

# Configuration virtualization



## Installation manual for system providers

4/1/2021

### Product line neo, version 6.x

The described functions can be used with the following ASC products:

EVOIPneo

Please note that you can always find the most up-to-date technical documentation and product updates in the partner area on our website at <http://www.asctechnologies.com>.

Copyright © 2021 ASC Technologies AG. All rights reserved.

Windows is a registered trademark of Microsoft Corporation. VMware® is a registered trademark of VMware, Inc. All other marks and names mentioned herein may be trademarks of their respective companies.



## Contents

<b>1</b>	<b>General information .....</b>	<b>4</b>
<b>2</b>	<b>Introduction .....</b>	<b>5</b>
<b>3</b>	<b>System requirements.....</b>	<b>6</b>
<b>4</b>	<b>Compatible VMware features .....</b>	<b>7</b>
<b>5</b>	<b>Installation and configuration Digi AnywhereUSB .....</b>	<b>8</b>
5.1	Install drivers .....	8
5.2	Configure Digi AnywhereUSB .....	8
5.2.1	Establish connection to the VMware server .....	8
5.2.2	Change connection to the VMware server .....	9
5.2.3	Change IP address .....	10
<b>6</b>	<b>Configuration vNetwork standard switches .....</b>	<b>12</b>
6.1	vSphere client .....	12
6.1.1	Create vSwitch for administration .....	12
6.1.2	Configure vSwitch for administration .....	15
6.1.3	Create vSwitch for passive recording.....	18
6.1.4	Configure vSwitch for passive recording.....	21
6.2	vCenter client .....	23
6.2.1	Configuration vCenter standard switches .....	23
<b>7</b>	<b>Configuration Hyper-V.....</b>	<b>31</b>
<b>8</b>	<b>Configuration System Configuration .....</b>	<b>32</b>
8.1	Tab Usage.....	32
8.2	Tab Keystore/Virtualization .....	33
<b>9</b>	<b>Quick guide.....</b>	<b>34</b>
9.1	Install and configure Digi AnywhereUSB .....	34
9.2	Create and configure vSwitch for administration .....	34
9.3	Create and configure vSwitch for passive recording.....	34
9.4	Configure virtualization in System Configuration .....	34
	<b>List of figures .....</b>	<b>35</b>
	<b>List of tables .....</b>	<b>37</b>
	<b>Glossary .....</b>	<b>38</b>

## 1 General information

In the context of this document ASC represents ASC Technologies AG, its subsidiaries, branch offices, and distributors. An up-to-date overview of the aforementioned entities can be found at <https://www.asctechnologies.com>

ASC assumes no guarantee for the actuality, correctness, integrity or quality of the information provided in the manuals.

ASC regularly checks the content of the released manuals for consistency with the described hardware and software. Nevertheless, deviations cannot be excluded. Necessary revisions are included in subsequent editions.

Some aspects of the ASC technology are described in general terms to protect the ownership and the confidential information or trade secrets of ASC.

The software programs and the manuals of ASC are protected by copyright law. All rights on the manuals are reserved including the rights of reproduction and multiplication of any kind, be it photo mechanical, typographical or on digital data media. This also applies to translations. Copying the manuals, completely or in parts, is only allowed with written authorization of ASC.

Representative, if not defined otherwise, is the technical status at the time of the delivery of the software, the devices and the manuals of ASC. Technical changes without specified announcements are reserved. Previous manuals lose their validity.

The general conditions of sales and delivery of ASC in their latest version apply.

## 2 Introduction

---

### 2 Introduction

This document describes the configurations required for running the EVOIP<sub>neo</sub> software in virtualized environments.



For information about the installation and configuration of Microsoft Windows refer to the respective installation manual for system providers *Configuration Windows Server 2012 R2*, *Configuration Windows Server 2016* or *Configuration Windows Server 2019*.



---

In virtual environments, you can exclusively use network drives for archiving, import, and export of data. Internal or **USB** drives are not supported as performance issues may occur when trying to access a drive that is no longer available.

---

### 3 System requirements



Exclusively install software approved by ASC!

For information about approved software refer to the current neo *Integration Overview* in the ASC Partner Portal.

To be able to configure the virtualization in the application System Configuration, the customer-specific license file must have been imported. For further information about licensing refer to the administration manual *System Configuration - License administration*.



For a virtualization, VMware Tools must be installed.

Virtual machines must not be cloned.



The volume IDs of the drives in Windows must be unambiguous in a virtual neo system. This means that in a distributed neo system, the volume ID must not exist more than once. You can run a query of the volume IDs in the Windows command line prompt by entering the command `MOUNTVOL /L`.

#### ATTENTION!

neo is a near real-time application which cannot work with resource sharing. Therefore, all VMware resources must be assigned exclusively to the virtual neo machines and drives must be configured as *Thick*. If this precondition is not fulfilled, loss of recordings is imminent!

For information about the system requirements for virtual environments refer to the installation manual *Installation requirements*.

VMware ESX/ESXi Server features	Compatibility
VM Templates (OVAs)	Yes <sup>3</sup>
Copy Virtual Machine	No
Restart Virtual Machine on Different ESXi Host	Yes <sup>1</sup>
Resize Virtual Machine	Yes <sup>1, 2</sup>
Multiple Physical NICs and vNICs	Yes
VMware High Availability (HA)	No
VMware vNetwork Distributed Switch	No
VMware vMotion	No
Long Distance vMotion	No
VMware Storage vMotion	No
VMware Consolidated Backup (VCB)	No
VMware Data Recovery (DR, VDR)	No
VMware Snapshots	Yes <sup>1</sup>
VMware Fault Tolerance (FT)	No
VMware vCenter Converter	Yes
VMware vShield	No
Virtual Appliance Packaging of UC apps	No
3rd-Party VM-based Backup Tools (e. g. Veeam, Viziocore, esXpress)	Yes <sup>1</sup>
3rd-Party Physical To Virtual (P2V) Migration Tools	Yes <sup>1</sup>
VMware Boot from SAN	Yes <sup>1</sup>
All not-listed	On request

<sup>1</sup> Downtimes are possible

<sup>2</sup> No downsizing possible

<sup>3</sup> Only for OVAs provided by ASC

## 5 Installation and configuration Digi AnywhereUSB

For the operation of the ASC recording software in a virtual environment a permanent Internet connection to ASC or alternatively a USB dongle is required. The Digi AnywhereUSB box can be used to connect USB components such as a USB dongle.

The following chapter describes the installation and the configuration of the Digi AnywhereUSB box which is required for the operation in a virtual environment.



The Digi AnywhereUSB box can only be operated with one server at the same time.

### 5.1 Install drivers

1. Connect the Digi AnywhereUSB box to the power supply.
2. Connect the Digi AnywhereUSB box to your network.
3. Download the driver and, if required, the latest firmware from the homepage indicated below:  
<https://www.digi.com/support/productdetail?pid=3747>
4. Install the appropriate driver according to the setup instructions.
5. After the installation of the drivers, a CMD window is opened automatically. Verify that the message *System driver installed successfully!* is displayed.

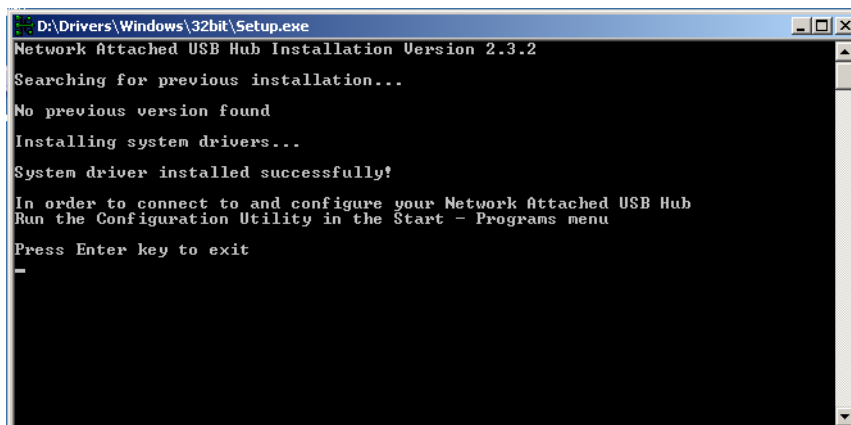



Fig. 1: Message informing about successful installation of driver

6. Press the [Enter] key to close the CMD window.

### 5.2 Configure Digi AnywhereUSB

#### 5.2.1 Establish connection to the VMware server

1. Press the Windows key.
2. Click on the icon .
  - ⇒ The installed apps are displayed.
3. Click on *AnywhereUSB Configuration Utility*.
  - ⇒ The following window appears:



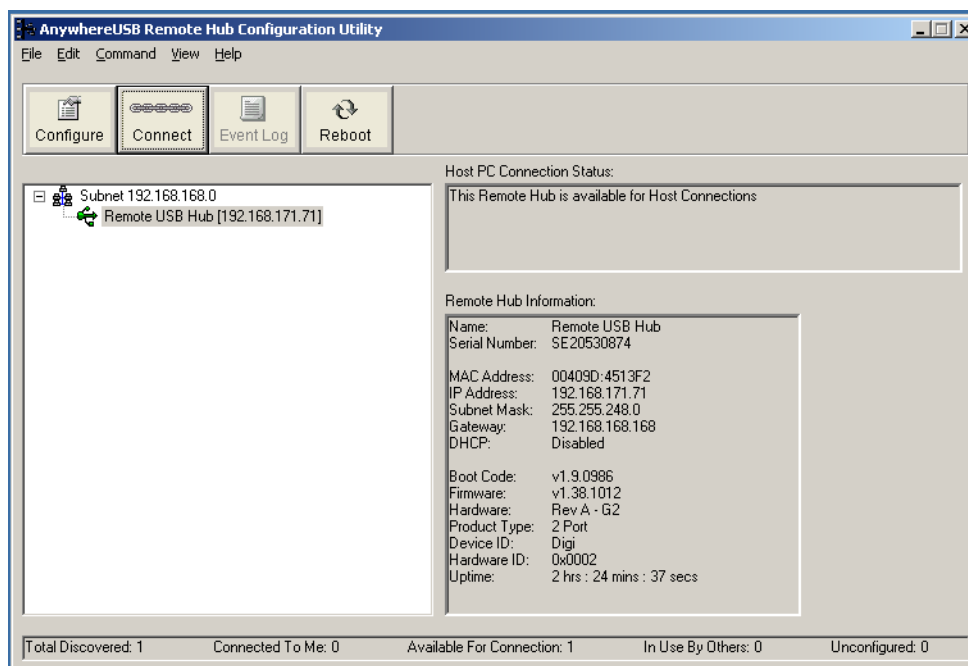



Fig. 2: Connect VMware server

4. Click on the button *Connect*.

### 5.2.2 Change connection to the VMware server

If the Digi AnywhereUSB box is supposed to be used on another VMware server, proceed as follows:

1. Press the Windows key.
2. Click on the icon .
  - ⇒ The installed apps are displayed.
3. Click on *AnywhereUSB Configuration Utility*.
  - ⇒ The following window appears:

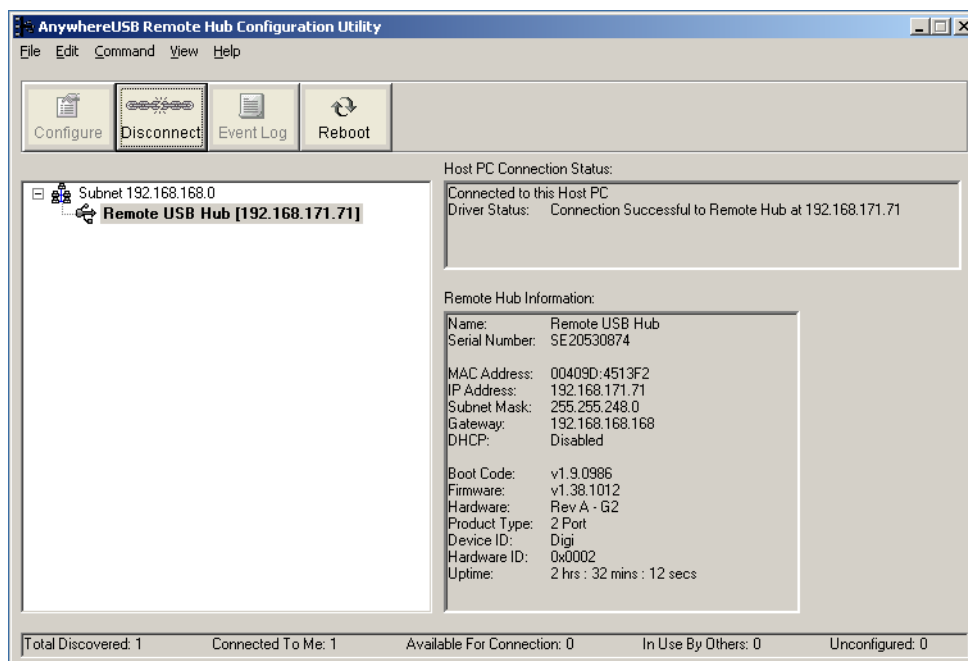


Fig. 3: Disconnect connection

4. Click on the button *Disconnect*.

5. Repeat all steps as described in [chapter "Install drivers", p. 8.](#)
6. Repeat all steps as described in [chapter "Establish connection to the VMware server", p. 8.](#)

### 5.2.3 Change IP address

By default, the Digi AnywhereUSB box has a **DHCP** network address. After the installation of the drivers, the Digi AnywhereUSB box is found automatically and the IP address of the VMware server is applied. This option has already been activated in the default setting.

To change the IP address, proceed as follows:

1. Start a browser.
2. Enter the IP address `https://192.168.175.20` in the address bar.
3. The configuration program *AnywhereUSB/2 Configuration and Management* is opened.

