SANGFOR SSL VPN

Quick Start Guide

This document is intended to assist users to install, debug, configure and maintain SANGFOR SSL VPN device quickly and efficiently.

Please read the followings carefully when you come across any problem on handling the device, and take any of the measures below:

1. Deploy and configure the SANGFOR SSL VPN device as instructed in this quick configuration guide. User manual and other related electronic materials can be downloaded at SANGFOR forum or official website.
2. Contact your hardware supplier (contractor) for technical support. To provide customers with fast and satisfying after-sale services, SANGFOR has assigned professional and qualified technicians to all distributors. Onsite and remote support will be provided for some special cases.
3. Go to SANGFOR forum to search for a solution if you do not need urgent response.
4. Contact SANGFOR Customer Service. Describe the issue in detail and notify your location and device supplier to SANGFOR Customer Service Representative. He/she will provide you the solution and let you know where you could contact and obtain technical support efficiently.
5. Please contact us through the followings:

   Forum: http://forums.sangfor.com/index.php

   Website: www.sangfor.com.cn

   Tel: 4006306430 (dial via telephone or mobile phone)

   Email: support@sangfor.com.cn

Table of Contents

Table of Contents 3
Declaration 4
Preface 5
Chapter 1: Knowing Your VPN Device 6
Operating Environment 6
Connecting to Power Supply 6
Network Interfaces 6
Connecting VPN Device 7
Chapter 2: Logging In to Administrator Console 9
Chapter 3: Deploying/Configuring VPN Device 11
VPN Device in Gateway Mode 11
VPN Device in Single-Arm Mode 14
Chapter 4: Setting Server&Client to Access SSL VPN 18
Configuring SSL VPN Server (VPN Device) 18
Configuring SSL VPN Client to Enable Auto-Login 22
Chapter 5: Modifying Administrator Password 25

Declaration

Preface

This configuration guide only offers the basic information of deploying and configuring the SANGFOR SSL VPN device. For detailed information, you can refer to the electronic user manual contained in the attached CD media or visit SANGFOR forum to download the user manual (under [Materials&Files] > [SSL VPN] > [User Manual]).

Note:

This quick start guide applies to all the models of SSL VPN devices. The device we use for example in this guide is M5100. Though product specifications may vary from model to model, configuration and usage are generally the same.

Chapter 1: Knowing Your VPN Device

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

Operating Environment

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

To ensure endurance and stability of the SSL VPN device, please ensure the followings:

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

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

Connecting to Power Supply

Connect the SSL VPN device to 110V/230V AC. Please check whether the power supply is well grounded before plugging in the VPN device.

Network Interfaces

Above is the front panel of a SANGFOR SSL VPN device (M5100). The interfaces from left to right are described as below:

Interface	Default IP Address	Description
CONSOLE	N/A	Network interface used for high availability (HA)
ETH0	10.254.254.254/24	LAN interface of the device
ETH1	10.254.253.254/24	DMZ interface of the device
ETH2	N/A	WAN1 interface of the device
ETH3	N/A	WAN2 interface of the device

Note:

- The picture above (M5100) is just for reference. The actual product you purchased and received may vary.
- If there are **ETH4** and/or **ETH5** port(s) on the front panel, **ETH4** is the third WAN interface (WAN3) and **ETH5** is the fourth WAN interface (WAN4).

Connecting VPN Device

1. Attach power supply to VPN device. Plug the power cable into the power interface on the rear panel of the device and switch on the power supply.

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

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

Note:

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

2. Use RJ-45 straight-through Ethernet cable to connect the **LAN** interface (**ETH0**) to the internal network (LAN).
3. Use RJ-45 Ethernet crossover cable (568A-568B) to connect the **WAN** interface (**ETH2)** to the external network, (i.e., router, optical fiber transceiver or ADSL Modem for external network).

Note:

Multi-line function allows multiple Internet lines to be connected to SSL VPN device. When you deploy multiple lines, please connect the second Internet line to WAN2 interface (**ETH 3**) and the third Internet line to WAN3 interface (**ETH4**), and so on.

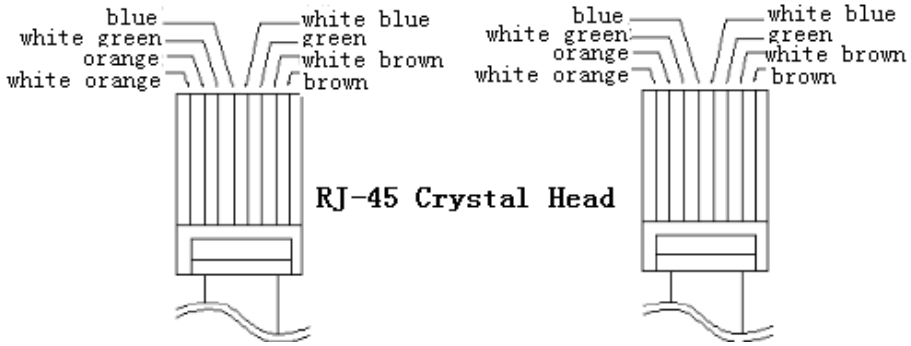
4. If you want the SSL VPN device to provide secure protection for DMZ (Demilitarized

Zone), use RJ-45 Ethernet cable to connect **ETH1** interface to the devices such as Web server, Mail server that provides services to external networks.

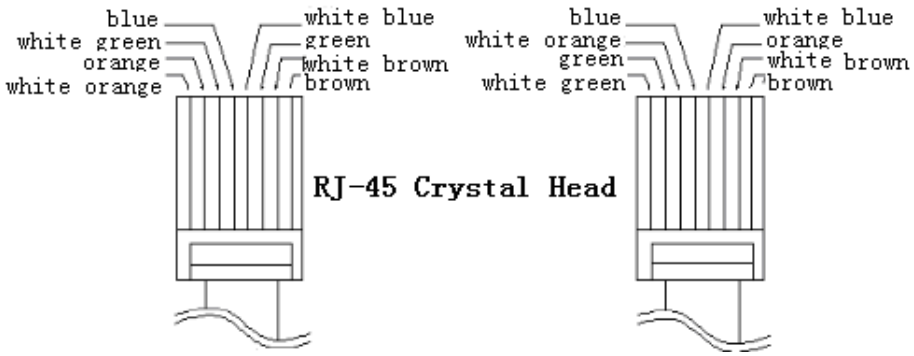
Note:

- Use crossover cable to connect **WAN** interface **(ETH2/3)** to the external network.
- Use straight-through cable to connect **LAN** interface **(ETH0)** to the internal network.
- For direct access to administrator Web console, use crossover cable to connect **LAN (ETH0)** interface to the computer.
- If session cannot be established but the corresponding LED indicates normal working status, please check whether the right type of cables are being used. The differences between straight-through cable and crossover cable are shown in the figures below:

