FusionHub User Manual and Installation Guide

SpeedFusion Virtual Appliance

October 2023

Table of Contents

1. Purpose

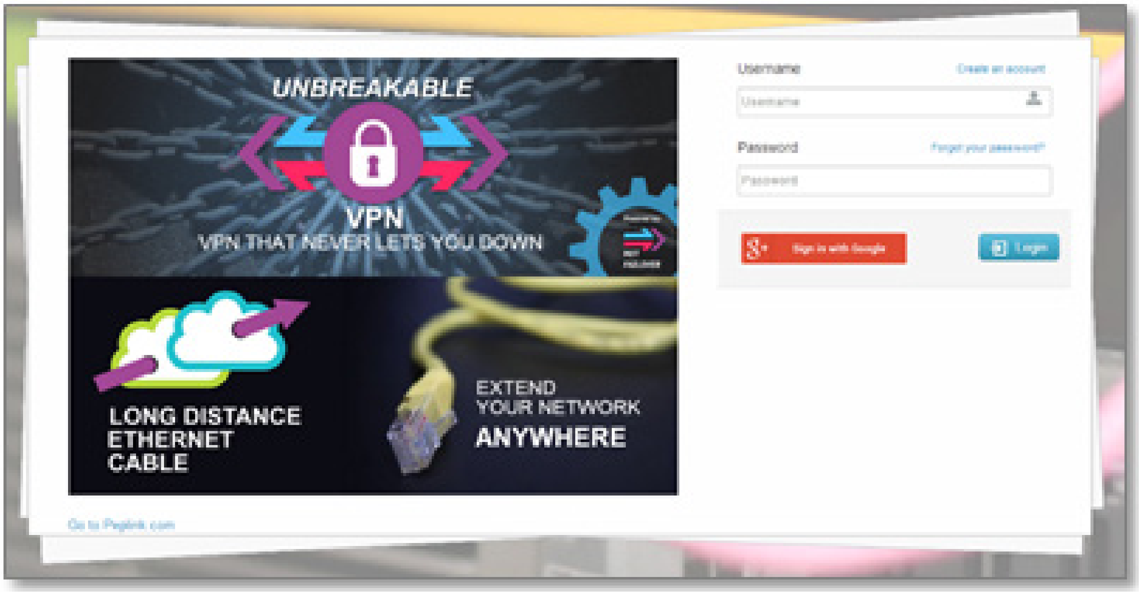
This manual is a step-by-step guide to building a Peplink FusionHub server.

2. FusionHub License

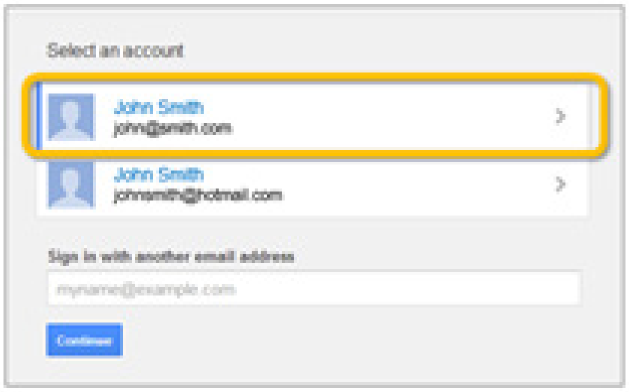
2.1. FusionHub License Generation

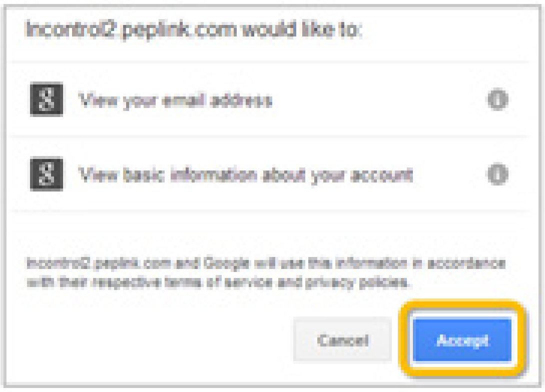
If you already have set up an InControl 2 account, please skip to step 5.

1. To obtain FusionHub evaluation license information and download the FusionHub ISO file from InControl 2, first sign in.



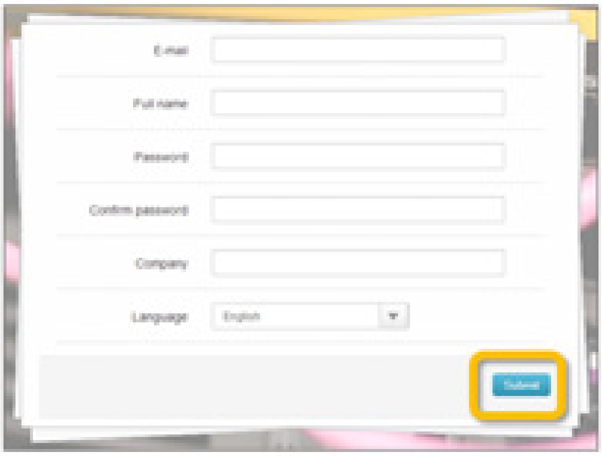
To sign in with Gmail, click **Sign in with Google**, choose your account, and then grant InControl 2 permissions.

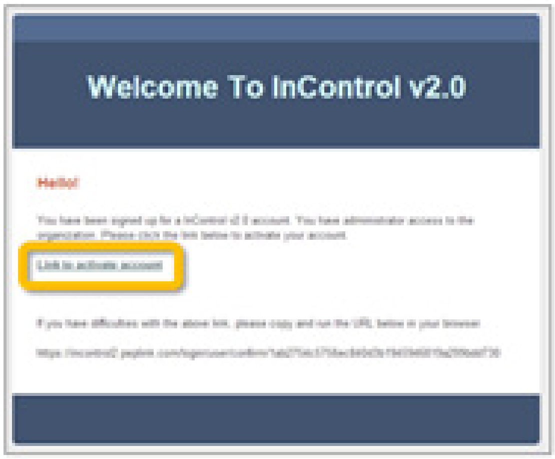



Incontrol2.peplink.com would like to:
View your email address
View basic information about your account
Cancel
Accept

Incontrol2.peplink.com and Google will use this information in accordance with their respective terms of service and privacy policies.

To sign in without Gmail, click **Login** and enter your information. Next, click the link found in your confirmation email. Return to the first screen to enter your username and password.





Welcome To InControl v2.0

Hello!

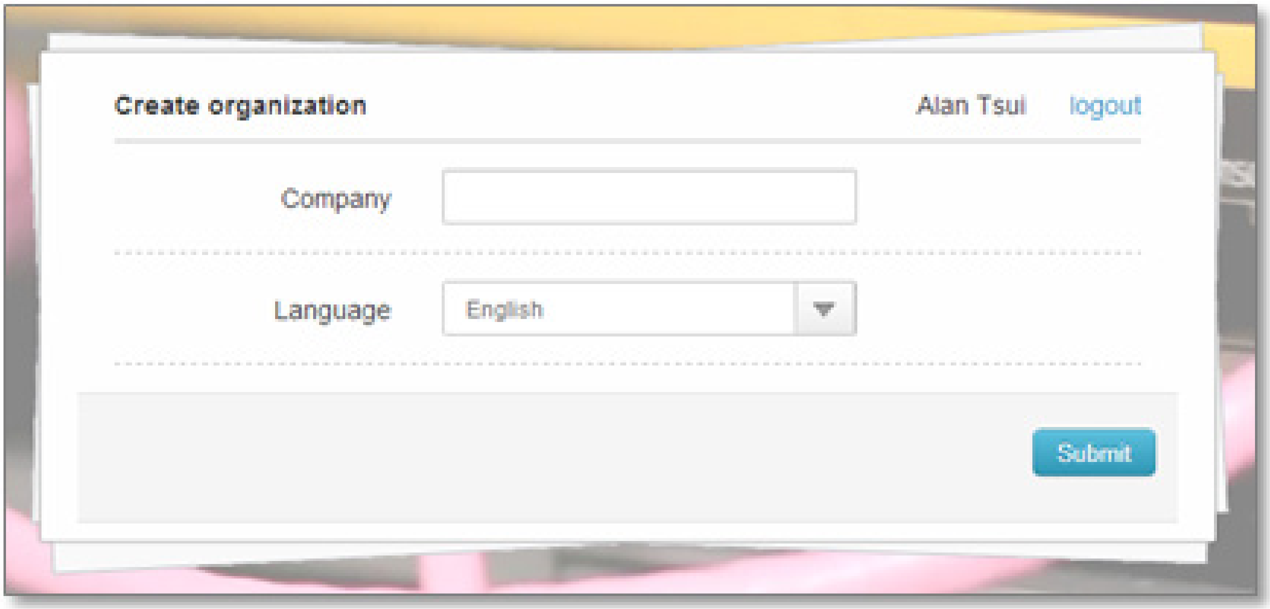
You have been signed up for a InControl v2.0 account. You have administrator access to the organization. Please click the link below to activate your account.

Link to activate account

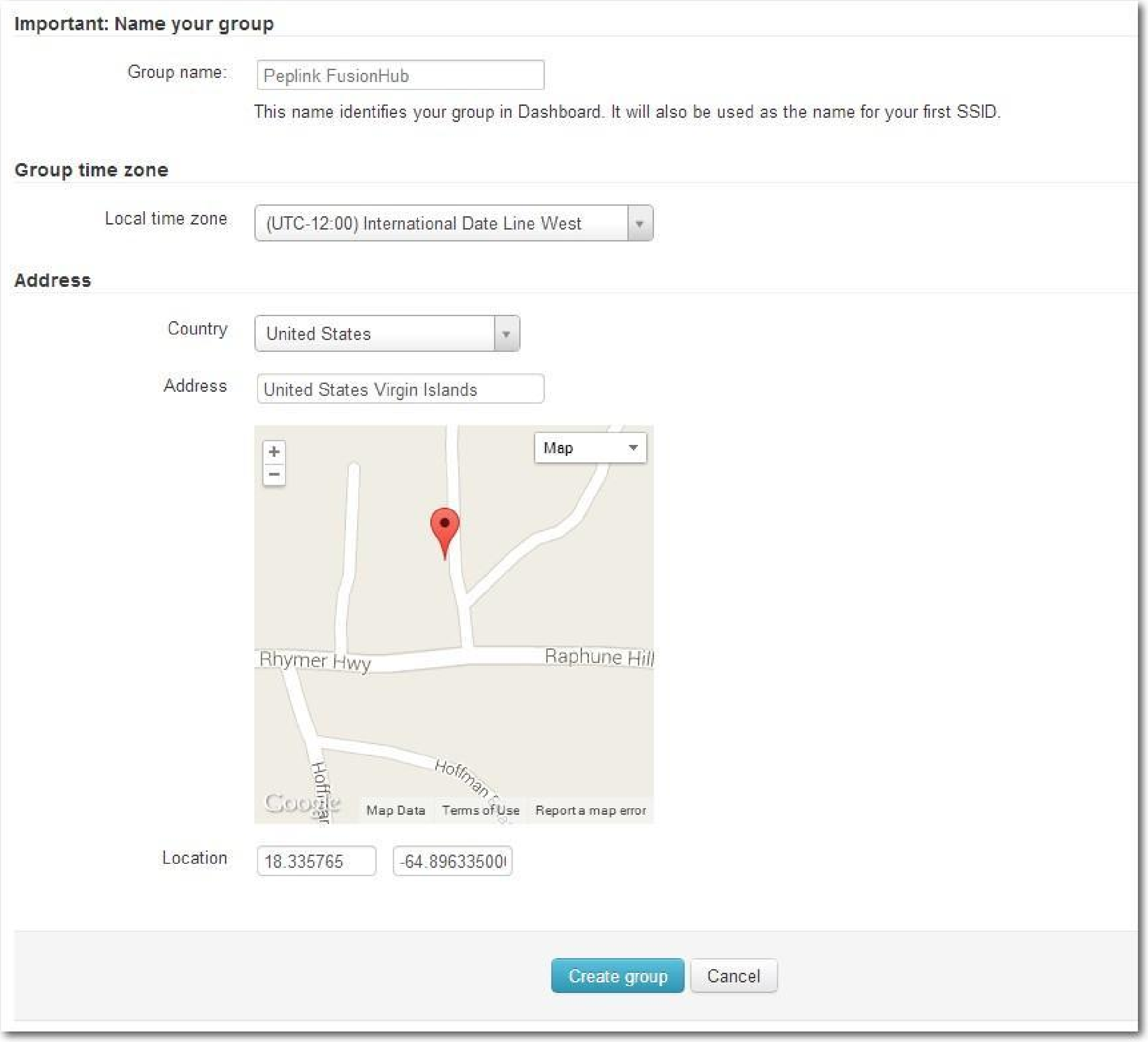
If you have difficulties with the above link, please copy and run the URL below in your browser:

https://incontrol2.peplink.com/login/user/confirm/[illegible]

2. Once you successfully login, InControl 2 will prompt you to name your organization and choose your language.



3. Name your group, choose a local time zone, and specify your location. Click **Create group** to finish.



Important: Name your group

Group name: Peplink FusionHub

This name identifies your group in Dashboard. It will also be used as the name for your first SSID.

Group time zone

Local time zone: (UTC-12:00) International Date Line West

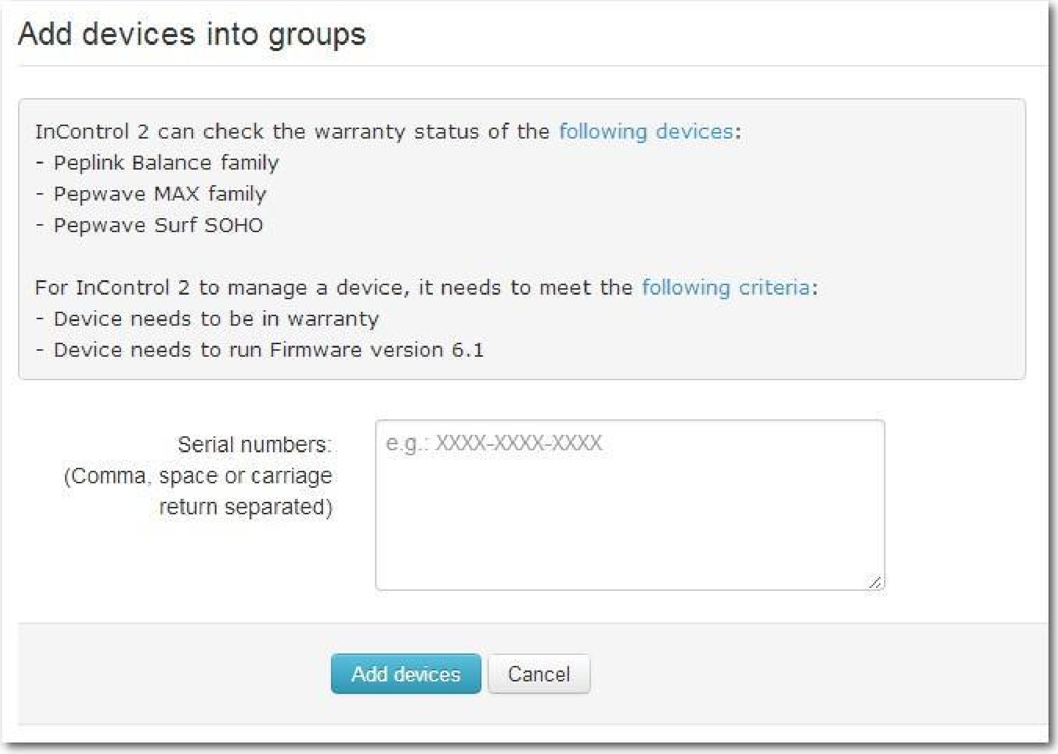
Address

Country: United States

Address: United States Virgin Islands

Location: 18.335765 -64.89633500(

4. On the **Add devices into groups** dialog, click **Cancel** to skip this step and create the group.



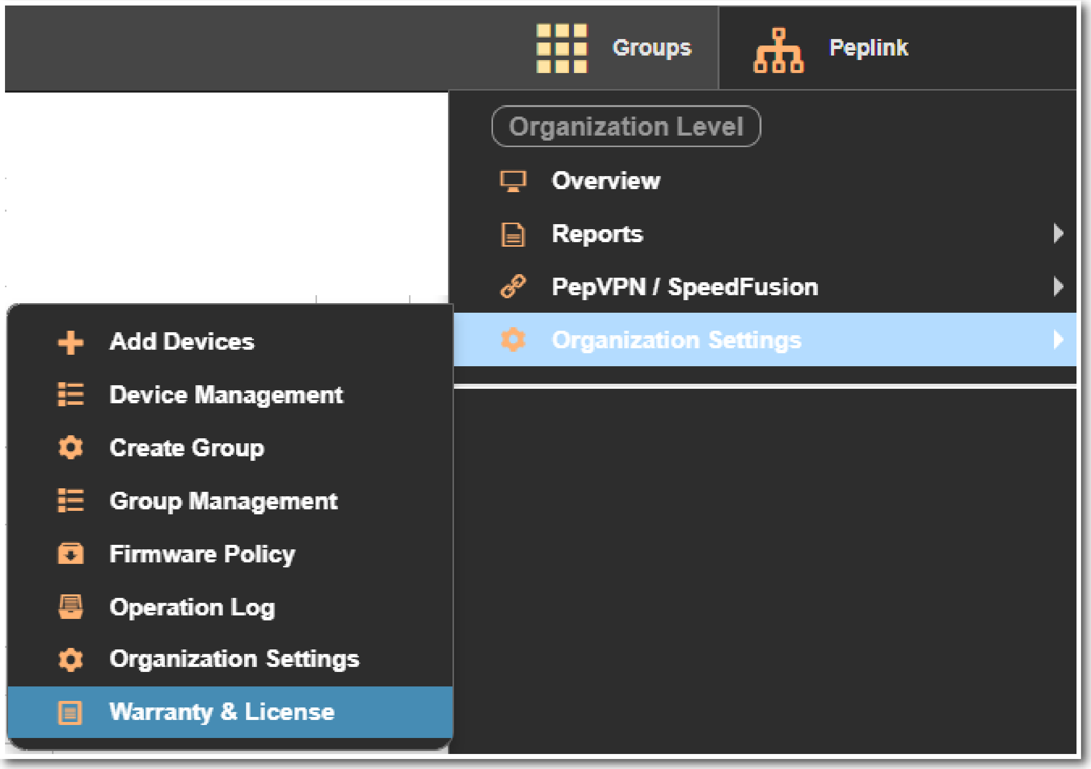
Add devices into groups

InControl 2 can check the warranty status of the following devices:
- Peplink Balance family
- Pepwave MAX family
- Pepwave Surf SOHO

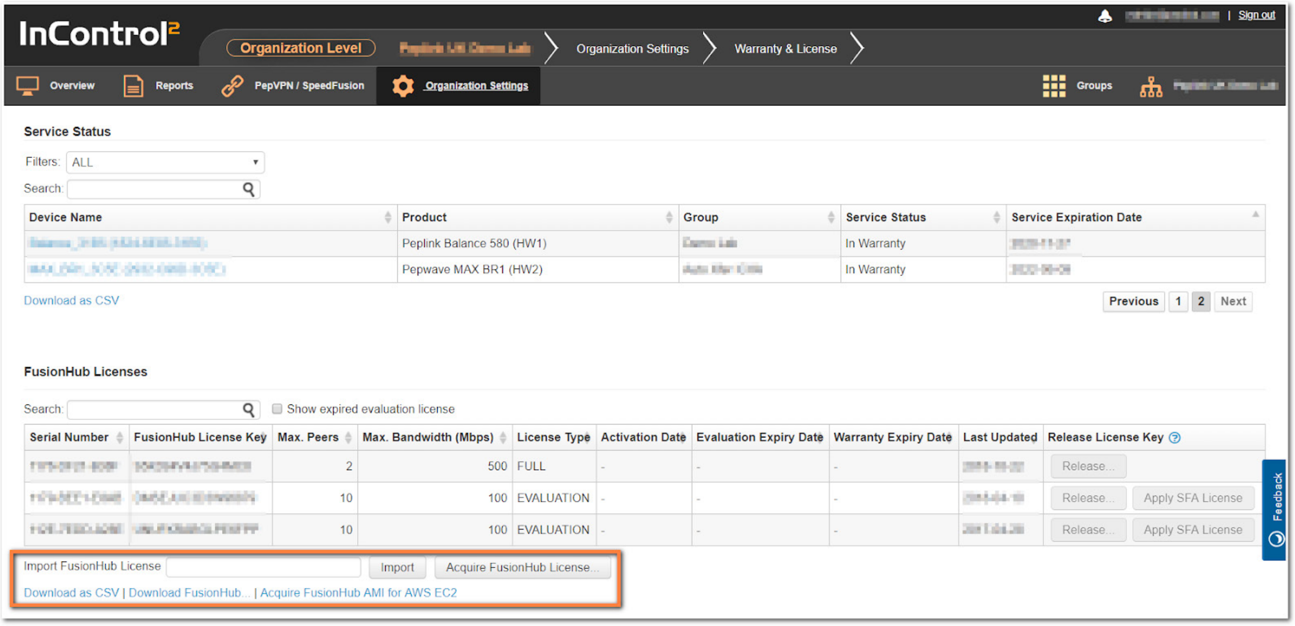
For InControl 2 to manage a device, it needs to meet the following criteria:
- Device needs to be in warranty
- Device needs to run Firmware version 6.1

Serial numbers: (Comma, space or carriage return separated) e.g.: XXXX-XXXX-XXXX

5. To obtain an evaluation license, navigate to **Organization>Settings>Warranty & License**.



6. On the “Warranty Status” screen, click the **Acquire FusionHub License** button.



Service Status

Filters: ALL

Search:

Device Name	Product	Group	Service Status	Service Expiration Date
[redacted]	Peplink Balance 580 (HW1)	[redacted]	In Warranty	[redacted]
[redacted]	Pepwave MAX BR1 (HW2)	[redacted]	In Warranty	[redacted]

Download as CSV

Previous 1 2 Next

FusionHub Licenses

Search: □ Show expired evaluation license

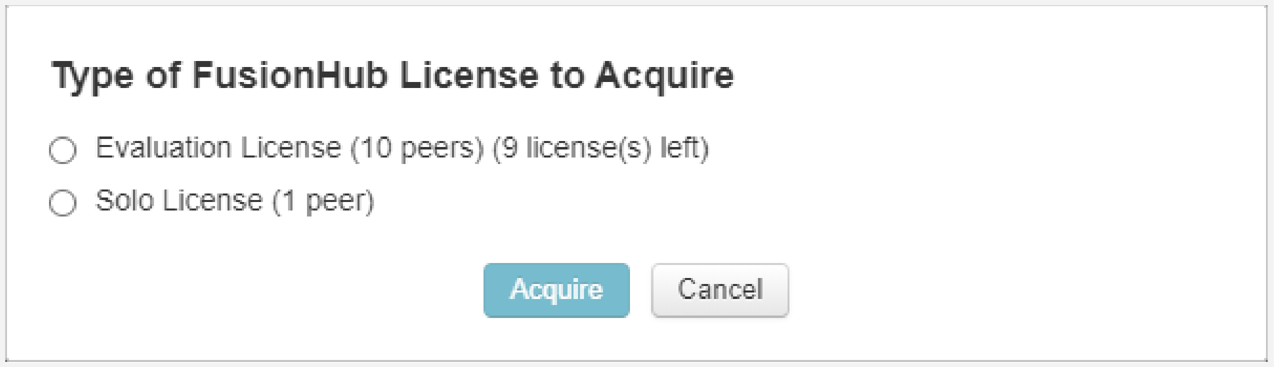
Serial Number	FusionHub License Key	Max. Peers	Max. Bandwidth (Mbps)	License Type	Activation Date	Evaluation Expiry Date	Warranty Expiry Date	Last Updated	Release License Key
[redacted]	[redacted]	2	500	FULL	-	-	-	[redacted]	Release...
[redacted]	[redacted]	10	100	EVALUATION	-	-	-	[redacted]	Release... Apply SFA License
[redacted]	[redacted]	10	100	EVALUATION	-	-	-	[redacted]	Release... Apply SFA License

Import FusionHub License [ ] Import | Acquire FusionHub License...

Download as CSV | Download FusionHub... | Acquire FusionHub AMI for AWS EC2

To download the FusionHub, click the **Download FusionHub** button located below the **Acquire FusionHub License** button.
Alternatively you can import an existing FusionHub License Key or acquire a FusionHub Amazon Machine Image for AWS EC2.

After selecting the **Acquire FusionHub License Button** a window pops up which allows you to select a temporary Evaluation License or a permanent Solo License.



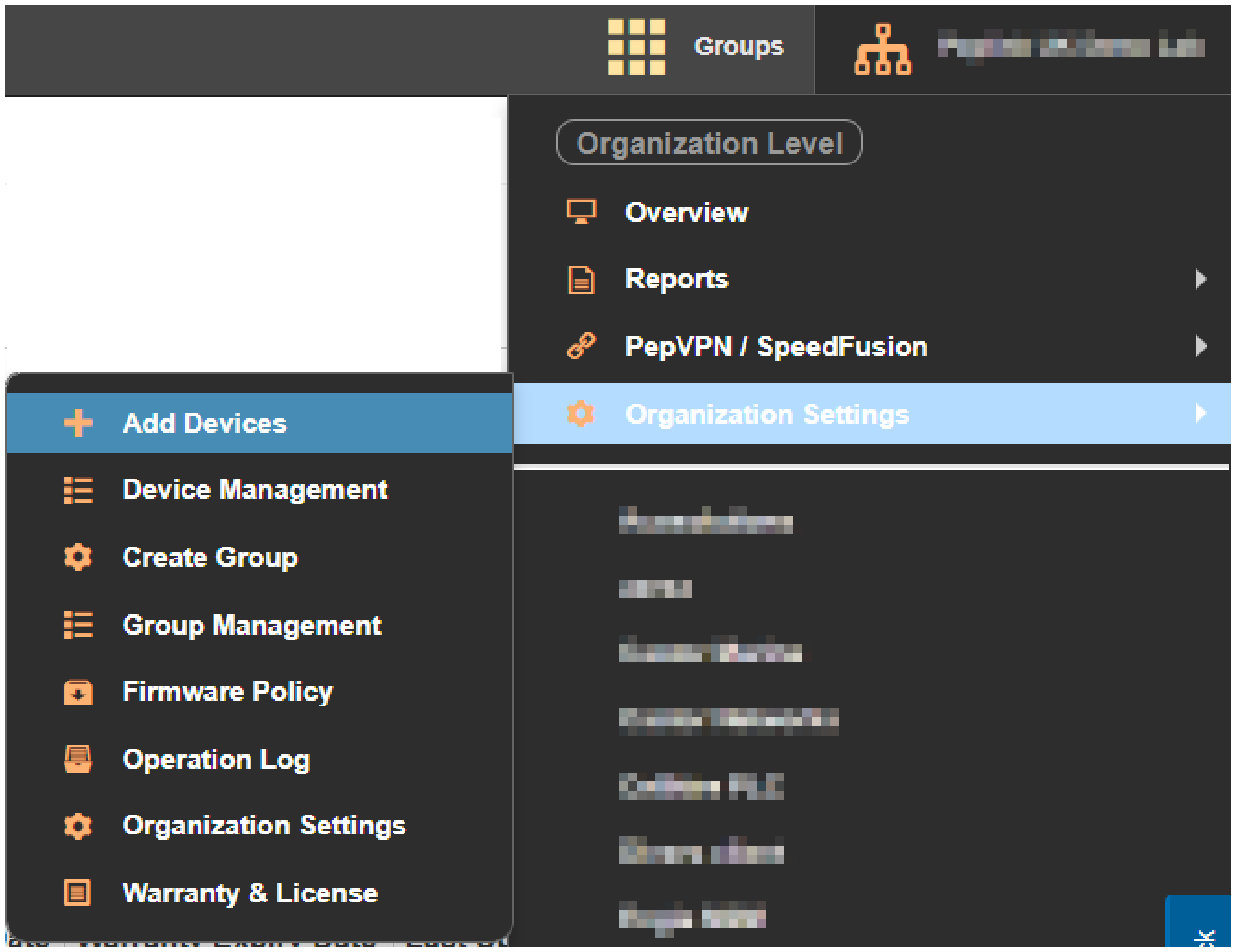
Type of FusionHub License to Acquire

○ Evaluation License (10 peers) (9 license(s) left)

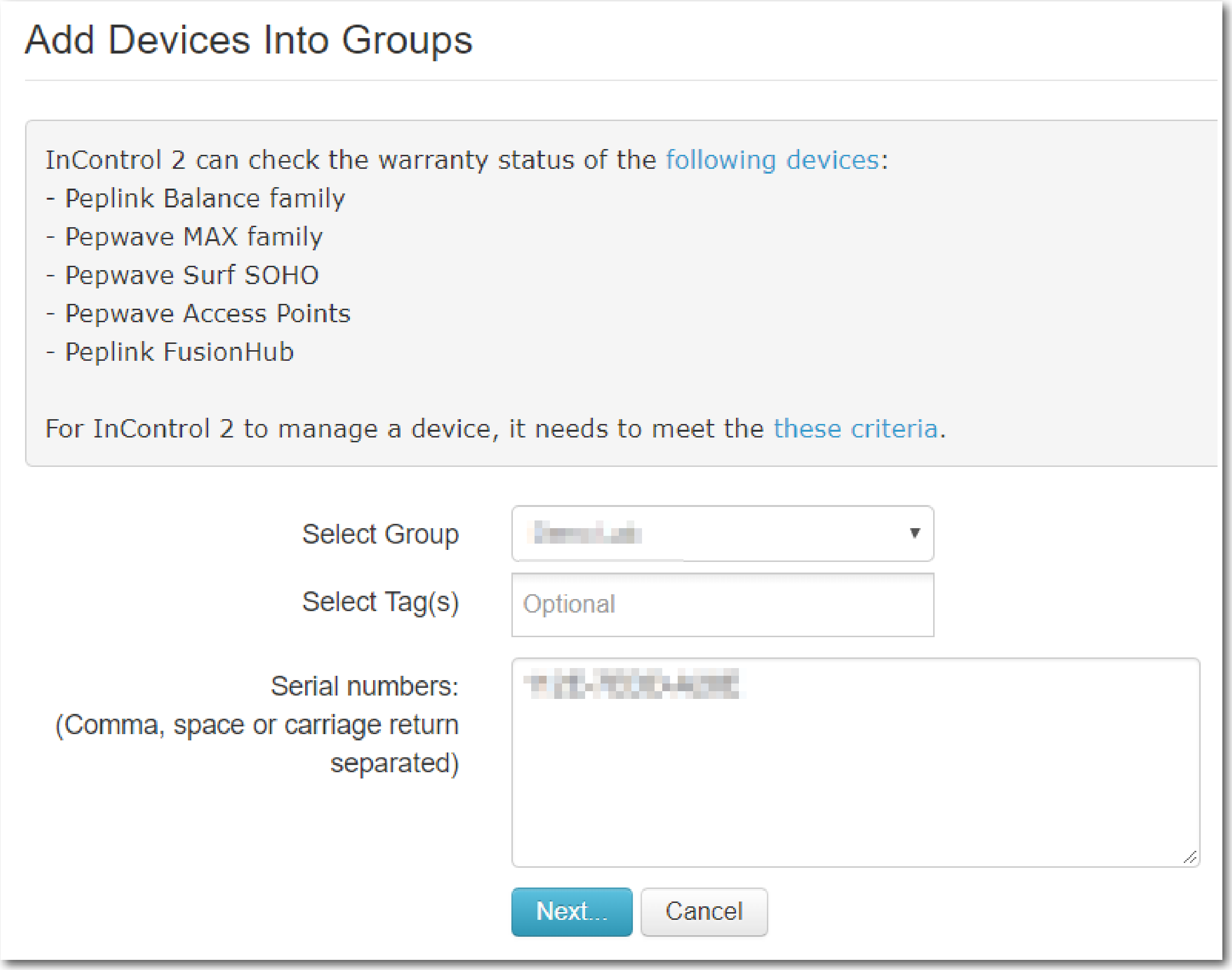
○ Solo License (1 peer)

7. InControl 2 will send the license information to the email address used to login. Follow the steps in the email to add a virtual router using your FusionHub serial number.

8. To add FusionHub onto your organization, navigate to **Organization>Settings>Add Devices**.



9. Enter the serial number from your license information email. Click **Add devices** and continue your FusionHub installation.



Add Devices Into Groups

InControl 2 can check the warranty status of the following devices:
- Peplink Balance family
- Pepwave MAX family
- Pepwave Surf SOHO
- Pepwave Access Points
- Peplink FusionHub

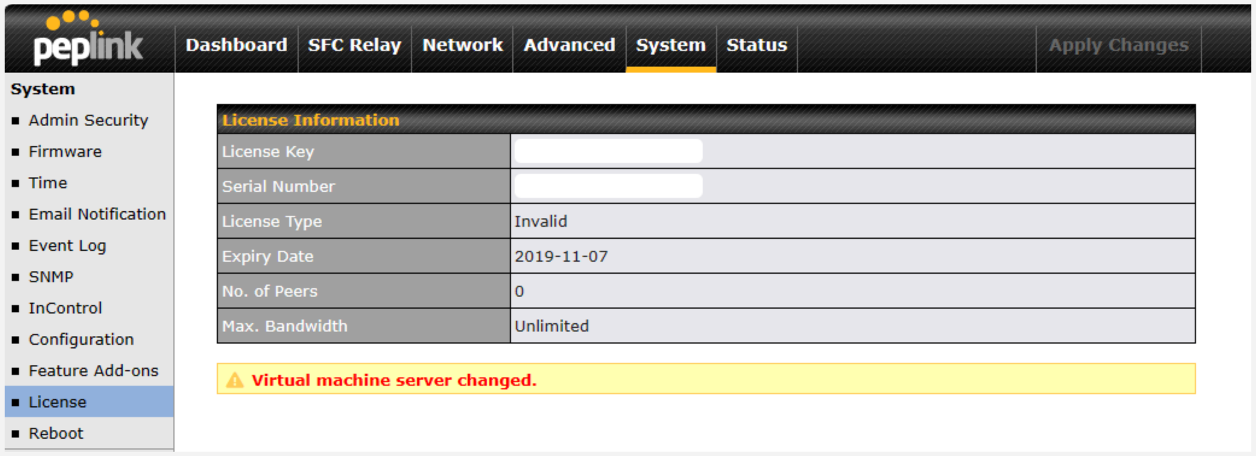
For InControl 2 to manage a device, it needs to meet the these criteria.

Select Group	[redacted] ▾
Select Tag(s)	Optional
Serial numbers: (Comma, space or carriage return separated)	[redacted]

2.2. FusionHub License Renewal

When the VM ID and/or host ID of FusionHub change, an error message, '**Virtual machine server changed**', will appear on the FusionHub Web Admin page.

- FusionHub > Web Admin

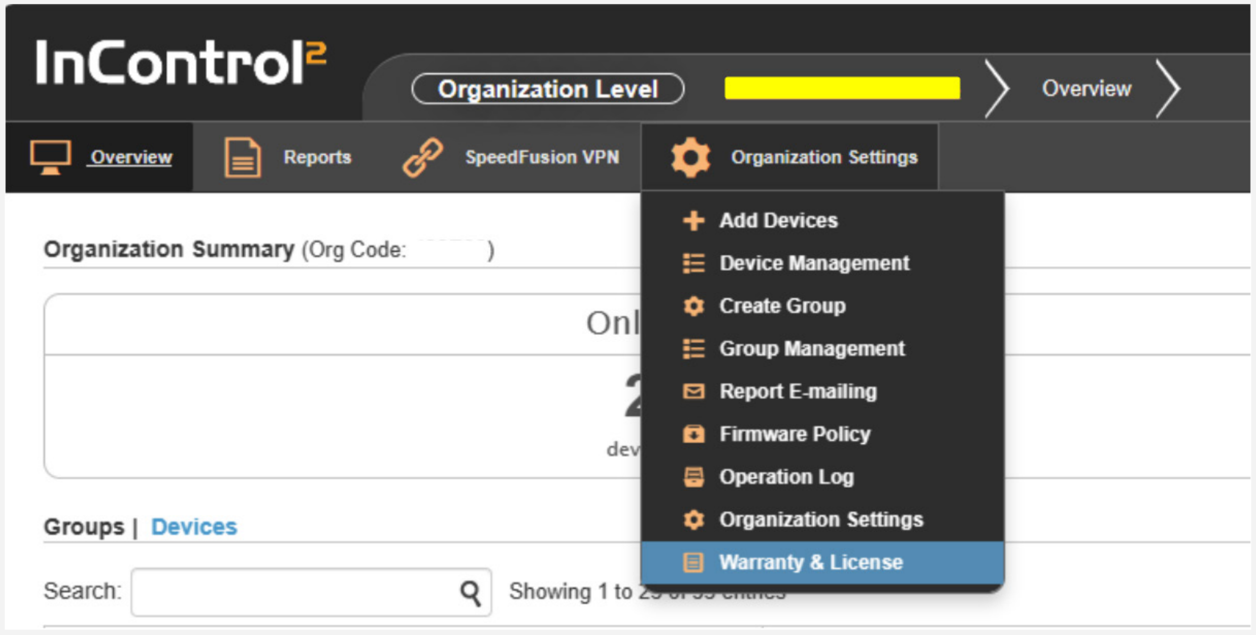


License Information	
License Key	
Serial Number	
License Type	Invalid
Expiry Date	2019-11-07
No. of Peers	0
Max. Bandwidth	Unlimited

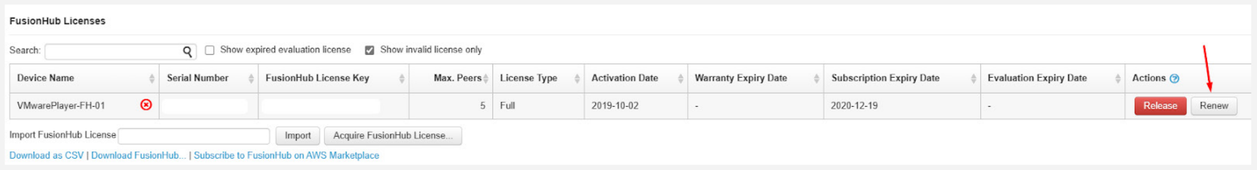
⚠ Virtual machine server changed.

If the user confirms that FusionHub has a valid license and wishes to retain the VM/host, they can re-associate the license key with FusionHub via InControl 2.

- InControl2 > Organization Settings > Warranty & License



Under the **FusionHub License** section, click the [Renew] button to apply the license key to FusionHub (if it has an invalid license key).



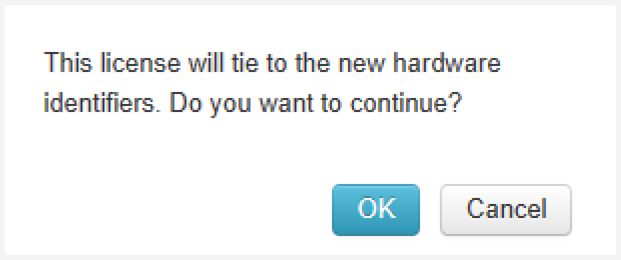
FusionHub Licenses

Search: □ Show expired evaluation license ☑ Show invalid license only

Device Name	Serial Number	FusionHub License Key	Max. Peers	License Type	Activation Date	Warranty Expiry Date	Subscription Expiry Date	Evaluation Expiry Date	Actions
VMwarePlayer-FH-01 ⊗			5	Full	2019-10-02	-	2020-12-19	-	Release Renew

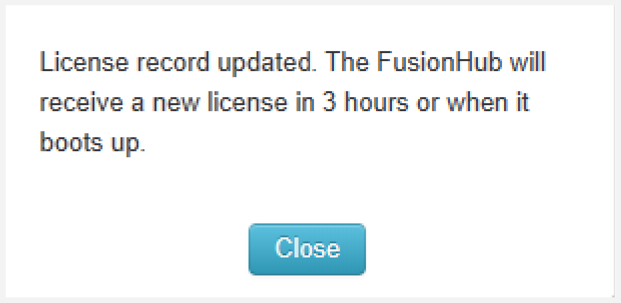
Import FusionHub License
Import
Acquire FusionHub License...
Download as CSV | Download FusionHub... | Subscribe to FusionHub on AWS Marketplace

Click "OK" to continue.



This license will tie to the new hardware identifiers. Do you want to continue?

The license record will be updated, and FusionHub will receive a new license within 3 hours or upon its next boot.



License record updated. The FusionHub will receive a new license in 3 hours or when it boots up.

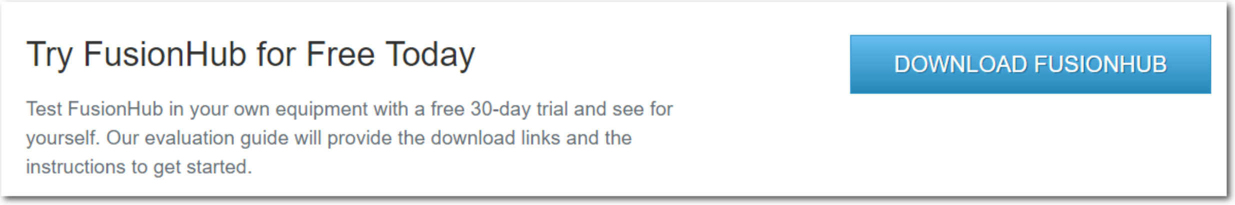
Once the license key is activated on FusionHub, the error message "**Virtual machine server changed**" will disappear from FusionHub > Web Admin.

3. FusionHub Download

For all VM platforms besides Amazon Web Services, please download FusionHub from the Peplink website by following the link below:

https://www.peplink.com/products/fusionhub/

Please scroll down to the section below to download the FusionHub base image for installation:



Try FusionHub for Free Today

Test FusionHub in your own equipment with a free 30-day trial and see for yourself. Our evaluation guide will provide the download links and the instructions to get started.

For Amazon Web Services, please refer to page 66 for instructions on how to download and install.

** Please upgrade to the latest firmware **after** the FusionHub installation is completed.*

4. FusionHub Deployment

This section will show how to implement FusionHub on VMware (ESXi server, Workstation, Player), Oracle VirtualBox, Citrix XenCenter, Microsoft Hyper-V, and Amazon Web Services. Please select your VM platform:

- VMware ESXI Server
- VMware Workstation
- VMware Player
- Oracle VirtualBox
- Citrix XenServer
- Microsoft Hyper-V
- Amazon Web Services

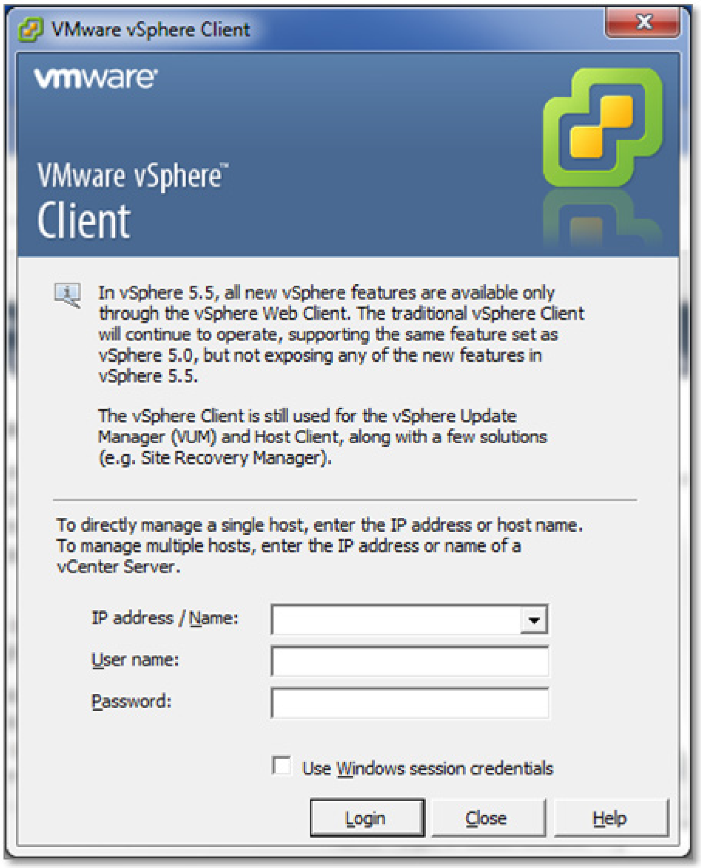
4.1. VMware ESXI Server

4.1.1. VMware ESXI 5.5.0

1. Download **VMware ESXi 5.5.0** from www.vmware.com/go/download-vsphere and install it.

2. For VMware vSphere server installation hardware requirements, refer to http://www.vmware.com/products/vsphere-hypervisor/gettingstarted.html

3. Open **VMware vSphere**. Enter the appropriate **IP address / Name**, **User name**, and **Password**. Click **Login** to login to the ESXi server. **Make sure that your computer and ESXi server are on the same network.** If your computer and ESXi server are not on the same network, you won't be able to connect to FusionHub's Web admin interface, even though you can remotely access the ESXi server through a router. Follow the steps found in **5 FusionHub Interface Configuration** to connect to FusionHub's Web admin interface.



In vSphere 5.5, all new vSphere features are available only through the vSphere Web Client. The traditional vSphere Client will continue to operate, supporting the same feature set as vSphere 5.0, but not exposing any of the new features in vSphere 5.5.

The vSphere Client is still used for the vSphere Update Manager (VUM) and Host Client, along with a few solutions (e.g. Site Recovery Manager).

To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a vCenter Server.

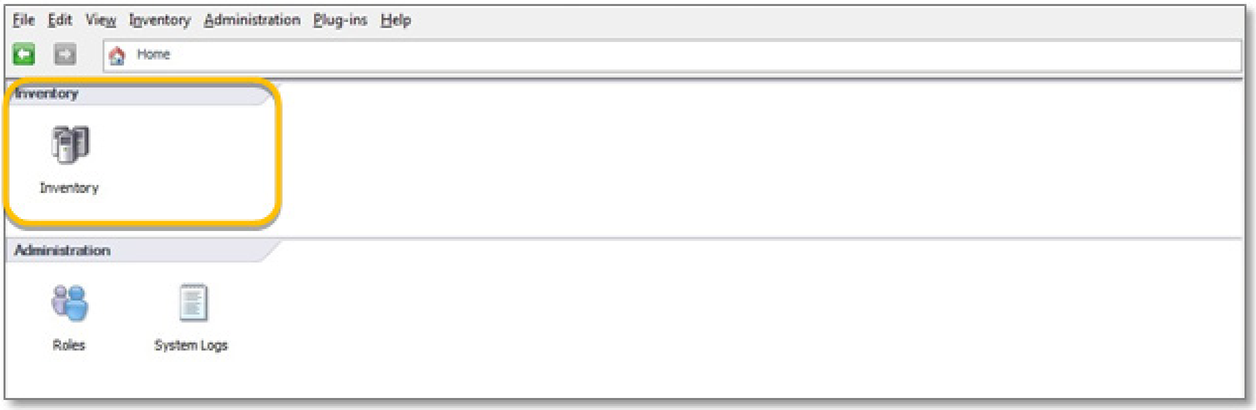
IP address / Name:

User name:

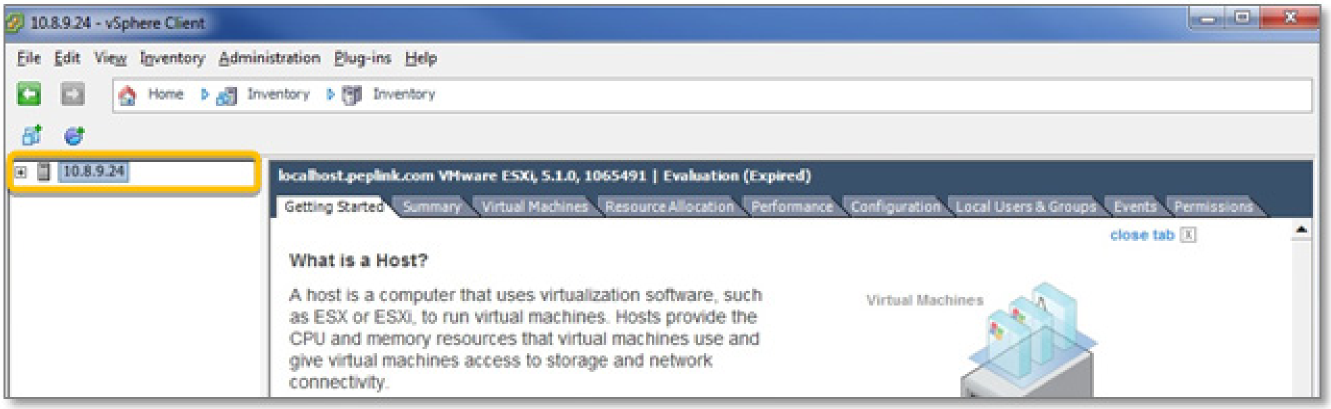
Password:

□ Use Windows session credentials

4. After successfully logging in, click **Inventory**. The remaining contents of this section will cover deploying a FusionHub virtual machine to your ESXi server.



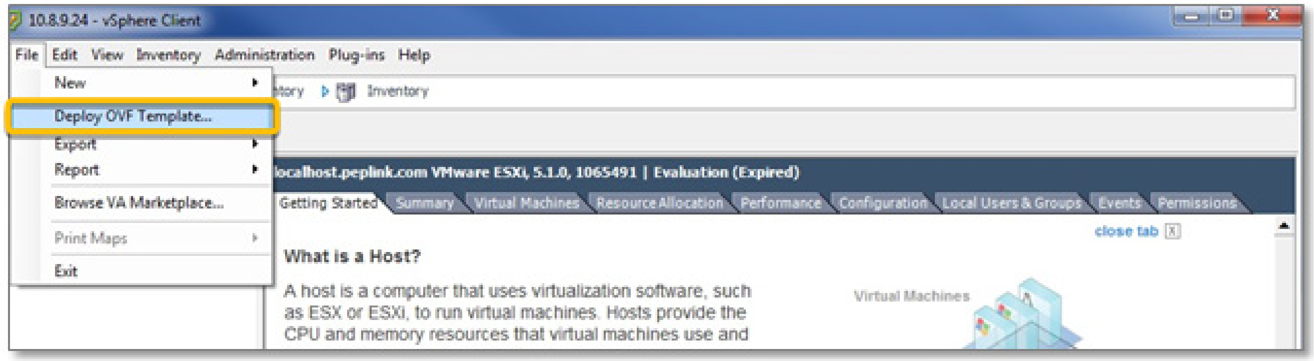
5. Click the **inventory object** to begin deploying the OVF template.



What is a Host?

A host is a computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity.

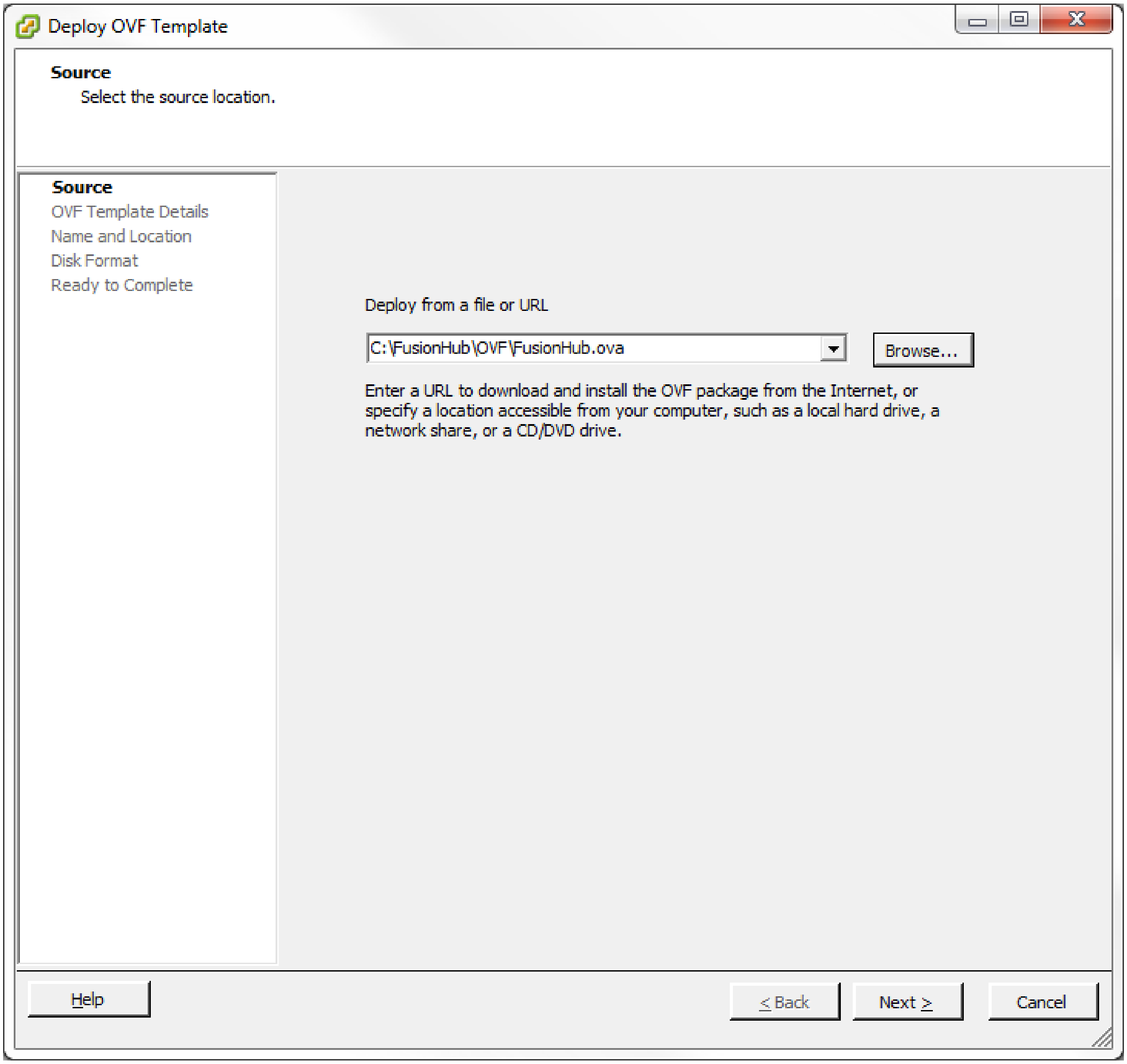
6. Click File > Deploy OVF Template... to deploy the FusionHub OVF template downloaded from InControl 2. In order to deploy the OVF template successfully, please make sure that your ESXi server supports virtual machine version 8, which runs on VMware ESXi 5.5 and later.



What is a Host?

A host is a computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and

7. On the **Source** dialog of the **Deploy OVF Template** wizard, click **Browse**. Locate the FusionHub.ova template file on your computer and click **Next**.



Source

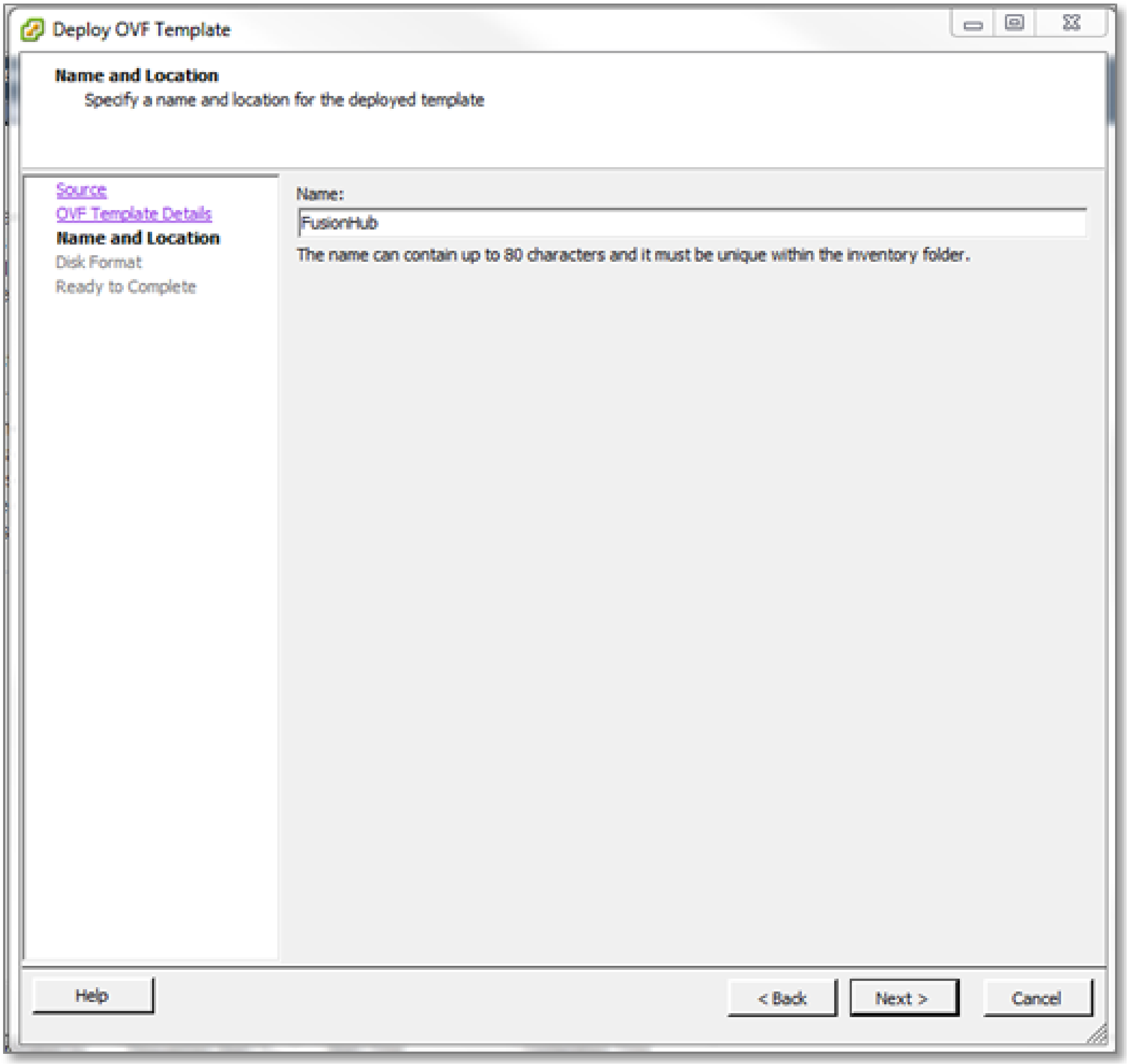
Select the source location.

Deploy from a file or URL

C:\FusionHub\OVF\FusionHub.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

8. On the **Name and Location** dialog, type a **name** or keep the default setting. Click **Next**.

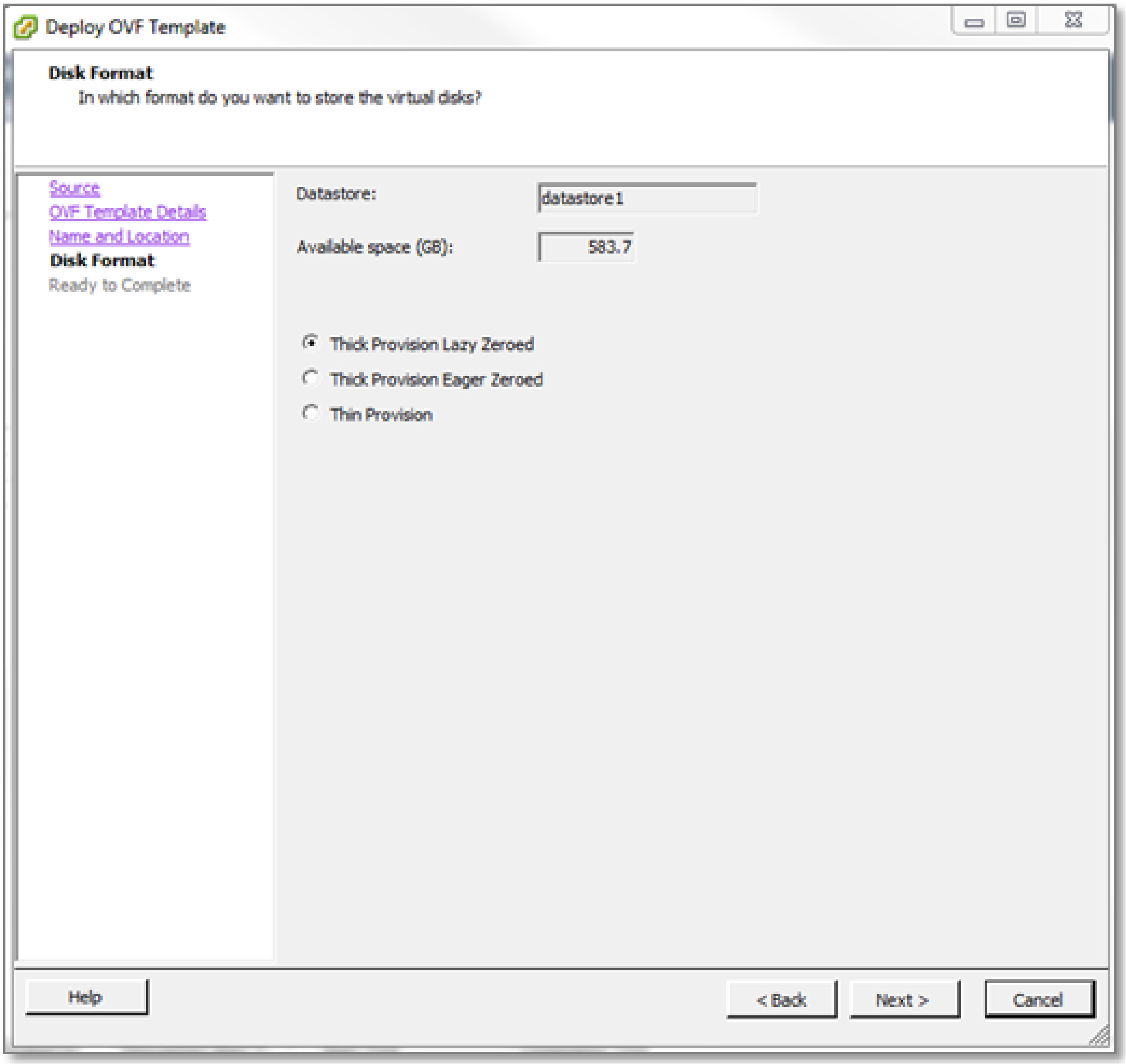


Name and Location
Specify a name and location for the deployed template

Name:
FusionHub

The name can contain up to 80 characters and it must be unique within the inventory folder.

9. Keep the default settings on the **Disk Format** dialog. Click **Next**.



Deploy OVF Template

Disk Format

In which format do you want to store the virtual disks?

Datastore: datastore1

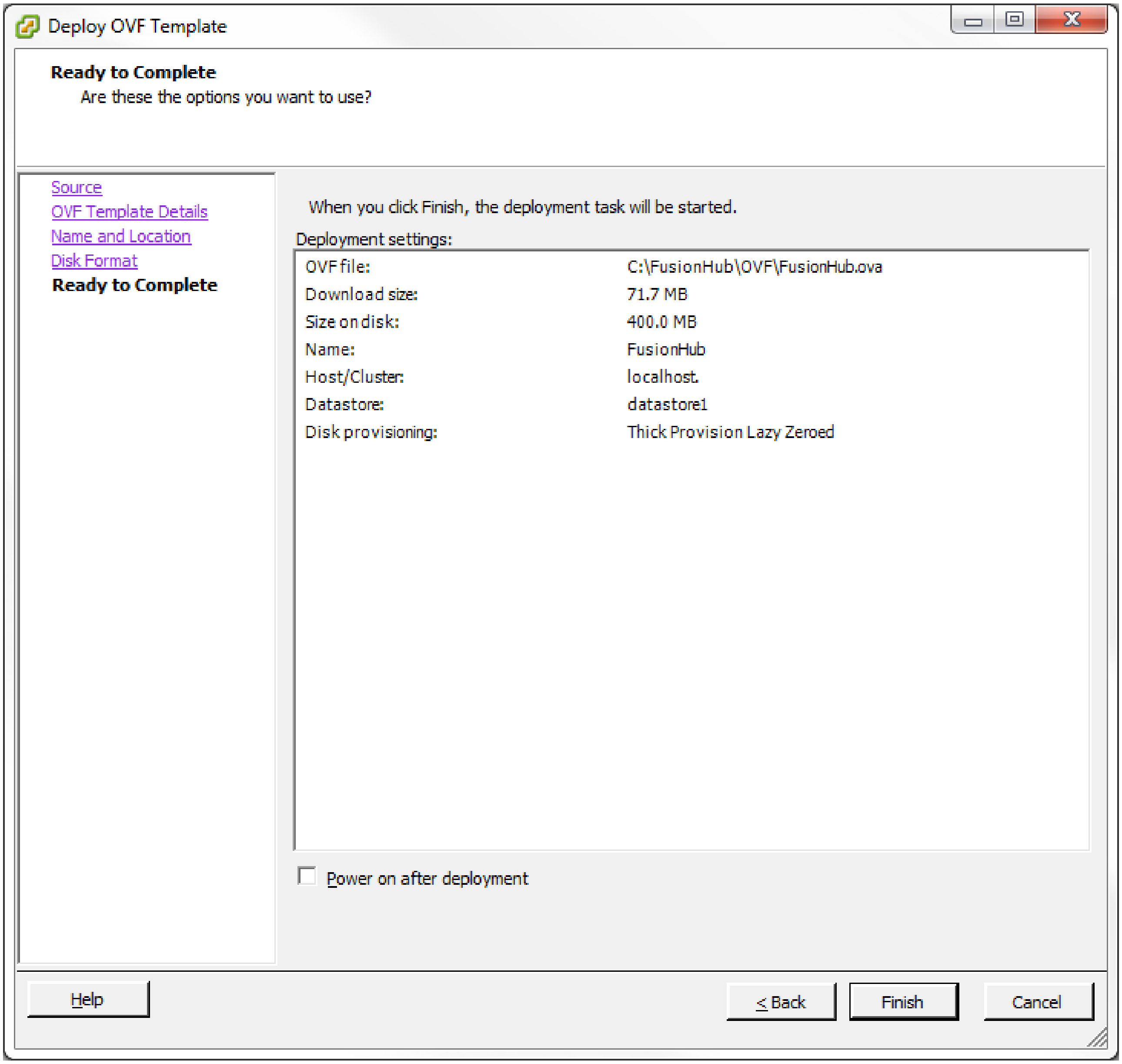
Available space (GB): 583.7

● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

10. On the **Ready to Complete** dialog, review the deployment settings. Click **Finish** to complete the process and close the wizard.



Ready to Complete

Are these the options you want to use?

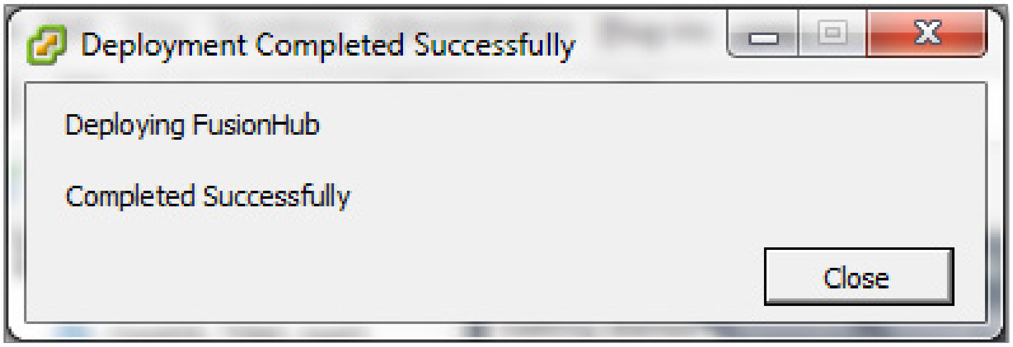
When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\FusionHub\OVF\FusionHub.ova
Download size:	71.7 MB
Size on disk:	400.0 MB
Name:	FusionHub
Host/Cluster:	localhost.
Datastore:	datastore1
Disk provisioning:	Thick Provision Lazy Zeroed

□ Power on after deployment

11. Once you have completed the steps above, a FusionHub virtual machine is created.

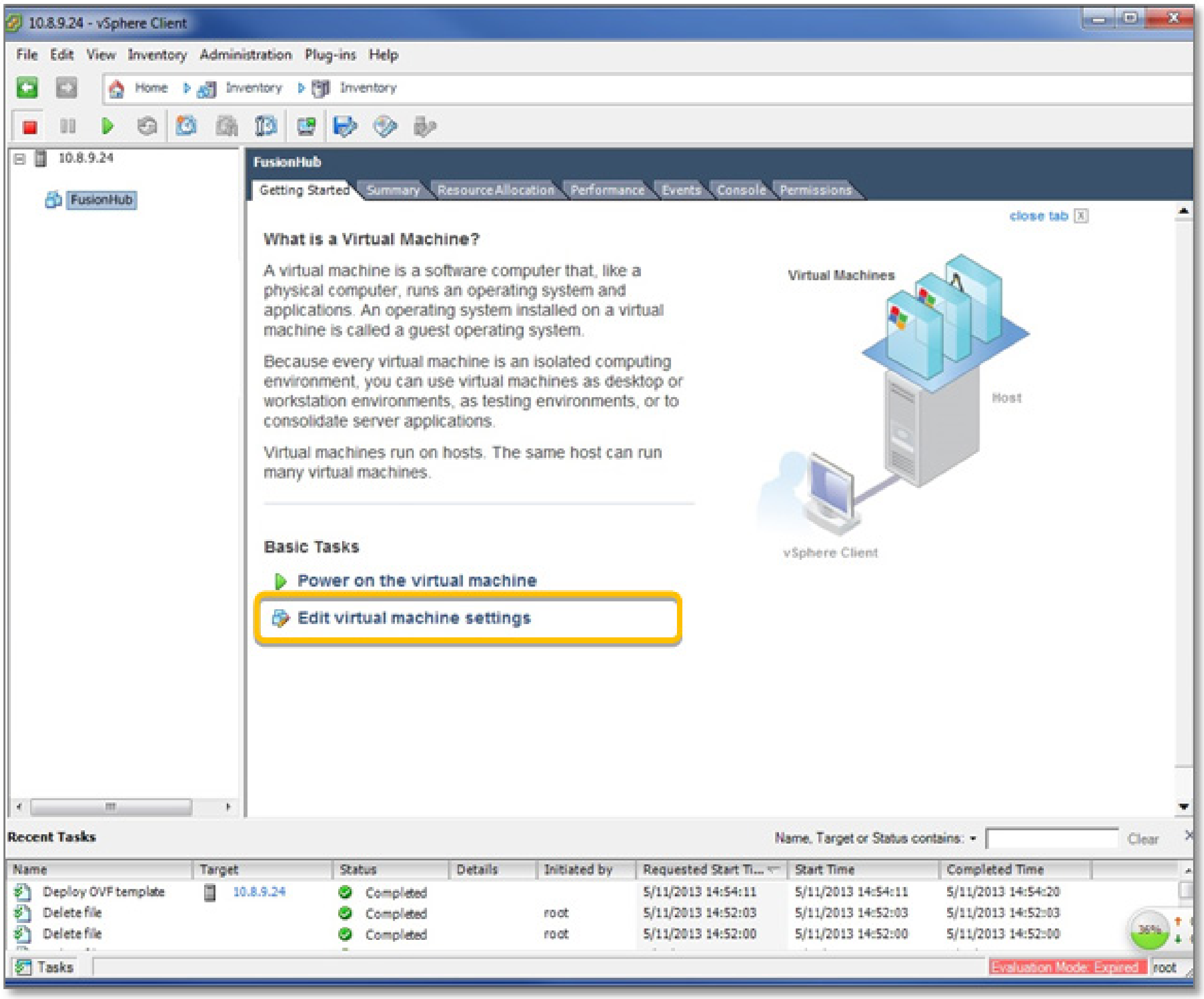


Deployment Completed Successfully

Deploying FusionHub

Completed Successfully

12. Click **FusionHub** in the column on the left side of the dialog to select the virtual machine. Click **Edit virtual machine settings** to begin adding an Ethernet adapter to the FusionHub virtual machine.



10.8.9.24 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
10.8.9.24
FusionHub
FusionHub
Getting Started Summary Resource Allocation Performance Events Console Permissions
close tab
Virtual Machines
Host
vSphere Client

What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Virtual machines run on hosts. The same host can run many virtual machines.

Basic Tasks

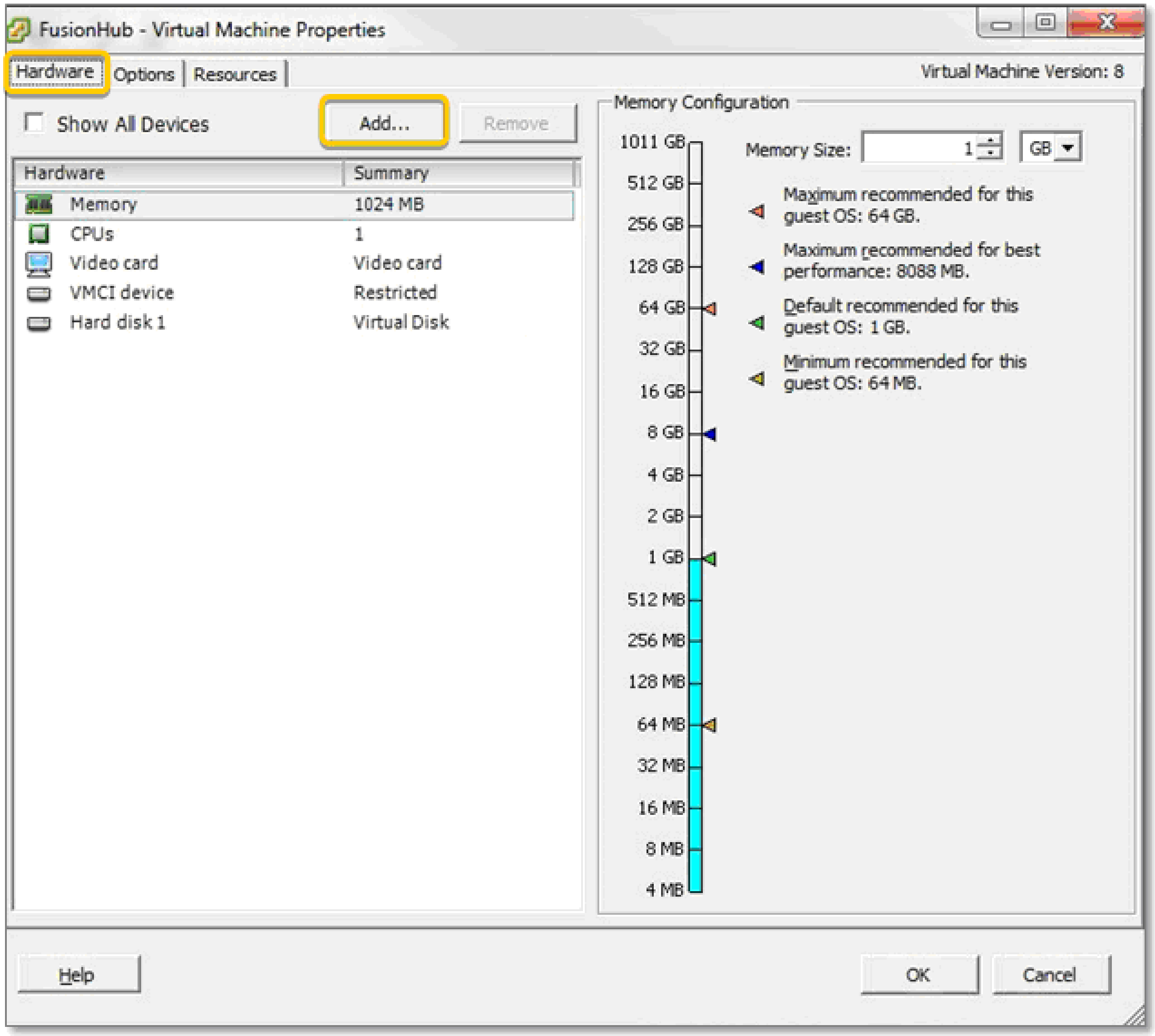
- Power on the virtual machine
- Edit virtual machine settings

Recent Tasks

Name, Target or Status contains: Clear

Name	Target	Status	Details	Initiated by	Requested Start Ti...	Start Time	Completed Time
Deploy OVF template	10.8.9.24	Completed			5/11/2013 14:54:11	5/11/2013 14:54:11	5/11/2013 14:54:20
Delete file		Completed		root	5/11/2013 14:52:03	5/11/2013 14:52:03	5/11/2013 14:52:03
Delete file		Completed		root	5/11/2013 14:52:00	5/11/2013 14:52:00	5/11/2013 14:52:00

13. Click Add, found under the Hardware tab on the FusionHub – Virtual Machine Properties dialog.



FusionHub - Virtual Machine Properties

Virtual Machine Version: 8

Hardware	Summary
Memory	1024 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
Hard disk 1	Virtual Disk

Memory Configuration

Memory Size: 1 GB

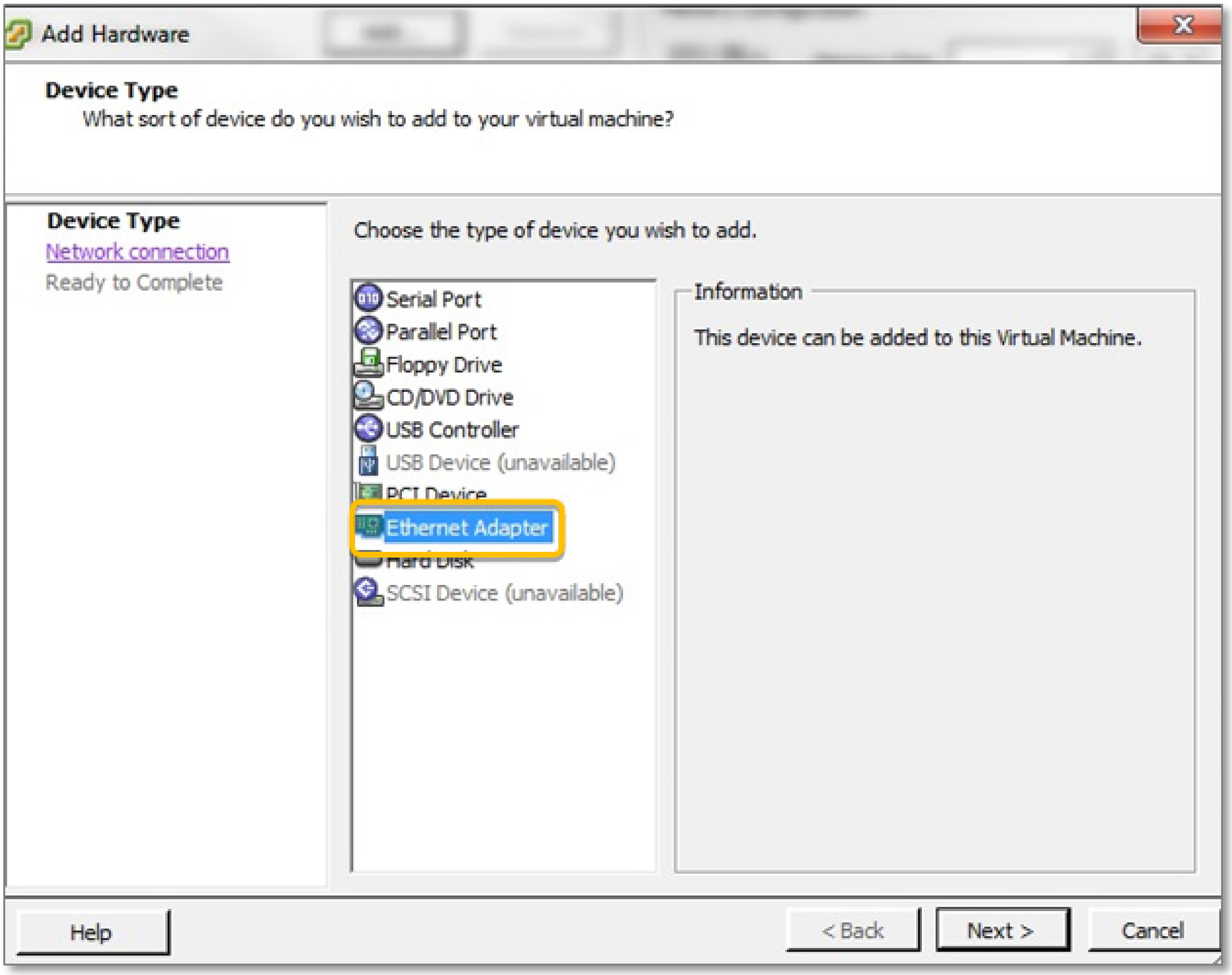
Maximum recommended for this guest OS: 64 GB.

Maximum recommended for best performance: 8088 MB.

Default recommended for this guest OS: 1 GB.

Minimum recommended for this guest OS: 64 MB.

14. On the **Add Hardware** dialog, select **Ethernet Adapter**. Click **Next**.



Add Hardware

Device Type

What sort of device do you wish to add to your virtual machine?

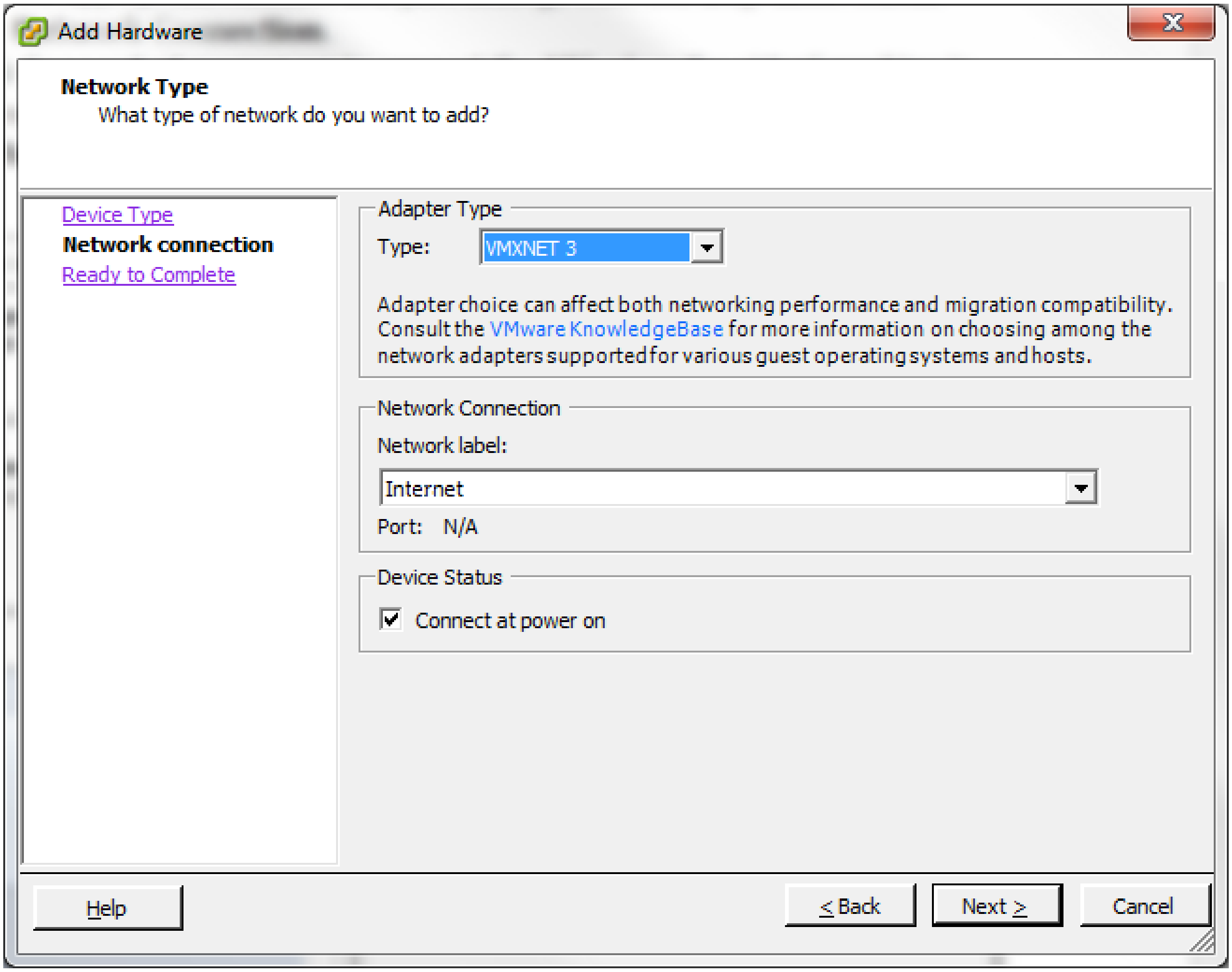
Choose the type of device you wish to add.

This device can be added to this Virtual Machine.

15. On the **Network Type** dialog, select **VMXNET 3** as the **Adapter Type**. Select the appropriate network and port settings from the drop-down menus under **Network Connection**.

16. Check **Connect at power on** to connect the NIC when the virtual machine is powered on.

17. Click **Next**.



Add Hardware

Network Type

What type of network do you want to add?

Adapter Type

Type: VMXNET 3

Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapters supported for various guest operating systems and hosts.

Network Connection

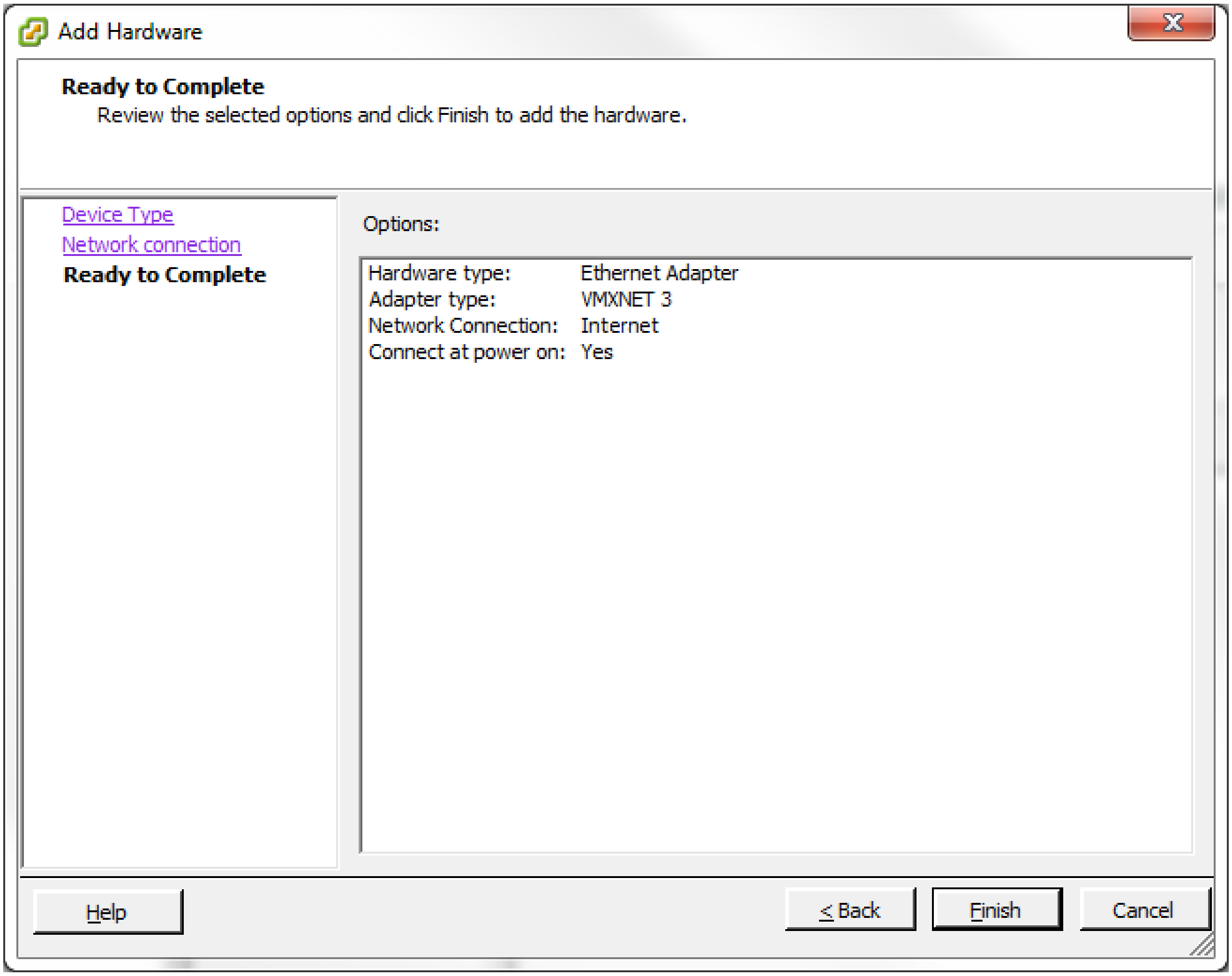
Network label: Internet

Port: N/A

Device Status

☑ Connect at power on

18. On the **Ready to Complete** dialog, review your settings and click **Finish**.



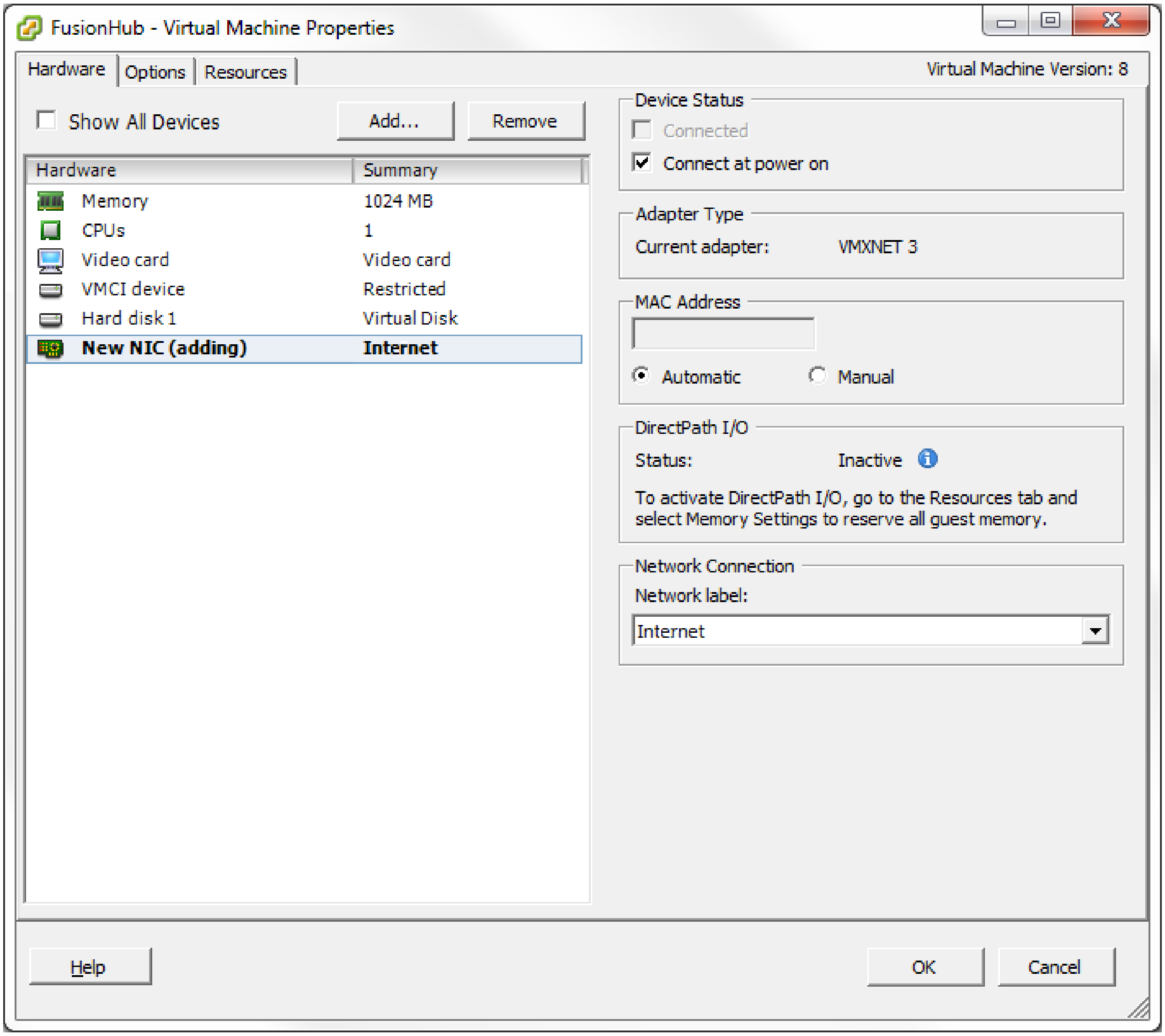
Ready to Complete

Review the selected options and click Finish to add the hardware.

Options:

Hardware type: Ethernet Adapter
Adapter type: VMXNET 3
Network Connection: Internet
Connect at power on: Yes

19. Click **OK** to finish adding hardware.



FusionHub - Virtual Machine Properties

Virtual Machine Version: 8

□ Show All Devices

Hardware	Summary
Memory	1024 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
Hard disk 1	Virtual Disk
New NIC (adding)	**Internet**

Device Status

□ Connected

☑ Connect at power on

Adapter Type

Current adapter: VMXNET 3

MAC Address

● Automatic ○ Manual

DirectPath I/O

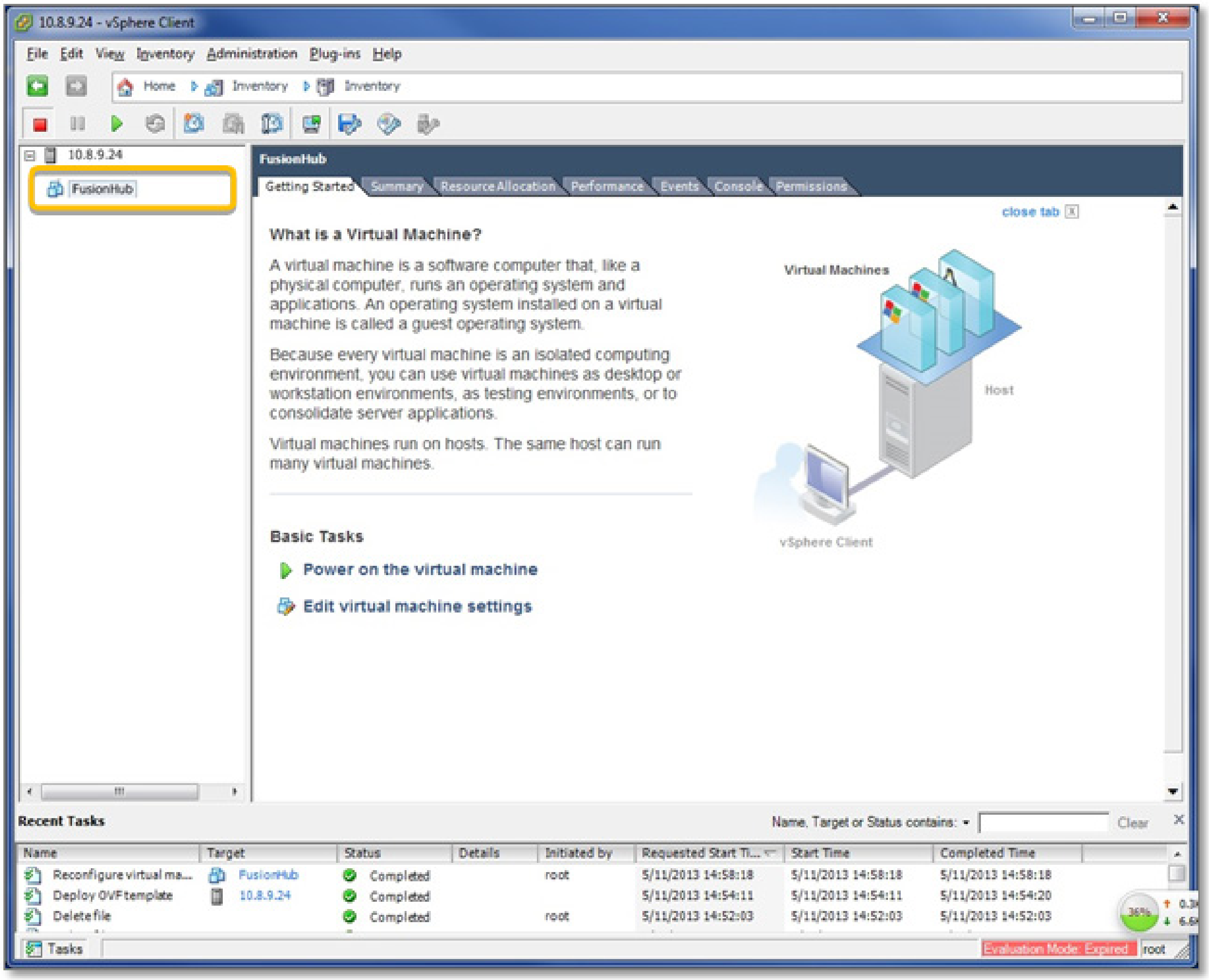
Status: Inactive

To activate DirectPath I/O, go to the Resources tab and select Memory Settings to reserve all guest memory.