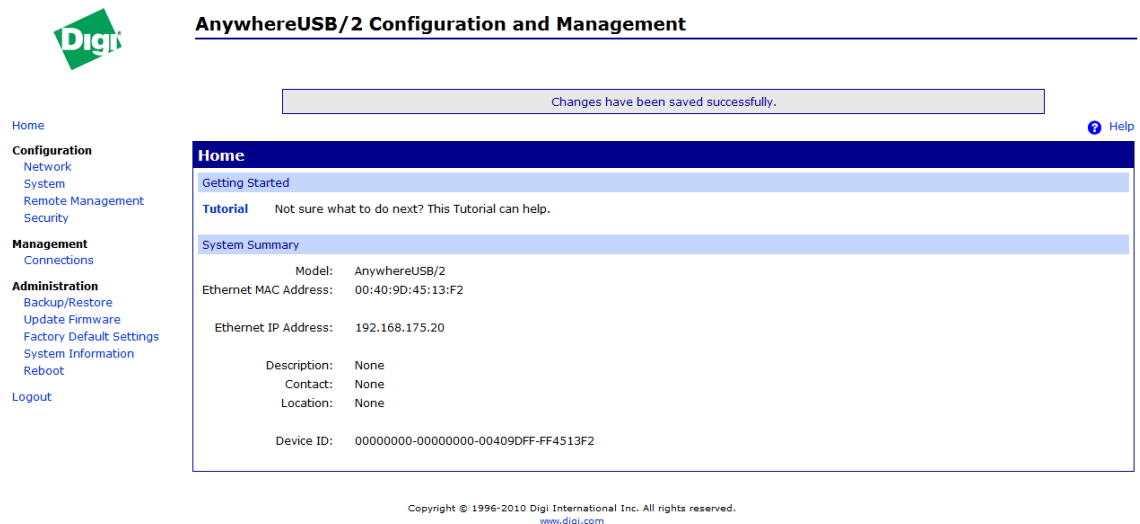


Fig. 4: Configuration program *AnywhereUSB/2 Configuration and Management*

4. Select the menu item *Configuration > Network* in the structure view.

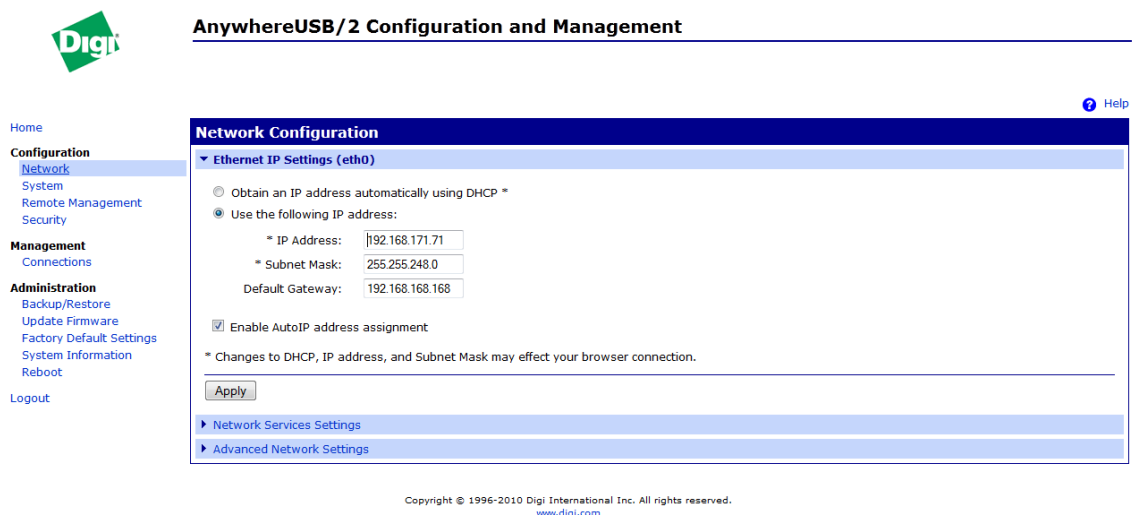


Fig. 5: Change IP address

5. In the field *Use the following IP address > IP Address*, enter the new IP address.
6. Click on the button *Apply*.
7. Confirm the security prompt with *Apply*.



## AnywhereUSB/2 Configuration and Management

? Help

**Apply Changes**

The configuration changes will cause your network settings to take effect immediately.

Copyright © 1996-2010 Digi International Inc. All rights reserved.  
[www.digi.com](http://www.digi.com)

Fig. 6: Confirm change

- The VMware server recognizes the change of the IP address automatically. The connection to the Digi AnywhereUSB box is reestablished.



## AnywhereUSB/2 Configuration and Management

? Help

**Reconnect In Progress**

The AnywhereUSB/2 with MAC address 00:40:9D:45:13:F2 is currently updating the network settings. You will be reconnected automatically in approximately 15 seconds.

If you are not reconnected automatically [click here](#) or use the discovery utility that was provided on your CD to find this device on the network.

Copyright © 1996-2010 Digi International Inc. All rights reserved.  
[www.digi.com](http://www.digi.com)

Fig. 7: Reconnect VMware server

- In the configuration menu, the message *Changes have been saved successfully* appears.



## AnywhereUSB/2 Configuration and Management

Changes have been saved successfully.

? Help

Home

**Configuration**

- Network
- System
- Remote Management
- Security

**Management**

- Connections

**Administration**

- Backup/Restore
- Update Firmware
- Factory Default Settings
- System Information
- Reboot

[Logout](#)

**Home**

[Getting Started](#)

**Tutorial** Not sure what to do next? This Tutorial can help.

**System Summary**

Model:	AnywhereUSB/2
Ethernet MAC Address:	00:40:9D:45:13:F2
Ethernet IP Address:	192.168.171.71
Description:	None
Contact:	None
Location:	None
Device ID:	00000000-00000000-00409DFF-FF4513F2

Copyright © 1996-2010 Digi International Inc. All rights reserved.  
[www.digi.com](http://www.digi.com)

Fig. 8: Change of the IP address completed successfully

## 6 Configuration vNetwork standard switches

The following chapters of this document describe the configuration of vSwitches for VMware ESXi servers by means of the VMware vSphere client or the VMware vCenter client. The configuration is necessary to guarantee that the ASC software functions correctly if it is supposed to be used in an ESXi-hosted virtual network.

This document merely covers the basic configuration of the vSwitches of the VMware ESXi software and not the basic installation or configuration of the VMware ESXi software in general. Neither the installation nor the configuration of the VMware vSphere Client and the VMware vCenter client are part of this document. This information can be found in the manufacturer documentation *Manual for the server configuration for ESXi*.

vNetwork standard switches are abstract network devices which fulfill the following tasks in a VMware ESXi-hosted virtual network:

- Control of the data traffic between virtual machines and external physical networks
- Control of the data traffic between virtual machines
- Combination of the bandwidth of several network adapters
- Distribution of the data traffic of several network adapters
- Mapping of failover scenarios in physical network adapters
- Substitution of a physical ethernet switch

When two or more virtual machines have been connected to the same vSwitch, the network data transfer between these virtual machines is controlled locally. When an uplink adapter is connected to the vSwitch, any virtual machine can access the external network that the adapter is connected to. In order to emulate the connection of the ASC software to a physical network best possible, two vSwitches have to be created. One for the administration of the ASC software and the ESXi server as well as another for the purpose of passive recording.

The following paragraphs of this chapter describe the setup of the vSwitches if the ASC software is supposed to be used in a VMware ESXi-hosted network.



For more information about the switch configuration refer to the administration manual *Configuration switch for passive VoIP recording*.

### 6.1 vSphere client

#### 6.1.1 Create vSwitch for administration

For communication with the ASC software for configuration and maintenance purposes a separate vSwitch is required which is created as follows:

1. Log into the vSphere Client and click on the host in the inventory list window.
2. Click on the tab *Configuration*.

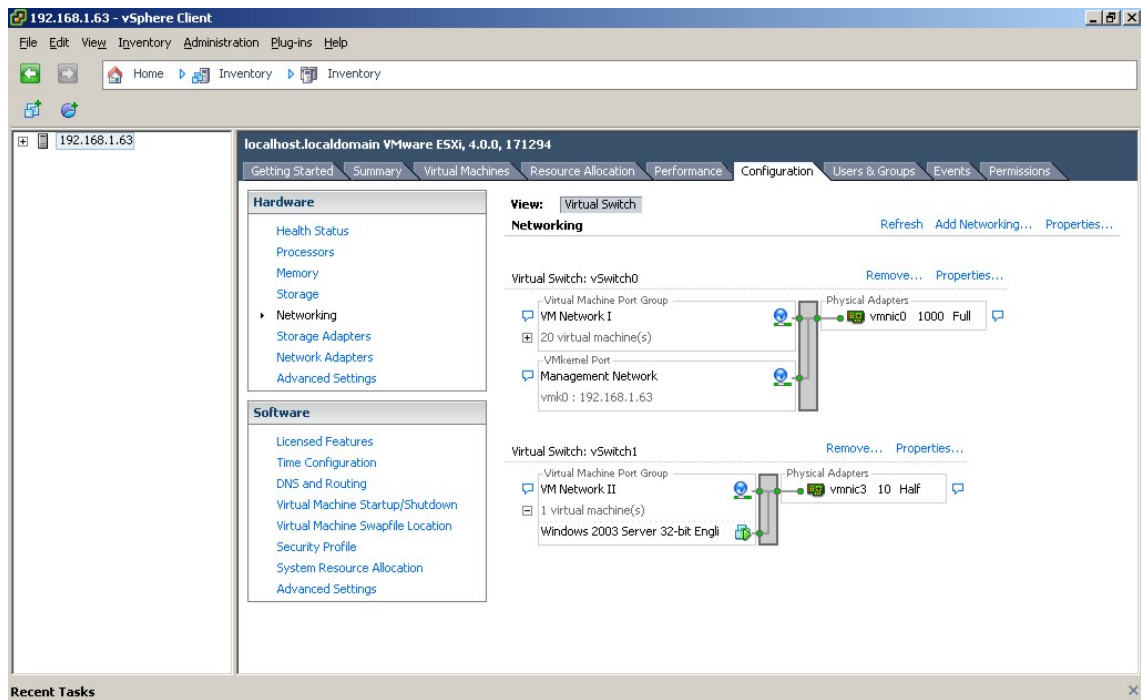


Fig. 9: vSphere Client (example)

3. Click on the menu item *Networking*.
4. Select the view *Virtual Switch*.
5. Click on *Add Networking*.
6. Accept the default connection type *Virtual Machine* and click on the button *Next*.

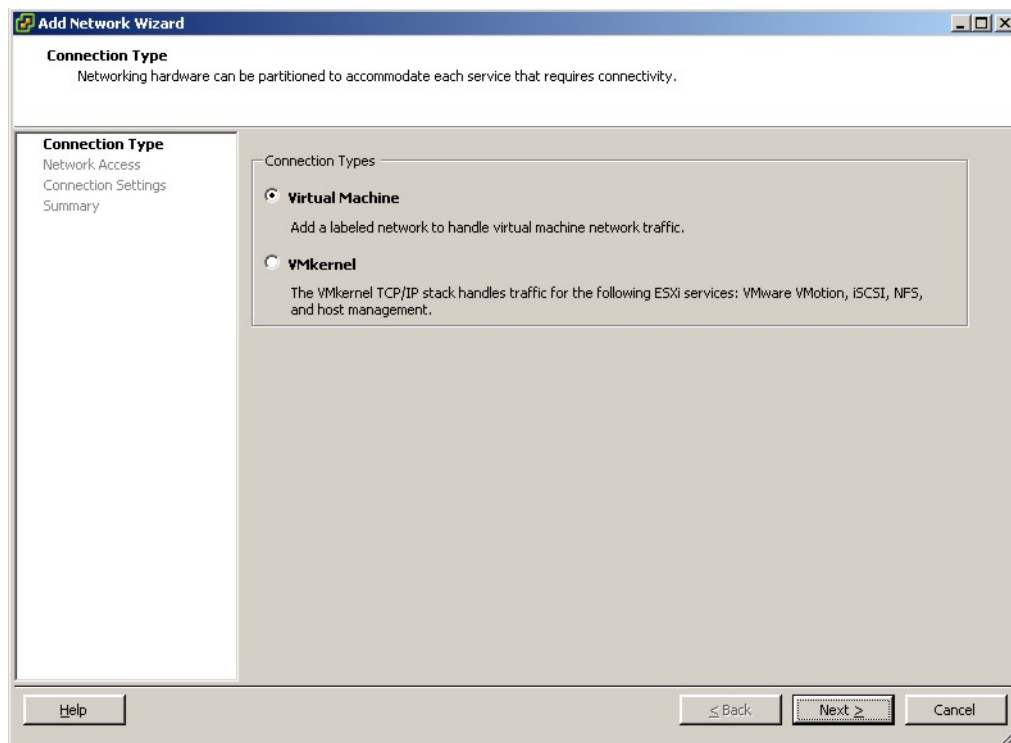


Fig. 10: Add virtual machine

7. Activate the option *Create a virtual switch* and the assigned physical adapters which are supposed to be connected to this vSwitch.

