Sangfor IAG

vIAG Implementation Guide

Product Version	13.0.47
Document Version	01
Released on	Dec.15, 2021

Disclaimer

Products, services or features described in this document, whether wholly or in part, may be not within your purchase scope or usage scope. The products, services or features you purchase must be subject to the commercial contract and terms as agreed by you and Sangfor. Unless otherwise provided in the contract, Sangfor disclaims warranties of any kind, either express or implied, for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Unless otherwise agreed, this document is used for reference only, and all statements, information, and recommendations therein do not constitute any express or implied warranties.

Technical Support

For technical support, please visit: https://www.sangfor.com/en/about-us/contact-us/technical-support

Send information about errors or any product related problem to tech.support@sangfor.com.

About This Document

This document describes the implementation guide of Sangfor vIAG (virtual IAG).

Intended Audience

This document is intended for:

- Network design engineers
- O&M personnel

Note Icons

English Icon	Description
	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
	Indicates a hazardous situation, which if not avoided, could result in minor or moderate injury.
	Indicates a hazardous situation, which if not avoided, could result in settings failing to take effect, equipment damage, or data loss. NOTICE addresses practices not related to personal injury.
	Calls attention to important information, best practices, and tips. NOTE addresses information not related to personal injury or equipment damage.

Change Log

Date	Change Description
Sep.15, 2021	This is the first release of this document.

Contents

Technical Support 1
Change Log 2
1 Introduction 4
1.1 Import into HCI 4
1.2 Network Setting for the HCI 5
1.3 Licensing for the HCI 6
1.4 Import to VMware 7
1.5 Setting Up Network for VMware 9
1.6 Licensing for VMware vIAG 16

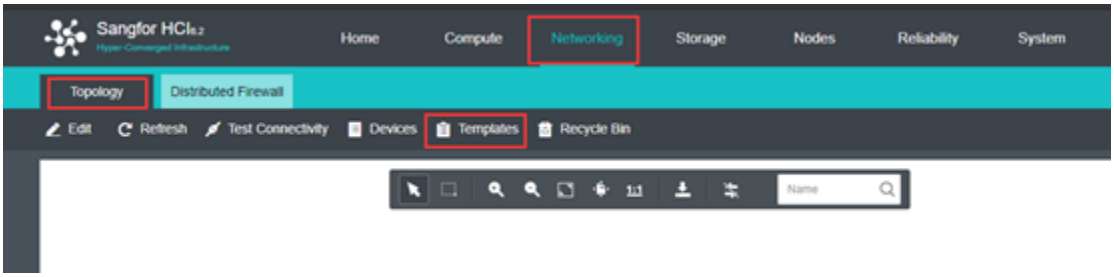
1 Introduction

For the image for HCI, VMware, kindly contact our local teams or live chat to obtain the download link for HCI and VMware.

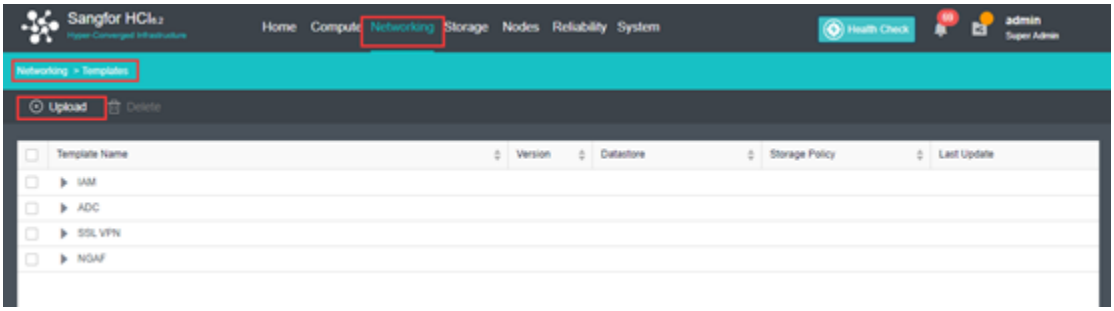
For your information, this virtual device only can support the IAG with IAG 12.0.44, and below, IAG 13.0.8 and IAG 13.0.15 are not supported in the virtual environment. IAG 13.0.47 is supported.

1.1 Import into HCI

1. Download the HCI template provided above.
2. Login to **HCI**, navigate to **Networking Topology** and choose **Templates**.

