SANGFOR aBOS User Manual

Oct 2nd , 2015

Table of Contents

Disclaimer

Preface

Contents in each chapter:

Chapter 1: Introduction to aBOS(a Box of Sangfor).

Chapter 2: Configuration through the aBOS GUI.

Case Study: Creating a virtual machine.

Configuration examples are based on Sangfor aBOS 1.0 official version. The actual product you have purchased and received may vary.

Document Conventions

Graphic Interface Conventions

This manual uses the following typographical conventions for special terms and instructions.

Item	Convention	Meaning
Button	Boldface	Click the **Save** button to save the settings.
Menu/submenu	Boldface	The basic **settings** are under **System** > **Settings**.
Multilevel menu and submenu	>	Navigate to **System** > **Network Interface** to configure the network interfaces.
Options, radio button option, checkbox option	Boldface	Select the option **Enable user** to enable this user account.
Page title	Boldface	Navigate to **System** > **Administrator** to enter the **Administrator** page.
Prompt	“ ”	The browser may pop up the prompt “The settings have been saved successfully. Do you want to restart the device now to apply the changes? ”

Symbol Conventions

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

 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

Contact Us

For technical support or other questions, you may contact us through the following:

Email: support@sangfor.com.cn

Tel: 400-630-6430

Forum: http://sangfor.360help.com.cn/

Website: www.sangfor.com.cn

Acknowledgments

Thanks for using our product and user manual. If you have any suggestion about our product or user manual, please provide feedback to us through phone call or email. Your suggestion will be much appreciated.

Chapter 1 Knowing Your Sangfor Device

This chapter introduces how to install Sangfor aBOS unit and connect it to your network. After proper installation, you can configure and debug this aBOS unit.

Operating Environment

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

To ensure endurance and stability of this aBOS unit, make sure the following are done:

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

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

Product Appearance

The above figure is the front panel of Sangfor aBOS unit.

The above picture is just for reference. The actual product you have purchased and received may vary.

Connecting Your Sangfor aBOS Unit

1. Deploy the Sangfor aBOS unit in your network.
2. Plug the power cable into the power interface on the rear panel of the aBOS unit. Attach and turn on power supply, and then watch the LEDs on the front panel of the unit. When the aBOS unit starts up, the **POWER** LED (in blue) will turn on.

   If the aBOS unit works properly, disk and ACT(data flow) LED indicators flicker, and POWER and ETH0 LED indicators stay on always.
3. Use RJ-45 straight-through Ethernet cable to connect the LAN interface (ETH0, the first interface on the rear panel) to the internal network (LAN).

Chapter 2 Initial Login to Admin Console

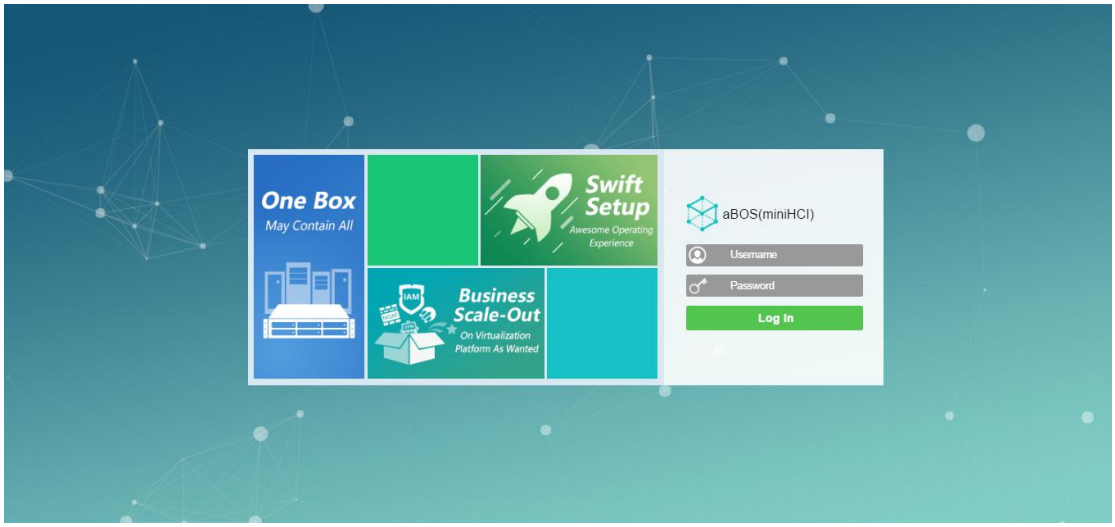
Sangfor aBOS unit provides web-based administration through administrator console. The initial URL for admin console access is https://10.250.0.7.

Before logging in to web admin console, make sure the following are done:

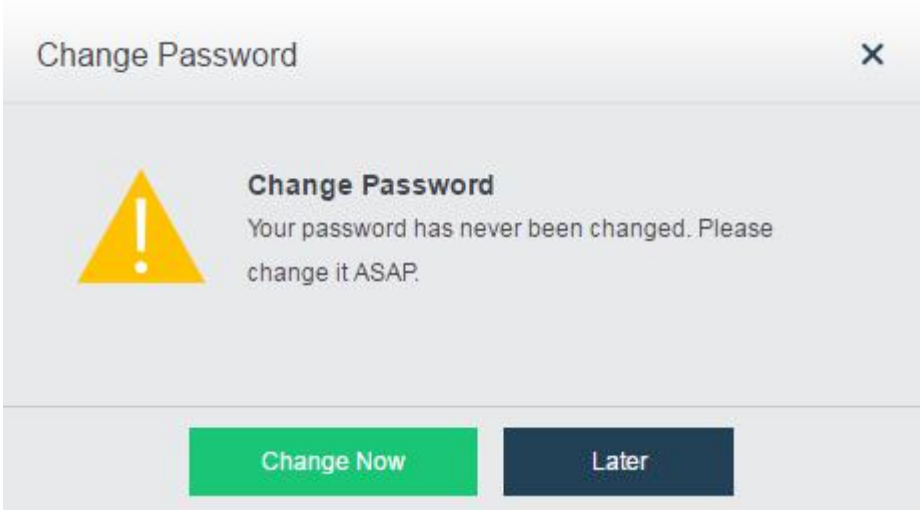
- Deploy a computer on a subnet where the Sangfor aBOS unit resides.
- Connect the PC's network interface card (NIC) and the aBOS unit's LAN interface to a same layer-2 switch using network cable.
- Add an IP address on the PC, which resides on the network segment 10.250.0.x.

Logging in to Admin Console

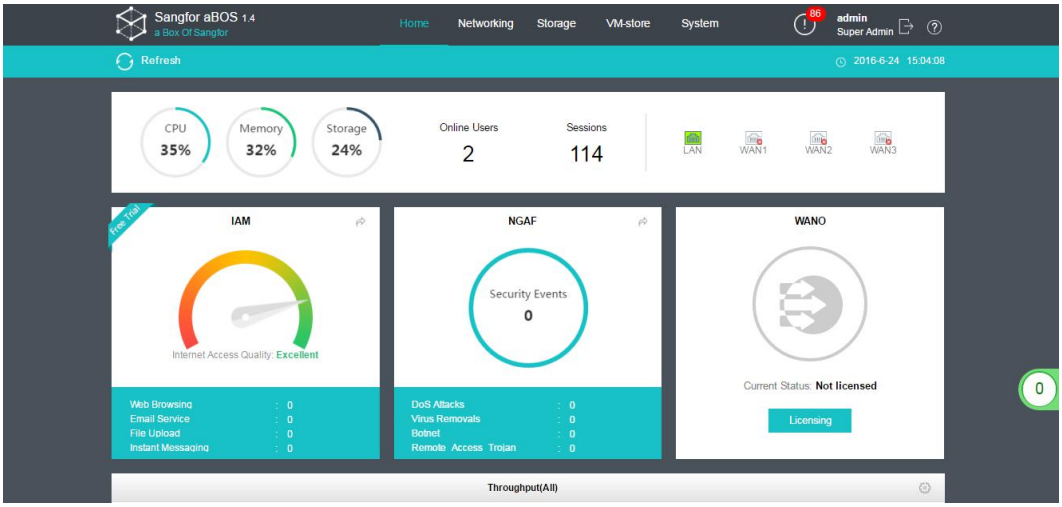
1. Turn on the PC and Sangfor aBOS unit.
2. Open a web browser and enter the IP address of the aBOS unit (https://10.250.0.7) into the address bar. Press **Enter** key to visit the login page to aBOS web Admin console, as shown below:



3. Enter the administrator username and password, and then click **Log In** Button. Both of the default username and password are **admin** (case-sensitive).
4. Upon successful login, the following dialog pops to prompt administrator to change password, as shown below:



To change password right now, click **Change Now**. If you do not want to change the password, click **Later** and enter the following page:



Web admin console of the aBOS unit can be accessed by using the following web browsers: Microsoft IE, Mozilla Firefox and Google Chrome, etc.

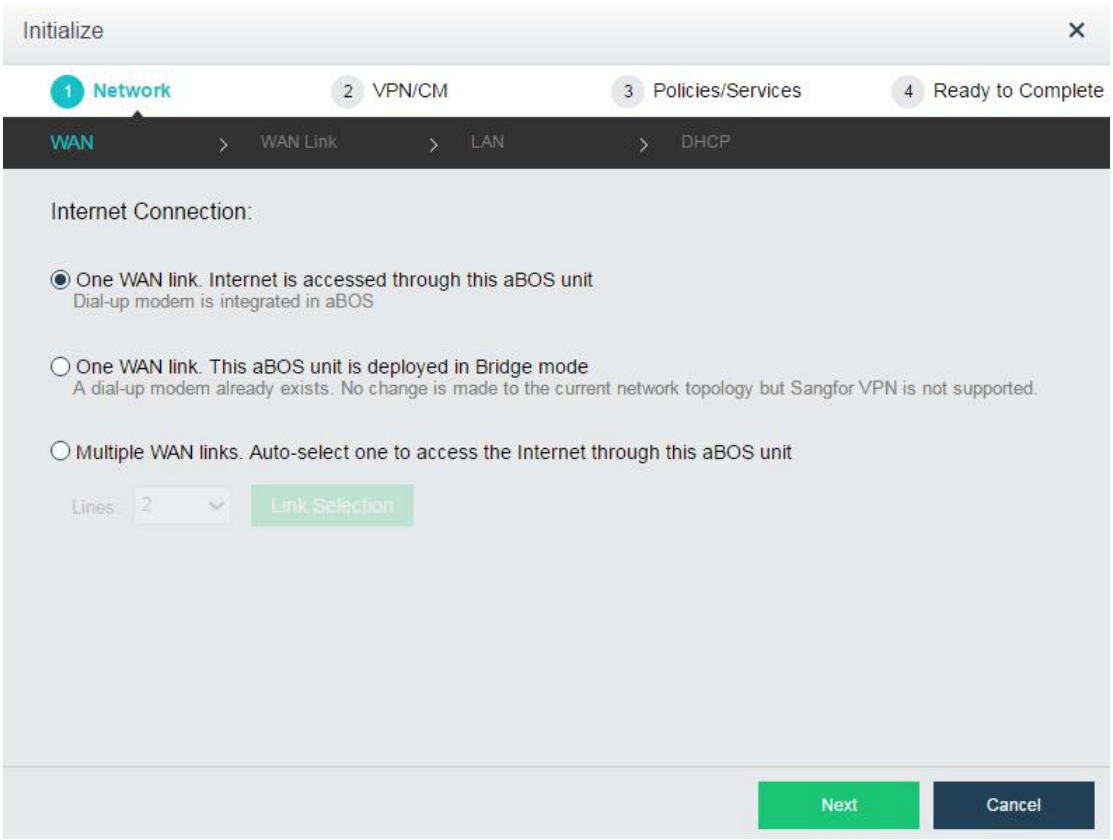
Initializing Network

Sangfor aBOS unit can be set up simply by initializing network. Network initialization settings cover the following: **Network**, **VPN/CM**, **Policies/Services**.

Configuring Network

You can configure **WAN**, **WAN Link**, **LAN** and **DHCP** settings on **Network** tab. The network settings are applied to the virtual network device connected to the edge. More specifically, if the IAM appliance is connected to the edge, the network settings will be applied to that IAM appliance; if the NGAF is connected to the edge, the network settings will be applied to that NGAF. Network configuration steps are as follows:

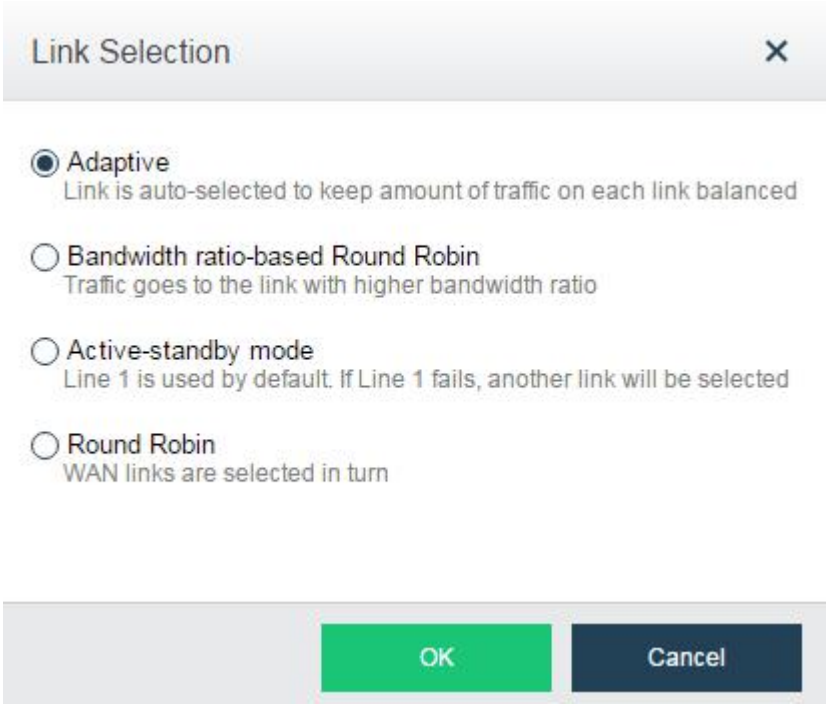
1. Select an Internet connection type. In this example, it is **One WAN link. Internet is accessed through this aBOS unit**, as shown below:



There are three types of Internet connections:

- **One WAN link. Internet is accessed through this aBOS unit**: The aBOS unit is deployed as a gateway in the network, and Internet is accessed through the unit over the WAN link. IP address for the WAN link can be assigned in the following ways: **Using PPPoE**, **Using DHCP**, and **Specified**.
- **One WAN link. This aBOS unit is deployed in Bridge mode**: It requires a gateway deployed between this aBOS unit and the external network, which connects to the Internet by using dial-up connection or using static IP address.

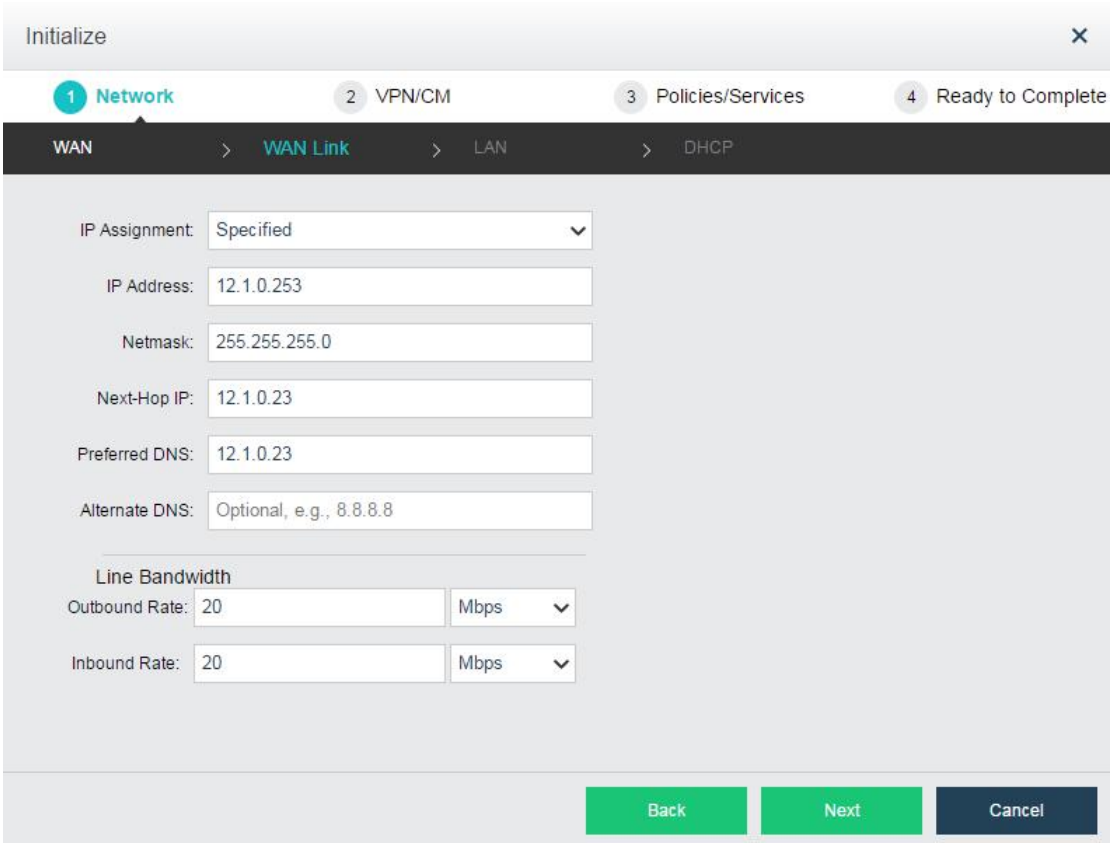
- **Multiple WAN links. Auto-select one to access the Internet through this aBOS unit**: The aBOS unit is deployed in Gateway mode. There are multiple WAN links, among which one is selected based on the link selection policy, as shown below:



Link can be selected from the multiple links by using any of the following means:

- **Adaptive**: Link is auto-selected to keep amount of traffic on each link balanced despite of the remaining bandwidth of each link.
- **Bandwidth Ratio-based Round Robin**: Traffic goes to the link with higher bandwidth ratio.
- **Active-Standby Mode**: Line 1 is used by default. If Line 1 fails, another line will be selected.
- **Round Robin**: WAN links are selected in turn.

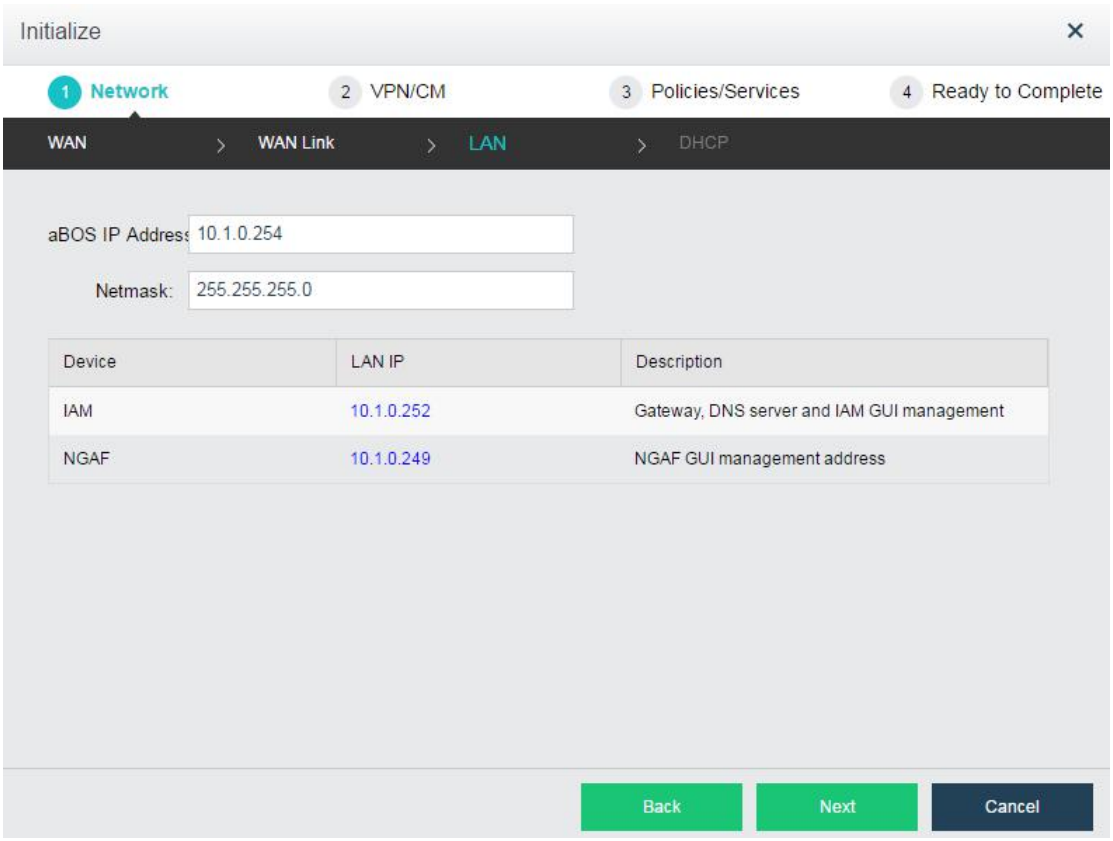
2. Configure WAN link. You can specify **IP Assignment**, **IP Address**, **Netmask**, **Next-Hop IP**, **Preferred DNS**, **Alternate DNS**, and **Line Bandwidth**, etc. In this example, IP assignment method is **Specified,** as shown below:



The contents on **WAN Link** tab are described as follows:

- **IP Assignment:** It can be **Using PPPoE**, **Using DHCP** or **Specified**.
- **IP Address**: Specifies IP address for the WAN link.
- **Netmask**: Specifies netmask of the specified IP address.
- **Next-Hop IP:** Specifies IP address of the gateway for the WAN link.
- **Preferred DNS**: Specifies IP address of the preferred DNS server.
- **Alternate DNS**: Specifies IP address of the alternate DNS server.
- **Line Bandwidth**: Specifies outbound and inbound rate.

3. Configure LAN interfaces. You can specify **aBOS IP Address**, **Netmask** and **LAN IP** addresses of virtual network devices.

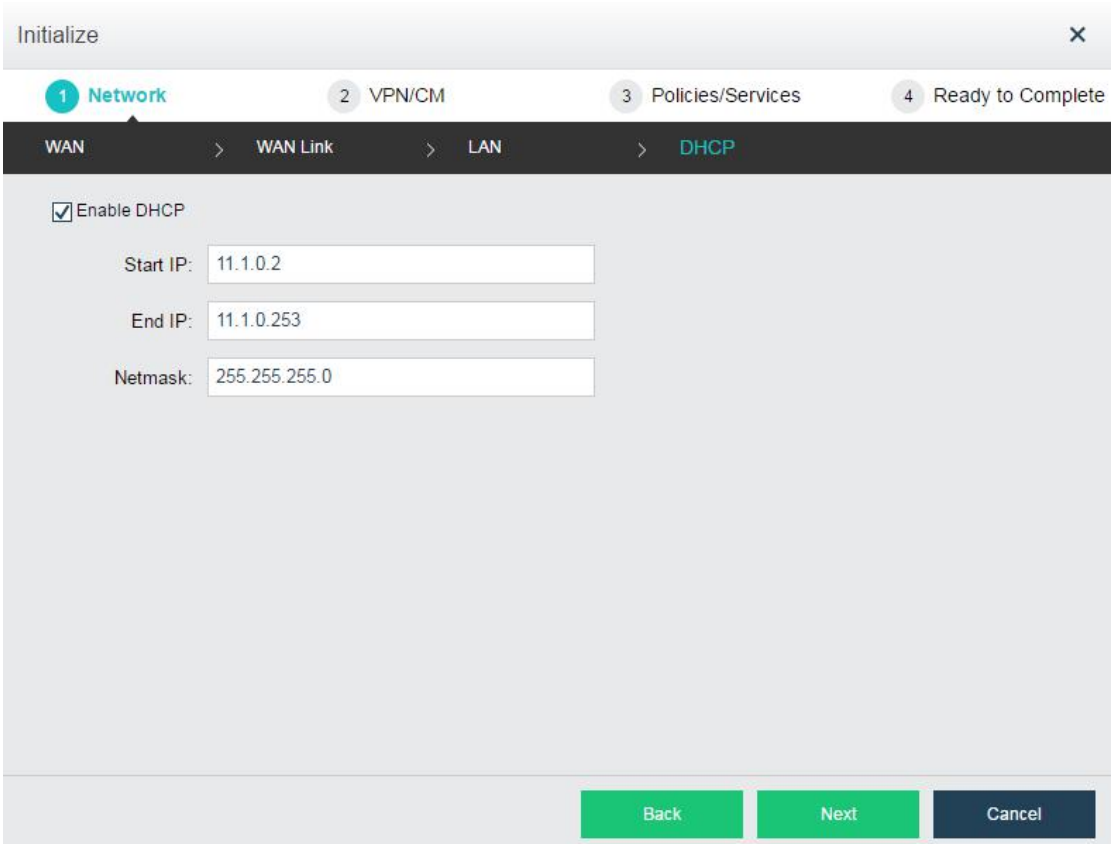


The following are contents included on **LAN** tab:

- **aBOS IP Address**: Specifies LAN interface address of the aBOS unit.
- **Netmask**: Specifies netmask of the aBOS IP address.
- **Device**: Displays the name of virtual network device.
- **LAN IP**: Displays GUI management IP addresses of virtual network devices. To change LAN IP address, click the IP address in **LAN IP** column to edit it.
- **Description**: Descriptive information to LAN IP address.

  Once aBOS IP address and netmask are specified, LAN IP addresses will be automatically generated for virtual network devices. If the auto-generated IP address conflicts with a local IP address, click that IP address in **LAN IP** column to change it.

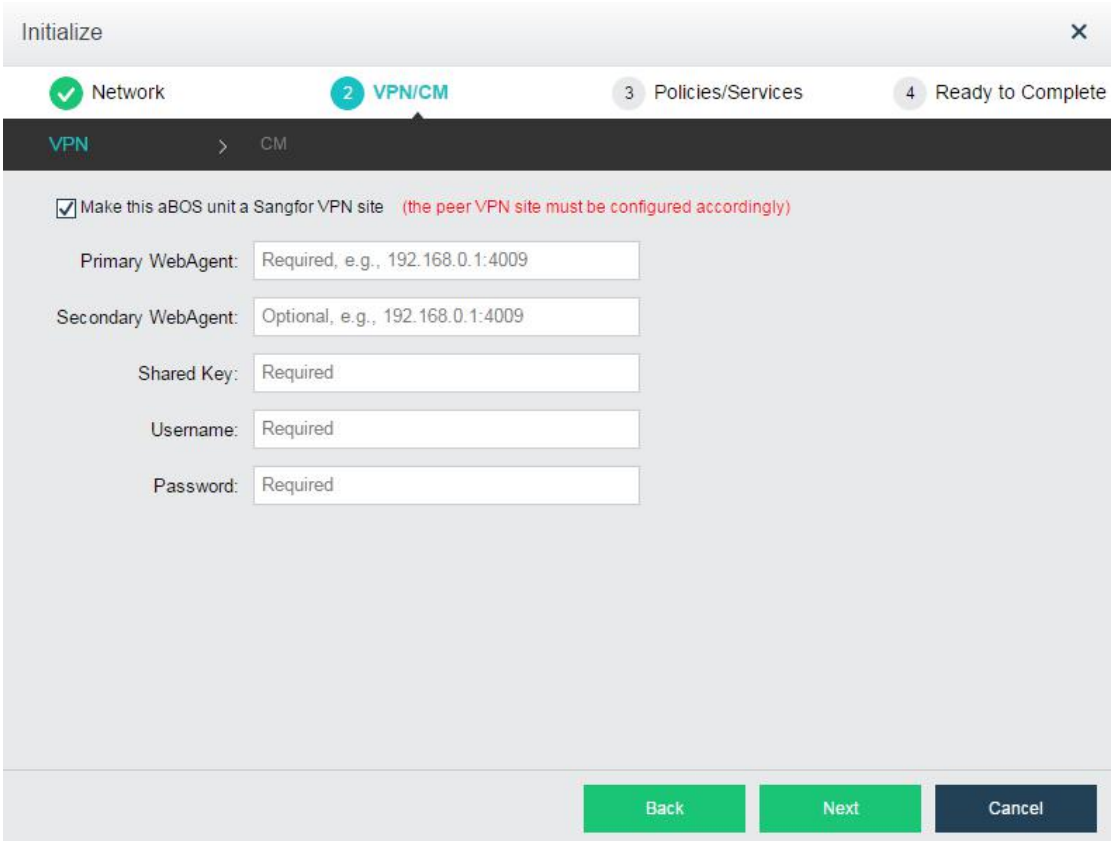
4. Configure DHCP, which is used to automatically allocate IP addresses to internal computers. Only when the aBOS unit is deployed as a gateway, the DHCP settings are available, and then this unit could assign IP addresses to the internal computers that are connected to the LAN interface of the aBOS unit. To configure DHCP, enable DHCP and specify **Start IP**, **End IP** and **Netmask** fields on the following page:



Configuring VPN/CM

You can configure **VPN**, **WAN Optimization** and **CM** on **VPN/VM** page.

