SANGFOR

SANGFOR Central Manager

User Manual

Version: CM 2.5.10

Declaration

Preface

The User Manual of Sangfor Central Manager has four major parts.

The first part gives an overview of the Sangfor Central Manager and describes the architecture and key features of Sangfor Central Manager respectively.

The second part describes the installation and deployment methods of Sangfor Central Manager, it states the hardware deployment and virtualized environment deployment, and also describes the steps of authorization and activation.

The third part elaborates how to use, manage and maintain the Sangfor Central Manager, including branch Access, quick deployment of mails, automatic creation of VPN, SD-WAN routing and unified pushdown of branch policies.

The fourth part summarizes the FAQs for the installation and use of Sangfor Central Manager.

The preface contains the following contents:

- Target Audience
- Product Version
- Document Convetions
- Data acquisition
- Technical Support
- Feedback
- Revision History
- The recommendations stated in this manual apply to the following objects:
- Network design engineer
- O & M Personnel
- Technical staff on site

Product version

The information of products and version contained in this document are as follows:

Product name	Version
SANGFOR CENTRAL MANAGER	2.5.10

Document Conventions

Graphic Interface Conventions

Text Description	Substituted Symbol	Examples
Button	Border + shadow + shading	The “OK” button can be simplified as OK
Menu item	[ ]	The menu item “System Settings” can be simplified as [System Settings];
Continuous selection of menu items and submenu items	→	Select [System Settings]→[Interface Configuration]
Options from drop-down box, radio box and combo box	[ ]	The combo box option “Enable User” can be simplified as [Enable User]
Window name	[ ]	Click to pop up the [Add User] window.
Prompt	“”	If the prompt box shows “Saving configuration succeeded and the configuration modified. Do you need to restart the service to take effect immediately?”

Symbol Conventions

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

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

Technical Support

Email for user support: tech.support@sangfor.com

Technical Support BBS: http://community.sangfor.com

Company website: www.sangfor.com

Acknowledgments

Thank you for using our products and user manual. If you have any comments or suggestions on our products or user manual, we would appreciate it if you can give us feedback by phone, forum or email.

Contents

Chapter 1 Terminology

Term	Interpretation
CM	Its full name is Central Manager, it aims to provide solutions for the operation and maintenance management of branch offices. The CM can flexibly deploy the cloud or private cloud of the enterprise, and it also can directly purchase Sangfor hardware products.
SD-WAN	SD-WAN, namely a software-defined wide area network, is a service formed by applying SDN technology to a wide area network scenario. This service is used to connect to enterprise networks, data centers, Internet applications and cloud services in a broad geological scope, aiming at helping users reduce WAN costs and improve network connectivity flexibility.

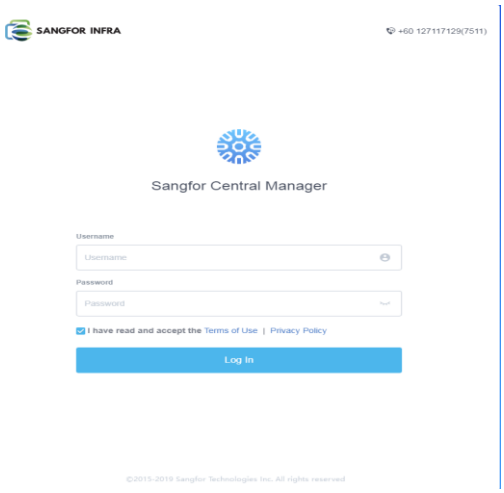
Chapter 2 Installation and Deployment of CM

Sangfor provides hardware CM and software CM. The installation and deployment of hardware CM is shown in Chapter 3.1. The software CM can be installed in Sangfor acloud, VMware, XYcloud, AliCloud and other scenarios.

2.1 Deployment of Hardware Devices

2.1.1 Login to CM Web Admin Console

1. Use web browser to Access: https://"CM Management IP", then the CM Web admin console will show as follows:



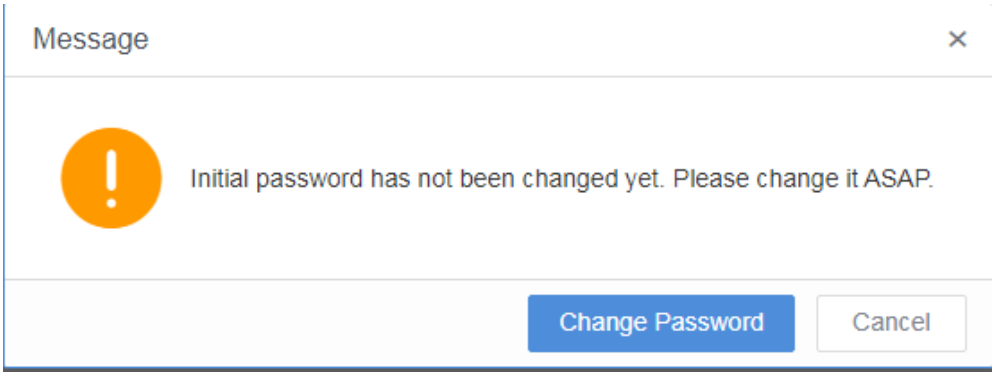
Description:

1) The Web console is used to manage and configure the Sangfor SANGFOR CENTRAL MANAGER, and requires the PC can Access to the management IP configured for the SANGFOR CENTRAL MANAGER host during the installation. If the IP address is not manually assigned during the installation, the default IP address will be 10.250.0.7. In this case, you need to connect the physical port of the PC and the LAN port of the SANGFOR CENTRAL MANAGER host to the same switch, and then configure an IP address at 10.250.0.x on the PC. Open the browser and enter https://10.250.0.7 in the address bar.

2) Sangfor Central Manager console can be Accessed with the following browsers: Internet Explorer, Firefox, Chrome, etc.

2. Enter the username and password in the login box, and click the Log In button to log in to the Central Manager console for configuration. By default, the username and password are both "admin" (excluding the quotes).

3. Upon login, you can change the password, as shown below:

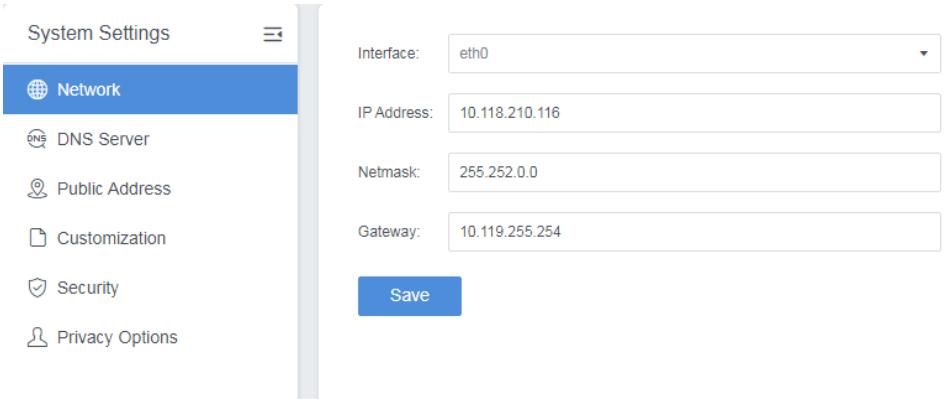


After success

2.1.2 CM Setup

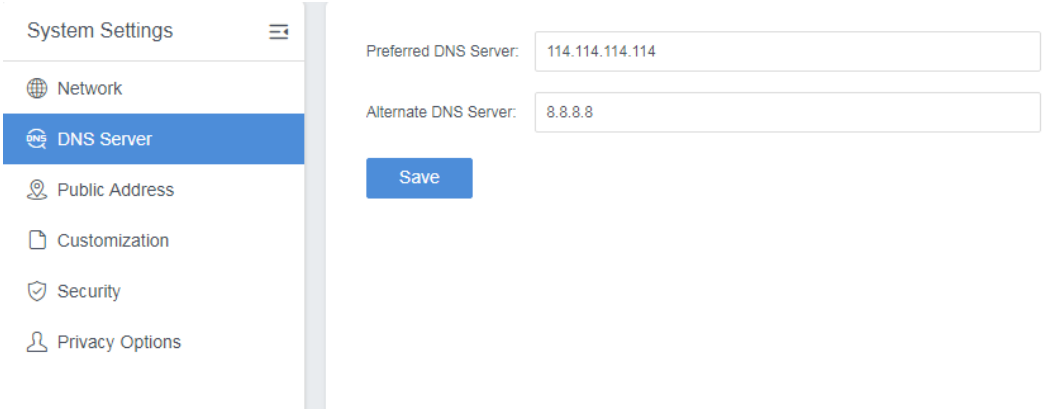
1. Check [System] -> [System Settings] to complete system configuration. It includes network configuration, DNS settings, port settings and customization settings.

[Network] is used to configure IP address, netmask and gateway address.

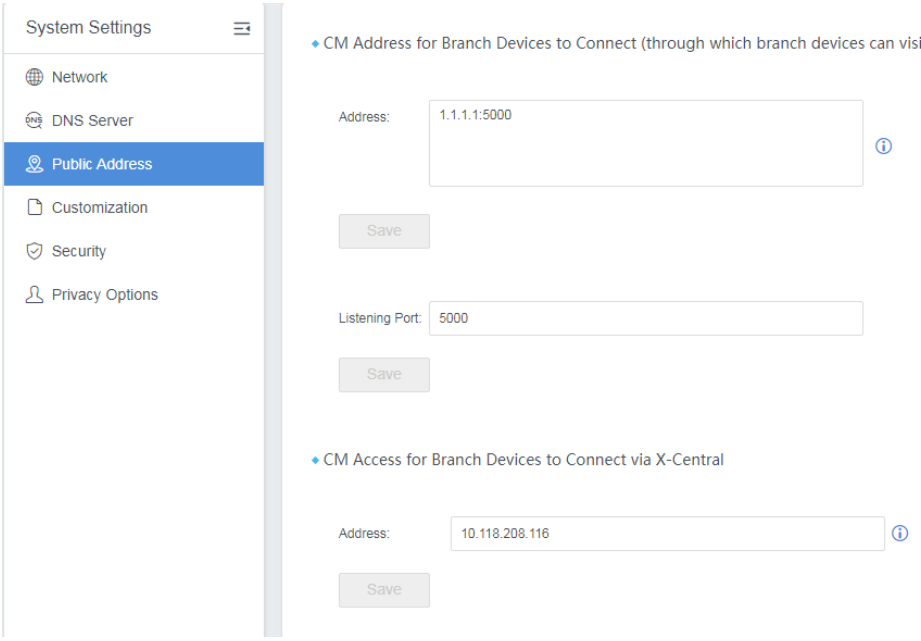


The Central Manager only supports single-arm deployment mode, and does not need to configure the deployment mode but configure the network settings directly.

2. [DNS Server] is used to configure the DNS server address for Central Manager to ensure that the device can parse the web page normally.



3. [Public Address] is used to set the address and listening port of the Central Manager, and it is used for the port connecting the branch device to the Central Manager. The page is as follows:



2.2 Deploy Central Manager on Sangfor acloud Platform

2.2.1 Resource Requirements

1. The configuration requirements for Central Manager deployment are as follows:

CPU	Memory	System Disk	Data Disk	Branches Supported
4 cores	8 GB	240 GB	500 GB	2,000
2 cores	8 GB	240 GB	500 GB	200

2. Recommended CPU model for the physical machine where .OVA file is located:

Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz or higher

2.2.2 Download Template

1. Download CM template of the version 2.5.1

http://community.sangfor.com/plugin.php?id=service:download&action=view&fid=88#/26/all

- BBC 2.5.6 EN

Name	Description	Size	File MD5	Last Update
BBC 2.5.6 EN	BBC 2.5.6 EN upgrade file. Support to direct upgrade from BBC 2.5.1	436MB	6FF6CA0A194F5ADD725A93C72935B632	06 Nov 2019 19

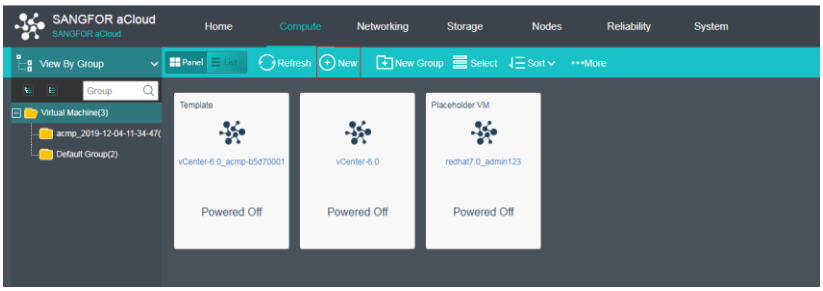
- BBC 2.5.1 EN OVA

Name	Description	Size	File MD5	Last Update
BBC 2.5.1 EN OVA	English version BBC 2.5.1 OVA file	2.8GB	5A88C113BDD0CAAC6E7A32568047E1E4	23 Aug 2019 18

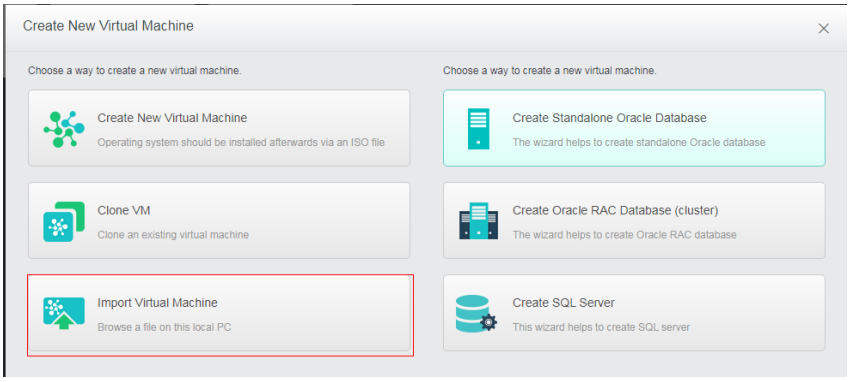
After the Central Manager is deployed, it can be upgraded to the latest version by installing the corresponding update package.

2.2.3 Import CM Template

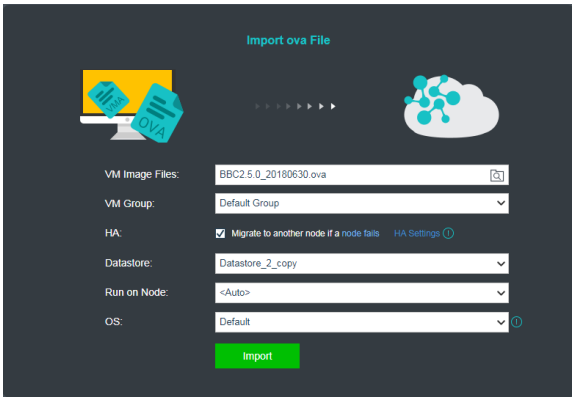
1. Log in to acloud platform, click New to create a new VM.

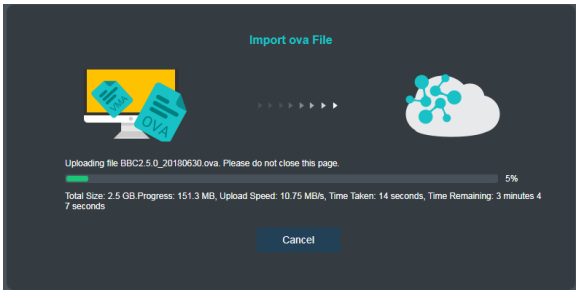


2. Click [Import Virtual Machine].

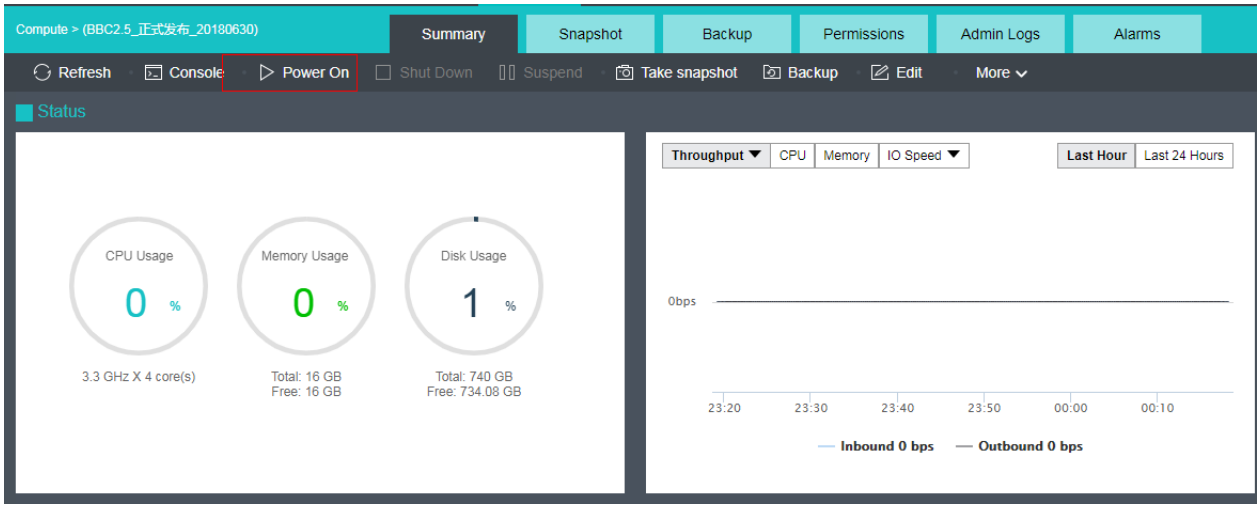


3. Select the downloaded OVA template with the version 2.5.0, specify the information such as [Group], [Datastore], click [Import], then wait for uploading and complete the creation.





4. After successful import, click on the Power On button on the VM summary page.



The default IP address of the eth0 port of Central Manager is 10.250.0.7/24. Configure computer with an IP address residing on the same network segment, use the browser to Access https://10.250.0.7 to log in to Central Manager, and then fill in the authorization information of vCM.

2.3 Deploying Virtual Central Manager on VMware vCenter

2.3.1 Resource Requirements

1. The configuration requirements for Central Manager deployment are as follows:

CPU	Memory	System Disk	Data Disk	Branches Supported
4-core	8G	240G	500G	2,000 pieces
2-core	8G	240G	500G	200 pieces

2. Recommended CPU model for the physical machine where .OVA file is located.

Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz or higher

2.3.2 Download CM Template

1. Download CM template of the version 2.5.1

http://community.sangfor.com/plugin.php?id=service:download&action=view&fid=88#/26/all

- BBC 2.5.6 EN

Name	Description	Size	File MD5	Last Update	Download	Operation
BBC 2.5.6 EN	BBC 2.5.6 EN upgrade file. Support to direct upgrade from BBC 2.5.1	436MB	6FF6CA0A194F5ADD725A93C72935B632	06 Nov 2019 19:04		Copy Link

- BBC 2.5.1 EN OVA

Name	Description	Size	File MD5	Last Update	Download	Operation
BBC 2.5.1 EN OVA	English version BBC 2.5.1 OVA file	2.8GB	5A88C113BDD0CAAC6E7A32568047E1E4	23 Aug 2019 18:04		Copy Link

After the Central Manager is deployed, it can be upgraded to the latest version by installing the corresponding update package.

2.3.3 Import CM Template

1. Open VMware Workstation, click [Open].
2. Click [Browse] to specify a location to store the VM.
3. Click Import to complete the deployment.

The default IP address of the eth0 port of Central Manager is 10.250.0.7/24. Configure computer with an IP address residing on the same network segment, use the browser to Access https://10.250.0.7 to log in to Central Manager, and then fill in the authorization information of vCM.

Chapter 3 Licensing Central Manager

3.1 Authorization Methods

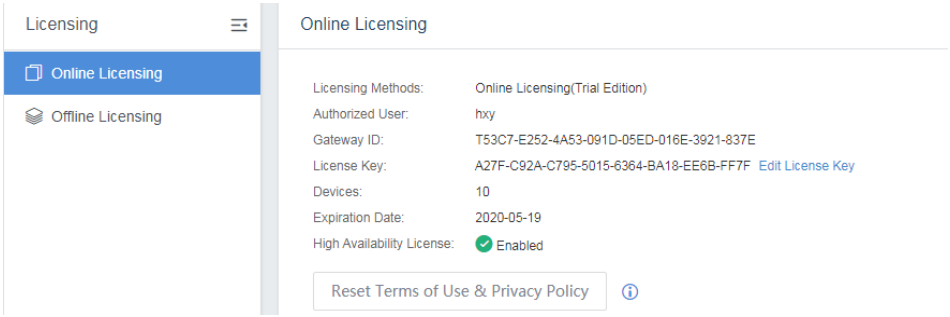
1. CM provides two authorization methods: [Online Licensing] and [Offline Licensing];
2. Online licensing: It is recommended when CM has Internet connection. If CM loses connection to Internet, all management functions will become invalid, but branch devices can connect to and report configurations to CM.

[Note]: The online licensing may cause delay in updating authorization due to network latency. Generally, it will take around 10 minutes to complete the update.

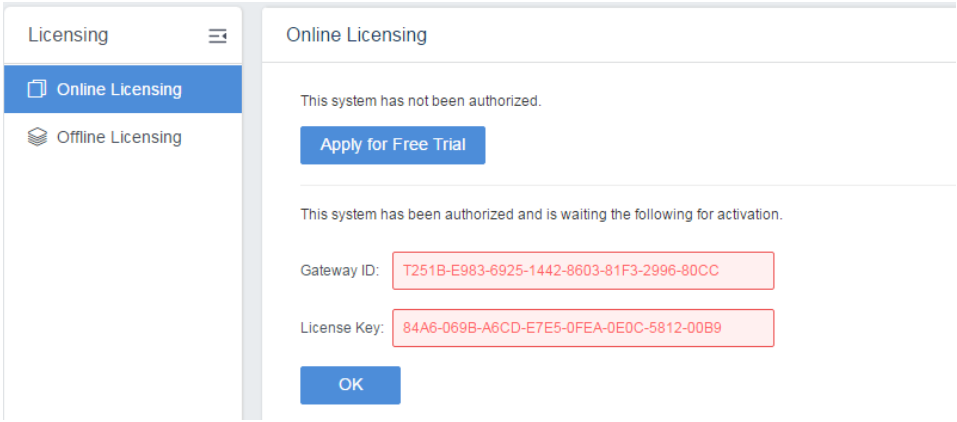
3. Offline licensing: If CM does not have Internet connection, USB key can be used for authorization. It is mainly used in the scenario where CM is deployed in intranet (when CM cannot connect to the Internet).

[Note]: When CM is deployed on Sangfor HCI platform as a software, it does not support the authorization method by using USB key.

4. The two authorization methods are shown in the following figure:

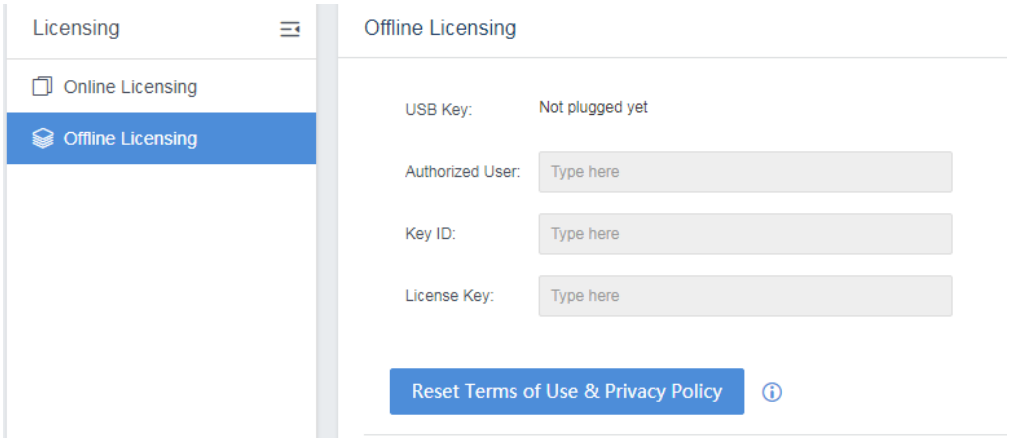


1) [Online Licensing] Fill in the applied gateway ID and license key correctly. The device must be connected to the Internet, and the authorization can be made successfully after the device is connected to an authorization server.



2) [Offline Licensing] It is required to use USB key and after the USB key is inserted into CM , it will

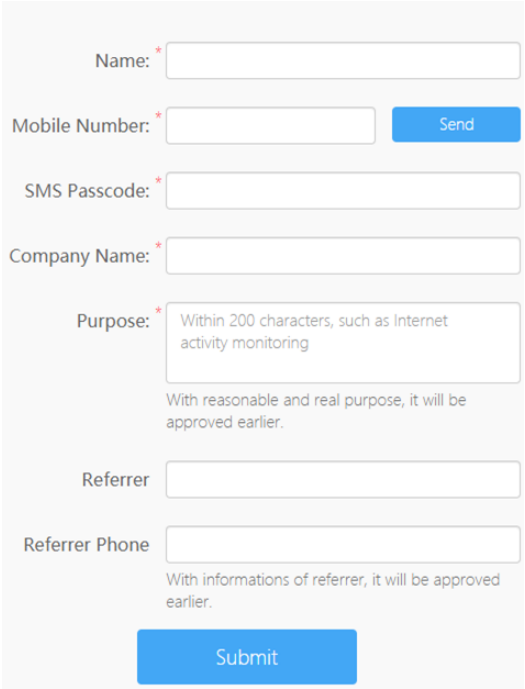
automatically identify the authorized user and the key ID, and fill in the license key information. With this authorization method, the device does not need to be connected to the Internet, but a USB key must be inserted. If the key is not inserted or the key is unplugged, the authorization will turn invalid immediately.



3.2 Licensing Test Device

On the [Online Licensing] page, click [Apply for Free Trial] to apply for license key for test device and then enter the application page and fill in the required fields. After successful application, the license key will be sent to specified mobile phone number by SMS.

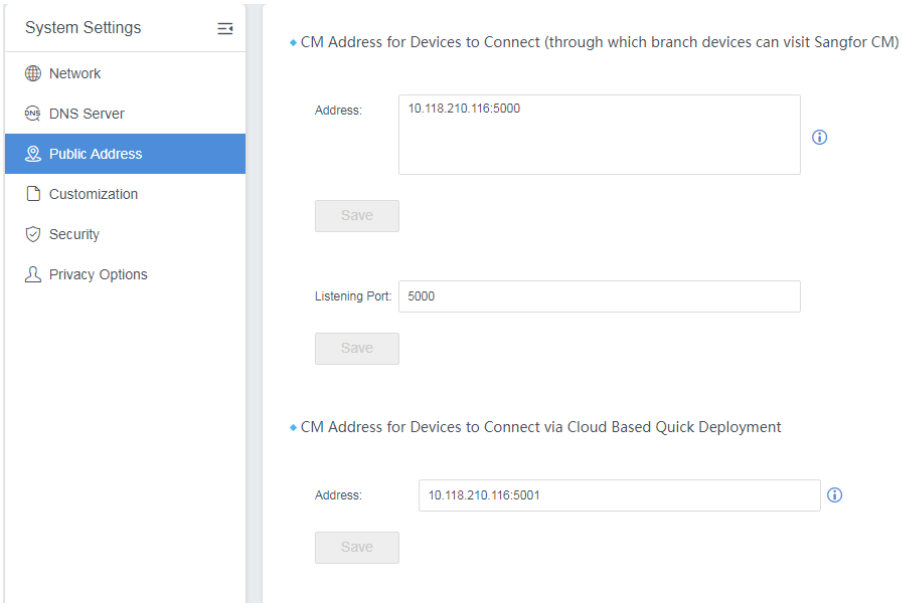
This method is [Online Licensing] and requires the device be connected to the Internet in order to apply and activate license key.



3.3 Port Requirements of Central Manager

1. The CM is deployed in single-arm mode. Generally, DNAT is required on the gateway device, and the port used for branch device connecting to CM needs to be open to the public network. The following ports need to be mapped on the gateway device:
2. TCP/UDP port 5000: A communication port through which the managed branch device is connected to CM. It must be mapped, otherwise the branch device cannot connect to CM platform.
3. TCP port 5530: A communication port through which branch devices can be managed remotely. It must be mapped, otherwise the function of remotely login to the branch device cannot be used on CM platform.
4. TCP port 443: It is a HTTPS communication port of CM. The administrator logs in to the CM platform port for management.

[Public Address]: Specify listening port and CM addresses for branch devices to connect, which is deployed with email containing quick deployment guide and deployed via cloud based quick deployment.



Chapter 4 Device Management

4.1 Adding Branch

[Scenario]

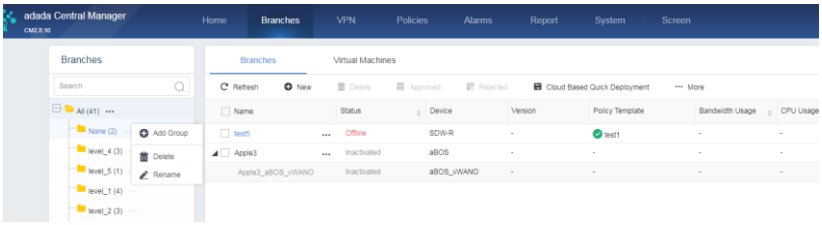
On Central Manager, create an account and password for the branch device, which is used by branch devices to connect to CM, so as to ensure connection security.

[Prerequisites]

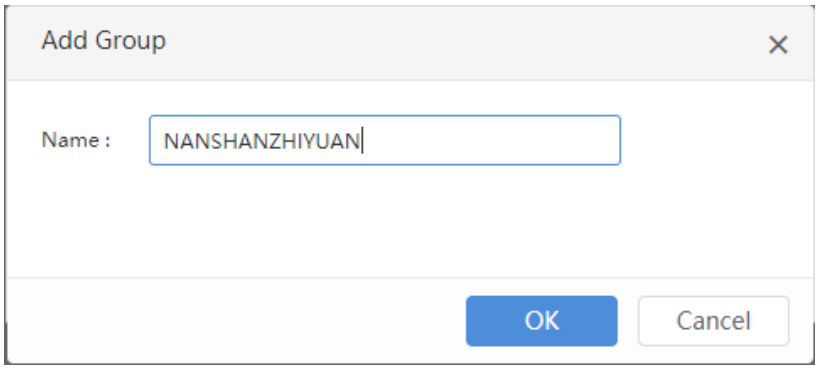
The CM deployment is completed. Branch devices and CM can communicate properly via the TCP ports 5000 and 5530.

[Steps]

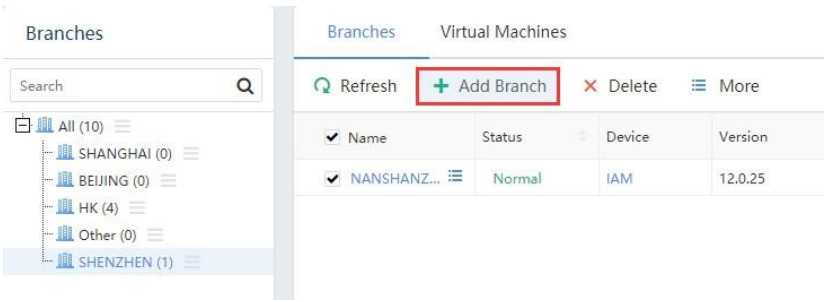
1. Add group.

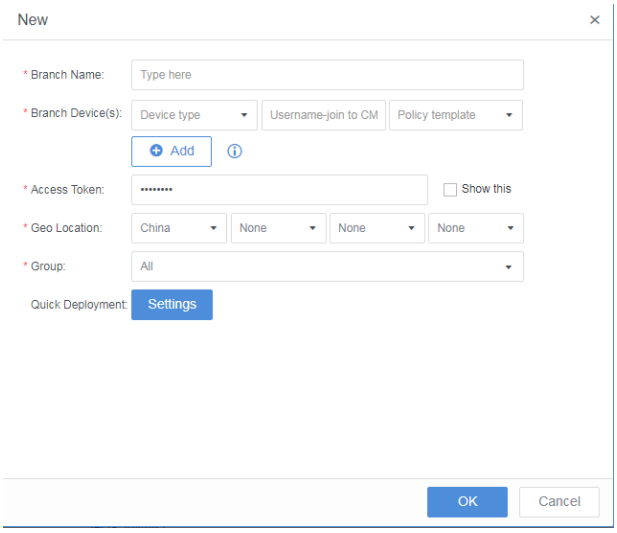


2. Specify group name.



3. Add branch.





[**Branch Name**]: Specifies name of the branch for easy identification.

[Branch Device(s)]: It include aBOS, IAM,NGAF, MIG, WANO, and SG.

[Access Token]: It is used by branch devices to connect to Sangfor CM.

[Geo Location]: Specifies the location where the branch device is located and displays easily on the Home page.

[Group]: Select the group which the branch belongs to.

4.2 Email Deployment for Branch

[Scenario]

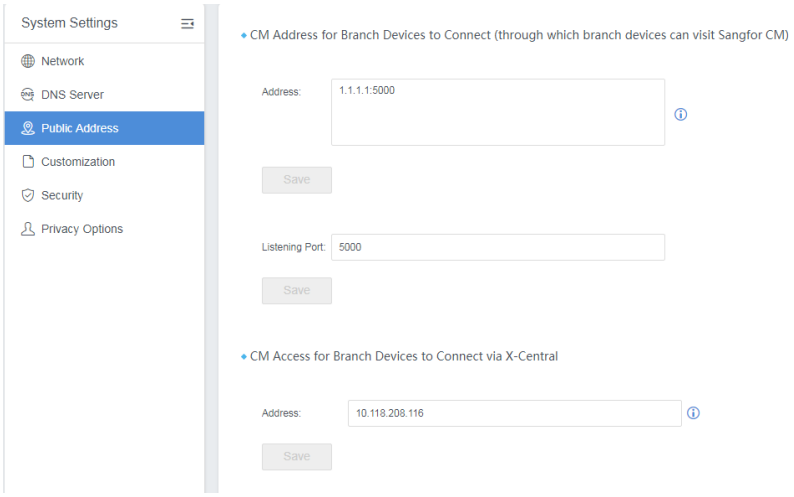
On SANGFOR CENTRAL MANAGER, configure the deployment mode of the branch. The branch administrator receives mails and clicks relevant links in the mail to quickly deploy the branch device online.

[Prerequisites]

1. The SANGFOR CENTRAL MANAGER device deployment is completed, and the branch device can normally Access TCP5000 and TCP5530 ports of SANGFOR CENTRAL MANAGER, and the configurations for [Access Address Settings] are correct.
2. The mailbox provided by the branch administrator can normally receive the mails in terms of quick deployment.

