SSLM6.8EN User Manual

FEB2015

Table of Contents

Declaration

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 M5.8ENuser manual includes the following chapters:

Chapter	Describe…
Chapter 1Knowing Your Sangfor Device	The product appearance, function features and performance parameters of SSL VPN M5.3EN, wiring and cautions before installation.
Chapter 2Initial Login to Admin Console	How administrator logs in to SSL VPN M5.3ENadministrator console for the first time and change initial administrator password.
Chapter 3System 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 4SSL VPN	How administrator configures SSL VPN related setting, including users, resources, roles, user authentication methods, policy sets, remote servers, endpoint security.
Chapter 6System Maintenance	Maintenance options of this SSL VPN hardware device.
Appendix A: End Users Accessing SSL VPN	How endusers 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 **Downloa**d 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	Navigate to **System**>**Network Interface** to configure

	submenu	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://data.sangfor.net/feedback.html
- **MSN, Email:***tech.support@sangfor.com.hk*
- **Tel:**+60 12711 7129 (7511)

Acknowledgements

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

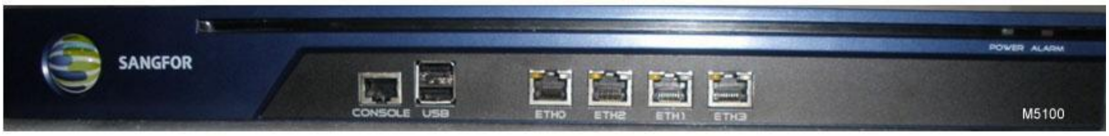
- Voltage input:110V/230V (AC, alternating current)
- Temperature:0-45℃
- Humidity: 5%-90%

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

- The power supply is well grounded
- Dustproof measures are taken
- Working environment iswell 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 countrywhere 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 turn on.

   After successful boot up, **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).

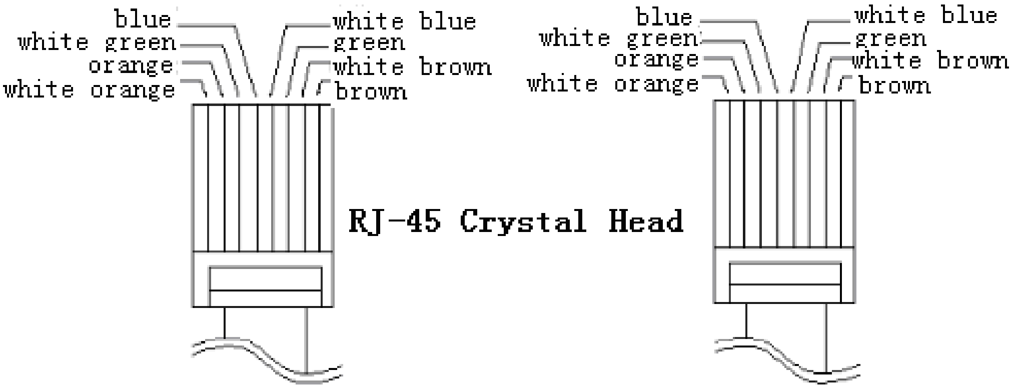
Multi-line function allows multiple Internet lines to be connected to Sangfor device. When deploy multiple lines, please connect the second Internet line to **WAN2** interface (**ETH3**) and the third Internet line to **WAN3** interface (**ETH4**), and so on.

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.

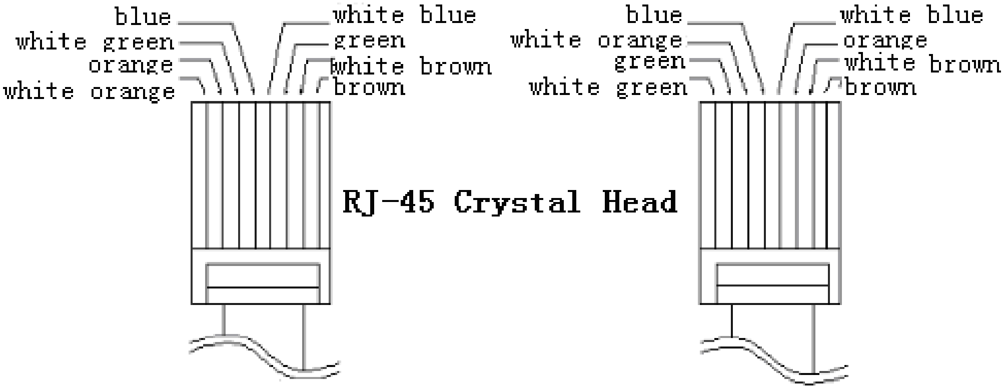
- Use crossover cable to connect **WAN** interface **(ETH2/3)** to the external network.
- Use straight-through cable to connect **LAN** interface **(ETH0)** to the internal network.
- For direct access to administrator Web console, use crossover cable to connect **LAN (ETH0)** interface to the computer.

In case, session cannot be established. However, 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

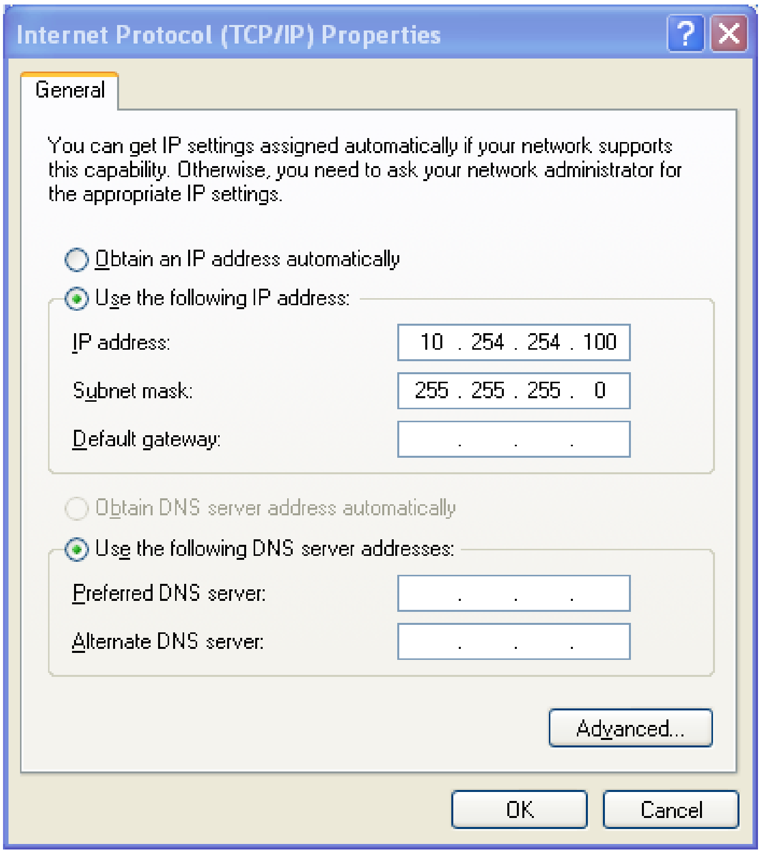
SANGFOR SSL VPN system provides Web-based administration through HTTPS port 4430. The initial URL for administrator console access is https://10.254.254.254:4430.

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:



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 254 . 254 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

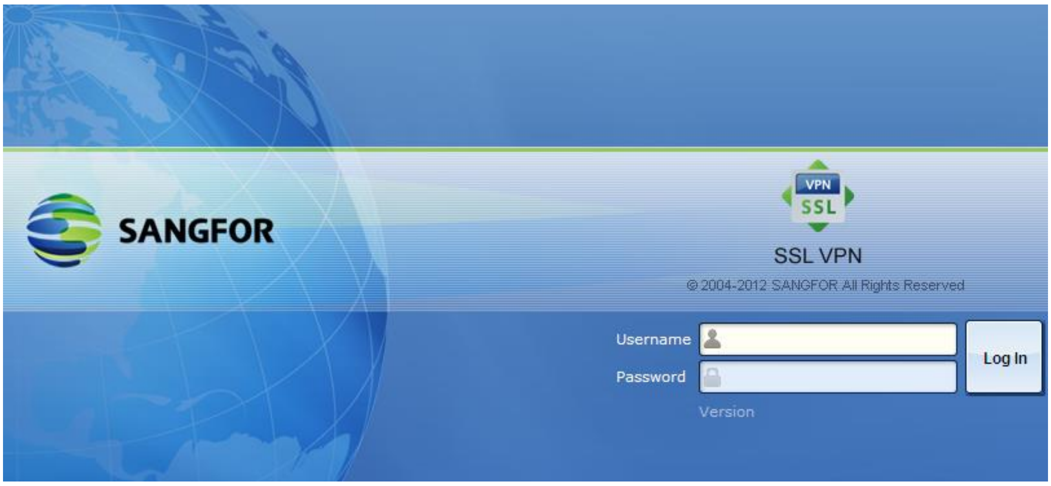
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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:



4. Enter the administrator username and password and click the **Log In** button. The default administrator username is **Admin** (case-sensitive) and password is **Admin** (case-sensitive).

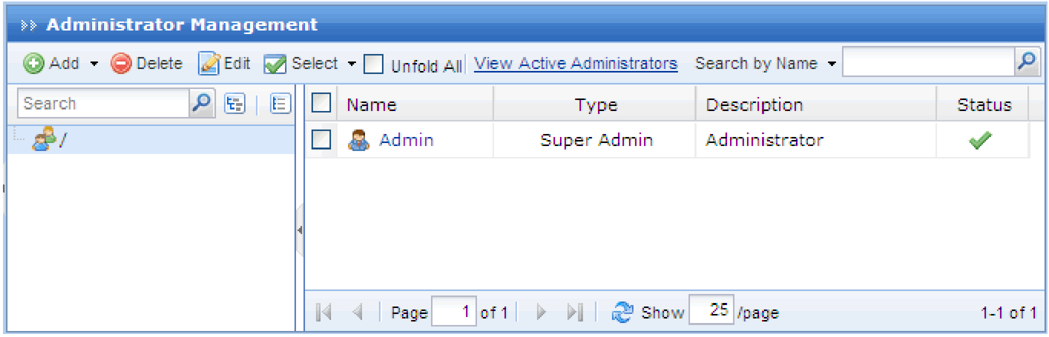
5. For version information of the software package, click on **Version** below the textboxes.

Modifying Administrator Password

We strongly recommend you to change the administrator password after initial login, 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.

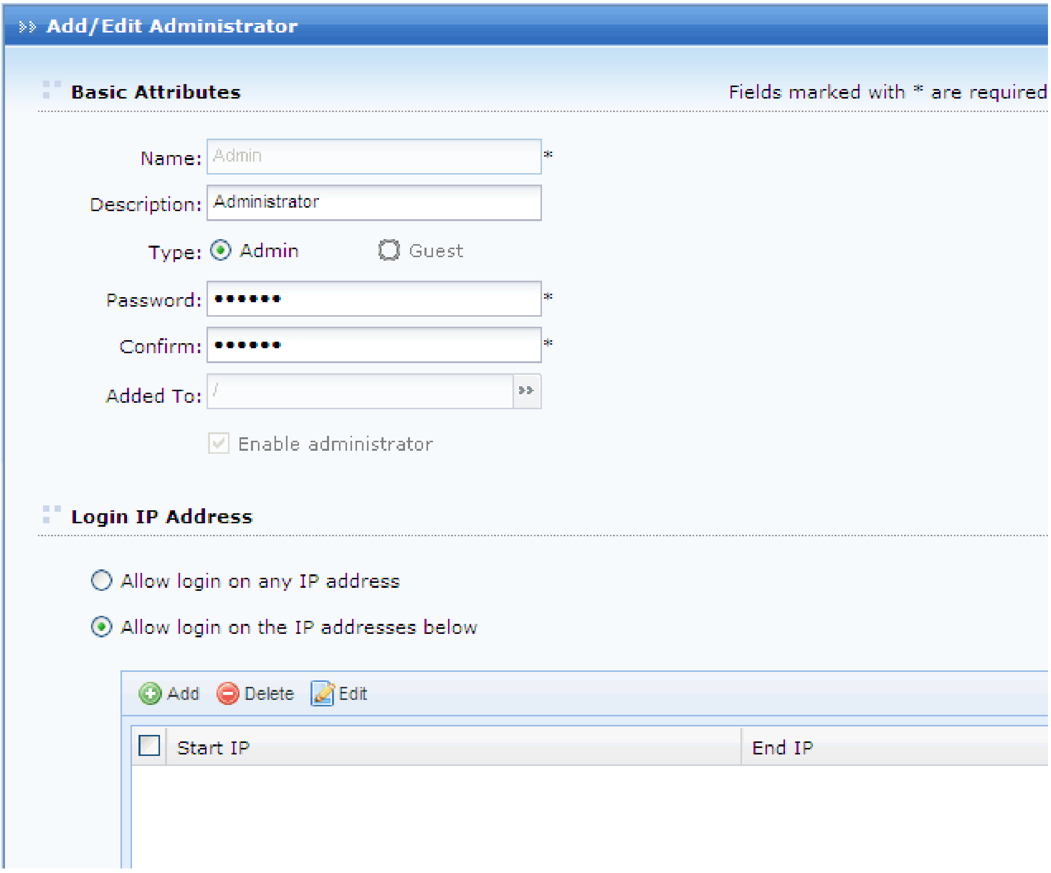
To modify default administrator password, perform the following steps:

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



□	Name	Type	Description	Status
□	Admin	Super Admin	Administrator	✓

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



Name: Admin *

Description: Administrator

Type: ● Admin ○ Guest

Password: •••••• *

Confirm: •••••• *

Added To: /

☑ Enable administrator

○ Allow login on any IP address

● Allow login on the IP addresses below

□	Start IP	End IP

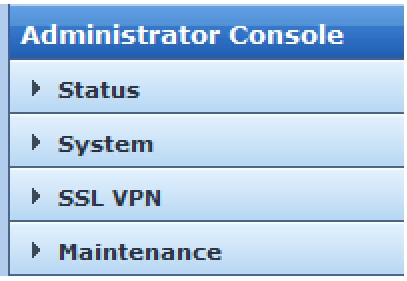
3. Modify the password and click the **Save** button on the above page.

- 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 four configuration modules in all:

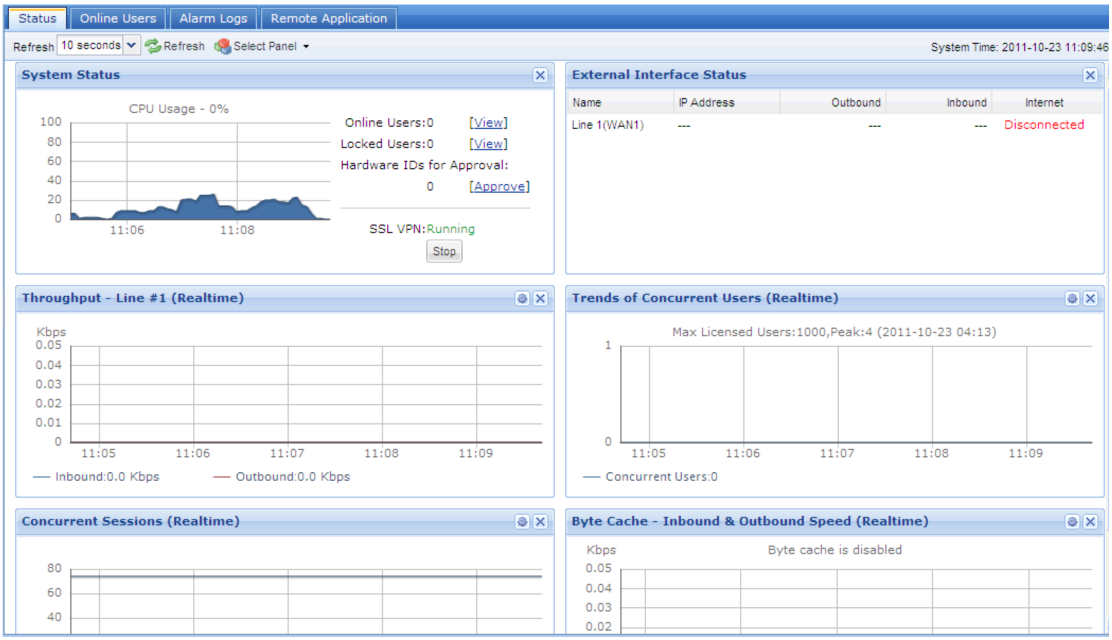


- **Status:** Shows the running status of the Sangfor device and the related modules.
- **System:** Configures the related licenses of the device, network settings and other global settings such as schedule, administrator, SSL VPN options, etc.
- **SSL VPN:** Configures the SSL VPN related settings, such as SSL VPN account, resources, roles, policy sets, remote servers and endpoint security rules and policies.
- **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**.



Refresh 10 seconds

System Time: 2011-10-23 11:09:46

Online Users:0 [View]

Locked Users:0 [View]

Hardware IDs for Approval: 0 [Approve]

SSL VPN:Running

Line 1(WAN1) --- --- --- Disconnected

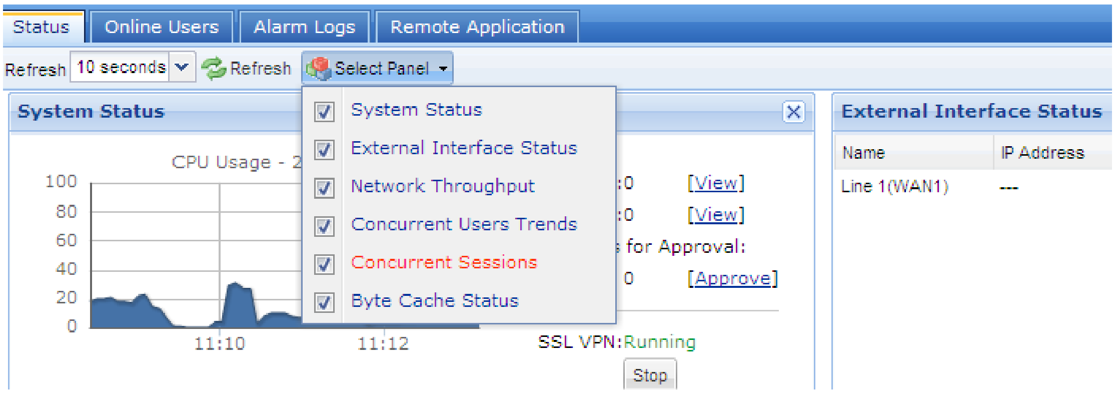
Inbound:0.0 Kbps Outbound:0.0 Kbps

Max Licensed Users:1000,Peak:4 (2011-10-23 04:13)

Concurrent Users:0

Byte cache is disabled

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:



Refresh 10 seconds

☑ System Status

☑ External Interface Status

☑ Network Throughput

☑ Concurrent Users Trends

☑ Concurrent Sessions

☑ Byte Cache Status

:0 [View]

:0 [View]

for Approval: 0 [Approve]

SSL VPN:Running

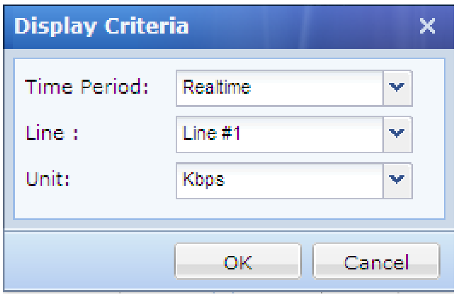
Line 1(WAN1) ---

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:



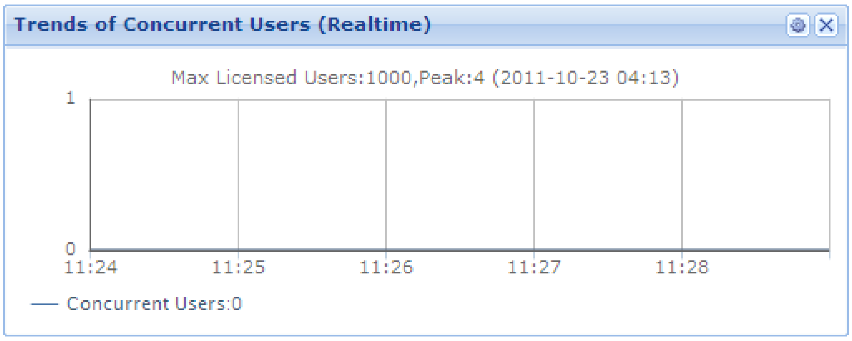
Display Criteria

Time Period: Realtime

Line : Line #1

Unit: Kbps

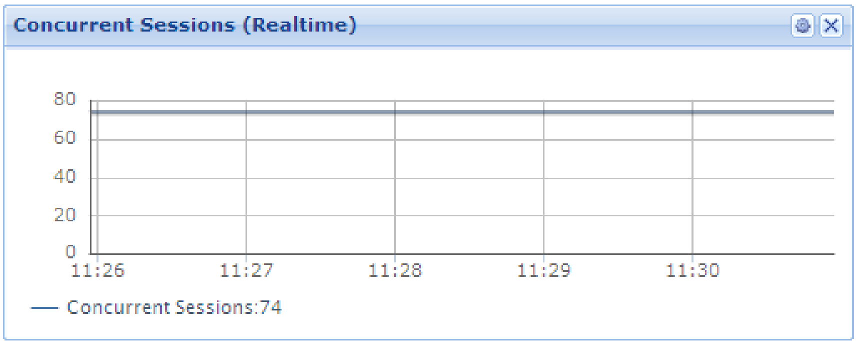
- **Trends of Concurrent Users:** This panel shows the number of users that are using SSL VPN concurrently during certain period of time, as shown below:



Trends of Concurrent Users (Realtime)
Max Licensed Users:1000,Peak:4 (2011-10-23 04:13)
1
0
11:24
11:25
11:26
11:27
11:28
Concurrent Users:0

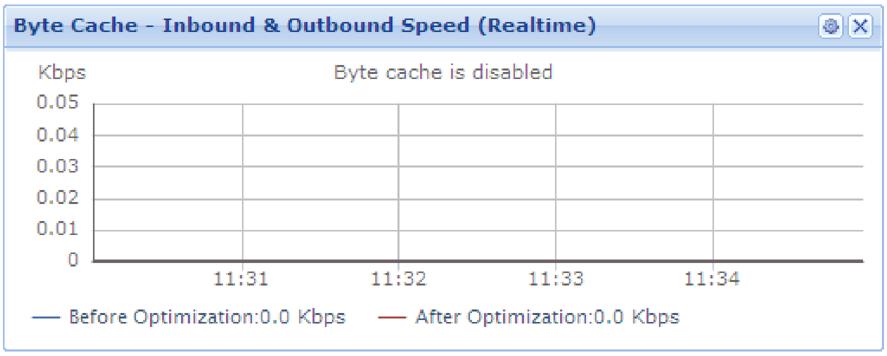
  Click the **Settings** icon ⚙ (at the upper right of the panel) to specify time period (real time, last 24 hours or last 7 days), as shown below:

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

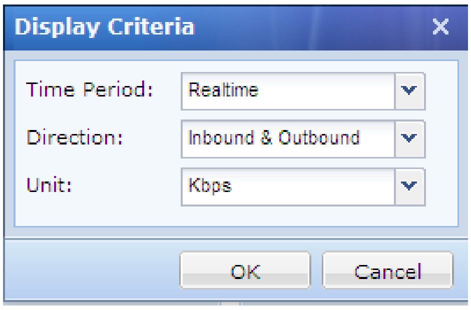


Click the **Settings** icon ⚙ (at the upper right of the panel) to specify time period (real time, last 24 hours or last 7 days).

- **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 (real time, last 24 hours or last 7 days) and direction of traffic speed (inbound & outbound, outbound or inbound), as shown below:



Time Period: Realtime

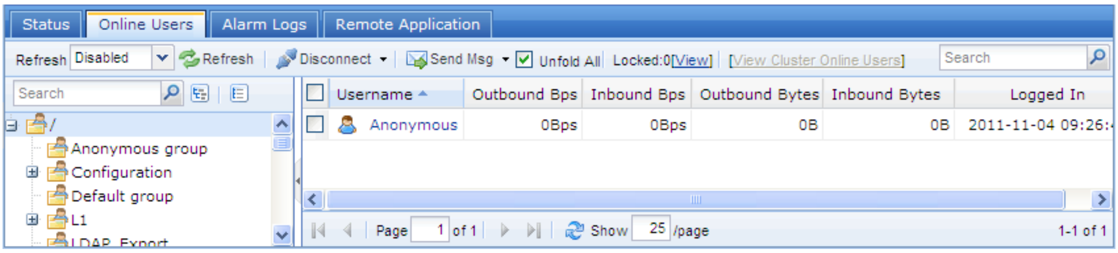
Direction: Inbound & Outbound

Unit: Kbps

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.

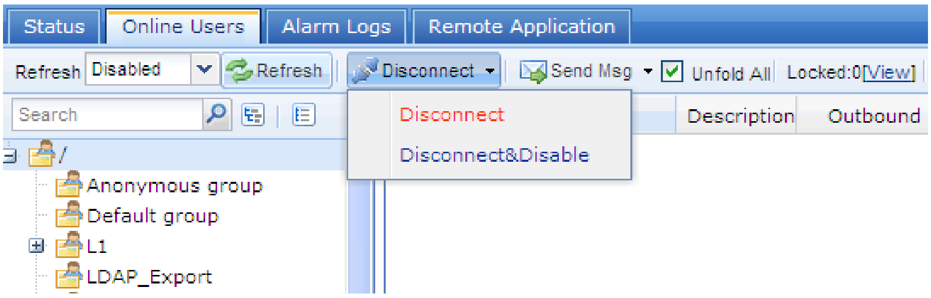
The **Online Users** page is as shown below:



□	Username	Outbound Bps	Inbound Bps	Outbound Bytes	Inbound Bytes	Logged In
□	Anonymous	0Bps	0Bps	0B	0B	2011-11-04 09:26:

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

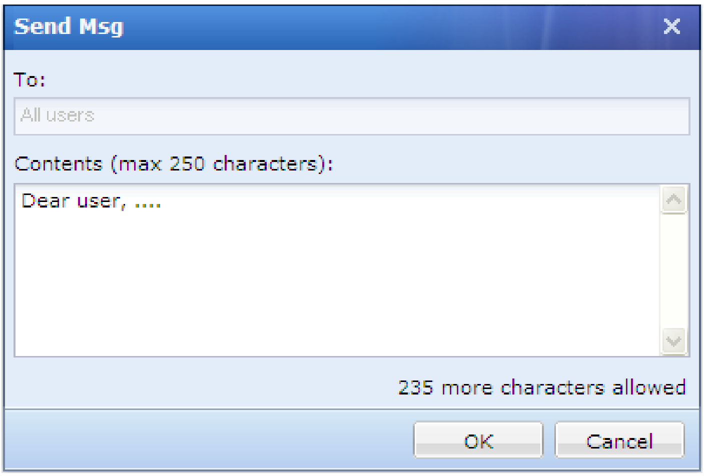
- **Auto Refresh:** Specifies the time interval for refreshing this page, or click **Refresh** to refresh the page manually and immediately.
- **Disconnect:** Click it and select an option to disconnect, or disconnect and disable the selected user(s), as shown below:



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

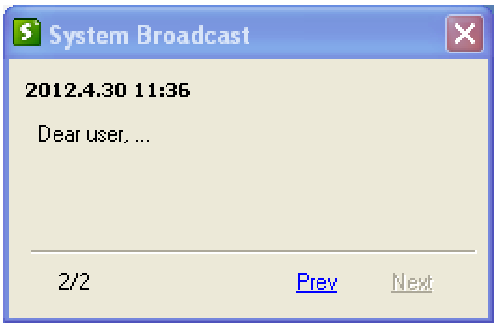
If **Disconnect & Disable** is selected and **Apply** button is clicked (on the pop-up bar at the top of the page), the selected user will be forced to disconnect with SSL VPN after are clicked and be prohibited from logging in again until it is unlocked.

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



Dear user, ...

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

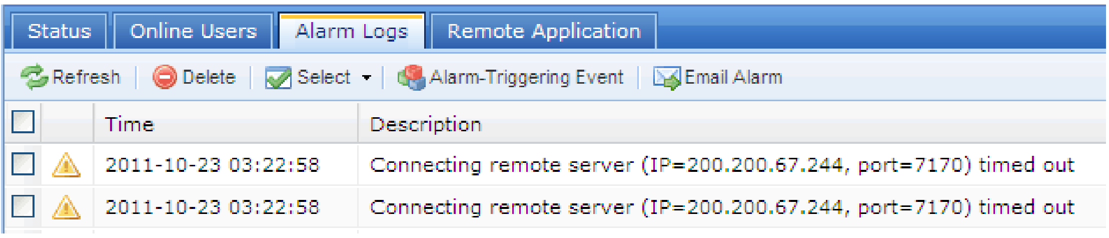


2012.4.30 11:36

Dear user, ...

Viewing Alarm Logs

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



□		Time	Description
□	⚠	2011-10-23 03:22:58	Connecting remote server (IP=200.200.67.244, port=7170) timed out
□	⚠	2011-10-23 03:22:58	Connecting remote server (IP=200.200.67.244, port=7170) timed out

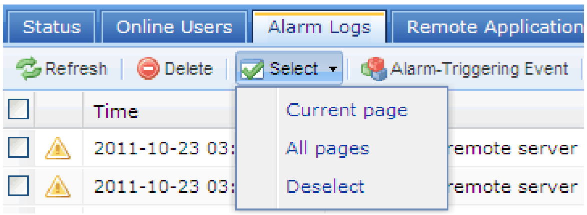
The following are the contents included on **Alarm Logs** page:

- **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**.

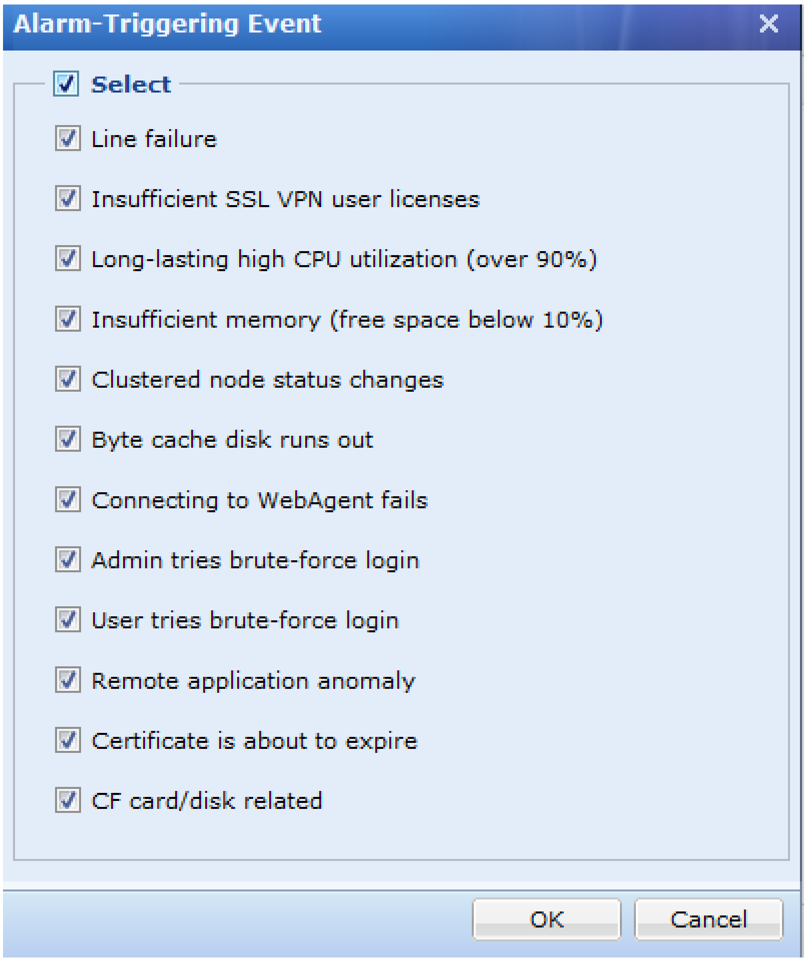
  If **Current page** option is selected, all the logs displayed on this page will be selected.

  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.



Alarm-Triggering Event

☑ Select

☑ Line failure

☑ Insufficient SSL VPN user licenses

☑ Long-lasting high CPU utilization (over 90%)

☑ Insufficient memory (free space below 10%)

☑ Clustered node status changes

☑ Byte cache disk runs out

☑ Connecting to WebAgent fails

☑ Admin tries brute-force login

☑ User tries brute-force login

☑ Remote application anomaly

☑ Certificate is about to expire

☑ CF card/disk related

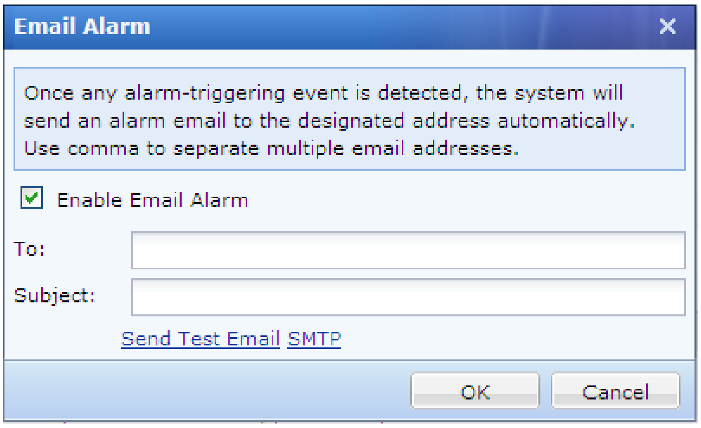
The following are the contents included on the **Alarm-Triggering Event** page:

- **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 Web Agent fails:** If the Web Agent 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 into 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 into 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:** SSL certificate expired will email an alarm event to the specified email address to notify the administrator of that.
- **CF card/disk related:** CF card or disk got error, 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).



Email Alarm

Once any alarm-triggering event is detected, the system will send an alarm email to the designated address automatically. Use comma to separate multiple email addresses.

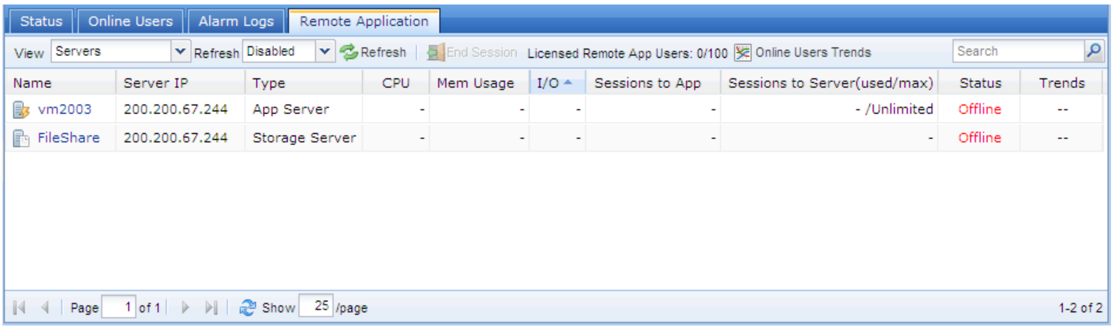
☑ Enable Email Alarm

To:

Subject:

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:



View: Servers Refresh: Disabled Licensed Remote App Users: 0/100

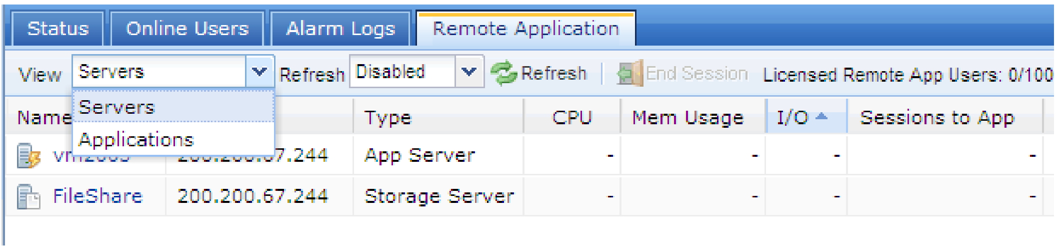
Name	Server IP	Type	CPU	Mem Usage	I/O	Sessions to App	Sessions to Server(used/max)	Status	Trends
vm2003	200.200.67.244	App Server	-	-	-	-	- /Unlimited	Offline	--
FileShare	200.200.67.244	Storage Server	-	-	-	-	-	Offline	--

Page 1 of 1 Show 25 /page 1-2 of 2

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.

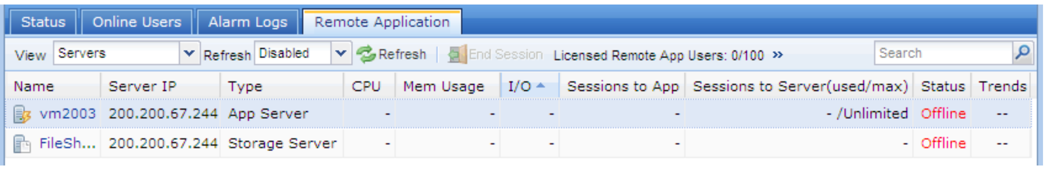
The following are the contents included on **Remote Application** page:

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



Name	Server IP	Type	CPU	Mem Usage	I/O	Sessions to App
vm2003	200.200.67.244	App Server	-	-	-	-
FileShare	200.200.67.244	Storage Server	-	-	-	-

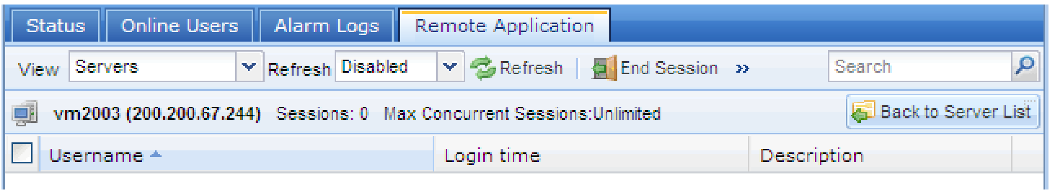
- **Servers:** Mainly offers the information of the involved servers that are providing services to VPN users. They are the servers configured in **SSL VPN**>**Remote Servers.** The page is as shown below:



View: Servers Refresh: Disabled Licensed Remote App Users: 0/100

Name	Server IP	Type	CPU	Mem Usage	I/O	Sessions to App	Sessions to Server(used/max)	Status	Trends
vm2003	200.200.67.244	App Server	-	-	-	-	- /Unlimited	Offline	--
FileSh...	200.200.67.244	Storage Server	-	-	-	-	-	Offline	--

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:



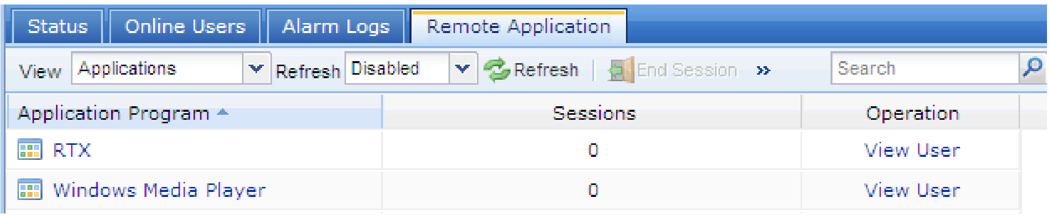
View: Servers Refresh: Disabled

vm2003 (200.200.67.244) Sessions: 0 Max Concurrent Sessions:Unlimited

□	Username	Login time	Description

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.

- **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:

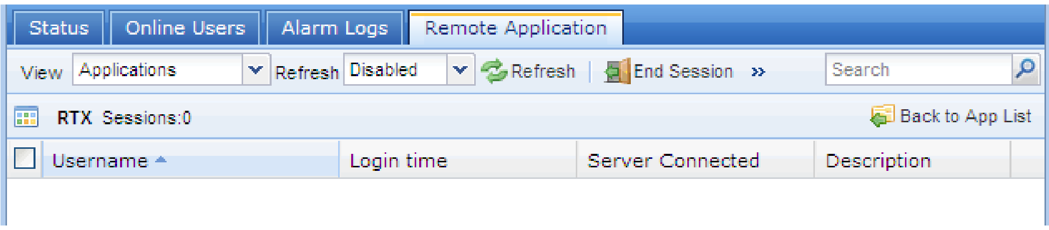


View: Applications

Refresh: Disabled

Application Program	Sessions	Operation
RTX	0	View User
Windows Media Player	0	View User

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



View: Applications

Refresh: Disabled

RTX Sessions:0

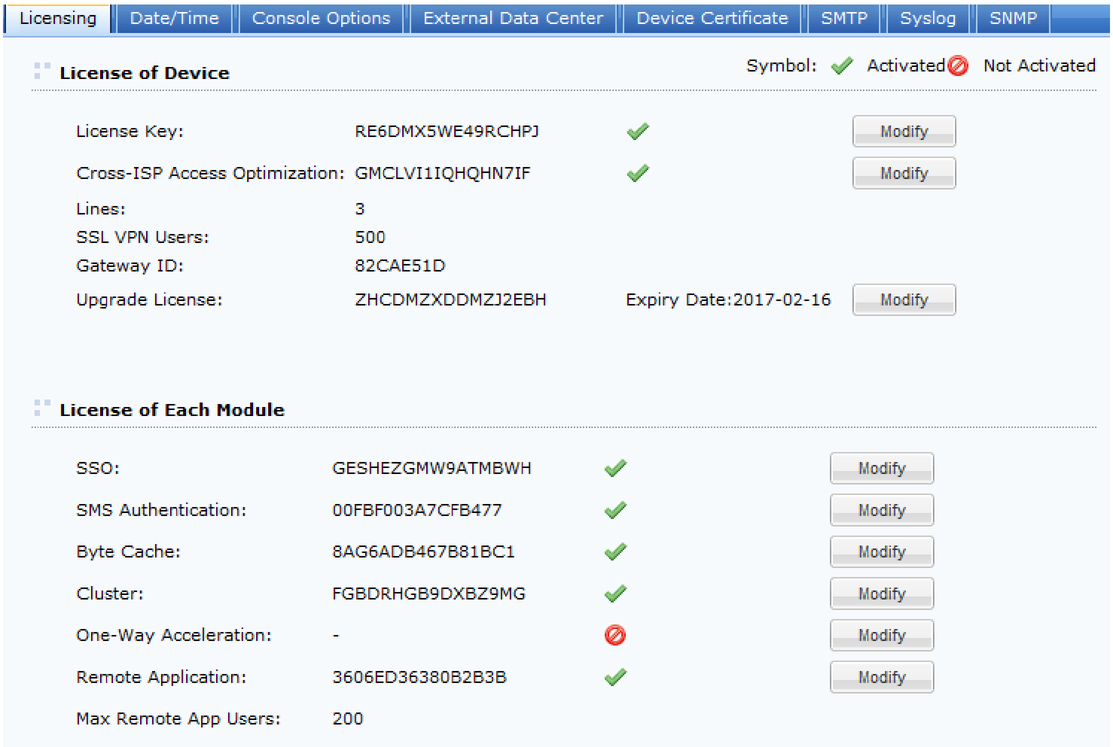
□	Username	Login time	Server Connected	Description

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 five pages are seen, namely, **Licensing**, **Date/Time**, **Console Options**, **External Data Center**, **Device Certificate, SMTP**, **Syslog** and **SNMP**, as shown below:



License of Device

Symbol: ✓ Activated ⊘ Not Activated

License Key:	RE6DMX5WE49RCHPJ	✓
Cross-ISP Access Optimization:	GMCLVI1IQHQHN7IF	✓
Lines:	3	
SSL VPN Users:	500	
Gateway ID:	82CAE51D	
Upgrade License:	ZHCDMZXDDMZJ2EBH	Expiry Date:2017-02-16

License of Each Module

SSO:	GESHEZGMW9ATMBWH	✓
SMS Authentication:	00FBF003A7CFB477	✓
Byte Cache:	8AG6ADB467B81BC1	✓
Cluster:	FGBDRHGB9DXBZ9MG	✓
One-Way Acceleration:	-	⊘
Remote Application:	3606ED36380B2B3B	✓
Max Remote App Users:	200	

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 function modules 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.).

- **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 priorto this date you can update this device to keep the software version up-to-date.
- **Device License:** 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.

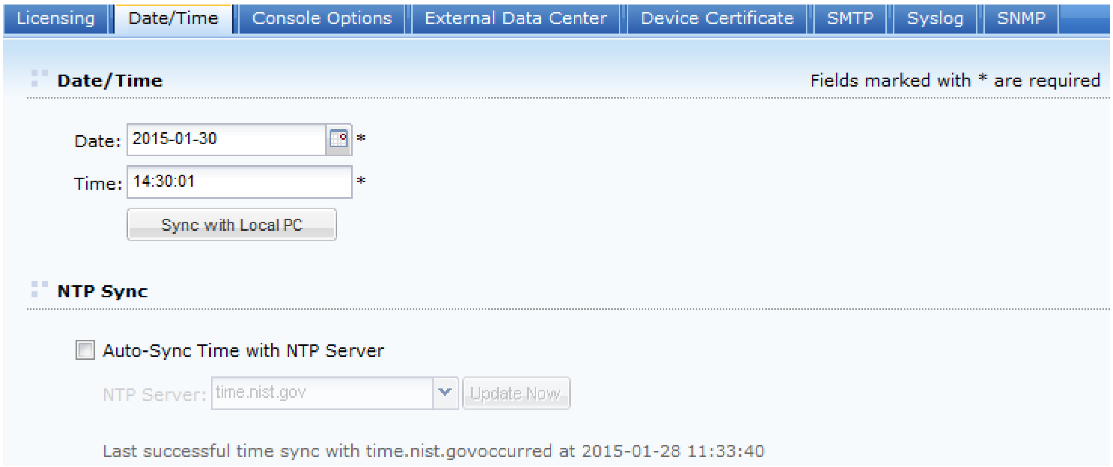
Mobile Sangfor VPN Users indicates the number of mobile users of Sangfor VPN (using the PDLAN client software). This number plus the number of SSL VPN users equals to the total number of VPN users (which decided by the license of the Sangfor device you have purchased from SANGFOR).

- **SSO:** With this license, Single Sign-On (SSO) 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.
- **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.
- **Secure Desktop:** This license makes **Secure Desktop** feature available. If **Secure Desktop** is enabled, users’ access could be strictly restricted and consequently data related to the visited resources will not be disclosed.
- **One-Way Acceleration**: This license is allow optimize transfer rate in high-latency and high packet loss network.
- **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.

Modifying System Date and Time

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



Date/Time Fields marked with * are required

Date: 2015-01-30 *

Time: 14:30:01 *

NTP Sync

□ Auto-Sync Time with NTP Server

NTP Server: time.nist.gov

Last successful time sync with time.nist.govoccurred at 2015-01-28 11:33:40

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:** Click this button to synchronize the date and time of the Sangfor device with your computer.

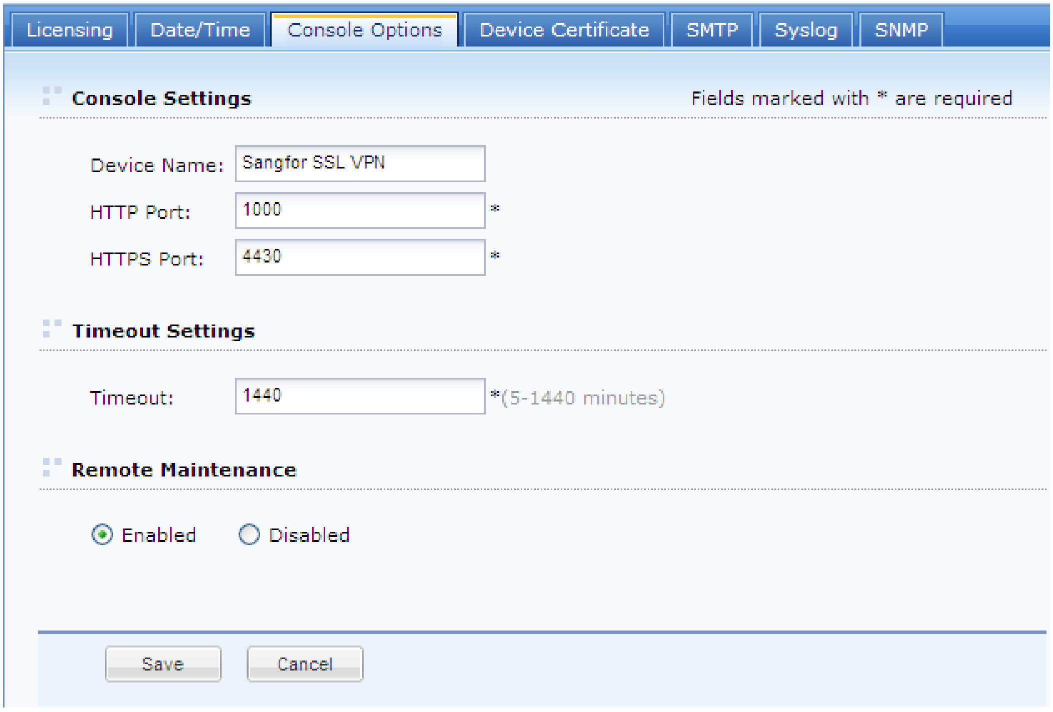
3. Click the **Save** button to save the settings, or click the **Cance**l button not to save the changes.

⚠

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:



Console Settings

Fields marked with * are required

Device Name: Sangfor SSL VPN

HTTP Port: 1000 *

HTTPS Port: 4430 *

Timeout Settings

Timeout: 1440 *(5-1440 minutes)

Remote Maintenance

● Enabled ○ Disabled

2. Configure the following:

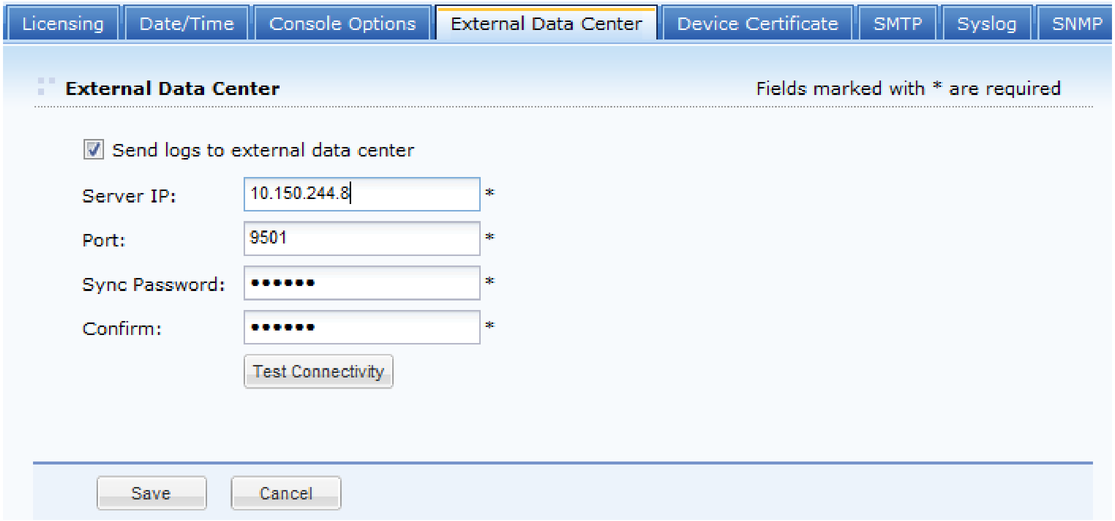
   - **Device Name:** Specifies the name of the Sangfor device, which helps to distinguish it from other clustered nodes if this device joins cluster. Elaborate
   - **HTTP Port:** Specifies the HTTP port used for logging into this Sangfor device. The defaults 1000.
   - **HTTPS Port:** Specifies the HTTPS port used for logging into this Sangfor device. The defaults 4430.
   - **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.

External Data Center

External Data Center is for generation system logs, user logs, management logs, alarm logs synchronize to External Data Center.

1. Navigate to **System**>**System**>**External Data Center** to enter External Data Center page, as shown below:



External Data Center

Fields marked with * are required

☑ Send logs to external data center

Server IP: 10.150.244.8 *

Port: 9501 *

Sync Password: •••••• *

Confirm: •••••• *

2. Configure the following:

- **External Data Center**: check the box “send logs to external data center “

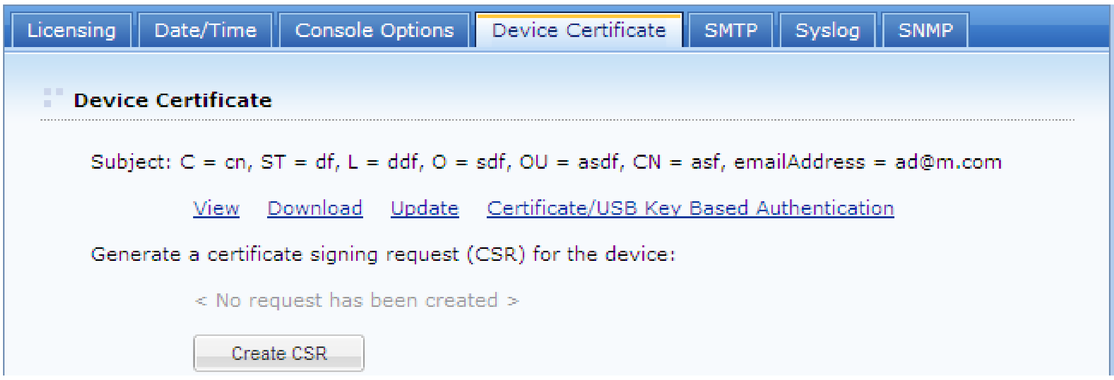
- **Server IP**: Specifies the IP Address for external data center

- **Port**: Specifies the port of external data center. The default is 9501

- **Sync Password**: Specified password login of the external data center, device and server must be same

Generating Certificate for Sangfor Device

Device certificate is intended for establishing sessions between the Sangfor device and client. 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:



Device Certificate

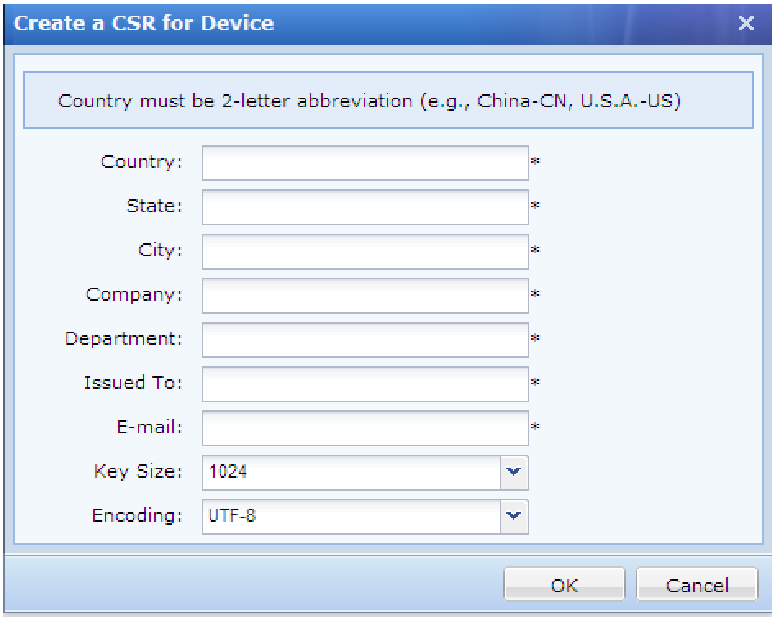
Subject: C = cn, ST = df, L = ddf, O = sdf, OU = asdf, CN = asf, emailAddress = ad@m.com

Generate a certificate signing request (CSR) for the device:

< No request has been created >

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 sectioning Chapter 4).
- **Create CSR:** Click this button to generate a certificate-signing request (CSR) which should be sent to the external CA to generate the device certificate. For more details, please refer to Scenario 17: Using External CA Root Certificate to Generate Device Certificate in Chapter 4.



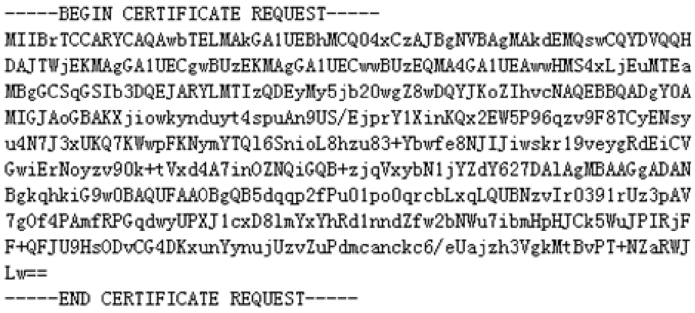
Create a CSR for Device

Country must be 2-letter abbreviation (e.g., China-CN, U.S.A.-US)

Country: *
State: *
City: *
Company: *
Department: *
Issued To: *
E-mail: *
Key Size: 1024
Encoding: UTF-8

Configure the required fields and then click the **OK** button.

Once the certificate signing request is generated, click the **Download** Link to download the request.The contents of the downloaded request file are as shown below:

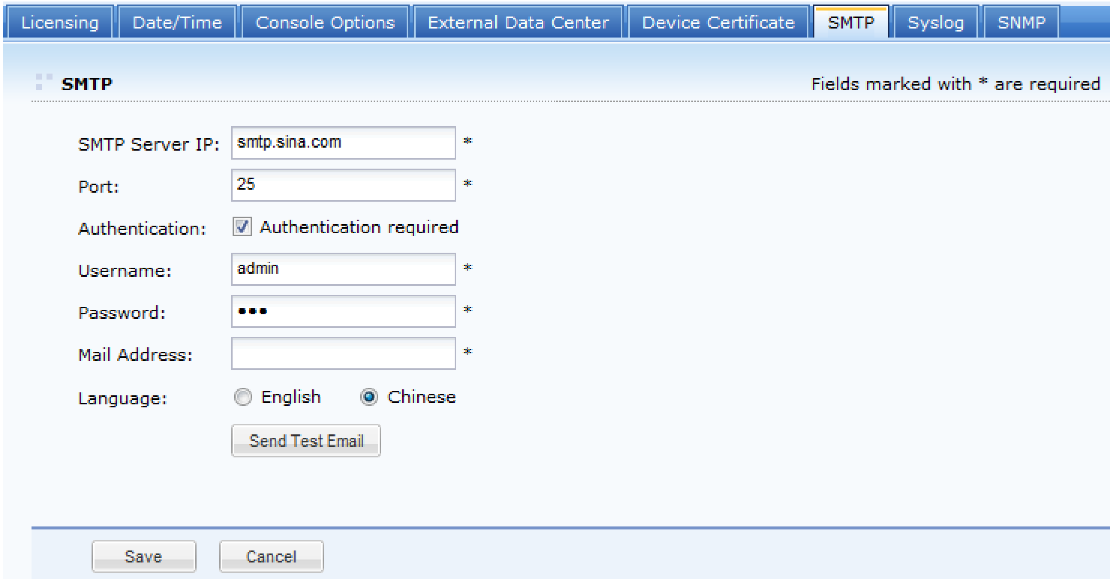


```
-----BEGIN CERTIFICATE REQUEST-----
MIIBrTCCARYCAQAwbTELMAkGA1UEBhMCQ04xCzAJBgNVBAgMAkdEMQswCQYDVQQH
DAJTWjEKMAgGA1UECgwBUzEKMAgGA1UECwwBUzEQMA4GA1UEAwwHMS4xLjEuMTEa
MBgGCSqGSIb3DQEJARYLMTIzQDEyMy5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAKXjiowkynduyt4spuAn9US/EjprY1XinKQx2EW5P96qzv9F8TCyENsy
u4N7J3xUKQ7KWwpFKNymYTQ16SnioL8hzu83+Ybwfe8NJIJiwskr19veygRdEiCV
GwiErNoyzv90k+tVxd4A7inOZNQiGQB+zjqVxybN1jYZdY627DAlAgMBAAGgADAN
BgkqhkiG9w0BAQUFAAOBgQB5dqqp2fPu01po0qrcbLxqLQUBNzvIr0391rUz3pAV
7g0f4PAmfRPGqdwyUPXJ1cxD8lmYxYhRd1nndZfw2bNWu7ibmHpHJCk5WuJPIRjF
F+QFJU9HsODvCG4DKxunYynujUzvZuPdmcanckc6/eUajzh3VgkMtBvPT+NZaRWJ
Lw==
-----END CERTIFICATE REQUEST-----
```

- **Update:** Click it to import the new external-CA-issued device certificate into the Sangfor device to replace the old one.

ConfiguringSMTP Server

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



SMTP

Fields marked with * are required

SMTP Server IP: smtp.sina.com *

Port: 25 *

Authentication: ☑ Authentication required

Username: admin *

Password: ••• *

Mail Address: *

Language: ○ English ● Chinese

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 configures **Username** and **Password**, if this SMTP server requires identity verification.
- **Mail Address:** Fill in the e-email address to send email
- **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.

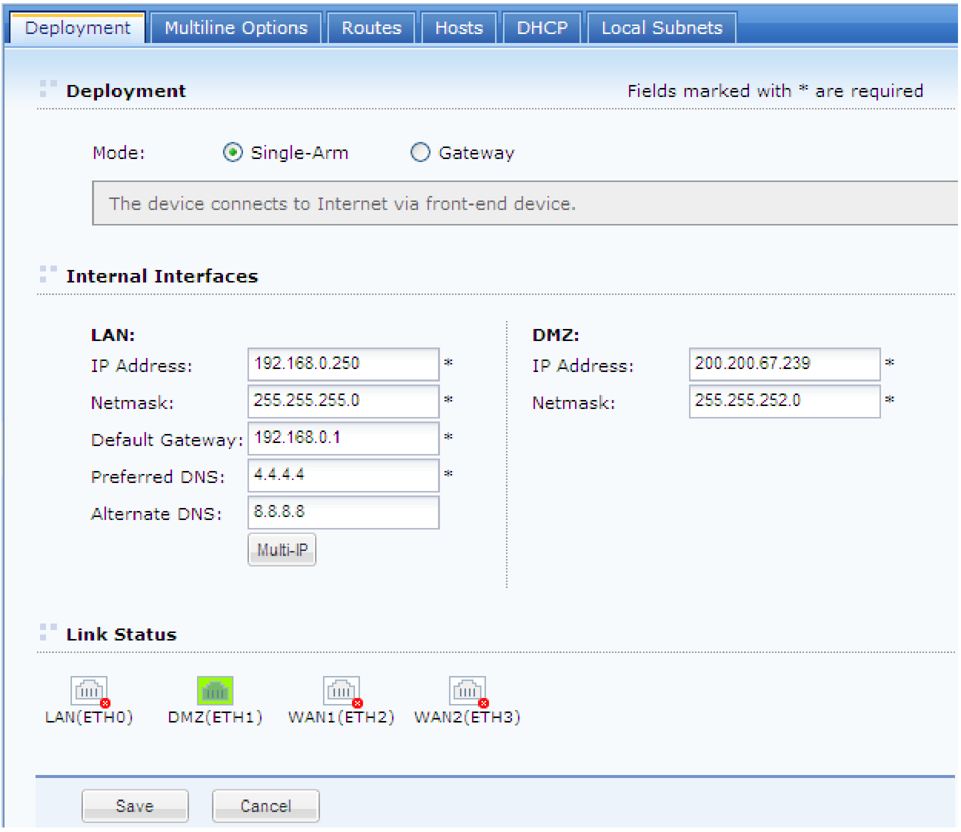
3. Click **Save** to save the settings on this page; otherwise, click **Cancel**.

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:



Deployment

Fields marked with * are required

Mode: ● Single-Arm ○ Gateway

The device connects to Internet via front-end device.

Internal Interfaces

LAN:

IP Address: 192.168.0.250 *

Netmask: 255.255.255.0 *

Default Gateway: 192.168.0.1 *

Preferred DNS: 4.4.4.4 *

Alternate DNS: 8.8.8.8

DMZ:

IP Address: 200.200.67.239 *

Netmask: 255.255.252.0 *

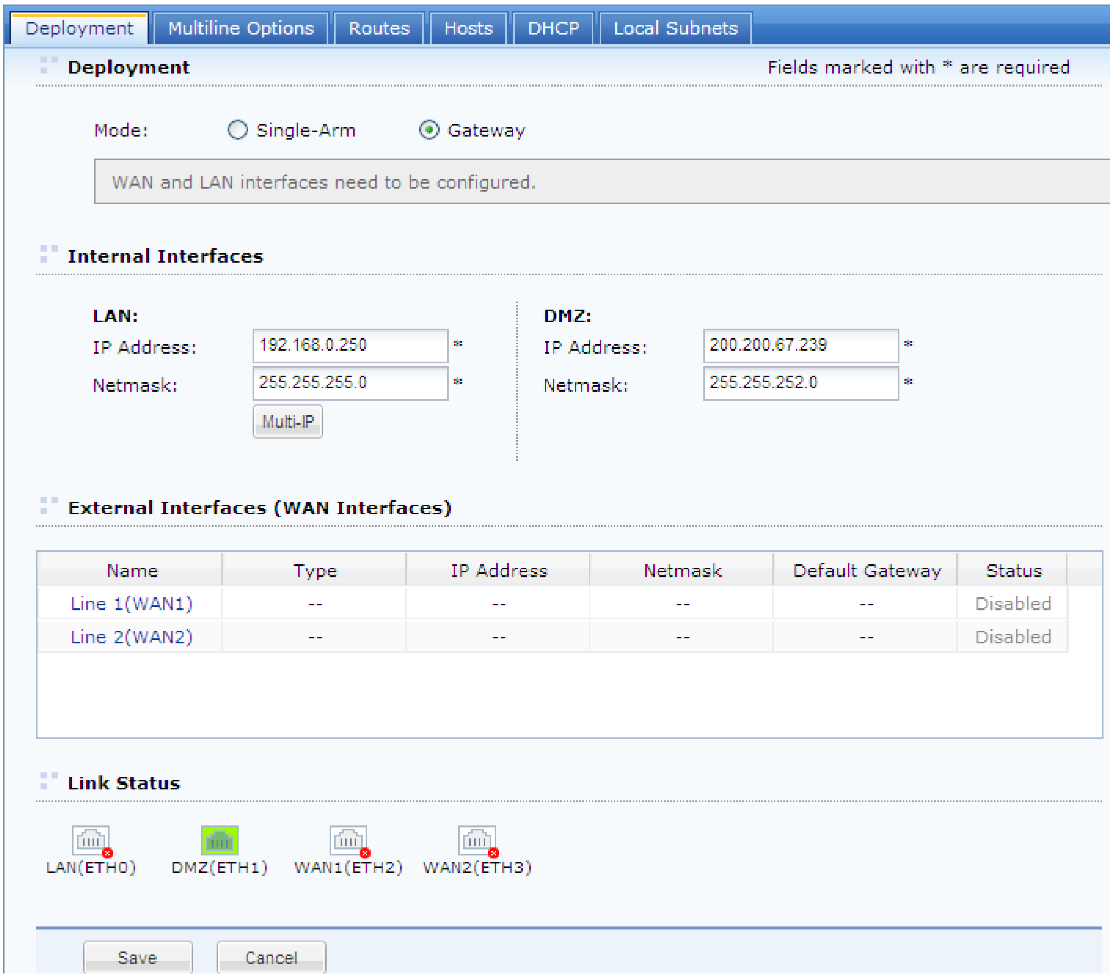
Link Status

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:



Deployment Fields marked with * are required

Mode: ○ Single-Arm ● Gateway

WAN and LAN interfaces need to be configured.

Internal Interfaces

LAN:
IP Address: 192.168.0.250 *
Netmask: 255.255.255.0 *

DMZ:
IP Address: 200.200.67.239 *
Netmask: 255.255.252.0 *

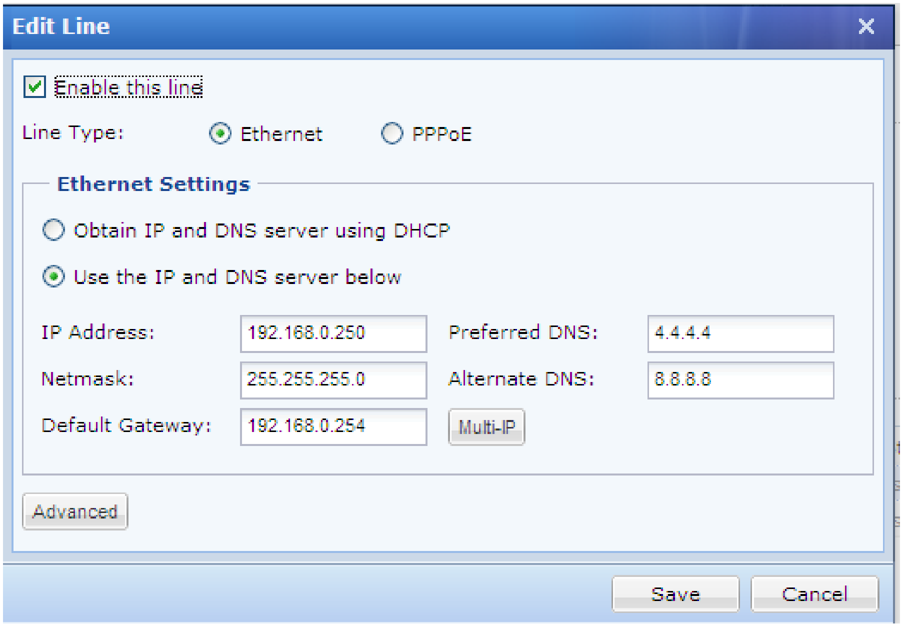
External Interfaces (WAN Interfaces)

Name	Type	IP Address	Netmask	Default Gateway	Status
Line 1(WAN1)	--	--	--	--	Disabled
Line 2(WAN2)	--	--	--	--	Disabled

Link Status

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:



Edit Line

☑ Enable this line

Line Type: ● Ethernet ○ PPPoE

Ethernet Settings

○ Obtain IP and DNS server using DHCP

● Use the IP and DNS server below

IP Address: 192.168.0.250

Netmask: 255.255.255.0

Default Gateway: 192.168.0.254

Preferred DNS: 4.4.4.4

Alternate DNS: 8.8.8.8

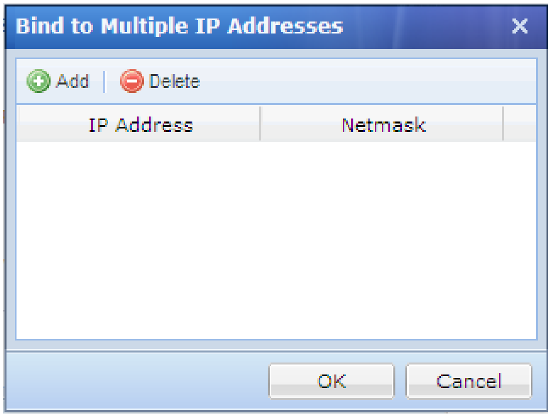
The following are the contents included on the **Edit Line** page, when line type is **Ethernet**:

- **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 they 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:



Bind to Multiple IP Addresses

IP Address	Netmask

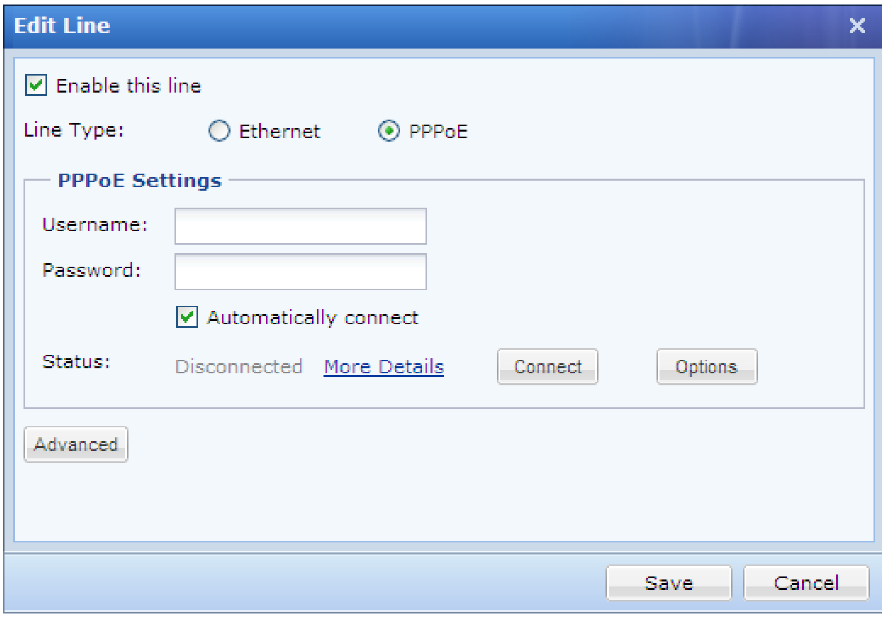
To add a new IP address entry, click **Add**.

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

⚠

The IP address added should reside in the same network segment as that of the WAN interface IP address, directing to a same gateway. Otherwise, it will turn out to be invalid for this Internet line.

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



Edit Line

☑ Enable this line

Line Type: ○ Ethernet ● PPPoE

PPPoE Settings

Username:

Password:

☑ Automatically connect

Status: Disconnected More Details

- **Username, Password:** Configure the ADSL account to get dial up 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 dial up, click **More Details**.
- **Options:** Click this button to enter the **PPPoE Properties** page and configure the parameters for dial up, such as handshake time, timeout, and max tries. Defaults are recommended to be adopted.

Scenario 1: Deploying Device in Gateway Mode

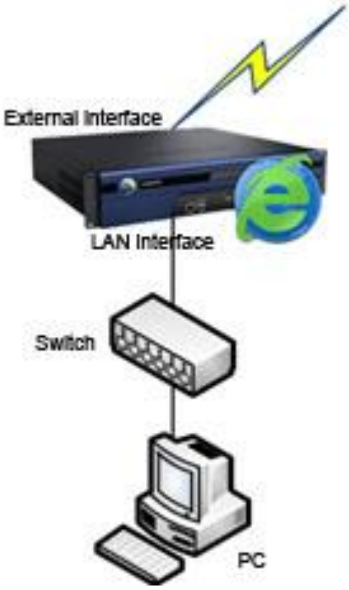
Background:

- 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 10.1.1.254.

Perform the following steps:

1. Deploy and connect the related devices as shown in the figure below:



2. Log in to the administrator console (for detailed guide, refer to the Logging in to Admin Consolesectioning Chapter 2).
3. Configure network interfaces of the device (for detailed guide, refer to the Device Deploymentsectioning Chapter 3).

If there are multiple Internet lines (which should be authorized), perform the steps followed to continue to configure the other line(s).

4. Configure the second Internet, its IP address, net mask, default gateway, DNS server, etc. (for detailed guide, refer to the Device Deployment sectioning Chapter 3).
5. Configure multi-line options (for detailed guide, refer to the Setting Multiline Options sectioning Chapter 3).
6. Click the **Save** button to save the settings and restart the Sangfor device.

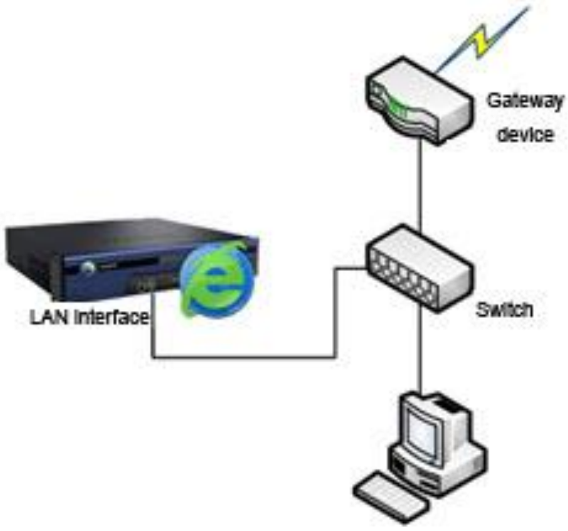
Scenario 2: Deploying Device in Single-Arm Mode

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 networks through an Internet line

Perform the following steps:

1. Deploy and connect the related devices, as shown in the figure below:



2. Log in to the administrator console (for detailed guide, refer to the Logging in to Admin Consolesectioning Chapter 2).
3. Go to **System**>**Network**>**Deployment** page and configure the network interfaces of the device (for detailed guide, refer to the Device Deployment section in Chapter 3).
4. Click the **Save** button to save the settings and restart the Sangfor device.
5. Configure the front-end firewall, and make sure that the corresponding ports (80 and 443 by default) of the front-end firewall are mapped to those on the Sangfor device.

If the front-end device is connected to two Internet lines, enable the multi-line policy of SSL VPN and configure the second line by performing the following two steps.

6. Go to **System**>**Network**>**Multiline Options** page. Select the option **Allow SSL VPN to Use Multiple Lines** and select **SSL VPN users connect in via front-end device (local device owns no public IP address)**, and then add the two Internet lines into the line list and click the **Save** button to save the settings.

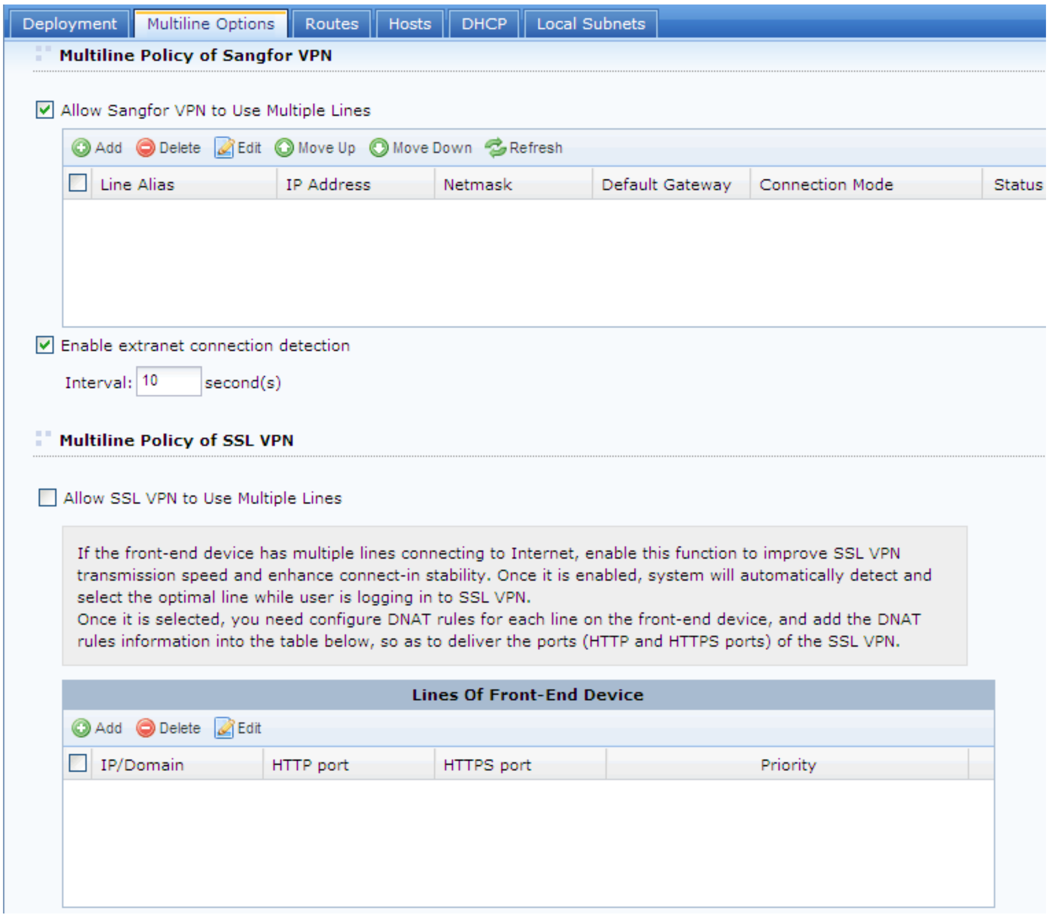
7. Configure the front-end firewall again, so that the two ports (TCP 80 and 443) of the public network IP addresses (of the second Internet line) can be mapped to the Sangfor device.

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** Pages as shown below, when deployment mode is **Single-arm**:



Multiline Policy of Sangfor VPN

☑ Allow Sangfor VPN to Use Multiple Lines

□	Line Alias	IP Address	Netmask	Default Gateway	Connection Mode	Status

☑ Enable extranet connection detection

Interval: 10 second(s)

Multiline Policy of SSL VPN

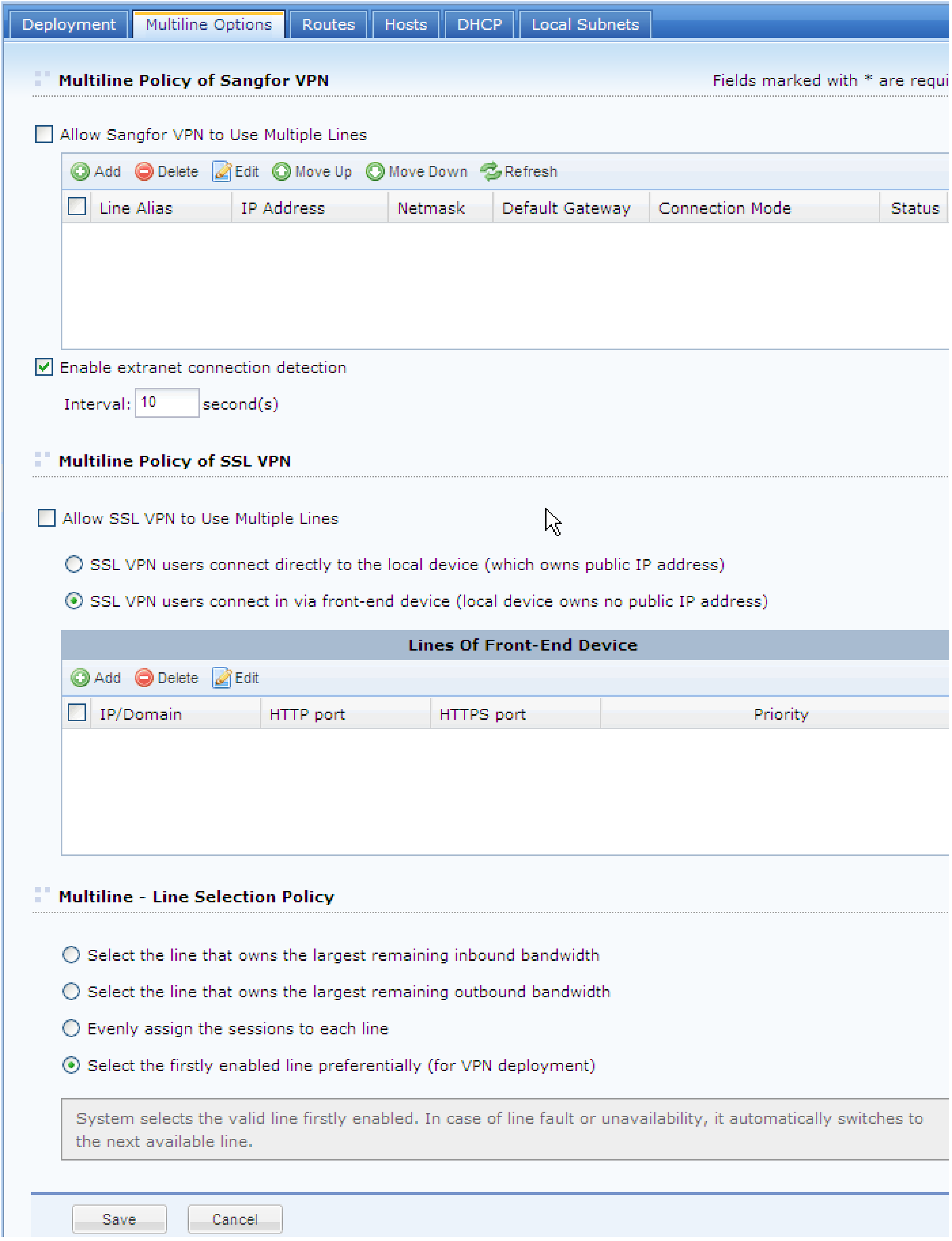
□ Allow SSL VPN to Use Multiple Lines

If the front-end device has multiple lines connecting to Internet, enable this function to improve SSL VPN transmission speed and enhance connect-in stability. Once it is enabled, system will automatically detect and select the optimal line while user is logging in to SSL VPN.
Once it is selected, you need configure DNAT rules for each line on the front-end device, and add the DNAT rules information into the table below, so as to deliver the ports (HTTP and HTTPS ports) of the SSL VPN.

Lines Of Front-End Device

□	IP/Domain	HTTP port	HTTPS port	Priority

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



Multiline Policy of Sangfor VPN Fields marked with * are requi

□ Allow Sangfor VPN to Use Multiple Lines

□	Line Alias	IP Address	Netmask	Default Gateway	Connection Mode	Status

☑ Enable extranet connection detection

Interval: 10 second(s)

Multiline Policy of SSL VPN

□ Allow SSL VPN to Use Multiple Lines

○ SSL VPN users connect directly to the local device (which owns public IP address)

● SSL VPN users connect in via front-end device (local device owns no public IP address)

Lines Of Front-End Device

□	IP/Domain	HTTP port	HTTPS port	Priority

Multiline - Line Selection Policy

○ Select the line that owns the largest remaining inbound bandwidth

○ Select the line that owns the largest remaining outbound bandwidth

○ Evenly assign the sessions to each line

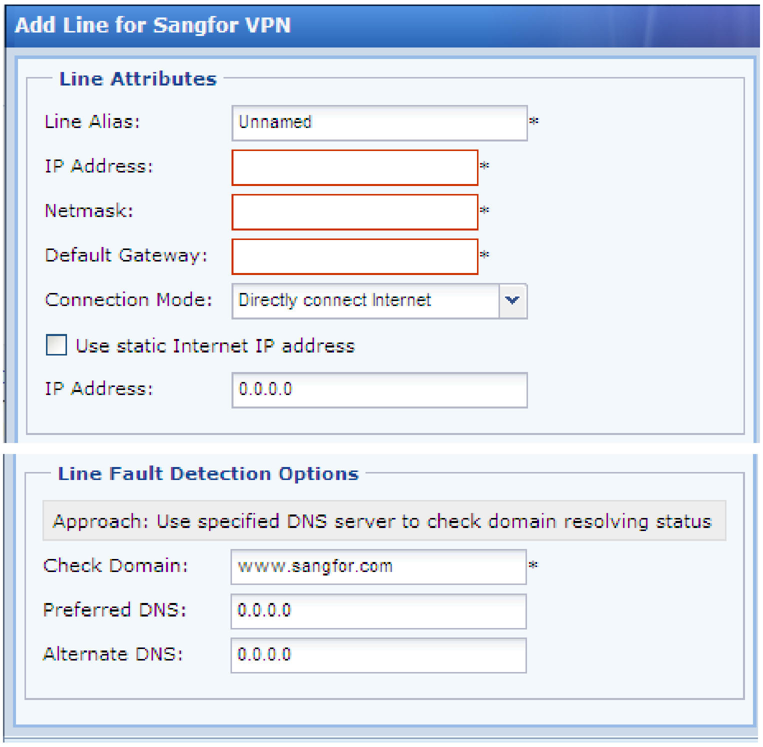
● Select the firstly enabled line preferentially (for VPN deployment)

System selects the valid line firstly enabled. In case of line fault or unavailability, it automatically switches to the next available line.

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

- **Allow Sangfor VPN to Use Multiple Lines:** Select this option under **Multiline Policy of Sangfor VPN**, the configured Internet lines will be availbe 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**:



Add Line for Sangfor VPN

Line Attributes

Line Alias: Unnamed *

IP Address: *

Netmask: *

Default Gateway: *

Connection Mode: Directly connect Internet

□ Use static Internet IP address

IP Address: 0.0.0.0

Line Fault Detection Options

Approach: Use specified DNS server to check domain resolving status

Check Domain: www.sangfor.com *

Preferred DNS: 0.0.0.0

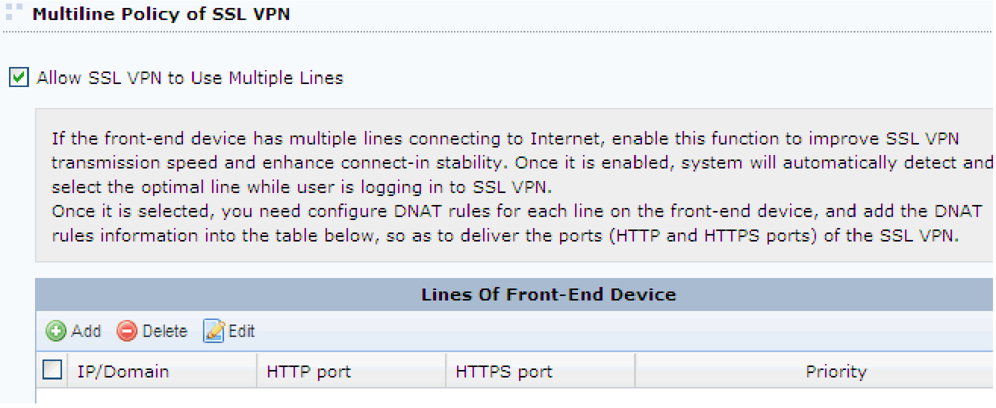
Alternate DNS: 0.0.0.0

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 extra net 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:



Multiline Policy of SSL VPN

☑ Allow SSL VPN to Use Multiple Lines

If the front-end device has multiple lines connecting to Internet, enable this function to improve SSL VPN transmission speed and enhance connect-in stability. Once it is enabled, system will automatically detect and select the optimal line while user is logging in to SSL VPN.
Once it is selected, you need configure DNAT rules for each line on the front-end device, and add the DNAT rules information into the table below, so as to deliver the ports (HTTP and HTTPS ports) of the SSL VPN.

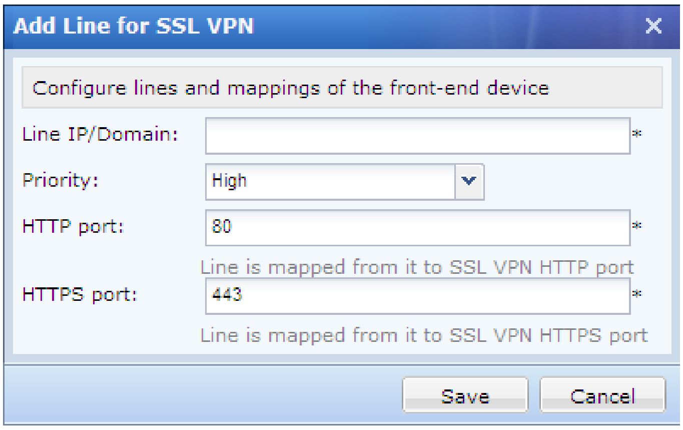
Lines Of Front-End Device

□	IP/Domain	HTTP port	HTTPS port	Priority

Once multiline policy of SSL VPN is enabled, theline selection policywillhelp 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.

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.

- If the Sangfor device is deployed in **Single-arm** mode and needs to use multiple Internet lines, map the 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:



Add Line for SSL VPN

Configure lines and mappings of the front-end device

Line IP/Domain: *

Priority: High

HTTP port: 80 *

Line is mapped from it to SSL VPN HTTP port

HTTPS port: 443 *

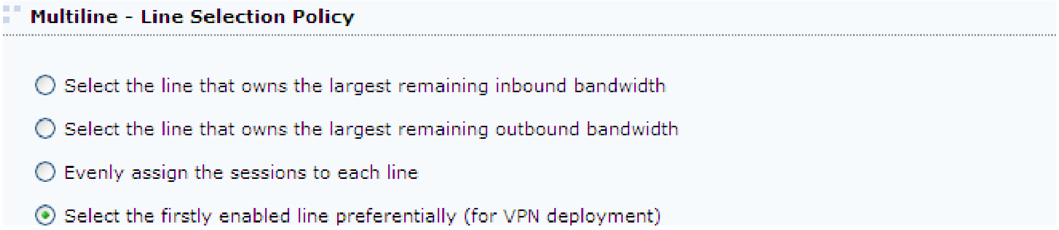
Line is mapped from it to SSL VPN HTTPS port

Configure the fields included onthe **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.

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:



Multiline - Line Selection Policy

○ Select the line that owns the largest remaining inbound bandwidth

○ Select the line that owns the largest remaining outbound bandwidth

○ Evenly assign the sessions to each line

● Select the firstly enabled line preferentially (for VPN deployment)

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.
- **Select the firstly enabled line preferentially (for VPN deployment):** 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.

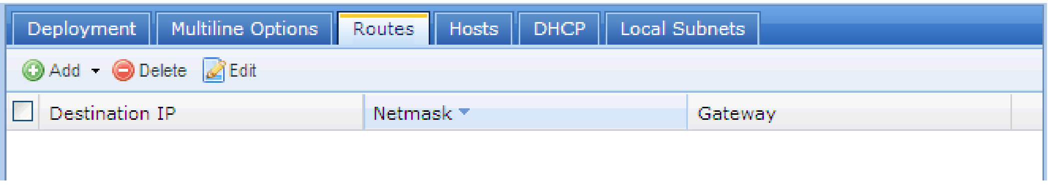
5. Click the **Save**button and that **Apply** button to save and apply the settings.

Configuring Route

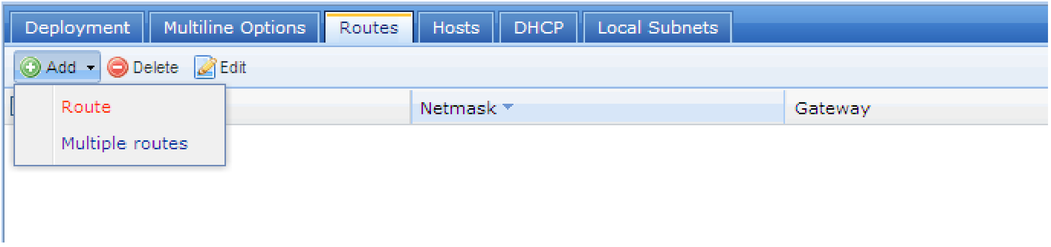
Route can route data of the Sangfor device itself, and route the data (either VPN data or VPN irrelevant data) to the Sangfor device, which then will forward the data to destination.

To add a new route, perform the steps below:

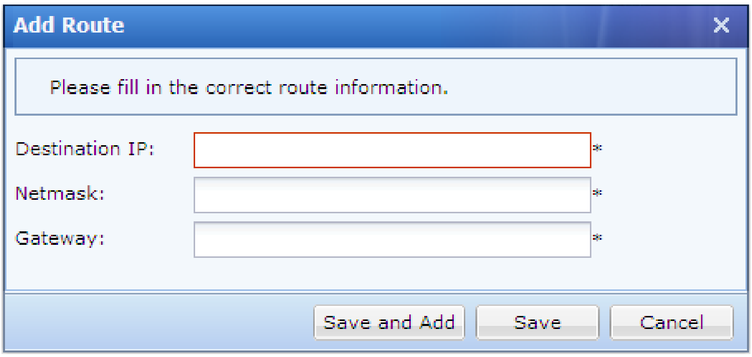
1. Navigate to **System**>**Network**>**Routes** to enter**Routes**page, as shown below:

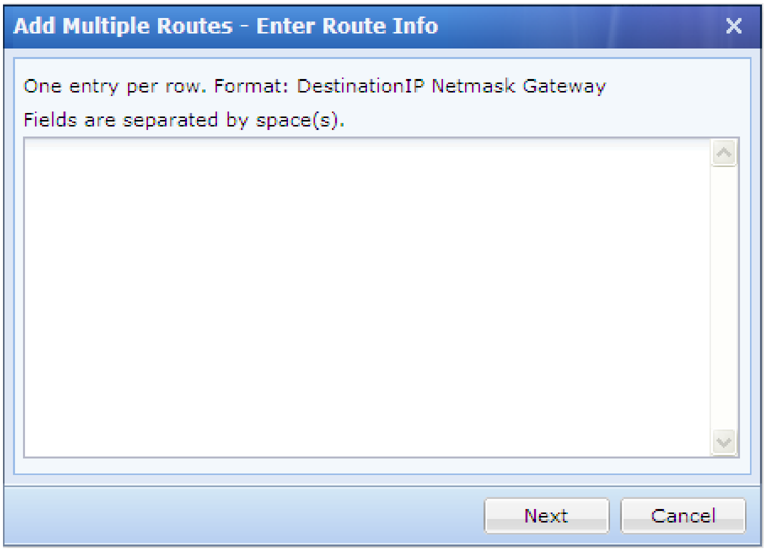


2. Click **Add**>**Routes** or **Multiple routes** to add a single route or a batch of routes, as shown below:



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.



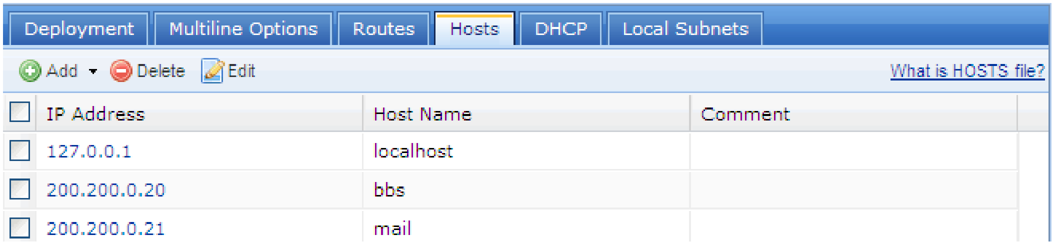

Add Multiple Routes - Enter Route Info
One entry per row. Format: DestinationIP Netmask Gateway
Fields are separated by space(s).
Next
Cancel

Configuring Host Mapping Rule (HOSTS)

HOSTS files 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.

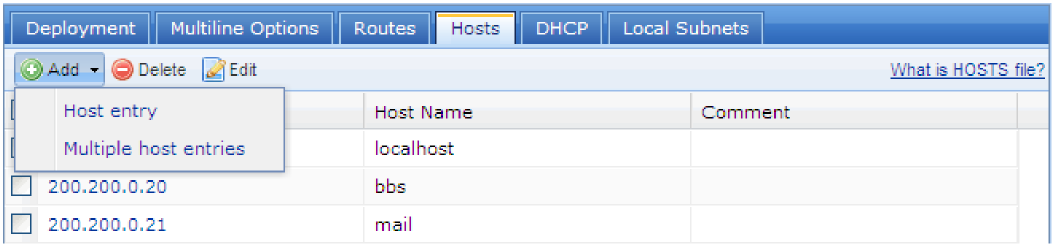
To add a new Host entry or a batch of Host entries:

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



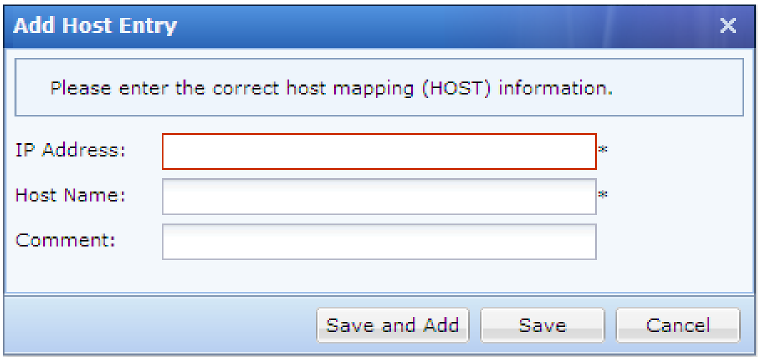
□	IP Address	Host Name	Comment
□	127.0.0.1	localhost	
□	200.200.0.20	bbs	
□	200.200.0.21	mail	

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



	Host Name	Comment
□	localhost	
□ 200.200.0.20	bbs	
□ 200.200.0.21	mail	

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



Please enter the correct host mapping (HOST) information.

IP Address: *

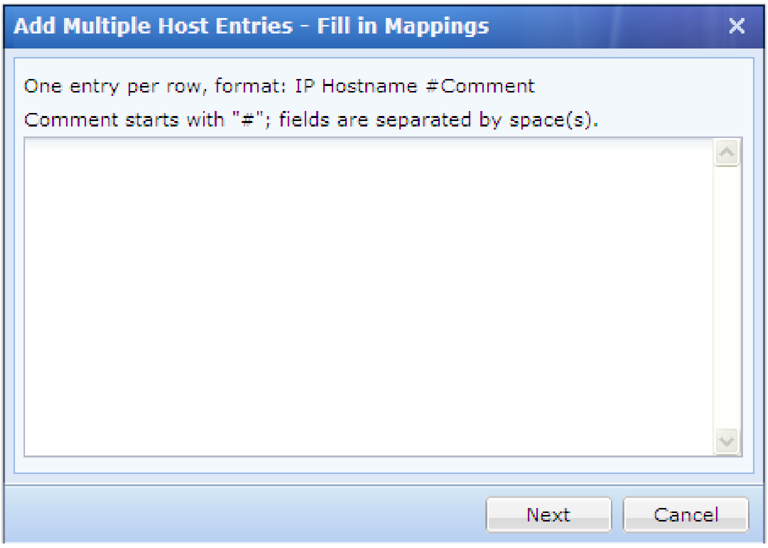
Host Name: *

Comment:

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 **multiplehost 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.

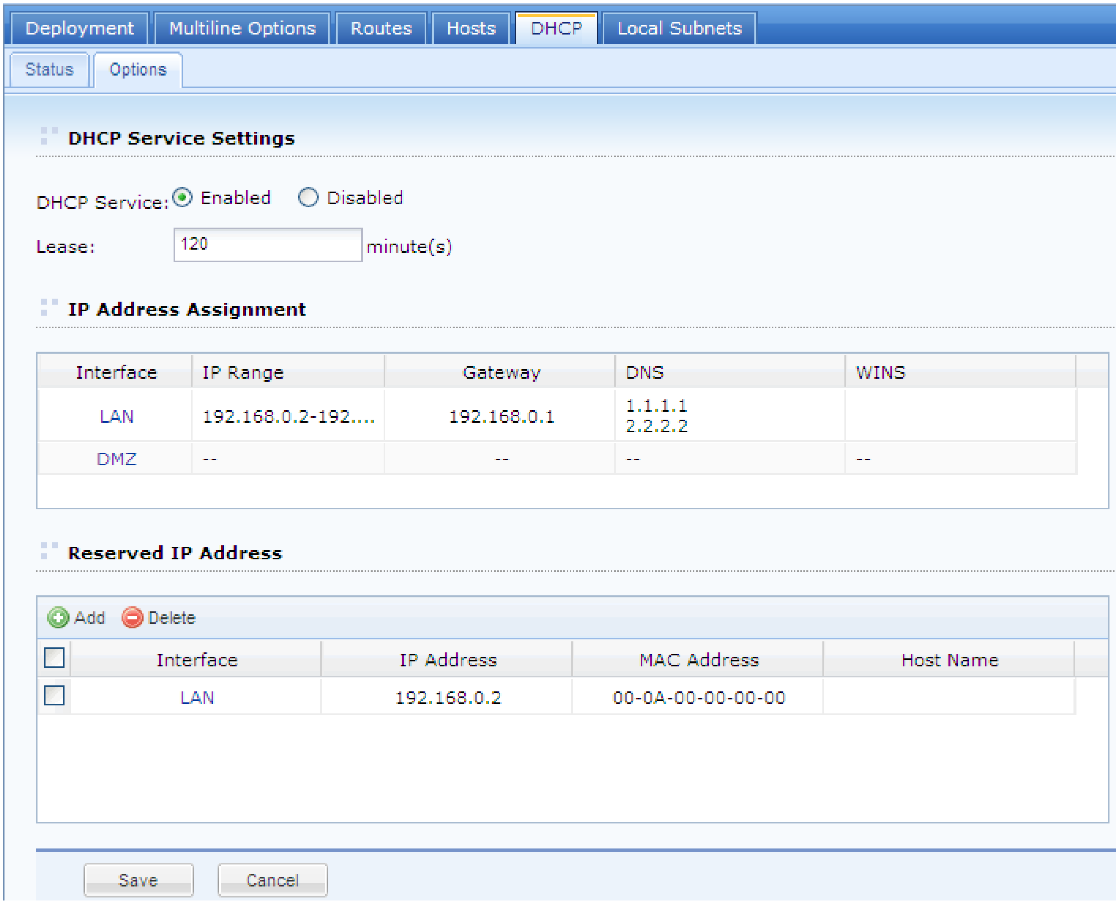


One entry per row, format: IP Hostname #Comment

Comment starts with "#"; fields are separated by space(s).

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:



DHCP Service Settings

DHCP Service: ● Enabled ○ Disabled

Lease: 120 minute(s)

IP Address Assignment

Interface	IP Range	Gateway	DNS	WINS
LAN	192.168.0.2-192....	192.168.0.1	1.1.1.1 2.2.2.2	
DMZ	--	--	--	--

Reserved IP Address

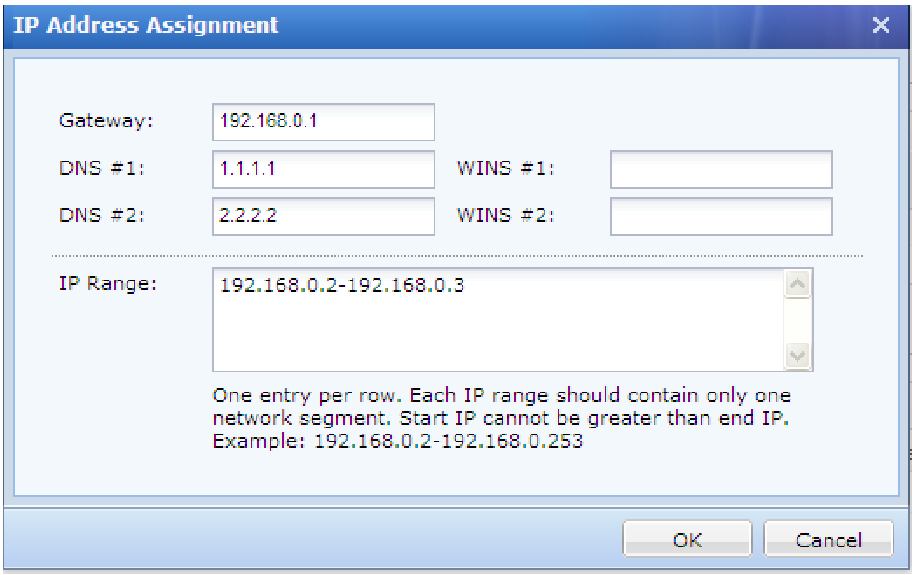
□	Interface	IP Address	MAC Address	Host Name
□	LAN	192.168.0.2	00-0A-00-00-00-00	

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:



Gateway: 192.168.0.1

DNS #1: 1.1.1.1 WINS #1:

DNS #2: 2.2.2.2 WINS #2:

IP Range: 192.168.0.2-192.168.0.3

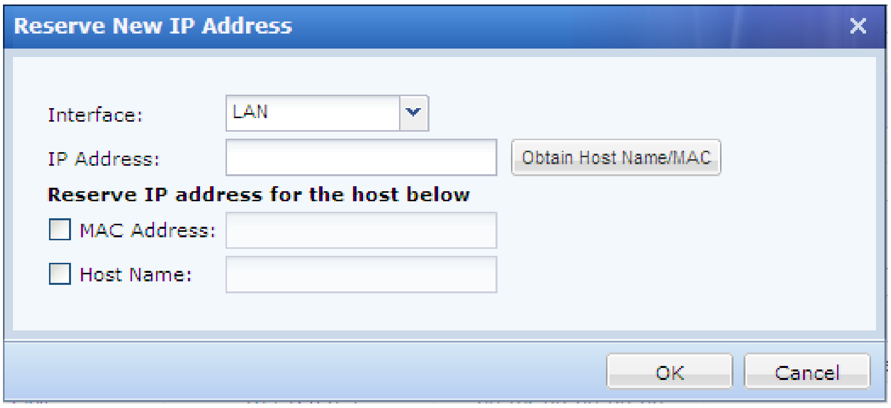
One entry per row. Each IP range should contain only one network segment. Start IP cannot be greater than end IP. Example: 192.168.0.2-192.168.0.253

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.

- **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:



Interface: LAN

IP Address:

Reserve IP address for the host below

□ MAC Address:

□ Host Name:

The fields on this page are described as follows:

- **Interface:** Specifies the network interface of this DHCP rule.

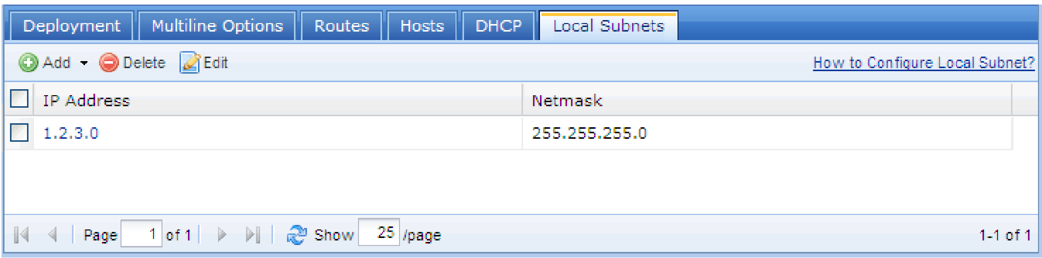
- **IP Address:** Specifies the IP address that to be served for certain computer. The reserved IP address will not be assigned to VPN users.
- **Obtain Host Name/MAC:** Click this button to obtain the MAC address and host name of the host for which this IP address is reserved.

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.

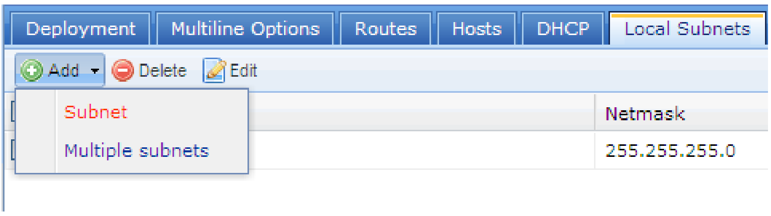
Assume that the HQ has two subnets (192.200.200.x and 192.200.254.x); the subnet 192.200.200.x is a network segment that is directly connected to the Sangfor device, while the subnet 192.200.254.x is indirectly connected to the Sangfor device. To add a local subnet entry,

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

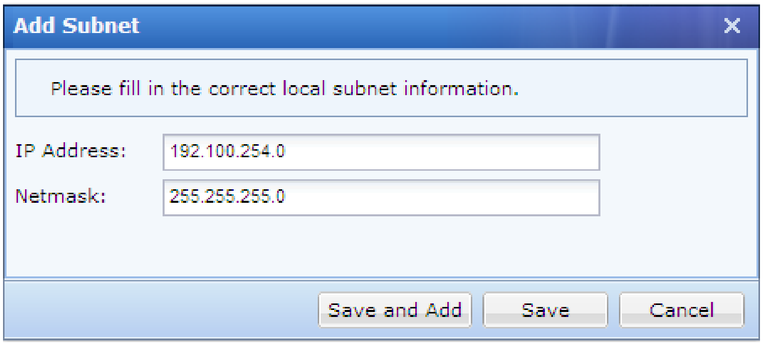


□	IP Address	Netmask
□	1.2.3.0	255.255.255.0

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:



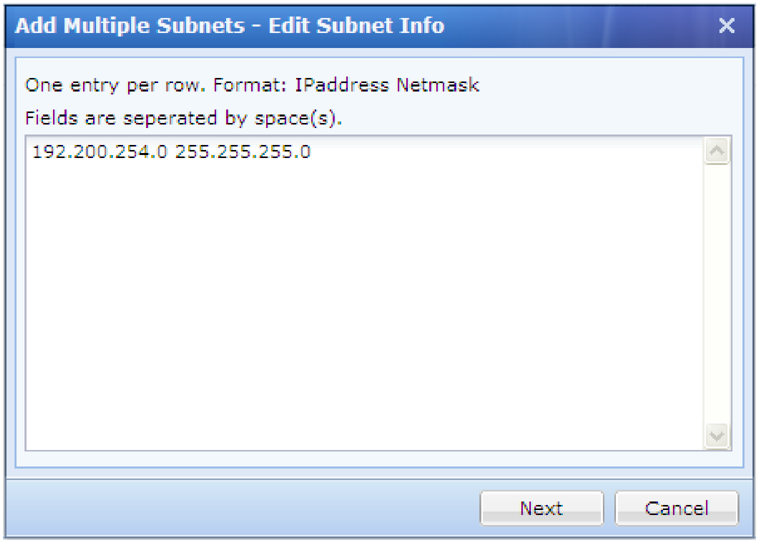
Please fill in the correct local subnet information.

IP Address: 192.100.254.0

Netmask: 255.255.255.0

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:



Add Multiple Subnets - Edit Subnet Info

One entry per row. Format: IPaddress Netmask

Fields are seperated by space(s).

```
192.200.254.0 255.255.255.0
```

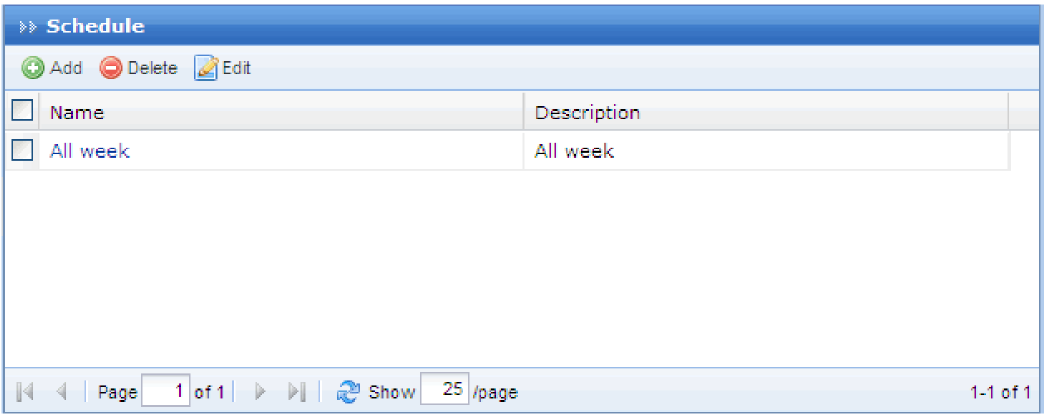
The local subnets are deemed as network segments of VPN by the Sangfor device and the client software, which means all the data sent from (or to) these network segments through the Sangfor device or software will be encapsulated into and transmitted through the VPN tunnels. For this reason, if you want to allow the VPN users to access certain subnet, add the related subnet into the list on the **Local Subnets** page and then go tithe **Routes** page to configure a corresponding route.

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:



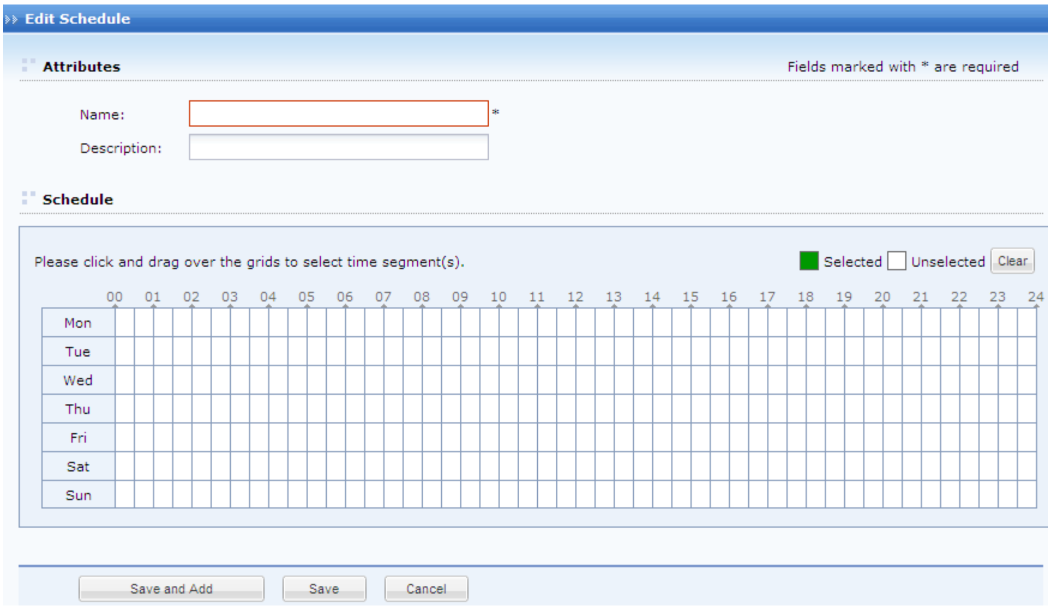
Schedule

Add Delete Edit

□	Name	Description
□	All week	All week

Page 1 of 1 Show 25 /page 1-1 of 1

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



Edit Schedule

Attributes

Fields marked with * are required

Name: *

Description:

Schedule

Please click and drag over the grids to select time segment(s).

