COMODO
Creating Trust Online®

cWatch

Comodo

cWatch Network

Software Version 3.3

NxSensor Installation Guide

Guide Version 3.3.010820

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1 Introduction

NxSensor is a monitoring tool that listens to network traffic and provides additional visibility for cWatch over network activity.

- NxSensor is used to communicate *network* information to cWatch. Endpoint monitoring is carried out by installing Nxlog and Rsyslog (as described in this guide)
- Customers who wish to add network monitoring in addition to endpoint monitoring should setup NxSensor
- NxSensor functionality is also available to trial customers.

2 NxSensor Installation

- **Requirements**
- **Create Installation Media (Option 1)**
- **Deploy Virtual Machine Environment (Option 2)**
- **Sensor Installation Steps**
- **Sensor Configuration Steps**

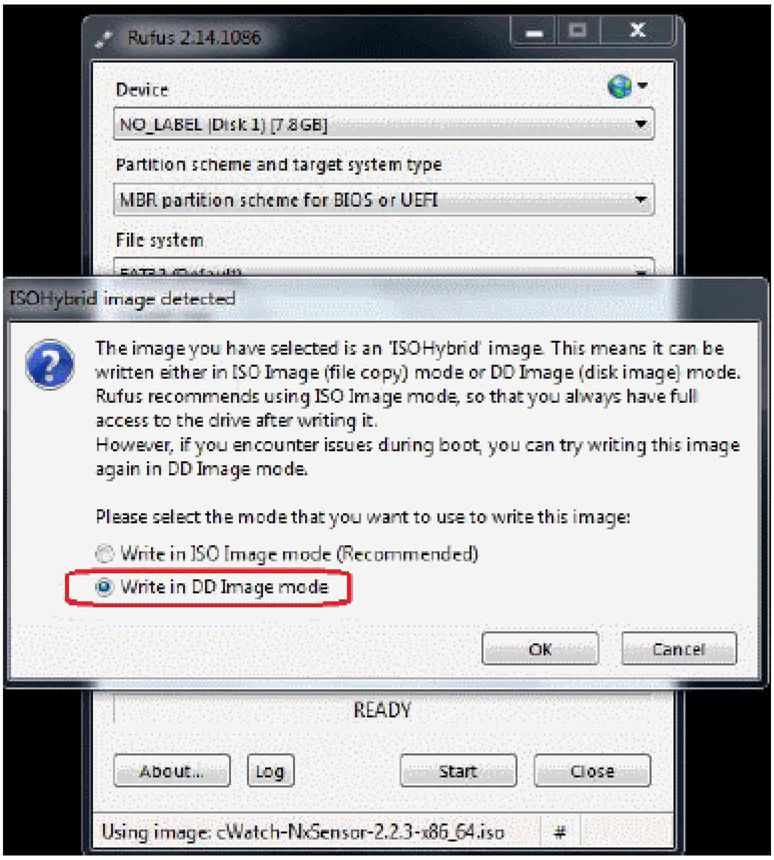
2.1 Requirements

- Quad Core CPU (4 x 2.40 Ghz)
- 8GB RAM
- 64GB available hard disk space
- 2 ethernet ports

3 (Option 1) Create Installation Media

This step is required only if you intend to install the cWatch Sensor to a hardware appliance.

- Insert a 2 GB or higher USB flash drive into your computer
- Start Rufus*
- Choose the downloaded sensor ISO and click “Start”
- At the next window choose 'Write in DD Image mode'


Rufus 2.14.1086
Device
NO_LABEL (Disk 1) [7.8GB]
Partition scheme and target system type
MBR partition scheme for BIOS or UEFI
File system
FAT32 (Default)

ISOHybrid image detected

The image you have selected is an 'ISOHybrid' image. This means it can be written either in ISO Image (file copy) mode or DD Image (disk image) mode. Rufus recommends using ISO Image mode, so that you always have full access to the drive after writing it.
However, if you encounter issues during boot, you can try writing this image again in DD Image mode.

Please select the mode that you want to use to write this image:

○ Write in ISO Image mode (Recommended)

● Write in DD Image mode

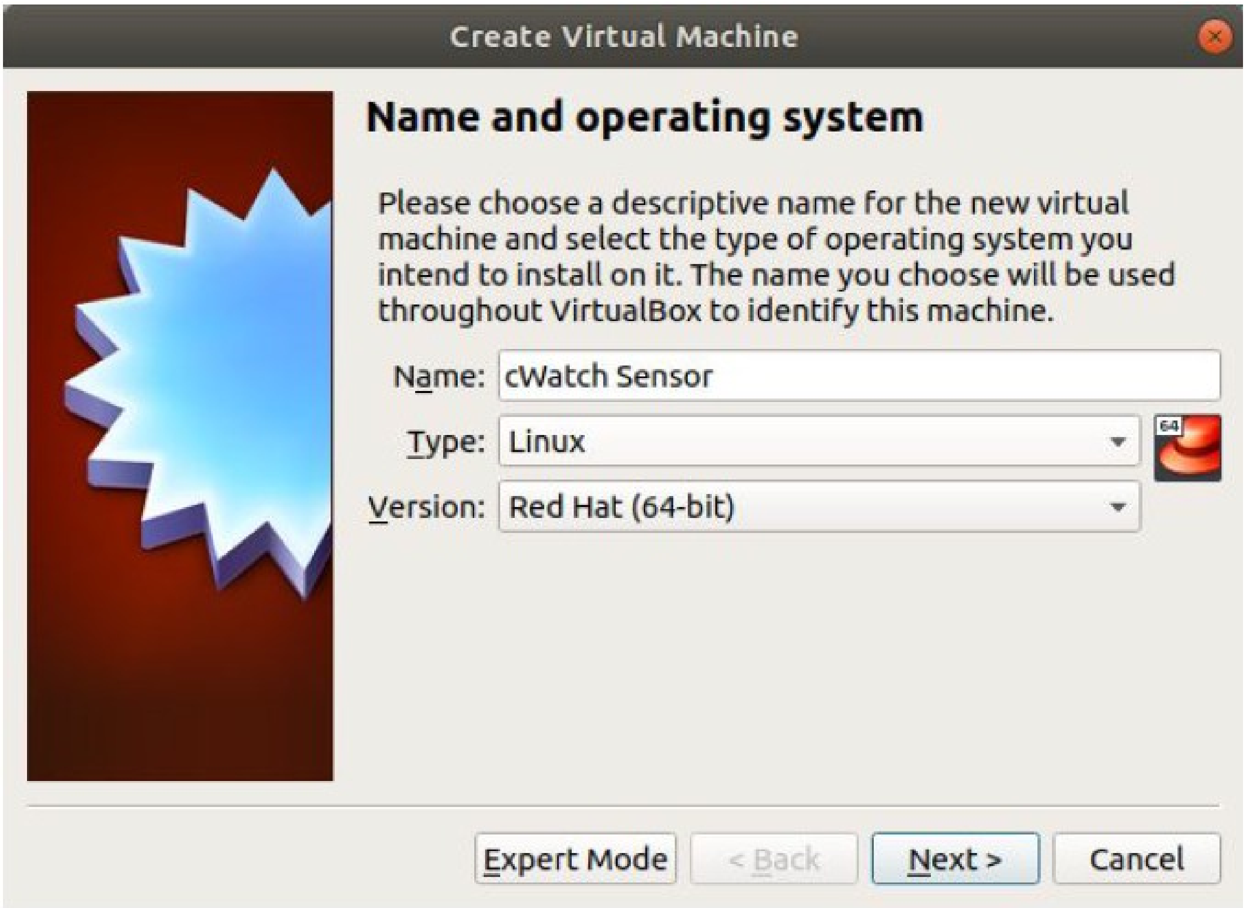
Using image: cWatch-NxSensor-2.2.3-x86_64.iso

4 (Option 2) Deploy Virtual Machine Environment

This step is required only if you intend to install the cWatch Sensor to a virtual environment.

4.1 Create a New Virtual Machine

- Create a new VirtualBox VM.
- Name as “cWatch Sensor”.
- Select the type as “Linux”.
- Select the version as “Red Hat (64-bit)”.



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.