[Notes]

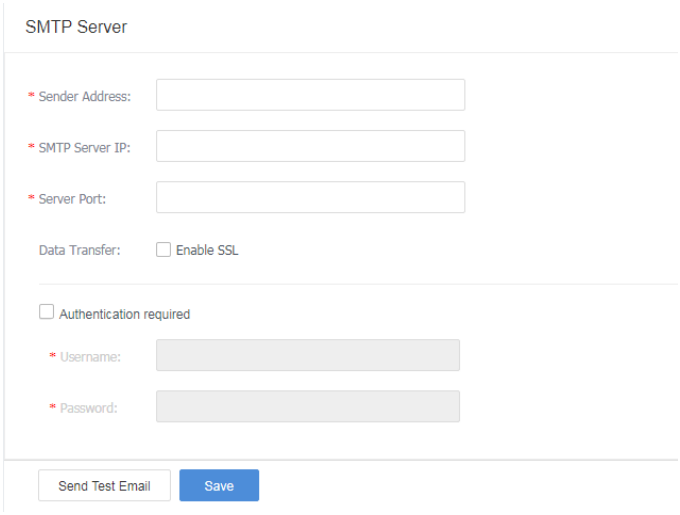
1. The device for quick deployment of mails must be a device in factory default. If the device has been configured, it needs to be restored to factory default, otherwise the quick deployment may fail.
2. Before setting the quick deployment configuration, it is required to set SANGFOR CENTRAL MANAGER address in advance. The mail for quick deployment will be push down together with this address. If the configuration is incorrect, the branch will fail to Access SANGFOR CENTRAL MANAGER. The address mentioned here must be an address that can be Accessed by the branch. If the single arm mode of SANGFOR CENTRAL MANAGER is enabled in intranet, and is to be mapped in through the gateway, the mapped public IP address shall be configured here. See the figure below:



3. The quick deployment mails as of WOC9.5.5 have been switched to using eth1 port for deployment. However, if the device is upgraded from version 9.5.3, then the quick deployment network port is still eth0. To maintain consistency with the mail, it is required to restore the device to factory default settings. (Operate on interface)

[Steps]

Step 1: Configure the SMTP server



[**Server Address**]: smtp.126.com (QQ: smtp.qq.com or 163: smtp.163.com)

[**SMTP Server IP**]: qxctest01@126.com (address of the sending mail)

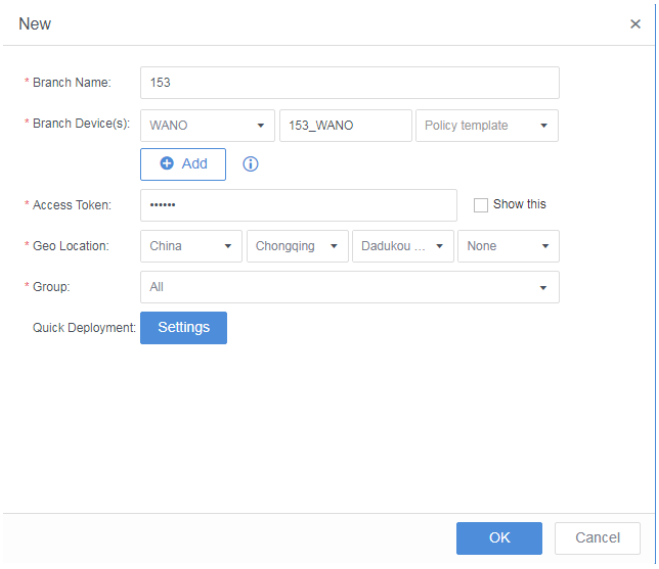
[**Service Port**]: 25 (25 by default, do not select SSL)

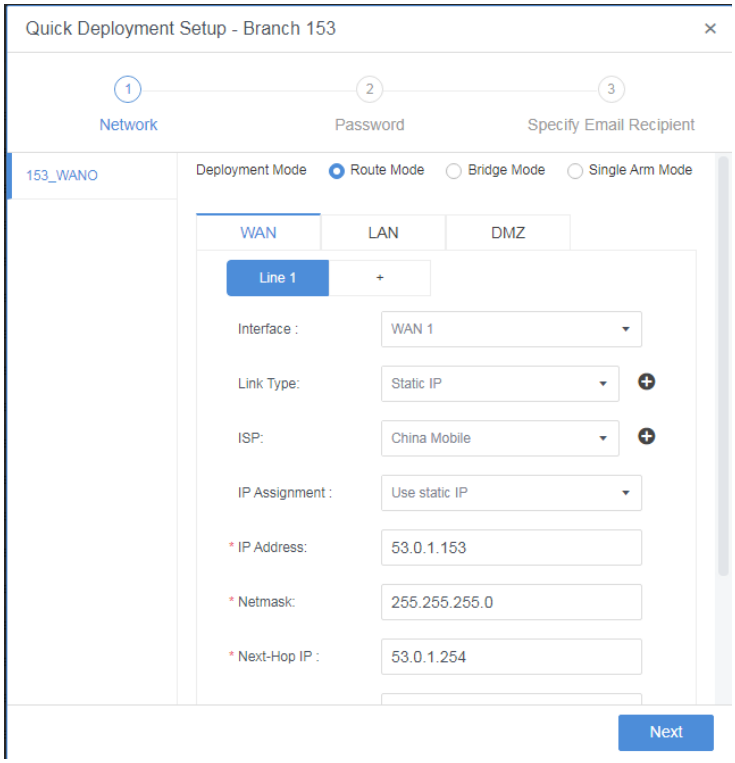
[**Username**]: qxctest01@126.com (same as the sending mail)

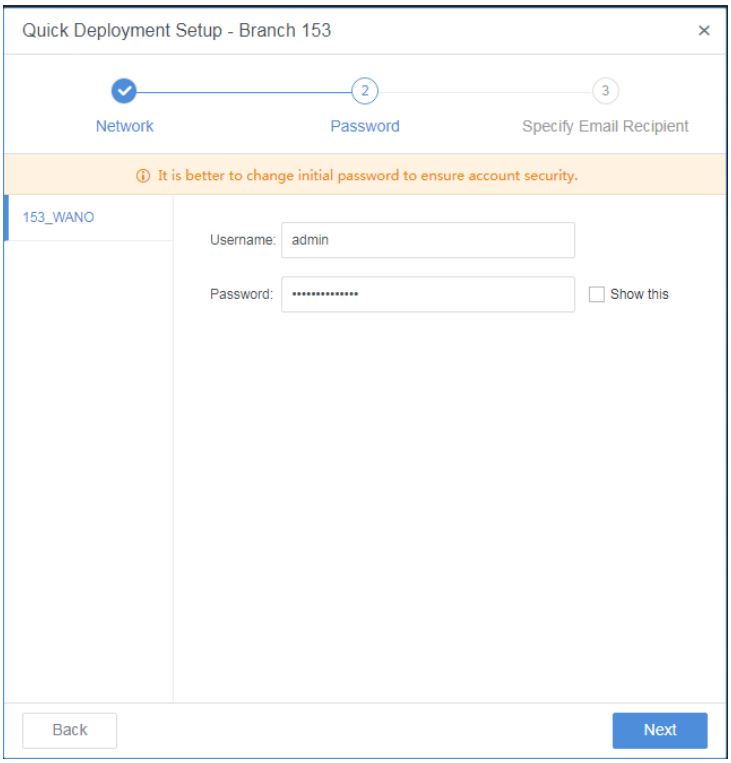
[**Password**]: XXX (not the login password of the mail, but the authorization code of the mail, see as follows)

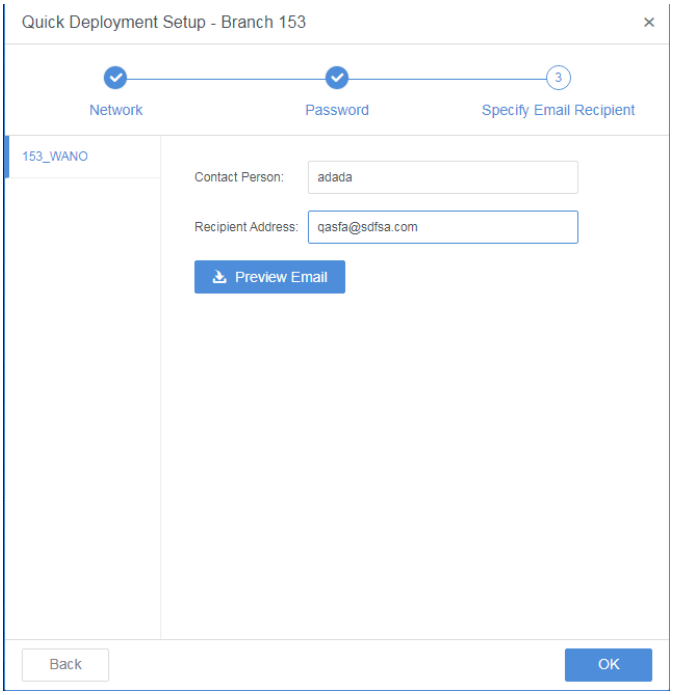
Step 2: Configure quick deployment information of the branch

1. On the page of [New], click [Settings] of [Quick Deployment] to configure.




Quick Deployment Setup - Branch 153
1
Network
2
Password
3
Specify Email Recipient
153_WANO
Deployment Mode
Route Mode
Bridge Mode
Single Arm Mode
WAN
LAN
DMZ
Line 1
+
Interface :
WAN 1
Link Type:
Static IP
ISP:
China Mobile
IP Assignment :
Use static IP
* IP Address:
53.0.1.153
* Netmask:
255.255.255.0
* Next-Hop IP :
53.0.1.254
Next

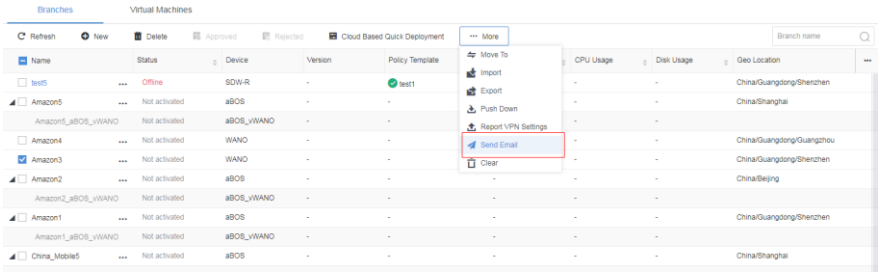

Quick Deployment Setup - Branch 153
Network
2
Password
3
Specify Email Recipient
It is better to change initial password to ensure account security.
153_WANO
Username:
admin
Password:
Show this
Back
Next



2. Click the [Preview Email] to preview the content of the mail.

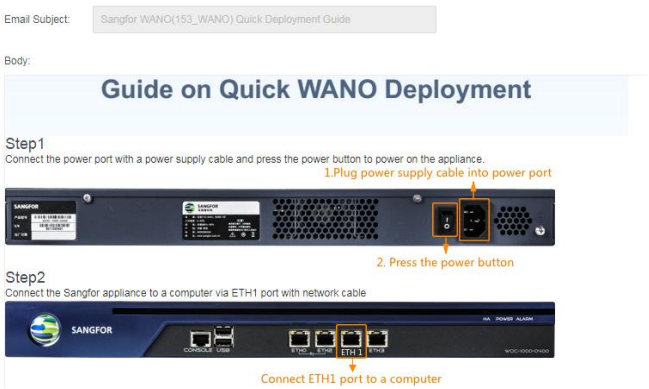
Step 3: Send deployment mail

On the page of branch overview, select the branch created, and click [More] -> [Send Email] to send deployment mail to the branch administrator.

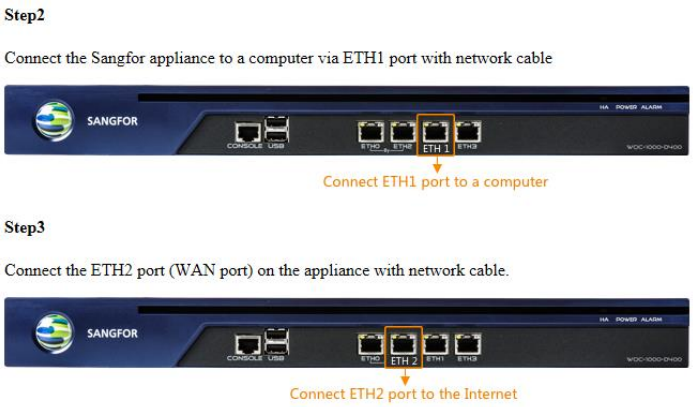


Step 4: Configuration at branch

1. The branch administrator receives the deployment mail.



2. Power on the device According to the instructions in the mail, connect network cables as instructed, and configure the computer's IP address (the current version of MIG and WOC supports obtaining IP address by using DHCP, that is, the computer configuration will be obtained automatically, and then the computer will be directly connected to the device to start quick deployment).



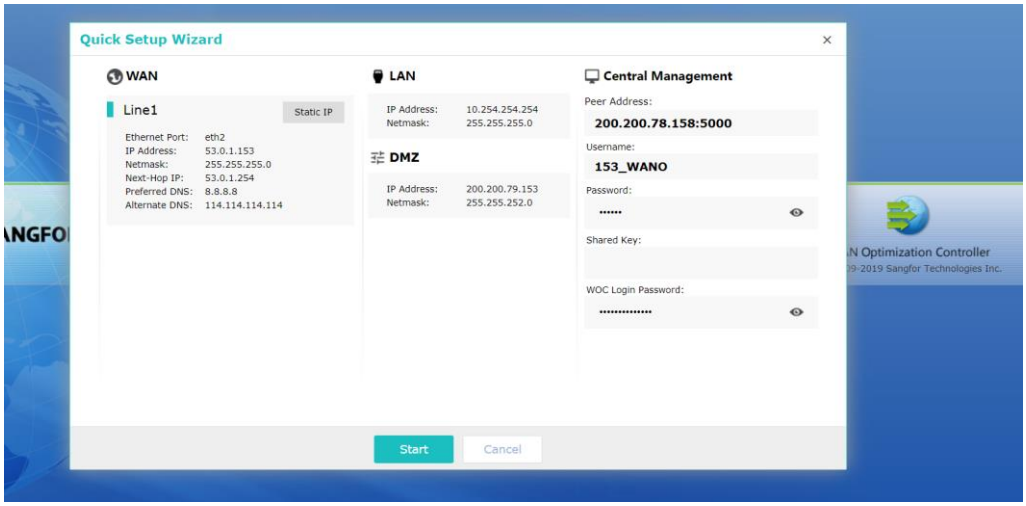
3. Click the link in quick deployment mail

Step 5

Visit the link below and the Web browser will be redirected to the GUI of WAN optimization controller.

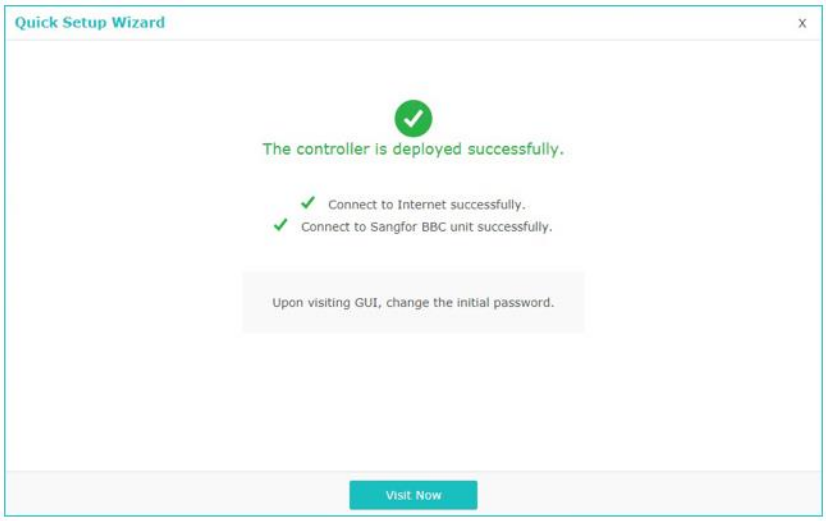
https://10.254.253.254/bbc?var=e061d446de0a3ac03a7691931020188cadd935375dd94df576b364199543fb39c09759b06bb4e3dce621aa06b0747ff5b26a28fe0695092cff277e8c7205fd29d82d7383f86d844683312b55d7e05773cc69bb0122314b997a62f0ff765e035f9f7dfbbf32d8d09479cf882e9a61855dd5520b0e9c3f7c64736b9fcf395034cbe308fbd633db4a2a6fc90b2c4e4f3556cbcd73f42ef82419e8eb488b5cab1e585820f996ee7720fd585616daff7a576bde617922ffe09662e171442d1d8ae25a3b5184daa8c4089e78f6e6b523196afcf7c905529b7a3e77f2b43155f846c043285574783fdd9cce8143756947b1ef48655e528b6deb34b1701a33d01a6be68e6de9a436e8c51bd60db77fdcbf7b920eeb2b7a7670669d9744caf61e8812bb7121648b6a9d50a54b93b2e53068e641891d9b90fe0af8f59283efae277bf4a52e475d4f220bae64e217253faf18eac5b05b2570d8a2f65d0510dc0c7d4a55f2f2bdf2c6444e7d9eac69a620447273b1e0016c27157693723100efc2a04cb840b8759aba0fecda39cb7bc24977b800690e716809c43110fa51dde2b1ff9dac7c213a78baa5188702dd8bfec3e43f99cf8f0eeb325ff19d5b5037e1ec6f227f70716c56bbe0b802023626f4a9281389068cf08804099cabf0f9c683c2abe46dbd96d9e0f232cf0c6b430de864a37968befdd69a02844f9f34f08700ed65e60f7ca5aabe8a68441fa57fddf68c539cf0ba506e83cb0a141e5b860dbe660f70a1ba6818657e2a506f39e14876da7abe2d23a5adaf007b1534936bce5a7a5172189aecbbea6b39db417ae26ece1e5c34c2a4a8

4. The browser will automatically open and log in to the device. After successful login, it will prompt the deployment information. Click [Start Deployment] after checking the information below.

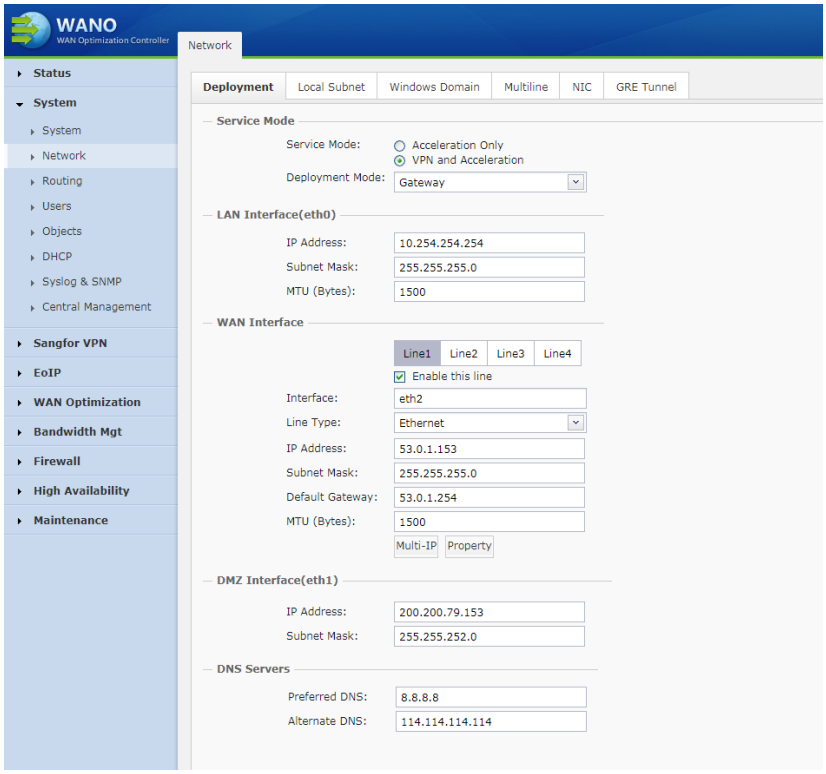


Step 5: Effect of quick deployment

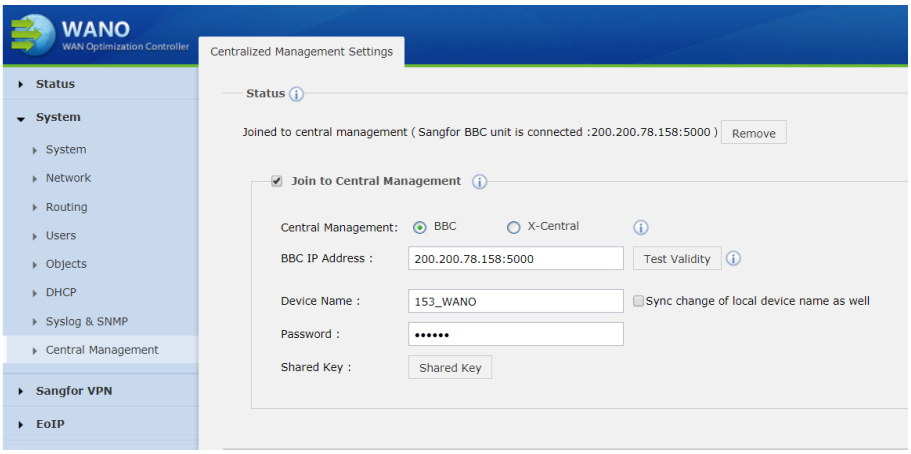
1. After the deployment of the branch is completed, you can see the prompt of successful deployment.



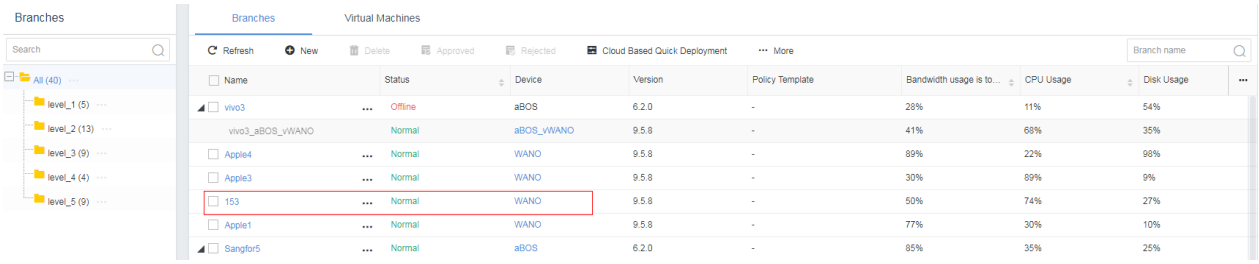
2. Click [Visit Now] to log in to the device directly.

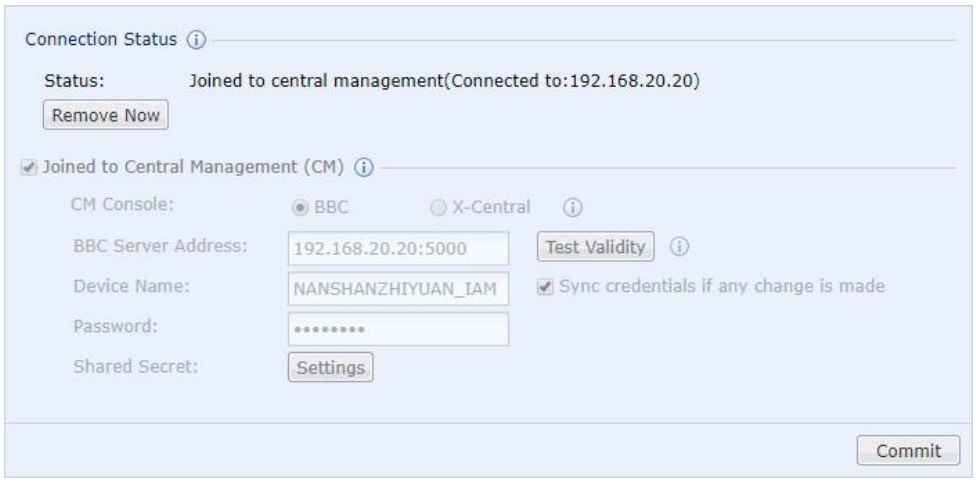


3. As shown in [Central Management], you can see that the device has automatically joined the SANGFOR CENTRAL MANAGER.



4. In SANGFOR CENTRAL MANAGER, you can see that the device is already online.





4.3 Branches Manual Connect to SANGFOR CENTRAL MANAGER

Besides the quick deployment, the branch device can also be connected to SANGFOR CENTRAL MANAGER by manually configuration, where the SANGFOR CENTRAL MANAGER device can be connected by properly setting the accounts on corresponding branch device in Accordance with the branch information created by the SANGFOR CENTRAL MANAGER.

4.3.1 aBos Connects to SANGFOR CENTRAL MANAGER

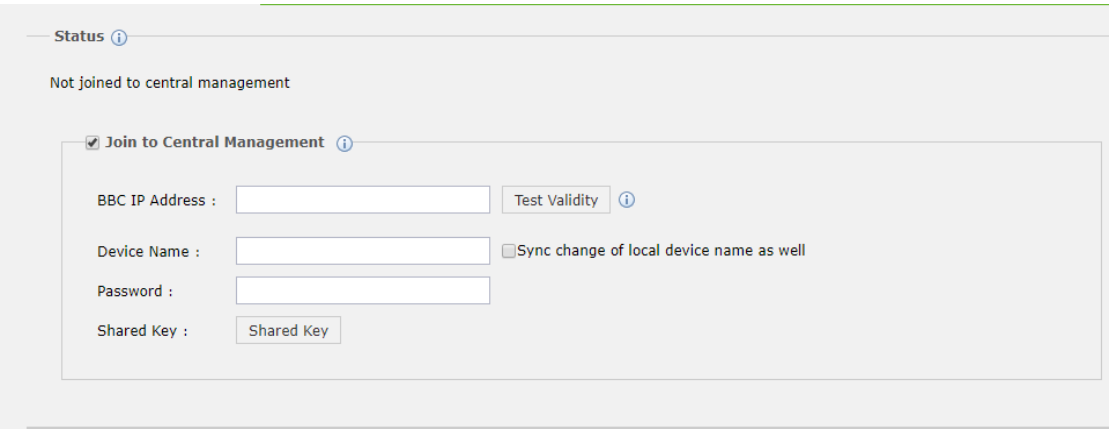
The SANGFOR CENTRAL MANAGER can be successfully connected by the branch aBOS administrator who logs in to the aBOS console, and opens the [**System**] -> [**Central Management**] to fill in the address, port, device name and password which are provided by the SANGFOR CENTRAL MANAGER administrator at the headquarters.

4.3.2 IAM Connects to SANGFOR CENTRAL MANAGER

The IAM administrator in the site shall login the IAM Console, open [Systemt] -> [Genera] -> [Central Management], and fill in address, port, site password and branch name provided by SANGFOR CENTRAL MANAGER administrator in the headquarters, and then SANGFOR CENTRAL MANAGER can be successfully connected.

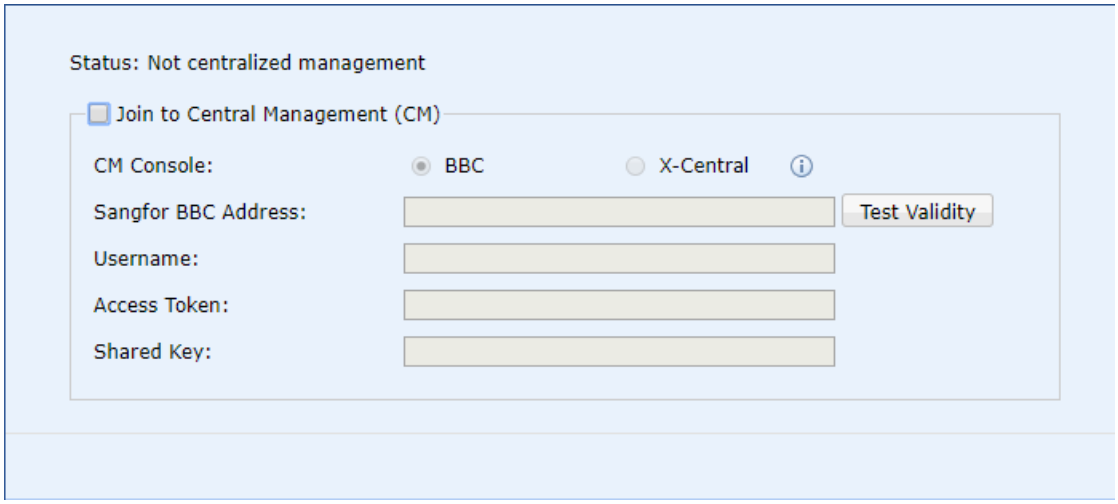
4.3.3 WANO Connects to SANGFOR CENTRAL MANAGER

The WANO administrator in the site shall login the WANO console, open [System] -> [Centralized Management Configuration], and fill in address, port, site password and branch name provided by SANGFOR CENTRAL MANAGER administrator in the headquarters, and then SANGFOR CENTRAL MANAGER can be successfully connected.



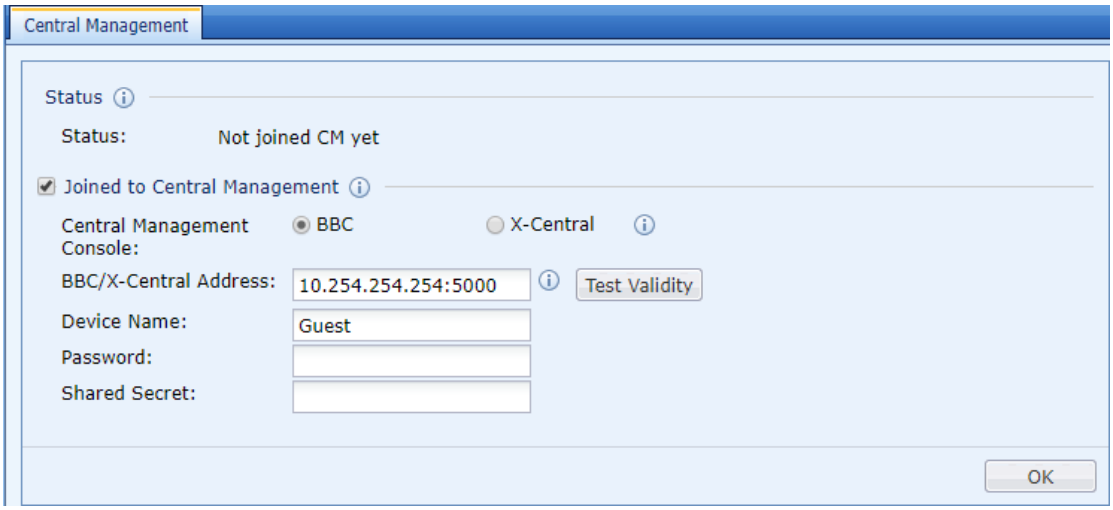
4.3.4 MIG Connects to SANGFOR CENTRAL MANAGER

The SANGFOR CENTRAL MANAGER can be successfully Accessed by the branch MIG administrator who logs in to the MIG console and opens the [**System**] -> [**Central Management**] to fill in the address and port provided by the SANGFOR CENTRAL MANAGER administrator at the headquarters as well as the password and name of the branch.



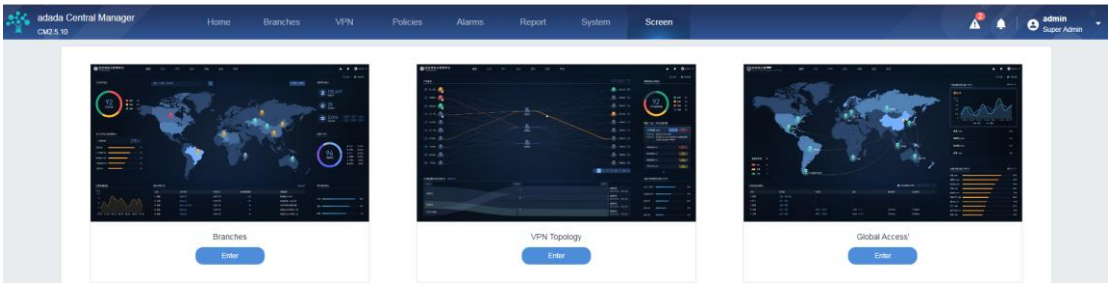
4.3.5 NGAF Connects to SANGFOR CENTRAL MANAGER

The NGAF administrator in the branch shall login the NGAF Console, open **[**General**]** -> **[**Central Management**]**, and fill in address, port, site password and branch name provided by SANGFOR CENTRAL MANAGER administrator in the headquarters, and then SANGFOR CENTRAL MANAGER can be successfully connected.



4.4 Screen

The console is added with a new function of screen, which includes the Branches, VPN Topology, and Global access, as shown in the figure below:



4.4.1 Branches Screen

1. The middle part of the **[Home] page** displays the current branch access status in a map. Green indicates that the current connected branch is normal, yellow indicates that an alarmon the current connected branch, red indicates that the current branch is off-line. If there is any inactive branch, the number of inactive branches is displayed.

2. The two sides of the home page are used to display the status of the SANGFOR CENTRAL MANAGER connected branches, including the Branch Devices, the Top Branch Devices by Alarms (24 hours), the Alarm Trending, the Alerting Branch Devices, the Branch Device Distribution, the Top 5 Branch Devices by Traffic, the Resource Usage, etc.

[Branch Devices] indicates the total number of current branches and is classified in accordance with different statuses. The green indicates the healthy branch devices. Yellow indicates the alarming branch devices. Red indicates the off-line branch devices. Gray indicates the total number of inactive branches.

[Top Branch Devices by Alarms (24 hrs)] indicates the alarm statistics of branch devices within 24 hours.

[Alerting Branch Devices] keeps statistics of unexpected error and alarm items of branch devices and makes a ranking.

[Alarm Trending] displays the usage of the abnormal branch devices and makes a ranking.

[Resource Usage] shows the CPU usage, memory usage, and disk usage of the SANGFOR CENTRAL MANAGER devices.

[Top 5 Branch Devices by Traffic] counts applications with high traffic occupancy in all branch devices, and then performs reasonable traffic control and monitoring.