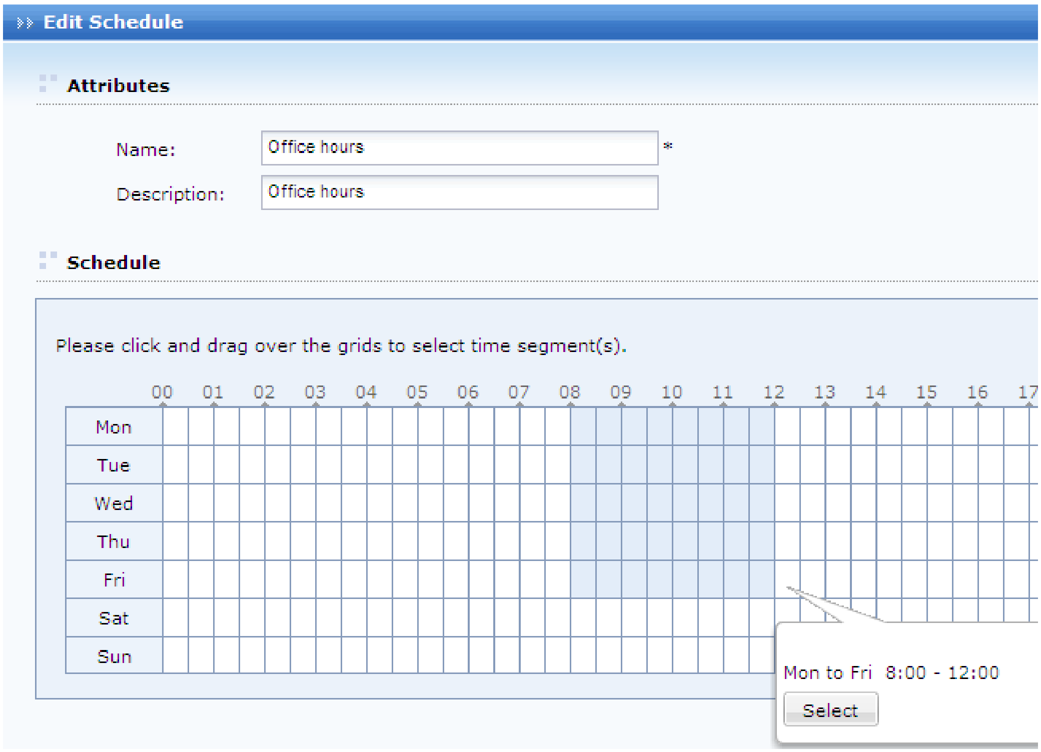
🟩 Selected □ Unselected Clear

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Mon																									
Tue																									
Wed																									
Thu																									
Fri																									
Sat																									
Sun																									

Save and Add Save Cancel

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


Edit Schedule

Attributes

Name: Office hours *

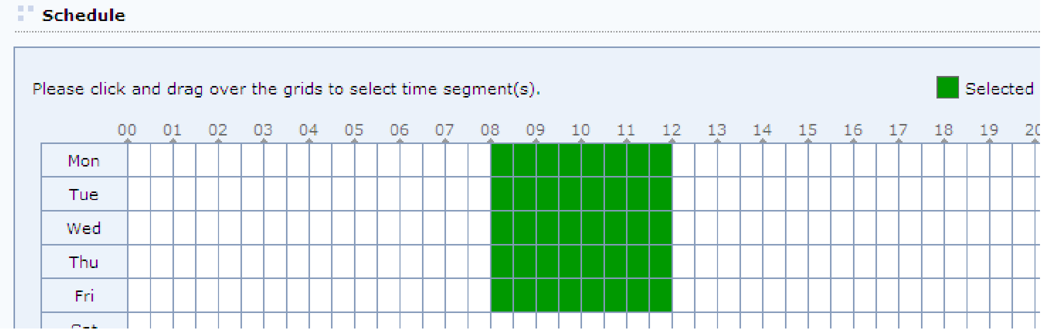
Description: Office hours

Schedule

Please click and drag over the grids to select time segment(s).

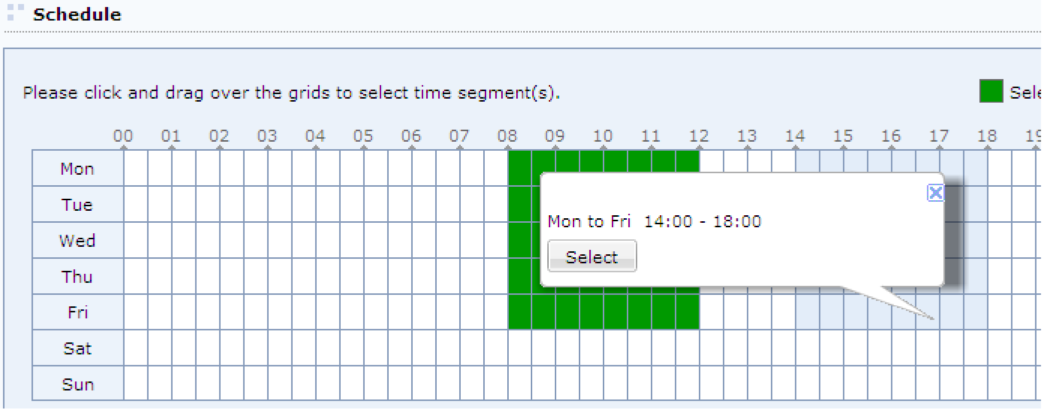
Mon to Fri 8:00 - 12:00

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


Schedule

Please click and drag over the grids to select time segment(s).

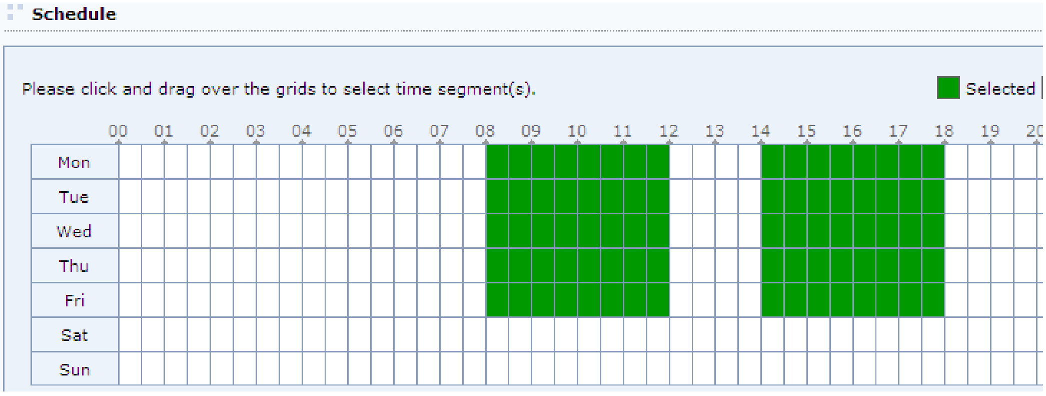
6. Go on to select the other time segment (14: 00-18: 00, from Monday to Friday) in the same way, as shown below:


Schedule

Please click and drag over the grids to select time segment(s).

Mon to Fri 14:00 - 18:00

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

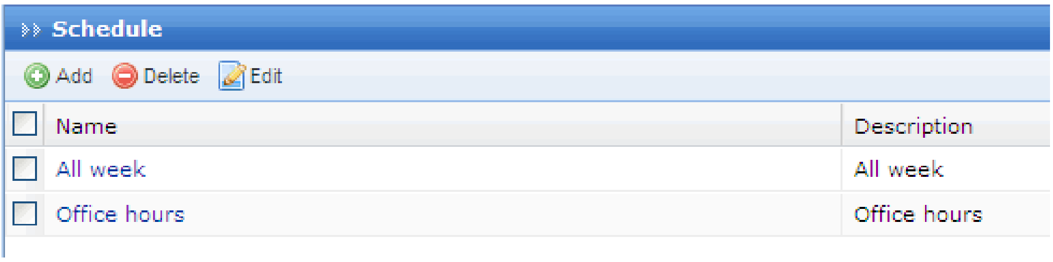


Schedule

Please click and drag over the grids to select time segment(s).

🟩 Selected

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

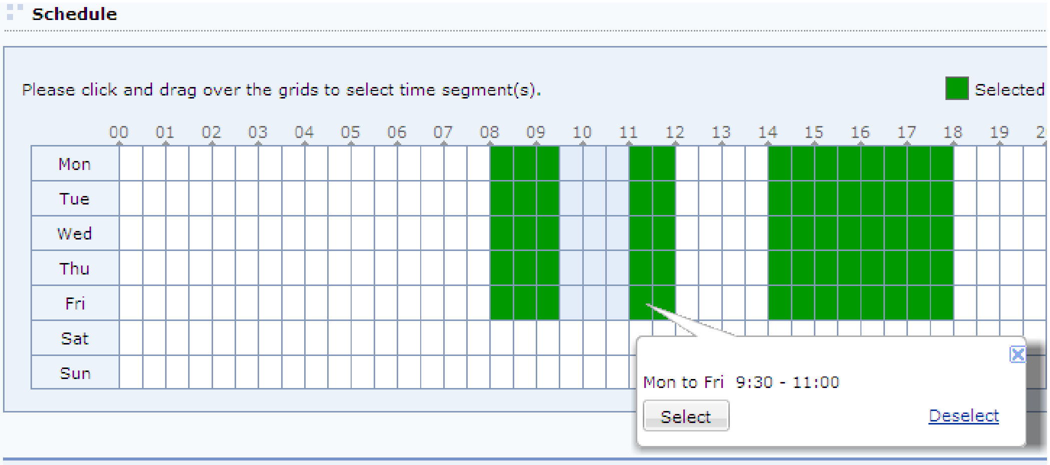


Schedule

□	Name	Description
□	All week	All week
□	Office hours	Office hours

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:



Schedule

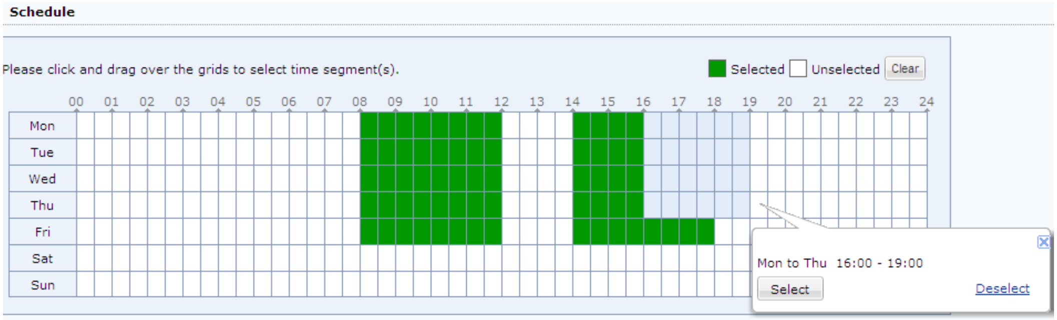
Please click and drag over the grids to select time segment(s).

🟩 Selected

Mon to Fri 9:30 - 11:00

2. Click **Deselect** to deselect the time segment that has turned to light blue (while green grid indicates that the time segments reselected 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:



Schedule

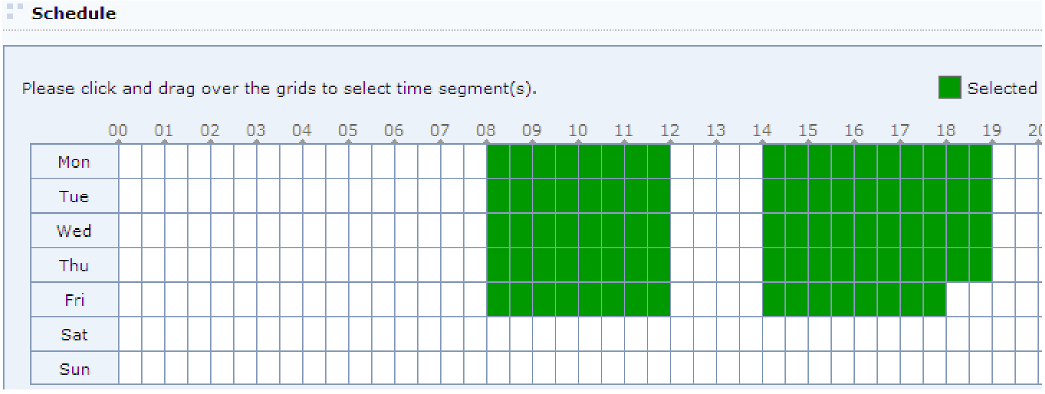
Please click and drag over the grids to select time segment(s).

🟩 Selected □ Unselected Clear

Mon to Thu 16:00 - 19:00

Select Deselect

- 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:

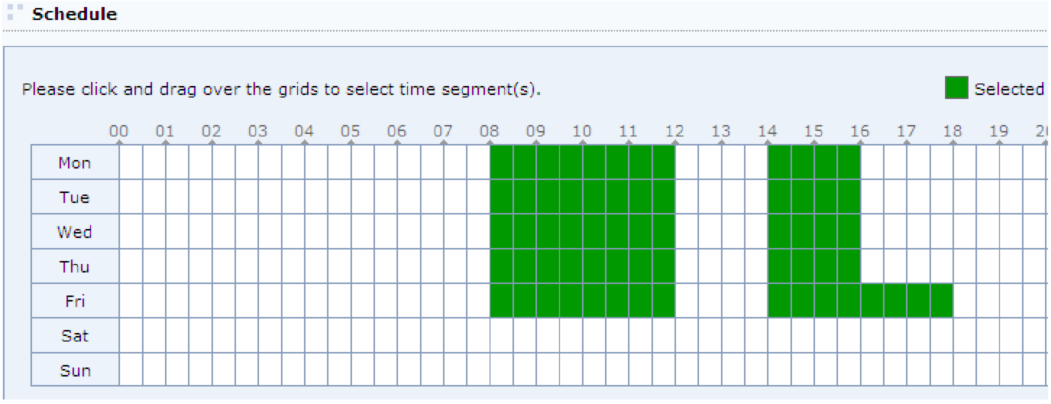


Schedule

Please click and drag over the grids to select time segment(s).

🟩 Selected

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



Schedule

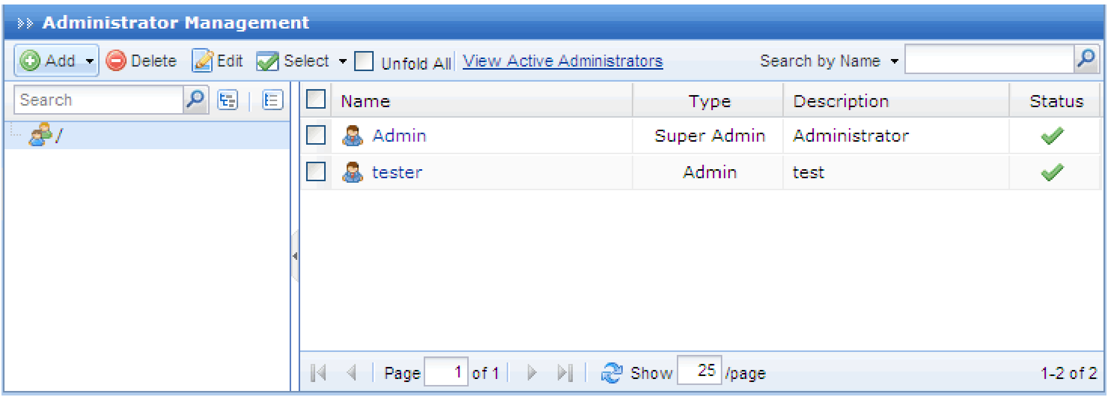
Please click and drag over the grids to select time segment(s).

🟩 Selected

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 Management** page is shown in the figure below:



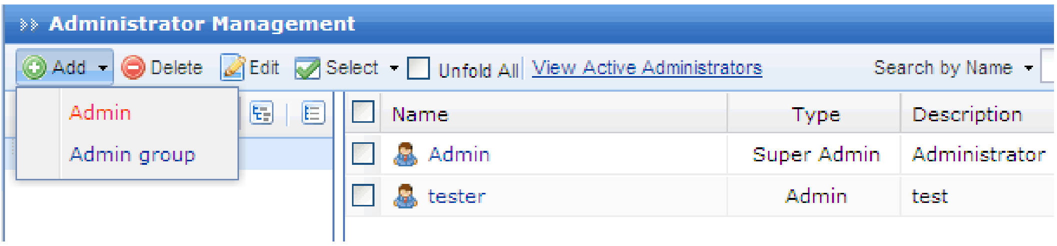
□	Name	Type	Description	Status
□	Admin	Super Admin	Administrator	✓
□	tester	Admin	test	✓

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

- **Unfold All:** Select the checkbox next to it andthe 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.

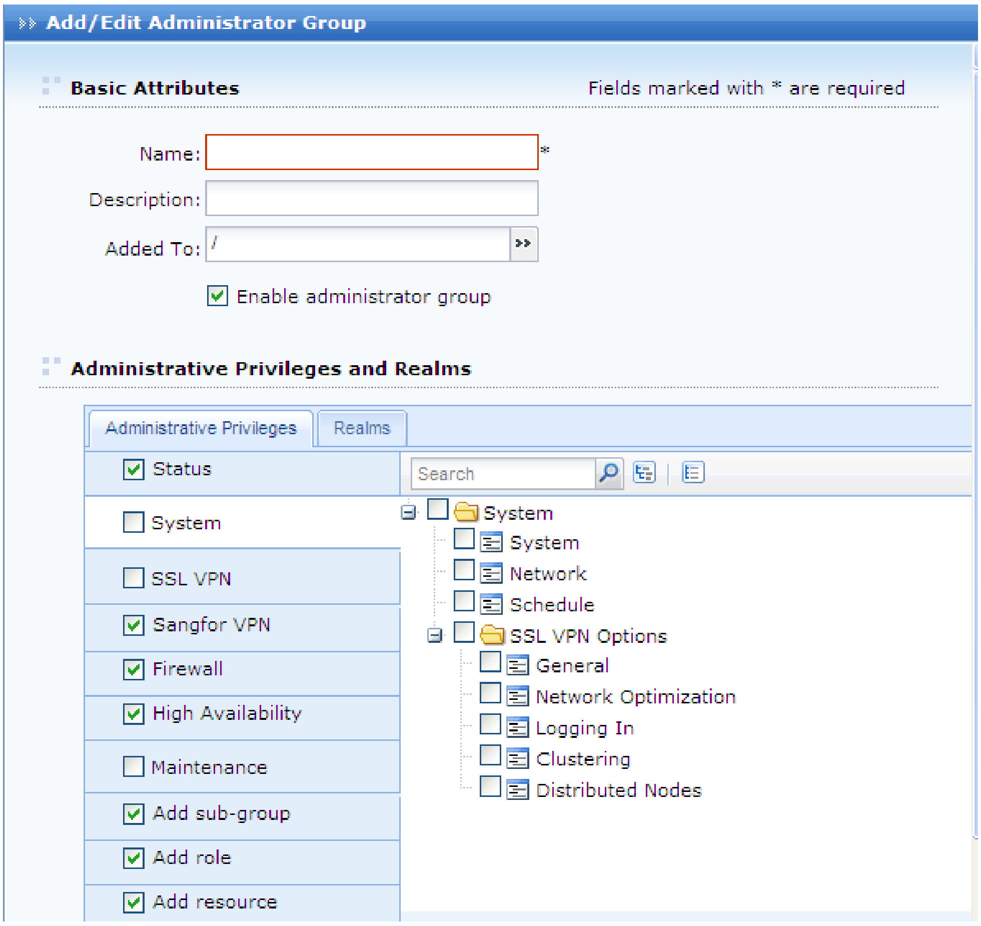
Adding Administrator Group

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



□	Name	Type	Description
□	Admin	Super Admin	Administrator
□	tester	Admin	test

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



Add/Edit Administrator Group

Basic Attributes

Fields marked with * are required

Name: *

Description:

Added To: /

☑ Enable administrator group

Administrative Privileges and Realms

Administrative Privileges | Realms

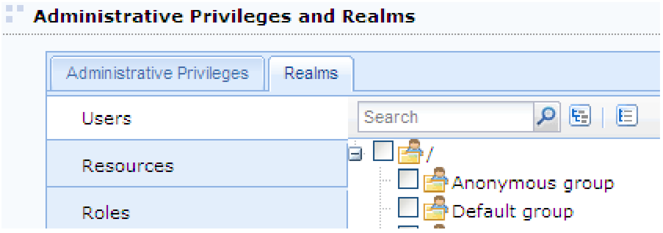
☑ Status
□ System
□ SSL VPN
☑ Sangfor VPN
☑ Firewall
☑ High Availability
□ Maintenance
☑ Add sub-group
☑ Add role
☑ Add resource

Search

- □ System
  - □ System
  - □ Network
  - □ Schedule
  - □ SSL VPN Options
    - □ General
    - □ Network Optimization
    - □ Logging In
    - □ Clustering
    - □ Distributed Nodes

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:



Administrative Privileges and Realms

Administrative Privileges | Realms

Users
Resources
Roles

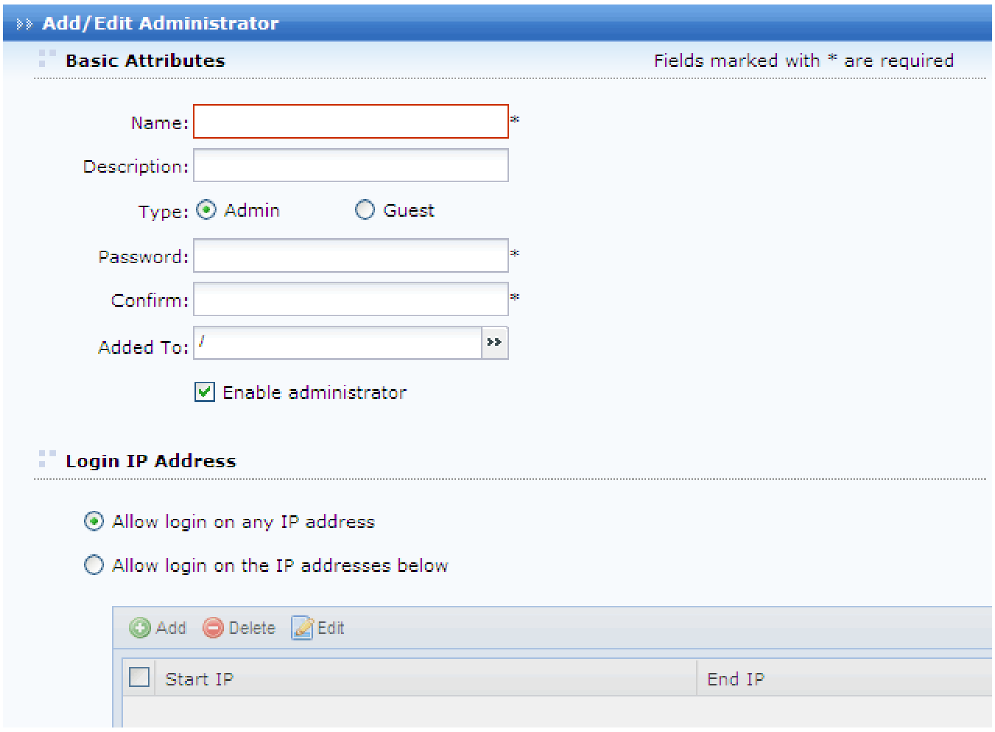
Search

- □ /
  - □ Anonymous group
  - □ Default group

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:



Add/Edit Administrator

Basic Attributes

Fields marked with * are required

Name: *

Description:

Type: ● Admin ○ Guest

Password: *

Confirm: *

Added To: /

☑ Enable administrator

Login IP Address

● Allow login on any IP address

○ Allow login on the IP addresses below

□	Start IP	End IP

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.

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

⚠

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.

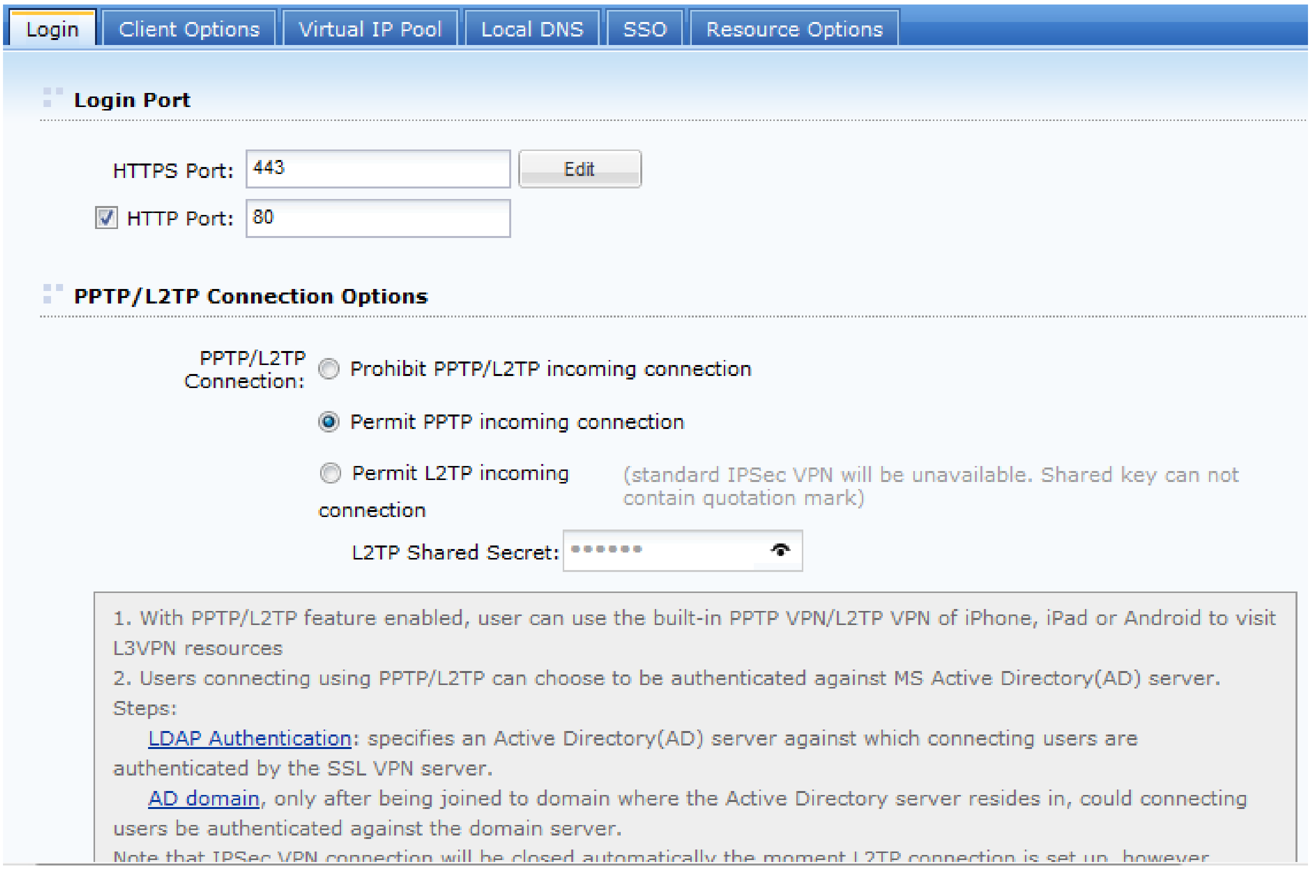
SSL VPN Options

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 show in the figure below:



Login Port

HTTPS Port: 443

☑ HTTP Port: 80

PPTP/L2TP Connection Options

PPTP/L2TP Connection:

○ Prohibit PPTP/L2TP incoming connection

● Permit PPTP incoming connection

○ Permit L2TP incoming connection (standard IPSec VPN will be unavailable. Shared key can not contain quotation mark)

L2TP Shared Secret: ••••••

1. With PPTP/L2TP feature enabled, user can use the built-in PPTP VPN/L2TP VPN of iPhone, iPad or Android to visit L3VPN resources
2. Users connecting using PPTP/L2TP can choose to be authenticated against MS Active Directory(AD) server.
Steps:
LDAP Authentication: specifies an Active Directory(AD) server against which connecting users are authenticated by the SSL VPN server.
AD domain, only after being joined to domain where the Active Directory server resides in, could connecting users be authenticated against the domain server.
Note that IPSec VPN connection will be closed automatically the moment L2TP connection is set up, however

2. Configure the following field sunder **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.

- 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 use renters the address to connectSSL 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 tovisit***https://202.96.137.75***.

3. Configure PPTP/L2TP connection options
PPTP/L2TP connection:

- **Prohibit PPTP/L2TP incoming connection:** configure as disallow PPTP/L2TP connection.
- **Permit PPTP incoming connection:** allow phone users able access L3VPN resource.
- **Permit L2TP incoming:** set the share key, phone users ca through L2TP VPN access L3VPN resource from system.

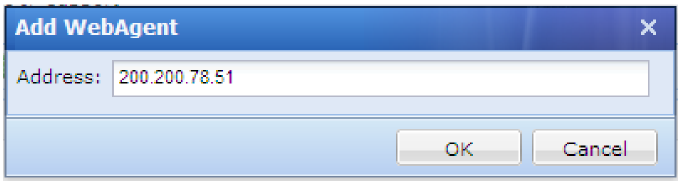
If you enable L2TP access service, then automatically turn off SSL standard IPSecVPN device user access. But won't impact Sangfor IPSec VPN access.

4. Encryption protocol for data encrypt algorithms.
SSL/TLS Algorithm:

- **RSA:** International encrypts Algorithm.
- **SM2:** China encryption Algorithm

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

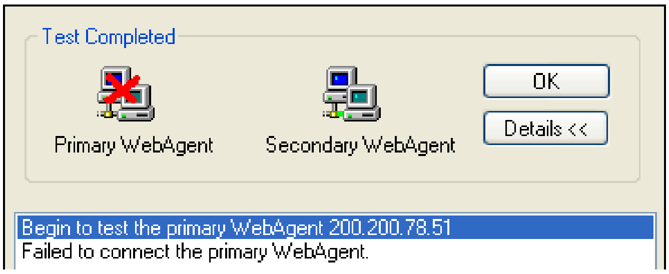
a. Click **Add** to enter the **Add Web Agent** page, as shown below:



Address: 200.200.78.51

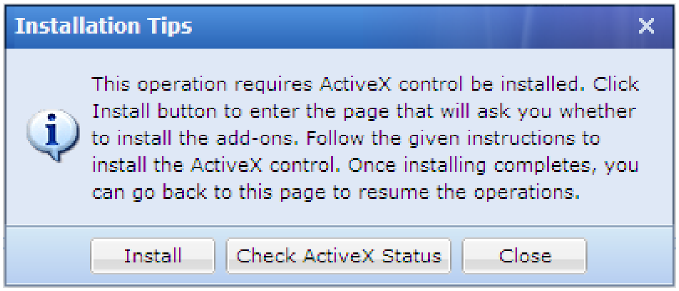
b. Enter the Web Agent address into the **Address** field and click the **OK** button.

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



Begin to test the primary WebAgent 200.200.78.51
Failed to connect the primary WebAgent.

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



This operation requires ActiveX control be installed. Click Install button to enter the page that will ask you whether to install the add-ons. Follow the given instructions to install the ActiveX control. Once installing completes, you can go back to this page to resume the operations.

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 Web Agent entry, select the desired entry and click **Delete** or **Edit**.

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

f. To refresh the status of the Web Agent, click **Refresh**.

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

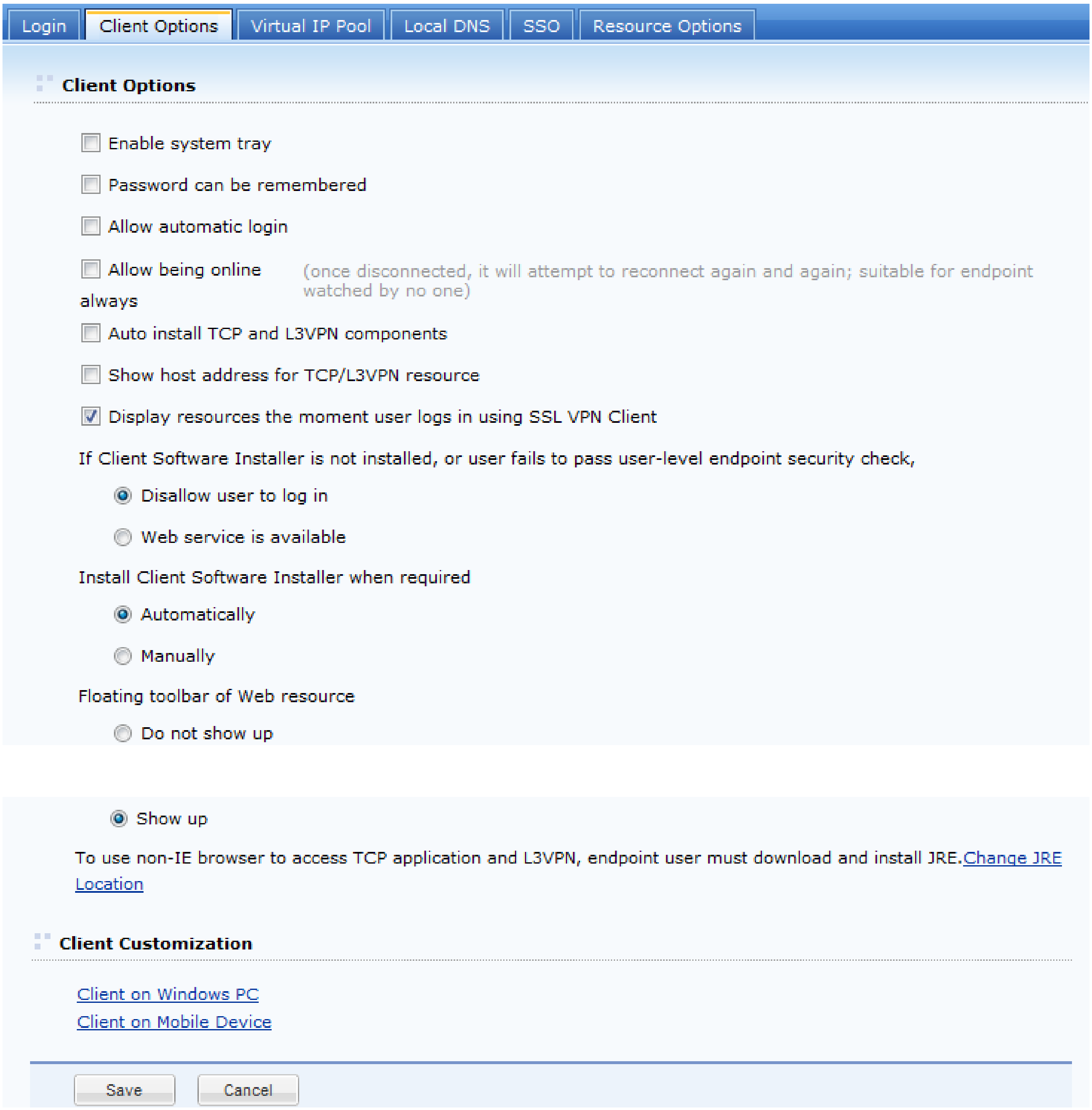
   Select **Enable defense against man-in-the-middle attack** option and the user will be required to enter the word verification code and be forced to install the related controls. This feature protects the transmitted data from being altered or intercepted by unauthorized user.

7. 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.

Navigate to **System**>**SSL VPN Options**>**General**>**Client Options** to configure client related options, as shown in the figure below:



Client Options

☐ Enable system tray

☐ Password can be remembered

☐ Allow automatic login

☐ Allow being online always (once disconnected, it will attempt to reconnect again and again; suitable for endpoint watched by no one)

☐ Auto install TCP and L3VPN components

☐ Show host address for TCP/L3VPN resource

☑ Display resources the moment user logs in using SSL VPN Client

If Client Software Installer is not installed, or user fails to pass user-level endpoint security check,

● Disallow user to log in

○ Web service is available

Install Client Software Installer when required

● Automatically

○ Manually

Floating toolbar of Web resource

○ Do not show up

● Show up

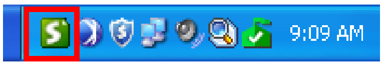
To use non-IE browser to access TCP application and L3VPN, endpoint user must download and install JRE.Change JRE Location

Client Customization

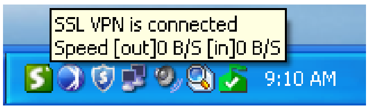
Client on Windows PC
Client on Mobile Device

The following are the contents under **SSL VPN Client Options**:

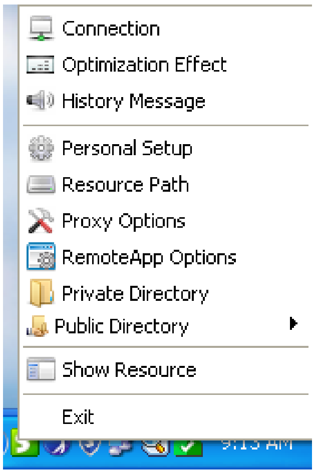
- **Enable system tray:** System tray is a taskbar status area showing status of and configure SSL VPN on the client end. Select this option and the browser window can minimize to a system tray when **Resource** page is closed.



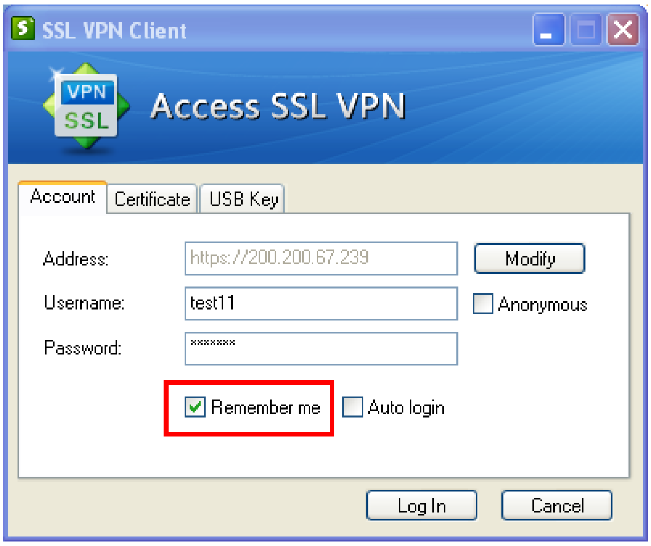
Put the cursor on the **System Tray** icon and the brief information of SSL VPN connection status is seen, as shown in the figure below:


SSL VPN is connected
Speed [out]0 B/S [in]0 B/S

Right-click on the **System Tray** icon and the **Floating Window** appears, as shown 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 **Rememberme** when he/she uses SSL VPN Client program to connect SSL VPN (for more details, refer to the Client in Chapter 3), as shown in the figure below:


SSL VPN Client

Access SSL VPN

Address: https://200.200.67.239

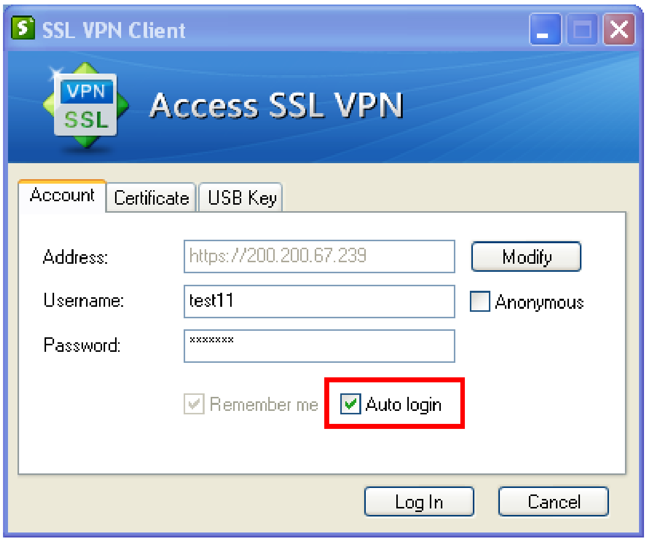
Username: test11

Password: *******

☑ Remember me □ Auto login

□ Anonymous

- **Allow automatic login:** Select this option to allow connecting users to use automatic login feature when they connect to SSL VPN (for more details, refer to the Client in Chapter 3), as shown below:



SSL VPN Client

Access SSL VPN

Address: https://200.200.67.239 Modify

Username: test11 □ Anonymous

Password: *******

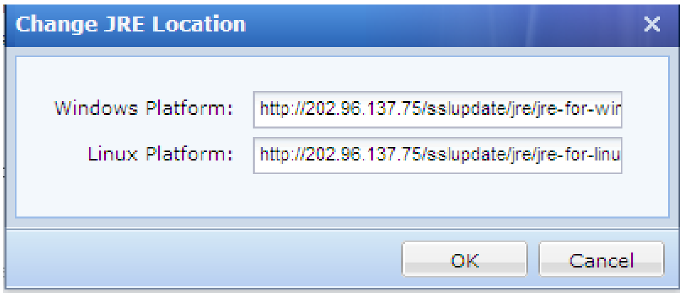
☑ Remember me ☑ Auto login

- **Allow begin online:** once disconnected, it will attempt to reconnect again and again; suitable for endpoint watched by no one
- **Auto install TCP and L3VPN components:** Select the checkbox next to this option and the components related to TCP application and L3VPN will be enabled and installed when users log in to the SSL VPN. Otherwise, the users need tomanually install and install the component if they want to access TCP or L3VPN resources when logging in to SSL VPN for the first time.
- To have the detailed addresses of TCP applications and L3VPNs seen by users after they log in to the SSL VPN, select the checkbox next to **Show host address for TCP/L3VPN resource**.
- **Display resource the moment user logs in using SSL VPN Client**
- **Install Client Software Installer when required:** Configures the way how the components are installed on the client side if the endpoint has not installed the required components. Options are **Automatically** and **Manually**.

  Automatically: Indicates that the components will be distributed and installed automatically on the client side, assuming that the user applies hardware ID based authentication or go through pre-authentication security check prior to access to SSL VPN. For details about hardware ID based authentication and pre-authentication security check, refer to the Authentication section and Settings section in Chapter 4 respectively.

  Manually: Indicates that the user will be prompted to install the components if user applies hardware ID based authentication or pre-authentication security check (which is conducted before login). The user decides whether or not to install the related components.
- **If Client Software Installer is not installed, or user fails to pass user-level endpoint security check:** If hardware ID based authentication is applied and user fails to pass the pre-authentication security check, he/she maybe prohibited from logging in or allowed to log in but can only access the Web resources. What will happen to user is subject to the option selected, **Disallow user to login** or **Allow user to login but access Web resources only**.

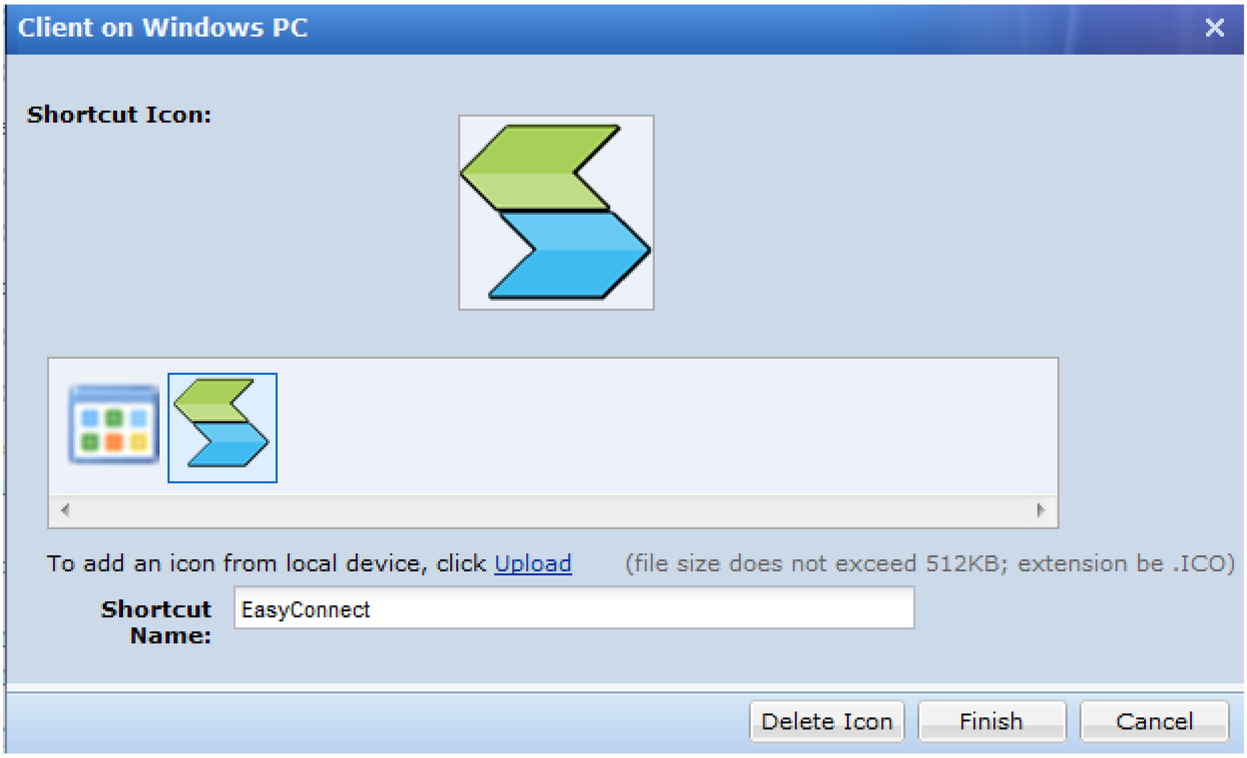
  Change JRE Location: Click this link and enter the addresses into the fields **Windows Platform** and **Linux Platform** respectively. Connecting users can download the JRE installation package and log in to SSL VPN when they uses non-IE browser. The **Change JRE Location** page is as shown in the figure below:



Windows Platform: http://202.96.137.75/sslupdate/jre/jre-for-wir

Linux Platform: http://202.96.137.75/sslupdate/jre/jre-for-linu

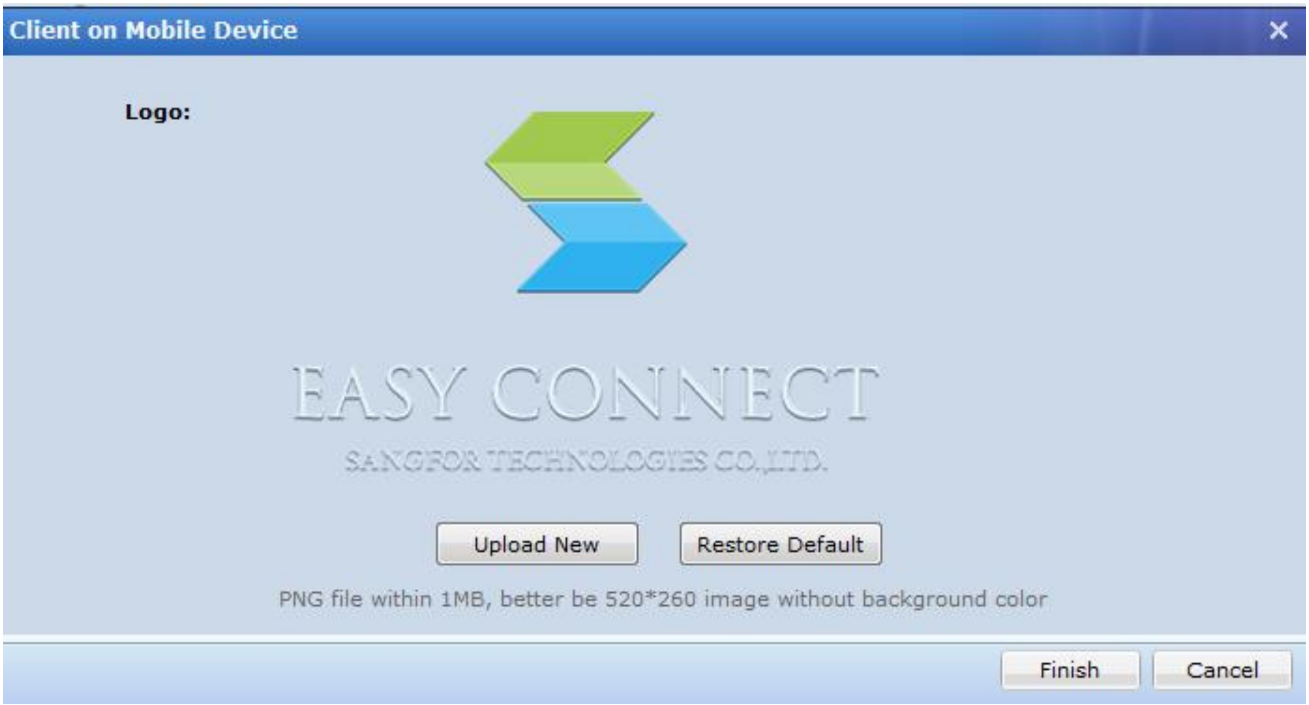
- **Client on Windows PC:** Specifies a shortcut icon of **System Tray** that appears on the taskbar, and able to upload icon the figure as shown below:



To add an icon from local device, click Upload (file size does not exceed 512KB; extension be .ICO)

Shortcut Name: EasyConnect

- **Client on Mobile Device:** remote access such as hand phone, Ipad etc..the figure shown below:



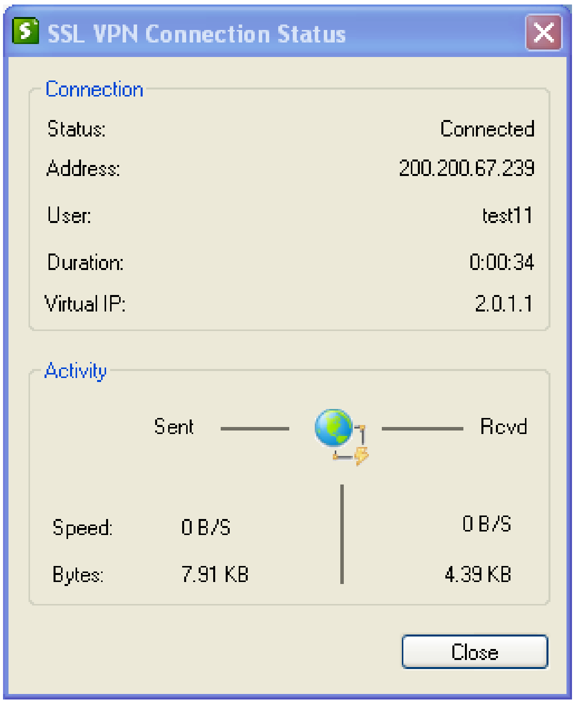
PNG file within 1MB, better be 520*260 image without background color

- The functionalities provided by **floating window** and **system tray** are the same.
- If **Enable system tray** is not selected but connecting user can access any TCP and/or L3VPN resource, the connecting user can still use the floating window after login to SSL VPN.
- If **Enable system tray** is not selected and connecting users can only access Web resource, the floating window will not be available to the connecting user.

- 32bitMAC OS only supports floating window, not supporting system tray.
- The floating window and system tray are attachments of SSL VPN Client. If the Client Software Installer is not installed, both floating window and system tray are not available.

The following are the menus included on the floating window:

- **Connection:** Click it to view the real-time SSL VPN connection status, IP address, current connecting user, online duration, virtual IP address, overall traffic and speed, as shown in the figure below:



SSL VPN Connection Status

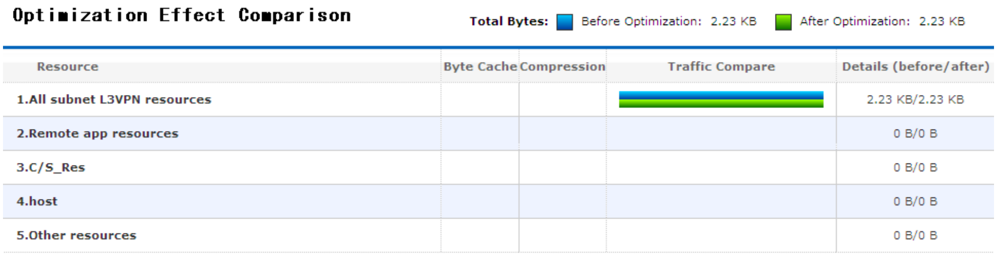
Connection

Status:	Connected
Address:	200.200.67.239
User:	test11
Duration:	0:00:34
Virtual IP:	2.0.1.1

Activity

	Sent	Rcvd
Speed:	0 B/S	0 B/S
Bytes:	7.91 KB	4.39 KB

- **Optimization Effect:** Click it to view the optimization effect.

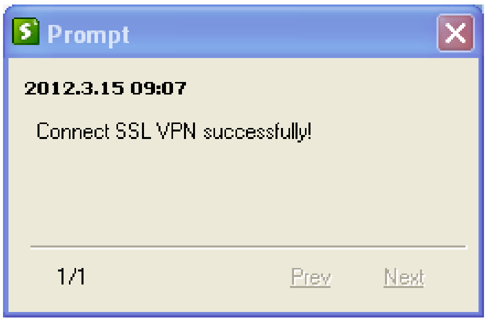


Optimization Effect Comparison

Total Bytes: 🟦 Before Optimization: 2.23 KB 🟩 After Optimization: 2.23 KB

Resource	Byte Cache	Compression	Traffic Compare	Details (before/after)
1.All subnet L3VPN resources				2.23 KB/2.23 KB
2.Remote app resources				0 B/0 B
3.C/S_Res				0 B/0 B
4.host				0 B/0 B
5.Other resources				0 B/0 B

- **History Message:** Click it to view the message(s) received.



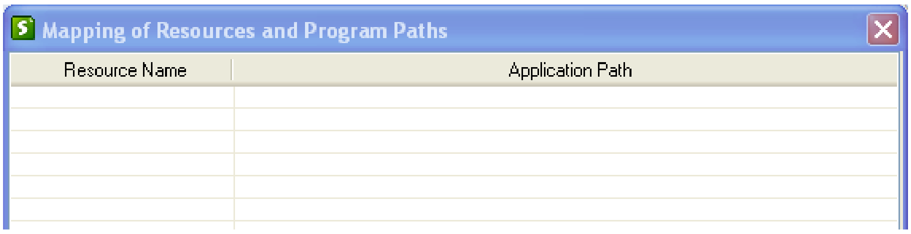
Prompt

2012.3.15 09:07

Connect SSL VPN successfully!

1/1

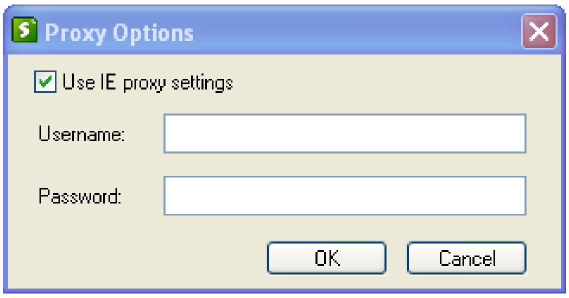
- **Resource Path:** Click it to view the mapping between resource and application path.



Mapping of Resources and Program Paths

Resource Name	Application Path

- **Proxy Options:** Click it to configure whether to use IE proxy settings, as shown below:



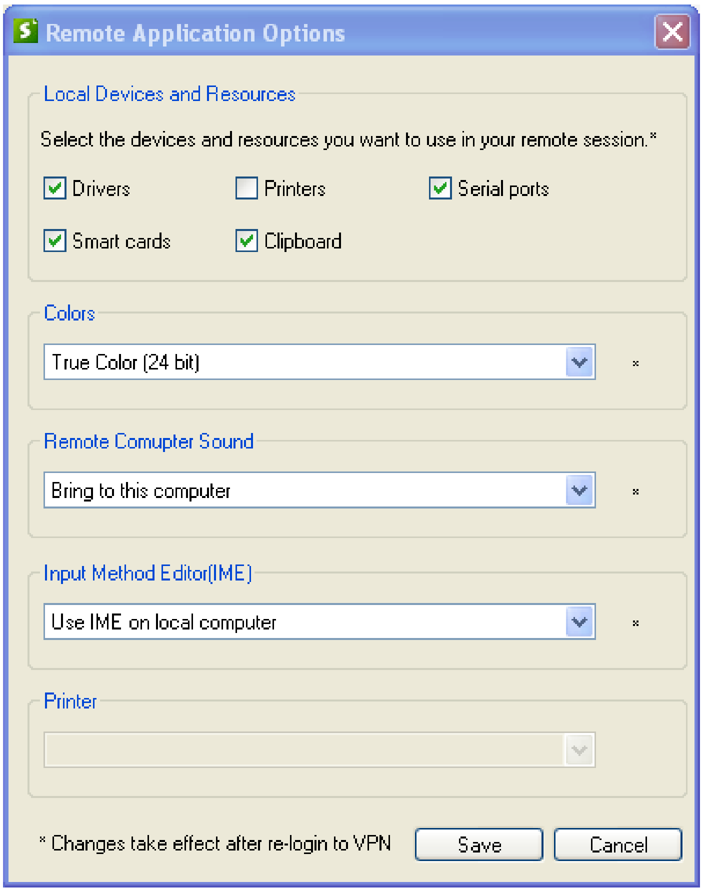
Proxy Options

☑ Use IE proxy settings

Username:

Password:

- **Remote Application Options:** Click it to view the options related to remote application. This menu is only available when there is **Remote Application** resource accessible to the connecting user.



Remote Application Options

Local Devices and Resources

Select the devices and resources you want to use in your remote session.*

☑ Drivers ☐ Printers ☑ Serial ports

☑ Smart cards ☑ Clipboard

Colors

True Color (24 bit) *

Remote Comupter Sound

Bring to this computer *

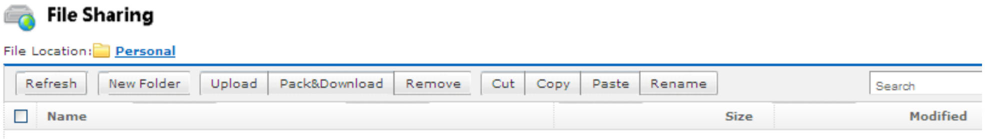
Input Method Editor(IME)

Use IME on local computer *

Printer

* Changes take effect after re-login to VPN

- **Private Directory:** Click it to view and access the private directory assigned to the connecting user. This menu is only available when there is remote storage server providing remote application resource and a private directory is accessible to the connecting user.

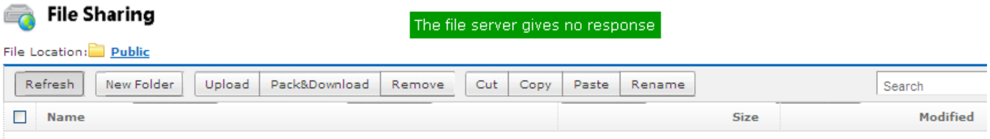


File Sharing

File Location: Personal

☐ Name	Size	Modified

- **Public Directory:** Click it to view and access the public directory assigned to the connecting user. This menu is only available when there is remote storage server providing remote application resource and a public directory is accessible to the connecting user.

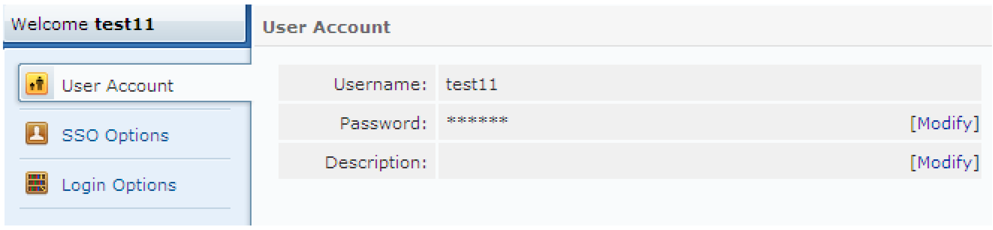


The file server gives no response

File Location: Public

□	Name	Size	Modified

- **Show Resource:** Click it to enter the **Resource** page to view and access the available internal resources.
- **Exit:** Click it to exit from the SSL VPN.
- **Personal Setup:** Click it to set the personal information of the connecting user, as shown in the figure below:

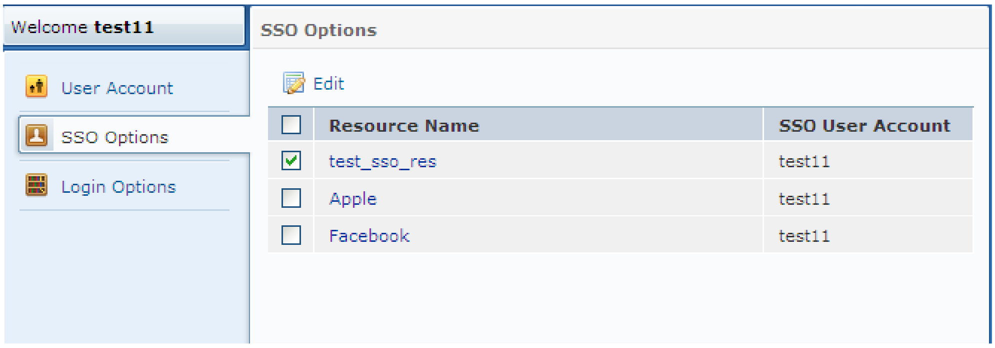


User Account

Username:	test11	
Password:	*******	[Modify]
Description:		[Modify]

The following are the contents included on the **User Account** page:

- **Username:** Name of the connecting user, not editable.
- **Password:** Password of the connecting user.
- **Description:** Descriptive information of this user.
- **Modify:** Click it to modify the corresponding information.

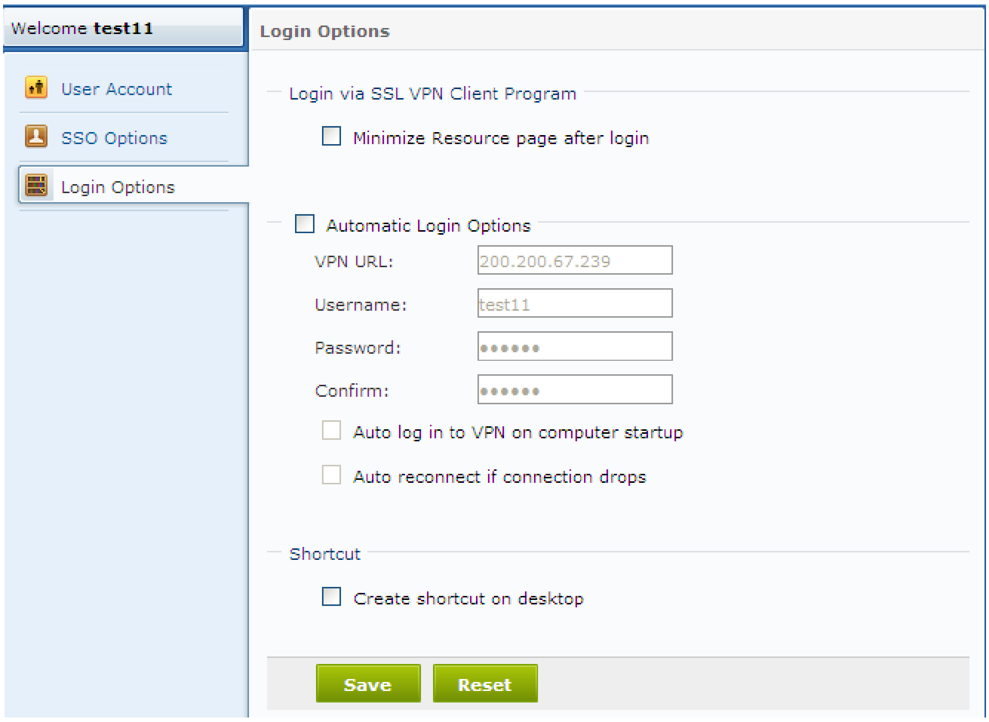


SSO Options

□	Resource Name	SSO User Account
☑	test_sso_res	test11
□	Apple	test11
□	Facebook	test11

The following are the contents included on the **SSO Options** page:

- **Resource Name:** Name of the resource available to the connecting user.
- **SSO User Account:** SSO user account that the connecting user can use to access a resource.
- **Edit:** Select an entry and click **Edit** to modify the SSO user account of the corresponding resource.



Login Options

Login via SSL VPN Client Program

□ Minimize Resource page after login

□ Automatic Login Options

VPN URL: 200.200.67.239

Username: test11

Password: ••••••

Confirm: ••••••

□ Auto log in to VPN on computer startup

□ Auto reconnect if connection drops

Shortcut

□ Create shortcut on desktop

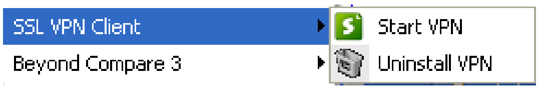
The following are the contents included on the **Login Options** page:

- **Minimize Resource page after login:** Indicates that the resource page will not show up after user logs in to SSL VPN through the SSL VPN Client.
- **Automatic Login Options:** The settings under it decide whether user can directly access the SSL VPN by double-clicking the shortcut icon on the desktop. If enabled, the VPN URL, username and passwords configured hereunder will be filled in automatically when user uses SSL VPN Client to access SSL VPN.
- **VPN URL:** Specifies the IP address or domain name of the SSL VPN that user is to access.
- **Username:** Specifies the username of the account that user uses to access the SSL VPN.
- **Password:** Specifies the password of the account that user uses to log in to the SSL VPN automatically.
- **Confirm:** Retype the password into this field. This password must be identical with the password entered in **Password** field.
- **Auto log in to VPN on computer startup:** With this option being selected, the user will automatically logs in to the SSL VPN while its computer starts up, without entering username and password manually.
- **Auto reconnect if connection drops:** If this option is selected, the connecting user can reconnect SSL VPN automatically once the connection is dropped.
- **Create Shortcut on Desktop:** If this option is selected, a shortcut of SSL VPN Client program named **Start VPN** will be created on desktop. This option, in association with the settings under **Automatic Login Options**, enables user to connect to SSL VPN when user double-clicks the

shortcut icon.

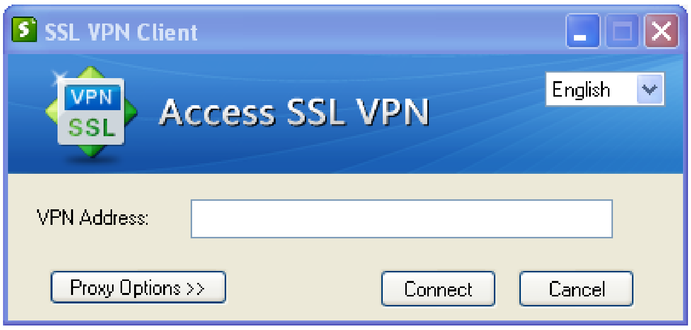
Scenario3:Enabling Automatic Access Using SSL VPN Client

1. Navigate to **Start**>**Programs**>**SSL VPN Client** to start SSL VPN, as shown below:

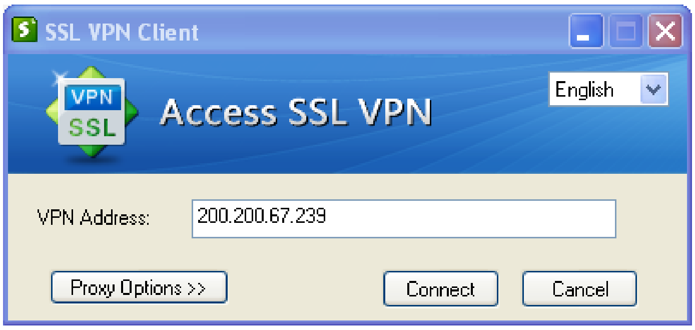


The first time user accesses the SSL VPN through browser, SSL VPN Client is installed on the user's PC automatically.

2. Click **SSL VPN Client** to open the **SSL VPN Client**window, as shown below:

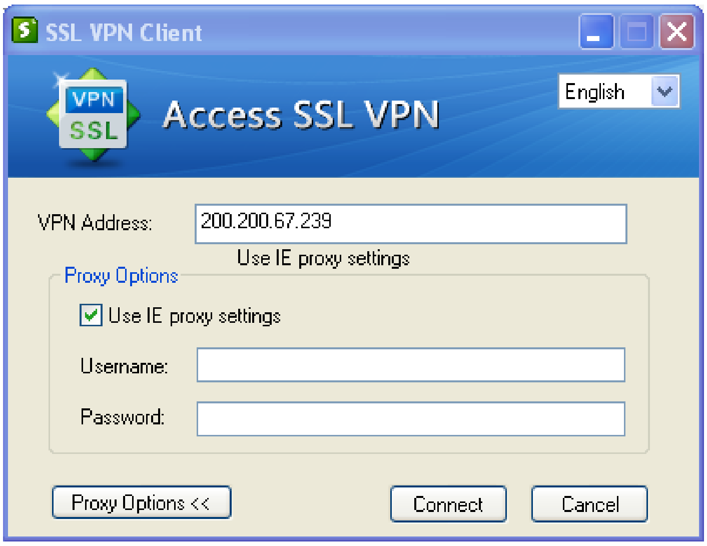


3. Enter the address of the SSL VPN, as shown below:



VPN Address: 200.200.67.239

4. Click the **Proxy Options** button and decide whether to use IE proxy settings. To use IE HTTP proxy server to connect TCP applications, select the option **Use IE proxy settings** and enter the username and password of the proxy server, as shown in the figure below:



SSL VPN Client

Access SSL VPN

English

VPN Address: 200.200.67.239

Use IE proxy settings

Proxy Options

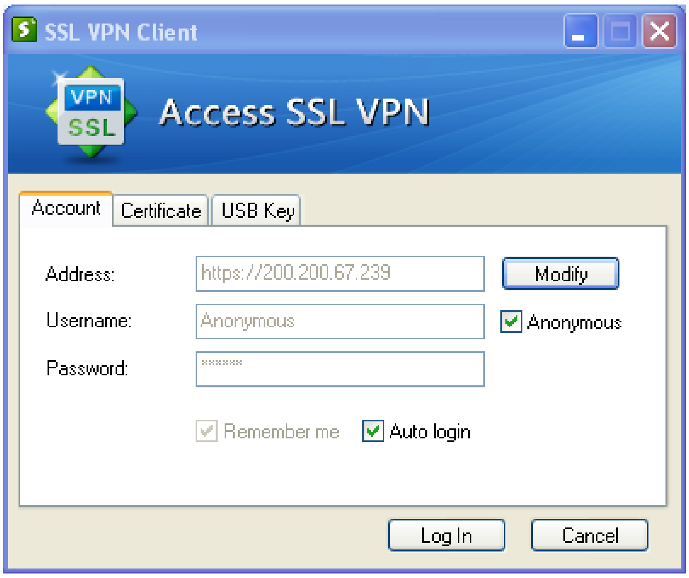
☑ Use IE proxy settings

Username:

Password:

5. Click the **Connect** button to enter the login page. On the login page, there are three tabs and contents on different tabs vary from authentication methods.

For authentication based on username and password, select **Account**. The **Account** tab is as shown in the figure below:



SSL VPN Client

Access SSL VPN

Account | Certificate | USB Key

Address: https://200.200.67.239

Username: Anonymous ☑ Anonymous

Password: ******

☑ Remember me ☑ Auto login

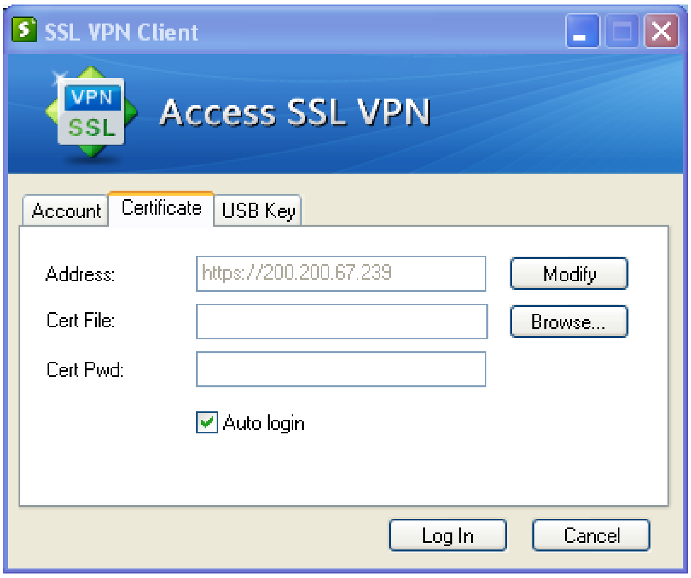
The following are the contents included on the **Account** tab:

- **Address:** Address of the SSL VPN.
- **Modify:** Click this button to modify the address of SSL VPN.
- **Username, Password:** Enter the username and password of the SSL VPN account respectively.
- **Anonymous:** If this option is selected, the user will use the default anonymous login account to access the SSL VPN.
- **Remember me:** If it is selected, the username and password will be automatically filled into the fields when user uses SSL VPN Client to connect SSL VPN next time.

- **Auto login:** If it is selected, the user will connect to SSL VPN directly next time when start SSL VPN. This option works in association with the **Remember me** option.

Please note that **word verification** must not be enabled; otherwise, auto-login feature will not take effect.

For authentication based on certificate, select **Certificate**. The **Certificate** tab is as shown in the figure below:



Address: https://200.200.67.239

Cert File:

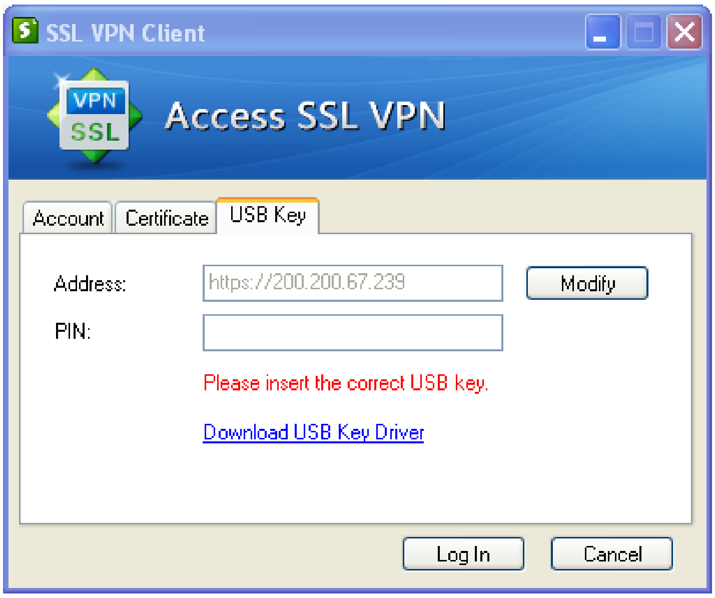
Cert Pwd:

☑ Auto login

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

- **Address:** Address of the SSL VPN.
- **Modify:** Click this button to modify the address of SSL VPN.
- **Cert File:** Browse and select the certificate used for SSL VPN access. This certificate should be the certificate binding to the SSL VPN account.
- **Cert Pwd:** Enter the password of the certificate file.
- **Anonymous:** If this option is selected, the user will use the default anonymous login account to access the SSL VPN.
- **Auto login:** If it is selected, the user will connect to SSL VPN directly next time when start SSL VPN.

For authentication based on USB key, select **USB Key**. The **USB Key** tab is as shown below:



Address: https://200.200.67.239

PIN:

Please insert the correct USB key.

Download USB Key Driver

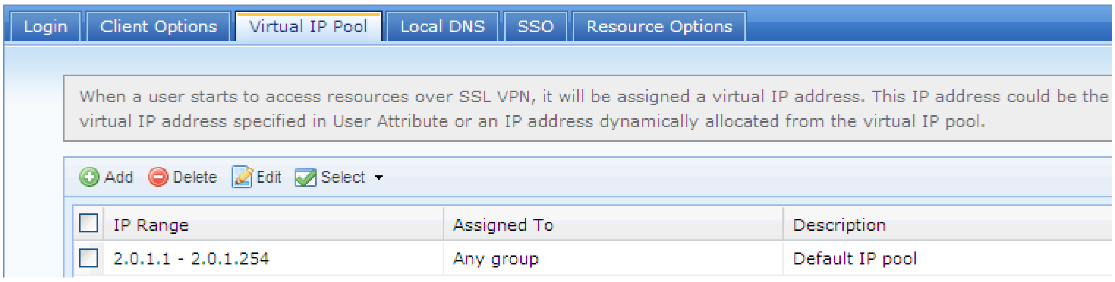
The following are the contents included on the **USB Key** tab:

- **Address:** Address of the SSL VPN.
- **Modify:** Click this button to modify the address of SSL VPN.
- **PIN:** Enter PIN of the USB key after inserting the USB key into PC’s USB port.
- **Download USB Key Driver:** For non driver-free USB key, connecting user needs to download and install the USB key driver to have USB key based authentication method work.

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:



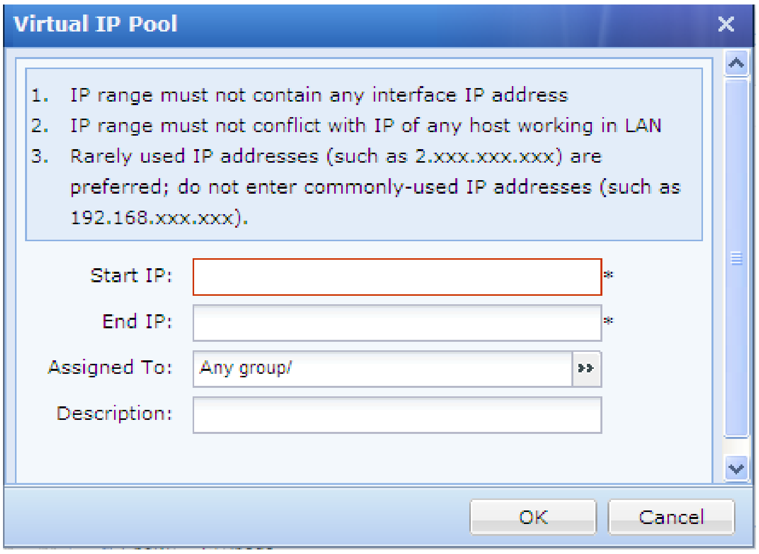
When a user starts to access resources over SSL VPN, it will be assigned a virtual IP address. This IP address could be the virtual IP address specified in User Attribute or an IP address dynamically allocated from the virtual IP pool.

□	IP Range	Assigned To	Description
□	2.0.1.1 - 2.0.1.254	Any group	Default IP pool

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:



Virtual IP Pool

1. IP range must not contain any interface IP address
2. IP range must not conflict with IP of any host working in LAN
3. Rarely used IP addresses (such as 2.xxx.xxx.xxx) are preferred; do not enter commonly-used IP addresses (such as 192.168.xxx.xxx).

Start IP: *

End IP: *

Assigned To: Any group/

Description:

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

⚠

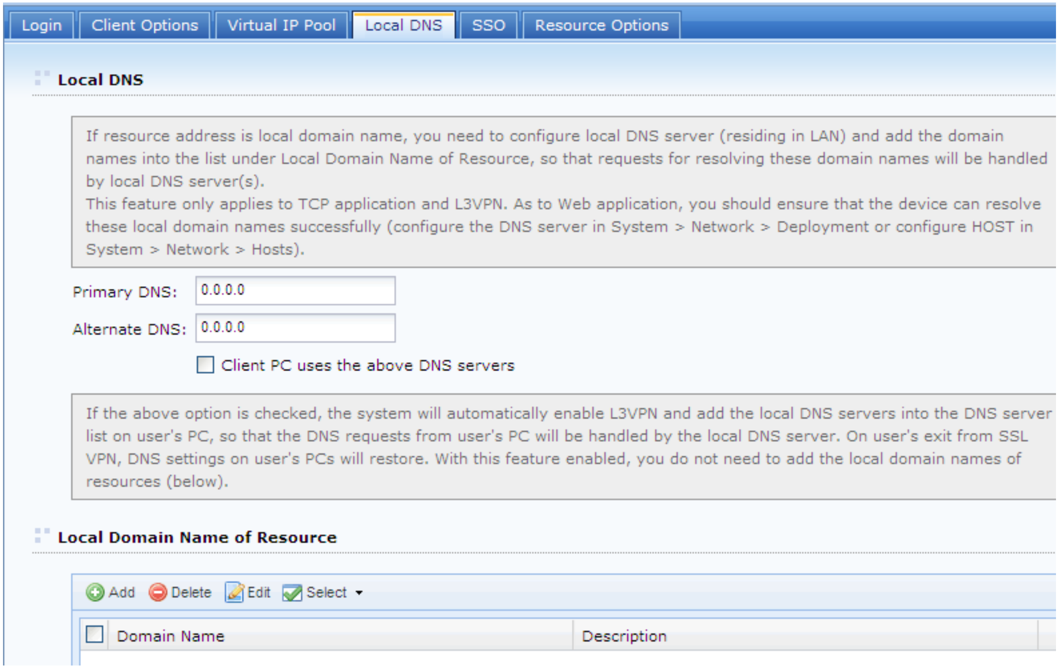
The IP ranges should not cover IP address of any network interface of the Sangfor device, or conflict with IP address of any running machine in the local area network.

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:



Local DNS

If resource address is local domain name, you need to configure local DNS server (residing in LAN) and add the domain names into the list under Local Domain Name of Resource, so that requests for resolving these domain names will be handled by local DNS server(s).
This feature only applies to TCP application and L3VPN. As to Web application, you should ensure that the device can resolve these local domain names successfully (configure the DNS server in System > Network > Deployment or configure HOST in System > Network > Hosts).

Primary DNS: 0.0.0.0

Alternate DNS: 0.0.0.0

□ Client PC uses the above DNS servers

If the above option is checked, the system will automatically enable L3VPN and add the local DNS servers into the DNS server list on user's PC, so that the DNS requests from user's PC will be handled by the local DNS server. On user's exit from SSL VPN, DNS settings on user's PCs will restore. With this feature enabled, you do not need to add the local domain names of resources (below).

Local Domain Name of Resource

□	Domain Name	Description

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.

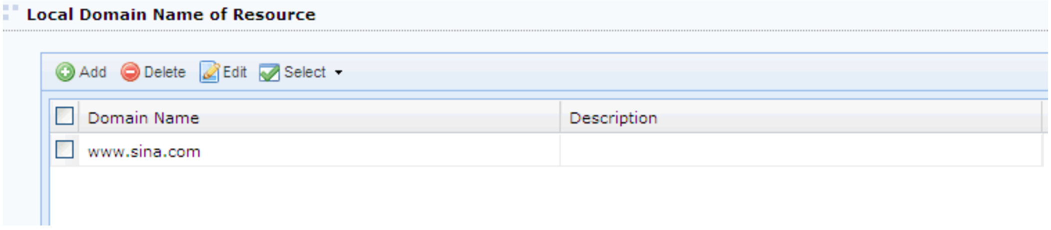
   If there is only one local DNS server, enter the server address into the **Primary DNS** field.

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 names 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.

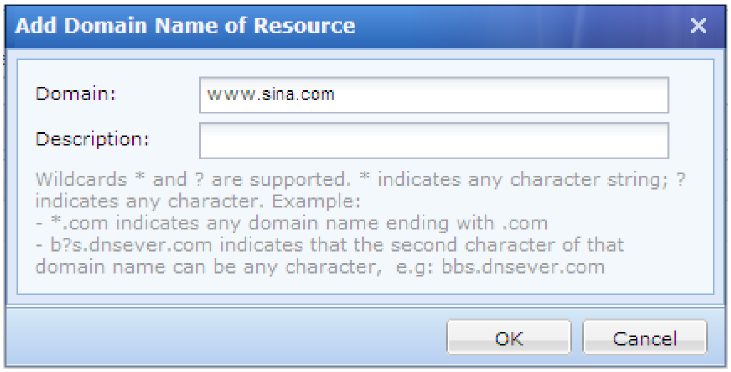


□	Domain Name	Description
□	www.sina.com	

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**end add enter the domain name of a resource, as shown below:



Domain: www.sina.com

Description:

Wildcards * and ? are supported. * indicates any character string; ? indicates any character. Example:
- *.com indicates any domain name ending with .com
- b?s.dnsever.com indicates that the second character of that domain name can be any character, e.g: bbs.dnsever.com

Make sure that the address is in form of IP address when configuring the address of the resource (refer to the Resource sectioning 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)sectioning Chapter 3).

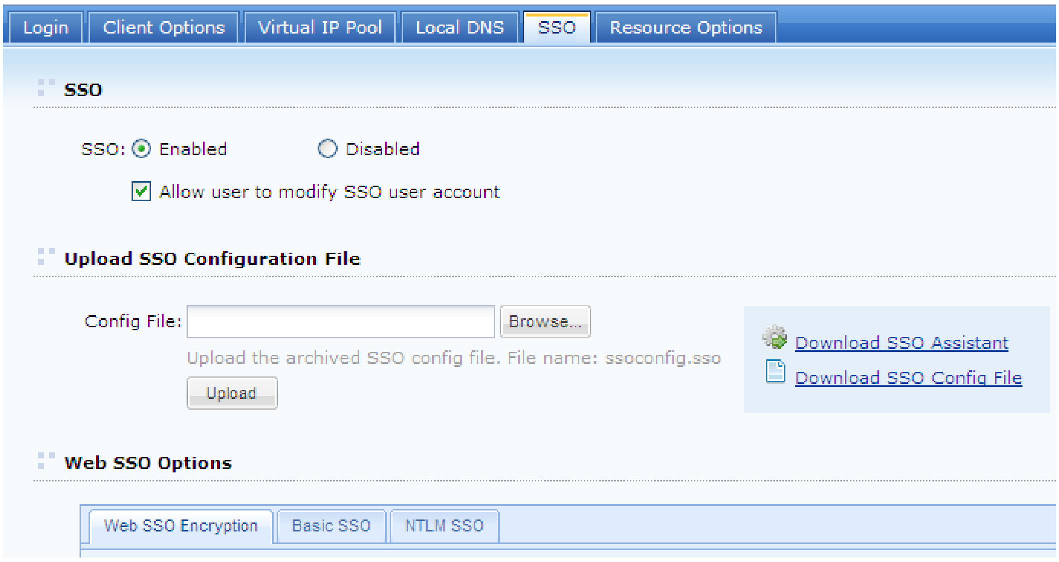
- If address of some resources are domain names and there is a specific DNS server in the local area network providing domain name resolving services, the domain name of that resource is recommended to be added to the list. That will have the requests of DNS handled preferentially by the local DNS server. 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.

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:



SSO

SSO: ● Enabled ○ Disabled

☑ Allow user to modify SSO user account

Upload SSO Configuration File

Config File:

Upload the archived SSO config file. File name: ssoconfig.sso

Download SSO Assistant

Download SSO Config File

Web SSO Options

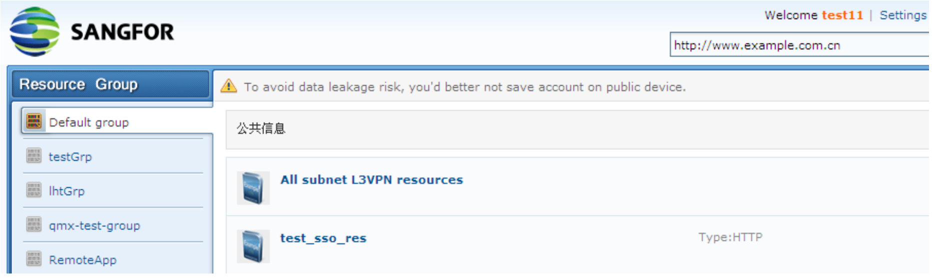
2. Configure the fields under **SSO** and **Upload SSO Configuration File**.

- **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 SSO Configuration File:**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:



SANGFOR

Welcome test11 | Settings

http://www.example.com.cn

Resource Group

To avoid data leakage risk, you'd better not save account on public device.

Default group

testGrp

lhtGrp

qmx-test-group

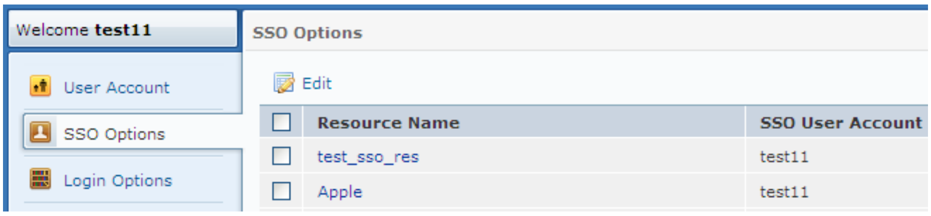
RemoteApp

公共信息

All subnet L3VPN resources

test_sso_res Type:HTTP

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



Welcome test11

User Account

SSO Options

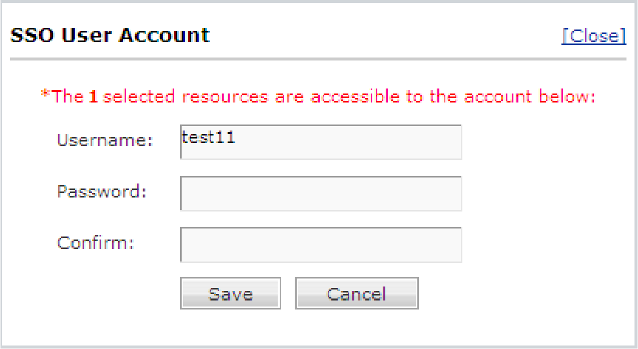
Login Options

SSO Options

Edit

□	Resource Name	SSO User Account
□	test_sso_res	test11
□	Apple	test11

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



SSO User Account [Close]

*The 1 selected resources are accessible to the account below:

Username: test11

Password:

Confirm:

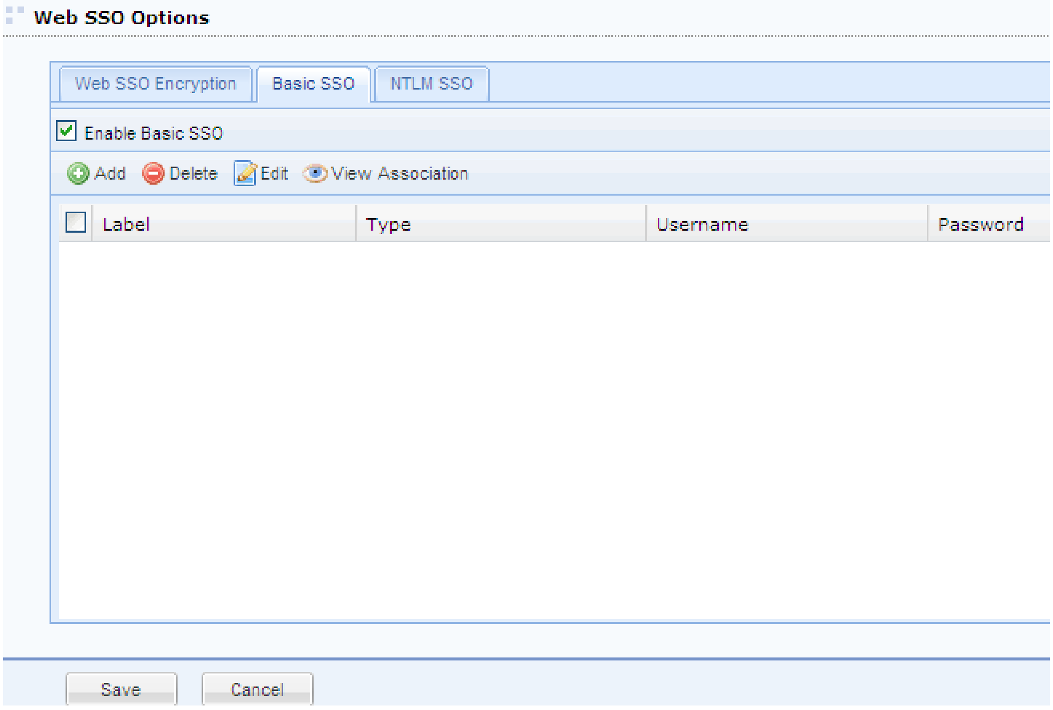
Save Cancel

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.

3. Configure **Web SSO Options**.



Web SSO Options

□	Label	Type	Username	Password

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

- **Web 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**.
- **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**.

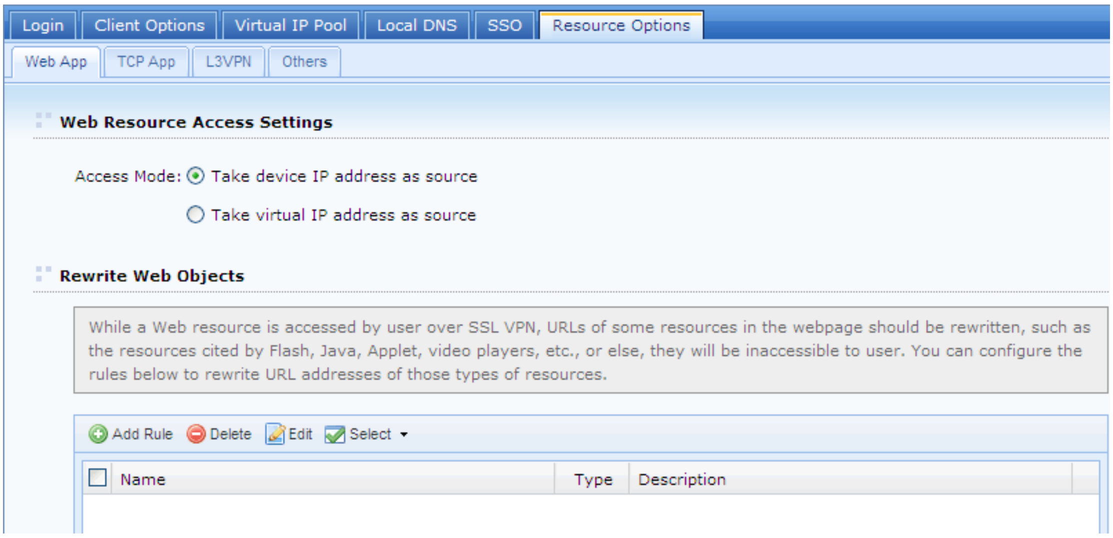
4. Click the **Save** button and **Apply** button to save and apply the settings.

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

Navigate to **System**>**SSL VPN Options**>**General**>**Resource Options**>**Web Apt**os configure the parameters related to Web resource access and object rewritten rule, as shown in the figure below:



Web Resource Access Settings

Access Mode: ● Take device IP address as source

○ Take virtual IP address as source

Rewrite Web Objects

While a Web resource is accessed by user over SSL VPN, URLs of some resources in the webpage should be rewritten, such as the resources cited by Flash, Java, Applet, video players, etc., or else, they will be inaccessible to user. You can configure the rules below to rewrite URL addresses of those types of resources.

□ Name	Type	Description

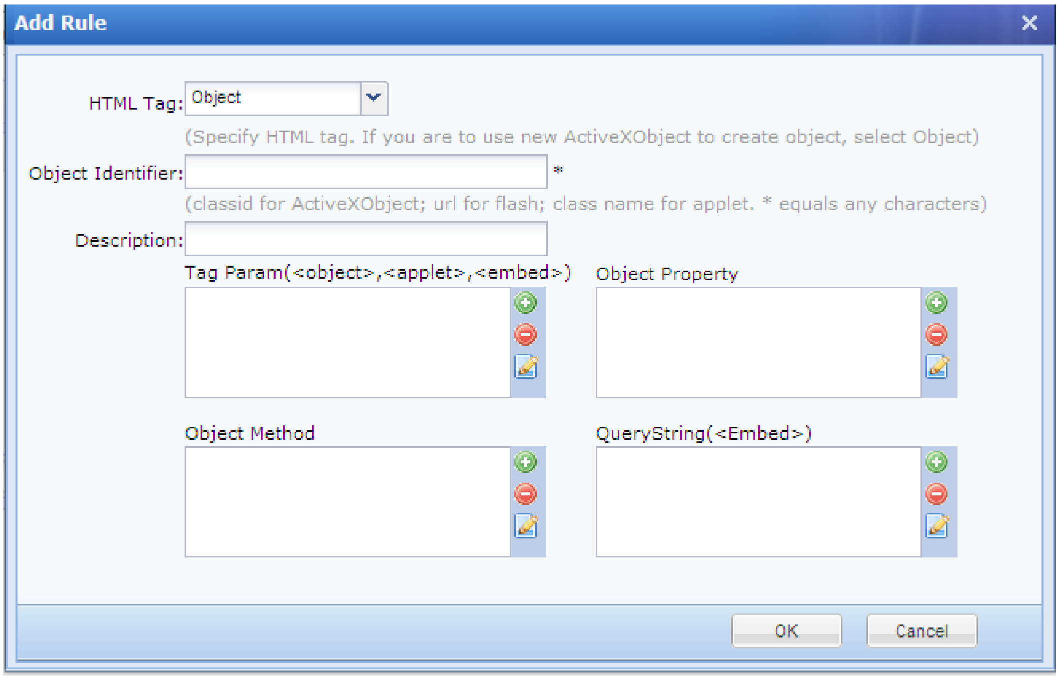
The following are the contents included on the **Resource Options** page:

- **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 sectioning 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 sectioning Chapter 3).

- **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:



Add Rule

HTML Tag: Object

(Specify HTML tag. If you are to use new ActiveXObject to create object, select Object)

Object Identifier: *

(classid for ActiveXObject; url for flash; class name for applet. * equals any characters)

Description:

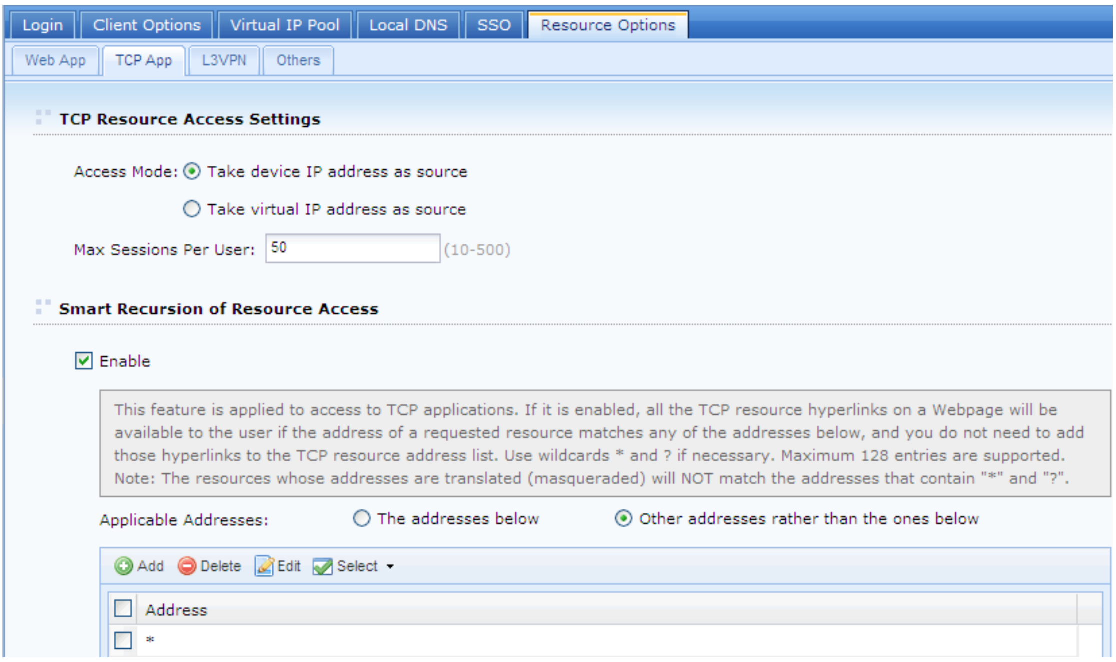
The following are the contents included on **Add Rule** page:

- **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.
- **Query String(<Embed>):**Specifies the Query strings 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.

TCP App Resource Options

Navigate to **System**>**SSL VPNOption**>**System**>**Resource Options**>**TCP App**to configurethe parameters related to TCP resource access and smart recursion feature, as shown below:



TCP Resource Access Settings

Access Mode: ● Take device IP address as source

○ Take virtual IP address as source

Max Sessions Per User: 50 (10-500)

Smart Recursion of Resource Access

☑ Enable

This feature is applied to access to TCP applications. If it is enabled, all the TCP resource hyperlinks on a Webpage will be available to the user if the address of a requested resource matches any of the addresses below, and you do not need to add those hyperlinks to the TCP resource address list. Use wildcards * and ? if necessary. Maximum 128 entries are supported. Note: The resources whose addresses are translated (masqueraded) will NOT match the addresses that contain "*" and "?".

Applicable Addresses: ○ The addresses below ● Other addresses rather than the ones below

□	Address
□	*

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 sectioning 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**.

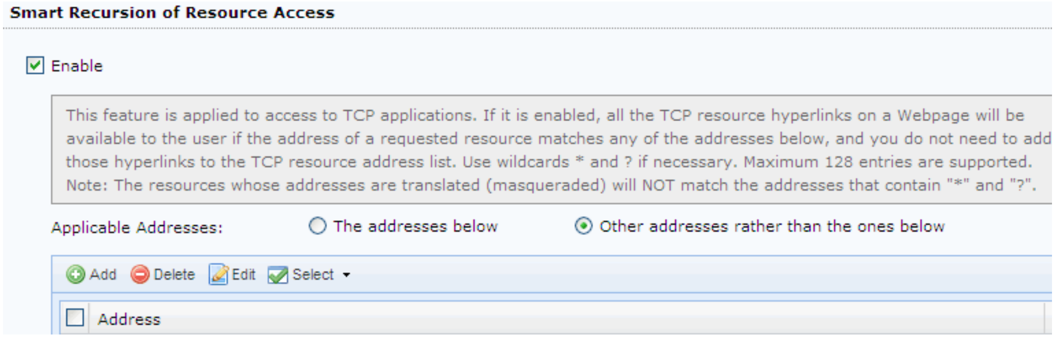
  To have the connecting users take the assigned virtual IP address as the source address to visit the server resources, select **Take virtual IP address as source** (to configure virtual IP address, refer to the Configuring Virtual IP sectioning Chapter 3).

- **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, **Enable** 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.



Smart Recursion of Resource Access

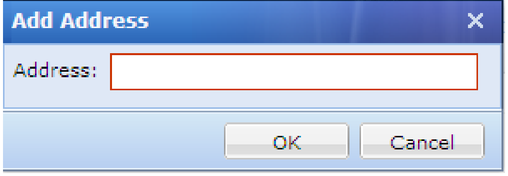
☑ Enable

This feature is applied to access to TCP applications. If it is enabled, all the TCP resource hyperlinks on a Webpage will be available to the user if the address of a requested resource matches any of the addresses below, and you do not need to add those hyperlinks to the TCP resource address list. Use wildcards * and ? if necessary. Maximum 128 entries are supported. Note: The resources whose addresses are translated (masqueraded) will NOT match the addresses that contain "*" and "?".

Applicable Addresses: ○ The addresses below ● Other addresses rather than the ones below

□ Address

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



Add Address

Address:

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 onein 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**ss** **VPN**>**Resources**>**Resource Management** 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**>**Others.** 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:

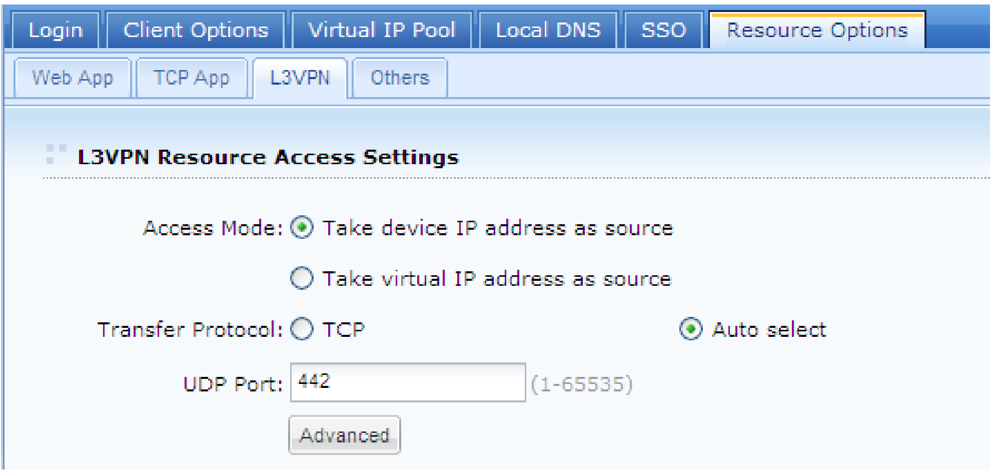
1. Navigate to **SSL VPN**>**Resources**, and click **Add**>**TCP app** to add the TCP resource of library homepage.
2. Configure the required fields and add library homepage (*www.library.com*) into the textbox next to the **Address** field.
3. Click **Others** tab and select the option **Apply smart recursion**.
4. Navigate to **System**>**SSL VPN Options**>**General**>**Resource Options**>**TCP App** and select **Enable**.
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:



L3VPN Resource Access Settings

Access Mode: ● Take device IP address as source
○ Take virtual IP address as source

Transfer Protocol: ○ TCP ● Auto select

UDP Port: 442 (1-65535)

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 sectioning 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 sectioning 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 sin **Single-arm** mode, this port should be mapped from the front-end firewall to the Sangfor device.

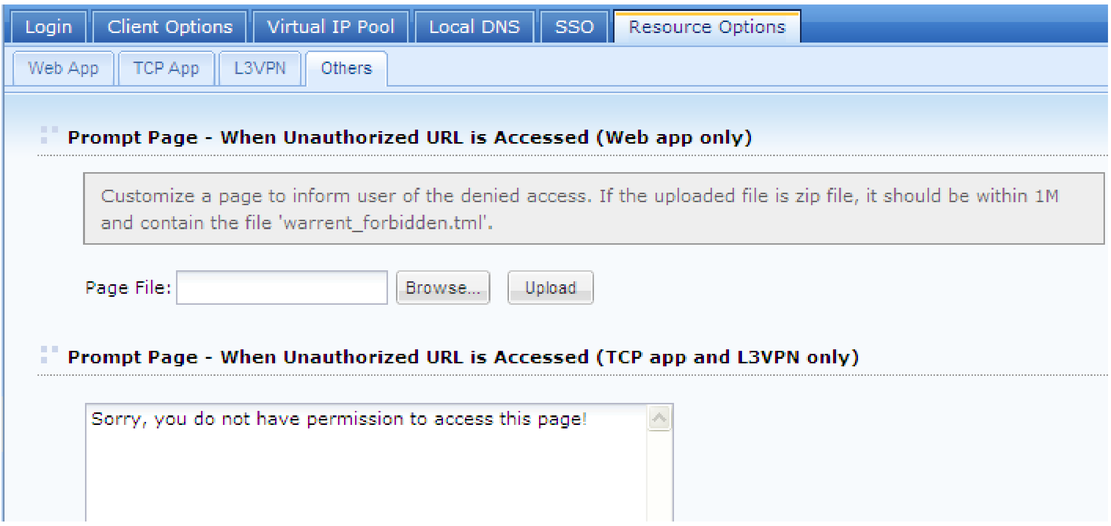
- **Advanced:** Click this button and optional advanced options appears, **ax Concurrent Users** and**IP of Local Virtual NIC**. The latter specifies the server-end IP address range to which the virtual NIC is applied.

⚠

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

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:



Prompt Page - When Unauthorized URL is Accessed (Web app only)

Customize a page to inform user of the denied access. If the uploaded file is zip file, it should be within 1M and contain the file 'warrent_forbidden.tml'.

Page File:

Prompt Page - When Unauthorized URL is Accessed (TCP app and L3VPN only)

Sorry, you do not have permission to access this page!

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 text box 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**.

💡

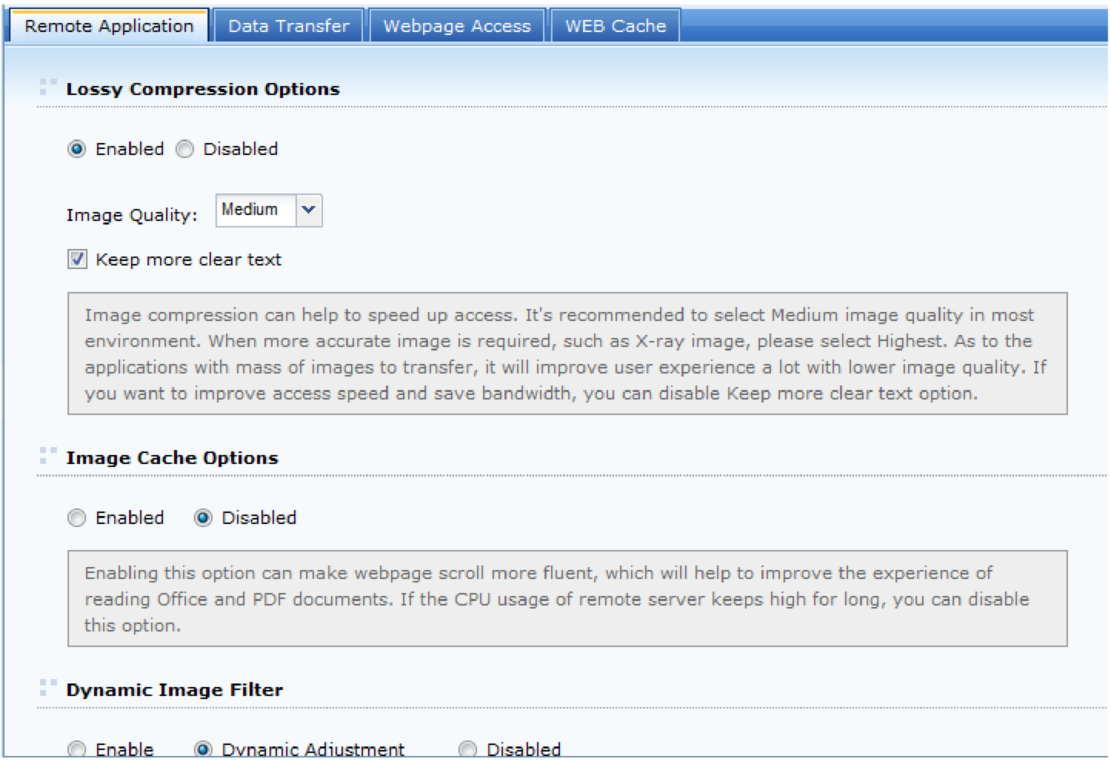
Unauthorized or authorized URL addresses are configured on **URL Access Control** tab while editing a Web/TCP/L3VPN resource (refer to the Resource sectioning Chapter 4).

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 data transfer, webpage access and Web cache.

Application Access

Navigate to **System**>**SSL VPN Options**>**Network Optimization** enter the page. The page shown below:



Lossy Compression Options

● Enabled ○ Disabled

Image Quality: Medium

☑ Keep more clear text

Image compression can help to speed up access. It's recommended to select Medium image quality in most environment. When more accurate image is required, such as X-ray image, please select Highest. As to the applications with mass of images to transfer, it will improve user experience a lot with lower image quality. If you want to improve access speed and save bandwidth, you can disable Keep more clear text option.

Image Cache Options

○ Enabled ● Disabled

Enabling this option can make webpage scroll more fluent, which will help to improve the experience of reading Office and PDF documents. If the CPU usage of remote server keeps high for long, you can disable this option.

Dynamic Image Filter

○ Enable ● Dynamic Adjustment ○ Disabled

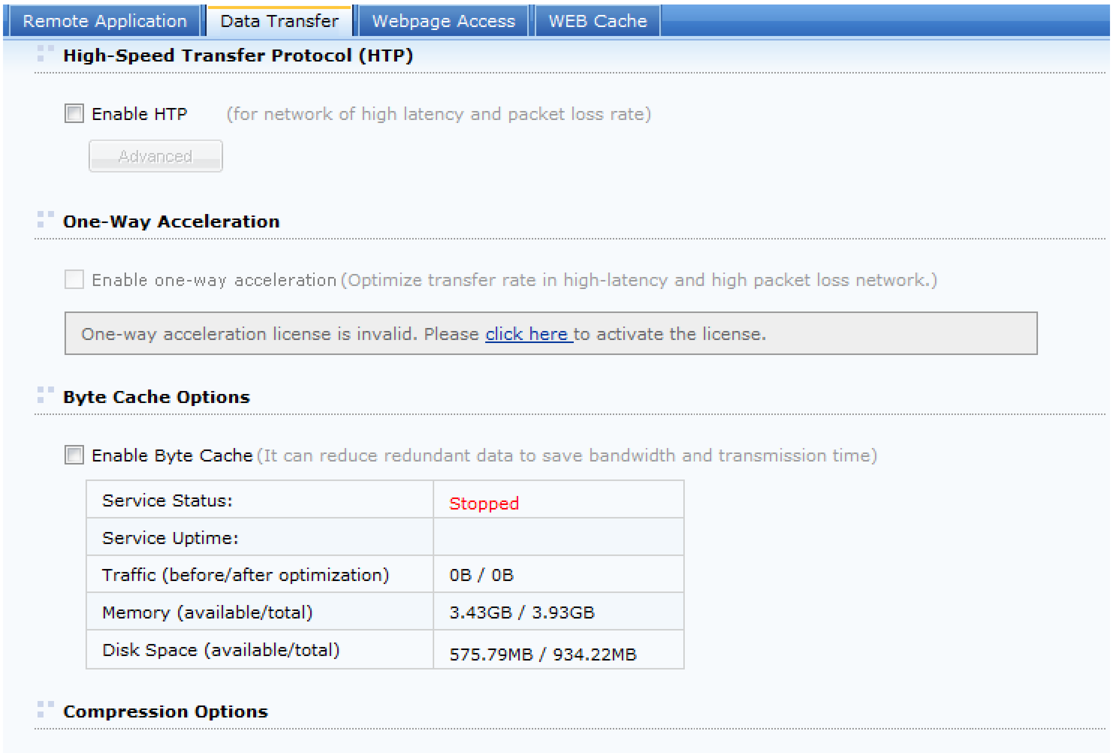
Loss Compression Options – After enable, Remote application displayed image will be compressed according to the quality level is set to improve the transmission efficiency.

Image Cache Options – After enable, Remote application will image cache to refresh the effect of improving the image scrolling.

Dynamic Image Filter - For remote applications, FLASH animation motion picture will be filtered in order to save bandwidth and improve application access speed.

Data Transfer Optimization

The **Data Transfer** page is as shown below:



High-Speed Transfer Protocol (HTP)

□ Enable HTP (for network of high latency and packet loss rate)

One-Way Acceleration

□ Enable one-way acceleration (Optimize transfer rate in high-latency and high packet loss network.)

