LiveSensor Installation Guide

by LiveAction Community

1. LiveSensor Installation Guide

LiveSensor Deployment

Deployment of LiveSensor is a simple black box tool that takes very little resources to run. The LiveSensor allows an administrator to deploy a VM and monitor mirrored/span traffic and have the LiveAction Sensor send flows to LiveNX for analysis.

There are several prerequisites required before deploying LiveSensor. These prerequisites require the administrator to know and understand how to span as well as connect the physical server to a mirrored port.

Here are the prerequisite steps

- 1 Physical port from the server has to be connected to an unused port on a router or switch. This is preferably at the egress/ingress of each site.
- Span has to be configured to the physically connected port of from the server where the VM resides
- The vmnic from vSphere that is connected has to also be configured in promiscuous mode. This will allow for the traffic to be read through the NIC specified.
    - There will be a short step-by-step to describe the VM portion of the configuration through vSphere.

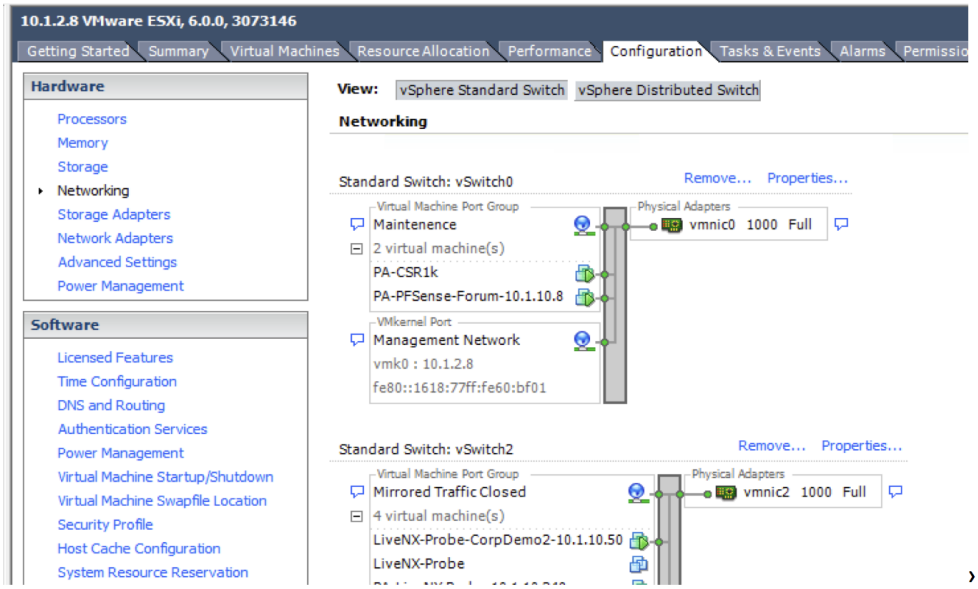
Hardware Requirements for the LiveSensor OVA

- 4 vCPU
- 8GB of RAM
- 50GB Disk

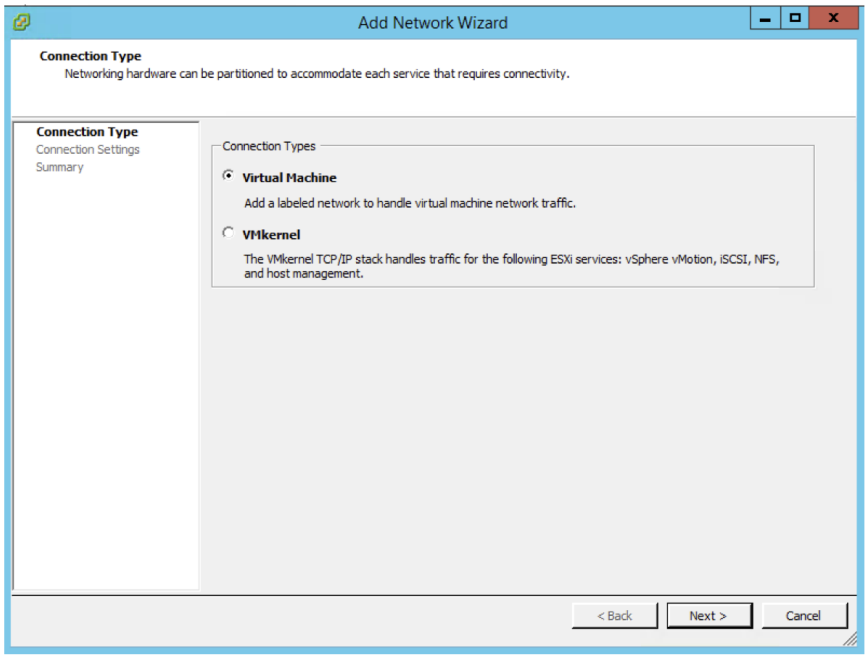
Create Virtual Machine Port Group and Configure Promiscuous Mode