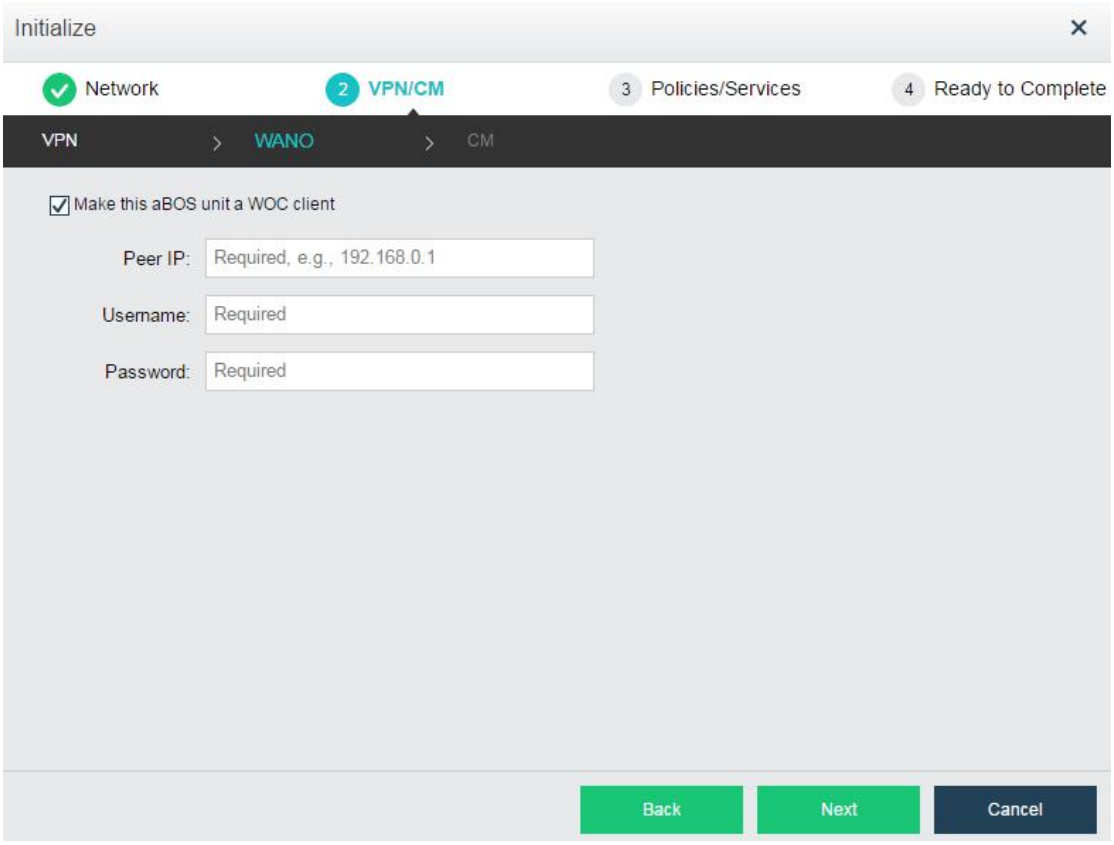
1. Configure VPN. If the IAM appliance is connected to the edge, the VPN settings will be pushed down to IAM appliance; if the NGAF is connected to the edge, the VPN settings will be pushed down to the NGAF.



The following are contents included on **VPN** tab:

- **Make this aBOS unit a Sangfor VPN site**: Select this option to make this aBOS unit a Sangfor VPN site.
- **Primary WebAgen**t: Specifies the address of primary WebAgent, which is used to connect to the peer unit.
- **Secondary WebAgent**: Specifies the address of secondary WebAgent, which is used to connect to the peer unit.
- **Shared Key:** Specifies the shared key used to establish a Sangor VPN connection to the peer, which should be the same as that specified on the peer.
- **Username**: Specifies the username used to connect to the peer, which is created on the peer.
- **Password**: Specifies the password used to connect to the peer, which is created on the peer.
- **Protocol**: Specifies the protocol, TCP or UDP, which determines the type of packets transferred via VPN tunnel.

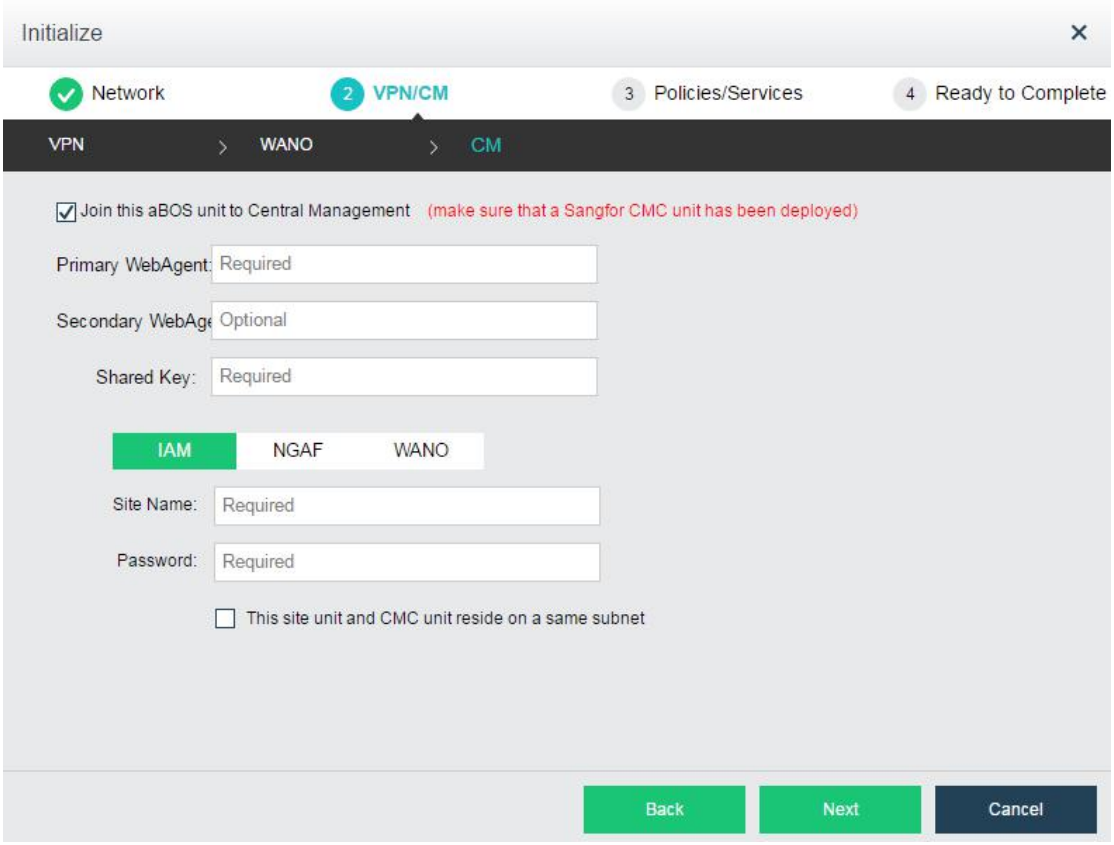
2. Configure WAN optimization on the following page.



The following contents are included on the above page:

- **Make this aBOS unit a WOC client**: Select this option to make this aBOS unit a WOC client.
- **Peer IP:** Specifies the IP address of LAN interface of the peer WOC unit.
- **Username**: Specifies the username used to connect to the peer WOC unit, which is created on that peer.
- **Password**: Specifies the password used to connect to the peer WOC unit, which is created on that peer.

3. Configure central management (CM) on **CM** tab, as shown below:



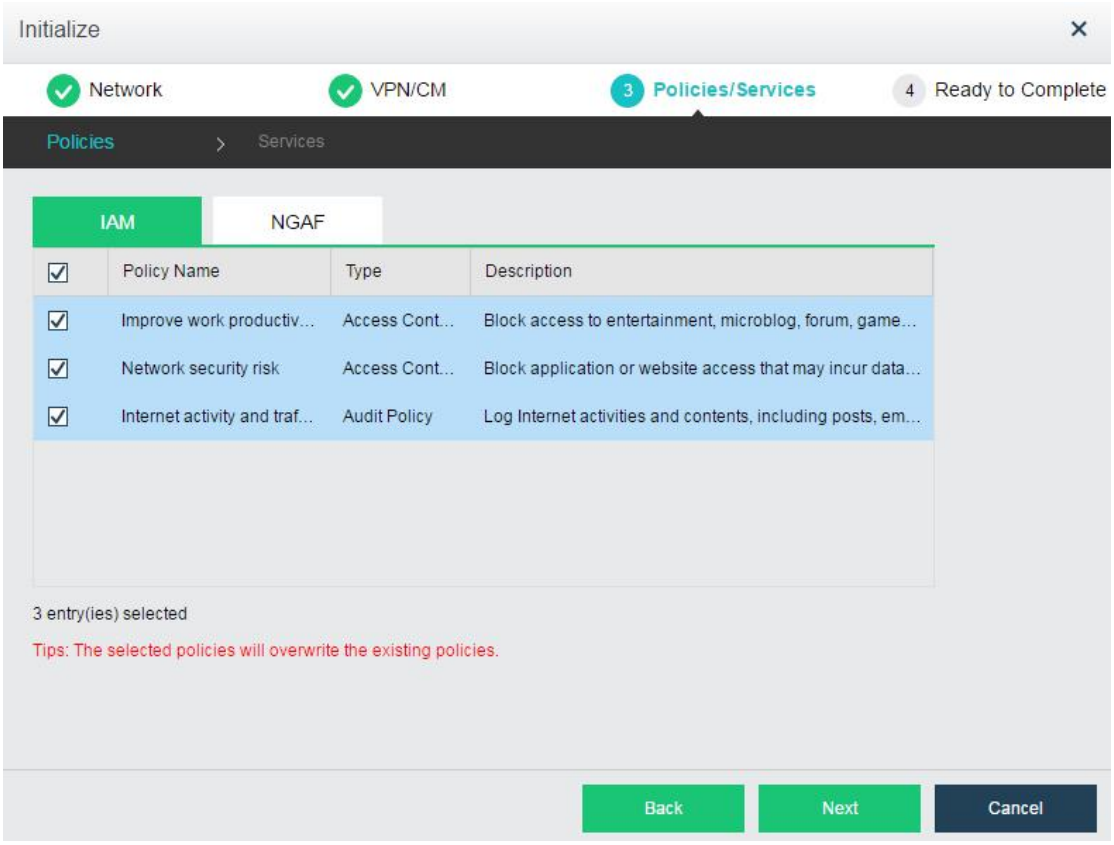
The contents included on **CM** tab are described as follows:

- **Join this aBOS unit to Central Management**: Select this option to have this aBOS unit joined to central management.
- **Primary WebAgent:** Specifies address of primary WebAgent to connect the CMC unit.
- **Secondary WebAgent:** Specifies address of secondary WebAgent to connect to the CMC unit.
- **Shared Key**: Specifies the shared key used to connect to the CMC unit, which should be same as that specified on that CMC unit.
- **Site Name**: Specifies the name of the site unit to be joined to CM.
- **Password**: Specifies the password to join the site to CM, which is created on the CMC unit.
- **This site unit and CMC unit reside on a same subnet**: If this option is selected, it indicates that the site unit resides on the same subnet as the CMC unit.

Configuring Policies/Services

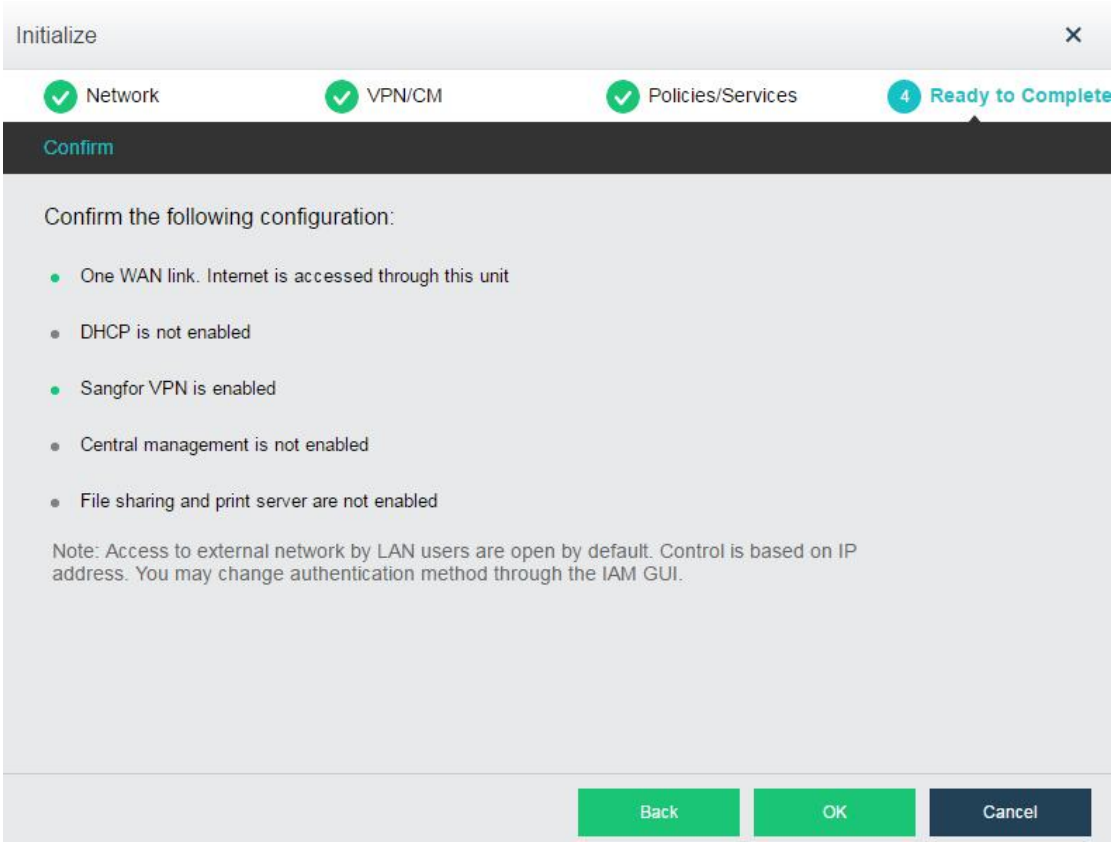
You can configure policies and services on **Policies/Services** page.

1. Select policies for IAM and NGAF and then click **Next**, as shown below:



2. Configure services. By default, the aBOS unit provides a file sharing and print server running Linux. Default IP address of that server is 10.251.251.200. To use the file sharing and print service, you need to change this IP address to one on the same subnet as the LAN interface address of the aBOS unit.

3. aBOS unit initialization is ready to complete when you come to **Ready to Complete** page. Before clicking **Commit**, make sure the configuration is correct, as shown below:



Viewing Status

After successful login to aBOS web admin console, home and some other function modules are seen on the top of the page, as shown below:

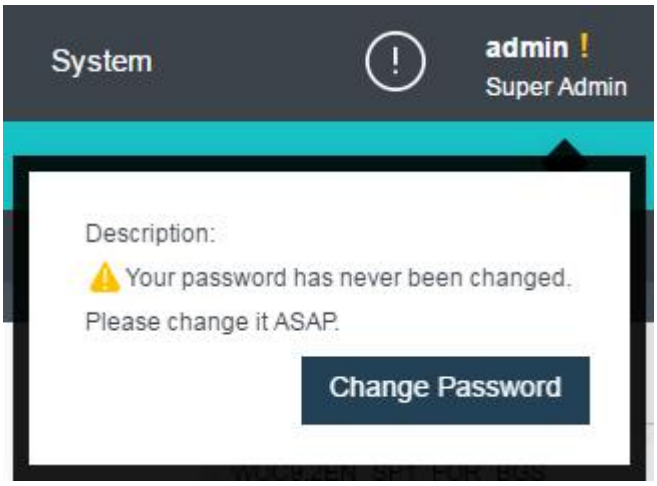
There are the following modules:

- **Home**: Displays the information about the aBOS unit, virtual network devices, throughput, application traffic ranking and user traffic ranking, etc.
- **Networking**: Configures virtual network devices.
- **Storage**: Displays storage status and manages storage nodes.
- **VM-store**: Displays licensing status of virtual network devices. You can also apply for free trial for the virtual network devices on **VM-store** page.
- **System**: Configures system related settings: **Licensing**, **Date and Time**, **Administrators**, **Alarm Options**, **Logs and Alarms**, **VM Backup and Recovery**, **System Backup and Restore**, **Upgrade**, **Service & Tech Support**, **Recycle Bin** and **System Options**.

To see alarm events, click on the 

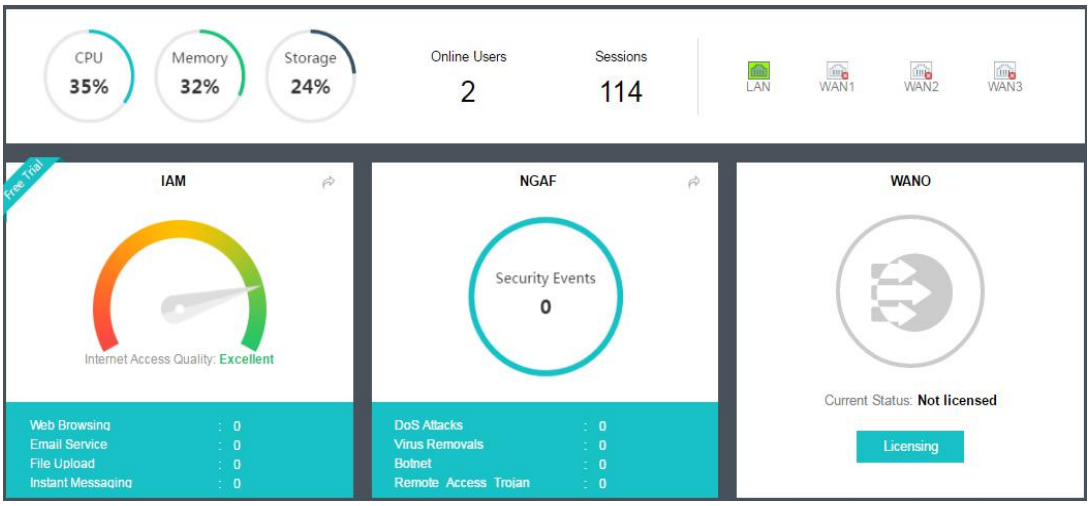
icon (the number on the icon means the number of the current alarm events). Then, you will see the latest 5 alarm events, as shown below:

If the administrator password is too weak, there will be an exclamation mark next to the administrator username. Click on the username, the following dialog pops up:



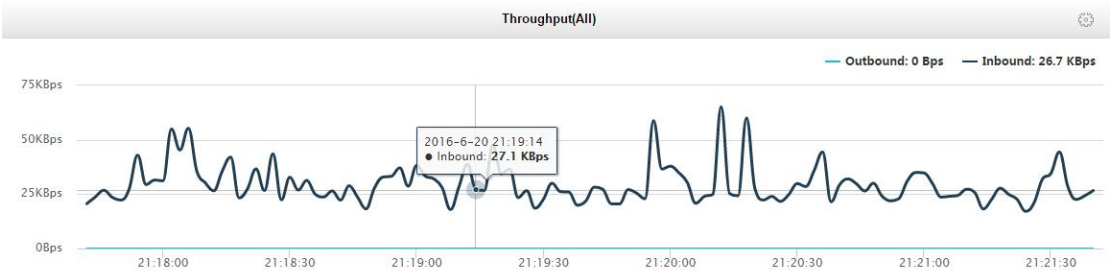
Viewing System Status

This section displays resources usage of this aBOS unit, including CPU, memory and storage usage, and information of online users and sessions, and status of interfaces, etc. What's more, it displays the basic information of virtual network devices.

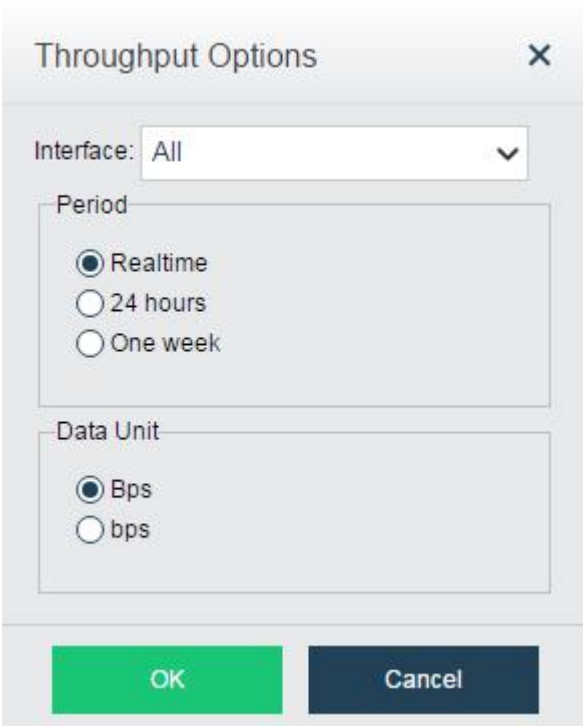


Viewing Throughput

The following line chart displays outbound and inbound rate in real time:



To specify throughput display criteria, click the icon and the following dialog pops up:



The following are contents on **Throughput Options** page:

- **Interface**: Specifies the interface. Throughput on that interface will be displayed.
- **Period**: Specifies the period, **Realtime**, **24 hours** or **One week**. Throughput in the specified period will be displayed.
- **Data Unit**: Specifies the traffic unit, **Bps** or **bps**.

Viewing Application Traffic Ranking

This section displays the top 10 applications by traffic, as shown below:

Application Traffic Ranking

Rank	Application Category	Outbound R...	Inbound Rate	Bidirectional	Percent
1	Visit Web Site	2.4 Mbps	27.7 Mbps	30 Mbps	41.4%
2	BT	13 Mbps	13.9 Mbps	26.9 Mbps	37.1%
3	HTTP_POST	6.7 Mbps	8 Mbps	14.8 Mbps	20.3%

Viewing User Traffic Ranking

This sections displays the top 10 users by traffic, as shown below:

User Traffic Ranking

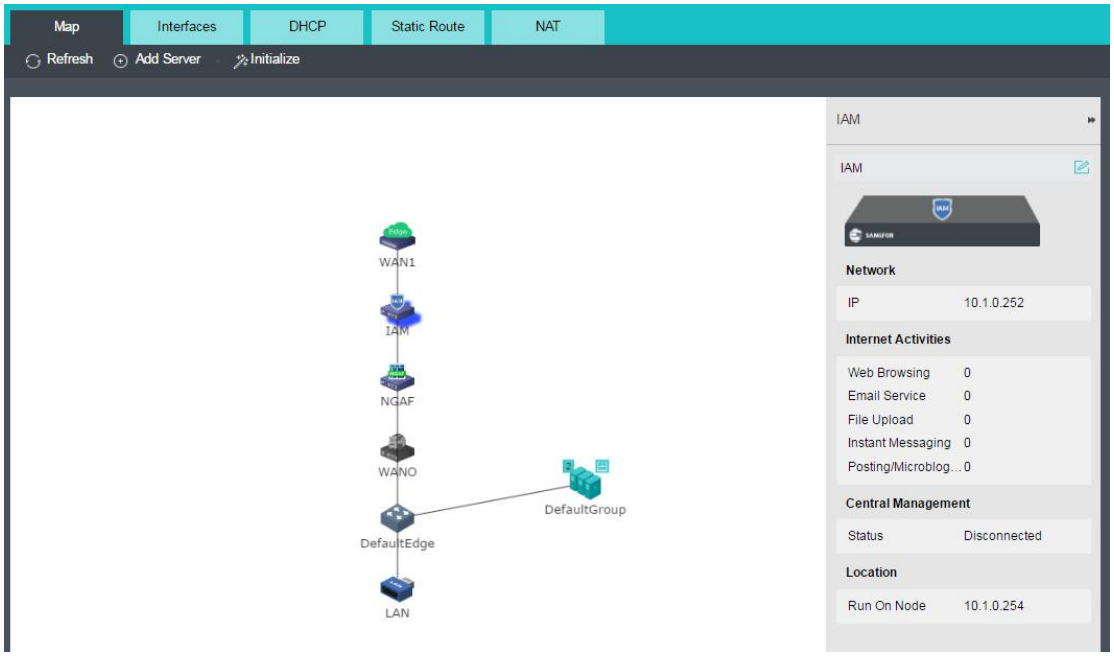
Rank	Username	Group	Outbound R...	Inbound Rate	Bidirectional
1	177.122.1.201	/	595.8 Kbps	693.1 Kbps	1.3 Mbps
2	177.122.1.202	/	595.8 Kbps	693.1 Kbps	1.3 Mbps
3	177.122.1.198	/	595.8 Kbps	693.1 Kbps	1.3 Mbps
4	177.122.1.197	/	595.8 Kbps	693.1 Kbps	1.3 Mbps
5	177.122.1.199	/	595.8 Kbps	693.1 Kbps	1.3 Mbps

Networking

You can configure **Map**, **Interfaces**, **DHCP**, **Static Route** and **NAT** in **Networking**.

Drawing Objects on Network Topology Map

You can view status of the network topology, and edit each virtual network device and virtual server on the **Map** page in **Networking**.

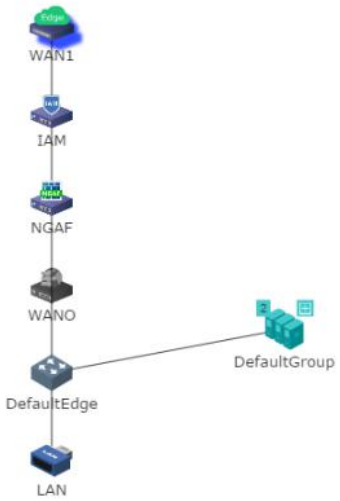


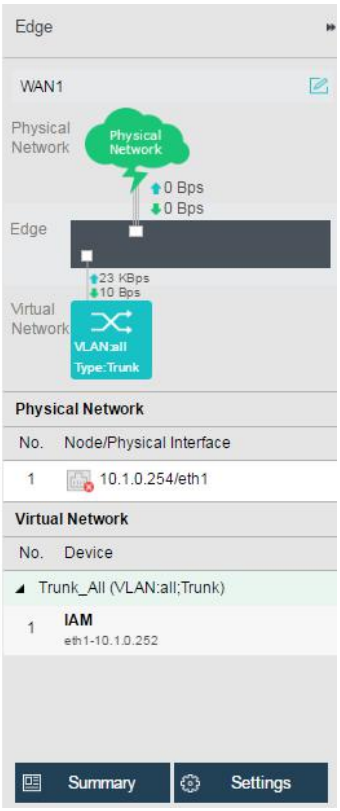
Configuring Edge

The edge connects the virtual network to the physical network. It is connected to the physical network through an aggregate interface or a physical network interface in Trunk mode. When configuring edge, you need to specify port group. A port group is an aggregate port that connect edge to virtual network, the member interfaces own the same configuration (such as VLAN).