1. Wire Sequence of Straight-through Cable



2. Wire Sequence of Crossover Cable

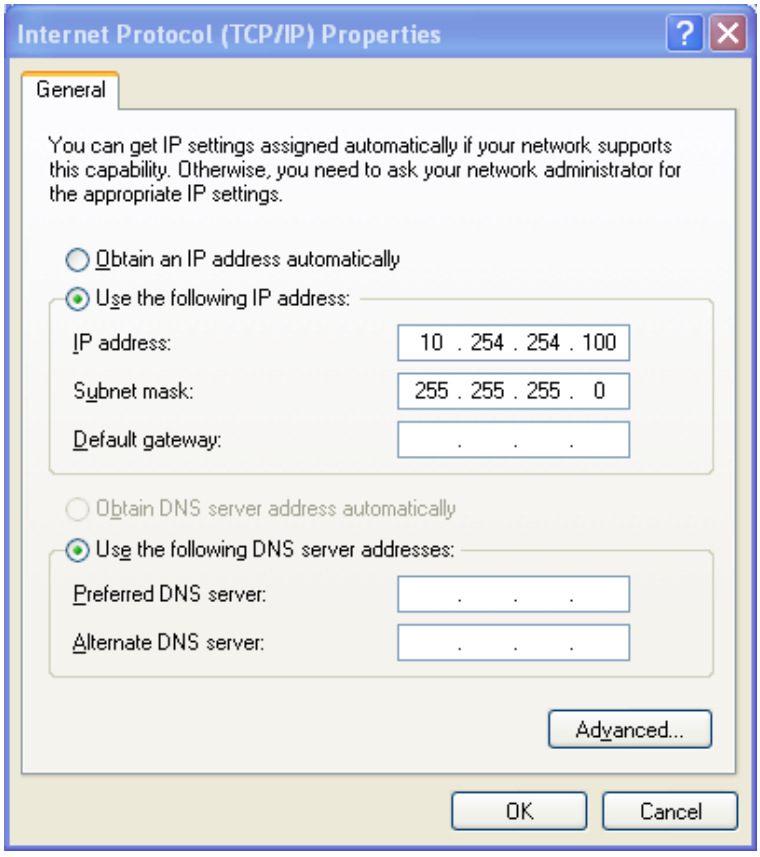


Chapter 2: Logging In to Administrator Console

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

Please perform the following steps:

1. Connect the PC's network interface card (NIC) and the VPN device's **ETH0** interface to a same layer-2 switch, or connect the PC's NIC to VPN device's **ETH0** interface directly with a network cable.
2. Add an IP address on the PC, an IP address that resides in the network segment **10.254.254.X** (for instance, 10.254.254.100) with subnet mask **255.255.255.0**, as shown in the figure below:



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

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

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

Chapter 3: Deploying/Configuring VPN Device

This chapter introduces the ways to deploy the device and complete basic settings.

SANGFOR SSL VPN device supports two deployment modes, **Gateway** mode and **Single-Arm** Mode.

VPN Device in Gateway Mode

About Gateway Mode

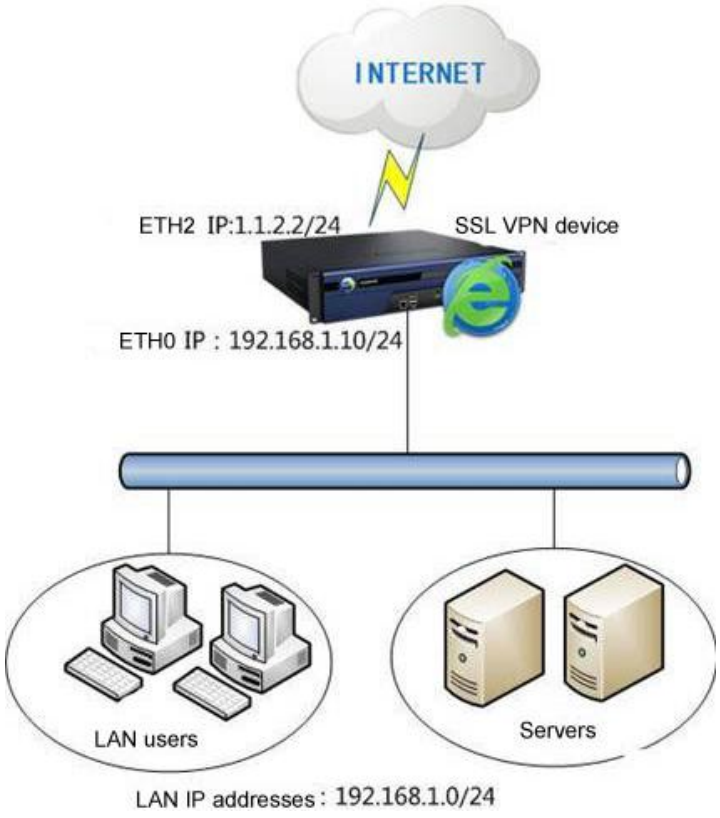
Under Gateway mode, SSL VPN device works as a router and you need to configure the internal interface (LAN and DMZ) and external interfaces (WAN). It can also work as a simple firewall device if you configure SNAT (Source Network Address Translation) rule and DNAT (Destination Network Address Translation) rule.

Scenario 1: Deploying/Configuring VPN Device in Gateway Mode

Prerequisite:

The enterprise network has one Internet line. A router for the external network is acting as the outgoing device.

Network topology example:

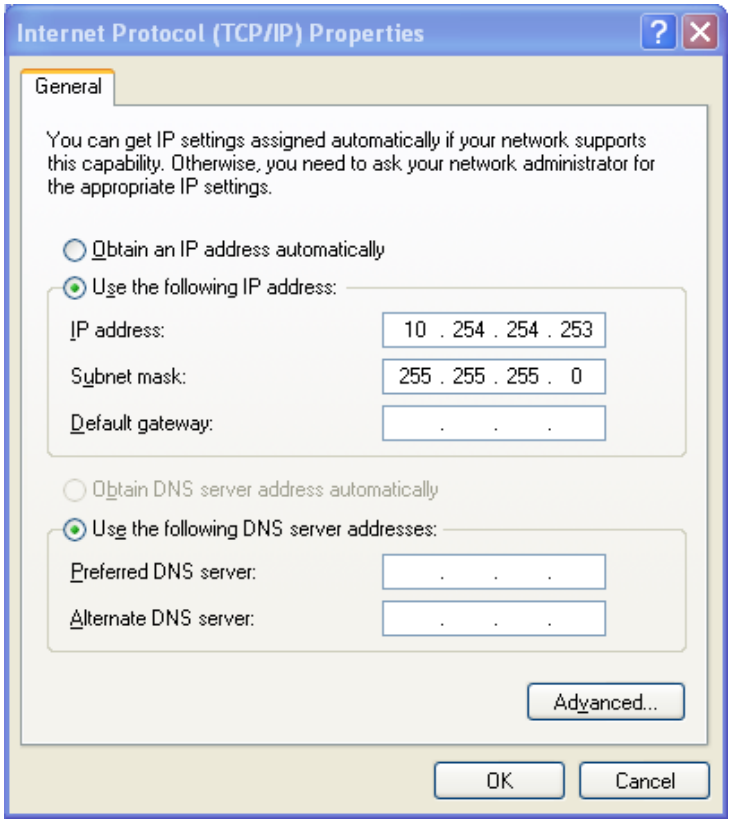


The followings are to be achieved:

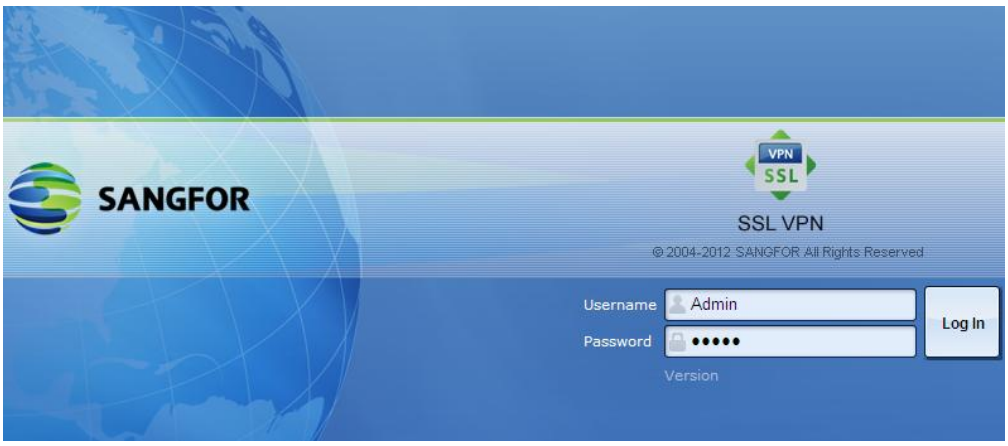
1. VPN device is deployed in Gateway mode and at the exit of the internal network
2. VPN device accesses the Internet on behalf of the LAN users and servers, allowing SSL VPN access.

Procedures to configure SSL VPN device in Gateway Mode:

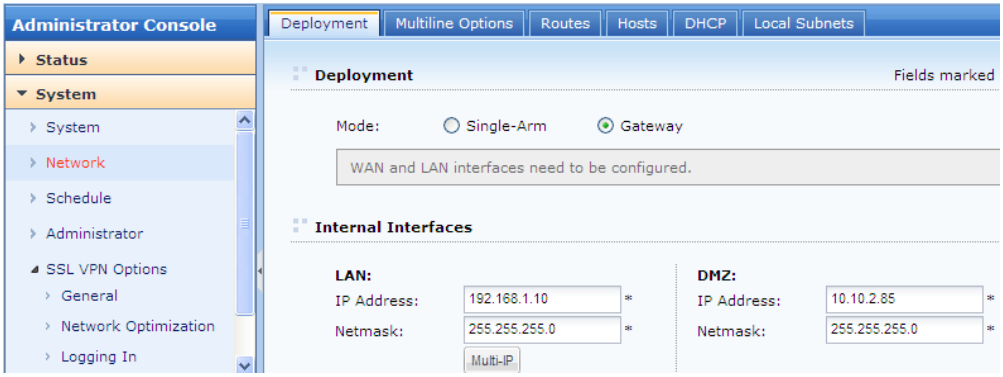
1. Attach the power supply to VPN device, connect and turn on the VPN device (for detailed steps, please refer to Chapter 1 Knowing Your VPN Device).
2. Turn on the computer that you want to use to log in to the administrator Web console and enter the IP address **10.254.254.253**, as shown in the figure below:



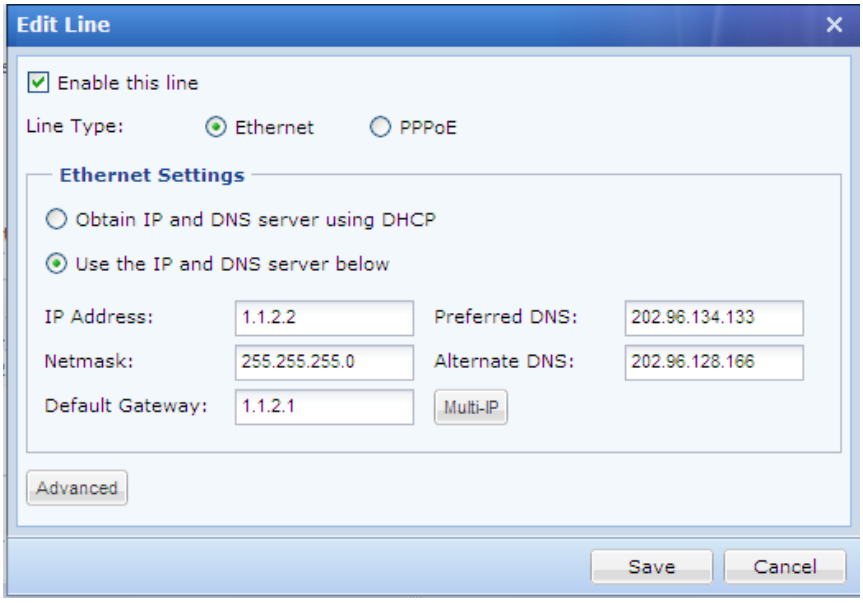
3. Open Internet Explorer (IE) browser and visit https://10.254.254.254:4430. You are to enter the login page to administrator Web console (as shown in the figure below). Log in using the default administrator credentials. Username and password are **Admin** (case-sensitive).



4. Navigate to [System] > [Network] > [Deployment], choose **Gateway** mode and configure the required fields, as shown in the figure below:



5. To configure external interface (WAN), click the line name to edit the line, as shown in the figure below.



6. Configure an SNAT rule to enable this SSL VPN device to access the Internet on behalf of LAN users and server. Navigate to [Firewall] > [NAT] > [SNAT Rule], create a SNAT rule and add the source IP addresses into the Source Address field (as shown in the

figure below).

7. When the above configuration is completed, connect the LAN interface of the VPN device to the internal network and the WAN interface to the external network.
8. Till then, Gateway mode deployment is completed.

Warning:

At the second step, you can also add an IP address that resides in the same network segment as DMZ interface (IP: 10.254.253.254). In that case, you should connect the **ETH1** interface to the computer at the first step and visit the address https://10.254.253.254:4430 at the third step.

