

Sangfor vSSL VPN

Quick Guide



May 2020

Table of Contents

Table of Contents	1
Declaration	4
Chapter 1 Install vSSL VPN VM.....	5
Prepare Virtual Machine	5
Install Image for Virtual Machine	5
Initialize Network	6
Chapter 2 Login to Admin Console	8
Logging in to Admin Console	8
Modifying Administrator Password	8
Chapter 3 System and Network Settings	10
System Settings	11
Configuring License.....	11
Network Settings.....	13
Device Deployment.....	13
Configuring Route.....	18
SSL VPN Options	20
General Settings	20
Configuring User Login Options	20
Configuring Local DNS Server	23
Chapter 4 SSL VPN	27
SSL VPN Users.....	27
Adding User Group.....	28
Adding User	34
Searching for Users.....	40
Managing Hardware IDs.....	42
Importing User to Device.....	44
Importing Users from File.....	45
Importing Users from LDAP Server	47
Moving Users to Another Group.....	49
Exporting Users.....	50
Associating Roles with User	51
Resources	53
Adding/Editing Resource Group.....	54
Adding/Editing Web Application	55
Adding/Editing TCP Application	62
Adding/Editing L3VPN	68
Adding/Editing Remote Application.....	72
Roles	76
Adding Role	77
Authentication Options	80
Primary Authentication Methods	81


Local Password Based Authentication.....	81
LDAP Authentication	82
Configuring LDAP Server	82
RADIUS Authentication	90
Configuring RADIUS Server.....	90
Certificate/USB Key Based Authentication.....	93
Configuring Local CA.....	94
Configuring External CA.....	96
Configuring USB Key Model.....	101
Client-Side Domain SSO.....	102
Secondary Authentication Methods	104
SMS Authentication.....	104
Using SMS Gateway of ISP to Send SMS Message	106
Using Webservice Based SMS Platform to Send SMS Message	106
Using Jasson MAS to Send SMS Message.....	107
Hardware ID Based Authentication.....	108
Dynamic Token Based Authentication.....	109
Other Authentication Options	110
Priority of LDAP and RADIUS Servers	110
Password Security Options.....	111
Anonymous Login.....	112
Policy Sets.....	115
Adding Policy Set	116
Remote Servers	126
Adding Remote Application Server	128
Adding Remote Storage Server.....	131
Chapter 5 System Maintenance	136
Backing Up/Restoring Configurations	136
Restarting/Shutting Down Device or Services.....	137
Chapter 6 Scenarios	140
Device Deployment.....	140
Deploying Device in Gateway Mode with Single Line	140
Deploying Device in Gateway Mode with Multiple Lines	143
Deploying Device in Single-Arm Mode With Single Line	147
Deploying Device in Single-Arm Mode With Multiple Lines	149
Configuring System Route.....	152
Adding User	154
Adding User Logging in with Local Password	154
Adding User Logging in with Certificate.....	154
Configuring VPN Resource	156
Adding Web Application.....	156
Masquerading Resource Address.....	159
Adding FileShare Type of Web Application	160
Adding Web Application Enabling Site Mapping.....	163

Configuring TCP Application	166
Configuring URL Access Control Feature	168
Adding L3VPN Application.....	169
Adding Remote Application.....	171
Configuring Authentication with External CA.....	180
Using External CA Root Certificate to Generate Device Certificate	180
Mapping User to Local Group Based on External Certificate	183
Configuring Resource Enabling SSO.....	185
Adding TCP Application Enabling SSO	185
Adding Remote Application Enabling SSO	189
Mobile Users Accessing SSL VPN	206
Configuring Firewall Rule	211
Adding SNAT Rule	211
Adding DNAT Rule.....	213
Typical Case Study.....	215
Required Environment	215
Configuring Sangfor Device	215
Appendix A: End Users Accessing SSL VPN.....	221
Required Environment	221
Configuring Browser and Accessing SSL VPN	221
Configuring Browser.....	221
Using Account to Log In to SSL VPN	225
Using USB Key to Log In to SSL VPN	227
Using VPN Client to Log In SSL VPN	228

Declaration

Copyright © 2016 Sangfor Inc. All rights reserved.

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

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

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

Chapter 1 Install vSSL VPN VM

This chapter introduces how to install vSSL VPN VM in public Cloud.

Prepare Virtual Machine

Resource Requirements	SSL Encryption Throughput	Concurrent User
2 CPU, 2G RAM, 64G Disk	200M	500
2 CPU,4G RAM, 64G Disk	300M	1000
4 CPU,4G RAM, 64G Disk	350M	2000
4 CPU,8G RAM, 64G Disk	540M	5000
8 CPU,8G RAM, 64G Disk	580M	10000
8 CPU,16G RAM, 64G Disk	640M	20000

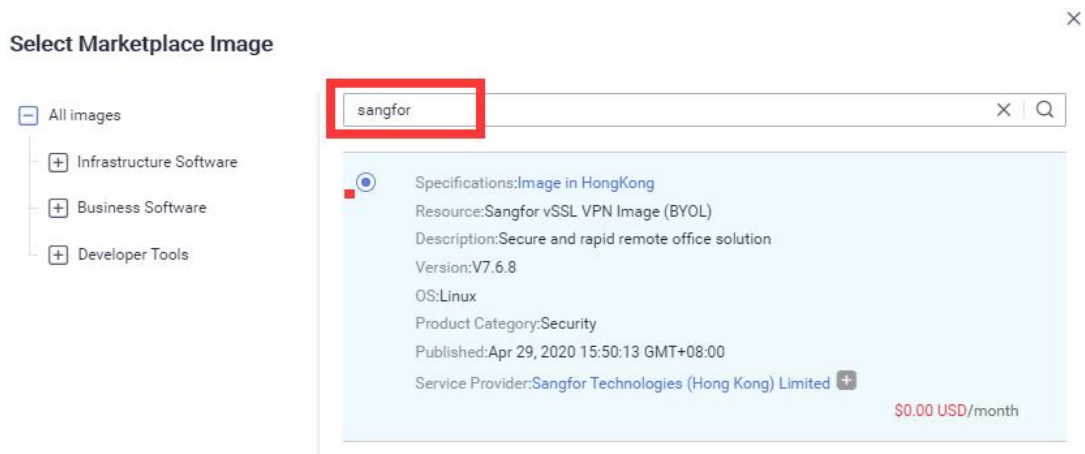
Install Image for Virtual Machine

Method 1:

Search “sangfor” in marketplace and select Sangfor vSSL VPN Image

The screenshot shows the Sangfor Marketplace search results for 'sangfor'. The search bar at the top contains 'sangfor' and a search icon. Below the search bar, there are navigation links for 'Marketplace', 'Categories', 'My Saved List', and 'Seller Learning Center'. The main content area displays 'All Categories (2 results)'. On the left, there are filters for 'Categories' (Infrastructure Software, Business Software, Developer Tools) and 'Operating Systems' (Windows, Linux). The search results list two items:

- Sangfor vSSL VPN Image (BYOL)**: Price is \$0.00 USD/hour. Description: Sangfor SSL VPN was born in 2005, focuses on the secure access and better user access experience for the remote office. Sangfor has accumulated more than 30... Image on Linux | Version V7.6.8 | Sold by: Sangfor Technologies (Hong Kon...)
- Sangfor vSSL VPN License**: Price is \$0.00 USD/month. Description: Sangfor SSL VPN was born in 2005, focuses on the secure access and better user access experience for the remote office. Sangfor has accumulated more than 30... License on Linux | Version V7.6.8 | Sold by: Sangfor Technologies (Hong Kon...)



Method 2:

Request Image from Sangfor and install Image from private image or shared image

Initialize Network

Start vSSL VPN Virtual Machine and remote login from public cloud console.

1. Set intranet IP for vSSL VPN:

- vSSL VPN will automatically get IP address from DHCP server by default and we can show current network settings.
- We can also modify network by Network Setup Wizard



2. Associate EIP with vSSL VPN intranet IP or make DNAT policy in VPC NAT Gateway

3. Set Security Group in VPC

vSSL VPN Default Service Port:

Port	Function	Mandatory or not	Modifiable or not

TCP 80	Path selection in multi-line network environment	No	Support
TCP 443	User access	Yes	Support
TCP 4430	Management port for Administrator	No	Support
TCP 51111	Firmware upgrades port	No	N/A
TCP 22	Shell port only for Sangfor engineer troubleshooting	No	N/A

Chapter 2 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://EIP:4430>.

Logging in to Admin Console

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



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

2. Enter the administrator username and password and click the **Log In** button. The default administrator username and password are **admin** (case-sensitive). You can also choose page language at the upper right corner of the login page as per your need .
3. For version information of the software package, click on **Version** below the textboxes.

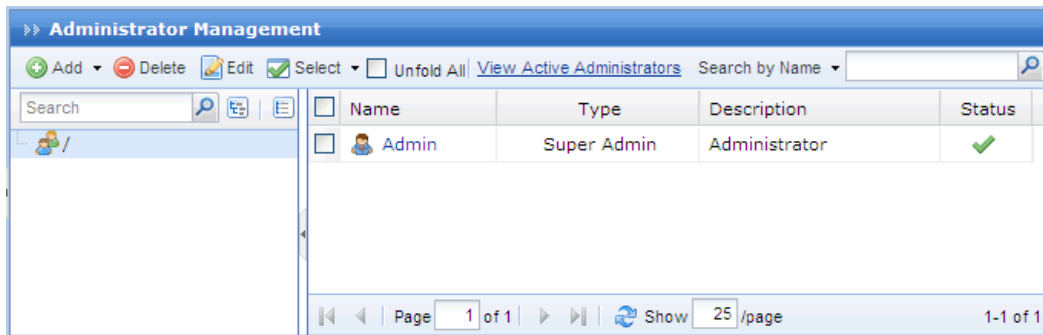
Modifying Administrator Password

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

To modify default administrator password, perform the following steps:

1. Navigate to **System > Administrator** to enter the **Administrator Management** page. The

default administrator account (super administrator) is as seen in the figure below:



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

Add/Edit Administrator

Basic Attributes Fields marked * 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

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



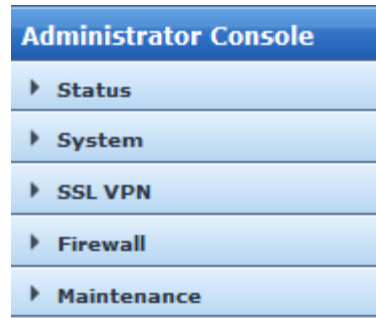
- Password of the account **Admin** should not be shared with anyone.
- If the Sangfor device is to be maintained by several administrators, create multiple administrator accounts for segregation of duty.

Chapter 3 System and Network Settings

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

There are five configuration modules in all:

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



System Settings

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

Configuring License

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

There are two methods to get a trial license.

Method 1: Online Authorization (Requires a Chinese phone number to receive SMS from Sangfor Authorization server)

Method 2: Contact with local Sangfor teams get a trial license.

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

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

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

Upgrade License: The license is used to update the current SANGFOR SSL VPN system with Sangfor Firmware Updater 6.0 (for more details, refer to Appendix 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.



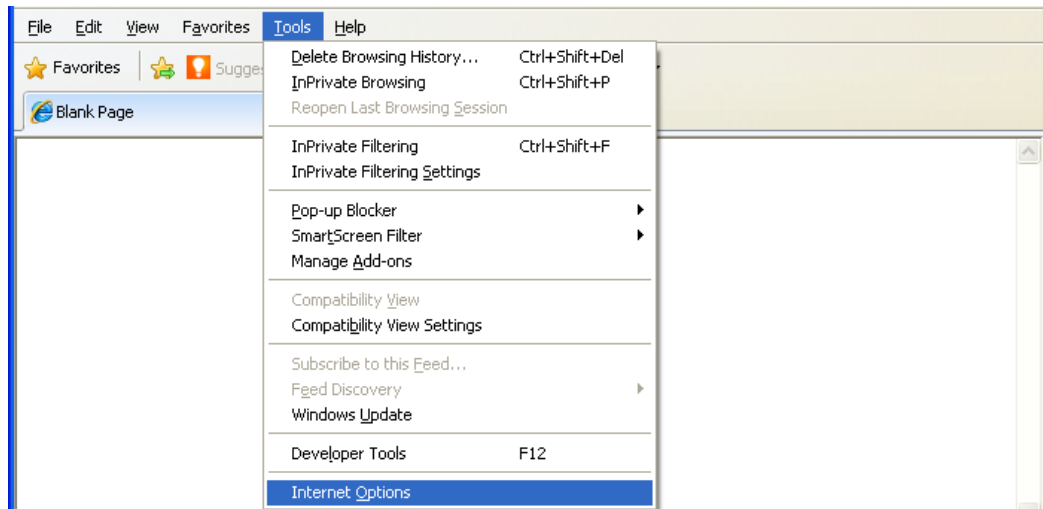
-
- Operating systems should be 32bit/64bit Windows XP/2003/Vista/Win7/Win10, 32bit Linux Ubuntu 11.04/RedHat 5.2/RedFlag/Fedora 13/SUSE 11.2, or Mac OS X Leopard(10.5)/Snow Leopard(10.6)/Lion(10.7).
 - SSL VPN client is available on iPhone and Android mobile phones.
-

Configuring Browser and Accessing SSL VPN

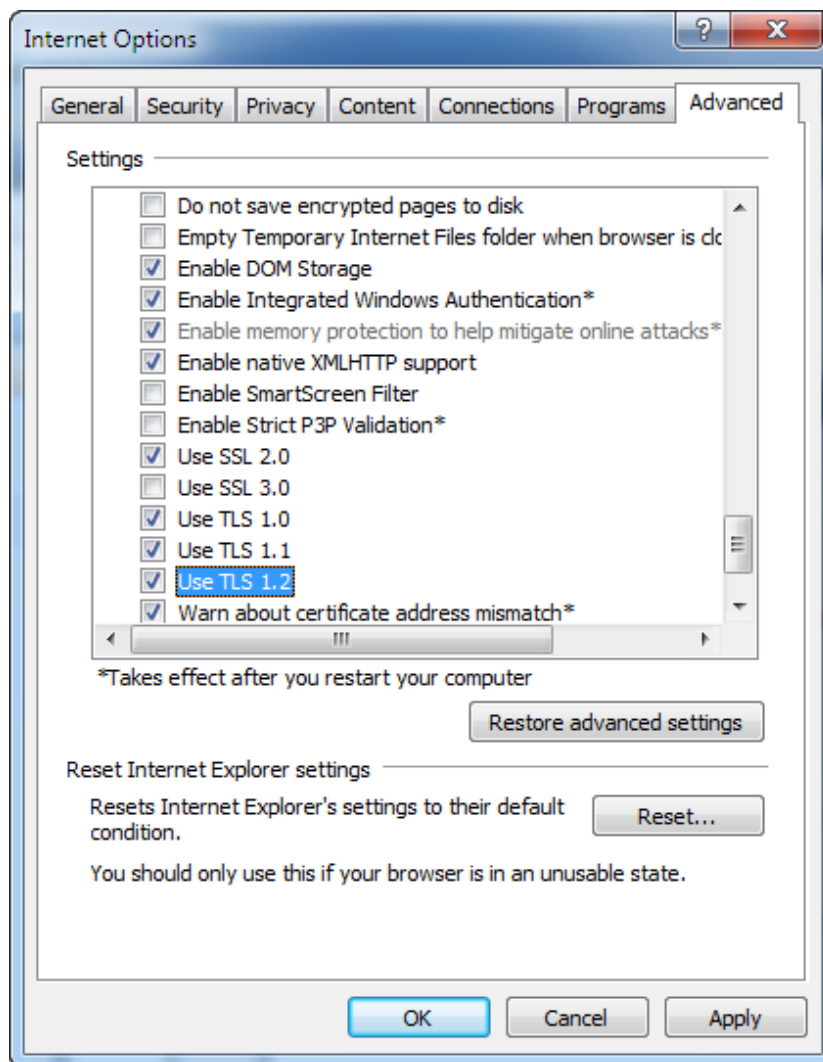
Configuring Browser

The following configuration takes Windows XP IE browser for example. Screenshots may vary with different operating systems.

1. Launch the IE browser and go to **Tools > Internet Options** to configure the IE browser, as shown in the figure below:



2. Click **Advanced** tab. Find the **Security** item and select the checkboxes next to **Use SSL 2.0**, and **Use TLS 1.0**, as shown in the figure below:

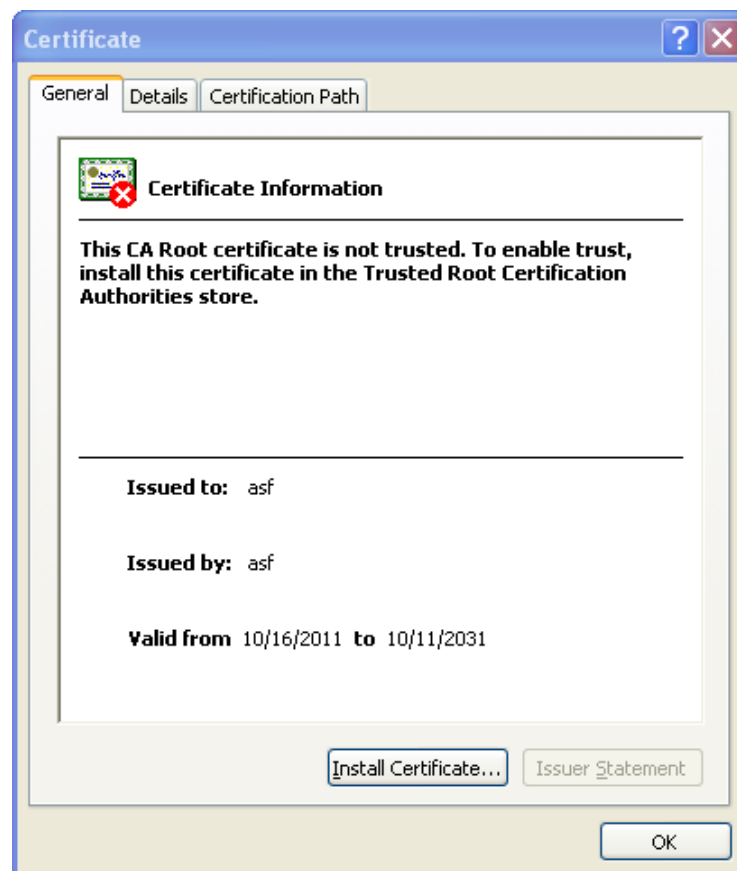


3. Enter the SSL VPN address into the address bar of the browser and visit the login page to SSL VPN.

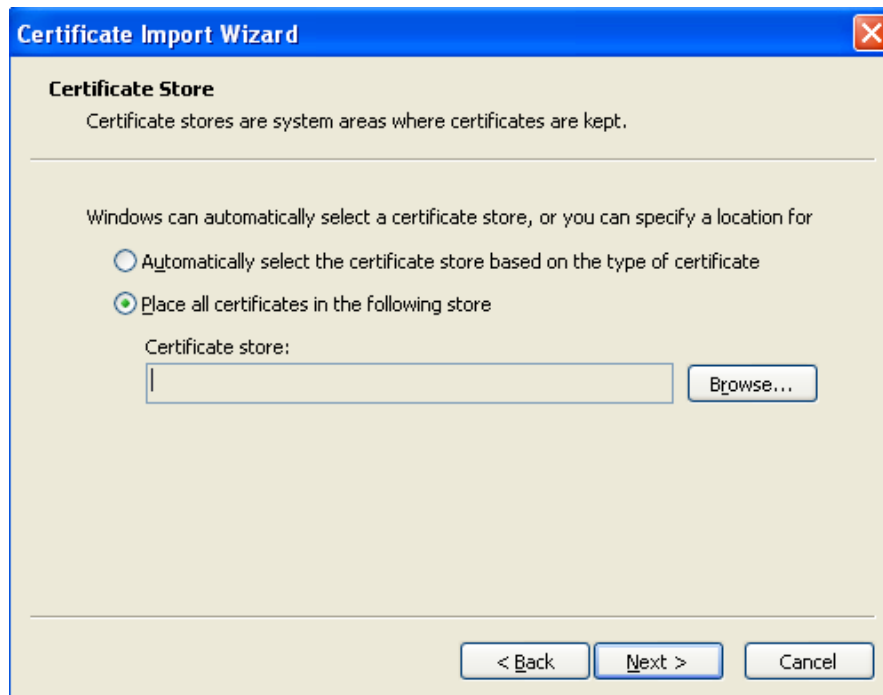
- When you visit the login page, a security alert may appear, requiring installation of security certificate, as shown in the figure below:



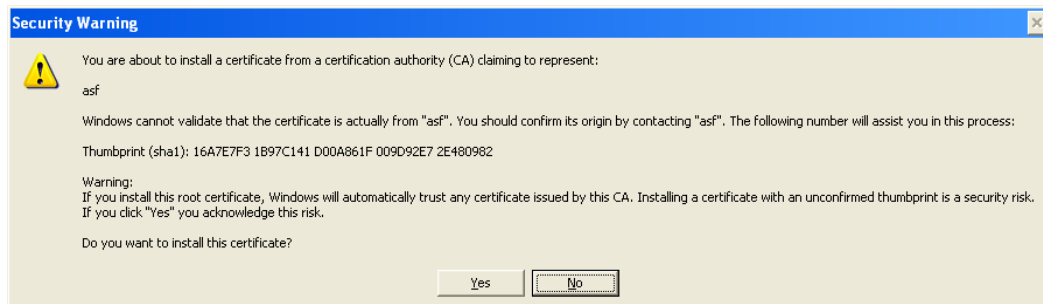
- Click the **View Certificate** button to complete installing the root certificate if this is the first time you log in to SSL VPN administrator Web console. The information of the root certificate is as shown below:



- Click the **Install Certificate** button and use the **Certificate Import Wizard** to import the root certificate, as shown in the figure below:



7. Select a directory to store the certificate and click the **Next** button. After confirming the settings and clicking the **Finish** button, another warning pops up asking whether to install the certificate, as shown in the figure below:



8. Click the **Yes** button to ignore the warning and the root certificate will be installed, as shown in the figure below:



Generally, root certificate is required to be installed when you logs in to the SSL VPN for the first time. Once root certificate is installed, you need only click the **Yes** button next time when logging in and see the security alert.

Using Account to Log In to SSL VPN

If root certificate has been installed, user can visit the login page to the SSL VPN. The login page is as shown in the figure below:



Access SSL VPN

Username:

Password:

Verification: t NZ q

Log In

Other Login Methods:

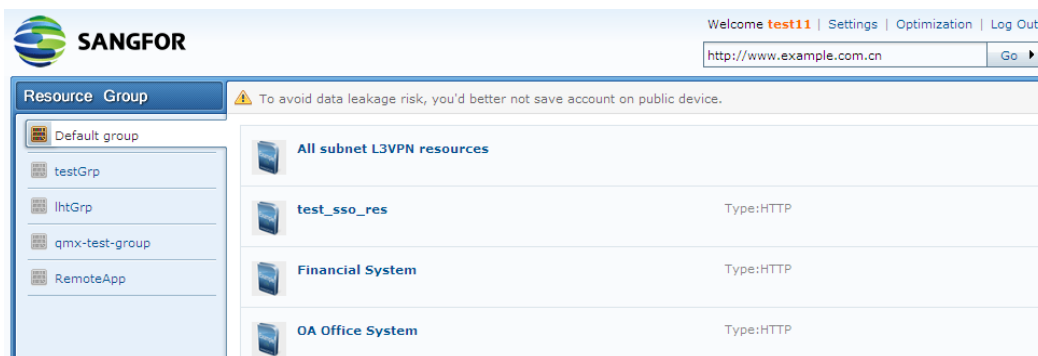
- Failed to read USB key. Please [install USB key driver](#).
- Login error. Please download SSL VPN repair tool to [repair components](#).
- For more help information, [click here](#)

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 get authenticated may need to install the USB key driver. For detailed guide, please refer to the SSL VPN Users section in Chapter 4.

2. Once user passes the required primary and secondary authentications, he/she will enter the **Resource** page, as shown in the figure below:

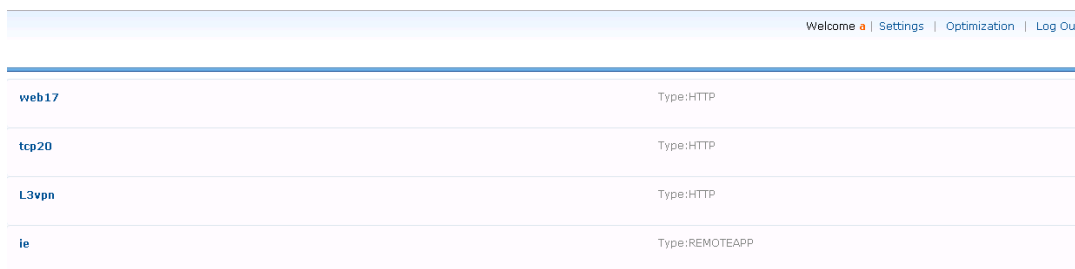


- All the resources or groups associated with the connecting user will be displayed on the **Resource** page. Click on any of the links to access the corresponding resource.

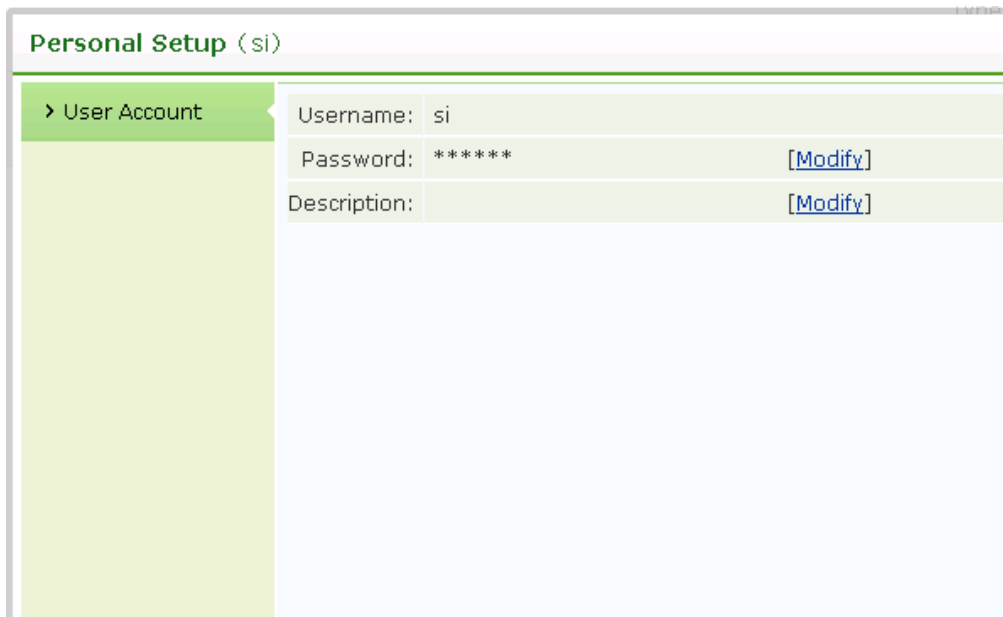
For Web application resources, user can access them simply by clicking on the resource link.

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.

- TCP and L3VPN components will be installed automatically when user accesses associated TCP resource or L3VPN resource.



- 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.
- 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:

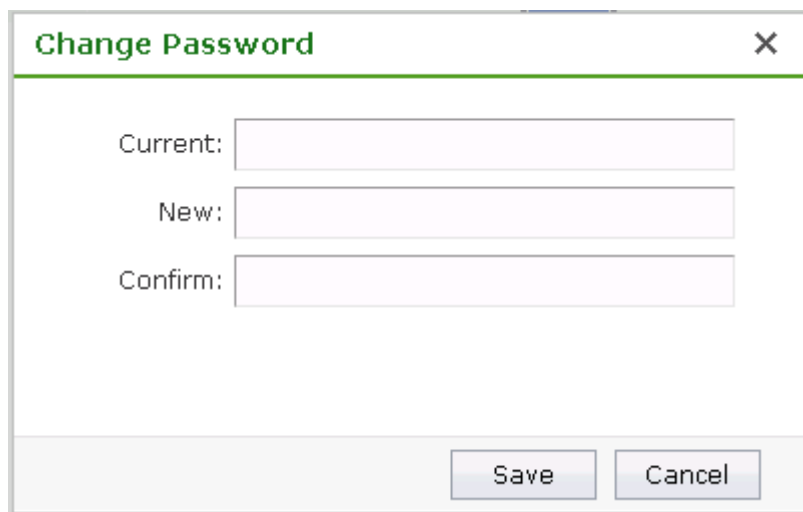


Personal Setup (si)

> User Account

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

As shown above, the current password is followed by **Modify**. Click it to enter the **Modify Password** page, as shown below:



Change Password [X]

Current:

New:

Confirm:

Save Cancel



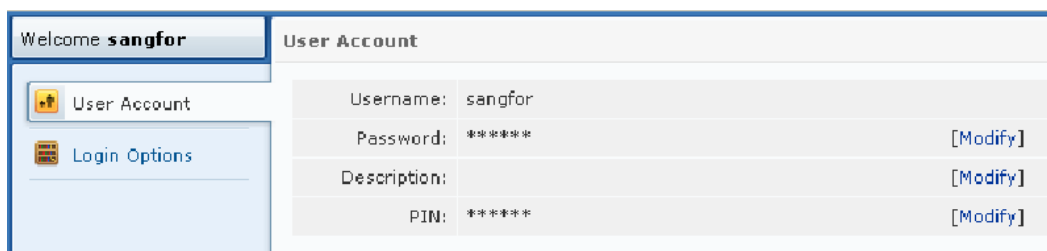
- If user keeps inactive for a long time during SSL VPN access, without performing any operation or accessing any resource, user will be disconnected and log out automatically.
- The contents shown in **Settings** are related with SSL VPN configurations. Those contents will be taken valid.

Using USB Key to Log In to SSL VPN

User login using USB key is a bit different from that using account.

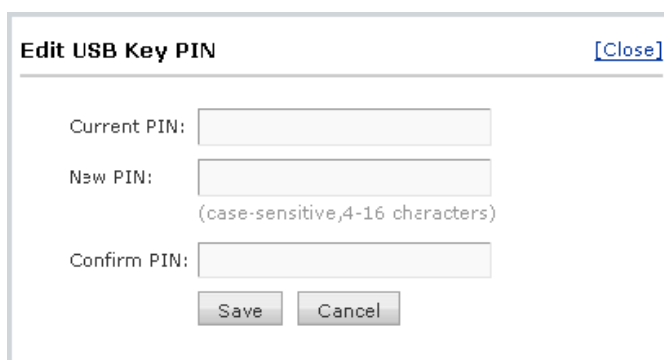
Main differences are the login process and login page. User should perform the following:

1. Launch the browser and visit the login page to the SSL VPN.
2. Insert the USB key into the USB port of the computer.
3. Select other login method **Use USB Key** to enter the next page that asks for PIN of the USB key.
4. Enter PIN of the USB key and login process completes.
5. To modify PIN of the USB key, click **Settings** at the upper right of the **Resource** page to enter **User Account** page, as shown below:



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 [Close]

Current PIN:

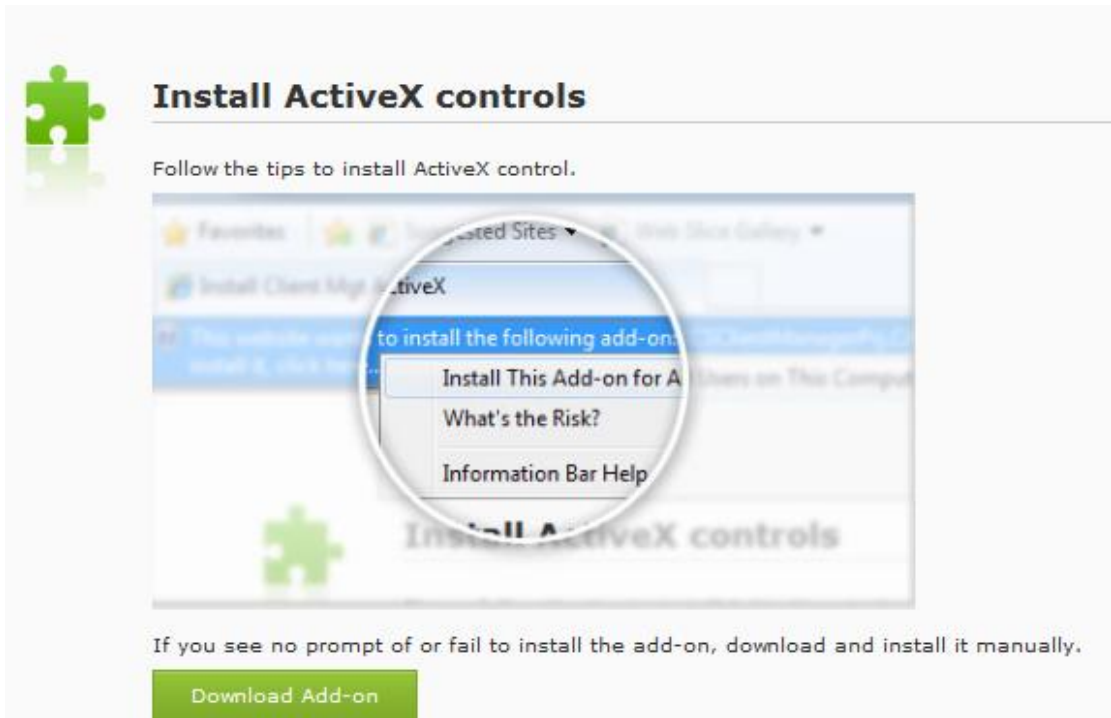
New PIN:
(case-sensitive, 4-16 characters)

Confirm PIN:

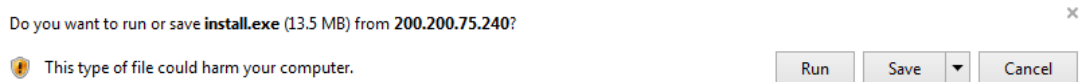
Save Cancel

Using VPN Client to Log In SSL VPN

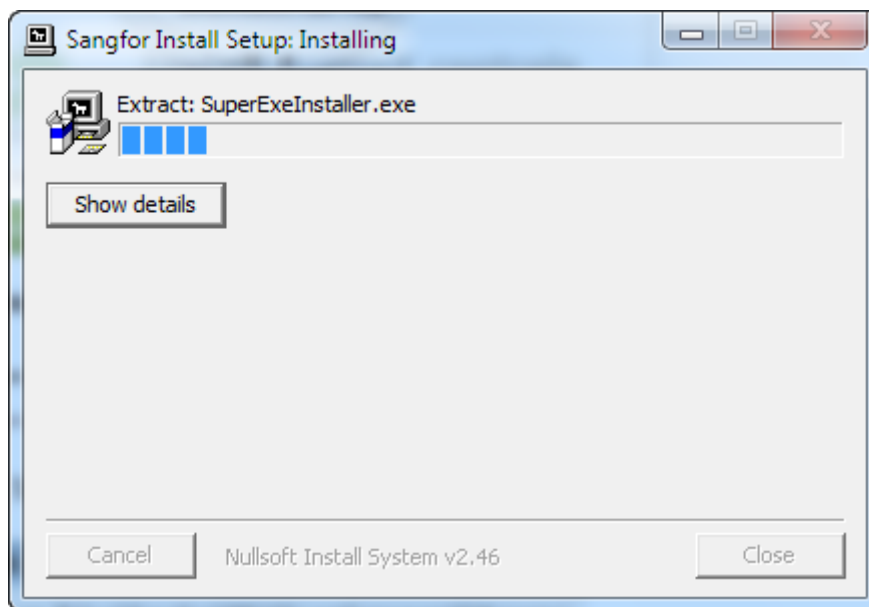
SSL VPN client components will be installed automatically when user logs in SSL VPN through IE browser. On **System > SSL VPN Options > Client Options** page, you can enable client software installer to be installed automatically or manually when required. If **Manually** corresponding to the **Install Client Software Installer when required** option is selected on the Sangfor device, the following page will pop up when user logs in VPN, as shown below:



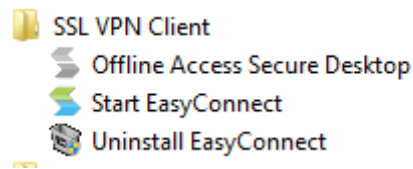
Click **Download Add-on**, a dialog appears, as shown below:



To install it, click **Run**. You will see the following installation page.

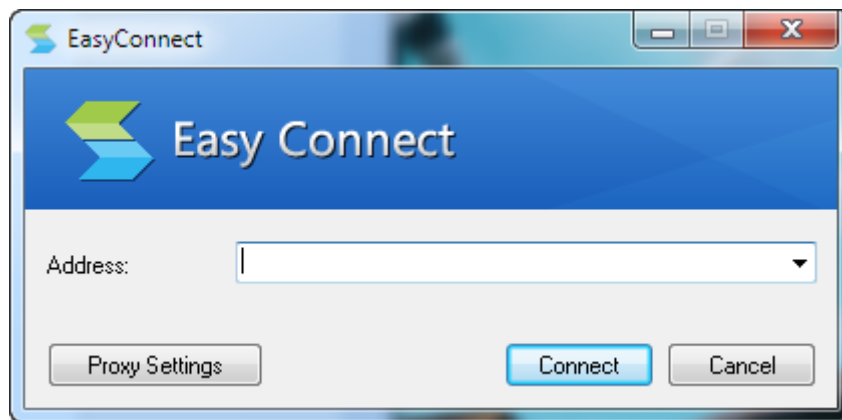


After software installer is installed, navigate to **Start > Programs** and you will see the following directory, as shown below:

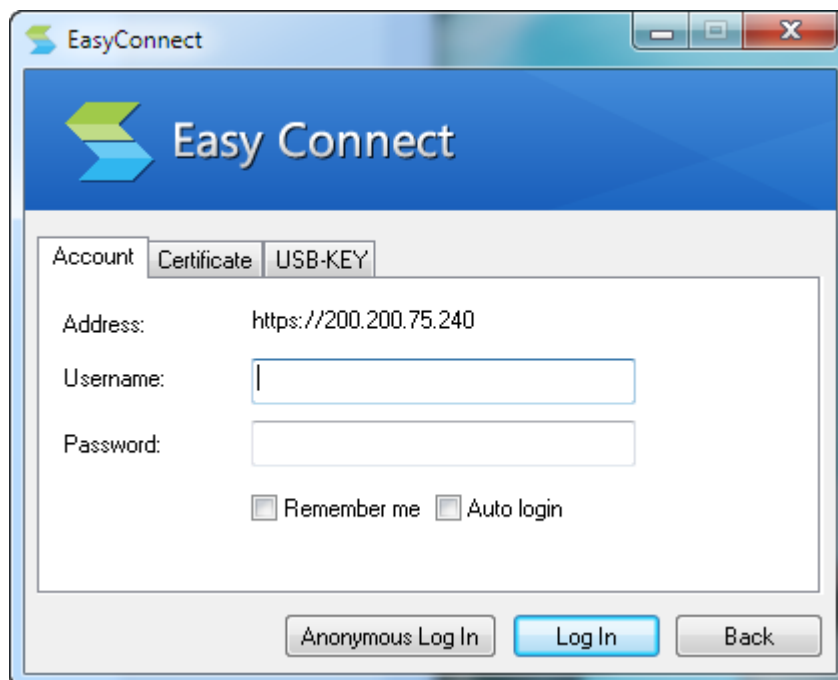


Please terminate firewall and antivirus software when installing client software installer; otherwise, the client will fail to be installed.

1. Click **Start EasyConnect** to open the SSL VPN client window, as shown below:

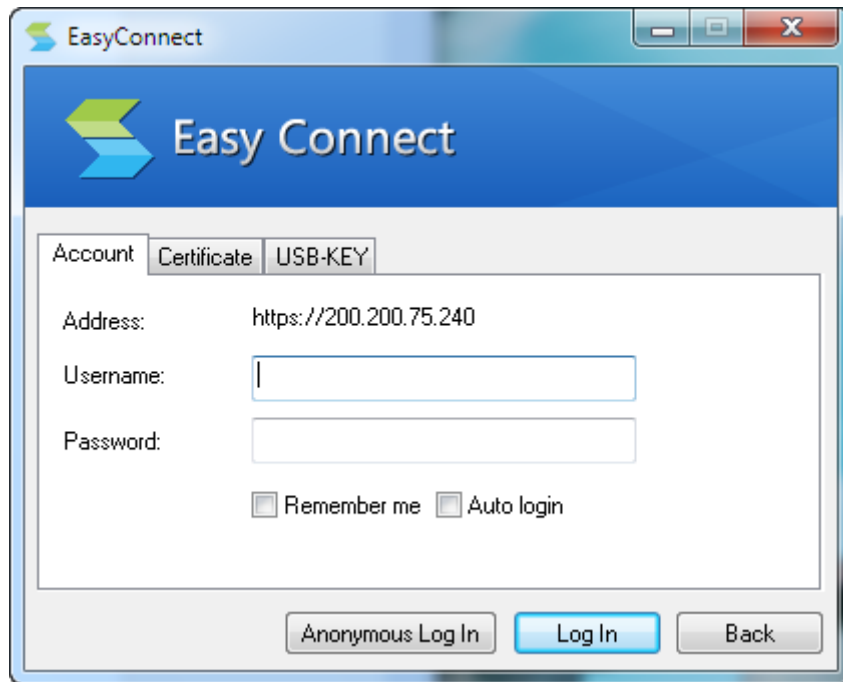


2. Enter the address of SSL VPN and click **Connect**, the following dialog appears.



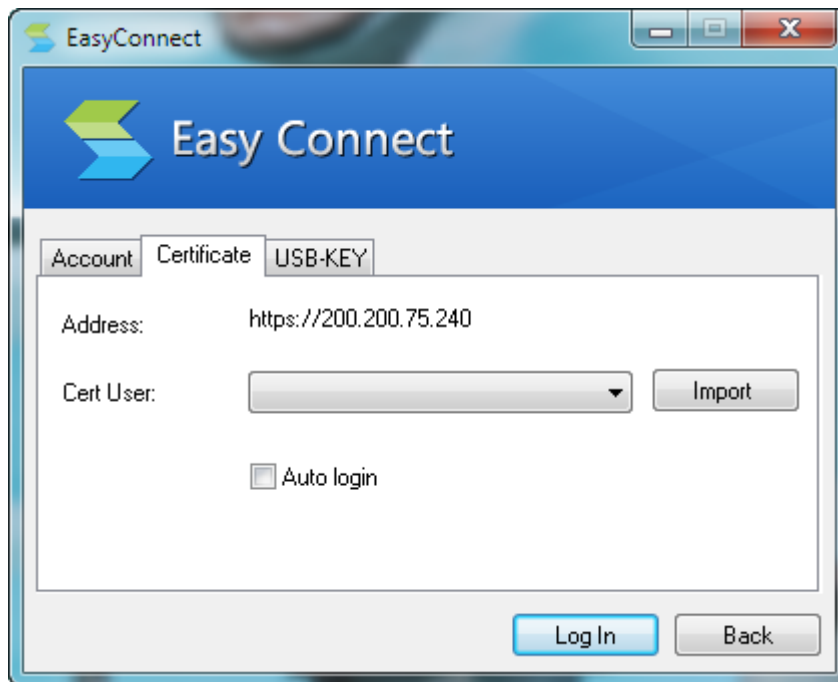
- For authentication based on username and password, select **Account**. The **Account** tab is as

shown in the figure below:

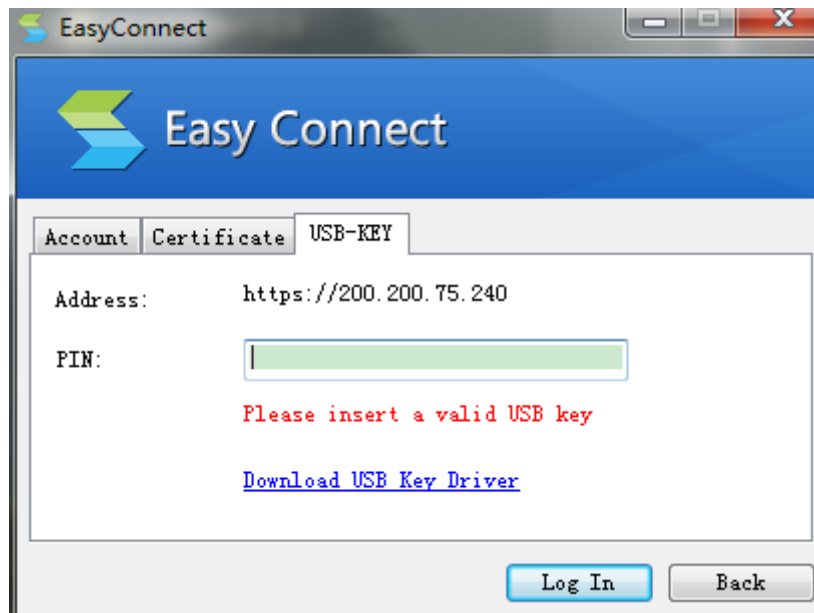


User can select **Remember me** and **Auto login** options if required, then he/she does not need to enter these information upon next login. The two options are available only when they are enabled on the device(for details, refer to Client Options in Chapter 3).

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



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

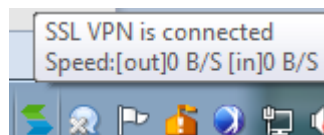


To create SSL VPN user, refer to Adding User in Chapter 4.

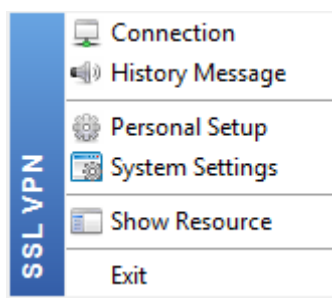
3. Select an authentication method as per your case. After logging in, a prompt dialog appears, as shown below:



If system tray is enabled when configuring Client Options on Sangfor device, the VPN client logo will be shown on the lower-right corner of the desktop. Put the cursor on it, you can see the connection status and VPN flow speed, as shown below:



To view VPN connection status and configure VPN-related settings, right-click on the **System Tray** icon and you will see the following floating window, as shown below



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

enabled.

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

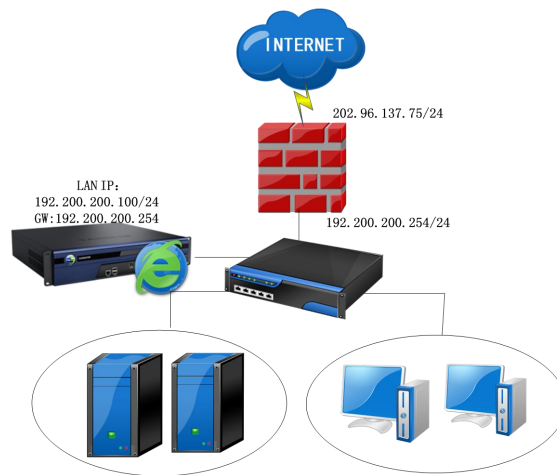
Network Settings

Device Deployment

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

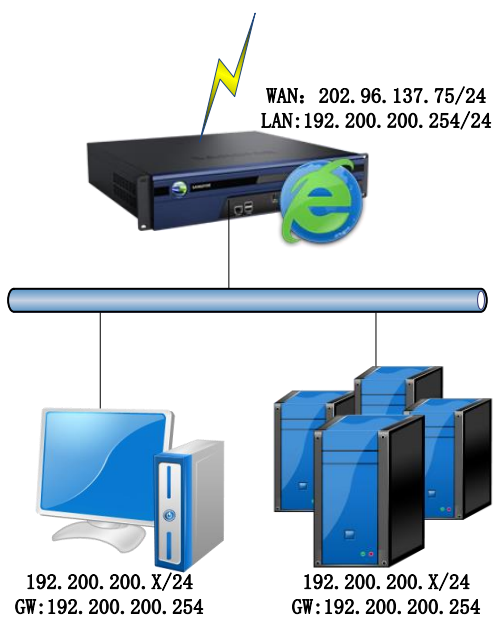
Single-Arm mode:

SSL VPN deploy as a server connecting to an intranet switch



Gateway mode:

SSL VPN deploy as a Router in the network edge



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

The screenshot shows the 'Deployment' configuration page in a web interface. At the top, there are tabs for 'Deployment', 'Multiline Options', 'Routes', 'Hosts', 'DHCP', and 'Local Subnets'. The 'Deployment' tab is active. Below the tabs, the 'Deployment' section is titled, and a note states 'Fields marked * are required'. The 'Mode' is set to 'Single-Arm' (selected with a radio button) and 'Gateway' (unselected). A text box below the mode selection contains the text: 'The device connects to Internet via front-end device.' The 'Internal Interfaces' section is divided into two columns. The left column is for the 'LAN' interface, with fields for IP Address (200.200.75.240), Netmask (255.255.252.0), Default Gateway (200.200.75.254), Preferred DNS (202.96.134.133), and Alternate DNS (empty). The right column is for the 'DMZ' interface, with fields for IP Address (10.254.253.195) and Netmask (255.255.255.0). A 'Multi-IP' button is located below the LAN fields. The 'Link Status' section at the bottom shows icons for LAN, DMZ, WAN1, and WAN2, with LAN and DMZ showing green status and WAN1 and WAN2 showing red status. At the very bottom, there are 'Save' and 'Cancel' buttons.

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 Multiline Options Routes Hosts DHCP Local Subnets

Deployment Fields marked * are required

Mode: Single-Arm Gateway

WAN and LAN interfaces need to be configured.

Internal Interfaces

LAN:

IP Address: *

Netmask: *

DMZ:

IP Address: *

Netmask: *

External Interfaces (WAN Interfaces)

Line	Type	IP Address	Netmask	Default Gateway	Status
Line 1	--	--	--	--	Disabled
Line 2	--	--	--	--	Disabled

Link Status

LAN
 DMZ
 WAN1
 WAN2

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 address and DNS server below

IP Address: 0.0.0.0 Preferred DNS: 0.0.0.0

Netmask: 0.0.0.0 Alternate DNS: 0.0.0.0

Default Gateway: 0.0.0.0 MTU: 1500

Multi-IP

Advanced

Save Cancel

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

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

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

IP address and DNS server could be assigned automatically or configured manually. The former is achieved by selecting the option **Obtain IP and DNS server using DHCP**, and the latter means that administrator needs to select the option **Use the IP and DNS server below** and configure the IP address, default gateway and DNS servers.

- **Multi-IP:** This button is only available for **Ethernet** type of Internet line, which means multiple IP addresses can be set on WAN interface. Click this button and the following dialog pops up, as shown below:

Multi-IP

+ Add - Delete

IP Address	Netmask

Save Cancel

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

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



In gateway mode, LAN, DMZ, and WAN interfaces cannot be configured on the same subnet.

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

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

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

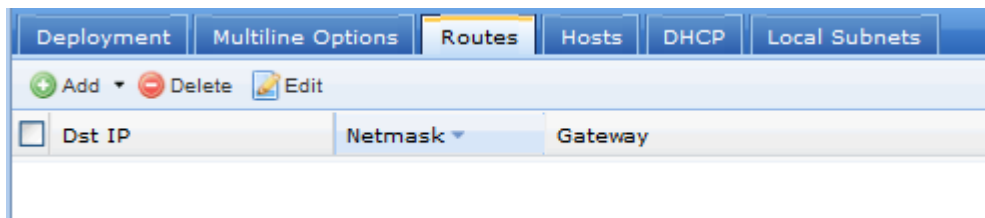
For detailed information of dialup, click **Details**.

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

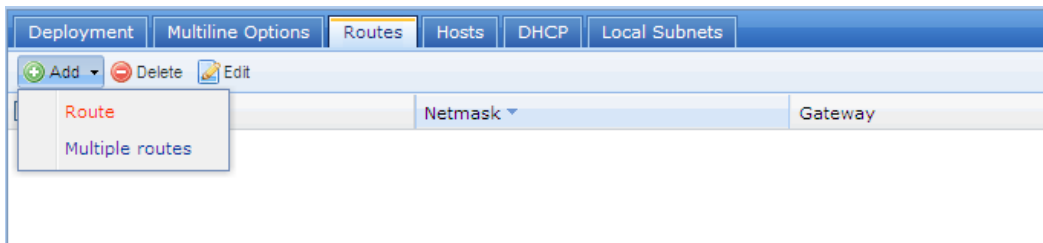
Configuring Route

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 Route

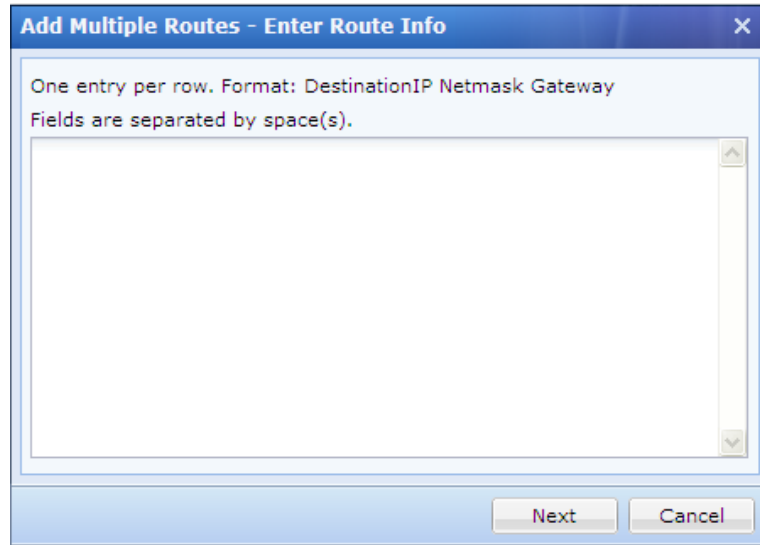
Please fill in the correct route information.

Dst IP: *

Netmask: *

Gateway: *

Save and Add Save Cancel



SSL VPN Options

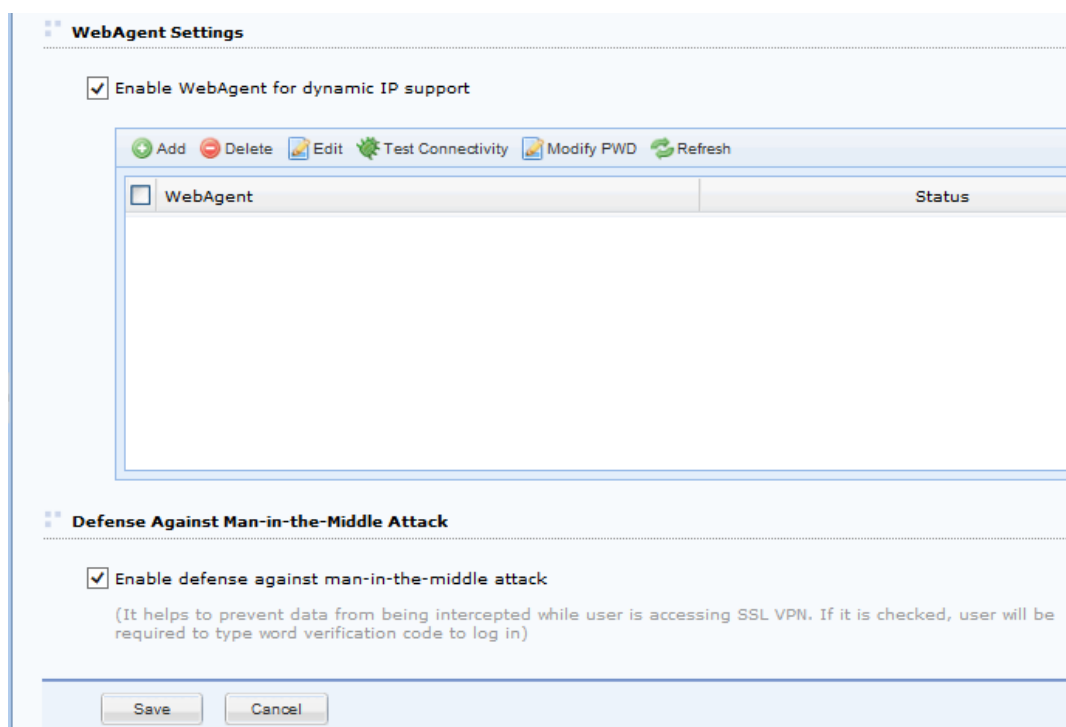
General Settings

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

Configuring User Login Options

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

The screenshot shows the configuration interface for the Login section. At the top, there are tabs for Login, Client Options, Virtual IP Pool, Local DNS, SSO, and Resource Options. The Login Port section includes fields for HTTPS Port (443) and HTTP Port (80), with an Edit button. The PPTP/L2TP Connection Options section has radio buttons for Prohibit PPTP/L2TP incoming connection, Permit PPTP incoming connection (selected), and Permit L2TP incoming connection. Below this is a field for L2TP Shared Secret. A text box contains instructions: 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, Sangfor VPN service will still be available. The Encryption Protocol section has radio buttons for RSA (selected) and SM2, and checkboxes for SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2.



2. Configure the following fields under **Login Port**.
 - **Login Port:** Specifies the HTTPS and HTTP port on which the SSL VPN service is being listened.
 - **HTTPS Port:** Specifies the HTTPS listening port. It is TCP 443 by default. Enter the port(s) into the field (ports should be separated by comma) or click the **Configure** button.
 - **HTTP Port:** Select this option and enter the HTTP listening port. It is TCP 80 by default.
3. Configure the following fields under **Login PPTP/L2TP Connection Options**.
 - **Prohibit PPTP/L2TP incoming connection:** If it is selected, PPTP/L2TP connection will be denied.
 - **Permit PPTP incoming connection:** Select it to allow PPTP incoming connection, and user can access L3VPN resources on mobile phone via VPN.
 - **Permit L2TP incoming connection:** Select it to allow L2TP incoming connection. If it is selected, you need to specify L2TP shared secret.
 - **L2TP Shared Secret:** Specifies L2TP shared secret, then user can access L3VPN resources on mobile phone via built-in L2TP VPN.