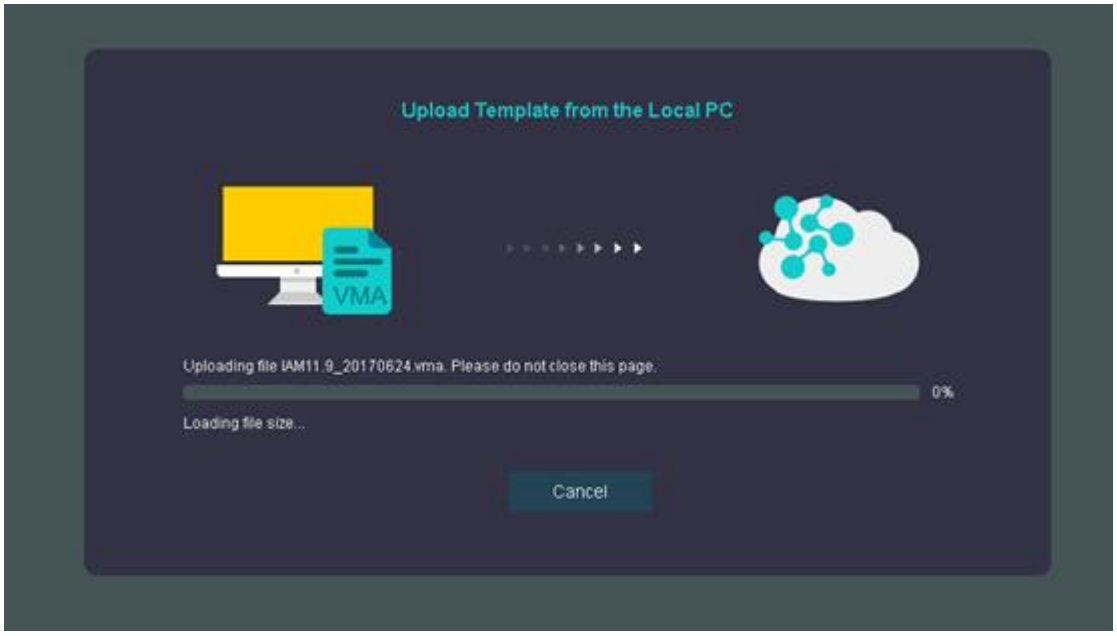


3. Click **Upload.**



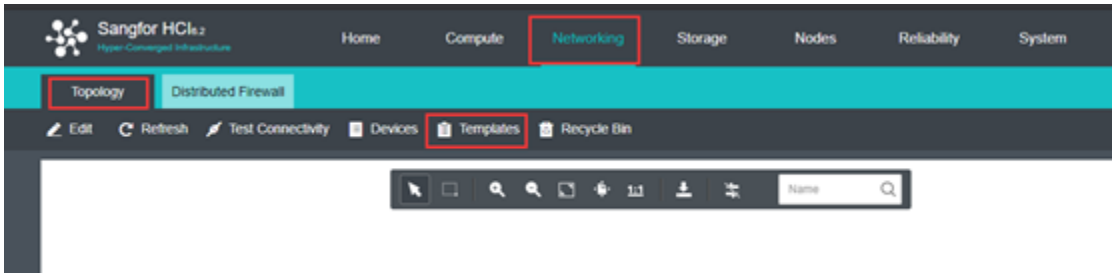
4. Select the downloaded VMA file and upload it to the selected datastore in HCI.

5. Wait for the VMA file to finish uploading.

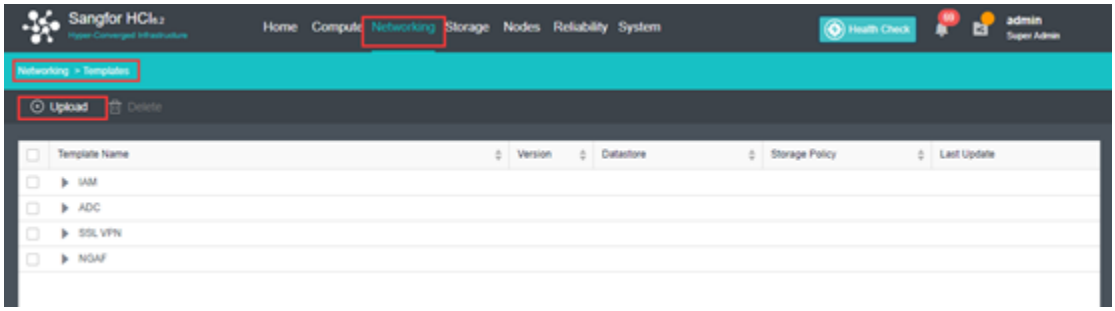


1.2 Network Setting for the HCI

1. After imported, navigate to **Networking**, under the **Topology**, drag the IAG from the left panel and paste on the edge or switch you wish to place.

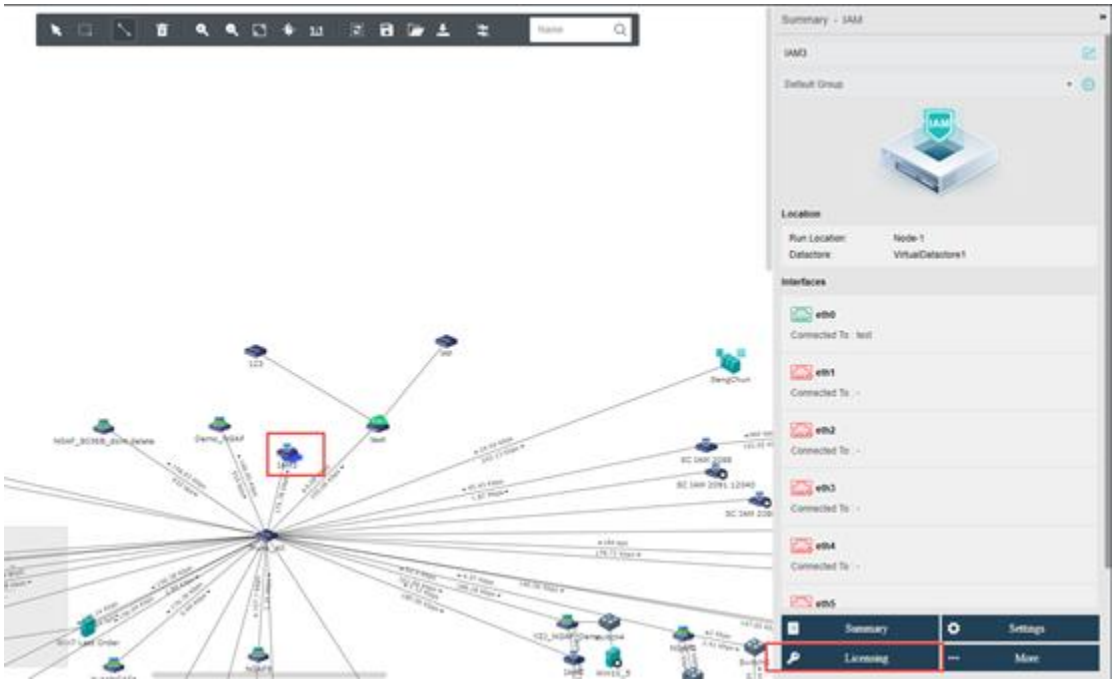


2. Check on the right panel setting. Confirm the IAG version, configure the required network card, and press apply the change to commit.

