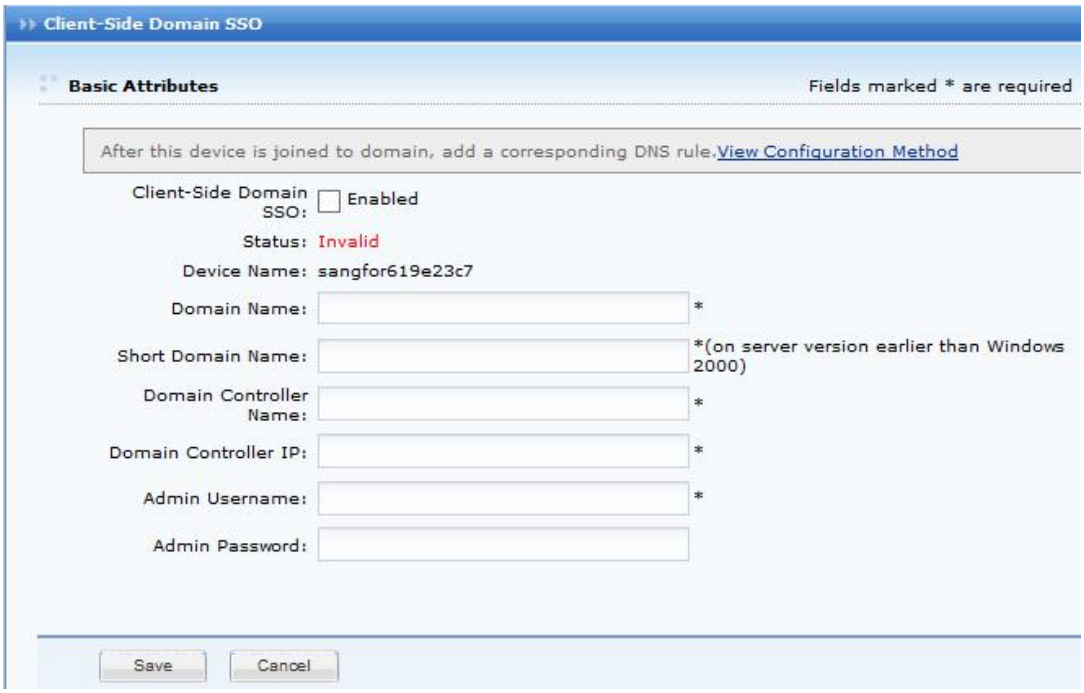
To remove an entry from the list, select the entry and click **Delete**.

To edit an entry, select the entry and click **Edit**.

Client-Side Domain SSO

Client-side domain SSO can achieve that when users logs in using VPN client, user does not need to type username and password and domain SSO will be performed automatically after client-side PC is joined AD domain. This feature is not applicable to user logging using Portal.

1. Navigate to **SSL VPN** > **Authentication** to enter **Authentication Options** page. Click the **Settings** button following **Client-Side Domain SSO** and **Client-Side Domain SSO** page appears, as shown below:



2. Configure **Basic Attributes** on above page:

- **Enabled**: Click it to enable client-side domain SSO feature.
- **Status:** Indicates whether this feature takes effect.
- **Device Name:** Indicates name of Sangfor device.
- **Domain Name:** Specifies the domain name of domain server
- **Short Domain Name:** Specifies the abbreviation of the domain name
- **Domain Controller Name: S**pecifies the name of domain controller in Window domain.
- **Domain Controller IP:** Specifies the IP address of the domain controller in Window domain.
- **Admin Username, Admin Password:** Specifies the administrator username and password used to log in to Window domain.

Secondary Authentication Methods

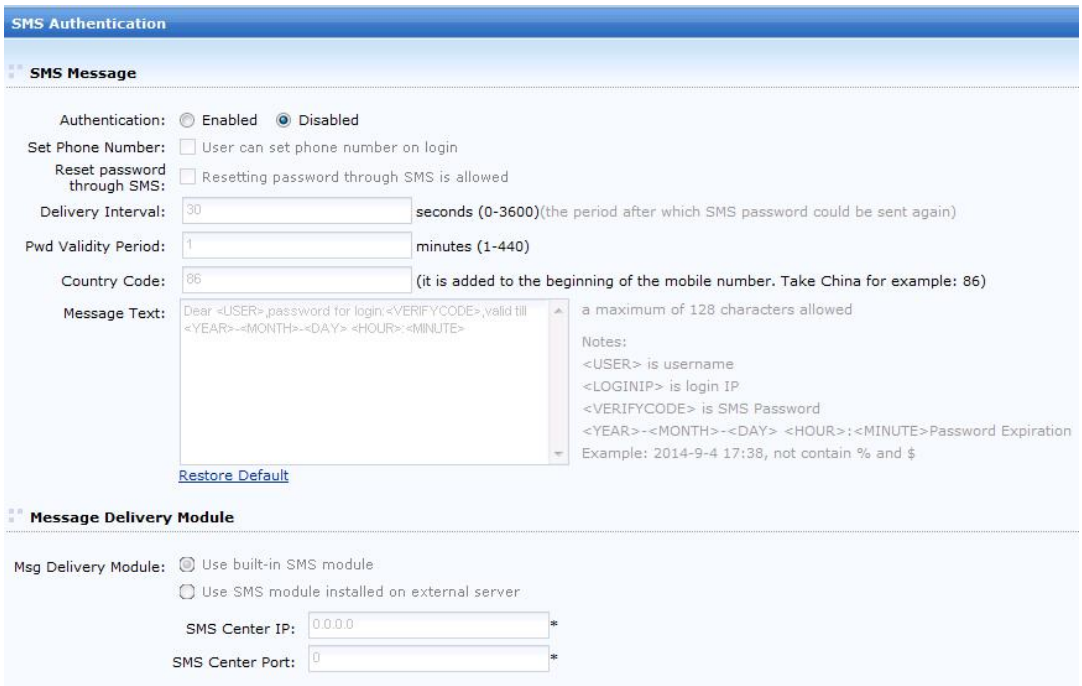
There are three secondary authentication methods, namely, **SMS** authentication, **Dynamic Token** based authentication and **Hardware ID** based authentication.

SMS Authentication

SMS authentication is a type of authentication method that requires connecting user to enter the received SMS password when he/she is logging in to and has passed the primary authentication(s).

The SMS password is a password dynamically generated and sent to the mobile phone of connecting user. Only after user enters and submits the SMS password can he/she access SSL VPN and the internal resources.

Navigate to **SSL VPN** > **Authentication** to enter the **Authentication Options** page. Click the **Settings** button following **SMS** and the **SMS Authentication** page appears, as shown below:



In case that the SMS license is invalid or has not been activated, tips show up under the subtitle **SMS Message**, saying "SMS authentication license key is invalid. Please *click here* to activate the license". To modify or activate the SMS license, click the **click here** link to enter **Licensing** page.

As shown on the above page, there are three sections related to SMS authentication, namely, **SMS Message**, **Message Delivery Module** and **Message Delivery Parameters**.

The following are the contents on **SMS Authentication** page:

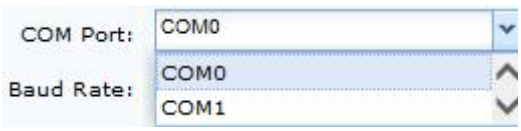
- **Authentication:** Indicates whether SMS authentication is enabled or not. Options are

Enabled and **Disabled**.

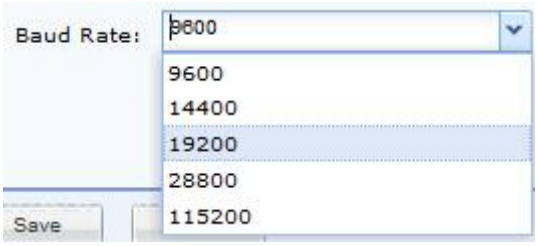
- **Set Phone Number**: If the option **User can set phone number on login** is selected, user can specify mobile phone number on login page. When adding user, administrator does not need to specify mobile phone number if **SMS password** is selected as secondary authentication. Then, user could specify mobile phone number to receive OTP. After successful authentication, the mobile phone number will be bound with the user account.
- **Reset password through SMS:** To enable users to reset password through SMS, select the option **Resetting password through SMS is allowed.**
- **Delivery Interval:** Specifies the interval for resending a SMS message.
- **Pwd Validity Period:** Configures the validity period of the SMS password. If user fails to enter and submit the SMS password within the time since the SMS password is sent, the SMS password will get invalid. Login with invalid SMS password will lead to login failure. The validity period should be between 1 and 1440 minutes.
- **Message Text:** Customizes the text of the SMS message that is to be sent to the end user.
- **Restore Default:** Click this link and the system default text will replace the current message text.
- **Message Delivery Mode:** There are two types of modules, built-in SMS module and SMS module installed on external server. Select either option and configure the other required fields.
- **Gateway Type:** Specifies the ways of delivering SMS messages. There are seven types of gateway, GSM modem, SANGFOR CDMA modem, CNMA modem, China Mobile V2, China Mobile V3, China Unicom, China Telecom V3, HTTP, Jasson MAS(WebService port). You can use **GSM modem** (connected to the server's COM port) or using **gateway** (such as China Mobile V2/V3, China Unicom and China Telecom V3, gateways usually used by enterprises) to send SMS messages.



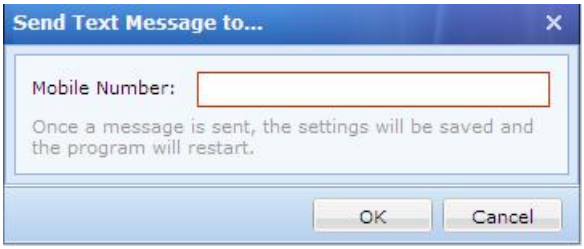
- **SMS Center:** Indicates the SMSC number of corresponding ISP.
- **COM Port:** Indicates the COM port used to connect to SMS modem. Options are **COM1** and **COM2**.



- Baud Rate: Specifies the baud rate of the specified COM port of Sangfor device. Default is 9600.



- **Send Test SMS Message:** Click this link to check whether SMS message can be sent to end user successfully through the configured GSM modem or gateway. A **Send Text Message to…** page will pop up asking for mobile number, as shown in the figure below:



Using Built-in SMS Module to Send SMS Message

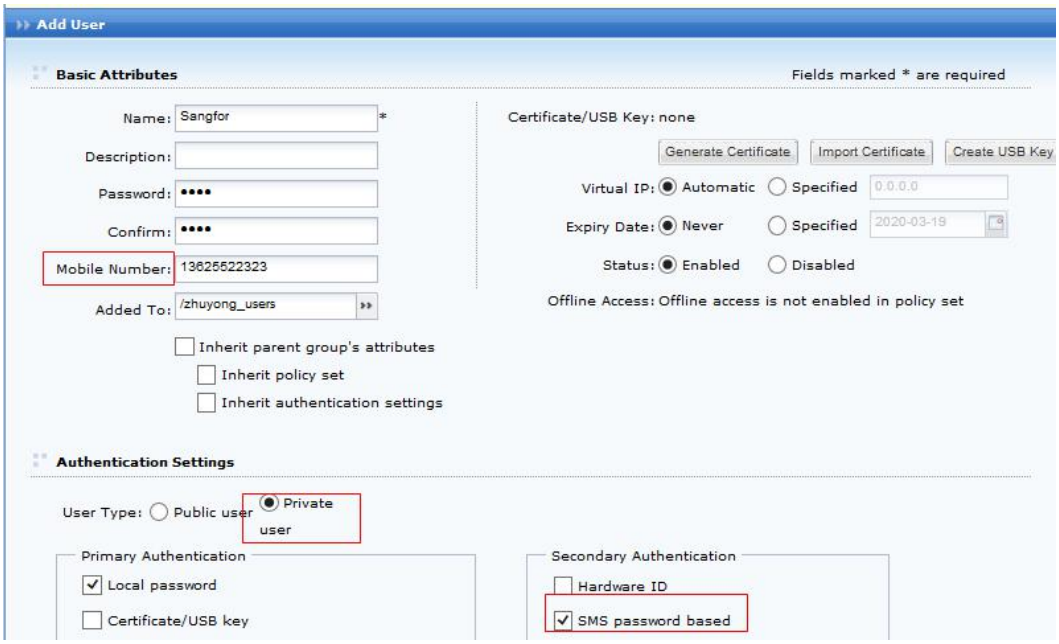
The so-called built-in SMS module indicates the module built in the Sangfor device.

To use GSM modem as the way to deliver SMS message, prepare a GSM modem and an IC telephone card, and then perform the steps below:

1. Insert the SIM card of a cellular phone into the GSM modem.
2. Use the serial cable (one end is male connector and the other end is female connector; attachment of Sangfor device when product is delivered) to connect the GSM modem to the **CONSOLE** interface on the rear panel of the Sangfor device. Please screw the plug/jack in until they are tightly attached.
3. On the **SMS Authentication** page, select gateway type **GSM modem**.
4. Enter the SMSC number of the local ISP into the **SMS Center** field. For example, if you are in Shenzhen, enter the number 8613800755500.
5. Select COM0 as the **COM Port**.
6. Configure **Baud Rate** (of the serial port) for communication between the Sangfor device and the GSM modem. It is 9600 by default. Change this value to keep it relevant to the GSM modem being used.
7. Click the **Save** button to save the settings. The configured fields are as shown below:



8. Go to **SSL VPN > Users > local Users** page to add or edit user. Configure the mobile number, select user type **Private user**, and select secondary authentication **SMS password**, as shown in the figure below:



9. End user logs in to the SSL VPN. After passing the primary authentication, user will be asked for SMS password, as shown in the figure below:



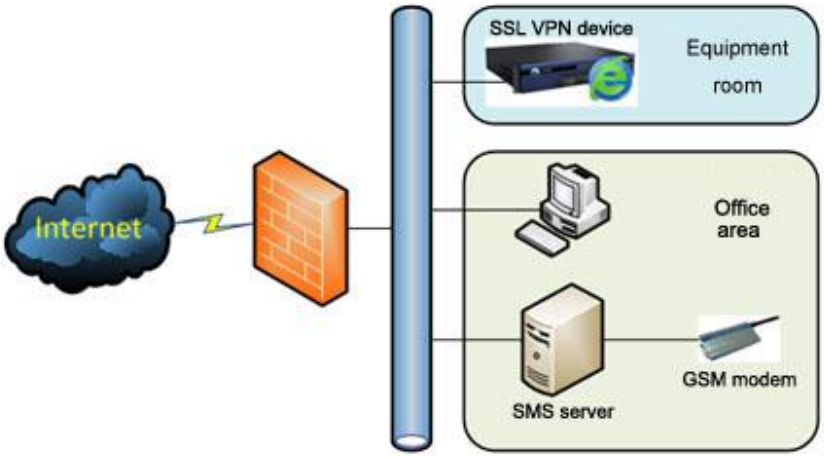
10. Enter the received SMS password, and click the **Submit** button. If user fails to receive the text message for a long time, he/she can click **get again** to get a new SMS password.

Using External SMS Module to Send SMS Message

This type of module is installed on an external server, through which the SMS messages are sent.

To use GSM modem as the way to deliver SMS message, prepare a GSM modem and a computer (SMS server) that has COM port and has installed the SMS software provided by SANGFOR. What should be noted is that they may not work if the facilities are placed in a machine room where electromagnetic shielding measures may be taken.

Network deployment is as shown in the figure below:



1. Insert the SIM card of a cellular phone into the GSM modem.
2. Use the serial cable (one end is male connector and the other end is female connector; attachment of Sangfor device when product is delivered) to connect the GSM modem to the **COM** port of SMS server. Please screw the plug/jack in until they are tightly attached.
3. On the SMS server, install the SMS software package provided by SANGFOR.

   Once installed, the software will run automatically as a system service. The process **SMSSP.exe** can be checked through **Windows Task Manager**.

   For the running status of SMS service, see the SMS service icon on the task bar, as shown in the two figures below. The figure on the left shows normal running status, while the figure on the right shows service error.



   If the software is installed on other drive rather than system drive C, the service might still refuse to work. In that case, uninstall the SMS software and reinstall it on the default drive.
4. Go to **Start** > **SmsService** to open the console or right-click the icon and select **Config**, and configure SMS service software.

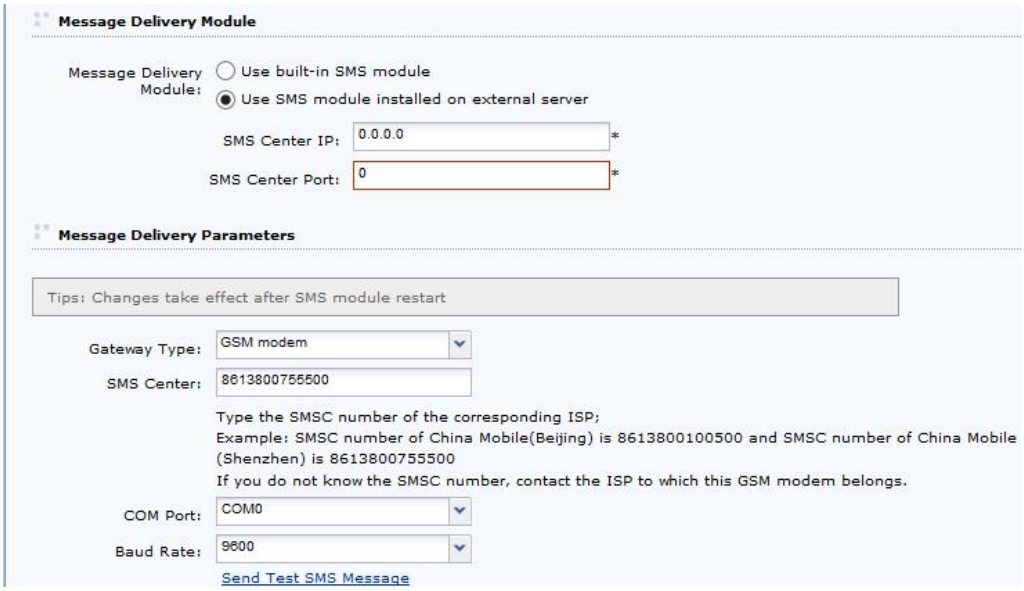


What needs to be configured for the SMS service is the listening port (TCP port). Make sure the configured listening port is not providing other services. To check if port conflict exists, use the command **netstat –na** to check all other listening ports used by this server.

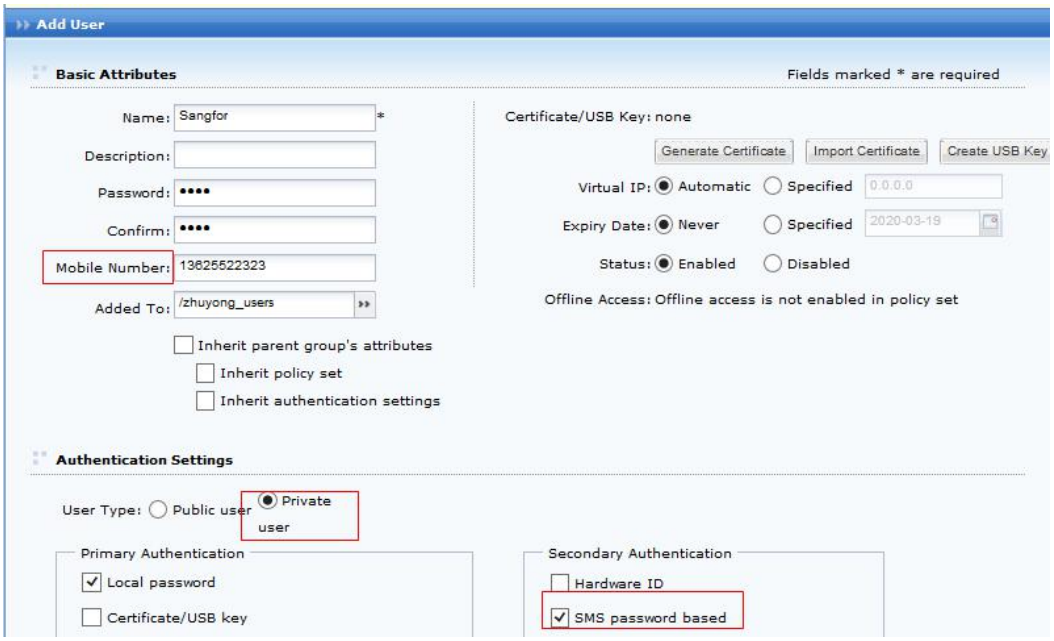
If the SMS server has installed firewall software, make sure that the firewall allows data transmission on the listening port.

5. Log in to the administrator console of the Sangfor device and navigate to **SSL VPN** > **Authentication** > **SMS Authentication** to configure SMS authentication.

   - **SMS Center IP:** Enter the IP address of the SMS server into the field. Make sure the Sangfor device and SMS server can communicate with each other, that is, the Sangfor device is connected to the SMS server.
   - **SMS Center Port:** Enter the listening port that has been configured for the SMS software.
   - **Gateway Type:** Select the option **GSM modem**.
   - **SMS Center:** Enter the SMSC number of the SIM card that has been inserted into the GSM modem. If the SMSC number of the SIM card is unknown, ask your ISP for that.
   - **COM Port:** Select the port being used to provide SMS service. If there is only one COM port, choose **COM0**; if there are two COM ports and the SMS modem is connecting to the second COM port, choose **COM1**.
   - **Baud Rate:** Select the default value **9600**. The configured fields are as shown below:



6. Add or edit user. Configure the mobile number, select user type **Private user**, and select secondary authentication **SMS password**, as shown in the figure below:



7. End user logs in to the SSL VPN. After passing the primary authentication, user will be asked to enter the received SMS password, as shown in the figure below:



8. Enter the received SMS password, and click the **Submit** button. If user fails to receive the

text message for a long time, he/she can click **get again** to get a new SMS password.

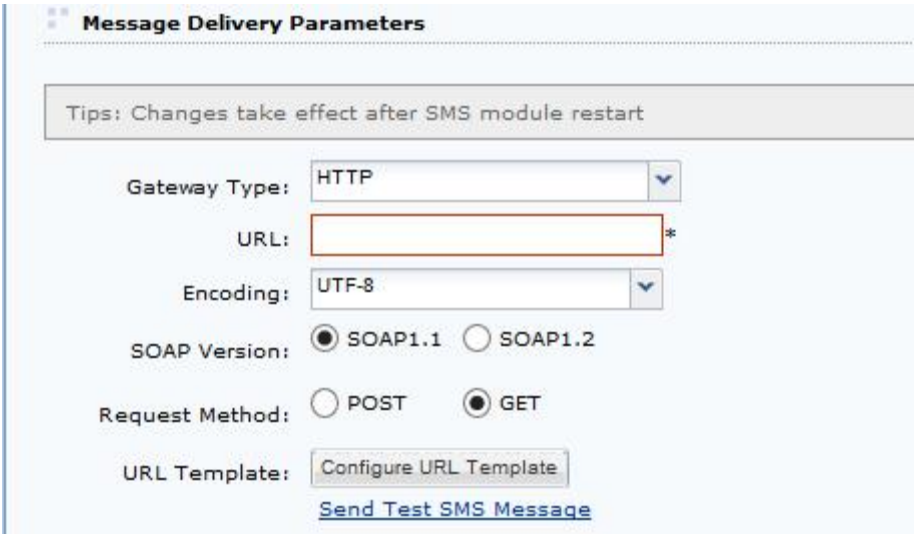
Using SMS Gateway of ISP to Send SMS Message

If the enterprise network is already deployed with SMS gateway of ISP, such as China Mobile, China Unicom, no other facility is needed except the Sangfor device. Configure the following:

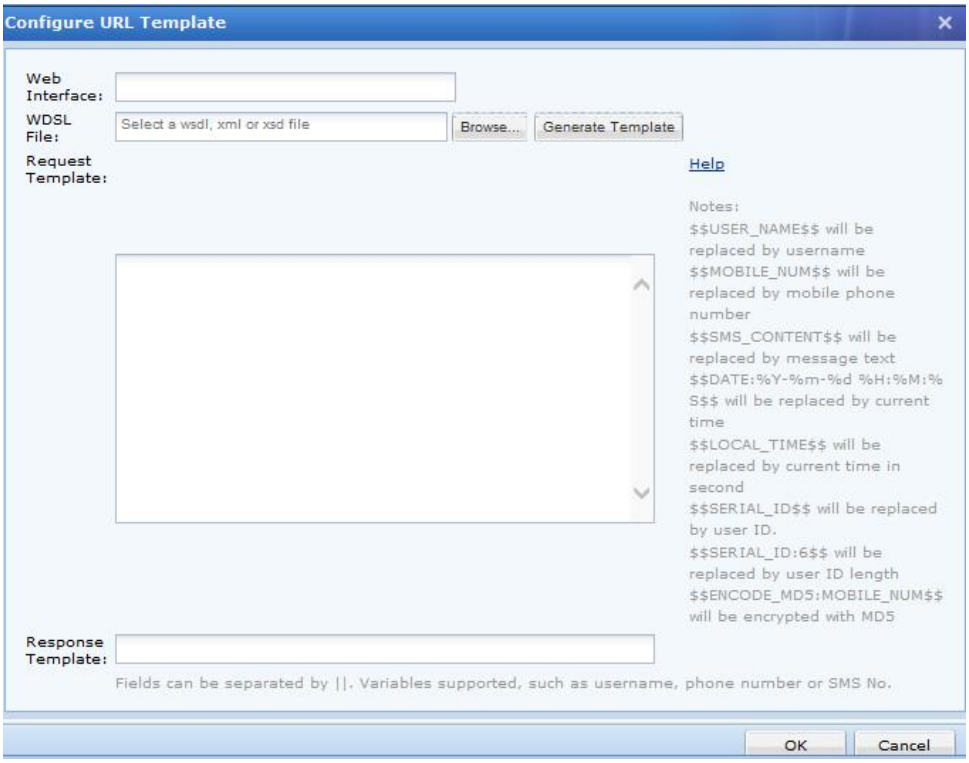
- **Gateway Type:** Select a gateway type that is available to the enterprise network.
- **SMS Center IP:** If the message delivery module is installed on an external server, enter the IP address of the server on which the SMS module is installed.
- **SMS Center Port:** Enter the port number being used to listen to SMS service.
- **Message Delivery Parameters:** Configure the required fields according to the information provided by the corresponding ISP.

Using Webservice Based SMS Platform to Send SMS Message

Sangfor device can communicate with Webservice-based SMS platform for sending SMS message to end users, enhancing the stability. Navigate to **SSL VPN > Authentication > SMS Authentication** page and select HTTP as **Gateway Type**. Configure the required fields, URL of webservice-based SMS platform, SOAP version, request mode and URL template.



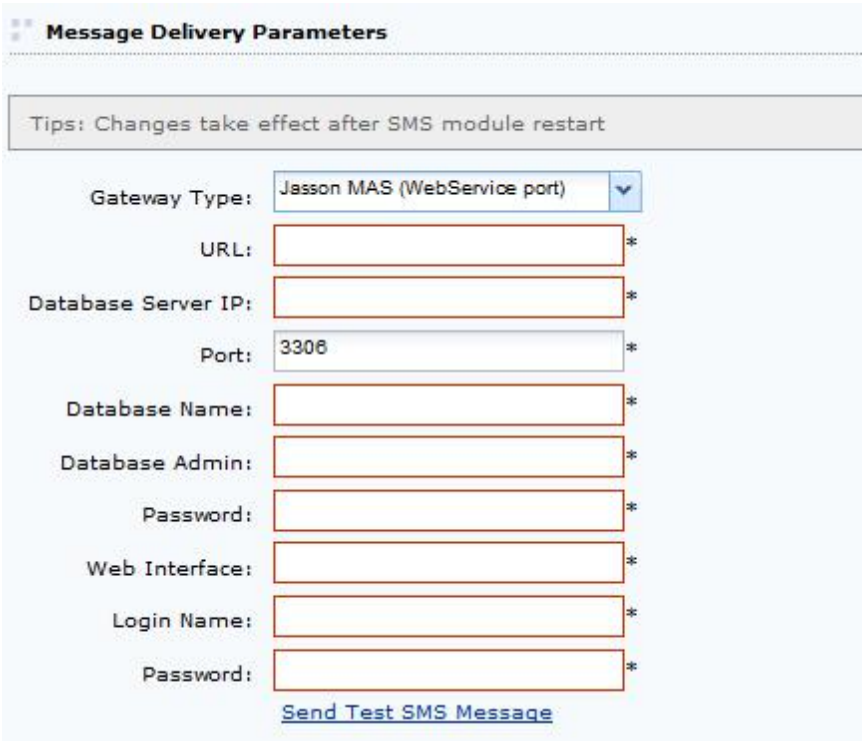
Click the link **Configure URL Template** to enter the **Configure URL Template** page, as shown below:



Configure the fields on above page and click **OK** to save the changes.

Using Jasson MAS to Send SMS Message

Sangfor device can use Jasson MAS for sending SMS message so as to enhance stability.



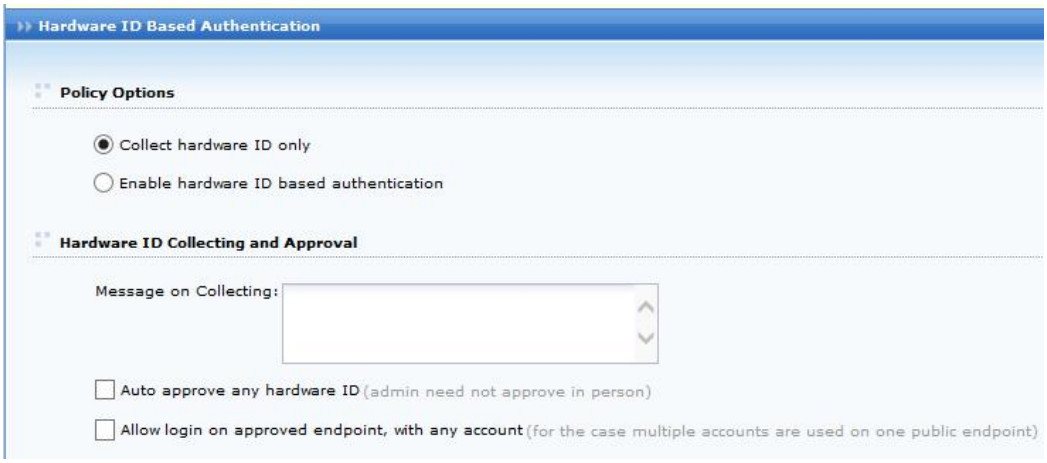
Configure the following contents included on above page:

- **URL:** Enter the URL of Jasson MAS.
- **Database Server IP:** Enter the IP address of database server on Jasson MAS.
- **Port:** Enter the database port according to your case. Default value is 3306.
- **Database Name:** Enter the name of database server on Jasson MAS. You need to confirm with the network administrator that the database name you entered is correct.
- **Database Admin, Password:** Enter the username and password of internal database on MAS. If you do not know the username or password, contact with the network administrator.
- **Web Interface:** Enter the interface of Jasson MAS used to send SMS message.
- **Login Name, Password:** Specifies username and password to log in Jasson MAS.

Hardware ID Based Authentication

Hardware ID is a unique serial number generated using the extracted features of hardware components in a computer, according to certain algorithm. The uniqueness of computer components makes the generated hardware ID unique.

Navigate to **SSL VPN** > **Authentication** to enter the **Authentication Options** page. Click the **Settings** button following **Hardware ID** and the **Hardware ID Based Authentication** page appears, as shown in the figure below:



The following are the contents included on **Hardware ID Based Authentication** page:

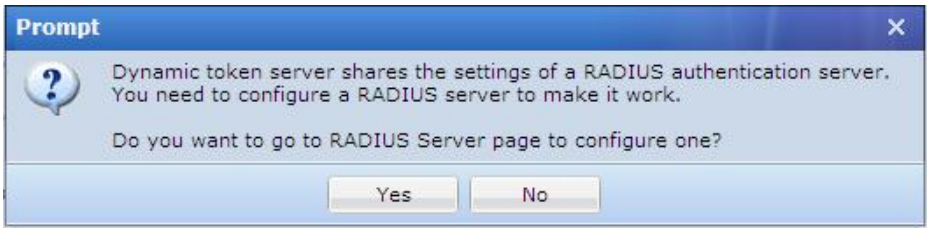
- **Collect hardware ID only:** If this option is selected, hardware IDs of endpoint computers will be collected, but hardware ID based authentication will not be enabled.
- **Enable hardware ID based authentication:** If this option is selected, hardware ID of endpoint computers will be collected and hardware ID based authentication enabled.
- **Message on Collecting:** This will turn out to be a prompt seen by end users when they go through hardware ID based authentication.

- **Auto approve any hardware ID:** Indicates that any hardware ID submitted by end user will be approved, and administrator need not approve them manually.
- **Allow login on approved endpoint, with any account:** Indicates that hardware IDs submitted by any user from certain endpoint(s) will be approved automatically if administrator has ever approved the hardware ID of the endpoint(s).
- **Save:** Click this button to save the settings when configuration is completed.

Dynamic Token Based Authentication

Dynamic token based authentication is an extension of RADIUS authentication, using a RADIUS server to distribute passcode to connecting user when they go through dynamic token based authentication. Dynamic token based authentication is a secondary authentication and can add security to SSL VPN access.

Navigate to **SSL VPN** > **Authentication** to enter the **Authentication Options** page. Click the **Settings** button following **Dynamic Token** and the following prompt appears:



To go to **RADIUS Server** page to configure RADIUS server, click the **Yes** button. For procedures of configuring RADIUS server, please refer to the RADIUS Authentication section in Chapter 4.

Other Authentication Options

This section includes configurations of **Priority of LDAP/RADIUS Servers, Password Security Options** related to password and brute-force login prevention, and **Anonymous Login** related settings.

Priority of LDAP and RADIUS Servers

If there are more than one LDAP servers or RADIUS servers available for user authentication, it becomes necessary to consider choosing an LDAP or RADIUS server as the first server from which the matching account will be searched for when user is connecting to SSL VPN and going through LDAP/RADIUS authentication.

Administrator can adjust the order (priority) of the available external LDAP/RADIUS servers on the **Sort External Authentication Servers** page.

Navigate to **SSL VPN** > **Authentication** to enter the **Authentication Options** page. Click the **Settings** button following **Priority of LDAP/RADIUS Servers** and the **Sort External Authentication Servers** page appears, as shown in the figure below:



Since the order indicates priority, the external authentication server sitting at the top of the list has the highest priority. User will go through this server first to find the matching account while connecting to SSL VPN.

If the connecting user is not found on the first external authentication server, the matching process will not stop. User will then go through the second (or third, or fourth) external authentication server until the right user account is matched. If no account is matched eventually, user authentication will fail.

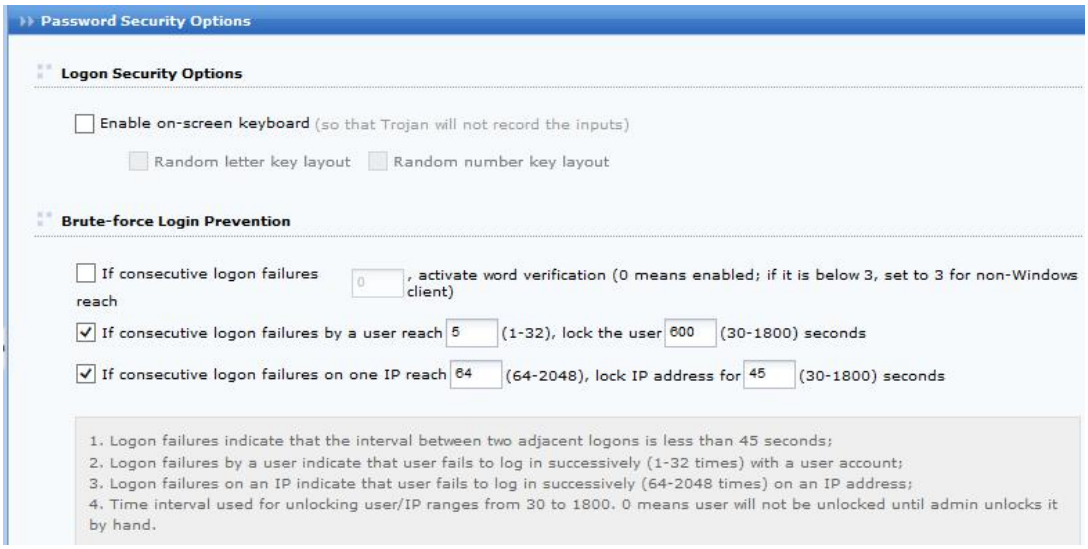
To adjust order of an external authentication server, select the server and click **Move to Top**, **Move Up**, **Move Down** or **Move to Bottom**.

When configuration is completed, click the **Save** button to save the changes.

Password Security Options

Password security options are settings related to login when user submits username and password to access the SSL VPN, including two parts, **Logon Security Options** and **Brute-force Login Prevention**.

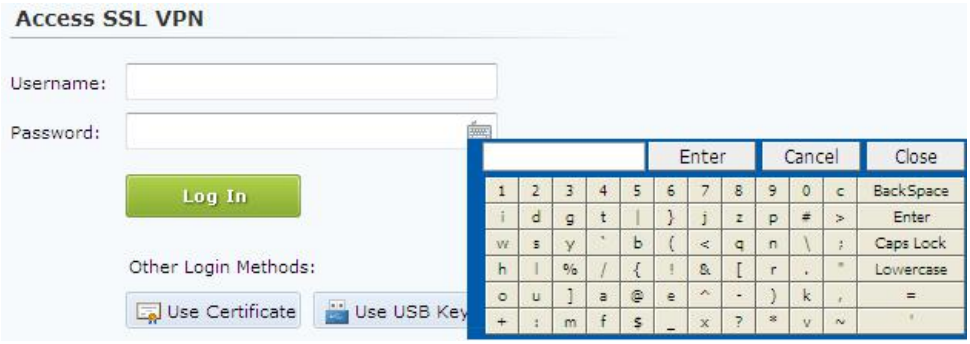
Navigate to **SSL VPN** > **Authentication** to enter the **Authentication Options** page. Click the **Settings** button following **Password Security Options** and the **Password Security Options** page appears, as shown in the figure below:



The following are the contents included on the **Password Security Options** page:

- **Enable on-screen keyboard:** On-screen keyboard is a virtual keyboard available on the login page to the SSL VPN and can prevent input disclosure, adding security to SSL VPN access. The other two options **Random letter key layout** and **Random number key layout** can have the letter keys and number keys on the virtual keyboard change positions randomly every time user uses this keyboard.

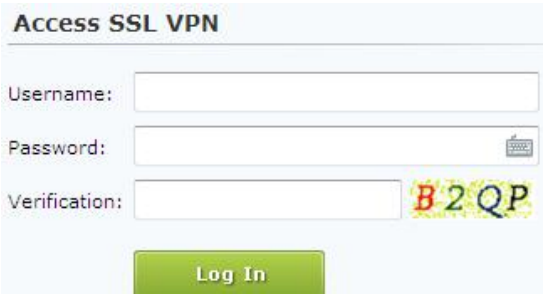
  When user logs in to the SSL VPN and wants to call the on-screen keyboard, he or she needs only to click the keyboard icon next to the **Password** field on the login page, as shown in the figure below:



- **Brute-force Login Prevention:** This security feature enables the system to take actions to stop brute-force login attempt. If user fails to log in many times, the login IP address or the user account would be locked up or word verification be enabled for a period of time. The prompt given is as shown below:



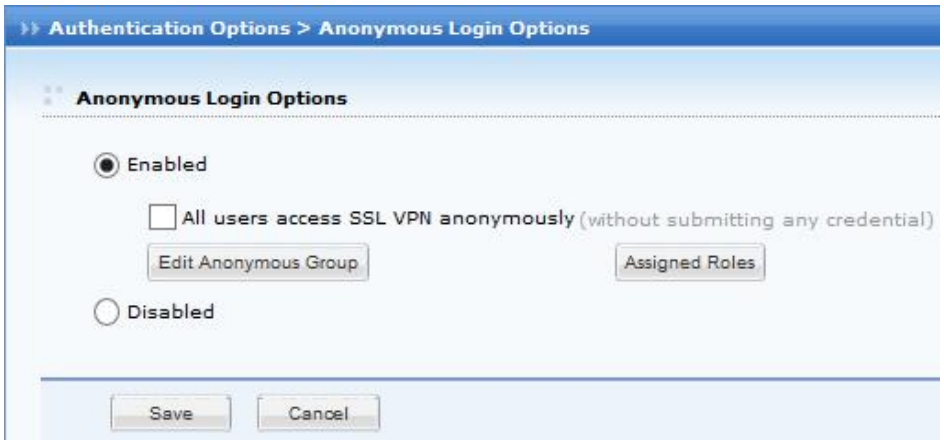
- **Word Verification:** It is also a feature that adds security to SSL VPN access. If this option "**If consecutive logon failures reach N, activate word verification"** is selected, 0 means word verification will be enabled forcibly; for non-Windows client-side, if the input value is less than 3, it will still be taken as 3. Once word verification is activated, end user will be required to enter the word he or she sees on the picture when visiting the login page and logging in to the SSL VPN, as shown below:



Anonymous Login

Anonymous login is a kind of login method that does not require connecting user to enter username and password, user accessing SSL VPN anonymously under the anonymous login user account and being able to access the resources that are associated with **Anonymous group**.

Navigate to **SSL VPN** > **Authentication** to enter the **Authentication Options** page. Click the **Configure** button following **Anonymous Login** and the **Anonymous Login Options** page appears, as shown in the figure below:

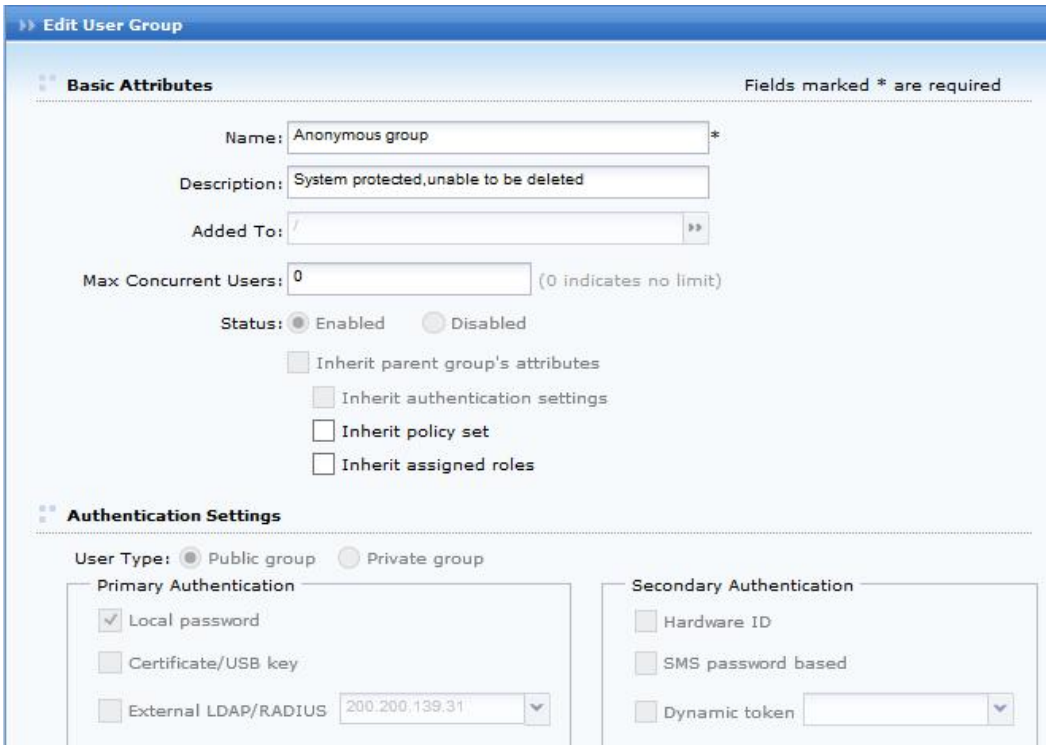


The following are the contents included on the **Anonymous Login Options** page:

- **Enabled, Disabled:** If **Disabled** is selected, no user could log in to the SSL VPN anonymously. If **Enabled** is selected, anonymous login is enabled, and end users can access the SSL VPN anonymously, simply by clicking the **Anonymous** button on the login page, as shown below:



- **All users access SSL VPN anonymously:** If this option is selected, all users can access SSL VPN anonymously (enter the **Resource** page, or the redirected-to page if this feature is enabled in the associated policy set), without submitting any credential through login page.
- **Edit Anonymous Group:** Click this button to configure the attributes of **Anonymous group**. For detailed guide, please refer to the Adding/Editing Resource Group section in Chapter 4. The attributes of **Anonymous group** are as shown in the figure below:

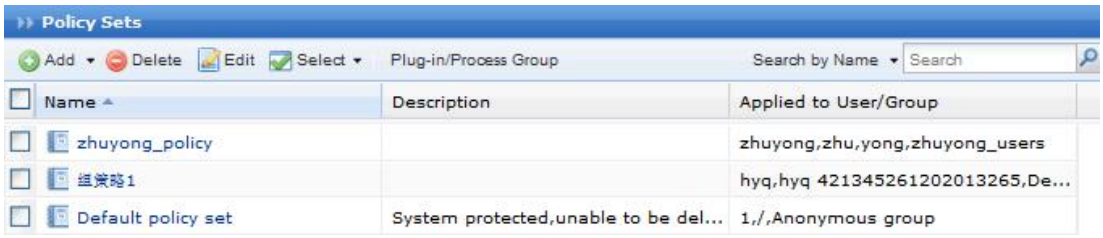


- **Assigned Roles:** Click this button to select and assign roles to the anonymous users. For detailed guide, please refer to the Adding Role section in Chapter 4.
- **Save:** Click it to save the settings. To apply changes, click the **Apply** button on the next page.

Policy Sets

A policy set is a collection of policies controlling end user's access to SSL VPN, rights at client end, and access rights on Security Desktop, including settings of **Client**, **Account Options**, **Remote Application and Cloud Storage**.

Navigate to **SSL VPN > Policy Sets** to enter the **Policy Sets** page, as shown below:



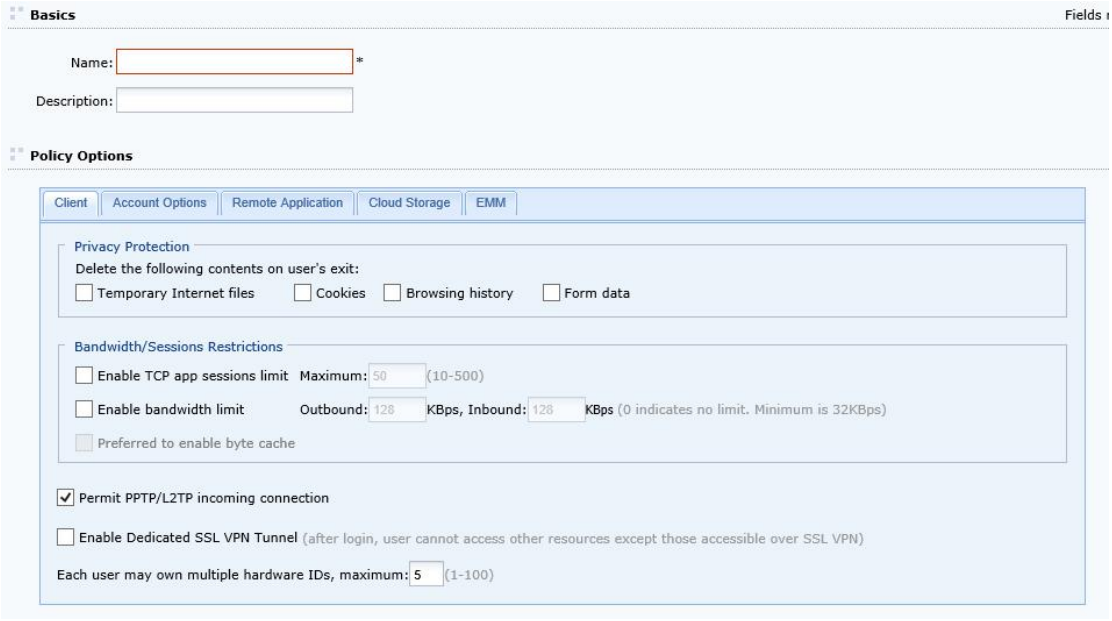
On the page displayed above, **Name** indicates the name of a policy set, **Description** indicates the descriptive information of a policy set and **Applied to User/Group** indicates the users/groups to which the corresponding policy set applies.

The following are some optional operations on the **Policy Set Management** page:

- To create a new policy set, click **Add > Policy set**.
- To create a policy set based on an existing policy set, select a policy set as template and click **Add > By using template**.
- To delete one or more policy sets, select the policy sets and then click **Delete**.
- To edit a policy set, select the policy set and then click **Edit**.
- To select policy sets on all pages, click **Select > All pages**.
- To select policy sets on the current page, click **Select > Current pages**.
- To deselect entries, click **Select > Deselect**.
- To search for a specific policy set, select **Search by Name**, **Search by Description** or **Search by User/Group**, enter the keyword and click the magnifier icon next to the textbox.

Adding Policy Set

1. Navigate to **SSL VPN > Policy Sets** and click **Add > Policy set** to enter the **Add Policy Set** page, as shown below:



2. Specify the name and descriptive information for the policy set.
3. Configure the following client-related options on the **Client** tab:
   - **Privacy Protection:** Specifies the contents to be automatically deleted at user's logout to protect user's privacy. Select **Temporary Internet files**, **Cookies**, **Browsing history** and/or **Form data**.
     - **Temporary Internet files:** Indicates the copies of webpages, images and media that are saved for faster viewing.
     - **Cookies:** Indicates the files stored on users' computer by websites to save preferences.
     - **Browsing history:** Indicates the links to the pages that users have visited.
     - **Form data:** Indicates the saved information that users have typed into forms.
   - **Bandwidth/Sessions Restrictions:** Specify limits on TCP app sessions and bandwidth for client, and select whether to preferentially enable byte cache.
     - **Enable TCP app sessions limit:** Check it to enable limit on TCP app sessions at client and then specify the maximum number of TCP application sessions allowed. The value range is 1 to 500. Unchecking it means no limit on TCP app sessions.
     - **Enable bandwidth limit:** Check it to enable limit on bandwidth for using Web applications, TCP applications and L3VPN at client and then specify maximum outbound and inbound bandwidth (KBps) allowed at client. The minimum value for

this field is 32 KBps and 0 means no limit. This function avoids the situation that some users preempt most of the HQ bandwidth with insufficient bandwidth left for others. Unchecking it means no limit on bandwidth used at client end.

- **Preferred to enable byte cache:** Check it to have the corresponding user preferentially enjoy the speedup of file access or downloading when the number of concurrent users reaches the maximum. Unchecking it means the corresponding user has no privileges to preferentially enjoy optimization.



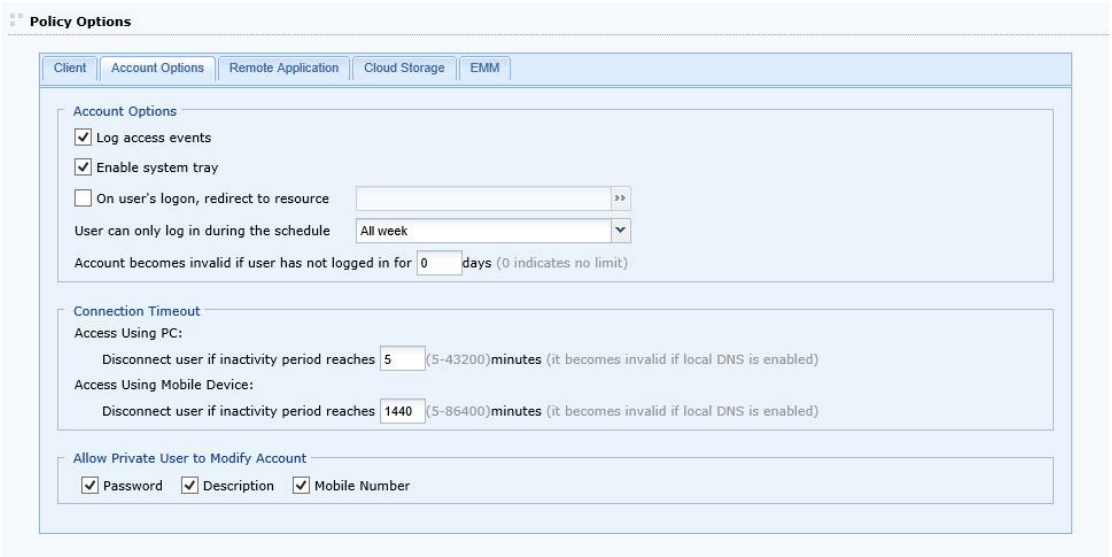
To make the **Preferred to enable byte cache** option available here, select the **Enable Byte Cache** option (in **System > SSL VPN Options > Network Optimization > Data Transfer > Byte Cache Options**. Please refer to the Network Optimization Related Settings section in Chapter 3**)**.

- **Permit PPTP/L2TP incoming connection:** Select whether to allow mobile users to log in through PPTP/L2TP.
- **Enable Dedicated SSL VPN Tunnel:** If this option is checked, users can only access the internal resources over SSL VPN. Unchecking it means users can access internal resources as well as the Internet after connecting to the SSL VPN. This feature is only applicable to the Windows or Android based client end.
- **Each user may own multiple hardware IDs, maximum:** Specify the maximum of hardware IDs that each use account can bind to. The value range is 1 to 100.



After configuring policy set completes, you need to associate it with user or user group when adding or editing user/group; otherwise, it will not work .

4. Click **Account Options** tab to enter the **Account Options** page and specify the account-related options, as shown below:



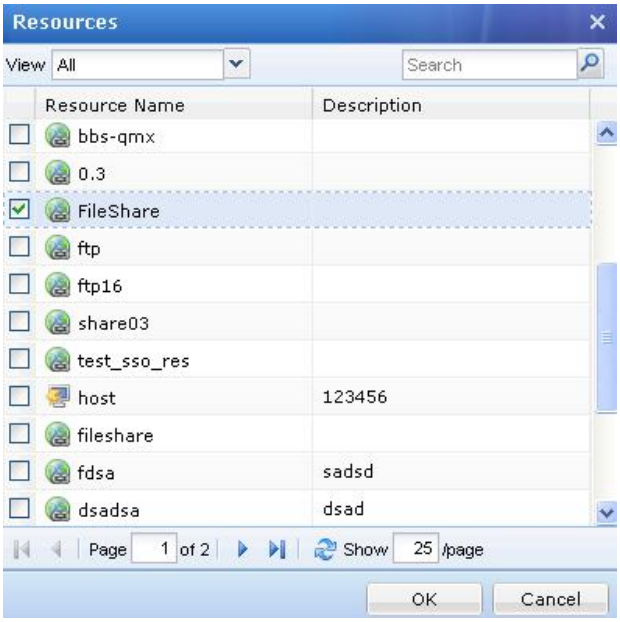
The following are the contents included on the **Account Options** tab:

- **Account Options:** Configure whether to log users' access, enable system tray and specify redirected-to resource, and specify valid period only during which user is allowed to login, maximum number of days required for a user account to be disabled due to not being used, and user idle timeout after login.
  - **Log access events:** Check it to log all the user's access events over SSL VPN.
  - **Enable system tray:** Check it to enable system tray for the user associated with this policy set (please refer to the Configuring Client Related Options section in Chapter 3).



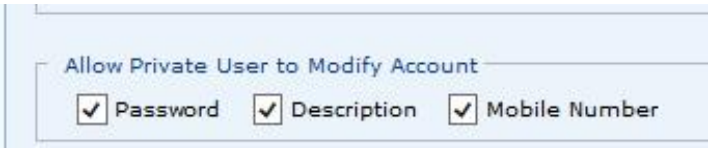
The **Enable system tray** option under **System > SSL VPN Options > General > Client Options** is a global option for all users. If it is checked, the **Enable system tray** option here is selected by default.

  - **On user's logon, redirect to resource:** Specify the resource to which the page will be redirected after user logs in to SSL VPN. Select this option and click the textbox to enter the **Resources** page, as shown below, and then select the resource (the resources available here are predefined in **SSL VPN > Resources**. Please refer to the Resource section in Chapter 4).



- **User can only log in during the schedule:** Specify the period of time only during which the user is allowed to access SSL VPN. Select a schedule from the drop-down list (the schedules available here are predefined in **System > Schedule**; please refer to the Schedules section in Chapter 3).
- **Account becomes invalid if user has not logged in for *N* days:** Specify the number of days required for a user account to be disabled due to not being used.

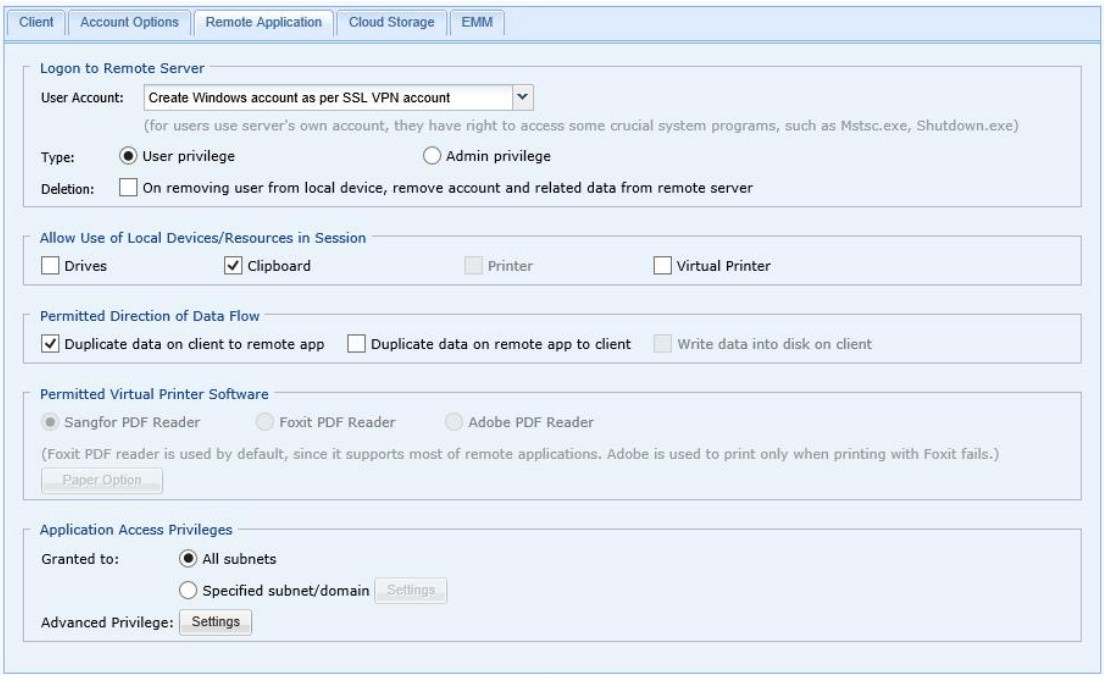
- **Connection Timeout:** Specifies the period of time to disconnect user due to inactivity for two logout scenarios.
- **Allow Private User to Modify Account:** Select **Password**, **Description** and/or **Mobile Number** if you allow private user to modify the password, description and mobile phone number.



If a private user is allowed to modify the password, description and mobile number, the user can click **Settings** (at upper right of the page) to modify its password, description and mobile number after logging in to SSL VPN.

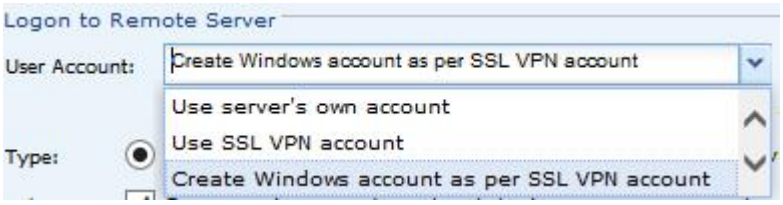
To allow a user to modify mobile number, enable SMS authentication for the user while adding or editing the user.

5. Click **Remote Application** tab to enter the **Remote Application** page and configure the related options.

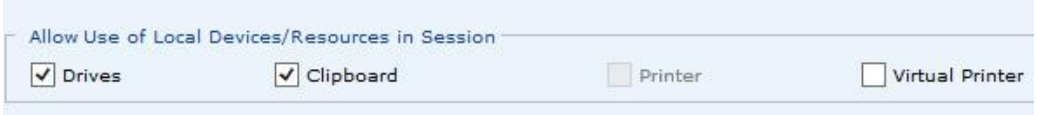


The following are the contents included on the **Remote Application** tab:

- **Logon to Remote Server:** Specifies what user account and privilege type is used by user to log into remote server.
  - **User Account:** Specifies what account can be used by mobile user to log in to remote server, as shown below:



  - **Type**: It appears when **Create Windows account as per SSL VPN account** is selected as **User Account**. It indicates the type of the created Windows account.
  - **Deletion:** If this option is selected, related account and data created on remote server will be removed together when user is removed from local device.
- **Allow Use of Local Devices/Resources in Session:** Select the device and/or resource you want to use in session, as shown below:



  - **Drives**: If it is selected, VPN users can save file onto local drives when accessing

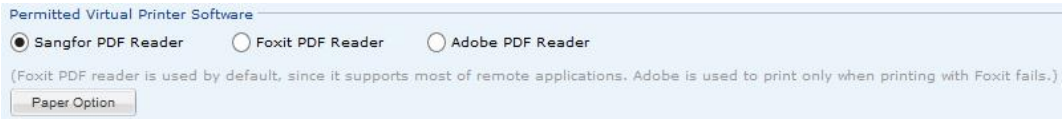
remote application resource.

- **Clipboard:** Select it to enable user to duplicate data from client end to remote server .
- **Printer:** If this option is selected, user can use the printer at client end to print the document in remote application after printer driver is installed on remote server.
- **Virtual Printer:** If it is selected, user can choose Sangfor virtual printer at remote server side to print file without need to install driver of local printer on remote server.

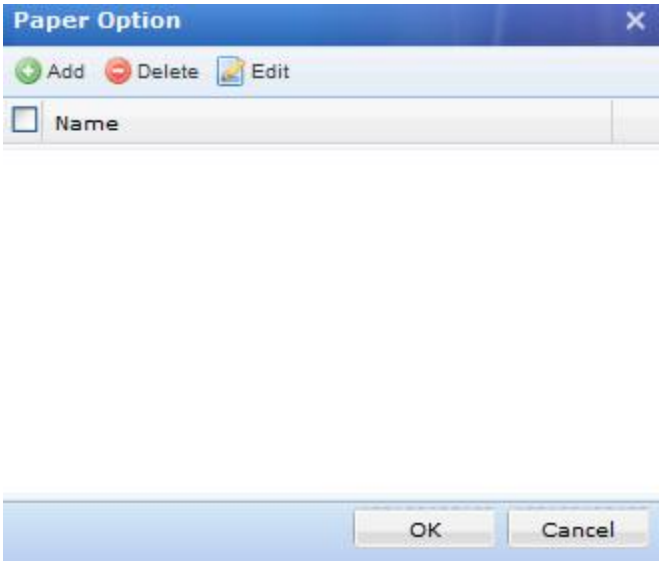
- **Permitted Direction of Data Flow:** It is available only when **Clipboard** option is selected.



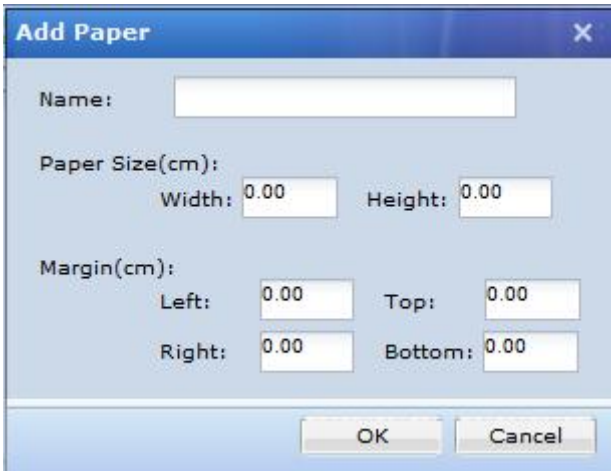
- **Permitted Virtual Printer Software:** It is configurable only when **Virtual Printer** option is selected. There are three types of virtual printer software, Sangfor PDF Reader, Foxit PDF Reader and Adobe PDF Reader. **Sangfor PDF Reader** is selected by default, which provides a better printing effect and supports more file types. If Sangfor PDF reader does not work, use Foxit or Adobe PDF reader instead. If you want to use Adobe PDF reader, it is recommended to use Adobe 9.4.



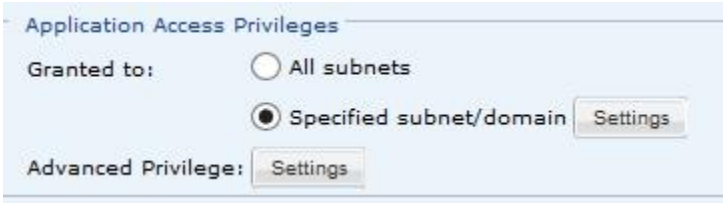
- **Paper Options:** Click it to configure paper-related options, as shown below:



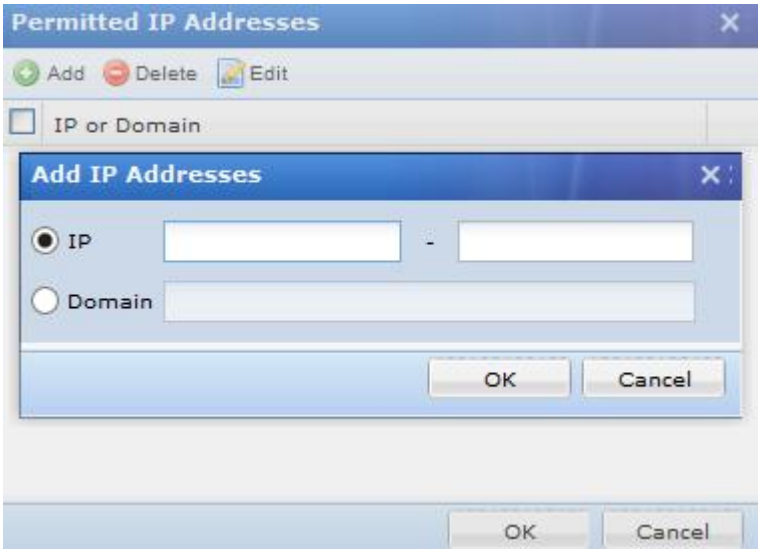
Click **Add** to enter the **Add Paper** page, specify the paper size and margin and click **OK** to save the changes, as shown below:



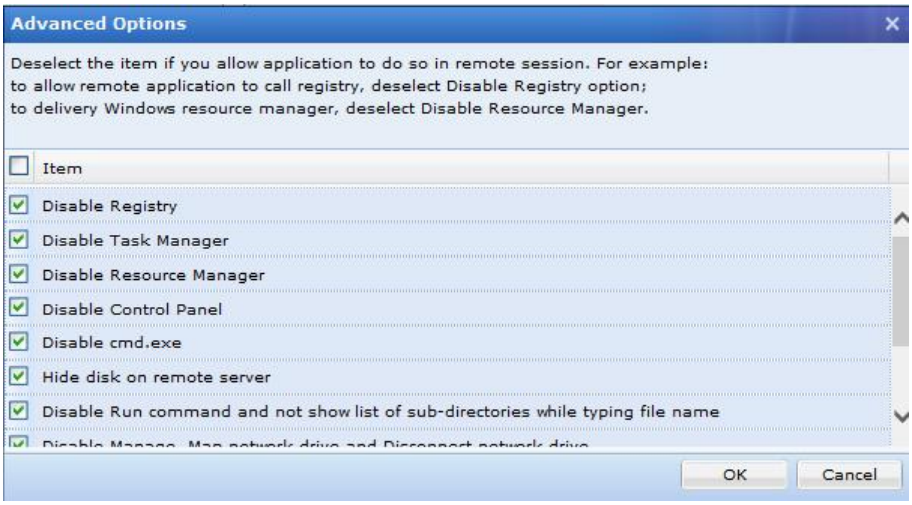
- **Application Access Privileges:** Specifies accessible subnet/domain for specific user, so as to achieve control over privilege of access to remote applications.



  - **All subnets:** Indicates user can access all subnets.
  - **Specified subnet/domain:** Specifies accessible subnet/domain for user**.** Click **Setting** to enter the **Permitted IP Addresses** page, click **Add** to add a entry, as shown in the figure below:



  - **Advanced Privilege**: Click to configure application-related advance options, as shown below:



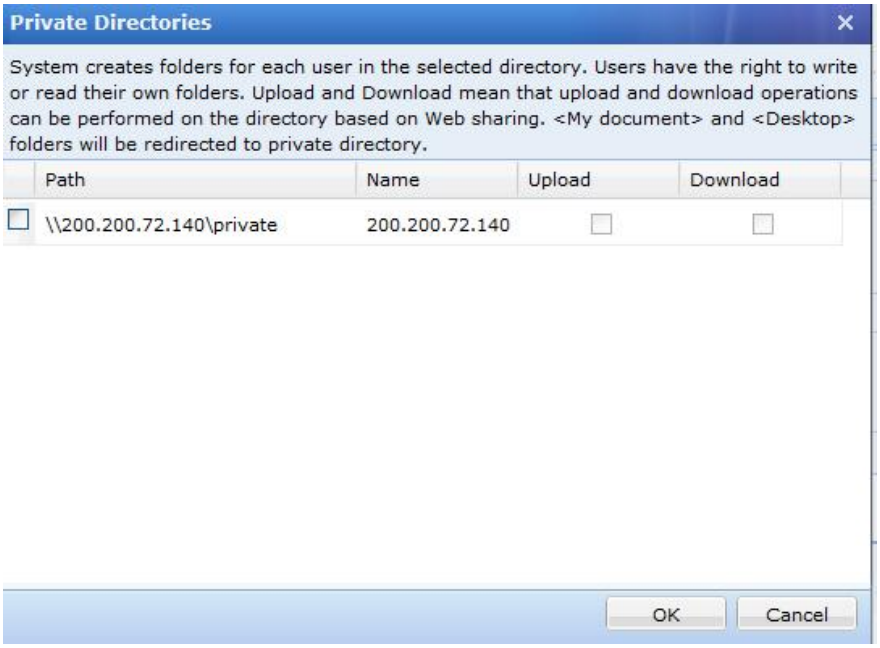
6. Click **Cloud Storage** to enter the **Cloud Storage** tab, and specify related options, as shown in the below figure:



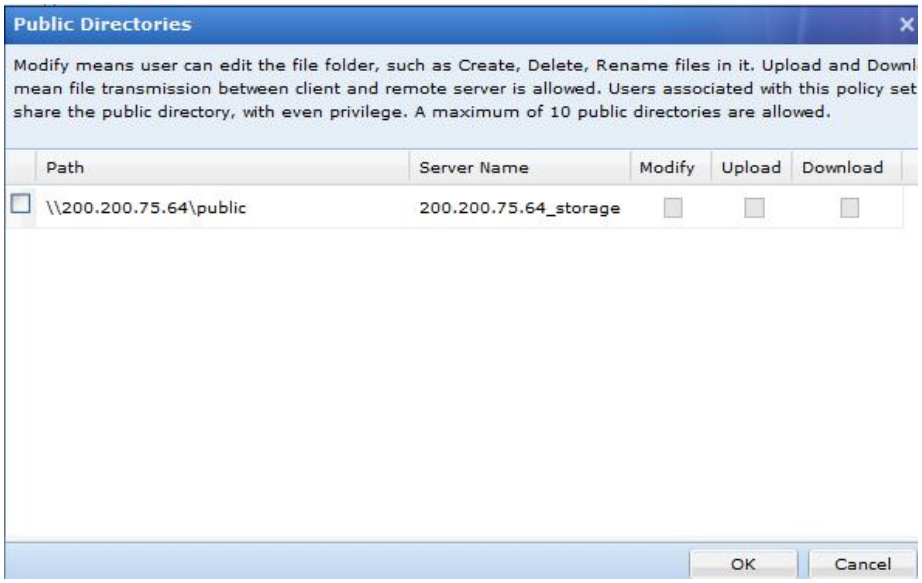
It specifies the storage privilege on remote server for users and server group used for EasyFile cloud storage.

- **Storage Directory:** Specifies the storage directory on remote server. Options are **Private Directory** and **Public Directory**. Click  following **Private Directory** or **Public Directory** to select desired directory. If no remote storage server is configured, you need to add storage server on **SSL VPN > Remote Servers > Storage Server** page(for details, refer to Adding Remote Storage Server in Chapter 4).

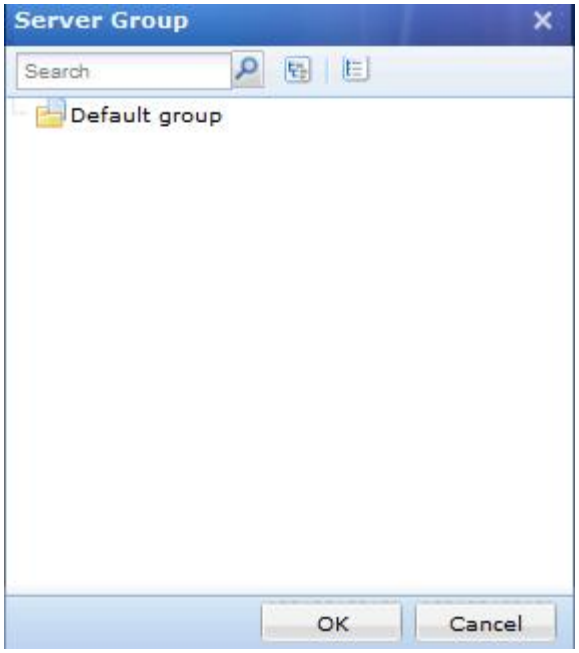
If **Private Directory** is selected, click  following it to enter the following page:



If **Public Directory** is selected, click » following it, and you will see the figure, as shown below:



- **EasyFile Cloud Storage:** Specifies the remote server group on which corresponding application will be invoked to open the file when the file on cloud is opened on mobile device, such as mobile phone, tablet.



7. Click **EMM** tab to enter the **EMM** tab. Enterprise mobility management(EMM) is to manage mobile devices that are connected to SSL VPN.



The following are contained on EMM tab:

- **Allow mobile device to register:** Determines whether mobile device is allowed to register.
- **Android MDM Policy:** Specifies MDM policy for Android devices.
- **iOS MDM Policy:** Specifies MDM policy for iOS devices.