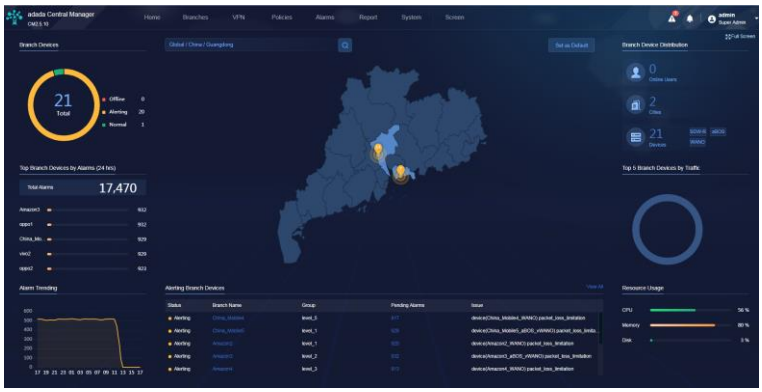
[Branch Device Distribution] shows the total number of branch devices, and cities

corresponds to the cities where the branch points are distributed. Online users

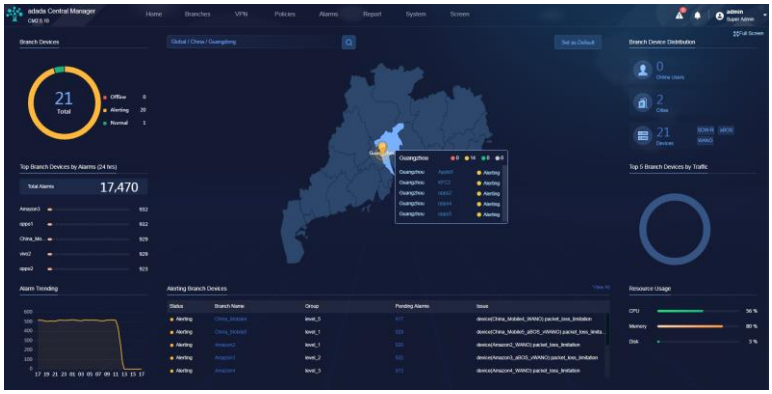
shows the statistics of on-line users at all branch devices.

3. Move the mouse to a different province on the map to check the status of connected branch of the province.

4. Select the province to check the distribution of branch devices in different cities of the province.

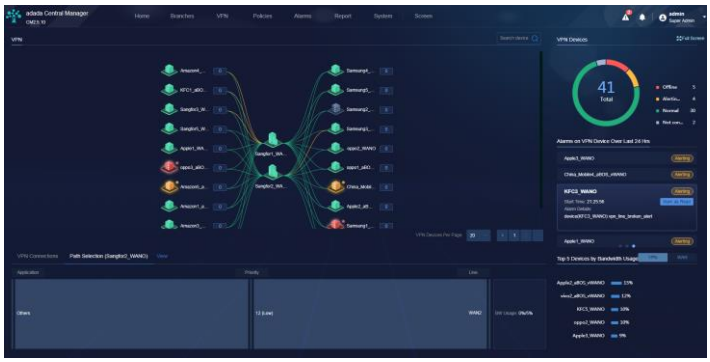


5. Select the city to check the distribution of branch devices in different regions of the city.



4.4.2 VPN Topology Screen

1. Click [Screen] -> [VPN Topology] to display the VPN connection information of the existing branch devices on large screen, where green means that the VPN connection of the connected branch is normal, orange means that the branch has alarms, red means that the branch is offline, and gray means that the branch is not activated.



[Search device] is used to search for a specified VPN device.

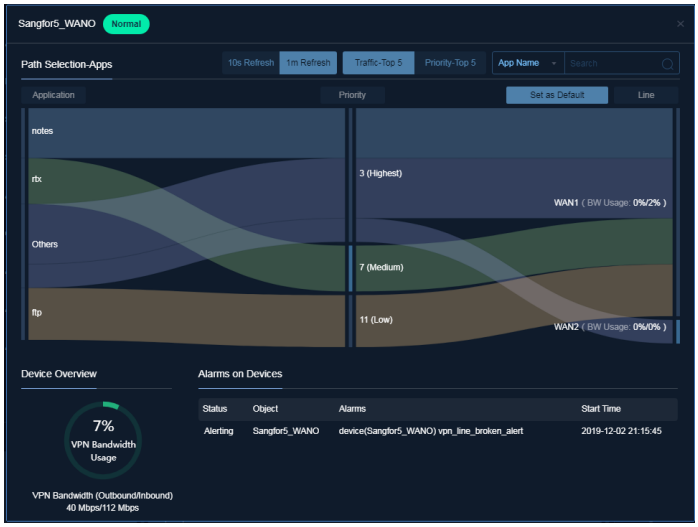
[VPN Devices] counts the status of all VPN devices on the whole network.

[Alarms on VPN Device Over Last 24 Hrs] displays the alarm information of each VPN device within 24 hours.

[Top5 Devices by Bandwidth Usage] counts the Top 5 applications of traffic occupancy in all branch VPN tunnels.

[Path Selection-Apps] intuitively shows the effect after the device has matched with the SDWAN path selection policy.

2. Click on corresponding device to view the distribution of unilateral traffic on the device regarding the SDWAN path selection result of the VPN device. Click the **Sangfor5_WANO Device** on the VPN Topology to view relevant traffic distribution diagrams, as shown in the figure below:



[10s Refresh, 1min Refresh] indicates the refresh interval of VPN device traffic distribution diagram for using SDWAN path-selection policy.

[Traffic-Top 5, Priority-Top 5] When there are many applications generating traffic or there are many priorities of applications, it can be selected to display the SDWAN path-selection diagram of the applications of top 5 traffic or top 5 priorities.

[Search] finds out the traffic diagram of corresponding application according to the application name or IP.

[Application] identifies the application customized According to the SDWAN path-selection policy.

[Priority] identifies According to the priority customized in the SDWAN path-selection policy.

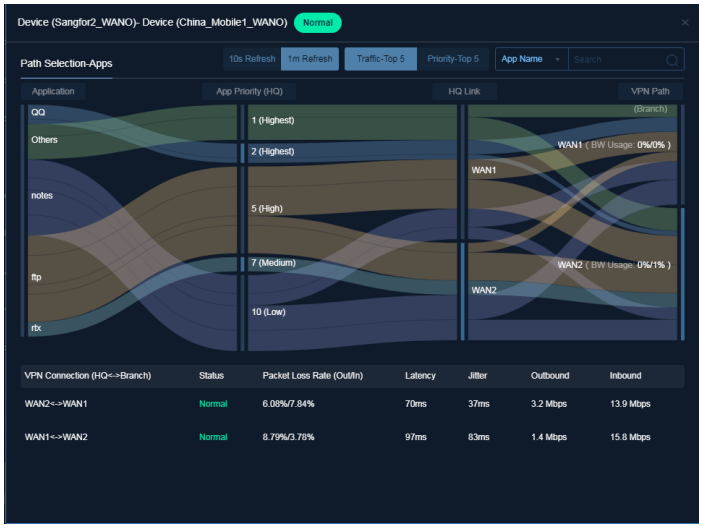
[Set as Default] After setup, display can be done in the lower left corner of the VPN Topology.

[Line] shows the effect diagram of traffic dispatched to specific line According to the SDWAN path-selection policy.

[Device Overview] shows the utilization of VPN total bandwidth.

[Alarms On Devices] shows the status, object, alarm details and start time of device alarm.

3. Click the corresponding tunnel of two VPN devices to view the traffic distribution diagram of SDWAN path-selection policy effect of VPN device inside the tunnel, as shown in the figure below: click the **Sangfir2_WANO-China_module_WANO** tunnel to view the traffic distribution inside the tunnel



[10s Refresh, 1min Refresh] indicates the refresh interval of VPN device traffic distribution diagram for using SDWAN path-selection policy.

[Traffic-Top 5, Priority-Top 5] When there are many applications generating traffic or there are many priorities of applications, it can be selected to display the SDWAN path-selection diagram of the applications of top 5 traffic or top 5 priorities.

[Search] finds out the traffic routing effect diagram of corresponding application According to the application name or IP.

[Application] identifies the application customized According to the SDWAN path-selection policy.

[App Priority (HQ)] identifies According to the priority customized in the SDWAN path-selection policy.

[HQ Link] shows the dispatching effect diagram of traffic on headquarters line According to the SDWAN intelligent routing policy.

[V**PN Path (Branch)]** shows the dispatching effect diagram of traffic on branch line According to the SDWAN path-selection policy.

[VPN Connection (HQ ⇔ Branch)] shows the VPN connection between HQ VPN device and branch.

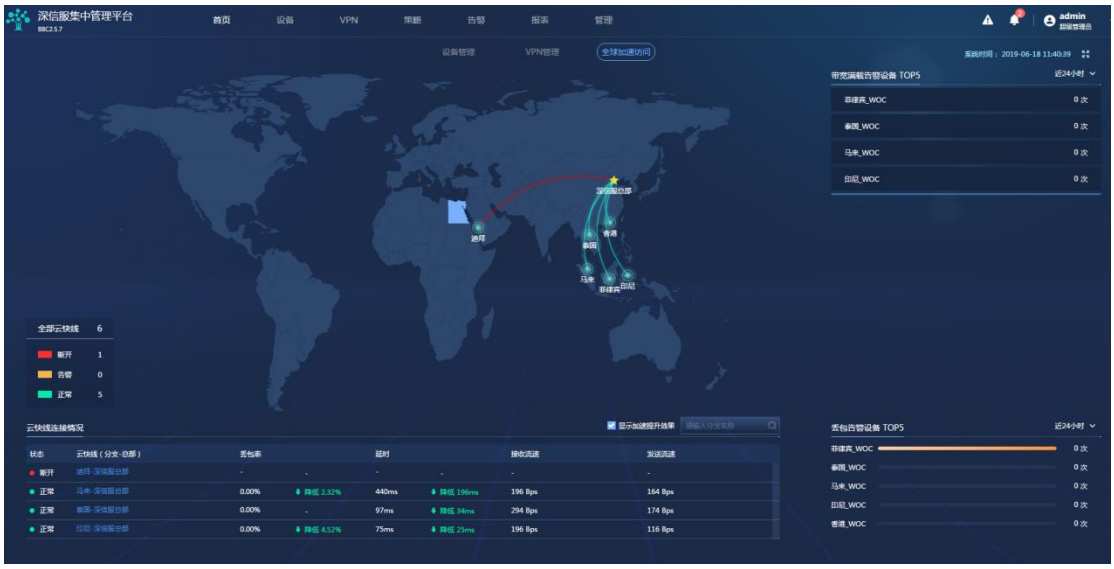
[Status] shows the status of VPN connection.

[Packet Loss Rate, Latency, Jitter] shows the real-time line quality of VPN connection.

[Outbound and Inbound] shows the real-time outbound and inbound bps of VPN connection.

4.4.3 Global Access Screen

Click [Screen] -> [Global Access] to display the operating status of currently global accelerated Access services, where green means that the existing branch connection is normal, orange means that the existing branch has alarms, and red means that the existing branch has been disconnected. See the figure below:



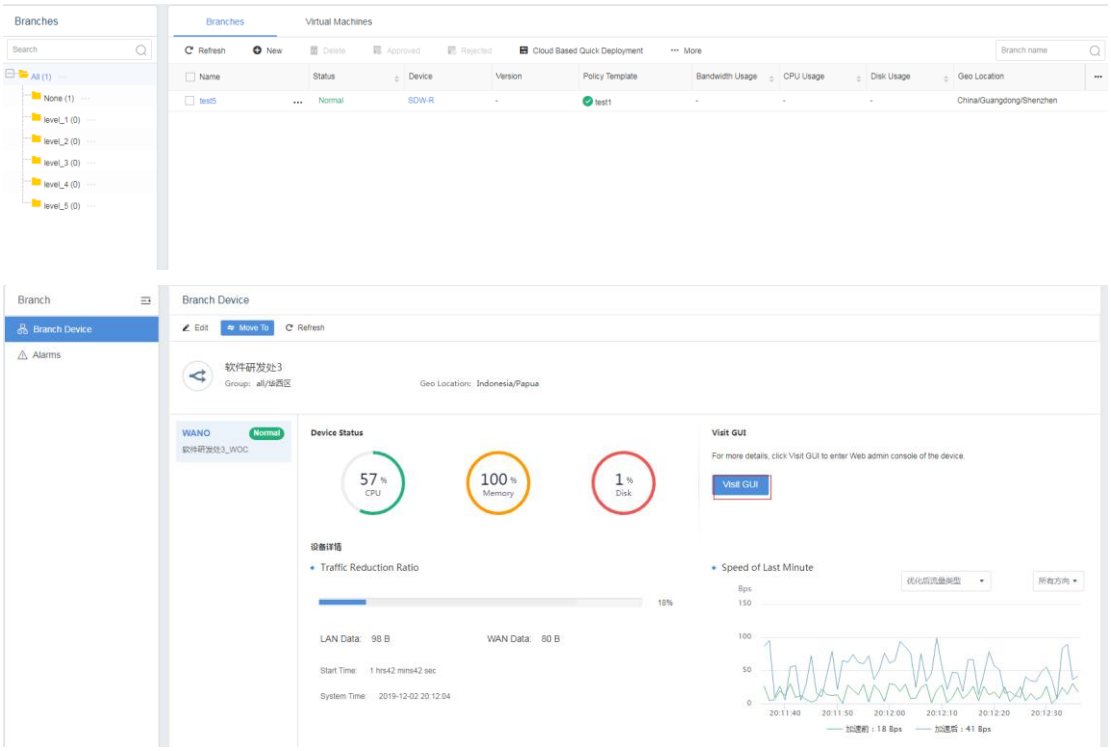
[TOP 5 Devices By Bandwidth Alarms] shows the number of full load alarms on each branch device in the last 24 hours.

[Outgoing Lines] shows the connected status information of the lines of each branch, including packet loss rate, latency, inbound and outbound, and shows the effect of lines optimization.

[Top 5 Devices by Alarms on Packet loss] shows the device reached the packet loss alarm threshold in the last 24 hours, and shows the alarm times.

4.4.4 Branch Overview

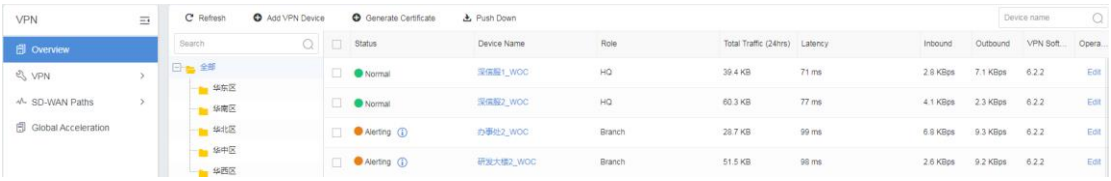
1. Click [Branch] to view the information such as currently configured branches, its online and offline status, CPU usage and disk usage.



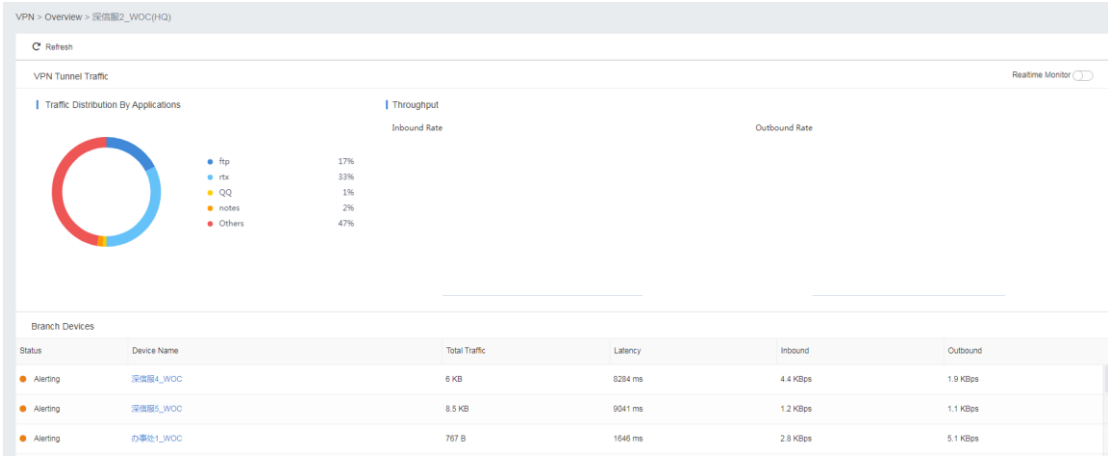
2. Click the **Online Branch** to view the overview of the existing branches, or to do single sign-on remotely.

4.4.5 VPN Overview

1. Click [VPN] to view [Overview], where the status information of VPN tunnel of the branches can be viewed.



2. Click the branch name to go to the page of VPN device overview of the existing branch.



[Branch Devices] indicates that the device type is HQ VPN device, and the following is the status of all branches connected therewith.

[VPN Tunnel Traffic] If there is only this option, it means that the device type is the branch VPN device, and the following is the status of each VPN link between the branch and the HQ VPN device.

[Throughput] displays the VPN trend of sending and receiving traffic in the latest day. Click to enable the refresh of real-time traffic trend.

[VPN Tunnel Traffic]] is to check the connection status of the device and all HQ VPN devices, including status, traffic distribution by applications, latency, inbound and outbound.

Chapter 5 Centralized VPN Management

5.1 VPN

[Scenario]

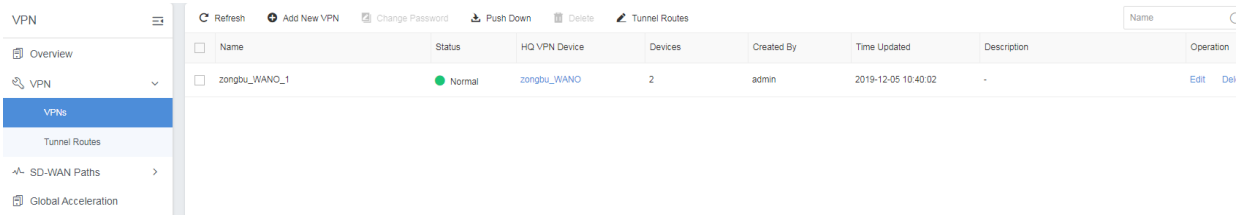
The VPN function supports the creation of VPN on Sangfor Central Manager, the configuration of basic information of HQ VPN device, and the selection of corresponding branch device; other information will be generated automatically by the Central Manager, and corresponding VPN configuration will be pushed down to establish VPN connection automatically, thereby simplifying the configuration by the headquarter administrator.

[Prerequisites]

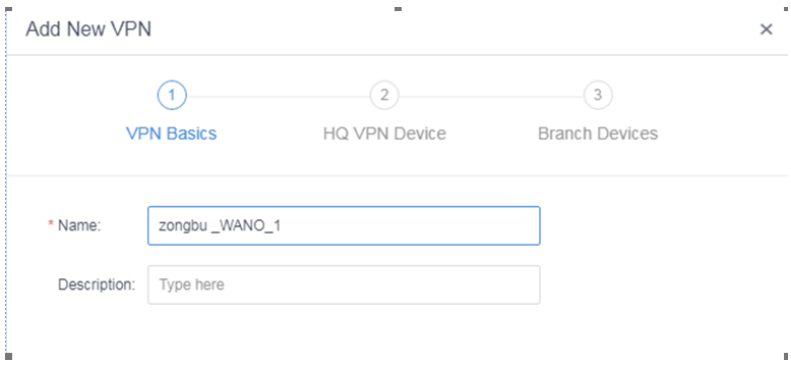
1. The HQ VPN device and the branch device are connected to the Sangfor Central Manager platform.
2. Relevant VPN ports of HQ VPN device have been released on the Internet (SANGFOR VPN TCP\UDP 4009); and normal VPN connection can be established through the Internet.

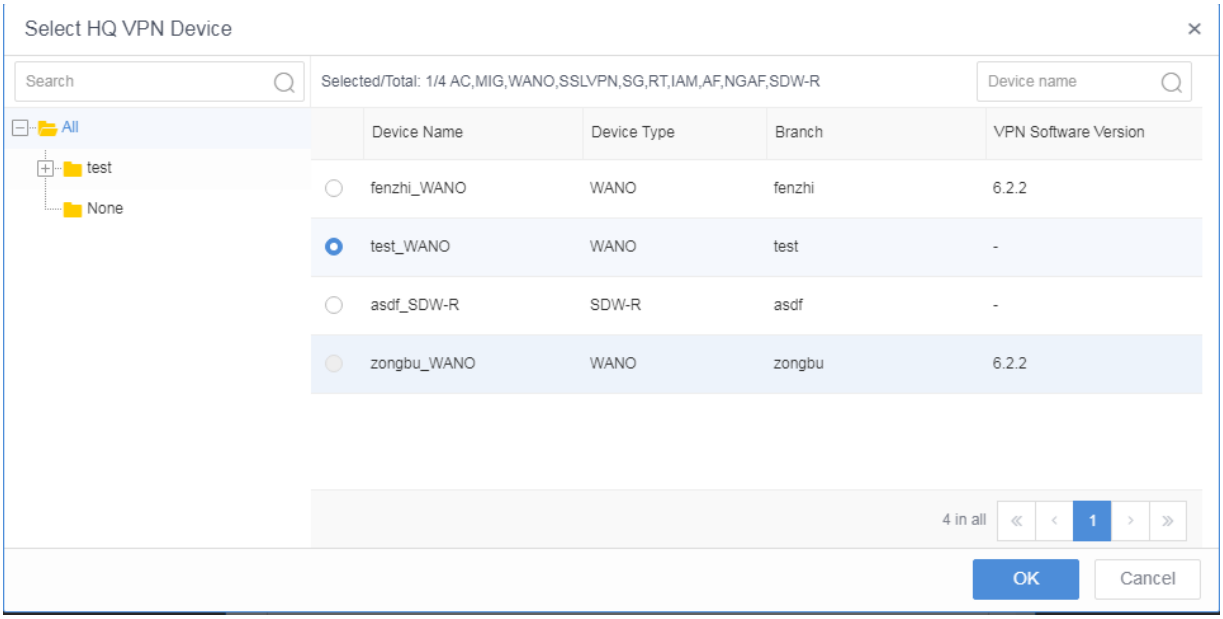
[Steps]

1. Click [Add New VPN] under the [VPNs] tab.

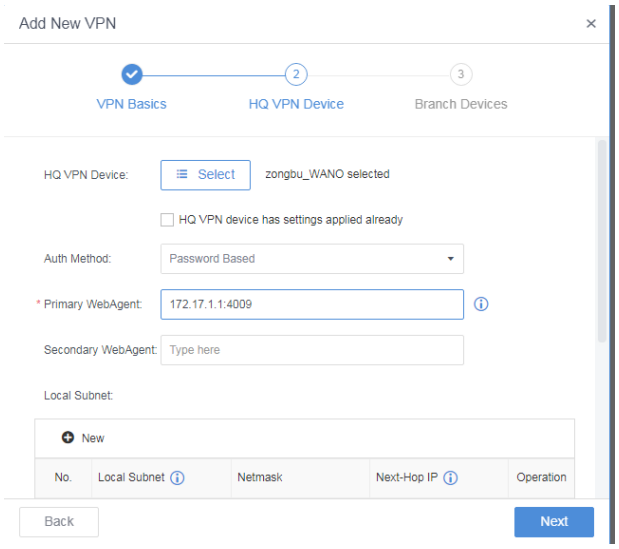


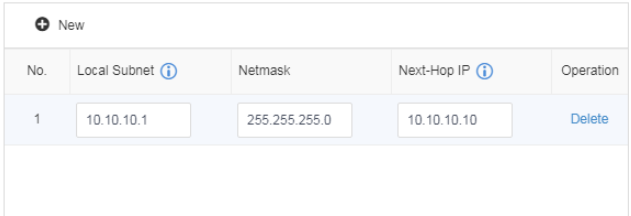
2. Input the name for the new VPN.
3. Select a HQVPN device.



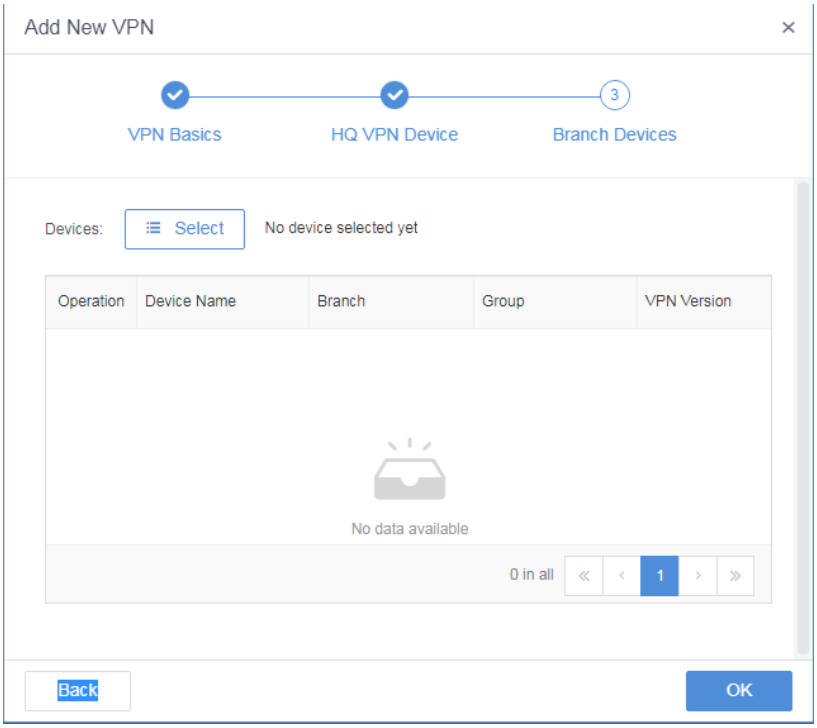


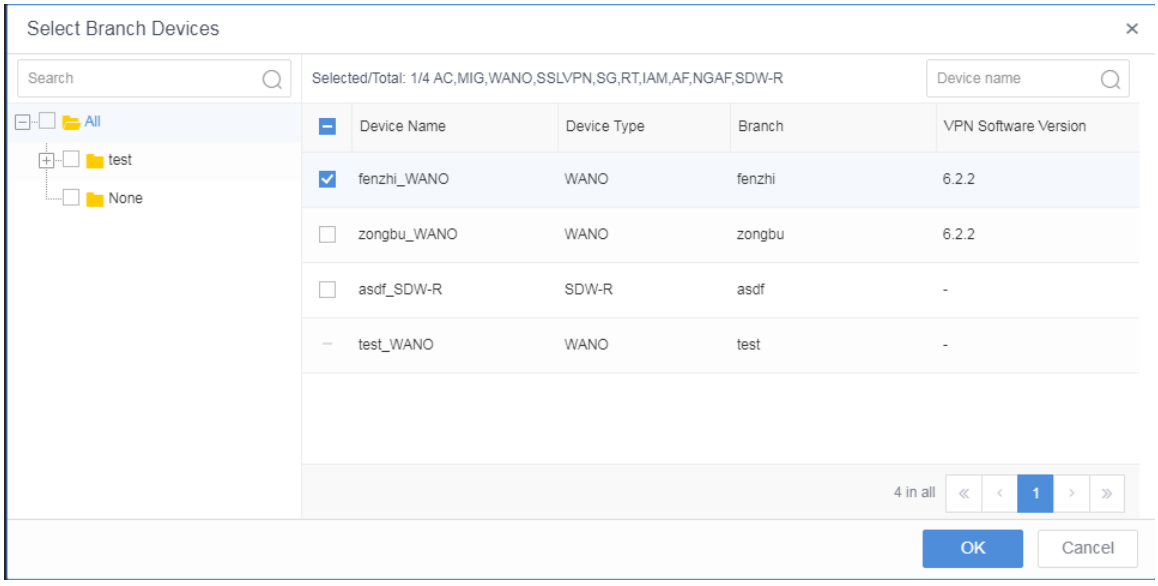
4. Configure VPN authentication method, WeAgent address, local subnet and other settings.



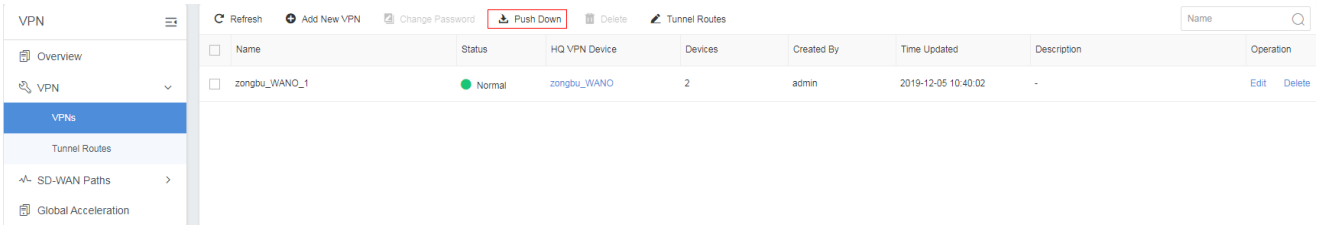


5. Select branch devices.

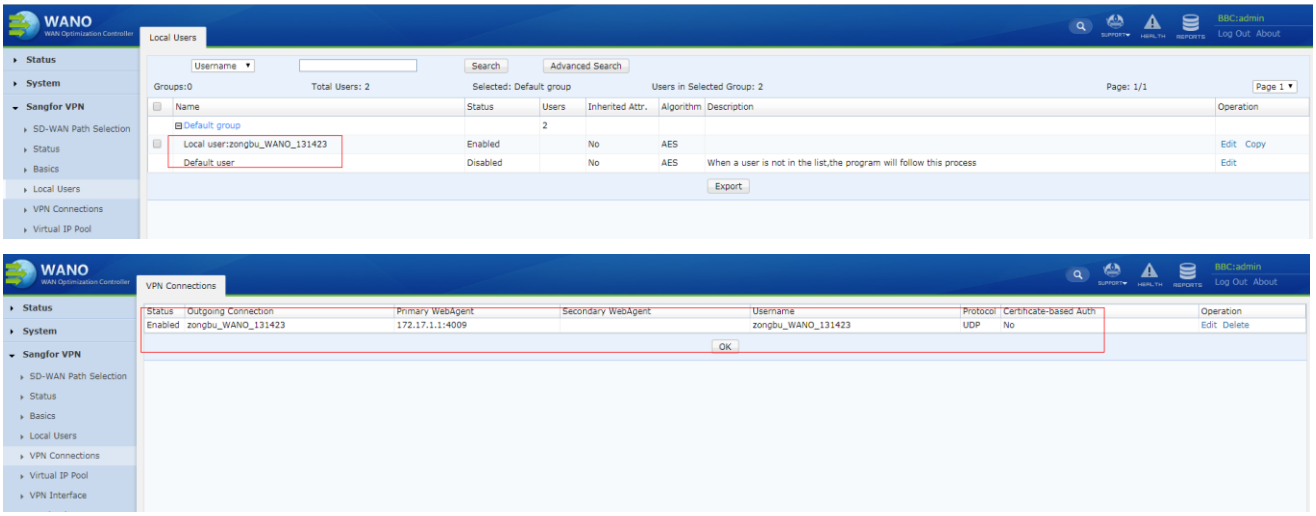




6. Click [Push Down] to distribute the configuration immediately to the managed branch devices .

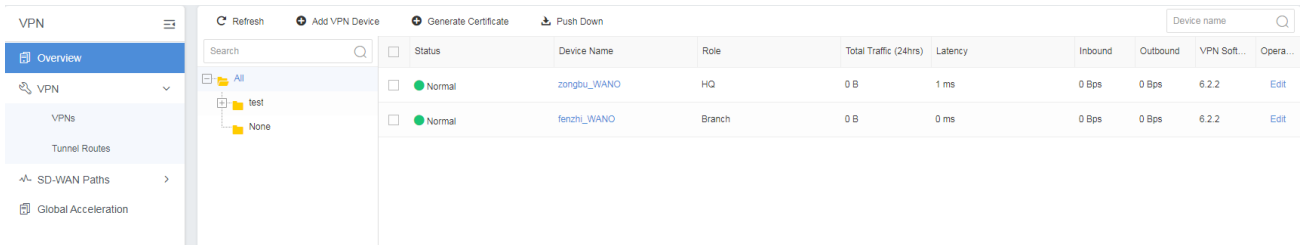


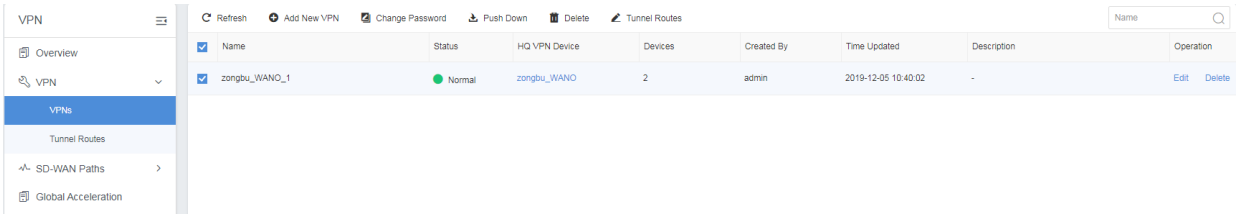
7. After distribution, log in to the HQ VPN device and branch device to view pushed-down VPN configurations.



8. VPN connection status shows whether a VPN connection is established between branch device and HQ VPN device.

9. On the Central Manager, it can be seen that the VPN branch and the VPN status are both normal.





10. If the HQ VPN device and the branch devices are connected to the Central Manager, the VPN connection has been established manually, and the VPN supports VPN devices to automatically report VPN configuration. Then the SANGFOR CENTRAL MANAGER can generate the VPN configuration automatically According to the reported VPN configuration.

5.2 Tunnel Routes

CM2.5.6 supports the distribution of tunnel route configuration, in order to make branch devices Accessed by each other via HQ VPN device.

[Scenario]

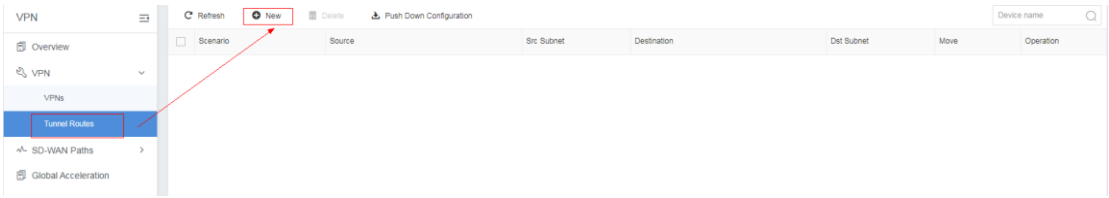
1. Access between branch devices: When branch A and branch B are connected to headquarter VPN device, tunnel route can be used to establish connection between between branch A and branch B via the headquarter VPN device.
2. Branch-to-Headquarter: When branch C is connected to the secondary headquarter B, tunnel route can be used to connect branch C and primary headquarter A via headquarter B..
3. Branch-to-Internet via Headquarter: When branch B has no Internet connection, but it is connected to headquarter A, tunnel route can be used to allow the intranet users in branch B to Access the Internet via headquarter A.
4. Backup Across HQs: Certain business system is Accessible from headquarters A and B. Connection from branch C is firstly made through HQ A, then through HQ B when connection to HQ A fails.