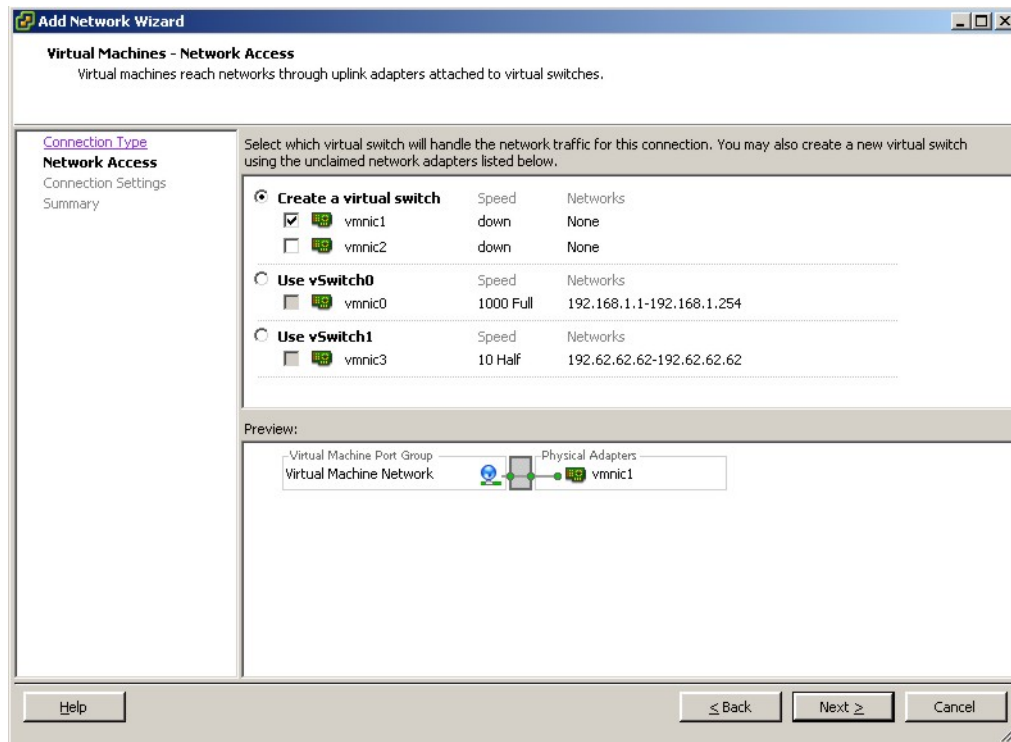


Fig. 11: Create a virtual switch (example)

8. Click on the button *Next*.
9. In the entry field *Network Label*, enter a term for the port group to be created (e. g. VM Network I).

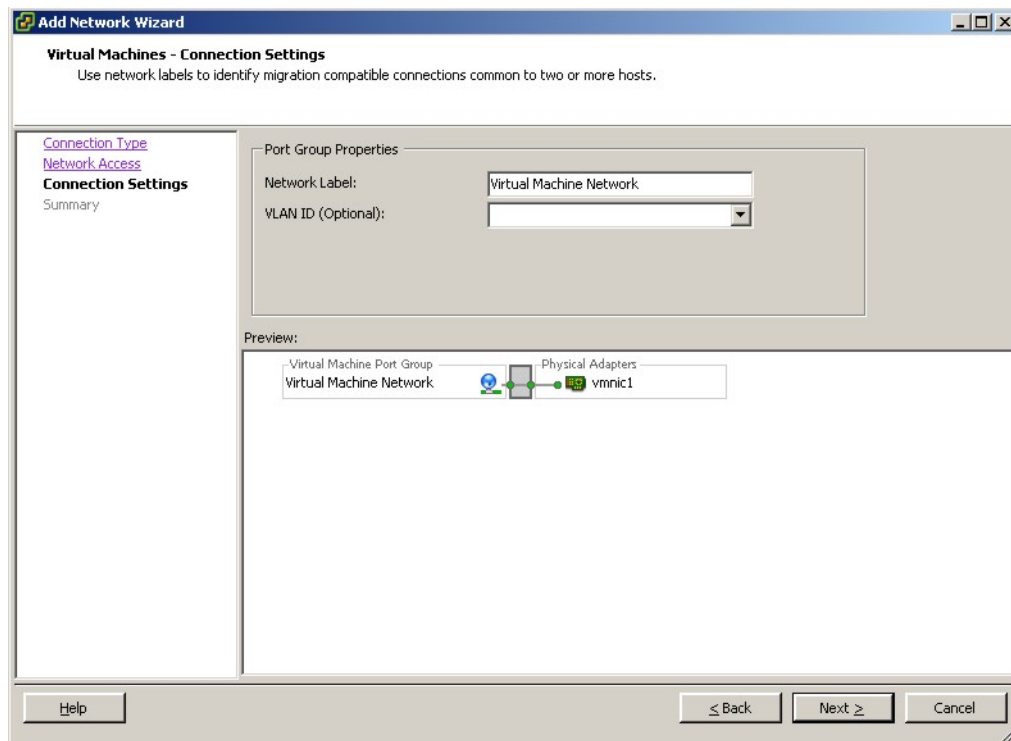


Fig. 12: Enter network label (example)

10. Click on the button *Next*.
11. Verify that the vSwitch has been configured properly.

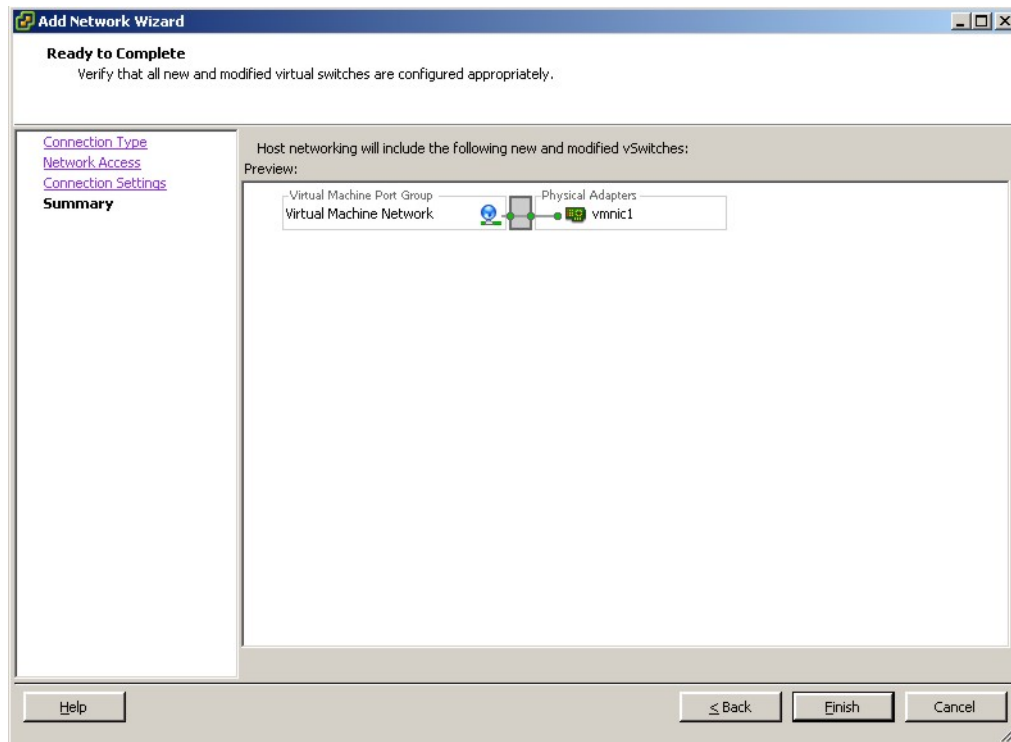


Fig. 13: Configuration ready to finalize (example)

12. Click on the button *Finish*.

When all configuration steps mentioned above have been concluded, the vSwitch has been created successfully and is ready for enhanced configuration.

### 6.1.2 Configure vSwitch for administration

For the new vSwitch for administration to be used with the ASC software, the following configuration steps have to be carried out:

1. Click on the *Properties* of the corresponding vSwitch.
2. Click on the configuration *vSwitch*.

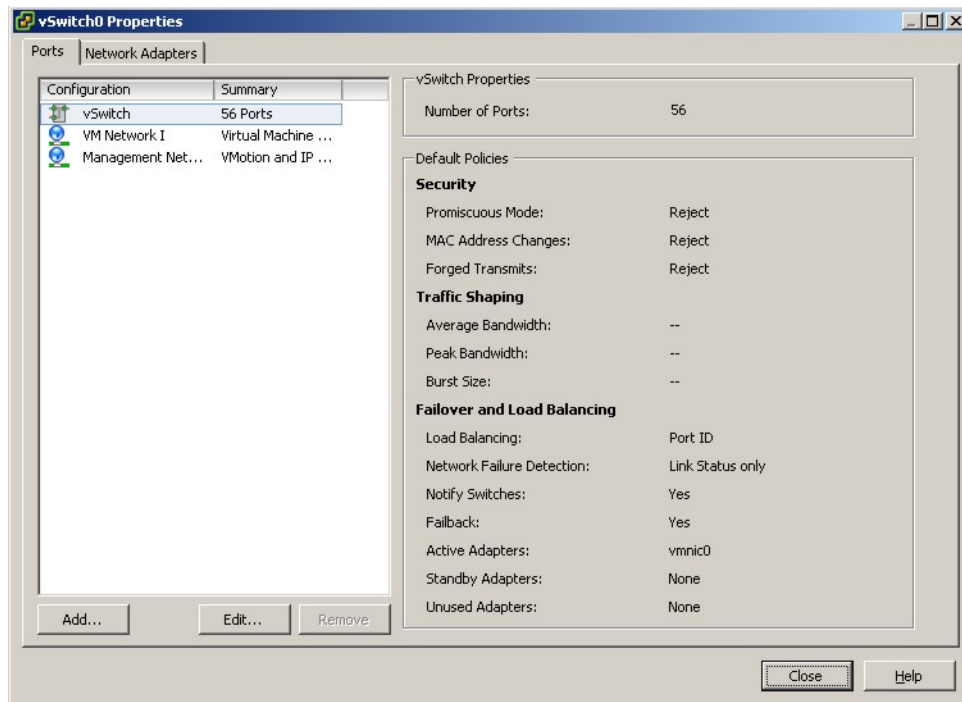


Fig. 14: Edit vSwitch (example)

3. Click on the button *Edit*.
4. Click on the tab *Security*.

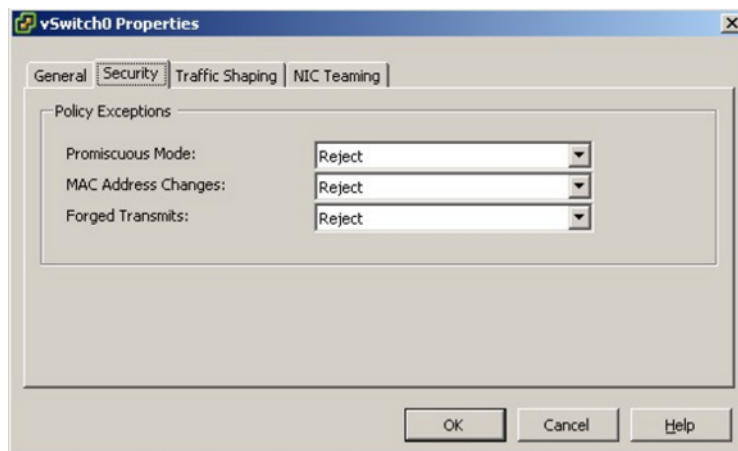


Fig. 15: Define policy exceptions

5. From the drop-down list, select the parameter *Reject* for the following options:
  - *Promiscuous Mode*
  - *MAC Address Changes*
  - *Forged Transmits*
6. Click on the button *OK*.
7. Verify the configuration.



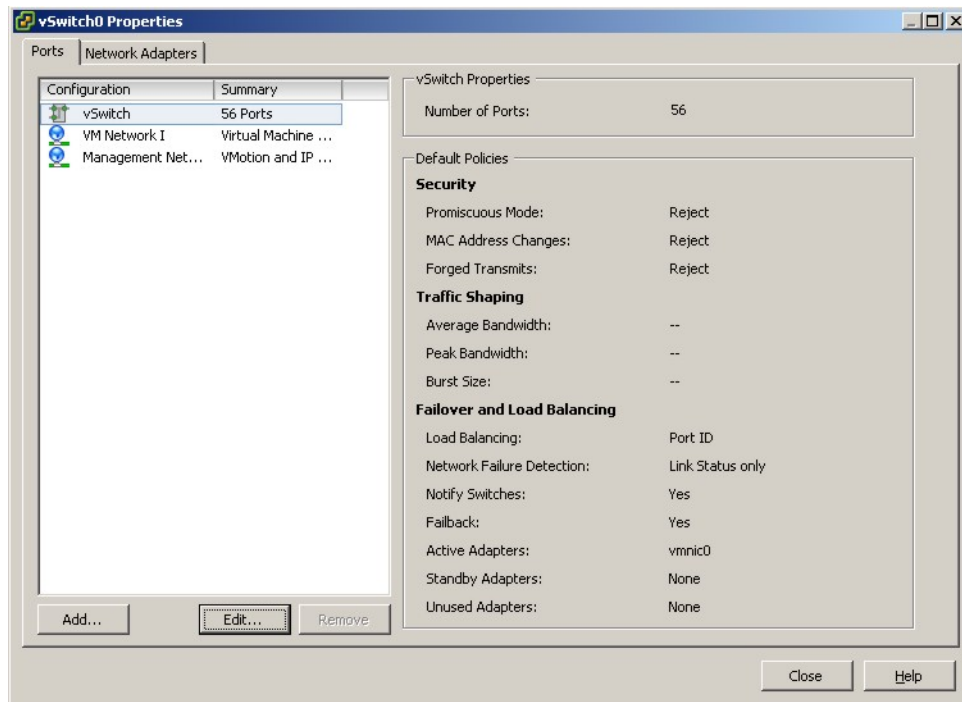


Fig. 16: Verify vSwitch configuration (example)

8. Select the respective virtual network which you have created in one of the previous configuration steps.

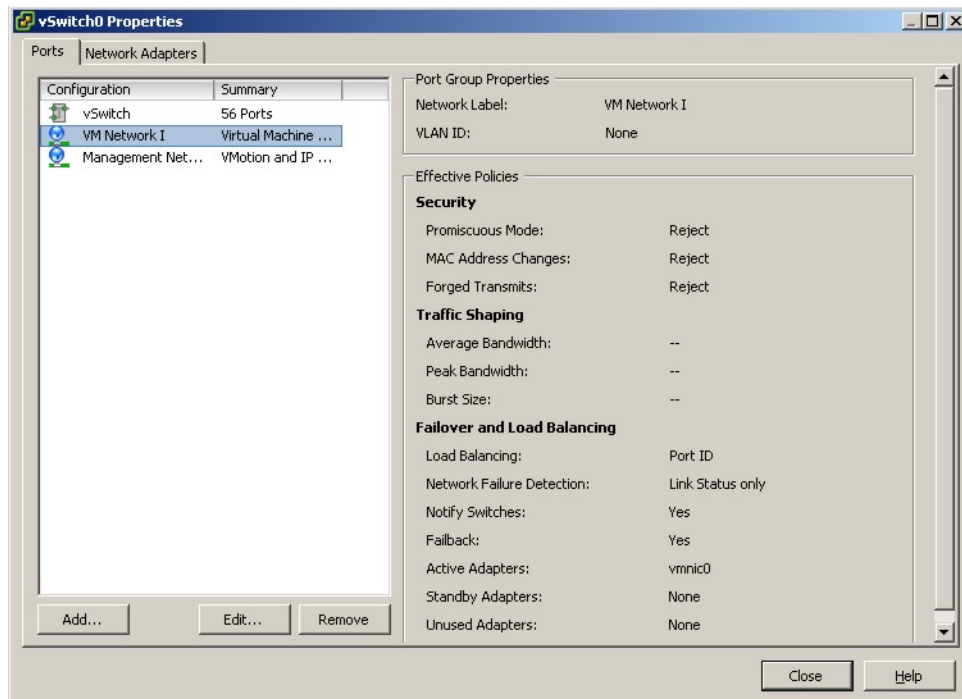


Fig. 17: Edit VM Network I (example)