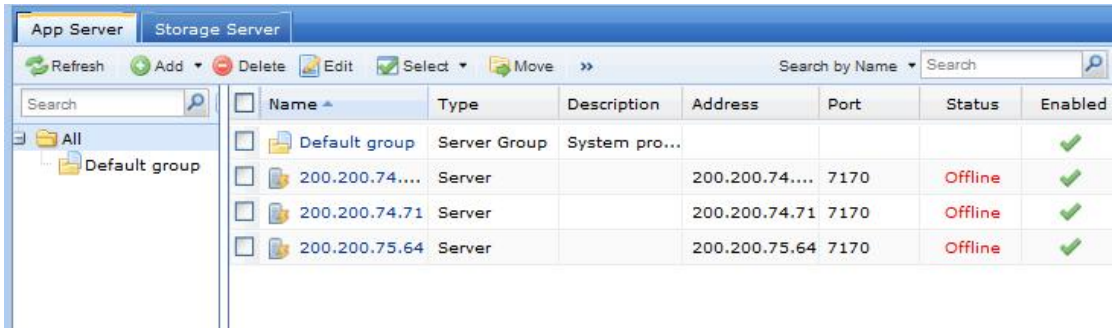
8. Click **Save** to save the settings or **Cancel** not to save the settings. To have settings take effect, click the **Apply** button at upper right of the next page.

***

Remote Servers

Remote server falls into application server and storage servers. Remote application servers are servers providing remote applications to SSL VPN users. After connecting to SSL VPN, users can use the remote applications even though they have not installed the corresponding application programs on their local computers. Remote storage servers are servers where the data or files can be saved in the remote application session. Before adding remote server, you need to install "Terminal Services" and "RemoteAppAgent" on remote server, and make sure these programs can work properly.

Navigate to **SSL VPN > Remote Servers** to enter the **App Server** page, as shown below:

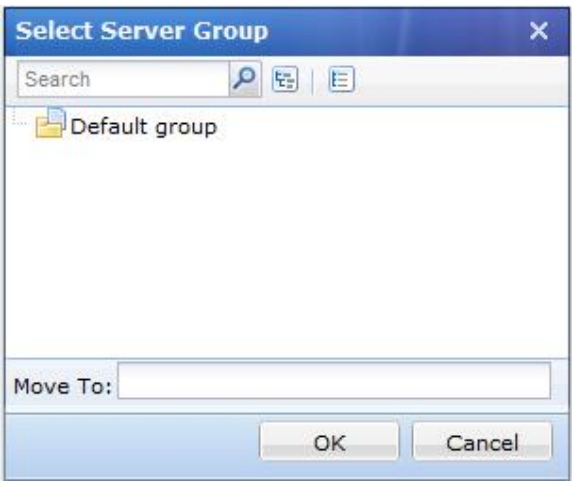


The following are the contents included on the **App Server** page:

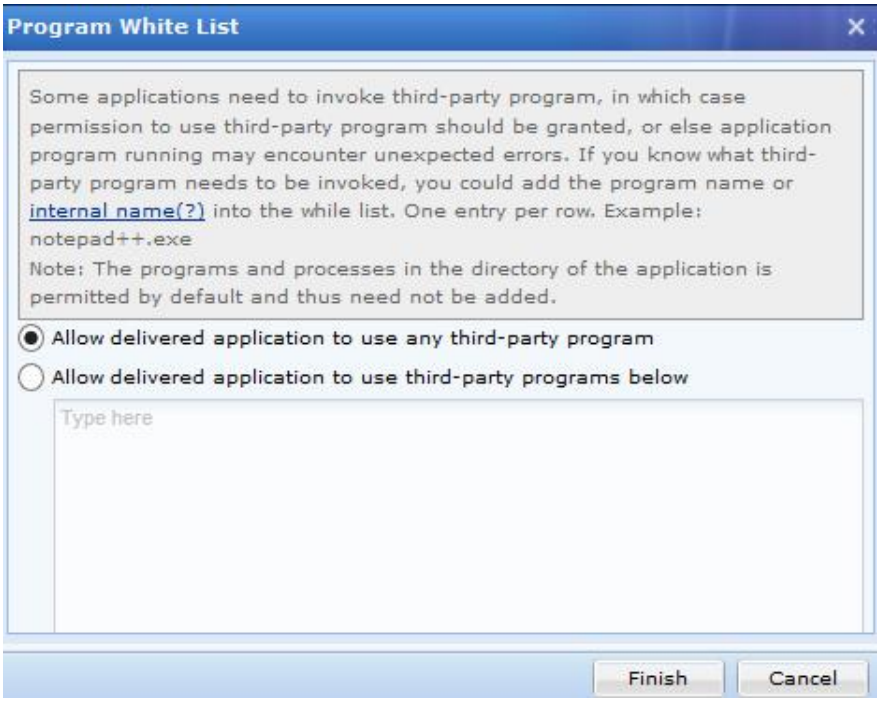
- **Name:** Displays the name of a remote server.
- **Address:** Displays the IP address of a remote server.
- **Port:** Displays the communication port of a remote server.
- **Description:** Displays the descriptive information of a remote server.
- **Type:** Displays the type of a app server, **Server** or **Server Group**.
- **Status:** Displays the status of a app server, **Online** or **Offline**.
- **Enabled:** Displays whether the app server is enabled or not.

The following are some optional operations on the **App Server** page:

- To add a app server, click **Add > App Server** or **Add > Storage Server**.
- To delete one or more app servers, select the remote servers and then click **Delete**.
- To edit a app server, select the remote server entry and then click **Edit**.
- To select app servers on all pages, click **Select > Server >All pages**.
- To select app servers on the current page, click **Select > Server > Current pages**.
- To cancel the selection, click **Select > Deselect**.
- To move the selected app server to a specified server group, click **Move** to enter the **Select Server Group** page, as shown below:



- To add multiple programs for one or more app servers, select the app servers and click **Add Multiple Programs**, and a dialog will appear, displaying the application programs available on existing remote servers. Please note that only the online app server can be associated with multiple programs.
- To allow delivered applications to invoke third-party programs, click **Program White List** and then specify third-party programs according to the specific case.



If **Allow delivered application to user third-party programs below** is selected, specify the allowed third-party programs in the textbox.

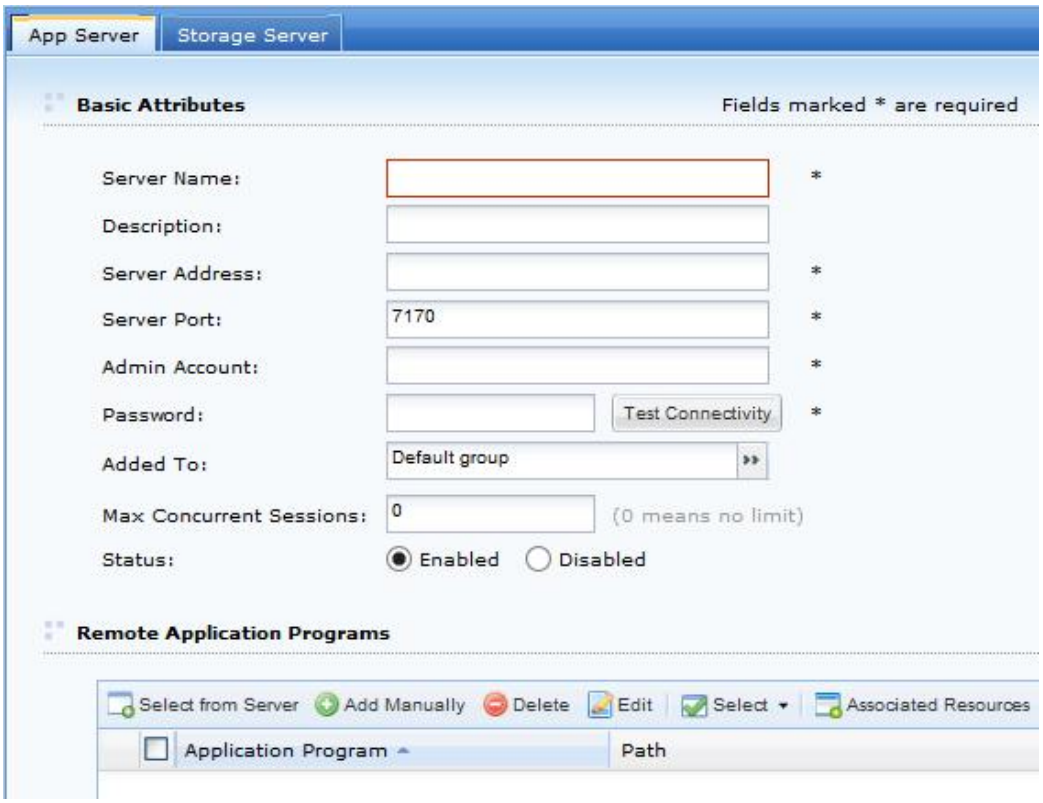
- To configure global settings for remote application servers, click **Server Options**.



- To download RemoteApp Agent and save it to local PC, click **Download RemoteApp Agent**.
- To update one or more app servers, select the app servers and then click **Update**.
- To view the status information of remote servers, click **Status** to enter **Status > SSL VPN > Remote Application** page.
- To search for a specific app server, select **Search by Name**, **Search by Description**, **Search by IP** or **Search by Program**, enter the corresponding keyword and then click the magnifier icon next to the textbox.

Adding Remote Application Server

1. Navigate to **SSL VPN > Remote Servers** to enter the **App Server** page.
2. Click **Add > Server** to enter the **App Server** page, as shown below:

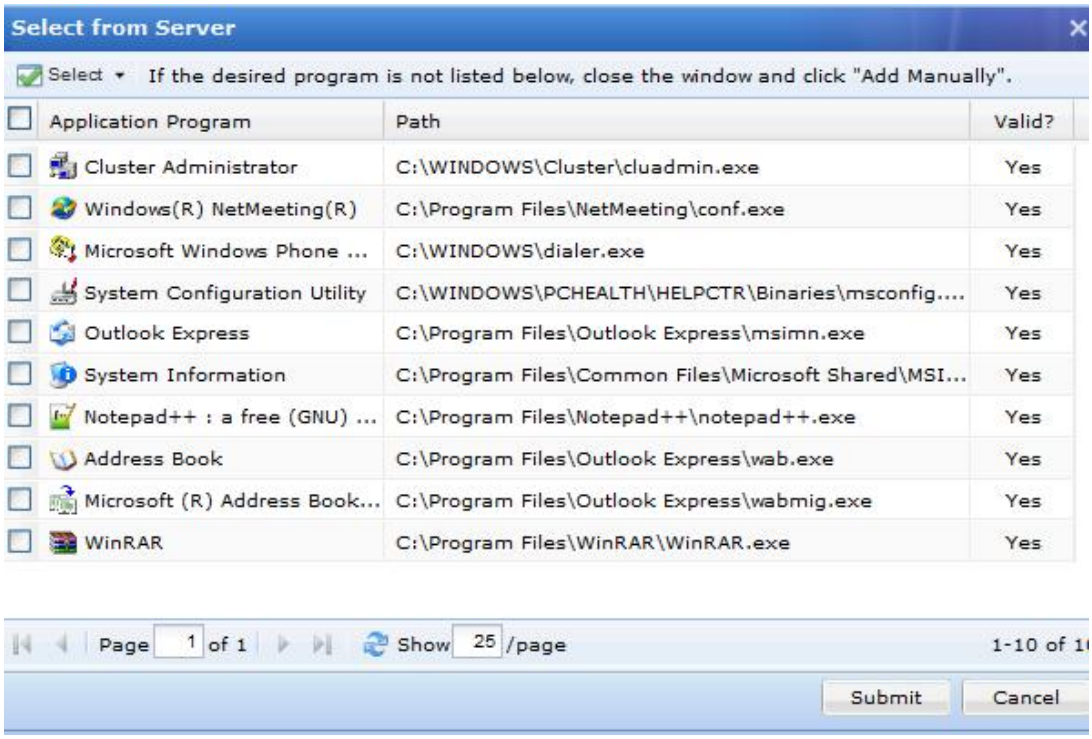


3. Configure **Basic Attributes** of the application server. The following are the basic attributes:

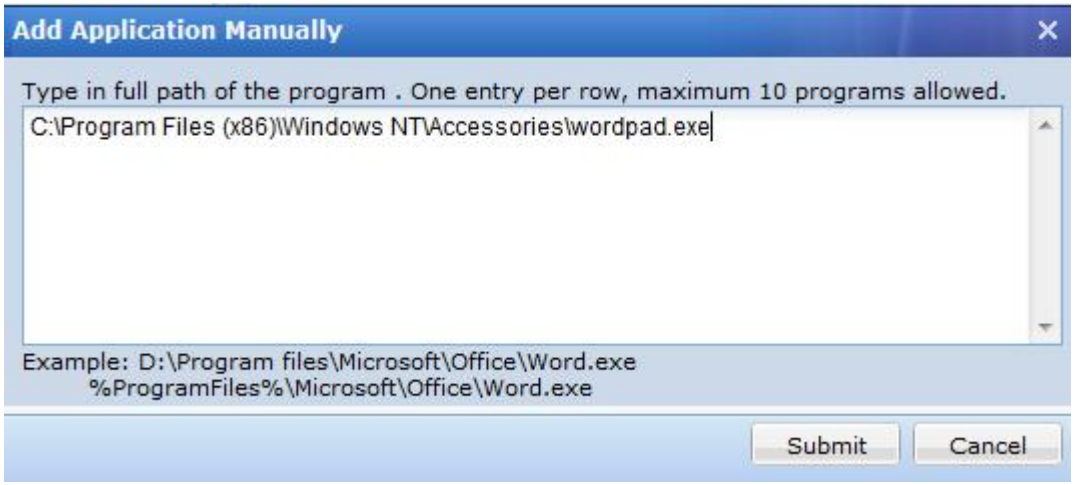
   - **Server Name**, **Description:** Enter a name and description for the remote application server.
   - **Server Address:** Enter the IP address of the remote application server that the Sangfor device will connect to.
   - **Server Port:** Specify the communication port of the remote server, through which the Sangfor device will connect to. It is 7170 by default.
   - **Admin Account:** Enter the administrator name for logging into the remote application server.
   - **Password:** Enter the administrator password for logging into the remote application server.
   - **Added To:** Specifies a server group to which this app server is added.
   - **Max Concurrent Sessions:** Specify the maximum number of concurrent connections to the remote application server.
   - **Status:** Select whether to enable the current app server.

4. Select and add the application programs under **Remote Application Programs**.

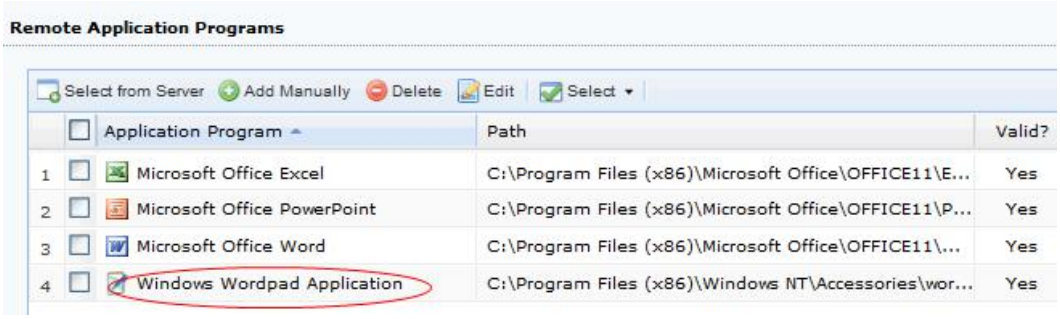
   - To select application programs already available on the server, click **Select from Server** to open the following page, as shown below:



- If the desired program is not available on the server, click **Add Manually** under **Remote Application Programs** to open the following dialog and then type the full path of the program, as shown below:



Click **Submit** to add the program, as shown below:



To delete the programs, select the program(s) and click **Delete**.

To edit a program, select the program and click **Edit**.

To select the programs on the current page, click **Select > Current pages**.

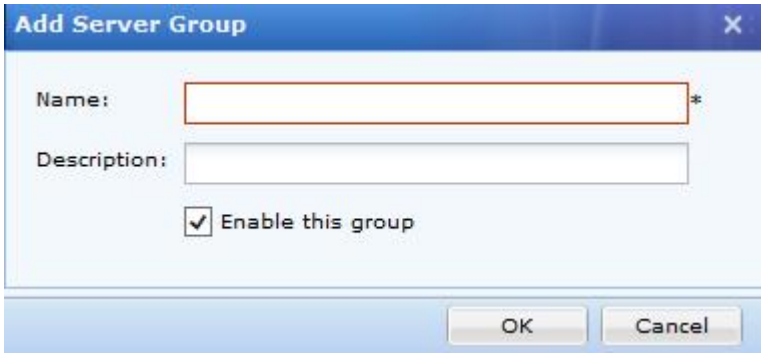
To select the programs on all pages, click **Select > All pages**.

To cancel the selection, click **Select > Deselect**.

To associate selected application program with existing resource quickly, click the **Associated Resource**s and a dialog appears, which shows all the resources owing name with that application program.

5. Click **Save** and then **Apply** to save and apply the settings.

If you want to add server group, click **Add > Server Group** to enter the **Add Server Group** page, as shown below:



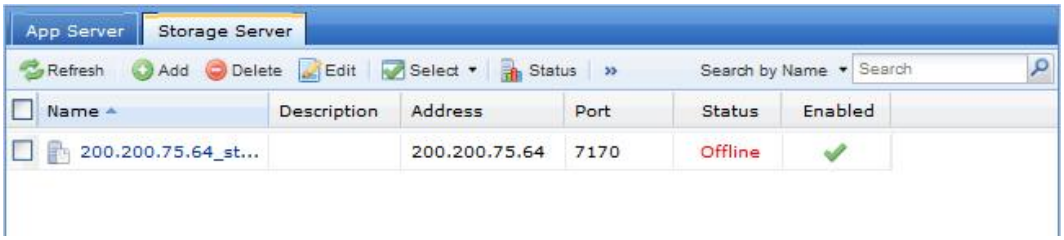
Enter the name and description for the server group and click **OK** to save the changes.

For how to deliver remote application, refer to Adding Remote Application in Chapter 7.

Adding Remote Storage Server

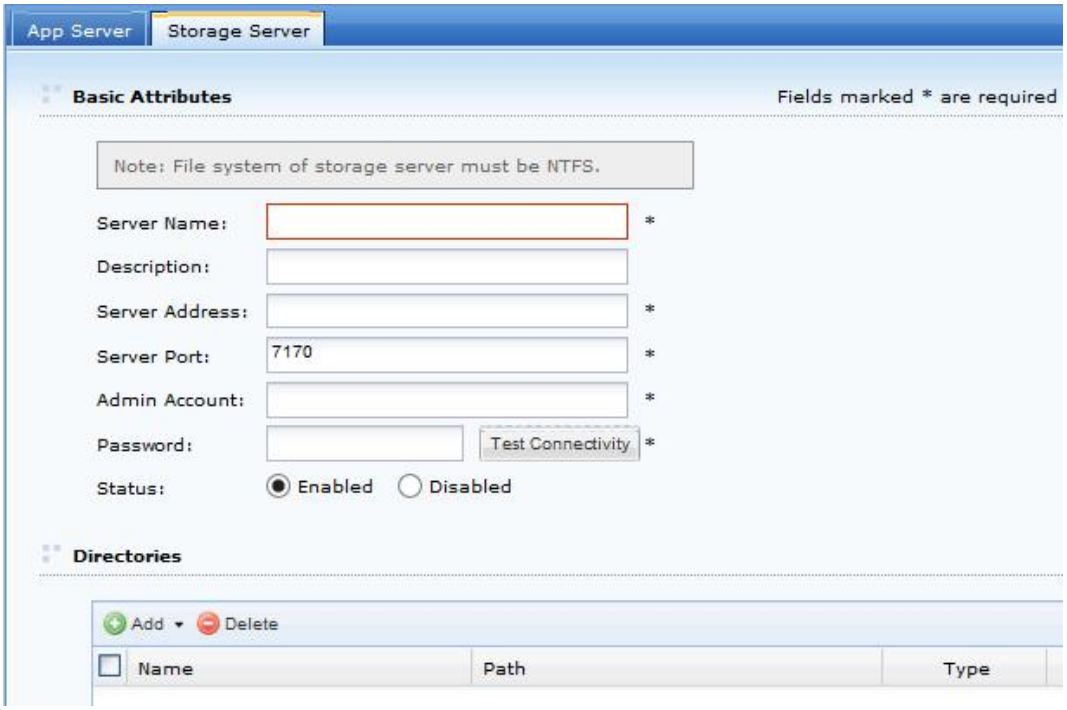
Remote storage server is used to save file modified in remote application. Private directory and public directory can be created on it.

1. Navigate to **SSL VPN > Remote Servers > Storage Server** page to enter the following page:



The contents included on above page are similar with those on **App Server** page. For related description, refer to **Remote Servers** section in this chapter.

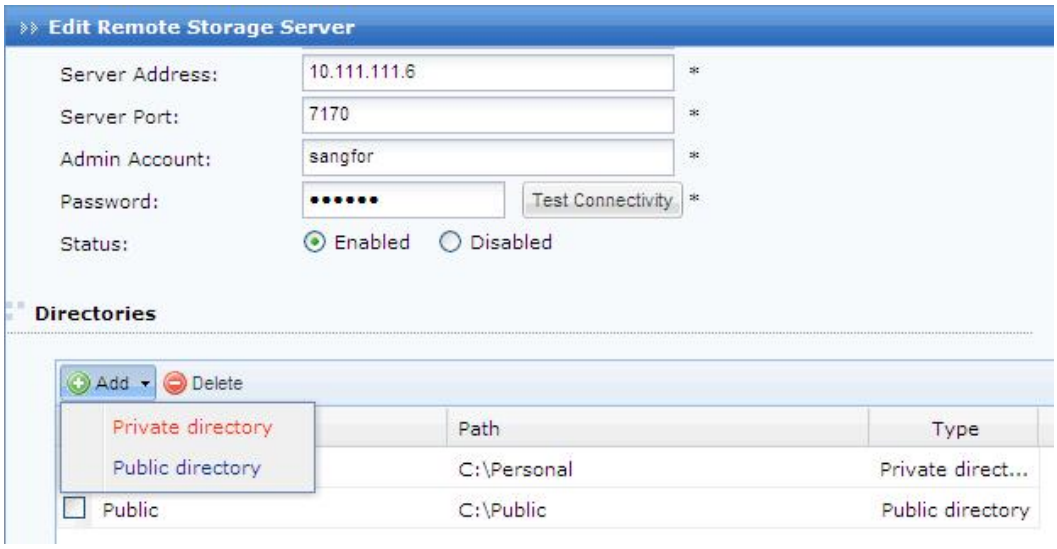
2. Click **Add** to add a storage server, as shown below:



3. Configure **Basic Attributes** of the storage server. The following are the basic attributes:

   - **Server Name**, **Description:** Enter a name and description for the remote storage server.
   - **Server Address:** Enter the IP address of the remote storage server that the Sangfor device will connect to.
   - **Server Port:** Specify the communication port of the remote storage server, through which the Sangfor device will connect to. Default port is 7170.
   - **Admin Account:** Enter the administrator name for logging into the remote storage server.
   - **Password:** Enter the administrator password for logging into the remote storage server.
   - **Status:** Select whether to enable the current remote storage server.

4. Under **Directories**, specify directory as private and/or public directory on the remote storage server.

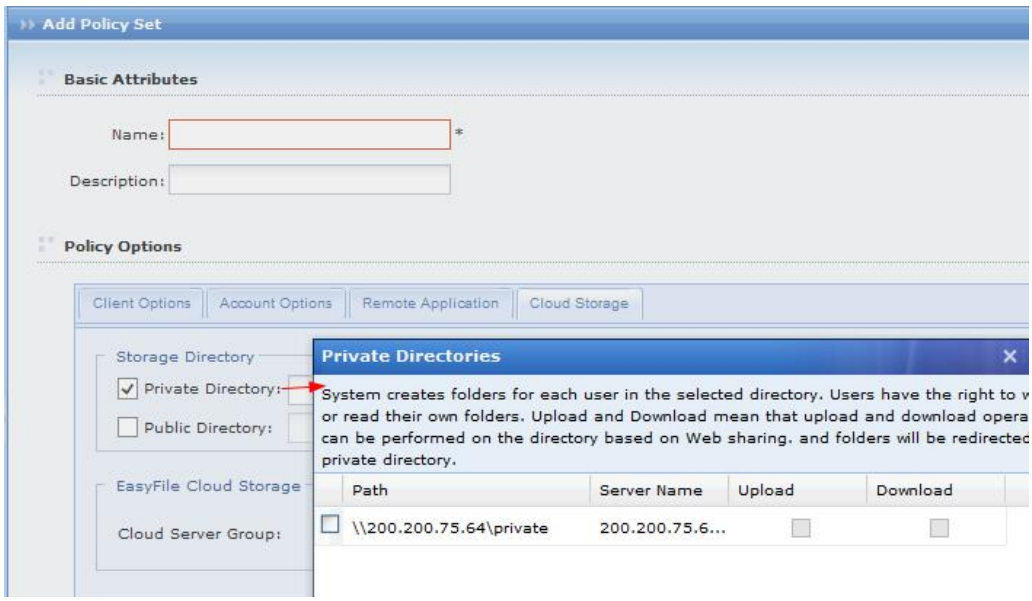


Private Directory: Each user owning private directory can see the private directory when he/she logs in to SSL VPN. This user has full privilege of this directory, he/she can create sub-directory, add, or delete file/file folder.

Public Directory: All users can see public directory associated with them. They can read file under this directory. The administrator has administrative privilege to determine whether user can write the file under this directory. If user has the right to write the file, he/she can save the modified file to the public directory.

To specify private directory or public directory, click **Add** > **Private directory** or **Public directory** to enter the **Private Directories** page or the **Public Directories** page, and then select a directory as the private or public directory.

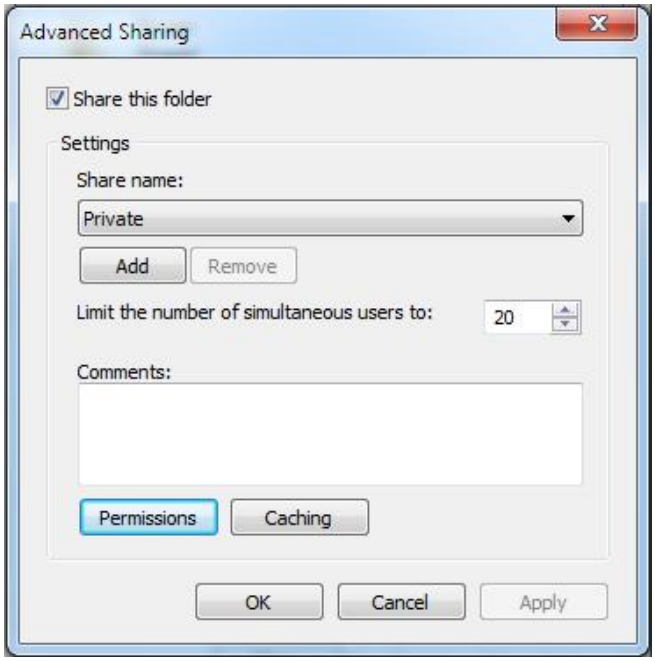
When an end user accesses to the remote application, a personal folder will be automatically created in the specified directory which is configured in the associated policy set, as shown in the figure below.

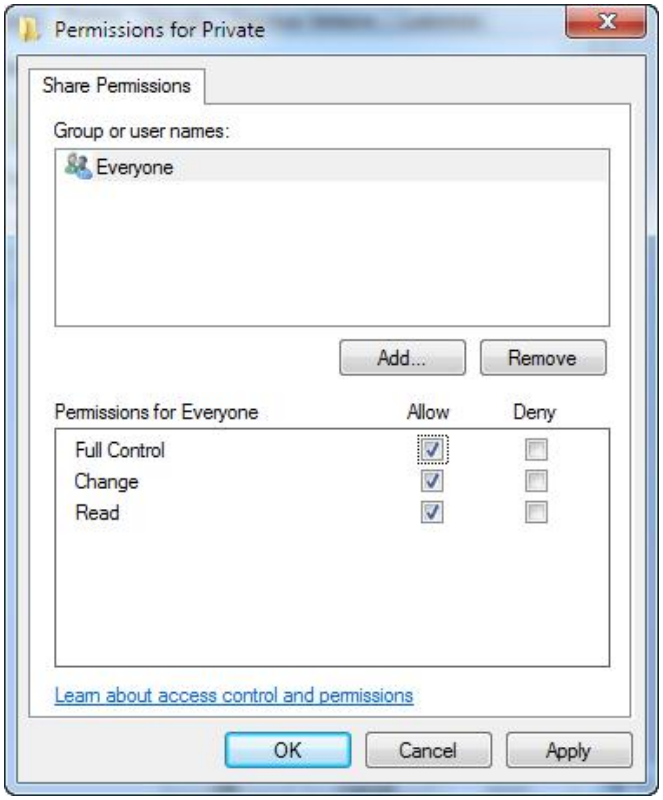


The difference between private directory and public directory is that each folder in private

directory can only be read and written by one user (the owner); while the folders in public directory can be read by all connecting users (if **Write**, **Upload** or **Download** are not selected).

The directory configured here can be configured as a shared folder on remote server. You can configure folder permission on remote server, as shown below:





5. Click **Save** and then **Apply** to save and apply the settings.

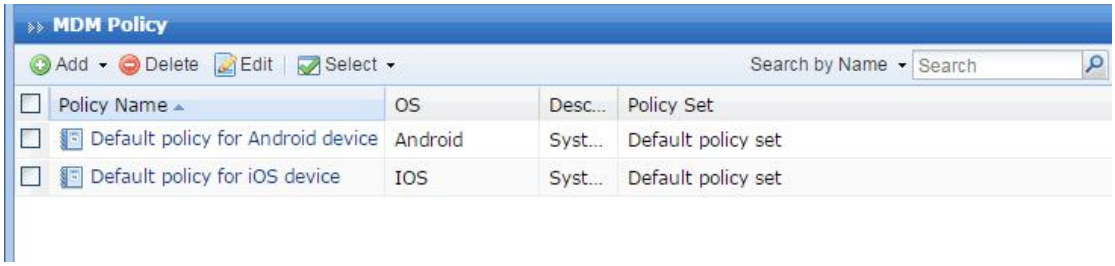
For how to apply remote storage server, refer to Cloud Storage section when Adding/Editing Policy set in Chapter 4.

EMM

Enterprise mobility management (EMM) enables users to deal with businesses on the go to with a smart device, and enables enterprise to manage the authorized use of smart devices.

MDM Policy

Navigate to **SSL VPN** > **EMM** > **MDM Policy** to enter **MDM Policy** page, as shown below. In **MDM Policy**, you can specify MDM policy for Android devices and iOS devices.

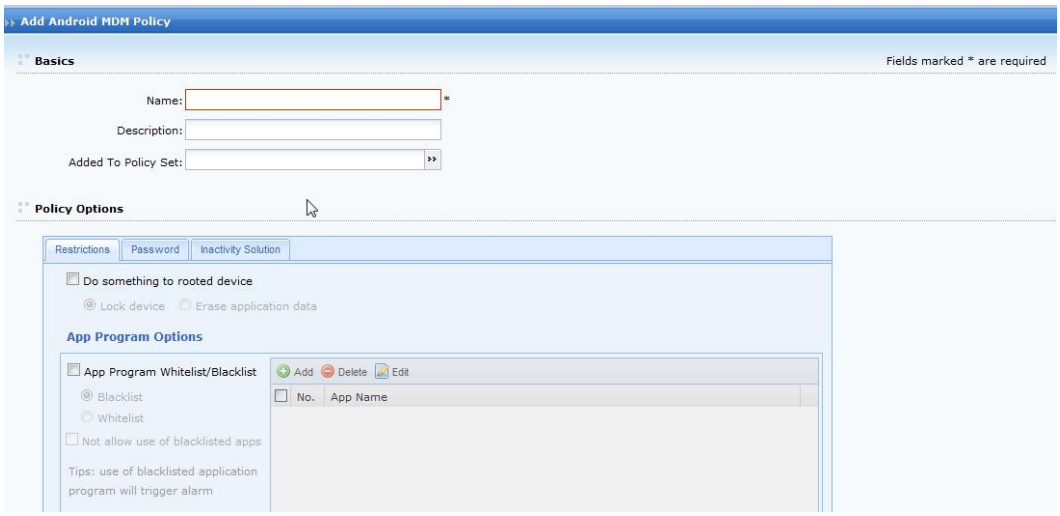


To add MDM policy for Android devices and iOS devices, click **Add** and select the corresponding option.



Adding Android MDM Policy

In **SSL VPN** > **EMM** > **MDM Policy**, click **Add** and select **Add Android MDM Policy**, to configure the **Restrictions**, **Password strength requirements** and **Inactivity Solutions** for the connecting Android devices, as shown below:

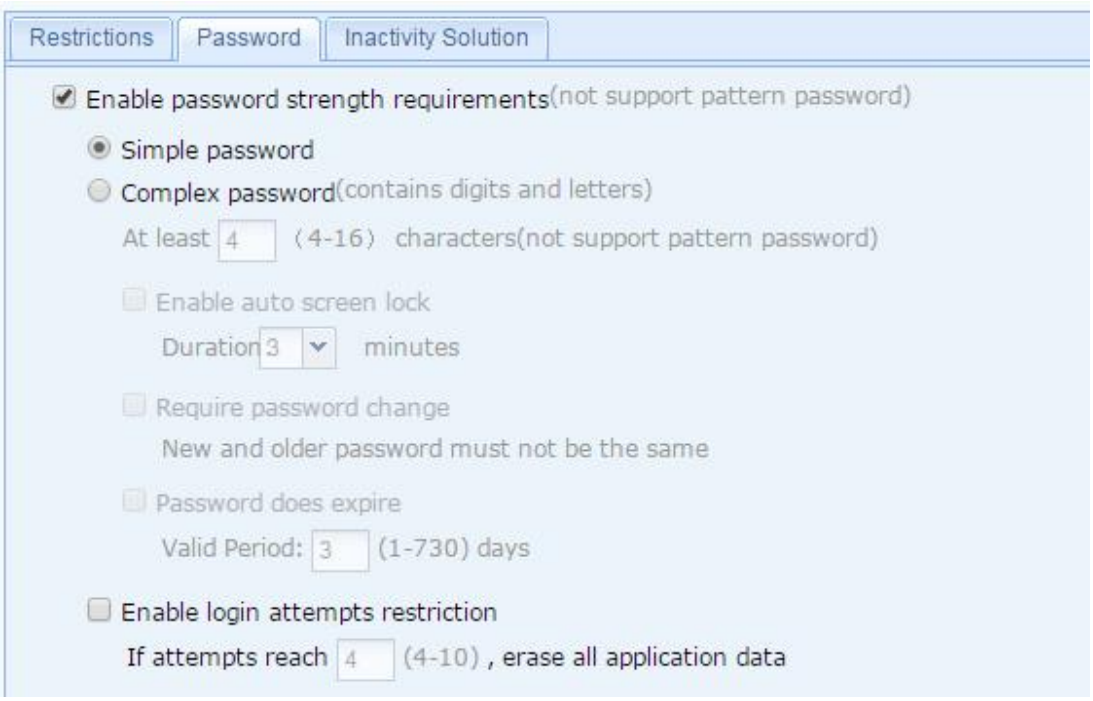


The following are the contents included in the Android MDM policy:

- **Name:** Specifies name of the Android MDM policy.
- **Description:** Specifies description for the policy.
- **Added to Policy Set:** Specifies the policy set to which the Android MDM policy will be added.
- **Restrictions:** Specifies restrictions for mobile devices.

  The following contents are included on **Restrictions** tab:

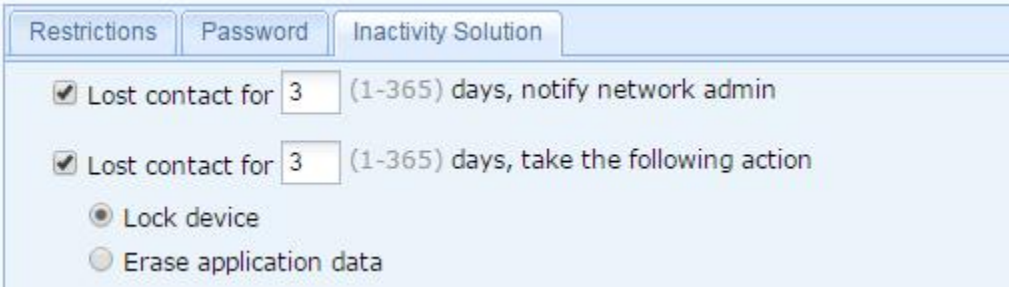
  - **Do something to rooted device:** If mobile device is rooted, you can choose to lock it or erase application data.
  - **App Program Whitelist/Blacklist:** A blacklisted app program cannot be accessed by end users through smart phones, while whitelisted app program can be accessed.
  - **Not allow use of blacklisted apps:** This makes alert message be sent to the network administrator. If **Blacklist** is selected above, application programs in the list are blacklisted; If **Whitelist** is selected above, application programs outside the list are blacklisted.
- **Password:** Specifies password strength requirements for mobile devices, as shown below:



The following contents are included on **Password** tab:

- **Enable password strength requirements:** Enable password strength requirements for mobile endpoints.
- **Simple password:** Indicates that there is no requirements for password strength.
- **Complex password:** Specifies complex password. You can specify password length, enable auto screen lock, require password change and specify password expiry date.
- **Enable login attempts restriction:** If number of login attempts reaches the threshold, application data will be erased.

- **Inactivity Solution:** Specifies the actions if system loses contact with the mobile device for specific days.



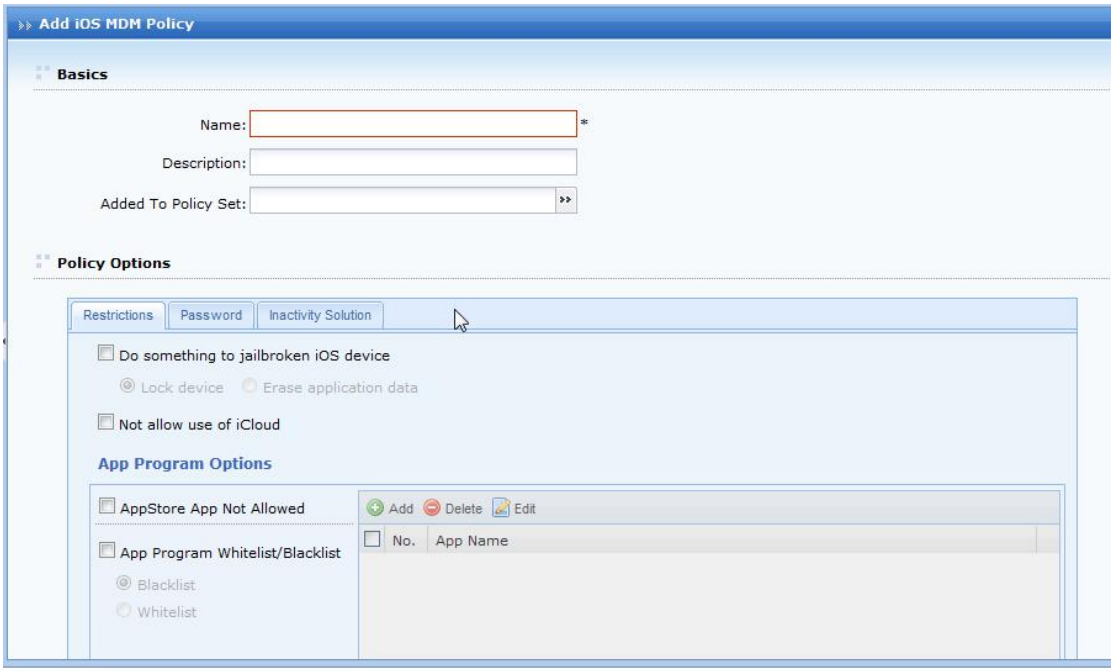
The following are contents on **Inactivity Solution** tab:

- **Lost contact for N days, notify network admin:** Specifies threshold. If system loses contact with mobile device for specific days, notify network administrator.
- **Lost contact for N days, take the following action:** Specifies threshold and action to the mobile device. You may lock the mobile device or erase application data if it loses

contact with system for specific days.

Adding iOS MDM Policy

In **SSL VPN** > **EMM** > **MDM Policy**, click **Add** and select **Add iOS MDM Policy**, to configure the **Restrictions**, **Password strength requirements** and **Inactivity Solutions** for the connecting iOS devices.



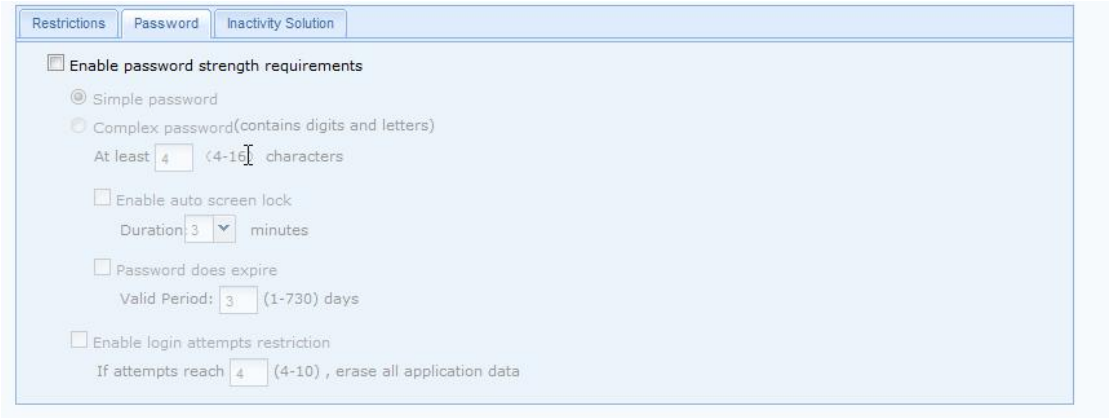
The following are contents included in iOS MDM policy:

- **Name:** Specifies name of the iOS MDM policy
- **Description:** Specifies description of the iOS MDM policy
- **Added To Policy Set:** Specifies policy set that the iOS MDM policy will be added to.
- **Restrictions:** Specifies restrictions for mobile devices.

  The following contents are included on **Restrictions** tab:

  - **Do something to jailbroken iOS device:** When mobile iOS devices are jailbroken, you can choose to **Lock device** or **Erase application data**.
  - **Not allow use of iCloud:** Once enabled, mobile iOS devices cannot use iCloud.
  - **App Program Options:** There are two options: **AppStore App Not Allowed** and **App Program Whitelist/Blacklist.** If **Blacklist** is selected, application programs in the list are blacklisted; If **Whitelist** is selected, application programs outside the list are blacklisted. Use of blacklisted application program will trigger alarm.
- **Password:** Specifies password strength requirements for mobile iOS endpoints, as shown

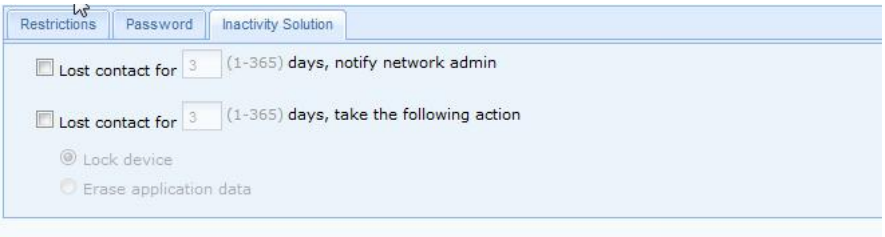
below:



The following contents are included on **Password** tab:

- **Enable password strength requirements:** Enable password strength requirements for mobile endpoints.
- **Simple password:** Indicates that there is no requirements for password strength.
- **Complex password:** Specifies complex password. You can specify password length, enable auto screen lock, require password change and specify password expiry date.
- **Enable login attempts restriction:** If number of login attempts reaches the threshold, application data will be erased.

- **Inactivity Solution:** Specifies the actions if system loses contact with the mobile device for specific days.



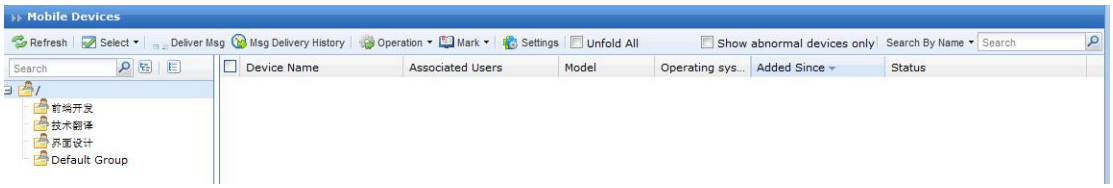
The following are contents on **Inactivity Solution** tab:

- **Lost contact for N days, notify network admin:** Specifies threshold. If system loses contact with mobile device for specific days, notify network administrator.
- **Lost contact for N days, take the following action:** Specifies threshold and action to the mobile device. You may lock the mobile device or erase application data if it loses contact with system for specific days.

Mobile Devices

Mobile Devices: Displays relations among SSL VPN users, user groups and applications.

Navigate to **SSL VPN** > **EMM** > **Mobile Devices** to enter **Mobile Devices** page, as shown below:



On the **Mobile Devices** page, user (group) list is on the left panel, while **Model**, **Operating System**, **Added Since**, and **Status** are on the right panel. To show subgroups and users under current suer group, click **Unfold All**. To show abnormal mobile devices, select **Show abnormal devices only.**

You can enter search term of the target user in the search bar on the right corner. Click magnifier icon to search. Then user groups that have been searched will be highlighted in the user(group) list.

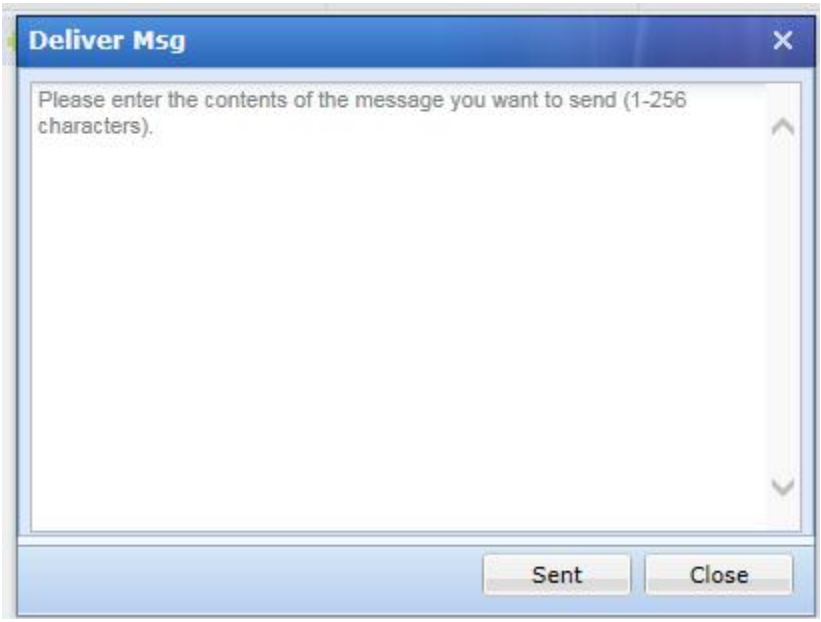


To search specific entries, you may search by device name, model, associated user, OS, IMEL/UDID.

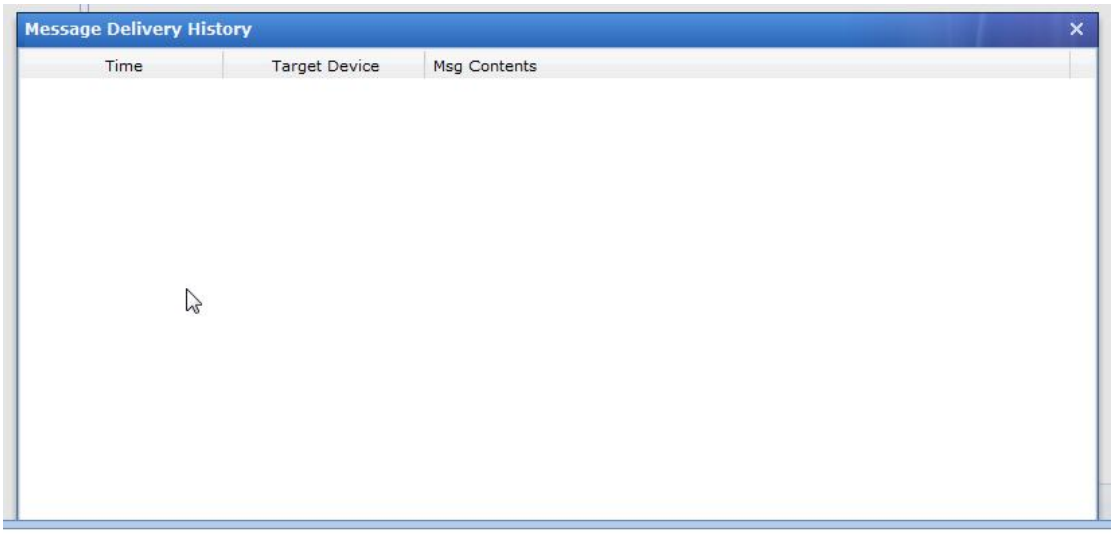
The following are contents on right panel:

- **Device Name:** Shows name of mobile devices.
- **Associated Users:** Shows users associated with mobile devices.
- **Model:** Shows model of mobile devices.
- **Operating System:** Shows OS of mobile devices.
- **Added Since:** Shows time when mobile device is registered.
- **Status:** Shows status of devices, normal, erased, lost or it loses contact.

To deliver message to specific mobile device, select **Device Name** and click **Deliver Msg.** Then, the following **Deliver Msg** dialog pops up and you can type message contents in this dialog.



To view message delivery history, click **Message Delivery History**, as shown below:



To lock screen, unlock screen, remove screen lock password, erase application data and remove device, click **Operation** and select the corresponding option, as shown below:



To mark mobile devices as lost or as found, click **Mark** and select the corresponding option .

To enable and configure mobile device management, click **Settings**, as shown below:



The following are the contents included on the **Settings** page:

- **Mobile Device Management (MDM):** Select this option to enable mobile device management.
- **VPN Address:** Specifies IP address/domain name and port number for accessing the SSL VPN device from public network. On that IP address, mobile device may register to access the SSL VPN, admin may manage and deliver message to the connecting mobile devices.
- **iOS MDM Certificate:** To enable mobile device to register, you need to upload MDM certificate, or else iOS device fails to register. To apply for MDM certificate, please refer to the instruction in **Application for IOS MDM Certificate**.

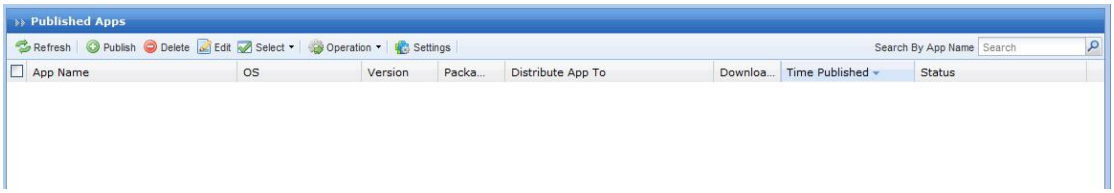


1. Once VPN address is changed, mobile devices previously registered will be lost control and become unassociated.
2. Dst ports must be consistent. Arbitrary ports are not supported (441 port of firewall to non-441 port of SSL).
3. Firewall or routers cannot contain ports already used by SSL VPN, for example, log in to console port 443, 80 and etc.

Published Apps

Published Apps: Manages published mobile Apps, and displays basic information of mobile Apps.

Navigate to **SSL VPN** > **EMM** > **Published Apps** to enter **Published Apps** page, as shown below:



App Name: Name of Apps

OS: Operating system applicable to mobile endpoints.

Version: Version information of Apps

Package Size: Size of Apps

Distribute App To: Users Apps distributed to

Downloads: Count downloads

Time Published: Time when Apps are published

Status: Status of Apps

Click **Refresh** to refresh information displayed on the page

Click **Publish** to publish wrapped Apps, as shown below:



App Name: Name of the App.

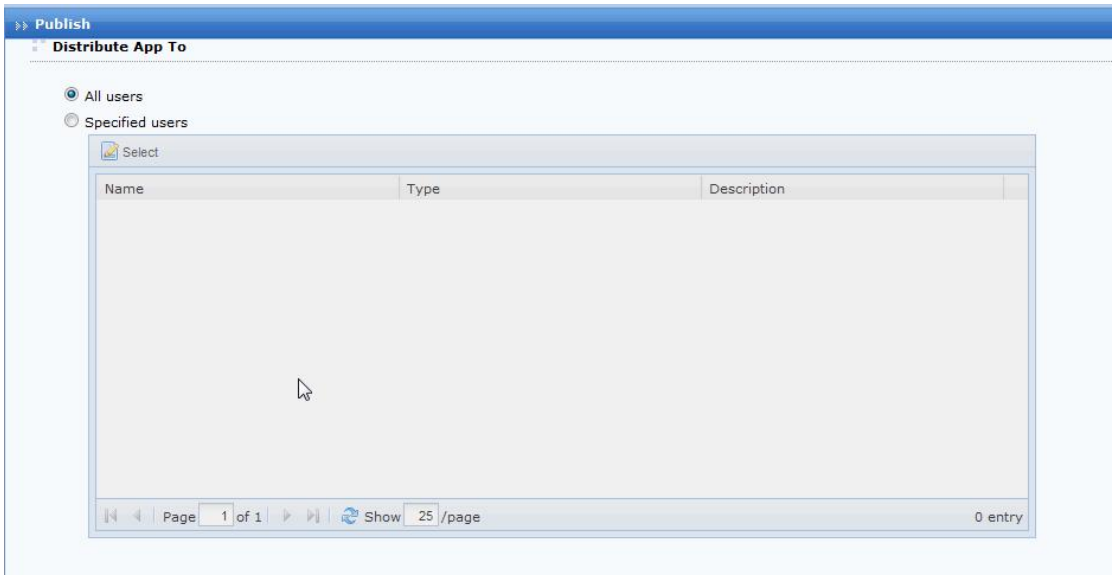
Package Size: Size of Apps

Version: Current version of Apps

Status: In my Apps and not in my Apps

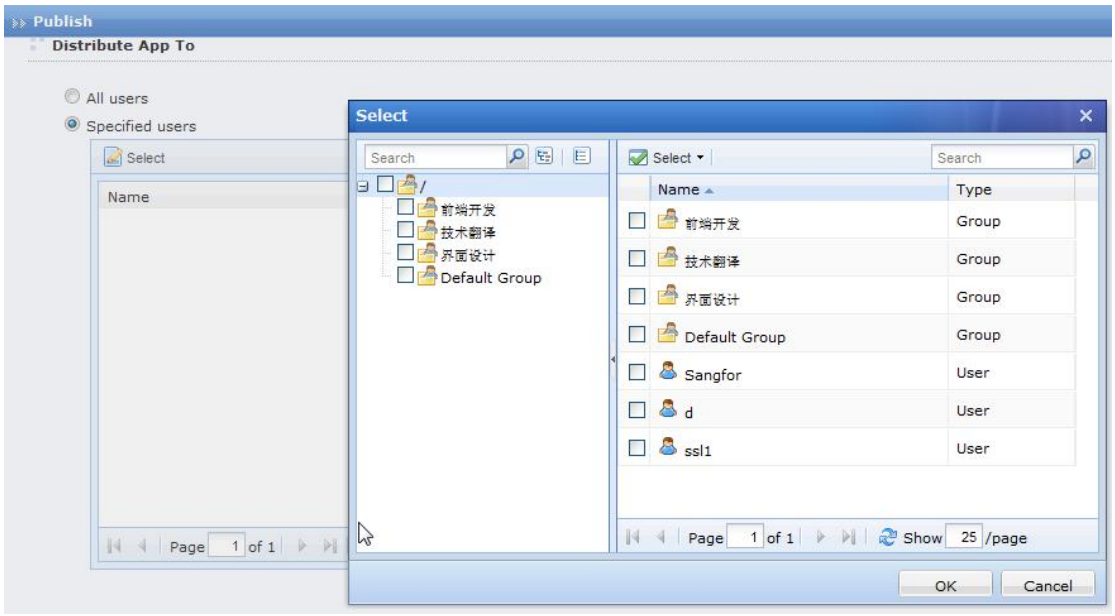
Description: Description of Apps

Mobile Device: Smartphone or Tablet



Select **All users**, all users are allowed to download this application.

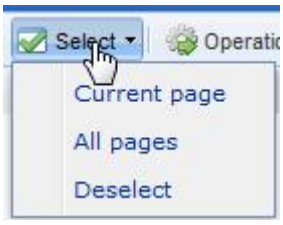
Select **Specified users**, only selected users or user group can download, as shown below:



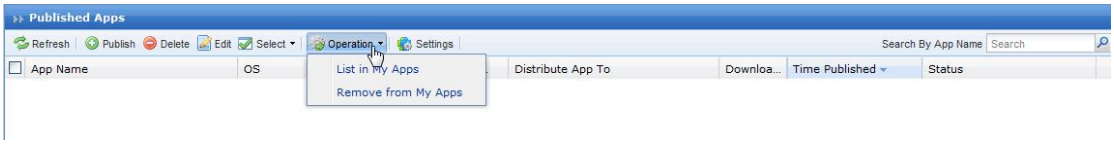
Click **Delete** to delete selected Apps.

Click **Edit** to edit selected Apps.

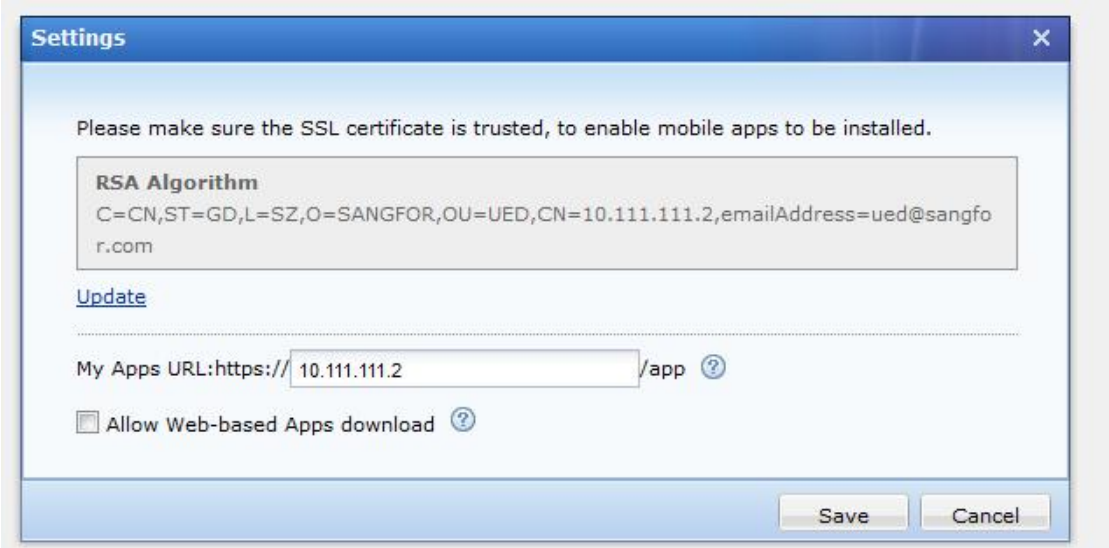
Click **Select** to select information displayed on the page, as shown below:



Click **Operation** to list or remove Apps from my Apps, as shown below:



Click **Settings** to enable Web-based Apps and configure external access address for published Apps, as shown below:



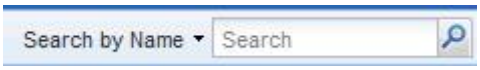
1. Please make sure the SSL certificate is trusted, to enable mobile apps to be installed. SSL certificate comes with the SANGFOR SSL device is issued by SANGFOR. Users should

pay extra money to SSL certificate supplier to buy trusted SSL certificate.

2. External network address of Published Apps matches with the trusted SSL certificate domain name.

3. If SSL service of the device uses non-default port 443, then you should enter the same SSL service port in external access address.

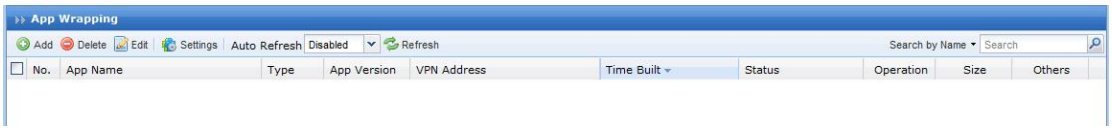
Search for Apps by name. Enter search term in **Search** and then click .



App Wrapping

App Wrapping: Wrap App to SSL VPN to realize secure access and visit.

Navigate to **SSL VPN** > **EMM** > **App Wrapping** to enter **App Wrapping** page, as shown below:



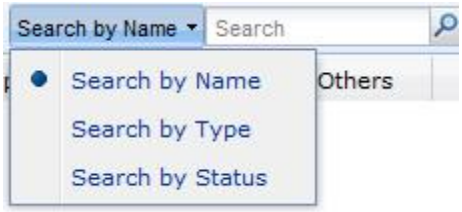
Click **Delete** to delete the selected application.

Click **Edit** to edit the selected application.

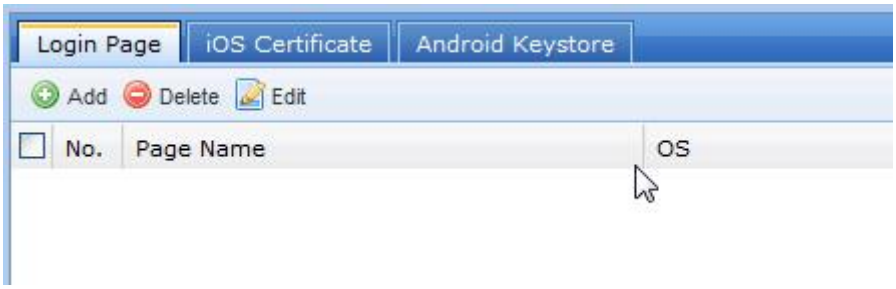
Auto Refresh: Configures refresh interval. Click **Refresh** to refresh the page, as shown below:



Select **Search by Name**, **Search by Type** or **Search by Status** to search for applications. Enter search term in **Search** and then click .



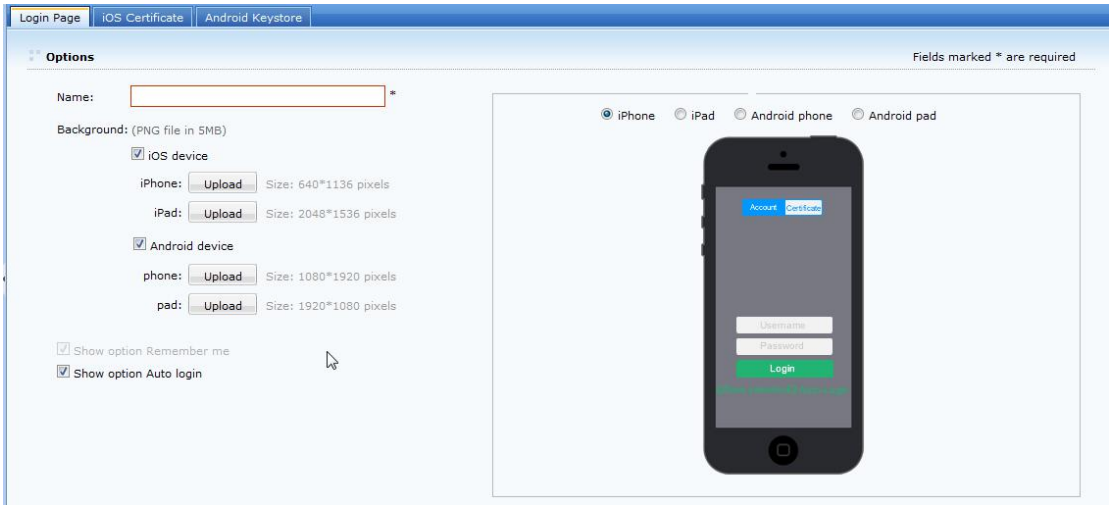
Click **Settings** to configure login page template and iOS certificate of App Wrapping, as shown below:



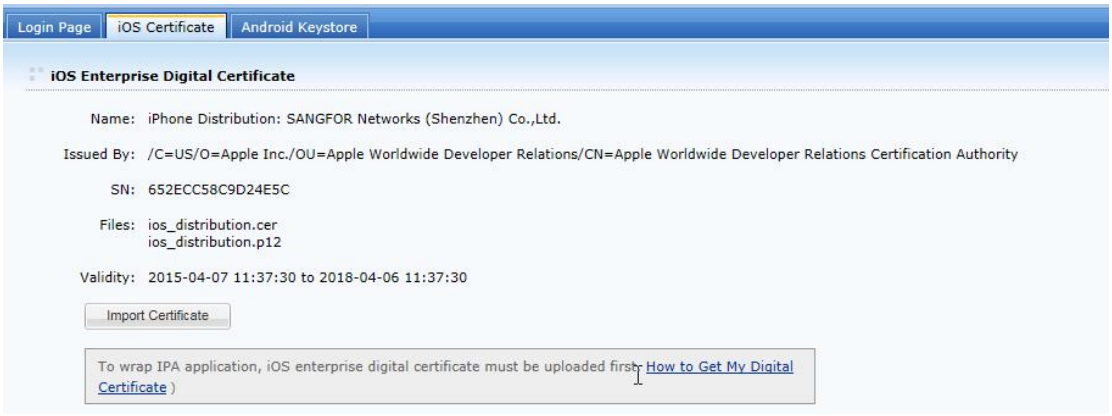
Click **Delete** to delete selected entry.

Click **Edit** to edit selected entry.

Click **Add** to add login page to VPN (Account or certificate based authentication). Upload iPhone, iPad, Android phone or Android Pad pictures, as shown below:

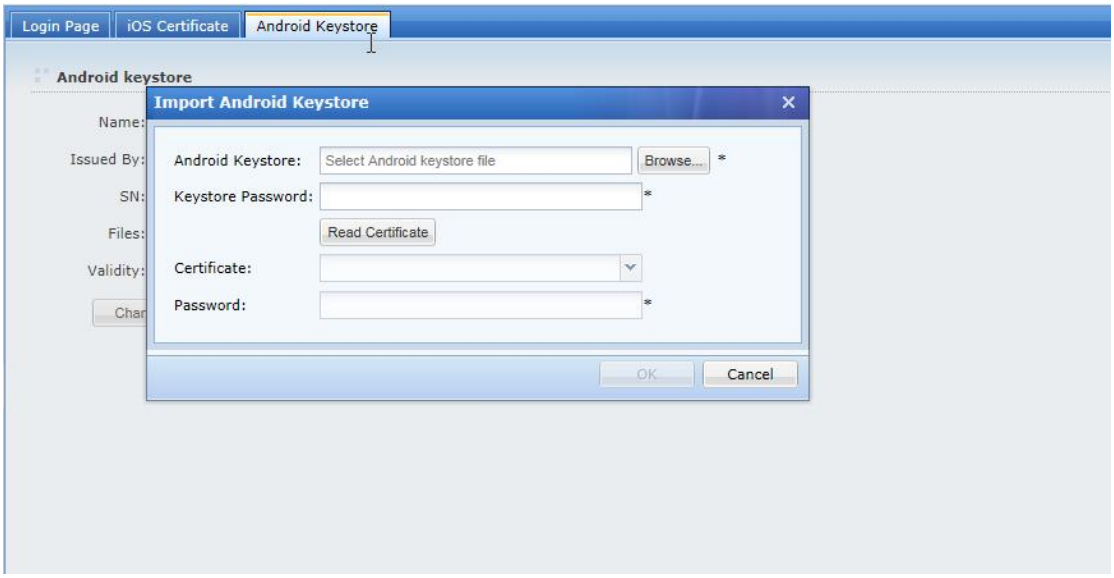


IOS Certificate: App wrapping for an .ipa file requires uploading an iOS enterprise digital certificate, as shown below:

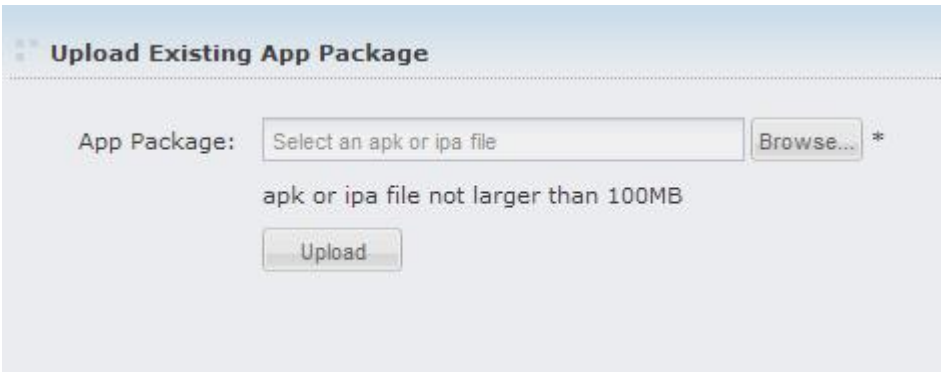


Upload iOS enterprise digital certificate, and then import iOS certificate, and wrap IPA application.

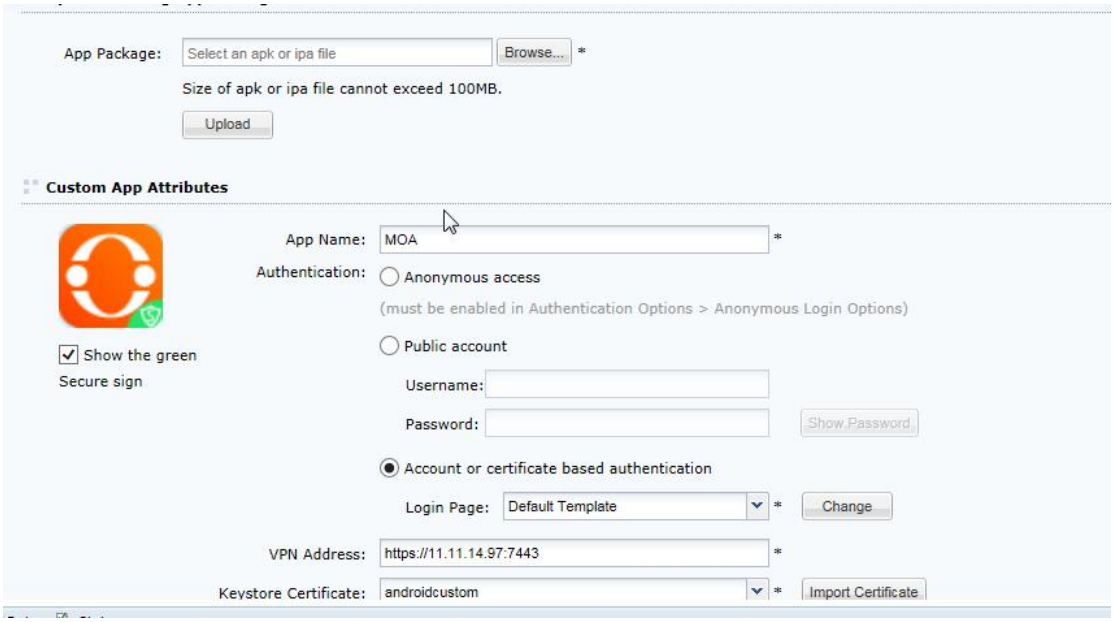
Android Keystore: Import Android Keystore to conduct APP wrapping for an .apk file, as shown below:



Click **Add** to add wrapping, as shown below:



Click **Browse...** to find an apk or ipa file, and click **Upload** to upload corresponding applications.



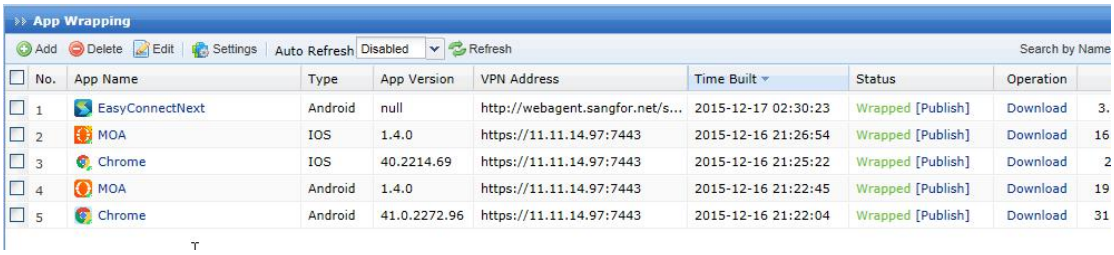
App Name: Name of the App

Authentication: Select **Anonymous access**, **Public account**, **Account or certificate based authentication**.

Anonymous access: Wrapped App anonymously accesses VPN. The anonymous access function should be enabled on SSL VPN with no authentication page.

Public account: Public account and password are required. Wrapped app accesses SSL VPN with the public account with no authentication page.

Account or certificate based authentication: Private authentication. Account is required for wrapped App to access SSL VPN. Download wrapped APP from console and install it.

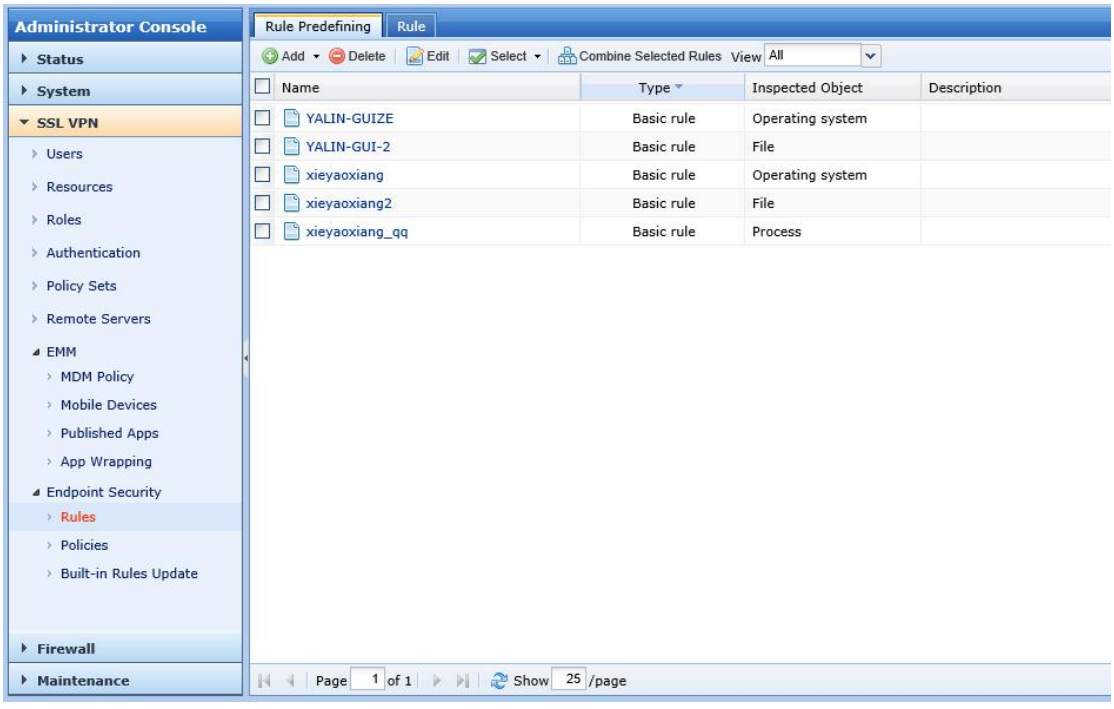


Endpoint Security

Endpoint security is ensured by host check at endpoint, based on security policies. Only when user's computer meets the requirements set by security policy can the user pass through pre-authentication or post-authentication check and connect to SSL VPN or access internal resources.