[Prerequisites]

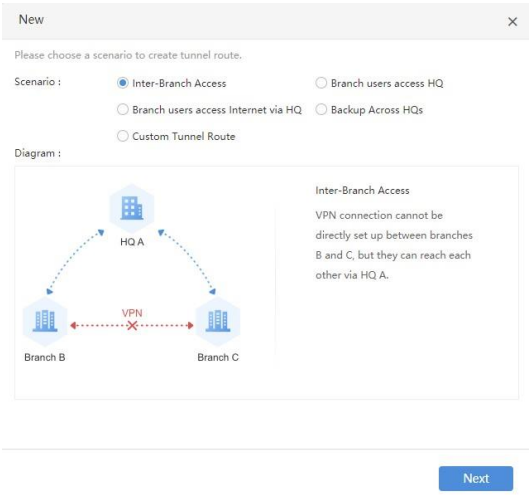
1. The headquarter device and branch device are connected to the Central Manager.
2. VPN has been created for these devices , and the tunnel is established normally.

[Steps]

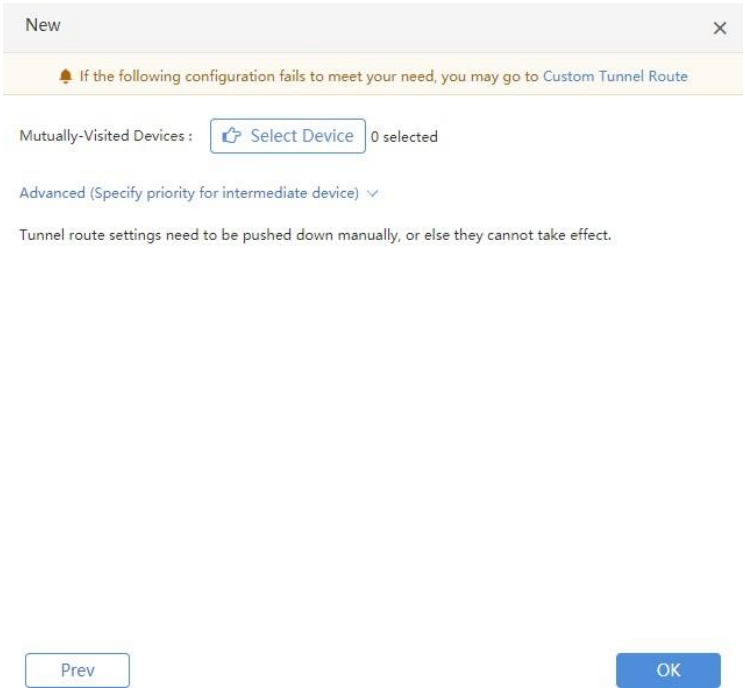
1. Select [New] in the [Tunnel Routes].

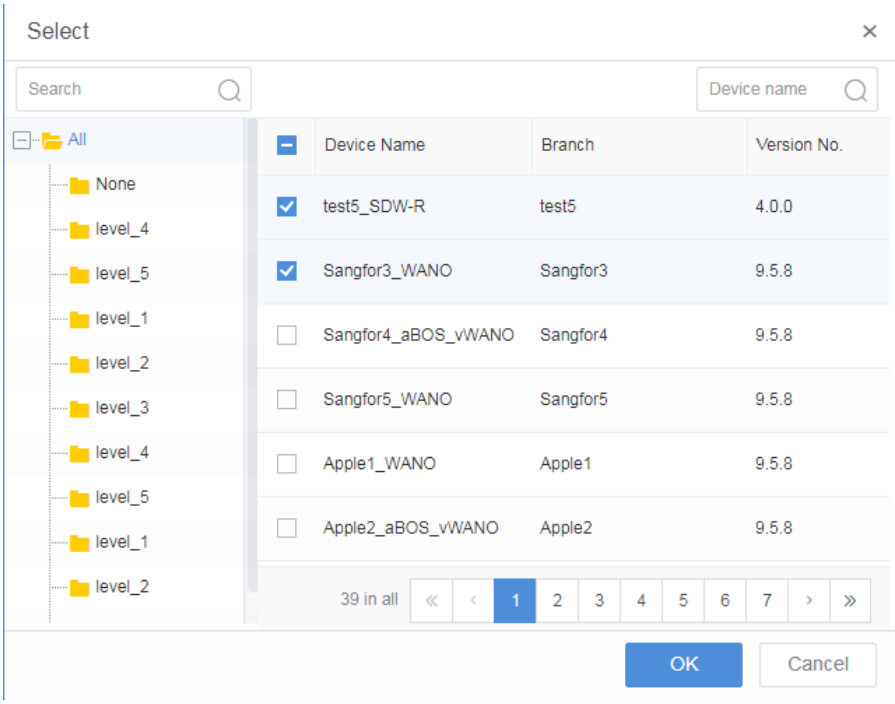


2. Select the type of tunnel routes According to the Actual scenario.

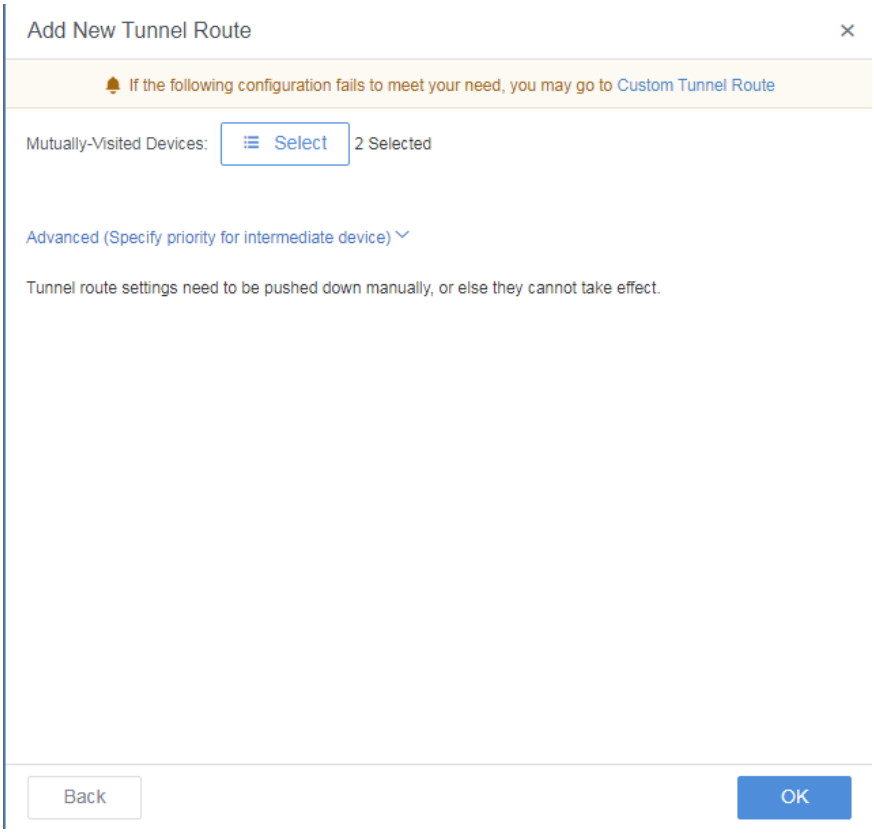


3. Select two devices that you want to connect.





4. Automatically select an intermediate device.



5. Click **OK** to complete the configuration of tunnel routes.

5.3 SD-WAN Path Selection

5.3.1 Basics

[Scenario]

SD-WAN path selection function is to schedule multiple lines flexibly According to business category; it supports the link quality QOE identification, and supports assignment of dedicated line for important business or selection of optimal line based on link quality.

Functions:

1. Identify applications based on LAN services.
2. Support four path selection modes:

1) Specified path: Select a path According to the LAN services. It is often used in video conferencing service, or some services that have some requirement for lines.
2) Session based link load balancing by remaining bandwidth percent: assign connections based on the real-time remaining bandwidth percent of lines. It is often used for file uploading or downloading service, and other services that have fewer requirements for line quality.
3) Session based link load balancing by optimal path select optimal line According to the real-time line quality. It is often used for services that have high requirements for line quality.
4) Packet based link load balancing: It is used for single bandwidth-intensive application , e.g., high-definition video conference, large file transmission over FTP.

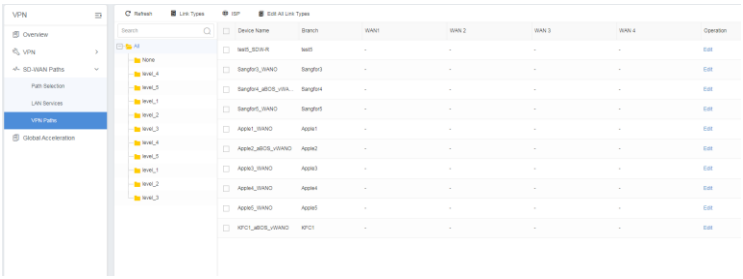
a) In case of the line fault, line switchover occurs within 1 s, without interrupting services.
b) There are five levels of priority. the business with higher priority will be forwarded first.
c) Line switchover will occur when a line is loaded...

[Prerequisites]

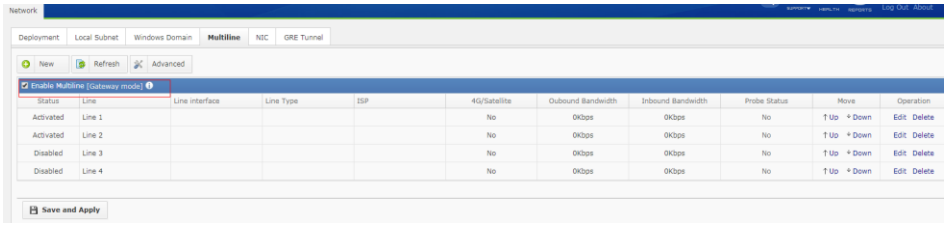
1. The headquarter device and branch device are connected to the Central Manager;
2. VPN has been created on these devices, and the tunnel is established normally;
3. The tunnel between HQ and and branch devices has2 or more VPN connections, e.g., 2 dedicated lines, 1 dedicated line and 1 Internet line.

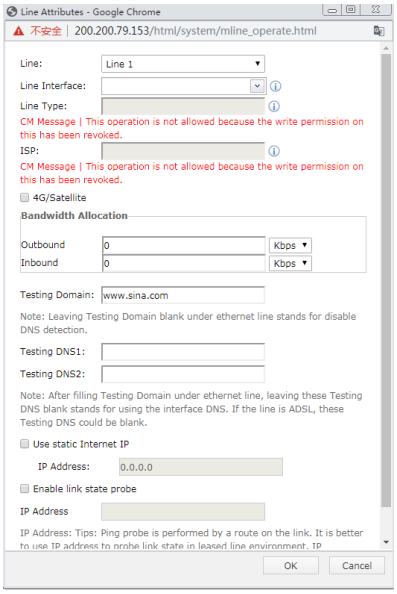
5.3.2 VPN Paths

1. Configure the types and the ISPs of the headquarter line and the branch line respectively in [SD-WAN Paths] - [VPN Paths].



2. Configure the specific bandwidth for lines on HQ VPN device and branch device, respectively.
3. Log in to the HQ WANO device and the branch WANO device respectively, and configure the line bandwidth and IP address According to the Actual bandwidth of each line.

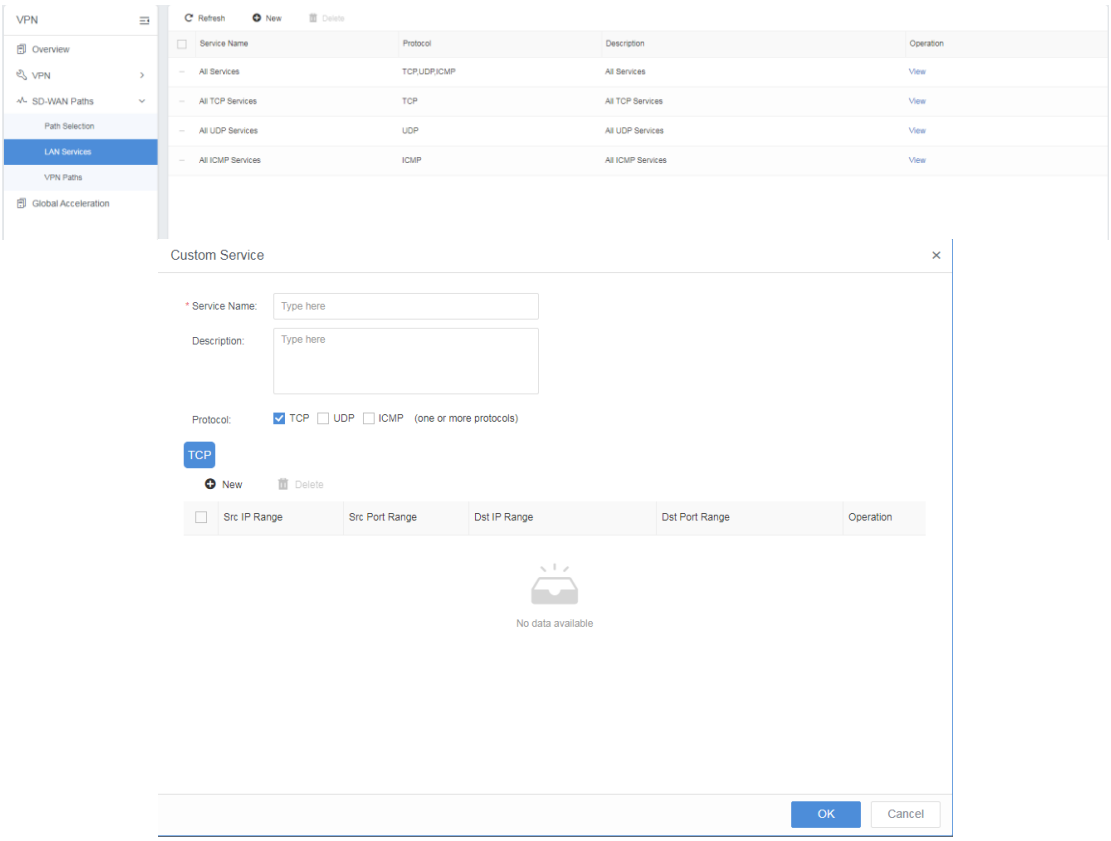




Because the device attempts to utilize line bandwidth much as possible and the bandwidth provided by certain ISP may not be up to the nominal value, it is suggested to set the bandwidth of multi-line device to 90%-95% of the Actual bandwidth of the line, in order to avoid the degradation of link quality, the increase in latency, packet loss and bad service experience after the link is on full load.

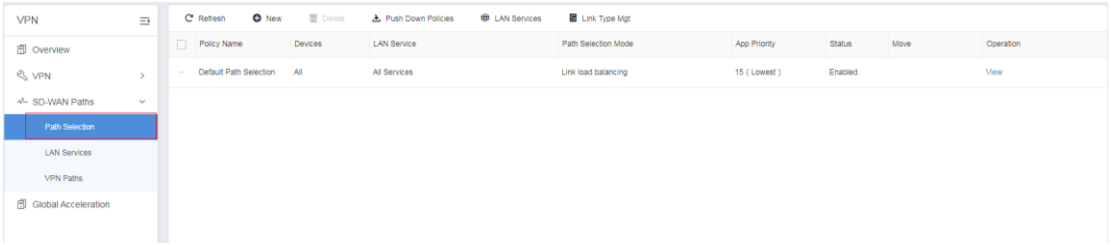
5.3.3 Defining LAN Services Routing Object

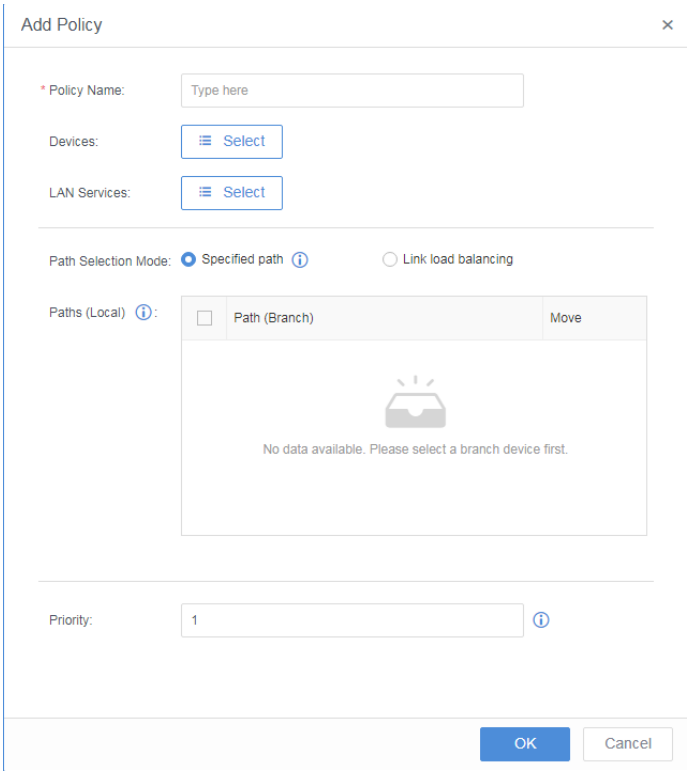
Define LAN service under the [LAN Services]..



5.3.4 Configuring Path Selection Policy

In SD-WAN Paths > Path Selection, click New to create the SD-WAN path selection policy. Then, select the existing branch device, select service, select Specified path] as path selection mode, and select a specific path.





[Policy Name] means the name of the policy.

[Devices] specifies the applicable VPN devices.

[LAN Services] specifies the applicable LAN services.

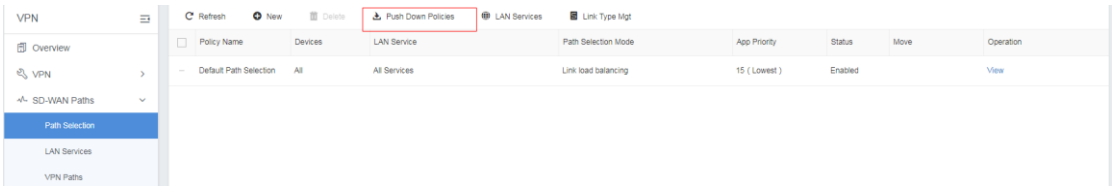
[Path Selection Mode]: Select path selection mode.

[Priority]: Select the flow control priority.

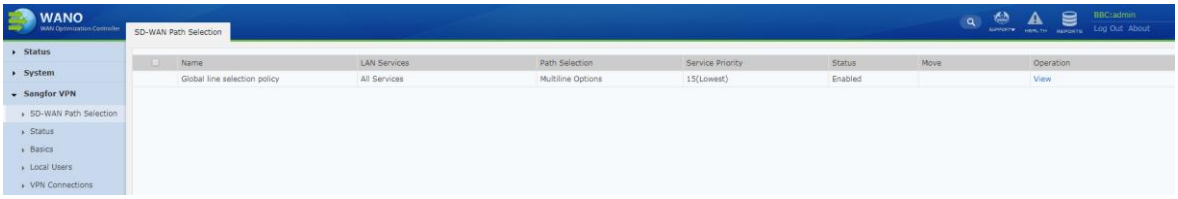
Move the SD-WAN path selection policy of the highest priority to the top, and policies will be matched from top to bottom.

5.3.5 Pushing Down Policy

1. After the policy configuration, the policy can be pushed down immediately.

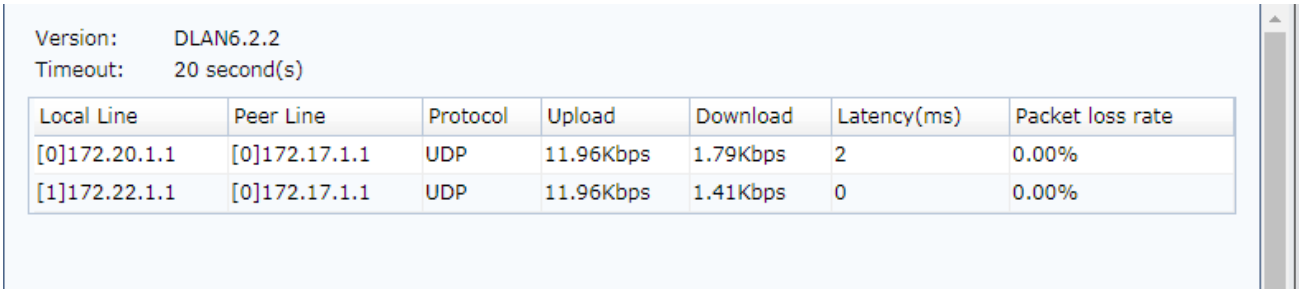


2. After clicking the **button** Push Down Policies, you may log in to branch devices and view the pushed down policies.



5.3.6 Effect Display

Log in to corresponding branch device to view the VPN status and VPN traffic, where the traffic is dispatched in Accordance with the specified path selection policy. The following figure shows the effects of specified line.



Version: DLAN6.2.2
Timeout: 20 second(s)

Local Line	Peer Line	Protocol	Upload	Download	Latency(ms)	Packet loss rate
[0]172.20.1.1	[0]172.17.1.1	UDP	11.96Kbps	1.79Kbps	2	0.00%
[1]172.22.1.1	[0]172.17.1.1	UDP	11.96Kbps	1.41Kbps	0	0.00%

5.4 Global Acceleration

[Scenario]

Following the development of the Belt and Road, more and more domestic enterprises go abroad. These enterprises need to establish networks between overseas branch offices and domestic headquarters. However, the network experience from many foreign countries is poor, affecting the data transmission between headquarter and branch offices. By establishing the global Access connection through the WAO, Global Access large screen shows status of lines in real time, so as to ensure line stability.

[Prerequisites]

1. The global Access service has to be provided, and corresponding license key files shall be imported to the device. The service files are described as follows:

1) The global Access service license exists in the form of file; the format of the license file used on Central Manager is different from that on WANO;
2) License key file on Central Manager: It includes the service information of all regions, named license.xls;
3) License key file on WANO:It includes the service information of single region, named as: region_bandwidth_start time_end time.csv, e.g., China_20Mb_20190603_20200603.csv;
4) This document only provides instructions on license key file used on Central Manager;
5) Importing non-official license key file is not allowed.

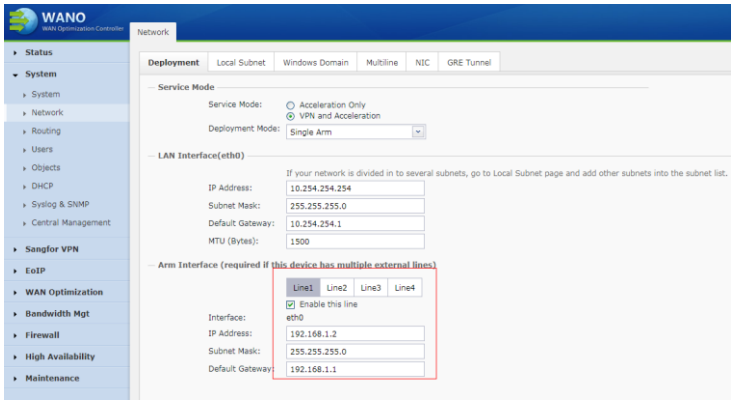
2. Add an outbound policy to allow TCP ports 443 and 12233 on the gateway device connected to the corresponding WANO.;

3. For the WOC device using the global Acceleration service, its license key shall support multiple lines, at least 2 lines.

[Note]

1. To ensure the line security, in addition to specifying one outgoing line, a connection can be established through the Internet.

2. When WANO is deployed in single-arm mode, multi-line must be enabled, and at least 1 line must be configured, otherwise the global Acceleration service cannot be connected.



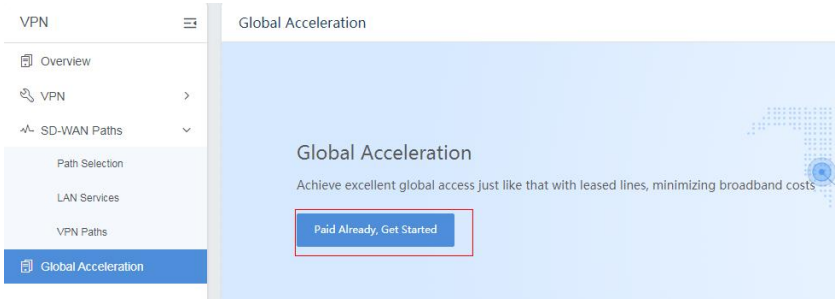
3. When two WANO devices form high availability environment, it is necessary to import the global Acceleration service license key file to the Active WANO device only, which will be synchronized to the standby WANO device automatically.D not import the same license key file to the two WANO devices.

4. Due to limitations of the realization mechanism of global Acceleration service, the corresponding outgoing line will multiplex a part of bandwidth resources of the outbound line. When you stop using the global Acceleration service, please be sure to restore the bandwidth settings of the line.

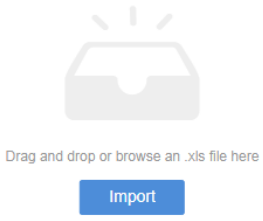
[Steps]

1. Import license key file

1) Log in to Sangfor Central Manager Web admin console, click [VPN] -> [Global Acceleration] -> [Paid Already, Get Started]



2) Click Import, select the corresponding .xls license key file file, and click OK to import the file.



2. Associate device

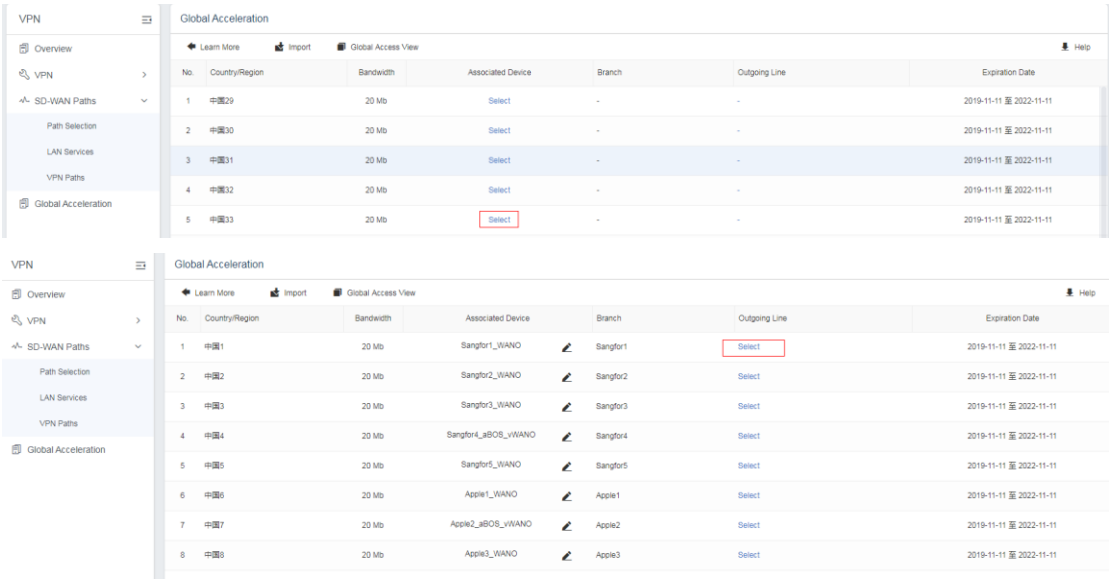
1) Service Description:

The detail information of regions included in the license key file can be viewed on the Global Acceleration page;

Each service can only be associated with one WANO device or one pair of Active and standby WANO devices; and one WOC device can only be associated with one service at the same time.

Click Select under Associated Device column, select the corresponding device in the pop-up box, and click **OK** to bind the service (it is unnecessary to separately import the license key file onto that WANO device; Central Manager will automatically push down the selected license to the WANO device);

1) When selecting a device, you may specify outgoing line and this is optional; when needed, please be sure that the selected line can connect to the Internetnormally, and the line bandwidth meets the bandwidth requirement for service activation.



Click Learn More to return to the introduction page of global Acceleration.

Click Import to import a new license key file.

Click the Global Access View to go to the [Home] -> [Global Access] page.

3. Check the Global Acceleration status of WANO

1) Log in to the Web admin console of the WANO device which has been associated with global Acceleration service (it can be Accessed with the SANGFOR CENTRAL MANAGER single sign-on function);

2) Click [Maintenance] -> [Global Acceleration] to check whether the status is "Connected". If so, it means that the WANO device can use the service;

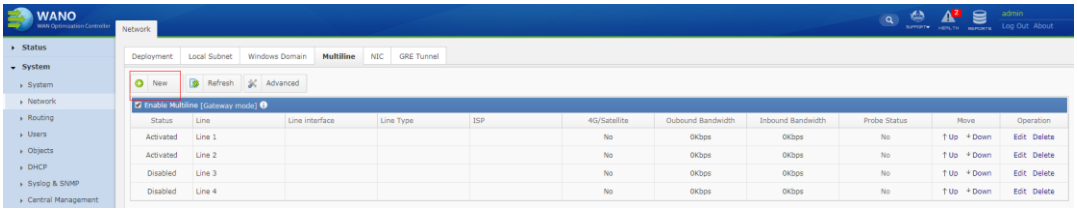
3) Check whether the "Region", "Bandwidth" and "License Expiration Date" are consistent with the service selected by the Central Manager;

4) Check whether the software-defined IP address has been generated, and write down that IP address of the headquarters WOC device.

Note: The software-defined IP address uses the 32-bit mask 192.168.160.x by default; if the same network segment exists in the intranet

4. Configure multi-line

1) Go to [System] -> [Network] -> [Multiline]; click New, or click Edit to edit the existing line (optional);

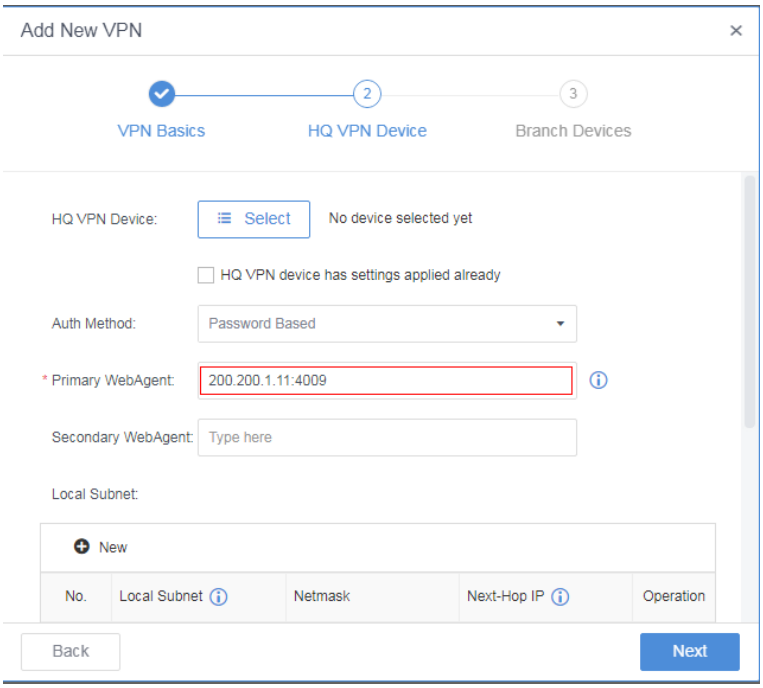


2) Select "vwan" for line interface, and configure the applied bandwidth value of the virtual outgoing line used for global Access. For instance,, the outgoing line is set to line 1 when configuring virtual outgoing line, the bandwidth of the corresponding physical link is 50 M, and the bandwidth of the virtual outgoing line is 20 M. Then that virtual outgoing line occupies 20 M bandwidth of that link, and only 30 M bandwidth can be used for Internet Access.

3) Check the [Enable Multiline] box, the configuration changes take effect after being saved.is successfully.

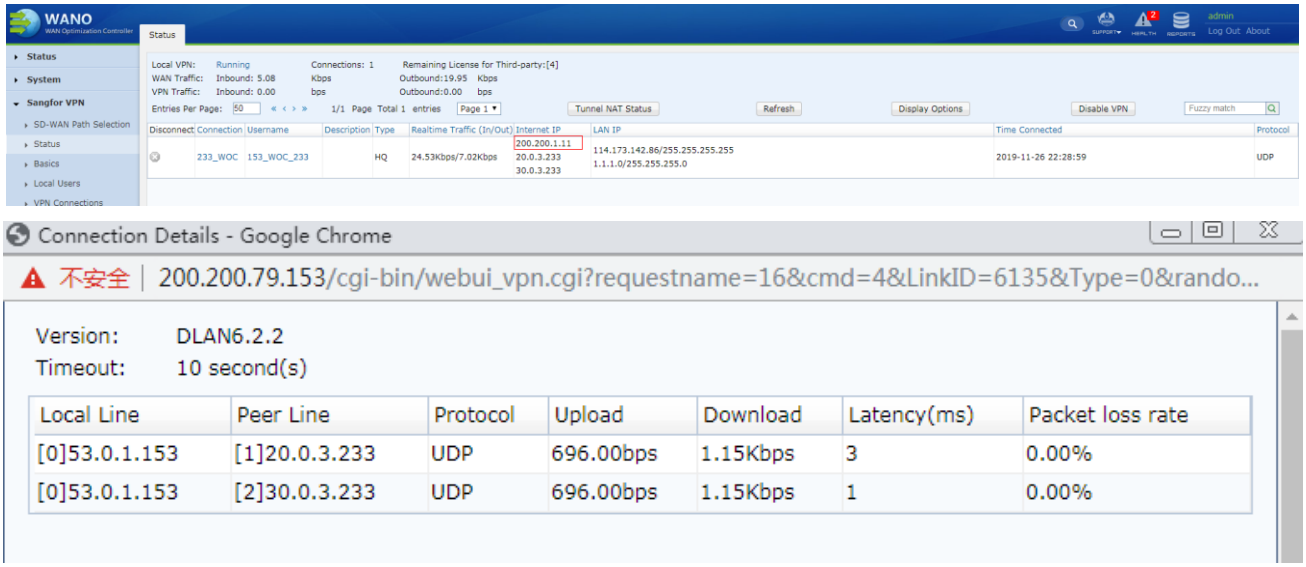
5. Create VPN on Central Manager

Create VPN for the device associated with global Acceleration service. To ensure the global Acceleration effect and the business stability, it is recommended to establish another connection via the Internet, where the IP addresses of vWAN virtual network adapter and public network are configured in the primary WebAgent (only the virtual outgoing line is configured in the example).

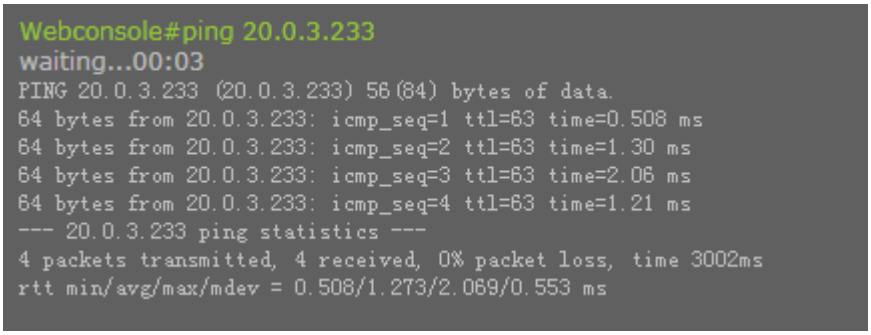


6. Verify the Result

1) Connection between headquarter and branch device has been established successfully through the virtual outgoing lienline.