9. Click on the button *Edit*.
10. Click on the tab *Security*.

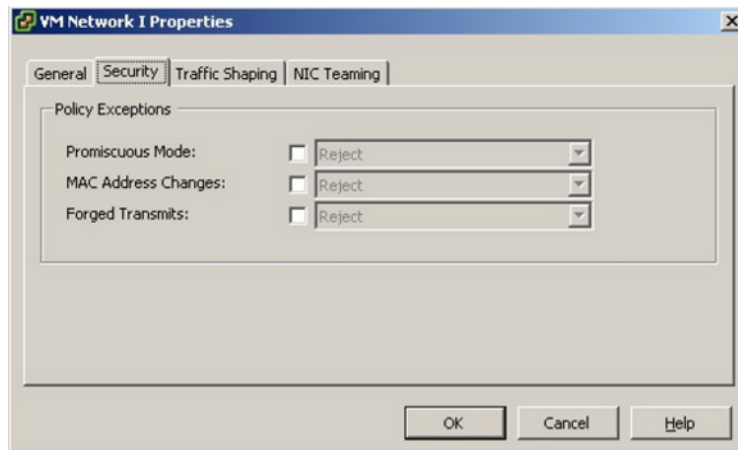


Fig. 18: Define policy exceptions

11. From the drop-down list, select the parameter *Reject* for the following options:

- *Promiscuous Mode*
- *MAC Address Changes*
- *Forged Transmits*

12. Click on the button **OK**.

When all mentioned configuration steps have been carried out successfully, the ASC software can be configured via this interface.

### 6.1.3 Create vSwitch for passive recording

For passive recording by means of the ASC software, a separate vSwitch is required which is created as follows:

1. Log into the vSphere Client and click on the host in the inventory list window.
2. Click on the tab *Configuration*.

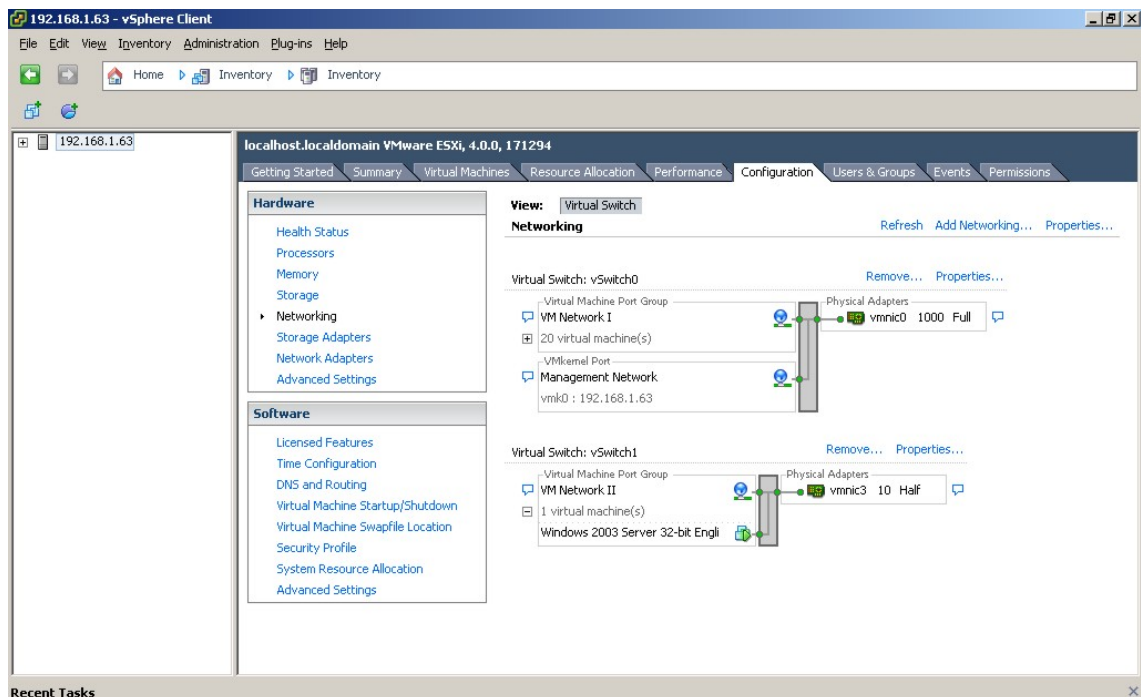


Fig. 19: vSphere Client (example)

3. Click on the menu item *Networking*.
4. Select the view *Virtual Switch*.

5. Click on *Add Networking*.
6. Accept the default connection type *Virtual Machine* and click on the button *Next*.

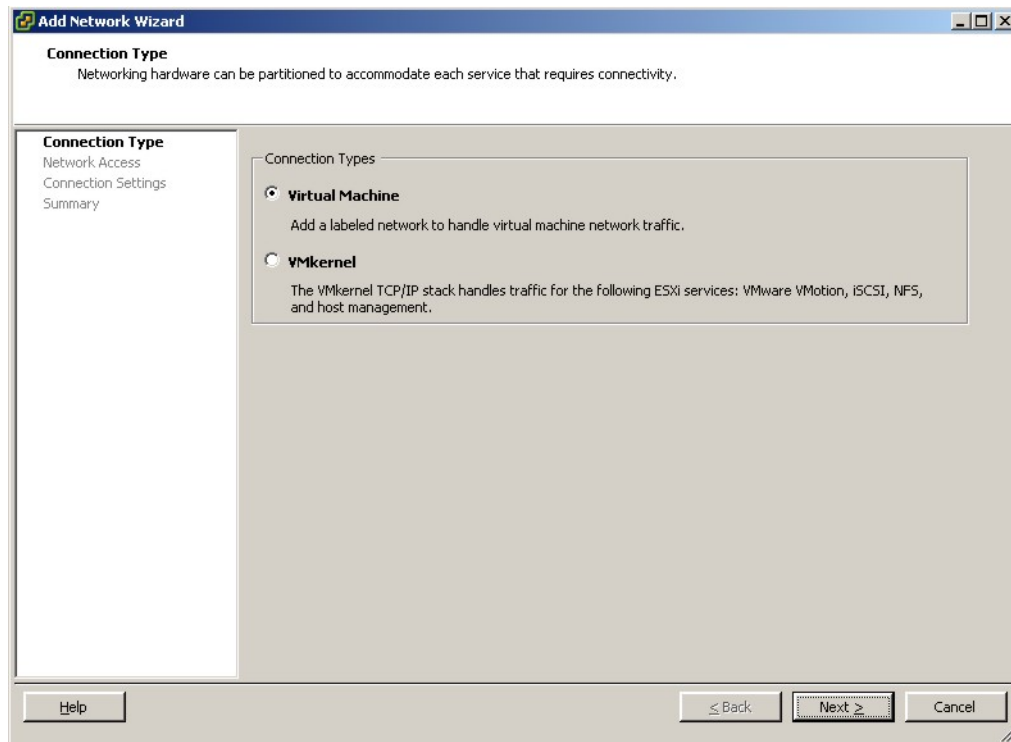


Fig. 20: Add virtual machine

7. Activate the option *Create a virtual switch* and the assigned physical adapters which are supposed to be connected to this vSwitch.

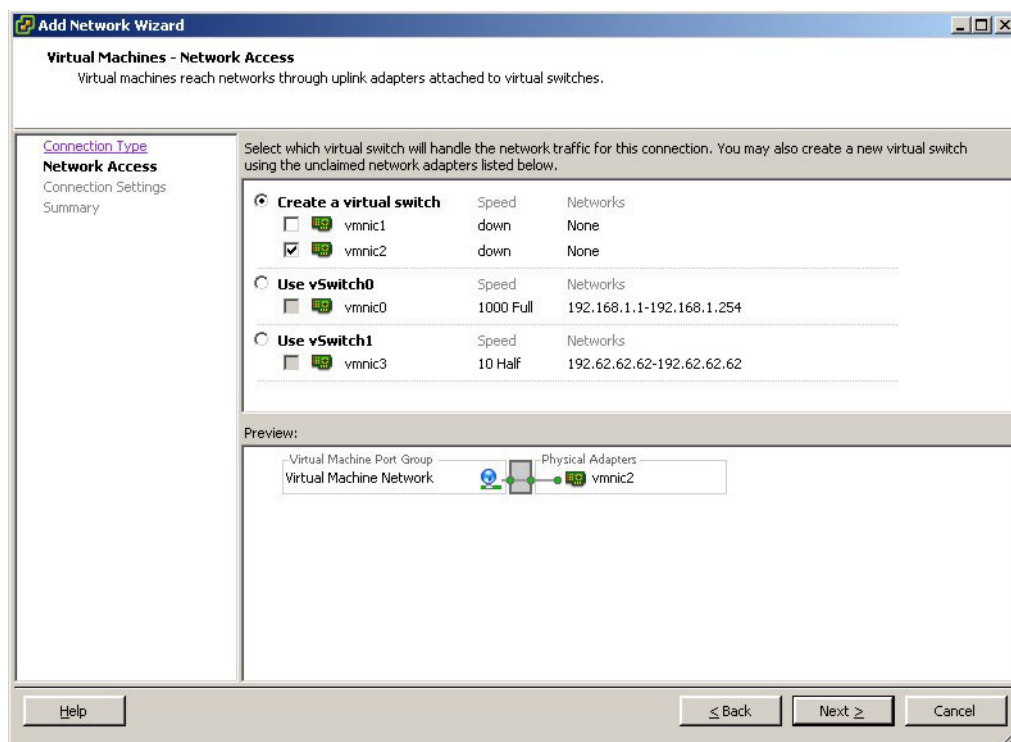


Fig. 21: Create a virtual switch (example)

8. Click on the button *Next*.
9. In the entry field *Network Label*, enter a description of the port group to be created (e. g. VM Network II).

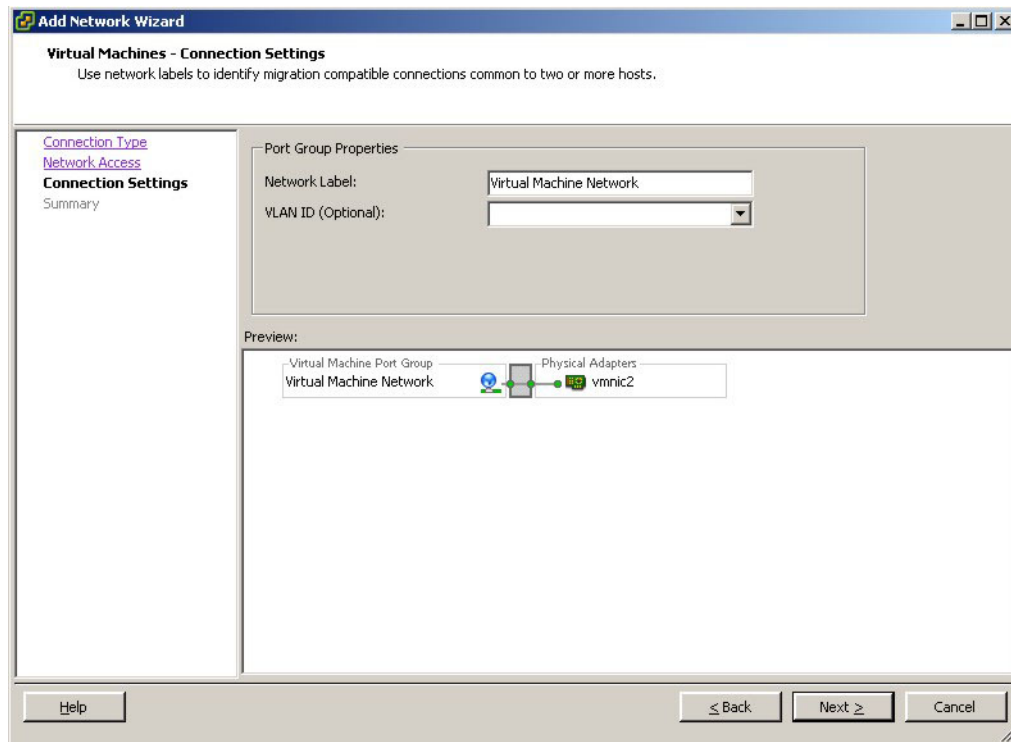


Fig. 22: Enter network label (example)

10. Click on the button *Next*.
11. Verify that the vSwitch has been configured properly.

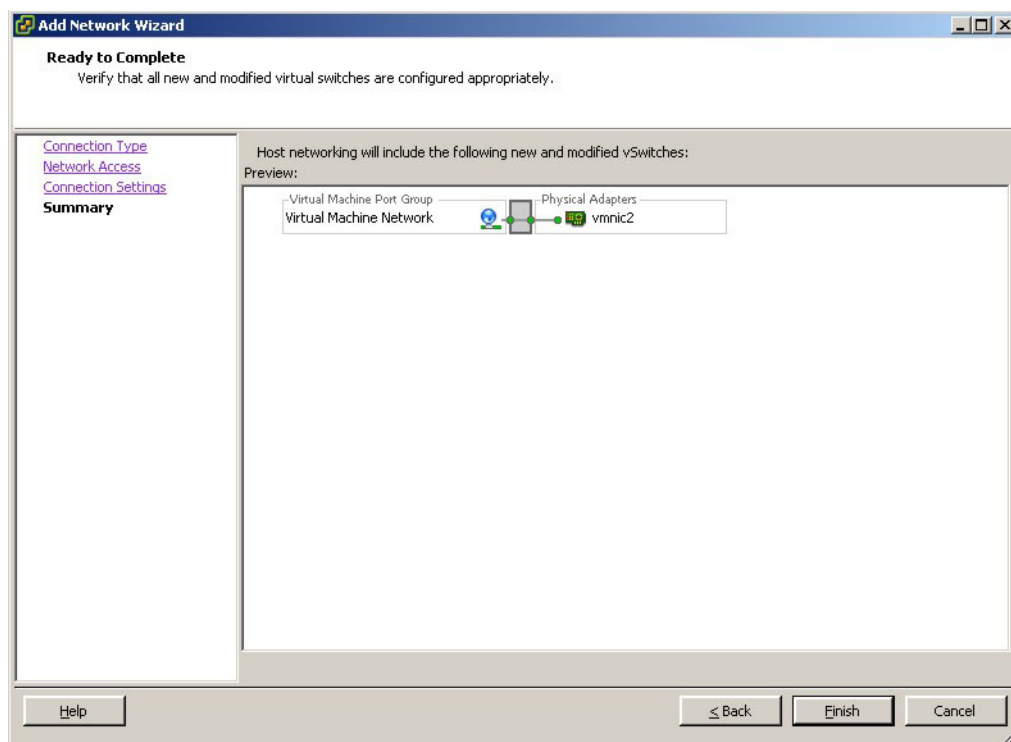


Fig. 23: Configuration ready to finalize (example)

12. Click on the button *Finish*.

When all configuration steps mentioned above have been concluded, the vSwitch has been created successfully and is ready for enhanced configuration.