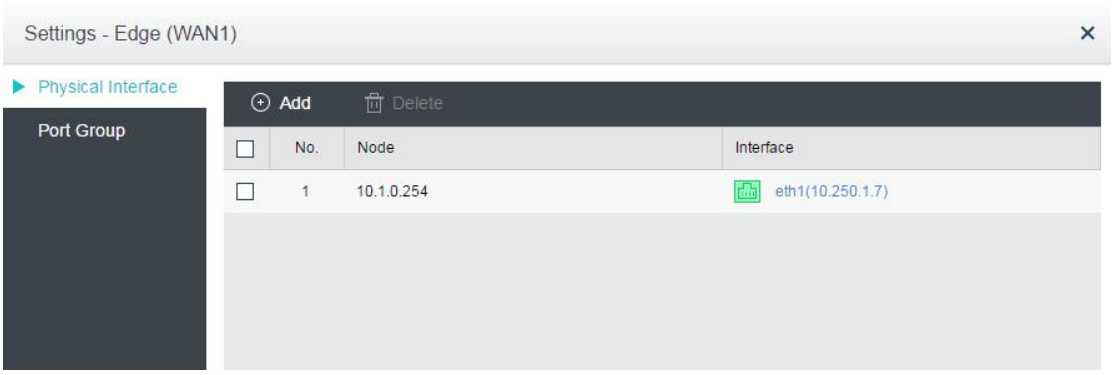
To configure the edge, do the followings:

1. Click on the edge and then the **Settings** button on the following page:

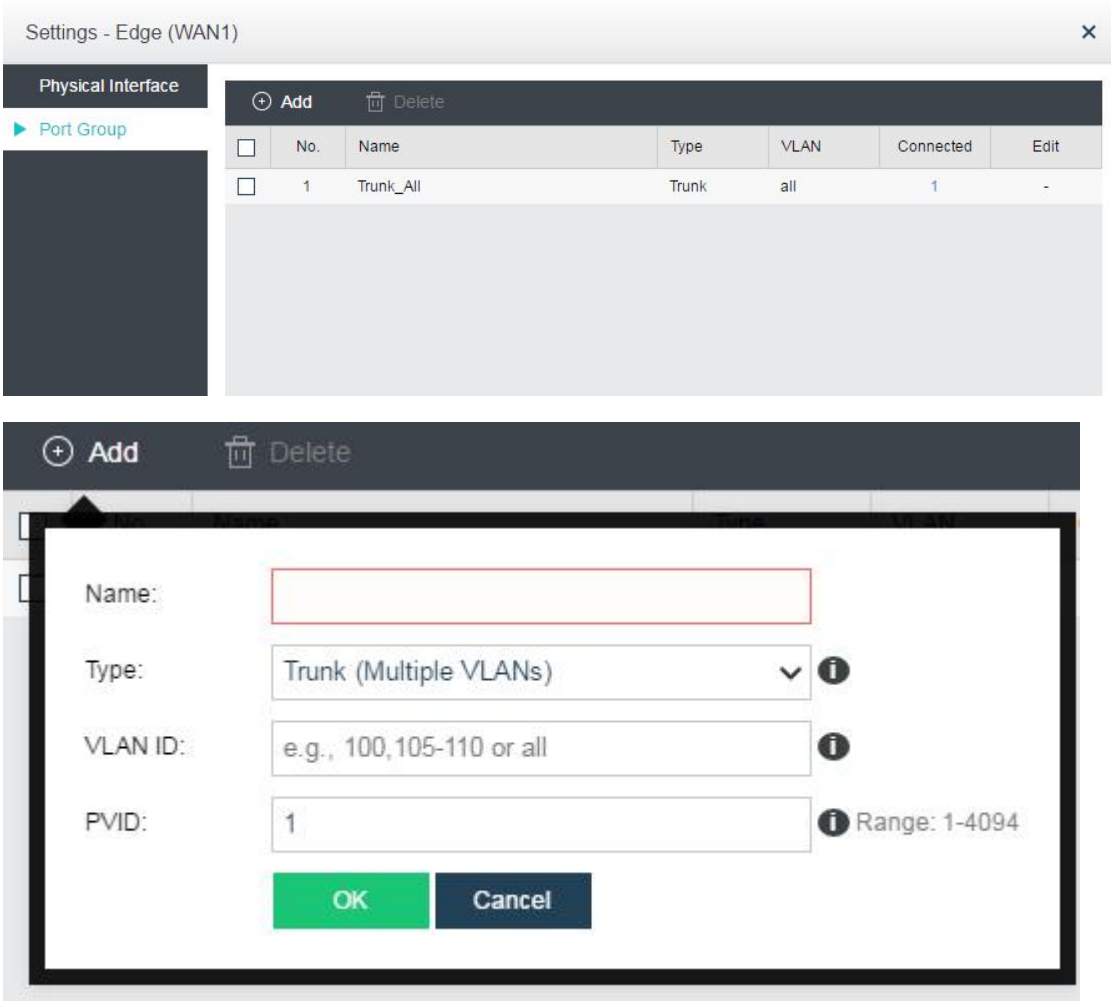




2. Configure physical interface. You can add a new or edit an existing physical interface on the following page:



3. Configure port group. You can perform the following operations on **Port Group** tab: **Add**, **Edit** and **Delete**. To add a new port group, click **Add** and configure related fields.



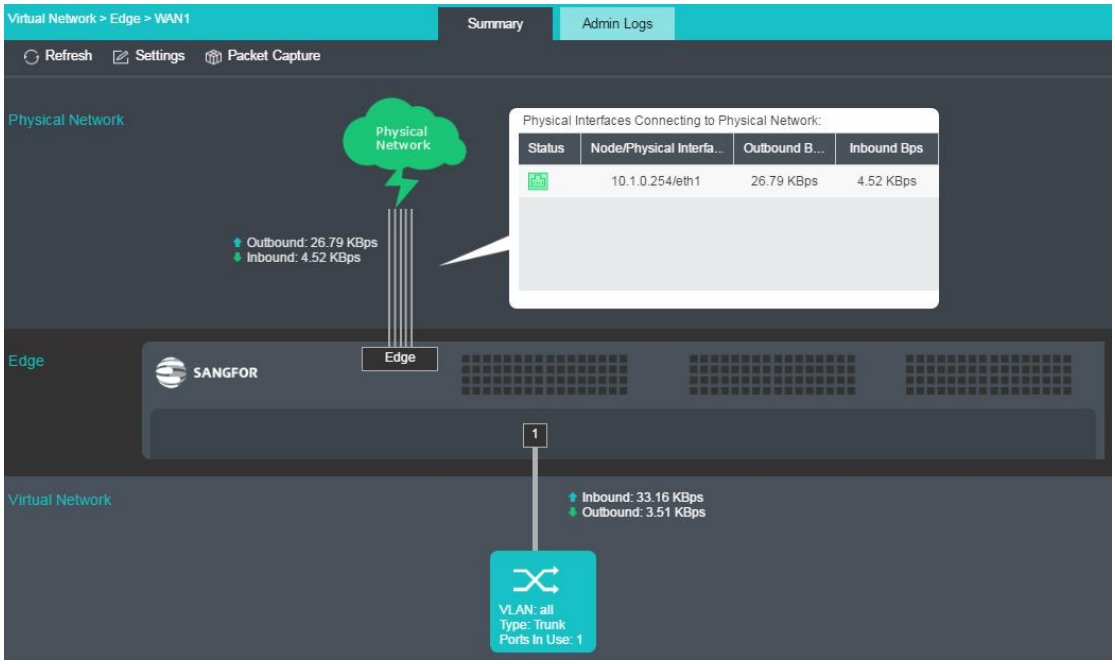
- **Name**: Specifies a distinguishable name for the port group.
- **Type**: Specifies the type of VLAN interface, **Trunk** or **Access**.

  Trunk port is used for VLAN trunking or VLAN aggregation. It allows packets which do not carry VLAN information, or packets which carry VLAN information and VLAN ID is within specific VLAN ID range. If the VLAN ID is not in the specific VLAN ID range, the packets will be rejected.

  Access port receives packets untagged with VLAN ID. It will tag the packets with specific VLAN IDs, which will be removed when the packets go out of that **Access** port.
- **VLAN ID**: It is required if type is **Trunk**.
- **PVID**: It is the default VLAN ID that will be tagged on packets going through the switch but carrying no VLAN ID.

Viewing Edge Summary

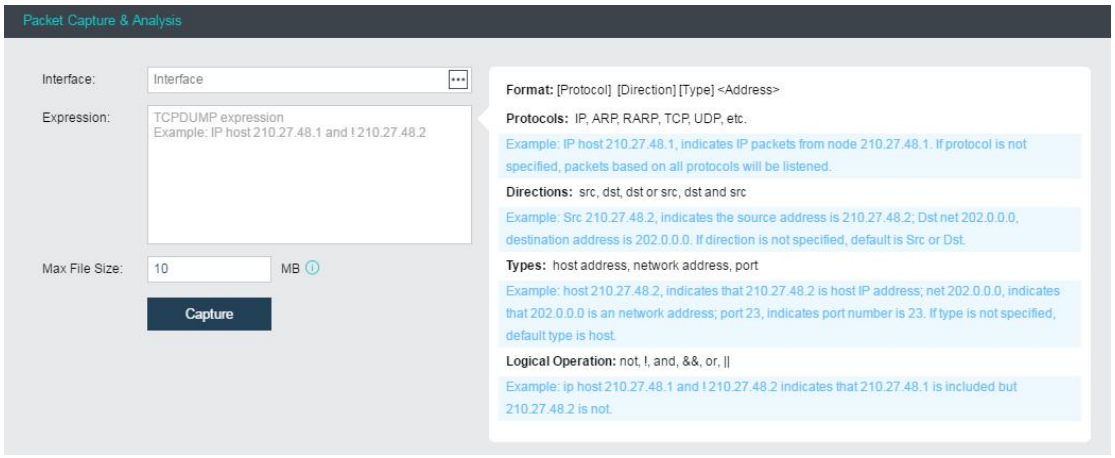
This section displays the basic information of the edge, and the outbound and inbound rate of the edge and port group.



To reload the current page, click **Refresh**.

To change edge settings, click **Settings**, and then configure physical interface and port group.

To capture and analyze packets, click **Packet Capture**, as shown below:

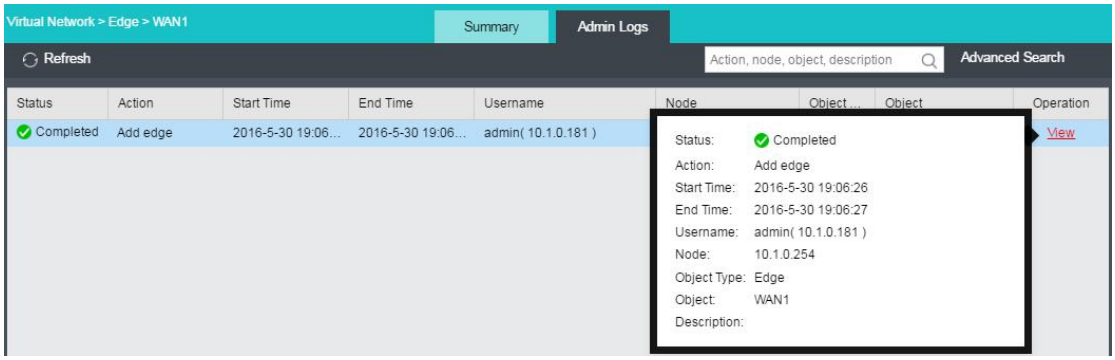


The following are contents on the above page:

- **Interface**: Specifies the interface. The packets passing through that interface will be captured.
- **Expression**: Specifies expression to filter packets. On the right panel of the **Packets Capture & Analysis** page, it displays the expression formats.
- **Max File Size**: Specifies the maximum size of the file. If a file size is larger than the maximum, capturing packet will stop.

Viewing Admin Logs

This section displays administrator logs, which record various operations performed by the administrator, such as creating edge. Each log contains the following information: **Status**, **Action**, **Start Time**, **End Time**, **Username**, **Node**, **Object Type**, **Object** and **Operation**.



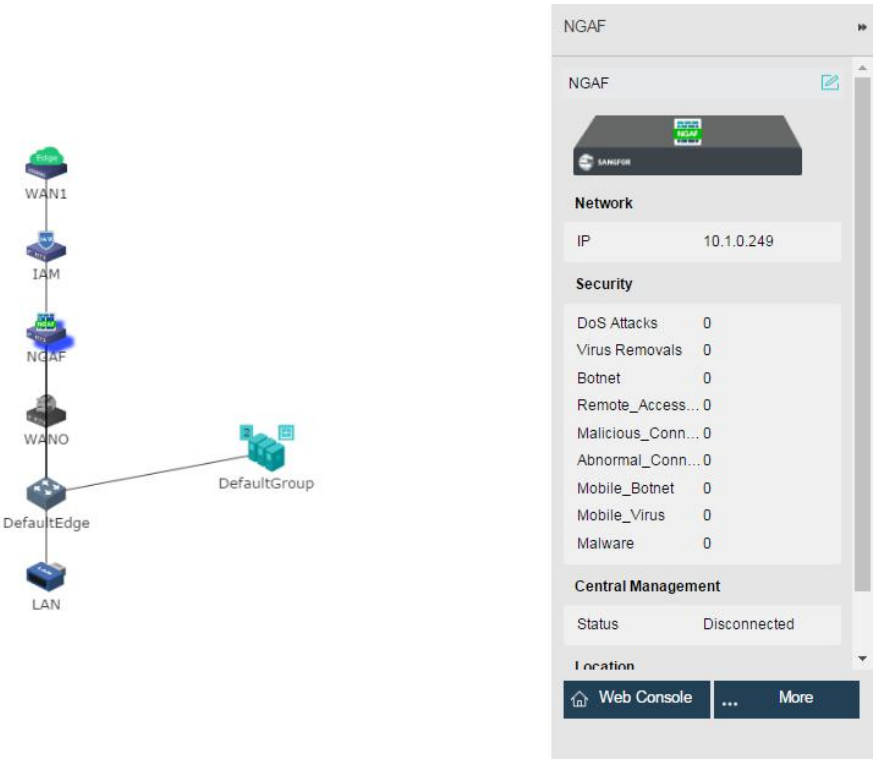
To view the details of each log, click **View** in **Operation** column.

Configuring Virtual Network Devices

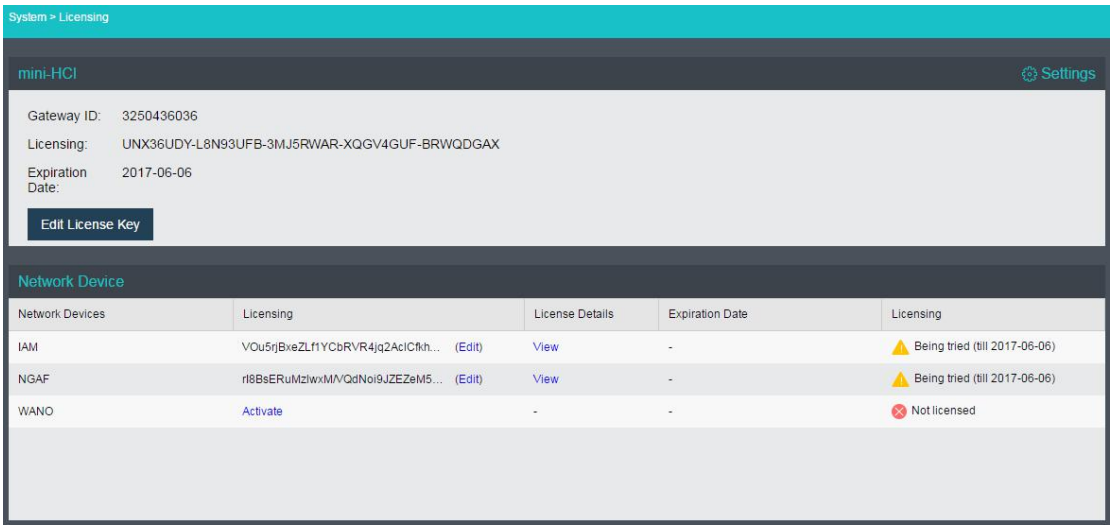
The following virtual network devices, IAM, NGAF, WANO, and SSL VPN, could be deployed into virtual network in **Networking** > **Map**.

Licensing Virtual Network Devices

To make a virtual network device available, you need to license that device first.



Click **License** and then you will be redirected to the following page:



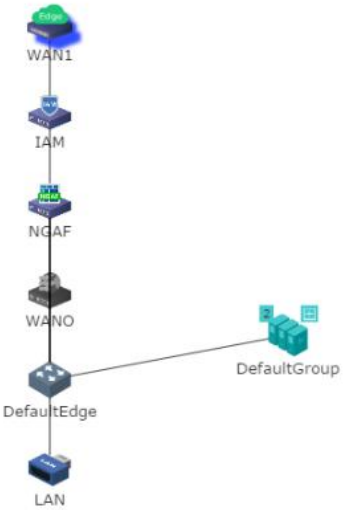
If the virtual network device is licensed, you will see the **Web Console** and **More** buttons on the right panel of the **Map** page in **Networking** when clicking on that device after it is automatically restarted.

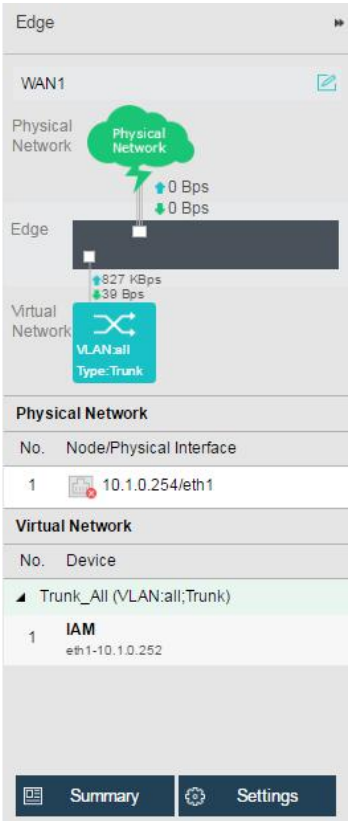
To perform more operations against the virtual network device, click **More** button, and select the operation, such as **Shut Down**, **Power Off**, **Backup** and **Recover**, etc.

To enter Web admin console of a virtual network device, click **Web Console**. The following page indicates that the administrator logs in to the web admin console successfully.

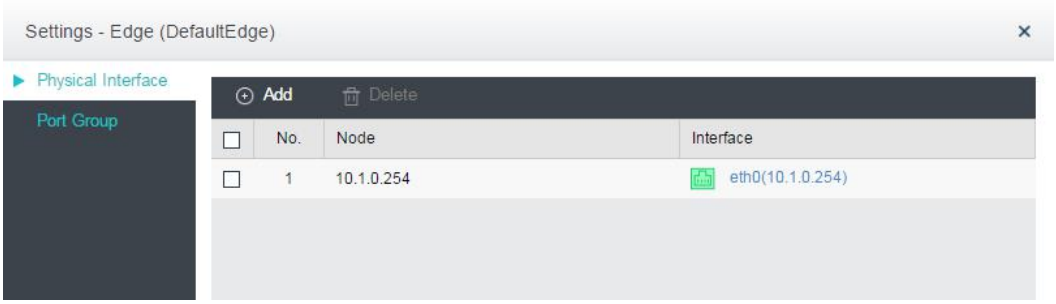
Configuring Virtual Switch

A virtual switch provides connection, access control list (ACL) and broadcast storm prevention.



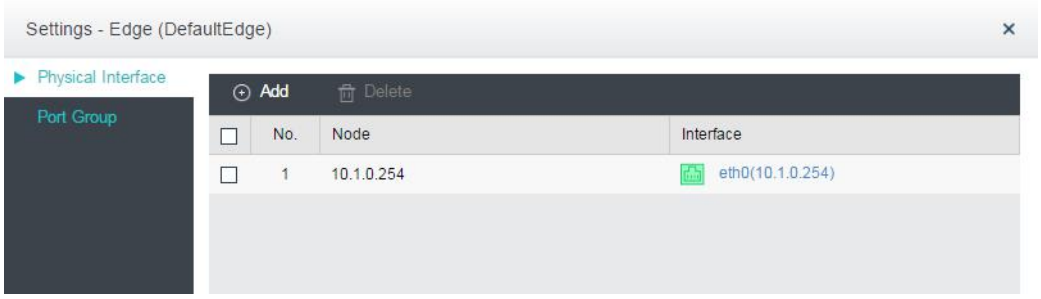


To configure a virtual switch, click **Settings** button and then configure physical interface and port group.



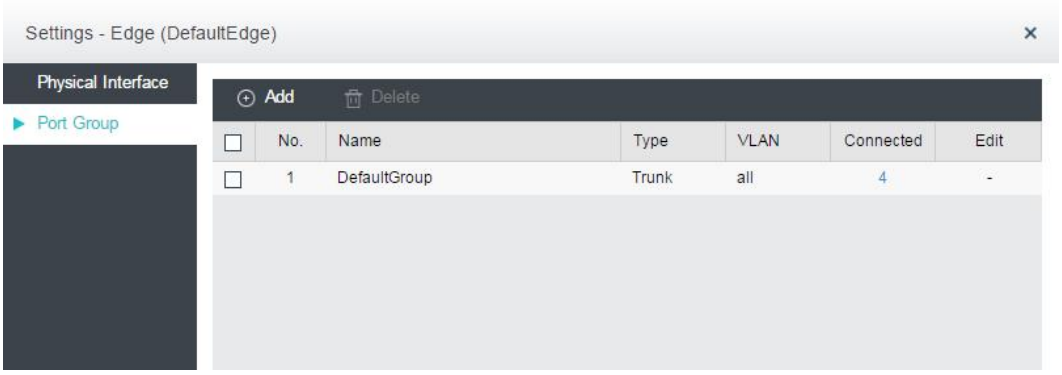
Configuring Physical Interface

You can add a new physical interface, delete and edit an existing physical interface on the following page:

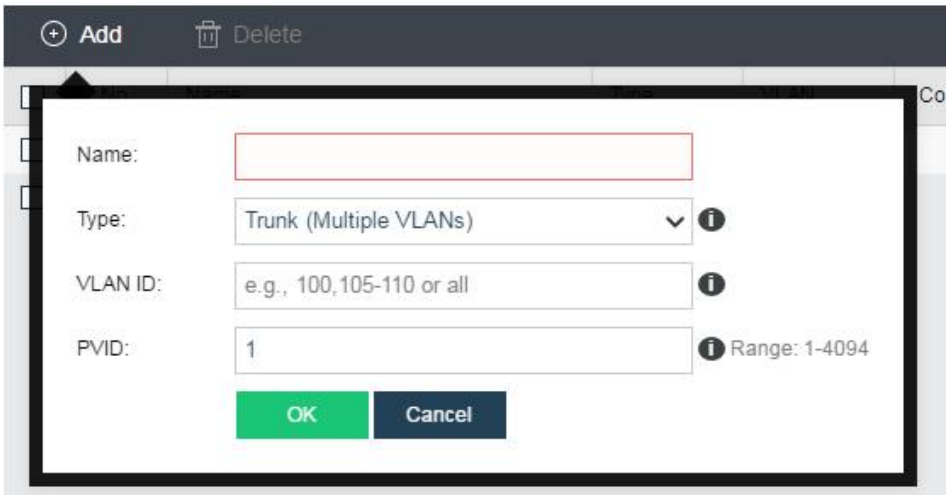


Configuring Port Group

You can perform the following operations on **Port Group** tab, add, edit and delete.



To add a new port group, click **Add** and configure the fields on the following page:



The following are contents included on the above page:

- **Name**: Specifies a distinguishable name for the port group.
- **Type**: Specifies type of VLAN interface, **Trunk** or **Access**.

  Trunk port is used for VLAN trunking or VLAN aggregation. It allows packets which do not carry VLAN information, or packets which carry VLAN information and VLAN ID is within specific VLAN ID range. If the VLAN ID is not in the specific VLAN ID range, the packets will be rejected.

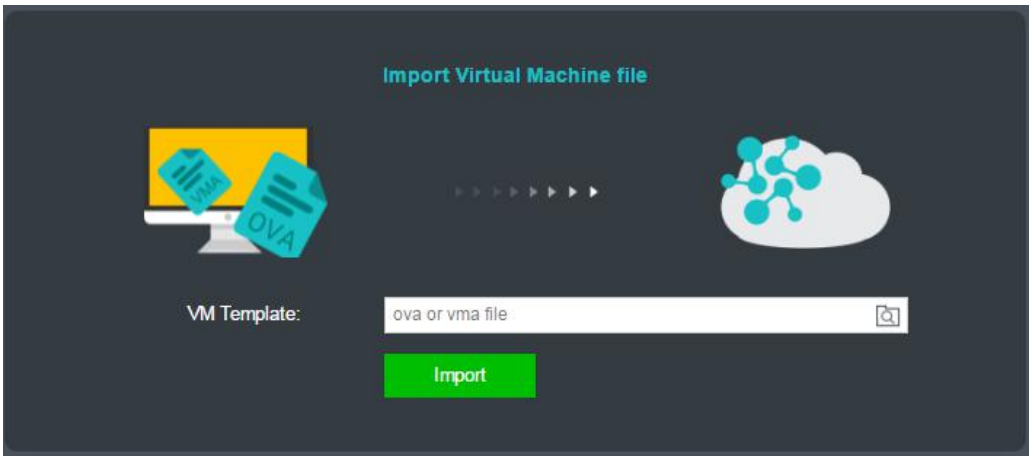
  Access port receives packets untagged with VLAN ID. It will tag the packets with specific VLAN IDs, which will be removed when the packets go out of that **Access** port.
- **VLAN ID**: It is required when type is **Trunk**.
- **PVID**: It is the default VLAN ID that will be tagged on data packets going through the switch but carrying no VLAN ID.

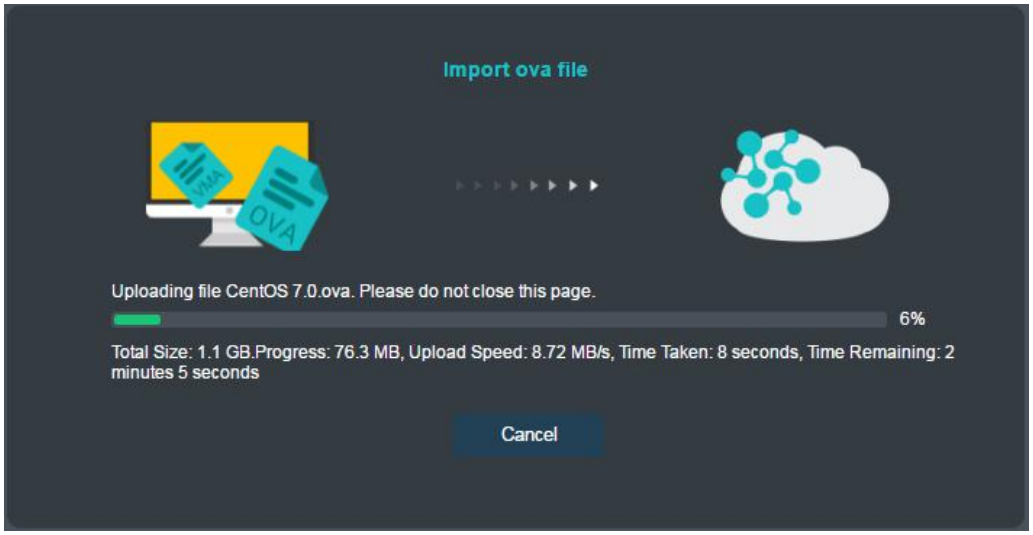
Adding Server

You can add a new server by importing a virtual machine or creating a new virtual machine.

Importing Virtual Machine

To import a virtual machine, click **Add Server** and choose **Import Virtual Machine** on **Create New Virtual Machine** page. Select an ova file from the local disk and then click **Import**.