One-way acceleration license is invalid. Please click here to activate the license.

Byte Cache Options

□ Enable Byte Cache (It can reduce redundant data to save bandwidth and transmission time)

Service Status:	Stopped
Service Uptime:	
Traffic (before/after optimization)	0B / 0B
Memory (available/total)	3.43GB / 3.93GB
Disk Space (available/total)	575.79MB / 934.22MB

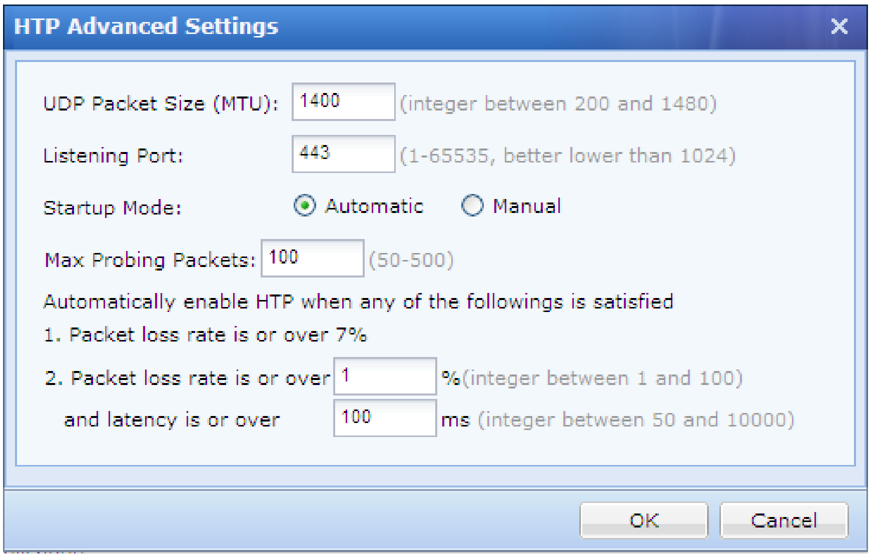
Compression Options

The following are the contents included on **Data Transfer** page:

- **Enable HTP:** Select this option if the client end is 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:



UDP Packet Size (MTU): 1400 (integer between 200 and 1480)

Listening Port: 443 (1-65535, better lower than 1024)

Startup Mode: ● Automatic ○ Manual

Max Probing Packets: 100 (50-500)

Automatically enable HTP when any of the followings is satisfied

1. Packet loss rate is or over 7%

2. Packet loss rate is or over 1 %(integer between 1 and 100)

and latency is or over 100 ms (integer between 50 and 10000)

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

If **Manual**s selected, HTP needs to be started by hand. If **Automatic**s 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.

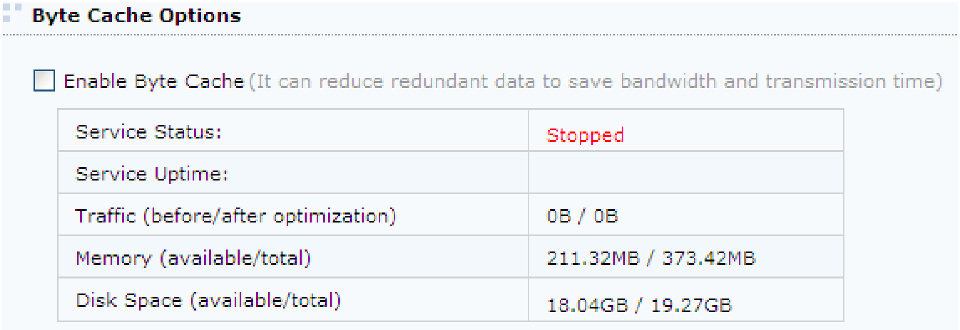
Network state detection is based on the two conditions: a). **Packet loss rate is or over 7%**; b).**Packet loss rate is or over _ % and latency is or over _ ms**. Either condition may trigger start up of HTP. Generally, defaults are recommended to be adopted.

⚠

- **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**: Select this option will get optimize transfer rate in high-latency and high packet loss network.

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

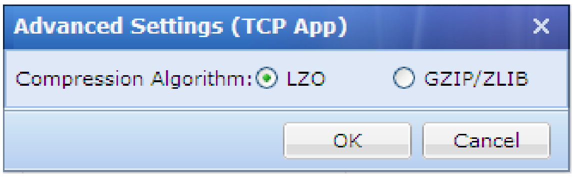


Byte Cache Options

□ Enable Byte Cache (It can reduce redundant data to save bandwidth and transmission time)

Service Status:	Stopped
Service Uptime:	
Traffic (before/after optimization)	0B / 0B
Memory (available/total)	211.32MB / 373.42MB
Disk Space (available/total)	18.04GB / 19.27GB

- **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:



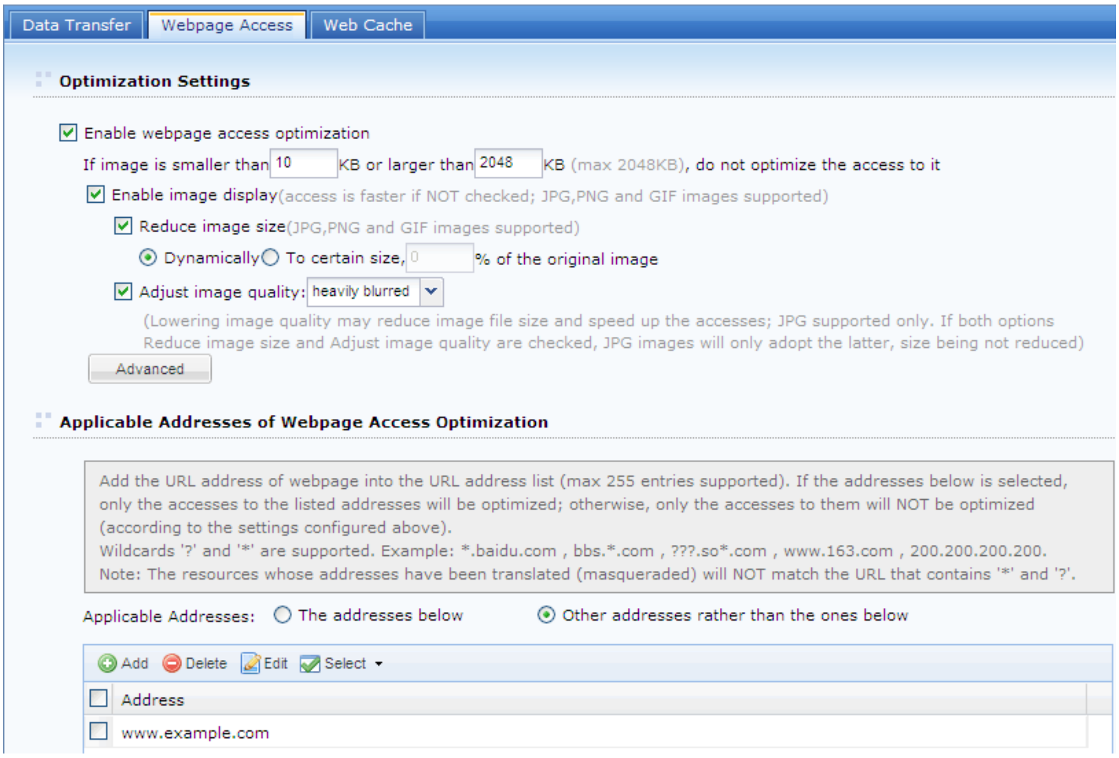
Advanced Settings (TCP App)

Compression Algorithm: ● LZO ○ GZIP/ZLIB

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 isan ideal feature for the users who are using PDA (Personal Digital Assistant) to access SSL VPN or the user’s computer is inpoor network. This feature should not be enabled for users in good network environment.

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



Optimization Settings

☑ Enable webpage access optimization

If image is smaller than 10 KB or larger than 2048 KB (max 2048KB), do not optimize the access to it

☑ Enable image display(access is faster if NOT checked; JPG,PNG and GIF images supported)

☑ Reduce image size(JPG,PNG and GIF images supported)

● Dynamically ○ To certain size, 0 % of the original image

☑ Adjust image quality: heavily blurred

(Lowering image quality may reduce image file size and speed up the accesses; JPG supported only. If both options Reduce image size and Adjust image quality are checked, JPG images will only adopt the latter, size being not reduced)

Advanced

Applicable Addresses of Webpage Access Optimization

Add the URL address of webpage into the URL address list (max 255 entries supported). If the addresses below is selected, only the accesses to the listed addresses will be optimized; otherwise, only the accesses to them will NOT be optimized (according to the settings configured above).
Wildcards '?' and '*' are supported. Example: *.baidu.com , bbs.*.com , ???.so*.com , www.163.com , 200.200.200.200.
Note: The resources whose addresses have been translated (masqueraded) will NOT match the URL that contains '*' and '?'.

Applicable Addresses: ○ The addresses below ● Other addresses rather than the ones below

□	Address
□	www.example.com

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

- **Enable webpage access optimization:** 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 **Images smaller than_ KB** and **or larger than _ KB**.
- **Enable image display:** Uncheck this option to disable image display and therefore enhance the access speed.

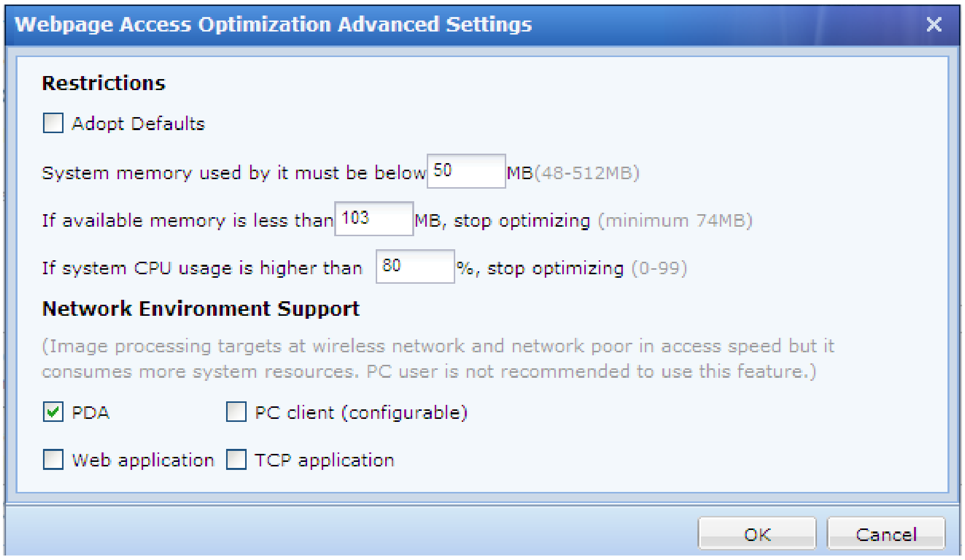
  - **Enable image display** only applies to the images with any of the following extensions:.jpg, .png and .gif.
  - **Enable image display** achieves the opposite optimization effect, comparing with the effect that **Adjust image quality** achieves.

- **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 ithelps 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:



Webpage Access Optimization Advanced Settings

Restrictions

□ Adopt Defaults

System memory used by it must be below 50 MB(48-512MB)

If available memory is less than 103 MB, stop optimizing (minimum 74MB)

If system CPU usage is higher than 80 %, stop optimizing (0-99)

Network Environment Support

(Image processing targets at wireless network and network poor in access speed but it consumes more system resources. PC user is not recommended to use this feature.)

☑ PDA □ PC client (configurable)

□ Web application □ TCP application

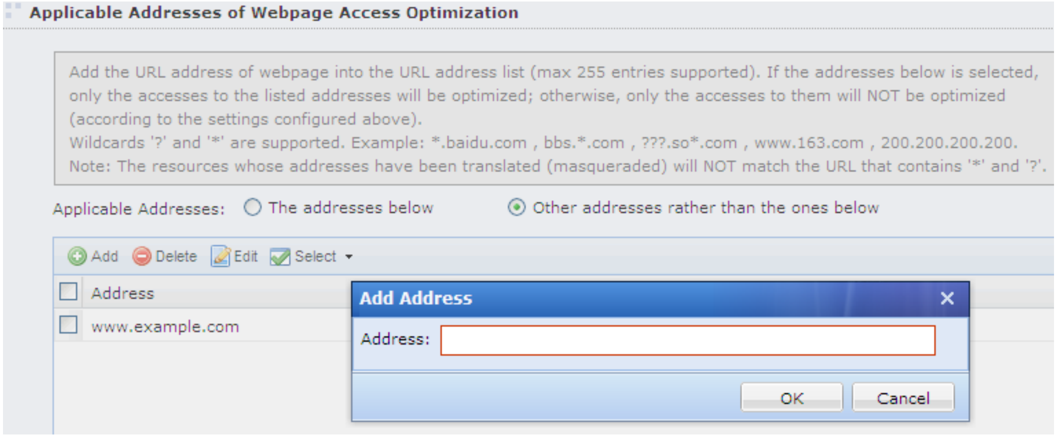
  - **Restrictions:** Indicates the thresholds determining when webpage access optimization functionality will start up. These thresholds could minimize the impact that webpage access optimization poses on the running and performance of other modules. The restrictions include those on **system memory**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



Applicable Addresses of Webpage Access Optimization

Add the URL address of webpage into the URL address list (max 255 entries supported). If the addresses below is selected, only the accesses to the listed addresses will be optimized; otherwise, only the accesses to them will NOT be optimized (according to the settings configured above).
Wildcards '?' and '*' are supported. Example: *.baidu.com , bbs.*.com , ???.so*.com , www.163.com , 200.200.200.200.
Note: The resources whose addresses have been translated (masqueraded) will NOT match the URL that contains '*' and '?'.

Applicable Addresses: ○ The addresses below ● Other addresses rather than the ones below

□ Address
□ www.example.com

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

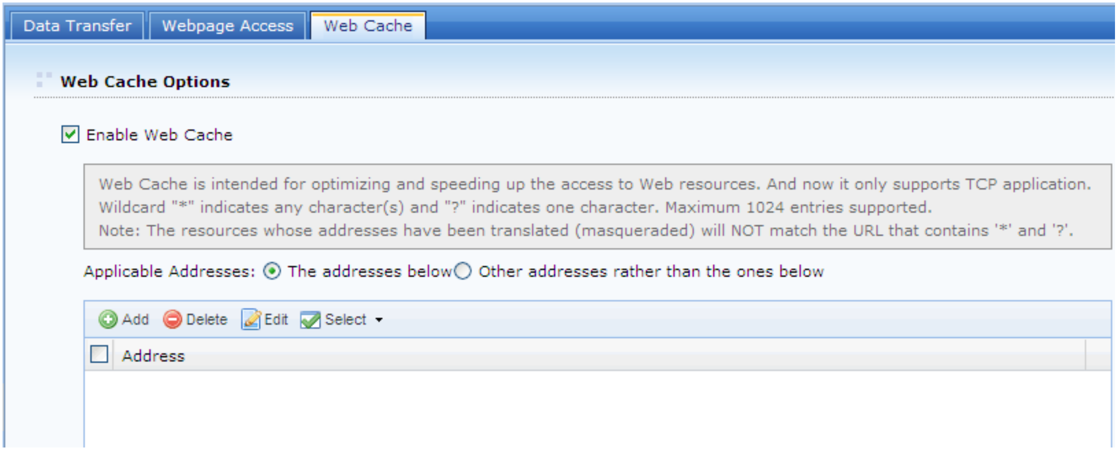
- **Applicable addresses:** If**the addresses below** is selected, only the access to the added URL addresses will be optimized. If **other addresses rather than the ones below** is selected, access to any other URL addresses (except the added addresses) will be optimized.
- **Add:** Click it to add 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:



Web Cache Options

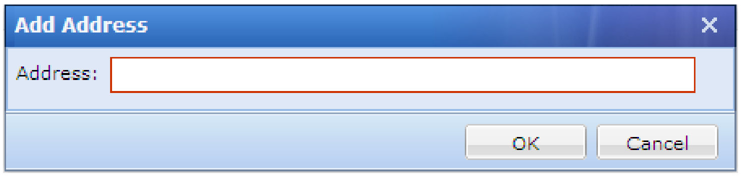
☑ Enable Web Cache

Web Cache is intended for optimizing and speeding up the access to Web resources. And now it only supports TCP application. Wildcard "*" indicates any character(s) and "?" indicates one character. Maximum 1024 entries supported.
Note: The resources whose addresses have been translated (masqueraded) will NOT match the URL that contains '*' and '?'.

Applicable Addresses: ● The addresses below ○ Other addresses rather than the ones below

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

- **Enable Web Cache:** 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.

⚠

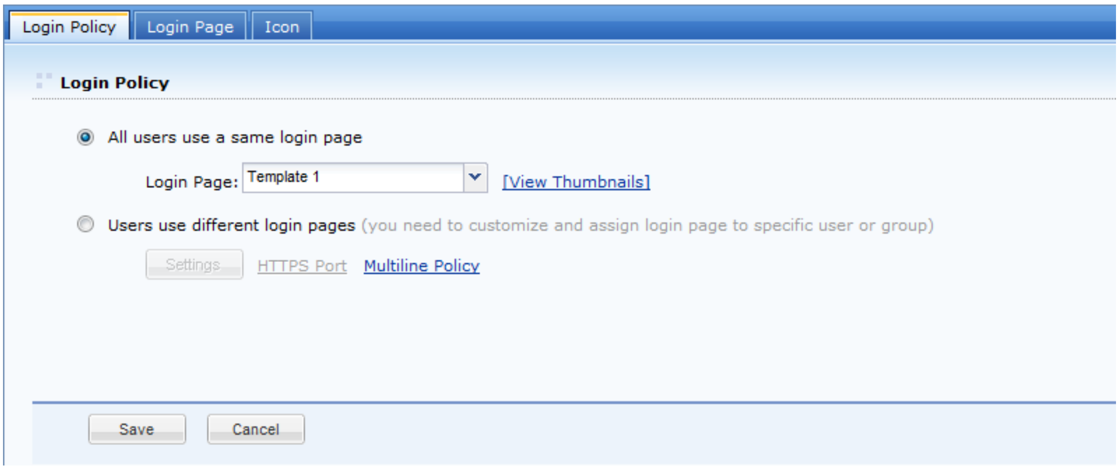
- At present, it only supports HTTP type of TCP application.
- Wildcards "?" and "*", and a maximum of 255 entries are supported.

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.



Login Policy

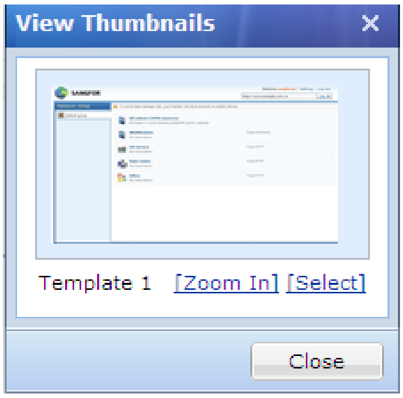
● All users use a same login page

Login Page: Template 1 [View Thumbnails]

○ Users use different login pages (you need to customize and assign login page to specific user or group)

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 pager accustom login page.
- **View Thumbnails:** Click to view thumbnails of the built-in page template, as shown below:

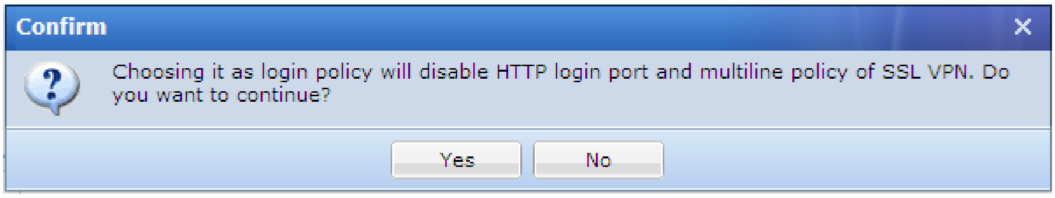


- **Default Login Method:** Specifies the default login method applied to connecting users. Options are **Any**, **Use password**, **Use certificate** and **Use USB key**.

If anonymous logon is enabled, the default login method is not selective.

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:

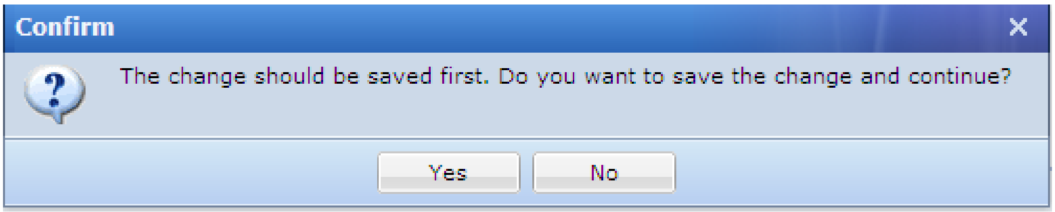
1. Click the **Yes** button to confirm choosing **Users use different login pages** as the policy selected. As shown in the following prompt, the HTTP login port and multiline policy of SSL VPN will be disabled.



Confirm

Choosing it as login policy will disable HTTP login port and multiline policy of SSL VPN. Do you want to continue?

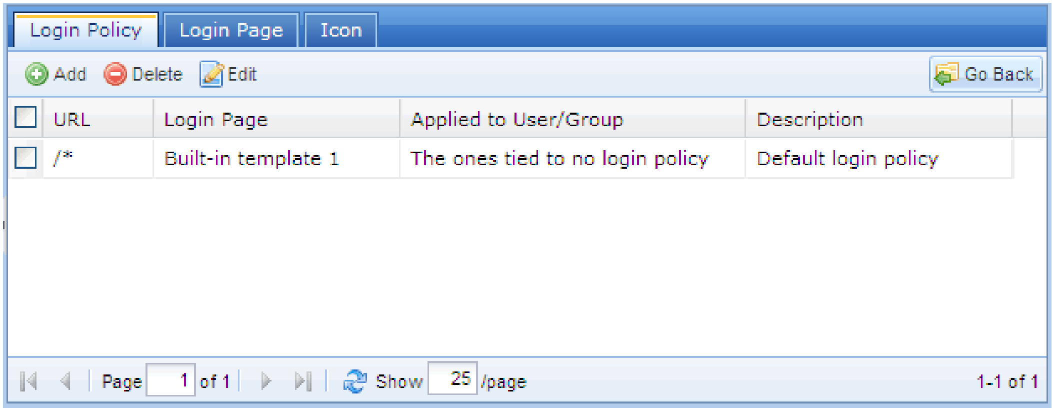
2. Clickthe **Configure** button on the **Login Policy** page to customize login pages and assign them to specific users/groups. If change is not saved, the following prompt will pop up:



Confirm

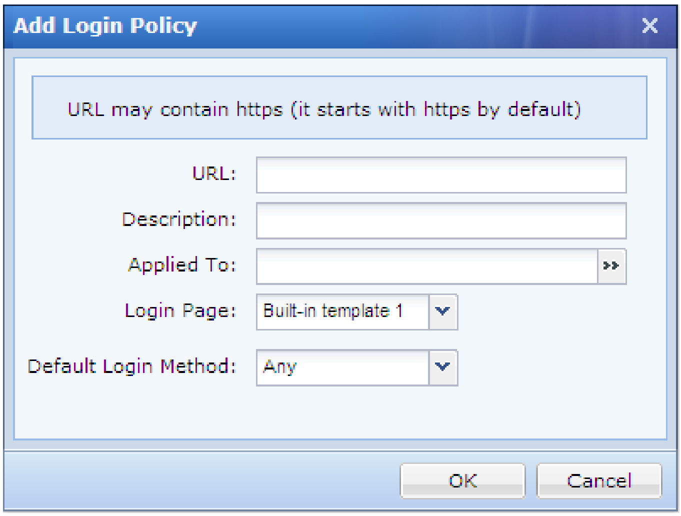
The change should be saved first. Do you want to save the change and continue?

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



☐	URL	Login Page	Applied to User/Group	Description
☐	/*	Built-in template 1	The ones tied to no login policy	Default login policy

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



Add Login Policy

URL may contain https (it starts with https by default)

URL:

Description:

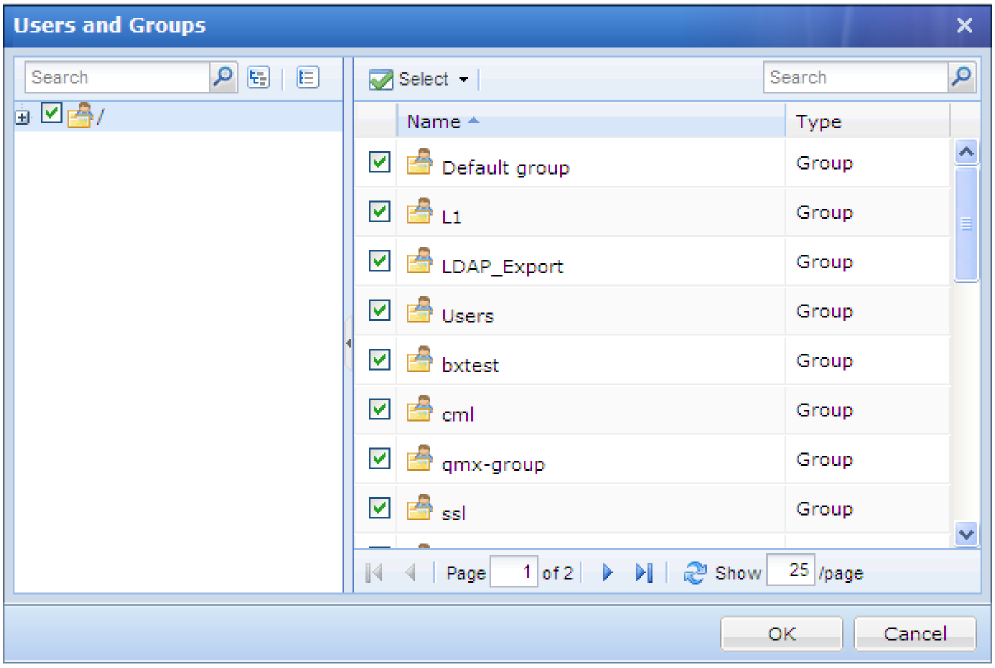
Applied To:

Login Page: Built-in template 1

Default Login Method: Any

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:



Users and Groups

	Name	Type
☑	Default group	Group
☑	L1	Group
☑	LDAP_Export	Group
☑	Users	Group
☑	bxtest	Group
☑	cml	Group
☑	qmx-group	Group
☑	ssl	Group

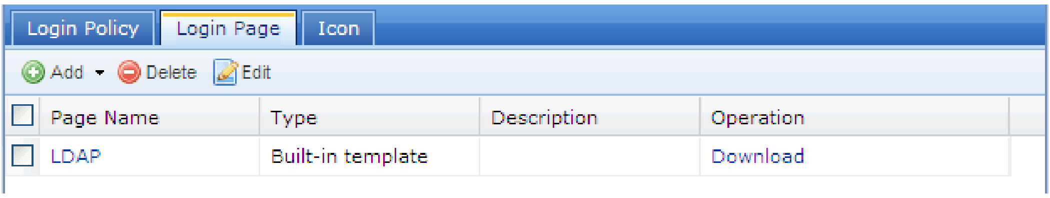
Select the desired users or groups to associate them with this login policy and click **OK**.

- **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.
- **Default Login Method:** Specifies the default login method applied to the specified users or groups. Options are **Any**, **Use password**, **Use certificate** and **Use USB key**.

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.

Configuring Login Page

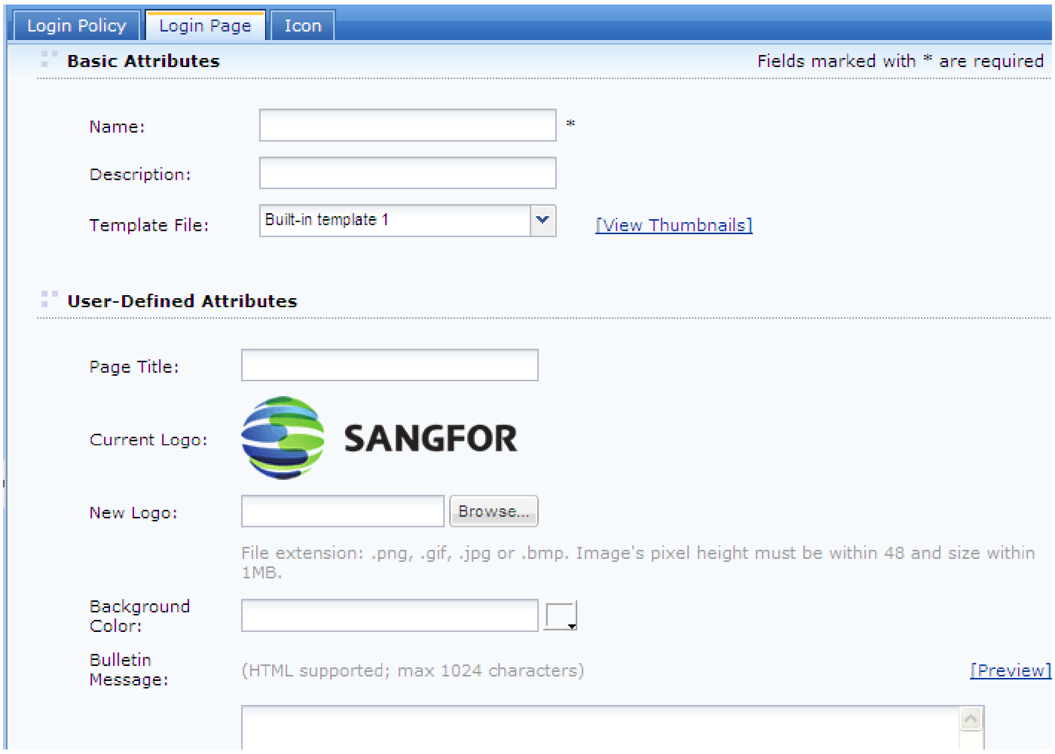
1. Navigate to **System**>**SSL VPN Options**>**Login Policy**>**Login Page**. The **Login Page** is as shown in the figure below:



□	Page Name	Type	Description	Operation
□	LDAP	Built-in template		Download

2. Click **Add** >**By using built-in template** to use built-item plateas 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:



Basic Attributes

Fields marked with * are required

Name: *

Description:

Template File: Built-in template 1

User-Defined Attributes

Page Title:

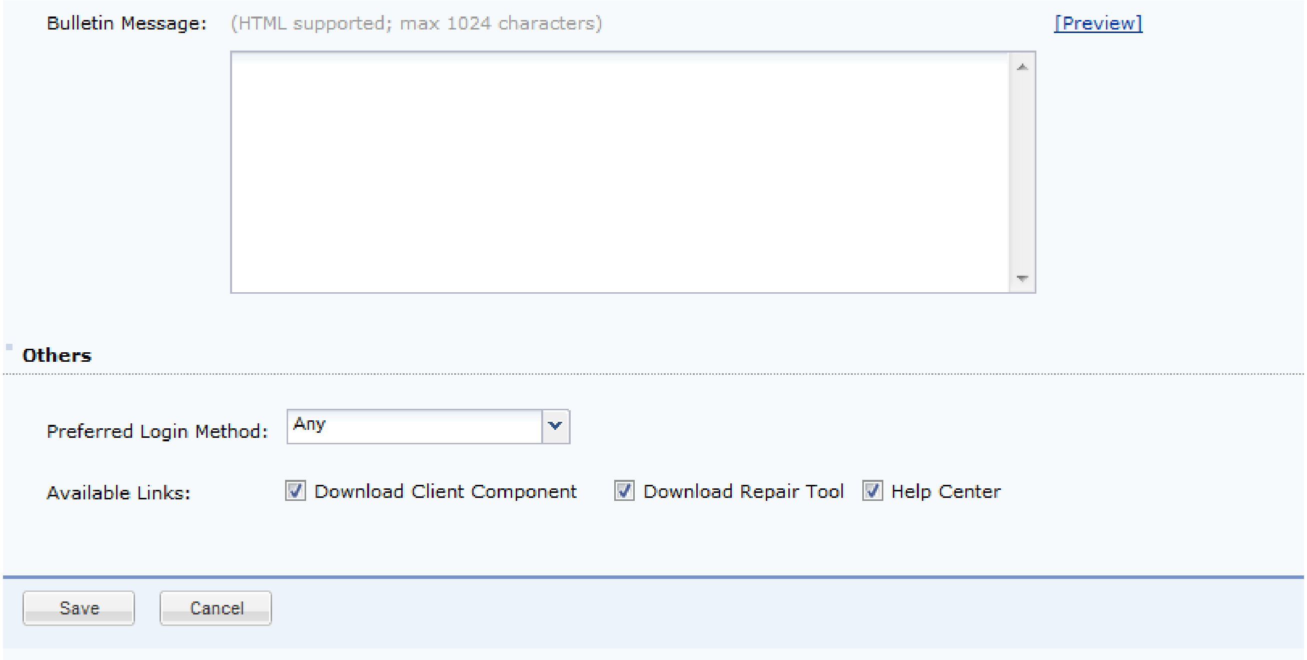
Current Logo:

New Logo:

File extension: .png, .gif, .jpg or .bmp. Image's pixel height must be within 48 and size within 1MB.

Background Color:

Bulletin Message: (HTML supported; max 1024 characters)



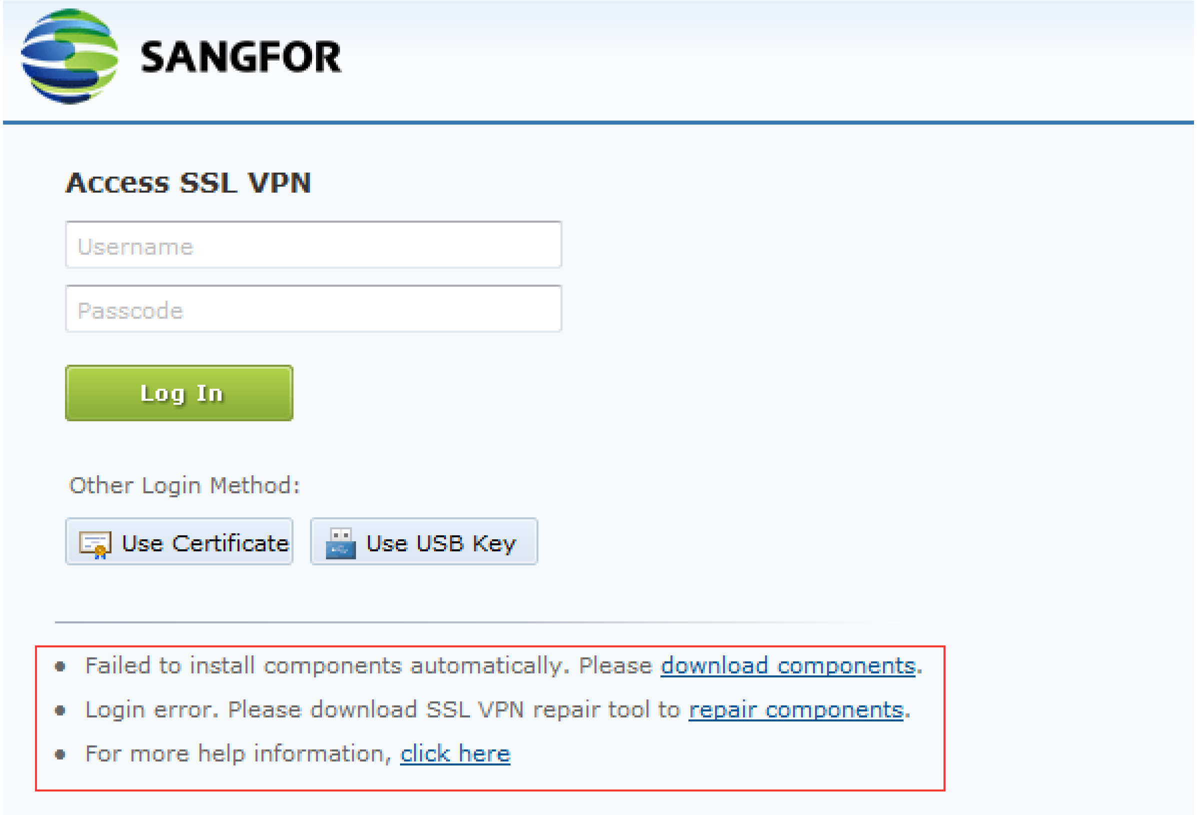
Bulletin Message: (HTML supported; max 1024 characters)

Preferred Login Method: Any

Available Links: ☑ Download Client Component ☑ Download Repair Tool ☑ Help Center

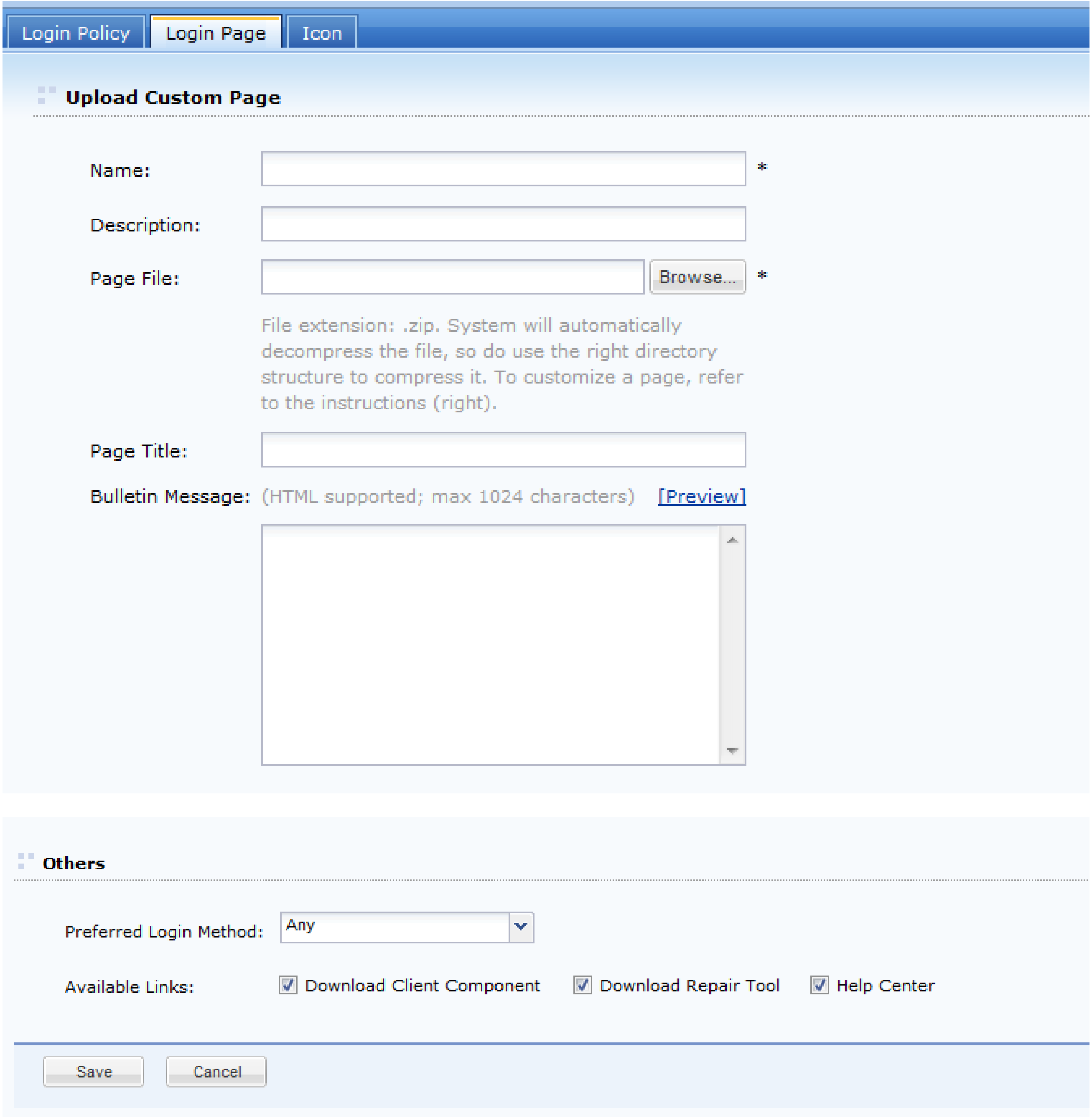
The following are the contents included in the above page:

- **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 themes age 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:**choose the login method you want to preferred.
- **available links:** if not choose some one ,it can be hidden



- Failed to install components automatically. Please download components.
- Login error. Please download SSL VPN repair tool to repair components.
- For more help information, click here

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



Upload Custom Page

Name: *

Description:

Page File: Browse... *

File extension: .zip. System will automatically decompress the file, so do use the right directory structure to compress it. To customize a page, refer to the instructions (right).

Page Title:

Bulletin Message: (HTML supported; max 1024 characters) [Preview]

Others

Preferred Login Method: Any

Available Links: ☑ Download Client Component ☑ Download Repair Tool ☑ Help Center

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**.

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

Scenario 5: Assigning Login Page to Specific User or Group

Background:

Accounts for the members of **Market** and **Finance** have been added to two user groups of different attributes respectively.

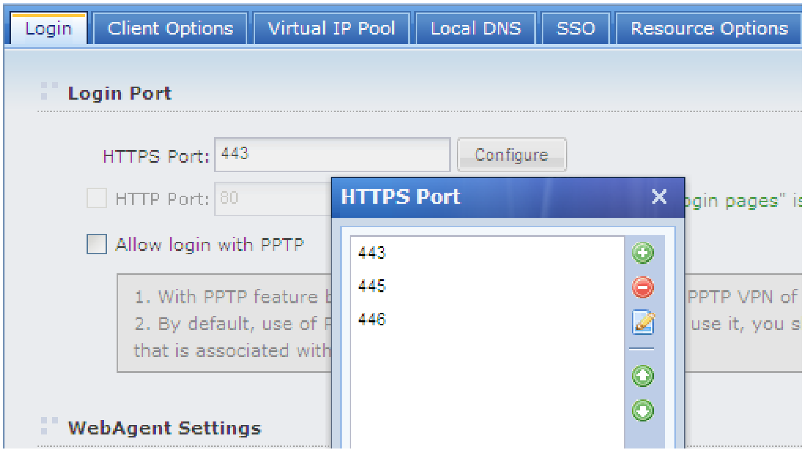
Purpose:

Users in both groups can access the intranet of this enterprise over SSL VPN, whereas each utilizes different login page that distinguishes from each other with their own department characteristics.

Configuration procedure is as follows:

1. Create two user groups, named **Market** and **Finance** respectively, and associate them with the resources that will be available to them after they connect to the SSL VPN.

2. Navigate to **System**>**SSL VPN Options**>**General**>**Login** and configure two HTTPS ports for these two categories of users, port **445** and **446**, as shown below:



Login Port

HTTPS Port: 443

□ HTTP Port: 80

□ Allow login with PPTP

1. With PPTP feature b

2. By default, use of P

that is associated with

ogin pages" is

PPTP VPN of

use it, you s

HTTPS Port

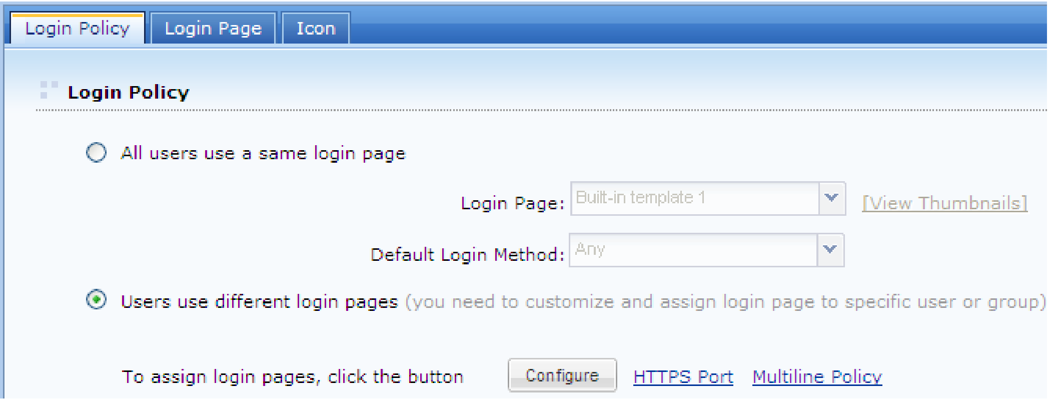
443

445

446

WebAgent Settings

3. Navigate to **System**>**SSL VPN Options**>**Logging in**>**Login Policy** and select **Users use different login pages**, as shown below:



Login Policy

○ All users use a same login page

Login Page: Built-in template 1 [View Thumbnails]

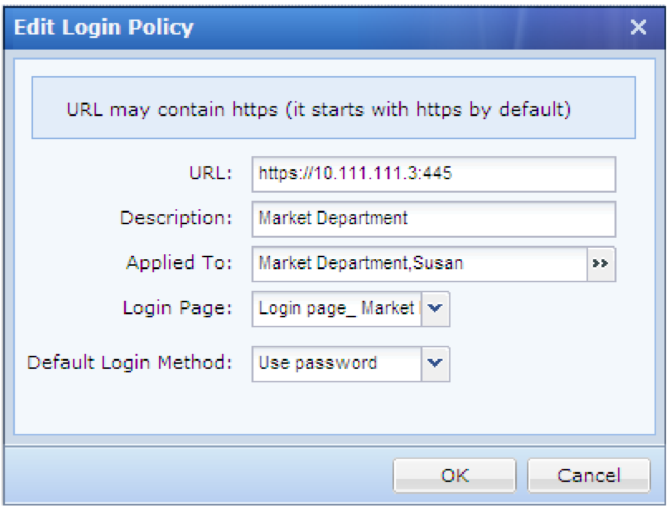
Default Login Method: Any

● Users use different login pages (you need to customize and assign login page to specific user or group)

To assign login pages, click the button Configure HTTPS Port Multiline Policy

4. Create two login policies named **Market** and **Finance** which are to be used by the users from corresponding departments (for detailed guide, refer to the Configuring Login Page sectioning Chapter 3).

   Configure the login policy for the **Market** department, as shown below:



Edit Login Policy

URL may contain https (it starts with https by default)

URL: https://10.111.111.3:445

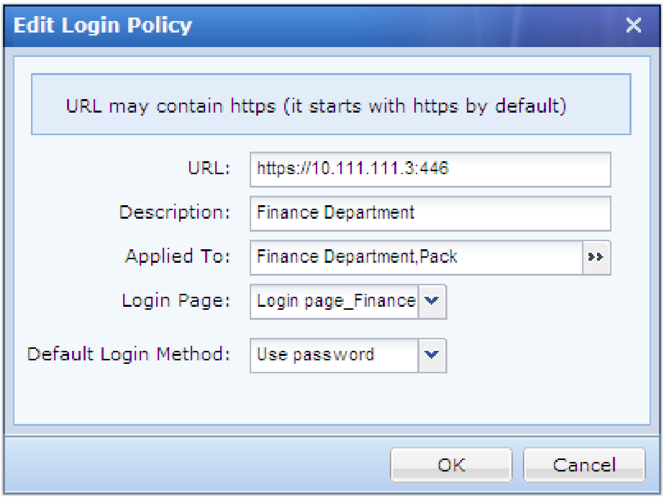
Description: Market Department

Applied To: Market Department,Susan

Login Page: Login page_ Market

Default Login Method: Use password

   Configure the login policy for the **Finance** department, as shown below:



Edit Login Policy

URL may contain https (it starts with https by default)

URL: https://10.111.111.3:446

Description: Finance Department

Applied To: Finance Department,Pack

Login Page: Login page_Finance

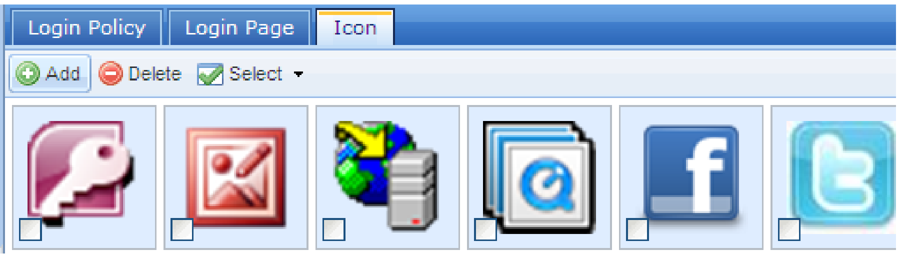
Default Login Method: Use password

5. Ask users in both departments to access SSL VPN via port 445 (for **Market** department) and 446 (for **Finance** department). They will see the login pages that they face are different.

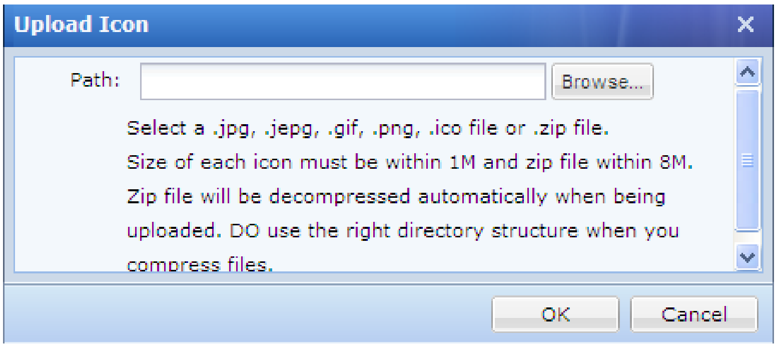
Uploading Icon to Device

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**>**Logging in**>**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:



Path:

Select a .jpg, .jepg, .gif, .png, .ico file or .zip file.
Size of each icon must be within 1M and zip file within 8M.
Zip file will be decompressed automatically when being uploaded. DO use the right directory structure when you compress files.

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 bea real server beingmanaged 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. User to access the SSL VPN if cluster is enabled also uses this IP address.

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.

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 servers 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:** Anode can be elected as dispatcher in an interval of two heartbeats.
  - **Dispatcherre-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 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**

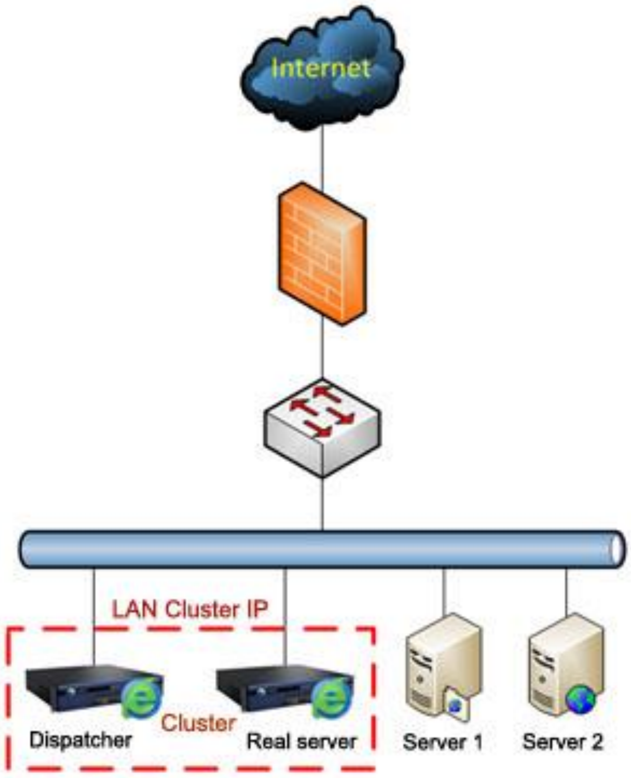
  With cluster being enabled, user can use any service provided by SSL VPN as long as at least one clustered Sangfor device keeps running. If useris using a static cluster IP address to access the services but that node gets into fault, the online users related to that node will be disconnected and required 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 Deployment sectioning Chapter 3). One additional configuration is **Cluster IP Address** of **LAN** interface (under **System**>**SSLVPN Options**>**Clustering**>**Deployment**).

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



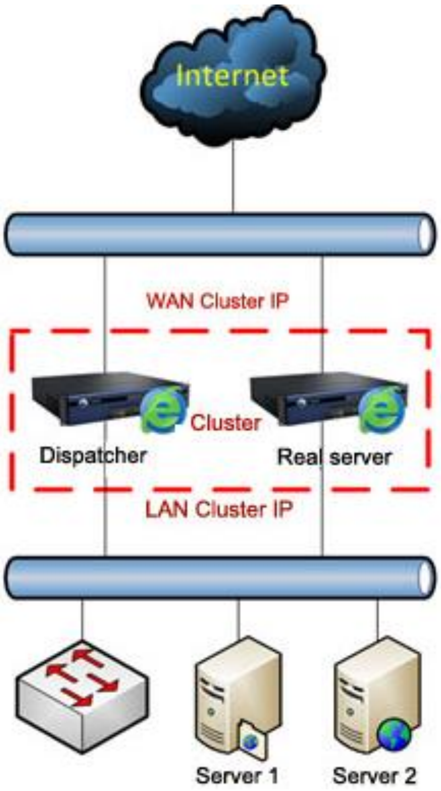
⚠

- **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**>**Deployment**) must be of a same network segment.

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 Deployment sectioning Chapter 3). One additional configuration is **Cluster IP Address** of **LAN** interface and **WAN** interface (under **System**>**SSLVPN Options**>**Clustering**>**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.

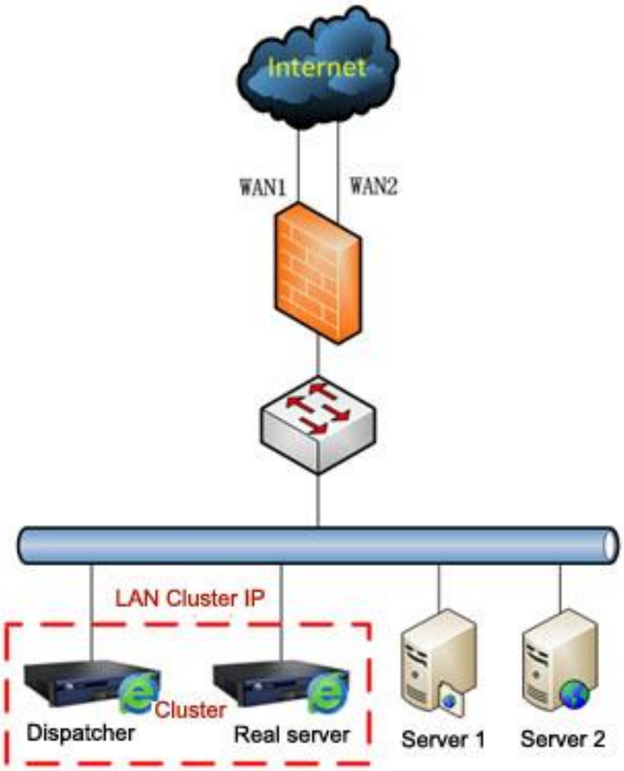
Deploying Clustered Device with Multiple Lines

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 Deployment sectioning Chapter 3). One additional configuration is **Cluster IP Address** of **LAN** interface and **WAN** interface (under **System**>**SSLVPN 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

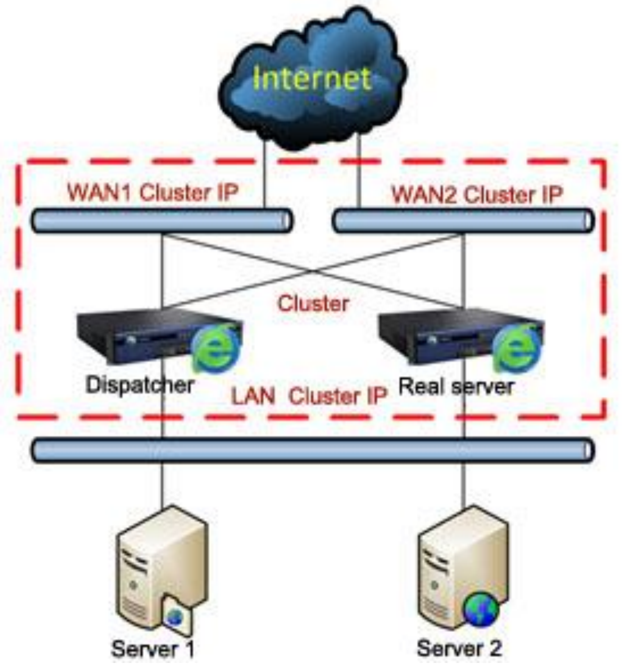
Typical network topology of cluster of **Single-arm** devices is as shown in the figure below:



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

Gateway-mode Sangfor Device with Multiple Lines

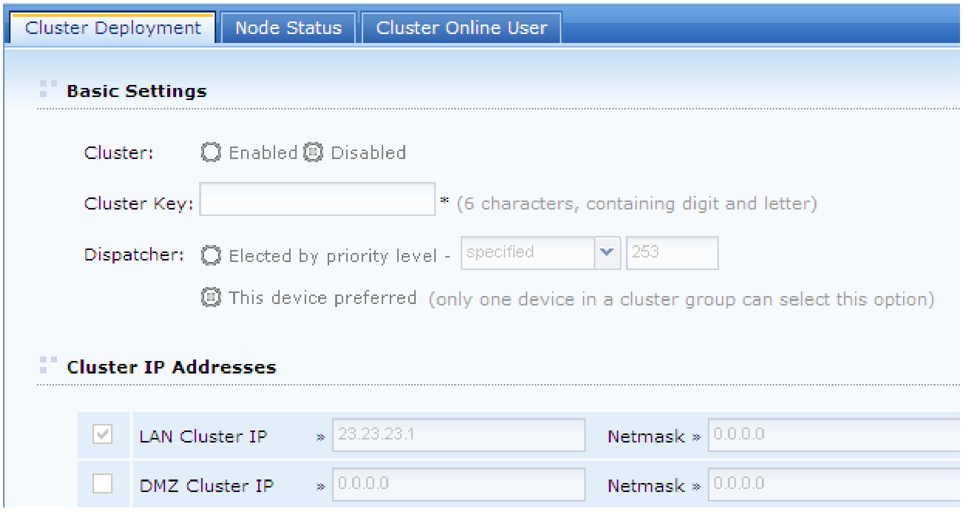
Typical network topology of cluster of **Gateway-mode** devices is as shown in the figure below:



Scenario 6: 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**>**Deployment**, as shown in the figure below:



Basic Settings

Cluster: ○ Enabled ● Disabled

Cluster Key: * (6 characters, containing digit and letter)

Dispatcher: ○ Elected by priority level - specified 253

● This device preferred (only one device in a cluster group can select this option)

Cluster IP Addresses

☑	LAN Cluster IP »	23.23.23.1	Netmask »	0.0.0.0
□	DMZ Cluster IP »	0.0.0.0	Netmask »	0.0.0.0

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 there lated 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 meansthat 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.

    ⚠

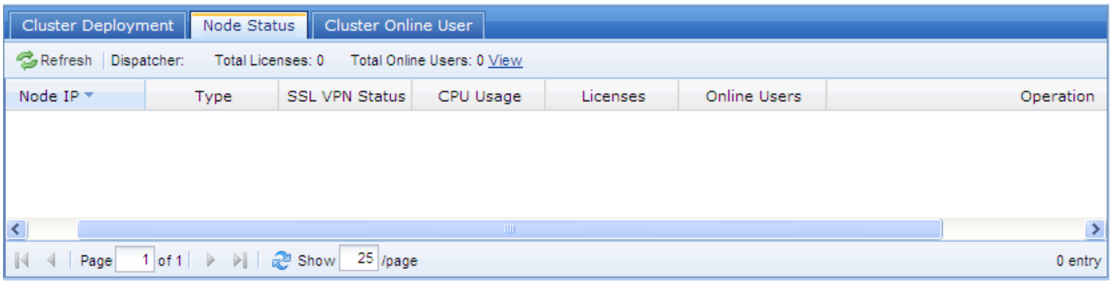
    Cluster IP address is a group of IP addresses of a cluster formed by more than one Sangfor devices, and will be launched to the external networks. These IP addresses configured on each clustered node must be consistent.

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

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:

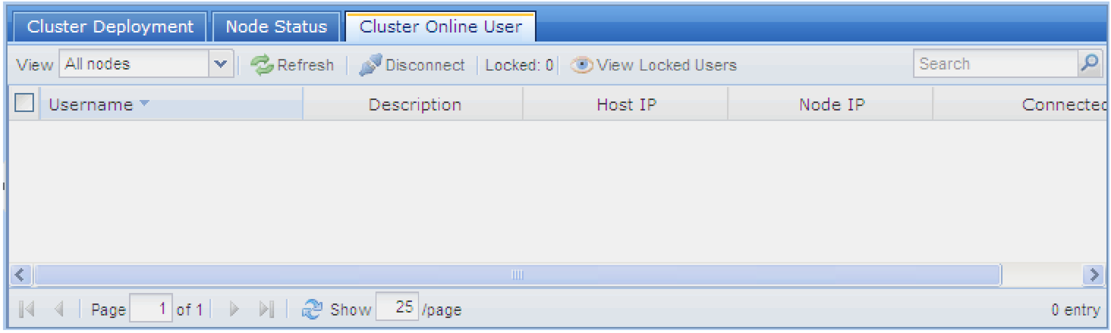


To enter the administrator console of a clustered node, click the **Login to Nod**e link.

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.

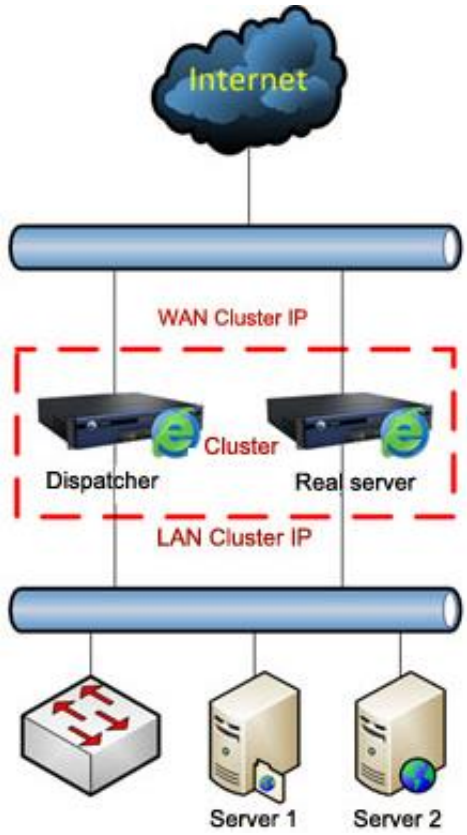
- **Search:** To search for a specific user, enter the keyword into **Search** field and then click the magnifier icon 🔍 or prese**nter** key.

Scenario 7:Configuring Clustered Sangfor Device

Configuring Clustered Device in Gateway Mode

IP address of an Internet line is 202.96.137.75 with subnet mask255.255.255.0.

Cluster network topology of Sangfor devices in **Gateway** mode is as shown in the figure below:



Configuration procedure is as follows:

1. Deploy the Sangfor devices into the network as that shown in the figure above. Make sure that the dispatcher and real server can communicate with each other via their WAN interfaces and LAN interfaces.

2. Select deployment mode and configure WAN and LAN interfaces on the dispatcher and real server.

   On the dispatcher**:** go to **System**>**Network**>**Deployment** page and select deployment mode **Gateway**. Configure the **LAN** interface (IP/netmask:192.168.1.10/255.255.255.0), **WAN** interface (IP/netmask:2.0.1.10/255.255.255.0) and default gateway (2.0.1.254). The preferred and alternate DNS must be valid DNS servers.

   On the real servers: go to **System**>**Network**>**Deployment** page and select deployment mode **Gateway**. Configure the **LAN** interface (IP/netmask:192.168.1.20/255.255.255.0), **WAN interface** (IP/netmask:2.0.1.20/255.255.255.0) and default gateway (2.0.1.254). The preferred and alternate DNS must be valid DNS servers.

3. Go to **System**>**SSL VPN Options**>**Clustering**>**Deployment**. Select **Enabled** to enable cluster and configure the **Cluster Key**.

4. Enable cluster on dispatcher and real servers. Cluster keys configured on dispatcher and real server must be identical.

5. Specify dispatcher.

   To set this Sangfor device as the dispatcher, select **This device preferred** to, in which case, the other nodes in this cluster will be a real servers.

   If you are not to set this SSL device as the dispatcher, select **Elected by priority level** and configure the priority level to have all the clustered nodes to compete for dispatcher. Please note that the lower the value of the priority level, the higher priority the node has. The device that has the highest priority (with the lowest value) will become the dispatcher.

6. Configure LAN cluster IP address and WAN cluster IP address.

   On dispatcher: configure the **LAN cluster IP** address (192.168.1.1) and network mask (255.255.255.0), the **WAN1 cluster**y address (the actual **WAN** interface IP address, 202.96.137.75) and network mask (255.255.255.0), and the **WAN1** interface gateway (202.96.137.254).

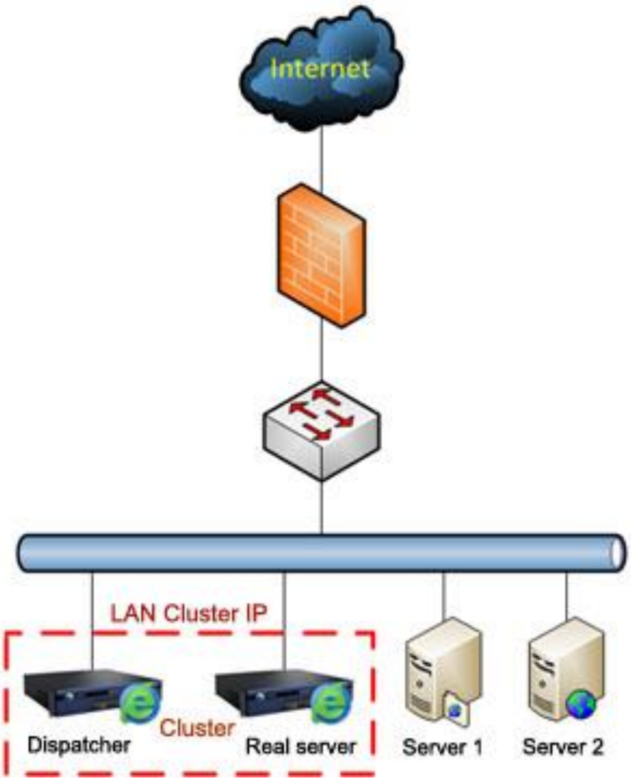
   On the real servers: configure the **LAN cluster IP** address (192.168.1.1) and network mask (255.255.255.0), the **WAN1 cluster IP** address (the actual **WAN** interface IP address, 202.96.137.75) and network mask (255.255.255.0), and the **WAN1** interface gateway (202.96.137.254).

⚠

- **LAN cluster IP** address and the **LAN interface IP** address of any Sangfor device in the cluster must be of a same network segment.
- The **WAN interface IP** address of each Sangfor device in the cluster can be an IP address of any network segment. However, the **WAN interface IP** addresses of both Sangfor devices must be of a same network segment.
- The default gateway of **WAN** interface can be any IP address (except 0.0.0.0). **WAN cluster IP** address and the **WAN interface IP** address should not be of a same network segment.
- If Sangfor device works in gateway mode, it cannot dial up to the Internet.

Configuring Clustered Device in Single-Arm Mode

IP address and subnet mask of the Internet line is 202.96.137.75 and 255.255.255.0 respectively. Cluster network topology of Sangfor devices in **Single-arm** mode is as shown below:



Configuration procedure is as follows:

1. Deploy the Sangfor devices into the network as that shown in the figure above. Make sure that the dispatcher and real server can communicate with each other via their LAN interfaces. WAN interfaces need not be connected.

2. Select deployment mode and configure LAN interface on the dispatcher and real server.

   On the dispatcher: go to **System**>**Network**>**Deployment** page and select deployment mode **Single-Arm**. Configure the **LA** interface (IP/netmask:192.168.1.10/255.255.255.0) and default gateway (192.168.1.254). The preferred and alternate **DNS** must be valid DNS servers.

   On the real server: go to **System**>**Network**>**Deployment** page, select deployment mode **Single-Arm**. Configure the **LA** interface (IP/netmask:192.168.1.20/ 255.255.255.0) and default gateway (192.168.1.254). The preferred and alternate **DNS** must be valid DNS servers.

3. Go to **System**>**SSL VPN Options**>**Clustering**>**Deployment** and Select **Enabled** to enable cluster and configure the **Cluster Key**.

   Enable cluster on dispatcher and real servers. Cluster keys configured on dispatcher and real server must be identical.

4. Specify dispatcher. To set this Sangfor device as the dispatcher, select **this device preferred**, in which case, the other nodes in this cluster will be real servers.

   If you are not to set this SSL device as the dispatcher, select **Elected by priority level** and configure the priority level to have all the clustered nodes to compete for dispatcher. Please note that the lower the value of the priority level, the higher priority the node has. The device that has the highest priority (with the lowest value) will become the dispatcher.

5. Configure LAN cluster IP address.

   On dispatcher: configure the **LAN cluster IP** address (192.168.1.1) and network mask (255.255.255.0).

   On the real server: configure the **LAN cluster IP** address (192.168.1.1) and network mask (255.255.255.0).

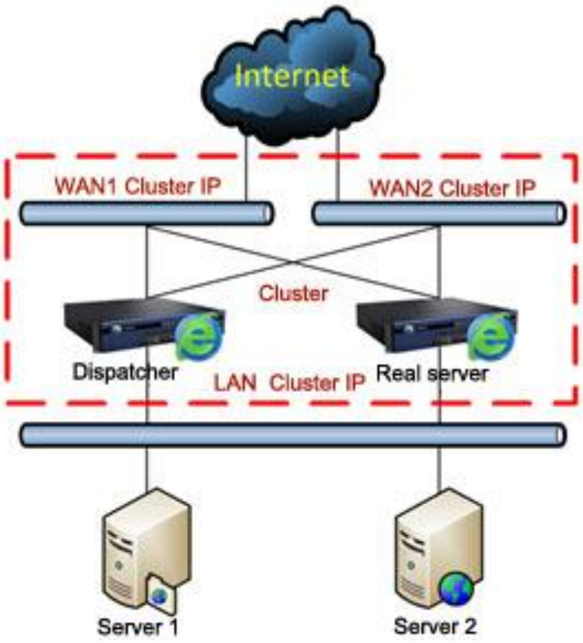
   ⚠

   - **LAN cluster IP** address and the **LAN** interface IP address of any Sangfor device in the cluster must be of a same network segment.
   - Sangfor device deployed in cluster does not support dynamic IP address assignment; the front-end gateway cannot dial up to the Internet.

6. Configure the front-end gateway device, and map the ports TCP 443, 80 and UDP 443 of WAN interface IP address (202.96.137.75) to those of the LAN cluster IP address (192.168.1.1).

Configuring Clustered Device in Gateway Mode (Multiple Lines)

WAN1 interface (IP/netmask:202.96.137.75/255.255.255.0) of the Sangfor device connects to the Telecom link, and WAN2 interface (IP/netmask:58.120.10.64/255.255.255.0) to the Netcom link. Cluster network topology of Sangfor devices in **Gateway** mode with multiple lines is as shown below:



Configuration procedure is as follows:

1. Deploy the Sangfor devices into the network as that shown in the figure above, WAN2 and WAN2 interface connecting to the Telecom and Netcom links respectively. Make sure that the dispatcher and real server can communicate with each other via their WAN1, WAN2 and LAN interfaces.

2. Select deployment mode and configure WAN and LAN interface on the dispatcher and real server.

   On the dispatcher: go to **System**>**Network**>**Deployment** page and select deployment mode **Gateway**. Configure the **LA** interface (IP/netmask:192.168.1.10/255.255.255.0), **WAN1**interface (IP/netmask:2.0.1.10/255.255.255.0; default gateway: 2.0.1.254), **WAN2**interface (IP/netmask:3.0.1.10/255.255.255.0, default gateway: 3.0.1.254), and preferred **DNS** server IP. The preferred and alternate DNS must be valid DNS servers.

   On the real server: go to **System**>**Network**>**Deployment** page and select deployment mode **Gateway.** Configure the **LAN** interface (IP/netmask:192.168.1.20/255.255.255.0), **WAN1**interface (IP/netmask:2.0.1.20/255.255.255.0; default gateway: 2.0.1.254), **WAN2**interface (IP/netmask:3.0.1.20/255.255.255.0; default gateway: 3.0.1.254), and preferred **DNS** server IP. The preferred and alternate DNS must be valid DNS servers.

3. Go to **System**>**Network**>**Multiline Options** page and select the option **Allow SSL VPN to Use Multiple Lines**. This option should be selected on dispatcher and all real servers, with a line selection policy being selected.

4. Go to **System**>**SSLVPN Options**>**Clustering**>**Deployment**, select **Enabled** to enable cluster and configure the **Cluster Key**. This option should be selected on dispatcher and all real servers, cluster keys being the same.

5. Specify dispatcher. To set this Sangfor device as dispatcher, select **this device preferred**, in which case, the other nodes in this cluster will be real servers.

   If you are not to set the local SSL device as the dispatcher, select **Elected by priority level** and configure the priority level to have all the clustered nodes to compete for dispatcher. Please note that the lower the value of the priority level, the higher priority the node has. The device that has the highest priority (with the lowest value) will become the dispatcher

6. Configure **LAN cluster IP** address and **WAN cluster IP** address.

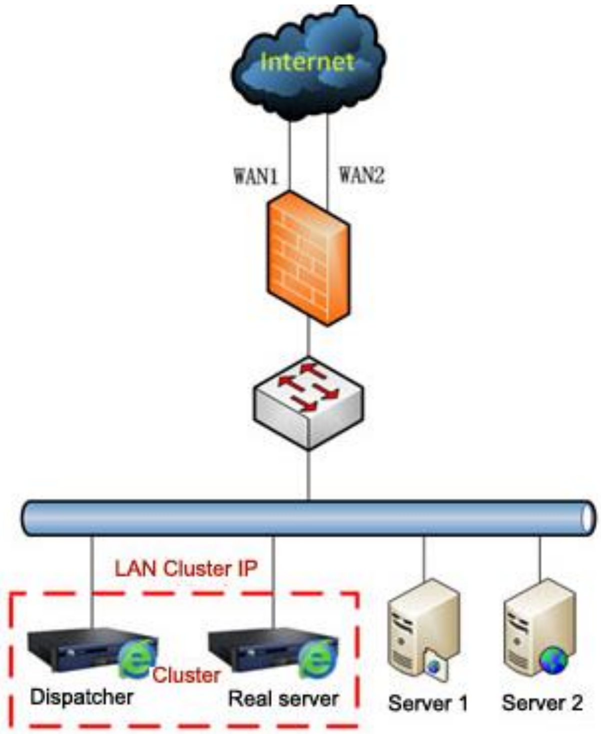
   On dispatcher: configure the **LAN cluster IP** address (192.168.1.1) and net mask (255.255.255.0), **WAN1 cluster IP** address (the actual WAN1 interface IP address, 202.96.137.75) and net mask (255.255.255.0), WAN1 interface gateway (202.96.137.254), **WAN2 cluster IP** address (the actual WAN2 interface IP address, 58.120.10.64) and net mask (255.255.255.0), WAN2 interface gateway (58.120.10.254).

   On the real server: configure the **LAN cluster IP** address (192.168.1.1) and net mask (255.255.255.0), **WAN1 cluster IP** address (the actual WAN1 interface IP address, 202.96.137.75) and net mask (255.255.255.0), **WAN1** interface gateway (202.96.137.254), **WAN2 cluster IP** address (the actual WAN2 interface IP address, 58.120.10.64) and net mask (255.255.255.0), WAN2 interface gateway (58.120.10.254).

Configuring Clustered Device in Single-Arm Mode (Multiple Lines)

WAN1 interface (IP/netmask:202.96.137.75/255.255.255.0) of the Sangfor device connects to the Telecom line.WAN2 interface (IP/netmask:58.120.10.64/255.255.255.0) of the Sangfor device connects to the Netcom line.

Cluster network topology of Sangfor devices in **Single-arm** mode with multiple lines is as shown below:



Configuration procedure is as follows:

1. Deploy the Sangfor devices into the network as that shown in the figure above. Make sure that the dispatcher and real server can communicate with each other via their LAN interfaces. WAN interfaces need not be connected.

2. Select deployment mode and configure LAN interface of the dispatcher and real server.

   On the dispatcher: go to **System**>**Network**>**Deployment** page and select deployment mode **Single-Arm**. Configure the **LAN** interface (IP/netmask:192.168.1.10/255.255.255.0) and default gateway (192.168.1.254). The preferred and alternate **DNS** must be valid DNS servers.

   On the real server: go to **System**>**Network**>**Deployment** page and select deployment mode **Single-Arm**. Configure the **LA** interface (IP/netmask:192.168.1.20/255.255.255.0) and default gateway (192.168.1.254). The preferred and alternate **DNS** must be valid DNS servers.

3. Go to **System**>**Network**>**Multiline Options** page and select the option **Allow SSL VPN to Use Multiple Lines**. This option should be selected on dispatcher and all real servers, with a line selection policy being selected.

4. Go to **System**>**Network**>**Multiline Options** and select connect-in method **SSL VPN users connect in via front-end device** (please refer to the Options sectioning Chapter 3).

   On the dispatcher: in the **Lines of Front-end Device** list, click **Add** to add a line (line 1, Telecom line) and configure the required fields (IP: 202.96.137.75, HTTP port: 80, HTTPS port: 443). Add another line (line 2, Netcom line) and configure the required fields (IP address:58.120.10.64, HTTP port:80, HTTPS port:443).

On the real server: in the **Lines of Front-end Device** list, click **Add** to add a line (line 1, Telecom line) by clicking **Add** and configuring the required fields (IP: 202.96.137.75, HTTP port: 80, HTTPS port: 443). Add another line (line 2, Netcom line) and configure the required fields (IP address:58.120.10.64, HTTP port:80, HTTPS port:443).

⚠

To deploy and configure a Sangfor device in Single-arm mode that has multiple Internet lines, select **SSL VPN users connect in via front-end device** and add the lines into the list.

5. Go to **System**>**SSL VPN Options**>**Clustering**>**Deployment**, select **Enabled** to enable cluster and configure the **Cluster Key**. This option should be enabled on dispatcher and all real servers. Cluster keys configured on dispatcher and real servers must be identical.

6. Specify dispatcher.

   To set Sangfor device as the dispatcher, select **This device preferred**, in which case, the other nodes in this cluster will be real servers.

   If you are not to set this SSL device as the dispatcher, select **Elected by priority level** and configure the priority level to have all the clustered nodes to compete for dispatcher. Please note that the lower the value of the priority level, the higher priority the node has. The device that has the highest priority (with the lowest value) will become the dispatcher.

7. Configure LAN cluster IP address.

   On the dispatcher: configure the **LAN cluster IP** address (192.168.1.1) and net mask (255.255.255.0).

   On the real server: configure the **LAN cluster IP** address (192.168.1.1) and net mask (255.255.255.0).

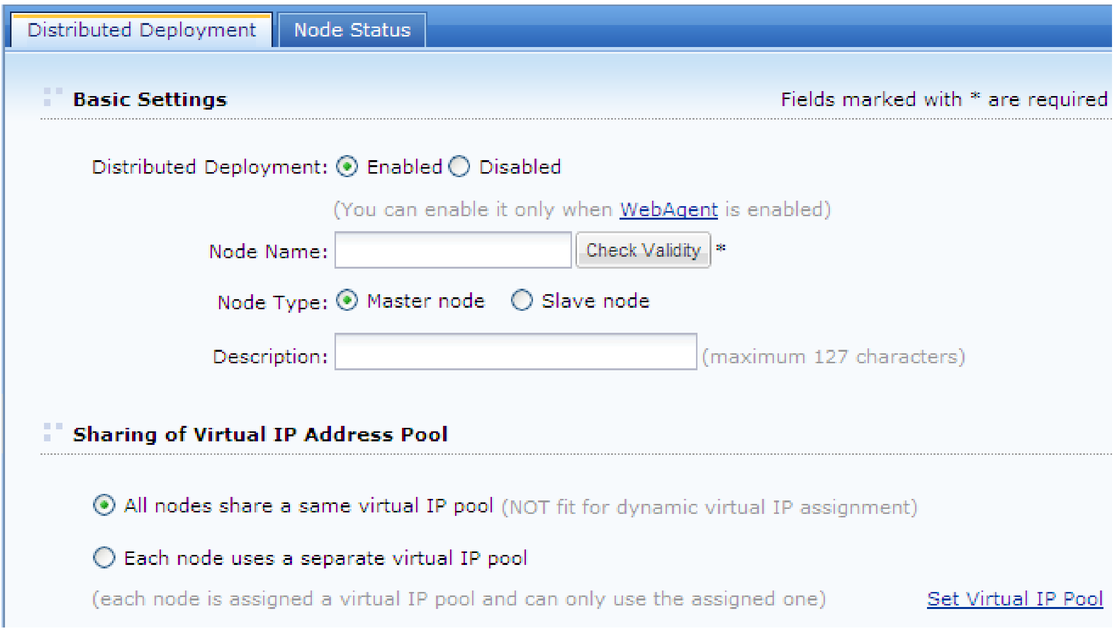
8. Configure the front-end gateway device. Map the ports TCP 443, 80 and UDP 443 of **WAN1** interface (connecting to Telecom line) IP address (202.96.137.75) to those of the **LAN cluster IP** address (192.168.1.1), and map the ports TCP 443, 80 and UDP 443 of **WAN2** interface (connecting to Netcom line) IP address (58.120.10.64) to those of the **LAN cluster IP** address (192.168.1.1).

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 Modes**to enter the **DistributedDeployment** page, as shown in the figure below:



Basic Settings

Fields marked with * are required

Distributed Deployment: ● Enabled ○ Disabled

(You can enable it only when WebAgent is enabled)

Node Name: [ ] Check Validity *

Node Type: ● Master node ○ Slave node

Description: [ ] (maximum 127 characters)

Sharing of Virtual IP Address Pool

● All nodes share a same virtual IP pool (NOT fit for dynamic virtual IP assignment)

○ Each node uses a separate virtual IP pool

(each node is assigned a virtual IP pool and can only use the assigned one) Set Virtual IP Pool

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

- **Distributed Deployment:**global switch intended for enabling or disabling distributed deployment of SSL VPN system. To enable the distributed deployment, select **Enabled**.
- **Node Name:** Specifies the name of the node (Sangfor device). After entering nodename, click the **Check Validity**button to check on the Web Agent 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 whologs in to a distributed nodewill 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 I sectioning Chapter 3).
- **Save:** Click it to save the settings.

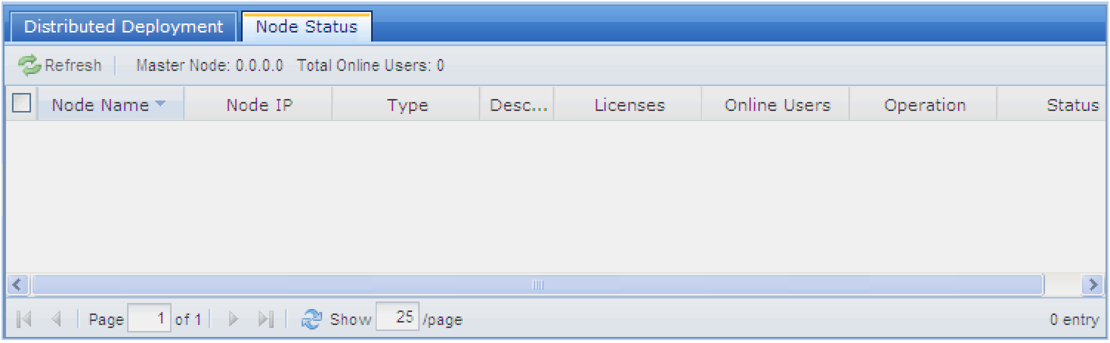
⚠

Distributed deployment requires that Web Agent is enabled and configured properly.

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** andthe **Node Status** page is seen, as shown in the figure below:



Master Node: 0.0.0.0 Total Online Users: 0

□	Node Name	Node IP	Type	Desc...	Licenses	Online Users	Operation	Status

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

Chapter 4 SSL VPN

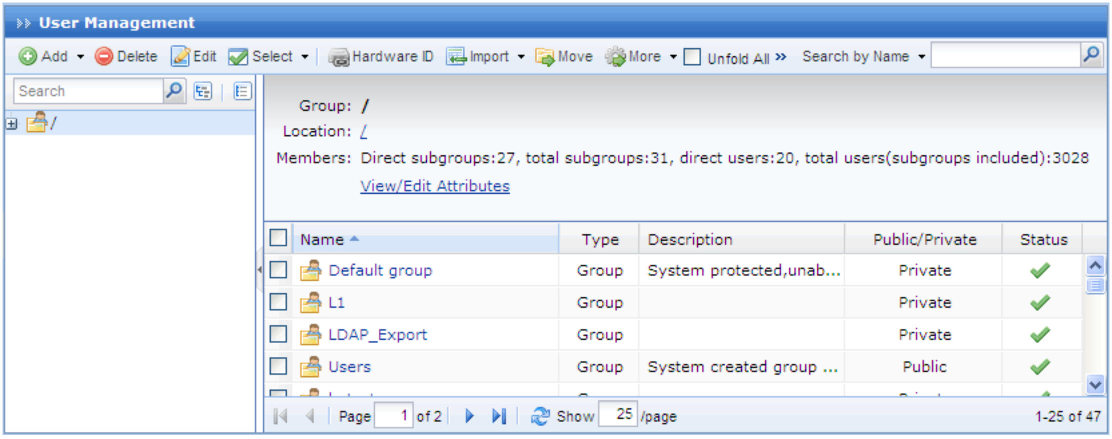
SSL Vancouver’s configurations of **Users**, **Resources**, **Roles**, **Authentication**, **Policy Sets, Remote Servers** and **Endpoint Security**.

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** toenter **User Management** page, as shown below:



Group: /
Location: /
Members: Direct subgroups:27, total subgroups:31, direct users:20, total users(subgroups included):3028
View/Edit Attributes

□	Name	Type	Description	Public/Private	Status
□	Default group	Group	System protected,unab...	Private	✓
□	L1	Group		Private	✓
□	LDAP_Export	Group		Private	✓
□	Users	Group	System created group ...	Public	✓

Page 1 of 2 Show 25 /page 1-25 of 47

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** fielding 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**.

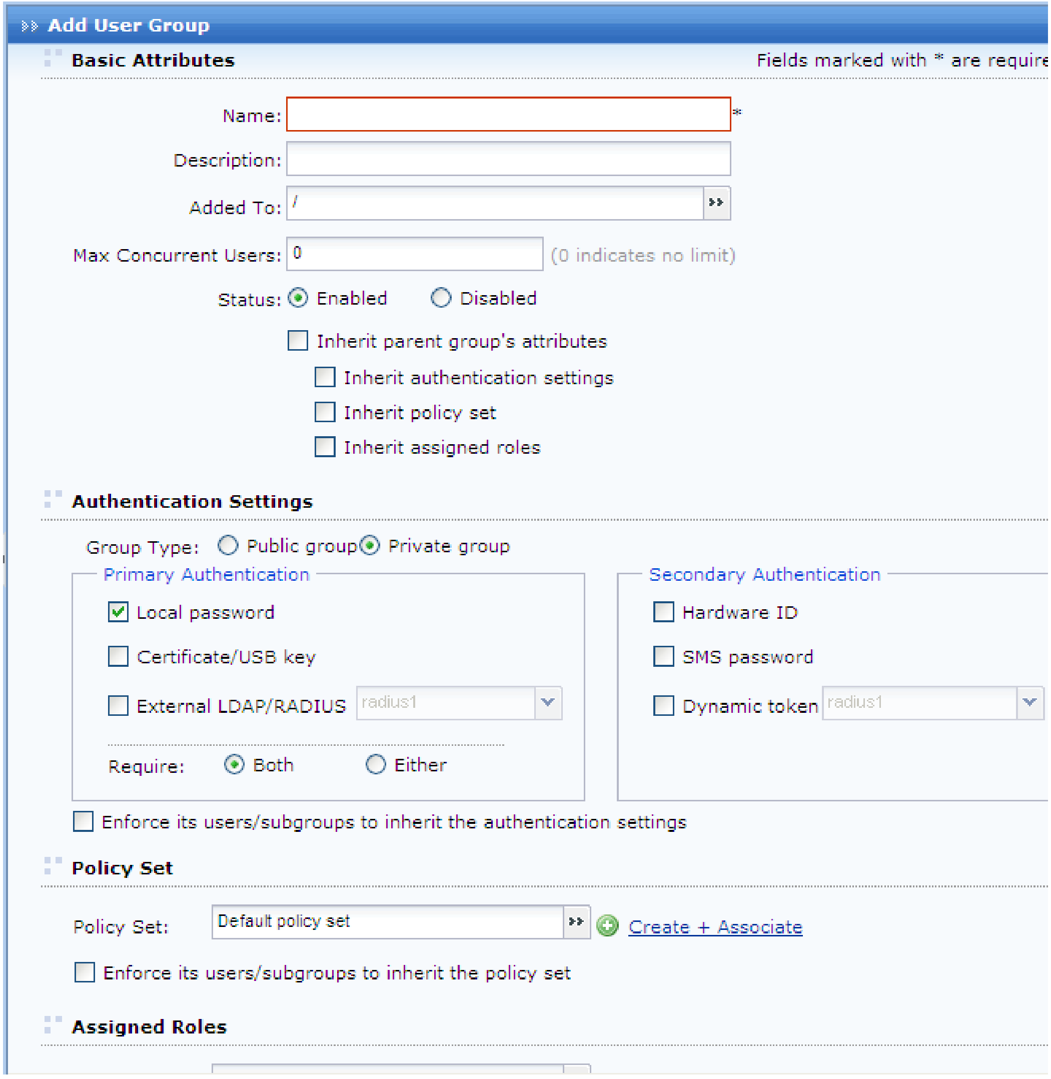
To choose the desired entries, click **Select**>**Current page** or**All pages**.

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 toss **VPN**>**Users**>**User Management** page. Click **Add**>**User Group** to enter **Add User Group** page, as shown in the figure below:



Basic Attributes

Fields marked with * are require

Name: *

Description:

Added To: /

Max Concurrent Users: 0 (0 indicates no limit)

Status: ● Enabled ○ Disabled

□ Inherit parent group's attributes

□ Inherit authentication settings

□ Inherit policy set

□ Inherit assigned roles

Authentication Settings

Group Type: ○ Public group ● Private group

Primary Authentication

☑ Local password

□ Certificate/USB key

□ External LDAP/RADIUS radius1

Require: ● Both ○ Either

Secondary Authentication

□ Hardware ID

□ SMS password

□ Dynamic token radius1

□ Enforce its users/subgroups to inherit the authentication settings

Policy Set

Policy Set: Default policy set

□ Enforce its users/subgroups to inherit the policy set

Assigned Roles

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

- **Name:** Entera name for this user group. This field is required.
- **Description:** Enterbrief description for this user group.
- **Added To:** Select the user group to which this user group is added.

- **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 multiple users to log in to the SSL VPN concurrently can use none of the user accounts in this group. 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 Authentication section and RADIUS Authentication sectioning 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.

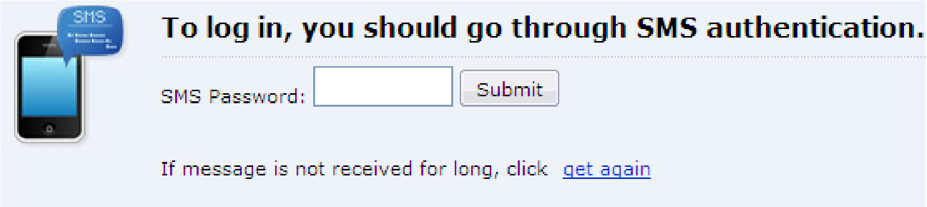
    Either means that the selected primary authentication methods (if two authentication methods are selected), and the user has to pass either of the selected primary authentications.

- 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.
  - **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. 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:

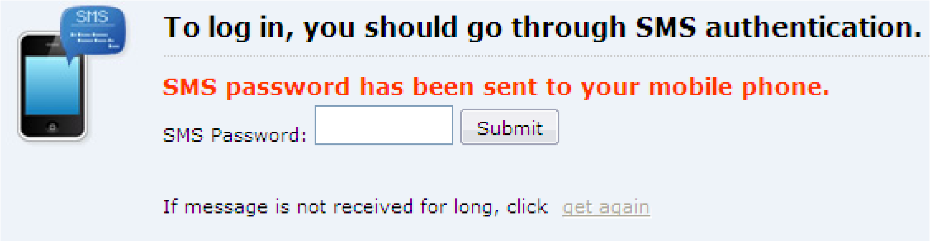


To log in, you should go through SMS authentication.

SMS Password: Submit

If message is not received for long, click get again

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.



To log in, you should go through SMS authentication.

SMS password has been sent to your mobile phone.

SMS Password: Submit

If message is not received for long, click get again

⚠

- 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 Authentication sectioning 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

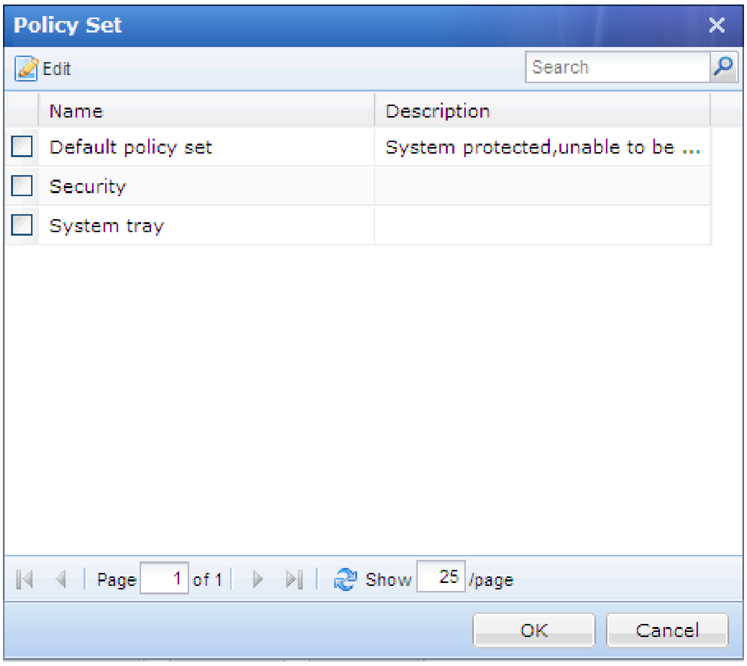
c. External LDAP/RADIUS+ SMS password/Hardware ID/Dynamic token

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 sets 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:



	Name	Description
□	Default policy set	System protected,unable to be ...
□	Security	
□	System tray	

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

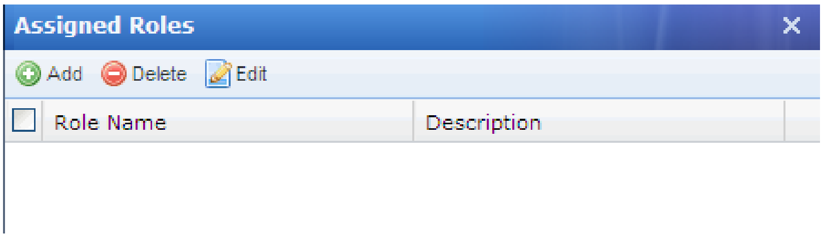
   To confirm the selection, click the **OK** button and the selected policy set will be filled in **Policy Set** field.

   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 sets the same as that in adding 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.

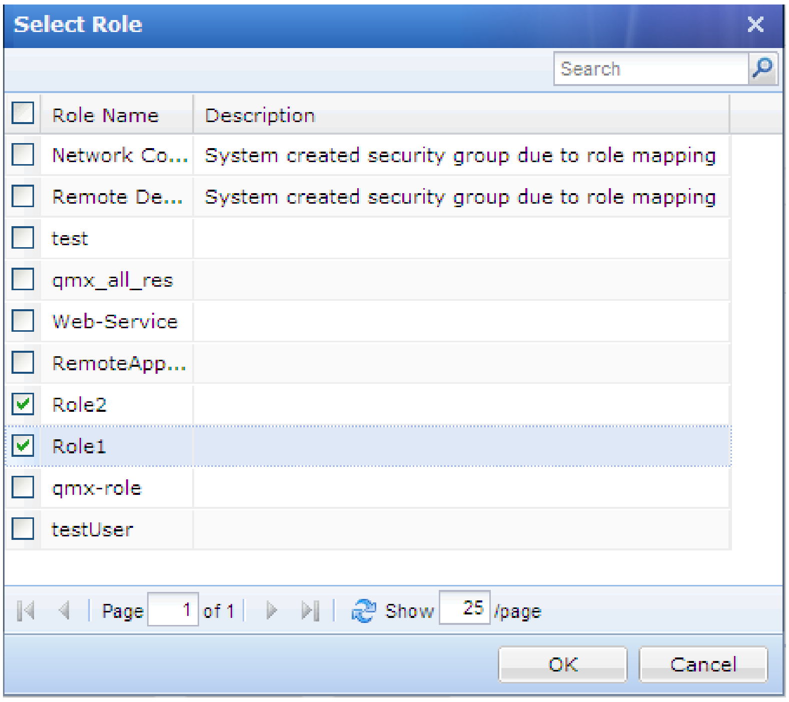
5. Assign roles to user group. For the procedures of configuring role, refer to the Adding Role section in Chapter 4.

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



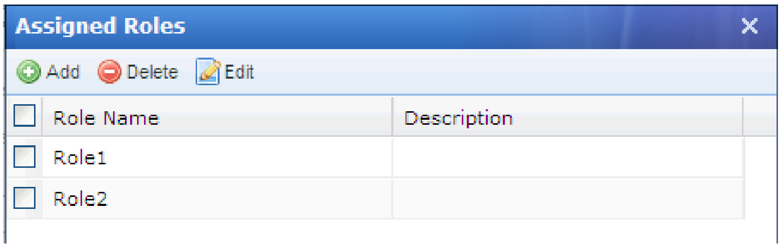
□	Role Name	Description

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



□	Role Name	Description
□	Network Co...	System created security group due to role mapping
□	Remote De...	System created security group due to role mapping
□	test	
□	qmx_all_res	
□	Web-Service	
□	RemoteApp...	
☑	Role2	
☑	Role1	
□	qmx-role	
□	testUser	

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:



□	Role Name	Description
□	Role1	
□	Role2	

d. Click the **OK** button and name of the assigned roles 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 section).

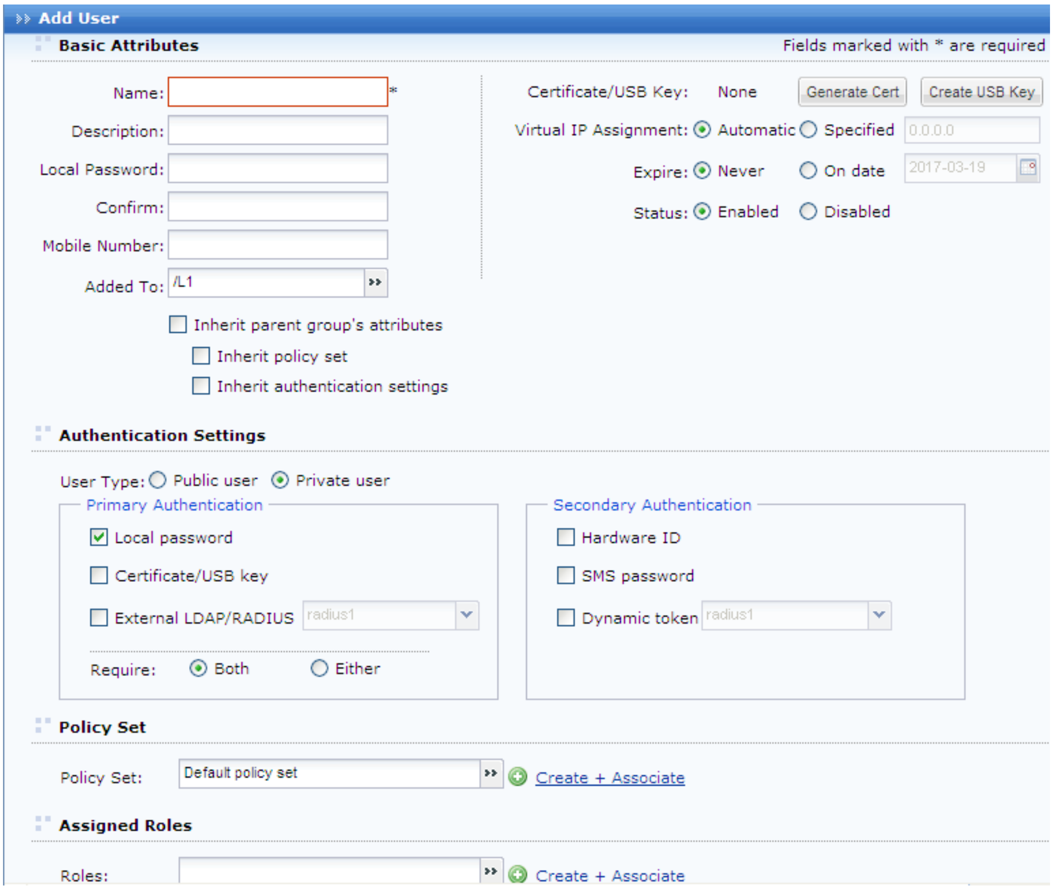
f. To remove a role from the list, select the role and click **Delete**.

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

- No user group can be added to **Default Group** or **Anonymous Group**.
- **Anonymous Group** is a user group automatically created by the system while anonymous login is enabled.

Adding User

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



Add User

Basic Attributes

Fields marked with * are required

Name: *

Description:

Local Password:

Confirm:

Mobile Number:

Added To: /L1

□ Inherit parent group's attributes

□ Inherit policy set

□ Inherit authentication settings

Certificate/USB Key: None

Virtual IP Assignment: ● Automatic ○ Specified 0.0.0.0

Expire: ● Never ○ On date 2017-03-19

Status: ● Enabled ○ Disabled

Authentication Settings

User Type: ○ Public user ● Private user

Primary Authentication

☑ Local password

□ Certificate/USB key

□ External LDAP/RADIUS radius1

Require: ● Both ○ Either

Secondary Authentication

□ Hardware ID

□ SMS password

□ Dynamic token radius1

Policy Set

Policy Set: Default policy set

Assigned Roles

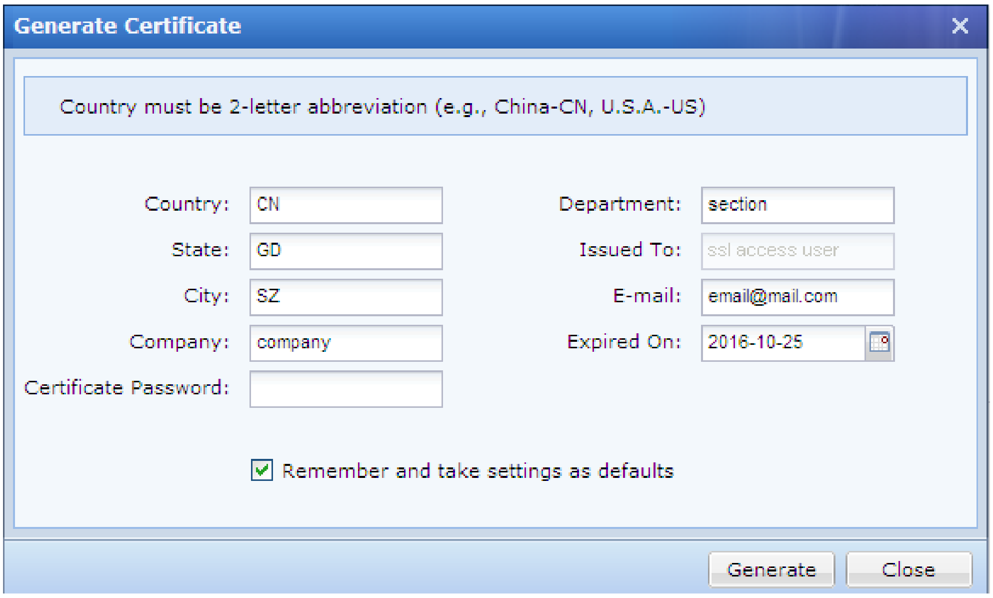
Roles:

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.

- **Local Password**, **Confirm:**Enter the password of this user account.
- **Mobile Number:** Enterthe 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. Click the**Generate Cert** button to enter **Generate Certificate** page to, as shown below:



Generate Certificate

Country must be 2-letter abbreviation (e.g., China-CN, U.S.A.-US)

Country:	CN	Department:	section
State:	GD	Issued To:	ssl access user
City:	SZ	E-mail:	email@mail.com
Company:	company	Expired On:	2016-10-25
Certificate Password:			

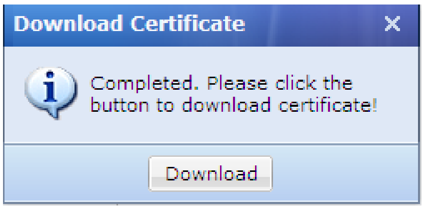
☑ Remember and take settings as defaults

   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** andthe 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:



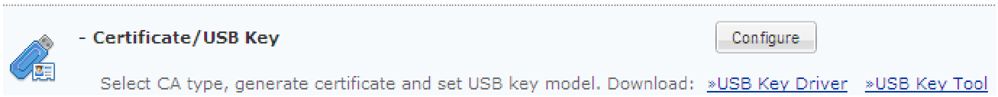
Download Certificate

Completed. Please click the button to download certificate!

e. Click the **Download** button and select a path to save the certificate into the computer. File extension of the certificate is .p12.

4. Generate USB key for the current user.

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



- Certificate/USB Key

Select CA type, generate certificate and set USB key model. Download: »USB Key Driver »USB Key Tool

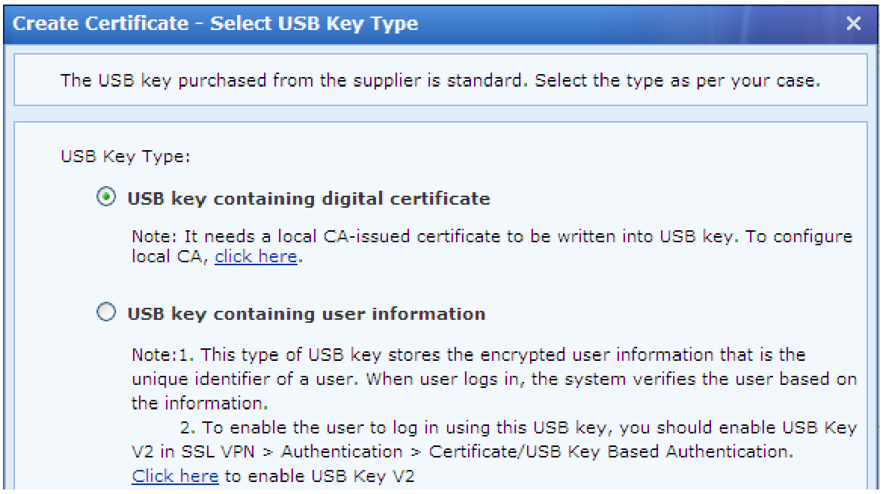
b. Install the USB key driver as instructed.

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** button to select a USB key type, as shown below:



Create Certificate - Select USB Key Type

The USB key purchased from the supplier is standard. Select the type as per your case.

USB Key Type:

● USB key containing digital certificate

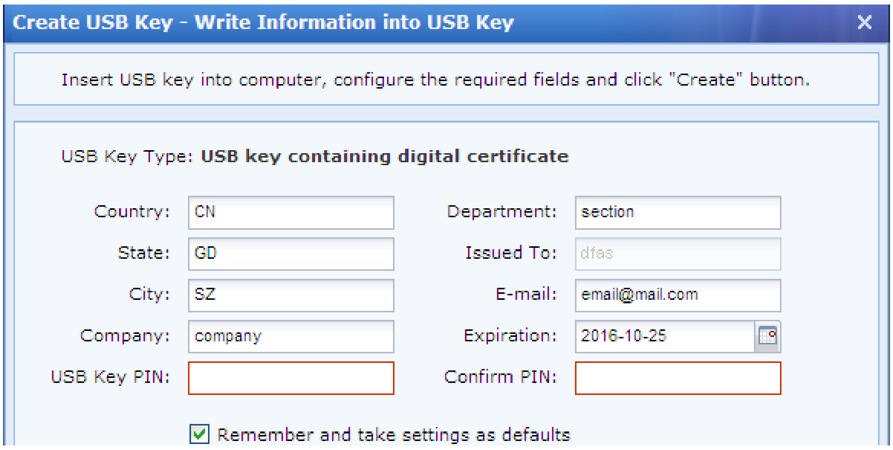
Note: It needs a local CA-issued certificate to be written into USB key. To configure local CA, click here.

○ USB key containing user information

Note:1. This type of USB key stores the encrypted user information that is the unique identifier of a user. When user logs in, the system verifies the user based on the information.

2. To enable the user to log in using this USB key, you should enable USB Key V2 in SSL VPN > Authentication > Certificate/USB Key Based Authentication. Click here to enable USB Key V2

If **USB key containing digital certificate**s selected, thus key should contain 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 VPNwith USB key, he or she has to enter the PIN.


Create USB Key - Write Information into USB Key

Insert USB key into computer, configure the required fields and click "Create" button.

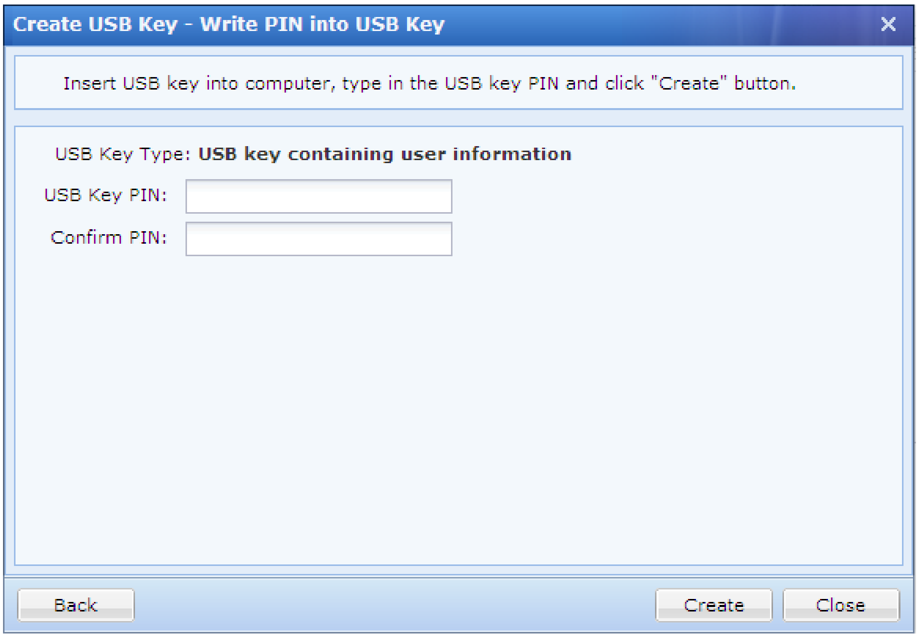
USB Key Type: **USB key containing digital certificate**

Country:	CN	Department:	section
State:	GD	Issued To:	dfas
City:	SZ	E-mail:	email@mail.com
Company:	company	Expiration:	2016-10-25
USB Key PIN:		Confirm PIN:	

☑ Remember and take settings as defaults

Above is one of thesolutions, 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 **USB key containing user information** is selected, thus key will storeuser'sstrictly encrypted features (unique identifier) based on which the connecting user will be verified, as shown in the figure below:


Create USB Key - Write PIN into USB Key

Insert USB key into computer, type in the USB key PIN and click "Create" button.

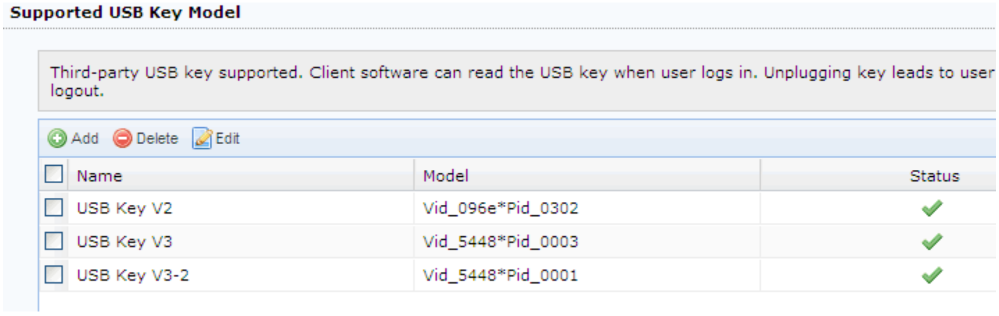
USB Key Type: **USB key containing user information**

USB Key PIN:

Confirm PIN:

The generated driver-free USB key cannot be reused to generate the other kind of USB key that needs driver.

For **USB key containing 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:



Supported USB Key Model

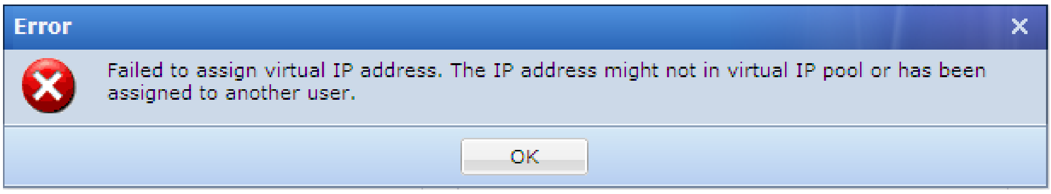
Third-party USB key supported. Client software can read the USB key when user logs in. Unplugging key leads to user logout.

□	Name	Model	Status
□	USB Key V2	Vid_096e*Pid_0302	✓
□	USB Key V3	Vid_5448*Pid_0003	✓
□	USB Key V3-2	Vid_5448*Pid_0001	✓

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:



Error

Failed to assign virtual IP address. The IP address might not in virtual IP pool or has been assigned to another user.

⚠

- 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. **Expire** indicates the date on which this user account will get invalid. If **Never** is selected, the user account will be valid always. If **On date** 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 sectioning Chapter 4.

   - **Public user:** Indicate sthat 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.

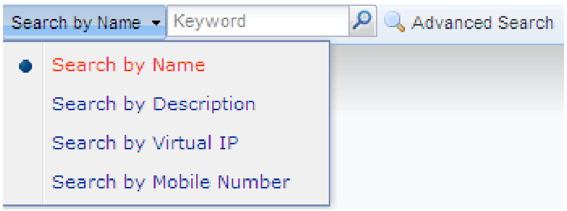
9. Associate user with policy set. For detailed guide, please refer to the Adding User Group sectioning Chapter 4.

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.