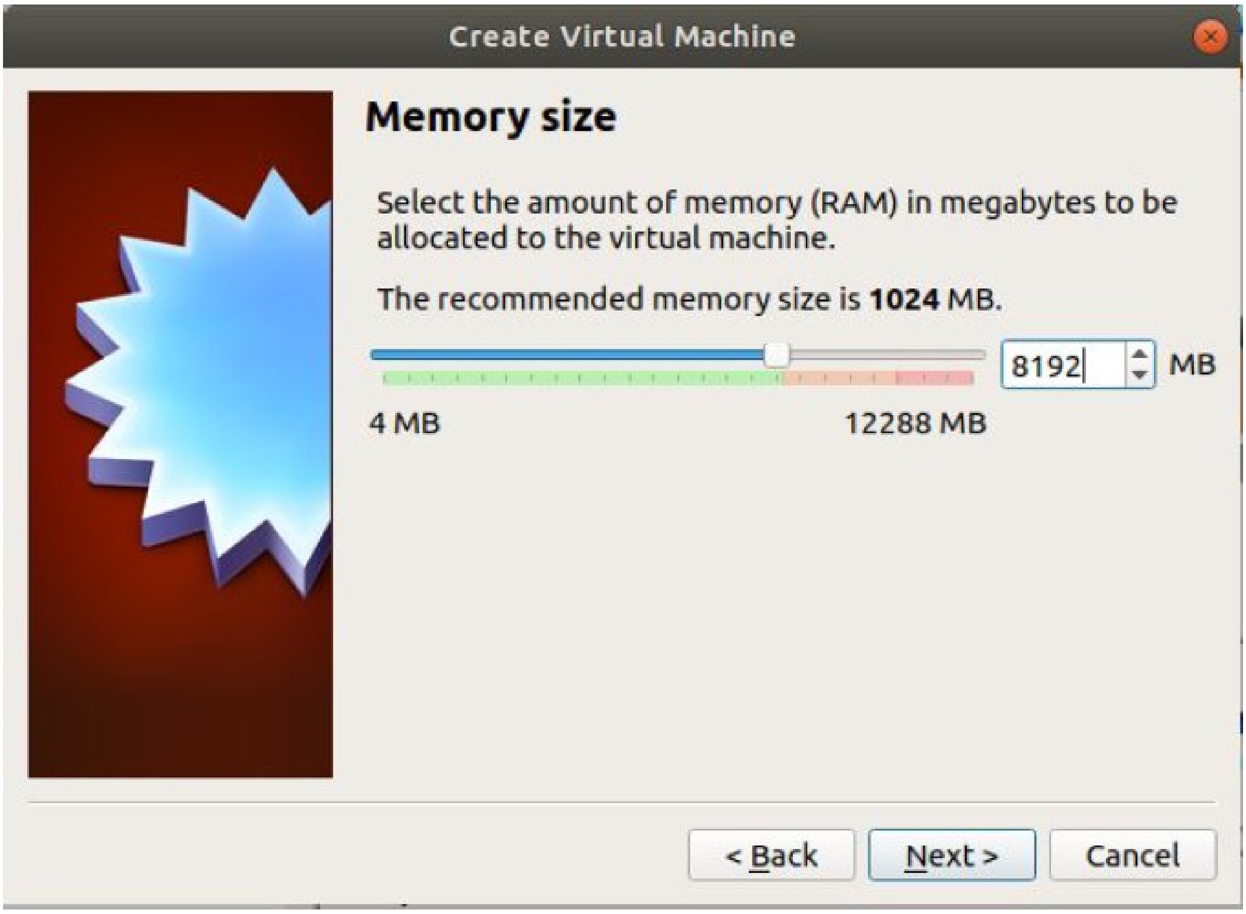
Name: cWatch Sensor

Type: Linux

Version: Red Hat (64-bit)

4.2 Configure Memory Size

- The minimum amount of memory required for the virtual machine is 8GB RAM.



Create Virtual Machine

Memory size

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

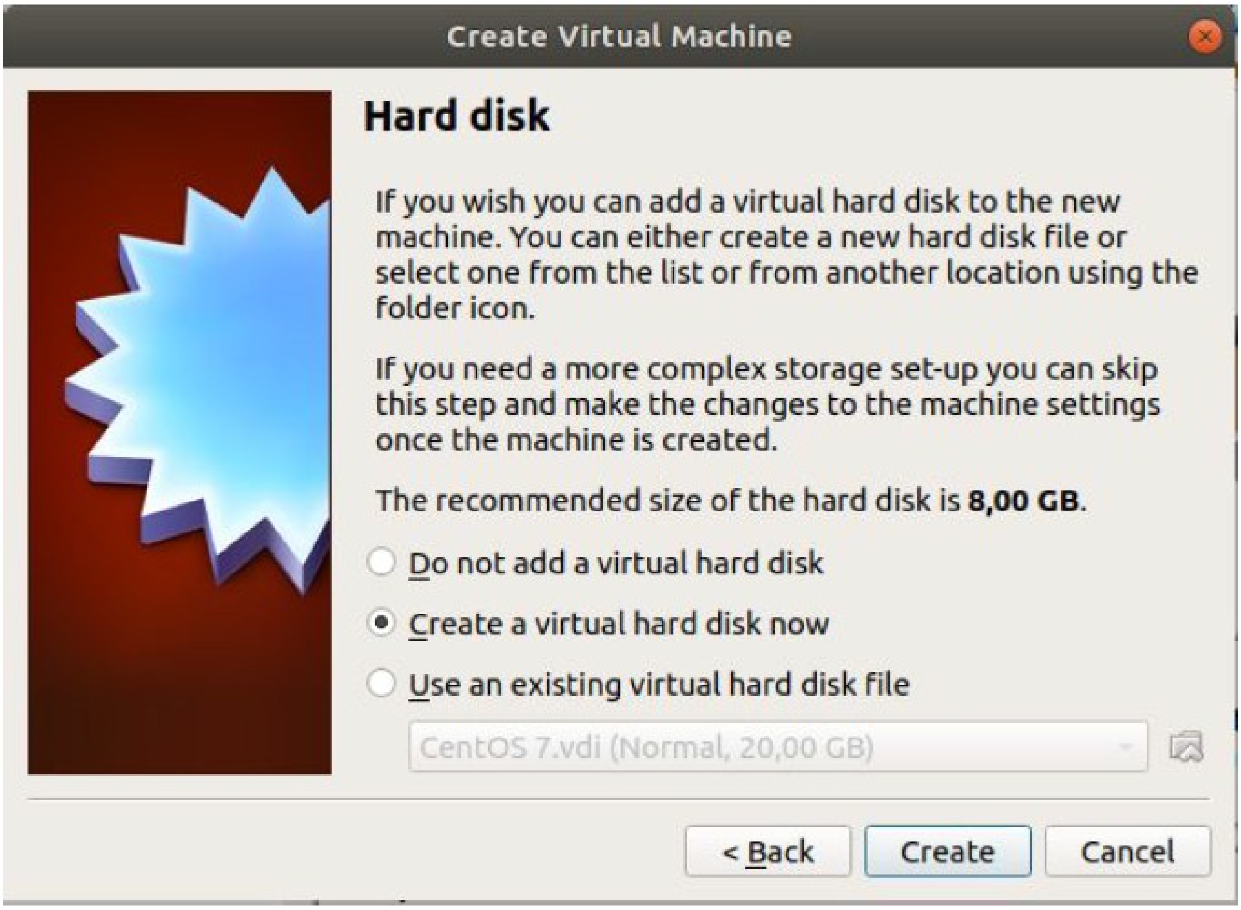
The recommended memory size is **1024** MB.

8192 MB

- Click 'Next'

4.3 Configure Hard Disk

- Select 'Create a virtual hard disk now'



Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk 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 disk is **8,00 GB**.

○ Do not add a virtual hard disk

● Create a virtual hard disk now

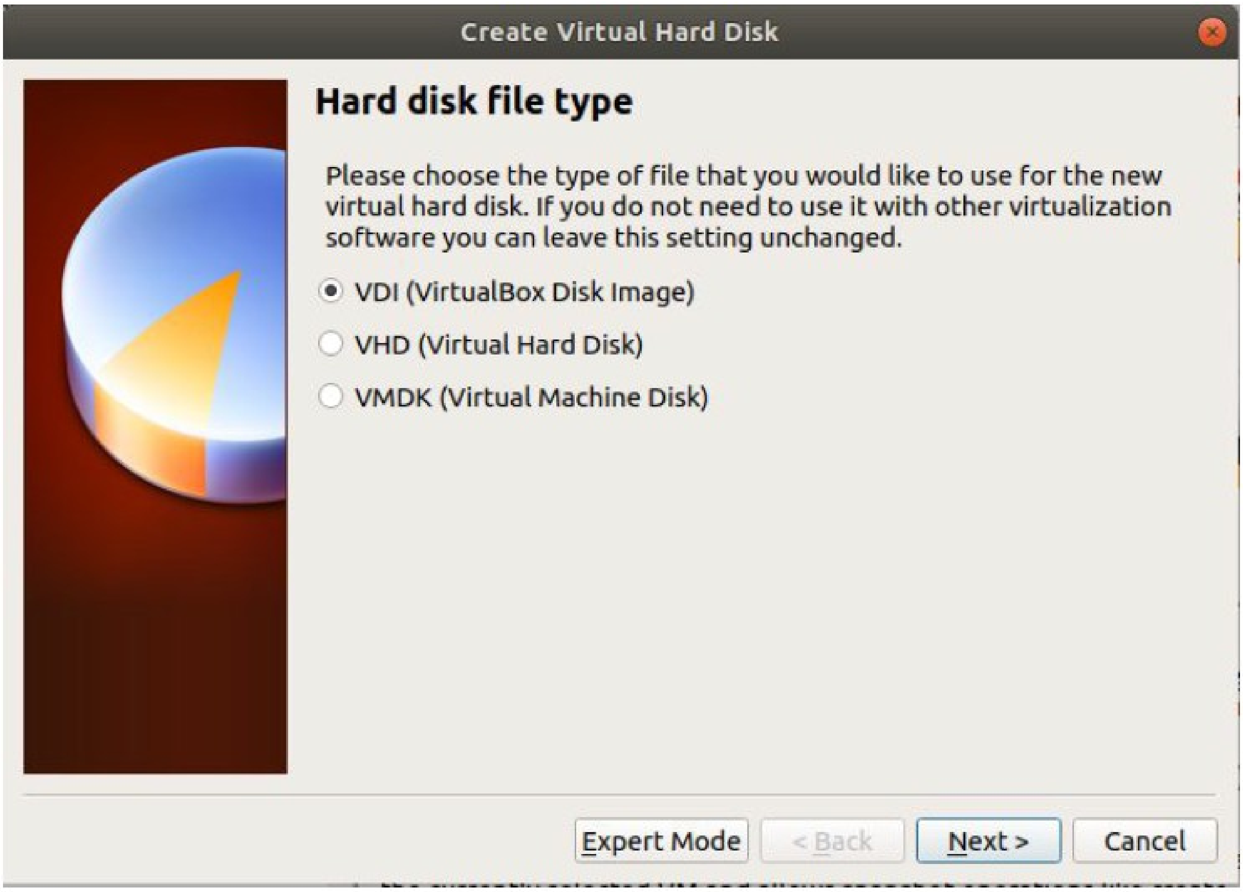
○ Use an existing virtual hard disk file

CentOS 7.vdi (Normal, 20,00 GB)

- Click 'Create'

4.4 Configure Hard Disk File Type

- Select “VDI (VirtualBox Disk Image)”



Create Virtual Hard Disk

Hard disk file type

Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

● VDI (VirtualBox Disk Image)