VPN Device in Single-Arm Mode

About Single-Arm Mode

Single-Arm mode is a deployment approach used by majority of our customers, for this type of deployment does not require any change to the original network architecture. To set up, you need connect the LAN interface (**ETH0**) of the device to the switch for internal network. The VPN device deployed in Single-arm mode mainly establishes a dedicated SSL VPN tunnel to let mobile users access resources over SSL VPN.

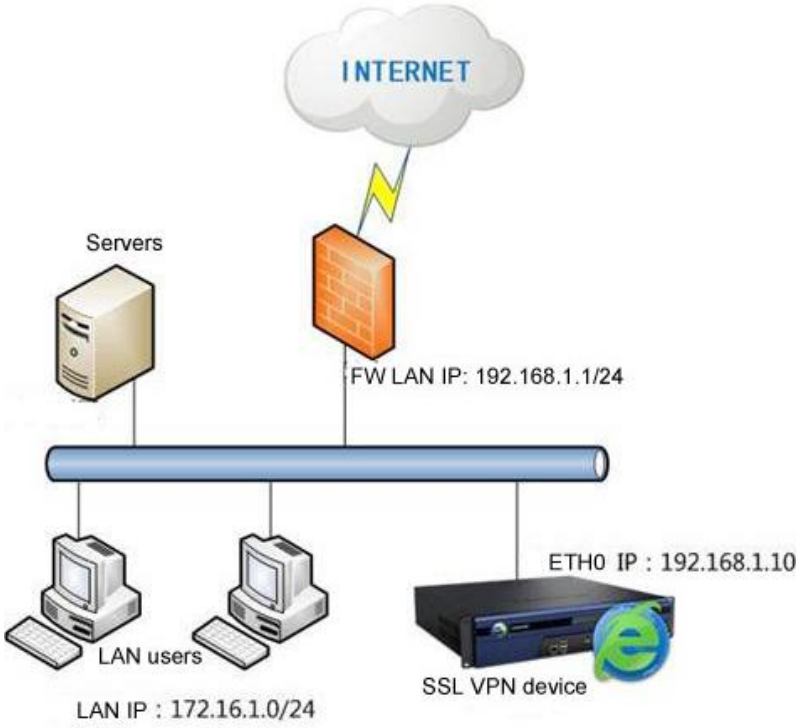
Scenario 2: Deploying/Configuring VPN Device in Single-Arm Mode

Prerequisite:

a) LAN users and servers connect to the Internet directly.

b) VPN device is deployed in Single-Arm mode and connects to layer-3 switch, achieving SSL VPN functionality.

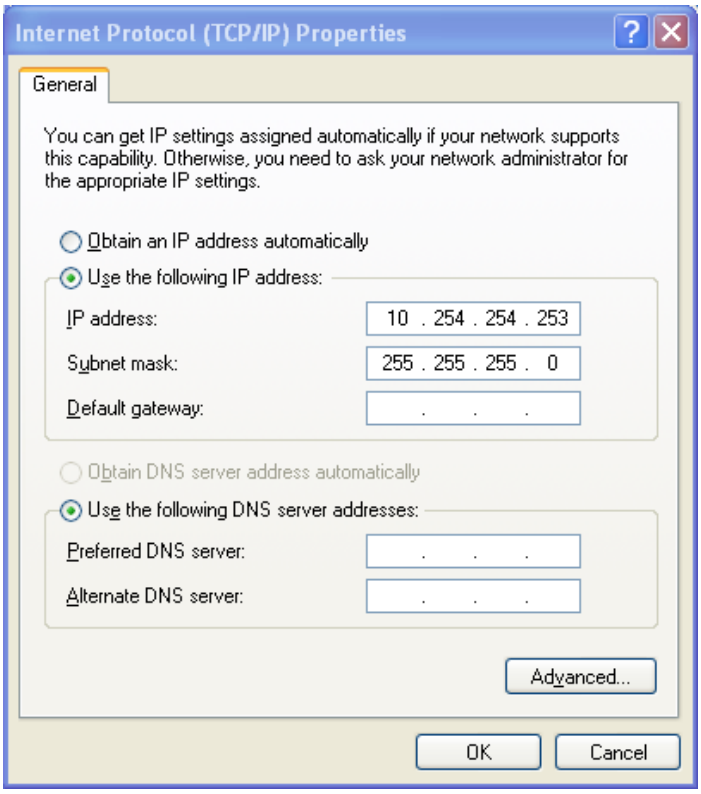
Network topology example:



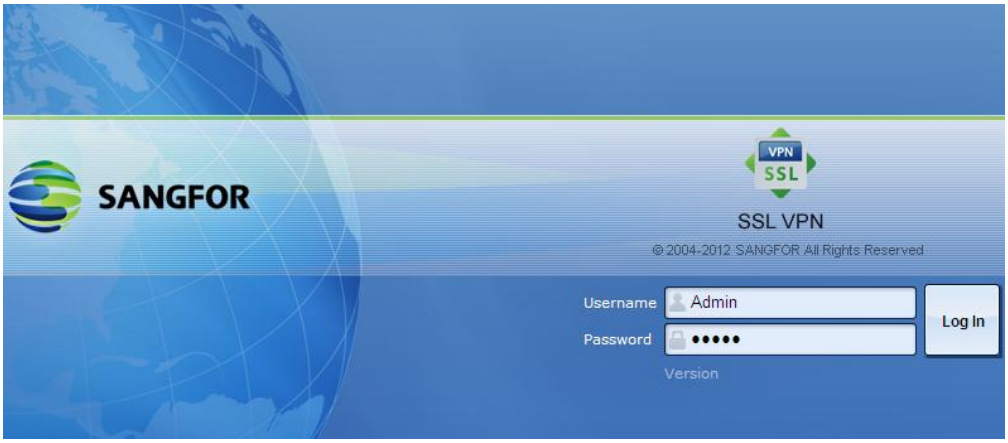
To configure Single-Arm mode, please perform the following steps:

1. Attach the power supply to VPN device, connect and turn on the VPN device (for detailed steps, please refer to Chapter 1 Knowing Your VPN Device).