2) The branch device is able to Access the business system at headquarter.



Chapter 6 Centralized Management of Policies

6.1 Supports to Central Management of Branch Policy

The following describes requirement for branch device version if branch device wants to connect to Central Manager or use policies pushed down from Central Manager.

Device Type	Version Required for Central Management	Version Required for Policy Distribution
IAM	Above 12.0.18	Above 12.0.18
vIAM	Consistent with IAM	Consistent with IAM
NGAF	7.5.2 (on demand)/8.0.7	7.5.2 (on demand)/8.0.7
vAF (on aBOS only)	7.5.3 (on demand)	7.5.3 (on demand)
WANO	Above 9.5.3	Above 9.5.3
vWANO (on aBOS,Sangfor acloud,XYcoud)	Above 9.5.3	Above 9.5.3
MIG	Above 6.2	Above 6.2
aBOS	3.2.1	Support vIAM, vAF and vWANO distribution
Note: 1. The supports list shall be subject to the latest version of Central Manager; 2. Cental Manager does not support connection from the devices outside the above list; 3. Refer to the release document of certain device type for the functions supporting pushdown. Future supports will be continuously updated along with the release version.		

6.2 Centralized Management of IAM Policy

[Scenario]

Central Manager supports the central management and the policy pushdown of IAM12.0.9 and later versions. If version of the managed IAM device is earlier than the version 12.0.9, the central management and the policy pushdown can be done on the Central Management Console (CMC).

The consistency between the branch device and the policy template is maintained by upgrading the template, for the purpose of easier unified pushdown of policy from Central Manager.

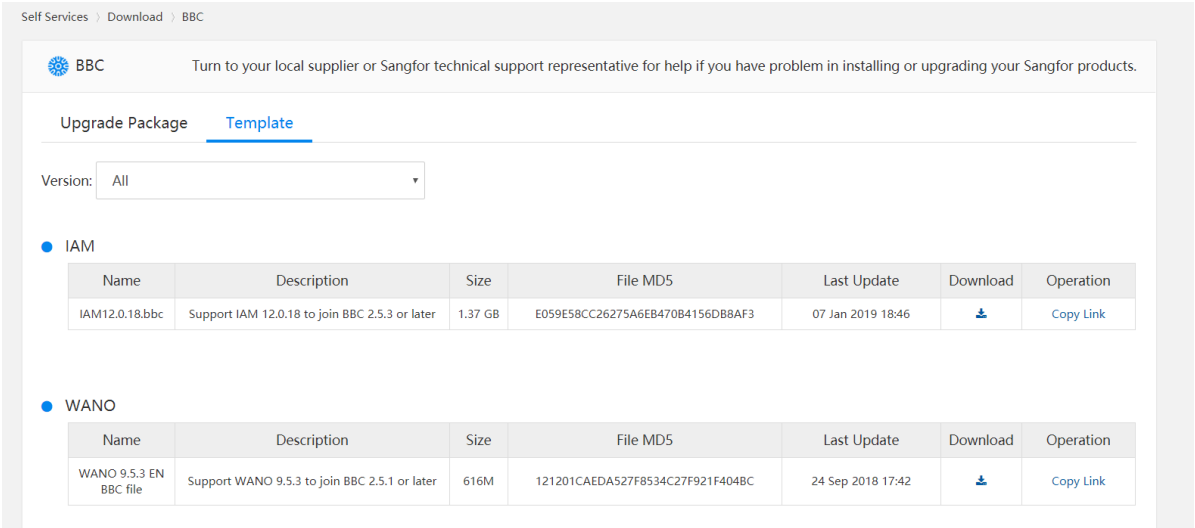
[Prerequisites]

1. The branch device is connected to Central Manager.
2. View the version information of the branch device to check whether it meets the requirement for CM and policy pushdown.

6.2.1 Downloading Branch Image File

Central Manager has restructured the architecture of CMC, replaced the original interface library with the docker, provided the high-performance framework, and simplified the configuration; and it supports the management of multiple versions; to Achieve the bulk management of branch device policies, it is necessary to import the template of the connected branch devices. Go to the site below to download:

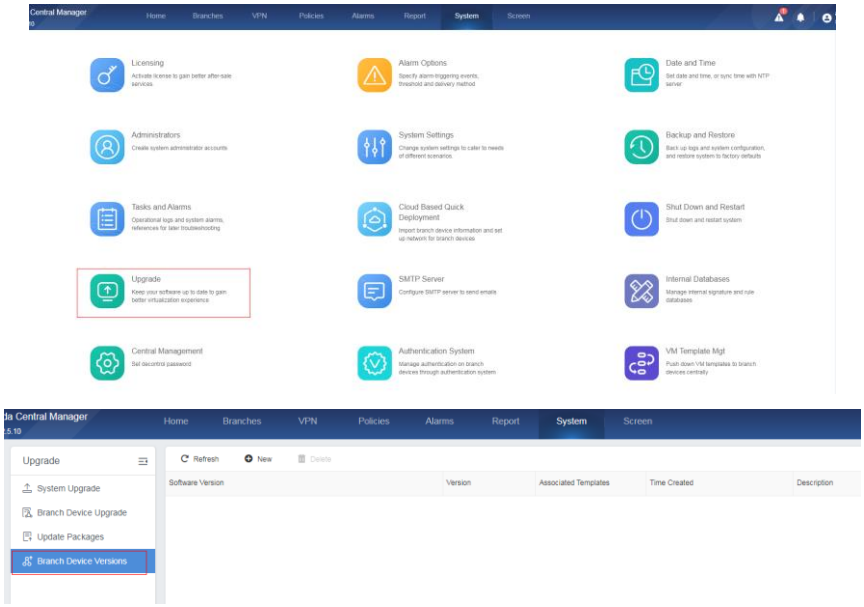
http://community.sangfor.com/plugin.php?id=service:download&action=view&fid=88#/27/all



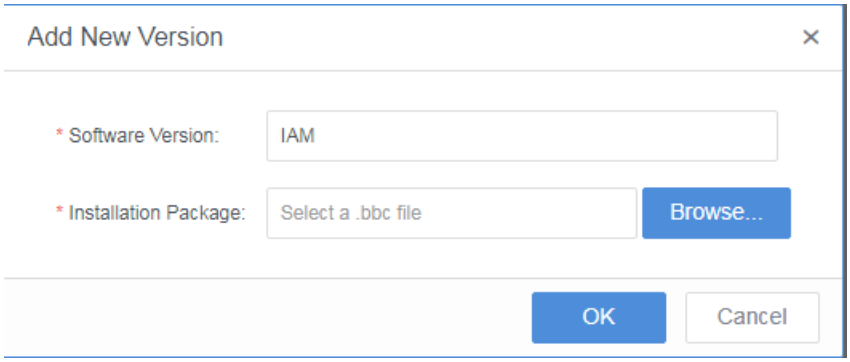
The suffix of the managed branch device template file is .Sangfor Central Manager

6.2.2 Importing Branch Device Template

1. In System, click the [Upgrade], select [Branch Device Versions]. Click [New] to enter the Add New Version page.

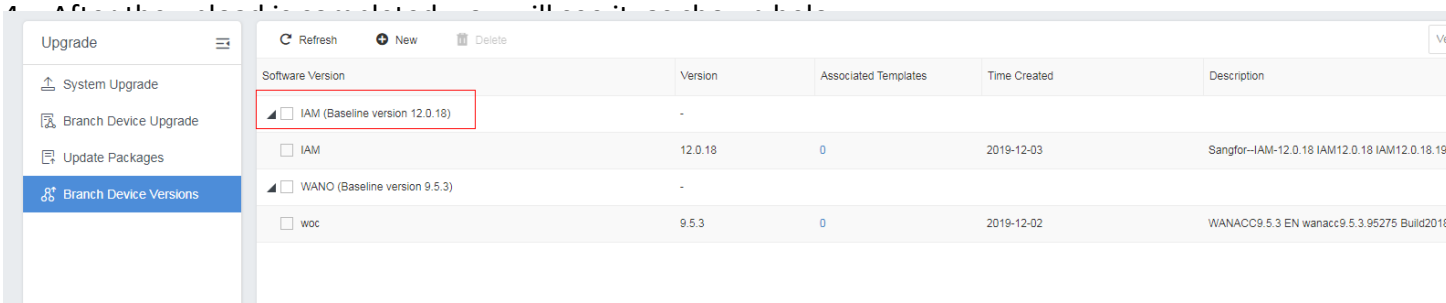


2. Specify the version name, and click [Browse] to select the downloaded template file.



3. Select the downloaded .Sangfor Central Manager file, which is an image file of branch device and wait for upload to complete.

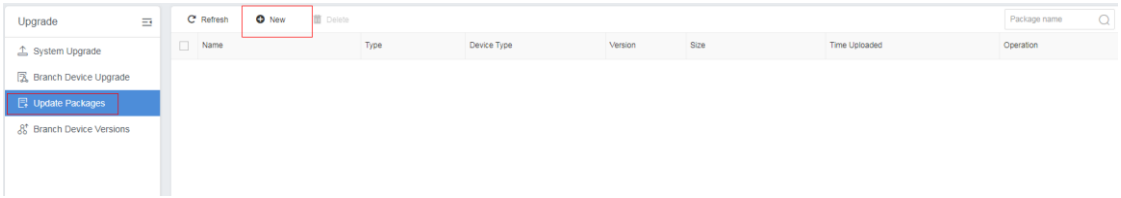
4. After the upload is completed, you will see it on the page below.

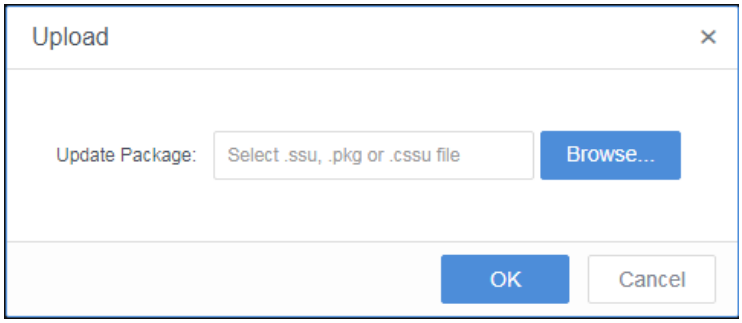


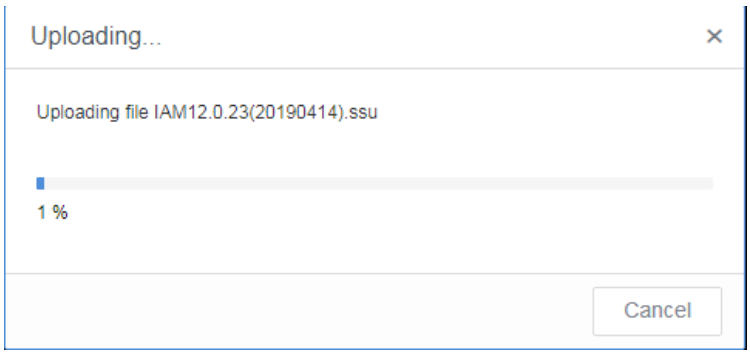
6.2.3 Upgrading Image File

The version of the downloaded branch device image file is the first version of the branch device the product line is connected to the SANGFOR CENTRAL MANAGER; if it is inconsistent with the version of managed branch device, i can be upgraded to the corresponding version.

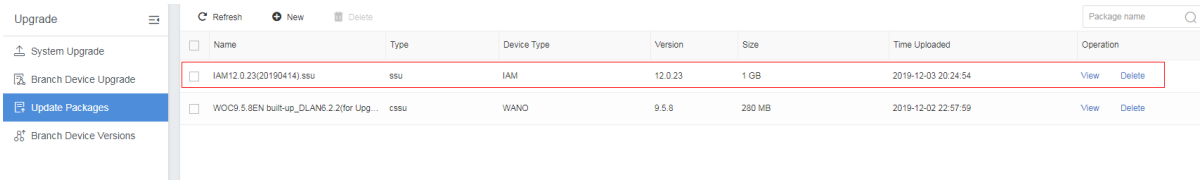
1. Download the update package of corresponding product.
2. In System > Upgrade > Update Packages, click New and select the update package downloaded in the previous step and upload it to the Central Manager platform.



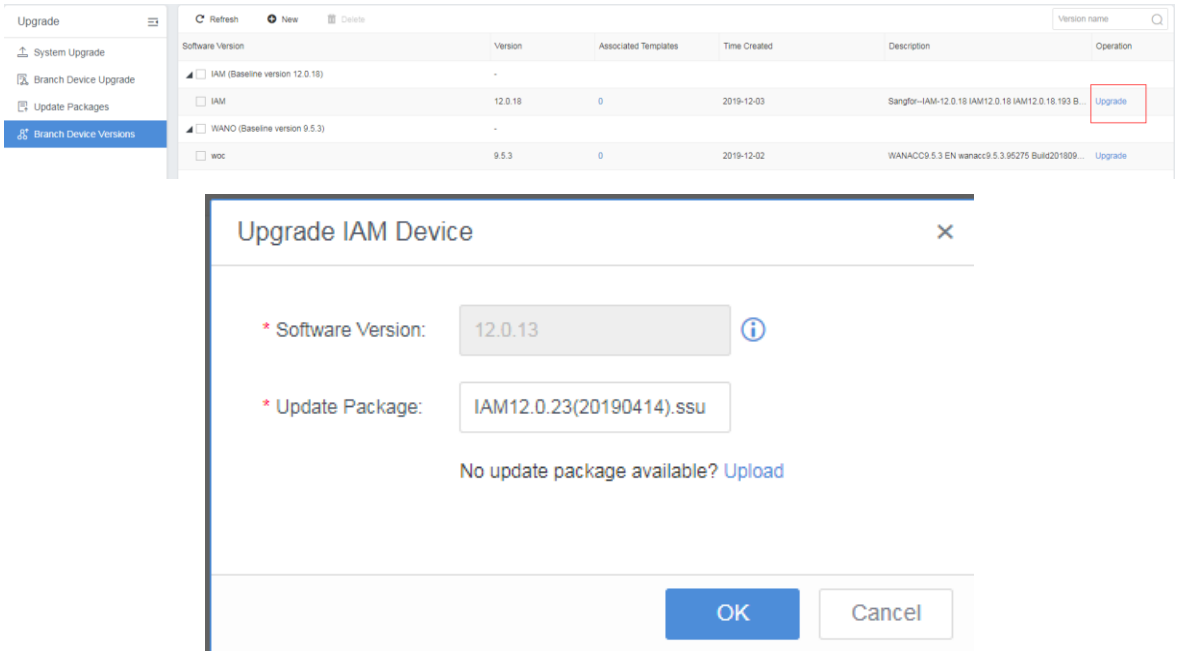




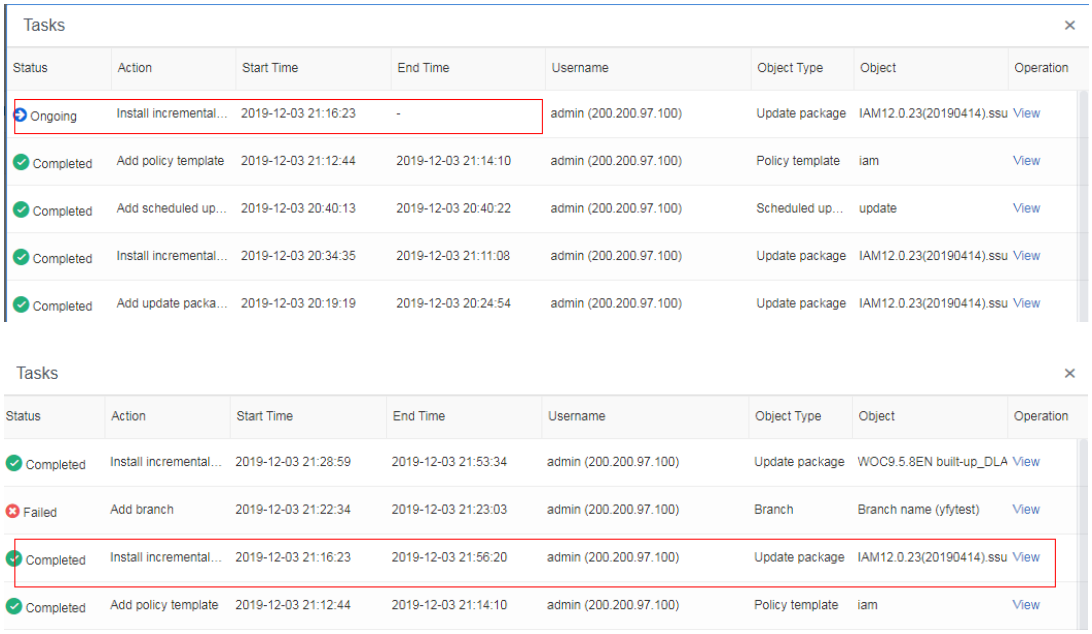
3. After the upload is completed, it will be added to Branch Device Versions list, as shown below:



4. Find the image file to be upgraded in the [Branch Device Versions], and click [Upgrade].



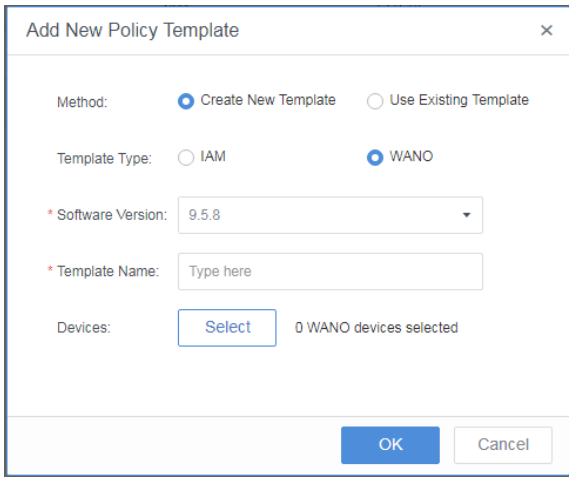
5. The upgrade task can be viewed in the Tasks in System > Tasks and Logs.

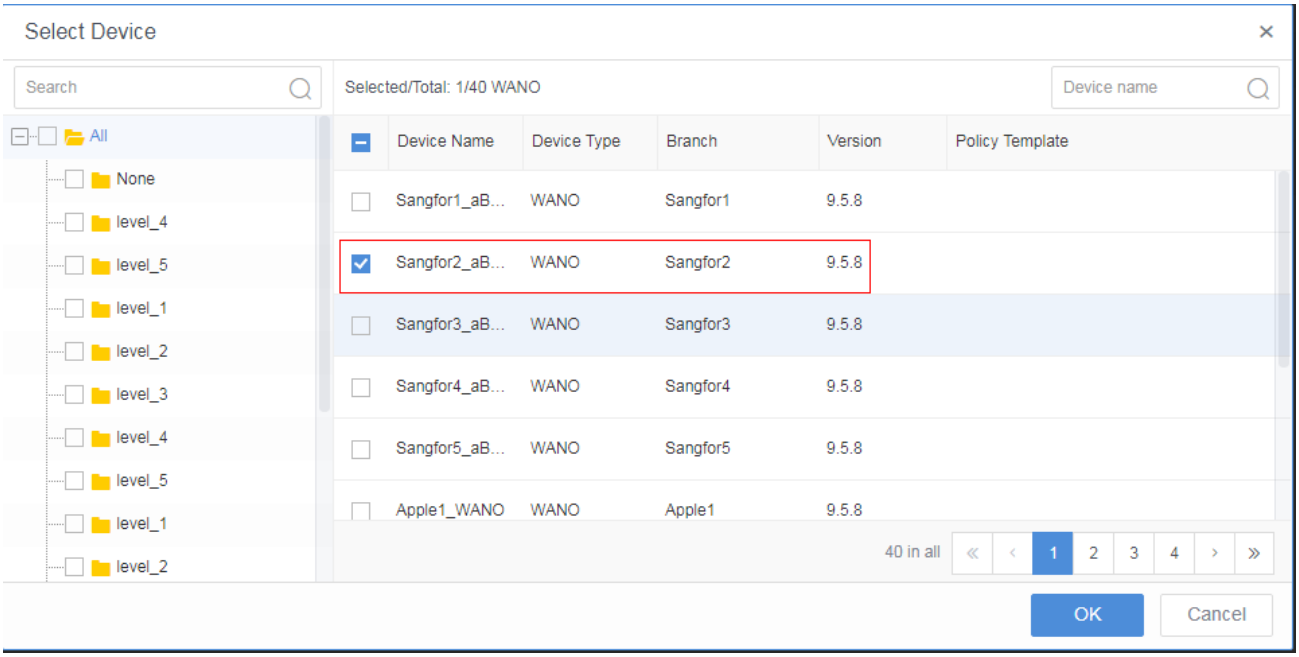


6.2.4 Creating Policy

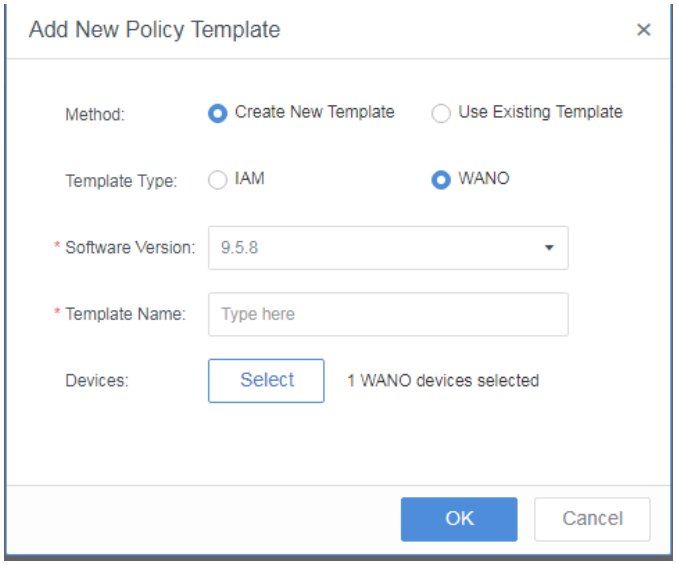
1. Click [New Policy Template] in Policies .

2. Select [Create New Template] as the method, choose template type and specify template name, then click [Select] to select branch devices.



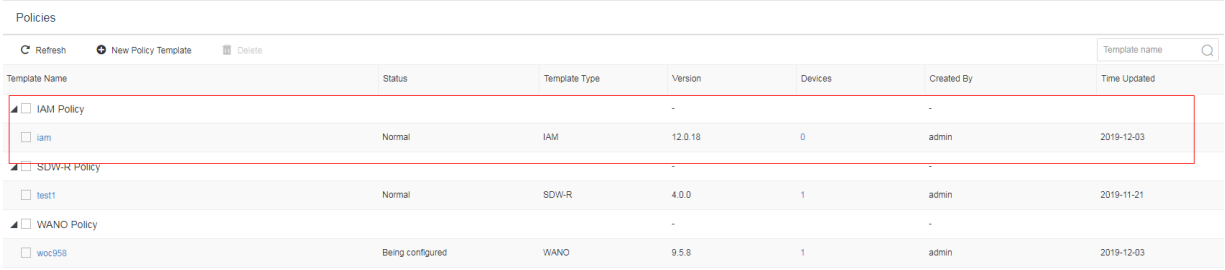


3. After choosing devices, click [OK] to save the settings.

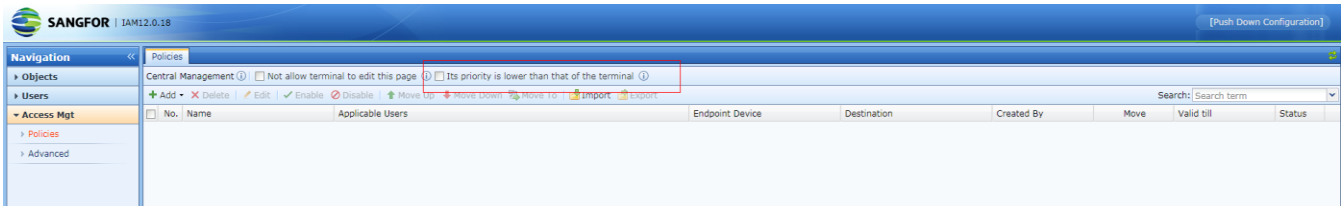


6.2.5 Configuring Policy Template

1. Click on the newly-created policy template to go to the policy configuration page.

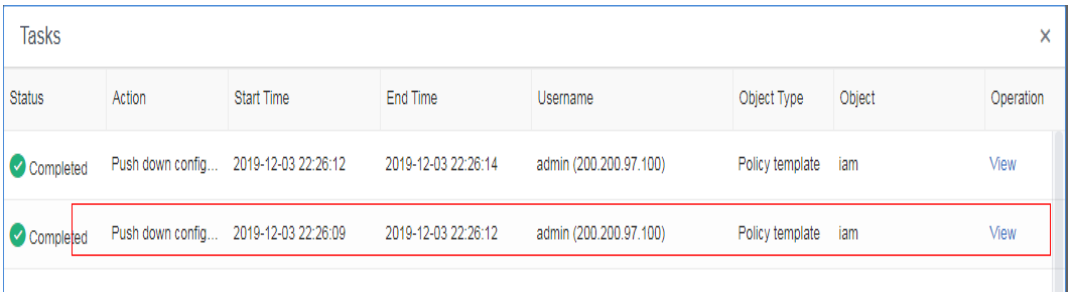


2. On this page, the detailed contents of the policy can be seen, and the policy can be configured According to Actual demands; To use the policy created on branch device preferentially, check the option Its priority is lower than that of the terminal.

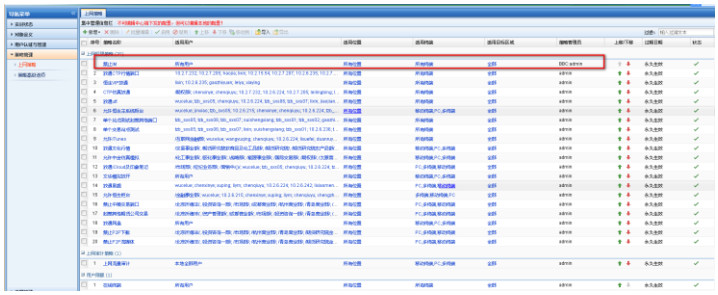


6.2.6 Checking Configuration Pushdown

1. If the [Push Down Configuration] is not clicked, the default time interval of automatic pushdown is 30 mins.
2. View tasks to check whether the configuration is successfully pushed down; click [View] to view task details.



3. If the configuration has been pushed down successfully, the pushed-down policy can be seen on the branch device.



6.3 Centralized Management of NGAF Policies

[Scenario]

Central Manager supports the central management and the policy distribution of version NGAF7.5.2 (on demand)/8.0.7.

The consistency between the branch device and the policy template is maintained by upgrading the template, for the purpose of easier pushdown of policy from Central Manager.

[Prerequisites]

1. The branch device is connected to the Central Manager.
2. View the version information of the branch device, check whether it meets the requirement for CM and policy pushdown (refer to Chapter 6.1 for more information).

[Steps]

Refer to the steps in the centralized management of IAM policies.

6.4 Centralized Management of WANO Policies

[Scenario]

CM supports the centralized management and the policy pushdown of WOC9.5.3 and later version.

The consistency between the branch device and the policy template is maintained by upgrading the template, for the purpose of easier unified pushdown of policy on the CM.

[Prerequisites]

1. The branch device is connected to the CM.
2. View the version information of the branch device, check whether it meets requirements for CM and push down (refer to Chapter 6.1 for more information).

[Note]

When the connected device is WANO, attentions shall be paid to the modules supporting policy pushdown.

[Steps]

Refer to the steps in the centralized management of IAM policies.

6.5 Centralized Management of aBOS Policies

[Scenario]

CM supports the centralized management and the policy pushdown of vIAM, vNGAF, vWANO deployed on aBOS.

The consistency between the branch device and the policy template is maintained by upgrading the template, for the purpose of easier unified pushdown of policy from the CM.

[Prerequisites]

1. Branch devices like aBOS vIAM, vNGAF and vWANO are connected to the CM.
2. View the version information of the branch device, check whether it meets the requirements for d CM and policy pushdown (refer to Chapter 6.1 for more information).

[Note]

For virtual components such as vIAM, vNGAF and vWANO in aBOS device, the consistency between the version of policy template and the version of virtual component shall be guaranteed when distributing policy.

[Steps]

Refer to the steps in the centralized management of IAM policies.

Chapter 7 Unified Management of Branch Devices

7.1 Unified Upgrade of Branch Device

On Central Manager, you can perform safe and reliable upgrade on the connected branch devices, in order to satisfy the requirement of concurrent upgrade of large number of branch devices.

[Scenario]

Through CM, administrator can perform bulk upgrade on the branch devices.

[Prerequisites]

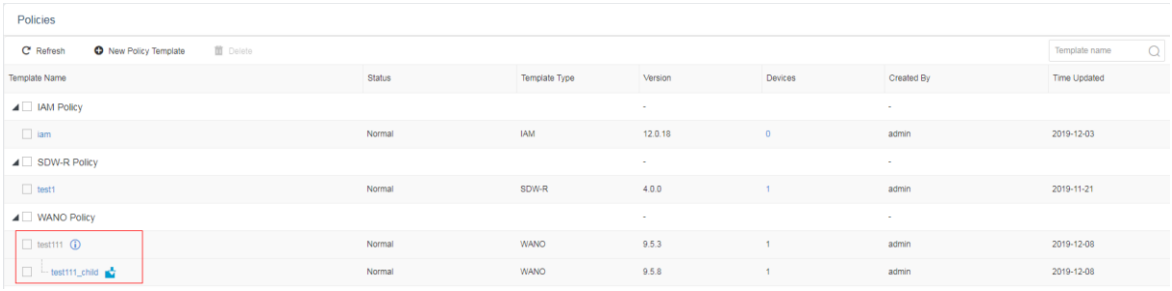
1. The branch device is connected to CM normally, and the access status is normal;
2. CM has been imported the template file of the branch device version before upgrade;
3. CM has been imported the .ssu update package to upgrade branch device.

[Note]

1. When creating the upgrade task, by default, the CM will preferentially download the update package from the GCS; if the GCS has no update package of the corresponding version, the update package will be downloaded from the CM; if the status of the upgrade task is observed in real time, it can be found that all branch devices will re-download update package from the CM if download process is interrupted.
2. After the upgrade task is created, it is suggested to control the CM bandwidth on the traffic control device at the Internet outlet; the CM itself has no rate restriction on downloading the update package; when several branch devices are downloading update packages from the CM, the whole bandwidth of the Internet outlet may be consumed by the download tasks.
3. At present, the CM supports only the upgrade plan by distributing pkg and ssu upgrade packages, that is, the KB package or sp package of each product line must be packed into the .ssu format for the unified distribution through the CM.
4. Multiple branch devices can be specified the upgrade task, but by default, there are only 20 concurrent downloads allowed by the CM, namely, only 20 branch devices can download update package from the CM at the same time.
5. After the connected branch device has finished downloading the update package and upgrade with the update, the CM cannot manage that branch device, until the upgraded device has rebooted and connected to the CM again. When exception occurs during the upgrade process of branch device, e.g., the branch device cannot start up or connect to the CM, the issue shall be fixed on site.
6. If the branch device image has been upgraded but the connected branch device has still not, the policy template owned by branch device must be an old version, and the image file in the Branch Device Versions swill split.
7. As shown in the figure below, after upgrading the IAM12.0.9 image to the version 12.0.12, the

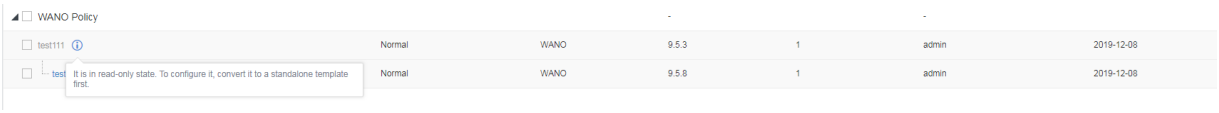
image file of the version 12.0.9 will be reserved, and an upgraded 12.0.12 image file will be split out.

8. The oldest and the latest version image files on the CM cannot be deleted.
9. If one policy template is associated with multiple branch devices, when some of the branches are upgraded, the policy template will split, and the upgraded branch devices will be associated with the split new version template, and the branch devices which are not upgraded will still be associated with the previous policy template.

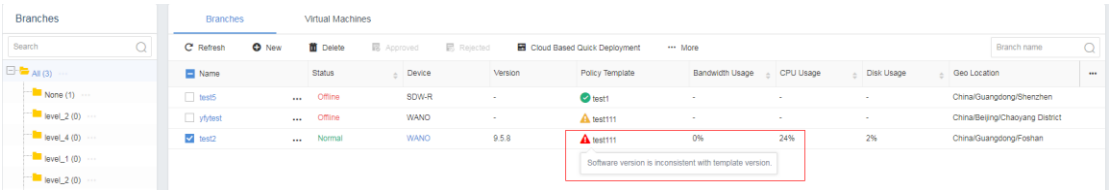


10. It is estimated to take about 40 minutes to split and associate the policy template with device.

    The split policy template is associated with the old policy template, and the old one will not be able to be configured.



11. The new version policy template will be converted to standalone template after all connected branch devices have been upgraded to the new version, and the old version policy template will be deleted automatically.
12. If the branch devices associated with the old policy template are deleted manually on the Branches page on CM, the process above will not be necessary, namely, the new policy template will not be converted to standalone template automatically, and the old template will not be deleted automatically. The new policy template has to be converted to standalone template manually.
13. If the branch device is separately upgraded by using the Sangfor Updater, and the CM has not been imported the image file or upgrade package of corresponding device, image and template split will not occur on the CM, the Branches page will prompt the error of inconsistency between device version and template version, and the pushing down of configuration of policy template associated with this branch device will also fail.



14. The CM manages the branch devices centrally; and the supported branch device upgrade procedure is as below:

    1) Upload the update package - upgrade the branch version image file - create upgrade task on CM to upgrade the branch device;

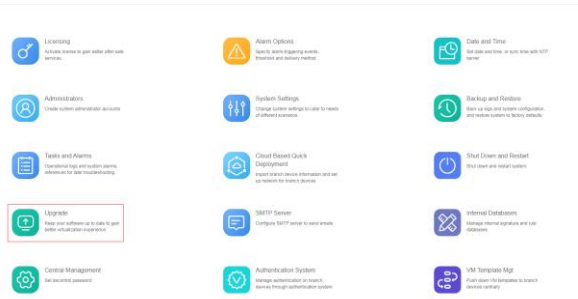
    2) Upload the update package -create upgrade task on CM to upgrade the branch device;

    3) Upload the update package - upgrade the branch version image file - use the Sangfor Updater to upgrade the branch device directly.