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

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

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

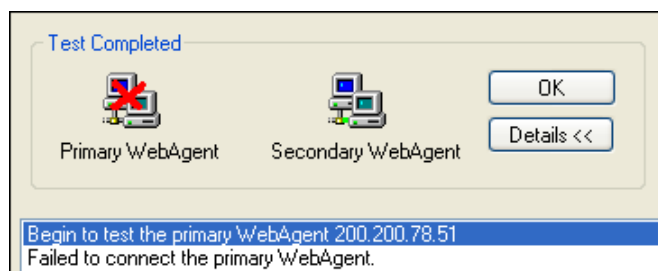


- Do not modify the ports unless it is absolutely necessary. Once the port is altered, the new port number should be entered to the end of the URL address when endpoint user enters the address to connect SSL VPN.
 - If the checkbox next to **HTTP Port** is selected, user can use HTTP protocol to communicate with the SSL VPN. Access to SSL VPN is achieved by redirecting HTTP to HTTPS, for instance, *http://202.96.137.75* is redirected to *https://202.96.137.75*. If **HTTP Port** is selected and configured, user can only use HTTPS protocol, in which case, he/she needs to visit <https://202.96.137.75>.
 - If **Permit L2TP incoming connection** is selected, user will be denied to connect to VPN through standard IPsec VPN, while users will be allowed to connect to VPN through Sangfor IPsec VPN.
4. Select encryption protocol for encrypting data. Options are **RSA**, **SM2**, **SSL3.0**, **SSL1.0**, **SSL1.1**, **SSL1.2**, as shown below:

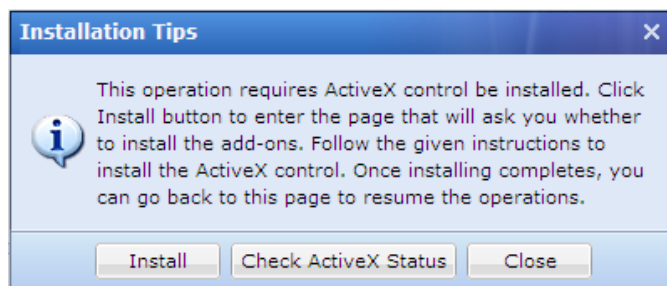
5. Configure **WebAgent Settings**. Select **Enable WebAgent for dynamic IP support** to enable this feature, and the Sangfor device will be able to get an IP using WebAgent dynamic addressing if it is not using a static Internet IP address. To add a Webagent entry:

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

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

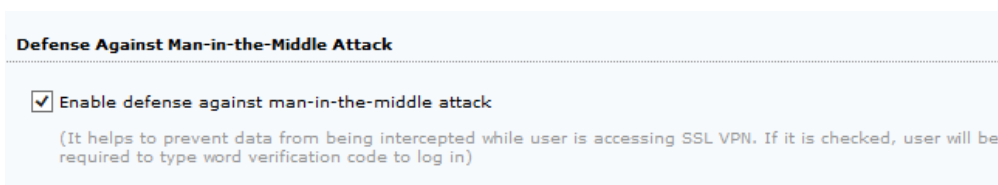


Before test begins, certain ActiveX control may need be installed (as shown below).



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

- d. To remove or edit a WebAgent entry, select the desired entry and click **Delete** or **Edit**.
 - e. To modify password of a WebAgent select the desire entry and click **Modify PWD**. Modifying password can prevent unauthorized user from using and updating a false IP address into the WebAgent page,
 - f. To refresh the status of the WebAgent, click **Refresh**.
6. Configure **Defense Against Man-in-the-Middle Attack** option.



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

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

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:

Alternate DNS:

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

+ Add - Delete Edit Select

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.

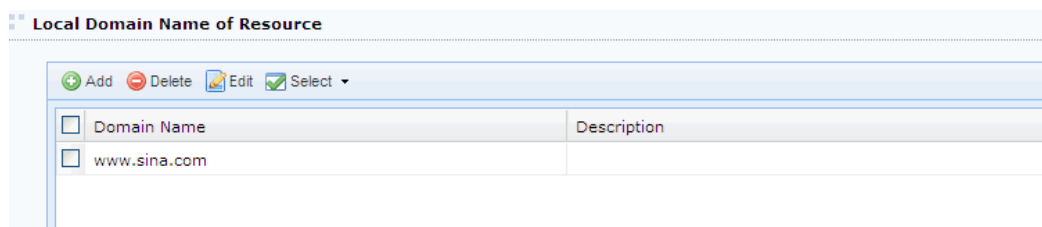
3. Configure **Client PC uses the above DNS servers** option.

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 name as their addresses, administrator needs to add the address (in form of domain name) of resource into

the list followed after specifying the local DNS servers. Later on, once a user accesses any of these resources by domain name, the local DNS server will resolve the requested domain name first, according to the local DNS server and domain names configured on this tab.

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



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

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

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



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

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

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



Beyond local DNS, the internal HOSTS file will also help to resolve the matching domain name and return the resolving result to user (refer to the **错误!未找到引用源。** S) section in Chapter 3).



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

Chapter 4 SSL VPN

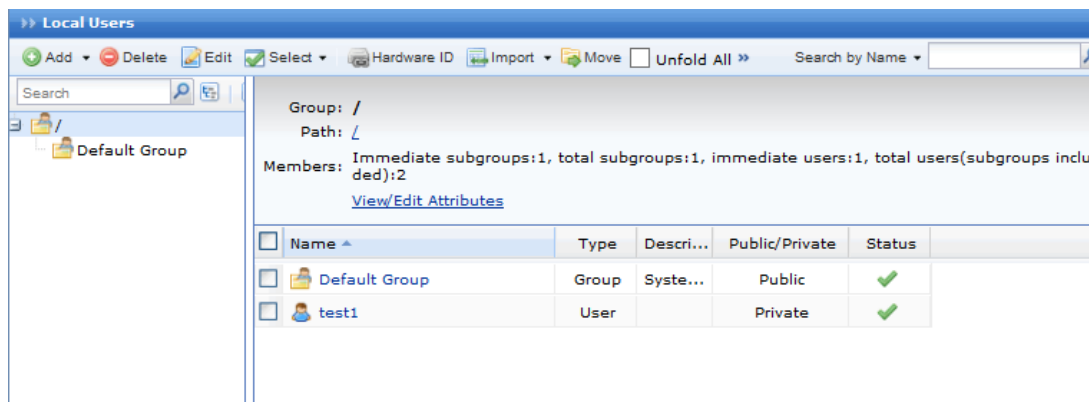
SSL VPN covers configurations of **Users**, **Resources**, **Roles**, **Authentication**, **Policy Sets**, **Remote Servers** and **Endpoint Security**.

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

SSL VPN Users

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

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



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

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

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

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

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

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

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

Adding User Group

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

Add User Group

Fields marked * are required

Basic Attributes

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

Require: Both Either

Secondary Authentication

Hardware ID

SMS password

Dynamic token

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:

[Create + Associate](#)

2. Configure **Basic Attributes** of the user group. The following are basic attributes:
 - **Name:** Enter a name for this user group. This field is required.
 - **Description:** Enter brief description for this user group.
 - **Added To:** Select the user group to which this user group is added. / indicates root group.

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

3. Configure **Authentication Settings**.

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

At least one primary authentication method should be selected, **Local password**, **Certificate/USB key** or **External LDAP/RADIUS**. However, two of them can form a combination.

- **Local password:** If this option is selected, the connecting users need to pass local password based authentication, using the SSL VPN account in this user group.
- **Certificate/USB key:** If this option is selected, all the user accounts in this group must own digital certificate or USB key (ordinary or driver-free USB key).
- **External LDAP/RADIUS:** If this option is selected, an external authentication server (LDAP or RADIUS server) should be specified, which means, the account user used to connect the SSL VPN must exist on the selected external authentication server (to configure external authentication server, refer to the LDAP Authentication section and RADIUS Authentication section in Chapter 4).
- **Require:** It helps to achieve combination of two primary authentication methods. Options are **Both** and **Either**.

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

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



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

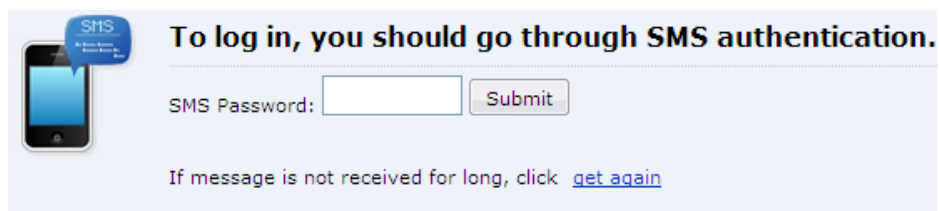
- **Secondary Authentication:** Secondary authentication is optional and supplementary authentication methods. Select any or all of them to require the connecting users to submit the corresponding credentials after he or she has passed the primary authentication(s), adding security to SSL VPN access.

- **Hardware ID:** This is the unique identifier of a client-end computer. Each computer is composed of some hardware components, such as NIC, hard disk, etc., which are unquestionably identified by their own features that cannot be forged. SSL VPN client software can extract the features of some hardware components of the terminal and generate the hardware ID consequently.

This hardware ID should be submitted to the Sangfor device and bind to the corresponding user account. Once administrator approves the submitted hardware ID, the user will be able to pass hardware ID based authentication when accessing SSL VPN through specified terminal(s). This authentication method helps to eliminate potential unauthorized access.

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

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

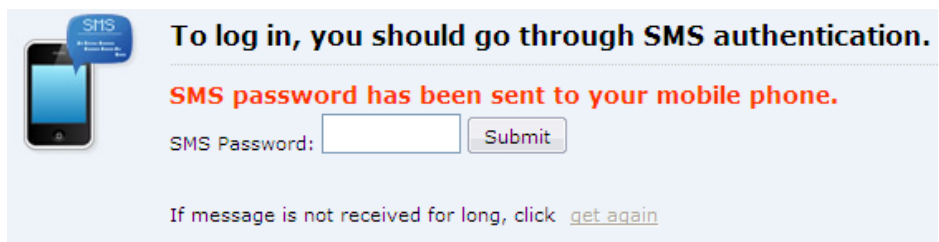


To log in, you should go through SMS authentication.

SMS Password:

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:

If message is not received for long, click [get again](#)



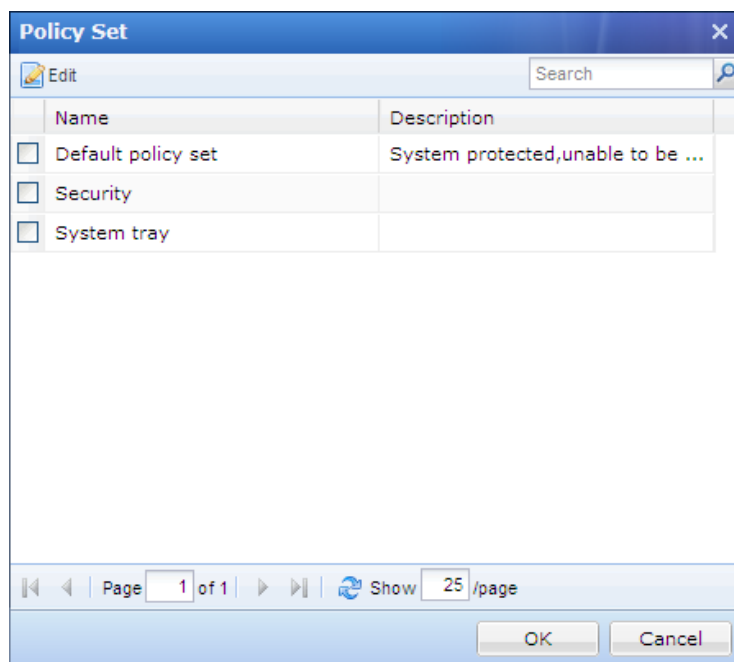
- By default, SMS authentication will not be enabled if mobile number is not configured. SMS authentication comes into use only after, a). mobile number has been configured; b). **SMS password** has been selected; c). the required options on **SMS Authentication** page have been configured properly.
 - 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 RADIUS Authentication section in Chapter 4).
 - **Enforce its users/subgroups to inherit the authentication settings:** If this option is selected, the subgroups and users included in this group will inherit the authentication settings configured above. However, its subgroups and sub-users could still use the other unselected authentication methods or use a different external authentication server, in addition to the inherited ones.

The combinations of authentication methods are as follows:

- a. Local password + SMS password/Hardware ID/Dynamic token
- b. Certificate/USB key + SMS password/ Hardware ID/Dynamic token
- c. External LDAP/RADIUS + SMS password/Hardware ID/Dynamic token
- d. Local password + Certificate/USB key + SMS password/Hardware ID /Dynamic token

- e. External LDAP/RADIUS + Certificate/USB key + SMS password/Hardware ID /Dynamic token
4. Associate policy set with user. A policy set is a collection of various access policies, which should be associated with user or group to control access to and use of SSL VPN (for details, refer to the Adding Policy Set section in Chapter 4).

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



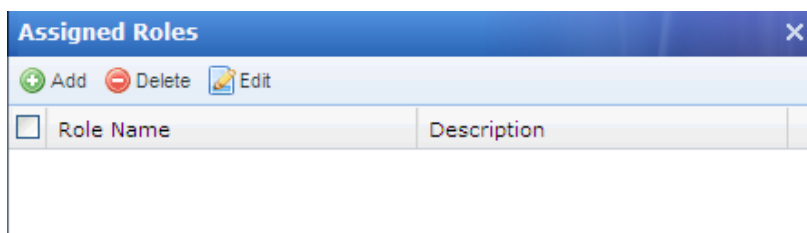
To edit a policy set, select a policy and click **Edit**.

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

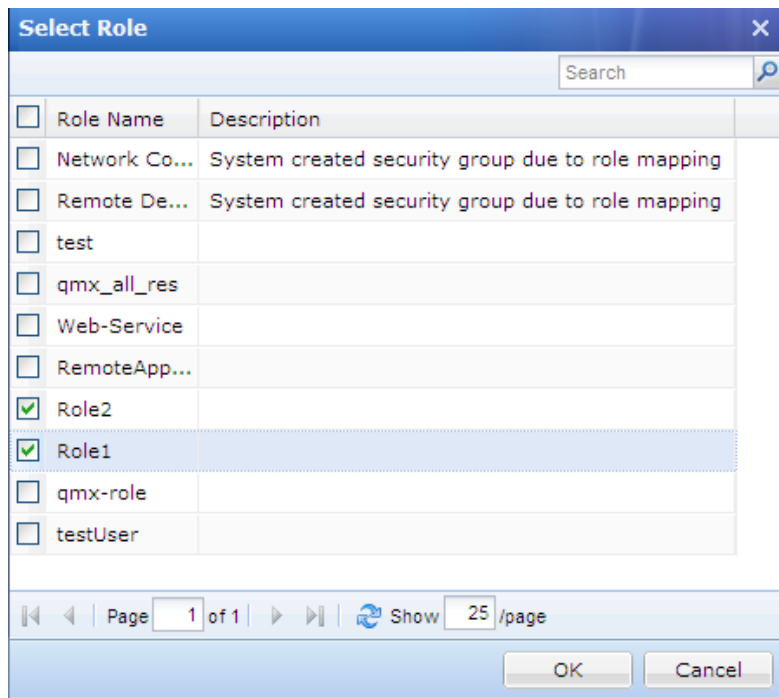
If the desired policy set is not found in the list, click **Create + Associate** to create a new policy set and associate it with the user group. The procedures of adding a policy set is the same as that in Adding Policy Set section.

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

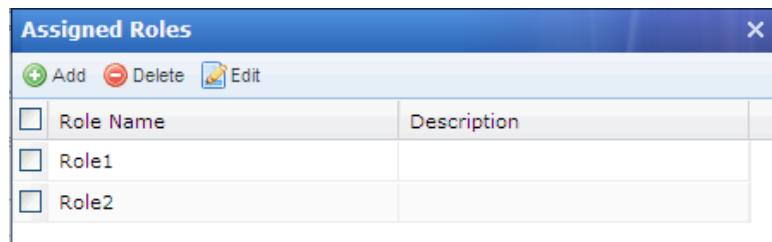
5. Assign roles to user group. For the procedures of configuring role, refer to the Adding Role section in Chapter 4.
- a. Click on **Roles** field to enter the **Assigned Roles** page, as shown below:



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



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



- d. Click the **OK** button and name of the assigned role is filled in the **Roles** field.
- e. If the desired role is not found in the list, click **Create + Associate** to create a new role and associate with the user group. The procedures of creating a role is the same as that in Adding Role section).
- f. To remove a role from the list, select the role and click **Delete**.
- g. To edit a role, select the role and click **Edit**.



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

Adding User

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

Add User

Fields marked * are required

Basic Attributes

Name: *

Description:

Password:

Confirm:

Mobile Number:

Added To:

Inherit parent group's attributes

Inherit policy set

Inherit authentication settings

Certificate/USB Key: none

Virtual IP: Automatic Specified

Expiry Date: Never Specified

Status: Enabled Disabled

Offline Access: Offline access is not enabled in policy set

Authentication Settings

User Type: Public user Private user

Primary Authentication

Local password

Certificate/USB key

External LDAP/RADIUS

Require: Both Either

Secondary Authentication

Hardware ID

SMS password based

Dynamic token

Policy Set

Policy Set:

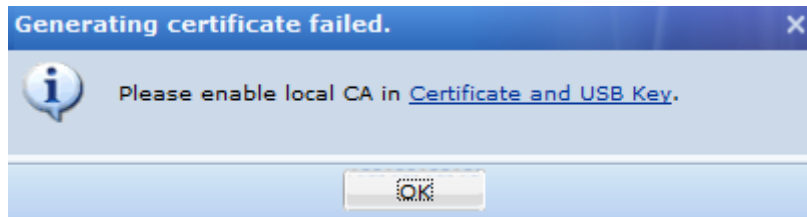
Assigned Roles

Roles:

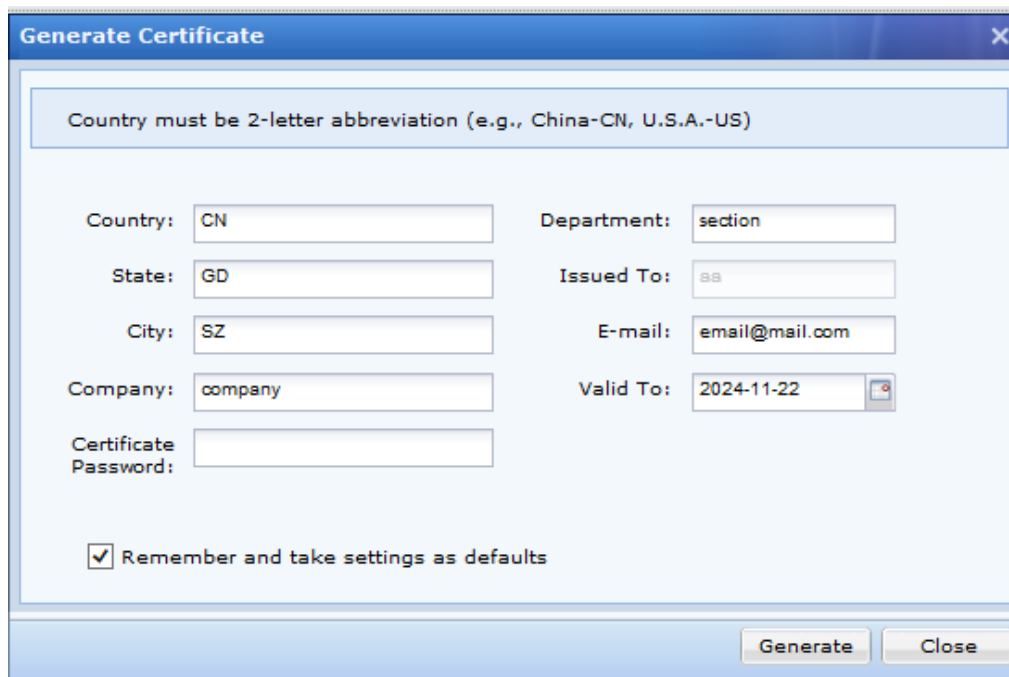
2. Configure **Basis Attributes** of user. The following are the basic attributes:
 - **Name:** Enter a name for this user. This field is required.
 - **Description:** Enter brief description for this user.
 - **Added To:** Select the user group to which this user is added.
 - **Password, Confirm:**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

parent group.

- **Inherit authentication settings:** Indicates that the authentication settings of this user are the same with its parent group.
3. Create and generate digital certificate for this user.
- a. To generate a certificate, local CA should be enabled on **SSL VPN > Authentication > Certificate/USB Key Based Authentication** page. If it is not enabled, click the **Generate Certificate** button and a prompt dialog will pop up, as shown below:



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



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

Country:	CN	Department:	section
State:	GD	Issued To:	ss
City:	SZ	E-mail:	email@mail.com
Company:	company	Valid To:	2024-11-22
Certificate Password:			

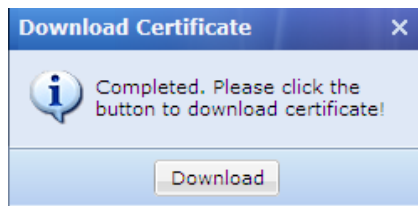
Remember and take settings as defaults

Generate Close

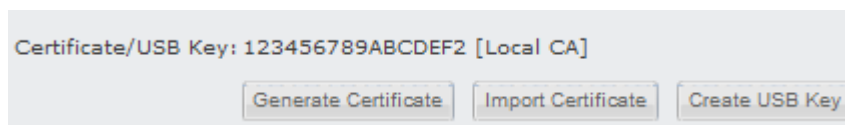
- b. Configure the fields on the above page. Since these fields are known by their name, we only introduce the following:
- **Issued To:** Indicates the username of the SSL VPN account. This field is read-only.
 - **Certificate Password:** This password is required while user imports or installs the digital certificate on his or her computer. Please inform the corresponding user of this password after configuration is completed.
- c. Select the checkbox next to **Remember and take settings as defaults** and the settings in all the fields will be remembered (exclusive of **Certificate Password** and **Issued To**)

and be re-used when generating certificate for users next time.

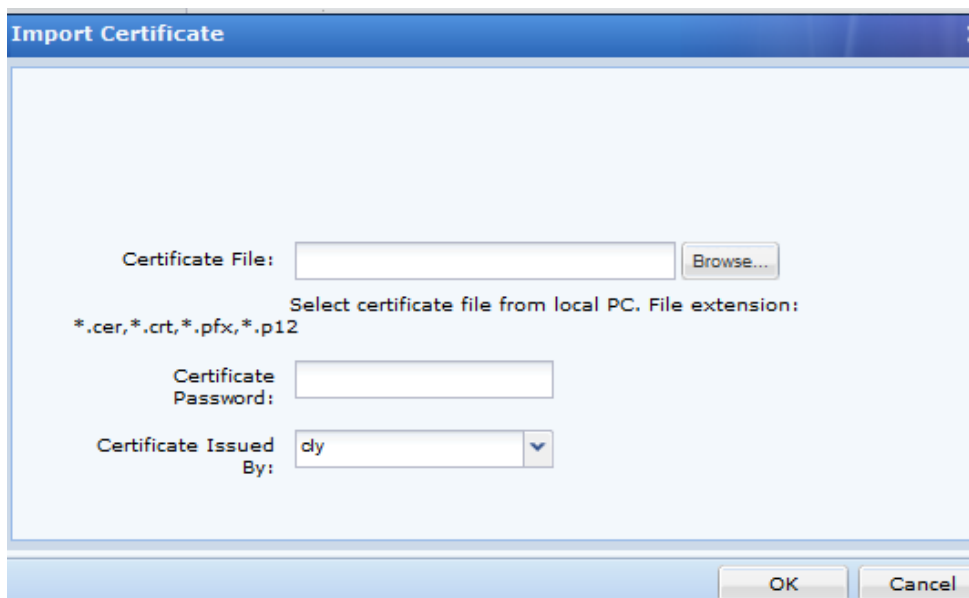
- d. Click the **Generate** button to start generating the certificate. When it completes, the following prompt appears:



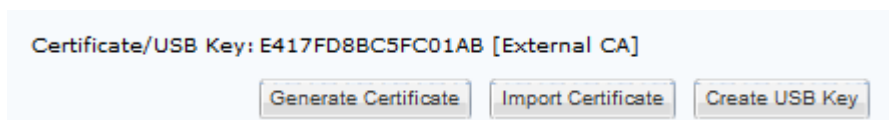
- e. Click the **Download Certificate** button and select a path to save the certificate to the computer. File extension of the certificate is .p12. Then certificate key will be shown in **Certificate/USB Key** field, as shown in the figure below:




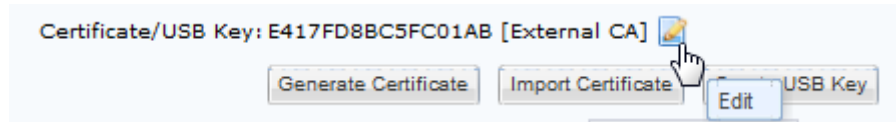
- f. **Import Certificate** option is used to import user certificate for the user being authenticated with third-party digital certificate. Click **Import Certificate** to enter the **Import Certificate** page, as shown below:



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



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



4. Generate USB key for the current user. The USB key can be with driver or no driver-free.
 - a. Navigate to **SSL VPN > Authentication > Authentication Options** and click the **USB Key Driver** link and **USB Key Tool** link to download and install USB key driver (file name is **dkeydrv.cab**) and USB key tool (file name is **DKeyImport.exe**) respectively, as shown in the figure below:

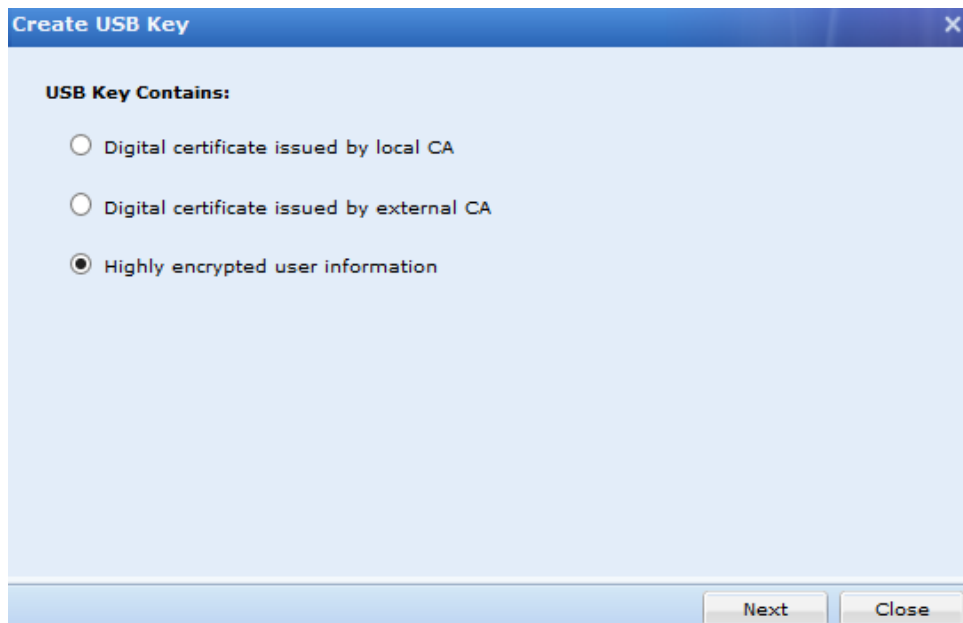


- b. Install the USB key driver as instructed.
 - c. Run USB Key Tool and install the tool on the computer.



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

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



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

The screenshot shows a window titled "Create USB Key" with a close button (X) in the top right corner. The main heading is "Digital certificate issued by local CA". Below this, there are several input fields arranged in two columns:

Country:	CN	Department:	section
State:	GD	Issued To:	s
City:	SZ	E-mail:	email@mail.com
Company:	company	Valid To:	2024-11-22
PIN:		Confirm PIN:	

Below the input fields, there is a checkbox labeled "Remember and take settings as defaults" which is checked. At the bottom of the main area, there is a text box containing the instruction "Plug in the USB key and click Create." At the very bottom of the window, there are three buttons: "Back", "Create", and "Close".

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

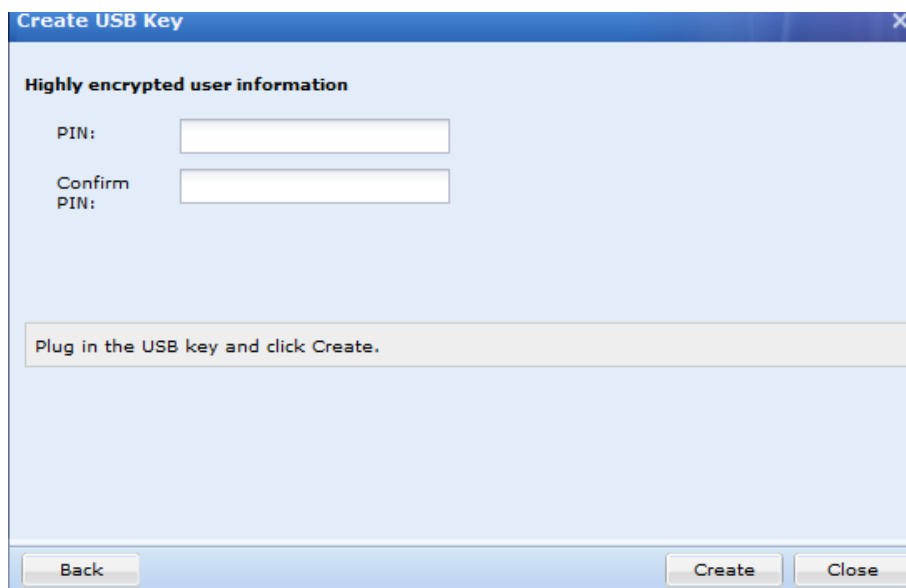
The screenshot shows a window titled "Create USB Key" with a close button (X) in the top right corner. The main heading is "Import digital certificate issued by external CA." Below this, there are several input fields and a dropdown menu:

Certificate File:		Browse...
File extension:	.pfx or .p12	
Certificate Issued By:	External CA	
Certificate Password:		
PIN:		
Confirm PIN:		

At the bottom of the window, there are three buttons: "Back", "Create", and "Close".

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

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



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

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

Supported USB Key Model

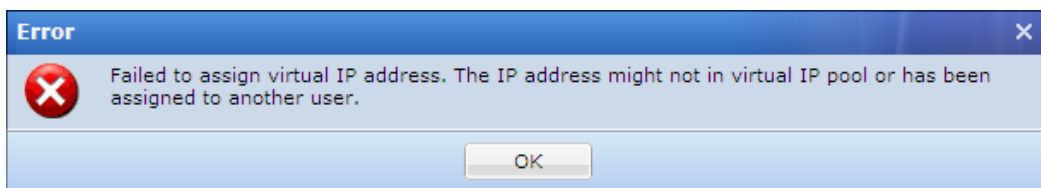
Third-party USB key supported. Client software can read the USB key when user logs in. Unplugging key leads to user logout.

<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/>			
<input type="checkbox"/>	Name	Model	Status
<input type="checkbox"/>	USB Key V2	Vid_096e*Pid_0302	✓
<input type="checkbox"/>	USB Key V3	Vid_5448*Pid_0003	✓
<input type="checkbox"/>	USB Key V3-2	Vid_5448*Pid_0001	✓

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

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

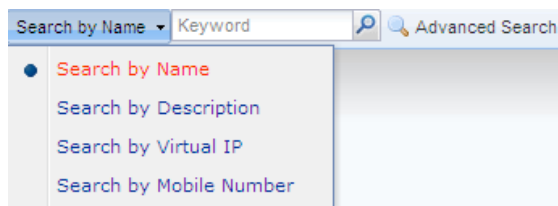
If **Specified** is selected, click **Get Idle IP** to obtain an available IP address or fill in a virtual IP address into the textbox by hand. This IP address will be assigned to the user in due course. However, if the entered IP address is not included in the virtual IP pool (that has been assigned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



-
- Automatic virtual IP address assignment applies only to private user.
 - By default, user inherits the attributes of its parent group, such as authentication options, policy set, etc. However, you could uncheck the option **Inherit parent group's attributes** and specify an authentication solution for a specific user.
-
6. Configure valid time of the user account. **Expiry Date** indicates the date on which this user account will get invalid. If **Never** is selected, the user account will be valid always. If **Specified** is selected, select a date as expiry date.
 7. Configure status of the user account. This user account will be enabled (valid) if **Enabled** is selected or disabled (invalid) if **Disabled** is selected.
 8. Configure **Authentication Settings**. For details, please refer to the **Adding User Group** section in Chapter 4.
 - **Public user:** Indicates that multiple users can use the user account to access SSL VPN concurrently.
 - **Private user:** Indicates that only one user can use the user account to log in to the SSL VPN at a time. If a second user uses this user account to connect SSL VPN, the previous user will be forced to log out.
 9. Associate user with policy set. For detailed guide, please refer to the Adding User Group section in Chapter 4.
 10. Assign roles to user group. For detailed guide, please refer to the **Adding User Group** section in Chapter 4.
 11. Click the **Save** button and the **Apply** button to save and apply the settings.

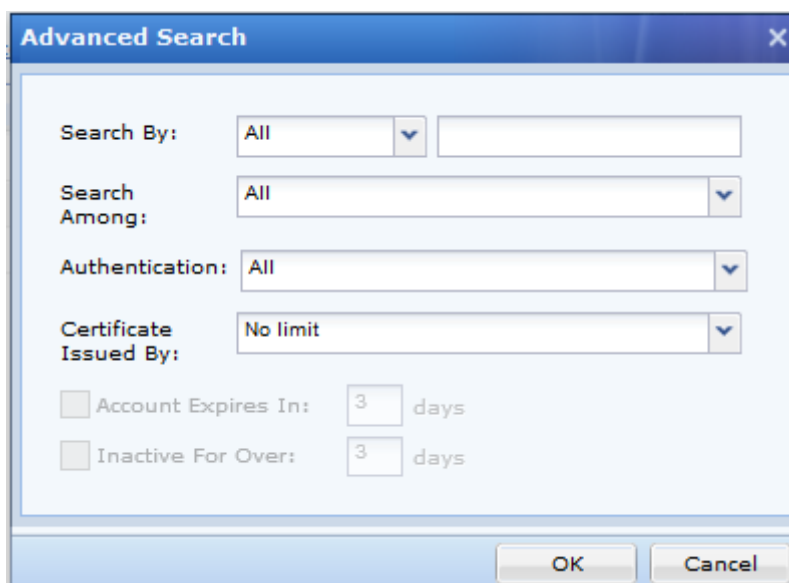
Searching for Users

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



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

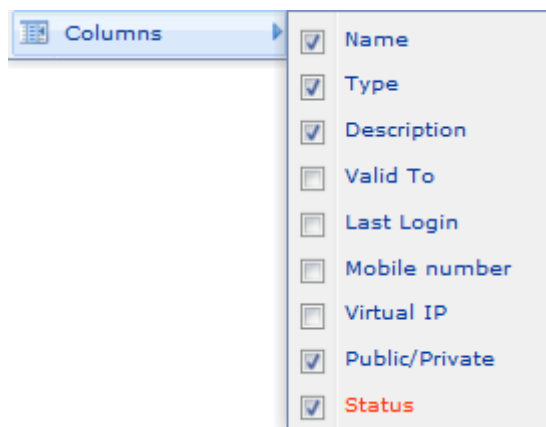
To search for a specific user or category of users with specific criteria, click **Advanced Search**. The criteria for advanced search are as shown in the figure below:



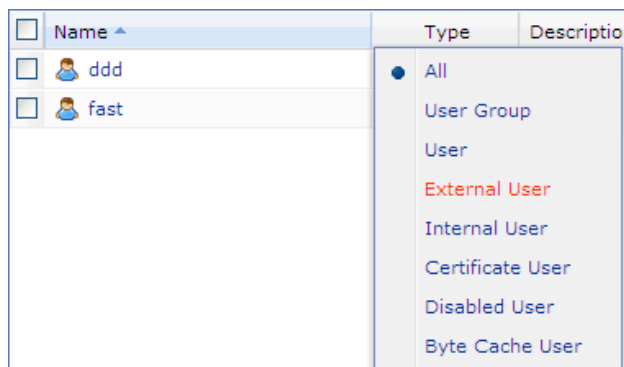
Search criteria are type of keyword, keyword, type of users, authentication method, certificate issuer, expiry date and idleness of the user account.

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

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

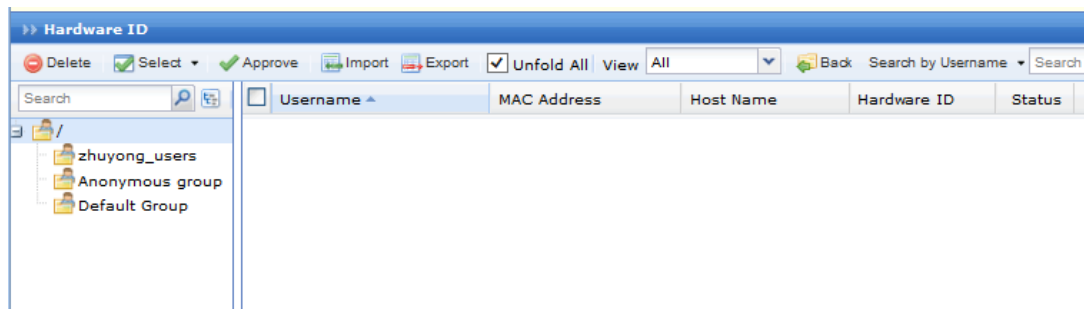


To filter users and view only one category of users, click column header **Type**, as shown below:



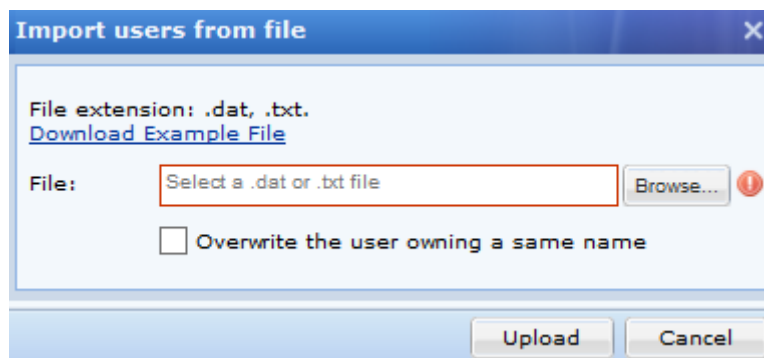
Managing Hardware IDs

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



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

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

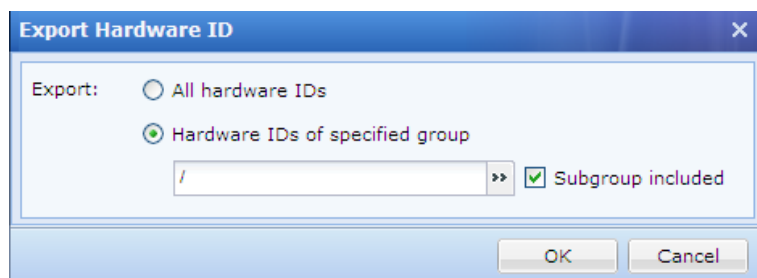


For the file format and the way of maintaining the file that contains hardware IDs, click the **Download Example File** link to download a copy to the local computer and main the hardware ID as instructed.

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

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

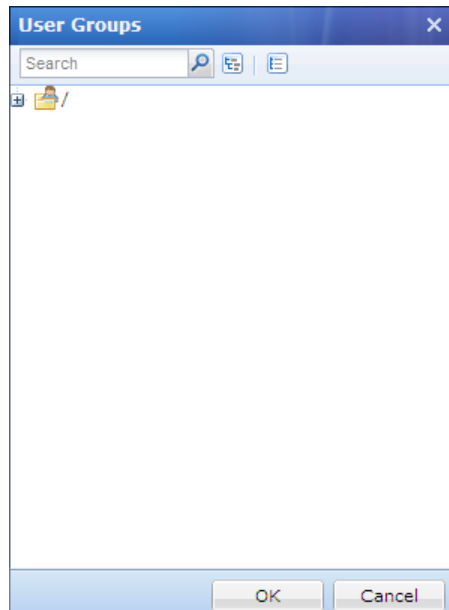
- **Export:** Click it to export the desired hardware IDs and save them into the computer, as shown in the figure below:



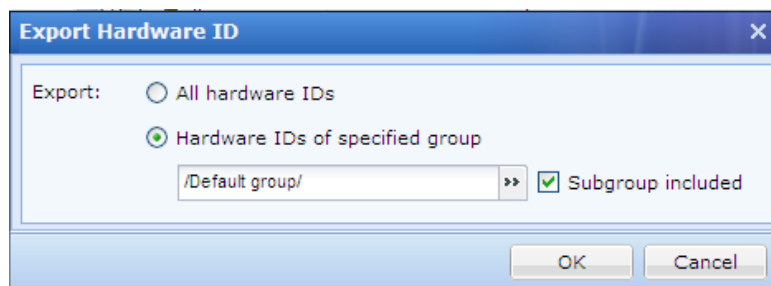
- a. Specify the hardware IDs that you want to export.

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

To export the desired hardware IDs of a specific user group, select **Hardware IDs of specified group** and click the textbox to specify a user group, as shown below:



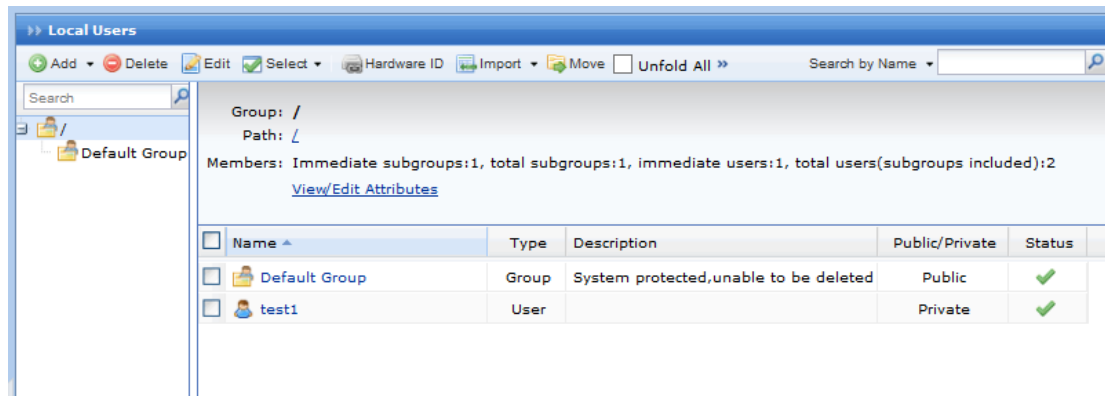
- b. Click the **OK** button and the name of the selected user group is filled in the textbox, as shown in the figure below:



- c. To also export the hardware IDs of the users that are included in the subgroups of the specified user group, select the checkbox next to **Subgroup included**. If this option is not selected, only the hardware IDs of the direct users in the selected group will be exported.
- d. Click the **OK** button to write the hardware IDs into a file and download the file into the computer.

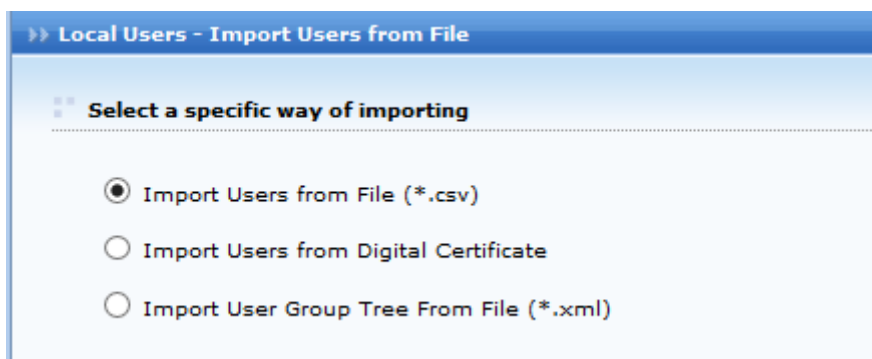
Importing User to Device

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



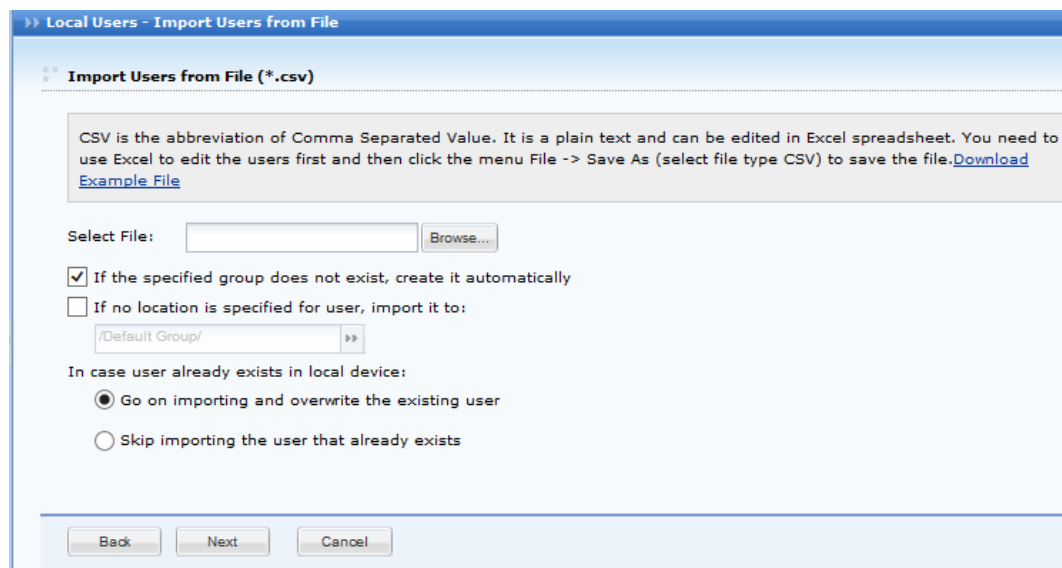
Importing Users from File

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



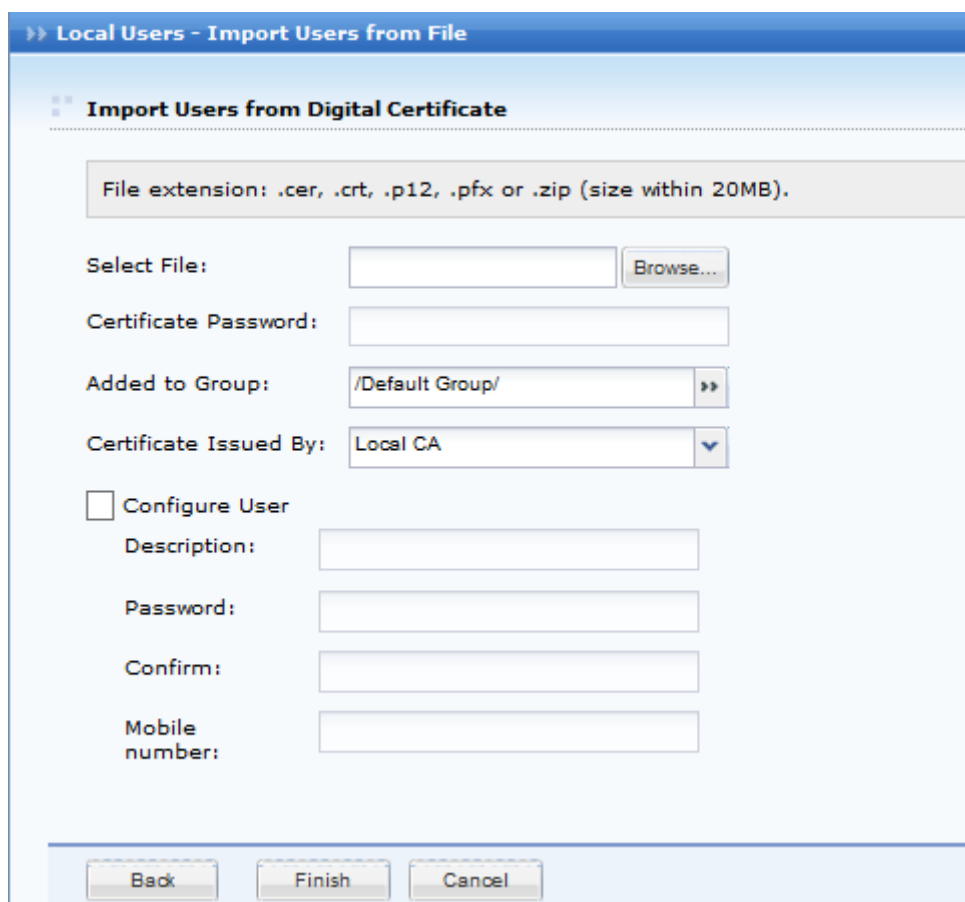
2. Select a way of importing.

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



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

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



The screenshot shows a web-based interface for importing users. The main title is 'Local Users - Import Users from File'. Below it, there is a sub-section titled 'Import Users from Digital Certificate'. A grey box contains the text: 'File extension: .cer, .crt, .p12, .pfx or .zip (size within 20MB)'. Below this, there are several input fields and buttons: 'Select File:' with a text box and a 'Browse...' button; 'Certificate Password:' with a text box; 'Added to Group:' with a dropdown menu showing '/Default Group/' and a right-pointing arrow; 'Certificate Issued By:' with a dropdown menu showing 'Local CA' and a downward arrow. Below these is a checkbox labeled 'Configure User'. If checked, there are four more text boxes: 'Description:', 'Password:', 'Confirm:', and 'Mobile number:'. At the bottom of the dialog, there are three buttons: 'Back', 'Finish', and 'Cancel'.

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

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

- **Select File:** Browse the XML file that you have edited. For more details of how to maintain the file, click the **Download Example File** link to download a copy and refer to the instructions in it.
 - **Added to Group:** This specifies the user group to which the group tree will be added.
3. Configure the corresponding options on the above pages.
 4. Click the **Finish** button to import the users.

Importing Users from LDAP Server

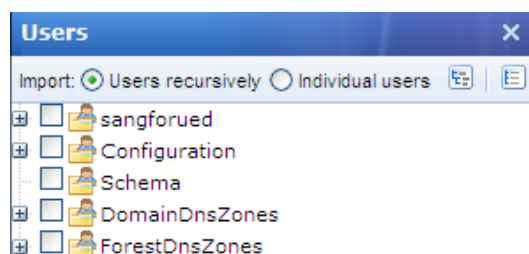
1. On the **Local Users** page, select **Import users from LDAP server**, and the **LDAP Server** page appears, as shown in the figure below:

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:

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

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



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

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

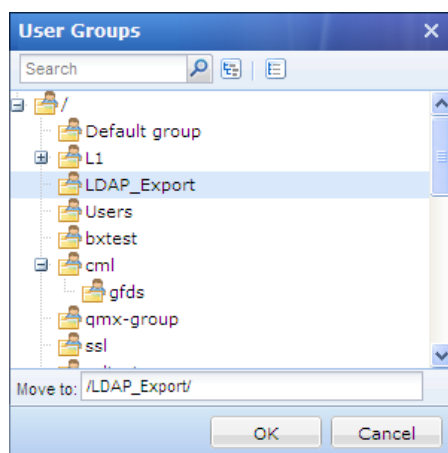


The objects imported automatically include users and groups.

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

Moving Users to Another Group

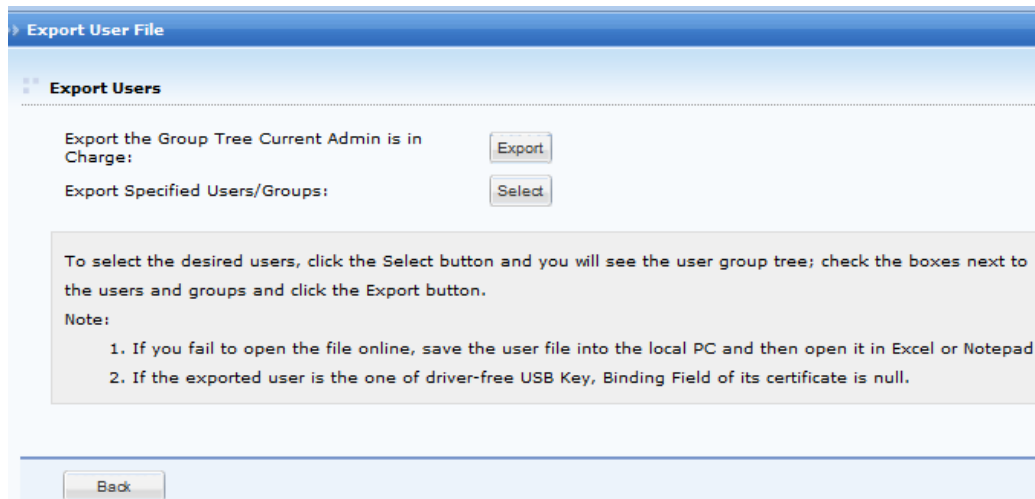
1. On the **Local Users** page, select the desired user/group(s) and click **Move** (on the toolbar) to enter **User Groups** page, as shown below:



2. Select a user group to which the user/group(s) is added.
3. Click the **OK** button.

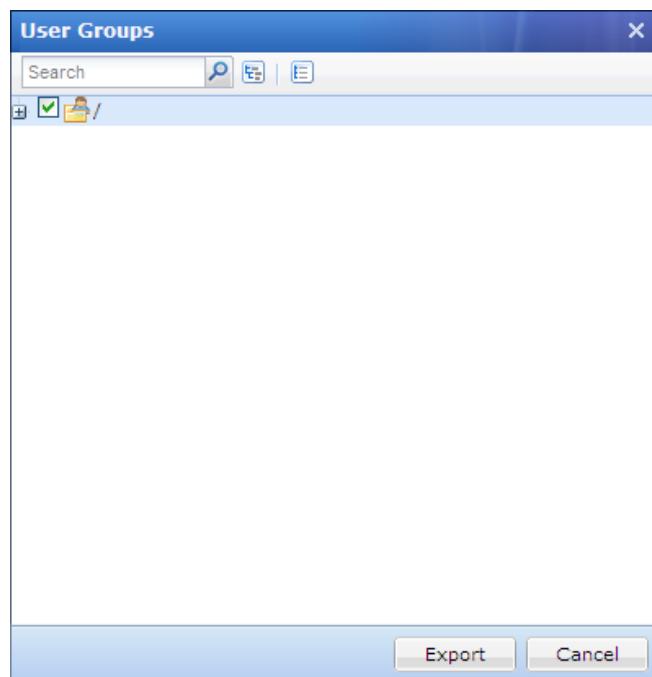
Exporting Users

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



2. Select the objects that you want to export.

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



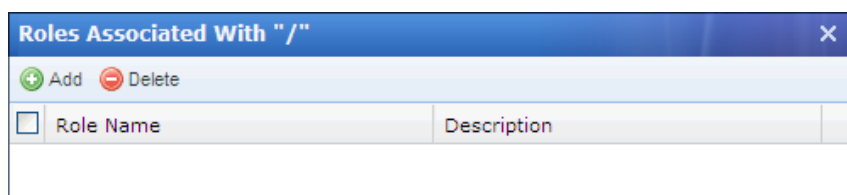
3. Select the desired user group and then click the **Export** button. The selected user will be written into a CSV file and saved on the local computer.

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

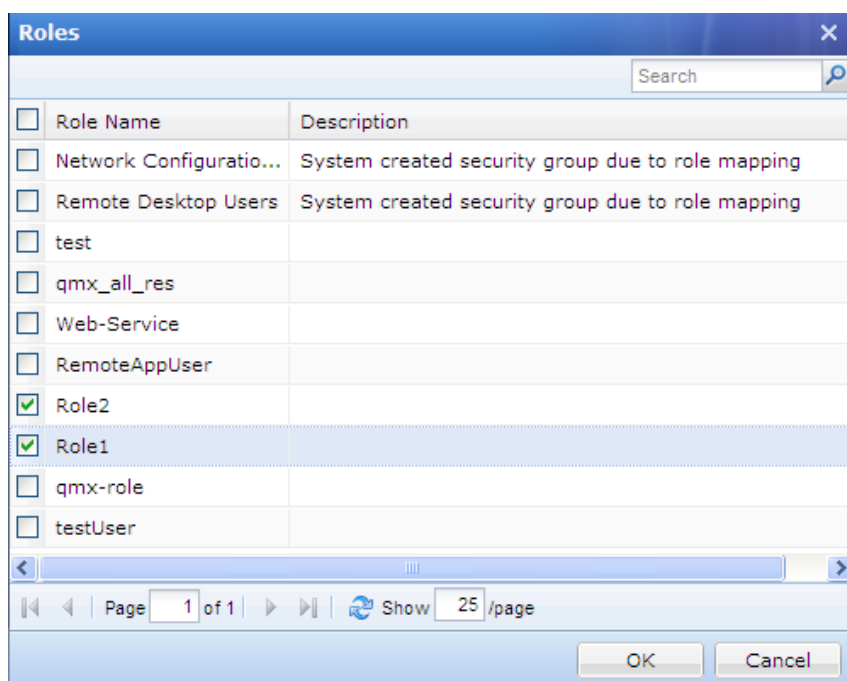
#Username	Added to Group	Password	Mobile Number	Virtual IP	Description	Last Login
hubin	/ssl	{ }	13666261525			Never logged in
webfs	/	{ }				Never logged in
hgfdhgfd	/	{ }	13666261525			Never logged in
lwq	/	{ }				Never logged in
aa	/	{ }				Never logged in
zsw	/	{ 30ec222ccc0fdc1e6 }				Never logged in
gfd	/	{ }				Never logged in
jhfg	/cml/gfds	{ }				Never logged in
lala	/ssl	{ 197fha71256ah35f3 }				Never logged in

Associating Roles with User

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



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



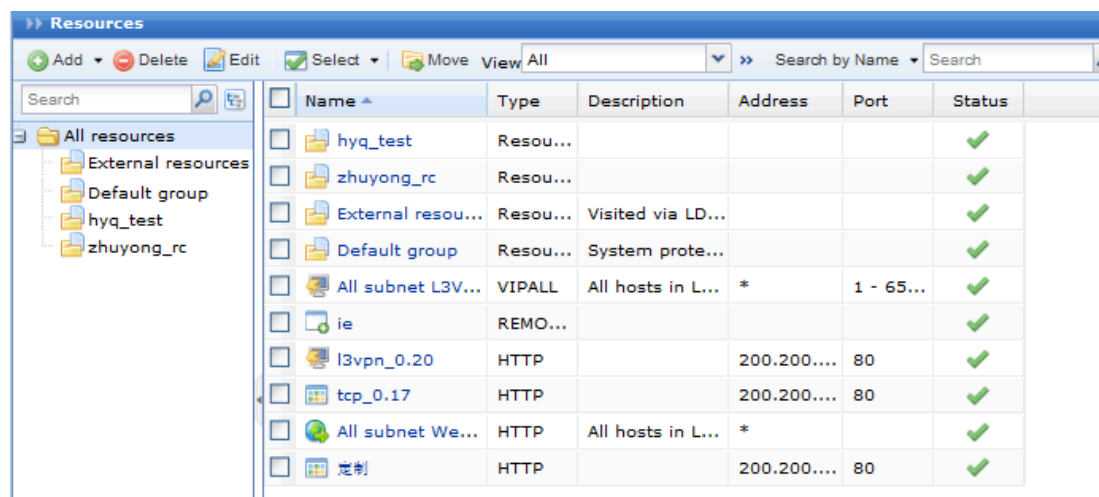
The roles on **Roles** page are all the roles predefined under **SSL VPN > Roles > Role Management**.