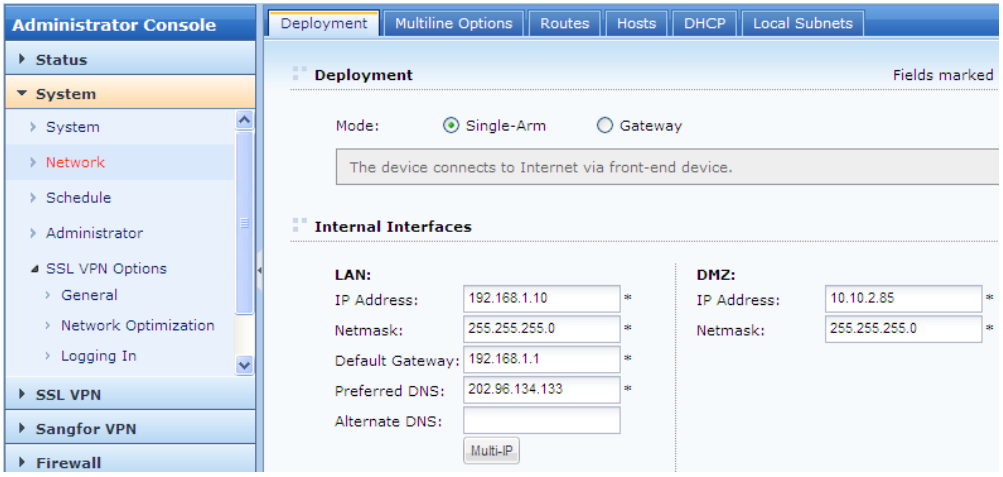
2. Turn on the computer that you want to use to log in to the administrator Web console and add the IP address **10.254.254.253**, as shown in the figure below:



3. Open Internet Explorer (IE) browser and visit https://10.254.254.254:4430. You are to enter the login page to administrator Web Console, as shown in the figure below. Log in using the default administrator credentials. Username and password are **Admin** (case-sensitive).



4. After logging in to the Administrator console, navigate to [System] > [Network] > [Deployment], choose **Single-Arm** mode and configure the required fields, as shown in the figure below:



5. Configure a DNAT rule on the front-end firewall. As the VPN device is placed in internal network and to act as server to enable mobile employees to access SSL VPN, you need to configure a DNAT rule on the front-end firewall device to map the ports to VPN device, so that the VPN device can connect to the Internet. By default, the port used for establishing SSL VPN tunnel is TCP port 443. Since the settings on firewall devices of different venders vary, we are not to provide the screenshots here.
6. When the above configuration is completed, connect the LAN interface (**ETH0**) of this VPN device to the switch for internal network and check whether you can log in to the administrator Web console.
7. Till then, Single-Arm mode deployment is completed.

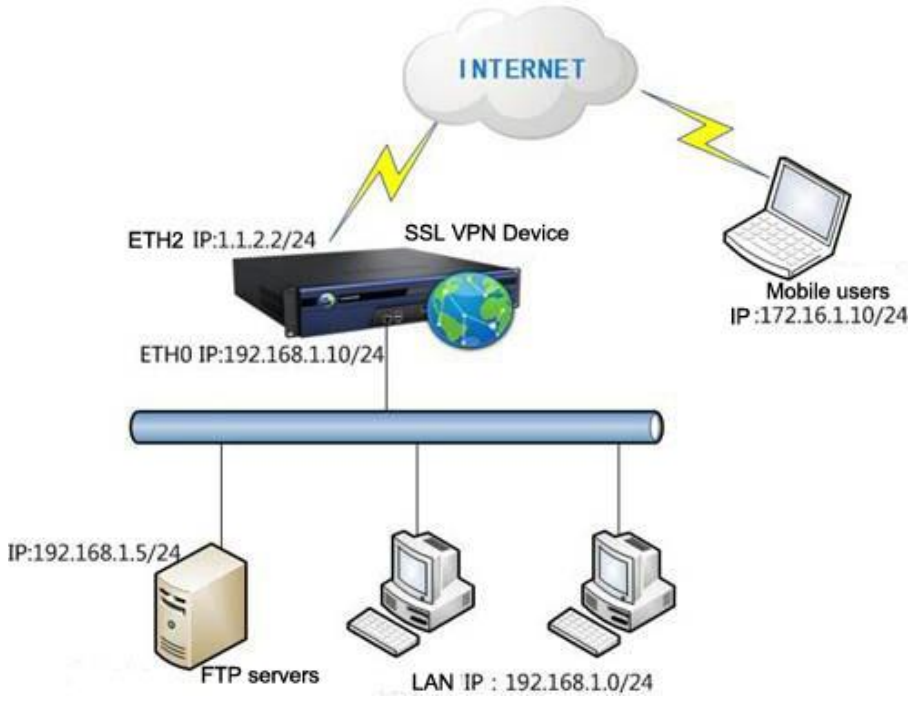
Warning:

- The port 443 is a default VPN listening port. You can modify it but should be noted that this port should be the one you configured while creating port mapping rule on the frontend device.
- To deploy the SSL VPN device in Single-arm mode, you should connect its LAN interface (**ETH0**) to the switch for internal network.

Chapter 4: Setting Server&Client to Access SSL VPN

The followings are to be achieved:

- SSL VPN device is deployed in Gateway mode and acts as gateway of the enterprise network, accessing the Internet on behalf of the LAN users and servers.
- The mobile employees can connect to corporate FTP server over SSL VPN, and optionally auto log in to SSL VPN.

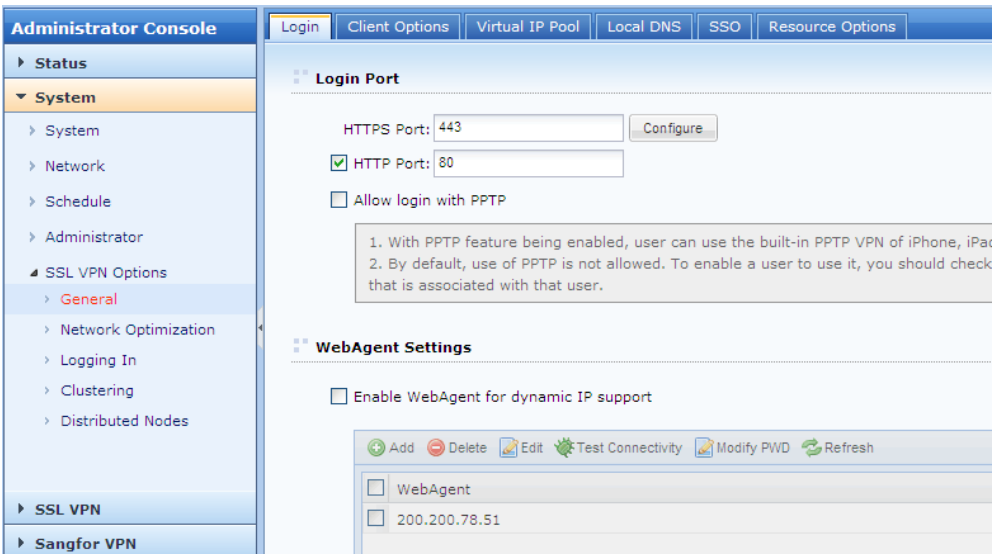


For configuration, three steps should be performed:

1. Deploy SSL VPN device.
2. Configure SSL VPN server. This enables mobile employees to establish SSL VPN session and access specified resources from external networks.
3. Enable automatic login feature on SSL VPN client.