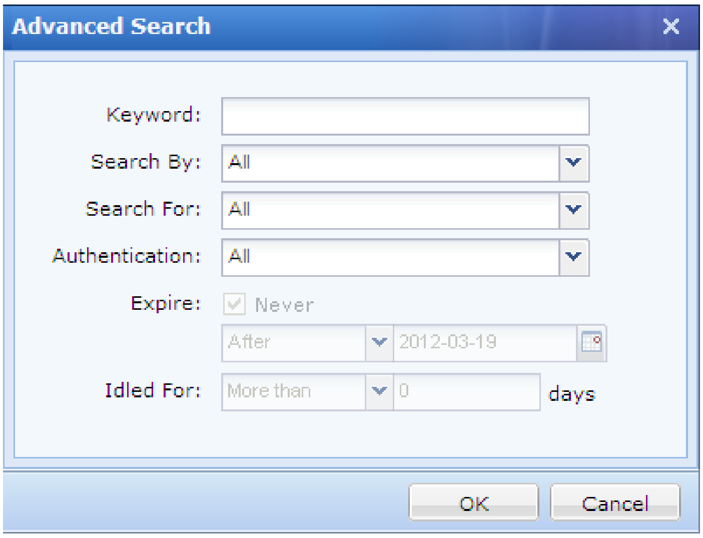
Searching for Users

At the upper right of **User Management** page, there IsaSearchtool 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:


Advanced Search

Keyword:

Search By: All

Search For: All

Authentication: All

Expire: ☑ Never

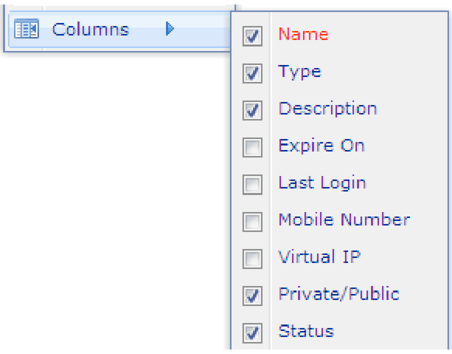
After 2012-03-19

Idled For: More than 0 days

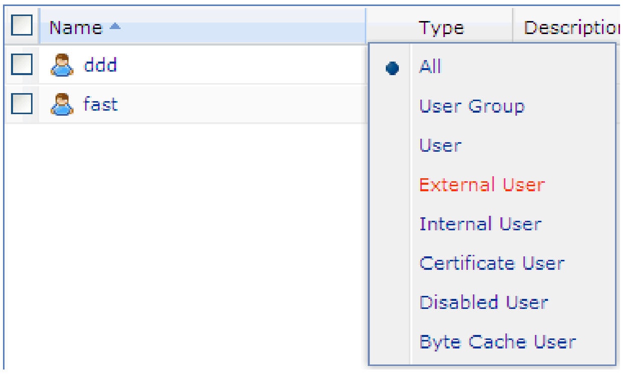
Search criteria are keyword, type of keyword, type of users, authentication method, expiry date and idleness of the user account.

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:

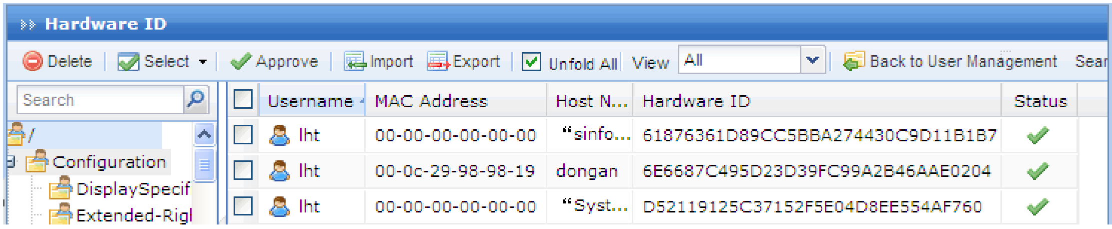


To filter users and view only one category of users, click column header **Type**, as shown below:



Managing Hardware IDs

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

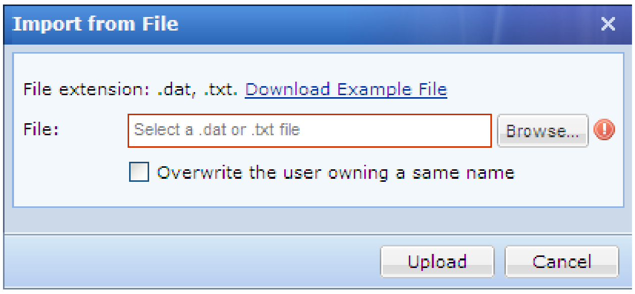


□	Username	MAC Address	Host N...	Hardware ID	Status
□	lht	00-00-00-00-00-00	“sinfo...	61876361D89CC5BBA274430C9D11B1B7	✓
□	lht	00-0c-29-98-98-19	dongan	6E6687C495D23D39FC99A2B46AAE0204	✓
□	lht	00-00-00-00-00-00	“Syst...	D52119125C37152F5E04D8EE554AF760	✓

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

- **Delete:** Clickit 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:** Clickit and the selected hardware ID(s) will be approved and the corresponding user will be able to passhardware 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:** Clickit to import hardware IDs by hand, as shown below:



Import from File

File extension: .dat, .txt. Download Example File

File: Select a .dat or .txt file

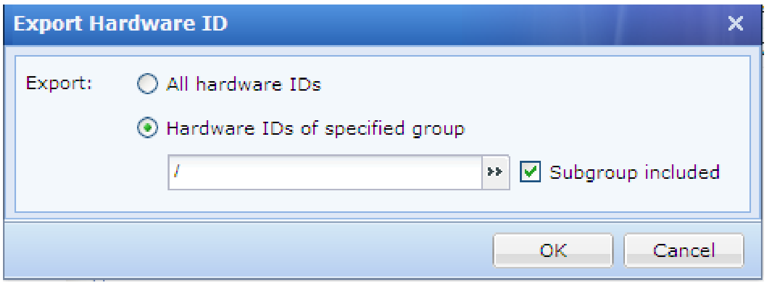
□ Overwrite the user owning a same name

For the file format and the way of maintaining the file that contains hardware IDs, click the **Download Example File** linkto 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:



Export Hardware ID

Export: ○ All hardware IDs

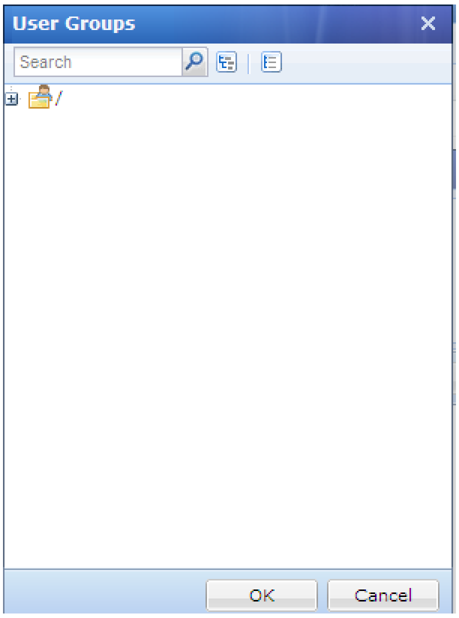
● Hardware IDs of specified group

/ ☑ Subgroup included

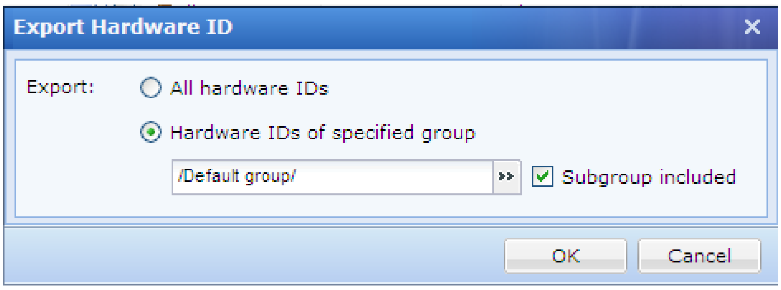
a. Specify the hardware IDs that you want to export.

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:


Export Hardware ID

Export: ○ All hardware IDs

● Hardware IDs of specified group

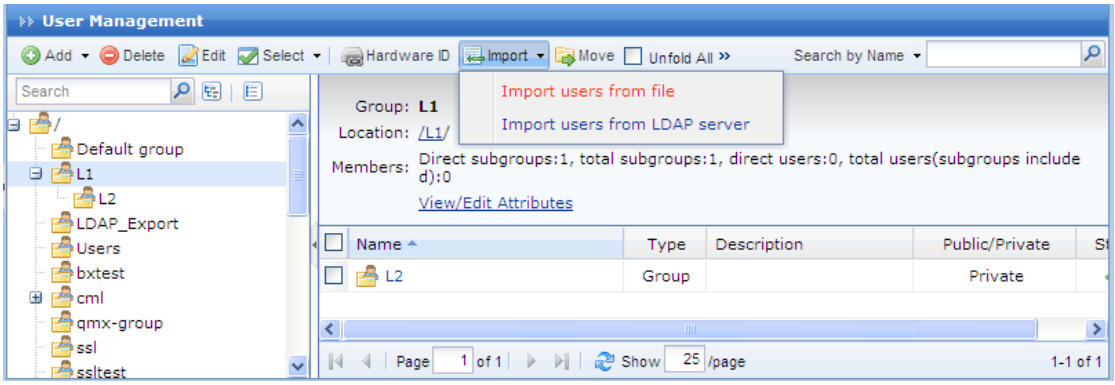
/Default group/ ☑ Subgroup included

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:



Group: **L1**

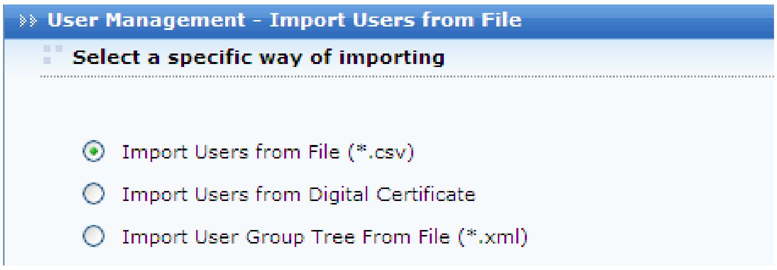
Location: /L1/

Members: Direct subgroups:1, total subgroups:1, direct users:0, total users(subgroups included):0

□	Name	Type	Description	Public/Private	St
□	L2	Group		Private	

Importing Users from File

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


User Management - Import Users from File

Select a specific way of importing

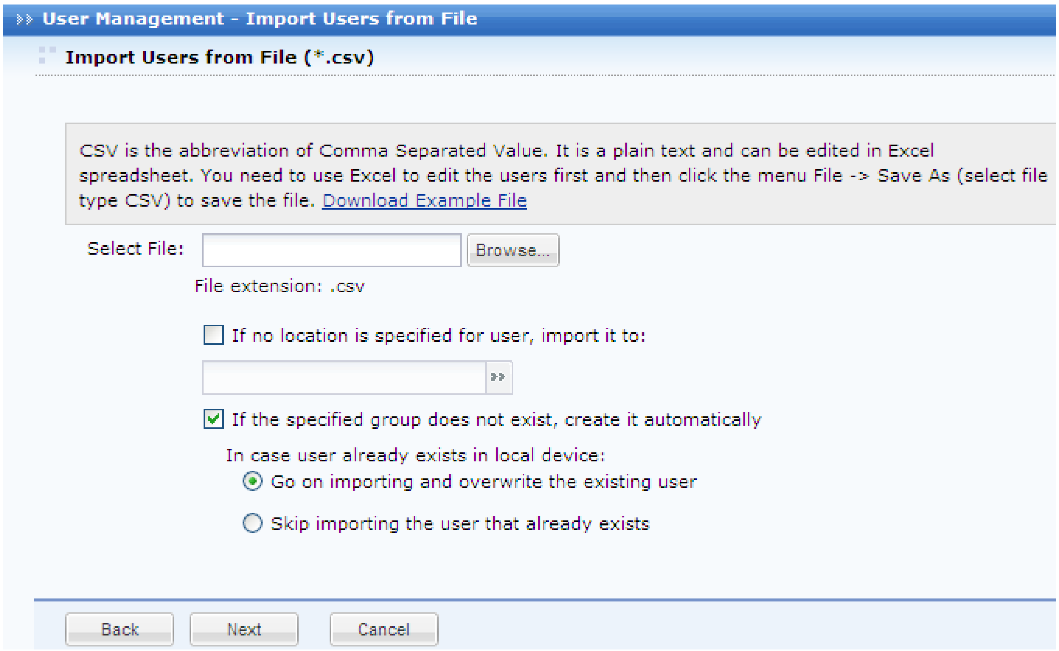
● Import Users from File (*.csv)

○ Import Users from Digital Certificate

○ Import User Group Tree From File (*.xml)

2. Select a way of importing.

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



Import Users from File (*.csv)

CSV is the abbreviation of Comma Separated Value. It is a plain text and can be edited in Excel spreadsheet. You need to use Excel to edit the users first and then click the menu File -> Save As (select file type CSV) to save the file. Download Example File

Select File: Browse...

File extension: .csv

□ If no location is specified for user, import it to:

☑ If the specified group does not exist, create it automatically

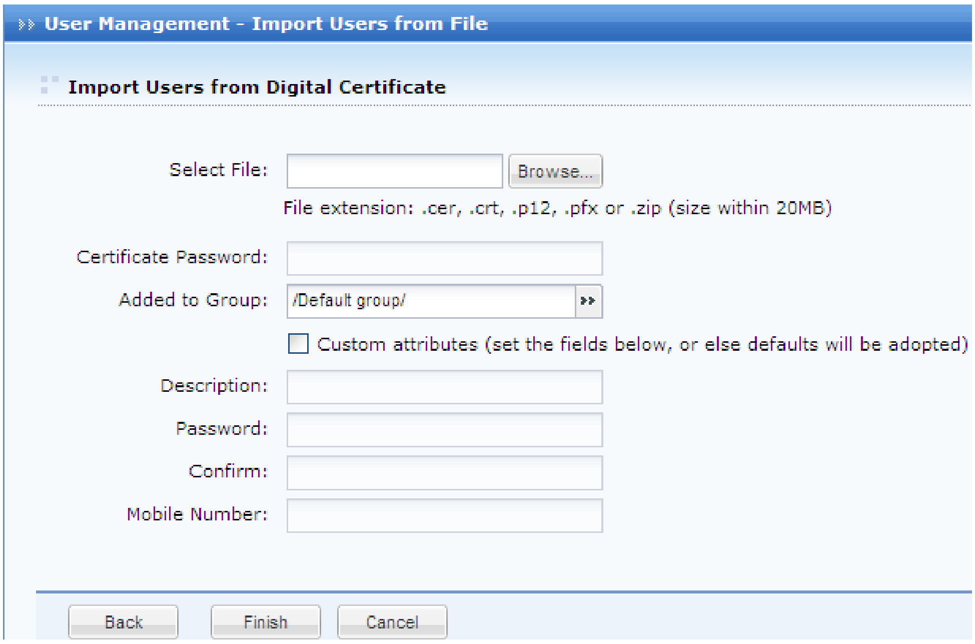
In case user already exists in local device:

● Go on importing and overwrite the existing user

○ Skip importing the user that already exists

- **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**s selected, the contents included are as follows:


User Management - Import Users from File

Import Users from Digital Certificate

Select File: Browse...

File extension: .cer, .crt, .p12, .pfx or .zip (size within 20MB)

Certificate Password:

Added to Group: /Default group/

□ Custom attributes (set the fields below, or else defaults will be adopted)

Description:

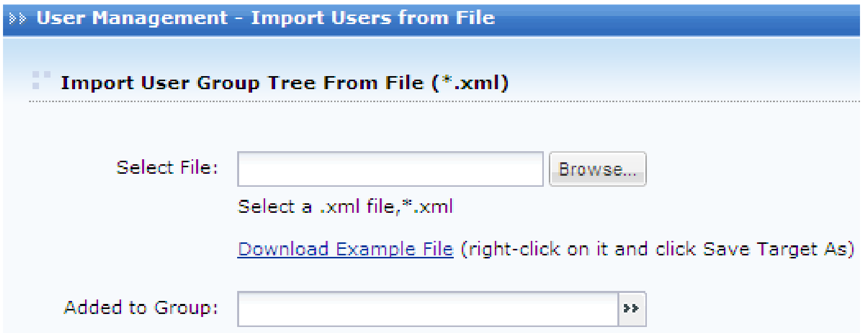
Password:

Confirm:

Mobile Number:

- **Select File:**Browse a certificate file with the .cer, .crt, .p12 or .pfxextension; 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 hereafter 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:


User Management - Import Users from File

Import User Group Tree From File (*.xml)

Select File: Browse...

Select a .xml file,*.xml

Download Example File (right-click on it and click Save Target As)

Added to Group:

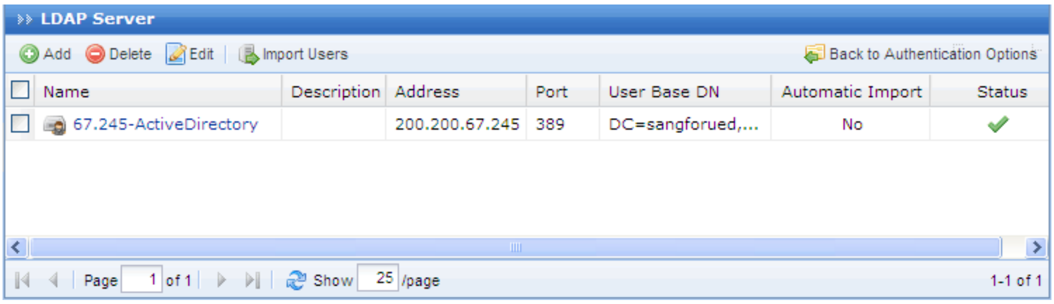
- **Select File:**Browse the XML file that you have edited. For more details of how to maintain the file, click the **Download Example File** link to download a copy and refer to the instructions in it.
- **Added to Group:** This specifies the user group to which the group tree will be added.

3. Configure the corresponding options on the above pages.

4. Click the **Finish** button to import the users.

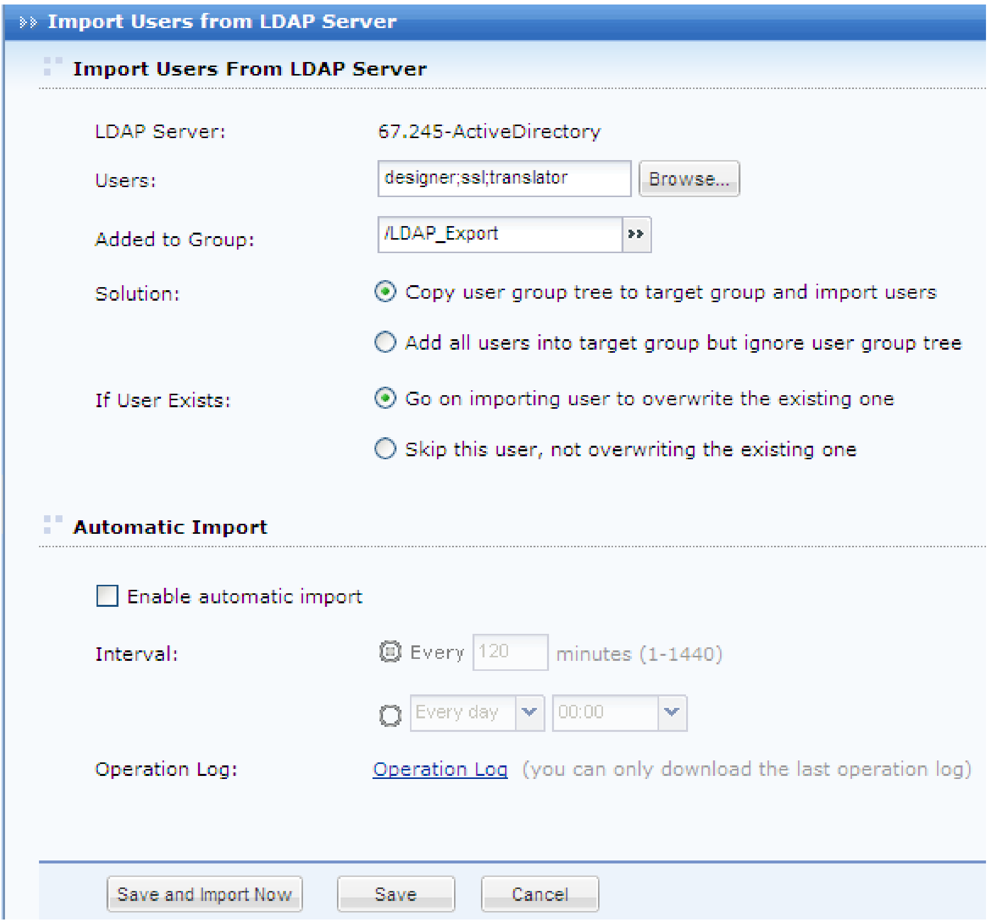
Importing Users from LDAP Server

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



□	Name	Description	Address	Port	User Base DN	Automatic Import	Status
□	67.245-ActiveDirectory		200.200.67.245	389	DC=sangforued,...	No	✓

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



Import Users From LDAP Server

LDAP Server: 67.245-ActiveDirectory

Users: designer;ssl;translator

Added to Group: /LDAP_Export

Solution: ● Copy user group tree to target group and import users ○ Add all users into target group but ignore user group tree

If User Exists: ● Go on importing user to overwrite the existing one ○ Skip this user, not overwriting the existing one

Automatic Import

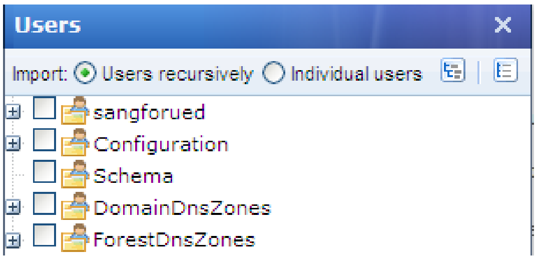
□ Enable automatic import

Interval: ○ Every 120 minutes (1-1440) ○ Every day 00:00

Operation Log: Operation Log (you can only download the last operation log)

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 **User Management** 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.
- **Solution:** Solution of importing users falls into two types. 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**.
- **Operation Log:** To view the log of the last operation, click **Operation Log**.

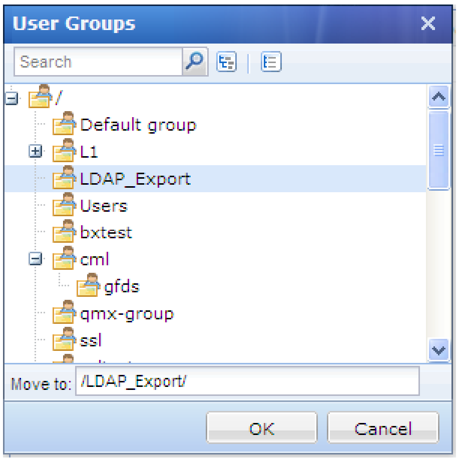
⚠

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 resultwill show up at the top of page.

Moving Users to Another Group

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



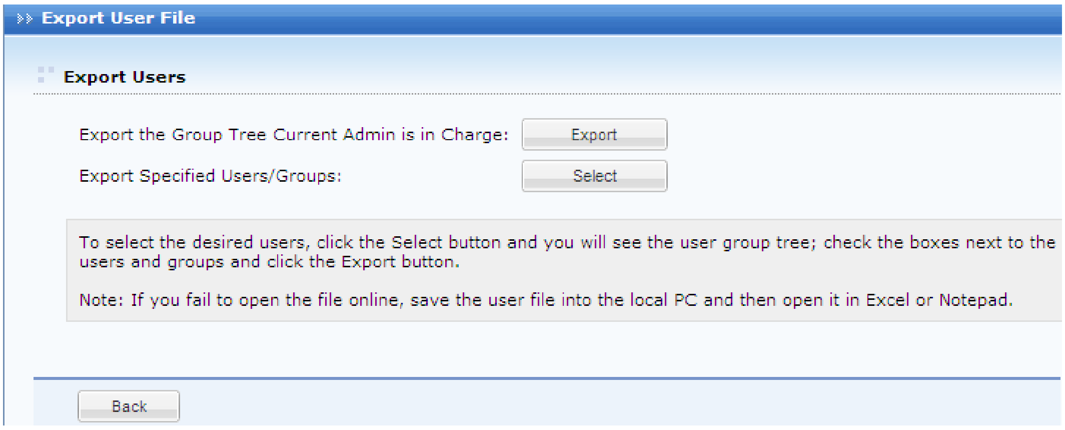
Move to: /LDAP_Export/

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

3. Click the **OK** button.

Exporting Users

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

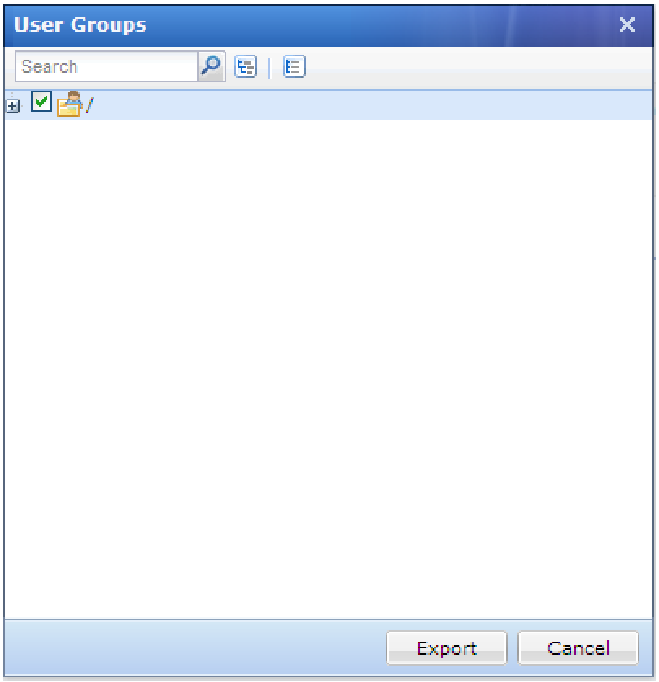

Export User File
Export Users
Export the Group Tree Current Admin is in Charge:
Export
Export Specified Users/Groups:
Select
Back

To select the desired users, click the Select button and you will see the user group tree; check the boxes next to the users and groups and click the Export button.

Note: If you fail to open the file online, save the user file into the local PC and then open it in Excel or Notepad.

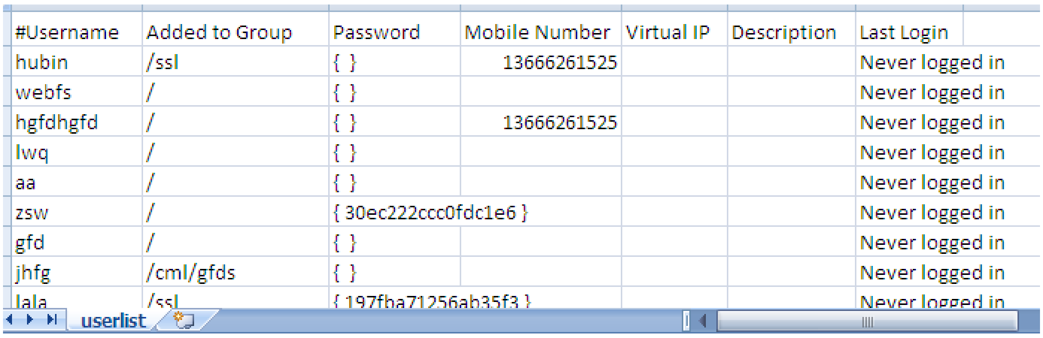
2. Select the objects that you want to export.

   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 thelocal computer.

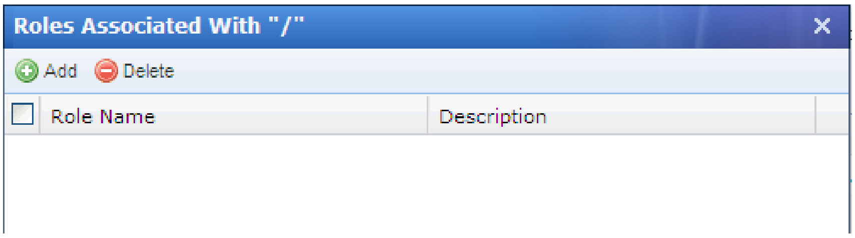
   The exported user information includes username, group path, password (encrypted by an algorithm developed by SANGFOR), mobile number, virtual IP address, description and the time user logged in last time, as shown below:



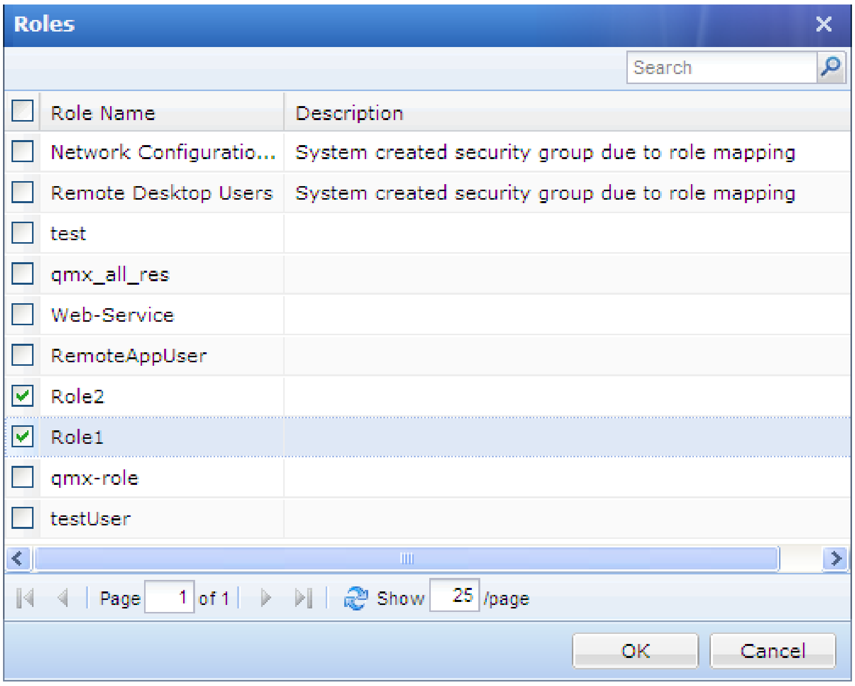
#Username	Added to Group	Password	Mobile Number	Virtual IP	Description	Last Login
hubin	/ssl	{ }	13666261525			Never logged in
webfs	/	{ }				Never logged in
hgfdhgfd	/	{ }	13666261525			Never logged in
lwq	/	{ }				Never logged in
aa	/	{ }				Never logged in
zsw	/	{ 30ec222ccc0fdc1e6 }				Never logged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

Associating Roles with User

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



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



	Role Name	Description
□	Network Configuratio...	System created security group due to role mapping
□	Remote Desktop Users	System created security group due to role mapping
□	test	
□	qmx_all_res	
□	Web-Service	
□	RemoteAppUser	
☑	Role2	
☑	Role1	
□	qmx-role	
□	testUser	

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.

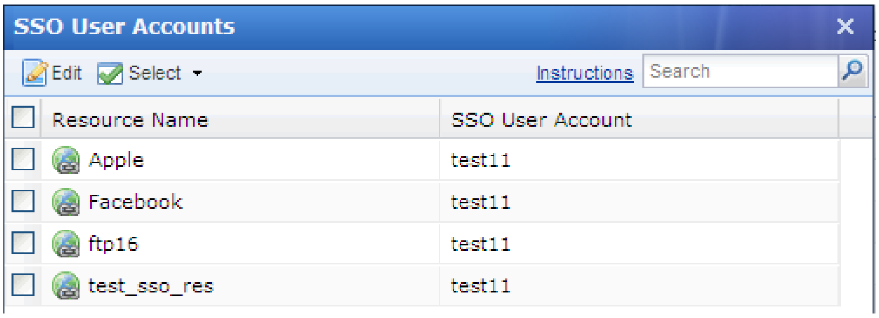
Configuring SSO User Account

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.

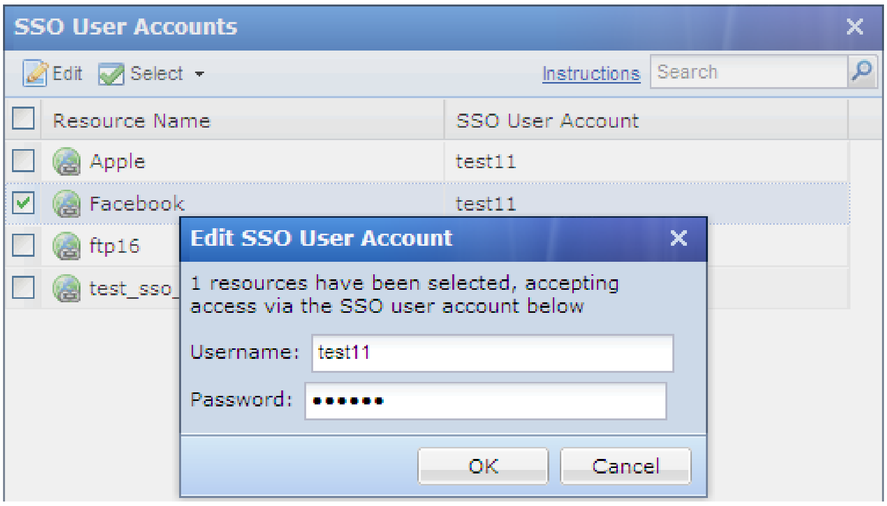
To configure SSO user account for a user, perform the following steps:

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



□	Resource Name	SSO User Account
□	Apple	test11
□	Facebook	test11
□	ftp16	test11
□	test_sso_res	test11

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



□	Resource Name	SSO User Account
□	Apple	test11
☑	Facebook	test11
□	ftp16	
□	test_sso_	

1 resources have been selected, accepting access via the SSO user account below

Username: test11

Password: ••••••

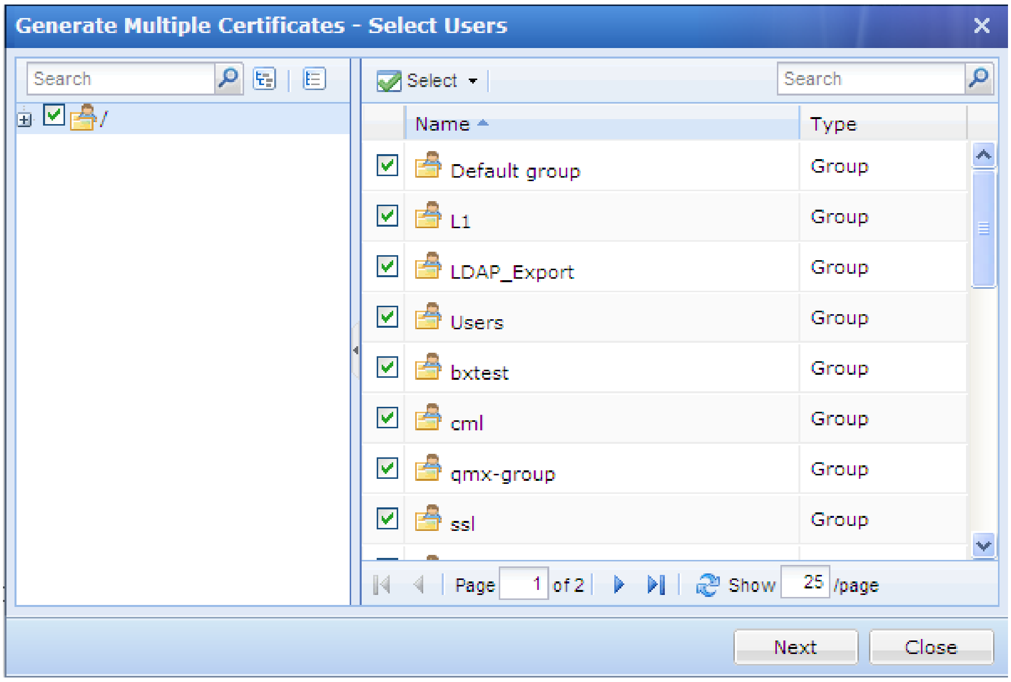
3. Enter the username and password of the SSO user account into the corresponding fields, and click the **OK** button. The newly created SSO user account is configured.

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**>**User Management** page and click **More**>**Generate multiple certificates**, as shown below:

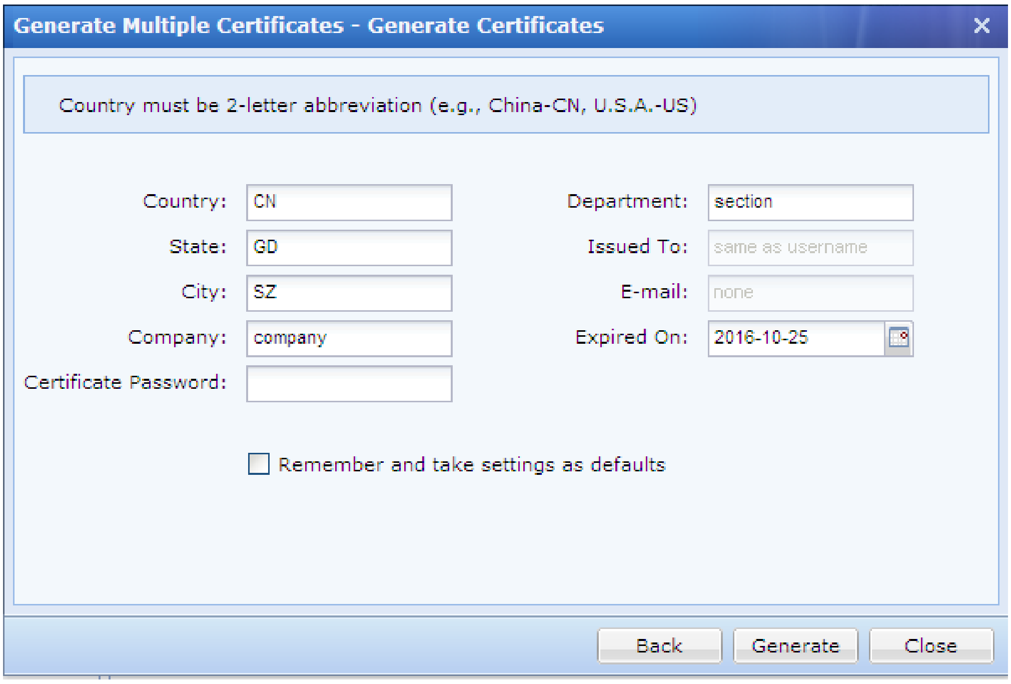


Generate Multiple Certificates - Select Users

	Name	Type
☑	Default group	Group
☑	L1	Group
☑	LDAP_Export	Group
☑	Users	Group
☑	bxtest	Group
☑	cml	Group
☑	qmx-group	Group
☑	ssl	Group

Page 1 of 2 Show 25 /page

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



Generate Multiple Certificates - Generate Certificates

Country must be 2-letter abbreviation (e.g., China-CN, U.S.A.-US)

Country: CN

State: GD

City: SZ

Company: company

Certificate Password:

Department: section

Issued To: same as username

E-mail: none

Expired On: 2016-10-25

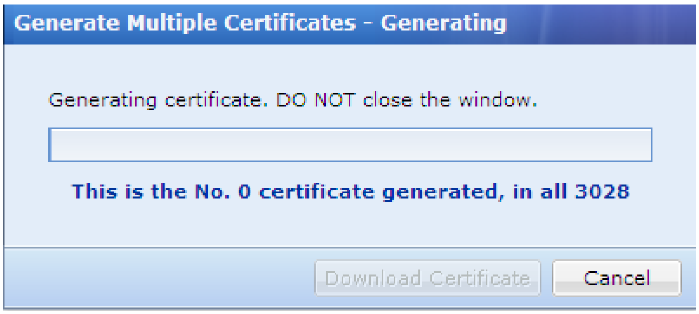
☐ Remember and take settings as defaults

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

- Configure the required fields, such as **Country**, **State**, **City**, **Company**, **Department**, **ExpiredOn** and **Certificate Password**. **E-Mail** is not configurable. **Issue 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:



Generating certificate. DO NOT close the window.

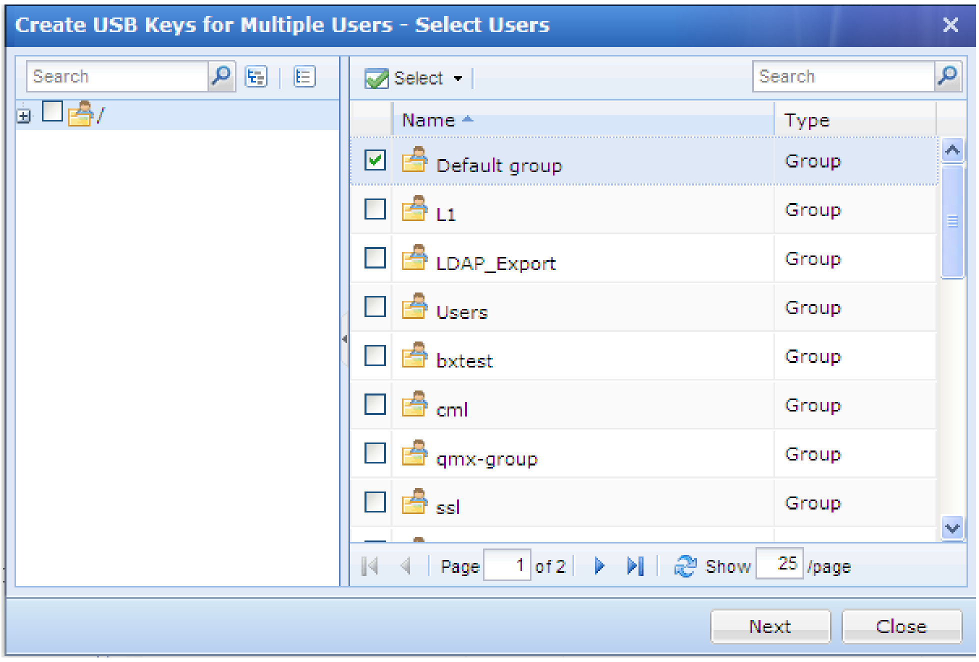
This is the No. 0 certificate generated, in all 3028

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

Creating Multiple USB Keys for Users

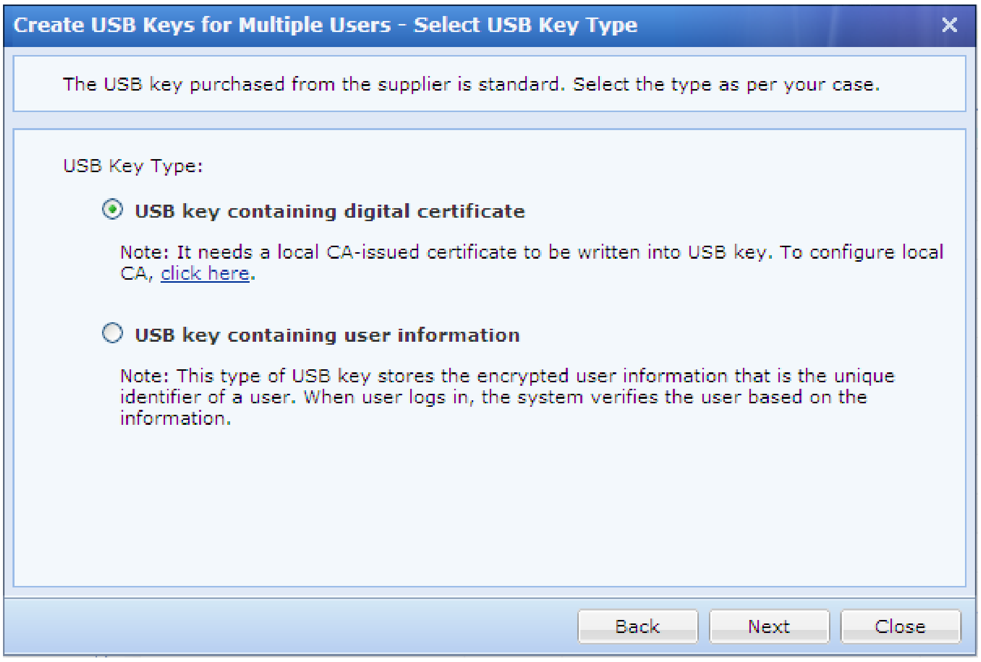
To save time and trouble, creating USB keys for a bunch of users is a good choice.

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



	Name	Type
☑	Default group	Group
□	L1	Group
□	LDAP_Export	Group
□	Users	Group
□	bxtest	Group
□	cml	Group
□	qmx-group	Group
□	ssl	Group

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



Create USB Keys for Multiple Users - Select USB Key Type

The USB key purchased from the supplier is standard. Select the type as per your case.

USB Key Type:

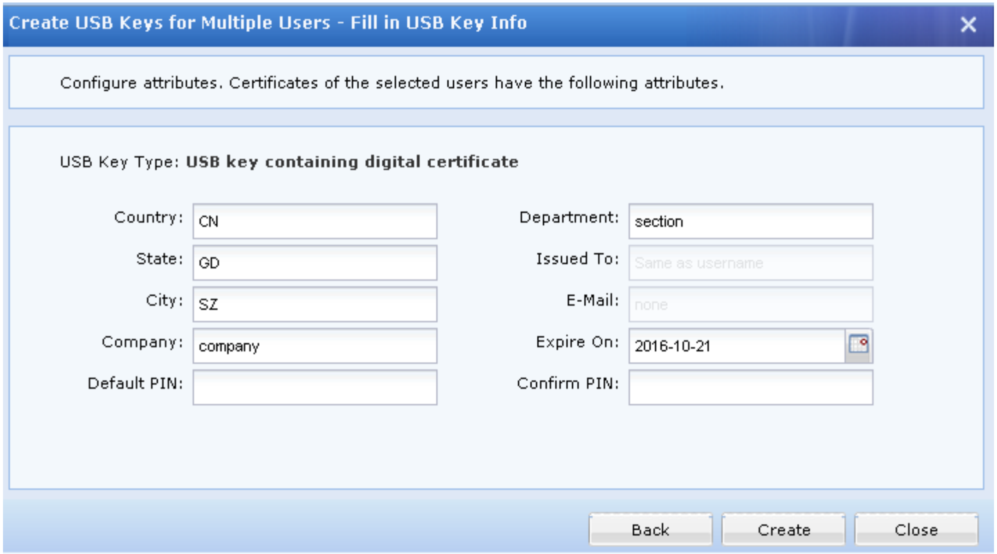
● **USB key containing digital certificate**

Note: It needs a local CA-issued certificate to be written into USB key. To configure local CA, click here.

○ **USB key containing user information**

Note: This type of USB key stores the encrypted user information that is the unique identifier of a user. When user logs in, the system verifies the user based on the information.

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



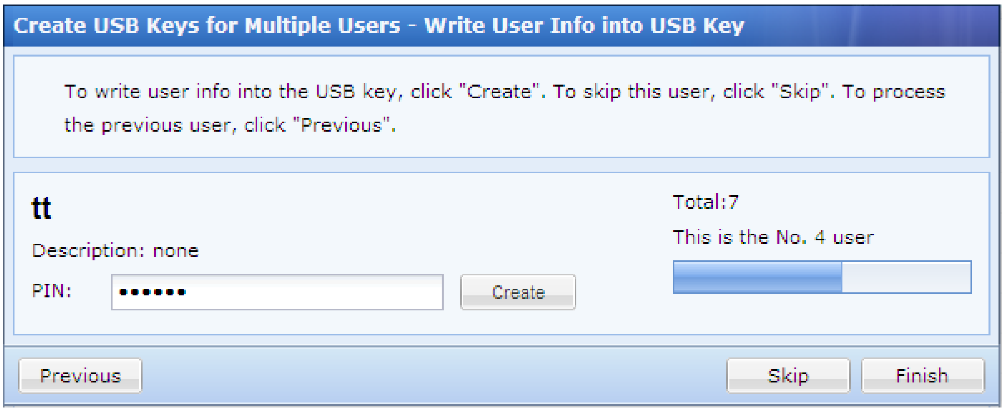
Create USB Keys for Multiple Users - Fill in USB Key Info

Configure attributes. Certificates of the selected users have the following attributes.

USB Key Type: **USB key containing digital certificate**

Country:	CN	Department:	section
State:	GD	Issued To:	Same as username
City:	SZ	E-Mail:	none
Company:	company	Expire On:	2016-10-21
Default PIN:		Confirm PIN:	

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


Create USB Keys for Multiple Users - Write User Info into USB Key

To write user info into the USB key, click "Create". To skip this user, click "Skip". To process the previous user, click "Previous".

tt

Description: none

PIN: ••••••

Total:7

This is the No. 4 user

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.

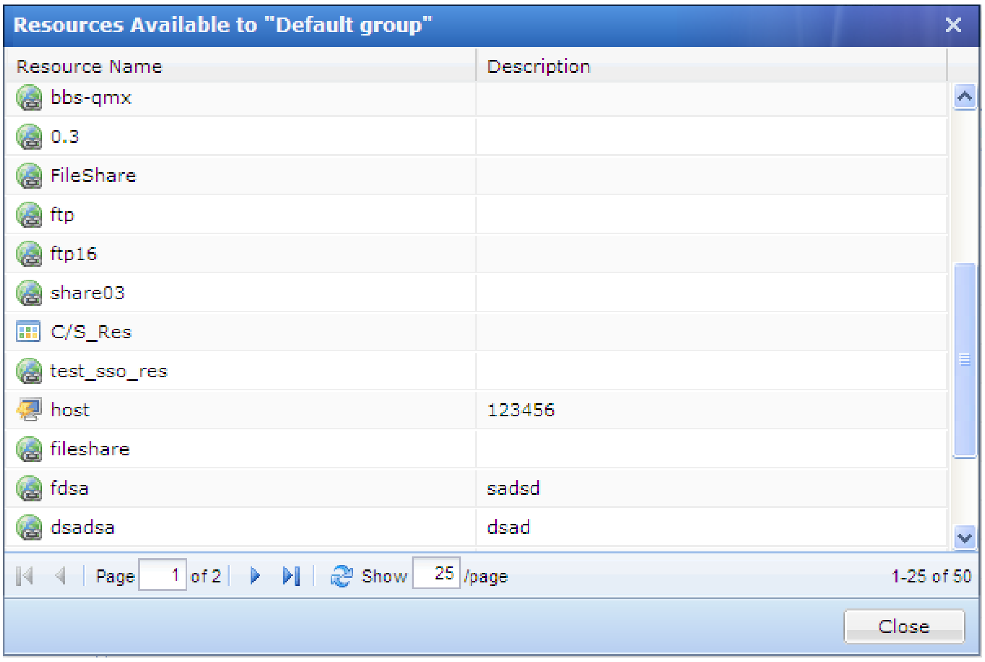
   To rewrite information into the USB key of the previous user, click the **previous** button.

   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:

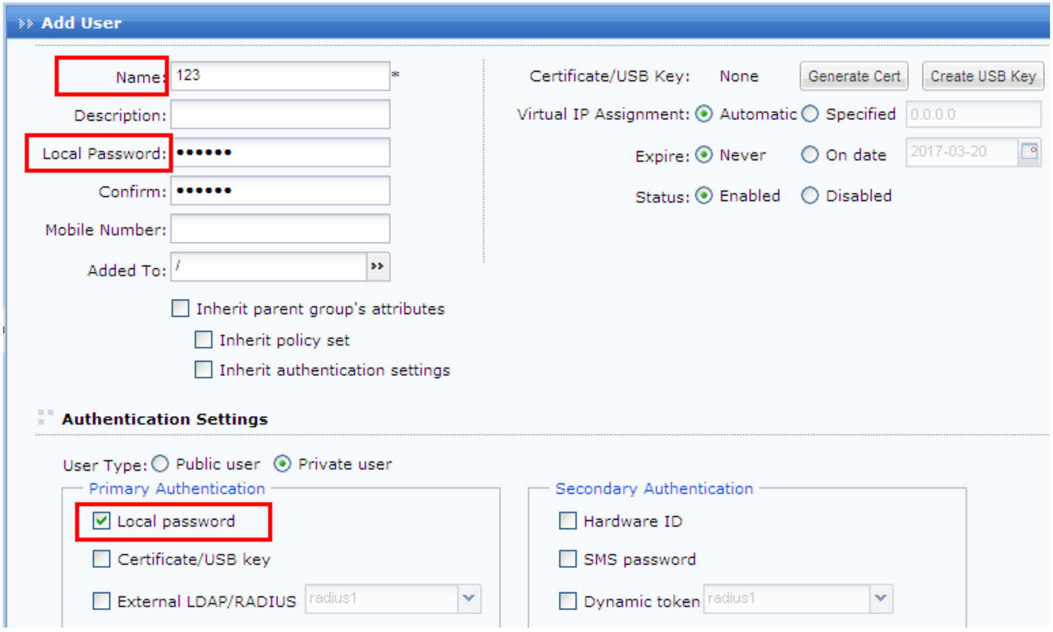

Resources Available to "Default group"

Resource Name	Description
bbs-qmx	
0.3	
FileShare	
ftp	
ftp16	
share03	
C/S_Res	
test_sso_res	
host	123456
fileshare	
fdsa	sadsd
dsadsa	dsad

Page 1 of 2 Show 25 /page 1-25 of 50

Scenario 8: Adding User Logging in with Local Password

1. Navigate to **SSL VPN**>**Users**>**User Management** and click **Add**>**User** to enter the **Add Us**er page.
2. Configure **Name** and **Local Password** fields.
3. Configure **Authentication Settings**. Select **Local password**, as shown below:



Name: 123 *
Description:
Local Password: ••••••
Confirm: ••••••
Mobile Number:
Added To: /

□ Inherit parent group's attributes
□ Inherit policy set
□ Inherit authentication settings

Certificate/USB Key: None
Virtual IP Assignment: ● Automatic ○ Specified 0.0.0.0
Expire: ● Never ○ On date 2017-03-20
Status: ● Enabled ○ Disabled

Authentication Settings

User Type: ○ Public user ● Private user

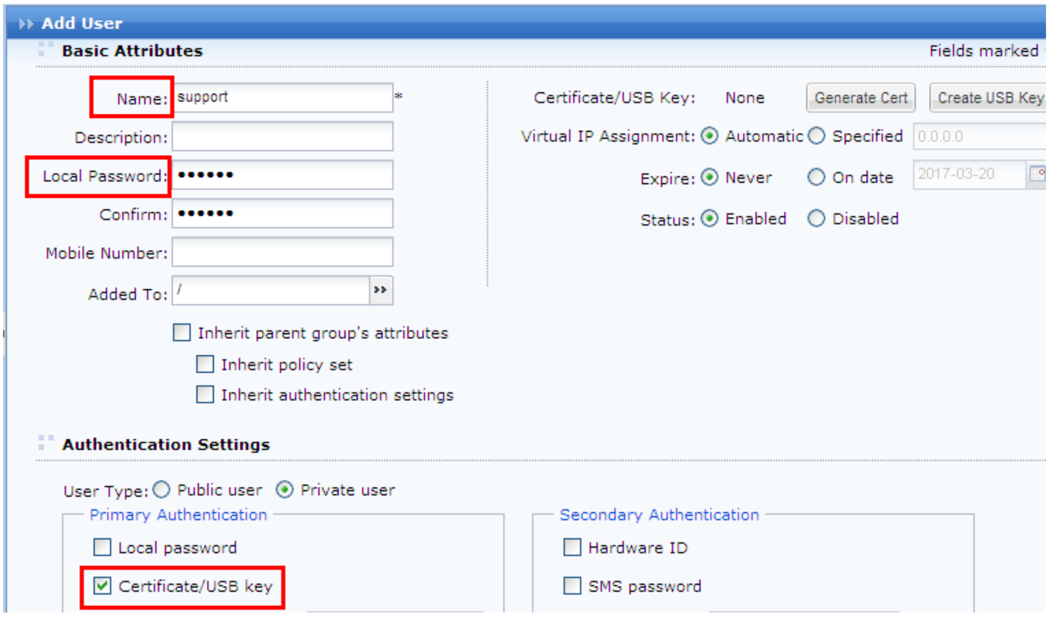
Primary Authentication
☑ Local password
□ Certificate/USB key
□ External LDAP/RADIUS radius1

Secondary Authentication
□ Hardware ID
□ SMS password
□ Dynamic token radius1

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

Scenario 9: 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**>**User Management** and click **Add**>**User** to add a new user, as shown in the figure below:



Basic Attributes

Fields marked

Name: support *

Description:

Local Password: ••••••

Confirm: ••••••

Mobile Number:

Added To: /

□ Inherit parent group's attributes

□ Inherit policy set

□ Inherit authentication settings

Certificate/USB Key: None

Virtual IP Assignment: ● Automatic ○ Specified 0.0.0.0

Expire: ● Never ○ On date 2017-03-20

Status: ● Enabled ○ Disabled

Authentication Settings

User Type: ○ Public user ● Private user

Primary Authentication

□ Local password

☑ Certificate/USB key

Secondary Authentication

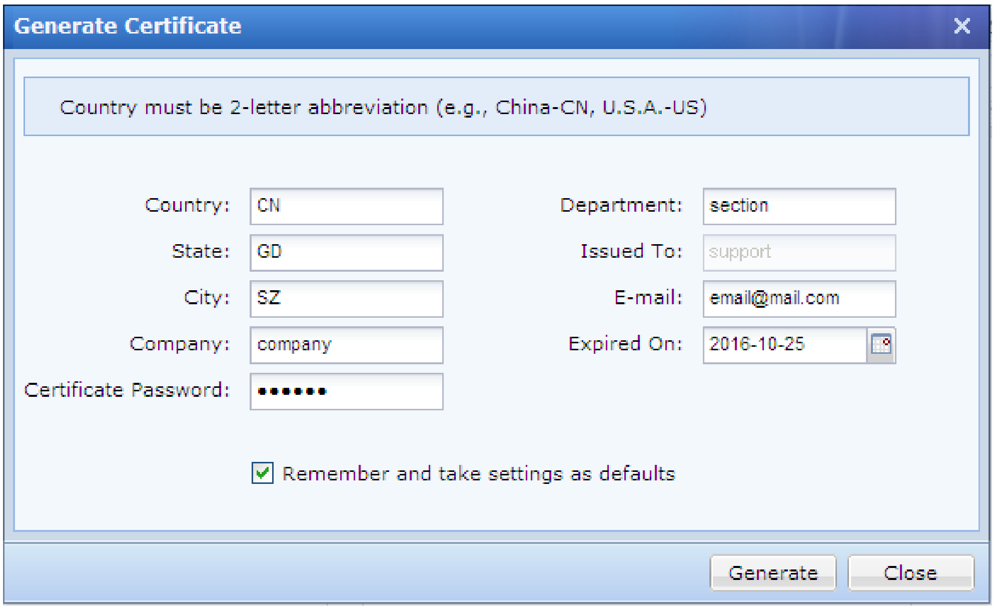
□ Hardware ID

□ SMS password

5. Configure **Name** and **Local Password** fields. Select user type **Private user**.

3. Configure **Authentication Settings**. Select primary authentication **Certificate/USB key**.

4. Click the **Generate Cert** button (button name is **Import Certificate** when current CA is external CA)to enter the **Generate Certificate** page and generate certificate for this user, as shown in the figure below:



Country must be 2-letter abbreviation (e.g., China-CN, U.S.A.-US)

Country: CN

State: GD

City: SZ

Company: company

Certificate Password: ••••••

Department: section

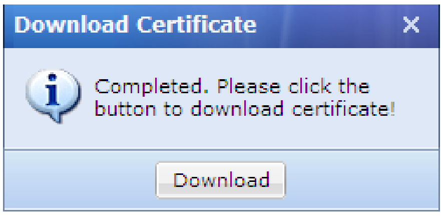
Issued To: support

E-mail: email@mail.com

Expired On: 2016-10-25

☑ Remember and take settings as defaults

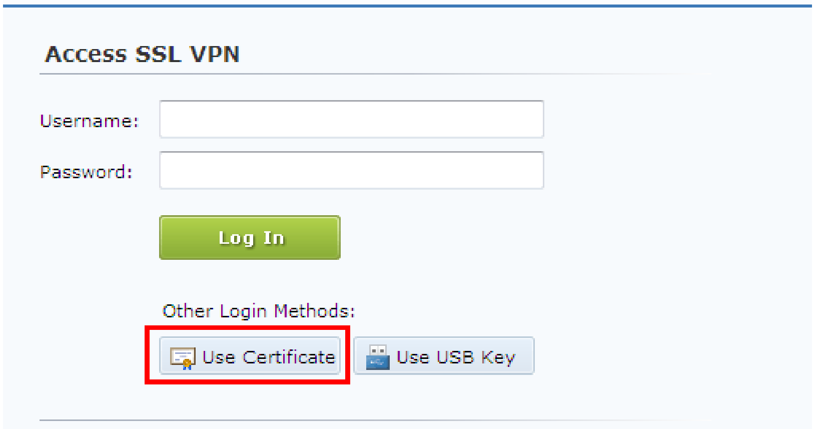
5. Configure the required fields and click the **Generate** button. If certificate is generated successfully, the following prompt will pop up:



Completed. Please click the button to download certificate!

6. Click **Download** to save the certificate file **support.p12** to the computer and send it to the end user.

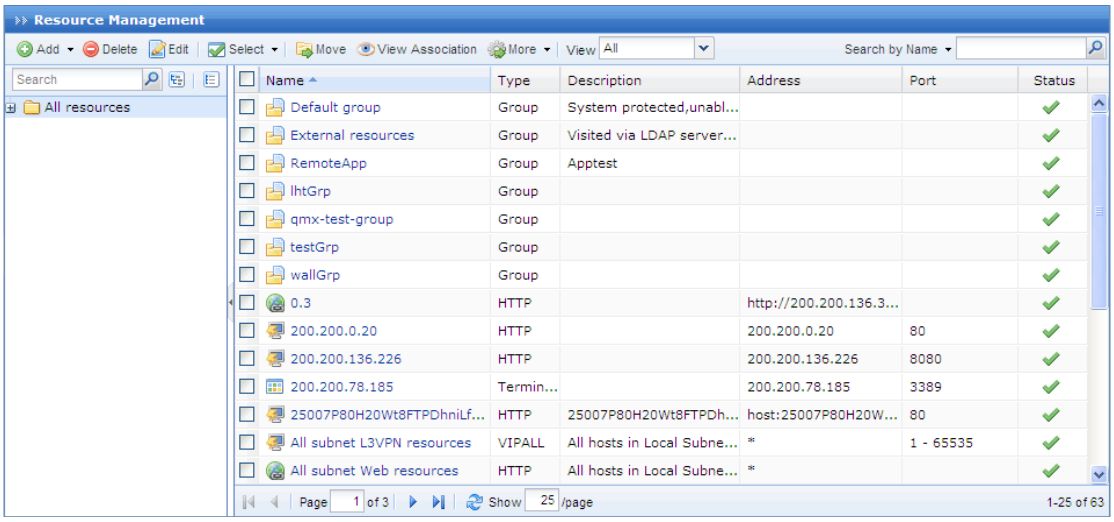
7. End user installs the certificate on his/her computer, visit the login page and select **Use Certificate** login method to connect to SSL VPN, as shown in the figure below:



Resources

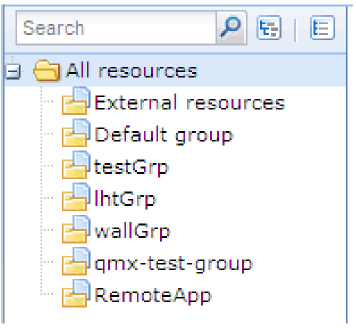
The resources we are talking about in this user manual are the resources that can be accessed by specified users over SSL VPN.

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



	Name	Type	Description	Address	Port	Status
□	Default group	Group	System protected,unabl...			✓
□	External resources	Group	Visited via LDAP server...			✓
□	RemoteApp	Group	Apptest			✓
□	lhtGrp	Group				✓
□	qmx-test-group	Group				✓
□	testGrp	Group				✓
□	wallGrp	Group				✓
□	0.3	HTTP		http://200.200.136.3...		✓
□	200.200.0.20	HTTP		200.200.0.20	80	✓
□	200.200.136.226	HTTP		200.200.136.226	8080	✓
□	200.200.78.185	Termin...		200.200.78.185	3389	✓
□	25007P80H20Wt8FTPDhniLf...	HTTP	25007P80H20Wt8FTPDh...	host:25007P80H20W...	80	✓
□	All subnet L3VPN resources	VIPALL	All hosts in Local Subne...	*	1 - 65535	✓
□	All subnet Web resources	HTTP	All hosts in Local Subne...	*		✓

A resource group could contain a number of resources entries. Similar trouser management, resources could be grouped according to categories and associated user or group, etc. Majority of administrators welcomes this kind of management because it makes resources more distinguishable.



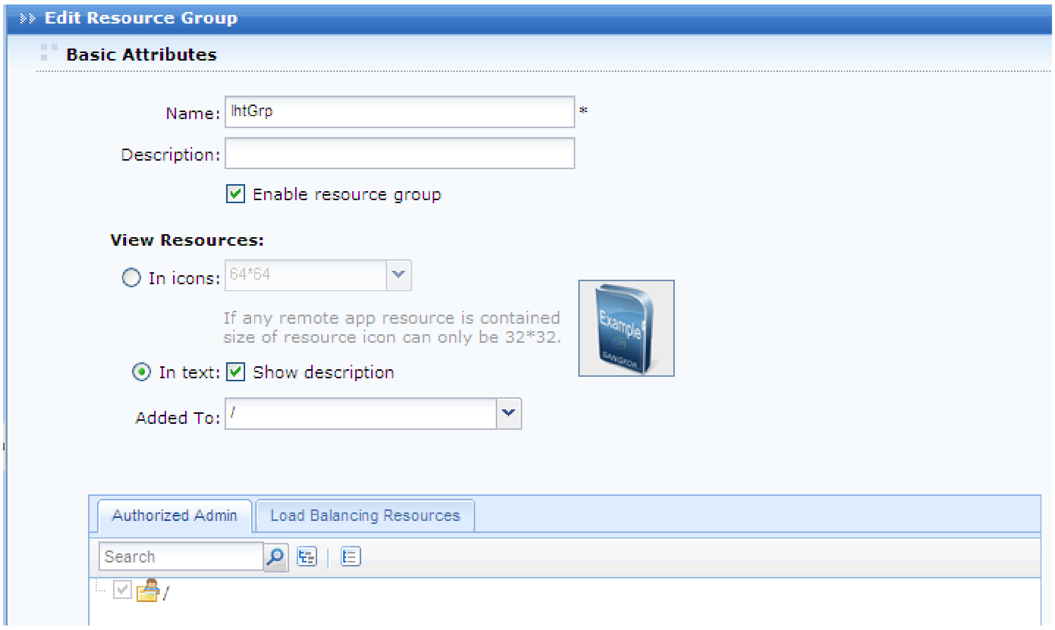
Navigate toss **VPN>Resources>Resources Management** and click on the resource group, and there sources included in the group are displayed on the right pane. The resource group tree is as shown in the figure on the right.

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**>**Group** to enter **Edit Resource Group**, as shown in the figure below:



Edit Resource Group

Basic Attributes

Name: lhtGrp *

Description:

☑ Enable resource group

View Resources:

○ In icons: 64*64

If any remote app resource is contained size of resource icon can only be 32*32.

● In text: ☑ Show description

Added To: /

Authorized Admin | Load Balancing Resources

Search

☑ /

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.

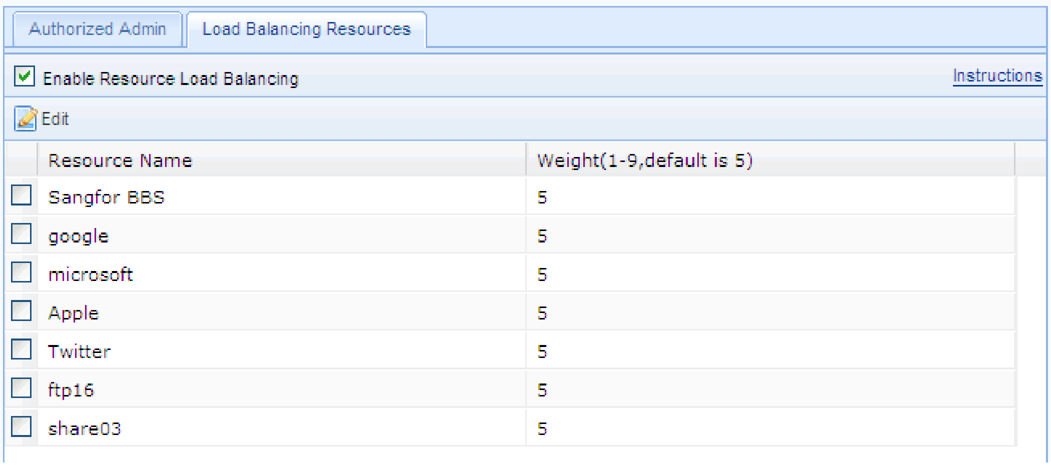
- **View resource:** Indicates the way resources are displayed on **Resource** page, in icon or in text. If **In Icons** is selected, define the icon size, **48*48**, **64*64** or **128*128**, so that the resources will be displayed in icon as wanted. If **In Text** is selected, you may select **Show description** of the resource. To manage icons, refer to the Uploading Icon to Device sectioning 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. The resources contained in this tab are attached with weight that ranges from 1 to 9 (by default, it is 5), as shown below:



☑ Enable Resource Load Balancing

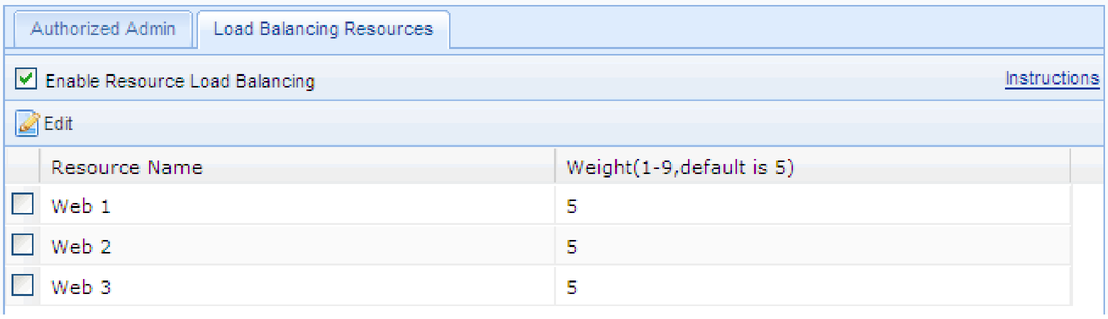
	Resource Name	Weight(1-9,default is 5)
□	Sangfor BBS	5
□	google	5
□	microsoft	5
□	Apple	5
□	Twitter	5
□	ftp16	5
□	share03	5

- 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 **five**, as shown below:

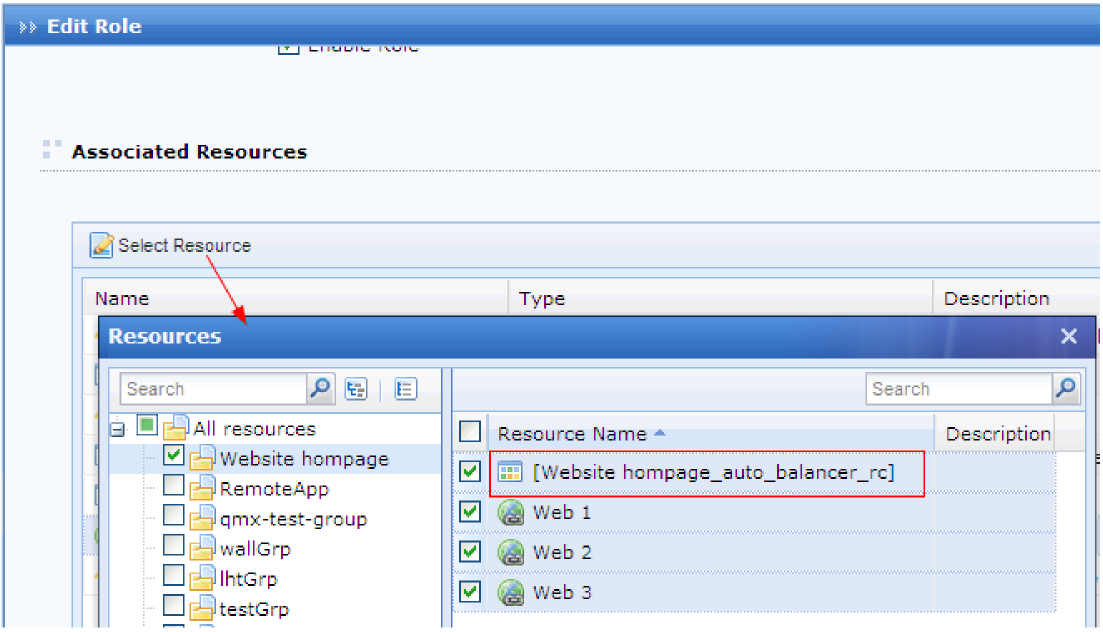


☑ Enable Resource Load Balancing

	Resource Name	Weight(1-9,default is 5)
□	Web 1	5
□	Web 2	5
□	Web 3	5

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:



Edit Role

Associated Resources

Select Resource

Name	Type	Description

Resources

Search

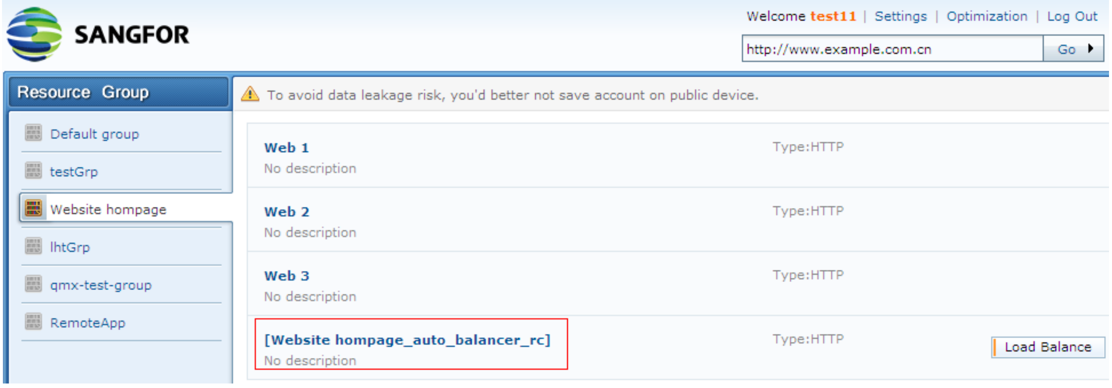
- ☐ All resources
  - ☑ Website hompage
  - ☐ RemoteApp
  - ☐ qmx-test-group
  - ☐ wallGrp
  - ☐ lhtGrp
  - ☐ testGrp

Search

☐	Resource Name	Description
☑	[Website hompage_auto_balancer_rc]	
☑	Web 1	
☑	Web 2	
☑	Web 3	

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 **Web1**, the second five users access there source launched by **Web2** and the third five connecting users access the resource launched by **Web3**. Through this way, load of the three servers is kept balanced (to associate resources with user or group, refer to the Role sectioning Chapter 4).

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



SANGFOR

Welcome test11 | Settings | Optimization | Log Out

http://www.example.com.cn Go

Resource Group

- Default group
- testGrp
- Website hompage
- lhtGrp
- qmx-test-group
- RemoteApp

To avoid data leakage risk, you'd better not save account on public device.

Web 1
No description
Type:HTTP

Web 2
No description
Type:HTTP

Web 3
No description
Type:HTTP

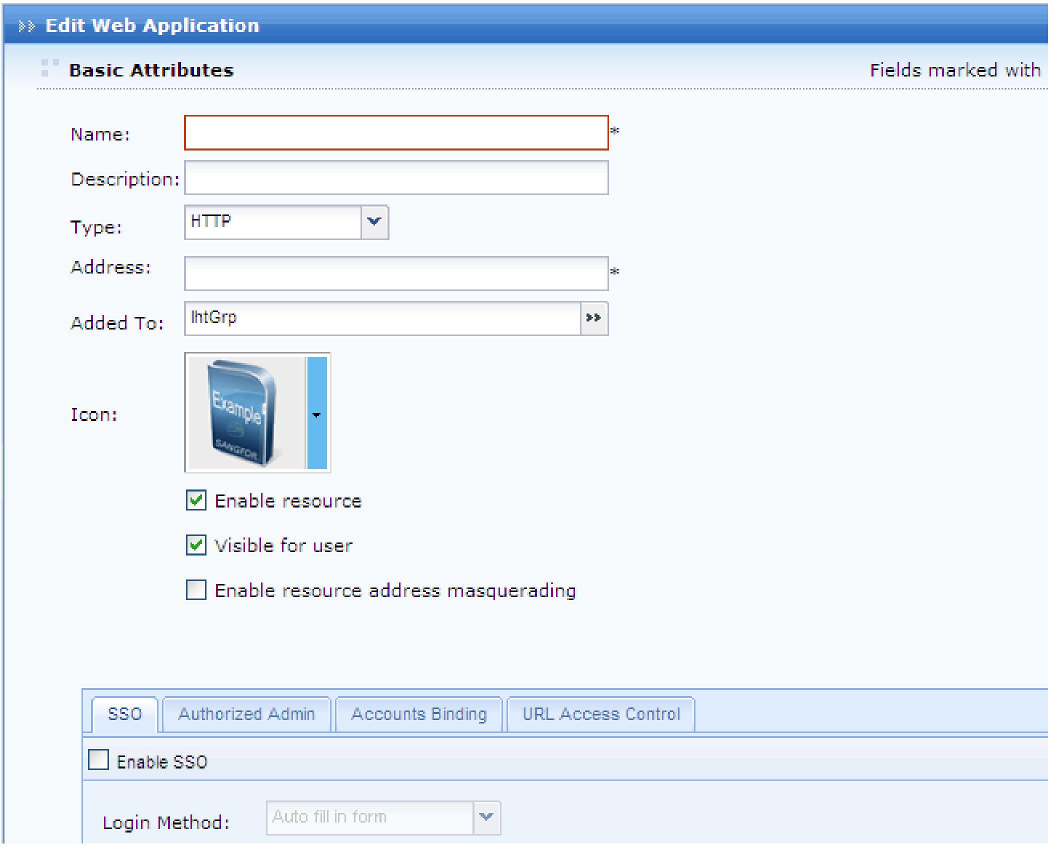
[Website hompage_auto_balancer_rc]
No description
Type:HTTP
Load Balance

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**>**Resource Management** page and click **Add**>**Web app** to enter **Edit Web**

Application page, as shown below:



Edit Web Application

Basic Attributes

Fields marked with

Name: *

Description:

Type: HTTP

Address: *

Added To: IhtGrp

Icon:

☑ Enable resource

☑ Visible for user

□ Enable resource address masquerading

□ Enable SSO

Login Method: Auto fill in form

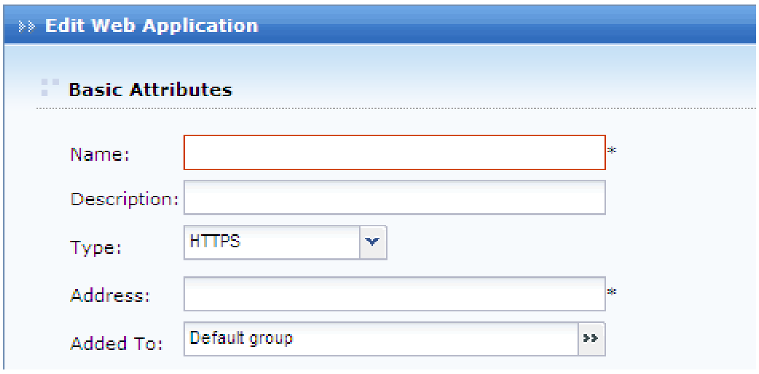
2. Configure **Basic Attributes** of the Web application. The following are the basic attributes:

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

- **Type:** Options are **HTTP**, **HTTPS**, **MAIL**, **File Share** 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:



Edit Web Application

Basic Attributes

Name: *

Description:

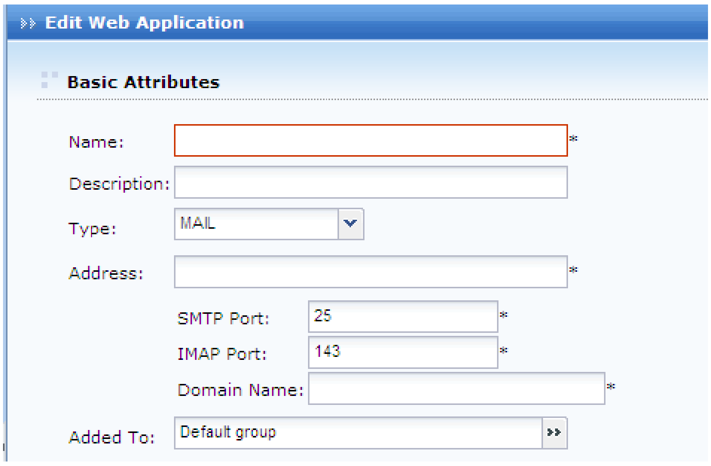
Type: HTTPS

Address: *

Added To: Default group

- 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)sectioning 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:



Edit Web Application

Basic Attributes

Name: *

Description:

Type: MAIL

Address: *

SMTP Port: 25 *

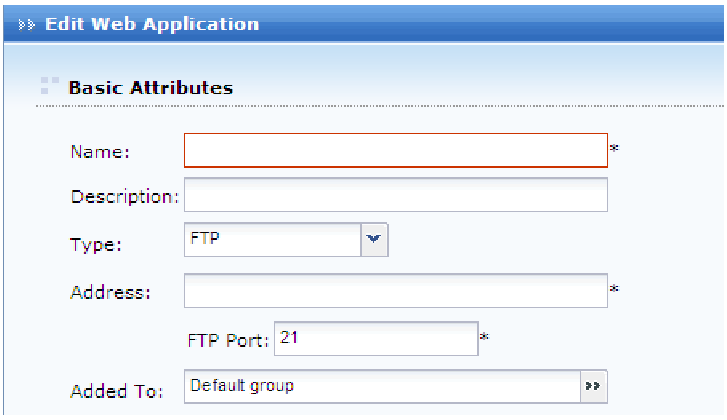
IMAP Port: 143 *

Domain Name: *

Added To: Default group

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:



Basic Attributes

Name: *

Description:

Type: FTP

Address: *

FTP Port: 21 *

Added To: Default group

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 sectioning Chapter 4).
- **Icon:** Indicates the icon forthis 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 sectioning 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.

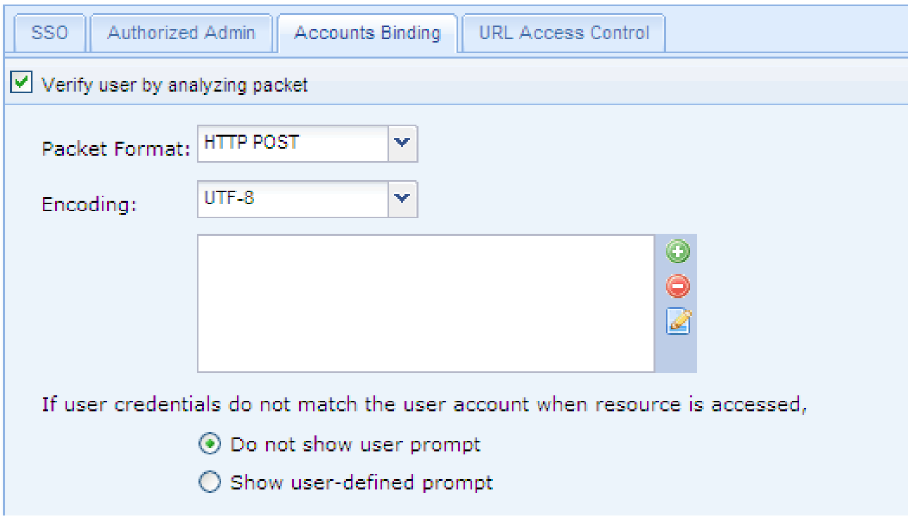
   To enable user to access corporate resources over SSL VPN using SSO, select **Enable SSO** option and configure the **SSO** page (under **System**>**SSL VPN Options**>**General**. For more details, refer to the Configuring SSO Options sectioning Chapter 3).

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, 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 **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.



☑ Verify user by analyzing packet

Packet Format: HTTP POST

Encoding: UTF-8

If user credentials do not match the user account when resource is accessed,

● Do not show user prompt

○ Show user-defined prompt

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.

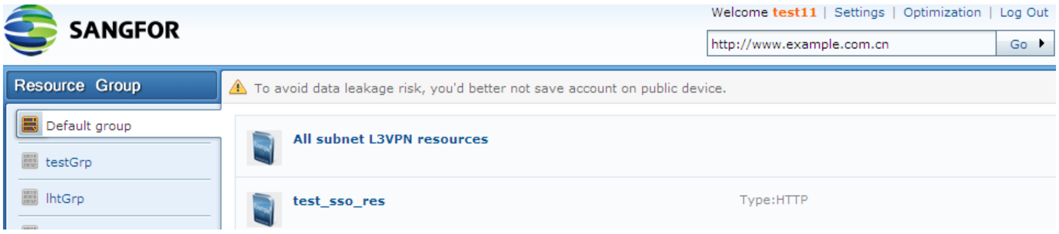
Applying **Verify user by analyzing packet** does not need SSO to be enabled.

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.

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

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

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


SANGFOR
Welcome test11 | Settings | Optimization | Log Out
http://www.example.com.cn
Go
Resource Group
Default group
testGrp
lhtGrp
All subnet L3VPN resources
test_sso_res
Type:HTTP

To avoid data leakage risk, you'd better not save account on public device.

   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.
- Since the addresses of majority of resources defined as Web application need to be rewritten, resource access might encounter many limitations. In contrast, TCP application supports almost all C/S applications, including Web, Mail, FTP, etc., and therefore, in case that a resource added as Web application could not meet the needs, define thesame resource asTCP application.
- Among various kinds of resources, there is a system-protected resource named **All subnet Web resources**. It stands for all Web resources (with address beginning with **http** or **https**) on the subnets configured on **Local Subnets** page and those resources on the subnets where LAN and DMZ interfaces reside. Like L3VPN, it can be associated with SSL VPN users; however, no attribute of it can be modified except for the name, description and visibility.

Scenario 10: 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:

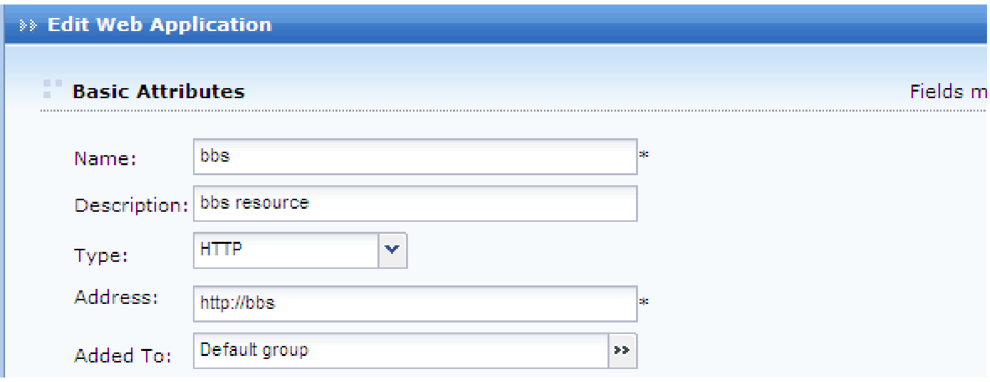
Enable employees to access these resources over SSL VPN, but no add-on needs to be installed.

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.

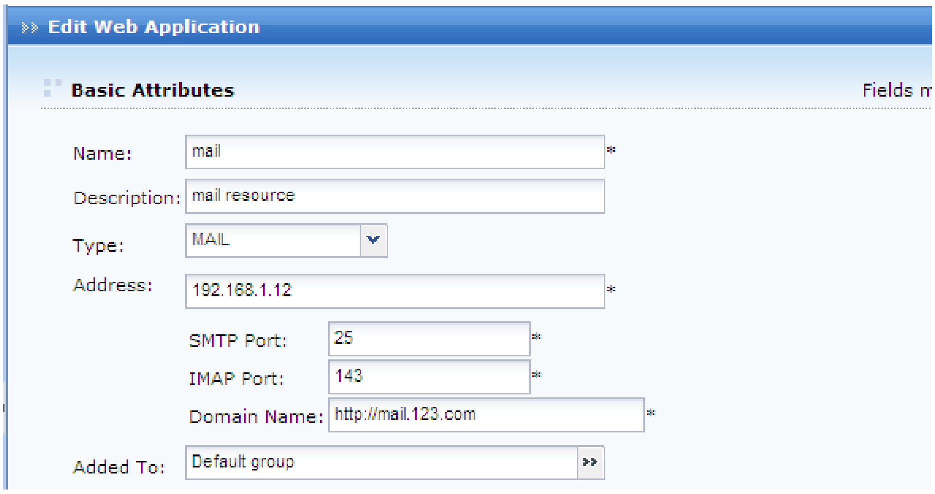
To achieve the expected purposes:

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 sectioning 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 **Resource Management** page, click **Add**>**Web app** to enter the **Edit Web Application** page, as shown in the figure below:



Name: bbs *
Description: bbs resource
Type: HTTP
Address: http://bbs *
Added To: Default group

   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 **Resource Management** page, click **Add**>**Webapp** to enter the **Edit Web Application** page, as shown in the figure below:



Name: mail *

Description: mail resource

Type: MAIL

Address: 192.168.1.12 *

SMTP Port: 25 *

IMAP Port: 143 *

Domain Name: http://mail.123.com *

Added To: Default group

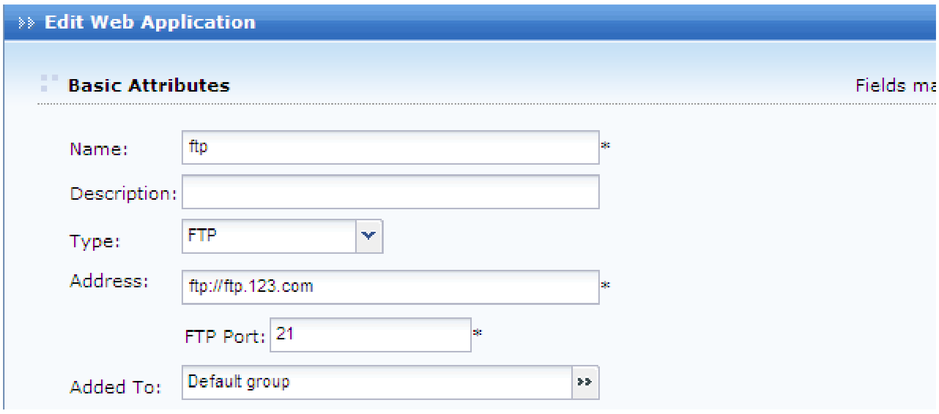
b. Choose resource type **MAIL**, and enter the IP address of the SMTP server into the **Address** field and the domain name into **Domain Name** field.

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:



Name: ftp *

Description:

Type: FTP

Address: ftp://ftp.123.com *

FTP Port: 21 *

Added To: Default group

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.

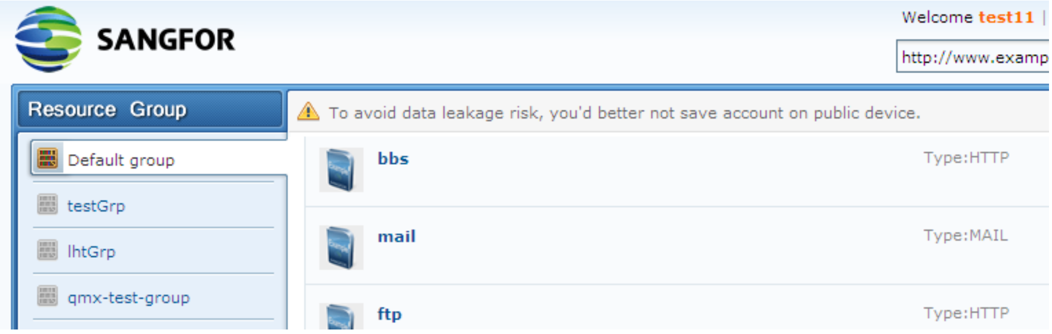
c. Click the **Save** button to save the settings.

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 sectioning 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:



To avoid data leakage risk, you'd better not save account on public device.

bbs Type:HTTP

mail Type:MAIL

ftp Type:HTTP

Scenario 11: Masquerading Resource Address

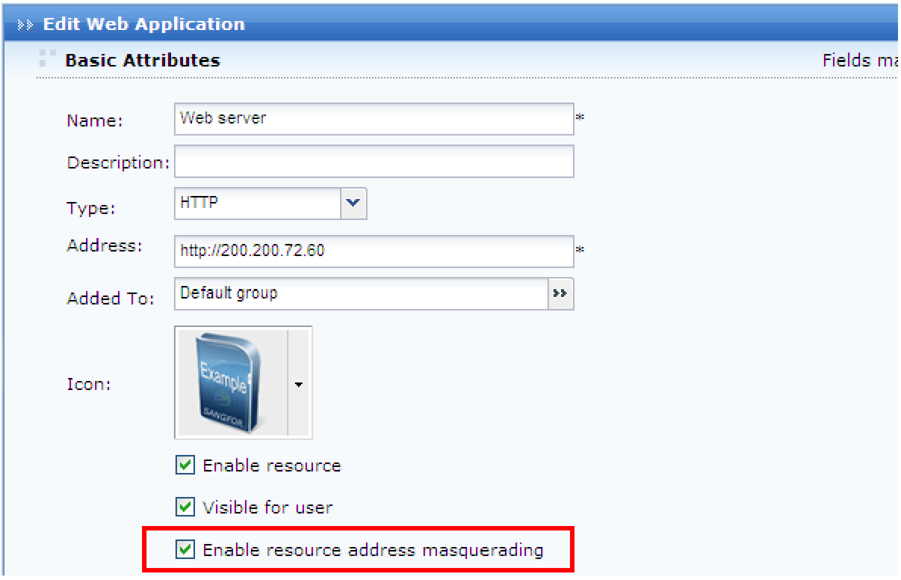
Purpose:

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 **File Share** 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 **Enable resource address masquerading**, as shown below:



Name: Web server *

Description:

Type: HTTP

Address: http://200.200.72.60 *

Added To: Default group

Icon:

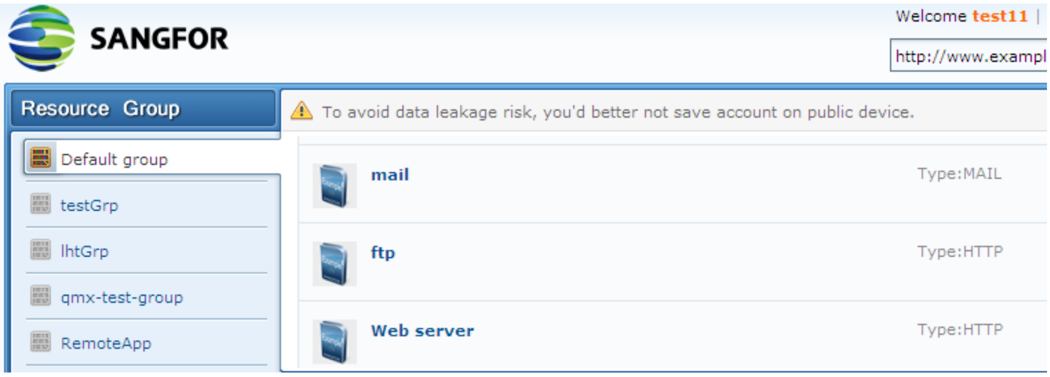
☑ Enable resource

☑ Visible for user

☑ Enable resource address masquerading

3. Associate the resource with the user. For detailed guide, refer to the Adding Role sectioning 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:



Welcome **test11** |

http://www.exampl

Resource Group

Default group

testGrp

lhtGrp

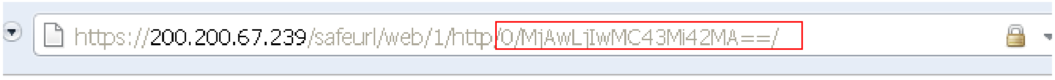
qmx-test-group

RemoteApp

To avoid data leakage risk, you'd better not save account on public device.

mail	Type:MAIL
ftp	Type:HTTP
Web server	Type:HTTP

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.



https://200.200.67.239/safeurl/web/1/http/0/MjAwLjIwMC43Mi42MA==/

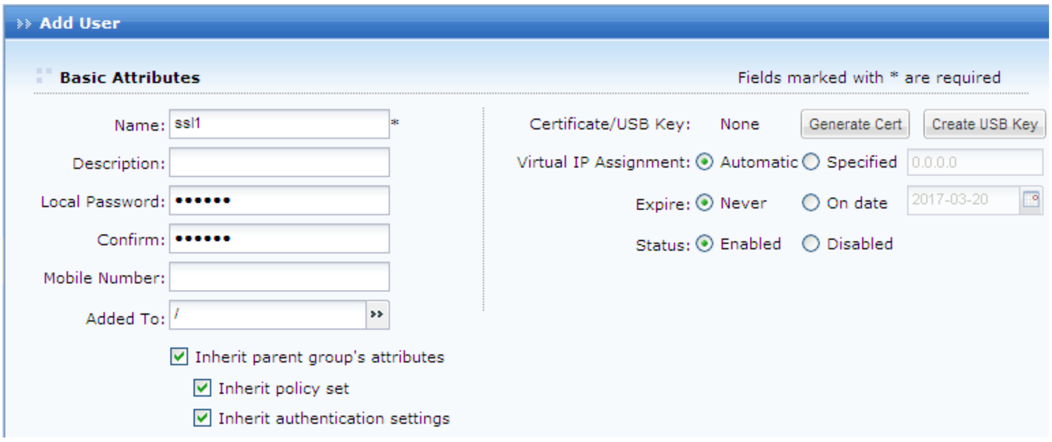
Scenario 12: Adding File Share Type of Web Resource

Purposes:

- When the employee **ssl1** accesses the Web-app-based file sharing server (IP: 200.200.72.169), he or she need not install any ActiveX control and can enjoy the speedup of access tithe file sharing server.
- Employees can log in to the server automatically, without entering username and password.

To achieve the expected purposes:

1. Navigate to**ss VPN**>**Users** and click **Add** to create a user account, as shown below:



Add User

Basic Attributes

Fields marked with * are required

Name: ssl1 *

Description:

Local Password: ••••••

Confirm: ••••••

Mobile Number:

Added To: /

☑ Inherit parent group's attributes

☑ Inherit policy set

☑ Inherit authentication settings

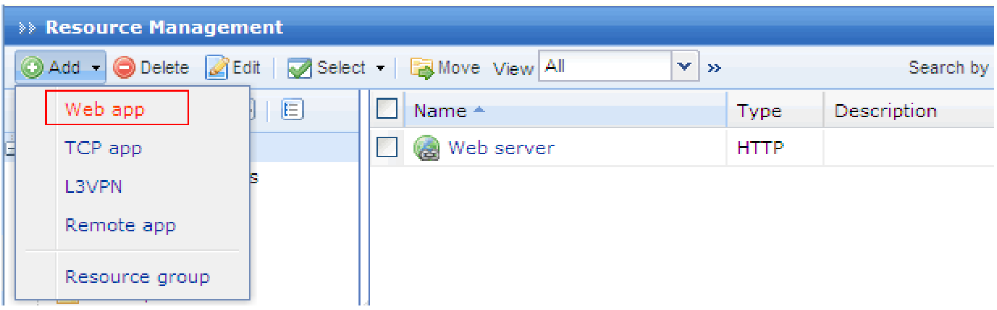
Certificate/USB Key: None [Generate Cert] [Create USB Key]

Virtual IP Assignment: ● Automatic ○ Specified 0.0.0.0

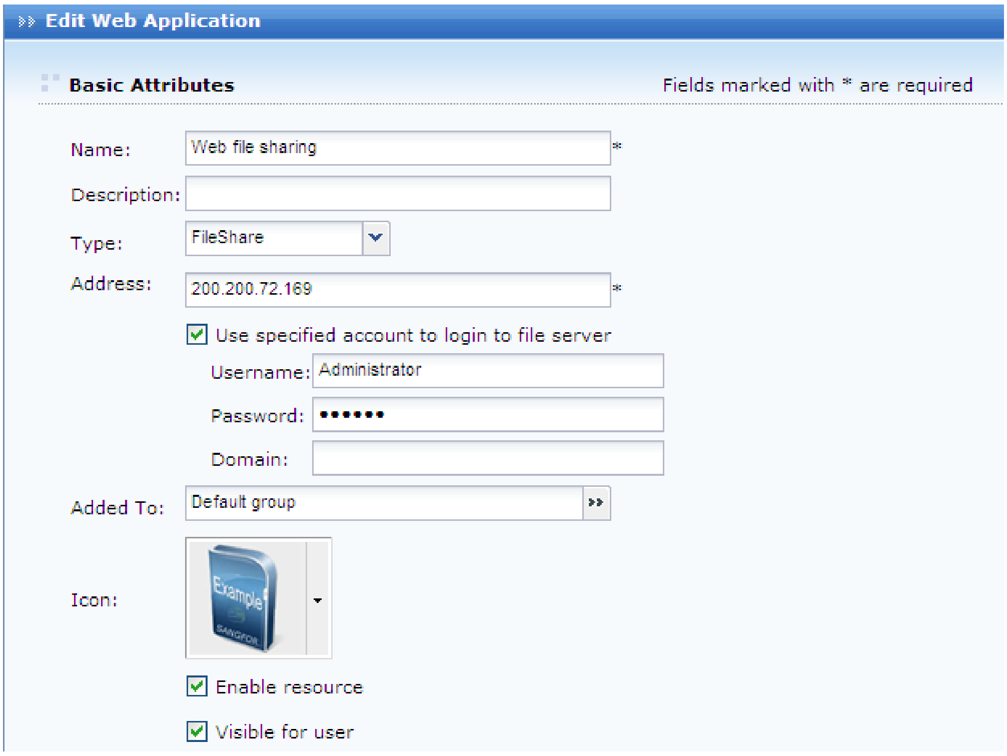
Expire: ● Never ○ On date 2017-03-20

Status: ● Enabled ○ Disabled

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 **File Share** type of application and configure the other required fields, as shown below:



Edit Web Application

Basic Attributes

Fields marked with * are required

Name: Web file sharing *

Description:

Type: FileShare

Address: 200.200.72.169 *

☑ Use specified account to login to file server

Username: Administrator

Password: ••••••

Domain:

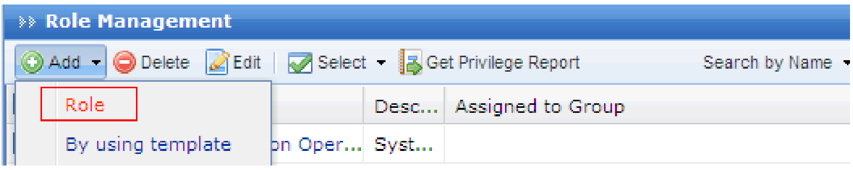
Added To: Default group

Icon:

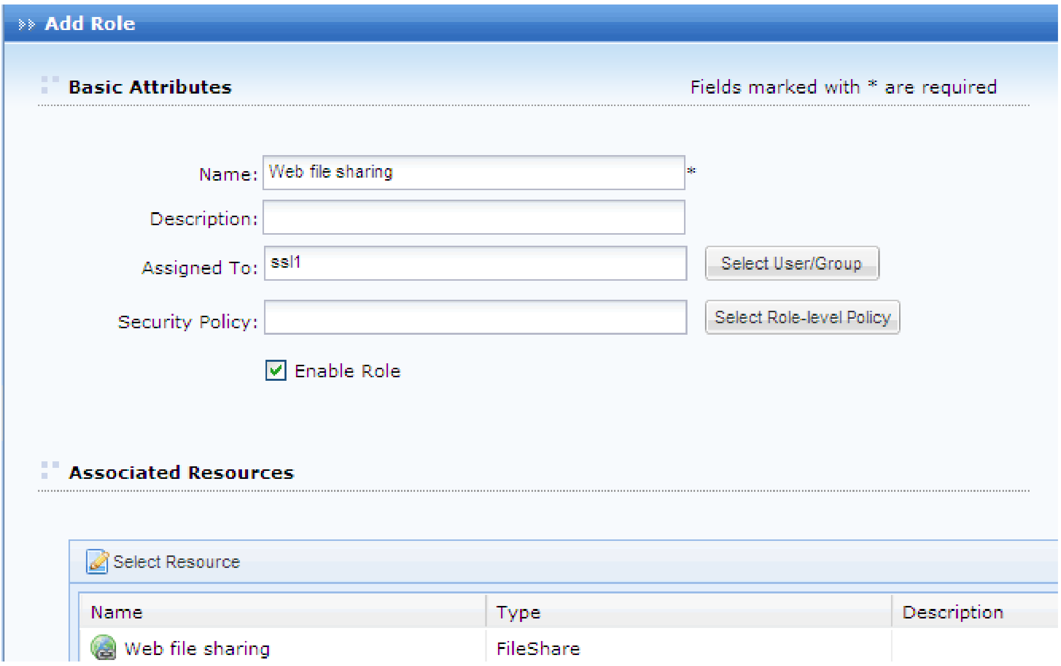
☑ Enable resource

☑ Visible for user

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.



Add Role

Basic Attributes — Fields marked with * are required

Name: Web file sharing *

Description:

Assigned To: ssl1 [Select User/Group]

Security Policy: [Select Role-level Policy]

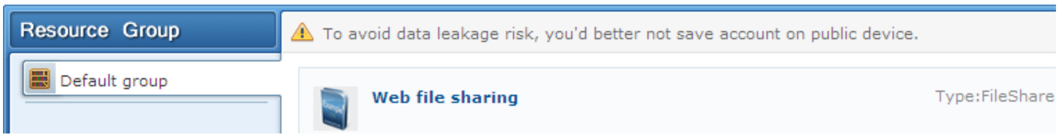
☑ Enable Role

Associated Resources

Select Resource

Name	Type	Description
Web file sharing	FileShare	

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:



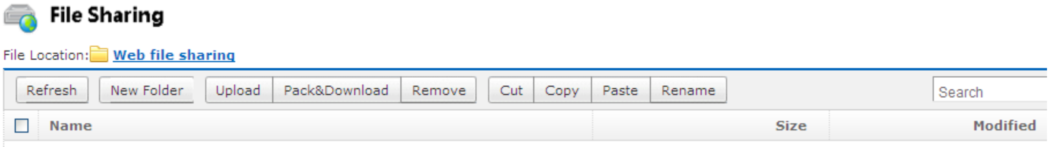
Resource Group

⚠ To avoid data leakage risk, you'd better not save account on public device.

Default group

Web file sharing — Type:FileShare

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:



File Sharing

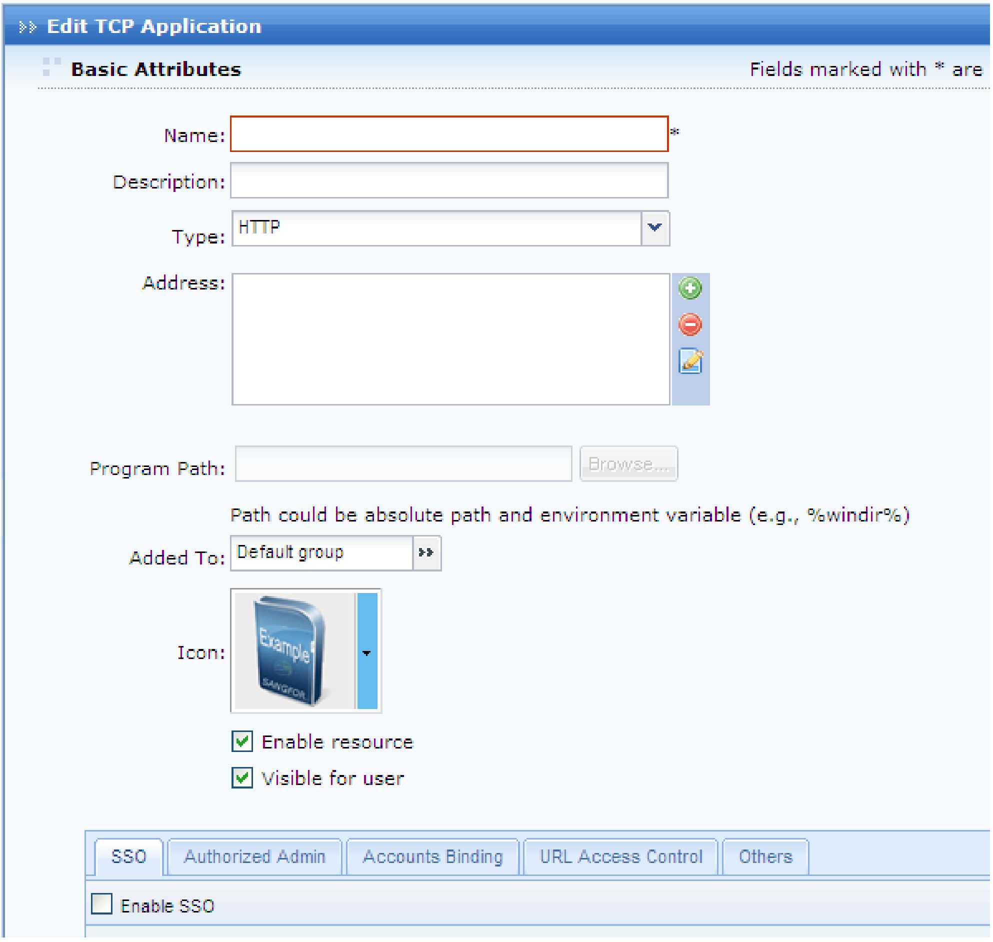
File Location: Web file sharing

□ Name	Size	Modified

Adding/Editing TCP Application

TCP application is typeof resource that allows end users to use C/S-based or TCP-based application on their local computer to access corporate resources and servers over SSL VPN.

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



Edit TCP Application

Basic Attributes

Fields marked with * are

Name: *

Description:

Type: HTTP

Address:

Program Path:

Path could be absolute path and environment variable (e.g., %windir%)

Added To: Default group

Icon:

☑ Enable resource

☑ Visible for user

□ Enable SSO

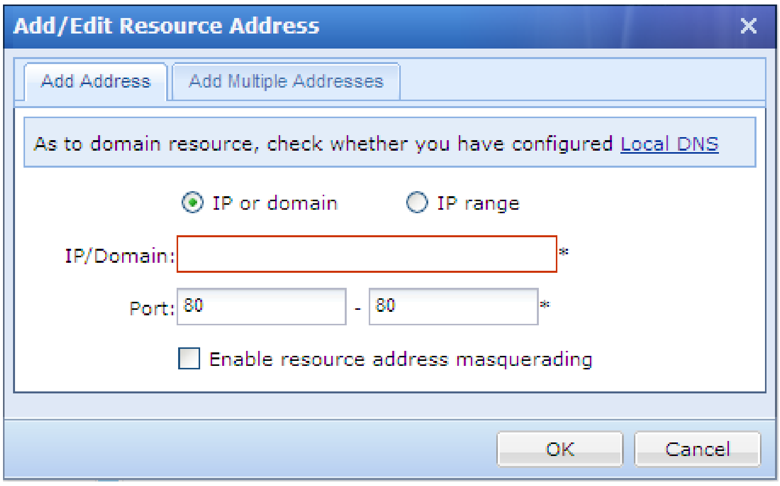
2. Configure **Basic Attributes** of the TCP application. The following are the basic attributes:

- **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 IPrange), click the **Add Address** tab. To add multiple entries of addresses, click the **Add Multiple Addresses** tab, as shown in the figures below:



Add/Edit Resource Address

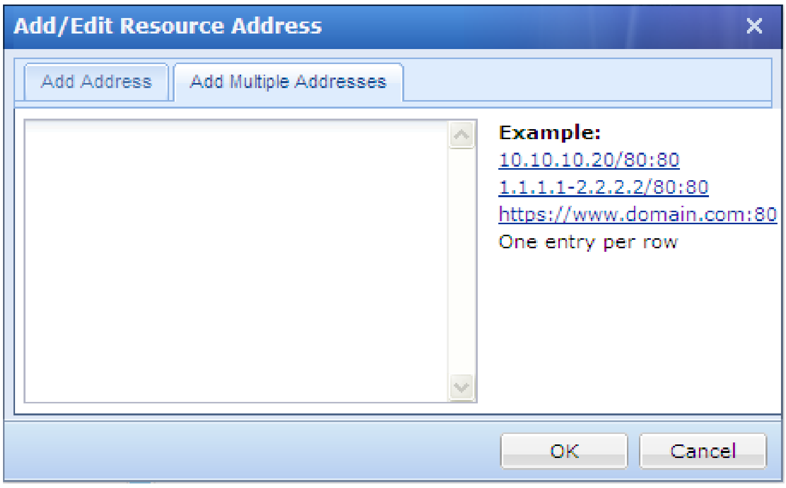
As to domain resource, check whether you have configured Local DNS

● IP or domain ○ IP range

IP/Domain: *

Port: 80 - 80 *

□ Enable resource address masquerading



Add/Edit Resource Address

Example:
10.10.10.20/80:80
1.1.1.1-2.2.2.2/80:80
https://www.domain.com:80
One entry per row

- **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 sectioning 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.

8. Configure **SSO** tab.

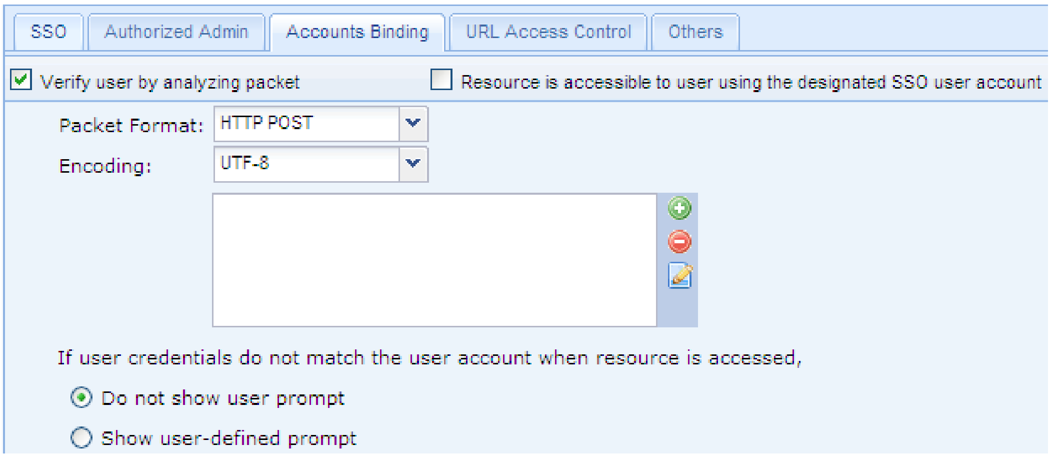
To enable connecting users to use SSO feature to access corporate resources over SSL VPN, select **Enable SSO** option and configure the **SSO** page (under **System**>**SSL VPN Options**>**General**> **SSO**. For more details, refer to the Configuring SSO Options sectioning Chapter 3).

9. 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 **Resource Management** page, but can see and associate them with users on the **Add Role** or **Edit Role** page.

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



☑ Verify user by analyzing packet ☐ Resource is accessible to user using the designated SSO user account

Packet Format: HTTP POST

Encoding: UTF-8

If user credentials do not match the user account when resource is accessed,

● Do not show user prompt

○ Show user-defined prompt

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.

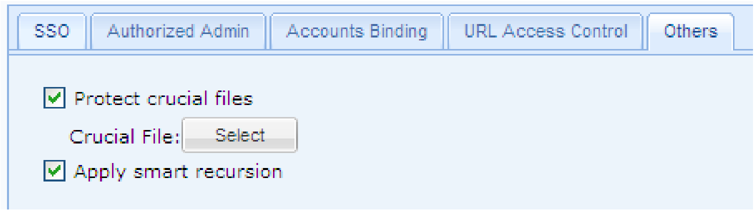
- To enable end users to single sign in to a resource, enable SSO for that resource (under **SSL VPN**>**Resources**>**Resource Management**>**Edit TCP Application**>**SSO** tab) and bind the SSL VPN account to the SSO user account (to configure SSO user account, refer to the Configuring SSO User Account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

11. 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.