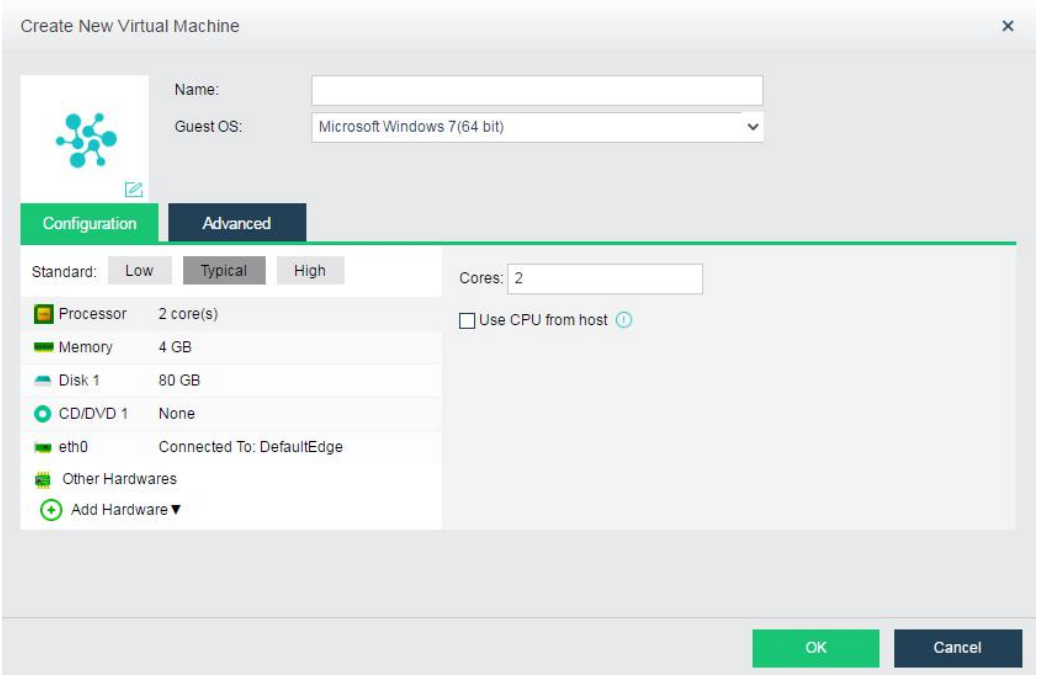




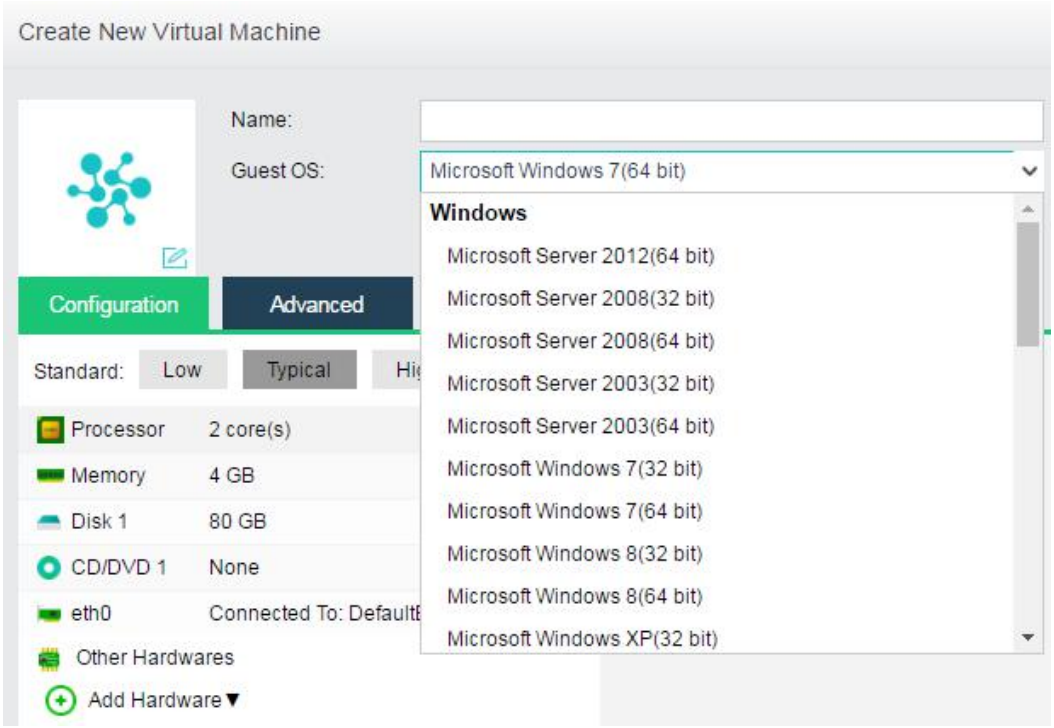
- **If an ova file of a Windows based virtual machine is imported, driver of the USB mouse needs to be updated and you will be prompted to install that driver.**
- **If an ova file of a Linux based virtual machine is imported, you need to configure IP address for NIC.**

Creating A New Virtual Machine

To create a new virtual machine, click **Add Server** and choose **Create New Virtual Machine.**



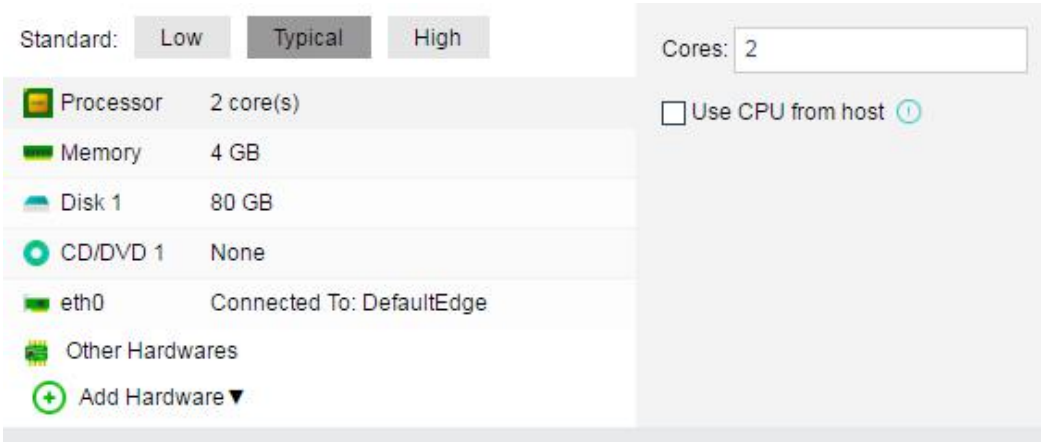
- **Name**: Specifies a distinguishable name for the virtual machine.
- **Guest OS**: Specifies an operating system for the virtual machine. The aBOS unit supports the following types of guest OSes: Windows, Linux, Sangfor and others. Sangfor based guest OS is used for aCenter.



- **Configuration**: It allows you to configure hardware resources, such as **Processor**, **Memory**, **Disk**, **CD/DVD** and **NIC**, etc.

  Configuration falls into **Low** configuration, **Typical** configuration and **High**

configuration. If the current configuration fails to meet business requirements, you can configure the corresponding hardware resource as required, as shown below:

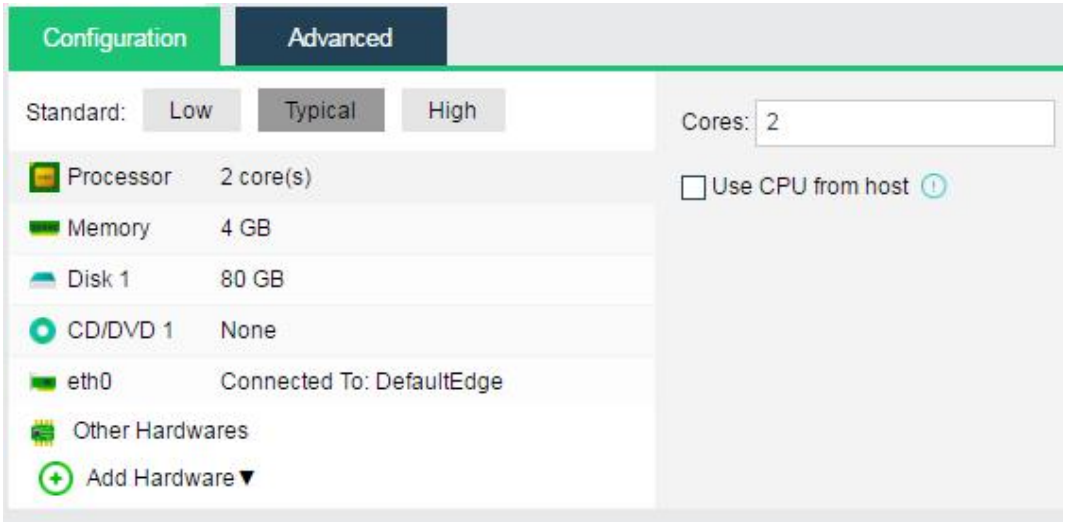


Default Low Configuration: Single-core processor, 2 GB memory, 40 GB disk, one CD/DVD, one NIC.

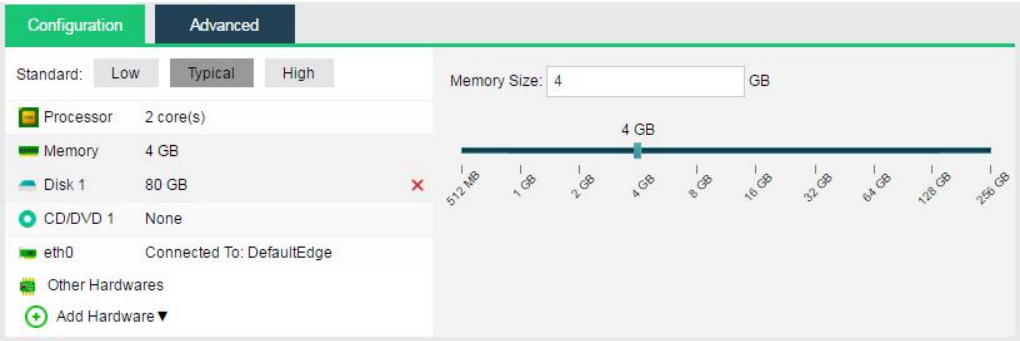
Default Typical Configuration: Dual-core processor, 4 GB memory, 80 GB disk, one CD/DVD, one NIC.

Default High Configuration: Quad-core processor, 8 GB memory, 80 GB disk, one CD/DVD, one NIC.

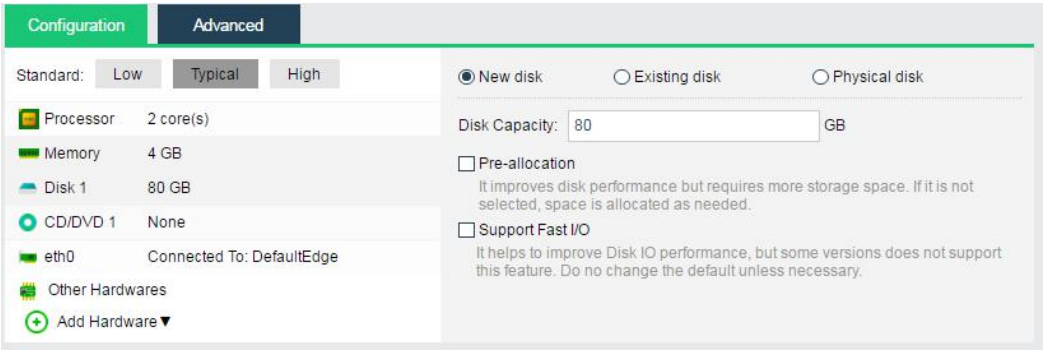
- **Processor**: Specifies the number of cores of each processor for the virtual machine.



- **Memory**: Specifies the memory size for the virtual machine. The minimum is 512 MB, and the maximum is 256 GB.



Disk: Specifies the disk for the virtual machine. **Note**: In later versions, to specify a disk for a virtual machine that is not stored on local storage, make sure the disk is on a NFS, iSCSI or FC storage that the virtual machine has access to.



A disk can be created by the three means: using a new disk, using an existing disk, using physical disk.

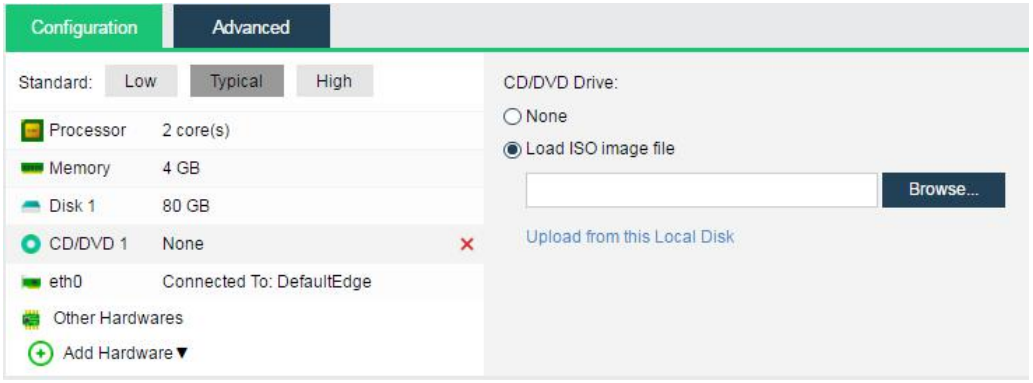
To use a new disk, select the option **New Disk** and configure the following fields:

- **Disk Capacity**: Specifies the capacity of the virtual disk, in GB.
- **Pre-allocation**: It improves disk performance but requires more storage space. If it is not selected, space is allocated as needed.

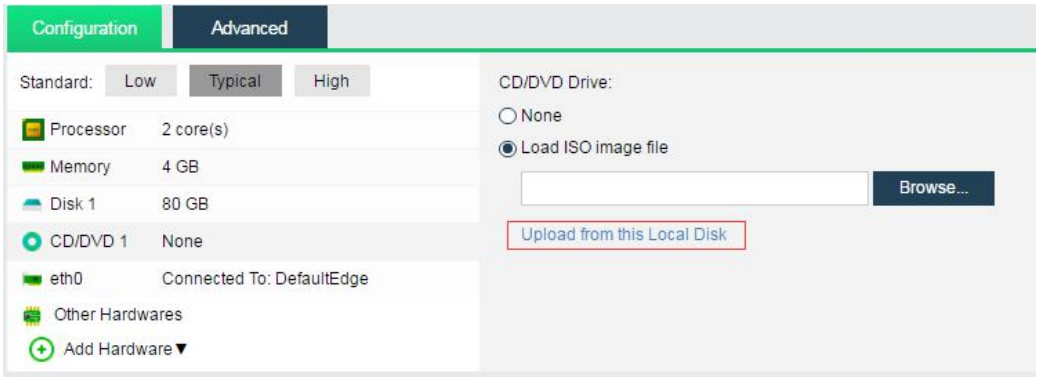
To use an existing disk, select the option **Existing Disk** and then select a qcow2 disk file.

To delete the source disk file and create a new disk file, select the option **Delete source disk files**.

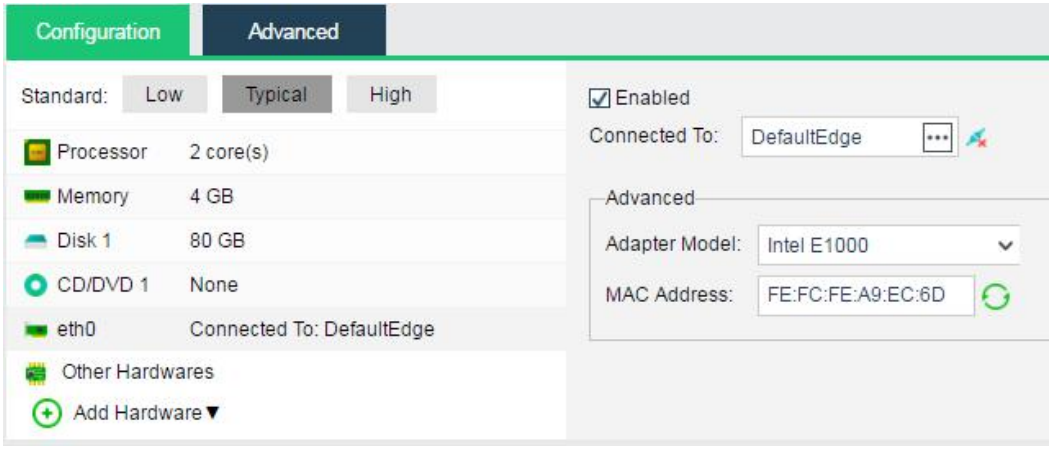
- **CD/DVD 1**: Specifies an ISO image file of CD/DVD drive to be used by the virtual machine. It can also be **None**, which indicates that the virtual machine does not use CD/DVD drive.



If the option **Load ISO image file** is selected, you need to select the corresponding ISO image file. If there is no ISO image file, you can upload it to the datastore from the local disk. Click **Upload from this Local Disk**, select the ISO image file and upload it.



- **Enabled**: Select this option to enable the eth0 interface.



- **eth0**: Specifies what the virtual machine is connected to.

- **Connected To**: Specifies the edge or a virtual switch to be connected to the virtual machine.
- **Adapter Model**: Specifies the adapter model, **Realtek RTL8139**, **Intel E1000** or **VirtIO**. If **VirtIO** is selected, you need to install the corresponding driver.
- **MAC Address**: It can be automatically generated or manually specified. MAC address examples: 00-11-22-33-44-55, 00:11:22:33:44:55.

To add more hardwares, click **Add Hardware**. Then, you can add disk, CD/DVD, serial port and NIC as per your need.

For example, click **Add Hardware** and select **Disk**. Then, disk 2 will be added to the configuration (as shown in following figure). You can add this disk by creating a new disk or using an existing disk. To delete a disk, click this  icon.

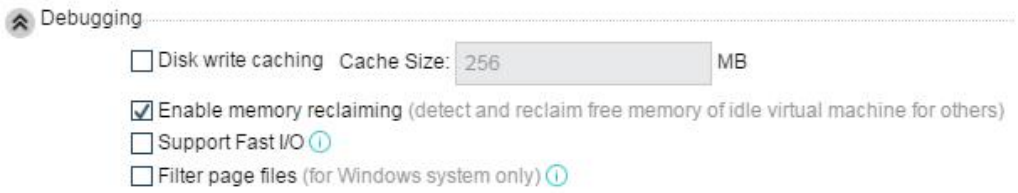
On **Advanced** tab, you can configure more options, such as **Boot Order**, **Others** and **Debugging**.

- **Boot Order**: Specifies the boot order for the virtual machine. You can choose an item (disk or CD/DVD) from the pull-down list.

- **Others**: Lists the following options:

- **Power on at node startup:** If it is selected, the virtual machine can automatically start up at node startup;
- **High priority:** If it is selected, resources will be allocated to the virtual machine preferentially in case that resources on the node are insufficient;
- **Reboot if fault occurs:** If it is selected, the virtual machine will reboot automatically when it is not responding due to stuck, blue screen, etc.

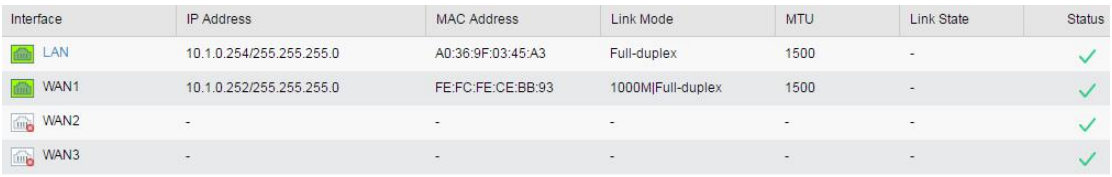
- **Debugging**: There are the following options:
  - **Disk write caching**: It can improve disk IO efficiency, because files in virtual disk are loaded to memory.
  - **Enable memory reclaiming**: Select this option to detect and reclaim free memory of idle virtual machine for others.
  - **Support Fast I/O**: Select this option to improve I/O performance.



Configuring Network Interfaces

Configure interfaces on the **Interfaces** tab in **Networking**, in Route mode and Bridge mode.

The following are on the **Interfaces** page:



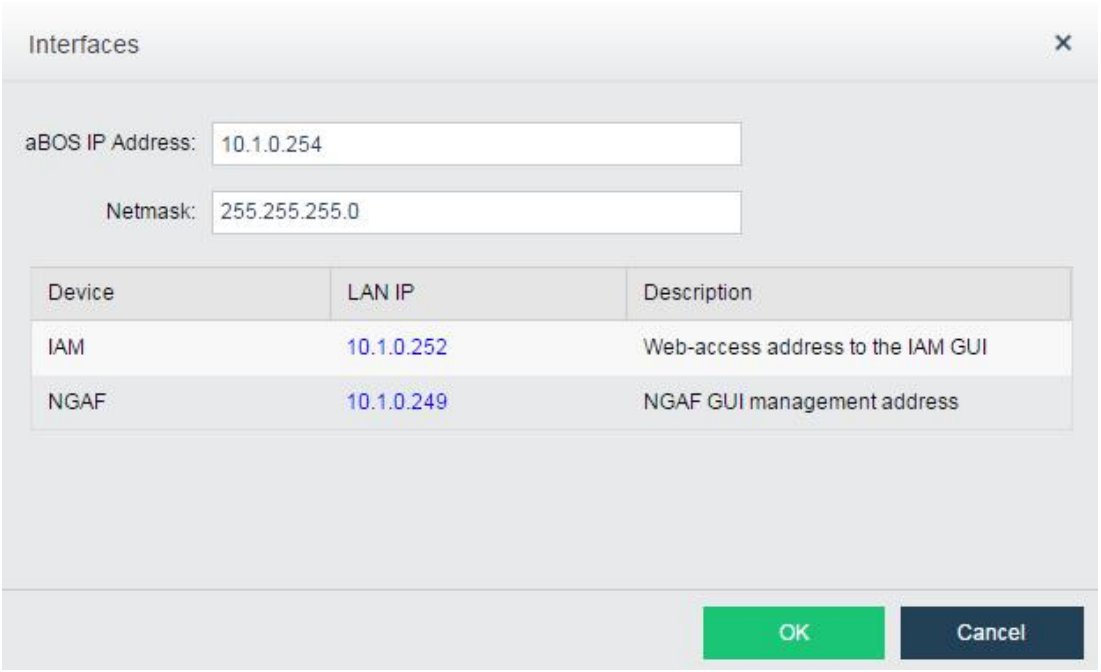
Interface	IP Address	MAC Address	Link Mode	MTU	Link State	Status
LAN	10.1.0.254/255.255.255.0	A0:36:9F:03:45:A3	Full-duplex	1500	-	✓
WAN1	10.1.0.252/255.255.255.0	FE:FC:FE:CE:BB:93	1000M|Full-duplex	1500	-	✓
WAN2	-	-	-	-	-	✓
WAN3	-	-	-	-	-	✓

The following are contents included on the above page:

- **Interface**: Indicates the status of the corresponding physical network interface. The  icon shows that the interface is connected. The  icon shows that it is disconnected.
- **IP Address**: Displays IP address of the interface.

- **MAC Address**: Displays MAC address of the interface.
- **Link Mode**: Displays mode of the interface.
- **MTU**: Displays MTU value of the interface.

To configure an interface, select the interface first. For example, click **LAN** and configure it on the page that pops up, as shown below:

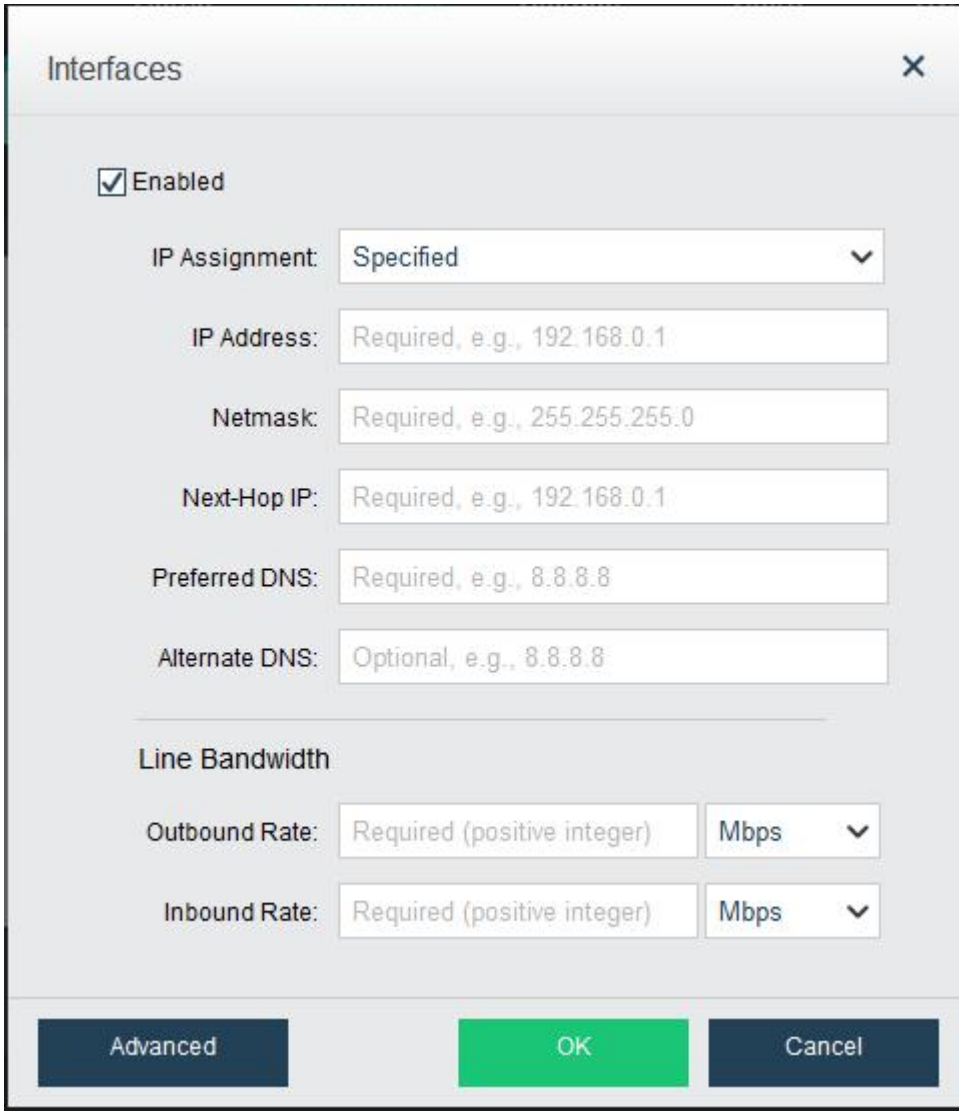


The following are contents included on the above page:

- **aBOS IP Address**: Specifies IP address for LAN interface.
- **Netmask**: Specifies netmask for LAN interface.

  Once aBOS IP address and netmask are specified, LAN IP addresses will be automatically generated for virtual network devices. If the auto-generated IP address conflicts with a local IP address, click that IP address in **LAN IP** column to change it.

