

# NetWatcher® Managed Detection & Response Service An MSP's Guide to Installing a Customer

## What is NetWatcher?

NetWatcher is a Security-as-a-Service platform that enables customers to have a cost-effective 24 x 7 security service monitoring their networks for vulnerabilities and exploits. Many government and industry compliance requirements, and security best practices, outline the need for continuous monitoring, intrusion detection, active scanning, log monitoring, net-flow analysis, event management and endpoint integration. NetWatcher enables customers to immediately deploy these services and take advantage of a fully-staffed Security Operations Center (SOC). This means superior security that is easy to use, accurate and affordable.

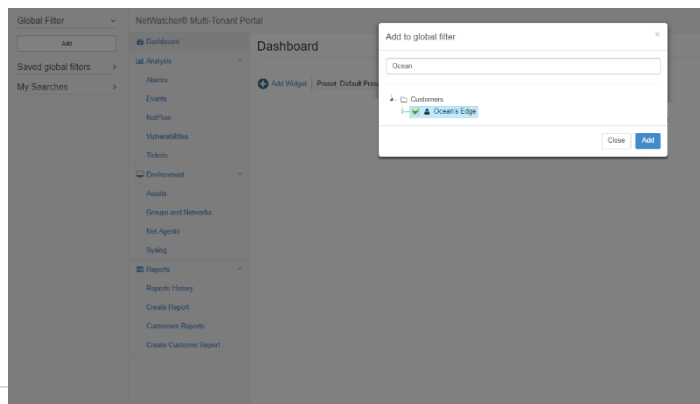
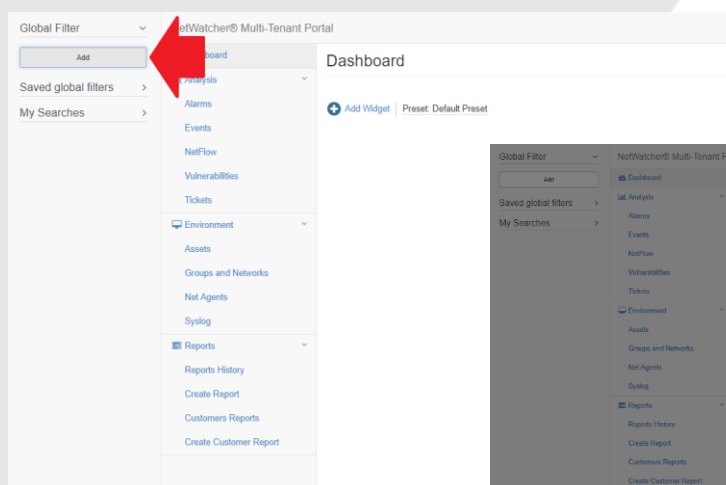
## Contents

Connecting Hardware Sensor to NetWatcher Cloud.....	3
Setting up Network Intrusion Detection (NIDS) .....	6
Setting up SYSLOG Ingestion .....	6
Setting up Server / Desktop / Laptop LOGS.....	8
Setting Up Reoccurring Vulnerability Scans .....	10
Setup Reoccurring Reports .....	12
Setup Notifications for Your Customer Contacts .....	13
Connecting Virtual Sensor to NetWatcher Cloud – VSphere .....	14
Installing the Virtual Sensor on Other Virtual Machine Platforms .....	21



## Connecting Hardware Sensor to NetWatcher Cloud

1. Ensure your customer is not blocking any of the following ports OUTBOUND. These ports are what the sensor uses to communicate back to the NetWatcher cloud.
  - TCP 22 => portal.netwatcher.com
  - TCP 8443 => p.netwatcher.com
  - UDP 443 => vpn.netwatcher.com
  - TCP 443 => vpn-tcp.netwatcher.com
  - TCP 443 => index.docker.io
  - TCP 443 => registry-1.docker.io
  - TCP 443 => public.update.core-os.net
  - TCP 80 to google.com => Used to test internet/DNS connectivity
2. Connect one of the LAN ports on the sensors to the internet (doesn't matter which one) and let the sensor download its OS/Containers/Rulesets. This can take 20 min.
3. If you need to setup a static IP address see [this article](#).
4. Run Setup
  - a. Login to the MSP Portal and add a global filter for the customer name by pressing the 'Add' button in the upper left corner of the screen.



- b. The find the sensor by going to <https://dsap.netwatcher.com/sensor>

- c. Select the name of the sensor. In this example its LR201411012067.

- d. Find 'Sensor Setup' on this page and put in the External IP address and press the 'Configure' button. You can find the External IP address by typing "what is my ip" in Google.

e. The Sensor will begin to count down.

Global Filter (clear) | NetWatcher® Multi-Tenant Portal

Home / Sensor / 75894c-862-453a-af2a-02ca20b0464f

### Sensor - LR201411012067

Base Info Get one time pass

- ID: 75894c-862-453a-af2a-02ca20b0464f
- Device: 05a7872b-6581-4172-af39-a1ba3841590f
- Status: Warning
- RIM Connected: Not Connected
- Type: HARDWARE
- Name: LR201411012067
- Last Config Check Time: 2017-08-10 17:20:00
- IP: s403aa5a2202ca20b0464f.s.n.w.io
- Local DNS: s403aa5a2202ca20b0464f.s.n.w.io
- Port: Ocean's Edge
- Customer: Ocean's Edge
- User: sensor\_LR201411012067
- Certificate Expiration: Invalid
- Last Event: Last Flow
- Last Heartbeat: 2017-08-10 17:20:00
- Date: 2017-08-10 17:20:00
- Backup: There is no valid certificate found
- Prefer Cloud: Prefer NetWatcher
- Syslog enabled: 
  - Syslog is Active
  - Sensor Syslog is Enabled
  - Tenant Syslog is Enabled
  - Partner Syslog is Enabled
- OpenWrt enabled: 
  - OpenWrt is Active
  - Sensor OpenWrt is Enabled
  - Tenant OpenWrt is Enabled
  - Partner OpenWrt is Enabled

Cancel Save

Heartbeat History

Sensor Config

State - Last Updated: Never

Sensor Setup Warning

274

f. The sensor will then say 'configured' if the sensor can communicate with the NetWatcher Cloud.