Network Connection

Network label: Internet

20. Click Power on the virtual machine to run FusionHub.



What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Virtual machines run on hosts. The same host can run many virtual machines.

Basic Tasks

- Power on the virtual machine
- Edit virtual machine settings

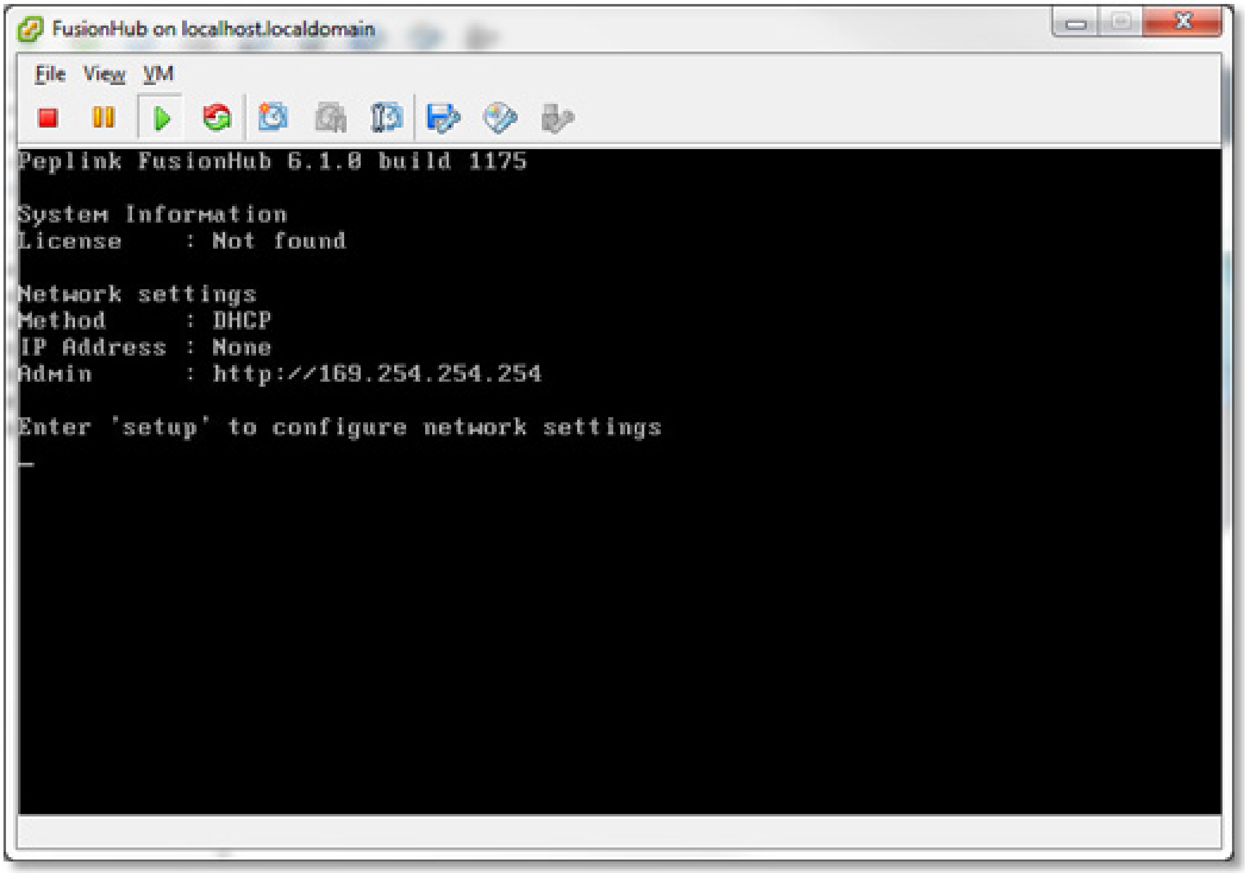
Recent Tasks

Name, Target or Status contains: Clear

Name	Target	Status	Details	Initiated by	Requested Start Ti...	Start Time	Completed Time
Reconfigure virtual ma...	FusionHub	Completed		root	5/11/2013 14:58:18	5/11/2013 14:58:18	5/11/2013 14:58:18
Deploy OVF template	10.8.9.24	Completed			5/11/2013 14:54:11	5/11/2013 14:54:11	5/11/2013 14:54:20
Delete file		Completed		root	5/11/2013 14:52:03	5/11/2013 14:52:03	5/11/2013 14:52:03

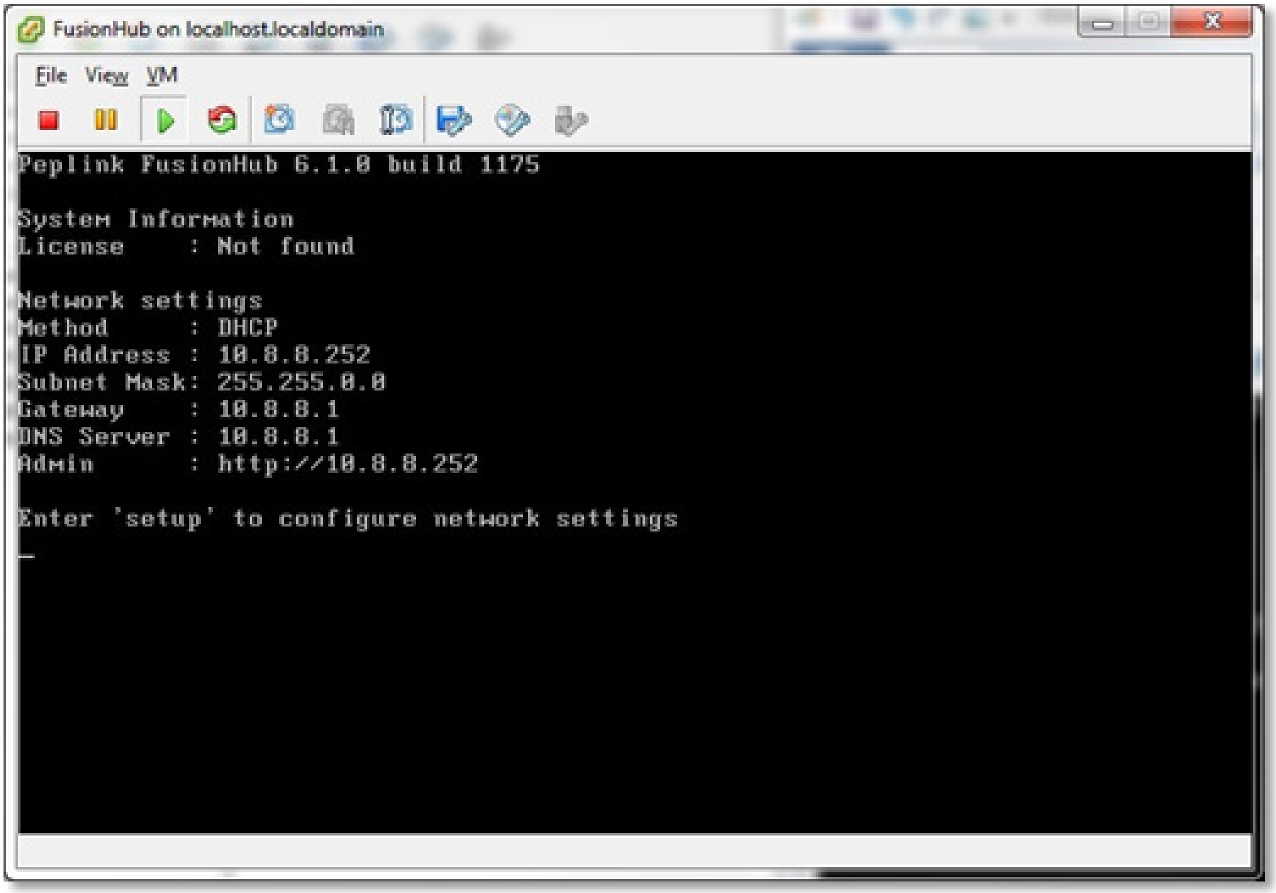
21. When the FusionHub virtual machine is powered on, right-click **FusionHub**. Select **Open Console** for general information about FusionHub, including:

- FusionHub version
- System information
- Network settings:
  Method: DHCP
  IP Address: None
  Admin: http://169.254.254.254



```
Peplink FusionHub 6.1.0 build 1175

System Information
License     : Not found

Network settings
Method      : DHCP
IP Address  : None
Admin       : http://169.254.254.254

Enter 'setup' to configure network settings
_
```

22. The default WAN connection method is DHCP. If the DHCP server is available on your network, the FusionHub IP address will be automatically obtained by the DHCP server. In this case, the console will look similar to the following:



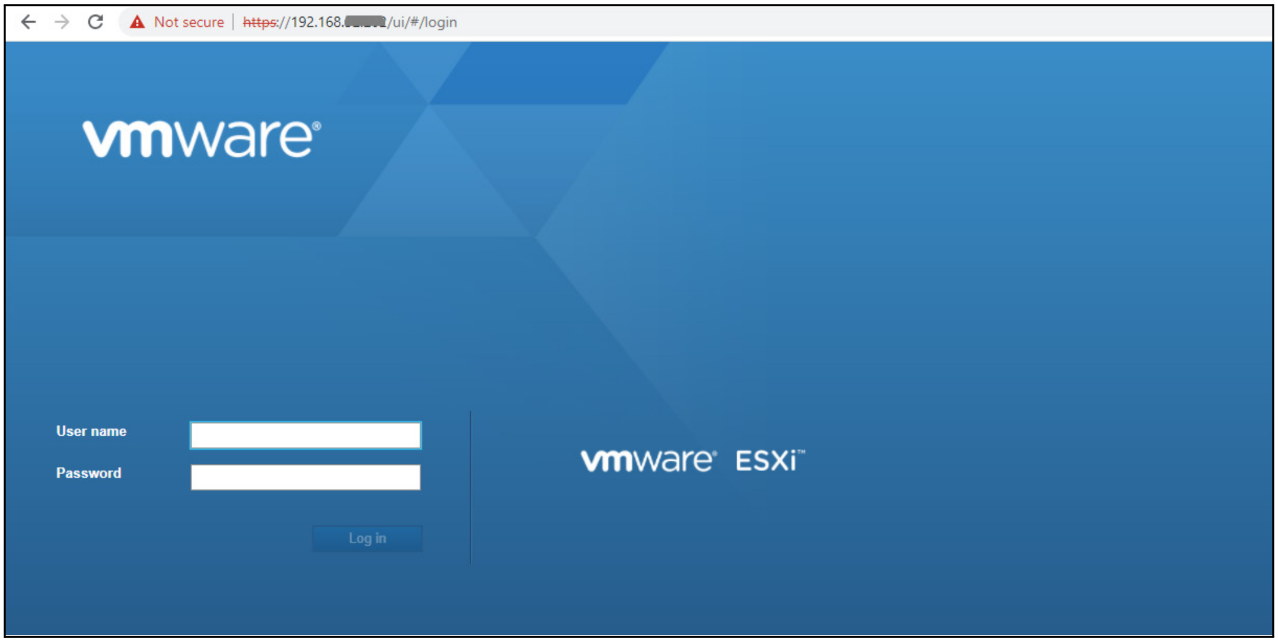
```
Peplink FusionHub 6.1.0 build 1175

System Information
License     : Not found

Network settings
Method      : DHCP
IP Address  : 10.8.8.252
Subnet Mask: 255.255.0.0
Gateway     : 10.8.8.1
DNS Server  : 10.8.8.1
Admin       : http://10.8.8.252

Enter 'setup' to configure network settings
_
```

Please navigate to **FusionHub Interface Configuration** to continue your installation.

4.1.2. VMware ESXI 7.0

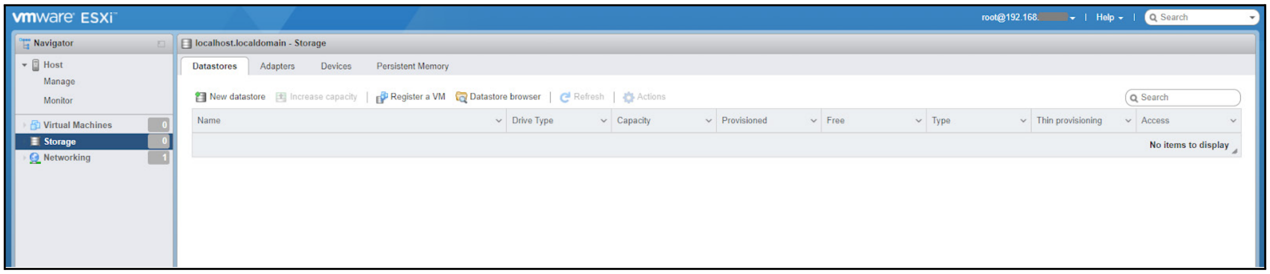
1. Download VMware ESXi 7.0 from the link below and install it.
https://customerconnect.vmware.com/en/downloads/info/slug/datacenter_cloud_infrastructure/vmware_vsphere/7_0

2. Open a browser and enter the appropriate **IP address / Name**, **User name**, and **Password**. Click **Login** to login to the ESXi server. **<u>Make sure that your computer and ESXi server are on the same network.</u>** If your computer and ESXi server are not on the same network, you won't be able to connect to FusionHub's Web admin interface, even if you can remotely access the ESXi server through a router. Follow the steps found in **5. FusionHub Interface Configuration** to connect to FusionHub's Web admin interface.



Not secure | ~~https~~://192.168.[redacted]/ui/#/login

3. After logging into the Host Web Ui, click on **Storage** in the left-hand Navigator console to set up storage for the host. Click **New Database** to configure the local datastore.



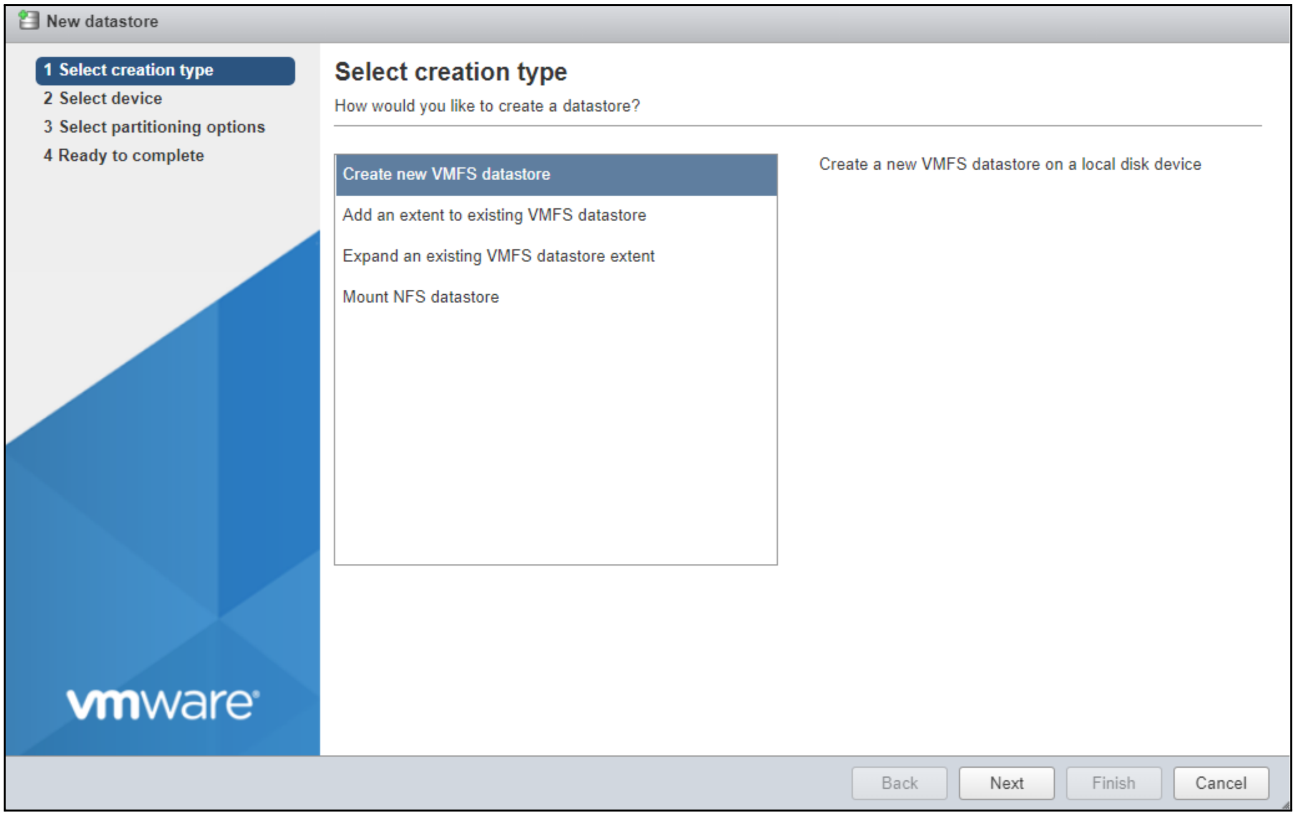
root@192.168.[redacted]

localhost.localdomain - Storage

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin provisioning	Access

No items to display

4. This process starts the New Datastore creation wizard. Select **Create new VMFS datastore**:



New datastore

1 Select creation type
2 Select device
3 Select partitioning options
4 Ready to complete

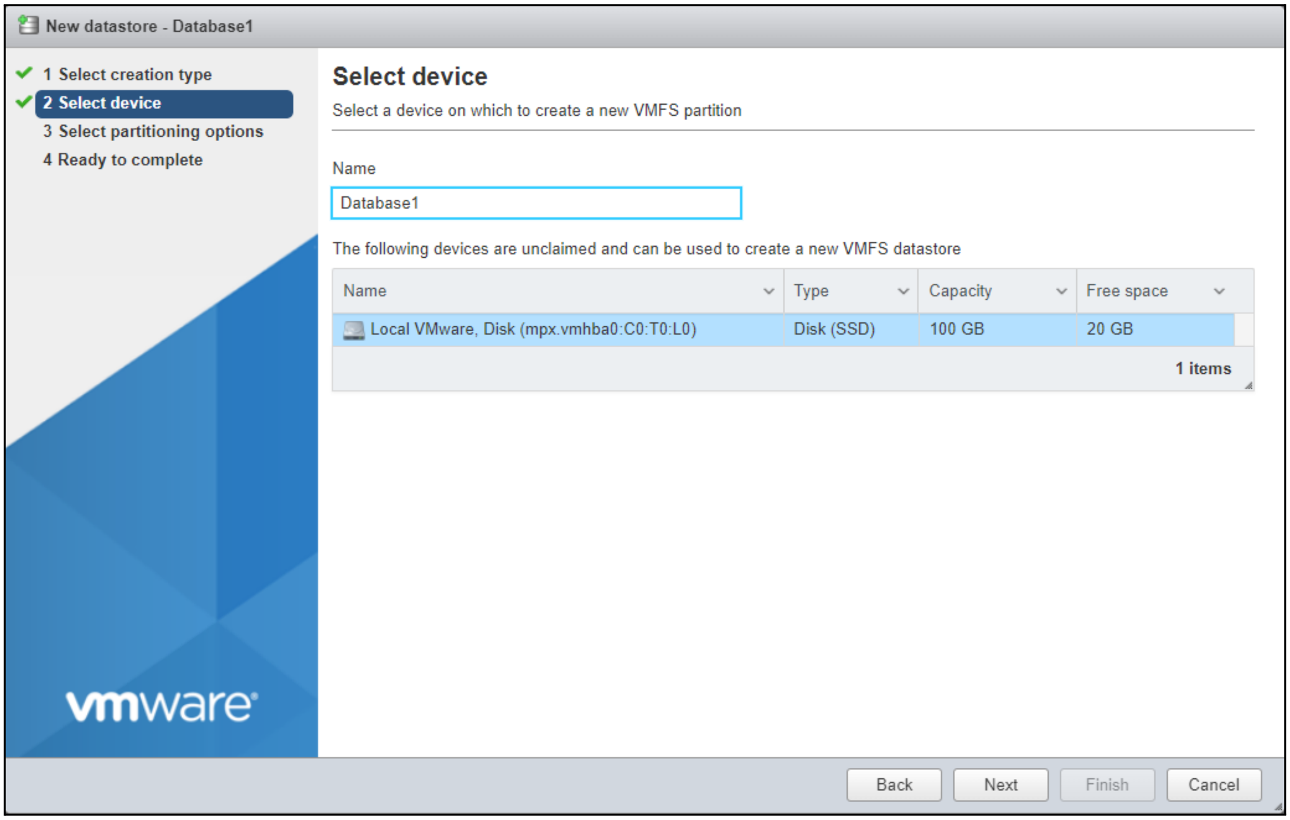
Select creation type

How would you like to create a datastore?

Create new VMFS datastore
Add an extent to existing VMFS datastore
Expand an existing VMFS datastore extent
Mount NFS datastore

Create a new VMFS datastore on a local disk device

5. Select an available datastore where you want to provision storage.



New datastore - Database1

Select device

Select a device on which to create a new VMFS partition

Name

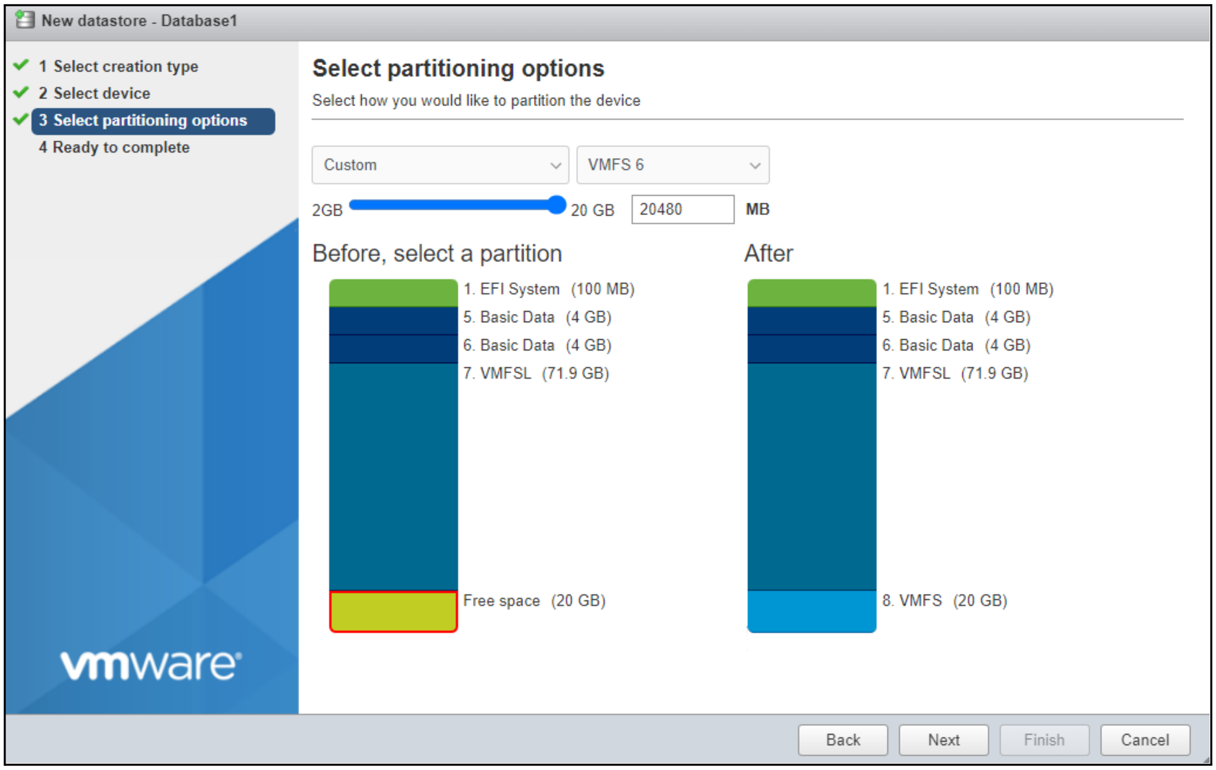
Database1

The following devices are unclaimed and can be used to create a new VMFS datastore

Name	Type	Capacity	Free space
Local VMware, Disk (mpx.vmhba0:C0:T0:L0)	Disk (SSD)	100 GB	20 GB

1 items

6. Select the partitioning scheme to partition and format the volume with VMFS. You can select either **Use Full Disk** or **Custom** partitioning scheme:



New datastore - Database1

- ✓ 1 Select creation type
- ✓ 2 Select device
- ✓ 3 Select partitioning options
- 4 Ready to complete

Select partitioning options

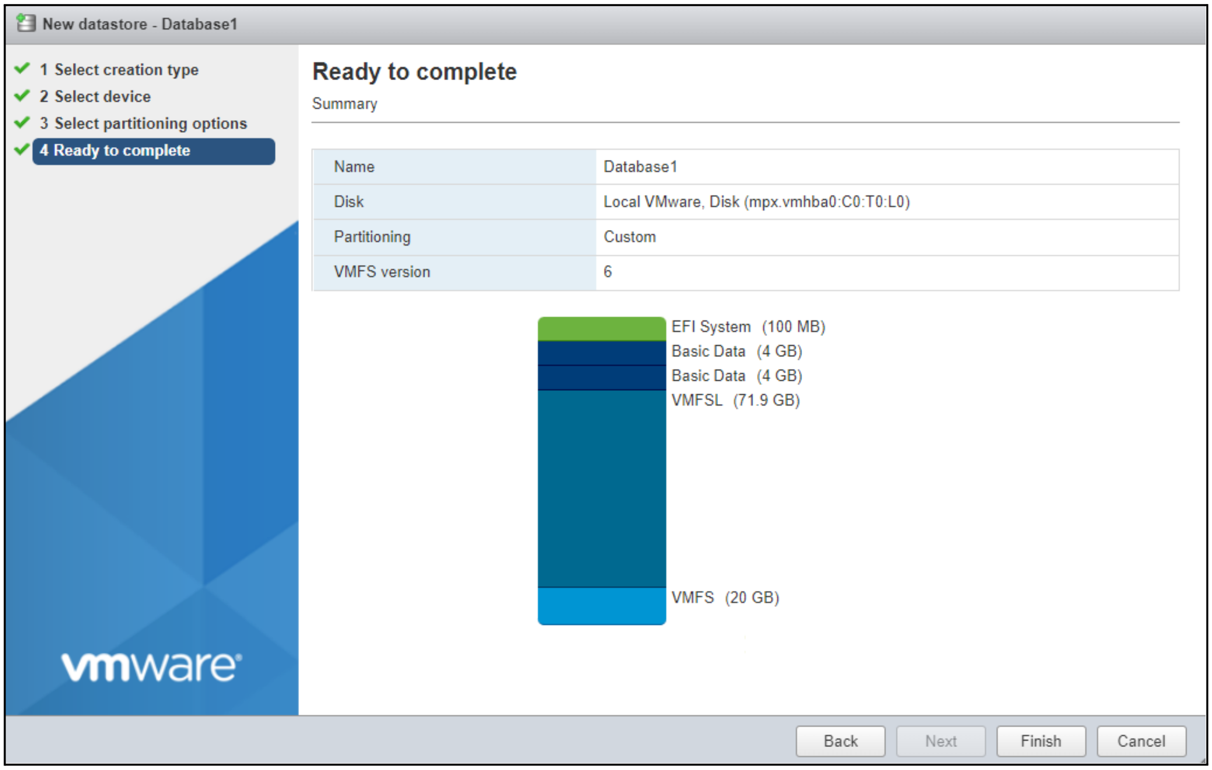
Select how you would like to partition the device

Custom | VMFS 6

2GB — 20 GB | 20480 MB

Before, select a partition	After
1. EFI System (100 MB)	1. EFI System (100 MB)
5. Basic Data (4 GB)	5. Basic Data (4 GB)
6. Basic Data (4 GB)	6. Basic Data (4 GB)
7. VMFSL (71.9 GB)	7. VMFSL (71.9 GB)
Free space (20 GB)	8. VMFS (20 GB)

7. Now you are ready to complete the process.



New datastore - Database1

- ✓ 1 Select creation type
- ✓ 2 Select device
- ✓ 3 Select partitioning options
- ✓ 4 Ready to complete

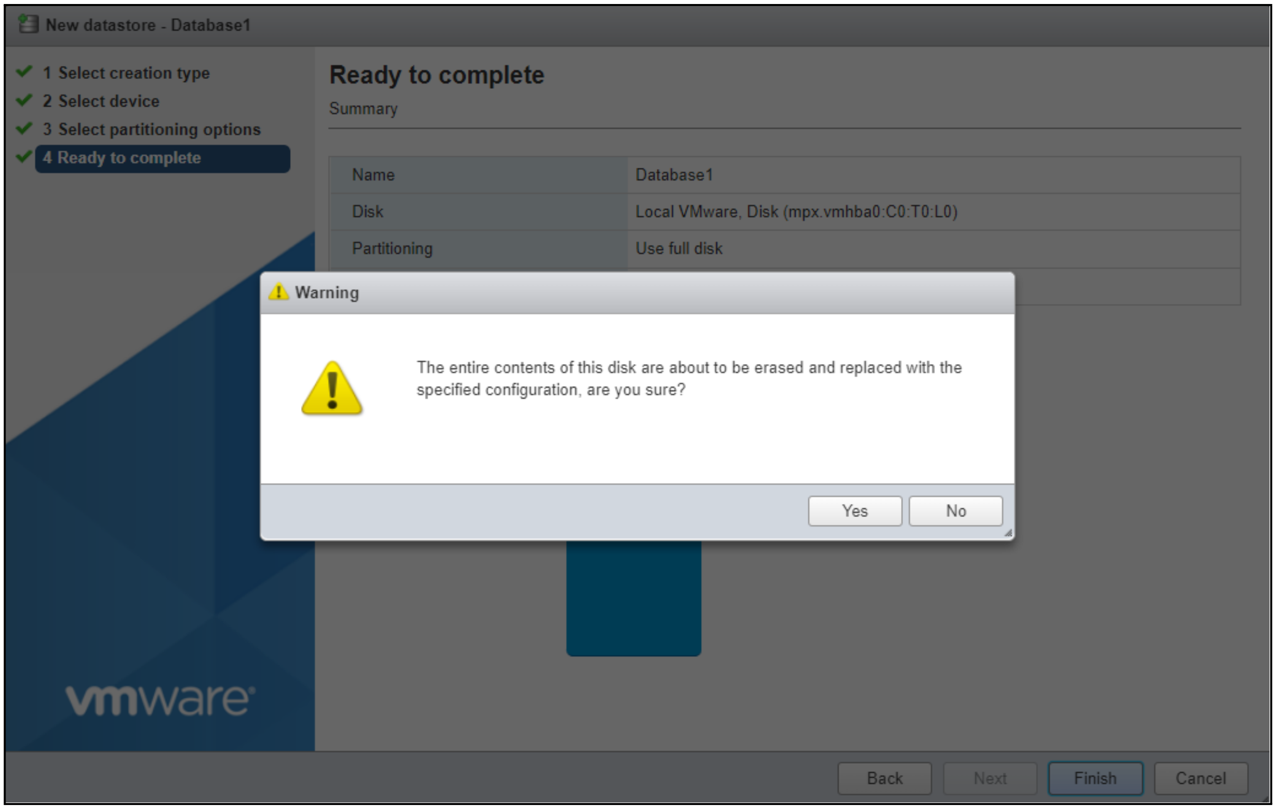
Ready to complete

Summary

Name	Database1
Disk	Local VMware, Disk (mpx.vmhba0:C0:T0:L0)
Partitioning	Custom
VMFS version	6

EFI System (100 MB)
Basic Data (4 GB)
Basic Data (4 GB)
VMFSL (71.9 GB)
VMFS (20 GB)

8. You will receive a warning that you are about to potentially destroy data by erasing the volume.



Ready to complete

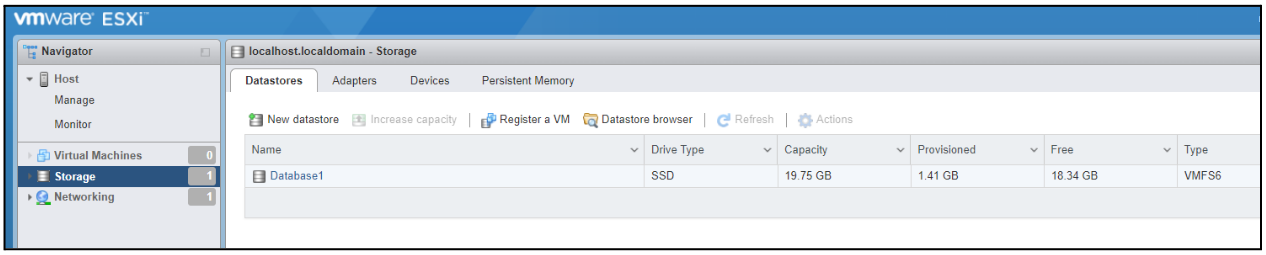
Summary

Name	Database1
Disk	Local VMware, Disk (mpx.vmhba0:C0:T0:L0)
Partitioning	Use full disk

Warning

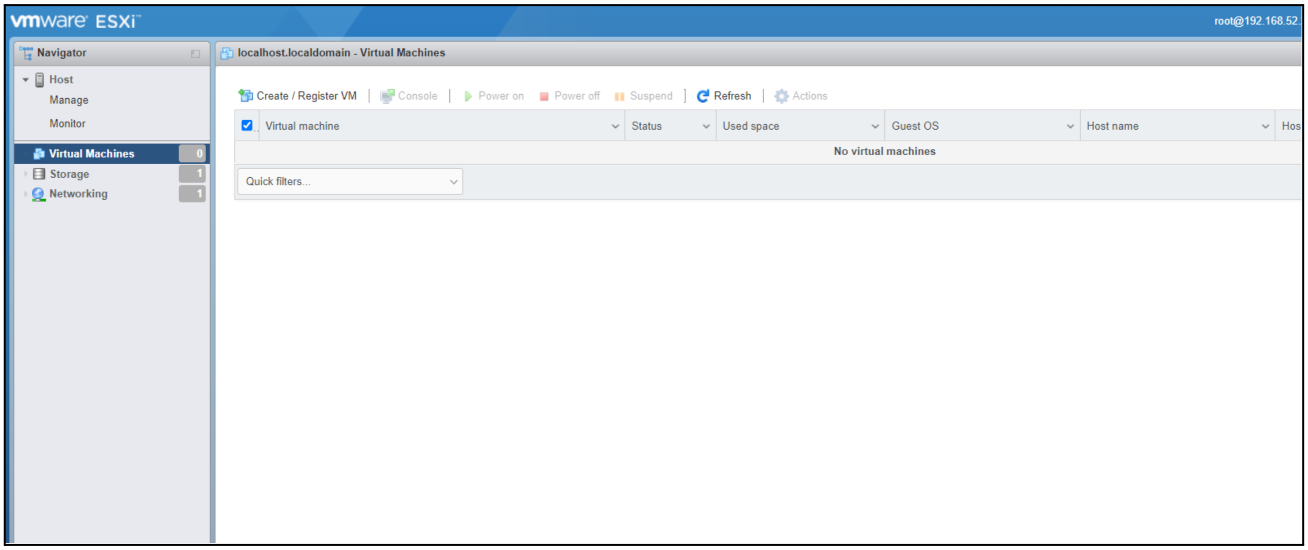
The entire contents of this disk are about to be erased and replaced with the specified configuration, are you sure?

9. The newly created datastore will be available on your host:



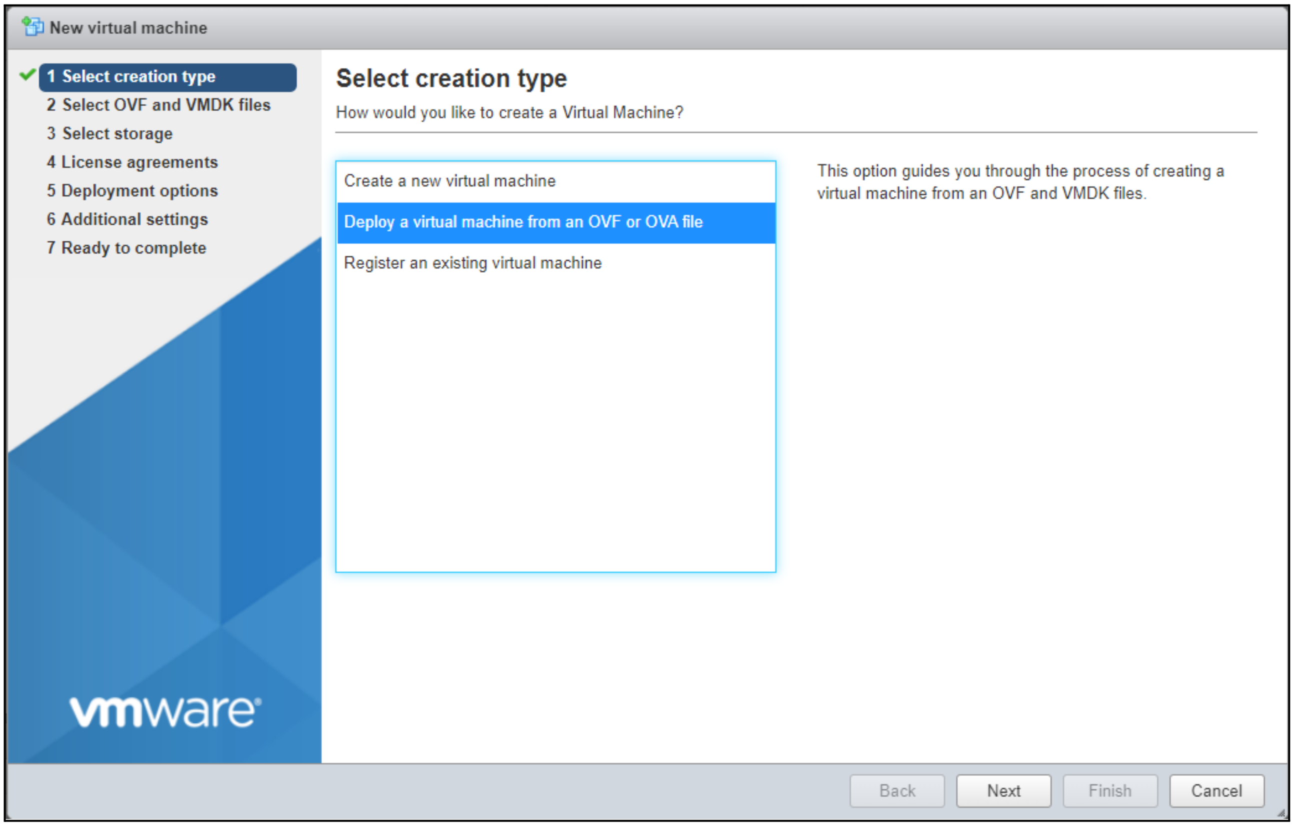
Name	Drive Type	Capacity	Provisioned	Free	Type
Database1	SSD	19.75 GB	1.41 GB	18.34 GB	VMFS6

10. Click the **Create / Register VM** to deploy a FusionHub virtual machine to the ESXi server.



No virtual machines

11. Select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.



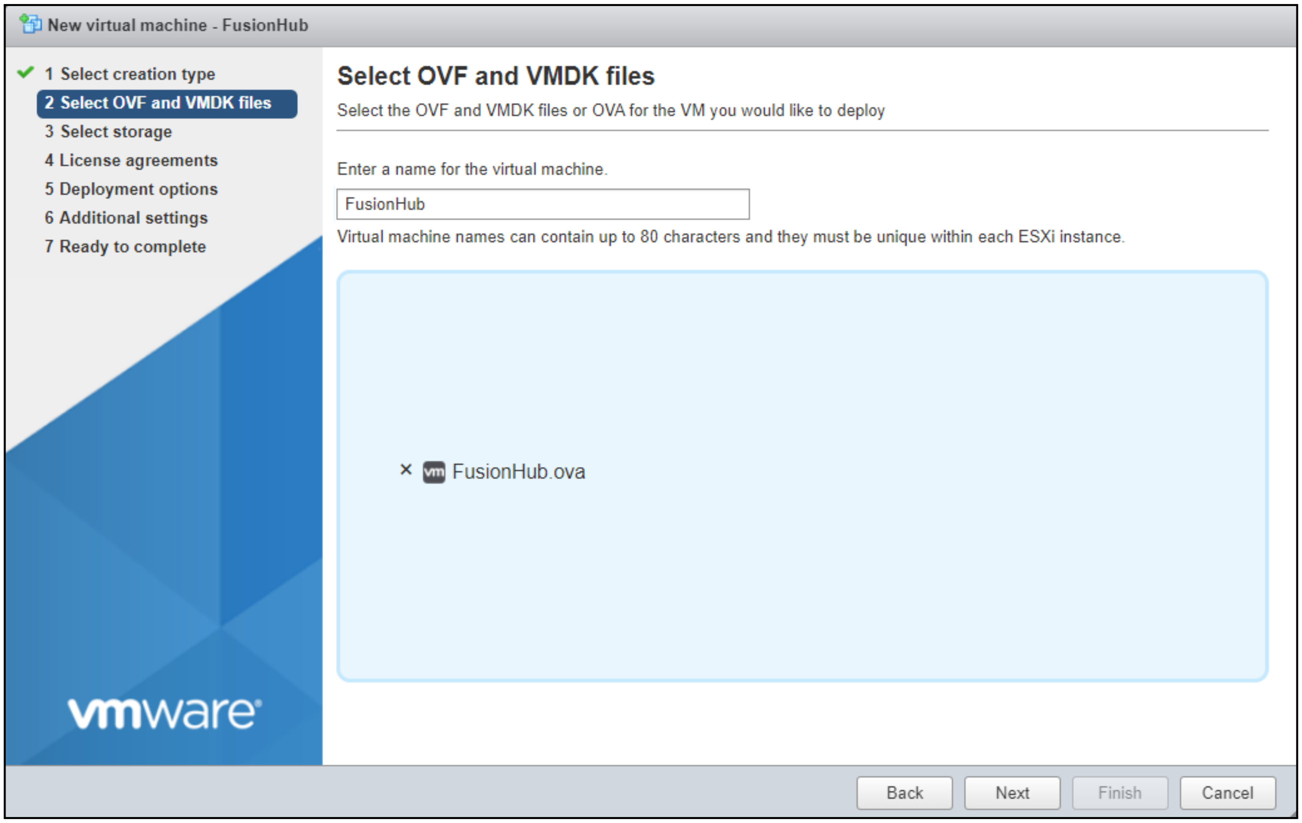
Select creation type

How would you like to create a Virtual Machine?

- Create a new virtual machine
- Deploy a virtual machine from an OVF or OVA file
- Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

12. Enter a name for the virtual machine and select either the OVF and VMDK files or the OVA file of the virtual machine that you would like to deploy.



New virtual machine - FusionHub

Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

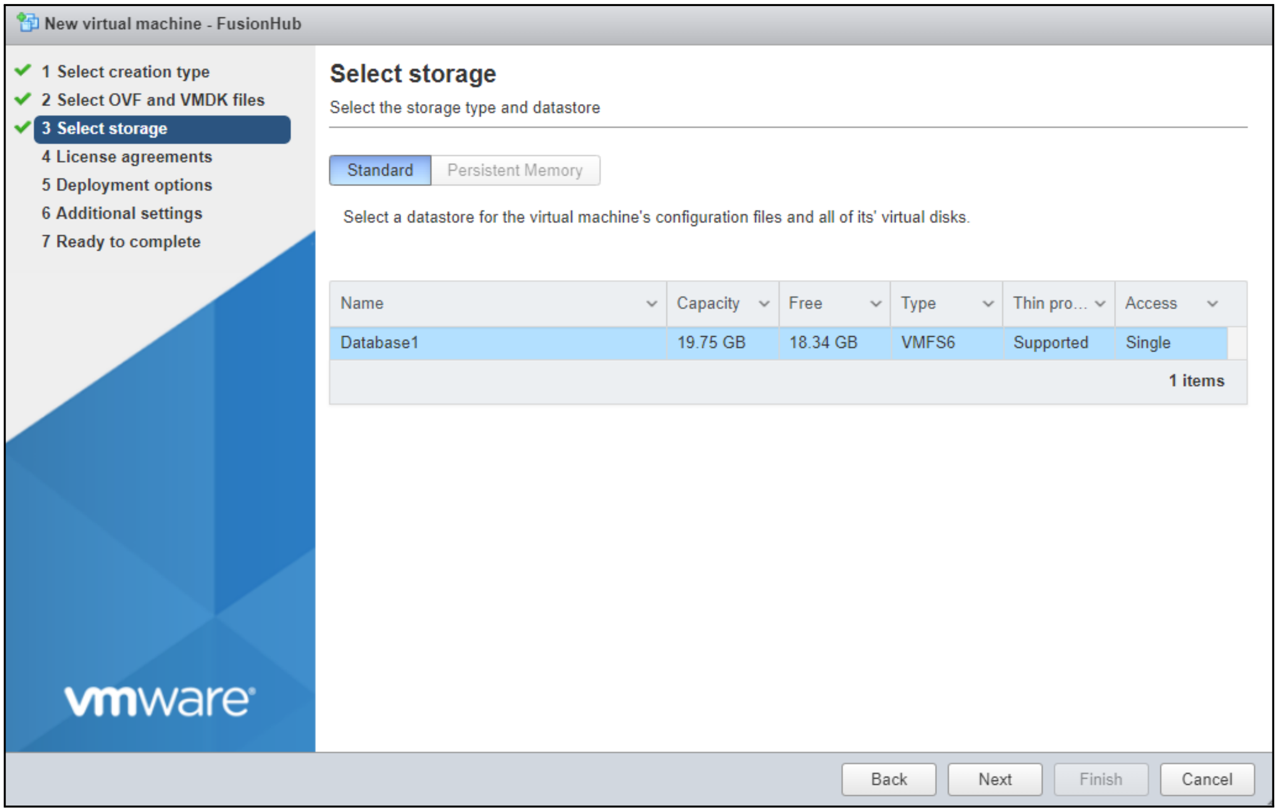
Enter a name for the virtual machine.

FusionHub

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

× FusionHub.ova

13. Select a storage type and the datastore in which you want to store the virtual machine’s configuration files and folders, and then click **Next**.



New virtual machine - FusionHub

✓ 1 Select creation type
✓ 2 Select OVF and VMDK files
✓ 3 Select storage
4 License agreements
5 Deployment options
6 Additional settings
7 Ready to complete

Select storage

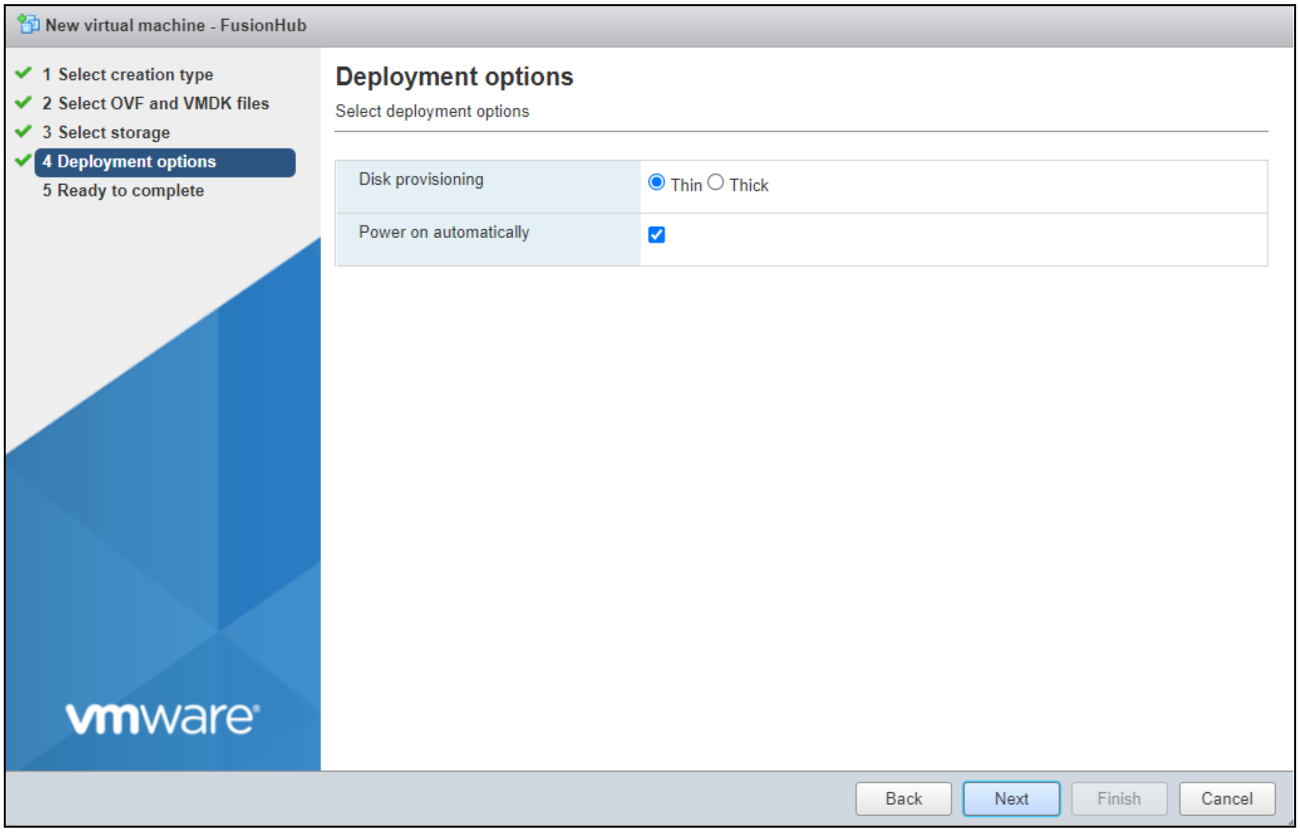
Select the storage type and datastore

Select a datastore for the virtual machine's configuration files and all of its' virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
Database1	19.75 GB	18.34 GB	VMFS6	Supported	Single

1 items

14. Select the desired **Deployment options** for disk provisioning and whether the virtual machine will power on automatically, then click **Next**.



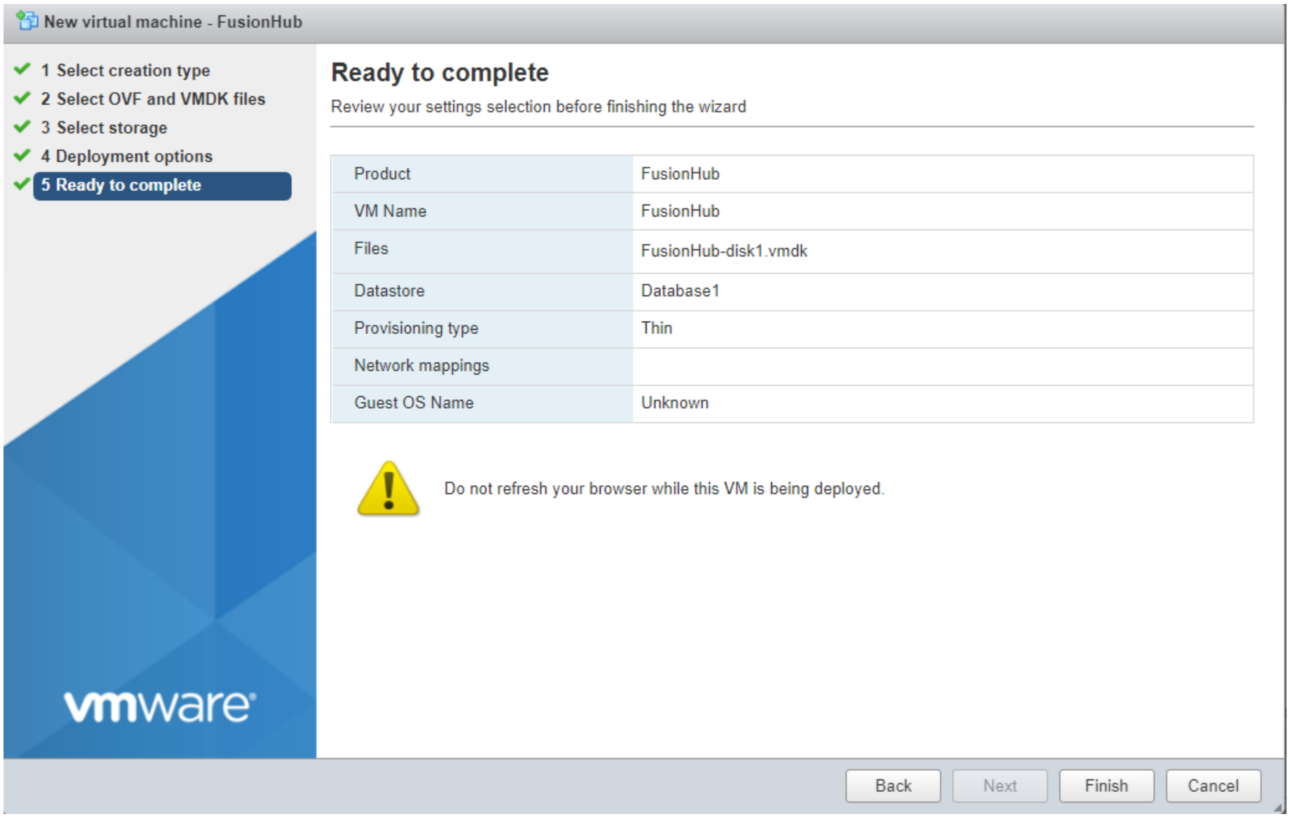
New virtual machine - FusionHub

Deployment options

Select deployment options

Disk provisioning	● Thin ○ Thick
Power on automatically	☑

15. Review the deployment settings in the **Ready to complete** dialog before clicking **Finish** to complete the process and close the wizard.



New virtual machine - FusionHub

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- ✓ 5 Ready to complete

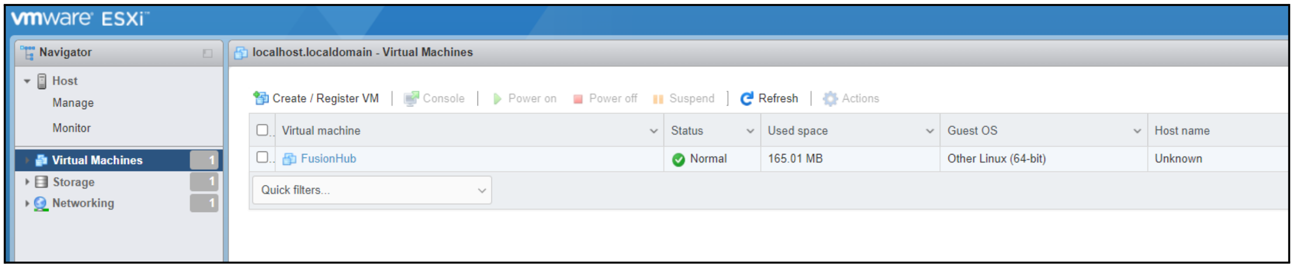
Ready to complete

Review your settings selection before finishing the wizard

Product	FusionHub
VM Name	FusionHub
Files	FusionHub-disk1.vmdk
Datastore	Database1
Provisioning type	Thin
Network mappings	
Guest OS Name	Unknown

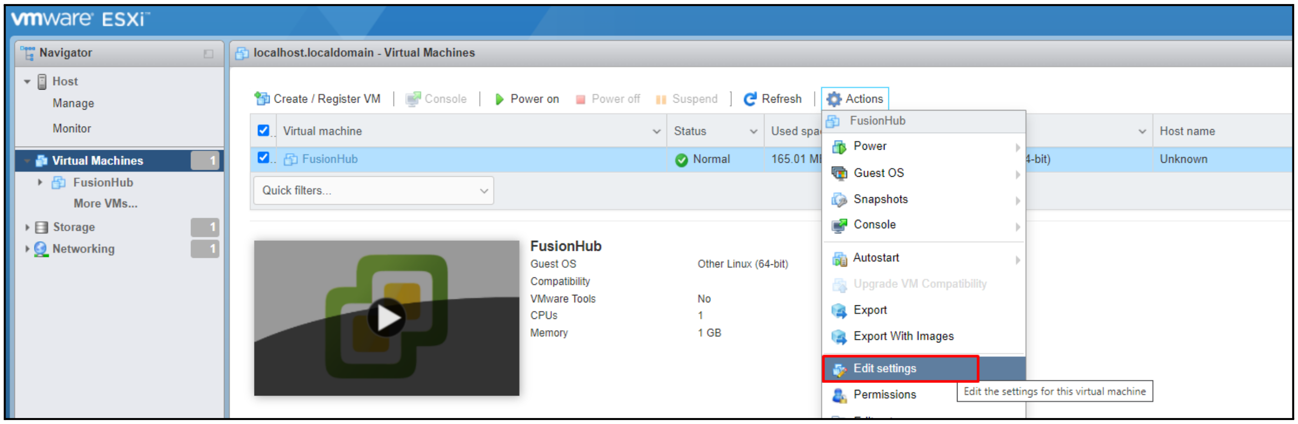
Do not refresh your browser while this VM is being deployed.

16. Once you have completed the steps above, a FusionHub Virtual Machine will be created.

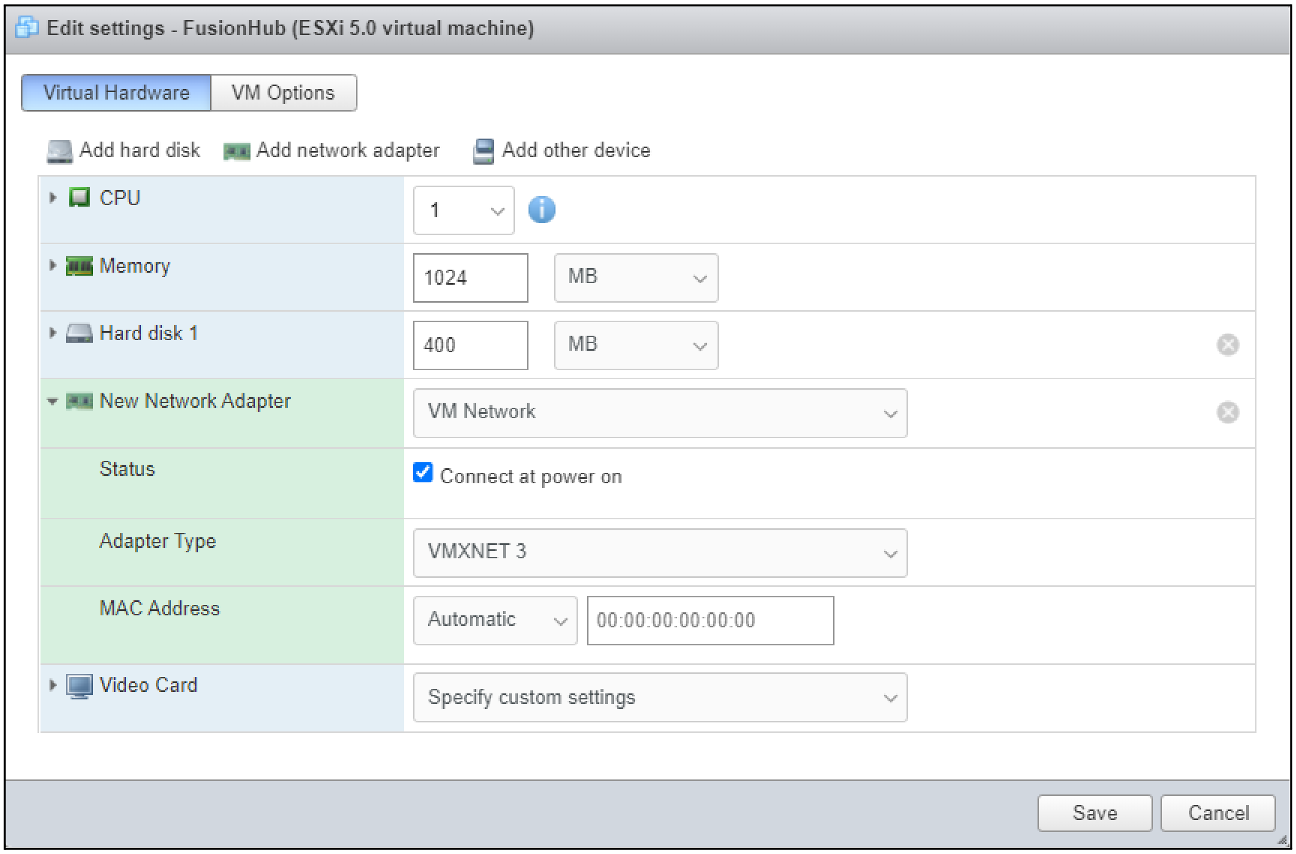


Virtual machine	Status	Used space	Guest OS	Host name
FusionHub	Normal	165.01 MB	Other Linux (64-bit)	Unknown

17. Click on **Actions** and select **Edit settings** to add a network adapter to the FusionHub virtual machine.



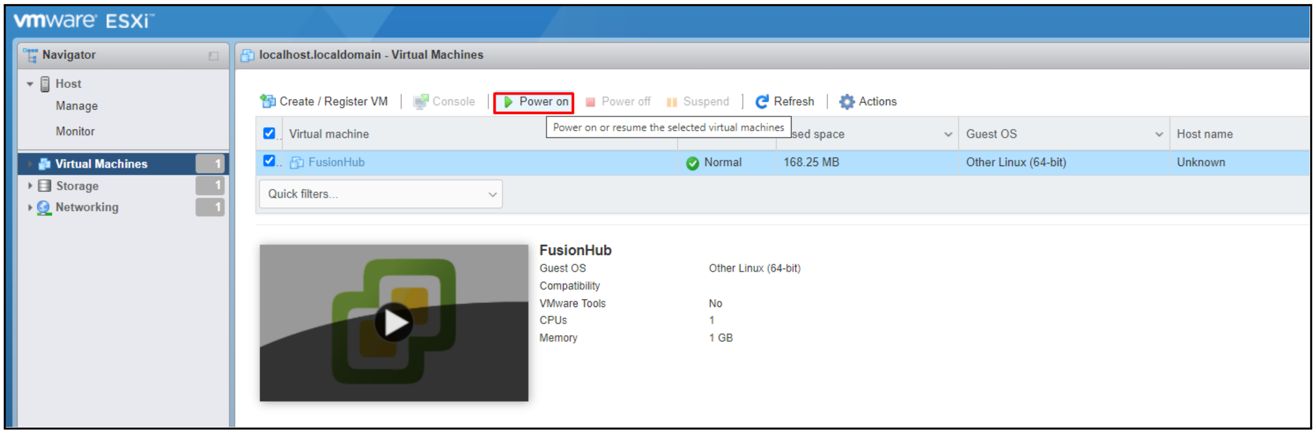
18. In the **Edit settings** dialog, expand the **New Network Adapter** tab. Change the **Adapter Type** to **VMXNET 3**. Tick the **Connect at power on** box to connect the NIC when the virtual machine is powered on. Click **Save**.



Edit settings - FusionHub (ESXi 5.0 virtual machine)

CPU	1
Memory	1024 MB
Hard disk 1	400 MB
New Network Adapter	VM Network
Status	☑ Connect at power on
Adapter Type	VMXNET 3
MAC Address	Automatic 00:00:00:00:00:00
Video Card	Specify custom settings

19. Click **Power on** to start the virtual machine and run FusionHub.

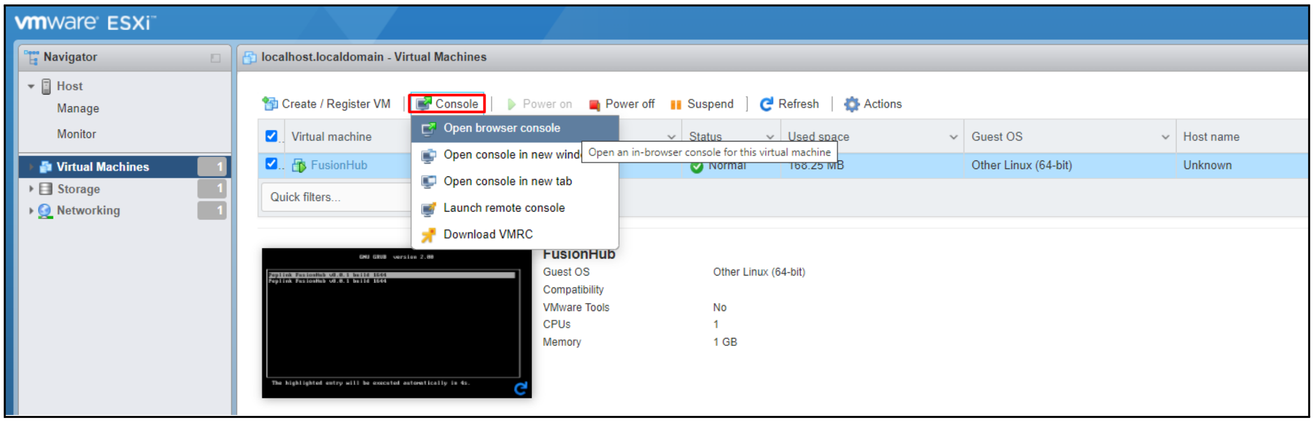


Virtual machine	Status	Used space	Guest OS	Host name
FusionHub	Normal	168.25 MB	Other Linux (64-bit)	Unknown

FusionHub

Guest OS	Other Linux (64-bit)
Compatibility	
VMware Tools	No
CPUs	1
Memory	1 GB

20. Select the desired virtual machine and then select a Launch Console option for the FusionHub.



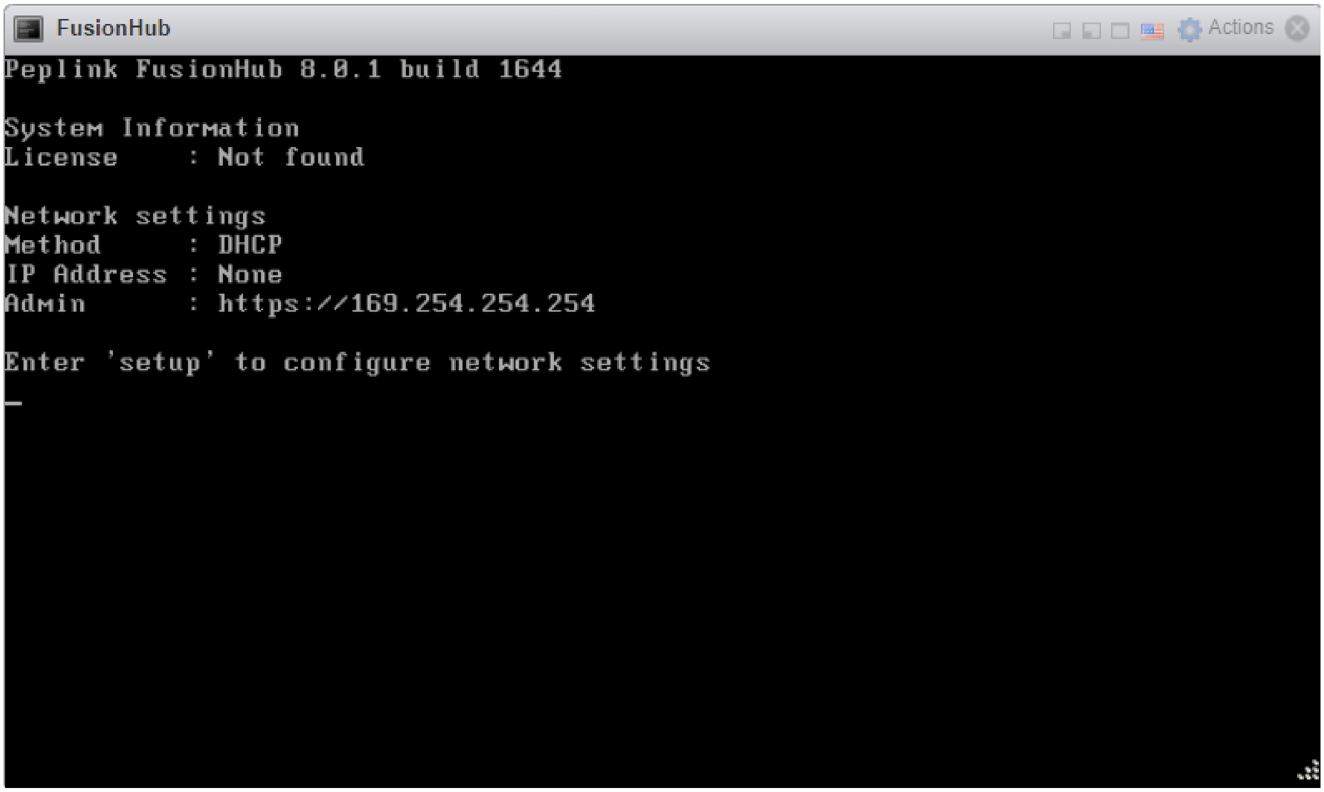
Virtual machine	Status	Used space	Guest OS	Host name
FusionHub	Normal	168.25 MB	Other Linux (64-bit)	Unknown

FusionHub

Guest OS	Other Linux (64-bit)
Compatibility	
VMware Tools	No
CPUs	1
Memory	1 GB

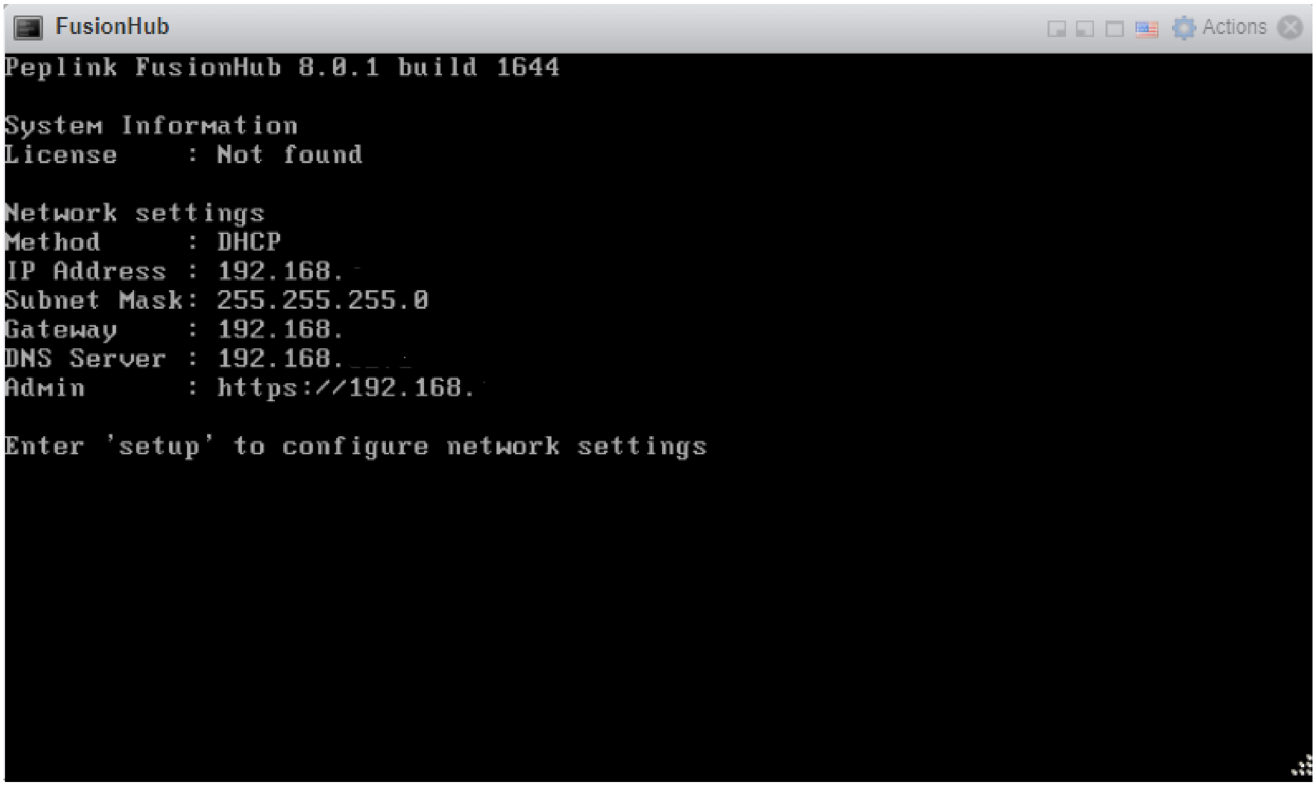
21. A browser/window will open after selecting Open Console, displaying general information about FusionHub, including:

- FusionHub version
- System information
- Network settings:
  Method: DHCP
  IP Address: None
  Admin: http://169.254.254.254



```
Peplink FusionHub 8.0.1 build 1644

System Information
License     : Not found

Network settings
Method      : DHCP
IP Address : None
Admin       : https://169.254.254.254

Enter 'setup' to configure network settings
_
```

22. The default WAN connection method is DHCP. If the DHCP server is available on your network, the FusionHub IP address will be automatically obtained by the DHCP server. In this case, the console will look similar to the following:



```
Peplink FusionHub 8.0.1 build 1644

System Information
License     : Not found

Network settings
Method      : DHCP
IP Address : 192.168.[redacted]
Subnet Mask: 255.255.255.0
Gateway     : 192.168.[redacted]
DNS Server : 192.168.[redacted]
Admin       : https://192.168.[redacted]

Enter 'setup' to configure network settings
```

Please navigate to **FusionHub Interface Configuration** to continue your installation.

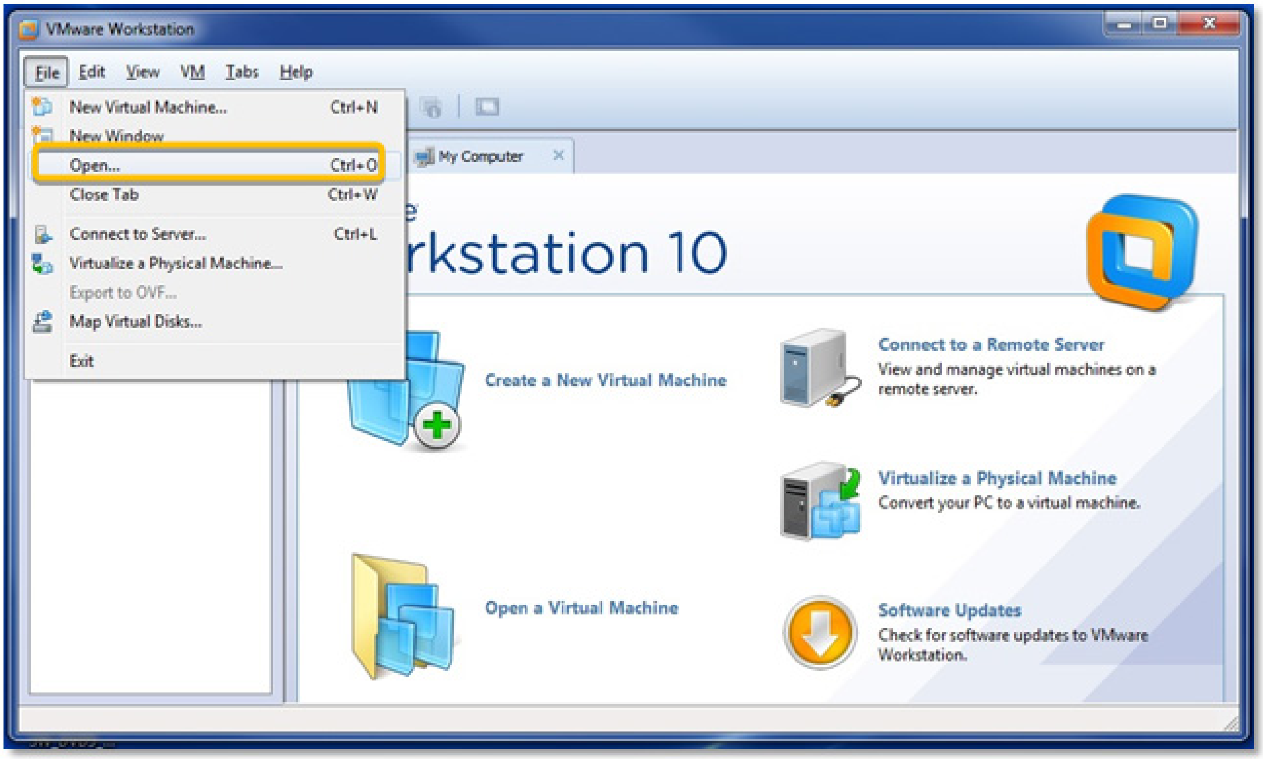
4.2. VMware Workstation

1. Click **FusionHub** in the column on the left side of the dialog to select the virtual machine. Click **Edit virtual machine settings** to begin adding an Ethernet adapter to the FusionHub virtual machine.

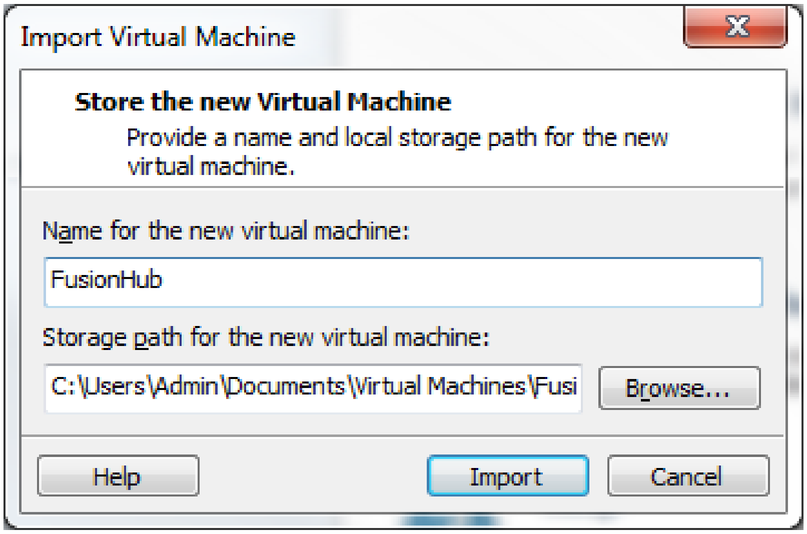
2. Download **VMware Workstation 10** from http://www.vmware.com/products/workstation/ and install it. For VMware Workstation installation hardware requirements, refer to http://pubs.vmware.com/workstation-10/index.jsp?topic=%2Fcom.vmware.ws.using.doc%2FGUID-55FF3F07-6C2E-41F7-B361-C7D870BCC4D7.html

3. Open VMware Workstation and deploy the OVF template.

4. Click **File > Open** to open the FusionHub.ova template downloaded from InControl 2.


VMware Workstation
File
Edit
View
VM
Tabs
Help
New Virtual Machine... Ctrl+N
New Window
Open... Ctrl+O
Close Tab Ctrl+W
Connect to Server... Ctrl+L
Virtualize a Physical Machine...
Export to OVF...
Map Virtual Disks...
Exit
My Computer
rkstation 10
Create a New Virtual Machine
Connect to a Remote Server
View and manage virtual machines on a remote server.
Virtualize a Physical Machine
Convert your PC to a virtual machine.
Open a Virtual Machine
Software Updates
Check for software updates to VMware Workstation.

5. On the Store the new Virtual Machine dialog, type a name for the new virtual machine (i.e., FusionHub) and select the storage path. Please note that the storage path for this FusionHub virtual machine should not be the same as for the downloaded FusionHub OVF template file. Click Import.



Import Virtual Machine

Store the new Virtual Machine

Provide a name and local storage path for the new virtual machine.

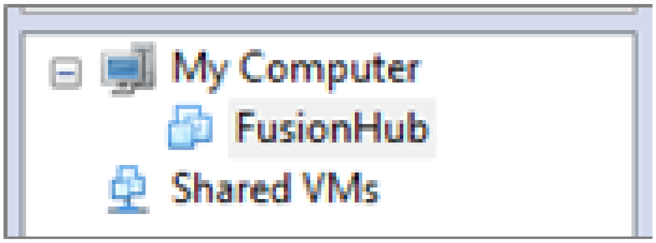
Name for the new virtual machine:

FusionHub

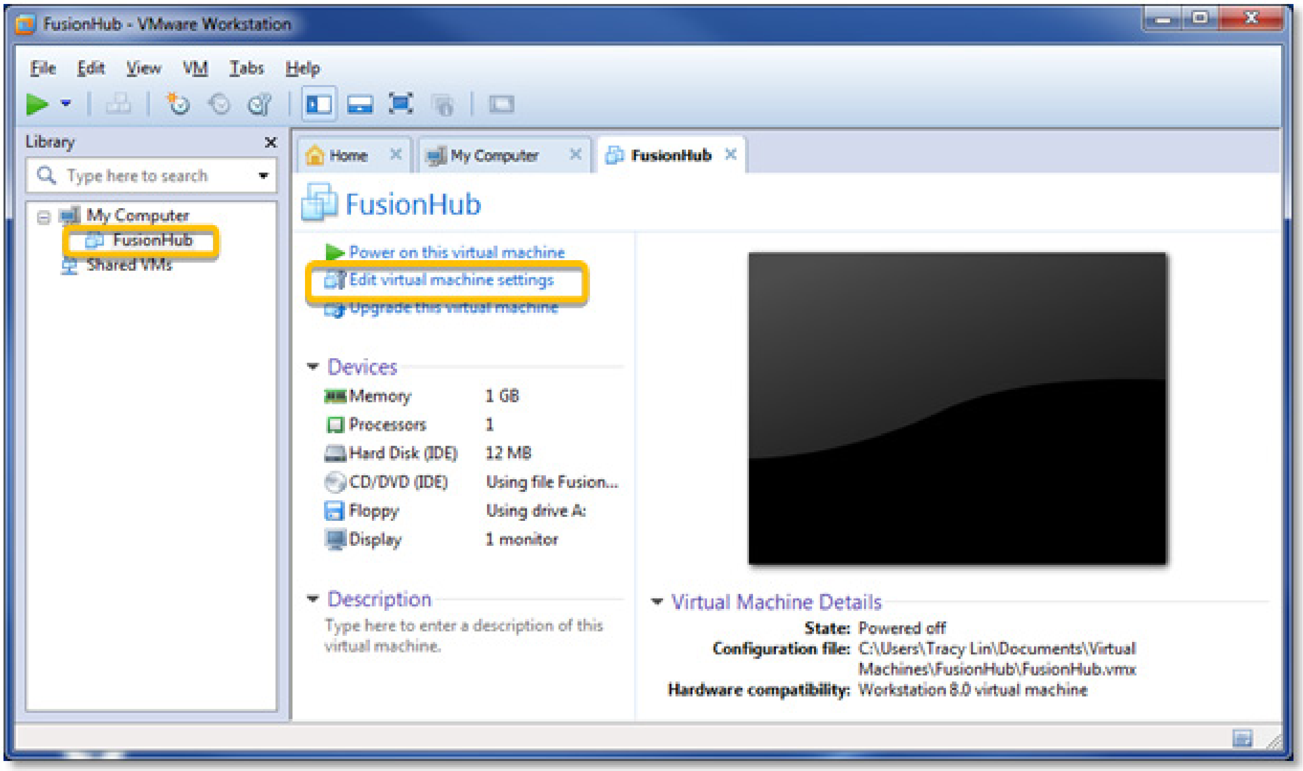
Storage path for the new virtual machine:

C:\Users\Admin\Documents\Virtual Machines\Fusi

6. After successful import, a FusionHub virtual machine is created.



7. Click **FusionHub** in the column on the left side of the dialog to select the virtual machine. Click **Edit virtual machine settings** to begin adding an Ethernet adapter.

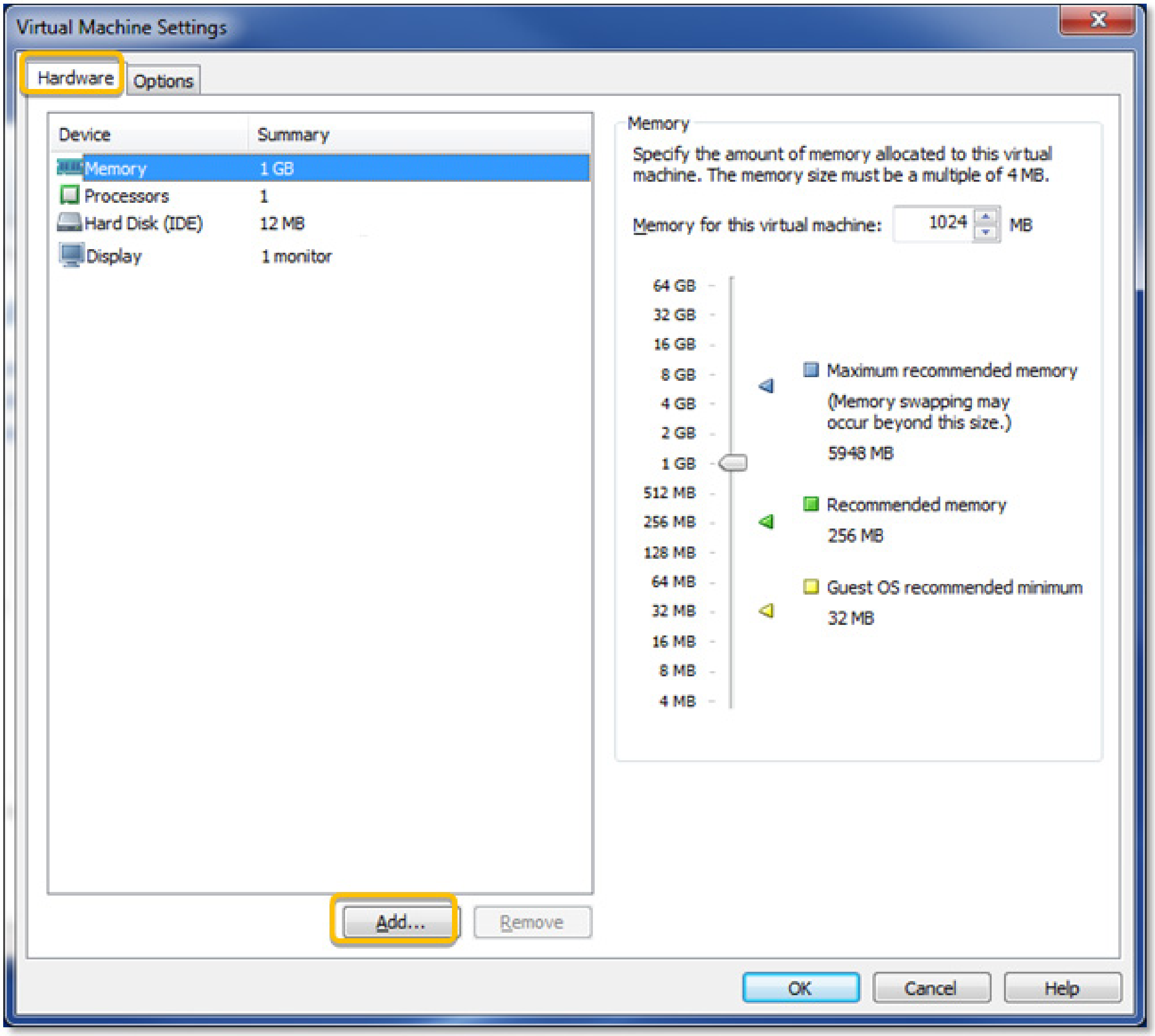


Memory	1 GB
Processors	1
Hard Disk (IDE)	12 MB
CD/DVD (IDE)	Using file Fusion...
Floppy	Using drive A:
Display	1 monitor

Type here to enter a description of this virtual machine.

State: Powered off
Configuration file: C:\Users\Tracy Lin\Documents\Virtual Machines\FusionHub\FusionHub.vmx
Hardware compatibility: Workstation 8.0 virtual machine

8. Click **Add**, found under the **Hardware** tab on the **Virtual Machine Settings** dialog.



Device	Summary
Memory	1 GB
Processors	1
Hard Disk (IDE)	12 MB
Display	1 monitor

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

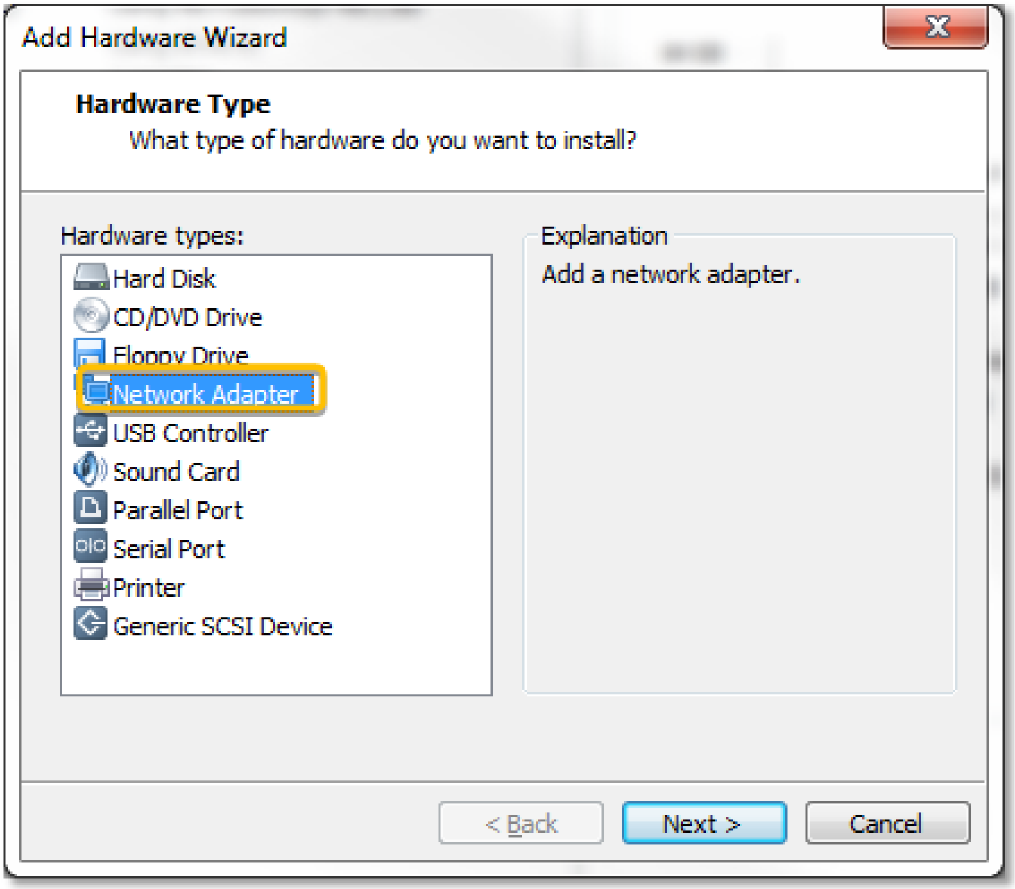
Memory for this virtual machine: 1024 MB

Maximum recommended memory
(Memory swapping may occur beyond this size.)
5948 MB

Recommended memory
256 MB

Guest OS recommended minimum
32 MB

9. On the Add Hardware Wizard dialog, select Network Adapter. Click Next.



Add Hardware Wizard

Hardware Type

What type of hardware do you want to install?

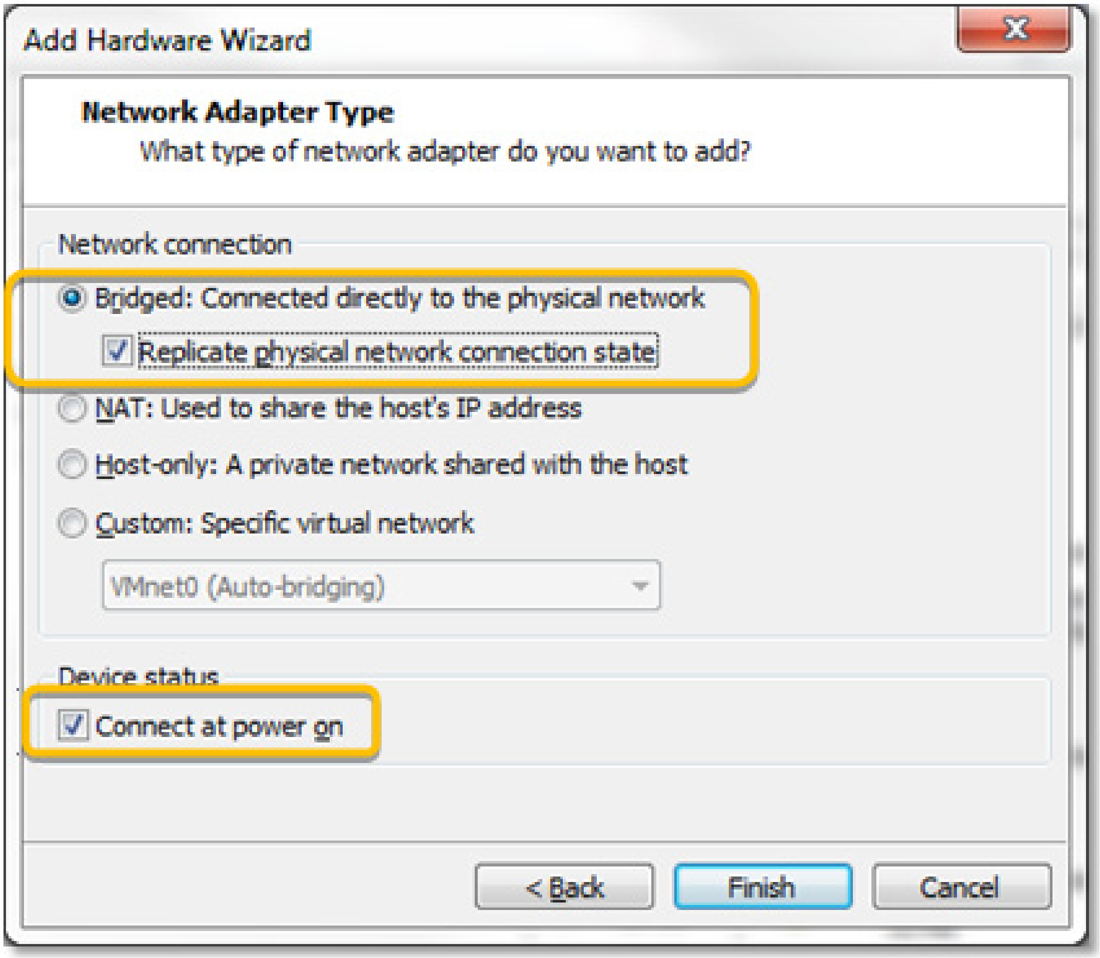
Hardware types:

- Hard Disk
- CD/DVD Drive
- Floppy Drive
- Network Adapter
- USB Controller
- Sound Card
- Parallel Port
- Serial Port
- Printer
- Generic SCSI Device

Explanation

Add a network adapter.

10. On the Network Adapter Type dialog, select Bridged: Connected directly to the physical network and Replicate physical network connection state. Check Connect at power on and click Finish.



Add Hardware Wizard

Network Adapter Type

What type of network adapter do you want to add?

Network connection

● Bridged: Connected directly to the physical network

☑ Replicate physical network connection state

○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

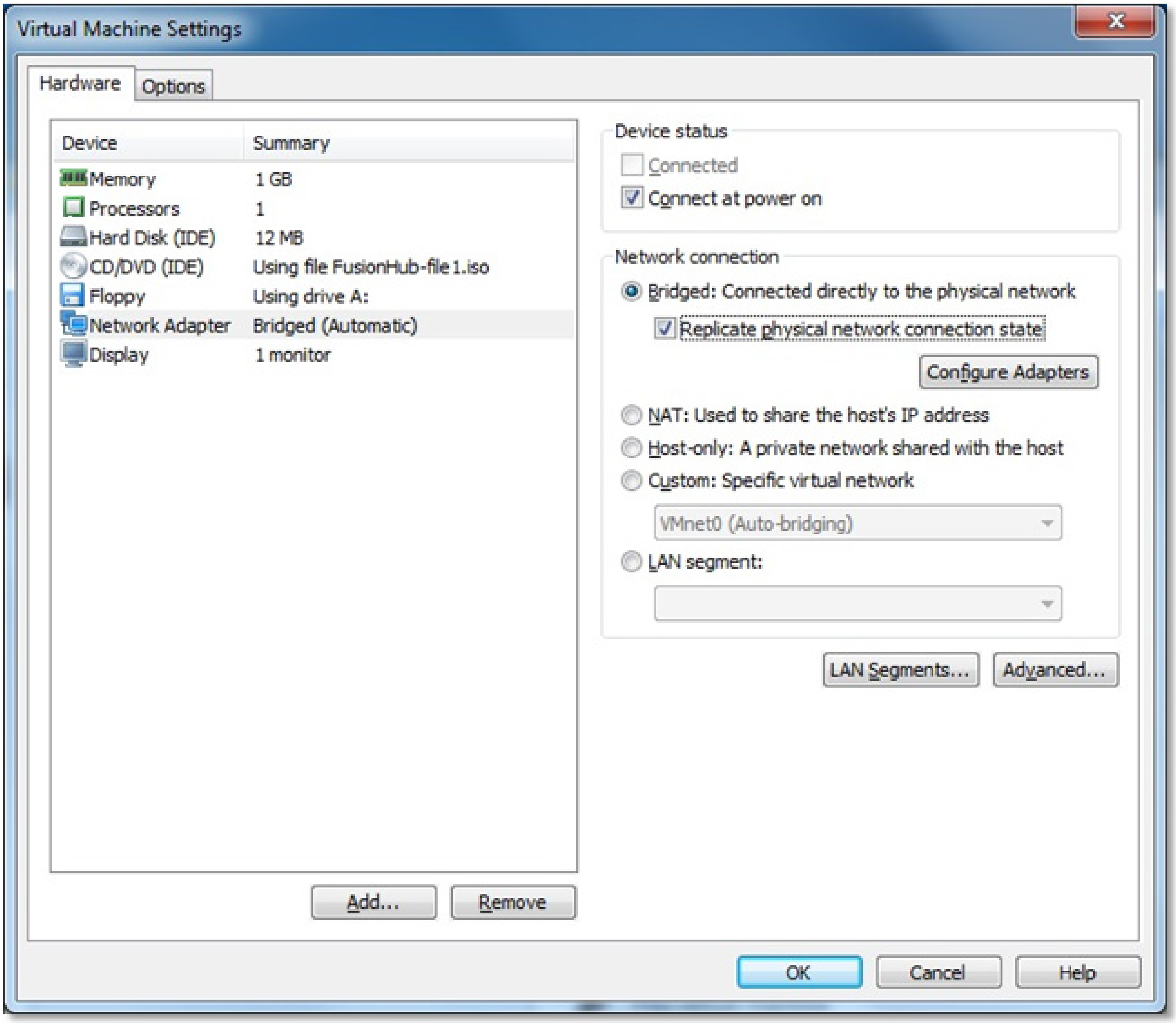
○ Custom: Specific virtual network

VMnet0 (Auto-bridging)

Device status

☑ Connect at power on

11. Click **Configure Adapters** to select the host adapter. This will apply only if you have more than one network adapter. Otherwise, skip this step.