A security policy is a combination of predefined rules that fall into basic and combined rules and can further form a security rule. These rules are about operating system, file of anti-virus software, process, service pack installed, etc.

Pre-authentication check is carried out before user logs in to the SSL VPN. If user fails the pre-authentication check, which means, user fails to satisfy the requirements set by the associated security policy (user-level policy and/or role-level policy), he/she will be unable to access SSL VPN or the role's associated resource. Post-authentication check is carried out periodically, after user logs in to the SSL VPN or is accessing a resource. If user fails to satisfy the post-authentication check, which means, user fails to satisfy the requirements set by the associated security policy (user-level policy and/or role-level policy), the connection or session will be dropped. To conduct periodic check, administrator needs to set the interval (refer to the Configuring Advanced Policy Settings section in Chapter 4).



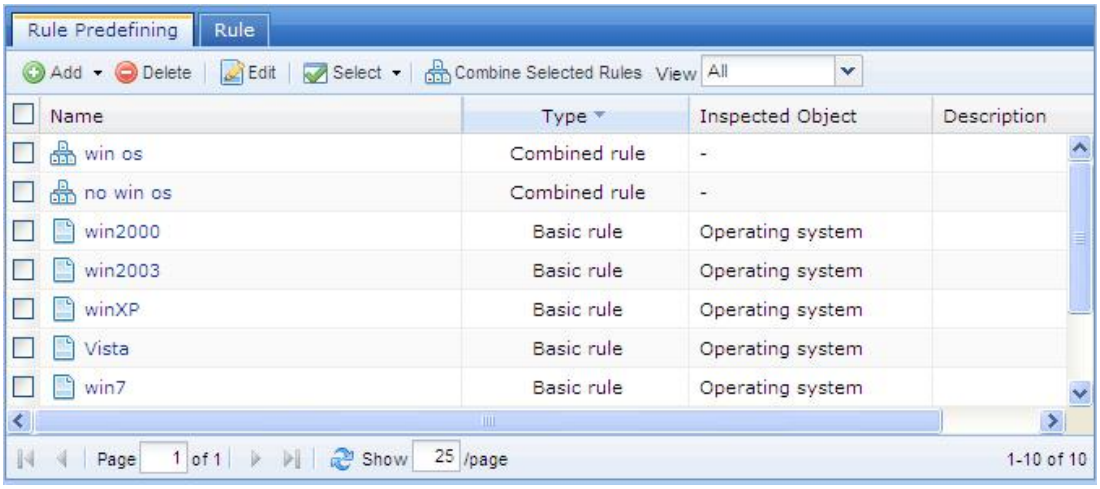
Security Rules

Security rule defining on the Sangfor device falls into two phases, the first phase is to predefine the rules that cannot be referenced directly by any security policy and should be combined with other basic rules and/or combined rules to form a "real" rule (security rule). The second phase is to

configure “real” rules. Only “real” rule can be referenced by security policy.

A basic rule is the smallest unit among the policy factors, while combined rule consists of one more basic rules. Basic rules and/or combine rules could be combined further to form “real” rule.

Navigate to **SSL VPN** > **Endpoint Security** > **Rules** to predefine security rules, as shown below:

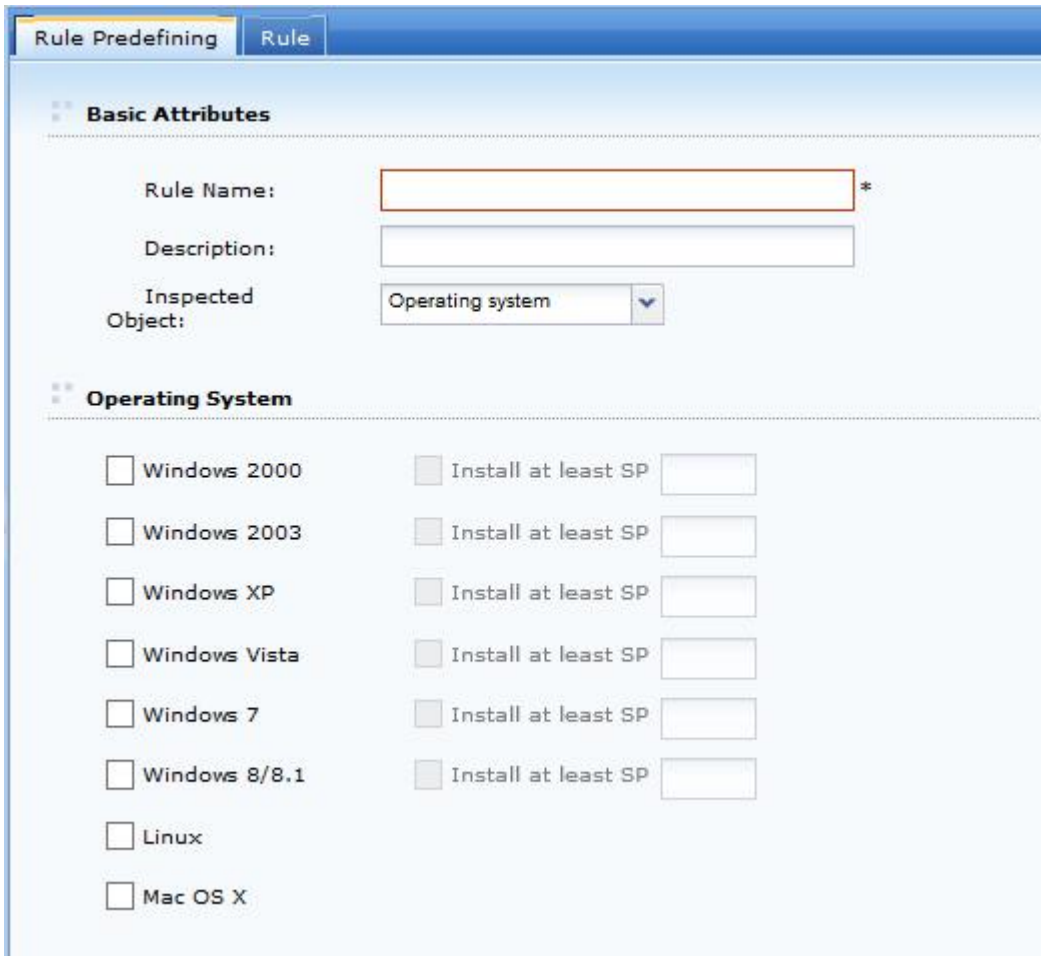


The following are the contents included on **Rule Predefining** page:

- **Name:** Indicates name of the rule.
- **Type:** Indicates type of the rule, basic rule or combined rule.
- **Inspected Object:** Indicates the object that will be checked if the connecting user does not satisfy the object restriction. Authentication check will fail. The objects are operating system, file, process, registry, source IP, WAN interface IP, login time and endpoint feature.
- **Add:** To add a new rule, click **Add** > **Basic rule** to configure a basic rule or **Add** > **Combined rule** to combine basic rules in one combined rule.
- **Delete:** Click it to delete the selected rule.
- **Edit:** Click it to edit the selected rule.
- **Select:** Click **Select** > **Current page** or **All pages** to choose the desired entries on this page or all pages; or click **Select** > **Deselect** to deselect entries.
- **View:** Select a type of rules, **All**, **Built-in rules** or **Custom rules**, to display that type of rules only.

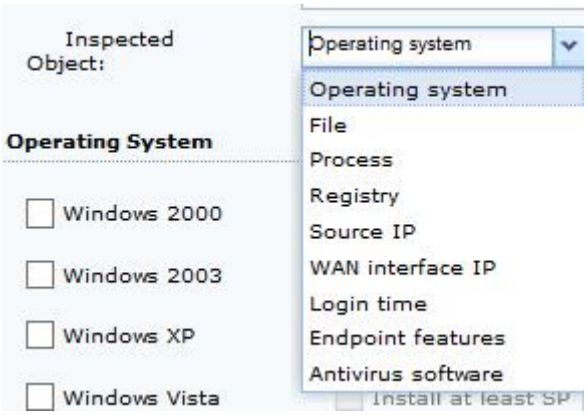
Predefining Basic Rule

1. Navigate to **SSL VPN** > **Endpoint Security** > **Rules** to enter the **Rule Predefining** page and click **Add** > **Basic rule**, as shown in the figure below:



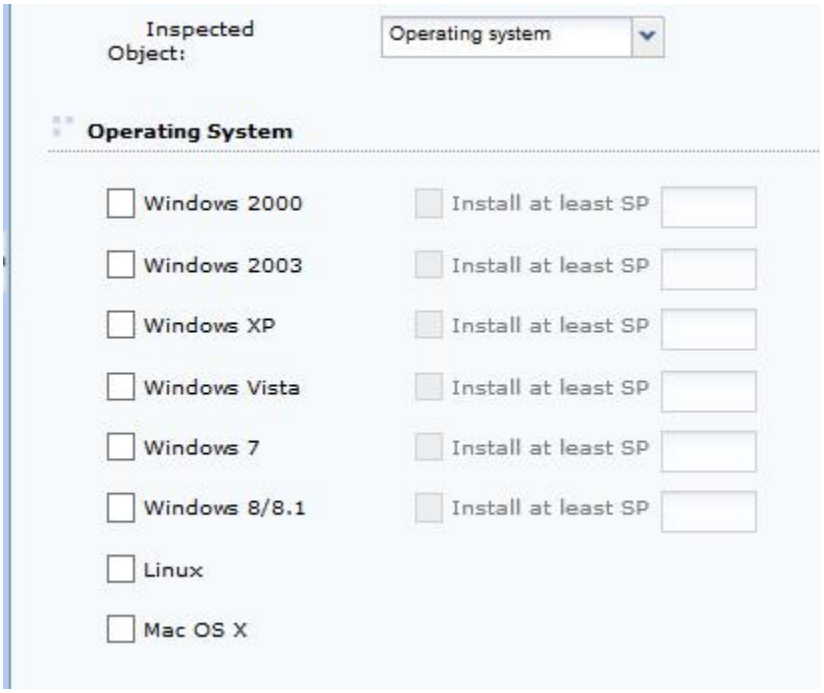
2. Configure the following fields on the above page.

- **Rule Name:** Configures the name of the basic rule. The rule name will be seen in a prompt when user fails to pass the authentication check.
- **Description:** Configures the description of the basic rule. The description will be seen in a prompt when user fails to pass the authentication check.
- **Inspected Object:** Configures the item that will be checked on user's computer and connecting user. Options are **Operating system**, **File**, **Process**, **Registry**, **Source IP**, **WAN interface IP**, **Login time**, **Endpoint features and Antivirus software** .



- **Operating System:** If the inspected object is **Operating system**, the options related to

operating system will appear, as shown in the figure below:



If any operating system is selected, the end user's PC must have installed the corresponding operating system if he or she wants to log in to SSL VPN.

For Windows OS, administrator can also specify the service pack (SP) that end users should install on their computer. Version number of the SP is entered in the **Install at least SP** field.

To save this rule, click the **Save** button.

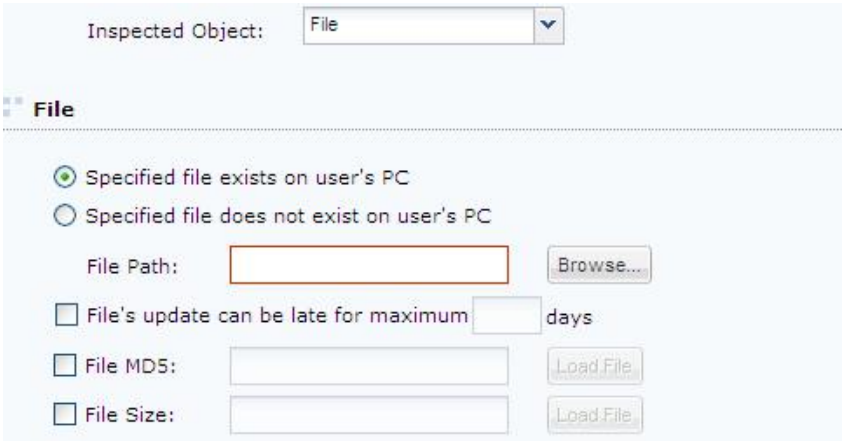
To save this rule and add another rule, not going back to the previous page, click the **Save and Add** button.

To cancel saving this rule, click the **Cancel** button.



If more than one operating systems are selected, the operating systems are with **OR** logic, that is to say, user would satisfy this rule if any of the selected operating systems is installed on user's computer. If SP is configured, the SP would be taken as a requirement for the operating system.

- **File:** If the inspected object is **File**, the options related to file will appear, as shown below:



The following are the contents under **File**:

- **Specified file exists on user's PC:** If this option is selected, the specified file must exist on the hard disk of user's computer. Otherwise, authentication check will fail.
- **Specified file does not exist on user's PC:** If this option is selected, the specified file should not exist on the hard disk of user's computer. Otherwise, authentication check will fail.
- **File Path:** Specifies the directory of the file on end user's computer. It can be absolute path, or system variable, such as, %SystemRoot%\log.txt.

  This field is required. The letters entered are case-insensitive.

- **File's update can be late for maximum _ days:** If this option is selected and a maximum of days is configured (for example, 5 days), the specified file's update should not lag behind over 5 days.
- **File Size:** If this option is selected and file size is obtained (click **Load File**, browse and select the file), size of the file on user's PC must be exactly the same with this file, that is to say, the file must not be edited by end user, otherwise, access to SSL VPN will be denied.
- **File MD5:** If this option is selected and MD5 of this file is obtained (click **Load File**, browse and select the file), contents in the file on user's PC must be exactly the same with this file, that is to say, the file must not be altered by end user, otherwise, access to SSL VPN or resource will be denied.

  The first time administrator clicks **Load File** to get MD5 or size of a file, the browser will ask whether the ActiveX control **WebUICtrl** has been installed, as shown in the figure below:

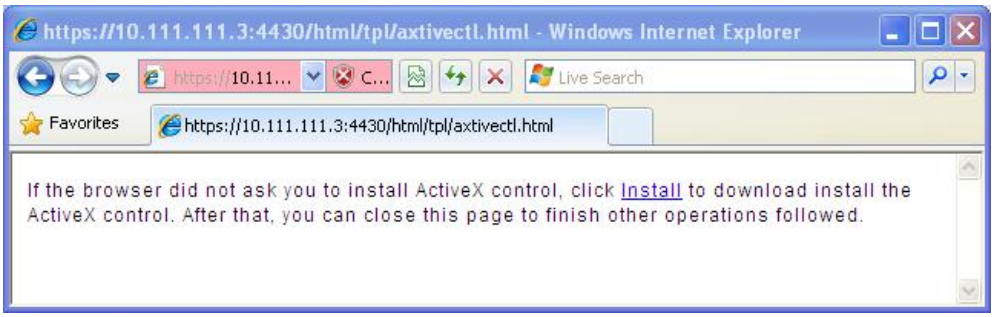


Click the **Check ActiveX Status** button to check if **WebUI Ctrl** has been installed. If not installed, click the **Install** button to enter another page and follow the pop-up prompt to install the ActiveX control.



When seeing the warning, click the **Install** button.

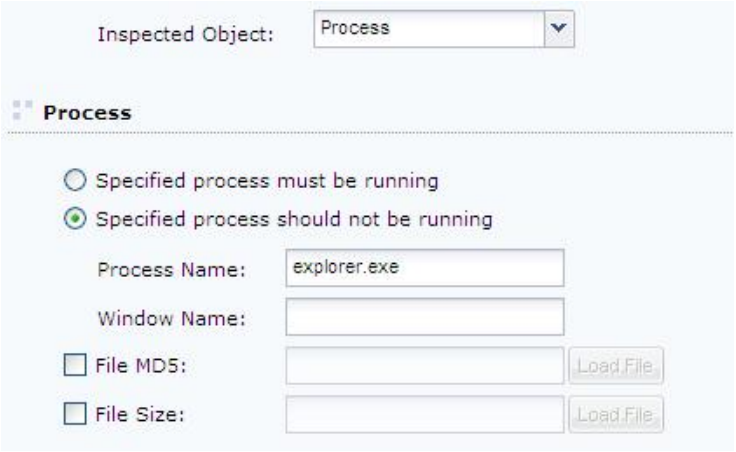
If the browser does not give any pop-up prompt of installing the ActiveX control, click the **Install** link to install it manually, as shown in the figure below:





The option under **File** are with **AND** logic. Only when all the options are satisfied will this rule is matched.

- **Process:** If the inspected object is **Process**, the options related to process will appear, as shown below:



The following are the contents under **Process**:

- **Specified process must be running:** If this option is selected, the specified process must exist on user's computer before and/or after user logs in to the SSL VPN or resource. Otherwise, authentication check will fail.
- **Specified process should not be running:** If this option is selected, the specified process should not exist on user's computer before and/or after user logs in to the SSL VPN or resource. Otherwise, authentication check will fail.
- **Process Name:** Specifies the name of the process that will be checked on end user's computer.
- **Window Name:** Specifies the name of the window in which the process runs.
- **File MD5:** If this option is selected and MD5 hash checksums of this file is obtained (click **Load File**, browse and select the file), contents in the file on user's PC must be exactly the same with this file, that is to say, the file must not be altered by end user, otherwise, access to SSL VPN or resource will be denied.
- **File Size:** If this option is selected and file size is obtained (click **Load File**, browse and select the file), size of the file on user's PC must be exactly the same with this file, that is to say, the file must not be edited by end user, otherwise, access to SSL VPN or resource will be denied.



The option under **File** are with **AND** logic. Only when all the options are satisfied will this rule is matched.

- **Registry:** If the inspected object is **Registry**, the options related to registry will appear, as shown below:



The following are the contents under **Registry**:

- **Specified item exists in registry:** If this option is selected, the specified item must exist in the registry of user's computer before and/or after user logs in to the SSL VPN or resource. Otherwise, authentication check will fail.
- **Specified item does not exist in registry:** If this option is selected, the specified item should not exist in the registry of user's computer before and/or after user logs in to the SSL VPN or resource. Otherwise, authentication check will fail.
- **Key:** Specifies the key that will be checked. It should be the location of the key in the registry.

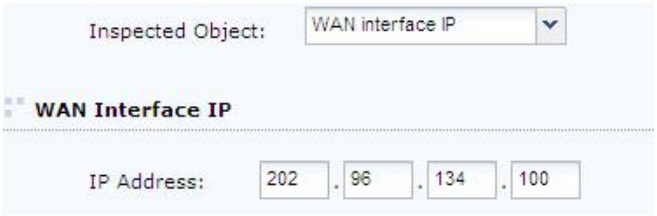
The option under **Registry** are with **AND** logic. Only when all the options are satisfied will this rule is matched.

- **Source IP:** If the inspected object is **Source IP**, the contents are as shown below:



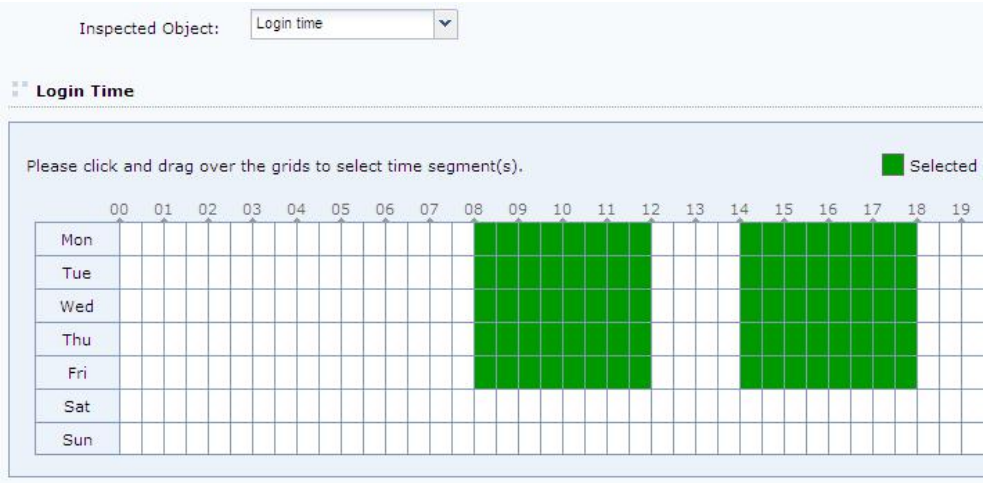
Start IP, End IP: Specifies the start IP address and end IP address of the IP range IP range from which user can log in to SSL VPN.

- **WAN Interface IP:** If the inspected object is **WAN Interface IP**, the contents are as shown below:



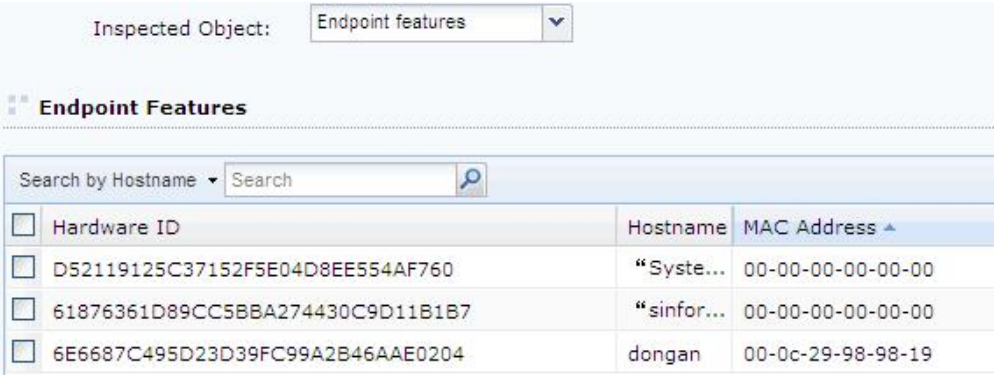
IP Address: Specifies the IP address of the WAN interface on Sangfor device. End user can connect to SSL VPN only through this WAN interface.

- **Login Time:** If the inspected object is **Login time**, the contents are as shown below:



In the above figure, the green part is selected time segments while white part is unselected time segments. Configuration is the same as that in Schedules section.

- **Endpoint Features:** If the inspected object is **Endpoint features**, the contents are as shown below:



The hardware IDs listed under **Endpoint Features** come from **Hardware ID** page (please refer to the Managing Hardware IDs section in Chapter 4).

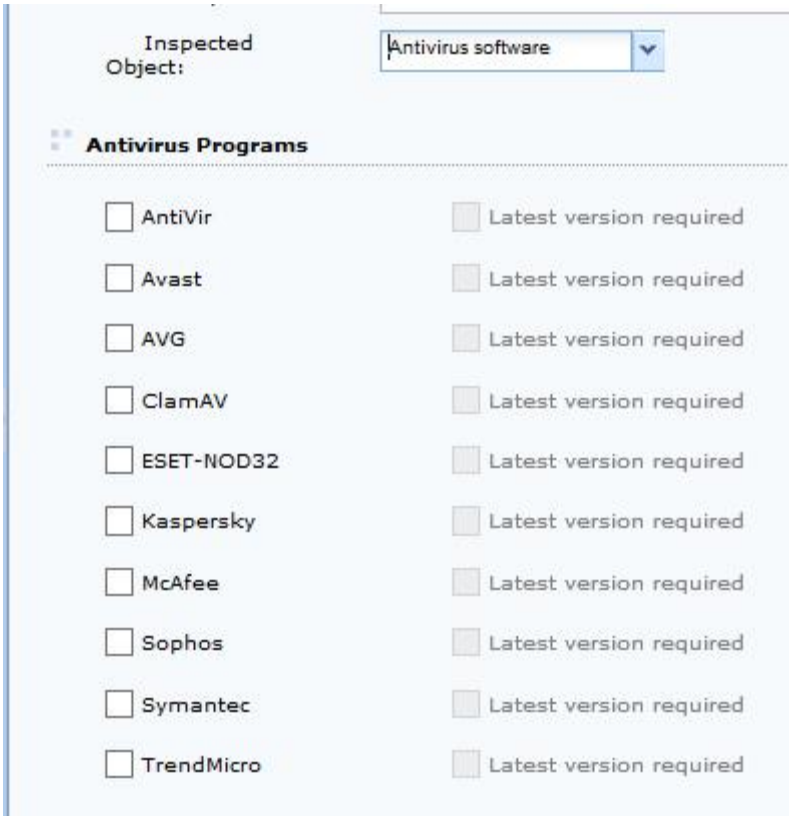
To select an entry, select the checkbox next to the entry. Selecting entry or entries means that the connecting user must have at least one of the hardware IDs. Otherwise, authentication check will fail.

To view the hardware IDs in descending or ascending order by hardware ID, hostname or MAC address, click on the column header, **Hardware ID**, **Hostname** or **MAC**

Address respectively.

To search for a specific entry, click **Search by Hostname/MAC Address**, enter the keyword and click the magnifier icon .

- **Antivirus Software:** If the inspected object is antivirus software, the contents are as follows:



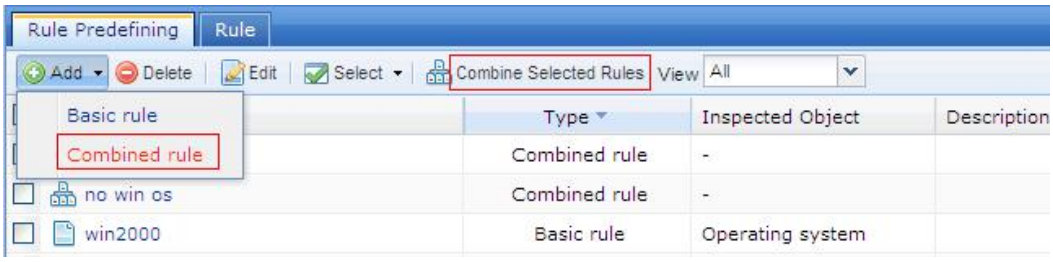
If any antivirus program is selected, the end user's PC must have installed the corresponding program if he or she wants to log in to SSL VPN. If **Latest version required** is also selected, user is required to install latest version of corresponding antivirus program.

If more than one antivirus programs are selected, the antivirus programs are with **OR** logic, that is to say, user would satisfy this rule if any of the selected antivirus programs is installed on user's computer. If **Latest version required** is selected, the latest version would be taken as a requirement for the antivirus program.

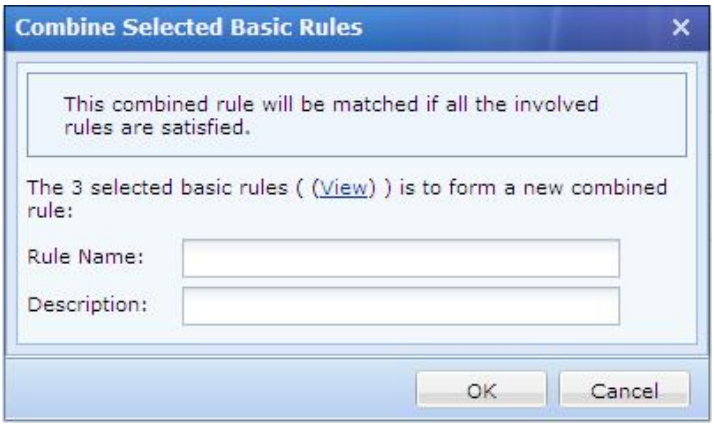
3. Click the **Save** button to save the settings.

Predefining Combined Rule

1. Navigate to **SSL VPN** > **Endpoint Security** > **Rules** to enter the **Rule Predefining** page and click **Add** > **Combined rule**, or click **Combine Selected Rules**, as shown below:



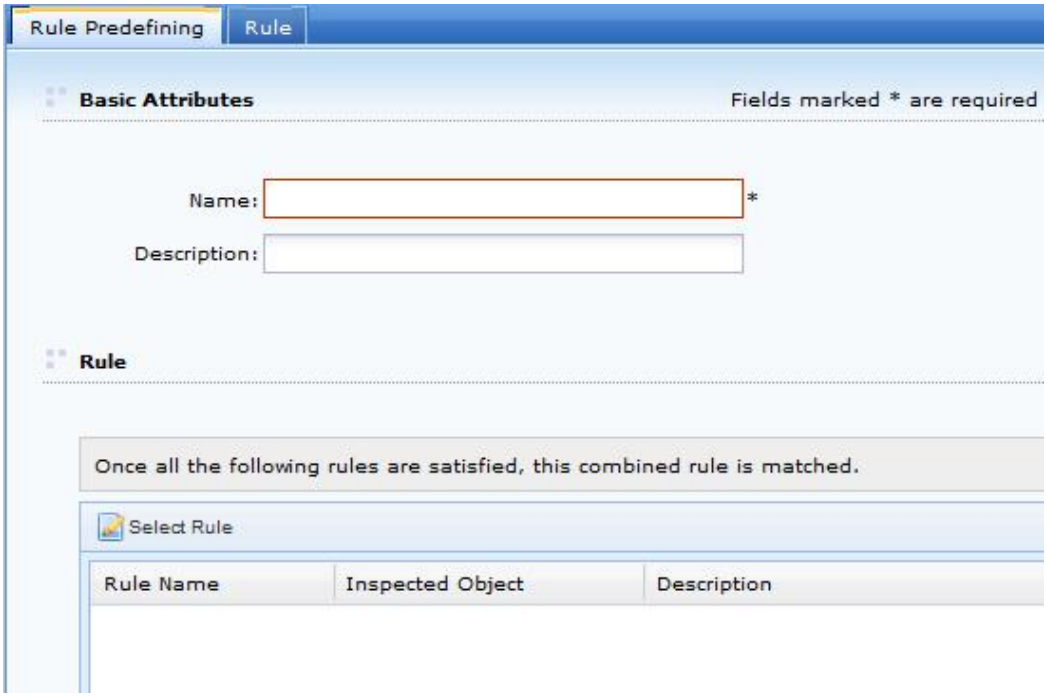
To use **Combine Selected Rules**, select the desired basic rules first and then click **Combine Selected Rules** to create a combined rule with the selected basic rules, as shown below:



Combined rule can only consist of basic rules. To view the selected basic rules that are to be included in this combined rule, put the cursor on **View**.

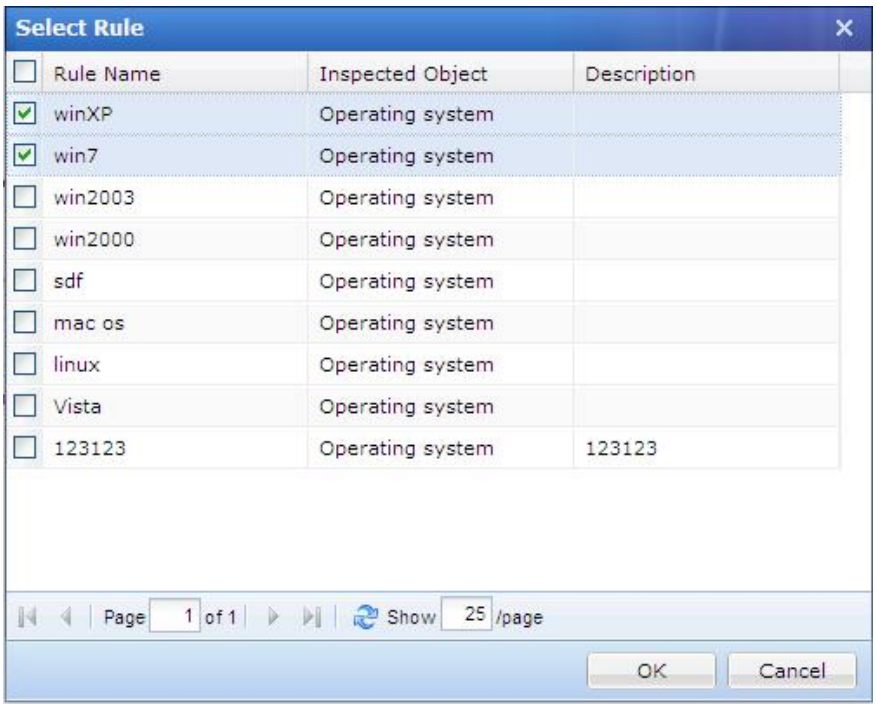
Enter name and description for this new combined rule and click the **OK** button to save the settings.

2. Or click **Add** > **Combined rule** to configure the combined rule, as shown below:



- **Name:** Configures the name of the combined rule.
- **Description:** Configures the description of the combined rule.

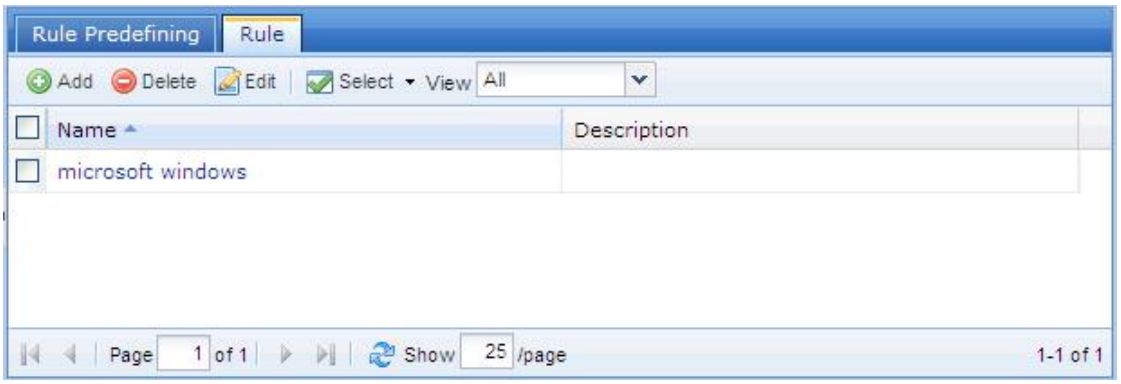
3. Click **Select Rule** to enter the **Select Rule** page and specify the basic rules that this combined rule will include. The **Select Rule** page shows all the predefined basic rules, as shown below:



4. Click the **OK** button to close the above page.
5. Click the **Save** button and then the **Apply** button to save and apply the settings.

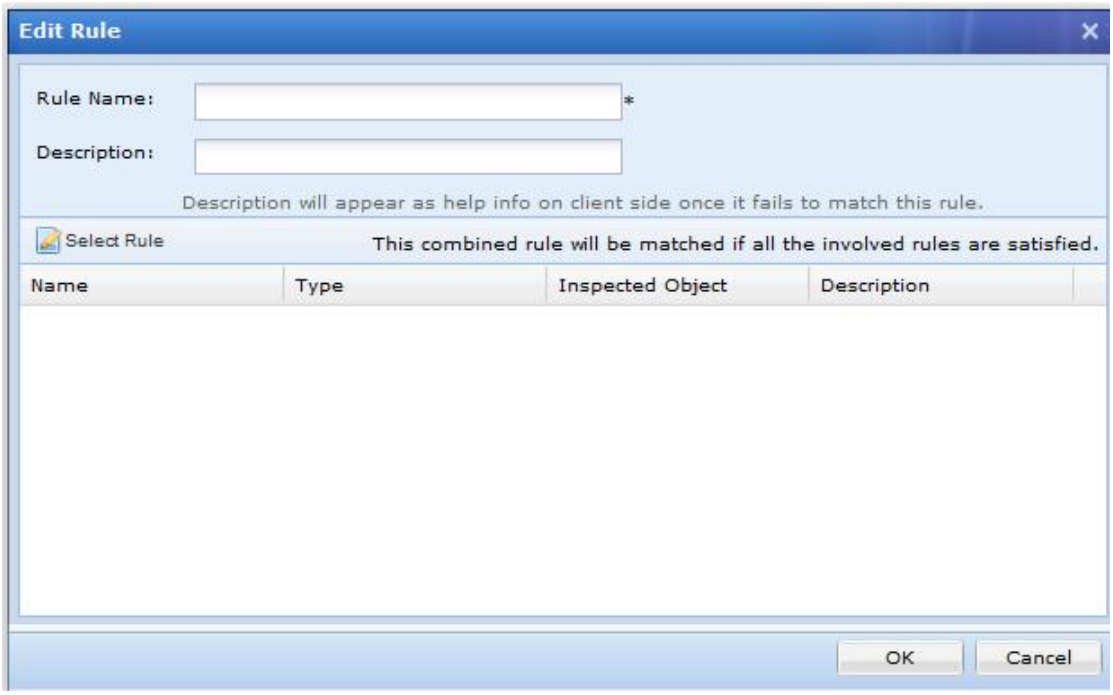
Configuring Security Rule

Security rule consists of basic rules and/or combined rules. When the connecting user satisfies one of these basic or combined rules, the security rule is matched. If the connecting user satisfies none of the basic or combined rules, the security rule will not be matched and user will fail the authentication check.



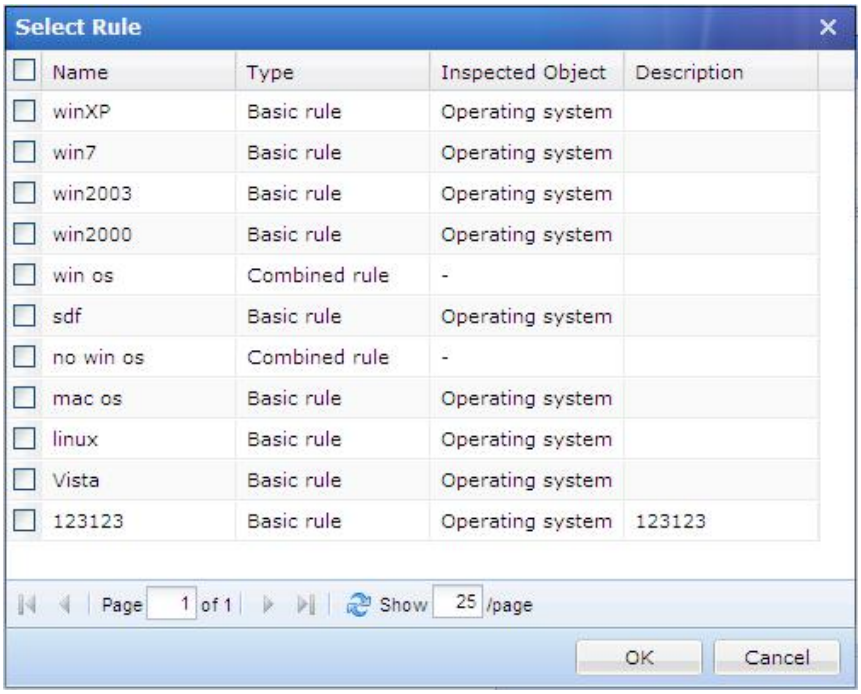
To add a security rule:

1. Navigate to **SSL VPN** > **Endpoint Security** > **Rules** > **Rule** and click **Add** to enter the **Edit Rule** page, as shown in the figure below:



2. Configure name and description for the security rule.
3. Click **Select Rule** to enter the **Select Rule** page and specify the basic rules that this combined rule will include.

   The **Select Rule** page shows all the predefined basic rules, as shown in the figure below:



4. Click the **OK** button to close the above page.

5. Click the **Save** button and then the **Apply** button to save and apply the settings.

The rules in the security rule are with **OR** logic. If any of the basic or combined rules is satisfied, the security rule is matched.

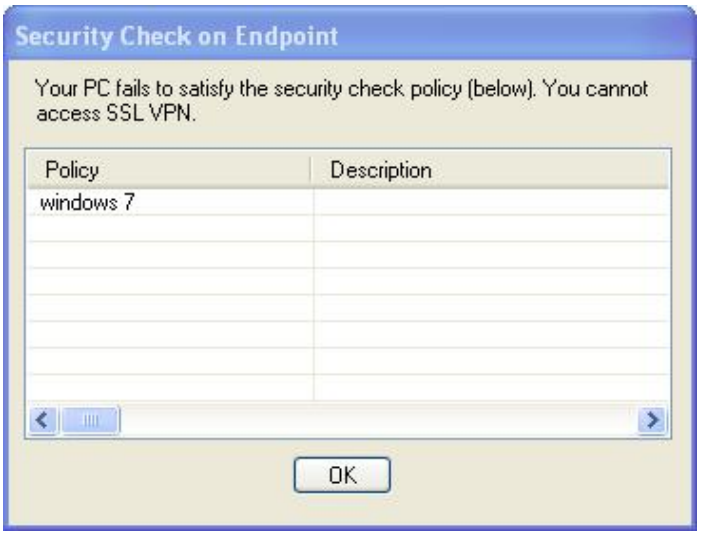
Policies

Based on security policy, endpoints will be checked when users connect to or have logged in to SSL VPN. There are two types of security policies. One is user-level policy and the other is role-level policy.

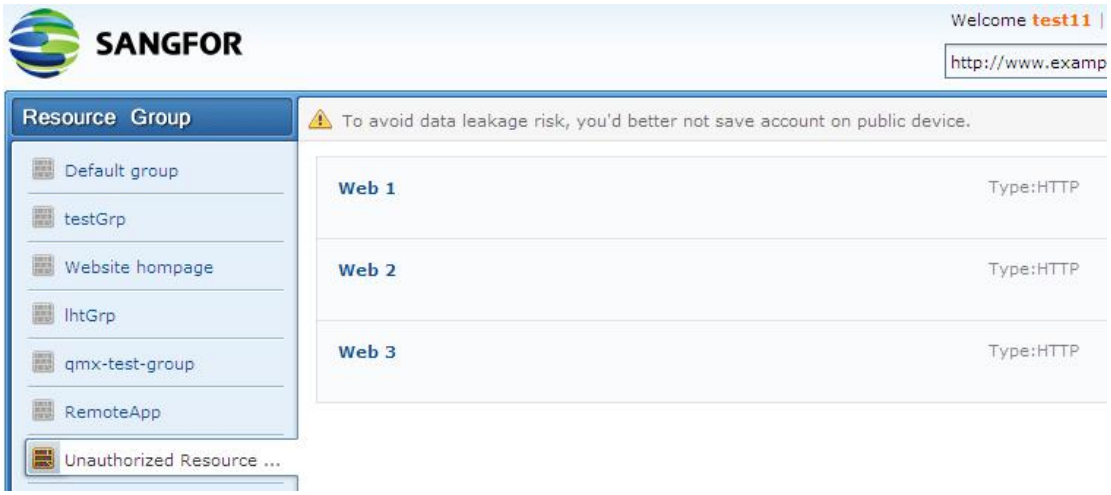
User-level policy is applied to users and checks the endpoints when users access SSL VPN (pre-authentication check) or after users log in to SSL VPN (post-authentication check). The connecting users have to satisfy the basic or combined rules included in the associated user-level policy. If the policy is satisfied, end users can enter the login page or stay connected to the SSL VPN, as shown in the figure below:



If user fails the security check, he or she will be informed of the security policy that makes him or her fail the security check, as shown in the figure below



Role-level policy is applied to roles that are associated with users, and checks the endpoint when the associated users access SSL VPN (pre-authentication check) or are accessing to the resource (post-authentication check). The connecting users have to satisfy basic or combined rules included in the associated role-level policy. If the policy is satisfied, end users can visit the associated resource or continue accessing the resource over SSL VPN; otherwise, security check will fail and the associated resources will be put into **Unauthorized Resource List** and therefore be unavailable to users, as shown in the figure below:

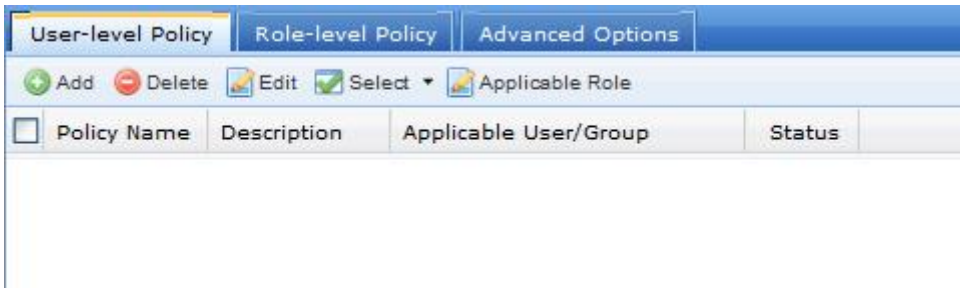


Click on any of the unauthorized resources, a prompt will pop up telling user which policy he or she fails to comply with, as shown in the figure below:



In case that a user is tied to a user-level policy and its associated role is tied to a role-level policy, when the user connects to SSL VPN, he/she goes through user-level security check first. If user fails the user-level security check, he/she cannot log in to the SSL VPN. Once user passes the user-level security check, he/she will then goes through role-level security check, however, if user fails to pass role-level security check, the role's associated resources will be put into the **Unauthorized Resource List** and be unavailable to the user.

Navigate to **SSL VPN** > **Endpoint Security** > **Policies** and the **User-level Policy** page appears, as shown in the figure below:

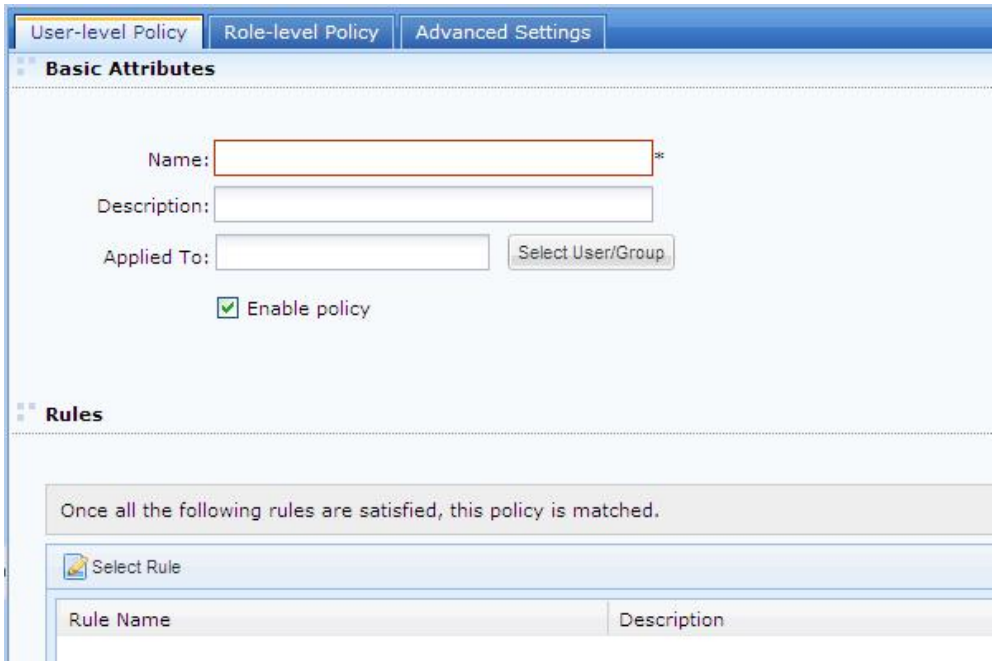


The following are the contents included on **User-level Policy** page:

- **Policy Name:** Indicates name of the user-level policy.
- **Description:** Indicates description of the user-level policy.
- **Applicable User/Group:** Indicates the users and/or groups that are associated with the user-level policy.
- **Status:** Indicates the status of the security policy, enabled or disabled.
- **Add:** Click it to add a new user-level policy.
- **Delete:** Click it to remove the selected user-level policy from the list.
- **Edit:** Click it to edit a selected user-level policy.
- **Select:** Click **Select > All pages** or **Current page** to select all the entries or only those showing on the present page; or click **Select** > **Deselect** to deselect entries.
- **Applicable Role:** Select and click a user-level policy to view the user and/or group to which this policy is applied. You can also select more users or remove user from the list.

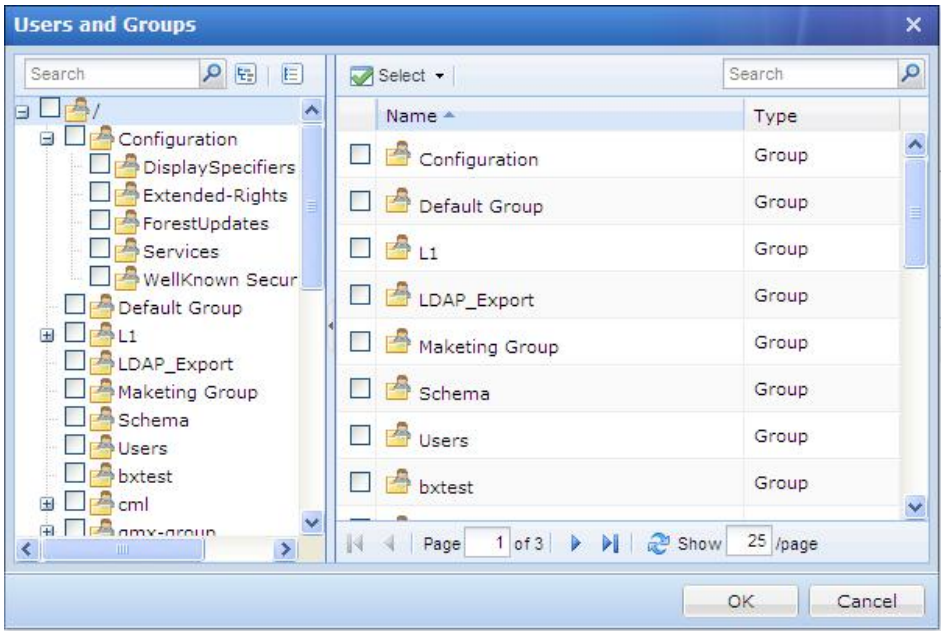
Adding User-Level Policy

1. Navigate to **SSL VPN** > **Endpoint Security** > **Policies** to enter the **User-level Policy** page and click **Add**, as shown below:



2. Configure the **Basic Attributes** of the user-level policy. The following are basic attributes:

- **Policy Name:** Configures name of the user-level policy.
- **Description:** Configures description of the user-level policy.
- **Enable Policy:** Select this option to enable the policy.
- **Applied To:** Click the **Select User/Group** button to enter the **Users and Groups** page and select the users and/or groups that are to be associated with this user-level policy. The applicable users' computer will be checked based on this user-level policy when the users connect to or have logged in to SSL VPN. The **Users and Groups** is as shown below:



To search for certain group, enter the group name into the **Search** filed on the left pane,

and click the magnifier icon . The user group will be highlighted in bold if found.

To search for certain user, enter the user name into the **Search** filed on the right pane, and click the magnifier icon .

To unfold all the groups and see all the users under the selected group, click **Unfold all** .

To fold all the groups and click **Fold all** .

To select all the subgroups of a group, select the group on the left pane, click **Select** > **Group** > **Select all subgroups** on the right pane.

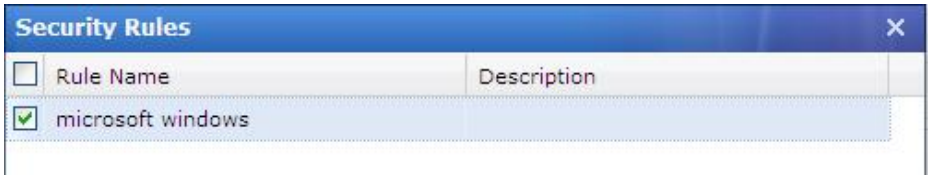
To deselect all the subgroups of a group, select the group on the left pane, click **Select** > **Group** > **Deselect all subgroups** on the right pane.

To select all the direct users of a group, select the group on the left pane, click **Select** > **User** > **Select all immediate users** on the right pane.

To deselect all the direct users of a group, select the group on the left pane, click **Select** > **User** > **Deselect immediate users**.

To save the settings, click the **OK** button.

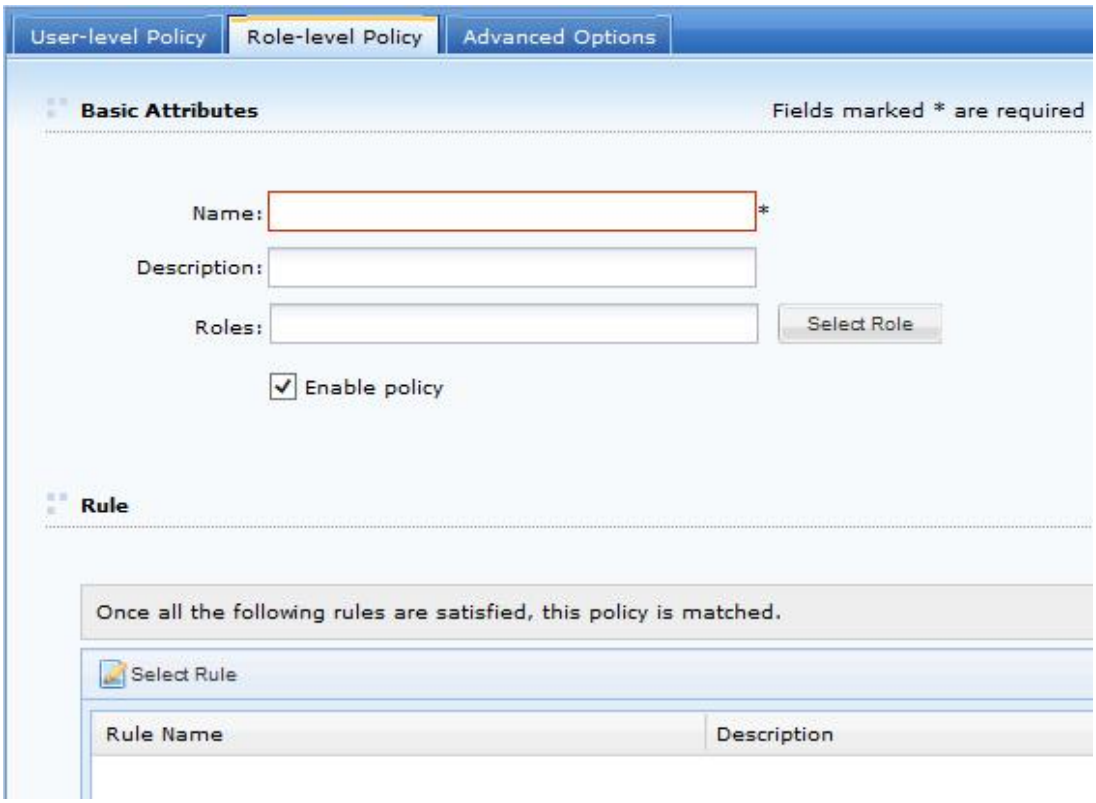
3. Specify the security rules that will be included in this policy and applied to the associated users and/or groups. Click **Select Rule** to enter the **Security Rules** page and select the rule, as shown in the figure below:



4. Click the **Save** button to save the setting.

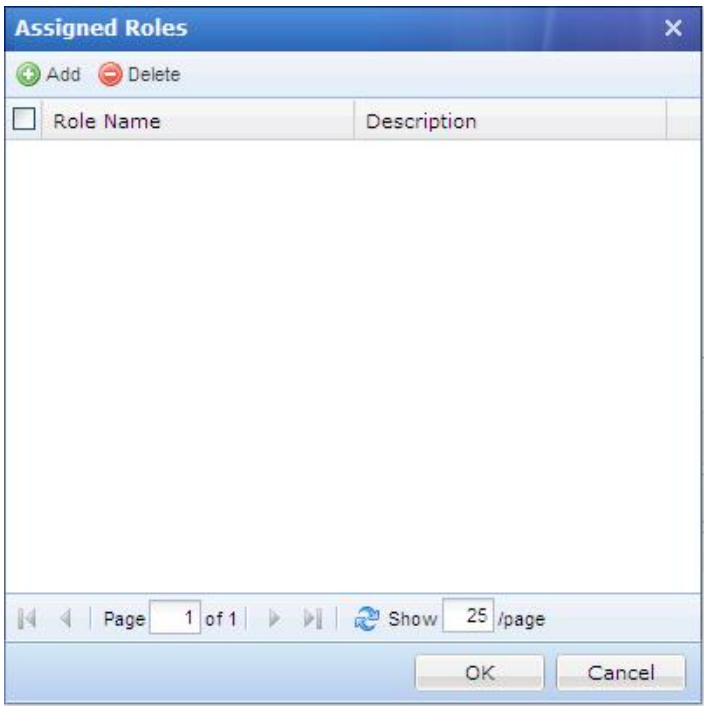
Adding Role-level Policy

1. Navigate to **SSL VPN** > **Endpoint Security** > **Policies** > **Role-level Policy** page and click **Add**, as shown below:

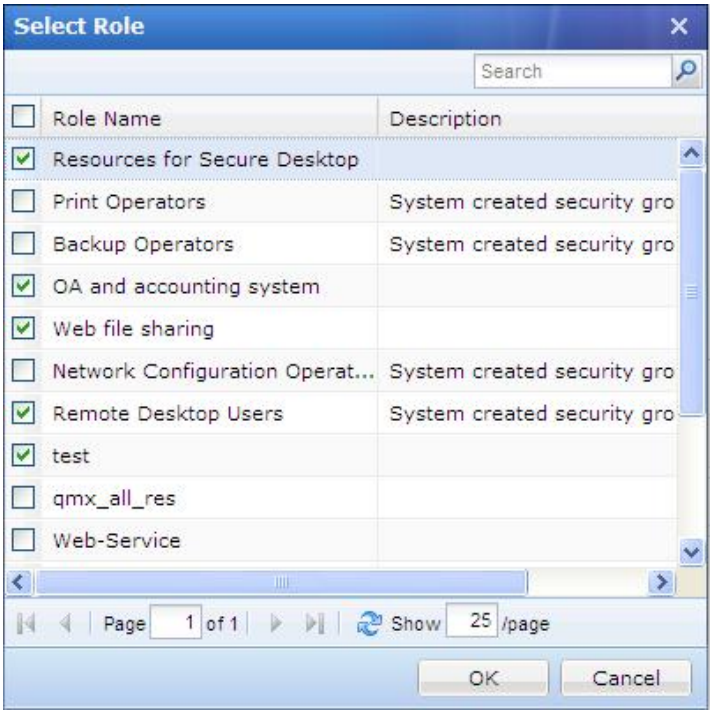


2. Configure the **Basic Attributes** of the role-level policy. The following are basic attributes:

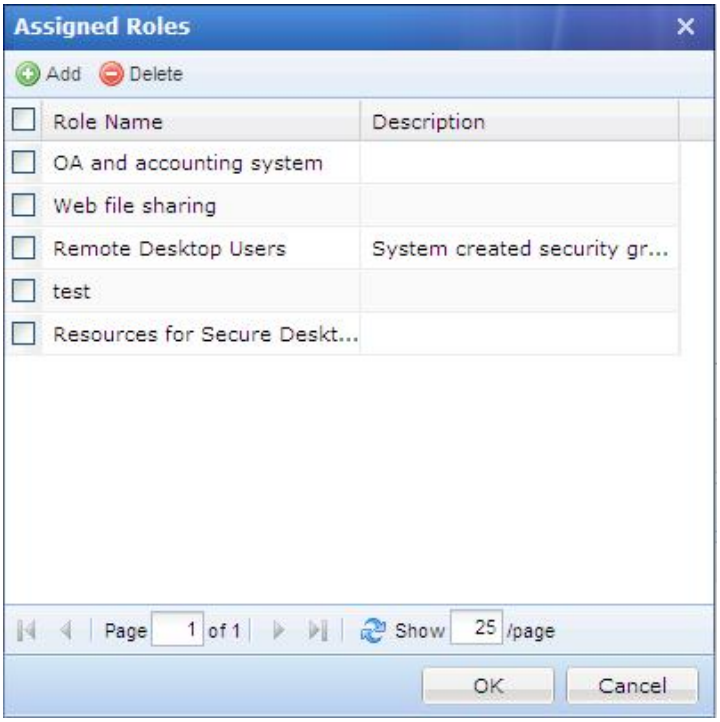
   - **Name:** Configures name of the role-level policy.
   - **Description:** Configures description of the role-level policy.
   - **Roles:** Click **Select Role** to enter the **Assigned Roles** page, and then select the roles that are to be associated with this security policy. Computers of the users corresponding to the selected roles will be checked based on this role-level policy when the users log in to SSL VPN. The **Assigned Roles** page is as shown in the figure below:



To select and add role, click **Add** to enter the **Select Role** page, as shown below:



Select the desired roles and click the **OK** button, and the selected roles are added to the assigned roles list, as shown in the figure below:



To remove a role from the list, select the role and click **Delete**.

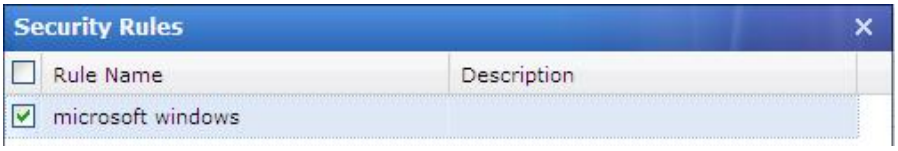
To add more roles, click **Add** again, select and add other roles into the list.

To save the settings, click the **OK** button.



Before selecting the desired role, make sure the role has been created. For detailed guide on how to configure role, refer to the Adding Role section in Chapter 4.

5. Specify the security rules that will be included in this policy and applied to the associated users and/or groups. Click **Select Rule** to enter the **Security Rules** page and select the rule, as shown in the figure below:



6. Click the **Save** button to save the setting.

Configuring Advanced Policy Settings



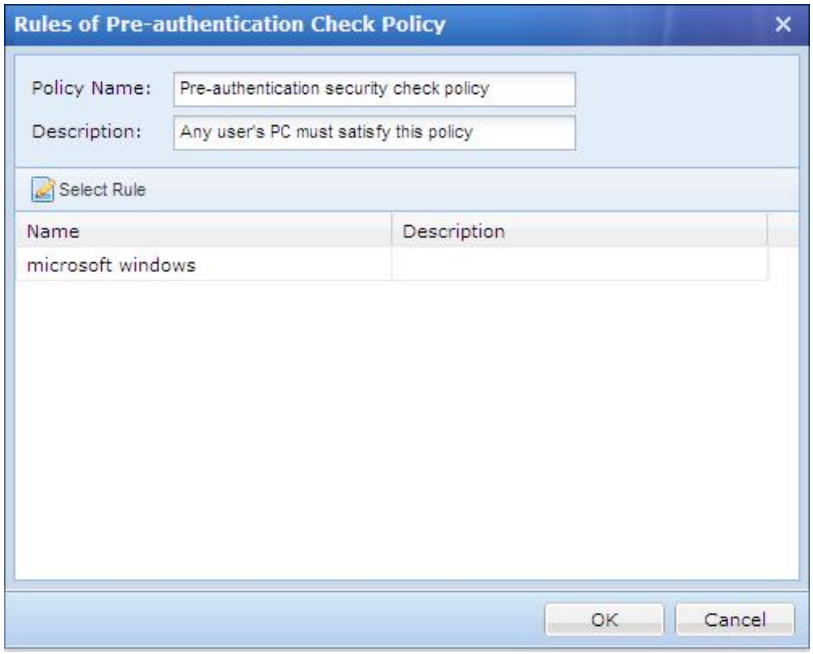
As mentioned above, there are check before login and post-authentication check. Post-authentication is conducted periodically after user's login to SSL VPN or access to resource.

The following are the contents included on **Advanced Settings** page:

- **Perform check before login:** Select this option and endpoint security check will be conducted on connecting users when they log in to SSL VPN. Once users fail the check, they cannot log in. Administrator needs to click the **Select a Solution** link to enter the **Client Options** page and choose a solution.

  This option is a global setting. Once it is selected, pre-authentication check will apply to all the users connecting to SSL VPN.

- **Pre-authentication Check Policy:** Click this button to enter the **Rules of Pre-authentication Check Policy** page to select the security rules that will be included in this policy, as shown in the figure below:



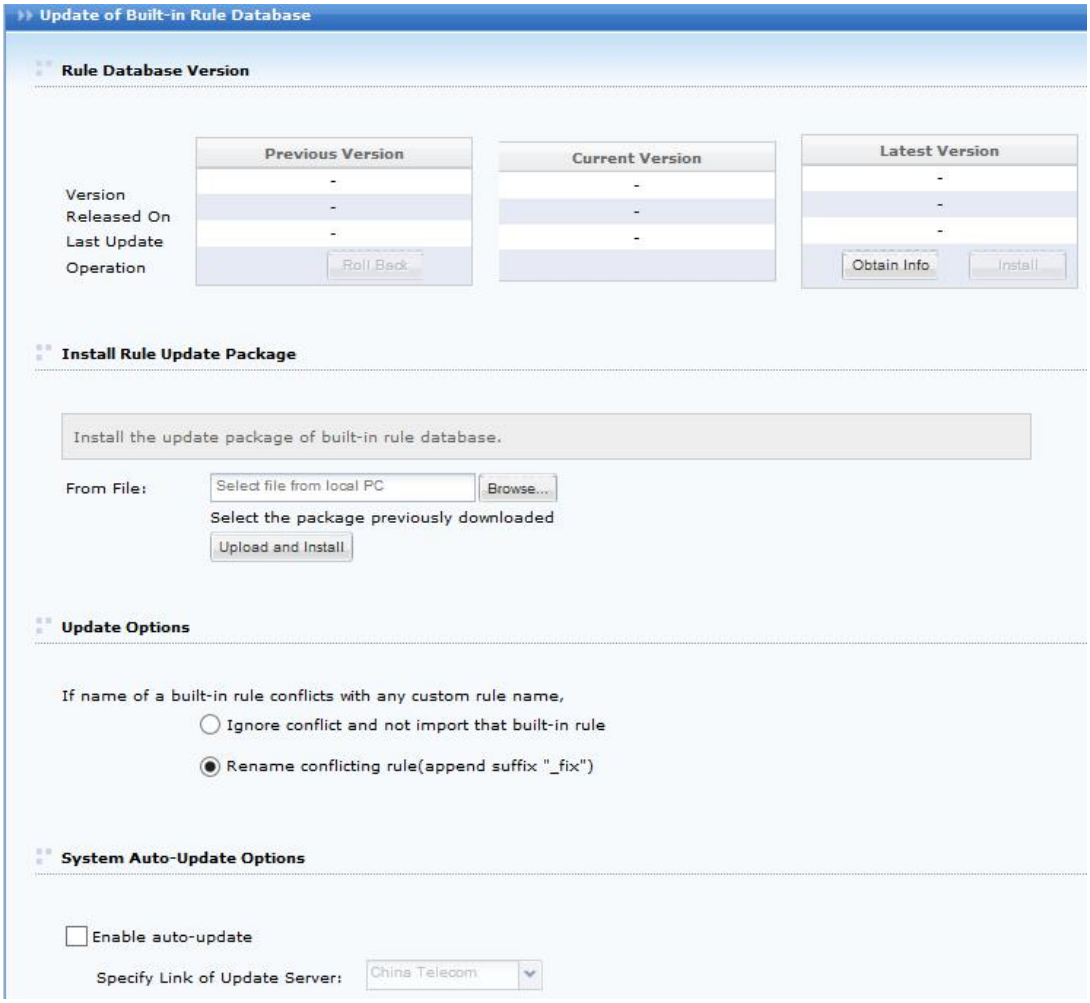
- **Post-authentication Check:** Select this option and endpoint security check on connecting users will be conducted periodically after they have connected to the SSL VPN. Administrator needs to configure the time interval for periodical check. Enter the time interval into **Every** field. The interval is in minute and ranges from 1 to 60.

When users log in to the SSL VPN, they will go through user-level security check first and then role-level security check.

Built-in Rules Update

Built-in rules are a set of rules provided by SANGFOR, more specifically, a database of commonly-used security rules that will be updated periodically.

Navigate to **SSL VPN** > **Endpoint Security** > **Built-in Rules Update**, and the **Update of Built-in Rule Database** page appears, as shown in the figure below:



The following are the contents included on **Built-in Rules Update** page:

- **Rule Database Version:** Shows the information of the rule database, the previous version, current version on the Sangfor device, and the latest version.
- **Roll Back:** Click this button and the current rule database will roll back to the previous version that this Sangfor device was using.
- **Obtain Info:** Click this button and information of the latest version of rule database will be obtained. To do so, administrator needs to specify the update server.
- **Install:** Click this button to install the latest rule database.
- **Install Rule Update Package:** Browse and load the rule update package through **From File** field, and then click the **Upload and Install** button. Before browsing the update package from the PC, administrator needs to click the **Download** link and go to the SANGFOR official website to download the update package by hand.
- **Update Options:** During update process, if name of a built-in rule conflicts with name of an existing custom rule, update will proceed but that built-in rule will not be imported or a suffix "_fix" will be appended to the name of that built-in rule.
- **Auto-Update Options:** Select **Enable auto-update** and specify the link to the update server, and the Sangfor device will check for updates on the specified update server to update the

built-in rules automatically.

- **Save:** Click this button to save the settings.

Chapter 5 Firewall

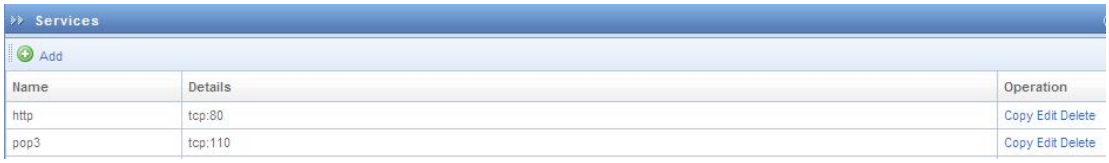
The Sangfor device, integrated the enterprise-level stateful firewall with high availability, can protect enterprise network against attacks initiated from Internet or other local area networks connected to VPN. Besides, the built-in anti-DoS function enables the Sangfor device to defend against DoS attacks from extranet as well as inside the intranet.

Defining Firewall Service

As the software and communication applications running over network may use different transfer protocols and ports, you need to define these transfer protocols and ports here before configuring the corresponding filter rules.

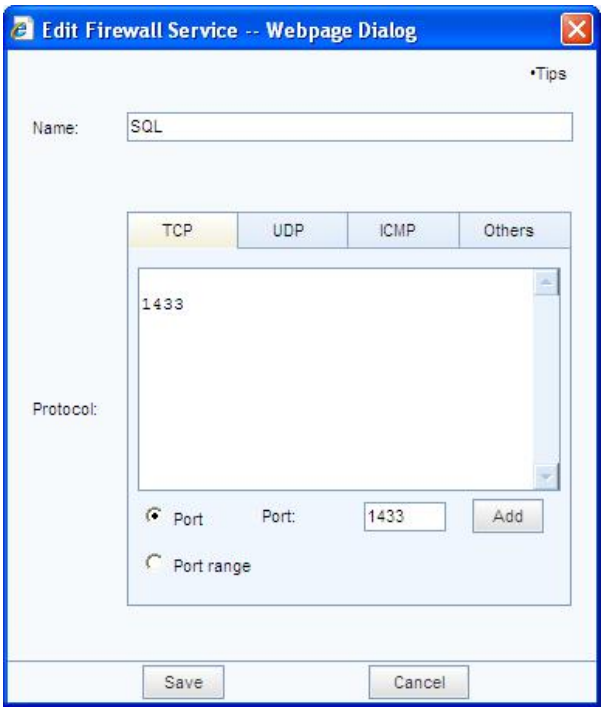
Note: The firewall setting module only supports IPv4 addresses and does not support IPv6 addresses.

Navigate to **Firewall** > **Services** to enter the **Services** page, as shown below:



For example, to configure filter rules on Sangfor device to filter the service data of SQL server, you need first define the protocol and port used by the SQL server.

Click **Add** to enter the **Edit Firewall Service** page, as shown below.

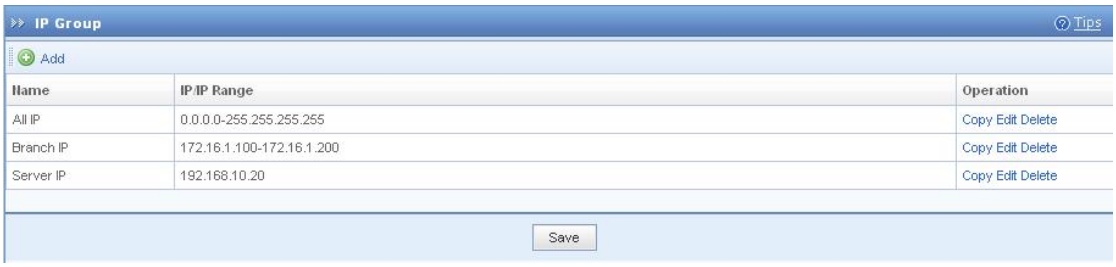


Then specify the service name, protocol and port, and click **Save** to save the settings.

Defining IP Group

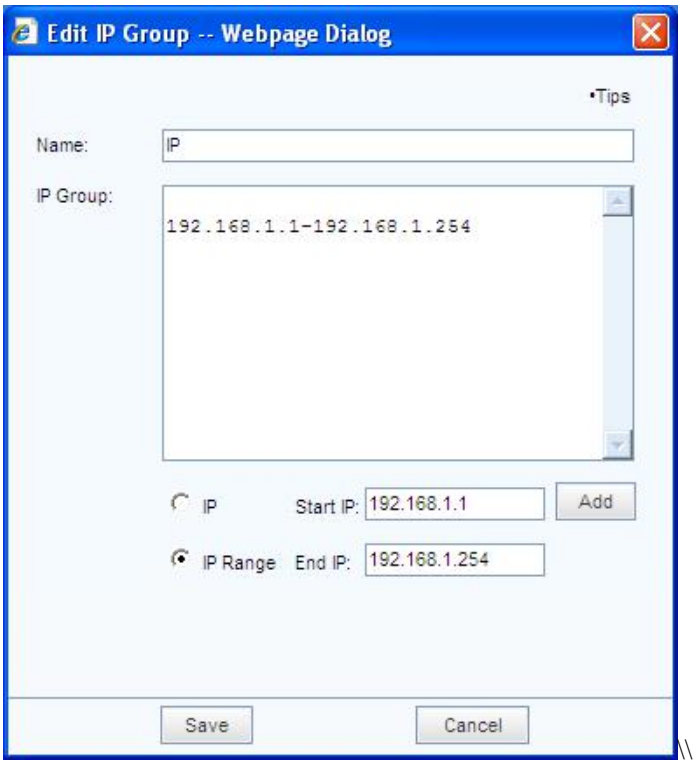
IP groups are predefined objects that can be referenced by firewall rules, as source or destination IP address.

To view and define IP group, navigate to **Firewall > IP Group** to enter the **IP Group** page, as shown below:



For example, to configure filter rules specific to the data requested from the 192.168.1.0/24 subnet, you need first add the IP subnet into the list on **IP Group** page.

Click **Add** to enter the **Edit IP Group** page, specify IP group name and IP range and click **Save** to save the settings, as shown below:



If **IP** is selected, specify a destination IP address, as shown below:



Configuring Filter Rule

The Sangfor device is integrated with the stateful inspection packet filtering technology, which helps filter data packets in a specified time schedule according to protocol, source IP address and destination IP address.