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

Resources

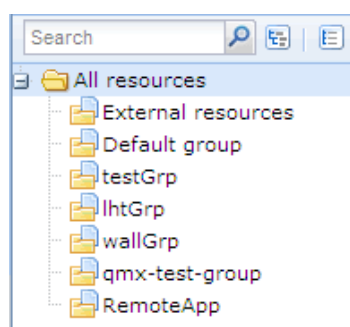
The resources we are talking about in this user manual are the resources that can be accessed by specified users over SSL VPN.

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



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

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



External resources is a group protected by system and cannot be deleted; however, its attributes could be modified. All the resources contained in this resource group are the resources associated with LDAP users.

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

Adding/Editing Resource Group

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

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



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

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

Authorized Admin		Load Balancing Resources	
<input checked="" type="checkbox"/> Enable Resource Load Balancing		Instructions	
 Edit			
Resource Name	Weight(1-9,default is 5)		
<input type="checkbox"/> Sangfor BBS	5		
<input type="checkbox"/> google	5		
<input type="checkbox"/> microsoft	5		
<input type="checkbox"/> Apple	5		
<input type="checkbox"/> Twitter	5		
<input type="checkbox"/> ftp16	5		
<input type="checkbox"/> 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.

Adding/Editing Web Application

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

Basic Attributes Fields marked * are required

Name: *

Description:

Type: HTTP

Address: *

Added To: Default group

Icon:

Enable resource

Visible for user

Enable resource address masquerading

SSO | Authorized Admin | Accounts Binding | URL Access Control | Site Mapping

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 be seen on the **Resource** page after user logs in to the SSL VPN successfully.
- **Type:** Options are **HTTP**, **HTTPS**, **MAIL**, **FileShare** and **FTP**.
- **Address:** Indicates the address of the resource. Enter the IP address or domain name of the Web server that is to be visited by user while this resource is requested.

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

Basic Attributes

Name: *

Description:

Type: HTTPS

Address: *

Added To: Default group

Enable resource

Visible for user

Enable resource address masquerading

SSO | Authorized Admin | Accounts Binding | URL Access Control | Site Mapping

Enable SSO

Login Method: Auto fill in form

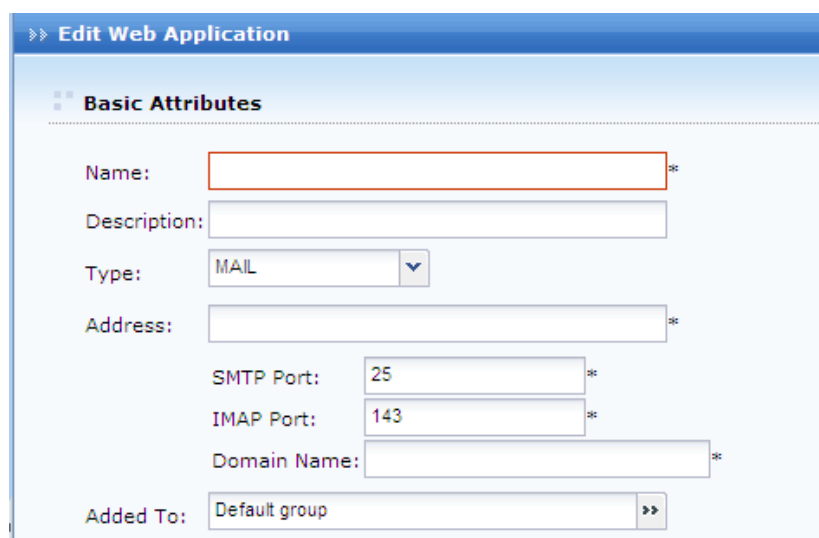


- Address field is required. The address must begin with **http://** or **https://**, for

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 **错误!未找到引用源。** section in Chapter 3), or configure the DNS server of the Sangfor device and ensure it can resolve the local domain names (in **System > Network > Deployment**).

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



The screenshot shows the 'Edit Web Application' configuration interface. The 'Basic Attributes' section is expanded, showing the following fields:

- Name:** An empty text input field with a red border and an asterisk (*).
- Description:** An empty text input field.
- Type:** A dropdown menu set to 'MAIL'.
- Address:** An empty text input field with an asterisk (*).
- SMTP Port:** A text input field containing '25' with an asterisk (*).
- IMAP Port:** A text input field containing '143' with an asterisk (*).
- Domain Name:** An empty text input field with an asterisk (*).
- Added To:** A dropdown menu set to 'Default group' with a right-pointing arrow (➤).



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:

The screenshot shows the 'Edit Web Application' interface. Under the 'Basic Attributes' section, there are several input fields: 'Name' (required), 'Description', 'Type' (set to FTP), 'Address' (required), 'FTP Port' (set to 21), and 'Added To' (set 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.

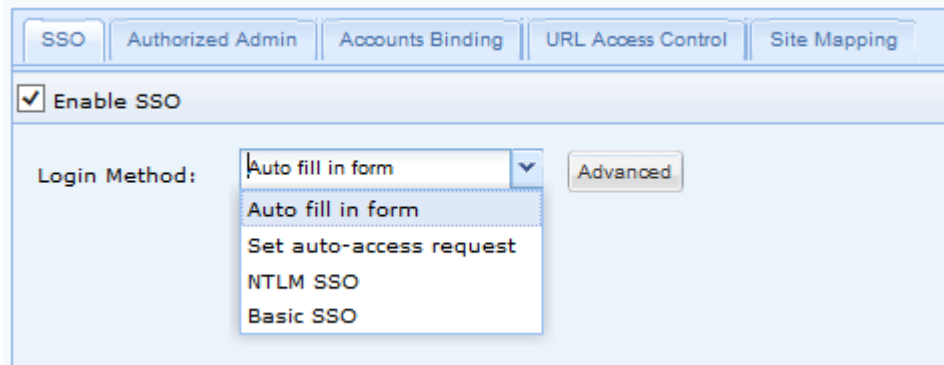
- **Added To:** Indicates the resource group to which this resource is added. By default, the selected resource group is **Default group** (to configure resource group, refer to the Adding/Editing Resource Group section in Chapter 4).
- **Icon:** Indicates the icon for this resource, which could be seen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

To browse an image and upload it from the local PC to the device, click **Upload** (for detailed guide, refer to the [错误!未找到引用源。](#) section in Chapter 3).

- **Visible for user:** To have connecting users see this resource on the **Resource** page, select this option. Invisibility here only means that the resource will not be seen on the **Resource** page; in fact, it is still accessible to the user.
- **Enable resource address masquerading:** To conceal the true IP address of the resource, select this option.

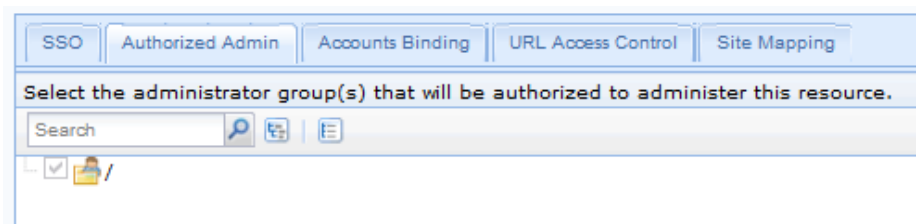
3. Configure SSO tab.

To enable user to access corporate resources over SSL VPN using SSO, select **Enable SSO** option and configure the **SSO** page (under **System > SSL VPN Options > General**. For more details, refer to the [错误!未找到引用源。](#) section in Chapter 3). Enable SSO on SSO tab and specify login method, as shown below:



4. Configure **Authorized Admin** tab.

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



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

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

Verify user by analyzing packet

Packet Format:

Encoding:

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.

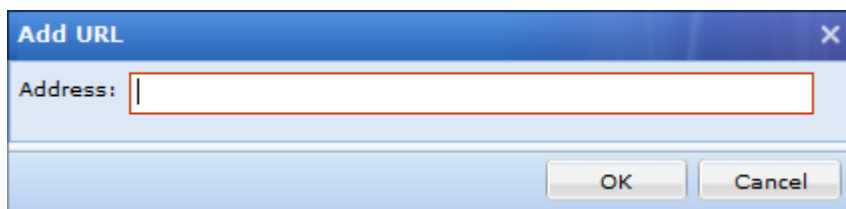
- Configure **URL Access Control** tab. This achieves the control over users' access to certain directory of a server, user being able or unable to access the specified directory.

Enable URL access control
 [Set Access-Denied Prompt Page](#)
[Instructions](#)

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

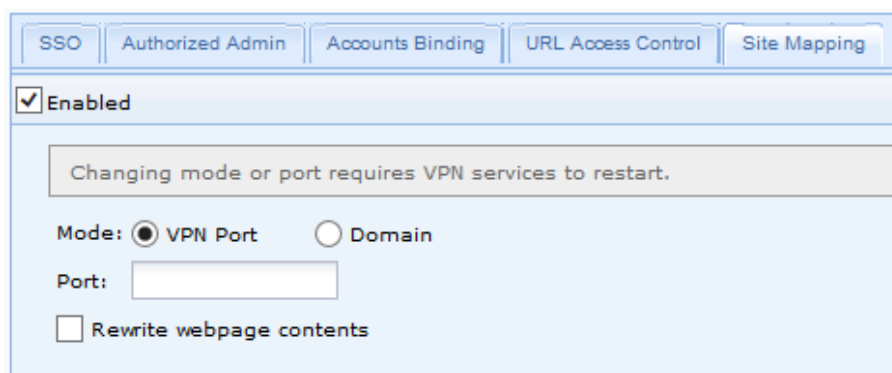
<input type="checkbox"/>	URL
--------------------------	-----

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




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

7. Configure **Site Mapping** tab.



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

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

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

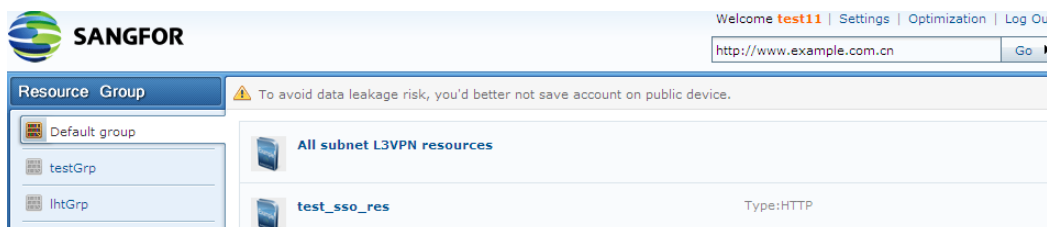


- Site mapping and resource address masquerading features cannot be enabled together.
- Site mapping feature is only available while Web application type is HTTP, HTTPS. The other types of Web application (FileShare, MAIL and FTP) do not support this feature.

- For the resource enabling site mapping feature, it can be accessed only through clicking resource link. It is not accessible through typing resource address into the **URL** field.

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

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



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



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

Adding/Editing TCP Application

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

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

Basic Attributes Fields marked * are required

Name: *

Description:

Type: HTTP

Address: + - ↻

Program Path: Browse...

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

Added To: Default group »

Icon: ▼

Enable resource

Visible for user

SSO | Authorized Admin | Accounts Binding | URL Access Control | Others

Enable SSO

Login Method: Auto fill in form Advanced

2. Configure **Basic Attributes** of the TCP application. The following are the basic attributes:
- **Name, Description:** Indicates the name and description of the TCP resource. This name may be seen on the **Resource** page after user logs in to the SSL VPN.
 - **Type:** Indicates the type of the TCP application. Some common types are built in the Sangfor device.
 This selection determines the port number entered in the **Port** field automatically. If the TCP application is not any of the built-in types, select **Other** and configure the port manually.
 - **Address:** Indicates the address of the TCP resource. To add one entry of address (IP address, domain name or IP range), click the **Add Address** tab. To add multiple entries of addresses, click the **Add Multiple Addresses** tab, as shown in the figures below:



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

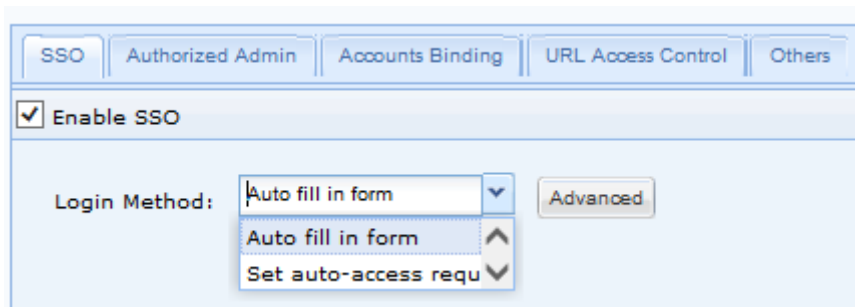
- **Program Path:** Indicates path of the client software program that may be used by C/S (client/server) application.
- **Added To:** Indicates the resource group to which this resource is added. By default, the selected resource group is **Default group** (to configure resource group, refer to the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

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

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

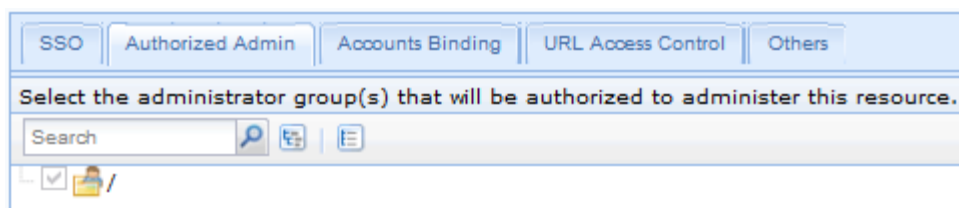
3. Configure **SSO** tab.

To enable connecting users to use SSO feature to access corporate resources over SSL VPN, select **Enable SSO** option and configure the **SSO** page (under **System > SSL VPN Options > General > SSO**). For more details, refer to the [错误!未找到引用源。](#) section in Chapter 3).



4. Configure **Authorized Admin** tab.

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



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

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

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

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

Web application, TCP application and L3VPN support accounts binding.



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

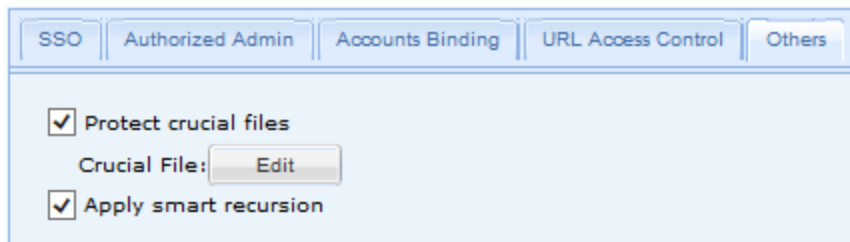
6. Configure **URL Access Control** tab.

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



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

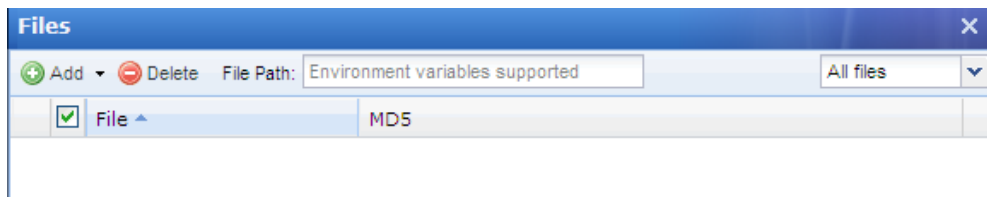
7. Configure **Others** tab. This tab covers two options, **Protect crucial files** and **Apply smart recursion**, as shown in the figure below:



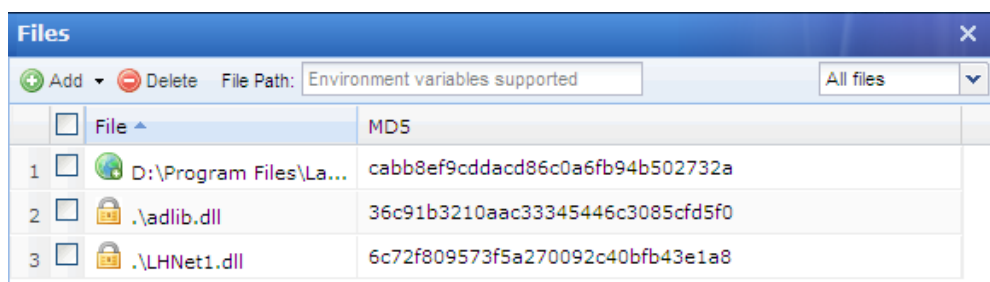
- **Apply smart recursion:** Select this option to apply smart recursion to this resource. Before doing so, go to **System > SSL VPN > General > Resource Options > TCP App** to enable and configure smart recursion. For more details, please refer to the **错误!未找到引用源。** in Chapter 3 and **错误!未找到引用源。** in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

To add crucial files, perform the following steps:

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



- b. Click **Add > Process related file** to select the process (file extension is .exe).
- c. The selected file and all the involved DLL files are added to the **Files** page, with the information of file directory and MD5, as shown in the figure below:



- d. To view a specific type of file, dll, exe or pdb, specify the file type in the textbox at the upper right of the page. By default, all files are displayed.
- e. To remove an entry, select the checkbox next to the entry and click **Delete**.
- f. Click the **OK** button to save the settings.



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

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

Adding/Editing L3VPN

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

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

Basic Attributes Fields marked * 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

SSO | Authorized Admin | Accounts Binding | URL Access Control

Enable SSO

Login Method: Auto fill in form

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

The screenshot shows the 'Add/Edit Resource Address' dialog box with the 'Add Address' tab selected. The dialog contains the following elements:

- Buttons: 'Add Address' (selected) and 'Add Multiple Addresses'.
- Text: 'As to domain resource, check whether you have configured [Local DNS](#)'.
- Radio buttons: 'IP or domain' (selected) and 'IP range'.
- Text input: 'IP/Domain:' followed by a text box containing a red border and an asterisk (*).
- Text input: 'Port: 80' followed by a minus sign and another text box containing '80' and an asterisk (*).
- Checkbox: 'Enable resource address masquerading' (unchecked).
- Buttons: 'OK' and 'Cancel'.

The screenshot shows the 'Add/Edit Resource Address' dialog box with the 'Add Multiple Addresses' tab selected. The dialog contains the following elements:

- Buttons: 'Add Address' and 'Add Multiple Addresses' (selected).
- Text area: An empty list area with a scroll bar.
- Text: 'Example:' followed by three lines of example addresses:
 - [10.10.10.20/80:80](#)
 - [1.1.1.1-2.2.2.2/80:80](#)
 - [https://www.domain.com:80](#)
- Text: 'One entry per row'.
- Buttons: 'OK' and 'Cancel'.



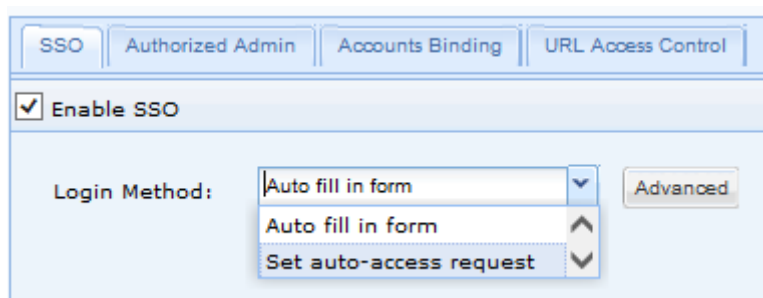
- **Port** indicates the port used by this L3VPN to provide services. For the built-in types, this port is predefined. For **Other** type of L3VPN, enter the port number that is to be

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 **错误!未找到引用源。** section in Chapter 3).



4. Configure **Authorized Admin** tab.

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



- The authorized administrators cannot edit the resource. They only have the right to assign this resource to users (in other words, the right to associate resources with the role under **SSL VPN > Roles > Edit Role**) and to grant other administrators (in its permitted realm) the privilege to manage this resource, rather than the privilege of editing resource.
- Please it keep in mind that the privilege of editing a resource always belongs to the

creator who has created this resource as well as the administrator with higher privilege. The authorized administrators cannot see those resources in the **Resource Management** page, but can see and associate them with users on the **Add Role** or **Edit Role** page.

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

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

If **Resource is accessible to user using the designated SSO user account** is selected, end user have to use the corresponding SSL VPN account and designated SSO user account to access this L3VPN resource, other user accounts being unable to match the credential.

Web application, TCP application and L3VPN support accounts binding.



- To enable end users to single sign in to a resource, enable SSO for that resource (under **SSL VPN > Resources > Edit L3VPN > SSO** tab) and bind the SSL VPN account to the SSO user account (to configure SSO user account, refer to the **错误!未找到引用源。** section in Chapter 4).
- Applying **Verify user by analyzing packet** does not require SSO to be enabled.

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

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



URL access control feature is only available while the selected L3VPN type is **HTTP**. The other types of L3VPN do not support this feature.

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



-
- The first time L3VPN resource is accessed over SSL VPN, L3VPN component may be installed on the user's PC automatically. However, installation of L3VPN component requires administrator privilege on the computer. If any firewall or anti-virus software is installed and runs on the computer, it will block installation process. To ensure the component installed successfully, terminate the firewall or anti-virus software first.
 - Among the L3VPN resources, there is a system-protected L3VPN resource named **All Subnet L3VPN resources**. This resource stands for all L3VPN resources with the addresses on the subnets where LAN and DMZ interfaces reside and those resources on the subnets where LAN and DMZ interfaces reside, using the protocol TCP, UDP or ICMP (port: 1-65535). Like other L3VPN resource, it can be associated with users; however, no attribute of it can be modified except for the name, description and visibility. If the subnet resources do not reside in the same network segment as the LAN and DMZ interface of the Sangfor device, which means, there is layer-3 router or switch on the way, add the subnet on the **Local Subnets** page (under **System** > **Network**) and a corresponding route on **Routes** page (under **System** > **Network**) to make that subnet "local". That will enable the machines on the two subnets to communicate directly.
-

Adding/Editing Remote Application

Remote applications are applications launched by remote servers and accessed by end users over SSL VPN. User runs the program on the local computers but access the data on the remote server

in the remote application session.

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

Basic Attributes Fields marked * are required

Name: *

Description:

Added To: >>

Icon:

Enable resource

Program:

Working Directory: ⓘ

Command Line:

Argument:

Maximize window after program is launched

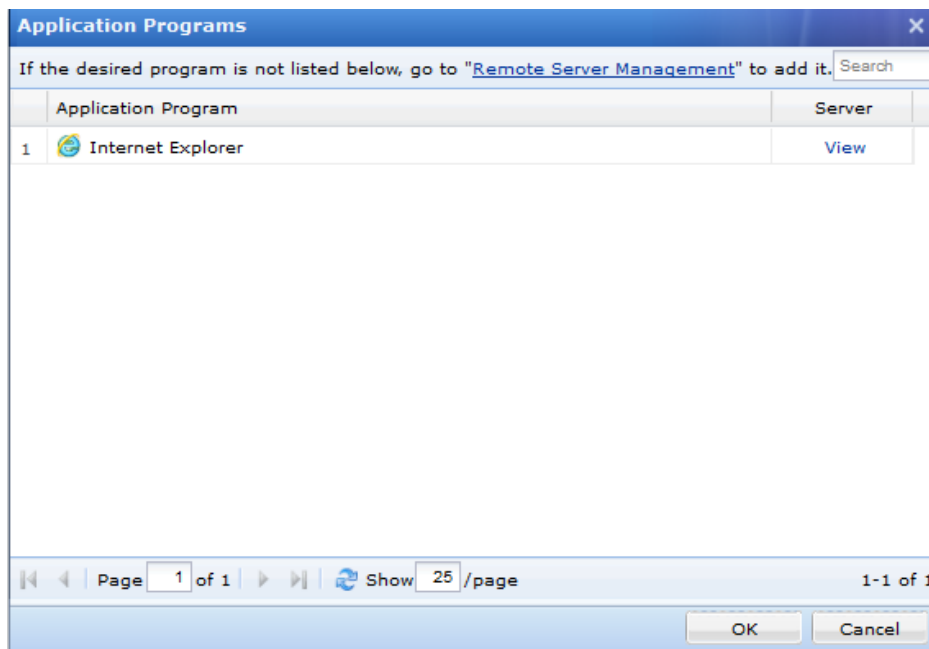
Single instance is allowed (for an application running on remote server, not allow user to run a second instance of the application)

App Server | SSO License | Authorized Admin

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

Search	Server 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:** Specifies the applications provided by remote application server. Click on **Select** to select the desired application, as shown in the below figure:

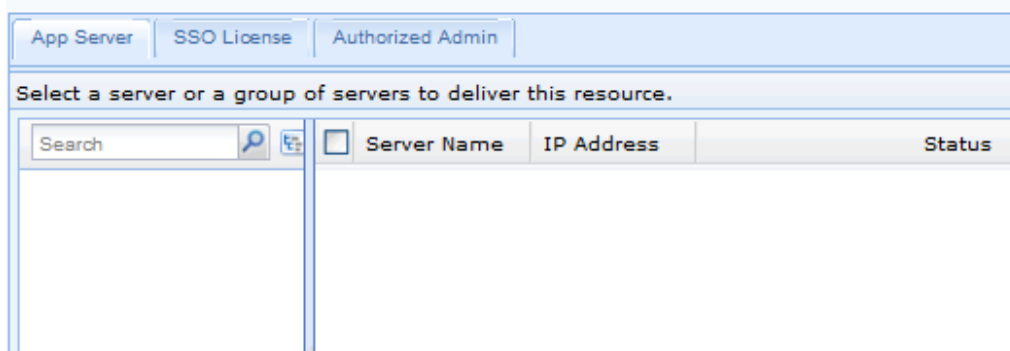


- **Working Directory:** Indicates the path of the application on remote application server.
- **Command Line Argument:** Specifies the parameters that may be used when some application program starts.

If **Maximize window after program is launched** is selected, program window will be maximized once program is launched.

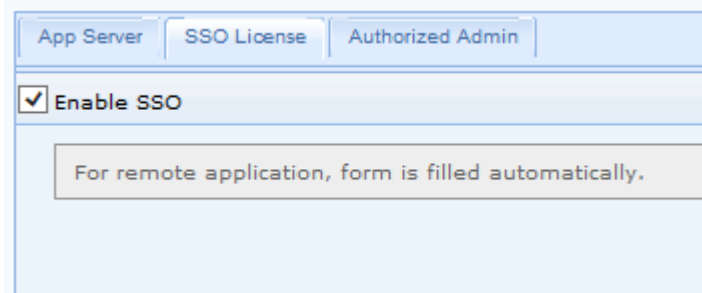
In case that **Single instance is allowed** is selected and user has launched an application, user will be redirected to the previously-launched application if user clicks on the resource link again, instead of launching a new instance. If command line argument is configured, this options is not recommended to enable.

3. Click the **App Server** tab and select remote application servers, so that they can provide the application (to configure remote server, refer to the Adding Remote Application Server section in Chapter 4).



4. Configure **SSO License** tab.

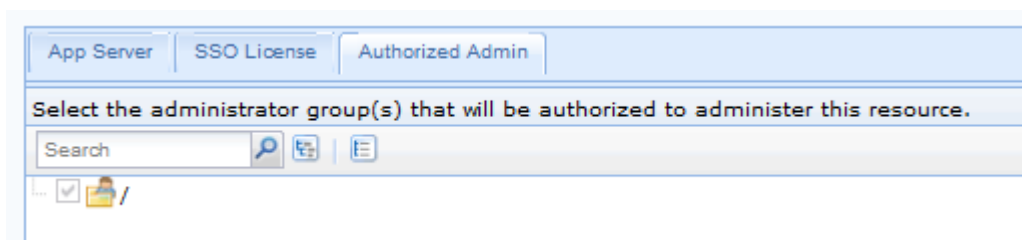
If SSO feature is enabled and SSO information is recorded, SSO will be performed automatically when user accesses specific remote application over SSL VPN.



- As to remote application, SSO feature only supports the method of auto fill in form.
- If you want to deliver a browser allowing SSO, only IE-cored browser can be delivered.
- When recording SSO information for remote application, only IE is taken as B/S-based resource, all the other resources are taken as C/S-based resource.

5. Configure **Authorized Admin** tab.

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



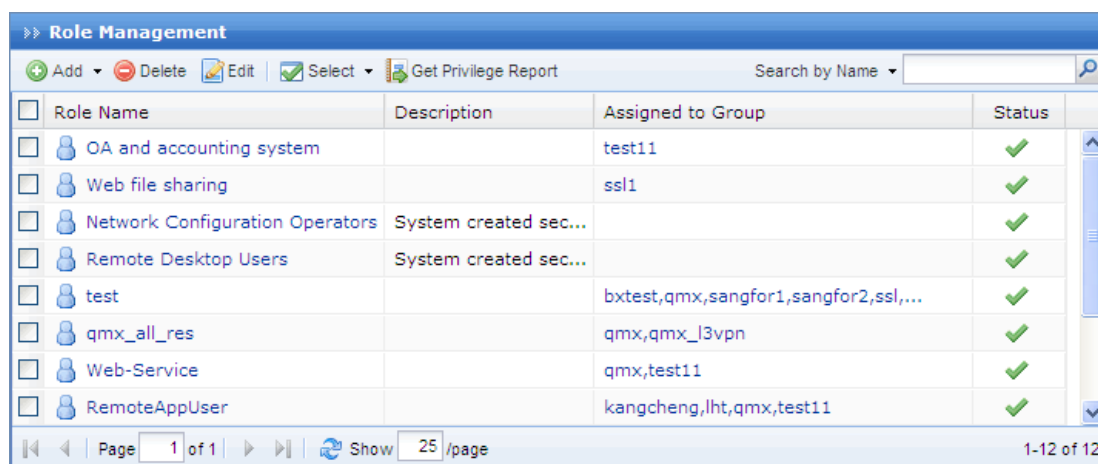
- The authorized administrators cannot edit the resource. They only have the right to assign this resource to users (in other words, the right to associate resources with the role under **SSL VPN > Roles > Edit Role**) and to grant other administrators (in its permitted realm) the privilege to manage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

Roles

A role is an intermediate that builds a connection between user/group and resource, more specifically, designates internal resources to user or group. Users can only access the designated internal resources over SSL VPN.

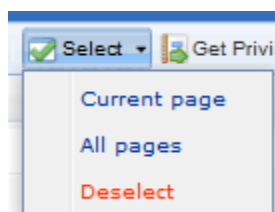
This kind of association enables one or multiple users or groups to associate with one or multiple resources, facilitating control over users' access to corporate resources.

Navigate to **SSL VPN > Roles** and the **Role Management** page appears, as shown below:



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

- **Search By Name/Description/User(Group):** To search for specific role or type of roles, select an option, enter the keyword into the textbox and click the magnifier icon. Name/description indicates the name/description of the role. User/group indicates the user and/or group that the role is assigned to.
- **Role Name:** Indicates name of the role.
- **Description:** Indicates description of the role.
- **Add:** Click it to add new role directly or using an existing role as template.
- **Edit:** Click it to edit a selected role.
- **Delete:** Click it to remove the selected role(s).
- **Select:** To select roles on all pages, click **Select > All pages**; click **Select > Current page** to select roles on current page. To deselect entries, click **Select > Deselect**.



Adding Role

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

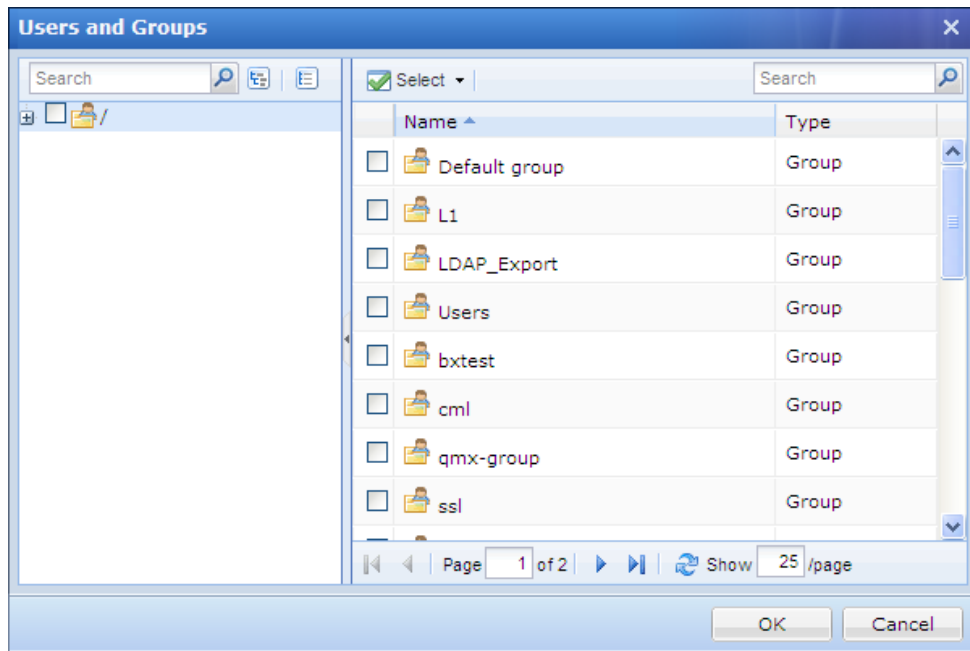
The screenshot shows the 'Add Role' configuration page. The 'Basic Attributes' section includes the following fields and controls:

- Name:** A text input field with a red border and an asterisk (*) indicating it is required.
- Description:** A text input field.
- Assigned To:** A text input field with a 'Select User/Group' button to its right.
- Security Policy:** A text input field with a 'Select Role-level Policy' button to its right.
- Enable Role**

The 'Associated Resources' section shows a 'Select Resource' dialog box with a table header:

Name	Type	Description
------	------	-------------

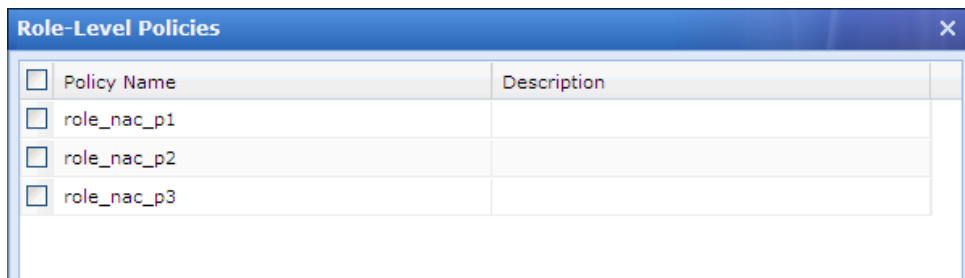
2. Configure the **Basic Attributes** of the role. The following are basic attributes:
 - **Name:** Configures name of the role.
 - **Description:** Configures description of the role.
 - **Assigned To:** Configures the user and/or group that can access the associated resources. To specify user and group, click the **Select User/Group** button, and all the predefined users and groups on **Local Users** page are seen in the list, as shown below:



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

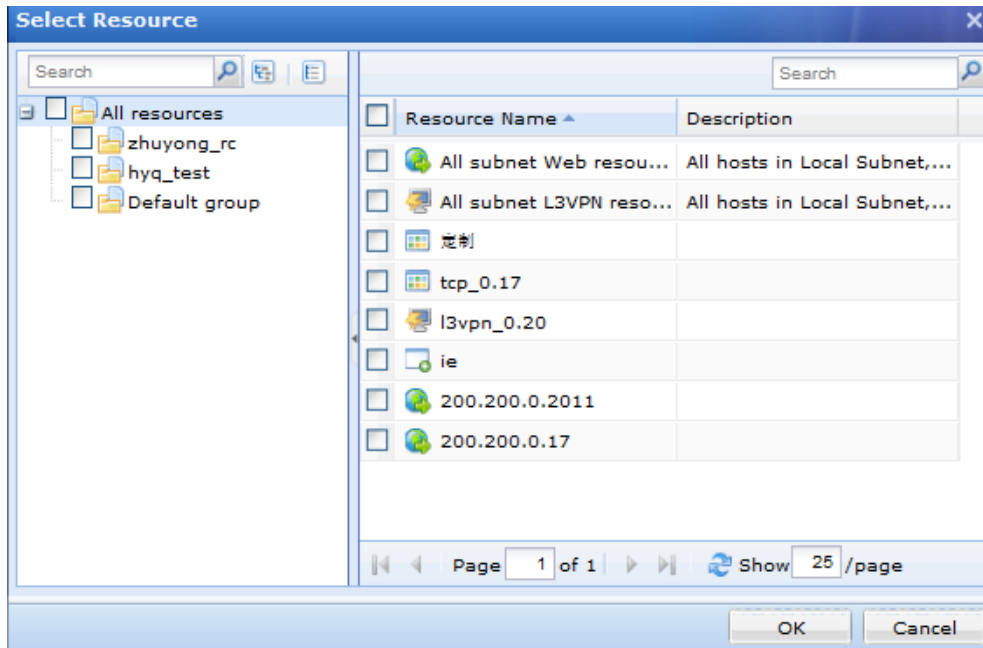
- **Security Policy:** This policy enforces host checking when user logs in to the SSL VPN. If user fails any security check, he or she cannot access the associated resources.

To specify a role-level policy, click the **Select Role-level Policy** button and all the predefined role-level policies are seen (to configure role-level policy, refer to the [错误! 未找到引用源。](#) section in chapter 4), as shown in the figure below:



If no role-level policy is configured, you do not need to configure security policy.

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



4. Click the **Save** button on the **Add Role** page to save the settings.

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** Settings
Sort LDAP/RADIUS servers to set the priority of each server for authentication.
- Password Security Options** Settings
Block insecure and brute-force login. Applied to LDAP, RADIUS and local password based authentications.
- Anonymous Login** Settings
Turn on/off the anonymous login feature and assign role to anonymous users.

Primary Authentication Methods

There are five primary authentication methods, namely, **local password** based authentication, **LDAP** authentication, **RADIUS** authentication, **certificate/USB key** based authentication and **client-side domain SSO** authentication.

The screenshot shows the 'Primary Authentication' configuration page with the following items:

- Local Password**: Password strength, the ways that users change password, applying only to the user accounts in local database. Includes a 'Settings' button.
- LDAP**: Manage LDAP servers. Authentication credentials are mapped or imported from LDAP server to local device. Includes a 'Settings' button.
- RADIUS**: Manage RADIUS servers. Authentication credentials are mapped or imported from RADIUS server to local device. Includes a 'Settings' button.
- Certificate/USB Key**: Select CA type, generate certificate and set USB key model. Includes links for [»USB Key Driver](#) and [» USB Key Tool](#). Includes a 'Settings' button.
- Client-Side Domain SSO**: Specify AD domain, so that users can perform SSO and install control using L2TP/PPTP connection. Includes a 'Settings' button.

Local Password Based Authentication

The settings related to local password based authentication include password security options and username options.

Navigate to **SSL VPN > Authentication** to enter the **Authentication Options** page (as shown in the figure above). Click the **Settings** button following **Local Password**, and the **Local Password Based Authentication** page appears, as shown in the figure below:

The screenshot shows the 'Local Password Based Authentication' configuration page with the following settings:

- Local Password Based Authentication** (Page Header)
- Password Security Options**
 - Enabled** (the options only apply to the private users in local database)
 - Password cannot contain username.
 - New password must be different from previous password
 - Minimum length is characters
 - Every days, user must change password. days before the password expires, remind 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. If enabled is selected, password security check will be performed when user logs in to SSL VPN. If user password fails to match the password security policy configured in this field, user will be asked to change password.
- **Username Options:** If the option **Ignore case of username** is selected, case of username would be ignored when users enter credentials to log in to SSL VPN. If any same usernames in different case already exist in user organization structure before this option is enabled, such as “HSw”, “hsw”, this user will fail to modify personal information after **Ignore case of username** is selected, he/she needs to modify its username first. Then enable this option.



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

LDAP Authentication

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

Configuring LDAP Server

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

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 > LDAP Server > Add/Edit LDAP Server

Basic Attributes Fields marked * are required


Server Name: *

Description:

Server Address:     

Admin DN:

Password:


Base DN: 

Subtree included (also verify the users in subtrees)

Authentication Timeout: * second(s)

Status: Enabled Disabled

Advanced

Server Type: 

User Attribute: *




User Filter: *

Mobile Number:

Other Attributes

Group Mapping | Role Mapping | LDAP Extensions | Password Encryption


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

 Add  Delete  Edit Automatic Mapping

<input type="checkbox"/>	OU	Sub-OU inc...	Map to Local Group
<input type="checkbox"/>	OU	Sub-OU inc...	Map to Local Group



3. Configure the **Basic Attributes** of the LDAP server. The following are basic attributes:

- **Server Name, Description:** Configures the name and description of the LDAP server.
- **Server Address:** Configures the usable IP address and port of the LDAP server. You can add multiple IP addresses and ports. Generally, only the first IP address/port is active and the others are standby. If the first IP address/port is unavailable, the second IP address/port will take the place; if the second IP address/port is unavailable, the third IP address/port will take the place, and so on; if none of the configured server IP addresses/ports is available, the server will be disconnected.

To add an entry of server address and port, click the **Add** icon  next to the **Server Address** field. The **Add Server Address** page is as shown in the figure below:

To remove an entry, click the entry and click **Delete** icon  next to **Server Address**.

To edit an entry, click the entry and click **Edit** icon  next to **Server Address**.

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

- **Admin DN, Password:** Configure the administrator account to read the organizational units (OU) and security groups on the LDAP server. The administrator account should be in DN format.



This administrator must have privilege to read path of users on the LDAP server.

- **Base DN:** Configures the location of the LDAP users that are to be verified.
 - **Subtree included:** Select this option so that the users contained in the sub-OU of the OU specified in **Base DN** field are included in. Otherwise, only the direct users in the specified OU level will be verified.
 - **Authentication Timeout:** Configures the time period that user authentication gets timed out if LDAP server gives no response.
 - **Status:** Indicates whether the LDAP server is enabled.
4. Configure the **Advanced** options. The values in these fields must be consistent with those on the LDAP server



Protocols supported are LDAP and MS Active Directory (AD). For MS AD, user authentication is achieved using attribute **sAMAccountName** and filter **objectCategory=person**. For LDAP, user authentication is achieved using attribute **uid** and filter **objectclass=person**. However, the attribute names could be modified.

5. Configure **Group Mapping** tab.

Group mapping only applies to the LDAP users that have not been imported to the Sangfor device. The users in specified OU on the LDAP server will be mapped to a local group after successful login, and therefore have the same privilege as the users that they are mapped to.

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, click it to enter the **Add Group Mapping Rule** page, as shown in the figure below:

Add Group Mapping Rule

OU:

Map to Group: >>

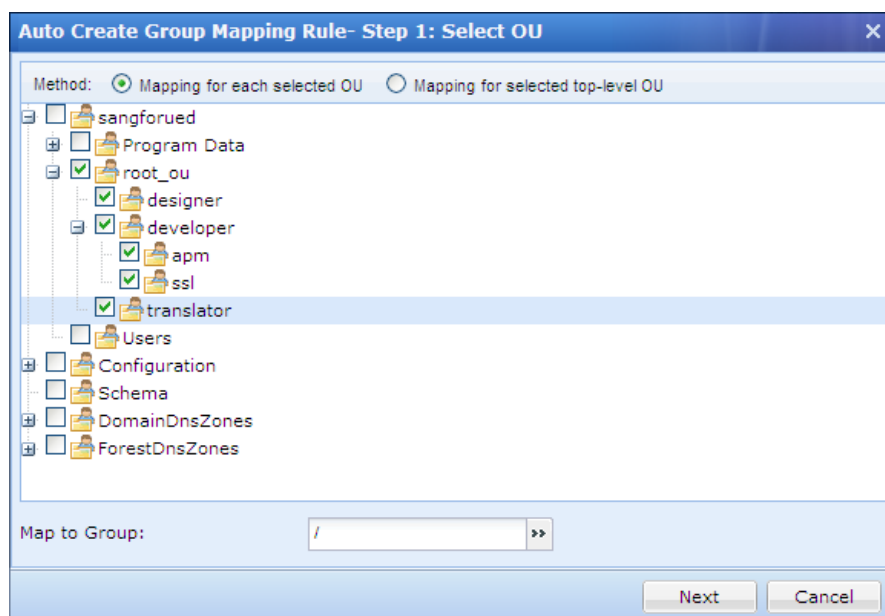
Sub-OU included

OK Cancel

- **OU:** Configures the OU that will be mapped to a local group, in format of DN.
- **Map to Group:** Configures the local group to which users of the specified OU will be mapped.
- **Sub-OU included:** If this option is selected, users in the sub-OU will also be included and mapped to the local group. If not selected, only the users in the

specified OU level will be mapped to the local group.

- **If LDAP user matches none of the above mapping rules, map the user to group:** For the users that match none of the group mapping rules, select this option and specify a local group, so that those LDAP users will be mapped to that group automatically.
- **Delete:** To delete a group mapping rule, select the rule and click **Delete**.
- **Edit:** To edit a group mapping rule, select the rule and click **Edit**.
- **Automatic Mapping:** This feature simplifies the process of adding a batch of mapping rules. Administrator needs only to select the LDAP user and/or group on the **Auto Create Group Mapping Rule – Step 1: Select OU** page (as shown in the figure below) and configure **Map to Group** field, without adding mapping rule one by one, and the involved mappings will be added to the group mapping rule list automatically. To configure automatic mapping, please perform the following steps:
 - a. Click **Automatic Mapping** to enter the **Auto Create Group Mapping Rule – Step 1: Select OU** page, as shown below:



- b. Select a mapping method, **Mapping for each selected OU** or **Mapping for selected top-level OU**, and then select the organizational units (OU).

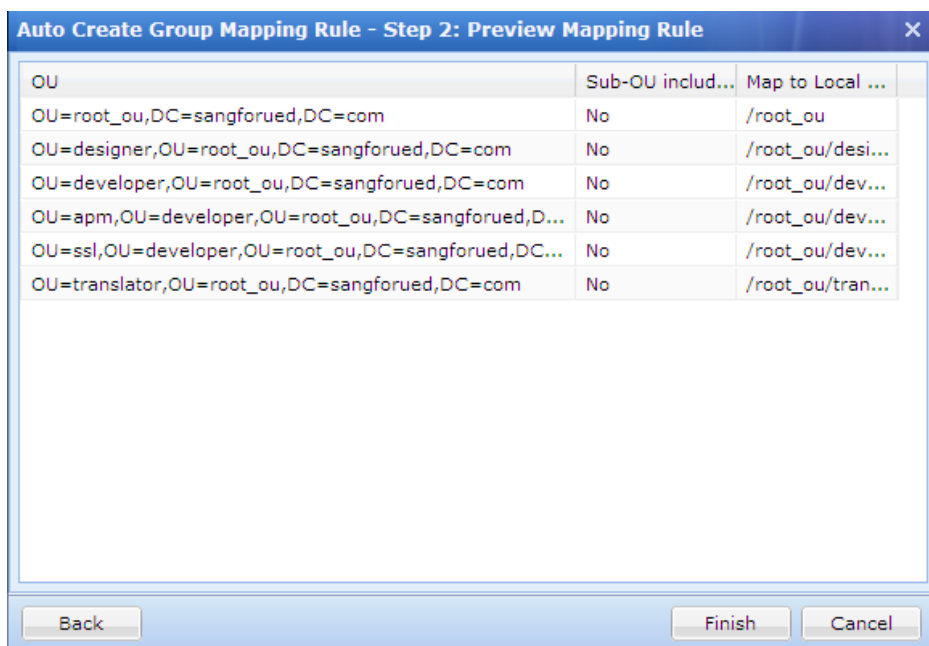
If the selected method is **Mapping for each selected OU**, every selected LDAP user group will be mapped to the respective local group (name of target group is the same as the OU name) specified in **Map to Group** field, organizational units (OU) not being changed.

If the selected method is **Mapping for selected top-level OU**, only one group will be created on the Sangfor device, name of the target group being the same as the top-OU name. All the users under the top-OU and/or the sub-OUs will be mapped to that group.

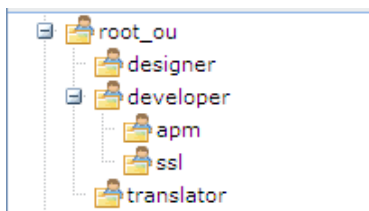
- c. Configure **Map to Group**. The specified group is a local user group to which the

specified LDAP users will be mapped.

- d. Click the **Next** button and the automatically added mapping rules are as shown below:

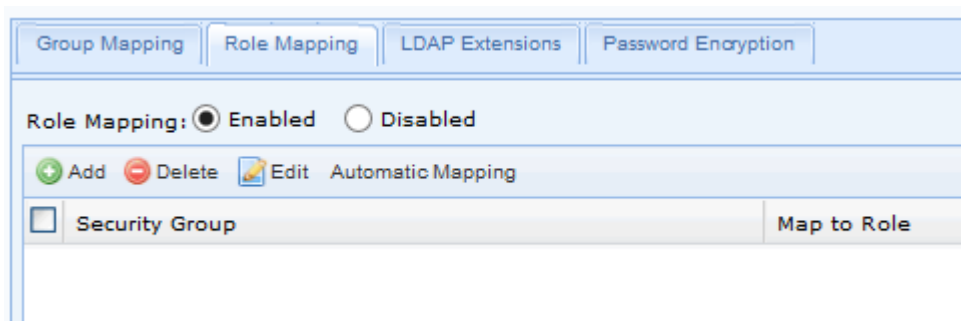


- e. Click the **Finish** and **Save** buttons and go back to **Local Users** page. Check whether the groups created through automatic mapping are in user group list, as shown below:



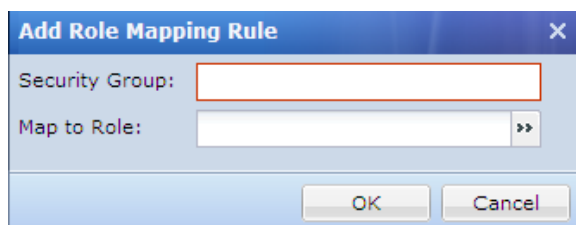
- 6. Configure **Role Mapping** tab (if you are adding an MS Active Directory server).

Role Mapping helps map the security groups from the MS Active Directory server to the roles on this Sangfor device. Once a user matches certain role mapping rule and is mapped to the role on the Sangfor device, the associated user will be permitted to access the resources that are associated with that role. The **Role Mapping** tab is as shown in the figure below:

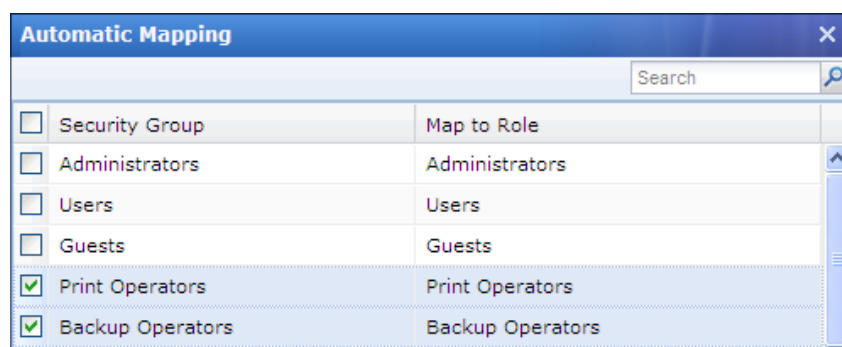


The following are the contents included on the **Role Mapping** tab:

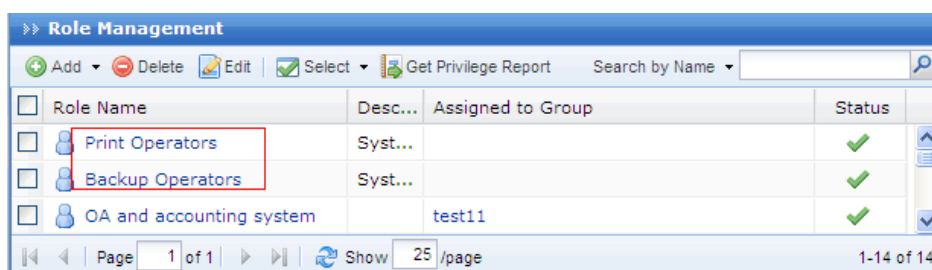
- **Add:** Click it to add a role mapping rule, mapping the security groups on MS Active Directory server to the local groups. To configure role mapping, please perform the following steps:
 - a. Select **Enabled** to enable role mapping feature.
 - b. Click **Add** to enter the **Add Role Mapping Rule** page, and configure the **Security Group** and **Map to Role** fields, as shown below:



- **Delete:** To delete a role mapping rule, select the rule and click **Delete**.
- **Edit:** To edit a role mapping rule, select the rule and click **Edit**.
- **Automatic Mapping:** Click it and some role mapping rules will be generated automatically according to the security groups on the MS Active Directory server. To configure automatic mapping, please perform the following steps:
 - a. Click **Automatic Mapping** and the following page pops up, as shown below:



- b. Select the desired role mapping rules and click the **OK** and **Save** buttons. The two selected roles are then added to **Role Management** page, as shown below:



7. Configure LDAP Extensions.

LDAP Extensions are extended attributes of the users on LDAP server. This feature enables some resources and virtual IP addresses of the users to be stored and maintained on the LDAP server.

Group Mapping | Role Mapping | **LDAP Extensions** | Password Encryption

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. What you need to do are, selecting the option Attribute names of associated resources, and adding the attribute name (ssl_resource) into the list. Attribute name format: '<resource name>:<protocol name://>host address: port', among which, the fields in '<>' are optional, and host address and port are required. Example: OA system: http://xxx.com:80, 192.168.1.1:1-65535.


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 **SSL VPN > Users**), this option is invalid.

8. Configure **Password Encryption** tab.

This feature enables user password to be encrypted before it is forwarded to LDAP server.

The following contents are included on above page:

- **Enabled:** Select it to enable password encryption feature.
 - **Encryption Protocol:** Specifies encryption protocol. Options are **MD5** and **SHA1**.
 - **Size:** Specifies the size of encryption key. It can be 32-bit or 16-bit.
 - **Character Case:** Specifies character case of password.
9. Click the **Save** button and then the **Apply** button to save and apply the settings.

RADIUS Authentication

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

Configuring RADIUS Server


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

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:



3. Configure the **Basic Attributes** of the RADIUS server. The following are basic attributes:

- **Server Name, Description:** Configures name and description of the RADIUS server.
- **Server Address:** Configures the usable IP address and port of the RADIUS server. You can add multiple IP addresses and ports. Generally, only the first IP address/port is active and others are standby. If the first IP address/port is unavailable, the second IP address/port will take the place; if the second IP address/port is unavailable, the third IP address/port will take the place, and so on; if none of the configured server IP address/port is available, the server will be disconnected.

To add a server address/port, click the **Add** icon  next to **Server Address** field. The **Add Server Address** page is as shown in the figure below:

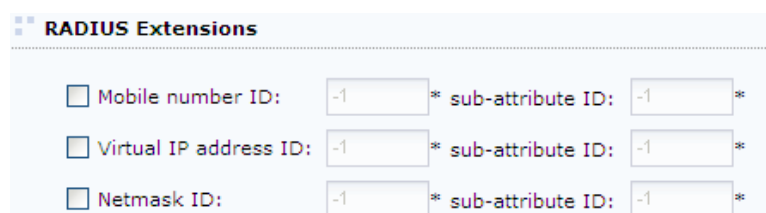
To remove an entry, click the entry and click **Delete** icon  next to **Server Address**.

To edit an entry, click the entry and click **Edit** icon  next to **Server Address**.

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

- **Authentication Protocol:** Options are **PAP, CHAP, Microsoft CHAP, Microsoft CHAP2 and EAP-MD5**. Select the protocol as needed.
- **Shared Secret:** Configures the shared key used for RADIUS authentication.
- **Character Set:** Configures the character set used for RADIUS authentication.
- **Authentication Timeout:** Configures the time period that user authentication times out if RADIUS server gives no response.
- **Status:** Indicates whether the external RADIUS server is enabled.

4. Configure **RADIUS Extensions**, as shown below:



RADIUS Extensions

Mobile number ID: * **sub-attribute ID:** *

Virtual IP address ID: * **sub-attribute ID:** *

Netmask ID: * **sub-attribute ID:** *

- **Mobile number ID:** Configures attribute ID and sub-attribute ID of the RADIUS user mobile number attribute. Once a RADIUS user logs in to the SSL VPN, the RADIUS server will return the attribute value to the Sangfor device.
- **Virtual IP address ID:** Configures the attribute ID and sub-attribute ID of RADIUS user's virtual IP address. When a RADIUS user logs in to the SSL VPN, the RADIUS server will return the attribute value to the Sangfor device.



-
- Mobile number ID only works in association with SMS authentication.
-

5. Configure **Group Mapping** rule.

The users with specified class attribute will be mapped to the corresponding group on the Sangfor device after successful login, and therefore have the same privilege as the users under the group to which they are mapped.

The following are the contents:

- **Add:** Click it to enter the **Add Group Mapping Rule** page and configure the two fields **Class** and **Map to Group**. The specified class attribute value on the RADIUS server will be mapped to the specified local group, as shown in the figure below:

- **Delete:** To delete a group mapping rule, select that rule and then click **Delete**.
 - **Edit:** To edit a group mapping rule, select that rule and then click **Edit**.
 - **If RADIUS user matches none of the above mapping rules, map the user to group:** For the users that match none of the group mapping rules, select this option and specify the local group to which the RADIUS users will be mapped automatically.
6. Click the **Save** button and then the **Apply** button to save and apply the settings.

Certificate/USB Key Based Authentication

Sangfor device not only supports built-in CA, but also supports external CA or more than one external CA, and can offer some certificate information. If Sangfor device is deployed in HQ, branch users can use certificate issued by different third-party CA for authentication when logging into SSL VPN. It increases flexibility of SSL VPN deployment. Certificates could be generated and configured through the **Certificate/USB Key Based Authentication** page.