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	1 GB
Processors	1
Hard Disk (IDE)	12 MB
CD/DVD (IDE)	Using file FusionHub-file1.iso
Floppy	Using drive A:
Network Adapter	Bridged (Automatic)
Display	1 monitor

Device status

□ Connected

☑ Connect at power on

Network connection

● Bridged: Connected directly to the physical network

☑ Replicate physical network connection state

○ NAT: Used to share the host's IP address

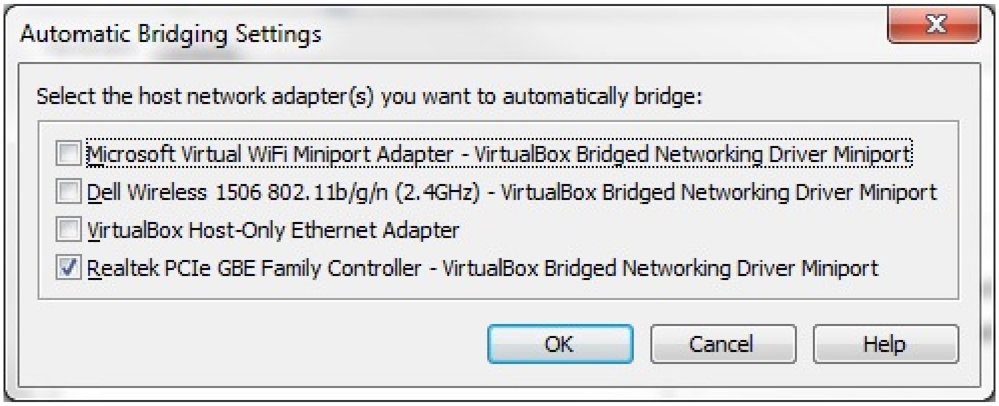
○ Host-only: A private network shared with the host

○ Custom: Specific virtual network

VMnet0 (Auto-bridging)

○ LAN segment:

12. When the **Automatic Bridging Settings** dialog opens, select the host network adapter you want to automatically bridge and click **OK**.



Automatic Bridging Settings

Select the host network adapter(s) you want to automatically bridge:

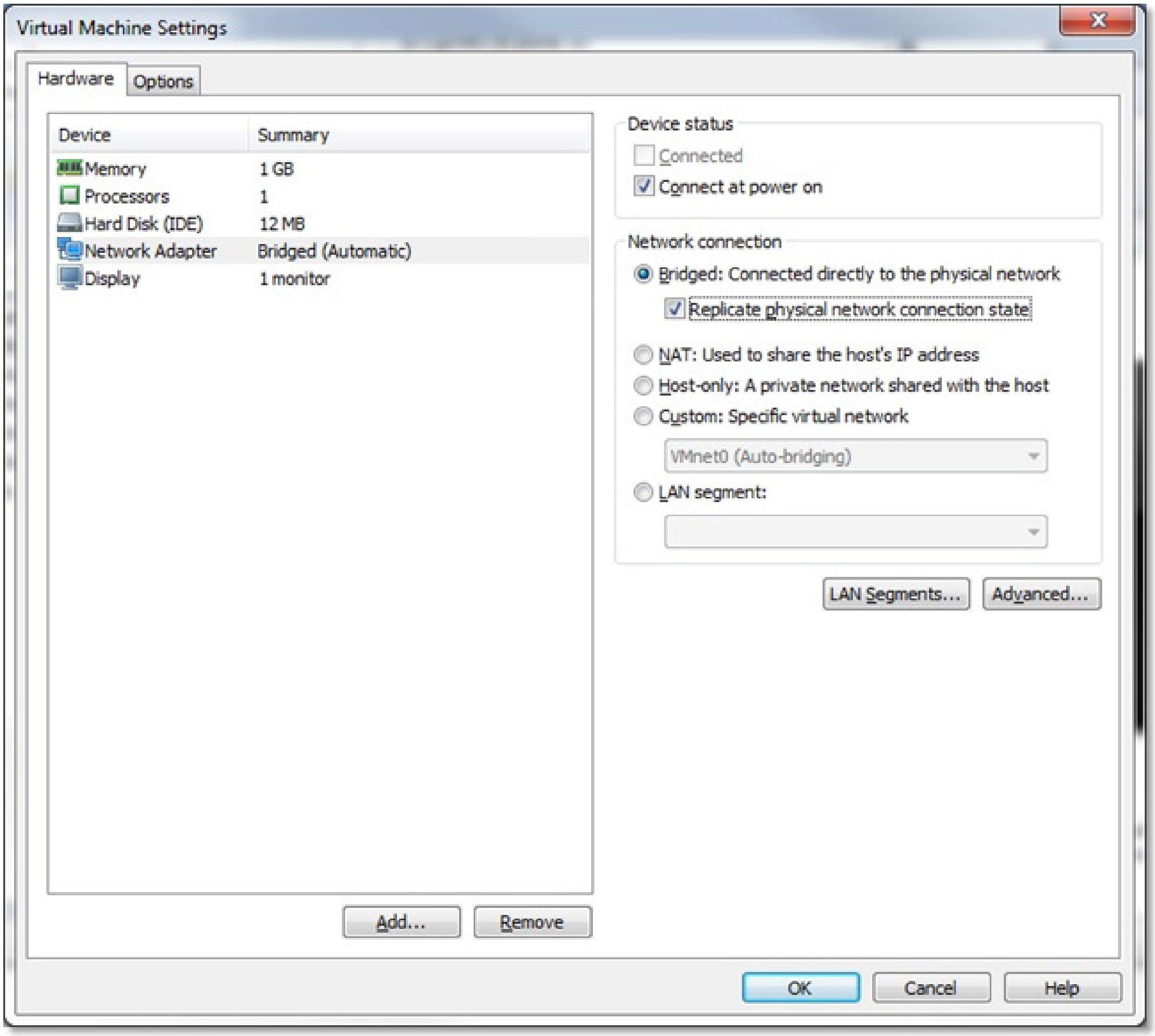
□ Microsoft Virtual WiFi Miniport Adapter - VirtualBox Bridged Networking Driver Miniport

□ Dell Wireless 1506 802.11b/g/n (2.4GHz) - VirtualBox Bridged Networking Driver Miniport

□ VirtualBox Host-Only Ethernet Adapter

☑ Realtek PCIe GBE Family Controller - VirtualBox Bridged Networking Driver Miniport

13. Click **OK** to finish adding hardware.



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	1 GB
Processors	1
Hard Disk (IDE)	12 MB
Network Adapter	Bridged (Automatic)
Display	1 monitor

Device status

□ Connected

☑ Connect at power on

Network connection

● Bridged: Connected directly to the physical network

☑ Replicate physical network connection state

○ NAT: Used to share the host's IP address

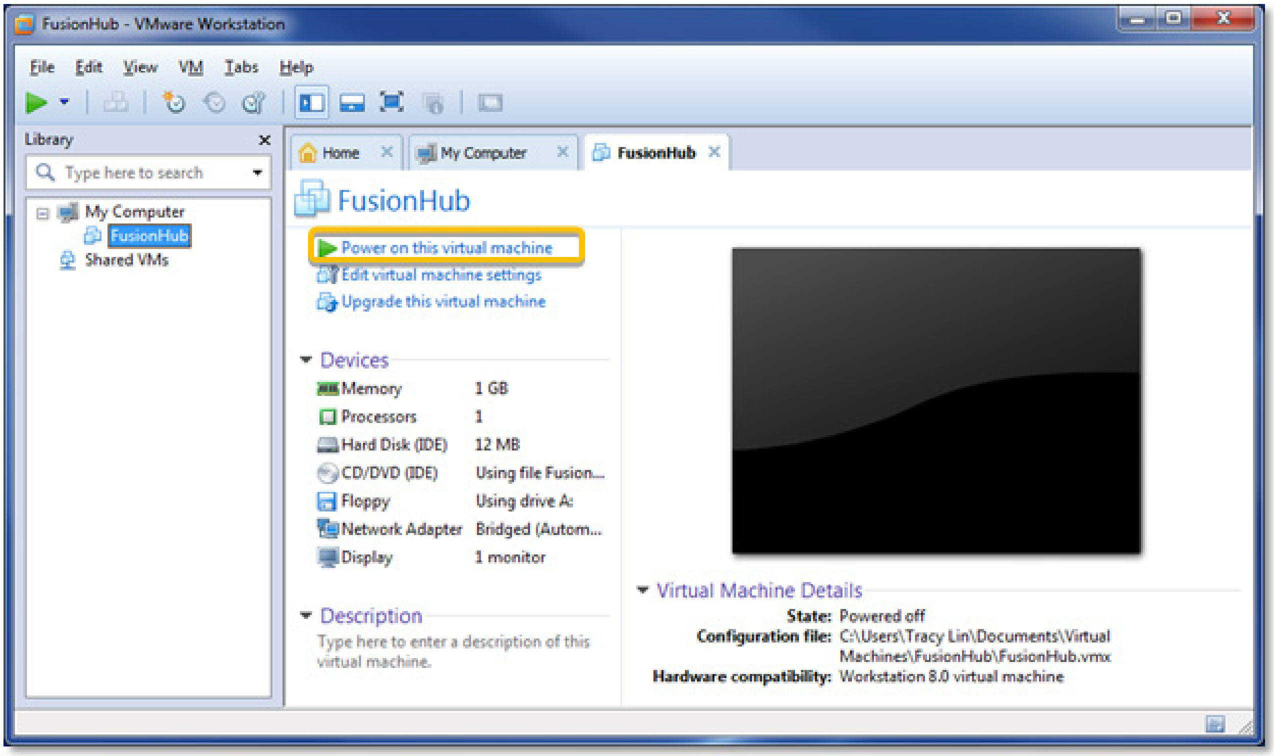
○ Host-only: A private network shared with the host

○ Custom: Specific virtual network

VMnet0 (Auto-bridging)

○ LAN segment:

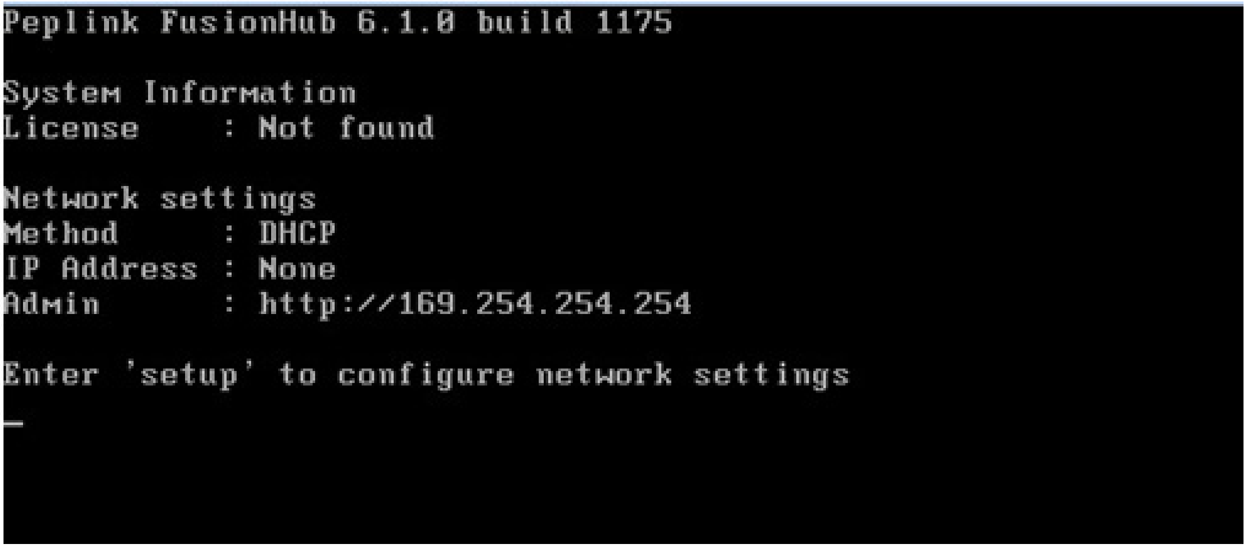
14. Click Power on this virtual machine to run FusionHub.


FusionHub - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
FusionHub
Shared VMs
Home
My Computer
FusionHub
FusionHub
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Devices
Description
Type here to enter a description of this virtual machine.
Virtual Machine Details

```
Memory              1 GB
Processors          1
Hard Disk (IDE)     12 MB
CD/DVD (IDE)        Using file Fusion...
Floppy              Using drive A:
Network Adapter     Bridged (Autom...
Display             1 monitor
```

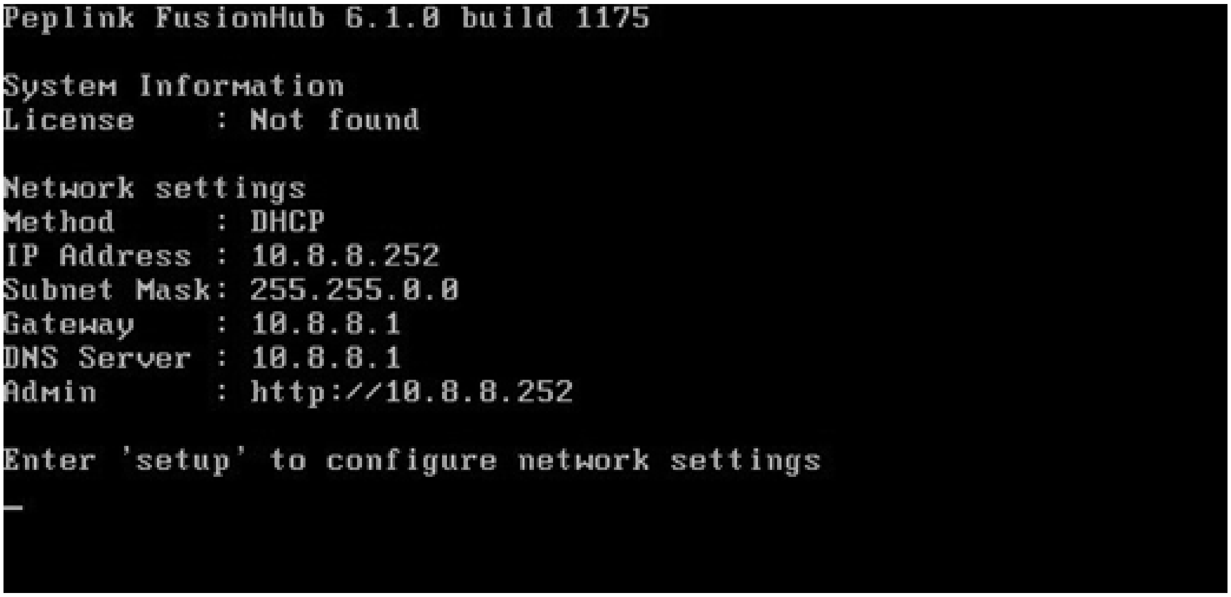
State: Powered off
Configuration file: C:\Users\Tracy Lin\Documents\Virtual Machines\FusionHub\FusionHub.vmx
Hardware compatibility: Workstation 8.0 virtual machine

15. The FusionHub console opens automatically and displays the following general information about FusionHub:
    - FusionHub version
    - System information
    - Network settings:
      Method: DHCP
      IP Address: None
      Admin: http://169.254.254.254



```
Peplink FusionHub 6.1.0 build 1175

System Information
License     : Not found

Network settings
Method      : DHCP
IP Address  : None
Admin       : http://169.254.254.254

Enter 'setup' to configure network settings
_
```

16. The default WAN connection method is DHCP. If the DHCP server is available on your network, the IP address of FusionHub will be automatically obtained by DHCP server. In this case, the console will look similar to the following.



```
Peplink FusionHub 6.1.0 build 1175

System Information
License     : Not found

Network settings
Method      : DHCP
IP Address  : 10.8.8.252
Subnet Mask: 255.255.0.0
Gateway     : 10.8.8.1
DNS Server  : 10.8.8.1
Admin       : http://10.8.8.252

Enter 'setup' to configure network settings
_
```

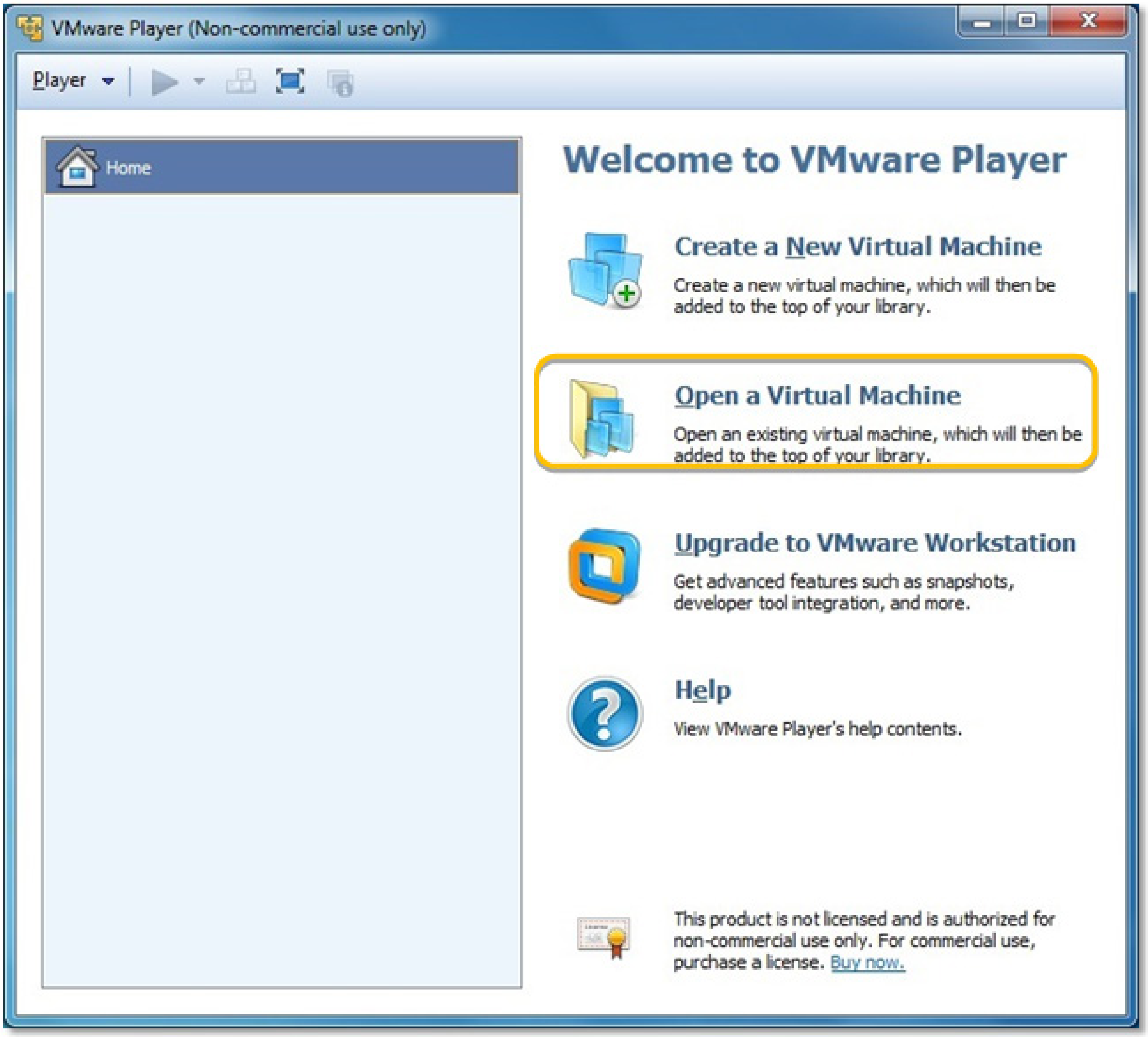
Please navigate to **FusionHub Interface Configuration** to continue your installation.

4.3. VMware Player

1. Download VMware Player 6.0 from the link below and install it. **https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_player/6_0**

2. Open **VMware Player** and install FusionHub.

3. Click **Open a Virtual Machine** to import the FusionHub.ova template downloaded from InControl 2.



VMware Player (Non-commercial use only)

Welcome to VMware Player

Create a New Virtual Machine

Create a new virtual machine, which will then be added to the top of your library.

Open a Virtual Machine

Open an existing virtual machine, which will then be added to the top of your library.

Upgrade to VMware Workstation

Get advanced features such as snapshots, developer tool integration, and more.

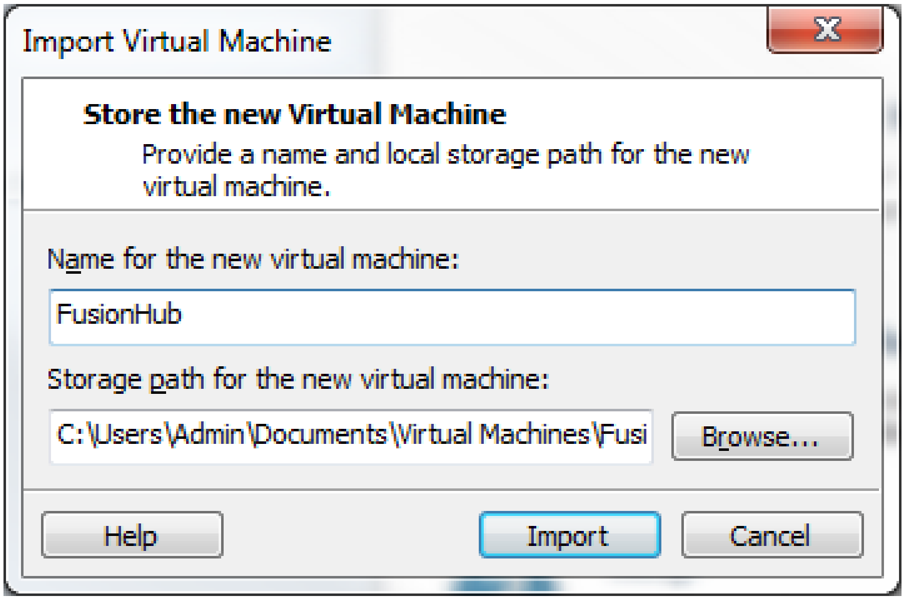
Help

View VMware Player's help contents.

This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.

4. On the Store the new Virtual Machine dialog, type a name for the new virtual machine (i.e., FusionHub) and select the storage path. Please note that the storage path for this FusionHub virtual machine should not be the same as that for the downloaded FusionHub

OVF template file. Click Import.



Import Virtual Machine

Store the new Virtual Machine

Provide a name and local storage path for the new virtual machine.

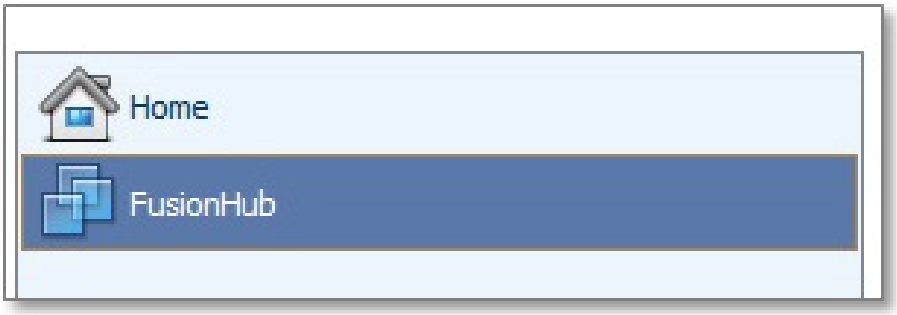
Name for the new virtual machine:

FusionHub

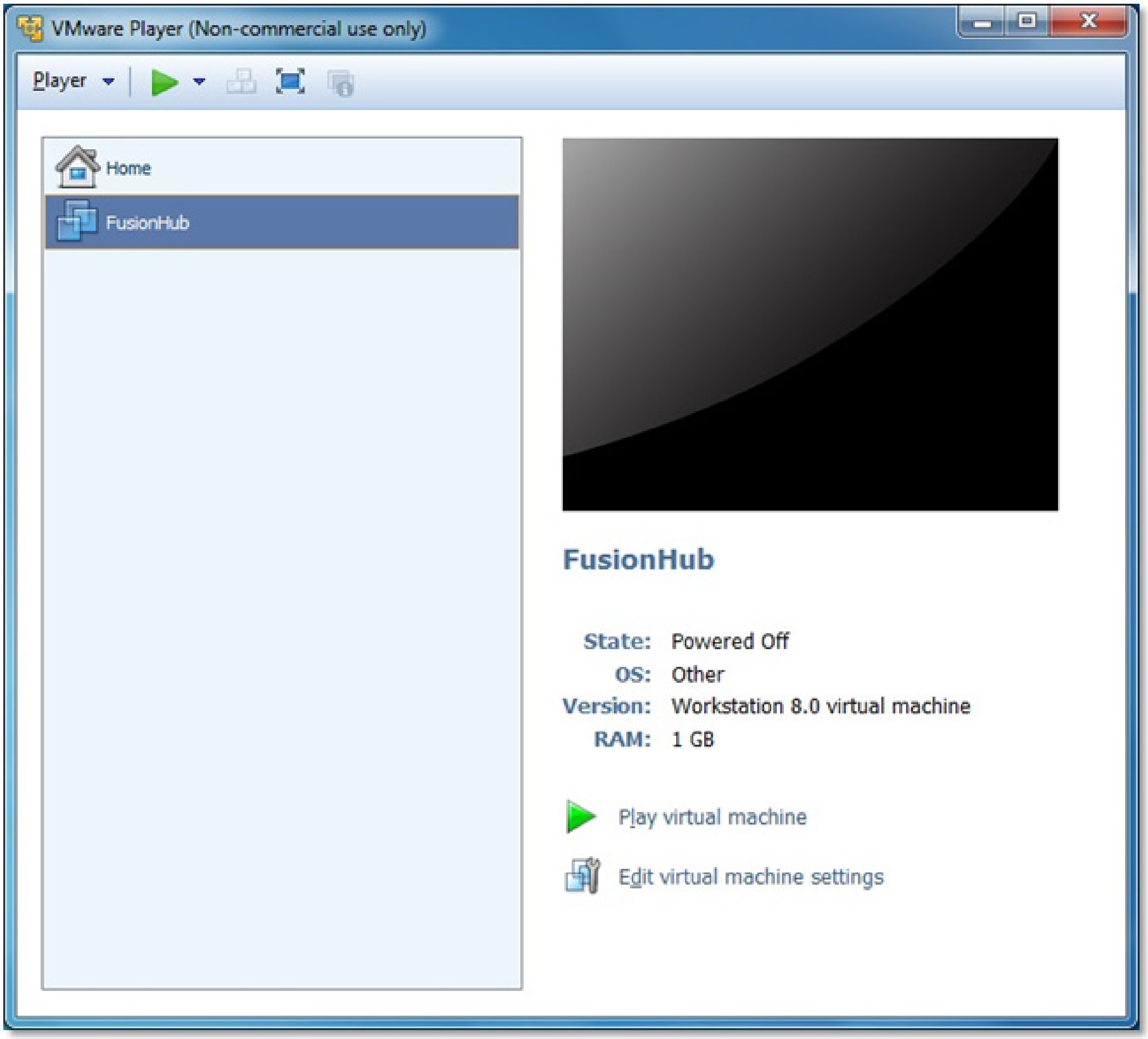
Storage path for the new virtual machine:

C:\Users\Admin\Documents\Virtual Machines\Fusi

5. After successful import, a FusionHub virtual machine is created.



6. Click **FusionHub** in the column on the left side of the dialog to select the virtual machine. Click **Edit virtual machine settings** to begin adding an Ethernet adapter to the FusionHub virtual machine.

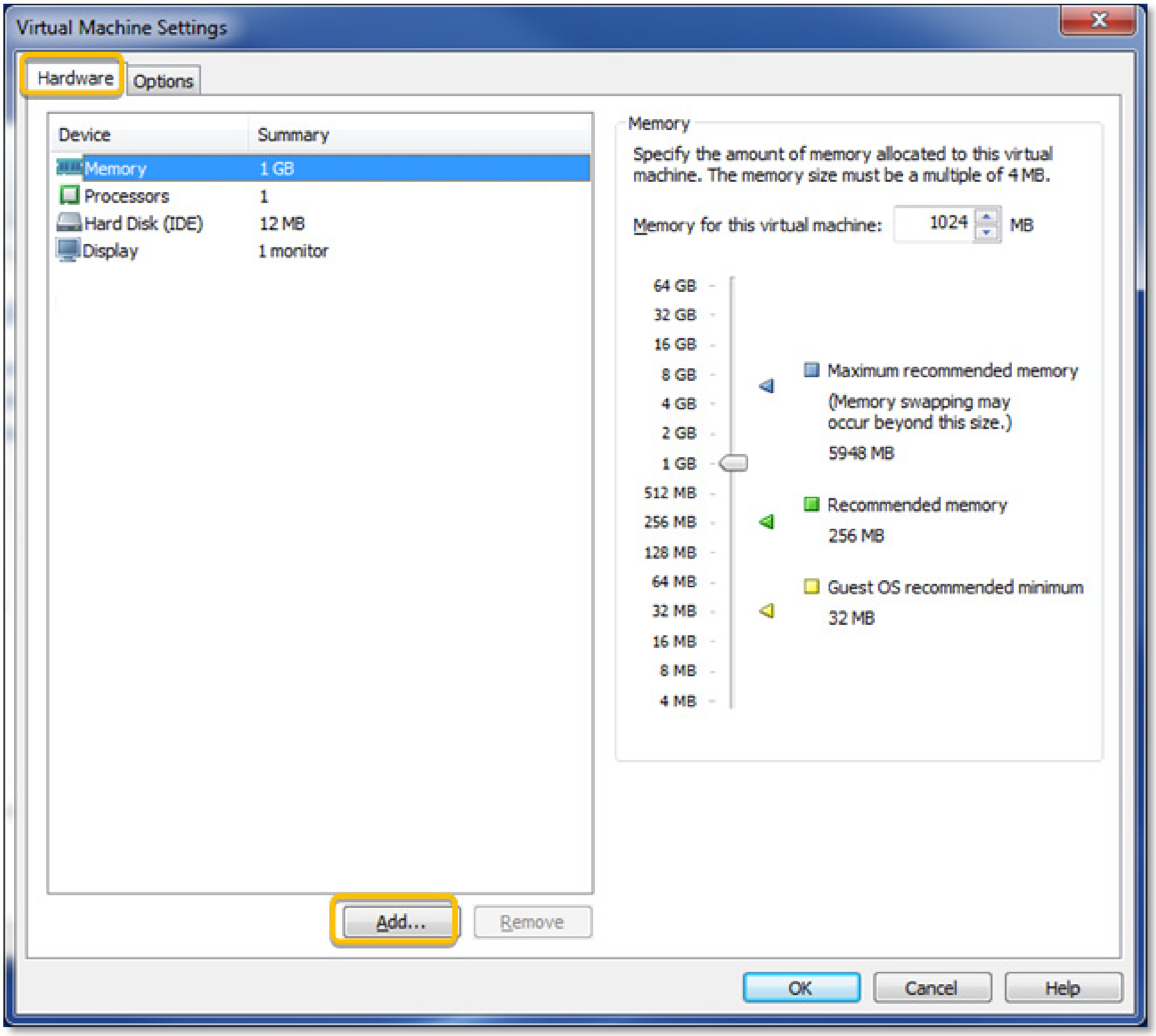

VMware Player (Non-commercial use only)
Player
Home
FusionHub

FusionHub

State: Powered Off
OS: Other
Version: Workstation 8.0 virtual machine
RAM: 1 GB

Play virtual machine
Edit virtual machine settings

7. Click **Add**, found under the **Hardware** tab on the **Virtual Machine Settings** dialog.



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	1 GB
Processors	1
Hard Disk (IDE)	12 MB
Display	1 monitor

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

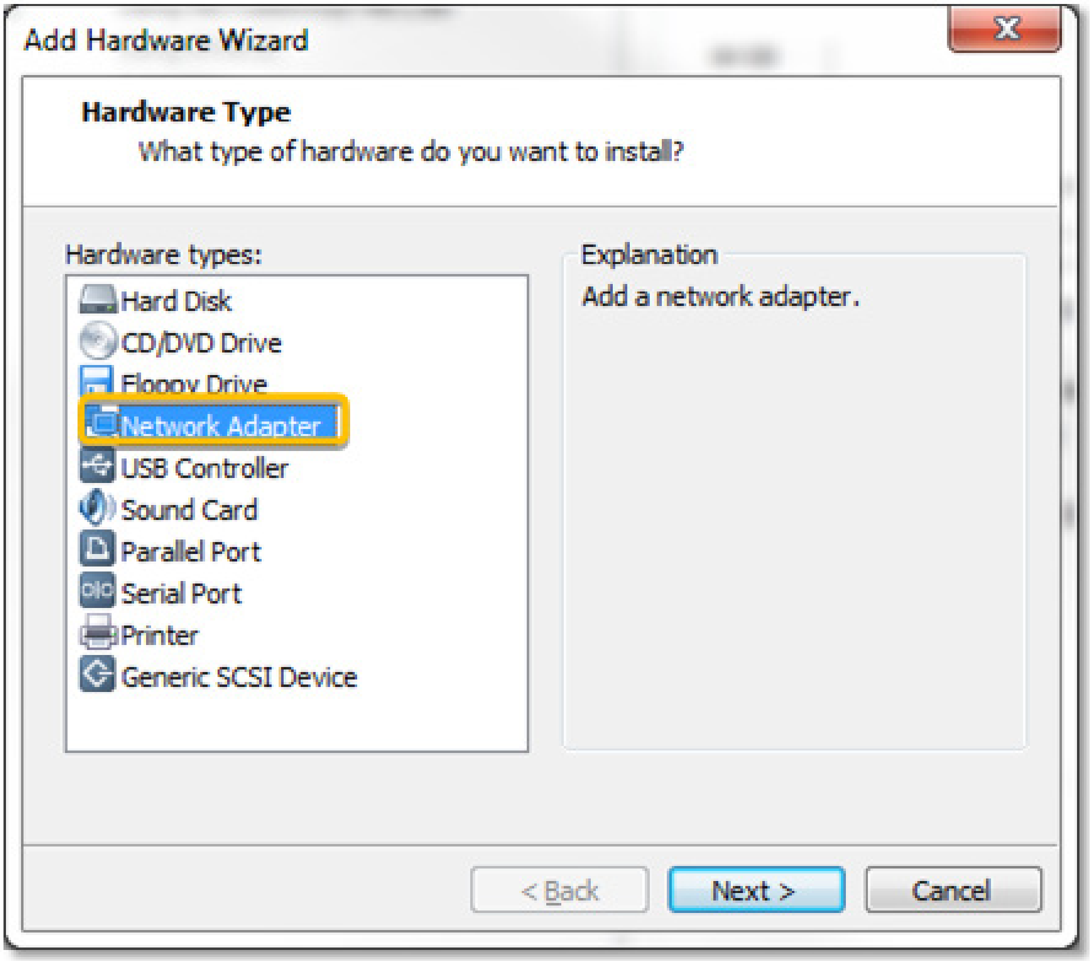
Memory for this virtual machine: 1024 MB

🟦 Maximum recommended memory (Memory swapping may occur beyond this size.) 5948 MB

🟩 Recommended memory 256 MB

🟨 Guest OS recommended minimum 32 MB

8. On the Add Hardware Wizard dialog, select Network Adapter. Click Next.



Add Hardware Wizard

Hardware Type

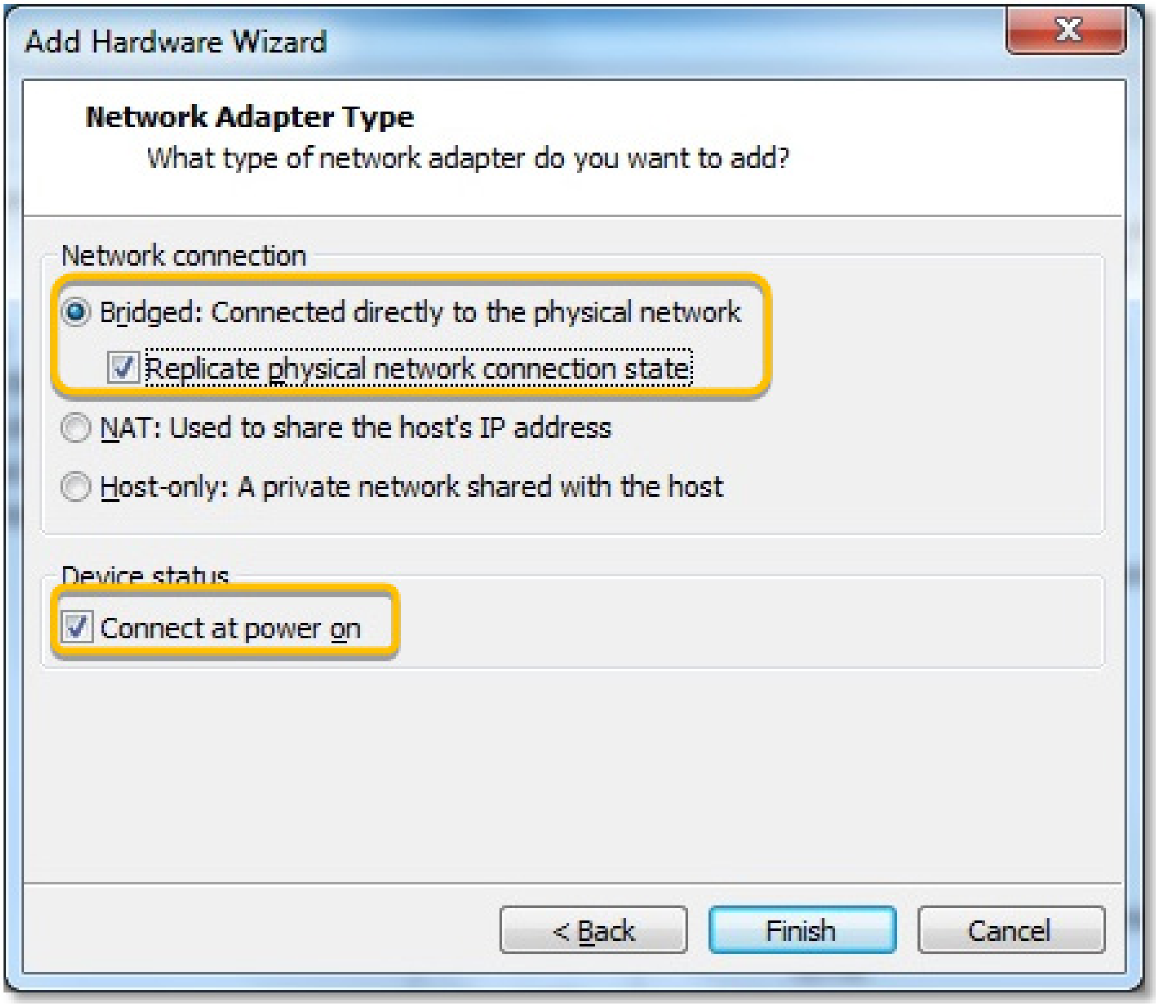
What type of hardware do you want to install?

Hardware types: Network Adapter

Explanation

Add a network adapter.

9. On the Network Adapter Type dialog, select Bridged: Connected directly to the physical network and Replicate physical network connection state. Check Connect at power on and click Finish.



Add Hardware Wizard

Network Adapter Type

What type of network adapter do you want to add?

Network connection

● Bridged: Connected directly to the physical network

☑ Replicate physical network connection state

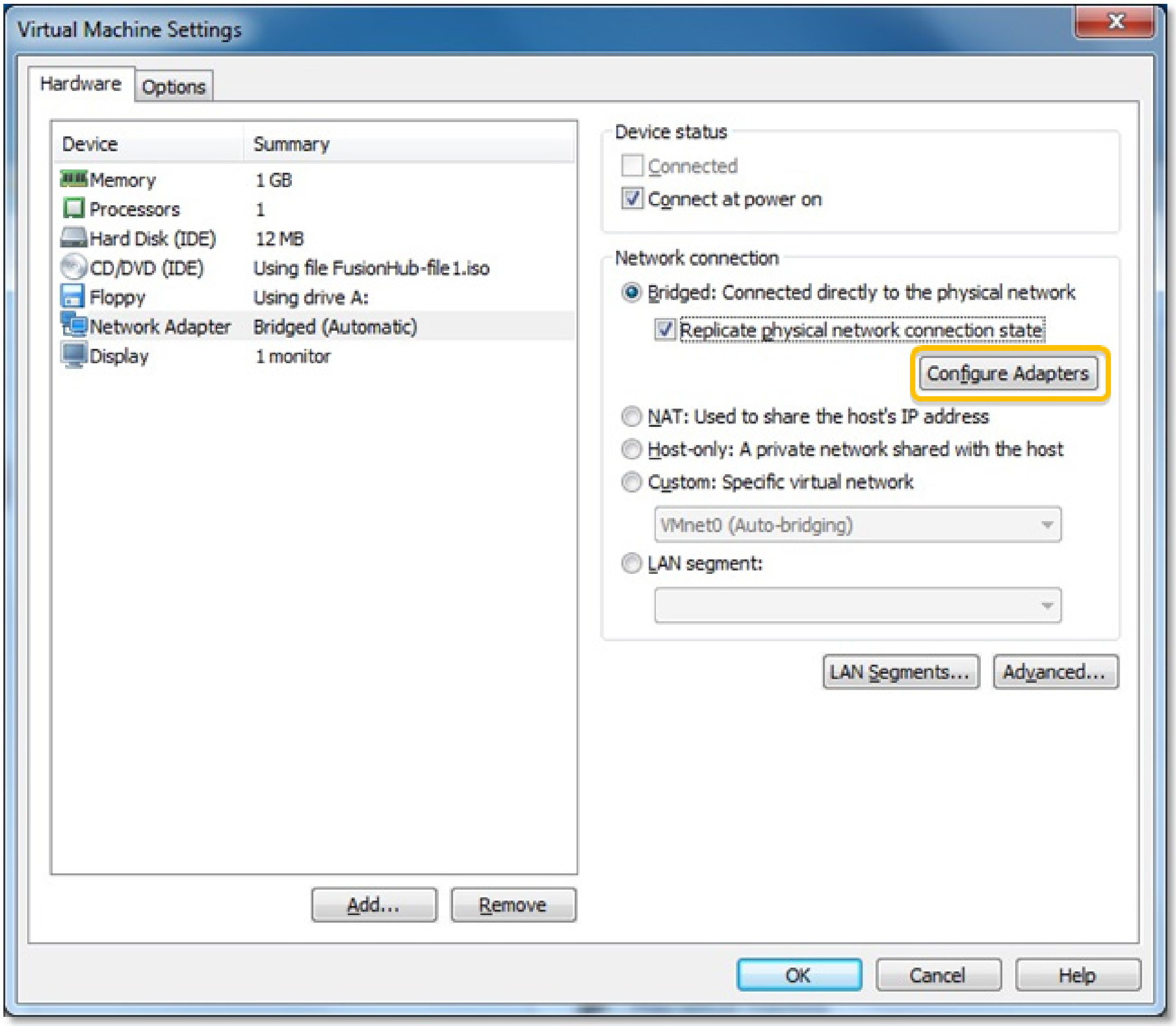
○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

Device status

☑ Connect at power on

10. Click **Configure Adapters** to select the host network adapter.



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	1 GB
Processors	1
Hard Disk (IDE)	12 MB
CD/DVD (IDE)	Using file FusionHub-file1.iso
Floppy	Using drive A:
Network Adapter	Bridged (Automatic)
Display	1 monitor

Device status

□ Connected

☑ Connect at power on

Network connection

● Bridged: Connected directly to the physical network

☑ Replicate physical network connection state

○ NAT: Used to share the host's IP address

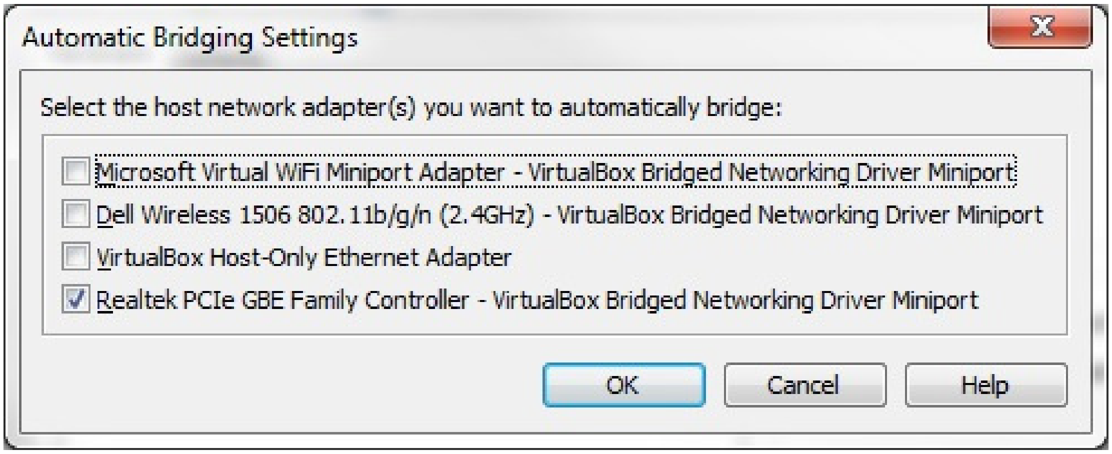
○ Host-only: A private network shared with the host

○ Custom: Specific virtual network

VMnet0 (Auto-bridging)

○ LAN segment:

11. On the **Automatic Bridging Settings** dialog, select the host network which you want to automatically bridge. Click **OK** to finish adding hardware.



Automatic Bridging Settings

Select the host network adapter(s) you want to automatically bridge:

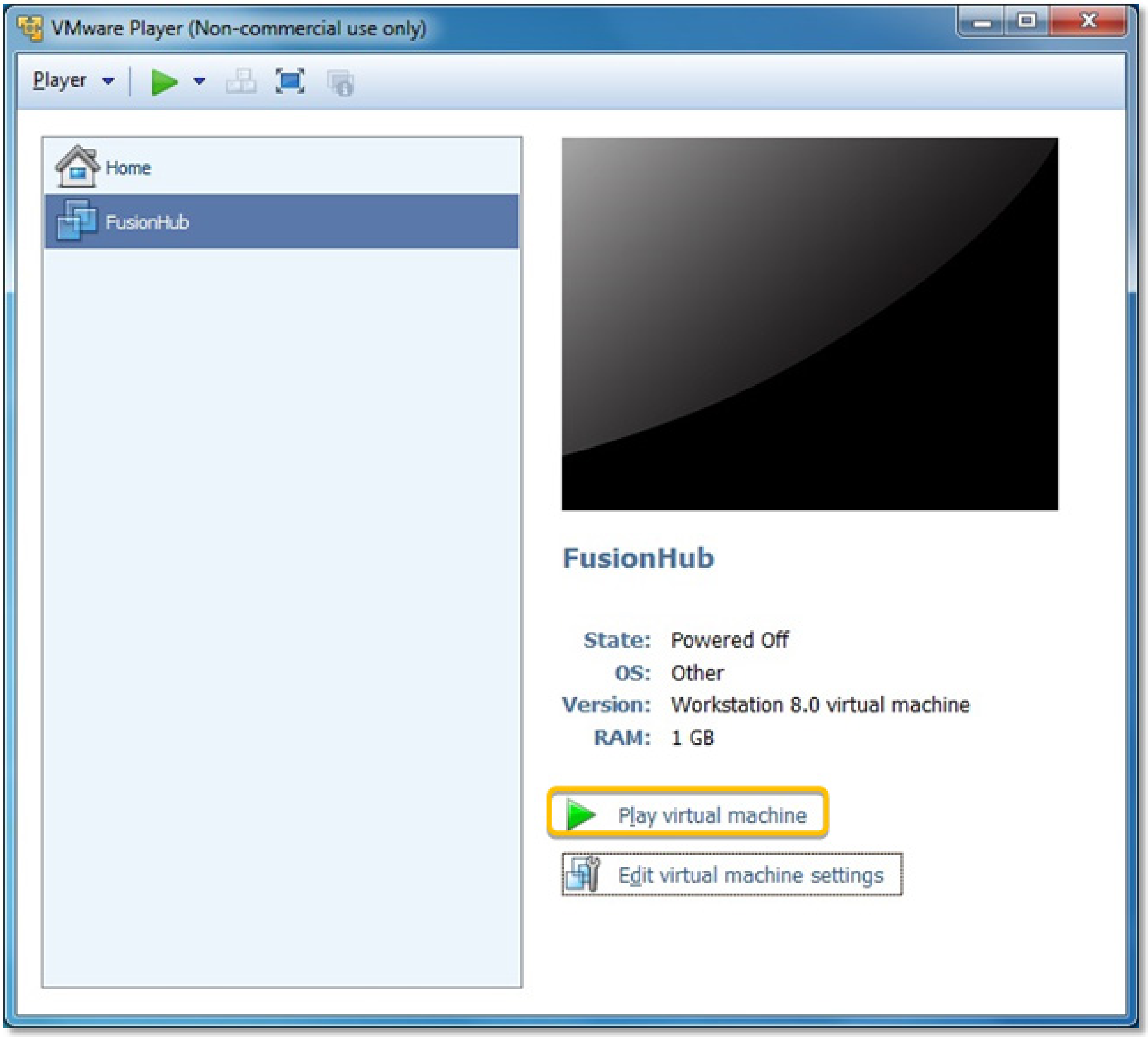
□ Microsoft Virtual WiFi Miniport Adapter - VirtualBox Bridged Networking Driver Miniport

□ Dell Wireless 1506 802.11b/g/n (2.4GHz) - VirtualBox Bridged Networking Driver Miniport

□ VirtualBox Host-Only Ethernet Adapter

☑ Realtek PCIe GBE Family Controller - VirtualBox Bridged Networking Driver Miniport

12. Click **Play virtual machine** to run FusionHub.

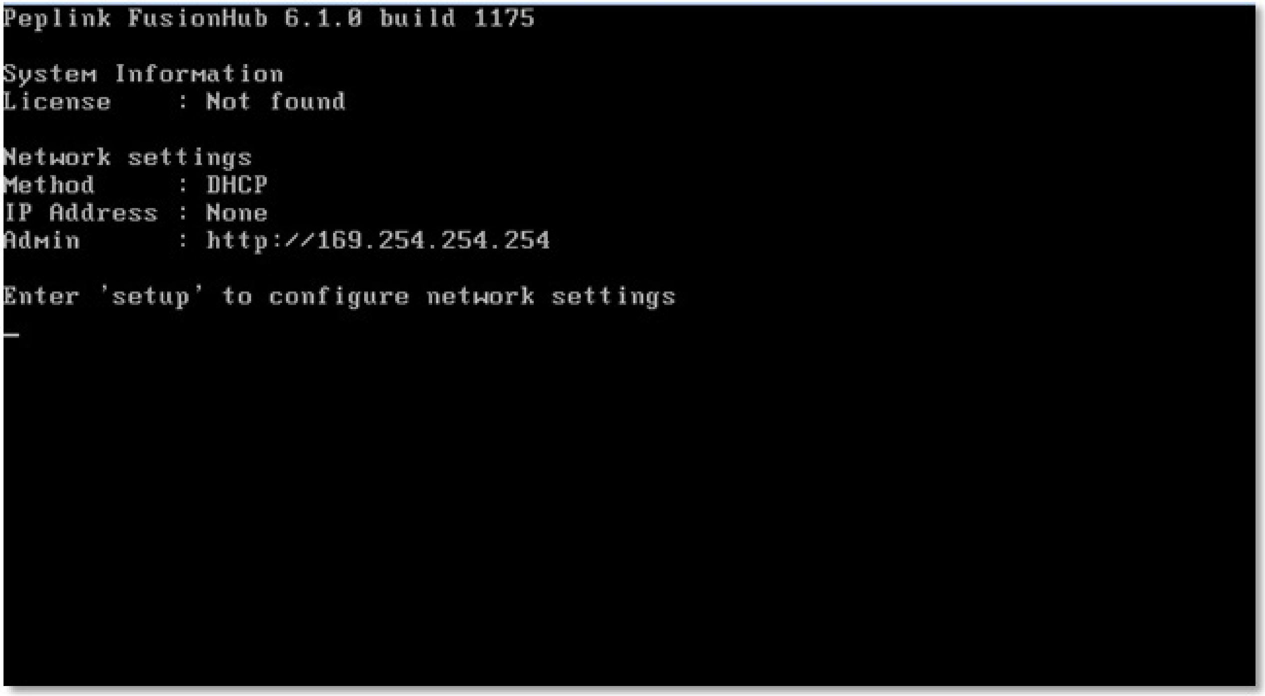

VMware Player (Non-commercial use only)
Player
Home
FusionHub
Play virtual machine
Edit virtual machine settings

FusionHub

State: Powered Off
OS: Other
Version: Workstation 8.0 virtual machine
RAM: 1 GB

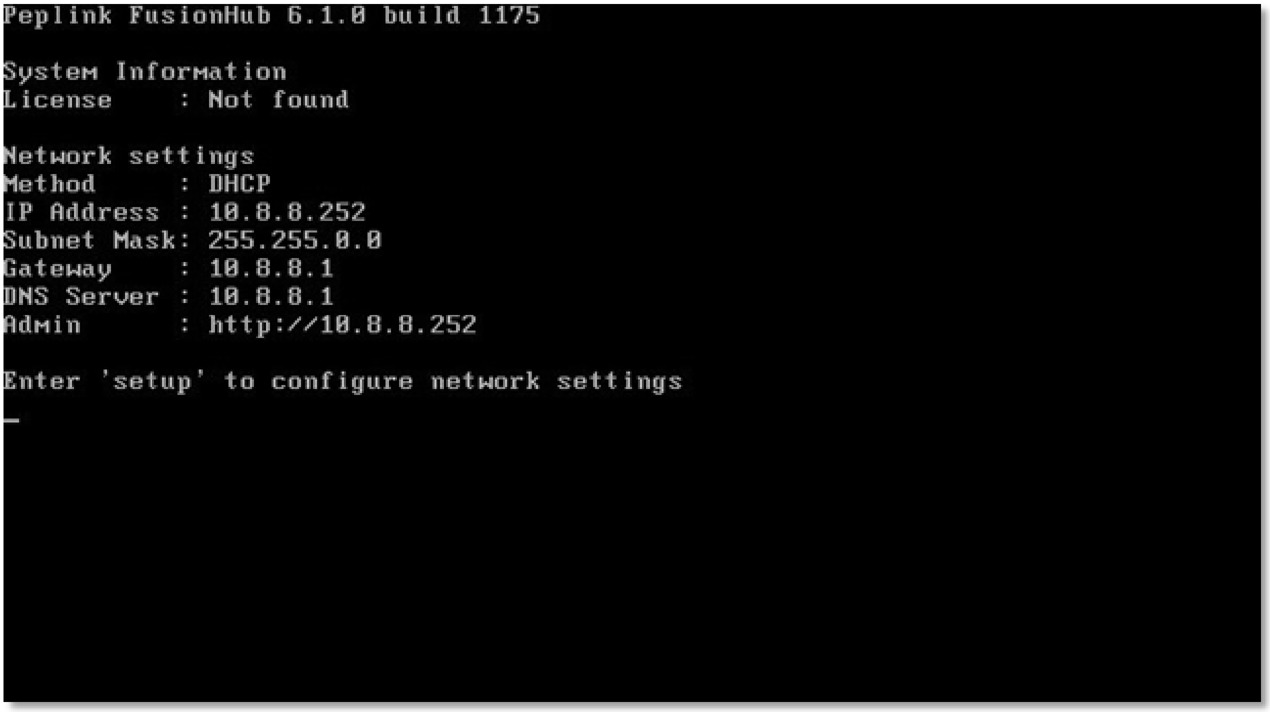
13. The FusionHub console opens automatically and displays the following general information about FusionHub:

   - FusionHub version
   - System information
   - Network settings:
     Method: DHCP
     IP Address: None
     Admin: http://169.254.254.254



```
Peplink FusionHub 6.1.0 build 1175

System Information
License     : Not found

Network settings
Method      : DHCP
IP Address  : None
Admin       : http://169.254.254.254

Enter 'setup' to configure network settings
_
```

14. The default WAN connection method is DHCP. If the DHCP server is available on your network, the FusionHub IP address will be automatically obtained by the DHCP server. In this case, the console looks similar to the following:



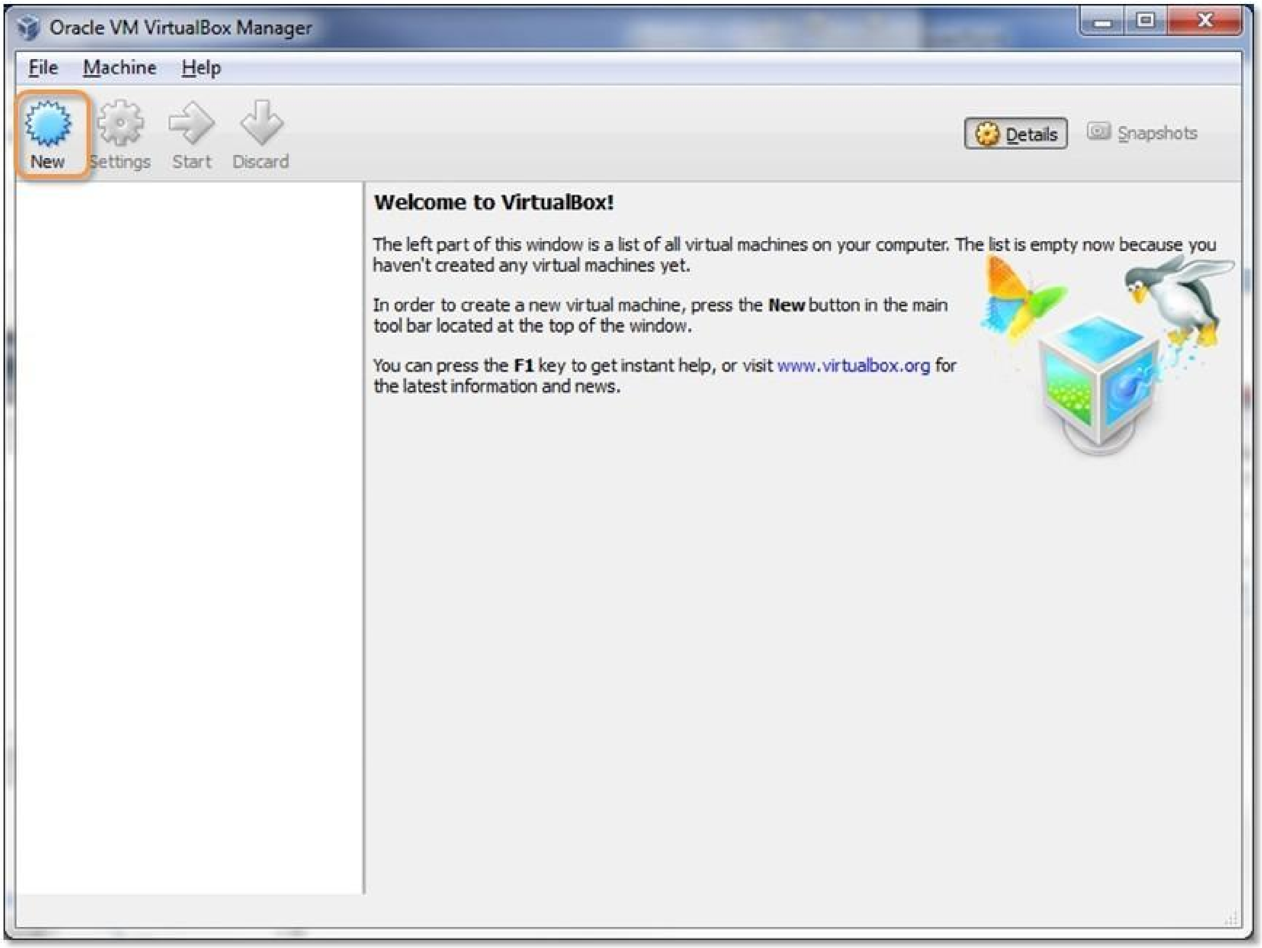
```
Peplink FusionHub 6.1.0 build 1175

System Information
License     : Not found

Network settings
Method      : DHCP
IP Address : 10.8.8.252
Subnet Mask: 255.255.0.0
Gateway     : 10.8.8.1
DNS Server : 10.8.8.1
Admin       : http://10.8.8.252

Enter 'setup' to configure network settings
_
```

Please navigate to **FusionHub Interface Configuration** to continue your installation.

4.4. Oracle VirtualBox

1. Download VirtualBox from the link and install it.
   https://www.virtualbox.org/wiki/Downloads

2. Open **VirtualBox**. Click **New** to create a virtual machine for FusionHub.



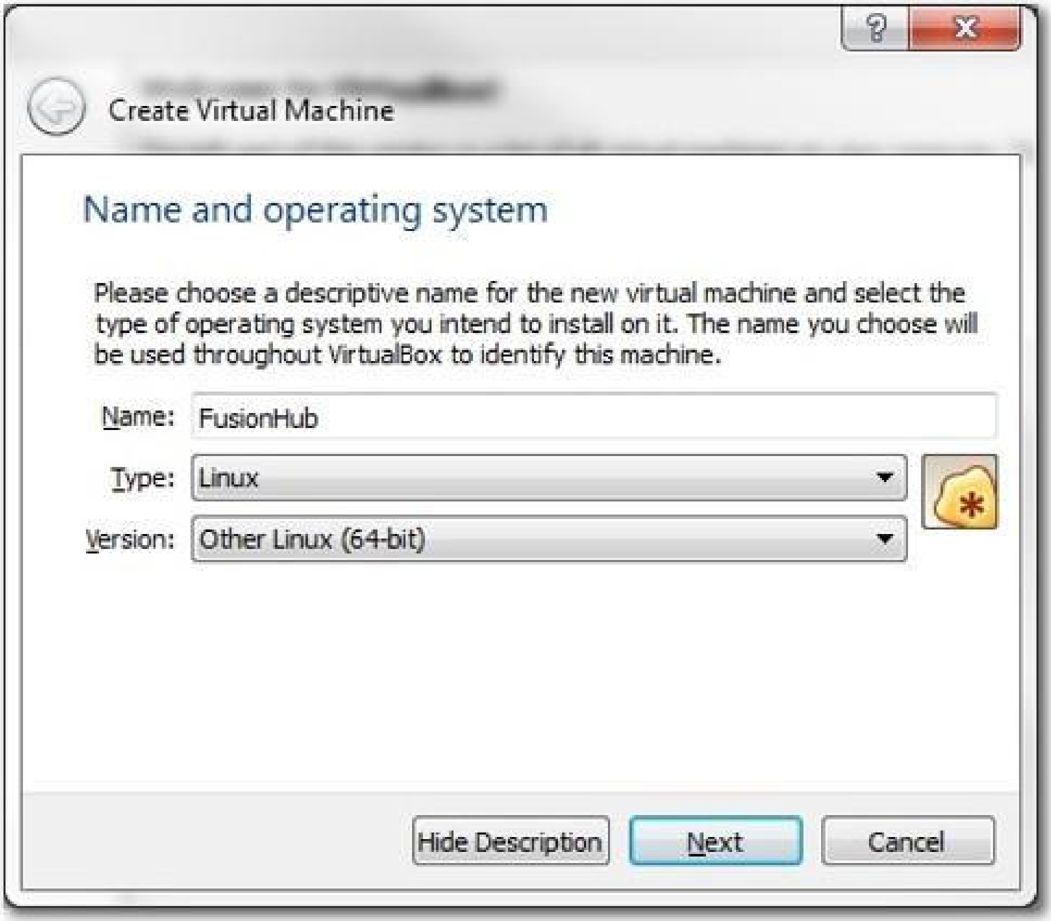
Welcome to VirtualBox!

The left part of this window is a list of all virtual machines on your computer. The list is empty now because you haven't created any virtual machines yet.

In order to create a new virtual machine, press the **New** button in the main tool bar located at the top of the window.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for the latest information and news.

3. On the **Create Virtual Machine** dialog, specify a **Name** for the virtual machine. Select **Linux** from the **Type** drop-down menu. Select **Other Linux (64-bit)** from the **Version** drop-down menu. Click **Next** to continue.



Create Virtual Machine

Name and operating system

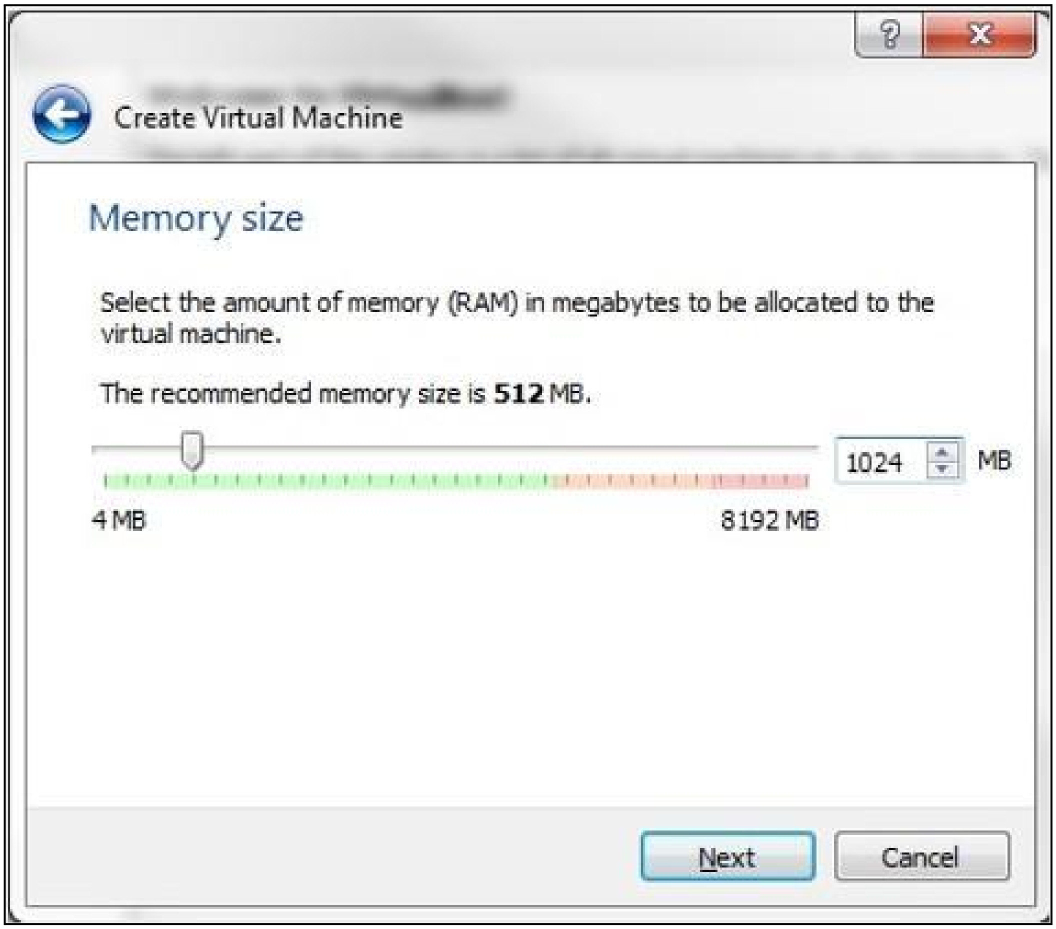
Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: FusionHub

Type: Linux

Version: Other Linux (64-bit)

4. Set the memory size to **1024MB**. Click **Next**.



Create Virtual Machine

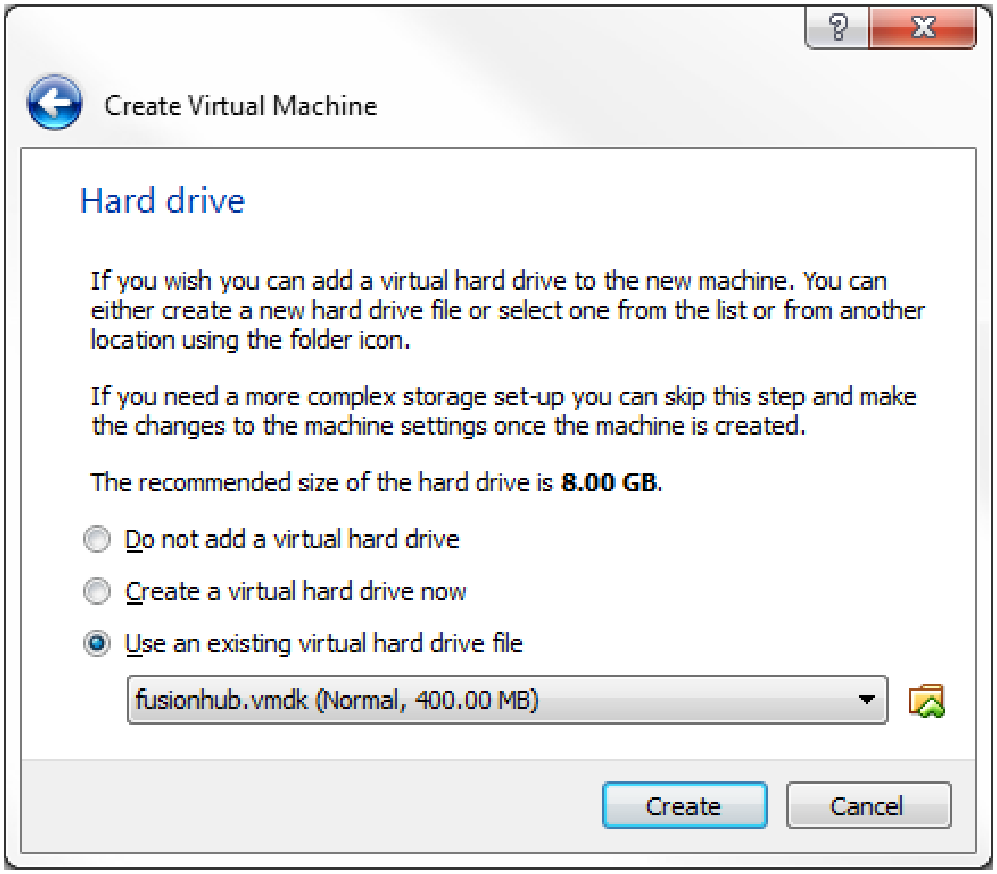
Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **512** MB.

1024 MB

5. Click **Use an existing virtual hard drive file**. Select the **fusionhub.vmdk** file downloaded from InControl 2. Click **Create** to create a virtual machine.



Hard drive

If you wish you can add a virtual hard drive to the new machine. You can either create a new hard drive file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard drive is **8.00 GB.**

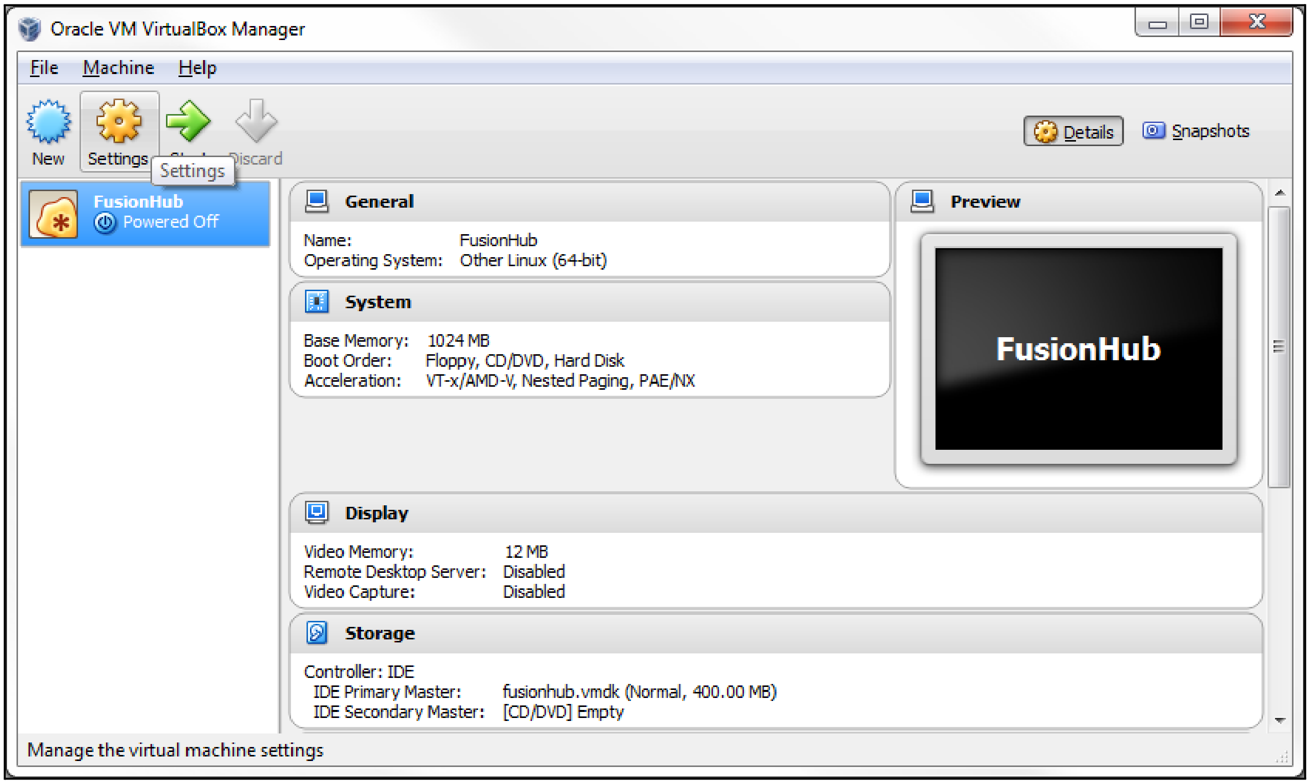
○ Do not add a virtual hard drive

○ Create a virtual hard drive now

● Use an existing virtual hard drive file

fusionhub.vmdk (Normal, 400.00 MB)

6. Select the newly created **FusionHub** VM and click **Settings**.



General

Name: FusionHub
Operating System: Other Linux (64-bit)

System

Base Memory: 1024 MB
Boot Order: Floppy, CD/DVD, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX

Display

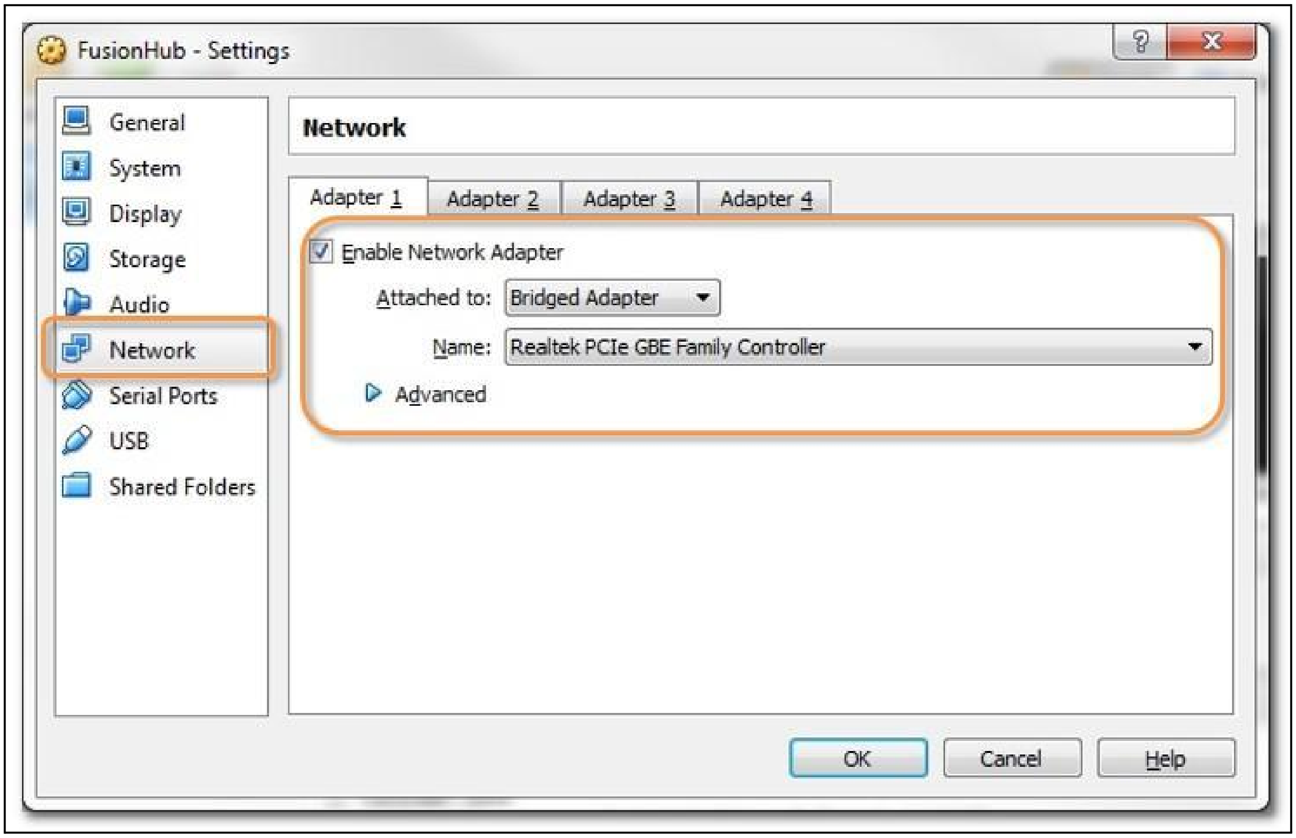
Video Memory: 12 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

Storage

Controller: IDE
IDE Primary Master: fusionhub.vmdk (Normal, 400.00 MB)
IDE Secondary Master: [CD/DVD] Empty

Manage the virtual machine settings

7. On the **FusionHub - Settings** dialog, click **Network**. Select the **Adapter 1** tab. Click **Enable Network Adapter** and select **Bridged Adapter** from the **Attached to:** drop-down menu. Select a proper adapter from the **Name** drop-down menu. Click **OK** to continue.

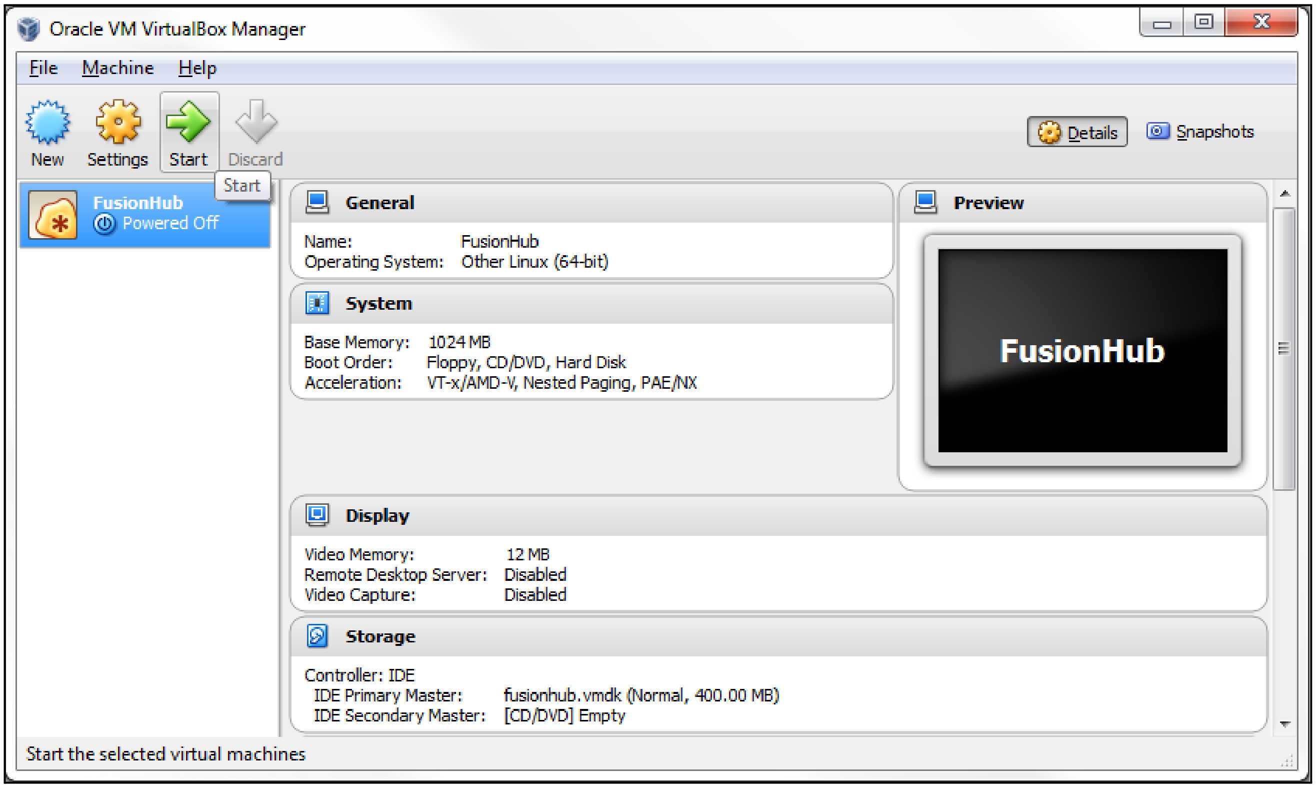


☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: Realtek PCIe GBE Family Controller

8. Select the **FusionHub** VM. Click **Start** to run FusionHub.



Oracle VM VirtualBox Manager

Name: FusionHub
Operating System: Other Linux (64-bit)

Base Memory: 1024 MB
Boot Order: Floppy, CD/DVD, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX

Video Memory: 12 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

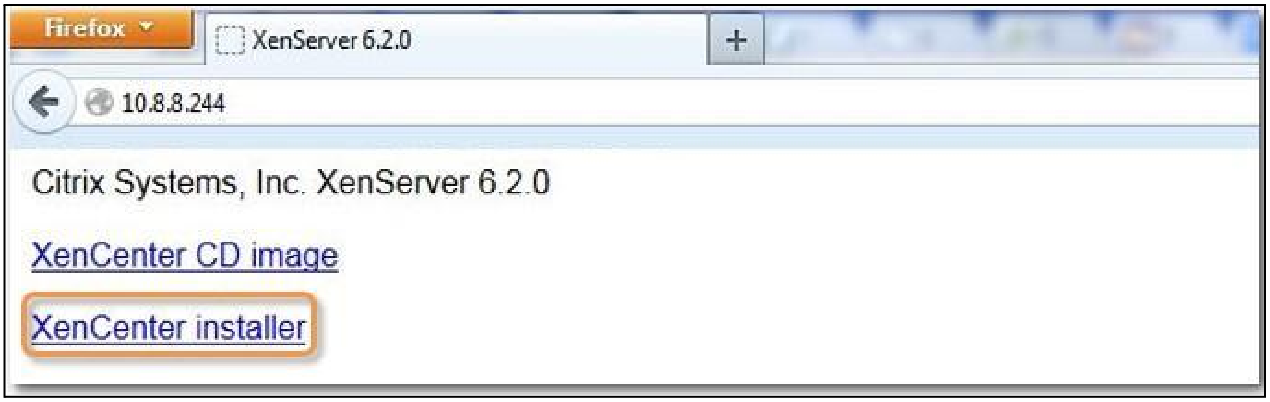
Controller: IDE
IDE Primary Master: fusionhub.vmdk (Normal, 400.00 MB)
IDE Secondary Master: [CD/DVD] Empty

Start the selected virtual machines

Please navigate to **FusionHub Interface Configuration** to continue your installation.

4.5. Citrix XenServer

1. Download and install the **XenCenter installer** from your XenCenter server.

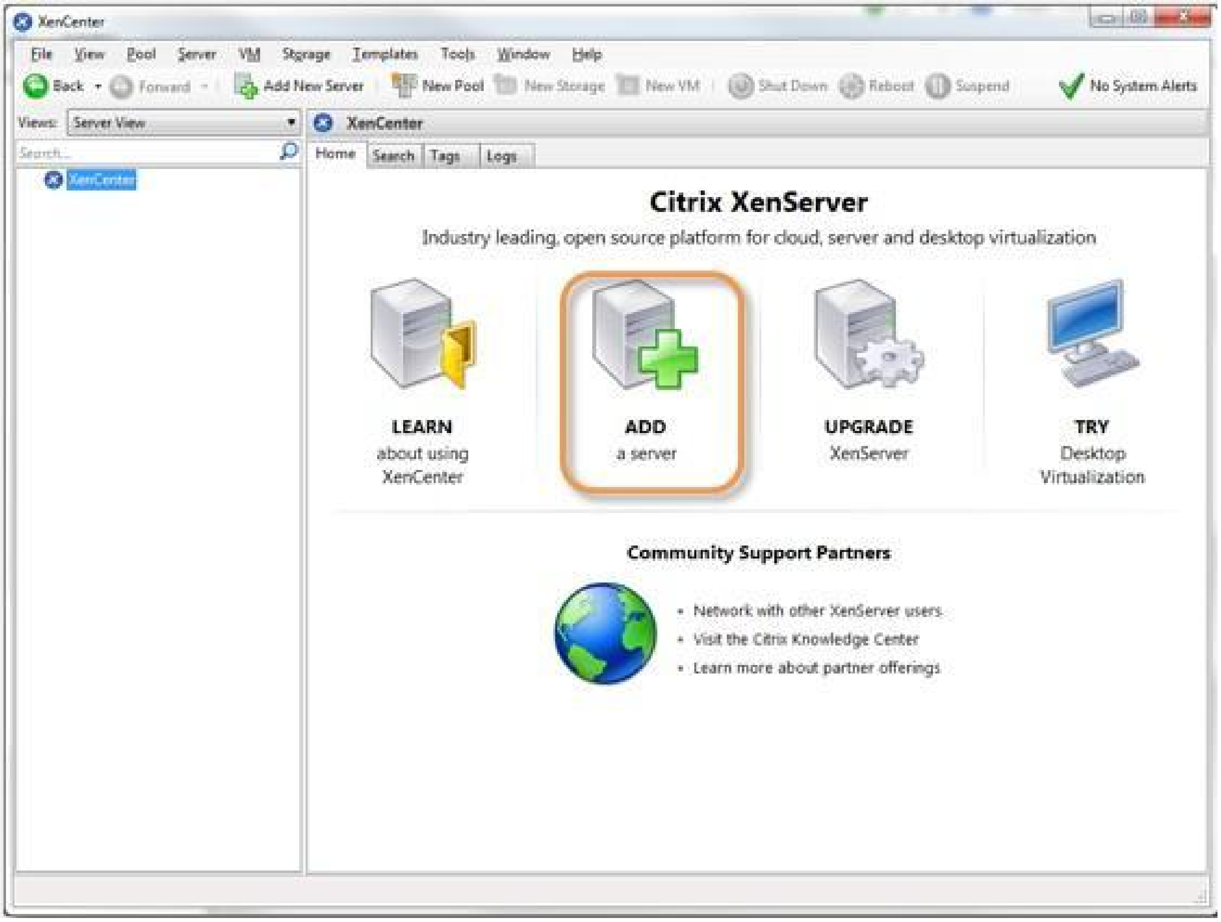


Citrix Systems, Inc. XenServer 6.2.0

XenCenter CD image

XenCenter installer

2. Open XenCenter. Click ADD a server.



XenCenter
File View Pool Server VM Storage Templates Tools Window Help
Back Forward Add New Server New Pool New Storage New VM Shut Down Reboot Suspend No System Alerts
Views: Server View
Search...
XenCenter
XenCenter
Home Search Tags Logs
LEARN
about using
XenCenter
ADD
a server
UPGRADE
XenServer
TRY
Desktop
Virtualization

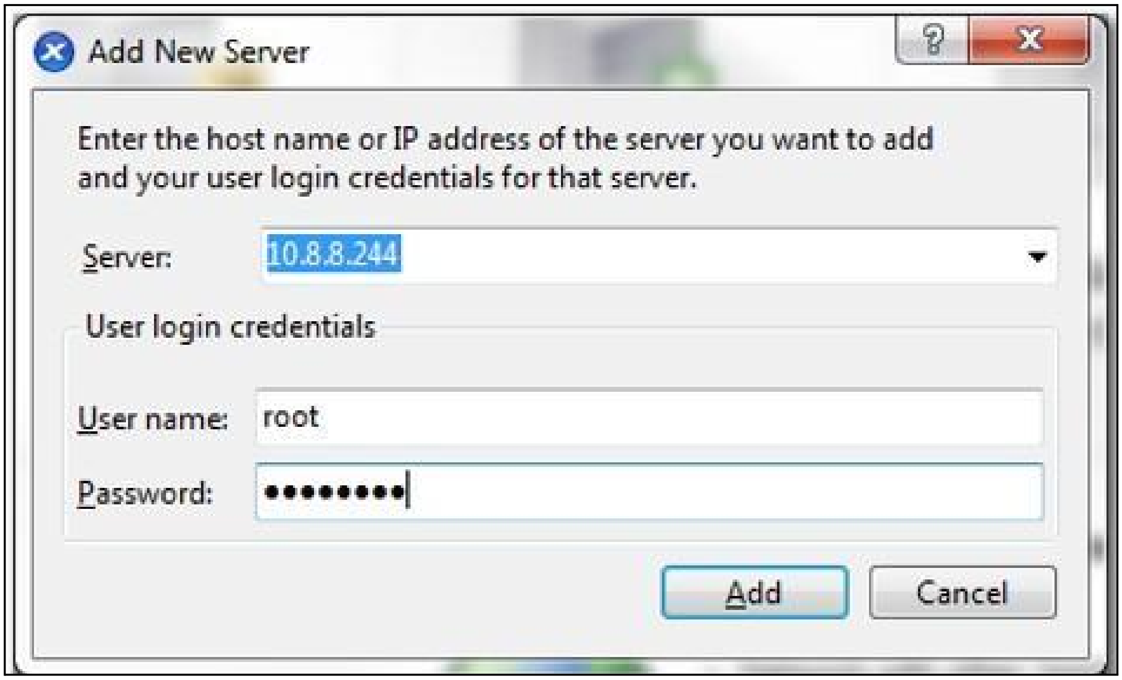
Citrix XenServer

Industry leading, open source platform for cloud, server and desktop virtualization

Community Support Partners

- Network with other XenServer users
- Visit the Citrix Knowledge Center
- Learn more about partner offerings

3. On the **Add New Server** dialog, enter the appropriate **Server** IP address/name, **User name**, and **Password**. Click **Add** to add the XenServer.



Enter the host name or IP address of the server you want to add and your user login credentials for that server.