Global Filter (clear) | NetWatcher® Multi-Tenant Portal

Home / Sensor / 75894c-862-453a-af2a-02ca20b0464f

### Sensor - LR201411012067

Base Info Get one time pass

- ID: 75894c-862-453a-af2a-02ca20b0464f
- Device: 05a7872b-6581-4172-af39-a1ba3841590f
- Status: Success
- RIM Connected: Not Connected
- Type: HARDWARE
- Name: LR201411012067
- Last Config Check Time: 2017-08-10 17:20:00
- IP: s403aa5a2202ca20b0464f.s.n.w.io
- Local DNS: s403aa5a2202ca20b0464f.s.n.w.io
- Port: Ocean's Edge
- Customer: Ocean's Edge
- User: sensor\_LR201411012067
- Certificate Expiration: Invalid
- Last Event: Last Flow
- Last Heartbeat: 2017-08-10 17:20:00
- Date: 2017-08-10 17:20:00
- Backup: There is no valid certificate found
- Prefer Cloud: Prefer NetWatcher
- Syslog enabled: 
  - Syslog is Active
  - Sensor Syslog is Enabled
  - Tenant Syslog is Enabled
  - Partner Syslog is Enabled
- OpenWrt enabled: 
  - OpenWrt is Active
  - Sensor OpenWrt is Enabled
  - Tenant OpenWrt is Enabled
  - Partner OpenWrt is Enabled

Cancel Save

Heartbeat History

Sensor Config

State - Last Updated: Never

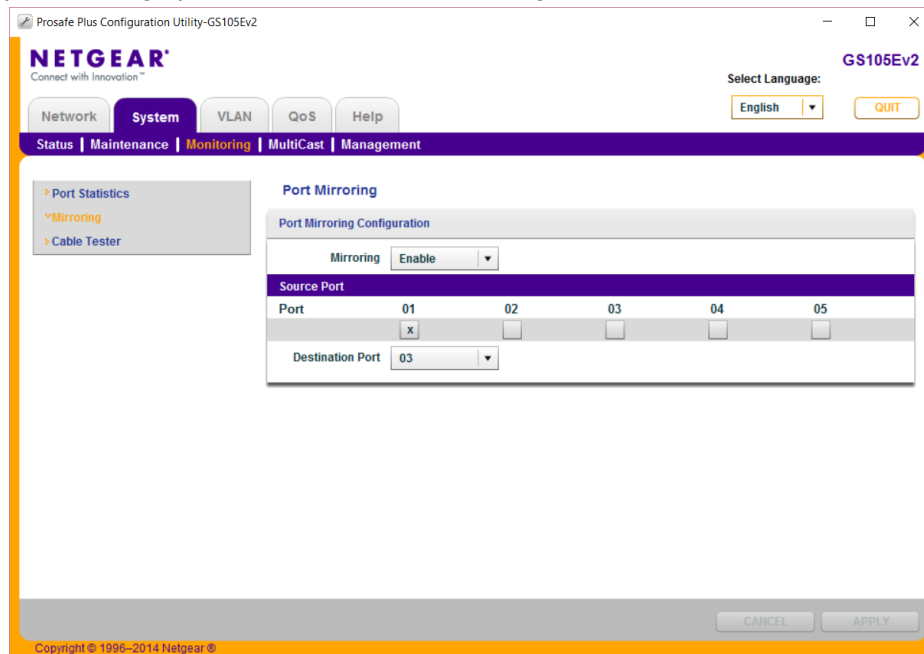
Sensor Setup Success

Red arrow pointing to Sensor Setup button

## Setting up Network Intrusion Detection (NIDS)

5. Create a mirror of the port that the firewall is plugged into on the router/switch

Here is an example of setting up a mirror on a NetGear managed switch:

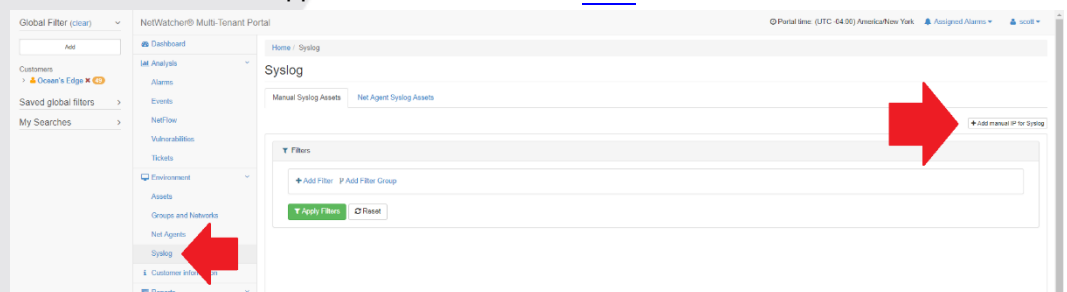


6. Connect the other LAN port on the sensor to the newly created mirror port.
7. Verify the sensor light turns green on the sensors tab in the MPS Portal

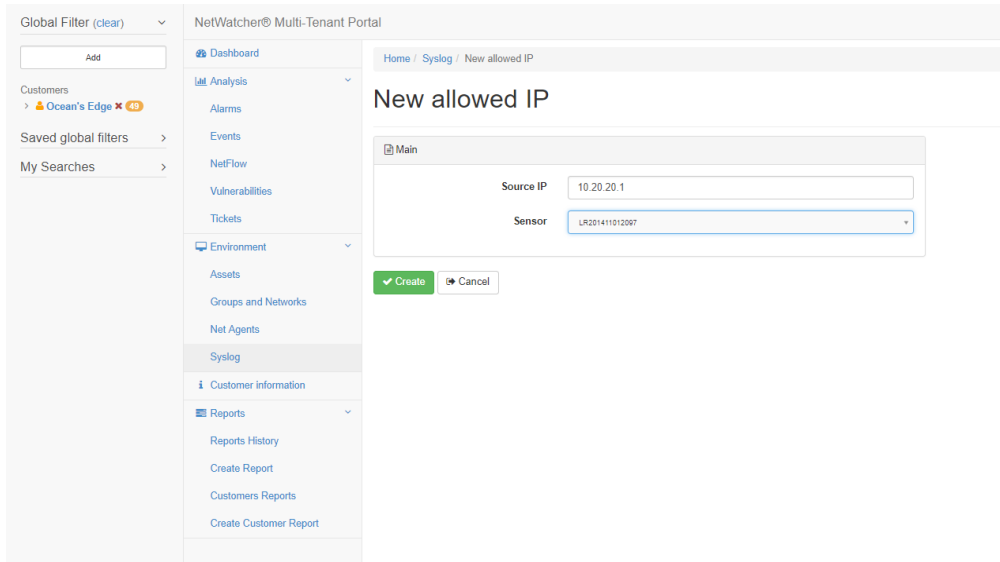
If you are setting up the SIEM for log aggregation this is accomplished in 2 parts (setting up hardware SYSLOGs like firewalls and setting up servers and desktop logs)

## Setting up SYSLOG Ingestion

8. Verify the device you want to monitor is on the supported device list found [here](#).
9. In the MSP Portal go to the "Syslog" tab and Choose "Add manual IP for SYSLOG"