The filter rules cover the rules applied to access to the local Sangfor device, and rules applied to access among four interfaces (LAN, DMZ, WAN, VPN interfaces), including the following directions: LAN<->DMZ, DMZ<->WAN, WAN<->LAN, LAN<->LAN, DMZ<->DMZ, VPN<->WAN and VPN<->LAN.

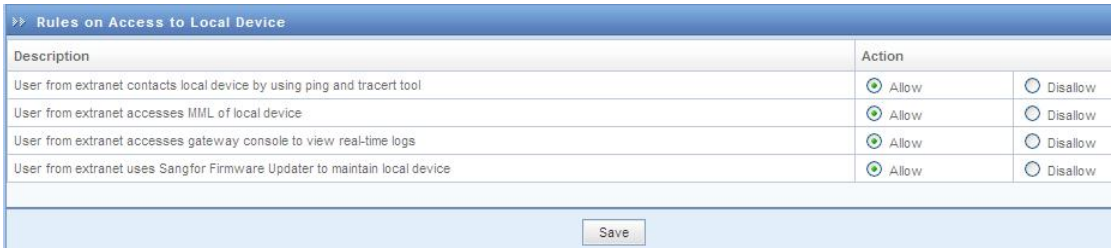


As all the VPN data will be transferred through the VPN interface (for example, the computers connecting to LAN interface and the computers connecting to the peer VPN device communicate with each other through the LAN interface and VPN interface of the local VPN device), the filter rules also applies to the VPN data.

Rules on Access to Local Device

The **Rules on Access to Local Device** page displays the filter rules applied only to the access to the local Sangfor device.

Navigate to **Firewall > Filter Rules > Local Device Access** to enter the **Rules on Access to Local Device** page, as shown below:



Select **Allow** or **Disallow** to allow or disallow users to perform the corresponding operations, and then click **Save** to save the settings.

Rules on Access among Sangfor Device's Interfaces

These rules are intended to filter the data transmitted among the four network interfaces of the Sangfor device, namely, LAN, DMZ, WAN and VPN interfaces.

- **LAN<->DMZ:** Defines the filter rules applied to data access between the LAN interface and DMZ interface of the Sangfor device.
- **DMZ<->WAN:** Defines the filter rules applied to data access between the DMZ interface and WAN interface of the Sangfor device.
- **WAN<->LAN:** Defines the filter rules applied to data access between the WAN interface and LAN interface of the Sangfor device.
- **VPN<->LAN:** Defines the filter rules applied to data access between the VPN interface and LAN interface of the Sangfor device. There are six filter rules built in each Sangfor device, which allow all TCP, UDP and ICMP data from VPN interface to LAN interface and from LAN interface to VPN interface.
- **VPN<->WAN:** Defines the filter rules applied to data access between the VPN interface and WAN interface of the Sangfor device. If the peer has configured a tunnel route to access another site and/or access Internet through the local Sangfor device, configure the filter rules in the VPN<->WAN direction on the local Sangfor device to control the Internet access of the peer (for more details about configuring tunnel route, refer to the Scenario 22: Configuring Tunnel NAT section in Chapter 5).
- **VPN<->DMZ:** Defines the filter rules applied to data access between the VPN interface and DMZ interface of the Sangfor device.

For control traffic of each certain direction, select action **Allow** or **Deny**.

Configuring NAT Rule

The NAT module covers the following configurations: **SNAT Rule**, **DNAT Rule**, **IP/MAC Binding**, **HTTP Port**, **URL Group**, **WAN Service** and **Access Right of Local Users**.

Configuring SNAT Rule

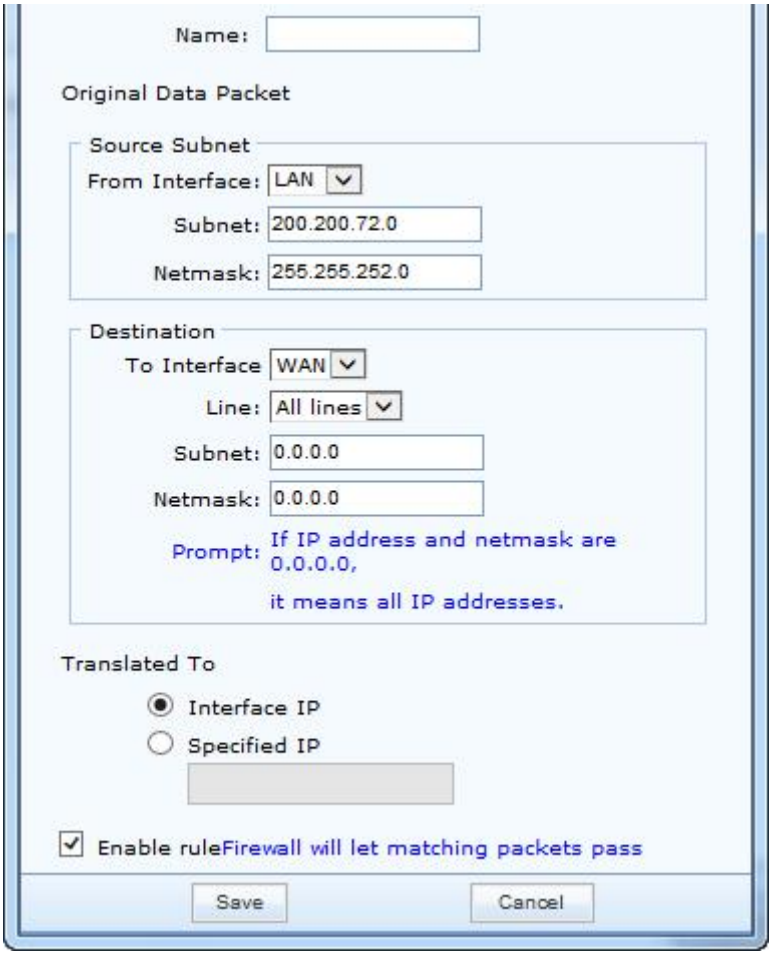
The **SNAT Rule** page, as shown below, enables you to set the Source Network Address Translation (SNAT) rules, which will convert the source IP addresses of the corresponding packets forwarded by the Sangfor device. The Sangfor device will not only provide the basic NAT function, but control (allow/deny) the data packets requested from LAN users for Internet access, in cooperate with the filter rules.

By default, there is no SNAT rule configured on the Sangfor device. If any SNAT rule is needed, configure the SNAT rule according to the specific case.

Navigate to **Firewall > NAT > SNAT Rule** to enter the **SNAT Rule** page, as shown below:



There is no SNAT rule on Sangfor device by default. If you want to configure a SNAT rule, click **Add** to enter the **Edit SNAT Rule**, as shown below:



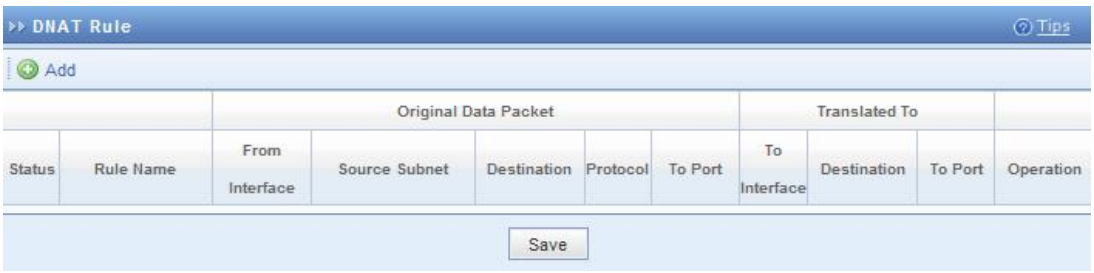
The following information are included on above page:

- **Name:** Indicates the name for this SNAT rule.
- **Source Subnet:** Specifies source interface, subnet and netmask for original data packet.
- **Destination:** Specifies egress interface, subnet and netmask for original data packet. Egress interface can be LAN, DMZ or VPN. Subnet and netmask are used to determine whether the destination IP address of data packet matches this SNAT rule.
- **Translated To:** Specifies what IP address the source IP address is translated to. If **Interface IP** is selected, the source IP of data packet will be translated to the IP address of destination interface. If **Specified IP** is selected, you need to specify an IP address manually.
- **Enable rule**: Select it to enable this SNAT rule. Firewall will let matching packets pass.

Configuring DNAT Rule

The **DNAT Rule** page, as shown below, enables you to configure the Destination Network Address Translation (DNAT) rules required if servers located in LAN provide services to the Internet.

Navigate to **Firewall > NAT > DNAT Rule** to enter the **DNAT Rule** page, as shown below:



Configuring IP/MAC Binding

The Sangfor device provides the IP/MAC binding function, through which you can get the MAC address of a machine in the LAN and bind the MAC address to its IP address.

Therefore, when an unknown internal machine connects to the Sangfor device, it cannot access the Internet through the Sangfor device if the IP address and MAC addresses are not in the IP/MAC binding list. If the MAC address of a certain IP address is found inconsistent with that in the IP/MAC binding list, the Sangfor device will also deny its request for Internet access. In this way, the IP/MAC binding function can also prevent IP address of a LAN computer from being altered.

Navigate to **Firewall > NAT > IP/MAC Binding** to enter the **IP/MAC Binding** page, as shown below:



To enable the IP/MAC binding function, select the **Enable IP/MAC binding** option.

With IP/MAC binding enabled, when a user initiates a request for Internet access, the Sangfor device will check whether the IP address is in the IP/MAC binding list. There are two cases:

- For IP address in the list, the Sangfor device will further check whether its MAC address matches that in the list. If yes, the user can successfully access the Internet; otherwise, its request will be denied.
- For IP address not in the list, the Sangfor device will handle its request according to the action specified in **Action (for IP not in the list below)**.

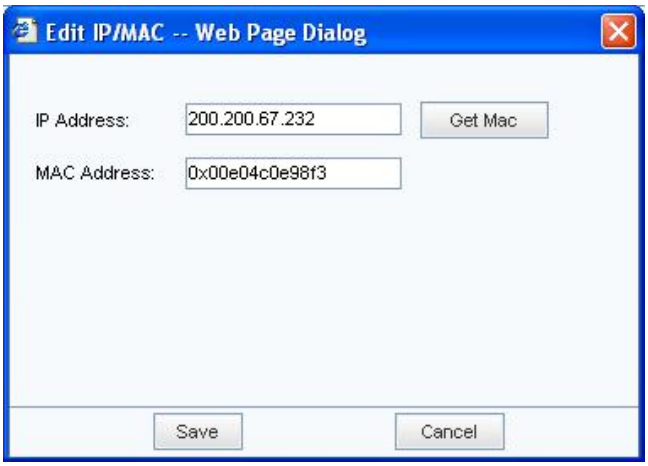
The **Action (for IP not in the list below)** option specifies the action to be taken for Internet access requests initiated by internal users whose IP/MAC addresses are not in the IP/MAC binding list. There are two actions:

- **Deny:** Indicates the user is NOT allowed to access the Internet if the IP address is not in the IP/MAC binding list.

- **Allow:** Indicates the user is allowed to access the Internet if the IP address is not in the IP/MAC binding list.

For IP address already in the IP/MAC binding list, the Sangfor device will check whether its MAC address matches that in the list (on the condition that the IP/MAC binding function is enabled). If yes, the corresponding user can access the Internet; otherwise, its request for Internet access will be denied.

To add an IP/MAC binding entry, click **Add** and then enter the IP address and MAC address (or click **Get MAC** to obtain MAC address automatically), as shown below:

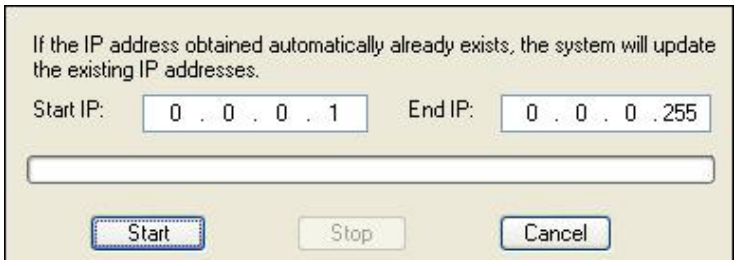


The search for IP/MAC addresses of the internal computers, perform the following steps:

1. Click **Search** and the following prompt appears.



2. Click **OK** and the following dialog appears.



3. Enter the IP range and then click **Start**.

The IP/MAC binding function is unavailable in a layer-3 switched environment.

Configuring HTTP Port

The **HTTP Port** page enables you to define the HTTP service port. By default, it is port 80. If the **Enable URL access** option is selected in **Firewall > NAT > Access Right > Access Right of Local Users**, the Sangfor device will record the information of the URL accessed by users through port 80 and filter the URL information sent through port 80. To record and filter the URL access on any other ports, add the ports here.

Navigate to **Firewall > NAT > HTTP Port** to enter the **HTTP Port** page, as shown below:



To add an HTTP port, click **Add** to open the following dialog, and then specify the corresponding information.



Defining URL Group

An enterprise-level stateful firewall is built in the Sangfor device and provides the URL filtering function. This function, coupled with the firewall, helps control LAN users' access to the Internet.

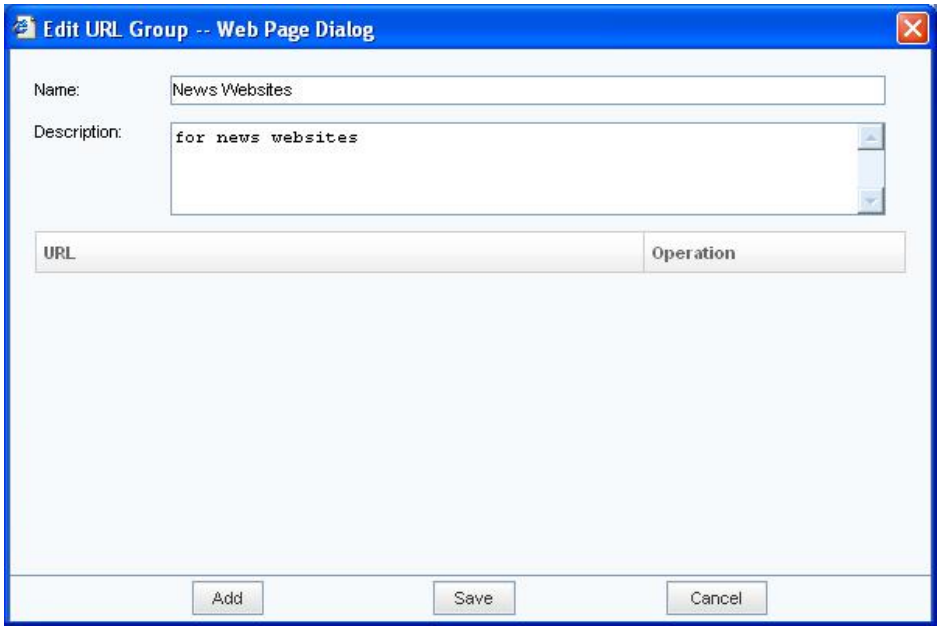
You need define the URL groups before using the URL filtering function.

Navigate to **Firewall > NAT > URL Group** to enter the **URL Group** page, as shown below:



To add a URL group:

1. Click **Add** to enter the **Edit URL Group** page, and then enter a name and description for the URL group, as shown below:



2. Click **Add** on the **Edit URL Group** page, enter the URL address (the first field supports the wildcard *) and then click **Save** to add it to the URL list.



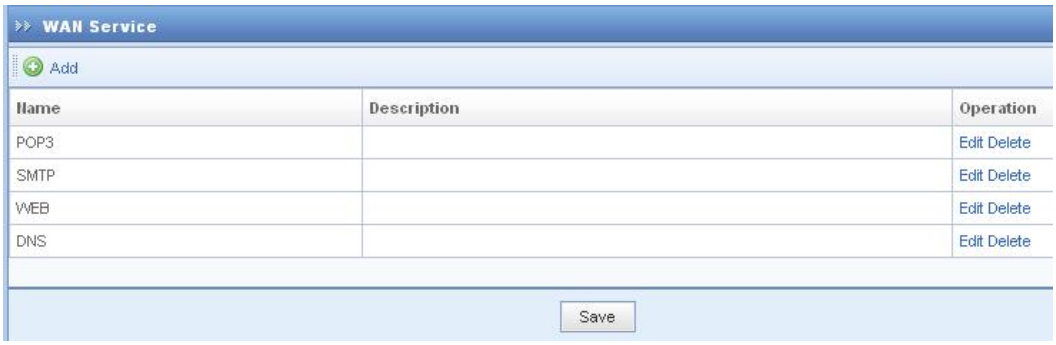
3. Click the **Save** button on the **URL Group** page to save the settings.

Defining WAN Service

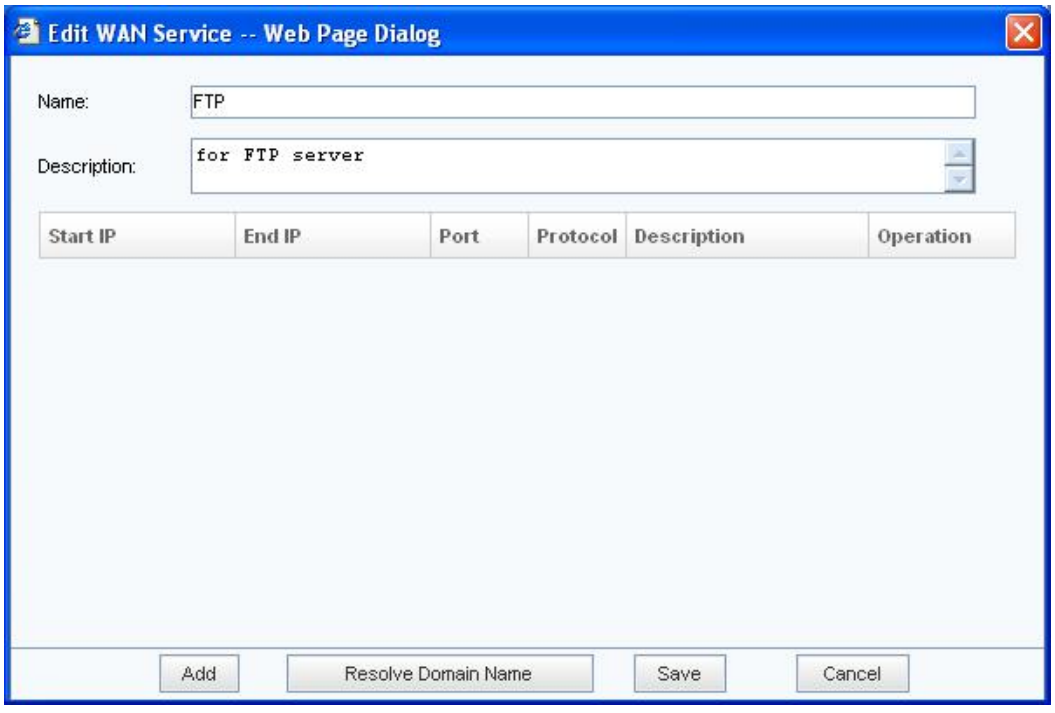
WAN services are services provided by external networks, which are initially accessible to LAN users if they can connect to the external network. However, access to WAN services can also be restrained by the WAN service entry configured on the Sangfor device.

By default, four types of services are already defined, namely, POP3, SMTP, WEB and DNS. If any other service is needed, define it according to the specific case. For example, to add the FTP service provided by the server (Internet IP address is 202.96.137.75; ports is 20-21), perform the following steps:

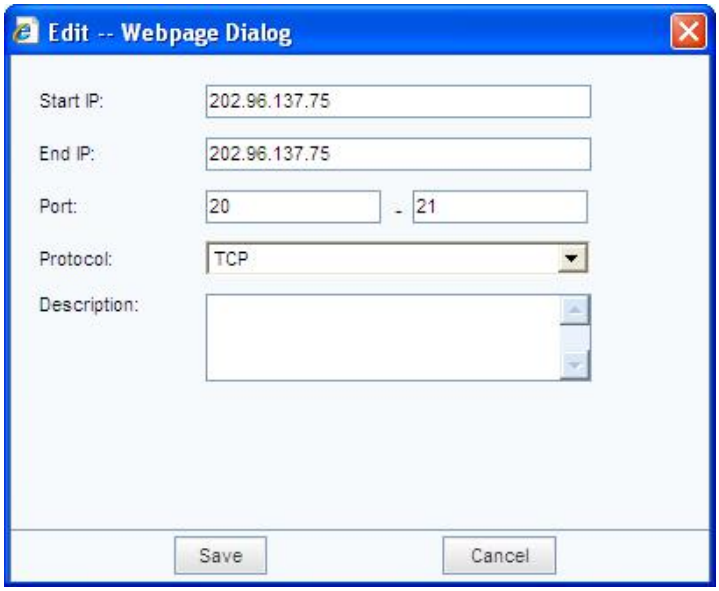
1. Navigate to **Firewall > NAT > WAN Service** to enter the **WAN Service** page, as shown below:



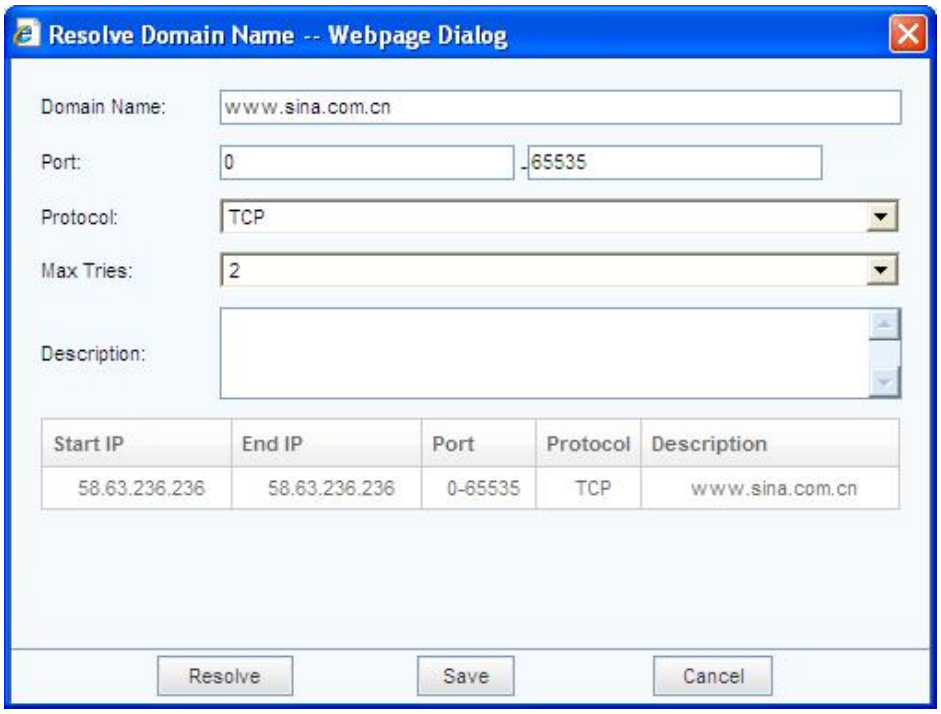
2. Click **Add** to enter the **Edit WAN Service** page, and then enter a name and description for the entry, as shown below:



3. Click **Add** on the **Edit WAN Service** page to specify the IP addresses and port of the external FTP server, as shown below:



4. If service address is domain name, click the **Resolve Domain Name** button on the **Edit WAN Service** page to enter the **Resolve Domain Name** page, and then enter the domain name and click the **Resolve** button to resolve the domain name. The corresponding IP address(es) will be listed, as shown below:



5. Click the **Save** buttons to save the settings.

Configuring Access Right of Local Users

The **Access Right of Local Users** page helps to conduct control over LAN users' access to the Internet. It is one of the most common ways used on firewall device to allow/block LAN users'

access to the services provided over external networks. Although the filter rules of firewall also provide the control function, it controls users' access based on IP address and port, which attaches the importance to the security of the entire network. For controlling LAN users' access to the Internet, **Access Right of Local Users** is more convenient.

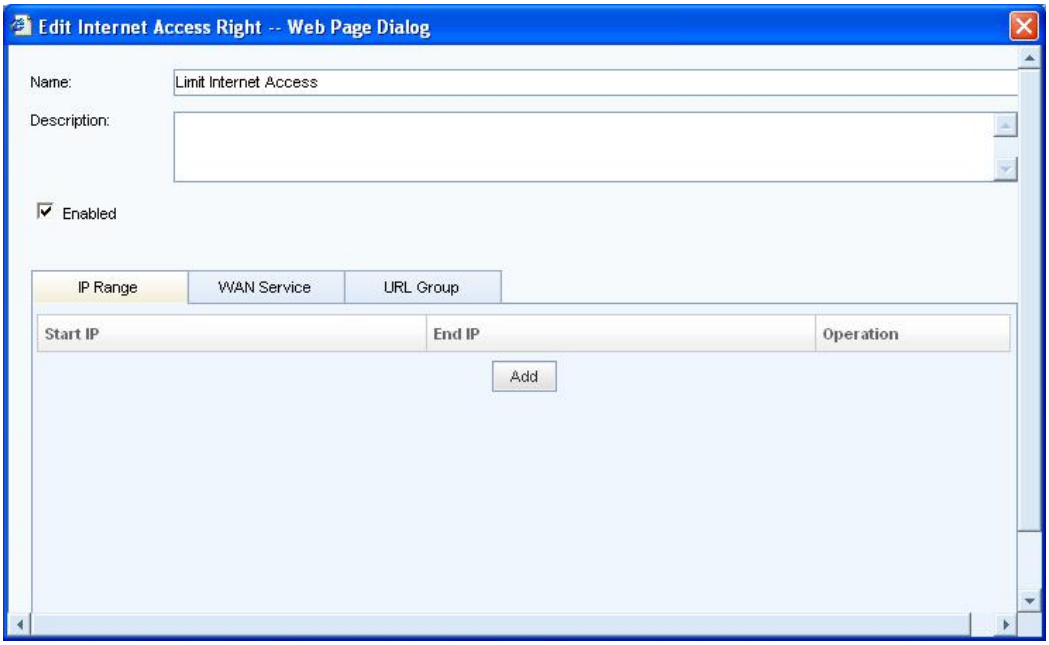
To configure an access right rule:

1. Navigate to **Firewall > NAT > Access Right** to enter the **Access Right of Local Users** page, as shown below:

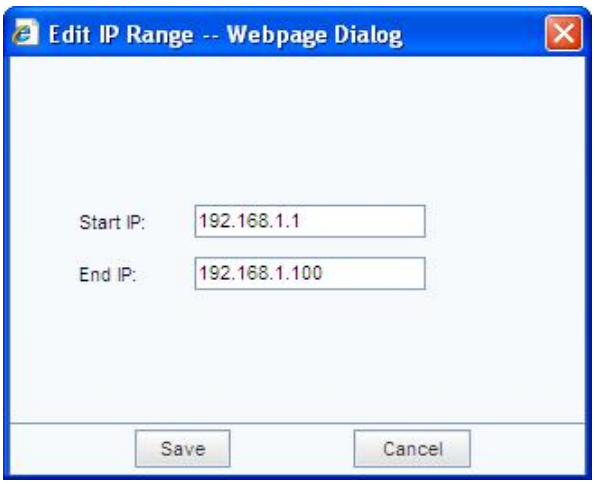


2. Select the **Enable URL access** option to enable URL filtering function and view URL access logs.

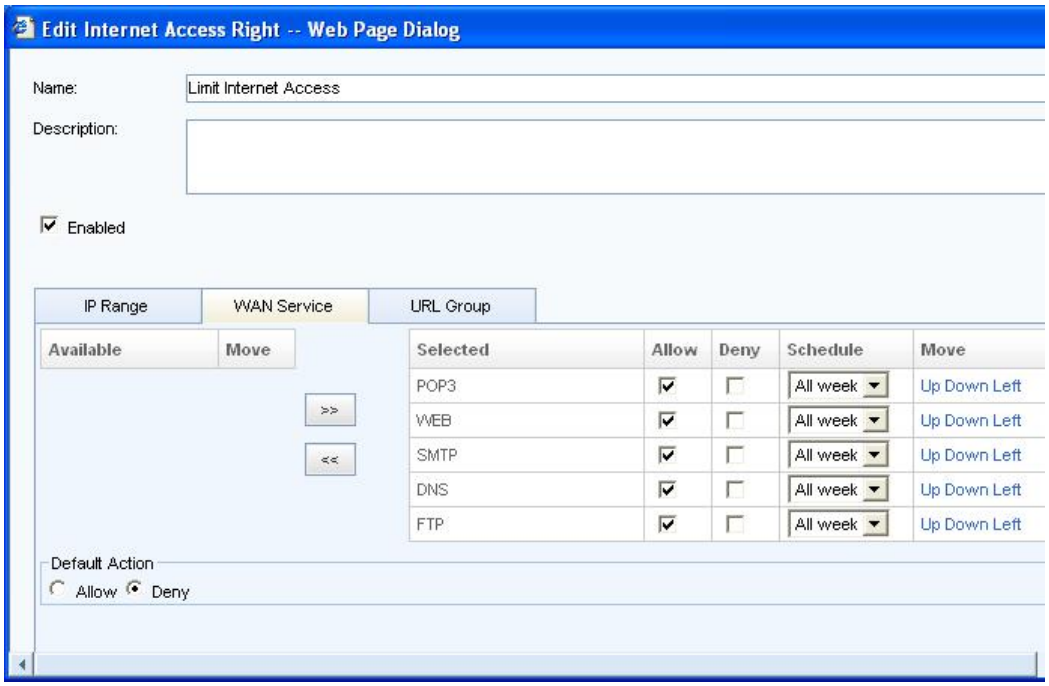
3. Click **Add** to enter the **Edit Internet Access Right** page, and then enter a name and description for this rule, as shown below:



4. Click the **Add** button on the **IP Range** tab and enter the LAN IP addresses applicable to this rule, as shown below:



5. Click to enter the **WAN Service** tab and specify the WAN services for the LAN users configured in Step 4. By default, the LAN users can access all the WAN services.

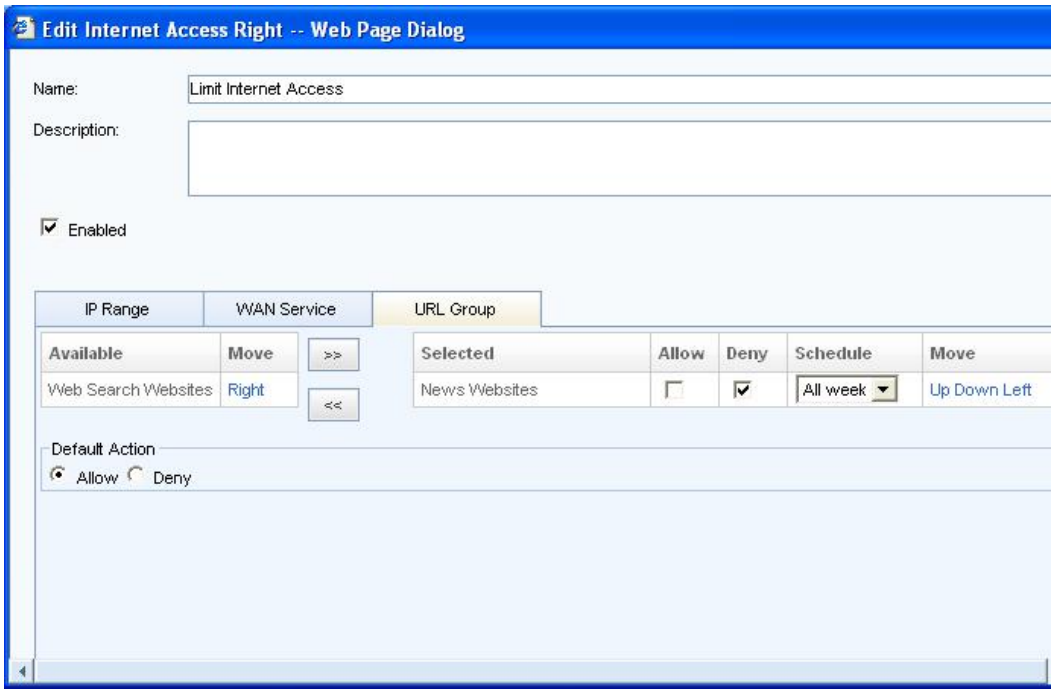




When a LAN user initiates a request for Internet access, the firewall will inspect the data packet based on the selected rules from top to bottom. The **Default Action** specifies the action that will to be taken if none of selected rules is matched.

6. Click to enter the **URL Group** tab, and specify the URL groups accessible to the LAN IP addresses configured on the **IP Range** tab. By default, the LAN users can access all URL addresses. To allow/deny access to a certain URL group, click **Right** to move it to the right

and then select **Allow**/**Deny**. In the following example, the applicable LAN users can access any URL address except those included in the URL group **News Websites**.



7. Click the **Save** buttons to save the settings.

Real-time Monitoring

Viewing Real-time Traffic

The **Traffic** page shows the information of inbound and outbound traffic related to LAN users.

Navigate to **Firewall > Monitor > Traffic** to enter the **Traffic** page, as shown below:



Viewing URL Access Logs

The **URL Access Logs** page displays the webpage access records of LAN users, including access time, status, IP address of the LAN user and URL of the visited webpage.

Navigate to **Firewall > Monitor > Logs** to enter the **URL Access Logs** page, as shown below:



To update the URL access logs, click the **Refresh** button.

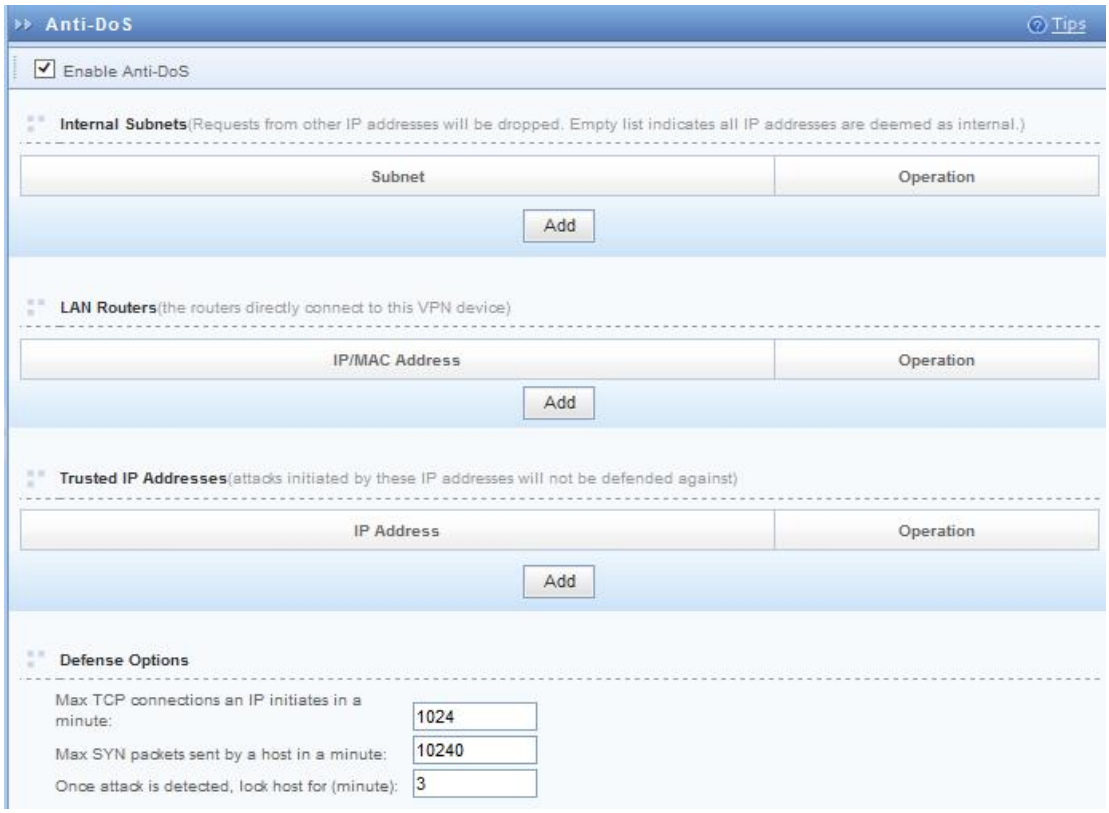


To have URL access entries displayed here, ensure the **Enable URL access** option is selected (in **Firewall** > **NAT** > **Access Right** > **Access Right of Local Users**).

Configuring Anti-DoS

The firewall shoulders the responsibilities of protecting the local area network (LAN) from being attacked by users over the Internet. However, apart from outside attacks, attacks from inside the LAN may also threaten the security of the LAN. For example, it often happens that a virus-infected computer sends massive data packets to the gateway, which may result in bandwidth congestion or gateway crash. In this case, deploying a Sangfor device in your network will easily solve the issue. As the Sangfor device, integrated with the anti-DoS function, will monitor the number of data packets sent from a certain IP address to the gateway. When the number reaches the threshold specified, the Sangfor device will regard the requests as a DoS attack and lock the IP address for a certain period to protect itself.

Navigate to **Firewall > Anti-DoS** to enter the **Anti-DoS** page, as shown below:



The following are the contents included on the **Anti-DoS** page:

- **Enable Anti-DoS:** Select this option to enabled anti-DoS function.
- **Internal Subnets:** Indicates the LAN subnets that can access the Internet through the Sangfor device. When a data packet is sent from a LAN IP address, the Sangfor device will first check whether the source IP address of the packet is in the Internal Subnets list. If not, the Sangfor device will directly drop the packet. If yes, the Sangfor device will further monitor and calculate the number of data packets sent from the IP address. Once the number of data packets reaches the corresponding threshold specified in the defense settings, the device will lock the IP address for a specified period.

Null list indicates all IP addresses are regarded as internal addresses, which means the Sangfor device will skip checking for source IP address of packet, directly monitor/calculate the number of packets sent and finally determine whether to lock the IP address according to the number calculated and thresholds configured in the defense settings below.

- **LAN Routers:** The function is **LAN Routers** is similar to that of **Internal Subnets**.
- **Trusted IP Addresses:** The attacks initiated from the IP addresses listed here will not be defended against. If no entry is added, the attack initiated from any IP address will be defended against.
- **Defense Options:** Configure the defense options. There are three options:
  - **Max TCP connections an IP initiates in a minute:** Specifies the maximum of TCP connections that each IP address is allowed to initiate to the same port of an IP address in one minute. If the threshold here is reached, the IP address will be locked for a specified period.
  - **Max SYN packets sent by a host in a minute:** Specifies the maximum of SYN packets that each host is allowed to send in one minute. If the threshold here is reached, the IP/MAC address will be locked for a specified period.
  - **Once attack is detected, lock host for (minute):** Specifies the period that the attacking host will be locked after the attack is detected.

Chapter 6 System Maintenance

The **Maintenance** module covers the following four parts: **System Update**, **Logs**, **Backup/Restore**, and **Restart/Shutdown.**

System Update

System Upgrade

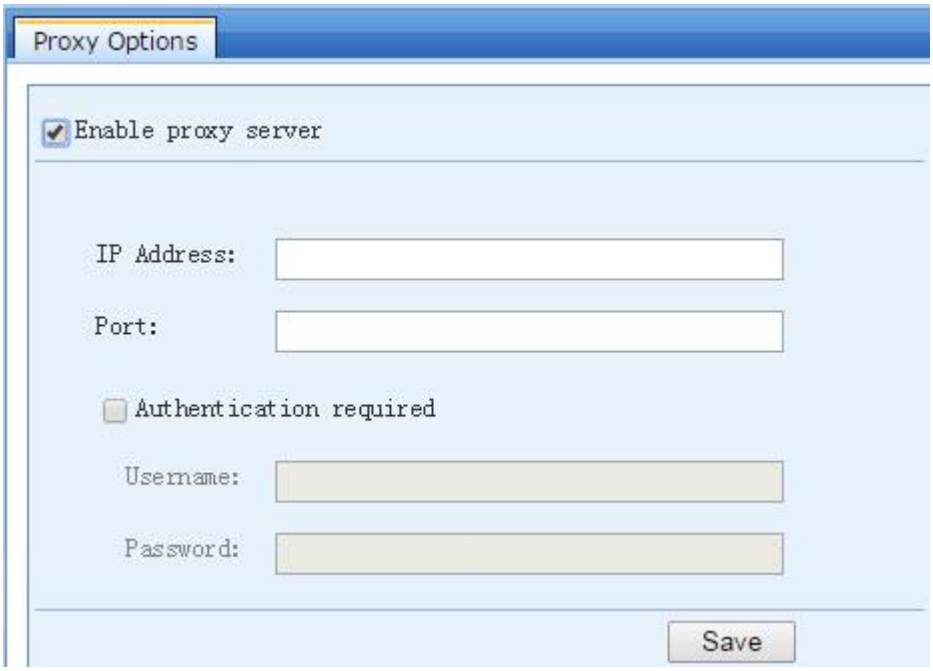
System can be updated through Web admin console, as shown below:



Follow the guide to update the system to the latest version. To update the system offline, there is no need to connect this SSL VPN device to the Internet.

Proxy Options

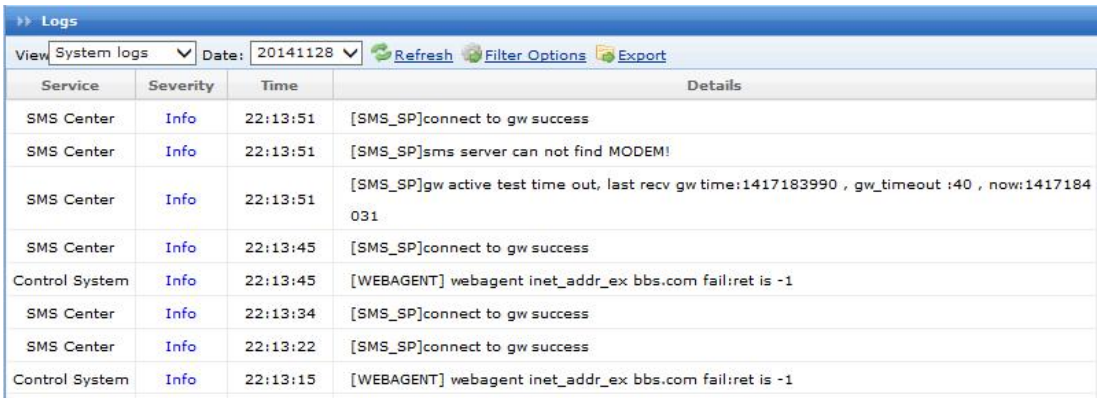
By enabling and configuring proxy server, SSL VPN unit could be connected to the Internet though proxy server. Configure proxy server, as shown below:



Viewing Logs

The **Logs** page displays running status information and error information of the Sangfor device. There are two types of logs: system logs and operation logs. The former displays the running information of each module of the current Sangfor device and the latter displays the information on operations performed by administrators.

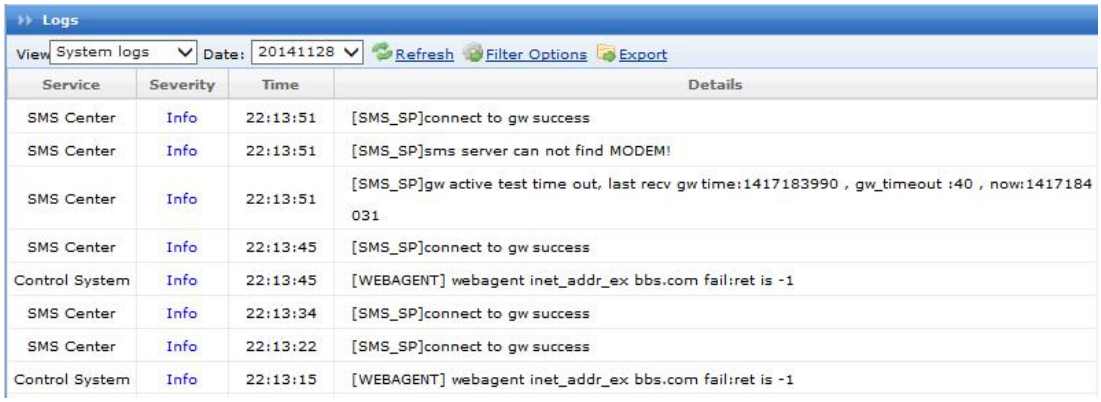
Navigate to **Maintenance > Logs** to enter the **Logs** page, as shown below:



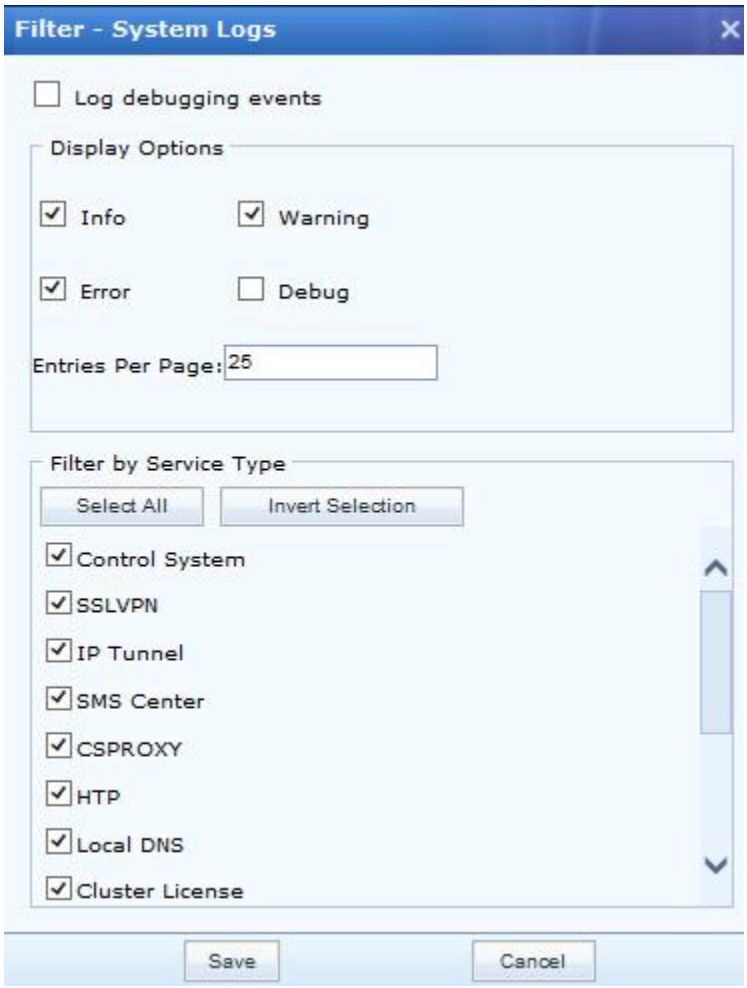
Service	Severity	Time	Details
SMS Center	Info	22:13:51	[SMS_SP]connect to gw success
SMS Center	Info	22:13:51	[SMS_SP]sms server can not find MODEM!
SMS Center	Info	22:13:51	[SMS_SP]gw active test time out, last recv gw time:1417183990 , gw_timeout :40 , now:1417184031
SMS Center	Info	22:13:45	[SMS_SP]connect to gw success
Control System	Info	22:13:45	[WEBAGENT] webagent inet_addr_ex bbs.com fail:ret is -1
SMS Center	Info	22:13:34	[SMS_SP]connect to gw success
SMS Center	Info	22:13:22	[SMS_SP]connect to gw success
Control System	Info	22:13:15	[WEBAGENT] webagent inet_addr_ex bbs.com fail:ret is -1

Viewing System Logs

To view the system logs, select **System logs** and specify a date, and the system logs of the specified date will be displayed, as shown below:



To filter the system logs, click the **Filter Options** button to enter the following page, and then select the desired options.



Viewing Operating Logs

To view the operation logs, select **Operation logs** and a date, and the operation logs of the

specified date will be displayed, as shown below:

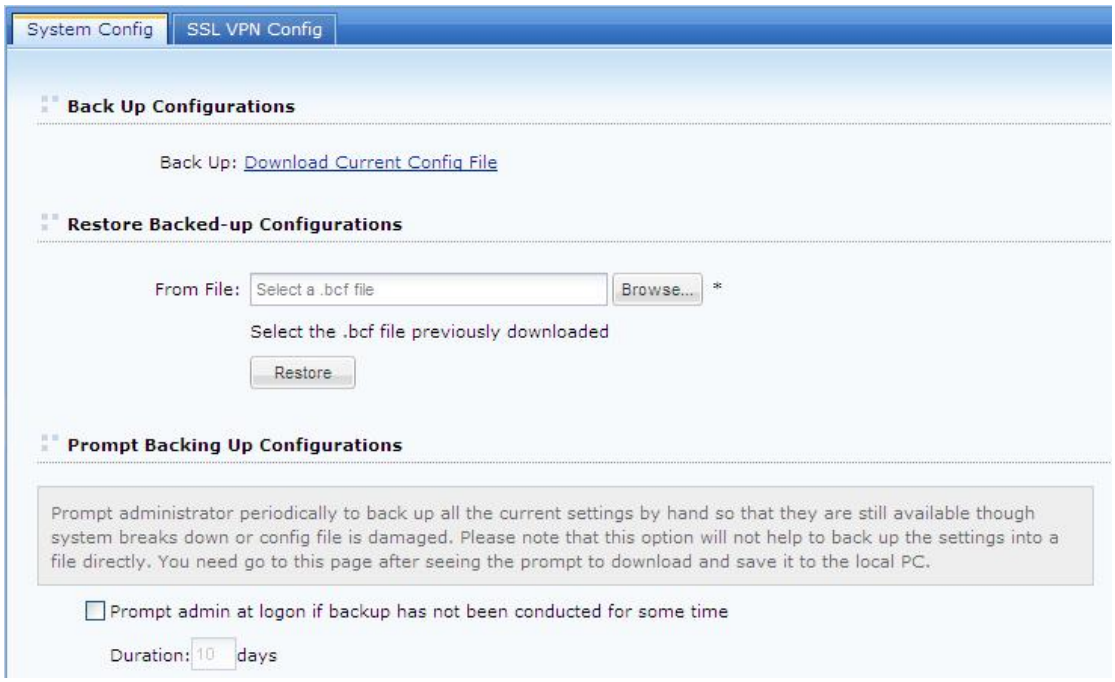


To filter the operation logs, click the **Filter Options** button to enter the following page, and then select the desired options.



Backing Up/Restoring Configurations

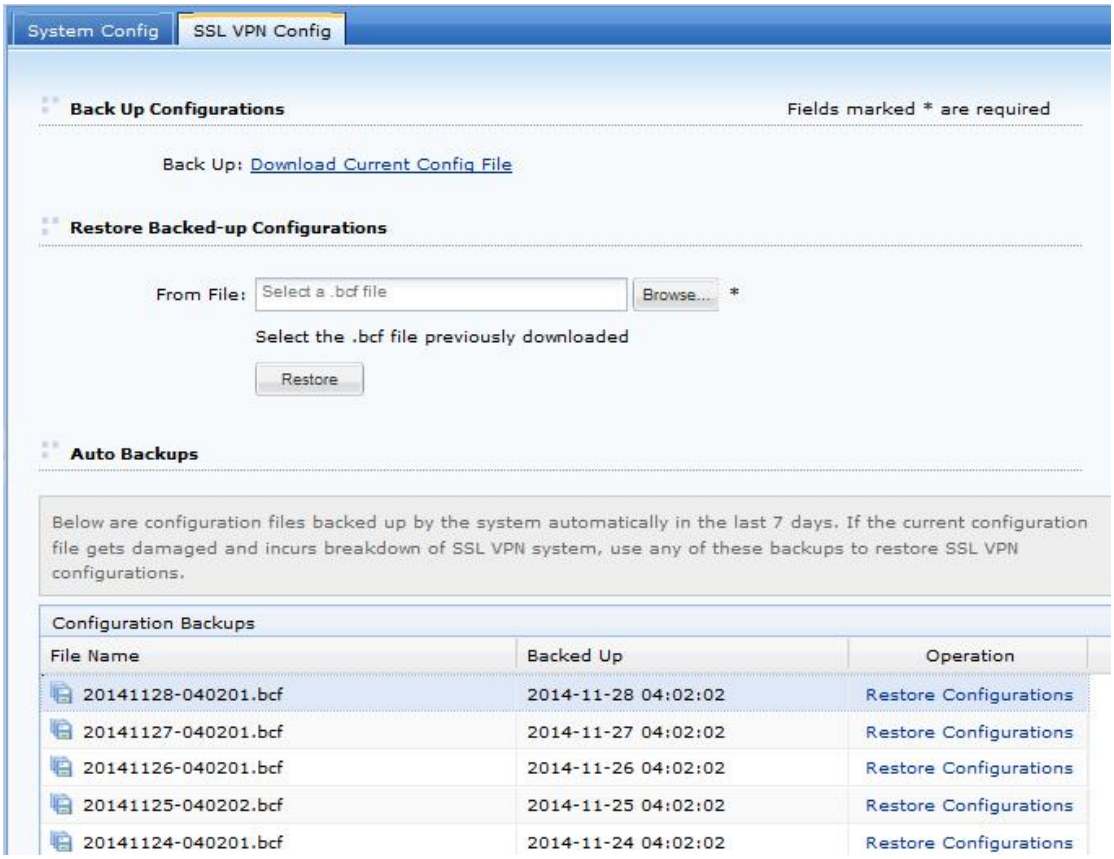
Navigate to **Maintenance > Backup/Restore** to backup or restore the system configurations and SSL VPN configurations on the **System Config** and **SSL VPN Config** pages respectively, as shown below:



The following are contents included on the **System Config** page:

- **Download Current Config File:** To back up the current configurations, click this link to download and save the current configurations to the local computer. The configurations are saved as a .bcf file.
- **Browse:** To restore the configurations previously backed up, click it to select the configuration file from the local computer.
- **Restore:** Click it to restore the configurations from the selected file.
- **Prompt admin at logon if backup has not been conducted for some time:** Select it and specify **Duration**, so that the system will prompt the administrator to back up the configurations when he logs into the administrator Web console if configurations have not been backed up for such a long time.

To back up and restore SSL VPN configurations, click **SSL VPN Config** to enter the **SSL VPN Config** page, as shown below:



The following are contents included on the **SSL VPN Config** tab:

- **Download Current Config File:** Click it to save the configurations to the local computer.
- **Browse:** To restore the configurations previously backed up, click it to select the configuration file from the local computer.
- **Restore:** Click it to restore the configurations from the selected file.
- **Auto Backups:** Displays configuration files automatically backed up by the system in the past 7 days. Click **Restore** to restore any of them.



The configurations here only indicate the configurations of the SSL VPN module.

Restarting/Shutting Down Device or Services

The **Restart/Shutdown** page allows you to shut down/restart the Sangfor device, restart all the services and stop/start the SSL VPN service.

Navigate to **Maintenance > Restart/Shutdown** to enter the **Restart/Shutdown** page, as shown below:



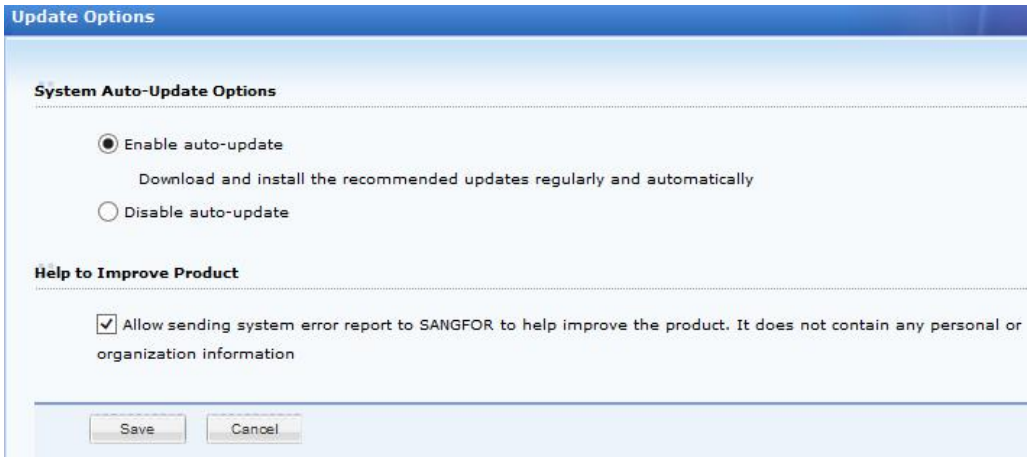
- **Shut Down Device:** To stop all the running services, save current configurations and shut down the Sangfor device.
- **Restart Device:** To shut down and restart the Sangfor device.
- **Restart Service:** To terminate all the sessions, release system resources and restart system services.
- **Stop SSL VPN Service:** To stop the SSL VPN service.
- **About SSL VPN:** To show SSL VPN version information and configure update options.



System Automatic Update

The **Update Options** page includes automatic update options. If auto-update is enabled, updates will be automatically downloaded and installed.

Navigate to **Maintenance > Restart/Shutdown** page and click **About SSL VPN** to enter the **About SSL VPN** page and then click on **Update Options**, the following page appears, as shown below:



- **Enable auto-update:** Select this option to enable automatic update function. The device will check for updates and download them regularly and automatically.
- If **Disable auto-update** is selected, updates will not be downloaded automatically.
- **Help to Improve Product:** Select the option below it to allow user to send system error report to SANGFOR to help improve the product. It does not contain any personal or organization information.
- **Save:** Click this button to make the settings take effect.



The auto-update is only applicable to service pack (SP) installation, but not applicable to upgrade of released version.

Chapter 7 Scenarios

Device Deployment

Sangfor device can work in two modes, **Single-Arm** mode and **Gateway** mode. You can configure device deployment mode under **System** > **Network** > **Deployment**.

Deploying Device in Gateway Mode with Single Line

Background:

- One network segment of a local area network is 192.200.200.0/24
- A Sangfor device is to be deployed in Gateway mode
- External network is an Ethernet network; the IP address assigned by the Internet server operator is 202.96.137.75.

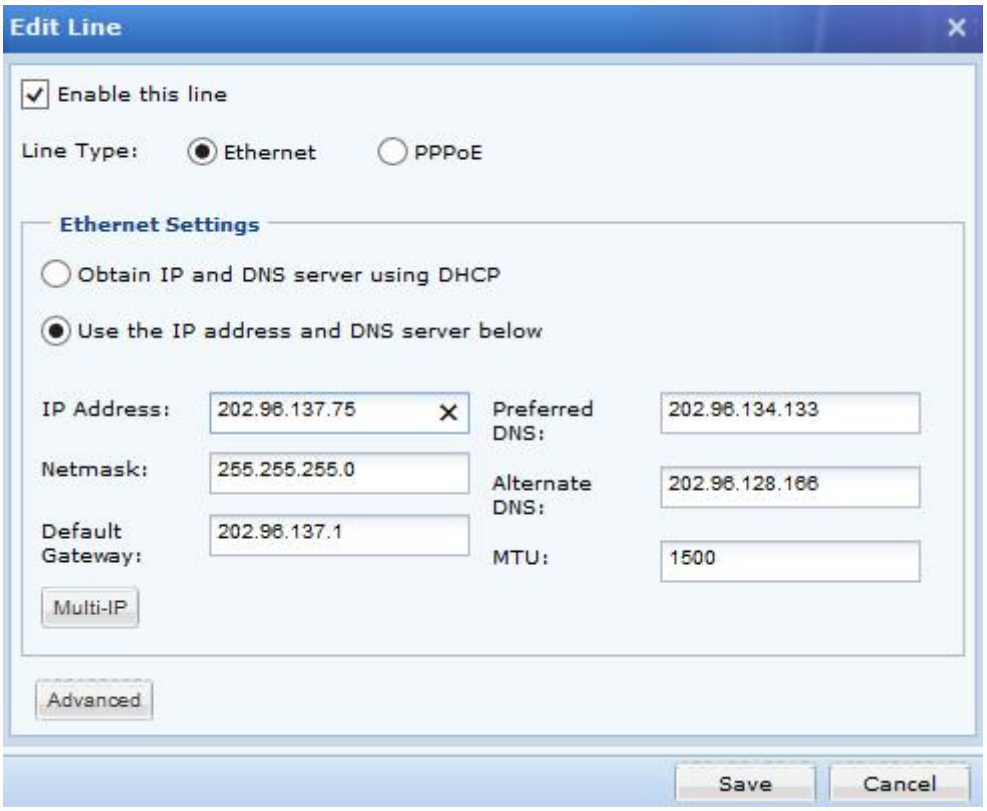
Perform the following steps:

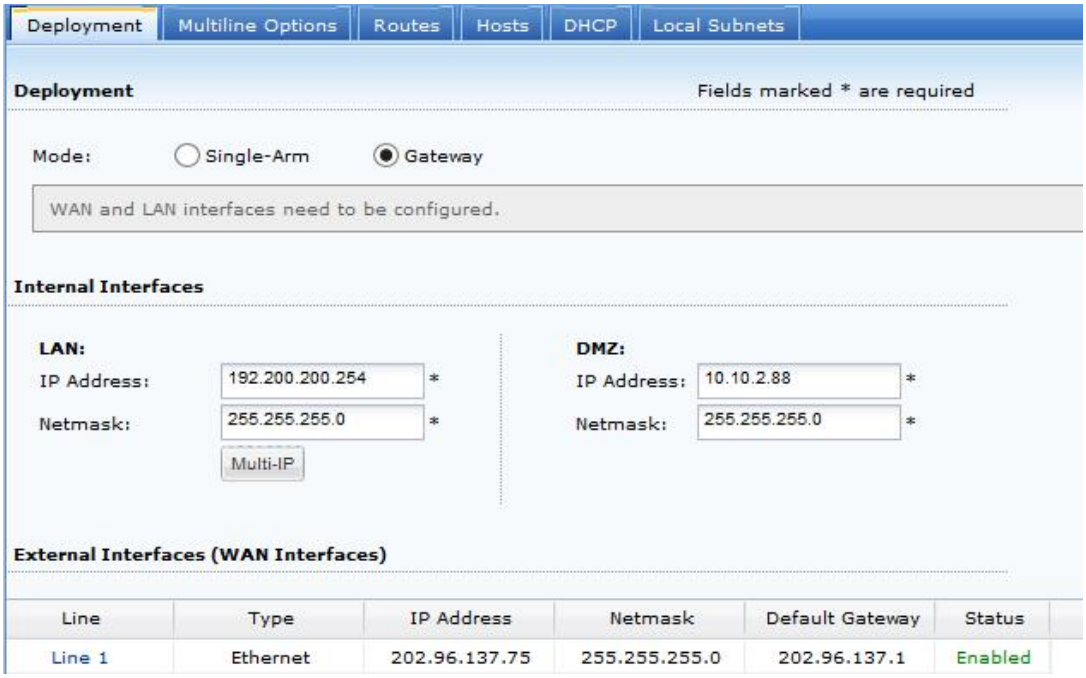
1. Deploy and connect the related devices as shown in the figure below:

2. Log into administrator console and navigate to **System > Network > Deployment** page, and select **Gateway** as the deployment mode, configure LAN interface, as shown in the figure below:

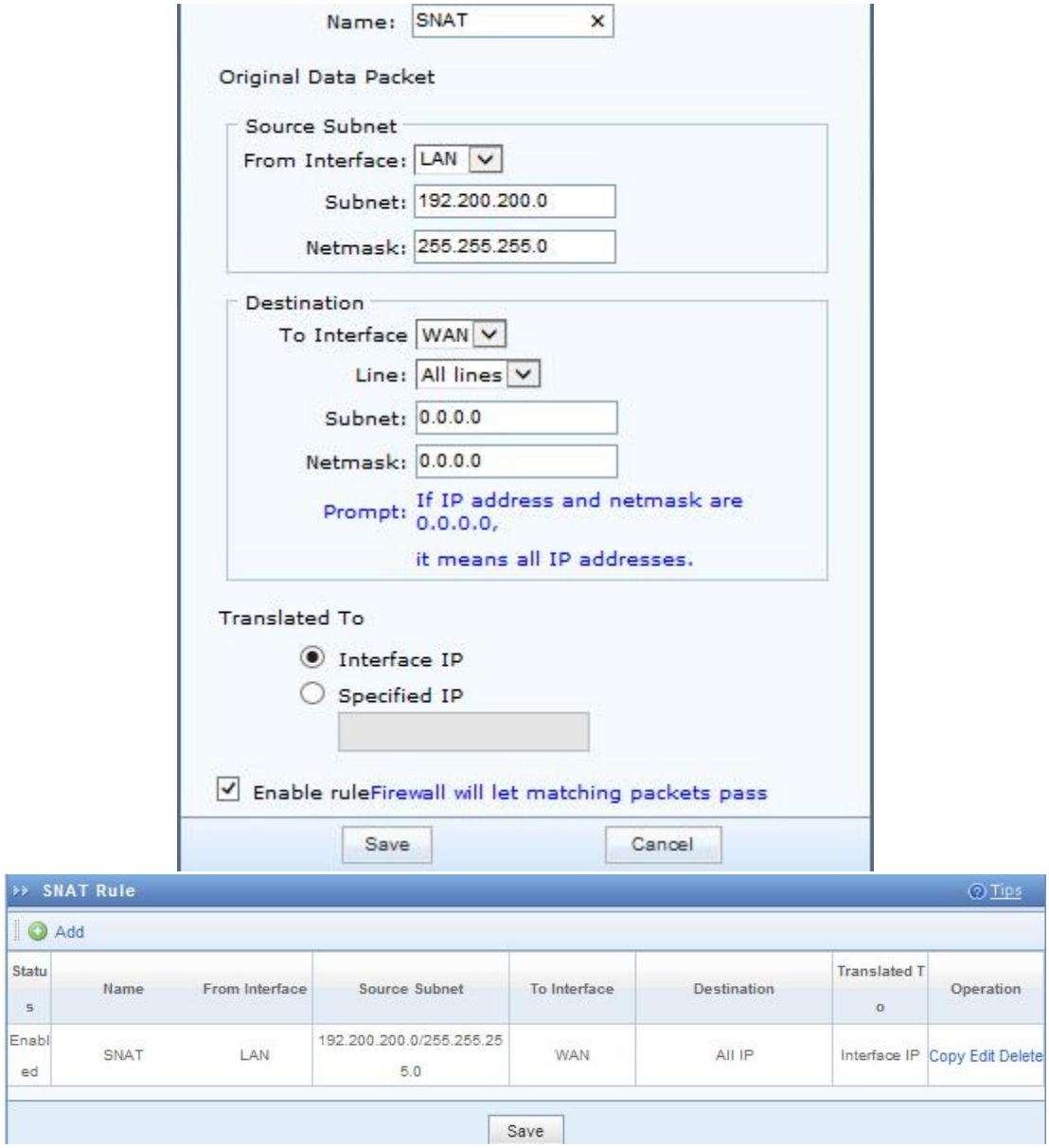


3. Configure WAN interface and corresponding line, as shown below:





4. Go to **Firewall > NAT** > **SNAT Rule** to enter the **SNAT Rule** page and click **Add** to enter **Edit SNAT Rule** page, as shown below:



5. Click **Save** button to save the settings and restart the Sangfor device.

Deploying Device in Gateway Mode with Multiple Lines

Background:

- One network segment of a local area network is 192.200.200.0/24
- A Sangfor device is to be deployed in Gateway mode
- There are two WAN lines: Telecom and Unicom.

Purpose:

User on business can connect to SSL VPN through the one of the two WAN lines, which has better performance.

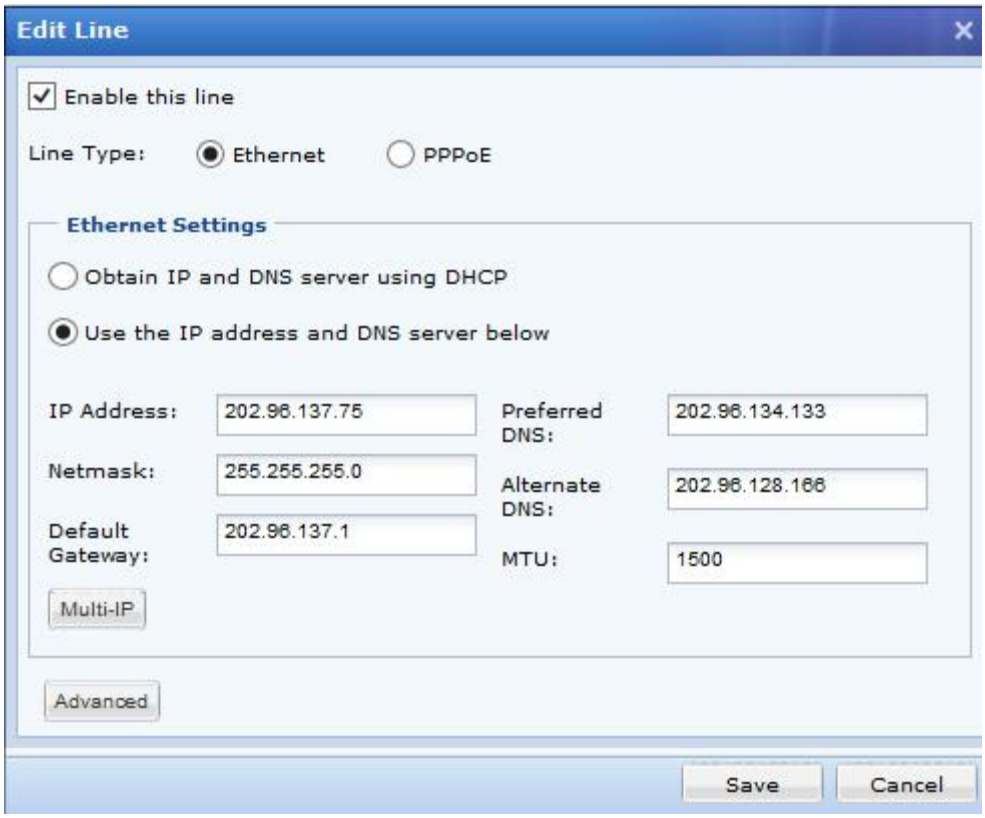
Perform the following steps:

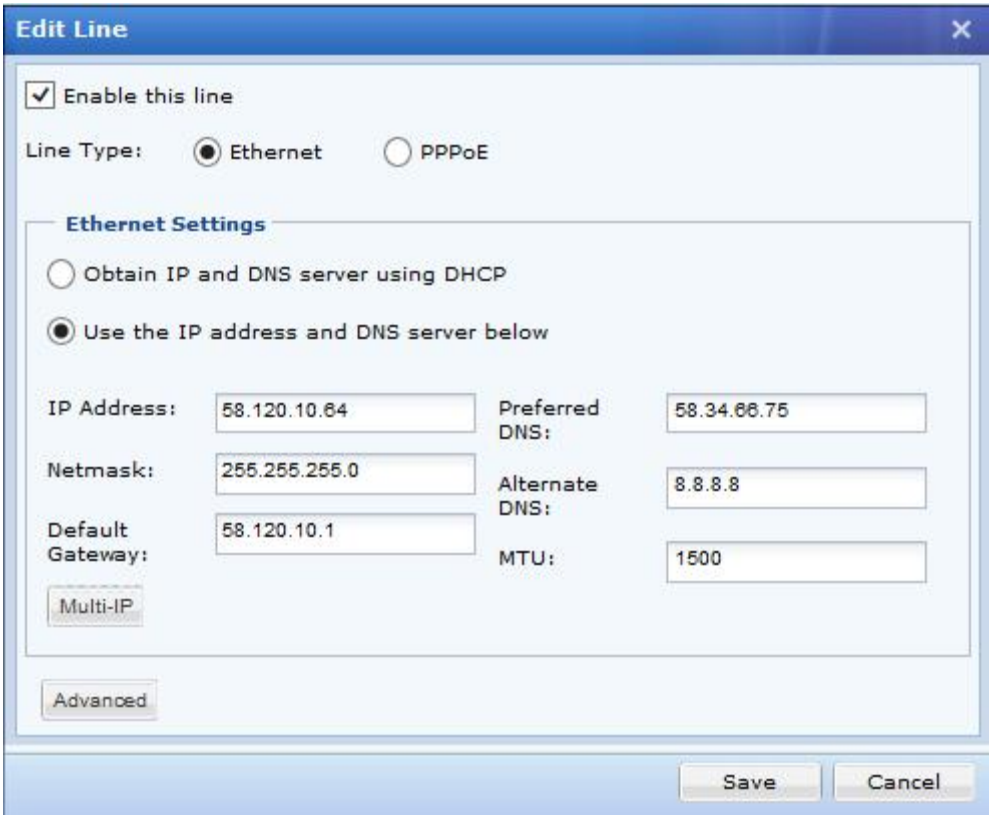
1. Deploy and connect the related devices as shown in the figure below:

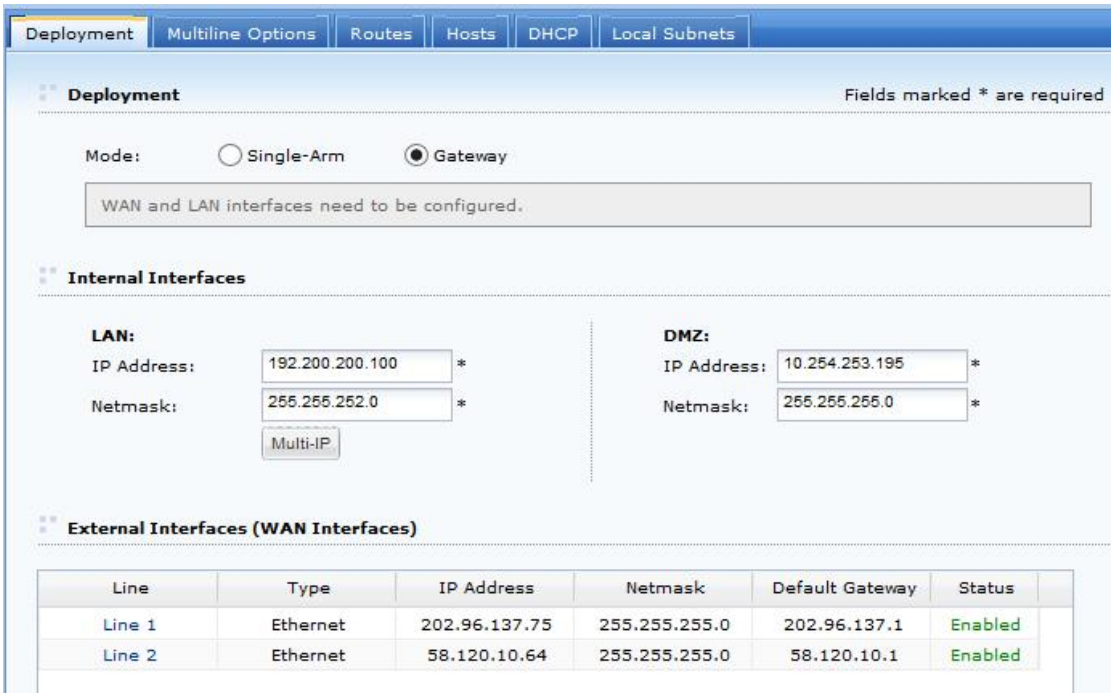
2. Log into administrator console and navigate to **System > Network > Deployment** page, and select **Gateway** as the deployment mode, configure LAN interface, as shown in the figure below:



3. Configure WAN interface and corresponding line, as shown below:



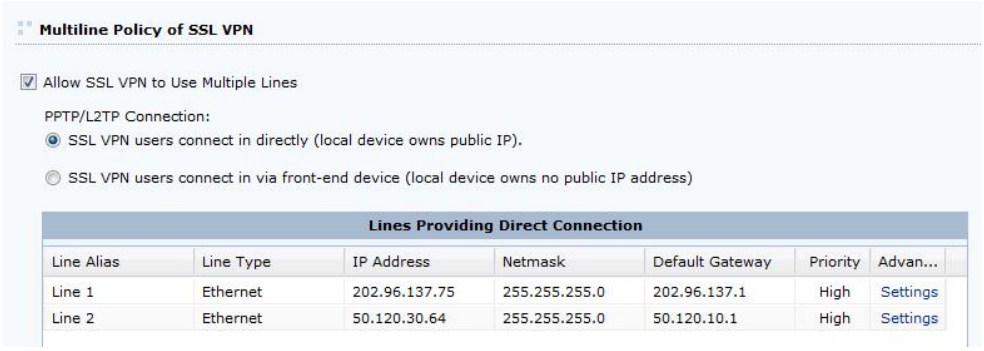




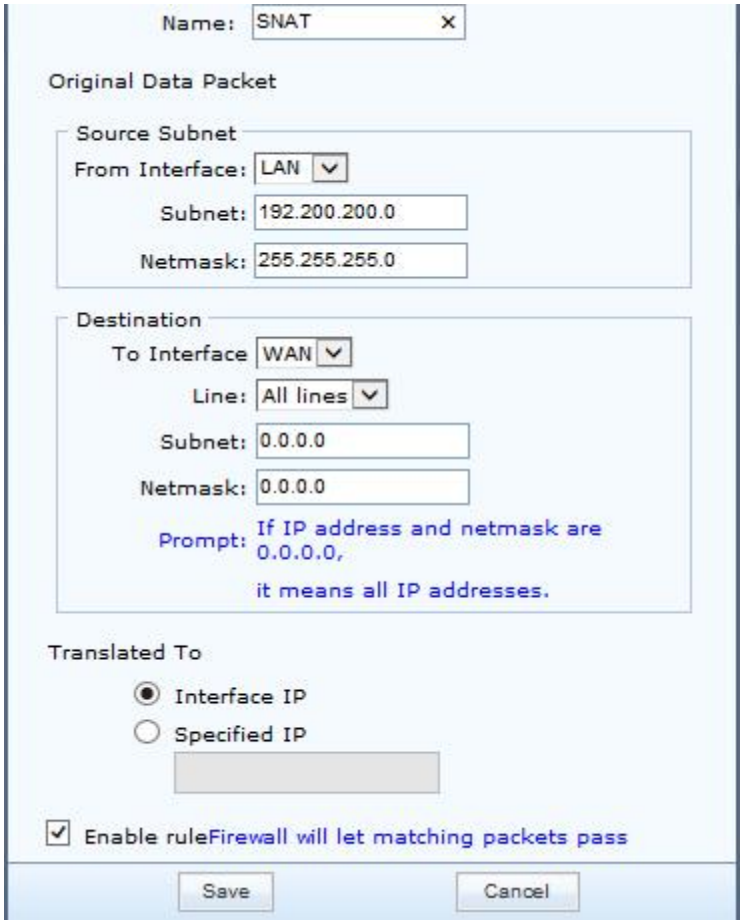
4. Go to **System > Network > Multiline Options** page and select the **Allow Sangfor VPN to Use Multiple Lines** option and add two Internet lines: Telecom and Unicom, as shown in the figure below:

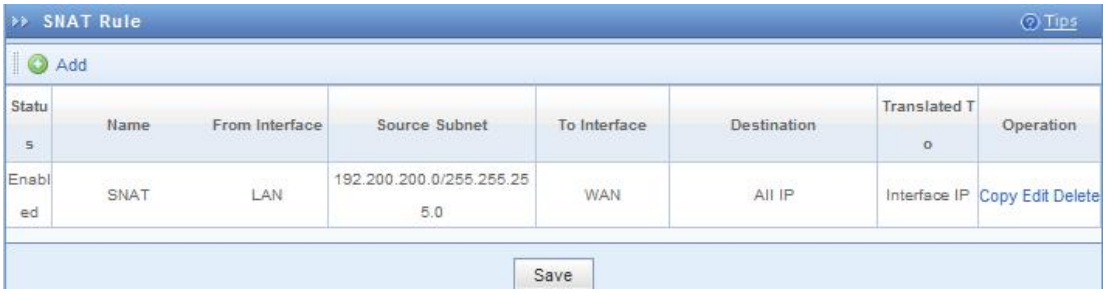


Select the **Allow SSL VPN to Use Multiple Lines** and **SSL VPN users connects in directly** Options under **Multiline Policy of SSL VPN** section, as shown below:



5. Navigate to **Firewall > NAT > SNAT Rule** and click **Add** to enter the **Edit SNAT Rule** page and configure required fields according to your need, as shown below:





6. Click **Save** to save all the changes and restart Sangfor device.



The option **Allow Sangfor VPN to Use Multiple Lines** needs to be selected only when Sangfor device is deployed in gateway mode with multiple lines and connected to Internet directly.