Server: 10.8.8.244

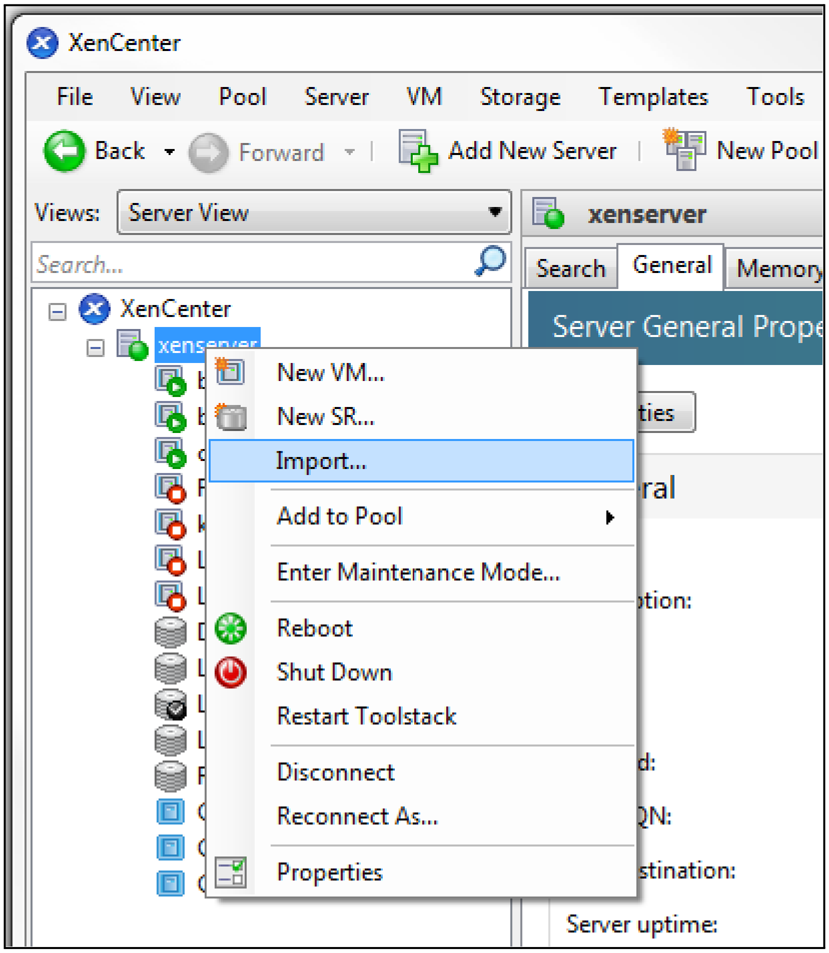
User login credentials

User name: root

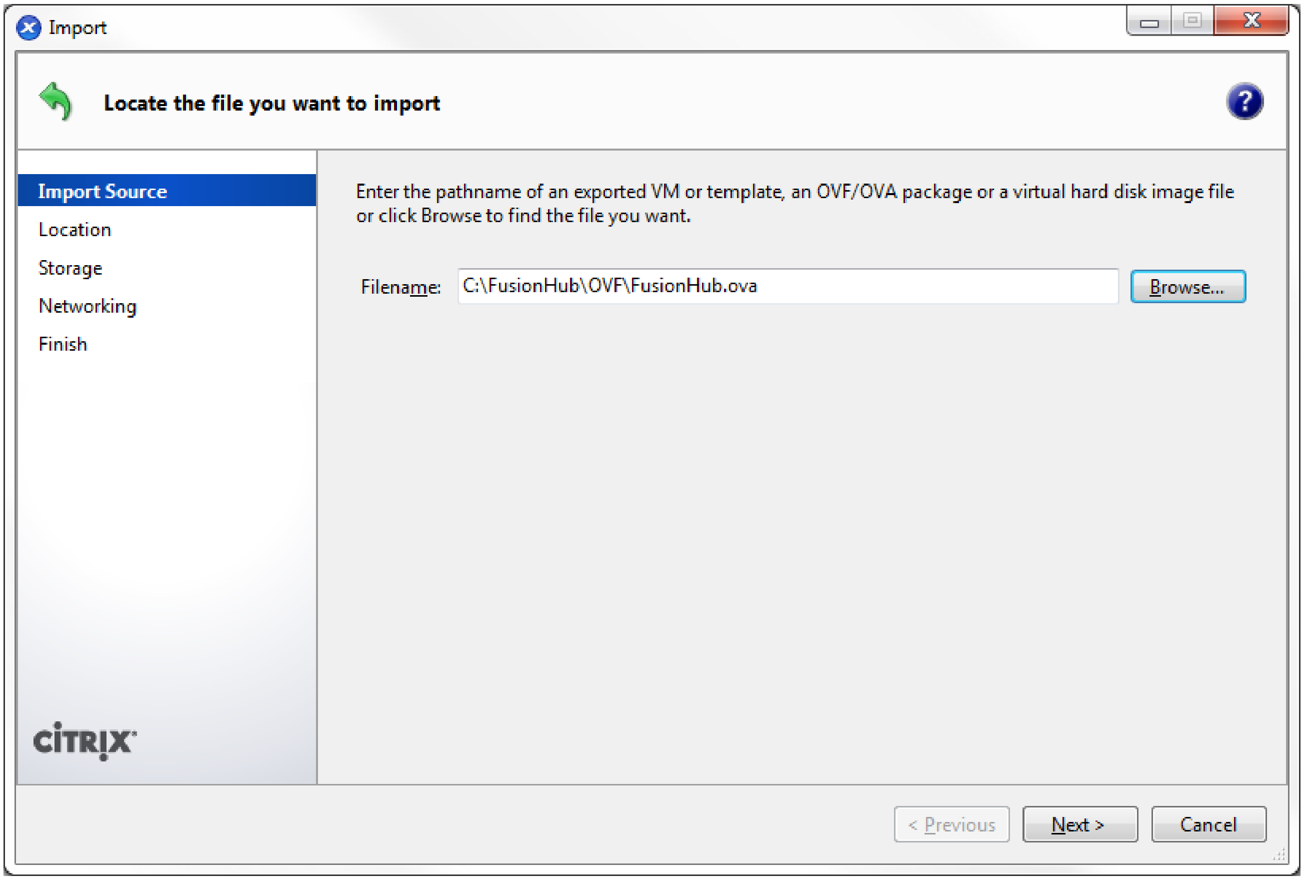
Password: ●●●●●●●●●

4. Enable E1000 gigabit device emulation in Citrix XenServer to take advantage of FusionHub's support for E1000 gigabit devices. For details, please refer to: http://www.netservers.co.uk/articles/open-source-howtos/citrix_e1000_gigabit

5. Right-click the XenServer and select **Import** to begin importing the OVA file to this XenServer.



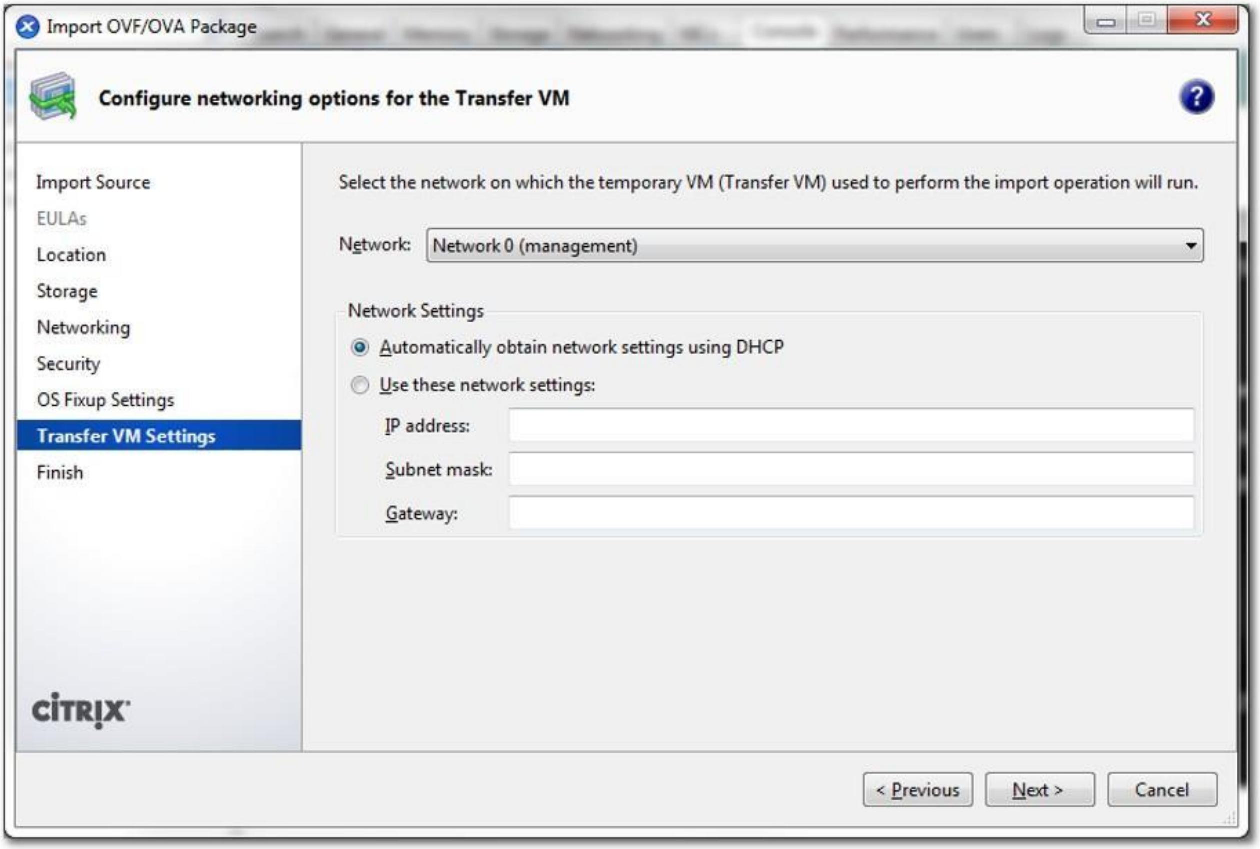
6. On the **Import** dialog, select the **FusionHub.ova** file downloaded from InControl 2.



Enter the pathname of an exported VM or template, an OVF/OVA package or a virtual hard disk image file or click Browse to find the file you want.

Filename: C:\FusionHub\OVF\FusionHub.ova

7. Click **Next** to keep the default settings and display the **Configure networking options for the Transfer VM** dialog. Select an appropriate network on which the temporary VM used to perform the import operation will run. Click **Next**. Click **Finish** to import the OVF file.



Import OVF/OVA Package

Configure networking options for the Transfer VM

Select the network on which the temporary VM (Transfer VM) used to perform the import operation will run.

Network: Network 0 (management)

Network Settings

● Automatically obtain network settings using DHCP

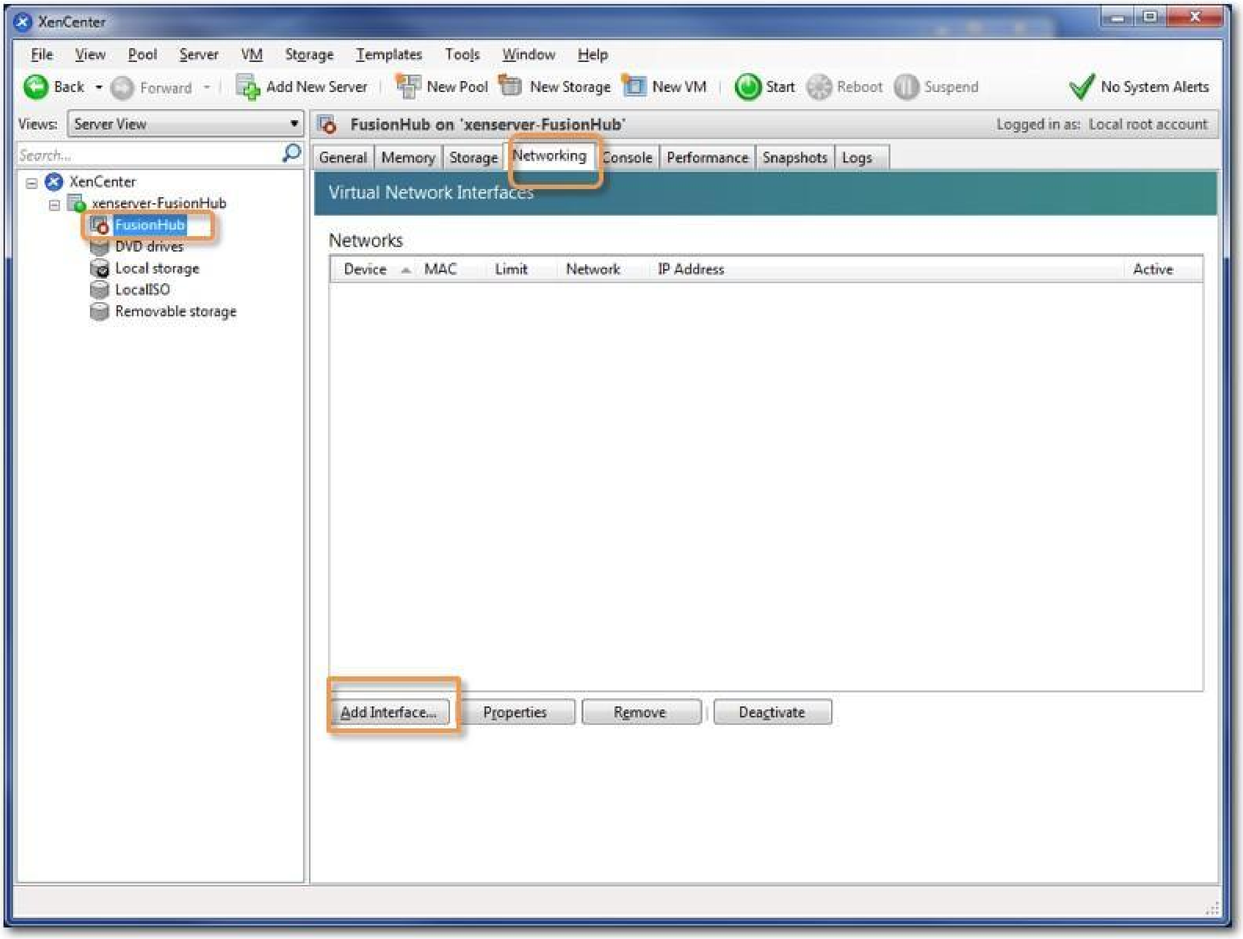
○ Use these network settings:

IP address:

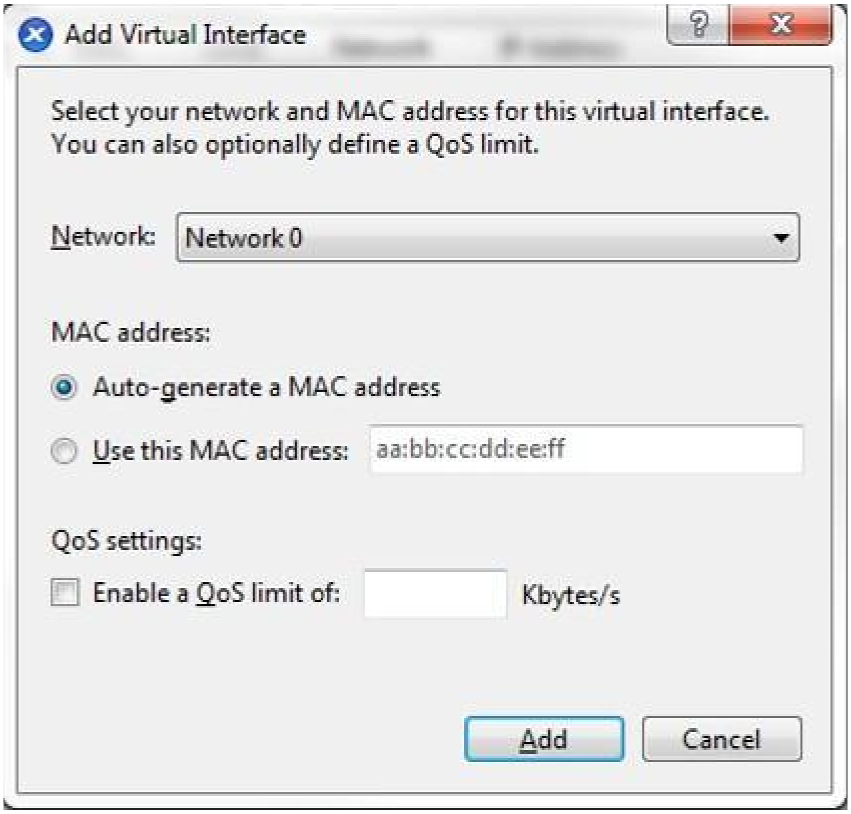
Subnet mask:

Gateway:

8. Click **FusionHub** > **Networking** > **Add Interface** to add a network interface.


XenCenter
File View Pool Server VM Storage Templates Tools Window Help
Back Forward Add New Server New Pool New Storage New VM Start Reboot Suspend No System Alerts
Views: Server View
FusionHub on 'xenserver-FusionHub'
Logged in as: Local root account
Search...
General Memory Storage Networking Console Performance Snapshots Logs
XenCenter
xenserver-FusionHub
FusionHub
DVD drives
Local storage
LocalISO
Removable storage
Virtual Network Interfaces
Networks
Device MAC Limit Network IP Address Active
Add Interface... Properties Remove Deactivate

9. On the **Add Virtual Interface** dialog, select the network and click **Add**.



Add Virtual Interface

Select your network and MAC address for this virtual interface. You can also optionally define a QoS limit.

Network: Network 0

MAC address:

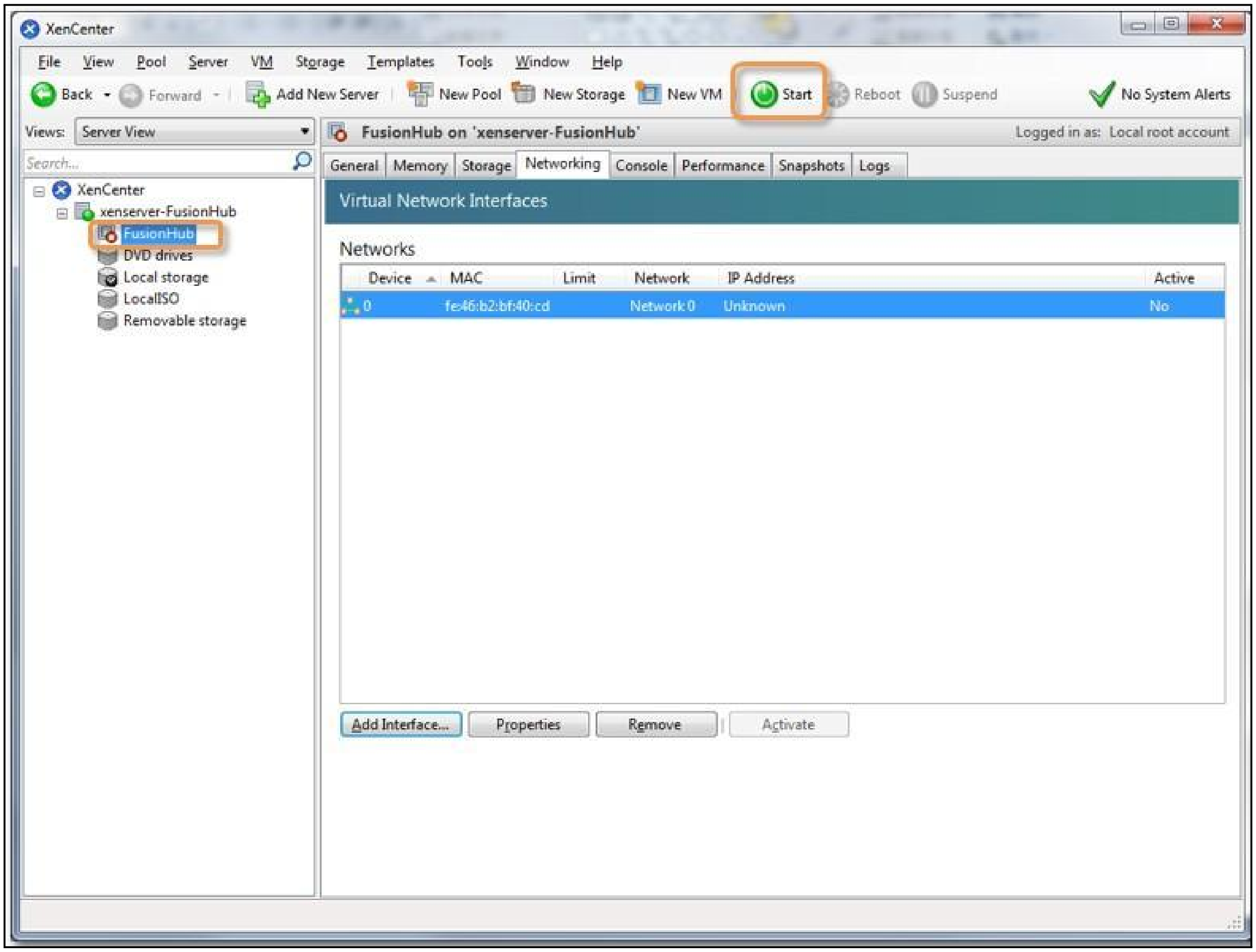
● Auto-generate a MAC address

○ Use this MAC address: aa:bb:cc:dd:ee:ff

QoS settings:

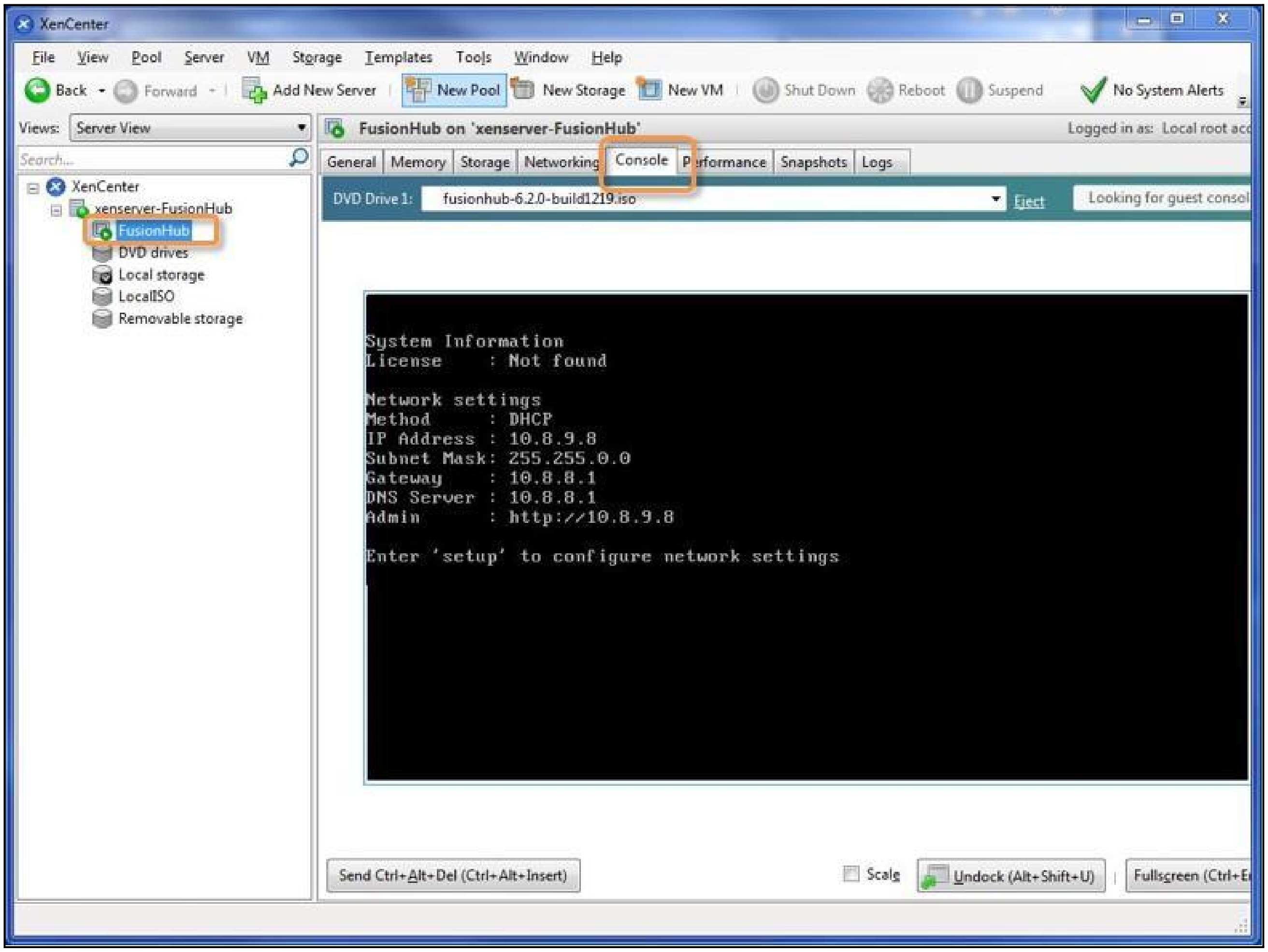
□ Enable a QoS limit of: Kbytes/s

10. Click **FusionHub** > **Start** to run this FusionHub virtual machine.


XenCenter
File View Pool Server VM Storage Templates Tools Window Help
Back Forward Add New Server New Pool New Storage New VM Start Reboot Suspend No System Alerts
Views: Server View
Search...
XenCenter
xenserver-FusionHub
FusionHub
DVD drives
Local storage
LocalISO
Removable storage
FusionHub on 'xenserver-FusionHub'
Logged in as: Local root account
General Memory Storage Networking Console Performance Snapshots Logs
Virtual Network Interfaces
Networks
Add Interface... Properties Remove Activate

Device	MAC	Limit	Network	IP Address	Active
0	fe:46:b2:bf:40:cd		Network 0	Unknown	No

11. Click **FusionHub** > **Console** to open the console.

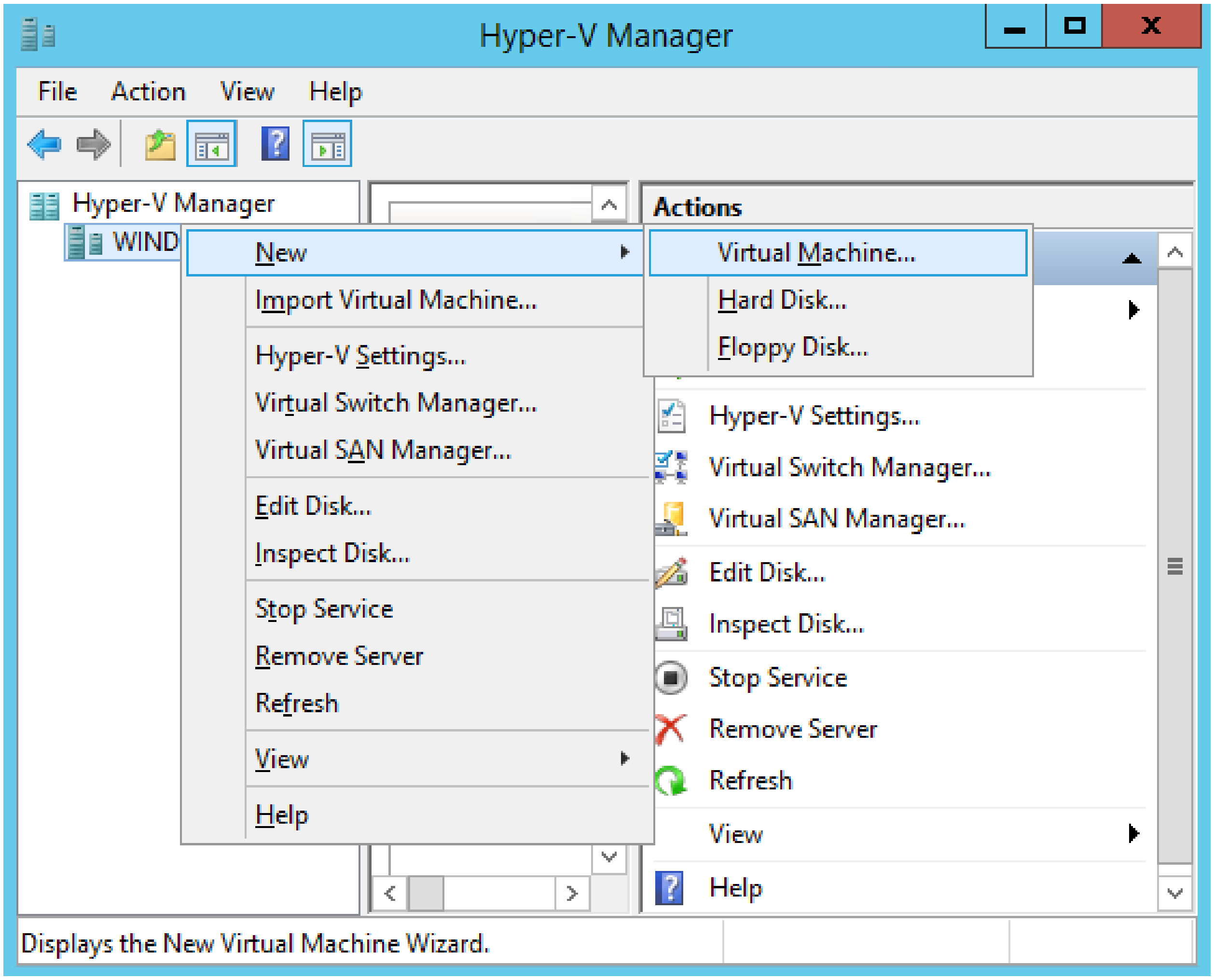

XenCenter
File View Pool Server VM Storage Templates Tools Window Help
Back Forward Add New Server New Pool New Storage New VM Shut Down Reboot Suspend No System Alerts
Views: Server View
FusionHub on 'xenserver-FusionHub'
Logged in as: Local root acc
Search...
General Memory Storage Networking Console Performance Snapshots Logs
XenCenter
xenserver-FusionHub
FusionHub
DVD drives
Local storage
LocalISO
Removable storage
DVD Drive 1: fusionhub-6.2.0-build1219.iso
Eject
Looking for guest consol
Send Ctrl+Alt+Del (Ctrl+Alt+Insert)
Scale
Undock (Alt+Shift+U)
Fullscreen (Ctrl+E

```
System Information
License     : Not found

Network settings
Method      : DHCP
IP Address : 10.8.9.8
Subnet Mask: 255.255.0.0
Gateway     : 10.8.8.1
DNS Server : 10.8.8.1
Admin       : http://10.8.9.8

Enter 'setup' to configure network settings
```

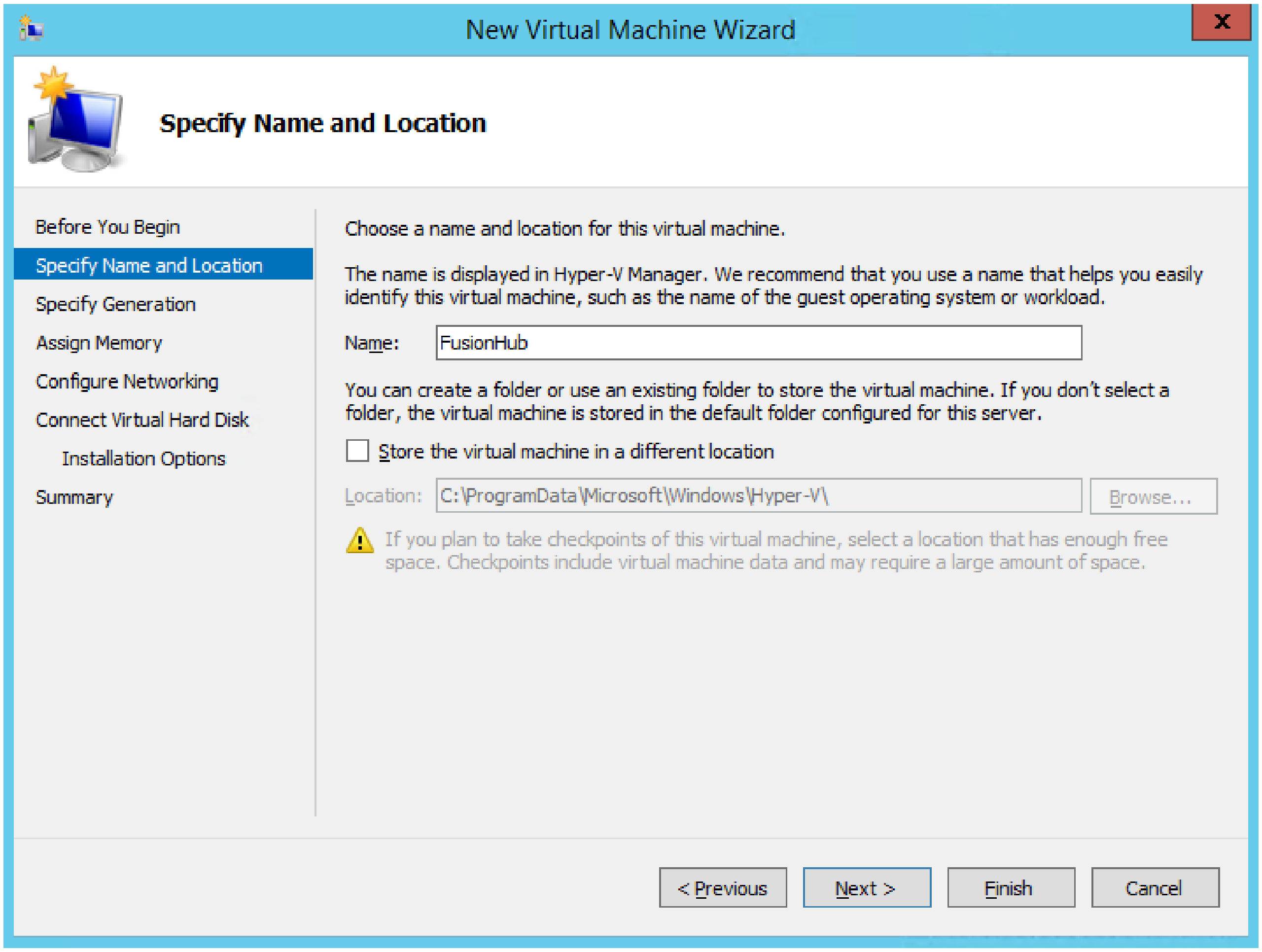
Please navigate to **FusionHub Interface Configuration** to continue your installation.

4.6. Microsoft Hyper-V

1. Open Hyper-V and install FusionHub, click **New** > **Virtual Machine** to create a virtual machine for FusionHub.



2. On the **Specify Name and Location** dialog, specify a name for the virtual machine. Click **Next**.



Specify Name and Location

Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: FusionHub

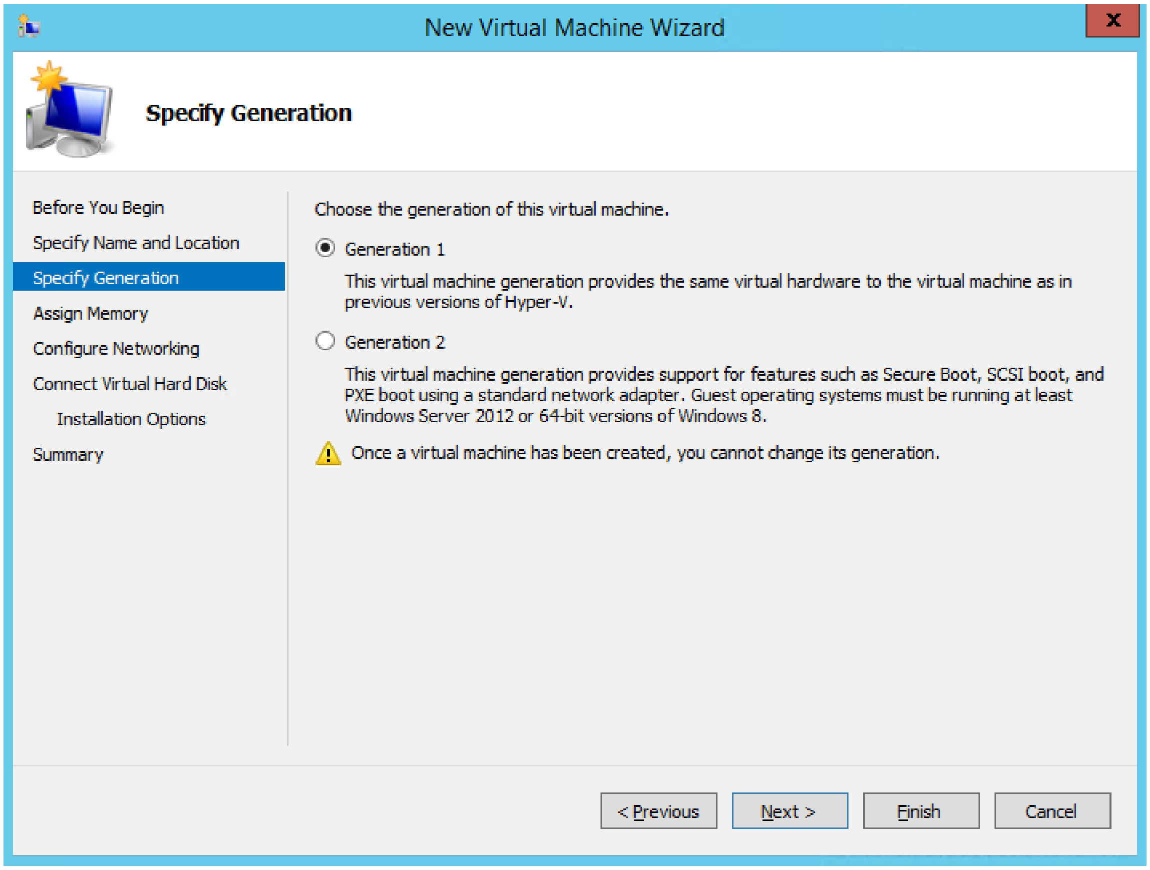
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☐ Store the virtual machine in a different location

Location: C:\ProgramData\Microsoft\Windows\Hyper-V\

If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

3. On the **Specify Generation** dialog, choose **Generation 1**. Click **Next**.



Specify Generation

Choose the generation of this virtual machine.

● Generation 1

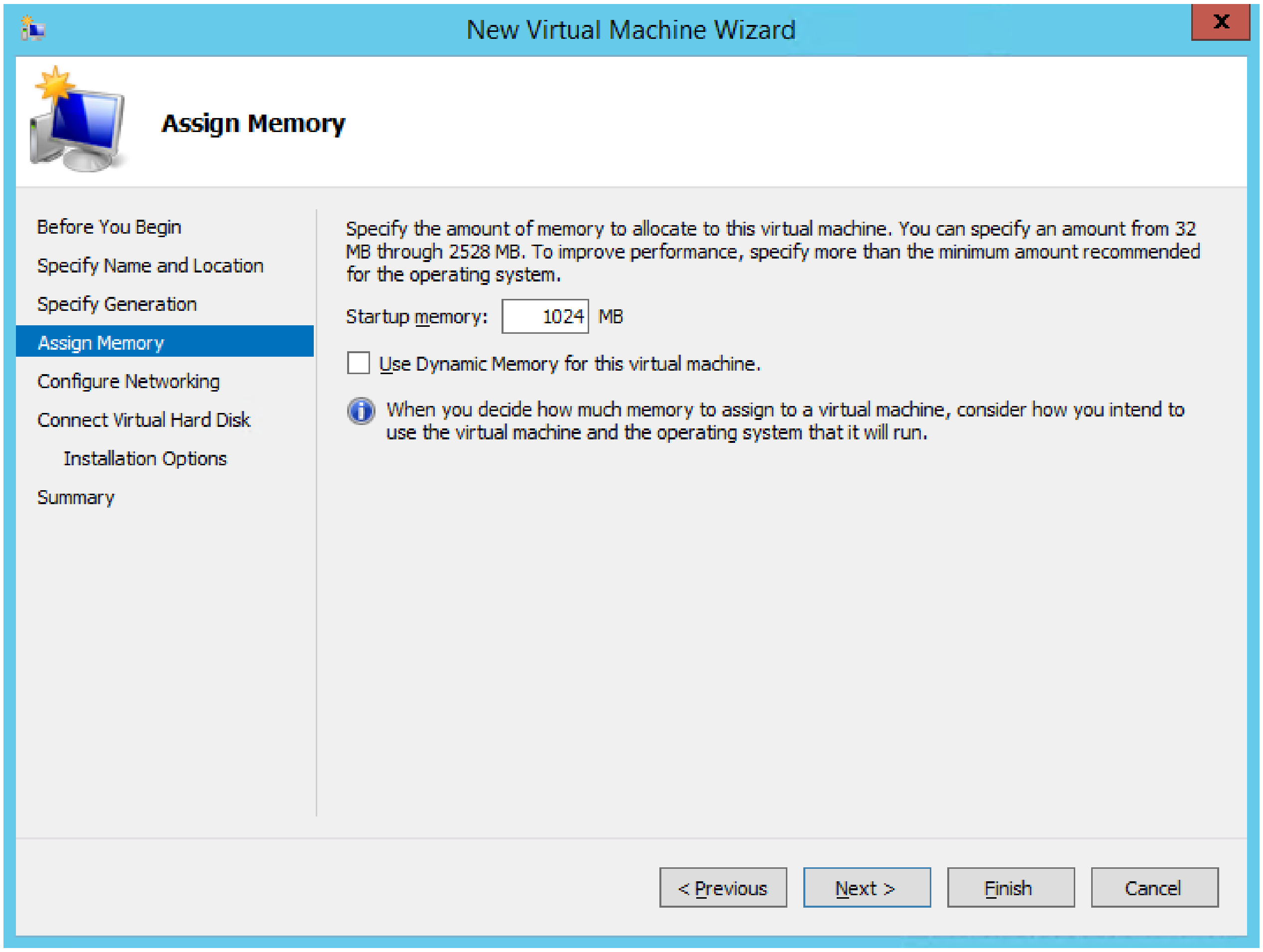
This virtual machine generation provides the same virtual hardware to the virtual machine as in previous versions of Hyper-V.

○ Generation 2

This virtual machine generation provides support for features such as Secure Boot, SCSI boot, and PXE boot using a standard network adapter. Guest operating systems must be running at least Windows Server 2012 or 64-bit versions of Windows 8.

⚠ Once a virtual machine has been created, you cannot change its generation.

4. On the **Assign Memory** dialog, set the memory size to **1024MB**. Click **Next.**



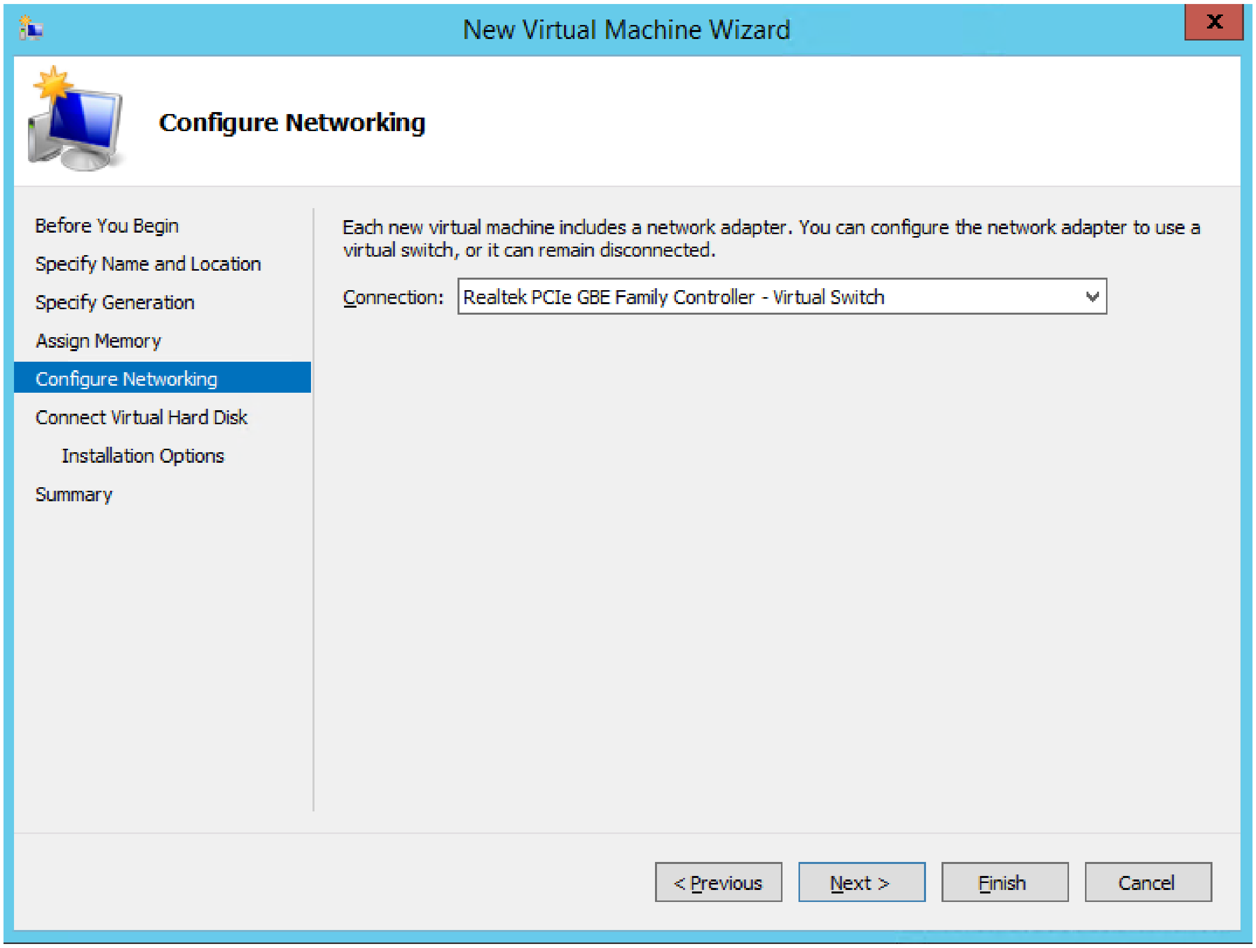
Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 2528 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: 1024 MB

□ Use Dynamic Memory for this virtual machine.

When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

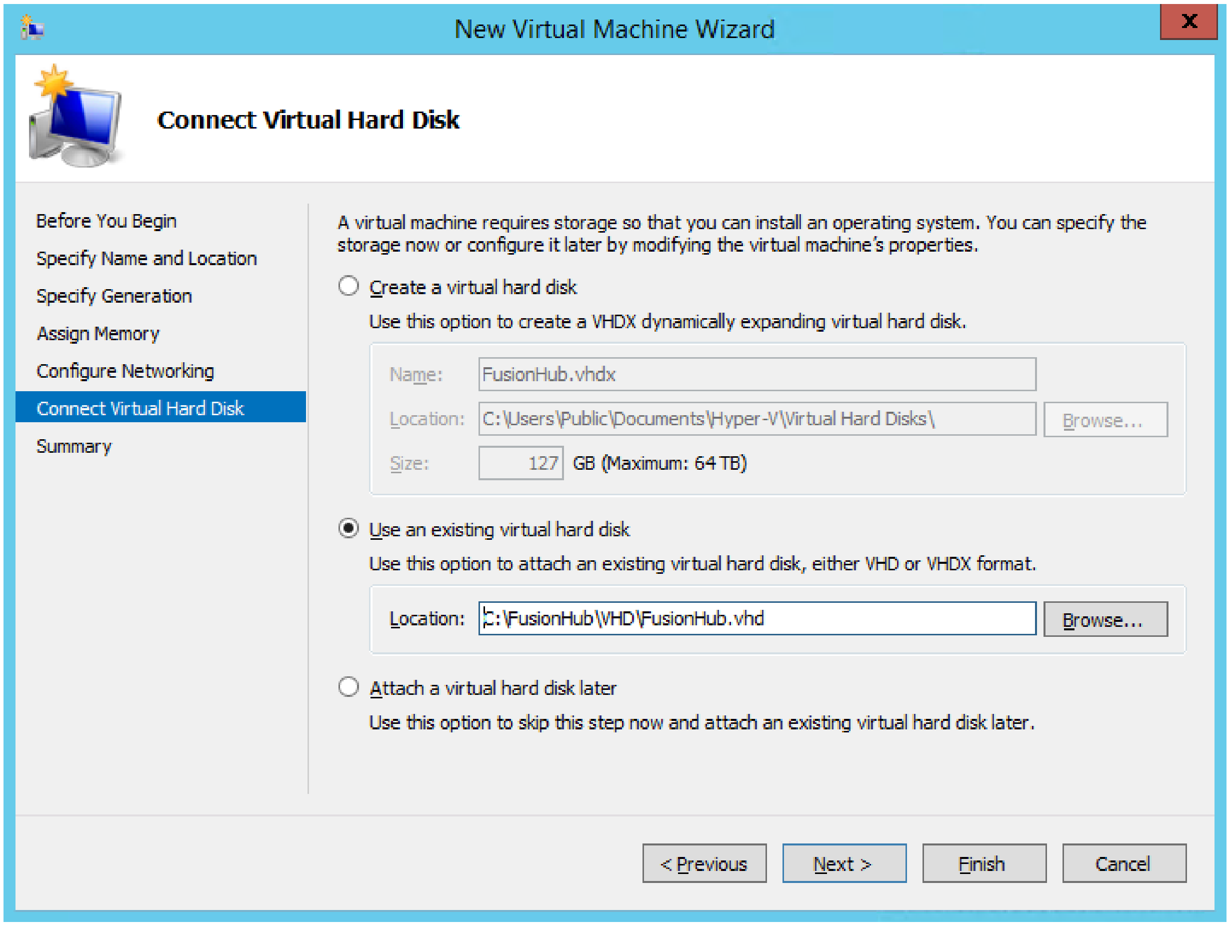
5. On the **Configure Networking** dialog, select a network adapter and click **Next**



Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: Realtek PCIe GBE Family Controller - Virtual Switch

6. On the **Connect Virtual Hard Disk** dialog, select “**Use an existing virtual hard disk**” and select FusionHub.vhd from the location you downloaded FusionHub. Click **Next**.



New Virtual Machine Wizard

Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

○ Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: FusionHub.vhdx

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ Browse...

Size: 127 GB (Maximum: 64 TB)

● Use an existing virtual hard disk

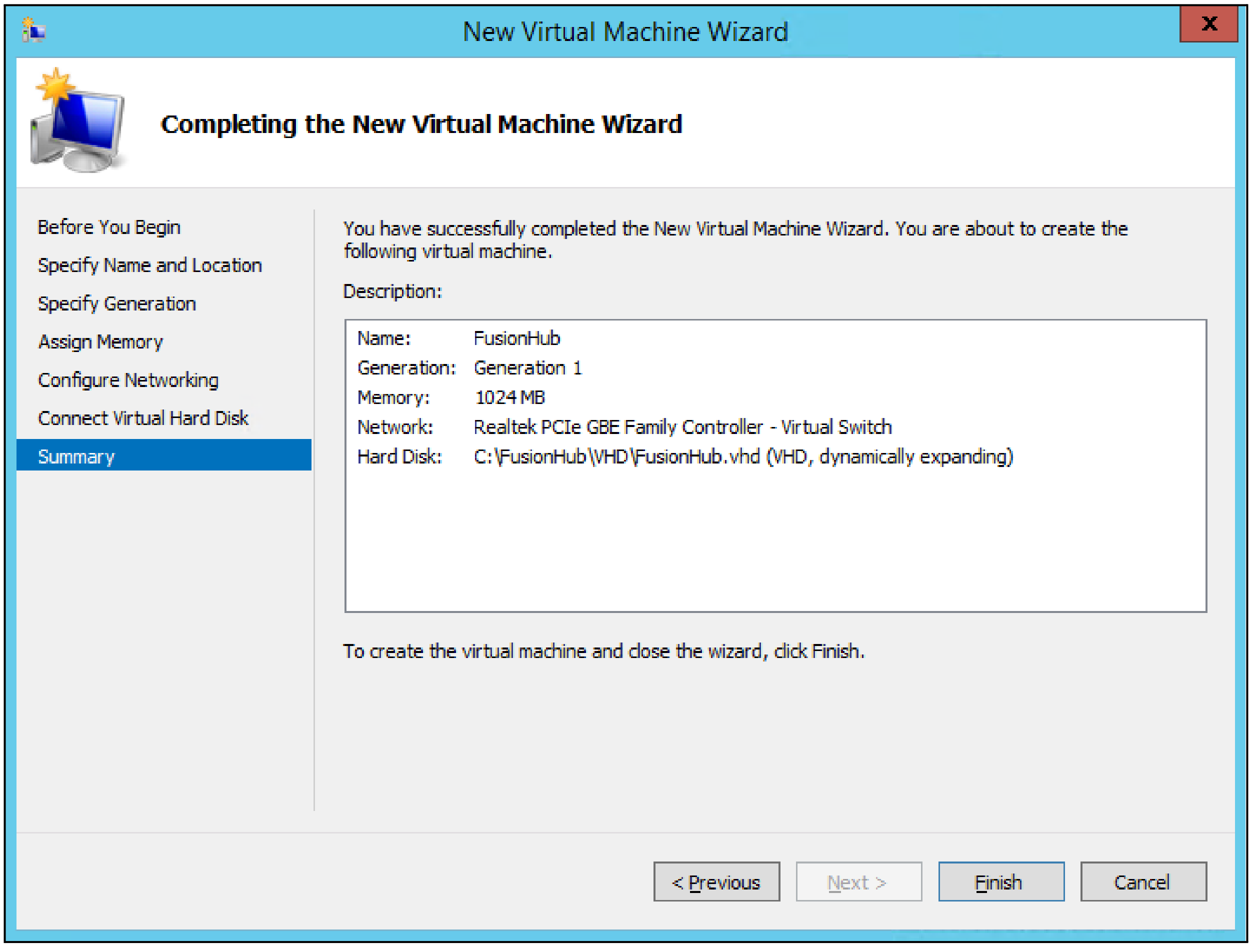
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location: C:\FusionHub\VHD\FusionHub.vhd Browse...

○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

7. Click **Finish** to complete virtual machine configuration.



New Virtual Machine Wizard

Completing the New Virtual Machine Wizard

Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Summary

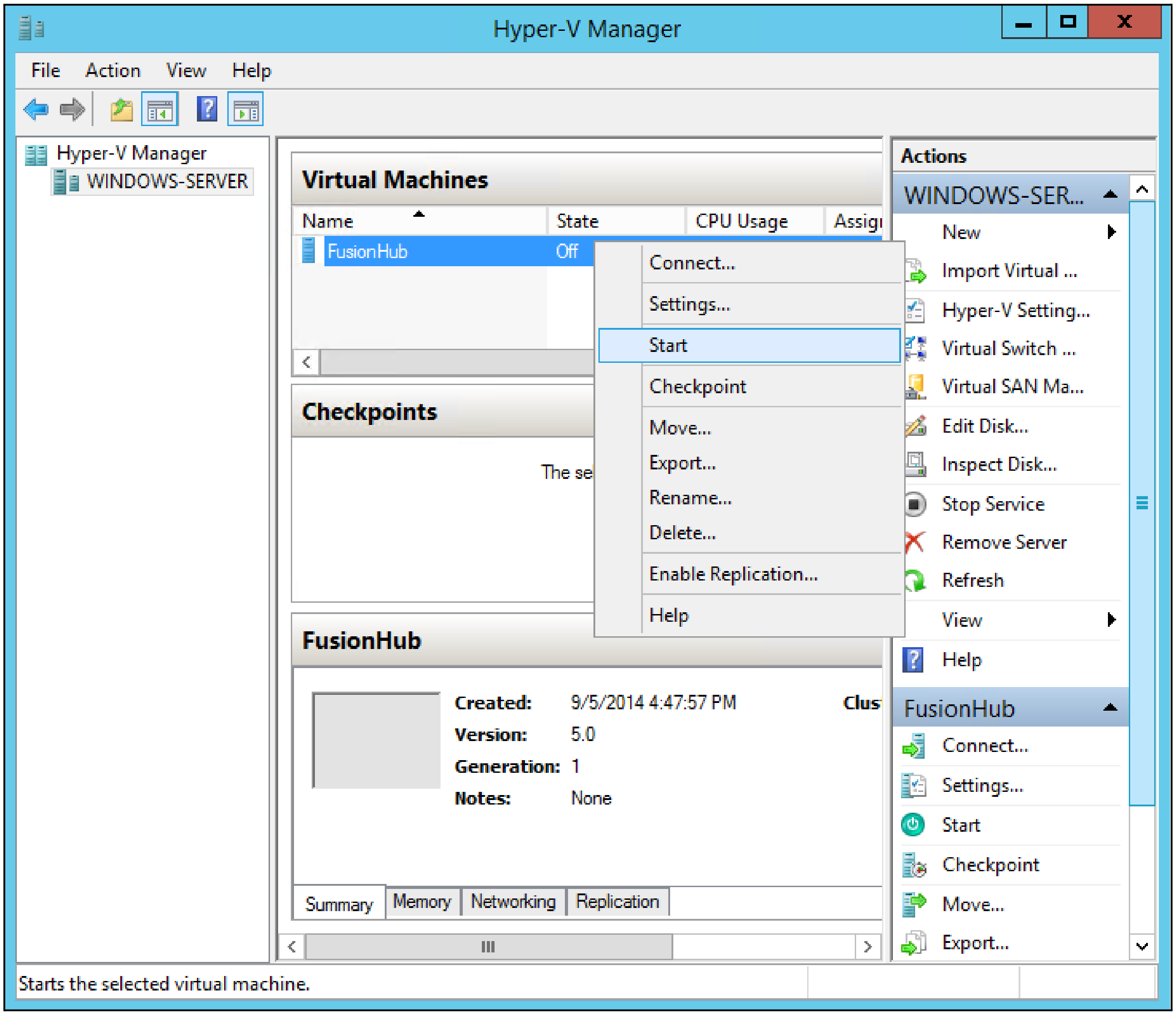
You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

Description:

Name: FusionHub
Generation: Generation 1
Memory: 1024 MB
Network: Realtek PCIe GBE Family Controller - Virtual Switch
Hard Disk: C:\FusionHub\VHD\FusionHub.vhd (VHD, dynamically expanding)

To create the virtual machine and close the wizard, click Finish.

8. Click **Start** to to run this FusionHub virtual machine.



Name	State
FusionHub	Off

Created: 9/5/2014 4:47:57 PM
Version: 5.0
Generation: 1
Notes: None

Starts the selected virtual machine.

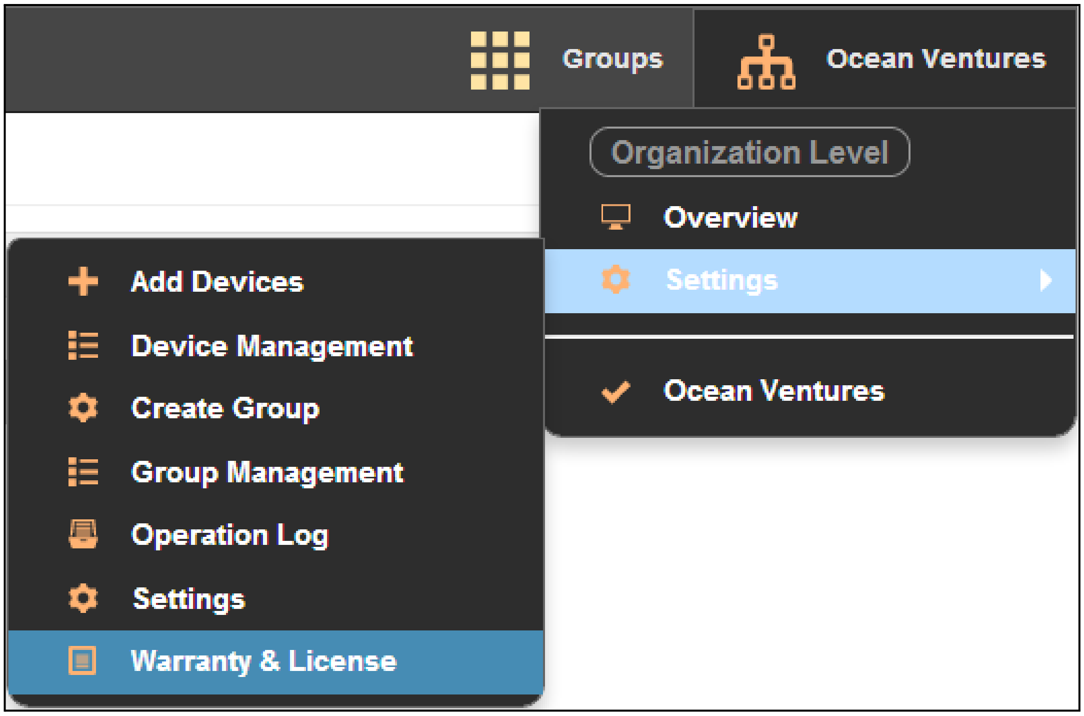
Please navigate to **FusionHub Interface Configuration** to continue your installation.

4.7. Amazon Web Services

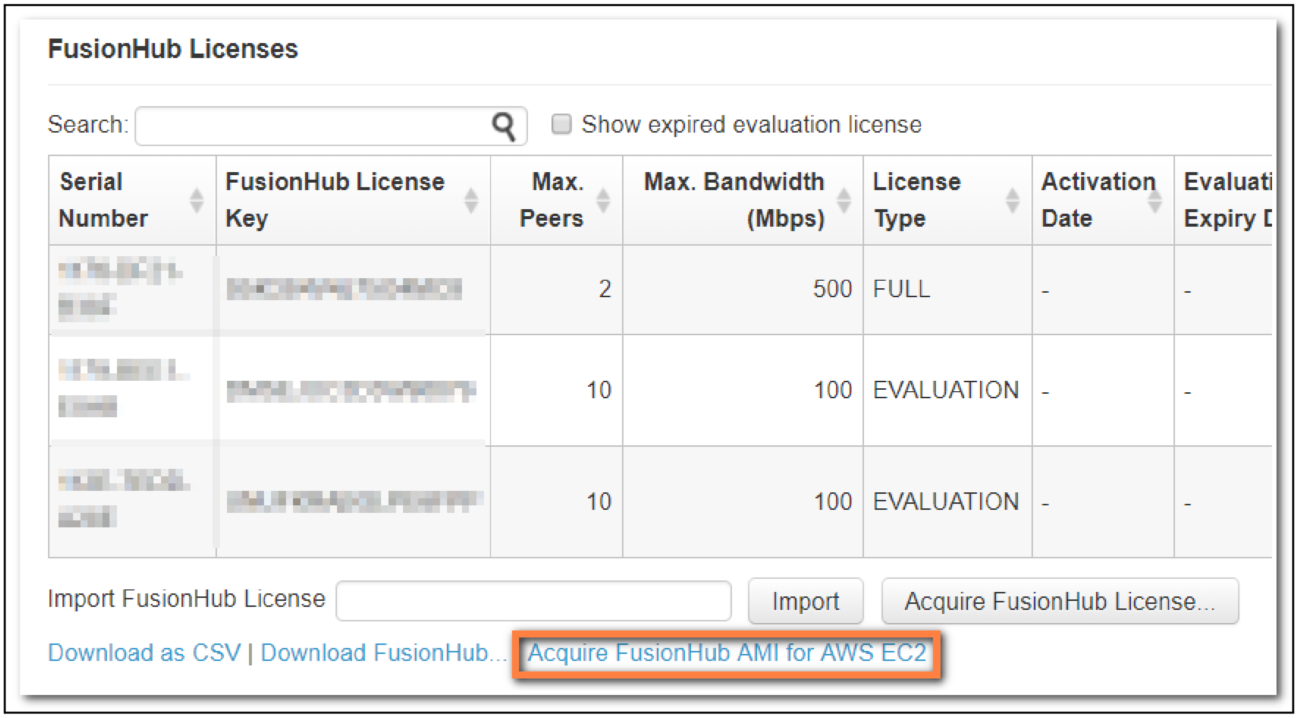
Acquiring FusionHub for AWS (Firmware 8.0.2 or below)

Note:
Starting from June 2020, you may obtain the FusionHub from AWS Marketplace. Do refer to this KB article for more information, https://community.peplink.com/forum/t/deploying-peplink-fusionhub-at-aws-marketplace

1. Get FusionHub AMI image
   - Login to InControl2 and navigate to Organization>Settings>Warranty & License



   - Click "Acquire FusionHub AMI for AWS EC2" and input your 12-digit Amazon ID.



FusionHub Licenses

Search: □ Show expired evaluation license

Serial Number	FusionHub License Key	Max. Peers	Max. Bandwidth (Mbps)	License Type	Activation Date	Evaluati Expiry D
[redacted]	[redacted]	2	500	FULL	-	-
[redacted]	[redacted]	10	100	EVALUATION	-	-
[redacted]	[redacted]	10	100	EVALUATION	-	-

Import FusionHub License

Import
Acquire FusionHub License...
Download as CSV | Download FusionHub...
Acquire FusionHub AMI for AWS EC2

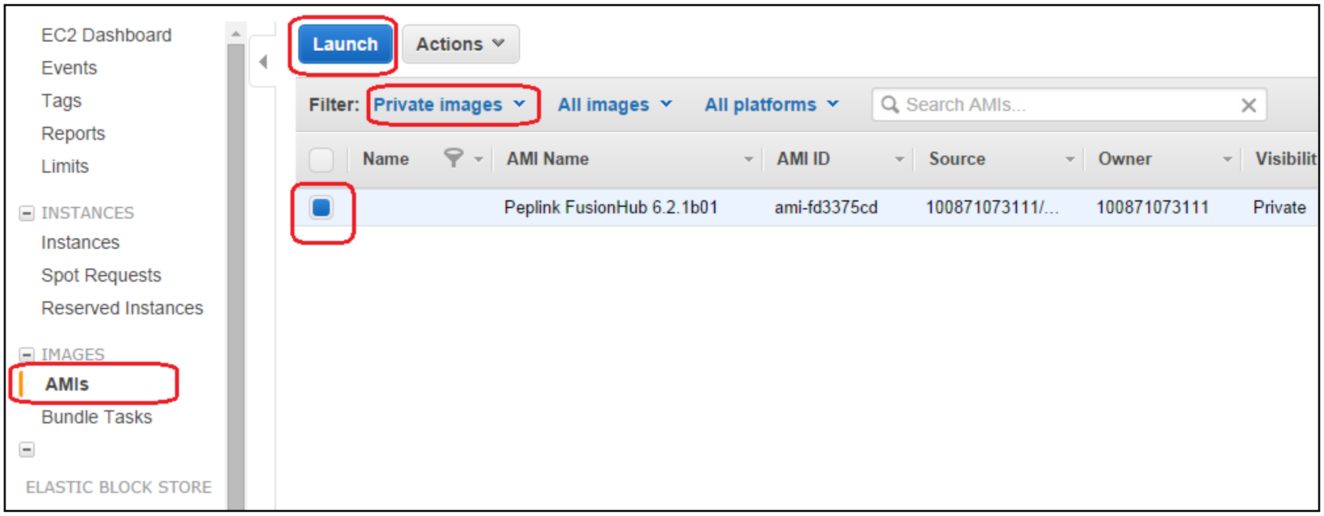
2. Login to your AWS Management Console after 10 minutes

3. In the left hand panel, expand “Images”, select “**AMIs**”.

4. At the top, locate “Filter:” and pick “**Private images**”.

5. Click on “**Peplink FusionHub**” to highlight it. A blue dot will appear to show that it is currently highlighted.

6. Click on the “**Launch**” button at the top.

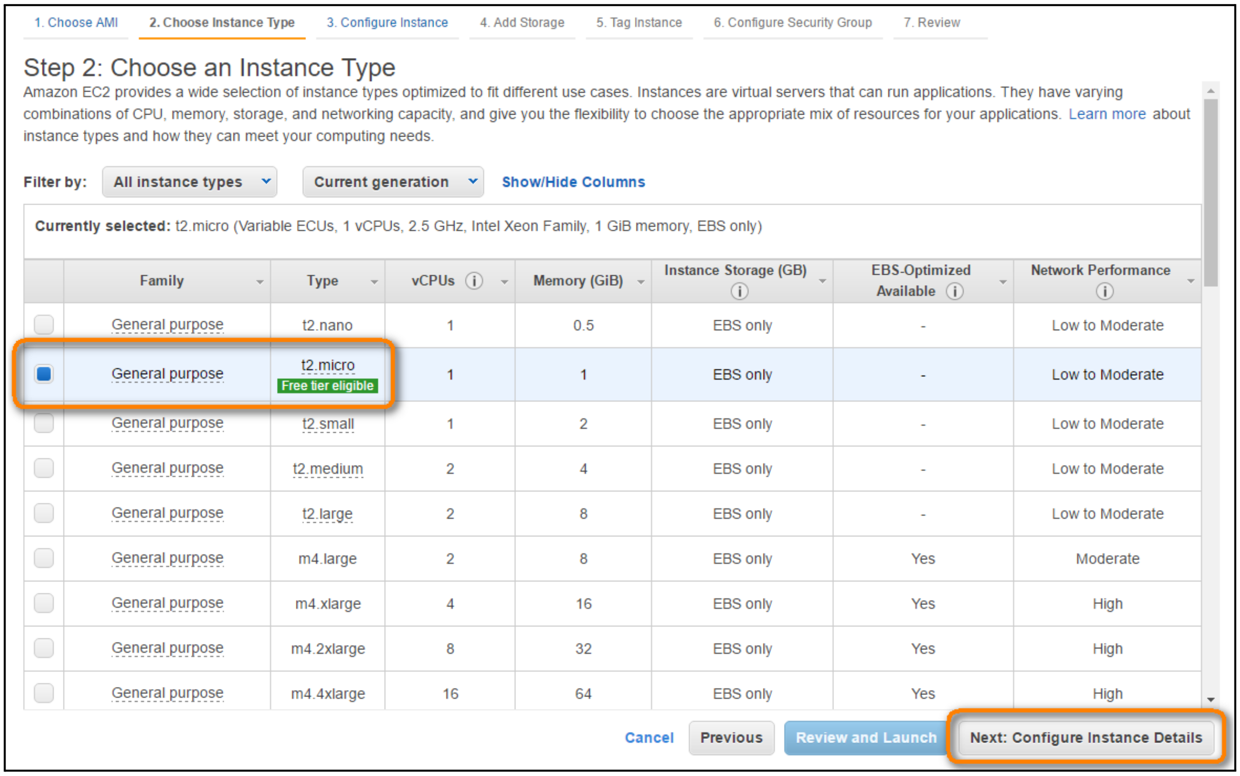


	Name	AMI Name	AMI ID	Source	Owner	Visibilit
■		Peplink FusionHub 6.2.1b01	ami-fd3375cd	100871073111/...	100871073111	Private

Setting the Instance type

1. In the next screen “Choose an Instance Type, click to highlight “**t2.micro**”

2. Then click “**Configure Instance Details**” at the bottom right of the page.



Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

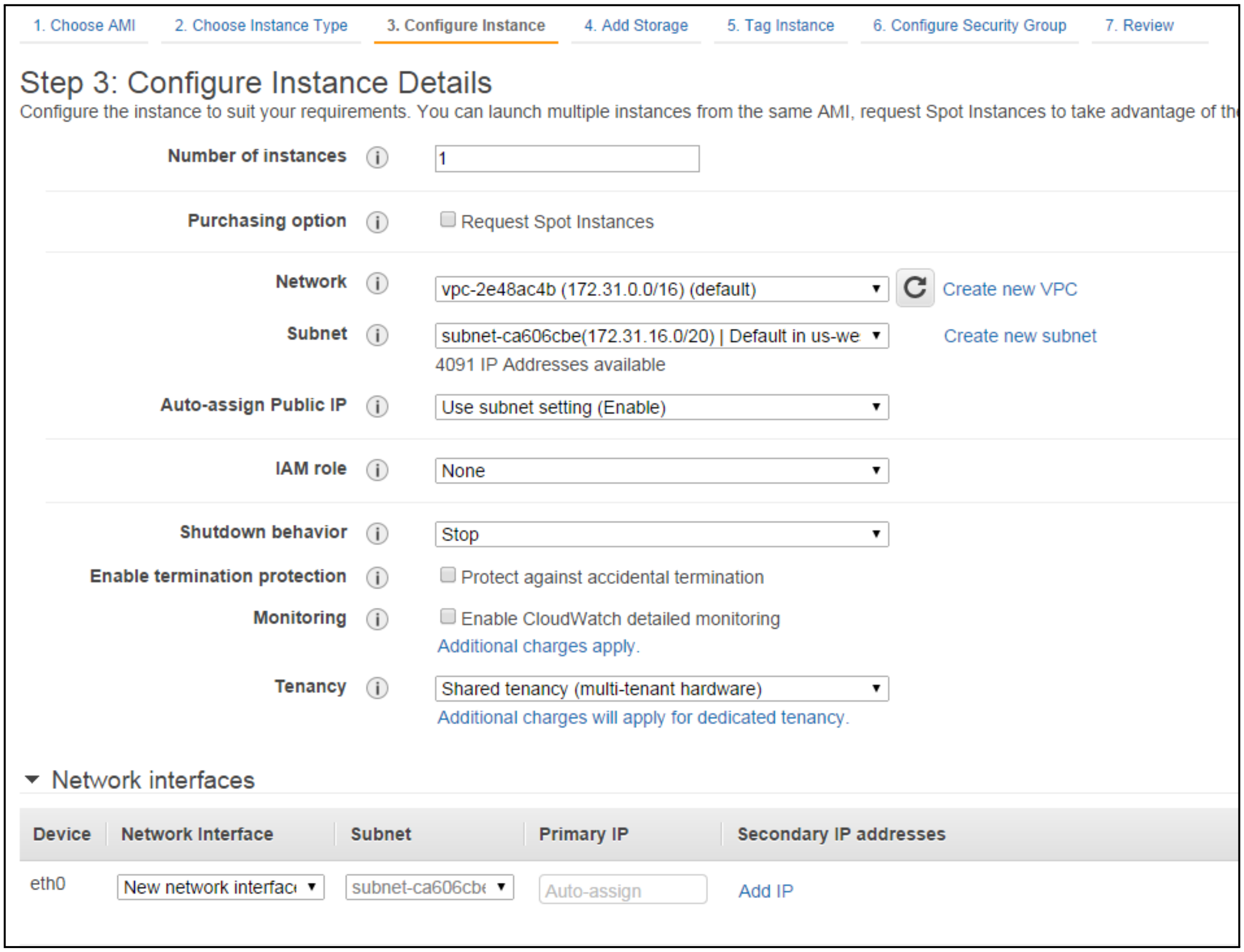
Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
□	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate
■	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate
□	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
□	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
□	General purpose	t2.large	2	8	EBS only	-	Low to Moderate
□	General purpose	m4.large	2	8	EBS only	Yes	Moderate
□	General purpose	m4.xlarge	4	16	EBS only	Yes	High
□	General purpose	m4.2xlarge	8	32	EBS only	Yes	High
□	General purpose	m4.4xlarge	16	64	EBS only	Yes	High

Configuring the Instance

1. The “Configure Instance Details” page allows you to make changes to the Instance details and network interfaces. If you’re unsure what these should be, then please skip this step.

2. Click “**Review and Launch**” at the bottom right.



Step 3: Configure Instance Details

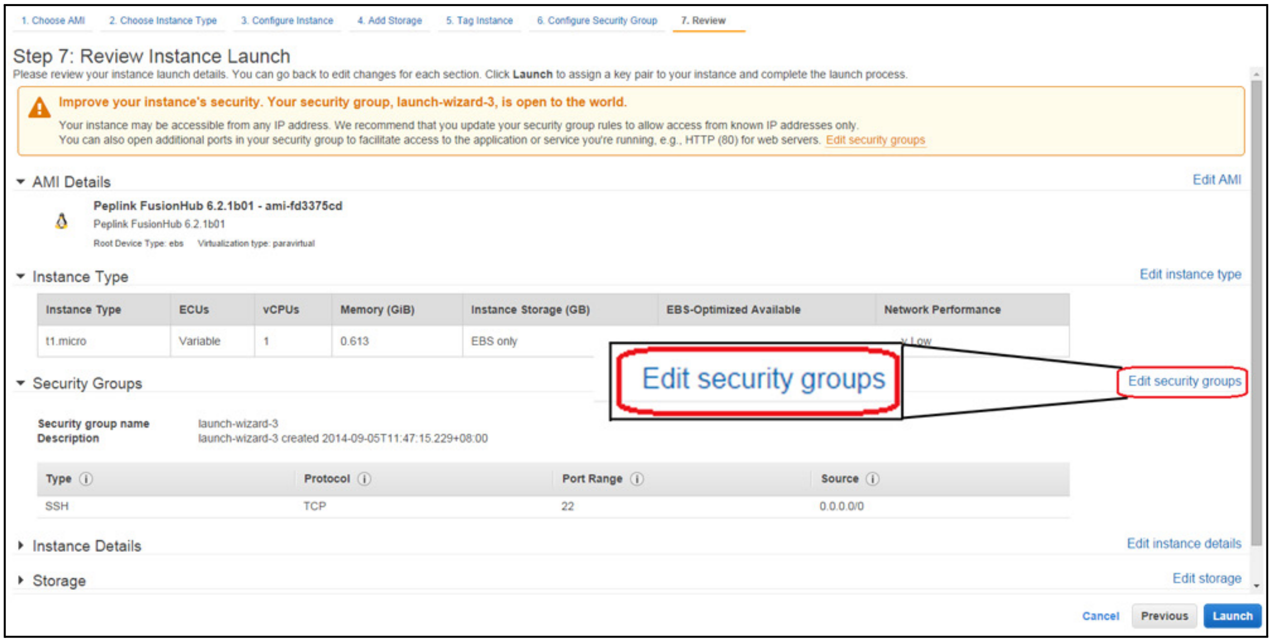
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot Instances to take advantage of th

Number of instances	1
Purchasing option	□ Request Spot Instances
Network	vpc-2e48ac4b (172.31.0.0/16) (default) ▾ Create new VPC
Subnet	subnet-ca606cbe(172.31.16.0/20) | Default in us-we ▾ Create new subnet 4091 IP Addresses available
Auto-assign Public IP	Use subnet setting (Enable) ▾
IAM role	None ▾
Shutdown behavior	Stop ▾
Enable termination protection	□ Protect against accidental termination
Monitoring	□ Enable CloudWatch detailed monitoring Additional charges apply.
Tenancy	Shared tenancy (multi-tenant hardware) ▾ Additional charges will apply for dedicated tenancy.

▾ Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses
eth0	New network interfac ▾	subnet-ca606cbe ▾	Auto-assign	Add IP

3. In the next page “Review Instance Launch”, click on “**Edit security groups**”.



Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Improve your instance's security. Your security group, launch-wizard-3, is open to the world.

Your instance may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups

AMI Details

Peplink FusionHub 6.2.1b01 - ami-fd3375cd
Peplink FusionHub 6.2.1b01
Root Device Type: ebs Virtualization type: paravirtual

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t1.micro	Variable	1	0.613	EBS only		v Low

Security Groups

Security group name launch-wizard-3
Description launch-wizard-3 created 2014-09-05T11:47:15.229+08:00

Type	Protocol	Port Range	Source
SSH	TCP	22	0.0.0.0/0

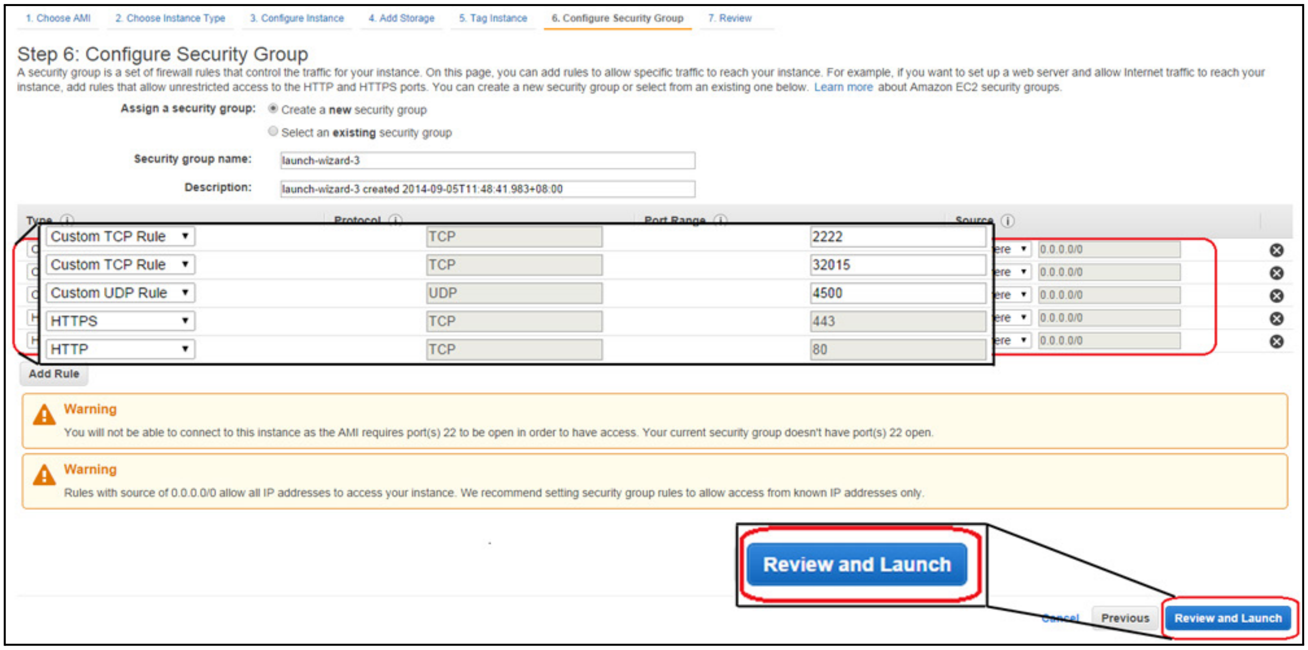
Instance Details

Storage

4. **Configure** the security group settings as follows:
    - Remove SSH
    - Add TCP 2222/32015
    - Add UDP 4500 to 4504 or UDP 32015 to 32019
    - Add HTTP/HTTPS

5. Click “**Review and Launch**”

6. Confirm that the details are correct, and then click “**Launch**”.



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ● Create a **new** security group

○ Select an **existing** security group

Security group name: launch-wizard-3

Description: launch-wizard-3 created 2014-09-05T11:48:41.983+08:00

Type	Protocol	Port Range	Source
Custom TCP Rule	TCP	2222	0.0.0.0/0
Custom TCP Rule	TCP	32015	0.0.0.0/0
Custom UDP Rule	UDP	4500	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0
HTTP	TCP	80	0.0.0.0/0

Warning

You will not be able to connect to this instance as the AMI requires port(s) 22 to be open in order to have access. Your current security group doesn't have port(s) 22 open.

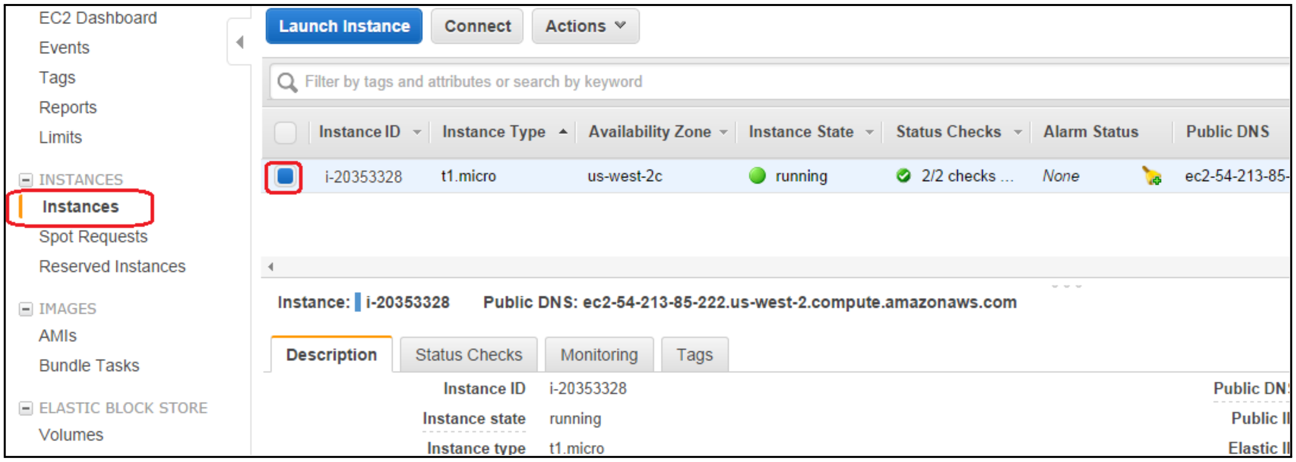
Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Tweak the running Instance

1. In the left hand panel, expand “Instances” and click on “**Instances**”.

2. Select FusionHub’s **running instance** by clicking on it once.



Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS
i-20353328	t1.micro	us-west-2c	running	2/2 checks ...	None	ec2-54-213-85-

Instance: i-20353328 Public DNS: ec2-54-213-85-222.us-west-2.compute.amazonaws.com

Instance ID i-20353328

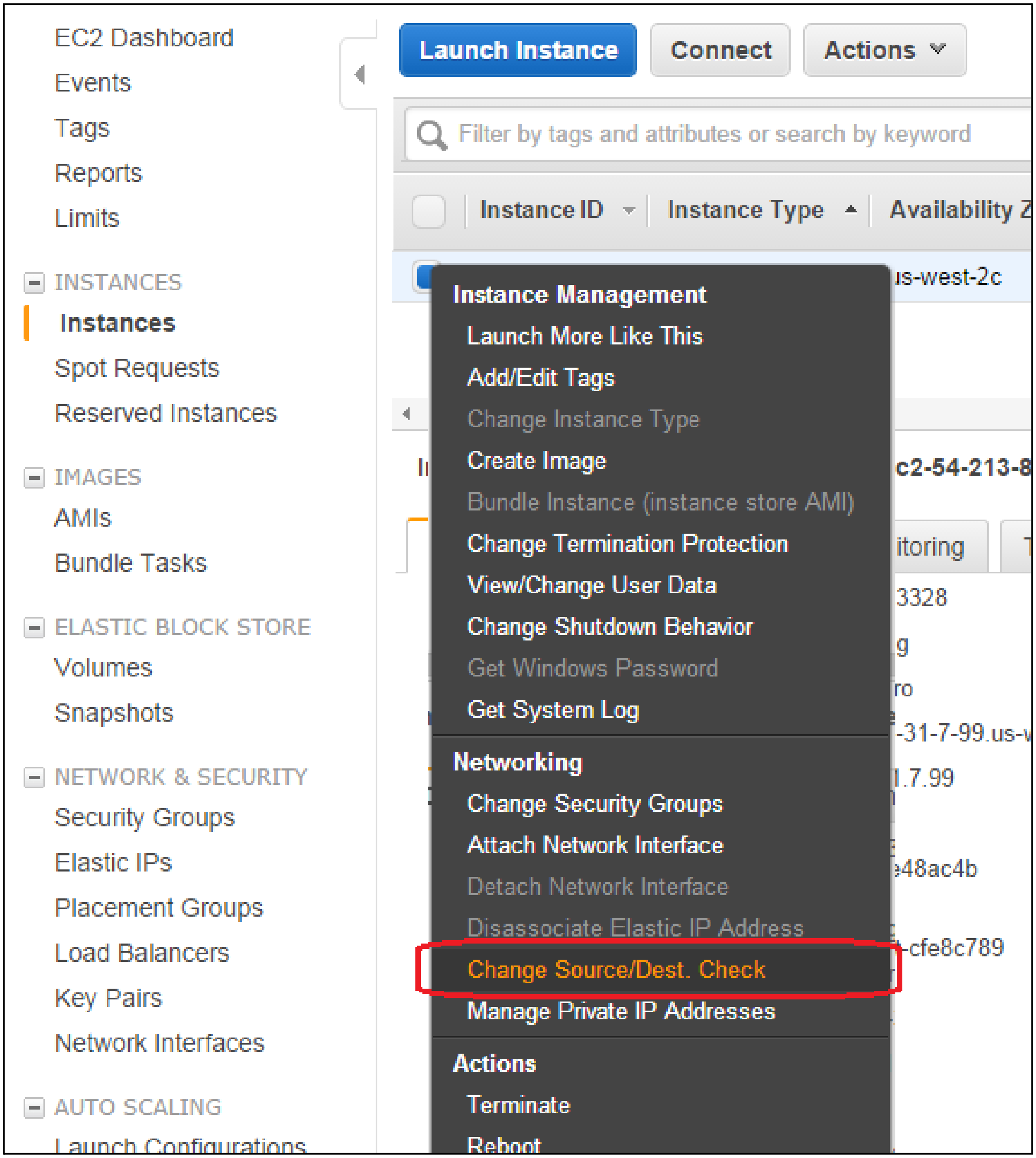
Instance state running

Instance type t1.micro

3. After highlighting the running instance, right-click to bring up the **context menu**.

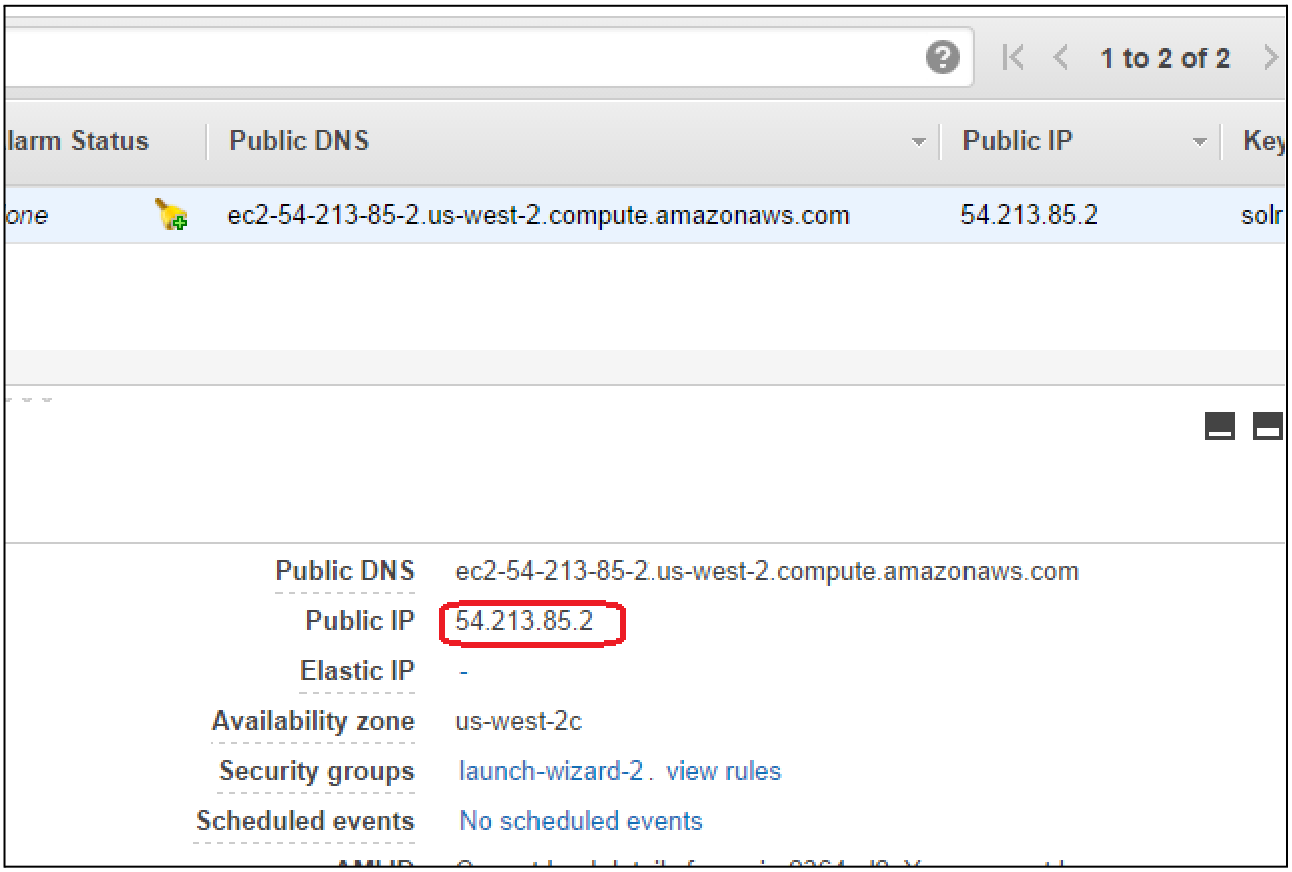
4. Click on “**Change Source/Des. Check**” in the context menu

5. Select “**Disable Source/Dest. Check**”.


EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Load Balancers
Key Pairs
Network Interfaces
AUTO SCALING
Launch Configurations
Launch Instance
Connect
Actions
Filter by tags and attributes or search by keyword
Instance ID
Instance Type
Availability Z
us-west-2c
Instance Management
Launch More Like This
Add/Edit Tags
Change Instance Type
Create Image
Bundle Instance (instance store AMI)
Change Termination Protection
View/Change User Data
Change Shutdown Behavior
Get Windows Password
Get System Log
Networking
Change Security Groups
Attach Network Interface
Detach Network Interface
Disassociate Elastic IP Address
Change Source/Dest. Check
Manage Private IP Addresses
Actions
Terminate
Reboot
c2-54-213-8
itoring
3328
-31-7-99.us-w
.7.99
48ac4b
-cfe8c789

Accessing FusionHub

1. Note down FusionHub's public **IP address**.



larm Status	Public DNS	Public IP	Key
one	ec2-54-213-85-2.us-west-2.compute.amazonaws.com	54.213.85.2	solr

Public DNS ec2-54-213-85-2.us-west-2.compute.amazonaws.com
Public IP 54.213.85.2
Elastic IP -
Availability zone us-west-2c
Security groups launch-wizard-2. view rules
Scheduled events No scheduled events

2. In your web browser, type in "**http://[FusionHub.instance.public.ip.address]**" in order to access FusionHub's administration interface. In our example, the line to type into the web browser would be: http://54.213.85.2/

3. Follow Section 5 to continue.

4.8. Other Cloud-Service Platform

4.8.1. Microsoft Azure

Do refer to this KB article for the FusionHub on Microsoft Azure installation guide:
https://forum.peplink.com/t/configuring-fusionhub-on-microsoft-azure/14187/1

4.8.2. Google Cloud Engine

Do refer to this KB article for the FusionHub on Google Cloud Engine installation guide:
https://forum.peplink.com/t/configuring-fusionhub-for-google-cloud-engine/14439/1

5. FusionHub Interface Configuration

5.1. Connecting to FusionHub's Web Admin Interface

1. Open a Web browser on the computer hosting your Peplink FusionHub virtual machine.

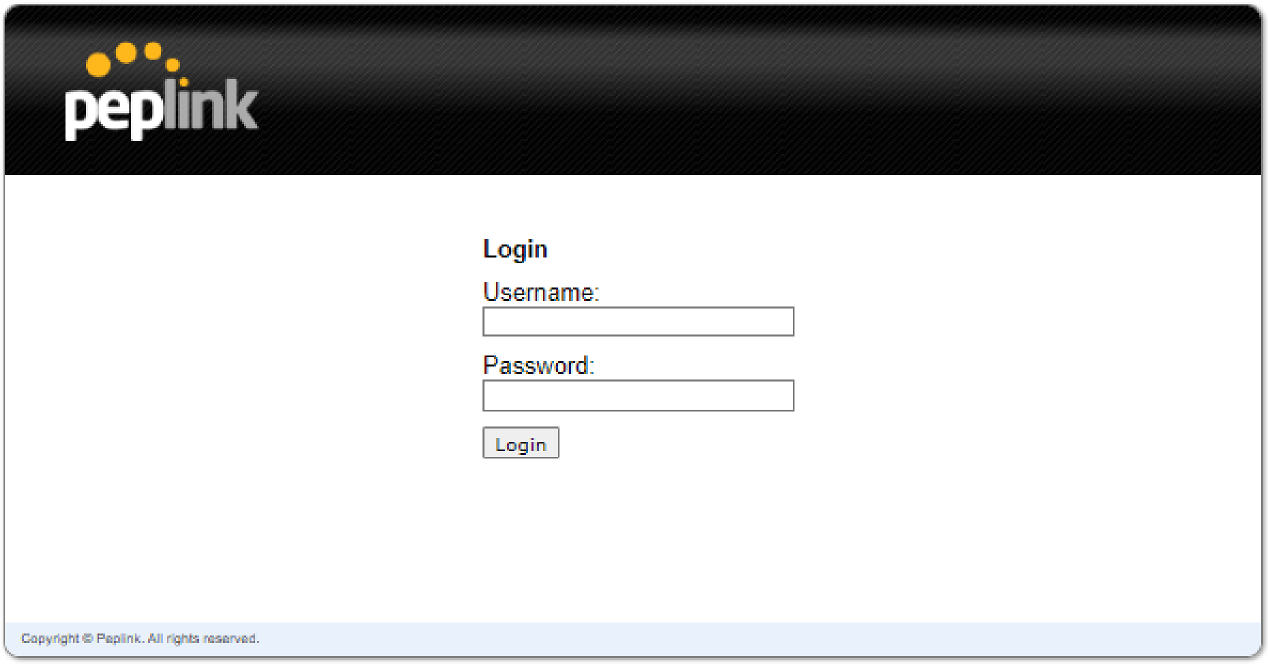
2. To access FusionHub's Web admin interface, connect your computer to the network on which FusionHub is running. The default WAN connection method for FusionHub is DHCP.

3. If the DHCP server is available in your network, the FusionHub IP address will be automatically obtained by the DHCP server. The Web admin address will appear on the FusionHub console automatically (i.e., Admin: http://10.8.8.252). Enter the Web admin address (i.e., http://10.8.8.252) in your Web browser's address field.

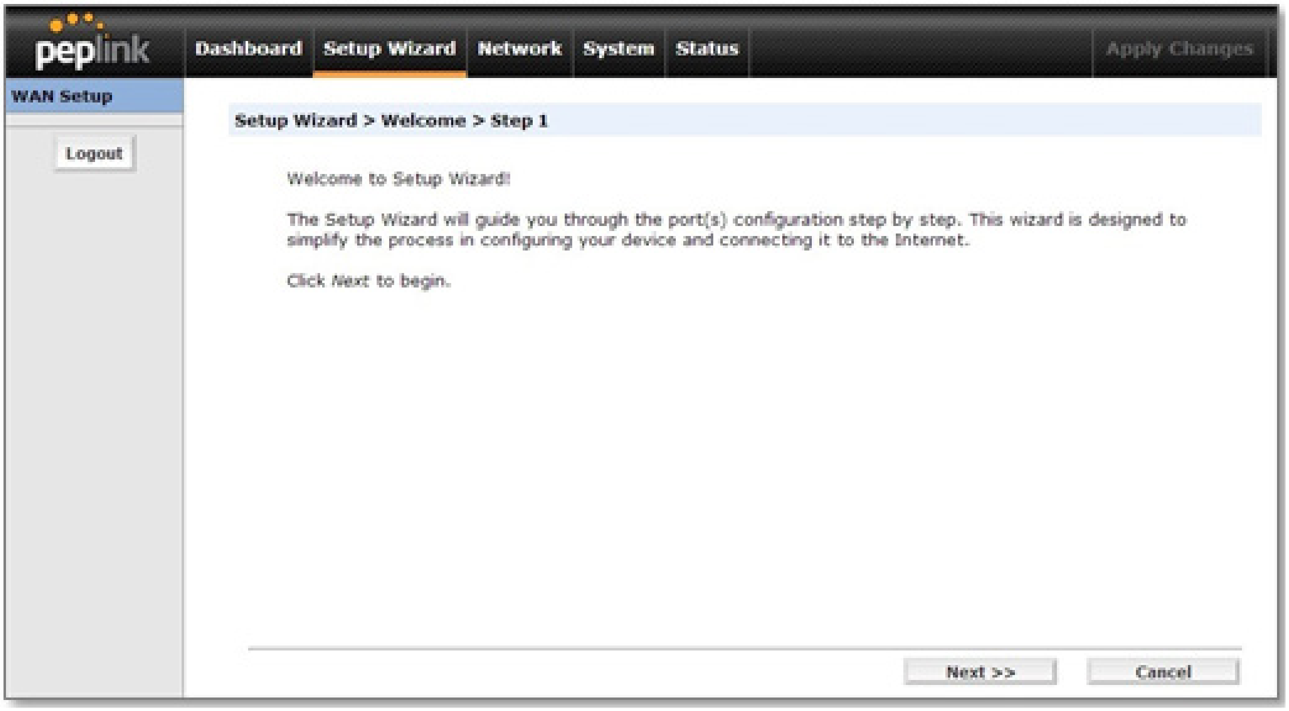
4. If there is no DHCP server in your network, set your computer's IP address to 169.254.x.x (*x* denotes any integer from 2 to 253), using a subnet mask of 255.255.0.0.

5. After successfully changing these settings, enter **http://169.254.254.254** in your Web browser's address field.

6. Next, access the Web admin interface by entering **admin** for both the username and password. The default admin and read-only user passwords can be changed after logging into the Web admin interface at **System > Admin Security**. Please take note that if the FusionHub is obtained from AWS Marketplace, the default password is the ***AWS Instance ID***.



7. Once you have successfully logged in, the **Setup Wizard** will be displayed.



Setup Wizard > Welcome > Step 1

Welcome to Setup Wizard!