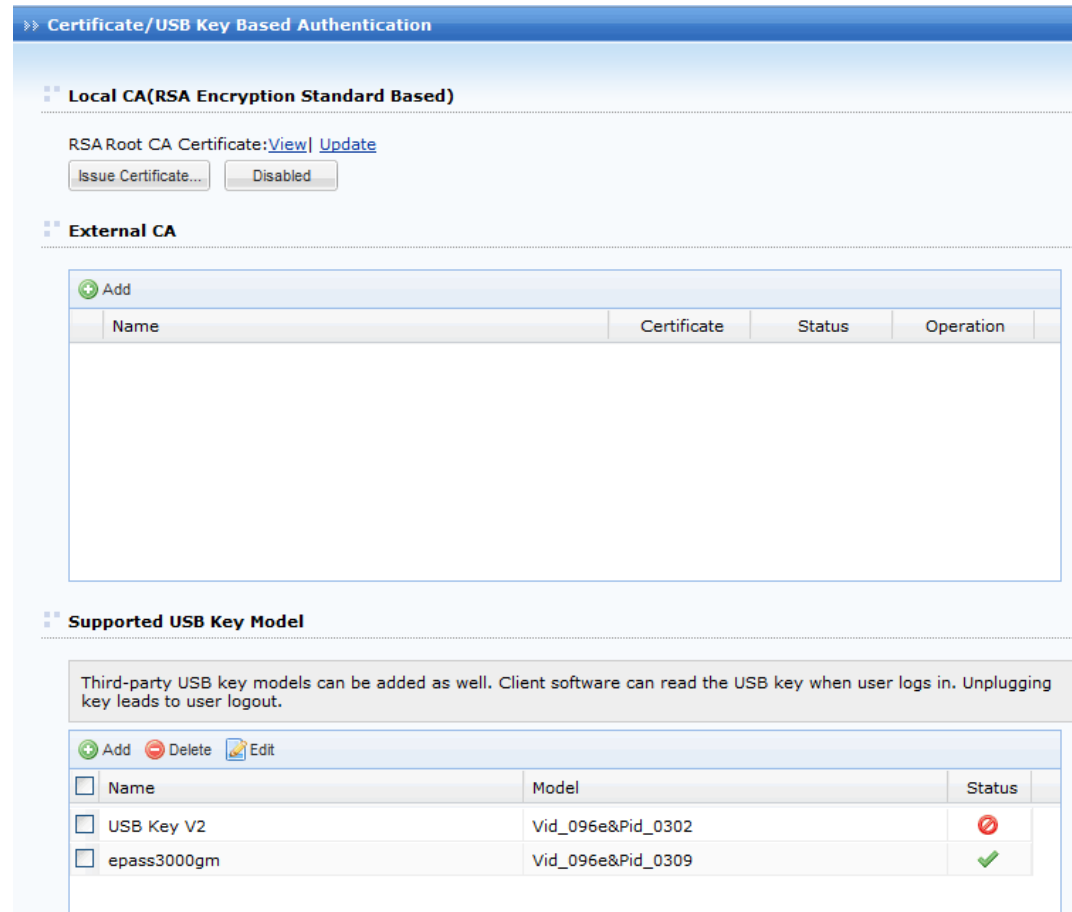
Navigate to **SSL VPN > Authentication** to enter the **Authentication Options** page.



To download and install USB key driver manually, click **USB Key Driver**.

To download and install USB key tool manually, click **USB Key Tool**.

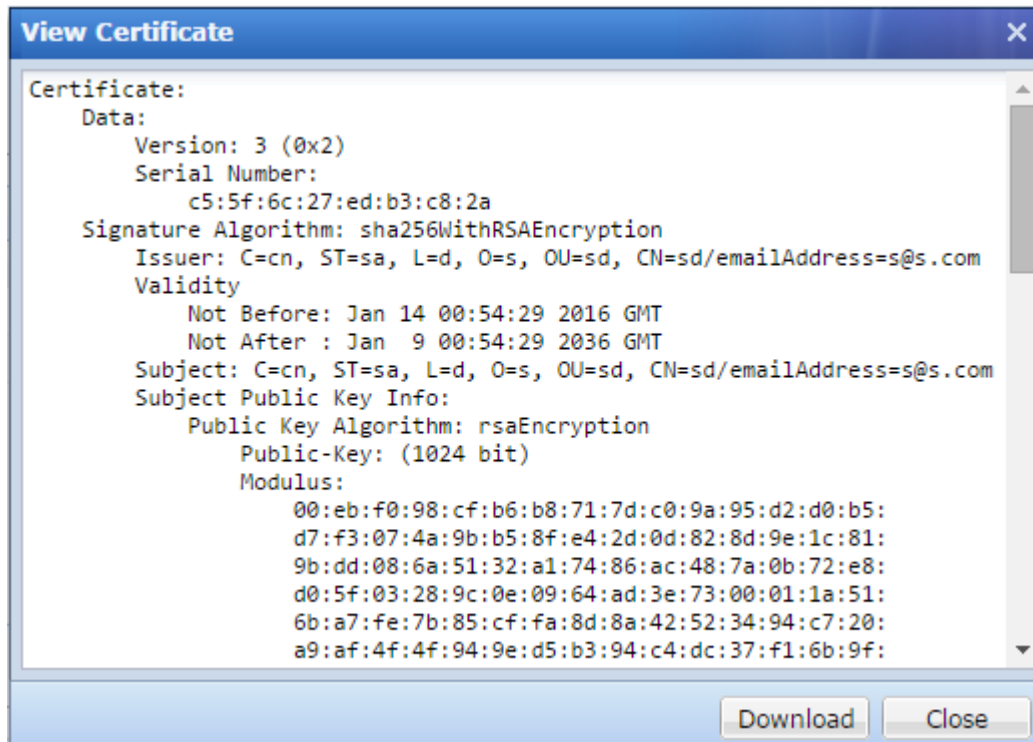
Click the **Settings** button following **Certificate/USB Key** and the **Certificate/USB Key Based Authentication** page appears, as shown in the figure below:



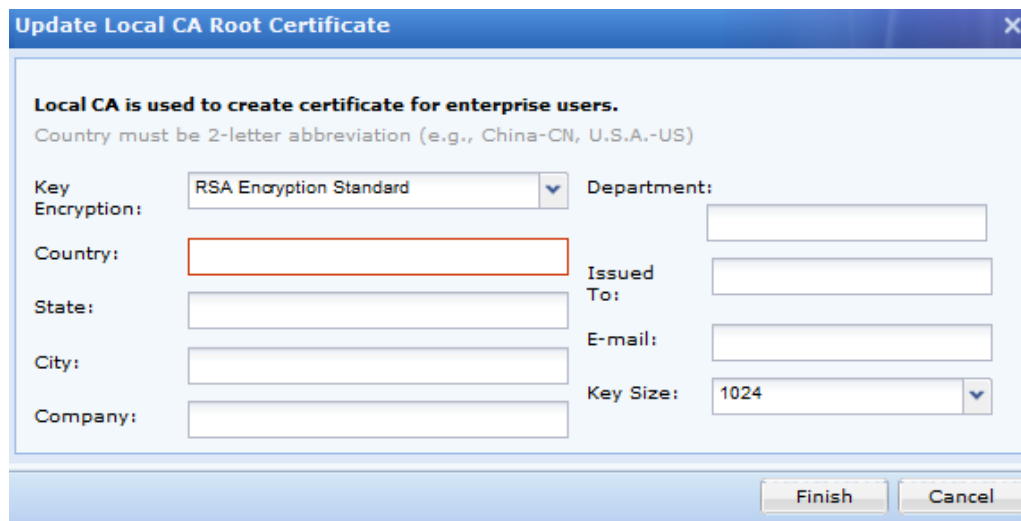
Configuring Local CA

The following contents are under **Local CA** section:

- **View:** Click it to view root certificate of local CA, as shown below:



- **Update:** Click it to update root certificate, as shown in the figure below:



When **RSA Encryption Standard** is selected in Key Encryption field, key size can be 1024, 2048 or 4096, while **SM2 Encryption Standard** is selected, key size can be 256 only. Configure all the required fields above and then click **Finish** to save the setting, and then a root certificate will be created, and it will be also taken as device certificate.



- Country must be a two-letter abbreviation of country, for example, CN indicates China.
 - Email address should not contain any full-angle characters.
-
- **Issue Certificate:** Click it to enter the **Issue a Certificate** page. The issued certificate can be used as user certificate or a server certificate.

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

Country: CN *
State: GD *
City: SZ *
Company: company *
Department: section *
Issued To: *
E-mail: *
Certificate Password:

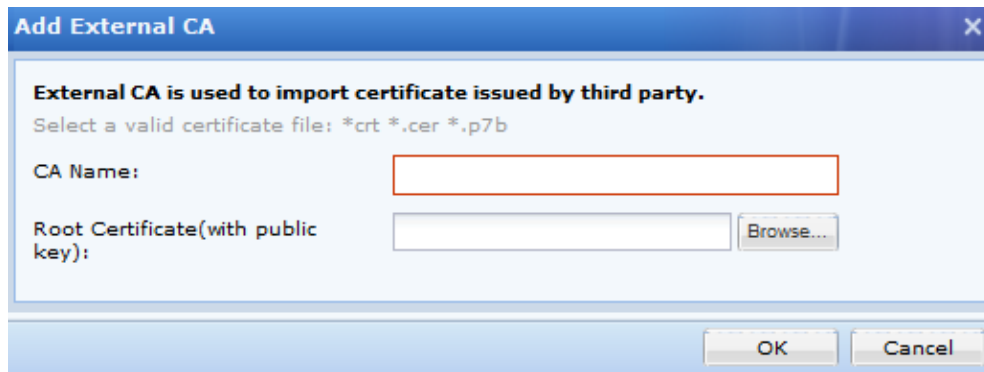
OK Cancel

To generate the certificate, configure all the fields and click **OK** to save the changes.

Configuring External CA

The following contents are under **External CA** section.

- **Add:** Click it to to enter the **Add External CA** page, as shown below:



Specify the CA name and select a root certificate from local PC. Click **OK** to save the changes. Then you will see the newly-imported external CA, as shown in the figure below:

External CA			
+ Add			
Name	Certificate	Status	Operation
1 External CA	View Update	✓	✗

A maximum of seven external CA is supported.

Click on the **External CA** in **Name** column. You will see the following page:

» External CA

Certificate Attributes

Instructions

Username Attr:

Binding Field:

CA Encoding:

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

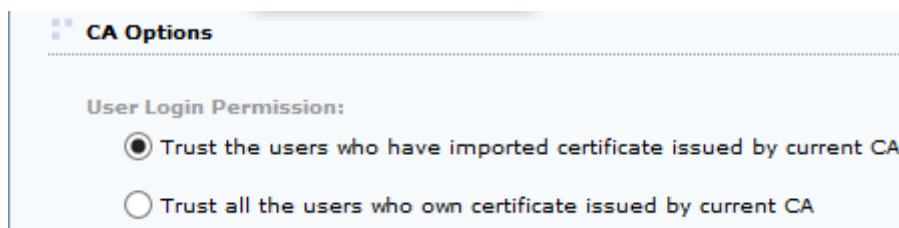
[Import File or Configure Auto-Update Server](#)

Online Certificate Status Protocol(OCSP)

Enable OCSP

The following information are included on above page:

- **Username Attr:** Indicates the field used to store username in certificate issued by this CA. The username will be displayed on the homepage of client. Options are **CN**, **Email Prefix** and **OID**.
- **Binding Field:** Indicates the certificate field binding to a user. It takes effect when current certificate is imported into Sangfor device.
 - **License Key:** If it is selected, CA will issue a new certificate when the certificate gets expired. As the license key of new certificate has changed, user needs to imports this new certificate on **Local Users** page.
 - **CN:** If it is selected, user does not need to import new certificate when user certificate is updated. Before selecting this option, user needs to make sure the DN of each certificate is different.
 - **OID:** It is similar with DN. Generally, user also needs to specify OID attribute for storing username.
 - **CA Encoding:** Indicates the encoding used by this certificate.
 - **CA Options:** It determines whether the users are trusted if they own certificate issued by the current external CA, that is to say, whether they are allowed to log in to the SSL VPN.

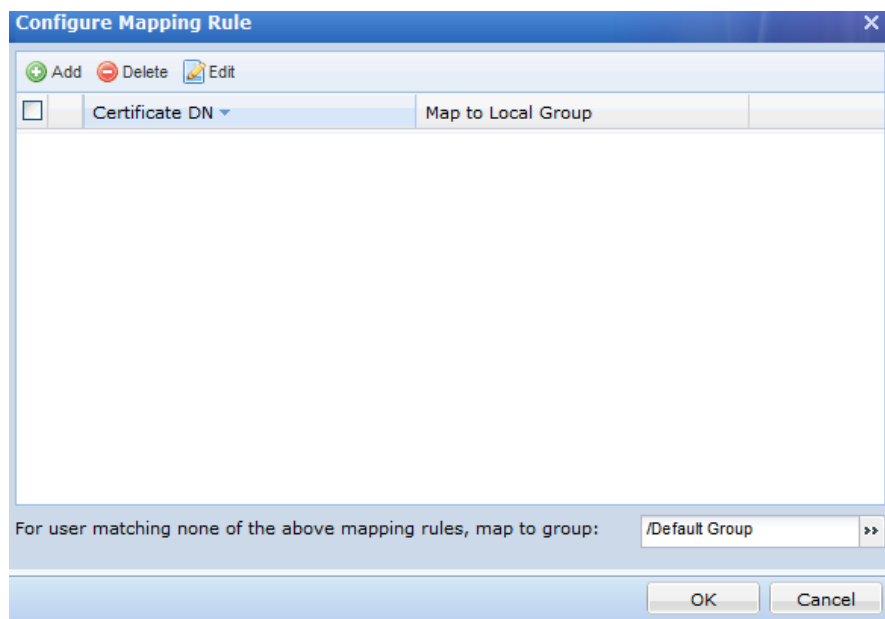


If **Trust the users who have imported certificate issued by current** is selected, only after the users certificates have been imported to the Sangfor device can they use their own certificates to log in to the SSL VPN.

If **Trust all the users who own certificate issued by current CA** is selected, all the users who own valid certificates issued the current external CA will be able to log in to the SSL VPN with their own certificates.



Click on the link **Configure Mapping Rule** to enter the **Configure Mapping Rule** page, as shown in the figure below:



Configure the **Mapping Rule** that can map the certificate users of certain certificate DN to a group on the Sangfor device, so that they will have the same privilege as others under the target group.

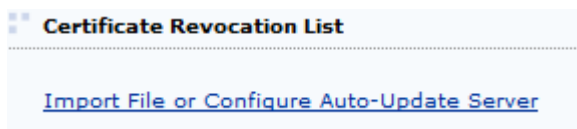
To delete a mapping rule, select the rule and click **Delete**.

To edit a mapping rule, select the rule and click **Edit**.

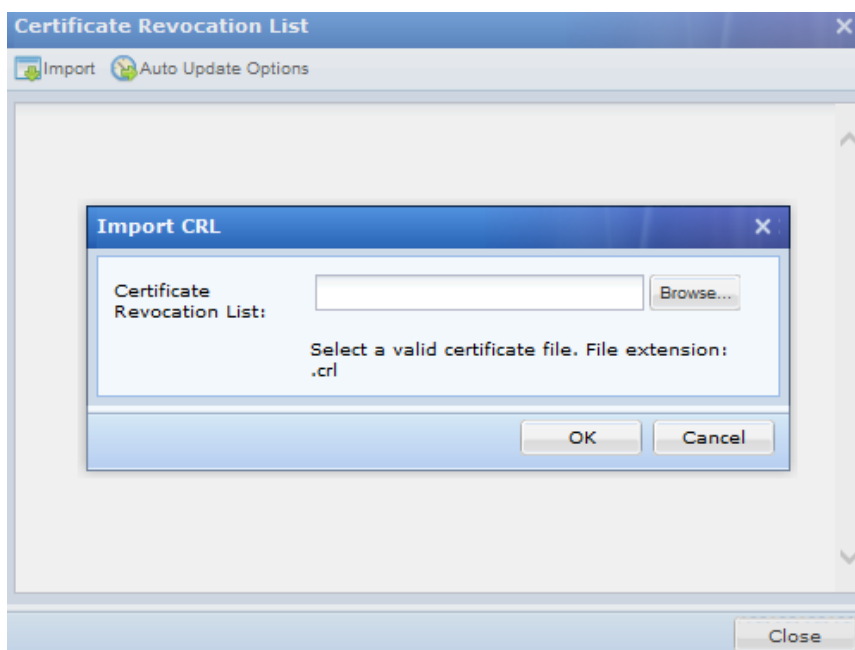
To add a new mapping rule, click **Add** and the **Add External Certificate User Mapping Rule** page appears, as shown below:



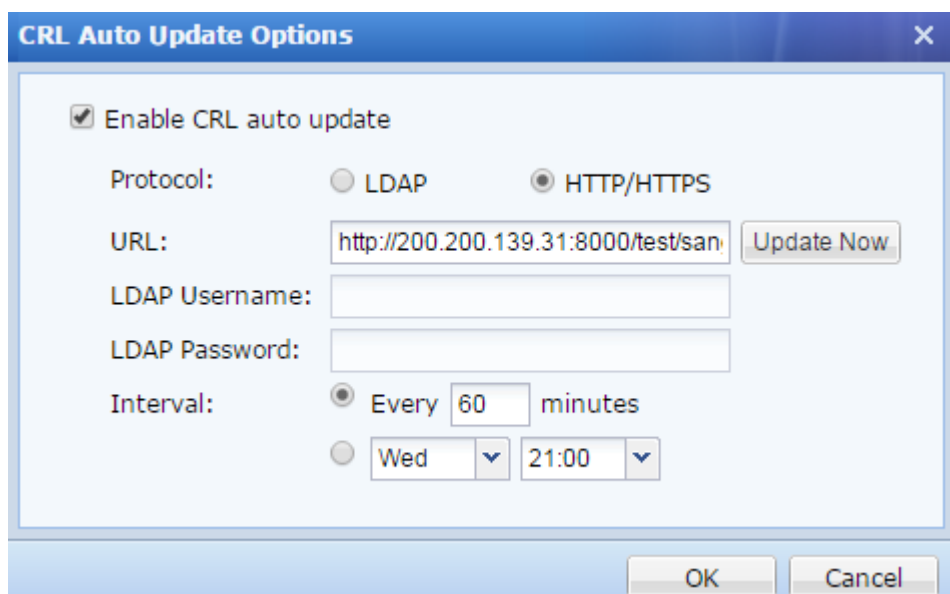
- **Certificate DN:** Configures DN of certificate, which can be referred to in certificate subject.
- **Map to Group:** Configures the local group to which the certificate users will be mapped if their certificates have the configured DN.
- **For user matching none of the above group mapping rules, map the user to group:** Configures the local group to which the certificate users will be mapped automatically if they match none of the mapping rules.



- Certificate Revocation List (CRL):** Click the link **Import File or Configure Auto-Update Server** to import certificate or enable auto-update, as shown below:



To have the CRL updated automatically and regularly, click the **Auto Update Options** link and configure the fields on the **Auto Update Options** page, as shown in the figure below:



Configure **Online Certificate Status Protocol(OCSP)**. This part includes options related to OCSP that supports online check of certificate validity, as shown in the figure below:

The contents under **Online Certificate Status Protocol(OCSP)** are as follows:

- **Enable OCSP:** Select this option and OCSP will be enabled and related options will appear.
- **Server Address, Server Port:** Configure the address and port of OCSP server that provides OCSP service.
- **Authentication required:** Select this option and the OCSP server will verify identity of the Sangfor device.
- **Test Connectivity:** Click it to check whether the Sangfor device can connect to the OCSP server.

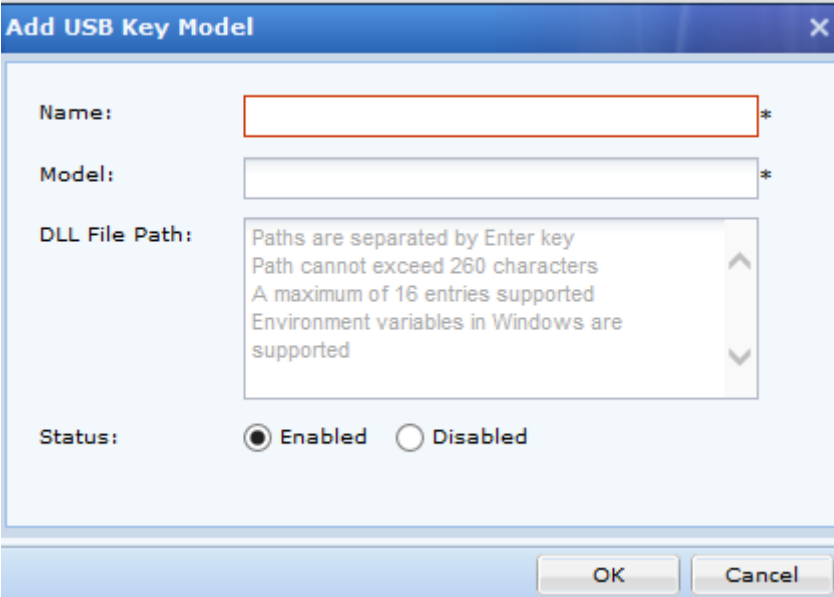
Configuring USB Key Model

Under **Supported USB Key Model**, configure the model of third-party USB keys that can be identified by the Sangfor device while USB key of this model is plugged in to the end user's PC. Unplugging key will lead to automatic logout.

The contents under this part are as shown below:

Name	Model	Status
USB Key V2	Vid_096e&Pid_0302	✓
epass3000gm	Vid_096e&Pid_0309	✓

To add a new USB key model, click **Add** to enter **Add USB Key** page, as shown below:



The following are the contents included on **Add USB Key** page:

- **Name:** Specifies name of this USB key model.
- **Model:** Specifies the model of USB key that supports automatic logout while end user unplugs the USB key.
- **DLL File Path:** Specifies the path of DLL file that is used to provide interface for SM2 encryption function. It is required when adding third-party USB key supporting SM2 encryption algorithm.
- **Status:** Configures whether this model of USB key is enabled or not, that is, whether to enable the feature of automatic logout while end user unplugs the USB key of this model.

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

To edit an entry, select the entry and click **Edit**.

Client-Side Domain SSO

Client-side domain SSO can achieve that when users logs in using VPN client, user does not need to type username and password and domain SSO will be performed automatically after client-side PC is joined AD domain. This feature is not applicable to user logging using Portal.

1. Navigate to **SSL VPN > Authentication** to enter **Authentication Options** page. Click the **Settings** button following **Client-Side Domain SSO** and **Client-Side Domain SSO** page appears, as shown below:

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: sangfor619e23c7

Domain Name: *

Short Domain Name: *(on server version earlier than Windows 2000)

Domain Controller Name: *

Domain Controller IP: *

Admin Username: *

Admin Password:

Save Cancel

2. Configure **Basic Attributes** on above page:
- **Enabled:** Click it to enable client-side domain SSO feature.
 - **Status:** Indicates whether this feature takes effect.
 - **Device Name:** Indicates name of Sangfor device.
 - **Domain Name:** Specifies the domain name of domain server
 - **Short Domain Name:** Specifies the abbreviation of the domain name
 - **Domain Controller Name:** Specifies the name of domain controller in Window domain.
 - **Domain Controller IP:** Specifies the IP address of the domain controller in Window domain.
 - **Admin Username, Admin Password:** Specifies the administrator username and password used to log in to Window domain.

Secondary Authentication Methods

There are three secondary authentication methods, namely, **SMS authentication**, **Dynamic Token** based authentication and **Hardware ID** based authentication.

SMS Authentication

SMS authentication is a type of authentication method that requires connecting user to enter the received SMS password when he/she is logging in to and has passed the primary authentication(s).

The SMS password is a password dynamically generated and sent to the mobile phone of connecting user. Only after user enters and submits the SMS password can he/she access SSL VPN and the internal resources.

Navigate to **SSL VPN > Authentication** to enter the **Authentication Options** page. Click the **Settings** button following **SMS** and the **SMS Authentication** page appears, as shown below:

SMS Authentication

SMS Message

Authentication: Enabled Disabled

Set Phone Number: User can set phone number on login

Reset password through SMS: Resetting password through SMS is allowed

Delivery Interval: seconds (0-3600)(the period after which SMS password could be sent again)

Pwd Validity Period: minutes (1-440)

Country Code: (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

Msg Delivery Module: Use built-in SMS module
 Use SMS module installed on external server

SMS Center IP: *

SMS Center Port: *

In case that the SMS license is invalid or has not been activated, tips show up under the subtitle **SMS Message**, saying “SMS authentication license key is invalid. Please [click here](#) to activate the license”. To modify or activate the SMS license, click the **click here** link to enter **Licensing** page.

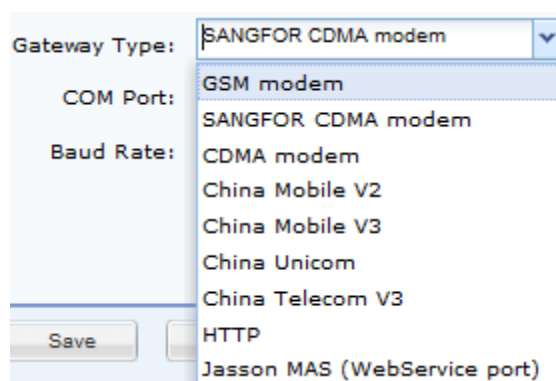
As shown on the above page, there are three sections related to SMS authentication, namely, **SMS Message**, **Message Delivery Module** and **Message Delivery Parameters**.

The following are the contents on **SMS Authentication** page:

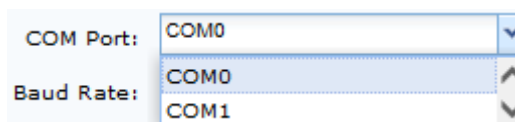
- **Authentication:** Indicates whether SMS authentication is enabled or not. Options are

Enabled and Disabled.

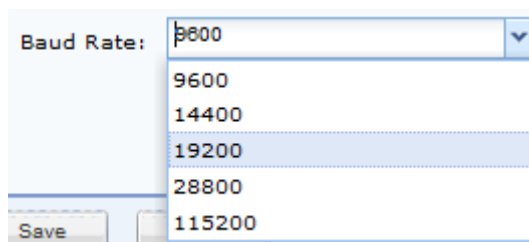
- **Set Phone Number:** If the option **User can set phone number on login** is selected, user can specify mobile phone number on login page. When adding user, administrator does not need to specify mobile phone number if **SMS password** is selected as secondary authentication. Then, user could specify mobile phone number to receive OTP. After successful authentication, the mobile phone number will be bound with the user account.
- **Reset password through SMS:** To enable users to reset password through SMS, select the option **Resetting password through SMS is allowed**.
- **Delivery Interval:** Specifies the interval for resending a SMS message.
- **Pwd Validity Period:** Configures the validity period of the SMS password. If user fails to enter and submit the SMS password within the time since the SMS password is sent, the SMS password will get invalid. Login with invalid SMS password will lead to login failure. The validity period should be between 1 and 1440 minutes.
- **Message Text:** Customizes the text of the SMS message that is to be sent to the end user.
- **Restore Default:** Click this link and the system default text will replace the current message text.
- **Message Delivery Mode:** There are two types of modules, built-in SMS module and SMS module installed on external server. Select either option and configure the other required fields.
- **Gateway Type:** Specifies the ways of delivering SMS messages. There are seven types of gateway, GSM modem, SANGFOR CDMA modem, CNMA modem, China Mobile V2, China Mobile V3, China Unicom, China Telecom V3, HTTP, Jasson MAS(WebService port). You can use **GSM modem** (connected to the server's COM port) or using **gateway** (such as China Mobile V2/V3, China Unicom and China Telecom V3, gateways usually used by enterprises) to send SMS messages.



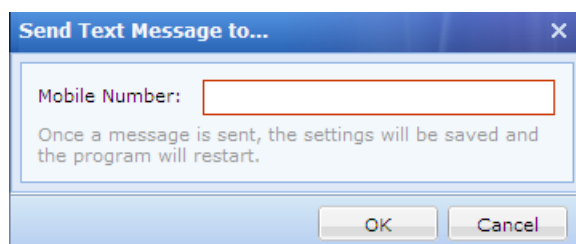
- **SMS Center:** Indicates the SMSC number of corresponding ISP.
- **COM Port:** Indicates the COM port used to connect to SMS modem. Options are **COM1** and **COM2**.



- **Baud Rate:** Specifies the baud rate of the specified COM port of Sangfor device. Default is 9600.



- **Send Test SMS Message:** Click this link to check whether SMS message can be sent to end user successfully through the configured GSM modem or gateway. A **Send Text Message to...** page will pop up asking for mobile number, as shown in the figure below:



Using SMS Gateway of ISP to Send SMS Message

If the enterprise network is already deployed with SMS gateway of ISP, such as China Mobile, China Unicom, no other facility is needed except the Sangfor device. Configure the following:

- **Gateway Type:** Select a gateway type that is available to the enterprise network.
- **SMS Center IP:** If the message delivery module is installed on an external server, enter the IP address of the server on which the SMS module is installed.
- **SMS Center Port:** Enter the port number being used to listen to SMS service.
- **Message Delivery Parameters:** Configure the required fields according to the information provided by the corresponding ISP.

Using Webservice Based SMS Platform to Send SMS Message

Sangfor device can communicate with Webservice-based SMS platform for sending SMS message to end users, enhancing the stability. Navigate to **SSL VPN > Authentication > SMS Authentication** page and select HTTP as **Gateway Type**. Configure the required fields, URL of webservice-based SMS platform, SOAP version, request mode and URL template.

Message Delivery Parameters

Tips: Changes take effect after SMS module restart

Gateway Type: HTTP

URL: *

Encoding: UTF-8

SOAP Version: SOAP1.1 SOAP1.2

Request Method: POST GET

URL Template: [Configure URL Template](#)

[Send Test SMS Message](#)

Click the link **Configure URL Template** to enter the **Configure URL Template** page, as shown below:

Configure URL Template

Web Interface:

WDSL File: Select a wsd, xml or xsd file [Browse...](#) [Generate Template](#)

Request Template:

[Help](#)

Notes:
 \$\$USER_NAME\$\$ will be replaced by username
 \$\$MOBILE_NUM\$\$ will be replaced by mobile phone number
 \$\$SMS_CONTENT\$\$ will be replaced by message text
 \$\$DATE:%Y-%m-%d %H:%M:%S\$\$ will be replaced by current time
 \$\$LOCAL_TIME\$\$ will be replaced by current time in second
 \$\$SERIAL_ID\$\$ will be replaced by user ID.
 \$\$SERIAL_ID:6\$\$ will be replaced by user ID length
 \$\$ENCODE_MD5:MOBILE_NUM\$\$ will be encrypted with MD5

Response Template:

Fields can be separated by []. Variables supported, such as username, phone number or SMS No.

[OK](#) [Cancel](#)

Configure the fields on above page and click **OK** to save the changes.

Using Jasson MAS to Send SMS Message

Sangfor device can use Jasson MAS for sending SMS message so as to enhance stability.

Message Delivery Parameters

Tips: Changes take effect after SMS module restart

Gateway Type: Jasson MAS (WebService port) ▼

URL: *

Database Server IP: *

Port: 3306 *

Database Name: *

Database Admin: *

Password: *

Web Interface: *

Login Name: *

Password: *

[Send Test SMS Message](#)

Configure the following contents included on above page:

- **URL:** Enter the URL of Jasson MAS.
- **Database Server IP:** Enter the IP address of database server on Jasson MAS.
- **Port:** Enter the database port according to your case. Default value is 3306.
- **Database Name:** Enter the name of database server on Jasson MAS. You need to confirm with the network administrator that the database name you entered is correct.
- **Database Admin, Password:** Enter the username and password of internal database on MAS. If you do not know the username or password, contact with the network administrator.
- **Web Interface:** Enter the interface of Jasson MAS used to send SMS message.
- **Login Name, Password:** Specifies username and password to log in Jasson MAS.

Hardware ID Based Authentication

Hardware ID is a unique serial number generated using the extracted features of hardware components in a computer, according to certain algorithm. The uniqueness of computer components makes the generated hardware ID unique.

Navigate to **SSL VPN > Authentication** to enter the **Authentication Options** page. Click the **Settings** button following **Hardware ID** and the **Hardware ID Based Authentication** page appears, as shown in the figure below:

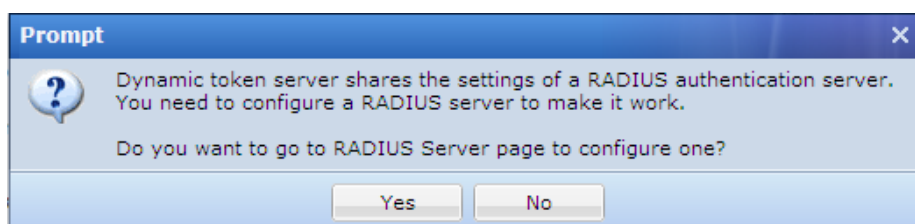
The following are the contents included on **Hardware ID Based Authentication** page:

- **Collect hardware ID only:** If this option is selected, hardware IDs of endpoint computers will be collected, but hardware ID based authentication will not be enabled.
- **Enable hardware ID based authentication:** If this option is selected, hardware ID of endpoint computers will be collected and hardware ID based authentication enabled.
- **Message on Collecting:** This will turn out to be a prompt seen by end users when they go through hardware ID based authentication.
- **Auto approve any hardware ID:** Indicates that any hardware ID submitted by end user will be approved, and administrator need not approve them manually.
- **Allow login on approved endpoint, with any account:** Indicates that hardware IDs submitted by any user from certain endpoint(s) will be approved automatically if administrator has ever approved the hardware ID of the endpoint(s).
- **Save:** Click this button to save the settings when configuration is completed.

Dynamic Token Based Authentication

Dynamic token based authentication is an extension of RADIUS authentication, using a RADIUS server to distribute passcode to connecting user when they go through dynamic token based authentication. Dynamic token based authentication is a secondary authentication and can add security to SSL VPN access.

Navigate to **SSL VPN > Authentication** to enter the **Authentication Options** page. Click the **Settings** button following **Dynamic Token** and the following prompt appears:



To go to **RADIUS Server** page to configure RADIUS server, click the **Yes** button. For procedures of configuring RADIUS server, please refer to the RADIUS Authentication section in Chapter 4.

Other Authentication Options

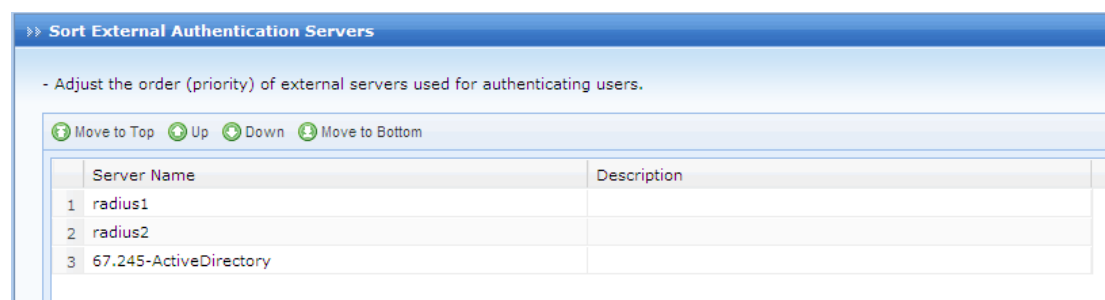
This section includes configurations of **Priority of LDAP/RADIUS Servers**, **Password Security Options** related to password and brute-force login prevention, and **Anonymous Login** related settings.

Priority of LDAP and RADIUS Servers

If there are more than one LDAP servers or RADIUS servers available for user authentication, it becomes necessary to consider choosing an LDAP or RADIUS server as the first server from which the matching account will be searched for when user is connecting to SSL VPN and going through LDAP/RADIUS authentication.

Administrator can adjust the order (priority) of the available external LDAP/RADIUS servers on the **Sort External Authentication Servers** page.

Navigate to **SSL VPN > Authentication** to enter the **Authentication Options** page. Click the **Settings** button following **Priority of LDAP/RADIUS Servers** and the **Sort External Authentication Servers** page appears, as shown in the figure below:



Since the order indicates priority, the external authentication server sitting at the top of the list has the highest priority. User will go through this server first to find the matching account while connecting to SSL VPN.

If the connecting user is not found on the first external authentication server, the matching process will not stop. User will then go through the second (or third, or fourth) external authentication server until the right user account is matched. If no account is matched eventually, user authentication will fail.

To adjust order of an external authentication server, select the server and click **Move to Top**, **Move Up**, **Move Down** or **Move to Bottom**.

When configuration is completed, click the **Save** button to save the changes.

Password Security Options

Password security options are settings related to login when user submits username and password to access the SSL VPN, including two parts, **Logon Security Options** and **Brute-force Login Prevention**.

Navigate to **SSL VPN > Authentication** to enter the **Authentication Options** page. Click the **Settings** button following **Password Security Options** and the **Password Security Options** page appears, as shown in the figure below:

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 , 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 (1-32), lock the user (30-1800) seconds

If consecutive logon failures on one IP reach (64-2048), lock IP address for (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:

The screenshot shows the 'Access SSL VPN' login interface. It includes a 'Username:' field, a 'Password:' field, a green 'Log In' button, and 'Other Login Methods' such as 'Use Certificate' and 'Use USB Key'. A keyboard overlay is positioned over the password field, showing a grid of keys including numbers, letters, and function keys like 'Enter', 'Cancel', and 'Close'.

- Brute-force Login Prevention:** This security feature enables the system to take actions to stop brute-force login attempt. If user fails to log in many times, the login IP address or the user account would be locked up or word verification be enabled for a period of time. The prompt given is as shown below:

The screenshot shows the 'Access SSL VPN' login page with a yellow warning box containing the message: "You are trying brute-force login. The user account is locked!". The 'Log In' button is still visible below the warning.

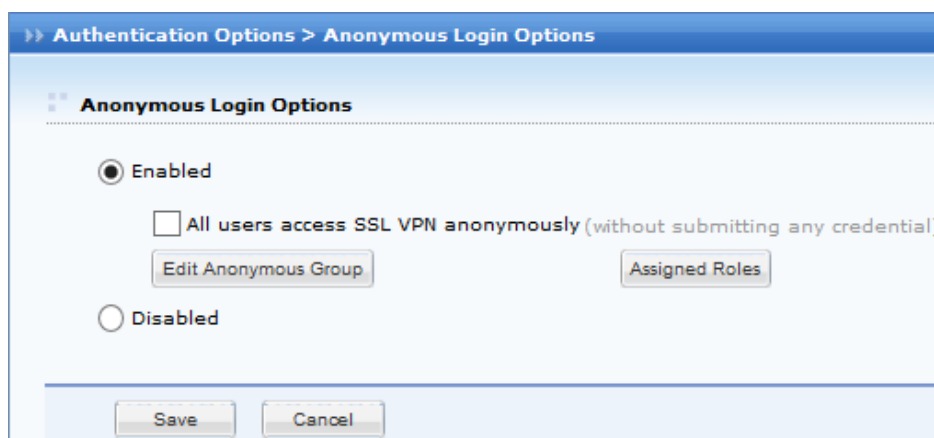
- Word Verification:** It is also a feature that adds security to SSL VPN access. If this option “If consecutive logon failures reach N, activate word verification” is selected, 0 means word verification will be enabled forcibly; for non-Windows client-side, if the input value is less than 3, it will still be taken as 3. Once word verification is activated, end user will be required to enter the word he or she sees on the picture when visiting the login page and logging in to the SSL VPN, as shown below:

The screenshot shows the 'Access SSL VPN' login page with a 'Verification' field. To the right of the field is a CAPTCHA image showing the characters 'B2QP'. A green 'Log In' button is located at the bottom of the form.

Anonymous Login

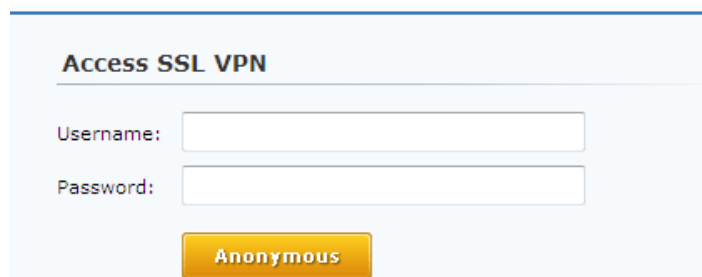
Anonymous login is a kind of login method that does not require connecting user to enter username and password, user accessing SSL VPN anonymously under the anonymous login user account and being able to access the resources that are associated with **Anonymous group**.

Navigate to **SSL VPN > Authentication** to enter the **Authentication Options** page. Click the **Configure** button following **Anonymous Login** and the **Anonymous Login Options** page appears, as shown in the figure below:



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

- **Enabled, Disabled:** If **Disabled** is selected, no user could log in to the SSL VPN anonymously. If **Enabled** is selected, anonymous login is enabled, and end users can access the SSL VPN anonymously, simply by clicking the **Anonymous** button on the login page, as shown below:



- **All users access SSL VPN anonymously:** If this option is selected, all users can access SSL VPN anonymously (enter the **Resource** page, or the redirected-to page if this feature is enabled in the associated policy set), without submitting any credential through login page.
- **Edit Anonymous Group:** Click this button to configure the attributes of **Anonymous group**. For detailed guide, please refer to the Adding/Editing Resource Group section in Chapter 4. The attributes of **Anonymous group** are as shown in the figure below:

» Edit User Group

Basic Attributes Fields marked * are required

Name: *

Description:

Added To: »

Max Concurrent Users: (0 indicates no limit)

Status: Enabled Disabled

Inherit parent group's attributes

Inherit authentication settings

Inherit policy set

Inherit assigned roles

Authentication Settings

User Type: Public group Private group

Primary Authentication

Local password

Certificate/USB key

External LDAP/RADIUS ▾

Secondary Authentication

Hardware ID

SMS password based

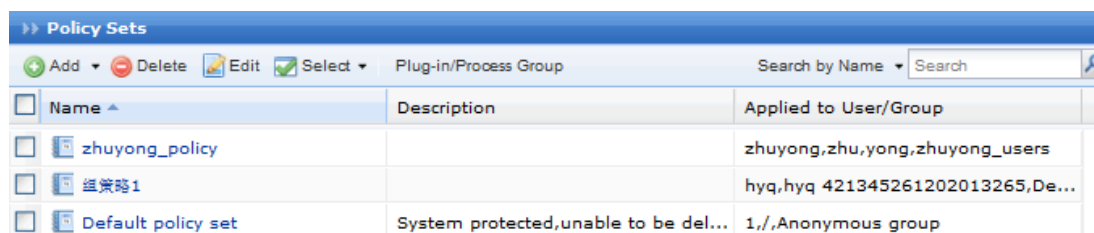
Dynamic token ▾

- **Assigned Roles:** Click this button to select and assign roles to the anonymous users. For detailed guide, please refer to the Adding Role section in Chapter 4.
- **Save:** Click it to save the settings. To apply changes, click the **Apply** button on the next page.

Policy Sets

A policy set is a collection of policies controlling end user's access to SSL VPN, rights at client end, and access rights on Security Desktop, including settings of **Client**, **Account Options**, **Remote Application and Cloud Storage**.

Navigate to **SSL VPN > Policy Sets** to enter the **Policy Sets** page, as shown below:



Name	Description	Applied to User/Group
zhuyong_policy		zhuyong,zhu,yong,zhuyong_users
组策略1		hyq,hyq 421345261202013265,De...
Default policy set	System protected,unable to be del...	1,/,Anonymous group

On the page displayed above, **Name** indicates the name of a policy set, **Description** indicates the descriptive information of a policy set and **Applied to User/Group** indicates the users/groups to which the corresponding policy set applies.

The following are some optional operations on the **Policy Set Management** page:

- To create a new policy set, click **Add > Policy set**.
- To create a policy set based on an existing policy set, select a policy set as template and click **Add > By using template**.
- To delete one or more policy sets, select the policy sets and then click **Delete**.
- To edit a policy set, select the policy set and then click **Edit**.
- To select policy sets on all pages, click **Select > All pages**.
- To select policy sets on the current page, click **Select > Current pages**.
- To deselect entries, click **Select > Deselect**.
- To search for a specific policy set, select **Search by Name**, **Search by Description** or **Search by User/Group**, enter the keyword and click the magnifier icon next to the textbox.

Adding Policy Set

1. Navigate to **SSL VPN > Policy Sets** and click **Add > Policy set** to enter the **Add Policy Set** page, as shown below:

2. Specify the name and descriptive information for the policy set.
3. Configure the following client-related options on the **Client** tab:
 - **Privacy Protection:** Specifies the contents to be automatically deleted at user's logout to protect user's privacy. Select **Temporary Internet files**, **Cookies**, **Browsing history** and/or **Form data**.
 - **Temporary Internet files:** Indicates the copies of webpages, images and media that are saved for faster viewing.
 - **Cookies:** Indicates the files stored on users' computer by websites to save preferences.
 - **Browsing history:** Indicates the links to the pages that users have visited.
 - **Form data:** Indicates the saved information that users have typed into forms.
 - **Bandwidth/Sessions Restrictions:** Specify limits on TCP app sessions and bandwidth for client, and select whether to preferentially enable byte cache.
 - **Enable TCP app sessions limit:** Check it to enable limit on TCP app sessions at client and then specify the maximum number of TCP application sessions allowed. The value range is 1 to 500. Unchecking it means no limit on TCP app sessions.
 - **Enable bandwidth limit:** Check it to enable limit on bandwidth for using Web applications, TCP applications and L3VPN at client and then specify maximum outbound and inbound bandwidth (KBps) allowed at client. The minimum value for

this field is 32 KBps and 0 means no limit. This function avoids the situation that some users preempt most of the HQ bandwidth with insufficient bandwidth left for others. Unchecking it means no limit on bandwidth used at client end.

- **Preferred to enable byte cache:** Check it to have the corresponding user preferentially enjoy the speedup of file access or downloading when the number of concurrent users reaches the maximum. Unchecking it means the corresponding user has no privileges to preferentially enjoy optimization.



To make the **Preferred to enable byte cache** option available here, select the **Enable Byte Cache** option (in **System > SSL VPN Options > Network Optimization > Data Transfer > Byte Cache Options**). Please refer to the **错误! 未找到引用源。** section in Chapter 3).

- **Permit PPTP/L2TP incoming connection:** Select whether to allow mobile users to log in through PPTP/L2TP.
- **Enable Dedicated SSL VPN Tunnel:** If this option is checked, users can only access the internal resources over SSL VPN. Unchecking it means users can access internal resources as well as the Internet after connecting to the SSL VPN. This feature is only applicable to the Windows or Android based client end.
- **Each user may own multiple hardware IDs, maximum:** Specify the maximum of hardware IDs that each use account can bind to. The value range is 1 to 100.



After configuring policy set completes, you need to associate it with user or user group when adding or editing user/group; otherwise, it will not work .

4. Click **Account Options** tab to enter the **Account Options** page and specify the account-related options, as shown below:

Policy Options

Client Account Options Remote Application Cloud Storage EMM

Account Options

Log access events

Enable system tray

On user's logon, redirect to resource >>

User can only log in during the schedule >

Account becomes invalid if user has not logged in for days (0 indicates no limit)

Connection Timeout

Access Using PC:
Disconnect user if inactivity period reaches (5-43200)minutes (it becomes invalid if local DNS is enabled)

Access Using Mobile Device:
Disconnect user if inactivity period reaches (5-86400)minutes (it becomes invalid if local DNS is enabled)

Allow Private User to Modify Account

Password Description Mobile Number

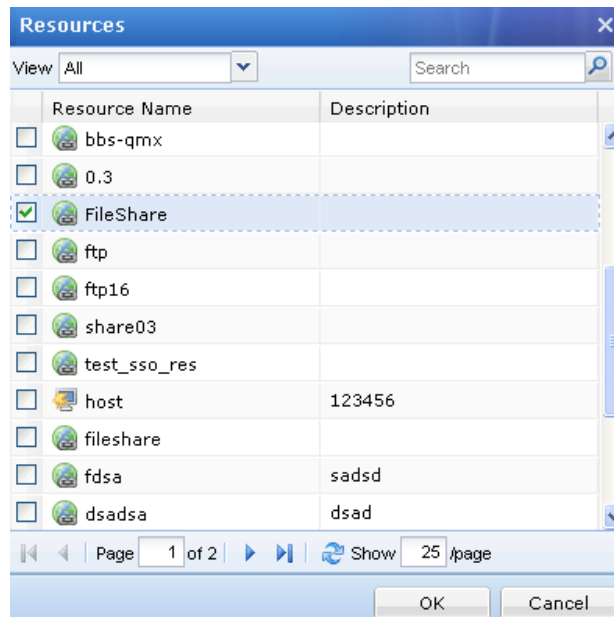
The following are the contents included on the **Account Options** tab:

- **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 for the user associated with this policy set (please refer to the [错误!未找到引用源。](#) section in Chapter 3).

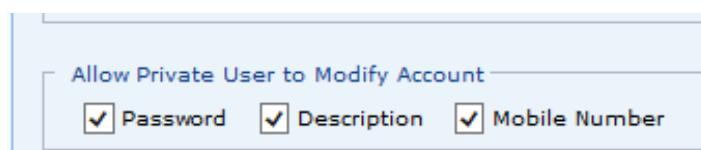


The **Enable system tray** option under **System > SSL VPN Options > General > Client Options** is a global option for all users. If it is checked, the **Enable system tray** option here is selected by default.

- **On user's logon, redirect to resource:** Specify the resource to which the page will be redirected after user logs in to SSL VPN. Select this option and click the textbox to enter the **Resources** page, as shown below, and then select the resource (the resources available here are predefined in **SSL VPN > Resources**. Please refer to the Resource section in Chapter 4).



- **User can only log in during the schedule:** Specify the period of time only during which the user is allowed to access SSL VPN. Select a schedule from the drop-down list (the schedules available here are predefined in **System > Schedule**; please refer to the [错误!未找到引用源。](#) section in Chapter 3).
- **Account becomes invalid if user has not logged in for N days:** Specify the number of days required for a user account to be disabled due to not being used.
- **Connection Timeout:** Specifies the period of time to disconnect user due to inactivity for two logout scenarios.
- **Allow Private User to Modify Account:** Select **Password**, **Description** and/or **Mobile Number** if you allow private user to modify the password, description and mobile phone number.



If a private user is allowed to modify the password, description and mobile number, the user can click **Settings** (at upper right of the page) to modify its password, description and mobile number after logging in to SSL VPN.



To allow a user to modify mobile number, enable SMS authentication for the user while adding or editing the user.

5. Click **Remote Application** tab to enter the **Remote Application** page and configure the related options.

The screenshot shows the 'Remote Application' configuration page. It includes the following sections:

- Logon to Remote Server:**
 - User Account: (dropdown)
 - (for users use server's own account, they have right to access some crucial system programs, such as Mstsc.exe, Shutdown.exe)
 - 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 client
- 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 printing with Foxit fails.)
 -
- Application Access Privileges:**
 - Granted to: All subnets Specified subnet/domain
 - Advanced Privilege:

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

- **Logon to Remote Server:** Specifies what user account and privilege type is used by user to log into remote server.
 - **User Account:** Specifies what account can be used by mobile user to log in to remote server, as shown below:

The close-up shows the 'User Account' dropdown menu with the following options:

- 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

- **Type:** It appears when **Create Windows account as per SSL VPN account** is selected as **User Account**. It indicates the type of the created Windows account.
 - **Deletion:** If this option is selected, related account and data created on remote server will be removed together when user is removed from local device.
- **Allow Use of Local Devices/Resources in Session:** Select the device and/or resource you want to use in session, as shown below:

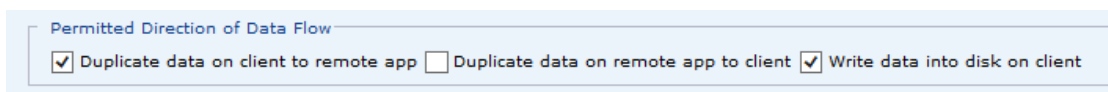
The close-up shows the following options selected:

- Drives
- Clipboard
- Printer
- Virtual Printer

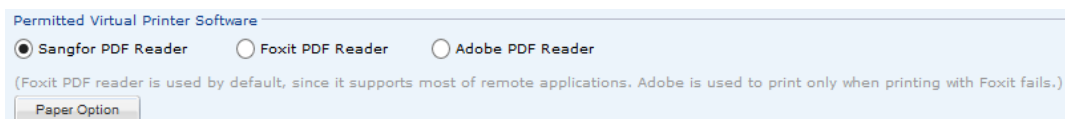
- **Drives:** If it is selected, VPN users can save file onto local drives when accessing

remote application resource.

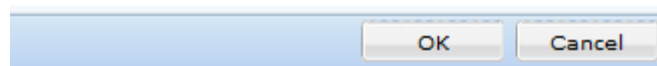
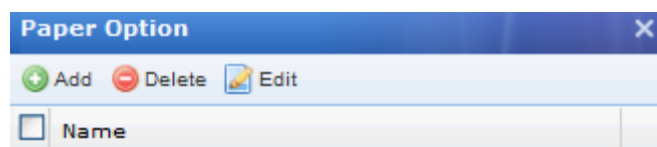
- **Clipboard:** Select it to enable user to duplicate data from client end to remote server .
- **Printer:** If this option is selected, user can use the printer at client end to print the document in remote application after printer driver is installed on remote server.
- **Virtual Printer:** If it is selected, user can choose Sangfor virtual printer at remote server side to print file without need to install driver of local printer on remote server.
- **Permitted Direction of Data Flow:** It is available only when **Clipboard** option is selected.



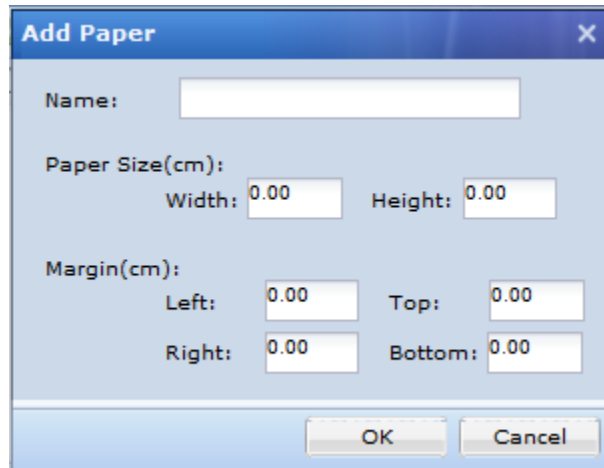
- **Permitted Virtual Printer Software:** It is configurable only when **Virtual Printer** option is selected. There are three types of virtual printer software, Sangfor PDF Reader, Foxit PDF Reader and Adobe PDF Reader. **Sangfor PDF Reader** is selected by default, which provides a better printing effect and supports more file types. If Sangfor PDF reader does not work, use Foxit or Adobe PDF reader instead. If you want to use Adobe PDF reader, it is recommended to use Adobe 9.4.



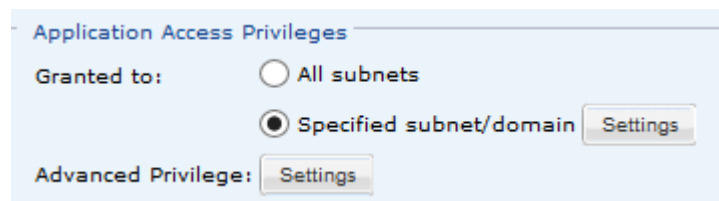
- **Paper Options:** Click it to configure paper-related options, as shown below:



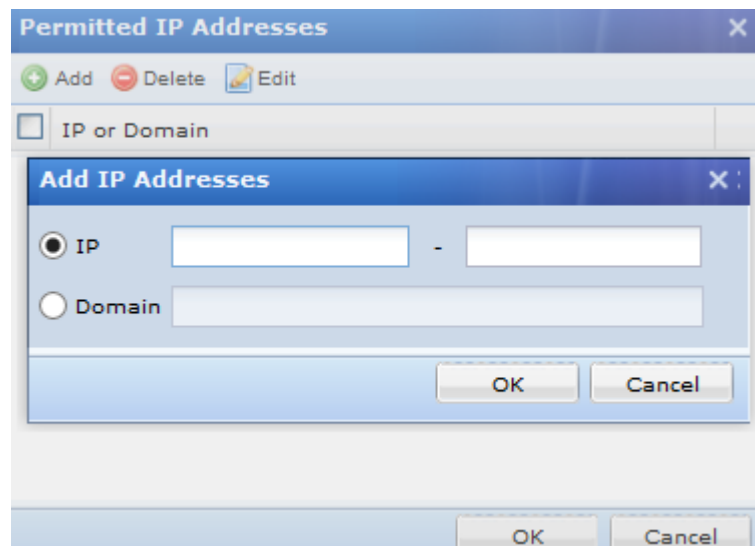
Click **Add** to enter the **Add Paper** page, specify the paper size and margin and click **OK** to save the changes, as shown below:



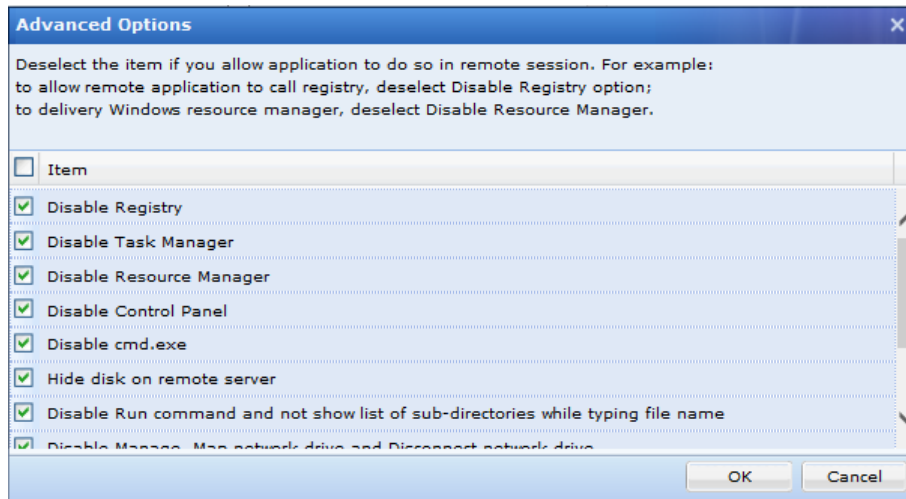
- **Application Access Privileges:** Specifies accessible subnet/domain for specific user, so as to achieve control over privilege of access to remote applications.