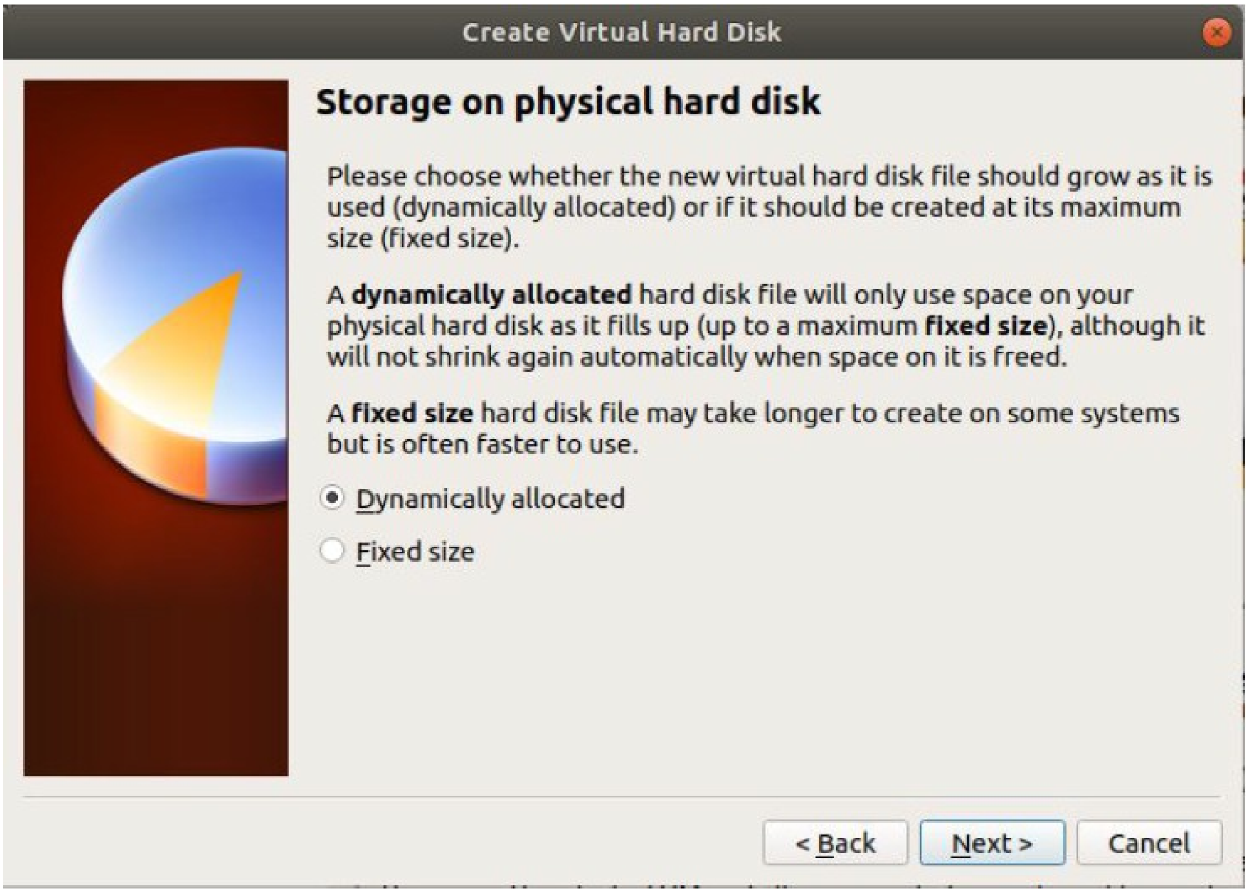
○ VHD (Virtual Hard Disk)

○ VMDK (Virtual Machine Disk)

- Click Next'

4.5 Configure Storage on Physical Hard Disk

- Select “Dynamically allocated” to allow the virtual disk to increase the space size if needed



Create Virtual Hard Disk

Storage on physical hard disk

Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

A **dynamically allocated** hard disk file will only use space on your physical hard disk as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

A **fixed size** hard disk file may take longer to create on some systems but is often faster to use.

● Dynamically allocated

○ Fixed size

- Click 'Next'

4.6 Configure Size of Virtual Hard Disk

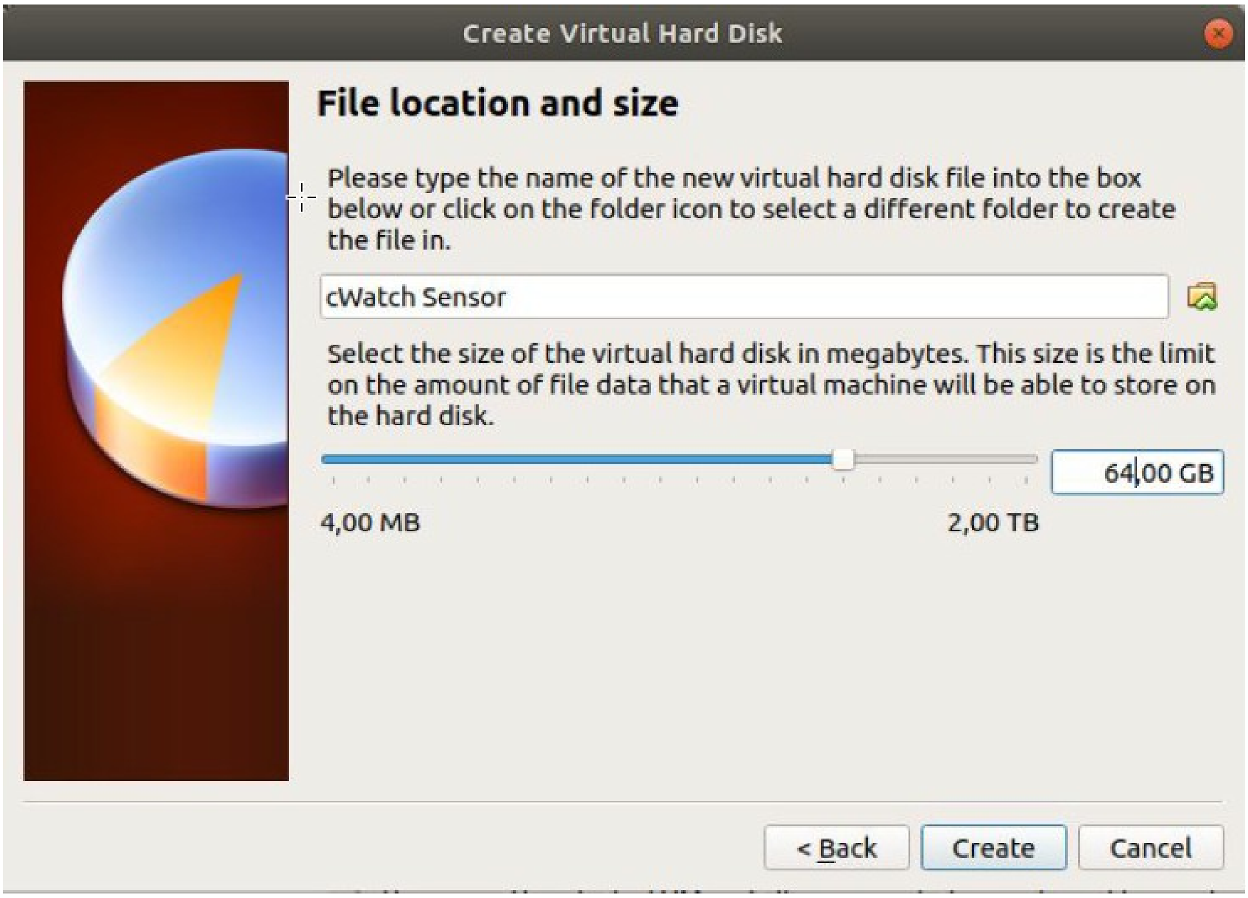
- The next step is to select the location and size of the file.

To do this:

- Leave the default name “cWatch Sensor”

  OR

- (Optional) Select the folder icon to change the location of the virtual disk on your host machine
  - The default location is “C:\Users\ [yourUser] \VirtualBox Vms\”
- Set 64GB to the virtual disk



File location and size

Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

cWatch Sensor

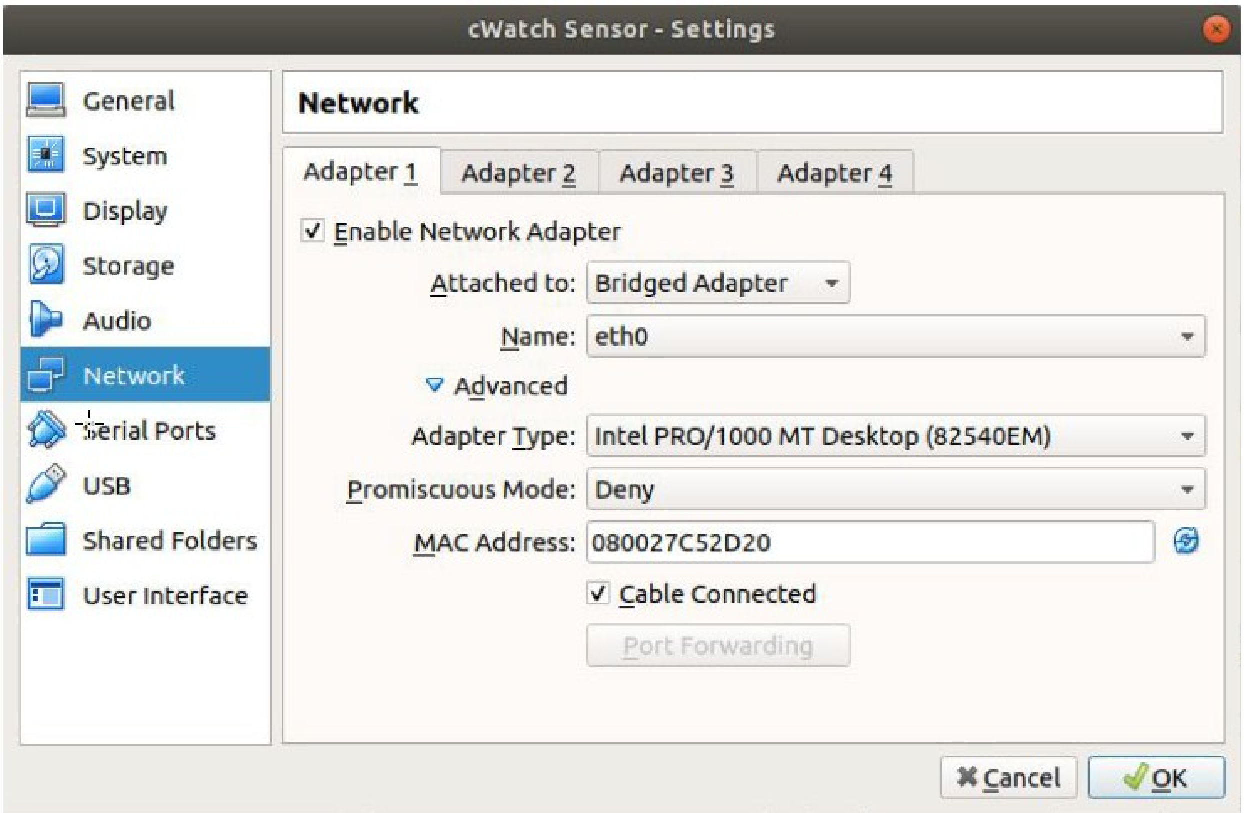
Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