10. Add the IP of the Device



Global Filter (clear) ▾ NetWatcher® Multi-Tenant Portal

Home / Syslog / New allowed IP

### New allowed IP

Main

Source IP: 10.20.20.1

Sensor: LR201411012067

11. Go back to the 'Sensor Details' and select Syslog Questionnaire



Global Filter (clear) ▾ NetWatcher® Multi-Tenant Portal

Home / Sensor / 768fef4c-f682-463a-a8a2-db2ad6b645a4

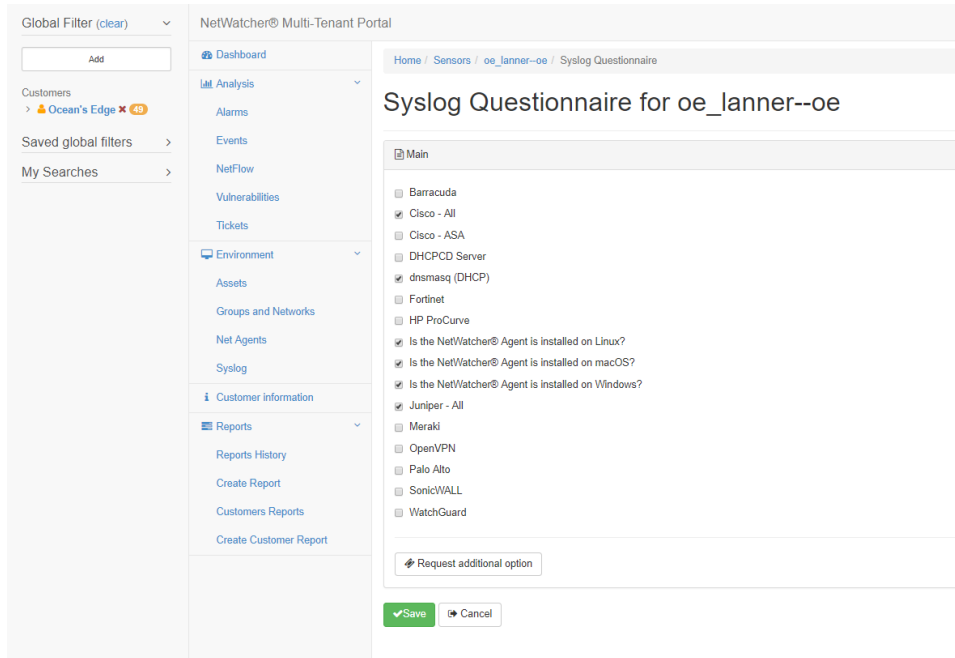
### Sensor - LR201411012067

Base Info  View Suricata Settings  Edit IPTables Settings  Syslog Questionnaire  Get one-time pass

**Id:** 768fef4c-f682-463a-a8a2-db2ad6b645a4

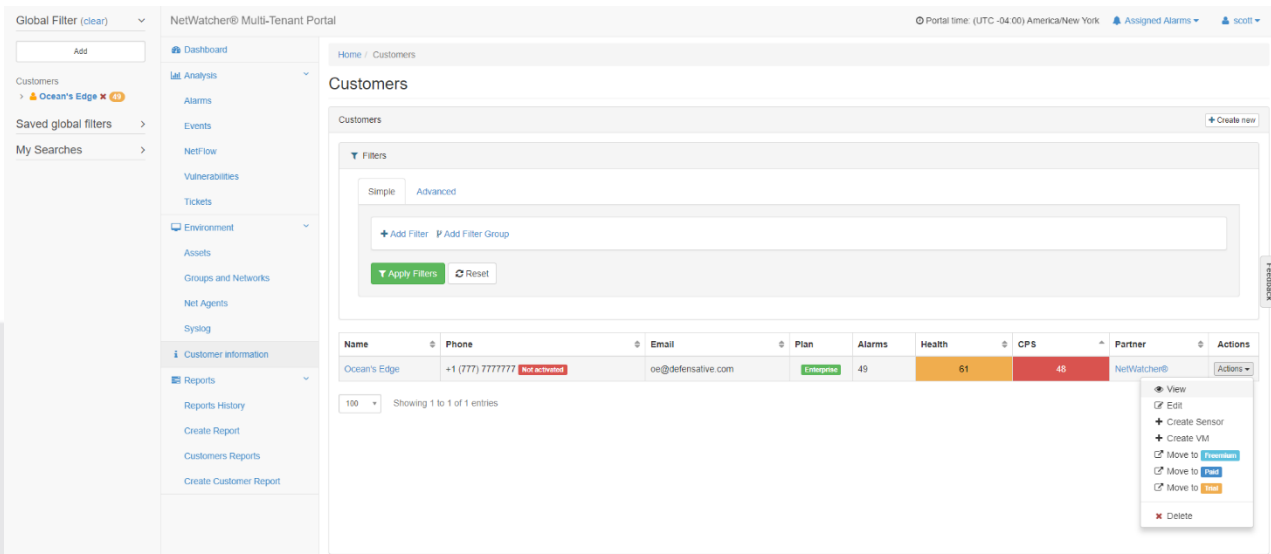
**Device:** 0da7672c-9581-4172-a259-e1ba3841589f

12. Select the device type that is sending the SYSLOG. If it is not on the list, choose 'Ask Question' and specify the device and the DevOps team will enable the ruleset manually.



## Setting up Server / Desktop / Laptop LOGS

- Go to the 'Customers' menu item (<https://dsap.netwatcher.com/customer>) and choose the Actions menu next to the customer name and select 'View'.



- Download the NetAgent (\*\*This binary is unique per customer\*\*)



NetWatcher® Multi-Tenant Portal

Portal time: (UTC -04:00) America/New York | Assigned Alarms | scott

### Customer - Ocean's Edge

Customer details

**ID:** 74be5a83-275f-fc60-8316-aa3cfa21a9b  
**Name:** Ocean's Edge  
**Email:** oe@defensive.com  
**Phone:** +1 (777) 7777777 Not activated  send activation sms

**Partner:** NetWatcher®  
**Groups:** [No](#) [Cisco Rules](#) [M01](#)  
**Date:** 2014-12-28 17:55:27  
**Sync Status:** Sync ID: 40254257