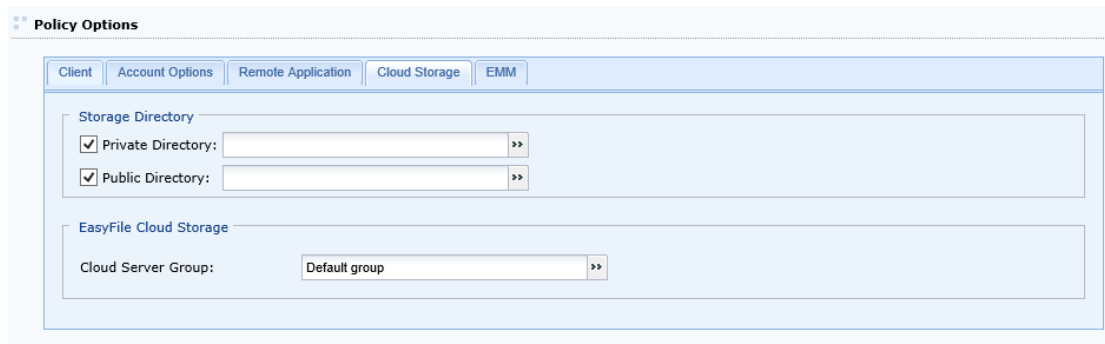
- **All subnets:** Indicates user can access all subnets.
- **Specified subnet/domain:** Specifies accessible subnet/domain for user. Click **Setting** to enter the **Permitted IP Addresses** page, click **Add** to add a entry, as shown in the figure below:




- **Advanced Privilege:** Click to configure application-related advance options, as shown below:



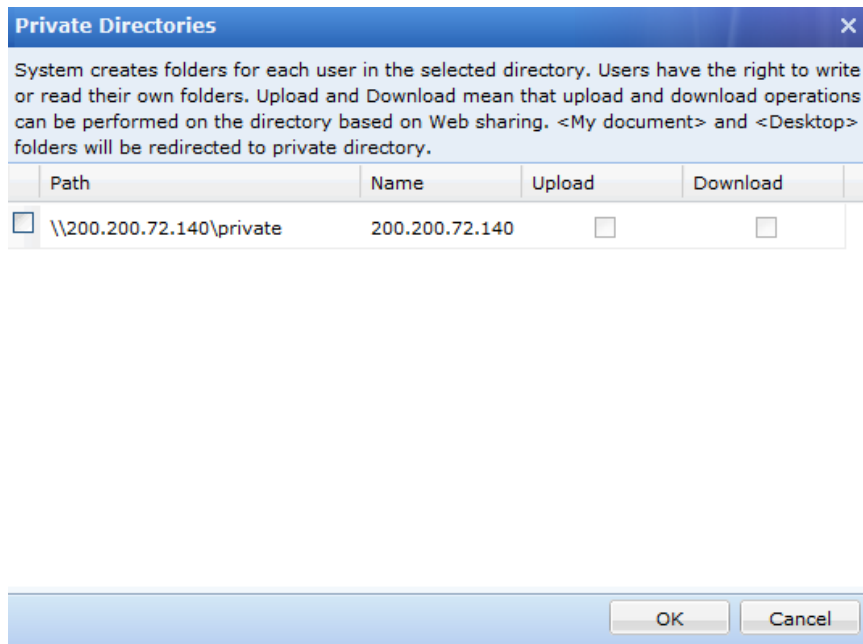
6. Click **Cloud Storage** to enter the **Cloud Storage** tab, and specify related options, as shown in the below figure:




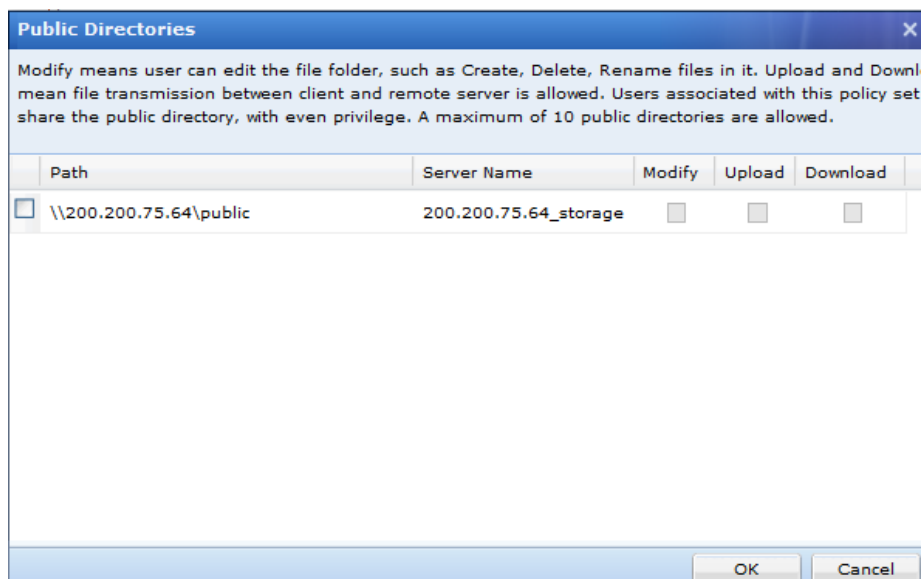
It specifies the storage privilege on remote server for users and server group used for EasyFile cloud storage.

- **Storage Directory:** Specifies the storage directory on remote server. Options are **Private Directory** and **Public Directory**. Click  following **Private Directory** or **Public Directory** to select desired directory. If no remote storage server is configured, you need to add storage server on **SSL VPN > Remote Servers > Storage Server** page (for details, refer to Adding Remote Storage Server in Chapter 4).

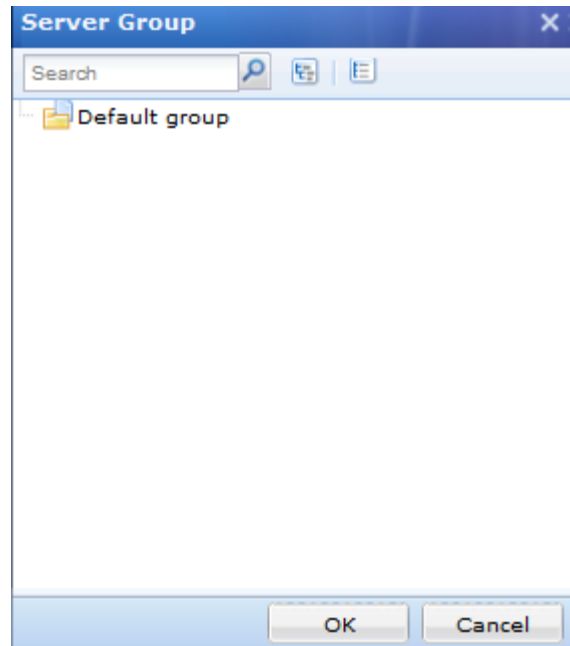
If **Private Directory** is selected, click  following it to enter the following page:



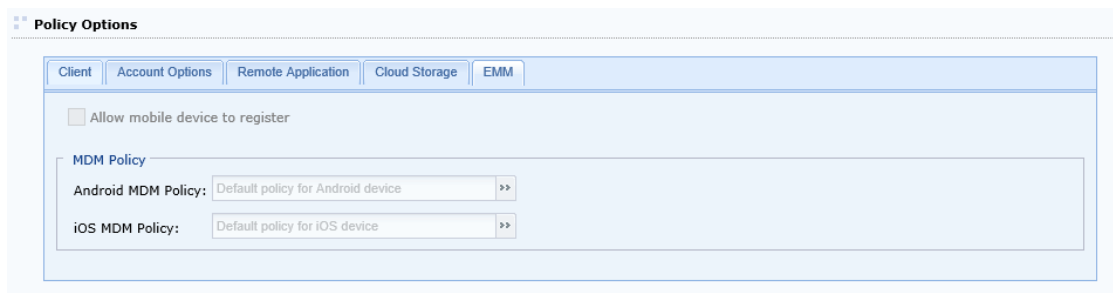
If **Public Directory** is selected, click  following it, and you will see the figure, as shown below:



- **EasyFile Cloud Storage:** Specifies the remote server group on which corresponding application will be invoked to open the file when the file on cloud is opened on mobile device, such as mobile phone, tablet.



7. Click **EMM** tab to enter the **EMM** tab. Enterprise mobility management(EMM) is to manage mobile devices that are connected to SSL VPN.



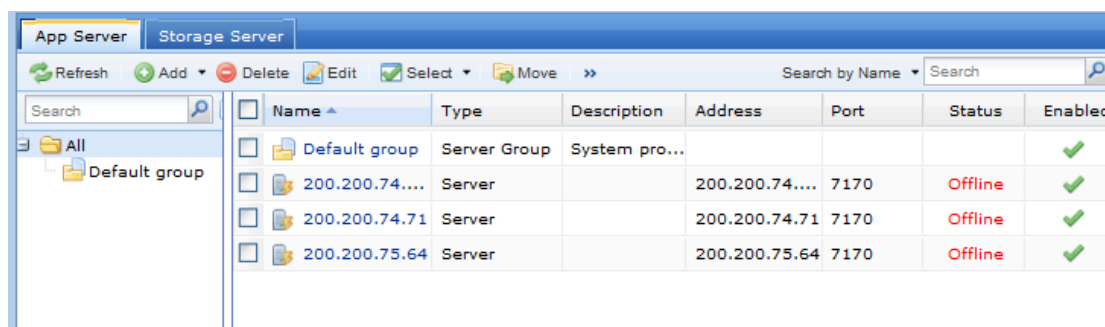
The following are contained on EMM tab:

- **Allow mobile device to register:** Determines whether mobile device is allowed to register.
 - **Android MDM Policy:** Specifies MDM policy for Android devices.
 - **iOS MDM Policy:** Specifies MDM policy for iOS devices.
8. Click **Save** to save the settings or **Cancel** not to save the settings. To have settings take effect, click the **Apply** button at upper right of the next page.

Remote Servers

Remote server falls into application server and storage servers. Remote application servers are servers providing remote applications to SSL VPN users. After connecting to SSL VPN, users can use the remote applications even though they have not installed the corresponding application programs on their local computers. Remote storage servers are servers where the data or files can be saved in the remote application session. Before adding remote server, you need to install “Terminal Services” and “RemoteAppAgent” on remote server, and make sure these programs can work properly.

Navigate to **SSL VPN > Remote Servers** to enter the **App Server** page, as shown below:

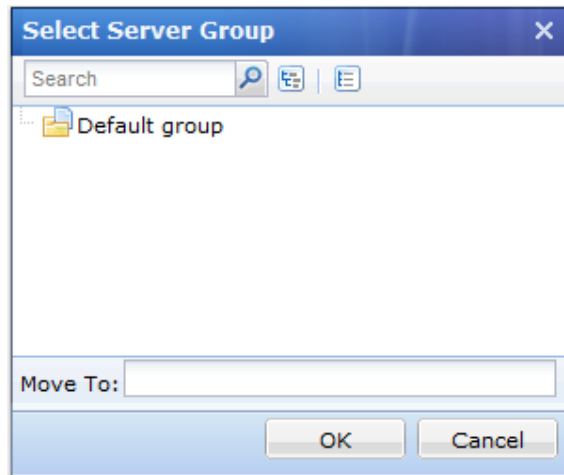


The following are the contents included on the **App Server** page:

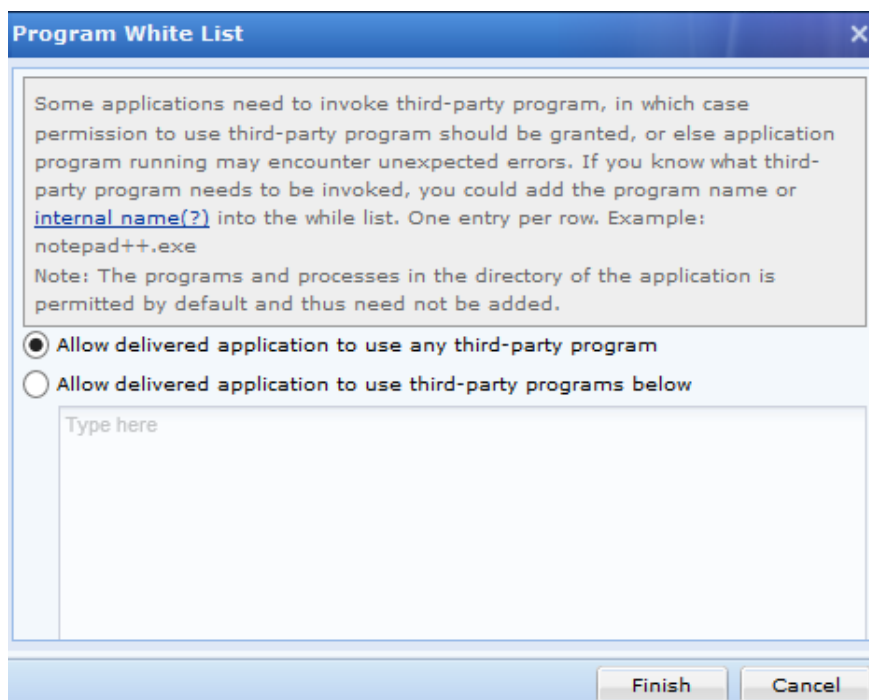
- **Name:** Displays the name of a remote server.
- **Address:** Displays the IP address of a remote server.
- **Port:** Displays the communication port of a remote server.
- **Description:** Displays the descriptive information of a remote server.
- **Type:** Displays the type of a app server, **Server** or **Server Group**.
- **Status:** Displays the status of a app server, **Online** or **Offline**.
- **Enabled:** Displays whether the app server is enabled or not.

The following are some optional operations on the **App Server** page:

- To add a app server, click **Add > App Server** or **Add > Storage Server**.
- To delete one or more app servers, select the remote servers and then click **Delete**.
- To edit a app server, select the remote server entry and then click **Edit**.
- To select app servers on all pages, click **Select > Server > All pages**.
- To select app servers on the current page, click **Select > Server > Current pages**.
- To cancel the selection, click **Select > Deselect**.
- To move the selected app server to a specified server group, click **Move** to enter the **Select Server Group** page, as shown below:

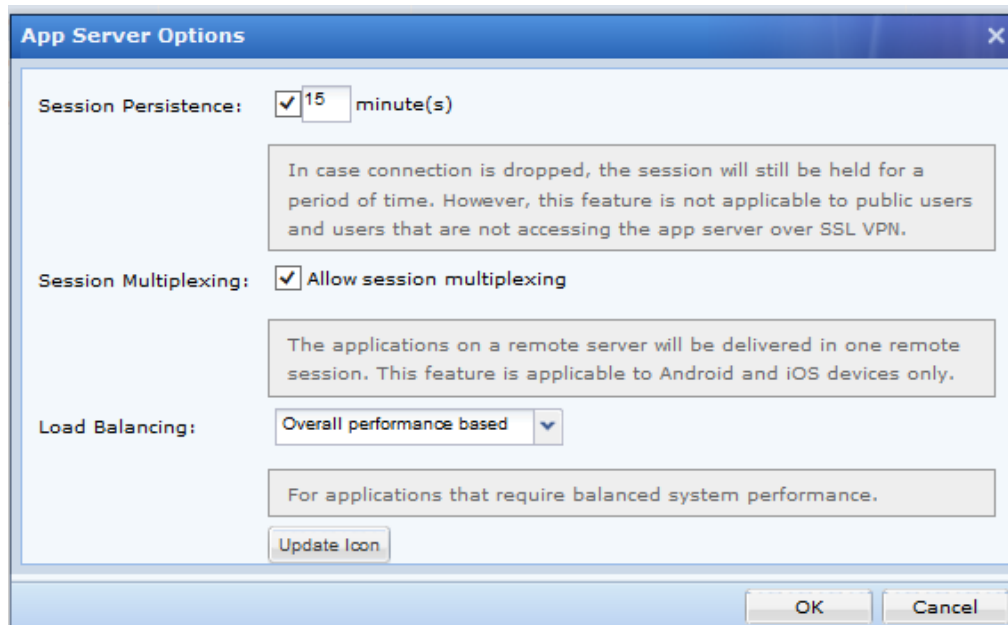


- To add multiple programs for one or more app servers, select the app servers and click **Add Multiple Programs**, and a dialog will appear, displaying the application programs available on existing remote servers. Please note that only the online app server can be associated with multiple programs.
- To allow delivered applications to invoke third-party programs, click **Program White List** and then specify third-party programs according to the specific case.



If **Allow delivered application to user third-party programs below** is selected, specify the allowed third-party programs in the textbox.

- To configure global settings for remote application servers, click **Server Options**.



- To download RemoteApp Agent and save it to local PC, click **Download RemoteApp Agent**.
- To update one or more app servers, select the app servers and then click **Update**.
- To view the status information of remote servers, click **Status** to enter **Status > SSL VPN > Remote Application** page.
- To search for a specific app server, select **Search by Name**, **Search by Description**, **Search by IP** or **Search by Program**, enter the corresponding keyword and then click the magnifier icon next to the textbox.

Adding Remote Application Server

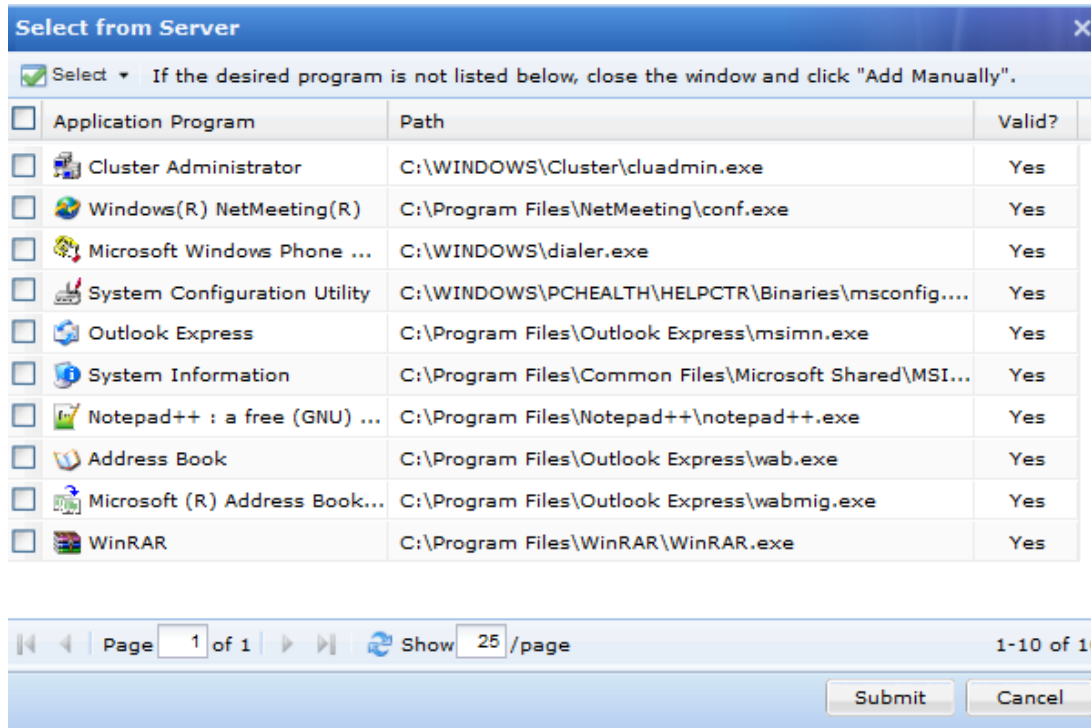
1. Navigate to **SSL VPN > Remote Servers** to enter the **App Server** page.
2. Click **Add > Server** to enter the **App Server** page, as shown below:

The screenshot shows the configuration page for an App Server. The 'Basic Attributes' section includes the following fields:

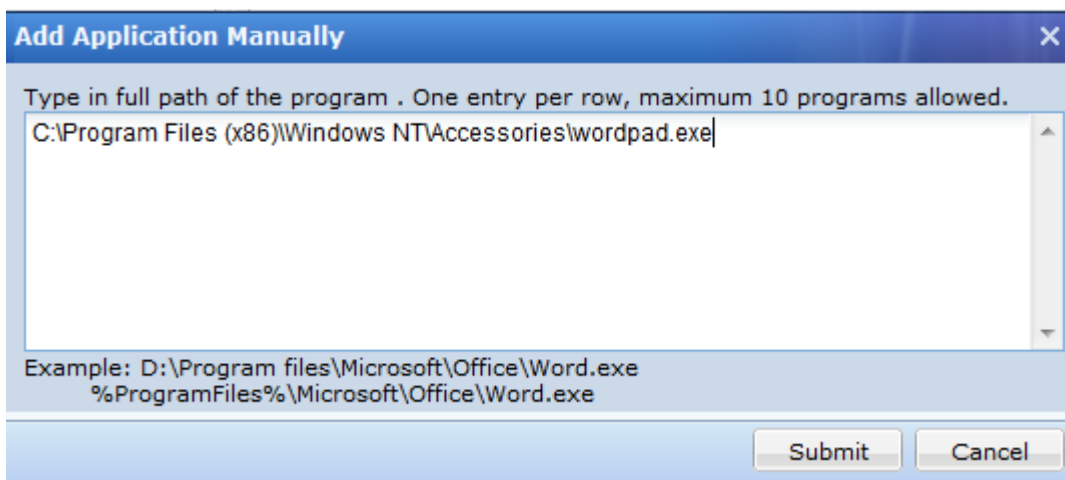
- Server Name: [] *
- Description: []
- Server Address: [] *
- Server Port: 7170 *
- Admin Account: [] *
- Password: [] Test Connectivity *
- Added To: Default group
- Max Concurrent Sessions: 0 (0 means no limit)
- Status: Enabled Disabled

The 'Remote Application Programs' section features a toolbar with the following buttons: Select from Server, Add Manually, Delete, Edit, Select, and Associated Resources. Below the toolbar is a table with the following columns: Application Program and Path.

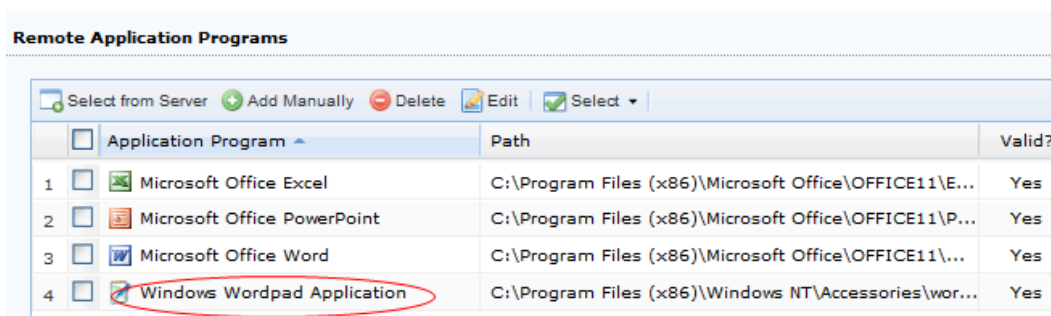
- Configure **Basic Attributes** of the application server. The following are the basic attributes:
 - Server Name, Description:** Enter a name and description for the remote application server.
 - Server Address:** Enter the IP address of the remote application server that the Sangfor device will connect to.
 - Server Port:** Specify the communication port of the remote server, through which the Sangfor device will connect to. It is 7170 by default.
 - Admin Account:** Enter the administrator name for logging into the remote application server.
 - Password:** Enter the administrator password for logging into the remote application server.
 - Added To:** Specifies a server group to which this app server is added.
 - Max Concurrent Sessions:** Specify the maximum number of concurrent connections to the remote application server.
 - Status:** Select whether to enable the current app server.
- Select and add the application programs under **Remote Application Programs**.
 - To select application programs already available on the server, click **Select from Server** to open the following page, as shown below:



- If the desired program is not available on the server, click **Add Manually** under **Remote Application Programs** to open the following dialog and then type the full path of the program, as shown below:



Click **Submit** to add the program, as shown below:



To delete the programs, select the program(s) and click **Delete**.

To edit a program, select the program and click **Edit**.

To select the programs on the current page, click **Select > Current pages**.

To select the programs on all pages, click **Select > All pages**.

To cancel the selection, click **Select > Deselect**.

To associate selected application program with existing resource quickly, click the **Associated Resources** and a dialog appears, which shows all the resources owing name with that application program.

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

If you want to add server group, click **Add > Server Group** to enter the **Add Server Group** page, as shown below:

Enter the name and description for the server group and click **OK** to save the changes.

For how to deliver remote application, refer to Adding Remote Application in Chapter 7.

Adding Remote Storage Server

Remote storage server is used to save file modified in remote application. Private directory and public directory can be created on it.

1. Navigate to **SSL VPN > Remote Servers > Storage Server** page to enter the following page:

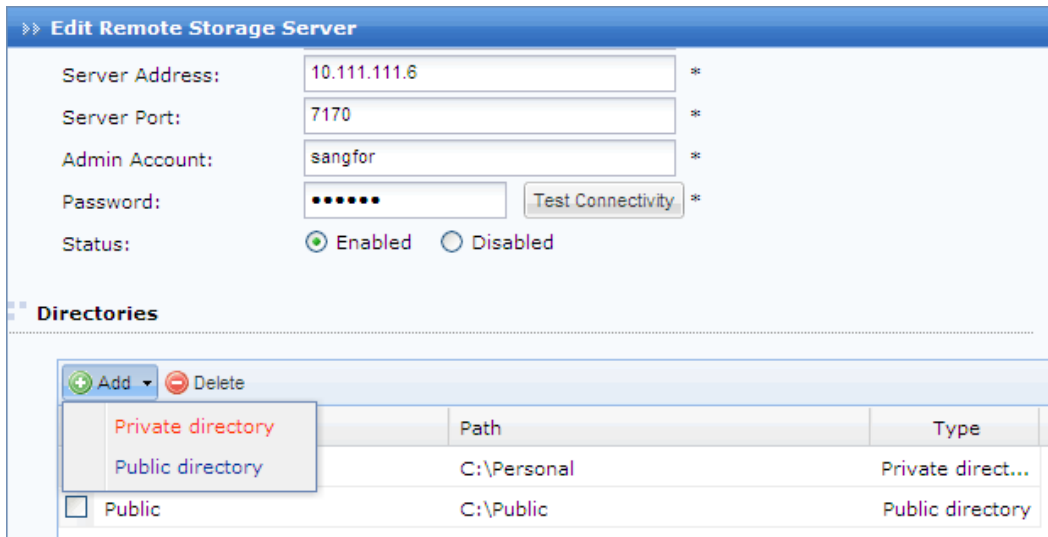
Name	Description	Address	Port	Status	Enabled
200.200.75.64_st...		200.200.75.64	7170	Offline	✓

The contents included on above page are similar with those on **App Server** page. For related description, refer to **Remote Servers** section in this chapter.

2. Click **Add** to add a storage server, as shown below:

The screenshot shows the 'Storage Server' configuration page. At the top, there are tabs for 'App Server' and 'Storage Server'. Below the tabs, the 'Basic Attributes' section is visible, with a note: 'Note: File system of storage server must be NTFS.' The fields include: 'Server Name' (required), 'Description', 'Server Address' (required), 'Server Port' (7170), 'Admin Account' (required), 'Password' (required) with a 'Test Connectivity' button, and 'Status' (radio buttons for 'Enabled' and 'Disabled'). Below this is the 'Directories' section, which has an 'Add' button and a table with columns 'Name', 'Path', and 'Type'.

3. Configure **Basic Attributes** of the storage server. The following are the basic attributes:
 - **Server Name, Description:** Enter a name and description for the remote storage server.
 - **Server Address:** Enter the IP address of the remote storage server that the Sangfor device will connect to.
 - **Server Port:** Specify the communication port of the remote storage server, through which the Sangfor device will connect to. Default port is 7170.
 - **Admin Account:** Enter the administrator name for logging into the remote storage server.
 - **Password:** Enter the administrator password for logging into the remote storage server.
 - **Status:** Select whether to enable the current remote storage server.
4. Under **Directories**, specify directory as private and/or public directory on the remote storage server.

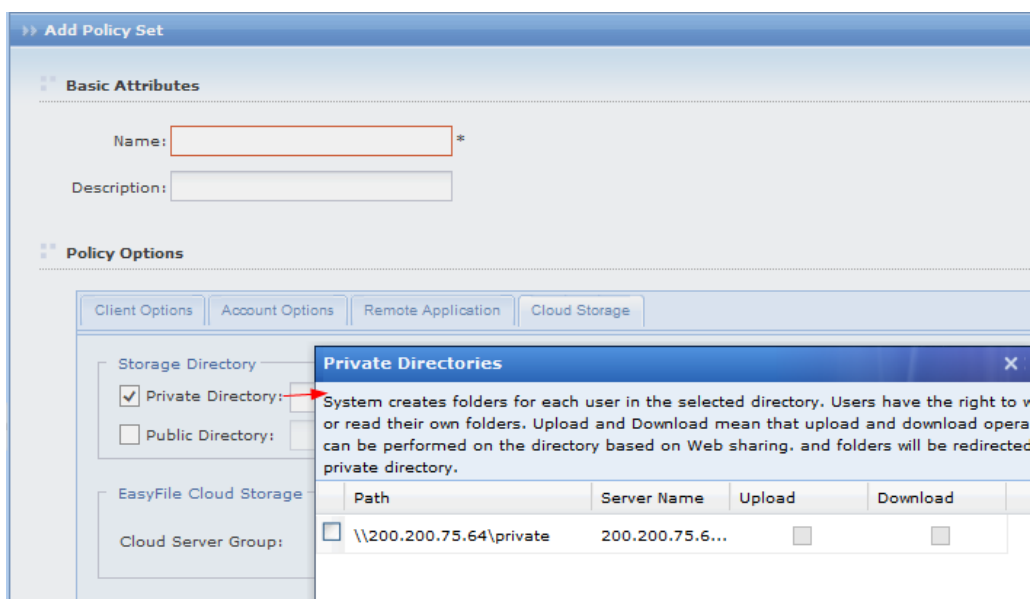


Private Directory: Each user owning private directory can see the private directory when he/she logs in to SSL VPN. This user has full privilege of this directory, he/she can create sub-directory, add, or delete file/file folder.

Public Directory: All users can see public directory associated with them. They can read file under this directory. The administrator has administrative privilege to determine whether user can write the file under this directory. If user has the right to write the file, he/she can save the modified file to the public directory.

To specify private directory or public directory, click **Add > Private directory** or **Public directory** to enter the **Private Directories** page or the **Public Directories** page, and then select a directory as the private or public directory.

When an end user accesses to the remote application, a personal folder will be automatically created in the specified directory which is configured in the associated policy set, as shown in the figure below.

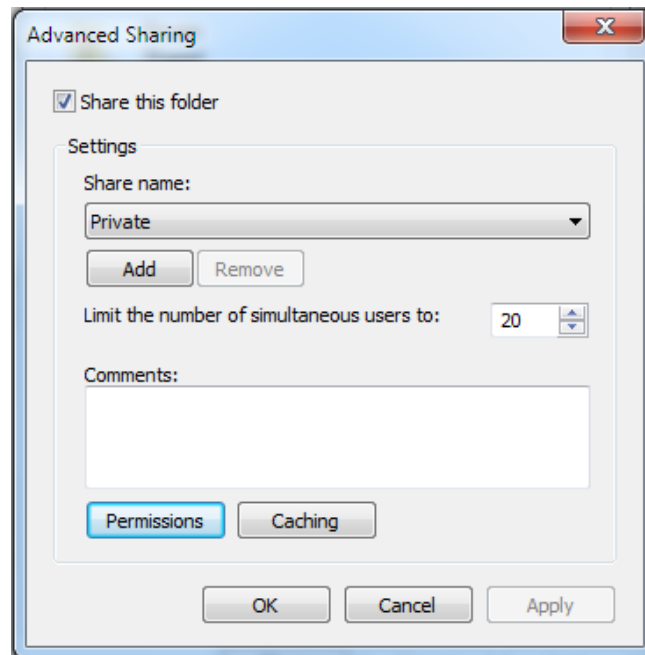


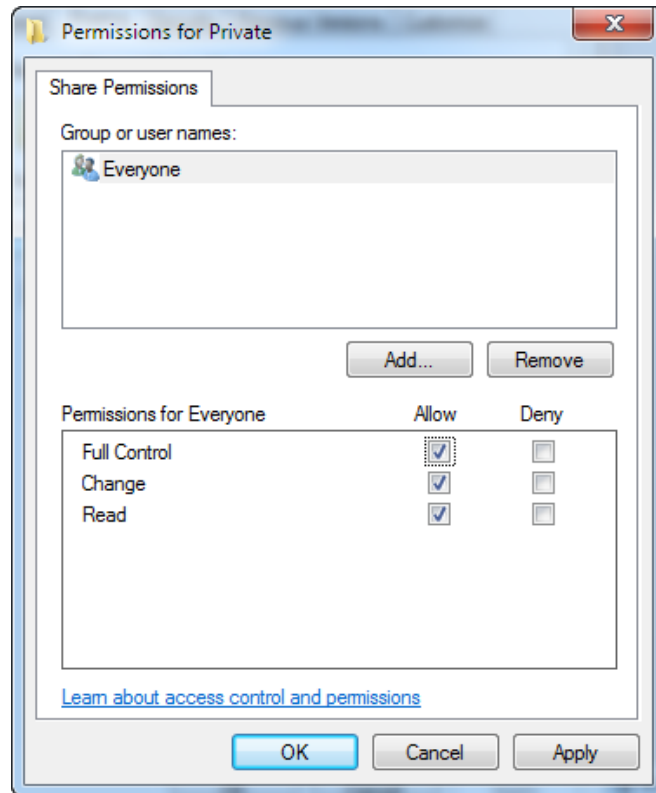
The difference between private directory and public directory is that each folder in private

directory can only be read and written by one user (the owner); while the folders in public directory can be read by all connecting users (if **Write**, **Upload** or **Download** are not selected).



The directory configured here can be configured as a shared folder on remote server. You can configure folder permission on remote server, as shown below:





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



For how to apply remote storage server, refer to Cloud Storage section when Adding/Editing Policy set in Chapter 4.

Chapter 5 System Maintenance

The **Maintenance** module covers the following four parts: **System Update**, **Logs**, **Backup/Restore**, and **Restart/Shutdown**.

Backing Up/Restoring Configurations

Navigate to **Maintenance > Backup/Restore** to backup or restore the system configurations and SSL VPN configurations on the **System Config** and **SSL VPN Config** pages respectively, as shown below:

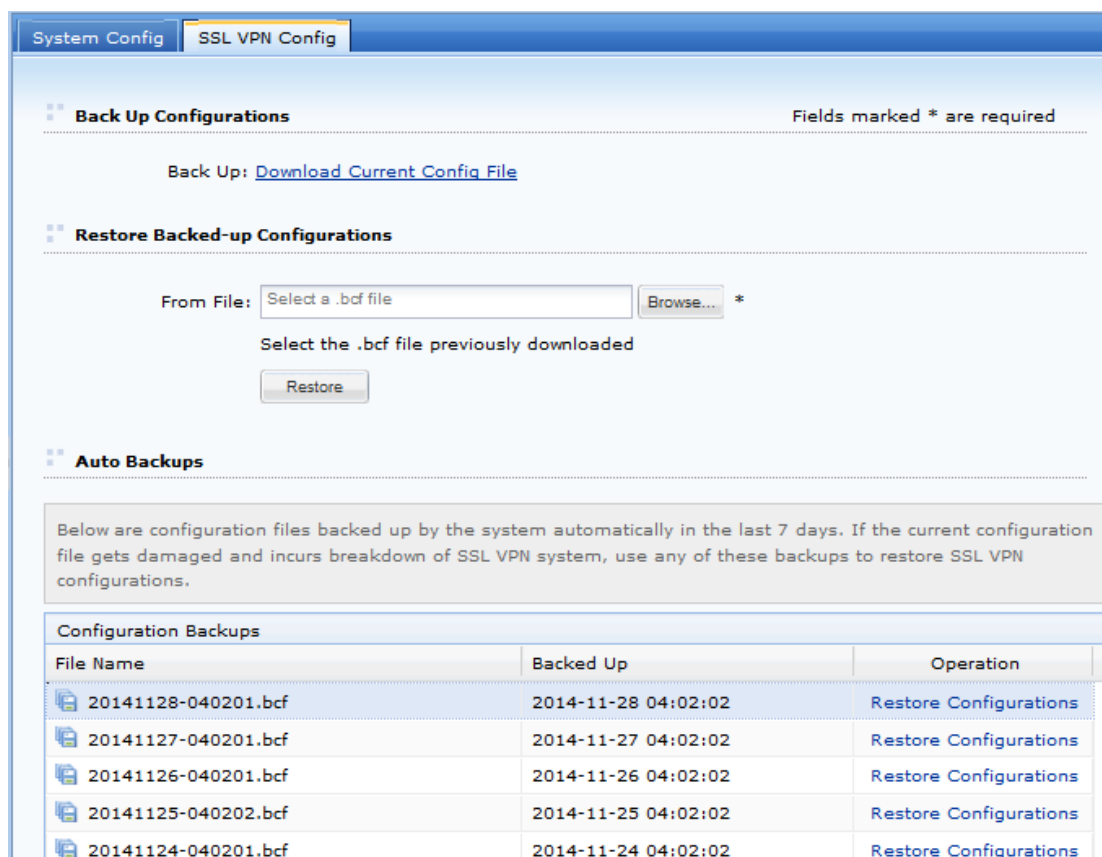
The screenshot shows a web interface with two tabs: "System Config" and "SSL VPN Config". The "System Config" tab is active. The page is titled "Back Up Configurations" and contains three main sections:

- Back Up:** A link labeled "Download Current Config File".
- Restore Backed-up Configurations:** A form with a "From File:" label, a text input field containing "Select a .bcf file", a "Browse..." button, and an asterisk. Below the input field is the instruction "Select the .bcf file previously downloaded" and a "Restore" button.
- Prompt Backing Up Configurations:** A text box containing the instruction: "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." Below this text box is a checkbox labeled "Prompt admin at logon if backup has not been conducted for some time" and a "Duration:" label with a text input field containing "10" and the word "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:



The screenshot shows the 'SSL VPN Config' page with three main sections:

- Back Up Configurations:** Includes a link for 'Download Current Config File'.
- Restore Backed-up Configurations:** Features a 'From File:' field with a 'Browse...' button and a 'Restore' button. A note states: 'Select the .bcf file previously downloaded'.
- Auto Backups:** Contains a text box explaining that the following table shows configuration files backed up automatically in the last 7 days. Below this is a table titled 'Configuration Backups'.

File Name	Backed Up	Operation
 20141128-040201.bcf	2014-11-28 04:02:02	Restore Configurations
 20141127-040201.bcf	2014-11-27 04:02:02	Restore Configurations
 20141126-040201.bcf	2014-11-26 04:02:02	Restore Configurations
 20141125-040202.bcf	2014-11-25 04:02:02	Restore Configurations
 20141124-040201.bcf	2014-11-24 04:02:02	Restore Configurations

The following are contents included on the **SSL VPN Config** tab:

- **Download Current Config File:** Click it to save the configurations to the local computer.
- **Browse:** To restore the configurations previously backed up, click it to select the configuration file from the local computer.
- **Restore:** Click it to restore the configurations from the selected file.
- **Auto Backups:** Displays configuration files automatically backed up by the system in the past 7 days. Click **Restore** to restore any of them.



The configurations here only indicate the configurations of the SSL VPN module.

Restarting/Shutting Down Device or Services

The **Restart/Shutdown** page allows you to shut down/restart the Sangfor device, restart all the

services and stop/start the SSL VPN service.

Navigate to **Maintenance > Restart/Shutdown** to enter the **Restart/Shutdown** page, as shown below:



- **Shut Down Device:** To stop all the running services, save current configurations and shut down the Sangfor device.
- **Restart Device:** To shut down and restart the Sangfor device.
- **Restart Service:** To terminate all the sessions, release system resources and restart system services.
- **Stop SSL VPN Service:** To stop the SSL VPN service.
- **About SSL VPN:** To show SSL VPN version information and configure update options.



Chapter 6 Scenarios

Device Deployment

Sangfor device can work in two modes, **Single-Arm** mode and **Gateway** mode. You can configure device deployment mode under **System > Network > Deployment**.

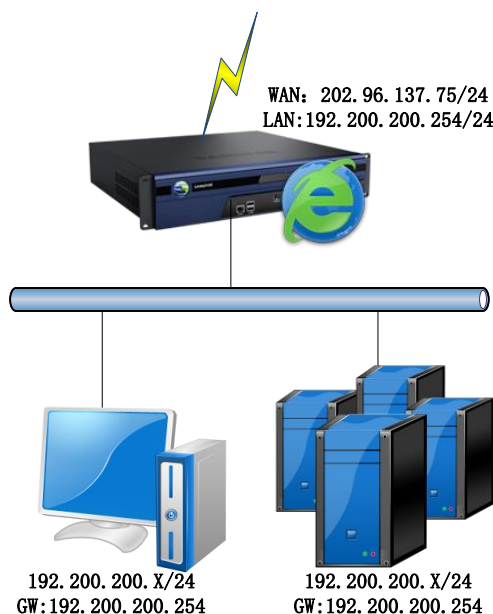
Deploying Device in Gateway Mode with Single Line

Background:

- One network segment of a local area network is 192.200.200.0/24
- A Sangfor device is to be deployed in Gateway mode
- External network is an Ethernet network; the IP address assigned by the Internet server operator is 202.96.137.75.

Perform the following steps:

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



2. Log into administrator console and navigate to **System > Network > Deployment** page, and select **Gateway** as the deployment mode, configure LAN interface, as shown in the figure below:

Deployment Multiline Options Routes Hosts DHCP Local Subnets

Deployment Fields marked * are required

Mode: Single-Arm Gateway

WAN and LAN interfaces need to be configured.

Internal Interfaces

LAN:		DMZ:	
IP Address:	192.200.200.254 *	IP Address:	10.10.2.88 *
Netmask:	255.255.255.0 *	Netmask:	255.255.255.0 *

Multi-IP

3. Configure WAN interface and corresponding line, as shown below:

Edit Line

Enable this line

Line Type: Ethernet PPPoE

Ethernet Settings

Obtain IP and DNS server using DHCP

Use the IP address and DNS server below

IP Address:	202.96.137.75 ✕	Preferred DNS:	202.96.134.133
Netmask:	255.255.255.0	Alternate DNS:	202.96.128.166
Default Gateway:	202.96.137.1	MTU:	1500

Multi-IP

Advanced

Save Cancel

Deployment Multiline Options Routes Hosts DHCP Local Subnets

Deployment Fields marked * are required

Mode: Single-Arm Gateway

WAN and LAN interfaces need to be configured.

Internal Interfaces

<p>LAN:</p> <p>IP Address: <input type="text" value="192.200.200.254"/> *</p> <p>Netmask: <input type="text" value="255.255.255.0"/> *</p> <p style="text-align: center;"><input type="button" value="Multi-IP"/></p>	<p>DMZ:</p> <p>IP Address: <input type="text" value="10.10.2.88"/> *</p> <p>Netmask: <input type="text" value="255.255.255.0"/> *</p>
--	--

External Interfaces (WAN Interfaces)

Line	Type	IP Address	Netmask	Default Gateway	Status
Line 1	Ethernet	202.96.137.75	255.255.255.0	202.96.137.1	Enabled

4. Go to **Firewall > NAT > SNAT Rule** to enter the **SNAT Rule** page and click **Add** to enter **Edit SNAT Rule** page, as shown below:

Name: x

Original Data Packet

Source Subnet

From Interface: v

Subnet:

Netmask:

Destination

To Interface: v

Line: v

Subnet:

Netmask:

Prompt: If IP address and netmask are 0.0.0.0, it means all IP addresses.

Translated To

Interface IP

Specified IP

Enable rule Firewall will let matching packets pass

SNAT Rule							
Status	Name	From Interface	Source Subnet	To Interface	Destination	Translated To	Operation
Enabled	SNAT	LAN	192.200.200.0/255.255.255.0	WAN	All IP	Interface IP	Copy Edit Delete

- Click **Save** button to save the settings and restart the Sangfor device.

Deploying Device in Gateway Mode with Multiple Lines

Background:

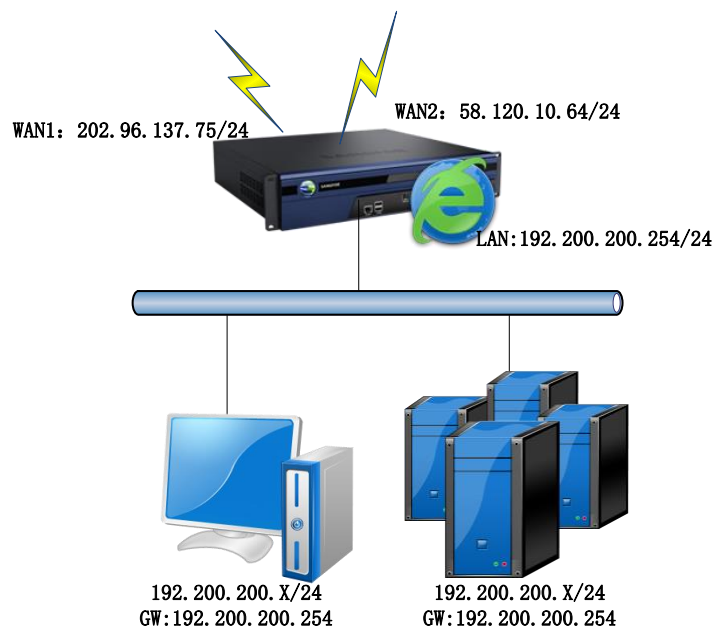
- One network segment of a local area network is 192.200.200.0/24
- A Sangfor device is to be deployed in Gateway mode
- There are two WAN lines: Telecom and Unicom.

Purpose:

User on business can connect to SSL VPN through the one of the two WAN lines, which has better performance.

Perform the following steps:

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



- Log into administrator console and navigate to **System > Network > Deployment** page, and select **Gateway** as the deployment mode, configure LAN interface, as shown in the figure

below:

The screenshot shows the 'Deployment' tab of the configuration interface. It includes a 'Mode' section with radio buttons for 'Single-Arm' and 'Gateway' (selected). A message box states 'WAN and LAN interfaces need to be configured.' Below this is the 'Internal Interfaces' section, which is divided into 'LAN' and 'DMZ' settings. The LAN section has input fields for IP Address (192.200.200.254) and Netmask (255.255.255.0), both marked with an asterisk, and a 'Multi-IP' button. The DMZ section has input fields for IP Address (10.10.2.88) and Netmask (255.255.255.0), also marked with an asterisk.

3. Configure WAN interface and corresponding line, as shown below:

The 'Edit Line' dialog box shows the configuration for a WAN interface. It has a checkbox for 'Enable this line' which is checked. The 'Line Type' is set to 'Ethernet' (selected) and 'PPPoE'. Under 'Ethernet Settings', the option 'Use the IP address and DNS server below' is selected. The configuration fields are: IP Address (202.96.137.75), Preferred DNS (202.96.134.133), Netmask (255.255.255.0), Alternate DNS (202.96.128.168), Default Gateway (202.96.137.1), and MTU (1500). There are 'Multi-IP' and 'Advanced' buttons at the bottom of the settings area, and 'Save' and 'Cancel' buttons at the bottom of the dialog.

Edit Line

Enable this line

Line Type: Ethernet PPPoE

Ethernet Settings

Obtain IP and DNS server using DHCP

Use the IP address and DNS server below

IP Address: Preferred DNS:

Netmask: Alternate DNS:

Default Gateway: MTU:

Deployment | Multiline Options | Routes | Hosts | DHCP | Local Subnets

Deployment Fields marked * are required

Mode: Single-Arm Gateway

WAN and LAN interfaces need to be configured.

Internal Interfaces

LAN:

IP Address: *

Netmask: *

DMZ:

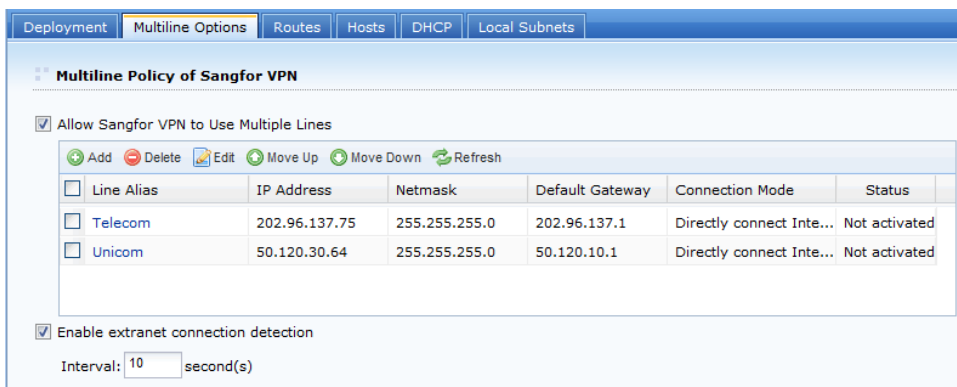
IP Address: *

Netmask: *

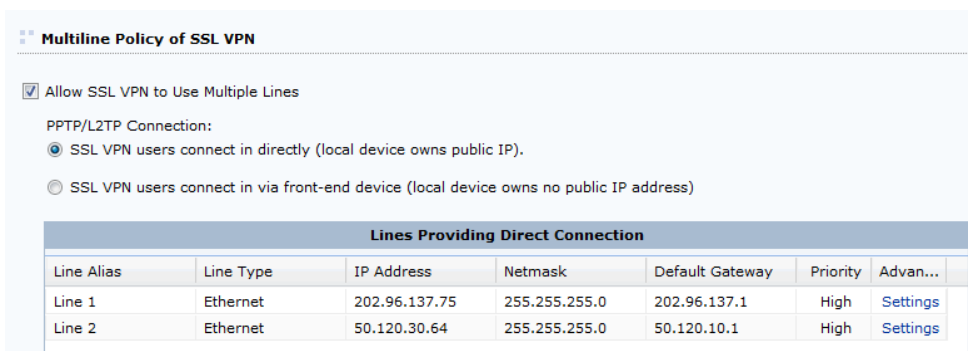
External Interfaces (WAN Interfaces)

Line	Type	IP Address	Netmask	Default Gateway	Status
Line 1	Ethernet	202.96.137.75	255.255.255.0	202.96.137.1	Enabled
Line 2	Ethernet	58.120.10.64	255.255.255.0	58.120.10.1	Enabled

4. Go to **System > Network > Multiline Options** page and select the **Allow Sangfor VPN to Use Multiple Lines** option and add two Internet lines: Telecom and Unicom, as shown in the figure below:



Select the **Allow SSL VPN to Use Multiple Lines** and **SSL VPN users connects in directly** Options under **Multiline Policy of SSL VPN** section, as shown below:



5. Navigate to **Firewall > NAT > SNAT Rule** and click **Add** to enter the **Edit SNAT Rule** page and configure required fields according to your need, as shown below:

Name: x

Original Data Packet

Source Subnet

From Interface:

Subnet:

Netmask:

Destination

To Interface:

Line:

Subnet:

Netmask:

Prompt: If IP address and netmask are 0.0.0.0, it means all IP addresses.

Translated To

Interface IP

Specified IP

Enable rule Firewall will let matching packets pass

>> SNAT Rule Tips

+ Add

Status	Name	From Interface	Source Subnet	To Interface	Destination	Translated To	Operation
Enabled	SNAT	LAN	192.200.200.0/255.255.255.0	WAN	All IP	Interface IP	Copy Edit Delete

- Click **Save** to save all the changes and restart Sangfor device.



The option **Allow Sangfor VPN to Use Multiple Lines** needs to be selected only when Sangfor device is deployed in gateway mode with multiple lines and connected to Internet directly.

Deploying Device in Single-Arm Mode With Single Line

Background:

- One network segment of a local area network is 192.200.200.0/24

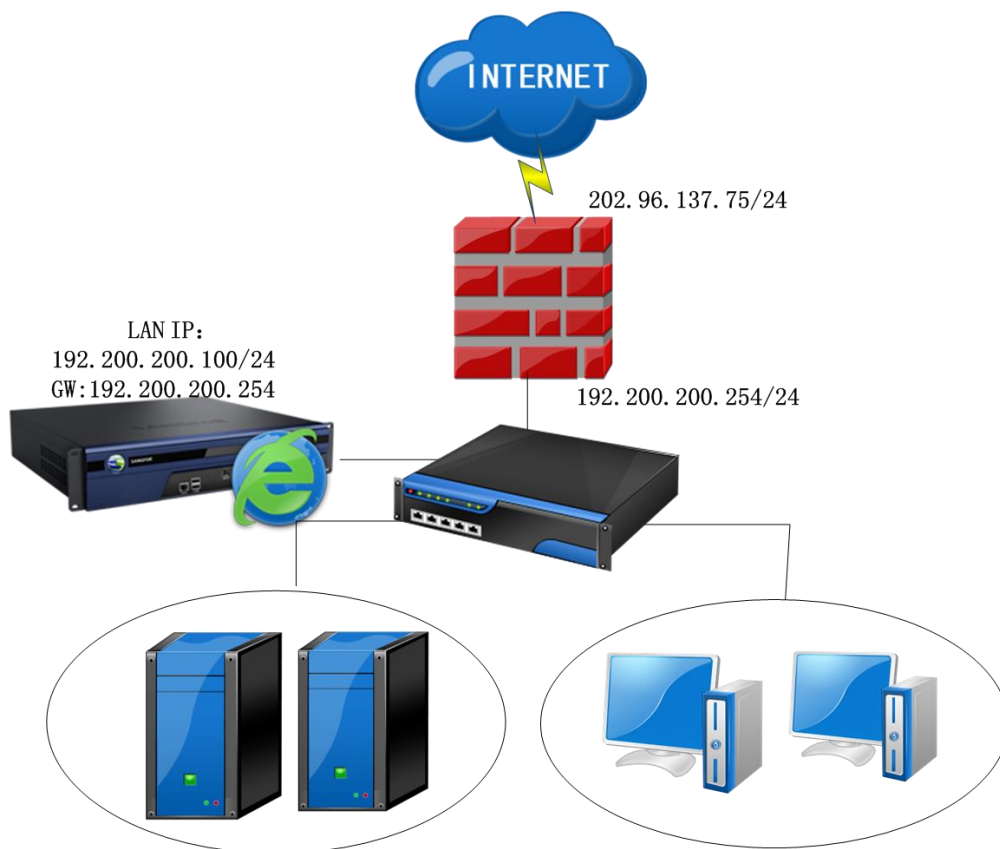
- A Sangfor device is to be deployed in the local area network, in Single-arm mode
- The front-end firewall is connected to external network through an Internet line

Purpose:

Users on business can access internal resources through SSL VPN.

Perform the following steps:

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



2. Go to **System > Network > Deployment** page and select Single-Arm as deployment mode, and configure the network interfaces of the device as well, as shown below:

Deployment | Multiline Options | Routes | Hosts | DHCP | Local Subnets

Deployment Fields marked * are required

Mode: Single-Arm Gateway

The device connects to Internet via front-end device.

Internal Interfaces

LAN:		DMZ:	
IP Address:	<input type="text" value="192.200.200.100"/> *	IP Address:	<input type="text" value="10.10.2.80"/> *
Netmask:	<input type="text" value="255.255.255.0"/> *	Netmask:	<input type="text" value="255.255.255.0"/> *
Default Gateway:	<input type="text" value="192.200.200.254"/> *		
Preferred DNS:	<input type="text" value="8.8.8.8"/> *		
Alternate DNS:	<input type="text"/>		

3. Click the **Save** button to save the settings and restart the Sangfor device.
4. Configure the front-end firewall, and make sure that the corresponding ports (443 by default) of the front-end firewall are mapped to those on the Sangfor device.



- Port 443 is the listening port of Sangfor device by default. It can be modified. If it is modified, corresponding port of the front-end firewall needs to be mapped to the modified listening port.
- LAN interface of Sangfor device in single arm mode should be connected to internal switch.

Deploying Device in Single-Arm Mode With Multiple Lines

Background:

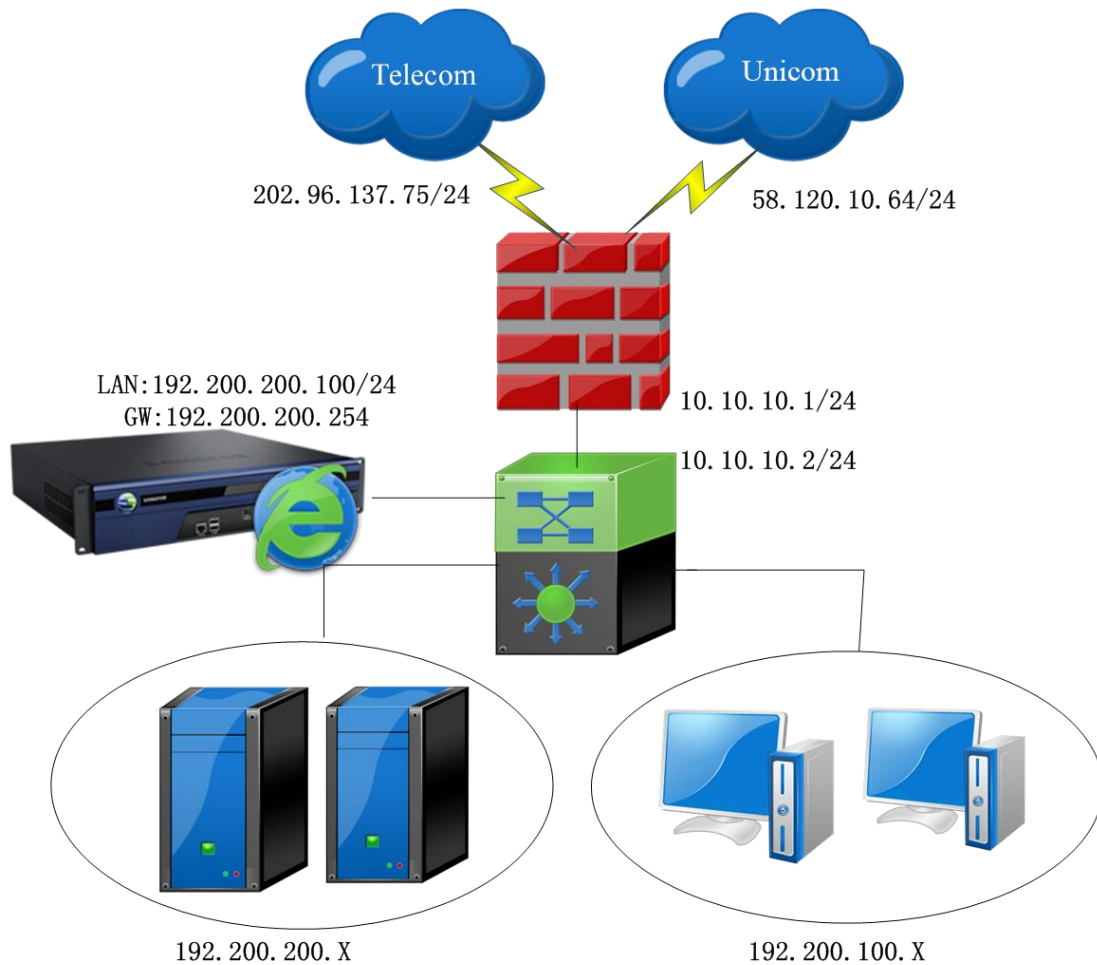
- There are two Internet lines connected to front-end firewall device: Telecom and Unicom
- A Sangfor device is to be deployed in the local area network, in Single-arm mode

Purpose:

User can connect to SSL VPN by typing into 202.96.137.75 or 58.120.10.64 in **Address** field on VPN client.