64,00 GB

- Click 'Create'

4.7 Configure Network Settings

- Right-click the VM in VirtualBox then select 'Settings'
- Select 'Network' on the left menu
  - Adapter 1
    - Attached to: 'Bridged Adapter'
    - Name: <YOUR MANAGEMENT INTERFACE>



☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: eth0

Advanced

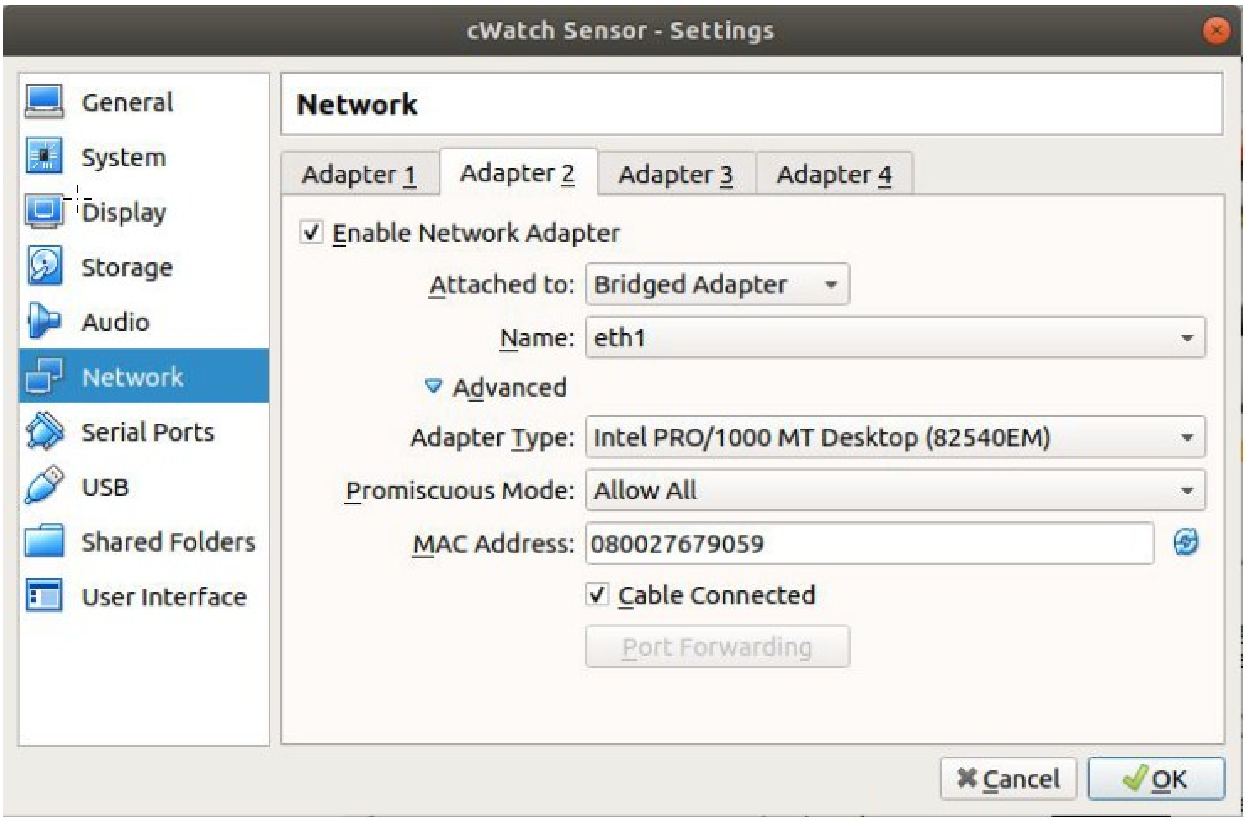
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 080027C52D20

☑ Cable Connected

- Adapter 2
  - Select 'Enable Network Adapter'
  - Attached to: 'Bridged Adapter'
  - Name: <YOUR CAPTURE INTERFACE>
  - Promiscuous Mode: 'Allow All'



☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: eth1

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

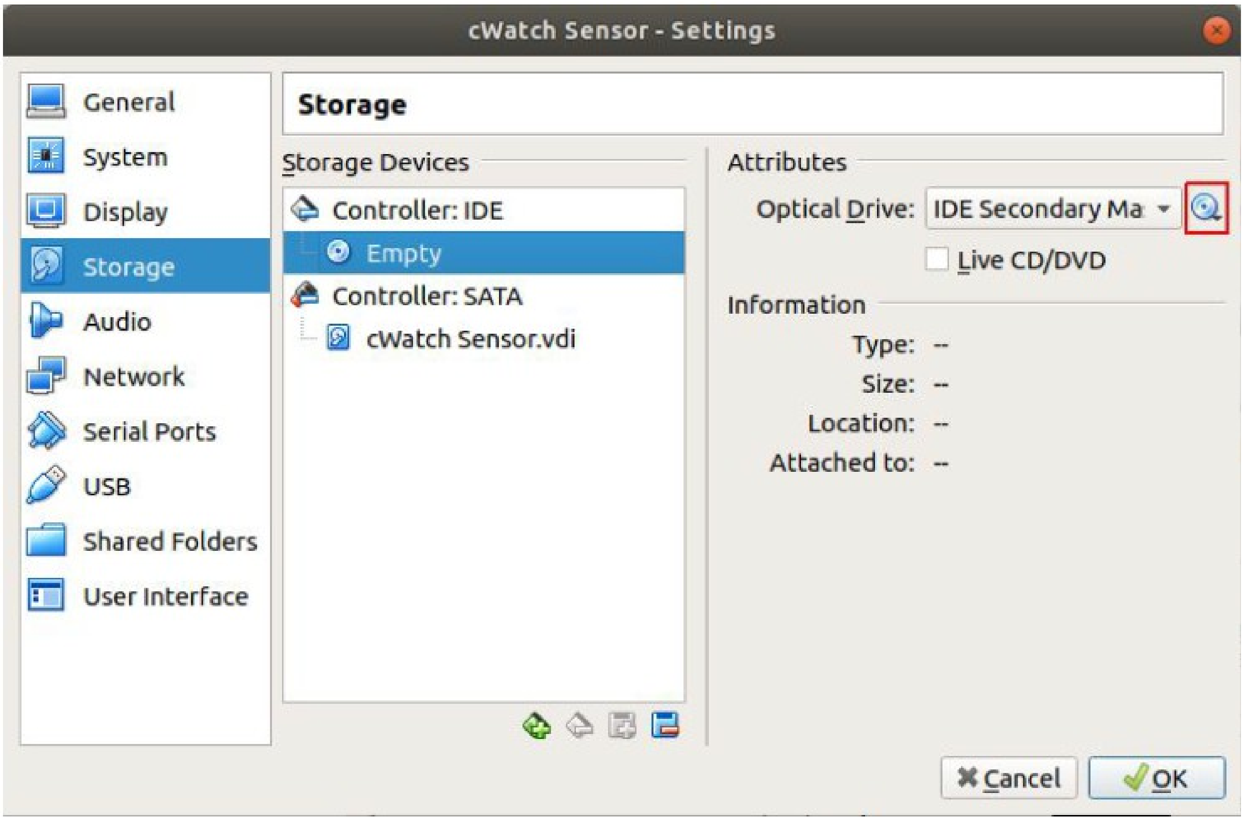
Promiscuous Mode: Allow All

MAC Address: 080027679059

☑ Cable Connected

4.8 Select VM Startup Disk

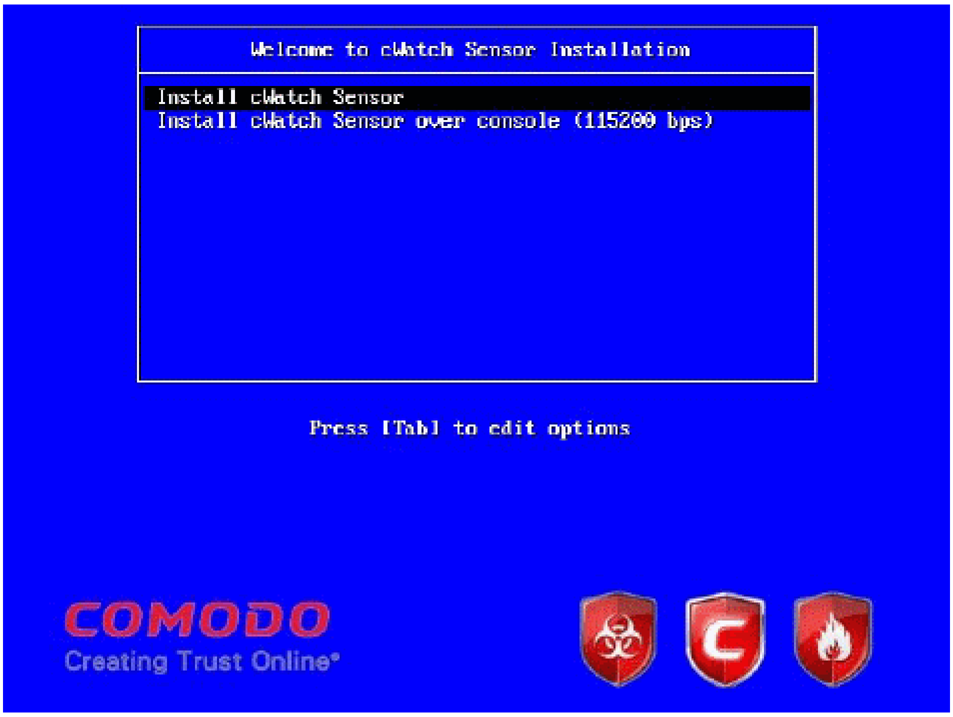
- Select 'Storage' in the left-hand menu
- Click the disk icon and select cWatch Sensor ISO from the files



- Click 'OK' to start the installation of cWatch Sensor.