Deploying Device in Single-Arm Mode With Single Line

Background:

- One network segment of a local area network is 192.200.200.0/24

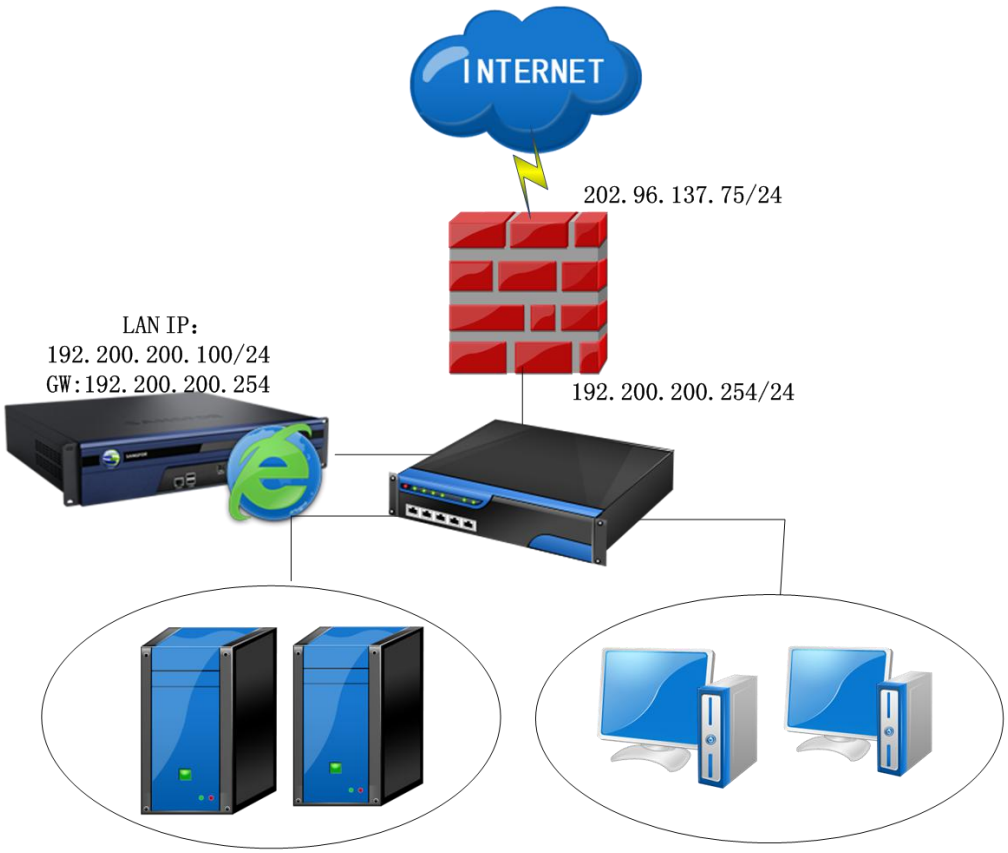
- A Sangfor device is to be deployed in the local area network, in Single-arm mode
- The front-end firewall is connected to external network through an Internet line

Purpose:

Users on business can access internal resources through SSL VPN.

Perform the following steps:

1. Deploy and connect the related devices, as shown in the figure below:



2. Go to **System** > **Network** > **Deployment** page and select Single-Arm as deployment mode, and configure the network interfaces of the device as well, as shown below:



3. Click the **Save** button to save the settings and restart the Sangfor device.
4. Configure the front-end firewall, and make sure that the corresponding ports (443 by default) of the front-end firewall are mapped to those on the Sangfor device.



- Port 443 is the listening port of Sangfor device by default. It can be modified. If it is modified, corresponding port of the front-end firewall needs to be mapped to the modified listening port.
- LAN interface of Sangfor device in single arm mode should be connected to internal switch.

Deploying Device in Single-Arm Mode With Multiple Lines

Background:

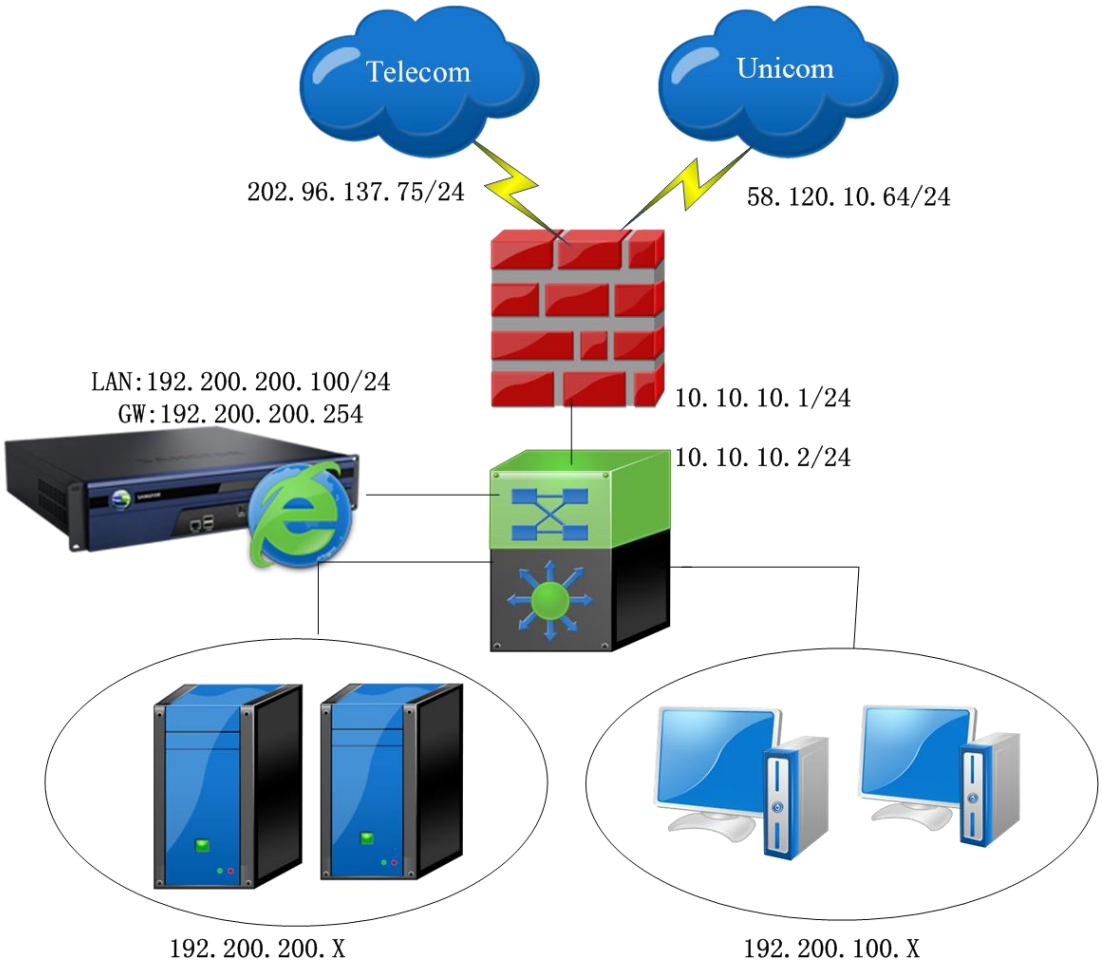
- There are two Internet lines connected to front-end firewall device: Telecom and Unicom
- A Sangfor device is to be deployed in the local area network, in Single-arm mode

Purpose:

User can connect to SSL VPN by typing into 202.96.137.75 or 58.120.10.64 in **Address** field on VPN client.

Perform the following steps:

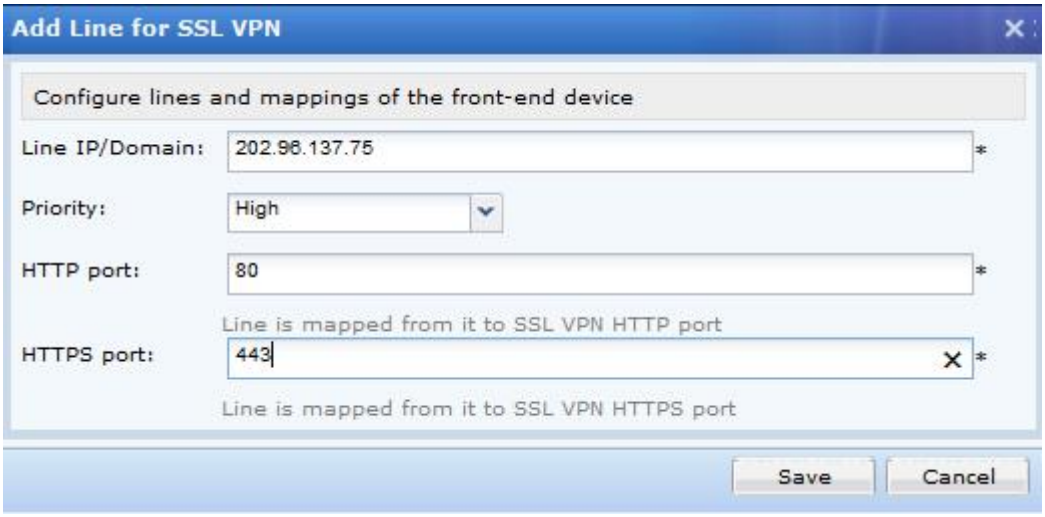
1. Deploy and connect the related devices, as shown in the figure below:

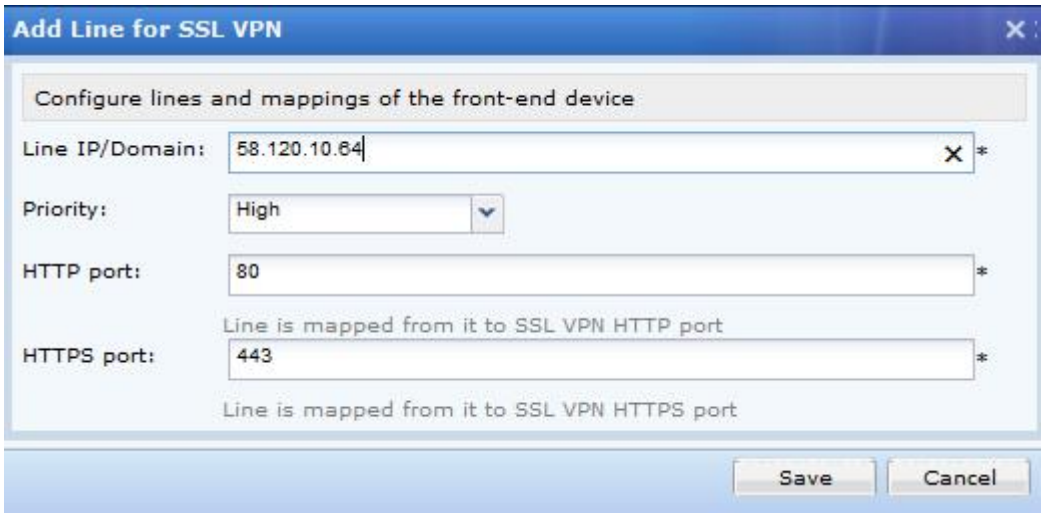


2. Go to **System** > **Network** > **Deployment** page and select Single-Arm as deployment mode, and configure the network interfaces of the device as well, as shown below:



3. Go to **System** > **Network** > **Multiline Option**s page to select the **Allow SSL VPN to use Multiple lines** option and add two Internet lines for SSL VPN, as shown below:







4. Configure the front-end firewall again, so that the two ports (TCP 80 and 443) of the public

network IP addresses (of the two Internet lines) can be mapped to the Sangfor device.

5. Click **Save** button to save the changes and restart Sangfor device.



When Sangfor device is deployed in single-arm mode, HTTPS port and HTTP port must be mapped to the Sangfor device; otherwise, multiline selection policy will not work.

Configuring System Route

Background:

- Two network segments of a local area network are 192.200.200.X and 192.200.254.X. Users in these two subnet communicate through layer 3 switch
- Sangfor device is to be deployed in the local area network, in gateway mode

Purpose:

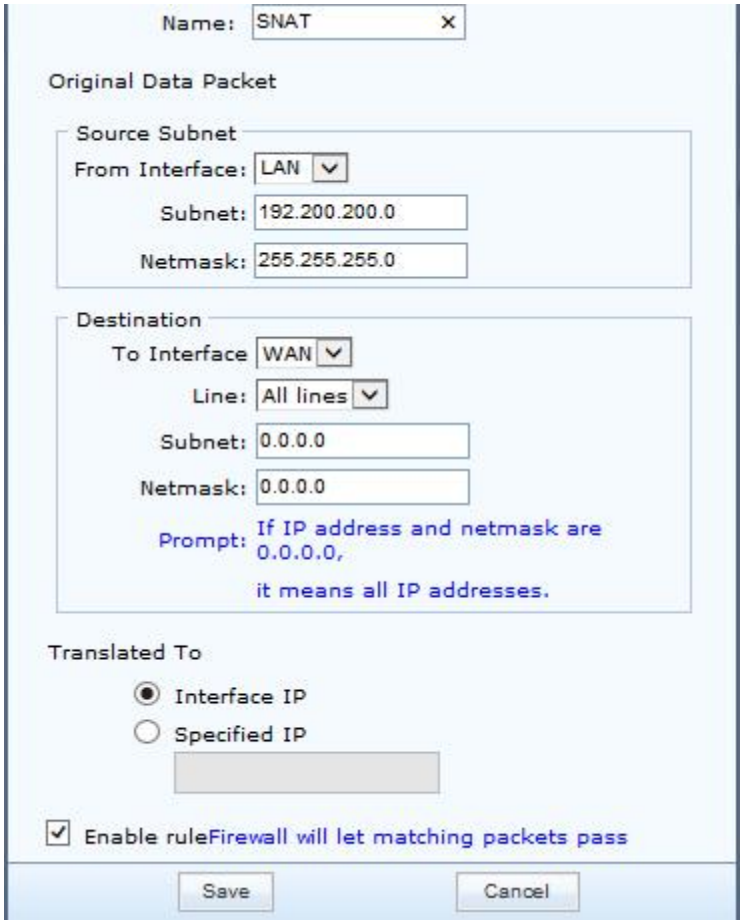
Users on the subnet 192.200.254.x can access Internet through Sangfor device

As 192.200.254.X and 192.200.200.254 on which LAN interface of Sangfor device resides are not on the same network segment, a system route is required to be configured on Sangfor device.

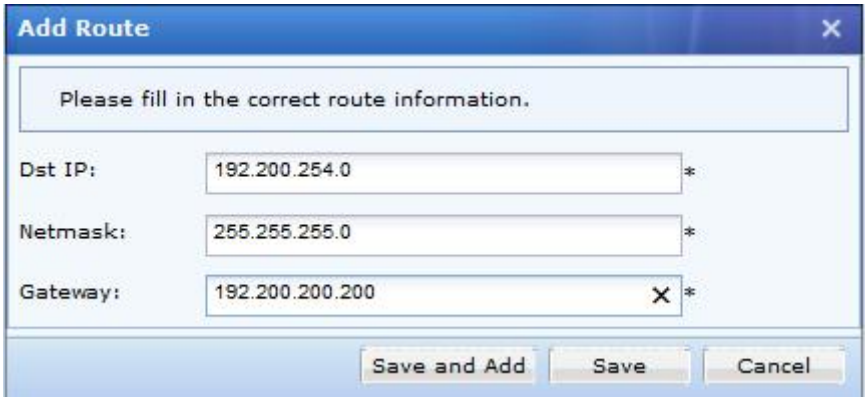
Perform the following steps:

1. Deploy and connect the related devices, as shown in the figure below:

2. Configure SNAT rule on **Firewall > NAT >SNAT Rul**e page, as shown below:



3. Go to **System > Network > Routes** page to add a route directing to 192.200.254.X, as shown below:



Deploying Clustered Sangfor Devices

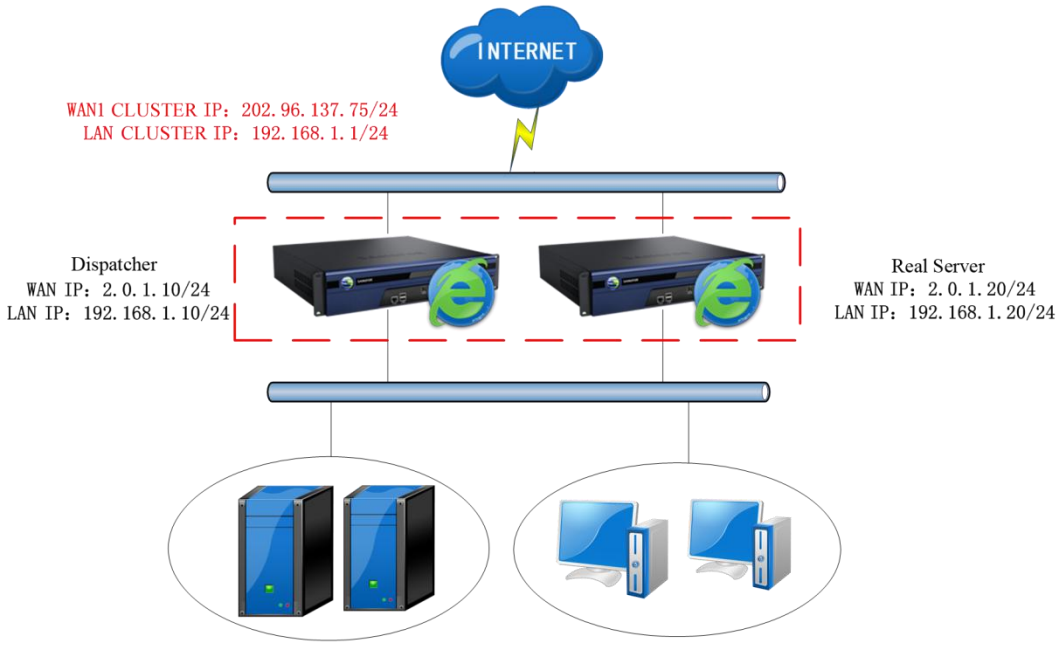
Deploying Clustered Device in Gateway Mode

Background:

- Sangfor device is deployed in cluster mode, in order to improve internal system stability.
- Sangfor device is deployed in gateway mode and directly connected to Internet line.
- The IP address of the Internet line is 202.96.137.75, netmask is 255.255.255.0.

For clustered nodes deployed in **Gateway** mode, the configurations of internal and external interfaces are the same as those on an individual Gateway-mode Sangfor device (please refer to the Device Deployment section in this Chapter). One additional configuration is **Cluster IP Address** of **LAN** interface and **WAN** interface (under **System** > **SSL VPN Options** > **Clustering** > **Cluster Deployment**).

Typical network topology of cluster in **Gateway** mode is as shown in the figure below:



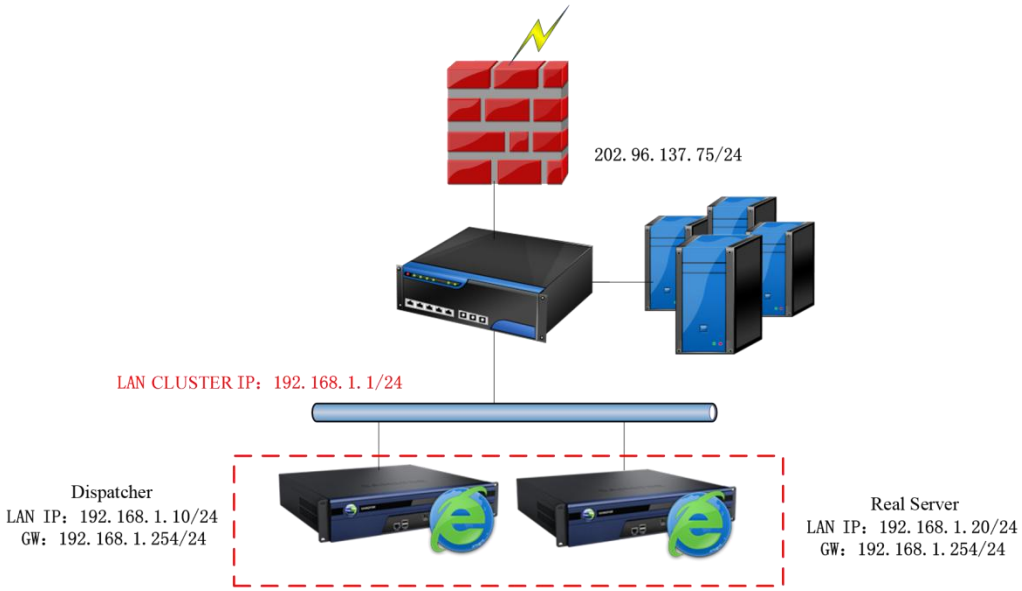
- **LAN Cluster IP** address on every clustered device should be identical; so is the **WAN Cluster IP** address.
- WAN interface IP address on every clustered device should be of a same network segment; whereas **WAN Cluster IP** address and **WAN Interface IP** address configured on a Sangfor device **must NOT** be a same network segment.
- Cluster will not work if the Sangfor device works as gateway and dials up to Internet.

Deploying Clustered Device in Single-Arm Mode

For clustered nodes deployed in **Single-arm** mode, the configurations of internal and external interfaces are the same as those on an individual Single-arm Sangfor device (please refer to the Device Deployment section in this Chapter). One additional configuration is **Cluster IP Address**

of **LAN** interface (under **System** > **SSL VPN Options** > **Clustering** > **Cluster Deployment**).

Typical network topology of cluster in **Single-arm** mode is as shown in the figure below:



- **LAN Cluster IP** address on every clustered device should be identical.
- **LAN interface IP** address (configured in **System** > **Network** > **Deployment**) and the **LAN Cluster IP** (configured in **System** > **SSL VPN Options** > **Clustering** > **Cluster Deployment**) must be of a same network segment.

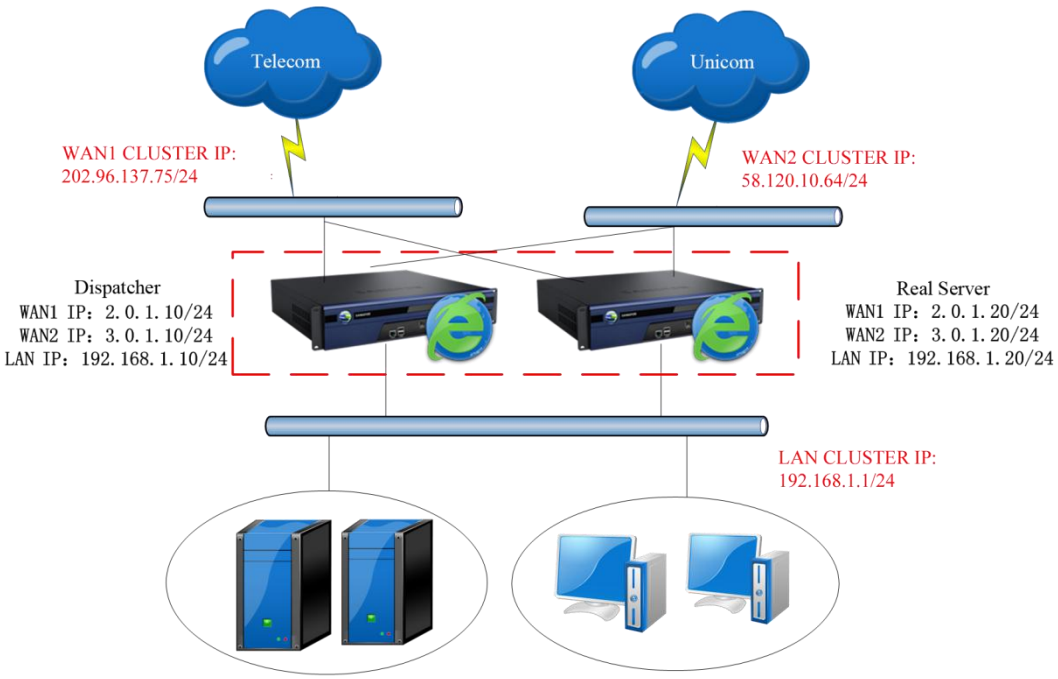
Deploying Clustered Device with Multiple Lines

For clustered nodes deployed with multiple lines, the configurations of internal and external interfaces are the same as those on an individual Sangfor device that has multiple lines (please refer to the Device Deployment section in this Chapter). One additional configuration is **Cluster IP Address** of **LAN** interface and **WAN** interface (under **System** > **SSL VPN Options** > **Clustering** > **Cluster Deployment**).

LAN Cluster IP address on every clustered device should be identical; so is the **WAN Cluster IP address**. As a Sangfor device has more than one line, the **WAN Cluster IP** addresses on every clustered device must be consistent.

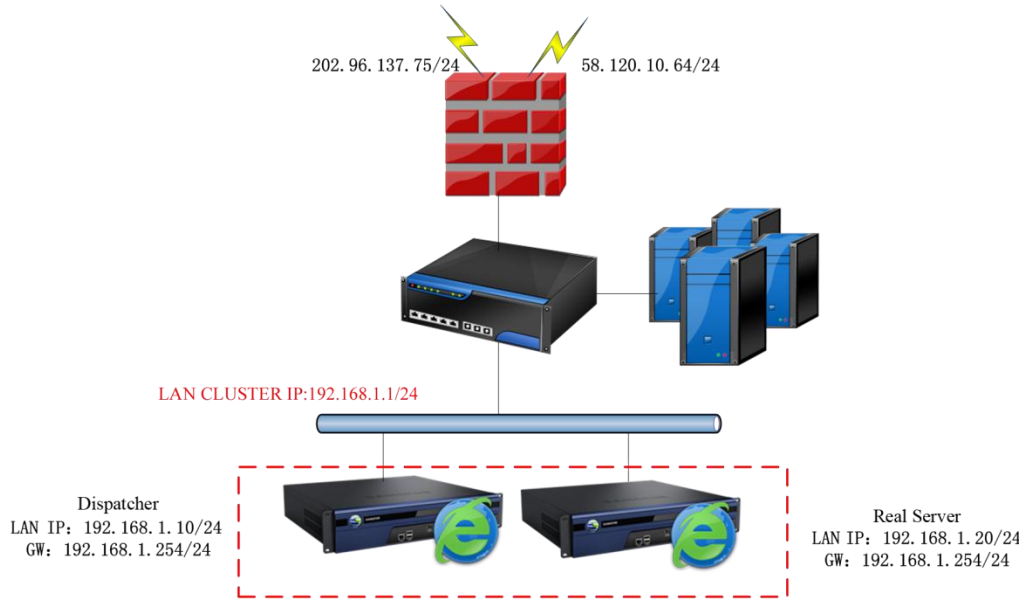
Gateway-mode Sangfor Device with Multiple Lines

Typical network topology of cluster of **Gateway-mode** devices is as shown in the figure below:



Single-Arm Sangfor Device with Multiple Lines

Typical network topology of cluster of **Single-arm** devices is as shown in the figure below:

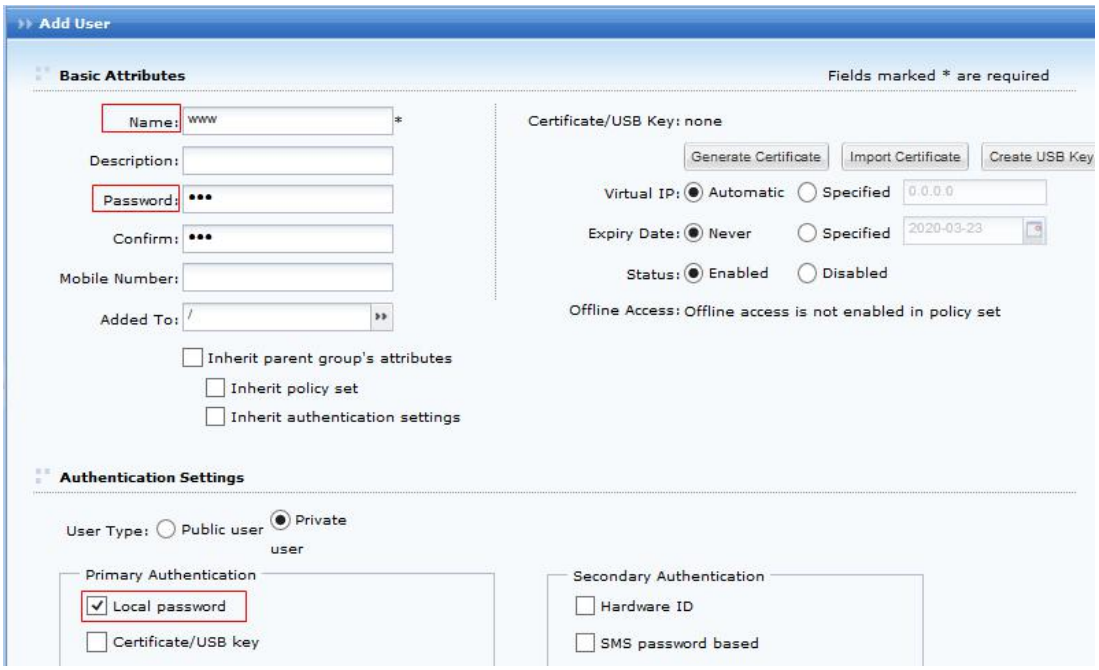


The cluster IP addresses configured on each clustered node (Sangfor device) should be consistent.

Adding User

Adding User Logging in with Local Password

1. Navigate to **SSL VPN** > **Users** > Local **Users s**and click **Add** > **User** to enter the **Add User** page.
2. Configure **Name** and **Local Password** fields.
3. Configure **Authentication Settings**. Select **Local password**, as shown below:

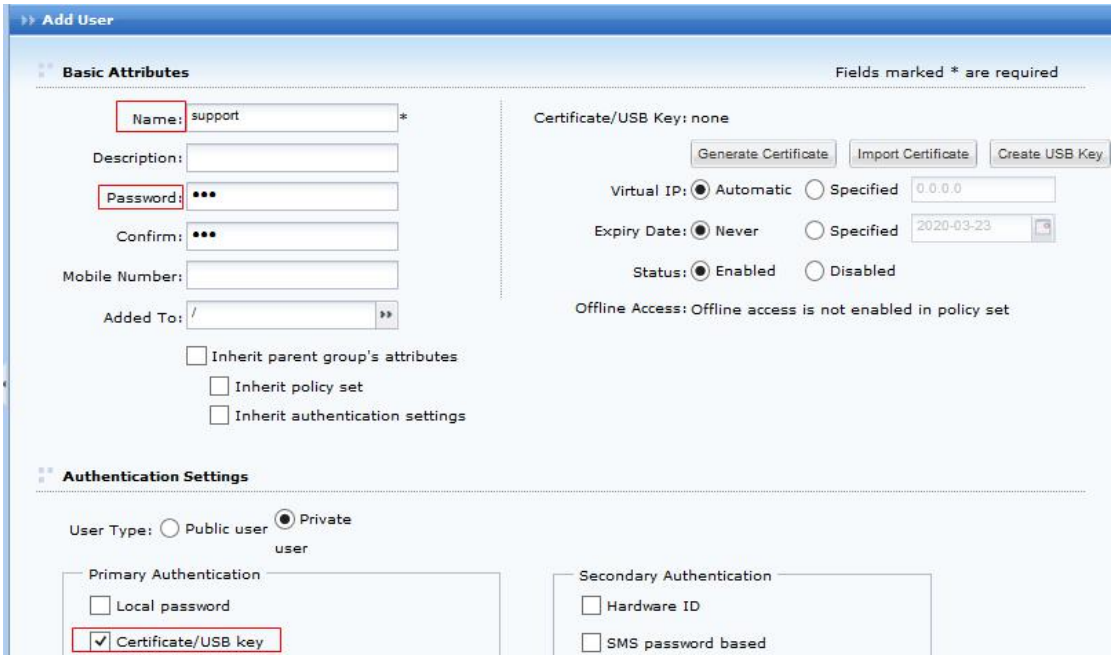


4. Click the **Save** button and **Apply** button to save and apply the settings.

Adding User Logging in with Certificate

1. Navigate to **SSL VPN** > **Authentication** to download and install the USB key driver and USB key tool (for importing USB key).
2. Navigate to **SSL VPN** > **Users** > **Local Users** and click **Add** > **User** to add a new user, as

shown in the figure below:



3. Configure **Name** and **Local Password** fields. Select user type **Private user**.
4. Configure **Authentication Settings**. Select primary authentication **Certificate/USB key**.
5. Click the **Generate Certificate** button to enter the **Generate Certificate** page and generate certificate for this user, as shown in the figure below:



6. Configure the required fields and click the **Generate** button. If certificate is generated successfully, the following prompt dialog will pop up:



7. Click **Download** to save the certificate file **support.p12** to the computer and send it to the end user.

8. End user installs the certificate on his/her computer, visit the login page and select **Use Certificate** login method to connect to SSL VPN, as shown in the figure below:



Configuring VPN Resource

Adding Web Application

Background:

One DNS server and four servers deployed in the enterprise network are providing services for employees:

- ***http://oa.123.com***: an OA system. Server address is 192.168.1.10. The employees mainly work via this platform.
- ***http://bbs***: a website where employees can communicate online. Server address is 192.168.1.11.
- ***http://mail.123.com***: a mail system of the company. Server address is 192.168.1.12.
- ***ftp://ftp.123.com***: a file sharing system of the company. Server address is 192.168.1.13.

Purpose:

Enable employees to access these resources over SSL VPN, but no add-on needs to be installed.

Analysis and solution:

OA system is a JSP-based system. Interactions among units of an OA system are complicated and many scripts and controls need to be invoked. Because of the complexity, defining OA system as Web application is not a wise choice, but TCP application and L3VPN are good choices for it. For the other three resources, they can be defined as Web application because they are static.

To achieve the expected purposes:

1. Navigate to **SSL VPN** > **Resources**, add a TCP resource named **OA System** (address is ***http://oa.123.com***) and associate it with the with the user accounts of the employees (to configure TCP application, please refer to the Adding/Editing TCP Application section in Chapter 4).
2. Navigate to **SSL VPN** > **Resources**, add a Web resource named **bbs** (address is ***http://bbs***) and associate it with the employees.
   a. On the **Resources** page, click **Add** > **Web app** to enter the **Edit Web Application** page, as shown in the figure below:



   b. Choose resource type **HTTP**, and enter the resource address into the **Address** field.
   c. Configure other required fields.
   d. Click the **Save** button to save the settings.
3. Navigate to **SSL VPN** > **Resources**, add a Web resource named **mail** (address is ***http://mail.123.com***) and associate it with the employees.
   a. On the **Resources** page, click **Add** > **Web app** to enter the **Edit Web Application** page, as shown in the figure below:



b. Choose resource type **MAIL**, and enter the IP address of the SMTP server into the **Address** field and the domain name into **Domain Name** field.

c. Configure other required fields.

d. Click the **Save** button to save the settings.

4. Add a Web resource **ftp** (address is ***ftp://ftp.123.com***) and associate it with the employees.

a. On the **Resource Management** page, click **Add** > **Web app** to enter the **Edit Web Application** page, as shown in the figure below:



e. Choose resource type **FTP**, and enter the resource address into the **Address** field and the port into **FTP Port** field.

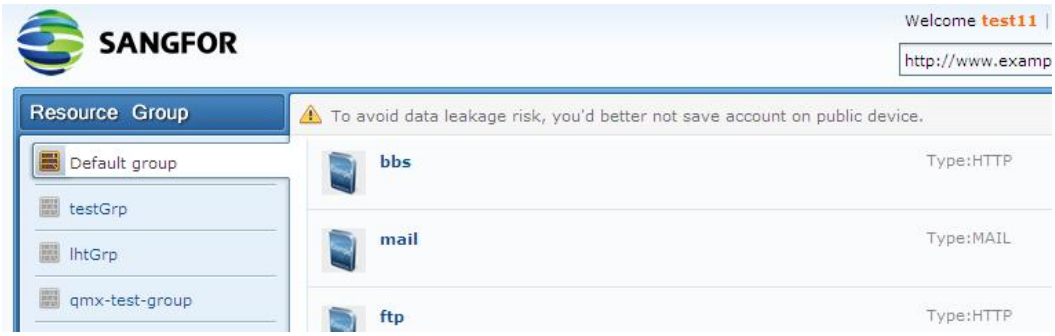
b. Configure other required fields.

c. Click the **Save** button to save the settings.

5. Navigate to **SSL VPN** > **Roles** to add a role, assign the role to the employees, and associate it with the resources named **bbs**, **mail** and **ftp**. For detailed procedure of adding or editing a role, please refer to the Roles section in Chapter 4.

6. Click the **Apply** button (on the yellow bar at the top of the page) to apply the settings.

7. Employees log in to SSL VPN and can visit the resources on the **Resource** page just by clicking on the corresponding resource link, as shown in the figure below:



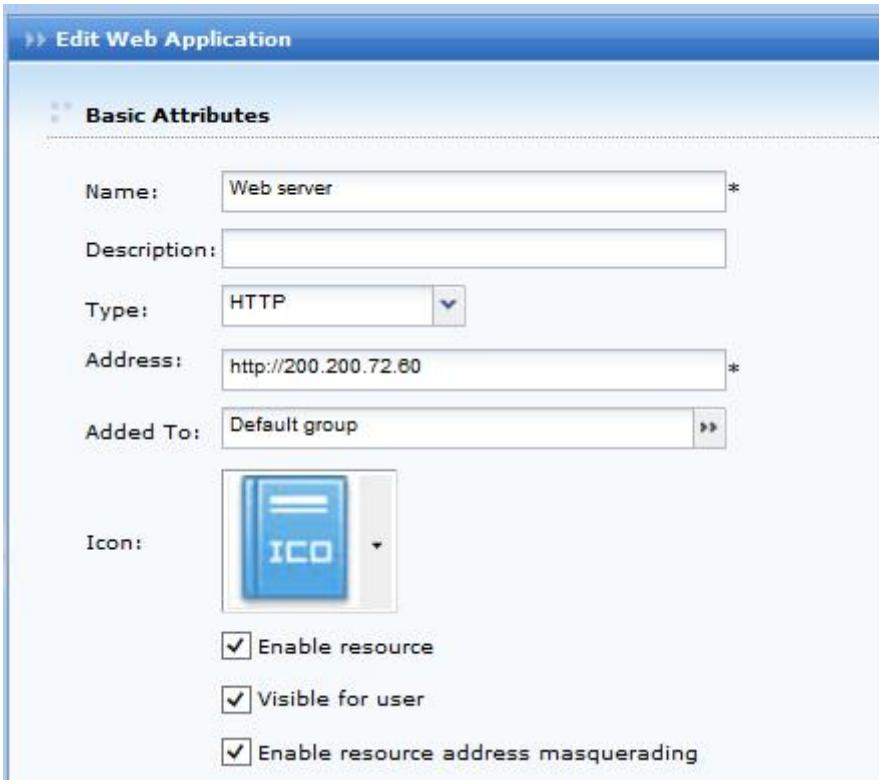
Masquerading Resource Address

Purpose:

Conceal the IP address of the server that provides resource to users. Resource address masquerading only applies to **HTTP**, **HTTPS**, **MAIL** and **FTP** types of Web resources. Real addresses of **FileShare** type of Web resources are visible to users.

To achieve the expected purposes:

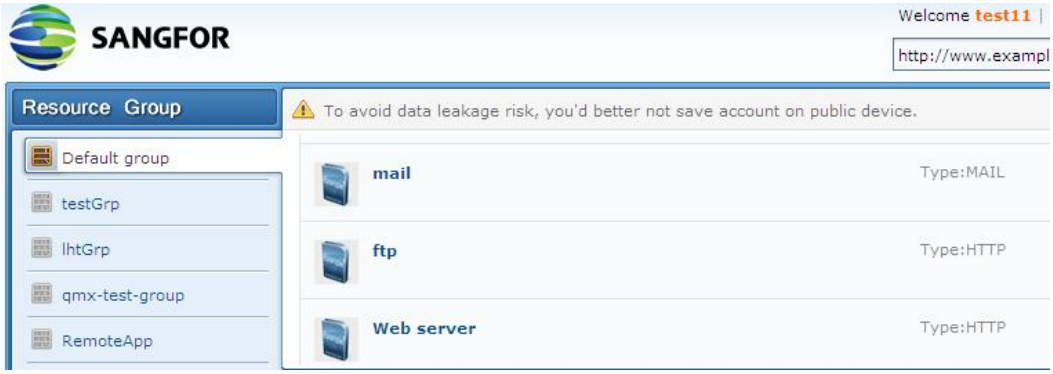
1. Navigate to **SSL VPN** > **Resources** and click **Add** > **Web app** to enter the **Edit Web Application** page.
2. Select resource type **HTTP** and enter the resource address (e.g., *http://200.200.72.60*) into **Address** field. Select the **Enable resource address masquerading** option, as shown below:



3. Associate the resource with the user. For detailed guide, refer to the Adding Role section in

Chapter 4.

4. End user logs in to SSL VPN and enters the **Resource** page. The **Resource** page is as shown in the figure below:



5. Click the resource link to access the resource **Web server**. As shown in the figure below, the URL address of the visited resource is not the real address (200.200.72.60) but a meaningless character string.



Adding FileShare Type of Web Application

Purposes:

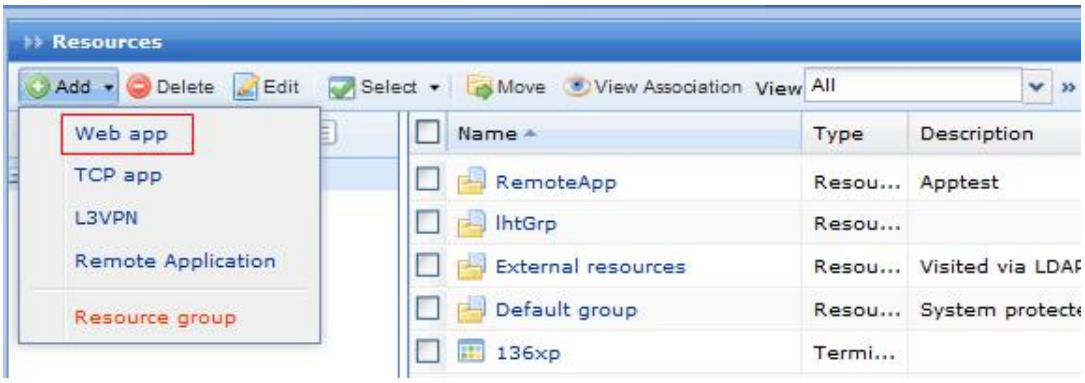
- When the employee **ssl1** accesses the Web-app-based file sharing server (IP: 200.200.72.169), he or she does not need to install any ActiveX control and can enjoy the speedup of access to the file sharing server.
- Employees can log in to the server automatically, without entering username and password.

To achieve the expected purposes:

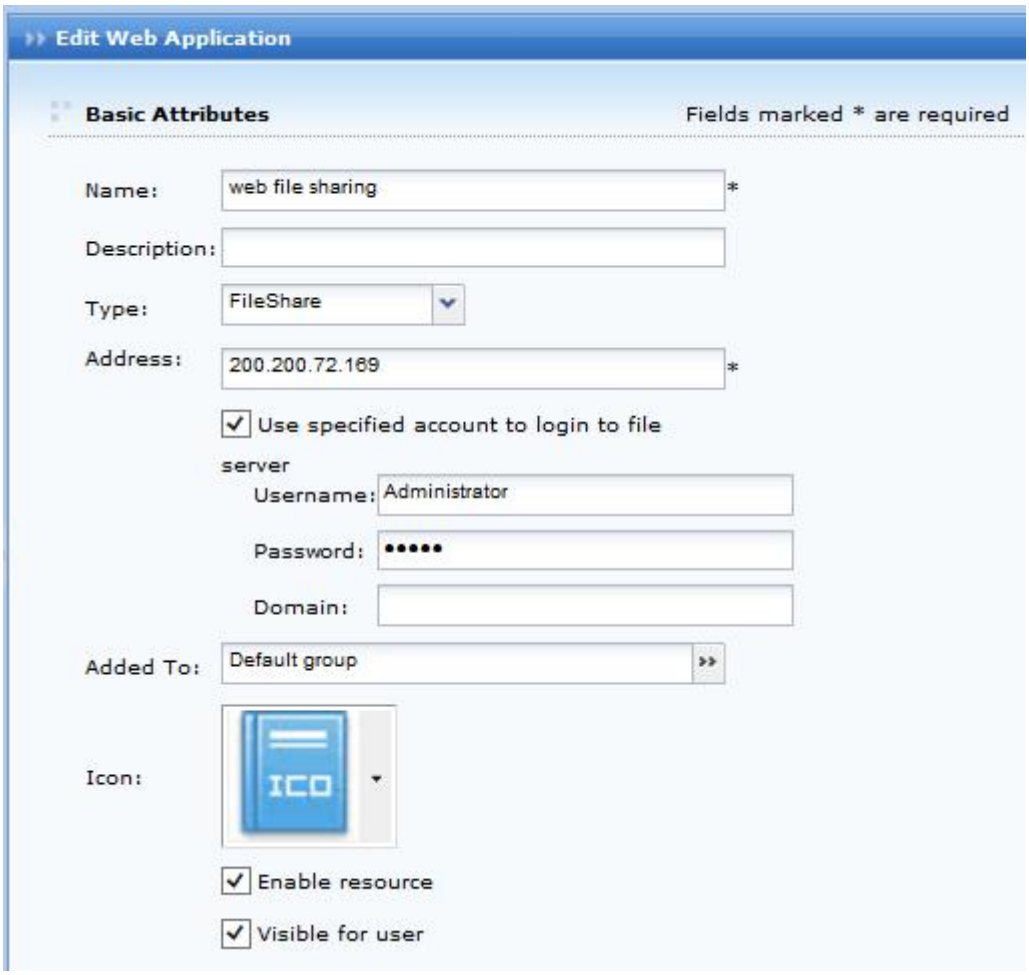
1. Navigate to **SSL VPN** > **Users** and click **Add** to create a user account, as shown below:



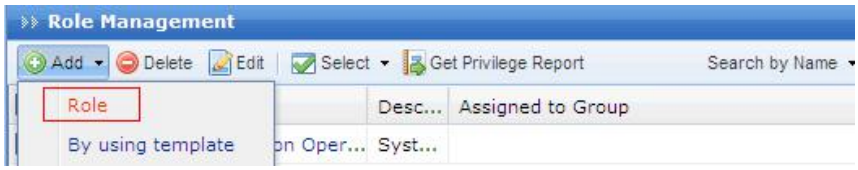
2. Navigate to **SSL VPN** > **Resources** and click **Add** > **Web app** to add a resource, as shown below:



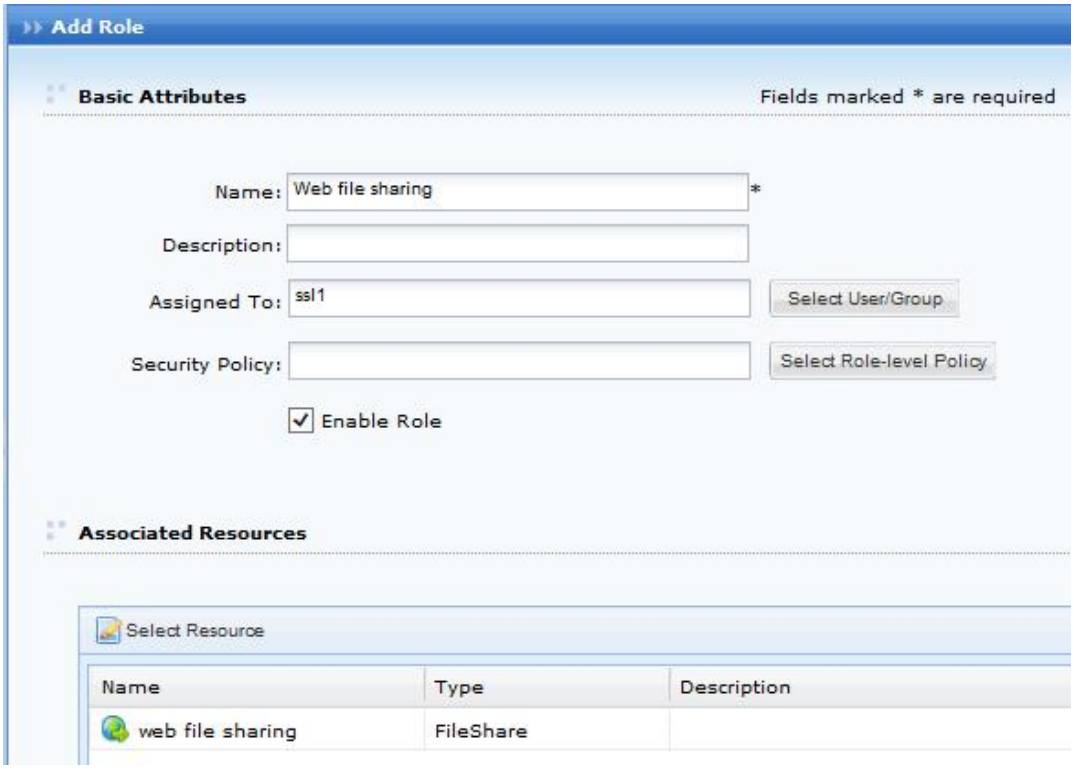
3. On the **Edit Web Application** page, select **FileShare** type of application and configure the other required fields, as shown below:



4. On the **Role Management** page, click **Add** to add a role, as shown below:



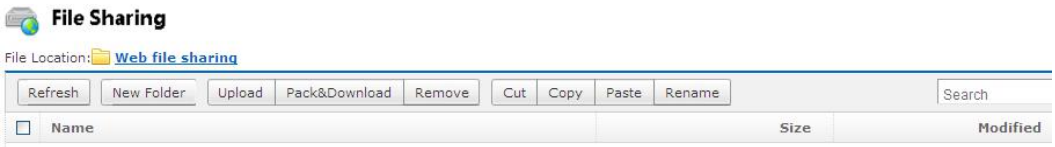
5. On the **Add Role** page, select user **ssl1** added in Step 1 and the resource **Web file sharing** to associate the resource with the user.



6. When the employee uses the user account **ssl1** to connect to SSL VPN, he/she will see the **Web file sharing** resource link on **Resource** page, as shown in the figure below:



7. Click on the resource link and the contents on the Web file sharing server and the available contents will be displayed, as shown in the figure below:



Adding Web Application Enabling Site Mapping

Background:

An OA system is JSP-based system and provides service for employees. Interactions among units of an OA system are complicated and many scripts and controls need to be invoked. Sangfor device is deployed in gateway mode. The network topology of custom network is shown in the figure below:

Purpose:

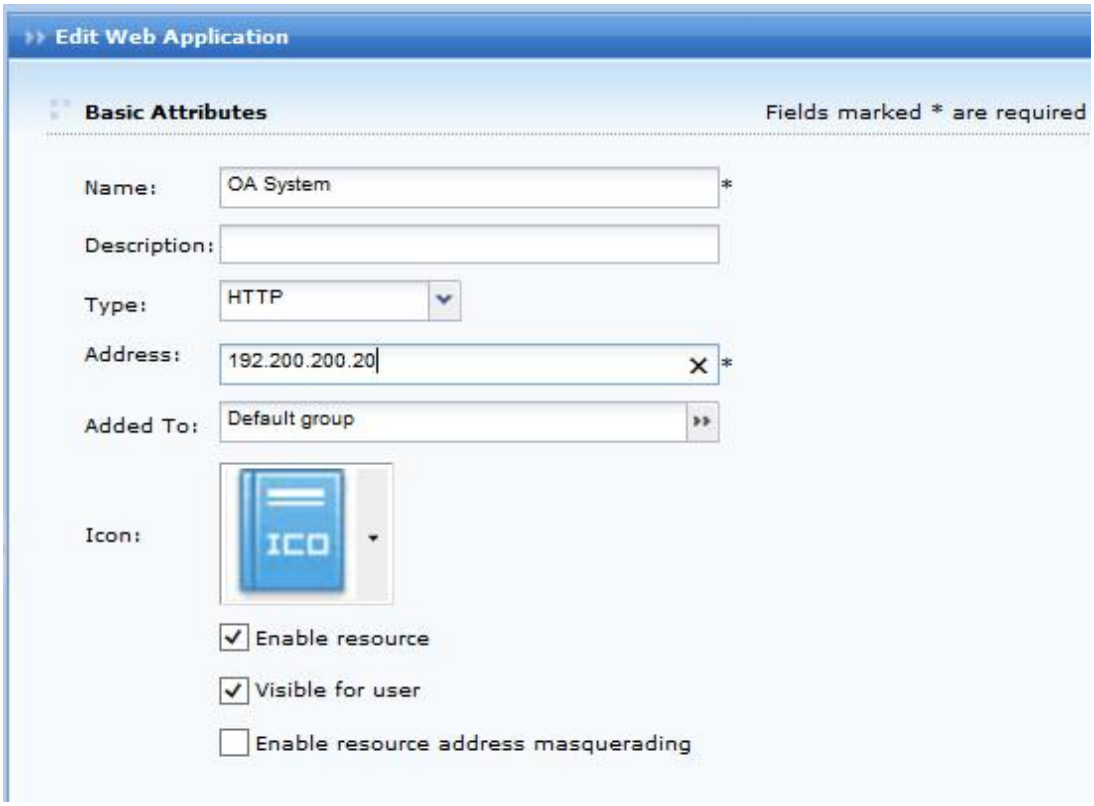
Enable employees to access OA system over SSL VPN easily.

Analysis and solution:

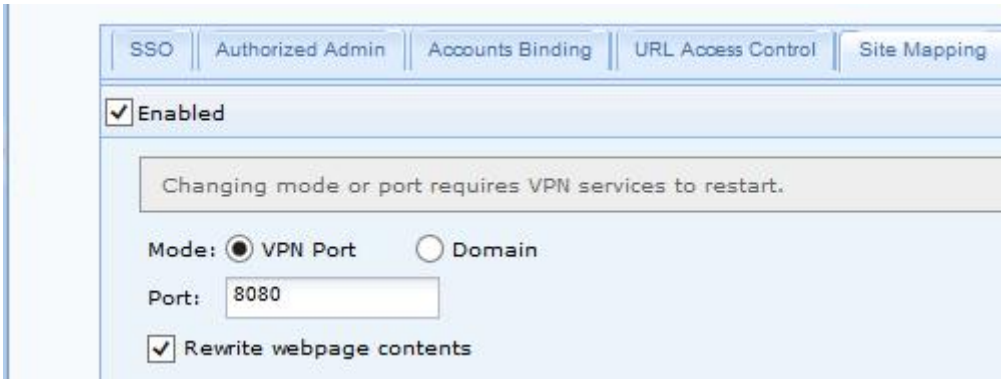
OA system is a JSP-based system. Interactions among units of an OA system are complicated and many scripts and controls need to be invoked. Except defining OA system as Web application, site mapping feature should be enabled for this Web application.

To achieve the expected purposes:

1. Navigate to **SSL VPN** > **Resources**, add a Web resource named **OA System** (address is 192.200.200.20), as shown in the figure below:



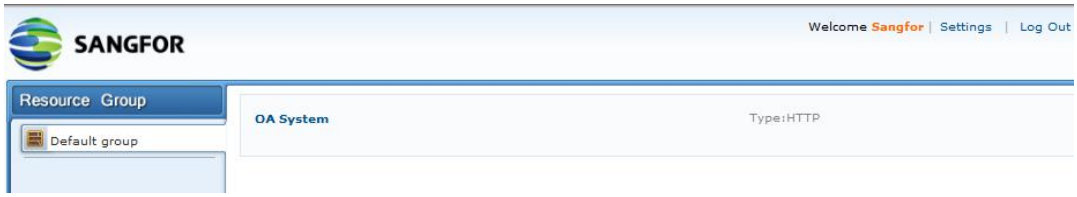
2. Click on **Site Mapping** tab and select **Enabled** to enable site mapping feature. Select VPN Port as **Mode** and enter 8080 in **Port** field. It is recommended to select the **Rewrite webpage contents** option. If it is selected, the webpage containing lots of scripts can be modified and rewrote.



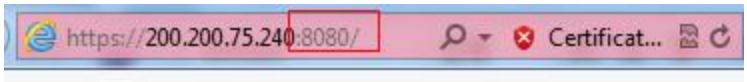
3. Navigate to **SSL VPN** > **Roles** to add a role, assign the role to the user **Sangfor**, and associate it with the resource named **OA System**. For detailed procedure of adding or editing a role, please refer to the Roles section in Chapter 4.

4. Click the **Apply** button (on the yellow bar at the top of the page) to apply the settings.

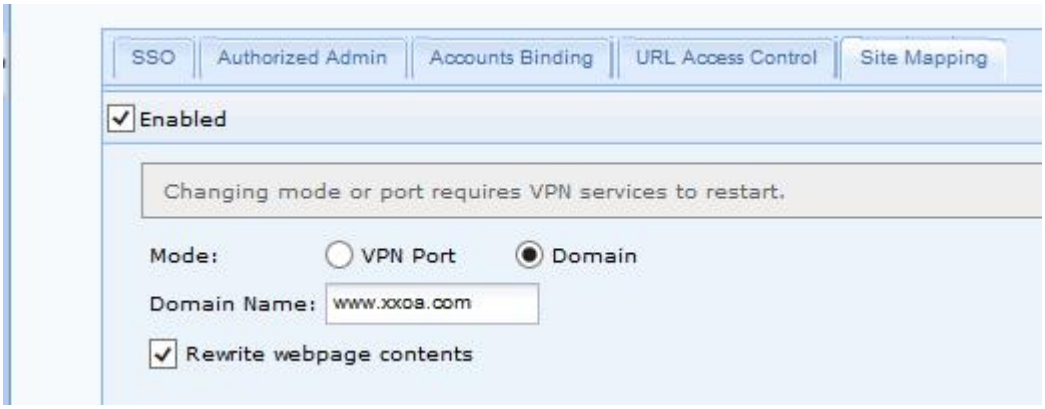
5. User **Sangfor** logs in to SSL VPN and can visit the resources on the **Resource** page just by clicking on the corresponding resource link, as shown in the figure below:



6. Click the resource link to access the resource **OA System**. As shown in the figure below, the URL address of the visited resource is not the real address.



If there is a domain name, obtained from ISP, directing to the Sangfor device, you can also select Domain as **Mode**, and enter the domain name into **Domain name** field in step 2, as shown below:





- Resource address masquerading and site mapping which is also called Easylink cannot be enabled together.
- The VPN port mapped to Web application cannot be used by other application.
- The domain name mapped to Web application cannot be used to connect to SSL VPN. User can connect to SSL VPN by typing the IP address of Sangfor device or other domain name. One domain name can only be mapped to one Web application.
- The Easylink resource mapped to VPN port can be accessed by typing corresponding address into the toolbar of IE browser, while the Easylink resource mapped to domain name cannot be accessed through typing domain name into toolbar.
- In case that Sangfor device is deployed in single-arm mode and port mapping is enabled, Web application is mapped to port 8080 of Sangfor device, corresponding port of front-end firewall needs to be mapped to Sangfor device, except mapping port 443, and access through port 8080 needs to be allowed by firewall.

Configuring TCP Application

Adding TCP Application

Background:

One DNS server and two servers are deployed in the enterprise network, providing services for the employees:

- *http://oa.123.com:* an OA system. Server address is 192.168.1.10.
- Accounting system: Server address is 192.168.1.15 and port is 4003, providing services such as pay rolling, payment claiming, etc.

Purposes:

- Enable employees to access OA system directly (i.e., visit OA system through browser).
- Employees can open the accounting system, and connect to the server over SSL VPN.

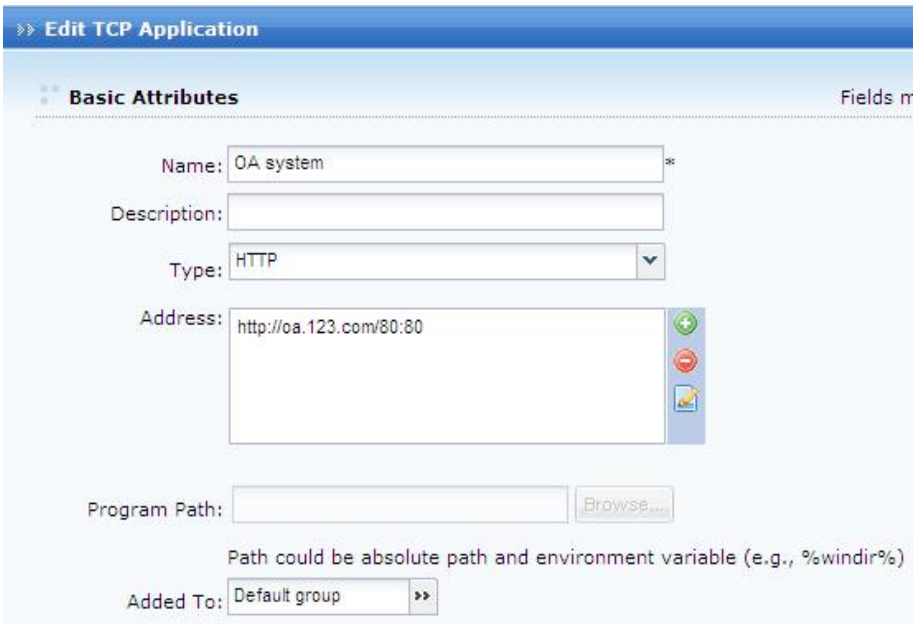
Analysis and solutions:

Both the OA system and Accounting system can be defined as TCP application. Since OA system is a type of system involving immense interactions and some even need links to a number of servers, we need to use the feature **Smart recursion of resource access** (for more details, please refer section TCP App Resource Options in Chapter 4).

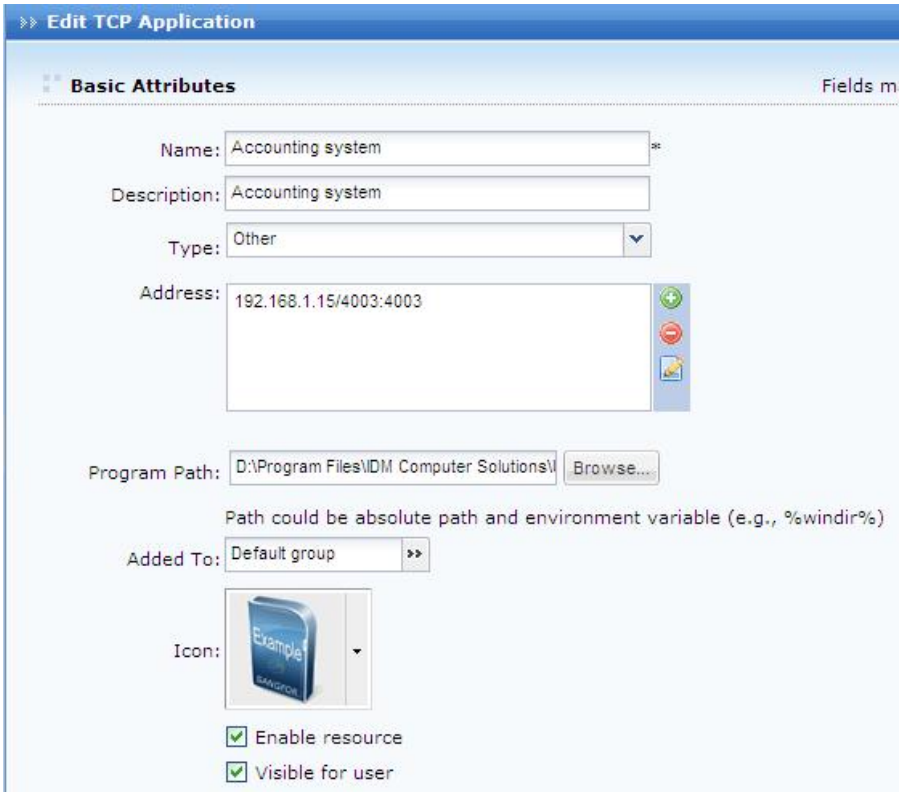
To achieve the expected purposes:

1. Navigate to **SSL VPN** > **Resources**. Click **Add** > **TCP app** to enter **Edit TCP Application**

page and add a TCP application (named **OA System**, with address ***http://oa.123.com***)., as shown below:



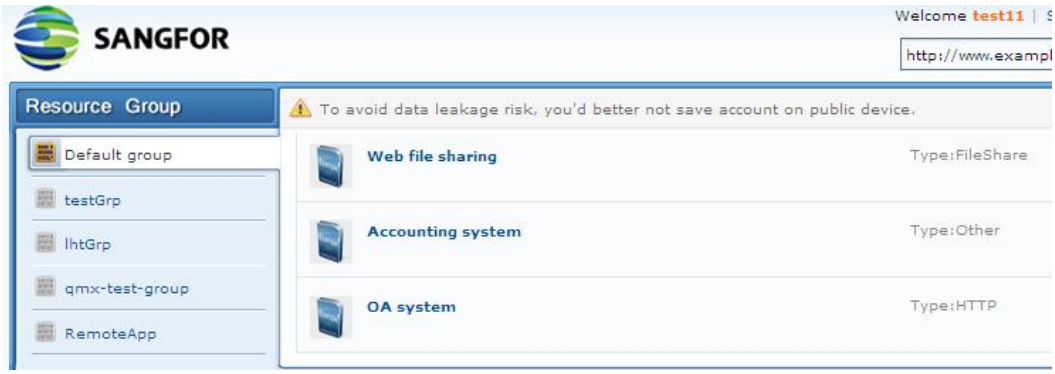
2. Click **Add** > **TCP app** to enter the **Edit TCP Application** page and add a TCP application (named **Accounting system**, server address: 192.168.1.15 and port is 4003), as shown below:



Choose the application type **Other** and specify the address and port.

3. Add or edit a role to associate the two resources (**OA System** and **Accounting system)** with it and assign the role to user (for detailed guide, please refer to the Adding Role section in Chapter 4).

4. After logging in to the SSL VPN with the specified SSL VPN account, the employees will see the resource link, as shown in the figure below:



OA system could be accessed when the employee clicks on the resource link, or visiting the server through browser.

The accounting system could be accessed directly by clicking the link if program path is specified in step 2. If it is not specified, employee needs to launch the program manually after clicking resource link.

Configuring URL Access Control Feature

Background:

A file server (*duan.sslt.com*) is deployed in the enterprise network, providing services for the employees.

Purposes:

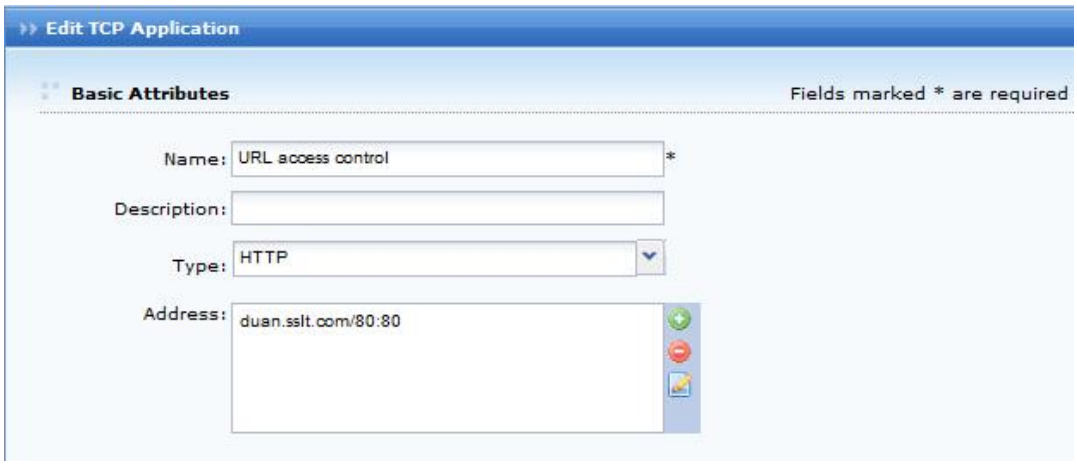
Only allow the members from **Finance** department to access this file server, and only the directory ***duan.sslt.com/frame*** can be accessed by them, others directory of the file server being inaccessible.

Analysis and solution:

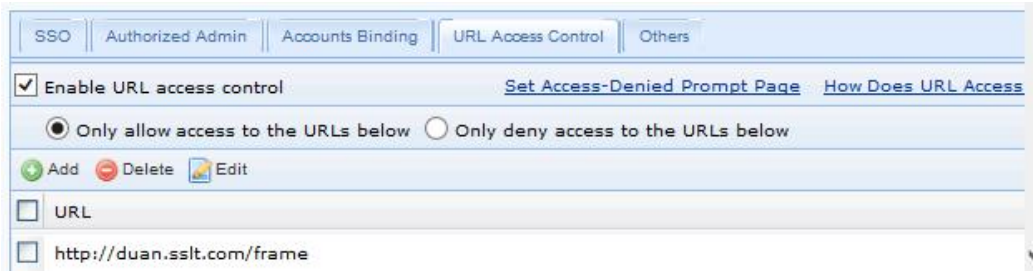
URL access control feature can achieve control over the access to the file server.