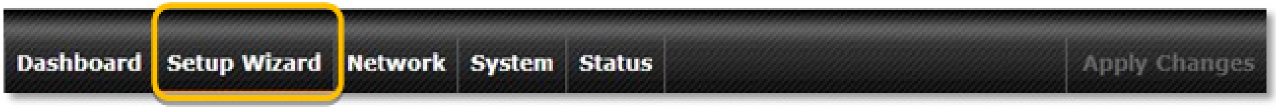
The Setup Wizard will guide you through the port(s) configuration step by step. This wizard is designed to simplify the process in configuring your device and connecting it to the Internet.

Click *Next* to begin.

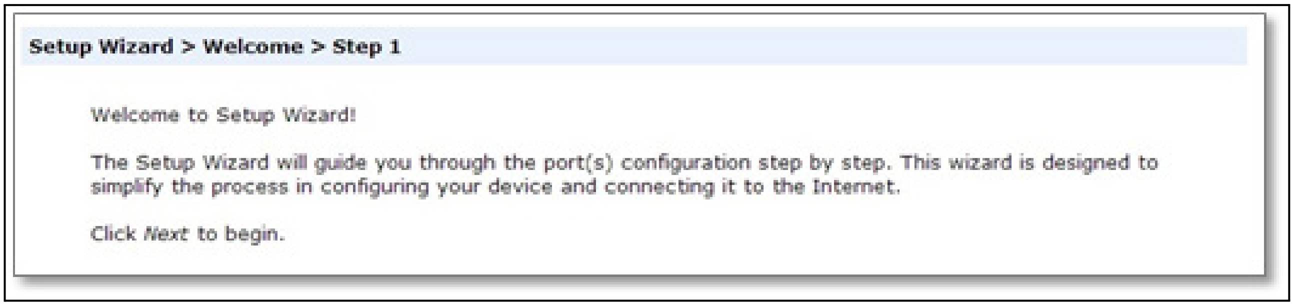
5.2. Configuration Using the Setup Wizard

FusionHub's **Setup Wizard** leads you step-by-step through the process of configuring your WAN connection.

1. Click **Setup Wizard** after connecting to the Web admin interface.



2. Click **Next** to begin.



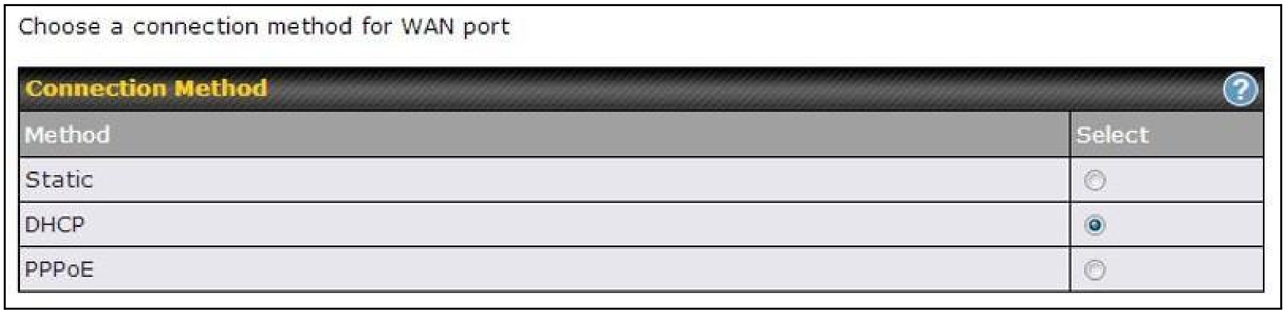
Setup Wizard > Welcome > Step 1

Welcome to Setup Wizard!

The Setup Wizard will guide you through the port(s) configuration step by step. This wizard is designed to simplify the process in configuring your device and connecting it to the Internet.

Click *Next* to begin.

3. Click **Next** to configure the WAN connection. Select the WAN connection method from the following screen. The default selection is **DHCP**.



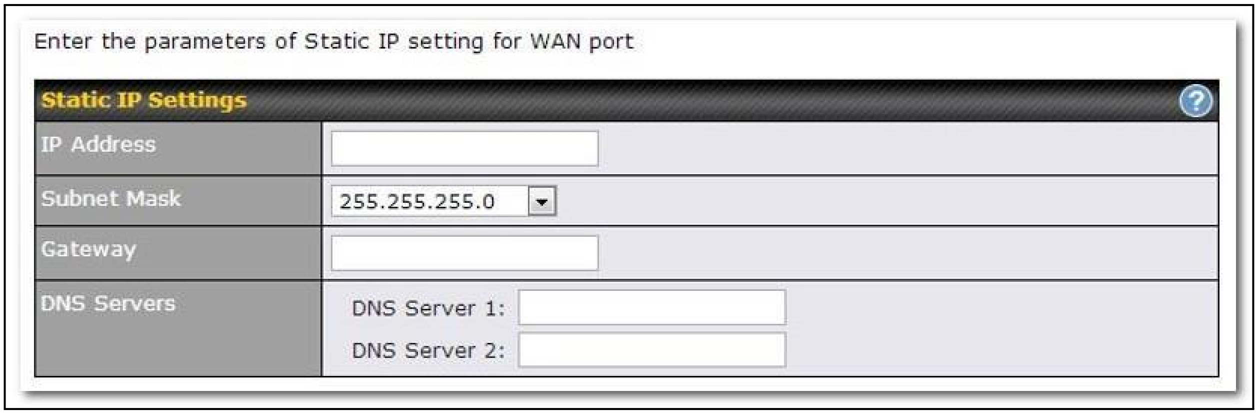
Choose a connection method for WAN port

Connection Method

Method	Select
Static	○
DHCP	●
PPPoE	○

4. Depending on the selected connection type, further configuration may be needed:

- If **Static** is selected, the Setup Wizard will display **Static IP Settings**.

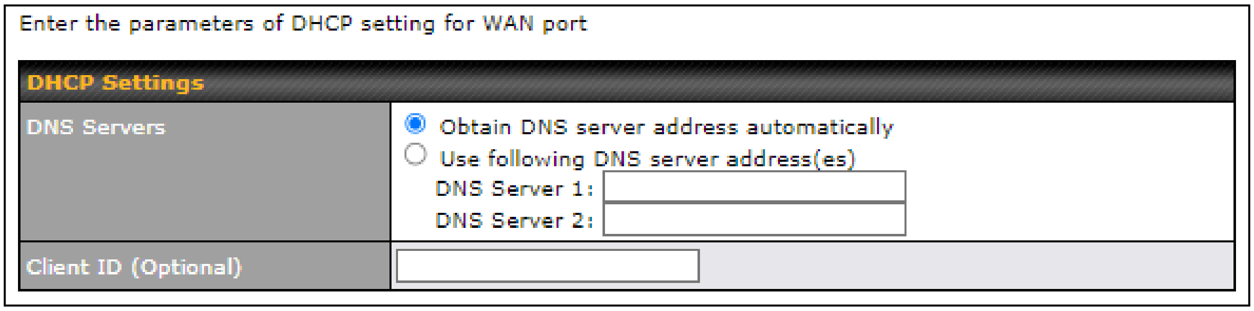


Enter the parameters of Static IP setting for WAN port

Static IP Settings

IP Address	
Subnet Mask	255.255.255.0 ▾
Gateway	
DNS Servers	DNS Server 1: DNS Server 2:

- If **DHCP** is selected, the Setup Wizard will display **DHCP Settings**.

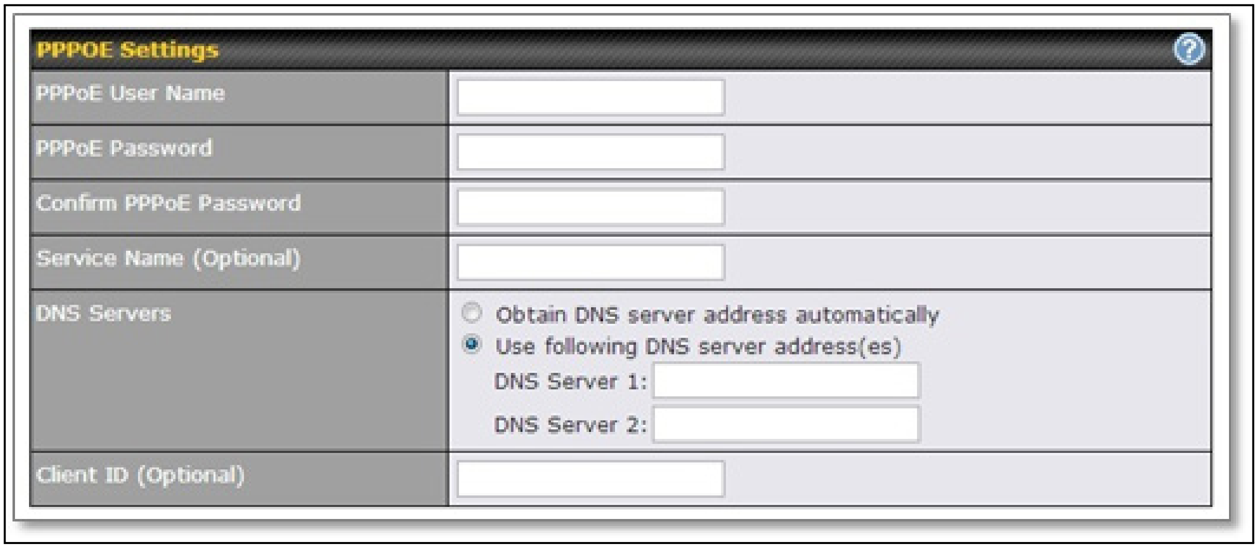


Enter the parameters of DHCP setting for WAN port

DHCP Settings

DNS Servers	● Obtain DNS server address automatically ○ Use following DNS server address(es) DNS Server 1: DNS Server 2:
Client ID (Optional)	

- If **PPPoE** is selected, the Setup Wizard will display **PPPoE Settings**.

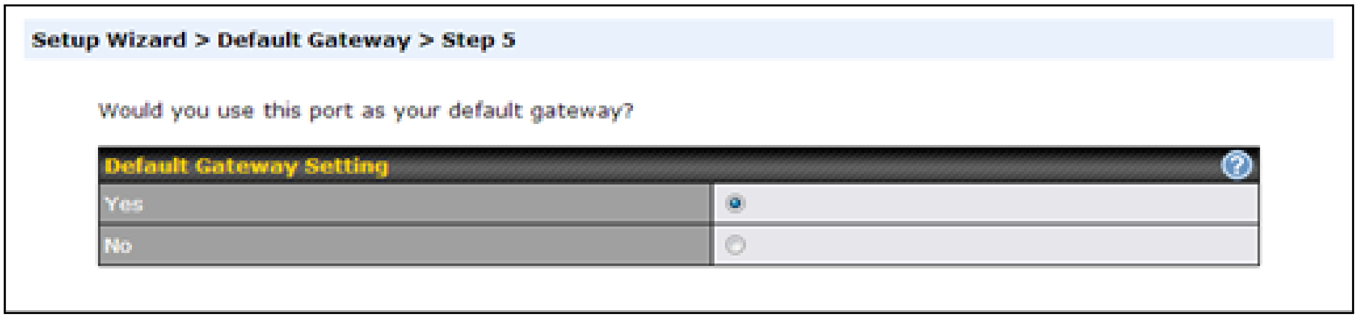


PPPOE Settings	
PPPoE User Name	
PPPoE Password	
Confirm PPPoE Password	
Service Name (Optional)	
DNS Servers	○ Obtain DNS server address automatically ● Use following DNS server address(es) DNS Server 1: DNS Server 2:
Client ID (Optional)	

During this step, make sure the FusionHub and ESXi servers are on the same network if **Static** is selected. For example:

If the ESXi server's IP settings are:
IP address: **10.8.9.124**
Subnet mask: **255.255.0.0**
Default gateway: **10.8.8.1**

Configure port settings as follows:
IP address: **10.8.x.x** (x denotes any integer from 2 to 254)
Subnet mask: **255.255.0.0**
Default gateway: **10.8.8.1**

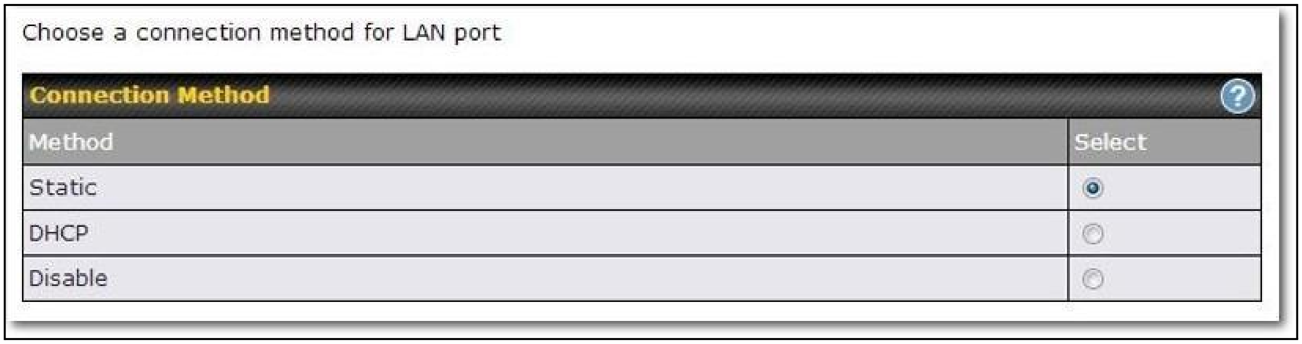


Setup Wizard > Default Gateway > Step 5

Would you use this port as your default gateway?

Default Gateway Setting	
Yes	●
No	○

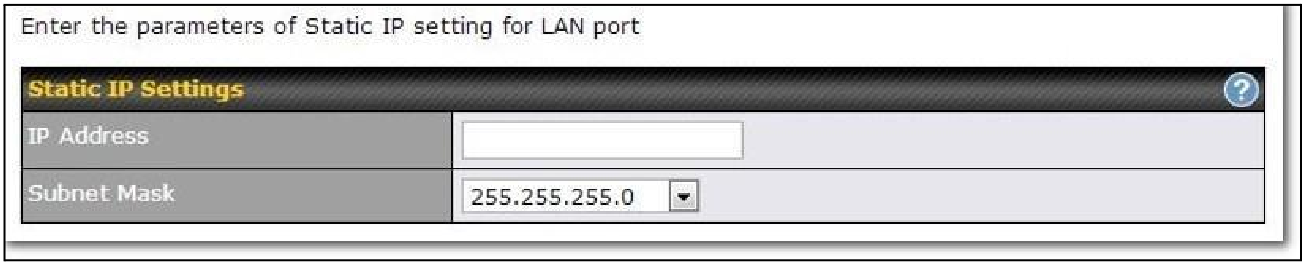
5. If there is more than one port on the ESXi server and you have assigned two network adapters to this FusionHub virtual machine, the LAN port configuration dialog will be open. The default selection is **Static**.



Choose a connection method for LAN port

Connection Method	
Method	Select
Static	●
DHCP	○
Disable	○

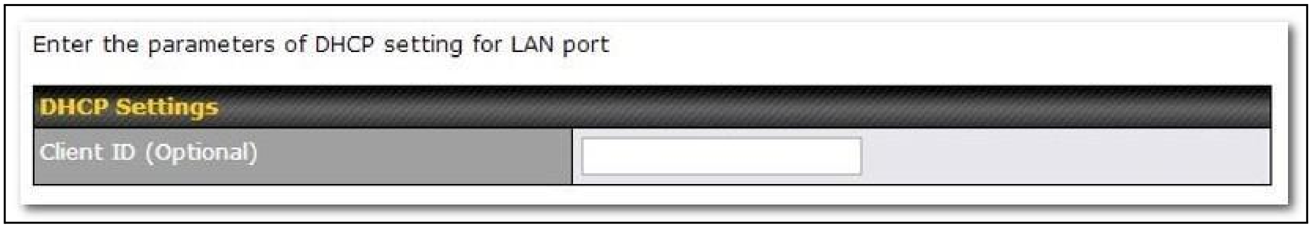
- If **Static** is selected, the Setup Wizard will display **Static IP Setting**s.



Enter the parameters of Static IP setting for LAN port

Static IP Settings	
IP Address	
Subnet Mask	255.255.255.0

- If **DHCP** is selected, the Setup Wizard will display **DHCP Settings**.

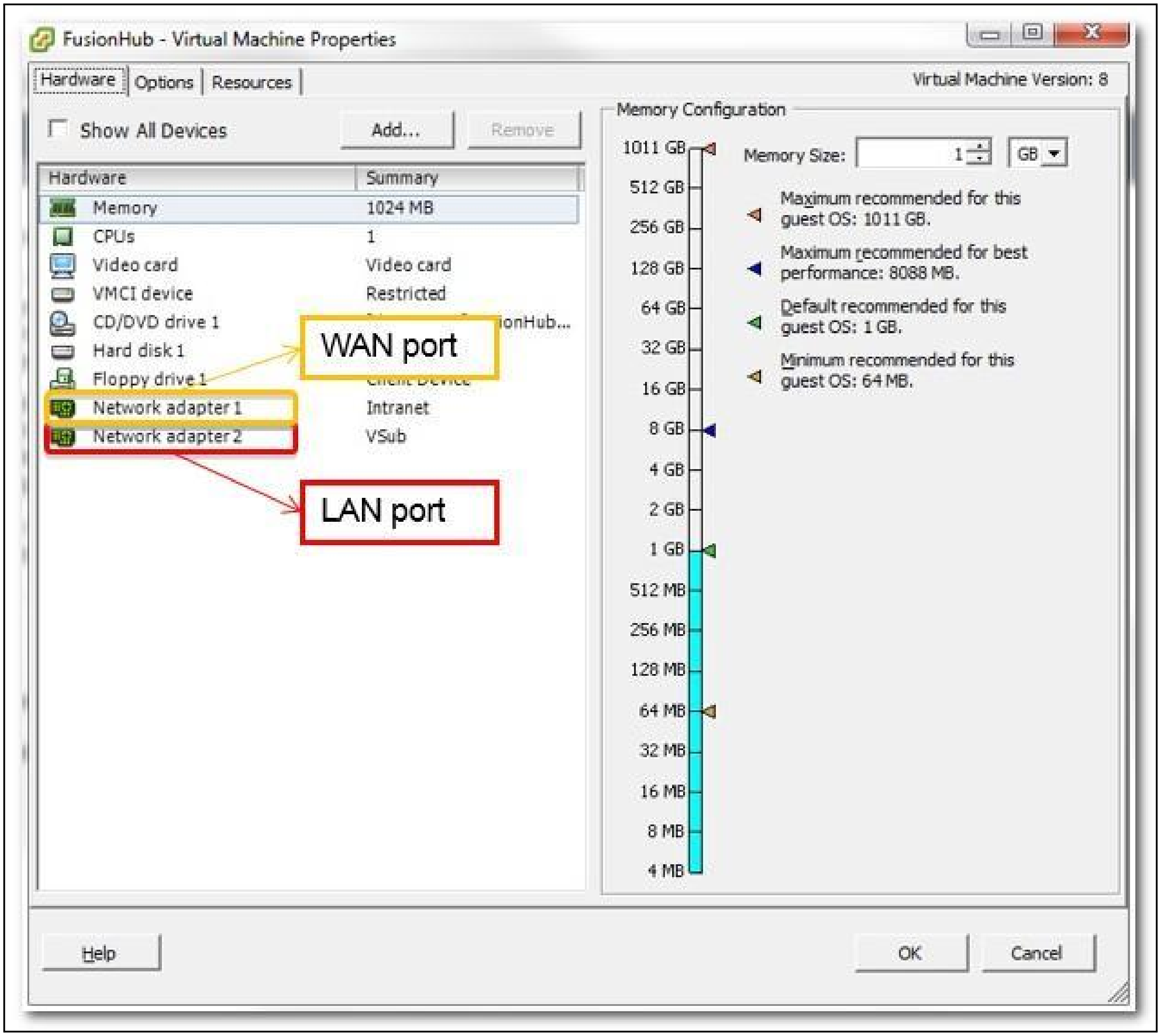


Enter the parameters of DHCP setting for LAN port

DHCP Settings	
Client ID (Optional)	

- If **Disable** is selected, the Setup Wizard will move to the next step.

Note: FusionHub virtual machines support a maximum number of two network adapters. By default, **Network adapter 1** is set as the WAN port, and **Network adapter 2** is set as the LAN port.



Hardware	Summary
Memory	1024 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
CD/DVD drive 1	ionHub...
Hard disk 1	
Floppy drive 1	Client Device
Network adapter 1	Intranet
Network adapter 2	VSub

Memory Size: 1 GB

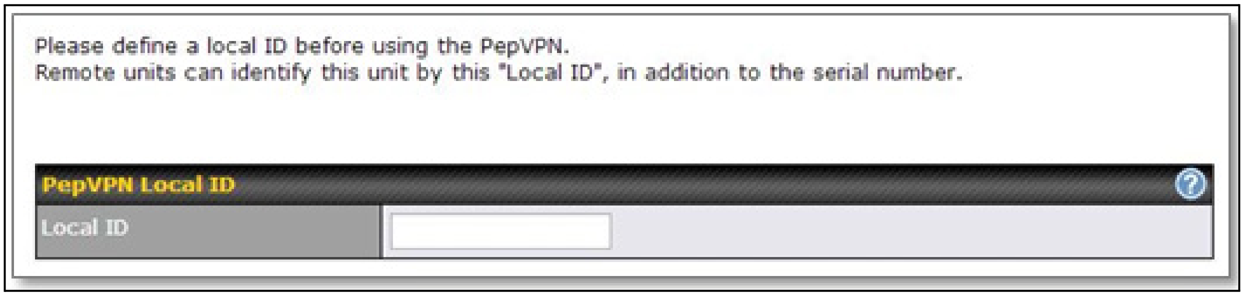
Maximum recommended for this guest OS: 1011 GB.

Maximum recommended for best performance: 8088 MB.

Default recommended for this guest OS: 1 GB.

Minimum recommended for this guest OS: 64 MB.

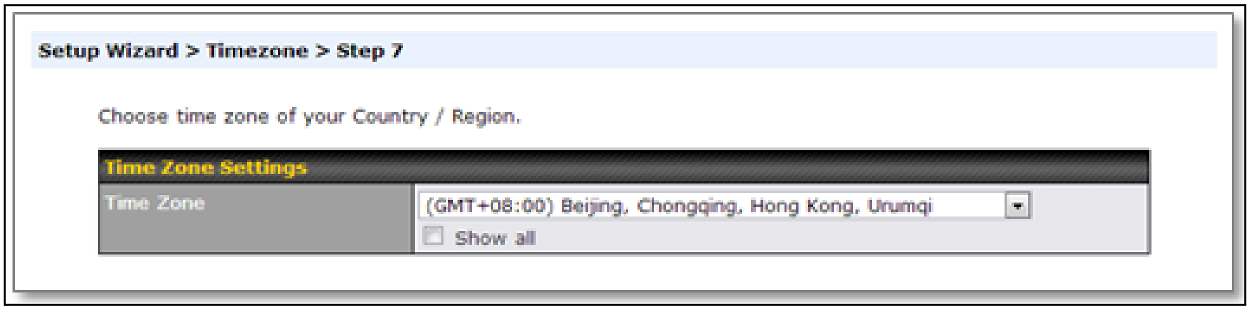
6. Click **Next** to define a **Local ID** before using PepVPN. The local ID is a text string that identifies this local unit when establishing a VPN connection. Remote units can identify this unit using the local ID, as well as by serial number. When creating a profile on a remote unit, this unit's local ID must be entered into the remote unit's **Remote ID** field.



Please define a local ID before using the PepVPN.
Remote units can identify this unit by this "Local ID", in addition to the serial number.

PepVPN Local ID	
Local ID	

7. Click **Next** to choose the time zone of your country/region. Check **Show all** to display all time zone options.

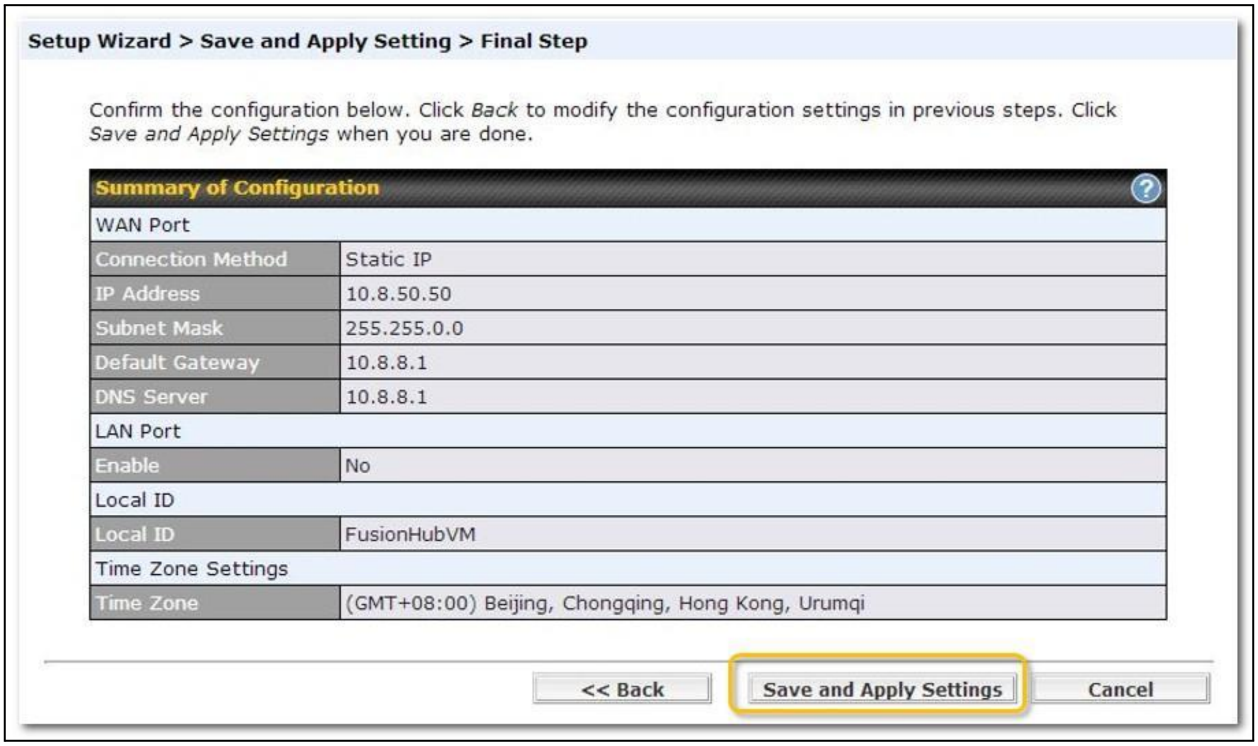


Setup Wizard > Timezone > Step 7

Choose time zone of your Country / Region.

Time Zone Settings	
Time Zone	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi □ Show all

8. Check to make sure all settings have been configured correctly, and then click **Save and Apply Settings** to confirm.



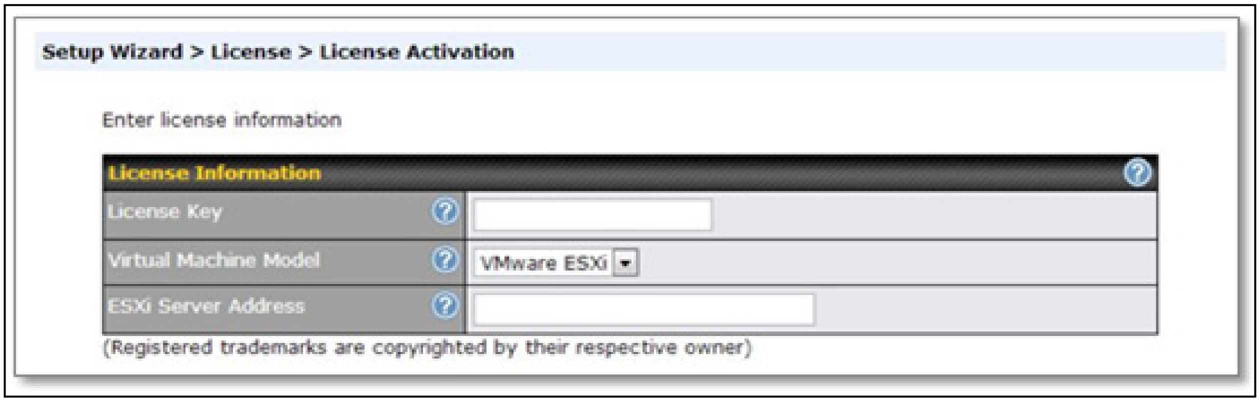
Setup Wizard > Save and Apply Setting > Final Step

Confirm the configuration below. Click *Back* to modify the configuration settings in previous steps. Click *Save and Apply Settings* when you are done.

Summary of Configuration	
WAN Port	
Connection Method	Static IP
IP Address	10.8.50.50
Subnet Mask	255.255.0.0
Default Gateway	10.8.8.1
DNS Server	10.8.8.1
LAN Port	
Enable	No
Local ID	
Local ID	FusionHubVM
Time Zone Settings	
Time Zone	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi

9. You will be redirected to the **License Information** dialog. The default selection for **Virtual**

Machine Model is **VMware ESXi.** The default **License Information** dialog looks similar to the following



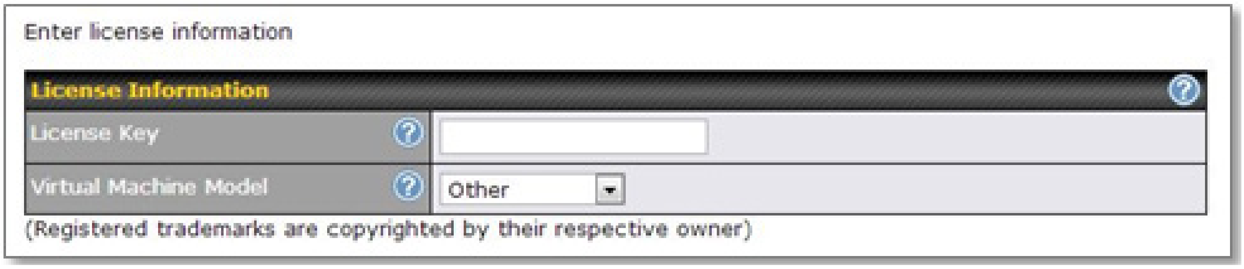
Setup Wizard > License > License Activation

Enter license information

License Information	
License Key	
Virtual Machine Model	VMware ESXi
ESXi Server Address	

(Registered trademarks are copyrighted by their respective owner)

If you are **not** using VMware ESXi, please select **Other** for the **Virtual Machine \Model**. In that case, the license activation dialog will look similar to this:



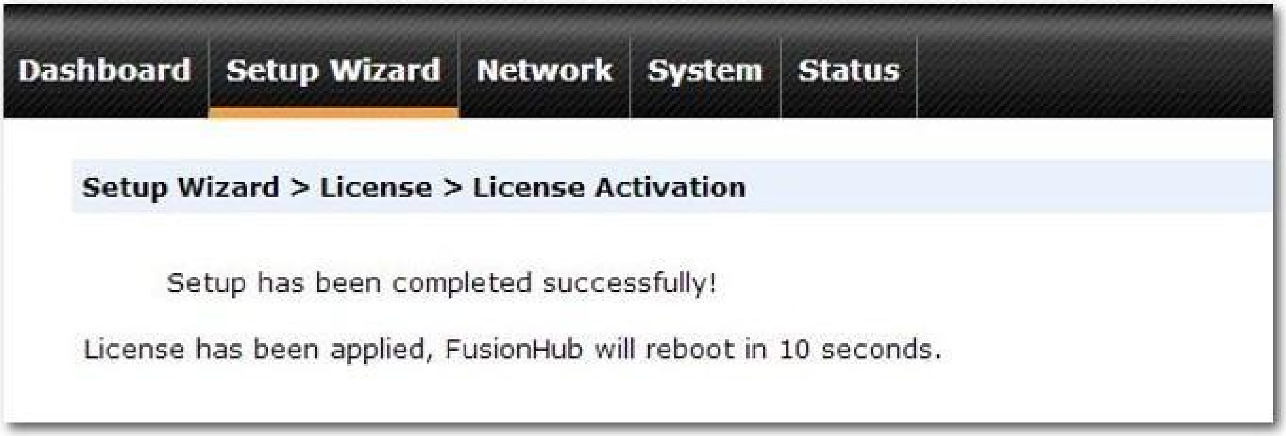
Enter license information

License Information	
License Key	
Virtual Machine Model	Other

(Registered trademarks are copyrighted by their respective owner)

- **License Key** is the FusionHub license key obtained from the InControl2 webpage. Please refer to **FusionHub License Generation** for details on creating this license key.
- **Virtual Machine Model** is the virtual machine platform on which FusionHub is implemented. If FusionHub is implemented on a VMware ESXi Server, please select **VMware ESXi**. If it is implemented on a VMware Workstation or VMware Player, please select **Other.**
- **ESXi Server address** is the ESXi server's hostname or IP address. Note: this column is shown only when **VMware ESXi** is selected.
- Click **Submit** after filling the form.

10. When the license is successfully activated, you will see the following screen.

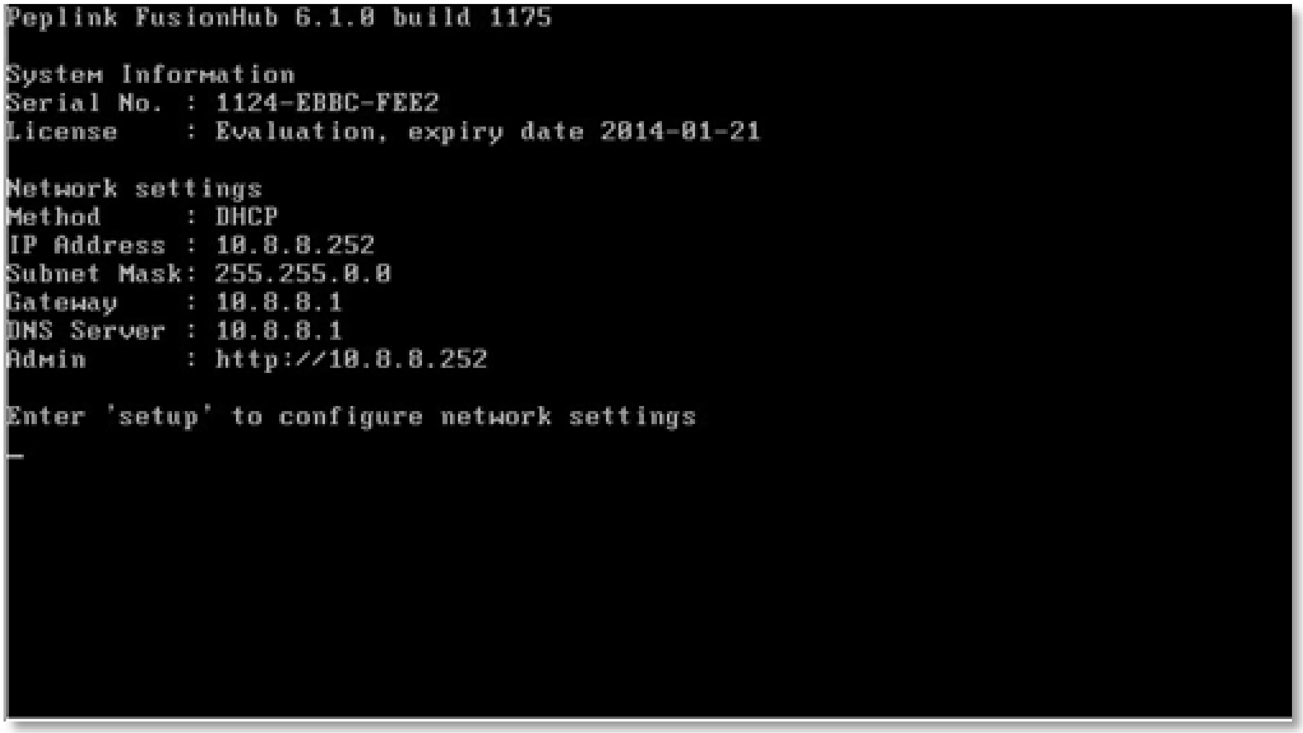


Setup Wizard > License > License Activation

Setup has been completed successfully!

License has been applied, FusionHub will reboot in 10 seconds.

The information shown on the FusionHub console will change to the following:



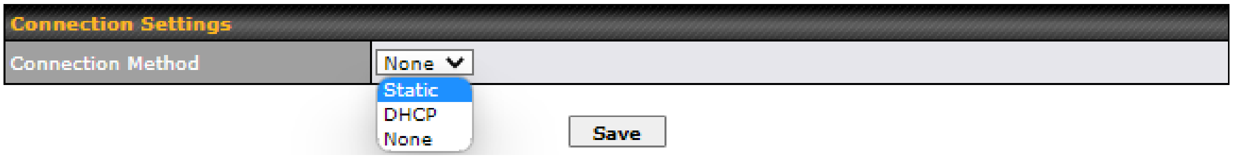
```
Peplink FusionHub 6.1.0 build 1175

System Information
Serial No.  : 1124-EBBC-FEE2
License     : Evaluation, expiry date 2014-01-21

Network settings
Method      : DHCP
IP Address  : 10.8.8.252
Subnet Mask: 255.255.0.0
Gateway     : 10.8.8.1
DNS Server  : 10.8.8.1
Admin       : http://10.8.8.252

Enter 'setup' to configure network settings
_
```

If you have changed your computer's IP to 169.254.x.x, please change the computer's IP settings so that they're the same as your FusionHub network settings, and then connect to FusionHub's Web admin again.

6. Network

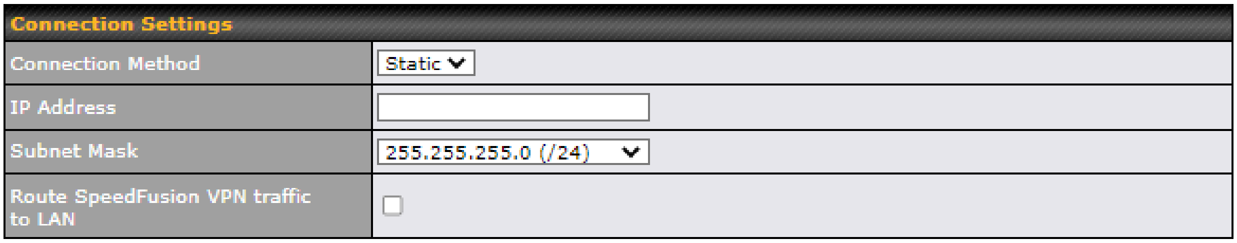
6.1. LAN

Navigate to the **Network > Interface > LAN**, to configure the LAN connectoin settings. The available options are:



Connection Settings	
Connection Method	None

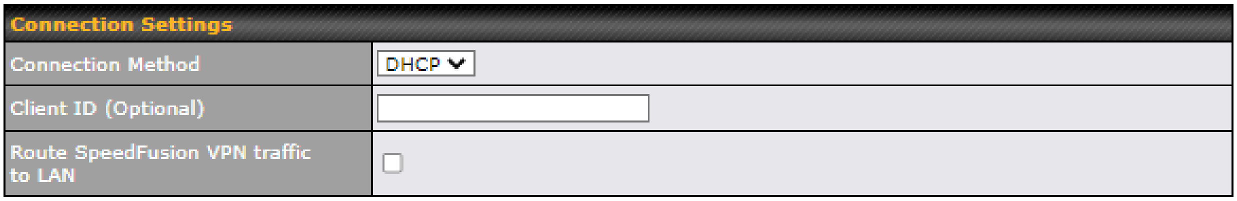
- **Static**



Connection Settings	
Connection Method	Static
IP Address	
Subnet Mask	255.255.255.0 (/24)
Route SpeedFusion VPN traffic to LAN	□

Connection Settings	
IP Address	This field is to allow you to configure the specific IP address of the Fusion Hub on the LAN connection
Subnet Mask	Select the subnet mask for LAN connection settings.
Gateway	If "**Route SpeedFusion VPN Trafic**" is ticked, the field will appear and need to configure the gateway for the LAN connection
Route SpeedFusion VPN Traffic	When this option is enabled, all traffic from SpeedFusion VPN will route to the LAN gateway.

- **DHCP**

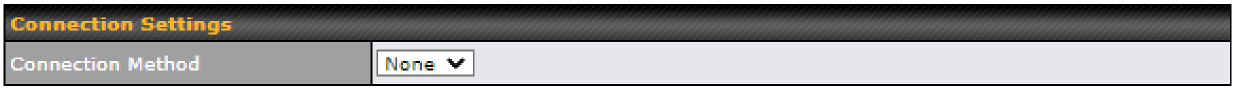


Connection Settings	
Connection Method	DHCP
Client ID (Optional)	
Route SpeedFusion VPN traffic to LAN	□

Connection Settings

Client ID (Option)	This field is the optional to allow you to configure the client ID for the WAN connection.
Route SpeedFusion VPN Traffic	When this option is enabled, all traffic from SpeedFusion VPN will route to the LAN gateway.

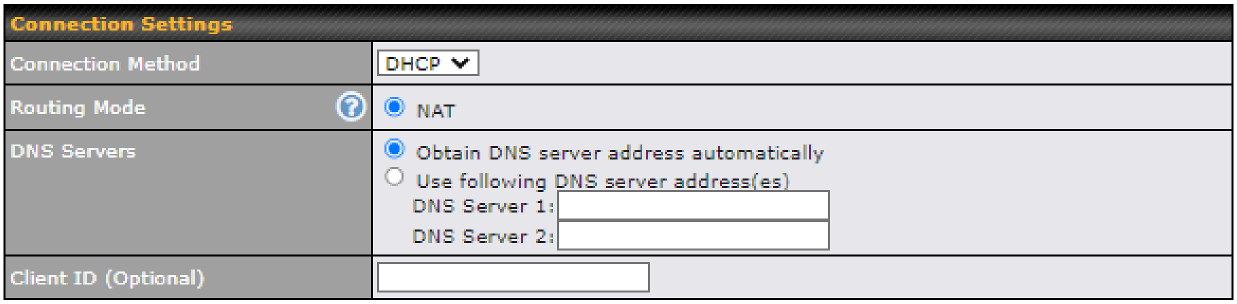
- **None**



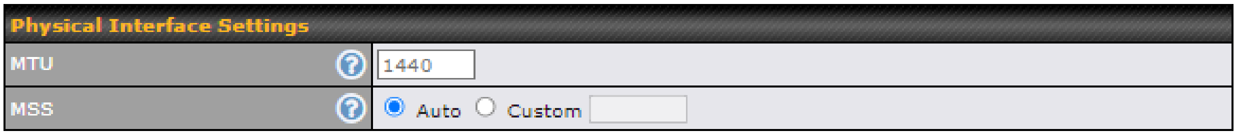
Connection Settings	
Connection Method	None ▾

6.2. WAN

Navigate to the **Network > Interface > WAN**, to configure the WAN connectoin settings. The available options are:

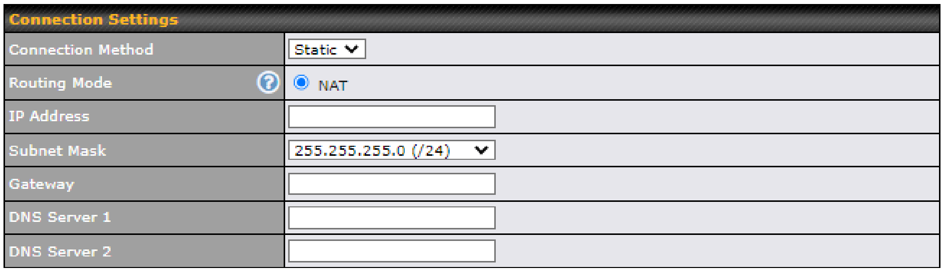


Connection Settings	
Connection Method	DHCP ▾
Routing Mode ?	● NAT
DNS Servers	● Obtain DNS server address automatically ○ Use following DNS server address(es) DNS Server 1: DNS Server 2:
Client ID (Optional)	



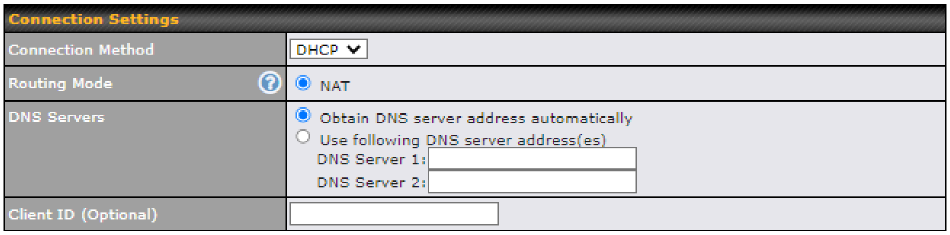
Physical Interface Settings	
MTU ?	1440
MSS ?	● Auto ○ Custom

Connection Settings	
Connection Method	There are three possible connection methods for the WAN: ● Static



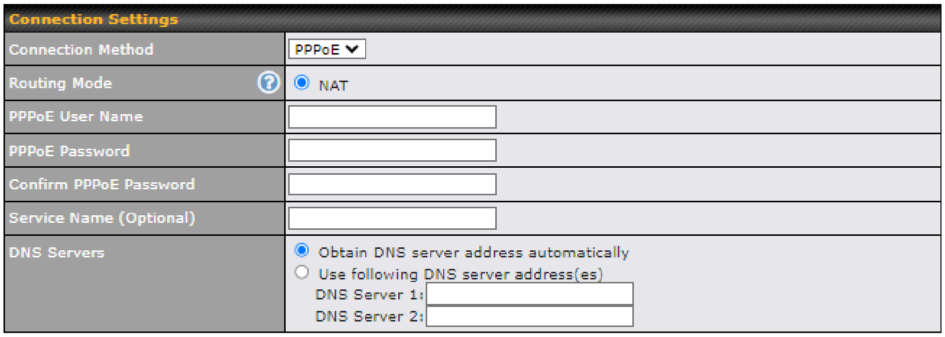
Connection Settings	
Connection Method	Static
Routing Mode ?	● NAT
IP Address	
Subnet Mask	255.255.255.0 (/24)
Gateway	
DNS Server 1	
DNS Server 2	

- DHCP



Connection Settings	
Connection Method	DHCP
Routing Mode ?	● NAT
DNS Servers	● Obtain DNS server address automatically ○ Use following DNS server address(es) DNS Server 1: DNS Server 2:
Client ID (Optional)	

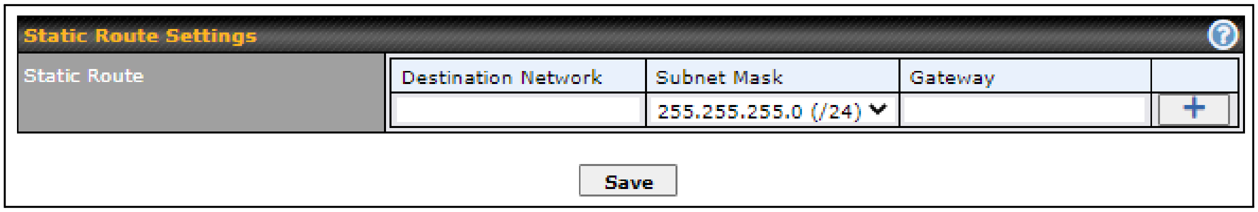
- PPPoE



Connection Settings	
Connection Method	PPPoE
Routing Mode ?	● NAT
PPPoE User Name	
PPPoE Password	
Confirm PPPoE Password	
Service Name (Optional)	
DNS Servers	● Obtain DNS server address automatically ○ Use following DNS server address(es) DNS Server 1: DNS Server 2:

Routing Mode	This field shows that **NAT** (network address translation) will be applied to the traffic routed over the WAN connection. **IP Forwarding** is available when you click the link in the help ? icon.
DNS Server	This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection.

6.3. Static Route



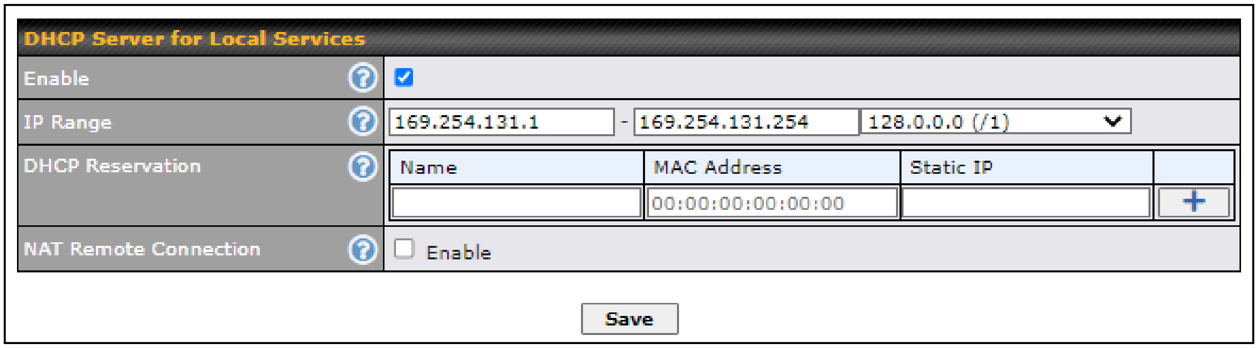
Static Route Settings

Static Route	Destination Network	Subnet Mask	Gateway	
		255.255.255.0 (/24)		+

This table is for defining static routing rules for the LAN segment. A static route consists of the network address, subnet mask, and gateway address. The address and subnet mask values are in w.x.y.z format.

Entries in this list will allow traffic to route to a different subnet that is connected to the LAN interface. Any traffic destined for a network/mask pair will be directed to the corresponding gateway.

6.4. DHCP Server



DHCP Server for Local Services

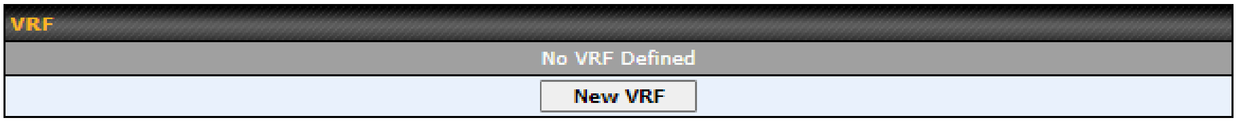
Enable	☑
IP Range	169.254.131.1 - 169.254.131.254 128.0.0.0 (/1)
DHCP Reservation	Name / MAC Address / Static IP 00:00:00:00:00:00 +
NAT Remote Connection	□ Enable

DHCP Server for Local Services	
Enable	DHCP server settings for profiles with NAT mode enabled. SpeedFusion VPN peer will get IP address from this DHCP settings if profile is set to NAT mode. You must enter DHCP server settings for NAT mode to work properly.
IP Range	This is to specify the range of IP addresses that the DHCP server will lease out.
DHCP Reservation	This setting reserves the assignment of fixed IP addresses on the LAN are identified by their MAC addresses.
NAT Remote Connection	If enabled, remote SpeedFusion VPN connections will be NAT'd to FusionHub's IP Address before deliver to internal network. Select "**Enable**" if DHCP IP Range is not routable in internal network.

7. Advanced

7.1. VRF

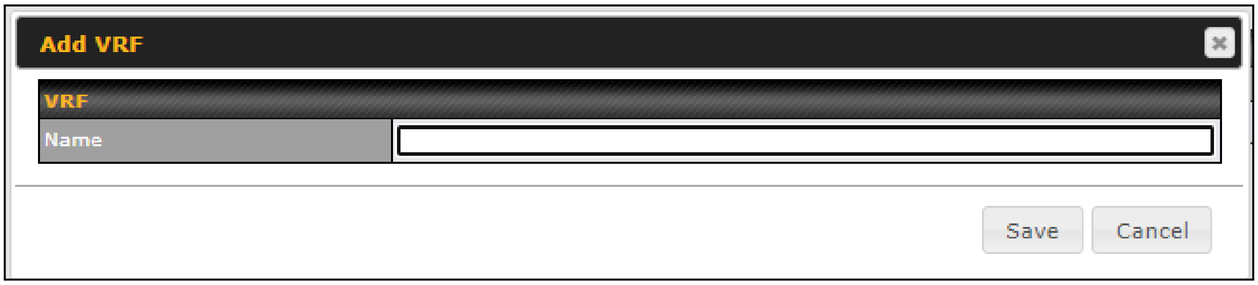
In IP-based computer networks, virtual routing and forwarding (VRF) is a technology that allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other. To configure the VRF settings, navigate to **Advanced > VRF**.



VRF

No VRF Defined

Click "**New VRF**", to create a new VRF name.



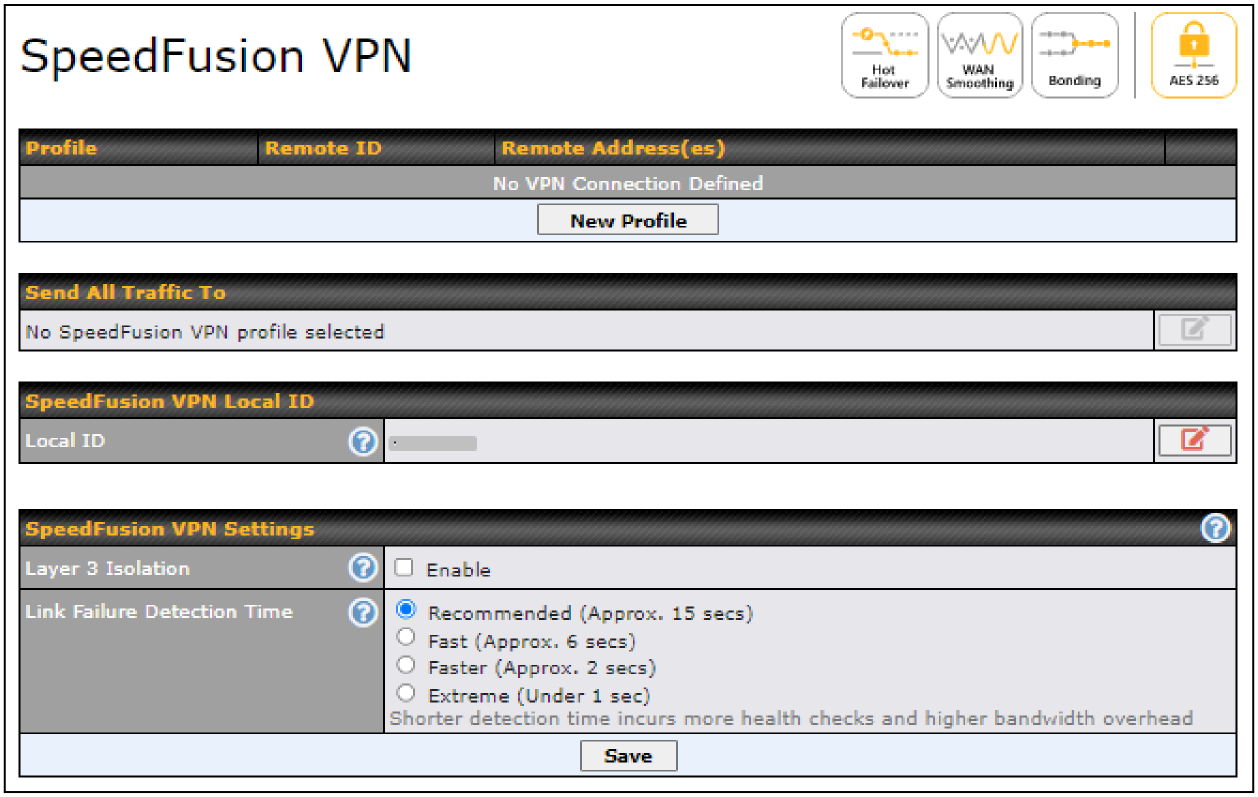
Add VRF

VRF

Name	

7.2. SpeedFusion VPN

This section will describe how to set up SpeedFusion VPN.



SpeedFusion VPN

Profile	Remote ID	Remote Address(es)
No VPN Connection Defined		

New Profile

Send All Traffic To

No SpeedFusion VPN profile selected

SpeedFusion VPN Local ID

Local ID	

SpeedFusion VPN Settings

Layer 3 Isolation	☐ Enable
Link Failure Detection Time	● Recommended (Approx. 15 secs) ○ Fast (Approx. 6 secs) ○ Faster (Approx. 2 secs) ○ Extreme (Under 1 sec) Shorter detection time incurs more health checks and higher bandwidth overhead

Save

7.2.1. Background

Peplink FusionHub securely connects one or more branch offices to your company's main datacenter or to other branches. Data, voice, and video communications between these locations are kept confidential across the public Internet.

FusionHub’s SpeedFusion Bandwidth Bonding feature, enabled by default, is specifically designed for multi-WAN environments. FusionHub can bond all WAN bandwidth for routing SpeedFusion traffic, and unless all of one site’s WAN connections are down, the Peplink FusionHub can keep your VPN up and running.

When supporting multiple VPN connections, FusionHub can act as a central hub that connects branch offices. For example, if Branch Office A and Branch Office B make VPN connections to Headquarters C, both branch office LAN subnets and the subnets behind them (e.g., static routes) will also be advertised to Headquarters C and the other branches. In this example, Branch Office A will be able to access Branch Office B via Headquarters C.

The local LAN subnet and subnets behind the LAN will be advertised to the VPN. All VPN members (branch offices and the datacenter) will be able to route to local subnets.

Note that all LAN subnets and subnets behind them must be unique. Otherwise, VPN members will not be able to access each other.

All data can be routed over the VPN using the 256-bit AES encryption standard.
In the following sections, three FusionHub application examples illustrate how to set up your devices.

7.2.2. Example One

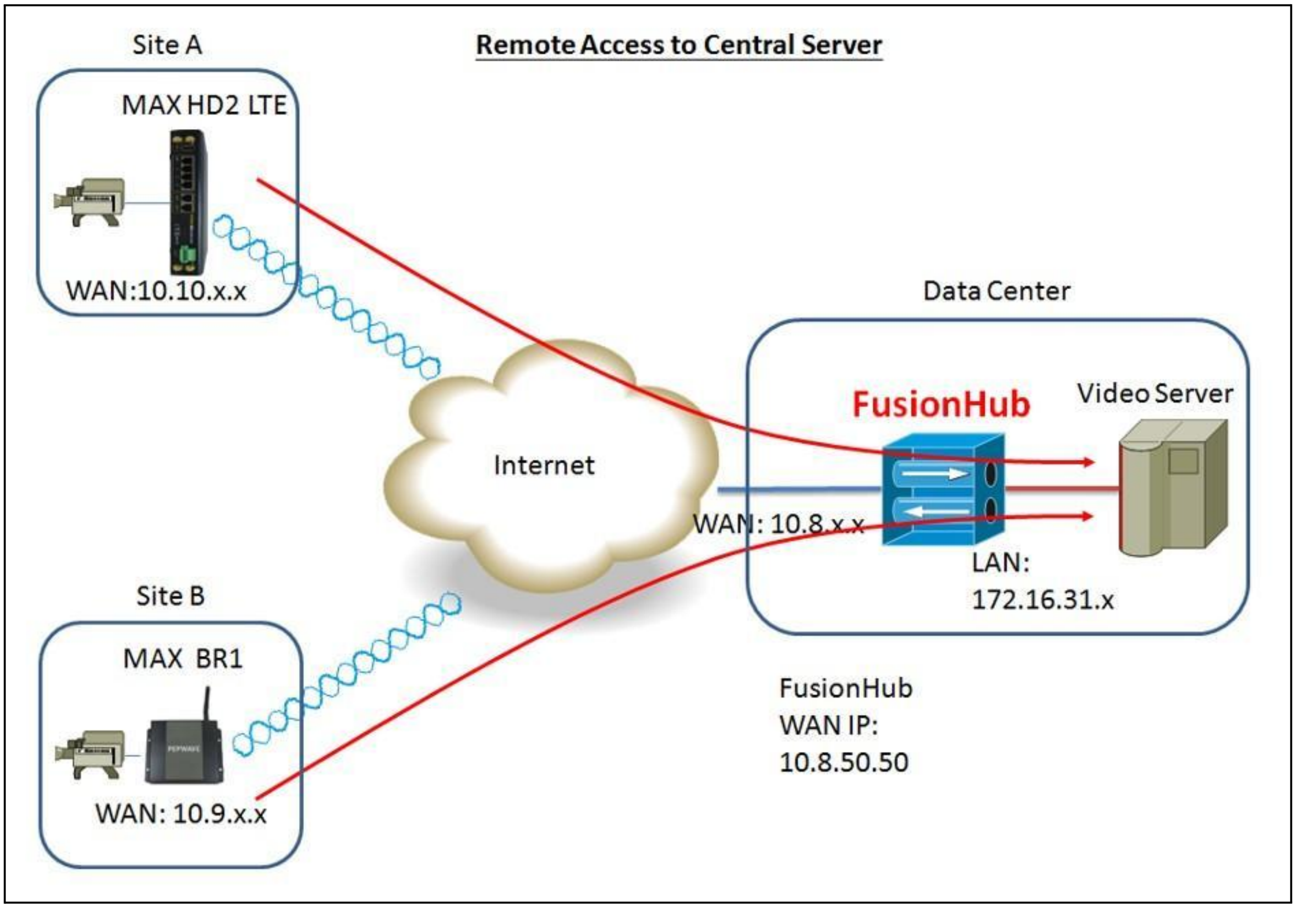


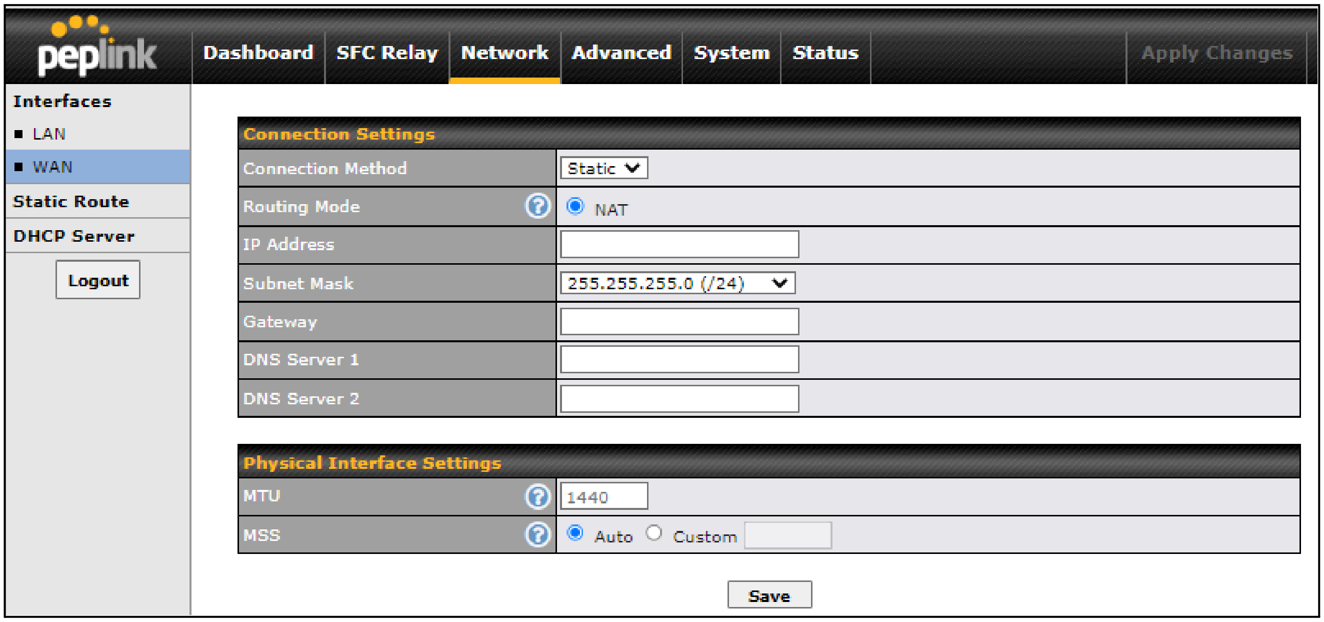
Figure 5.1 Remote Access to Central Server

To set up the scenario shown in Figure 5.1, we need to configure a MAX HD2 at Site A, a MAX BR1 at Site B, and FusionHub (two network adapters are needed) at the Datacenter.

In our case, FusionHub settings (*refer to* ***Configuration Using the Setup Wizard***) are as follows:

IP address: **10.8.50.50** (static IP)
Netmask: 255.255.0.0
Default gateway: **10.8.8.1**

Local ID: FusionHubVM



Connection Settings

Connection Method	Static
Routing Mode	● NAT
IP Address	
Subnet Mask	255.255.255.0 (/24)
Gateway	
DNS Server 1	
DNS Server 2	

Physical Interface Settings

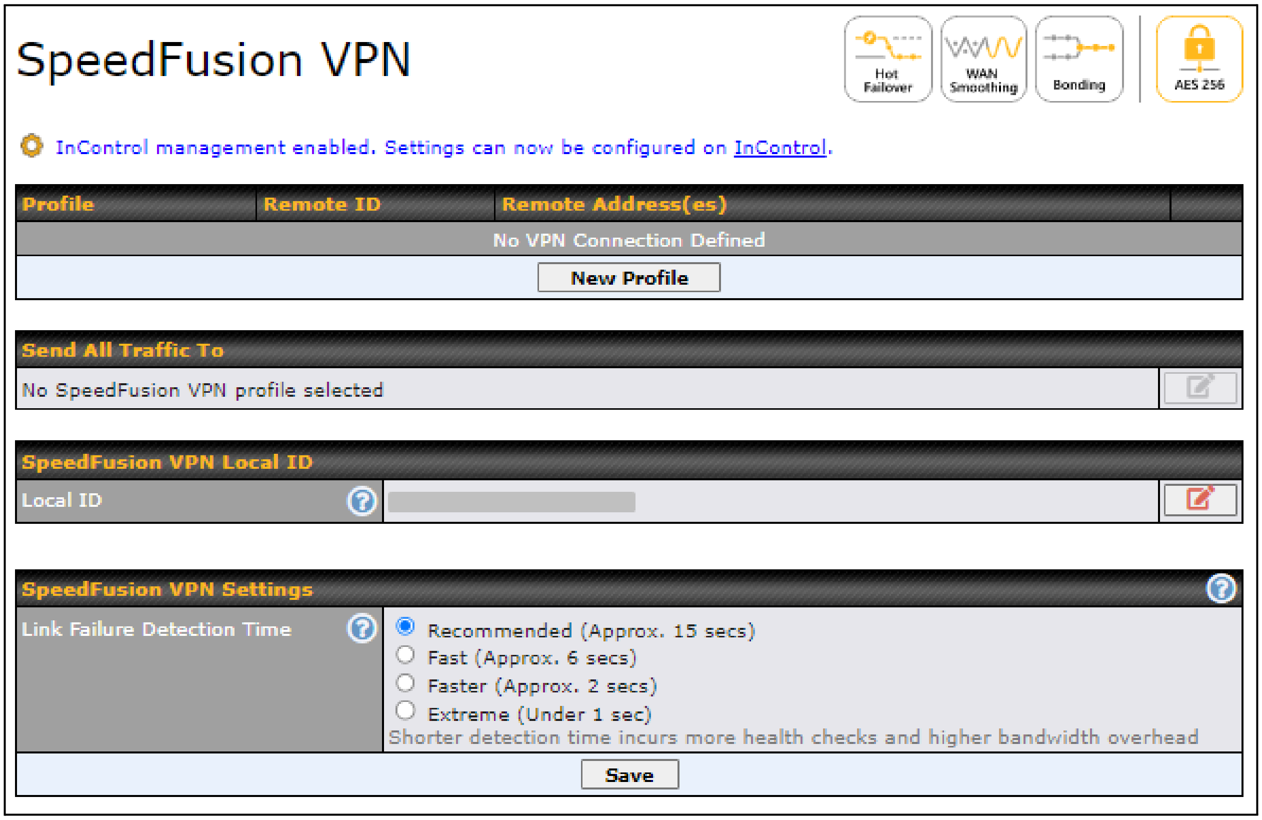
MTU	1440
MSS	● Auto ○ Custom

A. MAX HD2 LTE configuration (Site A)

Suppose that the MAX HD2 in Figure 5.1 is configured with the following IP settings:

WAN 1 IP address: **10.10.13.49**
WAN 2 IP address: **10.10.13.50**
LAN IP address: **192.168.150.1**

1. To configure, connect to the Web admin interface of the MAX HD2, and then navigate to **Advanced > SpeedFusion VPN**.



SpeedFusion VPN

InControl management enabled. Settings can now be configured on InControl.

Profile	Remote ID	Remote Address(es)	
No VPN Connection Defined			
New Profile			

Send All Traffic To

No SpeedFusion VPN profile selected

SpeedFusion VPN Local ID

Local ID	[redacted]

SpeedFusion VPN Settings

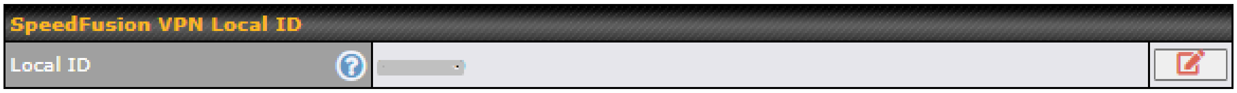
Link Failure Detection Time

- ● Recommended (Approx. 15 secs)
- ○ Fast (Approx. 6 secs)
- ○ Faster (Approx. 2 secs)
- ○ Extreme (Under 1 sec)

Shorter detection time incurs more health checks and higher bandwidth overhead

Save

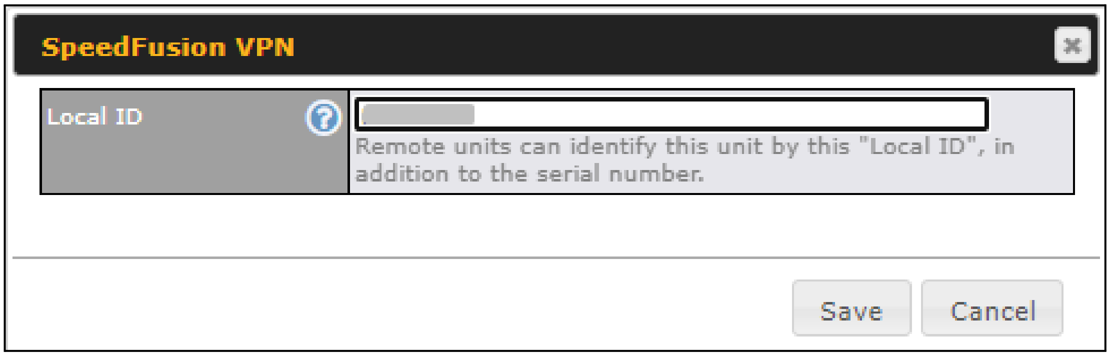
2. Next, click ✎ under **PepVPN**.



SpeedFusion VPN Local ID

Local ID	[redacted]

3. Enter a **Local ID**, such as **MAX-HD2**, for this MAX HD2, and then click **OK**.

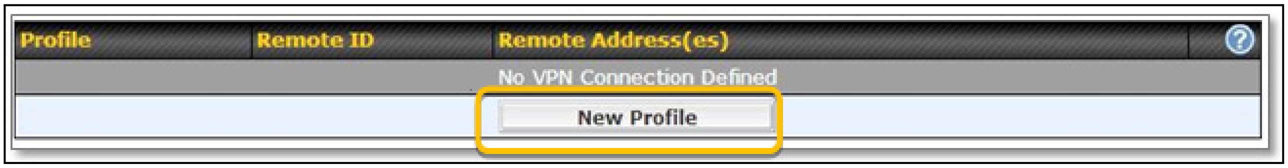


SpeedFusion VPN

Local ID	[redacted] Remote units can identify this unit by this "Local ID", in addition to the serial number.

Save Cancel

4. Click **New Profile** under **Profile** to add a new profile.



Profile	Remote ID	Remote Address(es)
No VPN Connection Defined		

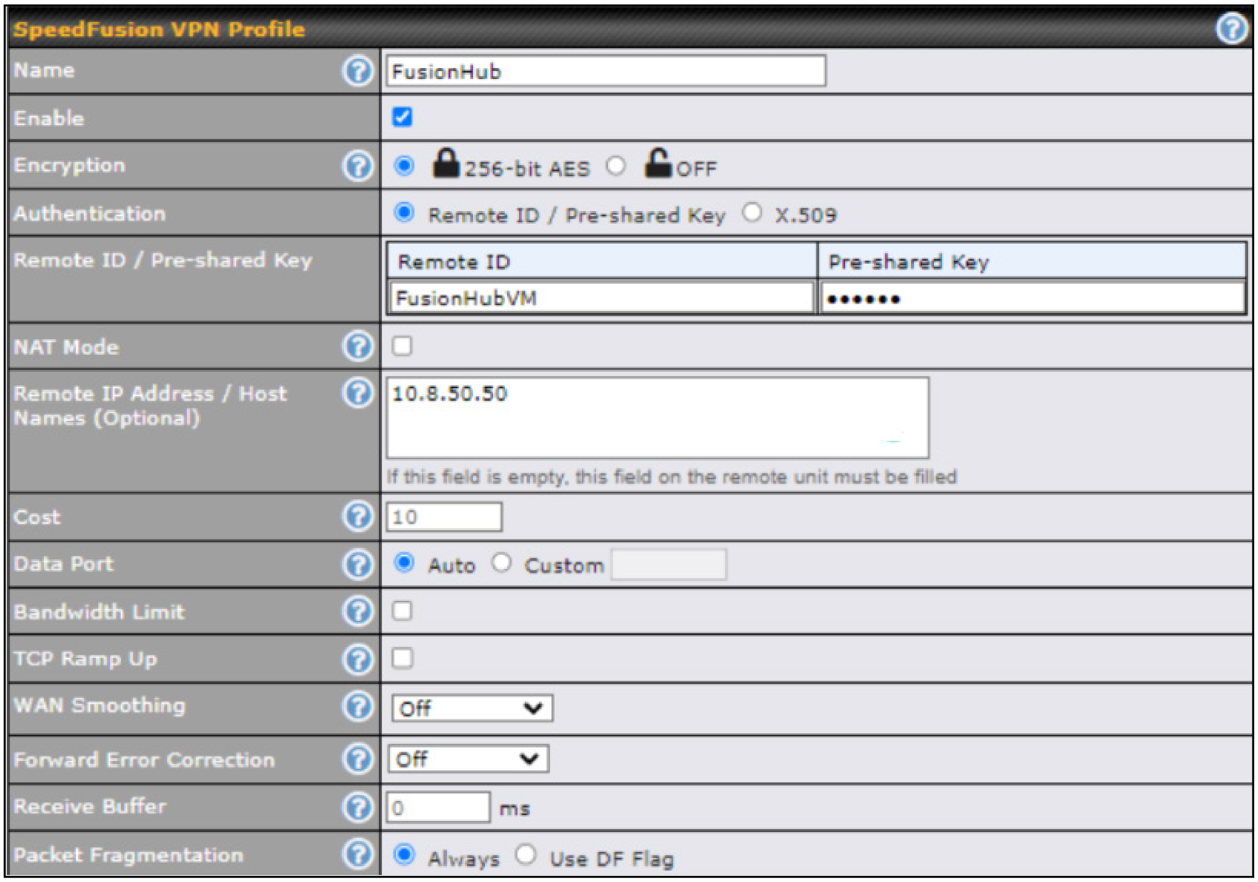
5. On the dialog displayed next, fill the form as follows:

   Name – Enter a name to represent this profile. In this case, we choose **FusionHub**.

   Remote ID – **Remote ID** should be the same as FusionHub's **Local ID**. In our case, the FusionHub local ID is **FusionHubVM**.

   Click **Preshared Key** and create a pre-shared key, which is **12345678** in our example.

   Remote IP addresses – Here, we've entered **10.8.50.50**, the FusionHub IP address.



SpeedFusion VPN Profile

Name	FusionHub
Enable	☑
Encryption	● 256-bit AES ○ OFF
Authentication	● Remote ID / Pre-shared Key ○ X.509
Remote ID / Pre-shared Key	Remote ID: FusionHubVM Pre-shared Key: ••••••
NAT Mode	□
Remote IP Address / Host Names (Optional)	10.8.50.50 If this field is empty, this field on the remote unit must be filled
Cost	10
Data Port	● Auto ○ Custom
Bandwidth Limit	□
TCP Ramp Up	□
WAN Smoothing	Off
Forward Error Correction	Off
Receive Buffer	0 ms
Packet Fragmentation	● Always ○ Use DF Flag

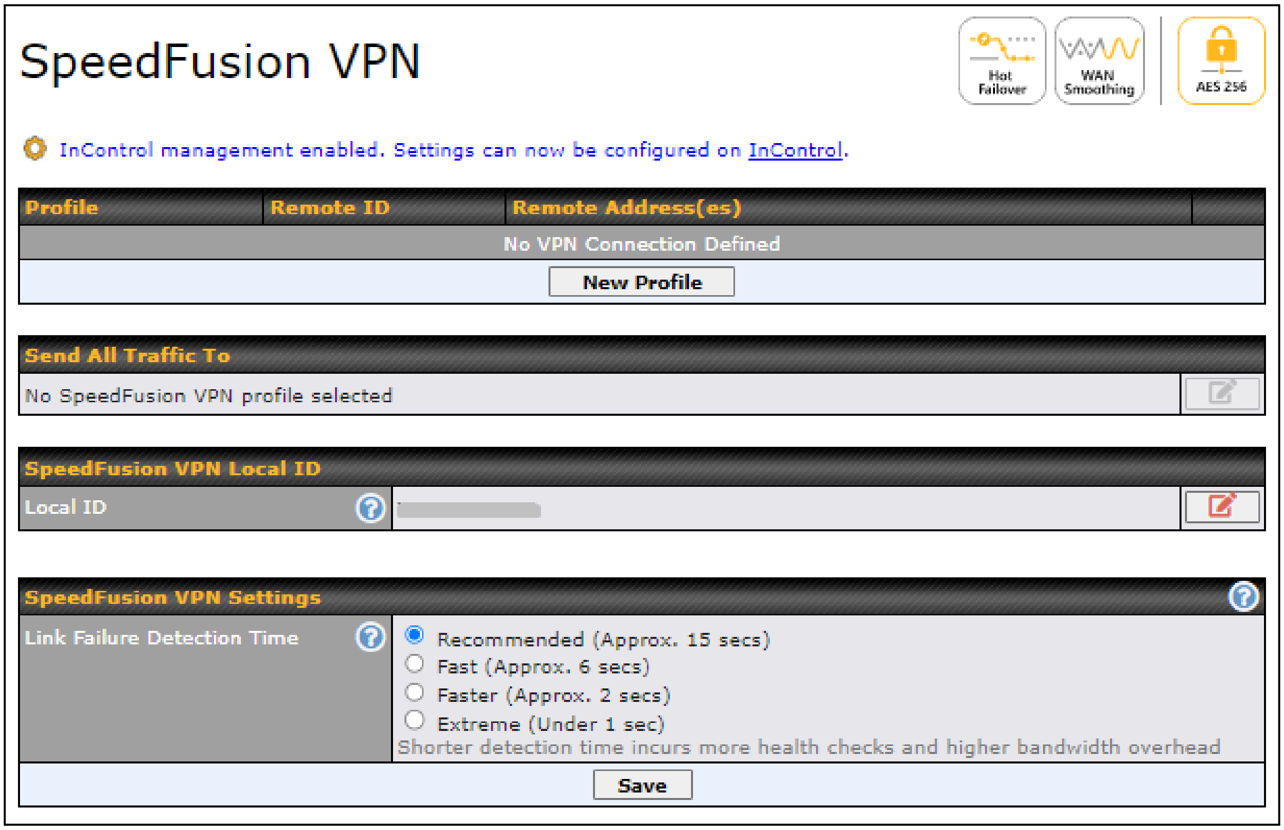
6. After completing the form, click **Save** and then **Apply Changes**.

B. MAX BR1 configuration (Site B)

Assume the MAX BR1's IP settings are:

WAN IP address: **10.9.3.167**
LAN IP address: **192.168.71.1**

1. To configure the MAX BR1, connect to the MAX BR1's Web admin interface (in our case, the Web admin interface address is **http://192.168.71.1**), and then navigate to **Advanced > SpeedFusion VPN**.



SpeedFusion VPN

InControl management enabled. Settings can now be configured on InControl.

Profile	Remote ID	Remote Address(es)	
No VPN Connection Defined			
New Profile			

Send All Traffic To

No SpeedFusion VPN profile selected

SpeedFusion VPN Local ID

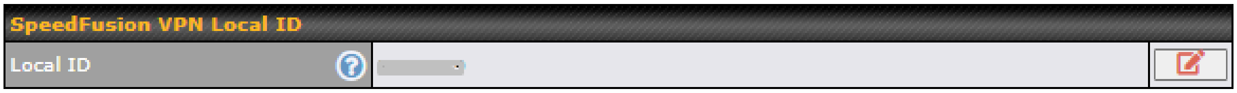
Local ID	[redacted]

SpeedFusion VPN Settings

Link Failure Detection Time	● Recommended (Approx. 15 secs) ○ Fast (Approx. 6 secs) ○ Faster (Approx. 2 secs) ○ Extreme (Under 1 sec) Shorter detection time incurs more health checks and higher bandwidth overhead

Save

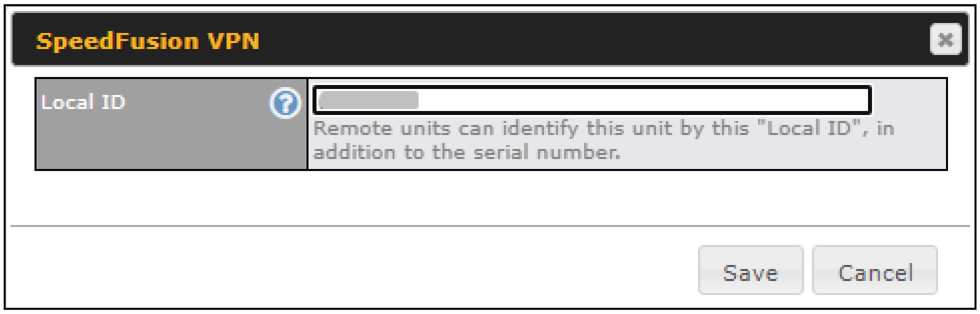
2. Click ✎ under **SpeedFusion VPN Local ID**.



SpeedFusion VPN Local ID

Local ID	[redacted]

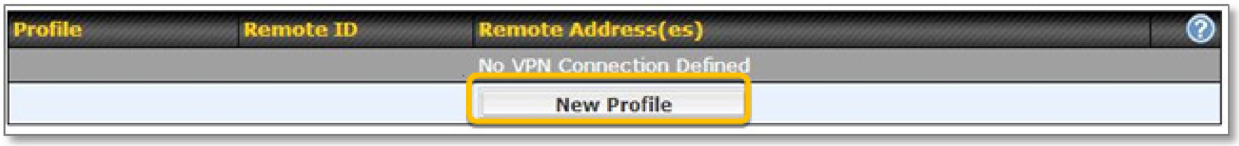
3. Enter a **Local ID**, such as **MAX_BR1_169B**, for this MAX BR1, and then click **OK.**



SpeedFusion VPN

Local ID	Remote units can identify this unit by this "Local ID", in addition to the serial number.

4. Click **New Profile** under **Profile** to add a new profile.



Profile	Remote ID	Remote Address(es)
No VPN Connection Defined		

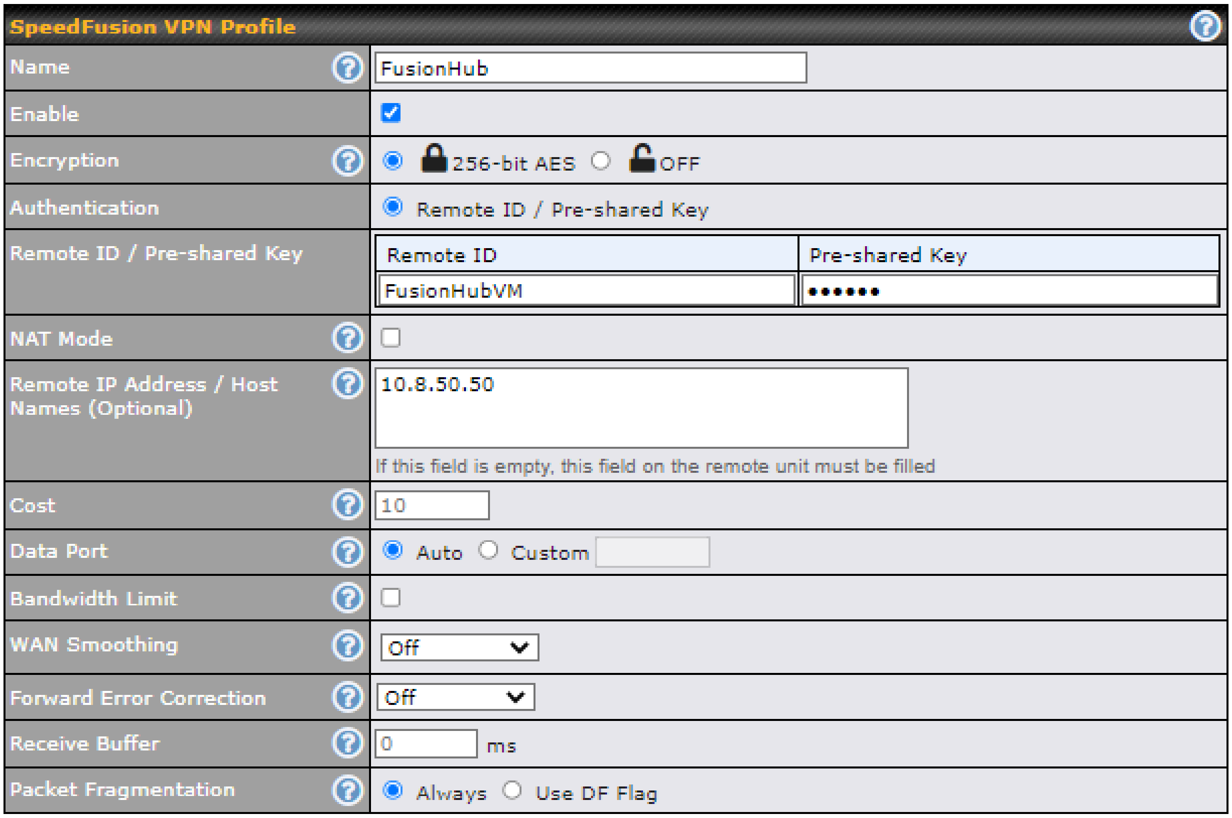
5. On the dialog displayed next, fill the form as follows:

   Name – Enter a name to represent this profile. In this case, we chose **FusionHub**.

   Remote ID – **Remote ID** should be the same as FusionHub's **Local ID**. In our case, the FusionHub local ID is **FusionHubVM**.

   Click **Preshared Key** and create a pre-shared key, which is **23456789** in our example.

   Remote IP addresses – Here, we've entered **10.8.50.50**, the FusionHub IP address.



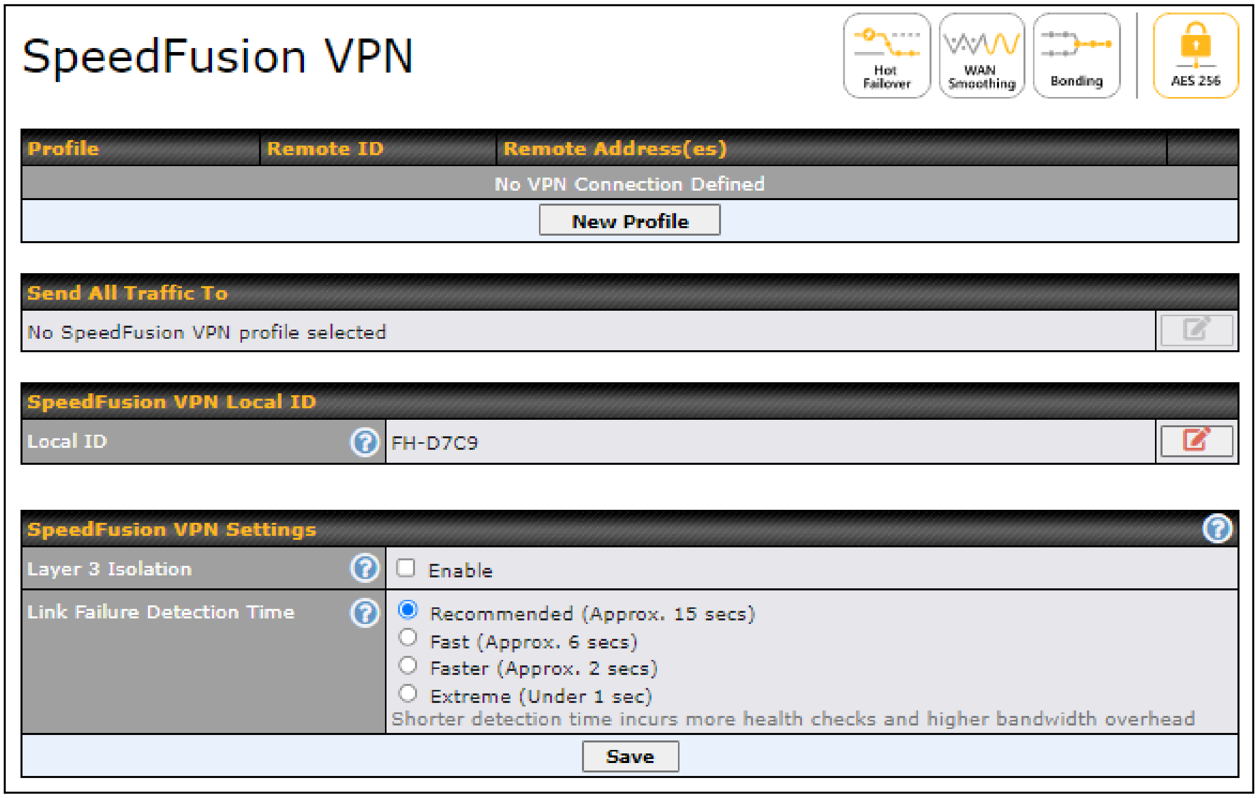
SpeedFusion VPN Profile	
Name	FusionHub
Enable	☑
Encryption	● 256-bit AES ○ OFF
Authentication	● Remote ID / Pre-shared Key
Remote ID / Pre-shared Key	Remote ID: FusionHubVM Pre-shared Key: ••••••
NAT Mode	□
Remote IP Address / Host Names (Optional)	10.8.50.50 If this field is empty, this field on the remote unit must be filled
Cost	10
Data Port	● Auto ○ Custom
Bandwidth Limit	□
WAN Smoothing	Off
Forward Error Correction	Off
Receive Buffer	0 ms
Packet Fragmentation	● Always ○ Use DF Flag

6. After completing the form, click **Save** and then **Apply Changes**.

C. FusionHub configuration (DataCenter)

In our example, the IP address of the ESXi server is **10.8.9.24/16**, and the FusionHub IP address is **10.8.50.50/16**.

1. To configure FusionHub, connect to the FusionHub Web admin interface (**http://10.8.50.50**) again. Then, navigate to **Advanced > SpeedFusion VPN**.



SpeedFusion VPN

Profile	Remote ID	Remote Address(es)
No VPN Connection Defined		

Send All Traffic To

No SpeedFusion VPN profile selected

SpeedFusion VPN Local ID

Local ID	FH-D7C9

SpeedFusion VPN Settings

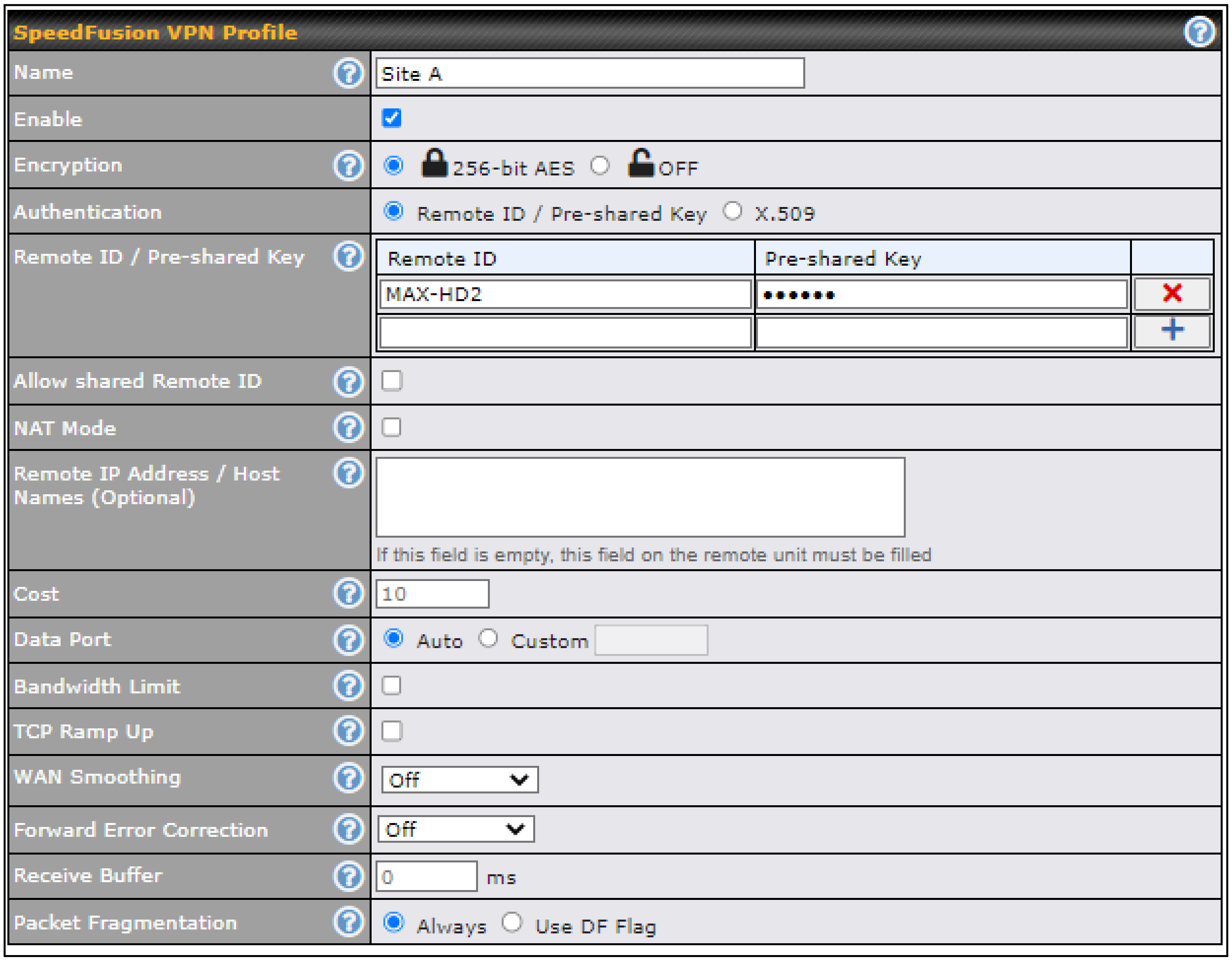
Layer 3 Isolation	□ Enable
Link Failure Detection Time	● Recommended (Approx. 15 secs) ○ Fast (Approx. 6 secs) ○ Faster (Approx. 2 secs) ○ Extreme (Under 1 sec) Shorter detection time incurs more health checks and higher bandwidth overhead

2. To add a new profile, click the **New Profile** button. On the dialog displayed next, fill the form as follows:

   Name – Enter a name to represent this profile. In this case, since we're adding the MAX HD2 to Site A, we chose **Site A**.

   Remote ID – **Remote ID** should be the same as the MAX HD2's **Local ID**. In our case, the MAX HD2's local ID is **MAX-HD2**.

   Click **Preshared Key**, and then enter the same pre-shared key used with the MAX HD2, **12345678** in our example.