5 Sensor Installation Steps

- Connect the interface with access to internet to eth0 and connect the mirrored port to eth1 of the sensor.
- Install the sensor software:
  - **Physical appliance** - Insert the previously created **USB media** which contains the sensor ISO in bootable format. Boot the appliance with the USB installed.
  - **Virtual Machine** - Mount the .iso on the virtual optical drive and start the VM
    - Please make sure that the capture interface of the VM allows promiscuous mode
    - If you do not see 64-bit VM profiles you may wish to double-check that VT is enabled in the BIOS.
- When the cWatch Sensor boot splash prompt is visible, please choose the appropriate option.
  - “Install cWatch Sensor” is the regular installation option on virtual devices and hardware devices with display output.
  - If you want to install the appliance on hardware over a console cable, please select “Install cWatch Sensor over console (115200 bps)” option.

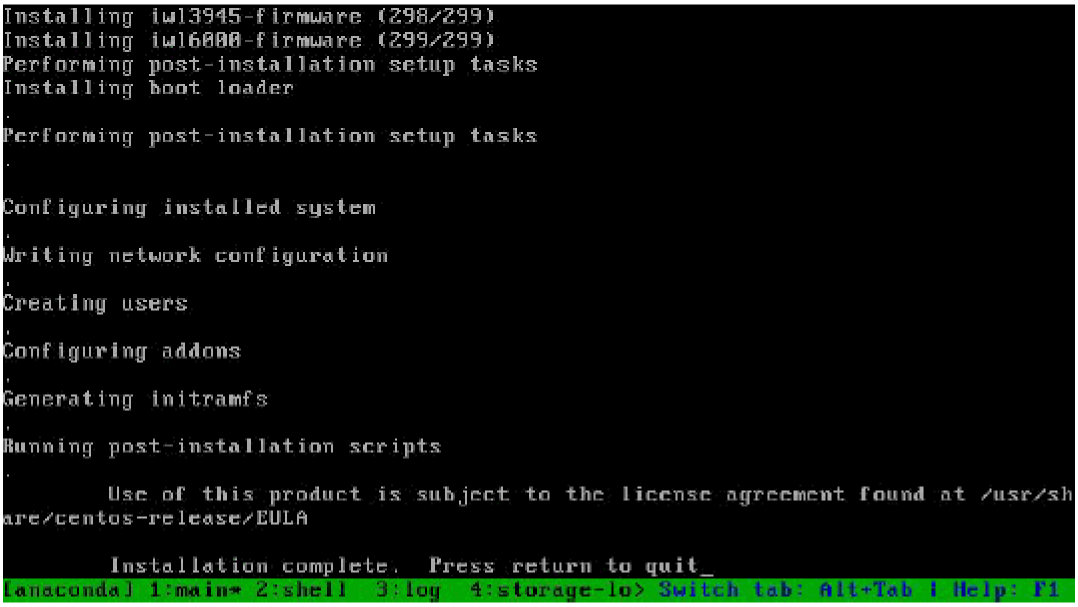


```
Welcome to cWatch Sensor Installation

Install cWatch Sensor
Install cWatch Sensor over console (115200 bps)

Press [Tab] to edit options
```

- The following screen is shown when installation is complete. Press ENTER to finish installation.

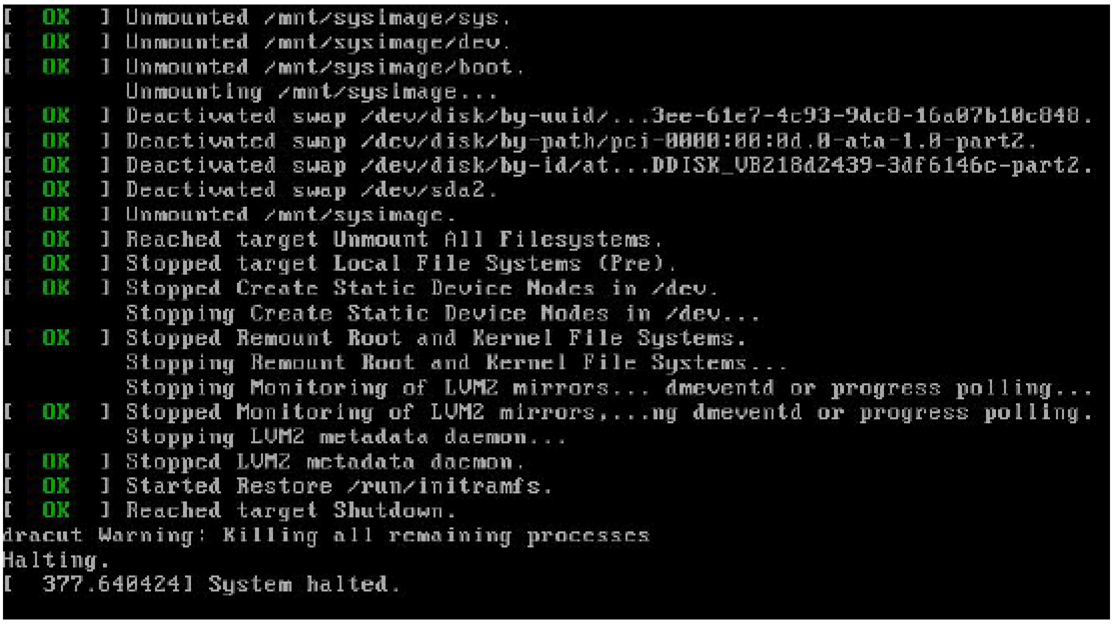


```
Installing iwl3945-firmware (298/299)
Installing iwl6000-firmware (299/299)
Performing post-installation setup tasks
Installing boot loader
.
Performing post-installation setup tasks
.

Configuring installed system
.
Writing network configuration
.
Creating users
.
Configuring addons
.
Generating initramfs
.
Running post-installation scripts
.
        Use of this product is subject to the license agreement found at /usr/sh
are/centos-release/EULA

        Installation complete.  Press return to quit_
[anaconda] 1:main* 2:shell  3:log  4:storage-lo> Switch tab: Alt+Tab | Help: F1
```

- You need to wait until the “System Halted” message appears:



```
[  OK  ] Unmounted /mnt/sysimage/sys.
[  OK  ] Unmounted /mnt/sysimage/dev.
[  OK  ] Unmounted /mnt/sysimage/boot.
         Unmounting /mnt/sysimage...
[  OK  ] Deactivated swap /dev/disk/by-uuid/...3ee-61e7-4c93-9dc8-16a07b10c848.
[  OK  ] Deactivated swap /dev/disk/by-path/pci-0000:00:0d.0-ata-1.0-part2.
[  OK  ] Deactivated swap /dev/disk/by-id/at...DDISK_VB218d2439-3df6146c-part2.
[  OK  ] Deactivated swap /dev/sda2.
[  OK  ] Unmounted /mnt/sysimage.
[  OK  ] Reached target Unmount All Filesystems.
[  OK  ] Stopped target Local File Systems (Pre).
[  OK  ] Stopped Create Static Device Nodes in /dev.
         Stopping Create Static Device Nodes in /dev...
[  OK  ] Stopped Remount Root and Kernel File Systems.
         Stopping Remount Root and Kernel File Systems...
         Stopping Monitoring of LVM2 mirrors... dmeventd or progress polling...
[  OK  ] Stopped Monitoring of LVM2 mirrors,...ng dmeventd or progress polling.
         Stopping LVM2 metadata daemon...
[  OK  ] Stopped LVM2 metadata daemon.
[  OK  ] Started Restore /run/initramfs.
[  OK  ] Reached target Shutdown.
dracut Warning: Killing all remaining processes
Halting.
[  377.640424] System halted.
```

- Installation is complete.
  - Remove the USB Flash media and reboot the physical device, or
  - Dismount the .iso and reboot the virtual machine
    - If required, take a snapshot to store the current status