#### 6.1.4 Configure vSwitch for passive recording

For the new vSwitch for passive recording to be used with the ASC software, the following configuration steps have to be carried out:

1. Click on the *Properties* of the corresponding vSwitch.
2. Click on the configuration *vSwitch*.

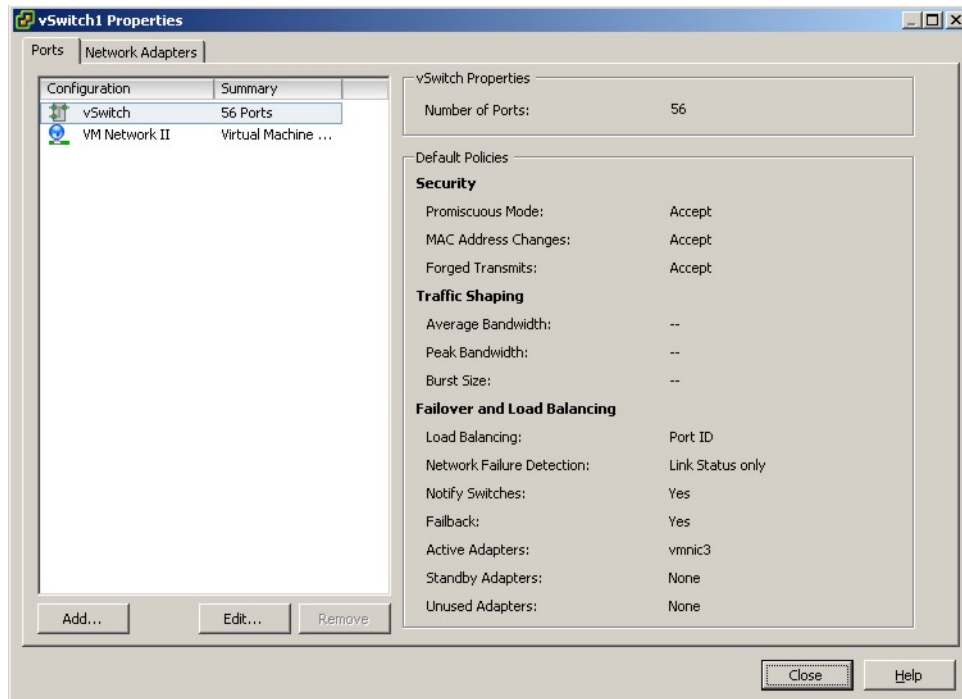


Fig. 24: Edit vSwitch (example)

3. Click on the button *Edit*.
4. Click on the tab *Security*.

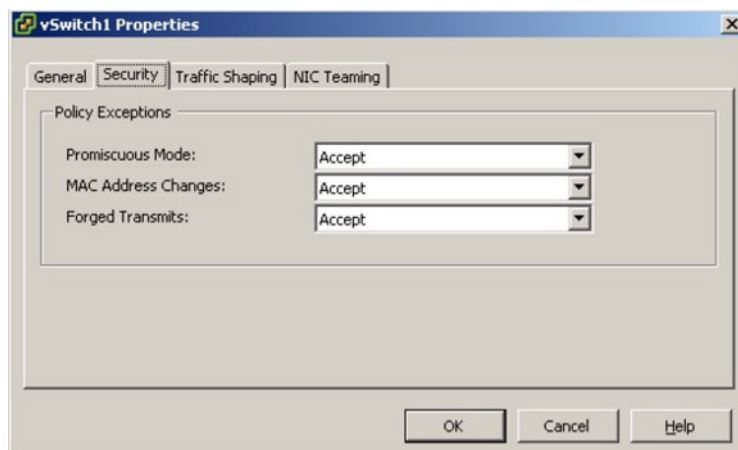


Fig. 25: Define policy exceptions

5. From the drop-down list, select the parameter *Accept* for the following options:
  - *Promiscuous Mode*
  - *MAC Address Changes*
  - *Forged Transmits*
6. Click on the button *OK*.
7. Verify the configuration.

8. Select the respective virtual network which you have created in one of the previous configuration steps.

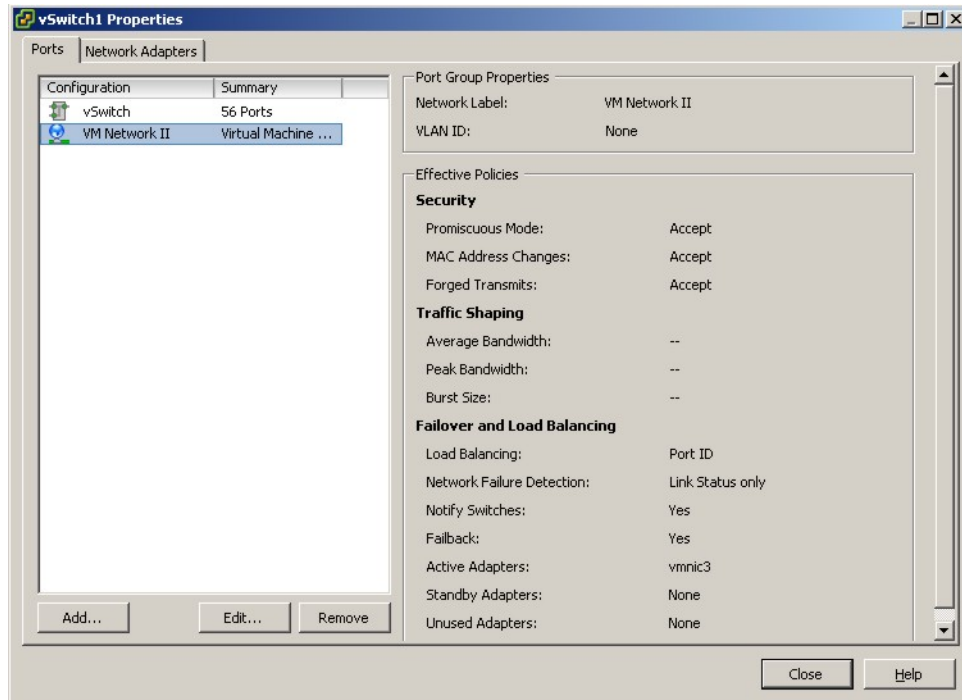


Fig. 26: Edit VM Network II (example)

9. Click on the button *Edit*.
10. Click on the tab *Security*.

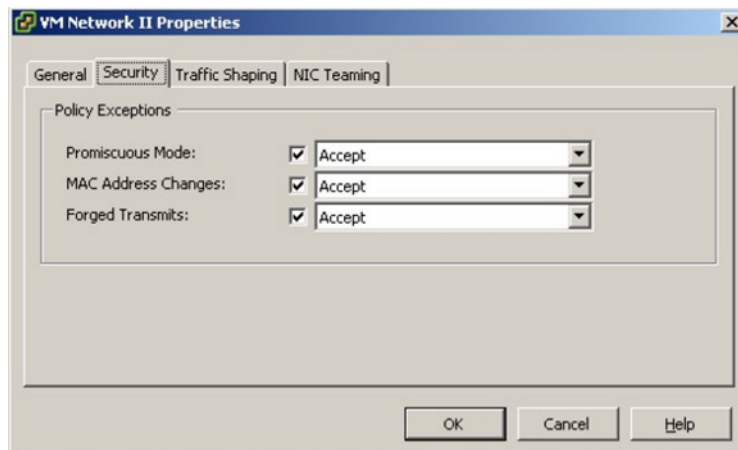


Fig. 27: Define policy exceptions

11. From the drop-down list, select the parameter *Accept* for the following options:
  - *Promiscuous Mode*
  - *MAC Address Changes*
  - *Forged Transmits*
12. Click on the button *OK*.

When all mentioned configuration steps have been carried out successfully, the ASC software can be used for passive recording via this interface.

## 6.2 vCenter client

### 6.2.1 Configuration vCenter standard switches

To communicate with the ASC software for configuration and maintenance purposes, a separate vSwitch is required which is created and configured as follows:

1. Log in to the vCenter client and click on the host in the inventory list window.
2. Click on the tab *Configure*.
3. Click on *Networking > Virtual switches*.
4. Open the virtual switch *Standard Switch: vSwitch8*.
5. Under the virtual switch *Standard Switch: vSwitch8*, click on the button *ADD NETWORKING*.

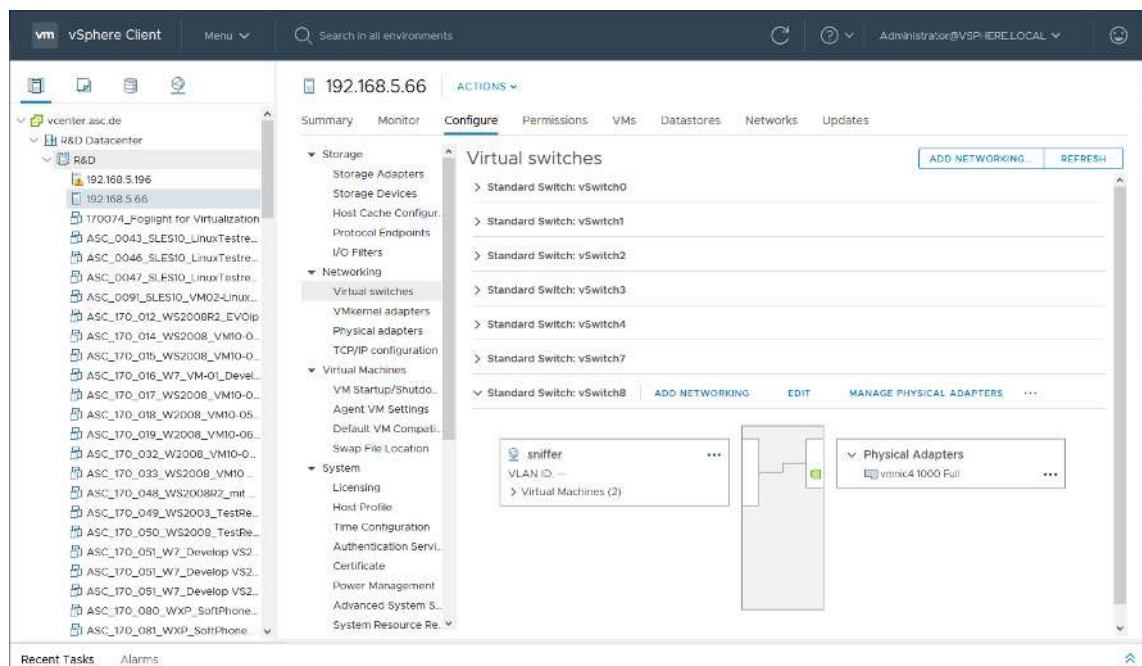


Fig. 28: Configure virtual switches (example)

6. Select the option *Virtual Machine Port Group for a Standard Switch* and click on the button *NEXT*.



192.168.5.66 - Add Networking

1 Select connection type

2 Select target device

3 Connection settings

4 Ready to complete

Select connection type

Select a connection type to create.

---

☐ VMkernel Network Adapter

The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN and host management.

☒ Virtual Machine Port Group for a Standard Switch

A port group handles the virtual machine traffic on standard switch.

☐ Physical Network Adapter

A physical network adapter handles the network traffic to other hosts on the network.

CANCEL

BACK

NEXT

Fig. 29: Add networking (example)

Select either the option *Select an existing standard switch* or the option *New standard switch* as required.

#### Select an existing standard switch

1. Select the option *Select an existing standard switch*.
2. Click on the button *BROWSE*.

192.168.5.66 - Add Networking

✓ 1 Select connection type

2 Select target device

3 Connection settings

4 Ready to complete

Select target device

Select a target device for the new connection.

---

☒ Select an existing standard switch

vSwitch8 BROWSE ...