Tenant Synced with ZaidDesk  
External Company Name: Customer: Ocean's Edge

**AuthorizeNet Customer Profile ID:** 1210174495  
**Pcap files are enabled:**

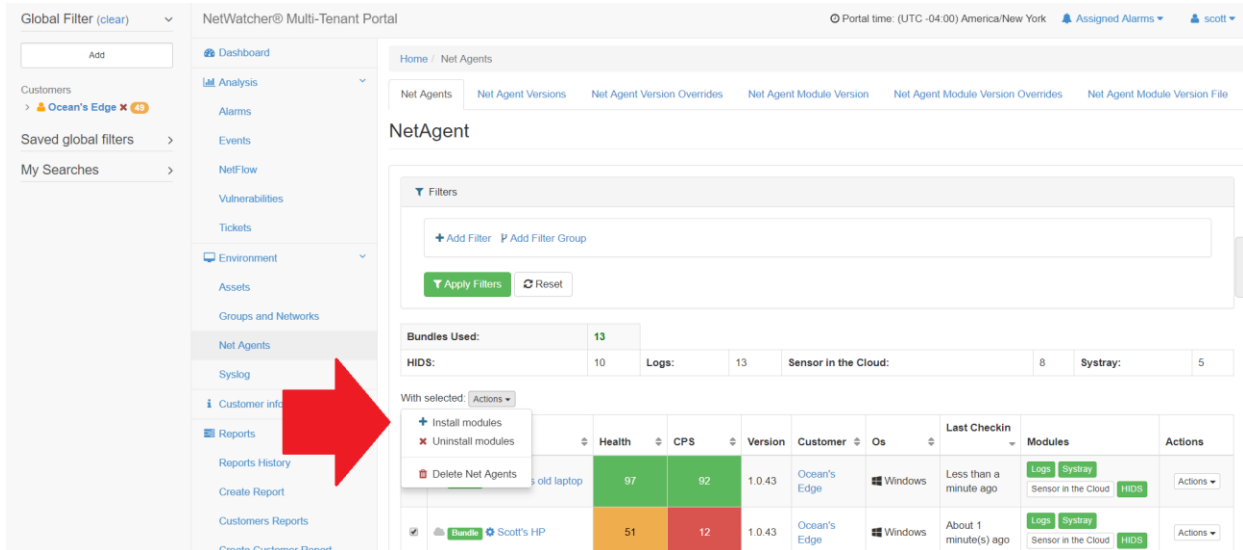
**NetWatcher® Agent** [Download](#)

**Net Agent Settings**

**NXLOG - Module**

syslog_ip	
syslog_ip_cloud	vpn.netwatcher.com
syslog_port_ssl	10514
syslog_port_tcp	10514
syslog_port_udp	514

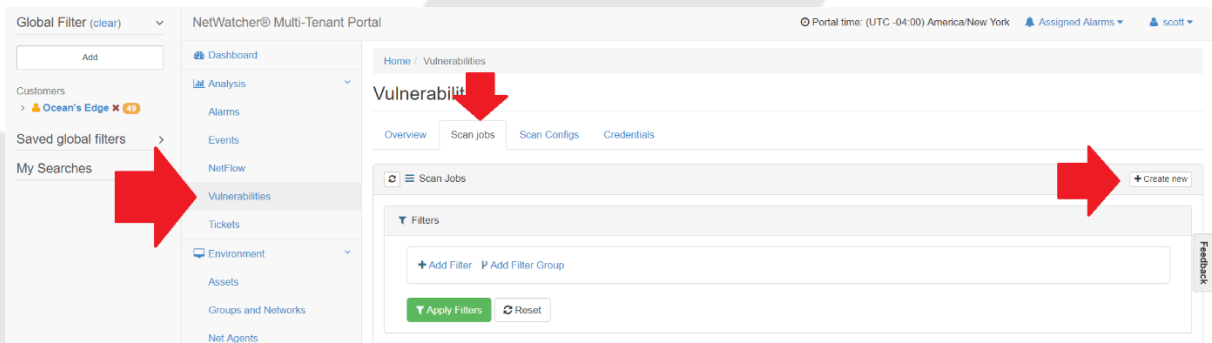
15. Once the NetAgent has been deployed the assets will show up on the NetAgents tab <https://dsap.netwatcher.com/netAgent> (may take a few minutes). Select the agents and choose the Actions dropdown menu and install the LOGs and HIDS modules.



16. The Dialog box will reflect a Pending Install and in a minute or so the Logs will begin to send to the sensor. If the sensor is not live, the Logs will go directly to the cloud over a secure VPN until the sensor goes live again.

## Setting Up Recurring Vulnerability Scans

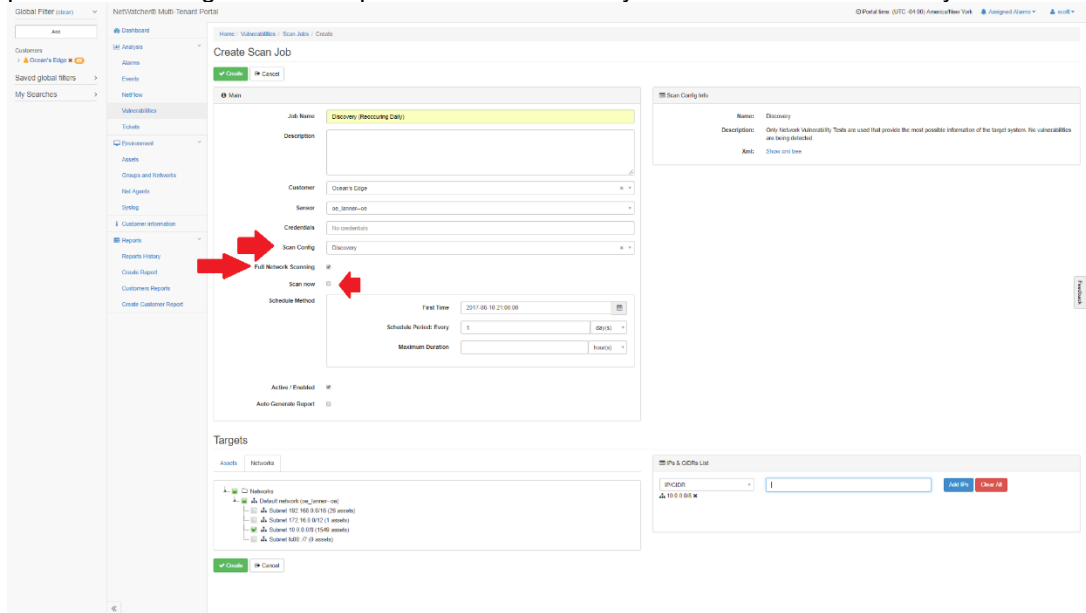
17. Go to the 'Vulnerabilities' tab and choose the 'Create Scan' tab and then choose the 'Create new' button.