This section assumes that the physical port of the vmnic has already been connected to a span port on a physical router or switch, and a vSwitch has already been configured. If this has not been performed, please consult vmware in order to configure a vSwitch before moving forward.

1. Log into vSphere
2. Select the target ESXi server
3. Click > Configuration
    1. Located on the right panel
4. Click > Networking
5. Find the vSwitch that is configured for the span port
6. Click > Properties…
7. Add a Virtual Machine Port Group to the vSwitch

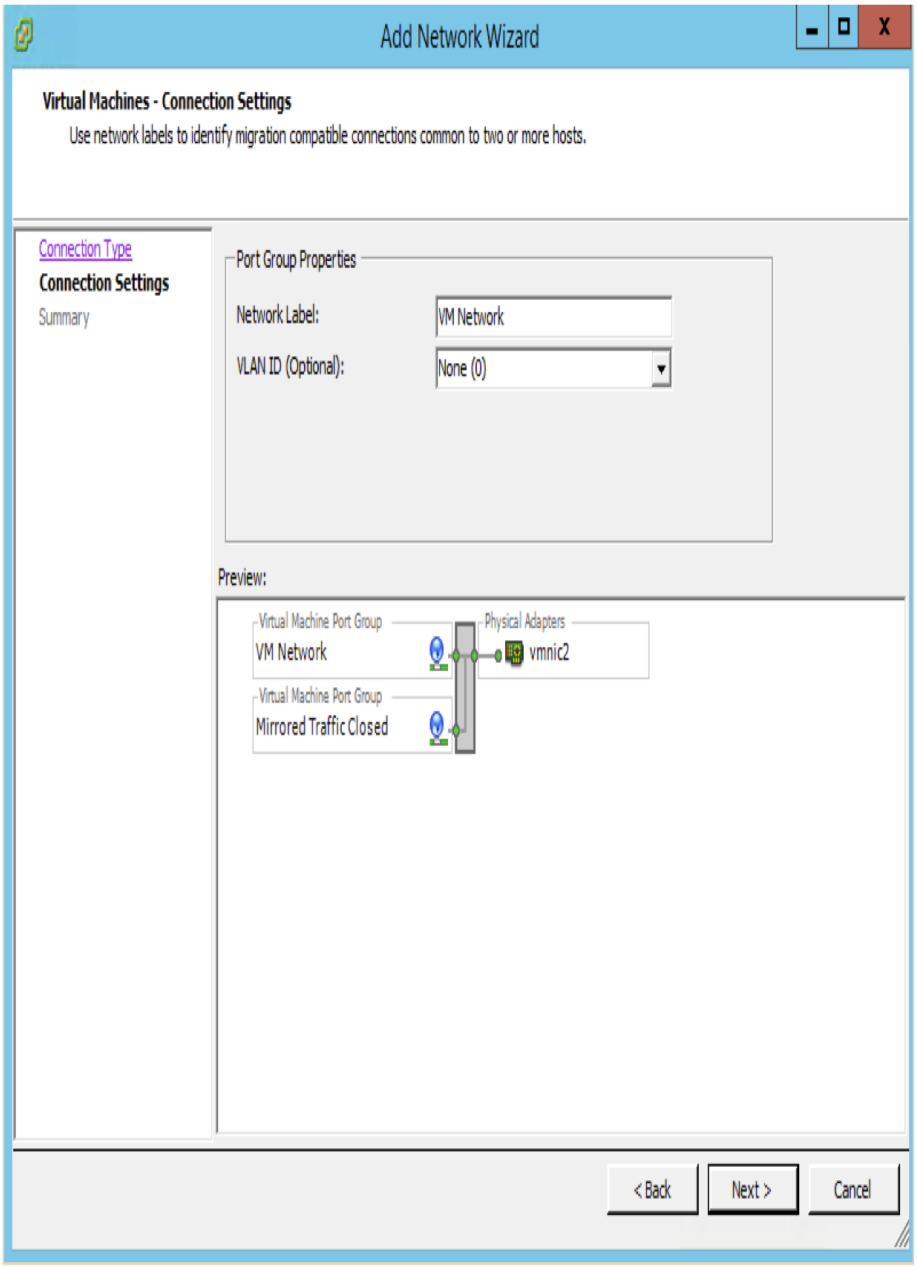


8. Select Virtual Machine > Next

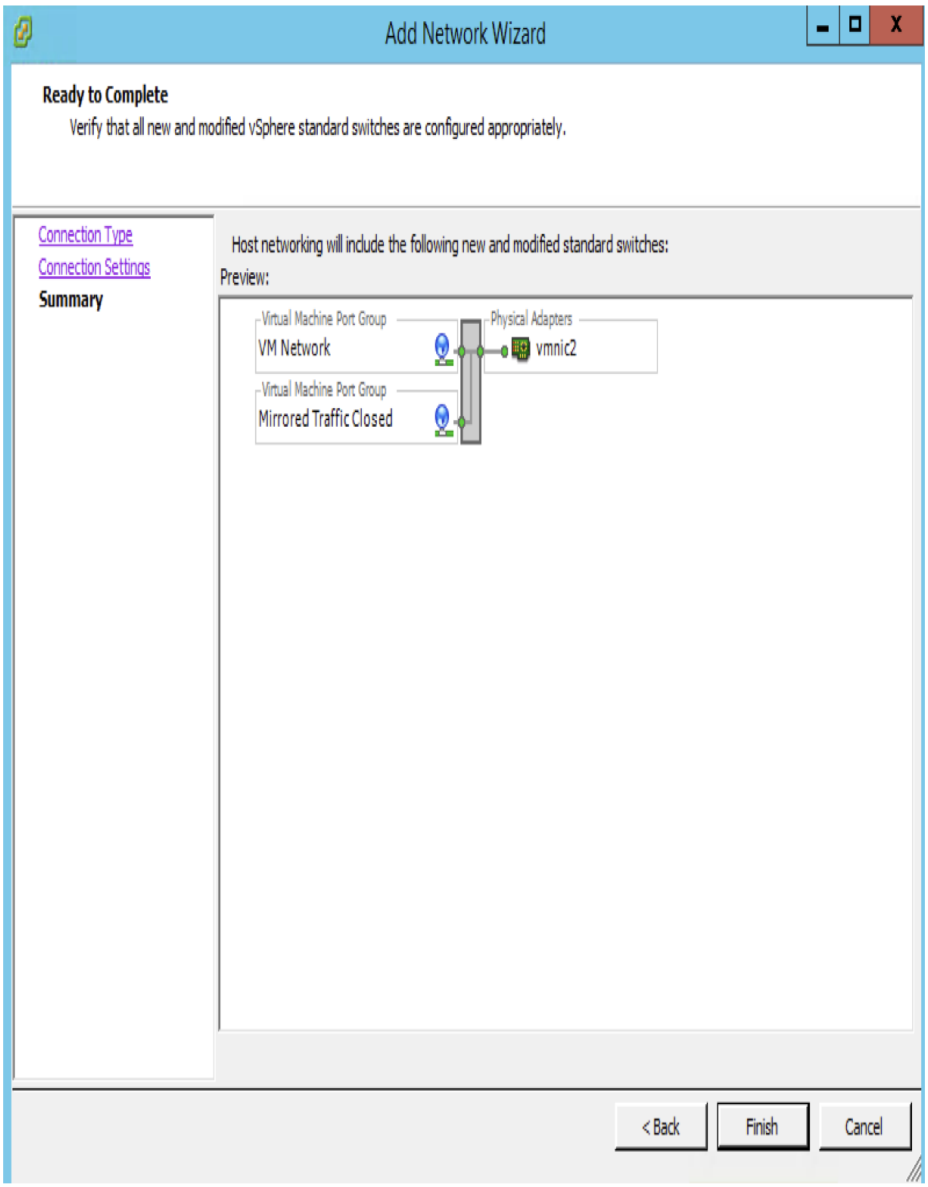


(http://communitylive.wpengine.com/wp-content/uploads/2016/09/Select-Virtual-Machine.png)