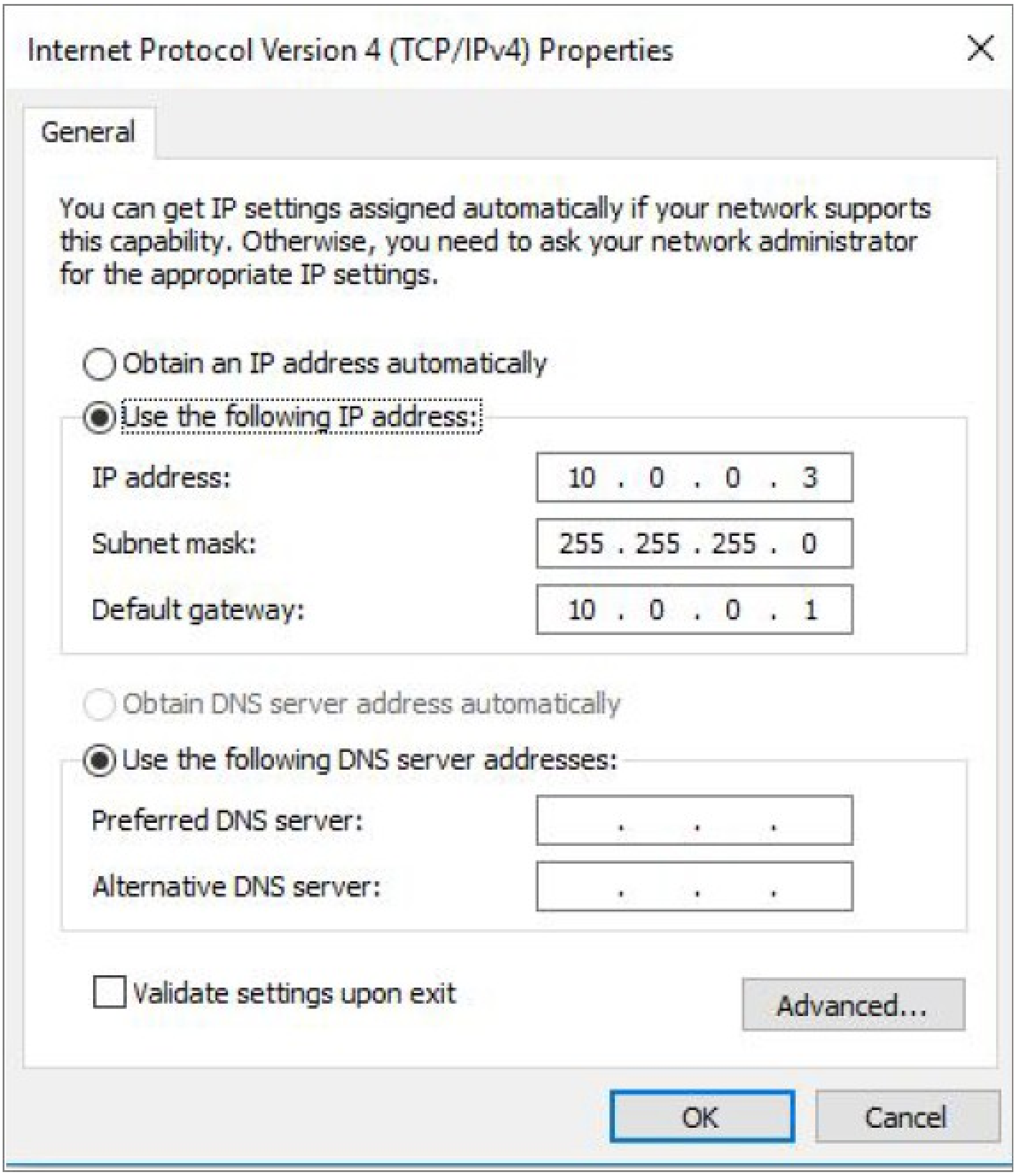
6 Sensor Configuration Steps

Click the following links for more details on configuring the sensor:

- **Login to the Web Portal**
- **User Settings**
- **Configure Network**
- **Configure Timezone**
- **Key Activation**
- **(Optional) Valkyrie Key Verdict**
- **(Optional) Forward Log**

6.1 Login to the Web Portal

- On your host machine, navigate to your network adapter settings to temporarily change to a static IP on the same network as the sensor
- Select 'Use the following IP address'
  - IP address: 10.0.0.3
  - Subnet mask: 255.255.255.0
- If your host machine has more than one network adapter, apply these settings to the primary adapter and temporarily disable other adapters



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 0 . 0 . 3

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 0 . 0 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

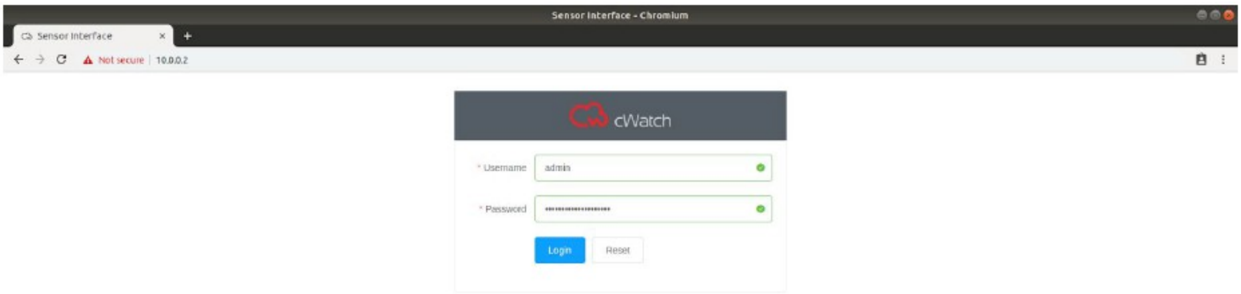
Alternative DNS server: . . .

□ Validate settings upon exit

- Open a browser on the host machine and type:

  “ http://10.0.0.2 ” into the address bar

- Enter the following default credentials to login to cWatch:
  - **Username**: admin
  - **Password**: cWatchSensorPass330!

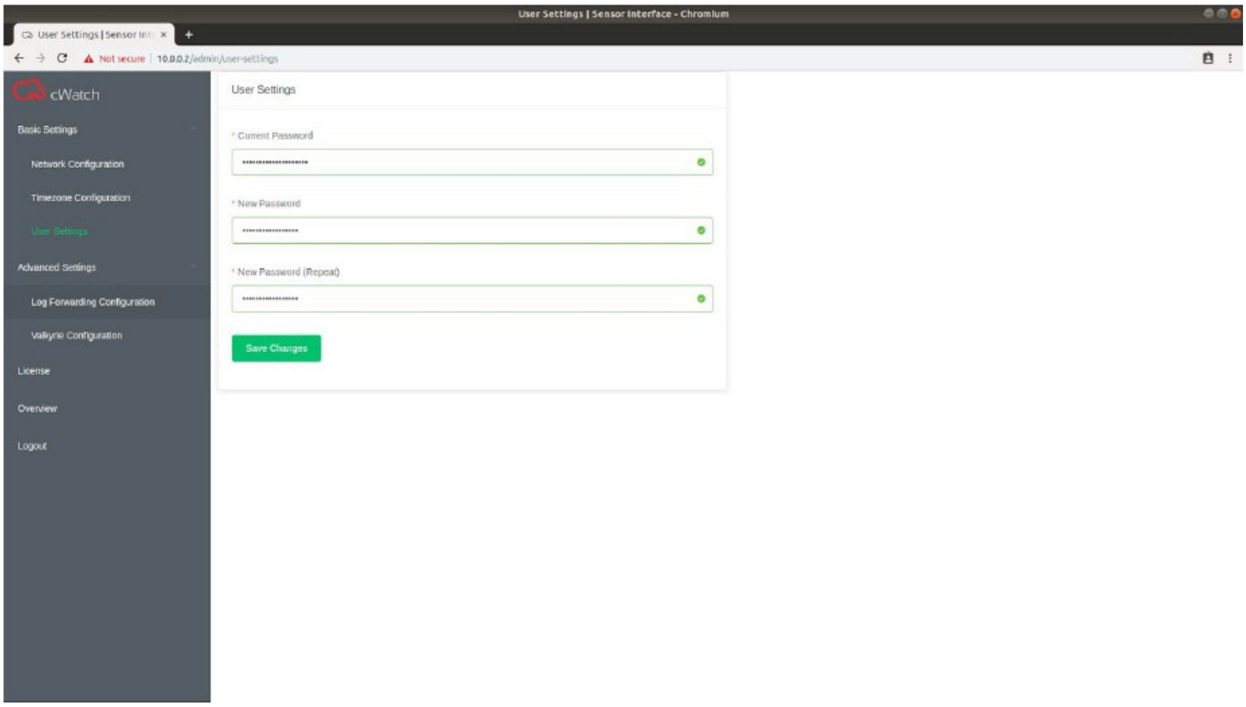


* Username: admin

* Password: ••••••••••••••••••••

6.2 User Settings

- Next, change the default password:
  - Click 'Basic Settings' in the left menu > 'User Settings'
  - Enter the default password (mentioned in **previous step**) and a new password



User Settings

* Current Password: ••••••••••••••••••••

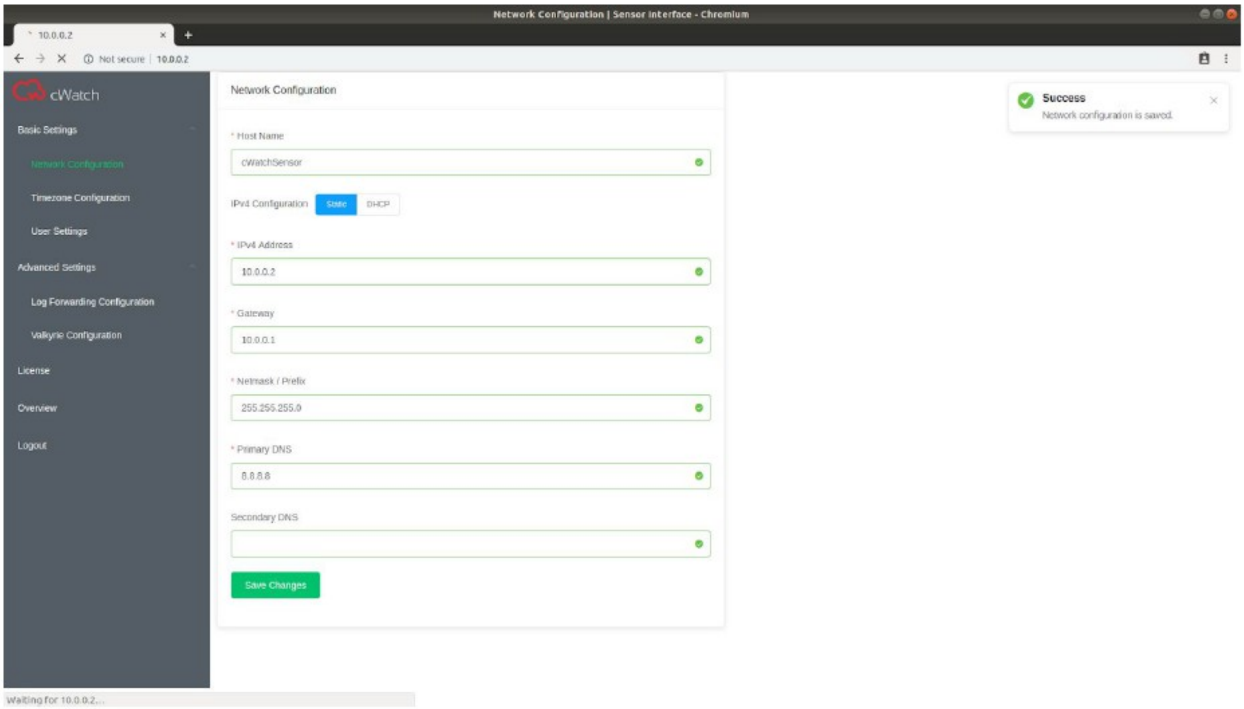
* New Password: ••••••••••••••••

* New Password (Repeat): ••••••••••••••••

- Click 'Save Changes'