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



☑ Protect crucial files

Crucial File:

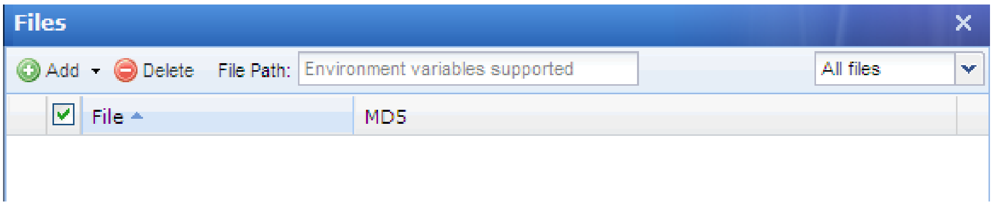
☑ Apply smart recursion

- **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 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 were altered, the

corresponding resource would not be accessible to the user.

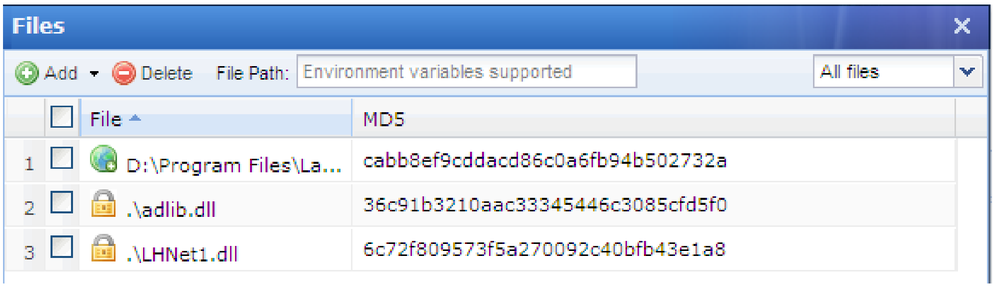
To add crucial files, perform the following steps:

a. Click the **Select** button next to **Crucial File**t 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 filesare added to the **Files** page, with the information of file directory and MD5, as shown in the figure below:



	□	File	MD5
1	□	D:\Program Files\La...	cabb8ef9cddacd86c0a6fb94b502732a
2	□	.\adlib.dll	36c91b3210aac33345446c3085cfd5f0
3	□	.\LHNet1.dll	6c72f809573f5a270092c40bfb43e1a8

d. To view a specific type of file, dll, exe or pdb, specify the file type in the textbox at the upperright 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.

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

Scenario 13: 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:*anOA 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:

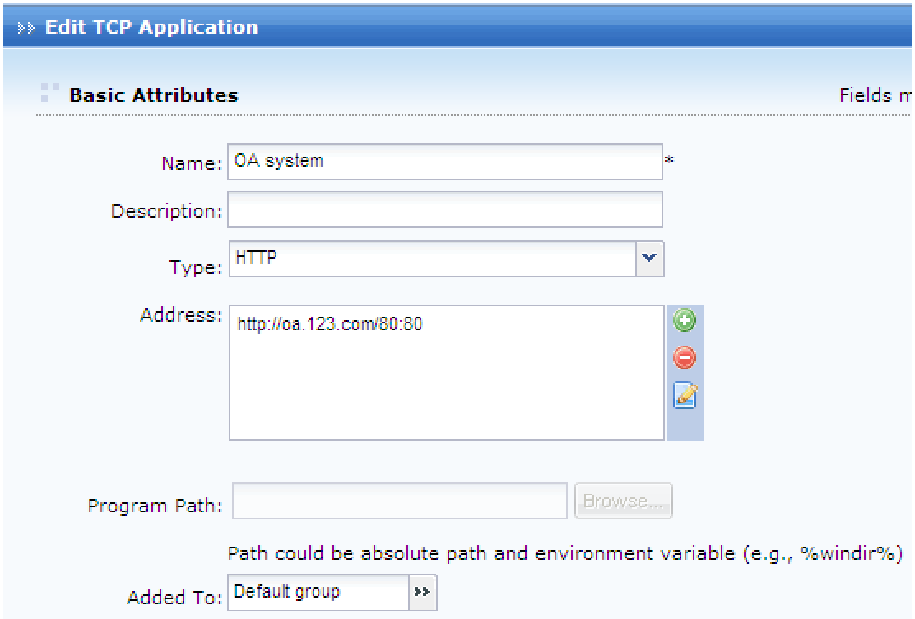
- Enable employees to access OA system directly (i.e., visit OA system through browser).
- Employees can open the accounting system, and connect to the server over SSL VPN.

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**>**Resource Management**. 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:



Name: OA system *

Description:

Type: HTTP

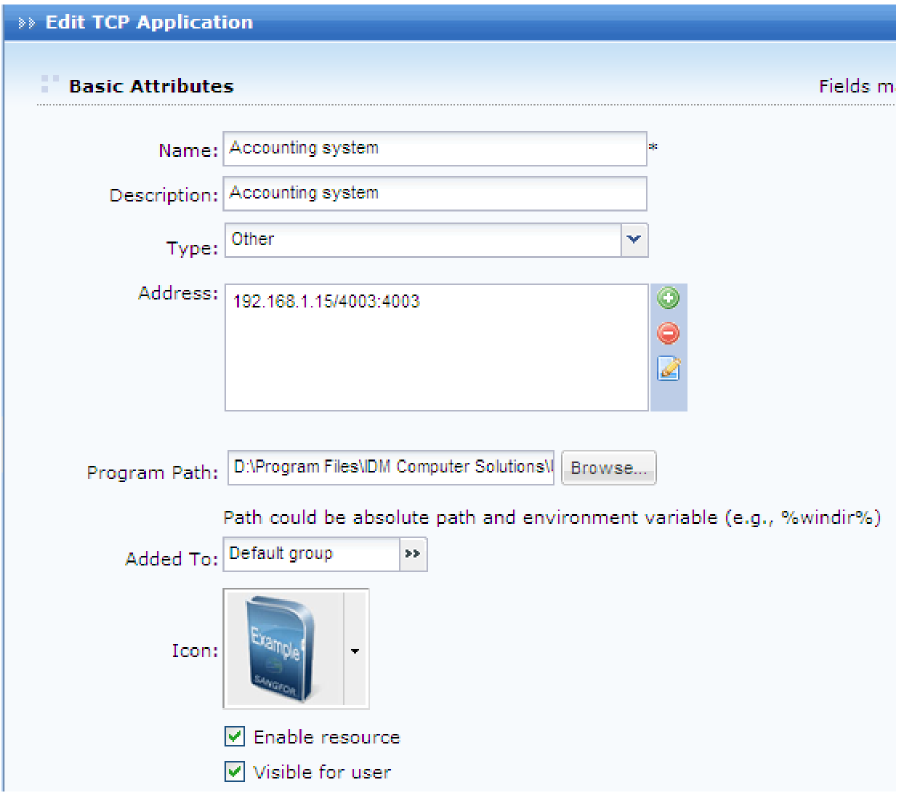
Address: http://oa.123.com/80:80

Program Path:

Path could be absolute path and environment variable (e.g., %windir%)

Added To: Default group

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:



Edit TCP Application

Basic Attributes

Fields m

Name: Accounting system *

Description: Accounting system

Type: Other

Address: 192.168.1.15/4003:4003

Program Path: D:\Program Files\IDM Computer Solutions\ Browse...

Path could be absolute path and environment variable (e.g., %windir%)

Added To: Default group

Icon:

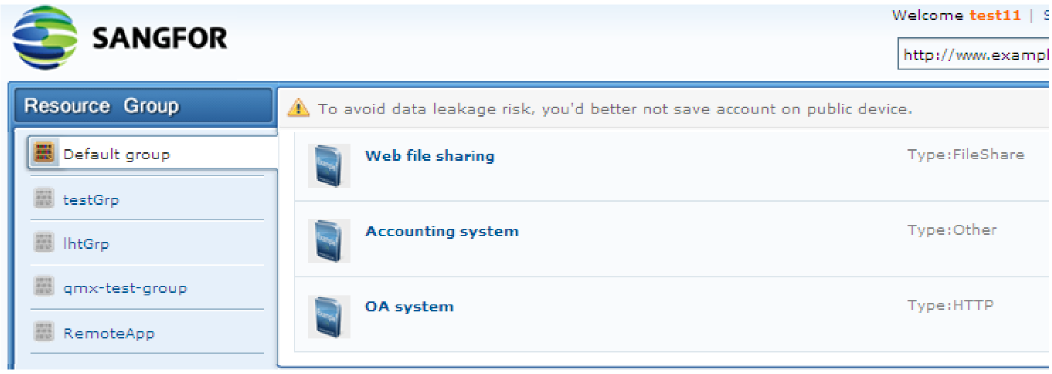
☑ Enable resource

☑ Visible for user

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:



To avoid data leakage risk, you'd better not save account on public device.

Web file sharing	Type:FileShare
Accounting system	Type:Other
OA system	Type:HTTP

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 SSO is enabled. If SSO is not enabled, employee needs to enter the user account manually after clicking resource link.

Scenario 14: Configuring URL Access Control Feature

Background:

A file server (*duan.sslt.com*)is deployed in the enterprise network, providing services for the employees.

Purposes:

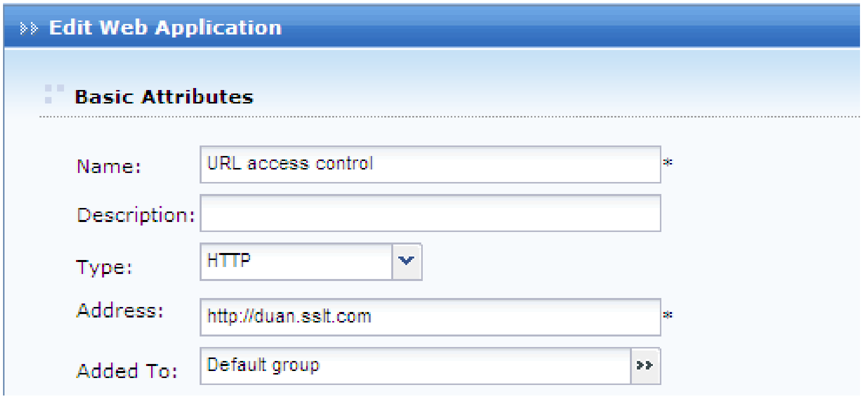
Only allow the members from **Finance** department to access this file server, and only they, others directory of the file server being inaccessible, can access the directory duan.sslt.com/frame.

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**>**Resource Management** and add a Web application (named **URL access control**, URL: *duan.sslt.com*), as shown in the figure below:



Edit Web Application

Basic Attributes

Name: URL access control *

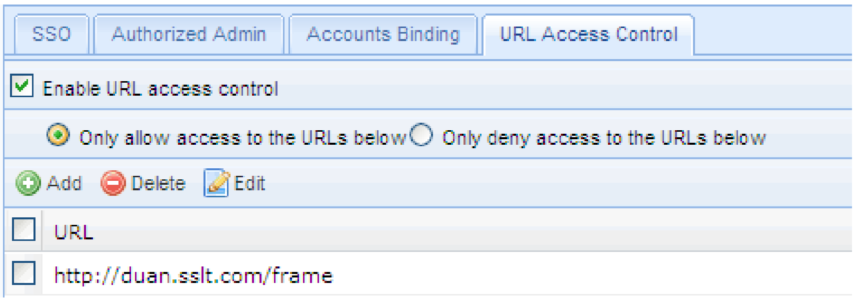
Description:

Type: HTTP

Address: http://duan.sslt.com *

Added To: Default group

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:



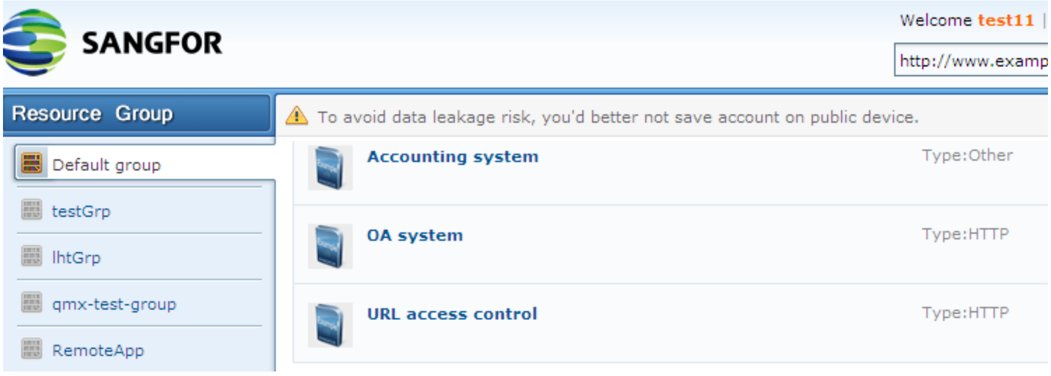
☑ Enable URL access control

● Only allow access to the URLs below ○ Only deny access to the URLs below

□	URL
□	http://duan.sslt.com/frame

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:



To avoid data leakage risk, you'd better not save account on public device.

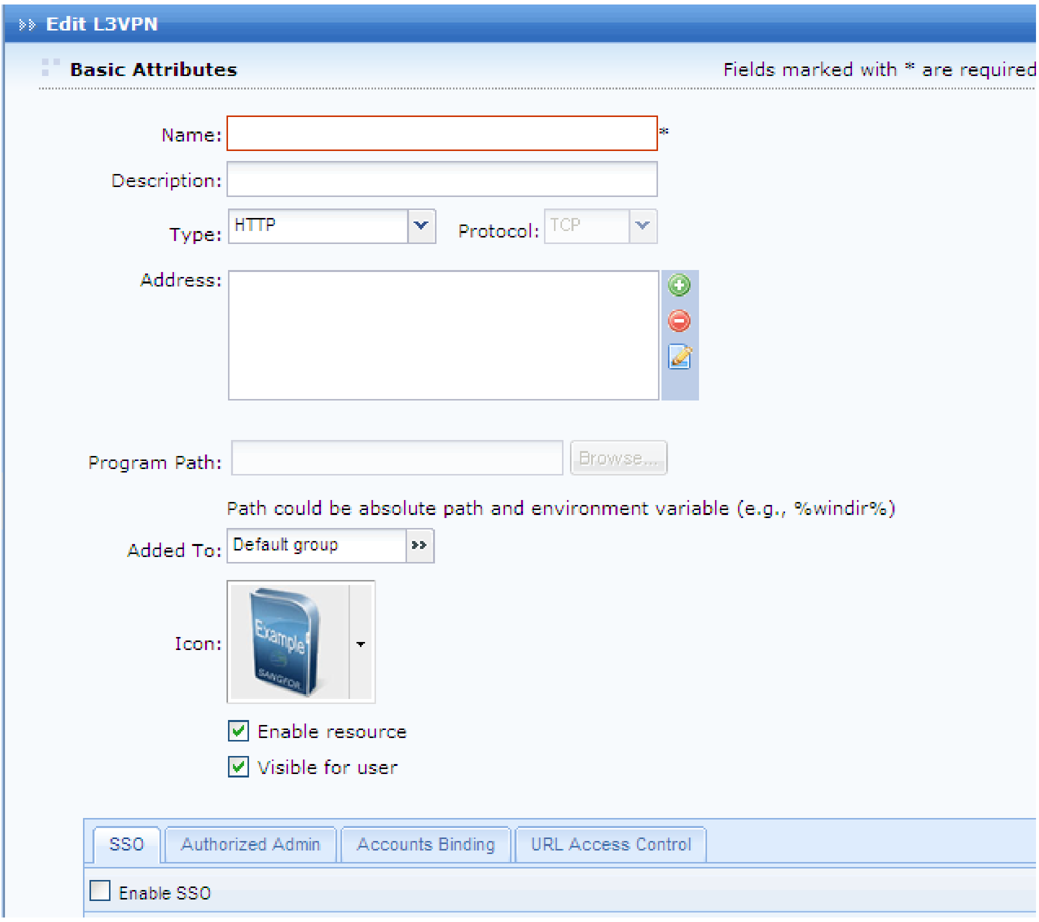
Accounting system	Type:Other
OA system	Type:HTTP
URL access control	Type:HTTP

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/Editing L3VPN

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

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



Fields marked with * are required

Name: *

Description:

Type: HTTP Protocol: TCP

Address:

Program Path:

Path could be absolute path and environment variable (e.g., %windir%)

Added To: Default group

Icon:

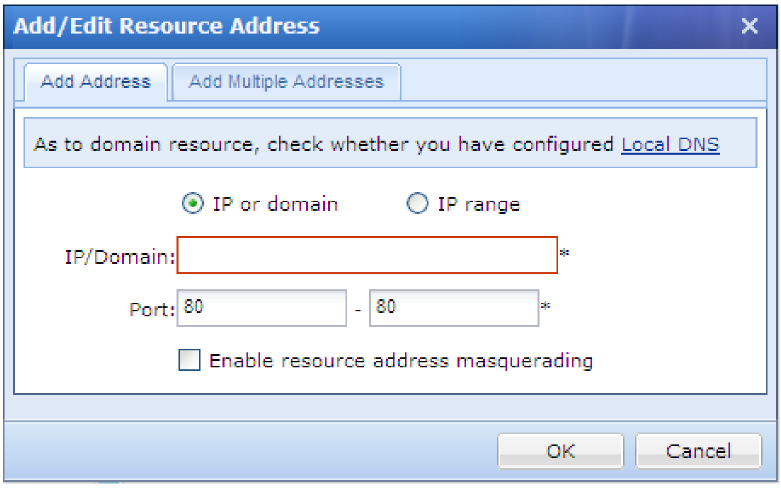
☑ Enable resource

☑ Visible for user

□ Enable SSO

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 I range), click the **Add Address** tab. To add multiple entries of addresses, click the **Add Multiple Addresses** tab, as shown in the figures below:


Add/Edit Resource Address

Add Address | Add Multiple Addresses

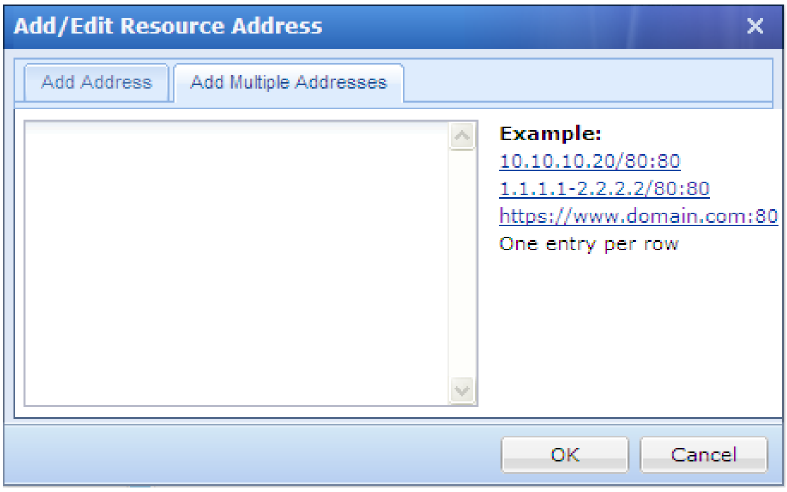
As to domain resource, check whether you have configured Local DNS

● IP or domain ○ IP range

IP/Domain: *

Port: 80 - 80 *

□ Enable resource address masquerading


Add/Edit Resource Address

Add Address | Add Multiple Addresses

Example:
10.10.10.20/80:80
1.1.1.1-2.2.2.2/80:80
https://www.domain.com:80
One entry per row

- **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.

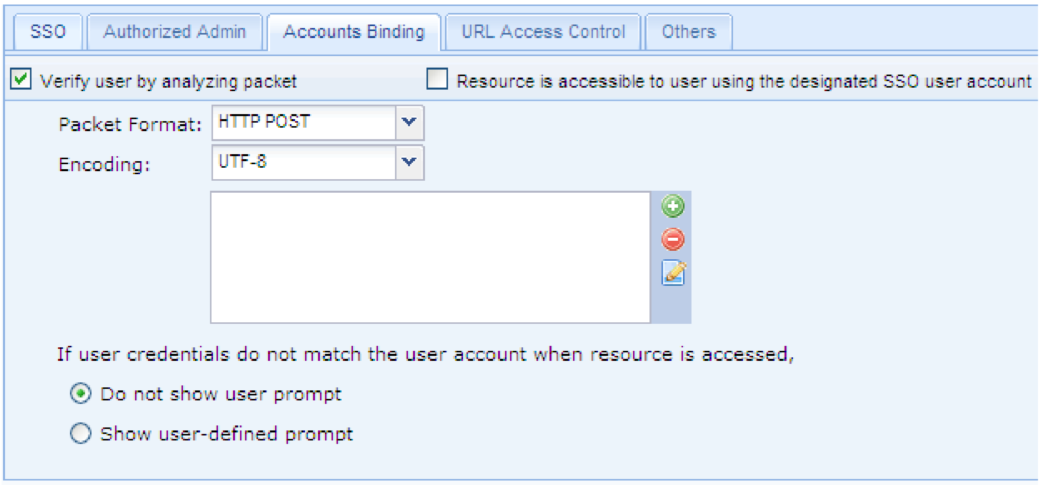
   To enable connecting users to use SSO feature to access corporate resources over SSL VPN, select **Enable SSO** option and configure the **SSO** page (under **System**>**SSL VPN Options**>**General**. For more details, refer to the Configuring SSO Options section in Chapter 3).

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.



☑ Verify user by analyzing packet ☐ Resource is accessible to user using the designated SSO user account

Packet Format: HTTP POST

Encoding: UTF-8

If user credentials do not match the user account when resource is accessed,

● Do not show user prompt

○ Show user-defined prompt

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**>**Resource Management**>**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.

14. 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.

15. 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.
- 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.

Scenario 15: Adding L3VPN

Background:

192.168.1.10-192.168.1.15 is a subnet in the enterprise network.

Purposes:

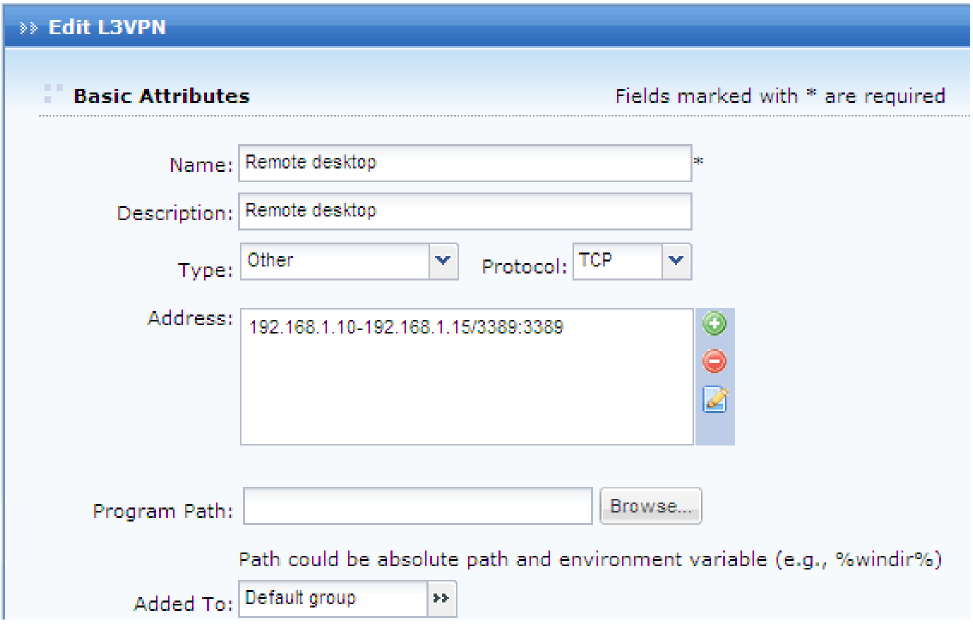
Enable network administrator to access internal machines on subnet 192.168.1.10-192.168.1.15 over SSL VPN and senior managers to access all internal machines in enterprise network over SSL VPN.

Analysis and solution:

For network administrator, defining the remote computers as L3VPN resource would allow him/her to access these machines remotely. For senior managers, associate those with **All Subnet L3VPN resources** can meet their needs of accessing all the internal machines.

To achieve the expected purposes:

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



Edit L3VPN

Basic Attributes — Fields marked with * are required

Name: Remote desktop *

Description: Remote desktop

Type: Other Protocol: TCP

Address: 192.168.1.10-192.168.1.15/3389:3389

Program Path: Browse...

Path could be absolute path and environment variable (e.g., %windir%)

Added To: Default group

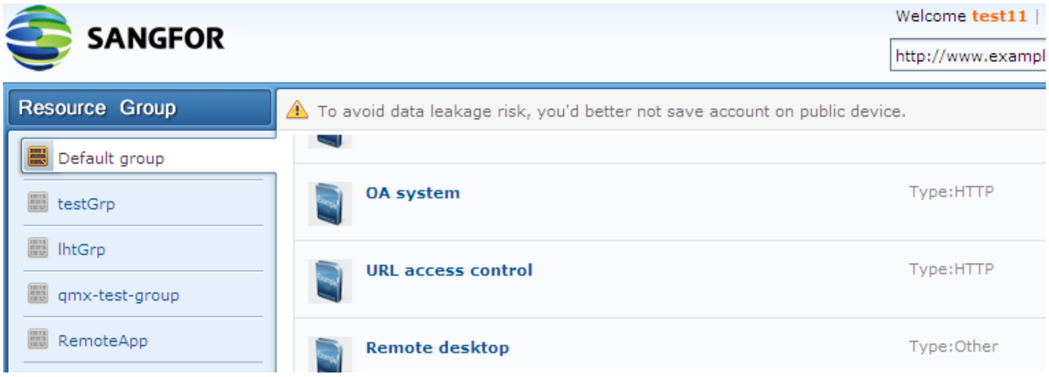
Enter resource name (for example, **Remote desktop**); configure other required fields and click the **Save** button to save the settings.

2. Add or edit a role to associate the resources **Remote desktop** with it and assign the role to the network administrator (for detailed guide, refer to the Adding Role section in Chapter 4).

3. Add or edit a role to associate **All subnet L3VPN resources** with the senior managers. There is no need to create this resource, because **All subnetL3VPN resources** is built in the Sangfor device.

4. Click the **Apply** button to apply the settings.

5. After network administrator and senior managers log in to the SSL VPN, they will see their associated resources respectively, as shown in the figures below:



SANGFOR

Welcome test11 |

http://www.exampl

Resource Group

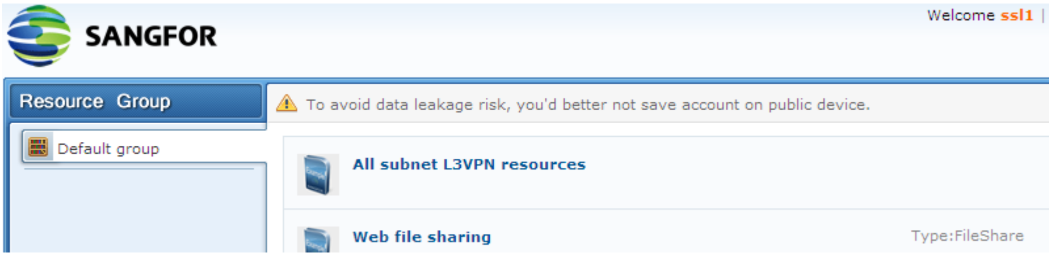
To avoid data leakage risk, you'd better not save account on public device.

Default group
testGrp
lhtGrp
qmx-test-group
RemoteApp

OA system Type:HTTP

URL access control Type:HTTP

Remote desktop Type:Other



SANGFOR

Welcome ssl1 |

Resource Group

To avoid data leakage risk, you'd better not save account on public device.

Default group

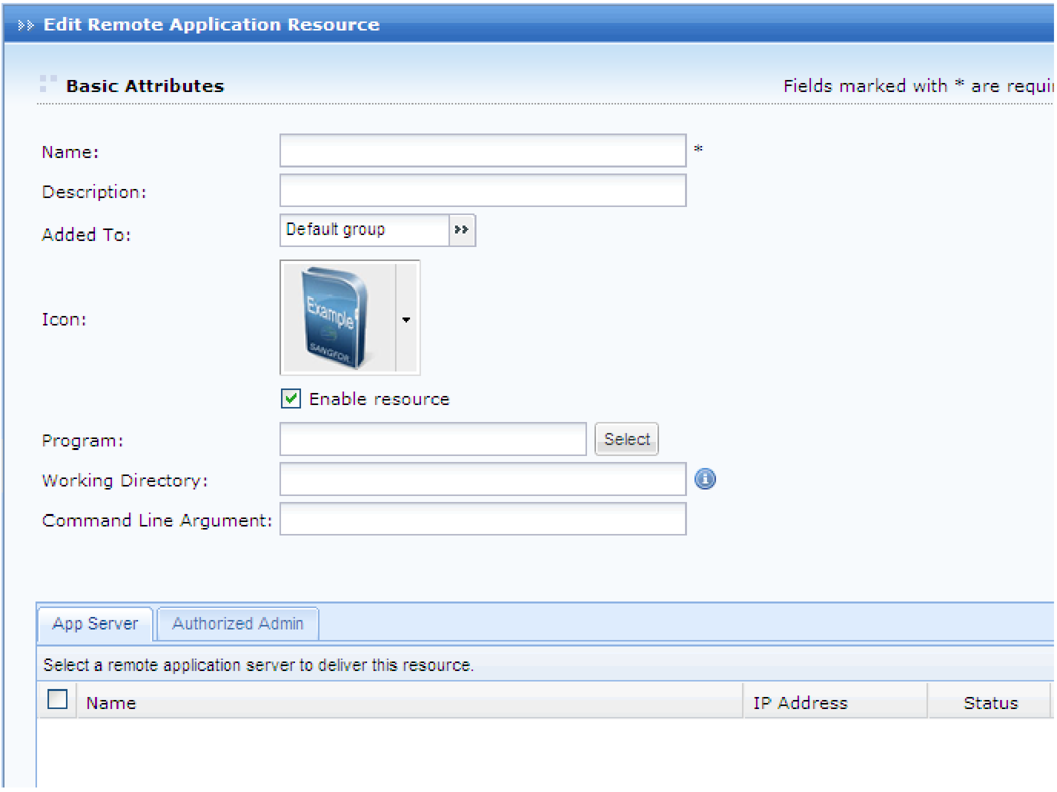
All subnet L3VPN resources

Web file sharing Type:FileShare

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**>**Resource Management** and click **Add**>**Remote app** to enter the **Edit Remote Application Resource** page, as shown below:



Edit Remote Application Resource

Basic Attributes

Fields marked with * are requi

Name: *

Description:

Added To: Default group

Icon:

☑ Enable resource

Program:

Working Directory:

Command Line Argument:

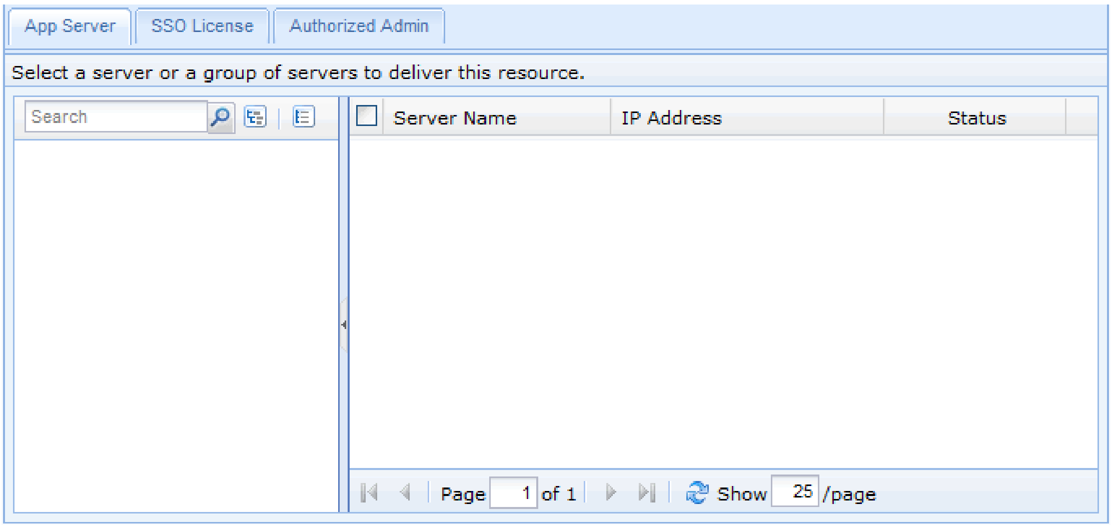
Select a remote application server to deliver this resource.

□	Name	IP Address	Status

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:** Indicates application program provided by remote application server (to configure remote server, refer to the Adding Remote Application Server section in Chapter 4).
- **Command Line Argument:** Specifies the parameters that may be used when some application program starts.

3. Click hea**p 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).



Select a server or a group of servers to deliver this resource.

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.

5. Configure **SSO License** tab.

   At the same time administrator to record a SSO of login information, then after the user logs VPN, remote access to the appropriate application of resources, the completion of the corresponding single sign-on process.

- 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 **Resource Management** page, but can see and associate them with users on the **Add Role** or **Edit Role** page.

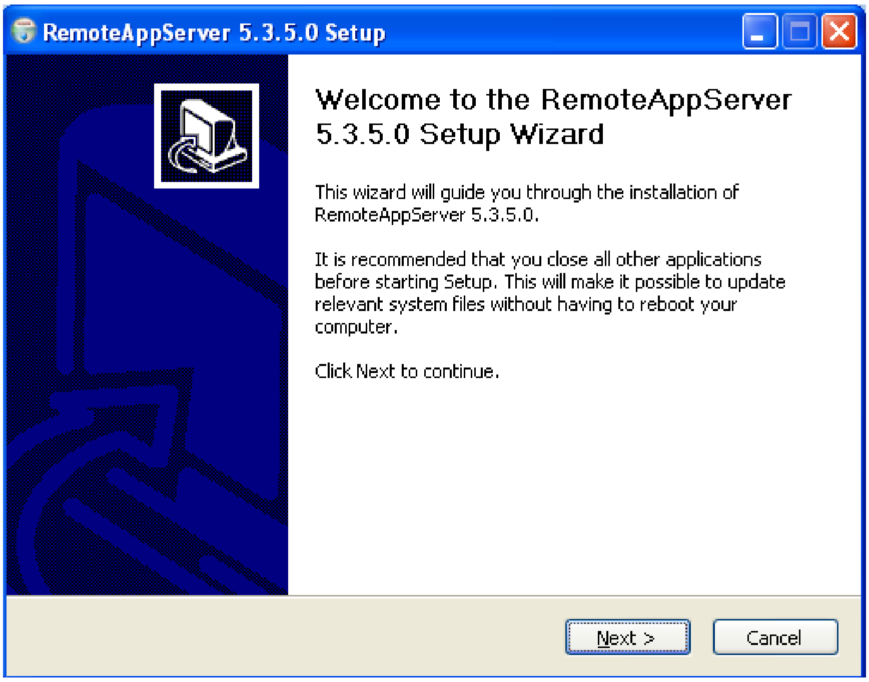
Scenario 16: Adding Remote Application

Purpose:

Enable enterprise’s remote employees to access **WordPad** on the internal application server (IP: 200.200.136.74, port: 7170).

To achieve the expected purpose:

1. Navigate to **SSL VPN**>**Remote Servers** to enter the **Remote Server Management** page and click **Download Remote App Agent** to download the Remote App Agent program.
2. Double-click the executable file named **SFRemoteAppServerInstall.exe** and follow the instructions to install the Remote App Agent, as show in the figure below:



RemoteAppServer 5.3.5.0 Setup

Welcome to the RemoteAppServer 5.3.5.0 Setup Wizard

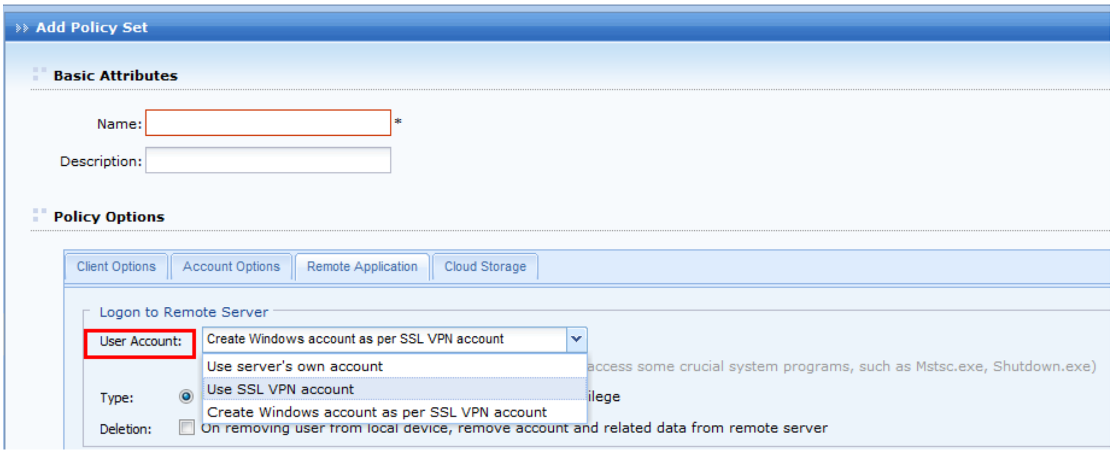
This wizard will guide you through the installation of RemoteAppServer 5.3.5.0.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

3. Navigate to **SSL VPN**>**Remote Servers** to enter the **Remote Server Management** page and configure a remote storage server on which the data and files in the remote application session will be saved (for detailed guide, refer to the Adding Remote Storage Server section in Chapter 4).
4. Navigate to **SSL VPN**>**Policy Sets** to enter the **Policy Set Management** 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.



Add Policy Set

Basic Attributes

Name: *

Description:

Policy Options

Client Options | Account Options | Remote Application | Cloud Storage

Logon to Remote Server

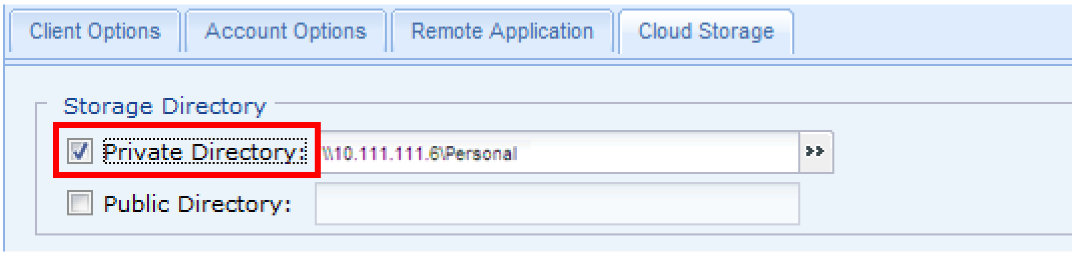
User Account: Create Windows account as per SSL VPN account

- Use server's own account
- Use SSL VPN account
- Create Windows account as per SSL VPN account

access some crucial system programs, such as Mstsc.exe, Shutdown.exe)

Type: ● ilege

Deletion: □ On removing user from local device, remove account and related data from remote server



Client Options | Account Options | Remote Application | Cloud Storage

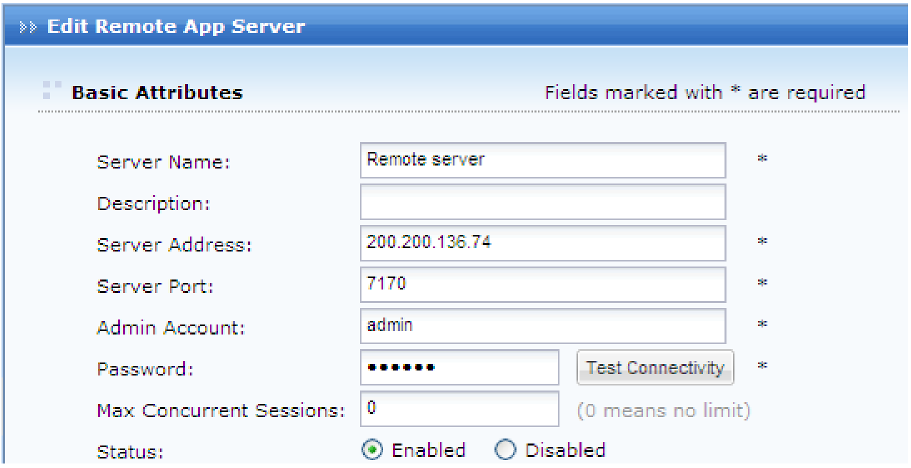
Storage Directory

☑ Private Directory: \\10.111.111.6\Personal

□ Public Directory:

5. Associate the policy set with the corresponding user (for detailed guide, refer to the Adding User section in Chapter 4).

6. Navigate to **SSL VPN**>**Remote Servers**>**Remote Server Management** to configure the remote application server that can provide **WordPad** for end user (for detailed guide, refer to the Adding Remote Application Server section in Chapter 4).



Edit Remote App Server

Basic Attributes — Fields marked with * are required

Server Name: Remote server *

Description:

Server Address: 200.200.136.74 *

Server Port: 7170 *

Admin Account: admin *

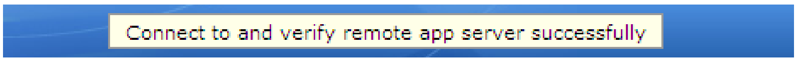
Password: •••••• [Test Connectivity] *

Max Concurrent Sessions: 0 (0 means no limit)

Status: ● Enabled ○ Disabled

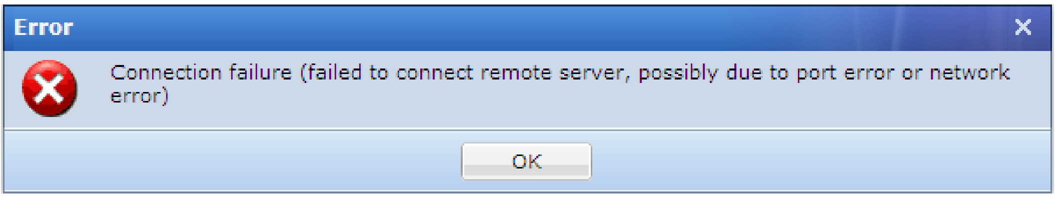
7. Configure admin account, password, and other required fields and make sure the application server can connect to the Sangfor device. You can click the **Test Connectivity** button to check whether this remote application server can be connected.

If the following prompt appears, the Sangfor device is then connected to the remote application server successfully.



Connect to and verify remote app server successfully

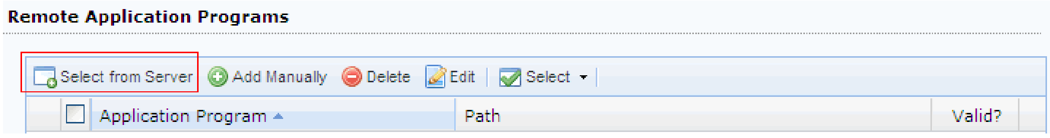
If the following prompt appears, the SSL VPN cannot connect to remote application server. In that case, check whether the remote server is configured properly.



Error

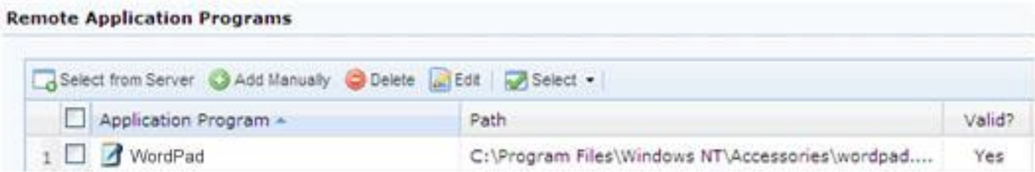
Connection failure (failed to connect remote server, possibly due to port error or network error)

8. Under **Remote Application Programs**, click **Select from Sever** to select the application program **WordPad**, as shown in the figure below:



Remote Application Programs

9. The selected programs are seen in the figure below:

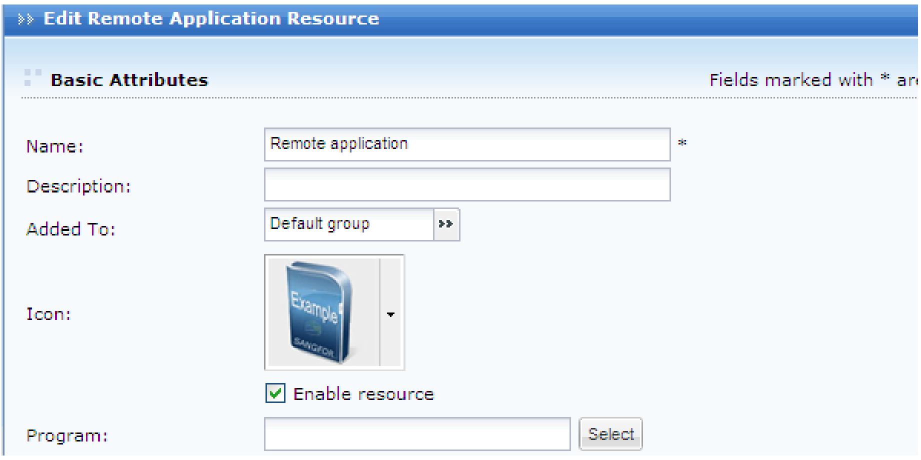


Remote Application Programs

	□	Application Program	Path	Valid?
1	□	WordPad	C:\Program Files\Windows NT\Accessories\wordpad....	Yes

10. Click the **Save** button on the **Edit Remote App Server** page to save the settings.

11. 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:



Edit Remote Application Resource

Basic Attributes

Fields marked with * ar

Name: Remote application *

Description:

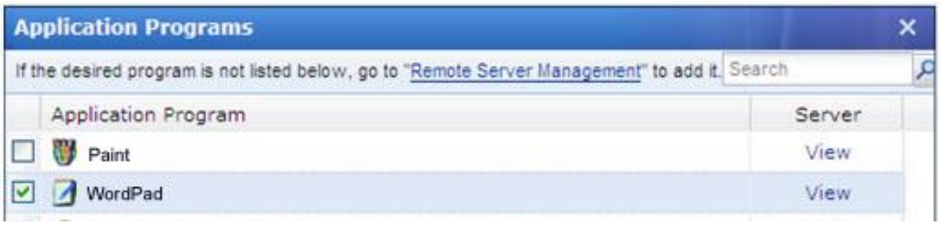
Added To: Default group

Icon:

☑ Enable resource

Program:

12. Click the **Select** button (next to **Program** field) to select program **WordPad**, as shown below:

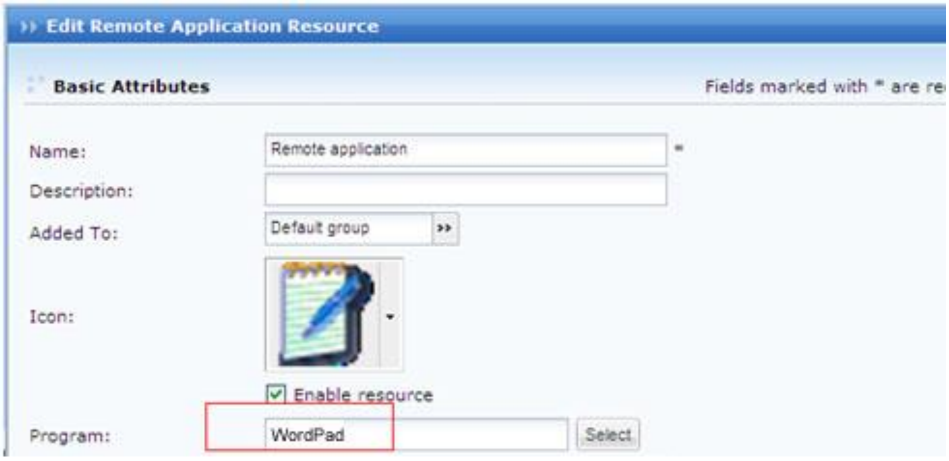


Application Programs

If the desired program is not listed below, go to "Remote Server Management" to add it. Search

	Application Program	Server
□	Paint	View
☑	WordPad	View

13. Click theOK button to save the settings and the program name is seen in the **Program** field:



Edit Remote Application Resource

Basic Attributes

Fields marked with * are re

Name: Remote application *

Description:

Added To: Default group

Icon:

☑ Enable resource

Program: WordPad Select

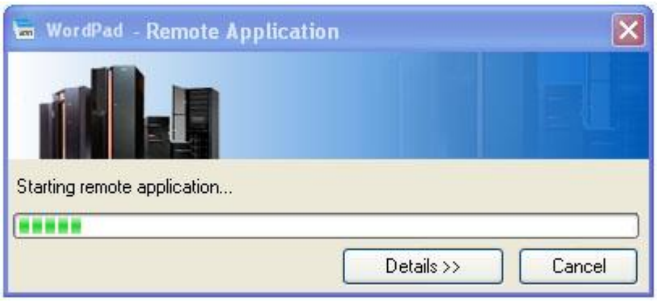
14. In the **App Server** tab, select an application server to publish **WordPad**.

15. Click the **Save** button on **Edit Remote Application Resource** page and then click the **Apply** button on the next page.

16. Navigate to **SSL VPN**>**Roles** to associate this remote application resource with the corresponding user (for detailed guide, please refer to the Roles sectioning 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.

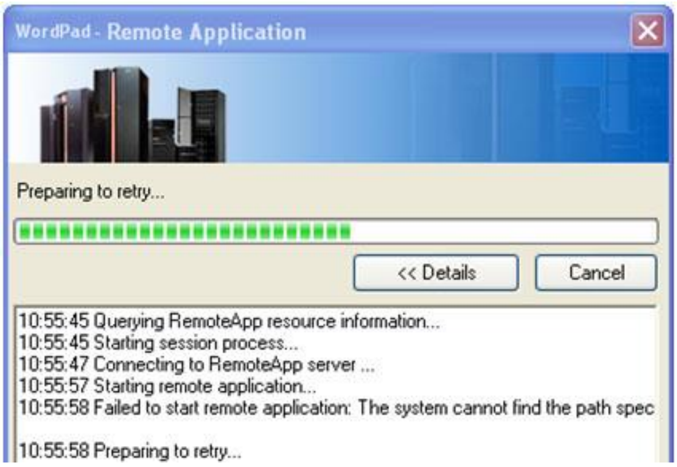
18. Click on the link to the remote application resource created in Step 11, and a remote application session will be established, as shown in the figure below:



WordPad - Remote Application

Starting remote application...

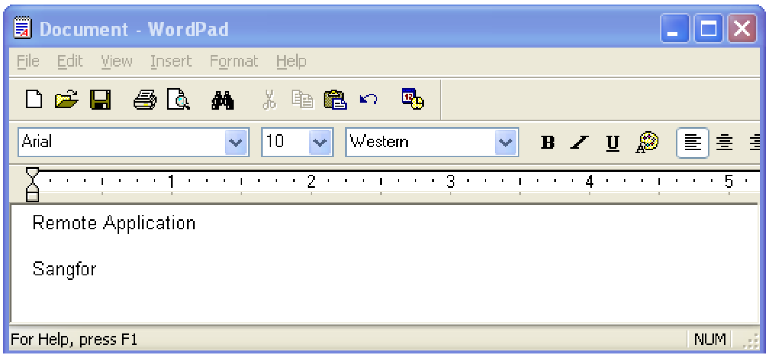
19. To view the connecting process, click the **Details** button. Progress details will be seen as follows:



```
10:55:45 Querying RemoteApp resource information...
10:55:45 Starting session process...
10:55:47 Connecting to RemoteApp server ...
10:55:57 Starting remote application...
10:55:58 Failed to start remote application: The system cannot find the path spec

10:55:58 Preparing to retry...
```

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.



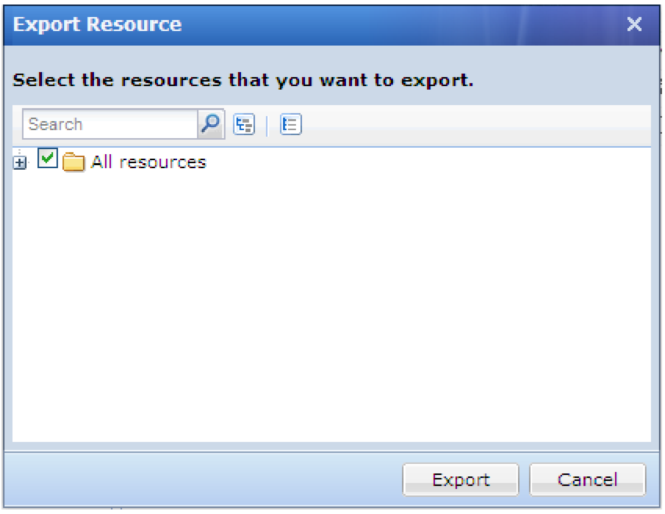
Remote Application

Sangfor

Exporting Resources

This feature helps export the existing resources from the current Sangfor device to the computer.

1. Navigate to **SSL VPN**>**Resources > Resource Management** and click **More**>**Export resource** to enter the **Export Resource** page, as shown the figure below:



Export Resource

Select the resources that you want to export.

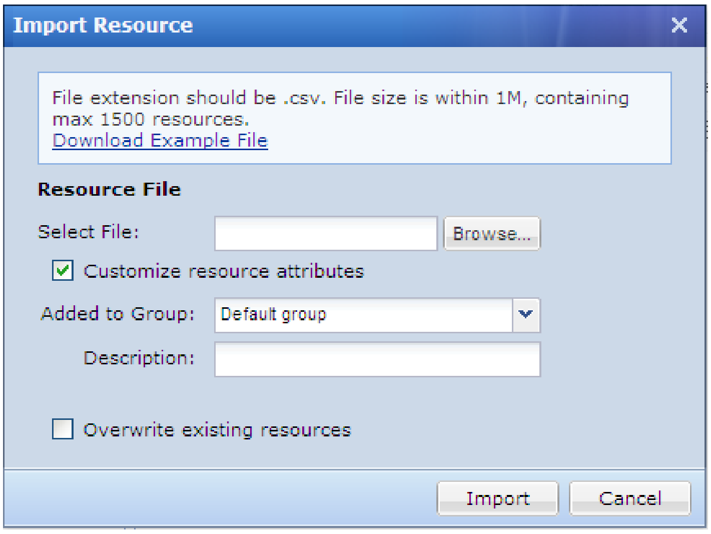
2. Select the checkboxes next to the resources or resource groups thatyou want to export.

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**>**Resource Management** and click **More**>**Import resource** to enter the **Import Resource** page, as shown in the figure below:



Import Resource

File extension should be .csv. File size is within 1M, containing max 1500 resources.
Download Example File

Resource File

Select File:

☑ Customize resource attributes

Added to Group: Default group

Description:

□ Overwrite existing resources

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.

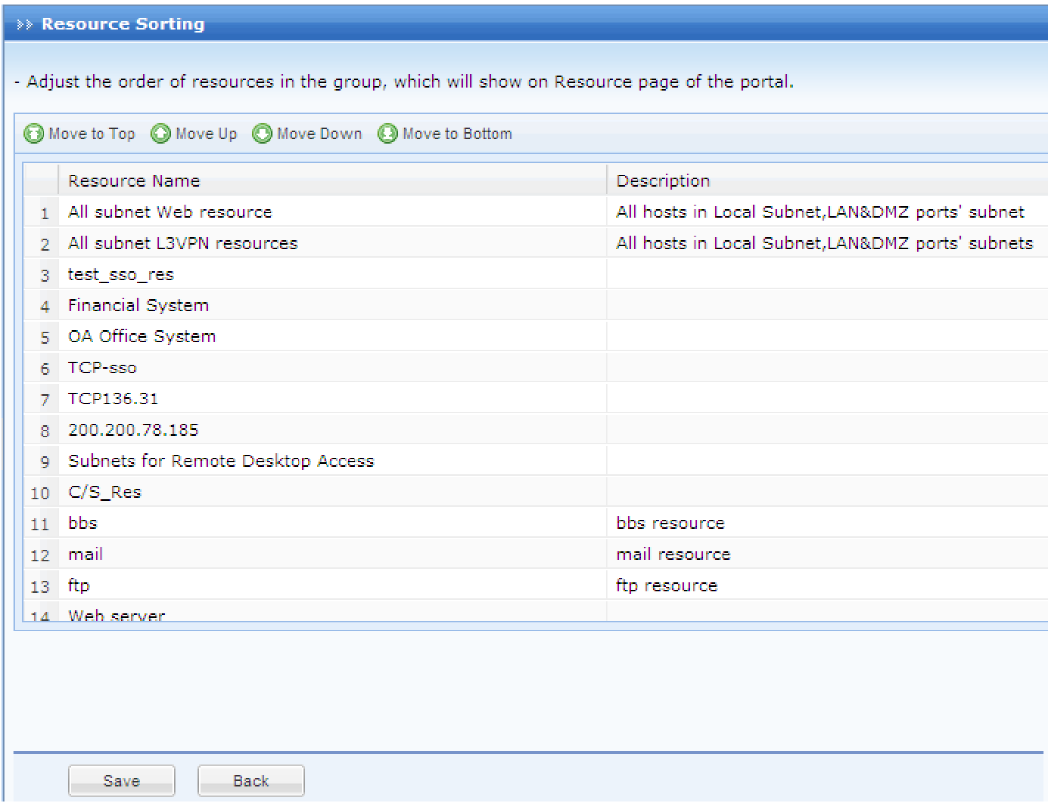
- **Customize resource attributes:** The two fields below it define the attributes of the imported resources, the description and the target group to which they are to be added.
- **Overwrite existing resources:** If this option is checked, the existing resource will be replaced by the imported resource that owns a same name.

3. Click the **Import** button.

Sorting Resources

Sorting resource is a feature applying to resource group. 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**>**Resource Management** and click **More**>**Import resource** to enter the **Import Resource** page, as shown in the figure below:



Resource Sorting

- Adjust the order of resources in the group, which will show on Resource page of the portal.

	Resource Name	Description
1	All subnet Web resource	All hosts in Local Subnet,LAN&DMZ ports' subnet
2	All subnet L3VPN resources	All hosts in Local Subnet,LAN&DMZ ports' subnets
3	test_sso_res	
4	Financial System	
5	OA Office System	
6	TCP-sso	
7	TCP136.31	
8	200.200.78.185	
9	Subnets for Remote Desktop Access	
10	C/S_Res	
11	bbs	bbs resource
12	mail	mail resource
13	ftp	ftp resource
14	Web server	

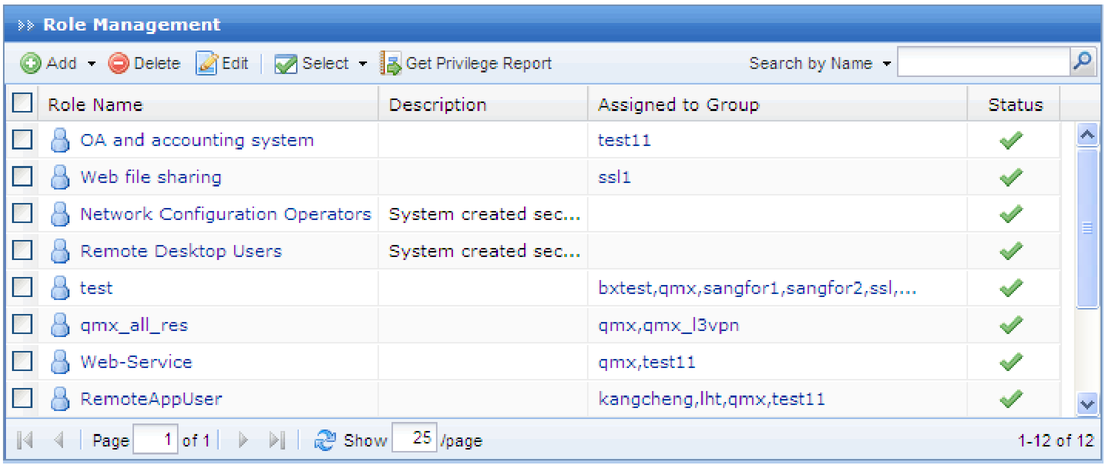
2. To move an entry to top of the list, click the entry and click **Move to Top**.
3. To move an entry to bottom of the list, click the entry and click **Move to Bottom**.
4. To move an entry up and exchange order with the upper entry, click the entry and click **Move Up**.
5. To move an entry down and exchange order with the lower entry, click the entry and click **Move Down**.

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:



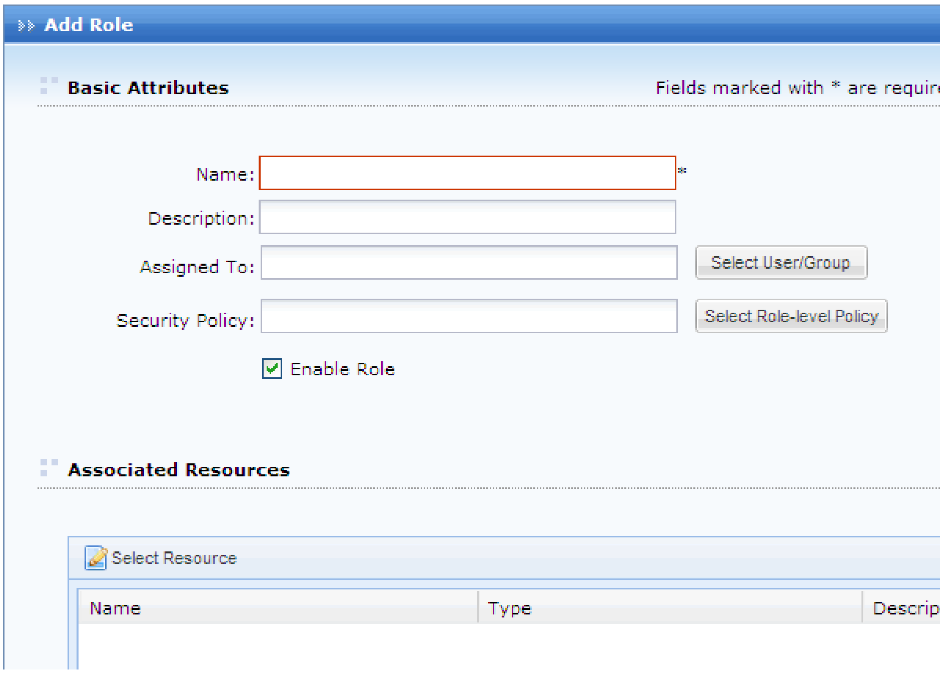
☐	Role Name	Description	Assigned to Group	Status
☐	OA and accounting system		test11	✓
☐	Web file sharing		ssl1	✓
☐	Network Configuration Operators	System created sec...		✓
☐	Remote Desktop Users	System created sec...		✓
☐	test		bxtest,qmx,sangfor1,sangfor2,ssl,...	✓
☐	qmx_all_res		qmx,qmx_l3vpn	✓
☐	Web-Service		qmx,test11	✓
☐	RemoteAppUser		kangcheng,lht,qmx,test11	✓

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).

Adding Role

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



Add Role

Basic Attributes

Fields marked with * are requir

Name: *

Description:

Assigned To:

Security Policy:

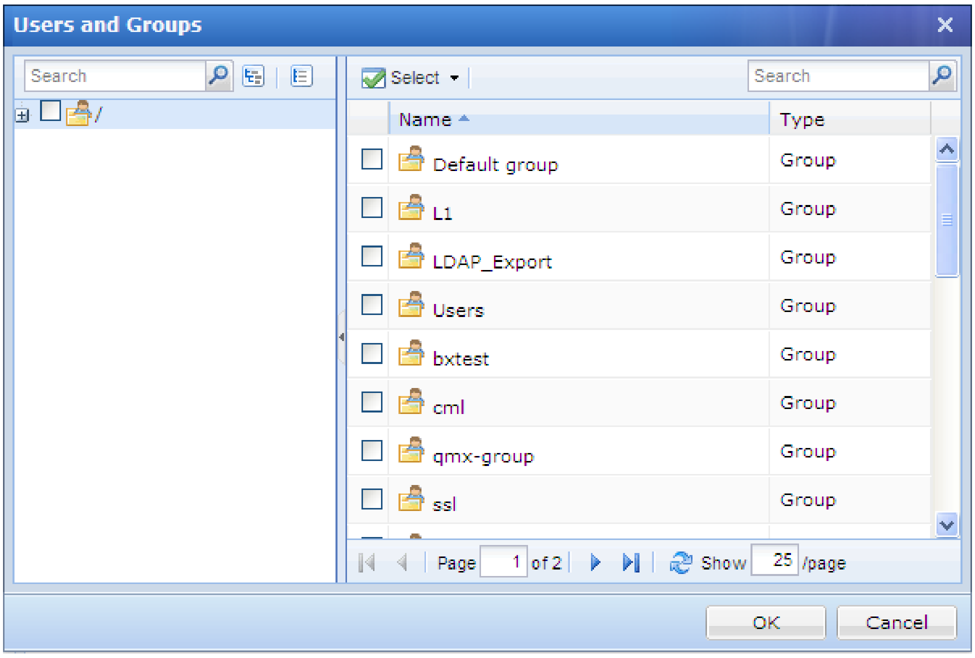
☑ Enable Role

Associated Resources

Name	Type	Descrip

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 **User Management** page are seen in the list, as shown below:



Users and Groups

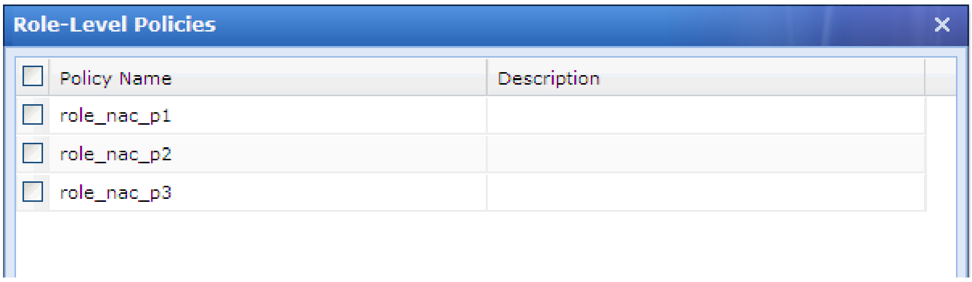
	Name	Type
□	Default group	Group
□	L1	Group
□	LDAP_Export	Group
□	Users	Group
□	bxtest	Group
□	cml	Group
□	qmx-group	Group
□	ssl	Group

Page 1 of 2 Show 25 /page

Select the user or group to which the role is to be assigned and click the **OK** button.

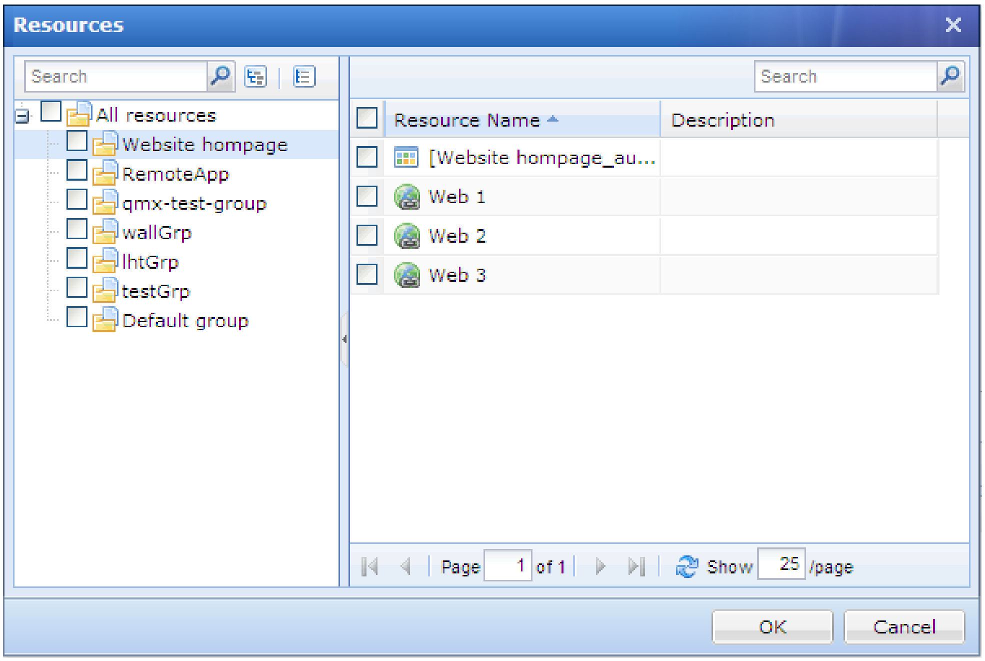
- **Security Policy:** This policy enforces host checking when user logs in to the SSL VPN. If user fails any security check, he or she cannot access the associated resources.

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 Policysectioning chapter 4), as shown in the figure below:



□	Policy Name	Description
□	role_nac_p1	
□	role_nac_p2	
□	role_nac_p3	

3. Configure associated resources. Click **Select Resources** to enter the **Resources** page and select resources that the associated users of this role can access, as shown below:



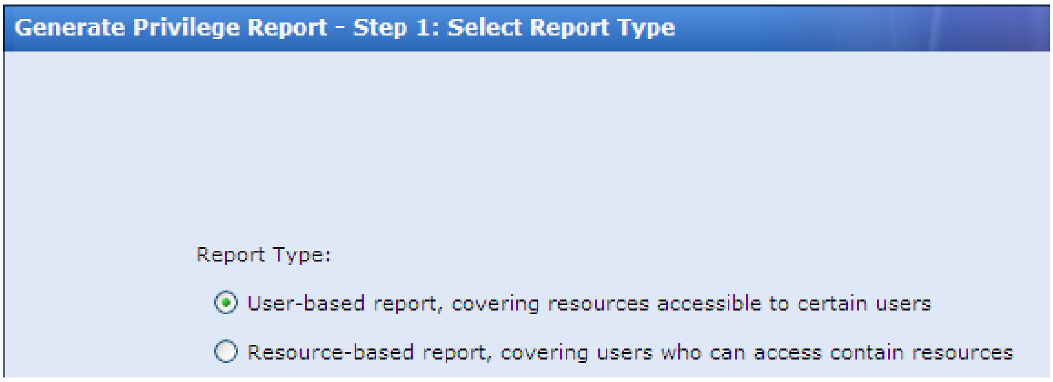
□	Resource Name ▲	Description
□	[Website hompage_au...	
□	Web 1	
□	Web 2	
□	Web 3	

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:



Generate Privilege Report - Step 1: Select Report Type

Report Type:

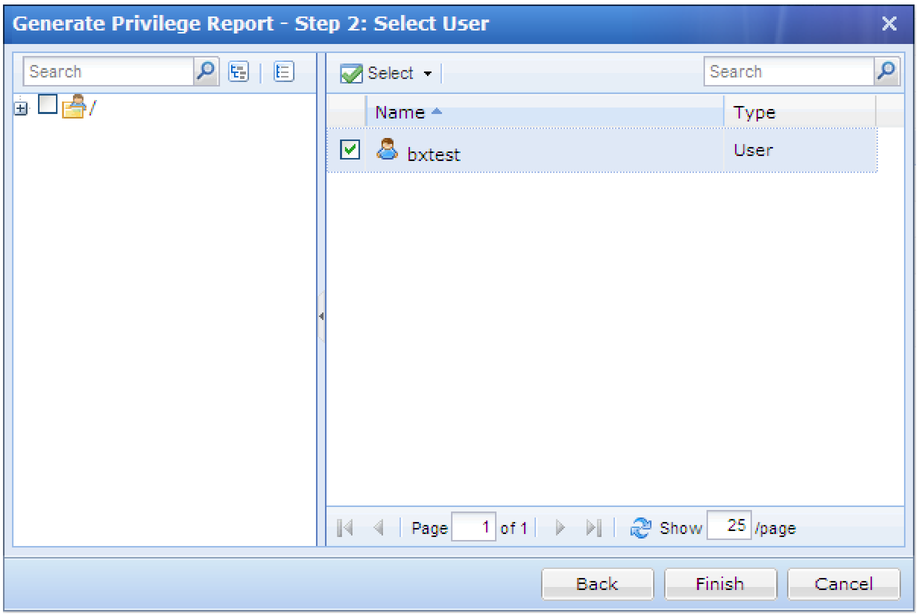
● User-based report, covering resources accessible to certain users

○ Resource-based report, covering users who can access contain resources

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:

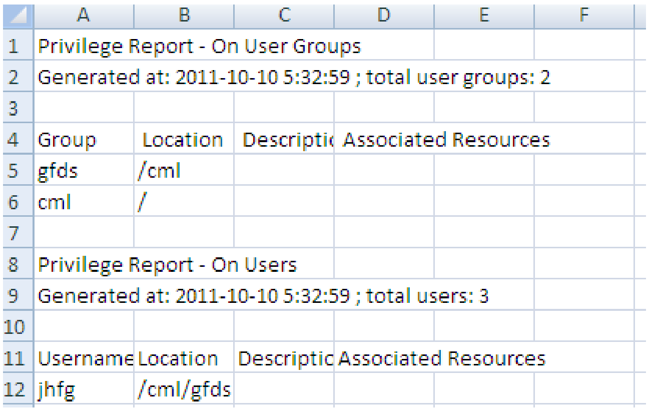


Generate Privilege Report - Step 2: Select User

	Name	Type
☑	bxtest	User

Page 1 of 1 Show 25 /page

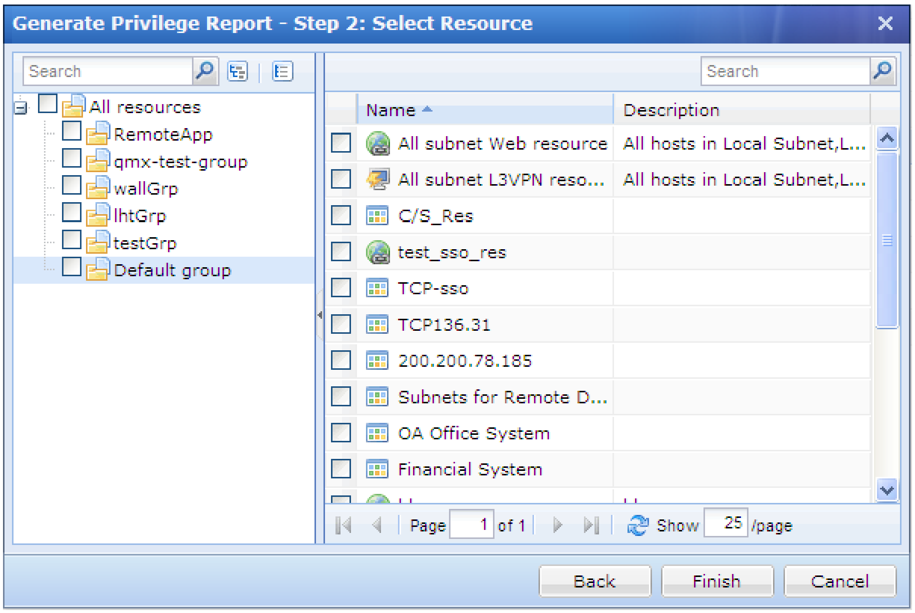
   b. Select the desired user(s) and click the **Finish** button to download the .csv file. The download user-based privilege report file is as shown below:



	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:



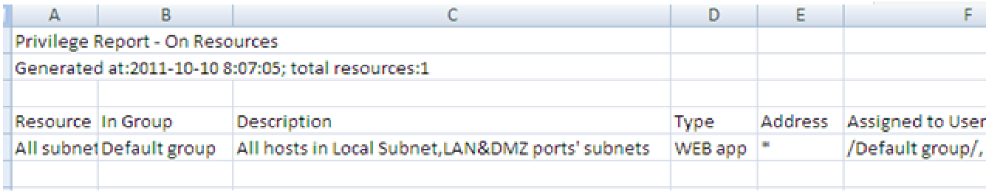
Generate Privilege Report - Step 2: Select Resource

- □ All resources
  - □ RemoteApp
  - □ qmx-test-group
  - □ wallGrp
  - □ lhtGrp
  - □ testGrp
  - □ Default group

	Name	Description
□	All subnet Web resource	All hosts in Local Subnet,L...
□	All subnet L3VPN reso...	All hosts in Local Subnet,L...
□	C/S_Res	
□	test_sso_res	
□	TCP-sso	
□	TCP136.31	
□	200.200.78.185	
□	Subnets for Remote D...	
□	OA Office System	
□	Financial System	

Page 1 of 1 Show 25 /page

b. Select the desired user(s) and click the **Finish** button to download the .csv file. The download resource-based privilege report file is as shown below:

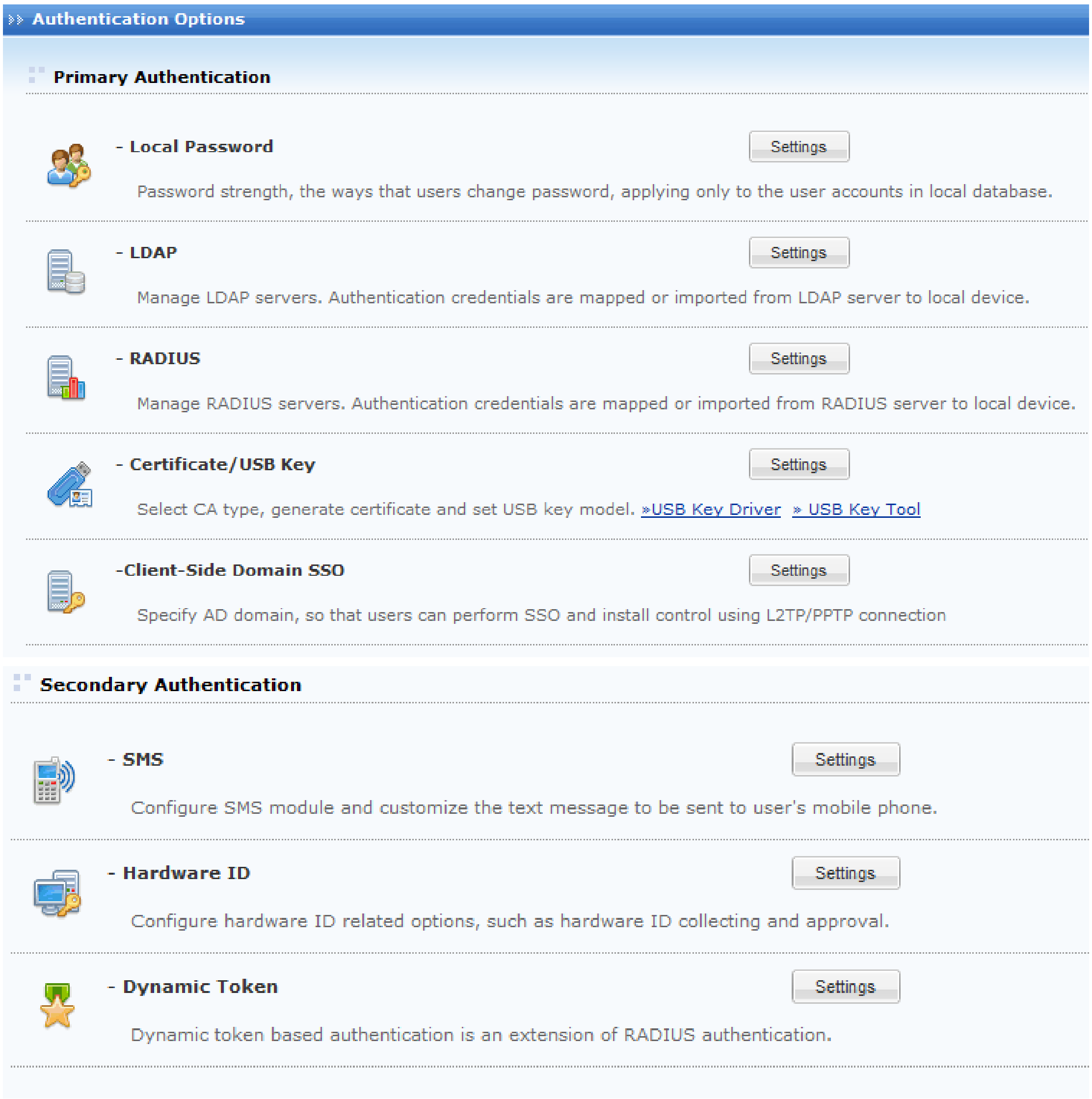


A	B	C	D	E	F
Privilege Report - On Resources					
Generated at:2011-10-10 8:07:05; total resources:1					
Resource	In Group	Description	Type	Address	Assigned to User
All subnet	Default group	All hosts in Local Subnet,LAN&DMZ ports' subnets	WEB app	*	/Default group/,

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:



Authentication Options

Primary Authentication

- Local Password [Settings]
Password strength, the ways that users change password, applying only to the user accounts in local database.

- LDAP [Settings]
Manage LDAP servers. Authentication credentials are mapped or imported from LDAP server to local device.

- RADIUS [Settings]
Manage RADIUS servers. Authentication credentials are mapped or imported from RADIUS server to local device.

- Certificate/USB Key [Settings]
Select CA type, generate certificate and set USB key model. »USB Key Driver » USB Key Tool

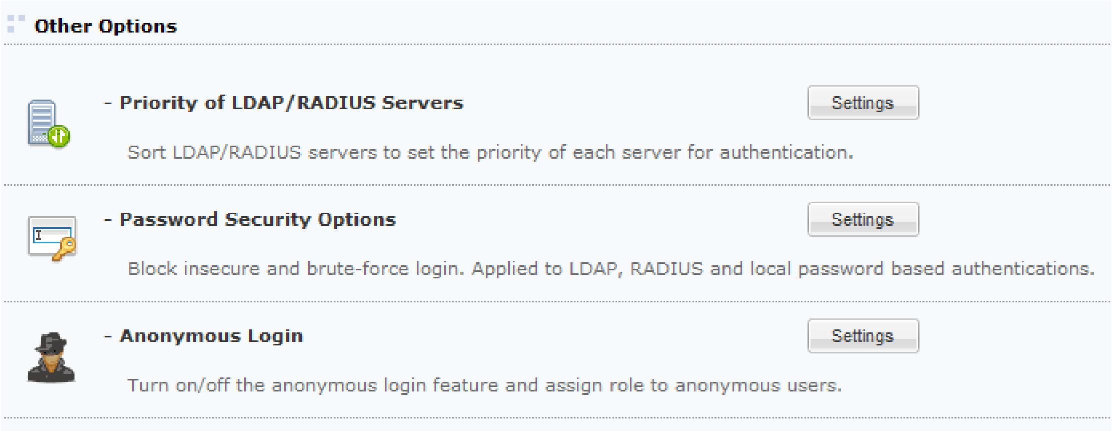
-Client-Side Domain SSO [Settings]
Specify AD domain, so that users can perform SSO and install control using L2TP/PPTP connection

Secondary Authentication

- SMS [Settings]
Configure SMS module and customize the text message to be sent to user's mobile phone.

- Hardware ID [Settings]
Configure hardware ID related options, such as hardware ID collecting and approval.

- Dynamic Token [Settings]
Dynamic token based authentication is an extension of RADIUS authentication.



Other Options

- Priority of LDAP/RADIUS Servers

Sort LDAP/RADIUS servers to set the priority of each server for authentication.

- Password Security Options

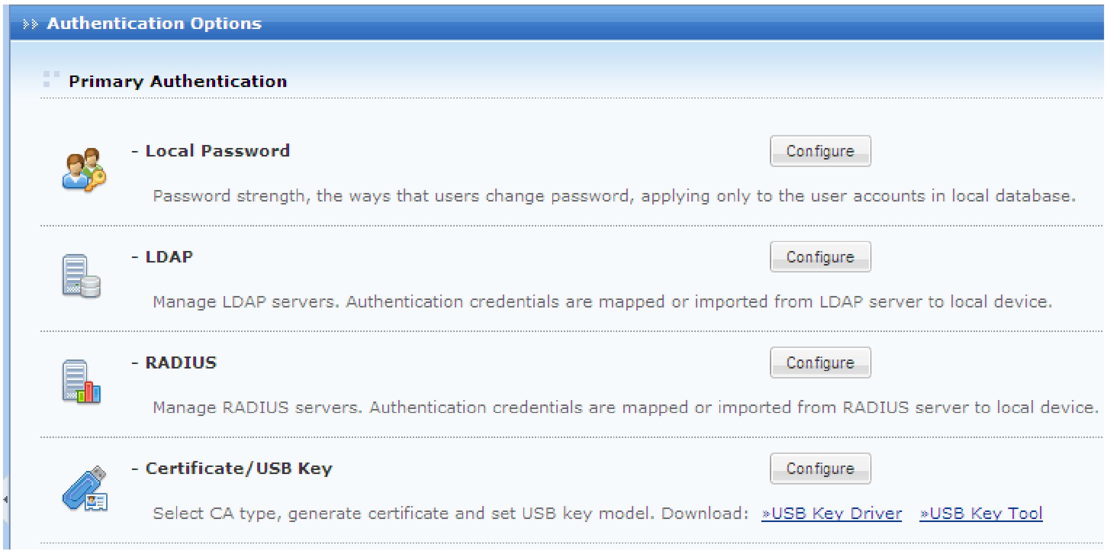
Block insecure and brute-force login. Applied to LDAP, RADIUS and local password based authentications.

- Anonymous Login

Turn on/off the anonymous login feature and assign role to anonymous users.

Primary Authentication Methods

There are four primary authentication methods, namely, **local password** based authentication, **LDAP** authentication, **RADIUS** authentication and **certificate/USB key** based authentication.



Authentication Options

Primary Authentication

- Local Password

Password strength, the ways that users change password, applying only to the user accounts in local database.

- LDAP

Manage LDAP servers. Authentication credentials are mapped or imported from LDAP server to local device.

- RADIUS

Manage RADIUS servers. Authentication credentials are mapped or imported from RADIUS server to local device.

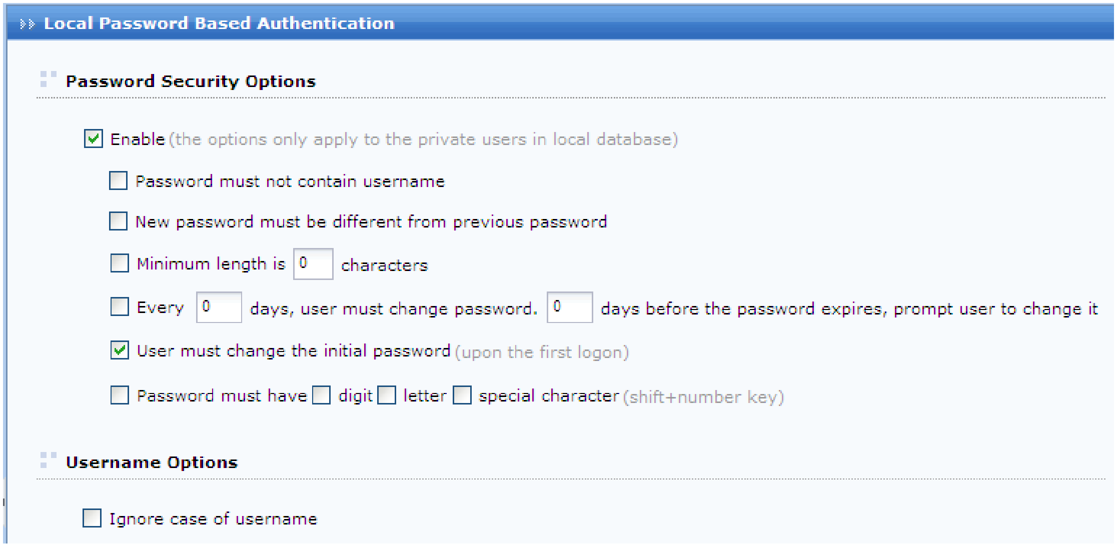
- Certificate/USB Key

Select CA type, generate certificate and set USB key model. Download: »USB Key Driver »USB Key Tool

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 **Configure** button following **Local Password**, and the **Local Password Based Authentication** page appears, as shown in the figure below:



Local Password Based Authentication

Password Security Options

☑ Enable (the options only apply to the private users in local database)

□ Password must not contain username

□ New password must be different from previous password

□ Minimum length is 0 characters

□ Every 0 days, user must change password. 0 days before the password expires, prompt user to change it

☑ User must change the initial password (upon the first logon)

□ Password must have □ digit □ letter □ special character (shift+number key)

Username Options

□ Ignore case of username

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.
- **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.

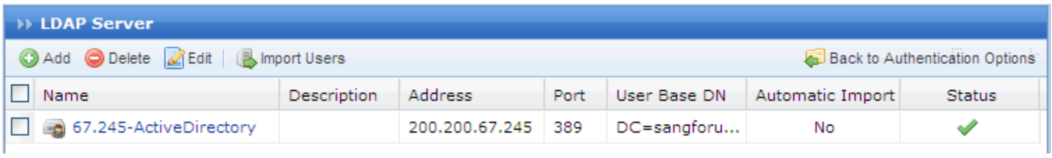
Password Security Options and **Username Options** only apply to the user accounts in local Sangfor device.

LDAP Authentication

Sangfor device supports third-party LDAP server to verify the users connecting the SSL VPN.

Configuring LDAP Server

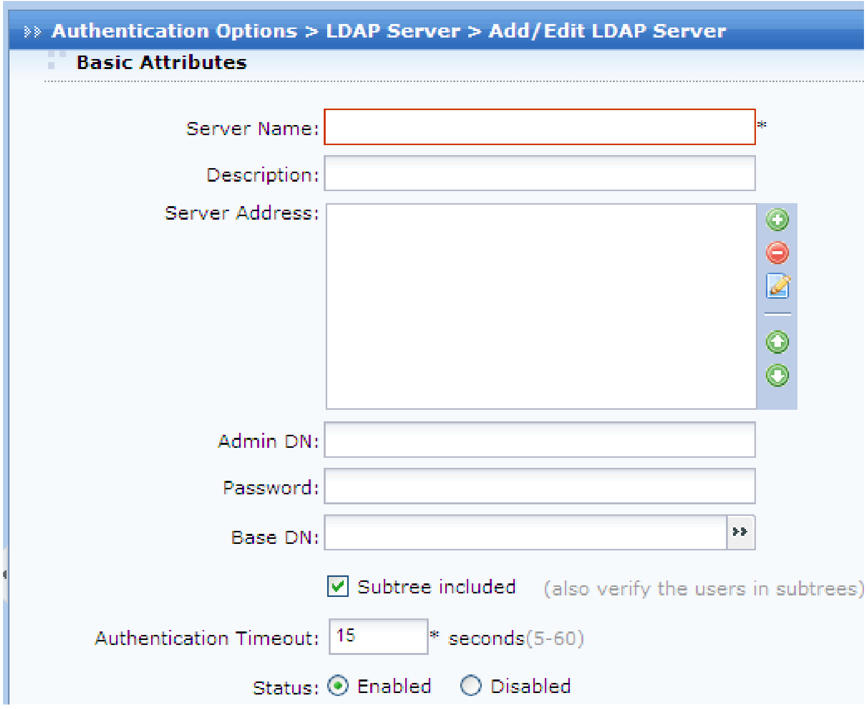
1. Navigate to **SSL VPN>Authentication** to enter the **Authentication Options** page. Click the **Configure** button following **LDAP** and the **LDAP Server** page appears, as shown below:



LDAP Server

□	Name	Description	Address	Port	User Base DN	Automatic Import	Status
□	67.245-ActiveDirectory		200.200.67.245	389	DC=sangforu...	No	✓

2. Click **Add** to enter the **Add/Edit LDAP Server** page, as shown below:



Authentication Options > LDAP Server > Add/Edit LDAP Server

Basic Attributes

Server Name: *

Description:

Server Address:

Admin DN:

Password:

Base DN:

☑ Subtree included (also verify the users in subtrees)

Authentication Timeout: 15 * seconds(5-60)

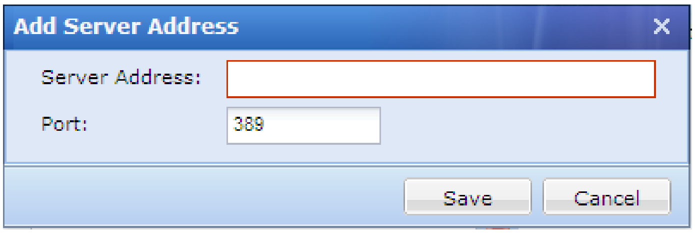
Status: ● Enabled ○ Disabled

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:



Add Server Address

Server Address:

Port: 389

  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**.

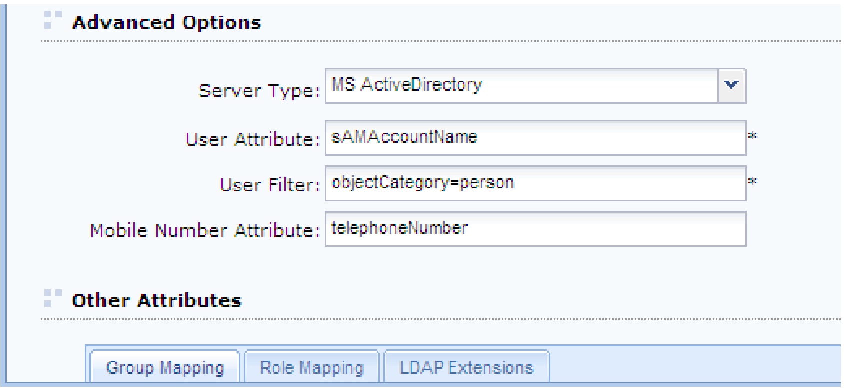
  To adjust order of an entry, click the entry and click **Move Up** icon or **Move Down** icon .

- **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.

Thisadministrator 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.
- **Sub tree 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 that user authentication is 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



Advanced Options

Server Type: MS ActiveDirectory

User Attribute: sAMAccountName *

User Filter: objectCategory=person *

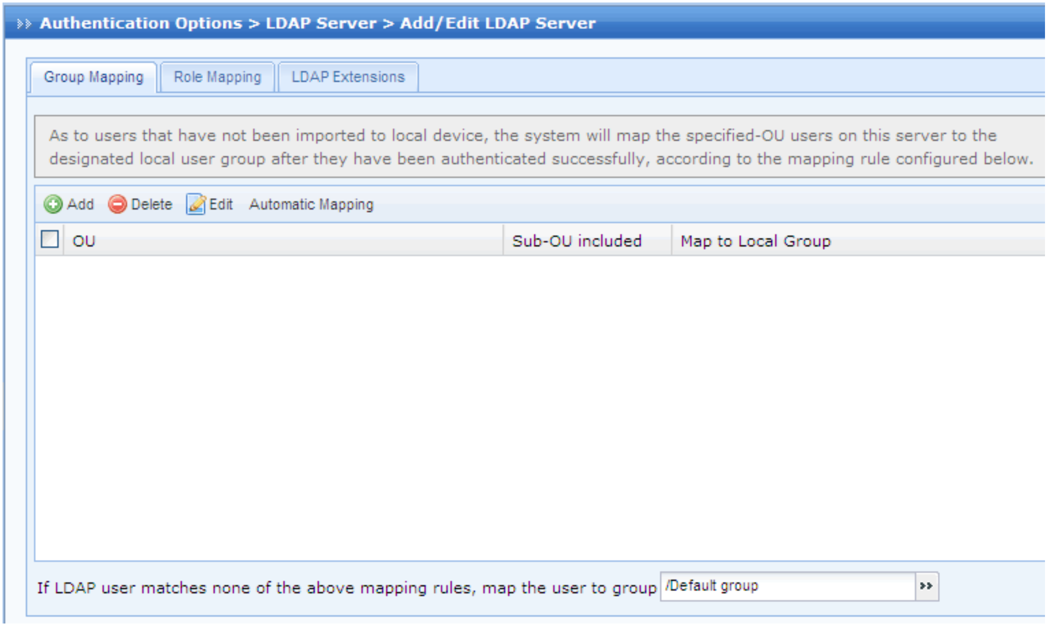
Mobile Number Attribute: telephoneNumber

Other Attributes

Protocols supported are LDAP and MS Active Directory (AD). For MS AD, user authentication is achieved using attribute **sAMAccountName** and filter **object Category=person**. For LDAP, user authentication is achieved using attribute **aid** and filter **object class=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.



Authentication Options > LDAP Server > Add/Edit LDAP Server

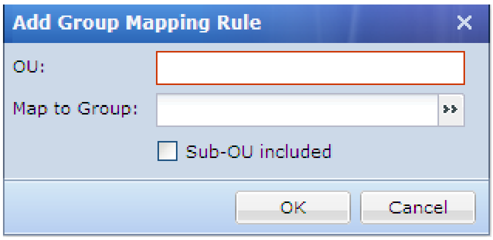
As to users that have not been imported to local device, the system will map the specified-OU users on this server to the designated local user group after they have been authenticated successfully, according to the mapping rule configured below.

☐ OU	Sub-OU included	Map to Local Group

If LDAP user matches none of the above mapping rules, map the user to group: /Default group

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, clickitto enter the **Add Group Mapping Rule** page, as shown in the figure below:



Add Group Mapping Rule

OU:

Map to Group:

☐ Sub-OU included

  - **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.

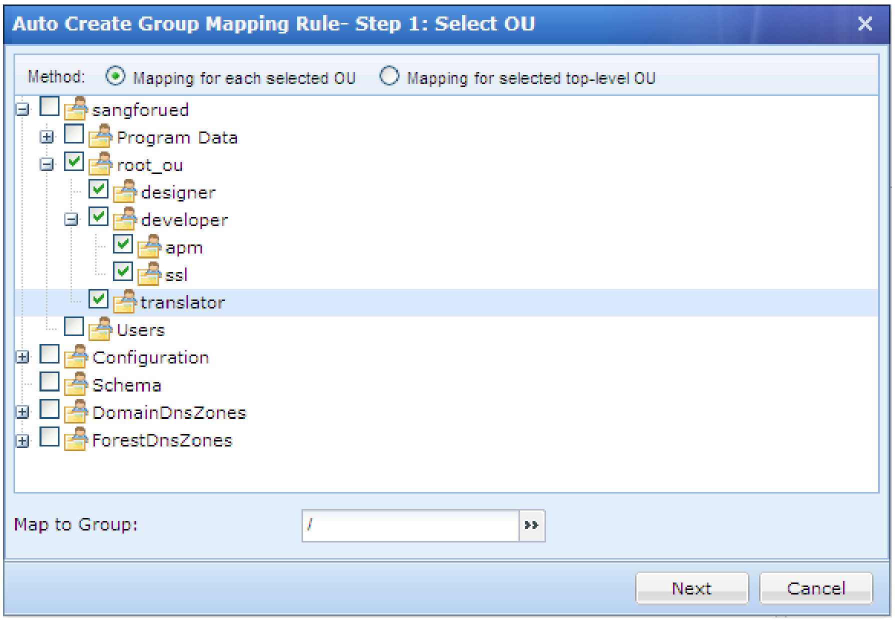
- **If LDAP user matches none of the above mapping rules, map the user to group:** For the users that match none of the group mapping rules, select this option and specify local group, so that those LDAP users will be mapped to that group automatically.

- **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:



Auto Create Group Mapping Rule- Step 1: Select OU

Method: ● Mapping for each selected OU ○ Mapping for selected top-level OU

- □ sangforued
  - □ Program Data
  - ☑ root_ou
    - ☑ designer
    - ☑ developer
      - ☑ apm
      - ☑ ssl
    - ☑ translator
  - □ Users
- □ Configuration
- □ Schema
- □ DomainDnsZones
- □ ForestDnsZones

Map to Group: /

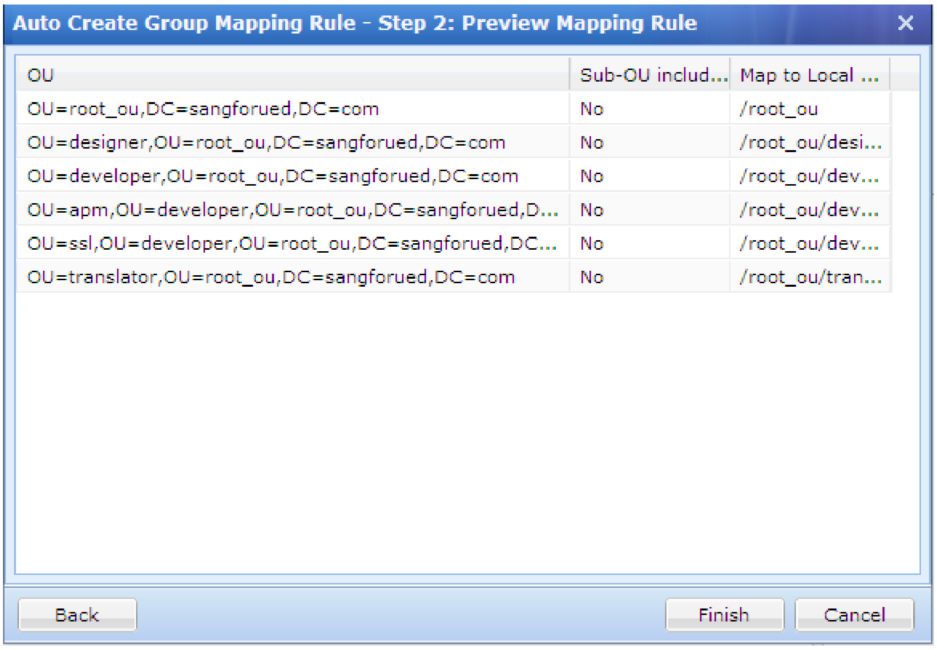
b. Select a mapping method, **Mapping for each selected OU** or **Mapping for selected top-level OU**, and then select the organizational units (OU).

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) specifiedin **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 theSangfor 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.

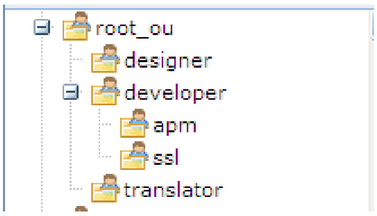
d. Click the **Next** button and the automatically added mapping rules are as shown below:



Auto Create Group Mapping Rule - Step 2: Preview Mapping Rule

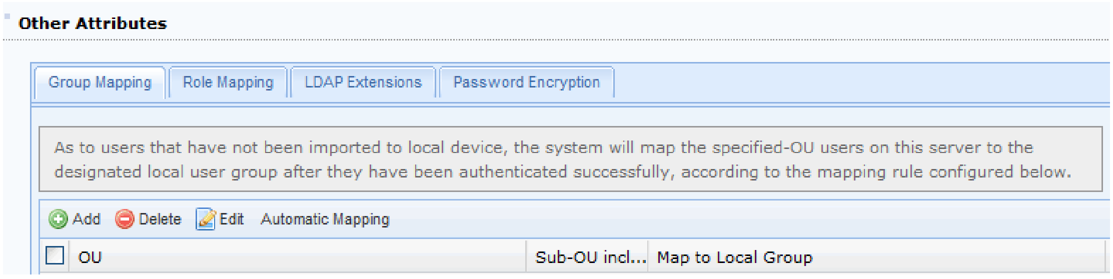
OU	Sub-OU includ...	Map to Local ...
OU=root_ou,DC=sangforued,DC=com	No	/root_ou
OU=designer,OU=root_ou,DC=sangforued,DC=com	No	/root_ou/desi...
OU=developer,OU=root_ou,DC=sangforued,DC=com	No	/root_ou/dev...
OU=apm,OU=developer,OU=root_ou,DC=sangforued,D...	No	/root_ou/dev...
OU=ssl,OU=developer,OU=root_ou,DC=sangforued,DC...	No	/root_ou/dev...
OU=translator,OU=root_ou,DC=sangforued,DC=com	No	/root_ou/tran...

e. Click the **Finish** and **save** buttons and go back to **User Management** 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:



Other Attributes

As to users that have not been imported to local device, the system will map the specified-OU users on this server to the designated local user group after they have been authenticated successfully, according to the mapping rule configured below.

□	OU	Sub-OU incl...	Map to Local Group

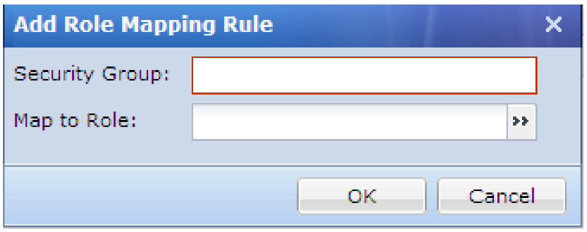
The following are the contents included on the **Role Mapping** tab:

- **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:



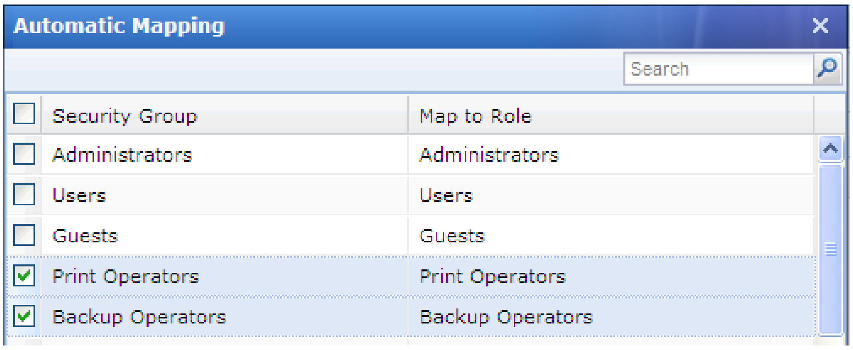
Add Role Mapping Rule

Security Group:

Map to Role:

- **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:

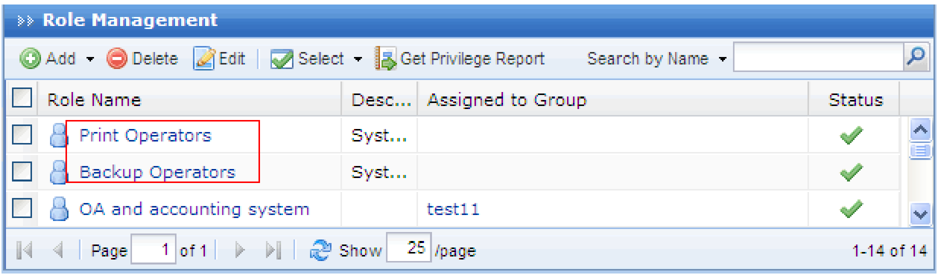
  a. Click **Automatic Mapping** and the following page pops up, as shown below:



Automatic Mapping

□	Security Group	Map to Role
□	Administrators	Administrators
□	Users	Users
□	Guests	Guests
☑	Print Operators	Print Operators
☑	Backup Operators	Backup Operators

  b. Select the desired role mapping rules, click the OK, and **Save** buttons. The two selected roles are then added to **Role Management** page, as shown below:

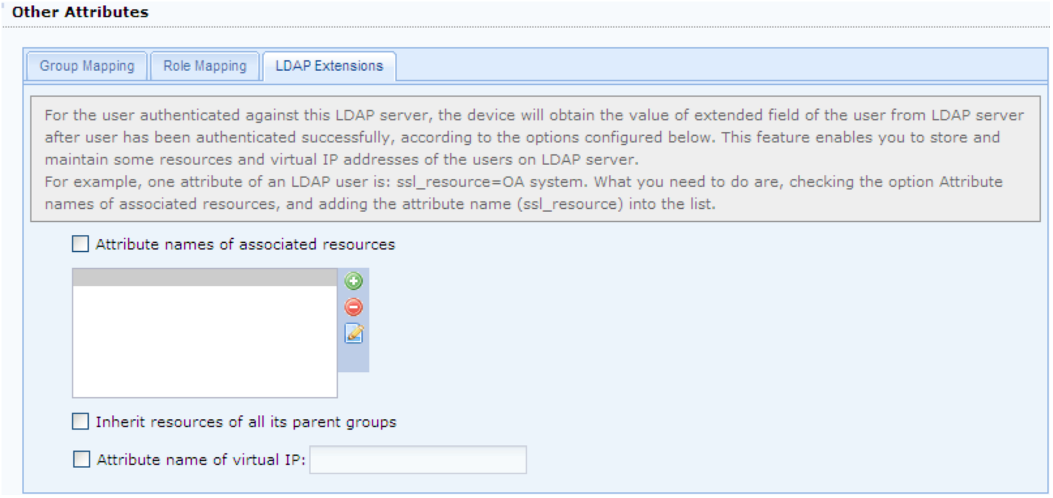


Role Management

□	Role Name	Desc...	Assigned to Group	Status
□	Print Operators	Syst...		✓
□	Backup Operators	Syst...		✓
□	OA and accounting system		test11	✓

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.



For the user authenticated against this LDAP server, the device will obtain the value of extended field of the user from LDAP server after user has been authenticated successfully, according to the options configured below. This feature enables you to store and maintain some resources and virtual IP addresses of the users on LDAP server.
For example, one attribute of an LDAP user is: ssl_resource=OA system. What you need to do are, checking the option Attribute names of associated resources, and adding the attribute name (ssl_resource) into the list.

□ Attribute names of associated resources

□ Inherit resources of all its parent groups

□ Attribute name of virtual IP:

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.

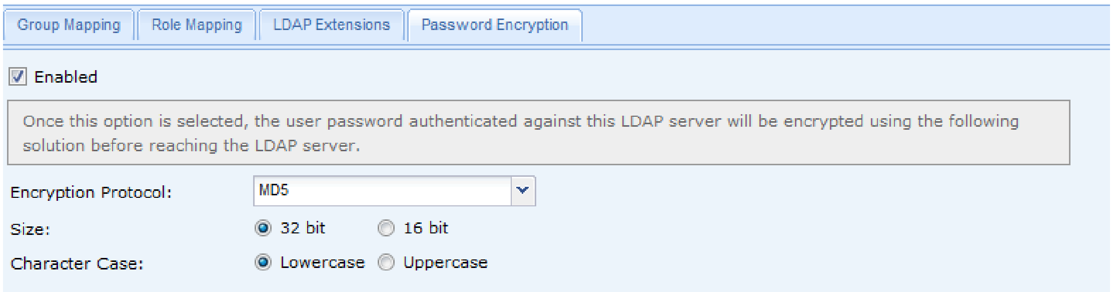
- **Inherit resources of all its parent groups:** Besides the resources with the specified attributes, all other resources (available to users in the specified OU and parent OUs of certain LDAP user) with the configured attributes will be displayed on **Resource** page and seen by the LDAP user once 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 **SSLVPN>Users**), this option is invalid.

8. Configure **Password Encryption**

For the user's password encryption processing, and then forwarded to the LDAP server for authentication.



☑ Enabled

Once this option is selected, the user password authenticated against this LDAP server will be encrypted using the following solution before reaching the LDAP server.

Encryption Protocol: MD5

Size: ● 32 bit ○ 16 bit

Character Case: ● Lowercase ○ Uppercase

- **Encryption Protocol**: able to choose **MD5** and **SHA1**for encrypt method.
- **Size**: select either 32bit or 16bit.
- **Character Case**: choose password lowercase or uppercase.

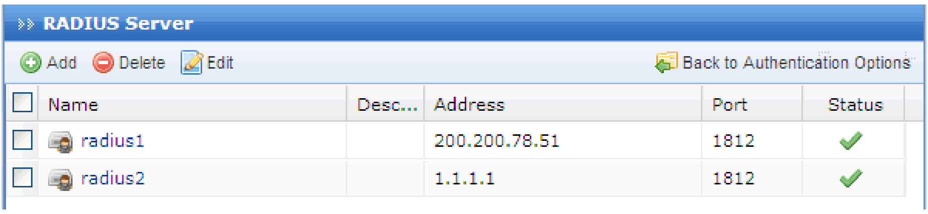
9. Click the **Save** button and thenthe **Apply** button to save and apply the settings.

RADIUS Authentication

Sangfor device supports third-party RADIUS server to verify the users connecting the SSL VPN.

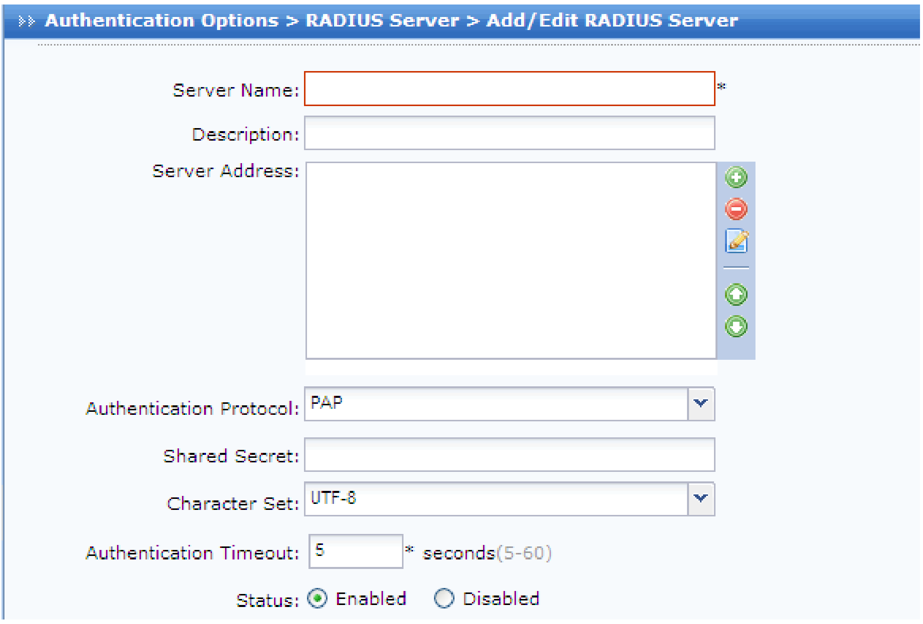
Configuring RADIUS Server

1. Navigate to **SSL VPN**>**Authentication** to enter **Authentication Options** page. Click the **Configure** button following **RADIUS** and **RADIUS Server** page appears, as shown below:



□	Name	Desc...	Address	Port	Status
□	radius1		200.200.78.51	1812	✓
□	radius2		1.1.1.1	1812	✓

2. click **Add** to enter the **Add/Edit RADIUS Server** page, as shown below:



»» Authentication Options > RADIUS Server > Add/Edit RADIUS Server

Server Name: *

Description:

Server Address:

Authentication Protocol: PAP

Shared Secret:

Character Set: UTF-8

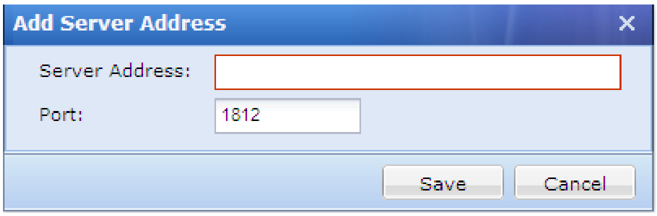
Authentication Timeout: 5 * seconds(5-60)

Status: ● Enabled ○ Disabled

10. 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:

  Add Server Address

  Server Address:

  Port: 1812

  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**.

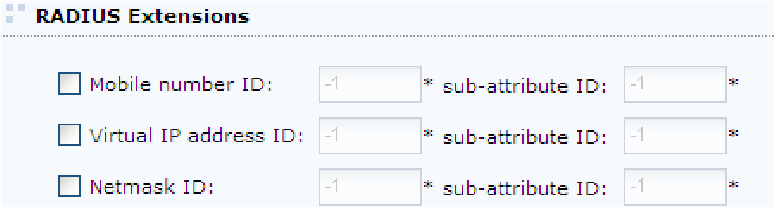
  To adjust order of an entry, click the entry and click **Move Up** icon or **Move Down** icon .

- **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 that user authentication times out if RADIUS server gives

no response.

- **Status:** Indicates whether the external RADIUS server is enabled.