9. Provide it a Name > Next

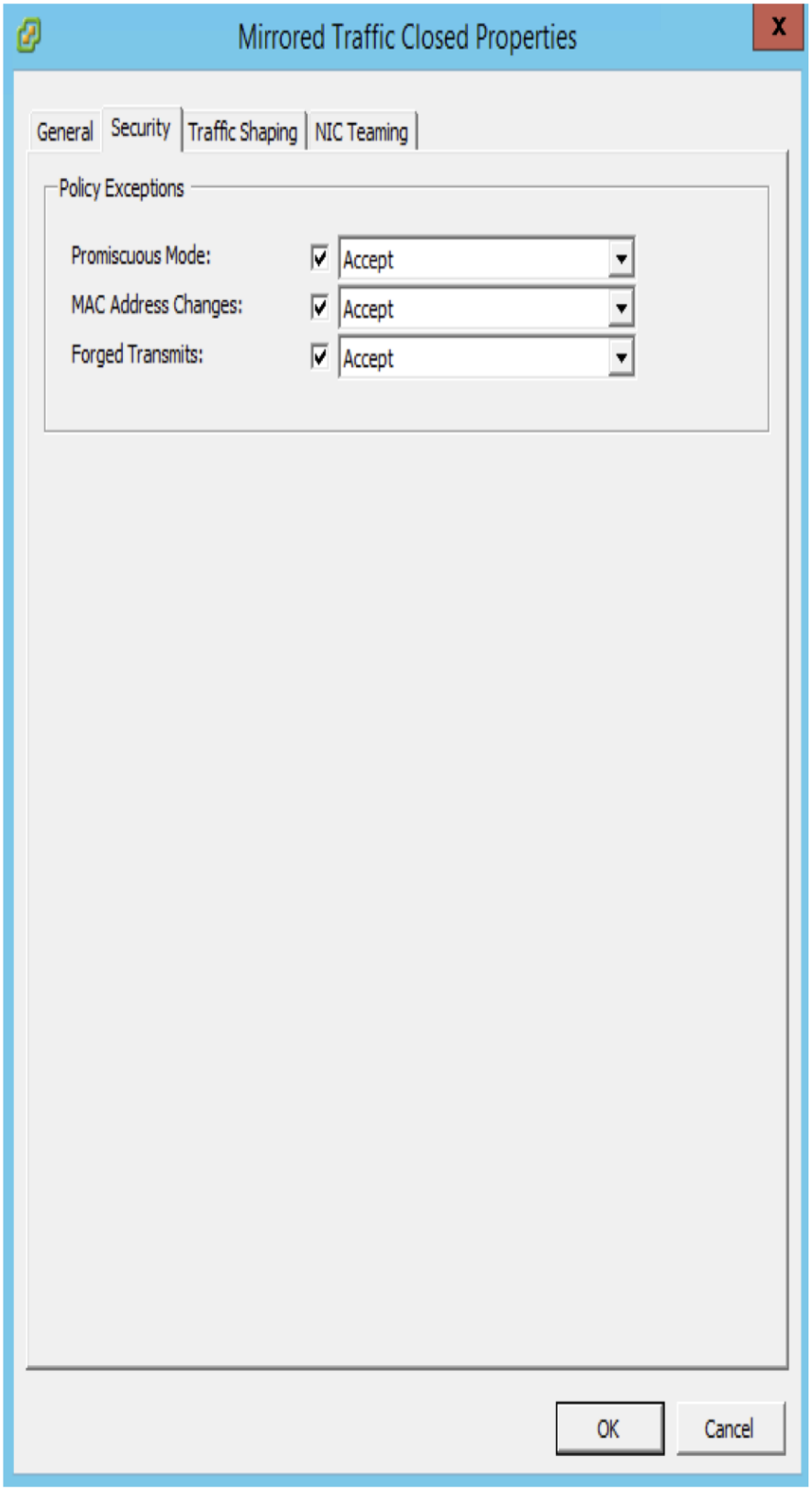


(http://communitylive.wpengine.com/wp-content/uploads/2016/09/Add-Network-Wizard.png)