18. We want to setup 2 scans (Discovery daily and a Full and Fast on a Weekend)

### Step 1: Setup the Discovery scan.

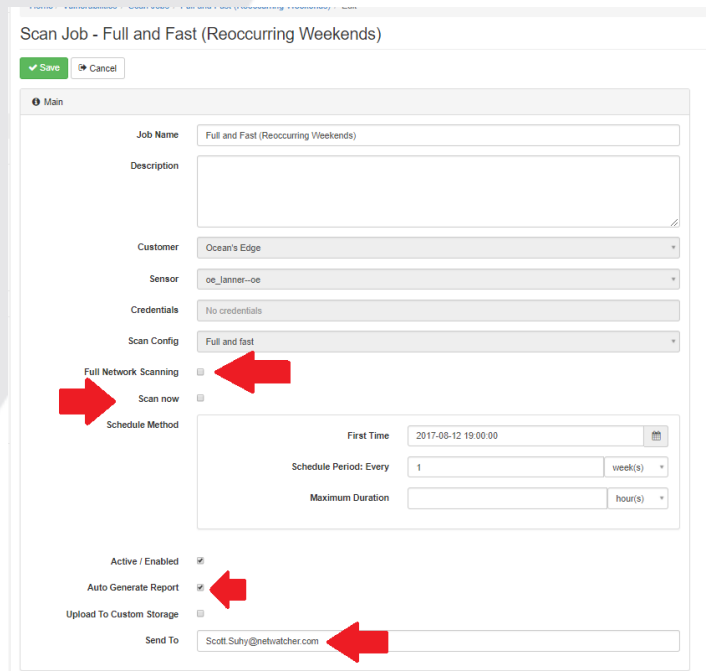
Note how the 'full network scanning' checkbox is checked. This ensures we see every IP in the range provided. Don't generate a report from the Discovery scan as it is not necessary.



### Step 2: Create the Full and Fast Scan

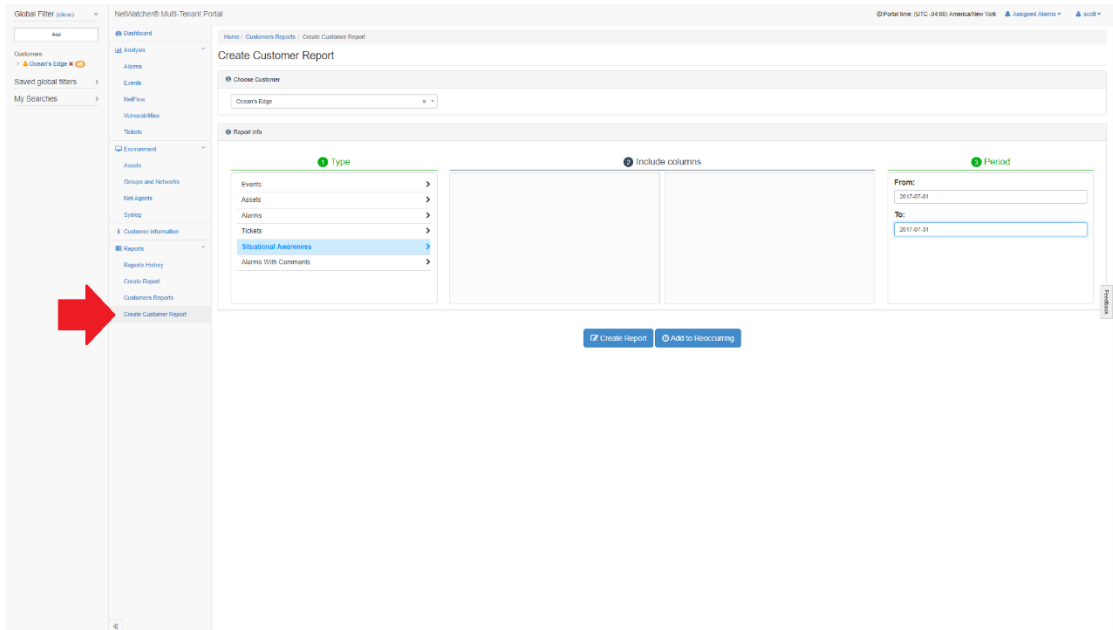
For this scan, you will **not** need to check the 'Full Network Scanning' because the Discovery scan already found all the assets. This will greatly shorten the time the "Full and Fast" scan runs. You also might want to generate a report and have it sent to an email address. To add credentials, go to the credentials tab <https://dsap.netwatcher.com/vulnerabilities#credentials>.

Note: Always schedule the "Discovery" scan at least 2 hours ahead of the "Full and Fast" scan so they don't overlap.

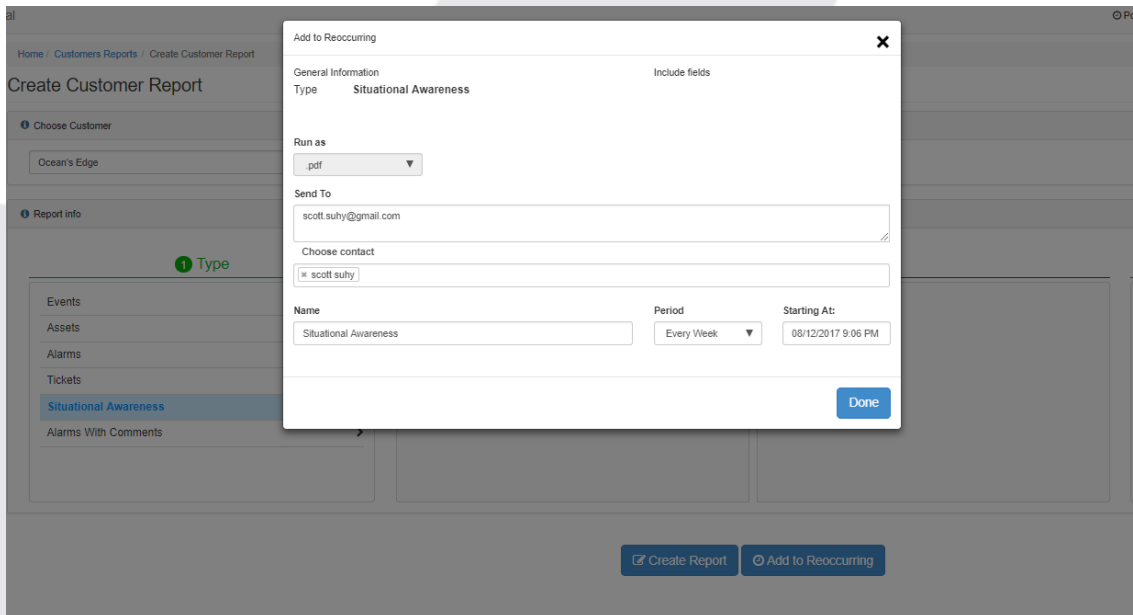


# Setup Reoccurring Reports

19. Go to the 'Reports' tab in the Customer Portal and choose the 'Situational Awareness' report. This gives you an overview of the entire landscape. Create the report from the beginning of a month to the end of a month.