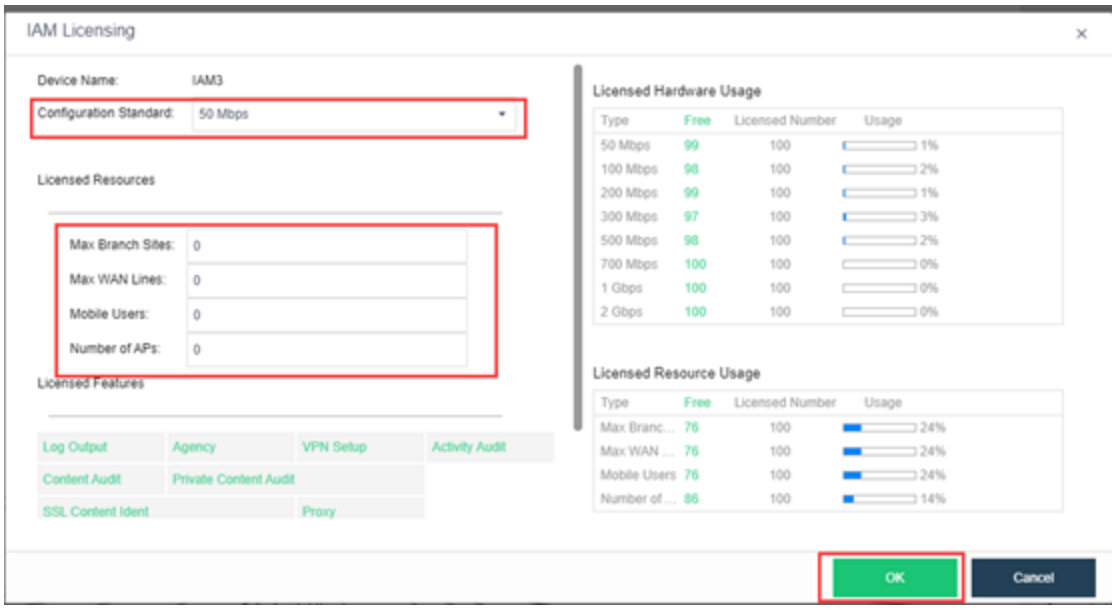


1.3 Licensing for the HCI

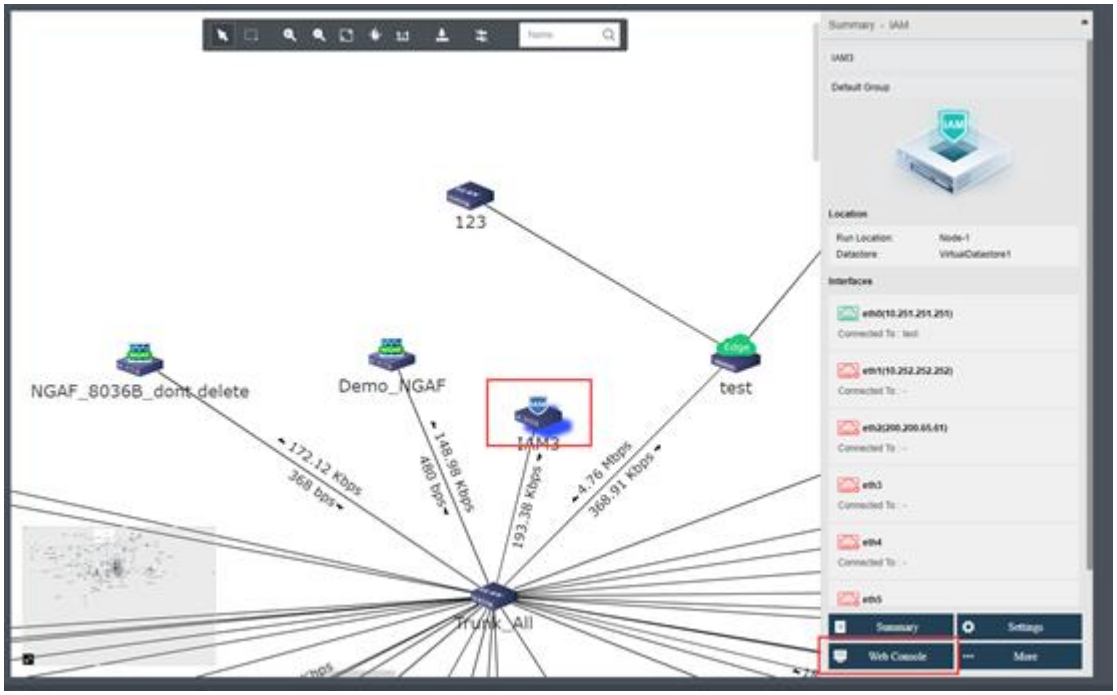
1. Click on the IAG, click the **Licensing** on the right panel.



2. Assign the licensing to the IAG according to the requirement.



3. You can access the VM directly with the following configuration.



1.4 Import to VMware

1. Download the template provided above.
2. Import the virtual machine template into the virtualization platform, where you can import vIAG as a normal Linux server. Follow the platform's virtual machine import instructions to import it.

NOTE

The current provided vIAG virtual machine template supports VMware ESXi 5.0 and above.

3. Edit virtual machine configuration. The default hardware configuration of the virtual machine template provided is as follows:

   CPU: 4

   Memory: 8G

   Number of network ports: 6

   Disk size: 80G

Among them, the CPU and memory can be adjusted as needed. Network ports can also be added as needed, and at least 3 network ports are required to work properly. The disk size does not support adjustment. If you need a larger virtual disk, you need to download the corresponding template.

Below is the authorized bandwidth and vIAG recommended configuration reference table, maximum support 2G bandwidth:

V Type	Performance	Recommended CPU	Recommended Memory
vAC-50	50M	1vCPU	2G
vAC-100	100M	1vCPU	2G
vAC-200	200M	2vCPU	4G
vAC-300	300M	4vCPU	8G
vAC-500	500M	4vCPU	8G
vAC-700	700M	4vCPU	8G
vAC-1000	1G	8vCPU	16G
vAC-2000	2G	8vCPU	16G