☐ New standard switch

MTU (Bytes)  ↑ ↓

CANCEL

BACK

NEXT

Fig. 30: Add networking (example)



3. Click on the required switch, e. g. *vSwitch8*.
4. Click on the button *OK*.

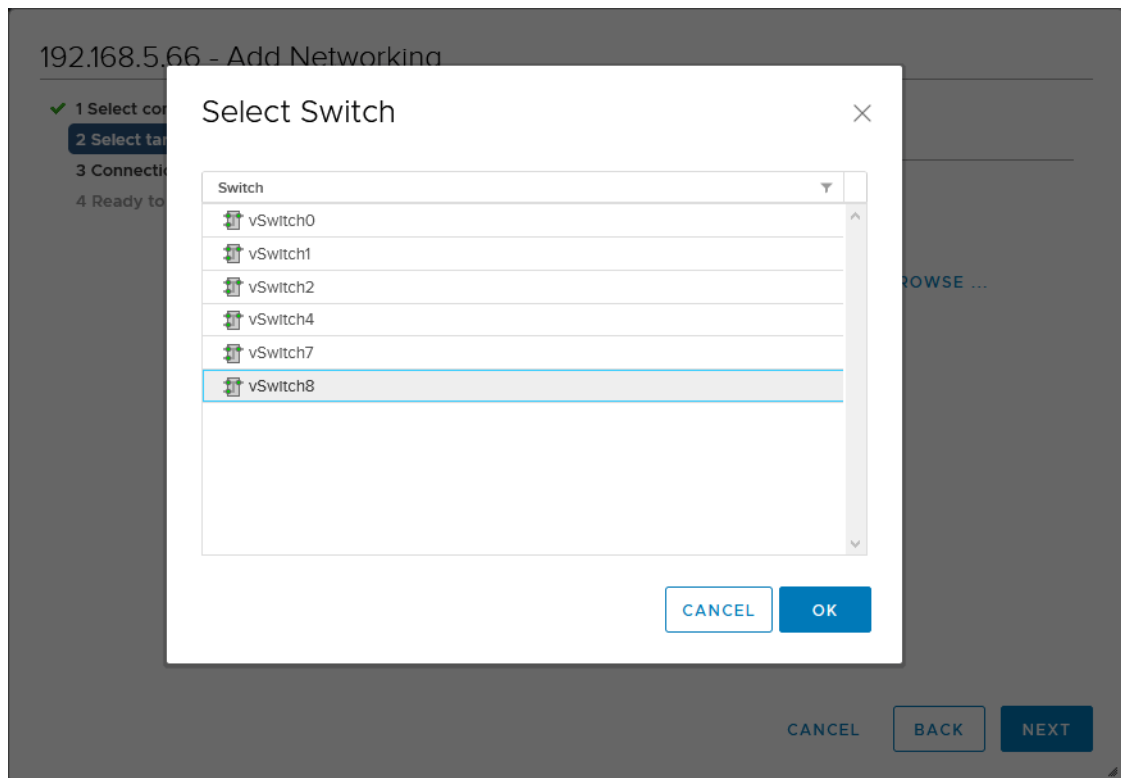


Fig. 31: Select switch (example)

5. Click on the button *NEXT*.
6. In the entry field *Network label*, enter a name for the network, e. g. *VM Network*.
7. Click on the button *NEXT*.

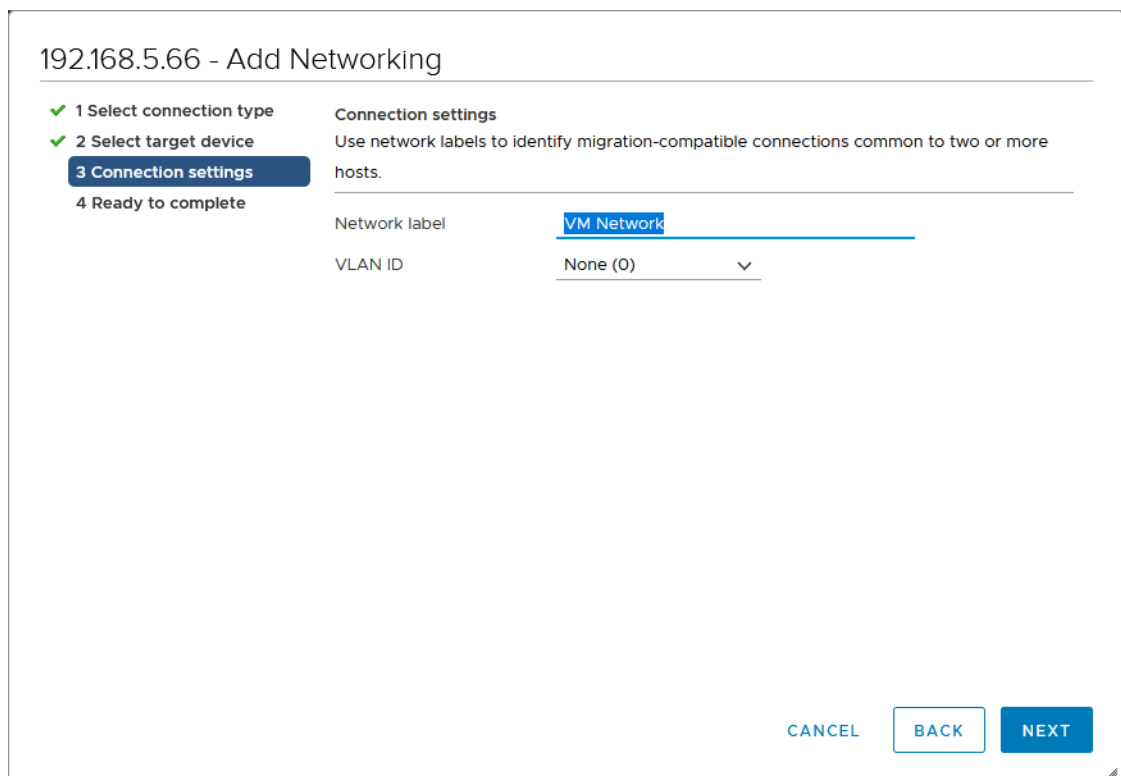
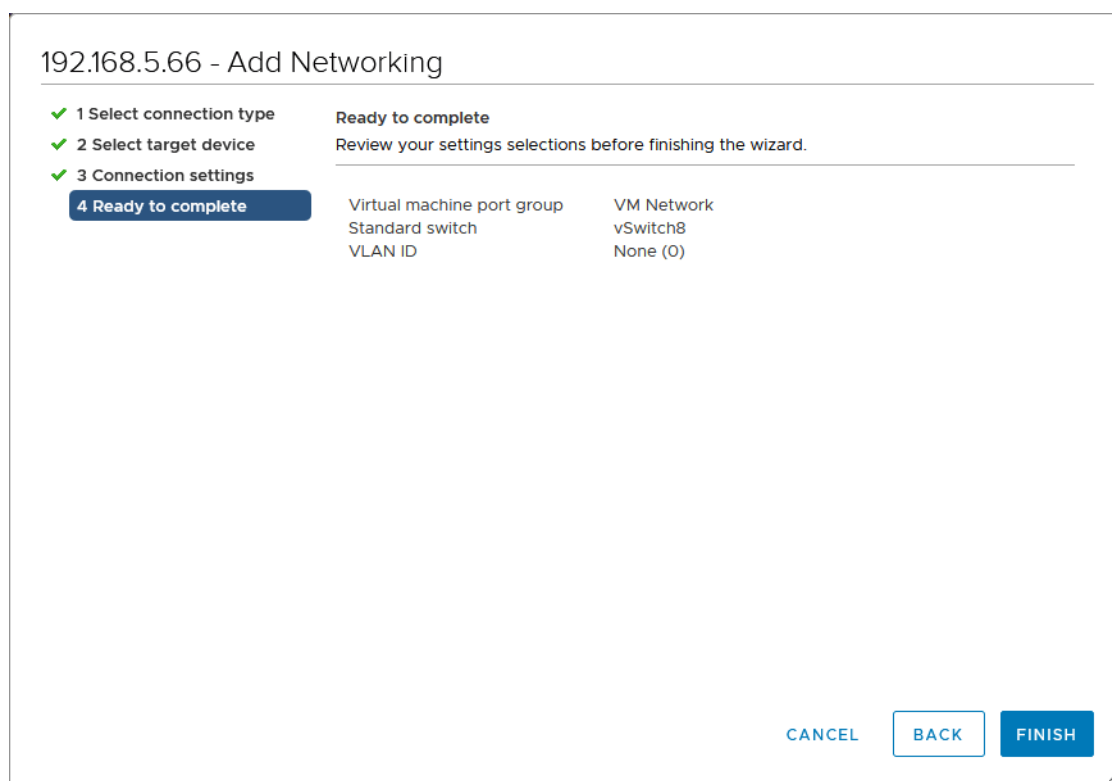


Fig. 32: Add networking (example)

- Click on the button *FINISH*.



192.168.5.66 - Add Networking

- ✓ 1 Select connection type
- ✓ 2 Select target device
- ✓ 3 Connection settings
- 4 Ready to complete**

**Ready to complete**  
Review your settings selections before finishing the wizard.

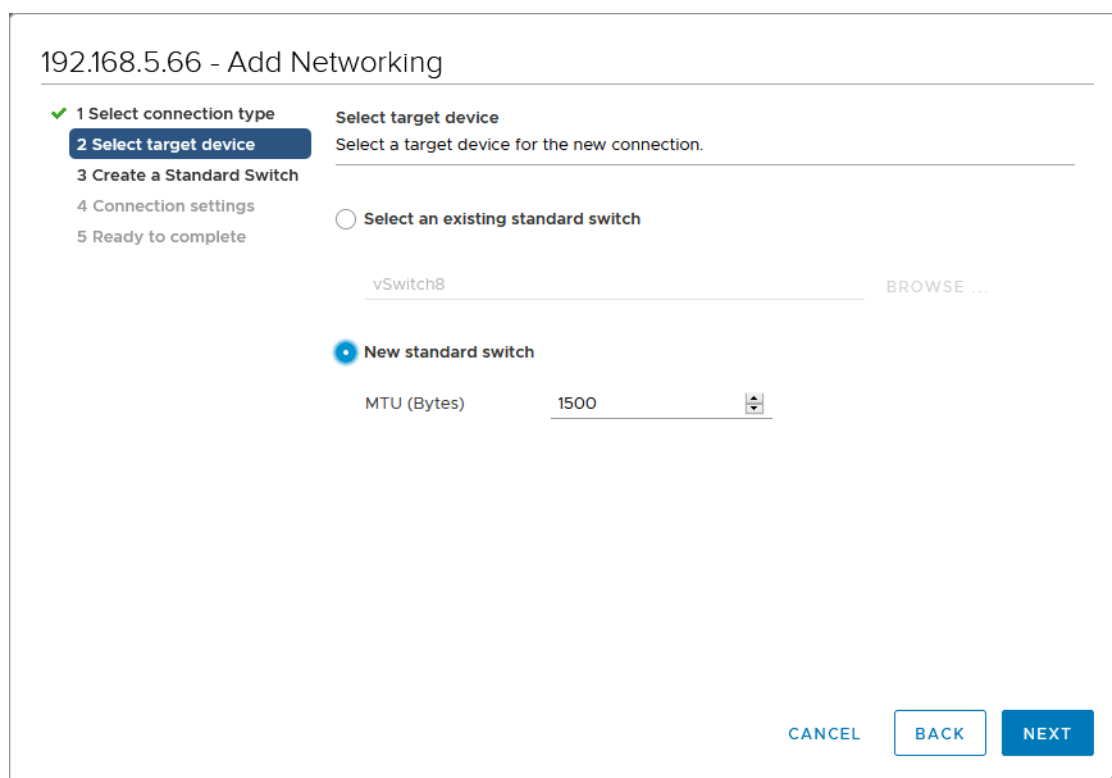
Virtual machine port group	VM Network
Standard switch	vSwitch8
VLAN ID	None (0)

CANCEL BACK FINISH

Fig. 33: Add networking (example)

### New standard switch

- Select the option *New standard switch* and click on the button *NEXT*.



192.168.5.66 - Add Networking

- ✓ 1 Select connection type
- 2 Select target device**
- 3 Create a Standard Switch
- 4 Connection settings
- 5 Ready to complete

**Select target device**  
Select a target device for the new connection.

☐ Select an existing standard switch


vSwitch8 BROWSE ...

☒ **New standard switch**

MTU (Bytes) 1500

CANCEL BACK NEXT

Fig. 34: Add networking (example)

- Click on *Active adapters*.
- Click on the icon  (*Add adapter*).