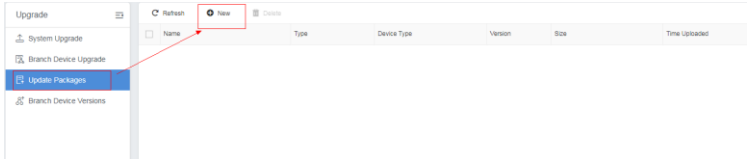
[Steps]

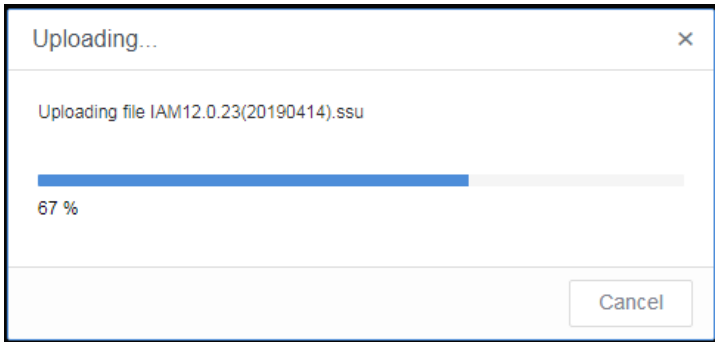
Step 1: upload the update package;

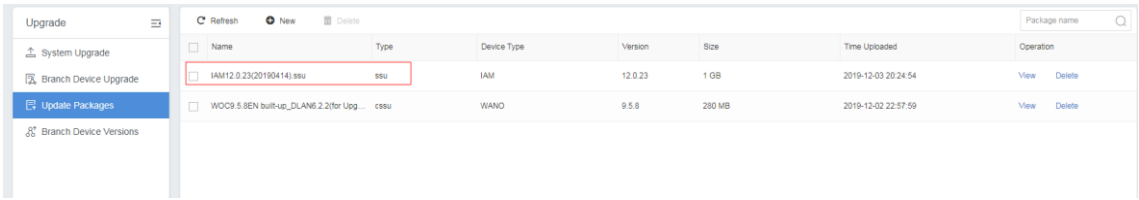
1. Click the [Upgrade] in System.



2. Select the [Update Packages], and click [New].

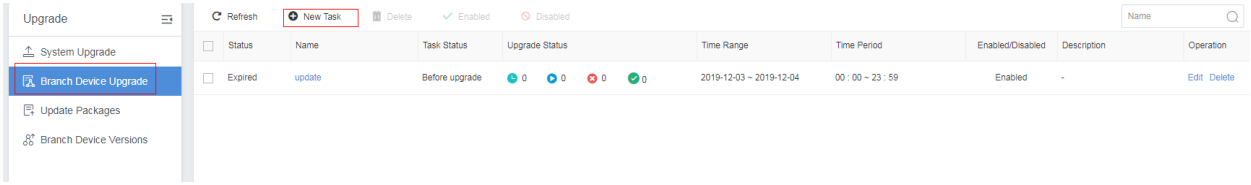




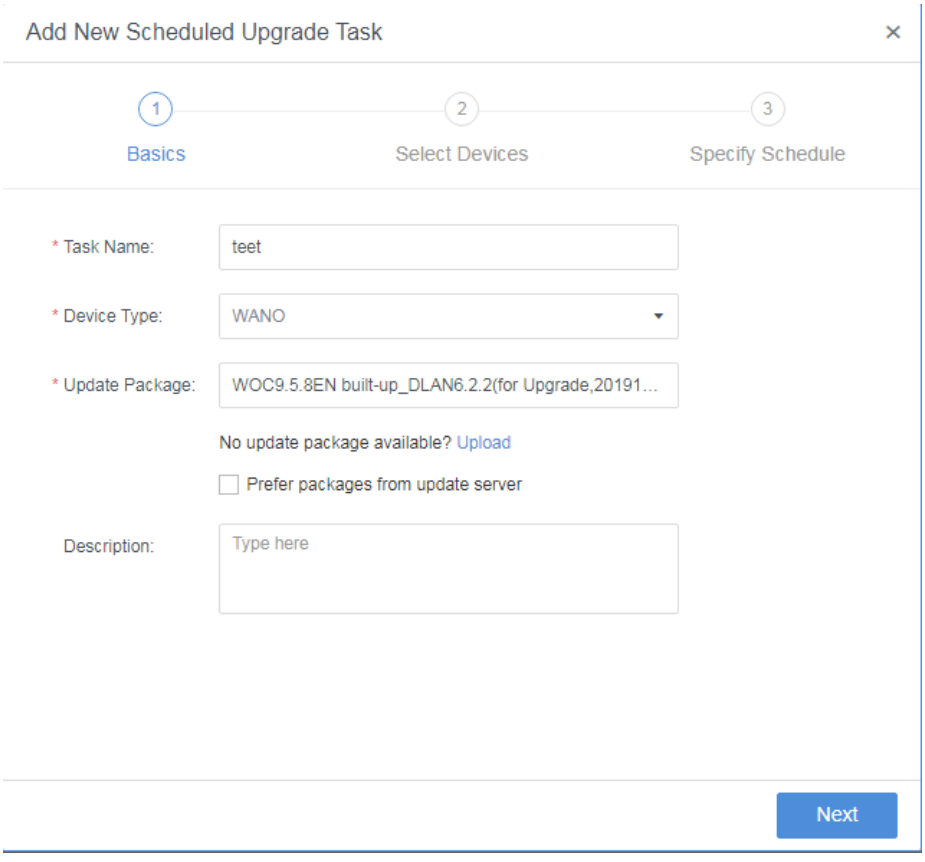


Step 2: Create the upgrade task;

1. Click [New Task] on the [Branch Device Upgrade] tab



2. Fill in the basic information for the scheduled upgrade task, and click [Next]



Relevant parameters are as follows:

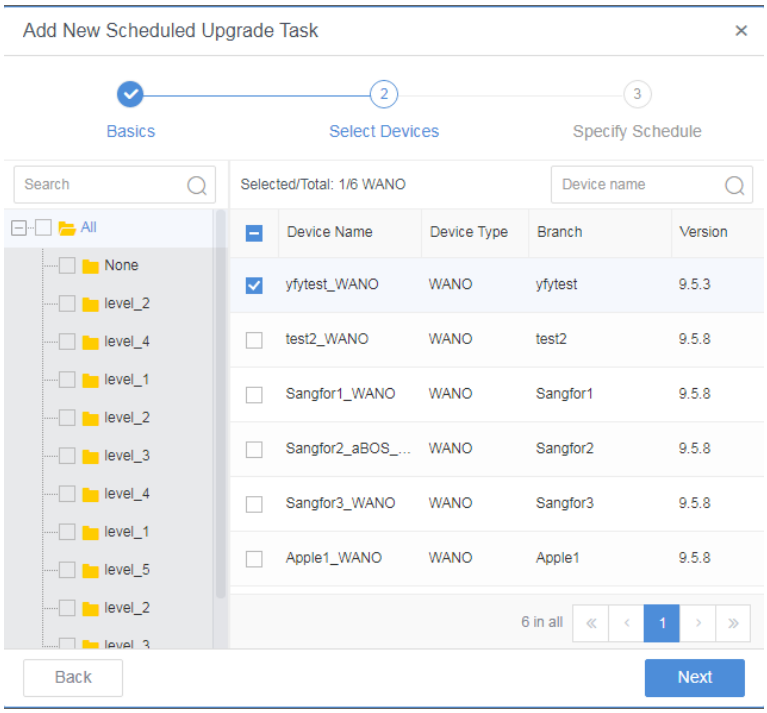
[Task Name]: Specifies the name for the upgrade task.

[Device Type]: Specifies the type of device to be upgraded, e.g., IAM or SG.

[Update Package]: Select the corresponding update package to be uploaded.

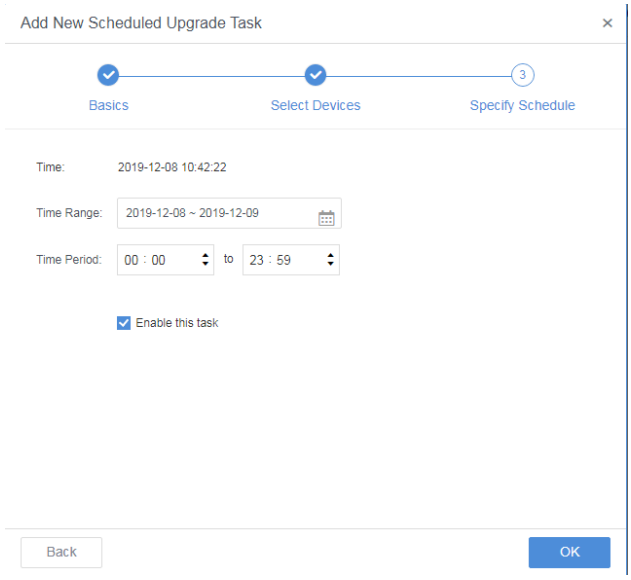
[Prefer packages from update server]: Check this option so that the branch devices will preferentially download the update package from the GCS (a public Sangfor update server); if the GCS server has no update package of the corresponding version, the update package will then be downloaded from the CM.

3. Select the branch devices to be upgraded, click [Next].

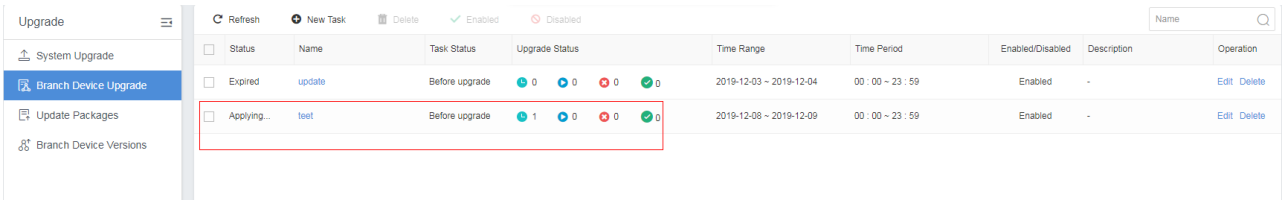


Step 3: Execute the upgrade task;

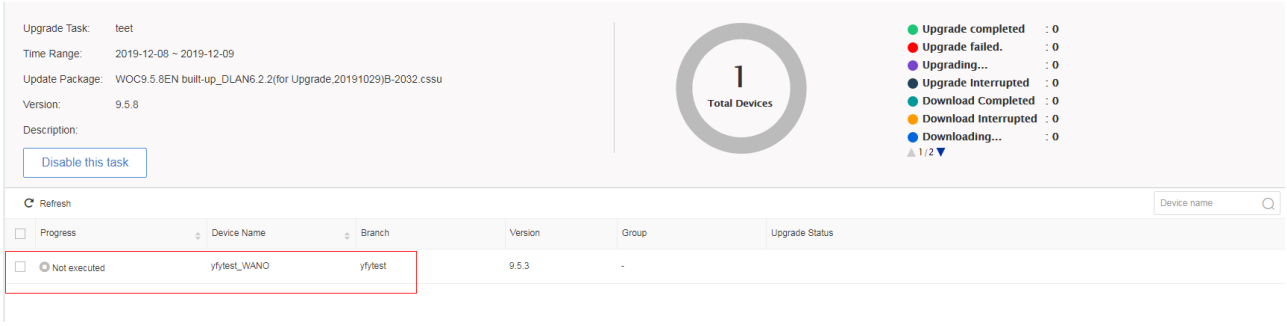
1. Select the execution time of the upgrade task, and then click OK.



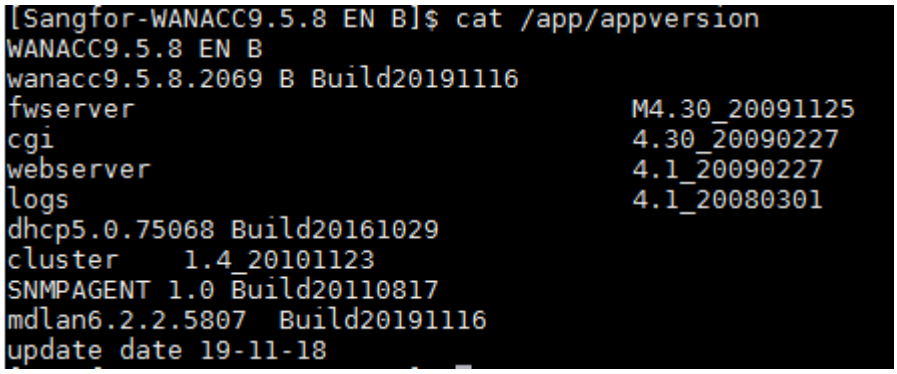
2. After creating the task and waiting for it to take effect, CM will automatically issue the upgrade task to IAM device for execution.



3. Click the name of the upgrade task, you can view the upgrade records of the device on CM.



4. The branch devices will be upgraded to the corresponding version, and there will be records of upgrade.



7.2 Updating License Key of Branch Devices

CM supports bulk reporting and update management of the license keys at the controlled terminals of the branch.

[Scenario]

CM allows the controlled terminal to report the license keys, and exports and imports the license keys at the controlled terminal in batches through CM so as to meet the requirement of unified update and management for the license keys of the branch.

[Prerequisites]

The branch device has been connected to CM normally, and has reported its own license keys normally.

Prepare the license keys in advance, and back up the existing license keys of the branch device.

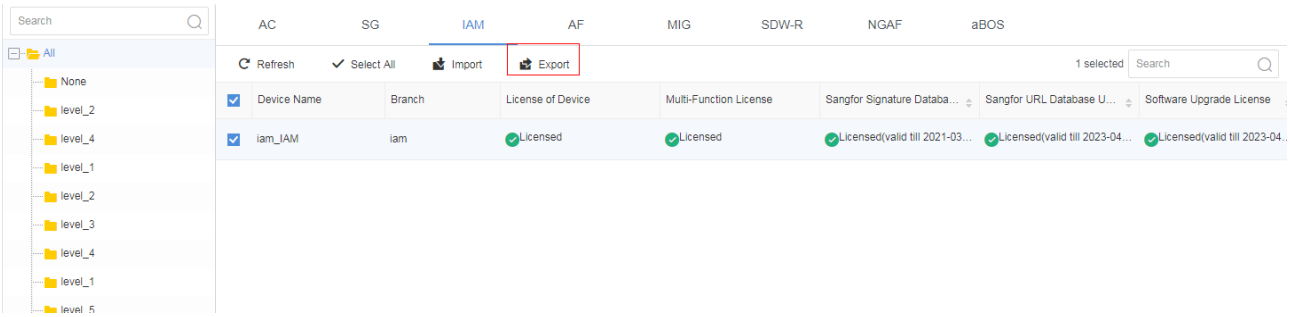
[Note]

When exporting the license keys in bulk from CM, only the gateway ID will be exported but not license keys of certain functions..

When the branch device is connected to CM for the first time, it takes about 5 minutes before triggering a report on license keys.

[Steps]

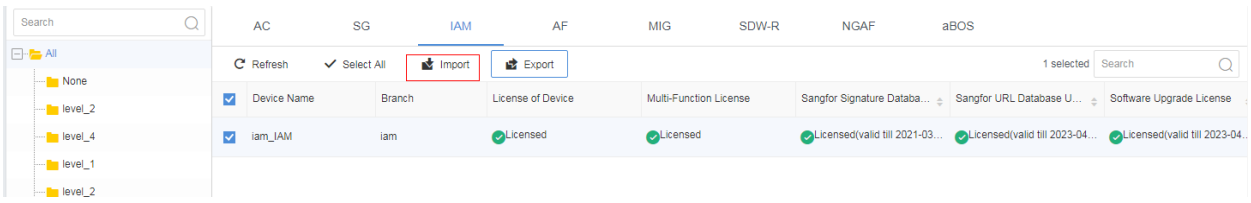
1. Check the branch which will issue the license keys, click More > **Export**.

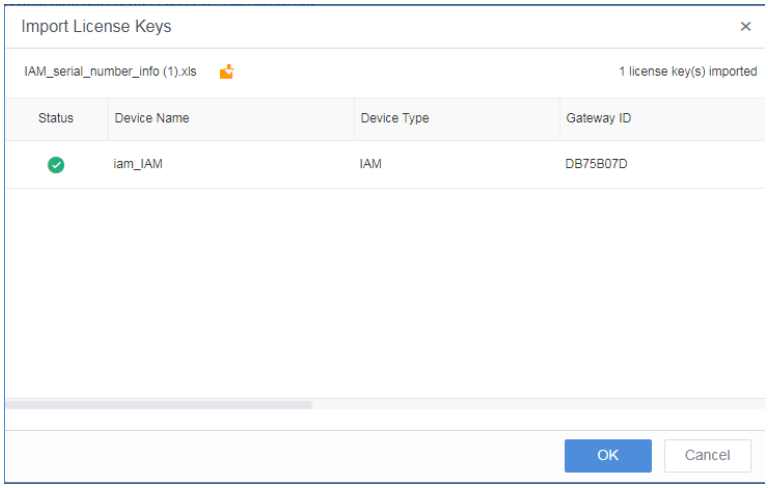


2. In the exported file, fill in the corresponding license keys.

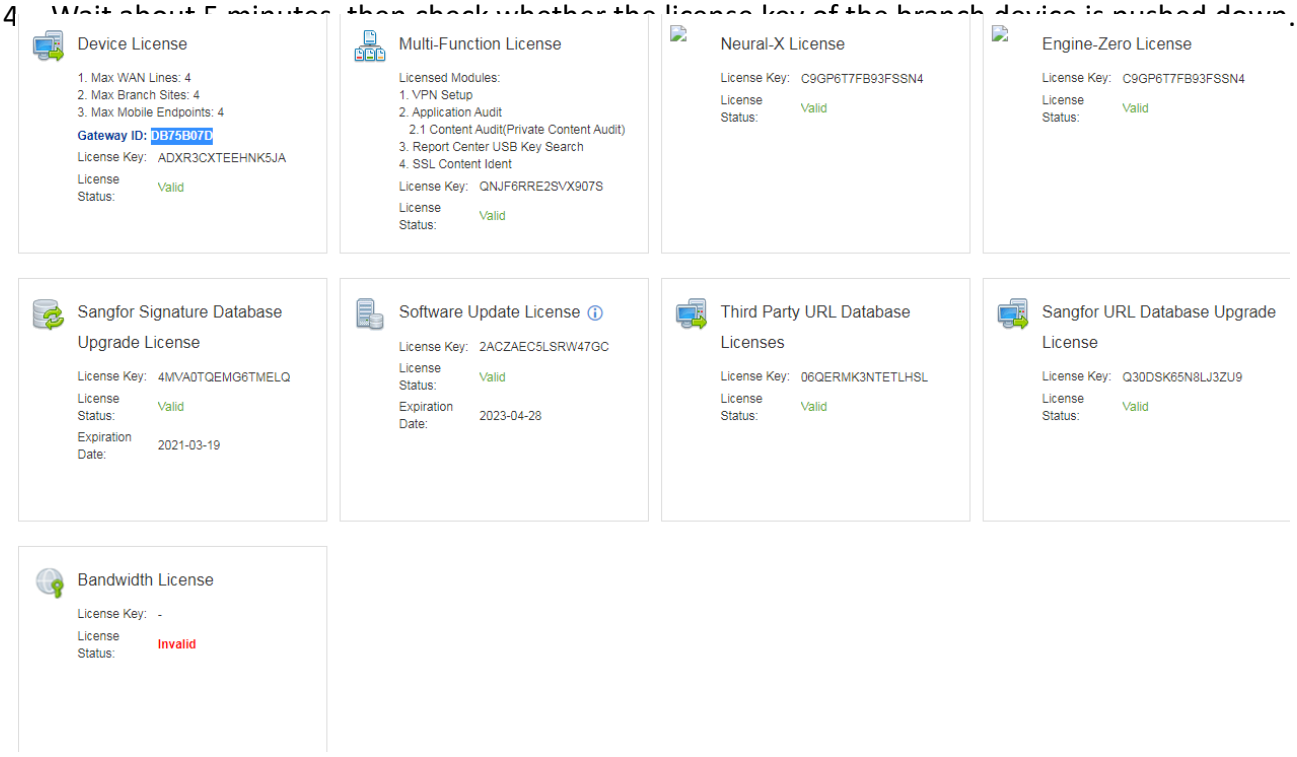
A	B	C	D	E	F	G	H	I	J	K	L
Device Name	Gateway ID	Device Type	Device License(SN)	Multi-Function License(multi)	Neural-X License(kvsn)	Engine-Zero License(savesn)	Application Signature Database Upgrade License(update)	Software Upgrade License(software)	Bandwidth License(bandwidth)	Third Party URL Database Licenses(parurl)	Sangfor URL Database Upgrade License1(updateurl)
test_IAM	0724ASJF	IAM			DFJSFJSIOFJSOIFJI		SDFSIOGJMDSFGA				

3. Import the file to CM.





4 Wait about 5 minutes, then check whether the license key of the branch device is pushed down.



7.3 Centralized Backup of Branch Devices

[Scenario]

CM supports bulk backup of the configuration files of branch devices, which solves the problem that the device configuration cannot be restored quickly in case of a failure of branch devices because there is has no IT staff at branch site to back up the configurations at regular intervals.

[Prerequisites]

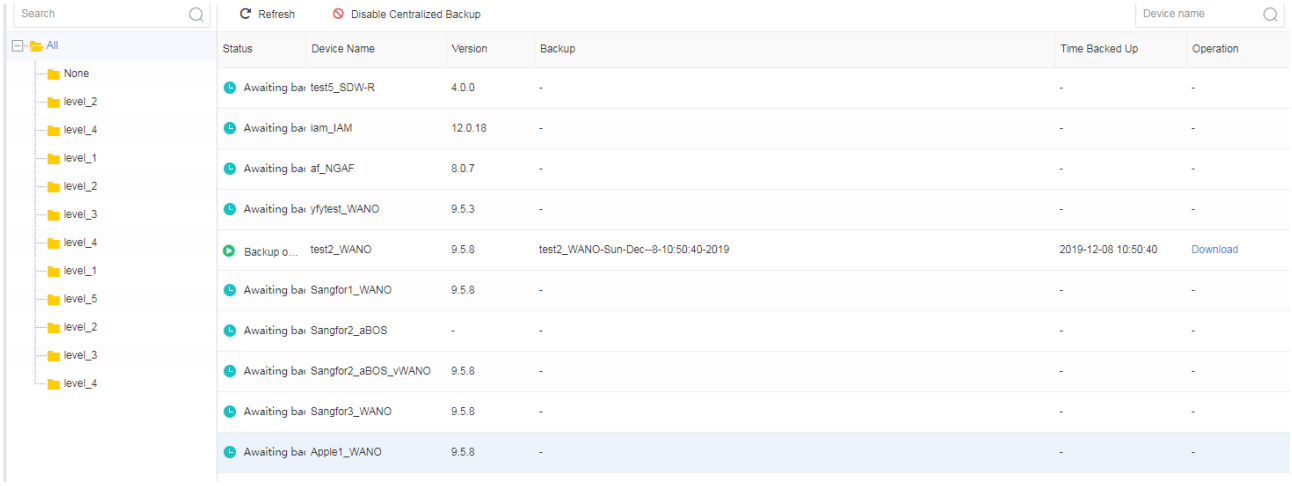
The branch device has been connected to CM normally.

[Note]

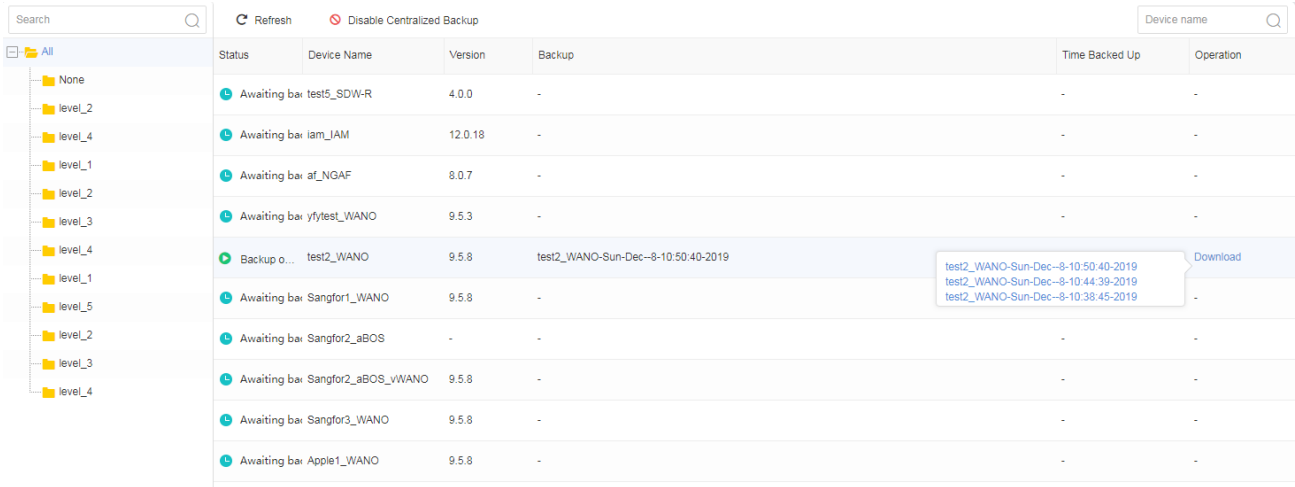
1. The backups of CM configurations will include the configuration of all policy templates, and therefore its configuration file will be relatively large.
2. The backup of branch device configuration will be triggered once from 00:00AM to 06:00AM on Sunday. If the backup is not completed, it will be carried out in the next cycle.
3. For a single branch device, CM can maximally keep three copies of its recent configurations.

[Steps]

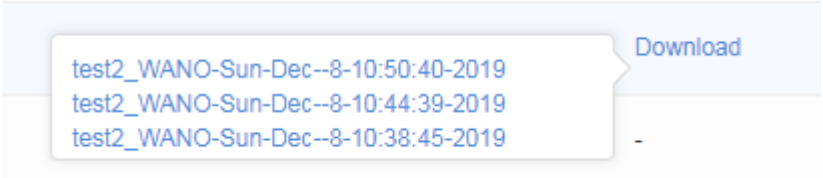
1. By default, CM has enabled automatic backup of branch device configurations. The backup does not need to be enabled manually. If the backup is not required, it can be disabled manually.



2. If you need to download the branch device configurations, you can click the option [Download] under Operation column, as shown below



3. Select the file on a certain date that needs to be downloaded

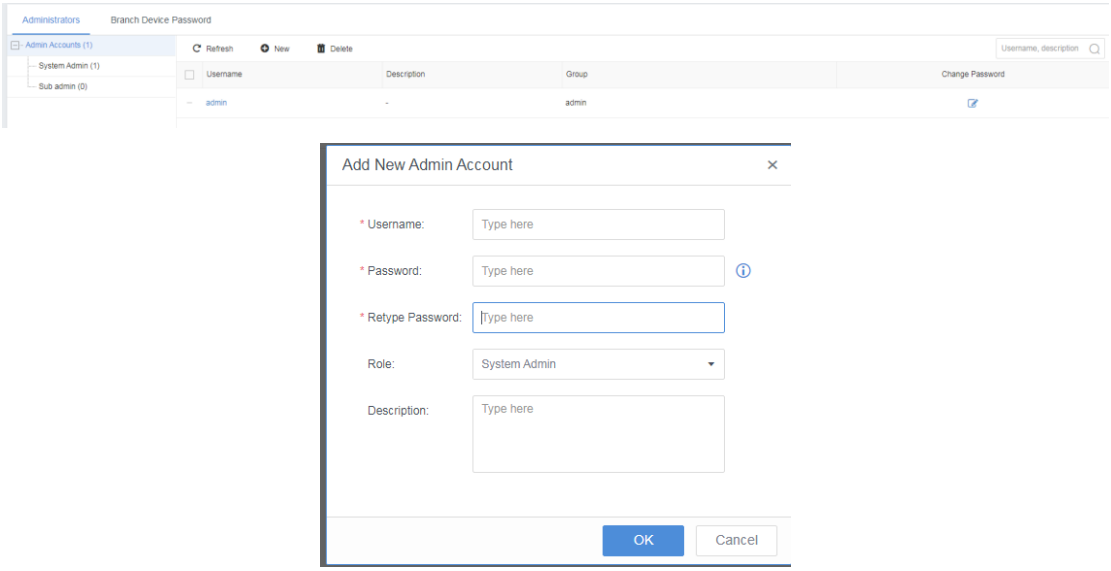


Chapter 8 CM Management

8.1 Administrators

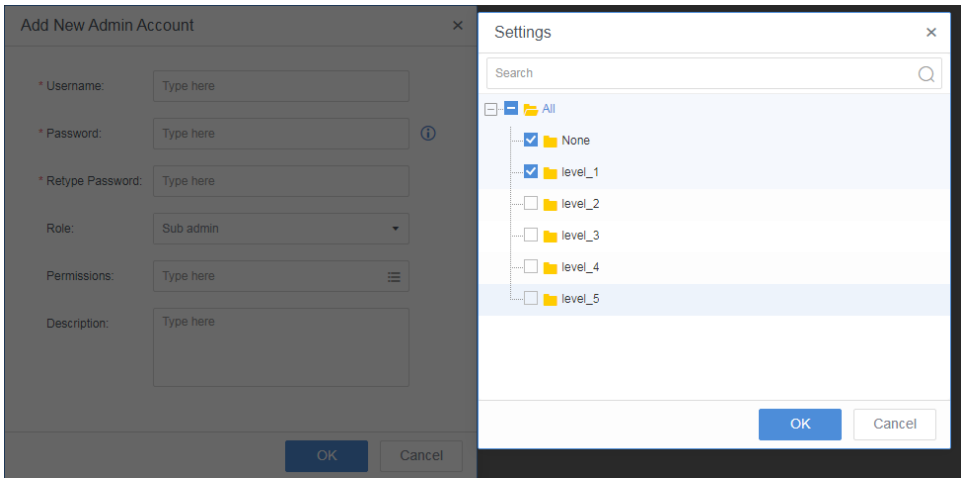
8.1.1 Creating System Administrator

Click [New] on [System] -> [Administrators], you can create a new administrator account, as shown below, select System Admin as the role.



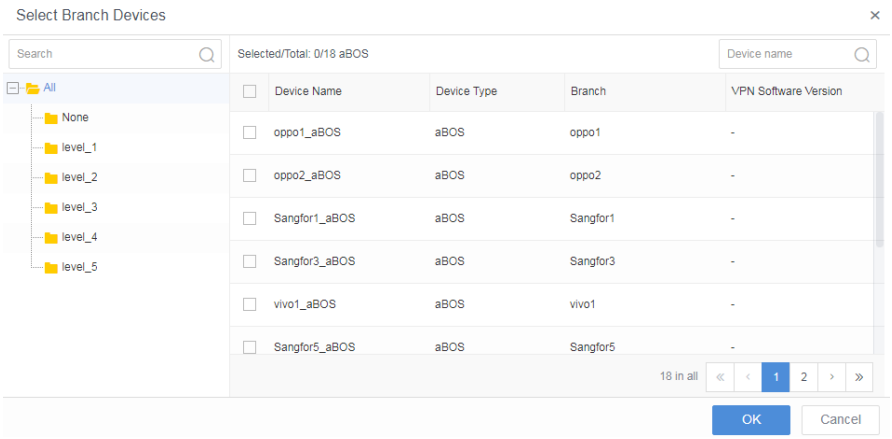
8.1.2 Creating Sub Administrator

To create a new sub administrator, select Sub admin as the role, and then click Permissions to select the regions that the administrator can manage.

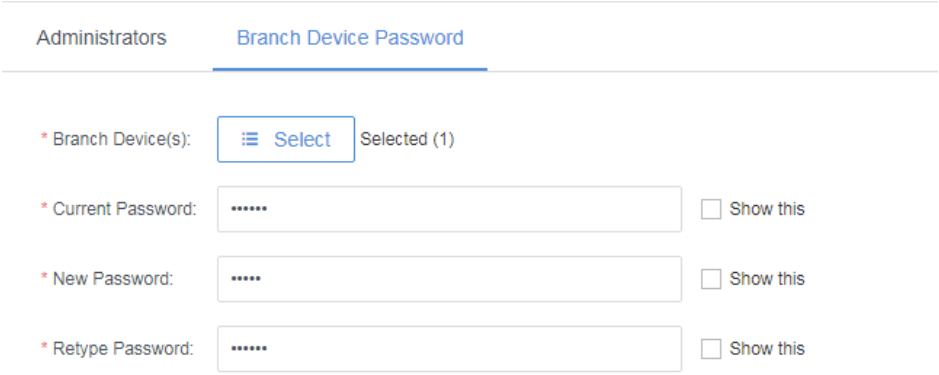


8.1.3 Changing Branch Device Password

1. On the Branch Device Password page, select the corresponding branch device to change the password (currently only aBOS password can be changed)



2. After selecting branch device, change the password of the corresponding aBOS device.



3. Enter the current password and new passwords of the device, and click **Save** to complete the operation.

8.2 Upgrading CM

[Scenario]

Upgrade Central Manager.