6.3 Configure Network

- Select 'Basic Settings' in the left menu then 'Network Configuration'
- (Optional) Change the Host Name (Default = cWatchSensor)
  - If you plan to deploy multiple sensors, please make sure each sensor has a unique hostname
- Edit the following fields to connect the sensor to the internet:
  - 'IPv4 Configuration'
  - 'IPv4 Address'
  - 'Gateway'
  - 'Netmask' / 'Prefix'
  - 'Primary DNS/ 'Secondary DNS' servers
  - It is recommended to use a static IP. This will make it easier to reconnect to the sensor.
- After modifying the network fields, click 'Save Changes'



Network Configuration

* Host Name: cWatchSensor

IPv4 Configuration: Static

* IPv4 Address: 10.0.0.2

* Gateway: 10.0.0.1

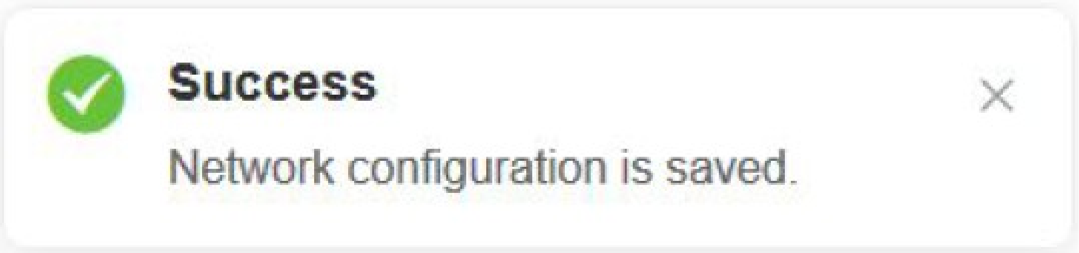
* Netmask / Prefix: 255.255.255.0

* Primary DNS: 8.8.8.8

Secondary DNS:

Success
Network configuration is saved.

The following success message appears in the top-right of the interface:

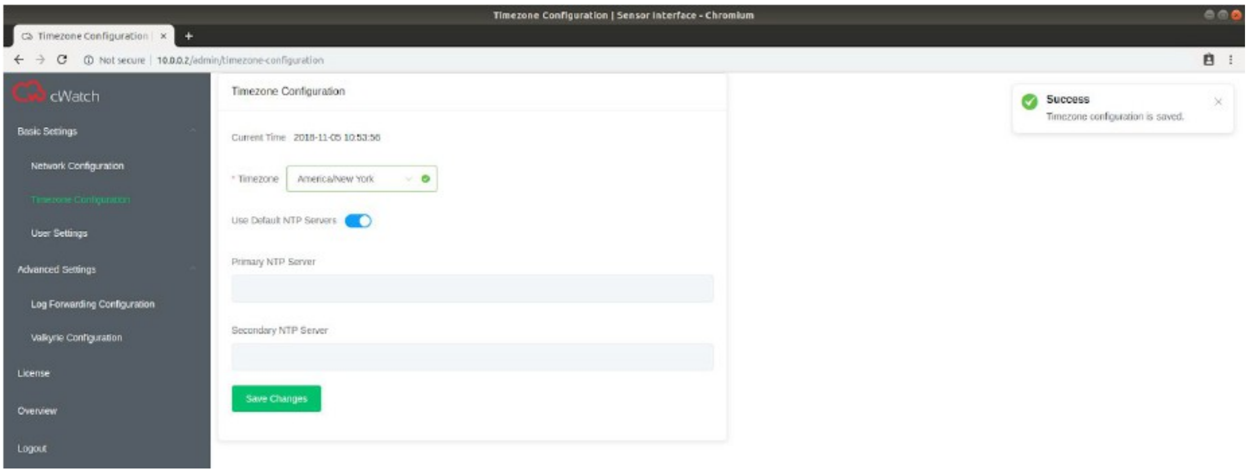


Success

Network configuration is saved.

6.4 Configure Timezone

- Select 'Basic Settings' > 'Timezone Configuration'
- Select your timezone in the 'Timezone' drop-down menu
- Enable the 'Use Default NTP Servers'
- Enter a NTP server in the fields below to change the default NTP Servers



Timezone Configuration

Current Time 2018-11-05 10:53:56

* Timezone America/New York

Use Default NTP Servers

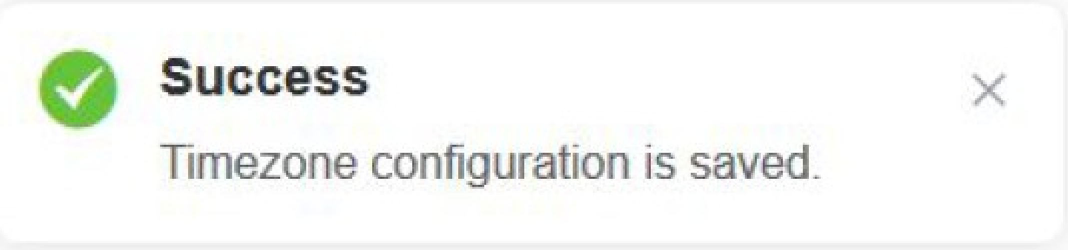
Primary NTP Server

Secondary NTP Server

Success

Timezone configuration is saved.

- The following success message appears in the top-right of the interface:

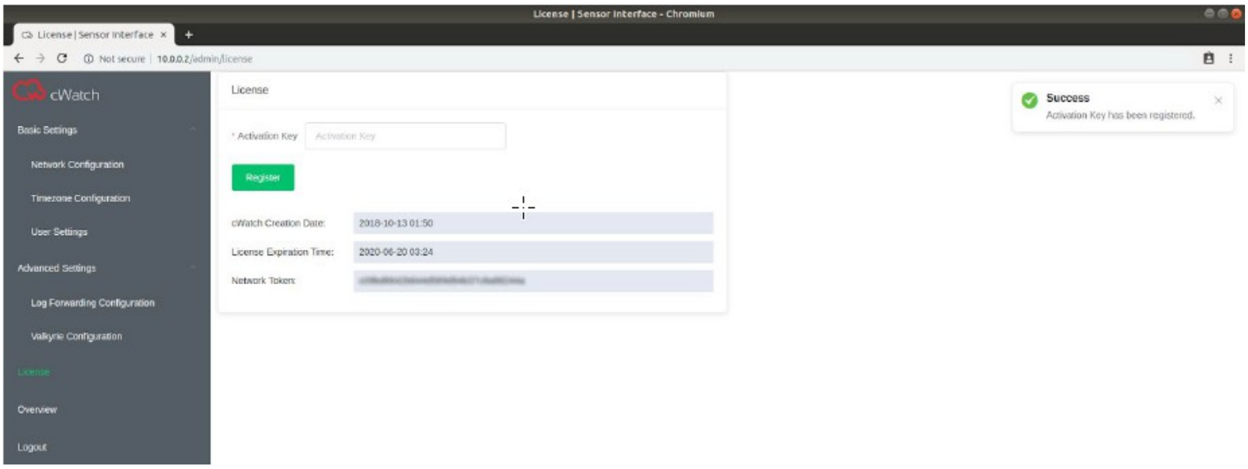


Success

Timezone configuration is saved.

6.5 Key Activation

- Select 'License' in the sensor web GUI to associate your sensor with your cWatch cloud account
- Get the required activation key - click 'Manage' > 'Asset Management' in the cWatch portal
  - Token = 32 alphanumeric characters
- Click 'Submit'
- The following fields will be populated. You will see a success message at top-right:



License

* Activation Key Activation Key

cWatch Creation Date: 2018-10-13 01:50

License Expiration Time: 2020-06-20 03:24

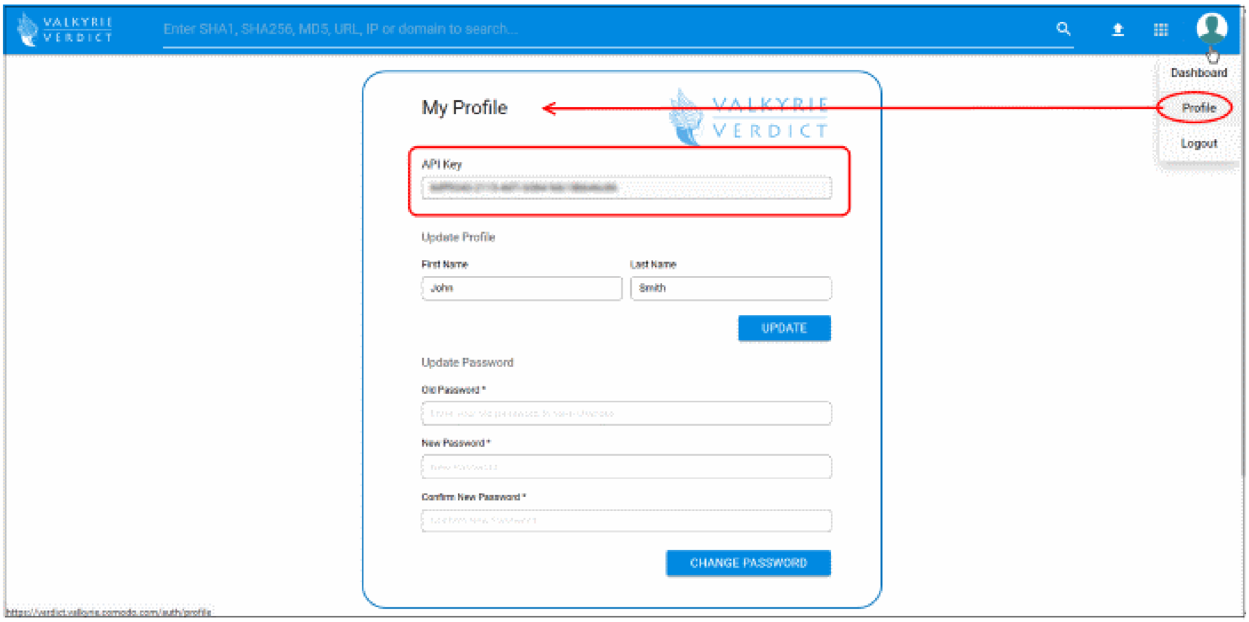
Network Token: [redacted]

Success

Activation Key has been registered.