  To configure the WAN1 network interface, click on the WAN1 name and enter the following page, as shown below:

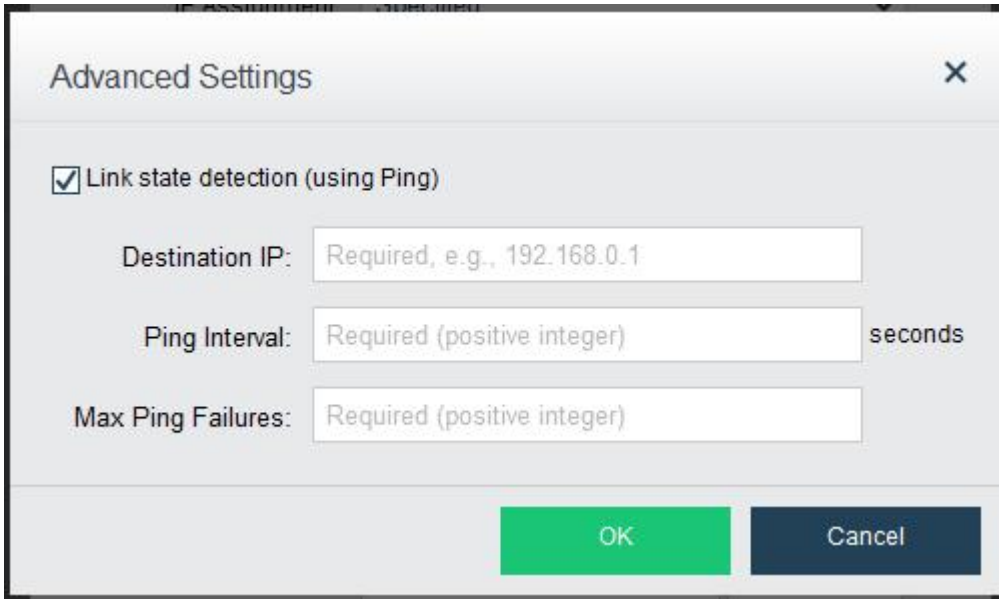


The following are contents included on the above page:

- **IP Assignment**: Options are **Using PPPoE**, **Using DHCP** and **Specified**.
- **IP Address**: Specifies IP address.
- **Netmask**: Specifies netmask.
- **Next-Hop IP**: Specifies IP address of the next-hop gateway.
- **Preferred DNS**: Specifies preferred DNS.
- **Alternate DNS**: Specifies alternate DNS.
- **Line Bandwidth**: Specifies outbound rate and inbound rate of the current line.

Configuring Advanced Settings

To enable and configure **Link state detection(using Ping)**, click **Advanced**. The **Advanced settings** are shown below:

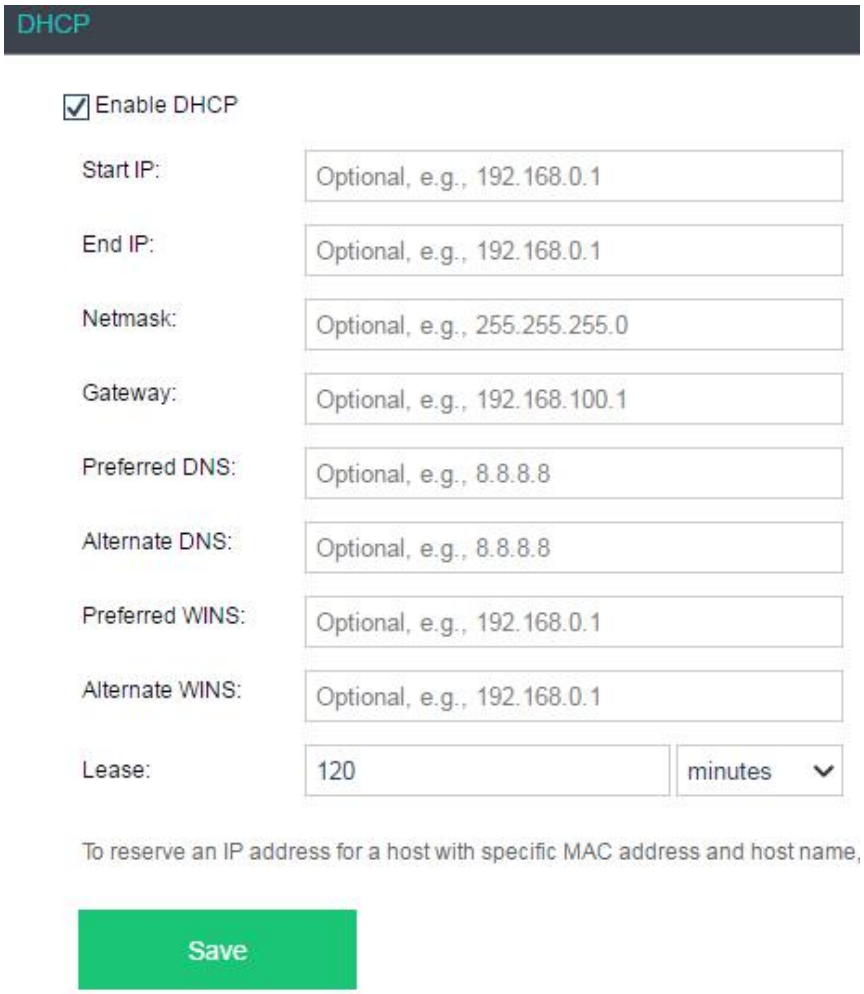


The following are contents included on the above page:

- **Link state detection (using Ping)**: Select the box next to this option to enable it.
- **Destination IP**: Specifies a destination IP address for link state detection.
- **Ping Interval**: Specifies detection interval, in seconds.
- **Max Ping Failures**: Specifies maximum number of detection failures. For example, if this field is **2** and destination IP address cannot be reached within N seconds twice, then the link is thought not working properly.

Configuring DHCP

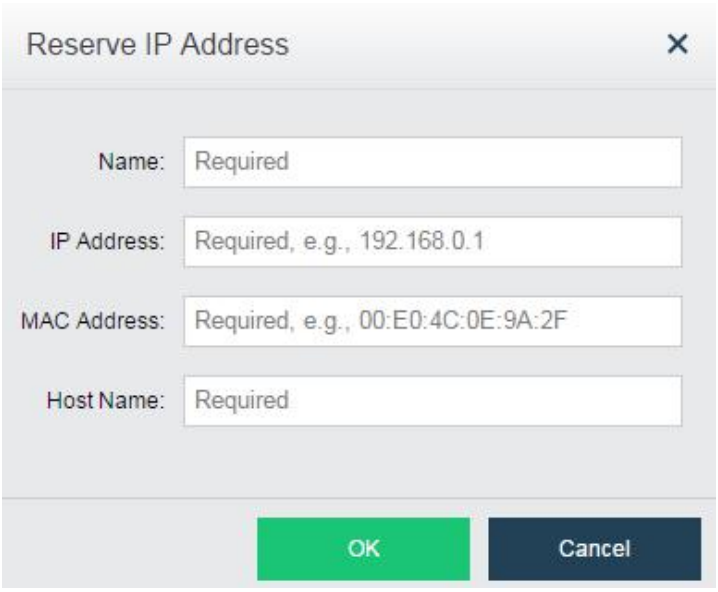
DHCP automatically allocates IP addresses to internal computers, but DHCP settings are only available when this aBOS unit functions as a gateway device. It can be configured as shown below:



To use DHCP service, enable DHCP and configure the required fields like **Start IP**, **End IP**, **Netmask**, **Gateway**, **Preferred DNS**, **Alternate DNS**, **Preferred WINS**, **Alternate WINS**, and **Lease**.

Assigning Reserved IP Addresses

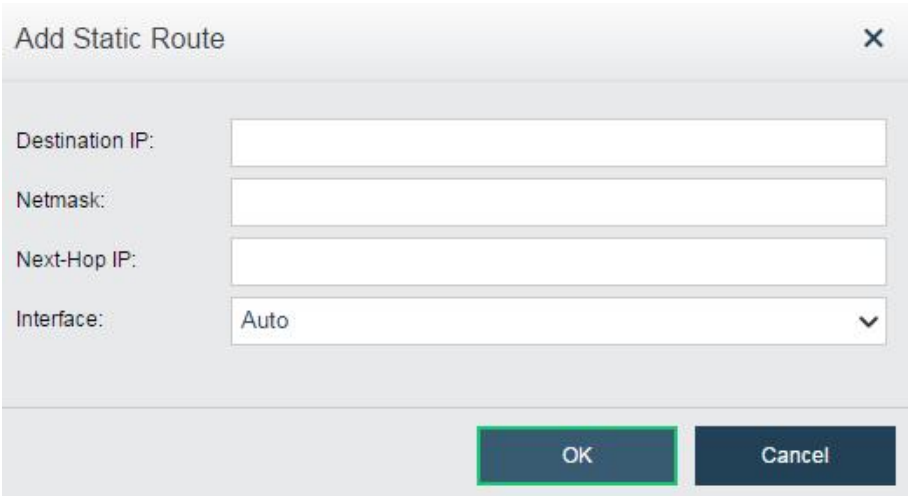
To assign an IP address that is exclusively reserved for one specific internal computer, click **Reserved IP Addresses**, and specify **Name**, **IP Address**, **MAC Address** and **Host Name**.



Configuring Static Route

If the aBOS unit is to communicate with IP addresses on different network segments, static route helps. Add static route one by one or add multiple static routes at a time.

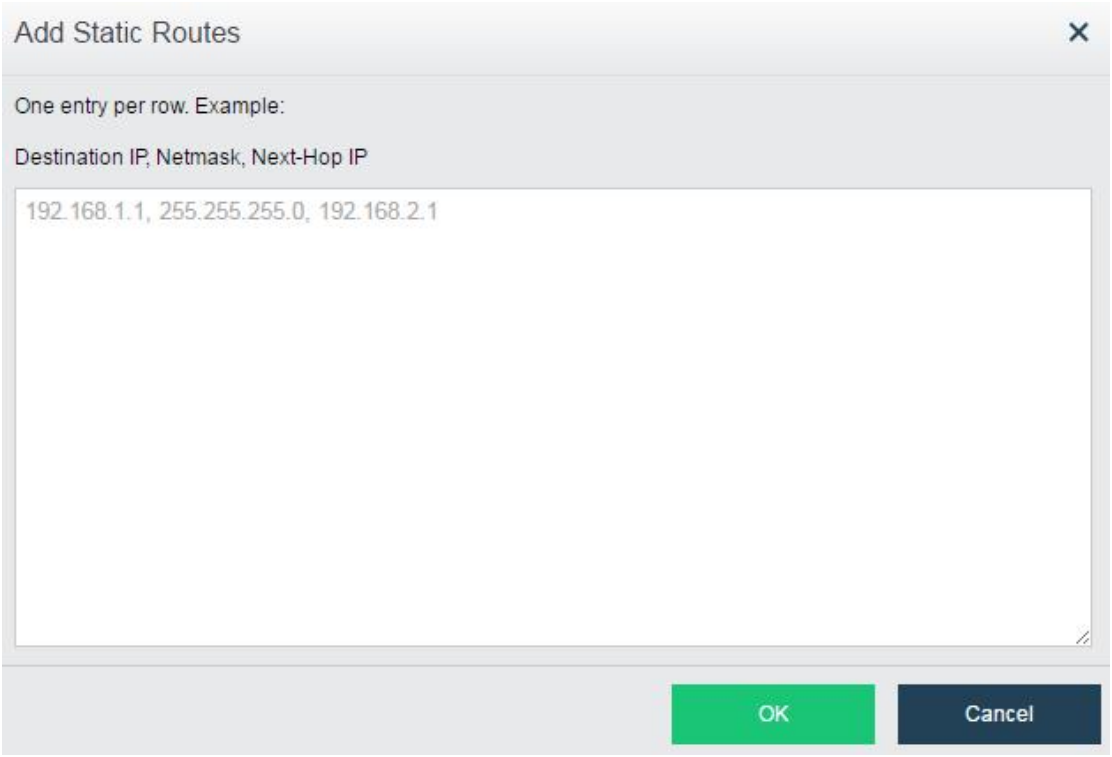
To configure a static route, click **Add** and the **Add Static Route** page pops up, as shown below:



The contents on **Add Static Route page** are described as follows:

- **Destination IP**: Specifies destination IP address.
- **Netmask**: Specifies netmask.
- **Next-Hop IP**: Specifies next-hop IP address.
- **Interface**: Specifies the interface through which data is forwarded.

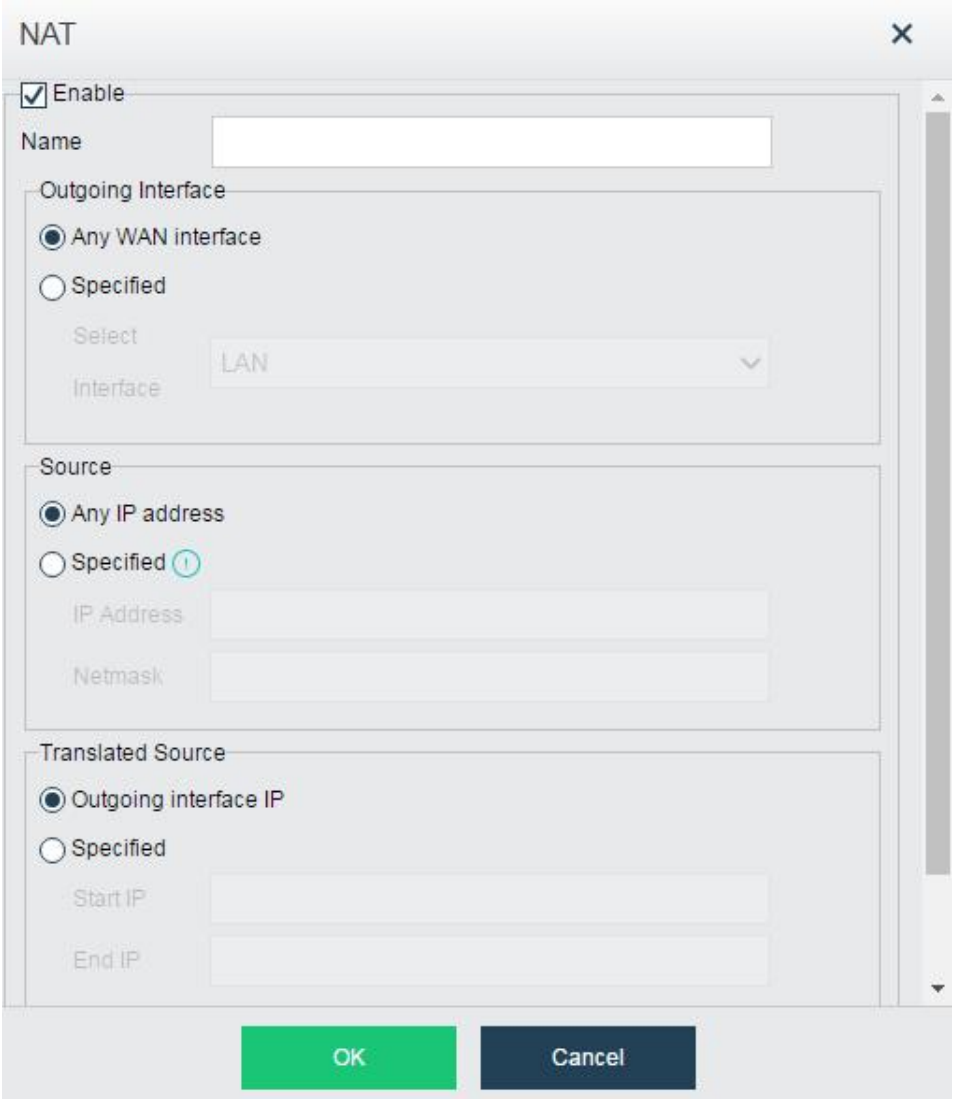
To configure multiple static routes at a time, click **Add Multiple**, and configure on the **Add Static Routes** page that pops up, as shown below:



Enter one entry per row. Example: **Destination IP**, **Netmask**, **Next-Hop IP**.

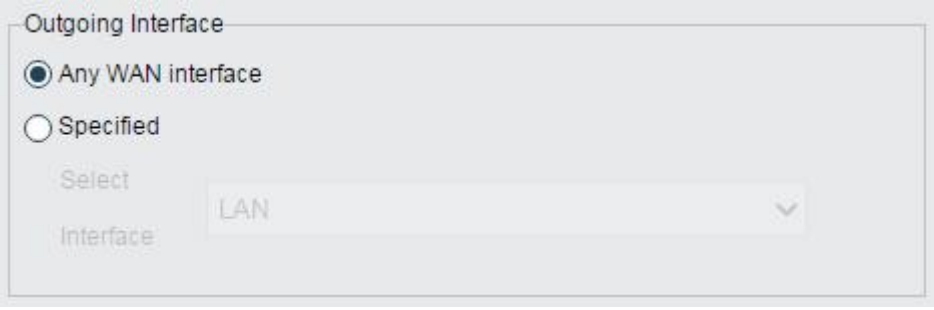
Configuring NAT Rules

To translate source IP addresses, click **Add** on **NAT** tab in **Networking**, and configure an NAT rule on **NAT** page that pops up, as shown below:

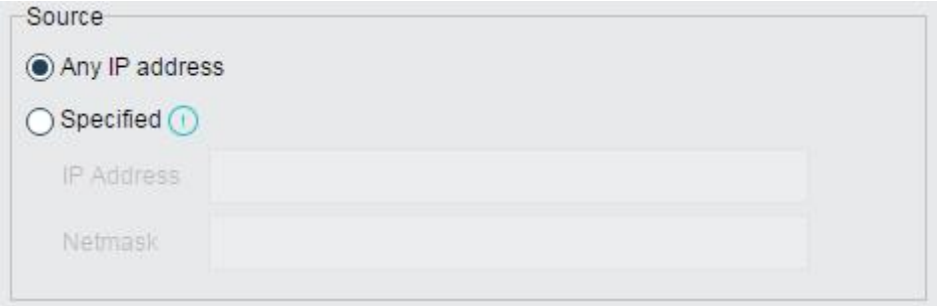


First, select **Enable**, then move on to the configure the following:

- **Outgoing Interface**: Specifies outgoing interface through which data is forwarded. Options are **Any WAN interface** and **Specified**. To forward data to a specific interface, select **Specified**. To forward data through any of the two WAN interfaces, select **Any WAN interface**, as shown below:

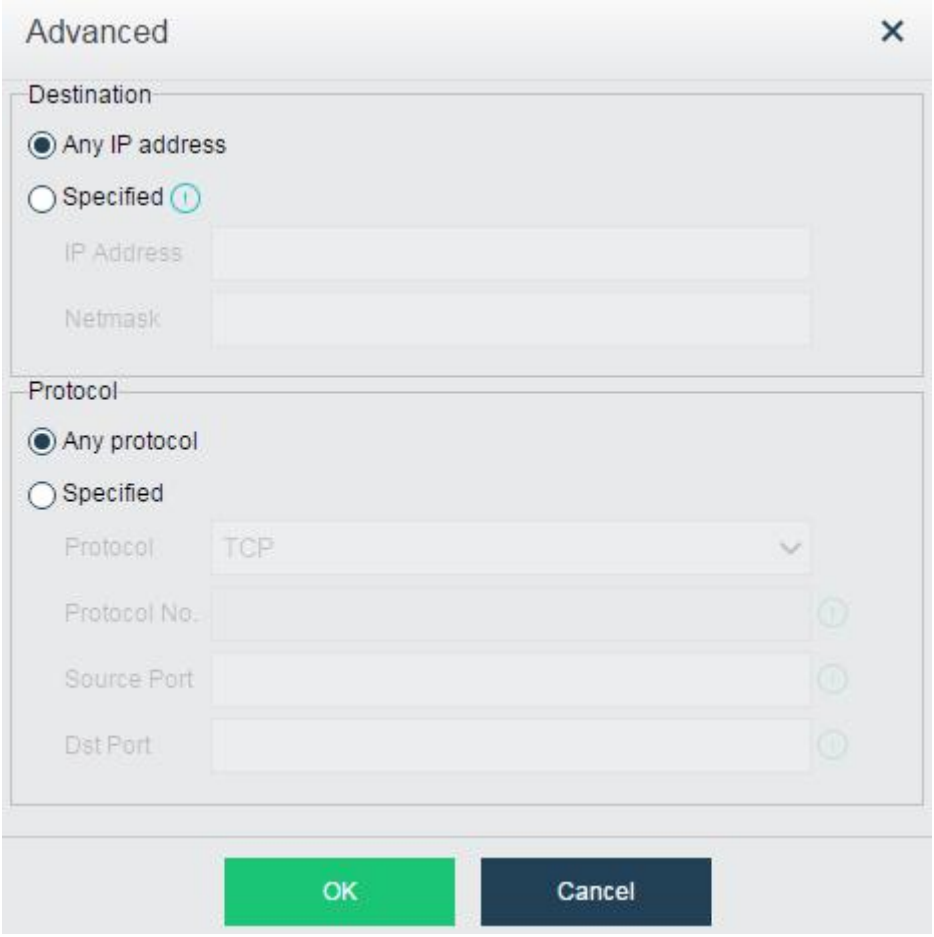


- **Source**: Specifies source IP addresses to be translated. Options are **Any IP address** and **Specified**. If **Any IP address** is selected, all the IP addresses can be translated. If **Specified** is selected, only source IP addresses which are within the specified IP address range will be translated.



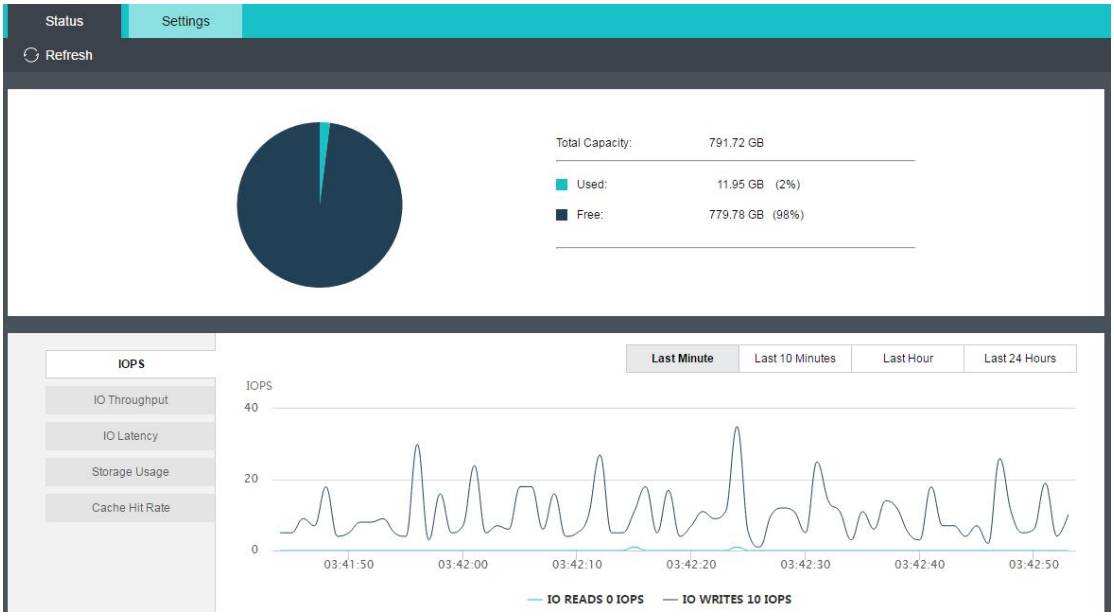
- **Translated Source**: Specifies translated IP addresses. If **Outgoing interface IP** is selected, source IP address will be translated to IP address of outgoing interface. If **Specified** is selected, IP addresses will be translated according to what has been specified.

- **Advanced**: Specifies destination IP addresses and protocol criteria. For example, when destination IP address is within the specified IP address range or when specified protocols are used, IP addresses will be translated, as shown below:



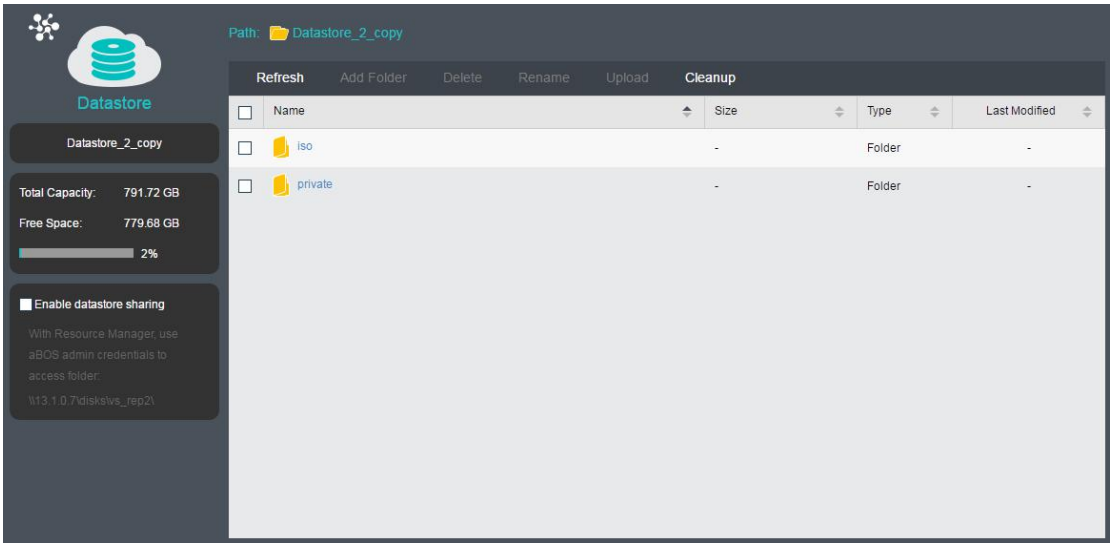
Configuring Storage

In **Storage** > **Status**, view the current status of storage and basic information, and configure storage in **Settings**. There are two kinds of status, online and offline. Value for offline storage is 0.

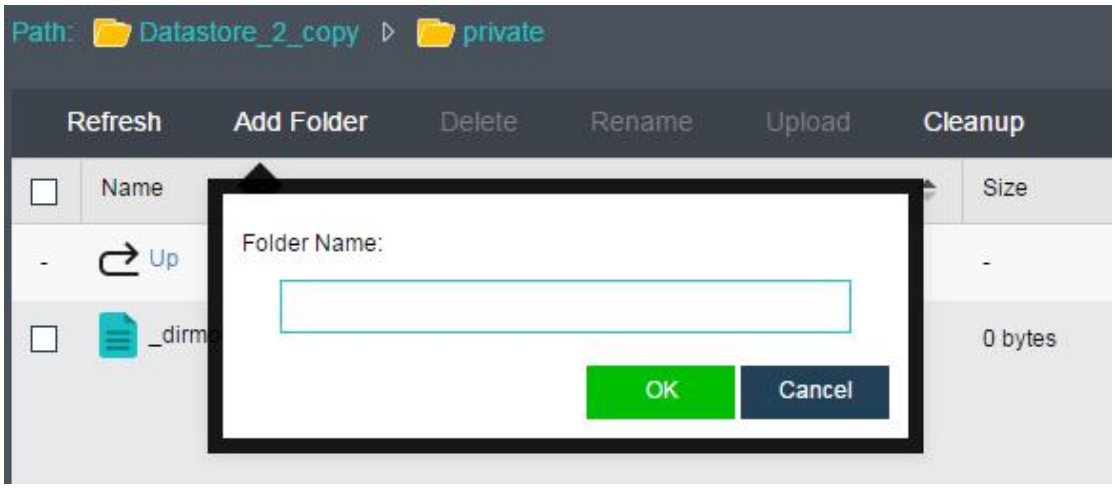


Managing Datastore

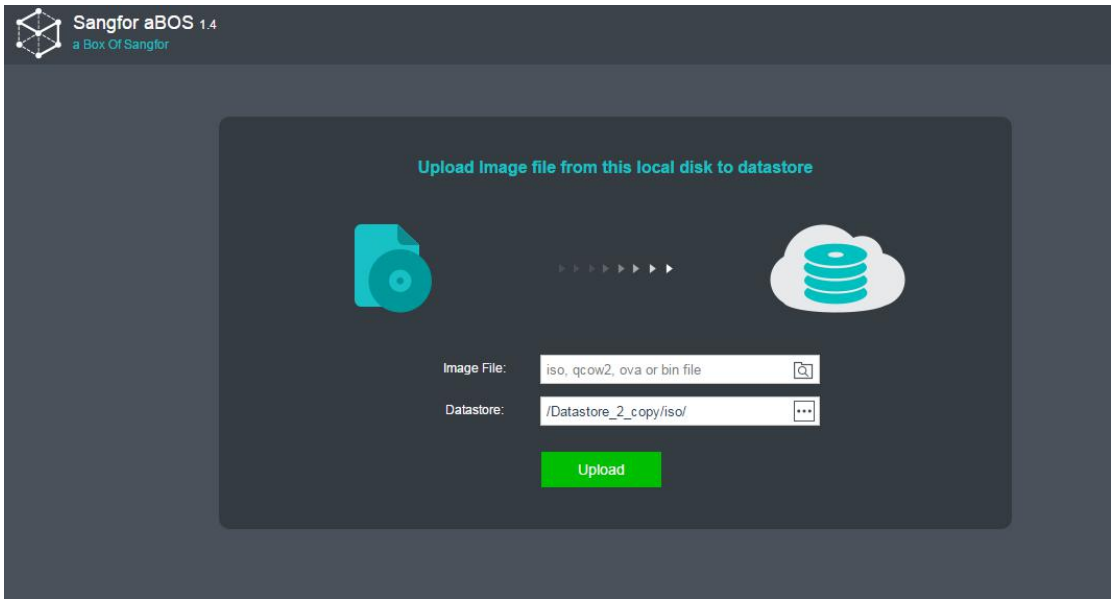
To manage datastore, click **Manage** on **Settings** tab and enter the following page. There are more operations available on the following page, such as **Refresh**, **Add Folder**, **Delete**, **Rename**, **Upload**, and **Cleanup**.