[Prerequisites]

The update package of CM has been downloaded. It can be downloaded from the following link:

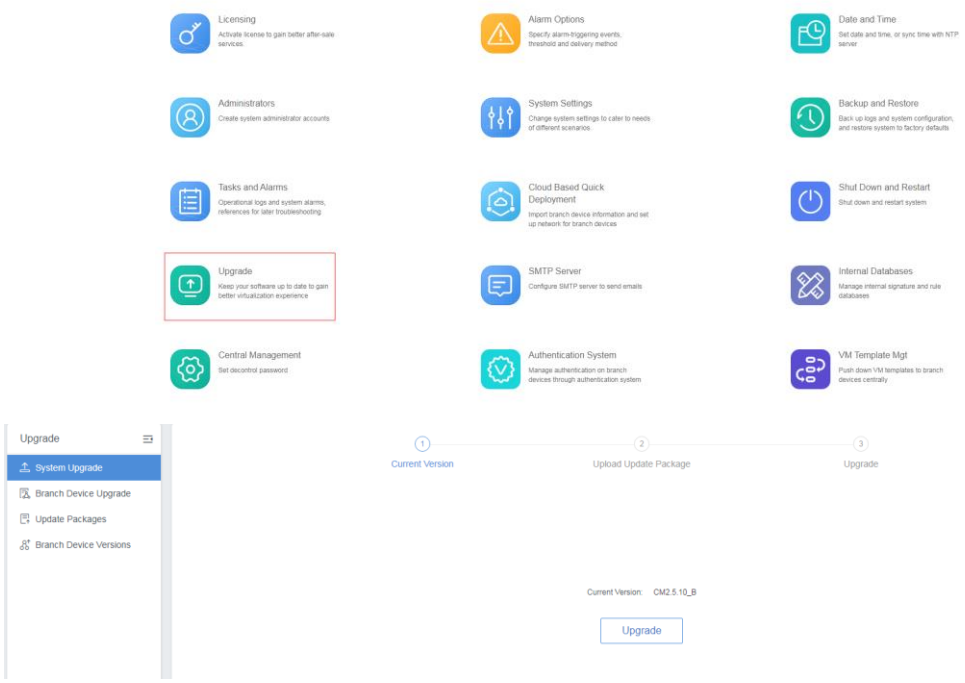
http://community.sangfor.com/plugin.php?id=service:download&action=view&fid=88#/26/all

[Note]

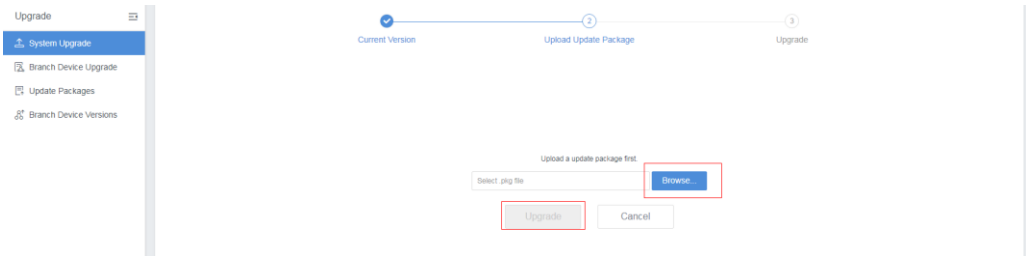
CM will restart when upgrade is completed. And branch devices cannot be managed during upgrade process.

[Steps]

1. Navigate to [System] -> [Upgrade].

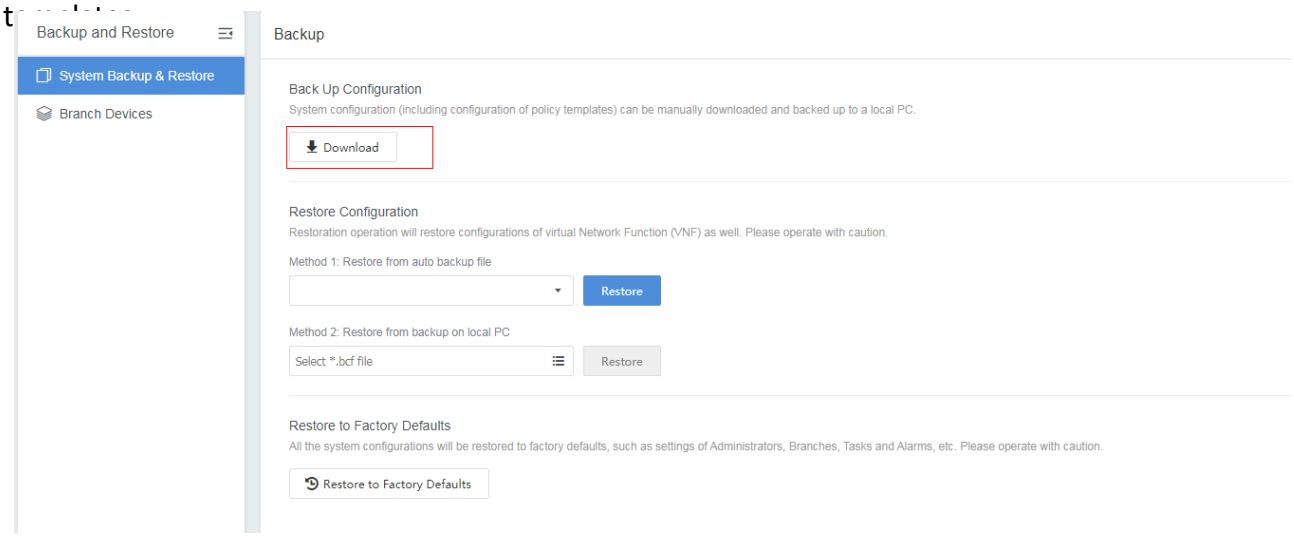


2. On the System Upgrade tab, click Upgrade and then click [Browse] to select the downloaded update package. Then, click [Upgrade] to start upgrade.



8.3 CM Configuration Backup

To download the configuration files of CM, you can go to [System] -> [System Backup & Restore] and click Download. The backup includes system configurations and the configurations of policy t



8.4 Configuring Alarm Options

[Scenario]

CM alarm options can trigger alarm messages for alarm events on branch devices.

[Prerequisites]

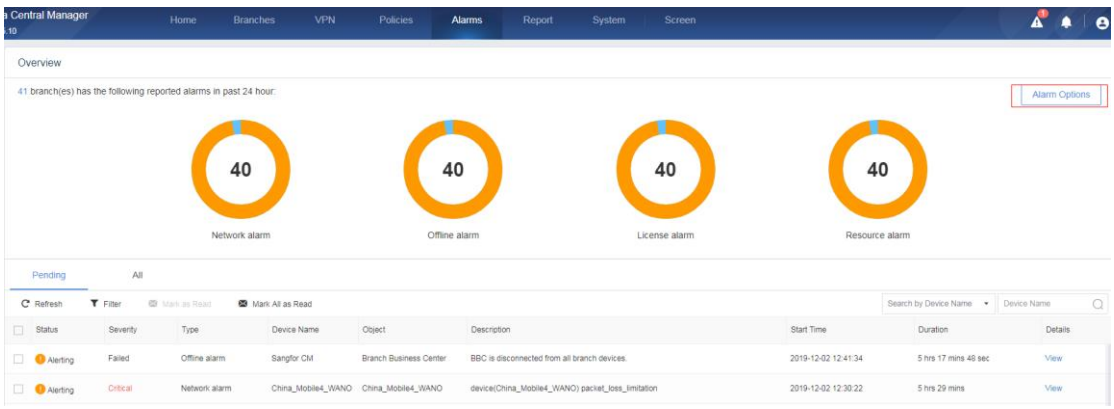
SMTP server is configured and recipient addresses of alarm emails are specified.

[Note]

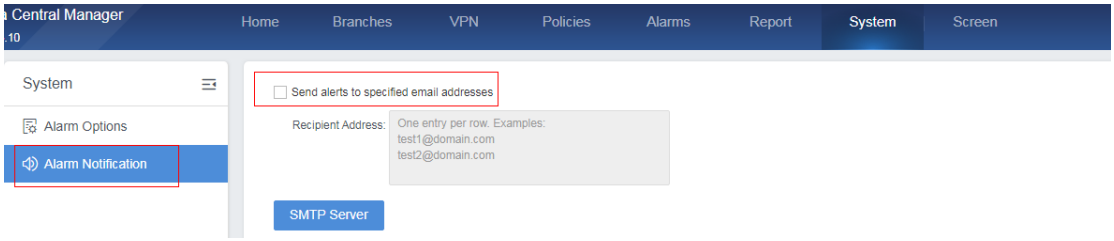
CM only supports email alarm.

[Steps]

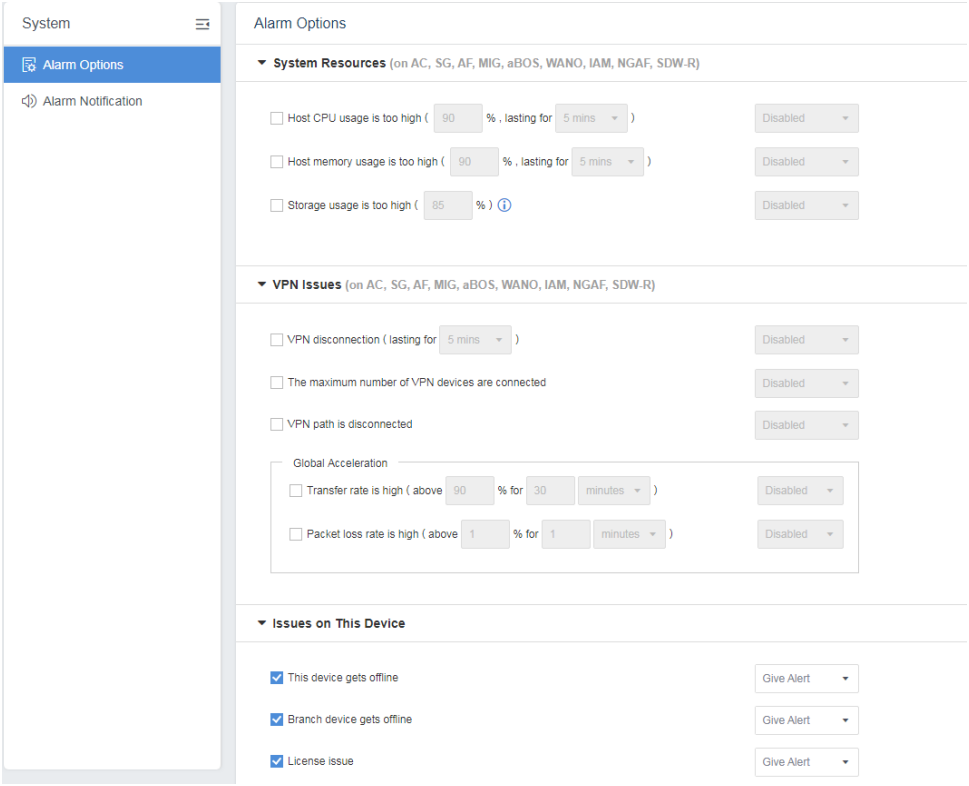
Step 1: Go to Alarms and click on the button [Alarm Options];



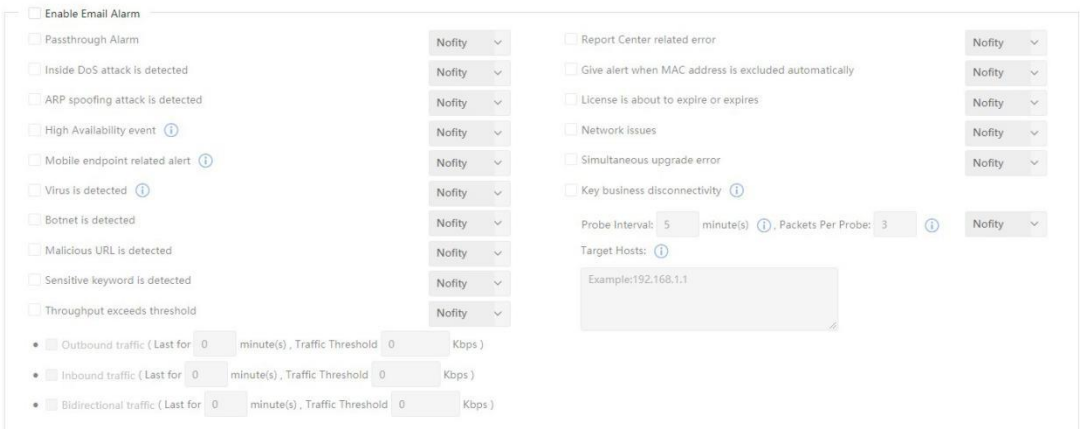
Step 2: Configure the recipient address to receive the alarm emails;



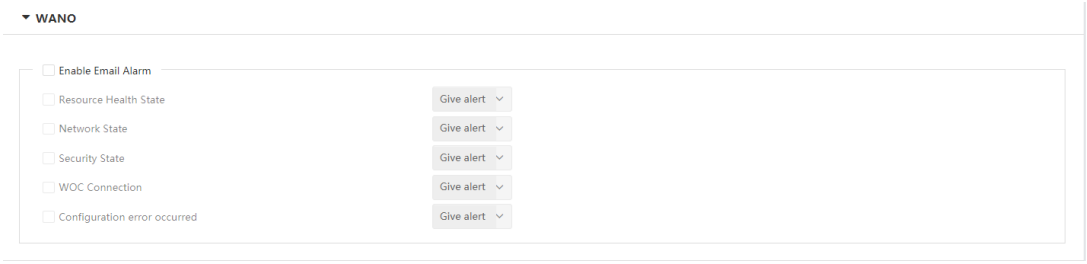
Step 3: Configure alarm-triggering events in [System] >[Alarm Options].



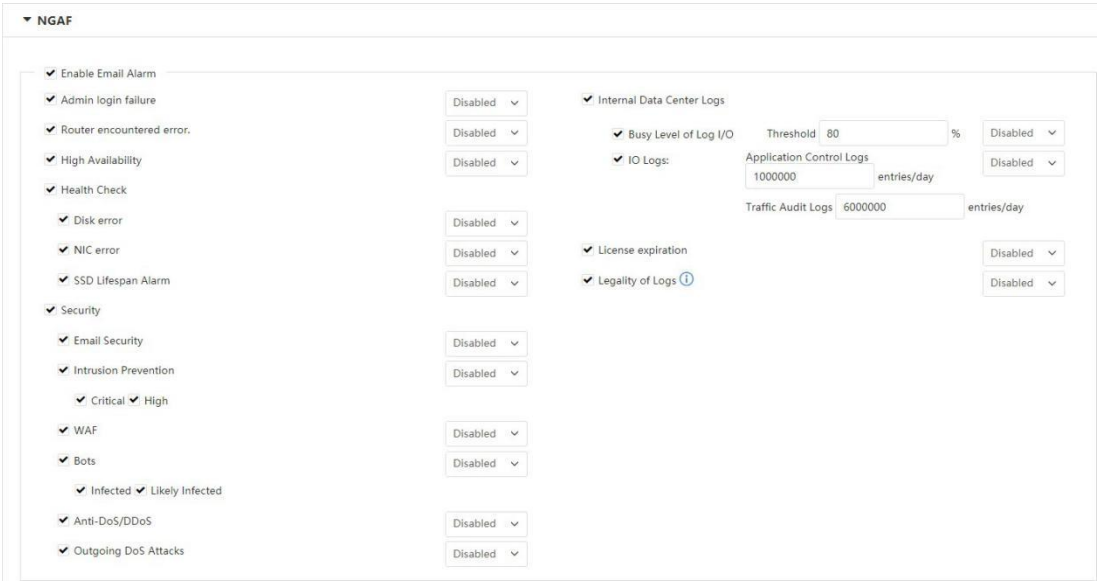
1. The figure below shows alarm-triggering events on IAM.



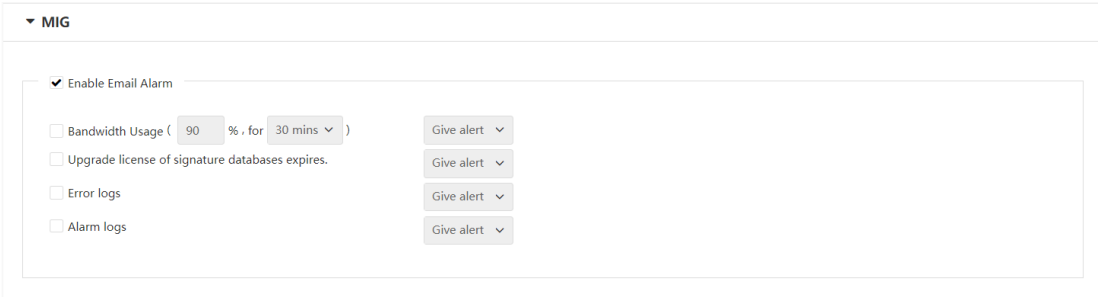
2. The figure below shows alarm-triggering events on WANO.



3. The figure below shows alarm-triggering events on NGAF.



4. The figure below shows alarm-triggering events on MIG.



8.5 High Availability

[Scenario]

CM supports high availability (HA) and can provide high-availability services.

[Prerequisites]

1. The CM version shall be BBC2.5.6 or later (BBC 2.5.7 does not support HA), and HA license has been activated.

2. The eth0 ports of active and standby CM devices must be connected to a switch port on the same VLAN.
3. CM needs to use two IP addresses on the same network segment, including two real IP addresses and one virtual IP address.

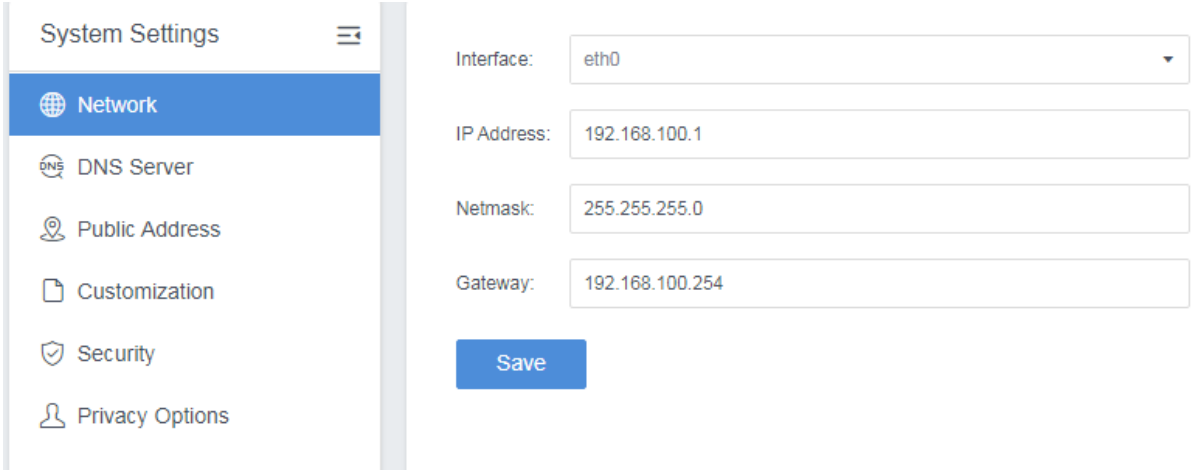
[Notes]

1. The business of the active and standby devices are done through the virtual IP address. All branch devices connect to CM using this virtual IP address, which will be bound with the business interface of the active device. When the active device encountered failure, the virtual IP address will be bound with the standby device and the business will also be switched. The environment set by the front-end gateway must be mapped to the virtual IP address of active and standby devices.
2. The business interface (eth0) of CM cannot be used as HA interface of the active and standby devices. The IP address of HA interfaces must reside on the same network segment as that of the business interface (eth0) . The interface used for failure detection is the business interface (eth0) by default and cannot be changed.
3. The license key of CM is prepared according to the original device. The licensed number of the devices is the same as that of standby devices, ensure that the device is a licensed device during configuration. When the active and standby devices are disconnected from each other for over 30 days, the license key will be restored to the number of a device.
4. If CM upgrade is needed, remove HA environment first, and form HA again after the two devices are upgraded respectively.

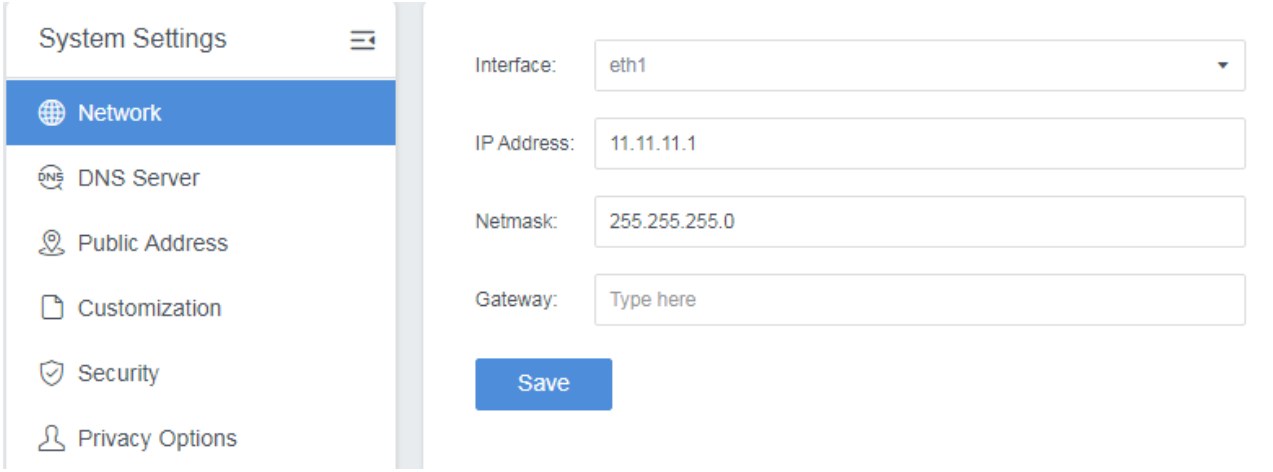
[Steps]

Step 1: Configure business interface and heartbeat interface for active and standby devices.

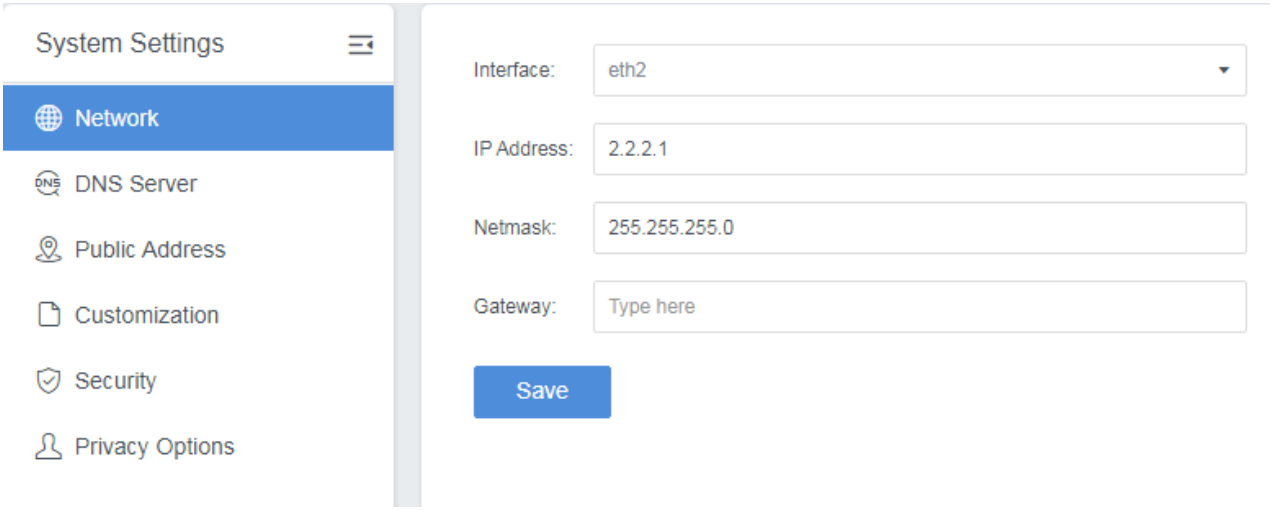
1. Select [System] -> [System Settings] -> [Network] on CM, and select eth0 port as interface, and configure the IP address for the interface;



2. Select eth1 port, and configure the IP address for it. It can be specified as primary HA interface. Since eth0 port has been configured with IP address, the gateway can be null.

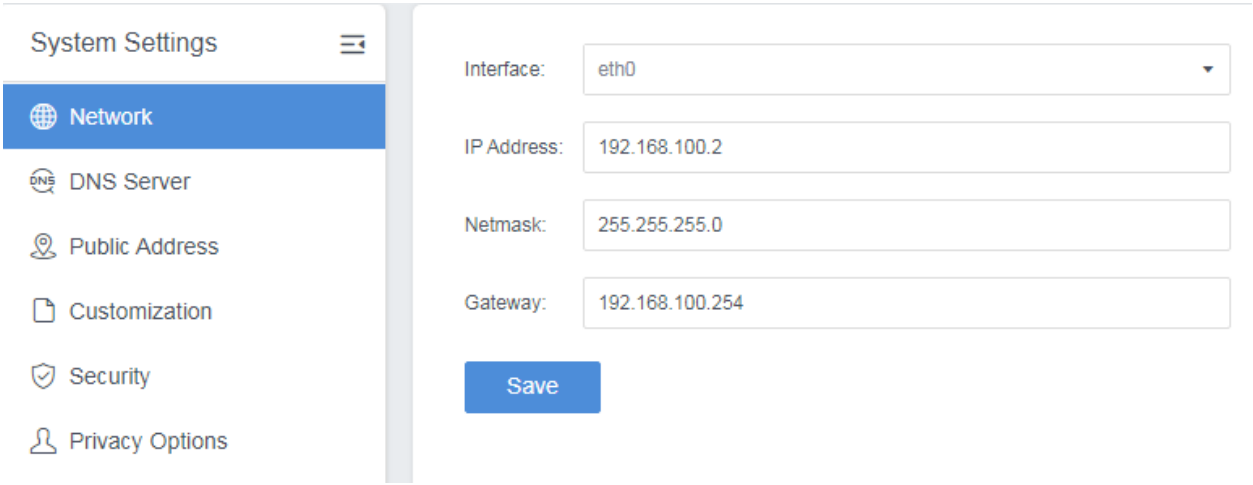


3. Select eth2 port and configure IP address for it. It can specified as secondary HA interface.

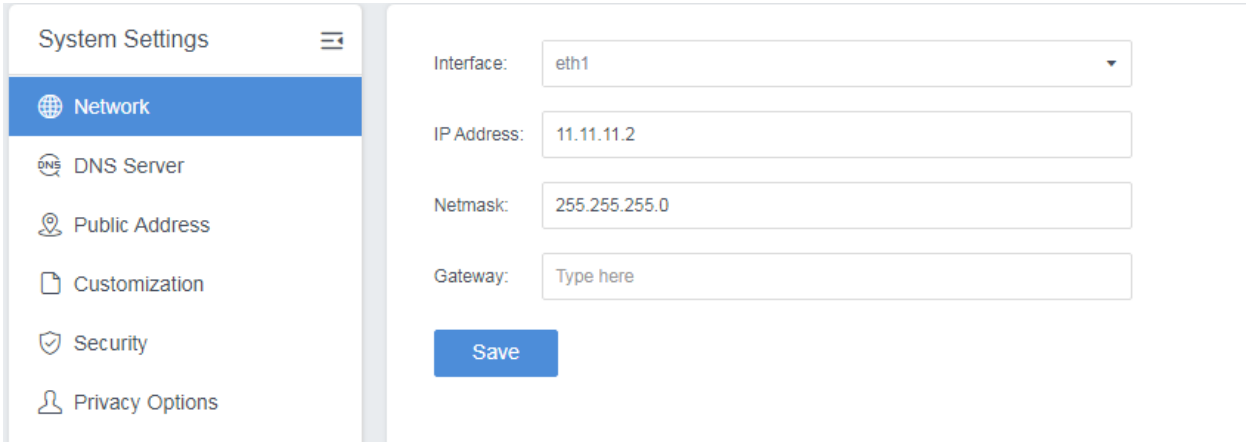


Step 2: Configure corresponding interfaces on the standby device.

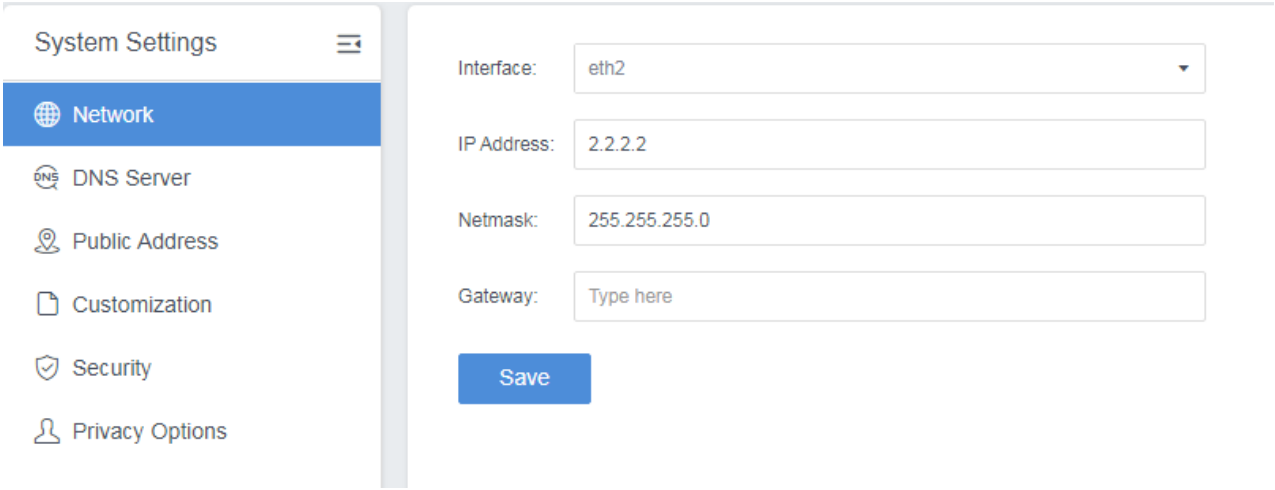
1. Navigate to [System] -> [System Settings] -> [Network] on CM, and select eth0 port as business interface, and configure the IP address for the interface;



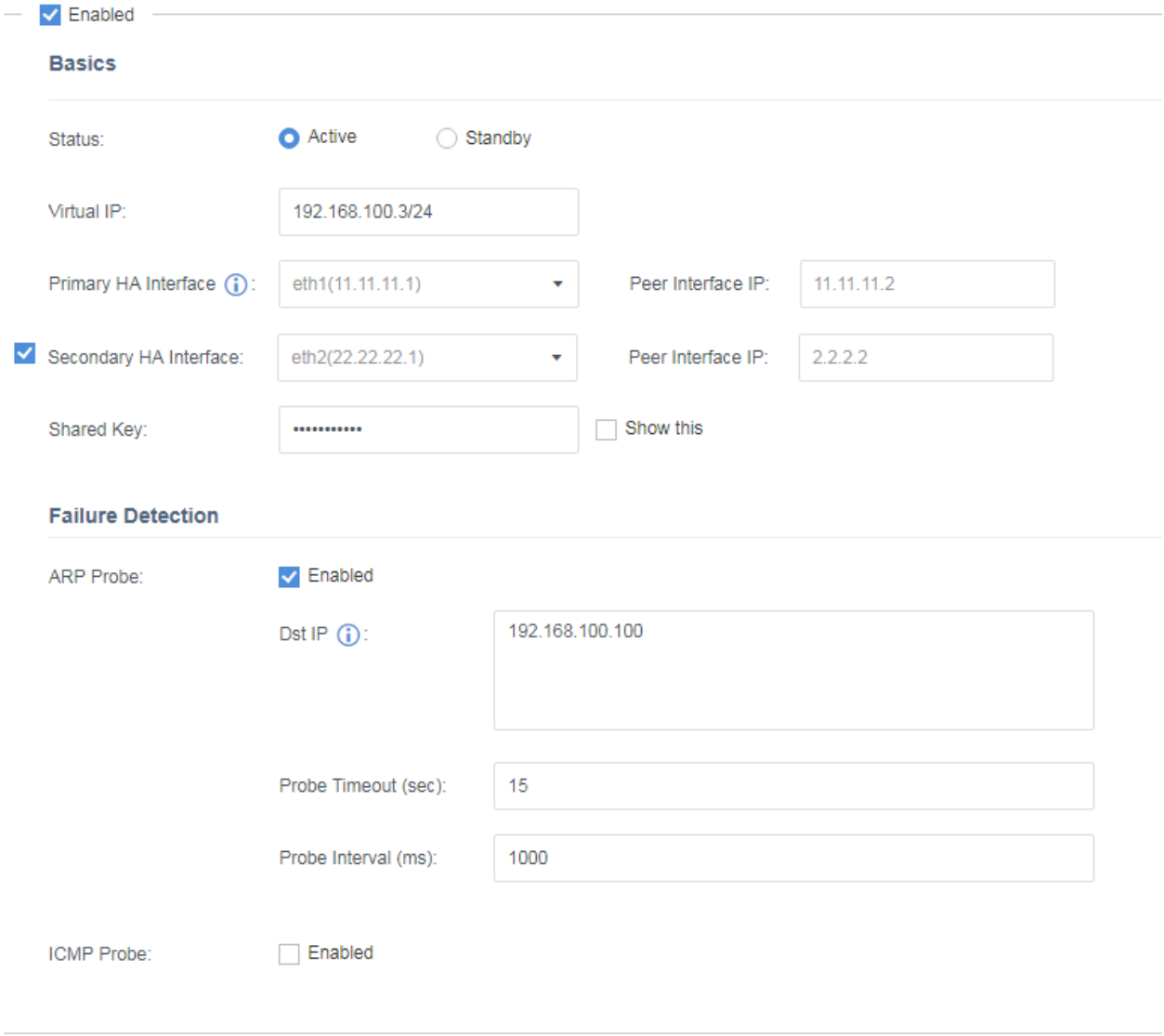
2. Select eth1 port and configure IP address. It can be used as primary HA interface.



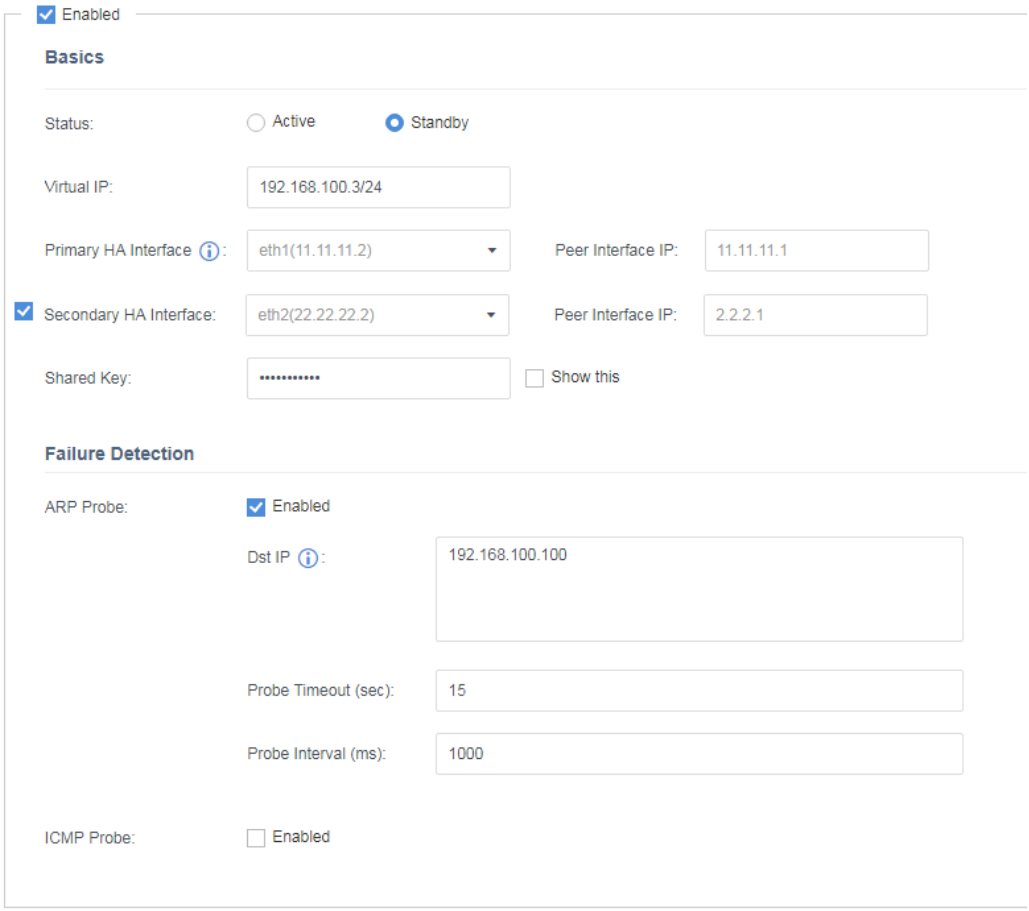
3. Select eth2 port and configure IP address. It can be used as secondary HA interface.