Configuring SSL VPN Server (VPN Device)

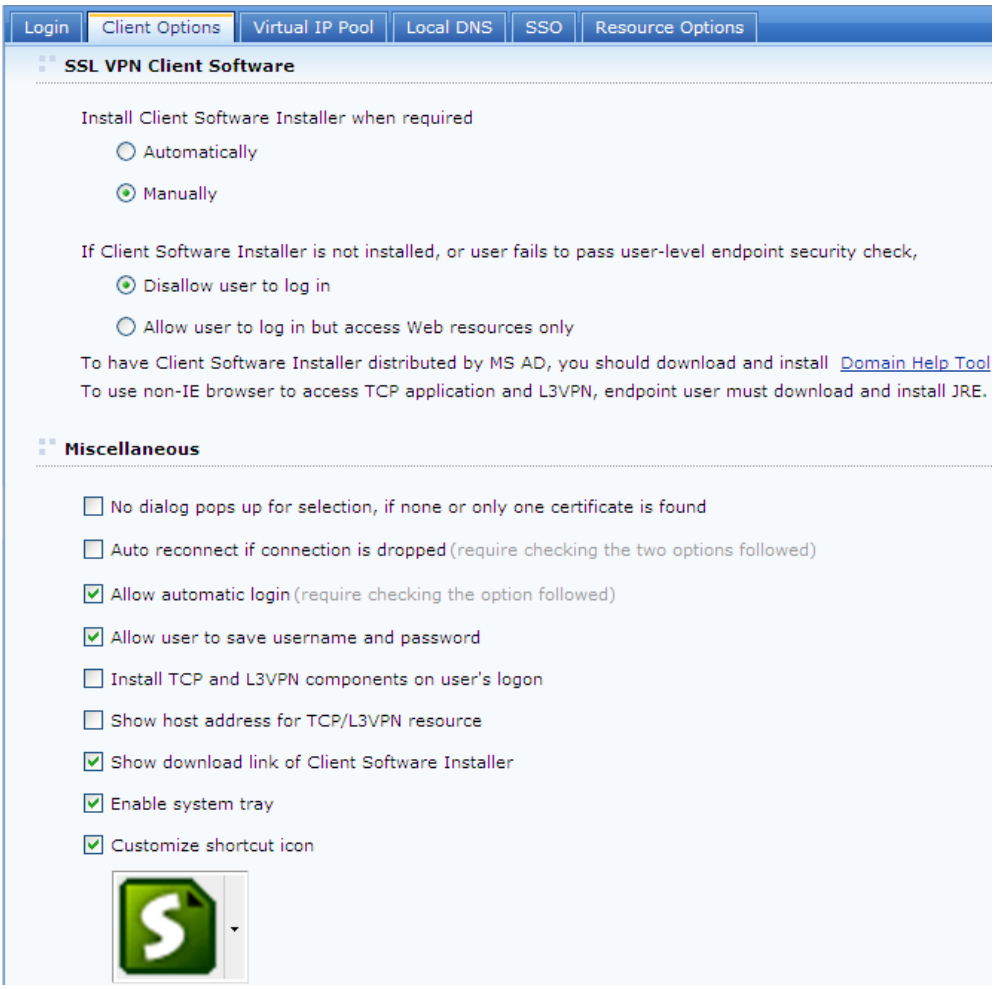
1. Deploy SSL VPN device in Gateway mode (please refer to Chapter 3 Deploying/Configuring VPN Device).
2. Navigate to [System] > [SSL VPN Options] > [General] > [Login] and configure the login ports and WebAgent, as shown in the figure below:



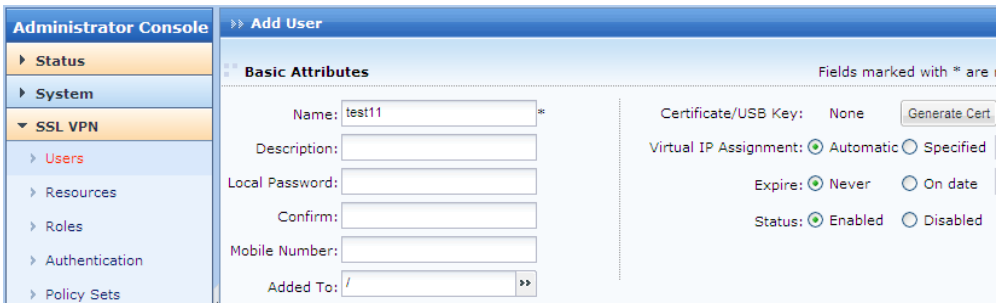
Note:

- Do not modify the port 443 unless it is absolutely necessary. Once it is altered, the new port number should be added to the end of the URL address when endpoint user enters the address to connect SSL VPN.
- If SSL VPN gateway has no static Internet IP address, enable and configure WebAgent to obtain dynamic IP address.

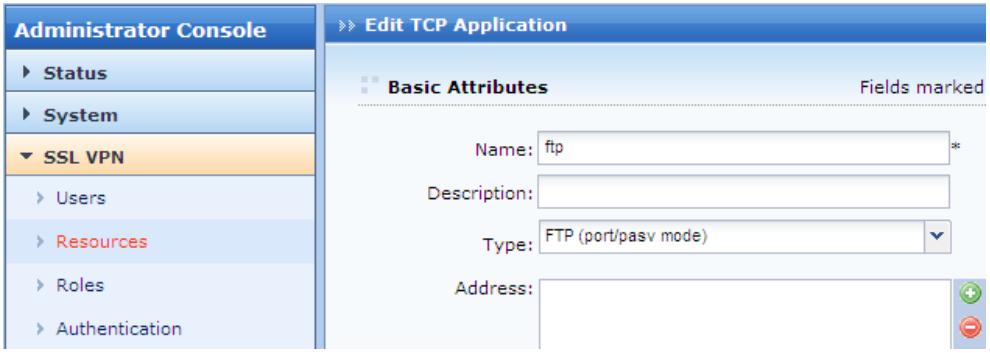
3. Navigate to [System] > [SSL VPN Options] > [General] > [Client Options] to configure VPN Client related options (as shown in the figure below). Select the [Allow automatic login] and [Allow user to save username and password] options.