- **Add Folder**: Create a new folder under the current directory.



- **Delete**: Delete selected files or folders.
- **Rename**: Rename selected files or folders.
- **Upload**: Upload files to the current directory. For example, upload an ISO image file to the ISO folder for the purpose of creating virtual machines later, as shown below:

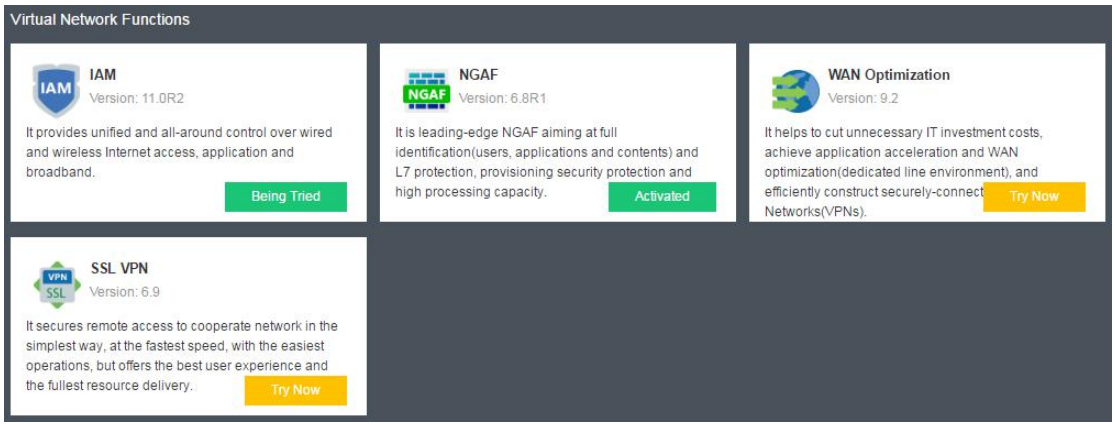


- **Enable datastore sharing:** To enable access to and management of these folders(\\ip\disks\vs_rep2\) through **Resource Manager** using aBOS admin credentials, select the option.

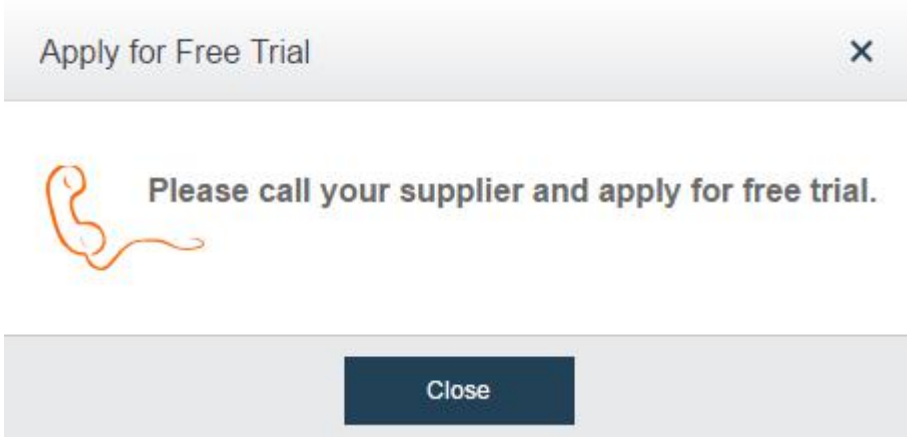
Trying VNFs in Store

In **Store**, customer can know what network functions are available on aBOS and choose to try any of them. Once a network function is tried, the status will be changed from **Try Now** to **Being Tried**. After one month trial, the status will be

turned from **Being Tried** to **Trial Expired**. For an activated network function, the status will be changed to **Activated**.



To apply for free trial, click **Try Now** to get in contact with supplier.

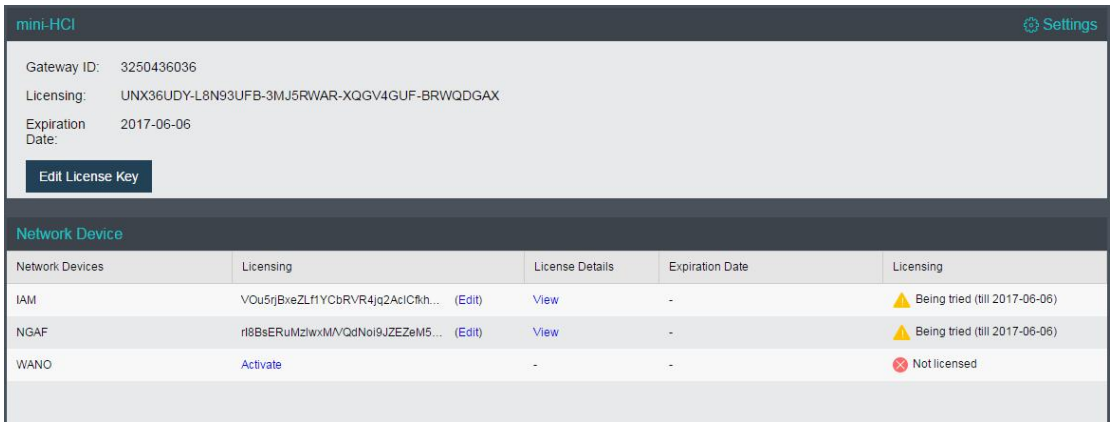


System Settings

In **System**, there are the following items: **Licensing**, **Date and Time**, **Administrators**, **Alarm Options**, **Logs and Alarms**, **VM Backup and Recovery**, **System Backup and Restore**, **Upgrade**, **Cluster**, **Service & Tech Support**, **Recycle Bin**, as shown below:

Licensing

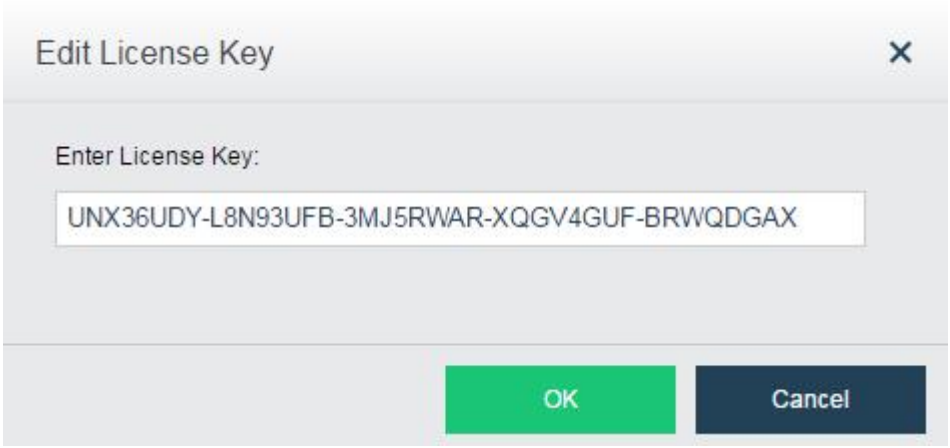
Click **Licensing** in **System**, to view license key of this aBOS unit and other virtual network devices. You may view the licensed features by clicking **View**, as shown below:



aBOS Basic License

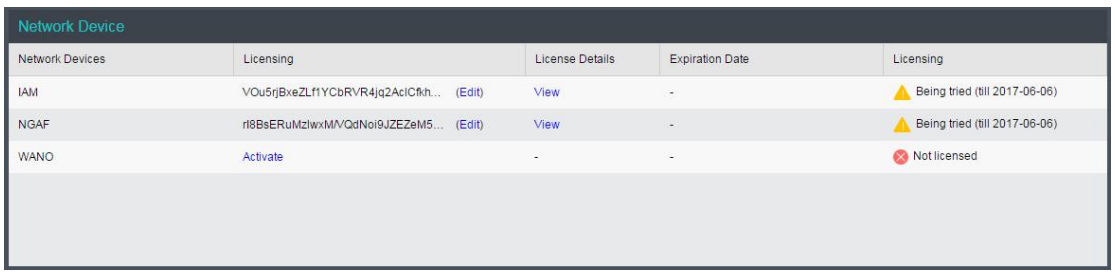
It displays **Gateway ID**, **License Key** and **Expiration Date** of this aBOS unit, as shown below:

To change the license key, click **Edit License Key**, and enter a new license key in **Enter License Key** field, as shown below:

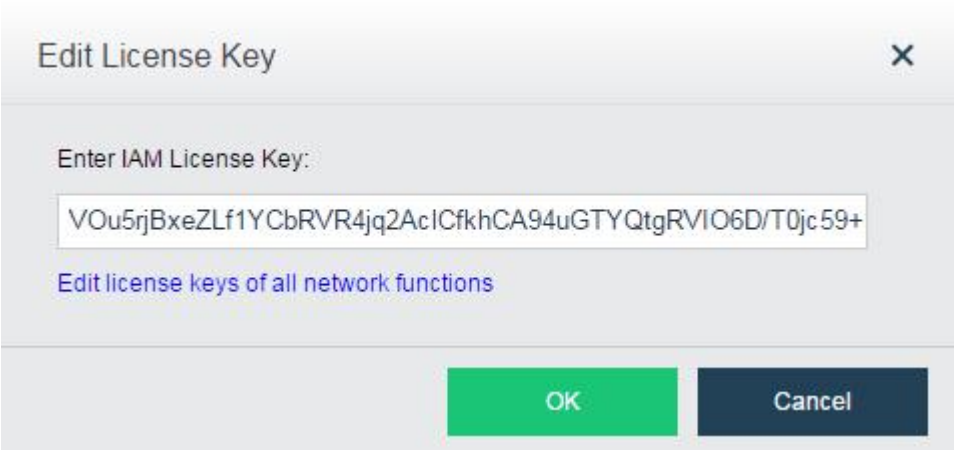


Virtual Network Function License

It displays **Network Devices**, **License Key**, **License Details**, **Expiration Date**, etc, as shown below:

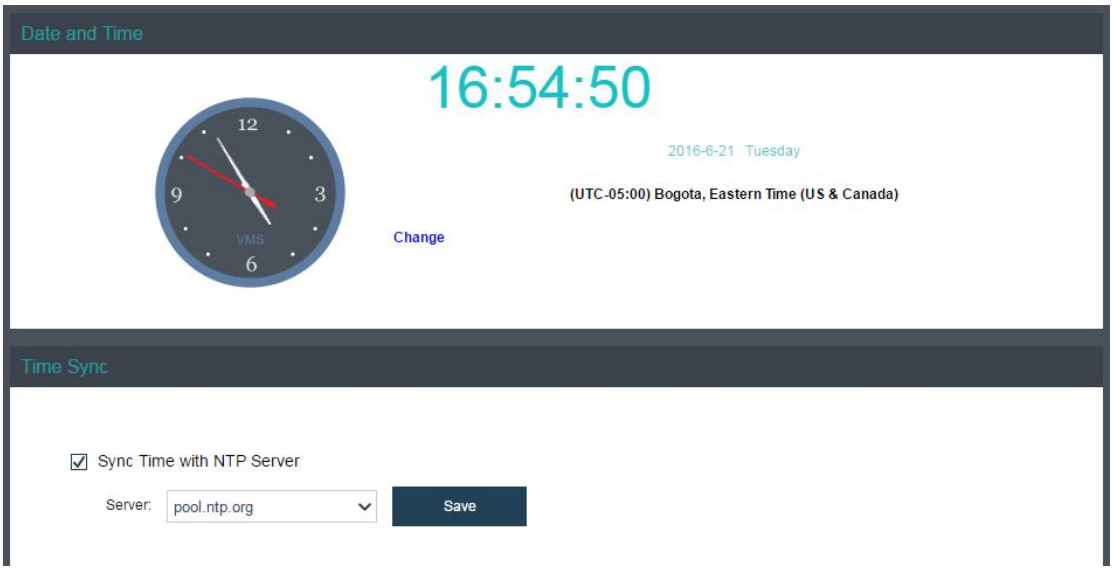


To activate the network device, click **Activate** and enter a license key for the selected network device on the **Edit license Key** page that pops up, as shown below:



Changing Date and Time

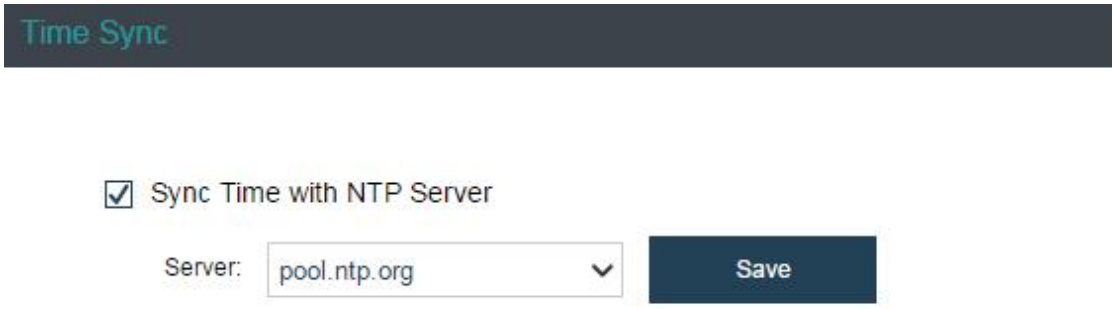
You may change date and time on this aBOS unit and also sync its time with that of NTP server on **Date and Time** tab in **System**, as shown below:



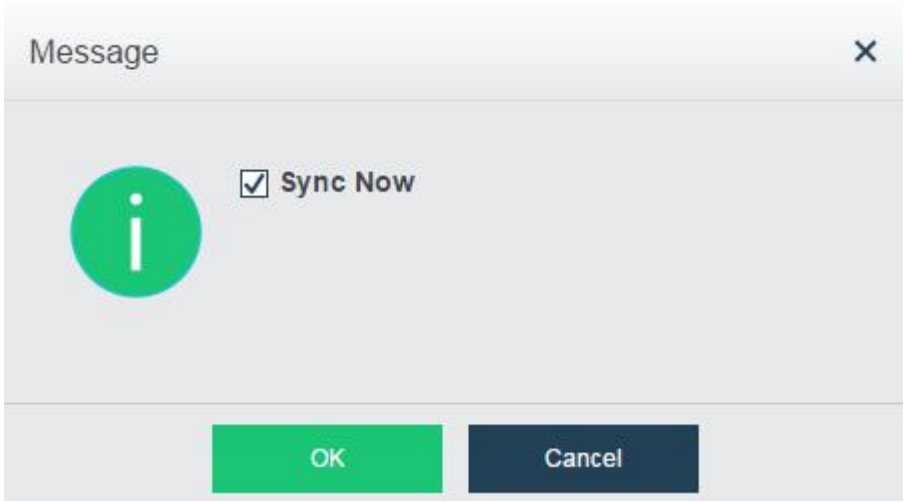
To change the date and time, click **Change** on this aBOS unit and select the date and time from the drop-down list.

To sync date and time with local PC, click **Sync with Local PC**, and click **OK** to confirm the changes. Please note that re-login is required if you want to apply the changes.

To sync time with a specific NTP server, select one NTP server from the drop-down list, as shown below:

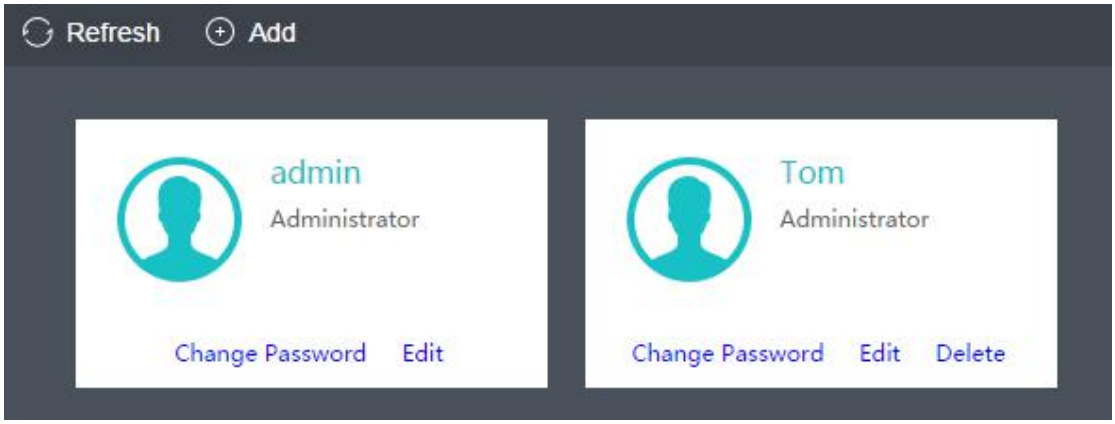


After NTP server is selected, click **Save**, then a message pops up asking whether to sync now, select **Sync Now** and click **OK** to confirm changes. Before syncing time with NTP server, make sure that DNS server on aBOS is configured correctly and this aBOS unit is connected to the Internet.

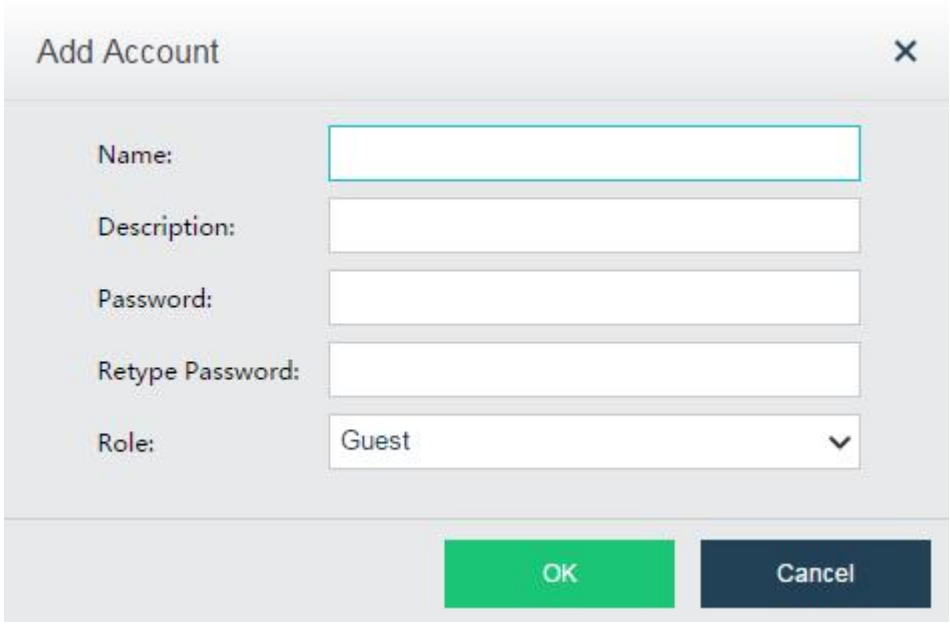


Configuring Administrator Account

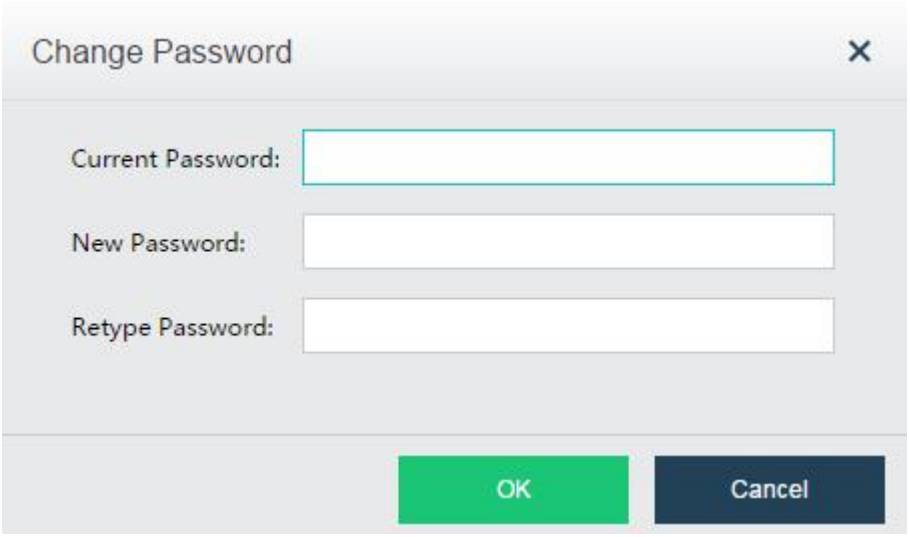
To configure admin account and password to log into this aBOS unit, click **Administrators** to enter the following page. You can add more than one admin accounts and assign different privileges to those accounts.



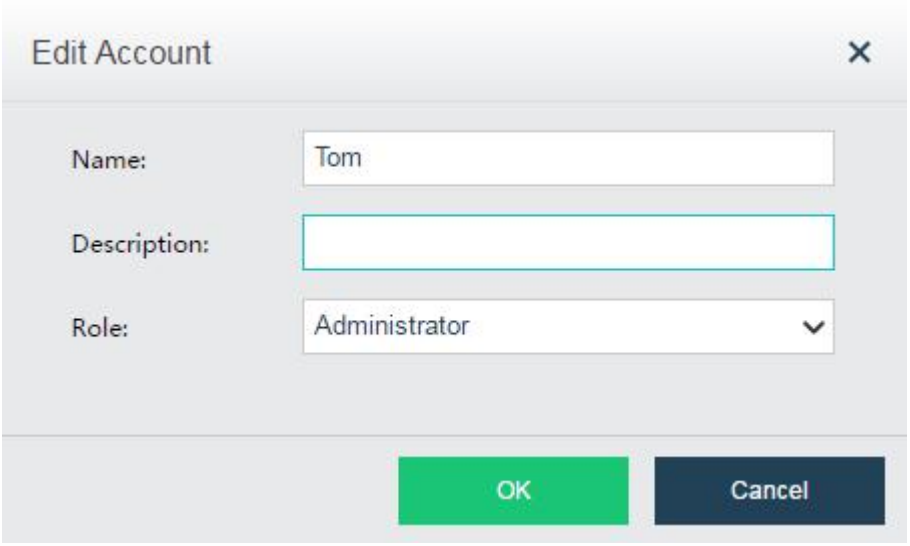
To create a new administrator account, click **Add** and specify **Name**, **Description**, **Password**, **Retype Password** and **Role** fields on **Add Account** page. **Retype password** field is required to avoid typing a wrong password. For **Role**, options are **Guest** and **Administrator**.



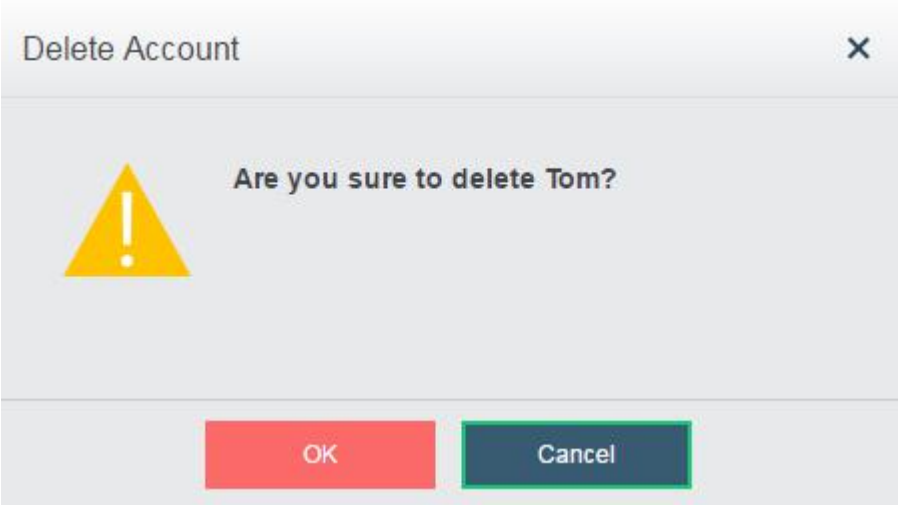
To change password of the selected admin, click **Change Password**, as shown below:



To edit the selected account, click **Edit**, as shown below:



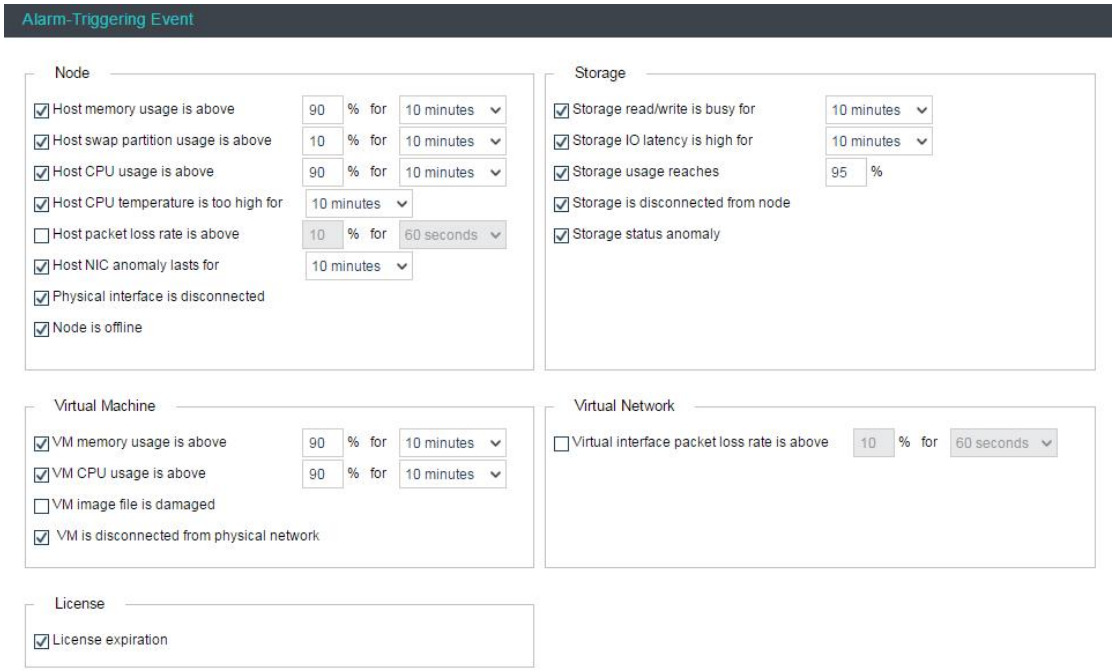
To delete a selected account, click **Delete**, as shown below:



Configuring Alarm Options

The **Alarm Options** page includes **Alarm-Triggering Event** and **Action**.