Perform the following steps:

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



2. Go to **System > Network > Deployment** page and select Single-Arm as deployment mode, and configure the network interfaces of the device as well, as shown below:

Deployment	Multiline Options	Routes	Hosts	DHCP	Local Subnets
Deployment Fields marked * are required					
Mode: <input checked="" type="radio"/> Single-Arm <input type="radio"/> Gateway					
The device connects to Internet via front-end device.					
Internal Interfaces					
LAN:			DMZ:		
IP Address:	192.200.200.100	*	IP Address:	10.10.2.80	*
Netmask:	255.255.255.0	*	Netmask:	255.255.255.0	*
Default Gateway:	192.200.200.254	*			
Preferred DNS:	0.0.0.0	*			
Alternate DNS:					
	<input type="button" value="Multi-IP"/>				

3. Go to **System > Network > Multiline Options** page to select the **Allow SSL VPN to use Multiple lines** option and add two Internet lines for SSL VPN, as shown below:

Add Line for SSL VPN

Configure lines and mappings of the front-end device

Line IP/Domain: 202.96.137.75 *

Priority: High

HTTP port: 80 *

HTTPS port: 443 *
Line is mapped from it to SSL VPN HTTPS port

Save Cancel

Add Line for SSL VPN

Configure lines and mappings of the front-end device

Line IP/Domain: 58.120.10.64 *

Priority: High

HTTP port: 80 *

HTTPS port: 443 *
Line is mapped from it to SSL VPN HTTPS port

Save Cancel

Multiline Policy of SSL VPN

Allow SSL VPN to Use Multiple Lines

PPTP/L2TP Connection:

SSL VPN users connect in directly (local device owns public IP).

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

Lines Of Front-End Device

+ Add - Delete Edit

IP/Domain	HTTP port	HTTPS port	Priority
202.96.137.75	80	443	High
58.120.10.64	80	443	High

4. Configure the front-end firewall again, so that the two ports (TCP 80 and 443) of the public

network IP addresses (of the two Internet lines) can be mapped to the Sangfor device.

5. Click **Save** button to save the changes and restart Sangfor device.



When Sangfor device is deployed in single-arm mode, HTTPS port and HTTP port must be mapped to the Sangfor device; otherwise, multiline selection policy will not work.

Configuring System Route

Background:

- Two network segments of a local area network are 192.200.200.X and 192.200.254.X. Users in these two subnet communicate through layer 3 switch
- Sangfor device is to be deployed in the local area network, in gateway mode

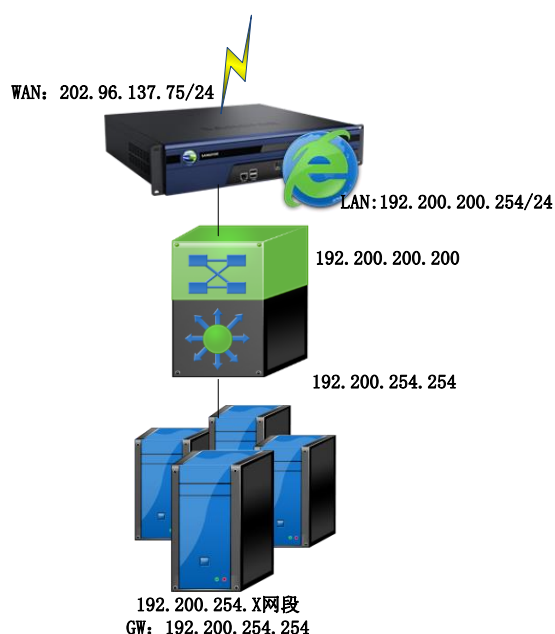
Purpose:

Users on the subnet 192.200.254.x can access Internet through Sangfor device

As 192.200.254.X and 192.200.200.254 on which LAN interface of Sangfor device resides are not on the same network segment, a system route is required to be configured on Sangfor device.

Perform the following steps:

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



2. Configure SNAT rule on **Firewall > NAT > SNAT Rule** page, as shown below:

Name: SNAT

Original Data Packet

Source Subnet

From Interface: LAN

Subnet: 192.200.200.0

Netmask: 255.255.255.0

Destination

To Interface: WAN

Line: All lines

Subnet: 0.0.0.0

Netmask: 0.0.0.0

Prompt: If IP address and netmask are 0.0.0.0, it means all IP addresses.

Translated To

Interface IP

Specified IP

Enable rule Firewall will let matching packets pass

Save Cancel

3. Go to **System > Network > Routes** page to add a route directing to 192.200.254.X, as shown below:

Add Route

Please fill in the correct route information.

Dst IP: 192.200.254.0 *

Netmask: 255.255.255.0 *

Gateway: 192.200.200.200 *

Save and Add Save Cancel

Adding User

Adding User Logging in with Local Password

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

The screenshot shows the 'Add User' configuration page. The 'Basic Attributes' section includes fields for Name (www), Description, Password (masked), Confirm (masked), Mobile Number, and Added To. There are also checkboxes for inheriting attributes, policy set, and authentication settings. The 'Authentication Settings' section shows 'User Type' set to 'Private user' and 'Local password' selected as the primary authentication method. Other options like 'Certificate/USB key', 'Hardware ID', and 'SMS password based' are unselected. The 'Status' is set to 'Enabled'.

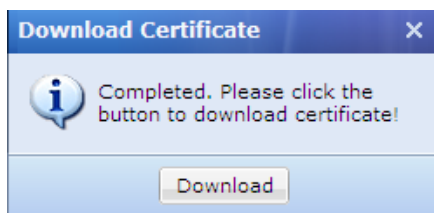
4. Click the **Save** button and **Apply** button to save and apply the settings.

Adding User Logging in with Certificate

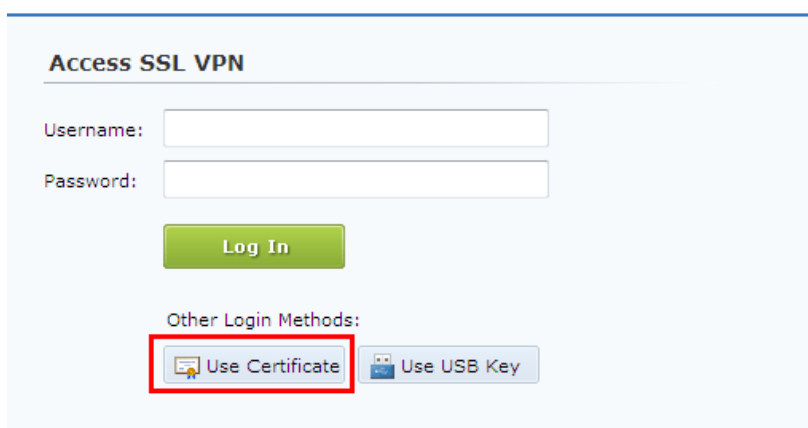
1. Navigate to **SSL VPN > Authentication** to download and install the USB key driver and USB key tool (for importing USB key).
2. Navigate to **SSL VPN > Users > Local Users** and click **Add > User** to add a new user, as shown in the figure below:

3. Configure **Name** and **Local Password** fields. Select user type **Private user**.
4. Configure **Authentication Settings**. Select primary authentication **Certificate/USB key**.
5. Click the **Generate Certificate** button to enter the **Generate Certificate** page and generate certificate for this user, as shown in the figure below:

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



7. Click **Download** to save the certificate file **support.p12** to the computer and send it to the end user.
8. End user installs the certificate on his/her computer, visit the login page and select **Use Certificate** login method to connect to SSL VPN, as shown in the figure below:



Configuring VPN Resource

Adding Web Application

Background:

One DNS server and four servers deployed in the enterprise network are providing services for employees:

- ***http://oa.123.com***: an OA system. Server address is 192.168.1.10. The employees mainly work via this platform.
- ***http://bbs***: a website where employees can communicate online. Server address is 192.168.1.11.
- ***http://mail.123.com***: a mail system of the company. Server address is 192.168.1.12.
- ***ftp://ftp.123.com***: a file sharing system of the company. Server address is 192.168.1.13.

Purpose:

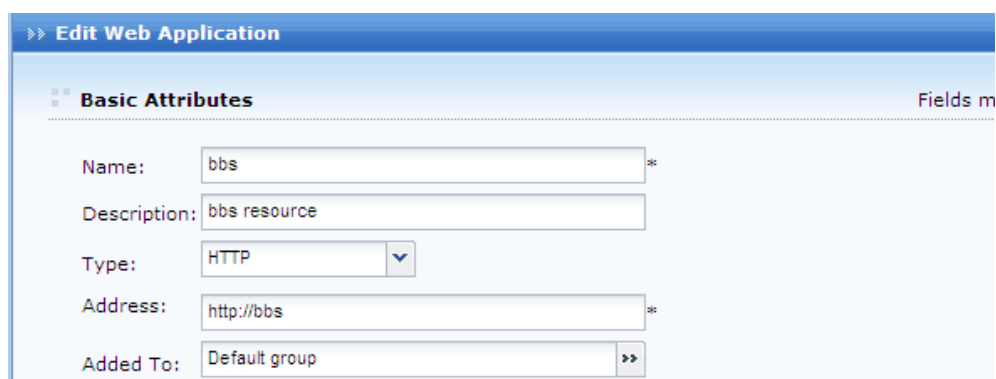
Enable employees to access these resources over SSL VPN, but no add-on needs to be installed.

Analysis and solution:

OA system is a JSP-based system. Interactions among units of an OA system are complicated and many scripts and controls need to be invoked. Because of the complexity, defining OA system as Web application is not a wise choice, but TCP application and L3VPN are good choices for it. For the other three resources, they can be defined as Web application because they are static.

To achieve the expected purposes:

1. Navigate to **SSL VPN > Resources**, add a TCP resource named **OA System** (address is ***http://oa.123.com***) and associate it with the with the user accounts of the employees (to configure TCP application, please refer to the Adding/Editing TCP Application section in Chapter 4).
2. Navigate to **SSL VPN > Resources**, add a Web resource named **bbs** (address is ***http://bbs***) and associate it with the employees.
 - a. On the **Resources** page, click **Add > Web app** to enter the **Edit Web Application** page, as shown in the figure below:



The screenshot shows the 'Edit Web Application' interface. The 'Basic Attributes' section contains the following fields:

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

The screenshot shows the 'Edit Web Application' interface. The 'Basic Attributes' section is expanded, showing the following fields:

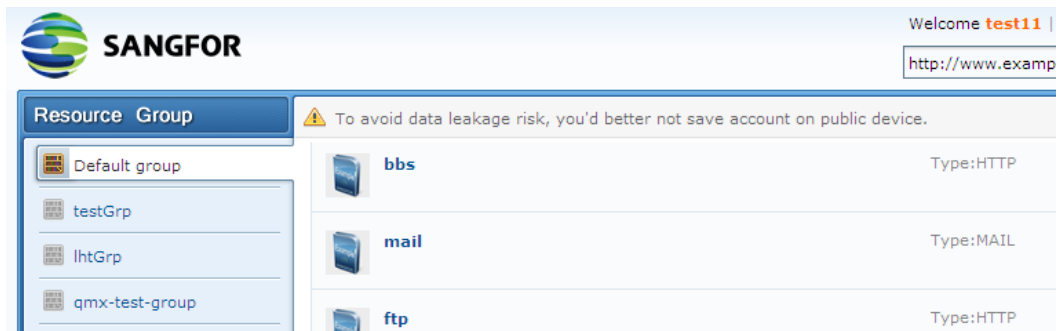
- Name:** mail
- Description:** mail resource
- Type:** MAIL (selected from a dropdown menu)
- Address:** 192.168.1.12
- SMTP Port:** 25
- IMAP Port:** 143
- Domain Name:** http://mail.123.com
- Added To:** Default group

- 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:

The screenshot shows the 'Edit Web Application' interface for an FTP resource. The 'Basic Attributes' section is expanded, showing the following fields:

- Name:** ftp
- Description:** (empty)
- Type:** FTP (selected from a dropdown menu)
- 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 section in Chapter 4.
 6. Click the **Apply** button (on the yellow bar at the top of the page) to apply the settings.
 7. Employees log in to SSL VPN and can visit the resources on the **Resource** page just by clicking on the corresponding resource link, as shown in the figure below:



Masquerading Resource Address

Purpose:

Conceal the IP address of the server that provides resource to users. Resource address masquerading only applies to **HTTP**, **HTTPS**, **MAIL** and **FTP** types of Web resources. Real addresses of **FileShare** type of Web resources are visible to users.

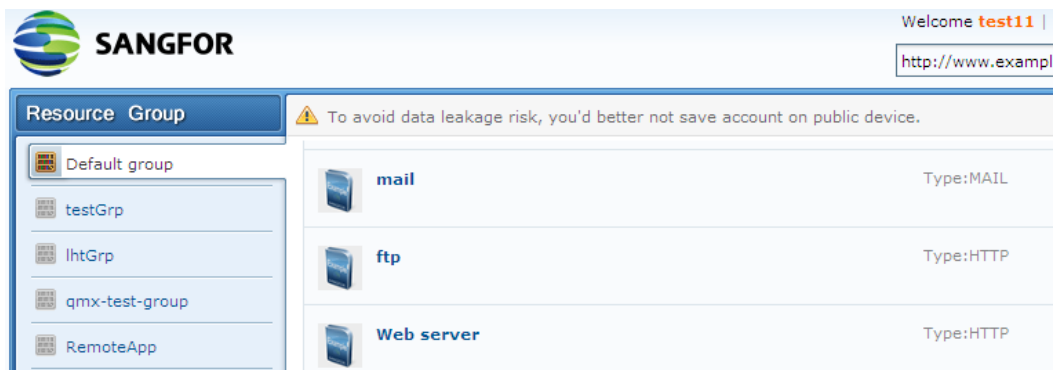
To achieve the expected purposes:

1. Navigate to **SSL VPN > Resources** and click **Add > Web app** to enter the **Edit Web Application** page.
2. Select resource type **HTTP** and enter the resource address (e.g., *http://200.200.72.60*) into **Address** field. Select the **Enable resource address masquerading** option, as shown below:

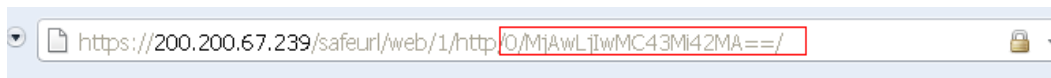
3. Associate the resource with the user. For detailed guide, refer to the Adding Role section in

Chapter 4.

- End user logs in to SSL VPN and enters the **Resource** page. The **Resource** page is as shown in the figure below:



- Click the resource link to access the resource **Web server**. As shown in the figure below, the URL address of the visited resource is not the real address (200.200.72.60) but a meaningless character string.



Adding FileShare Type of Web Application

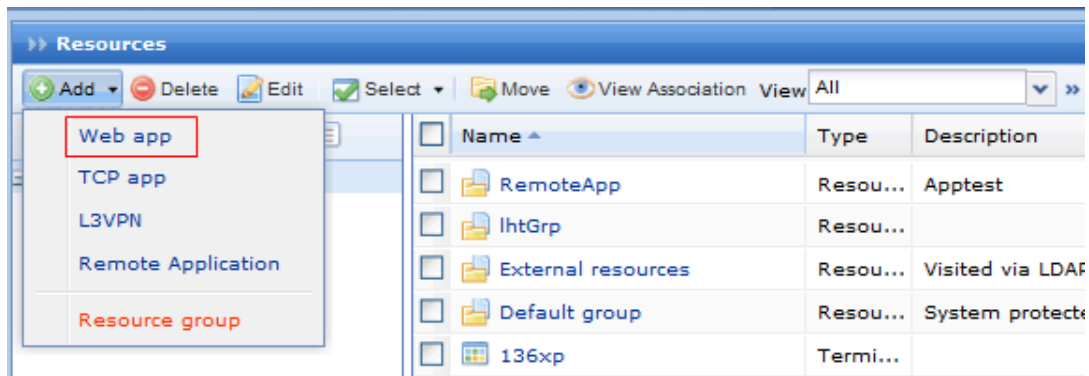
Purposes:

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

To achieve the expected purposes:

- Navigate to **SSL VPN > Users** and click **Add** to create a user account, as shown below:

2. Navigate to **SSL VPN > Resources** and click **Add > Web app** to add a resource, as shown below:

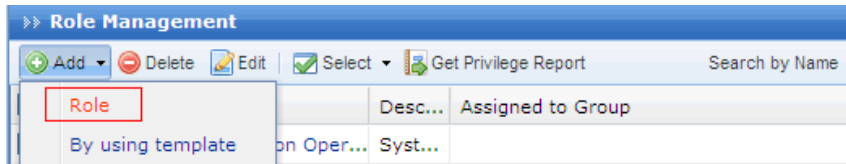


3. On the **Edit Web Application** page, select **FileShare** type of application and configure the other required fields, as shown below:

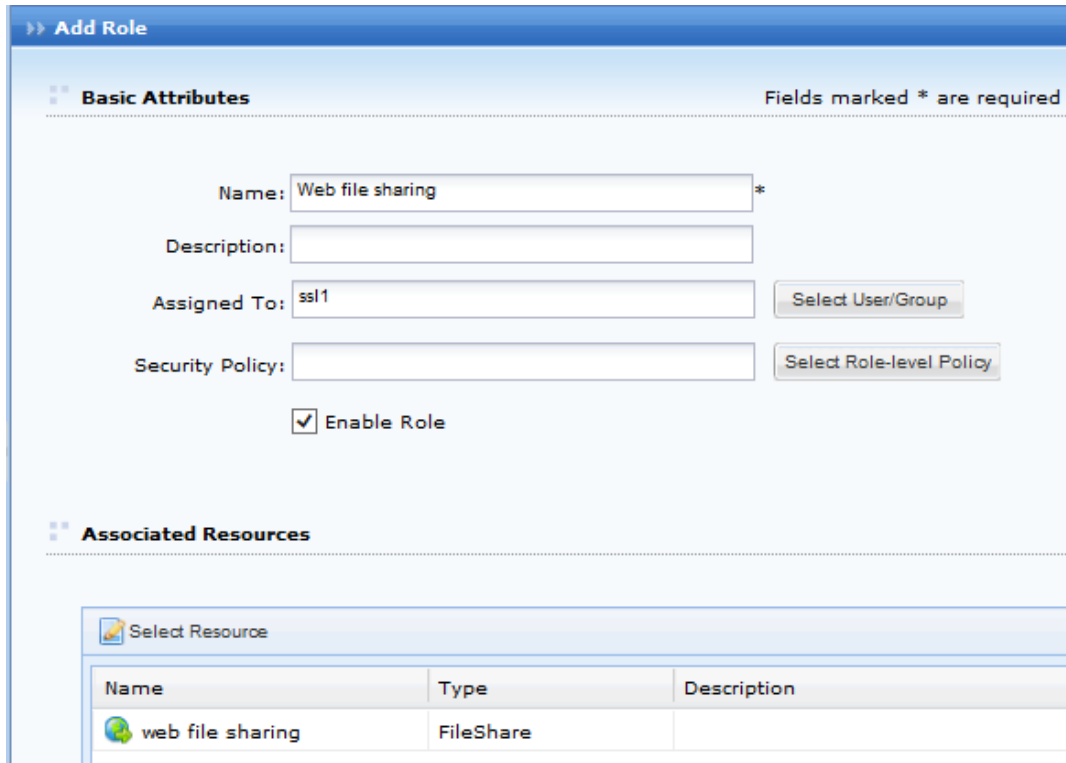
The screenshot shows the 'Edit Web Application' configuration page. The page title is 'Edit Web Application'. Below the title, there is a section 'Basic Attributes' with a note 'Fields marked * are required'. The form contains the following fields and options:

- Name: web file sharing *
- Description: (empty)
- Type: FileShare (dropdown menu)
- Address: 200.200.72.169 *
- Use specified account to login to file server
- server
 - Username: Administrator
 - Password: (masked with dots)
 - Domain: (empty)
- Added To: Default group (dropdown menu)
- Icon: (dropdown menu showing an icon with 'ICO')
- Enable resource
- Visible for user

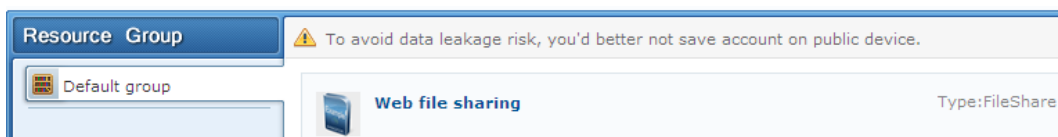
4. On the **Role Management** page, click **Add** to add a role, as shown below:



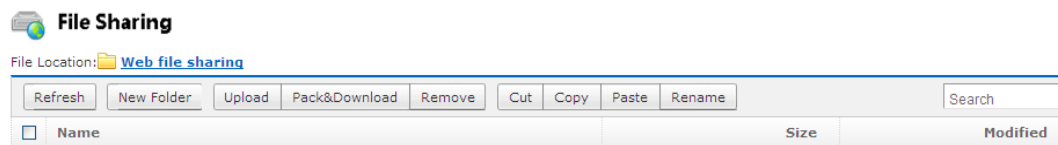
- On the **Add Role** page, select user **ssl1** added in Step 1 and the resource **Web file sharing** to associate the resource with the user.



- 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:



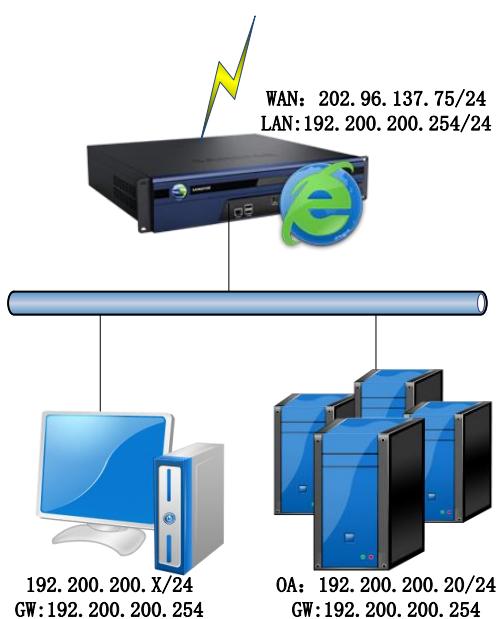
- Click on the resource link and the contents on the Web file sharing server and the available contents will be displayed, as shown in the figure below:



Adding Web Application Enabling Site Mapping

Background:

An OA system is JSP-based system and provides service for employees. Interactions among units of an OA system are complicated and many scripts and controls need to be invoked. Sangfor device is deployed in gateway mode. The network topology of custom network is shown in the figure below:



Purpose:

Enable employees to access OA system over SSL VPN easily.

Analysis and solution:

OA system is a JSP-based system. Interactions among units of an OA system are complicated and many scripts and controls need to be invoked. Except defining OA system as Web application, site mapping feature should be enabled for this Web application.

To achieve the expected purposes:

1. Navigate to **SSL VPN > Resources**, add a Web resource named **OA System** (address is 192.200.200.20), as shown in the figure below:

Edit Web Application

Basic Attributes Fields marked * are required

Name: *

Description:

Type:

Address: *

Added To:

Icon:

Enable resource

Visible for user

Enable resource address masquerading

- Click on **Site Mapping** tab and select **Enabled** to enable site mapping feature. Select VPN Port as **Mode** and enter 8080 in **Port** field. It is recommended to select the **Rewrite webpage contents** option. If it is selected, the webpage containing lots of scripts can be modified and rewrote.

SSO | Authorized Admin | Accounts Binding | URL Access Control | **Site Mapping**

Enabled

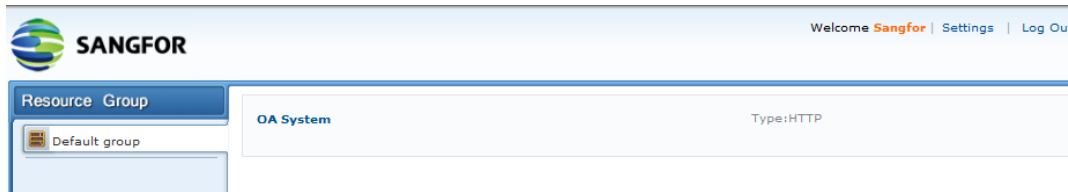
Changing mode or port requires VPN services to restart.

Mode: VPN Port Domain

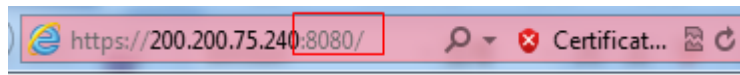
Port:

Rewrite webpage contents

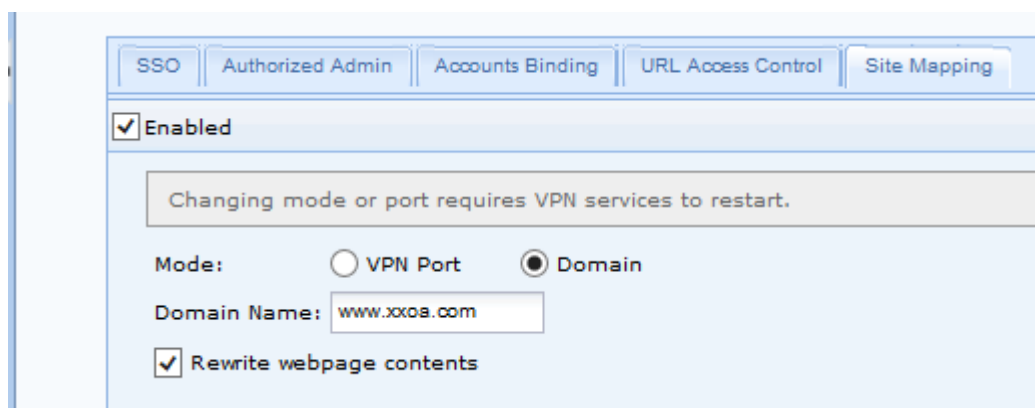
- Navigate to **SSL VPN > Roles** to add a role, assign the role to the user **Sangfor**, and associate it with the resource named **OA System**. For detailed procedure of adding or editing a role, please refer to the Roles section in Chapter 4.
- Click the **Apply** button (on the yellow bar at the top of the page) to apply the settings.
- User **Sangfor** logs in to SSL VPN and can visit the resources on the **Resource** page just by clicking on the corresponding resource link, as shown in the figure below:



6. Click the resource link to access the resource **OA System**. As shown in the figure below, the URL address of the visited resource is not the real address.



If there is a domain name, obtained from ISP, directing to the Sangfor device, you can also select Domain as **Mode**, and enter the domain name into **Domain name** field in step 2, as shown below:



- Resource address masquerading and site mapping which is also called Easylink cannot be enabled together.
- The VPN port mapped to Web application cannot be used by other application.
- The domain name mapped to Web application cannot not be used to connect to SSL VPN. User can connect to SSL VPN by typing the IP address of Sangfor device or other domain name. One domain name can only be mapped to one Web application.
- The Easylink resource mapped to VPN port can be accessed by typing corresponding address into the toolbar of IE browser, while the Easylink resource mapped to domain name cannot be accessed through typing domain name into toolbar.
- In case that Sangfor device is deployed in single-arm mode and port mapping is enabled, Web application is mapped to port 8080 of Sangfor device, corresponding port of front-end firewall needs to be mapped to Sangfor device, except mapping port 443, and access through port 8080 needs to be allowed by firewall.

Configuring TCP Application

Adding TCP Application

Background:

One DNS server and two servers are deployed in the enterprise network, providing services for the employees:

- *http://oa.123.com*: an OA system. Server address is 192.168.1.10.
- Accounting system: Server address is 192.168.1.15 and port is 4003, providing services such as pay rolling, payment claiming, etc.

Purposes:

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

Analysis and solutions:

Both the OA system and Accounting system can be defined as TCP application. Since OA system is a type of system involving immense interactions and some even need links to a number of servers, we need to use the feature **Smart recursion of resource access** (for more details, please refer section [错误!未找到引用源。](#) in Chapter 4).

To achieve the expected purposes:

1. Navigate to **SSL VPN > Resources**. Click **Add > TCP app** to enter **Edit TCP Application** page and add a TCP application (named **OA System**, with address *http://oa.123.com*), as shown below:

The screenshot shows the 'Edit TCP Application' configuration interface. The 'Basic Attributes' section includes the following fields:

- Name:** OA system
- Description:** (empty)
- Type:** HTTP
- Address:** http://oa.123.com/80:80
- Program Path:** (empty) with a 'Browse...' button
- Added To:** Default group

A note below the Program Path field reads: 'Path could be absolute path and environment variable (e.g., %windir%)'.

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: *

Description:

Type: ▼

Address: + - 📄

Program Path:

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

Added To: >>

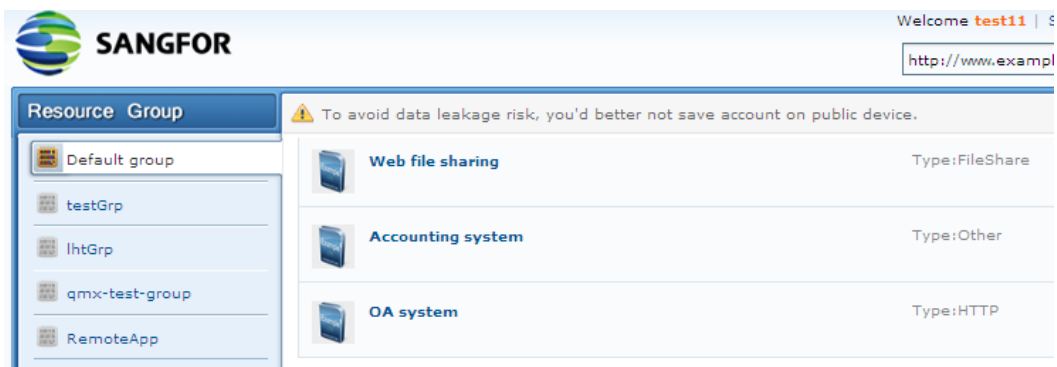
Icon: ▼

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:



OA system could be accessed when the employee clicks on the resource link, or visiting the server through browser.

The accounting system could be accessed directly by clicking the link if program path is specified in step 2. If it is not specified, employee needs to launch the program manually after clicking resource link.

Configuring URL Access Control Feature

Background:

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

Purposes:

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

Analysis and solution:

URL access control feature can achieve control over the access to the file server.

To achieve the expected purposes:

1. Navigate to **SSL VPN > Resources** and add a TCP application (named **URL access control**, URL: *duan.sslt.com*), as shown in the figure below:

The screenshot shows the 'Edit TCP Application' window. Under the 'Basic Attributes' tab, the following fields are present:

- Name:** URL access control *
- Description:** (empty)
- Type:** HTTP
- Address:** duan.sslt.com/80:80

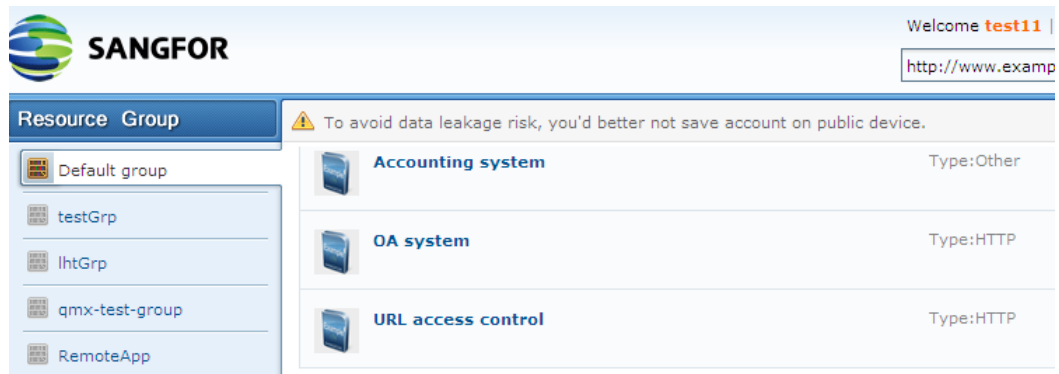
A note at the top right states: 'Fields marked * are required'.

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:

The screenshot shows the 'URL Access Control' configuration page. The 'Enable URL access control' checkbox is checked. The radio button for 'Only allow access to the URLs below' is selected. The 'Add', 'Delete', and 'Edit' buttons are visible. The table below shows the list of URLs:

URL
<input type="checkbox"/> 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:



5. To access the **frame** directory, the employees needs only to click the **URL access control** link. Access to the upper-level directory will be denied.

Adding L3VPN Application

Background:

192.168.1.10-192.168.1.15 is a subnet in the enterprise network.

Purposes:

Enable network administrator to access internal machines on subnet 192.168.1.10-192.168.1.15 over SSL VPN

Analysis and solution:

For network administrator, defining the remote computers as L3VPN resource would allow him/her to access these machines remotely.

To achieve the expected purposes:

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

Basic Attributes Fields marked * are required

Name: *

Description:

Type: Protocol:

Address:

Program Path:

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

Added To:

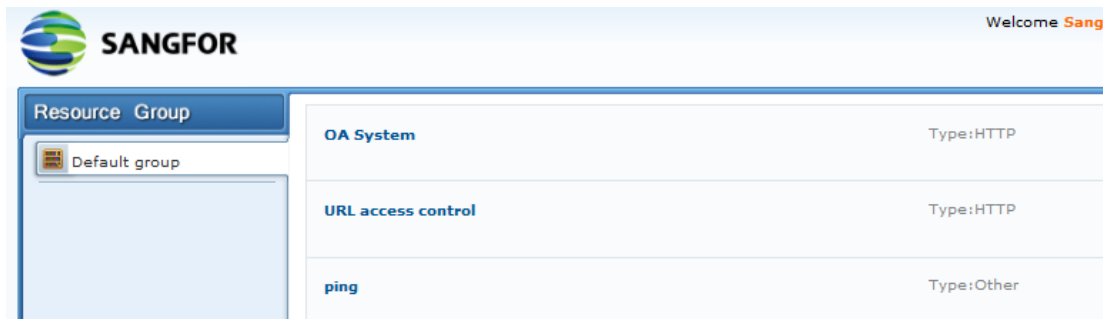
Icon:

Enable resource

Visible for user

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

2. Add or edit a role to associate the resources **ping** with it and assign the role to the network administrator (for detailed guide, refer to the Adding Role section in Chapter 4).
3. Click the **Apply** button to apply the settings.
4. After network administrator logs in to the SSL VPN, he/she will see associated resources, as shown in the figures below:



Network administrator can launch CMD.exe on local PC to ping the connectivity of the computers residing in the network segment 192.168.1.10-192.168.1.1.

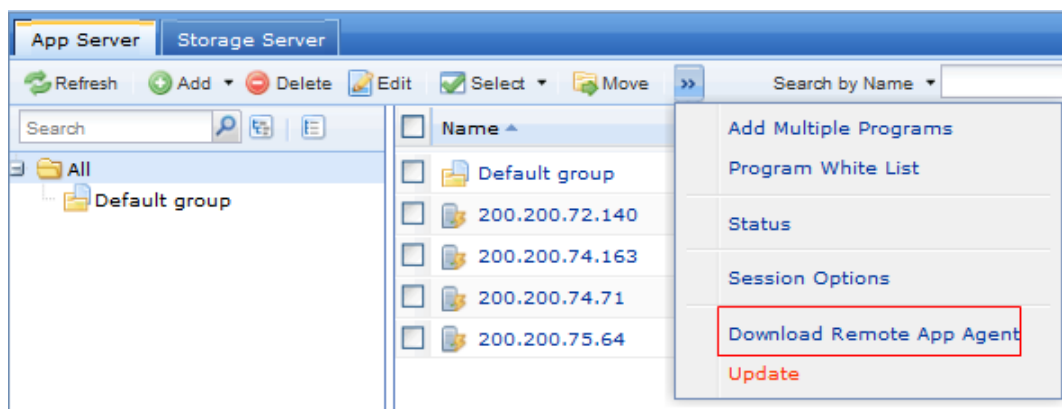
Adding Remote Application

Purposes:

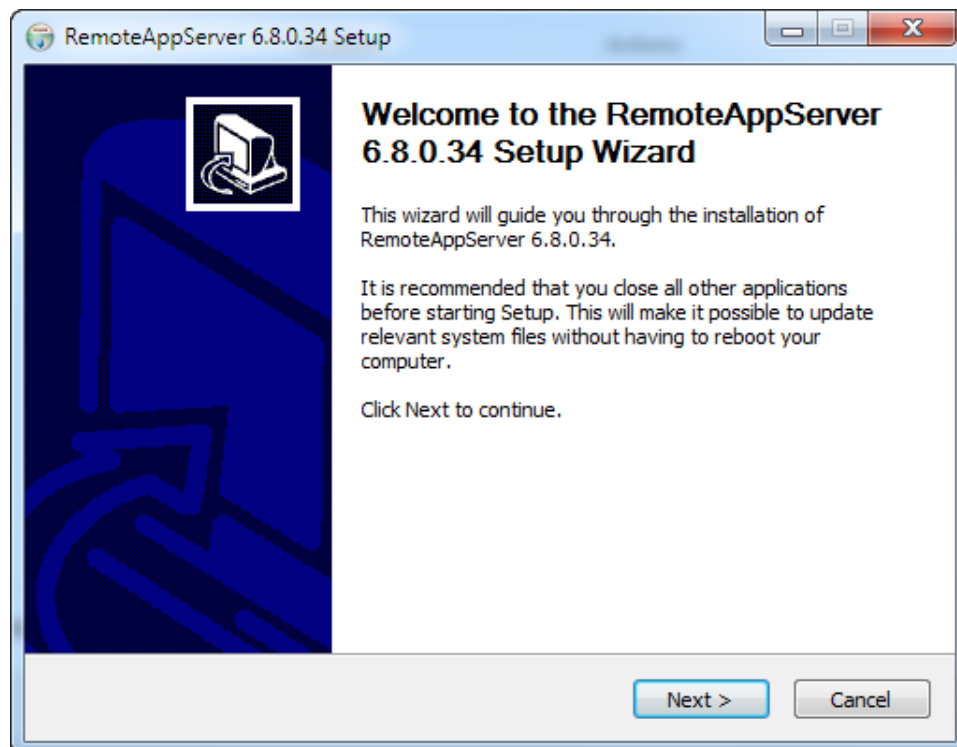
Enable employees to access **WordPad** on the remote application server (IP: 172.16.253.119, port: 7170) and save modified file to private directory or public directory on remote server.

To achieve the expected purpose:

1. Install Terminal Service and RemoteAppAgent program. To download RemoteAppAgent program, navigate to **SSL VPN > Remote Servers** to enter the **App Server** page and click **Download RemoteApp Agent** to download the RemoteApp Agent program, as shown below:

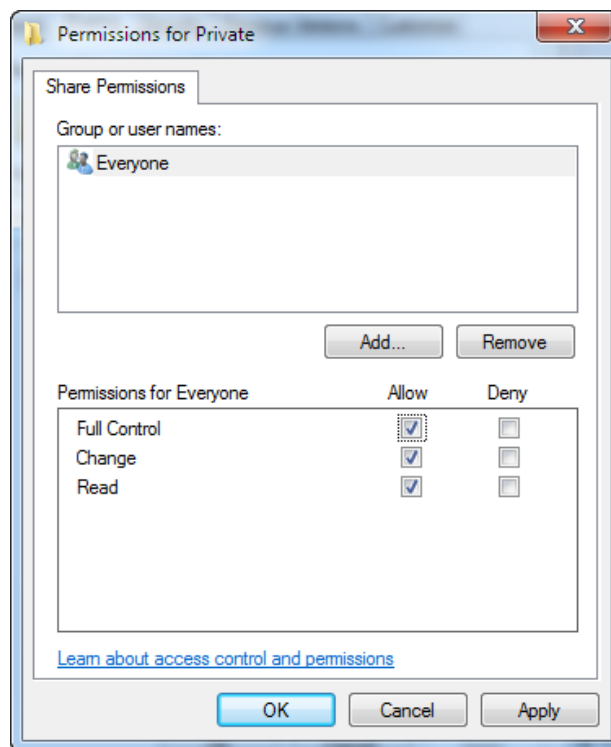
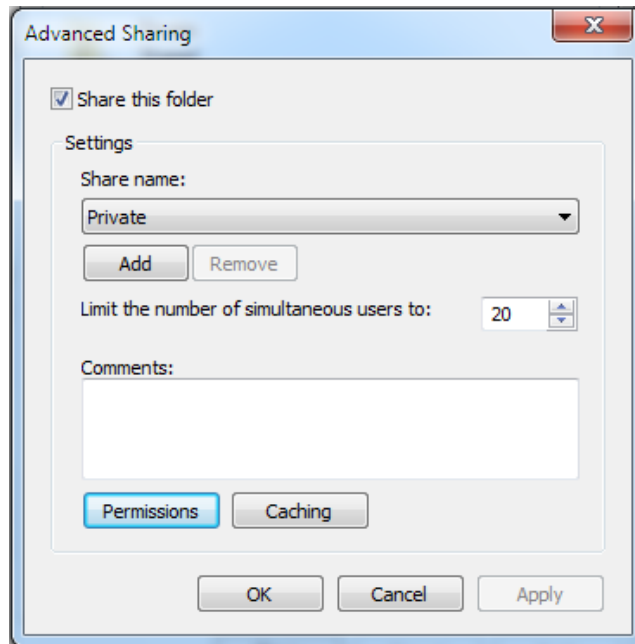


2. Double-click the executable file named **SFRemoteAppServerInstall.exe** and follow the instructions to install the RemoteApp Agent, as show in the figure below:



3. Create private folder and public folder on storage server. The file system format should be

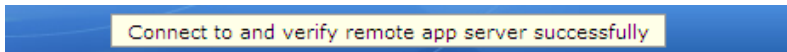
NTFS. Share this private directory and specify user permission for access to this folder.



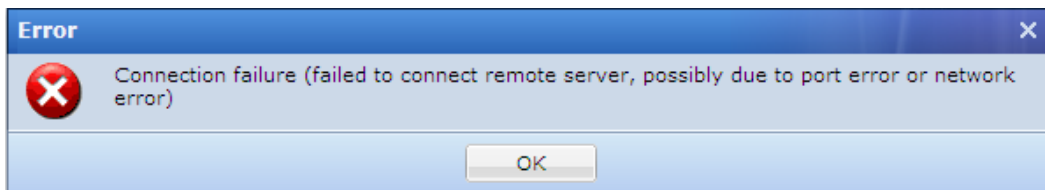
4. Navigate to **SSL VPN > Remote Servers** to enter the **App Server** page and click **Add > Server** to add an application server, as shown below:

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

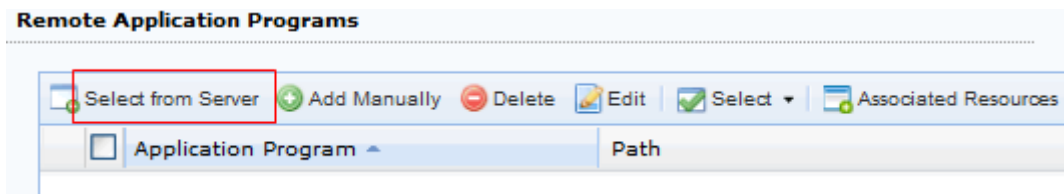
If the following prompt appears, the Sangfor device is then connected to the remote application server successfully.



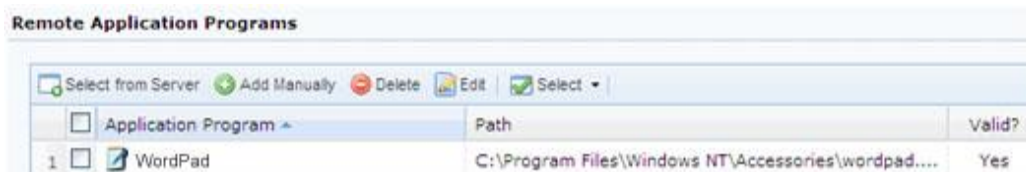
If the following prompt appears, the SSL VPN cannot connect to remote application server. In that case, check whether the remote server is configured properly.



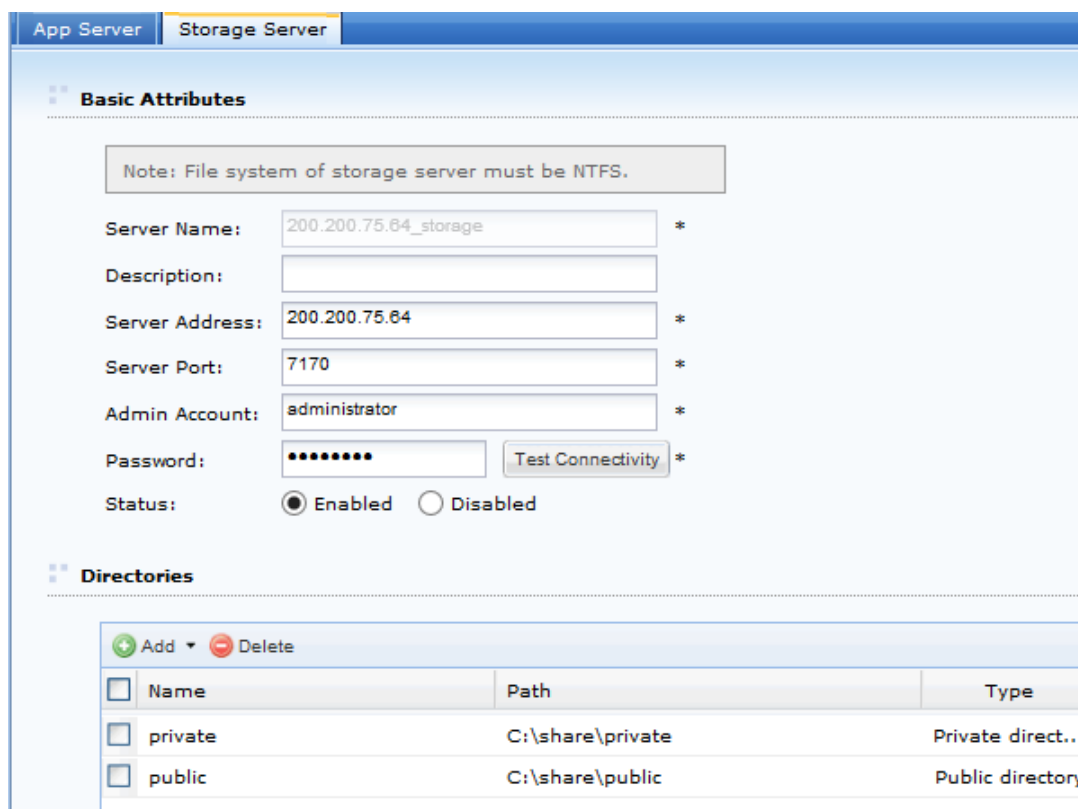
- Under **Remote Application Programs**, click **Select from Sever** to select the application program **WordPad**, as shown in the figure below:



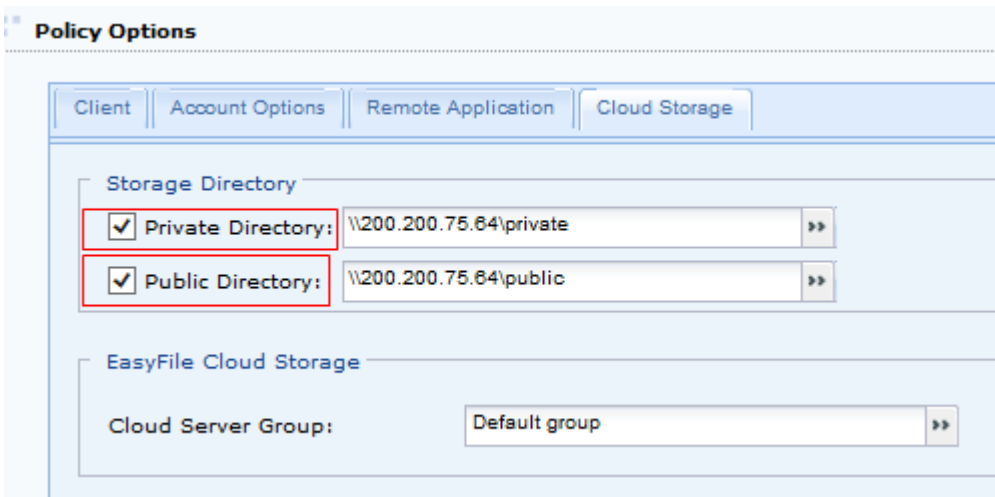
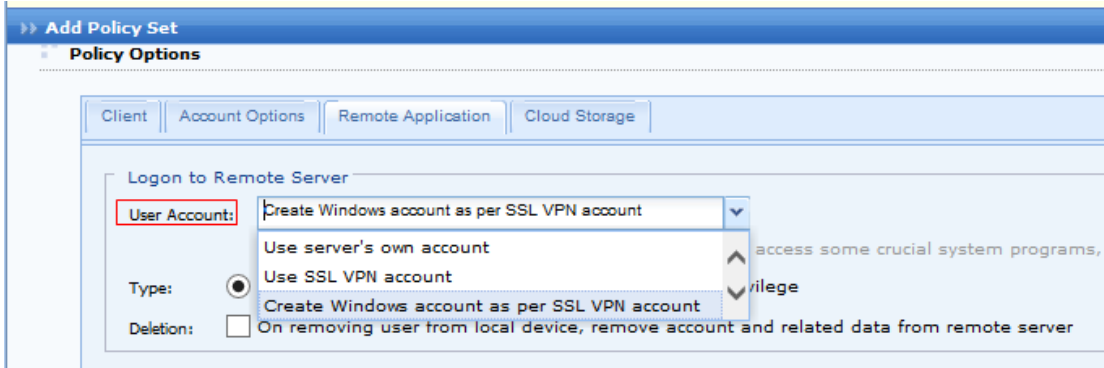
- The selected programs are seen in the figure below:



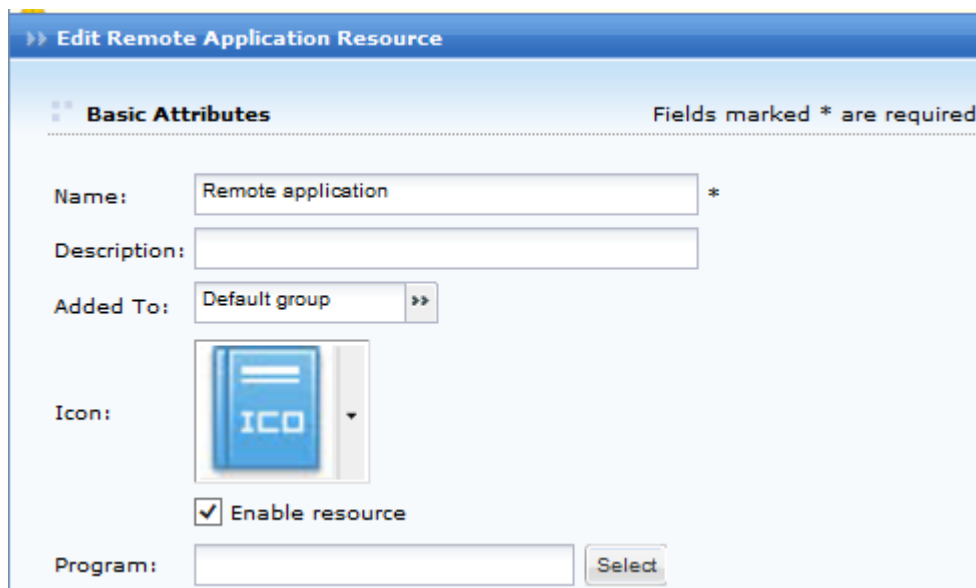
8. Click the **Save** button on the editing app server page to save the settings.
9. Go to **SSL VPN > Remote Servers > Storage Server** to enter the **Storage Server** page, click **Add** to add a storage server and create private directory and public directory for it, as shown below:



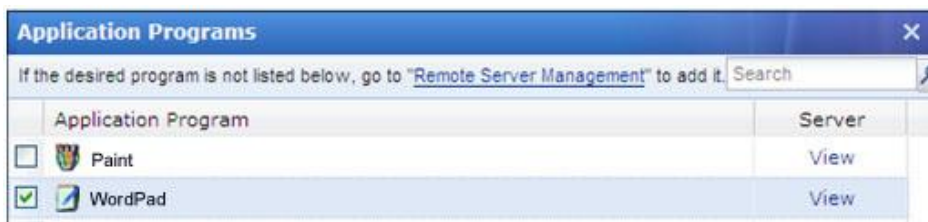
10. Navigate to **SSL VPN > Policy Sets** to enter the **Policy Sets** page and add a policy set that will associate with the corresponding user (for procedures of configuring policy set, refer to the Adding Policy Set section in Chapter 4). While configuring the **Remote Application** tab (as shown in the figure below), ensure the following:
 - The user account for logging in to the remote application server is the **SSL VPN account** or **Windows account created as per the SSL VPN account**.
 - Directory is specified, so that the data or files in remote application session will be saved in the storage server and available to user for future access. Private directory indicates that a folder will be created in the specified directory automatically when user connects to the remote server, and is solely visible for that user.



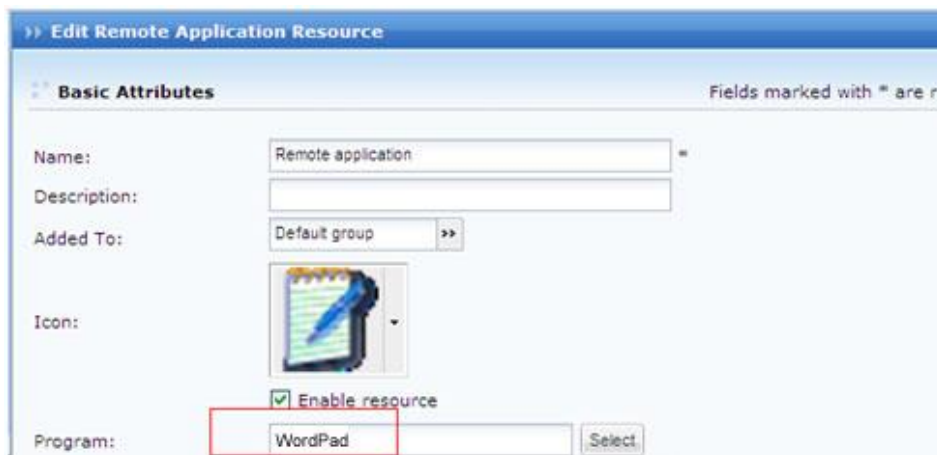
11. Associate the policy set with the corresponding user (for detailed guide, refer to the Adding User section in Chapter 4).
12. Navigate to **SSL VPN > Resources** to add a remote application resource (for detailed guide, refer to the Adding/Editing Remote Application section in Chapter 4), as shown below:



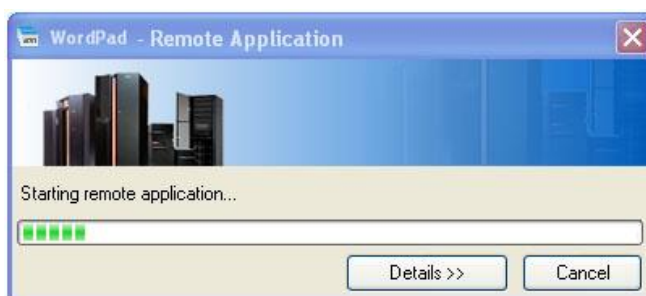
13. Click the **Select** button (next to **Program** field) to select program **WordPad**, as shown below:



14. Click the **OK** button to save the settings and the program name is seen in the **Program** field.



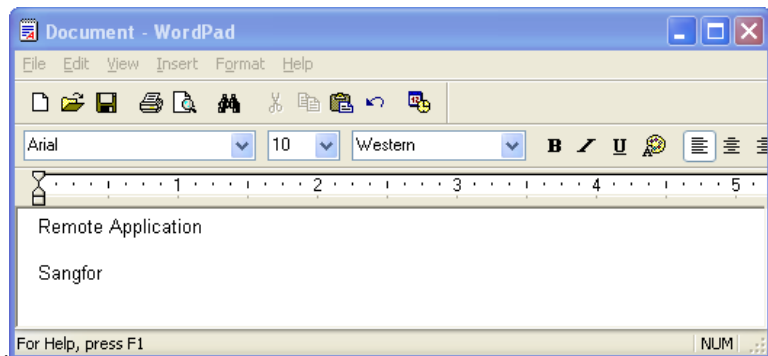
15. In the **App Server** tab, select an application server to publish **WordPad**.
16. Navigate to **SSL VPN > Roles** to associate this remote application resource with the corresponding user (for detailed guide, please refer to the Roles section in chapter 4).
17. After the employee logs in to the SSL VPN, he or she will see the **Resource** page with the resource link to that remote application.
18. Click on the link to the remote application resource created in Step 12, and a remote application session will be established, as shown in the figure below:



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



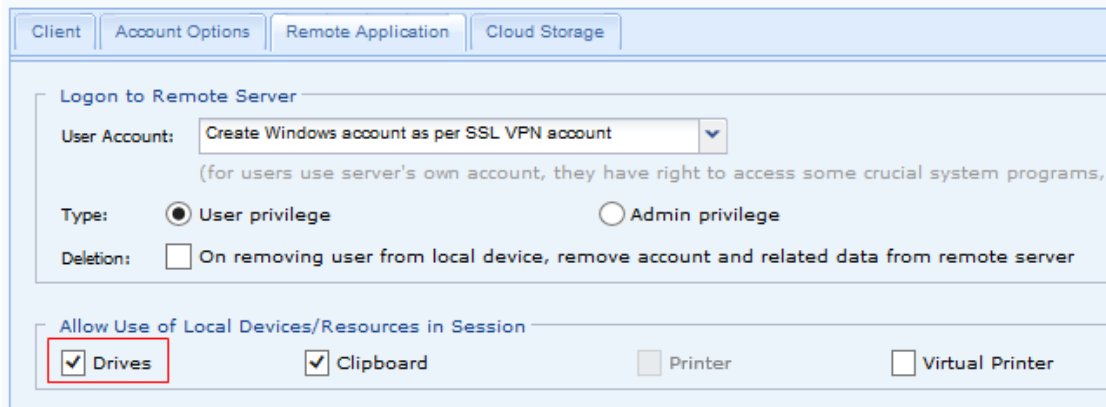
Once the session is established successfully, **WordPad** will be launched. The employee can edit and save the document to the specified directory on the remote storage server. Next time logging in to SSL VPN, he or she can edit this document again in remote application session



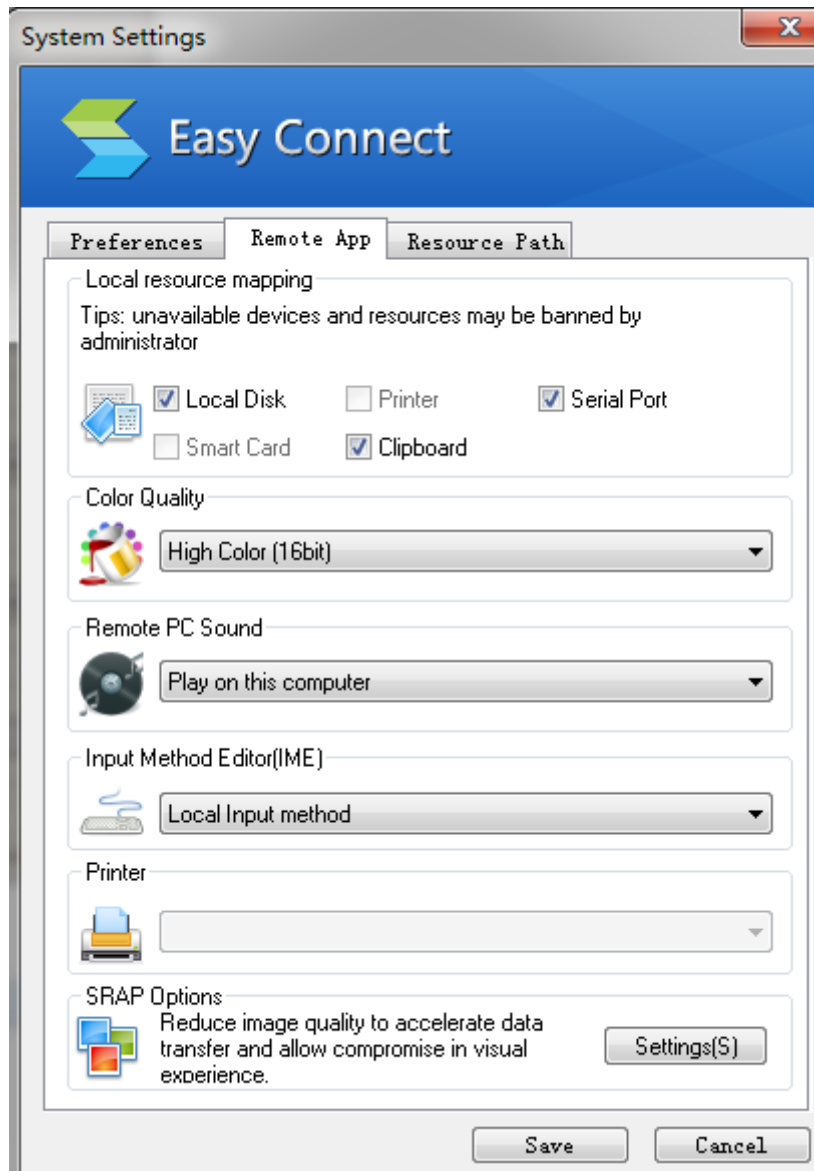
If the employee wants to save the modified file on client side. There are two methods to achieve that:

Method 1:

- a. Select **Drives** option on **Remote Application** tab when adding/editing policy set, as shown in the figure below:



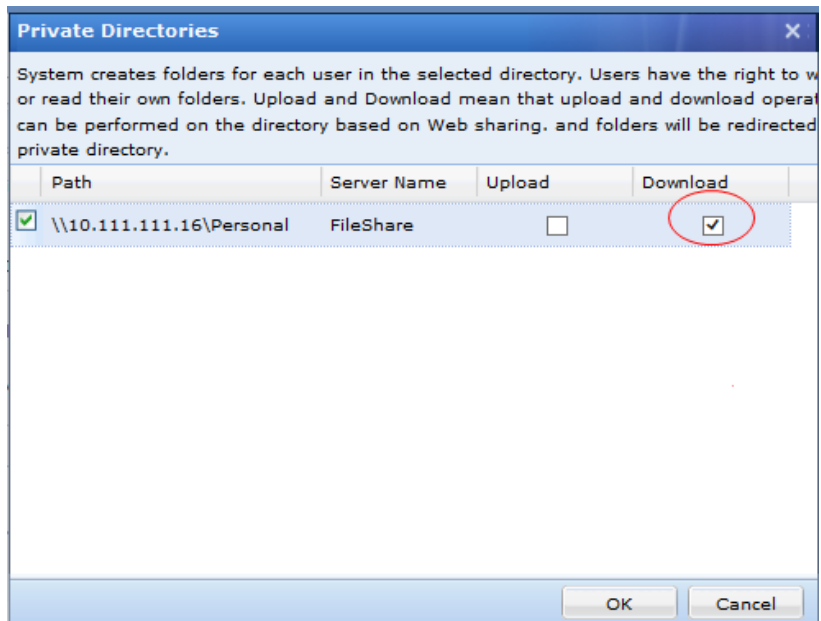
- b. Log in to SSL VPN using VPN client. Right-click on VPN client logo and click on **System Settings** to enter the **System Setting** page and click **Remote Application** tab to enter the following page, as shown below, and select the **Local Disk** option.