To achieve the expected purposes:

1. Navigate to **SSL VPN** > **Resources** and add a TCP application (named **URL access control**, URL: *duan.sslt.com*), as shown in the figure below:

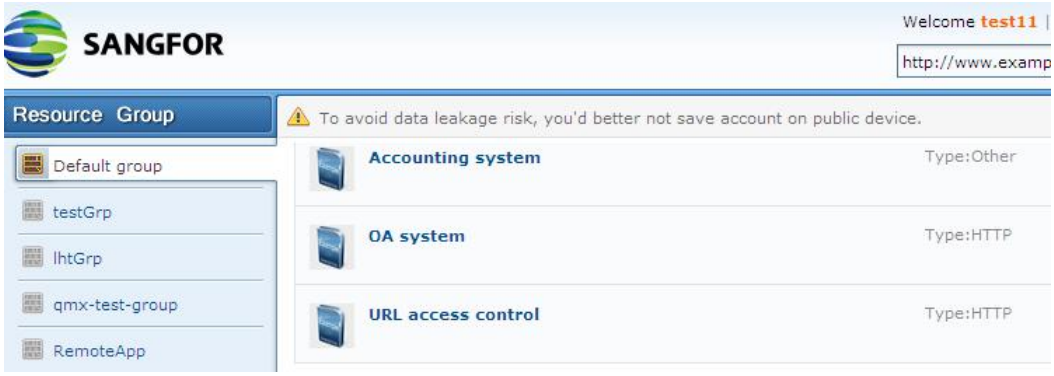


2. Click the **URL Access Control** tab, select the option **Only allow access to the URLs below** and add a new entry (URL: *http://duan.sslt.com/frame*) into the list, as shown below:



3. Create or edit a role and associate the resource with the user account of the employee (for detailed guide, please refer to the Adding Role section in Chapter 4).

4. After logging in to the SSL VPN with the specified SSL VPN account, the employees will see the resource link, as shown in the figure below:



5. To access the **frame** directory, the employees needs only to click the **URL access control** link. Access to the upper-level directory will be denied.

Adding L3VPN Application

Background:

192.168.1.10-192.168.1.15 is a subnet in the enterprise network.

Purposes:

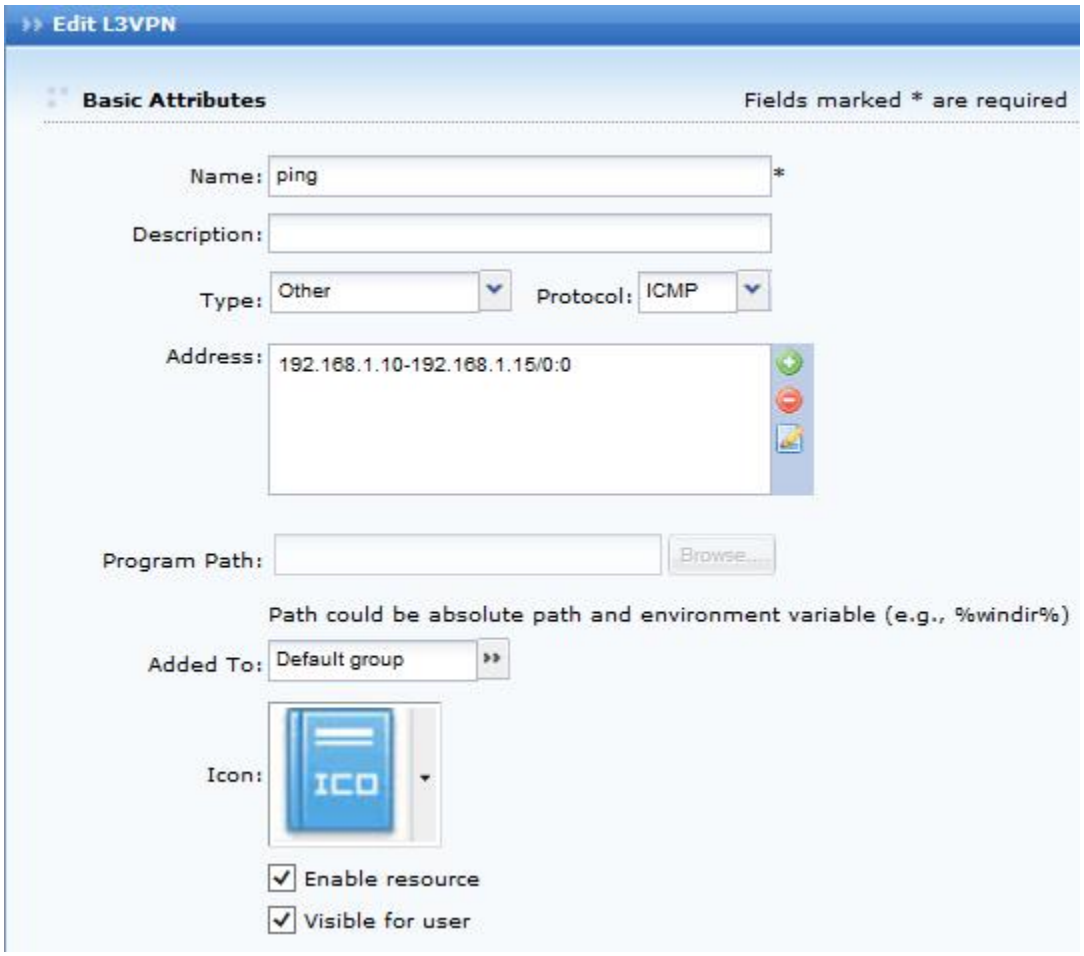
Enable network administrator to access internal machines on subnet 192.168.1.10-192.168.1.15 over SSL VPN

Analysis and solution:

For network administrator, defining the remote computers as L3VPN resource would allow him/her to access these machines remotely.

To achieve the expected purposes:

1. Navigate to **SSL VPN** > **Resources** and click **Add** > **L3VPN** to enter **Edit L3VPN** page, as shown in the figure below:



Enter resource name (for example, ping), configure other required fields and click the **Save** button to save the settings.

2. Add or edit a role to associate the resources **ping** with it and assign the role to the network administrator (for detailed guide, refer to the Adding Role section in Chapter 4).
3. Click the **Apply** button to apply the settings.
4. After network administrator logs in to the SSL VPN, he/she will see associated resources, as shown in the figures below:



Network administrator can launch CMD.exe on local PC to ping the connectivity of the computers residing in the network segment 192.168.1.10-192.168.1.1.

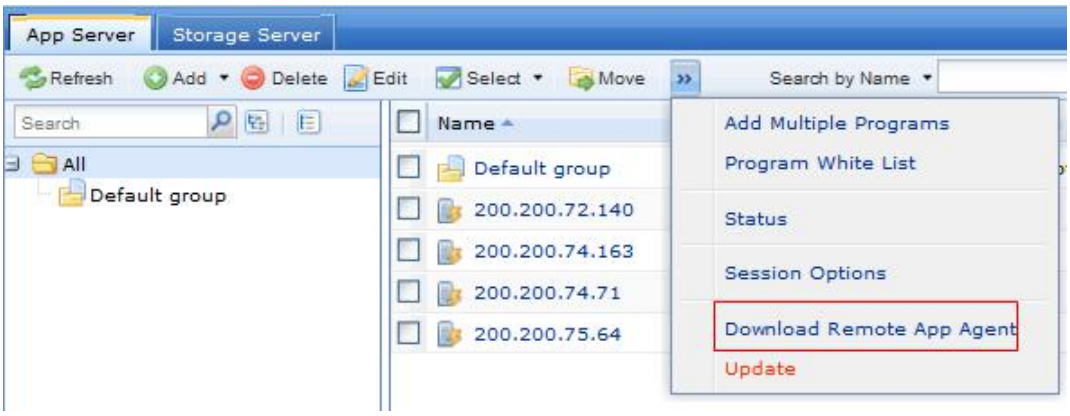
Adding Remote Application

Purposes:

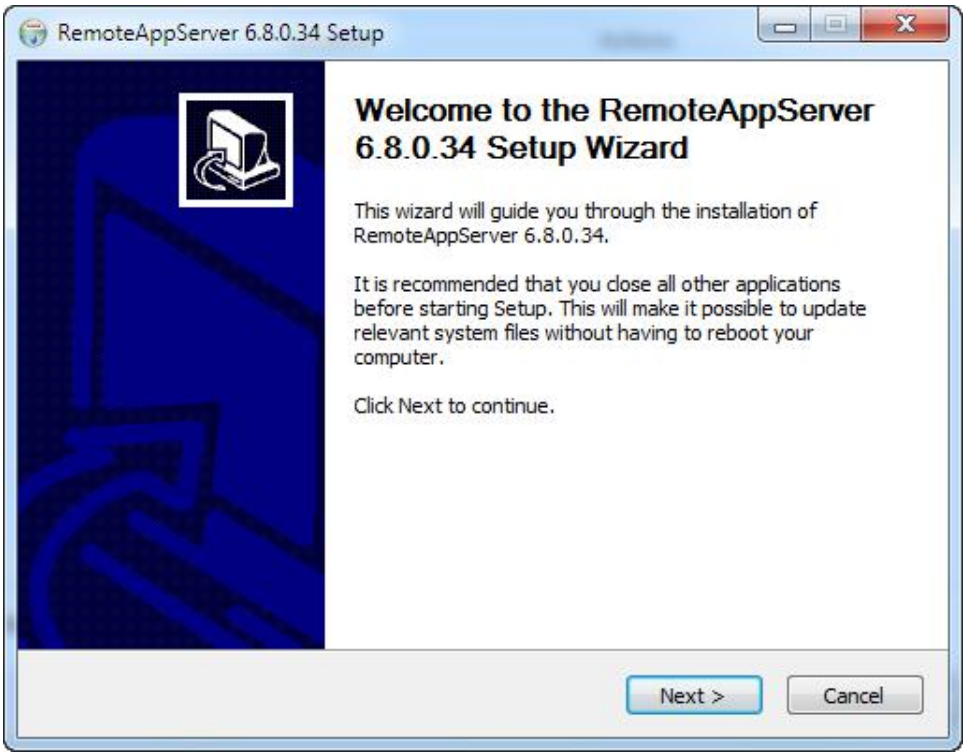
Enable employees to access **WordPad** on the remote application server (IP: 172.16.253.119, port: 7170) and save modified file to private directory or public directory on remote server.

To achieve the expected purpose:

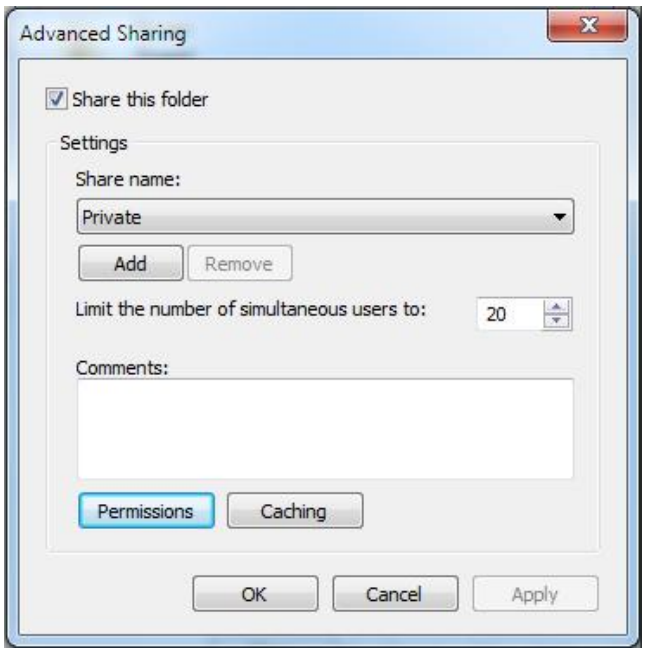
1. Install Terminal Service and RemoteAppAgent program. To download RemoteAppAgent program, navigate to **SSL VPN** > **Remote Servers** to enter the **App Server** page and click **Download RemoteApp Agent** to download the RemoteApp Agent program, as shown below:

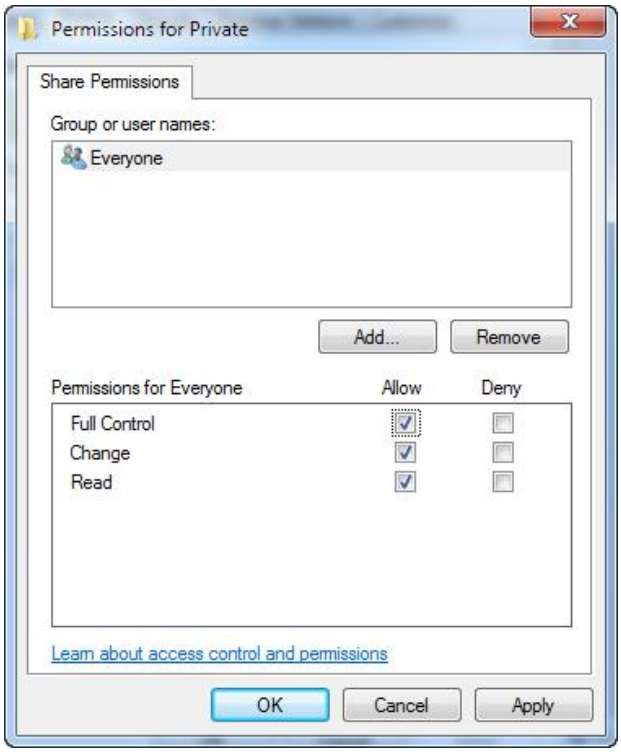


2. Double-click the executable file named **SFRemoteAppServerInstall.exe** and follow the instructions to install the RemoteApp Agent, as show in the figure below:



3. Create private folder and public folder on storage server. The file system format should be NTFS. Share this private directory and specify user permission for access to this folder.





4. Navigate to **SSL VPN** > **Remote Servers** to enter the **App Server** page and click **Add** > **Server** to add an application server, as shown below:

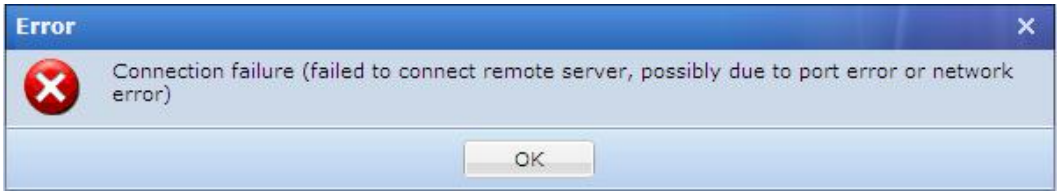


5. Configure admin account, password, and other required fields and make sure the application server can connect to the Sangfor device. You can click the **Test Connectivity** button to check whether this remote application server can be connected.

   If the following prompt appears, the Sangfor device is then connected to the remote application server successfully.



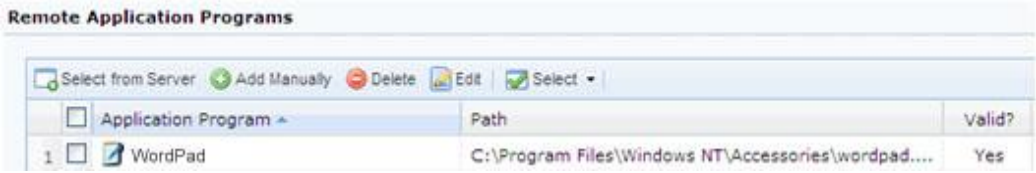
If the following prompt appears, the SSL VPN cannot connect to remote application server. In that case, check whether the remote server is configured properly.



6. Under **Remote Application Programs**, click **Select from Sever** to select the application program **WordPad**, as shown in the figure below:

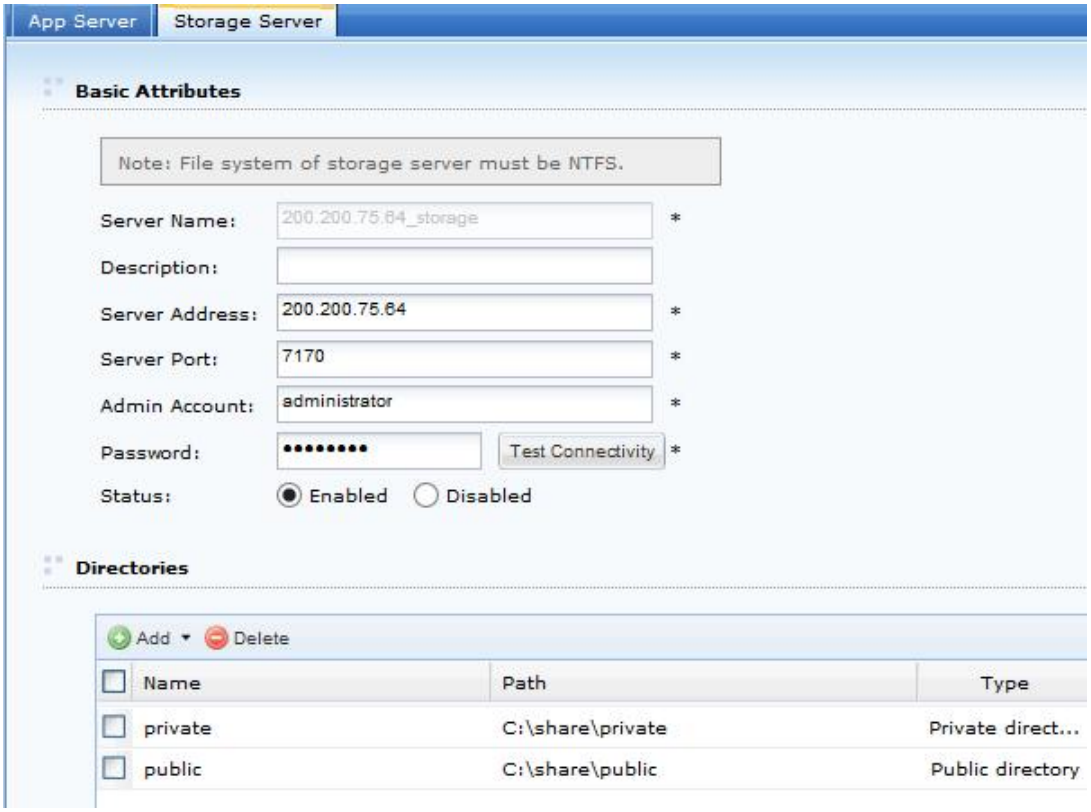


7. The selected programs are seen in the figure below:



8. Click the **Save** button on the editing app server page to save the settings.

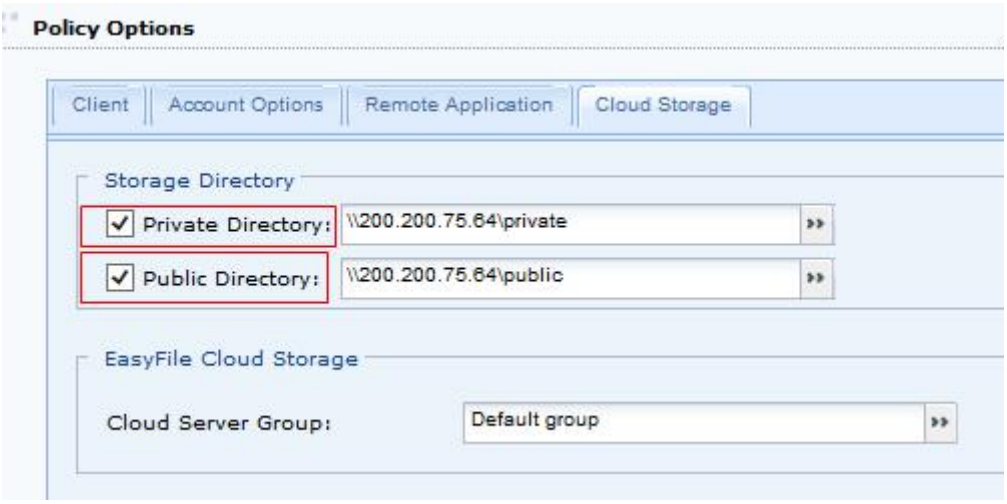
9. Go to **SSL VPN** > **Remote Servers** > **Storage Server** to enter the **Storage Server** page, click **Add** to add a storage server and create private directory and public directory for it, as shown below:



10. Navigate to **SSL VPN** > **Policy Sets** to enter the **Policy Sets** page and add a policy set that will associate with the corresponding user (for procedures of configuring policy set, refer to the Adding Policy Set section in Chapter 4). While configuring the **Remote Application** tab (as shown in the figure below), ensure the following:

    - The user account for logging in to the remote application server is the **SSL VPN account** or **Windows account created as per the SSL VPN account**.
    - Directory is specified, so that the data or files in remote application session will be saved in the storage server and available to user for future access. Private directory indicates that a folder will be created in the specified directory automatically when user connects to the remote server, and is solely visible for that user.





11. Associate the policy set with the corresponding user (for detailed guide, refer to the Adding User section in Chapter 4).

12. Navigate to **SSL VPN** > **Resources** to add a remote application resource (for detailed guide, refer to the Adding/Editing Remote Application section in Chapter 4), as shown below:



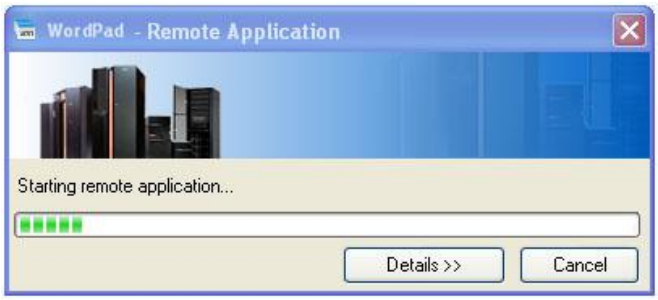
13. Click the **Select** button (next to **Program** field) to select program **WordPad**, as shown below:



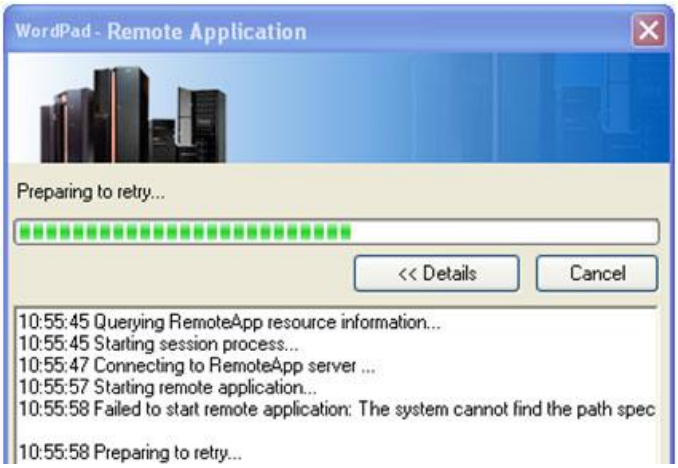
14. Click the **OK** button to save the settings and the program name is seen in the **Program** field.



15. In the **App Server** tab, select an application server to publish **WordPad**.
16. Navigate to **SSL VPN** > **Roles** to associate this remote application resource with the corresponding user (for detailed guide, please refer to the Roles section in chapter 4).
17. After the employee logs in to the SSL VPN, he or she will see the **Resource** page with the resource link to that remote application.
18. Click on the link to the remote application resource created in Step 12, and a remote application session will be established, as shown in the figure below:

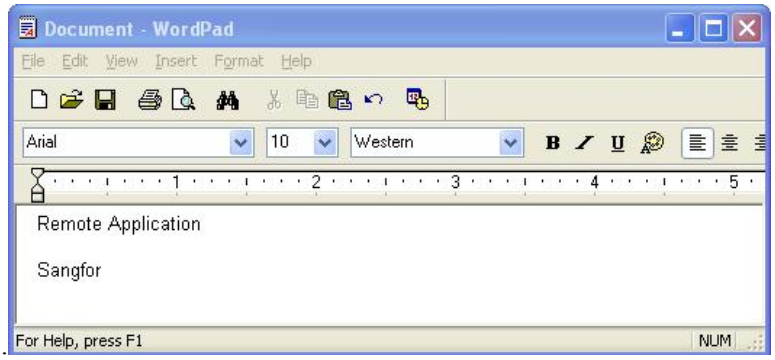


19. To view the connecting process, click the **Details** button. Progress details will be seen as follows:



Once the session is established successfully, **WordPad** will be launched. The employee can

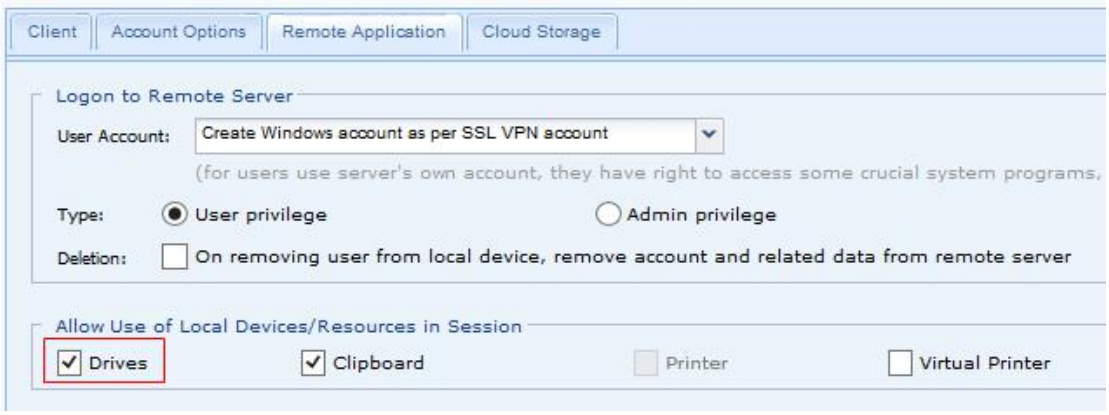
edit and save the document to the specified directory on the remote storage server. Next time logging in to SSL VPN, he or she can edit this document again in remote application session



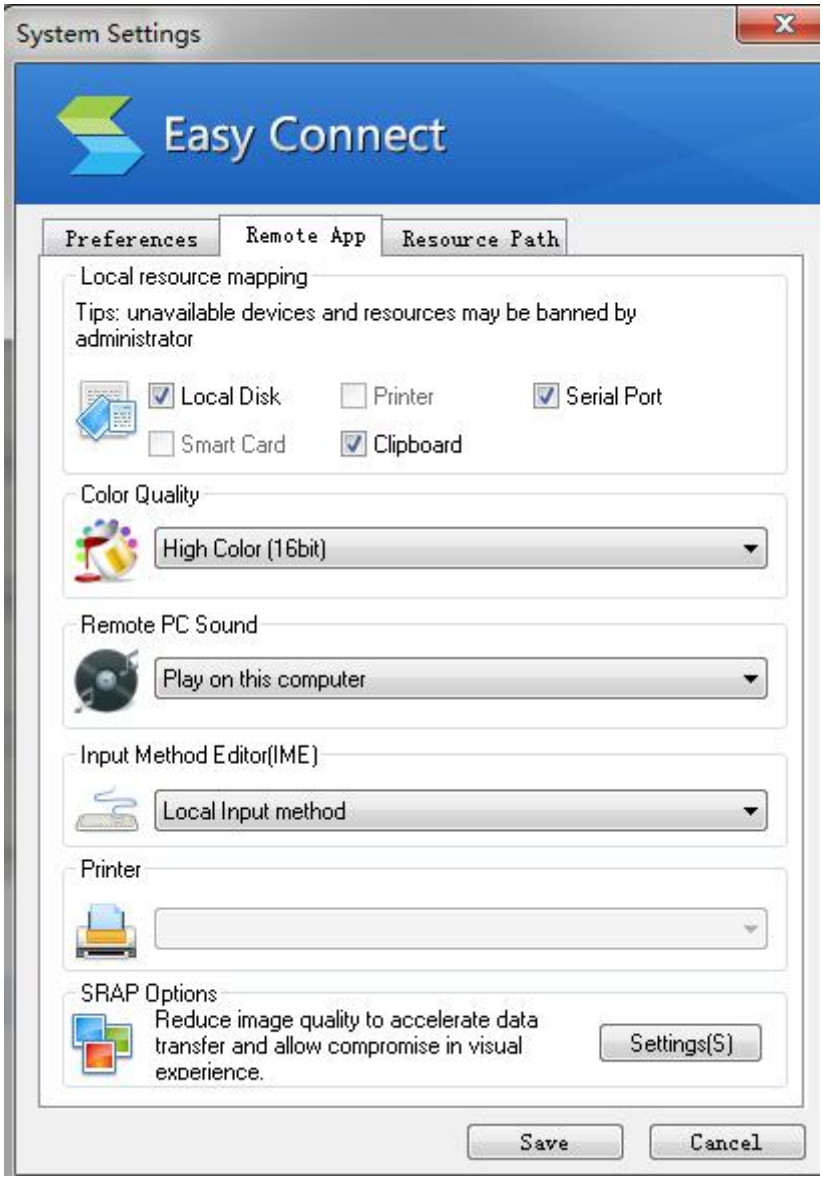
If the employee wants to save the modified file on client side. There are two methods to achieve that:

Method 1:

a. Select **Drives** option on **Remote Application** tab when adding/editing policy set, as shown in the figure below:



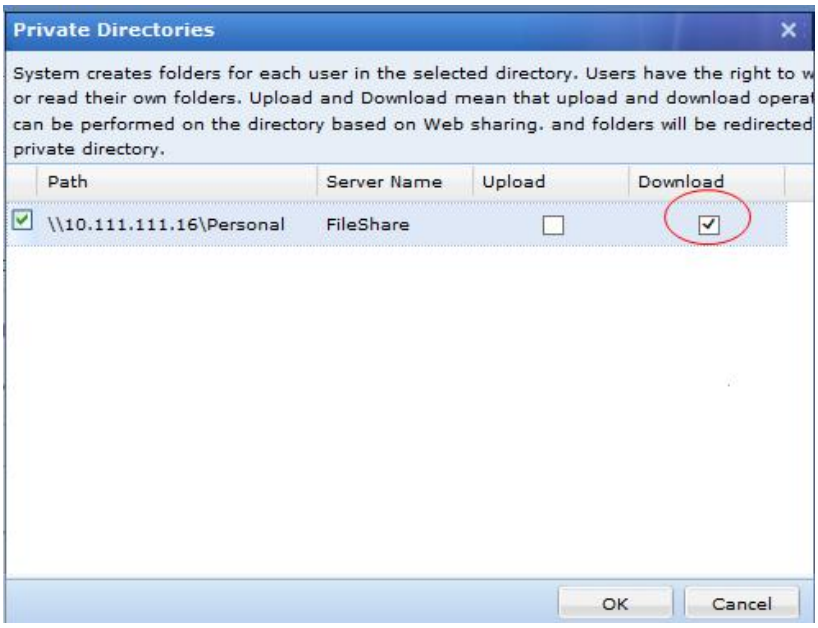
b. Log in to SSL VPN using VPN client. Right-click on VPN client logo and click on **System Settings** to enter the **System Setting** page and click **Remote Application** tab to enter the following page, as shown below, and select the **Local Disk** option.



Click **Save** to save the changes. Then you can save file to the local drives.

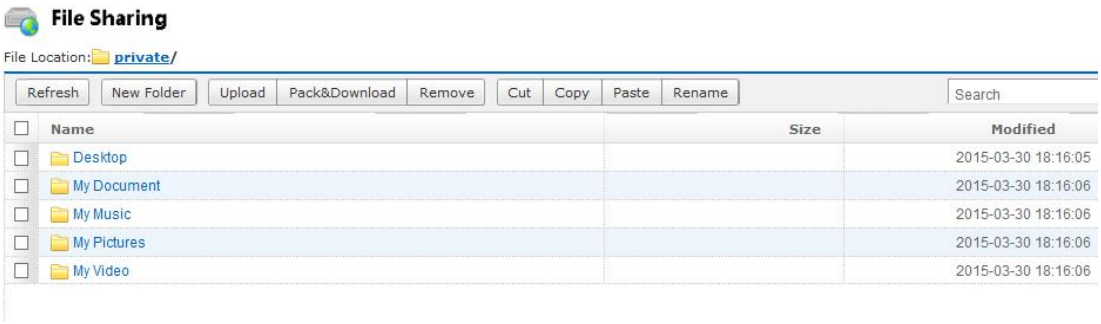
Method 2: Download the file by the means of file sharing

a. Select **Download** when selecting private directory or public directory on **Cloud Storage** tab, as show in the figure below:



b. Log in to SSL VPN and right-click on VPN client logo, you will see the following figure:

c. Click **Private Directory** to enter the **File Sharing** page, as shown in the figure below and you can download desired file here:



Configuring Authentication with External CA

Using External CA Root Certificate to Generate Device Certificate

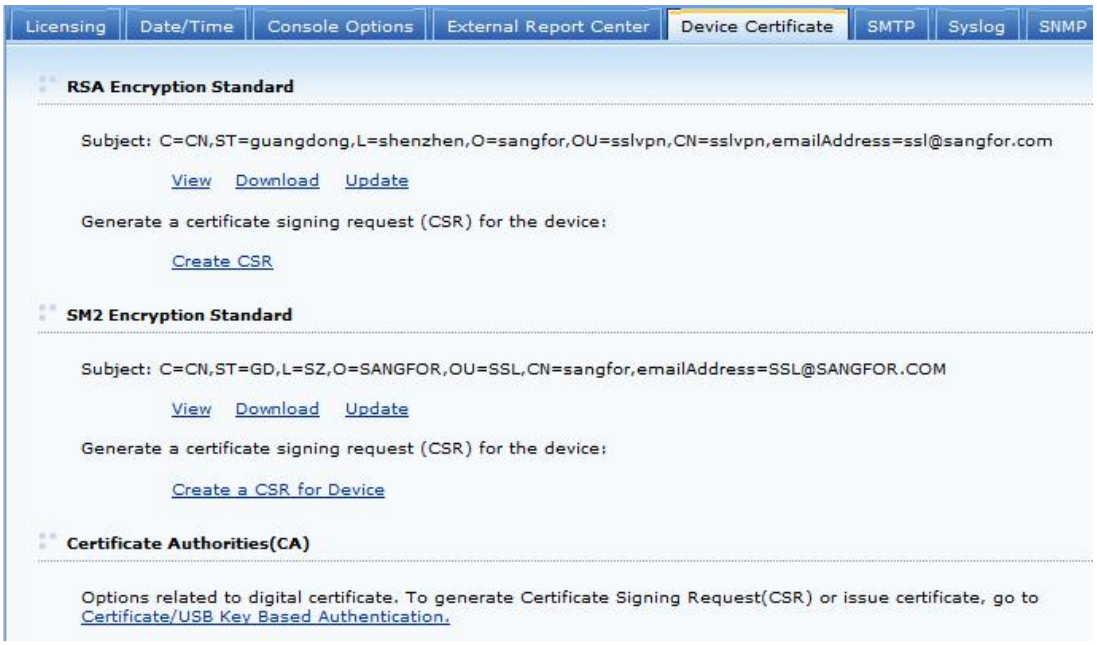
Purpose:

Import and use the external CA root certificate to generate certificate for the Sangfor device, so that end users can pass certificate based authentication when logging in to the SSL VPN if they

own certificates issued by that external CA.

To achieve the expected purpose:

1. Navigate to **System** > **System** > **Device Certificate**, as shown in the figure below:



2. Click the **Create CSR** button to generate a certificate signing request (CSR) for the Sangfor device. The **Create a CSR for Device** page is as shown in the figure below:



3. Configure the required fields. In this scenario, country is **CN** (China), state is **GD** (Guangdong), city is **SZ** (Shenzhen), company is **SANGFOR**, department is **SUPPORT**, email address is **support@sangfor.com.cn**, and the certificate is issued to the login page (address is **10.111.111.3**) to the administrator Web console of Sangfor device.

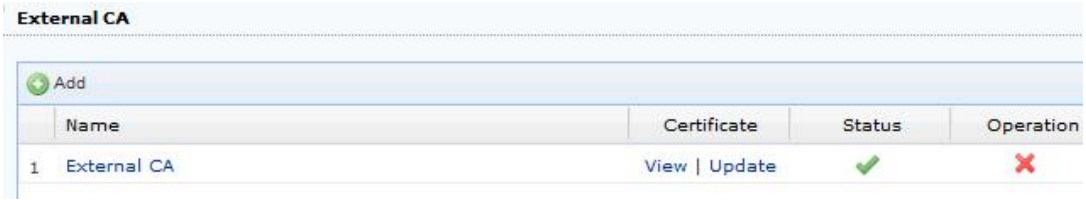


- Country should be a two-letter abbreviation.
- State name can contain a maximum of 20 characters.

4. Click the **OK** button to save the settings.
5. Once the CSR is generated, click **Download** to download the request or copy the above request contents into a text file. The contents in the .csr file are as shown below:

-----BEGIN CERTIFICATE REQUEST-----
MIIB0DCCATkCAQAwgY8xCzAJBgNVBAYTAkNOMQswCQYDVQQIEwJHRDELMAkGA1UE
BxMCU1oxEDAOBgNVBAoTB1NBTkdGT1IxEDAOBgNVBAsTB1NVUFBPUlQxGzAZBgNV
BAMTEnd3dy5zYW5nZm9yLmNvbS5jbjElMCMGCSqGSIb3DQEJARYWc3VwcG9ydEBz
YW5nZm9yLmNvbS5jbjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAxLfml4gT
VGib8SuYYvy4txDzSN6DrGI031kAZRHRw77tEs8LbEu1HozLwCSfZDVgk3fueOBe
K3dkkx7nsZ+QMZ/OiCOLnoJuzH+SXwsb1OSN0u3z633wYlh1qS2n04nB51kKPc9I
rcohT9sDXHEsf8NZJeh+6u9y2xnTCdjfNxECAwEAAaAAMA0GCSqGSIb3DQEBBQUA
A4GBAChre1tw+81CkkB6QCKaX71Wih88K0QEUntW5nZCjW+rlTBwKzZAl3oxAN8I
BX99sSiDKu5Hruh3TN4jk5R+VbCtHW7rPkdJPK0df26Sv1REVuw6p7u1xr/qVJyV
OHCYdmjA8e0mVZMLVYu9m0BjMZe1Udfxaef82xr9ehKpM+K4
-----END CERTIFICATE REQUEST-----

6. Submit the generated CSR to the external CA.
7. Get the Sangfor device certificate from the external CA.
8. Navigate to **SSL VPN > Authentication > Certificate/USB Key Based Authentication** page, and click **Add** under **External CA** section to upload the device certificate you have received from external CA to Sangfor device, as shown below:



9. Click on the **External CA** in **Name** column to enter the **External CA** page and configure **CA Options**, as shown in the figure below:



10. Users can log in to SSL VPN with the certificated issued by this external CA.

Mapping User to Local Group Based on External Certificate

Background:

Take Microsoft CA for example. As we know, for user accounts stored on LDAP server, the users under different OUs have varied privileges.

Now, the prerequisite is that each user owns a certificate issued by a third party CA already. We are to have these users (under different OUs) automatically granted with different levels of privilege to access the SSL VPN, hoping that they can pass the certificate based authentication with the certificate issued by the third-party CA when they connect to SSL VPN.

Suppose LDAP user **test1** is under **ou1**, and user **test1** is under **ou2**.

Purposes:

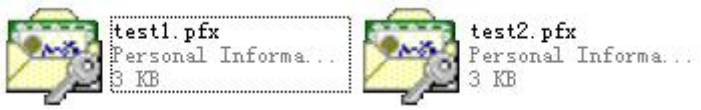
To assign different resources to the two users automatically after they log in to the SSL VPN successfully, but the two users need not be imported into the Sangfor device.

Analysis and solution:

Firstly, we need to configure external CA and use the CA to generate certificate, so that users can use third-party certificate to log into the SSL VPN. Secondly, we need to map the certificate users to the user group on Sangfor device, so that they can be granted with the same privilege as the users under the target group.

To achieve the expected purposes:

1. Configure external CA (for detailed guide, please refer to Configuring External CA in Chapter 4).
2. Navigate to **SSL VPN** > **Users** and create two user groups named **ou1** and **ou2** (for detailed guide, please refer to the Adding User Group section in Chapter 4). Primary authentication **Certificate/USB key** need not be selected for both users **ou1** and **ou2**.
3. Generate certificates for the two users, **test1** and **test2**.



   Check the subjects of the two certificates, as shown below.

   DN of test1: CN=test1, OU=ou1, DC=zy, DC=sangfor, DC=com

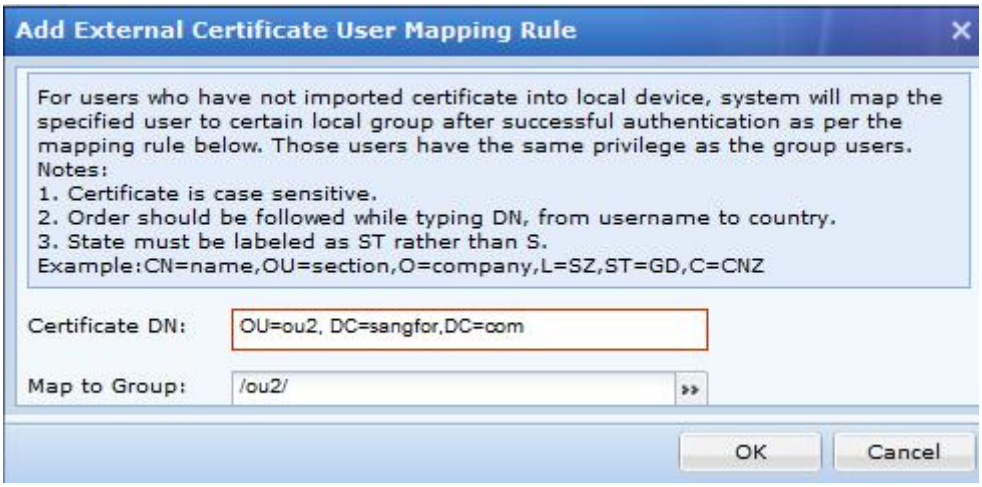
   DN of test2: CN=test2, OU=ou2, DC=zy, DC=sangfor, DC=com

4. Configure CA option. Select **Trust all the users who own certificate issued by current CA** option, as shown in the figure below:



5. Click the link **Configure Mapping Rule** to configure two mapping rules, one rule mapping LDAP **ou1** to the local group **ou1**, and the other mapping LDAP **ou2** to the local group **ou2**, as shown in the figures below:





6. Navigate to **SSL VPN** > **Roles**, create two roles and associate the local groups **ou1** and **ou2** with different resources (for detailed guide, please refer to the Adding Role section in Chapter 4).

7. Save the setting and then click the **Apply** button when configuration is completed.

   After logging in to the SSL VPN, what **test1** and **test2** will see on the **Resource** page will be the corresponding associated resource.

Configuring Resource Enabling SSO

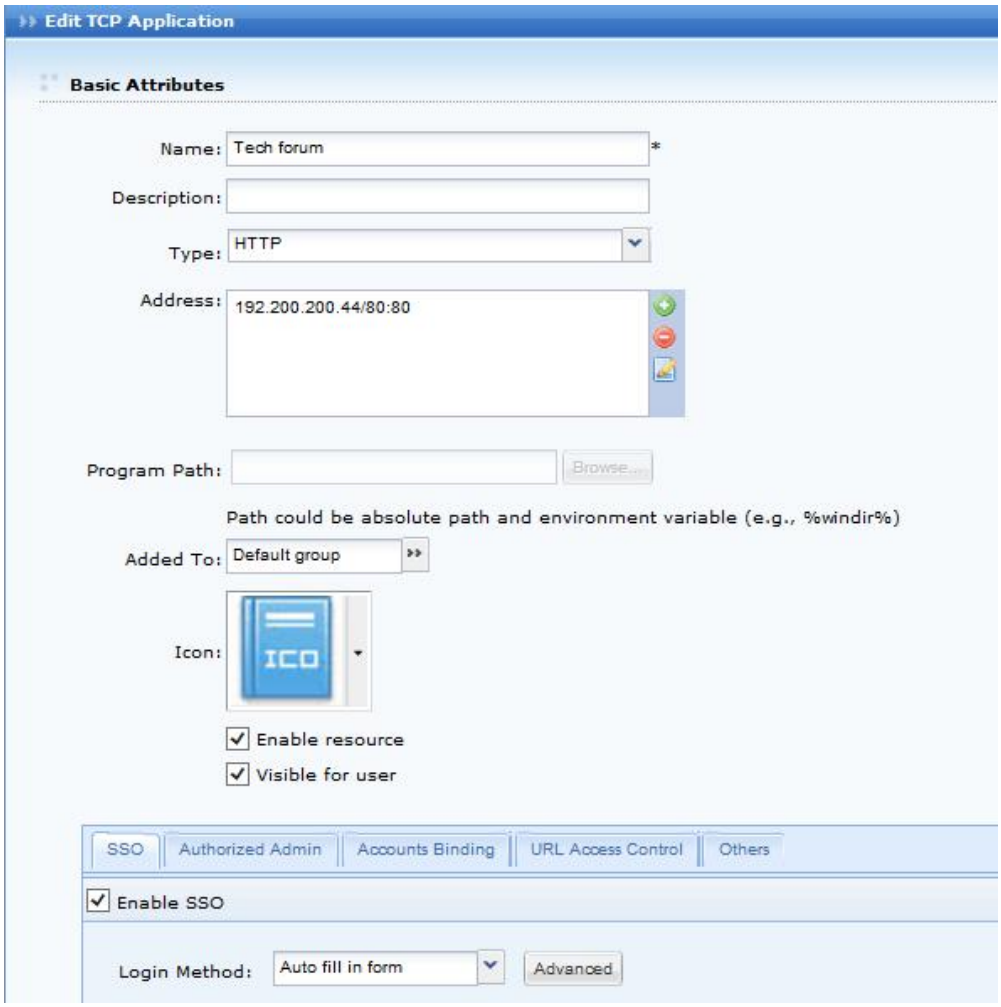
Adding TCP Application Enabling SSO

Purpose:
When end users access tech forum of their company, they do not need to enter username and password again, which will be filled in automatically with their SSL VPN accounts.

Analysis and solution:
Firstly, we need to configure the tech forum as a TCP application. Secondly, enable SSO feature for this resource and choose a login method, which can be **Auto fill in form** or **Set auto-access request**. In this scenario, we take the former as example.

To achieve expected purpose:

1. Navigate to **SSL VPN > Users > Local User**s and click **Add > User** to add a user(for detailed guide, refer to Adding User in Chapter 4)
2. Go to **SSL VPN > Resources** page and click **Add > TCP app** to add a TCP resource, as shown below:



Click on **SSO** tab and select the **Enable SSO** to enable SSO feature, and choose auto fill in form as **Login Method.**

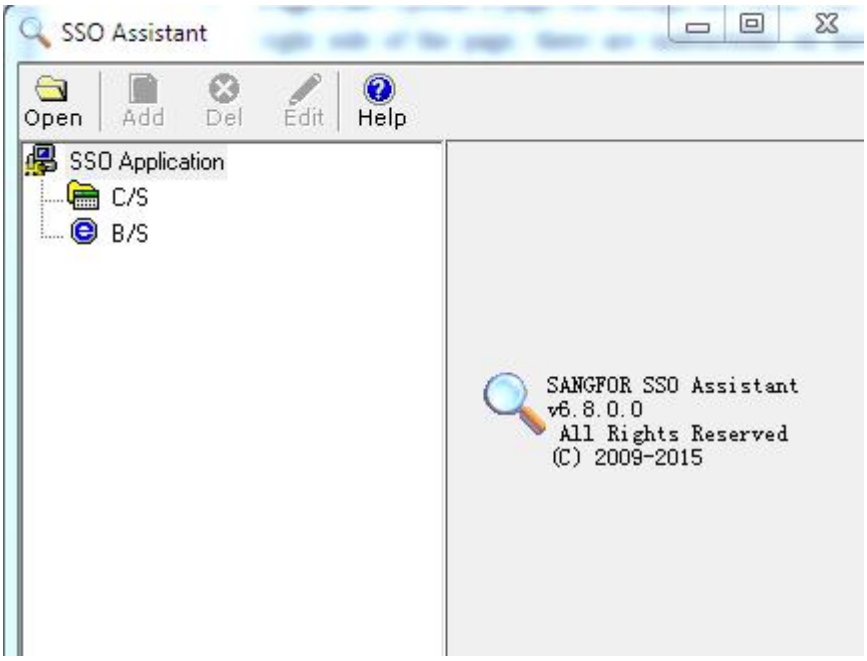
3. Go to **System > SSL VPN Options > General > SSO** page to download SSO assistant and config file, as shown in the figure below:



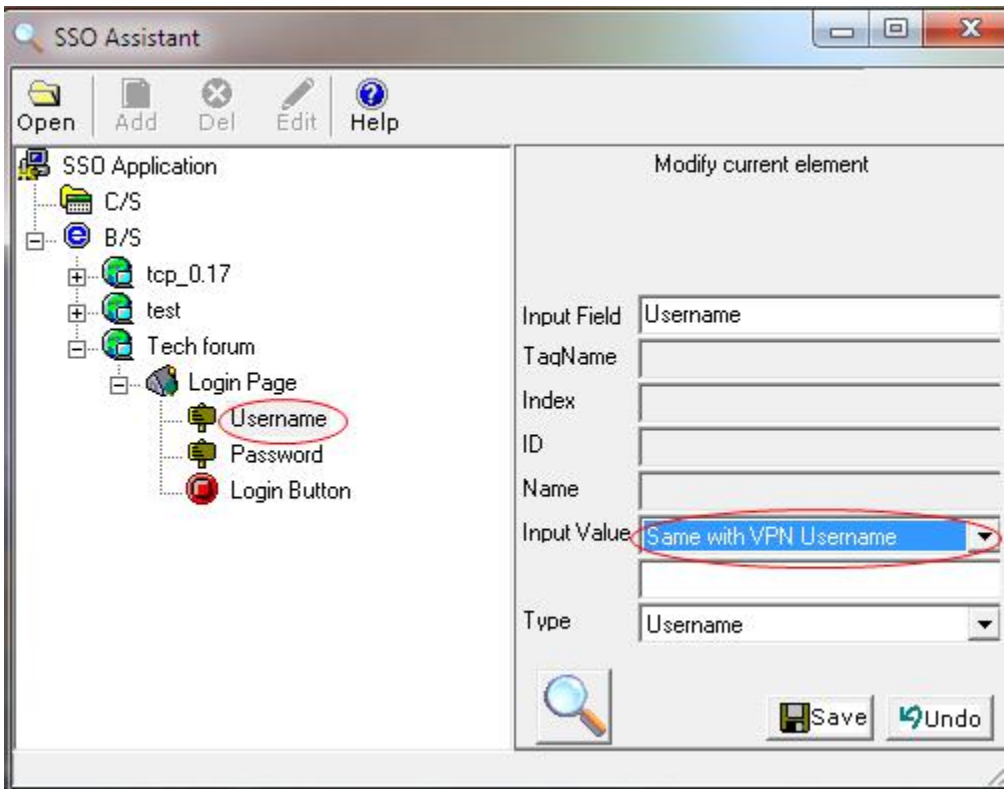
4. Install the SSO assistant. After installation completes, a corresponding shortcut will be created for the SSO assistant, as shown below:



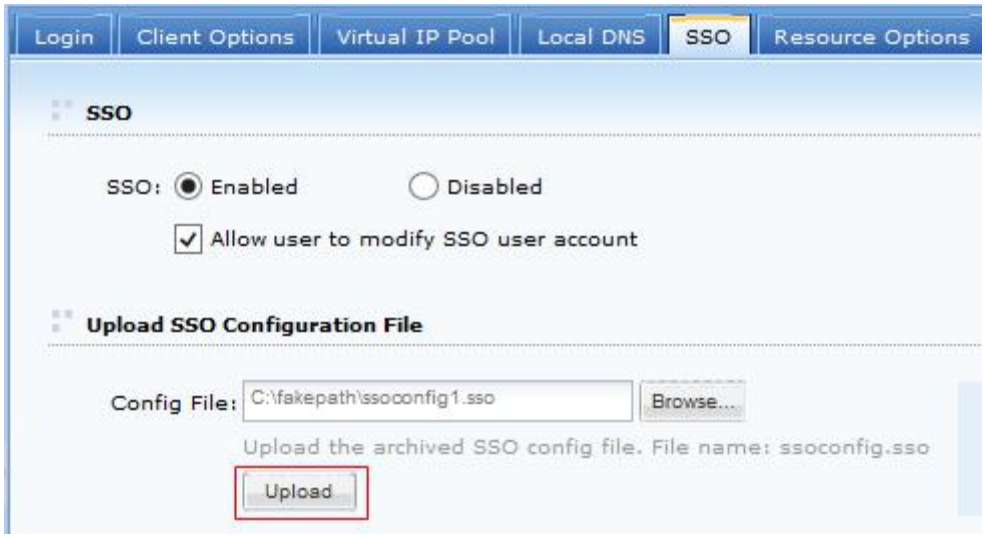
5. Double-click on the shortcut to launch SSO assistant, as shown below:



Click **Open** to import SSO config file downloaded in step 3and record SSO information with SSO Assistant. Click on the **Username** under the desired resource and right-click it to click **Edit**, then drag the magnifier on current page to **Username** textbox on the login page of this tech forum and select **Same as VPN Username** in **Input Value** field. Click **Save** to save the changes. The method to record password and login button is similar with that of recording username.



6. After recording SSO information completes, upload the SSO config file to Sangfor device. Go to **System > SSL VPN Options > General > SSO** page and click **Browse** under **Upload SSO Config File** section to select desired SSO config file, and then click **Upload** to upload it to the device, as shown below:



7. Navigate to **SSL VPN > Roles > Role Management** to add a role and associate it with the user created in step1 and the resource created in step2(for detailed guide, refer to Adding Role in Chapter 4).

8. After user logs in to SSL VPN, he/she can click the resource link to access the tech forum directly without entering username and password.

Adding Remote Application Enabling SSO

Background:

RXT,a instant messaging tool, is published over SSL VPN. Employee's account for logging in to RTX is not the same as that for logging in to SSL VPN. The username of RTX account is the abbreviation of employee's name, and the password is their work number.

Purpose:

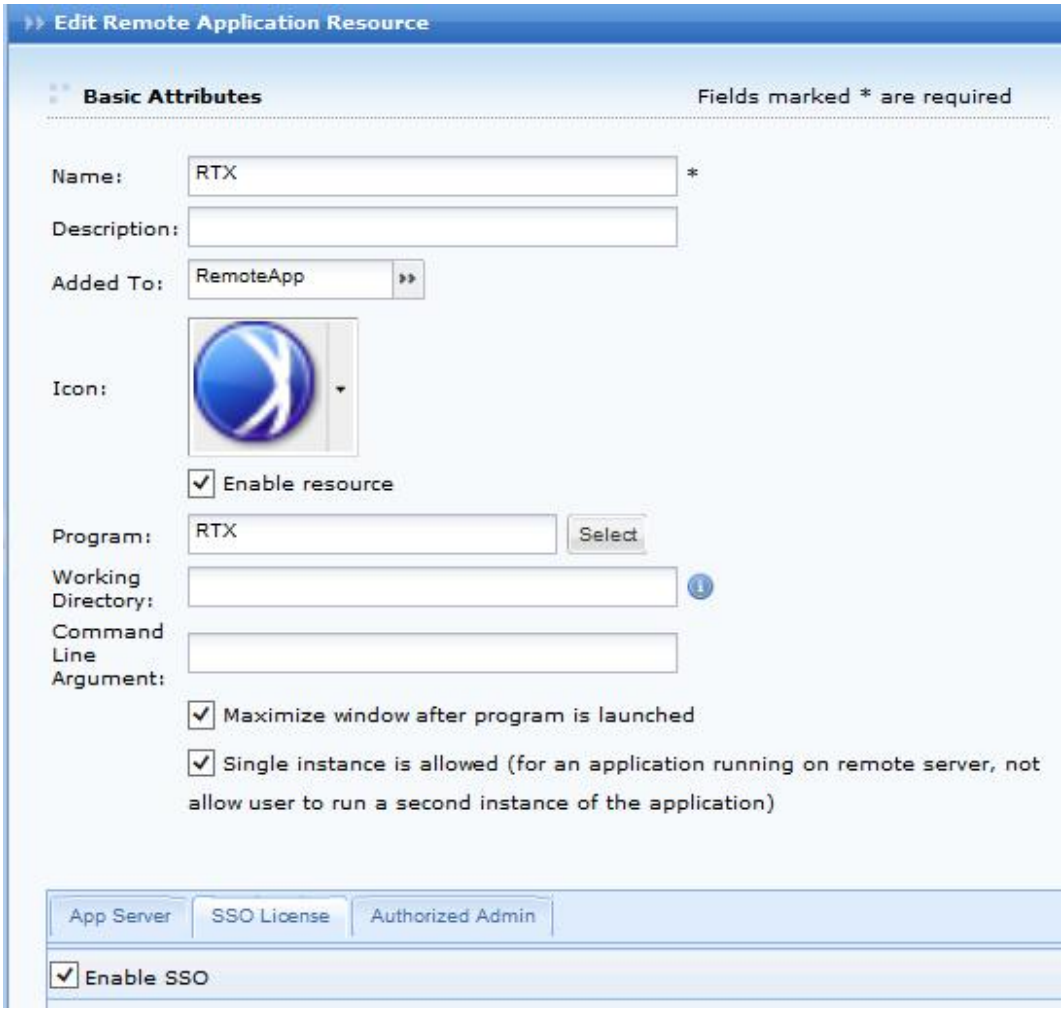
Enable employees to access RXT directly without need to provide RTX account after they log into SSL VPN.

Analysis and Solution:

As employee's account for logging in to RTX is different from the account for logging in to SSL VPN, **Allow user to modify SSO user account** option should be selected when configuring SSO.

To achieve expected purpose:

1. Configure a remote server(for details, refer to Adding Remote Application in this Chapter)
2. Navigate to **SSL VPN > Users > Local Users** and click **Add > User** to add a user(named **ssl1**, password is 123). For detailed guide, refer to Adding User in Chapter 4.
3. Go to **SSL VPN > Resources** page and click **Add > Remote app** to add a remote application named RTX, as shown below:



Click on **SSO License** tab to select the **Enable SSO** option.

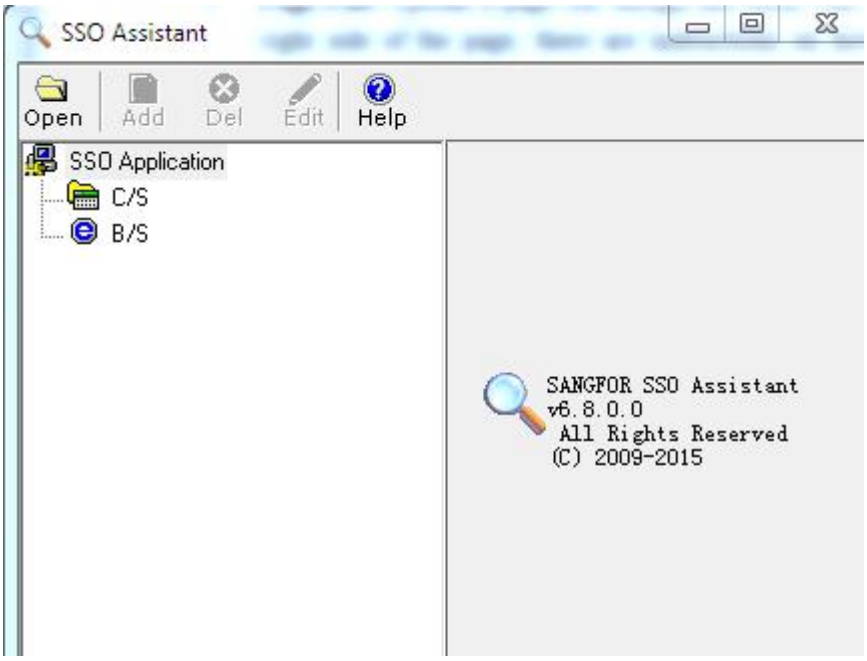
4. Go to **System > SSL VPN Options > General > SSO** page, select the **Allow user to modify SSO user account** option, and download SSO assistant and config file, as shown in the figure below:



5. Install the SSO assistant. After installation completes, a corresponding shortcut will be created for the SSO assistant, as shown below:



6. Double-click on the shortcut to launch SSO assistant, as shown below:

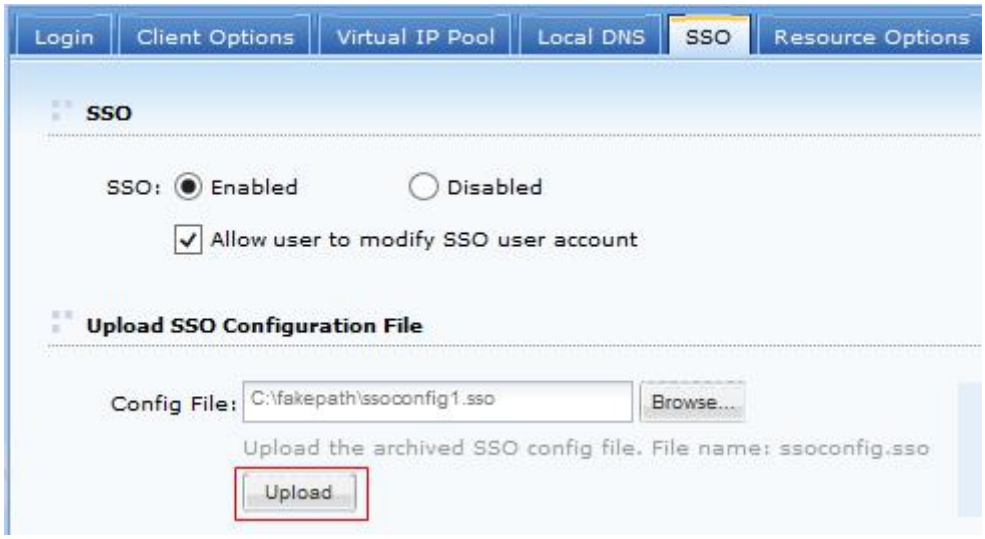


Click **Open** to import SSO config file and record SSO information with SSO Assistant.

Click on the **Username** under the desired resource and right-click it to select **Edit**, then drag the magnifier on current page to **Username** textbox on RTX login page and select **Same as VPN Username** in **Input Value** field.

Click **Save** to save the changes.

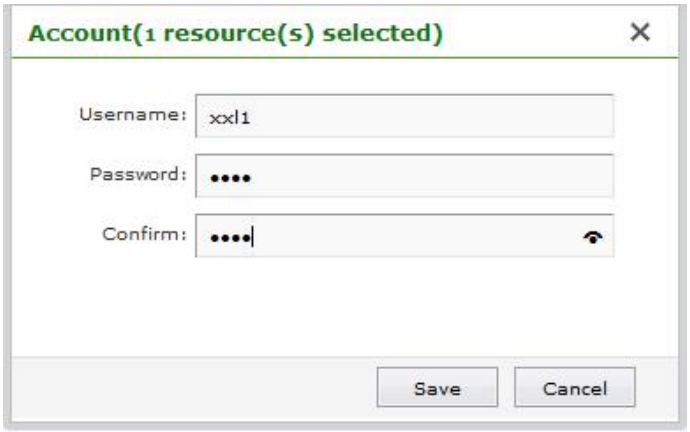
7. After recording SSO information completes, upload the SSO config file to Sangfor device. Go to **System > SSL VPN Options > General > SSO** page and click **Browse** under **Upload SSO Config File** section to select desired SSO config file, and then click **Upload** to upload it to the device, as shown below:

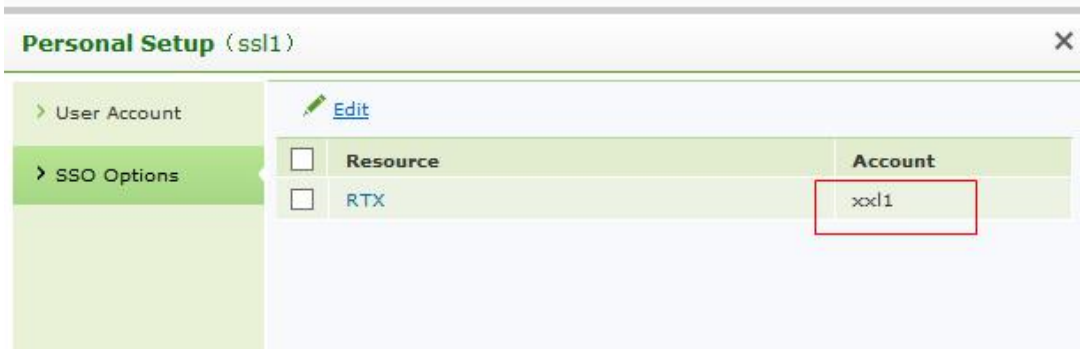


8. Navigate to **SSL VPN > Roles > Role Management** to add a role and associate it with the user **ssl1** created in step2 and the resource **RXT** created in step3(for detailed guide, refer to Adding Role in Chapter 4).

9. After user **ssl1** logs in to SSL VPN, click **Settings** on the upper right of the page to modify the RTX account(for example, modify username to your real name xxl1, password to your work number).







10. Back to **Resource** page and click on the resource link, then user can log in RTX automatically.

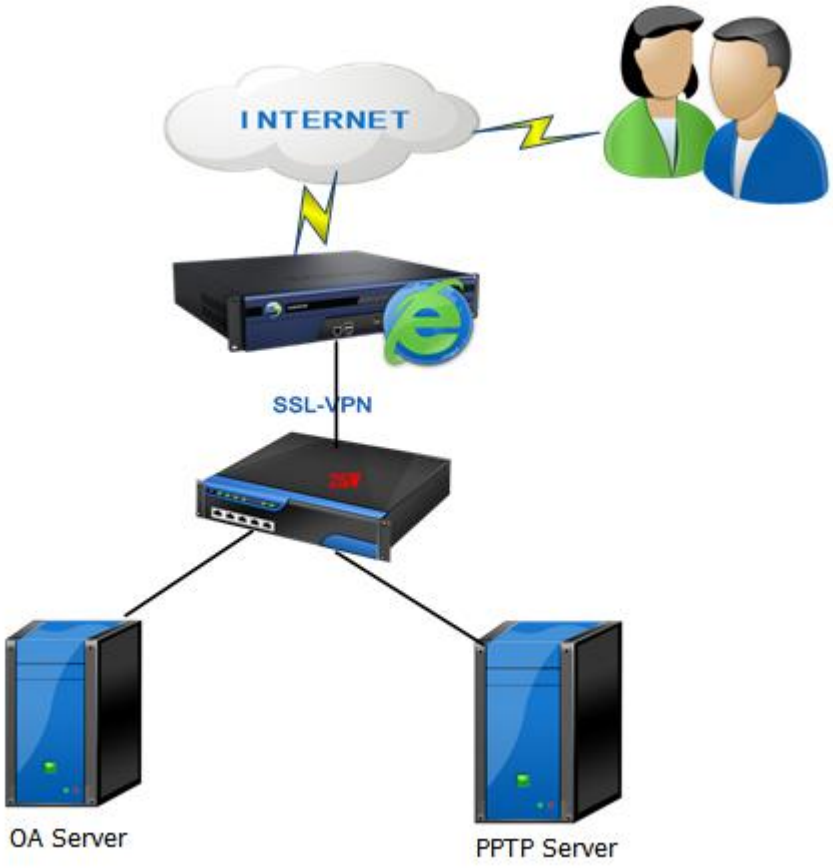


- SSO feature has two login methods: **Auto fill in form** and **Set auto-access request**. The SSO feature with **Auto fill in form** as login method applies to web app, TCP app, all B/S-based and C/S-based L3VPN app, while SSO feature with **Set auto-access request** as login method supports web app, TCP app, HTTP-based and HTTPS-based L3VPN app.
- Remote application only supports the SSO feature with **Auto fill in form** as login method

Configuration Case of Accessing SSL VPN through PPTP

One customer wants to access internal network through SSL VPN by using browser of their own iPhone, iPad or Android mobile phones, that is, realize mobile office by using mobile phones.

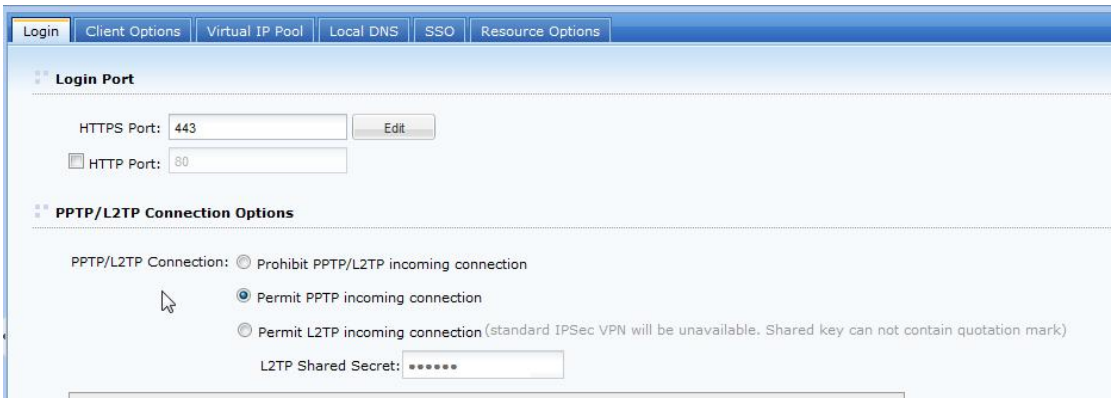
Since internal BBS system of the customer is written by JSP, systems are rather complex, a lot of scripts and controls are used, therefore WEB application is not applicable, L3VPN is a better choice.



Configurations are as follows:

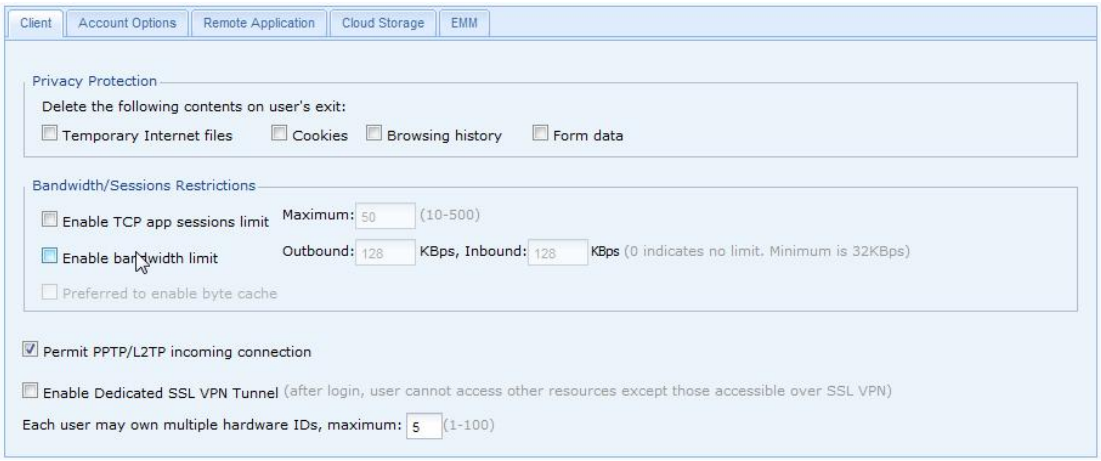
Configurations of SSL

Step 1: Navigate to **System** > **SSL VPN Options** > **General** > **Login**, select **Permit PPTP incoming connection**, as shown below:

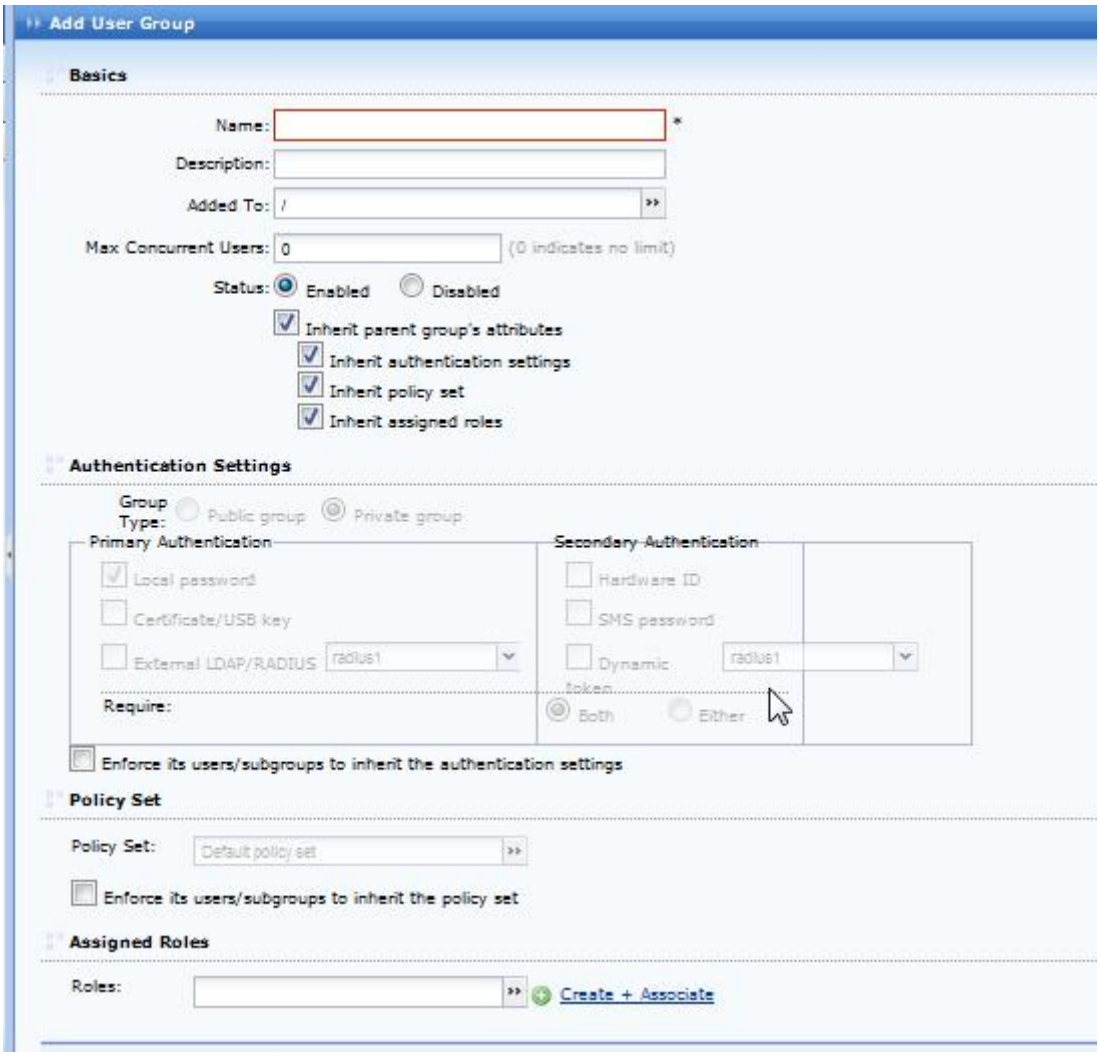


Step 2: Navigate to **SSL VPN** > **Policy Sets**, click **Add** to add policy set and to enter the **Add**

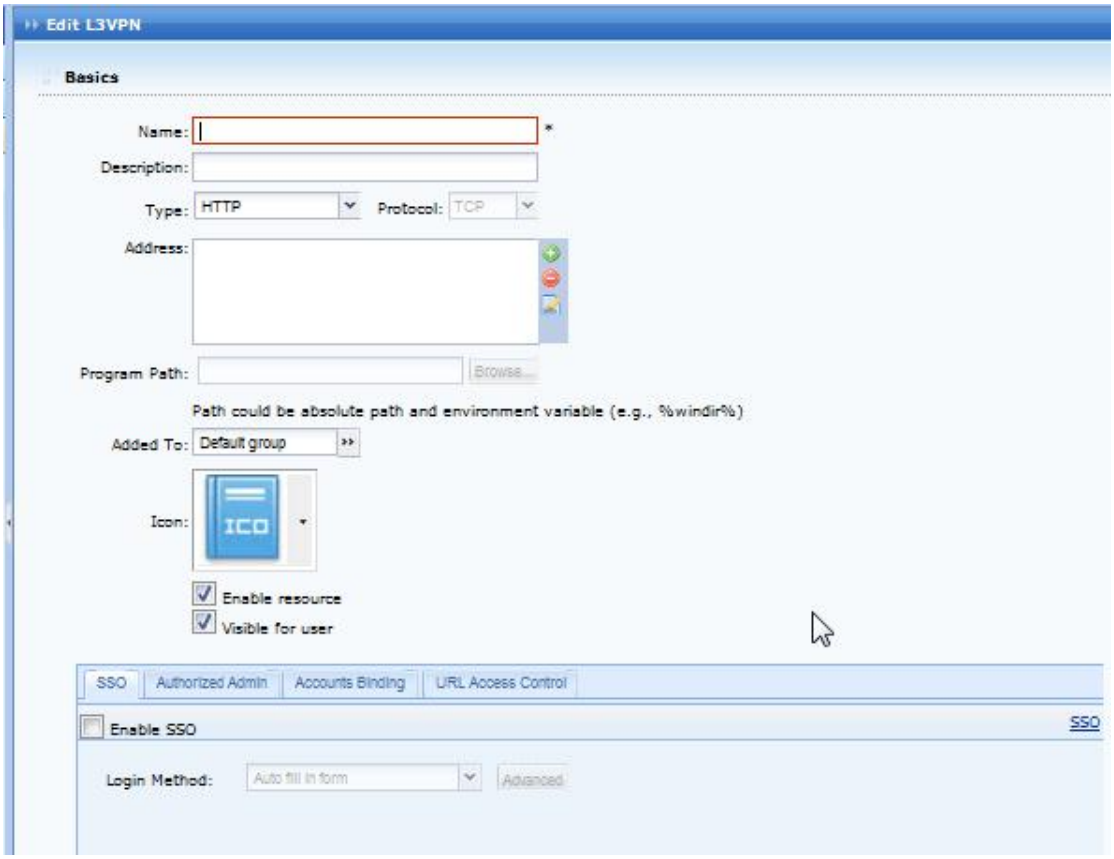
Policy Set page. Select **Permit PPTP/L2TP incoming connection**, as shown below:



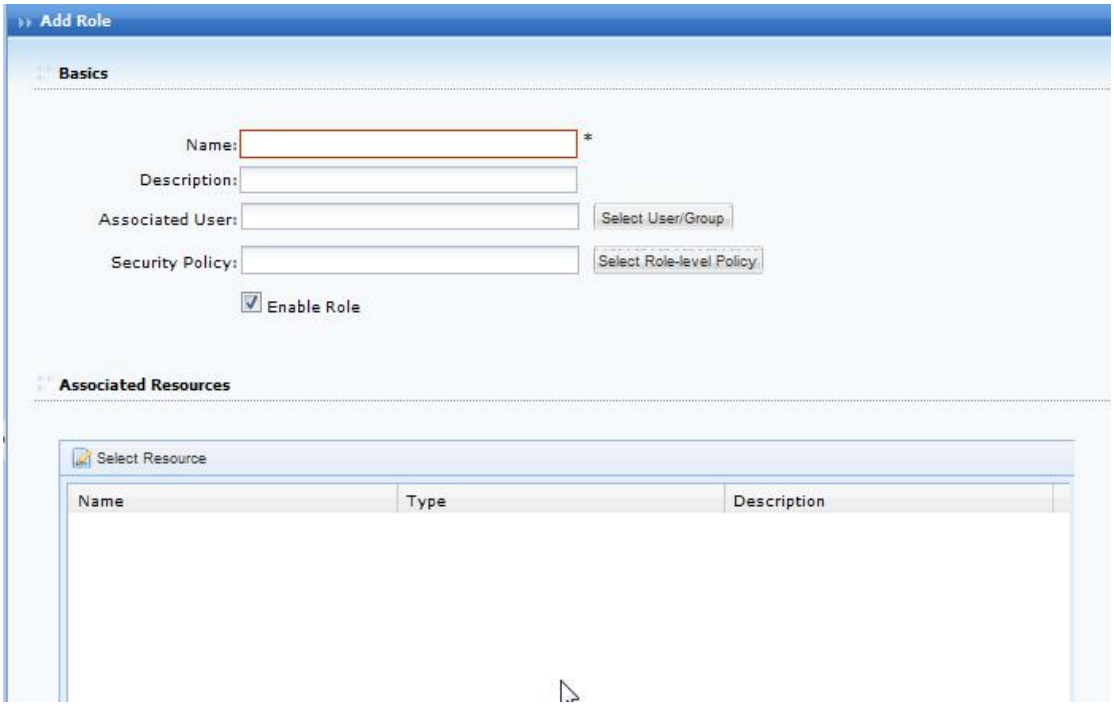
Step 3: Navigate to **SSL VPN** > **Users**, Click **Add** > **Group** to enter the **Add User Group** Page. Associate policy sets in **Attribute** of use/user group which get connected through PPTP.