Step 3: Go to [System] -> [High Availability] to enable HA, select the status of the current device as Active, and use the virtual IP address of business interface as the virtual IP address of the active device. Select the primary HA interface, secondary HA interface, shared key, detection port and failure detection method;

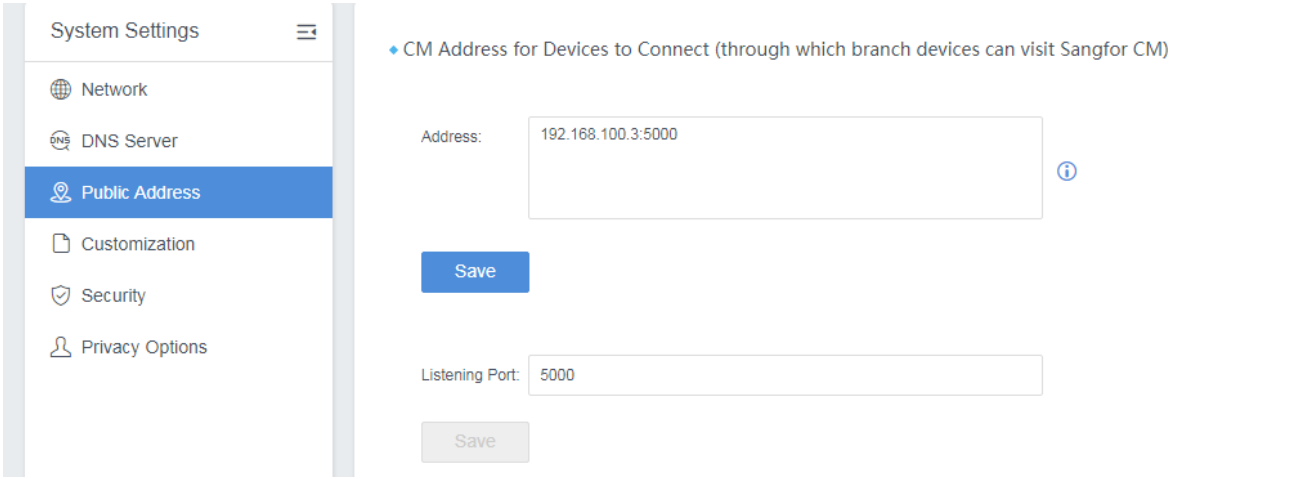


Step 4: Go to [System] -> [High Availability] to enable HA, configure the status of the current device as Standby, and use the virtual IP address of business interface as the virtual IP address of standby device (consistent with the active device). Select the primary HA interface, secondary HA interface, shared key, detection port and failure detection method.

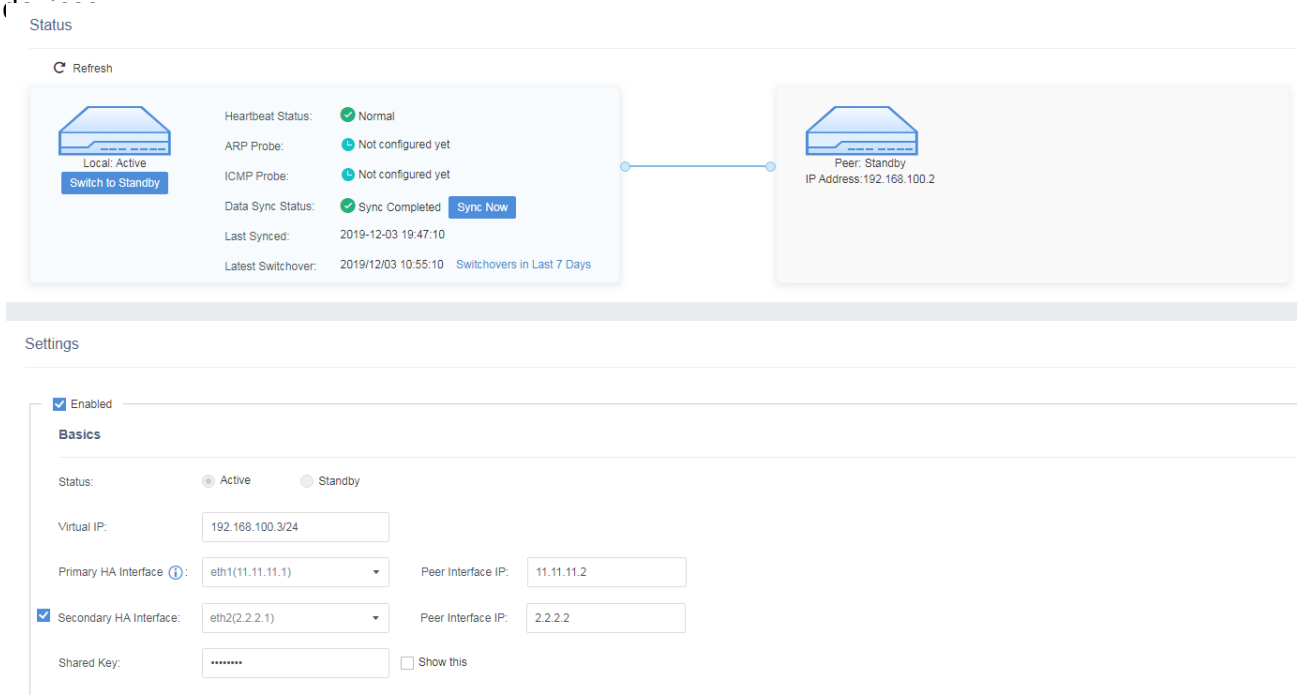


Step 5: Configure the CM address in [System] -> [System Settings] -> [Public Address].

Note: The address here must be an address that can be accessed by the branch devices. If CM is deployed in single-arm mode on the internal network and is mapped through the gateway, then the mapped public IP address shall be configured here. The front-end gateway needs to map the public IP address to the virtual IP address of business interface.



Step 6: On the [System] -> [High Availability] page, you can see the status of the active and standby



8.6 Specifying Decontrol Password

[Scenario]

Configure a decontrol password on the CM to enable branch devices to remove from central management. One-time decontrol password can also be set.

[Prerequisites]

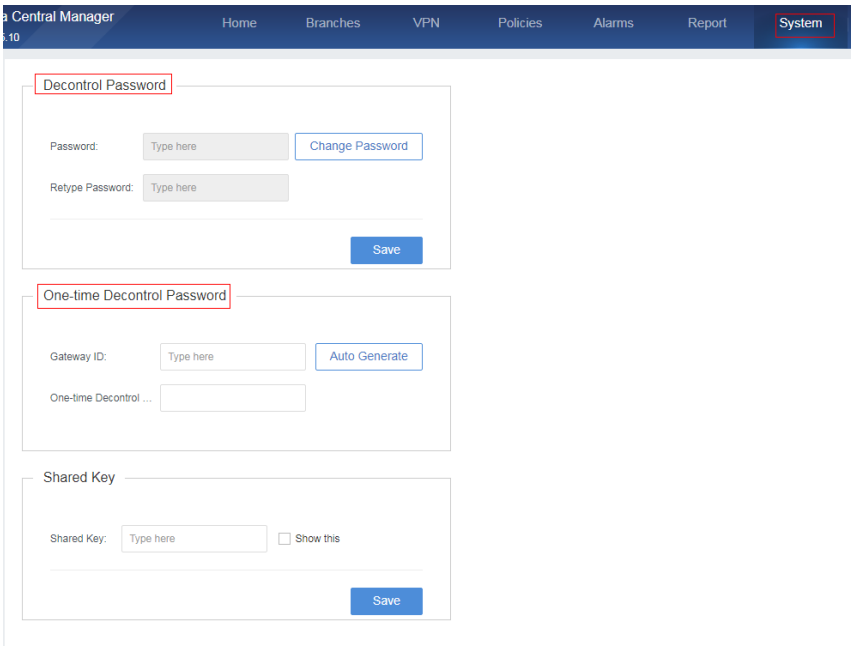
The branch device has connected to the CM.

[Note]

If the branch device decontrols from CM, the pushed down policy will not be lost, but it will not be under the management of CM.

[Steps]

1. Select [System] -> [Central Management] -> [Decontrol Password] or set [One-time Decontrol Password];



8.7 VM Template Management

[Scenario]

The CM supports the pushdown of VM and VNF templates for aBOS to meet software-defined branch device requirements.

[Prerequisites]

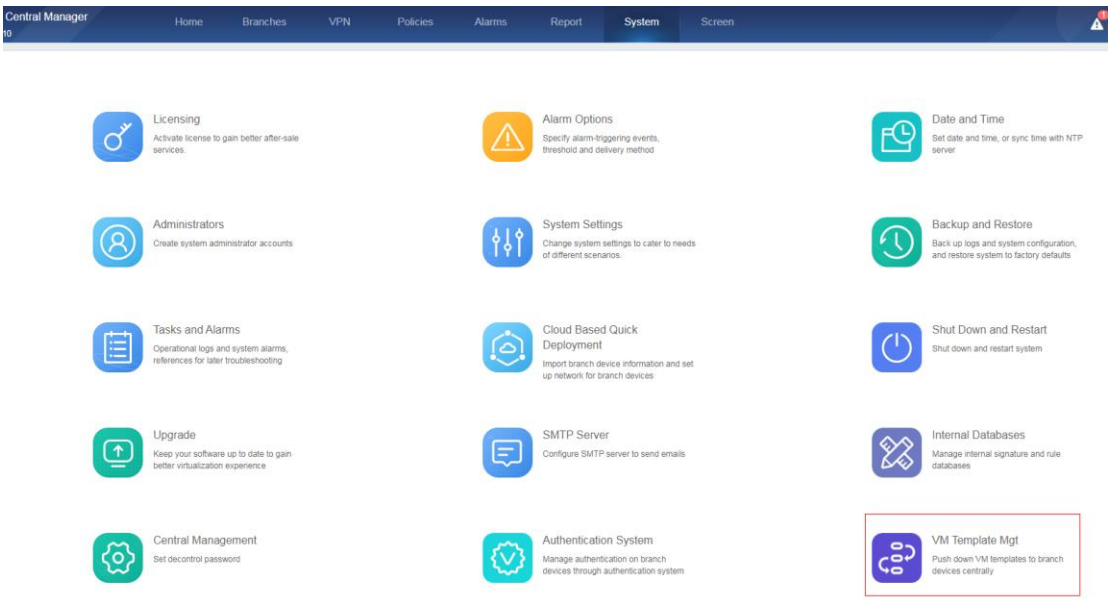
1. The branch device has connected to the CM.
2. The branch device is aBOS.

[Note]

1. When selecting an ordinary VM, only aBOS devices later than version 3.2.3 can be selected.
2. When selecting a VNF template, the template can be checked only when aBOS device has license of that VNF, otherwise it cannot be pushed down.

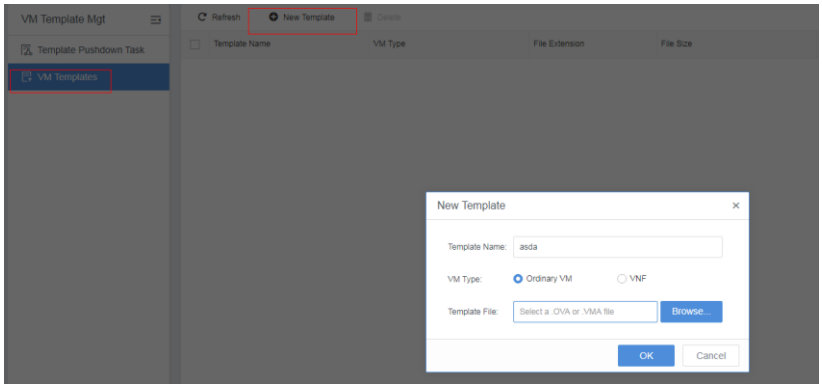
[Steps]

Step 1: Select [System] > [VM Template Mgt];

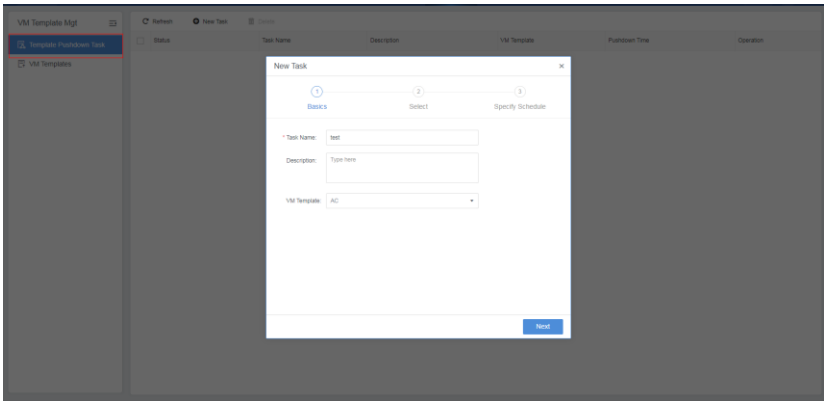


Step 2: Add a VM template and upload the VM template which is to be pushed down.

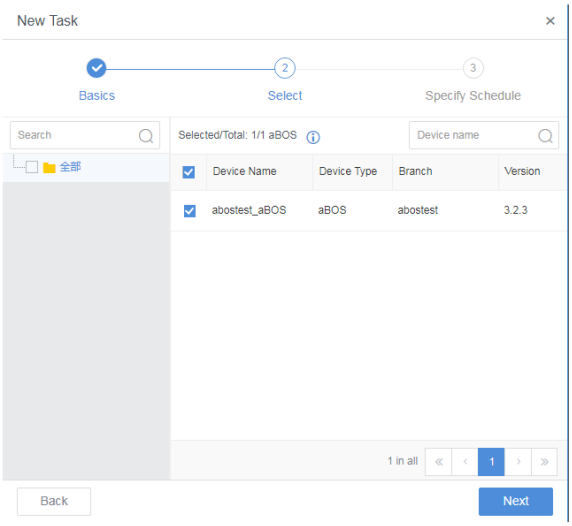
1. Click [VM Template Mgt] -> [VM Templates], and upload the image, which can be an image of a virtual machine or a virtual network device.



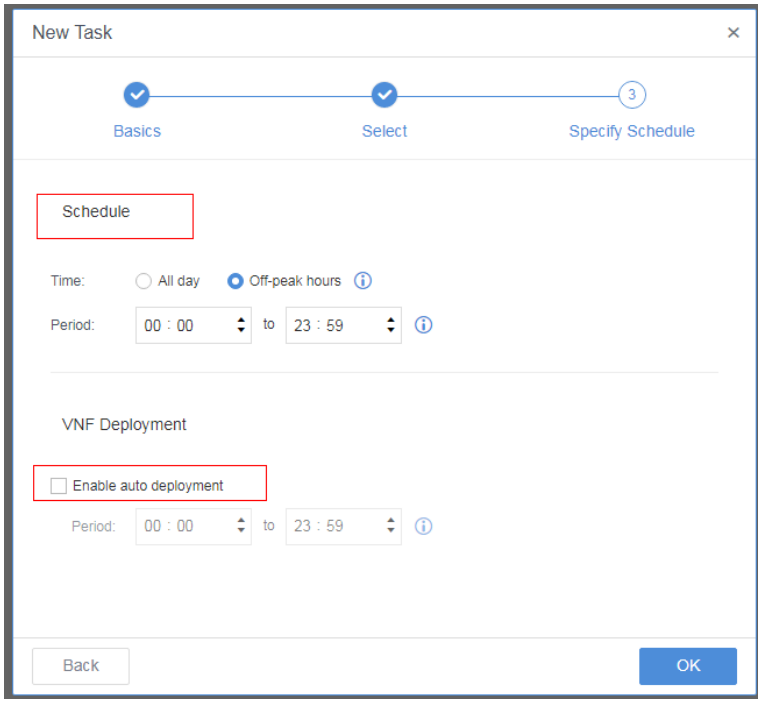
2. Add a new pushdown task.



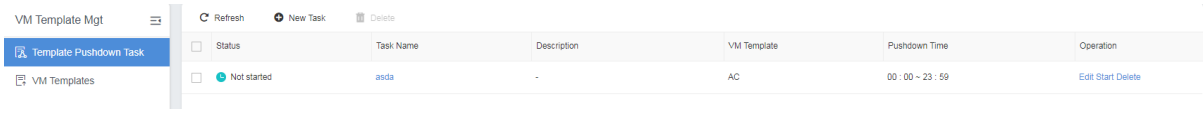
3. Select the target device, that is, the aBOS device.



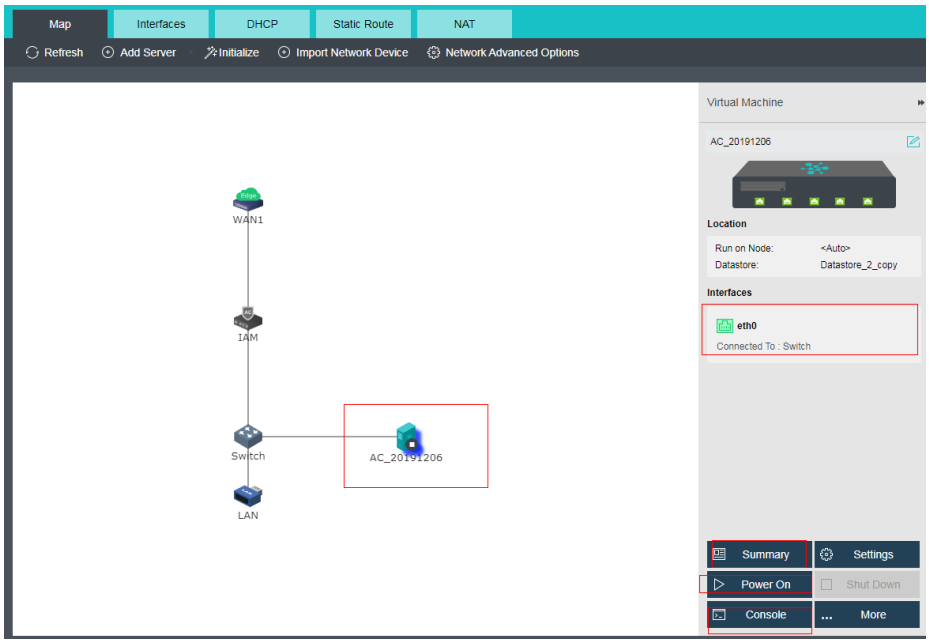
4. Specify schedule.



5. View the status of the pushdown task.



Step 3: Log in to aBOS Web admin console, you can see that the corresponding VM has been pushed down.



Chapter 9 Maintenance and Troubleshooting

In order to ensure the stable operation of the devices, the device administrator needs to check the device regularly to ensure operational risks can be detected in advance. The routine check items are as follows:

9.1 Daily Maintenance Precautions

Maintenance Items	Maintenance Instructions
Device removal	Be sure to unplug all power lines and external cables before moving the devices.
Mount devices on rack	1. If the user does not have a standard cabinet, the user can mount the devices on a clean workbench. The user shall ensure that the workbench is mounted firm enough to bear the weight of the devices and cables, leaving 10 cm space for heat dissipation around the devices. 2. Do not place heavy objects on the devices. 3.In the process of mounting the devices on the rack, pay attention to other devices in the same cabinet to avoid unplugging the power and network cable interfaces of other devices.
Installation of lugs for devices	After the devices are installed with trays or guide rails, lugs may not be installed as appropriate. Lugs must be installed in other cases.
Cable Layout	1. Cables laid on walkway must be bound. The bound cables shall be tightly close to each other, the appearance shall be straight and in order, and the cable clips shall be with even spacing and moderate tightness. Cables laid in conduits may not be bound. 2. The signal cables, tail fibers and power lines shall be laid apart from each other, they shall not be laid too close or even bound together. After the cables are bundled in the cabinet, they shall be straight and neat, and shall not be twisted or bent. 3. Before binding the tail fibers, check whether there are objects with burrs, sharp edges or sharp angles near the fiber laying area. If any, try to avoid them as much as possible. When the tail fibers are laid outside the cabinet, it is recommended to install fiber protection casings (corrugated pipes).
Power supply	The Sangfor CM series are supplied by 110V - 230V AC power. Please ensure the good grounding measures before turning on the power.

Label	The cable must be labeled with clear indication 1. Power line label: The content is the location information of the opposite end of the cable. Fill in the location information of the peer device of the cable, control cabinet, junction box or socket on the cable side where the label is located. 2. Signal line label: Both sides of the tag respectively identify the location information of the ports connected to both ends of the cable. 3. Before pasting the labels, fill in or print the contents of the labels on the full page of tag paper, and then peel it off and paste it on the cables or the wire clips of signboards.

9.2 Checking Hardware Status

9.2.1 Checking LED Status

When Sangfor CM is working normally, the POWER LED shall be always on, and the ALARM LED will only be on (for about 1 to 5 minutes) due to system loading when the device is booted, and the indicator will be off when operating normally. If the LED is always on during use and the device cannot be used properly, follow the steps below:

1. Please power off the device immediately and switch the system to standby mode;
2. Restart the device after half an hour. If the ALARM LED is still on and cannot be turned off after restarting the device, contact Sangfor to check whether the device is damaged.

9.2.2 Checking LED Status

Normally, the link indicator at the interface will be green when it senses electrical signals (100 Mbps link; if it is a Gbps link, the indicator will be orange) and it will be always on. When data passes through, the ACT indicator at the interface will be orange and flashing constantly. If the link or ACT LED does not flicker or is not on, follow the steps below:

1. Check whether the network cable is damaged;
2. Check whether the RJ of interface is damaged;
3. Check whether the interface is in full-duplex mode and whether it is negotiated and matched;
4. If no aforesaid problems, please restart the device in time to switch active/standby status, and contact Sangfor for technical support in time.

9.2.3 Checking CPU Operation

CM will check [CM System Status] shown on the monitoring of [Home] to confirm whether the CPU usage is high for a long time. If the CPU usage exceeds 90% for a long time, contact Sangfor for technical support and confirmation.

9.2.4 Checking Exception of Device

Check whether there is any exception on device hardware (whether there is any abnormal sound on the fan and hard disk).

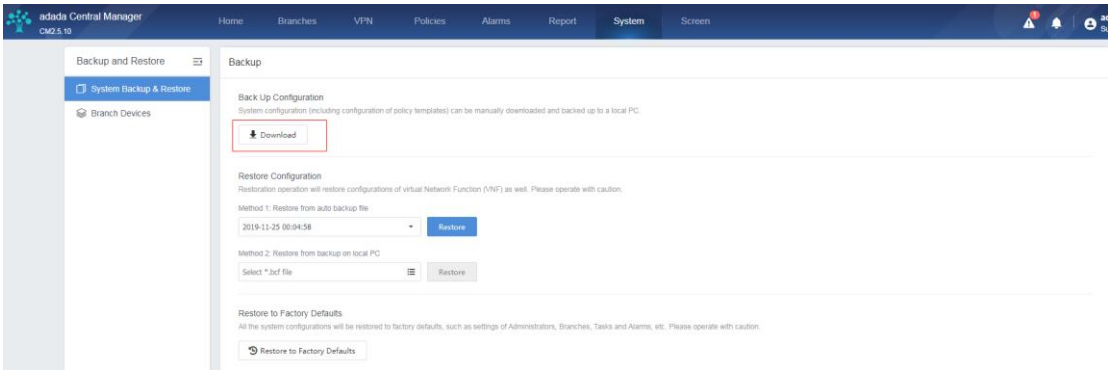
If there is any abnormal noise inside the device, it may be caused by abnormal working of the hard disk or fan, please cut off the power immediately and shut down the device. If there is a standby device, switch the system to the standby host immediately, and contact Sangfor in time to confirm the fault and repair the device.

9.3 Checking Configuration Information of Device

9.3.1 Device Configuration Backup

To ensure the stable operation of the network, it is recommended that the customers to back up the configuration once a month, so as to prevent the system from being unable to be recovered rapidly due to accidental breakdown of CM device. Steps are as follows:

1. Log in to the CM console, click [System] -> [Backup and Restore] -> [System Backup & Restore], then click [Download] to download the configuration and save it properly.



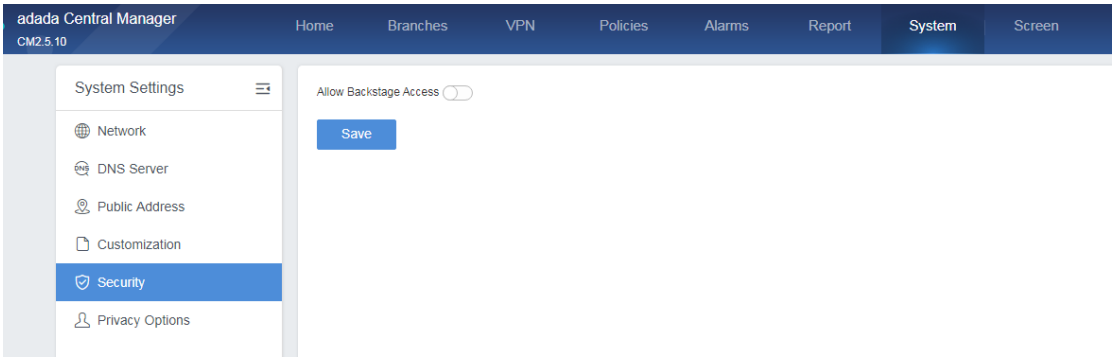
9.4 Security Check

9.4.1 Checking Security of Account

1. Whether the administrator password is the default password admin or simple password such as 123456.
2. If the password is a default password or simple password, change the password immediately.
3. The administrator password has not been changed within a month.
4. If the administrator password has not been changed within a month, change the password immediately and keep it properly.
5. Check whether the console has extra accounts or the console has unnecessary simple accounts such as Sangfor, test, and English name of the company. If any, delete the extra accounts and keep the authorized administrator account only.

9.4.2 Checking Security of Console

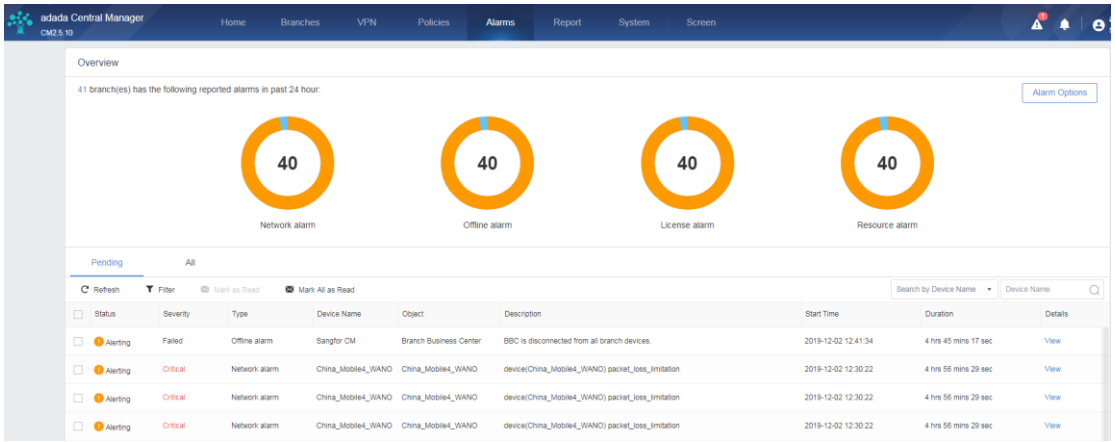
Through [System] -> [System Settings] -> [Security] -> [Allow Backstage Access], CM will check whether the backstage access of the device is enabled. The backstage access is disabled by default to prevent the device from being logged in by unauthorized personnel in the backstage.



9.5 Checking Logs

If there are a large number of error and alarm logs in system logs, contact Sangfor in time to confirm whether the program encountered failure.

The CM can check whether there is any alarm on [Alarms] page.

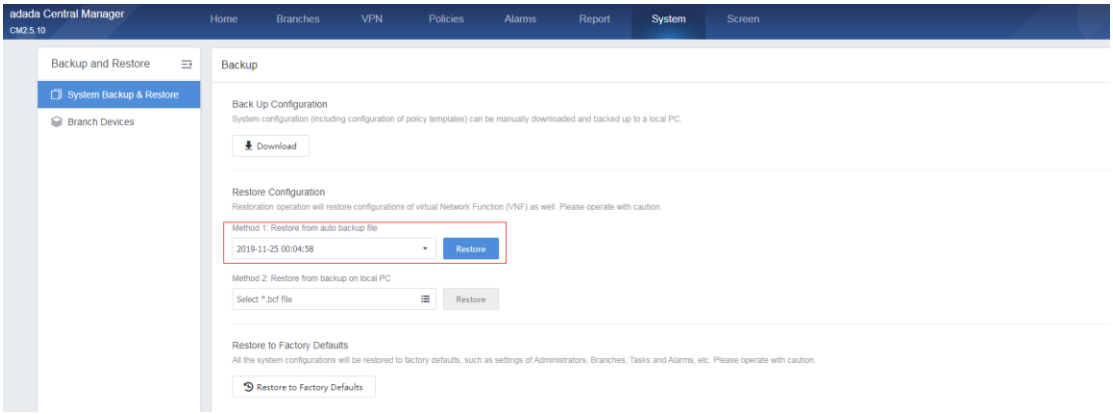


Chapter 10 Configuration and Password Restoration

10.1 CM Configuration and Password Restoration

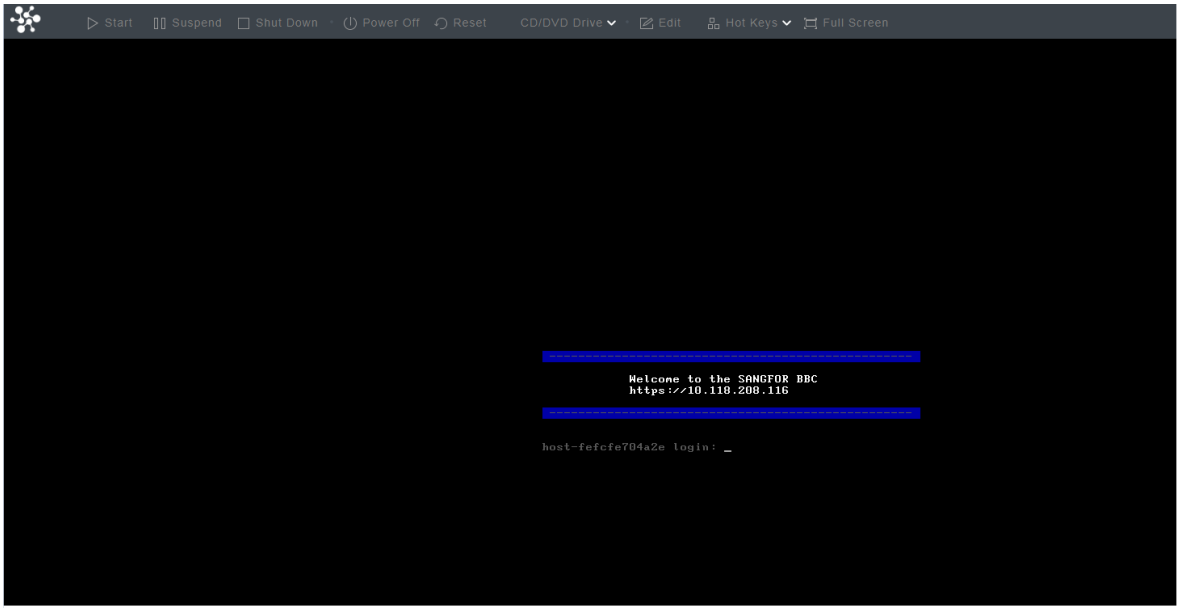
Restore the console to the factory default configurations.

1. Log in to the CM console, select [System] -> [Backup and Restore] -> [Back Up Configuration] to restore the configurations, and then save the downloaded backup configuration files properly.



[Note]: CM can directly restore factory default settings on device management page. During restoration, all the parameters configured by CM will be restored to factory defaults, including: users, branch data, alarm logs, operation logs, etc. Please operate with caution.

[Note]: For the virtualized version or hardware device with VGA display interface, you can directly check the IP address of the current device through the console.



Chapter 11 Troubleshooting

11.1 Unable to Log in to CM Web Admin Console

1. Check whether the red alarm LED on the device panel is always on.
2. Use ping to detect whether the intranet port on the device can be connected normally.
3. Execute telnet command on intranet to check whether the ports such as 443 and 51111 can be connected.
4. Check the address of intranet port of Tracert device to confirm whether the data packet can reach the intranet port of the CM.
5. Try to use a computer to directly connect the device with a network cable and use ping to check whether the device can be connected.
6. If you still can not log in to the device after having tried the above steps, contact Sangfor for technical support immediately.

11.2 Branch Device Cannot Connect to CM

1. Check whether the CM device is working properly.
2. Check whether the login address for CM console and the listening port are correct, ensure that the account of the branch device is correct.
3. Check whether the port mapping of the front-end device is correct, and make sure that there is no problem with the port mapping of TCP5000 port.
4. Execute telnet command on intranet to check whether the branch device can access the TCP5000 port of CM.
5. Check the CM connection configuration of the branch device, ensure that the account, password and the CM address are configured correctly.
6. If the branch still cannot connect to CM after the above steps are tried, contact Sangfor for technical support immediately.

11.3 CM Cannot Manage Branch Device

1. Check whether the CM is working properly.
2. Check whether the login address for CM console and the listening port are correct, and whether the branch device can connected to CM normally.
3. Check whether the port mapping of the front-end device is correct, and make sure that there is no problem with the port mapping of TCP port 5530.
4. Execute telnet command on intranet to check whether the branch device can access the TCP

port 5530 of CM.

5. Check the CM connection configuration of the branch device, ensure that the account, password and the CM address are configured correctly.
6. If you still cannot manage the branch device after having tried the above steps, contact Sangfor for technical support immediatel