10. Click > Finish
    (http://communitylive.wpengine.com/wp-content/uploads/2016/09/Click-Finish.png)

11. Click > the new Virtual Machine Port Group > Edit
12. Click > Security



(http://communitylive.wpengine.com/wp-content/uploads/2016/09/Mirrored-Traffic.png)

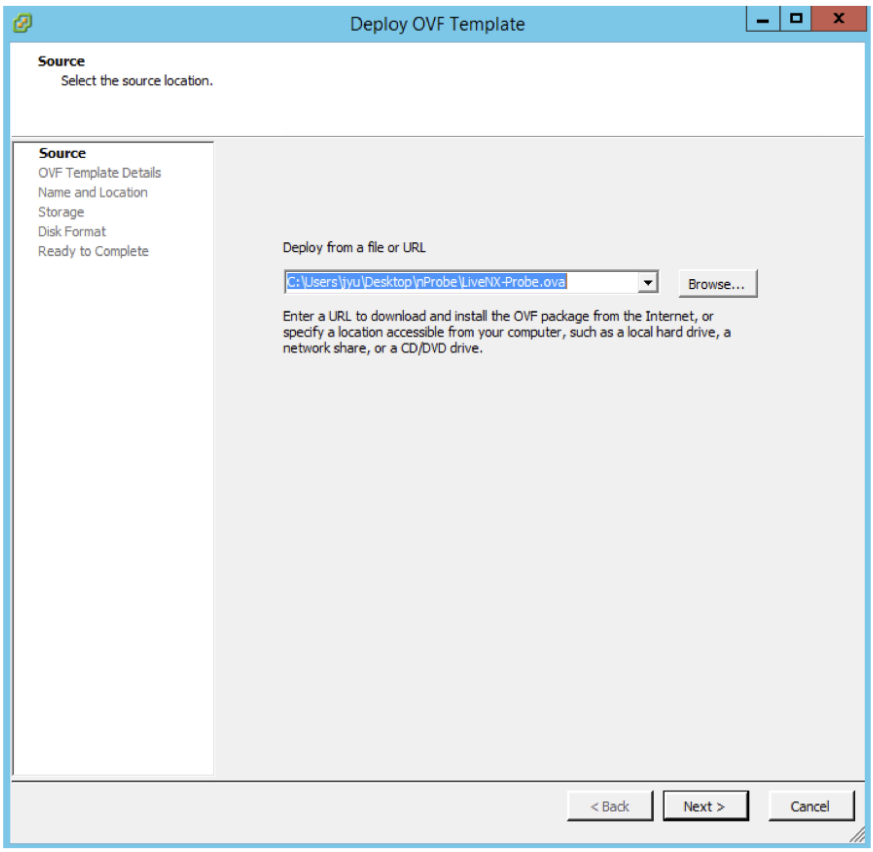
13. Check Promiscuous Mode > Accept
14. Check MAC Address Changes > Accept

15. Check Forged Transmits > Accept
16. Click > OK
17. Under vSwitch Properties > Close

Deployment of Live Sensor

(Screenshots to be done later)