Table 1: vIAG Configuration Reference Table

1.5 Setting Up Network for VMware

1. Modify the vIAG management address.

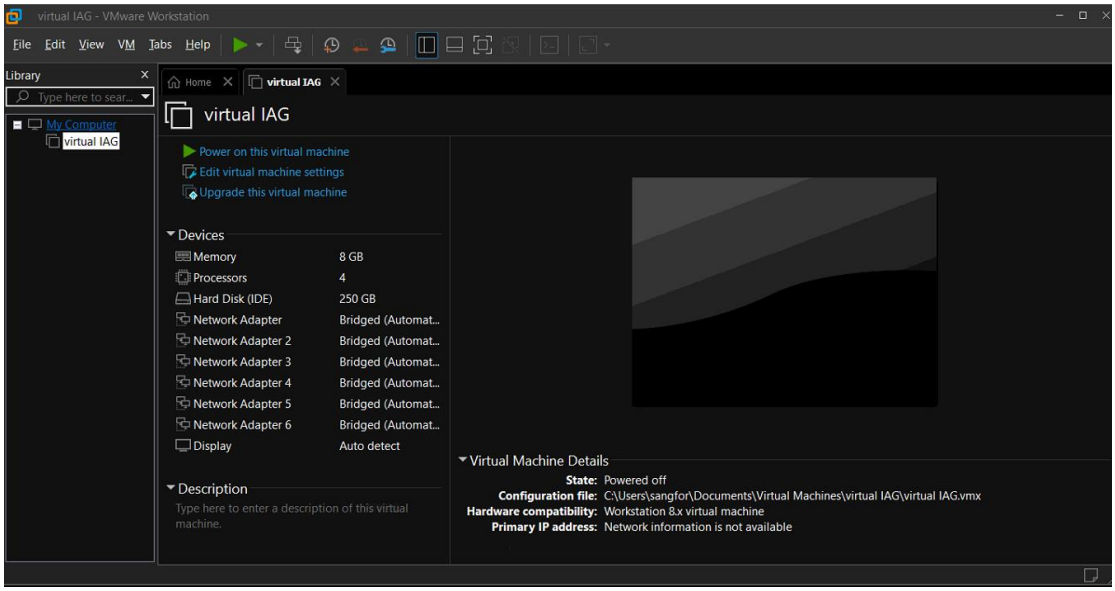
Modify the configuration of the vIAG virtual machine and connect the DMZ port (eth1) of the device to a PC's virtual network interface that can communicate with the vIAG, and connect the WAN port (eth2) of the device to a virtual network that can access the external network. After the vIAG is turned on, it must first obtain or configure the DMZ port IP, which is used to access the management console page.

There are two ways to access the IP address of the DMZ port of the device:

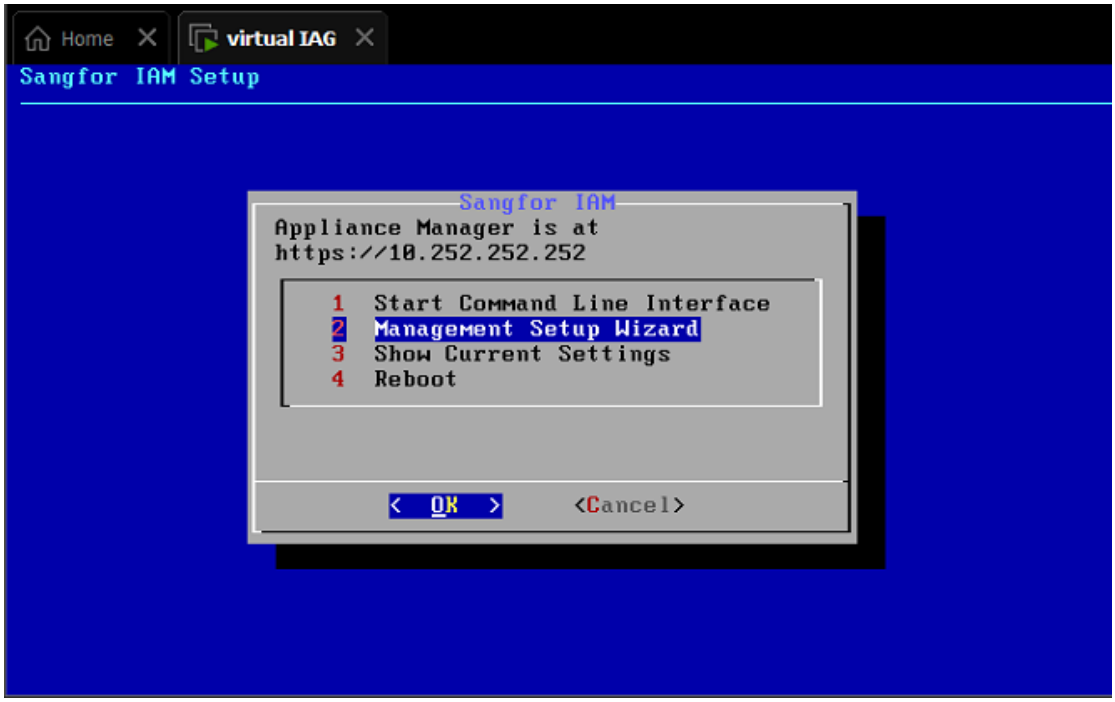
- Configure the PC with the IP address of the same network segment and directly connect to the default IP address of the DMZ port: 10.252.252.252/24 or 128.128.125.252/28, but it is necessary to ensure that there is no IP conflict in the network.
- Open the VMware console and modify the IP address of the DMZ port.

The first method will not be explained here. The second way, configure the DMZ port IP address of vIAG through the VMware console is shown as below, which can be used as a reference for configuration of other platforms:

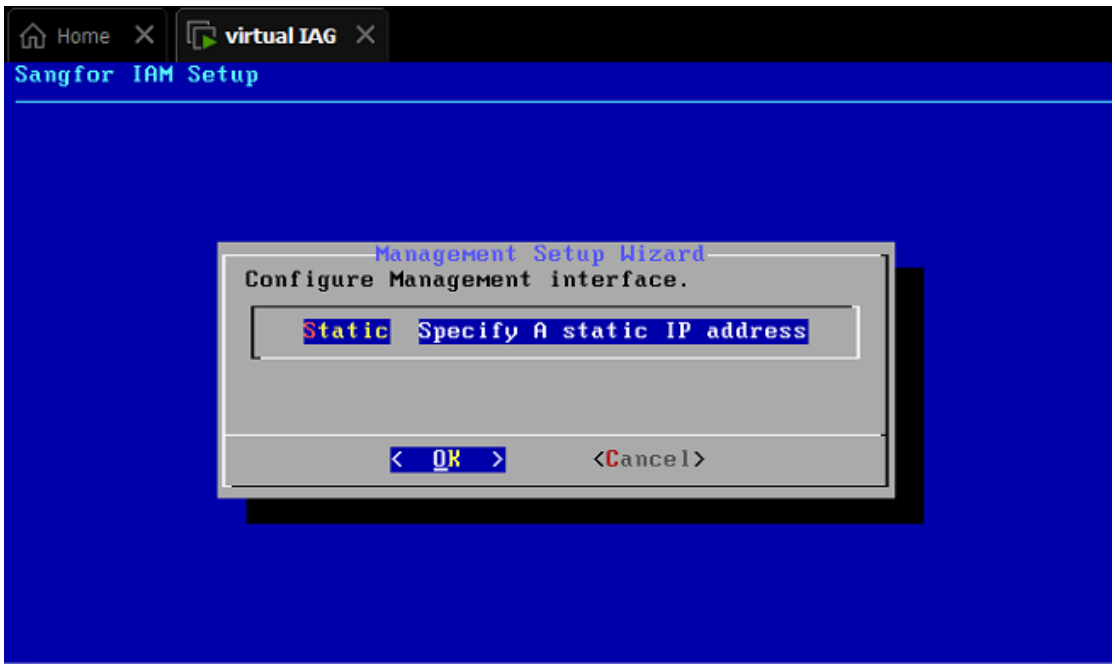
2. Open the virtual machine console.