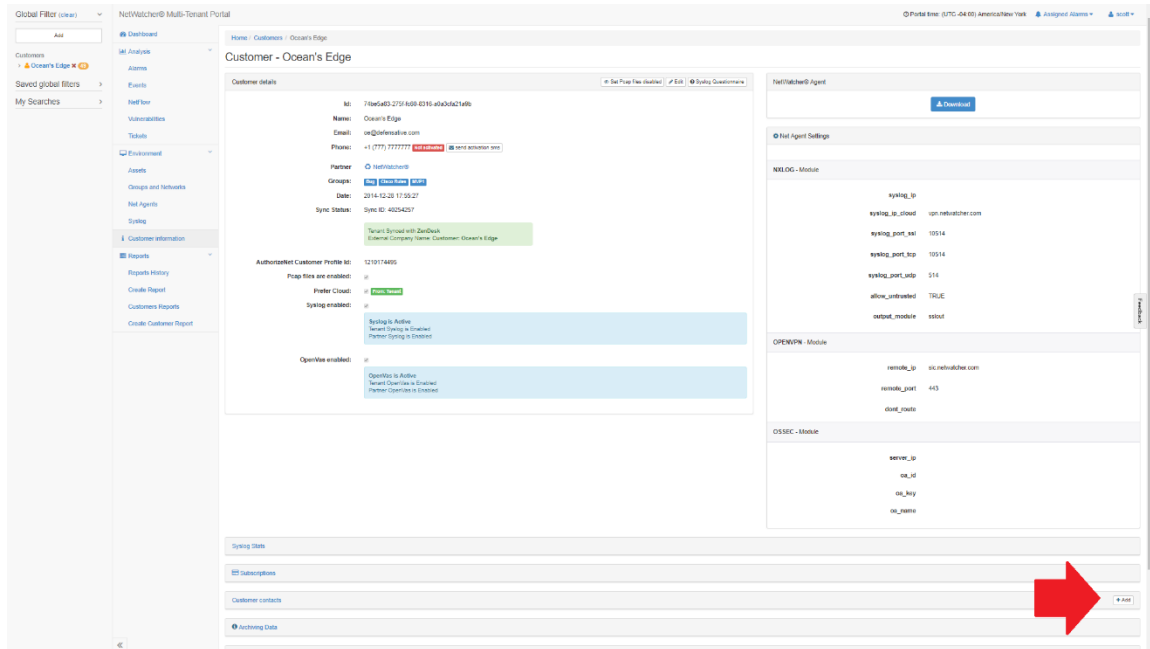


20. Choose where to send the report to (email address, but it will also store it on the portal for you to download in the future) and choose how often you want to receive the report.

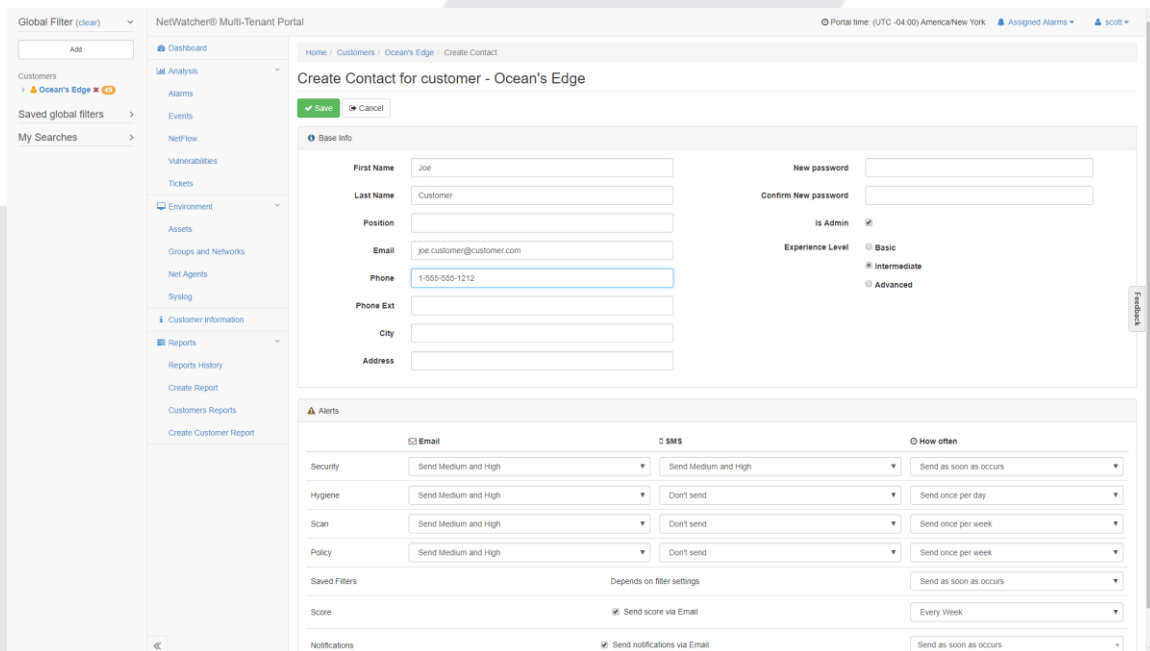


# Setup Notifications for Your Customer Contacts

21. Setup your notifications for your Customer by going back to the customer view on <https://dsap.netwatcher.com/customer> and select the customer. Find the Add button for Customer Contacts