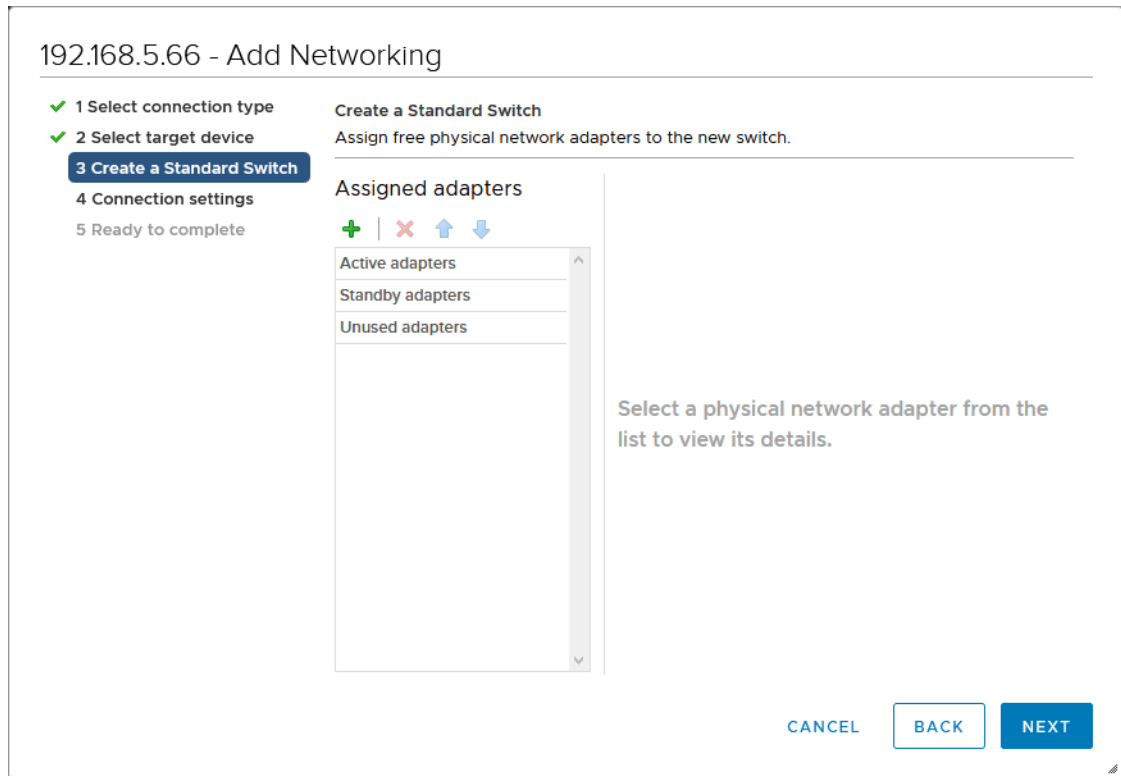


Fig. 35: Add networking (example)

4. Click on the respective network adapter, e. g. *vmnic5*.
5. Click on the button *OK*.

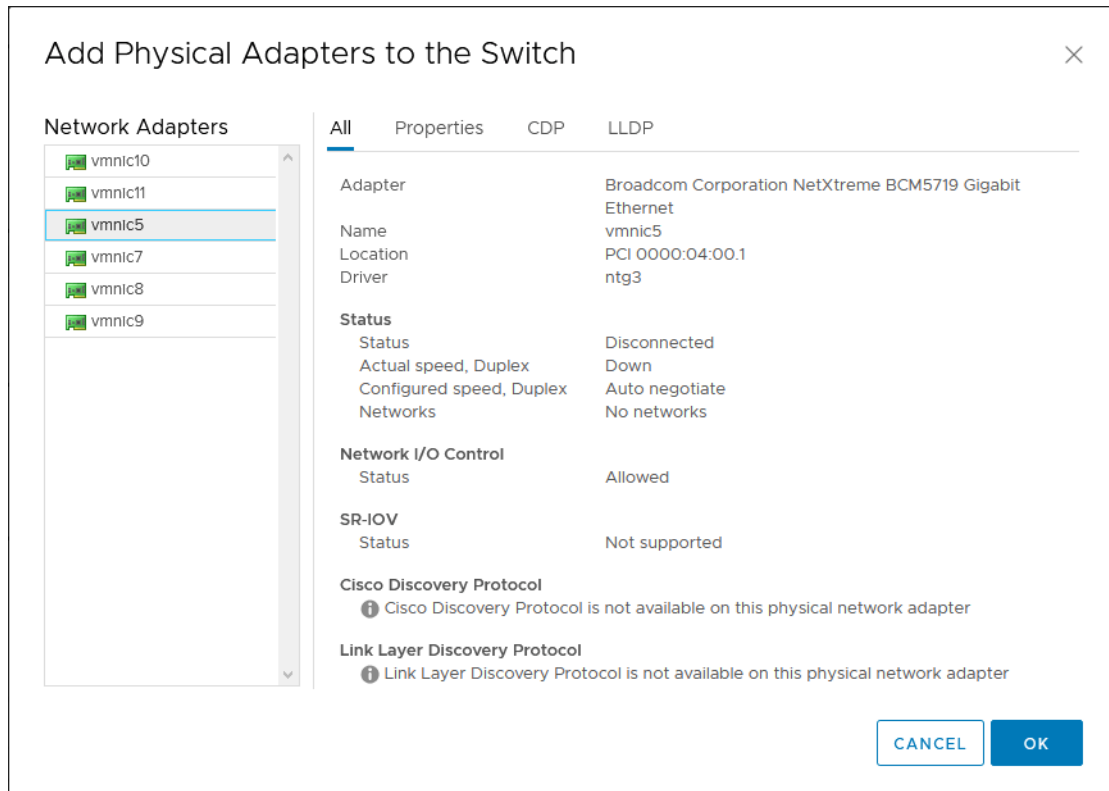


Fig. 36: Add Physical Adapters to the Switch (example)

6. Click on the button *NEXT*.

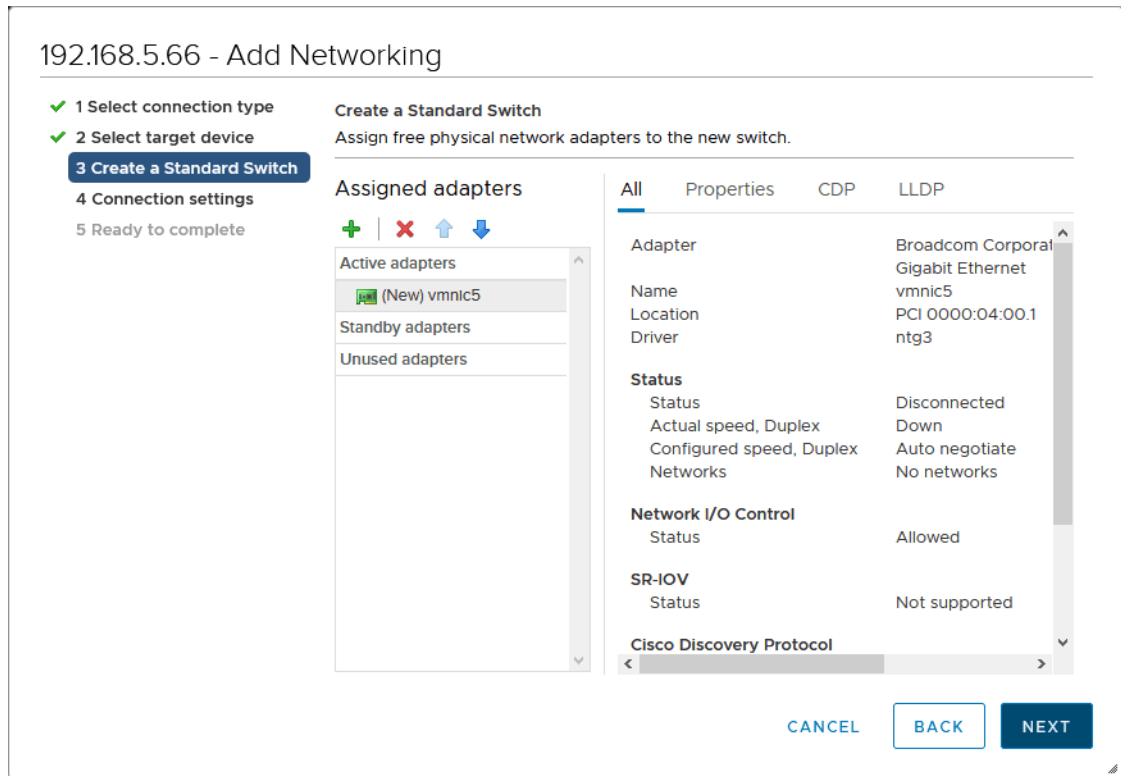


Fig. 37: Add networking (example)

7. Click on the button **OK**.

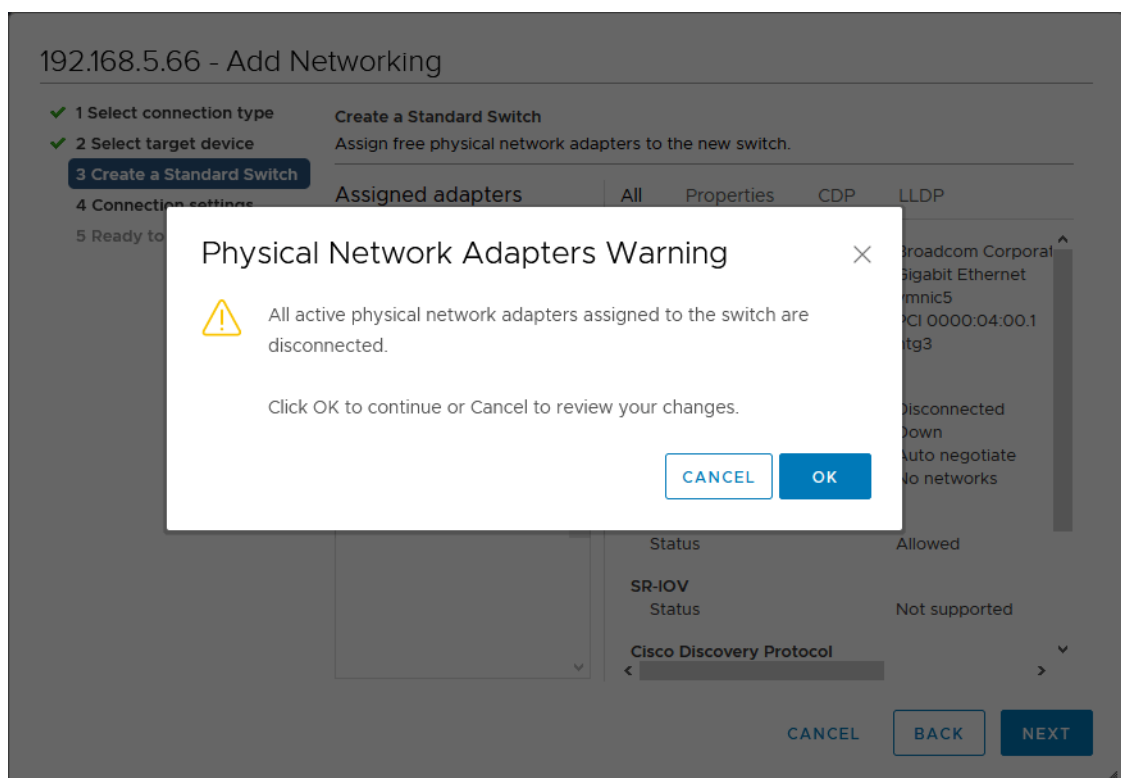


Fig. 38: Physical Network Adapters Warning

8. In the entry field *Network label*, enter a name for the network, e. g. *VM Network*.
9. Click on the button **NEXT**.

192.168.5.66 - Add Networking

- ✓ 1 Select connection type
- ✓ 2 Select target device
- ✓ 3 Create a Standard Switch
- 4 Connection settings**
- 5 Ready to complete

**Connection settings**  
Use network labels to identify migration-compatible connections common to two or more hosts.

Network label	<u>VM Network</u>
VLAN ID	None (0) ▼

CANCEL BACK NEXT

Fig. 39: Add networking (example)

10. Click on the button *FINISH*.

192.168.5.66 - Add Networking

- ✓ 1 Select connection type
- ✓ 2 Select target device
- ✓ 3 Create a Standard Switch
- ✓ 4 Connection settings
- 5 Ready to complete**

**Ready to complete**  
Review your settings selections before finishing the wizard.

New standard switch	vSwitch3
Virtual machine port group	VM Network
Assigned adapters	vmnic5
Switch MTU	1500
VLAN ID	None (0)

CANCEL BACK FINISH

Fig. 40: Add networking (example)

### Configure security settings

- To configure security settings, click on the button *EDIT* under the virtual switch *Standard Switch: vSwitch8*.

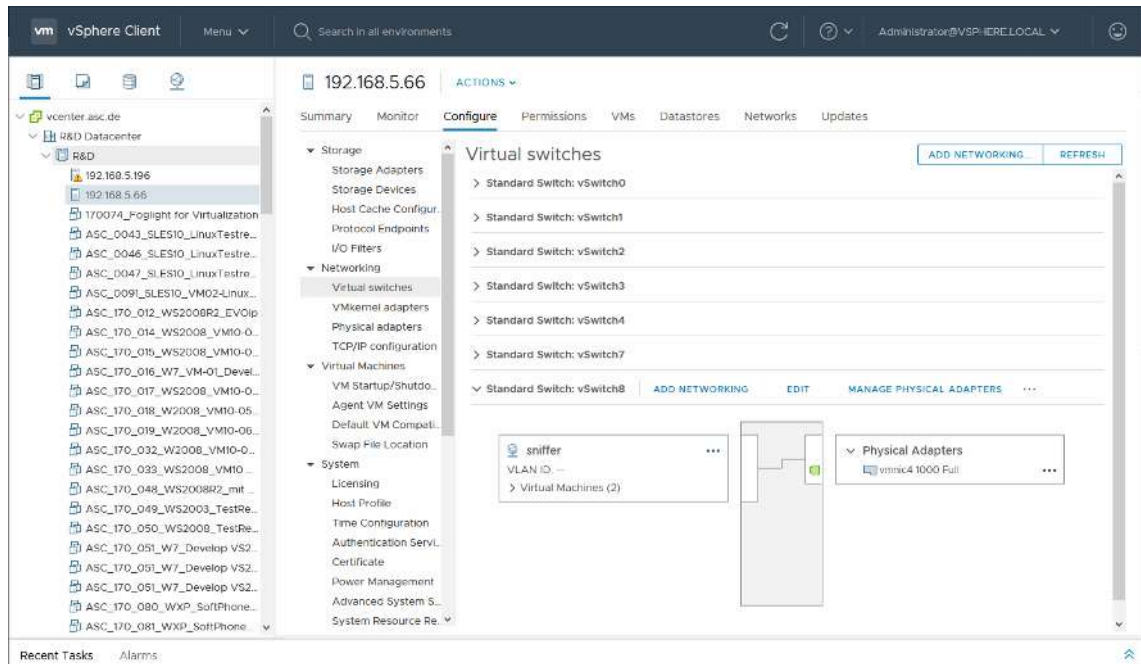


Fig. 41: Configure virtual switches (example)

- Click on the menu item *Security*.