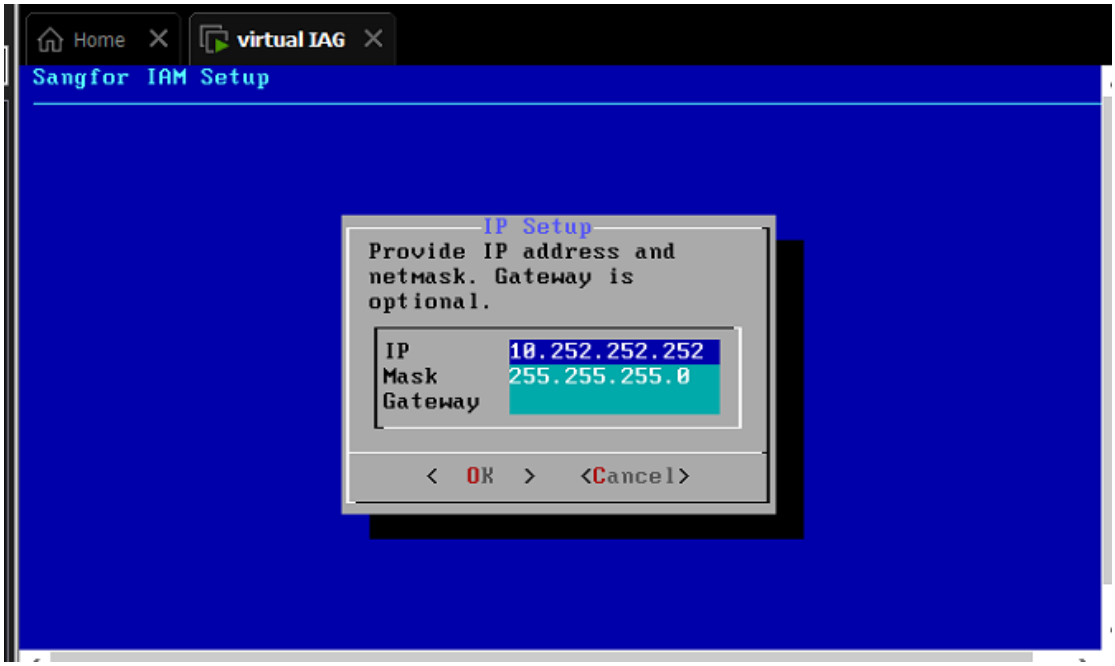
3. Select **Management Setup Wizard** and press **Enter**:



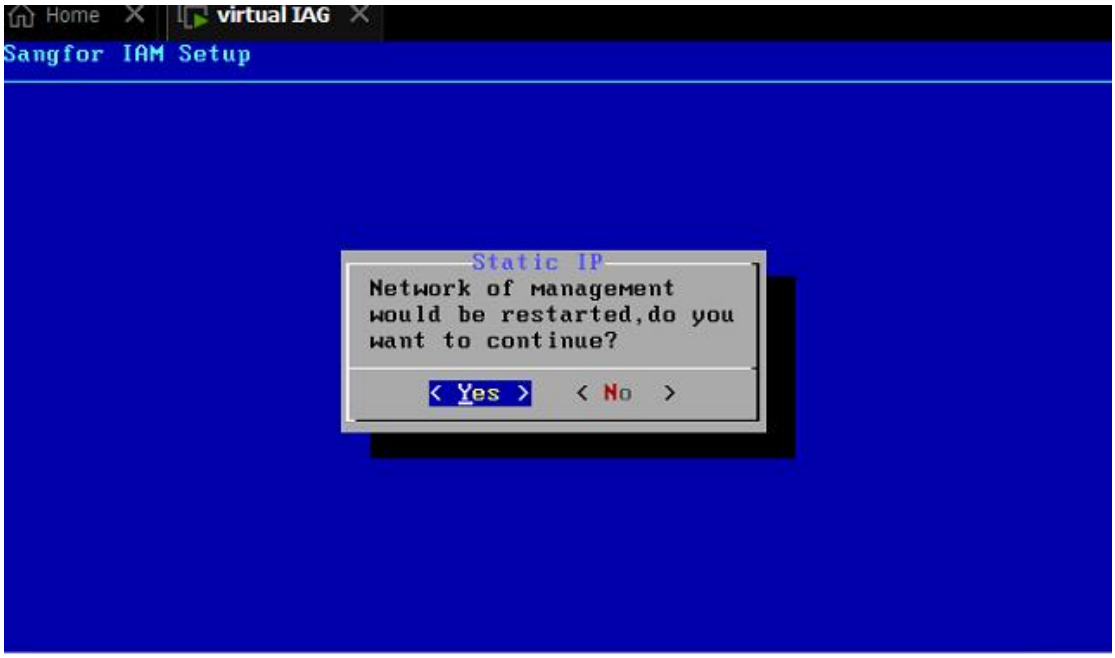
4. Select **OK**.