SpeedFusion VPN Profile

Name	Site A
Enable	☑
Encryption	● 256-bit AES ○ OFF
Authentication	● Remote ID / Pre-shared Key ○ X.509
Remote ID / Pre-shared Key	Remote ID: MAX-HD2 Pre-shared Key: •••••• ✕ +
Allow shared Remote ID	□
NAT Mode	□
Remote IP Address / Host Names (Optional)	If this field is empty, this field on the remote unit must be filled
Cost	10
Data Port	● Auto ○ Custom
Bandwidth Limit	□
TCP Ramp Up	□
WAN Smoothing	Off
Forward Error Correction	Off
Receive Buffer	0 ms
Packet Fragmentation	● Always ○ Use DF Flag

3. After completing the form, click **Save** and then **Apply Changes**.

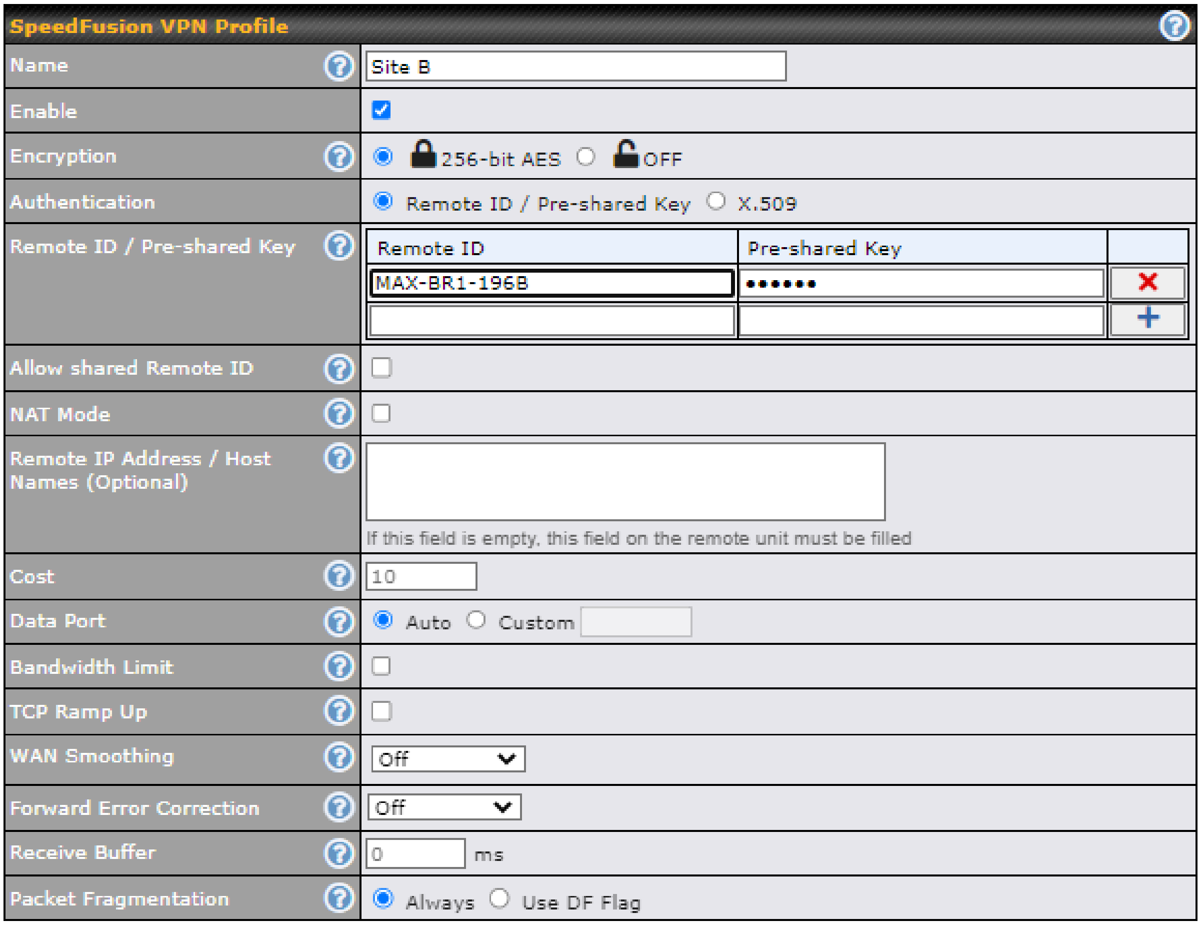
4. Click **New Profile** again to add the MAX BR1 to Site B.

   Name – Enter a name to represent this profile. In this case, since we're adding the MAX BR1 to Site B, we chose **Site B**.

   Remote ID – **Remote ID** should be the same as the MAX BR1's **Local ID**. In our case, the local ID is **MAX-BR1-169B**.

   Click **Preshared Key** and enter the same pre-shared key used with the MAX BR1, **23456789** in our example.

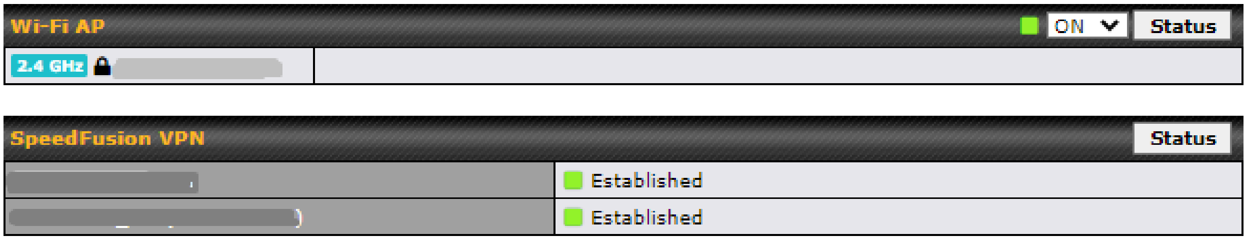
5. After completing the form, click **Save** and then **Apply Changes**.



SpeedFusion VPN Profile

Name	Site B
Enable	☑
Encryption	● 256-bit AES ○ OFF
Authentication	● Remote ID / Pre-shared Key ○ X.509
Remote ID / Pre-shared Key	Remote ID: MAX-BR1-196B Pre-shared Key: ••••••
Allow shared Remote ID	□
NAT Mode	□
Remote IP Address / Host Names (Optional)	If this field is empty, this field on the remote unit must be filled
Cost	10
Data Port	● Auto ○ Custom
Bandwidth Limit	□
TCP Ramp Up	□
WAN Smoothing	Off
Forward Error Correction	Off
Receive Buffer	0 ms
Packet Fragmentation	● Always ○ Use DF Flag

6. On the **Dashboard**, we see that SpeedFusion VPN has been established for Site A and B.



[redacted]

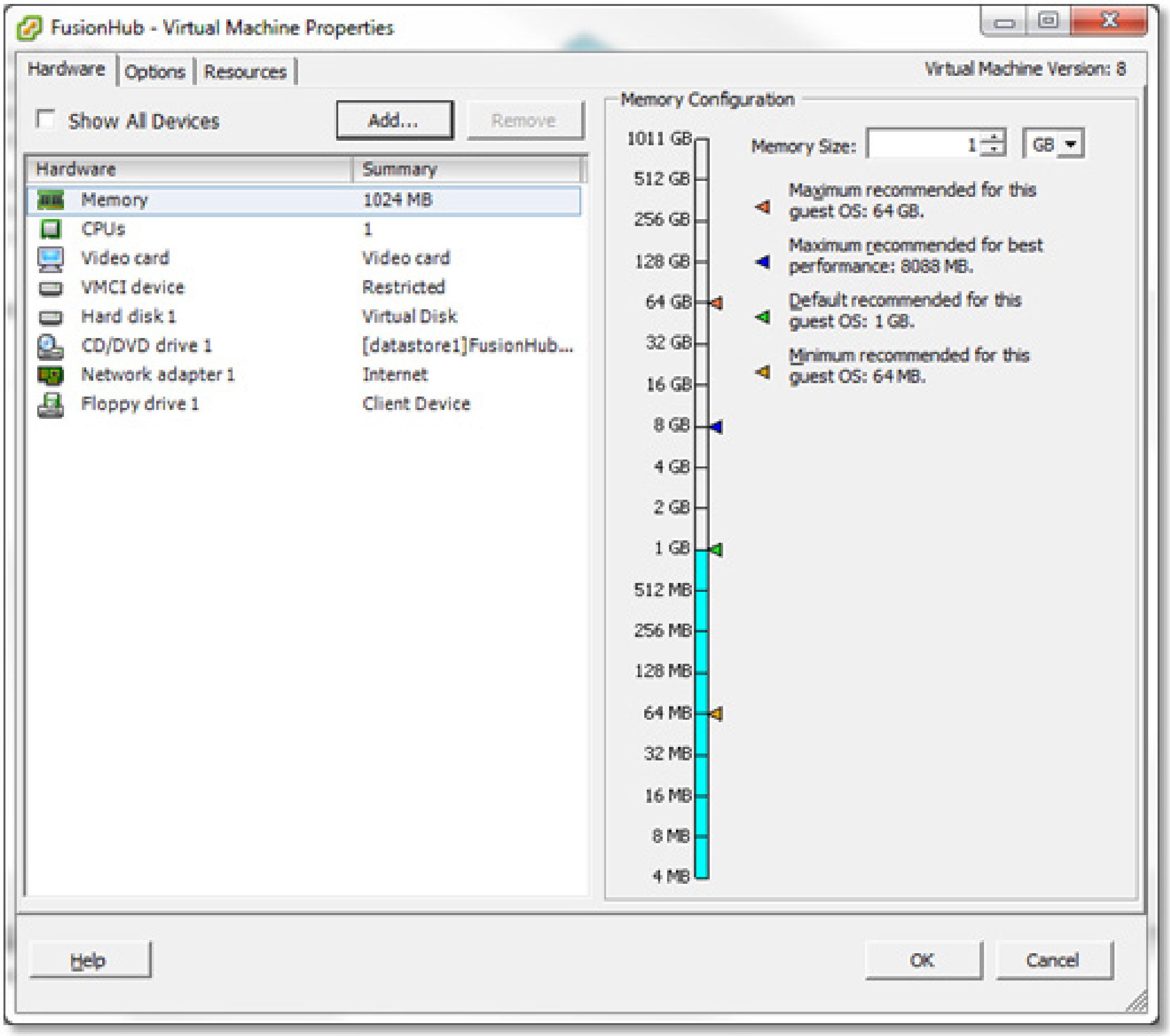
SpeedFusion VPN

[redacted]	🟩 Established
[redacted]	🟩 Established

7. In order to make a direct link between FusionHub and the video server shown on the right-hand side of Figure 5.1, we need to add one more port (a network adapter) to FusionHub's virtual machine.

Adding a network adapter when using ESXi server

a. Login to the ESXi server again, and then power off the FusionHub virtual machine. Next, click **Edit virtual machine settings**. On the **FusionHub – Virtual Machine Properties** dialog, click **Add** to add another network adapter.



FusionHub - Virtual Machine Properties

Virtual Machine Version: 8

□ Show All Devices

Hardware	Summary
Memory	1024 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
Hard disk 1	Virtual Disk
CD/DVD drive 1	[datastore1]FusionHub...
Network adapter 1	Internet
Floppy drive 1	Client Device

Memory Configuration

Memory Size: 1 GB

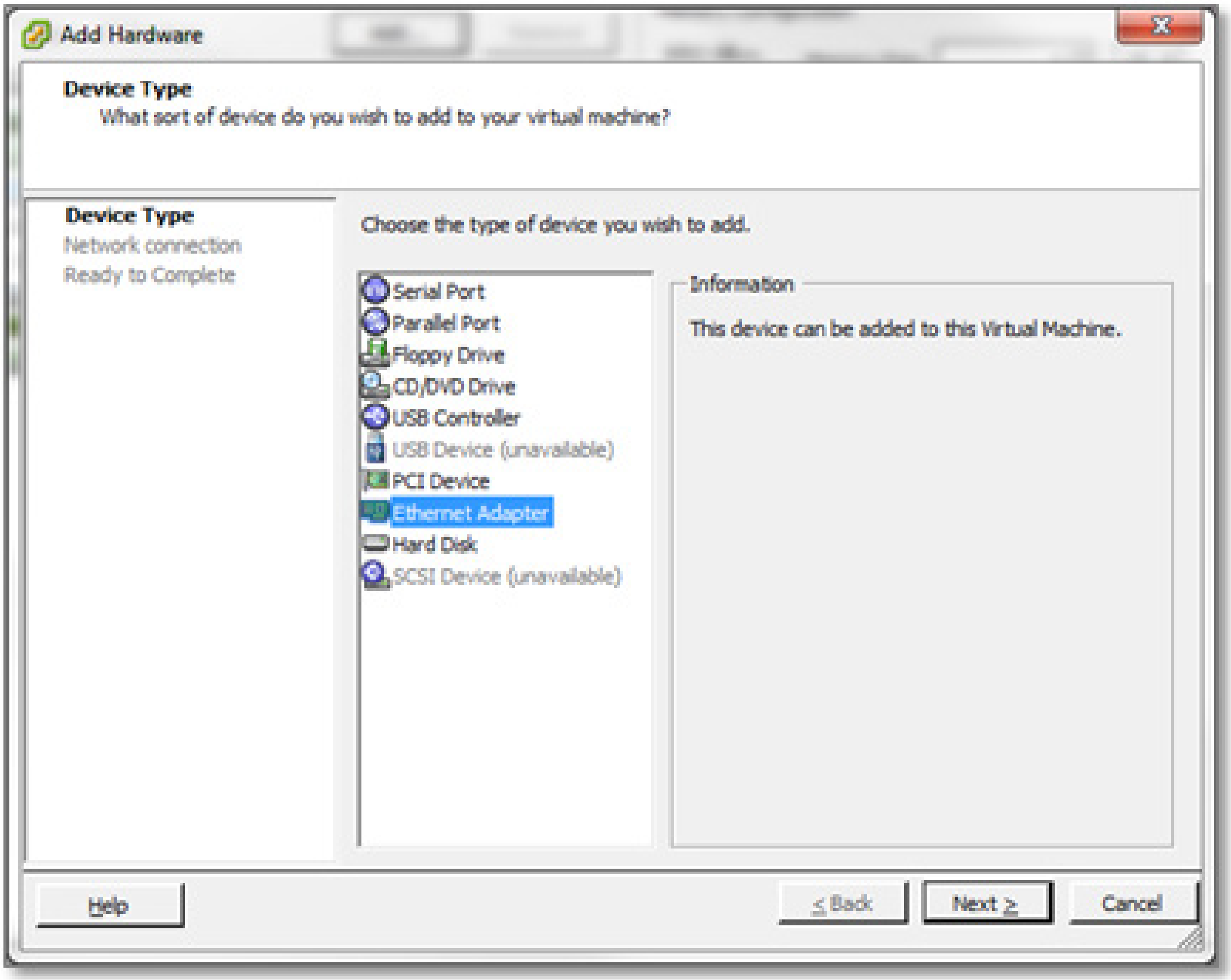
Maximum recommended for this guest OS: 64 GB.

Maximum recommended for best performance: 8088 MB.

Default recommended for this guest OS: 1 GB.

Minimum recommended for this guest OS: 64 MB.

b. Select **Ethernet Adapter**, and then click **Next.**



Add Hardware

Device Type

What sort of device do you wish to add to your virtual machine?

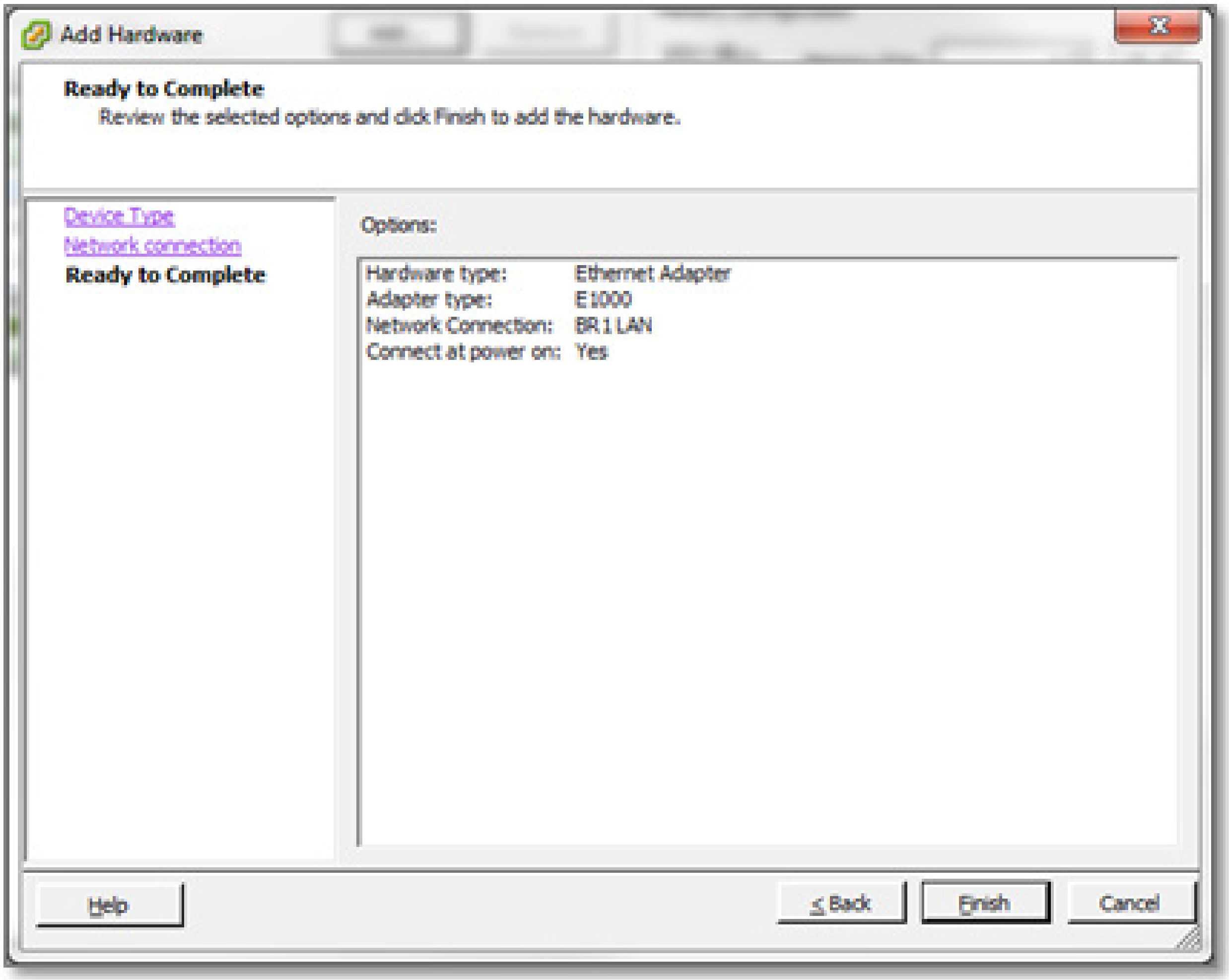
Choose the type of device you wish to add.

- Serial Port
- Parallel Port
- Floppy Drive
- CD/DVD Drive
- USB Controller
- USB Device (unavailable)
- PCI Device
- Ethernet Adapter
- Hard Disk
- SCSI Device (unavailable)

Information

This device can be added to this Virtual Machine.

c. Select a network and adapter from the drop-down menus, and then click **Next**.

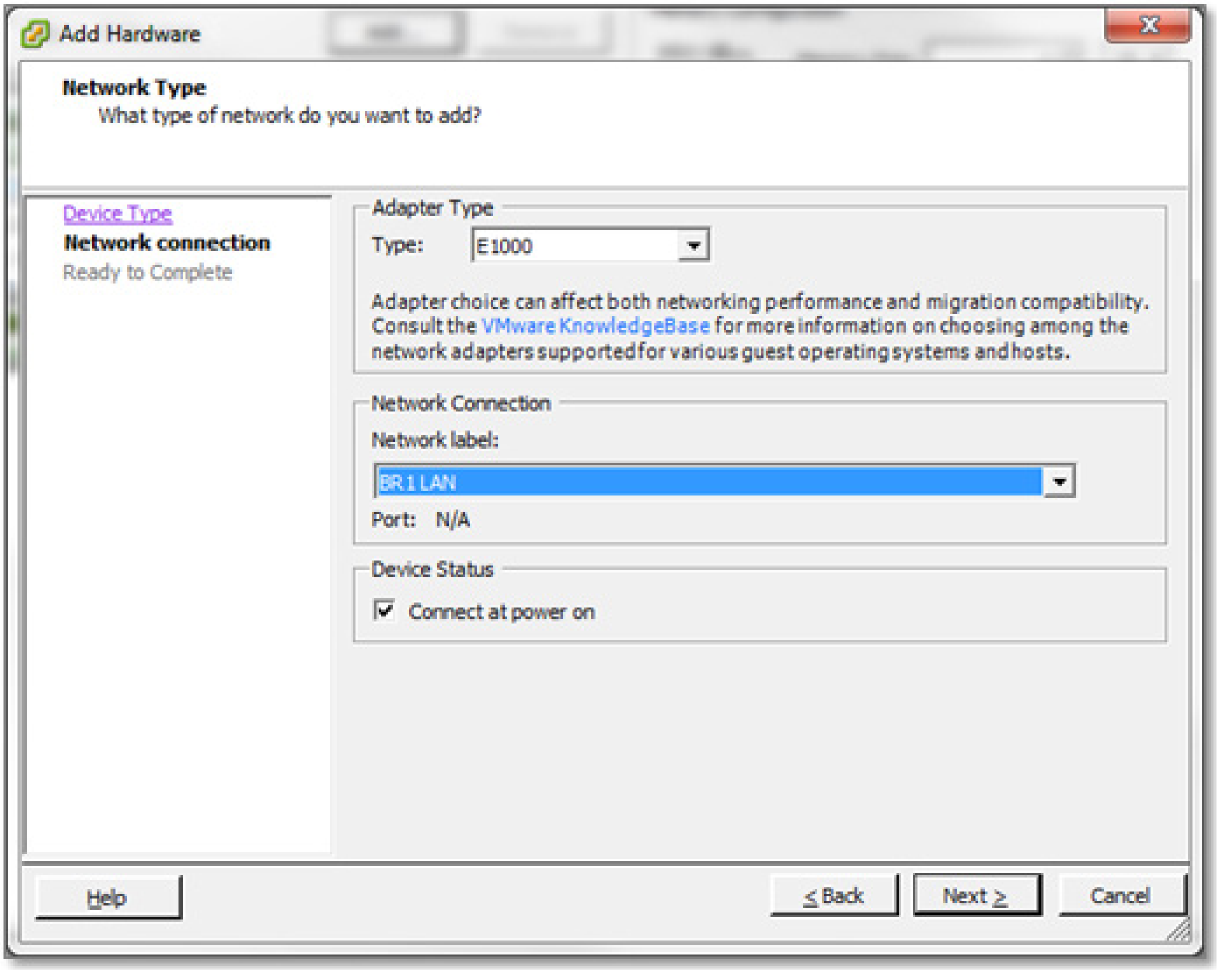


Ready to Complete
Review the selected options and click Finish to add the hardware.

Options:

Hardware type: Ethernet Adapter
Adapter type: E1000
Network Connection: BR1 LAN
Connect at power on: Yes

d. Click **Finish** and then **OK** to save your settings.



Add Hardware

Network Type

What type of network do you want to add?

Adapter Type

Type: E1000

Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapters supported for various guest operating systems and hosts.

Network Connection

Network label: BR1 LAN

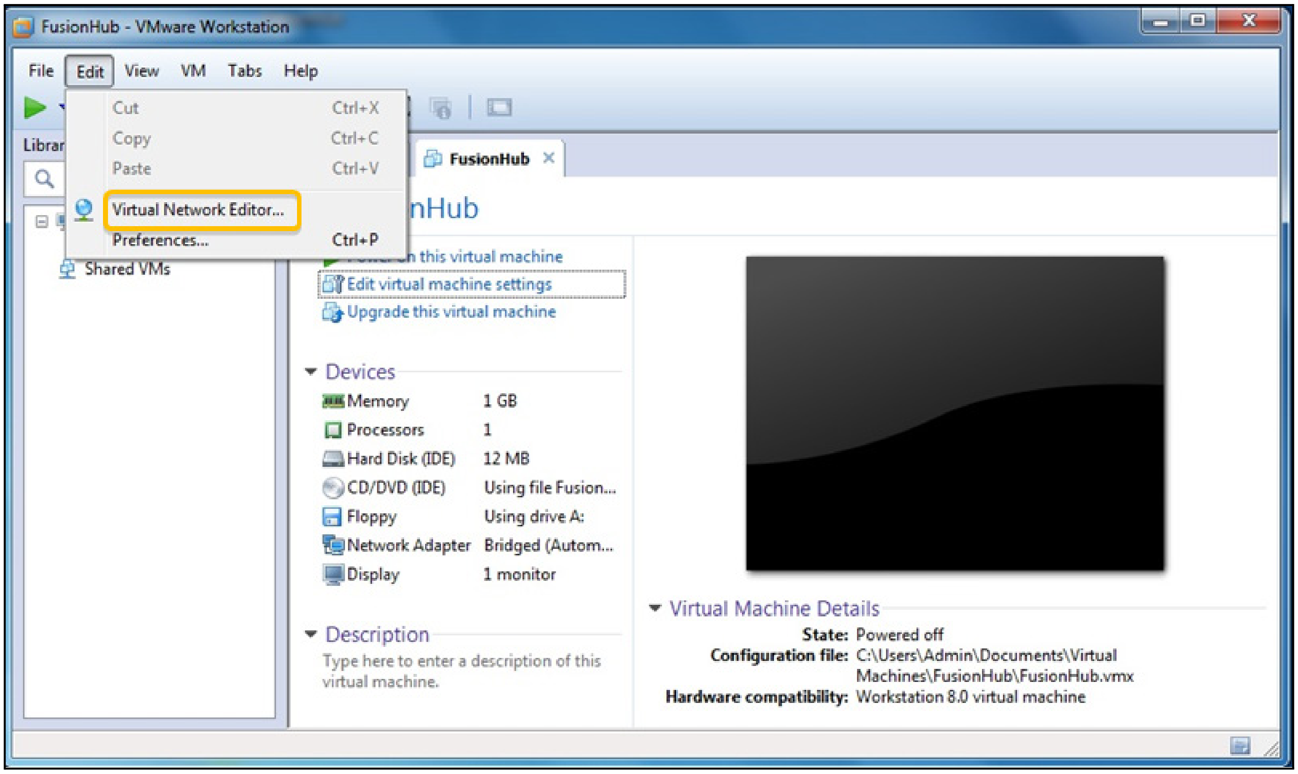
Port: N/A

Device Status

☑ Connect at power on

Adding a network adapter when using VMware Workstation

a. Power off the FusionHub virtual machine and select **Edit > Virtual Network Editor**

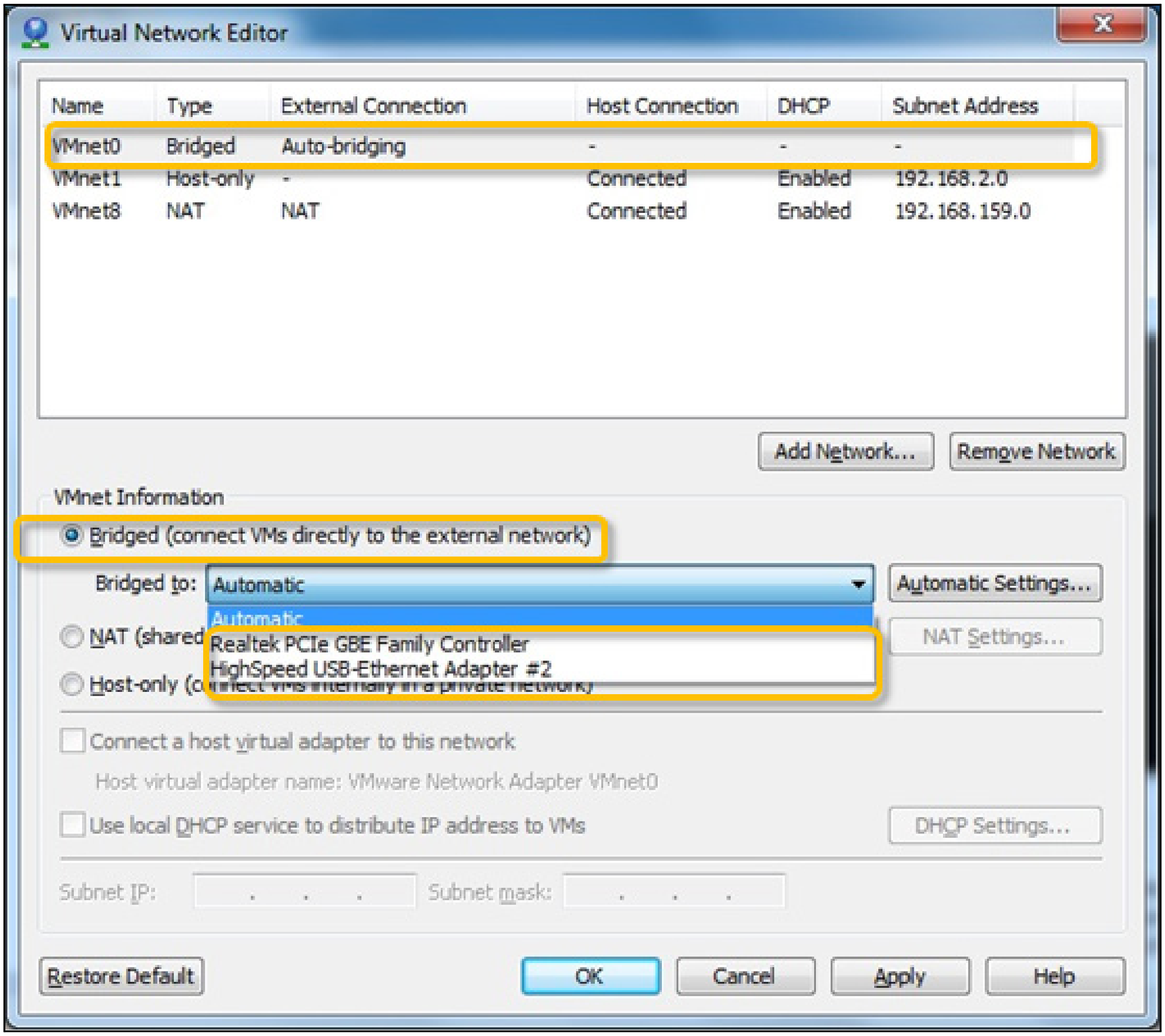


Memory	1 GB
Processors	1
Hard Disk (IDE)	12 MB
CD/DVD (IDE)	Using file Fusion...
Floppy	Using drive A:
Network Adapter	Bridged (Autom...
Display	1 monitor

Type here to enter a description of this virtual machine.

State: Powered off
Configuration file: C:\Users\Admin\Documents\Virtual Machines\FusionHub\FusionHub.vmx
Hardware compatibility: Workstation 8.0 virtual machine

b. Under VMnet Information, select **VMnet0** and check **Bridged (connect VMs directly to the external network)**. Select the appropriate network adapter from the drop-down menu and click **OK**.



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.2.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.159.0

VMnet Information

● Bridged (connect VMs directly to the external network)

Bridged to: Automatic

Automatic
Realtek PCIe GBE Family Controller
HighSpeed USB-Ethernet Adapter #2

○ NAT (shared

○ Host-only (connect VMs internally in a private network)

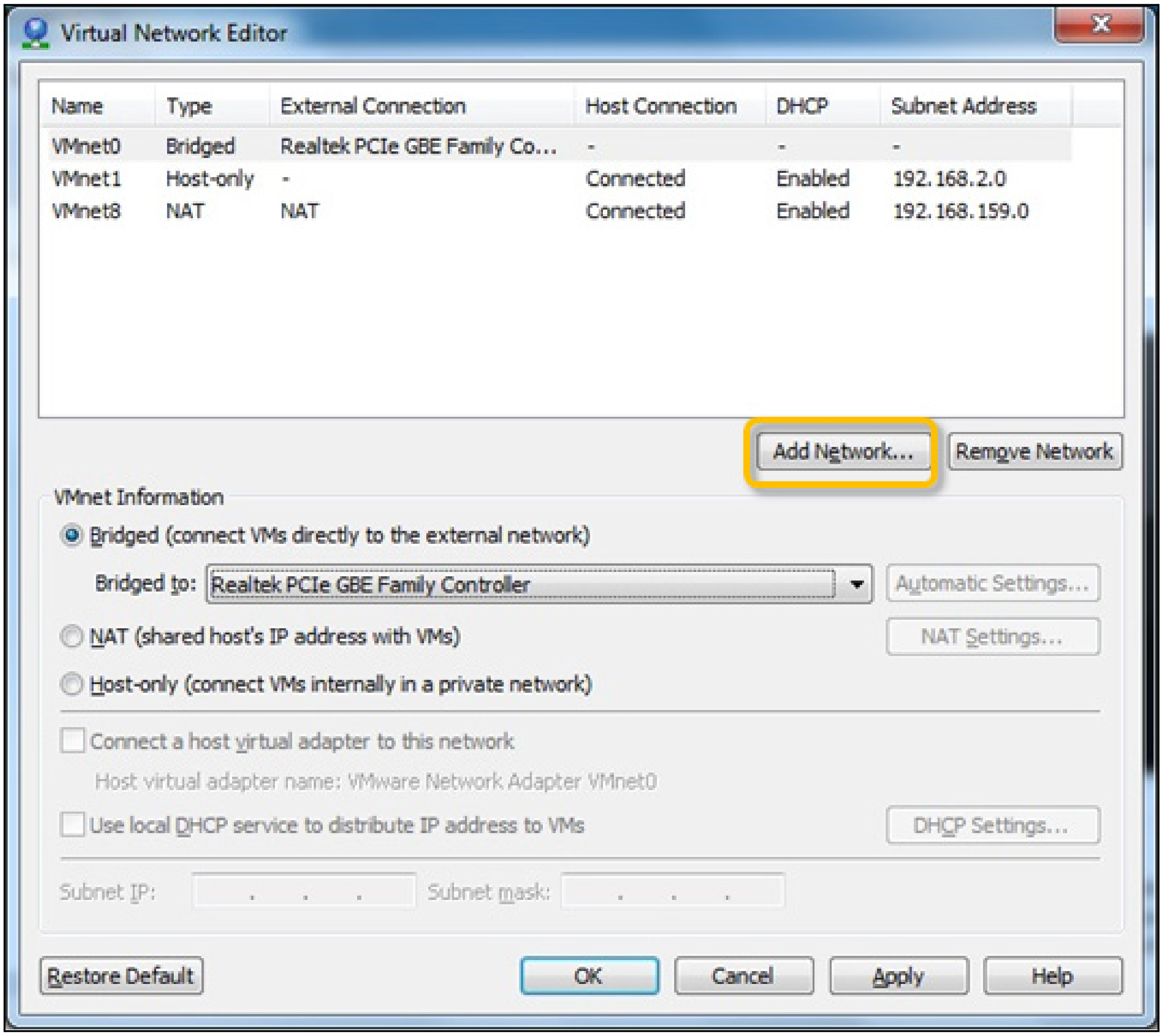
□ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet0

□ Use local DHCP service to distribute IP address to VMs

Subnet IP: . . . Subnet mask: . . .

c. Click Add **Network**.



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Realtek PCIe GBE Family Co...	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.2.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.159.0

VMnet Information

● Bridged (connect VMs directly to the external network)

Bridged to: Realtek PCIe GBE Family Controller

○ NAT (shared host's IP address with VMs)

○ Host-only (connect VMs internally in a private network)

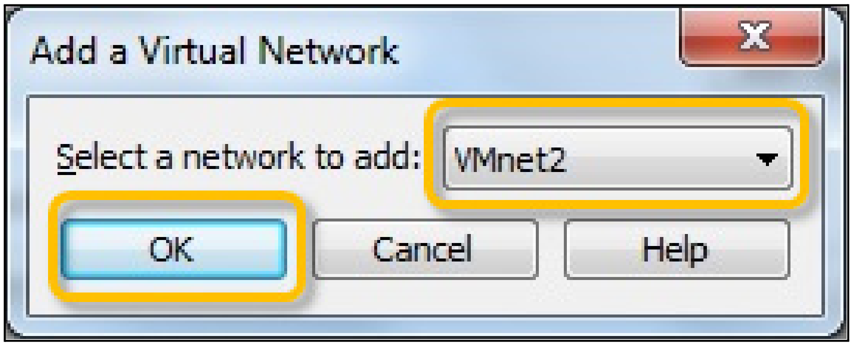
□ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet0

□ Use local DHCP service to distribute IP address to VMs

Subnet IP: . . .   Subnet mask: . . .

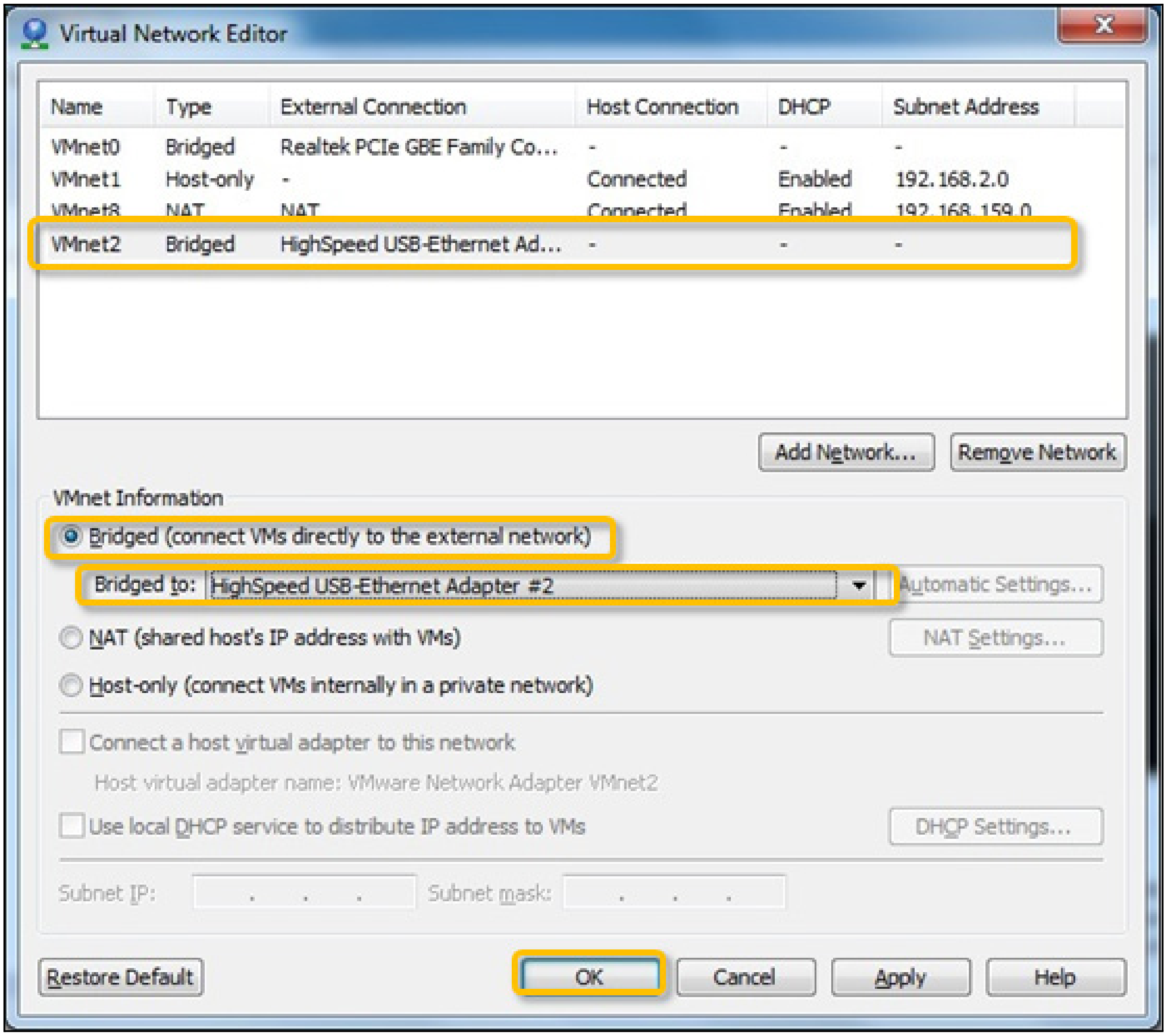
d. On the **Add a Virtual Network** dialog, select a network to add from the drop-down menu and click OK. In this example, we selected **VMnet2.**



Add a Virtual Network

Select a network to add: VMnet2

e. Select the **VMnet2** network added in the previous step and check **Bridged (connect VMs directly to the external network)**. Click **OK** to apply changes.



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Realtek PCIe GBE Family Co...	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.2.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.159.0
VMnet2	Bridged	HighSpeed USB-Ethernet Ad...	-	-	-

VMnet Information

● Bridged (connect VMs directly to the external network)

Bridged to: HighSpeed USB-Ethernet Adapter #2

○ NAT (shared host's IP address with VMs)

○ Host-only (connect VMs internally in a private network)

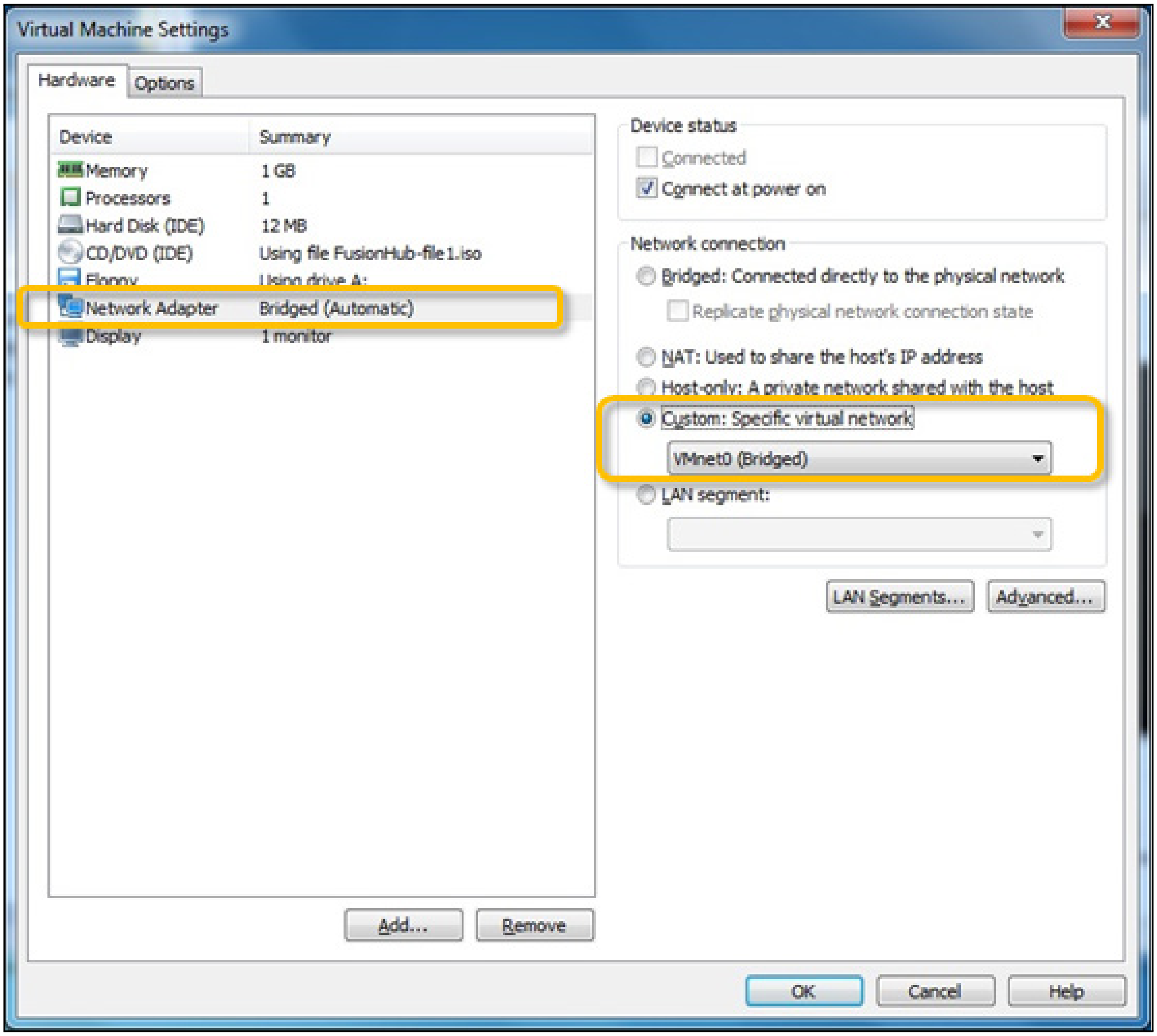
□ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet2

□ Use local DHCP service to distribute IP address to VMs

Subnet IP: . . .   Subnet mask: . . .

f. Click FusionHub and select Edit virtual machine settings. On the Virtual Machine Settings dialog, select Network adapter. Check Custom: Specific virtual network and select VMnet0 (Bridged). Then click Add to add another network adapter.



Virtual Machine Settings

Device	Summary
Memory	1 GB
Processors	1
Hard Disk (IDE)	12 MB
CD/DVD (IDE)	Using file FusionHub-file1.iso
Floppy	Using drive A:
Network Adapter	Bridged (Automatic)
Display	1 monitor

Device status

□ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

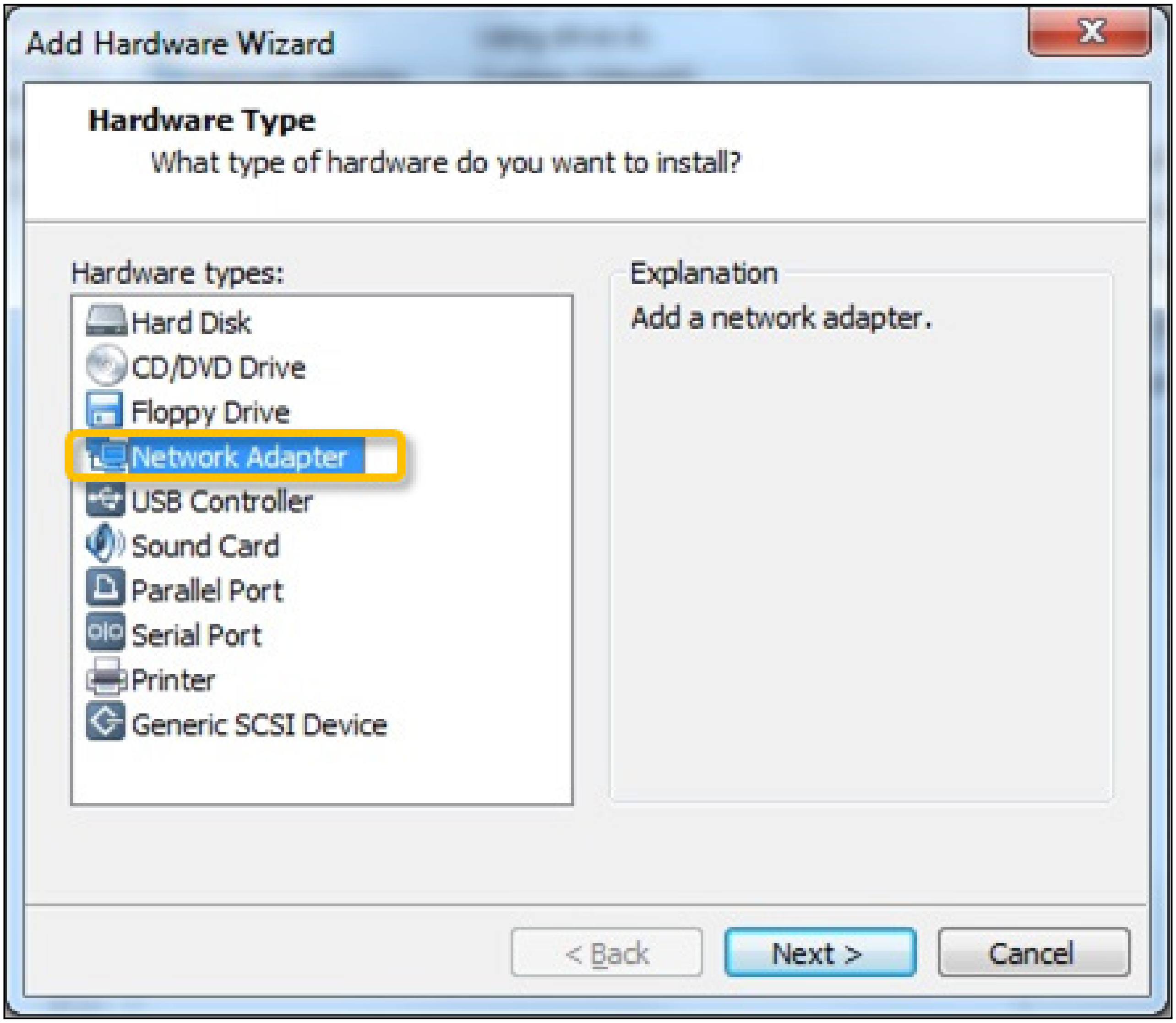
○ Host-only: A private network shared with the host

● Custom: Specific virtual network

VMnet0 (Bridged)

○ LAN segment:

g. Select **Network Adapter** and click **Next**.



Add Hardware Wizard

Hardware Type

What type of hardware do you want to install?

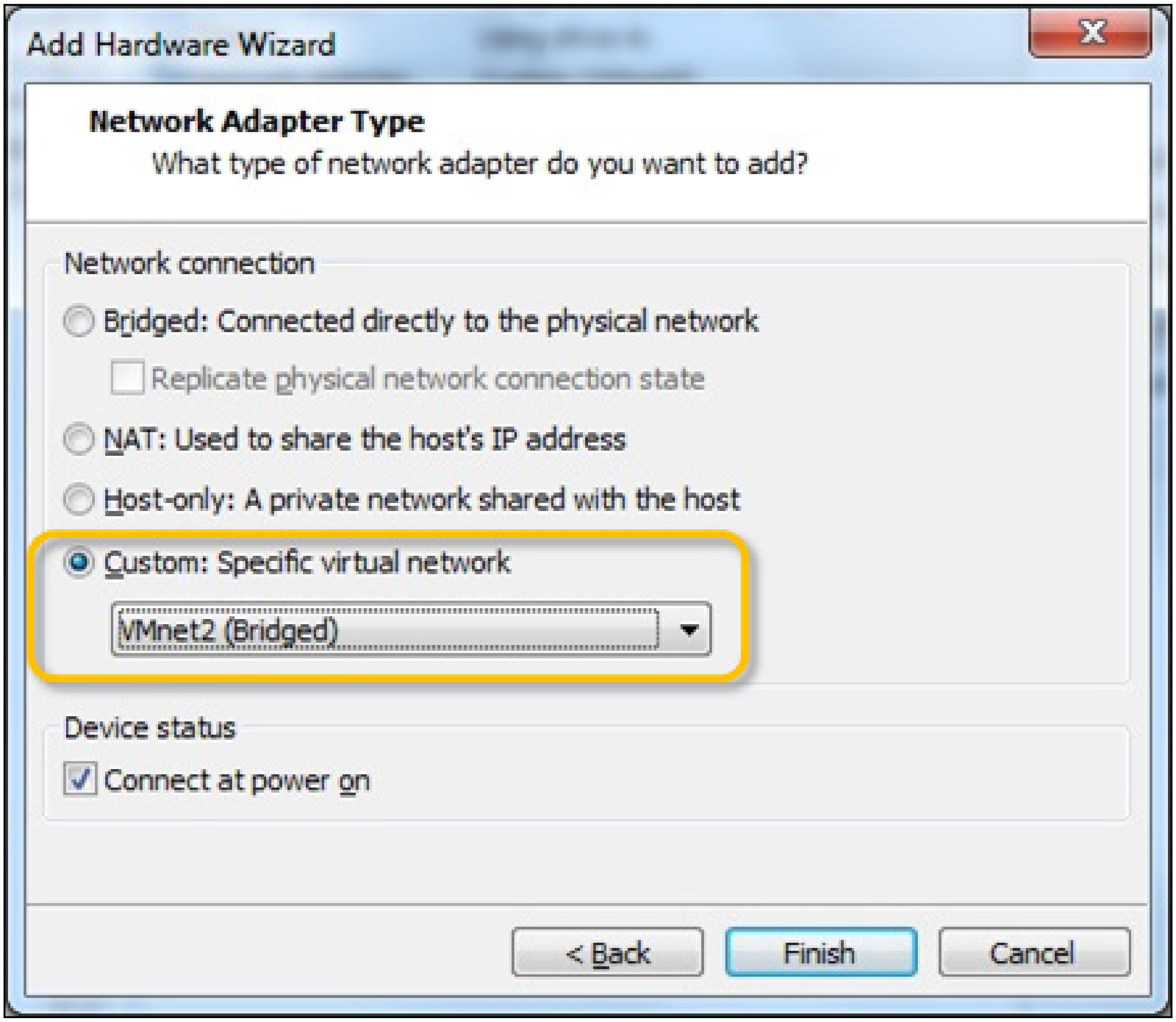
Hardware types:

- Hard Disk
- CD/DVD Drive
- Floppy Drive
- Network Adapter
- USB Controller
- Sound Card
- Parallel Port
- Serial Port
- Printer
- Generic SCSI Device

Explanation

Add a network adapter.

h. Check **Custom: Specific virtual network** and select **VMnet2 (Bridged)** from the drop-down menu. Click **Finish** to complete the network adapter addition process.



Add Hardware Wizard

Network Adapter Type

What type of network adapter do you want to add?

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

● Custom: Specific virtual network

VMnet2 (Bridged)

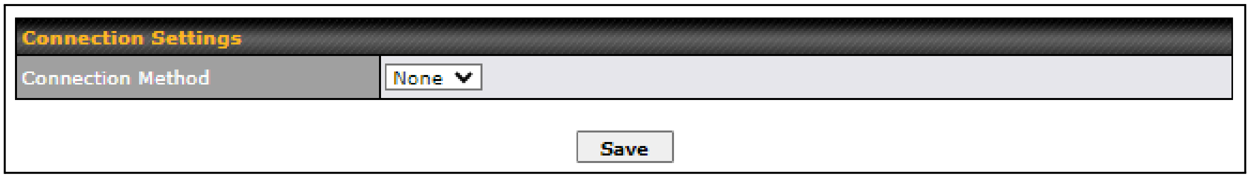
Device status

☑ Connect at power on

Adding a network adapter when using VMware Player

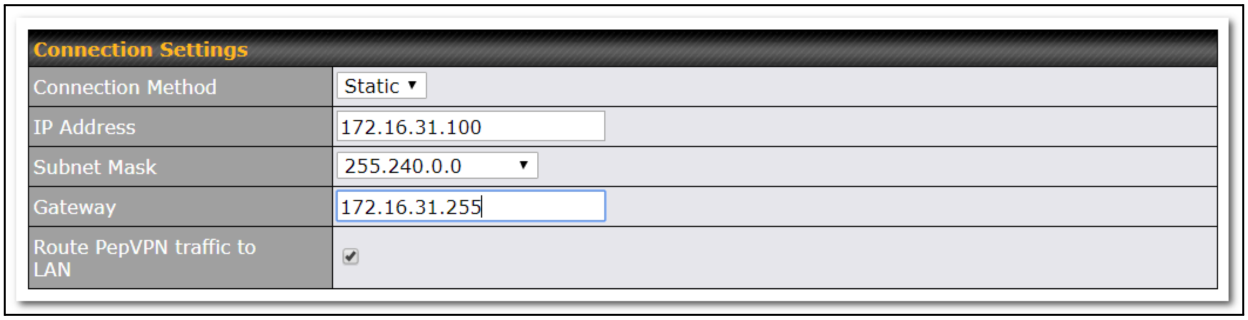
The **Virtual Network Editor** is not available in **VMware Player**. If you want to test this example with VMware Player, first add a virtual network editor to VMware Player. Then follow the steps described in **VMware Workstation** to modify and add network adapters. For details on adding a virtual network editor to VMware Player, refer to http://www.eightforums.com/virtualization/5137-how-add-virtual-network-editor-vmware-player-2.html#post275406

8. After adding one or more network adapters to the FusionHub virtual machine, select **FusionHub** again. Click **Power on the virtual machine**, and then reconnect to the FusionHub Web admin interface. Navigate to **Network > LAN**.



Connection Settings	
Connection Method	None

9. Once you've set up the LAN port, click **Save** and then **Apply Changes**. In this case, the IP address of Port 2 is **172.16.31.100**.



Connection Settings	
Connection Method	Static
IP Address	172.16.31.100
Subnet Mask	255.240.0.0
Gateway	172.16.31.255
Route PepVPN traffic to LAN	☑

10. To set up the video server as shown in Figure 5.1, enter **172.16.31.x** as its IP address, and then set the default gateway so that it is the same as the IP address of FusionHub's port (in this example, the video server's default gateway address is **172.16.31.100**). Finally, directly link the video server and FusionHub Port 2 with one network cable.

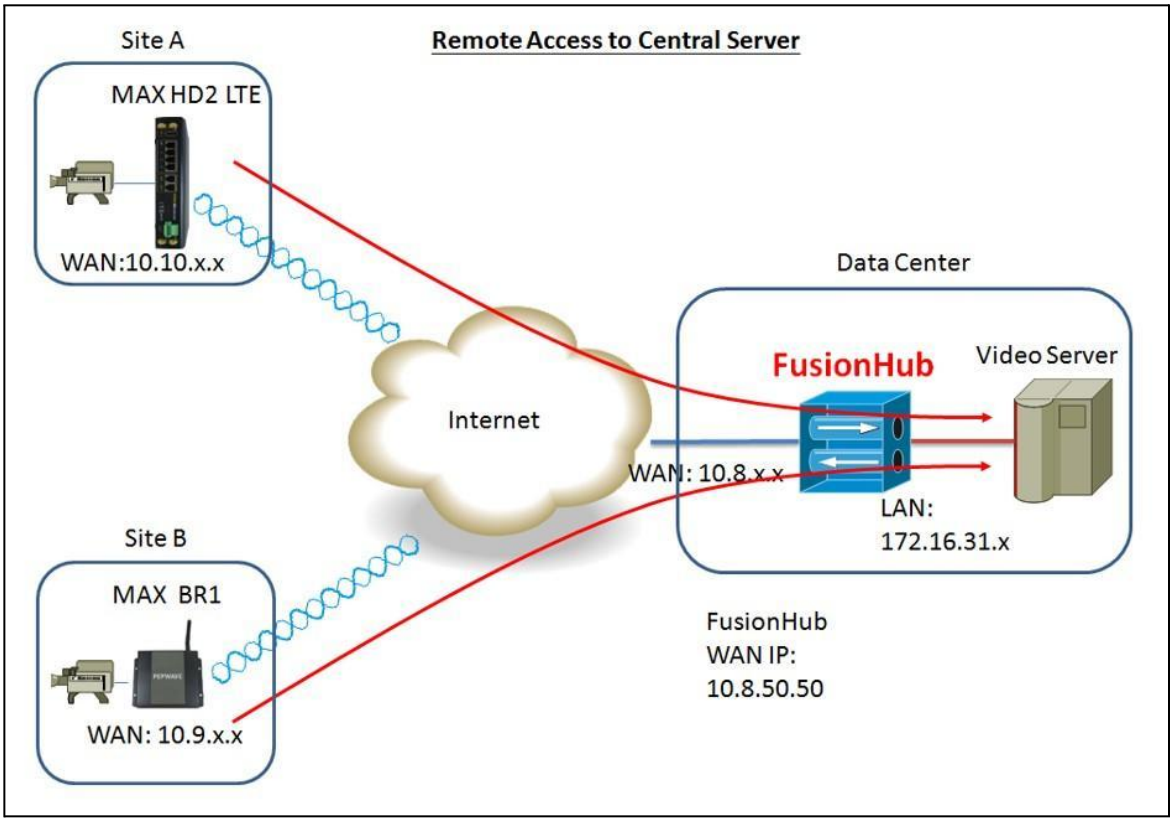


Figure 5.1 Remote access to central server

7.2.3. Example Two

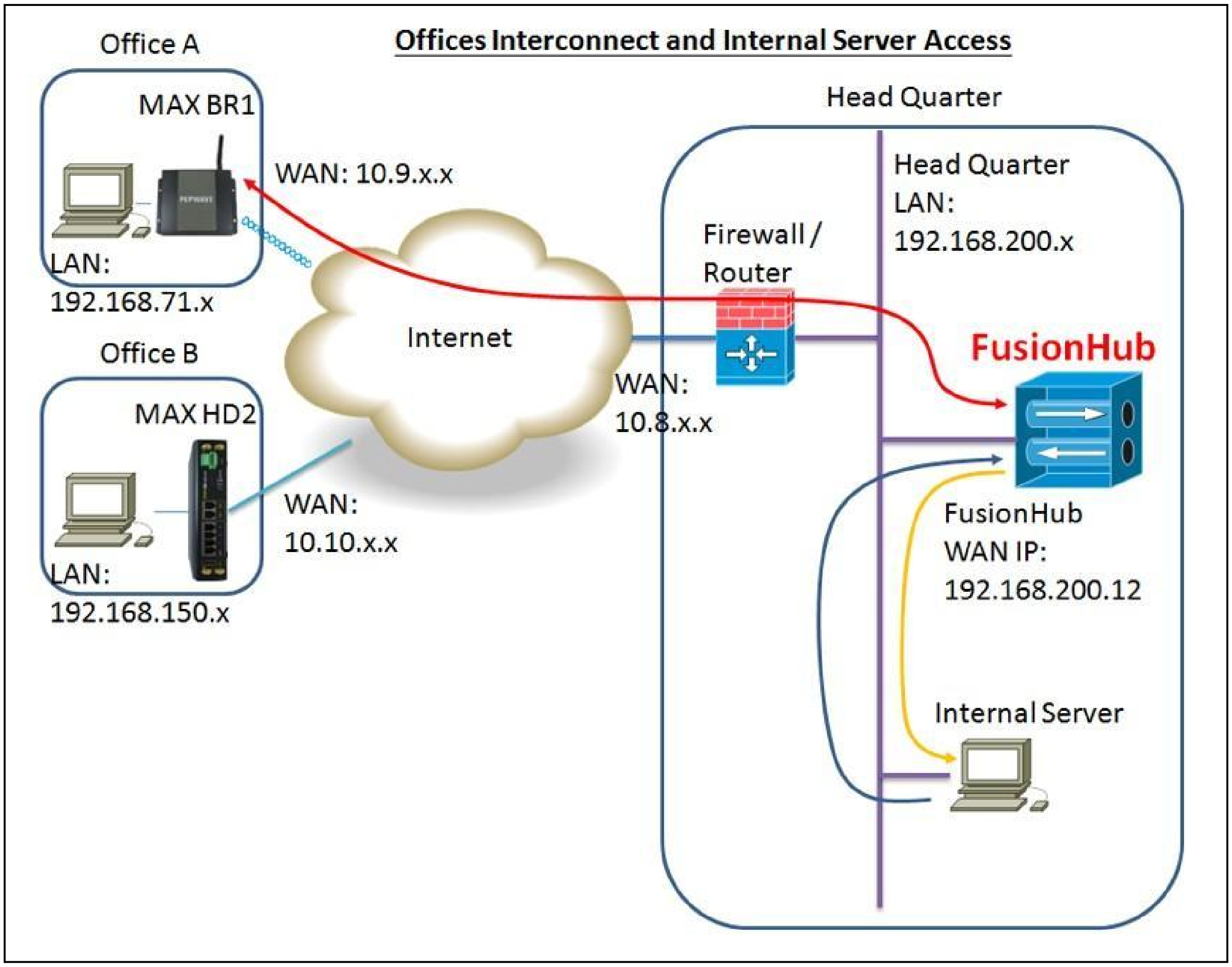


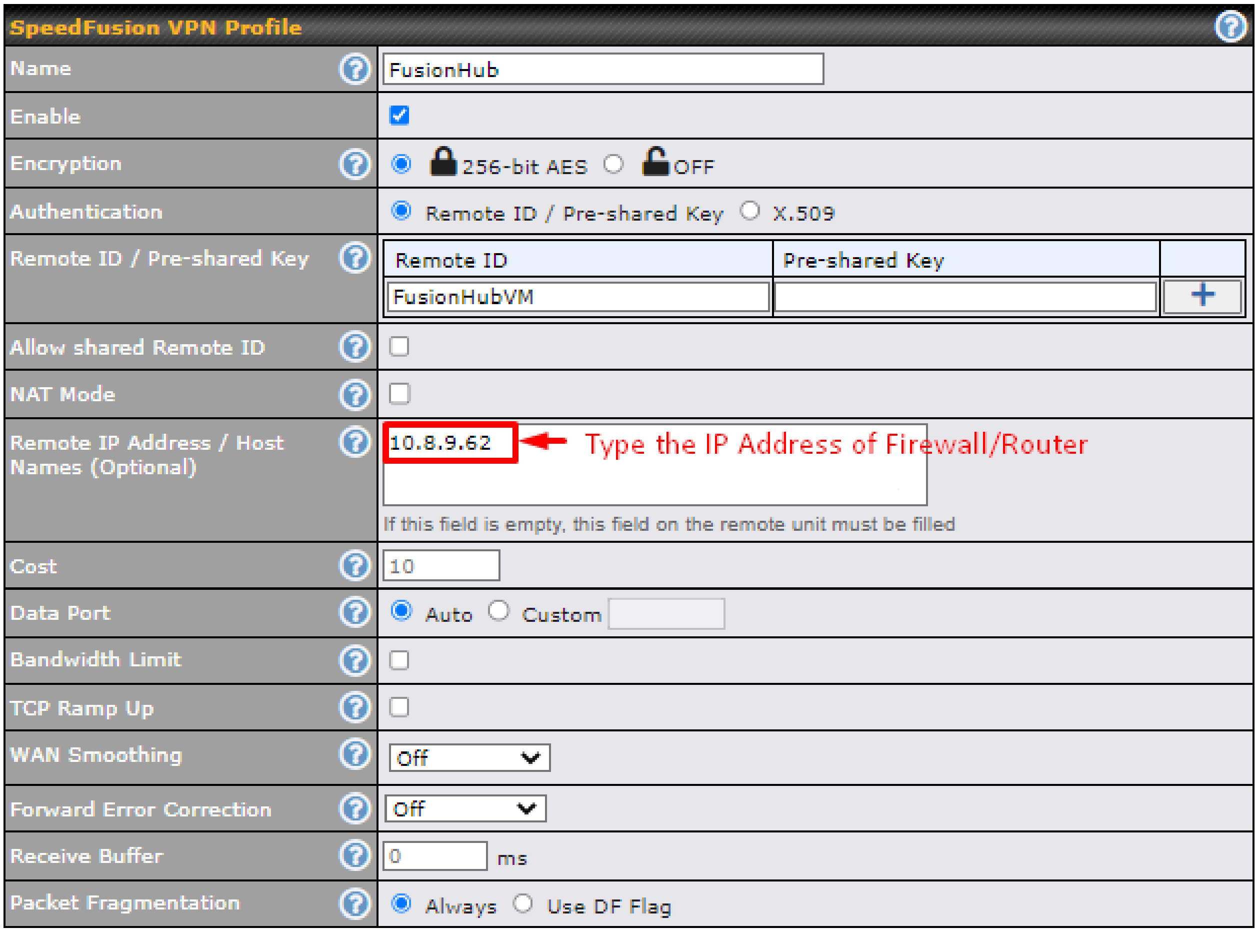
Figure 5.2 Offices interconnect

In this example, the hosts located at Office A want to communicate with the host located at Headquarters.

Case one: Supposing that network access is always made from Office A to Headquarters, setup your devices as follows:

A. MAX BR1 Settings

The settings for the MAX BR1 in Office A are the same as those in the first example, except that the **Remote IP Address/Host Names Optional** item in the PepVPN profile for FusionHub should be changed to the IP address of the firewall/router .
MAX BR1 Setting: Advanced > SpeedFusion VPN > Profile > FusionHub



SpeedFusion VPN Profile	
Name	FusionHub
Enable	☑
Encryption	● 256-bit AES ○ OFF
Authentication	● Remote ID / Pre-shared Key ○ X.509
Remote ID / Pre-shared Key	Remote ID: FusionHubVM Pre-shared Key: +
Allow shared Remote ID	□
NAT Mode	□
Remote IP Address / Host Names (Optional)	10.8.9.62 If this field is empty, this field on the remote unit must be filled
Cost	10
Data Port	● Auto ○ Custom
Bandwidth Limit	□
TCP Ramp Up	□
WAN Smoothing	Off
Forward Error Correction	Off
Receive Buffer	0 ms
Packet Fragmentation	● Always ○ Use DF Flag

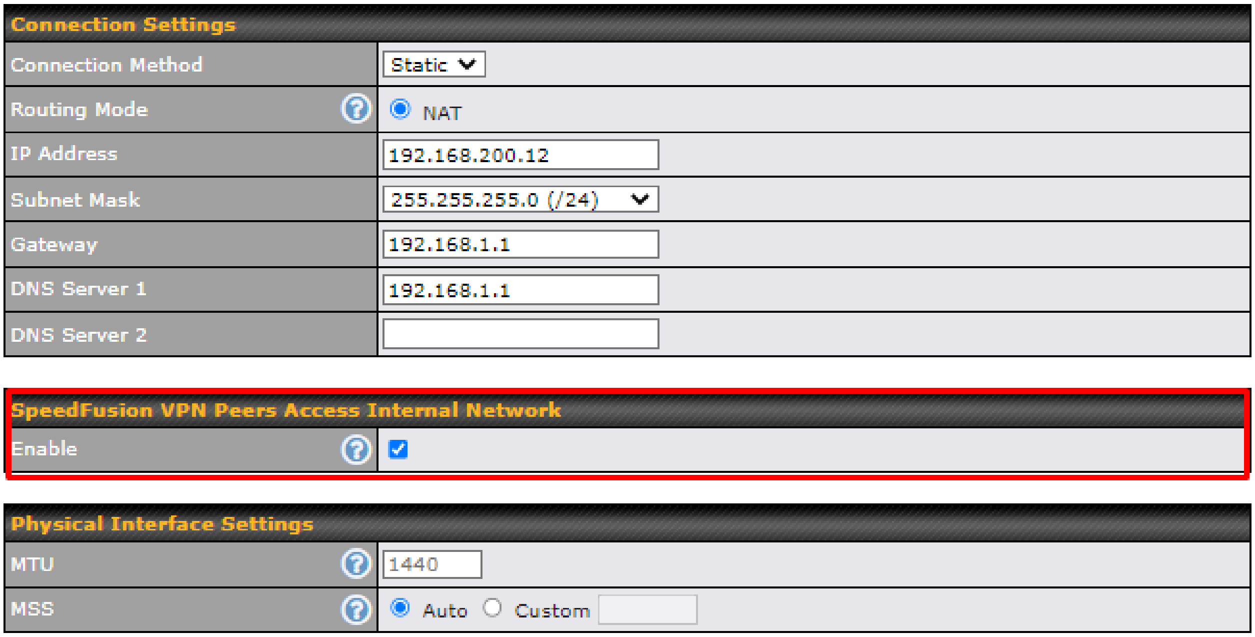
Type the IP Address of Firewall/Router

B. FusionHub Configuration Settings

The FusionHub settings are also the same as those used in the first example, except that we need only one FusionHub port in this example. Therefore, if you have added a second port during Example One, please complete the following steps to remove one port:

1. Power off the FusionHub
2. Remove the network adapter added in Example One
3. Power on the FusionHub

Next, connect to the FusionHub Web admin interface. Navigate to **Network > Interface > WAN**. Check the box under **SpeedFusion VPN Peers Access Internal Network** to enable it. To save your changes, click **OK** and then **Apply Changes**.



Connection Settings	
Connection Method	Static
Routing Mode	● NAT
IP Address	192.168.200.12
Subnet Mask	255.255.255.0 (/24)
Gateway	192.168.1.1
DNS Server 1	192.168.1.1
DNS Server 2	

SpeedFusion VPN Peers Access Internal Network	
Enable	☑

Physical Interface Settings	
MTU	1440
MSS	● Auto ○ Custom

Check **NAT Mode** in the SpeedFusion VPN profile for FusionHub.

C. Firewall/Router settings

Forward **UDP port 4500** to FusionHub (192.168.200.12, in our example). Then forward **TCP port 32015** to FusionHub (192.168.200.12, in our example).

Case two: Supposing that network access needs to be available on both sides:
Follow the same steps in case one except in Step 2 do not check **NAT Mode** in the PepVPN profile for FusionHub.

Configuring the hosts located on the Headquarters LAN

In Figure 5.2, the host located on the Headquarters LAN is a PC named **Internal Server**. In this example, you would need to add a static return route on this PC. For a PC running Windows, the command to add a static route is *route add -p* <MAX BR1 LAN's network> <MAX BR1's netmask> <FusionHub's local IP address>.

Example: > *route add -p 192.168.71.0 mask 255.255.255.0 192.168.200.12* (assuming FusionHub's local IP is 192.168.200.12). Here, *-p* makes the added route persistent across system reboots. This option is not supported in Windows 95.

NOTE: If you use a Peplink product as your firewall/router in this example, you will need to disable all PepVPN with SpeedFusion profiles.

7.2.4. Example Three

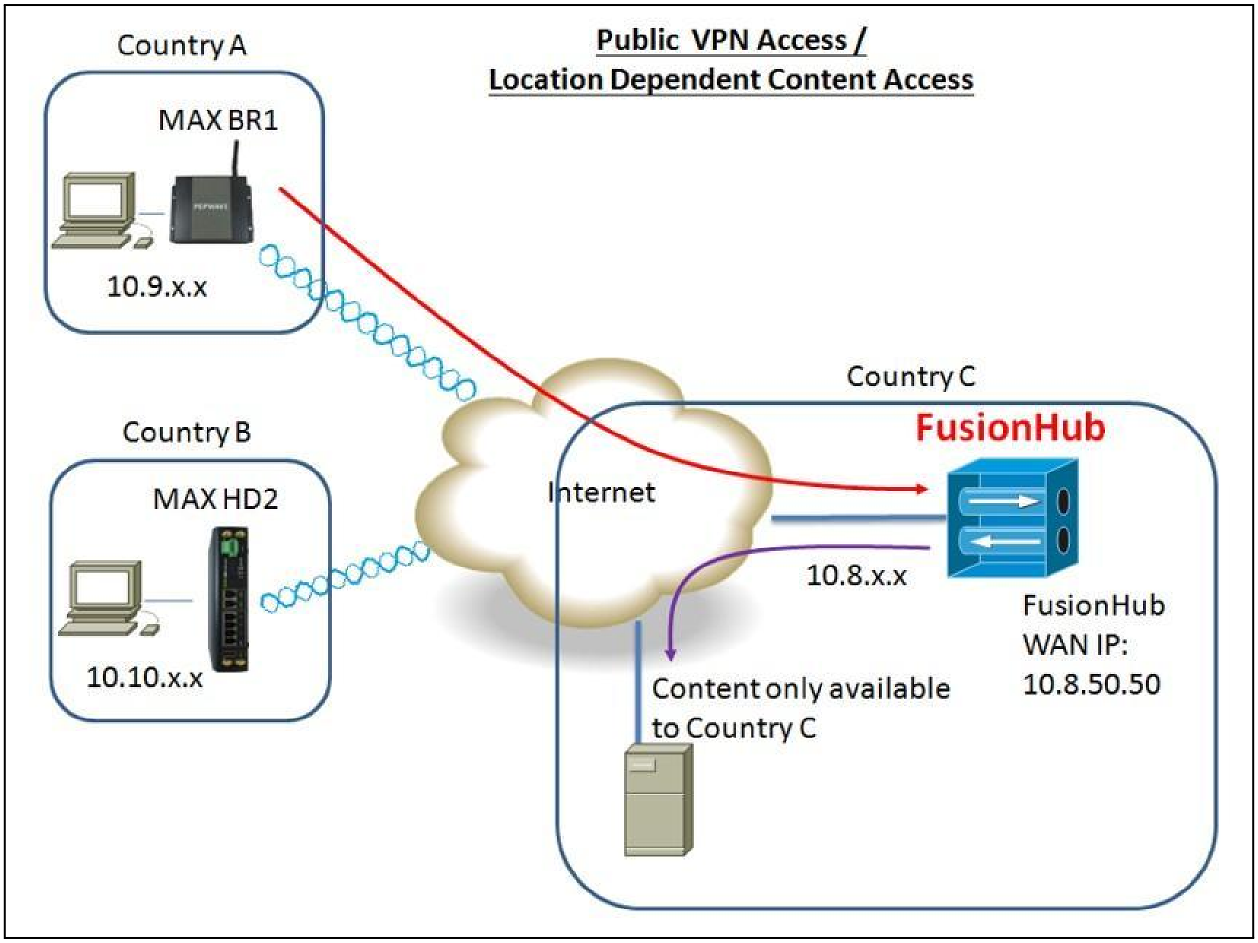
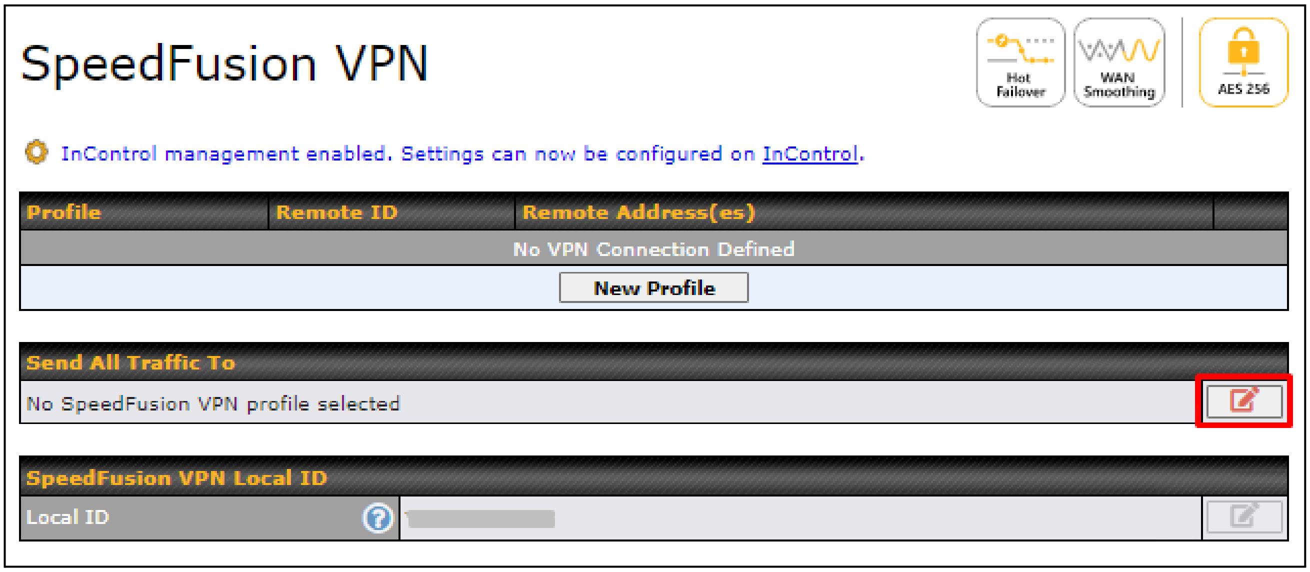


Figure 5.3 Public VPN Access / Location Dependent Content Access

In this case, the settings of the MAX BR1 in Country A and the MAX HD2 in Country B are similar to those settings in the first example. However, the following changes must be made:

A. MAX BR1 Configuration Settings

1. Navigate to **Advanced > SpeedFusion VPN**, and then click ✎ under **Send All Traffic To**.



SpeedFusion VPN

InControl management enabled. Settings can now be configured on InControl.

Profile	Remote ID	Remote Address(es)
No VPN Connection Defined		

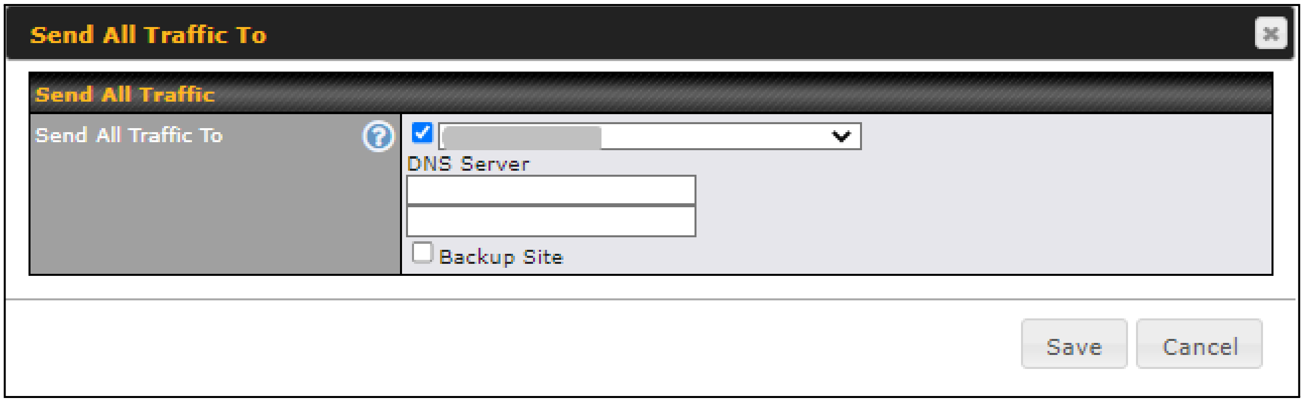
Send All Traffic To

No SpeedFusion VPN profile selected

SpeedFusion VPN Local ID

Local ID: [redacted]

2. On the dialog displayed next, check the box under **Send All Traffic To**. Select **FusionHub** from the drop-down menu. Here, **FusionHub** is the profile name. Next, set **DNS server** to the same address used by FusionHub's DNS server, which is **10.8.8.1** in this example. To save your changes, click **OK** and then **Apply Changes**.



Send All Traffic To

Send All Traffic

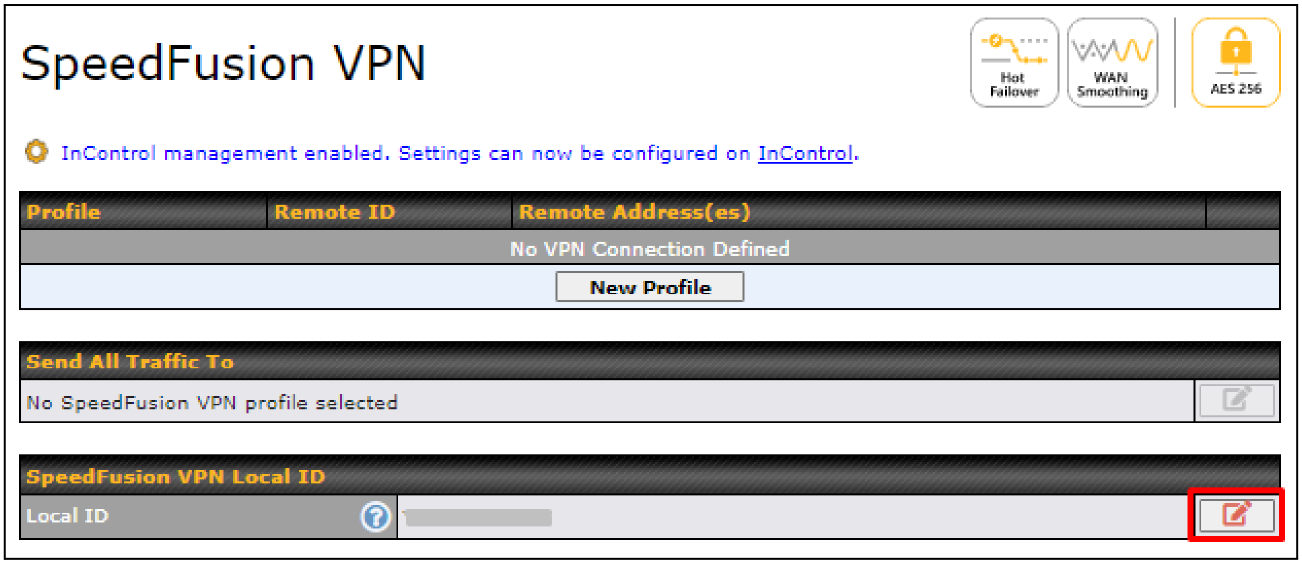
Send All Traffic To: ☑ [redacted]

DNS Server

□ Backup Site

B. MAX HD2 Configuration Settings

1. Navigate to **Advanced > SpeedFusion**, and then click ✎ under **Send All Traffic To**.



SpeedFusion VPN

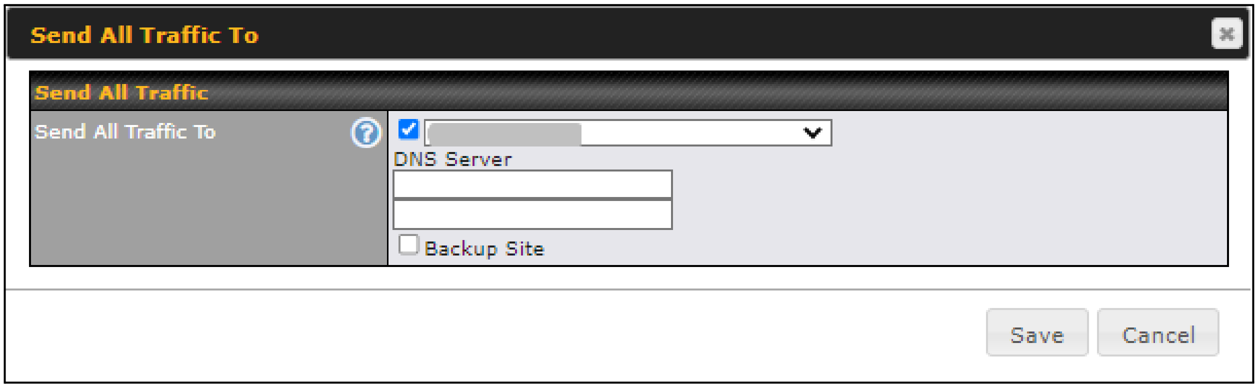
InControl management enabled. Settings can now be configured on InControl.

Profile	Remote ID	Remote Address(es)	
No VPN Connection Defined			
New Profile			

Send All Traffic To	
No SpeedFusion VPN profile selected	✎

SpeedFusion VPN Local ID		
Local ID ?	[redacted]	✎

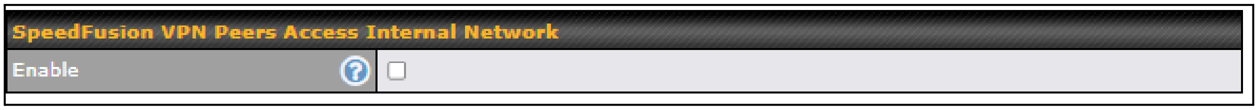
2. On the dialog displayed next, check the box under **Send All Traffic To**. Select **FusionHub** from the drop-down menu. Here, **FusionHub** is the profile name. Next, set **DNS Server** to the same address used by FusionHub's DNS server, which is **10.8.8.1** in this example. To save your changes, click **OK** and then **Apply Changes**.



Send All Traffic To

Send All Traffic	
Send All Traffic To ?	☑ [redacted] ▾ DNS Server _____ _____ □ Backup Site

The FusionHub settings are also similar to those settings in the first example, except that we need only one FusionHub port in this example. Enabling **SpeedFusion VPN Peers Access Internal Network** is not needed here, so we've left the box unchecked.



SpeedFusion VPN Peers Access Internal Network	
Enable ?	□

7.3. IPsec VPN

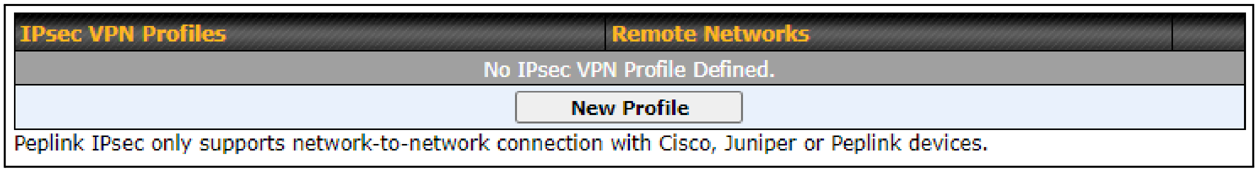
IPsec VPN functionality securely connects one or more branch offices to your company's main headquarters or to other branches. Data, voice, and video communications between these locations are kept safe and confidential across the public Internet.

All Peplink products can make multiple IPsec VPN connections with Peplink routers, as well as Cisco and Juniper routers.

Note that all LAN subnets and the subnets behind them must be unique. Otherwise, VPN members will not be able to access each other.

All data can be routed over the VPN with a selection of encryption standards, such as 3DES, AES-128, and AES-256.

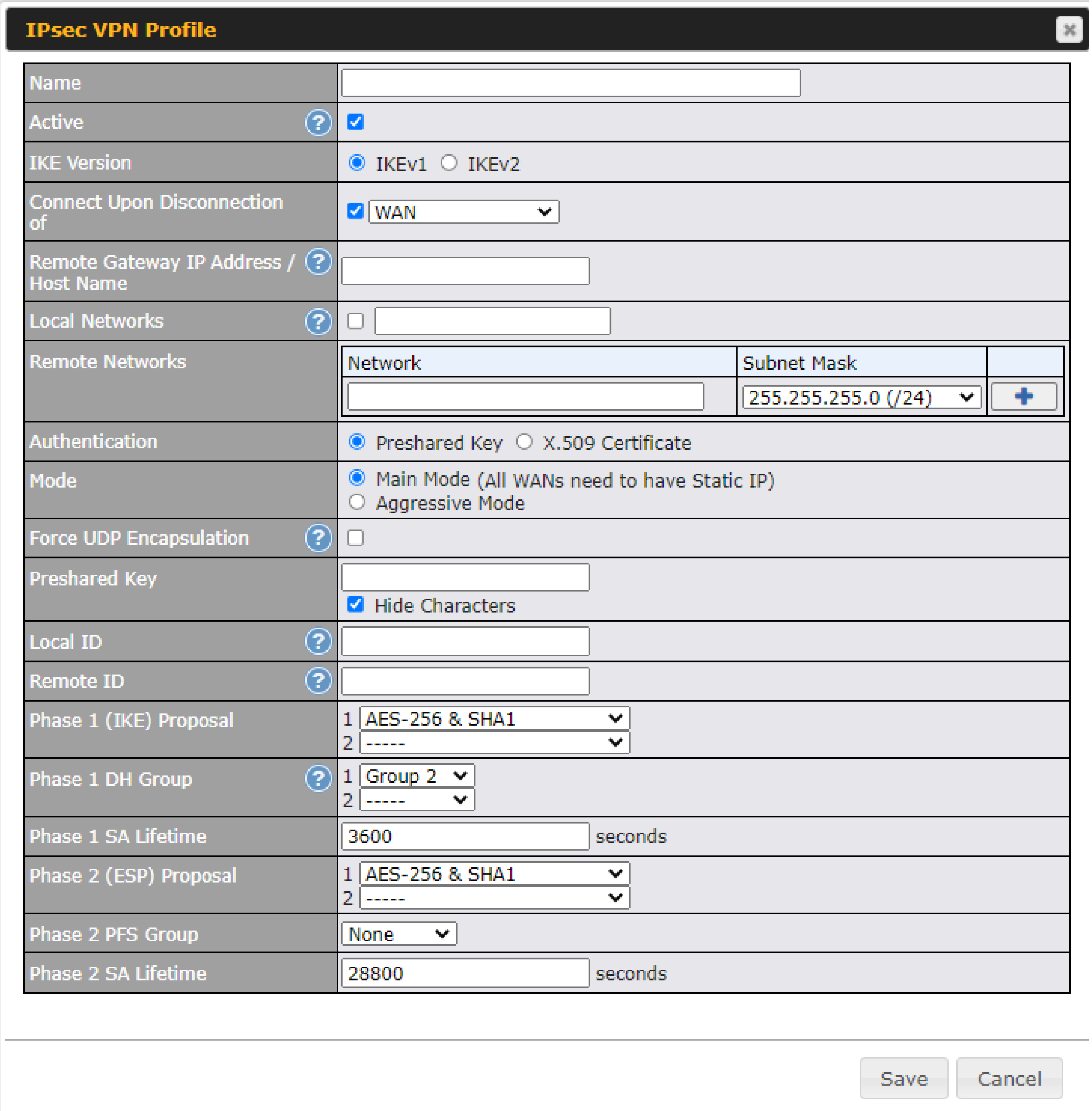
To configure, navigate to **Advanced > IPsec VPN.**



IPsec VPN Profiles	Remote Networks	
No IPsec VPN Profile Defined.		

Peplink IPsec only supports network-to-network connection with Cisco, Juniper or Peplink devices.

Click the **New Profile** button to create new IPsec VPN profiles that make VPN connections to remote Peplink, Cisco, or Juniper Routers via available WAN connections. To edit any of the profiles, click on its associated connection name in the leftmost column.



IPsec VPN Profile

Name	
Active	☑
IKE Version	● IKEv1 ○ IKEv2
Connect Upon Disconnection of	☑ WAN
Remote Gateway IP Address / Host Name	
Local Networks	□
Remote Networks	Network: Subnet Mask: 255.255.255.0 (/24) +
Authentication	● Preshared Key ○ X.509 Certificate
Mode	● Main Mode (All WANs need to have Static IP) ○ Aggressive Mode
Force UDP Encapsulation	□
Preshared Key	☑ Hide Characters
Local ID	
Remote ID	
Phase 1 (IKE) Proposal	1 AES-256 & SHA1 2 -----
Phase 1 DH Group	1 Group 2 2 -----
Phase 1 SA Lifetime	3600 seconds
Phase 2 (ESP) Proposal	1 AES-256 & SHA1 2 -----
Phase 2 PFS Group	None
Phase 2 SA Lifetime	28800 seconds

IPsec VPN Profile Settings	
Name	This field is for specifying a local name to represent this connection profile.
Active	When this box is checked, this IPsec VPN connection profile will be enabled. Otherwise, it will be disabled.
IKE Version	Choose the IKE version that is used to establish a security association

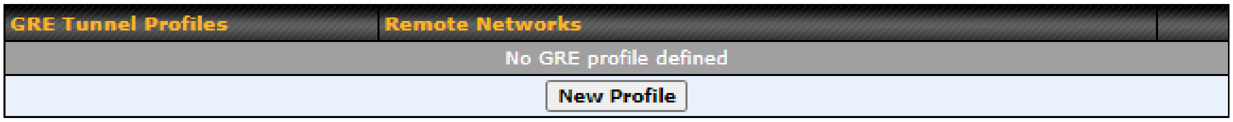
	(SA) in the IPsec protocol.
Connect Upon Disconnection of	Check this box and select a WAN to connect to this VPN automatically when the specified WAN is disconnected. To activate this function, click the ? button next to the “Active” option.
Remote Gateway IP Address / Host Name	Enter the remote peer’s public IP address. For **Aggressive Mode**, this is optional.
Local Networks	Select or add required local networks for IPsec site-to-site VPN connection. Using NAT, you can map a specific local network / IP address to another, and the packets received by remote gateway will appear to be coming from the mapped network / IP address. This allows you to establish IPsec connection to a remote site that has one or more subnets overlapped with local site. Two types of NAT policies can be defined: **One-to-One NAT policy**: if the defined subnet in Local Network and NAT Network has the same size, for example, policy "192.168.50.0/24 > 172.16.1.0/24" will translate the local IP address 192.168.50.10 to 172.16.1.10 and 192.168.50.20 to 172.16.1.20. This is a bidirectional mapping which means clients in remote site can initiate connection to the local clients using the mapped address too. **Many-to-One NAT policy**: if the defined NAT Network on the right hand side is an IP address (or having a network prefix /32), for example, policy "192.168.1.0/24 > 172.168.50.1/32" will translate all clients in 192.168.1.0/24 network to 172.168.50.1. This is a unidirectional mapping which means clients in remote site will not be able to initiate a connection to the local clients.
Remote Networks	Enter the LAN and subnets that are located at the remote site here.
Authentication	To access your VPN, clients will need to authenticate by your choice of methods. Choose between the **Preshared Key** and **X.509 Certificate** methods of authentication.
Mode	Choose **Main Mode** if both IPsec peers use static IP addresses. Choose **Aggressive Mode** if one of the IPsec peers uses dynamic IP addresses.
Force UDP	For forced UDP encapsulation regardless of NAT-traversal, tick this

Encapsulation	checkbox.
Pre-shared Key	This defines the peer authentication pre-shared key used to authenticate this VPN connection. The connection will be up only if the pre-shared keys on each side match.
Remote Certificate (pem encoded)	Available only when **X.509 Certificate** is chosen as the **Authentication** method, this field allows you to paste a valid X.509 certificate.
Local ID	In **Main Mode**, this field can be left blank. In **Aggressive Mode**, if **Remote Gateway IP Address** is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN.
Remote ID	In **Main Mode**, this field can be left blank. In **Aggressive Mode**, if **Remote Gateway IP Address** is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN.
Phase 1 (IKE) Proposal	In **Main Mode**, this allows setting up to six encryption standards, in descending order of priority, to be used in initial connection key negotiations. In **Aggressive Mode**, only one selection is permitted.
Phase 1 DH Group	This is the Diffie-Hellman group used within IKE. This allows two parties to establish a shared secret over an insecure communications channel. The larger the group number, the higher the security. **Group 2**: **1024-bit** is the default value. **Group 5**: **1536-bit** is the alternative option.
Phase 1 SA Lifetime	This setting specifies the lifetime limit of this Phase 1 Security Association. By default, it is set at **3600** seconds.
Phase 2 (ESP) Proposal	In **Main Mode**, this allows setting up to six encryption standards, in descending order of priority, to be used for the IP data that is being transferred. In **Aggressive Mode**, only one selection is permitted.
Phase 2 PFS Group	Perfect forward secrecy (PFS) ensures that if a key was compromised, the attacker will be able to access only the data protected by that key. **None** - Do not request for PFS when initiating connection. However, since there is no valid reason to refuse PFS, the system will allow the connection to use PFS if requested by the remote peer. This is the default value. **Group 2**: 1024-bit Diffie-Hellman group. The larger the group number, the higher the security. **Group 5**: **1536-bit** is the third option.
Phase 2 SA Lifetime	This setting specifies the lifetime limit of this Phase 2 Security Association. By default, it is set at **28800** seconds.