Step 4: Navigate to **SSL VPN** > **Resources**, click **Add** > **L3VPN** to enter the **Edit L3VPN** page. Add resources to be accessed by using PPTP.



Step 5: Navigate to **SSL VPN** > **Roles**. On the **Role Management** page, click **Add** > **Role** to enter the **Add Role** page, and associate user/user group and resources.



PPTP Client Access Configuration:

Here is an example of one user who uses iphone to configure PPTP access resources:

Log in to SSL VPN through browser of the iphone, as shown below:



Note: Resources marked with is L3VPN and should be accessed by using PPTP.

1. Click Access **SSLVPN Through PPTP**. Access tips pop up. Install description file to mobile phone.



2. Set PPTP VPN login. Go back to iphone homepage, and go to **Settings** as follows:



3. VPN switch turns green after connection. A small icon **VPN** shows on the upper left. Then you can access internal network applications through browser or application program.

4. When you want to exit PPTP VPN, switch off **VPN** option. Next time you can directly get connected to PPTP VPN to access resources.



5. Remember PPTP login password. Go to **General** > **Network** > **VPN** and click the blue arrow, as shown below:



Enter password in **Password** and click **Save**. You do not have to enter password again for later connections.

PPTP configuration is completed. You can use your mobile phone to access BBS.



When SSL device is deployed in single-arm mode, the following is required: (1) TCP 80 and Port 443 connected by SSL users should be mapped, TCP 1723 port should also be mapped. (2) PPTP data package can penetrate front-end device, and also protocol 47 can penetrate front-end device.



Applications accessed through PPTP should be added as L3VPN resources. If the application can be accessed through WEB, then the application can directly get connected to SSL VPN without building PPTP connections.



Telecom operators in some districts (For example, Beijing Unicom) will block PPTP of 3G network. If, after deployment, you can get accessed through wifi , but not through 3G, it is probable that operators have blocked.



When PPTP fails to get connected, make sure whether devices from local network to SSL support PPTP penetration. For example, TP-link supports 32 PPTP penetrations, D-Link does not support PPTP penetration, and Tenda supports PPTP penetration.

Configuration Case of Accessing SSL VPN through L2TP

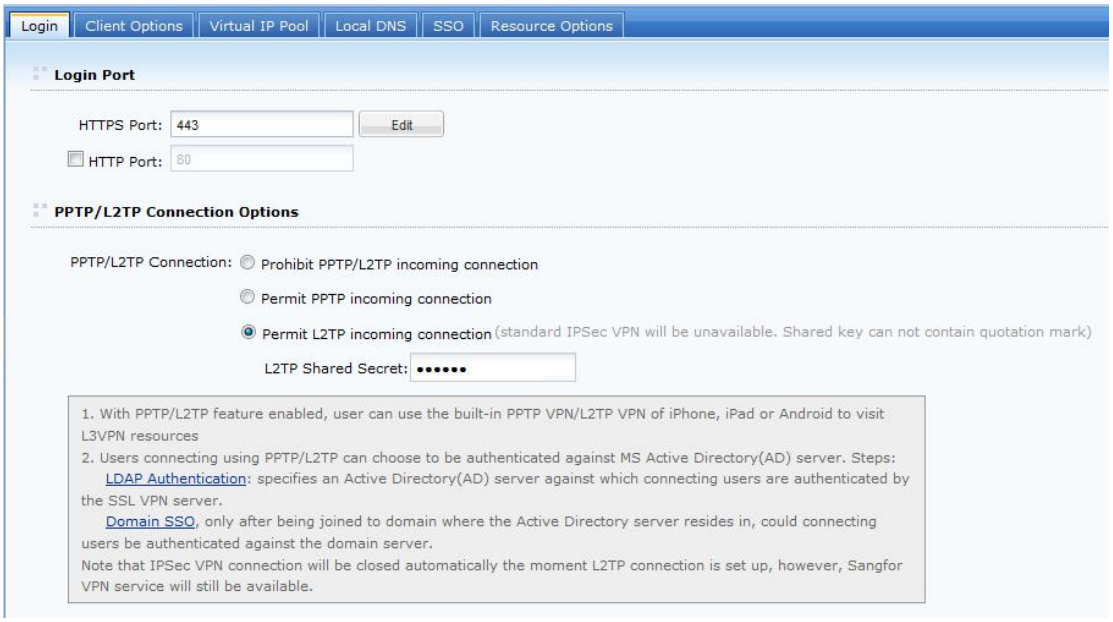
Internal network in headquarter has DNS. One customer wants to access SSL through L2TP on mobile endpoints, access internal network with domain account, and realize mobile office on mobile endpoints.



Configurations are as follows:

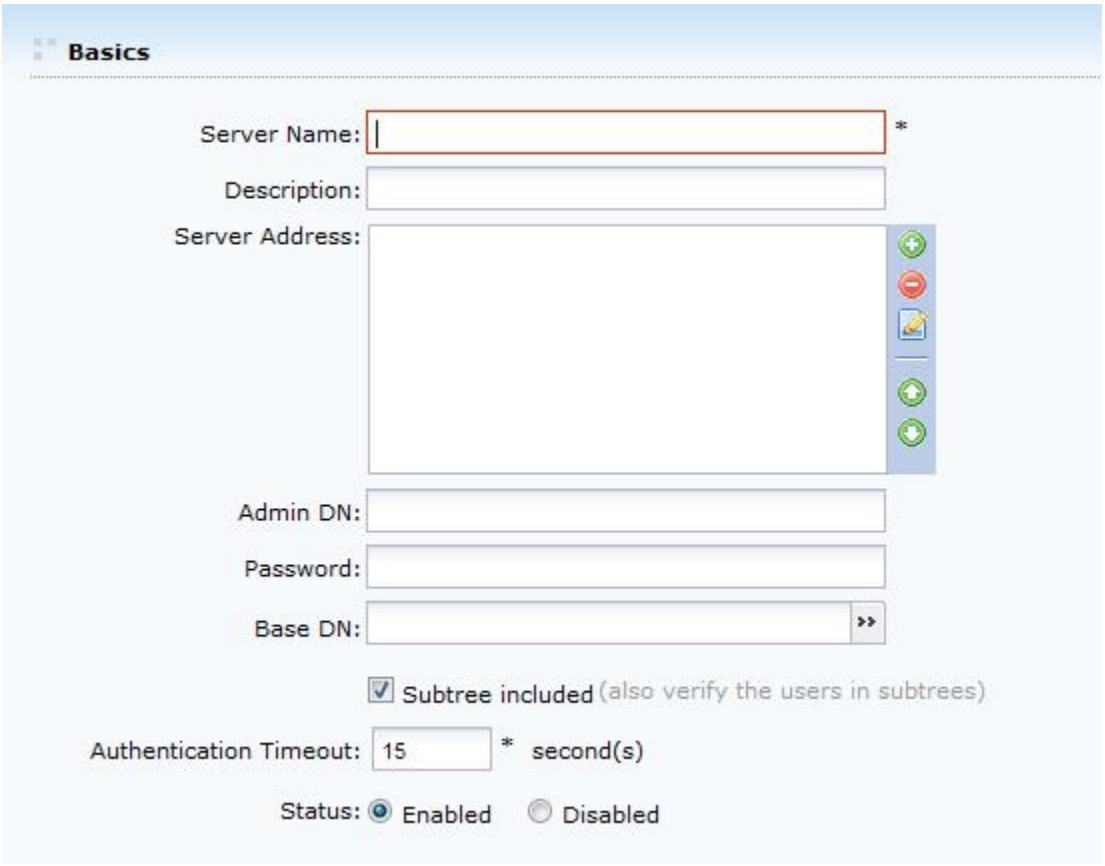
Configuration of SSL:

Step 1: Navigate to **System** > **SSL VPN Options** > **General** > **Login**, select **Permit L2TP incoming connection** and set **L2TP Shared Secret**, as shown below:

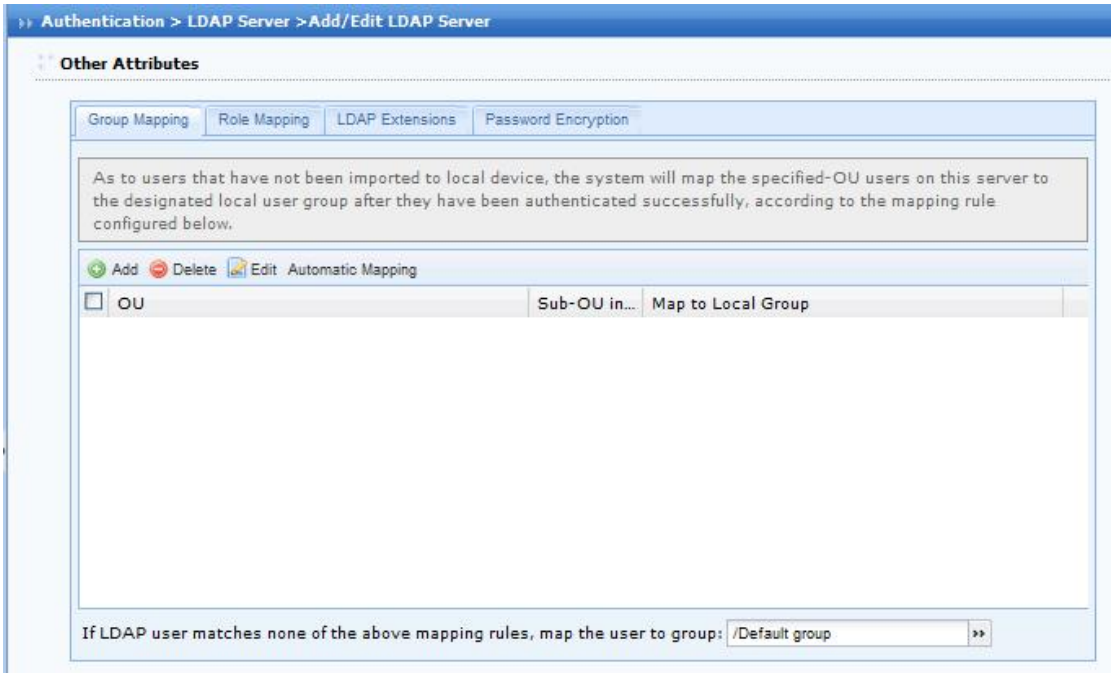


Step 2: Navigate to **SSL VPN** > **Authentication**. Click **Settings** after **LDAP**. On **LDAP Server**

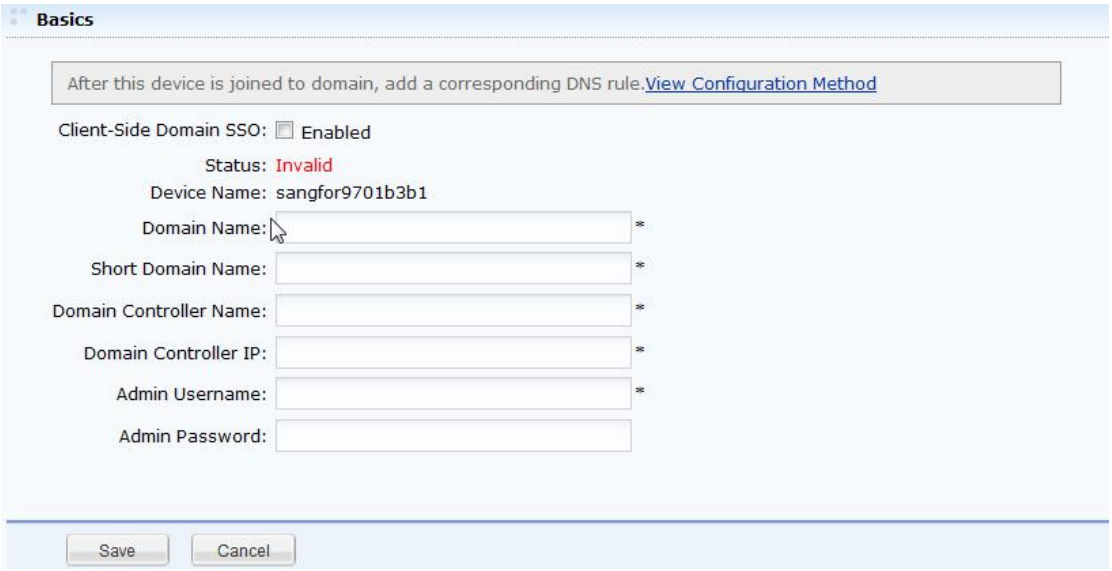
page click **Add** to add LDAP server, as shown below:



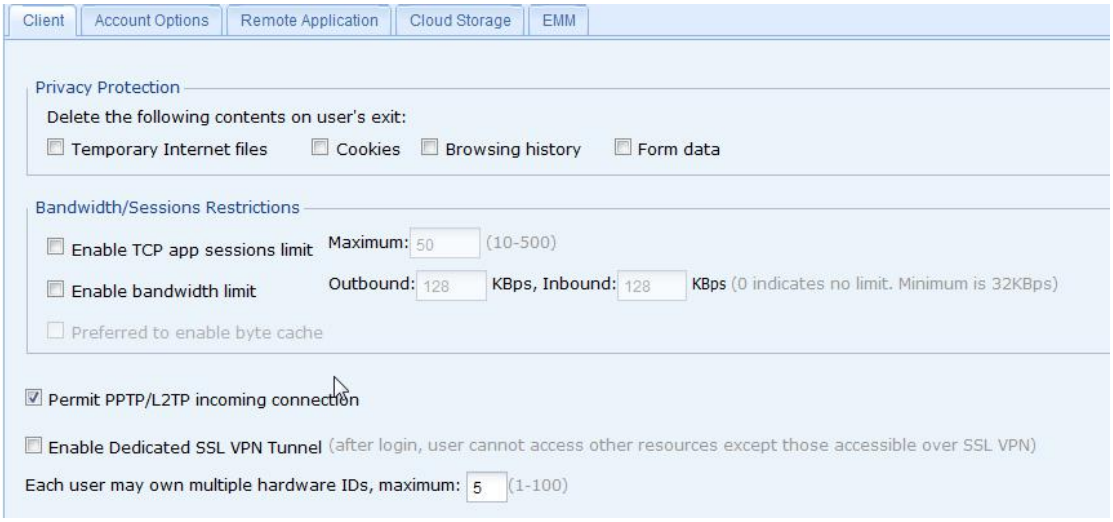
Other Attributes > **Group Mapping**. Add group mapping as below:



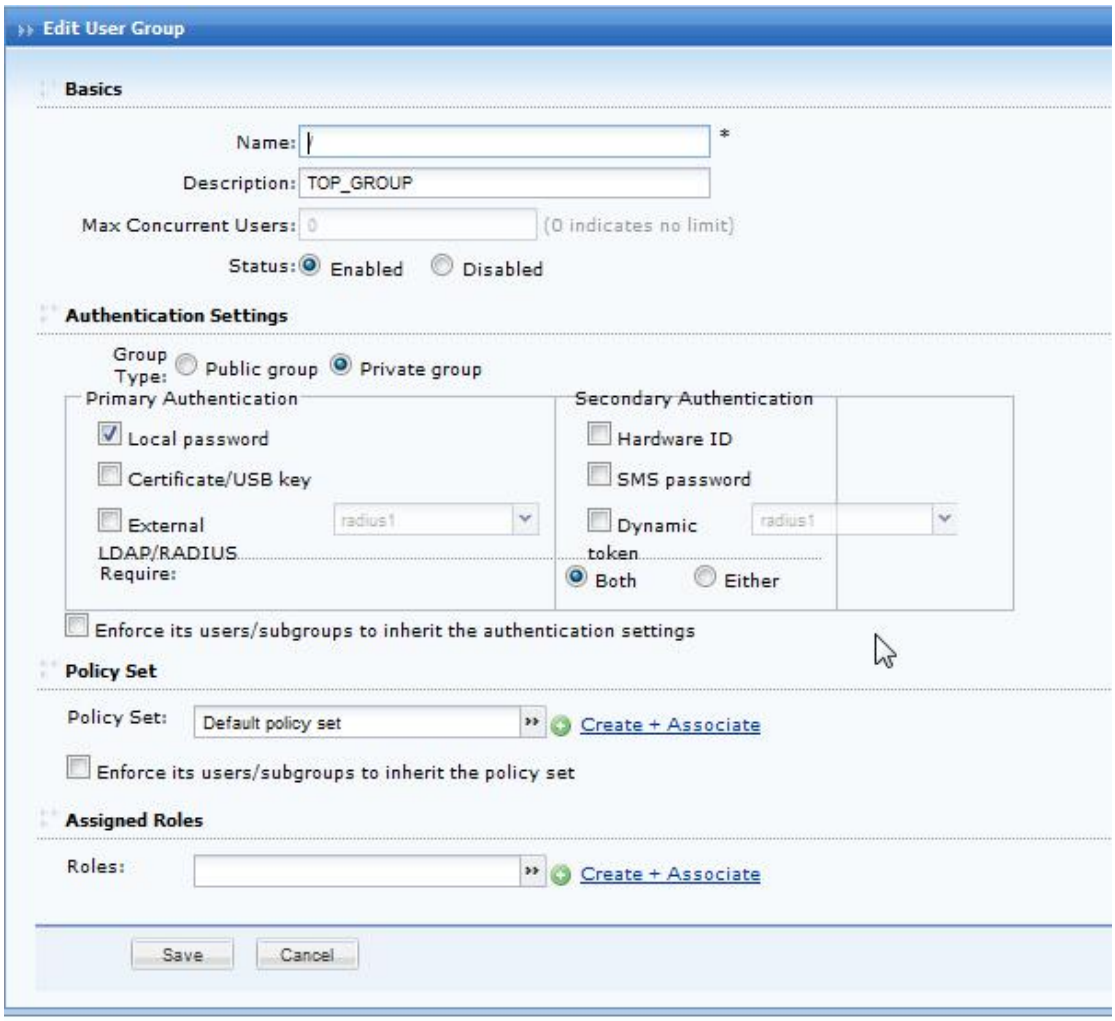
Step 3: Navigate to **SSL VPN** > **Authentication**, click **Settings** after **Client-Side Domain SSO**, and add SSL device to AD domain. Configuration page is shown as below:



Step 4: Navigate to **SSL VPN** > **Policy Sets**. On the **Policy Set Management** page, click **Add** > **Policy set** to enter the **Add Policy Set** page, and select **Permit PPTP/L2TP incoming connection**, as shown below:



Step 5: Navigate to **SSL VPN** > **Users** to enter the **Local Users** page. Associate policy sets in **Attribute** of use/user group which get connected through L2TP.



Step 6: Navigate to **SSL VPN** > **Resources** and click **Add** > **L3VPN** to add resources accessed by using L2TP.

Step 7: Navigate to **SSL VPN** > **Roles** and click **Add** > **Roles** to associate user/user group and resources.

L2TP Client Access Configuration

Here is an example of one user who uses iphone to configure L2TP access resources:

Go to **Settings** > **General** > **VPN**, click **Add VPN Configuration**, as shown below:



Description: Enter name of VPN connection.

Server: Enter public network address of SSL.

Account: Enter username to access SSL. If it is AD domain authentication, then enter domain username.

Password: Enter password to access SSL.

Secret: The same as L2TP shared secret of SSL.

When SSL device is deployed in single-arm mode, the following is required: (1) TCP 80 and Port 443 connected by SSL users should be mapped, UDP 500, UDP 4500 and UDP1701 should also be mapped. (2) L2TP data package can penetrate front-end device.

Applications accessed through L2TP should be added as L3VPN resources. If the application can be accessed through WEB, then the application can directly get connected to SSL VPN without building PPTP connection.



Telecom operators in some districts (For example, Beijing Unicom) will block L2TP of 3G network. If, after deployment, you can get accessed through wifi , but not through 3G, it is probable that operators have blocked.



L2TP connection service is enabled, standard IPSec VPN service of SSL cannot be used, but SANGFOR VPN still works.

Mobile Users Accessing SSL VPN

Remote desktop and remote application are accessible over SSL VPN on mobile device, such as iPhone, iPad and Android devices. Taking Android mobile device as example, this section introduces how to use EasyConnect to login and access remote resources.

1. Download EasyConnect from Google Store and install it. Launch it, and you will see the figure as shown in Figure 1 .
2. Enter URL to the Sangfor device and click **Connect** button. Then you need to be authenticated before logging in to VPN, as shown in Figure 2. You can click on **Account** tab to provide username and password, or click on **Certificate** tab to use certificate to log in to SSL VPN.
3. After logging in to SSL VPN, if user is associated with L3VPN resource, a prompt dialog appears, as shown in Figure 3. Check **I trust this application** option and VPN connection will be established. To view connection status, click the EasyConnet logo shown at system status toolbar, as shown in Figure 4.

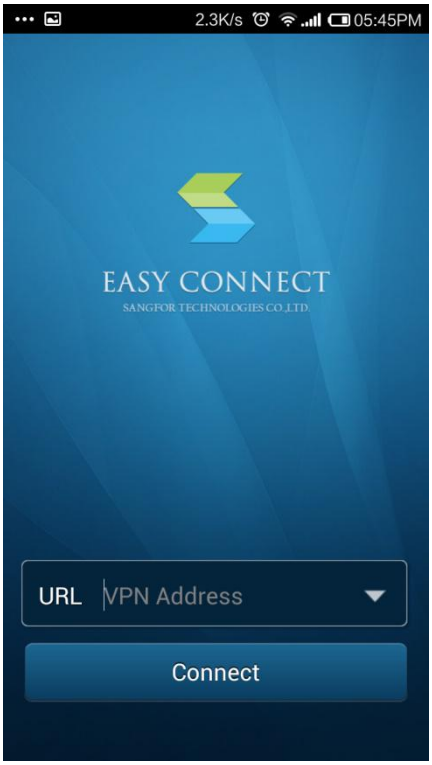


Figure1

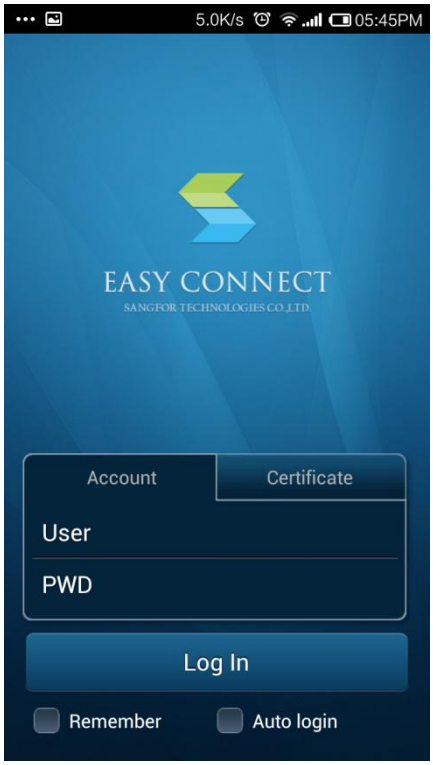


Figure2

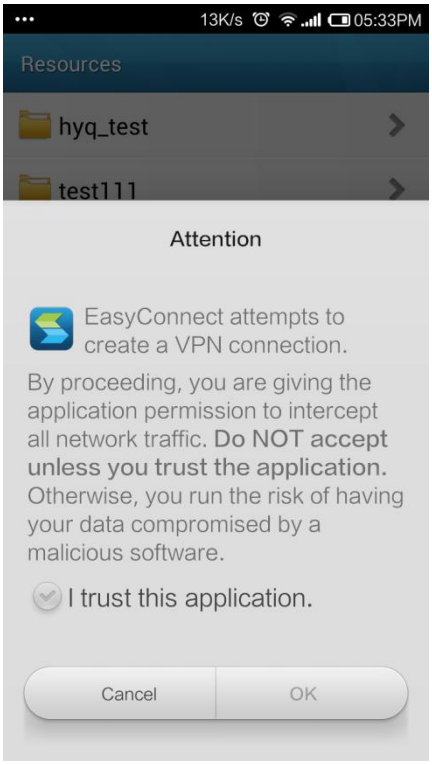


Figure 3

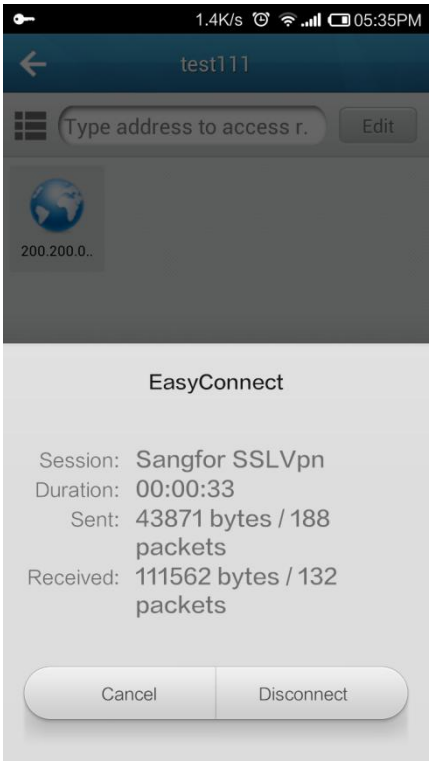


Figure 4

After VPN connection is set up, user can access L3VPN resource using other programs. If he/she does not set up VPN connection, L3VPN resource cannot be accessed, while Web app, TCP pp and remote app are accessible.

Authorized resources will be shown on the right pane of the **Resource** page. Click on the icon to change the method to display the resources, as shown in Figure 5, Figure6.

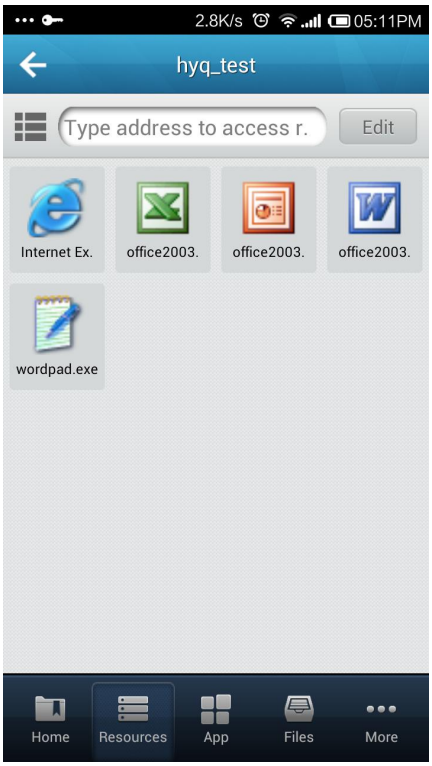


Figure 5 Icon Mode

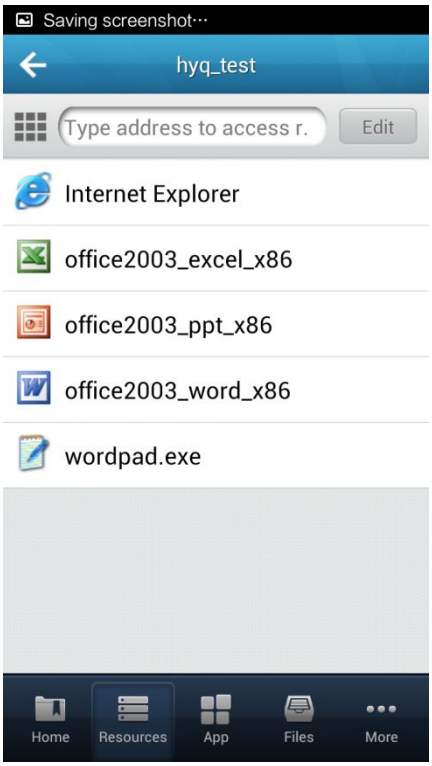


Figure 6 List Mode

To add the desired resource into **Favorites**, click **Edit** to enter the following page, as shown in Figure 7. Click on the golden star icon next to that resource and click **Finish** to exit editing page. Then the corresponding resource will be added into **Favorites** list, as shown in Figure 8.

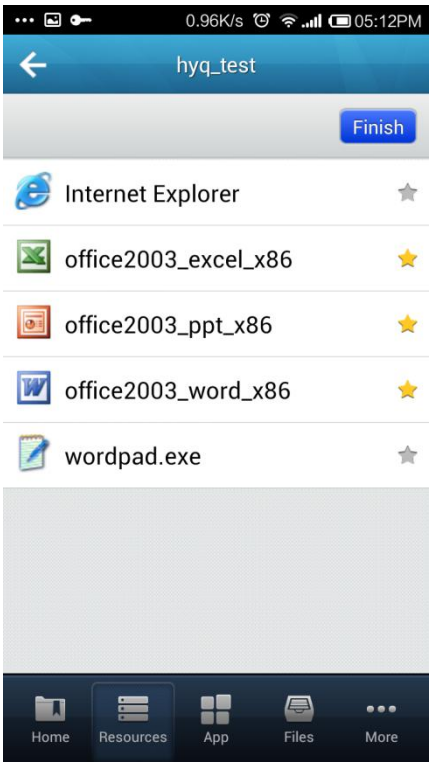


Figure 7

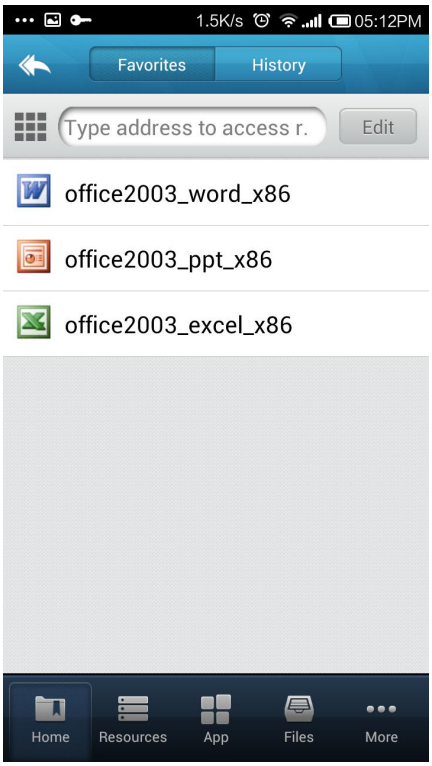


Figure 8

To view accessible personal cloud, public cloud and local storage of mobile device, click **Files** to enter the **Files** page, as shown in Figure 9.

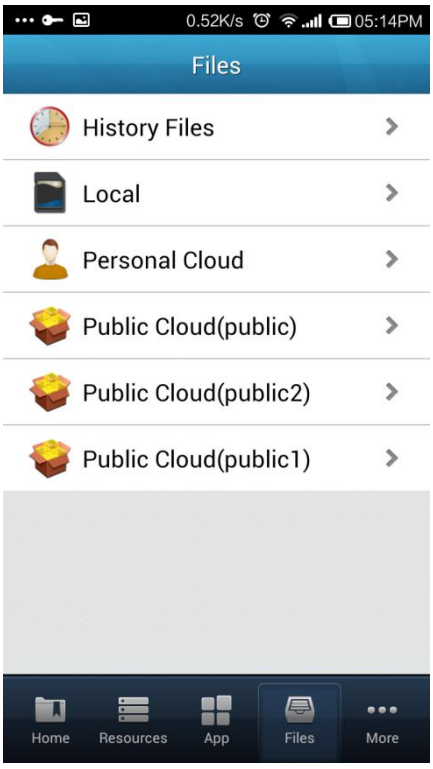


Figure 9

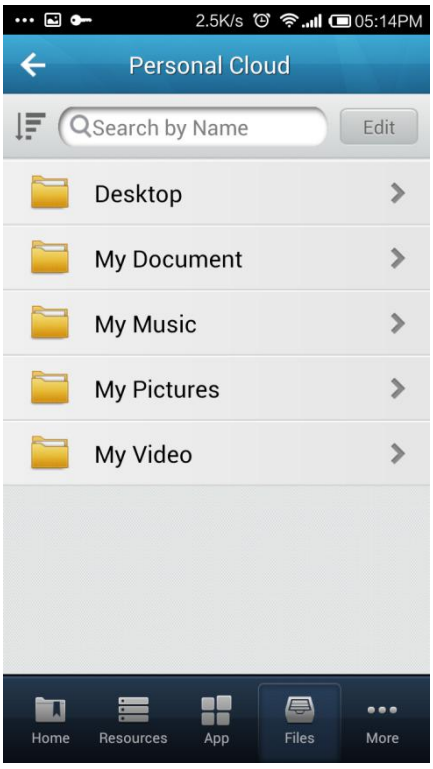


Figure 10

To operate a desired file, for example, **Personal Cloud**, click the arrow icon next to that file

to enter the **Personal Cloud** page as shown in Figure 10.

To open the selected file remotely, click **Open** to open that file using the application program on remote application server.

To download and open a specified file, click **Down &Open** to download that file onto mobile device and open it with default application program installed on mobile device.

To download the selected file, click **Down** to download it to mobile device and that file will be saved into local directory. You can also see that file by clicking **Local** in Figure 9.

To remove a specific file, click **Delete**.

To operate multiple files simultaneously, click **Edit** on the upper right. You will see the page, as shown in Figure 12.

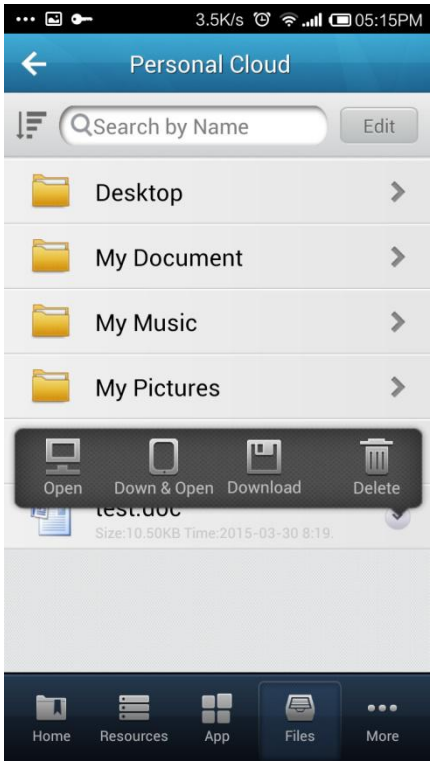


Figure 11

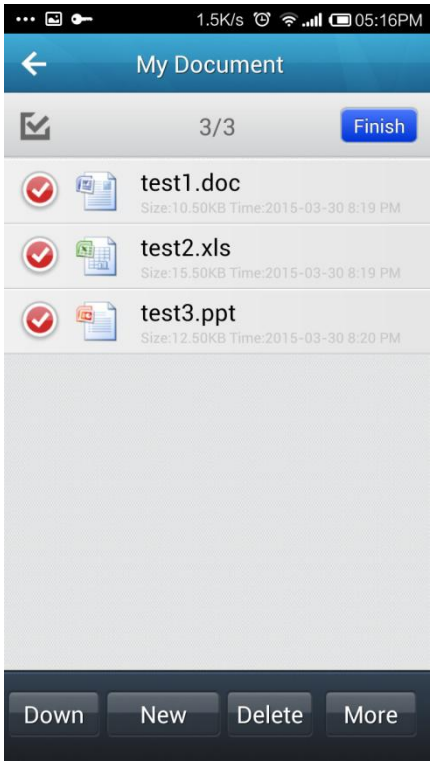


Figure 12

Take the remote application **office2003_Word_x86** shown in Figure 7 as example. Open it and you will see a floating toolbar. Tool icons are listed on the toolbar, namely, cursor, magnifier, keyboard, navigation, program list, menu and a button to hide toolbar.

Private directory and public directory, as well as local storage are available to this remote application. Camera installed on mobile device can be invoked in this remote application. The new photos can be uploaded to remote application. You can choose image quality when uploading image, as shown in Figure 13. You can also share it on EasyConnect through the built-in sharing feature of mobile device. After clicking on **Share**, you need to specify a directory on remote storage server to save the image. Then you can insert that image into the previously-opened Word document.

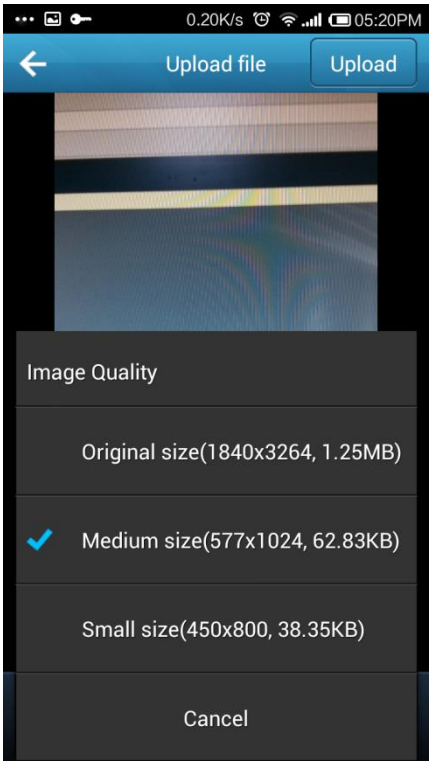

0.20K/s
05:20PM
Upload file
Upload
Image Quality
Original size(1840x3264, 1.25MB)
Medium size(577x1024, 62.83KB)
Small size(450x800, 38.35KB)
Cancel

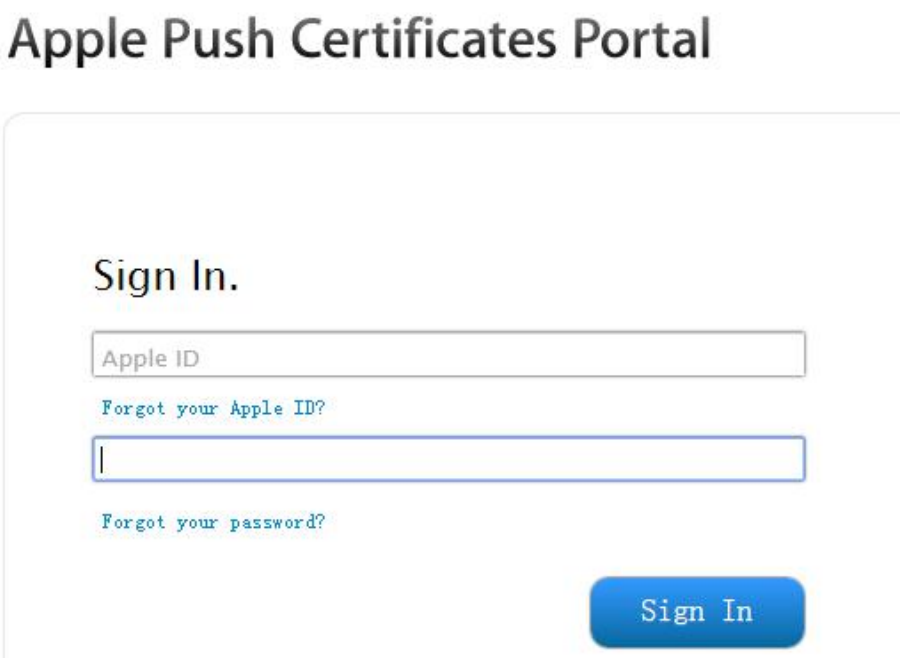
Figure 13

Application for IOS MDM Certificate

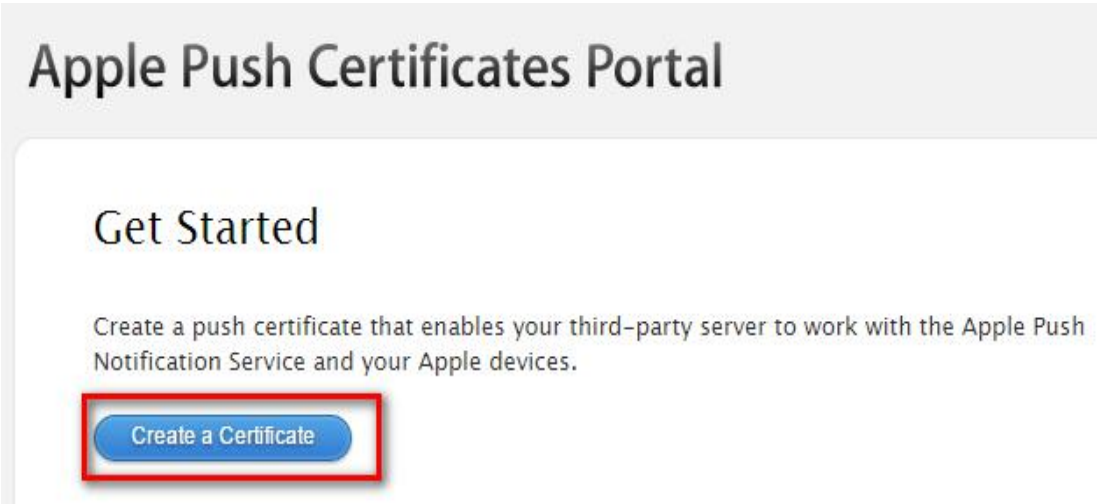
A .pem **file** and a .p12 file should be imported. The .p12 certificate can be provided by Sangfor, but the .pem file should be applied for it.

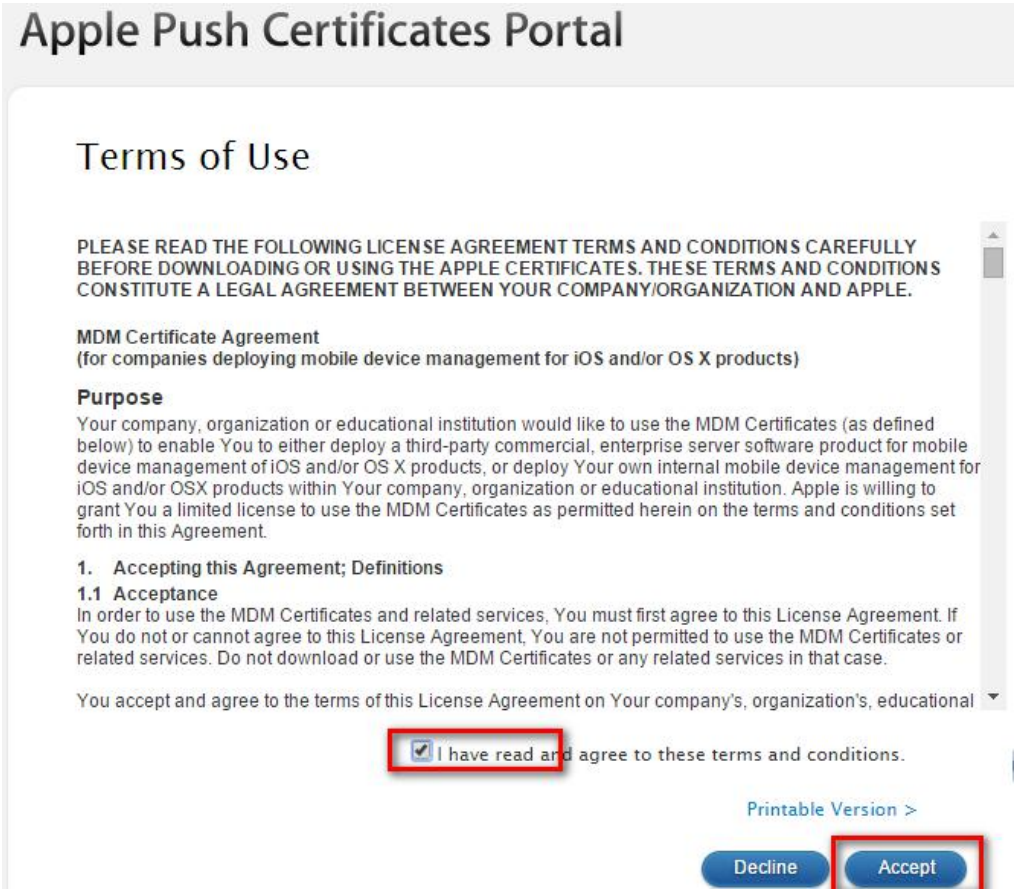
Application for .Pem file:

Step 1: Log in to https://identity.apple.com/pushcert/ with Apple ID, as shown below:

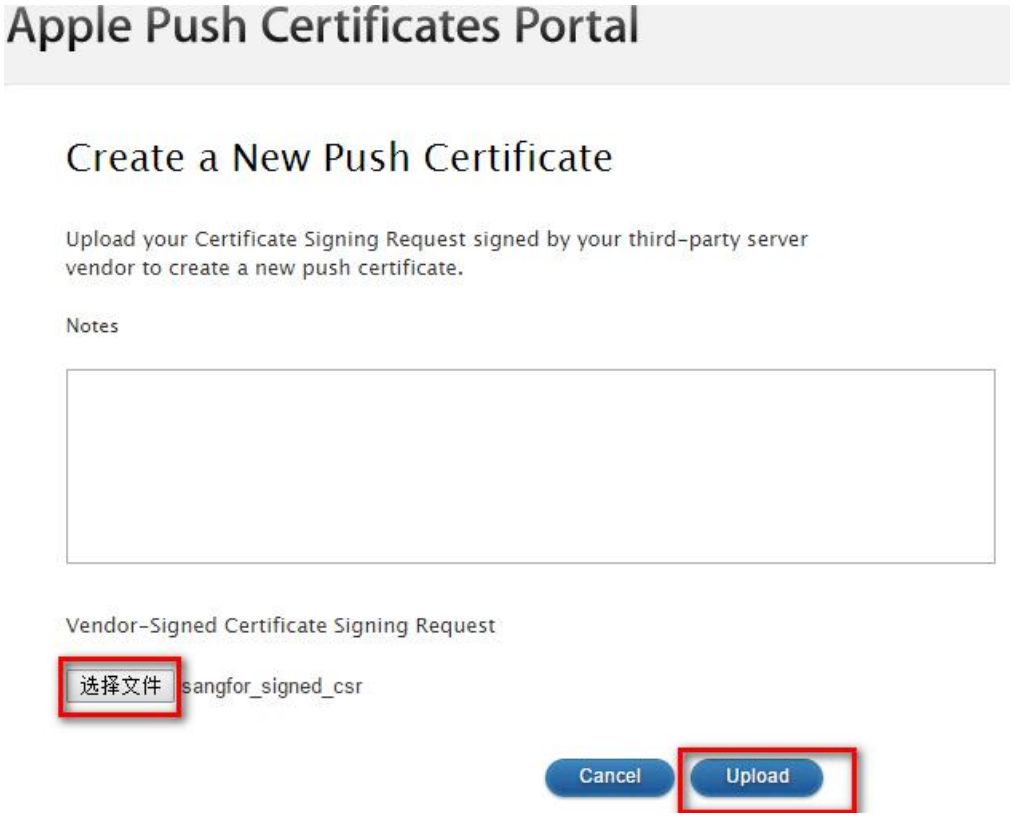


Step 2: To create a certificate application, click **Create a Certificate**, as shown below:

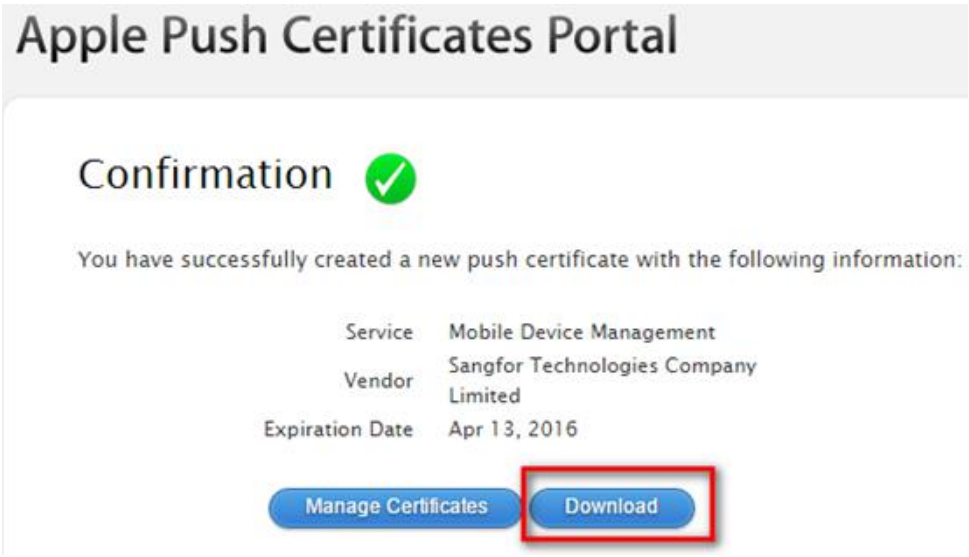




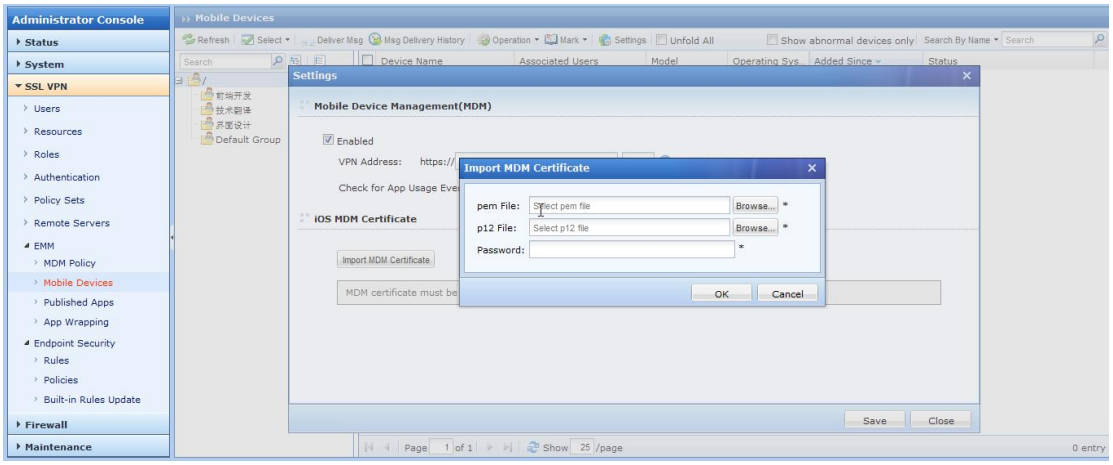
Step 3: Upload your **Certificate Signing Request**. Upload **sangfor_signed_csr** file (Contact Sangfor Customer Service), and click **Upload** as shown below:



Step 4: MDM push certificate is applied successfully after Certificate Signing Request is uploaded. Click **Download** to complete MDM certificate application.



Step 5: Navigate to **SSL VPN** > **EMM** > **Mobile Devices** to enter the **Mobile Devices** page. Click **Settings** > **Import MDM Certificate** to import MDM certificate, as shown below:



1. MDM certificate remains valid for one year.

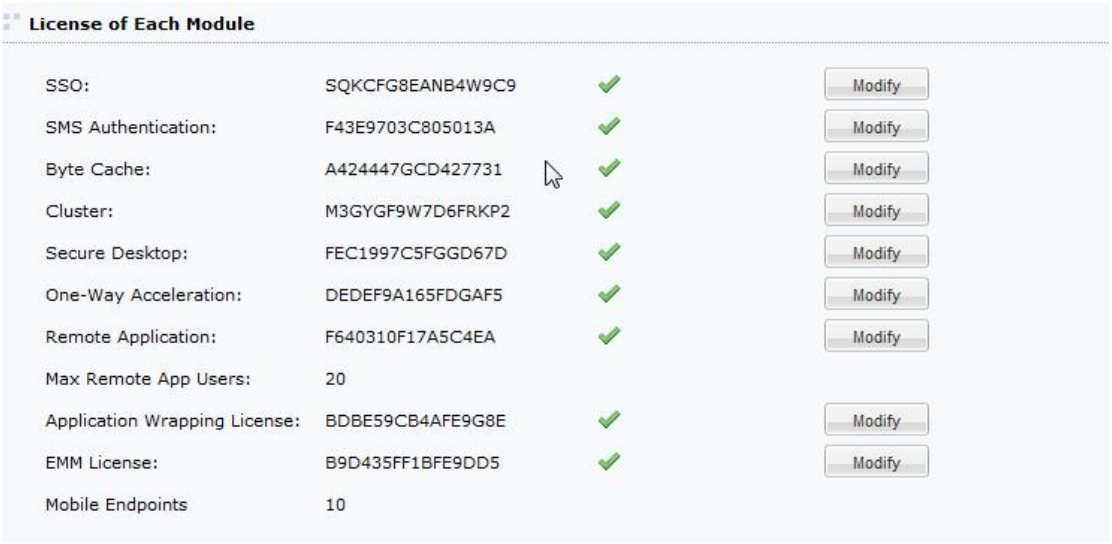
2. When MDM certificate expires, it should be renewed. Use Apple ID to log in to https://identity.apple.com/pushcert/ and you can view previously applied certificate. Click Renew, contact SANGFOR technical support to obtain a new sangfor_signed_csr file, and follow the above steps to apply for a new .pem file.

EMM Configuration Case

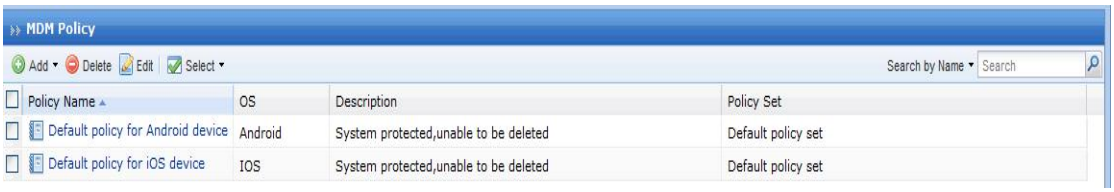
EMM of SSL functions to register mobile devices, manage and deliver messages, strengthen password security for mobile devices, notify admin to lock and erase data when mobile devices are lost, and protect resources security.

The configurations are as follows:

Step1: Navigate to **System** > **System** > **Licensing**. Click **Modify** to enable **EMM License**, as shown below:



Step 2: Navigate to **SSL VPN** > **EMM** > **MDM Policy** to enter the **MDM Policy** page. Add Android or iOS MDM Policy or edit default ones, as shown below:



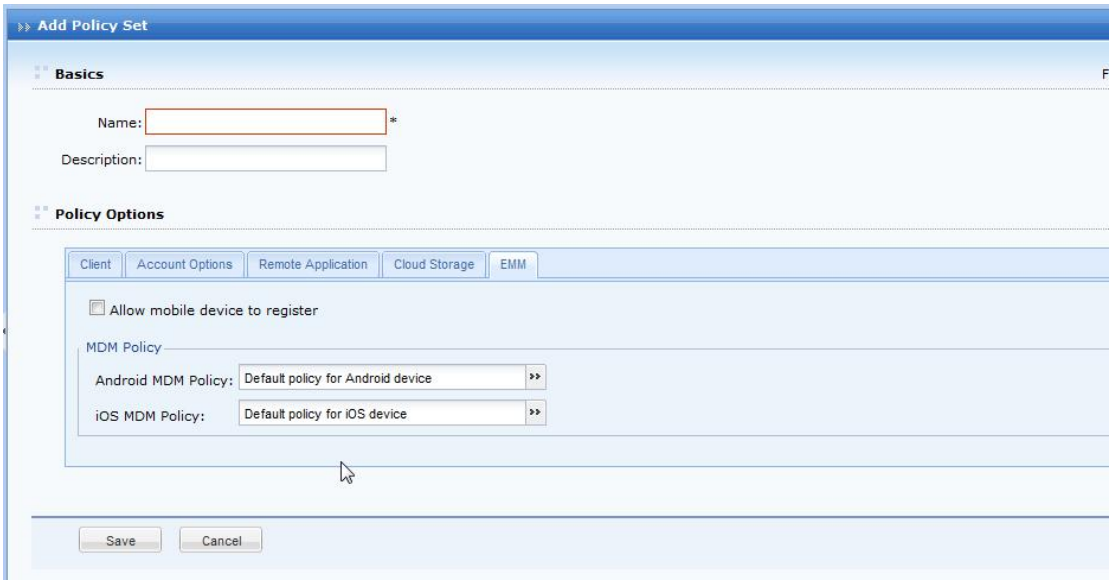
Step 3: Navigate to **SSL VPN** > **EMM** > **Mobile Devices** to enter the **Mobile Devices** page. Click **Settings** to select **Enabled**, enter VPN address, and click **Import MDM Certificate** to import IOS MDM Certificate, as shown below:



1. If SSL is deployed in internal network, then port 441 should be mapped to SSL on public network devices.

2. IOS MDM certificate must be imported, otherwise IOS device cannot be registered successfully.

Step 4: Navigate to **SSL VPN** > **Policy Sets** to enter the **Policy Set Management** page. Click **Add** > **Policy Set** to enter the **Add Policy Set** page. Click **EMM**, select **Allow mobile device to register**, and select default policy for Android device or for iOS device correspondingly, as shown below.



Step 5: Navigate to **SSL VPN** > **Users** to enter the **Local Users** page. Click **Add** > **Group** to enter the **Add User Group** page. Associate policy sets for user or user group under **Policy Set**, as

shown below:



Step 6: When you use mobile endpoints to log in to SSL through EC, your registration information will be submitted automatically and you will get logged in.

Configuring Firewall Rule

Configuring LAN<->VPN Filter Rules

Background:

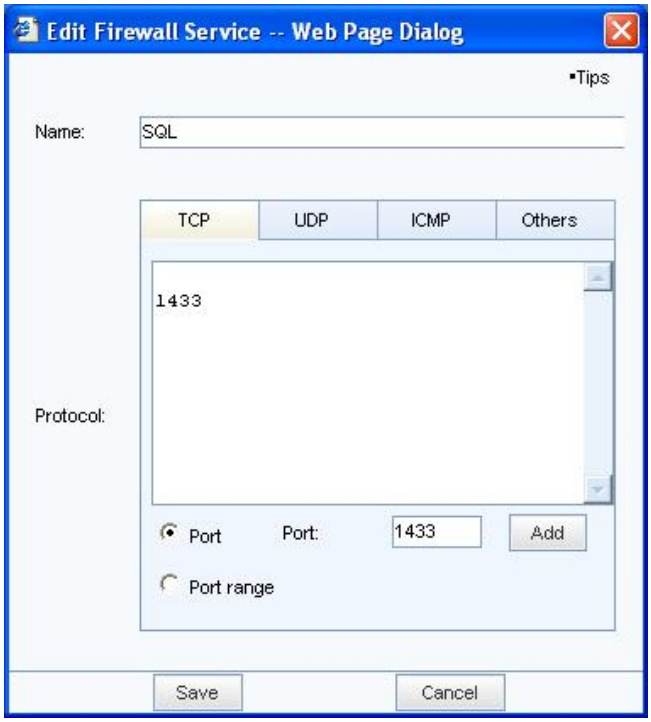
- The branch (172.16.1.0/24) has established VPN connection with the Headquarters.
- There is a server (192.168.10.20) located at Headquarters, providing Web service and SQL SERVER service.

Purpose:

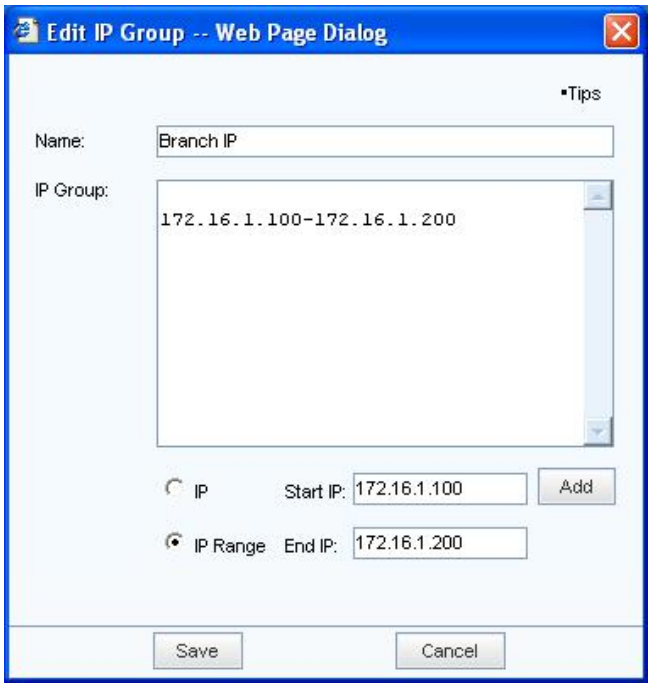
- Only the IP range 172.16.1.100-172.16.1.200 on the LAN subnet of the branch can access the Web service provided by the server 192.168.10.20.
- IP range 172.16.1.100-172.16.1.200 cannot access the SQL Server service provided by the same server 192.168.10.20.

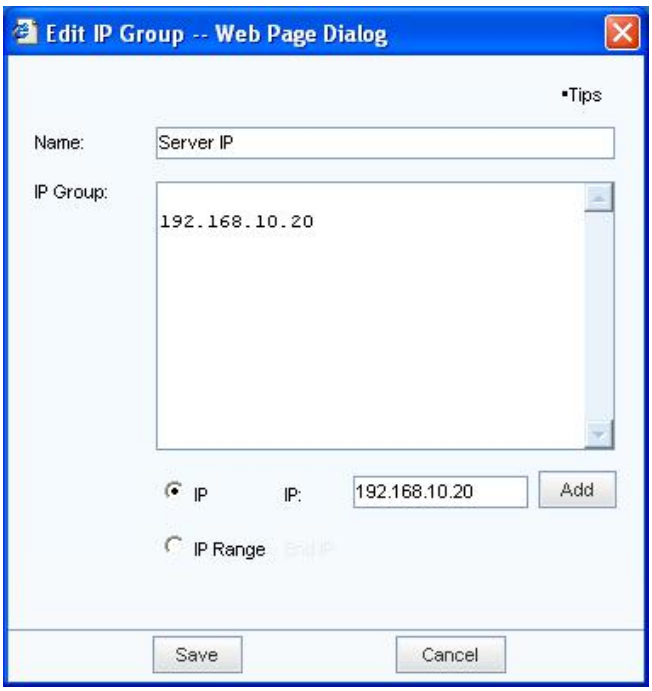
To achieve the expected purposes:

1. Navigate to **Firewall > Services** to define the SQL Server service.

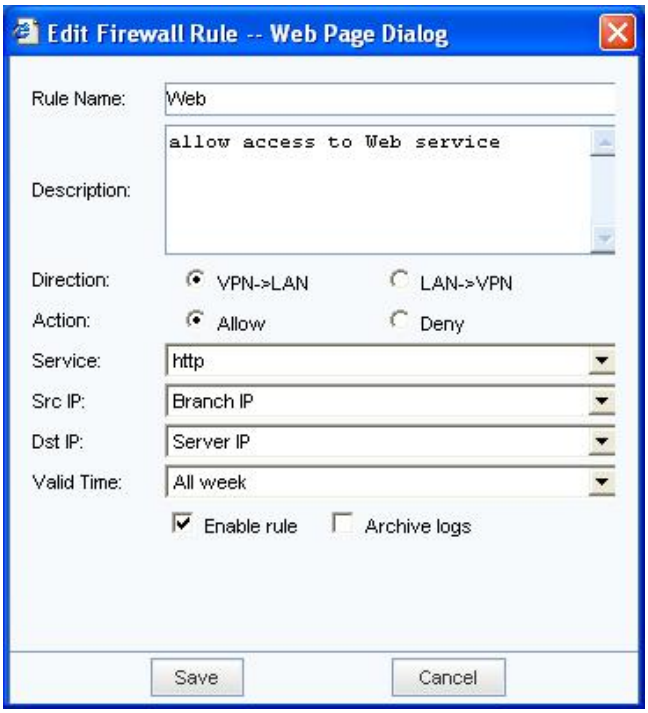


2. Navigate to **Firewall > IP Group** to define two IP groups, as shown below:

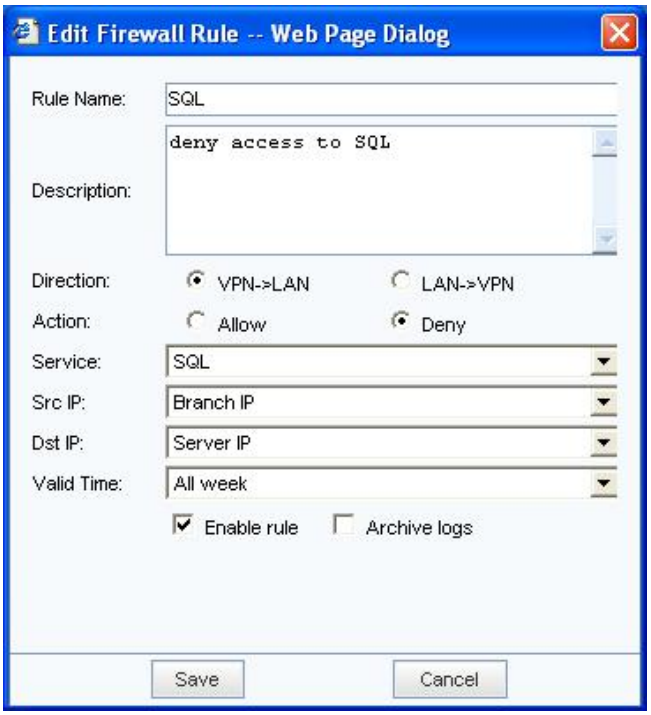




3. Configure the filter rule for Web service, as shown below:



4. Configure the filter rule for SQL Server service, as shown below:



To implement control over HQ employees' access to other services provided by the branch or over branch employees' Internet access through HQ, configure the corresponding filter rules to filter data sent between two interfaces.

Adding SNAT Rule

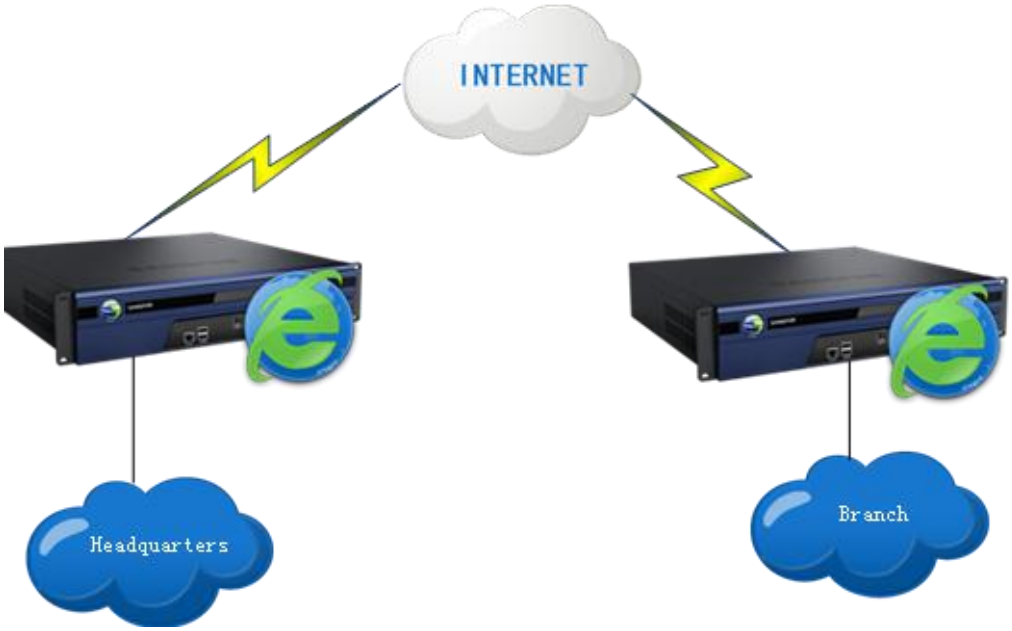
Background:

- The Sangfor device located at Headquarters is deployed in Route mode.
- The branch has established VPN connection with the Headquarters.

Purpose:

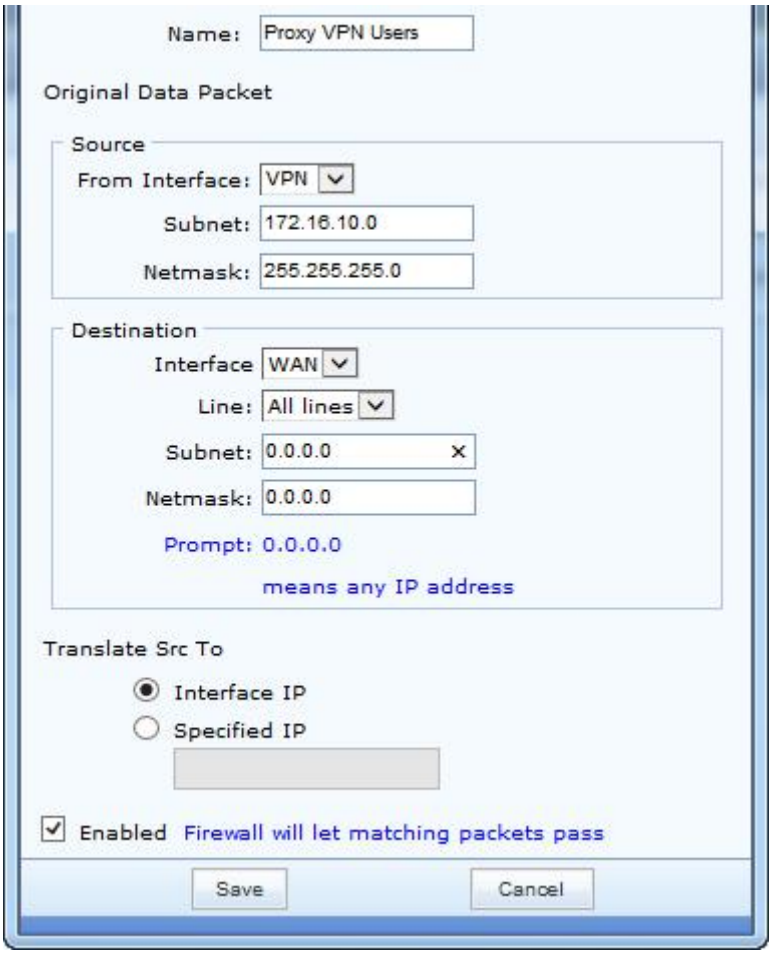
Configure a SNAT rule on the Sangfor device located at headquarters, so that users from branch (172.16.10.0/24) can access Internet after connecting to Headquarters through VPN connection.