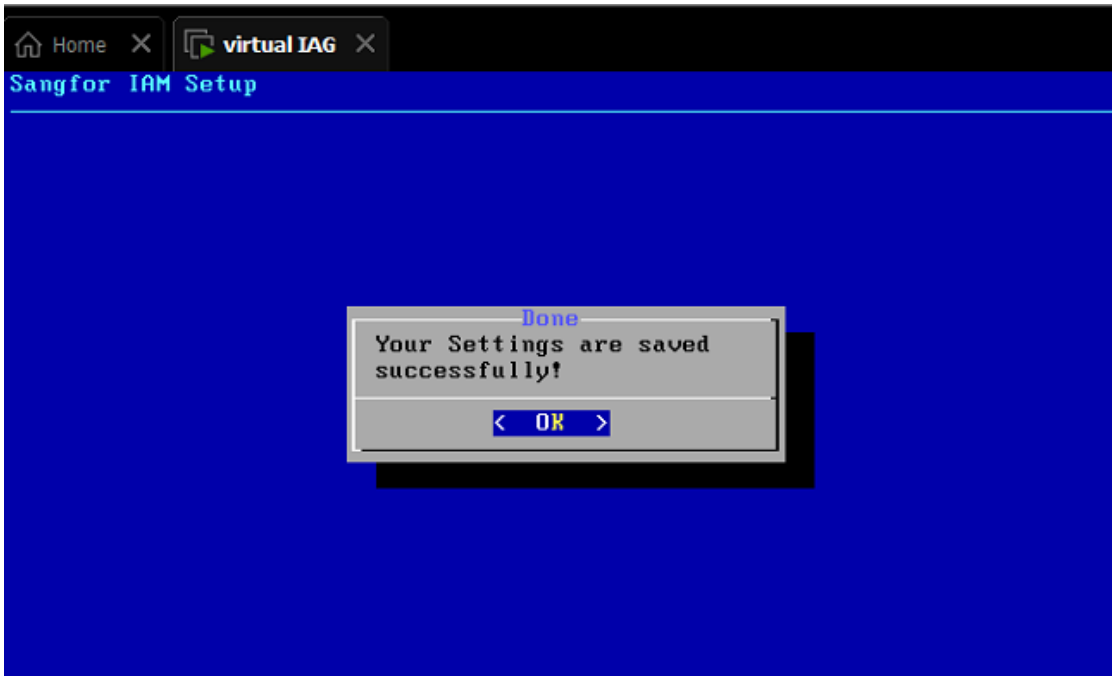
5. The IP configuration page appears, fill in the **IP address**, **Mask** and **Gateway** to be configured (can be omitted), and then press **Enter** to confirm:



6. Select **Yes.**

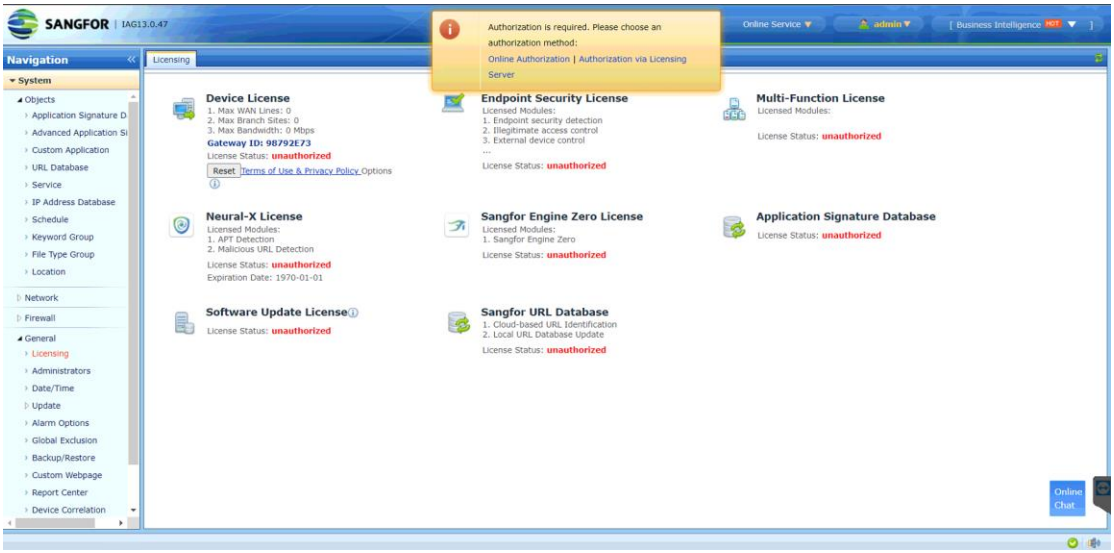


7. After a while, the following page will prompt up to indicate that the IP configuration is successful. If the IP or mask configuration is incorrect, there will be a prompt to reconfigure. Return to modify the incorrect configuration by repeating the above operation:

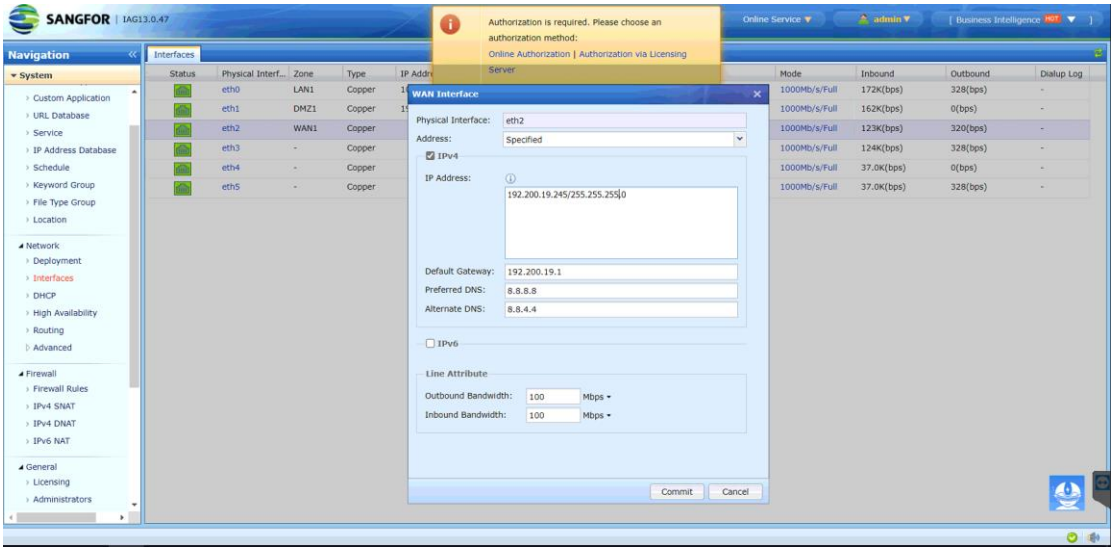


8. Log in to the management console. After the IP configuration is successful, visit https://DMZ IP and log in to the console management interface. The default login username and password are both admins. Unauthorized devices can only display the system section interface. After the