6.6 (Optional) Valkyrie Key Verdict

- Visit https://verdict.valkyrie.comodo.com/
  - Create an account if you do not already have one
  - Make sure to verify your email or the API key will not be activated
  - Once you are logged in to your Valkyrie account, click the user icon at top-right, then 'Profile':



My Profile

API Key

Update Profile

First Name

John

Last Name

Smith

Update Password

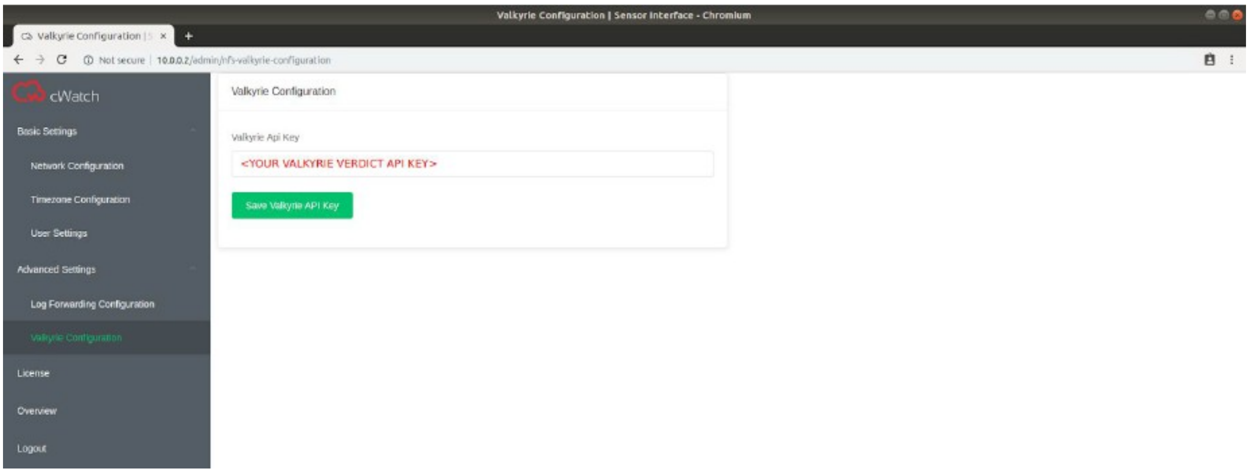
Old Password *

New Password *

Confirm New Password *

https://verdict.valkyrie.comodo.com/auth/profile

  - Note down the Valkyrie API key listed in the profile area
- Go back to the sensor web interface and:
  - Click 'Advanced Settings' > select 'Valkyrie Configuration'



10.0.0.2/admin/nfs-valkyrie-configuration

Valkyrie Configuration

Valkyrie Api Key

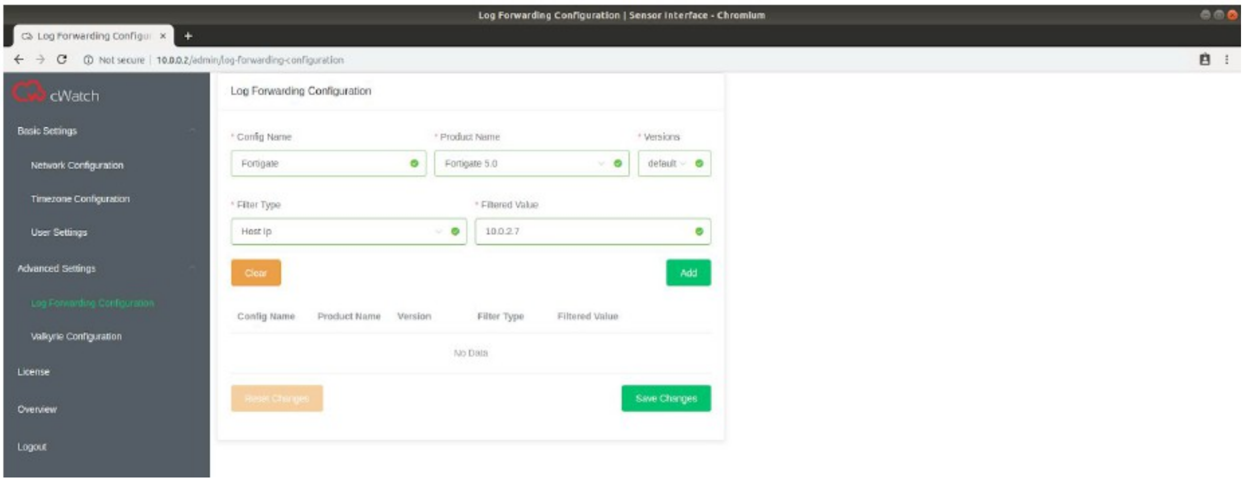
<YOUR VALKYRIE VERDICT API KEY>

  - Enter your Valkyrie API key then click 'Save Valkyrie API Key'

6.7 (Optional) Forward Log

NxSensor can forward logs of different network products to your cWatch portal account. You have to configure the sensor in order to do that:

- Open the sensor web interface
- Select 'Advanced Settings' > 'Log Forwarding Configuration' in the left menu



Log Forwarding Configuration

* Config Name: Fortigate

* Product Name: Fortigate 5.0

* Versions: default

* Filter Type: Host Ip

* Filtered Value: 10.0.2.7

Config Name	Product Name	Version	Filter Type	Filtered Value
No Data				

- Config Name – Label of the log forwarding configuration
- Product Name – Select the network product from the drop-down
- Version – Select the product version number
- Filter Type – Select from the options:
  - Host IP
  - Keyword
  - App Name
- Filtered Value – Enter the appropriate value, for example the IP number if host IP is selected.
- Click the 'Add' button

The log forwarding configuration is shown in the table below.

- Click 'Save Changes'

You can view saved configurations in the 'Log Forwarding Configuration' and 'Overview' tabs.

- The image above shows an example for Fortigate5.0 log forwarding.

Note: The 'Product Name' drop-down has a list of products that cWatch supports.

Frequently Asked Questions

What is cWatch Sensor?

cWatch Sensor is a passive network sensor image which is used to collect and analyze network traffic for the purpose of identifying suspicious events. Hence, cWatch Sensor is distributed as an ISO image, it can be easily installed on both physical server devices and any virtualization environment. The sensor has inbuilt PF_RING support as packet capture accelerator in order to increase packet capture performance and decrease packet loss.

The primary purpose of the cWatch Sensor is to collect raw network traffic via mirror port configuration, or using hub or tap devices. Our sensor combines signature and heuristics based IDS, which provides a strong mechanism for SOC teams to run network analysis and security monitoring. cWatch Sensor also provides a log forwarder service to collect supported third-party network device logs, normalize them and forward to our cWatch NDR servers using our common event model.

cWatch Sensor provides external threat intelligence integration capability. Additionally, it has Valkyrie integration for advanced extracted file analysis.

cWatch Sensor also provides passive OS and service fingerprinting. All the collected information about the network is sent to cWatch servers to be presented to users over cWatch portal. cWatch Sensor tuning and maintenance operations such as managing new signatures, tuning the signature sets to keep event volume at acceptable levels, minimizing false-positives, and maintaining up/down health status of sensors and managing data feeds are performed regularly by Comodo SOC team.

Which Services are Running on cWatch Sensor?

In addition to the default CentOS 7 services, there's also PF_RING support for BRO IDS and Suricata IDS. There are also custom Comodo services for integration, management and updates.

The following table shows open ports and related programs and whether or not the sensor firewall blocks the connection:

Port	Program	Firewall Blocking Status
22	sshd	Allowed
68	dhclient	Allowed
80	httpd	Allowed
514	rsyslogd	Allowed

Which configurations must be done at first install?

It is essential to set IP Address, Gateway and Network Token as the first step of installing cWatch sensor.

Which Network Interfaces are Active on a Hardware Sensor?

“eth0” interface is active and being used for management and communication to cWatch Servers.

“eth1” interface is responsible for listening network traffic coming from mirror interface. Therefore it works on promiscuous mode.

Which Rule-set do IDS Services Use?

IDS services are using mainly Emerging Threats Pro Ruleset which are customized and improved by Comodo cWatch team.

What is the Log Forward Feature?

In addition to collecting information about network security, cWatch sensor also collects and forwards logs from other products in the network.

Which External IPs or Domains does cWatch Sensor Need to Access?

For remote management:

Domain: sensor.mssp.comodo.com

Address: 35.169.33.2

For rule update:

Domain: rules.emergingthreatspro.com

Address: 204.12.217.18, 96.43.137.98

For Amazon Kinesis:

Domain: kinesis.us-east-1.amazonaws.com

Address: 52.119.196.103

Domain: monitoring.us-east-1.amazonaws.com

Address: 52.94.238.171

DNS address:

Default DNS is set as 8.8.8.8. If the customer wants to use this dns, it should to be allowed. If the customer wants to use their own DNS, that should be allowed only after we are sure that the hosts above are resolved correctly by that DNS.

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email: **EnterpriseSolutions@Comodo.com**