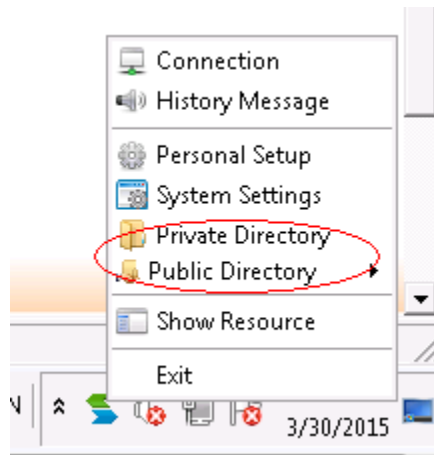
Click **Save** to save the changes. Then you can save file to the local drives.

Method 2: Download the file by the means of file sharing

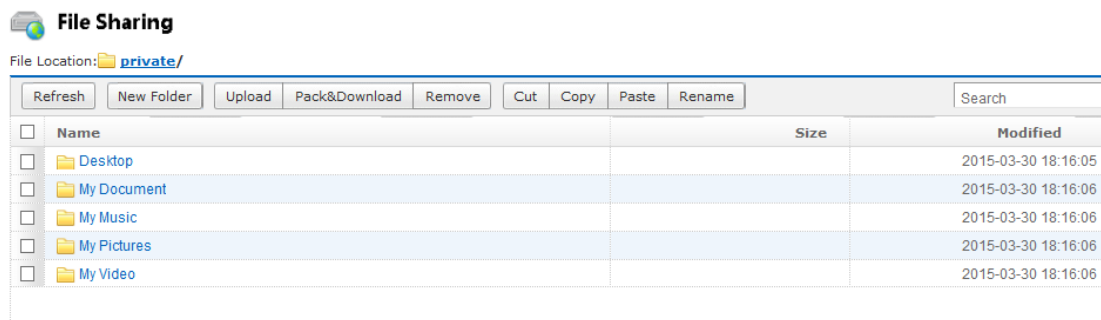
- a. Select **Download** when selecting private directory or public directory on **Cloud Storage** tab, as show in the figure below:



b. Log in to SSL VPN and right-click on VPN client logo, you will see the following figure:



c. Click **Private Directory** to enter the **File Sharing** page, as shown in the figure below and you can download desired file here:



Configuring Authentication with External CA

Using External CA Root Certificate to Generate Device Certificate

Purpose:

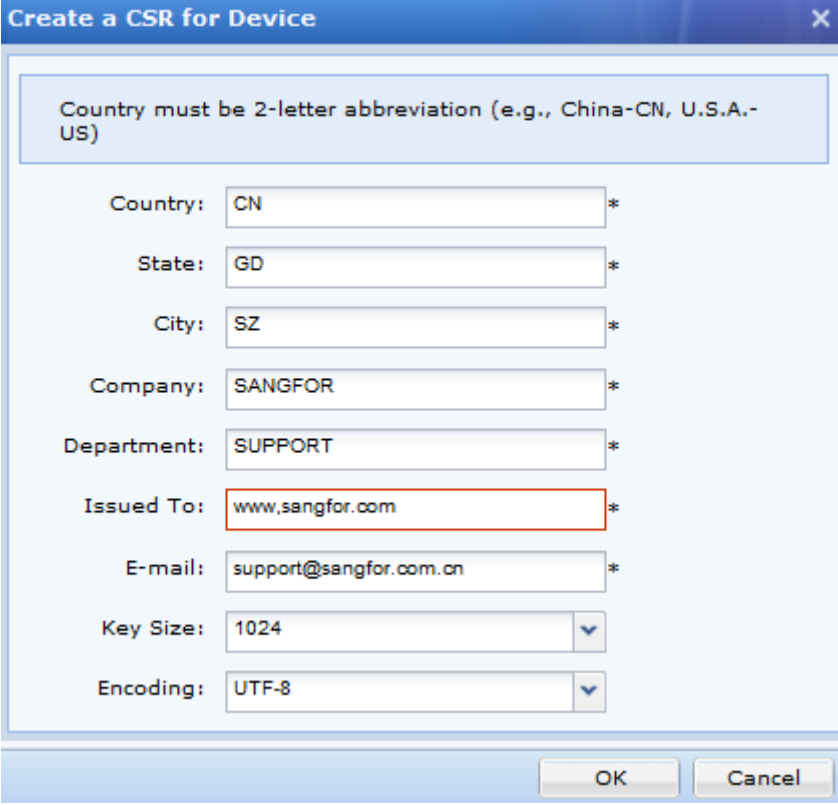
Import and use the external CA root certificate to generate certificate for the Sangfor device, so that end users can pass certificate based authentication when logging in to the SSL VPN if they own certificates issued by that external CA.

To achieve the expected purpose:

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



2. Click the **Create CSR** button to generate a certificate signing request (CSR) for the Sangfor device. The **Create a CSR for Device** page is as shown in the figure below:



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: www.sangfor.com *

E-mail: support@sangfor.com.cn *

Key Size: 1024 ▼

Encoding: UTF-8 ▼

OK Cancel

3. Configure the required fields. In this scenario, country is **CN** (China), state is **GD** (Guangdong), city is **SZ** (Shenzhen), company is **SANGFOR**, department is **SUPPORT**, email address is **support@sangfor.com.cn**, and the certificate is issued to the login page (address is **10.111.111.3**) to the administrator Web console of Sangfor device.



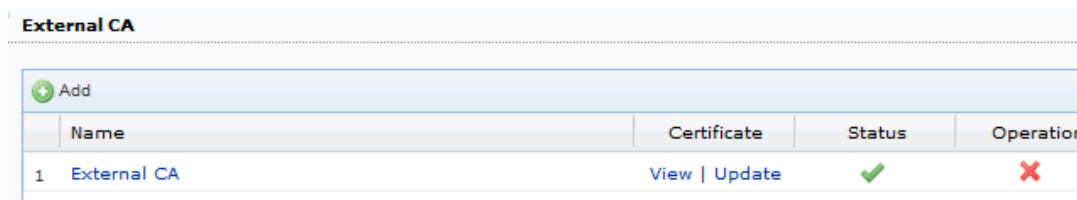
-
- Country should be a two-letter abbreviation.
 - State name can contain a maximum of 20 characters.
-

4. Click the **OK** button to save the settings.
5. Once the CSR is generated, click **Download** to download the request or copy the above request contents into a text file. The contents in the .csr file are as shown below:

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBODCCATkCAQAwwY8xCzAJBgNVBAYTAkNOMQswCQYDVQQIEwJHRDELMAkGA1UE
BxMCMCU1oxEDA0BgNVBAoTB1NBTKdGT1IxEDA0BgNVBAsTB1NVUFBPULQxGzAZBgNV
BAMTEnd3dy5zYW5nZm9yLmNvbS5jbjE1MCMGCSqGSIb3DQEJARYWc3VwcG9ydEBz
YW5nZm9yLmNvbS5jbjBzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAxLfm14gT
VGib8SuYYvy4txDzSN6DrGI031kAZRHRw77tEs8LbEu1HozLwCSfZDVgk3fue0Be
K3dkkx7nsZ+QMZ/OiCOLnoJuzH+SXwsb10SN0u3z633wYlh1qS2n04nB51kKPC9I
rcohT9sDXHEsf8NZJeh+6u9y2xnTCdjfNxECAwEAaAAMA0GCSqGSIb3DQEBBQUA
A4GBAChre1tw+81CkkB6QCKaX71Wih88K0QEUntW5nZCjW+r1TBwKzZAL3oxAN8I
BX99sSiDKu5Hruh3TN4jk5R+VbCtHW7rPkDJPK0df26Sv1REVuw6p7u1xr/qVJyV
OHCYdmjA8e0mVZMLVYu9mOBjMZe1UdfxaeF82xr9ehKpM+K4
-----END CERTIFICATE REQUEST-----
    