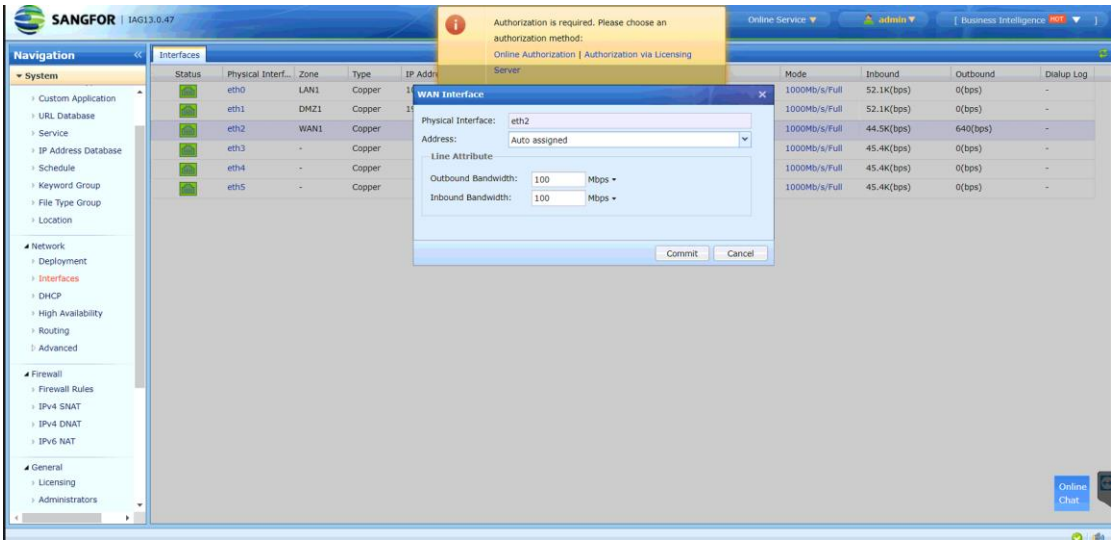
authorization is successful, you can see all the management interfaces after logging in to the device.



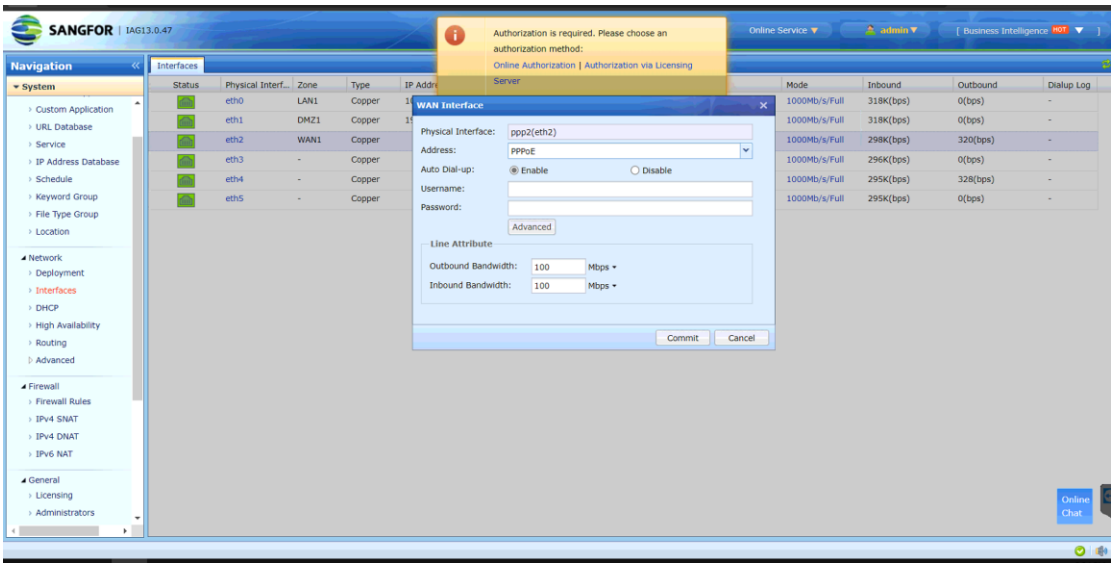
9. Configure the device's WAN port address. To use online authorization, the device must be able to connect to the external network, so you need to modify the device's WAN port IP address, gateway, and DNS configuration to ensure that the device can access the online authorization server.



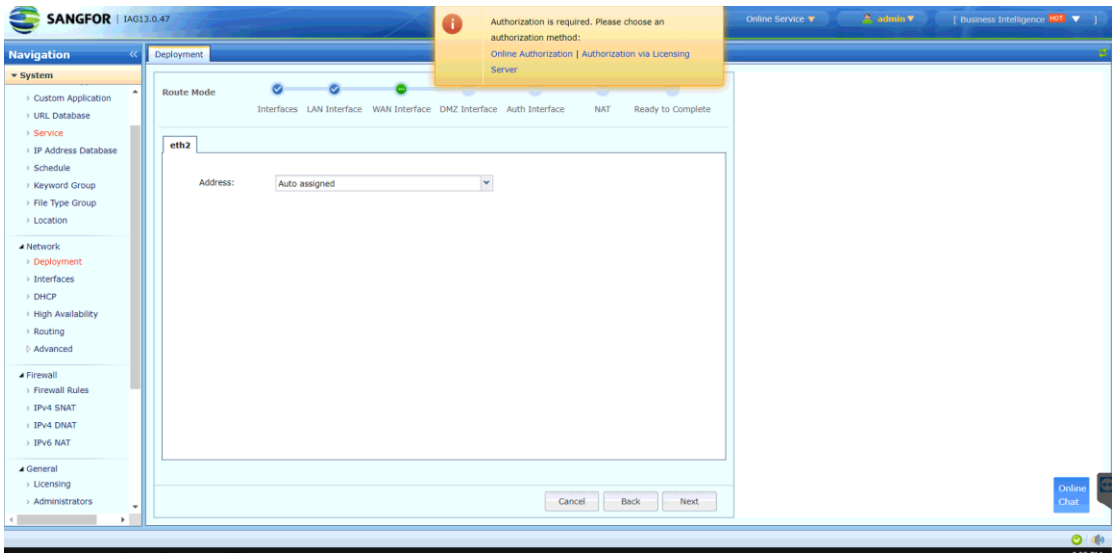
10. Navigate to **System > Network > Interface**, open the network port configuration page, click **WAN (eth2) port**, configure IP, mask, default gateway, DNS, and submit. After submitting the modification, it will automatically log out, and you need to log in to the device again.