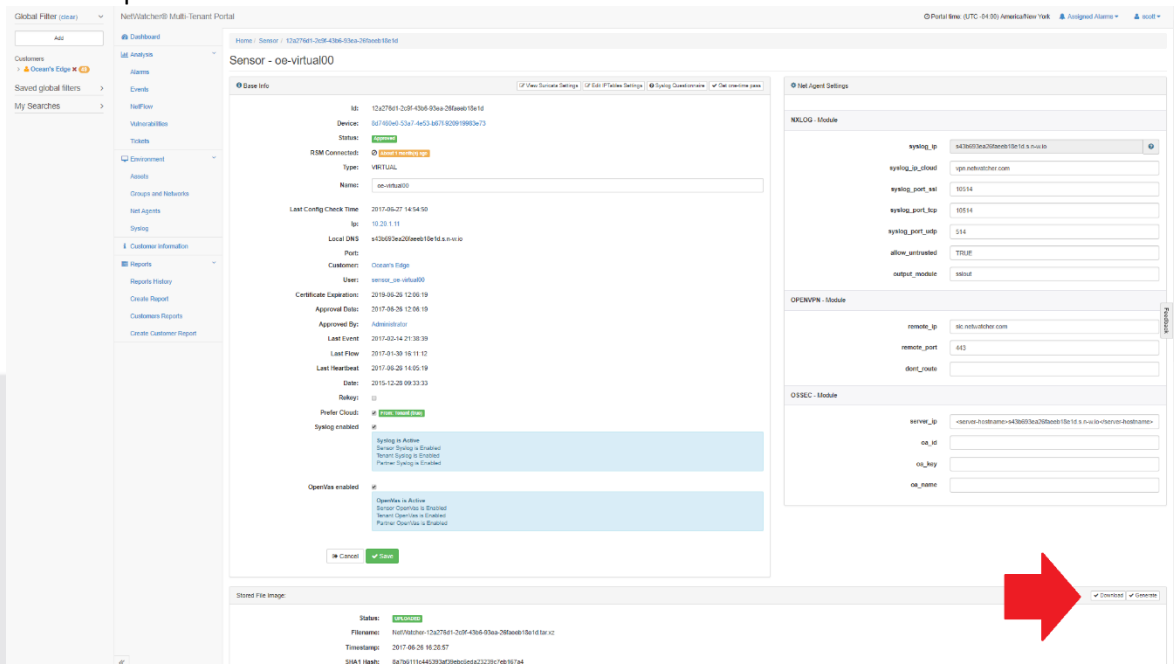


22. Fill in your customer's contact information. This will trigger an Activate email so they can create a password and login to their customer portal at <https://portal.netwatcher.com/login>

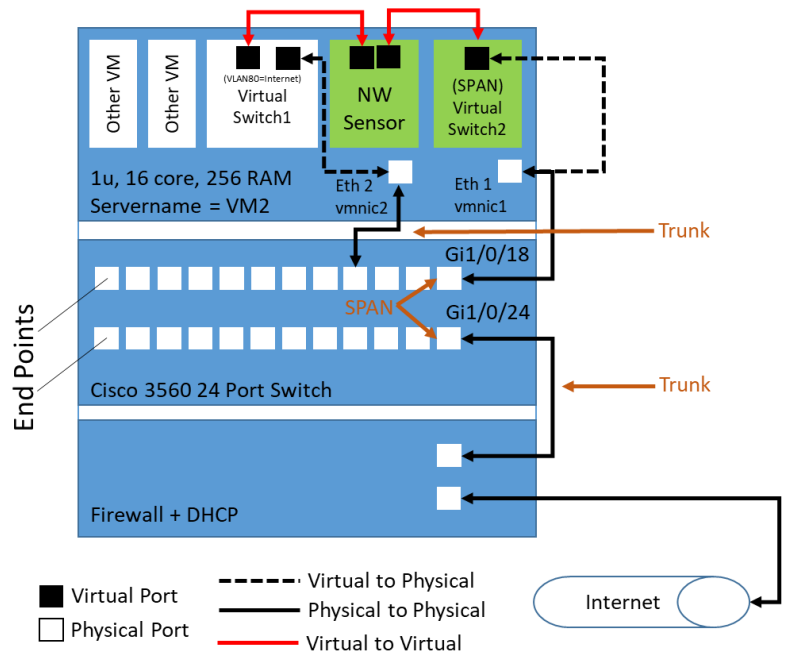


# Connecting Virtual Sensor to NetWatcher Cloud – VSphere

1. Ensure you are not blocking any of the following ports OUTBOUND. These ports are what the sensor uses to communicate back to the NetWatcher cloud.
  - TCP 22 => portal.netwatcher.com
  - TCP 8443 => p.netwatcher.com
  - UDP 443 => vpn.netwatcher.com
  - TCP 443 => vpn-tcp.netwatcher.com
  - TCP 443 => index.docker.io
  - TCP 443 => registry-1.docker.io
  - TCP 443 => public.update.core-os.net
  - TCP 80 to google.com => Used to test internet/DNS connectivity
2. The find the sensor by going to <https://dsap.netwatcher.com/sensor> and click on your Virtual Machine sensor. On the sensor details page press the download button next to the Virtual Machine. It will take a while to download as it's a large file. We use <http://www.7-zip.org> for compression and there is no password. There are two parts, extract the first one and it will continue into the second one. • Unzip, then untar downloaded .xz file. Compare the SHA1 hash.



- Understand your current VM architecture and map out how you will setup your sensor VM. Here is a typical setup:



- Create a mirror of the firewall traffic for the Network Intrusion Detection (NIDS)

Example on a Cisco device: See <https://learningnetwork.cisco.com/docs/DOC-26018>

### Identify Source port for SPAN

```
#show run int Gi1/0/24
```

```
Building configuration...
Current configuration : 92 bytes
interface GigabitEthernet1/0/24
description Trunk to Internet Firewall
switchport mode trunk
end
```

### Identify Destination port for SPAN

```
#show run int Gi1/0/18
```

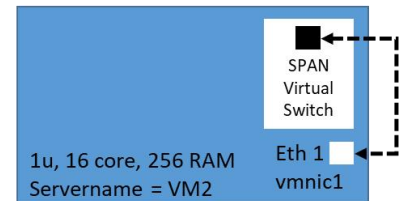
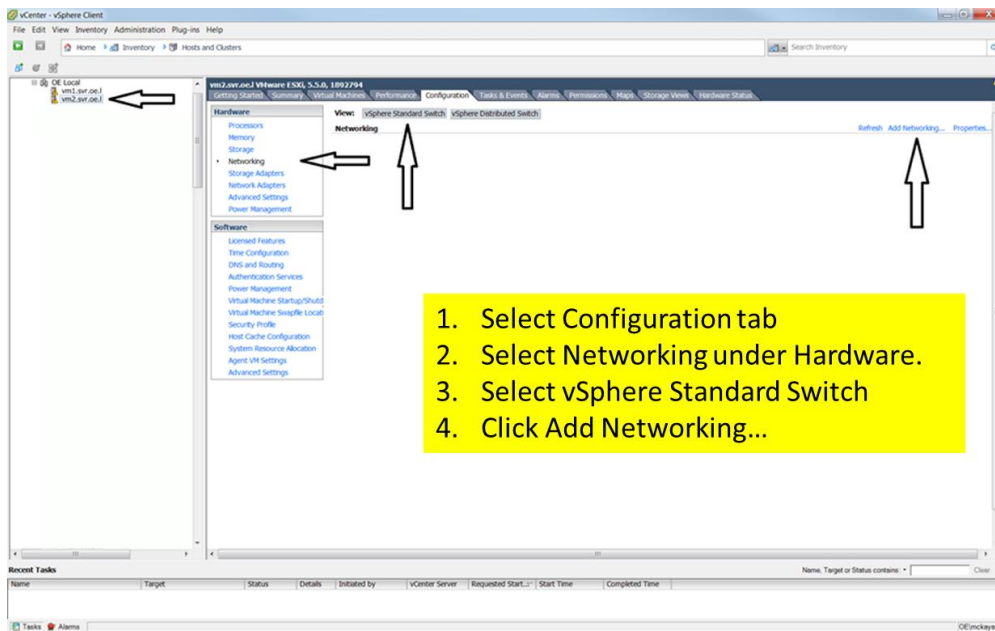
```
Building configuration...
Current configuration : 86 bytes
interface GigabitEthernet1/0/18
description Link to vm2 vmnic1
switchport mode trunk
switchport nonegotiate
end
```