7.4. GRE Tunnel

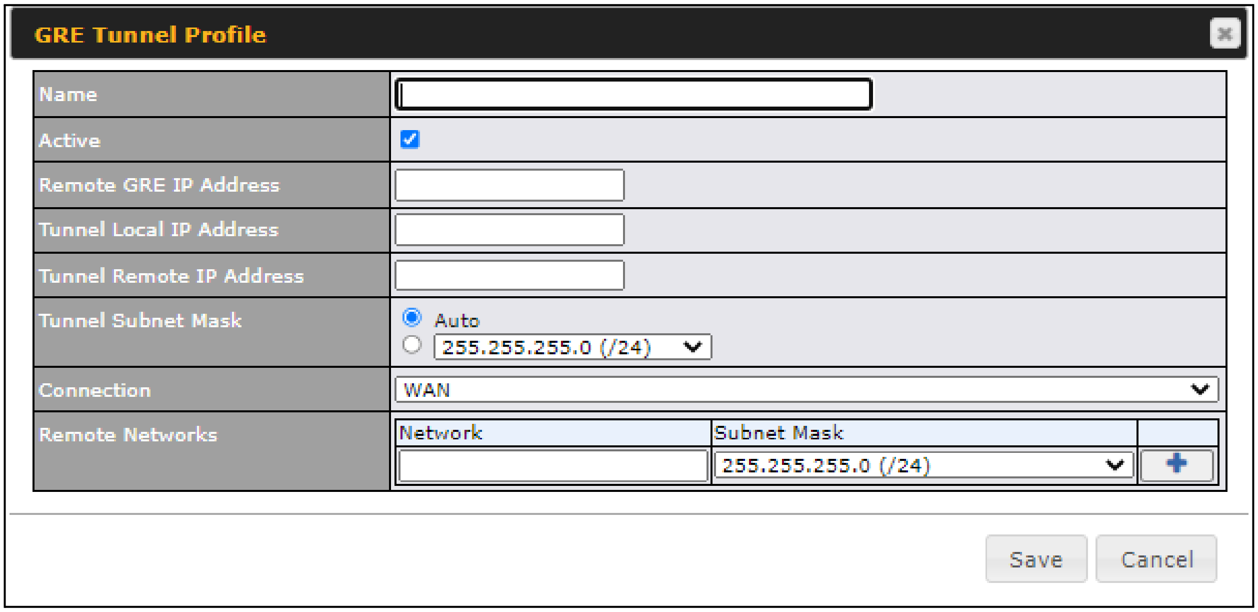
Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network. A GRE tunnel is similar to IPSec or PepVPN.

To configure a GRE Tunnel, navigate to **Advanced > GRE Tunnel**.



GRE Tunnel Profiles	Remote Networks	
No GRE profile defined		

Click the **New Profile** button to create new GRE tunnel profiles that establish tunnel connections to remote tunnel endpoints via available WAN connections. To edit a profile, click on its associated connection name in the leftmost column.



GRE Tunnel Profile

Name	
Active	☑
Remote GRE IP Address	
Tunnel Local IP Address	
Tunnel Remote IP Address	
Tunnel Subnet Mask	● Auto ○ 255.255.255.0 (/24)
Connection	WAN
Remote Networks	Network: Subnet Mask: 255.255.255.0 (/24)

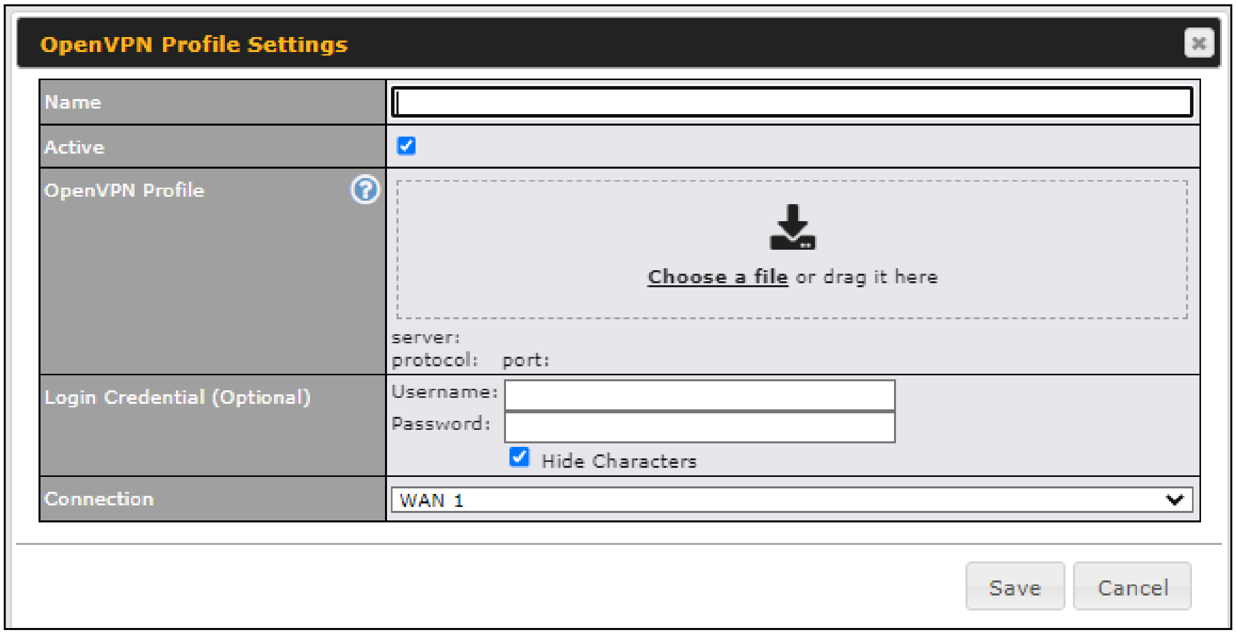
GRE Tunnel Profile Settings	
Name	This field is for specifying a name to represent this GRE Tunnel connection profile.
Active	When this box is checked, this GRE Tunnel connection profile will be enabled. Otherwise, it will be disabled.
Remote GRE IP Address	This field is for entering the remote GRE's IP address.
Tunnel Local IP	This field is for specifying the tunnel source IP address.

Address	
Tunnel Remote IP Address	This field is for specifying the tunnel destination IP address
Tunnel Subnet Mask	This field is to select the subnet mask that is to be used for the GRE tunnel.
Connection	Select the appropriate WAN connection from the drop-down menu.
Remote Networks	Input the LAN and subnets that are located at the remote site here.

7.5. OpenVPN

OpenVPN is a site to site VPN mode that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network.

To configure a OpenVPN, navigate to **Advanced > OpenVPN** and click the **New Profile**.



OpenVPN Profile Settings

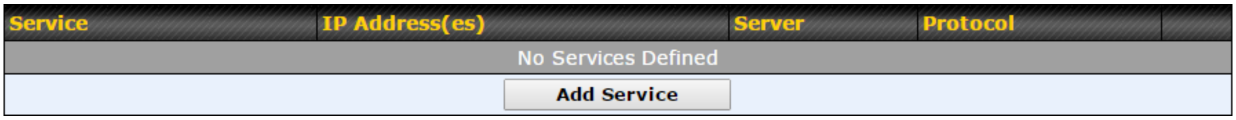
Name	
Active	☑
OpenVPN Profile	Choose a file or drag it here server: protocol: port:
Login Credential (Optional)	Username: Password: ☑ Hide Characters
Connection	WAN 1

OpenVPN Profile Settings	
Name	This field is for specifying a name to represent this OpenVPN profile.
Active	When this box is checked, this OpenVPN connection profile will be enabled. Otherwise, it will be disabled.

OpenVPN Profile	Upload the OpenVPN configuration (.ovpn) file from your service provider.
Login Credential (Optional)	This option is an optional for you to enter the username and password to login for the OpenVPN connection if the profile need to login.
Connection	Select the appropriate WAN connection from the drop-down menu.

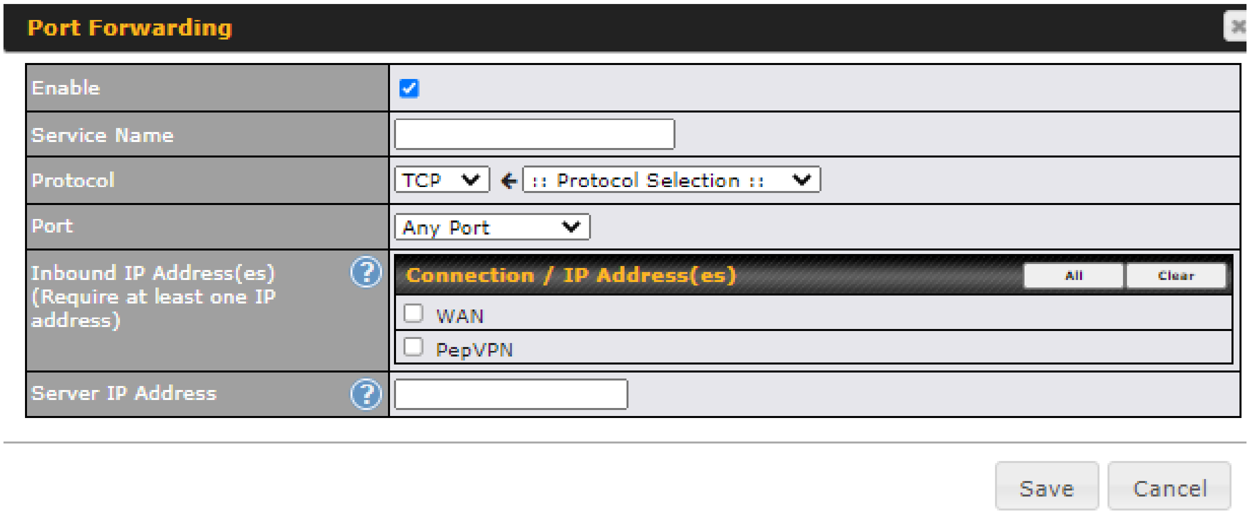
7.6. Port Forwarding

FusionHub can act as a firewall that blocks, by default, all inbound access from the Internet. Inbound port forwarding rules can be defined at **Advanced > Port Forwarding**.



Service	IP Address(es)	Server	Protocol
No Services Defined			

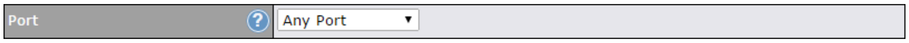
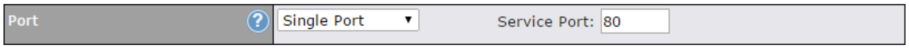
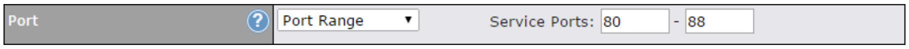
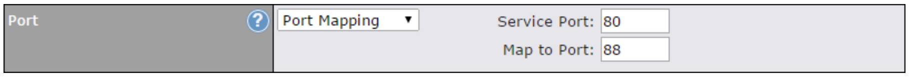
To define a new service, click **Add Service**.

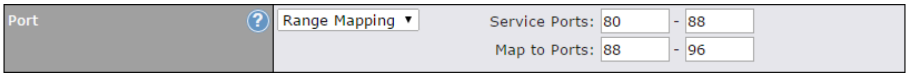


Port Forwarding

Enable	☑
Service Name	
Protocol	TCP ← :: Protocol Selection ::
Port	Any Port
Inbound IP Address(es) (Require at least one IP address)	Connection / IP Address(es) □ WAN □ PepVPN
Server IP Address	

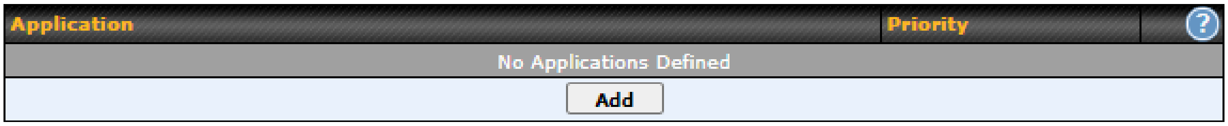
Port Forwarding Settings	
Enable	This setting specifies whether the inbound service takes effect. When **Enable** is checked, the inbound service takes effect: traffic is matched and actions are taken by the FusionHub based on the other parameters of the rule. When this setting is disabled, the inbound service does not take effect: device disregards the other parameters of the rule.
Service Name	This setting identifies the service to the system administrator. Valid values for this setting consist of only alphanumeric and underscore "_" characters.

Protocol	The **Protocol** setting, along with the **Port** setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Traffic that is received by the unit via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the **Servers** setting. Please see below for details on the **Port** and **Servers** settings. Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and a single port number of common Internet services (e.g. HTTP, HTTPS, etc.). After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remain manually modifiable.
Port	The **Port** setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners: **Any Port**, **Single Port**, **Port Range**, **Port Map**, and **Range Mapping**  Port ? Any Port ▾ **Any Port**: all traffic that is received by the unit via the specified protocol is forwarded to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Any Port**, all TCP traffic is forwarded to the configured servers.  Port ? Single Port ▾ Service Port: 80 **Single Port**: traffic that is received by the unit via the specified protocol at the specified port is forwarded via the same port to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Single Port** and **Service Port** 80, TCP traffic received on port 80 is forwarded to the configured servers via port 80.  Port ? Port Range ▾ Service Ports: 80 - 88 **Port Range**: traffic that is received by the unit via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Port Range** and **Service Ports** 80-88, TCP traffic received on ports 80 through 88 is forwarded to the configured servers via the respective ports.  Port ? Port Mapping ▾ Service Port: 80 Map to Port: 88 **Port Mapping**: traffic that is received by the unit via the specified protocol at the specified port is forwarded via a different port to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Port Mapping**, **Service Port** 80, and **Map to Port** 88, TCP traffic on port 80 is forwarded to the configured servers via port 88. (Please see below for details on the **Servers** setting.)

	 Port Range Mapping ▾ Service Ports: 80 - 88 Map to Ports: 88 - 96 **Range Mapping**: traffic that is received by the unit via the specified protocol at the specified port range is forwarded via a different port to the servers specified by the **Servers** setting.
Inbound IP Address(es)	This setting allows you to select the connection(s) and IP address(es) that are to be listened from.
Server IP Address	Enter the server IP address where the inbound traffic should be forwarded to. This unit will act as a virtual server listening to requests from the WANs. It forwards requests to the server that is entered in this field.

8. QoS

8.1. Application

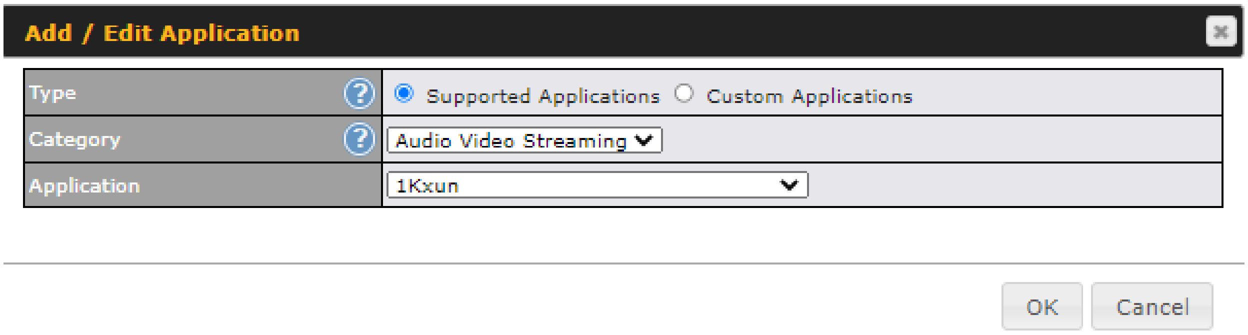


Application	Priority
No Applications Defined	
Add	

Define the priority level of selected applications. Available priorities are **High**, **Normal**, and **Low**. Applications not defined in the table are assigned a "**Normal**" priority level.

System supports detecting various application traffic by inspecting the packets' content. Select an application by choosing a supported application, or by defining a custom application manually. The priority preference of supported applications is placed at the top of the table. Custom applications are at the bottom.

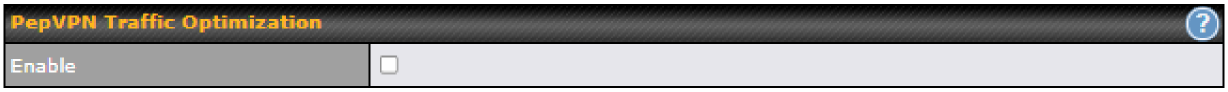
Click the **Add** button to define an application's priority. Click the button **X** to delete the application in the corresponding row. Click on a custom application's name to edit.



Add / Edit Application

Type	● Supported Applications ○ Custom Applications
Category	Audio Video Streaming
Application	1Kxun

When the **Supported Applications** is selected, the device will inspect network traffic and prioritize the selected application. Alternatively, you can select the **Custom Applications** and define the application by supplying the protocol/scope, port number, and DSCP value. You can choose the **Category** of the application and the Application name from the below list.



PepVPN Traffic Optimization	
Enable	□

Enabling the PepVPN Traffic Optimization is to allow PepVPN traffic to have highest priority when WAN is congested.

9. Firewall

A firewall is a mechanism that selectively filters data traffic between the WAN side (the Internet) and the LAN side of the network. It can protect the local network from potential hacker attacks, access to offensive websites, and/or other inappropriate uses.

The firewall functionality of device supports the selective filtering of data traffic in both directions:

Outbound (LAN to WAN)
Inbound (WAN to LAN)
Internal Network (VLAN to VLAN)
Local Service

The firewall also supports the following functionality:

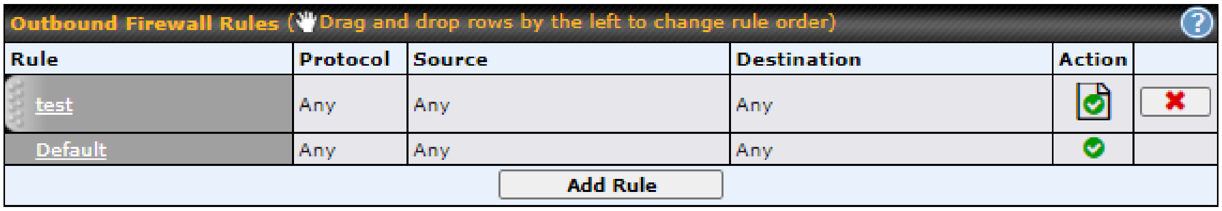
- Intrusion detection and DoS prevention
- Web blocking

With SpeedFusion^{TM} enabled, the firewall rules also apply to VPN tunneled traffic. The Firewall function can be found at **Advanced > Firewall**.

9.1. Access Rules

Outbound Firewall Rules

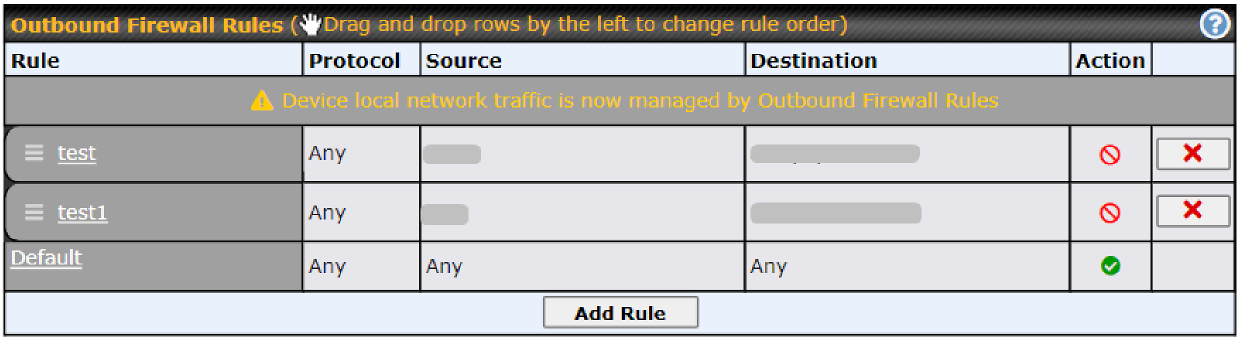
The outbound firewall settings are located at **Advanced > Firewall > Access Rules**.



Outbound Firewall Rules (Drag and drop rows by the left to change rule order) ?

Rule	Protocol	Source	Destination	Action	
test	Any	Any	Any	✓	✖
Default	Any	Any	Any	✓	

To enable or disable the Outbound Firewall to manage device local network traffic, click on the help icon ? and click here, the sceen will shows below.



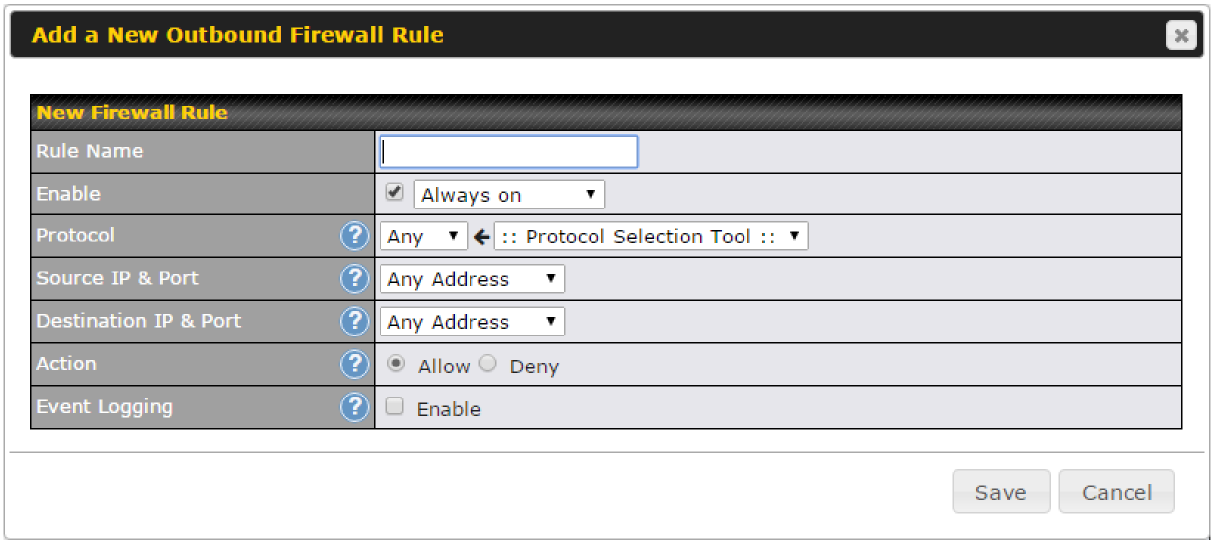
Outbound Firewall Rules (Drag and drop rows by the left to change rule order)

Rule	Protocol	Source	Destination	Action	
⚠ Device local network traffic is now managed by Outbound Firewall Rules					
test	Any	[redacted]	[redacted]	⦸	✕
test1	Any	[redacted]	[redacted]	⦸	✕
Default	Any	Any	Any	✓	

Note

To utilize the Outbound Firewall Rule to block the Peplink device from contacting InControl 2. may refer to the link below:
https://forum.peplink.com/t/faq-prevent-device-reaching-incontrol-2./63f48fdfd466df34ab475f55/

Click **Add Rule** to display the following screen:



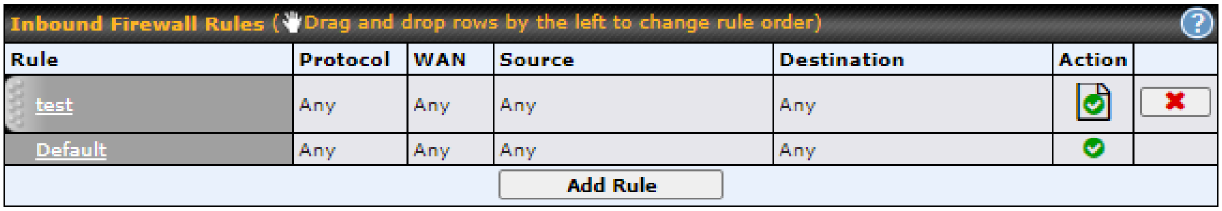
Add a New Outbound Firewall Rule

New Firewall Rule

Rule Name	
Enable	☑ Always on
Protocol	Any ← :: Protocol Selection Tool ::
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	● Allow ○ Deny
Event Logging	□ Enable

Inbound Firewall Rules

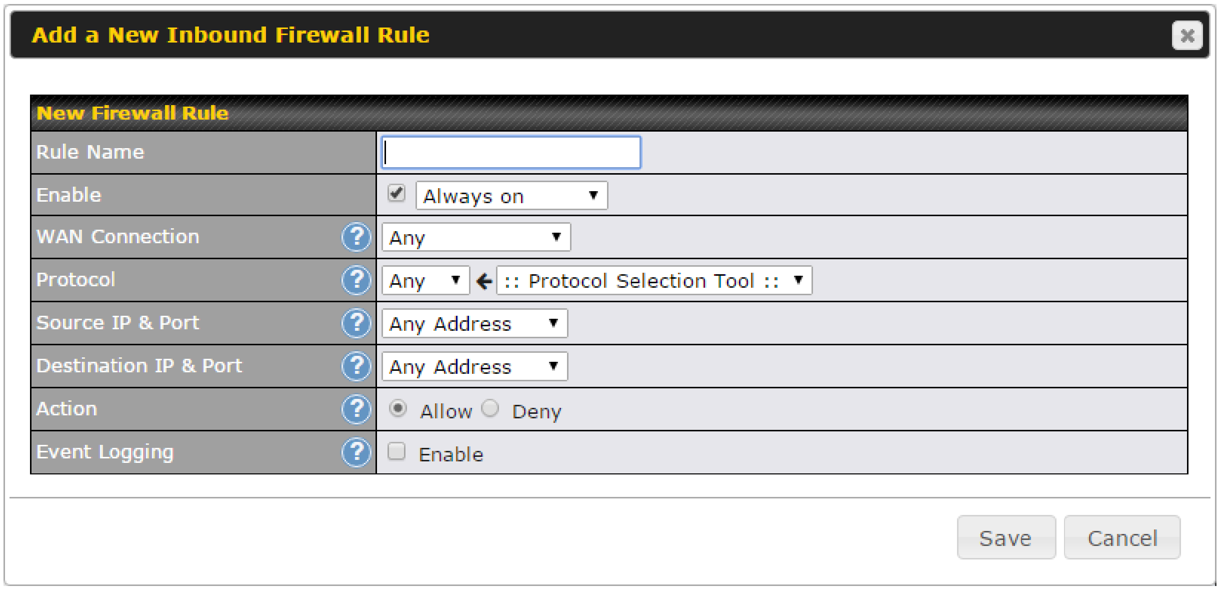
The inbound firewall settings are located at **Advanced > Firewall > Access Rules**.



Inbound Firewall Rules (Drag and drop rows by the left to change rule order)

Rule	Protocol	WAN	Source	Destination	Action	
test	Any	Any	Any	Any	✓	✕
Default	Any	Any	Any	Any	✓	

Click **Add Rule** to display the following window:

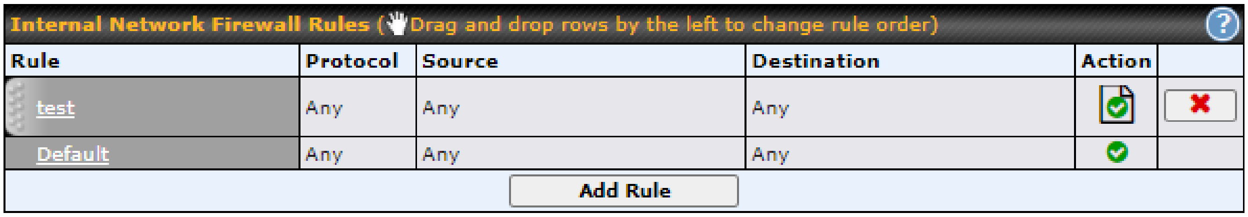


Add a New Inbound Firewall Rule

New Firewall Rule	
Rule Name	
Enable	☑ Always on
WAN Connection	Any
Protocol	Any ← :: Protocol Selection Tool ::
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	● Allow ○ Deny
Event Logging	□ Enable

Internal Network Firewall Rules

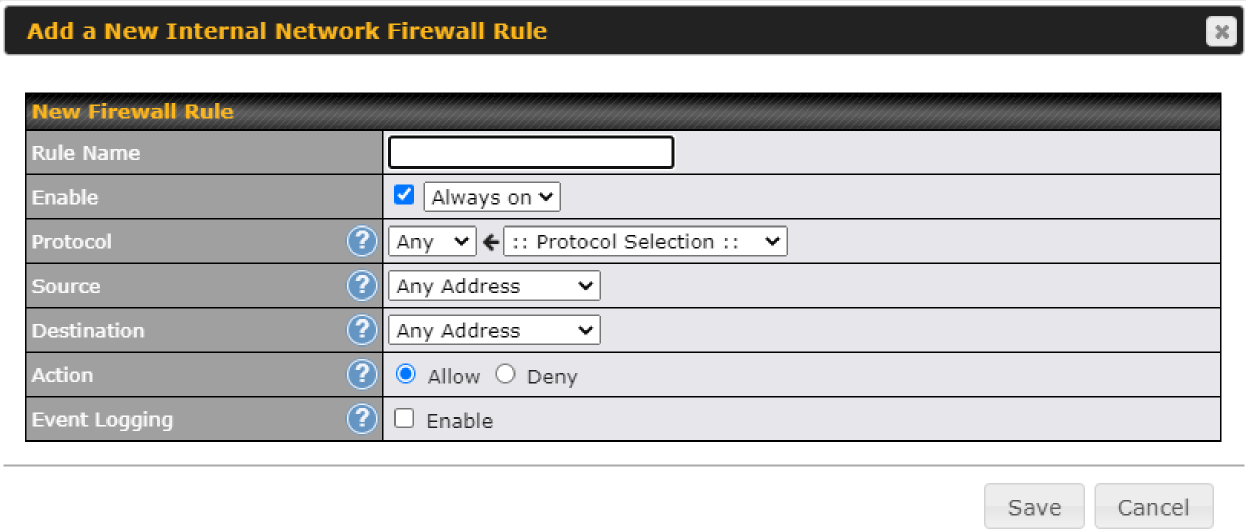
The Internal Network firewall settings are located at **Advanced > Firewall > Access Rules**.



Internal Network Firewall Rules (Drag and drop rows by the left to change rule order)

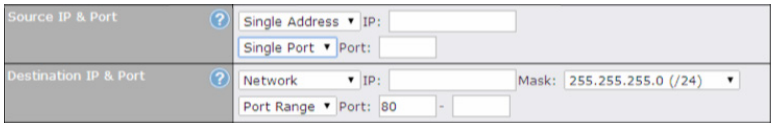
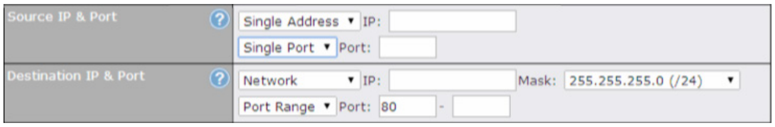
Rule	Protocol	Source	Destination	Action	
test	Any	Any	Any	✓	✗
Default	Any	Any	Any	✓	

Click **Add Rule** to display the following window:



Add a New Internal Network Firewall Rule

New Firewall Rule	
Rule Name	
Enable	☑ Always on
Protocol	Any ← :: Protocol Selection ::
Source	Any Address
Destination	Any Address
Action	● Allow ○ Deny
Event Logging	□ Enable

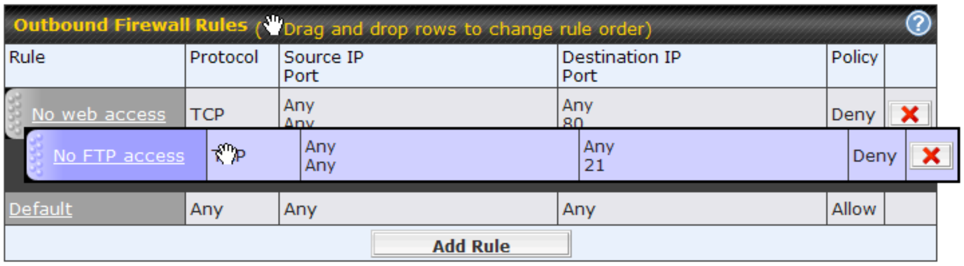
Inbound / Outbound / Internal Network Firewall Settings	
Rule Name	This setting specifies a name for the firewall rule.
Enable	This setting specifies whether the firewall rule should take effect. If the box is checked, the firewall rule takes effect. If the traffic matches the specified protocol/IP/port, actions will be taken by this unit based on the other parameters of the rule. If the box is not checked, the firewall rule does not take effect. The unit will disregard the other parameters of the rule.
Protocol	This setting specifies the protocol to be matched. Via a drop-down menu, the following protocols can be specified: ● **Any** ● **TCP** ● **UDP** ● **ICMP** ● **DSCP** ● **IP** Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.) After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remains manually modifiable.
Source and Port	This specifies the source IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the **Source IP & Port** setting, as indicated with the following screenshots:  Source IP & Port: Single Address ▾ IP: ; Single Port ▾ Port: Destination IP & Port: Network ▾ IP: Mask: 255.255.255.0 (/24) ▾ ; Port Range ▾ Port: 80 - In addition, a single port, or a range of ports, can be specified for the **Source** settings.
Destination and Port	This specifies the destination IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the **Destination IP & Port** setting, as indicated with the following screenshots:  Source IP & Port: Single Address ▾ IP: ; Single Port ▾ Port: Destination IP & Port: Network ▾ IP: Mask: 255.255.255.0 (/24) ▾ ; Port Range ▾ Port: 80 - In addition, a single port, or a range of ports, can be specified for the

	settings.
Action	This setting specifies the action to be taken by the router upon encountering traffic that matches the both of the following: ● Source IP & port ● Destination IP & port With the value of **Allow** for the **Action** setting, the matching traffic passes hrough the unit (to be routed to the destination). If the value of the **Action** setting is set to **Deny**, the matching traffic does not pass through the unit (and is discarded).
Event Logging	This setting specifies whether or not to log matched firewall events. The logged messages are shown on the page **Status>Event Log**. A sample message is as follows: Aug 13 23:47:44 Denied CONN=Ethernet WAN SRC=20.3.2.1 DST=192.168.1.20 LEN=48 PROTO=TCP SPT=2260 DPT=80 ● **CONN:** The connection where the log entry refers to ● **SRC:** Source IP address ● **DST:** Destination IP address ● **LEN:** Packet length ● **PROTO:** Protocol ● **SPT:** Source port ● **DPT:** Destination port

Click **Save** to store your changes. To create an additional firewall rule, click **Add Rule** and repeat the above steps.

To change a rule's priority, simply drag and drop the rule:

- Hold the left mouse button on the rule.
- Move it to the desired position.
- Drop it by releasing the mouse button.



Outbound Firewall Rules (Drag and drop rows to change rule order)

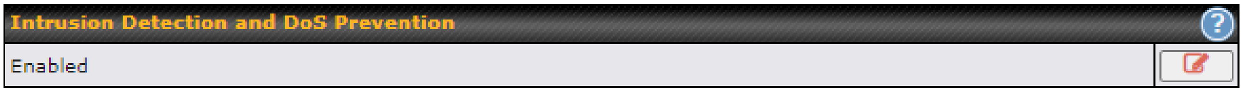
Rule	Protocol	Source IP Port	Destination IP Port	Policy	
No web access	TCP	Any Any	Any 80	Deny	✖
No FTP access	P	Any Any	Any 21	Deny	✖
Default	Any	Any	Any	Allow	

To remove a rule, click the ✖ button.

Rules are matched from top to the bottom. If a connection matches any one of the upper rules, the matching process will stop. If none of the rules match the connection, the **Default rule** will be applied.

The **Default rule** is **Allow** for Outbound, Inbound and Internal Network access.

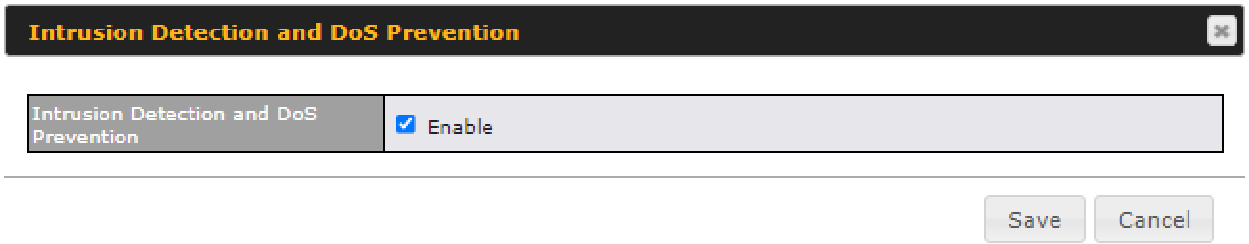
Intrusion Detection and DoS Prevention



Intrusion Detection and DoS Prevention

Enabled	✎

The Intrusion Detection and DoS Prevention can detect and prevent intrusions and denial-of-service (DoS) attacks from the Internet. To turn on this feature, click ✎, check the **Enable** check box for the **Intrusion Detection and DoS Prevention**, and press the **Save** button.



Intrusion Detection and DoS Prevention

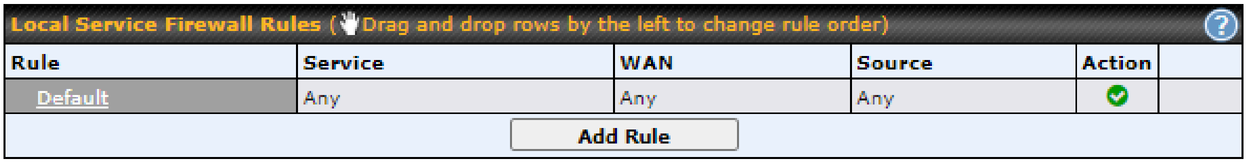
Intrusion Detection and DoS Prevention	☑ Enable

When this feature is enabled, the unit will detect and prevent the following kinds of intrusions and denial-of-service attacks.

- Port scan
  - NMAP FIN/URG/PSH
  - Xmas tree
  - Another Xmas tree
  - Null scan
  - SYN/RST
  - SYN/FIN
- SYN flood prevention
- Ping flood attack prevention

Local Service Firewall Rules

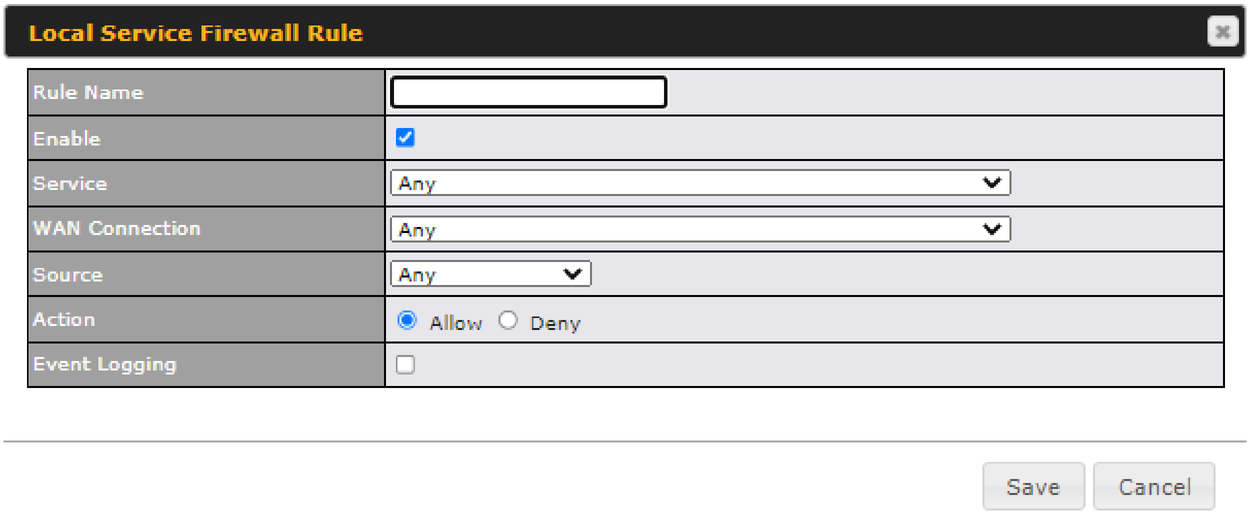
This table displays all the configured local service firewall rules and their details which are located at **Advanced > Firewall > Access Rules**. For every WAN inbound traffic to local service, rules will be matched to take the defined action.



Local Service Firewall Rules (Drag and drop rows by the left to change rule order)

Rule	Service	WAN	Source	Action
Default	Any	Any	Any	✓

Click **Add Rule** to display the following window:

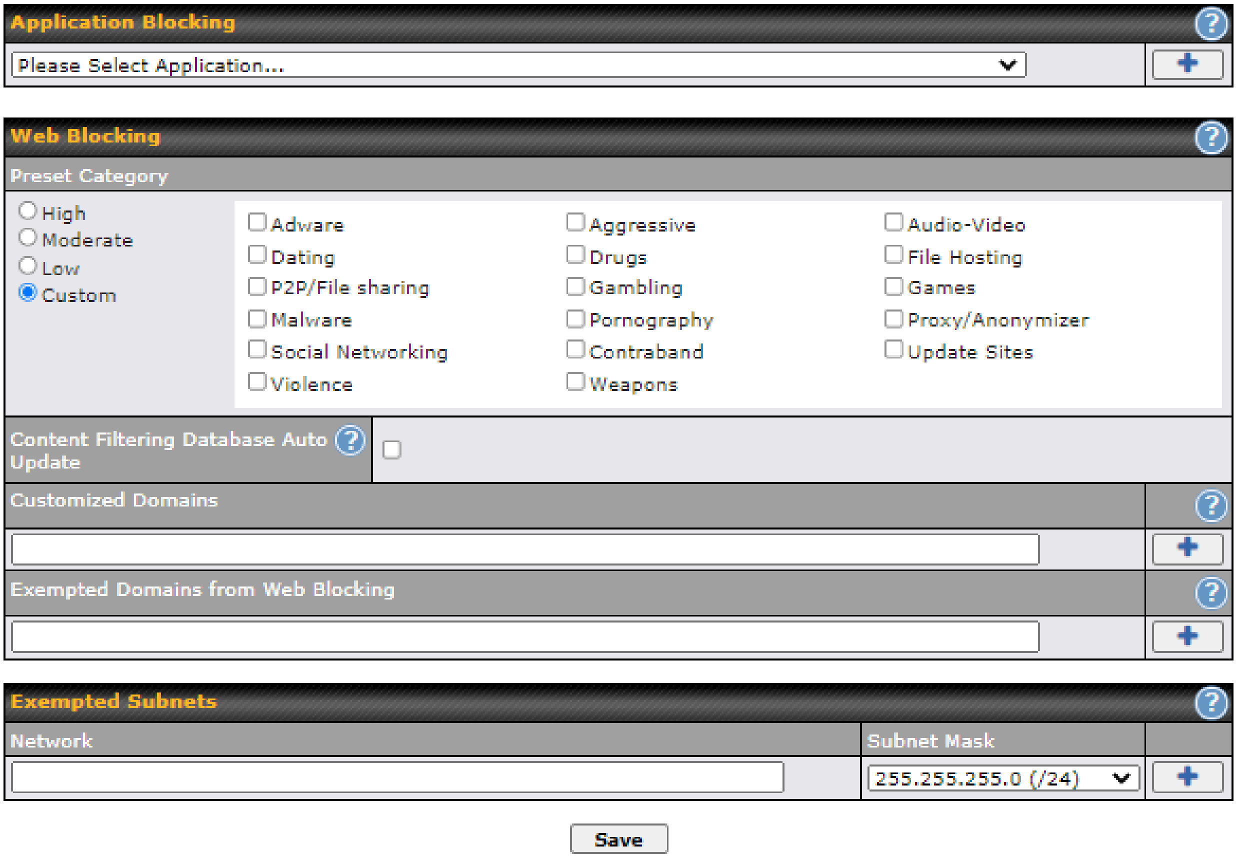


Local Service Firewall Rule

Rule Name	
Enable	☑
Service	Any
WAN Connection	Any
Source	Any
Action	● Allow ○ Deny
Event Logging	□

Local Service Firewall Settings	
Rule Name	This setting specifies a name for the firewall rule.
Enable	This setting specifies whether the firewall rule should take effect. If the box is checked, the firewall rule takes effect. If the traffic matches the specified Service/Source, action will be taken by this unit based on the other parameters of the rule. If the box is not checked, the firewall rule does not take effect. The unit will disregard the other parameters of the rule.
Service	This settings allows you to select the local service. If choosing **Any** means including all below services. ● SpeedFusion / PepVPN Handshake ● SpeedFusion / PepVPN Data port ● DNS ● SNMP server
WAN Connection	Select the WAN connection that this firewall rule should apply to.
Source	This specifies the source IP address(es) to be matched for the firewall rule.
Action	With the value of **Allow** for the **Action** setting, the matching traffic passes through the unit. If the value of the **Action** setting is set to **Deny**, the matching traffic does not pass through the unit.

9.2. Content Blocking



Application Blocking

Please Select Application...

Web Blocking

Preset Category

○ High
○ Moderate
○ Low
● Custom

□ Adware
□ Dating
□ P2P/File sharing
□ Malware
□ Social Networking
□ Violence
□ Aggressive
□ Drugs
□ Gambling
□ Pornography
□ Contraband
□ Weapons
□ Audio-Video
□ File Hosting
□ Games
□ Proxy/Anonymizer
□ Update Sites

Content Filtering Database Auto Update □

Customized Domains

Exempted Domains from Web Blocking

Exempted Subnets

Network	Subnet Mask
	255.255.255.0 (/24)

Application Blocking

Choose applications to be blocked from LAN/PPTP/PepVPN peer clients' access, except for those on the Exempted User Groups or Exempted Subnets defined below.

Web Blocking

Defines website domain names to be blocked from LAN/PPTP/PepVPN peer clients' access except for those on the Exempted User Groups or Exempted Subnets defined below.
If "foobar.com" is entered, any web site with a host name ending in foobar.com will be blocked, e.g. www.foobar.com, foobar.com, etc. However, "myfoobar.com" will not be blocked.

You may enter the wild card ".*" at the end of a domain name to block any web site with a host name having the domain name in the middle. For example, If you enter "foobar.*," then "www.foobar.com," "www.foobar.co.jp," or "foobar.co.uk" will be blocked. Placing the wild card in any other position is not supported.

The Peplink FusionHub will inspect and look for blocked domain names on all HTTP traffic. Secure web (HTTPS) traffic is not supported.

Customized Domains

You may enter the wild card ".*" at the end of a domain name to block any web site with a host name having the domain name in the middle. For example, If you enter "foobar.*," then "www.foobar.com," "www.foobar.co.jp," or "foobar.co.uk" will be blocked. Placing the wild card in any other position is not supported.

The Peplink FusionHub will inspect and look for blocked domain names on all HTTP traffic. Secure web (HTTPS) traffic is not supported.

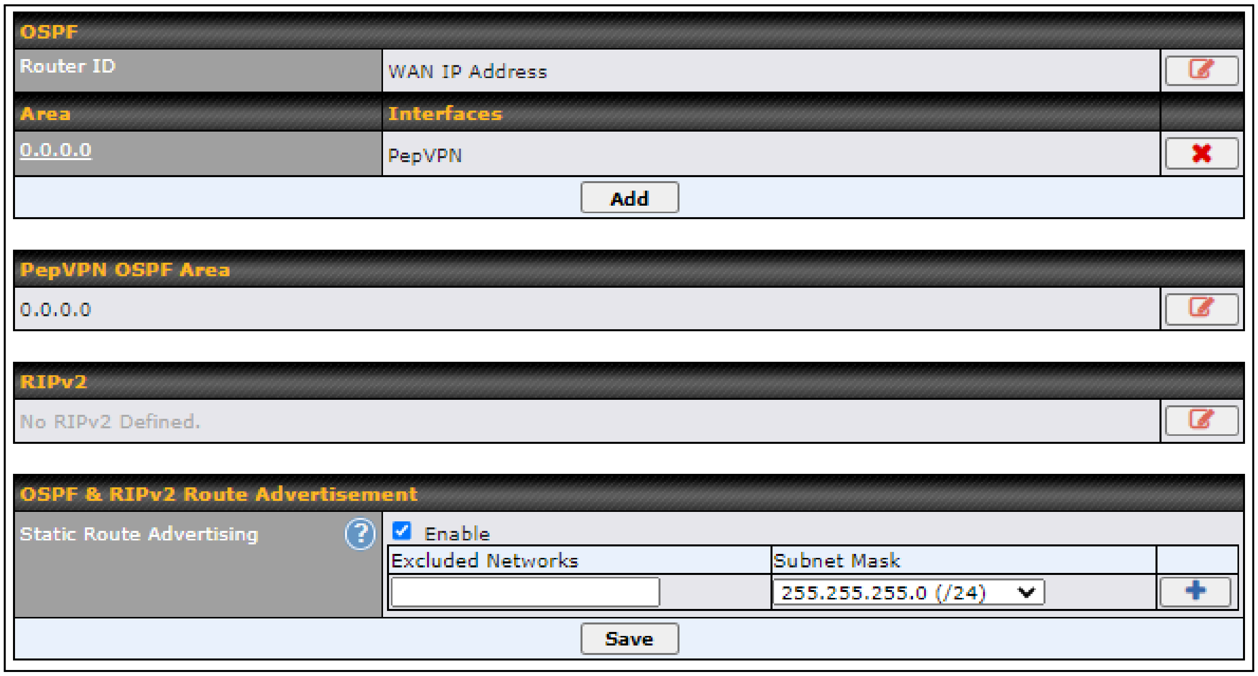
Exempted Subnets

With the subnet defined in the field, clients on the particular subnet(s) can be exempted from the access blocking rules.

10. Routing Protocol

10.1. OSPF & RIPv2

FusionHub supports OSPF and RIPv2 dynamic routing protocols. Click the **Advanced** tab along the top bar, and then click the **Routing Protocols > OSPF & RIPv2** item on the sidebar to reach the following menu:



OSPF

Router ID	WAN IP Address	
Area	**Interfaces**	
0.0.0.0	PepVPN	✖

Add

PepVPN OSPF Area

0.0.0.0

RIPv2

No RIPv2 Defined.

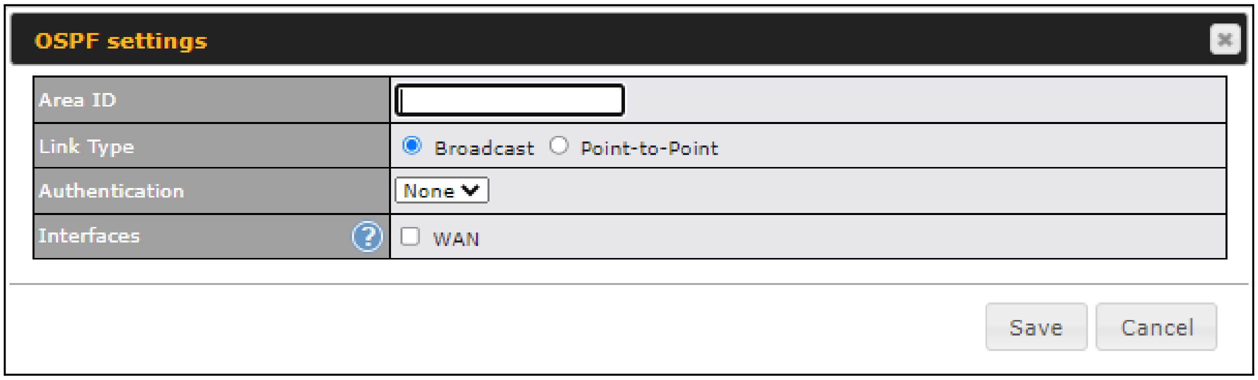
OSPF & RIPv2 Route Advertisement

Static Route Advertising ? ☑ Enable

Excluded Networks	Subnet Mask	
	255.255.255.0 (/24)	+

Save

OSPF	
Router ID	This field determines the ID of the router. By default, this is specified as the WAN IP address. If you want to specify your own ID, enter it into the **Custom** field.
Area	This is an overview of the OSPF areas that you have defined. Clicking on the name under **Area** allows you to configure the connection. To define a new area, click **Add**. To delete an existing area, click on the ✖.

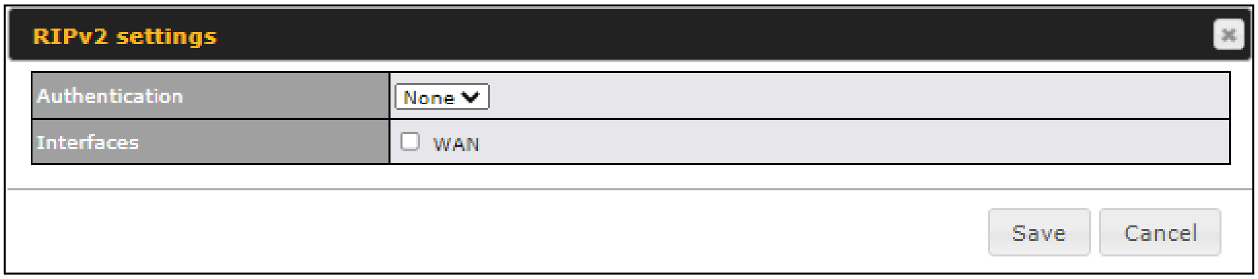


OSPF settings

Area ID	
Link Type	● Broadcast ○ Point-to-Point
Authentication	None
Interfaces	□ WAN

OSPF Settings	
Area ID	Assign a name to be applied to this group. Machines linked to this group will send and receive related OSPF packets, while unlinked machines will ignore them.
Link Type	Choose the type of network that this area will use.
Authentication	If an authentication method is used, select one from this drop-down menu. Available options are **MD5** and **Text**. Authentication key(s) may be input next to the drop-down menu after selecting an authentication method.
Interfaces	Select the interface(s) that this area will use to listen to and deliver OSPF packets.

To access RIPv2 settings, click on .

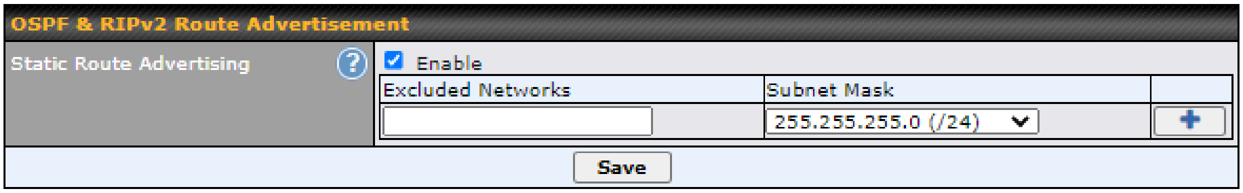


RIPv2 settings

Authentication	None
Interfaces	□ WAN

RIPv2 Settings	
Authentication	If an authentication method is used, select one from this drop-down menu. Available options are **MD5** and **Text**. Authentication key(s) may be input next to the drop-down menu after selecting an authentication method.
Interfaces	Select the interface(s) that this area will use to listen to and deliver RIPv2 packets.

Enabling OSPF & RIPv2 Route Advertising allows it to advertise LAN static routes over OSPF & RIPv2. Static routes on the Excluded Networks table will not be advertised.



OSPF & RIPv2 Route Advertisement

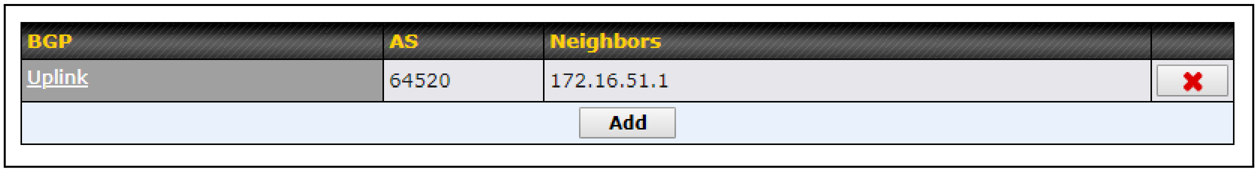
Static Route Advertising ?	☑ Enable

Excluded Networks	Subnet Mask	
	255.255.255.0 (/24)	+

Save

10.2. BGP

Click the **Advanced** tab along the top bar, and then click the **BGP** item on the sidebar to configure BGP.

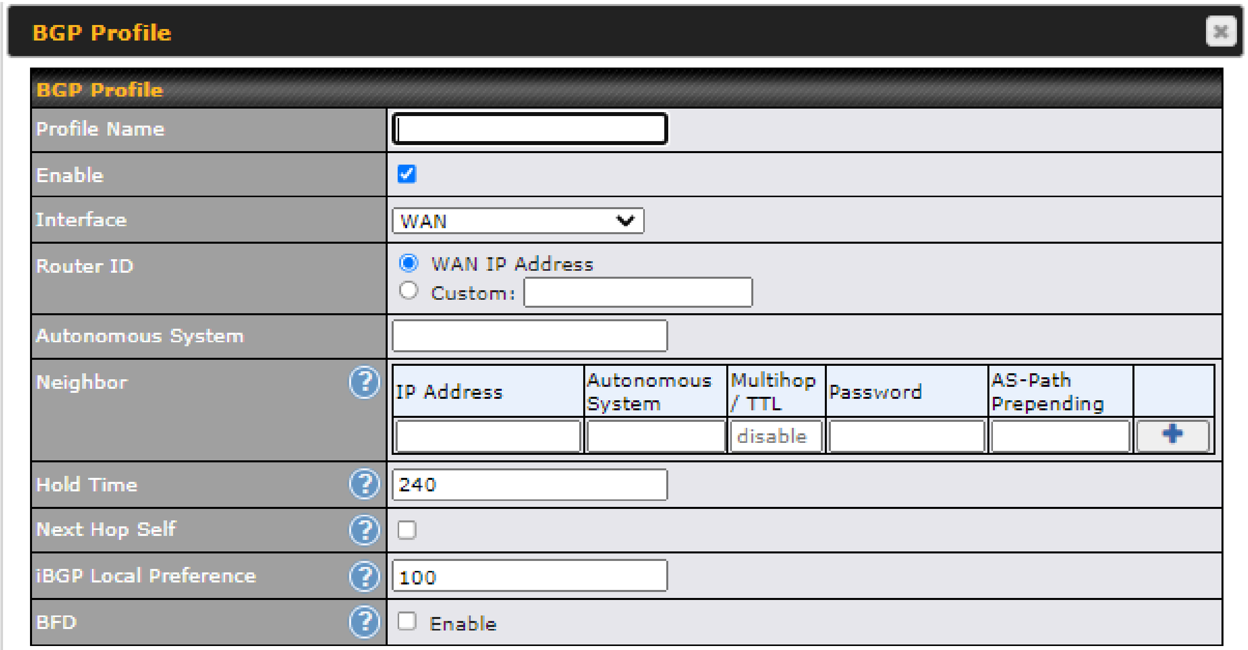


BGP	AS	Neighbors	
Uplink	64520	172.16.51.1	✖

Add

Click the "x" to delete a BGP profile.

Click "**Add**" to create a new BGP profile.



BGP Profile

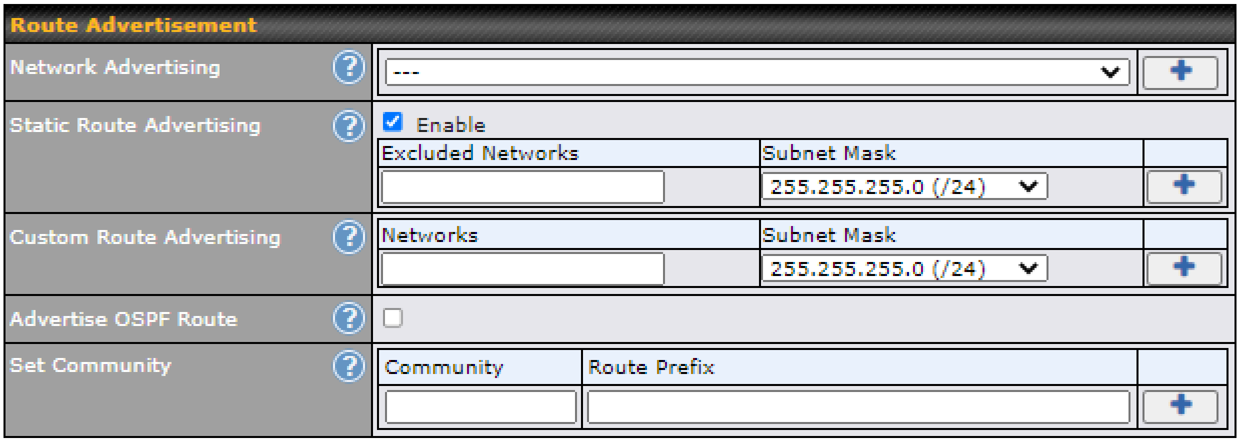
BGP Profile	
Profile Name	
Enable	☑
Interface	WAN
Router ID	● WAN IP Address ○ Custom:
Autonomous System	
Neighbor ?	
Hold Time ?	240
Next Hop Self ?	□
iBGP Local Preference ?	100
BFD ?	□ Enable

Neighbor:

IP Address	Autonomous System	Multihop / TTL	Password	AS-Path Prepending	
		disable			+

BGP	
Name	This field specifies the name that represents this profile.
Enable	When this box is checked, this BGP profile will be enabled. If it is left unchecked, it will be disabled.
Interface	The interface in which the BGP neighbor is located.
Autonomous System	The Autonomous System Number (ASN) assigned to this profile.
Neighbor	BGP Neighbors and their details.
IP address	The IP address of the Neighbor.
Autonomous System	The Neighbor's ASN.
Multihop/TTL	This field determines the Time-to-live (TTL) of BGP packets. Leave this field blank if the BGP neighbor is directly connected, otherwise you must specify a TTL value. This option should be used if the configured Neighbor's IP address does not match the selected Interface's network subnets. The TTL value must be between 2 to 255.
Password	(Optional) Assign a password for MD5 authentication of BGP sessions.
AS-Path Prepending:	AS path to be prepended to the routes received from this Neighbor. Values must be ASN and separated by commas. For example: inputting "64530,64531" will prepend "64530, 64531" to received routes.
Hold Time	Wait time in seconds for a keepalive message from a Neighbor before considering the BGP connection as stalled. The value must be either 0 (infinite hold time) or between 3 and 65535 inclusively. Default: 240
Next Hop Self	Enable this option to advertise your own source address as the next hop when propagating routes.
iBGP Local Preference	This is the metric advertised to iBGP Neighbors to indicate the preference for external routes. The value must be between 0 to 4294967295 inclusively. Default: 100
BFD	Enable this option to add Bidirectional Forwarding Detection to detect path failures. All directly connected Neighbors that use the same physical interface share the same BFD settings. All multihop Neighbors share the

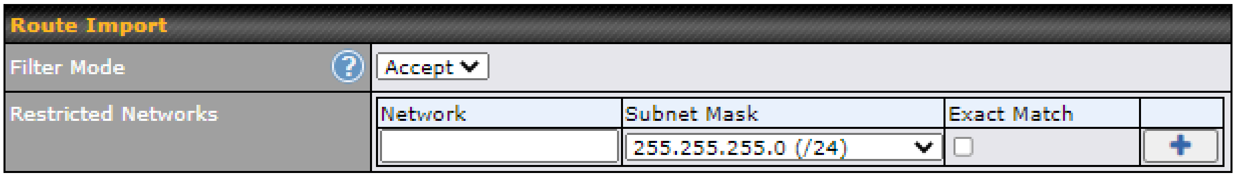
	same multihop BFD settings. You can configure BFD settings in the BGP profile listing page after this option is enabled.



Route Advertisement	
Network Advertising	--- ▾ +
Static Route Advertising	☑ Enable Excluded Networks / Subnet Mask: 255.255.255.0 (/24) ▾ +
Custom Route Advertising	Networks / Subnet Mask: 255.255.255.0 (/24) ▾ +
Advertise OSPF Route	□
Set Community	Community / Route Prefix +

Route Advertisement	
Network Advertising	Select the networks that will be advertised to BGP Neighbors.
Static Route Advertising	Enable this option to advertise static LAN routes. Static routes that match the Excluded Networks table will not be advertised.
Custom Route Advertising	Additional routes to be advertised to the BGP Neighbor.
Advertise OSPF Route	When this box is checked, every learnt OSPF route will be advertised.
Set Community	Assign a prefix to a Community. Community: Two numbers in new-format. e.g. 65000:21344 Well-known communities: no-export 65535:65281 no-advertise 65535:65282 no-export-subconfed 65535:65283 no-peer 65535:65284

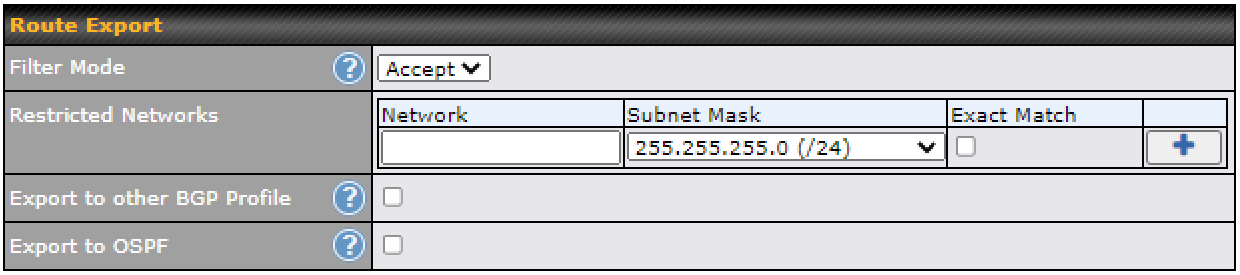
	Route Prefix: Comma separated networks. e.g. 172.168.1.0/24,192.168.1.0/28



Route Import

Filter Mode	Accept			
Restricted Networks	Network	Subnet Mask	Exact Match	
		255.255.255.0 (/24)	□	+

Route Import Settings	
Filter Mode	This field allows for the selection of the filter mode for route import. **None**: All BGP routes will be accepted. **Accept**: Routes in "Restricted Networks" will be accepted, routes not in the list will be rejected. **Reject**: Routes in "Restricted Networks" will be rejected, routes not in the list will be accepted.
Restricted Networks	This field specifies the network(s) in the “route import” entry. **Exact Match:** When this box is checked, only routes with the same Network and Subnet Mask will be filtered. Otherwise, routes within the Networks and Subnets will be filtered.



Route Export

Filter Mode	Accept			
Restricted Networks	Network	Subnet Mask	Exact Match	
		255.255.255.0 (/24)	□	+
Export to other BGP Profile	□			
Export to OSPF	□			

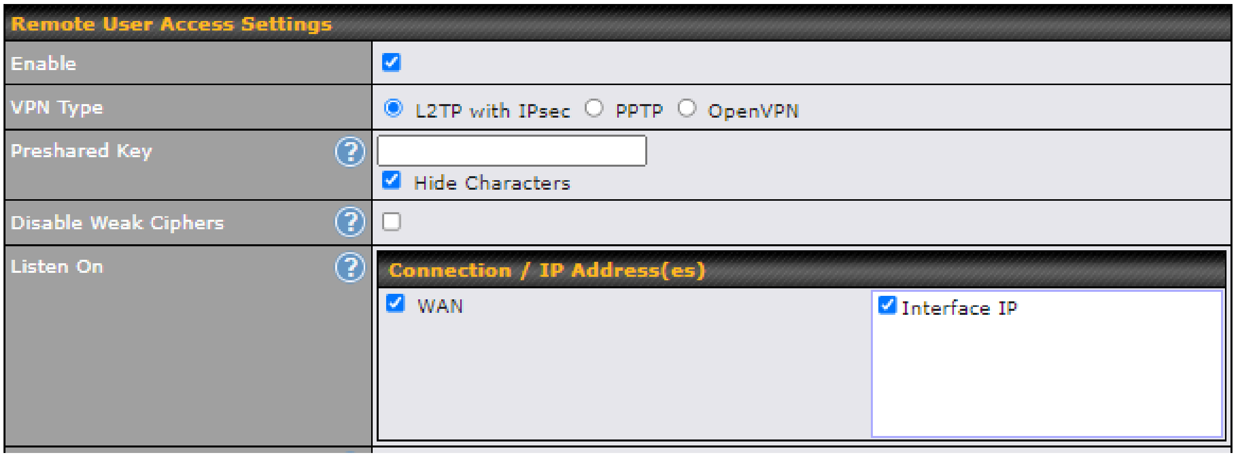
Route Export Settings	
Filter Mode	This field allows for the selection of the filter mode for route export. **None**: All BGP routes will be accepted. **Accept**: Routes in "Restricted Networks" will be accepted, routes not in the list will be rejected. **Reject**: Routes in "Restricted Networks" will be rejected, routes not in the

	list will be accepted.
Restricted Networks	This field specifies the network(s) in the “route export” entry. **Exact Match:** When this box is checked, only routes with the same Network and Subnet Mask will be filtered. Otherwise, routes within the Networks and Subnets will be filtered.
Export to other BGP Profile	When this box is checked, routes learnt from this BGP profile will be exported to other BGP profiles.
Export to OSPF	When this box is checked, routes learnt from this BGP profile will be exported to the OSPF routing protocol.

11. Remote User Access

A remote-access VPN connection allows an individual user to connect to a private business network from a remote location using a laptop or desktop computer connected to the Internet. It can be remotely accessed via OpenVPN, L2TP with IPsec or PPTP. To configure this feature, navigate to **Advanced > Remote User Access** and choose the required VPN type.

11.1. L2TP with IPsec

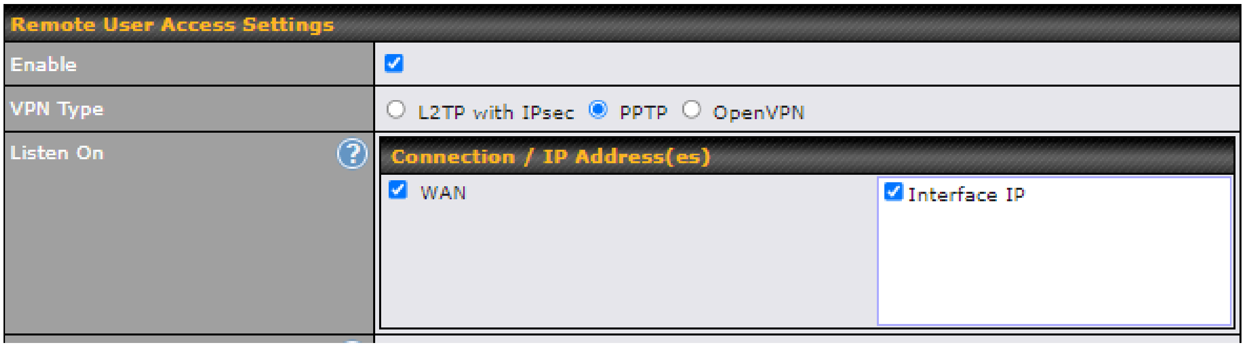


Remote User Access Settings

Enable	☑
VPN Type	● L2TP with IPsec ○ PPTP ○ OpenVPN
Preshared Key ?	☑ Hide Characters
Disable Weak Ciphers ?	□
Listen On ?	**Connection / IP Address(es)** ☑ WAN ☑ Interface IP

L2TP with IPsec Remote User Access Settings	
Pre-shared Key	Enter your preshared key in the text field. Please note that remote devices will need this preshared key to access the Balance.
Disable Weak Ciphers	Click the ? button to show and enable this option. When checked, weak ciphers such as 3DES will be disabled.
Listen On	This setting is for specifying the WAN IP addresses where the PPTP server of the router should listen on.

11.2. PPTP



Remote User Access Settings

Enable ☑

VPN Type ○ L2TP with IPsec ● PPTP ○ OpenVPN

Listen On

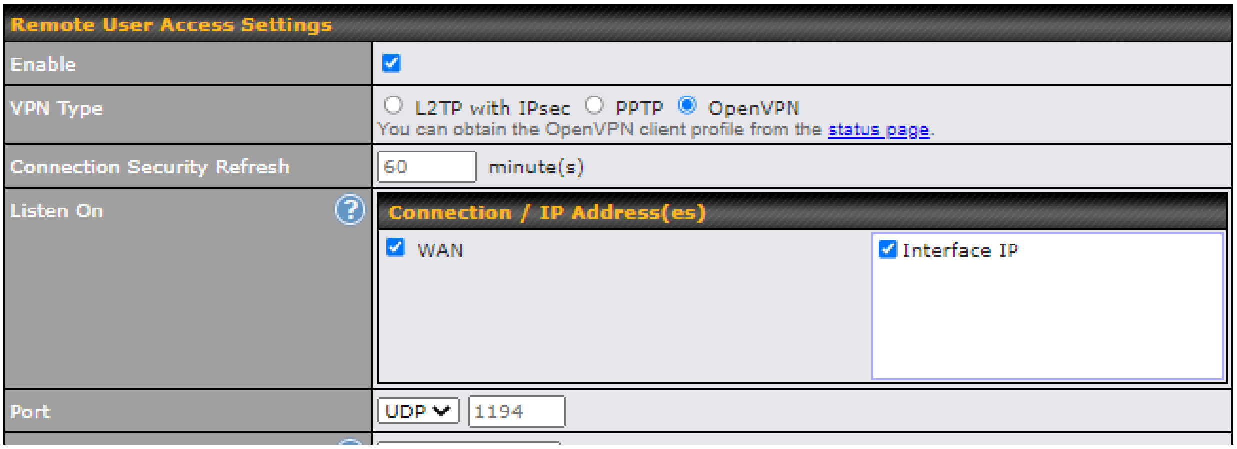
Connection / IP Address(es)	
☑ WAN	☑ Interface IP

No additional configuration required.

The Point-to-Point Tunneling Protocol (PPTP) is an obsolete method for implementing virtual private networks. PPTP has many well known security issues

Continue to configure authentication methods.

11.3. OpenVPN



Remote User Access Settings

Enable ☑

VPN Type ○ L2TP with IPsec ○ PPTP ● OpenVPN
You can obtain the OpenVPN client profile from the status page.

Connection Security Refresh 60 minute(s)

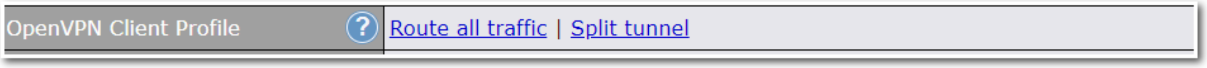
Listen On

Connection / IP Address(es)	
☑ WAN	☑ Interface IP

Port UDP 1194

Select OpenVPN and continue to configure the authentication method.

The OpenVPN Client profile can be downloaded from the **Status > device** page after the configuration has been saved.



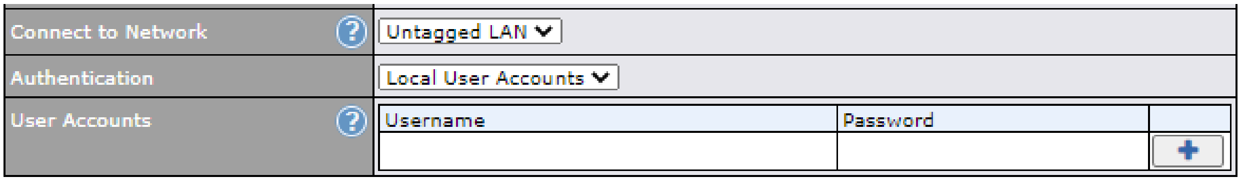
OpenVPN Client Profile Route all traffic | Split tunnel

You have a choice between 2 different OpenVPN Client profiles:

Option 1: "Route all traffic" profile
Using this profile, VPN clients will send all the traffic through the OpenVPN tunnel

Option 2: "Split tunnel" profile
Using this profile, VPN clients will ONLY send those traffic designated to the untagged LAN and VLAN segment through the OpenVPN tunnel.

11.4. Authentication Method

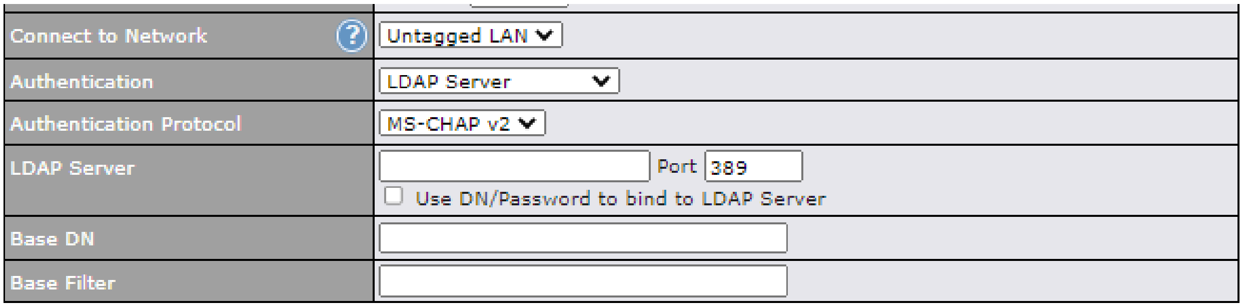


Connect to Network	Untagged LAN
Authentication	Local User Accounts
User Accounts	Username | Password | +

Authentication Method	
Connect to Network	Users establish VPN connection to the selected network require a DHCP server to offer IP addresses to them. You can either use a standalone DHCP server, or use the internal DHCP server of the selected network.
Authentication	Determine the method of authenticating remote users
User Accounts	This setting allows you to define User Accounts. Click Add to input username and password to create an account. After adding the user accounts, you can click on a username to edit the account password.

Note:
The username must contain lowercase letters, numerics, underscore(_), dash(-), at sign(@), and period(.) only.
The password must be between 8 and 12 characters long.

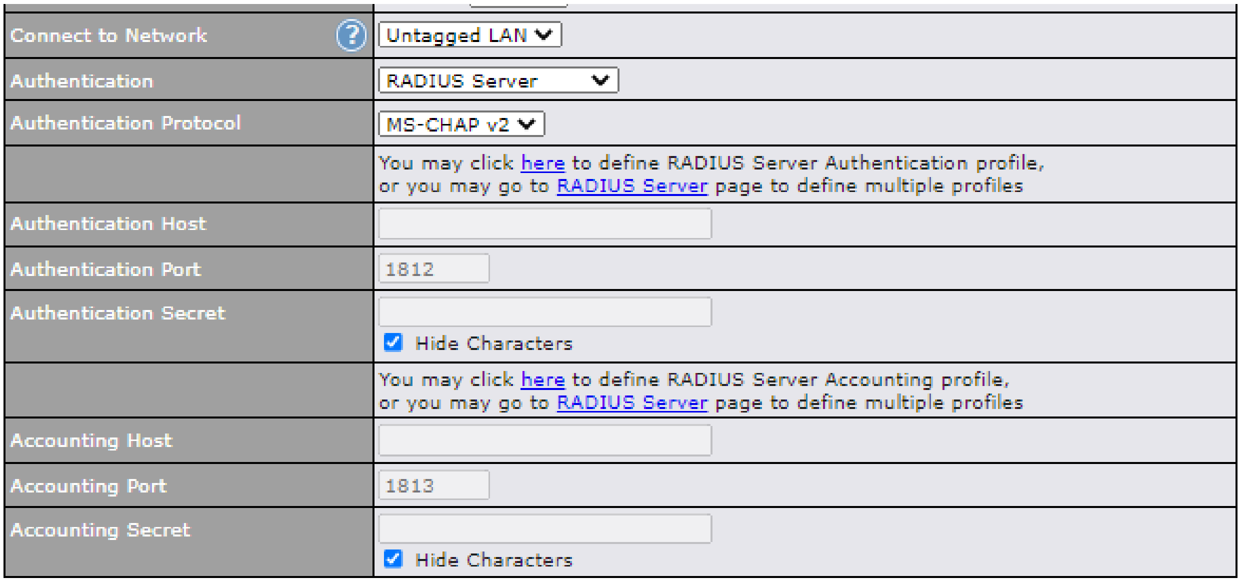
LDAP Server



Connect to Network	Untagged LAN
Authentication	LDAP Server
Authentication Protocol	MS-CHAP v2
LDAP Server	Port 389 □ Use DN/Password to bind to LDAP Server
Base DN	
Base Filter	

Enter the matching LDAP server details to allow for LDAP server authentication.

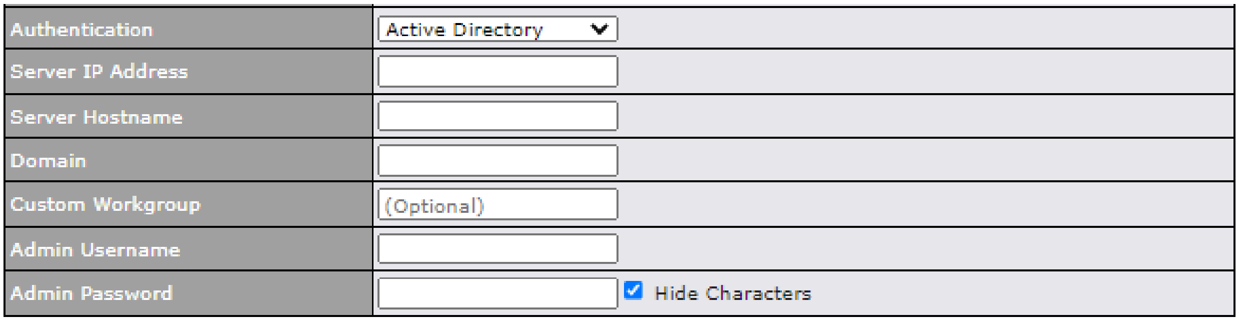
Radius Server



Connect to Network	Untagged LAN
Authentication	RADIUS Server
Authentication Protocol	MS-CHAP v2
	You may click here to define RADIUS Server Authentication profile, or you may go to RADIUS Server page to define multiple profiles
Authentication Host	
Authentication Port	1812
Authentication Secret	☑ Hide Characters
	You may click here to define RADIUS Server Accounting profile, or you may go to RADIUS Server page to define multiple profiles
Accounting Host	
Accounting Port	1813
Accounting Secret	☑ Hide Characters

Enter the matching Radius server details to allow for Radius server authentication.

Active Directory



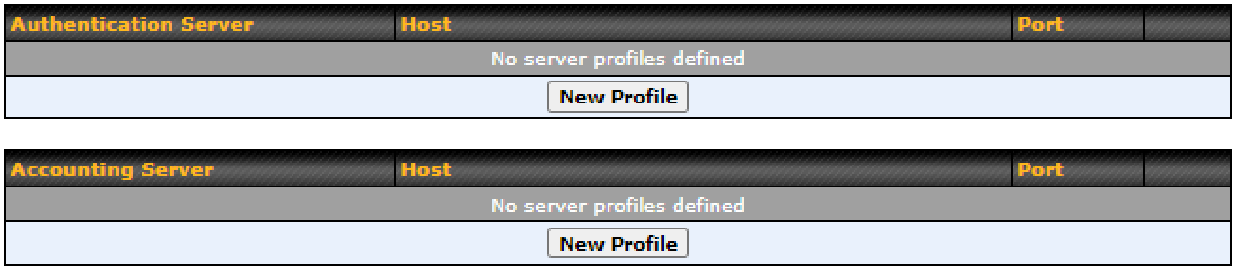
Authentication	Active Directory
Server IP Address	
Server Hostname	
Domain	
Custom Workgroup	(Optional)
Admin Username	
Admin Password	☑ Hide Characters

Enter the matching Active Directory details to allow for Active Directory server authentication.

12. Mics. Settings

12.1. RADIUS Server

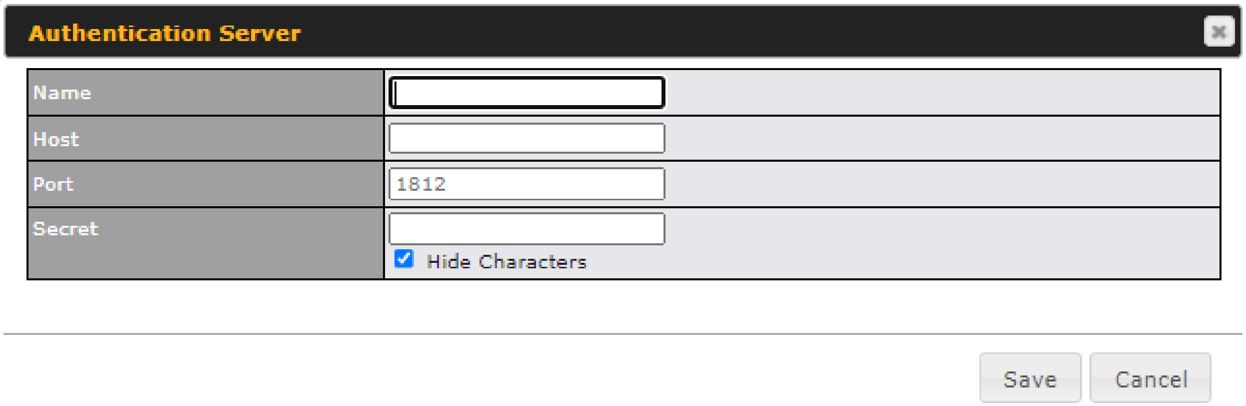
This section is to configure the RADIUS server profile, navigate to **Advanced > Misc. Settings > RADIUS Server**.



Authentication Server	Host	Port
No server profiles defined		
New Profile		

Accounting Server	Host	Port
No server profiles defined		
New Profile		

Authentication Server

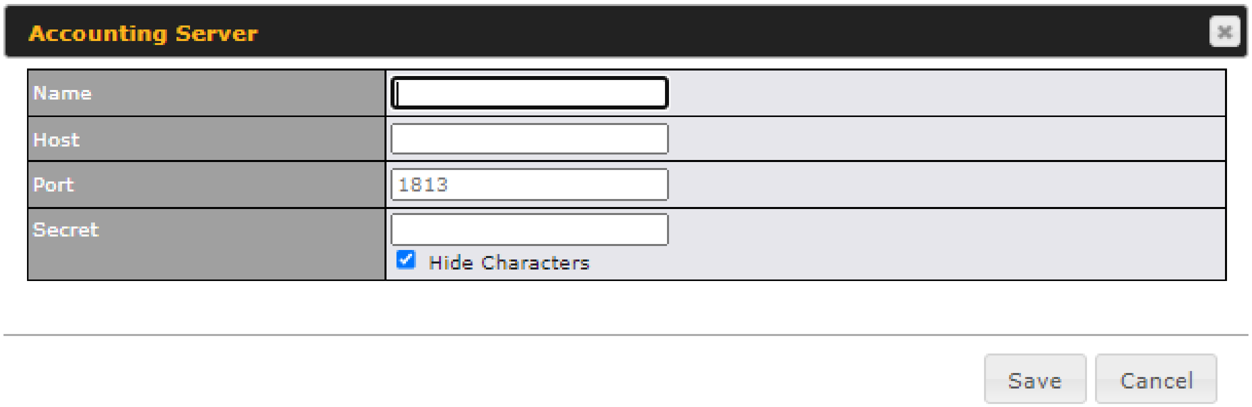


Authentication Server

Name	
Host	
Port	1812
Secret	 ☑ Hide Characters

Authentication Server Settings	
Name	Enter the name of the RADIUS Authentication Server.
Host	Enter the IP address of the RADIUS Authentication Server.
Port	In the field, enter the UDP authentication port(s) used by your RADIUS server(s). The default: 1812.
Secret	Enter the RADIUS shared secret for the Authentication Server.

Accounting Server

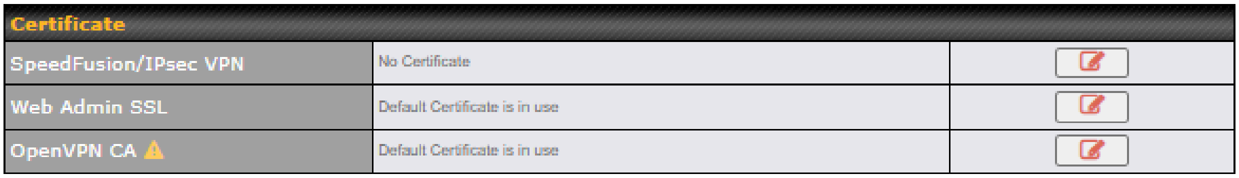


Accounting Server

Name	
Host	
Port	1813
Secret	 ☑ Hide Characters

Accounting Server Settings	
Name	Enter the name of the RADIUS Accounting Server.
Host	Enter the IP address of the RADIUS Accounting Server.
Port	In the field, enter the UDP accounting port(s) used by your RADIUS server(s). The default: 1813.
Secret	Enter the RADIUS shared secret for the Accounting Server.

12.2. Certification Manager



Certificate		
SpeedFusion/IPsec VPN	No Certificate	
Web Admin SSL	Default Certificate is in use	
OpenVPN CA ⚠	Default Certificate is in use	

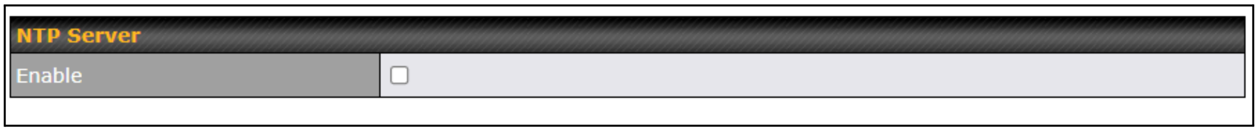
This section allows you to assign certificates for the local VPN, OpenVPN, and web admin SSL for extra security.

Read the following knowledgebase article for full instructions on how to create and import a self-signed certificate:

https://forum.peplink.com/t/how-to-create-a-self-signed-certificate-and-import-it-to-a-peplink-product/

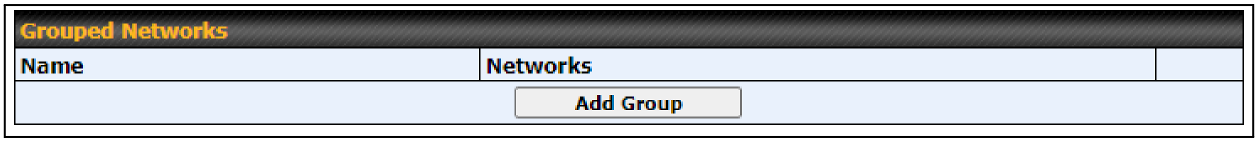
12.3. NTP

Now, the unit can serve as a local NTP server. Upon start up, it is now able to provide connected devices with the accurate time, precise UTC from either an external NTP server or via GPS and ensuring that connected devices always receive the correct time. NTP Server settings can be found via: **Advanced > Misc. Settings > NTP Server.**



NTP Server	
Enable	□

12.4. Grouped Networks

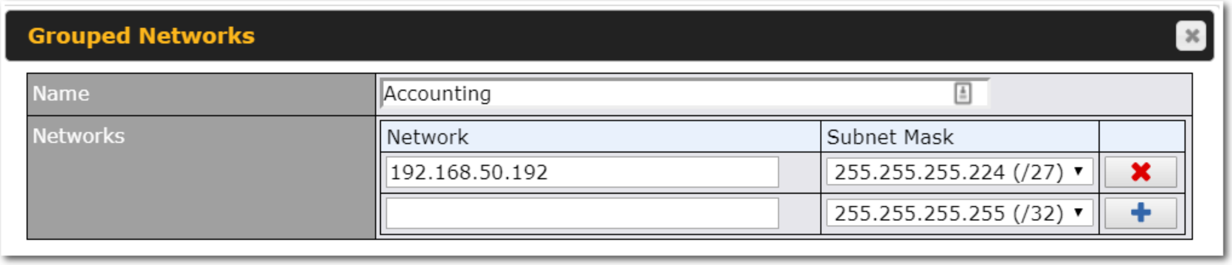


Grouped Networks

Name	Networks	
	Add Group	

Using “Grouped Networks” you can group and name a range of IP addresses, which can then be used to define firewall rules or outbound policies.

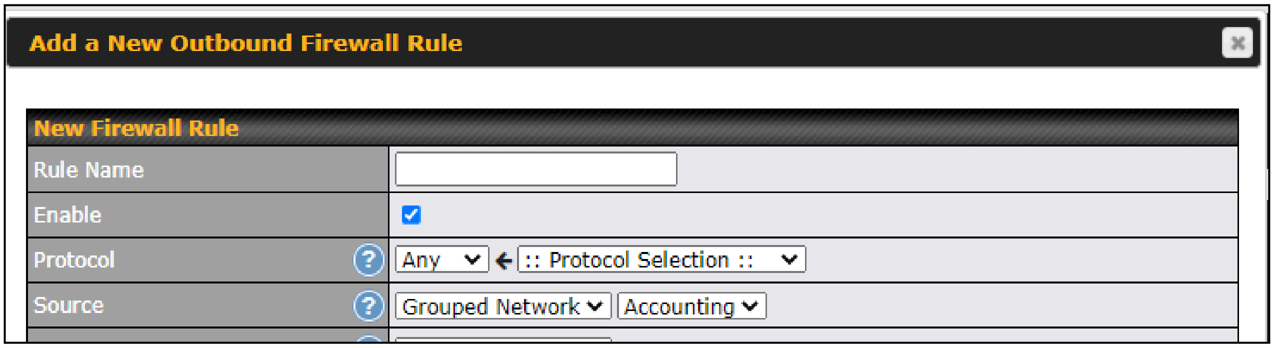
Start by clicking on “add group” then fill in the appropriate field. In this example we’ll create a group “Accounting” Click save when you have finished adding the required networks.



Grouped Networks

Name	Accounting
Networks	Network: 192.168.50.192 — Subnet Mask: 255.255.255.224 (/27) Network: (empty) — Subnet Mask: 255.255.255.255 (/32)

The grouped network “*Accounting*” can now be used to configure a firewall rule.



Add a New Outbound Firewall Rule

New Firewall Rule	
Rule Name	
Enable	☑
Protocol	Any ← :: Protocol Selection ::
Source	Grouped Network, Accounting

13. System Tab

13.1. System

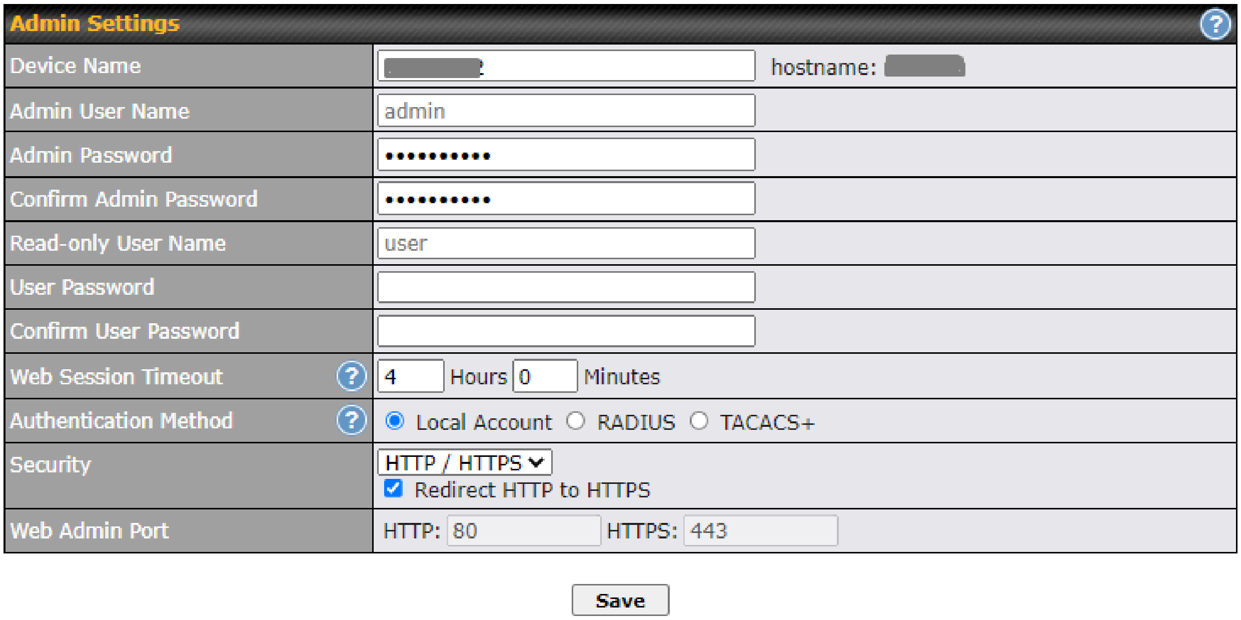
13.1.1. Admin Security

There are two types of user accounts available for accessing the web admin: *admin* and *user*. They represent two user levels: the admin level has full administrative access, while the user level is read-only. The user level can access only the device's status information; users cannot make any changes on the device.

A web login session will be logged out automatically when it has been idle longer than the **Web Session Timeout**. Before the session expires, you may click the **Logout** button in the web admin to exit the session.

0 hours 0 minutes signifies an unlimited session time. This setting should be used only in special situations, as it will lower the system security level if users do not log out before closing the browser. The **default** is 4 hours, 0 minutes.