```

6. Submit the generated CSR to the external CA.
7. Get the Sangfor device certificate from the external CA.
8. Navigate to **SSL VPN > Authentication > Certificate/USB Key Based Authentication** page, and click **Add** under **External CA** section to upload the device certificate you have received from external CA to Sangfor device, as shown below:



9. Click on the **External CA** in **Name** column to enter the **External CA** page and configure **CA Options**, as shown in the figure below:



10. Users can log in to SSL VPN with the certificated issued by this external CA.

Mapping User to Local Group Based on External Certificate

Background:

Take Microsoft CA for example. As we know, for user accounts stored on LDAP server, the users under different OUs have varied privileges.

Now, the prerequisite is that each user owns a certificate issued by a third party CA already. We are to have these users (under different OUs) automatically granted with different levels of privilege to access the SSL VPN, hoping that they can pass the certificate based authentication with the certificate issued by the third-party CA when they connect to SSL VPN.

Suppose LDAP user **test1** is under **ou1**, and user **test2** is under **ou2**.

Purposes:

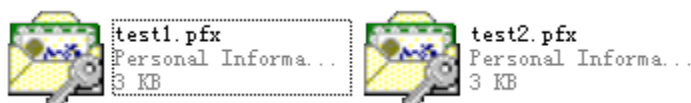
To assign different resources to the two users automatically after they log in to the SSL VPN successfully, but the two users need not be imported into the Sangfor device.

Analysis and solution:

Firstly, we need to configure external CA and use the CA to generate certificate, so that users can use third-party certificate to log into the SSL VPN. Secondly, we need to map the certificate users to the user group on Sangfor device, so that they can be granted with the same privilege as the users under the target group.

To achieve the expected purposes:

1. Configure external CA (for detailed guide, please refer to Configuring External CA in Chapter 4).
2. Navigate to **SSL VPN > Users** and create two user groups named **ou1** and **ou2** (for detailed guide, please refer to the Adding User Group section in Chapter 4). Primary authentication **Certificate/USB key** need not be selected for both users **ou1** and **ou2**.
3. Generate certificates for the two users, **test1** and **test2**.



Check the subjects of the two certificates, as shown below.

DN of test1: CN=test1, OU=ou1, DC=zy, DC=sangfor, DC=com

DN of test2: CN=test2, OU=ou2, DC=zy, DC=sangfor, DC=com

4. Configure CA option. Select **Trust all the users who own certificate issued by current CA** option, as shown in the figure below:

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

Group Mapping Rule: [Configure Mapping Rule](#). Mapping user to a local group will have this user associate with policies and authentication methods of this group.

5. Click the link **Configure Mapping Rule** to configure two mapping rules, one rule mapping LDAP **ou1** to the local group **ou1**, and the other mapping LDAP **ou2** to the local group **ou2**, as shown in the figures below:

Add External Certificate User Mapping Rule

For users who have not imported certificate into local device, system will map the specified user to certain local group after successful authentication as per the mapping rule below. Those users have the same privilege as the group users.

Notes:

1. Certificate 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=CNZ

Certificate DN:

Map to Group:

OK Cancel

Add External Certificate User Mapping Rule

For users who have not imported certificate into local device, system will map the specified user to certain local group after successful authentication as per the mapping rule below. Those users have the same privilege as the group users.

Notes:

1. Certificate 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=CNZ

Certificate DN:

Map to Group:

OK Cancel

6. Navigate to **SSL VPN > Roles**, create two roles and associate the local groups **ou1** and **ou2** with different resources (for detailed guide, please refer to the Adding Role section in Chapter 4).
7. Save the setting and then click the **Apply** button when configuration is completed.

After logging in to the SSL VPN, what **test1** and **test2** will see on the **Resource** page will be the corresponding associated resource.

Configuring Resource Enabling SSO

Adding TCP Application Enabling SSO

Purpose:

When end users access tech forum of their company, they do not need to enter username and password again, which will be filled in automatically with their SSL VPN accounts.

Analysis and solution:

Firstly, we need to configure the tech forum as a TCP application. Secondly, enable SSO feature for this resource and choose a login method, which can be **Auto fill in form** or **Set auto-access request**. In this scenario, we take the former as example.

To achieve expected purpose:

1. Navigate to **SSL VPN > Users > Local Users** and click **Add > User** to add a user(for detailed guide, refer to Adding User in Chapter 4)
2. Go to **SSL VPN > Resources** page and click **Add > TCP app** to add a TCP resource, as shown below:

Edit TCP Application

Basic Attributes

Name: Tech forum *

Description:

Type: HTTP

Address: 192.200.200.44/80:80

Program Path: Browse...

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

Added To: Default group

Icon: ICO

Enable resource

Visible for user

SSO | Authorized Admin | Accounts Binding | URL Access Control | Others

Enable SSO

Login Method: Auto fill in form | Advanced

Click on **SSO** tab and select the **Enable SSO** to enable SSO feature, and choose auto fill in form as **Login Method**.

- Go to **System > SSL VPN Options > General > SSO** page to download SSO assistant and config file, as shown in the figure below:

Login | Client Options | Virtual IP Pool | Local DNS | **SSO** | Resource Options

SSO

SSO: Enabled Disabled

Allow user to modify SSO user account

Upload SSO Configuration File

Config File: Browse...

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

Upload

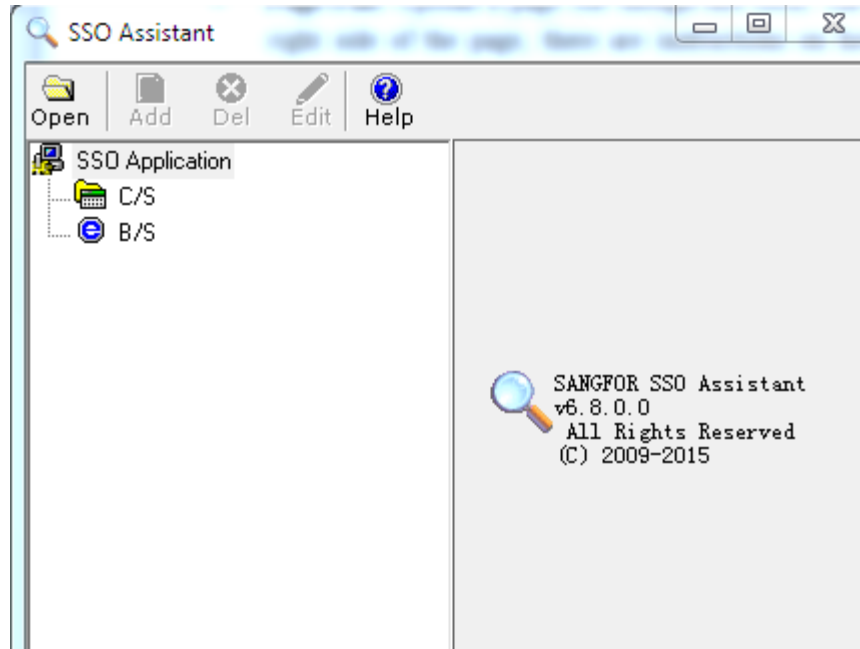
[Download SSO Assistant](#)

[Download SSO Config File](#)

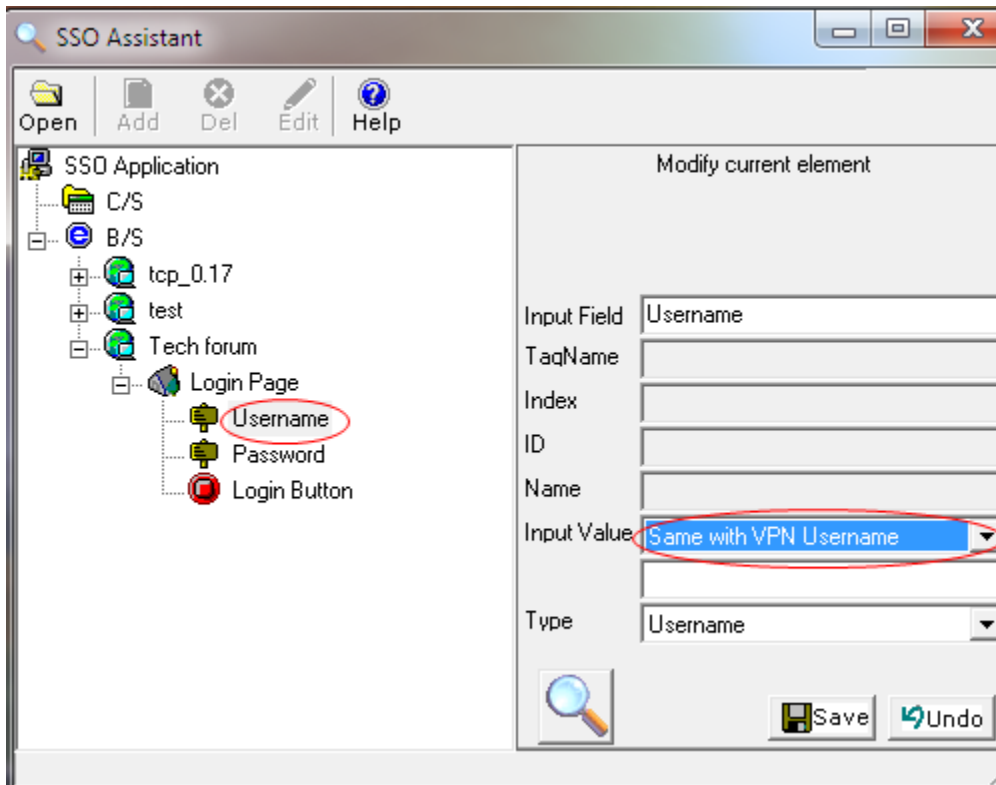
- Install the SSO assistant. After installation completes, a corresponding shortcut will be created for the SSO assistant, as shown below:



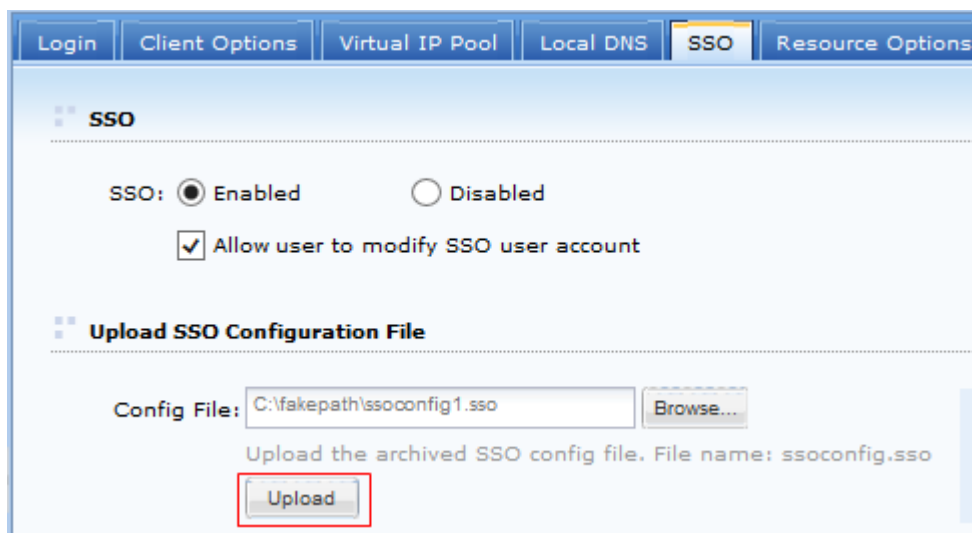
5. Double-click on the shortcut to launch SSO assistant, as shown below:



Click **Open** to import SSO config file downloaded in step 3 and record SSO information with SSO Assistant. Click on the **Username** under the desired resource and right-click it to click **Edit**, then drag the magnifier on current page to **Username** textbox on the login page of this tech forum and select **Same as VPN Username** in **Input Value** field. Click **Save** to save the changes. The method to record password and login button is similar with that of recording username.



6. After recording SSO information completes, upload the SSO config file to Sangfor device. Go to **System > SSL VPN Options > General > SSO** page and click **Browse** under **Upload SSO Config File** section to select desired SSO config file, and then click **Upload** to upload it to the device, as shown below:



7. Navigate to **SSL VPN > Roles > Role Management** to add a role and associate it with the user created in step1 and the resource created in step2(for detailed guide, refer to Adding Role in Chapter 4).
8. After user logs in to SSL VPN, he/she can click the resource link to access the tech forum directly without entering username and password.

Adding Remote Application Enabling SSO

Background:

RXT, a instant messaging tool, is published over SSL VPN. Employee's account for logging in to RTX is not the same as that for logging in to SSL VPN. The username of RTX account is the abbreviation of employee's name, and the password is their work number.

Purpose:

Enable employees to access RXT directly without need to provide RTX account after they log into SSL VPN.

Analysis and Solution:

As employee's account for logging in to RTX is different from the account for logging in to SSL VPN, **Allow user to modify SSO user account** option should be selected when configuring SSO.

To achieve expected purpose:

1. Configure a remote server(for details, refer to Adding Remote Application in this Chapter)
2. Navigate to **SSL VPN > Users > Local Users** and click **Add > User** to add a user(named **ssl1**, password is 123). For detailed guide, refer to Adding User in Chapter 4.
3. Go to **SSL VPN > Resources** page and click **Add > Remote app** to add a remote application named RTX, as shown below:

Edit Remote Application Resource

Fields marked * are required

Basic Attributes

Name: RTX *

Description:

Added To: RemoteApp

Icon:

Enable resource

Program: RTX

Working Directory: ⓘ

Command Line Argument:

Maximize window after program is launched

Single instance is allowed (for an application running on remote server, not allow user to run a second instance of the application)

App Server | **SSO License** | Authorized Admin

Enable SSO

Click on **SSO License** tab to select the **Enable SSO** option.

- Go to **System > SSL VPN Options > General > SSO** page, select the **Allow user to modify SSO user account** option, and download SSO assistant and config file, as shown in the figure below:

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

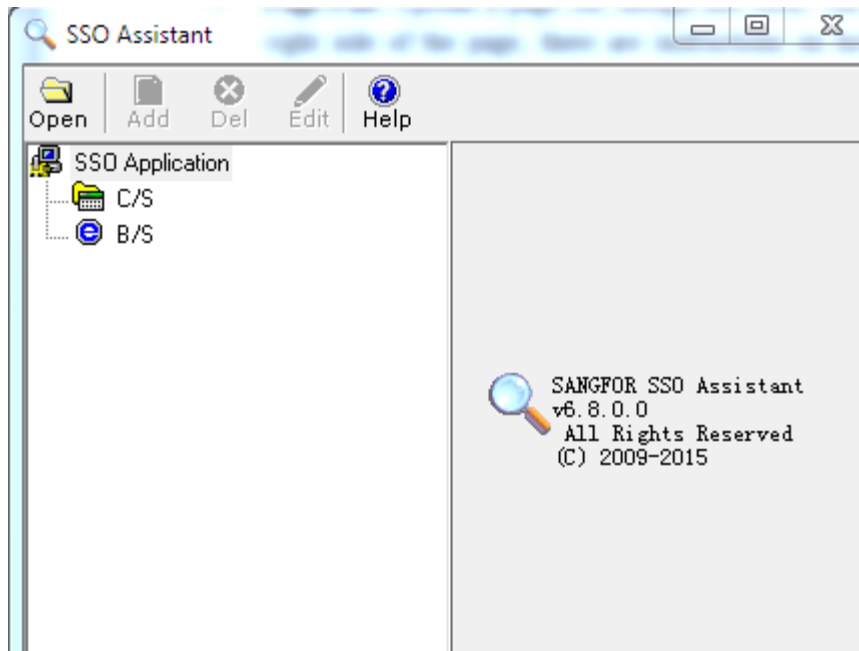
[Download SSO Assistant](#)

[Download SSO Config File](#)

- Install the SSO assistant. After installation completes, a corresponding shortcut will be created for the SSO assistant, as shown below:



6. Double-click on the shortcut to launch SSO assistant, as shown below:

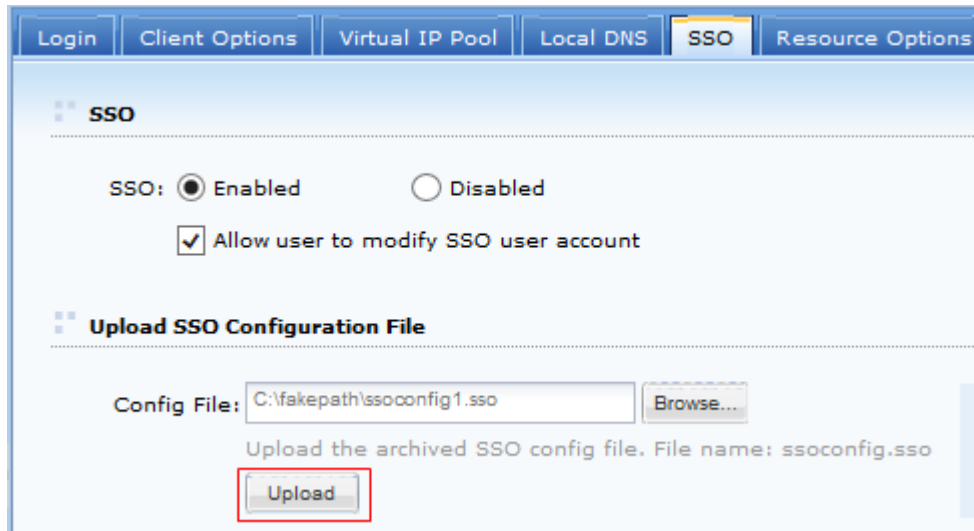


Click **Open** to import SSO config file and record SSO information with SSO Assistant.

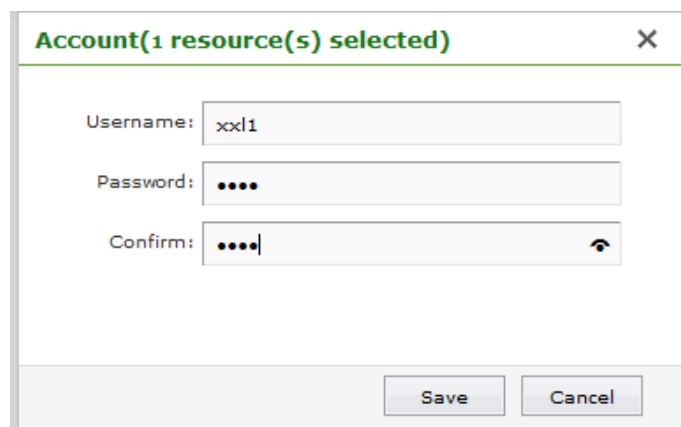
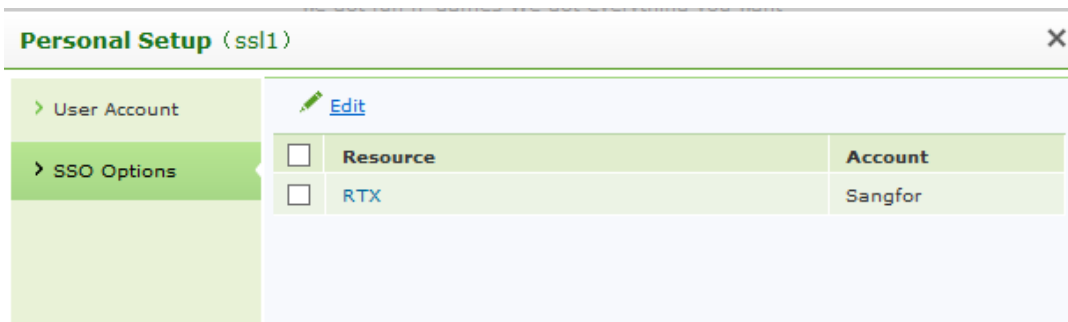
Click on the **Username** under the desired resource and right-click it to select **Edit**, then drag the magnifier on current page to **Username** textbox on RTX login page and select **Same as VPN Username** in **Input Value** field.

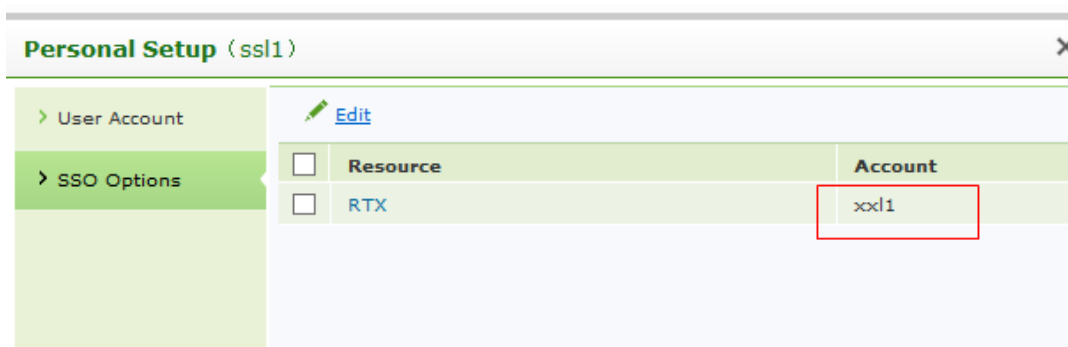
Click **Save** to save the changes.

7. After recording SSO information completes, upload the SSO config file to Sangfor device. Go to **System > SSL VPN Options > General > SSO** page and click **Browse** under **Upload SSO Config File** section to select desired SSO config file, and then click **Upload** to upload it to the device, as shown below:



8. Navigate to **SSL VPN > Roles > Role Management** to add a role and associate it with the user **ssl1** created in step2 and the resource **RXT** created in step3(for detailed guide, refer to Adding Role in Chapter 4).
9. After user **ssl1** logs in to SSL VPN, click **Settings** on the upper right of the page to modify the RTX account(for example, modify username to your real name xx11, password to your work number).





10. Back to **Resource** page and click on the resource link, then user can log in RTX automatically.

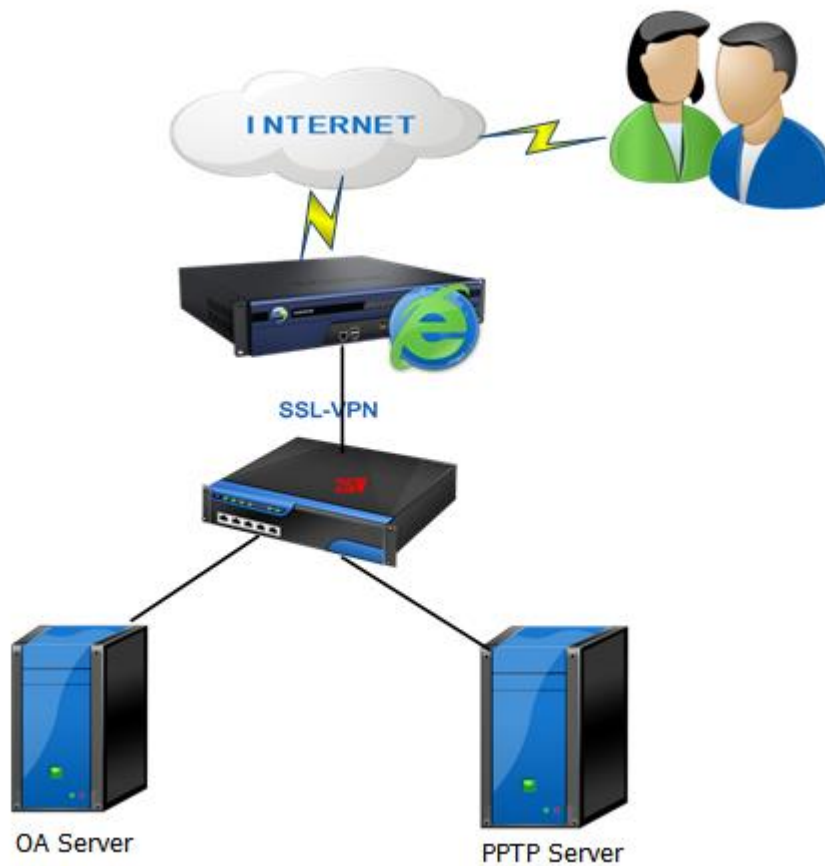


- SSO feature has two login methods: **Auto fill in form** and **Set auto-access request**. The SSO feature with **Auto fill in form** as login method applies to web app, TCP app, all B/S-based and C/S-based L3VPN app, while SSO feature with **Set auto-access request** as login method supports web app, TCP app, HTTP-based and HTTPS-based L3VPN app.
- Remote application only supports the SSO feature with **Auto fill in form** as login method

Configuration Case of Accessing SSL VPN through PPTP

One customer wants to access internal network through SSL VPN by using browser of their own iPhone, iPad or Android mobile phones, that is, realize mobile office by using mobile phones.

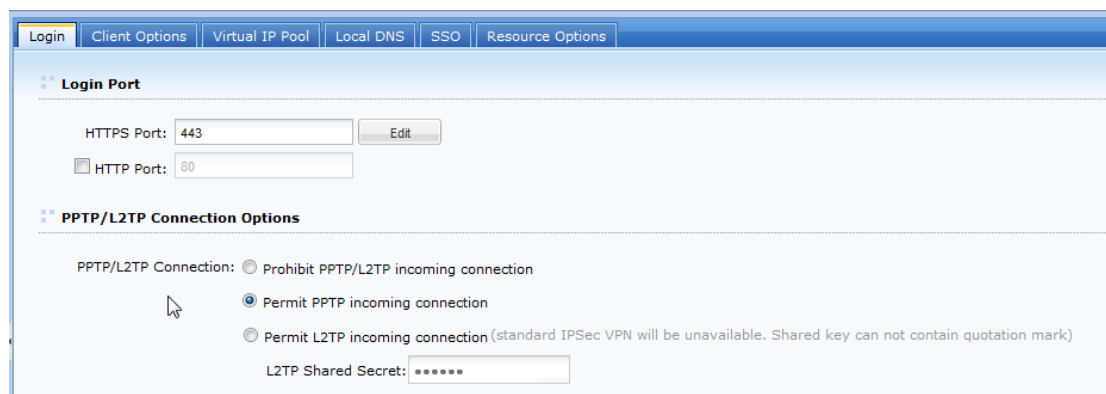
Since internal BBS system of the customer is written by JSP, systems are rather complex, a lot of scripts and controls are used, therefore WEB application is not applicable, L3VPN is a better choice.



Configurations are as follows:

Configurations of SSL

Step 1: Navigate to **System > SSL VPN Options > General > Login**, select **Permit PPTP incoming connection**, as shown below:



Step 2: Navigate to **SSL VPN > Policy Sets**, click **Add** to add policy set and to enter the **Add**

Policy Set page. Select **Permit PPTP/L2TP incoming connection**, as shown below:

The screenshot shows a configuration page with several sections:

- 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 Maximum: 50 (10-500)
 - Enable bandwidth limit Outbound: 128 KBps, Inbound: 128 KBps (0 indicates no limit. Minimum is 32KBps)
 - Preferred to enable byte cache
- Permit PPTP/L2TP incoming connection
- Enable Dedicated SSL VPN Tunnel (after login, user cannot access other resources except those accessible over SSL VPN)
- Each user may own multiple hardware IDs, maximum: 5 (1-100)

Step 3: Navigate to **SSL VPN > Users**, Click **Add > Group** to enter the **Add User Group** Page. Associate policy sets in **Attribute** of use/user group which get connected through PPTP.

The screenshot shows the 'Add User Group' configuration page with the following sections:

- Basics:**
 - 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
 - Secondary Authentication:
 - Hardware ID
 - SMS password
 - Dynamic: radius1
 - Require: Both Either
 - 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: >> [Create + Associate](#)

Step 4: Navigate to **SSL VPN > Resources**, click **Add > L3VPN** to enter the **Edit L3VPN** page. Add resources to be accessed by using PPTP.

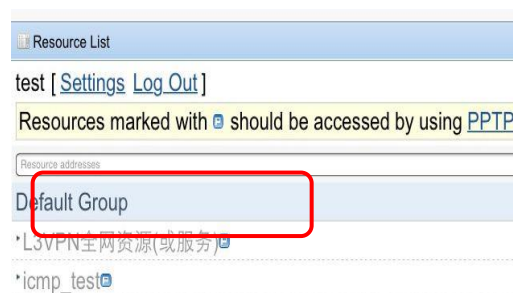
The screenshot shows the 'Edit L3VPN' configuration window. The 'Basics' tab is active. The 'Name' field is empty and has a red border. The 'Description' field is empty. The 'Type' is set to 'HTTP' and 'Protocol' is set to 'TCP'. The 'Address' field is empty. The 'Program Path' field is empty with a 'Browse...' button. Below it, a note says 'Path could be absolute path and environment variable (e.g., %windir%)'. The 'Added To' dropdown is set to 'Default group'. The 'Icon' dropdown is set to 'ICO'. There are two checked checkboxes: 'Enable resource' and 'Visible for user'. At the bottom, there are tabs for 'SSO', 'Authorized Admin', 'Accounts Binding', and 'URL Access Control'. The 'SSO' tab is active, showing an 'Enable SSO' checkbox and a 'Login Method' dropdown set to 'Auto fill in form'.

Step 5: Navigate to **SSL VPN > Roles**. On the **Role Management** page, click **Add > Role** to enter the **Add Role** page, and associate user/user group and resources.

PPTP Client Access Configuration:

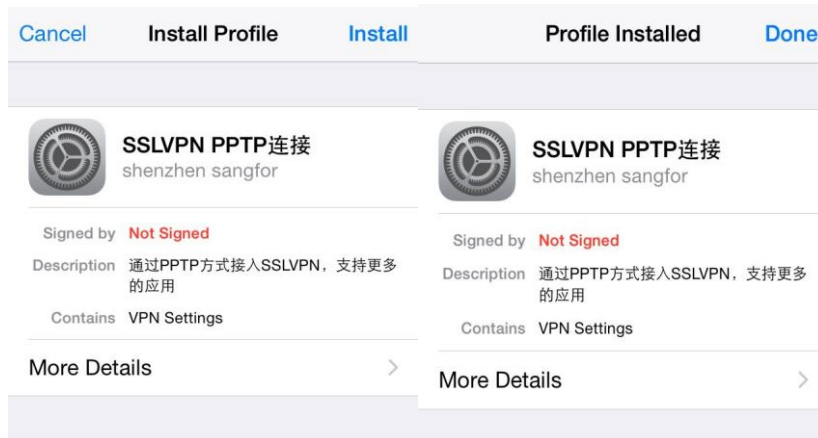
Here is an example of one user who uses iphone to configure PPTP access resources:

Log in to SSL VPN through browser of the iphone, as shown below:



Note: Resources marked with  is L3VPN and should be accessed by using PPTP.

1. Click Access **SSLVPN Through PPTP**. Access tips pop up. Install description file to mobile phone.



2. Set PPTP VPN login. Go back to iPhone homepage, and go to **Settings** as follows:



3. VPN switch turns green after connection. A small icon **VPN** shows on the upper left. Then you can access internal network applications through browser or application program.
4. When you want to exit PPTP VPN, switch off **VPN** option. Next time you can directly get connected to PPTP VPN to access resources.



- Remember PPTP login password. Go to **General > Network > VPN** and click the blue arrow, as shown below:



Enter password in **Password** and click **Save**. You do not have to enter password again for later connections.

PPTP configuration is completed. You can use your mobile phone to access BBS.



When SSL device is deployed in single-arm mode, the following is required: (1) TCP 80 and Port 443 connected by SSL users should be mapped, TCP 1723 port should also be mapped. (2) PPTP data package can penetrate front-end device, and also protocol 47 can penetrate front-end device.



Applications accessed through PPTP should be added as L3VPN resources. If the application can be accessed through WEB, then the application can directly get connected to SSL VPN without building PPTP connections.



Telecom operators in some districts (For example, Beijing Unicom) will block PPTP of 3G network. If, after deployment, you can get accessed through wifi , but not through 3G, it is probable that operators have blocked.



When PPTP fails to get connected, make sure whether devices from local network to SSL support PPTP penetration. For example, TP-link supports 32 PPTP penetrations, D-Link does not support PPTP penetration, and Tenda supports PPTP penetration.

Configuration Case of Accessing SSL VPN through L2TP

Internal network in headquarter has DNS. One customer wants to access SSL through L2TP on mobile endpoints, access internal network with domain account, and realize mobile office on mobile endpoints.



Configurations are as follows:

Configuration of SSL:

Step 1: Navigate to **System > SSL VPN Options > General > Login**, select **Permit L2TP incoming connection** and set **L2TP Shared Secret**, as shown below:

The screenshot shows the configuration interface for the SANGFOR vSSL VPN. The 'Login' tab is selected. Under 'Login Port', the 'HTTPS Port' is set to 443 and the 'HTTP Port' is set to 80. Under 'PPTP/L2TP Connection Options', the 'Permit L2TP incoming connection' radio button is selected. The 'L2TP Shared Secret' field is filled with seven dots. A note at the bottom explains the L2TP feature and its interaction with IPsec VPN.

Login Port

HTTPS Port: 443 Edit

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.
[Domain SSO](#), 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, Sangfor VPN service will still be available.

Step 2: Navigate to **SSL VPN > Authentication**. Click **Settings** after **LDAP**. On **LDAP Server**

page click **Add** to add LDAP server, as shown below:

Basics

Server Name: *

Description:

Server Address:

Admin DN:

Password:

Base DN: >>

Subtree included (also verify the users in subtrees)

Authentication Timeout: * second(s)

Status: Enabled Disabled

Other Attributes > Group Mapping. Add group mapping as below:

Authentication > LDAP Server > Add/Edit LDAP Server

Other Attributes

Group Mapping | Role Mapping | LDAP Extensions | Password Encryption

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.

Add Delete Edit Automatic Mapping

<input type="checkbox"/> OU	Sub-OU in...	Map to Local Group

If LDAP user matches none of the above mapping rules, map the user to group: >>

Step 3: Navigate to **SSL VPN > Authentication**, click **Settings** after **Client-Side Domain SSO**, and add SSL device to AD domain. Configuration page is shown as below:

Basics

After this device is joined to domain, add a corresponding DNS rule. [View Configuration Method](#)

Client-Side Domain SSO: Enabled

Status: **Invalid**

Device Name: sangfor9701b3b1

Domain Name: *

Short Domain Name: *

Domain Controller Name: *

Domain Controller IP: *

Admin Username: *

Admin Password:

Step 4: Navigate to **SSL VPN > Policy Sets**. On the **Policy Set Management** page, click **Add > Policy set** to enter the **Add Policy Set** page, and select **Permit PPTP/L2TP incoming connection**, as shown below:

Client Account Options Remote Application Cloud Storage EMM

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 Maximum: (10-500)

Enable bandwidth limit Outbound: Kbps, Inbound: Kbps (0 indicates no limit. Minimum is 32KBps)

Preferred to enable byte cache

Permit PPTP/L2TP incoming connection

Enable Dedicated SSL VPN Tunnel (after login, user cannot access other resources except those accessible over SSL VPN)

Each user may own multiple hardware IDs, maximum: (1-100)

Step 5: Navigate to **SSL VPN > Users** to enter the **Local Users** page. Associate policy sets in **Attribute** of use/user group which get connected through L2TP.

Edit User Group

Basics

Name: *

Description:

Max Concurrent Users: (0 indicates no limit)

Status: Enabled Disabled

Authentication Settings

Group Type: Public group Private group

Primary Authentication	Secondary Authentication
<input checked="" type="checkbox"/> Local password	<input type="checkbox"/> Hardware ID
<input type="checkbox"/> Certificate/USB key	<input type="checkbox"/> SMS password
<input type="checkbox"/> External <input type="text" value="radius1"/> ▼	<input type="checkbox"/> Dynamic <input type="text" value="radius1"/> ▼
LDAP/RADIUS Require:	token
	<input checked="" type="radio"/> Both <input type="radio"/> Either

Enforce its users/subgroups to inherit the authentication settings

Policy Set

Policy Set: >> [Create + Associate](#)

Enforce its users/subgroups to inherit the policy set

Assigned Roles

Roles: >> [Create + Associate](#)

Step 6: Navigate to **SSL VPN > Resources** and click **Add > L3VPN** to add resources accessed by using L2TP.

Step 7: Navigate to **SSL VPN > Roles** and click **Add > Roles** to associate user/user group and resources.

L2TP Client Access Configuration

Here is an example of one user who uses iphone to configure L2TP access resources:

Go to **Settings > General > VPN**, click **Add VPN Configuration**, as shown below:

The screenshot shows the configuration interface for a VPN connection on a mobile device. At the top, the status bar shows '中国联通' (China Unicom), signal strength, time '15:39', and battery '90%'. The app header displays '< VPN' and '总部北京' (Headquarters Beijing). The configuration fields are as follows:

类型	L2TP
描述	总部北京
服务器	61.50.189.53
帐户	test
RSA SecurID	<input type="checkbox"/>
密码	•••••
密钥	••••••••
发送所有流量	<input checked="" type="checkbox"/>

Below these fields is a '代理' (Proxy) section with three buttons: '关闭' (Off), '手动' (Manual), and '自动' (Automatic). At the bottom, there is a '保存 VPN 配置' (Save VPN Configuration) button.

Description: Enter name of VPN connection.

Server: Enter public network address of SSL.

Account: Enter username to access SSL. If it is AD domain authentication, then enter domain username.

Password: Enter password to access SSL.

Secret: The same as L2TP shared secret of SSL.



When SSL device is deployed in single-arm mode, the following is required: (1) TCP 80 and Port 443 connected by SSL users should be mapped, UDP 500, UDP 4500 and UDP1701 should also be mapped. (2) L2TP data package can penetrate front-end device.



Applications accessed through L2TP should be added as L3VPN resources. If the application can be accessed through WEB, then the application can directly get connected to SSL VPN without building PPTP connection.



Telecom operators in some districts (For example, Beijing Unicom) will block L2TP of 3G network. If, after deployment, you can get accessed through wifi , but not through 3G, it is probable that operators have blocked.



L2TP connection service is enabled, standard IPSec VPN service of SSL can not be used, but SANGFOR VPN still works.

Mobile Users Accessing SSL VPN

Remote desktop and remote application are accessible over SSL VPN on mobile device, such as iPhone, iPad and Android devices. Taking Android mobile device as example, this section introduces how to use EasyConnect to login and access remote resources.

1. Download EasyConnect from Google Store and install it. Launch it, and you will see the figure as shown in Figure 1 .
2. Enter URL to the Sangfor device and click **Connect** button. Then you need to be authenticated before logging in to VPN, as shown in Figure 2. You can click on **Account** tab to provide username and password, or click on **Certificate** tab to use certificate to log in to SSL VPN.
3. After logging in to SSL VPN, if user is associated with L3VPN resource, a prompt dialog appears, as shown in Figure 3. Check **I trust this application** option and VPN connection will be established. To view connection status, click the EasyConnet logo shown at system status toolbar, as shown in Figure 4.

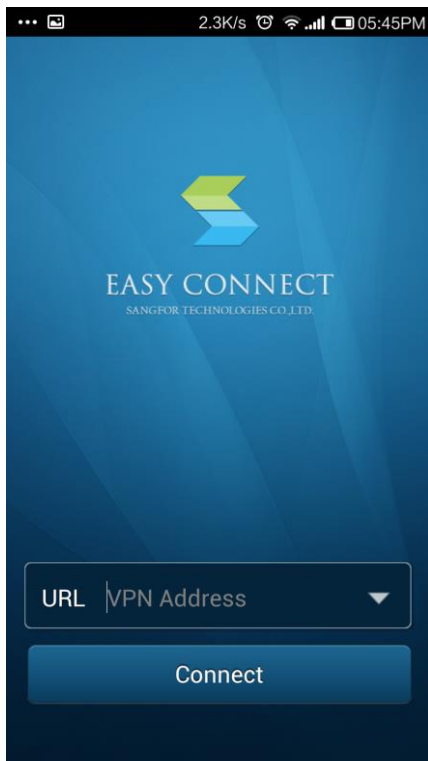


Figure1

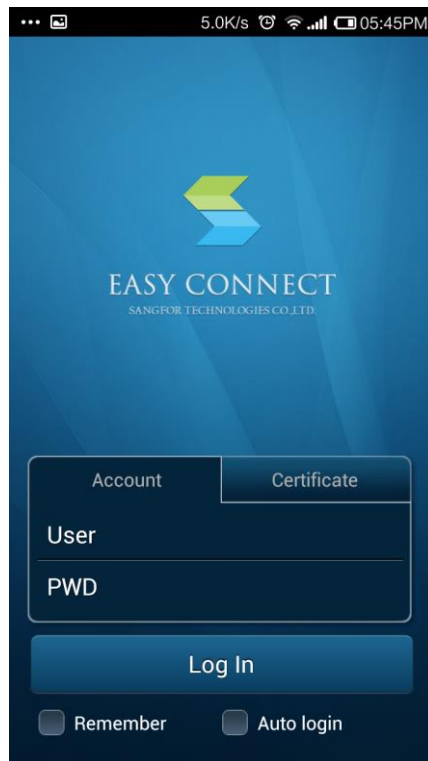


Figure2

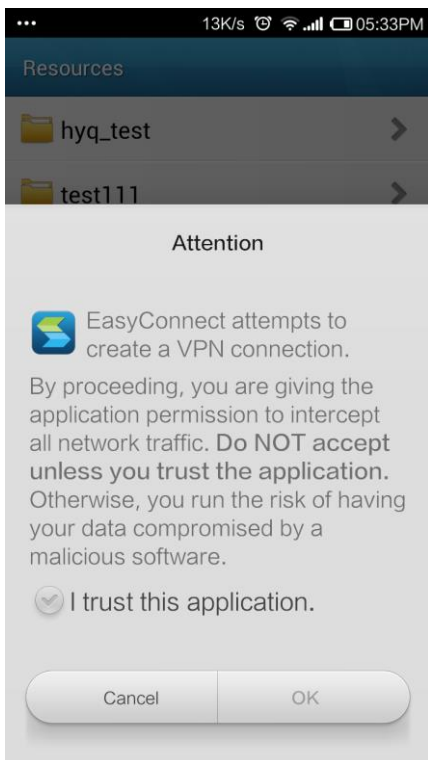


Figure 3

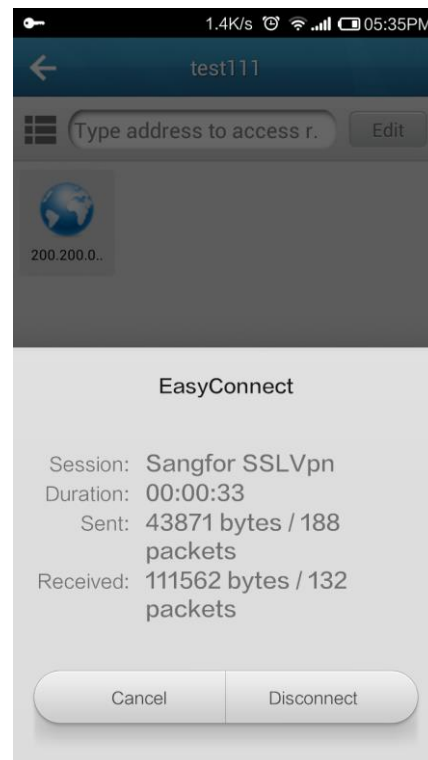



Figure 4

After VPN connection is set up, user can access L3VPN resource using other programs. If he/she does not set up VPN connection, L3VPN resource cannot be accessed, while Web app, TCP pp and remote app are accessible.

Authorized resources will be shown on the right pane of the **Resource** page. Click on the icon  to change the method to display the resources, as shown in Figure 5, Figure6.

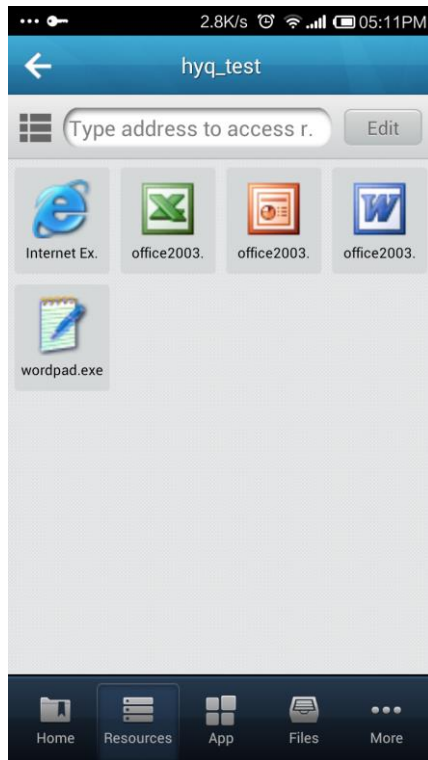


Figure 5 Icon Mode

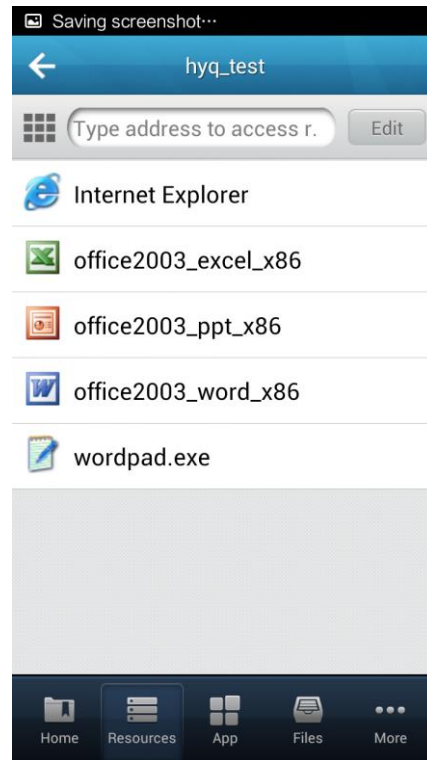



Figure 6 List Mode

To add the desired resource into **Favorites**, click **Edit** to enter the following page, as shown in Figure 7. Click on the golden star icon  next to that resource and click **Finish** to exit editing page. Then the corresponding resource will be added into **Favorites** list, as shown in Figure 8.

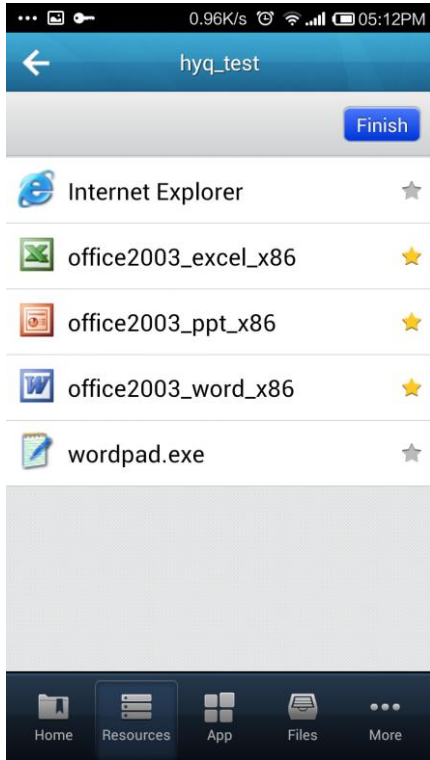


Figure 7

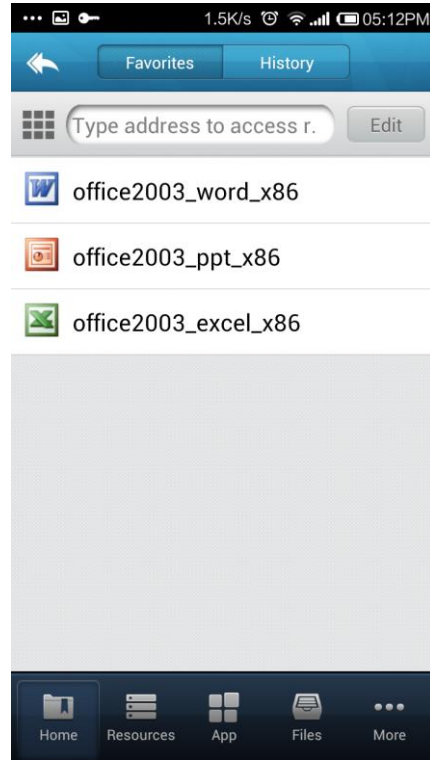


Figure 8

To view accessible personal cloud, public cloud and local storage of mobile device, click **Files** to enter the **Files** page, as shown in Figure 9.

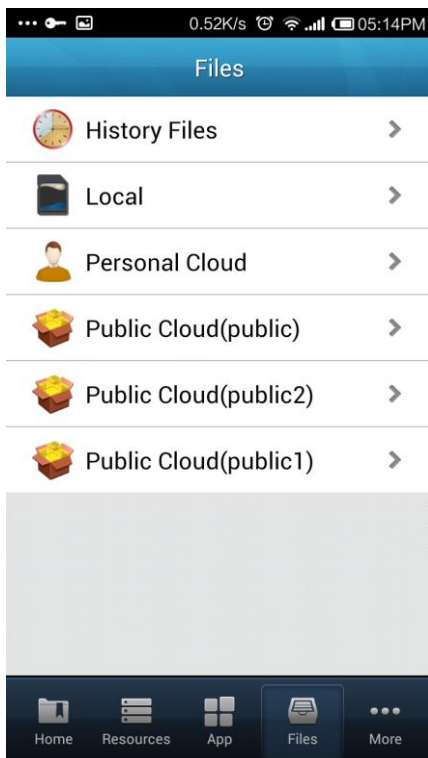


Figure 9

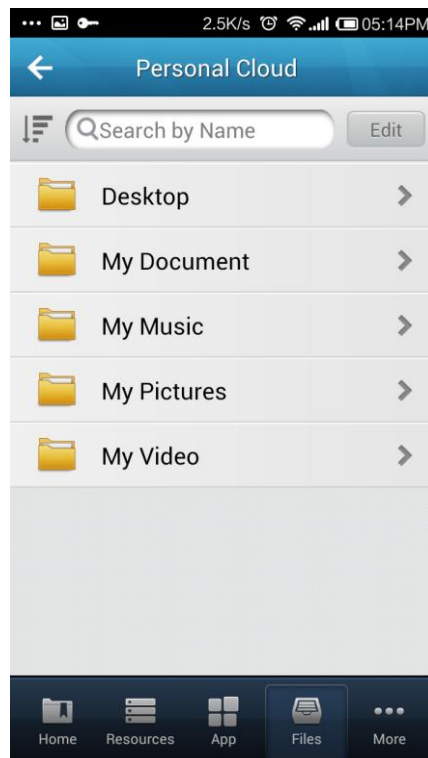


Figure 10

To operate a desired file, for example, **Personal Cloud**, click the arrow icon next to that file

to enter the **Personal Cloud** page as shown in Figure 10.

To open the selected file remotely, click **Open** to open that file using the application program on remote application server.

To download and open a specified file, click **Down & Open** to download that file onto mobile device and open it with default application program installed on mobile device.

To download the selected file, click **Down** to download it to mobile device and that file will be saved into local directory. You can also see that file by clicking **Local** in Figure 9.

To remove a specific file, click **Delete**.

To operate multiple files simultaneously, click **Edit** on the upper right. You will see the page, as shown in Figure 12.

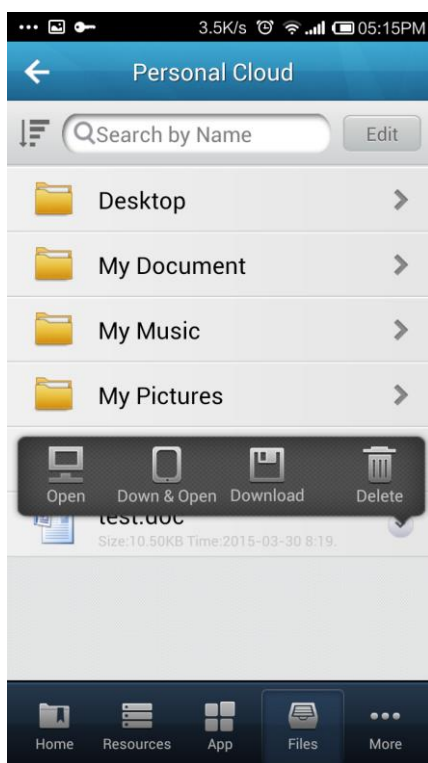


Figure 11

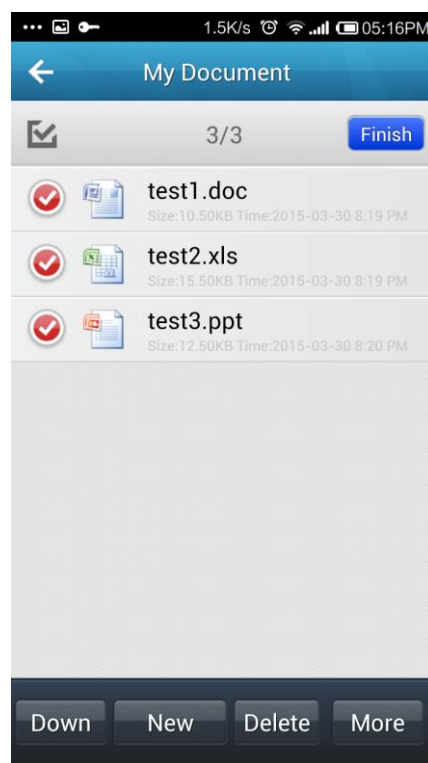


Figure 12

Take the remote application **office2003_Word_x86** shown in Figure 7 as example. Open it and you will see a floating toolbar. Tool icons are listed on the toolbar, namely, cursor, magnifier, keyboard, navigation, program list, menu and a button to hide toolbar.

Private directory and public directory, as well as local storage are available to this remote application. Camera installed on mobile device can be invoked in this remote application. The new photos can be uploaded to remote application. You can choose image quality when uploading image, as shown in Figure 13. You can also share it on EasyConnect through the built-in sharing feature of mobile device. After clicking on **Share**, you need to specify a directory on remote storage server to save the image. Then you can insert that image into the previously-opened Word document.

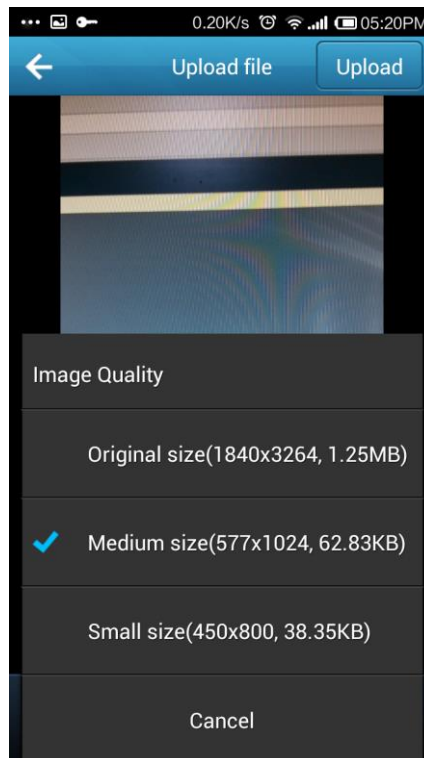


Figure 13

Configuring Firewall Rule

Adding SNAT Rule

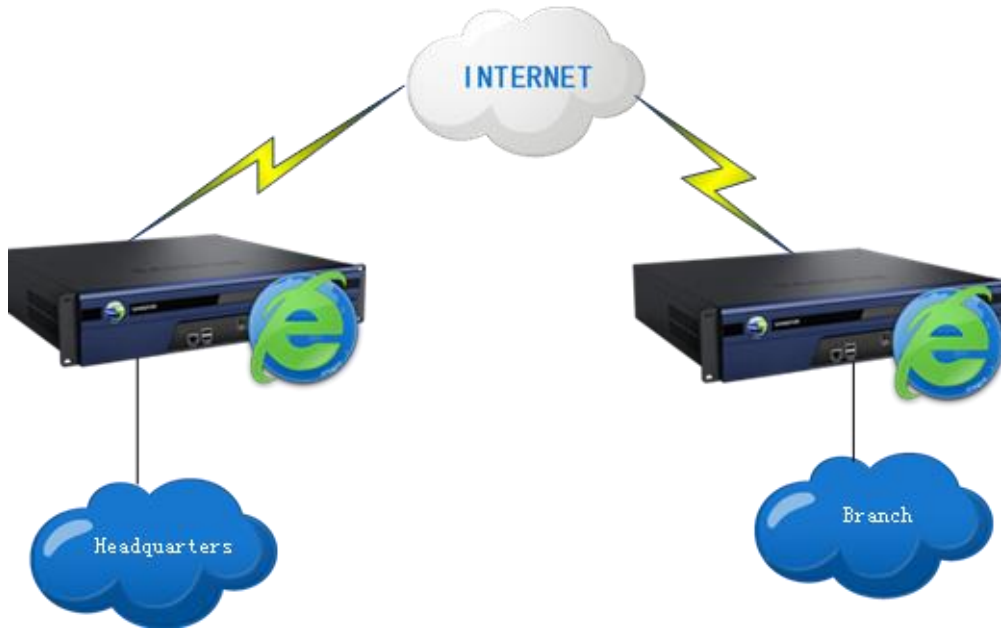
Background:

- 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:

The screenshot shows the 'Edit DNAT Rule' configuration page. The 'Name' field is set to 'Proxy VPN Users'. The 'Original Data Packet' section is expanded, showing the following configuration:

- 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

The 'Translate Src To' section has the following options:

- Interface IP
- Specified IP

The 'Enabled' checkbox is checked, and the text 'Firewall will let matching packets pass' is displayed. The 'Save' and 'Cancel' buttons are visible at the bottom.

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:

Name:

Original Data Packet

Source

Interface:

Line:

Subnet:

Netmask:

Prompt: 0.0.0.0
means any IP address

Protocol:

Destination IP:

Destination Port:

Translated Data Packet

Interface:

Destination IP:

Destination Port:

Enabled Firewall 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.

Typical Case Study

Required Environment

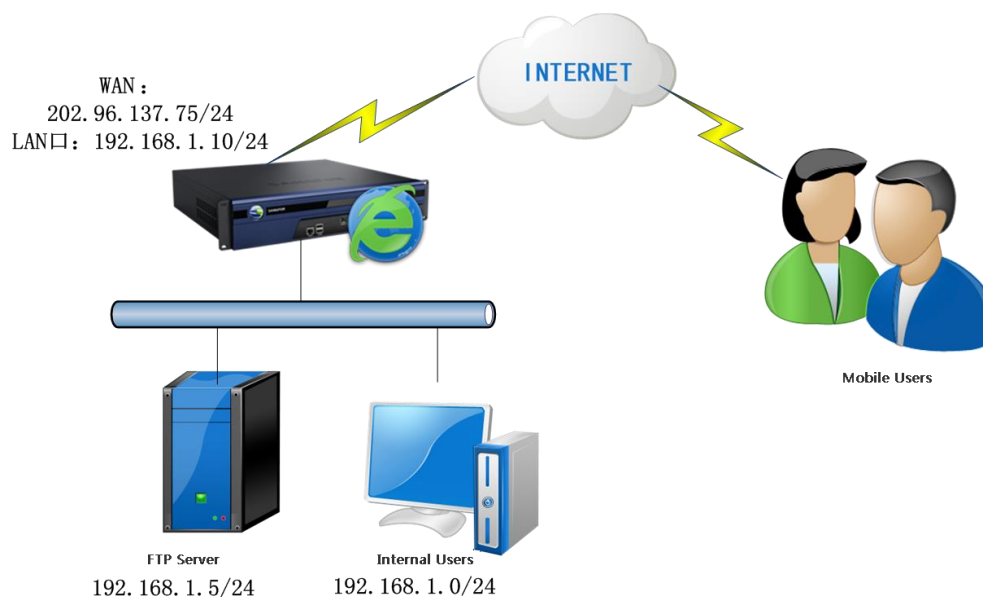
Background:

Sangfor device is deployed in Gateway mode and connected to Internet directly.

Purpose:

Mobile employees can access internal FTP server over SSL VPN and log in to SSL VPN automatically after their mobile device starts up.

Network Topology:



Configuration steps:

1. Deploy and connect related device as shown in the above network topology.
2. Create SSL VPN user and the resource which will be accessed by mobile users
3. Configure Sangfor device to enable user to log in SSL VPN automatically after mobile device starts up

Configuring Sangfor Device

1. Navigate to **System > Network > Deployment**, select Gateway as **Deployment Mode** and

configure LAN interface, as shown below:

Deployment

Mode: Single-Arm Gateway

WAN and LAN interfaces need to be configured.

Internal Interfaces

LAN:

IP Address: 192.168.1.10 *

Netmask: 255.255.252.0 *

Multi-IP

DMZ:

IP Address: 10.10.2.88 *

Netmask: 255.255.255.0 *

Internet line will be displayed under **External Interfaces** section and click corresponding line to configure it, 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 address and DNS server below

IP Address: 202.96.137.75 Preferred DNS: 202.96.134.133

Netmask: 255.255.255.0 Alternate DNS: 202.96.128.168

Default Gateway: 202.96.137.1 *

MTU: 1500

Multi-IP

Advanced

Save Cancel

2. Add a SNAT rule on the **Firewall > NAT > SNAT Rule** page, as shown below:

Name: x

Original Data Packet

Source

From Interface: ▾

Subnet:

Netmask:

Destination

Interface: ▾

Line: ▾

Subnet:

Netmask:

Prompt: 0.0.0.0
means any IP address

Translate Src To

Interface IP

Specified IP

Enabled Firewall will let matching packets pass

3. Go to **System > SSL VPN Options > General > Login** page to specify HTTP port and HTTPS port and configure WebAgent, as shown below:

Login Client Options Virtual IP Pool Local DNS SSO Resource Options

Login Port

HTTPS Port:

HTTP Port:

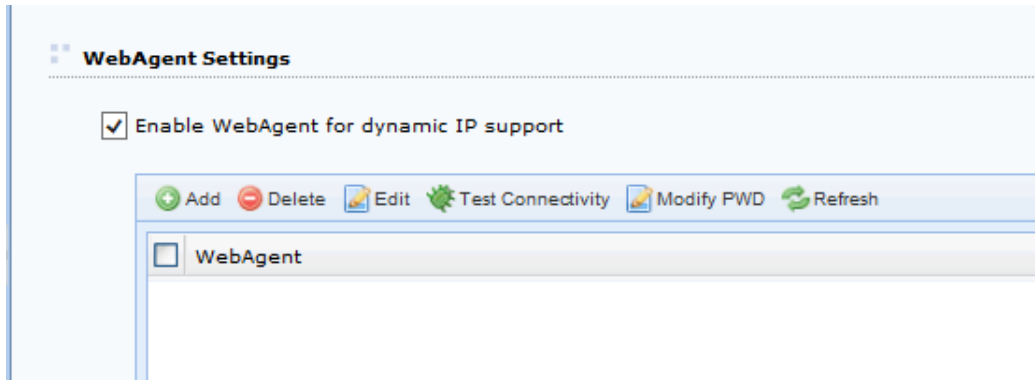
PPTP/L2TP Connection Options

PPTP/L2TP Connection: Prohibit PPTP/L2TP incoming connection

Permit PPTP incoming connection

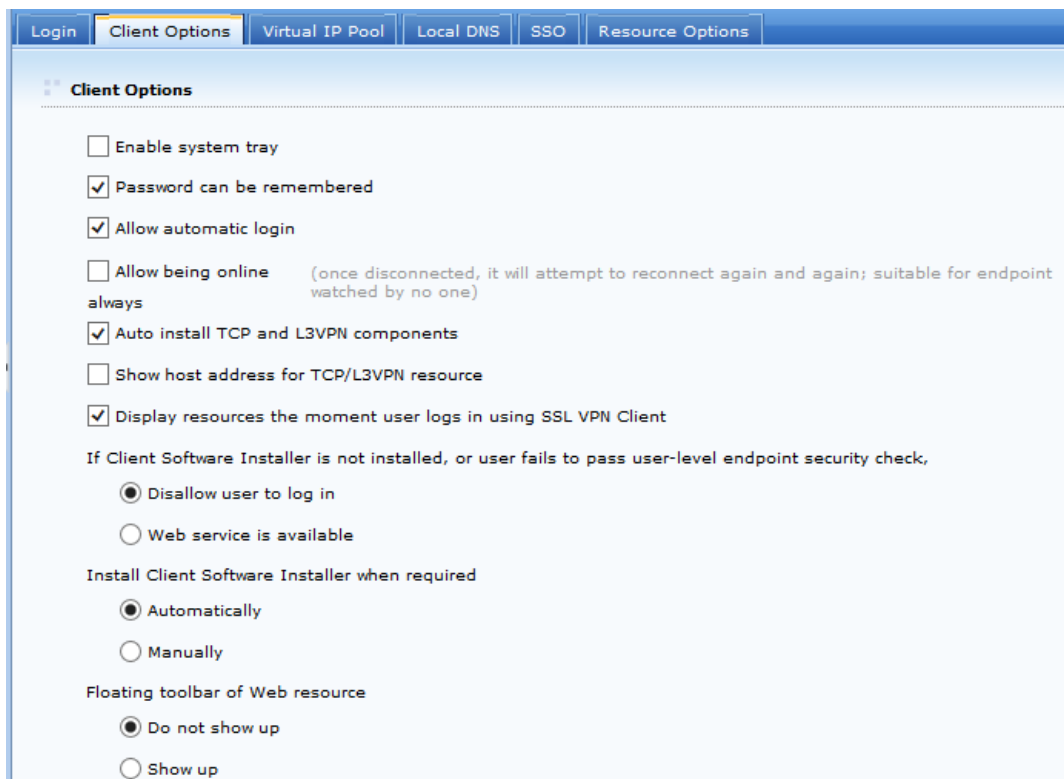
Permit L2TP incoming (standard IPsec VPN will be unavailable. Shared key can not contain quotation mark)

L2TP Shared Secret:



- Port 443 is default HTTPS port. If it is modified, you need to append it following the URL of Sangfor device when accessing SSL login page. Do not modify it unless necessary.
- If Sangfor device has no fixed public IP address, you can use WebAgent to discover IP address.

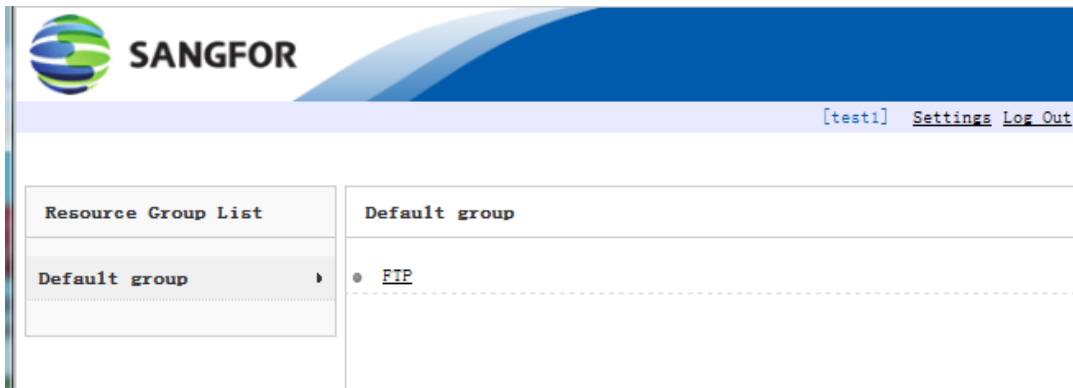
4. Go to **System > SSL VPN Options > General > Client Options** page to configure related options for this scenario, as shown in the figure below:



5. Go to **SSL VPN > Users > Local Users** and click **Add > User** to add a user named **test1**, as shown below:

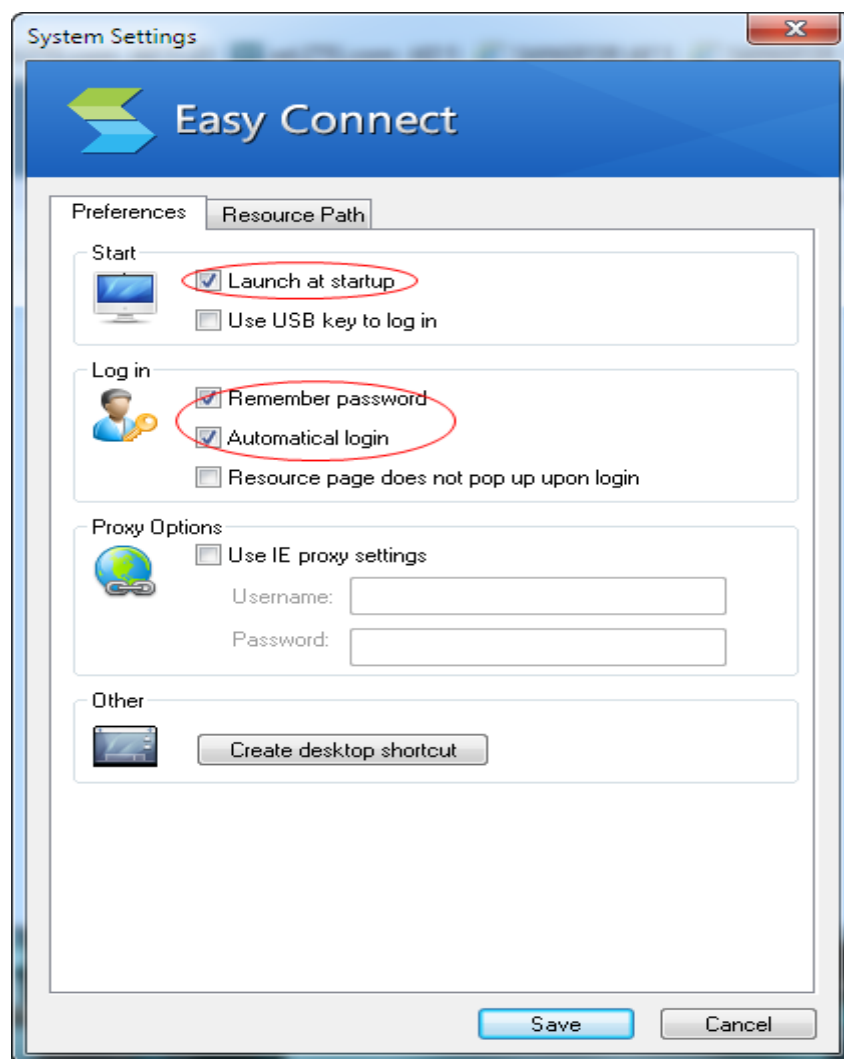
6. Add a TCP app, named FTP, on **SSL VPN > Resources** page, as shown below:

7. Go to **SSL VPN > Roles > Role Management** page to create a role and associate it with the user **test1** created in step 7 and the TCP resource created in step 8(for detailed guide, refer to Adding Role in Chapter 4).
8. Click Save to save all the changes and click **Apply** button to apply the settings.
9. After user **test1** logs in to SSL VPN, he/she will see the following resource page:



To access FTP server, click on the FTP link.

10. Right-click on VPN client logo and click **System Settings** and select related options, as shown below:



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

Appendix A: End Users Accessing SSL VPN

This section introduces how end users configure browser and log in to SSL VPN.

Required Environment

- End user's computer can connect to the Internet.
- No security assistant software is installed on the computer, because this kind of software may influence the use of SSL VPN.
- Any mainstream browser is installed on the computer, such as, Internet Explorer (IE), Opera, Firefox, Safari, Chrome, etc.



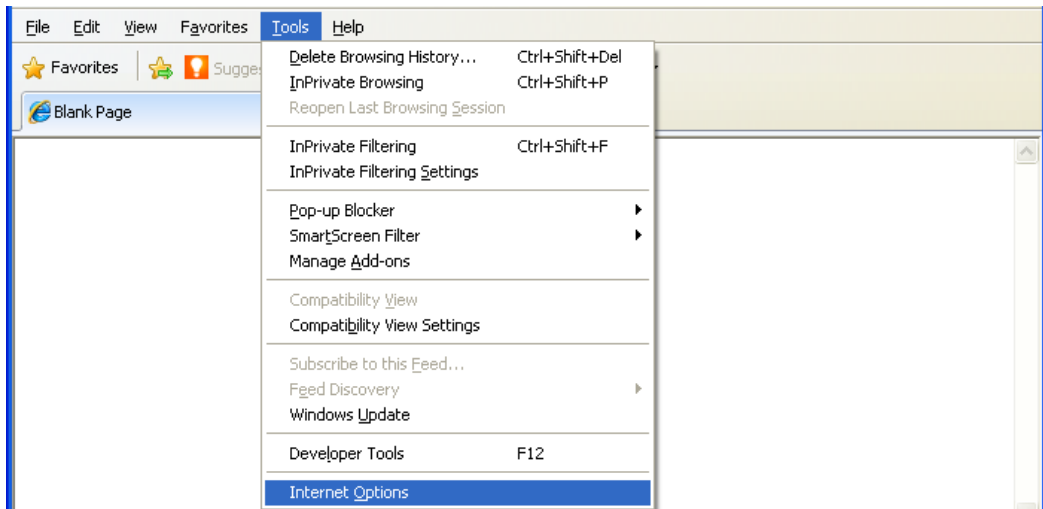
-
- Operating systems should be 32bit/64bit Windows XP/2003/Vista/Win7/Win10, 32bit Linux Ubuntu 11.04/RedHat 5.2/RedFlag/Fedora 13/SUSE 11.2, or Mac OS X Leopard(10.5)/Snow Leopard(10.6)/Lion(10.7).
 - SSL VPN client is available on iPhone and Android mobile phones.
-

Configuring Browser and Accessing SSL VPN

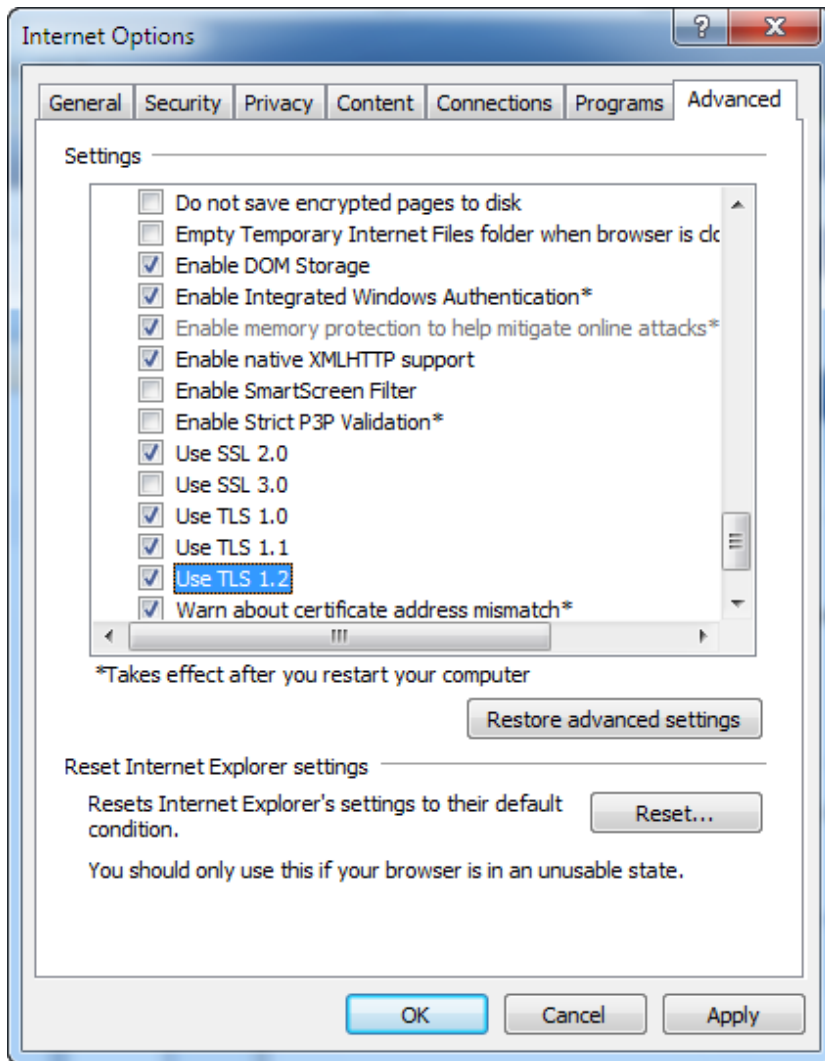
Configuring Browser

The following configuration takes Windows XP IE browser for example. Screenshots may vary with different operating systems.

9. Launch the IE browser and go to **Tools > Internet Options** to configure the IE browser, as shown in the figure below:



10. Click **Advanced** tab. Find the **Security** item and select the checkboxes next to **Use SSL 2.0**, and **Use TLS 1.0**, as shown in the figure below:

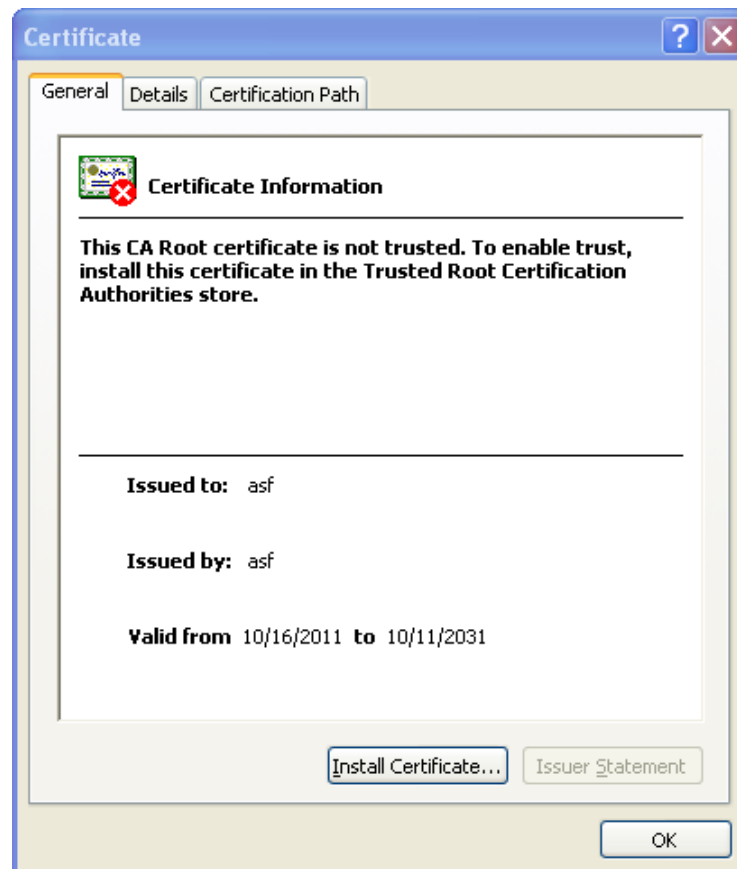


11. Enter the SSL VPN address into the address bar of the browser and visit the login page to SSL VPN.

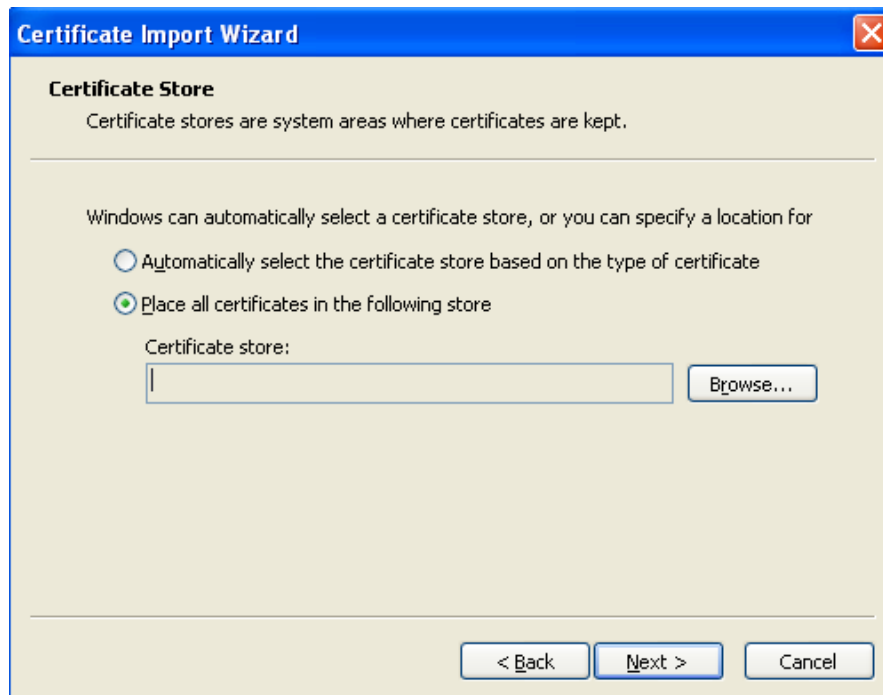
12. When you visit the login page, a security alert may appear, requiring installation of security certificate, as shown in the figure below:



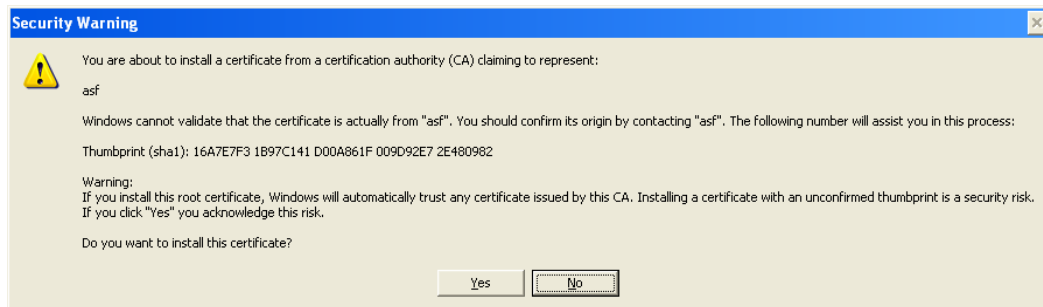
13. Click the **View Certificate** button to complete installing the root certificate if this is the first time you log in to SSL VPN administrator Web console. The information of the root certificate is as shown below:



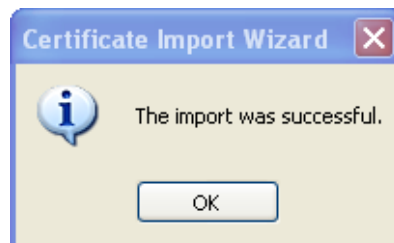
14. Click the **Install Certificate** button and use the **Certificate Import Wizard** to import the root certificate, as shown in the figure below:



15. 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:



16. Click the **Yes** button to ignore the warning and the root certificate will be installed, as shown in the figure below:



Generally, root certificate is required to be installed when you logs in to the SSL VPN for the first time. Once root certificate is installed, you need only click the **Yes** button next time when logging in and see the security alert.

Using Account to Log In to SSL VPN

If root certificate has been installed, user can visit the login page to the SSL VPN. The login page is as shown in the figure below:

Access SSL VPN

Username:

Password:

Verification: t NZ q

Log In

Other Login Methods:

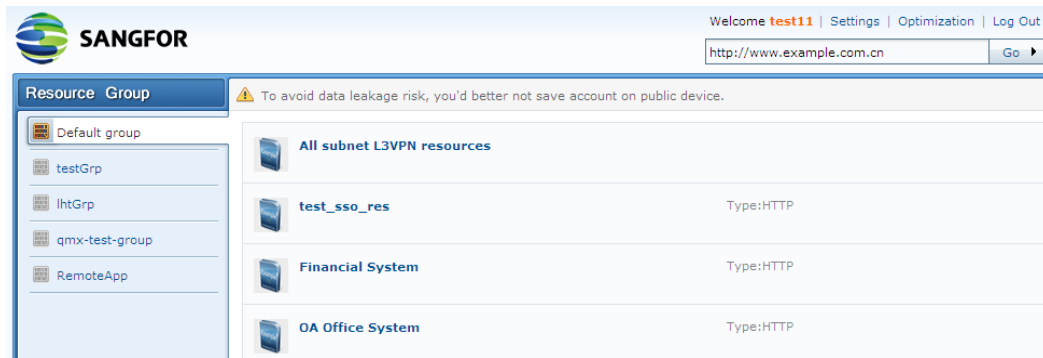
- Failed to read USB key. Please [install USB key driver](#).
- Login error. Please download SSL VPN repair tool to [repair components](#).
- For more help information, [click here](#)

7. Enter and submit the required credentials through the login page. The following are the contents included on the login page:
 - **Username, Password:** Enter the username and password of the SSL VPN account to connecting to the SSL VPN.
 - **Verification:** Enter the word on the picture. Word verification feature adds security to SSL VPN access and could be enabled by administrator manually, or activated automatically when brute-force login attempt is detected.
 - **Use Certificate:** A login method that enables user to use certificate to go through the user authentication. The certificate should have been imported to the IE browser manually.
 - **Use USB Key:** A login method that enables user to use USB key to go through the user authentication. There are two types of USB keys, one type has driver and the other type is driver free.



User using USB key to get authenticated may need to install the USB key driver. For detailed guide, please refer to the SSL VPN Users section in Chapter 4.

8. Once user passes the required primary and secondary authentications, he/she will enter the **Resource** page, as shown in the figure below:



9. 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.

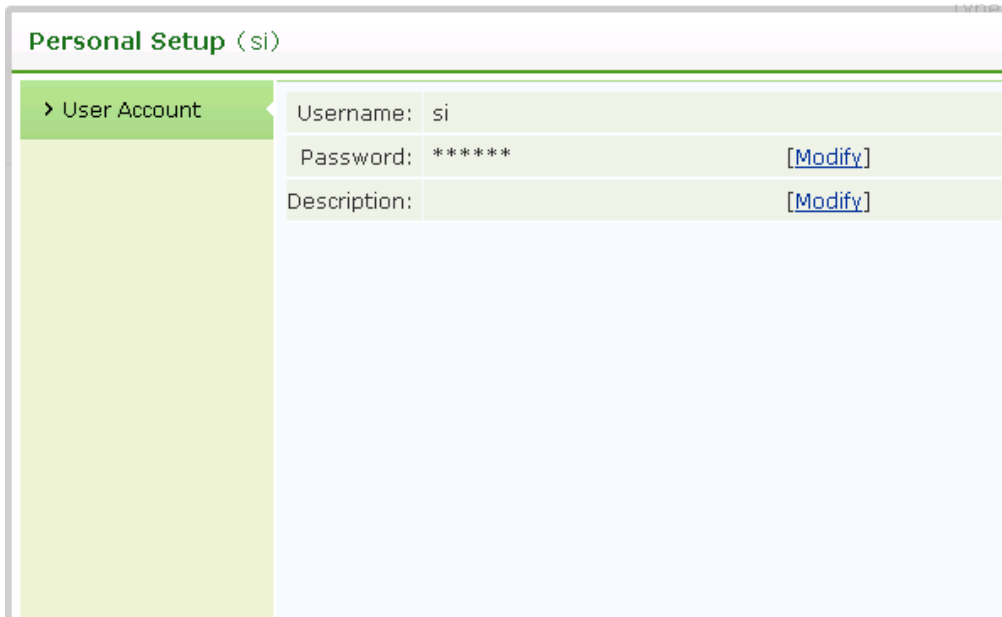
For Web application resources, user can access them simply by clicking on the resource link.

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.

10. TCP and L3VPN components will be installed automatically when user accesses associated TCP resource or L3VPN resource.

Welcome test11 Settings Optimization Log Out	
web17	Type:HTTP
tcp20	Type:HTTP
L3vpn	Type:HTTP
ie	Type:REMOTEAPP

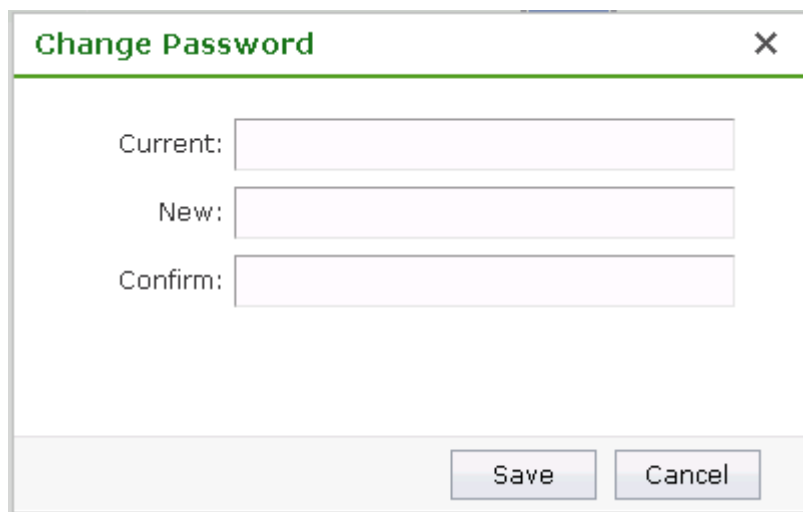
11. To log out of the SSL VPN, click **Log Out** at the upper right of the page. Once user logs out, he/she cannot access the internal resources any more.
12. To modify password of the SSL VPN account, click **Settings** at the upper right of the page to enter the **User Account** page, as shown in the figure below:



The screenshot shows a web interface titled "Personal Setup (si)". On the left, there is a sidebar with a green header "> User Account". The main content area displays a table with the following information:

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

As shown above, the current password is followed by **Modify**. Click it to enter the **Modify Password** page, as shown below:



The screenshot shows a dialog box titled "Change Password" with a close button (X) in the top right corner. It contains three input fields:

- Current:
- New:
- Confirm:

At the bottom right, there are two buttons: "Save" and "Cancel".



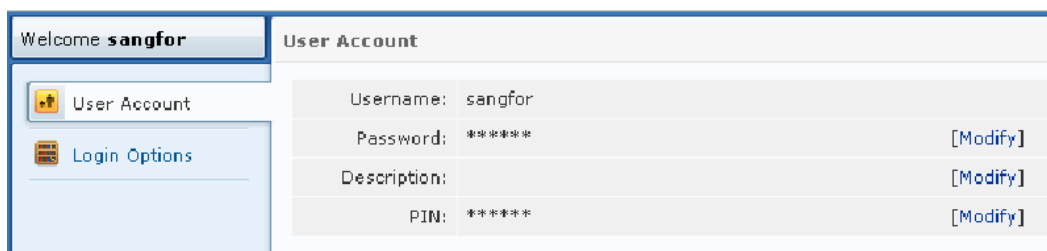
- If user keeps inactive for a long time during SSL VPN access, without performing any operation or accessing any resource, user will be disconnected and log out automatically.
- The contents shown in **Settings** are related with SSL VPN configurations. Those contents will be taken valid.

Using USB Key to Log In to SSL VPN

User login using USB key is a bit different from that using account.

Main differences are the login process and login page. User should perform the following:

6. Launch the browser and visit the login page to the SSL VPN.
7. Insert the USB key into the USB port of the computer.
8. Select other login method **Use USB Key** to enter the next page that asks for PIN of the USB key.
9. Enter PIN of the USB key and login process completes.
10. To modify PIN of the USB key, click **Settings** at the upper right of the **Resource** page to enter **User Account** page, as shown below:



Click **Modify** to enter the **Edit USB Key PIN** page, enter the current PIN and the new PIN and click the **Save** button, as shown below:

Edit USB Key PIN [\[Close\]](#)

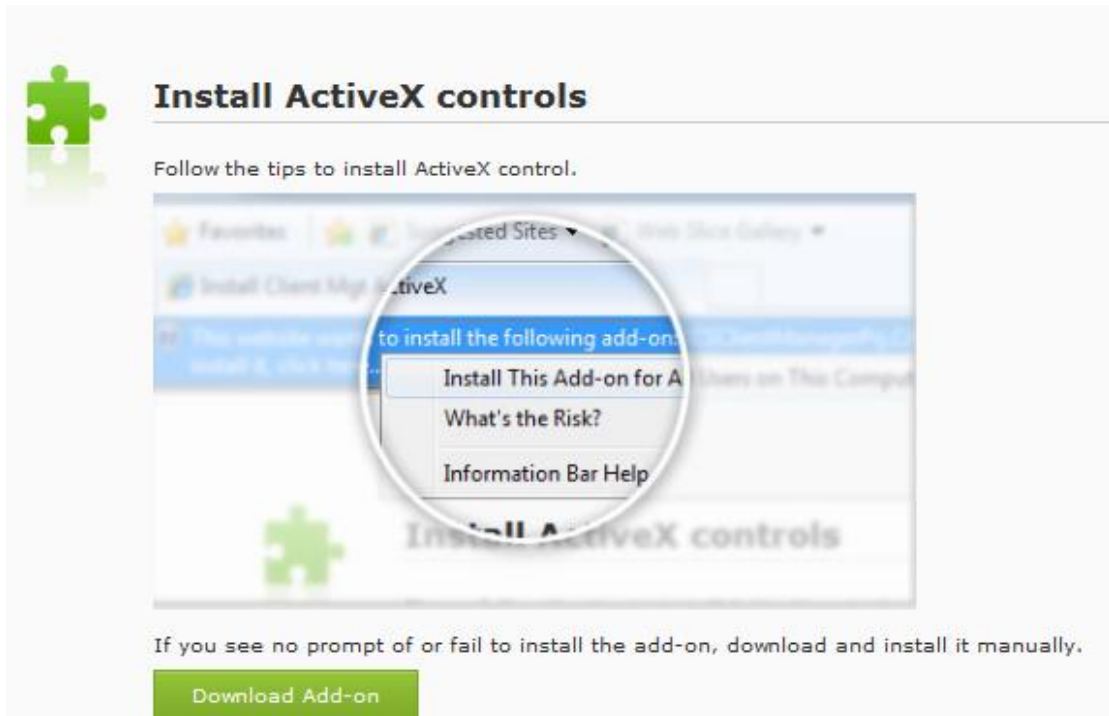
Current PIN:

New PIN:
(case-sensitive, 4-16 characters)

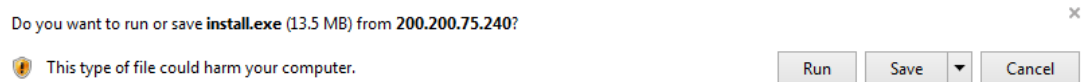
Confirm PIN:

Using VPN Client to Log In SSL VPN

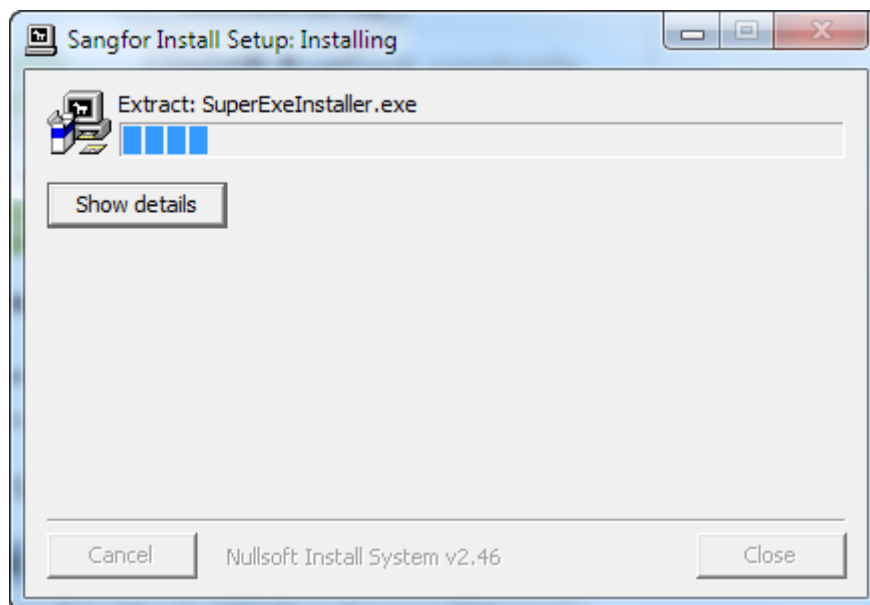
SSL VPN client components will be installed automatically when user logs in SSL VPN through IE browser. On **System > SSL VPN Options > Client Options** page, you can enable client software installer to be installed automatically or manually when required. If **Manually** corresponding to the **Install Client Software Installer when required** option is selected on the Sangfor device, the following page will pop up when user logs in VPN, as shown below:



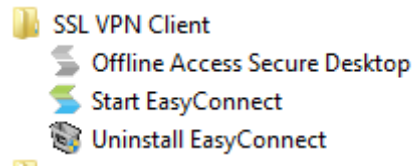
Click **Download Add-on**, a dialog appears, as shown below:



To install it, click **Run**. You will see the following installation page.

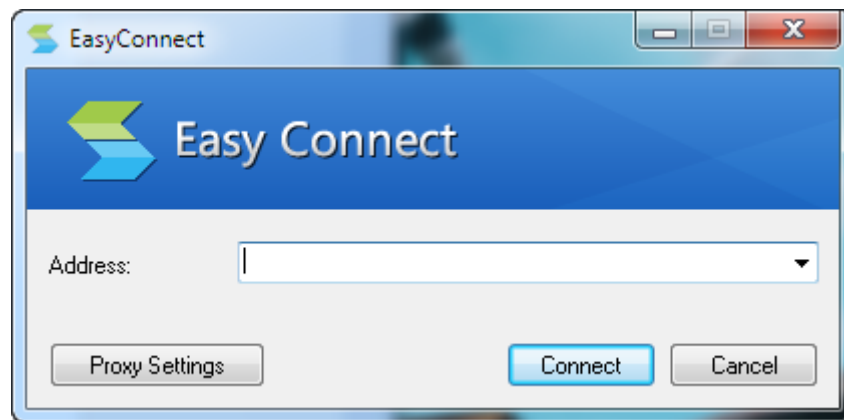


After software installer is installed, navigate to **Start > Programs** and you will see the following directory, as shown below:

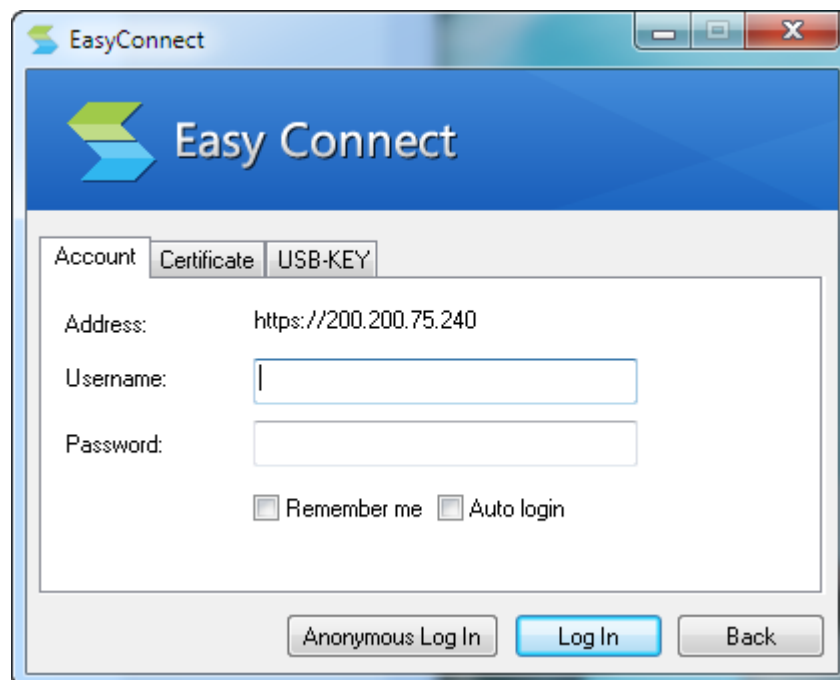


Please terminate firewall and antivirus software when installing client software installer; otherwise, the client will fail to be installed.

4. Click **Start EasyConnect** to open the SSL VPN client window, as shown below:

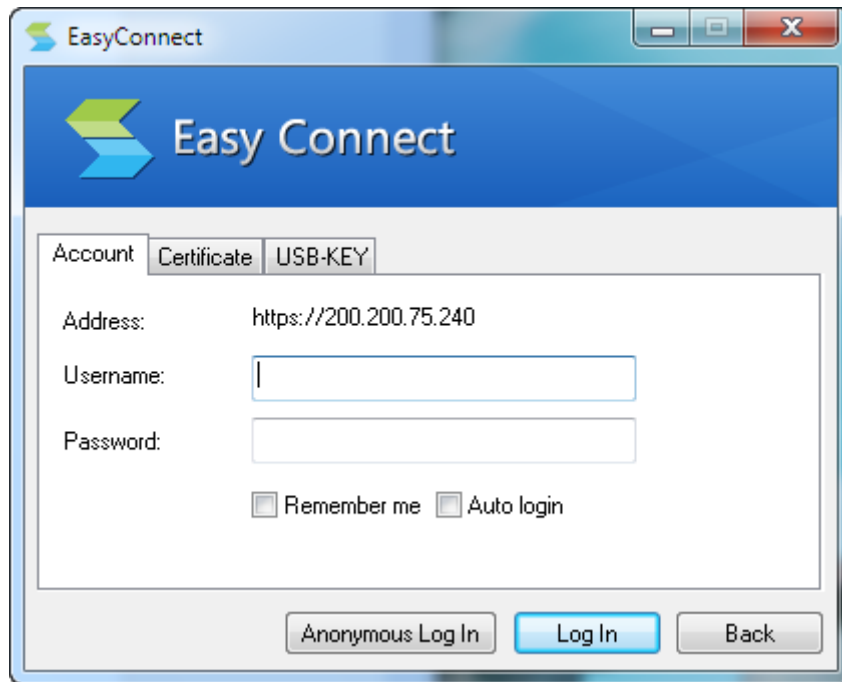


5. Enter the address of SSL VPN and click **Connect**, the following dialog appears.



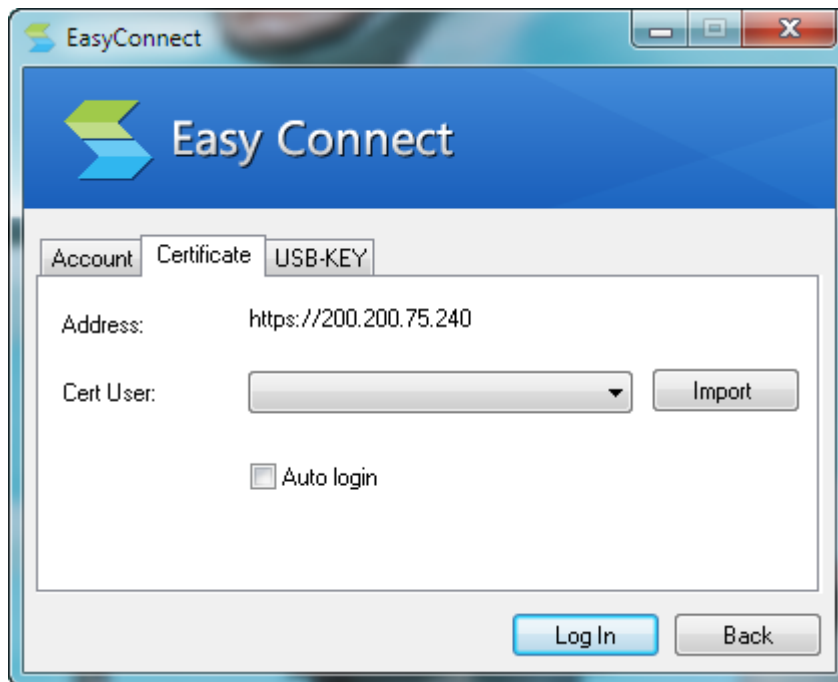
- For authentication based on username and password, select **Account**. The **Account** tab is as

shown in the figure below:

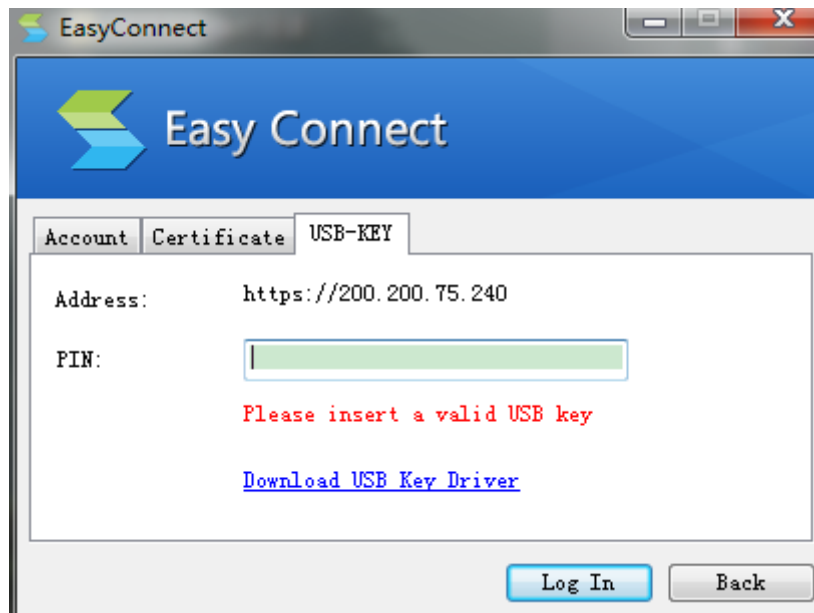


User can select **Remember me** and **Auto login** options if required, then he/she does not need to enter these information upon next login. The two options are available only when they are enabled on the device(for details, refer to Client Options in Chapter 3).

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



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

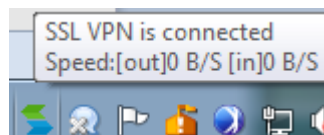


To create SSL VPN user, refer to Adding User in Chapter 4.

6. Select an authentication method as per your case. After logging in, a prompt dialog appears, as shown below:



If system tray is enabled when configuring Client Options on Sangfor device, the VPN client logo will be shown on the lower-right corner of the desktop. Put the cursor on it, you can see the connection status and VPN flow speed, as shown below:



To view VPN connection status and configure VPN-related settings, right-click on the **System Tray** icon and you will see the following floating window, as shown below