11. Configure **RADIUS Extensions**, as shown below:



RADIUS Extensions

□ Mobile number ID: -1 * sub-attribute ID: -1 *

□ Virtual IP address ID: -1 * sub-attribute ID: -1 *

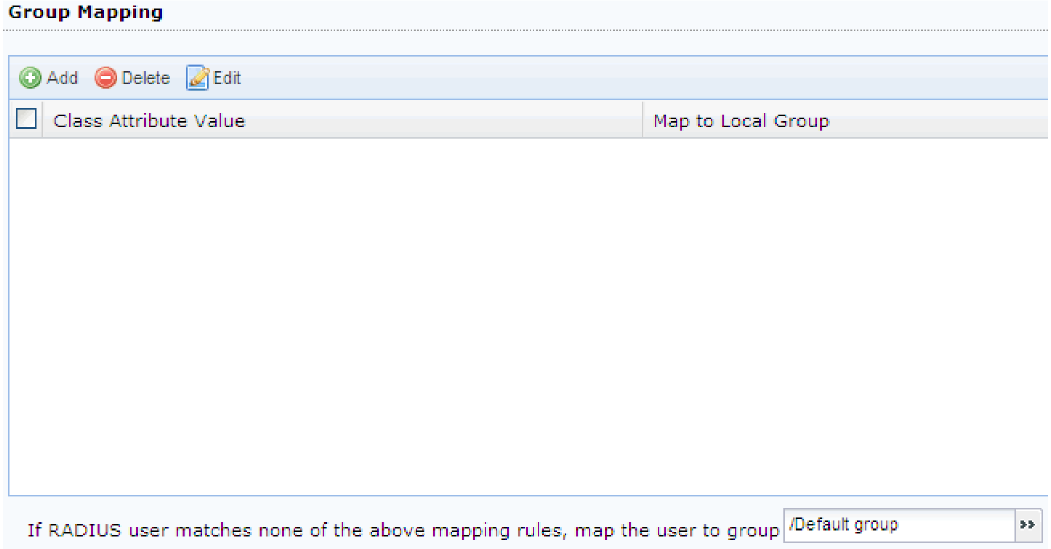
□ Netmask ID: -1 * sub-attribute ID: -1 *

- **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.
- RADIUS extensions apply to the RADIUS users that own or do not own a corresponding account on the Sangfor device (under **SSL VPN**>**Users**). To have it work, ensure that the primary authentication method configured for the user account on the Sangfor device includes external RADIUS.

12. 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 underthe group to which they are mapped.



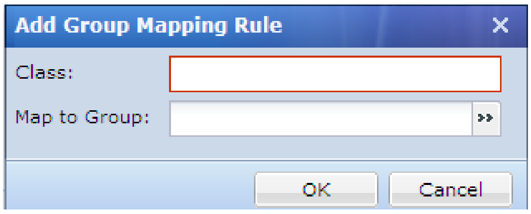
Group Mapping

□	Class Attribute Value	Map to Local Group

If RADIUS user matches none of the above mapping rules, map the user to group /Default group »

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:



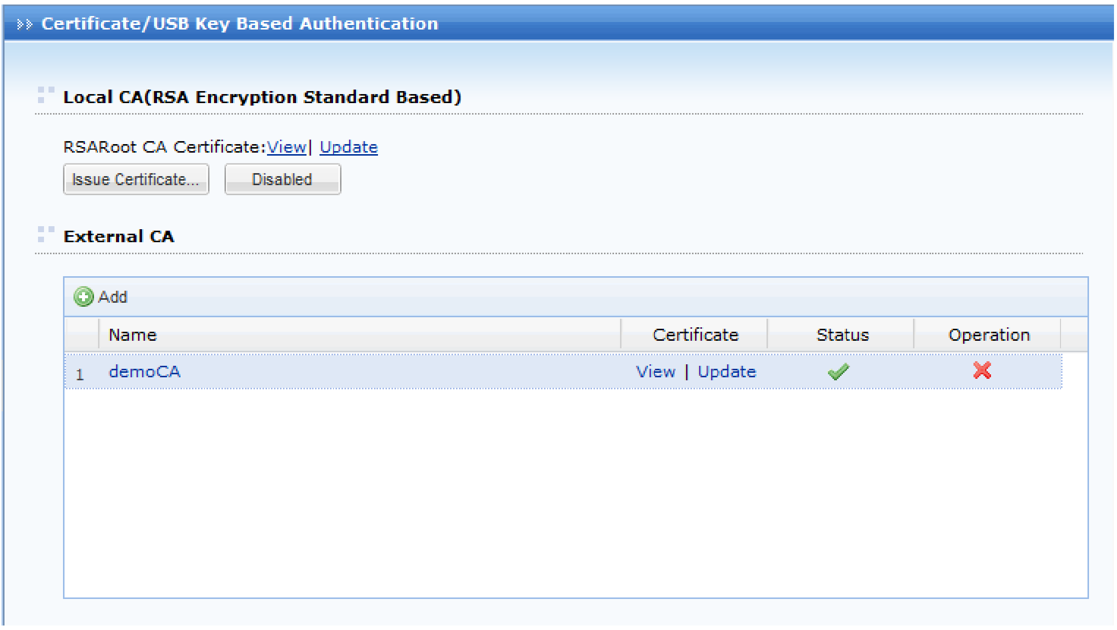
- **Delete:** To delete a group mapping rule, select that rule and then click **Delete**.
- **Edit:** To edit a group mapping rule, select that rule and then click **Edit**.
- **If RADIUS user matches none of the above mapping rules, map the user to group:** For the users that match none of the group mapping rules, select this option and specify the local group to which the RADIUS users will be mapped automatically.

13. 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 and can offer some certificate information. 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. Click the **Configure** button following **Certificate/USB Key** and the **Certificate/USB Key Based Authentication** page appears, as shown in the figure below:



Certificate/USB Key Based Authentication

Local CA(RSA Encryption Standard Based)

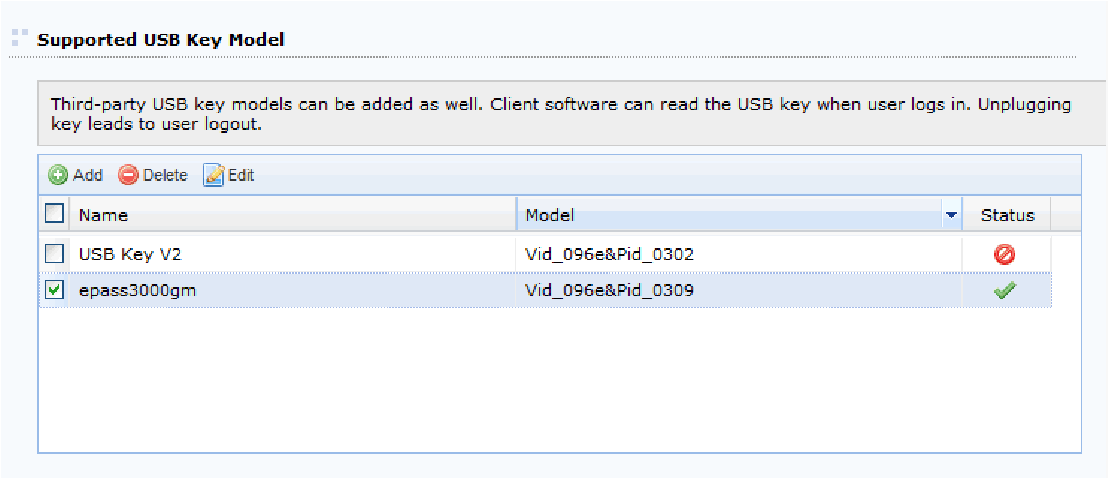
RSARoot CA Certificate:View| Update

Issue Certificate... | Disabled

External CA

Add

	Name	Certificate	Status	Operation
1	demoCA	View | Update	✓	✗



Supported USB Key Model

Third-party USB key models can be added as well. Client software can read the USB key when user logs in. Unplugging key leads to user logout.

Add | Delete | Edit

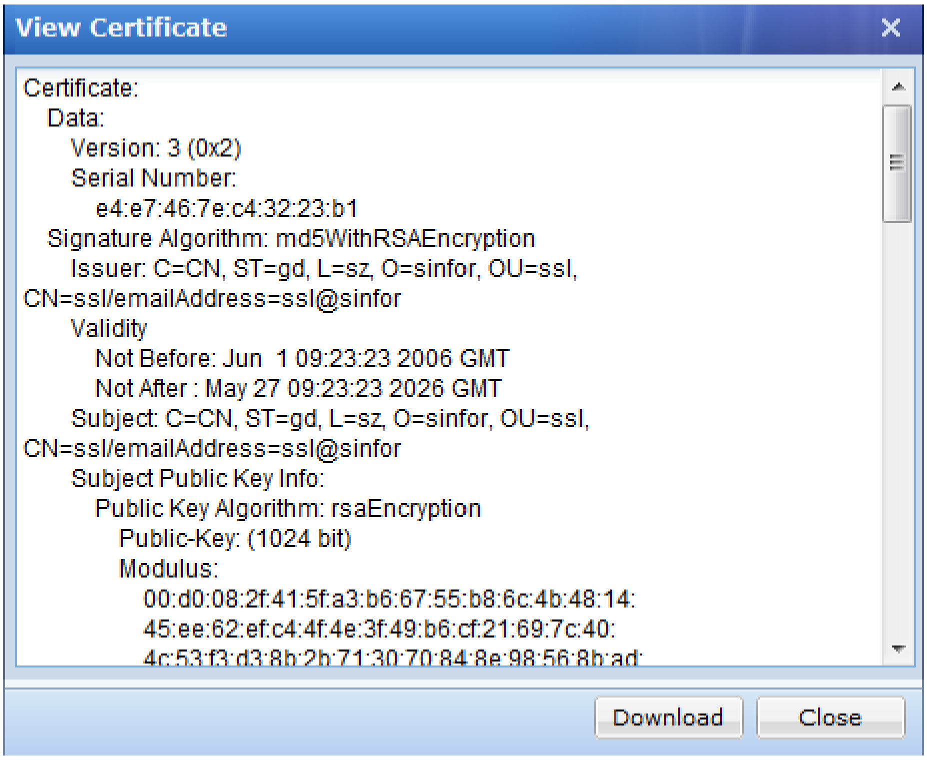
□	Name	Model	Status
□	USB Key V2	Vid_096e&Pid_0302	⊘
☑	epass3000gm	Vid_096e&Pid_0309	✓

The above figure shows the contents on the **Certificate/USB Key Based Authentication** page when the current CA is **external CA**.

If the current CA is **local CA**, the**ca Options** and **Online Certificate Status Protocol (OCSP**) part will be absent.

Local CA (RSA Encryption Standard Based)

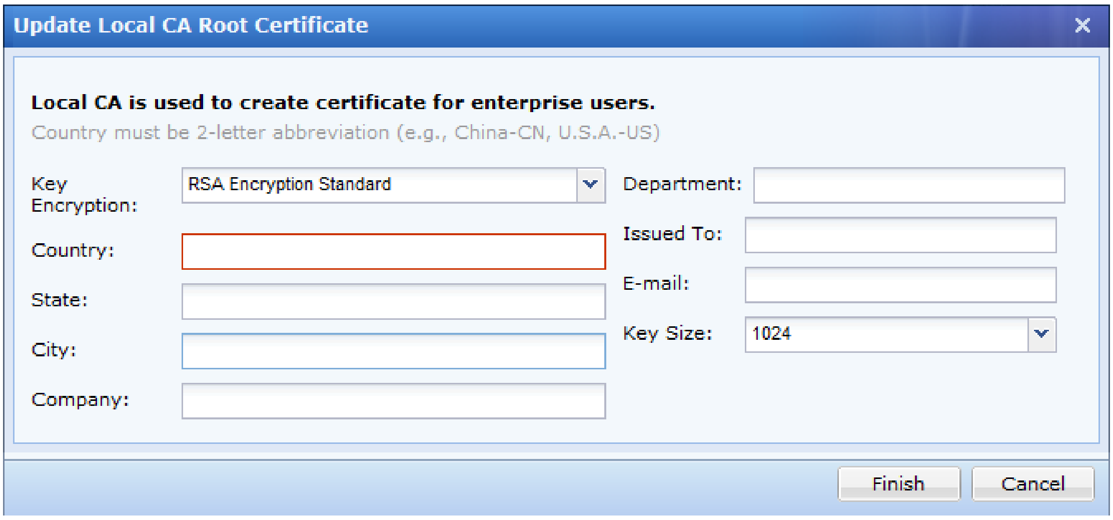
1. Under **CA Type** section, click **View** to see the certificate information, as shown in the figure below:



View Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            e4:e7:46:7e:c4:32:23:b1
    Signature Algorithm: md5WithRSAEncryption
        Issuer: C=CN, ST=gd, L=sz, O=sinfor, OU=ssl,
CN=ssl/emailAddress=ssl@sinfor
        Validity
            Not Before: Jun  1 09:23:23 2006 GMT
            Not After : May 27 09:23:23 2026 GMT
        Subject: C=CN, ST=gd, L=sz, O=sinfor, OU=ssl,
CN=ssl/emailAddress=ssl@sinfor
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:d0:08:2f:41:5f:a3:b6:67:55:b8:6c:4b:48:14:
                    45:ee:62:ef:c4:4f:4e:3f:49:b6:cf:21:69:7c:40:
                    4c:53:f3:d3:8b:2b:71:30:70:84:8e:98:56:8b:ad:
```

2. Click **Update** to entry create certificate for enterprise users, as shown in the figure below:



Update Local CA Root Certificate

Local CA is used to create certificate for enterprise users.

Country must be 2-letter abbreviation (e.g., China-CN, U.S.A.-US)

Key Encryption: RSA Encryption Standard

Country:

State:

City:

Company:

Department:

Issued To:

E-mail:

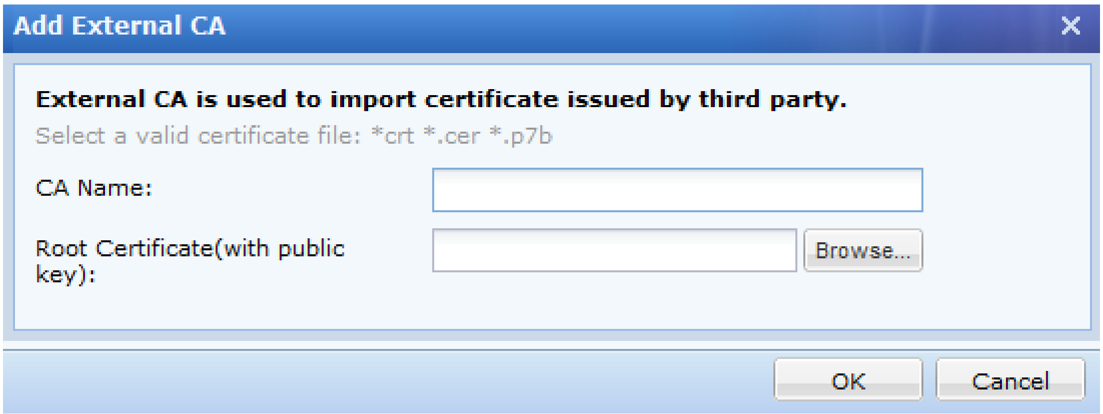
Key Size: 1024

Select **Key Encryption** option, available to choose for RSA Encryption Standard (Standard International Encryption)& SM2 Encryption Standard (Standard China Encryption).RMA password range able to select 1024/2048/4096, SM2 password range only can select 256.

- Country must be a two-letter abbreviation of country, for example, CN indicates China.

External CA

1. Click the **Add** to entry External CA, as shown in the figure below:



Add External CA

External CA is used to import certificate issued by third party.

Select a valid certificate file: *crt *.cer *.p7b

CA Name:

Root Certificate(with public key):

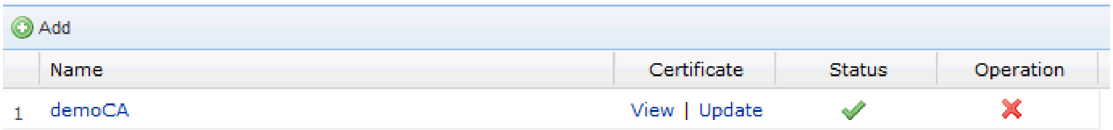
Import **External CA**and configure CA name, as shown in the figure below:

2. Browse and select a CA root certificate from the computer. Certificate file extension should be .crt, .cer or .p7b.

3. If necessary, browse and select the corresponding certificate to update the device certificate. This certificate should be a certificate that has a private key and the certificate file should be in format of .crt, .cer, .p12 or .pfx.

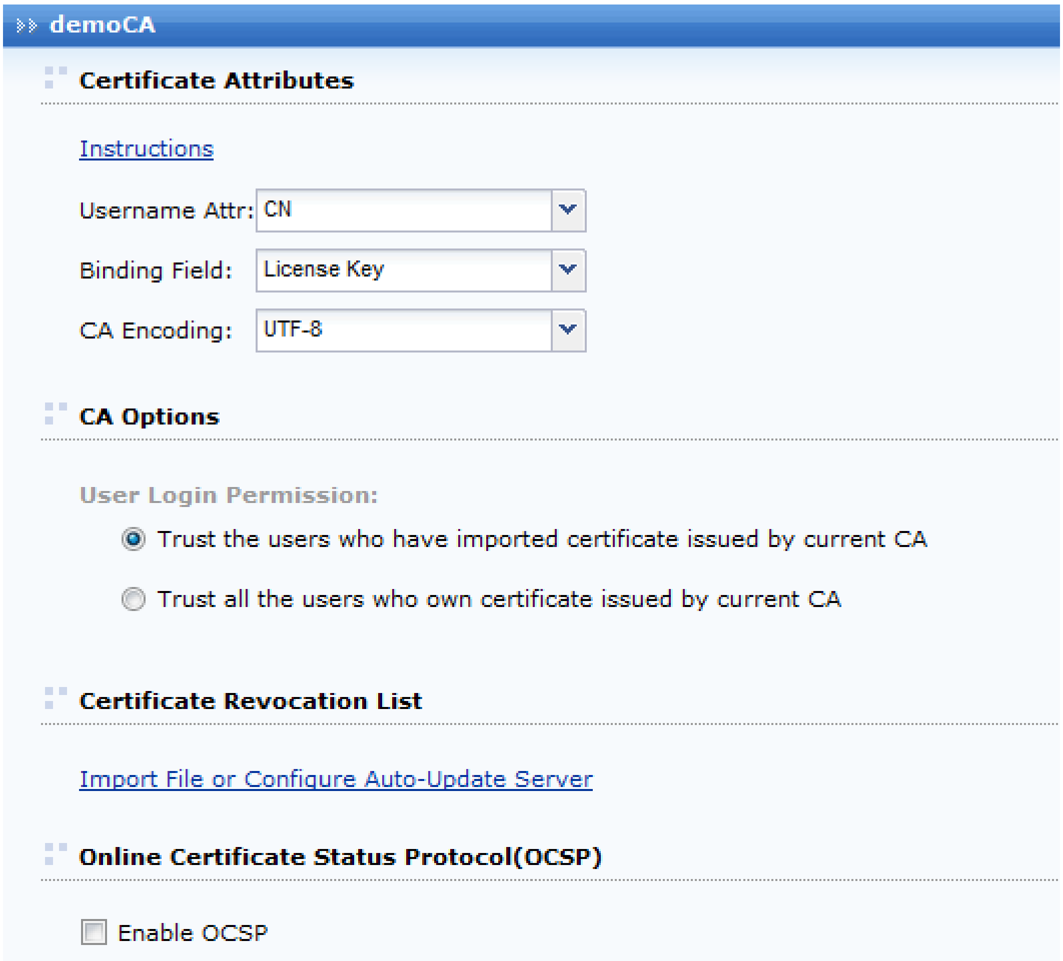
   Certificate Password should be the password of the device certificate. The password is required only when the certificate file is in format of .p12 or .pfx.

4. Click the **Finish** button to return to **Certificate/USB Key Based Authentication** page, and the CA types **External CA**, as shown in the figure below:



	Name	Certificate	Status	Operation
1	demoCA	View | Update	✓	✗

5. Click the **External CA,** shown in the figure below:



demoCA

Certificate Attributes

Instructions

Username Attr: CN

Binding Field: License Key

CA Encoding: UTF-8

CA Options

User Login Permission:

● Trust the users who have imported certificate issued by current CA

○ Trust all the users who own certificate issued by current CA

Certificate Revocation List

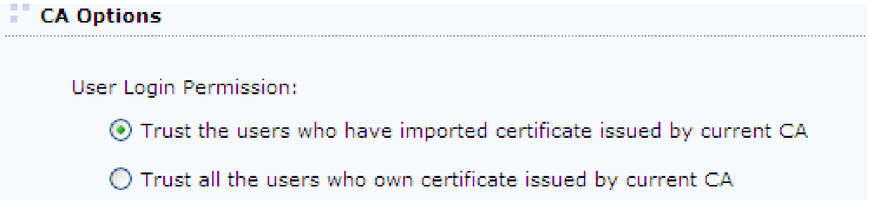
Import File or Configure Auto-Update Server

Online Certificate Status Protocol(OCSP)

□ Enable OCSP

- **Username Attr**: This is a certificate issued by the CA, store the user name field; the user name is display in the main interface on the client, supported CN, Email and OID.
- **Binding Field**: when you import the CA certificate issued to the local user certificate field bound.
    - **License Key**: After the certificate expires, CA will be re-signed certificate, because the new certificate serial number has been changed to be in the local user management, re-import the new certificate
    - **DN**:Compared certificate serial number, you can avoid the need to re-import the user certificate. When you select this option, you must ensure that the certificate is different DN name only.
    - **OID**:Similar as DN, usually stored user names and etc. Need to fill uniquely identify the user's OID property.

6. Configure CA Option. CA options determine 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.



CA Options

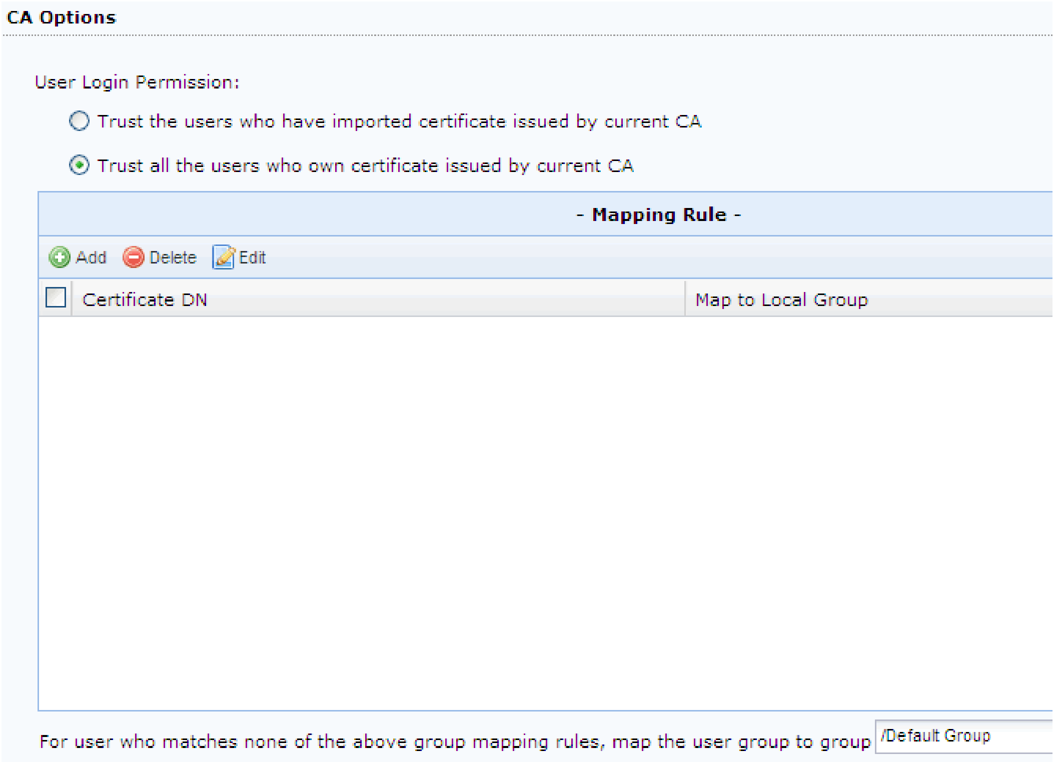
User Login Permission:

● Trust the users who have imported certificate issued by current CA

○ Trust all the users who own certificate issued by current CA

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.



CA Options

User Login Permission:

○ Trust the users who have imported certificate issued by current CA

● Trust all the users who own certificate issued by current CA

- Mapping Rule -

□	Certificate DN	Map to Local Group

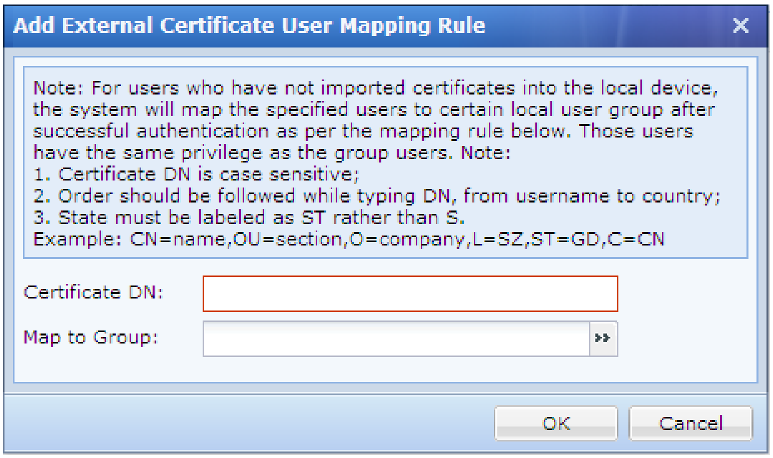
For user who matches none of the above group mapping rules, map the user group to group /Default Group

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:



Add External Certificate User Mapping Rule

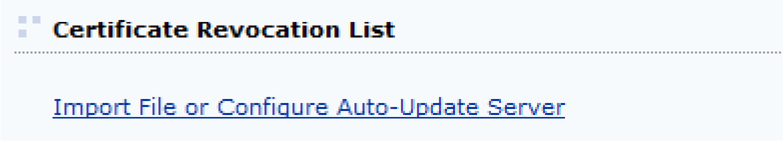
Note: For users who have not imported certificates into the local device, the system will map the specified users to certain local user group after successful authentication as per the mapping rule below. Those users have the same privilege as the group users. Note:
1. Certificate DN is case sensitive;
2. Order should be followed while typing DN, from username to country;
3. State must be labeled as ST rather than S.
Example: CN=name,OU=section,O=company,L=SZ,ST=GD,C=CN

Certificate DN:

Map to Group:

- **Certificate DN:** Configures DN of certificate, whichcan 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 who matches none of the above group mapping rules, map the user group to group:** Configures the local group to which the certificate users will be mapped automatically if they match none of the mapping rules.

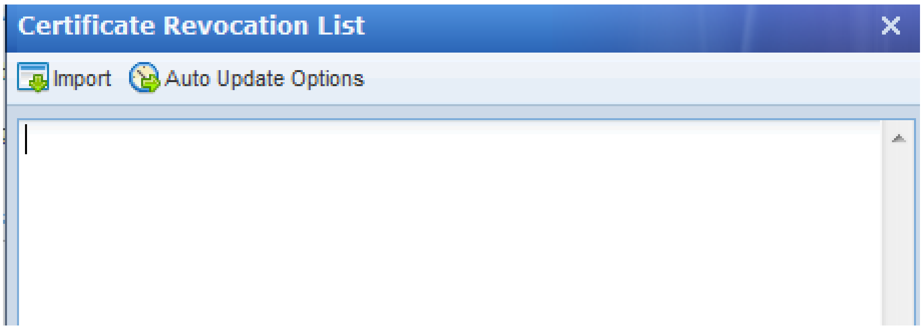
7. Configure certificate revocation list (CRL).This part includes CRL update options, as shown in the figure below:



Certificate Revocation List

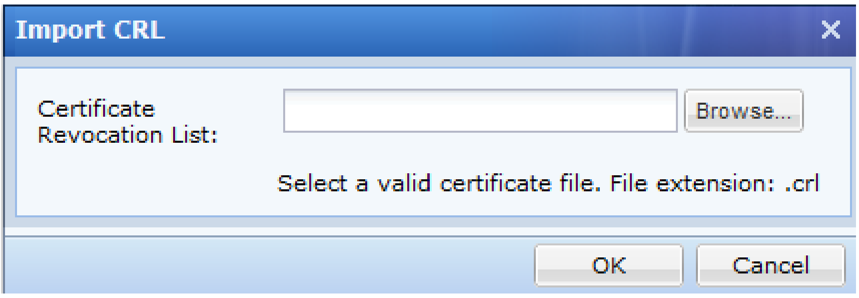
To ignore the expiry date of the certificate revocation lists, select **Ignore expiry date of CRL** option.

To update certificate revocation list manually, click the **Import File or Configure Auto-Update Server** and enter the **Certificate Revocation List** page (as shown in the figure below). Browse and upload the certificate file with the file extension .crl.



Certificate Revocation List

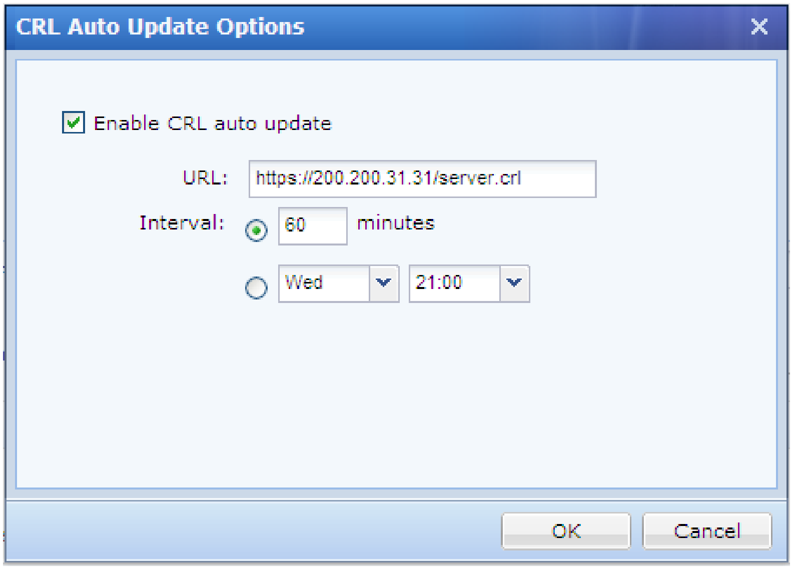
Click **Import** to entry **Import CRL** page. shown in the figure below.



Certificate Revocation List:

Select a valid certificate file. File extension: .crl

To have the CRL update automatically and regularly, clickthe **Auto-Update Options**linkand configure the fields on the **Auto Update Options** page, as shown in the figure below:



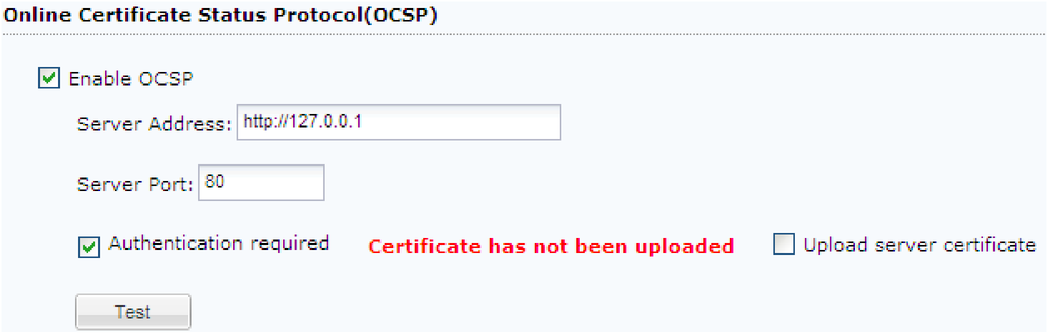
☑ Enable CRL auto update

URL: https://200.200.31.31/server.crl

Interval: ● 60 minutes

○ Wed 21:00

8. 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:



Online Certificate Status Protocol(OCSP)

☑ Enable OCSP

Server Address: http://127.0.0.1

Server Port: 80

☑ Authentication required Certificate has not been uploaded □ Upload server certificate

The contents under **Online Certificate Status Protocol(OCSP)** are as follows:

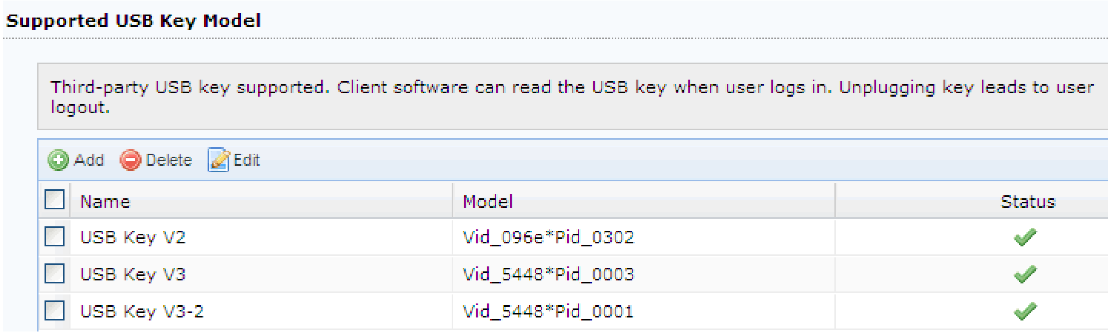
- **Enable OCSP:** Select this option and OCSP will be enabled and related options will appear.
- **Server Address, Server Port:** Configure the address and port of OCSP server that provides OCSP service.
- **Authentication required:** Select this option and the OCSP server will verify identity of the Sangfor device.

- **Upload server certificate:** Upload the device certificate that is trusted by the OCSPserver, so that the Sangfor device can use this certificate to go through identity verification and check validity of end user's certificate.
- **Test:** 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:

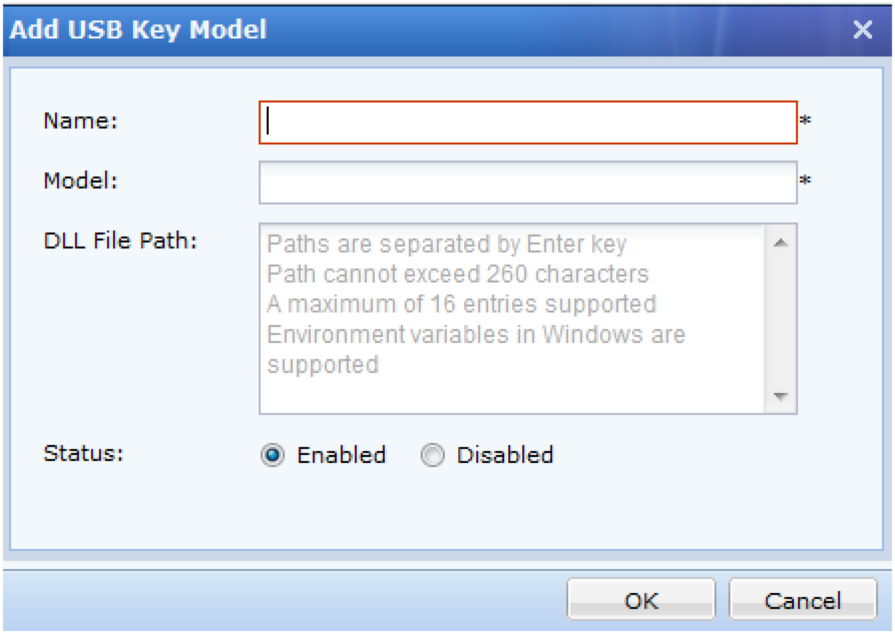


Supported USB Key Model

Third-party USB key supported. Client software can read the USB key when user logs in. Unplugging key leads to user logout.

□	Name	Model	Status
□	USB Key V2	Vid_096e*Pid_0302	✓
□	USB Key V3	Vid_5448*Pid_0003	✓
□	USB Key V3-2	Vid_5448*Pid_0001	✓

To add a new USB key model, click **Add** toenter **Key Settings** page, as shown below:



Add USB Key Model

Name: *

Model: *

DLL File Path: Paths are separated by Enter key
Path cannot exceed 260 characters
A maximum of 16 entries supported
Environment variables in Windows are supported

Status: ● Enabled ○ Disabled

The following are the contents included on **USB Key Settings** page:

- **Name:** Configures name of this USB key model.

- **Model:** Configures the model of USB key that supports automatic logout while end user unplugs the USB key.
- **DLL file path:** When you add a third party to support the Chinese National KEY password encryption algorithm standard SM2 certification, you need to specify the KEY driver file encryption function interface provided SM2
- **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**.

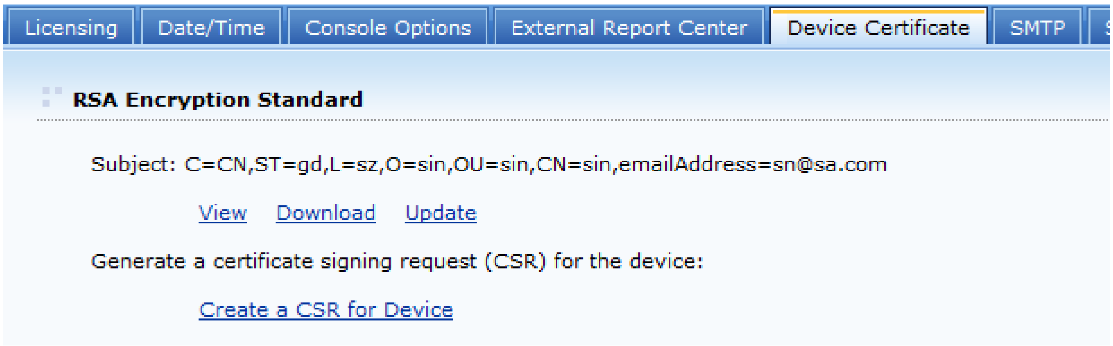
Scenario 17: Using External CA Root Certificate to Generate Device Certificate

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 into the SSL VPN if they own certificates issued by that external CA.

To achieve the expected purpose:

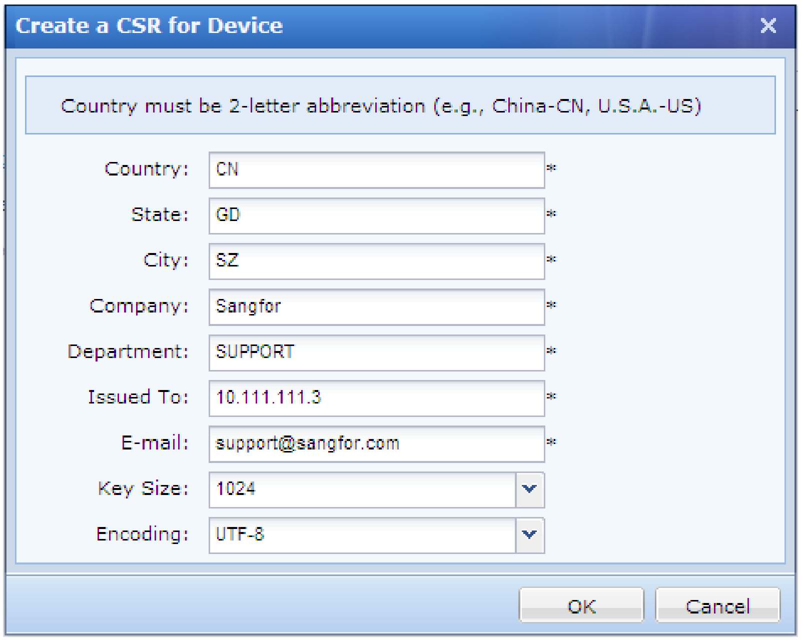
1. Navigate to **SSL VPN**>**System**>**Device Certificate**, as shown in the figure below:



Subject: C=CN,ST=gd,L=sz,O=sin,OU=sin,CN=sin,emailAddress=sn@sa.com

Generate a certificate signing request (CSR) for the device:

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:



Country must be 2-letter abbreviation (e.g., China-CN, U.S.A.-US)

Country: CN *

State: GD *

City: SZ *

Company: Sangfor *

Department: SUPPORT *

Issued To: 10.111.111.3 *

E-mail: support@sangfor.com *

Key Size: 1024

Encoding: UTF-8

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**, 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.

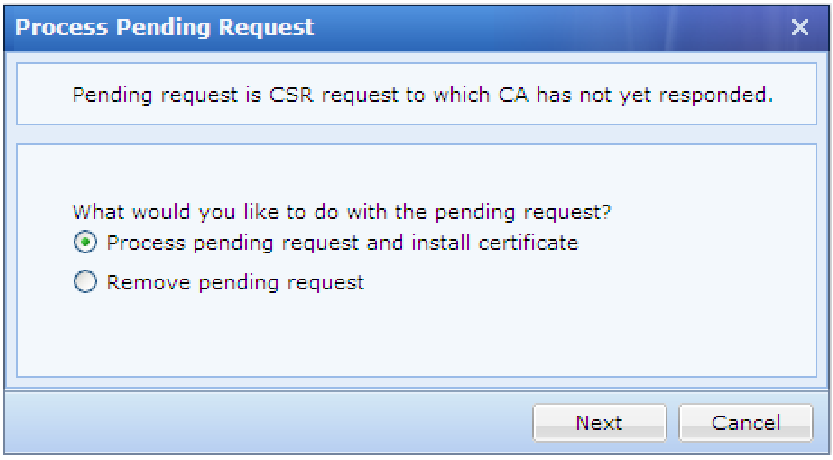
4. Click the **OK** button to save the settings.
5. Once the CSR is generated, click **Download** to download the request or copy the above request contents into a text file. The contents in the .csr file are as shown below:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBODCCATkCAQAwgY8xCzAJBgNVBAYTAkNOMQswCQYDVQQIEwJHRDELMAkGA1UE
BxMCU1oxEDAOBgNVBAoTB1NBTkdGT1IxEDAOBgNVBAsTB1NVUFBPU1QxGzAZBgNV
BAMTEnd3dy5zYW5nZm9yLmNvbS5jbjElMCMGCSqGSIb3DQEJARYWc3VwcG9ydEBz
YW5nZm9yLmNvbS5jbjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAxLfml4gT
VGib8SuYYvy4txDzSN6DrGI031kAZRHRw77tEs8LbEu1HozLwCSfZDVgk3fue0Be
K3dkkx7nsZ+QMZ/0iCOLnoJuzH+SXwsb1OSN0u3z633wYlh1qS2n04nB51kKPc9I
rcohT9sDXHEsf8NZJeh+6u9y2xnTCdjfNxECAwEAAaAAMA0GCSqGSIb3DQEBBQUA
A4GBAChre1tw+81CkkB6QCKaX71Wih88K0QEUntW5nZCjW+rlTBwKzZAl3oxAN8I
BX99sSiDKu5Hruh3TN4jk5R+VbCtHW7rPkdJPK0df26Sv1REVuw6p7u1xr/qVJyV
0HCYdmjA8e0mVZMLVYu9mOBjMZe1Udfxaef82xr9ehKpM+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**>**System**>**Device Certificate** againand click the **Process Pending Request** link to process the pending request, as shown below:



Process Pending Request

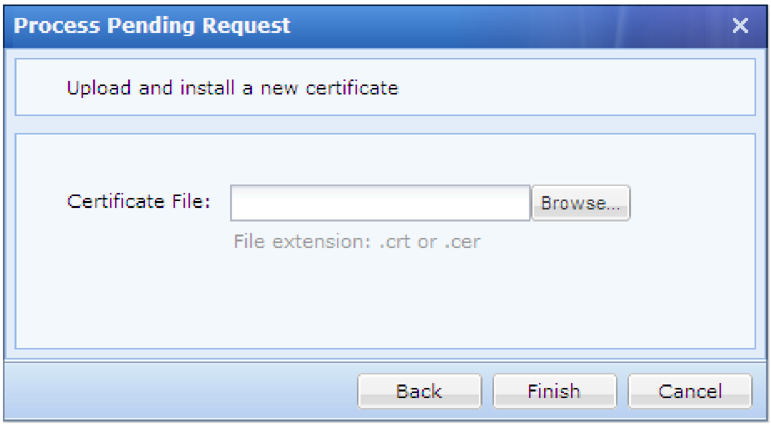
Pending request is CSR request to which CA has not yet responded.

What would you like to do with the pending request?

● Process pending request and install certificate

○ Remove pending request

9. Select the **Process pending request and install certificate** option and click the **Next** button to proceed, as shown below:



Process Pending Request

Upload and install a new certificate

Certificate File:

File extension: .crt or .cer

10. Upload the device certificate you have received from the external CA and click the **Finish** button.

Scenario 18: 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:

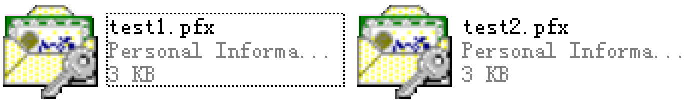
To assign different resources to the two users automatically after they log in to the SSL VPN successfully, but the two users need not be imported into the Sangfor device.

Analysis and solution:

Firstly, we need to configure external CA and use the CA to generate certificate, so that users canuse 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 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 Groupsectioning Chapter 4). Primary authentication **Certificate/USB key** need not be selected for both users**ou1** and**ou2**.
3. Generate certificates for the trousers, **test1** and **test2**.

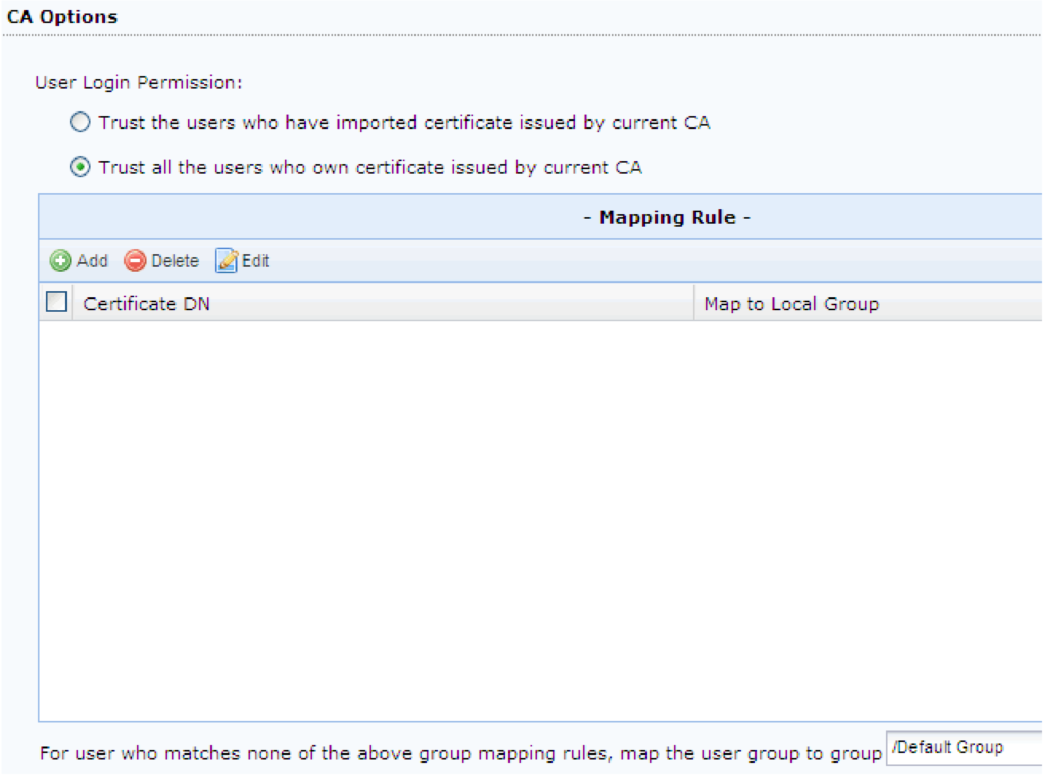


Check the subjects of the two certificates, as shown below.

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**, as shown in the figure below:



CA Options

User Login Permission:

○ Trust the users who have imported certificate issued by current CA

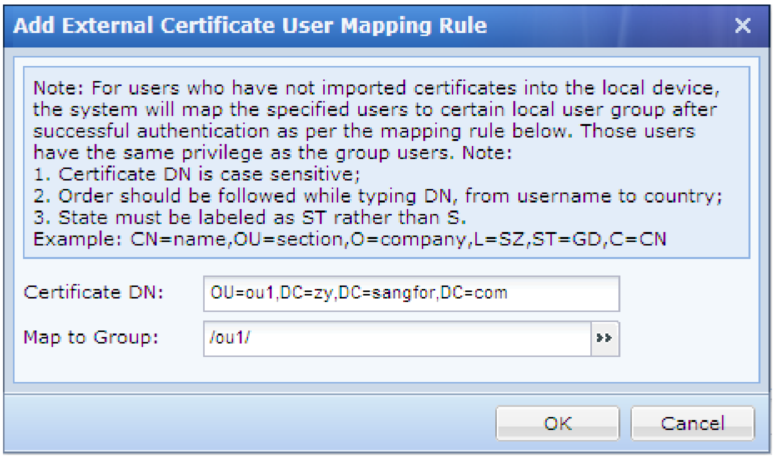
● Trust all the users who own certificate issued by current CA

- Mapping Rule -

□	Certificate DN	Map to Local Group

For user who matches none of the above group mapping rules, map the user group to group /Default Group

5. 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:

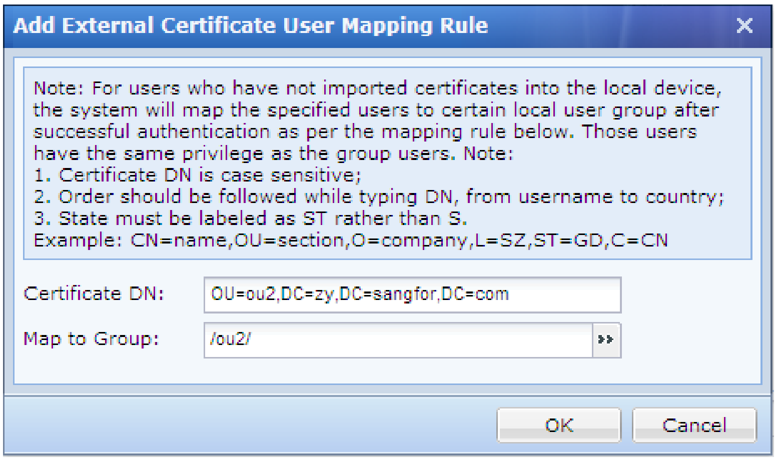


Add External Certificate User Mapping Rule

Note: For users who have not imported certificates into the local device, the system will map the specified users to certain local user group after successful authentication as per the mapping rule below. Those users have the same privilege as the group users. Note:
1. Certificate DN is case sensitive;
2. Order should be followed while typing DN, from username to country;
3. State must be labeled as ST rather than S.
Example: CN=name,OU=section,O=company,L=SZ,ST=GD,C=CN

Certificate DN: OU=ou1,DC=zy,DC=sangfor,DC=com

Map to Group: /ou1/



Note: For users who have not imported certificates into the local device, the system will map the specified users to certain local user group after successful authentication as per the mapping rule below. Those users have the same privilege as the group users. Note:
1. Certificate DN is case sensitive;
2. Order should be followed while typing DN, from username to country;
3. State must be labeled as ST rather than S.
Example: CN=name,OU=section,O=company,L=SZ,ST=GD,C=CN

Certificate DN: OU=ou2,DC=zy,DC=sangfor,DC=com

Map to Group: /ou2/

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 sectioning Chapter 4).

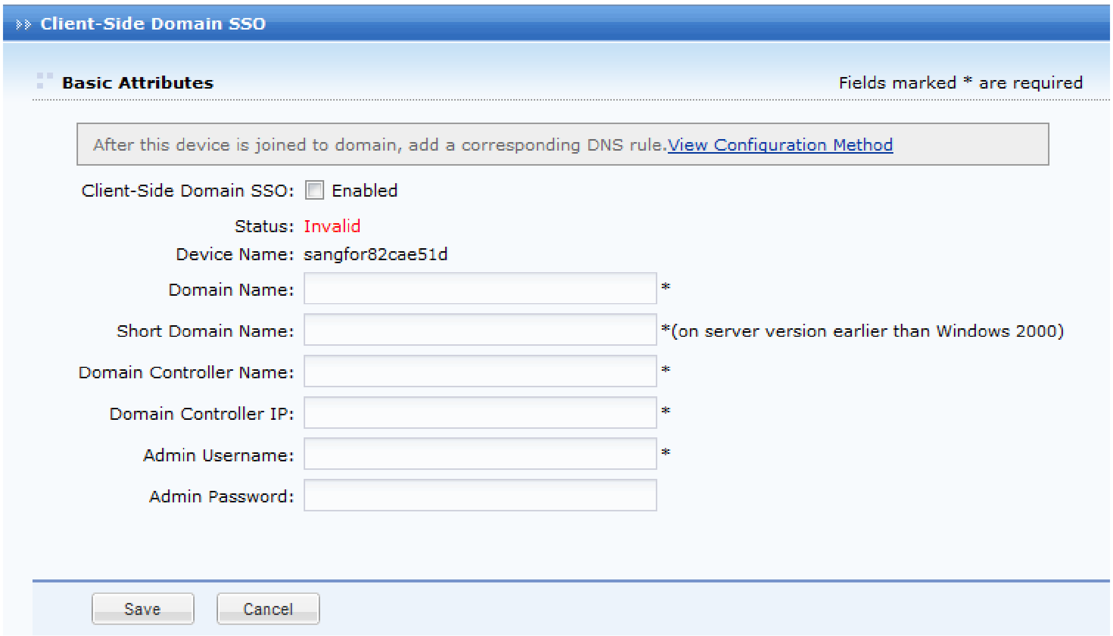
7. Save the setting and then click the **Apply** button when configuration is completed.

   After logging in to the SSL VPN, what **test1** and **test2** will see on the **Resource** page will be the corresponding associated resource.

Client-Side Domain SSO

Case domain single sign-on authentication for solving the client PC has logged a domain, using C / S Log customers no longer need to enter a user name and password to log end SSL VPN, domain authentication can be done automatically, successful login SSL. Domain single sign-on authentication supports only way to log the client does not support the web login form.

Navigate SSLVPN > Authentication > Client-Side Domain SSO



Client-Side Domain SSO

Basic Attributes

Fields marked * are required

After this device is joined to domain, add a corresponding DNS rule.View Configuration Method

Client-Side Domain SSO: □ Enabled

Status: Invalid

Device Name: sangfor82cae51d

Domain Name: *

Short Domain Name: *(on server version earlier than Windows 2000)

Domain Controller Name: *

Domain Controller IP: *

Admin Username: *

Admin Password:

- **Domain Name**: Used to set the Windows domain name
- **Short Domain Name**: Used to set the short name of Windows domain
- **Domain Controller Name**: Used to set Windows Controller Name
- **Domain Controller IP**: Used to set Windows domain controller IP address
- **Admin Username**: Used to set for Windows domain Admin ID
- **Admin Password**: set for Windows domain ID password

Secondary Authentication Methods

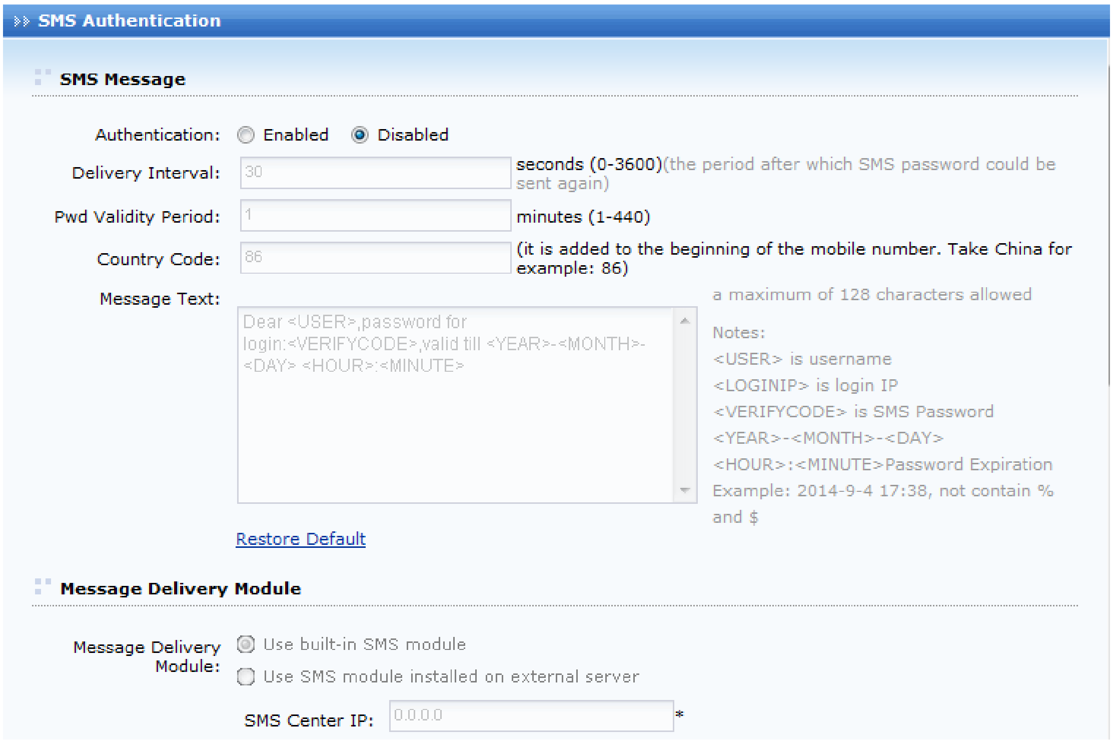
There are three secondary authentication methods, namely, **SMS** authentication, **Dynamic Token** based authentication and **Hardware ID** based authentication.

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 toad 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 **Configure** button following**SMS** and the **SMS Authentication** page appears, as shown below:



SMS Authentication

SMS Message

Authentication: ○ Enabled ● Disabled

Delivery Interval: 30 seconds (0-3600)(the period after which SMS password could be sent again)

Pwd Validity Period: 1 minutes (1-440)

Country Code: 86 (it is added to the beginning of the mobile number. Take China for example: 86)

Message Text: Dear <USER>,password for login:<VERIFYCODE>,valid till <YEAR>-<MONTH>-<DAY> <HOUR>:<MINUTE>

a maximum of 128 characters allowed

Notes:
<USER> is username
<LOGINIP> is login IP
<VERIFYCODE> is SMS Password
<YEAR>-<MONTH>-<DAY>
<HOUR>:<MINUTE>Password Expiration
Example: 2014-9-4 17:38, not contain % and $

Restore Default

Message Delivery Module

Message Delivery Module: ● Use built-in SMS module ○ Use SMS module installed on external server

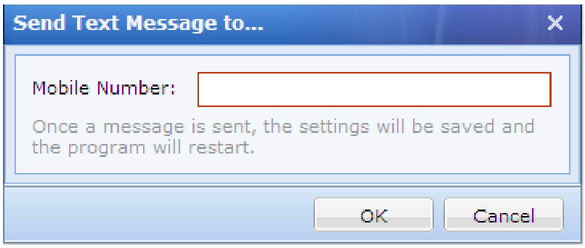
SMS Center IP: 0.0.0.0 *

In case that the SMS license is invalid or has not been activated, tips show up under the subtitle **SMS Message**, saying, and “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**.
- **Delivery Interval:** Password will reset after the seconds.
- **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.
- **Country Code:** Insert valid country code.
- **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.
- **Message Delivery Parameters:** Configures the ways of delivering SMS messages, using **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.
- **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 pops up asking for mobile number, as shown in the figure below:


Send Text Message to...

Mobile Number:

Once a message is sent, the settings will be saved and the program will restart.

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:

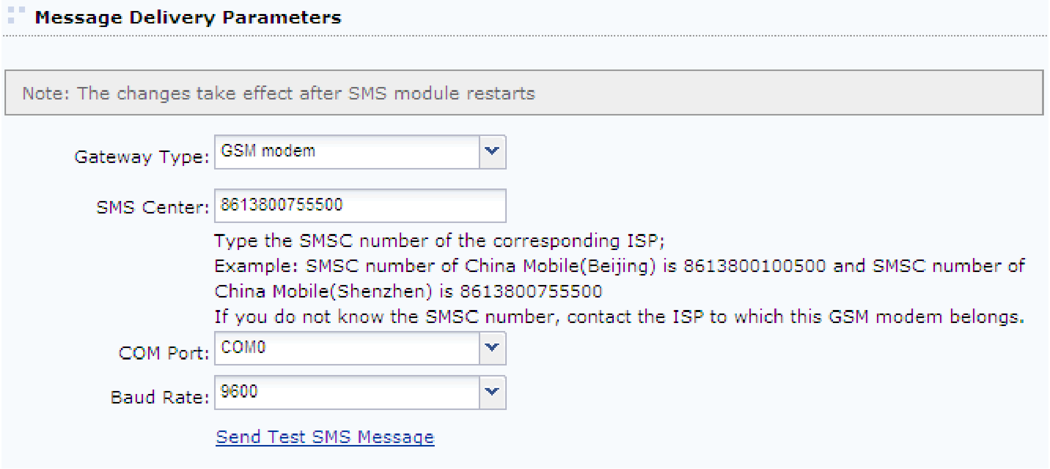
1. Insert the SIM card of a cellular phone into the GSM modem.
2. Use the serial cable (one end is male connector and the other end is female connector; attachment of Sangfor device when product is delivered) to connect the GSM modem to the **CONSOLE** interface on the rear panel of the Sangfor device. 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:



Message Delivery Parameters

Note: The changes take effect after SMS module restarts

Gateway Type: GSM modem

SMS Center: 8613800755500

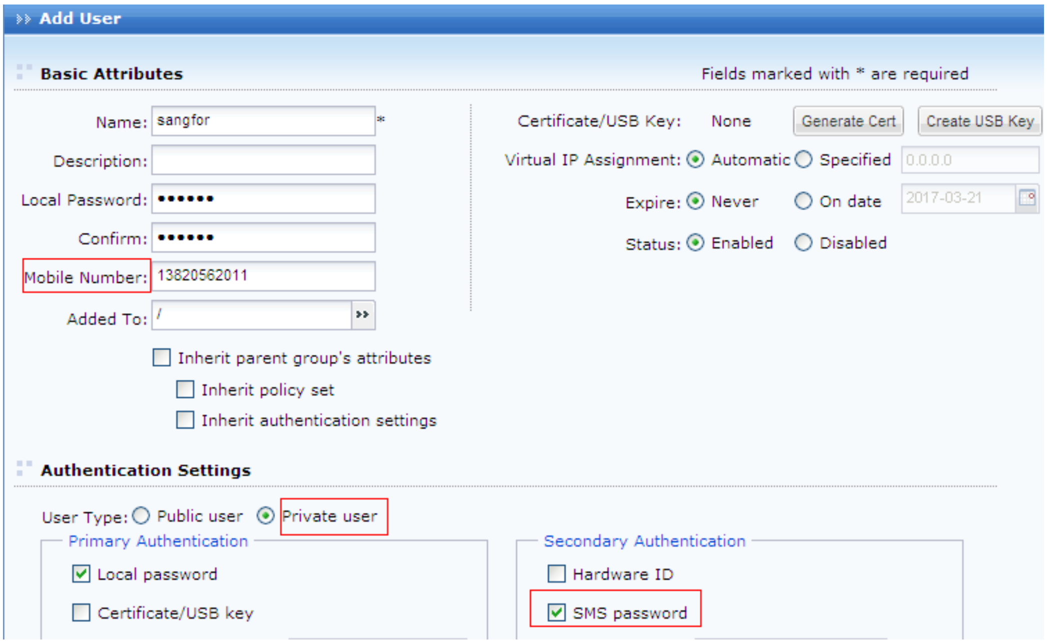
Type the SMSC number of the corresponding ISP;
Example: SMSC number of China Mobile(Beijing) is 8613800100500 and SMSC number of China Mobile(Shenzhen) is 8613800755500
If you do not know the SMSC number, contact the ISP to which this GSM modem belongs.

COM Port: COM0

Baud Rate: 9600

Send Test SMS Message

8. 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:



Add User

Basic Attributes

Fields marked with * are required

Name: sangfor *

Description:

Local Password: ••••••

Confirm: ••••••

Mobile Number: 13820562011

Added To: /

□ Inherit parent group's attributes

□ Inherit policy set

□ Inherit authentication settings

Certificate/USB Key: None

Virtual IP Assignment: ● Automatic ○ Specified 0.0.0.0

Expire: ● Never ○ On date 2017-03-21

Status: ● Enabled ○ Disabled

Authentication Settings

User Type: ○ Public user ● Private user

Primary Authentication

☑ Local password

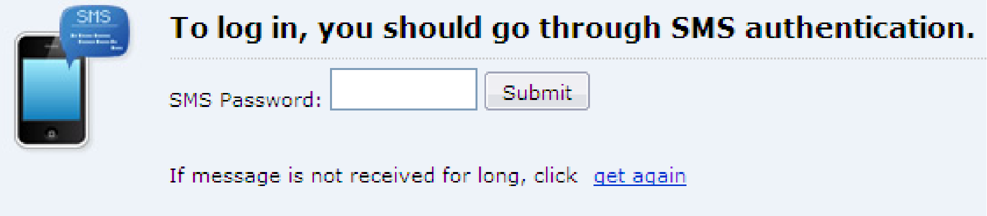
□ Certificate/USB key

Secondary Authentication

□ Hardware ID

☑ SMS password

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:



To log in, you should go through SMS authentication.

SMS Password: Submit

If message is not received for long, click get again

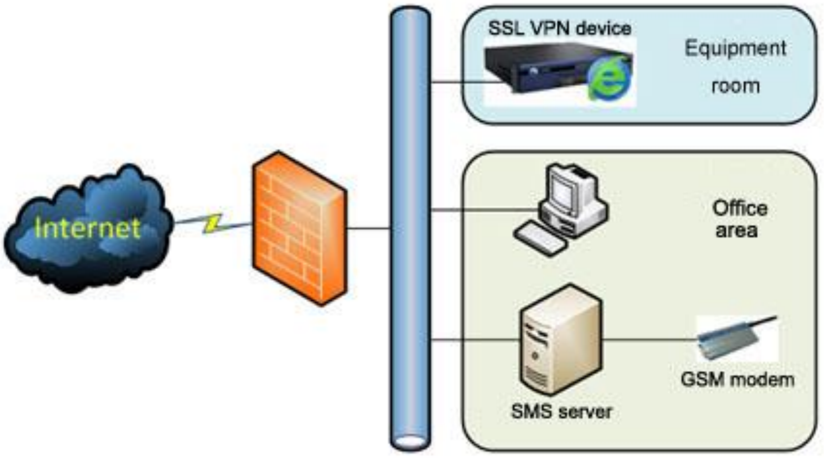
10. Enter the received SMS password, and click the **Submit** button. If user fails to receive the text message for a long time, he/she can click **get again** to get a new SMS password.

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:



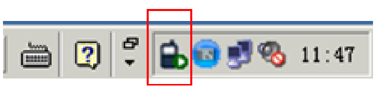
1. Insert the SIM card of a cellular phone into the GSM modem.

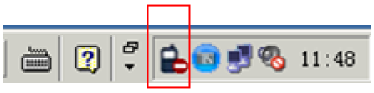
2. Use the serial cable(one end is male connector and the other end is female connector; attachment of Sangfor device when product is delivered) to connect the GSM modem to the **COM** port of SMS server. Please screw the plug/jack in until they are tightly attached.

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**.

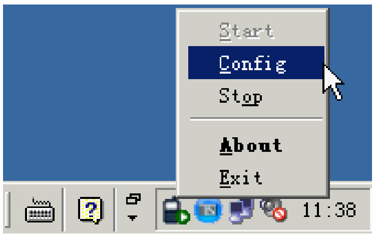
   For the running status of SMS service, see the SMS service icon on the task bar, as shown in the two figures below. The figure on the left shows normal running status, while the figure on the right shows service error.





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.

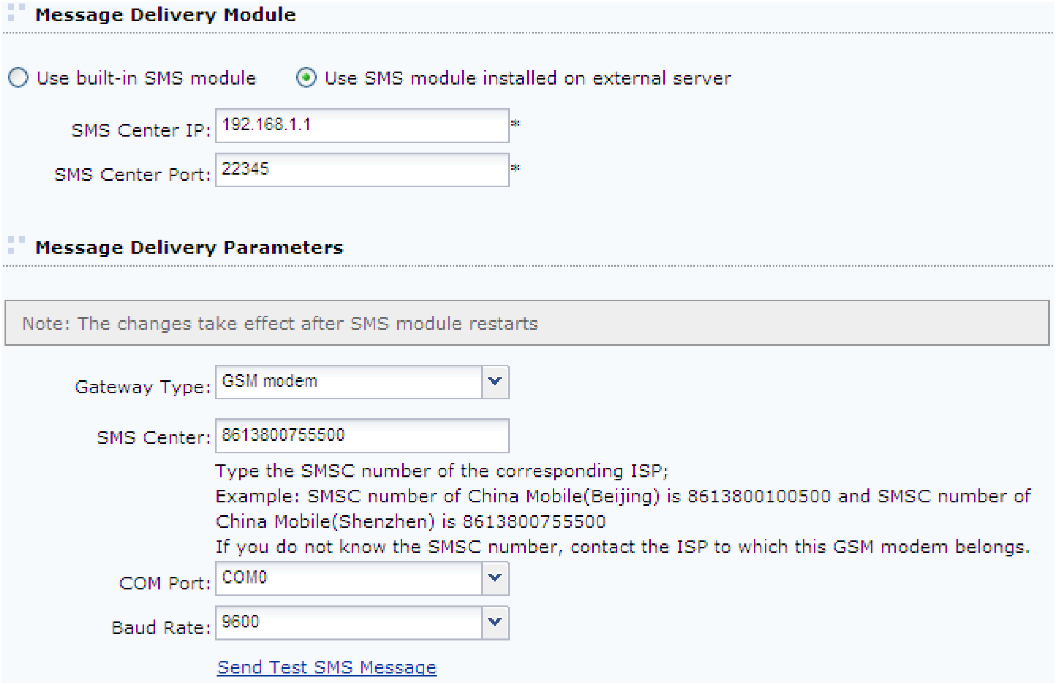


What needs to be configured for the SMS service is the listening port (TCP port). Make sure the configured listening port is not providing other services. To check if port conflict exists, use the command **netstat –na** to check all other listening ports used by this server.

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 **SSLVPN**>**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:



Message Delivery Module

○ Use built-in SMS module ● Use SMS module installed on external server

SMS Center IP: 192.168.1.1 *

SMS Center Port: 22345 *

Message Delivery Parameters

Note: The changes take effect after SMS module restarts

Gateway Type: GSM modem

SMS Center: 8613800755500

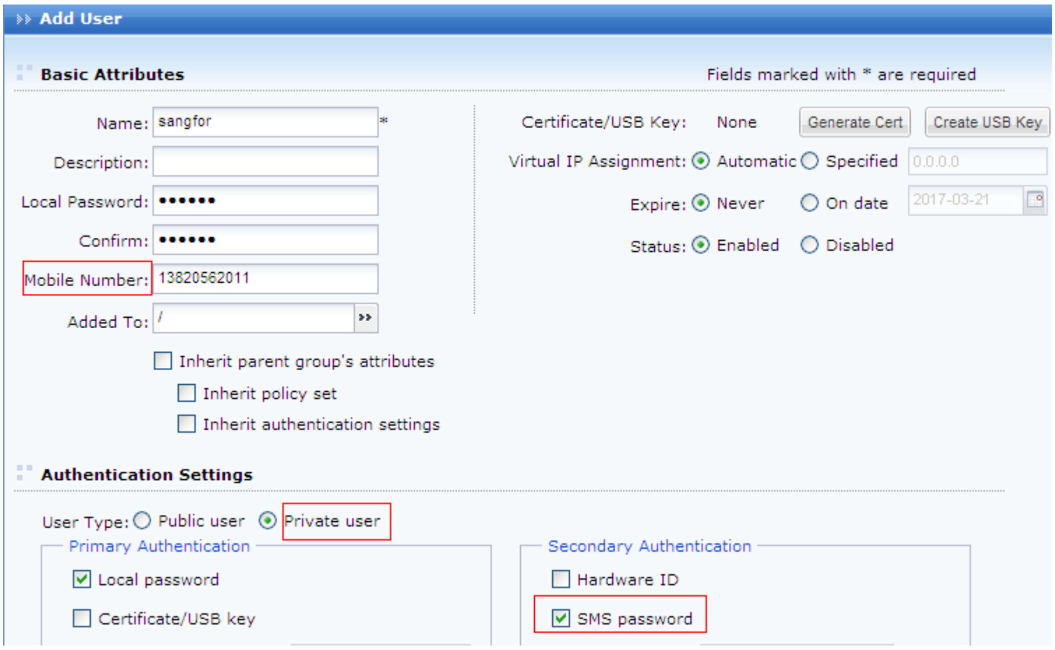
Type the SMSC number of the corresponding ISP;
Example: SMSC number of China Mobile(Beijing) is 8613800100500 and SMSC number of China Mobile(Shenzhen) is 8613800755500
If you do not know the SMSC number, contact the ISP to which this GSM modem belongs.

COM Port: COM0

Baud Rate: 9600

Send Test SMS Message

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:



Add User

Basic Attributes Fields marked with * are required

Name: sangfor *

Description:

Local Password: ••••••

Confirm: ••••••

Mobile Number: 13820562011

Added To: /

□ Inherit parent group's attributes
□ Inherit policy set
□ Inherit authentication settings

Certificate/USB Key: None

Virtual IP Assignment: ● Automatic ○ Specified 0.0.0.0

Expire: ● Never ○ On date 2017-03-21

Status: ● Enabled ○ Disabled

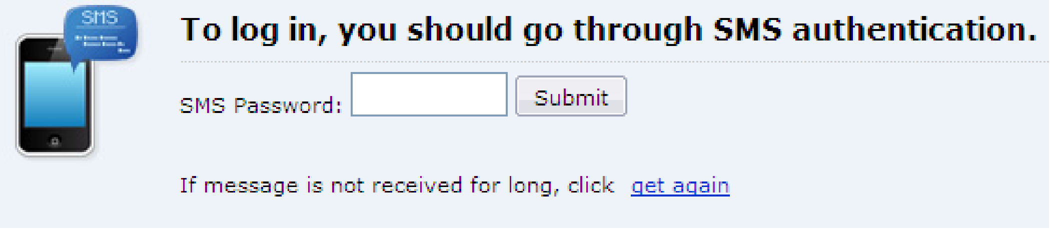
Authentication Settings

User Type: ○ Public user ● Private user

Primary Authentication
☑ Local password
□ Certificate/USB key

Secondary Authentication
□ Hardware ID
☑ SMS password

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:


To log in, you should go through SMS authentication.

SMS Password: Submit

If message is not received for long, click get again

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

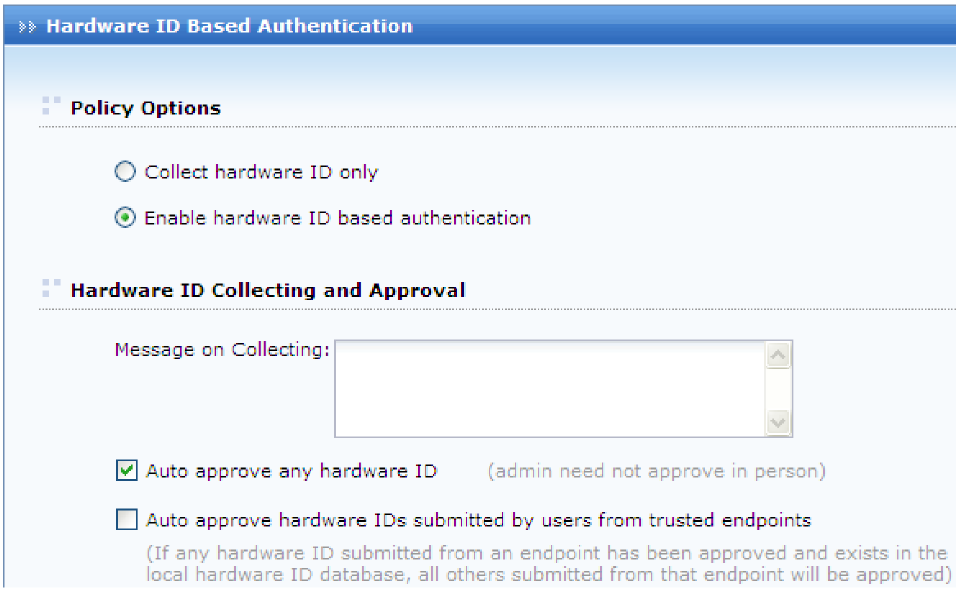
If the enterprise network is already deployed with SMS gateway of ISP, such as China Mobile, China Unicom, no other facility is needed except the Sangfor device. Configure the following:

- **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.

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 **Configure** button following **Hardware ID** and the **Hardware ID Based Authentication** page appears, as shown in the figure below:



Hardware ID Based Authentication

Policy Options

○ Collect hardware ID only

● Enable hardware ID based authentication

Hardware ID Collecting and Approval

Message on Collecting:

☑ Auto approve any hardware ID (admin need not approve in person)

□ Auto approve hardware IDs submitted by users from trusted endpoints

(If any hardware ID submitted from an endpoint has been approved and exists in the local hardware ID database, all others submitted from that endpoint will be approved)

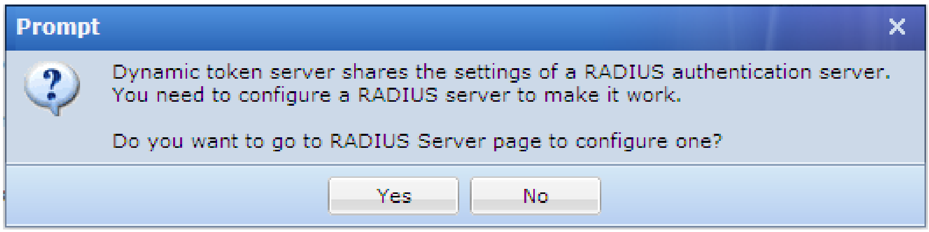
The following are the contents included on **Hardware ID Based Authentication** page:

- **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.
- **Auto approve hardware IDs submitted by users from trusted endpoints:** 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 **Configure** button following **Dynamic Token** and the following prompt appears:



Prompt

Dynamic token server shares the settings of a RADIUS authentication server. You need to configure a RADIUS server to make it work.

Do you want to go to RADIUS Server page to configure one?

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 sectioning Chapter 4.

Other Authentication Options

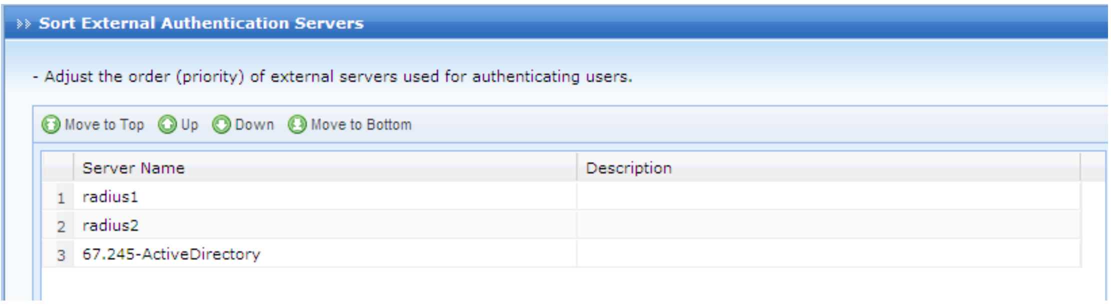
This section includes configurations of **Priority of LDAP/RADIUS Servers, Password Security Options** related to password and brute-force login prevention, and **Anonymous Login** related settings.

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 **Configure** button following **Priority of LDAP/RADIUS Servers** and the **Sort External Authentication Servers** page appears, as shown in the figure below:



Sort External Authentication Servers

- Adjust the order (priority) of external servers used for authenticating users.

	Server Name	Description
1	radius1	
2	radius2	
3	67.245-ActiveDirectory	

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.

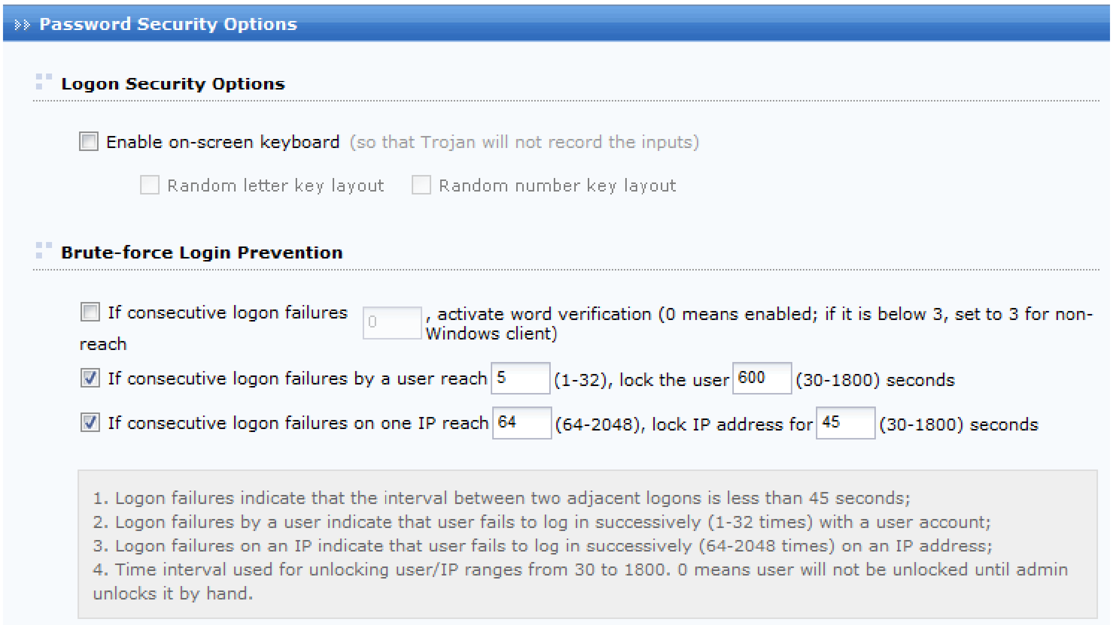
To adjust order of an external authentication server, select the server and click **Move to Top**, **Move Up**, **Move Down** or **Move to Bottom**.

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 **Configure** button following **Password Security Options** and the **Password Security Options** page appears, as shown in the figure below:



Password Security Options

Logon Security Options

□ Enable on-screen keyboard (so that Trojan will not record the inputs)

□ Random letter key layout □ Random number key layout

Brute-force Login Prevention

□ If consecutive logon failures reach 0 , activate word verification (0 means enabled; if it is below 3, set to 3 for non-Windows client)

☑ If consecutive logon failures by a user reach 5 (1-32), lock the user 600 (30-1800) seconds

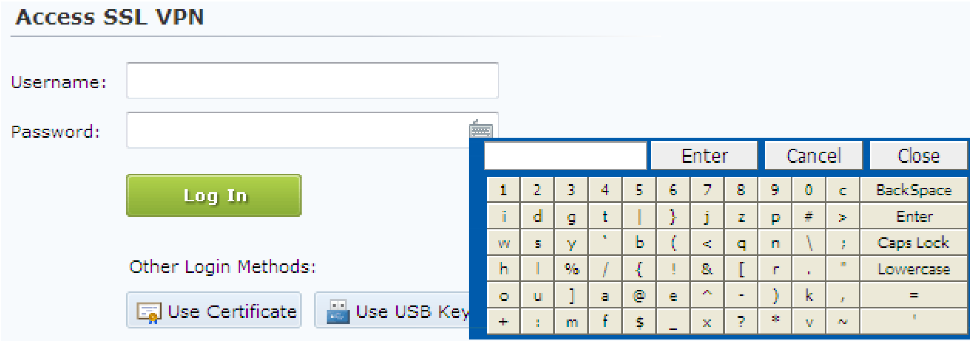
☑ If consecutive logon failures on one IP reach 64 (64-2048), lock IP address for 45 (30-1800) seconds

1. Logon failures indicate that the interval between two adjacent logons is less than 45 seconds;
2. Logon failures by a user indicate that user fails to log in successively (1-32 times) with a user account;
3. Logon failures on an IP indicate that user fails to log in successively (64-2048 times) on an IP address;
4. Time interval used for unlocking user/IP ranges from 30 to 1800. 0 means user will not be unlocked until admin unlocks it by hand.

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:

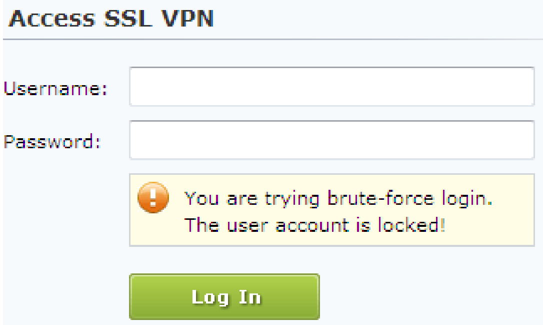


Access SSL VPN

Username:

Password:

- **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 lockedup or word verification be enabled for a period of time. The prompt given is as shown below:



Access SSL VPN

Username:

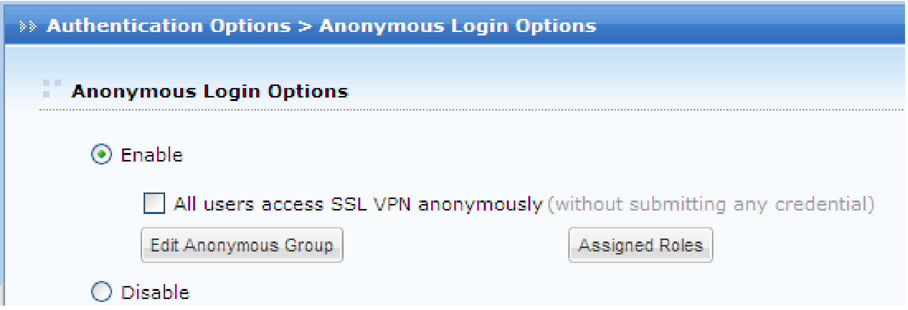
Password:

You are trying brute-force login.
The user account is locked!

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:



Authentication Options > Anonymous Login Options

Anonymous Login Options

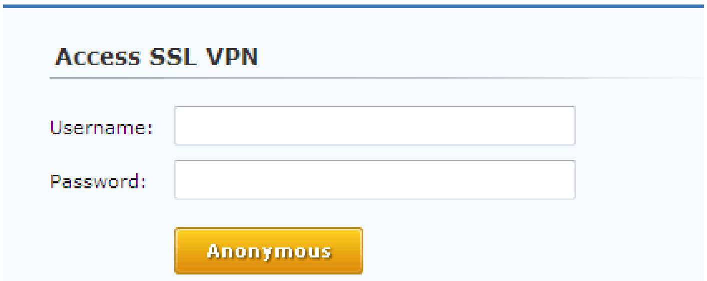
● Enable

□ All users access SSL VPN anonymously (without submitting any credential)

○ Disable

The following are the contents included on the **Anonymous Login Options** page:

- **Enable, Disable:** If **Disable** is selected, no user could log in to the SSL VPN anonymously. If **Enable** 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:

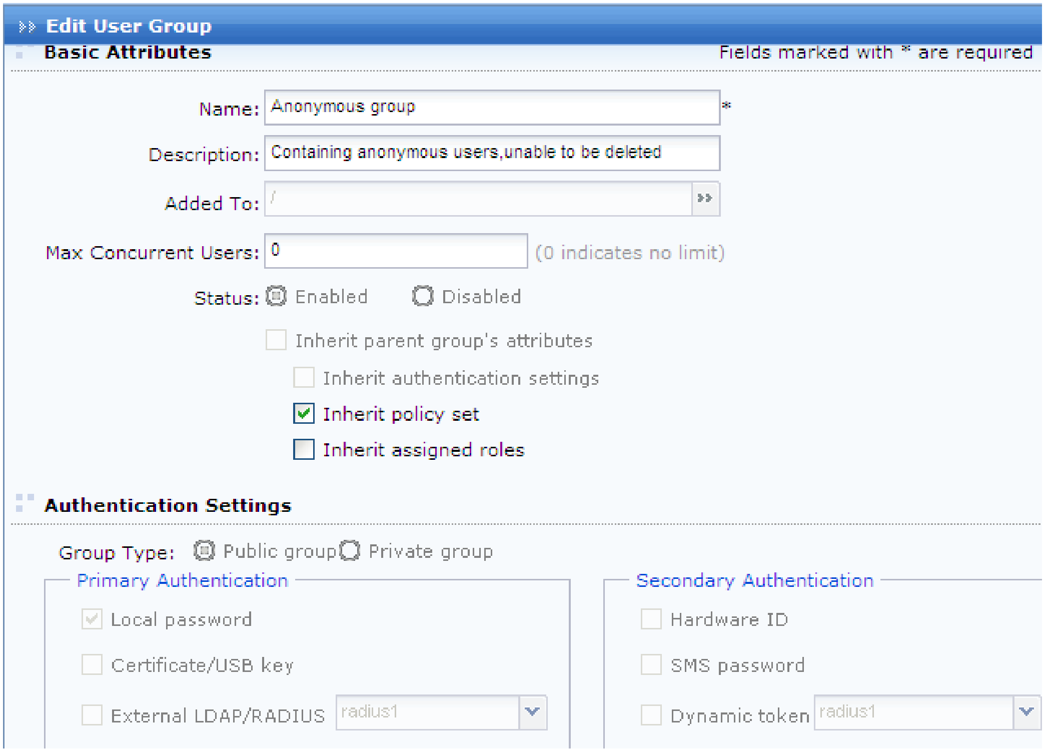


Access SSL VPN

Username:

Password:

- **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 GroupsectioningChapter 4. The attributes of **Anonymous group** are as shown in the figure below:



Edit User Group

Basic Attributes

Fields marked with * are required

Name: Anonymous group *

Description: Containing anonymous users,unable to be deleted

Added To: /

Max Concurrent Users: 0 (0 indicates no limit)

Status: ● Enabled ○ Disabled

□ Inherit parent group's attributes

□ Inherit authentication settings

☑ Inherit policy set

□ Inherit assigned roles

Authentication Settings

Group Type: ● Public group ○ Private group

Primary Authentication

☑ Local password

□ Certificate/USB key

□ External LDAP/RADIUS radius1

Secondary Authentication

□ Hardware ID

□ SMS password

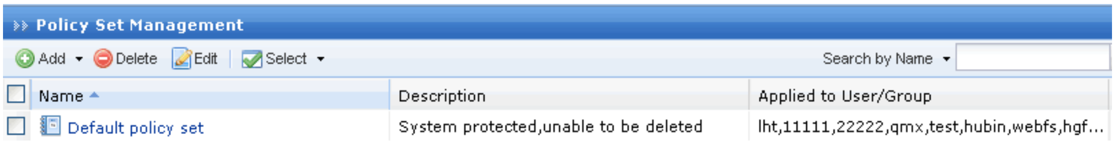
□ Dynamic token radius1

- **Assigned Roles:** Click this button to select and assign roles to the anonymous users. For detailed guide, please refer to the Adding Role sectioning Chapter 4.
- **Save:** Click it to save the settings. To apply changes, click the **Apply** button on the next page.

Policy Sets

A policy sets 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**, **SecureDesktop** and **Remote Application**.

Navigate to **SSL VPN > Policy Set**-to enter the **Policy Set Management** page, as shown below:



□	Name	Description	Applied to User/Group
□	Default policy set	System protected,unable to be deleted	lht,11111,22222,qmx,test,hubin,webfs,hgf...

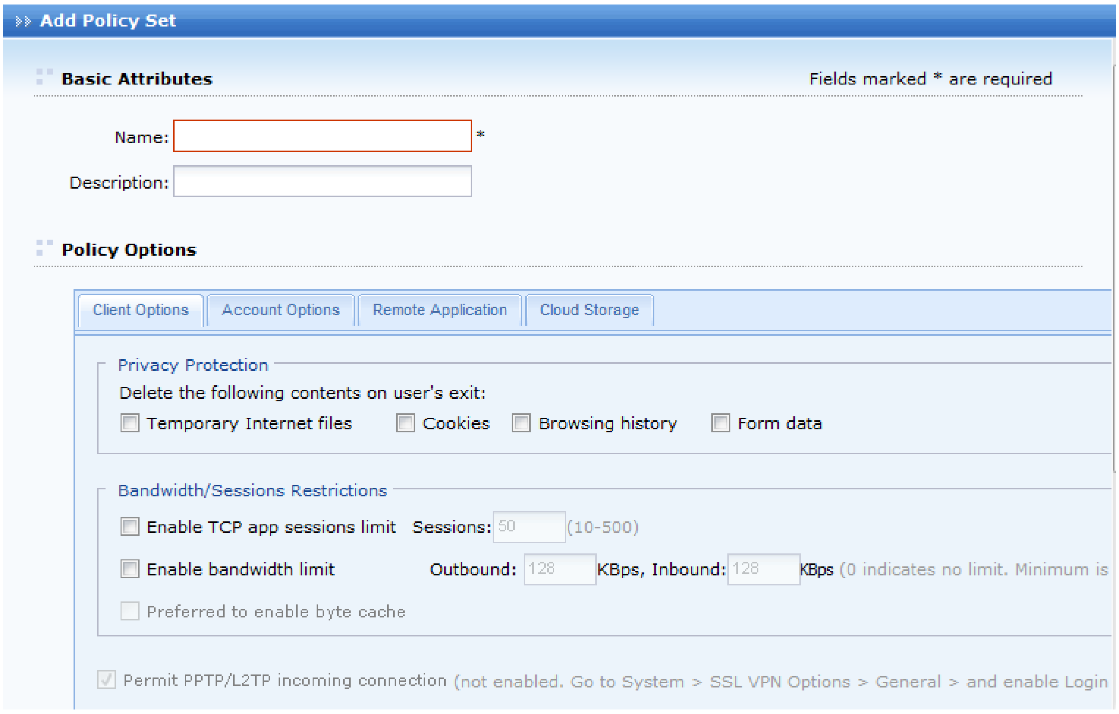
On the page displayed above, **Name** indicates the name of a policy set, **Description** indicates the descriptive information of a policy set and **Applied to User/Group** indicates the users/groups to which the corresponding policy set applies.

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:



Add Policy Set

Basic Attributes

Fields marked * are required

Name: *

Description:

Policy Options

Privacy Protection

Delete the following contents on user's exit:

☐ Temporary Internet files ☐ Cookies ☐ Browsing history ☐ Form data

Bandwidth/Sessions Restrictions

☐ Enable TCP app sessions limit Sessions: 50 (10-500)

☐ Enable bandwidth limit Outbound: 128 KBps, Inbound: 128 KBps (0 indicates no limit. Minimum is

☐ Preferred to enable byte cache

☑ Permit PPTP/L2TP incoming connection (not enabled. Go to System > SSL VPN Options > General > and enable Login

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 oppressions 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.

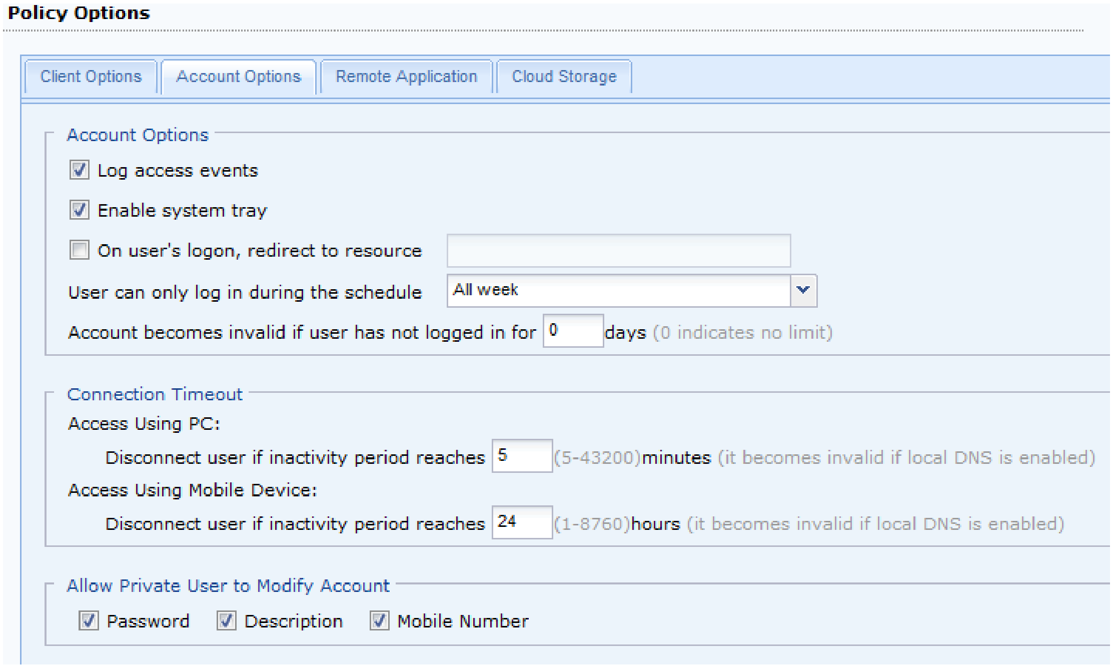
  - **Enable bandwidth limit:** Check it to enable limit on bandwidth for using Web applications, TCP applications and L3VPN at client and then specify maximum outbound and inbound bandwidth (KBps) allowed at client. The minimum value for this field is 32KBps and 0 means no limit. This function avoids 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 Settings section in Chapter 3**)**.

- **Allow login with PPTP:** Select whether to allow users to log in with PPTP.
- **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.
- **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.

4. Click **Account Options** to enter the **Account Options** tab and specify the account-related options, as shown below:



Account Options

☑ Log access events

☑ Enable system tray

☐ On user's logon, redirect to resource

User can only log in during the schedule: All week

Account becomes invalid if user has not logged in for 0 days (0 indicates no limit)

Connection Timeout

Access Using PC:

Disconnect user if inactivity period reaches 5 (5-43200)minutes (it becomes invalid if local DNS is enabled)

Access Using Mobile Device:

Disconnect user if inactivity period reaches 24 (1-8760)hours (it becomes invalid if local DNS is enabled)

Allow Private User to Modify Account

☑ Password ☑ Description ☑ Mobile Number

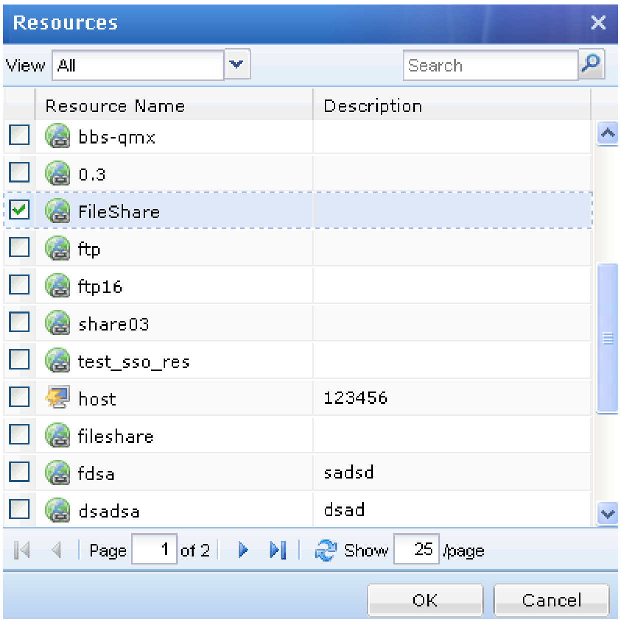
The following are the contents included on the **Account Options** tab:

- **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 (please refer to the Configuring Client Related Options sectioning Chapter 3).

The **Enable system tray** option under **System** > **SSL VPN Options** > **General** > **Client Options>Miscellaneous** 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 Resourcesectioning Chapter 4).



	Resource Name	Description
□	bbs-qmx	
□	0.3	
☑	FileShare	
□	ftp	
□	ftp16	
□	share03	
□	test_sso_res	
□	host	123456
□	fileshare	
□	fdsa	sadsd
□	dsadsa	dsad

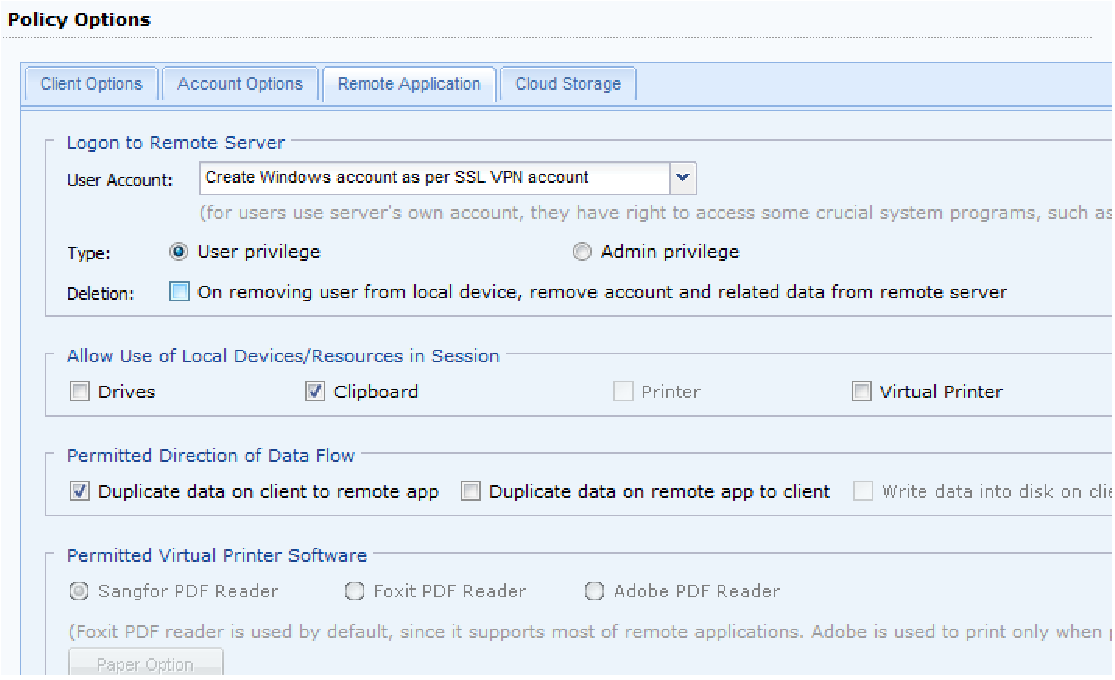
- **User can only log in during the schedule:** Specify the period of time only during which the user is allowed to access SSL VPN. Select a schedule from the drop-down list (the schedules available here are predefined in **System> Schedule**; please refer to the Schedules section in Chapter 3).
- **Account gets 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.
- **Disconnect user if user idles for (5-43200) minutes:** Specify the period to disconnect user due to inactivity. The value range is 5 to 43200 minutes.

- **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** to enter the **RemoteApplication** tab and then specify the related options, as shown below:



Policy Options

Client Options | Account Options | Remote Application | Cloud Storage

Logon to Remote Server

User Account: Create Windows account as per SSL VPN account

(for users use server's own account, they have right to access some crucial system programs, such as

Type: ● User privilege ○ Admin privilege

Deletion: □ On removing user from local device, remove account and related data from remote server

Allow Use of Local Devices/Resources in Session

□ Drives ☑ Clipboard □ Printer □ Virtual Printer

Permitted Direction of Data Flow

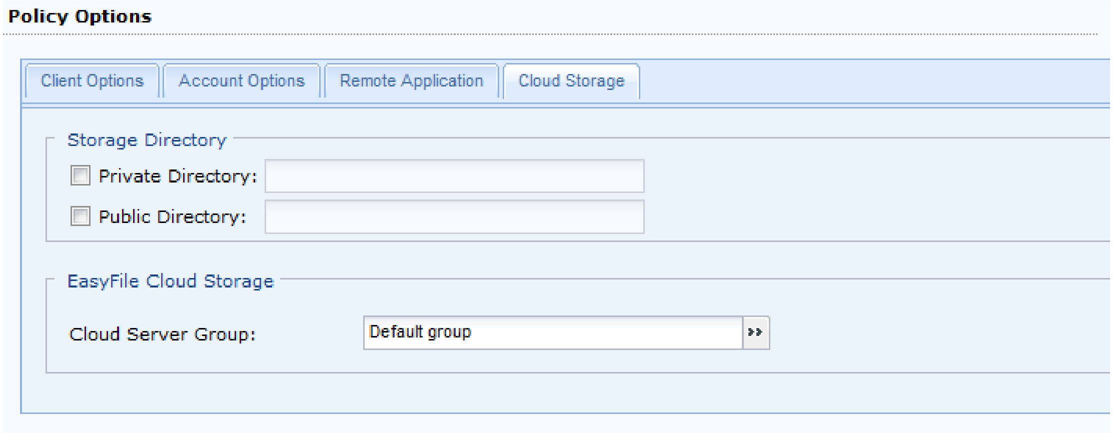
☑ Duplicate data on client to remote app □ Duplicate data on remote app to client □ Write data into disk on cli

Permitted Virtual Printer Software

● Sangfor PDF Reader ○ Foxit PDF Reader ○ Adobe PDF Reader

(Foxit PDF reader is used by default, since it supports most of remote applications. Adobe is used to print only when

6. Click **Cloud Storage** to enter the **Cloud Storage**, as shown below:



Policy Options

Storage Directory

□ Private Directory:

□ Public Directory:

EasyFile Cloud Storage

Cloud Server Group: Default group

7. Select the desired directory to store files on a remote server, including [private directory] and [public directory]

8. Click **Save** to save the settings or **Cancel** notto save the settings. To have settings take effect, click the **Apply**button at upper right of the next page.

Scenario19: Configuring Secure Desktop

Background:

- The user group named **Default Group** and its users have been configured (for detailed procedures of configuring user and user group, please refer to the SSL VPN Users section in Chapter 4).
- The user named **Guest** has been configured under the user group **Marketing Group**.
- The TCP application resources **OA Office System** and **Financial System** have been configured (for detailed procedures of configuring TCP application resource, please refer to the Resource section in Chapter 4).

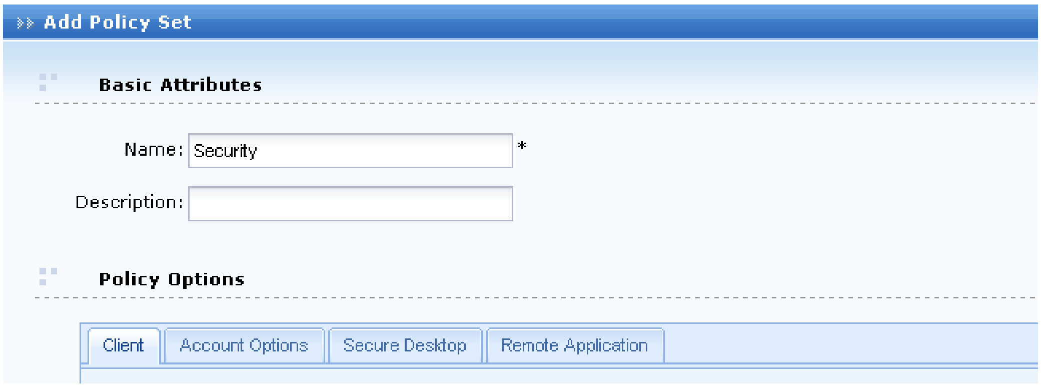
Purposes:

After the users under the **Default Group** and the user named **Guest** (under Marketing Group) log into SSL VPN, they can do the following:

- Access the resources **OA Office System** and **Financial System** on Secure Desktop
- Use COM port and printer on Secure Desktop
- Switch between default desktop and Secure Desktop
- Access the 192.168.1.1-192.168.1.254 subnet on Secure Desktop

To achieve the expected purposes:

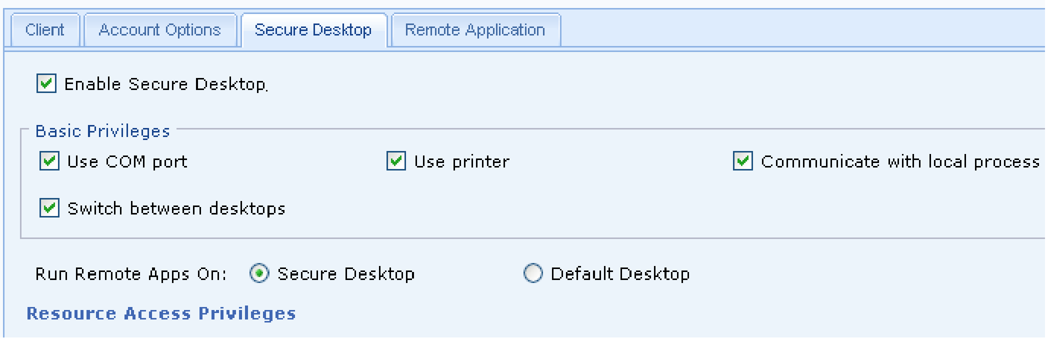
1. Navigate to **SSL VPN > Policy Set**-to enter the **Policy Set Management** page.
2. Click **Add** > **Policy set** to enter the **Add Policy Set** page, as shown below:



Name: Security *

Description:

3. Enter a name and description for the policy set and click **Secure Desktop** to enter the **Secure Desktop** tab, as shown below:



☑ Enable Secure Desktop.

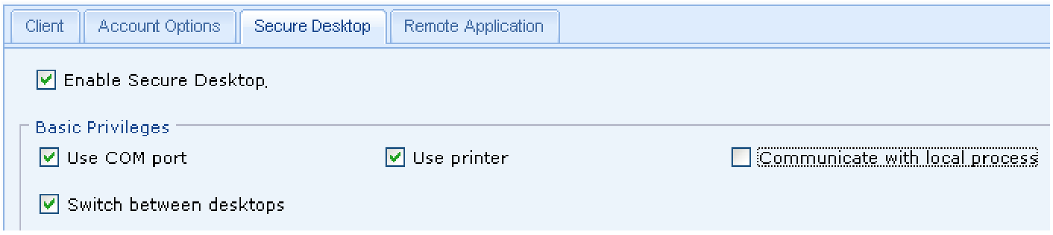
☑ Use COM port ☑ Use printer ☑ Communicate with local process

☑ Switch between desktops

Run Remote Apps On: ● Secure Desktop ○ Default Desktop

4. Check the **Enable Secure Desktop** option to enable Secure Desktop, and all the options displayed on the **Secure Desktop** tab are available.

5. Specify the basic privileges. As using printer and COM port on Secure Desktop and switching between desktops are expected, check **Use COM port**, **Use Printer** and **Switch between desktops**, as shown below:

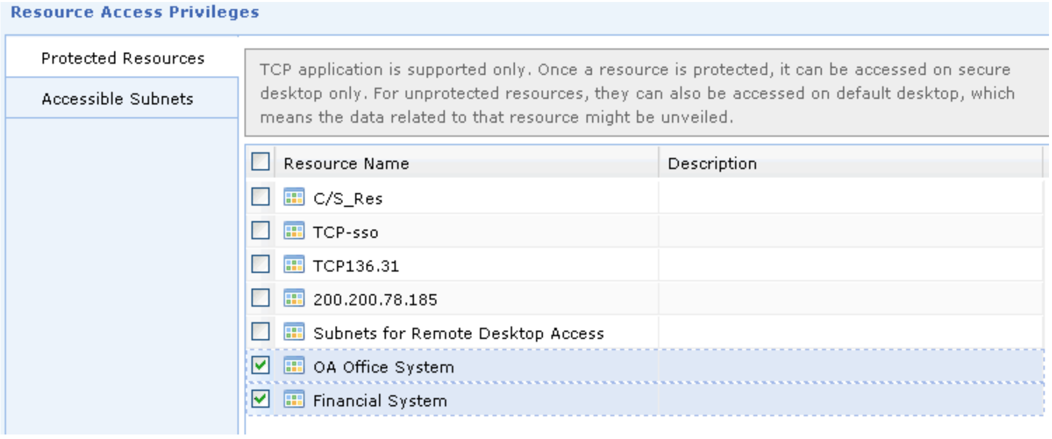


☑ Enable Secure Desktop.

☑ Use COM port ☑ Use printer □ Communicate with local process

☑ Switch between desktops

6. Configure the protected resources. All the available TCP application resources are in the list. As using OA office system and financial system are expected on Secure Desktop, select the **OA Office System** and **Financial System** resources, as shown below:

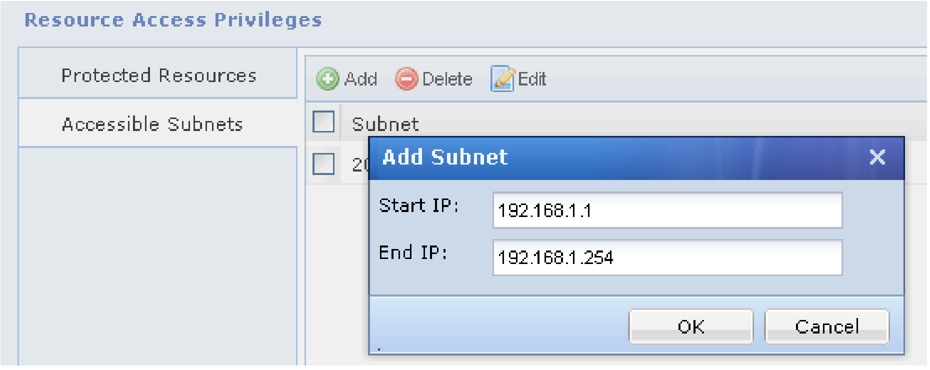


TCP application is supported only. Once a resource is protected, it can be accessed on secure desktop only. For unprotected resources, they can also be accessed on default desktop, which means the data related to that resource might be unveiled.

□	Resource Name	Description
□	C/S_Res	
□	TCP-sso	
□	TCP136.31	
□	200.200.78.185	
□	Subnets for Remote Desktop Access	
☑	OA Office System	
☑	Financial System	

7. Configure **Accessible Subnets** to have the 192.168.1.1-192.168.1.254 subnet accessible to users after they log in to SSL VPN.

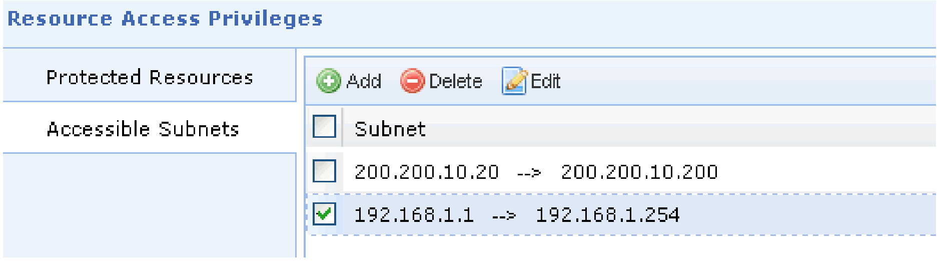
   a. Click **Add** to enter the **Add Subnet** page, and then enter 192.168.1.1 and 192.168.1.254 respectively, as shown below:



Start IP: 192.168.1.1

End IP: 192.168.1.254

   b. Click the**OK** button and the subnet is added into the list. Check the entry, as shown below:

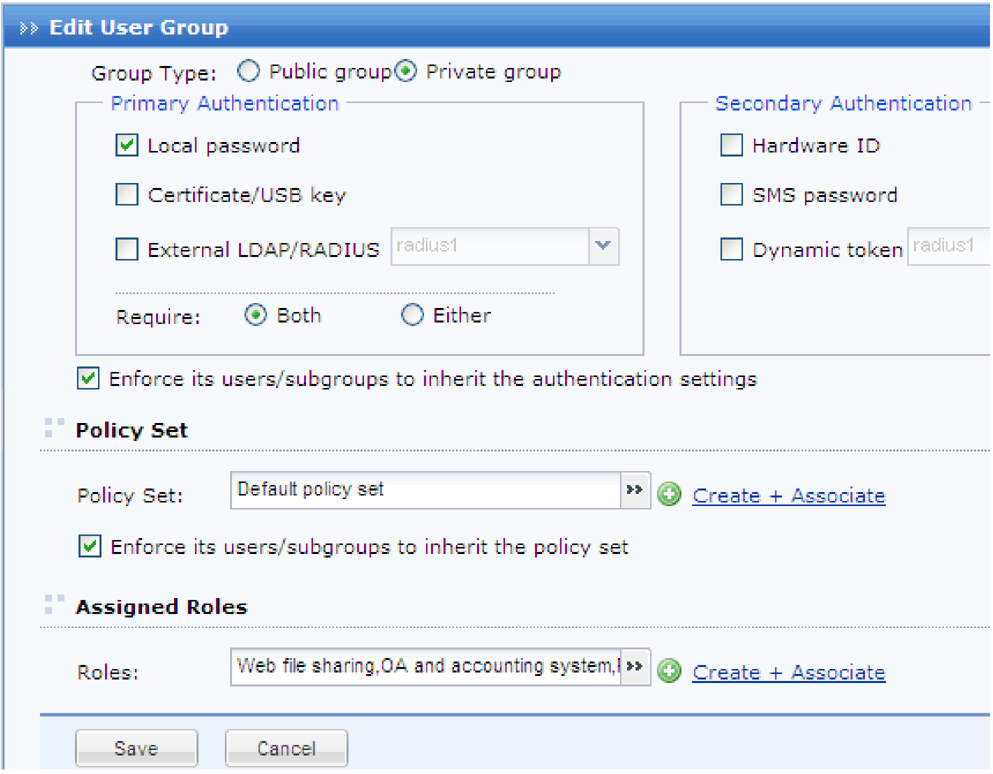


□	Subnet
□	200.200.10.20 --> 200.200.10.200
☑	192.168.1.1 --> 192.168.1.254

8. Click the **Save** button on the **Add Policy Set** page to save the above settings.

9. Associate the policy set **Security** with the user group named **Default Group**.

   a. Navigate to the **SSL VPN** > **Users** > **User Management** page, select **Default Group** and click **Edit** to enter the **Edit User Group** page, as shown below:



Edit User Group

Group Type: ○ Public group ● Private group

Primary Authentication

☑ Local password

☐ Certificate/USB key

☐ External LDAP/RADIUS radius1

Require: ● Both ○ Either

Secondary Authentication

☐ Hardware ID

☐ SMS password

☐ Dynamic token radius1

☑ Enforce its users/subgroups to inherit the authentication settings

Policy Set

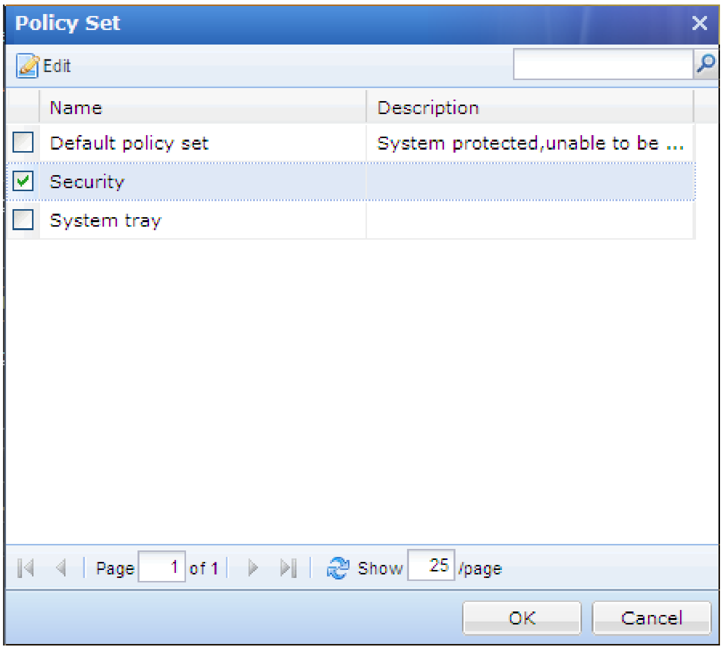
Policy Set: Default policy set

☑ Enforce its users/subgroups to inherit the policy set

Assigned Roles

Roles: Web file sharing,OA and accounting system,I

b. Under **Policy Set**, click on the textbox to enter the **Policy Set** page, select the policy set **Security** and click the **OK** button, as shown below:



Policy Set

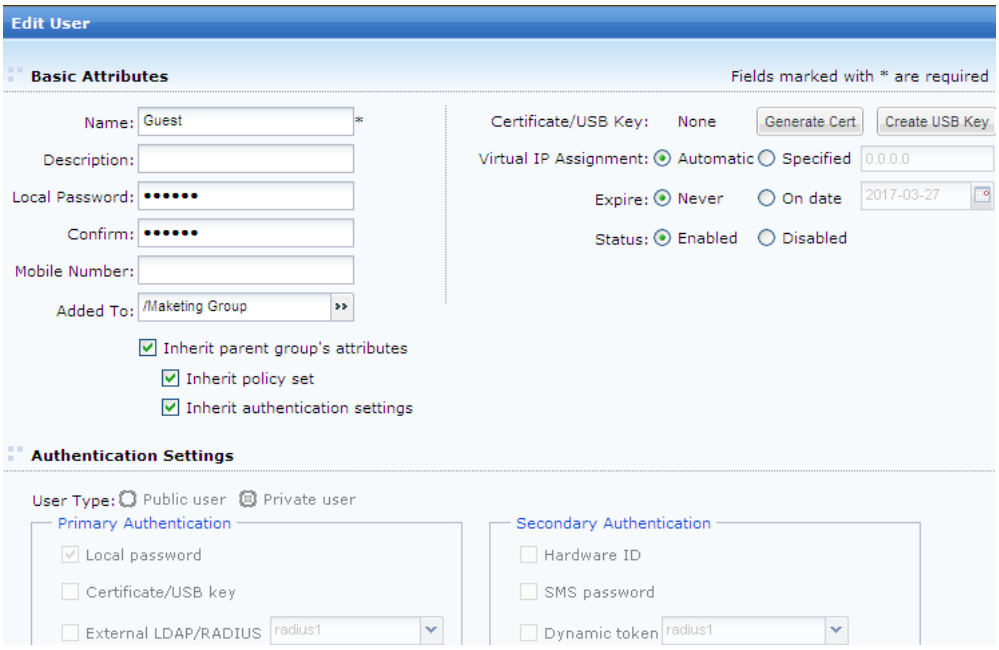
	Name	Description
☐	Default policy set	System protected,unable to be ...
☑	Security	
☐	System tray	

c. Check **Enforce its users/subgroups to inherit the policy set** to have all the subgroups and users under the **Default Group** associate with the policy set **Security** as well or uncheck it to only have the **Default Group** itself and its direct users associate with the policy set.

d. Click the **Save** button and **Apply** buttonto save and apply the settings.

10. Associate the policy set **Security** with the user named **Guest**.

   a. Navigate to the **SSL VPN** > **Users** > **User Management** page, select the user **Guest** and click **Edit** to enter the **Edit User** page, as shown below:



Edit User

Basic Attributes — Fields marked with * are required

Name: Guest *
Description:
Local Password: ••••••
Confirm: ••••••
Mobile Number:
Added To: /Maketing Group
☑ Inherit parent group's attributes
☑ Inherit policy set
☑ Inherit authentication settings

Certificate/USB Key: None
Virtual IP Assignment: ● Automatic ○ Specified 0.0.0.0
Expire: ● Never ○ On date 2017-03-27
Status: ● Enabled ○ Disabled

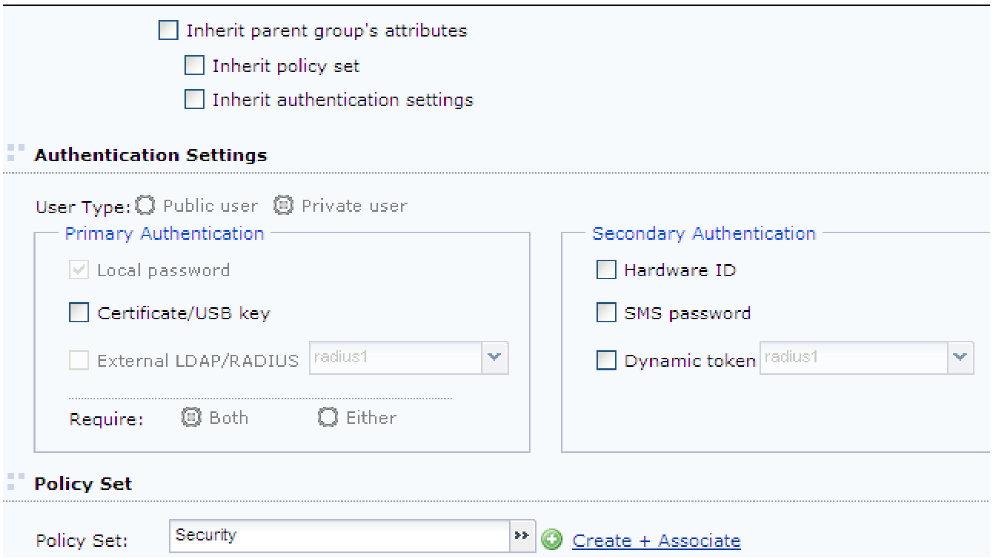
Authentication Settings

User Type: ○ Public user ● Private user

Primary Authentication
☑ Local password
□ Certificate/USB key
□ External LDAP/RADIUS radius1

Secondary Authentication
□ Hardware ID
□ SMS password
□ Dynamic token radius1

   b. Uncheck **Inherit parent group's attributes** to have the user associate its own policy set and authentication settings instead of inheriting its parent group's attributes, and the authentication options and policy set option turn available, as shown below:



□ Inherit parent group's attributes
□ Inherit policy set
□ Inherit authentication settings

Authentication Settings

User Type: ○ Public user ● Private user

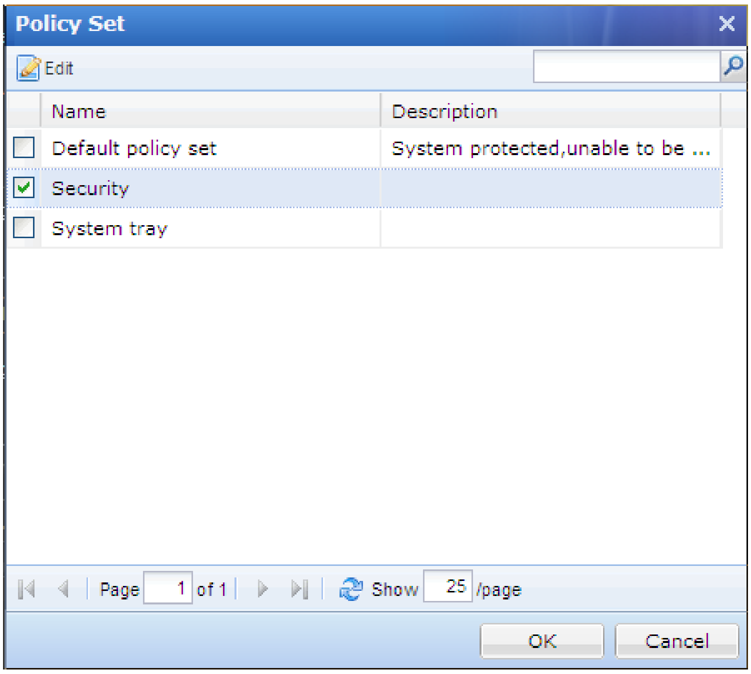
Primary Authentication
☑ Local password
□ Certificate/USB key
□ External LDAP/RADIUS radius1
Require: ● Both ○ Either

Secondary Authentication
□ Hardware ID
□ SMS password
□ Dynamic token radius1

Policy Set

Policy Set: Security

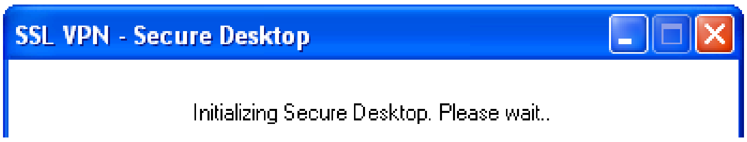
   c. Under **Policy Set**, click in the textbox to enter the **Policy Set** page, select the policy set **Security** and click the**OK** button, as shown below:



	Name	Description
□	Default policy set	System protected,unable to be ...
☑	Security	
□	System tray	

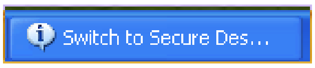
d. Click the **Save** button and then the **Apply** button to save and apply the settings.

11. End user logs in to SSL VPN. The minute he or she connects to SSL VPN. The required components will be automatically installed on user computer and Secure Desktop will start initializing, as shown below:



Initializing Secure Desktop. Please wait..

After SecureDesktop initialization, the taskbar button **Switch to Secure Desktop** will be displayed on taskbar.



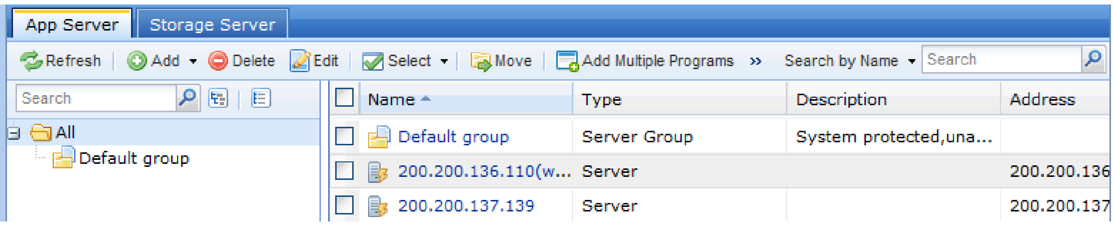
Click it to enter Secure Desktop and the protected TCP applications will be available on the **Resource** page.

When users log out of SSL VPN, they will also exit from Secure Desktop.

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.

Navigate to **SSL VPN > Remote Servers** to enter the **App Server** page, as shown below:



	Name	Type	Description	Address
□	Default group	Server Group	System protected,una...	
□	200.200.136.110(w...	Server		200.200.136
□	200.200.137.139	Server		200.200.137

The following are the contents included on the **Remote Server Management** 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 remote server, **Storage Server** or **App Server**.
- **Status:** Displays the status of a remote server, **Online** or **Offline**.
- **Enabled:** Displays whether the remote server is enabled or not.

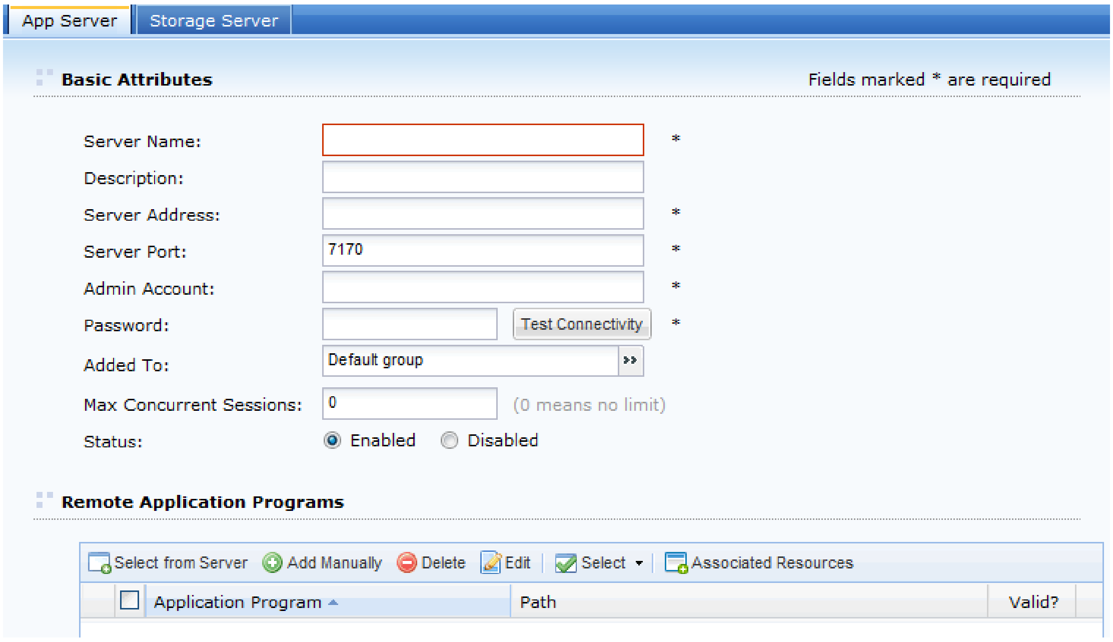
The following are some optional operations on the **Remote Server Management** page:

- To add a **Remote Server** or **Storage Server**
- To delete one or more remote servers, select the remote servers and then click **Delete**.
- To edit a remote server, select the remote server entry and then click **Edit**.
- To select remote servers on all pages, click **Select > All pages**.
- To select remote servers on the current page, click **Select > Current pages**.
- To cancel the selection, click **Select > Deselect**.
- To add multiple programs for one or more remote serversselect the remote servers and click **Add Multiple Programs**, and a dialog will appear, displaying the application programs available on existing remote servers.
- To allow delivered applications to invoke third-party programs, click **Program White List** and then specify third-party programs according to the specific case.
- To configure global settings for remote application servers, click **App Server Options**.

- To download RemoteApp Agent, click **Download RemoteApp Agent**.
- To update one or more remote servers, select the remote 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 remote 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 **Remote Server Management** page.
2. Click **Add > App Server** to enter the **Edit Remote App Server** page, as shown below:



Basic Attributes

Fields marked * are required

Server Name: *
Description:
Server Address: *
Server Port: 7170 *
Admin Account: *
Password: *
Added To: Default group
Max Concurrent Sessions: 0 (0 means no limit)
Status: ● Enabled ○ Disabled

Remote Application Programs

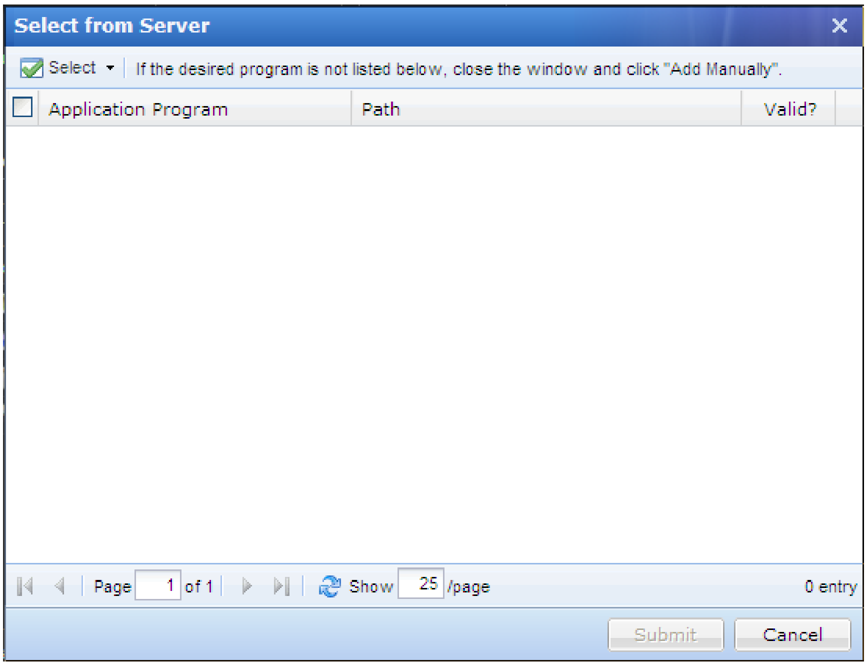
3. Configure **Basic Attributes** of the application server. The following are the basic attributes:
   - **Server Name**, **Description:** Enter a name and description for the remote application server.
   - **Server Address:** Enter the IP address of the remote application server that theSangfor device 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.
   - **Max Concurrent Sessions:** Specify the maximum number of concurrent connections to the remote

application server.

- **Status:** Select whether to enable the current remote 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:



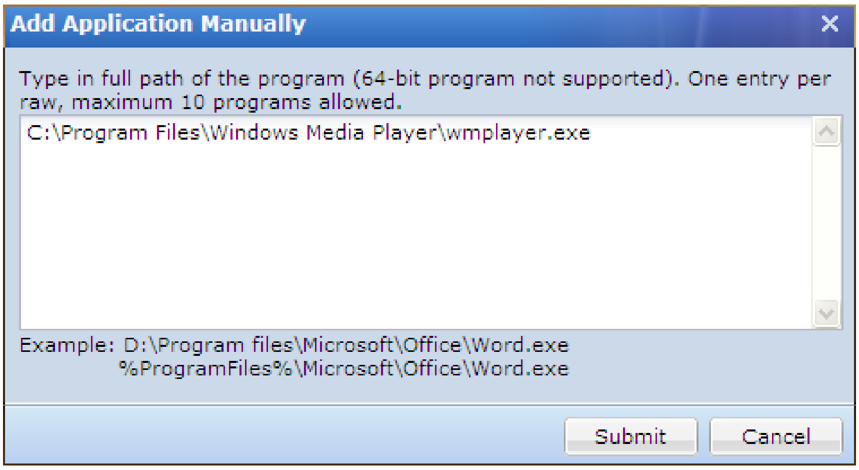
Select from Server

If the desired program is not listed below, close the window and click "Add Manually".

□ Application Program	Path	Valid?

Page 1 of 1 · Show 25 /page · 0 entry

- 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:



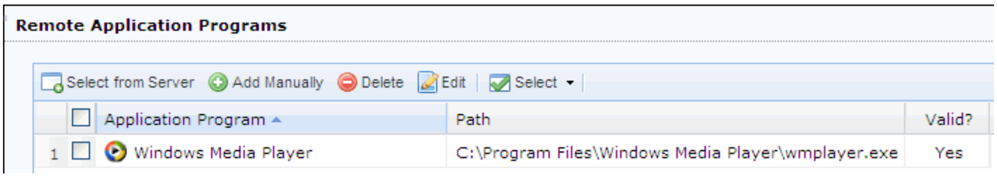
Add Application Manually

Type in full path of the program (64-bit program not supported). One entry per raw, maximum 10 programs allowed.

C:\Program Files\Windows Media Player\wmplayer.exe

Example: D:\Program files\Microsoft\Office\Word.exe
%ProgramFiles%\Microsoft\Office\Word.exe

Click **Submit** to add the program, as shown below:



Remote Application Programs

□	Application Program	Path	Valid?
1 □	Windows Media Player	C:\Program Files\Windows Media Player\wmplayer.exe	Yes

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**.

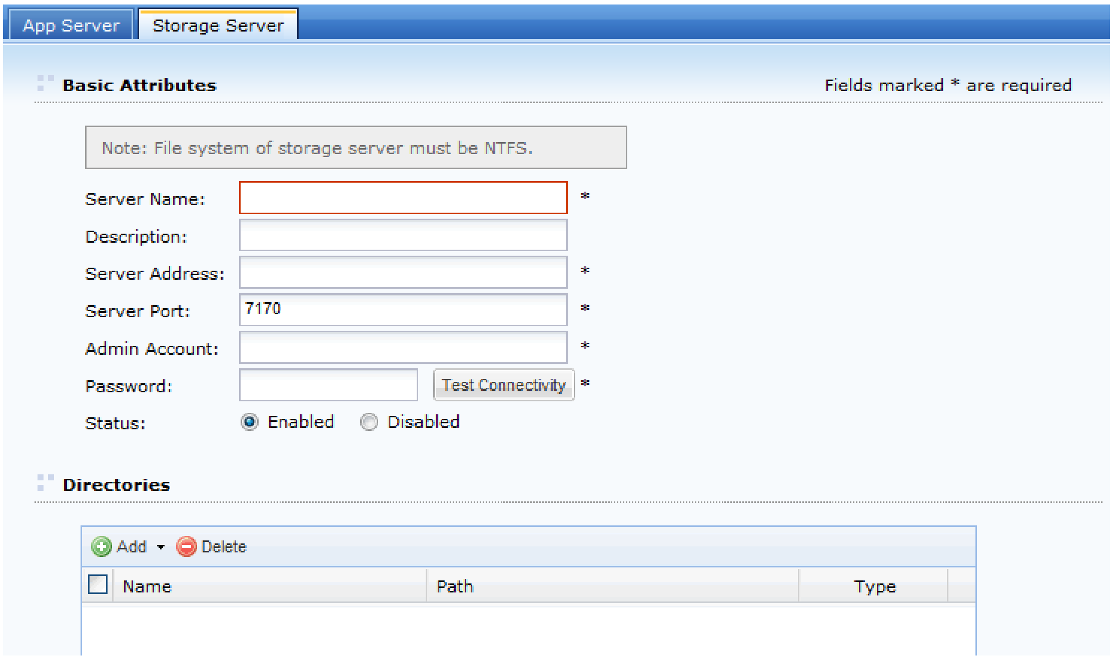
To select the programs on all pages, click **Select** > **All pages**.

To cancel the selection, click **Select** > **Deselect**.

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

Adding Remote Storage Server

1. Navigate to **SSL VPN** > **Remote Servers** to enter the **Remote Server Management** page.
2. Click **Add** >**Storage Server** to enter the **Edit Remote Storage Server** page, as shown below:



Basic Attributes

Fields marked * are required

Note: File system of storage server must be NTFS.

Server Name: *

Description:

Server Address: *

Server Port: 7170 *

Admin Account: *

Password: Test Connectivity *

Status: ● Enabled ○ Disabled

Directories

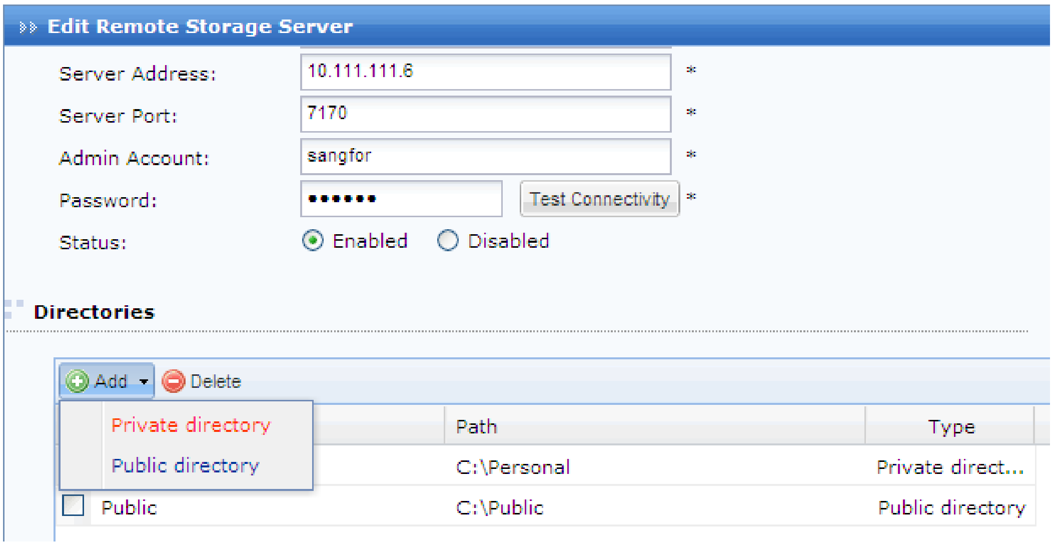
□	Name	Path	Type

3. Configure **Basic Attributes** of the storage server. The following are the basic attributes:

- **Server Name**, **Description:** Enter a name and description for theremote 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. It is 7170 by default.
- **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**,specifydirectory as private and/or public directory on the remote storage server.



Edit Remote Storage Server

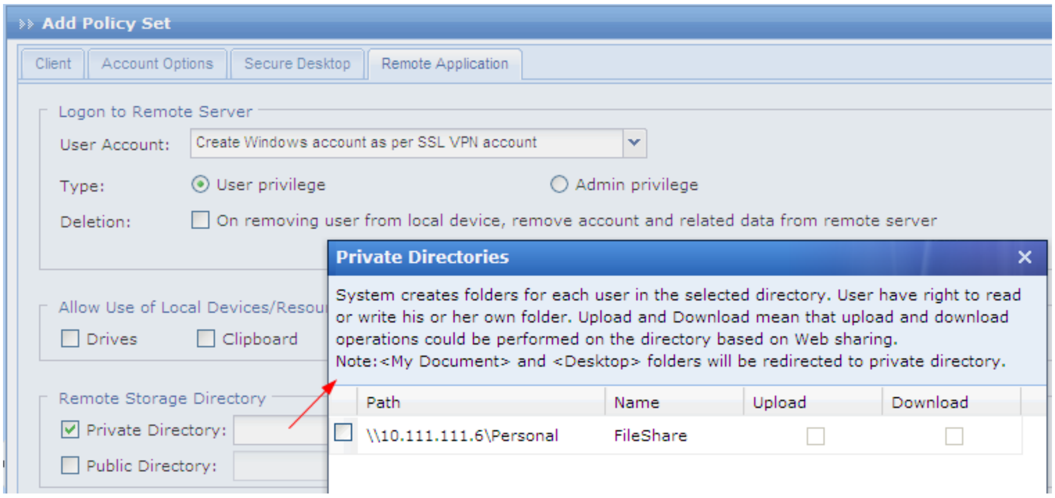
Server Address:	10.111.111.6 *
Server Port:	7170 *
Admin Account:	sangfor *
Password:	•••••• Test Connectivity *
Status:	● Enabled ○ Disabled

Directories

		Path	Type
		C:\Personal	Private direct...
□	Public	C:\Public	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.



Add Policy Set

Logon to Remote Server

User Account: Create Windows account as per SSL VPN account

Type: ● User privilege ○ Admin privilege

Deletion: □ On removing user from local device, remove account and related data from remote server

Allow Use of Local Devices/Resou

□ Drives □ Clipboard

Remote Storage Directory

☑ Private Directory:

□ Public Directory:

Private Directories

System creates folders for each user in the selected directory. User have right to read or write his or her own folder. Upload and Download mean that upload and download operations could be performed on the directory based on Web sharing.
Note:<My Document> and <Desktop> folders will be redirected to private directory.

	Path	Name	Upload	Download
□	\\10.111.111.6\Personal	FileShare	□	□

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).

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

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.

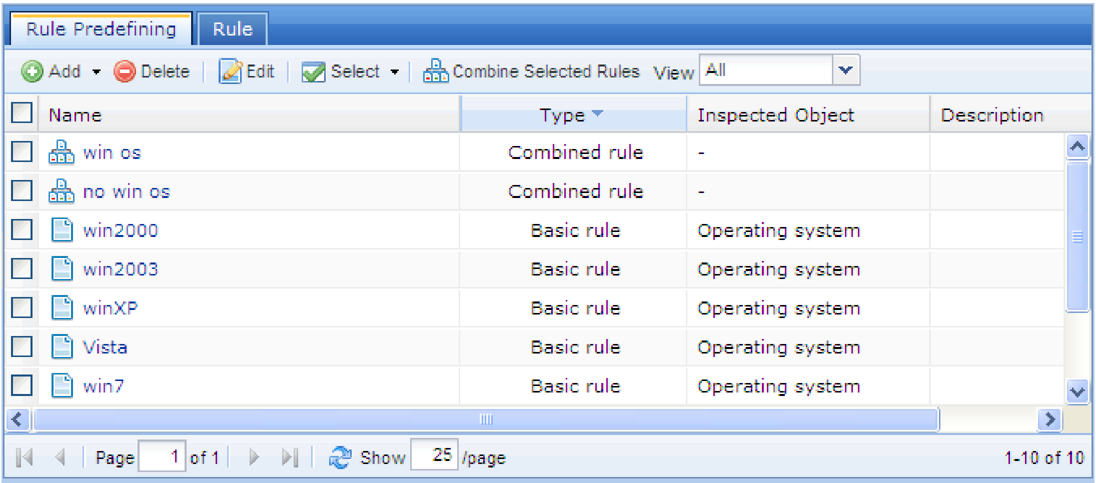
Pre-authentication check is carried out before user logs in to the SSL VPN. If user fails the pre-authentication check, which means, user fails to satisfy the requirements set by the associated security policy (user-level policy and/or role-level policy), he/she will be unable to access SSL VPN or the 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 sectioning 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:



□	Name	Type	Inspected Object	Description
□	win os	Combined rule	-	
□	no win os	Combined rule	-	
□	win2000	Basic rule	Operating system	
□	win2003	Basic rule	Operating system	
□	winXP	Basic rule	Operating system	
□	Vista	Basic rule	Operating system	
□	win7	Basic rule	Operating system	

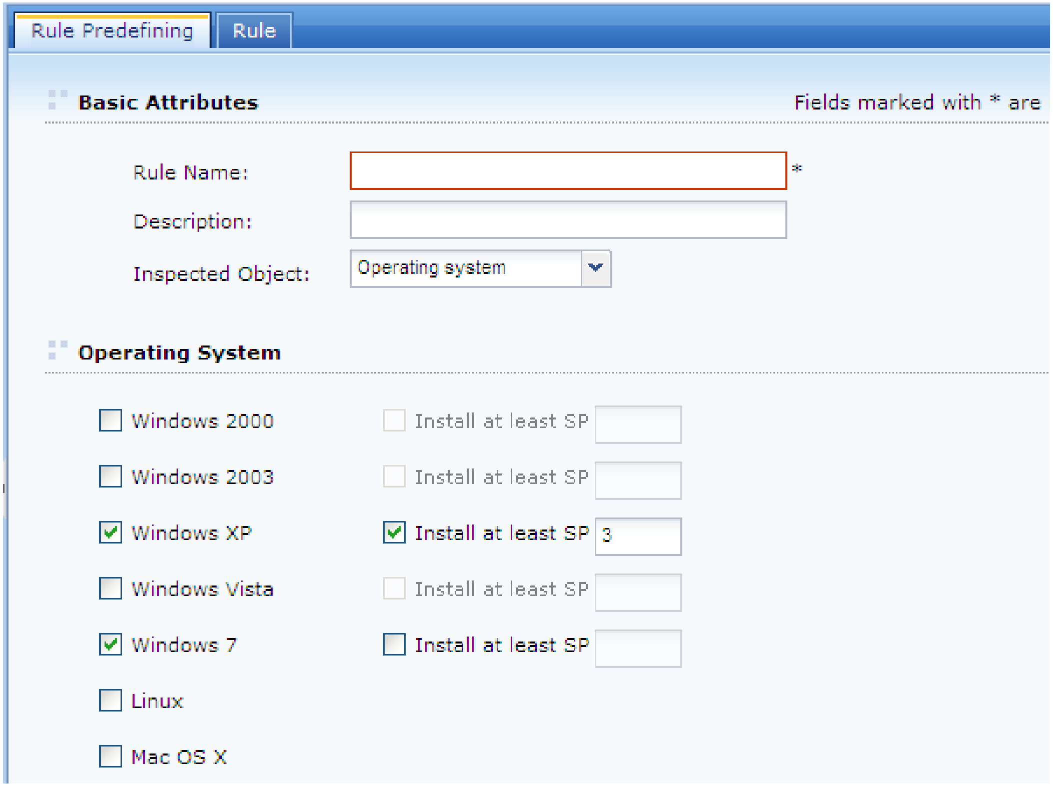
Page 1 of 1 Show 25 /page 1-10 of 10

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:



Basic Attributes

Fields marked with * are

Rule Name: *

Description:

Inspected Object: Operating system

Operating System

☐ Windows 2000 ☐ Install at least SP

☐ Windows 2003 ☐ Install at least SP

☑ Windows XP ☑ Install at least SP 3

☐ Windows Vista ☐ Install at least SP

☑ Windows 7 ☐ Install at least SP

☐ Linux

☐ Mac OS X

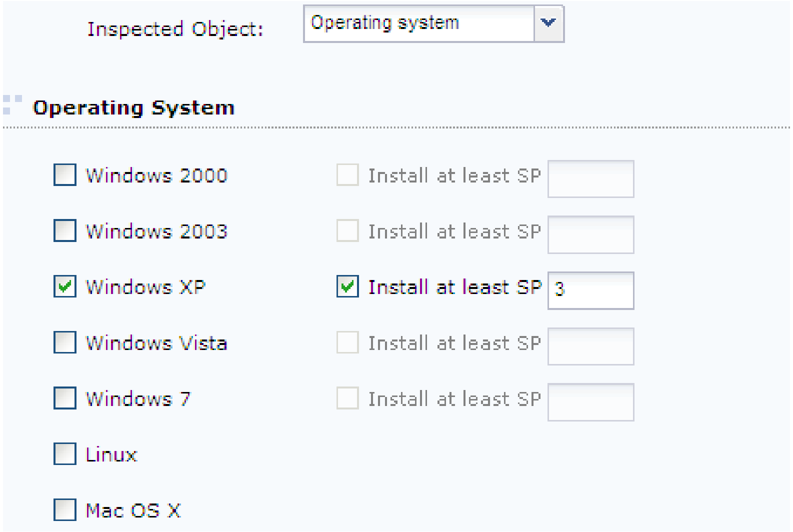
2. Configure the following fields on the above page.

- **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** and **Endpoint feature**.

- **Operating System:** If the inspected object is **Operating system**, the options related to operating system will appear, as shown in the figure below:



Inspected Object: Operating system

Operating System

□ Windows 2000 □ Install at least SP

□ Windows 2003 □ Install at least SP

☑ Windows XP ☑ Install at least SP 3

□ Windows Vista □ Install at least SP

□ Windows 7 □ Install at least SP

□ Linux

□ Mac OS X

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.

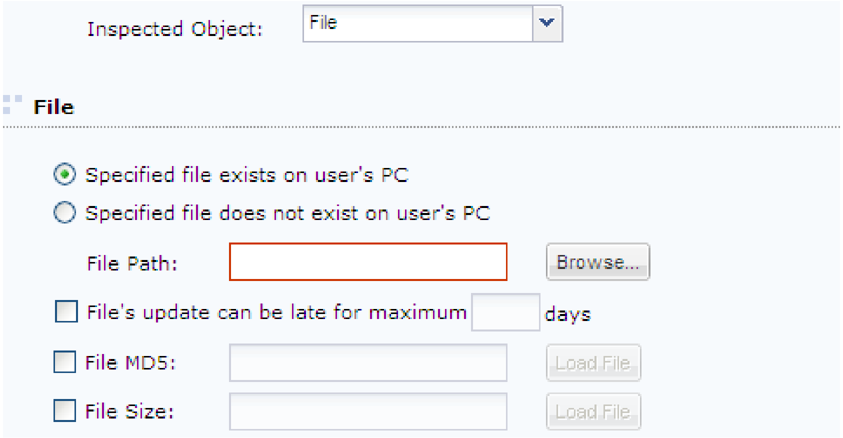
To save this rule, click the **Save** button.

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:



Inspected Object: File

File

● Specified file exists on user's PC

○ Specified file does not exist on user's PC

File Path:

□ File's update can be late for maximum days

□ File MD5:

□ File Size:

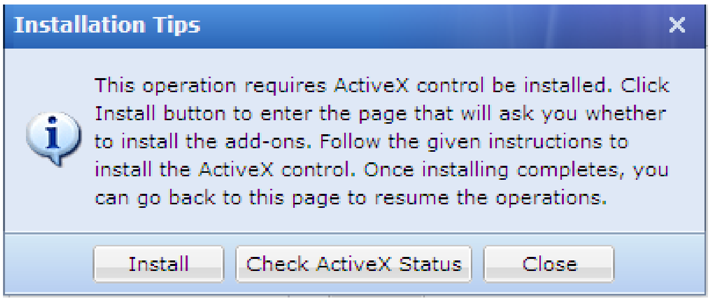
The following are the contents under **File**:

- **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.

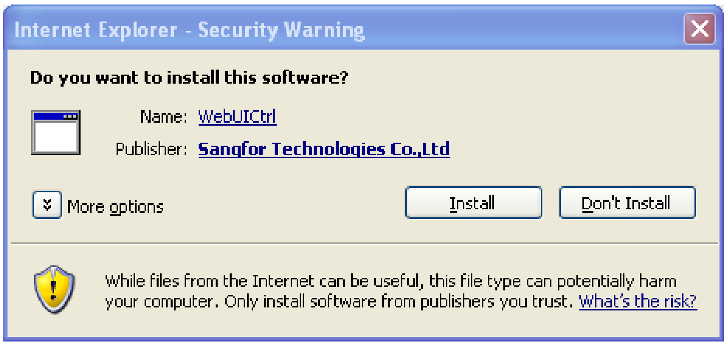
  The first time administrator clicks **Load File** to get MD5 or size of a file, the browser will ask whether the ActiveX control **WebUICtrl** has been installed, as shown in the figure below:



Installation Tips