11. You can also use DHCP or PPPOE dial-up to automatically obtain the WAN port configuration:

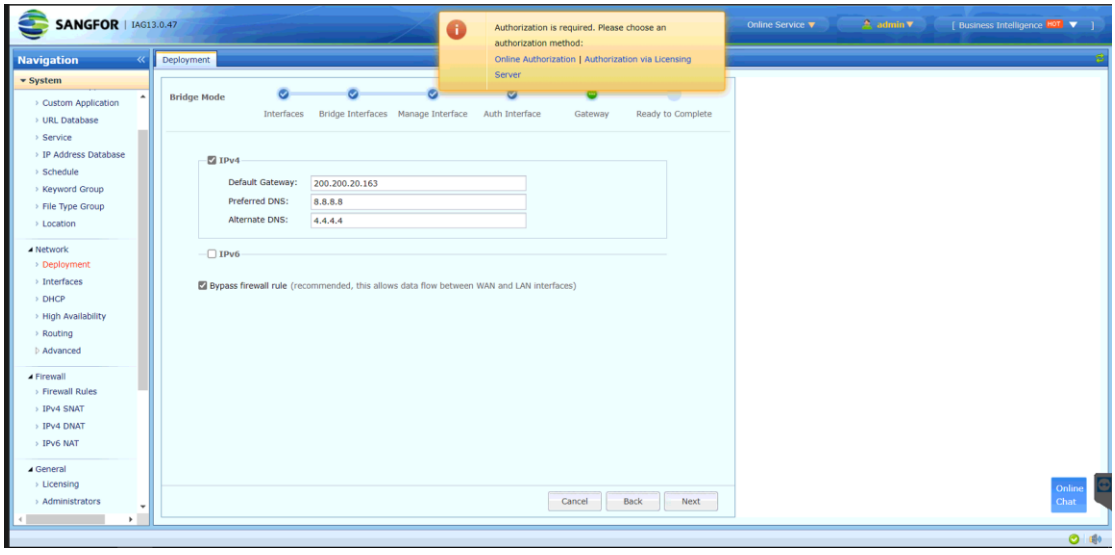


12. In addition to modifying the network port configuration, you can also modify the deployment mode to configure the WAN port address. Click **System > Network > Deployment**, open the deployment mode configuration page, follow the configuration to configure it step by step, and submit after the configuration is complete. After submitting the modification, you will be prompted to restart the device and log in again after the restart is complete:



NOTE

If the device deployment mode needs to be changed from route mode to bridge mode, bypass mode, or single-arm mode, it needs to be configured to access the external network through the DMZ port or single-arm port.



13. After the configuration is complete, you can test whether ping vls.sangfor.com.cn can work in the command console. If it can ping, the network is available. If the ping fails, you need to confirm whether the default gateway, DNZ, or IP address is configured correctly.

1.6 Licensing for VMware vIAG

Online authorization:

You can contact local sales for consultation and purchase online authorization. Authorization includes authorization ID and serial number. For example:

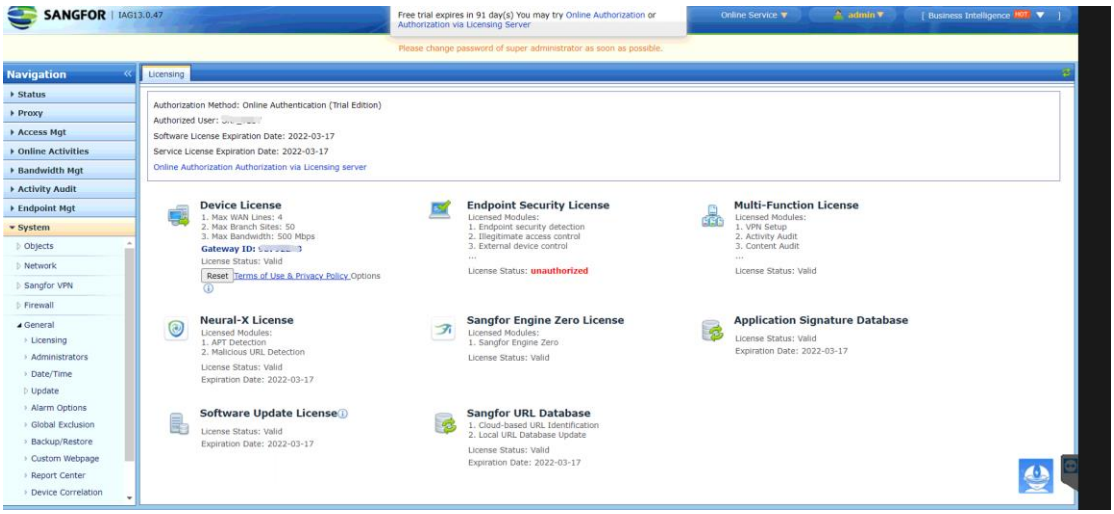
Authorization ID: S8234-5678-90AB-CDEF-1234-5678-90AB-CDEF

Serial number: 1234-5678-90AB-CDEF-1234-5678-90AB-CDEF

Click the online authorization link at the top of the console page, then enter the authorization ID and serial number to submit:

After the authorization is successful, the page will prompt to log in again:

After authorization, if it is authorized by bandwidth, the login interface will display the authorized model:



On the authorization page, you can view the current authorization information, authorization time, enabled functions, service hours, etc. Online authorization can change the serial number or delete the authorization.

NOTE

To use online authorization, you must ensure that vIAG remains connected to the Internet. If you cannot connect to the Internet for 7 consecutive days, the authorization will become illegal, the system function will be limited, and the core configuration interface will be hidden and cannot be edited. If you cannot connect to the Internet for 30 consecutive days, the authorization will become invalid, and the business will be interrupted, which may cause the network to be disconnected.

The authorization ID and the serial number of online authorization can only be used in one system. Suppose the authorization ID and serial number have been used elsewhere. In that case, the authorization ID and serial number in the original system must be deleted before being used on the new system.

For more information, you can refer to **IAG Vmware for vIAG Implementation Guide**

Precaution

1. Not support cross-cable or USB drive factory default recovery method, you may only access to the vmware's console to run reset_cfg to reset the configuration.
2. Not support cross-cable or USB drive password recovery method, you may may only access to the vmware's console to run reset_pwd to reset the password.
3. Vmware not support for the Active-standby High available deployment.
4. Not support hardware bypass feature including network interface bypass or fiber optic bypass feature.
5. Not support High available deployment mode for Active-standby.

SANGFOR