### Configure SPAN:

```
#monitor session 2 source interface Gi1/0/24
```

#monitor session 2 destination interface Gi1/0/18

5. Create a Virtual Switch w/Virtual SPAN Port & Map it to a Physical Port



6. Create a Virtual Switch w/Virtual SPAN Port & Map it to a Physical Port--Create the SPAN Port to mirror all traffic. Set VLAN ID to 4095 (Step 3) to ensure proper handling of VLAN tags.



**1**

**2**

Unselect in use physical ports (vmnic3 above) and select desired dedicated/unused physical port (vmnic1 above).

**3**

Change Network Label to "SPAN Target" and VLAN ID to None (0)

**4**

Click Finish

7. Create a Virtual Switch w/Virtual SPAN Port & Map it to a Physical Port--Enable Promiscuous Mode

**1**

Select Properties, Select vSwitch

**2**

Select Edit

**3**

Select Security Tab

**4**

Enable Promiscuous Mode

8. Import NetWatcher Sensor VM

Run VMWare Converter  
<https://www.vmware.com/products/converter>

**1**

**Click Convert machine:**

- Select source type: VMWare Workstation or other VMWare virtual machine
- Browse to and select .vmtx file among your downloaded files

**2**

**Source System**  
 Select the source system you want to convert

Source type: VMware Workstation or other VMware virtual machine

Virtual machine file: Be1d\NetWatcher - VirtualNetWatcher - OVF.vmtx

**3**

**Click on source details and it should look like this:**

Name: NetWatcher - OVF  
 Machine type: VMware desktop virtual machine  
 Firmwares: BIOS  
 Operating system: Other (32 bit)  
 Total size: 500 GB  
 Number of vCPUs: 4 (4 sockets \* 1 cores)  
 RAM: 4096 MB  
 Network: ethernet0, ethernet1

Source disks/volumes layout:  
 Disk 1 <GPT> - 500 GB  
 EFI-SYSTEM (Volume 1) - 62.97 MB used / 128 MB total <FAT>  
 (Volume 2) - 2 MB used / 2 MB total <unknown>  
 (Volume 3) - 1 GB used / 1 GB total <unknown>  
 (Volume 4) - 1 GB used / 1 GB total <unknown>  
 (Volume 5) - 128 MB used / 128 MB total <unknown>  
 (Volume 6) - 64 MB used / 64 MB total <unknown>  
 (Volume 7) - 497.68 GB used / 497.68 GB total <unknown>

**4**

**Click Next.**  
 Select Destination type: VMware Infrastructure virtual machine  
 Server: This is your ESXi/vSphere cluster and login credentials.



## 9. Import NetWatcher Sensor VM

1

2

3

4

## 10. Import NetWatcher Sensor VM

Let it build.

## 11. Map NetWatcher Sensors Network Adapter 1 and Network Adapter 2

1 Log into vCenter

2 Navigate to newly created VM -> Click vCenter, VMs and Templates, locate where you placed the VM

3 Click Edit Virtual Machine Settings

4 Make Network Adapter 1 point to a network with DHCP and which will have access to the internet (VLAN80 in this case) and Network Adapter 2 point to 'SPAN Target'

12. Open NetWatcher Sensor Console

Click Power on the virtual machine

Click Actions -> Open Console Verify IP Address

```

[ 158.186482] device veth06e971 left promiscuous mode
[ 158.187865] docker0: port 1(veth06e971) entered disabled state
[ 158.98469] device veth1a7794 entered promiscuous mode
[ 158.982216] IPv6: ADDRCONF(NETDEV_UP): veth1a7794: link is not ready
[ 158.998142] IPv6: ADDRCONF(NETDEV_CHANGE): veth1a7794: link becomes ready
[ 158.991969] docker0: port 1(veth1a7794) entered forwarding state
[ 158.993593] docker0: port 1(veth1a7794) entered forwarding state
[ 159.019966] docker0: port 1(veth1a7794) entered disabled state
[ 159.027311] eth0: renamed from veth1a65ca2ef
[ 159.035431] docker0: port 1(veth1a7794) entered forwarding state
[ 159.035191] docker0: port 1(veth1a7794) entered forwarding state
[ 163.521196] tun: Universal TUN/TAP device driver, 1.6
[ 163.522269] tun: (C) 1999-2004 Max Krasnyansky <maxk@qualcomm.com>
[ 174.051508] docker0: port 1(veth1a7794) entered forwarding state

This is localhost (Linux x86_64 4.2.2-coreos-r1) 17:37:35
SSH host key: SHA256:Rc5LIntsLwS6GR1qgZ3Dn6Z41P-r0gbyuJ06B080 (RSA)
SSH host key: SHA256:6bnv250R1p80XfRg1LX0X30w0LX21u1e9cz8tjU (ED25519)
SSH host key: SHA256:Br42YRkMkka+Inh45Fw/cb10LFBjBFX38tCf12X1N02o (RSA)
eno16777728: 18.28.7.65 fe80::258:56ff:fe8a:e9c7
eno3354952: fe80::258:56ff:fe8a:d144

localhost login: _
    
```

13. If you need to setup a static IP address see [this article](#).

14. Login to the Customer Portal to Verify Sensor is Live (Sensor will turn amber if it can connect to the NetWatcher cloud; Sensor will turn green if it can also see the mirror/SPAN traffic)

## Installing the Virtual Sensor on Other Virtual Machine Platforms

- For VMWare workstation (for testing only, not production) find details [here](#)
- For Hyper-V find details [here](#)

We hope you enjoy the NetWatcher service. We've designed the service to be useful for managers, help desk techs and for advanced security analysts. We've tried to make the User Interface (UI) intuitive and easy to use as well as powerful. If you have any questions don't hesitate to contact us at [info@netwatcher.com](mailto:info@netwatcher.com)

Follow us on Twitter [@netwatcher](#).

<https://netwatcher.com>