Network Topology:



To achieve the expected purpose:

1. Navigate to **Firewall** > **NAT > SNAT Rule**, and click **Add** to enter the **Edit DNAT Rule** page, as shown below:



Adding DNAT Rule

Background:

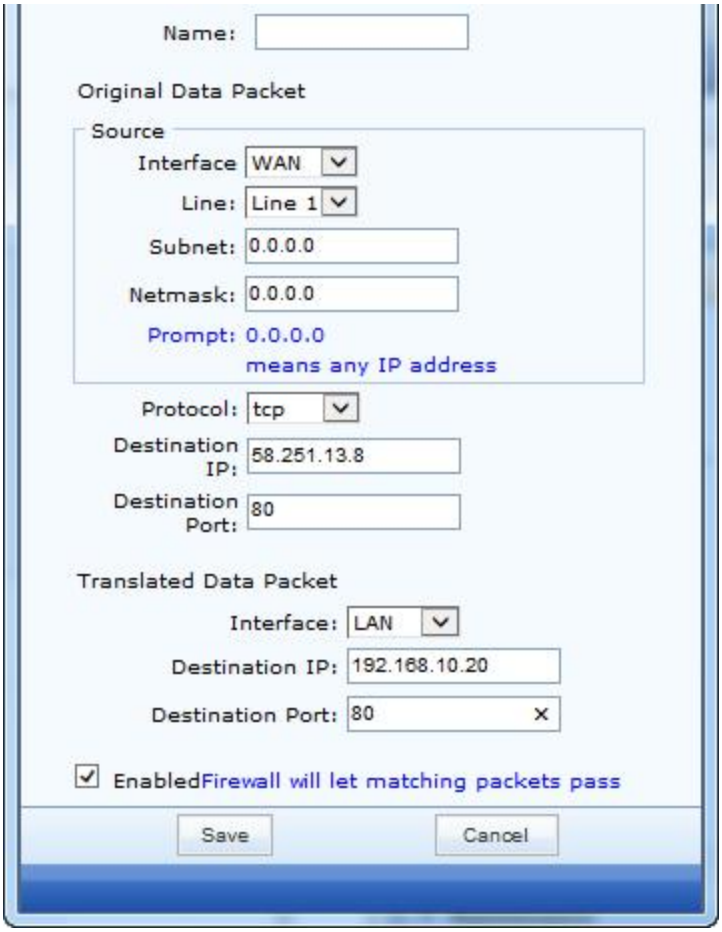
There is a LAN server (IP address: 192.168.10.20) providing Web service through the port 80.

Purpose:

Configure a DNAT rule to publish the Web service to the Internet on port 80, so that Internet users can access the Web service.

To achieve the expected purpose:

1. Click **Add** to enter the **Edit DNAT Rule** page, as shown below:



2. Configure the DNAT rule as shown in the figure above.
3. Click the **Save** buttons to save the settings.

After the above configurations are saved, Internet users can access the Web service by accessing the WAN interface of the Sangfor device.



To have the LAN server accessed by Internet users through configuring DNAT rules on the Sangfor device, the Sangfor device must act as gateway of the LAN computers or router to external network; otherwise, the DNAT rule will not work.

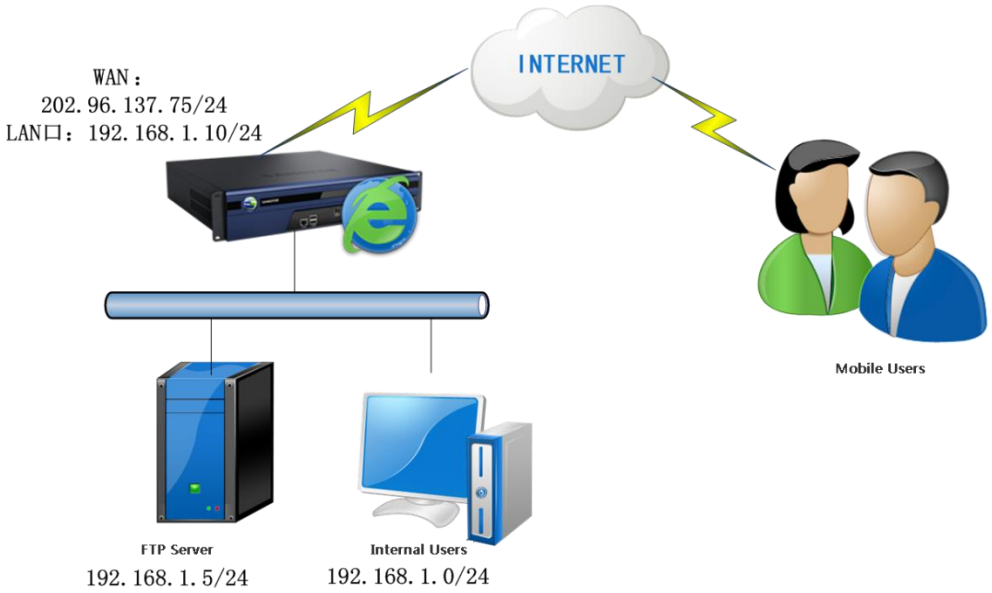
Typical Case Study

Required Environment

Background:
Sangfor device is deployed in Gateway mode and connected to Internet directly.

Purpose:
Mobile employees can access internal FTP server over SSL VPN and log in to SSL VPN automatically after their mobile device starts up.

Network Topology:



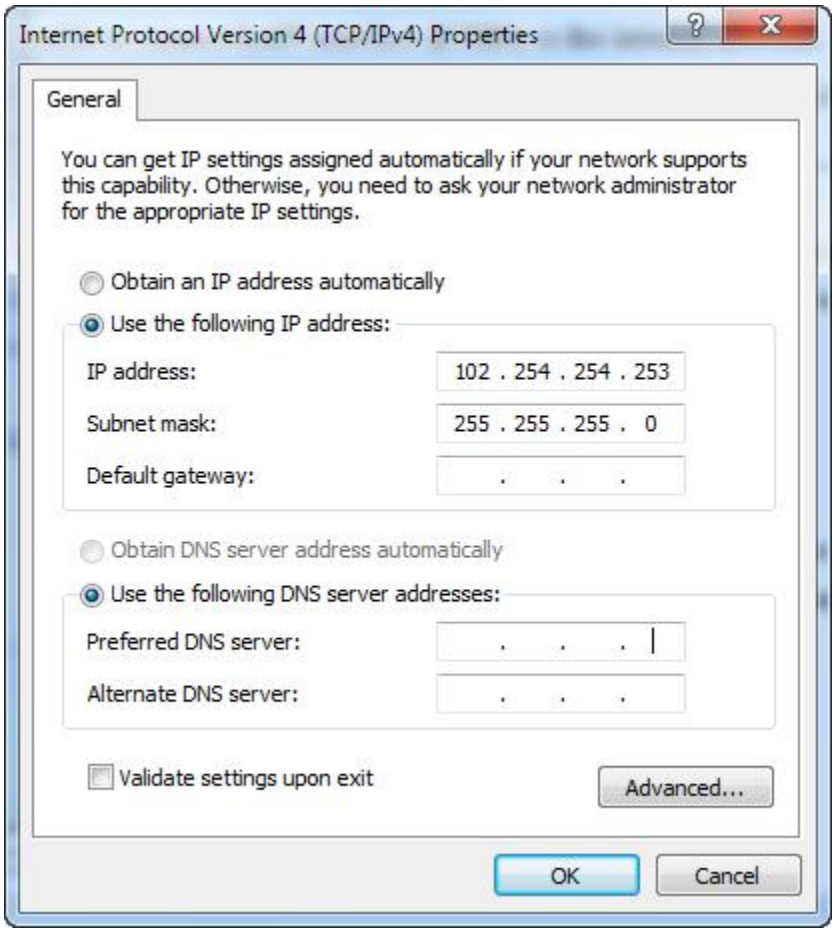
Configuration steps:

1. Deploy and connect related device as shown in the above network topology.
2. Create SSL VPN user and the resource which will be accessed by mobile users
3. Configure Sangfor device to enable user to log in SSL VPN automatically after mobile device starts up

Configuring Sangfor Device

1. Turn on the PC and Sangfor device. Use Ethernet cable to connect LAN interface (ETH0) of the device to the internal network(LAN). Add an IP address on the PC, an IP address that

resides in the network segment **10.254.254.X** (for instance, 10.254.254.100) with subnet mask **255.255.255.0**, as shown below:



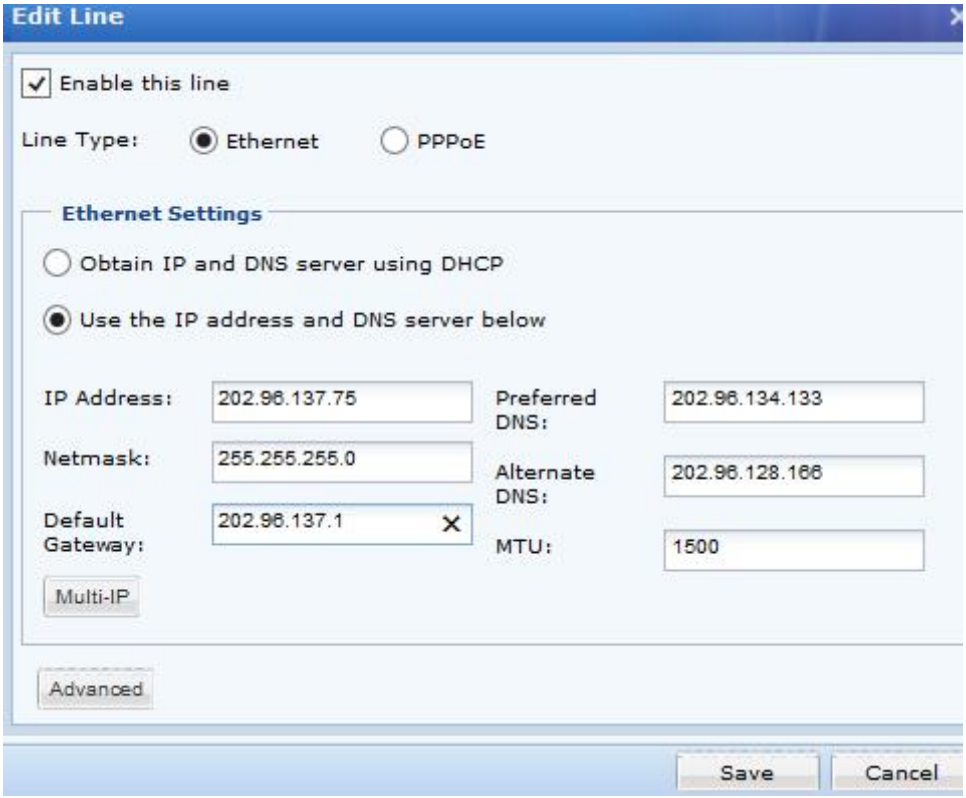
2. Open the IE browser and enter the SSL VPN address and HTTPS port (https://10.254.254.254:4430) into the address bar. Press **Enter** key to visit the login page to SSL VPN administrator Web console, as shown below:



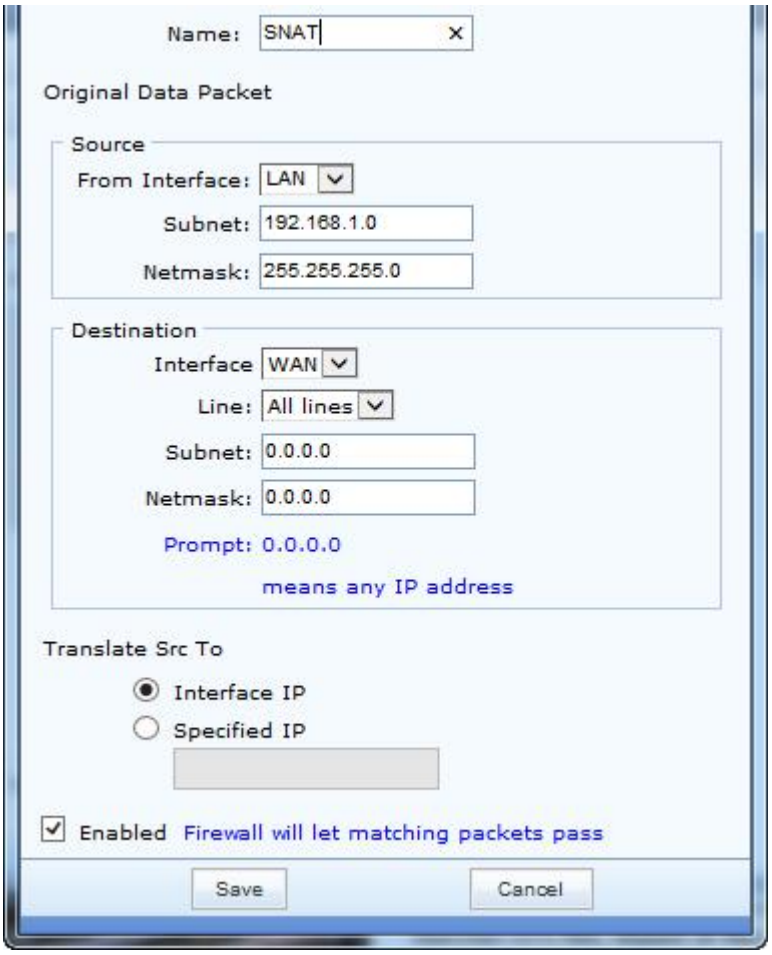
3. Navigate to **System > Network > Deployment**, select Gateway as **Deployment Mode** and configure LAN interface, as shown below:



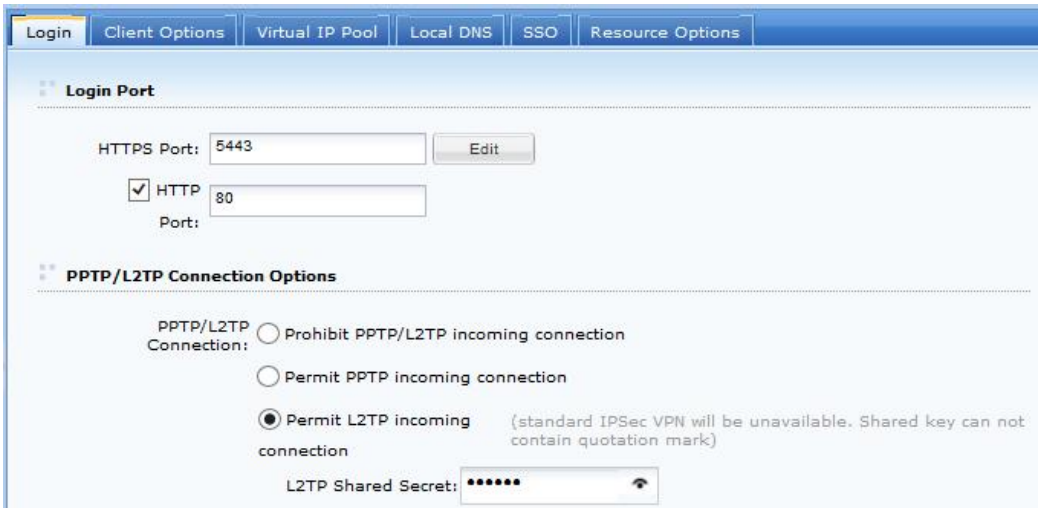
Internet line will be displayed under **External Interfaces** section and click corresponding line to configure it, as shown in the figure below:

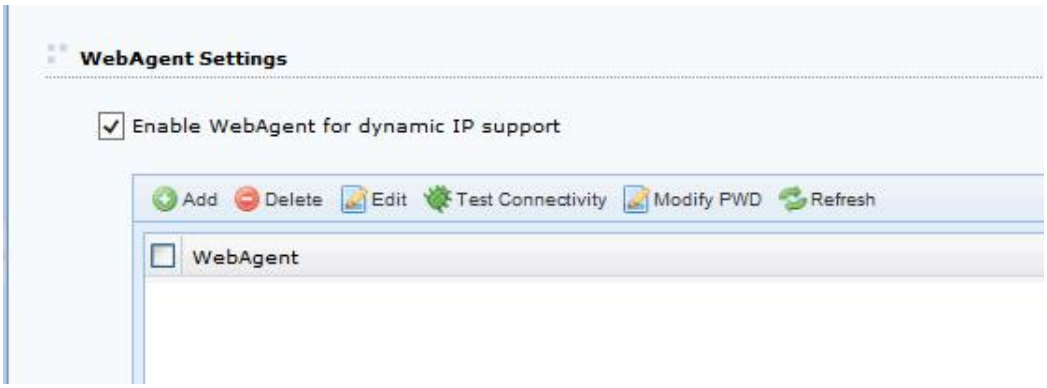


4. Add a SNAT rule on the **Firewall > NAT > SNAT Rule** page, as shown below:



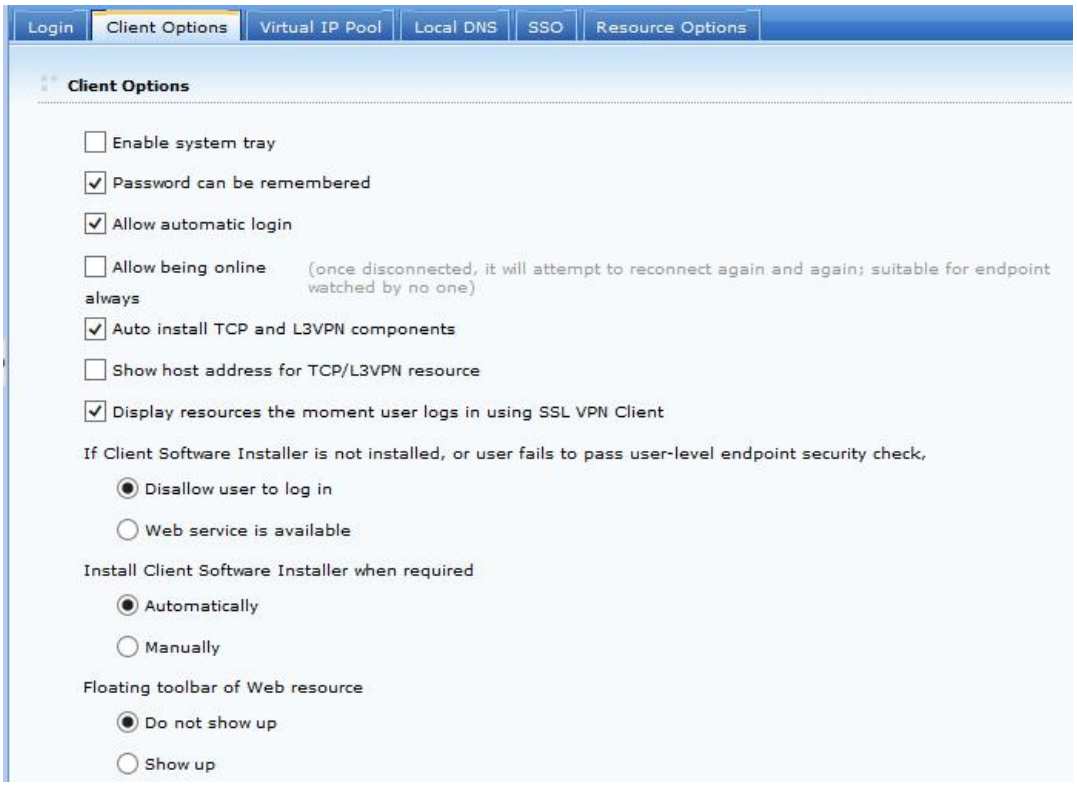
5. Go to **System > SSL VPN Options > General > Login** page to specify HTTP port and HTTPS port and configure WebAgent, as shown below:



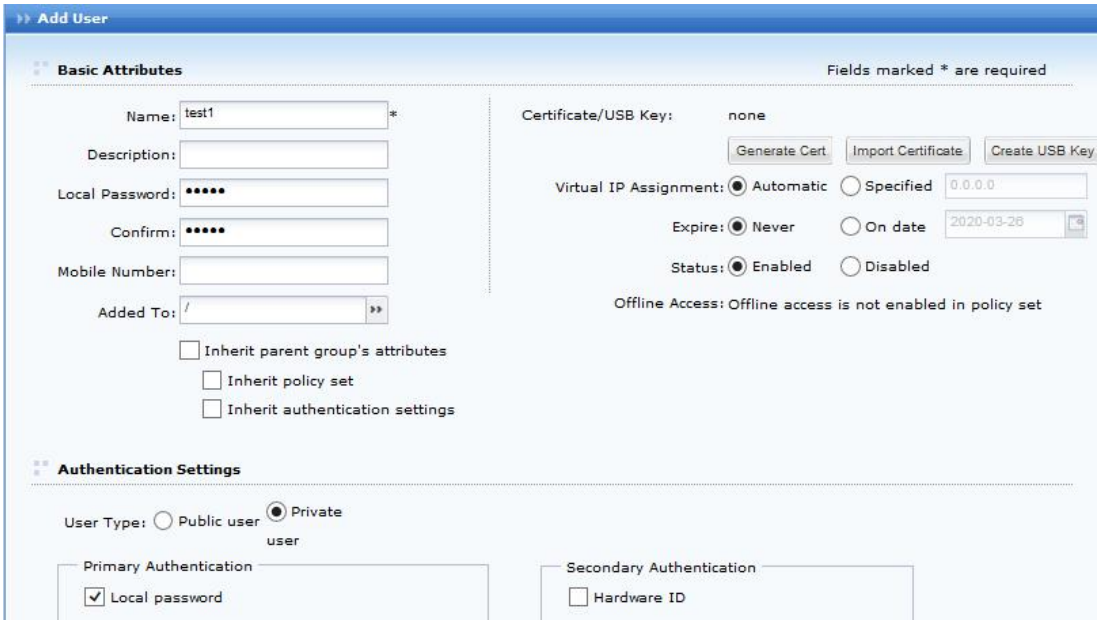


- Port 443 is default HTTPS port. If it is modified, you need to append it following the URL of Sangfor device when accessing SSL login page. Do not modify it unless necessary.
- If Sangfor device has no fixed public IP address, you can use WebAgent to discover IP address.

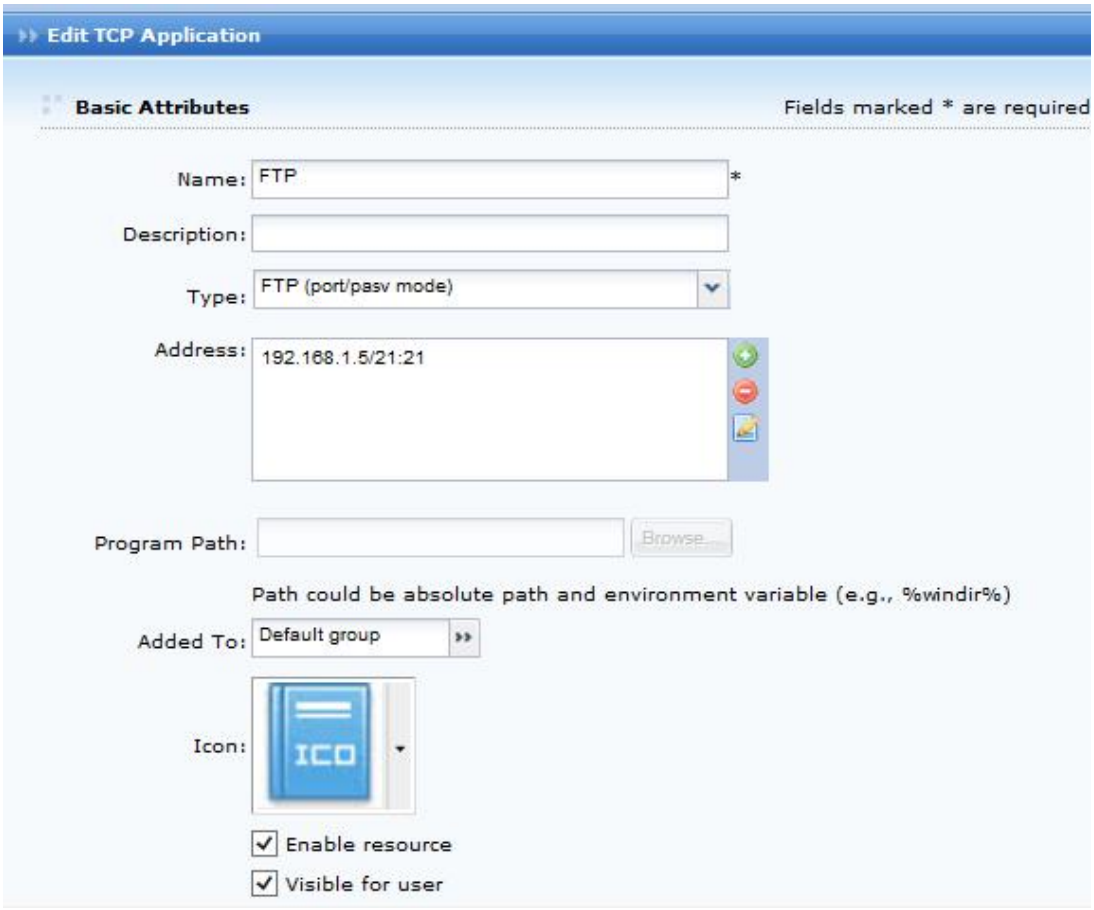
6. Go to **System > SSL VPN Options > General > Client Options** page to configure related options for this scenario, as shown in the figure below:



7. Go to **SSL VPN > Users > Local Users** and click **Add > User** to add a user named **test1**, as shown below:



8. Add a TCP app, named FTP, on **SSL VPN > Resources** page, as shown below:

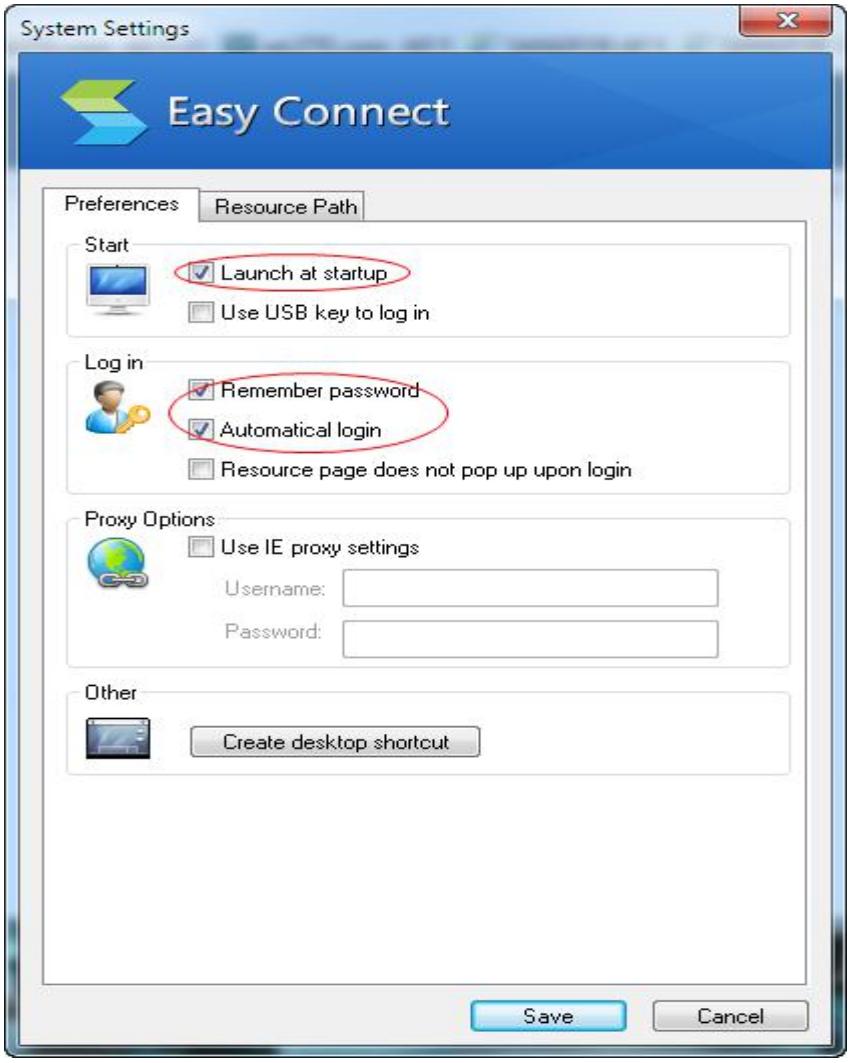


9. Go to **SSL VPN > Roles > Role Management** page to create a role and associate it with the user **test1** created in step 7 and the TCP resource created in step 8(for detailed guide, refer to Adding Role in Chapter 4).
10. Click Save to save all the changes and click **Apply** button to apply the settings.
11. After user **test1** logs in to SSL VPN, he/she will see the following resource page:



To access FTP server, click on the FTP link.

12. Right-click on VPN client logo and click **System Settings** and select related options, as shown below:



13. Click **Save** to save the changes.

Appendix A: End Users Accessing SSL VPN

This section introduces how end users configure browser and log in to SSL VPN.

Required Environment

- End user's computer can connect to the Internet.
- No security assistant software is installed on the computer, because this kind of software may influence the use of SSL VPN.
- Any mainstream browser is installed on the computer, such as, Internet Explorer (IE), Opera, Firefox, Sarafi, Chrome, etc.



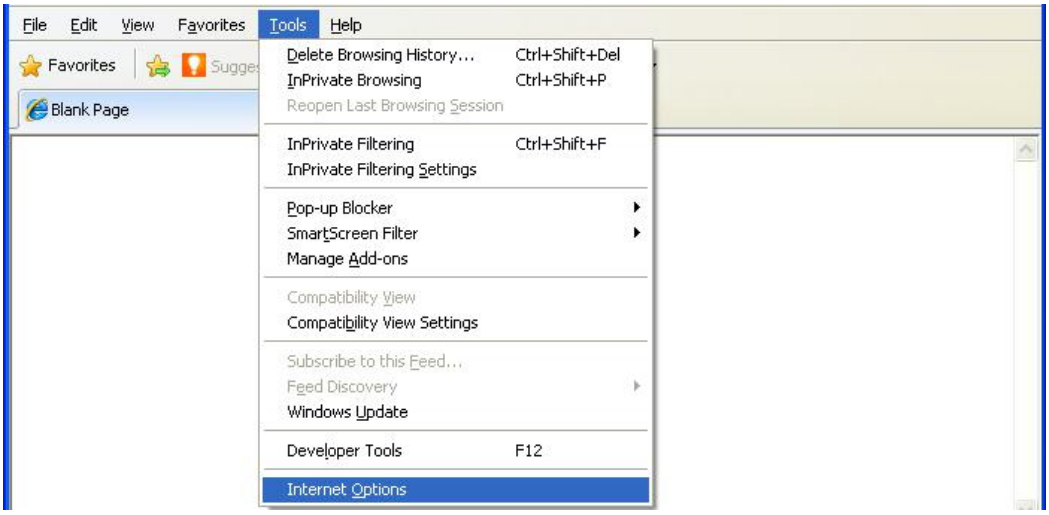
- Operating systems should be 32bit/64bit Windows XP/2003/Vista/Win7, 32bit Linux Ubuntu 11.04/RedHat 5.2/RedFlag/Fedora 13/SUSE 11.2, or Mac OS X Leopard(10.5)/Snow Leopard(10.6)/Lion(10.7).
- SSL VPN client is available on iPhone and Android mobile phones.

Configuring Browser and Accessing SSL VPN

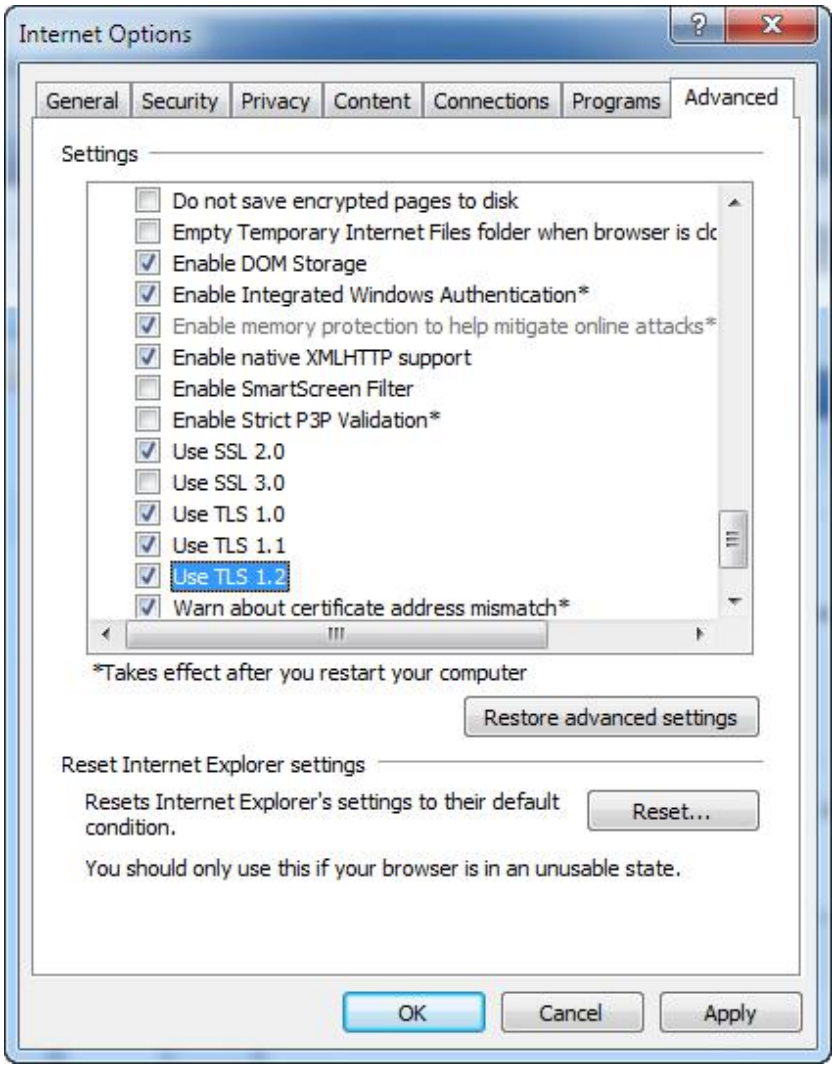
Configuring Browser

The following configuration takes Windows XP IE browser for example. Screenshots may vary with different operating systems.

1. Launch the IE browser and go to **Tools** > **Internet Options** to configure the IE browser, as shown in the figure below:



2. Click **Advanced** tab. Find the **Security** item and select the checkboxes next to **Use SSL 2.0**, and **Use TLS 1.0**, as shown in the figure below:



3. Enter the SSL VPN address into the address bar of the browser and visit the login page to SSL VPN.

4. When you visit the login page, a security alert may appear, requiring installation of security certificate, as shown in the figure below:



5. Click the **View Certificate** button to complete installing the root certificate if this is the first time you log in to SSL VPN administrator Web console. The information of the root certificate is as shown below:



6. Click the **Install Certificate** button and use the **Certificate Import Wizard** to import the root certificate, as shown in the figure below:



7. Select a directory to store the certificate and click the **Next** button. After confirming the settings and clicking the **Finish** button, another warning pops up asking whether to install the certificate, as shown in the figure below:



8. Click the **Yes** button to ignore the warning and the root certificate will be installed, as shown in the figure below:



Generally, root certificate is required to be installed when you logs in to the SSL VPN for the first time. Once root certificate is installed, you need only click the **Yes** button next time when logging in and see the security alert.

Using Account to Log In to SSL VPN

If root certificate has been installed, user can visit the login page to the SSL VPN. The login page is as shown in the figure below:

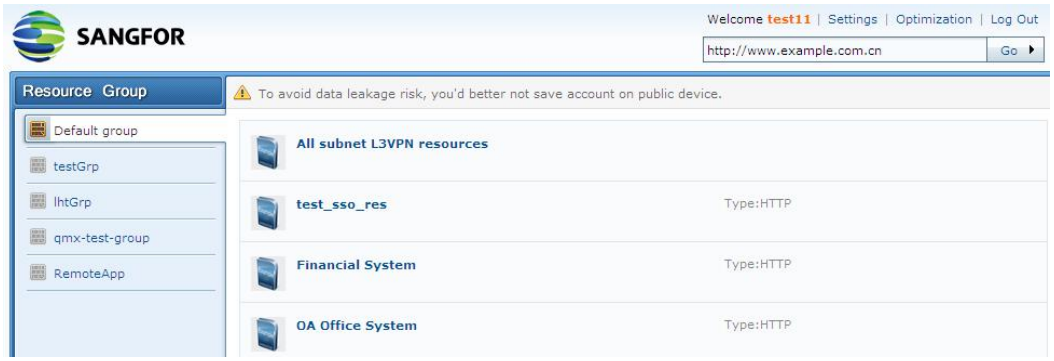


1. Enter and submit the required credentials through the login page. The following are the contents included on the login page:

   - **Username**, **Password:** Enter the username and password of the SSL VPN account to connecting to the SSL VPN.
   - **Verification:** Enter the word on the picture. Word verification feature adds security to SSL VPN access and could be enabled by administrator manually, or activated automatically when brute-force login attempt is detected.
   - **Use Certificate:** A login method that enables user to use certificate to go through the user authentication. The certificate should have been imported to the IE browser manually.
   - **Use USB Key:** A login method that enables user to use USB key to go through the user authentication. There are two types of USB keys, one type has driver and the other type is driver free.

   User using USB key to get authenticated may need to install the USB key driver. For detailed guide, please refer to the SSL VPN Users section in Chapter 4.

2. Once user passes the required primary and secondary authentications, he/she will enter the **Resource** page, as shown in the figure below:



3. All the resources or groups associated with the connecting user will be displayed on the **Resource** page. Click on any of the links to access the corresponding resource.

   For Web application resources, user can access them simply by clicking on the resource link.

   For C/S applications that cannot be accessed through browser, user can start the SSL VPN Client program (under **Start** > **Programs** > **SSL VPN Client**) and access the application by entering IP address of the server, as if user's PC resides in the enterprise network.

4. TCP and L3VPN components will be installed automatically when user accesses associated TCP resource or L3VPN resource.



5. To log out of the SSL VPN, click **Log Out** at the upper right of the page. Once user logs out, he/she cannot access the internal resources any more.

6. To modify password of the SSL VPN account, click **Settings** at the upper right of the page to enter the **User Account** page, as shown in the figure below:



As shown above, the current password is followed by **Modify**. Click it to enter the **Modify Password** page, as shown below:



- If user keeps inactive for a long time during SSL VPN access, without performing any operation or accessing any resource, user will be disconnected and log out automatically.
- The contents shown in **Settings** are related with SSL VPN configurations. Those contents will be taken valid.

Using USB Key to Log In to SSL VPN

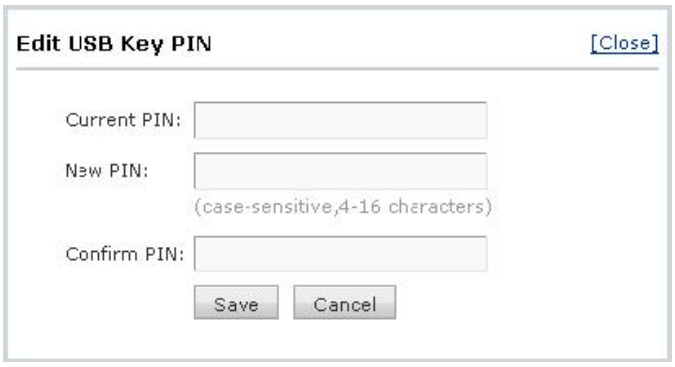
User login using USB key is a bit different from that using account.

Main differences are the login process and login page. User should perform the following:

1. Launch the browser and visit the login page to the SSL VPN.
2. Insert the USB key into the USB port of the computer.
3. Select other login method **Use USB Key** to enter the next page that asks for PIN of the USB key.
4. Enter PIN of the USB key and login process completes.
5. To modify PIN of the USB key, click **Settings** at the upper right of the **Resource** page to enter **User Account** page, as shown below:

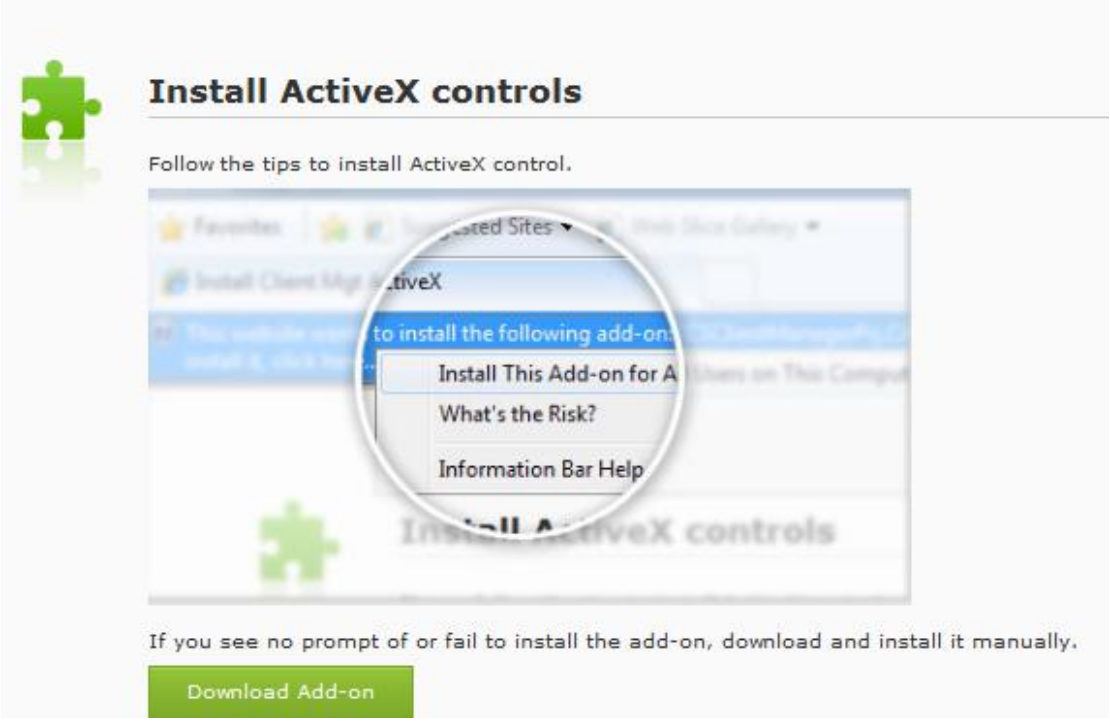


Click **Modify** to enter the **Edit USB Key PIN** page, enter the current PIN and the new PIN and click the **Save** button, as shown below:



Using VPN Client to Log In SSL VPN

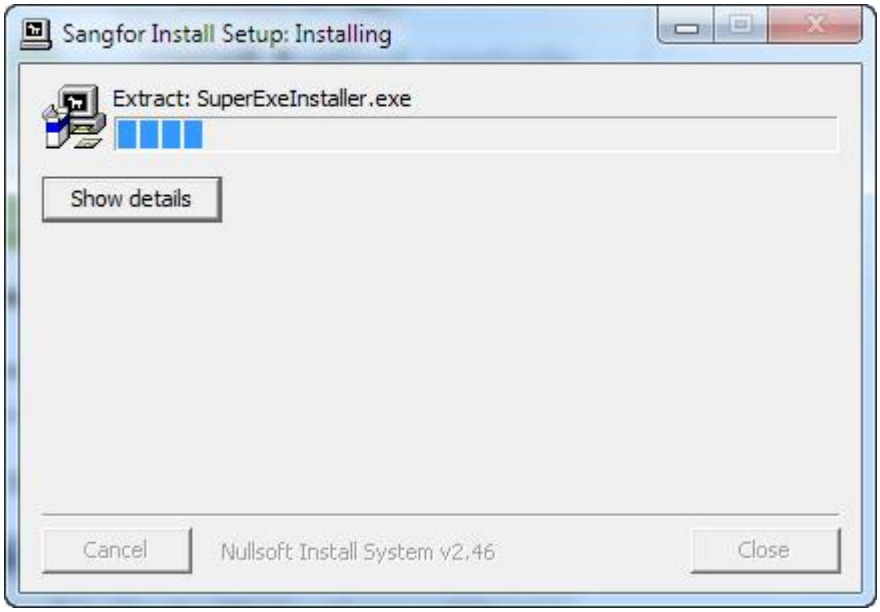
SSL VPN client components will be installed automatically when user logs in SSL VPN through IE browser. On **System > SSL VPN Options > Client Options** page, you can enable client software installer to be installed automatically or manually when required. If **Manually** corresponding to the **Install Client Software Installer when required** option is selected on the Sangfor device, the following page will pop up when user logs in VPN, as shown below:



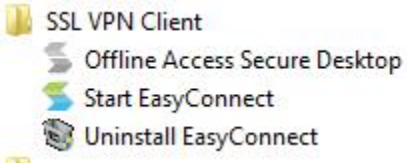
Click **Download Add-on**, a dialog appears, as shown below:



To install it, click **Run**. You will see the following installation page.

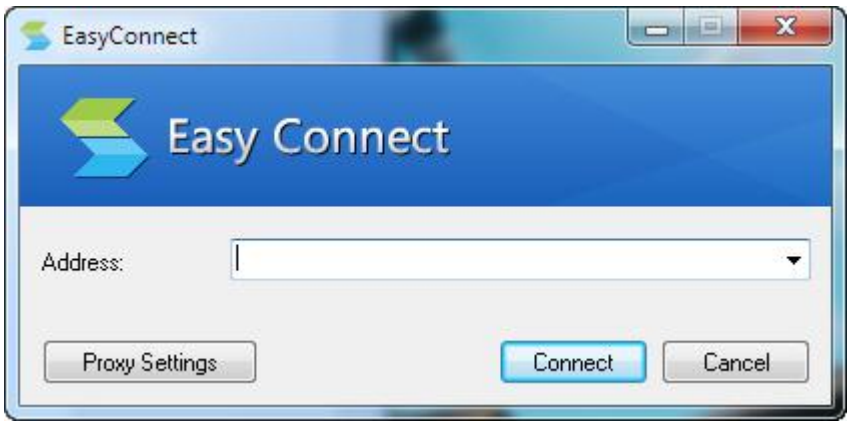


After software installer is installed, navigate to **Start** > **Programs** and you will see the following directory, as shown below:

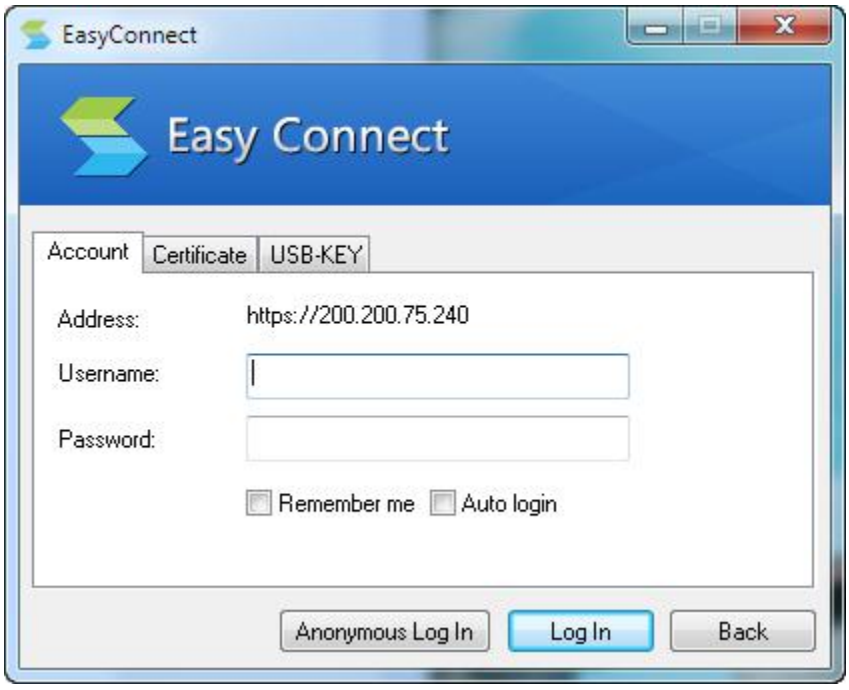


Please terminate firewall and antivirus software when installing client software installer; otherwise, the client will fail to be installed.

1. Click **Start EasyConnect** to open the SSL VPN client window, as shown below:

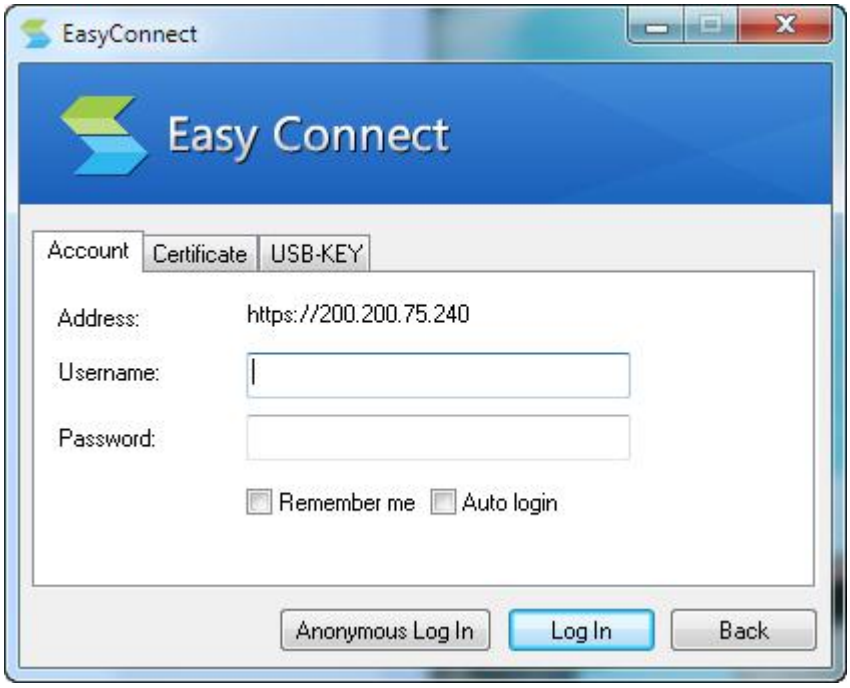


2. Enter the address of SSL VPN and click **Connect**, the following dialog appears.



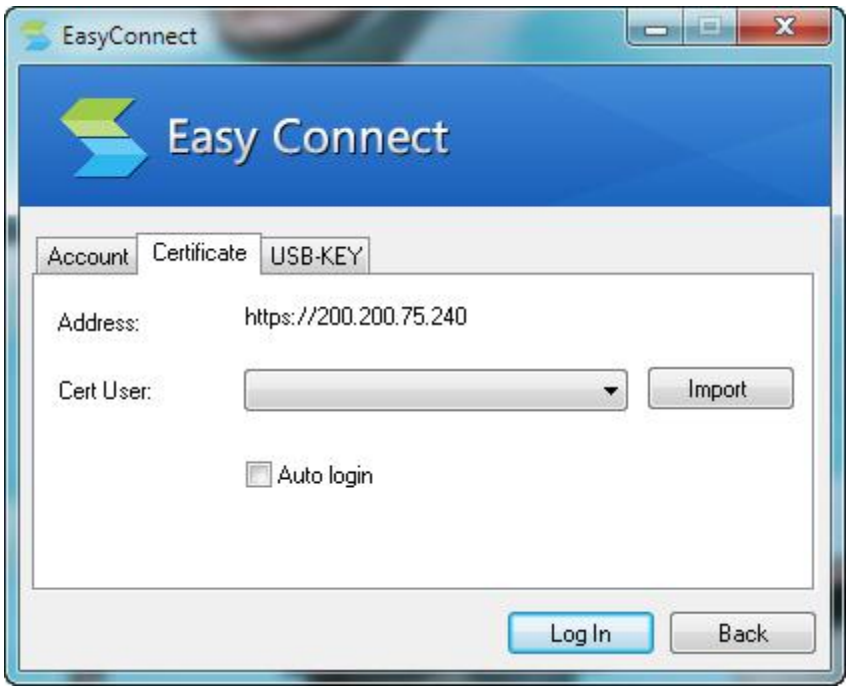
- For authentication based on username and password, select **Account**. The **Account** tab is as

shown in the figure below:



User can select **Remember me** and **Auto login** options if required, then he/she does not need to enter these information upon next login. The two options are available only when they are enabled on the device(for details, refer to Client Options in Chapter 3).

- For authentication based on certificate, select **Certificate**. The **Certificate** tab is as shown in the figure below:



- For authentication based on USB key, select **USB Key**. The **USB-KEY** tab is as shown below:



To create SSL VPN user, refer to Adding User in Chapter 4.

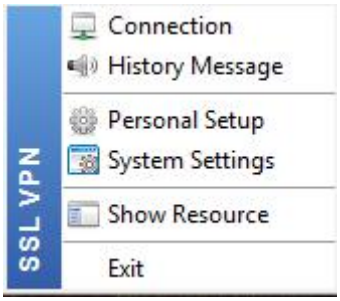
3. Select an authentication method as per your case. After logging in, a prompt dialog appears, as shown below:



If system tray is enabled when configuring Client Options on Sangfor device, the VPN client logo will be shown on the lower-right corner of the desktop. Put the cursor on it, you can see the connection status and VPN flow speed, as shown below:



To view VPN connection status and configure VPN-related settings , right-click on the **System Tray** icon and you will see the following floating window, as shown below


SSL VPN
Connection
History Message
Personal Setup
System Settings
Show Resource
Exit

Appendix B: Sangfor Firmware Updater 6.0

Sangfor Firmware Updater 6.0 is intended to update version and restore configurations of any Sangfor device, IAM, SSL VPN, WANO, AD. Compared to the previous version 5.0, Firmware Updater v6.0 is improved on the following:

1. Simplified update process

   Firmware Updater v6.0 works as an update wizard, support **online update** feature that helps search for updates and analyze versions of available updates for the connected Sangfor device in the local area network.

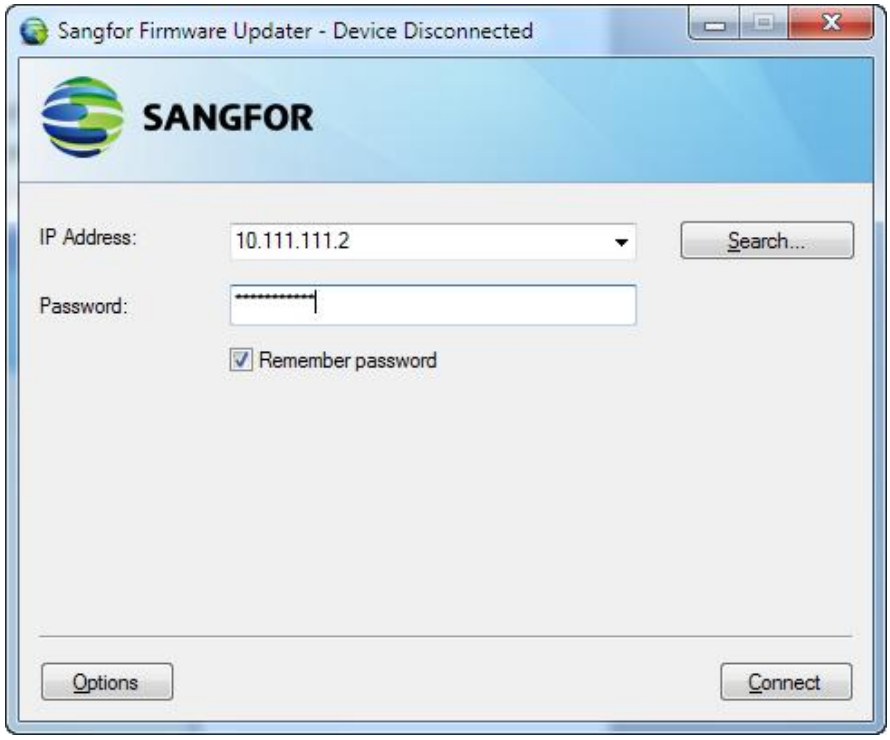
   Using online update method to update Sangfor device, network administrators need not handle some troubles such as preparing Sangfor device, checking current version of their Sangfor device, downloading update package, etc., but only choose an available version and click buttons.

   In addition to online update, administrators can browse and upload an existing package from the computer to update the Sangfor device manually or restore the configurations if the configuration is backed up previously.

2. The program file that can launch **Sangfor Firmware Updater** is included in a compressed file and available once the compressed file is decompressed, without being installed on the computer.

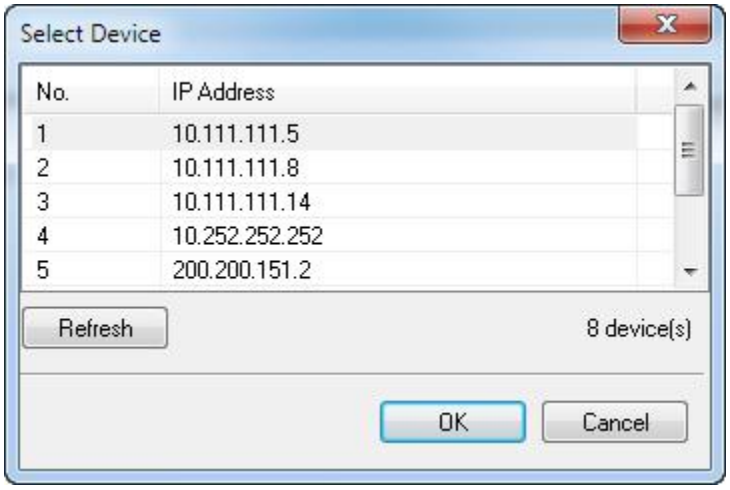
Updating Your Sangfor Device

1. Download the **SANGFOR-Updater6.0.zip** file from the Sangfor official website.
2. Double-click the executive file **SANGFOR Firmware Updater.exe**, and then specify or search for the Sangfor device that you want to connect to and update, as shown below:

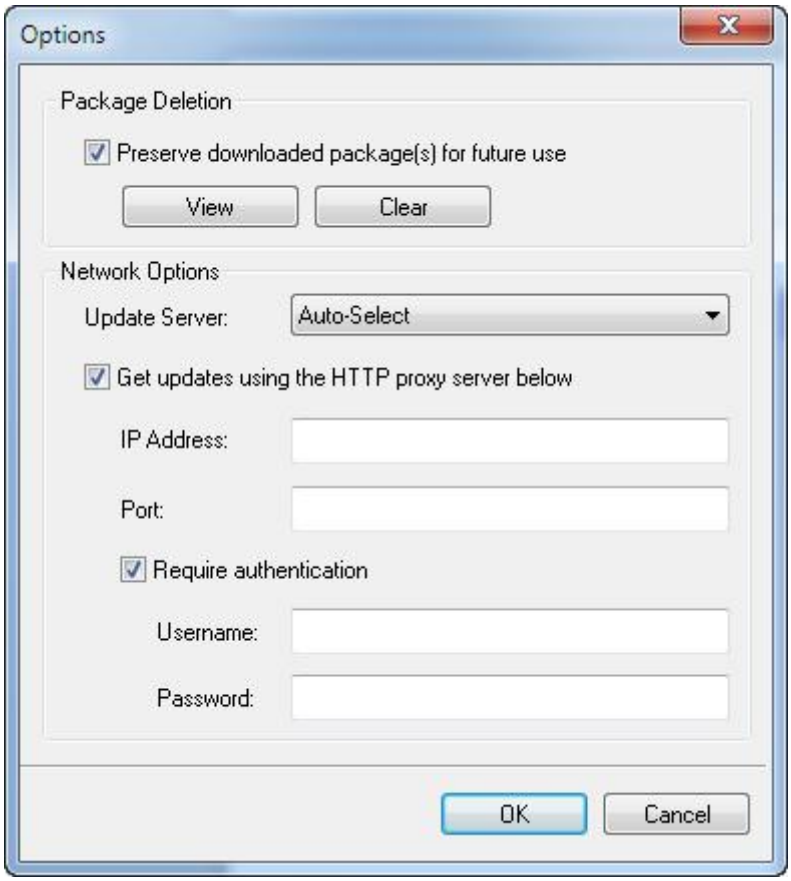


The following are the contents included on the above page:

- **IP Address:** Enter the LAN interface IP address of the Sangfor device that you want to connect to and update. IP:Port format is supported.
- **Password:** Enter the password for connecting to the Sangfor device specified above. The default password is **dlanrecover** (case-sensitive), or password of the default administrator account (**Admin** or **admin**) for connecting to the administrator console.
- **Remember password:** Select this option to remember the password so that the password need not be entered once again when you connect to this device via Sangfor Firmware Updater next time.
- **Search:** Click this button to search for Sangfor devices in the local area network. If any Sangfor device is found, it will be displayed on **Select Device** page, as shown below:



3. Click the **Options** button to configure **Package Deletion** option and network related settings, as shown below:



The following are the contents included on the **Options** page:

- **Preserve downloaded package(s) for future use:** Select this option and the previously downloaded packages (in **Download** folder) will be preserved and can be used for future update or configuration restoring.

  To open **Download** folder and view the downloaded package(s), click the **View** button.

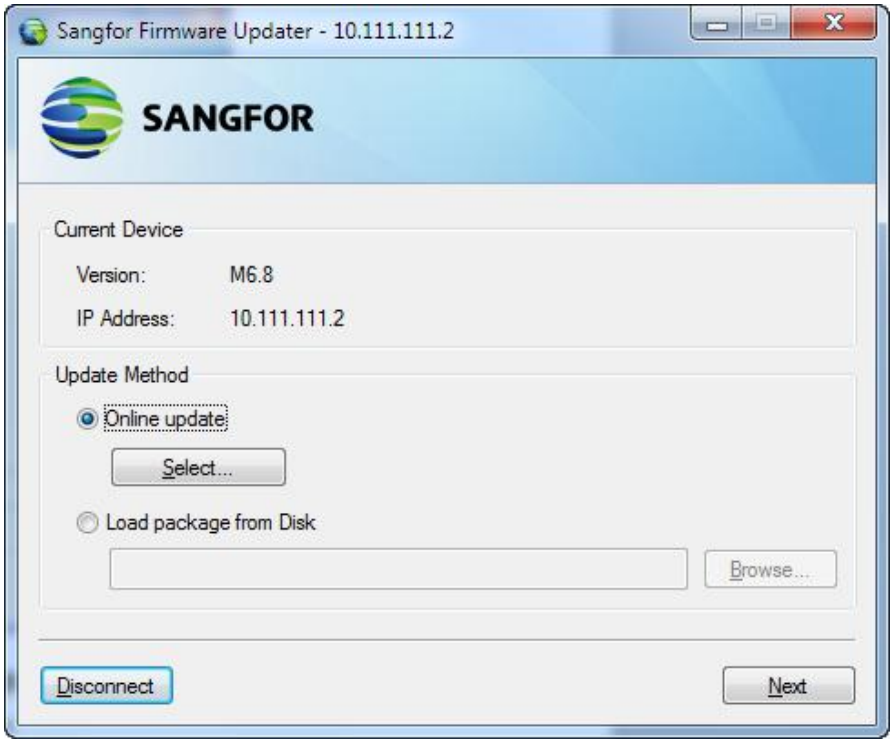
  To delete all the downloaded packages in **Download** folder, click the **Clear** button.

- **Update Server:** Select an update server, **Shenzhen** or **Shanghai,** which will always be used to get updates, or select **Auto-Select** to have the system select update server every time. This option only works when update method is online update.

- **Get updates using the HTTP proxy server below:** To specify a HTTP proxy server to get updates for the connected Sangfor device, select this option and enter the IP address and port of the HTTP proxy server in the **IP Address** and **Port** fields respectively.

- **Require authentication:** To have the HTTP proxy server require authentication, select this option and enter the username and password into the **Username** and **Password** fields respectively.

4. Click the **Connect** button to connect to the specified Sangfor device and select **Online update** method or **Load package from Disk**, as shown in the figure below:



Under **Current Device** are the version information (e.g., **M5.2** of SSL VPN) and IP address (e.g., **10.111.111.2**) of the currently connected Sangfor device.

Under **Update Method** are two options, **Online update** and **Load package from Disk**. The former is the previously mentioned feature that can automatically get updates for the connected Sangfor device, and the latter enables administrator to choose a package to update the current device or restore the configurations on the current Sangfor device with those contained in the chosen package.

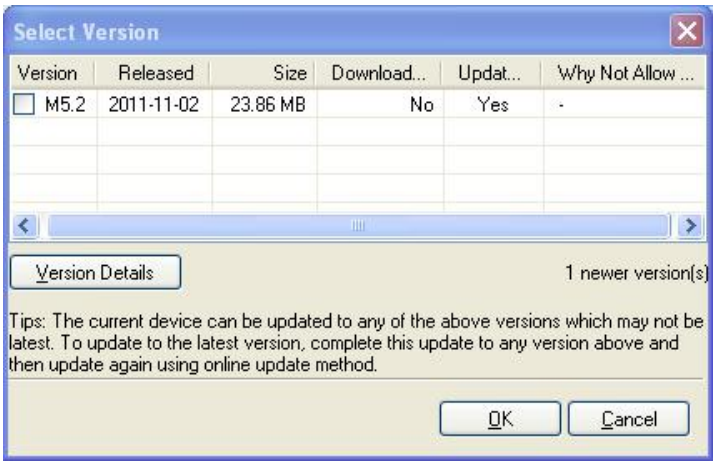


Currently, online update only supports update of version SSL M5.0 and above. For update of lower versions and other series of Sangfor devices, please select the update method **Load package from Disk**.

5. Search for newer version and download update package, or load package.

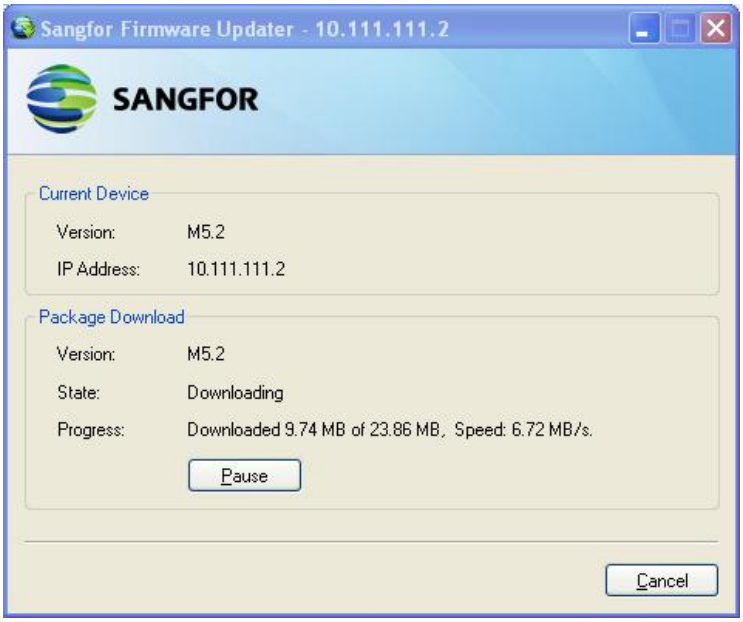
   - Select new version and download package. It happens when method is **Online update**.

     a. Click the **Select** button and the firmware updater will check for updates. After updates checking and analyzing, the available and updatable version(s) are displayed on the **Select Version** page, as shown in the figure below:



b. Select the checkbox next to a version and click the **OK** button to close this page.

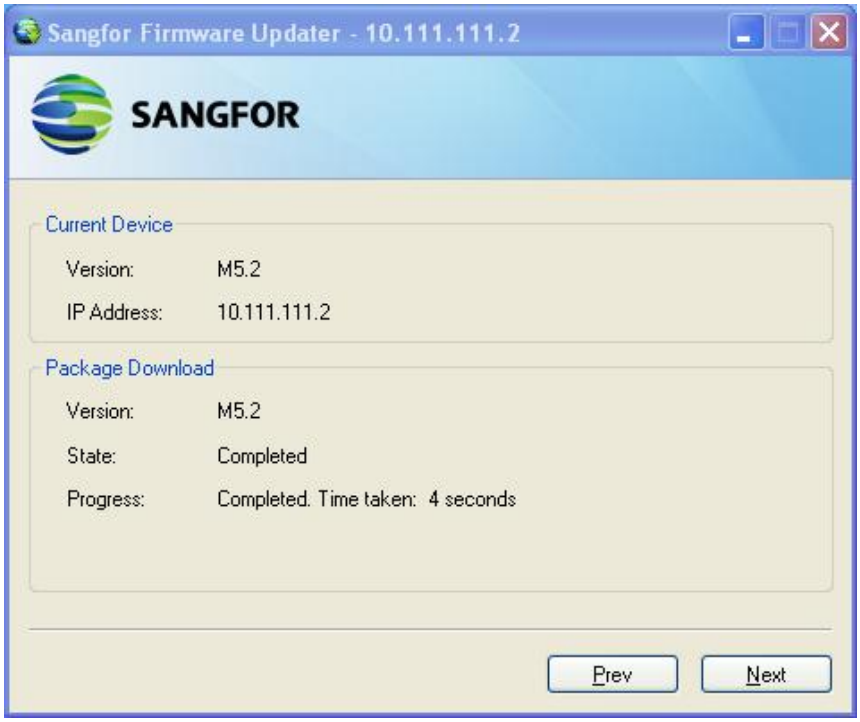
c. Click the **Next** button to download package of the selected version. The download process is as shown in the figure below:



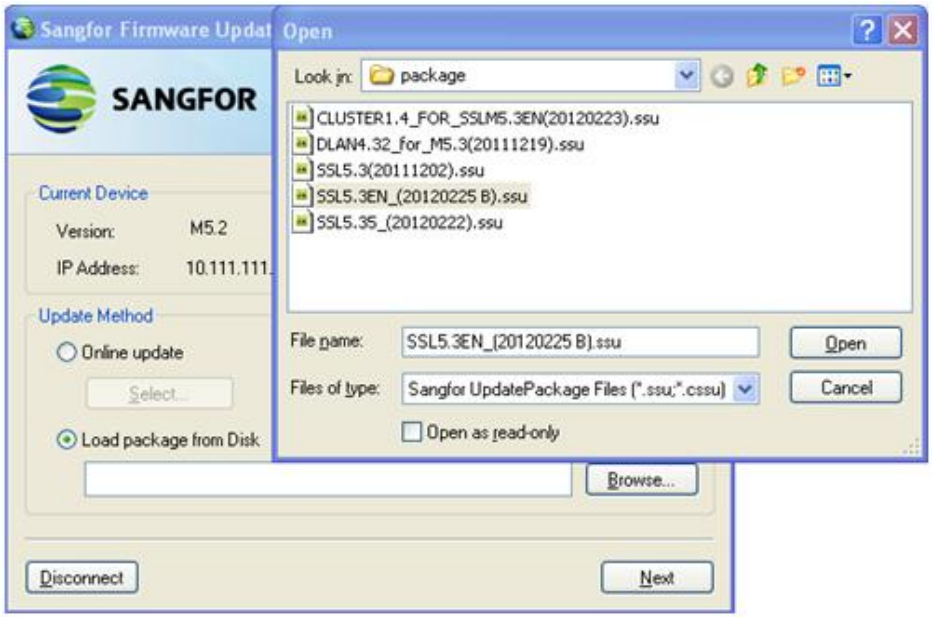
To stop downloading the package, click the **Pause** button which will then turn to a **Resume** button.

To cancel downloading the package, click the **Cancel** button.

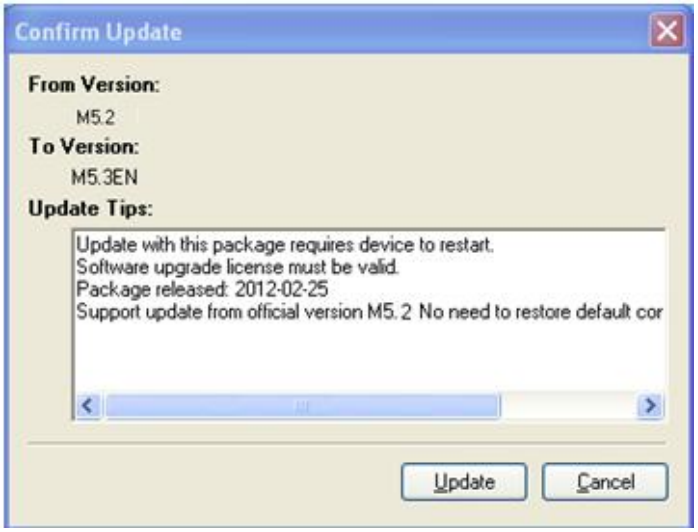
d. While package download is completed, click the **Next** button to confirm version information and update the current device, as shown in the figure below:



- Load update package. It happens when update method is **Load package from Disk**. Browse a package from local PC, click the **Open** button and **Next** button, as shown below:



6. Confirm the update information and click the **Update** button to update the current Sangfor device, as shown in the figure below:





- For online update, it is required that the computer connected to Sangfor device can access Internet.
- Please DO NOT cancel updating during the update process. Otherwise, the current device will meet unexpected error.
- Sangfor device can only be updated to a newer version from lower version. Cross-version update is not supported.
- Update operation has potential risk for misoperation will damage the device. Do not perform update by yourself. If necessary, contact Custom Service.

Appendix C: Restore Network Configuration and Password using USB drive

SANGFOR SSL support network configuration and password restore using USB drive. Create a txt file and rename the file and plug in the USB drive to SSL device to execute desired function accordingly.

Function 1: Restore network configuration by using USB drive

Function 2: Check the ETH port configuration by using USB drive

Function 3: Restore web UI admin login password by using USB drive.

Restore network configuration by using USB

1. Move/Copy **reset-network.txt** file into the USB root directory.
2. Plug in the USB drive on the SSL device, reboot the SSL device.
3. Wait until the red LED of SSL device disappear, take out USB drive.
4. Check the reset-network.log in the USB drive; If the device network configuration has been restore, the message will be shown in the log file, else, fail message will be shown in the log file.
5. Reboot the device again to ensure the new network configuration effectiveness.

Check the ETH port configuration by using USB

1. Move/Copy **show-ifconfig.txt** file into the USB root directory.

2. Plug in the USB drive on the SSL device, reboot the SSL device.

3. Wait until the red LED of SSL device disappear, take out USB drive.

4. Check the show-ifconfig.log file content to get the current ETH port configuration.

Restore Web UI admin login password by using USB

1. Move/Copy **reset-password.txt** file into the USB root directory.

2. Plug in the USB drive on the SSL device, reboot the SSL device.

3. Wait until the red LED of SSL device disappear, take out USB drive.

4. Check the reset-password.log in the USB drive; If the device password has been restore, the new password will be shown in the log file, else, fail message will be shown in the log file.

Precautions

1. All the 3 txt blank files can be created on a Windows OS platform, rename the txt file base on requirement.

2. The txt file must be located under root directory of the USB drive.

3. USB drive must be formatted into FAT32. USB drive could be single partition or multiple partitions; for multiple partitions scenario, the txt file must be located in the first partition which is FAT32 format.

4. All the functions above are mutual exclusion, support to run multiple actions at once.