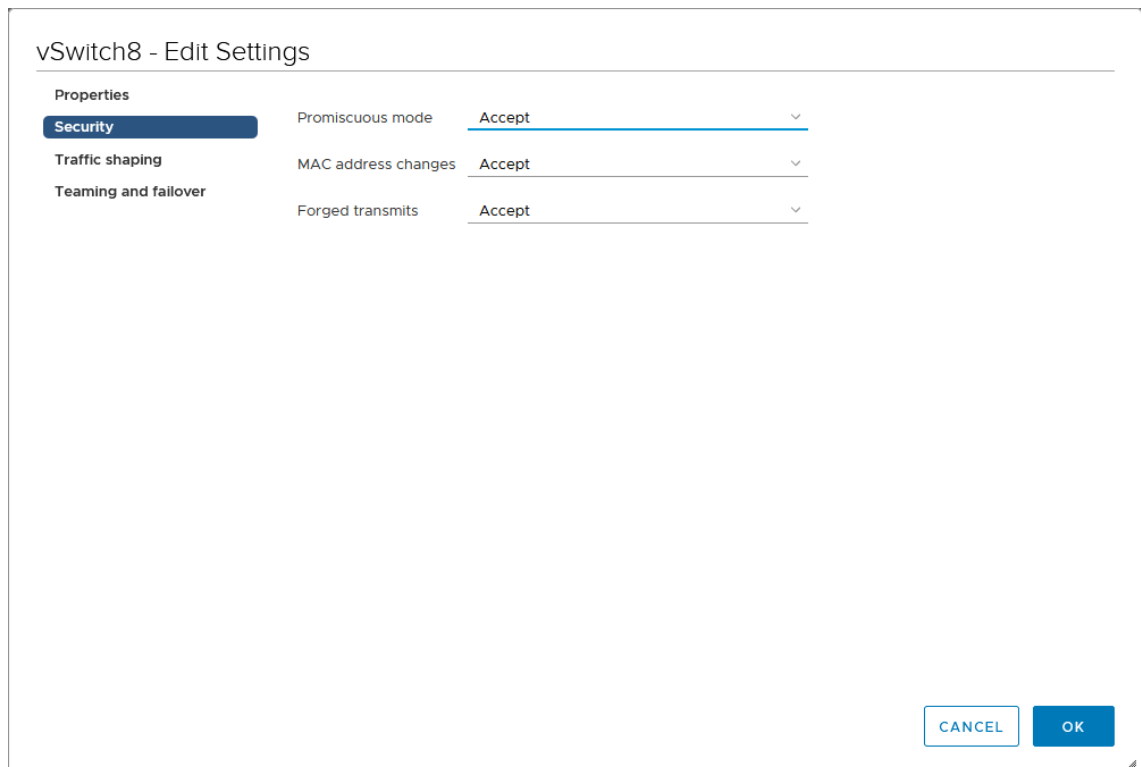


Fig. 42: Edit settings (example)

- From the drop-down list, select the parameter *Accept* for the following options:
  - Promiscuous mode*
  - MAC address changes*
  - Forged transmits*
- Click on the button **OK**.



Please be aware that *Hyper-V Live-Migration* is not supported.

Since *Hyper-V* works with its own [NTP](#) server, you have to use one of the following options to ensure an accurate time synchronization:



- The same *NTP* servers must have been configured for the recording system and for [Hyper-V](#).
- Switch off the [NTP](#) server in the recording system.
- Remove the [NTP](#) server in the recording system.

For further information about the administration of the [NTP](#) servers of the recording system refer to the installation manual *Configuration of servers and recording architectures*.

### When using passive recording solutions

To use *Hyper-V* in promiscuous mode to monitor external data traffic in virtual environments, enter the following commands with your configuration parameters in the Hyper-V console:

#### Examples:

```
Set-VMNetworkAdapter MyVM -PortMirroring Destination
Get-VMNetworkAdapter MyVM | ? MacAddress -eq 'xxxxxxx' | Set-
VMNetworkAdapter MyVM -PortMirroring Destination
$portFeature=Get-VMSystemSwitchExtensionPortFeature -FeatureName "Ethernet
Switch Port Security Settings"
# None = 0, Destination = 1, Source = 2
$portFeature.SettingData.MonitorMode = 2
Add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName MySwitch -
VMSwitchExtensionFeature $portFeature
```

## 8 Configuration System Configuration

To be able to operate the recording system in a virtual environment, you have to adjust the following configurations in the Servers module of the application System Configuration:

1. Activate the VM support, see [chapter "Tab Usage", p. 32](#).
2. Enter the connection data to the dongle, see [chapter "Tab Keystore/Virtualization", p. 33](#).
3. To save the settings, click on the button **Save** in the detail view.

For information about starting and using the application System Configuration refer to the user manual *Usage System Configuration*.

### 8.1 Tab Usage

In this tab, you can configure the purpose of the selected server.

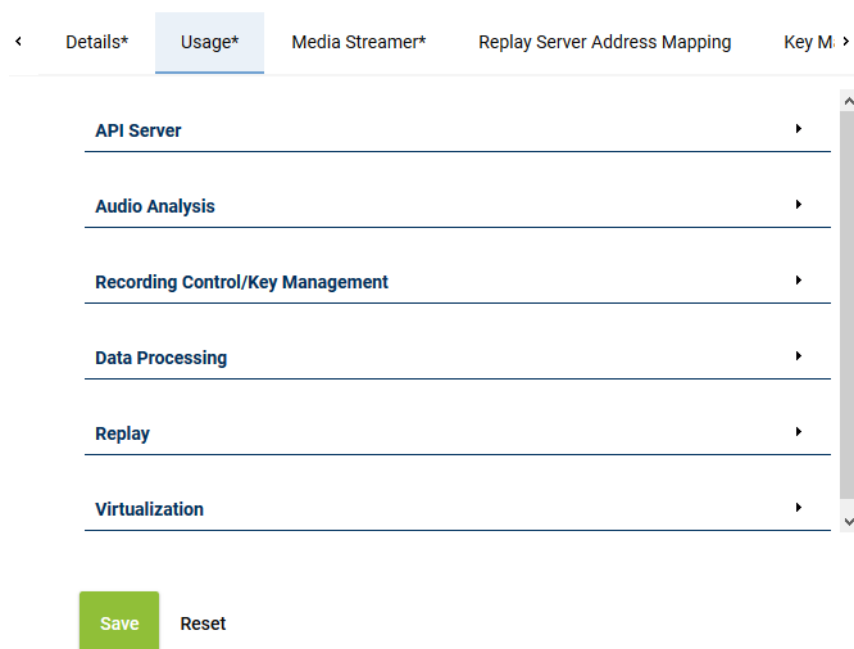


Fig. 43: Servers module - tab Usage

#### Group field Virtualization

1. Open the group field *Virtualization*.



Fig. 44: Group field Virtualization

2. Enter the following parameters:

<b>VM support</b>	<p>If the system has been installed in a virtual environment, you have to activate the VM support.</p> <p><input checked="" type="checkbox"/> = VM support has been activated.</p> <p><input type="checkbox"/> = VM support has not been activated.</p> <p>When activating this functionality, the Licensing module has to authenticate on one of the following instances:</p> <p>Dongle Manager or ASC License Management System</p>
-------------------	---



The system therefore requires a permanent connection either to the ASC License Management System at the ASC headquarters or to a dongle on one of the servers of the system. About the configuration of the connection data, see [chapter "Tab Keystore/Virtualization", p. 33](#).

**NOTICE!** This functionality can only be activated on servers with an Enterprise Core.

**NOTICE!** This function can only be activated if the system has been installed in a virtual environment.



For *virtualization* without an Internet connection, a Trusted License is required.

## 8.2

### Tab Keystore/Virtualization

1. Click on the tab *Keystore/Virtualization* in the detail view.

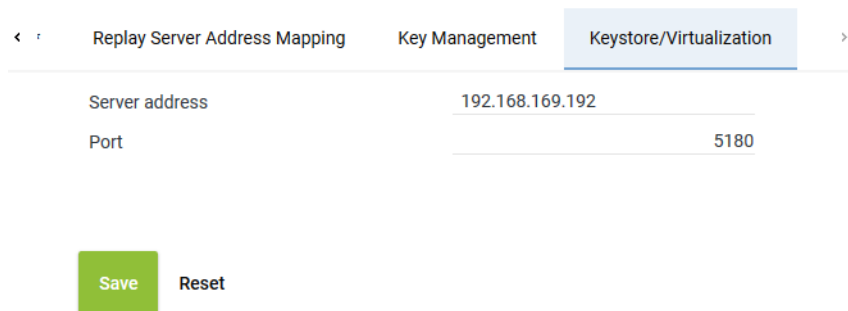
In this tab, you can configure the connection data for the service *DongleMan* for the *neo* key management and for the authentication of the *VM*.



If your system has been installed in a virtualized environment and you are deploying a dongle, the port that the dongle has been plugged in to must have been assigned to the server that the application of the Dongle Manager has been installed on to enable access to the dongle.



For detailed information about neo key management refer to the administration manual *Encryption of recordings*.



Navigation: < Replay Server Address Mapping | Key Management | **Keystore/Virtualization** >

Server address	192.168.169.192
Port	5180




Buttons: Save, Reset

Fig. 45: Servers module - tab Keystore/Virtualization

<b>Server address</b>	<p>Enter the address of the server for this connection.</p> <ul style="list-style-type: none"> <li>If you use the neo key management as well as the virtualization: IP address of the server that the service <i>DongleMan</i> has been installed on.</li> <li>If you use only virtualization, you can authenticate the <i>VM</i> via the ASC License Management System, too. In this case, enter the following address: <i>licensing.asc.de</i></li> <li>If you use only the ASC key management: IP address of the server with the master password database</li> </ul>
<b>Port</b>	<p>Enter the port for the connection.</p> <p>Default value: 5180</p>

## 9 Quick guide

### 9.1 Install and configure Digi AnywhereUSB

- Install drivers:  
Download drivers from homepage and follow setup instructions.
- Establish connection to the VMware server:  
**Windows key > icon  > AnywhereUSB Configuration Utility > Connect.**
- Change connection to the VMware server:  
**Windows key > icon  > AnywhereUSB Configuration Utility > Disconnect > follow setup instructions > Install Drivers > Windows key > icon  > AnywhereUSB Configuration Utility > Connect.**

### 9.2 Create and configure vSwitch for administration

- Create vSwitch:  
Register vSphere Client > in the inventory window on host > **Configuration > Networking > Virtual Switch > Add Networking > Virtual Machine > Next > Create a virtual switch and activate adapter > Next > Enter network label > Next > Finish.**
- Configure vSwitch:  
Select vSwitch > **Properties > vSwitch > Edit > Security > Promiscuous Mode: Reject > MAC Address Changes: Reject > Forged Transmits: Reject > OK > Click on previously created network > Edit > Security > Promiscuous Mode: Reject > MAC Address Changes: Reject > Forged Transmits: Reject > OK.**

### 9.3 Create and configure vSwitch for passive recording

- Create vSwitch:  
Register vSphere Client > in the inventory window on host > **Configuration > Networking > Virtual Switch > Add Networking > Virtual Machine > Next > Create a virtual switch and activate adapter > Next > Enter network label > Next > Finish.**
- Configure vSwitch:  
Select vSwitch > **Properties > vSwitch > Edit > Security > Promiscuous Mode: Accept > MAC Address Changes: Accept > Forged Transmits: Accept > OK > Click on previously created network > Edit > Security > Promiscuous Mode: Accept > MAC Address Changes: Accept > Forged Transmits: Accept > OK.**

### 9.4 Configure virtualization in System Configuration

- Activate VM support:  
**Servers module > Usage > Virtualization > Activate VM support > Save**
- Enter connection data for authentication:  
**Servers module > Keystore/Virtualization > Server address: enter licensing.asc.de or IP address to the server with the dongle enter > Port: port (default 5180) > Save**

## List of figures

Fig. 1	Message informing about successful installation of driver .....	8
Fig. 2	Connect VMware server.....	9
Fig. 3	Disconnect connection .....	9
Fig. 4	Configuration program AnywhereUSB/2 Configuration and Management.....	10
Fig. 5	Change IP address .....	10
Fig. 6	Confirm change .....	11
Fig. 7	Reconnect VMware server .....	11
Fig. 8	Change of the IP address completed successfully .....	11
Fig. 9	vSphere Client (example).....	13
Fig. 10	Add virtual machine.....	13
Fig. 11	Create a virtual switch (example).....	14
Fig. 12	Enter network label (example) .....	14
Fig. 13	Configuration ready to finalize (example).....	15
Fig. 14	Edit vSwitch (example).....	16
Fig. 15	Define policy exceptions .....	16
Fig. 16	Verify vSwitch configuration (example) .....	17
Fig. 17	Edit VM Network I (example) .....	17
Fig. 18	Define policy exceptions .....	18
Fig. 19	vSphere Client (example).....	18
Fig. 20	Add virtual machine.....	19
Fig. 21	Create a virtual switch (example).....	19
Fig. 22	Enter network label (example) .....	20
Fig. 23	Configuration ready to finalize (example).....	20
Fig. 24	Edit vSwitch (example).....	21
Fig. 25	Define policy exceptions .....	21
Fig. 26	Edit VM Network II (example) .....	22
Fig. 27	Define policy exceptions .....	22
Fig. 28	Configure virtual switches (example) .....	23
Fig. 29	Add networking (example) .....	24
Fig. 30	Add networking (example) .....	24
Fig. 31	Select switch (example) .....	25
Fig. 32	Add networking (example) .....	25
Fig. 33	Add networking (example) .....	26
Fig. 34	Add networking (example) .....	26
Fig. 35	Add networking (example) .....	27
Fig. 36	Add Physical Adapters to the Switch (example) .....	27
Fig. 37	Add networking (example) .....	28
Fig. 38	Physical Network Adapters Warning .....	28
Fig. 39	Add networking (example) .....	29
Fig. 40	Add networking (example) .....	29
Fig. 41	Configure virtual switches (example) .....	30

---

Fig. 42	Edit settings (example).....	30
Fig. 43	Servers module - tab Usage .....	32
Fig. 44	Group field Virtualization .....	32
Fig. 45	Servers module - tab Keystore/Virtualization .....	33

---

List of tables

---

## Glossary

### DHCP

---

A Dynamic Host Configuration Protocol allows integrating computers into an existing network without configuring the network interface manually. Necessary information such as IP address, net mask, gateway, name server (DNS) and additionally required settings are distributed dynamically. (Source: Wikipedia 5th April 2017)

### NTP

---

Network Time Protocol NTP is a standard for the synchronization of clocks in computer systems via packet-based communication networks. NTP uses the connectionless transport protocol UDP. It has been developed with the objective to guarantee reliable time verification across networks with variable packet runtime. (Source: Wikipedia 12th June 2018)

### USB

---

Universal Serial Bus

### VM

---

Virtual machine