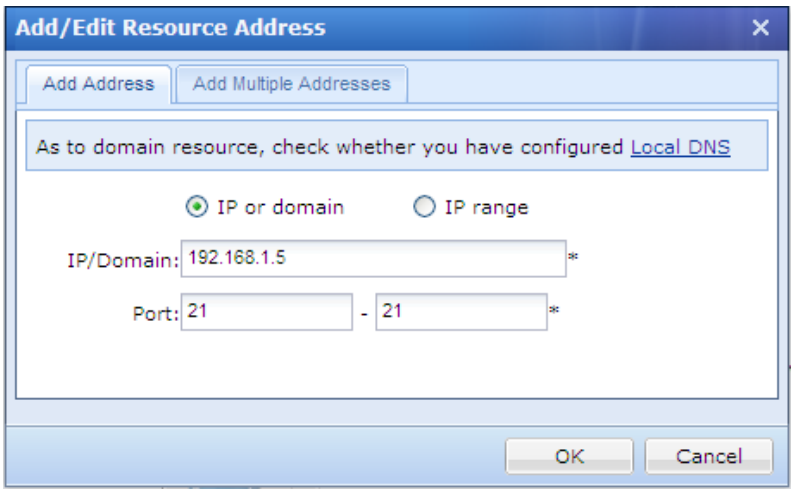
4. Create a user account. Navigate to [SSL VPN] > [Users] and click [Add] to enter the [Add User] page, as shown in the figure below:



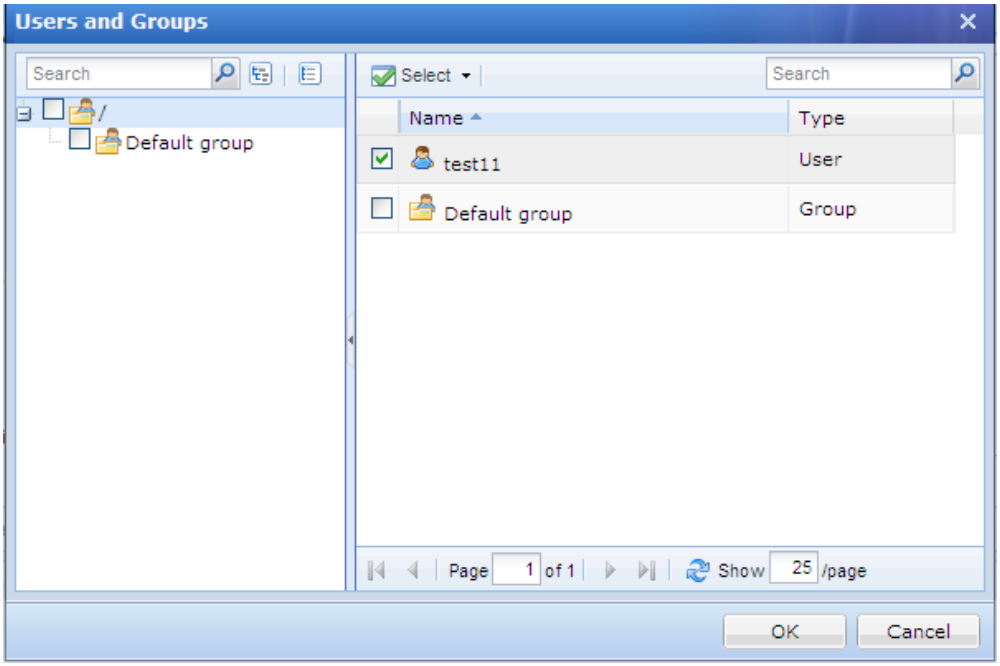
5. Add resource. Navigate to [SSL VPN] > [Resources] and click [Add] to add a TCP application. The [Edit TCP Application] page is shown in the figure below:



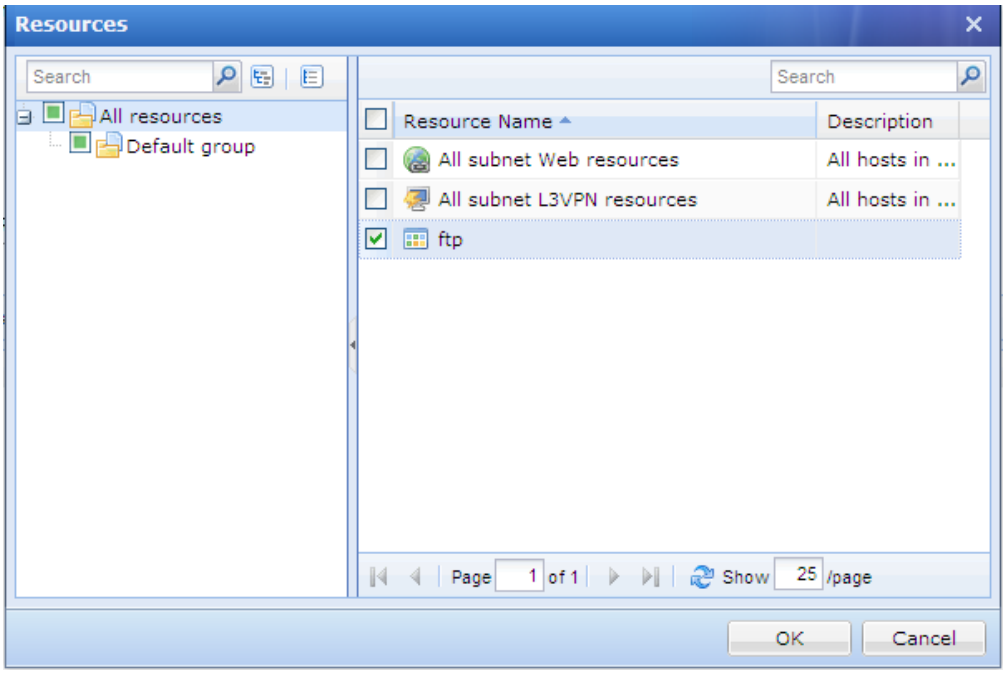
Enter the name, and configure the resource address by clicking the **Add** icon next to the textbox. The [Add/Edit Resource Address] page is as shown in the figure below:



6. Create a role. Navigate to [SSL VPN] > [Role] and click [Add] to add a role and assign the role to the user (in this scenario, it is **test11**), as shown in the figure below:



To associate the role with resources, click [Select Resource] on the [Edit Role] page and select the resources (as shown in the figure below). The selected resource will be available to the specified user.