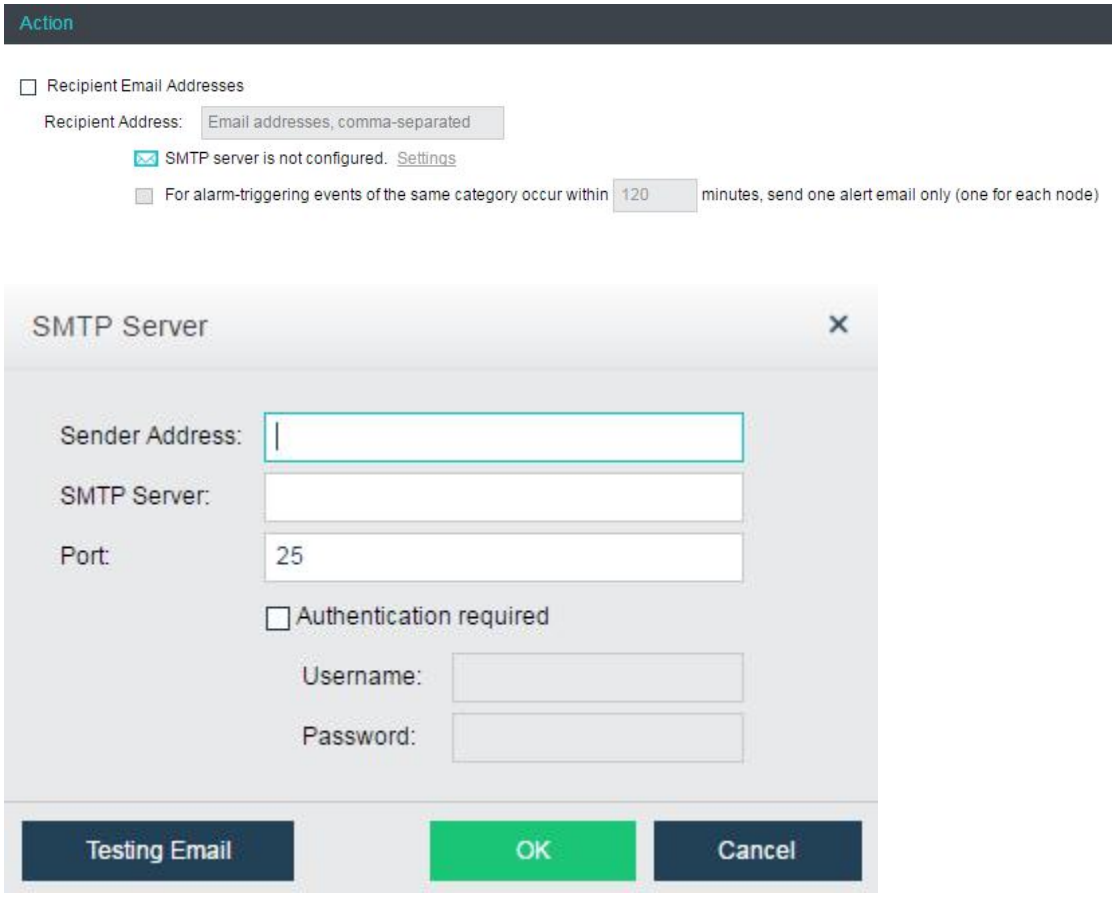
Alarm-triggering event is what can trigger alarm and generate alarm log when the any of the thresholds is reached.



There are thresholds for **Node**, **Storage**, **Virtual Machine**, **Virtual Network** and **License**.

To send alerts to specified email addresses, select the option **Send email to specified**

email addresses, specify the recipient email addresses. What is more, configure the SMTP server by clicking on **Settings**, as shown below:

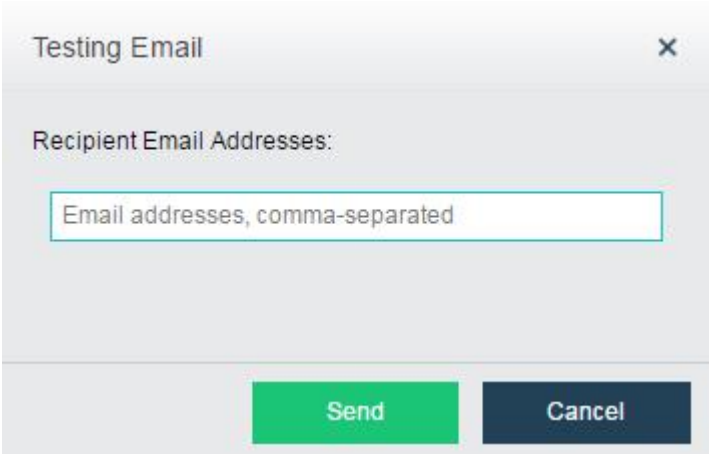


On the **SMTP Server** page, specify the following fields:

- **Sender Address**: Specifies sender email address.
- **SMTP Server**: Specifies IP address and domain name of SMTP server.
- **Port**: Specifies port of SMTP server. Default port number is 25.

If the SMTP server requires authentication, select **Authentication required** and enter the username and password.

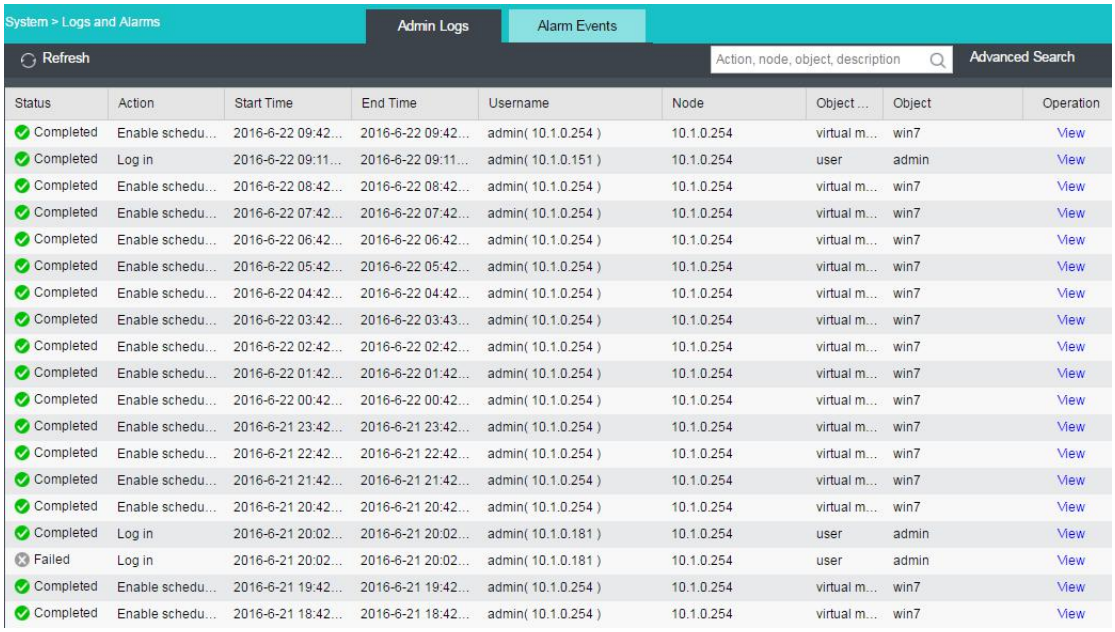
To send a testing email, click **Test Validity**, enter an email address in **Recipient Email Addresses** field, and click **OK**.



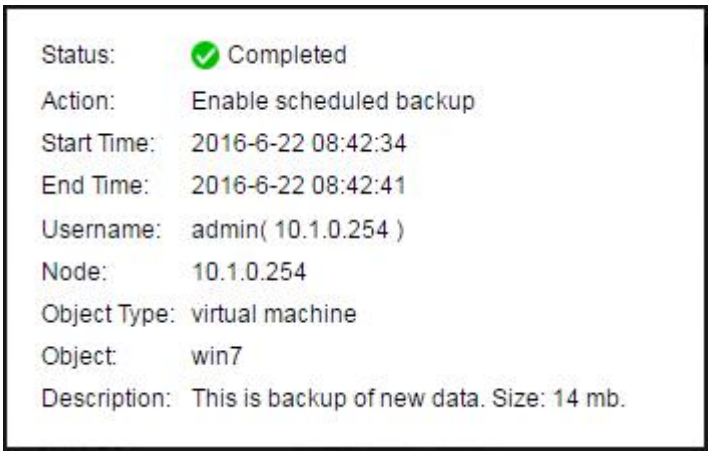
If **For alarm-triggering events of the same category occur within N minutes, send one alert email only (one for each node)** is selected, only one alert email will be sent for alarm-triggering events of the same category within the specified period.

Viewing Admin Logs and Alarm Events

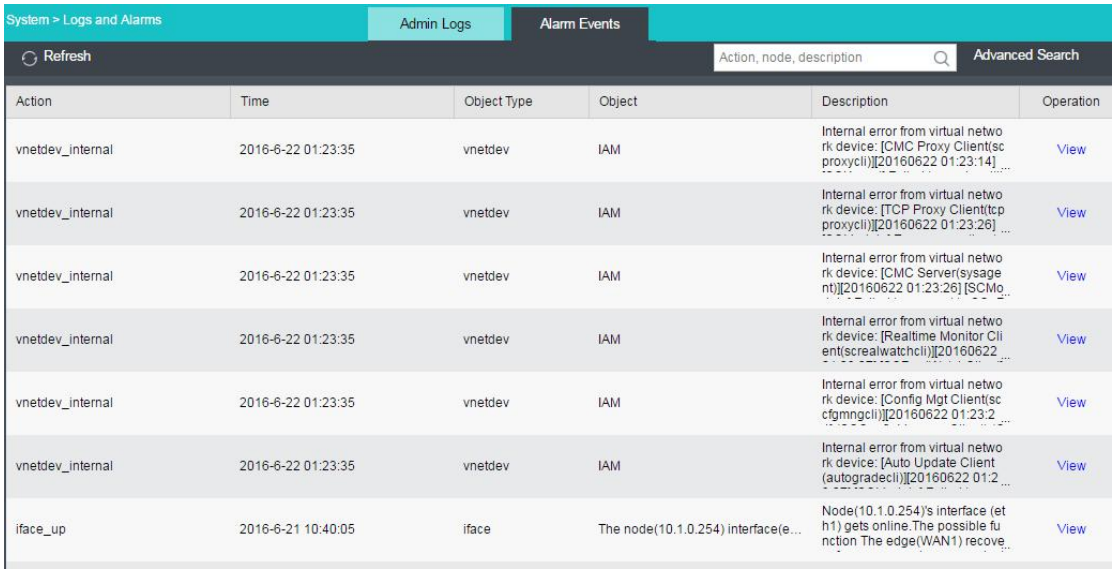
Click **Logs and Alarms** to enter the page as shown below, which includes **Admin Logs** and **Alarm Events** modules:



Admin logs archive all kinds of operations, such as creating new VMs, etc. It presents information like **Status**, **Action**, **Start Time**, **End Time**, **Username**, **Node**, **Object Type**, etc. Click **View** to view details of the log.



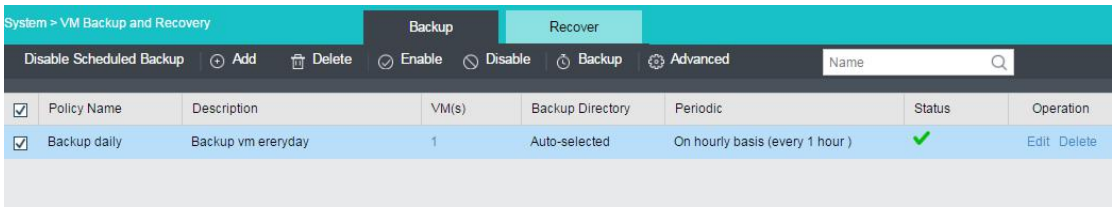
The events are alarm-triggering events, for example, VM CPU usage is above the threshold, etc. It presents information like **Action**, **Time**, **Object Type**, **Object**, **Description**, and **Operation**. For details, click **View**. For configuration of alarm thresholds, see Configuring Alarm Options.



Backing Up Virtual Machines

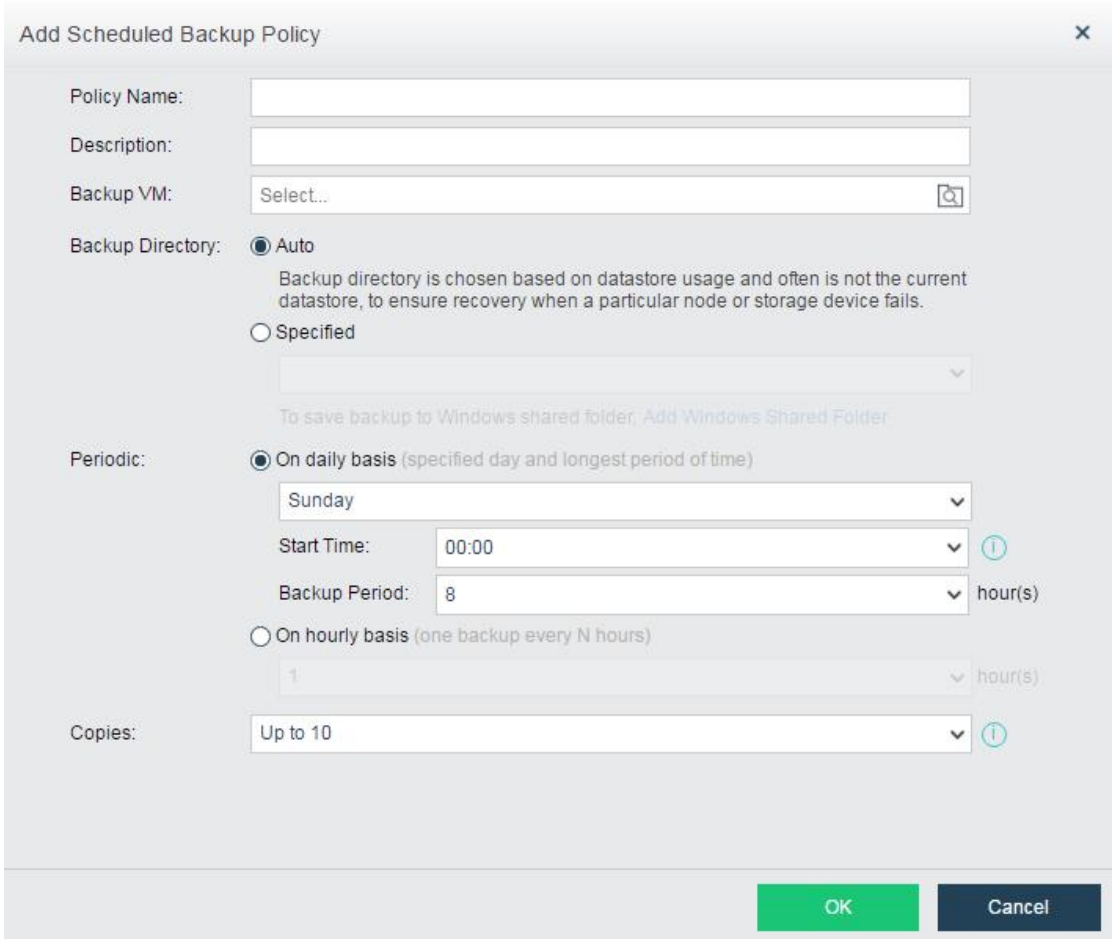
Based on a scheduled backup policy, virtual machines that are stored on local storage can be automatically and periodically backed up onto another storage. For virtual machines stored on shared storage, they can be migrated to storage on another node automatically when the current node fails, and therefore they do not need to be

backed up with any scheduled backup policy.



The following are contents included on the above page:

- **Enable Scheduled Backup:** Click **Enable Scheduled Backup** to enable scheduled backup, and it displays **Disable Scheduled Backup**. Click a second time to disable it, and it displays **Enable Scheduled Backup**.
- **Add**: Click **Add** to add a scheduled backup policy.



The following are contents included on the above page:

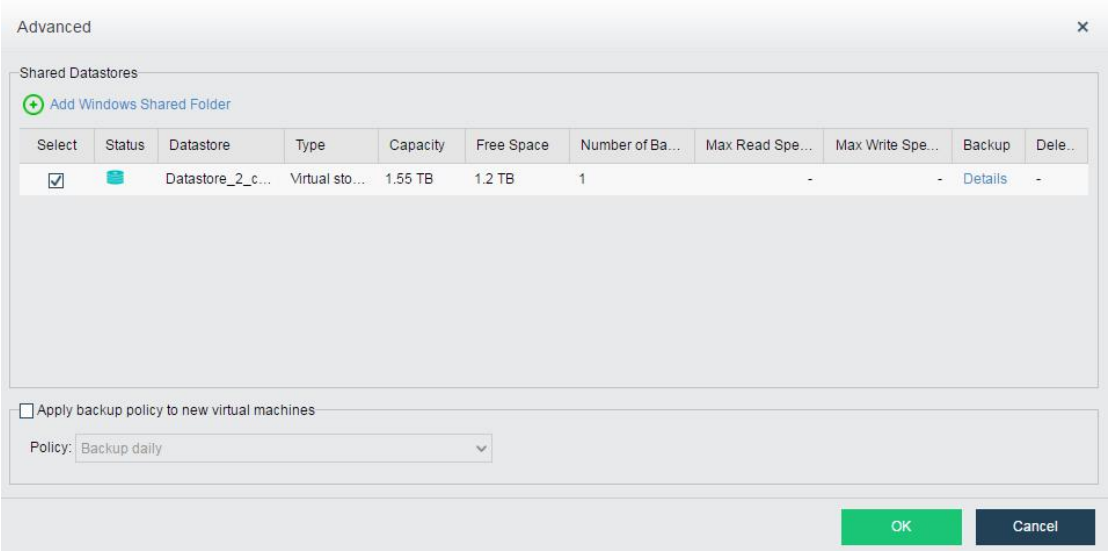
- **Policy Name**: Specifies name of the new backup policy.
- **Description**: Specifies description of the new backup policy.
- **Backup VM**: Specifies virtual machines you want to back up.

- **Backup Directory**: Options are **Auto** and **Specified**.
- **Auto**: Backup directory is chosen based on storage usage and often is not the current datastore to ensure recovery occurs when the node or storage on which the specified virtual machines are running fails.
- **Specified**: Specifies a specific backup directory.
- **Periodic**: Options are **On daily basis** and **On hourly basis**.
- **On daily basis**: Options are from **Sunday** to **Saturday**.
- **Start Time**: Specifies time to start backup. Select a period that service is not busy, because backup may bring impact to system service.
- **Backup Period**: Due to the fact that the backup process may take a rather long period of time, specify the longest period that a backup process may take. The backup process will stop after the specified hours and continue the next day at the specified start time again.
- **On hourly basis**: Indicates that backup occurs every few hours.
- **Copies**: Specifies the largest amount of copies that will be preserved. The earliest copies will be automatically deleted upon reaching threshold.
- **Delete**: Delete the selected backup policy.
- **Enable**: To enable the backup policy, click **Enable**, or click the  icon.
- **Disable**: To disable the backup policy, click **Disable**, or click the  icon.
- **Backup**: Click **Backup** to enable the selected backup policy.

There is no need to back up virtual machines on shared storage because they can be migrated to another node automatically if node fails.

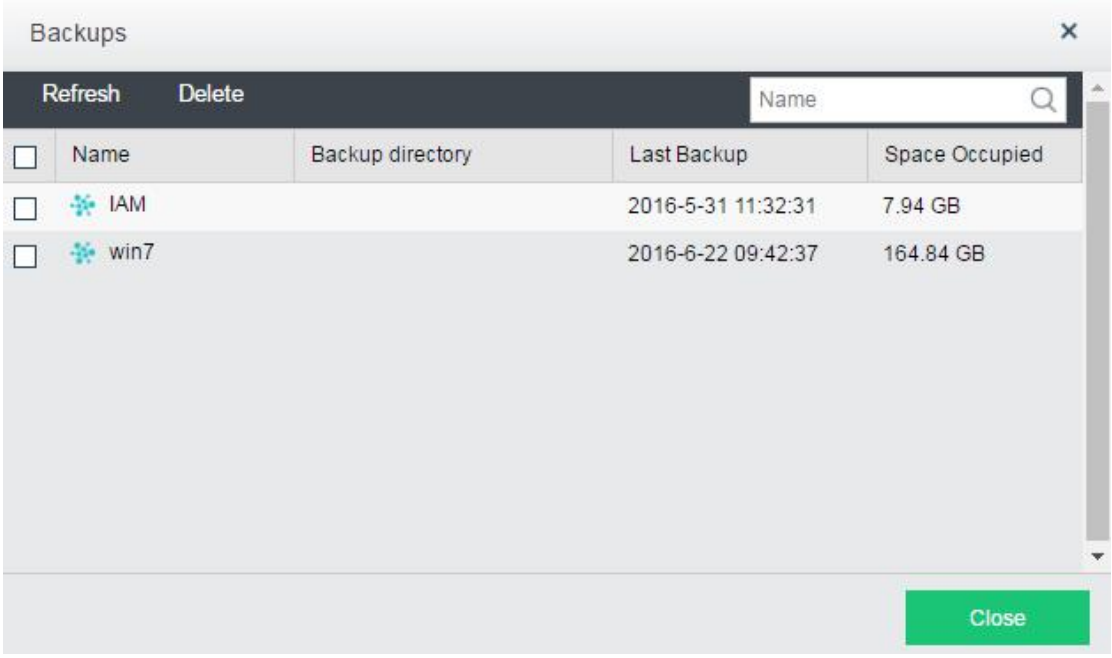
- **Advanced**

To specify datastore for new backup policies, click **Advanced**.



There are the available shared datastores and Windows shared folders which can be added manually, and information like name, type, capacity and free space and status of the datastore, whether backup on that datastore is allowed, and how many backups already exist on that datastore.

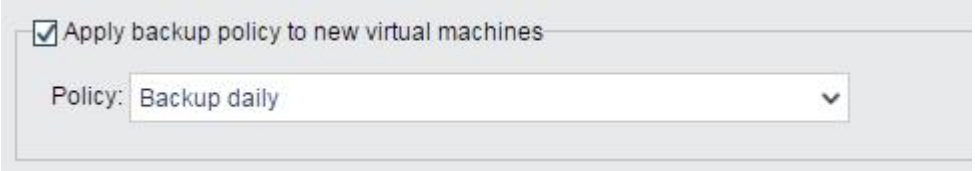
To view the backed up files on a specified datastore, click **Details**. The following information is available: name of backed up virtual machines, directory for backed up virtual machines, time of last backup, and space occupied by backup.



To delete backup files of certain network devices, first select files that have been backed up and then click **Delete**.

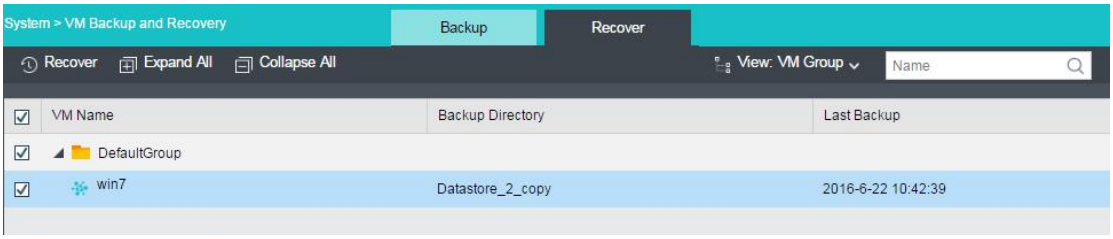
- **Apply backup policy to new virtual machines**: Specifies whether new virtual machines should be backed up, and specifies datastore for backed up virtual machines. By default, virtual machines are backed up to the current datastore.

You may specify another datastore to back up the virtual machines.

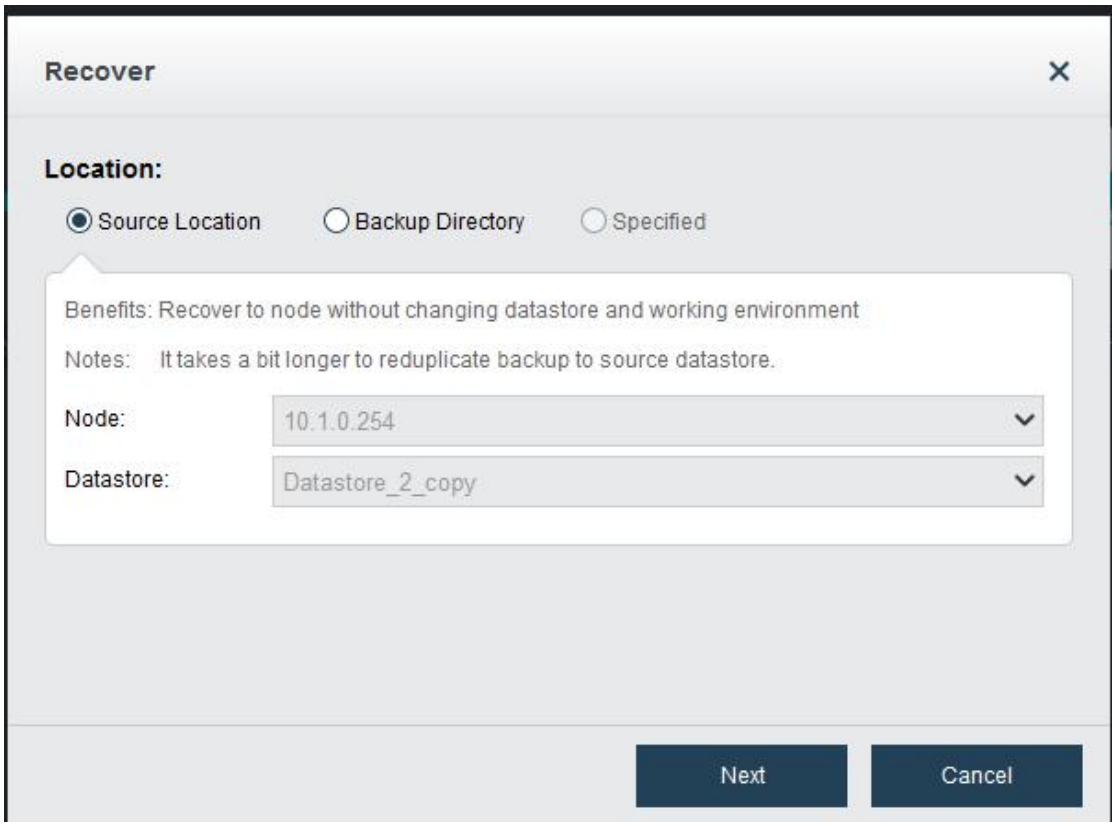


Recovering Virtual Machines

To recover a virtual machine, select the backed up virtual machines in the **Recover** tab and recover them to their previous status and configuration.

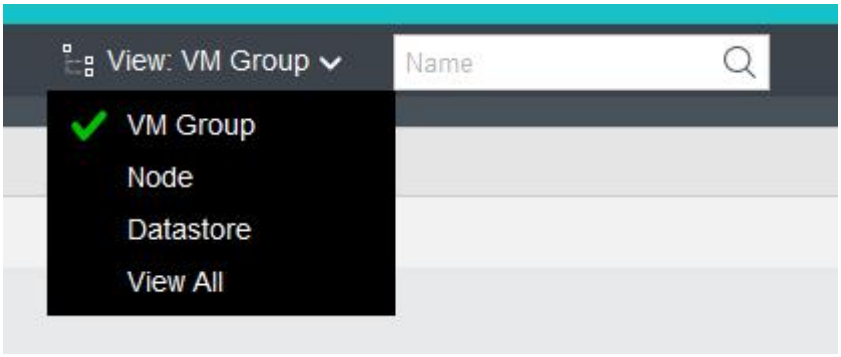


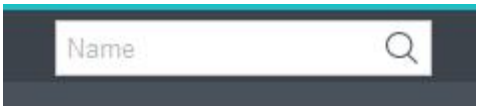
There are three options of location for recovering virtual machines, **Source Location**, **Backup Directory** and **Specified**. Select one of them to recover the virtual machines, as shown below:



- **Source Location:** Virtual machine will be recovered onto the current node without changing datastore and working location(node).
- **Backup Directory**: There is no need to duplicate the virtual machine and the recovery operation can be performed immediately.
- **Specified:** Specifies the most favorable datastore.