This operation requires ActiveX control be installed. Click Install button to enter the page that will ask you whether to install the add-ons. Follow the given instructions to install the ActiveX control. Once installing completes, you can go back to this page to resume the operations.

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.



Internet Explorer - Security Warning

Do you want to install this software?

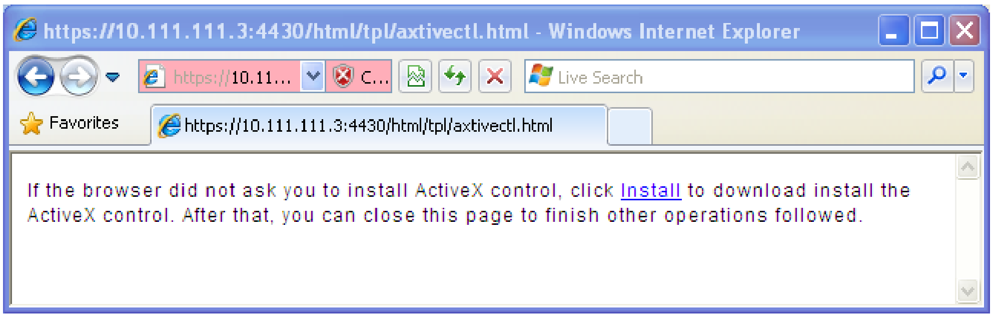
Name: WebUICtrl

Publisher: Sangfor Technologies Co.,Ltd

While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

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:



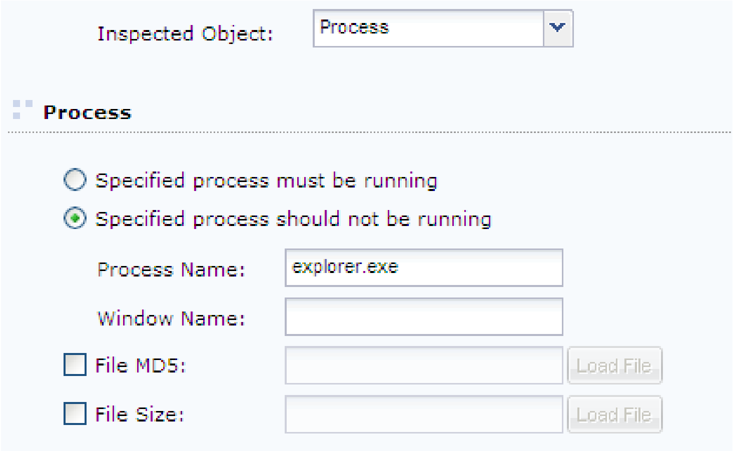
https://10.111.111.3:4430/html/tpl/axtivectl.html - Windows Internet Explorer

If the browser did not ask you to install ActiveX control, click Install to download install the ActiveX control. After that, you can close this page to finish other operations followed.

⚠

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:



Inspected Object: Process

Process

○ Specified process must be running

● Specified process should not be running

Process Name: explorer.exe

Window Name:

□ File MD5:

□ File Size:

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.

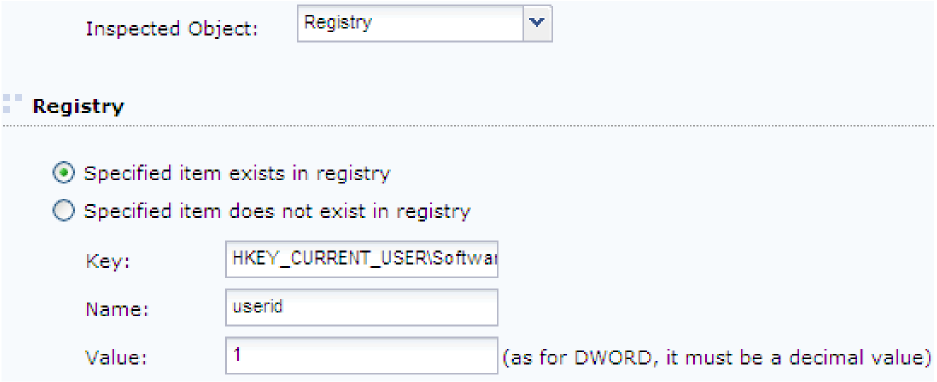
- **File MD5:** If this option is selected and MD5 hash checksums of this file is obtained (click **Load File**, browse and select the file), contents in the file on user's PC must be exactly the same with this file, that is to say, the file must not be altered by end user, otherwise, access to SSL VPN 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:



Inspected Object: Registry

Registry

● Specified item exists in registry
○ Specified item does not exist in registry

Key: HKEY_CURRENT_USER\Softwar

Name: userid

Value: 1 (as for DWORD, it must be a decimal value)

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.

⚠

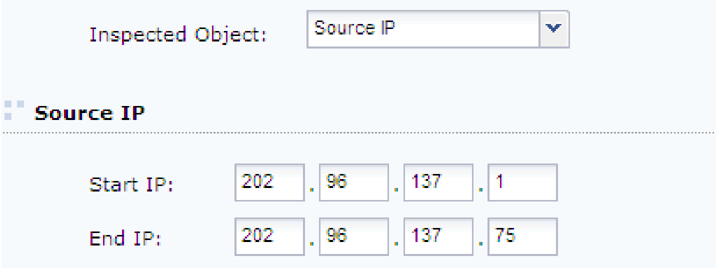
This field is required. Letters entered are case-insensitive.

- **Name:** Specifies the name of the key that will be checked.
- **Value:** Specifies the value of the key that will be checked. For DWORD, it must be a decimal value.

⚠

The option under **Registry** arewith **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:



Inspected Object: Source IP

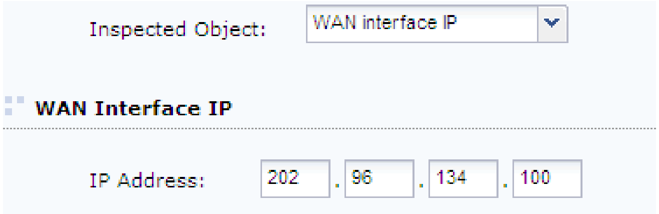
Source IP

Start IP: 202 . 96 . 137 . 1

End IP: 202 . 96 . 137 . 75

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:



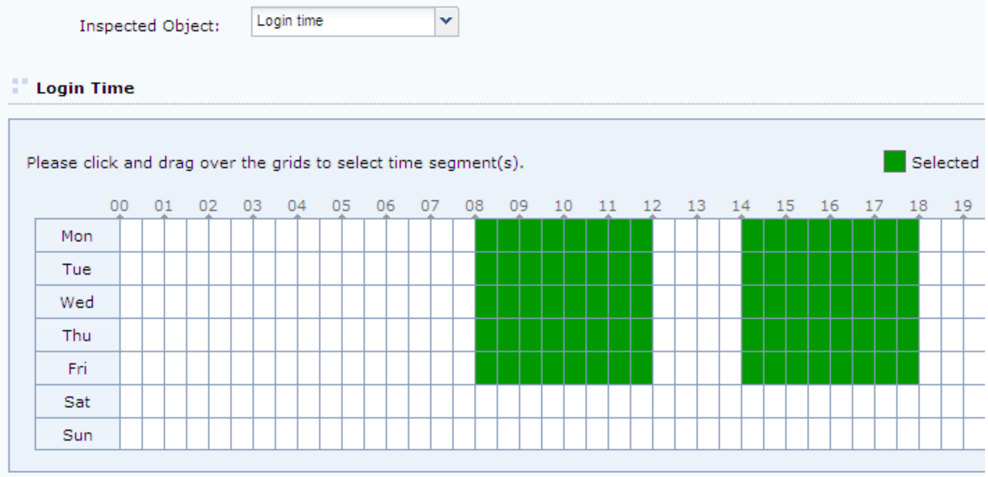
Inspected Object: WAN interface IP

WAN Interface IP

IP Address: 202 . 96 . 134 . 100

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:



Inspected Object: Login time

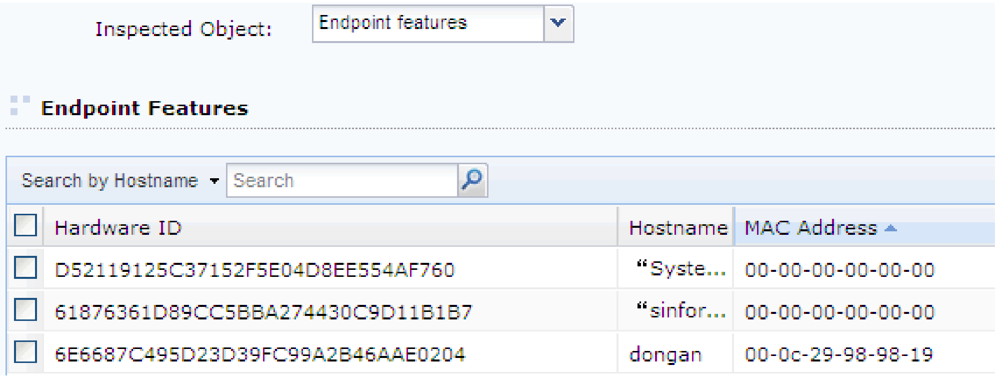
Login Time

Please click and drag over the grids to select time segment(s). 🟩 Selected

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19
Mon									🟩	🟩	🟩	🟩			🟩	🟩	🟩	🟩		
Tue									🟩	🟩	🟩	🟩			🟩	🟩	🟩	🟩		
Wed									🟩	🟩	🟩	🟩			🟩	🟩	🟩	🟩		
Thu									🟩	🟩	🟩	🟩			🟩	🟩	🟩	🟩		
Fri									🟩	🟩	🟩	🟩			🟩	🟩	🟩	🟩		
Sat																				
Sun																				

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:



Inspected Object: Endpoint features

Endpoint Features

Search by Hostname ▾ Search

□	Hardware ID	Hostname	MAC Address ▲
□	D52119125C37152F5E04D8EE554AF760	"Syste...	00-00-00-00-00-00
□	61876361D89CC5BBA274430C9D11B1B7	"sinfor...	00-00-00-00-00-00
□	6E6687C495D23D39FC99A2B46AAE0204	dongan	00-0c-29-98-98-19

The hardware IDs listed under **Endpoint Features** come from **Hardware ID** page (please refer to the Managing Hardware IDssectionin 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.

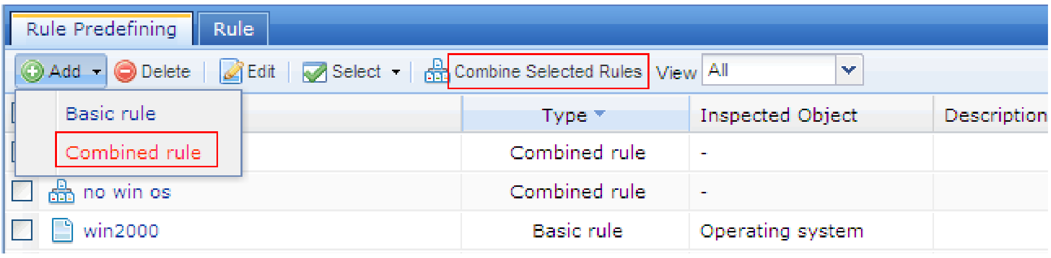
To view the hardware IDs in descending or ascending order by hardware ID, hostname or MAC address, click on the column header, **Hardware ID**, **Hostname** or **MAC Address** respectively.

To search for a specific entry, click **Search by Hostname/MAC Address**, enter the keyword and click the magnifier icon 🔍.

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

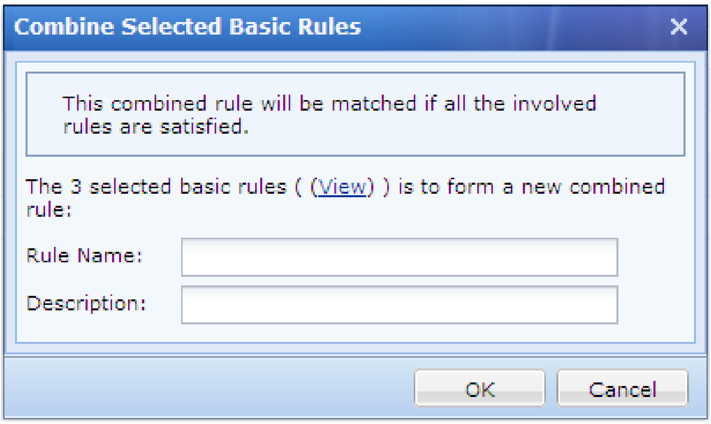
Predefining Combined Rule

1. Navigate to **SSL VPN**>**Endpoint Security**>**Rules** to enter the **Rule Predefining** pageand click **Add**>**Combined rule**, or click **Combine Selected Rules**, as shown below:



	Type	Inspected Object	Description
	Combined rule	-	
no win os	Combined rule	-	
win2000	Basic rule	Operating system	

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:


Combine Selected Basic Rules

This combined rule will be matched if all the involved rules are satisfied.

The 3 selected basic rules ((View)) is to form a new combined rule:

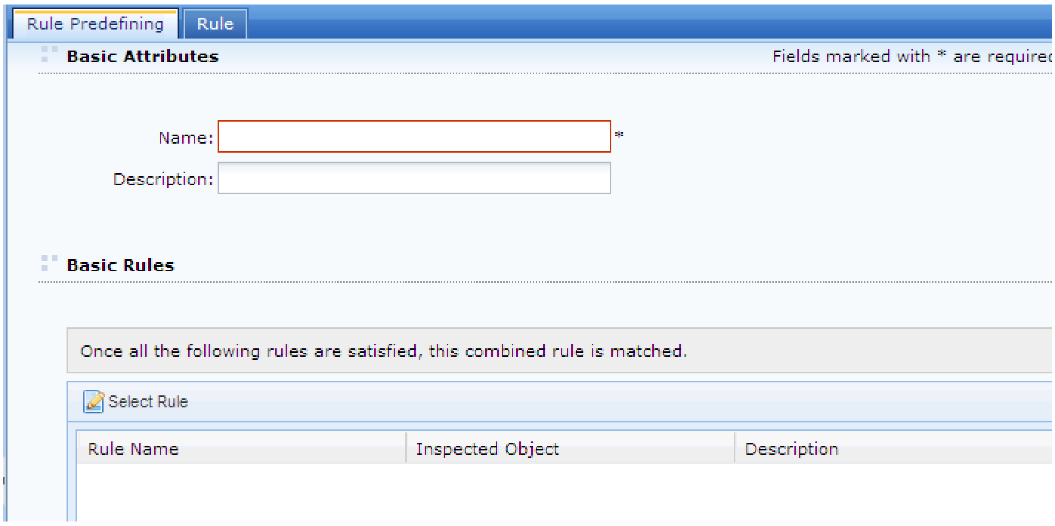
Rule Name:

Description:

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:



Basic Attributes

Fields marked with * are requirec

Name: *

Description:

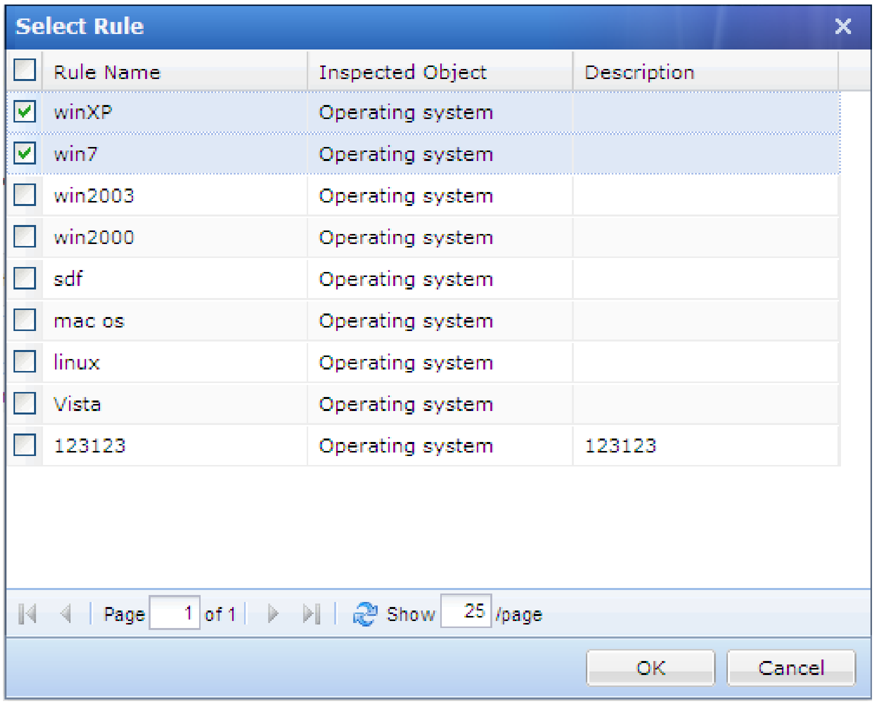
Basic Rules

Once all the following rules are satisfied, this combined rule is matched.

Rule Name	Inspected Object	Description

- **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:



Select Rule

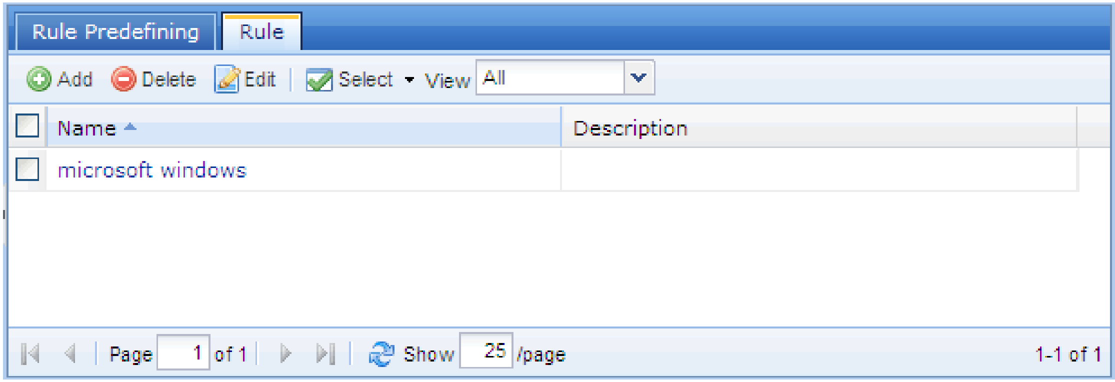
□	Rule Name	Inspected Object	Description
☑	winXP	Operating system	
☑	win7	Operating system	
□	win2003	Operating system	
□	win2000	Operating system	
□	sdf	Operating system	
□	mac os	Operating system	
□	linux	Operating system	
□	Vista	Operating system	
□	123123	Operating system	123123

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

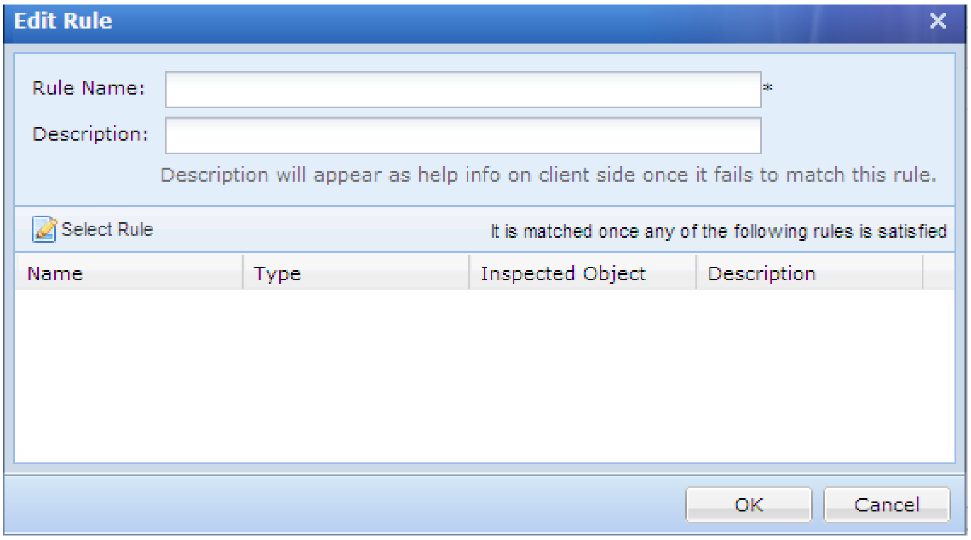
Security rule consists of basic rules and/or combined rules. When the connecting user satisfies one of these basic or combined rules, the security rule is matched. If the connecting user satisfies none of the basic or combined rules, the security rule will not be matched and user will fail the authentication check.



□	Name	Description
□	microsoft windows	

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:



Rule Name: *

Description:

Description will appear as help info on client side once it fails to match this rule.

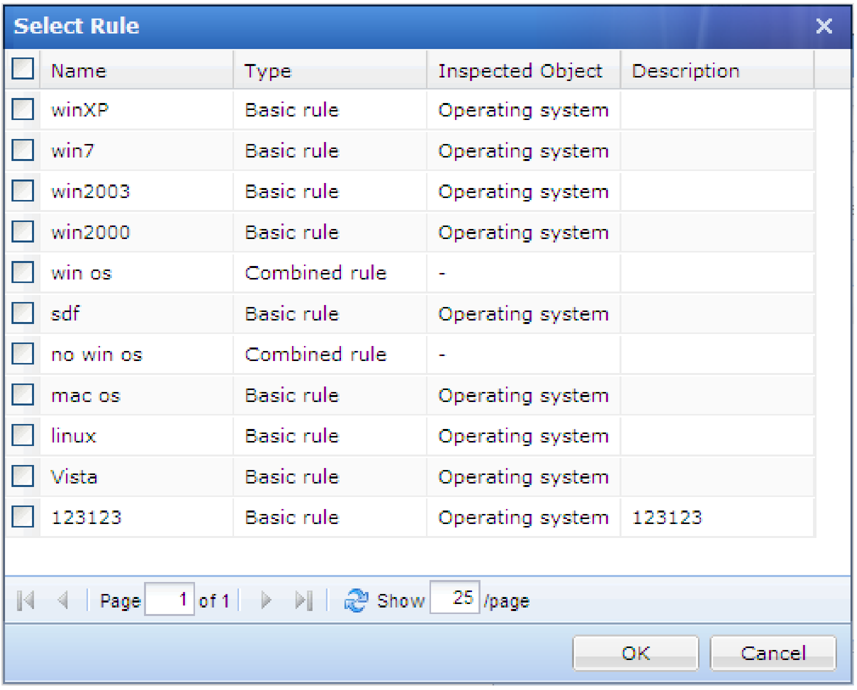
It is matched once any of the following rules is satisfied

Name	Type	Inspected Object	Description

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:



□	Name	Type	Inspected Object	Description
□	winXP	Basic rule	Operating system	
□	win7	Basic rule	Operating system	
□	win2003	Basic rule	Operating system	
□	win2000	Basic rule	Operating system	
□	win os	Combined rule	-	
□	sdf	Basic rule	Operating system	
□	no win os	Combined rule	-	
□	mac os	Basic rule	Operating system	
□	linux	Basic rule	Operating system	
□	Vista	Basic rule	Operating system	
□	123123	Basic rule	Operating system	123123

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.

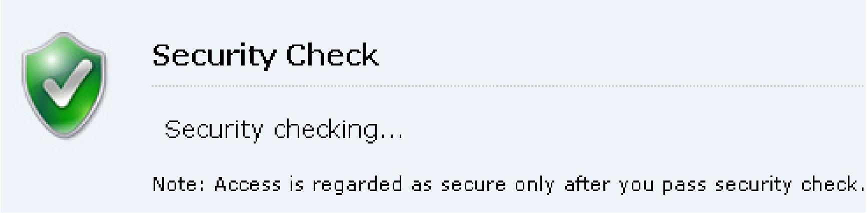
⚠

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.

Security Policy

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 toss 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:

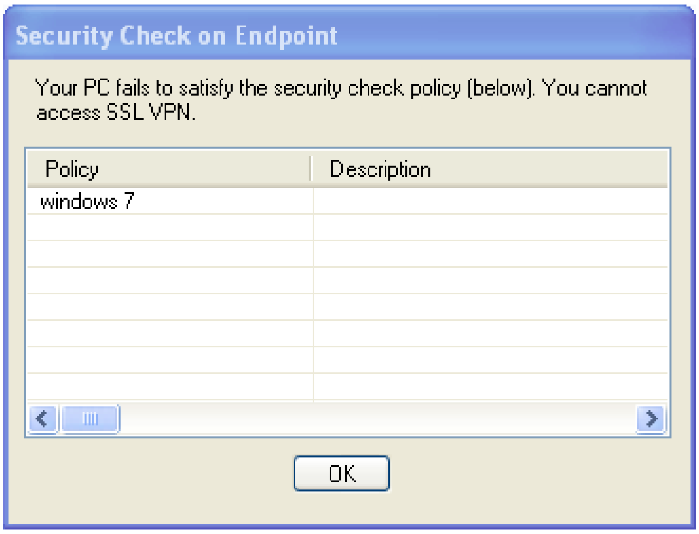


Security Check

Security checking...

Note: Access is regarded as secure only after you pass security check.

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

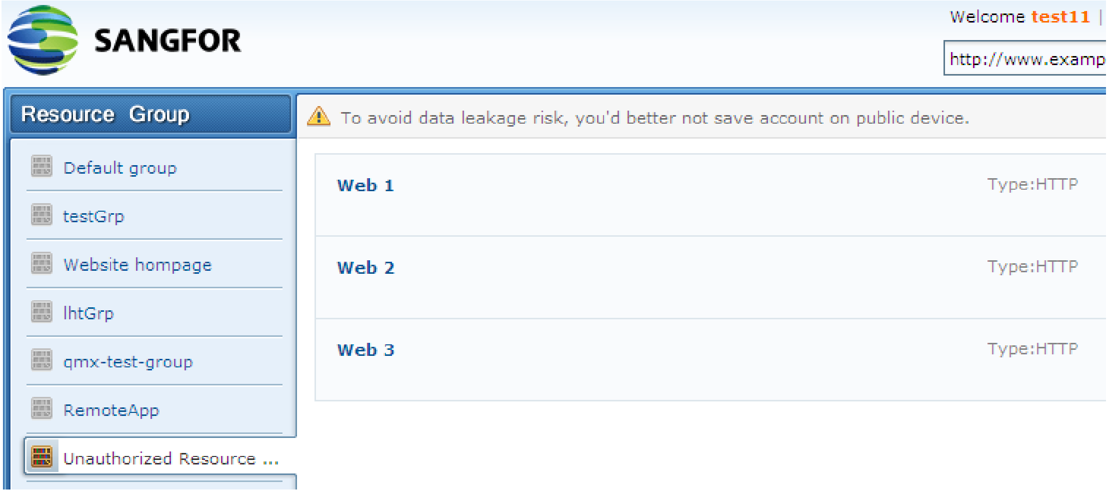


Security Check on Endpoint

Your PC fails to satisfy the security check policy (below). You cannot access SSL VPN.

Policy	Description
windows 7	

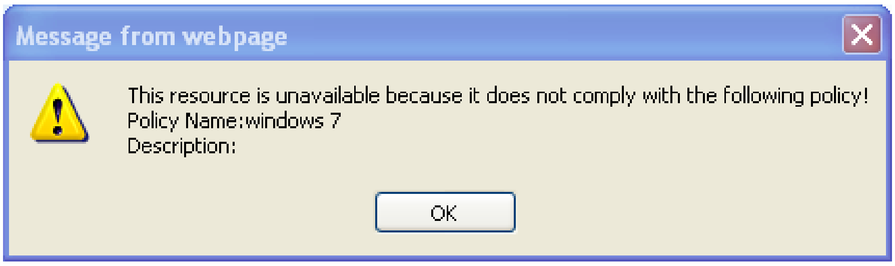
Role-level policy is applied to roles that are associated with users, and checks the endpoint when the associated users access SSL VPN (pre-authentication check) or are accessing to the resource (post-authentication check). The connecting users have to satisfy basic or combined rules included in the 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:



To avoid data leakage risk, you'd better not save account on public device.

Web 1	Type:HTTP
Web 2	Type:HTTP
Web 3	Type:HTTP

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:

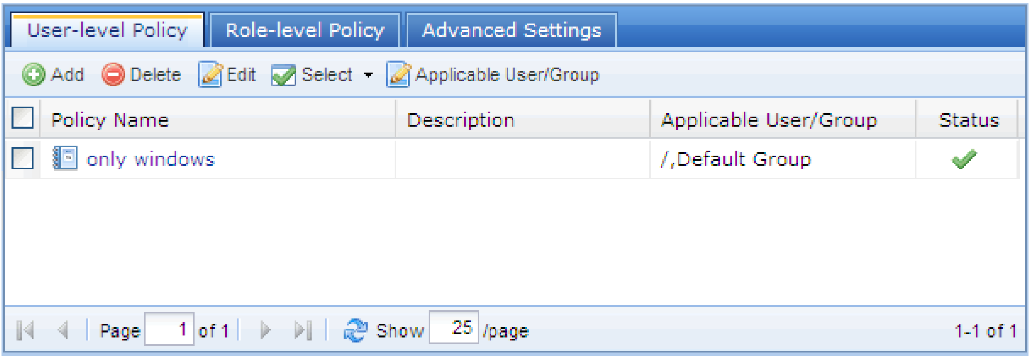


Message from webpage

This resource is unavailable because it does not comply with the following policy!
Policy Name:windows 7
Description:

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:



□	Policy Name	Description	Applicable User/Group	Status
□	only windows		/,Default Group	✓

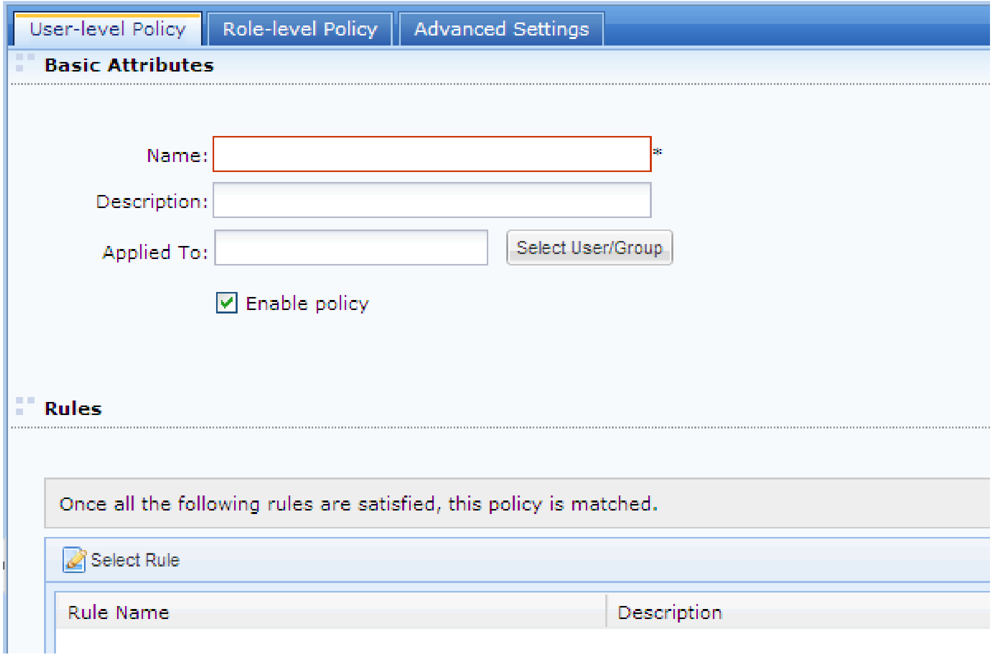
The following are the contents included on **User-level Policy** page:

- **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 User/Group:** Select and click a user-level policy to view the user and/or group to which this policy is applied. You can also selectmore users or remove user from the list.

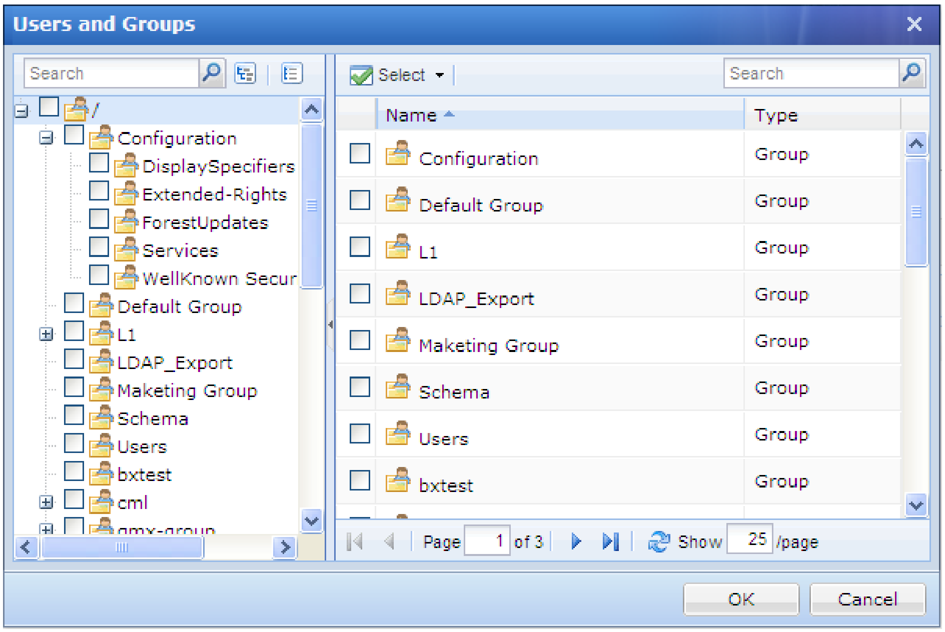
Adding User-Level Policy

1. Navigate to **SSL VPN**>**Endpoint Security**>**Policies** to enter the **User-level Policy**page andclick **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:



Name	Type
□ Configuration	Group
□ Default Group	Group
□ L1	Group
□ LDAP_Export	Group
□ Maketing Group	Group
□ Schema	Group
□ Users	Group
□ bxtest	Group

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.

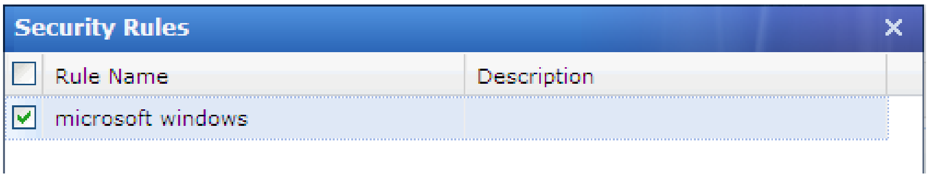
To deselect all the subgroups of a group, select the group on the left pane, click **Select**>**Group**>**Deselect all subgroups** on the right pane.

To select all the direct users of a group, select the group on the left pane, click **Select**>**User**>**Select all direct 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 direct 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:



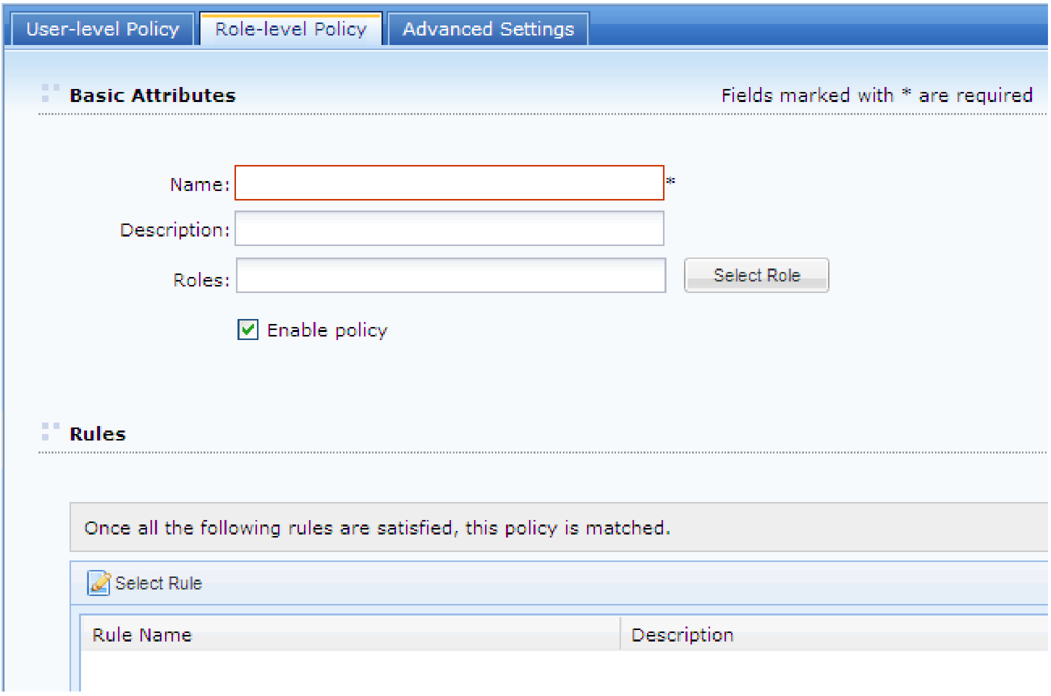
Security Rules

□ Rule Name	Description
☑ microsoft windows	

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:



Basic Attributes

Fields marked with * are required

Name: *

Description:

Roles:

☑ Enable policy

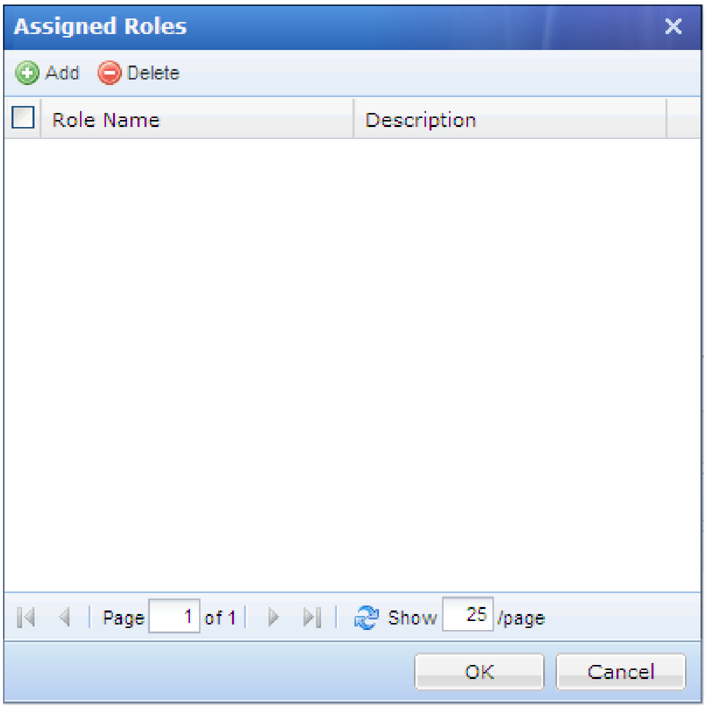
Rules

Once all the following rules are satisfied, this policy is matched.

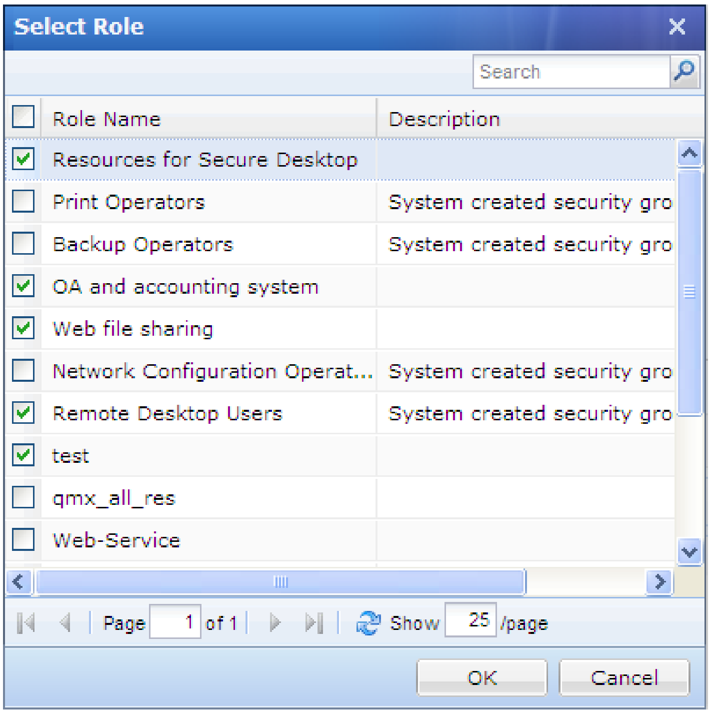
Rule Name	Description

2. Configure the **Basic Attributes** of the role-level policy. The following are basic attributes:

- **Policy 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:

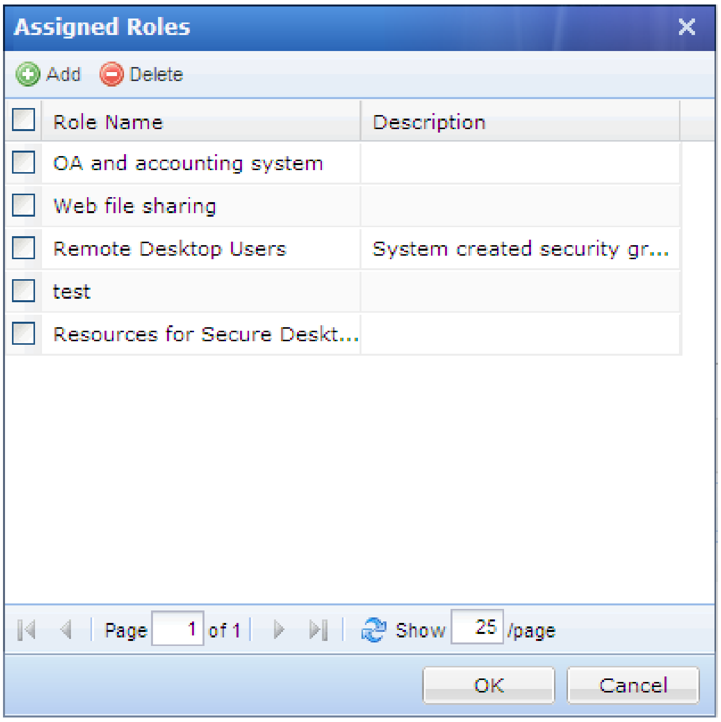


To select and add role, click **Add** to enter the **Select Role** page, as shown below:



□	Role Name	Description
☑	Resources for Secure Desktop	
□	Print Operators	System created security gro
□	Backup Operators	System created security gro
☑	OA and accounting system	
☑	Web file sharing	
□	Network Configuration Operat...	System created security gro
☑	Remote Desktop Users	System created security gro
☑	test	
□	qmx_all_res	
□	Web-Service	

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:



☐	Role Name	Description
☐	OA and accounting system	
☐	Web file sharing	
☐	Remote Desktop Users	System created security gr...
☐	test	
☐	Resources for Secure Deskt...	

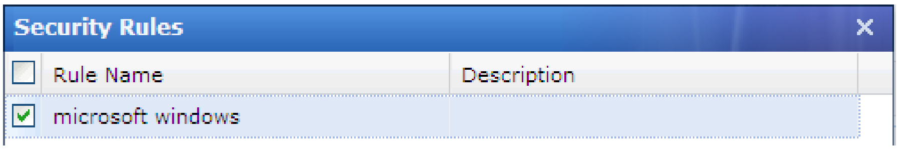
To remove a role from the list, select the role and click **Delete**.

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 sectioning Chapter 4.

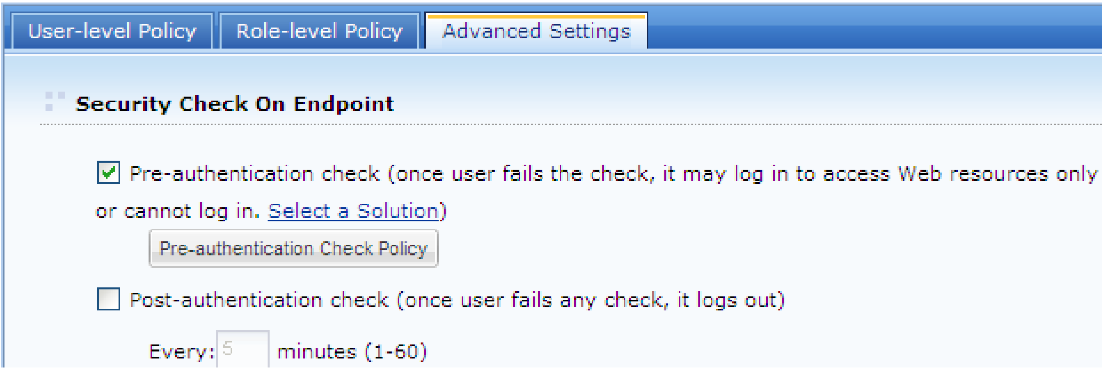
5. Specify the security rules that will be included in this policy and applied to the associated users and/or groups. Click **Select Rule** to enter the **Security Rules** page and select the rule, as shown in the figure below:



☐	Rule Name	Description
☑	microsoft windows	

6. Click the **Save** button to save the setting.

Configuring Advanced Policy Settings



Security Check On Endpoint

☑ Pre-authentication check (once user fails the check, it may log in to access Web resources only or cannot log in. Select a Solution)

Pre-authentication Check Policy

□ Post-authentication check (once user fails any check, it logs out)

Every: 5 minutes (1-60)

As mentioned above, there are pre-authentication check and post-authentication check. Post-authentication is conducted periodically after user’s login to SSL VPN or access to resource.

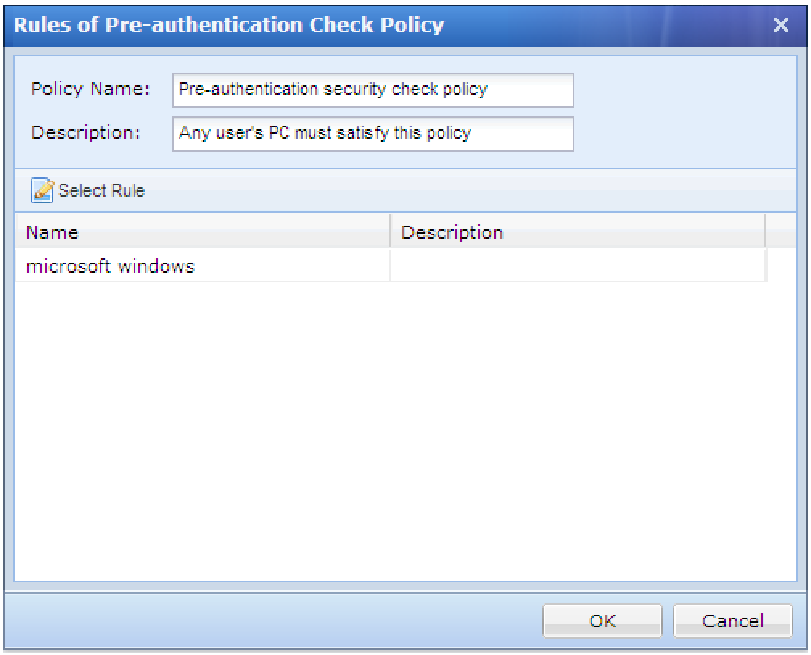
The following are the contents included on **Advanced Settings** page:

- **Pre-authentication check:** 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 may log in to access Web resources only or cannot log in. Administrator needs to click the **Select a Solution** linkto 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:



Policy Name: Pre-authentication security check policy

Description: Any user's PC must satisfy this policy

Name	Description
microsoft windows	

- **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.

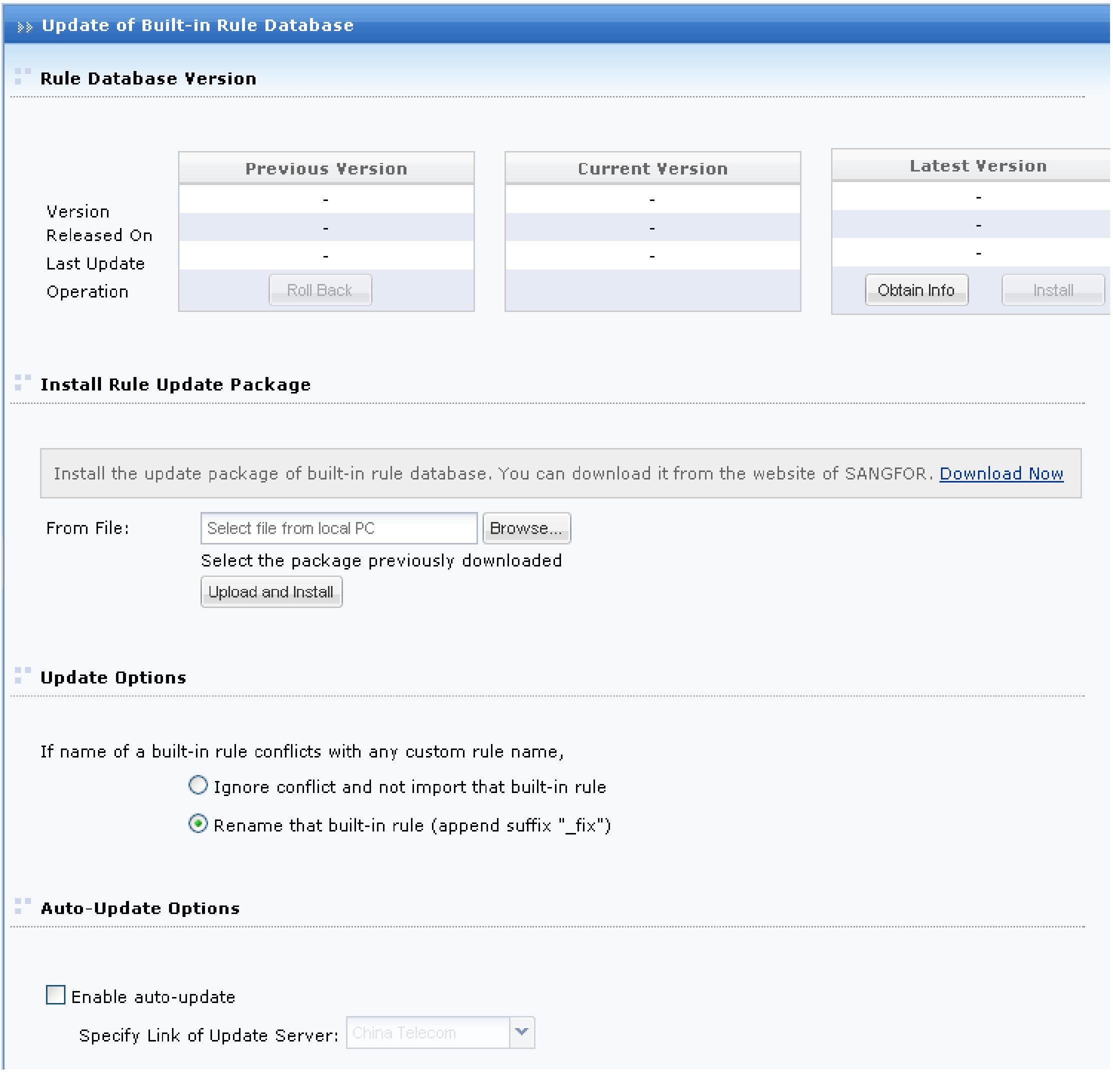
  ⚠

  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:



Update of Built-in Rule Database

Rule Database Version

	Previous Version	Current Version	Latest Version
Version	-	-	-
Released On	-	-	-
Last Update	-	-	-
Operation	Roll Back		Obtain Info Install

Install Rule Update Package

Install the update package of built-in rule database. You can download it from the website of SANGFOR. Download Now

From File: Select file from local PC Browse...

Select the package previously downloaded

Upload and Install

Update Options

If name of a built-in rule conflicts with any custom rule name,

○ Ignore conflict and not import that built-in rule

● Rename that built-in rule (append suffix "_fix")

Auto-Update Options

□ Enable auto-update

Specify Link of Update Server: China Telecom

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.

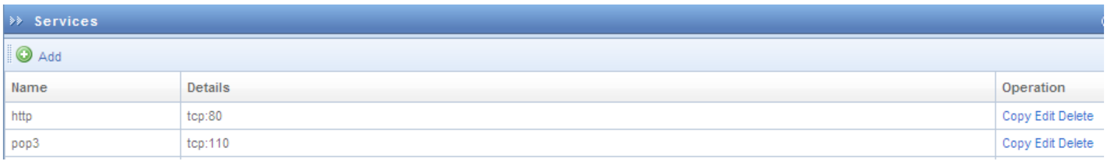
Chapter 5 Firewall

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.

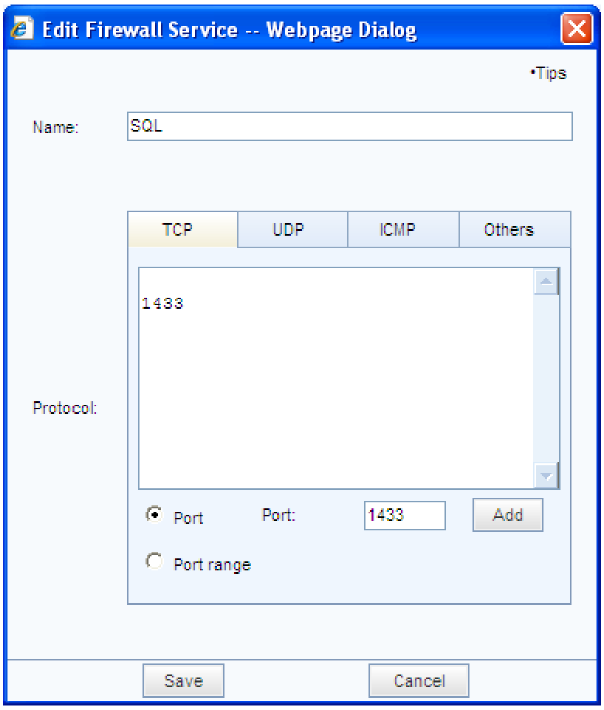
Navigate to **Firewall** > **Service** to enter the **Services** page, as shown below:



Name	Details	Operation
http	tcp:80	Copy Edit Delete
pop3	tcp:110	Copy Edit Delete

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.



Name: SQL

Protocol: TCP

1433

● Port Port: 1433

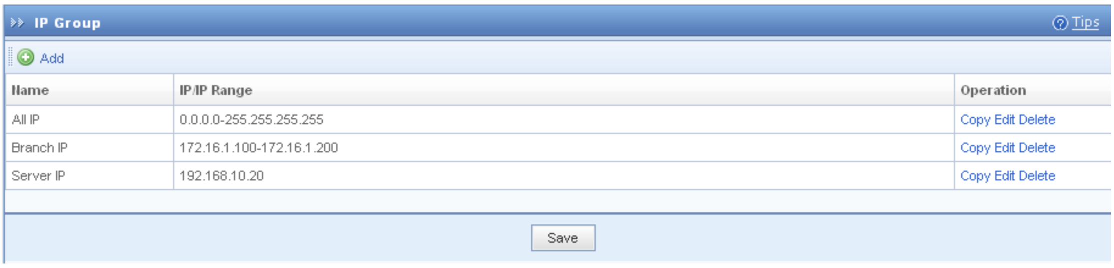
○ Port range

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.

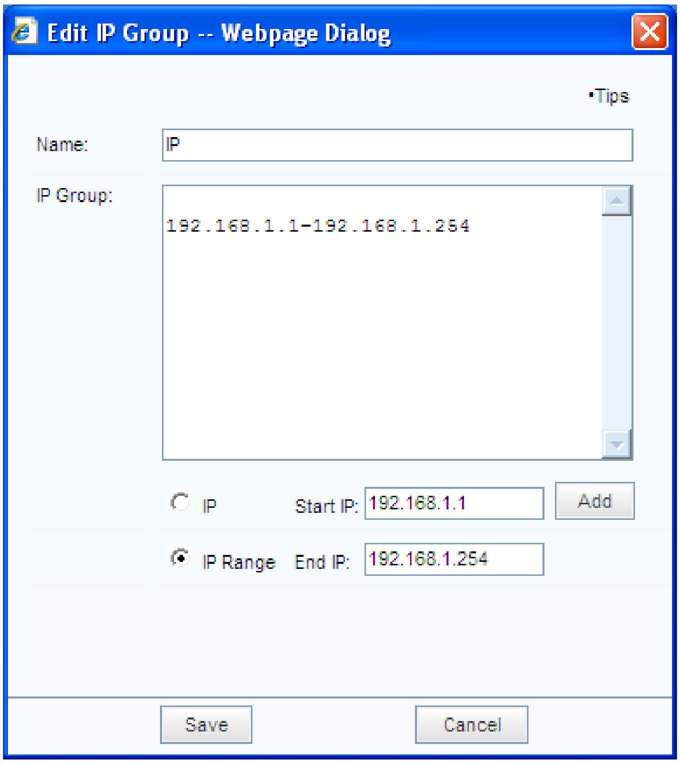
To view and define IP group, navigate to **Firewall > IP Group** to enter the **IP Group** page, as shown below:



Name	IP/IP Range	Operation
All IP	0.0.0.0-255.255.255.255	Copy Edit Delete
Branch IP	172.16.1.100-172.16.1.200	Copy Edit Delete
Server IP	192.168.10.20	Copy Edit Delete

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:



Name: IP

IP Group: 192.168.1.1-192.168.1.254

○ IP Start IP: 192.168.1.1

● IP Range End IP: 192.168.1.254

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.

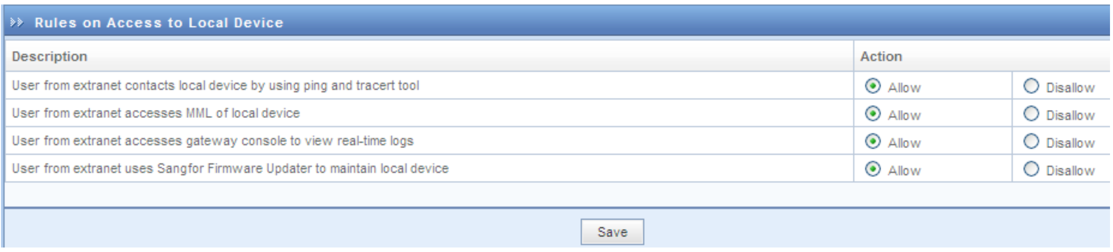
The filter rules cover the rules applied to access to the local Sangfor device, and rules applied to access among four interfaces (LAN, DMZ, WAN, VPN interfaces), including the following directions: LAN<->DMZ, DMZ<->WAN, WAN<->LAN, LAN<->LAN, DMZ<->DMZ, VPN<->WAN and VPN<->LAN.

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:



Rules on Access to Local Device

Description	Action	
User from extranet contacts local device by using ping and tracert tool	● Allow	○ Disallow
User from extranet accesses MML of local device	● Allow	○ Disallow
User from extranet accesses gateway console to view real-time logs	● Allow	○ Disallow
User from extranet uses Sangfor Firmware Updater to maintain local device	● Allow	○ Disallow

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 **Error! Reference source not found.** 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**.

Scenario 20: Configuring LAN<->DMZ Filter Rules

Purposes:

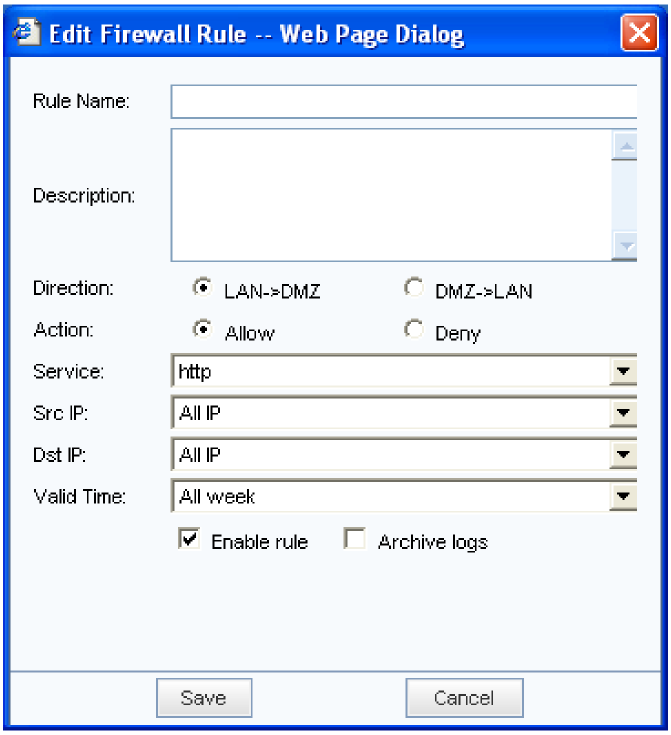
- The LAN interface and the DMZ interface can access each other.
- The Ping command can be used for testing connectivity between the LAN and DMZ interfaces.

Analysis and solution:

To achieve the above purposes, configure an LAN<->DMZ filter rule to open all the TCP, UDP and ICMP services on both directions.

To configure an LAN<->DMZ filter rule:

1. Navigate to **Firewall > Filter Rule > LAN<->DMZ** to enter the **Filter Rule (LAN<->DMZ)** page and then click **Add** to enter the **Edit Firewall Rule** page, as shown below:



Edit Firewall Rule -- Web Page Dialog

Rule Name:

Description:

Direction: ● LAN->DMZ ○ DMZ->LAN

Action: ● Allow ○ Deny

Service: http

Src IP: All IP

Dst IP: All IP

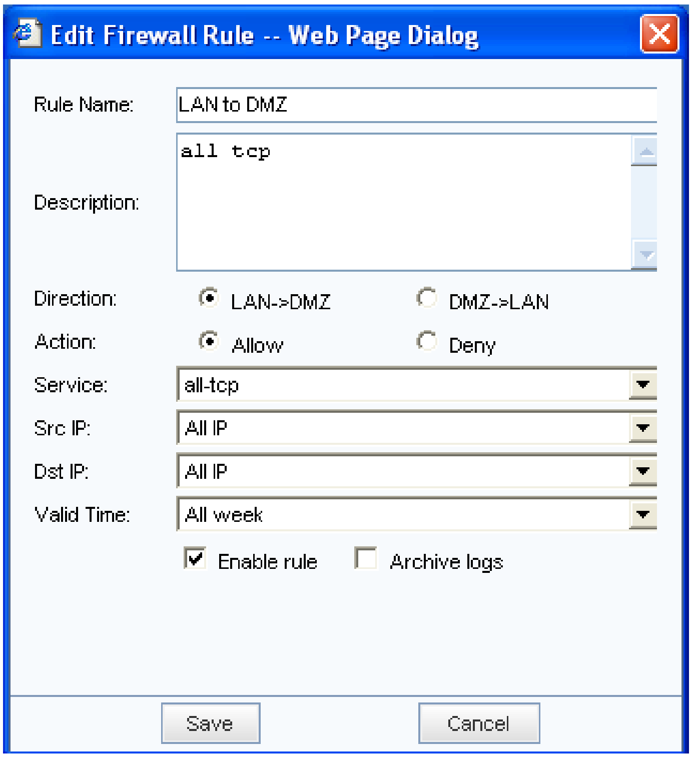
Valid Time: All week

☑ Enable rule □ Archive logs

The following are the contents included on **Edit Firewall Rule** page:

- **Rule Name**, **Description:** Enter a name and description for the rule.
- **Direction:** Select the data forwarding direction to which this filter rule applies.
- **Action:** Specify the action to be taken if packets match the criteria of this filter rule.
- **Service:** Select the service to which this filter rule applies. The services available here are predefined under **Firewall** > **Service** (please refer to the Defining Firewall Service section in Chapter 6).
- **Src IP:** Select the source IP group of the packets to which this filter rule applies. The IP groups available here are predefined under **Firewall** > **IP Group** (please refer to the Defining IP Group section in Chapter 6).
- **Dst IP:** Select the destination IP group of the packets to which this filter rule applies. The IP groups available here are predefined under **Firewall** > **IP Group** (please refer to the Defining IP Group section in Chapter 6).
- **Valid Time:** Select a schedule in which this filter rule is in effect. The schedules available here are predefined under **System** > **Schedule** (please refer to Schedules section in Chapter 3).
- **Enable rule:** Select it to enable the current filter rule.
- **Archive logs:** Select it to enable the corresponding firewall log, and the system will record the logs if the data packets matching this filter rule go through the Sangfor device. Generally, it is recommended to uncheck this option to avoid massive logs.

2. Configure a filter rule applicable to data sent from LAN to DMZ, as shown below:



Edit Firewall Rule -- Web Page Dialog

Rule Name: LAN to DMZ

Description: all tcp

Direction: ● LAN->DMZ ○ DMZ->LAN

Action: ● Allow ○ Deny

Service: all-tcp

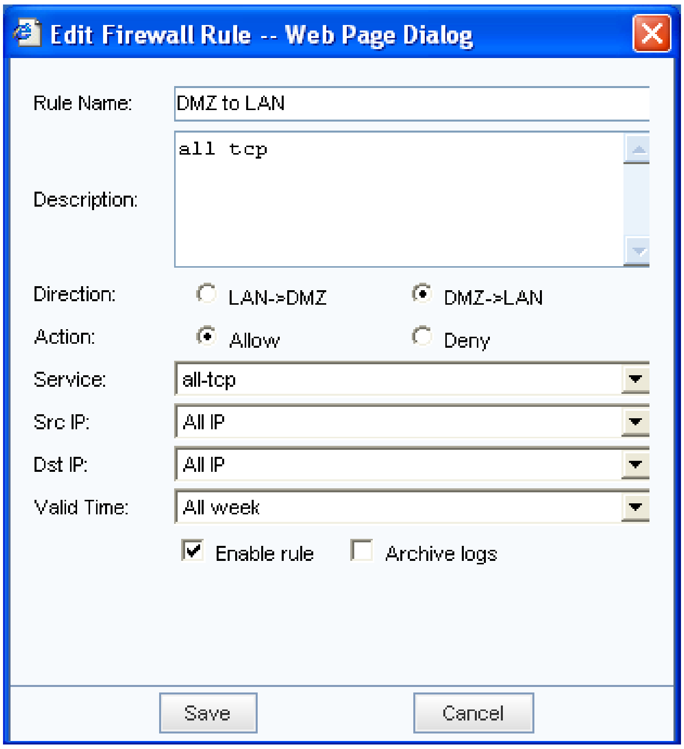
Src IP: All IP

Dst IP: All IP

Valid Time: All week

☑ Enable rule □ Archive logs

3. Configure a filter rule applicable to data sent from DMZ to LAN, as shown below:



Edit Firewall Rule -- Web Page Dialog

Rule Name: DMZ to LAN

Description: all tcp

Direction: ○ LAN->DMZ ● DMZ->LAN

Action: ● Allow ○ Deny

Service: all-tcp

Src IP: All IP

Dst IP: All IP

Valid Time: All week

☑ Enable rule □ Archive logs

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

Scenario 21: Configuring LAN<->VPN Filter Rules

Background:

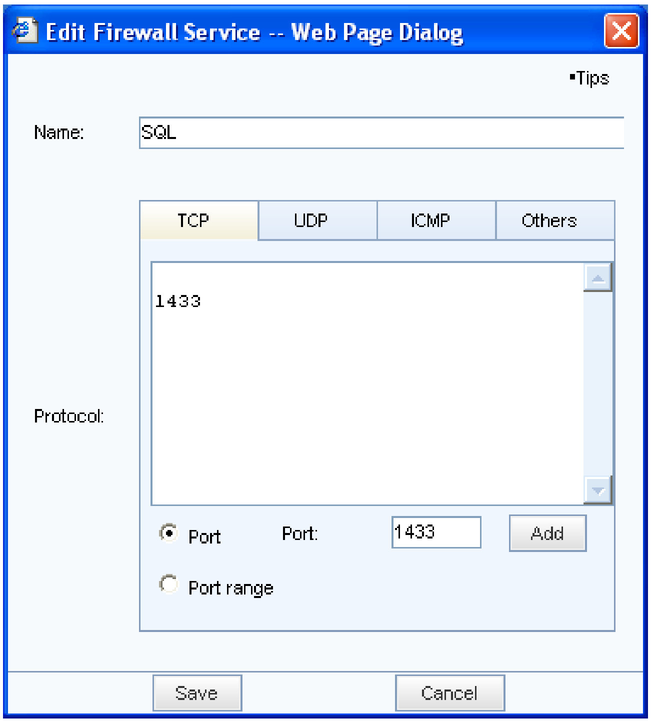
- The branch (172.16.1.0/24) has established VPN connection with the Headquarters.
- There is a server (192.168.10.20) located at Headquarters, providing Web service and SQL SERVER service.

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** > **Service** to define the SQL Server service.



Edit Firewall Service -- Web Page Dialog

Name: SQL

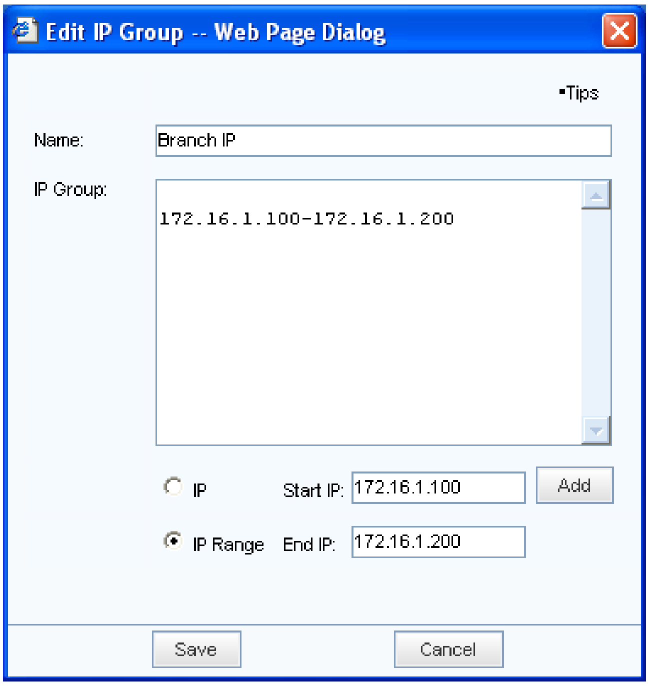
Protocol:

1433

● Port Port: 1433

○ Port range

2. Navigate to **Firewall** > **IP Group** to define two IP groups, as shown below:



Edit IP Group -- Web Page Dialog

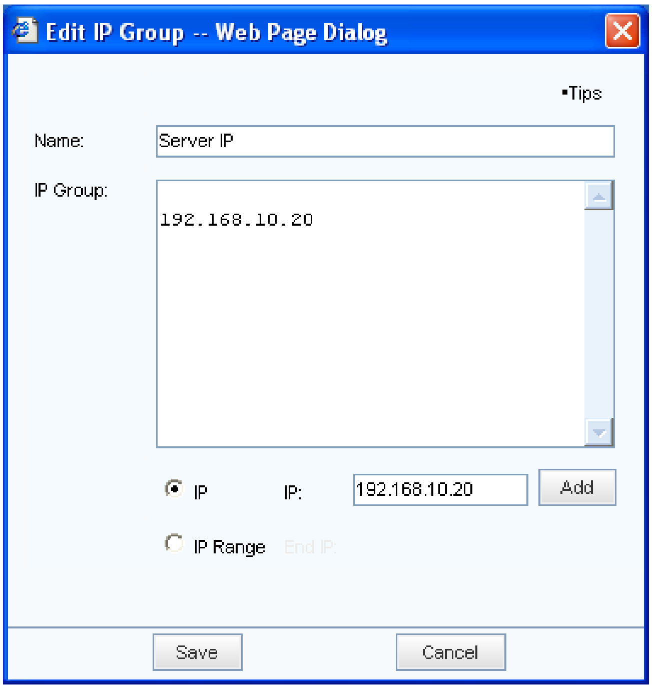
▪Tips

Name: Branch IP

IP Group: 172.16.1.100-172.16.1.200

○ IP Start IP: 172.16.1.100 Add

● IP Range End IP: 172.16.1.200



Edit IP Group -- Web Page Dialog

▪Tips

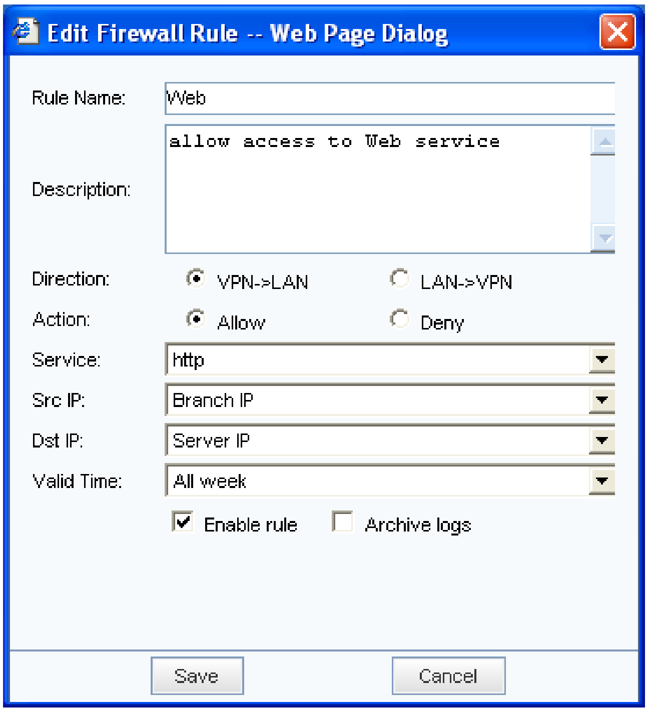
Name: Server IP

IP Group: 192.168.10.20

● IP IP: 192.168.10.20 Add

○ IP Range End IP:

3. Configure the filter rule for Web service, as shown below:



Edit Firewall Rule -- Web Page Dialog

Rule Name: Web

Description: allow access to Web service

Direction: ● VPN->LAN ○ LAN->VPN

Action: ● Allow ○ Deny

Service: http

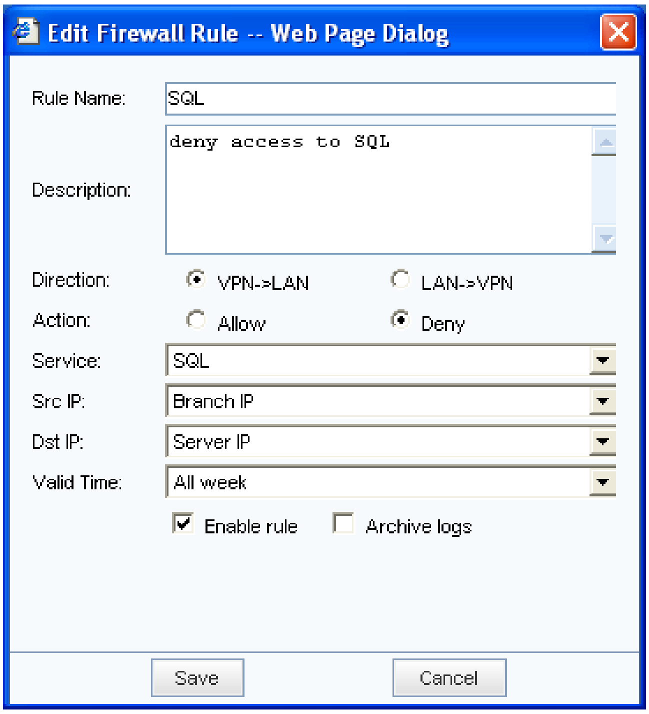
Src IP: Branch IP

Dst IP: Server IP

Valid Time: All week

☑ Enable rule □ Archive logs

4. Configure the filter rule for SQL Server service, as shown below:



Edit Firewall Rule -- Web Page Dialog

Rule Name: SQL

Description: deny access to SQL

Direction: ● VPN->LAN ○ LAN->VPN

Action: ○ Allow ● Deny

Service: SQL

Src IP: Branch IP

Dst IP: Server IP

Valid Time: All week

☑ Enable rule □ Archive logs

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.

Configuring NAT Rule

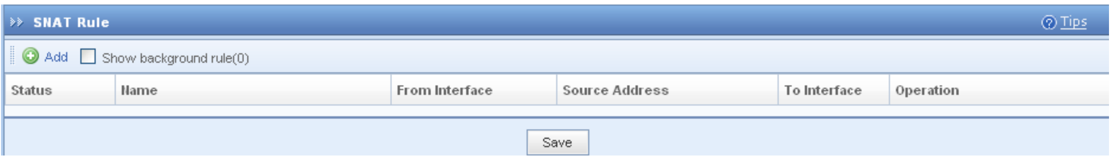
The NAT module covers the following configurations: **SNAT Rule**, **DNAT Rule**, **IP/MAC Binding**, **HTTP Port**, **URL Group**, **WAN Service** and **Access Right of Local Users**.

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 **SANT Rule** page, as shown below:



Status	Name	From Interface	Source Address	To Interface	Operation

Scenario 22: Adding SNAT Rule

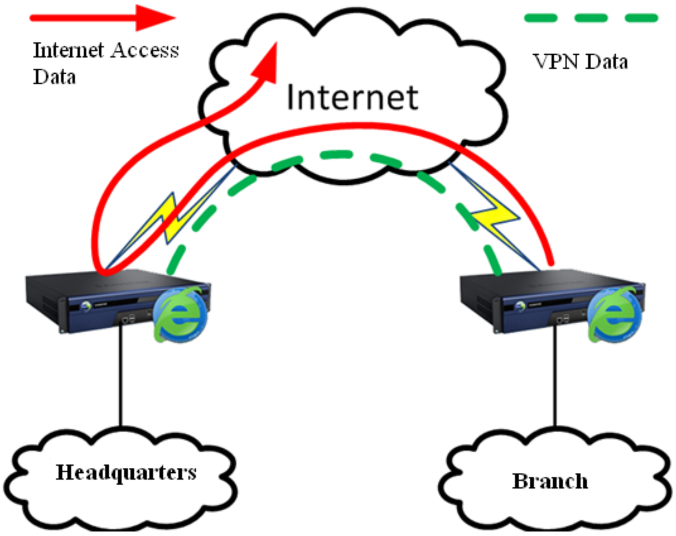
Background:

- The Sangfor device located at Headquarters is deployed in Route mode.
- The branch has established VPN connection with the Headquarters.

Purpose:

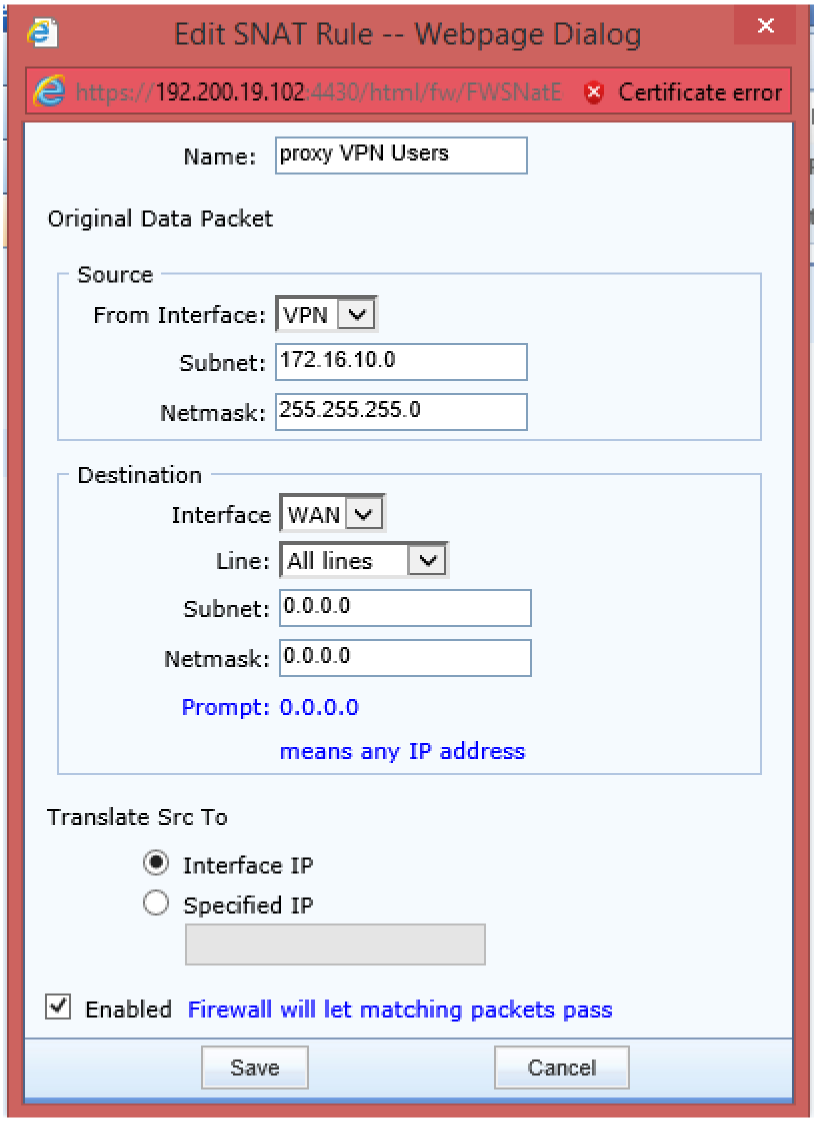
Configure a SNAT rule on the Sangfor device located at headquarters, so that users from branch (172.16.10.0/24) can access Internet after connecting to Headquarters through VPN connection.

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


Edit SNAT Rule -- Webpage Dialog
https://192.200.19.102:4430/html/fw/FWSNatE
Certificate error

Name: proxy VPN Users

Original Data Packet

Source

From Interface: VPN

Subnet: 172.16.10.0

Netmask: 255.255.255.0

Destination

Interface WAN

Line: All lines

Subnet: 0.0.0.0

Netmask: 0.0.0.0

Prompt: 0.0.0.0 means any IP address

Translate Src To

● Interface IP

○ Specified IP

☑ Enabled Firewall will let matching packets pass

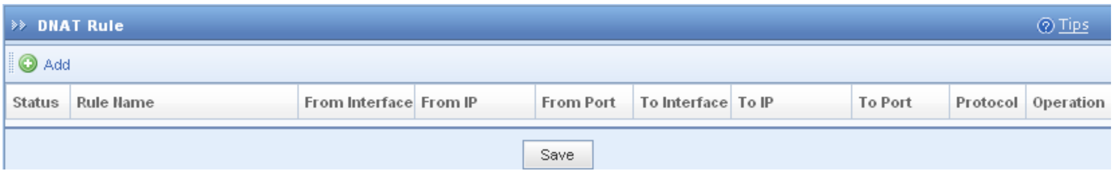
2. Configure the SNAT rule as shown in the figure above, ingress interface being VPN and source address being the LAN subnet of the branch.

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

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:



Status	Rule Name	From Interface	From IP	From Port	To Interface	To IP	To Port	Protocol	Operation

Scenario 23: Adding DNAT Rule

Background:

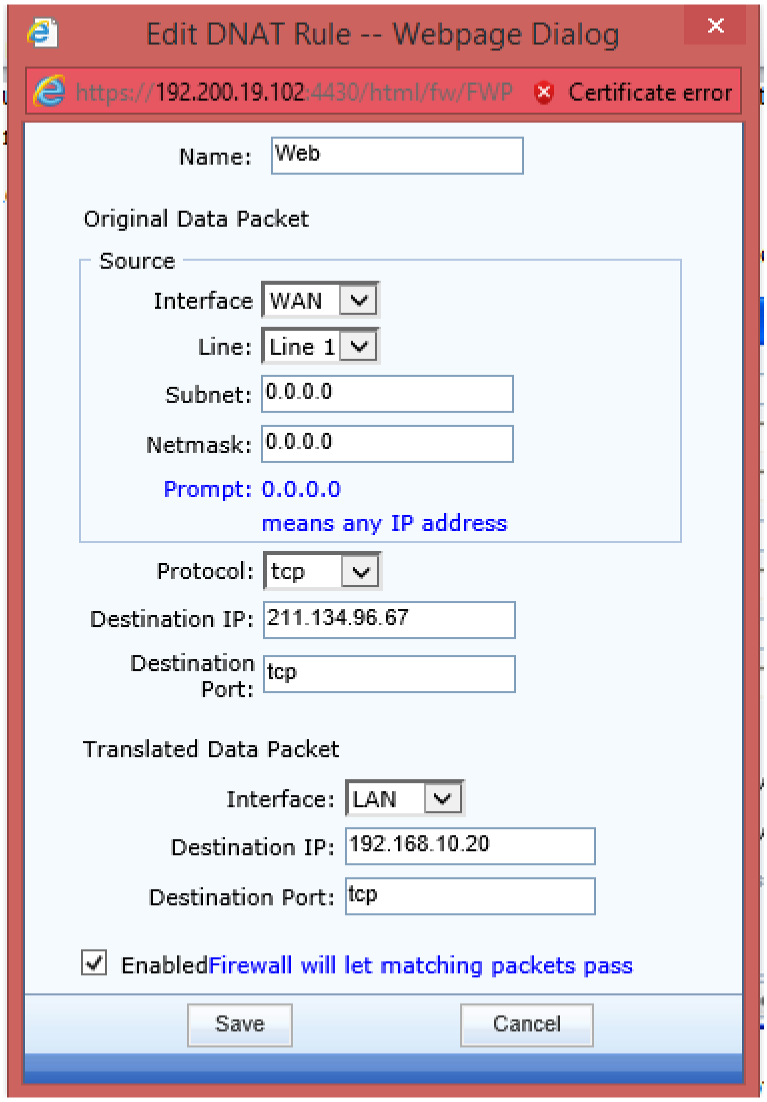
There is a LAN server (IP address: 192.168.10.20) providing Web service through the port 80.

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:


Edit DNAT Rule -- Webpage Dialog
https://192.200.19.102:4430/html/fw/FWP
Certificate error
Save
Cancel

Name: Web

Original Data Packet

Source

Interface WAN

Line: Line 1

Subnet: 0.0.0.0

Netmask: 0.0.0.0

Prompt: 0.0.0.0 means any IP address

Protocol: tcp

Destination IP: 211.134.96.67

Destination Port: tcp

Translated Data Packet

Interface: LAN

Destination IP: 192.168.10.20

Destination Port: tcp

☑ EnabledFirewall will let matching packets pass

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.

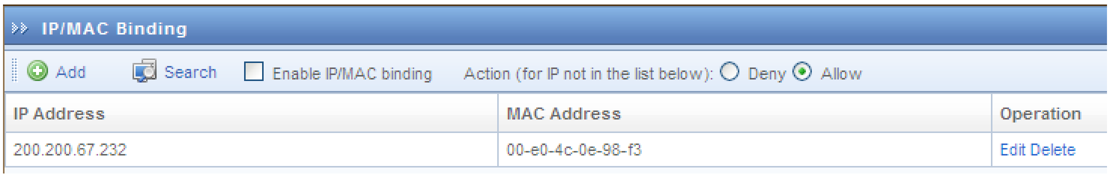
To have the LAN server accessed by Internet users through configuring DNAT rules on the Sangfor device, the Sangfor device must act as gateway of the LAN computers or router to external network; otherwise, the DNAT rule will not work.

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:



IP/MAC Binding

Add Search □ Enable IP/MAC binding Action (for IP not in the list below): ○ Deny ● Allow

IP Address	MAC Address	Operation
200.200.67.232	00-e0-4c-0e-98-f3	Edit Delete

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)**.

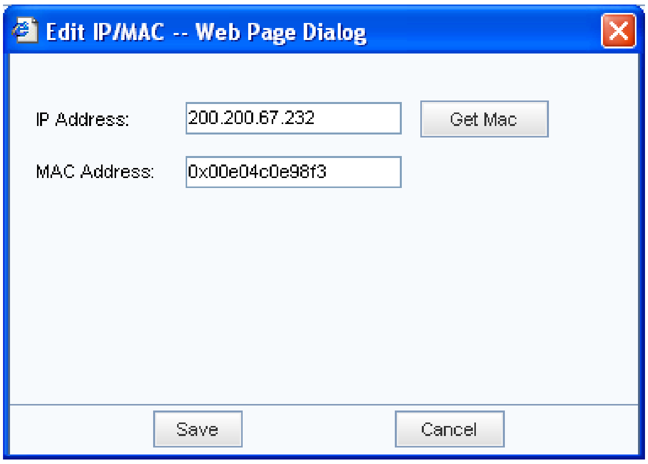
The **Action (for IP not in the list below)** option specifies the action to be taken for Internet access requests initiated by internal users whose IP/MAC addresses are not in the IP/MAC binding list. There are two actions:

- **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:



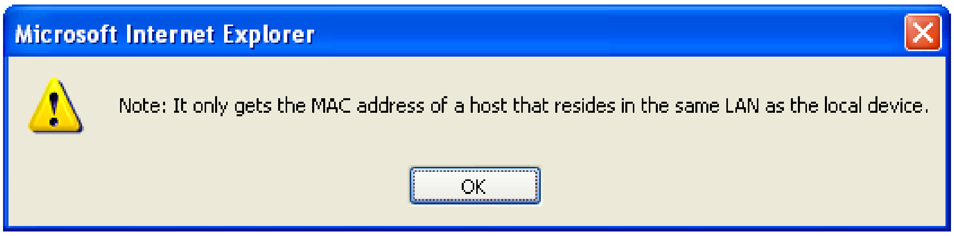
Edit IP/MAC -- Web Page Dialog

IP Address: 200.200.67.232

MAC Address: 0x00e04c0e98f3

The search for IP/MAC addresses of the internal computers, perform the following steps:

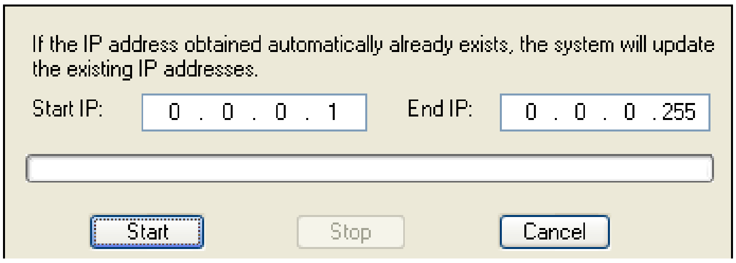
1. Click **Search** and the following prompt appears.



Microsoft Internet Explorer

Note: It only gets the MAC address of a host that resides in the same LAN as the local device.

2. Click **OK** and the following dialog appears.



If the IP address obtained automatically already exists, the system will update the existing IP addresses.

Start IP: 0 . 0 . 0 . 1 End IP: 0 . 0 . 0 . 255

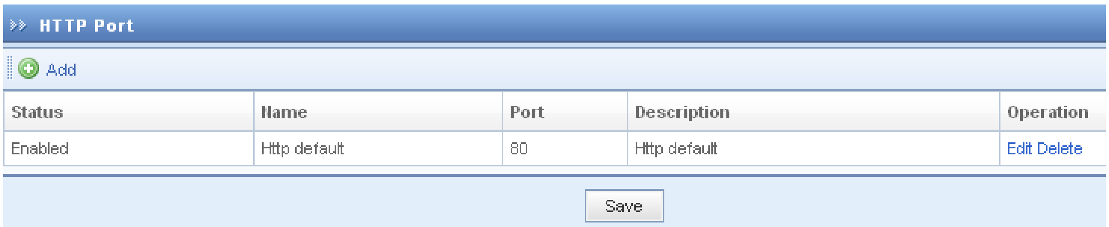
3. Enter the IP range and then click **Start**.

The IP/MAC binding function is unavailable in a layer-3 switched environment.

Configuring HTTP Port

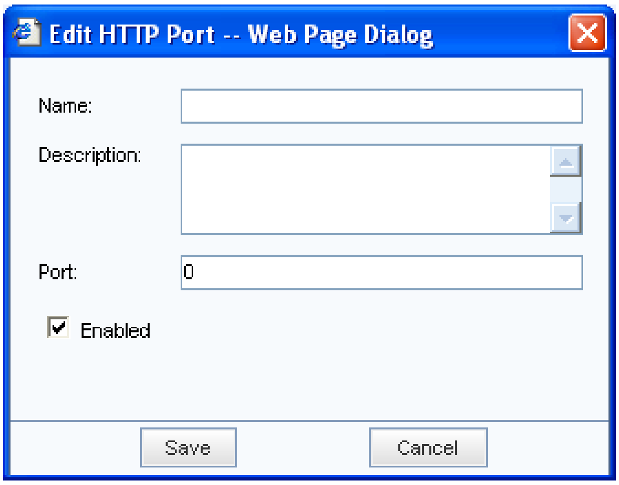
The **HTTP Port** page enables you to define the HTTP service port. By default, it is port 80. If the **Enable URL access** option is selected in **Firewall** > **NAT** > **Access Right** > **Access Right of Local Users**, the Sangfor device will record the information of the URL accessed by users through 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:



Status	Name	Port	Description	Operation
Enabled	Http default	80	Http default	Edit Delete

To add an HTTP port, click **Add** to open the following dialog, and then specify the corresponding information.



Name:

Description:

Port: 0

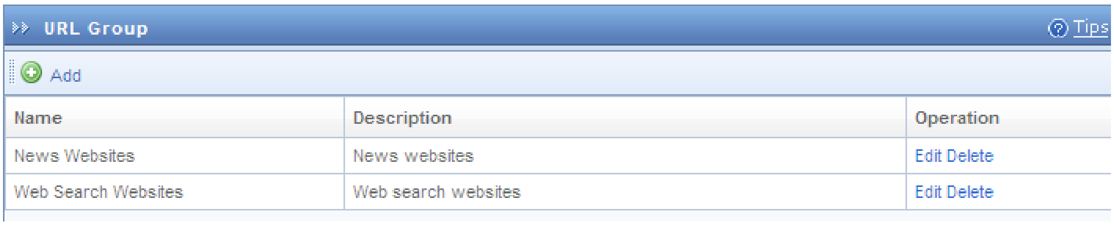
☑ Enabled

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.

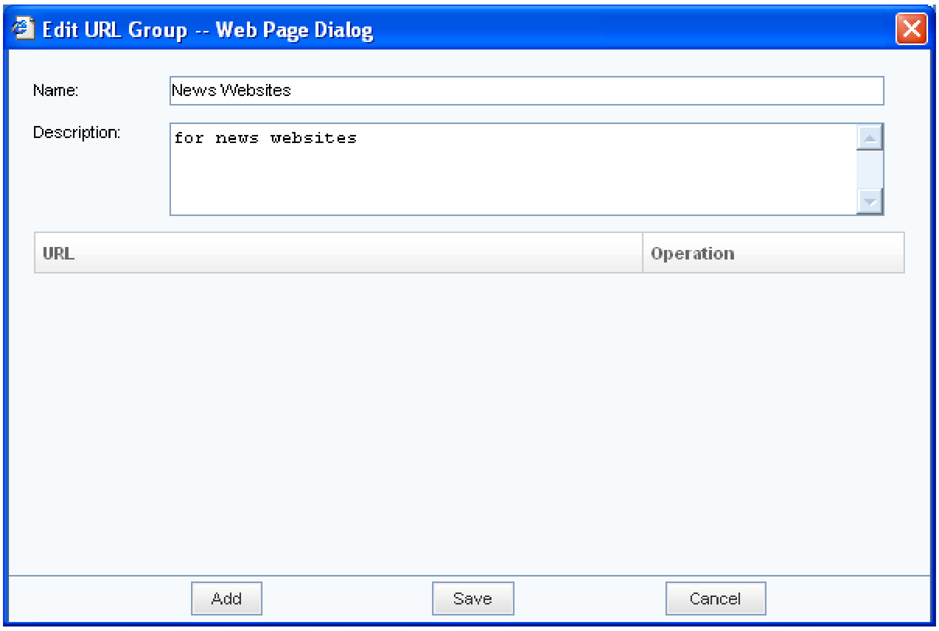
Navigate to **Firewall** > **NAT** > **URL Group** to enter the **URL Group** page, as shown below:



Name	Description	Operation
News Websites	News websites	Edit Delete
Web Search Websites	Web search websites	Edit Delete

To add a URL group:

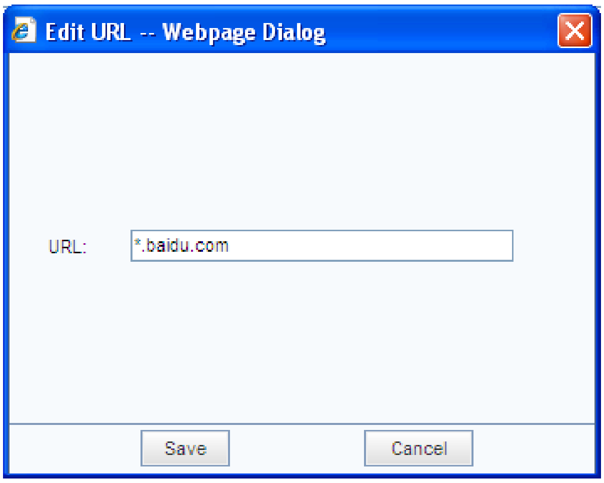
1. Click **Add** to enter the **Edit URL Group** page, and then enter a name and description for the URL group, as shown below:



Name: News Websites

Description: for news websites

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.



URL: *.baidu.com

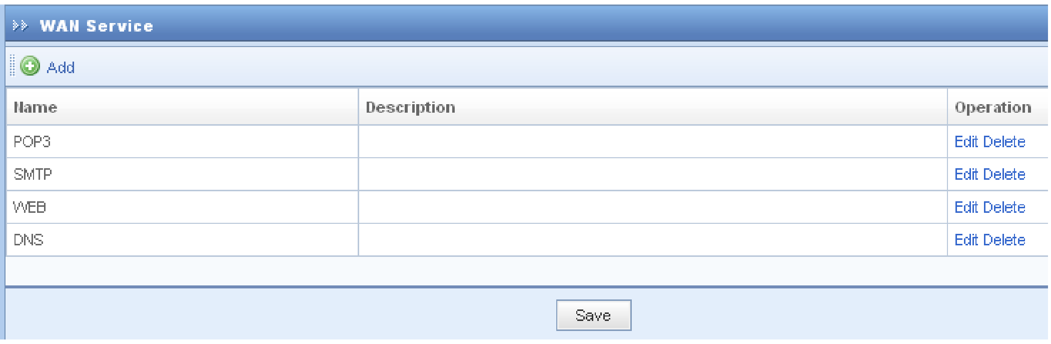
3. Click the **Save** button on the **URL Group** page to save the settings.

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.

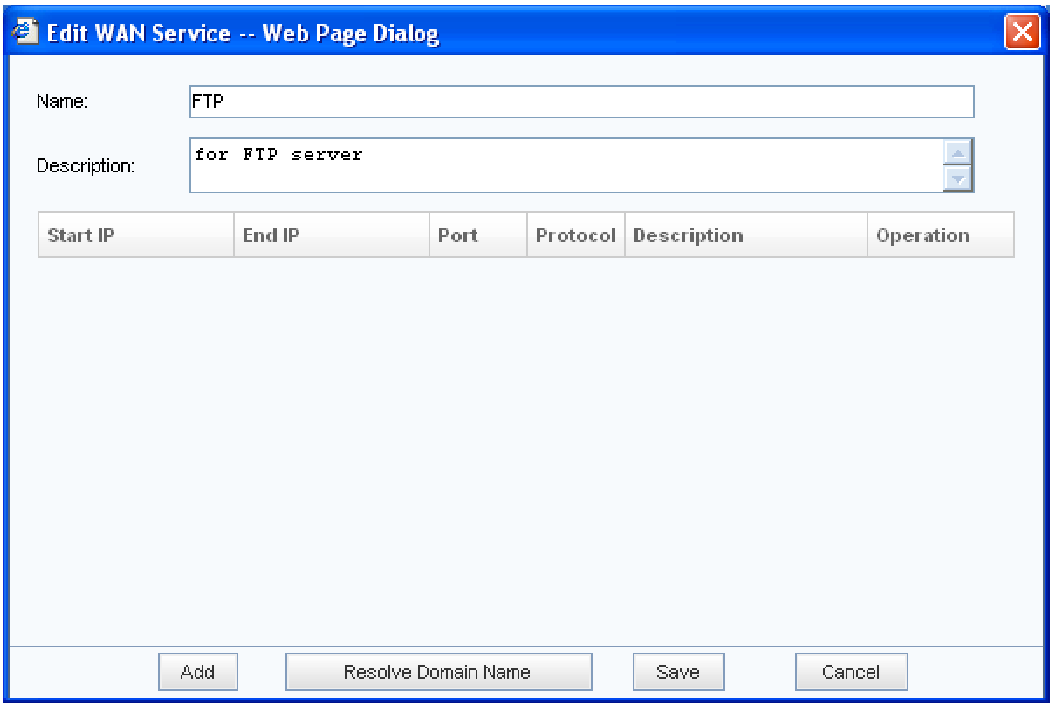
By default, four types of services are already defined, namely, POP3, SMTP, WEB and DNS. If any other service is needed, define it according to the specific case. For example, to add the FTP service provided by the server (Internet IP address is 202.96.137.75; ports is 20-21), perform the following steps:

1. Navigate to **Firewall** > **NAT** > **WAN Service** to enter the **WAN Service** page, as shown below:



Name	Description	Operation
POP3		Edit Delete
SMTP		Edit Delete
WEB		Edit Delete
DNS		Edit Delete

2. Click **Add** to enter the **Edit WAN Service** page, and then enter a name and description for the entry, as shown below:

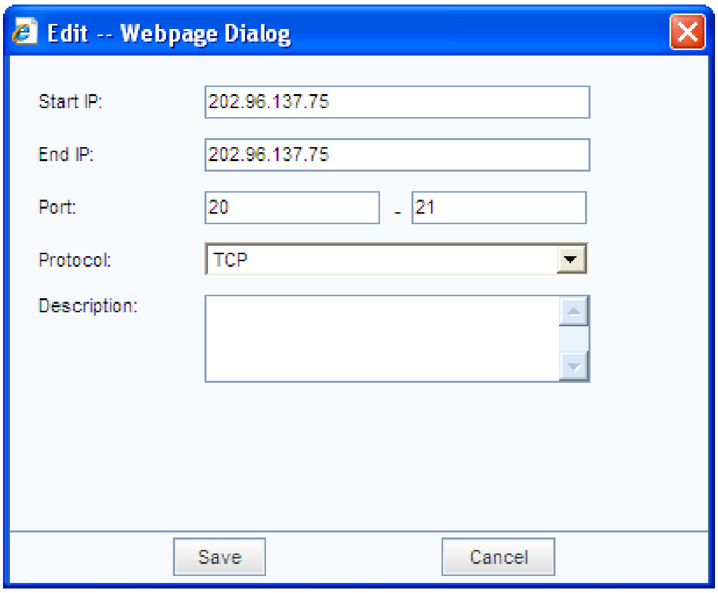


Name: FTP

Description: for FTP server

Start IP	End IP	Port	Protocol	Description	Operation

3. Click **Add** on the **Edit WAN Service** page to specify the IP addresses and port of the external FTP server, as shown below:



Edit -- Webpage Dialog

Start IP: 202.96.137.75

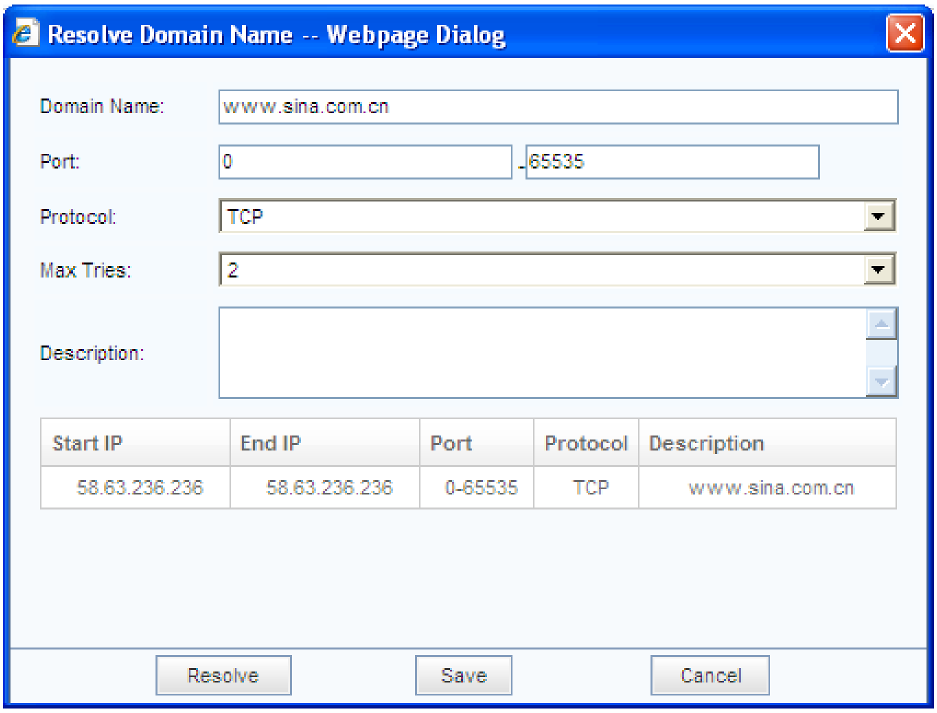
End IP: 202.96.137.75

Port: 20 - 21

Protocol: TCP

Description:

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:



Resolve Domain Name -- Webpage Dialog

Domain Name: www.sina.com.cn

Port: 0 - 65535

Protocol: TCP

Max Tries: 2

Description:

Start IP	End IP	Port	Protocol	Description
58.63.236.236	58.63.236.236	0-65535	TCP	www.sina.com.cn

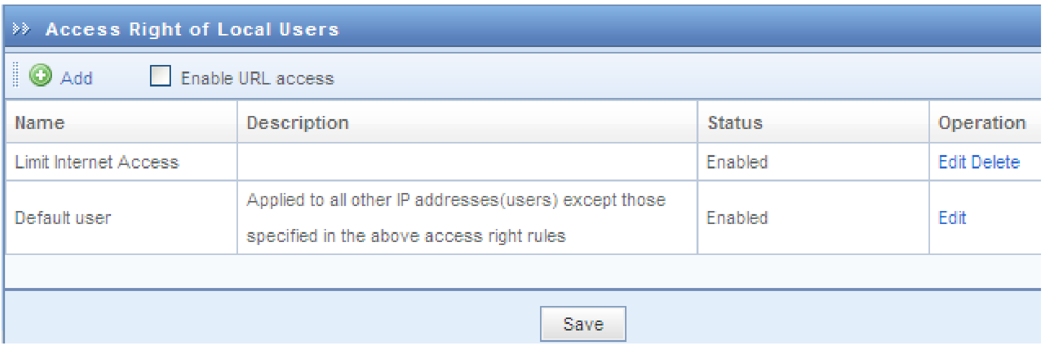
5. Click the **Save** buttons to save the settings.

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:

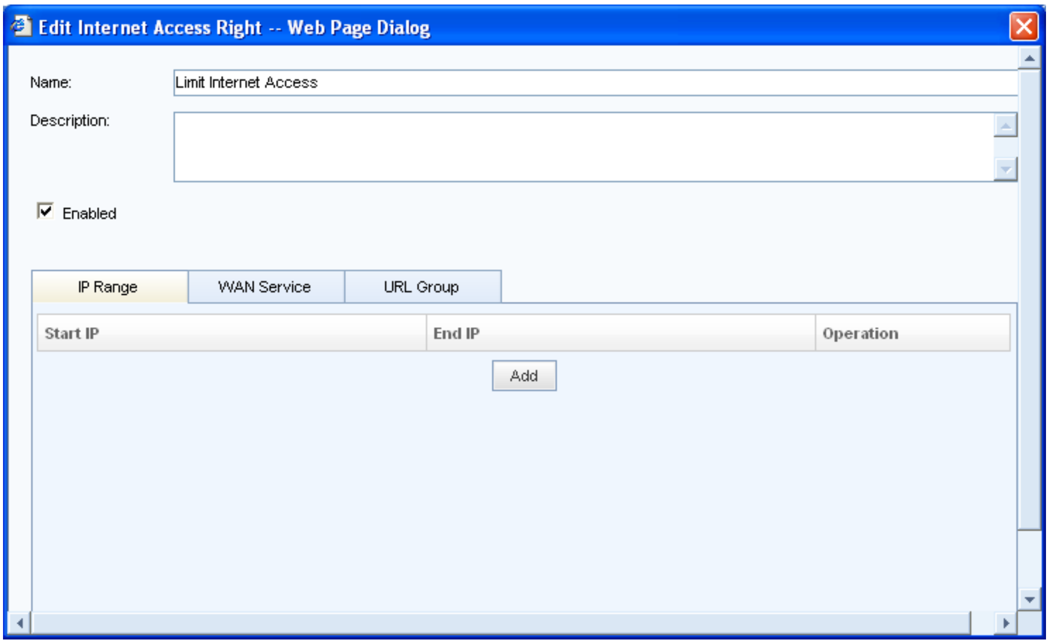


Access Right of Local Users

Add □ Enable URL access

Name	Description	Status	Operation
Limit Internet Access		Enabled	Edit Delete
Default user	Applied to all other IP addresses(users) except those specified in the above access right rules	Enabled	Edit

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:



Edit Internet Access Right -- Web Page Dialog

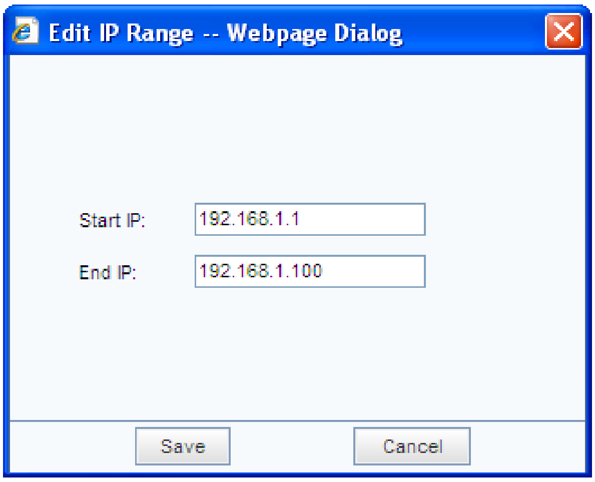
Name: Limit Internet Access

Description:

☑ Enabled

Start IP	End IP	Operation

4. Click the **Add** button on the **IP Range** tab and enter the LAN IP addresses applicable to this rule, as shown below:

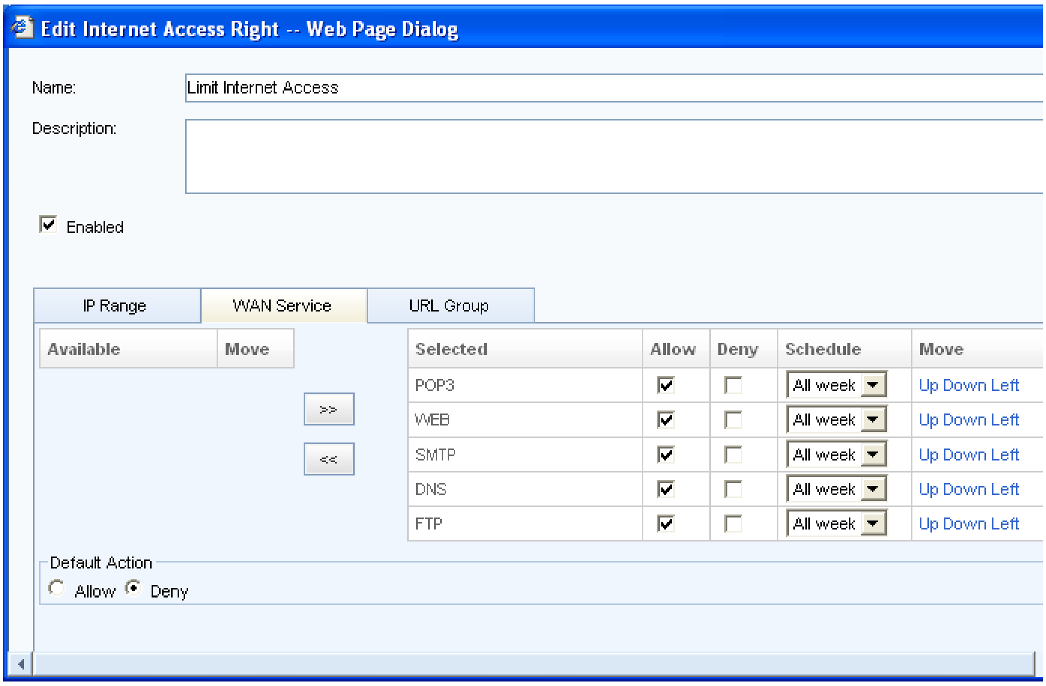


Edit IP Range -- Webpage Dialog

Start IP: 192.168.1.1

End IP: 192.168.1.100

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. In the following example, as shown below, the applicable LAN users can only access the POP3, SMTP, WEB, DNS and FTP services (access to other services will be denied).



Edit Internet Access Right -- Web Page Dialog

Name: Limit Internet Access

Description:

☑ Enabled

Available	Move

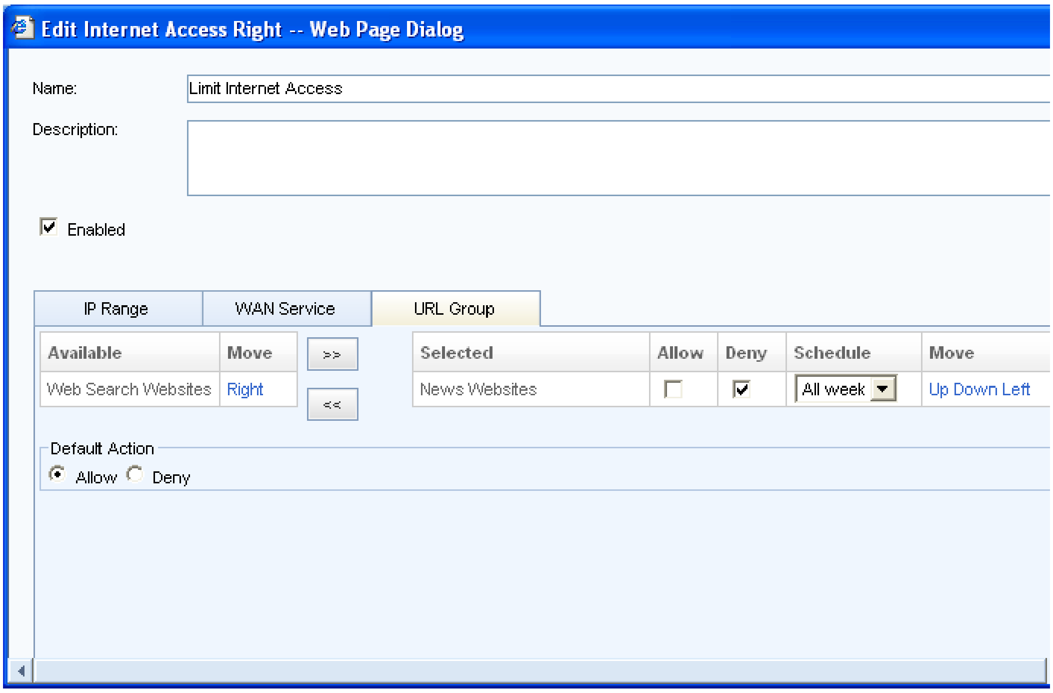
Selected	Allow	Deny	Schedule	Move
POP3	☑	□	All week	Up Down Left
WEB	☑	□	All week	Up Down Left
SMTP	☑	□	All week	Up Down Left
DNS	☑	□	All week	Up Down Left
FTP	☑	□	All week	Up Down Left

Default Action

○ Allow ● Deny

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**.



Edit Internet Access Right -- Web Page Dialog

Name: Limit Internet Access

Description:

☑ Enabled

Available	Move
Web Search Websites	Right

Selected	Allow	Deny	Schedule	Move
News Websites	□	☑	All week	Up Down Left

Default Action
● Allow ○ Deny

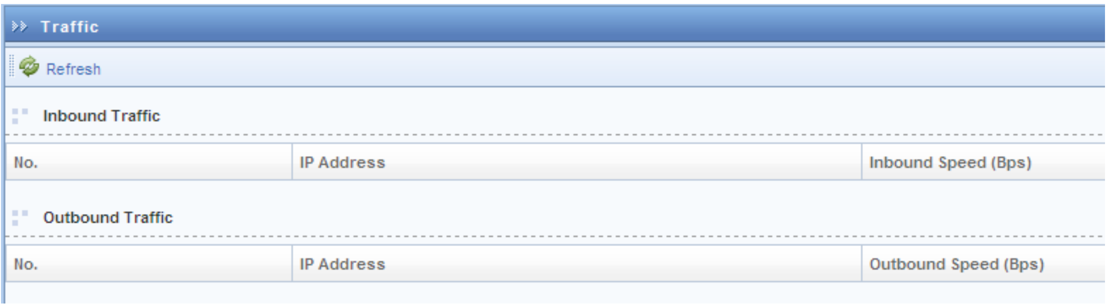
7. Click the **Save** buttons to save the settings.

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:



Inbound Traffic

No.	IP Address	Inbound Speed (Bps)

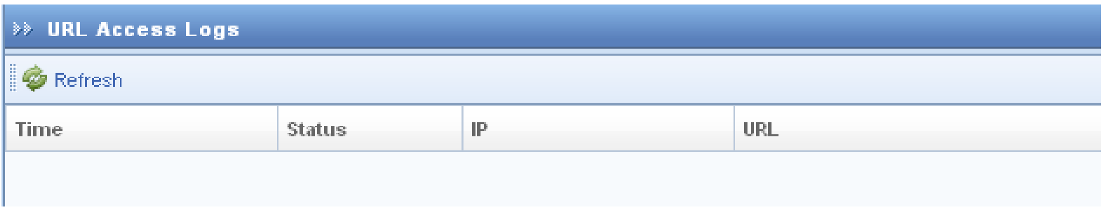
Outbound Traffic

No.	IP Address	Outbound Speed (Bps)

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:



Time	Status	IP	URL

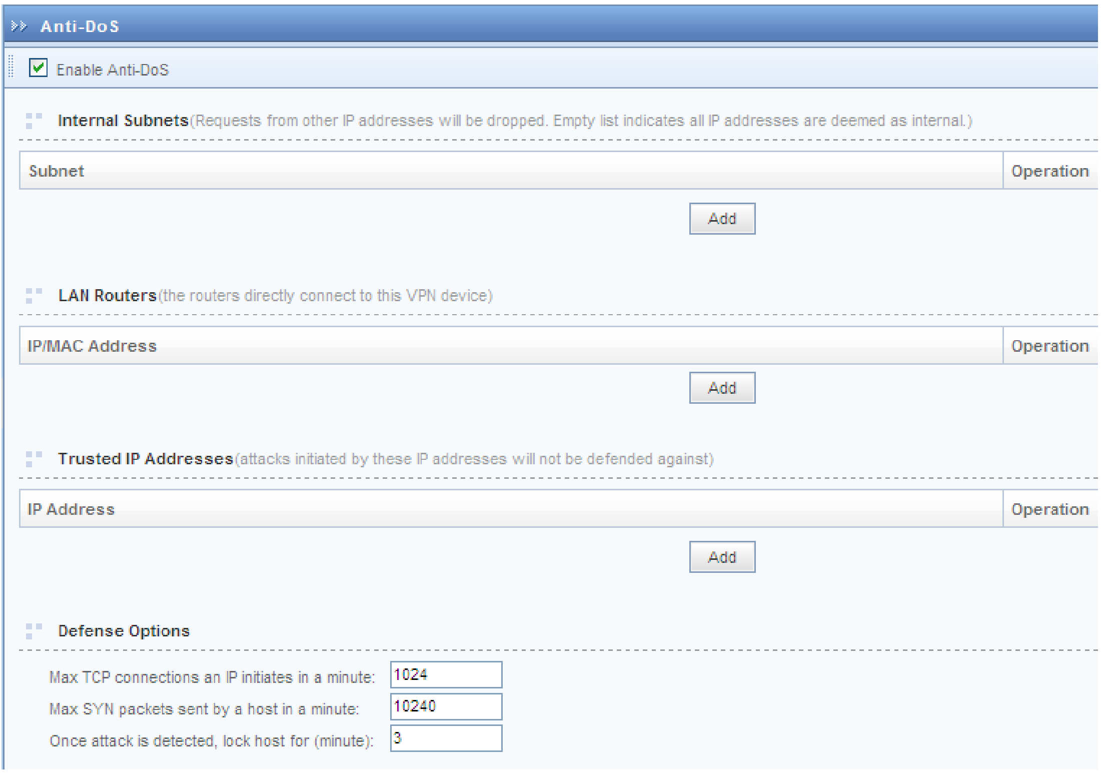
To update the URL access logs, click the **Refresh** button.

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:



Anti-DoS

☑ Enable Anti-DoS

Internal Subnets(Requests from other IP addresses will be dropped. Empty list indicates all IP addresses are deemed as internal.)

Subnet	Operation

Add

LAN Routers(the routers directly connect to this VPN device)

IP/MAC Address	Operation

Add

Trusted IP Addresses(attacks initiated by these IP addresses will not be defended against)

IP Address	Operation

Add

Defense Options

Max TCP connections an IP initiates in a minute: 1024

Max SYN packets sent by a host in a minute: 10240

Once attack is detected, lock host for (minute): 3

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.

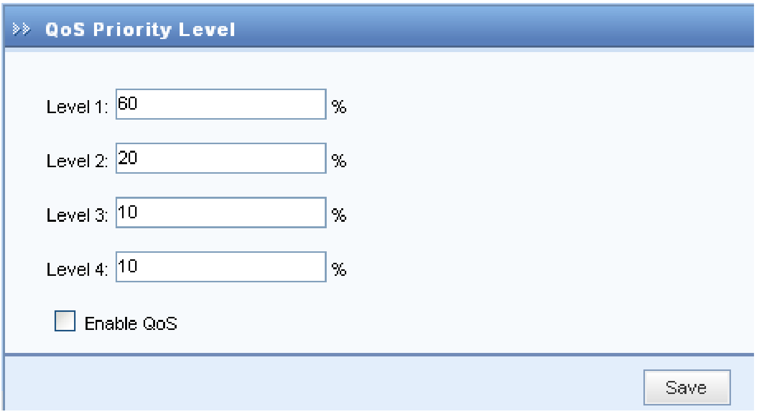
- **LAN Routers:** The function is **LAN Routers** is similar to that of **Internal Subnets**.
- **Trusted IP Addresses:** The attacks initiated from the IP addresses listed here will not be defended against. If no entry is added, the attack initiated from any IP address will be defended against.
- **Defense 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.

Configuring QoS Priority

The Quality of Service (QoS) priority enables you to guarantee sufficient bandwidth for important services when the network bandwidth is insufficient.

There are four priority levels, and higher priority level stands for higher bandwidth percent. You can configure the bandwidth allowed for each priority level, so that varied amount of bandwidth can be assigned to different services, ensuring smooth running of critical business.

Navigate to **Firewall > QoS Priority** to enter the **QoS Priority Level** page, as shown below:



QoS Priority Level

Level 1: 60 %

Level 2: 20 %

Level 3: 10 %

Level 4: 10 %

☐ Enable QoS

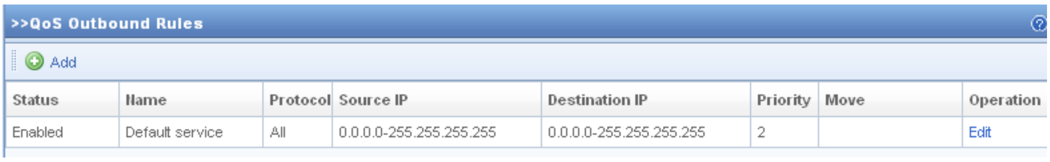
To enable QoS control feature, do select the **Enable QoS** option on the above page.

Configuring QoS Outbound Rule

QoS outbound rule enables administrator to set priority for specific data sent through the WAN interface(s) of the Sangfor device. You can set higher priority for data of critical business, so that they will be given more bandwidth and be transmitted earlier and faster. The default rule named **Default service** is a built-in rule, and only its priority level is editable.

To add a QoS outbound rule:

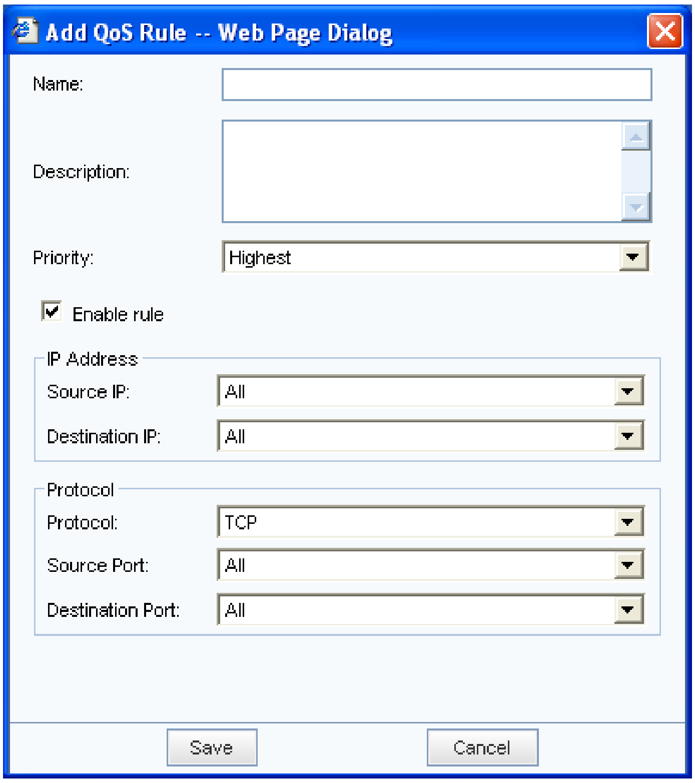
1. Navigate to **Firewall > QoS Outbound Rule** to enter the **QoS Outbound Rules** page, as shown below:



>>QoS Outbound Rules

Status	Name	Protocol	Source IP	Destination IP	Priority	Move	Operation
Enabled	Default service	All	0.0.0.0-255.255.255.255	0.0.0.0-255.255.255.255	2		Edit

2. Click **Add** to enter the **Add QoS Rule** page, as shown below:



Add QoS Rule -- Web Page Dialog

Name:

Description:

Priority: Highest

☑ Enable rule

IP Address

Source IP: All

Destination IP: All

Protocol

Protocol: TCP

Source Port: All

Destination Port: All

3. Specify the following information.

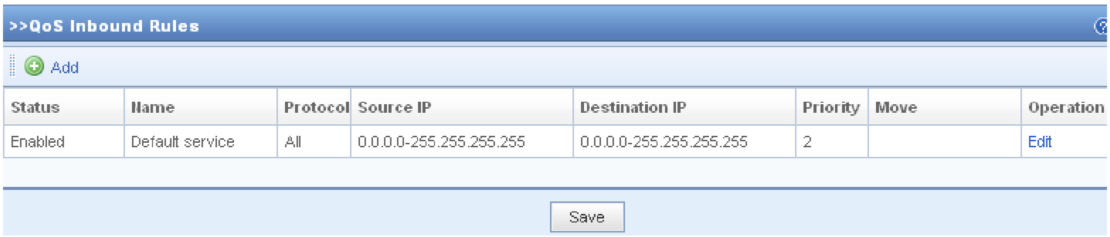
   - **Name, Description:** Enter a name and description for the rule.
   - **Priority:** Select a priority level for the current rule. Apart from the four levels as listed on the **QoS Priority Level** page, there is a **Highest** level, which means the corresponding service can occupy all the bandwidth.
   - **Enable rule:** Select it to enable the current QoS outbound rule.
   - **IP Address:** Specify the source and destination IP addresses of the data packets applicable to this rule. You can specify all or a specific IP address/range.
   - **Protocol:** Specify the protocol and ports of the services applicable to this rule.

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

Configuring QoS Inbound Rule

QoS inbound rule enables administrator to set priority for specific data received through the WAN interface(s) of the Sangfor device. You can set higher priority for data of critical business, so that they will be given more bandwidth and be transmitted earlier and faster.

Navigate to **Firewall > QoS Inbound Rule** to enter **QoS Inbound Rules** page, as shown below:

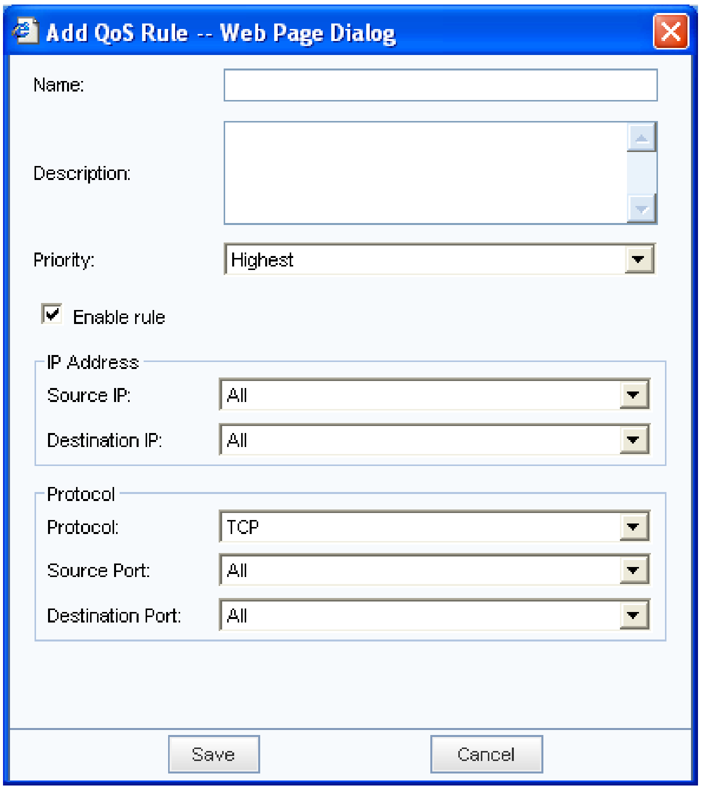


>>QoS Inbound Rules

Status	Name	Protocol	Source IP	Destination IP	Priority	Move	Operation
Enabled	Default service	All	0.0.0.0-255.255.255.255	0.0.0.0-255.255.255.255	2		Edit

To add a QoS inbound rule, please refer to the above section Configuring QoS Outbound Rule.

The following figure shows the contents included on **Add QoS Inbound Rule** page.



Add QoS Rule -- Web Page Dialog

Name:

Description:

Priority: Highest

☑ Enable rule

IP Address

Source IP: All

Destination IP: All

Protocol

Protocol: TCP

Source Port: All

Destination Port: All

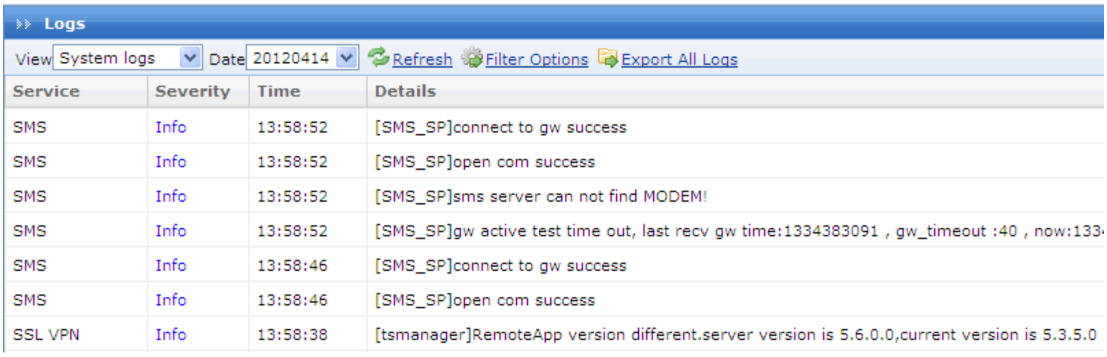
Chapter 6 System Maintenance

The **Maintenance** module covers the following four parts: **Logs**, **Backup/Restore**, **Restart/Shutdown** and **System Update**.

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.

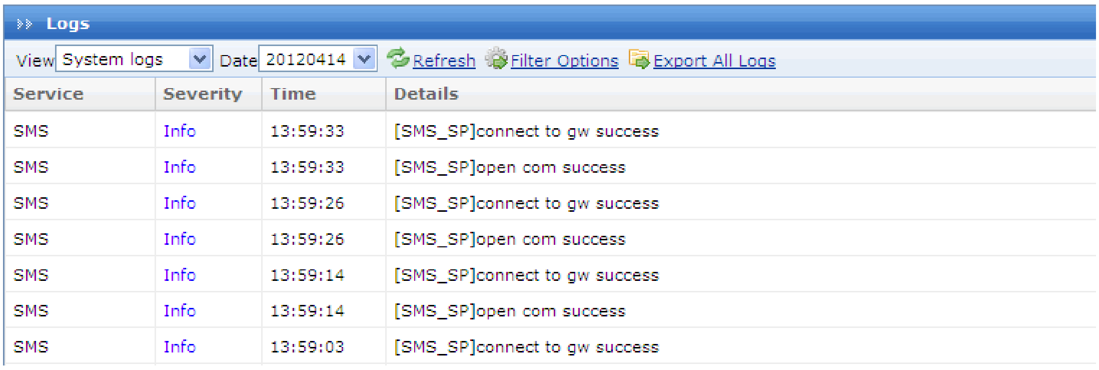
Navigate to **Maintenance > Logs** to enter the **Logs** page, as shown below:



Service	Severity	Time	Details
SMS	Info	13:58:52	[SMS_SP]connect to gw success
SMS	Info	13:58:52	[SMS_SP]open com success
SMS	Info	13:58:52	[SMS_SP]sms server can not find MODEM!
SMS	Info	13:58:52	[SMS_SP]gw active test time out, last recv gw time:1334383091 , gw_timeout :40 , now:133
SMS	Info	13:58:46	[SMS_SP]connect to gw success
SMS	Info	13:58:46	[SMS_SP]open com success
SSL VPN	Info	13:58:38	[tsmanager]RemoteApp version different.server version is 5.6.0.0,current version is 5.3.5.0

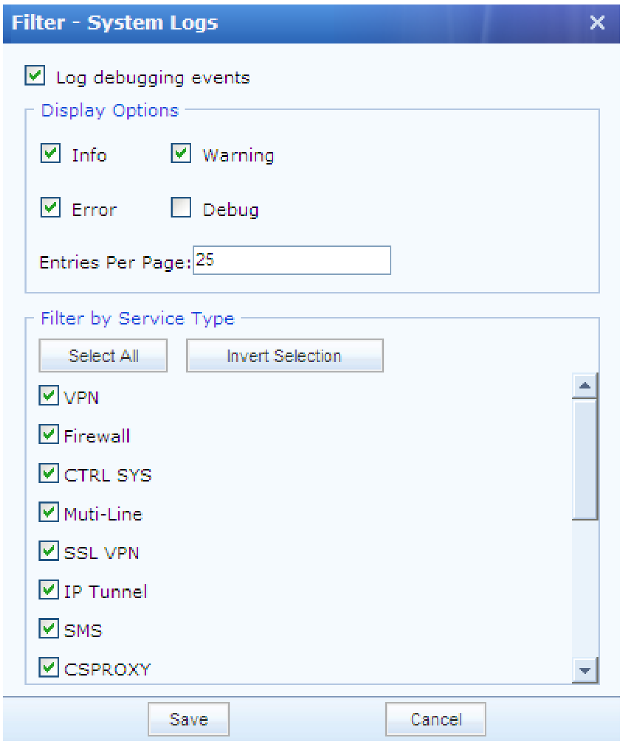
Viewing System Logs

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:



Service	Severity	Time	Details
SMS	Info	13:59:33	[SMS_SP]connect to gw success
SMS	Info	13:59:33	[SMS_SP]open com success
SMS	Info	13:59:26	[SMS_SP]connect to gw success
SMS	Info	13:59:26	[SMS_SP]open com success
SMS	Info	13:59:14	[SMS_SP]connect to gw success
SMS	Info	13:59:14	[SMS_SP]open com success
SMS	Info	13:59:03	[SMS_SP]connect to gw success

To filter the system logs, click the **Filter Options** button to enter the following page, and then select the desired options.



Filter - System Logs

☑ Log debugging events

Display Options

☑ Info ☑ Warning

☑ Error □ Debug

Entries Per Page: 25

Filter by Service Type

☑ VPN

☑ Firewall

☑ CTRL SYS

☑ Muti-Line

☑ SSL VPN

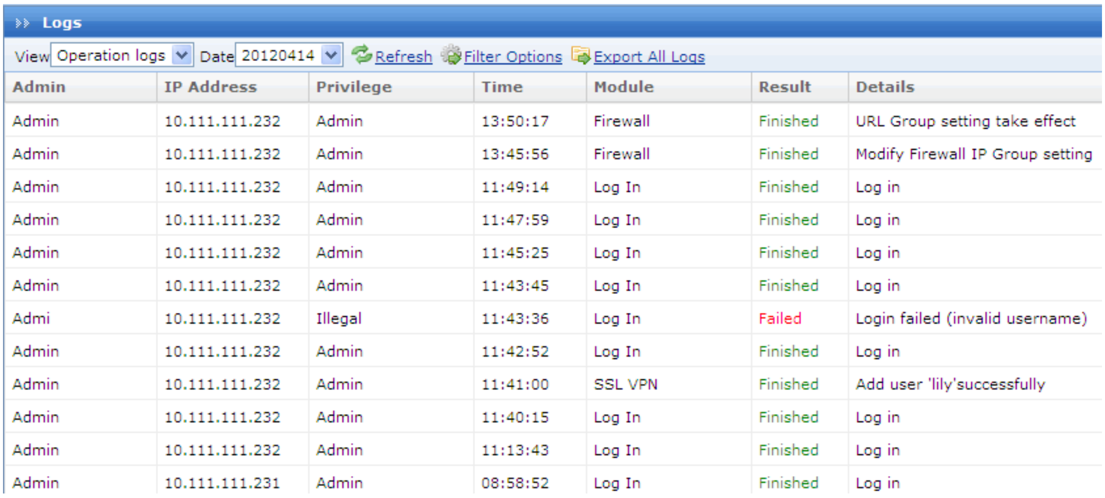
☑ IP Tunnel

☑ SMS

☑ CSPROXY

Viewing Operating Logs

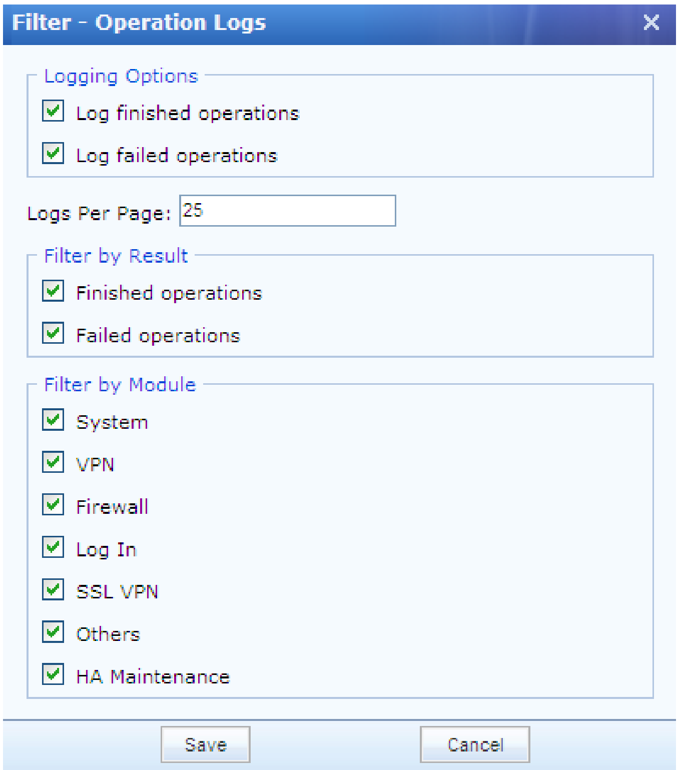
To view the operation logs, select **Operation logs** and a date, and the operation logs of the specified date will be displayed, as shown below:



View: Operation logs Date: 20120414

Admin	IP Address	Privilege	Time	Module	Result	Details
Admin	10.111.111.232	Admin	13:50:17	Firewall	Finished	URL Group setting take effect
Admin	10.111.111.232	Admin	13:45:56	Firewall	Finished	Modify Firewall IP Group setting
Admin	10.111.111.232	Admin	11:49:14	Log In	Finished	Log in
Admin	10.111.111.232	Admin	11:47:59	Log In	Finished	Log in
Admin	10.111.111.232	Admin	11:45:25	Log In	Finished	Log in
Admin	10.111.111.232	Admin	11:43:45	Log In	Finished	Log in
Admi	10.111.111.232	Illegal	11:43:36	Log In	Failed	Login failed (invalid username)
Admin	10.111.111.232	Admin	11:42:52	Log In	Finished	Log in
Admin	10.111.111.232	Admin	11:41:00	SSL VPN	Finished	Add user 'lily'successfully
Admin	10.111.111.232	Admin	11:40:15	Log In	Finished	Log in
Admin	10.111.111.232	Admin	11:13:43	Log In	Finished	Log in
Admin	10.111.111.231	Admin	08:58:52	Log In	Finished	Log in

To filter the operation logs, click the **Filter Options** button to enter the following page, and then select the desired options.



Filter - Operation Logs

Logging Options

☑ Log finished operations

☑ Log failed operations

Logs Per Page: 25

Filter by Result

☑ Finished operations

☑ Failed operations

Filter by Module

☑ System

☑ VPN

☑ Firewall

☑ Log In

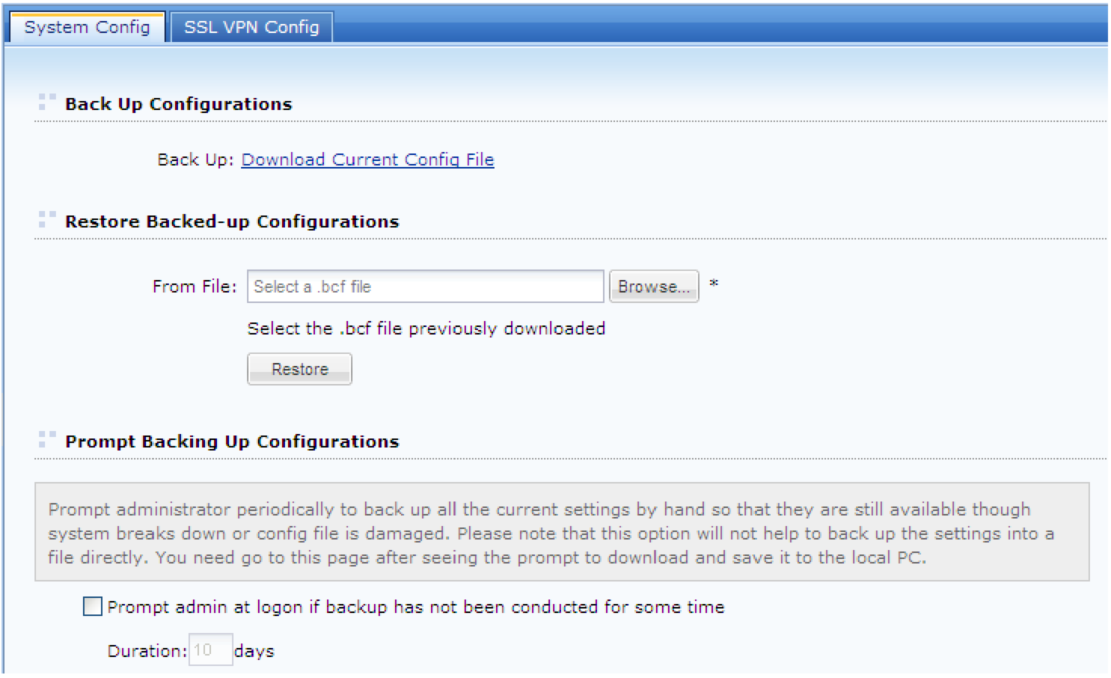
☑ SSL VPN

☑ Others

☑ HA Maintenance

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:



Back Up Configurations

Back Up: Download Current Config File

Restore Backed-up Configurations

From File: Select a .bcf file

Select the .bcf file previously downloaded

Prompt Backing Up Configurations

Prompt administrator periodically to back up all the current settings by hand so that they are still available though system breaks down or config file is damaged. Please note that this option will not help to back up the settings into a file directly. You need go to this page after seeing the prompt to download and save it to the local PC.

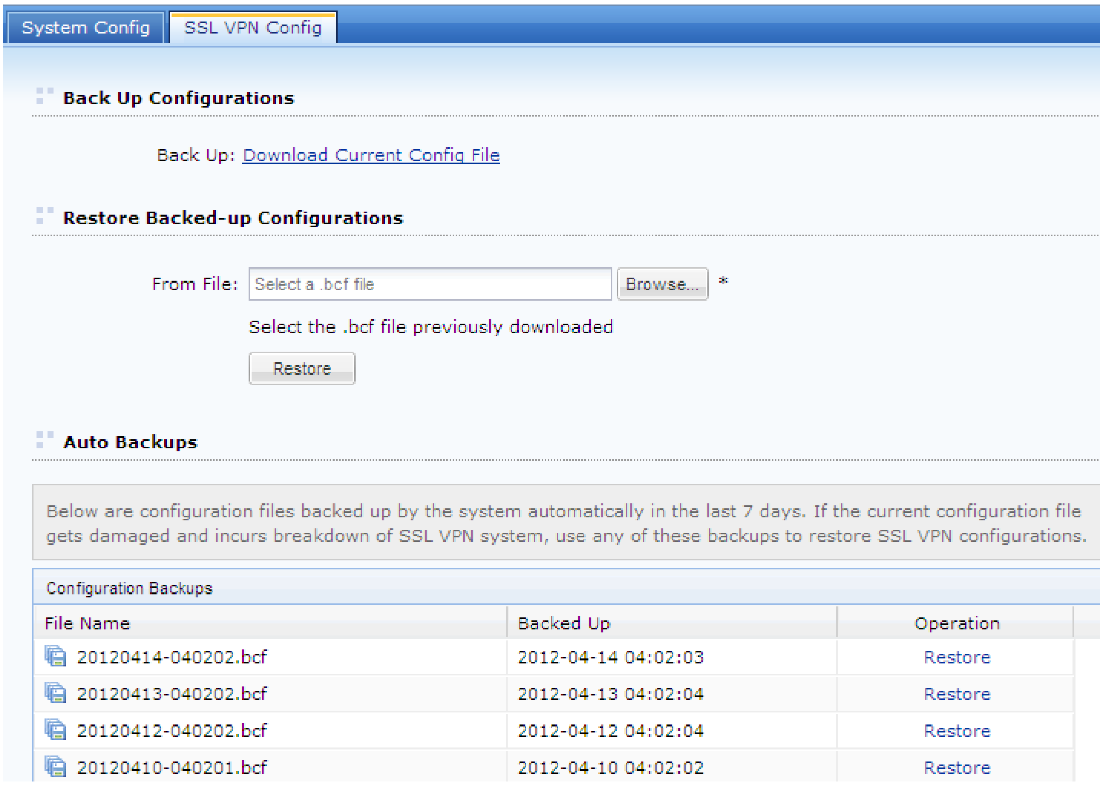
☐ Prompt admin at logon if backup has not been conducted for some time

Duration: 10 days

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:



Back Up Configurations

Back Up: Download Current Config File

Restore Backed-up Configurations

From File: Select a .bcf file Browse... *

Select the .bcf file previously downloaded

Auto Backups

Below are configuration files backed up by the system automatically in the last 7 days. If the current configuration file gets damaged and incurs breakdown of SSL VPN system, use any of these backups to restore SSL VPN configurations.

Configuration Backups

File Name	Backed Up	Operation
20120414-040202.bcf	2012-04-14 04:02:03	Restore
20120413-040202.bcf	2012-04-13 04:02:04	Restore
20120412-040202.bcf	2012-04-12 04:02:04	Restore
20120410-040201.bcf	2012-04-10 04:02:02	Restore

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.
- **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.

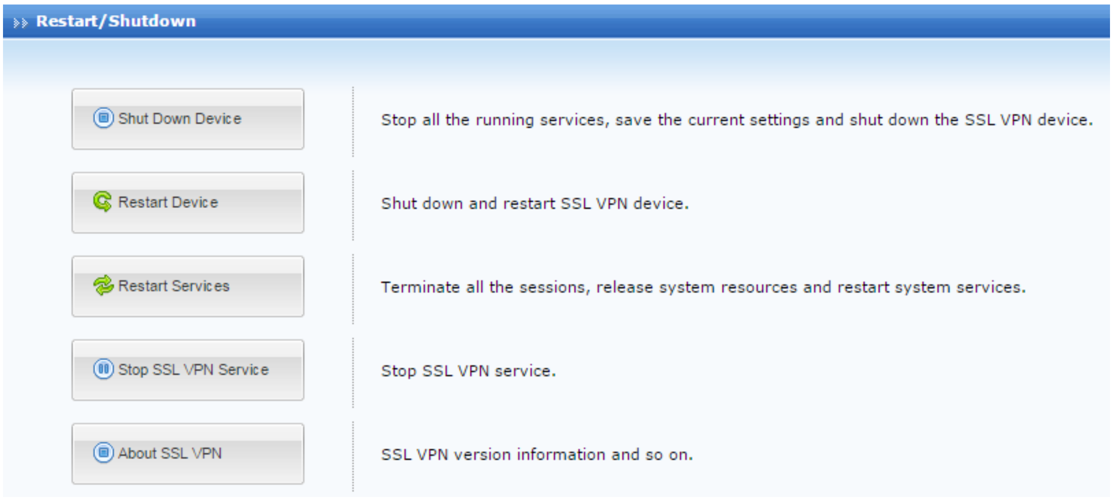
- **Auto Backups:** Displays configuration files automatically backed up by the system in the past 7 days. Click **Restore** to restore any of them.

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:



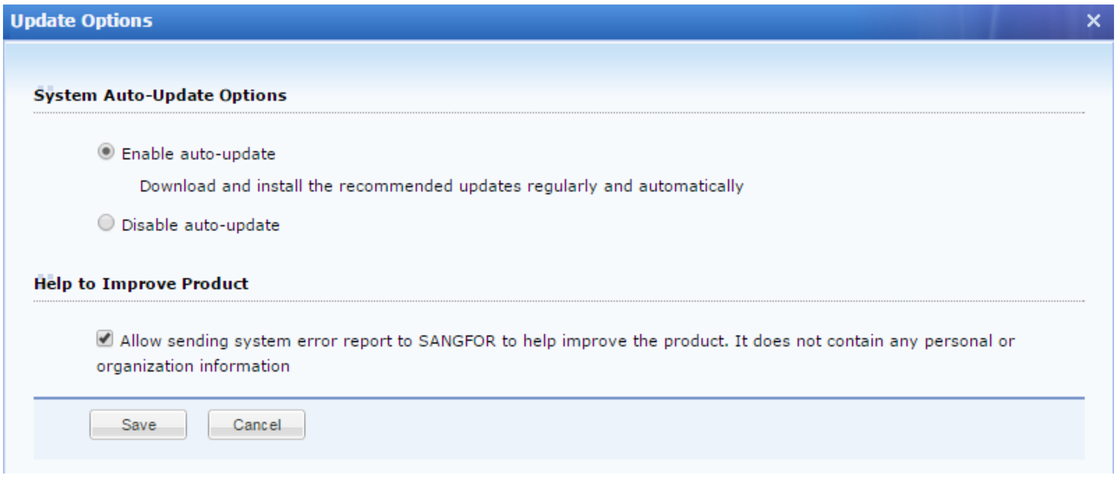
Shut Down Device	Stop all the running services, save the current settings and shut down the SSL VPN device.
Restart Device	Shut down and restart SSL VPN device.
Restart Services	Terminate all the sessions, release system resources and restart system services.
Stop SSL VPN Service	Stop SSL VPN service.
About SSL VPN	SSL VPN version information and so on.

- **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 SSLVPN:** Reviewing the version

System Automatic Update

The **System Auto-Update Options** page includes automatic update options. If auto-update is enabled, updates will be automatically downloaded and installed.

Navigate to **Maintenance >Restart/Shutdown > About SSL VPN**to enter the**Update options** page, as shown below:



System Auto-Update Options

● Enable auto-update

Download and install the recommended updates regularly and automatically

○ Disable auto-update

Help to Improve Product

☑ Allow sending system error report to SANGFOR to help improve the product. It does not contain any personal or organization information

- **Enable auto-update:** Select this option to enable automatic update function, and specify the **Interval**. The device will check for updates and download them automatically at intervals of a specified period.
- If **Disable auto-update** is selected, updates will not be downloaded automatically.
- **Save:**Click this button to make the settings take effect.

The auto-update only applies to service pack (SP) installation, not applicable to upgrade of released version.

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, Safari, Chrome, etc.

⚠

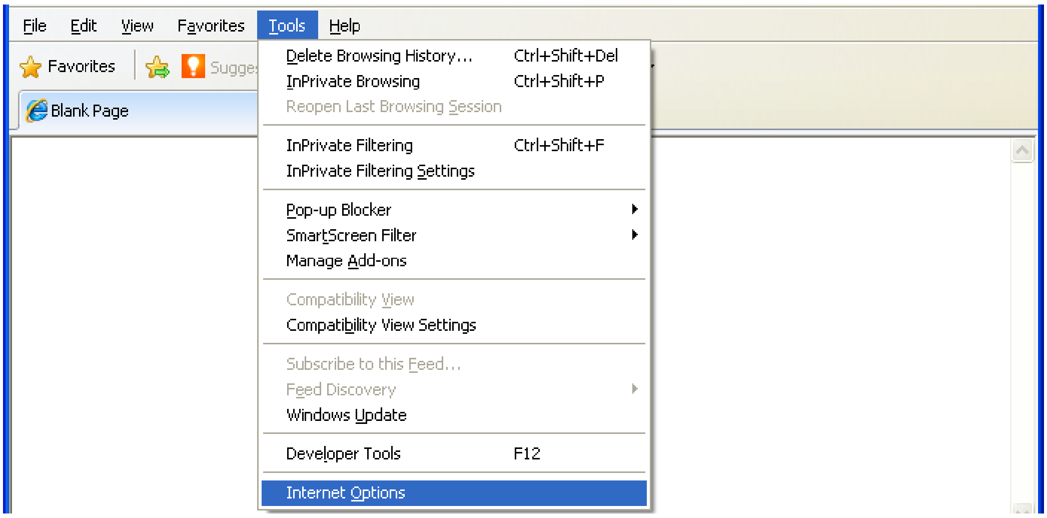
Operating systems should be 32bit/64bit Windows XP/2003/Vista/Win7, 32bit Linux Ubuntu 11.04/Red Hat 5.2/Reflag/Fedora 13/SUSE 11.2, or Mac OS X Leopard(10.5)/Snow Leopard(10.6)/Lion(10.7).

Configuring Browser and Accessing SSL VPN

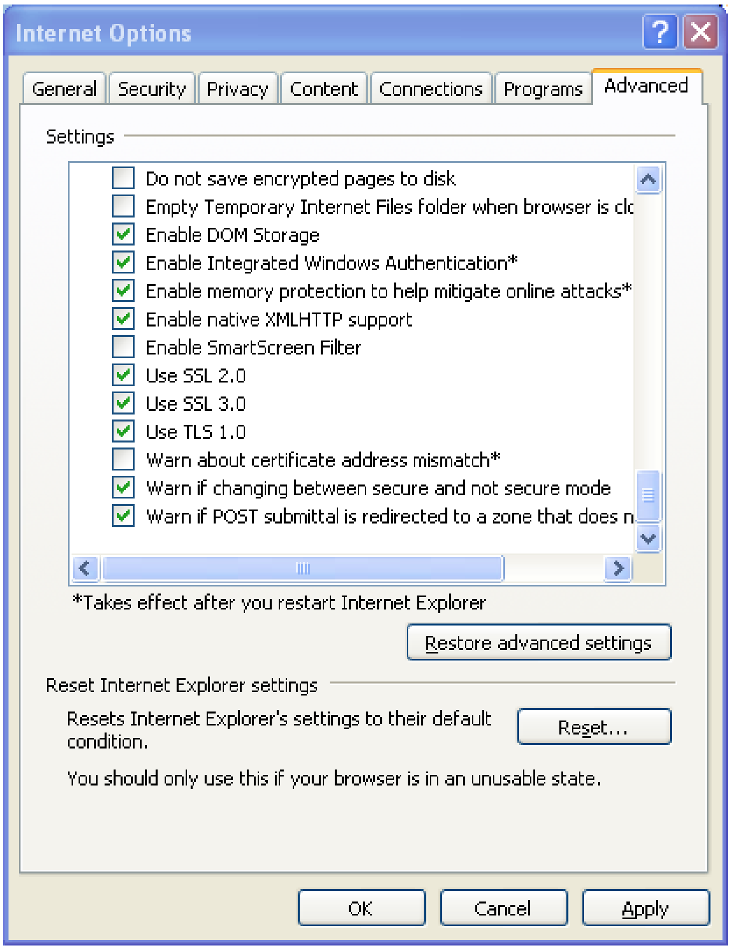
Configuring Browser

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:


File
Edit
View
Favorites
Tools
Help
Favorites
Sugges
Blank Page
Delete Browsing History... Ctrl+Shift+Del
InPrivate Browsing Ctrl+Shift+P
Reopen Last Browsing Session
InPrivate Filtering Ctrl+Shift+F
InPrivate Filtering Settings
Pop-up Blocker
SmartScreen Filter
Manage Add-ons
Compatibility View
Compatibility View Settings
Subscribe to this Feed...
Feed Discovery
Windows Update
Developer Tools F12
Internet Options

2. Click **Advanced** tab. Find the **Security** item and select the checkboxes next to **Use SSL 2.0**, **Use SSL 3.0** and **UseTLS 1.0**, as shown in the figure below:



Settings

- □ Do not save encrypted pages to disk
- □ Empty Temporary Internet Files folder when browser is clo
- ☑ Enable DOM Storage
- ☑ Enable Integrated Windows Authentication*
- ☑ Enable memory protection to help mitigate online attacks*
- ☑ Enable native XMLHTTP support
- □ Enable SmartScreen Filter
- ☑ Use SSL 2.0
- ☑ Use SSL 3.0
- ☑ Use TLS 1.0
- □ Warn about certificate address mismatch*
- ☑ Warn if changing between secure and not secure mode
- ☑ Warn if POST submittal is redirected to a zone that does n

*Takes effect after you restart Internet Explorer

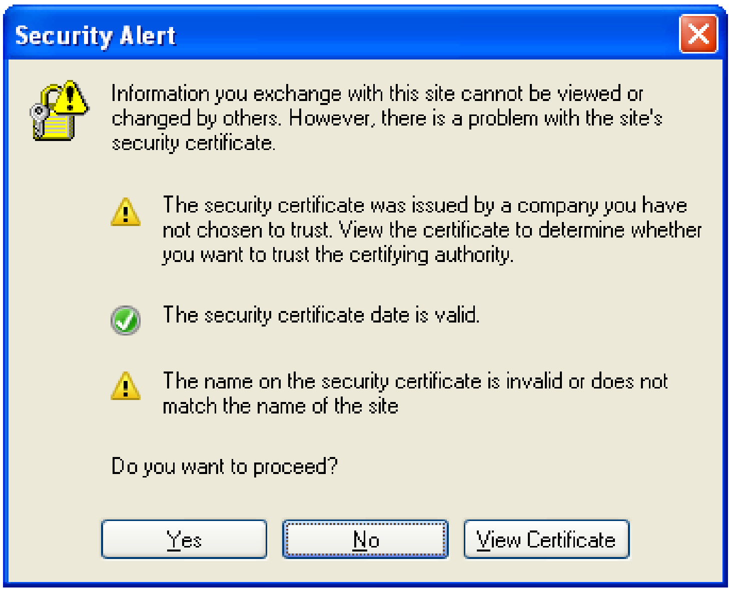
Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

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:



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

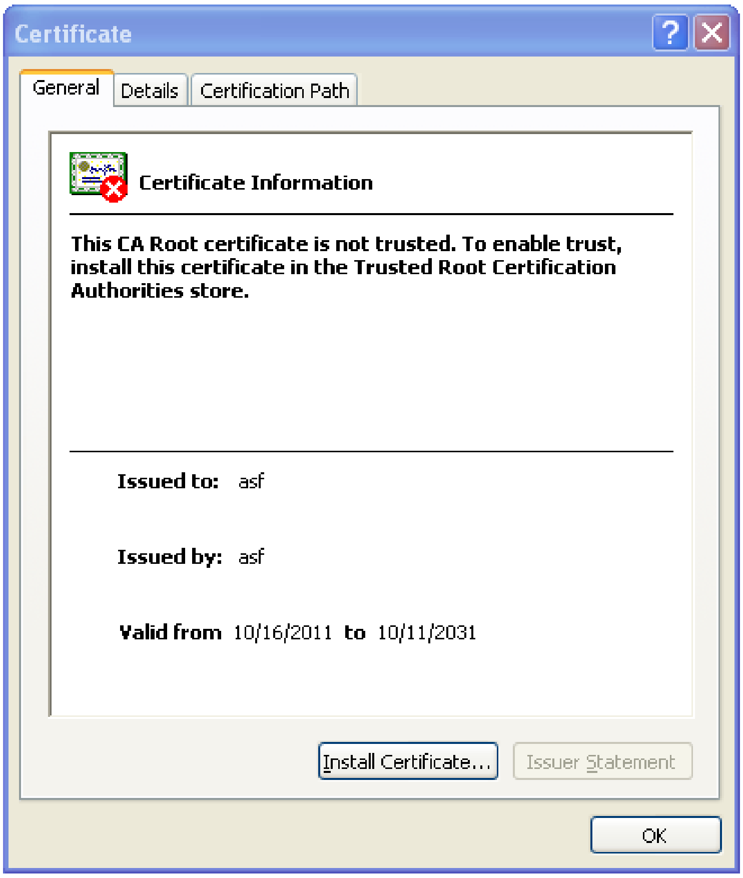
⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

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:



Certificate

Certificate Information

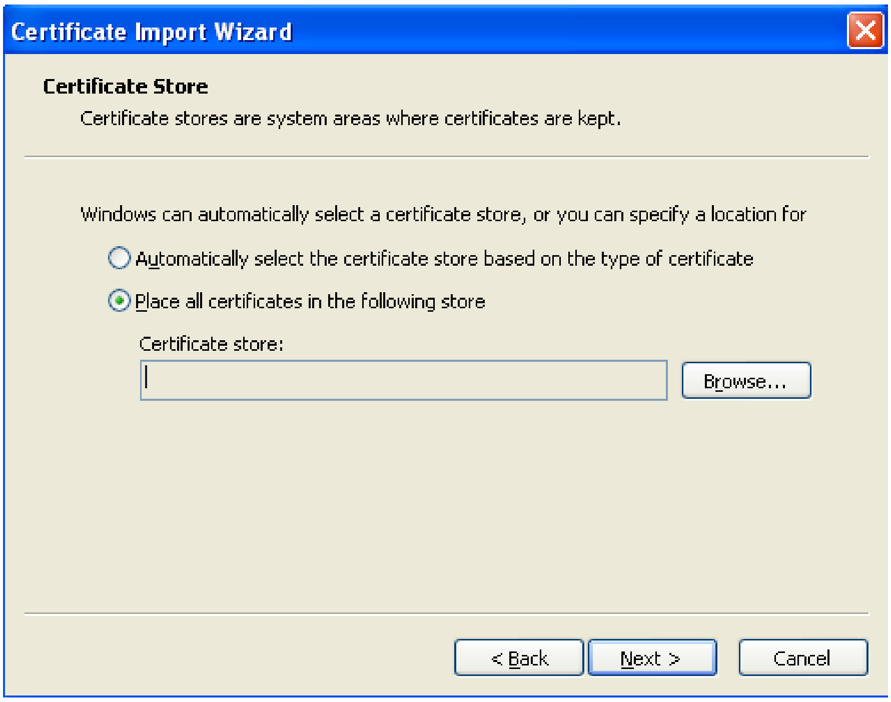
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: asf

Issued by: asf

Valid from 10/16/2011 **to** 10/11/2031

6. Click the **Install Certificate** button and use the **Certificate Import Wizard** to import the root certificate, as shown in the figure below:



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

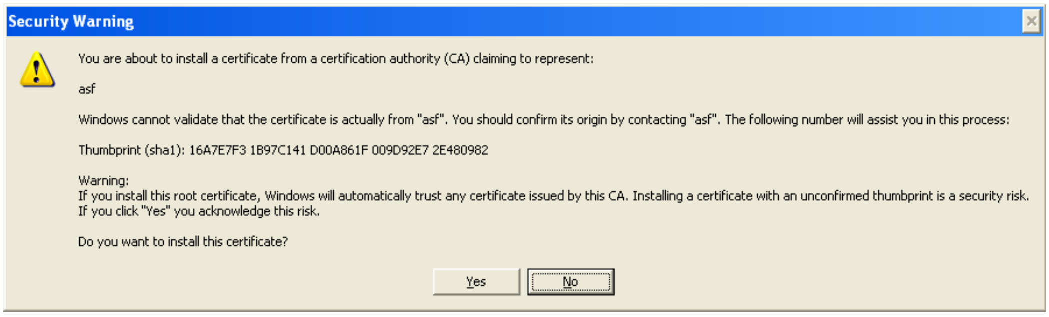
Windows can automatically select a certificate store, or you can specify a location for

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

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:



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

asf

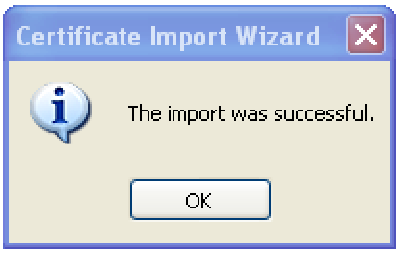
Windows cannot validate that the certificate is actually from "asf". You should confirm its origin by contacting "asf". The following number will assist you in this process:

Thumbprint (sha1): 16A7E7F3 1B97C141 D00A861F 009D92E7 2E480982

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk.
If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

8. Click the **Yes** button to ignore the warning and the root certificate will be installed, as shown in the figure below:



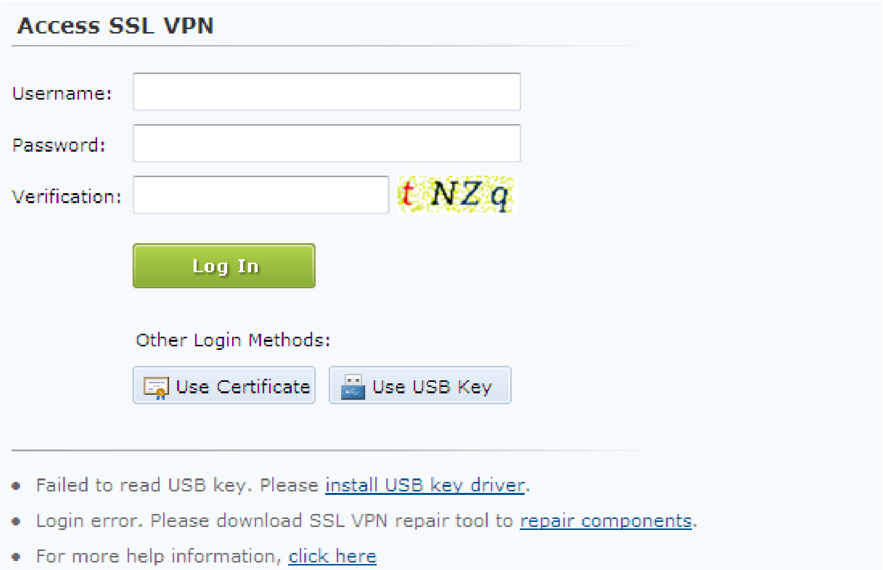
Certificate Import Wizard

The import was successful.

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:



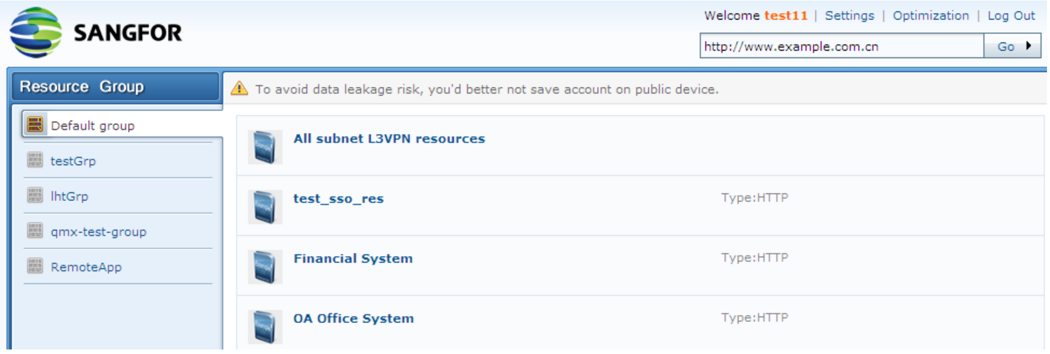
- Failed to read USB key. Please install USB key driver.
- Login error. Please download SSL VPN repair tool to repair components.
- For more help information, click here

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 be authenticated may need toinstall theUSB key driver. For detailed guide, please refer to the SSL VPN Userssectioning 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:


SANGFOR
Welcome test11 | Settings | Optimization | Log Out
http://www.example.com.cn
Go
Resource Group
Default group
testGrp
lhtGrp
qmx-test-group
RemoteApp

To avoid data leakage risk, you'd better not save account on public device.

All subnet L3VPN resources

test_sso_res Type:HTTP

Financial System Type:HTTP

OA Office System Type:HTTP

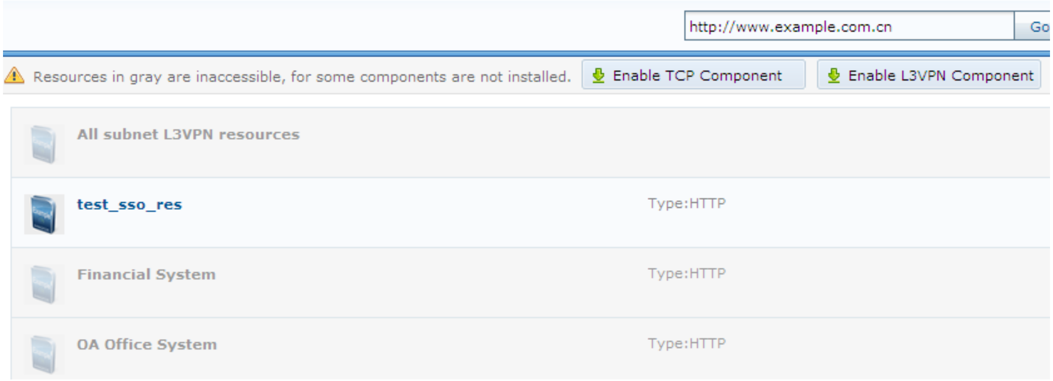
3. All the resources or groups associated with the connecting user will be displayed on the **Resource** page. Click on any of the links to access the corresponding resource.

   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. Install TCP and L3VPN components if connecting user is assigned any TCP resource or L3VPN resource.

   TCP and L3VPN components could be installed automatically if administrator has selected the option **Install TCP and L3VPN components on user's logon** on the Sangfor device, or installed by end user after end user clicks the **Enable TCP Component** and **Enable L3VPN component** buttons, as shown in the figure below:



Resources in gray are inaccessible, for some components are not installed.

All subnet L3VPN resources

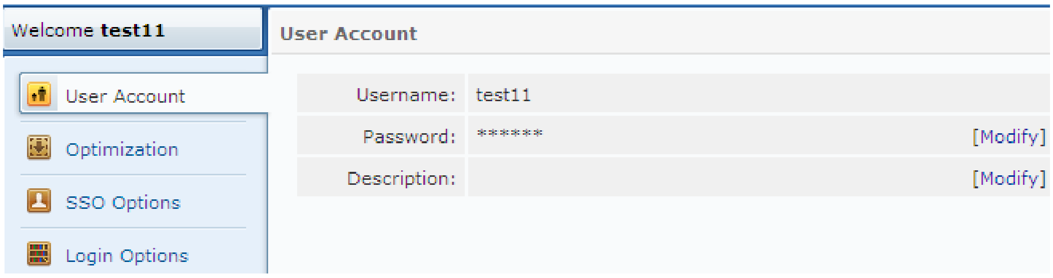
test_sso_res Type:HTTP

Financial System Type:HTTP

OA Office System Type:HTTP

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:

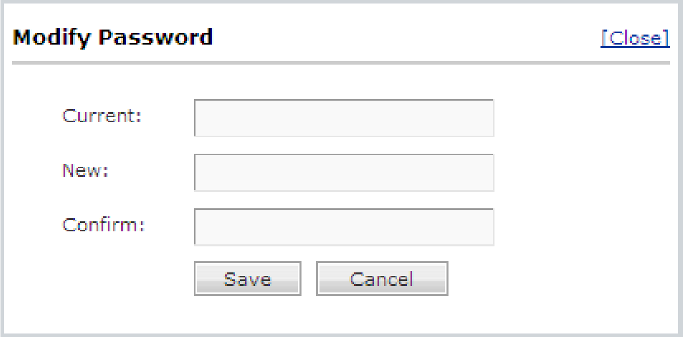


Username: test11

Password: *******

Description:

As shown above, the current password is followed by **Modify**. Click it to enter the **Modify Password** page, as shown below:



Current:

New:

Confirm:

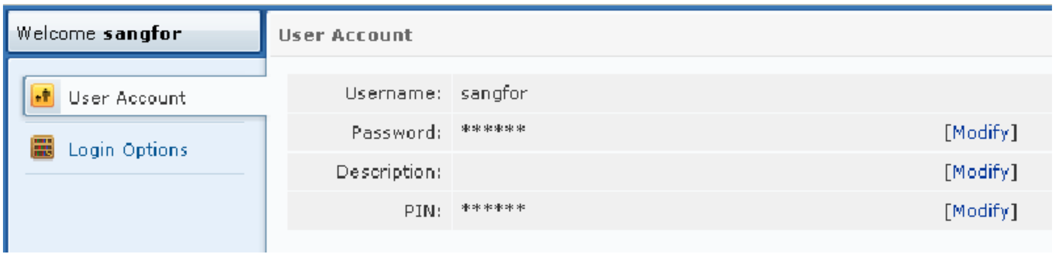
If user keeps inactive for a long time during SSL VPN access, without performing any operation or accessing any resource, user will be disconnected and log out automatically.

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** pageto enter **User Account** page, as shown below:



User Account

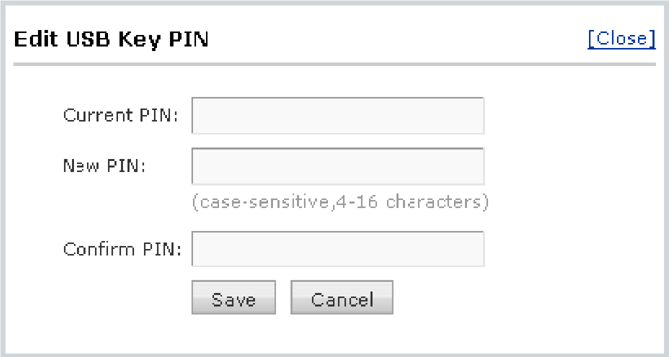
Username: sangfor

Password: ****** [Modify]

Description: [Modify]

PIN: ****** [Modify]

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:



Edit USB Key PIN

Current PIN:

New PIN:

(case-sensitive,4-16 characters)

Confirm PIN:

.

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.

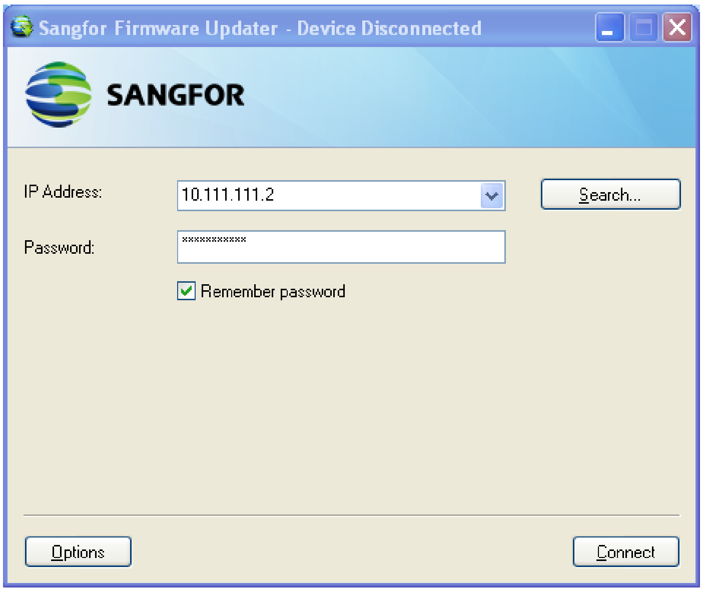
   Using online update method to update Sangfor device, network administrators need not handle some troubles such as preparing Sangfor device, checking current version of their Sangfor device, downloading update package, etc., but only choose an available version and click buttons.

   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:



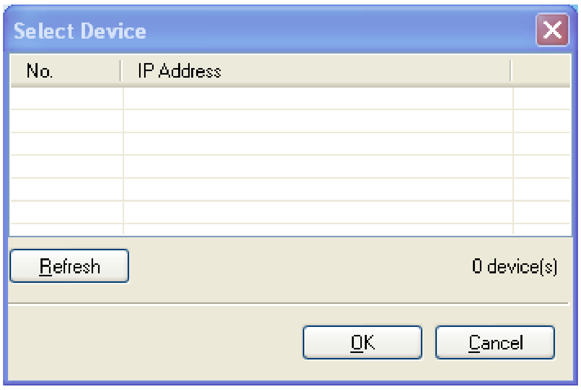
IP Address: 10.111.111.2

Password: ***********

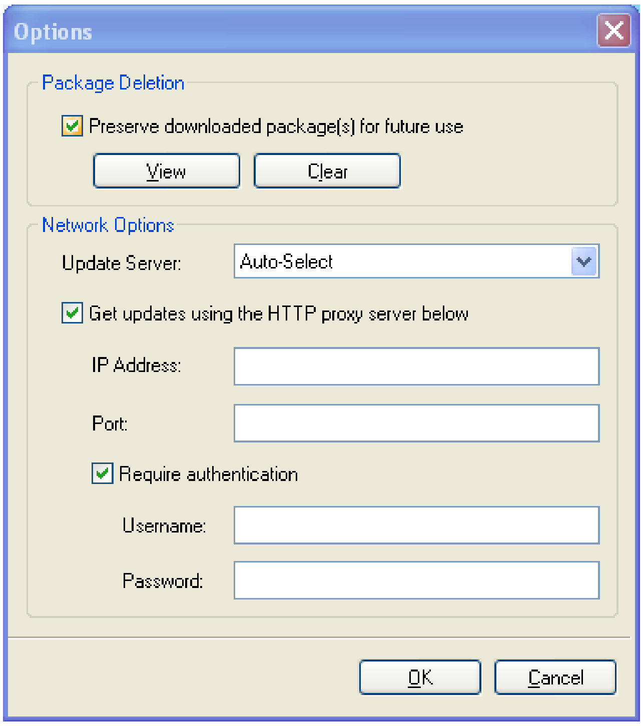
☑ Remember password

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:



☑ Preserve downloaded package(s) for future use

Update Server: Auto-Select

☑ Get updates using the HTTP proxy server below

☑ Require authentication

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

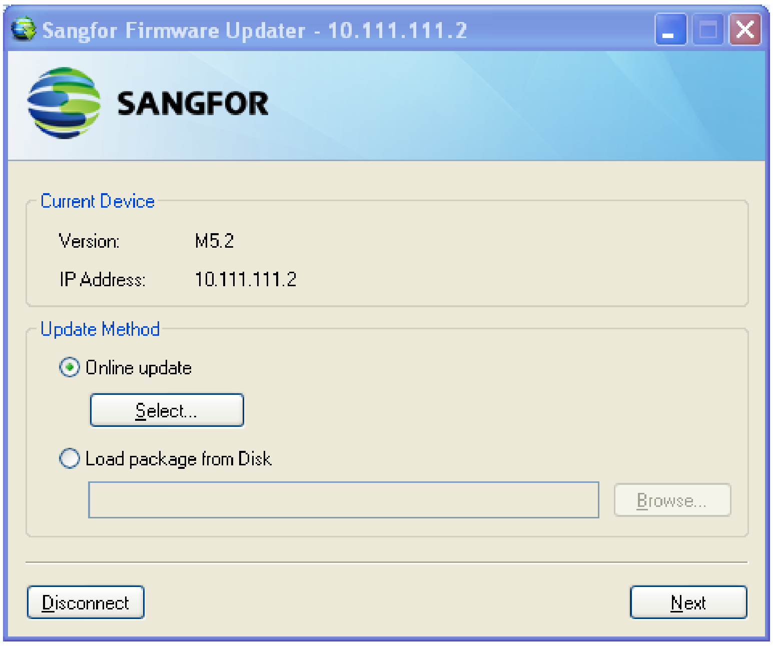
- **Preserve downloaded package(s) for future use:** Select this option and the previously downloaded packages (in **Download** folder) will be preserved and can be used for future update or configuration restoring.

  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 **IPAddress** 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:



Sangfor Firmware Updater - 10.111.111.2

Current Device

Version: M5.2

IP Address: 10.111.111.2

Update Method

● Online update

○ Load package from Disk

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.

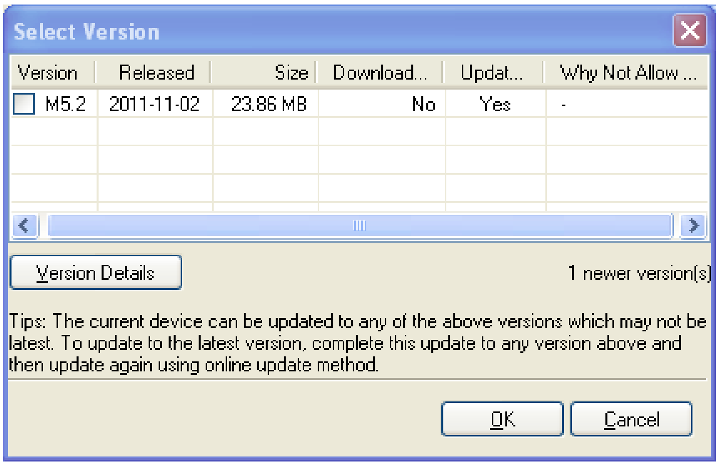
Under **Update Method** are two options, **Online update** and **Load package from Disk**. The former is the previously mentioned feature that can automatically get updates for the connected Sangfor device, and the latter enables administrator to choose a package to update the current device or restore 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 methodis **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:



Select Version

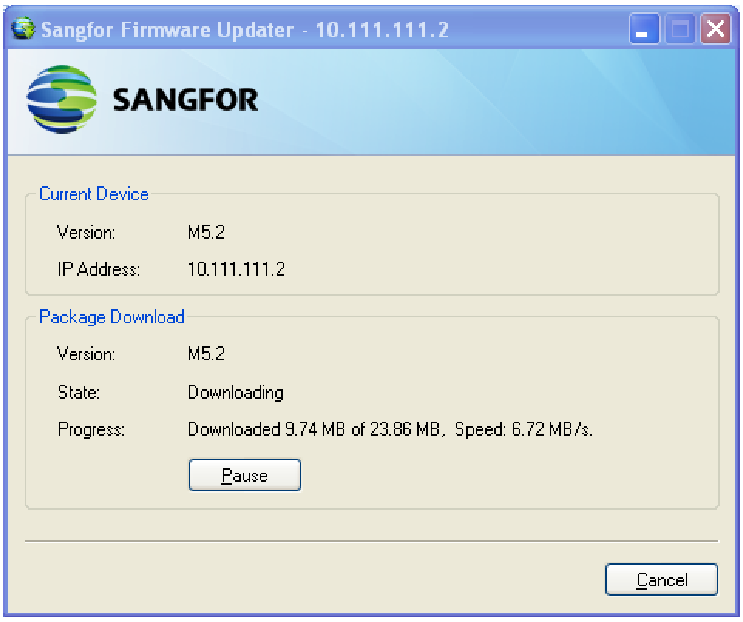
Version	Released	Size	Download...	Updat...	Why Not Allow ...
□ M5.2	2011-11-02	23.86 MB	No	Yes	-

1 newer version(s)

Tips: The current device can be updated to any of the above versions which may not be latest. To update to the latest version, complete this update to any version above and then update again using online update method.

  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:



Current Device

Version: M5.2

IP Address: 10.111.111.2

Package Download

Version: M5.2

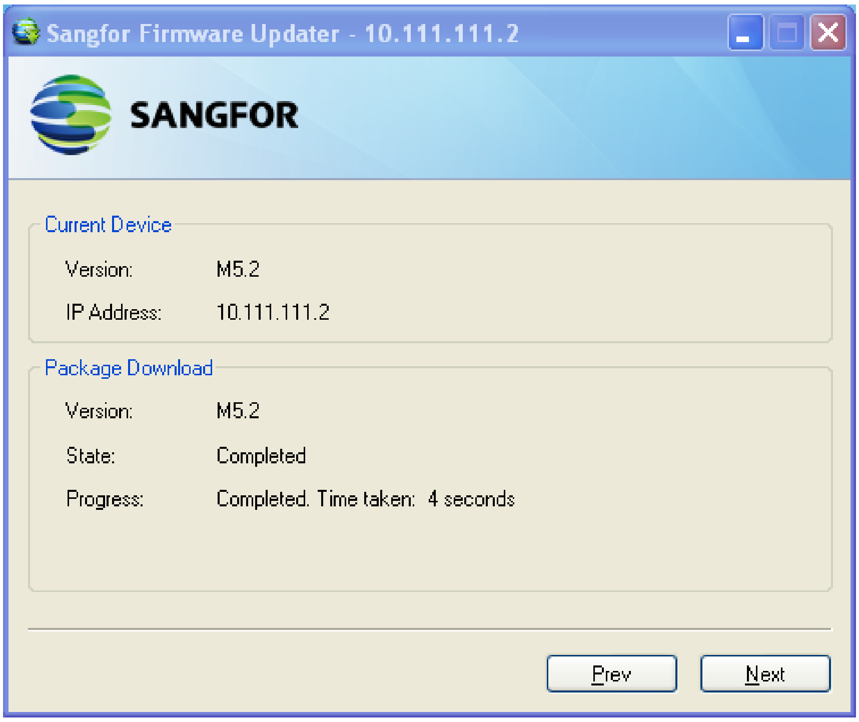
State: Downloading

Progress: Downloaded 9.74 MB of 23.86 MB, Speed: 6.72 MB/s.

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:



Current Device

Version: M5.2

IP Address: 10.111.111.2

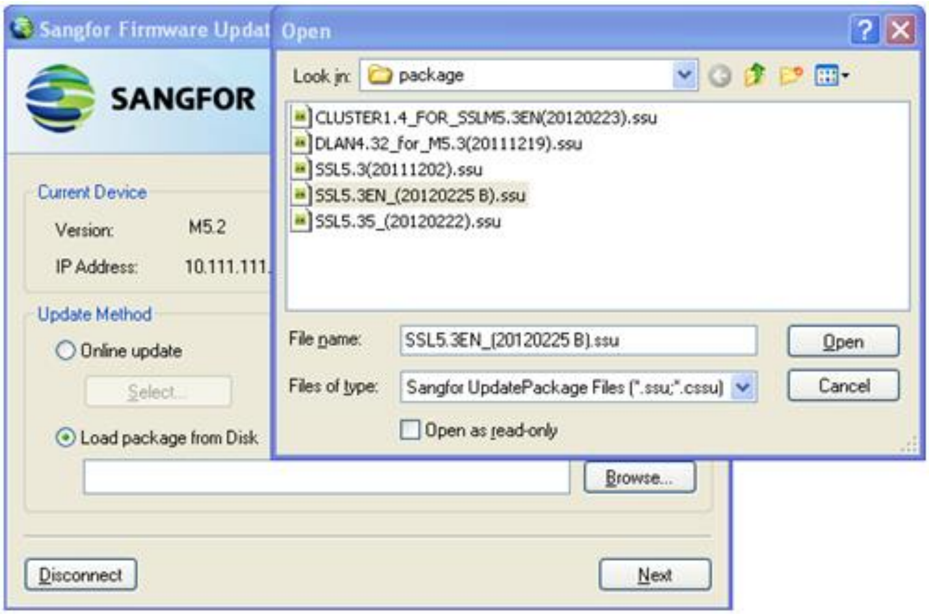
Package Download

Version: M5.2

State: Completed

Progress: Completed. Time taken: 4 seconds

- 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:



Current Device

Version: M5.2

IP Address: 10.111.111.

Update Method

○ Online update

● Load package from Disk

Look in: package

CLUSTER1.4_FOR_SSLM5.3EN(20120223).ssu

DLAN4.32_for_M5.3(20111219).ssu

SSL5.3(20111202).ssu

SSL5.3EN_(20120225 B).ssu

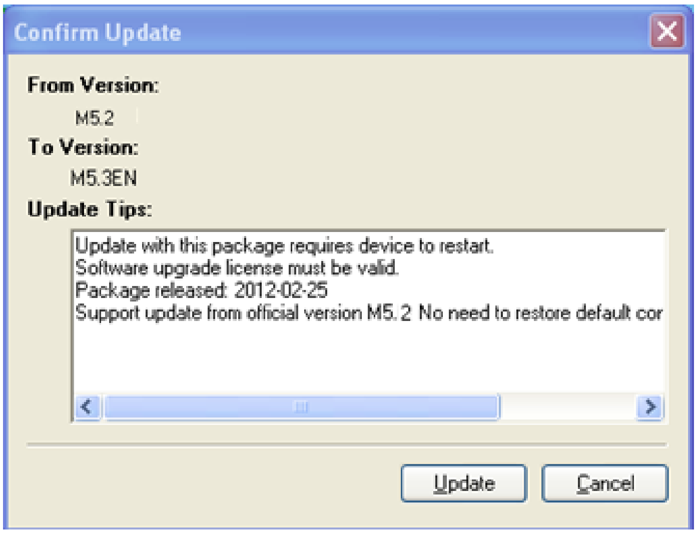
SSL5.35_(20120222).ssu

File name: SSL5.3EN_(20120225 B).ssu

Files of type: Sangfor UpdatePackage Files (*.ssu;*.cssu)

□ Open as read-only

6. Confirm the update information and click the **Update** button to update the current Sangfor device, as shown in the figure below:



Confirm Update

From Version:

M5.2

To Version:

M5.3EN

Update Tips:

Update with this package requires device to restart.
Software upgrade license must be valid.
Package released: 2012-02-25
Support update from official version M5. 2 No need to restore default cor

Please DO NOT cancel updating during the update process. Otherwise, the current device will meet unexpected error.