7. When you have completed configuring the [Add Role] page, click <Save> button to save the settings.

Warning:

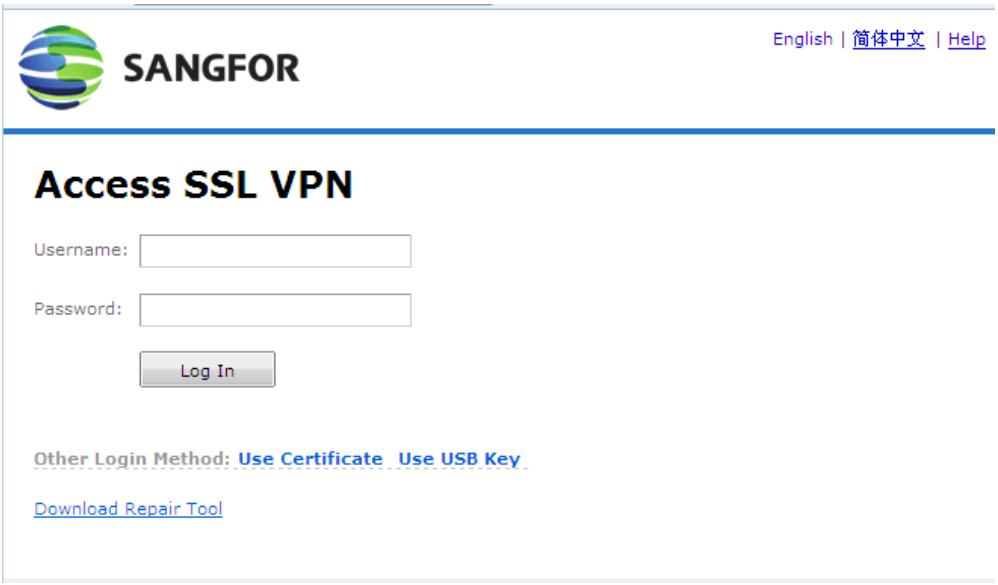
To apply settings or changes, click the <Apply> button at the upper right corner of the next page; otherwise, no change will take effect.

Configuring SSL VPN Client to Enable Auto-Login

The above chapters depict how to complete basic setup of the SSL VPN device. This chapter describes how end users access the designated resources over SSL VPN.

To access the SSL VPN, end users should perform the following steps:

1. Log in to SSL VPN. Open IE browser and enter the SSL VPN address to access the portal. The default login page is shown in the figure below:



2. Enter the SSL VPN account created in Step 4 under Configuring SSL VPN Server.

   After login to SSL VPN, users will see the Resource page. All the resources available to users are listed here, as shown in the figure below:

   SSL VPN client will be installed on user's PC automatically when user logs in to SSL VPN through Webpage for the first time, and be available in Start > Programs (as shown in the figure below). You can use SSL VPN Client program to access SSL VPN.

3. Click Start > Programs > SSL VPN Client > Start VPN and the SSL VPN client appears (as shown in the figure below). Enter the VPN address and click the <Connect> button to connect to the SSL VPN.

4. Once the SSL VPN is connected, enter the SSL VPN account, select the checkbox next to [Auto login] and click the <Log In> button (as shown in the figure below):

5. Till then, all the necessary configurations are completed. Next time, user can connect to SSL VPN by starting SSL VPN client, without entering username and password.

Note:

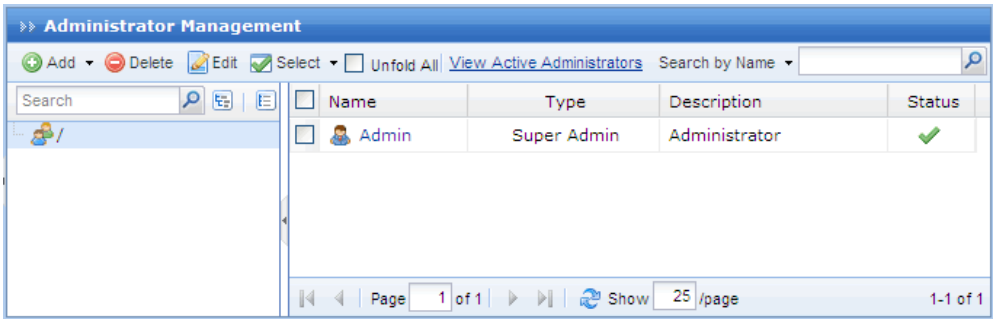
SSL VPN client supports 32bit/64bit Windows XP/2003/Vista/Win7, 32bit Linux Ubuntu 11.04/RedHat 5.2/RedFlag/Fedora 13/SUSE 11.2, and Mac OS X Leopard(10.5)/Snow Leopard(10.6)/Lion(10.7).

Chapter 5: Modifying Administrator Password

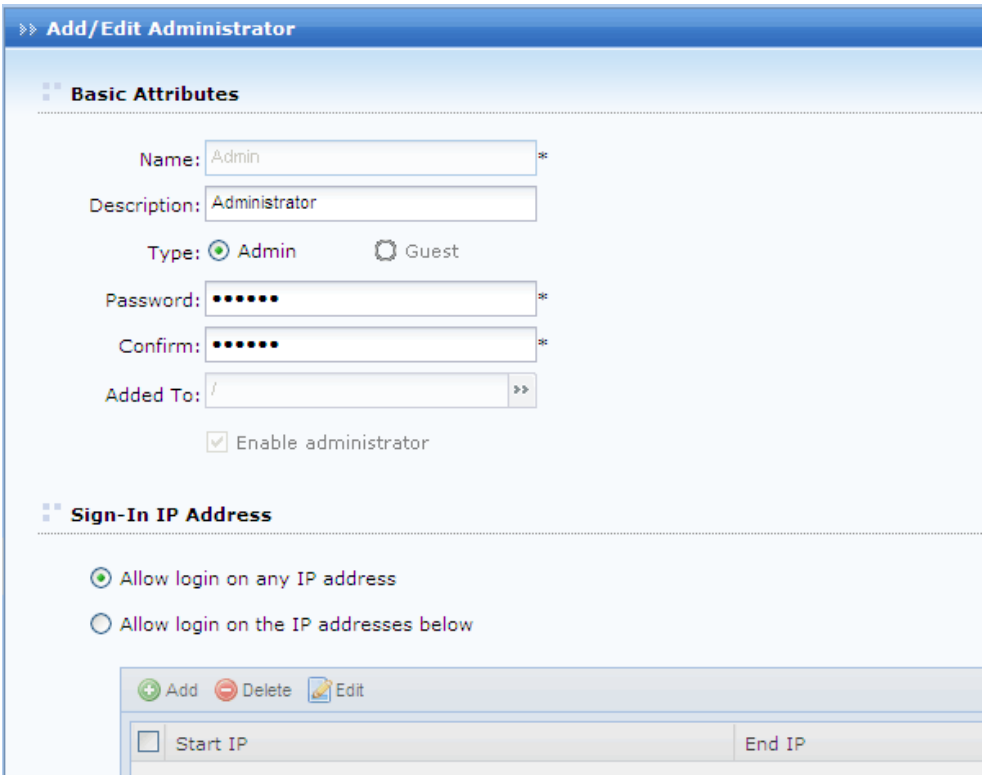
We strongly recommend you to change the password after initial login, so as to prevent others from logging in to the administrator Web console and using default Admin credentials to make unauthorized changes on the administrator account and initial configurations.

To modify default administrator password,

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



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



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

Note:

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