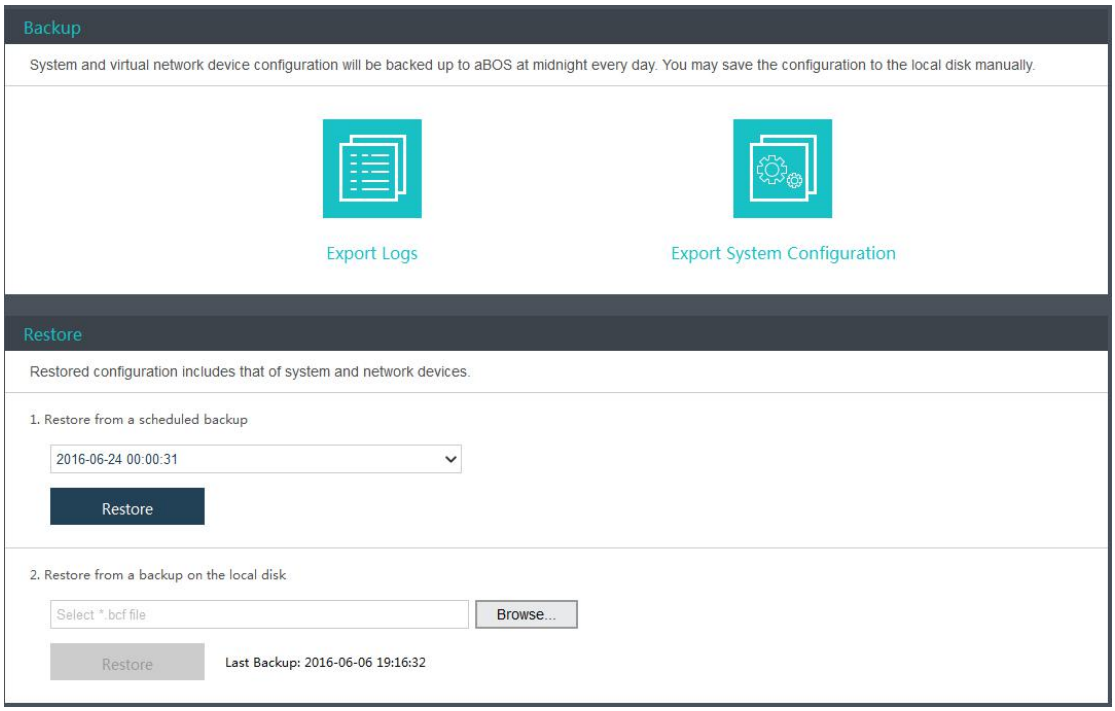
In **System** > **VM Backup and Recovery** > **Recover**, virtual machines can be viewed by **VM Group**, **Node**, **Datastore**, or **View All**. To search for a specific virtual machine, enter search term in the search box. Fuzzy match is supported.



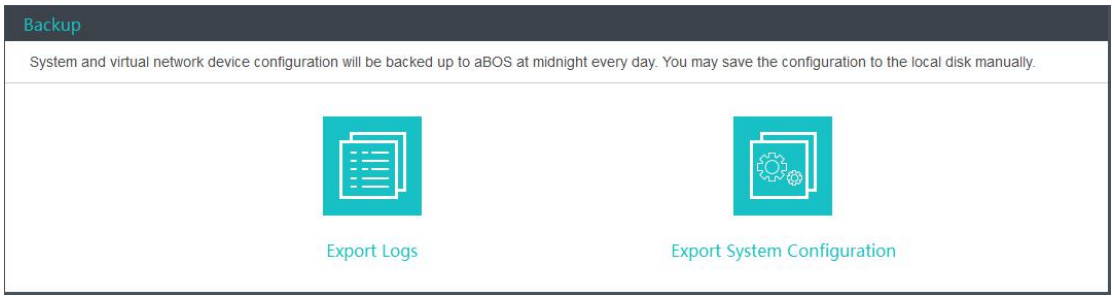


Backing Up or Restoring System Settings

To back up and restore configurations of system and virtual network devices, or restore to factory defaults, go to **System** > **System Backup and Restore**.

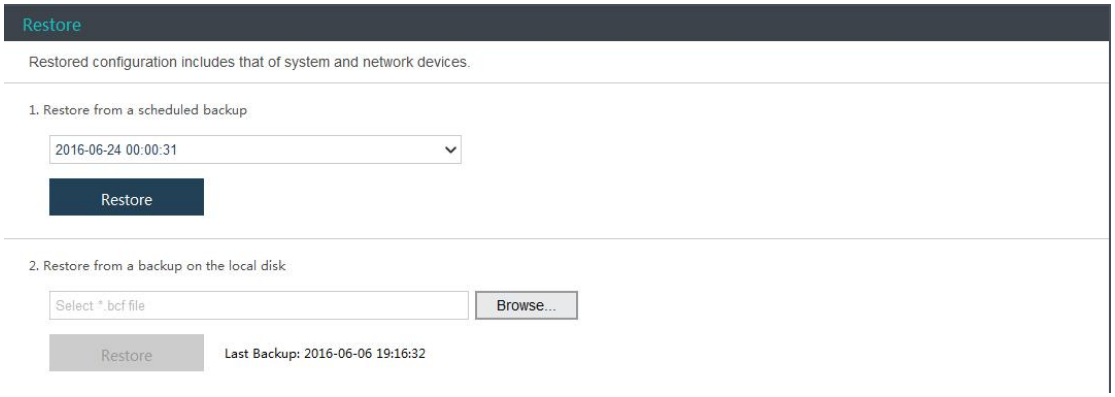


You may back up the settings using the **Export System Configuration** option, as shown below:



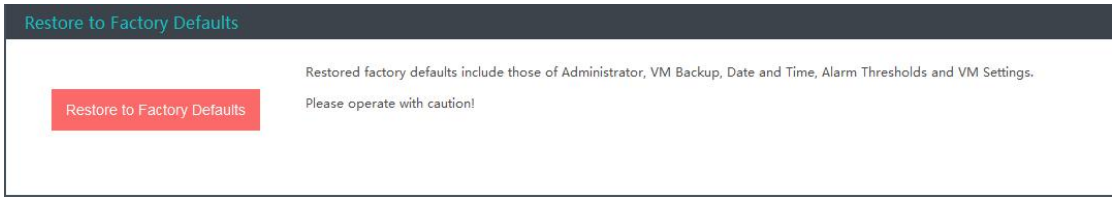
To back up logs of specified period and specified nodes onto local disk, click **Export Logs**.

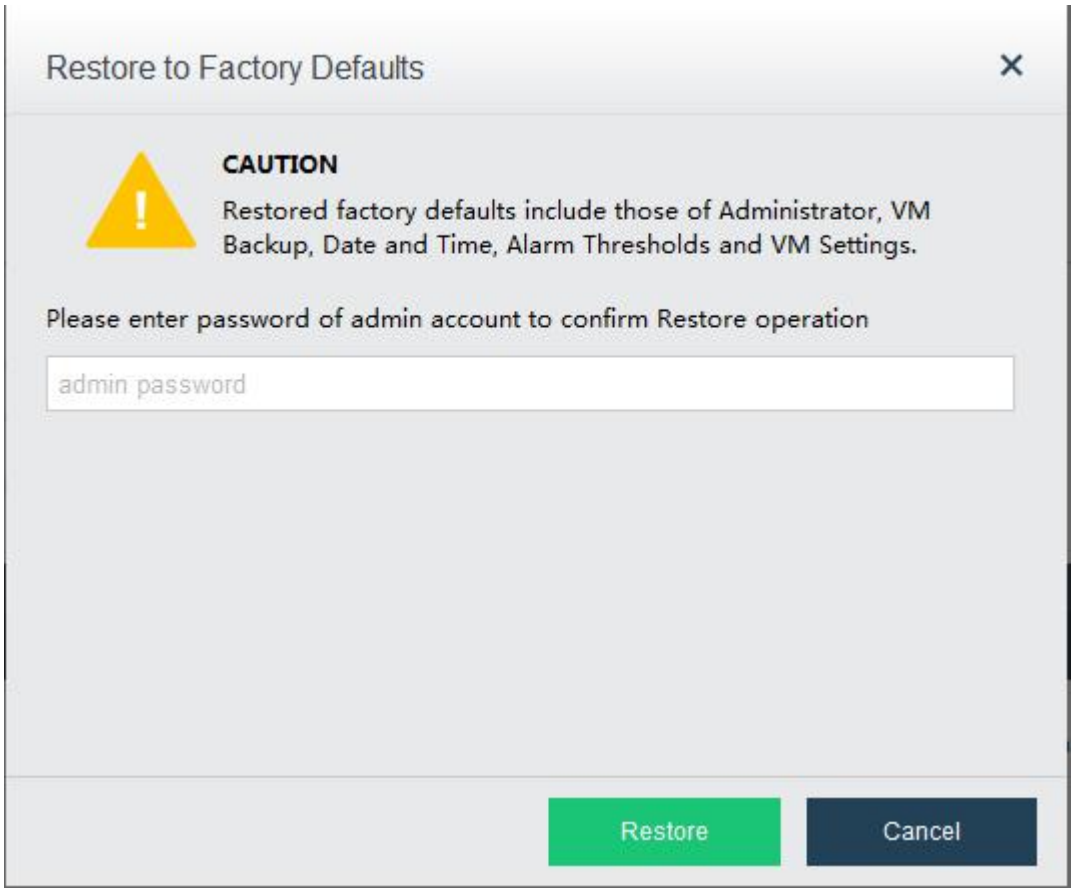
To restore settings of this aBOS unit from a backup or a backup on the local disk, upload the file and click **Restore**.



Restoring to Factory Defaults

To restore this aBOS unit to its factory defaults, click **Restore to Factory Defaults**.

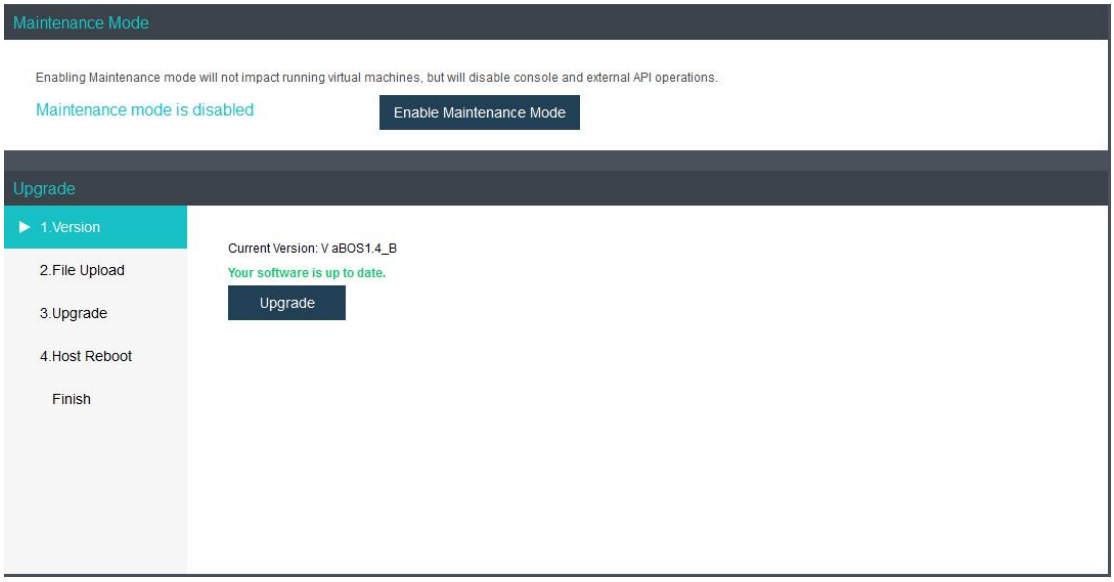




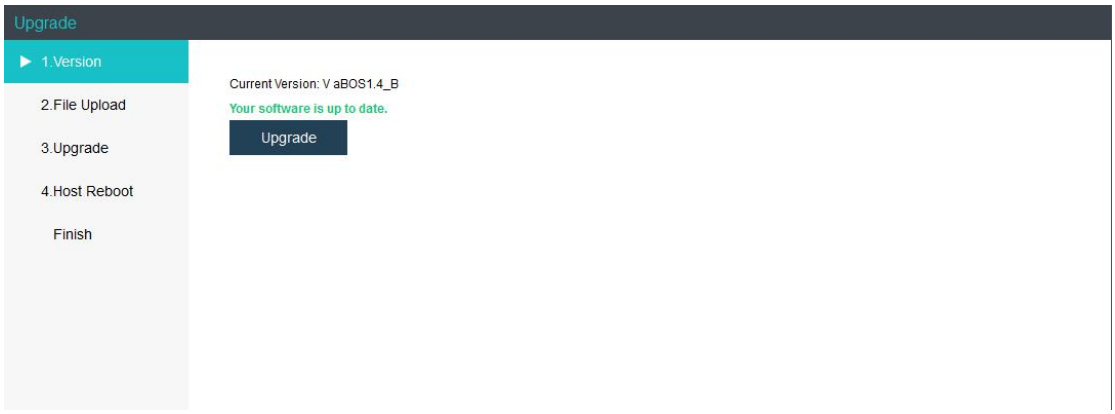
Click **Restore to Factory Defaults**, enter password of admin account on the page that pops up, and click **Restore** to start Restore operation.

Updating System

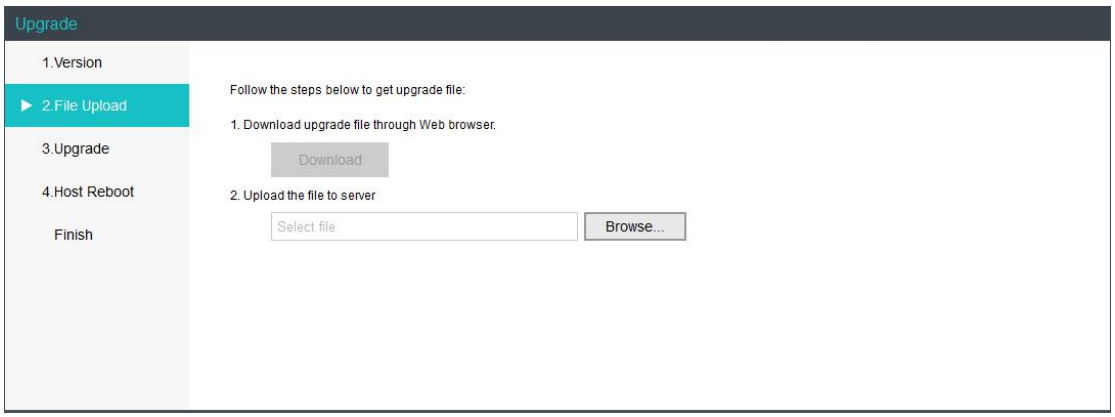
In **System** > **Upgrade**, you can enable/disable maintenance mode, upgrade this aBOS unit and view details of the upgrade operation.



To upgrade this aBOS unit, upload update package, as shown below:

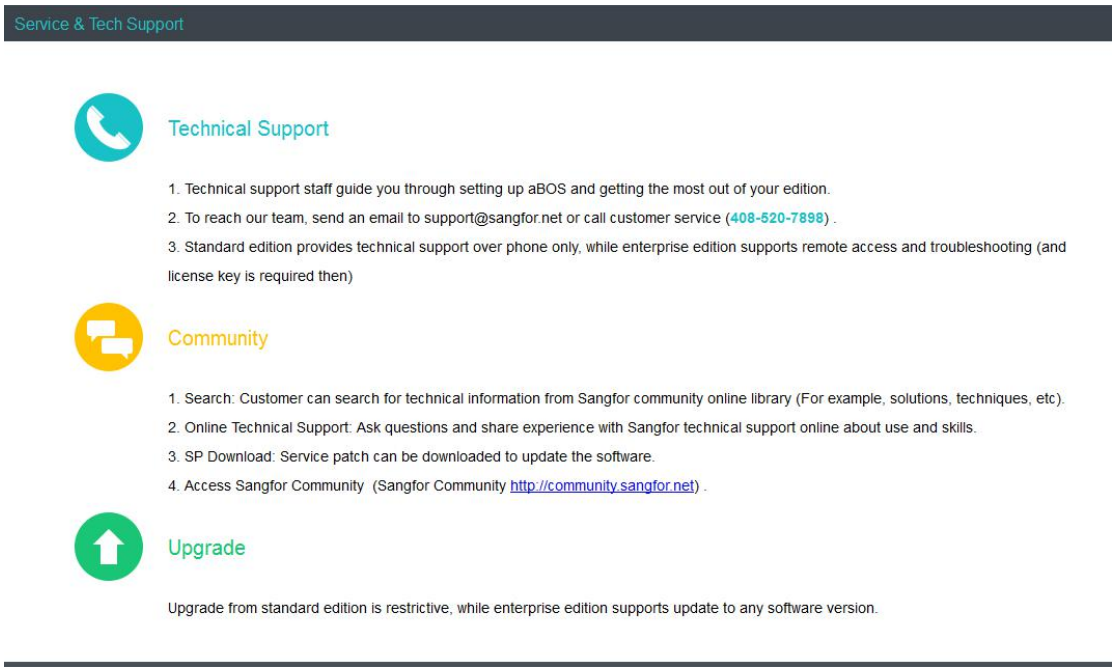


Click **Upgrade** and do as required. It will reboot when Upgrade operation completes.



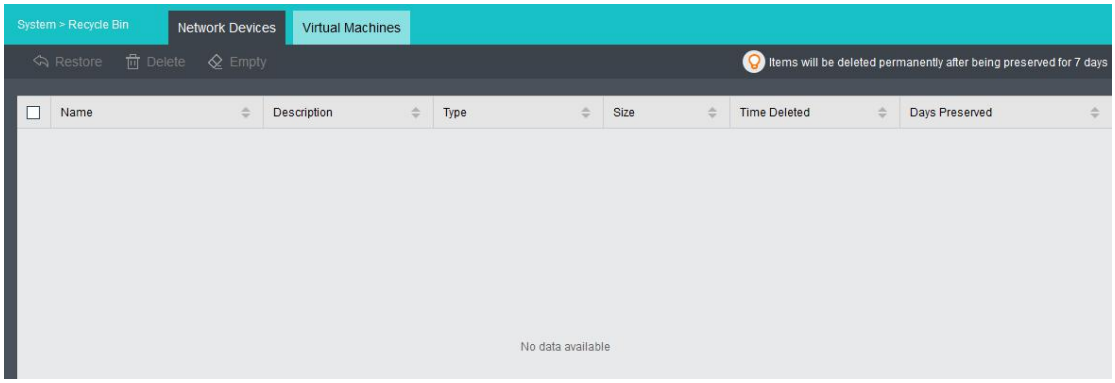
Gaining Service & Tech Support

The following services are supported, **Technical Support**, **Community, Upgrade, etc**, which are available to both standard edition and enterprise edition.



Removing Items From Recycle Bin

The items in the Recycle Bin, including network devices and virtual machines, will be deleted permanently after being preserved for 7 days, and connections to those devices can not be restored.

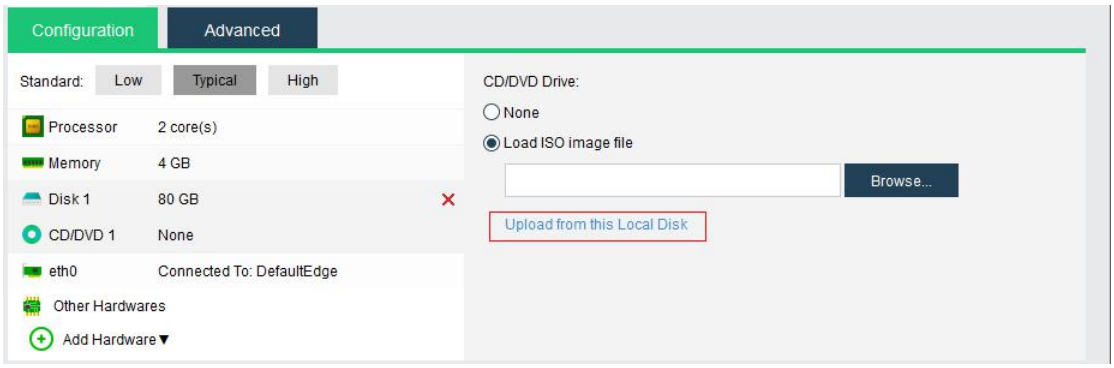


Case Study: Creating a Virtual Machine

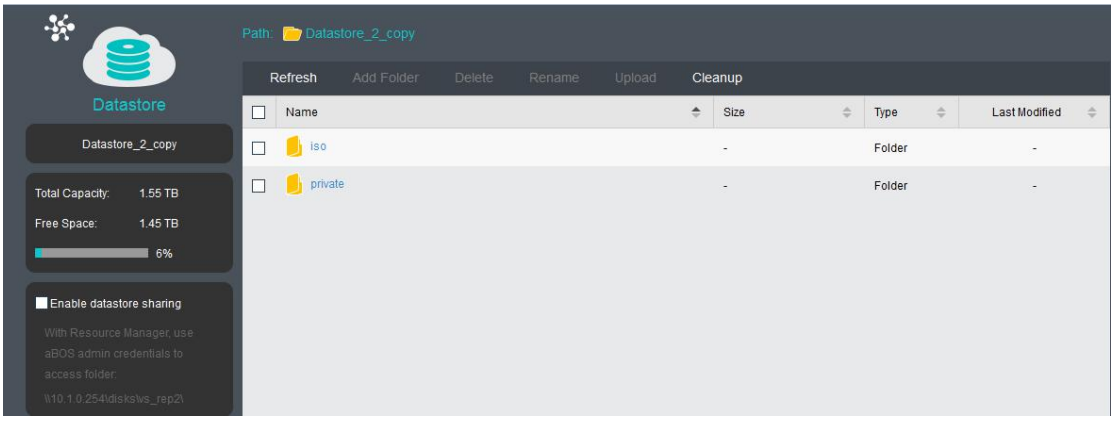
1. Go to **Networking** > **Map** > **Add server**, click **Create New Virtual Machine** and see Creating A New Virtual Machine to complete creating a new virtual machine in Windows 7.

2. Upload ISO image file to install the operating system. There are three ways to upload the ISO image file.

   a. Go to **Networking** > **Map** > **Add server**, click **Create New Virtual Machine**, and click **CD/DVD 1** > **Upload from this Local Disk**, specify **Image File** and **Datastore** fields, and click **Upload** to start this operation.

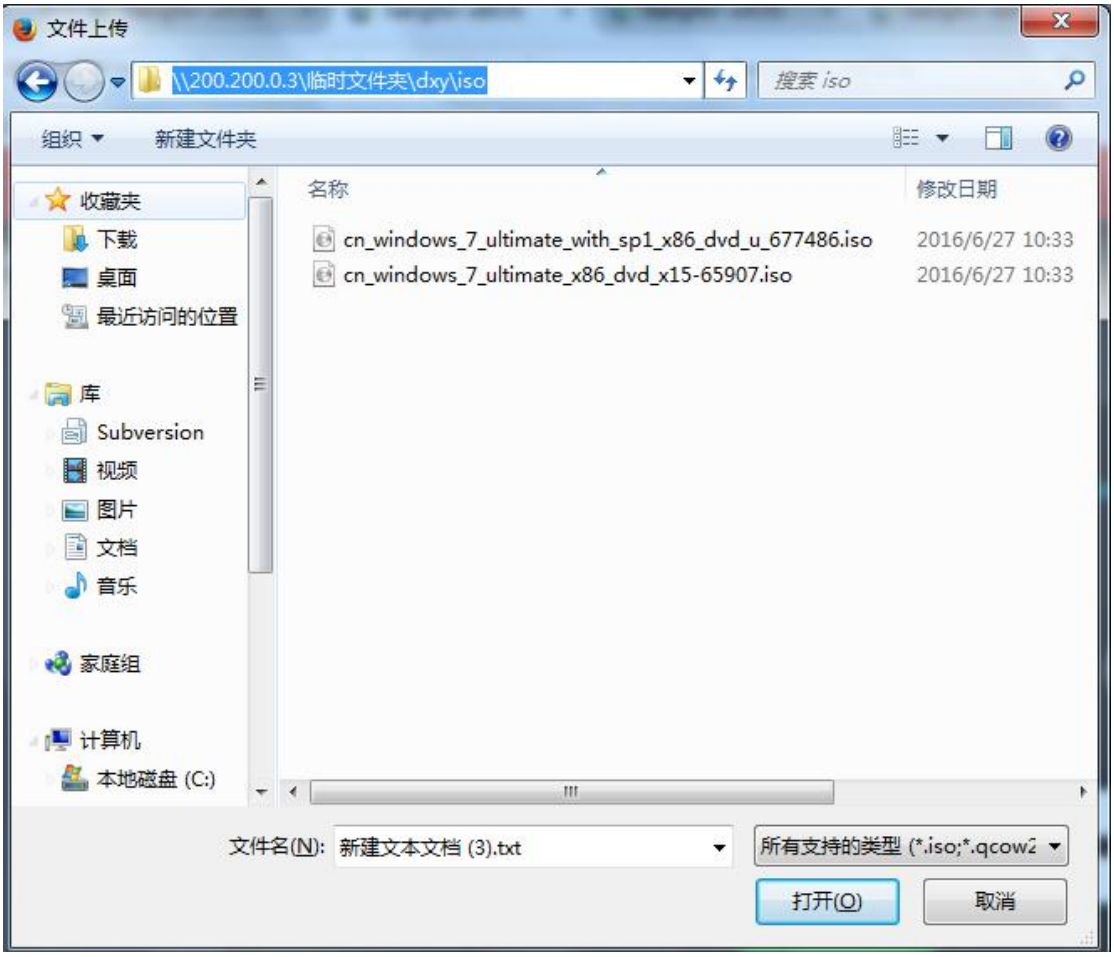


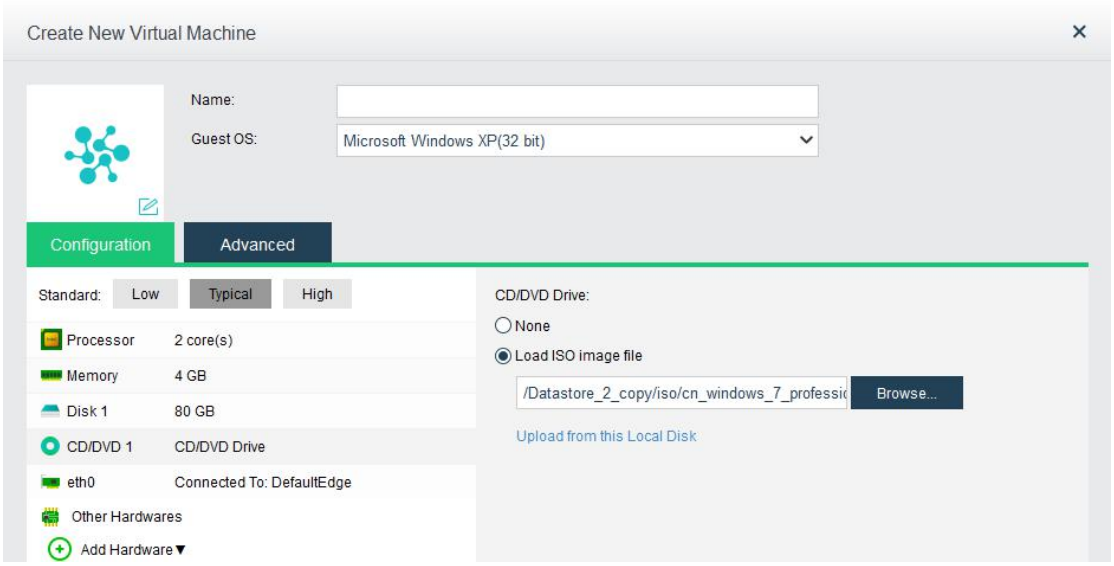
   b. Go to **Storage** > **Settings** > **Manage** and upload the ISO image file to the specified directory, as shown below:



   c. Go to **Networking** > **Add Server** > **Create New Virtual Machine**, click **CD/DVD 1**, and click **Browse** to enter the **Select ISO Image** page, and then click **Upload ISO Image** to enter the **Upload Image file from this local disk to datastore** page, click  icon and enter **\\IP address of the host** in the

address bar on the page that pops up and then you may be required to provide the admin account of that host. After entering the correct username and password, you get access to the files on that host, find the ISO image file and upload it to a specific datastore. Click **CD/DVD 1** to enter the ISO image file that has been uploaded in the **Load ISO image file** field.





3. After the virtual machine is created, click **Power on** to finish installing operating system and applications.