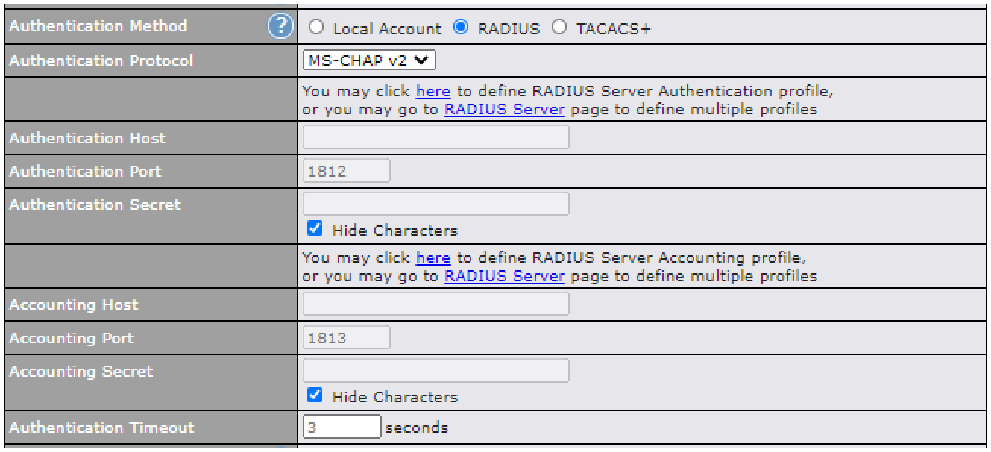
For security reasons, after logging in to the web admin Interface for the first time, it is recommended to change the administrator password. Configuring the administration interface to be accessible only from the LAN can further improve system security. Administrative settings configuration is located at **System > Admin Security**.



Admin Settings

Device Name	[redacted] hostname: [redacted]
Admin User Name	admin
Admin Password	••••••••••
Confirm Admin Password	••••••••••
Read-only User Name	user
User Password	
Confirm User Password	
Web Session Timeout	4 Hours 0 Minutes
Authentication Method	● Local Account ○ RADIUS ○ TACACS+
Security	HTTP / HTTPS ☑ Redirect HTTP to HTTPS
Web Admin Port	HTTP: 80 HTTPS: 443

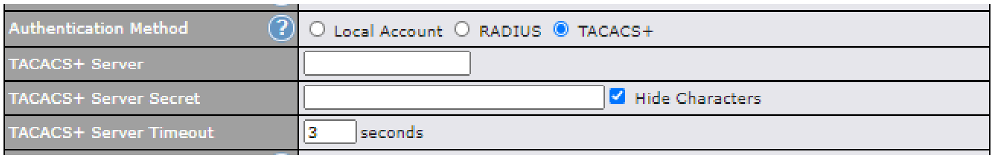
Admin Settings	
Device Name	This field allows you to define a name for this Pepwave router. By default, **Device Name** is set as **FSH_XXXX**, where *XXXX* refers to the last 4 digits of the unit's serial number.
Admin User Name	**Admin User Name** is set as *admin* by default, but can be changed, if desired.
Admin Password	*This field allows you to specify a new administrator password.
Confirm Admin Password	This field allows you to verify and confirm the new administrator password.
Read-only User Name	**Read-only User Name** is set as *user* by default, but can be changed, if desired.
Read-only Password	This field allows you to specify a new user password. Once the user password is set, the read-only user feature will be enabled.
Confirm Read-only Password	This field allows you to verify and confirm the new user password.
Web Session Timeout	This field specifies the number of hours and minutes that a web session can remain idle before the Pepwave router terminates its access to the web admin interface. By default, it is set to **4 hours**.
Authentication Method	With this box is checked, the web admin will authenticate using an external RADIUS server. Authenticated users are treated as either "admin" with full read-write permission or "user" with read-only access. Local admin and user accounts will be disabled. When the device is not able to communicate with the external RADIUS server, local accounts will be enabled again for emergency access. Additional authentication options will be available once this box is checked. Available options: ● Local Account ● RADIUS



Authentication Method	○ Local Account ● RADIUS ○ TACACS+
Authentication Protocol	MS-CHAP v2
	You may click here to define RADIUS Server Authentication profile, or you may go to RADIUS Server page to define multiple profiles
Authentication Host	
Authentication Port	1812
Authentication Secret	☑ Hide Characters
	You may click here to define RADIUS Server Accounting profile, or you may go to RADIUS Server page to define multiple profiles
Accounting Host	
Accounting Port	1813
Accounting Secret	☑ Hide Characters
Authentication Timeout	3 seconds

Authentication Protocol	This specifies the authentication protocol used. Available options are **MS-CHAP v2** and **PAP**.
Authentication Host	This specifies the IP address or hostname of the RADIUS server host.
Authentication Port	This setting specifies the UDP destination port for authentication requests.
Authentication Secret	This field is for entering the secret key for accessing the RADIUS server.
Accounting Host	This specifies the IP address or hostname of the RADIUS server host.
Accounting Port	This setting specifies the UDP destination port for accounting requests.
Accounting Secret	This field is for entering the secret key for accessing the accounting server.
Authentication Timeout	This option specifies the time value for authentication timeout

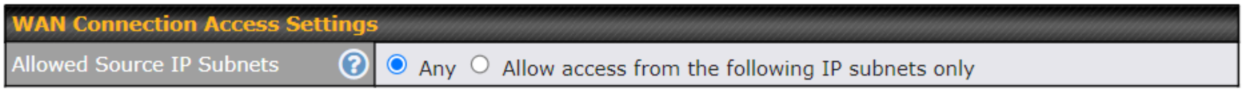
- TACACS+



Authentication Method	○ Local Account ○ RADIUS ● TACACS+
TACACS+ Server	
TACACS+ Server Secret	☑ Hide Characters
TACACS+ Server Timeout	3 seconds

<table>
<tr><td></td><td>
<table>
<tr><td><b>TACACS+ Server</b></td><td>This specifies the access address of the external TACACS+ server.</td></tr>
<tr><td><b>TACACS+ Server Secret</b></td><td>This field is for entering the secret key for accessing the RADIUS server.</td></tr>
<tr><td><b>TACACS+ Server Timeout</b></td><td>This option specifies the time value for TACACS+ timeout</td></tr>
</table>
</td></tr>
<tr><td><b>Security</b></td><td>This option is for specifying the protocol(s) through which the web admin interface can be accessed:
● HTTP
● HTTPS
● HTTP/HTTPS
HTTP to HTTPS redirection is enabled by default to force HTTPS access to the web admin interface.</td></tr>
<tr><td><b>Web Admin Access</b></td><td>This option is for specifying the network interfaces through which the web admin interface can be accessed:
● LAN only
● LAN/WAN
If LAN/WAN is chosen, the <b>WAN Connection Access Settings</b> form will be displayed.</td></tr>
<tr><td><b>Web Admin Port</b></td><td>This field is for specifying the port number on which the web admin interface can be accessed.</td></tr>
</table>

*We recommend changing the Admin Password every 3 months for security reasons.



WAN Connection Access Settings

Allowed Source IP Subnets ? ● Any ○ Allow access from the following IP subnets only

WAN Connection Access Settings	
Allowed Source IP Subnets	This field allows you to restrict web admin access only from defined IP subnets. ● **Any** - Allow web admin accesses to be from anywhere, without IP address restriction. ● **Allow access from the following IP subnets only** - Restrict web admin access only from the defined IP subnets. When this is chosen, a text input area will be displayed beneath:

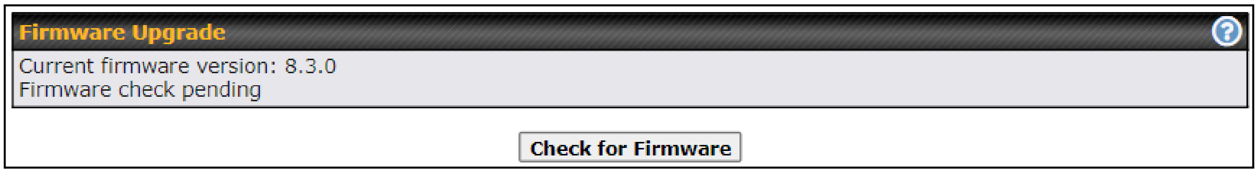
	The allowed IP subnet addresses should be entered into this text area. Each IP subnet must be in form of *w.x.y.z/m*, where *w.x.y.z* is an IP address (e.g., *192.168.0.0*), and *m* is the subnet mask in CIDR format, which is between 0 and 32 inclusively (For example, *192.168.0.0/24*). To define multiple subnets, separate each IP subnet one in a line. For example: ● 192.168.0.0/24 ● 10.8.0.0/16

13.1.2. Firmware

Upgrading firmware can be done in one of three ways:

- Using the FusionHub's interface to automatically check for an update,
- Using the FusionHub's interface to manually upgrade the firmware, or
- Using InControl2 to push an upgrade to a router.

The automatic upgrade can be done from **System** > **Firmware**.

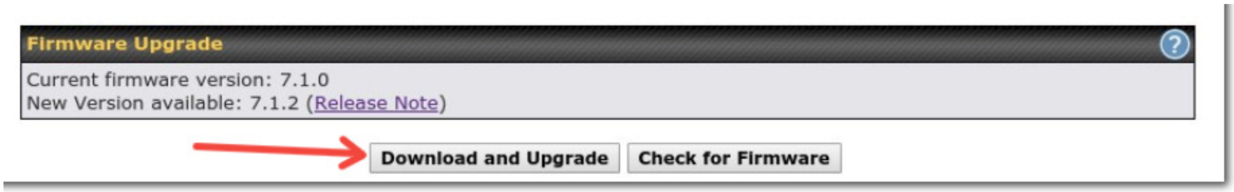


Firmware Upgrade

Current firmware version: 8.3.0
Firmware check pending

Web admin interface : Automatically check for updates

If an update is found the buttons will change to allow you to **Download and Update** the firmware.

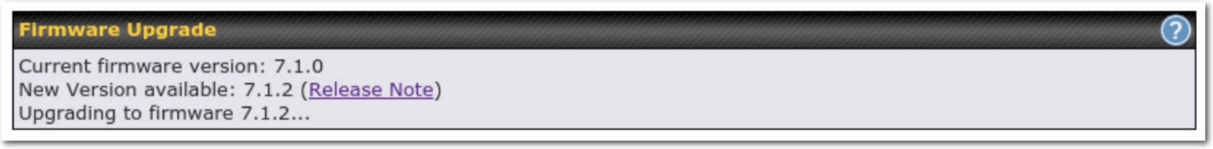


Firmware Upgrade

Current firmware version: 7.1.0
New Version available: 7.1.2 (Release Note)

Click on the **Download and Upgrade** button. A prompt will be displayed advising to download the Current Active Configuration. Please click on the underlined download text. After downloading the current config click the **Ok** button to start the upgrade process.

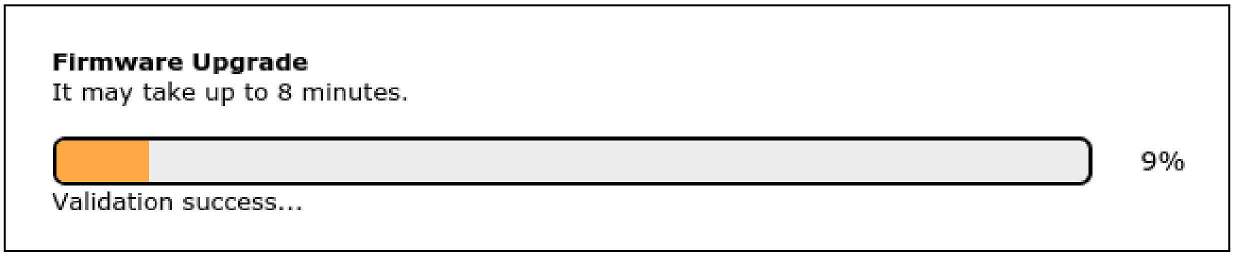
It will download and then apply the firmware. The time that this process takes will depend on your internet connection's speed.



Firmware Upgrade

Current firmware version: 7.1.0
New Version available: 7.1.2 (Release Note)
Upgrading to firmware 7.1.2...

The firmware will now be applied to the FusionHub*. The amount of time it takes for the firmware to upgrade will also depend on the router that's being upgraded.



Firmware Upgrade
It may take up to 8 minutes.

9%

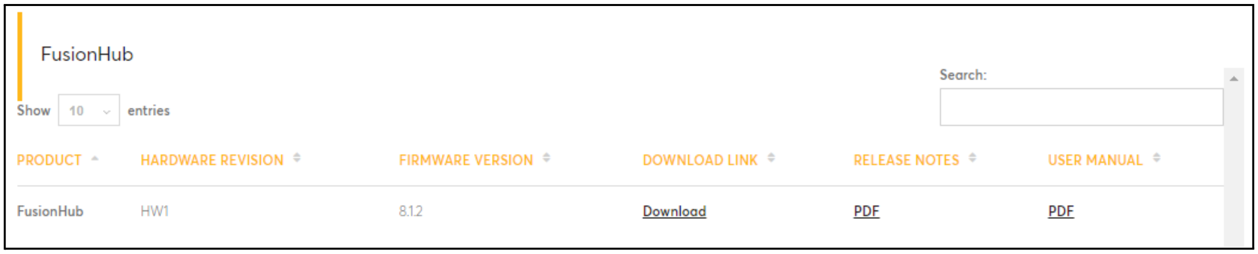
Validation success...

***Upgrading the firmware will cause the router to reboot.**

Web admin interface: Install updates manually

In some cases, a special build may be provided via a ticket or it may be found in the forum. Upgrading to the special build can be done using this method, or using IC2 if you are using that to manage your firmware upgrades. A manual upgrade using the GA firmware posted on the site may also be recommended or required for a couple of reasons.

All of the Peplink/Pepwave GA firmware can be found here Navigate to the relevant product line (ie. Balance, Max, FusionHub, SOHO, etc). Some product lines may have a dropdown that lists all of the products in that product line. Here is a screenshot from the FusionHub line.



FusionHub

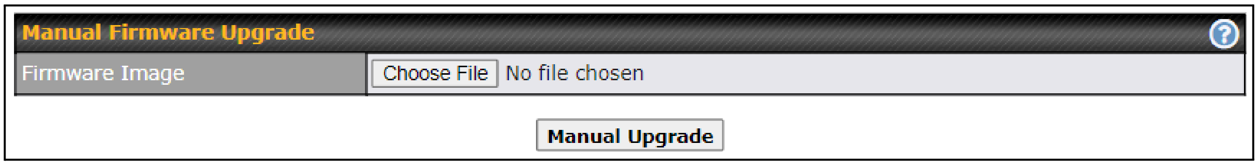
Show 10 entries

Search:

PRODUCT	HARDWARE REVISION	FIRMWARE VERSION	DOWNLOAD LINK	RELEASE NOTES	USER MANUAL
FusionHub	HW1	8.1.2	Download	PDF	PDF

Navigate to **System > Firmware** and click the **Choose File** button under the Manual Firmware Upgrade section. Navigate to the location that the firmware was downloaded to select the ".img" file and click the **Open** button.

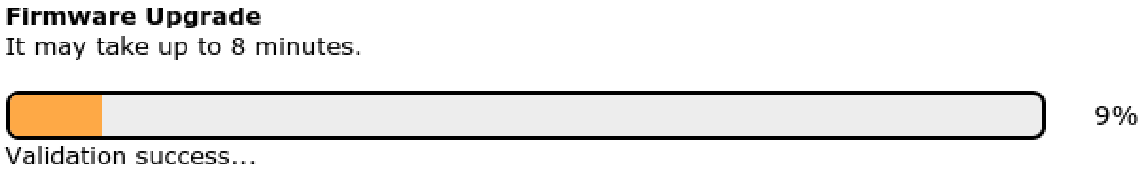
Click on the **Manual Upgrade** button to start the upgrade process.



Manual Firmware Upgrade

Firmware Image	Choose File No file chosen

A prompt will be displayed advising to download the Current Active Configuration. Please click on the underlined download text. After downloading the current config click the Ok button to start the upgrade process. The firmware will now be applied to the router*. The amount of time it takes for the firmware to upgrade will depend on the router that's being upgraded.



Firmware Upgrade
It may take up to 8 minutes.

9%

Validation success...

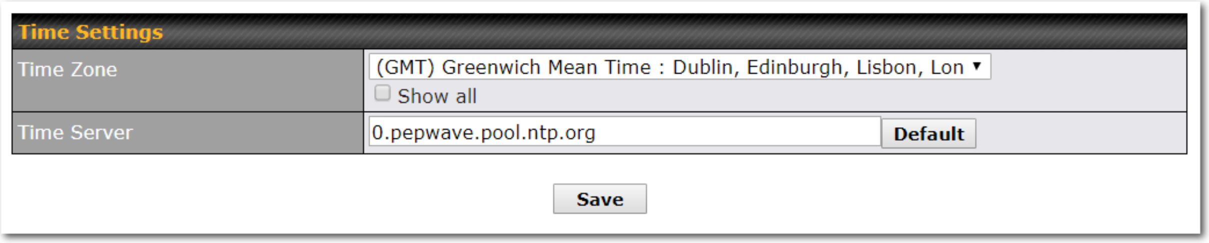
***Upgrading the firmware will cause the router to reboot.**

The InControl 2 method

[Described in this knowledgebase article on our forum.]

13.1.3. Time

The time server functionality enables the system clock of the FusionHub to be synchronized with a specified time server. The settings for time server configuration are located at **System > Time**.

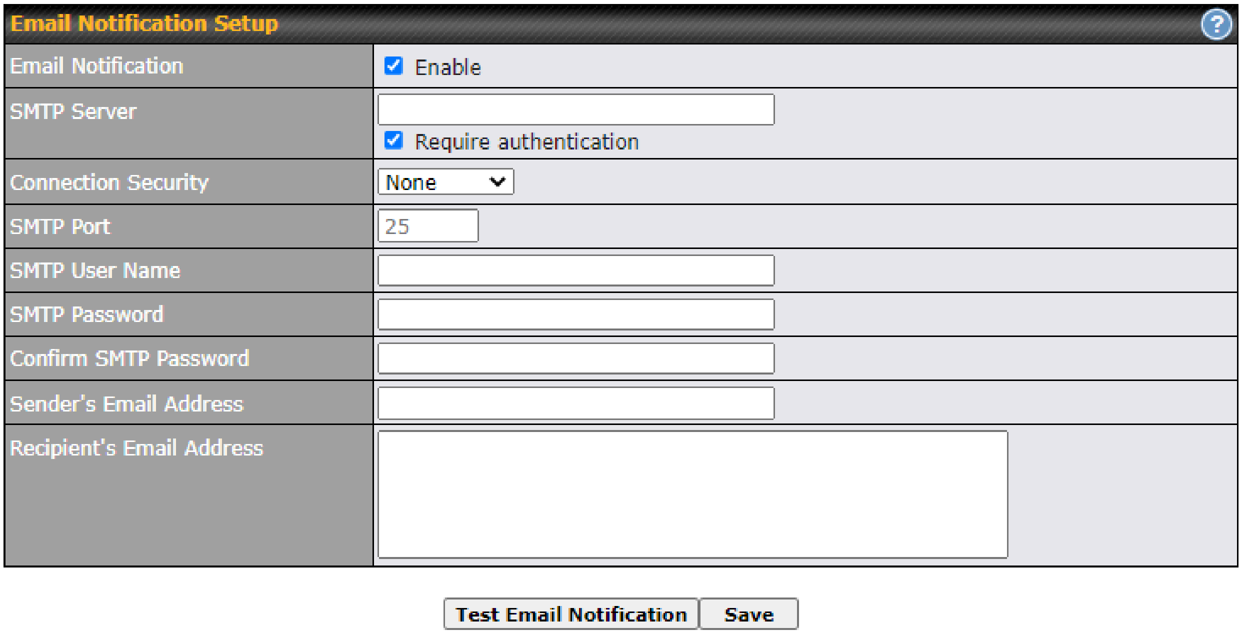


Time Settings	
Time Zone	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, Lon ▾ □ Show all
Time Server	0.pepwave.pool.ntp.org

Time Settings	
Time Zone	This specifies the time zone (along with the corresponding Daylight Savings Time scheme) in which Peplink FusionHub operates. The **Time Zone** value affects the time stamps in the event log of the FusionHub and e-mail notifications. Check **Show all** to show all time zone options.
Time Server	This setting specifies the NTP network time server to be utilized by the Peplink FusionHub.

13.1.4. Email Notification

The email notification functionality of the FusionHub provides a system administrator with up-to-date information on network status. The settings for configuring email notification are found at **System > Email Notification**.

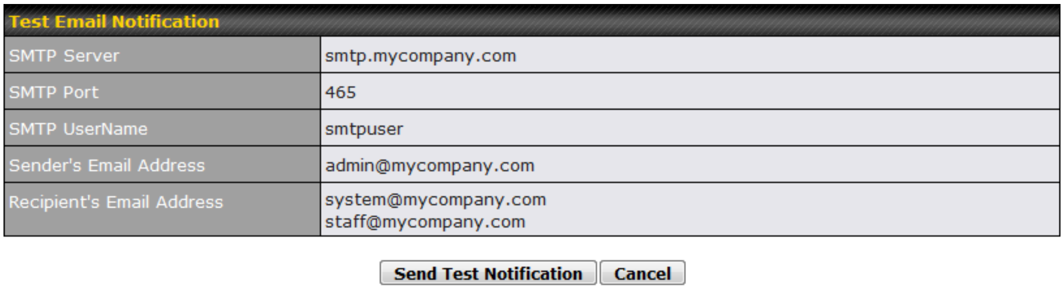


Email Notification Setup	
Email Notification	☑ Enable
SMTP Server	☑ Require authentication
Connection Security	None
SMTP Port	25
SMTP User Name	
SMTP Password	
Confirm SMTP Password	
Sender's Email Address	
Recipient's Email Address	

Email Notification Settings	
Email Notification	This setting specifies whether or not to enable email notification. If **Enable** is checked, the FusionHub will send email messages to system administrators when the WAN status changes or when new firmware is available. If **Enable** is not checked, email notification is disabled and it will not send email messages.
SMTP Server	This setting specifies the SMTP server to be used for sending email. If the server requires authentication, check **Require authentication**.
Connection Security	This setting specifies via a drop-down menu one of the following valid Connection Security: ● None ● STARTTLS ● SSL/TLS
SMTP Port	This field is for specifying the SMTP port number. By default, this is set to **25**. If the Connection Security is selected "**STARTTLS**", the default port number will be set to **587**. If the Connection Security is selected

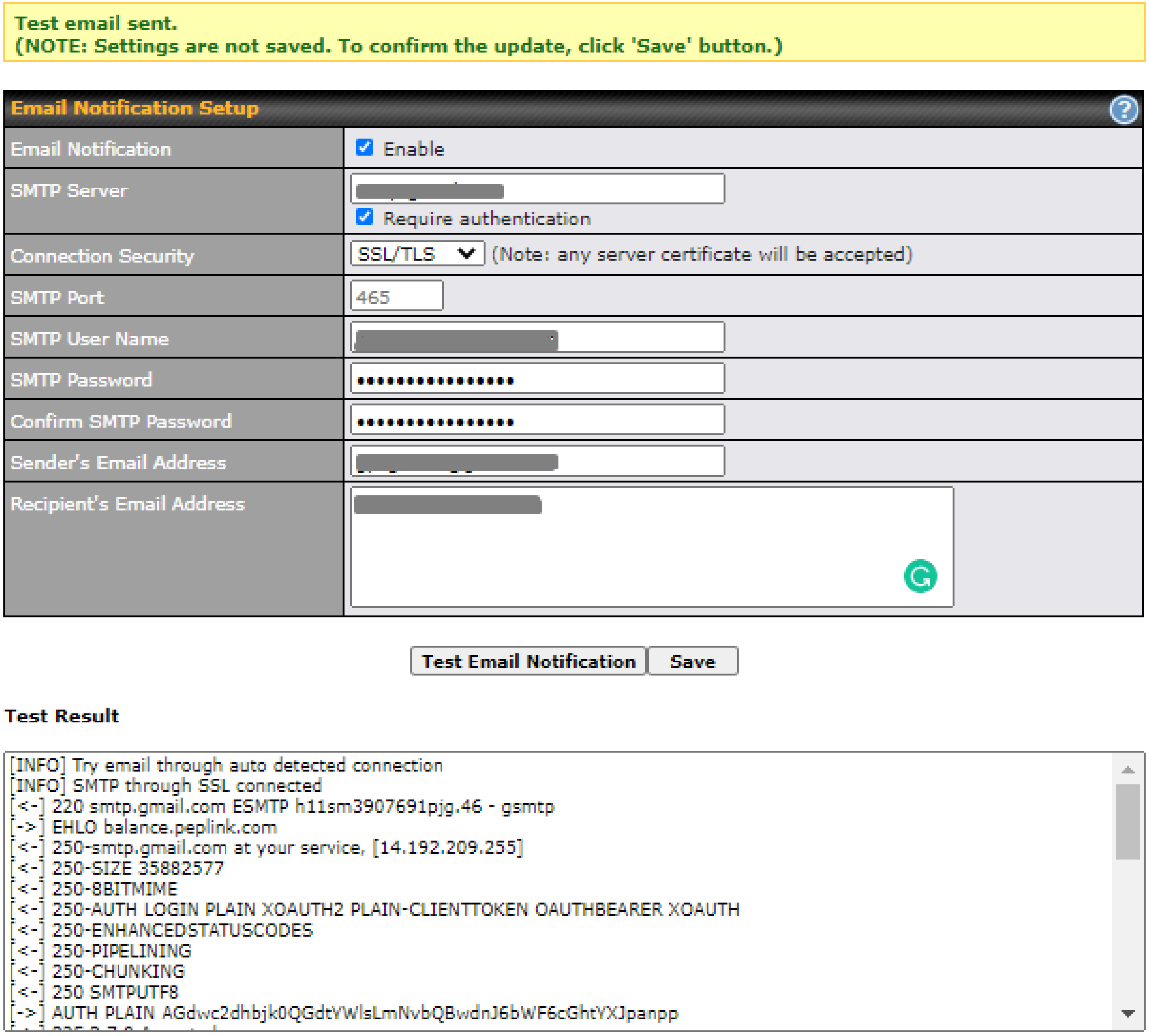
	"**SSL/TLS**", the default port number will be set to **465**. You may customize the port number by editing this field.
SMTP User Name / Password	This setting specifies the SMTP username and password while sending email. These options are shown only if **Require authentication** is checked in the **SMTP Server** setting.
Confirm SMTP Password	This field allows you to verify and confirm the new administrator password.
Sender's Email Address	This setting specifies the email address which the Peplink FusionHub will use to send its reports.
Recipient's Email Address	This setting specifies the email address(es) to which the Peplink FusionHub will send email notifications. For multiple recipients, separate each email using the enter key.

After you have finished setting up email notifications, you can click the **Test Email Notification** button to test the settings before saving. After **Test Email Notification** is clicked, you will see this screen to confirm the settings:



Test Email Notification	
SMTP Server	smtp.mycompany.com
SMTP Port	465
SMTP UserName	smtpuser
Sender's Email Address	admin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

Click **Send Test Notification** to confirm. In a few seconds, you will see a message with detailed test results.



Test email sent.
(NOTE: Settings are not saved. To confirm the update, click 'Save' button.)

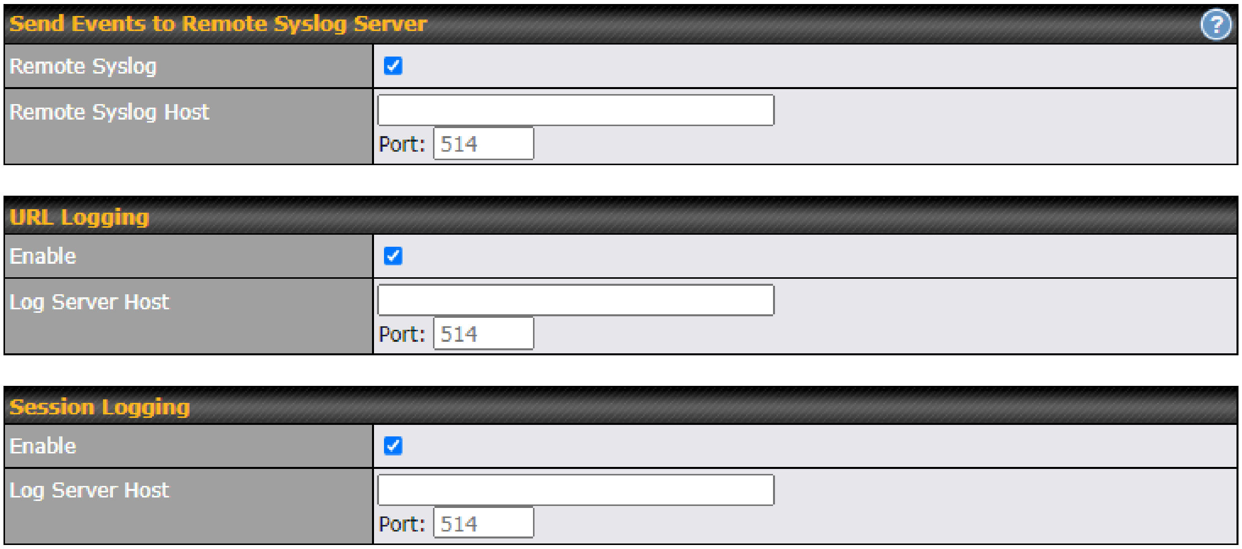
Email Notification Setup	
Email Notification	☑ Enable
SMTP Server	[redacted] ☑ Require authentication
Connection Security	SSL/TLS (Note: any server certificate will be accepted)
SMTP Port	465
SMTP User Name	[redacted]
SMTP Password	••••••••••••••••
Confirm SMTP Password	••••••••••••••••
Sender's Email Address	[redacted]
Recipient's Email Address	[redacted]

Test Result

```
[INFO] Try email through auto detected connection
[INFO] SMTP through SSL connected
[<-] 220 smtp.gmail.com ESMTP h11sm3907691pjg.46 - gsmtp
[->] EHLO balance.peplink.com
[<-] 250-smtp.gmail.com at your service, [14.192.209.255]
[<-] 250-SIZE 35882577
[<-] 250-8BITMIME
[<-] 250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN OAUTHBEARER XOAUTH
[<-] 250-ENHANCEDSTATUSCODES
[<-] 250-PIPELINING
[<-] 250-CHUNKING
[<-] 250 SMTPUTF8
[->] AUTH PLAIN AGdwc2dhbjk0QGdtYWlsLmNvbQBwdnJ6bWF6cGhtYXJpanpp
```

13.1.5. Event Log

Event log functionality enables event logging at a specified remote server. The settings for configuring the remote system log can be found at **System > Event Log**.



Send Events to Remote Syslog Server	
Remote Syslog	☑
Remote Syslog Host	Port: 514

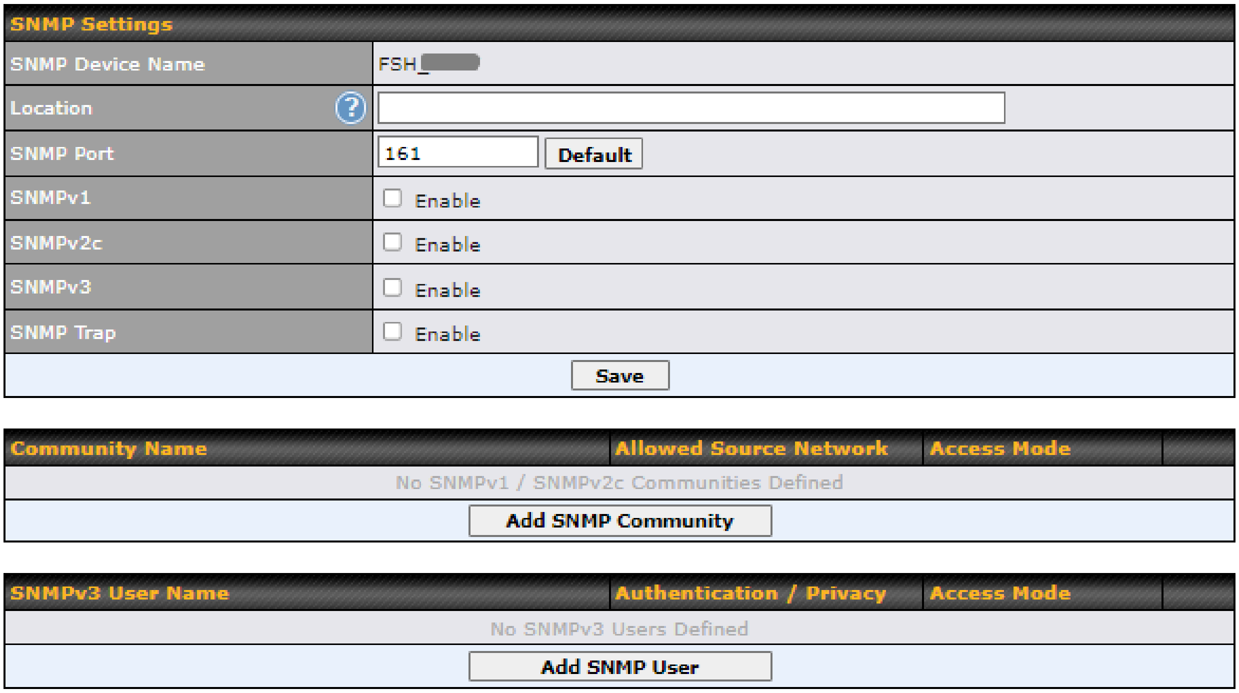
URL Logging	
Enable	☑
Log Server Host	Port: 514

Session Logging	
Enable	☑
Log Server Host	Port: 514

Event Log Settings	
Remote Syslog	This setting specifies whether or not to log events at the specified remote syslog server.
Remote Syslog Host	This setting specifies the IP address or hostname of the remote syslog server.
URL Logging	This setting is to enable event logging at the specified log server.
URL Logging Host	This setting specifies the IP address or hostname of the URL log server.
Session Logging	This setting is to enable event logging at the specified log server.
Session Logging Host	This setting specifies the IP address or hostname of the Session log server.

13.1.6. SNMP

SNMP or simple network management protocol is an open standard that can be used to collect information about the unit. SNMP configuration is located at **System > SNMP**.



SNMP Settings	
SNMP Device Name	FSH_[redacted]
Location	
SNMP Port	161 Default
SNMPv1	□ Enable
SNMPv2c	□ Enable
SNMPv3	□ Enable
SNMP Trap	□ Enable

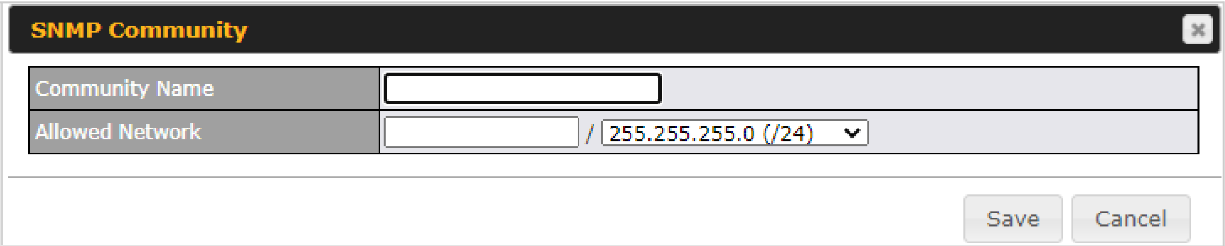
Community Name	Allowed Source Network	Access Mode
No SNMPv1 / SNMPv2c Communities Defined		

SNMPv3 User Name	Authentication / Privacy	Access Mode
No SNMPv3 Users Defined		

SNMP Settings	
SNMP Device Name	This field shows the SNMP device name defined at **System > Admin Security**.
SNMP Port	This option specifies the port which SNMP will use. The default port is **161**.
SNMPv1	This option allows you to enable SNMP version 1.
SNMPv2	This option allows you to enable SNMP version 2.
SNMPv3	This option allows you to enable SNMP version 3.
SNMP Trap	This option allows you to enable SNMP Trap. If enabled, the following entry fields will appear.
SNMP Trap Community	This setting specifies the SNMP Trap community name.
SNMP Trap Server	Enter the IP address of the SNMP Trap server.
SNMP Trap	This option specifies the port which the SNMP Trap server will use. The

Port	default port is **162**.
SNMP Trap Server Heartbeat	This option allows you to enable and configure the heartbeat interval for the SNMP Trap server.

To add a community for either SNMPv1 or SNMPv2, click the **Add SNMP Community** button in the **Community Name** table, upon which the following screen is displayed:

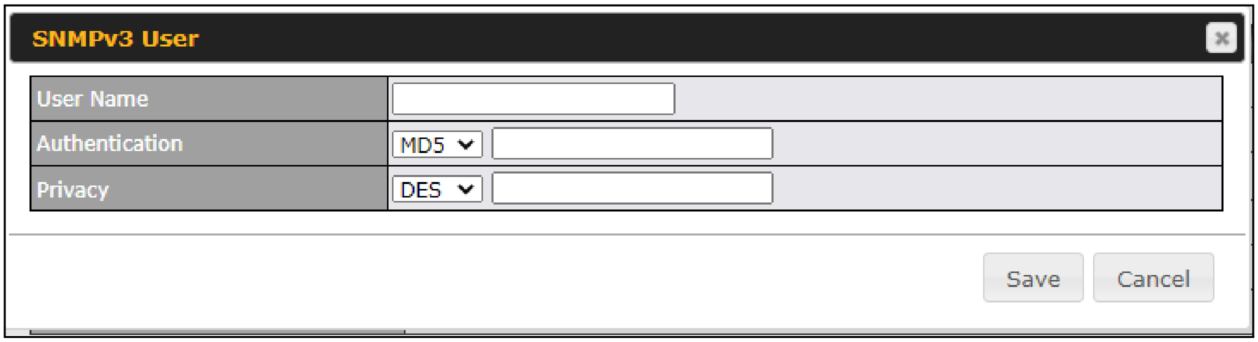


SNMP Community

Community Name	
Allowed Network	/ 255.255.255.0 (/24)

SNMP Community Settings	
Community Name	This setting specifies the SNMP community name.
Allowed Network	This setting specifies a subnet from which access to the SNMP server is allowed. Enter subnet address here (e.g., *192.168.1.0*) and select the appropriate subnet mask.

To define a user name for SNMPv3, click **Add SNMP User** in the **SNMPv3 User Name** table, upon which the following screen is displayed:



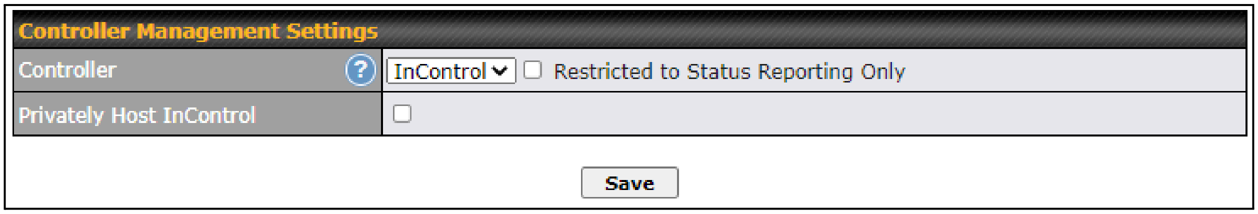
SNMPv3 User

User Name	
Authentication	MD5
Privacy	DES

SNMPv3 User Settings	
User Name	This setting specifies a user name to be used in SNMPv3.
Authentication Protocol	This setting specifies via a drop-down menu one of the following valid authentication protocols: ● NONE

	● MD5 ● SHA When MD5 or SHA is selected, an entry field will appear for the password.
Privacy Protocol	This setting specifies via a drop-down menu one of the following valid privacy protocols: ● NONE ● DES When DES is selected, an entry field will appear for the password.

13.1.7. InControl



Controller Management Settings	
Controller	InControl ☐ Restricted to Status Reporting Only
Privately Host InControl	☐

InControl is a cloud-based service which allows you to manage all of your Peplink and Pepwave devices with one unified system. With it, you can generate reports, gather statistics, and configure your devices automatically. All of this is now possible with InControl.

When this checkbox is checked, the device's status information will be sent to the Peplink InControl system. This device's usage data and configuration will be sent to the system if you enable the features in the system.

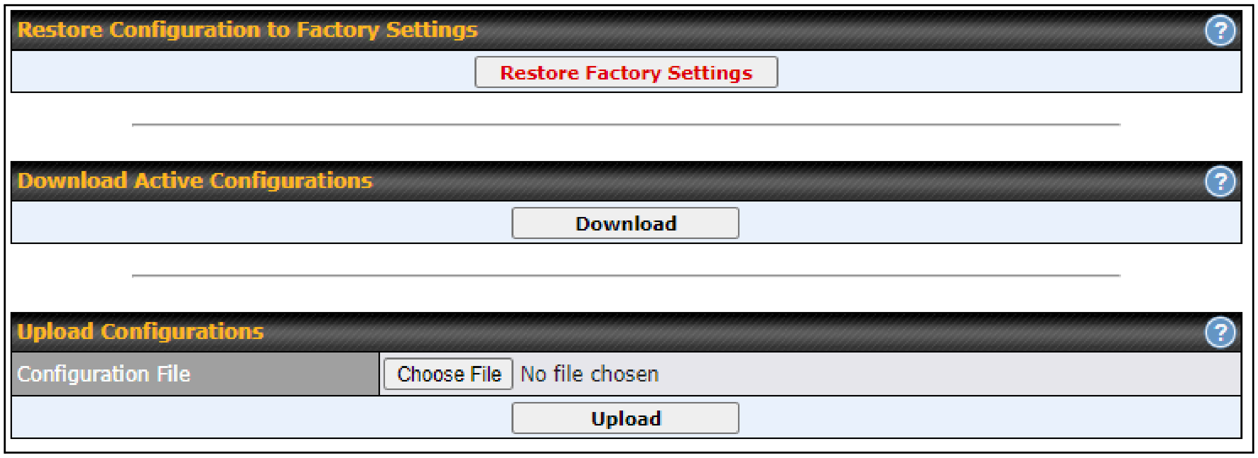
When the box **Restricted to Status Reporting Only** is ticked, the device will only report its status, but can't be managed or configured by InControl.

Alternatively, you can also privately host InControl. Simply check the "***Privately Host InControl***" box and enter the IP Address of your InControl Host. If you have multiple hosts, you may enter the primary and backup IP addresses for the InControl Host and tick the "***Fail over to InControl in the cloud***" box. The device will connect to either the primary InControl Host or the secondary/backup ICA/IC2.

You can sign up for an InControl account at https://incontrol2.peplink.com/. You can register your devices under the account, monitor their status, see their usage reports, and receive offline notifications.

13.1.8. Configuration

Backing up FusionHub settings immediately after successful completion of initial setup is strongly recommended. The functionality to download and upload FusionHub settings is found at **System > Configuration**.



Restore Configuration to Factory Settings

Restore Factory Settings

Download Active Configurations

Download

Upload Configurations

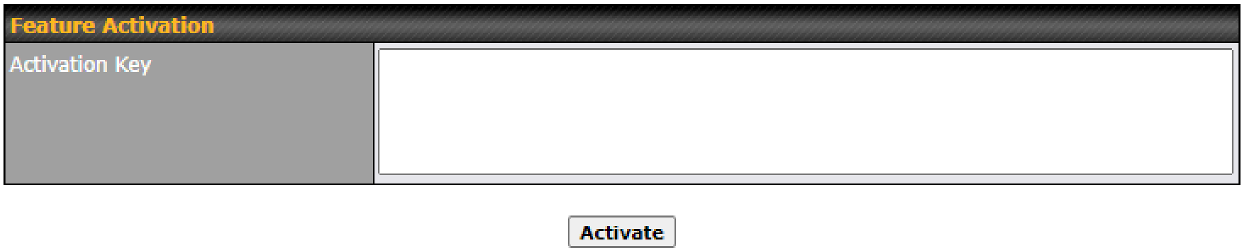
Configuration File	Choose File No file chosen

Upload

Restore Configuration to Factory Settings	
Restore Configuration to Factory Settings	The **Restore Factory Settings** button is to reset the configuration to factory default settings. After clicking the button, you will need to click the **Apply Changes** button on the top right corner to make the settings effective.
Download Active Configurations	Click **Download** to backup the current active settings.
Upload Configurations	To restore or change settings based on a configuration file, click **Choose File** to locate the configuration file on the local computer, and then click **Upload**. The new settings can then be applied by clicking the **Apply Changes** button on the page header, or you can cancel the procedure by pressing **discard** on the main page of the web admin interface.

13.1.9. Feature Add-ons

This section is to activate the features upon purchase. Once the purchase is complete, you will receive an activation key. Enter the key in the **Activation Key** field, click **Activate**, and then click **Apply Changes**.



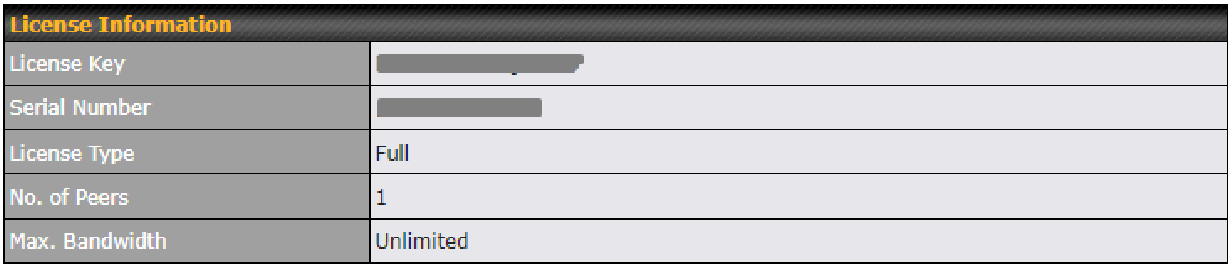
Feature Activation

Activation Key	

Activate

13.1.10. License

This section allows you to review the license information for FusionHub.



License Information	
License Key	[redacted]
Serial Number	[redacted]
License Type	Full
No. of Peers	1
Max. Bandwidth	Unlimited

License Information	
License Key	This field is to view the license key of FusionHub.
Serial Number	This field is to view the serial number of FusionHub.
License Type	Showing the type of the FusionHub license.
No. of Peers	This field is to show the number of peers to be supported for the FusionHub license.
Max. Bandwidth	This is to show the maximum bandwidth of the FusionHub license.

If you are running an Evaluation license of FusionHub and intend to convert it into the Full license edition, you can refer to the type of licenses and pricing available from our online store, or contact our certified partners for more information.

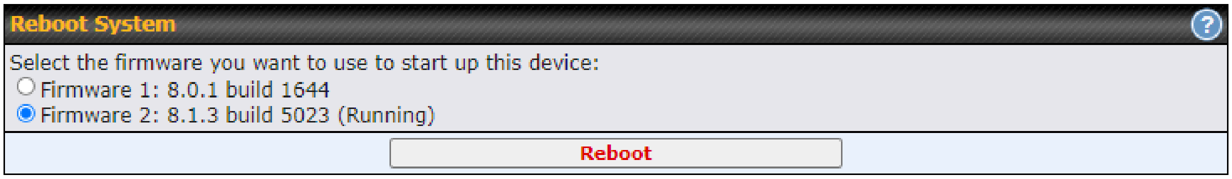
A list of available FusionHub licenses and comparisons can be found here.

FusionHub Essential	FusionHub Pro	FusionHub 100	FusionHub 500
FusionHub 1000	FusionHub 2000	FusionHub 4000	

13.1.11. Reboot

This page provides a reboot button for restarting the system. For maximum reliability, the Peplink FusionHub can be equipped with two copies of firmware, and each copy can be a different version. You can select the firmware version you would like to reboot the unit with. The firmware marked with **(Running)** is the current system boot up firmware.

Please note that a firmware upgrade will always replace the inactive firmware partition.



Reboot System

Select the firmware you want to use to start up this device:

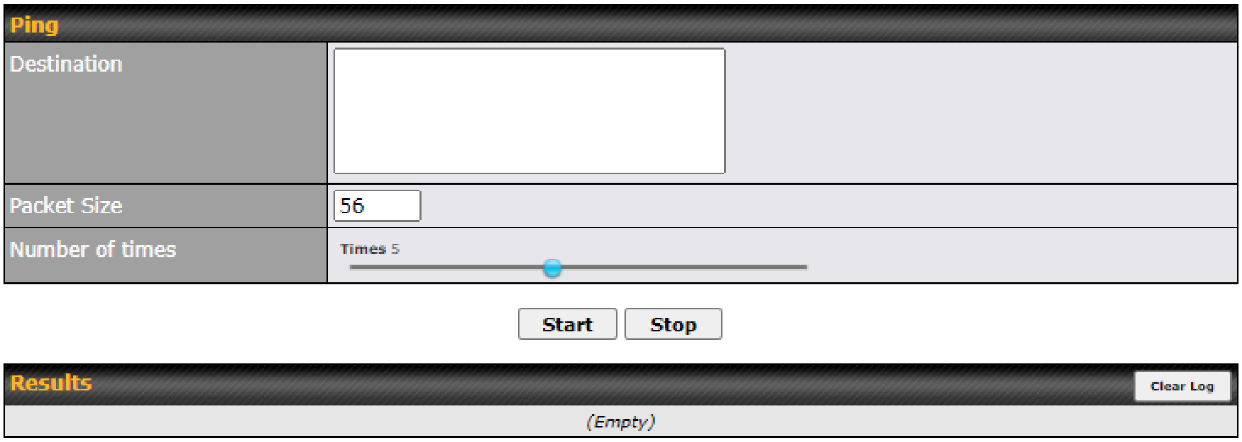
○ Firmware 1: 8.0.1 build 1644

● Firmware 2: 8.1.3 build 5023 (Running)

13.2. Tools

13.2.1. Ping

The ping test tool sends pings to check the connection. You can specify the number of pings in the field **Number of times** to a maximum number of 10 times. **Packet Size** can be set to a maximum of 1472 bytes. The ping utility is located at **System > Tools > Ping,** illustrated below:

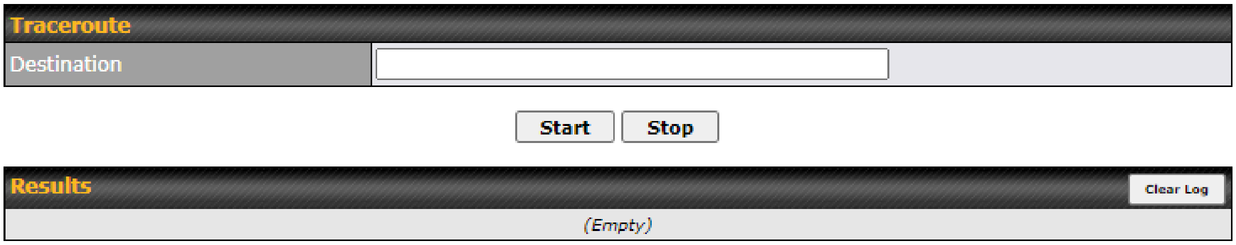


Ping

Destination	
Packet Size	56
Number of times	Times 5

13.2.2. Traceroute

The traceroute test tool traces the routing path to the destination. The traceroute test utility is located at **System > Tools > Traceroute**.

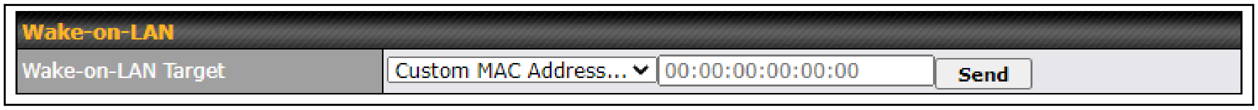


Traceroute

Destination	

13.2.3. Wake-on LAN

This feature can send special “magic packets” to any client specified from the Web UI. To access this feature, navigate to **System > Tools > Wake-on-LAN**

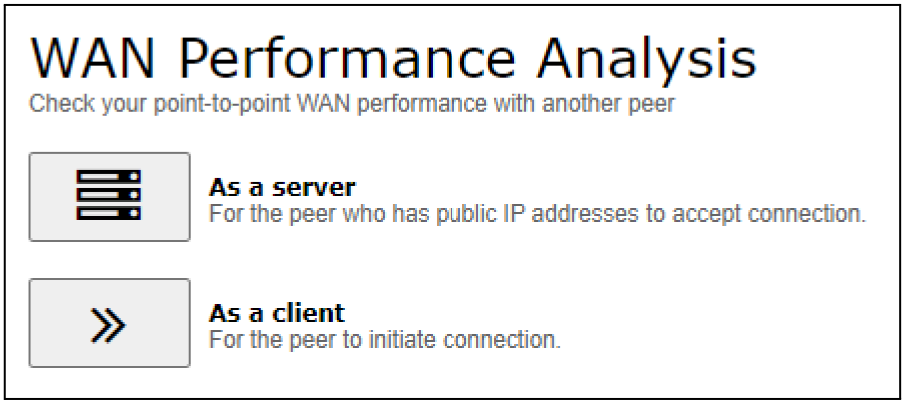


Wake-on-LAN	
Wake-on-LAN Target	Custom MAC Address... 00:00:00:00:00:00

13.2.4. WAN Analysis

The WAN Analysis feature allows you to run a WAN to WAN speed test between 2 Peplink.

You can set a device up as a **Server** or a **Client**. One device must be set up as a server to run the speed tests and the server must have a public IP address.



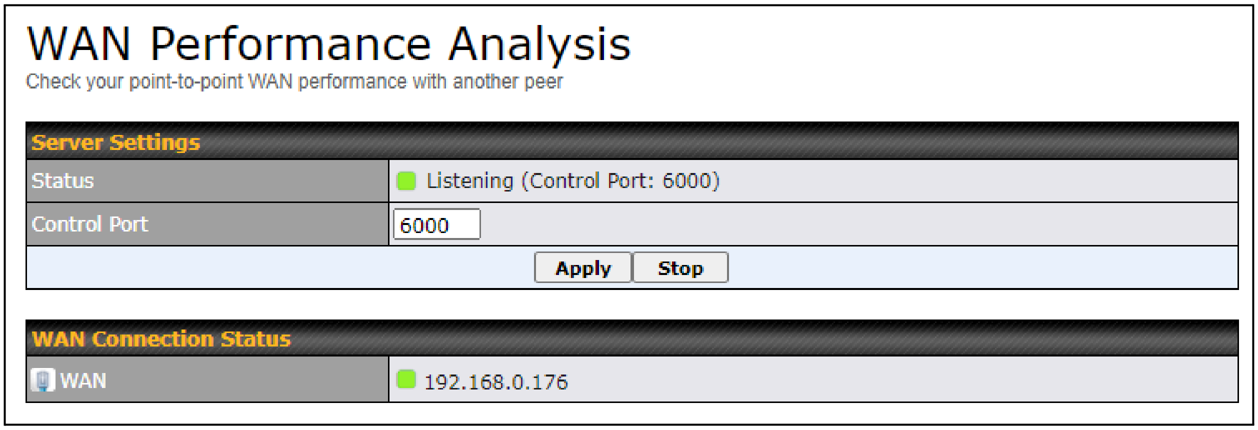
WAN Performance Analysis

Check your point-to-point WAN performance with another peer

As a server
For the peer who has public IP addresses to accept connection.

As a client
For the peer to initiate connection.

The default port is **6000** and can be changed if required. The IP address of the WAN interface will be shown in the **WAN Connection Status** section.



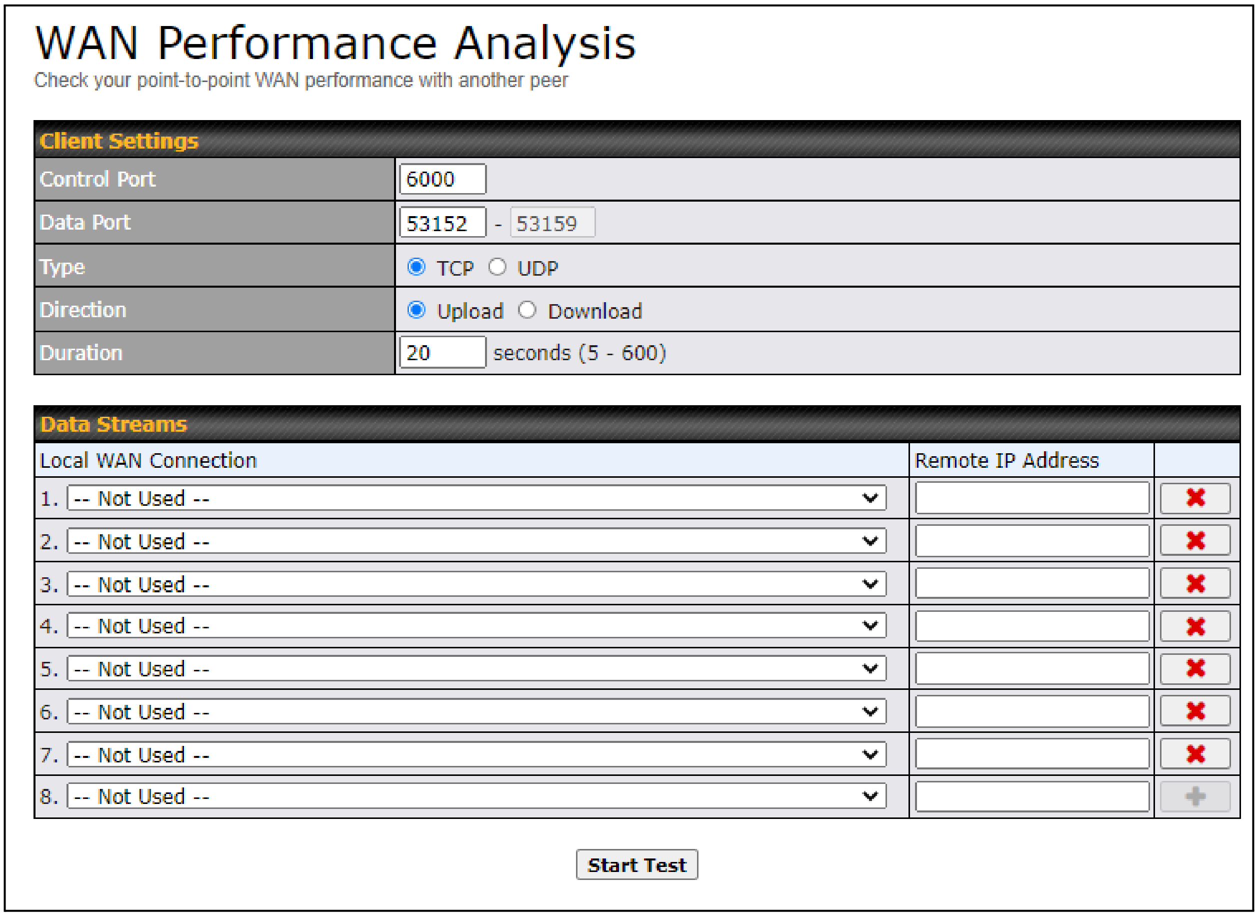
WAN Performance Analysis

Check your point-to-point WAN performance with another peer

Server Settings	
Status	🟩 Listening (Control Port: 6000)
Control Port	6000

WAN Connection Status	
WAN	🟩 192.168.0.176

The client side has a few more settings that can be changed. Make sure that the **Control Port** matches what's been entered on the server side. Select the WAN(s) that will be used for testing and enter the Servers WAN IP address. Once all of the options have been set, click the **Start Test** button.



WAN Performance Analysis

Check your point-to-point WAN performance with another peer

Client Settings	
Control Port	6000
Data Port	53152 - 53159
Type	● TCP ○ UDP
Direction	● Upload ○ Download
Duration	20 seconds (5 - 600)

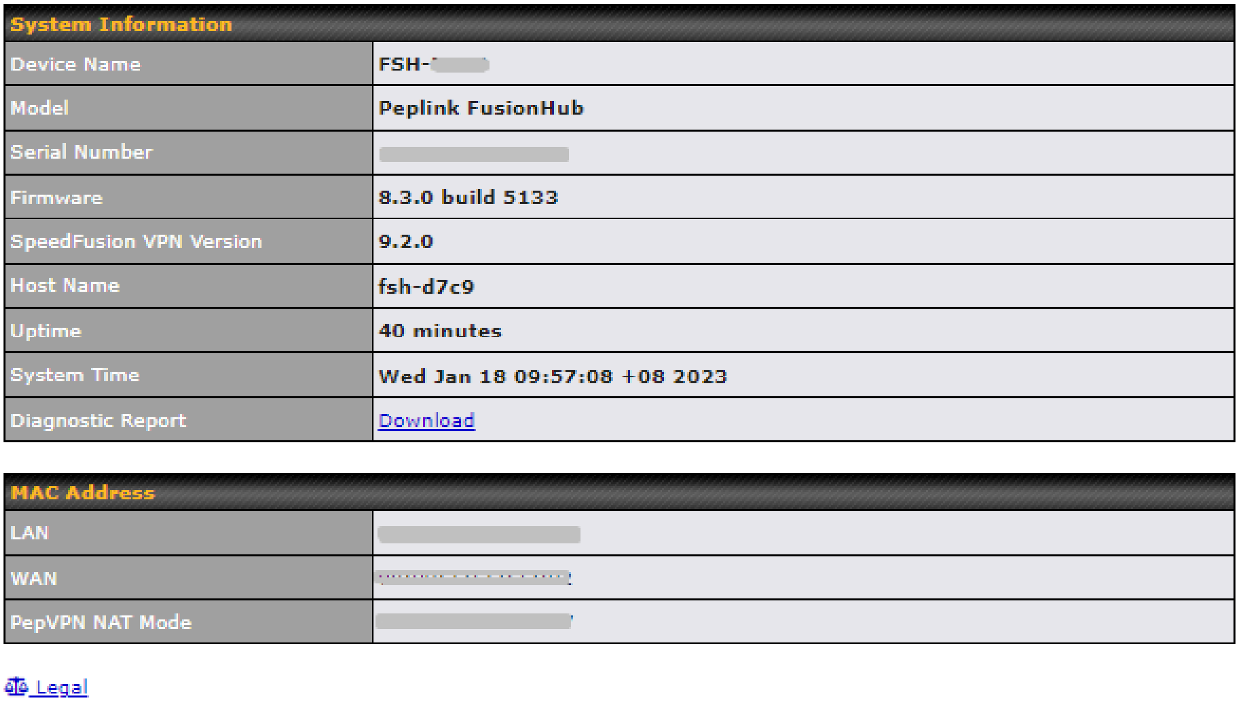
Data Streams

Local WAN Connection	Remote IP Address	
1. -- Not Used --		✖
2. -- Not Used --		✖
3. -- Not Used --		✖
4. -- Not Used --		✖
5. -- Not Used --		✖
6. -- Not Used --		✖
7. -- Not Used --		✖
8. -- Not Used --		+

14. Status

14.1. Device

System information is located at **Status > Device**.



System Information	
Device Name	FSH-[redacted]
Model	Peplink FusionHub
Serial Number	[redacted]
Firmware	8.3.0 build 5133
SpeedFusion VPN Version	9.2.0
Host Name	fsh-d7c9
Uptime	40 minutes
System Time	Wed Jan 18 09:57:08 +08 2023
Diagnostic Report	Download

MAC Address	
LAN	[redacted]
WAN	[redacted]
PepVPN NAT Mode	[redacted]

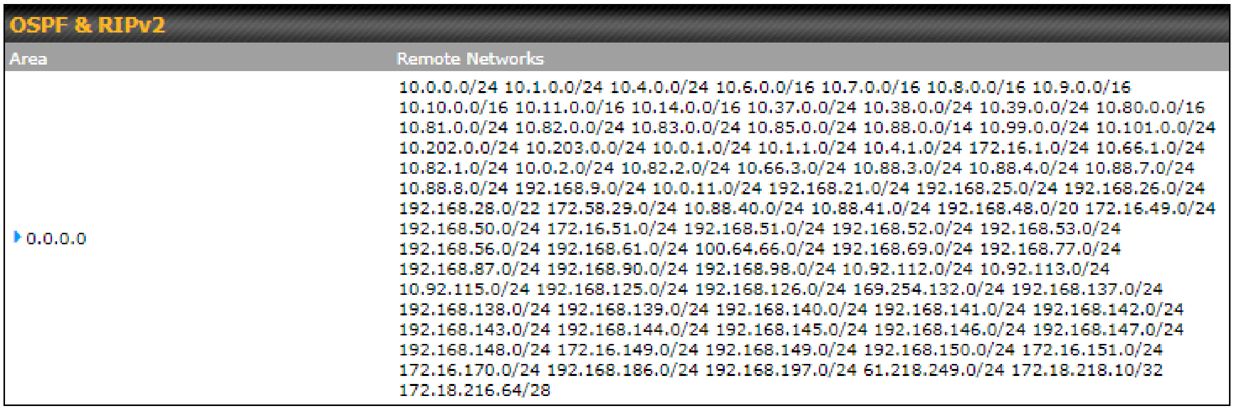
Legal

System Information	
Device Name	This is the name specified in the **Device Name** field located at **System > Admin Security**.
Model	This shows the model name and number of this FusionHub.
Serial Number	This shows the serial number of this FusionHub.
Firmware	This shows the firmware version this FusionHub is currently running.
SpeedFusion VPN Version	This shows the PepVPN version this FusionHub.
Host Name	This shows the host name of the FusionHub.
Uptime	This shows the length of time since the FusionHub has been rebooted.
System Time	This shows the current system time.
Diagnostic	The **Download** link is for exporting a diagnostic report file required for

Report	system investigation.
Remote Assistance	Click **Turn on** to enable remote assistance.

14.2. OSPF & RIPv2

Information on OSPF and RIPv2 routing setup can be found at **Status > OSPF & RIPv2**.

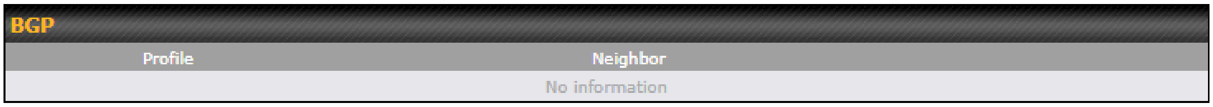


OSPF & RIPv2

Area	Remote Networks
0.0.0.0	10.0.0.0/24 10.1.0.0/24 10.4.0.0/24 10.6.0.0/16 10.7.0.0/16 10.8.0.0/16 10.9.0.0/16 10.10.0.0/16 10.11.0.0/16 10.14.0.0/16 10.37.0.0/24 10.38.0.0/24 10.39.0.0/24 10.80.0.0/16 10.81.0.0/24 10.82.0.0/24 10.83.0.0/24 10.85.0.0/24 10.88.0.0/14 10.99.0.0/24 10.101.0.0/24 10.202.0.0/24 10.203.0.0/24 10.0.1.0/24 10.1.1.0/24 10.4.1.0/24 172.16.1.0/24 10.66.1.0/24 10.82.1.0/24 10.0.2.0/24 10.82.2.0/24 10.66.3.0/24 10.88.3.0/24 10.88.4.0/24 10.88.7.0/24 10.88.8.0/24 192.168.9.0/24 10.0.11.0/24 192.168.21.0/24 192.168.25.0/24 192.168.26.0/24 192.168.28.0/22 172.58.29.0/24 10.88.40.0/24 10.88.41.0/24 192.168.48.0/20 172.16.49.0/24 192.168.50.0/24 172.16.51.0/24 192.168.51.0/24 192.168.52.0/24 192.168.53.0/24 192.168.56.0/24 192.168.61.0/24 100.64.66.0/24 192.168.69.0/24 192.168.77.0/24 192.168.87.0/24 192.168.90.0/24 192.168.98.0/24 10.92.112.0/24 10.92.113.0/24 10.92.115.0/24 192.168.125.0/24 192.168.126.0/24 169.254.132.0/24 192.168.137.0/24 192.168.138.0/24 192.168.139.0/24 192.168.140.0/24 192.168.141.0/24 192.168.142.0/24 192.168.143.0/24 192.168.144.0/24 192.168.145.0/24 192.168.146.0/24 192.168.147.0/24 192.168.148.0/24 172.16.149.0/24 192.168.149.0/24 192.168.150.0/24 172.16.151.0/24 172.16.170.0/24 192.168.186.0/24 192.168.197.0/24 61.218.249.0/24 172.18.218.10/32 172.18.216.64/28

14.3. BGP

Information on BGP routing setup can be found at **Status > BGP**.



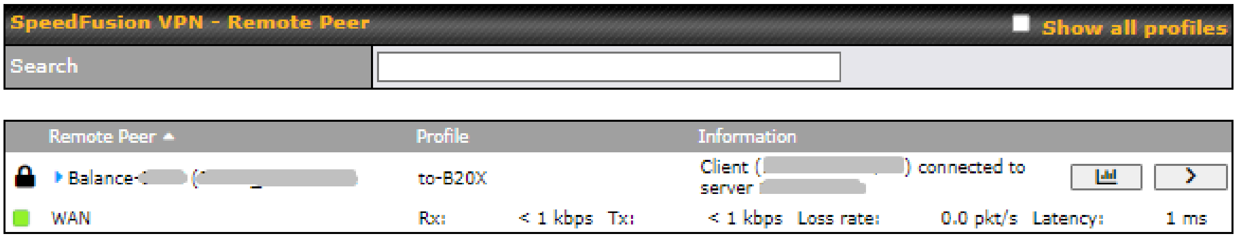
BGP

Profile	Neighbor
No information	

14.4. SpeedFusion VPN

SpeedFusion VPN shows the current connection status of each connection profile and is displayed at **Status > SpeedFusion VPN.**

Click on the corresponding peer name to explore the WAN connection(s) status and subnet information of each VPN peer.

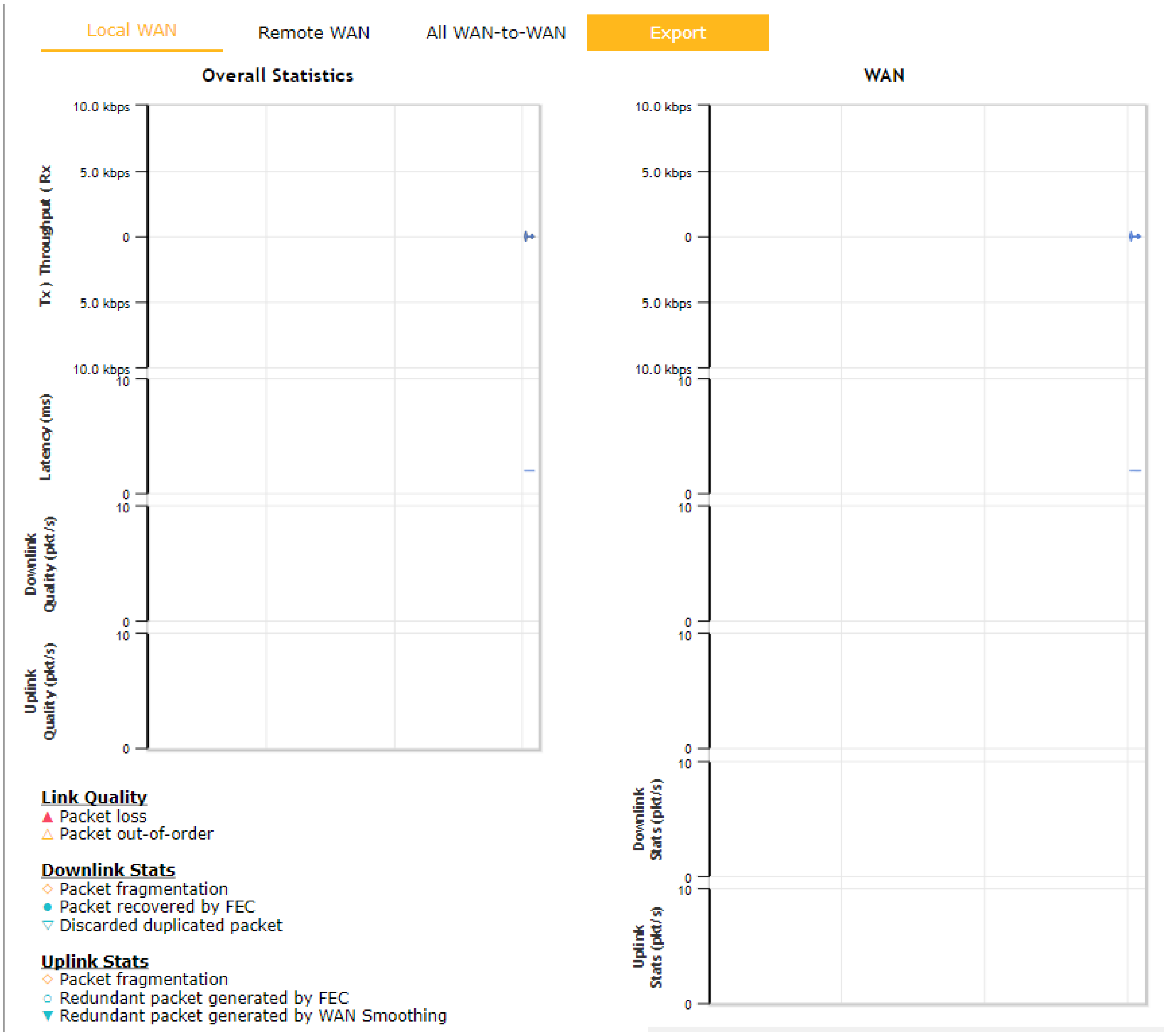


SpeedFusion VPN - Remote Peer □ **Show all profiles**

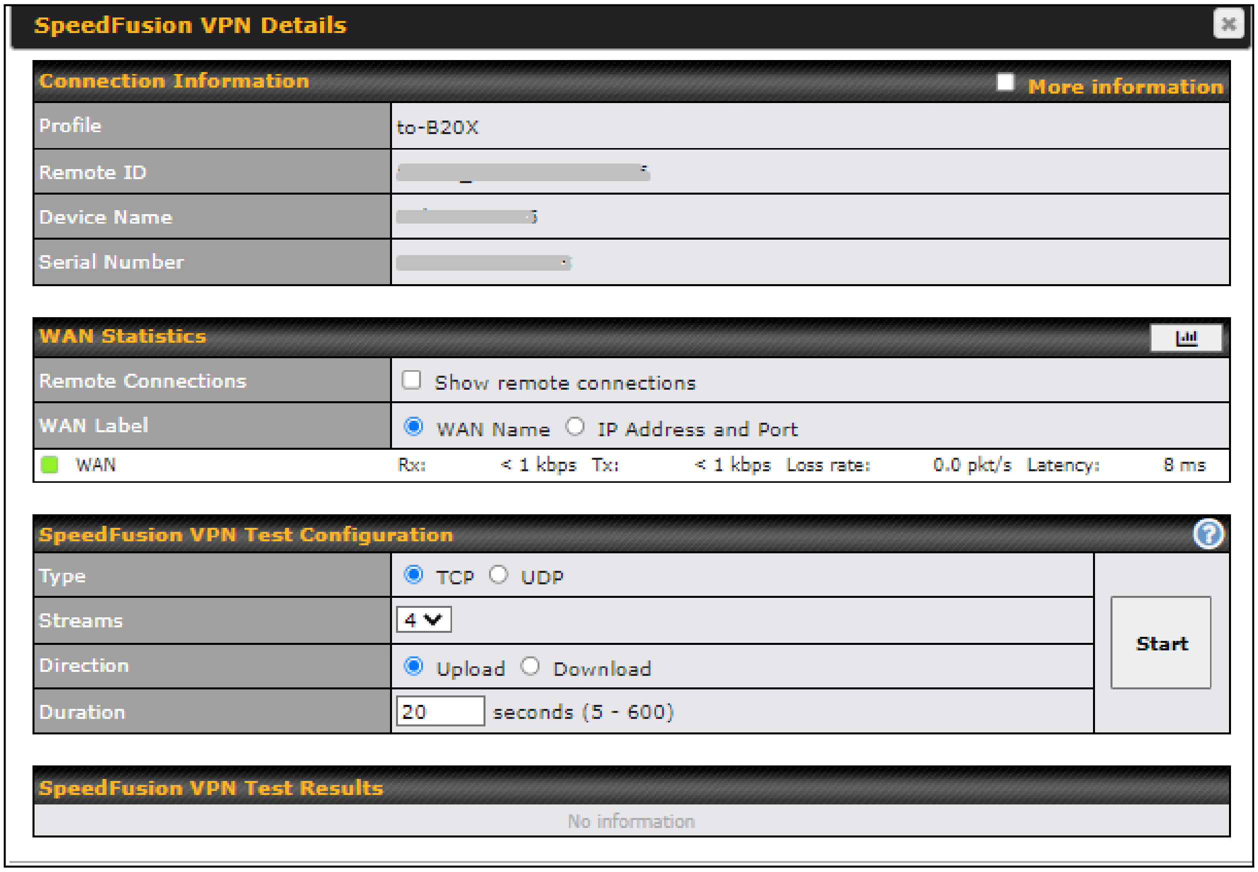
Search	

Remote Peer ▲	Profile	Information
🔒 ▸ Balance-[redacted] ([redacted])	to-B20X	Client ([redacted]) connected to server [redacted]
🟩 WAN	Rx: < 1 kbps Tx: < 1 kbps	Loss rate: 0.0 pkt/s Latency: 1 ms

Click the 📊 button for SpeedFusion chart displaying real-time throughput, latency, and drop-rate information for each WAN connection.



When pressing the > button for a SpeedFusion Tunnel Bandwidth Test Tool, the following menu will appear:



SpeedFusion VPN Details

Connection Information	■ More information
Profile	to-B20X
Remote ID	[redacted]
Device Name	[redacted]
Serial Number	[redacted]

WAN Statistics	
Remote Connections	□ Show remote connections
WAN Label	● WAN Name ○ IP Address and Port
🟩 WAN	Rx: < 1 kbps Tx: < 1 kbps Loss rate: 0.0 pkt/s Latency: 8 ms

SpeedFusion VPN Test Configuration		
Type	● TCP ○ UDP	Start
Streams	4	
Direction	● Upload ○ Download	
Duration	20 seconds (5 - 600)	

SpeedFusion VPN Test Results
No information

The **connection information** shows the details of the selected SpeedFusion VPN profile, consisting of the **Profile name**, **Router ID**, **Device Name** and **Serial Number** of the remote router

Advanced features for the SpeedFusion VPN profile will also be shown when the **More Information** checkbox is selected.

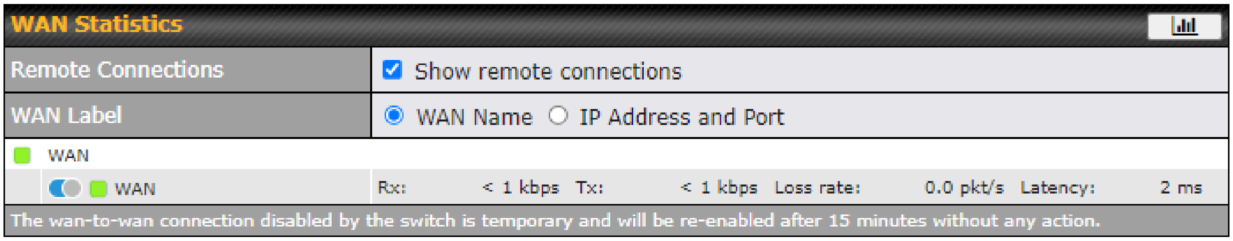
The **WAN Statistics** show information about the local and remote WAN connections (when **Show remote connections**) is selected.

The available details are **WAN Name, IP address** and **Port** used for the Speedfusion connection. **Rx and Tx rates, Loss rate and Latency**.

Connections can be temporarily disabled by sliding the switch button next to a WAN connection to the left.

The wan-to-wan connection disabled by the switch is temporary and will be re-enabled after 15 minutes without any action.

This can be used when testing the SpeedFusion VPN speed between two locations to see if there is interference or network congestion between certain WAN connections.



WAN Statistics

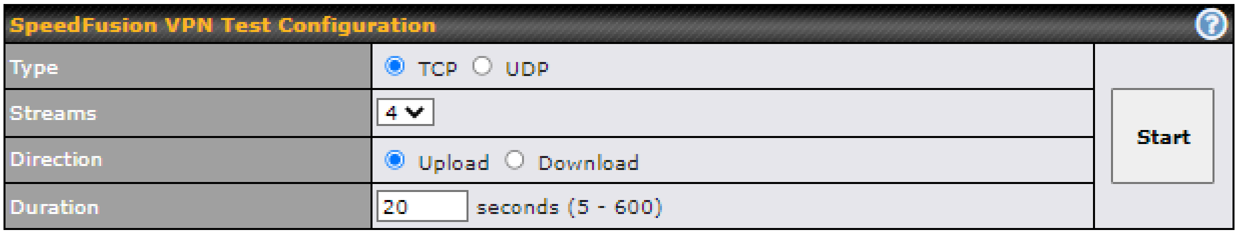
Remote Connections	☑ Show remote connections
WAN Label	● WAN Name ○ IP Address and Port

🟩 WAN

🟩 WAN	Rx: < 1 kbps Tx: < 1 kbps Loss rate: 0.0 pkt/s Latency: 2 ms

The wan-to-wan connection disabled by the switch is temporary and will be re-enabled after 15 minutes without any action.

The SpeedFusion VPN test configuration allows us to configure and perform thorough tests. This is usually done after the initial installation of the routers and in case there are problems with aggregation.



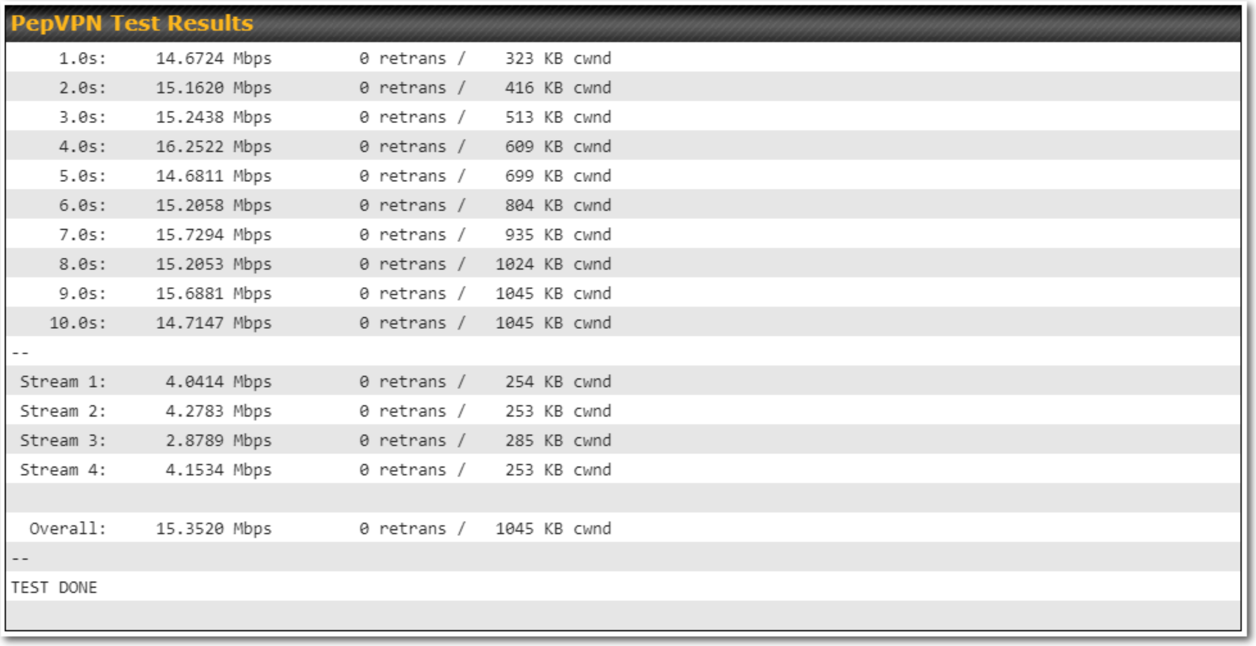
SpeedFusion VPN Test Configuration

Type	● TCP ○ UDP
Streams	4
Direction	● Upload ○ Download
Duration	20 seconds (5 - 600)

Press the **Start** button to perform a throughput test according to the configured options.

If **TCP** is selected, 4 parallel streams will be generated to get the optimal results by default. This can be customized by selecting a different value of streams.

Using more streams will typically get better results if the latency of the tunnel is high.



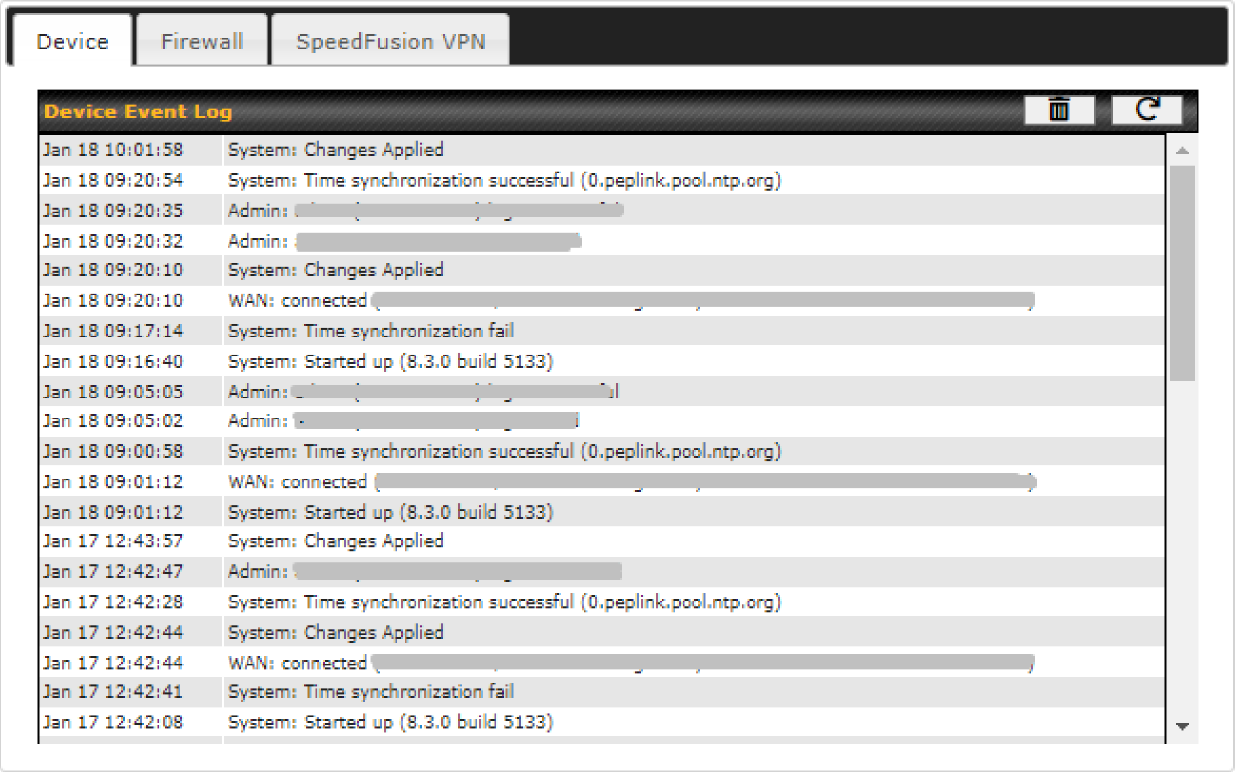
PepVPN Test Results

```
     1.0s:     14.6724 Mbps         0 retrans /    323 KB cwnd
     2.0s:     15.1620 Mbps         0 retrans /    416 KB cwnd
     3.0s:     15.2438 Mbps         0 retrans /    513 KB cwnd
     4.0s:     16.2522 Mbps         0 retrans /    609 KB cwnd
     5.0s:     14.6811 Mbps         0 retrans /    699 KB cwnd
     6.0s:     15.2058 Mbps         0 retrans /    804 KB cwnd
     7.0s:     15.7294 Mbps         0 retrans /    935 KB cwnd
     8.0s:     15.2053 Mbps         0 retrans /   1024 KB cwnd
     9.0s:     15.6881 Mbps         0 retrans /   1045 KB cwnd
    10.0s:     14.7147 Mbps         0 retrans /   1045 KB cwnd
--
 Stream 1:      4.0414 Mbps         0 retrans /    254 KB cwnd
 Stream 2:      4.2783 Mbps         0 retrans /    253 KB cwnd
 Stream 3:      2.8789 Mbps         0 retrans /    285 KB cwnd
 Stream 4:      4.1534 Mbps         0 retrans /    253 KB cwnd

  Overall:     15.3520 Mbps         0 retrans /   1045 KB cwnd
--
TEST DONE
```

14.5. Event Log

Event log information is located at **Status > Event Log**.

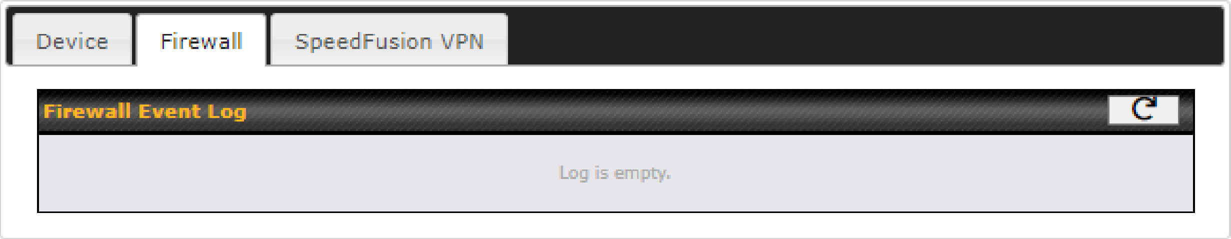
Device Event Log



```
Jan 18 10:01:58   System: Changes Applied
Jan 18 09:20:54   System: Time synchronization successful (0.peplink.pool.ntp.org)
Jan 18 09:20:35   Admin: [redacted]
Jan 18 09:20:32   Admin: [redacted]
Jan 18 09:20:10   System: Changes Applied
Jan 18 09:20:10   WAN: connected [redacted]
Jan 18 09:17:14   System: Time synchronization fail
Jan 18 09:16:40   System: Started up (8.3.0 build 5133)
Jan 18 09:05:05   Admin: [redacted]
Jan 18 09:05:02   Admin: [redacted]
Jan 18 09:00:58   System: Time synchronization successful (0.peplink.pool.ntp.org)
Jan 18 09:01:12   WAN: connected [redacted]
Jan 18 09:01:12   System: Started up (8.3.0 build 5133)
Jan 17 12:43:57   System: Changes Applied
Jan 17 12:42:47   Admin: [redacted]
Jan 17 12:42:28   System: Time synchronization successful (0.peplink.pool.ntp.org)
Jan 17 12:42:44   System: Changes Applied
Jan 17 12:42:44   WAN: connected [redacted]
Jan 17 12:42:41   System: Time synchronization fail
Jan 17 12:42:08   System: Started up (8.3.0 build 5133)
```

The Device section displays a list of events that have taken place on the Peplink FusionHub. Tick the ↻ button to refresh log entries automatically. Click the **Clear Log** button to clear the log.

Firewall Event Log

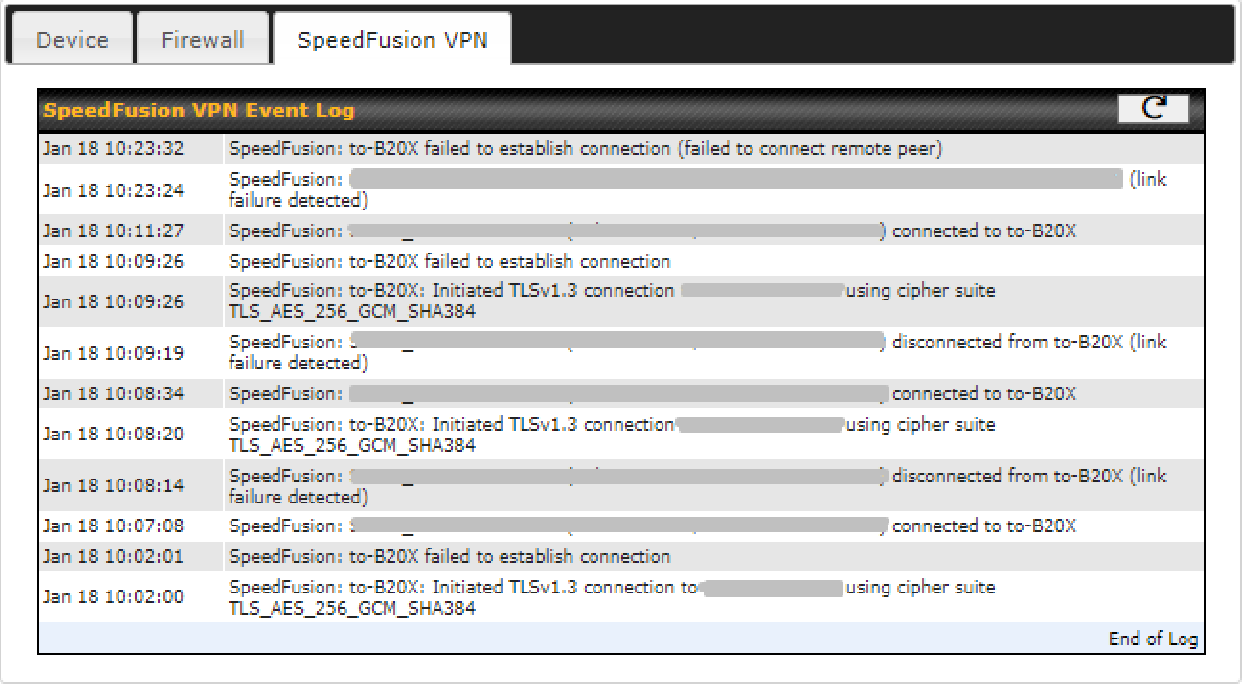


```
Log is empty.
```

This section displays a list of events that have taken place on the firewall. Tick the ↻

button and the log will be refreshed automatically.

SpeedFusion VPN Event Log



```
Jan 18 10:23:32   SpeedFusion: to-B20X failed to establish connection (failed to connect remote peer)
Jan 18 10:23:24   SpeedFusion: [redacted] (link
                  failure detected)
Jan 18 10:11:27   SpeedFusion: [redacted]) connected to to-B20X
Jan 18 10:09:26   SpeedFusion: to-B20X failed to establish connection
Jan 18 10:09:26   SpeedFusion: to-B20X: Initiated TLSv1.3 connection [redacted] using cipher suite
                  TLS_AES_256_GCM_SHA384
Jan 18 10:09:19   SpeedFusion: [redacted]) disconnected from to-B20X (link
                  failure detected)
Jan 18 10:08:34   SpeedFusion: [redacted] connected to to-B20X
Jan 18 10:08:20   SpeedFusion: to-B20X: Initiated TLSv1.3 connection [redacted] using cipher suite
                  TLS_AES_256_GCM_SHA384
Jan 18 10:08:14   SpeedFusion: [redacted]) disconnected from to-B20X (link
                  failure detected)
Jan 18 10:07:08   SpeedFusion: [redacted] connected to to-B20X
Jan 18 10:02:01   SpeedFusion: to-B20X failed to establish connection
Jan 18 10:02:00   SpeedFusion: to-B20X: Initiated TLSv1.3 connection to [redacted] using cipher suite
                  TLS_AES_256_GCM_SHA384
                                                                                         End of Log
```

This section displays a list of events that have taken place on the SpeedFusion VPN. **Tick the ↻ button** and the log will be refreshed automatically.

15. Support

Peplink provides multiple layers of support: technical support, knowledge sharing with its expert community, documentation and firmware downloads, and RMA and warranty services. More information can be found at Peplink Support Page.

15.1. Support Service Plans

There are several service plans available for Peplink products, including FusionHub; namely PrimeCare, Essential Care, and SmartCare, each of which provide different levels of support.

PrimeCare makes SpeedFusion networks easier to build. It’s a subscription that bundles InControl, Warranty, SpeedFusion license upgrades, and FusionHub licenses together.

EssentialCare and SmartCare are designed to simplify network maintenance, so that you can focus on building your business.

Firmware versions and User Manuals can be found at this link.

If you need further technical assistance from the Peplink Support Team, you may submit a ticket via this URL: https://ticket.peplink.com/ticket/new/public

15.2. Management & Monitoring via InControl2

InControl 2 is a cloud-based management system. We recommend using it to monitor the status of FusionHub, conduct maintenance, and automatically backup configurations. It can also store and manage the Web Admin Password.
Details: https://www.peplink.com/software/network-management-solution-incontrol-2/

15.3. Backing Up Configurations and Recovery

Backing Up Configurations
InControl 2 will automatically backup configuration changes toFusionHub. For details, please refer to this FAQ (https://forum.peplink.com/t/backing-up-and-restoring-device-configurations/8153).

Recovering FusionHub

To recover FusionHub, follow the steps below:

1. Release the FusionHub License from the Organization that the FusionHub belongs to. “Organization Settings” > “Warranty & License” > “FusionHub Licenses”

2. Create a new FusionHub VM from the ground up, and apply the released FusionHub license.
3. Restore the configuration, which can be obtained from InControl 2 as mentioned above.

15.4. Miscellaneous

The FusionHub Disk image is encrypted by OS, and configurations are also stored there.