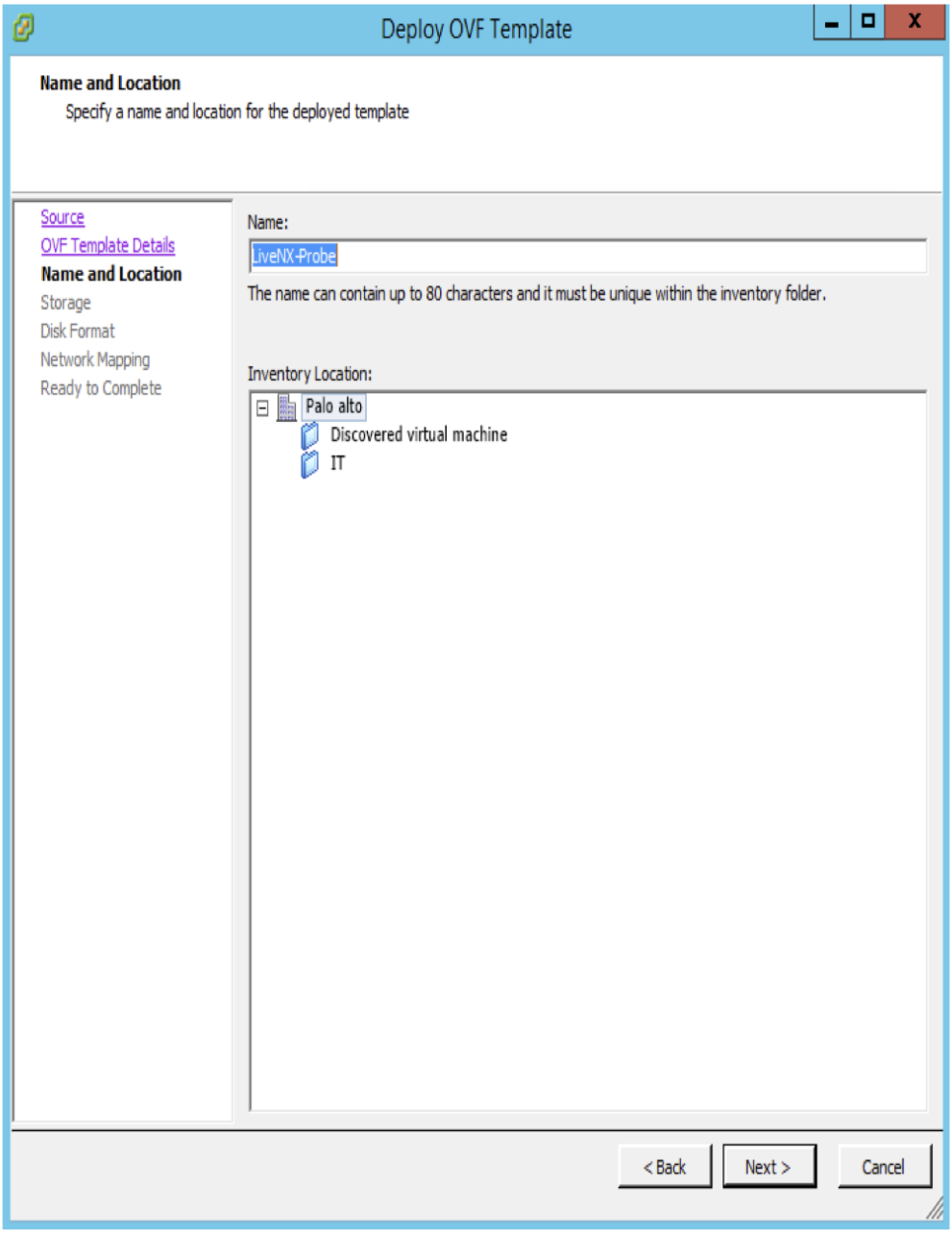
1. Download the LiveSensor OVA at: xxxxxxxxxxxxxxxxxxx
2. Open vSphere and choose a local server
3. Click on File > Deploy OVF Template



(http://communitylive.wpengine.com/wp-content/uploads/2016/09/deploy-OVF.png)

4. Search for the LiveSensor and follow the installation wizard

a. The Sensor deployment is almost identical to the node and AIO deployment on ESX



(http://communitylive.wpengine.com/wp-content/uploads/2016/09/Template.png)

5. After the OVA has finished deploying the vm on the ESXi server power it on

6. Deployment of Live Sensor has been completed

Configuration of Live Sensor


Live Sensor
Network Information:
HostName: localhost
IP Address:
Subnet Mask:
Gateway:
DNS 1:
DNS 2:
NTP Server:
Live Sensor Configuration:
Sensor License ID:
Sensor System ID: 68BC4F6182072B23
Sensor Version: 7.4.160805
NX's Server IP:
NX's Server Port:
Settings Menu:
[1] Static IP
[2] Install Sensor License
[3] Configure Sensor
[4] Restart Sensor
[5] Download Logs
[6] Reboot
Please Enter Your Choice:

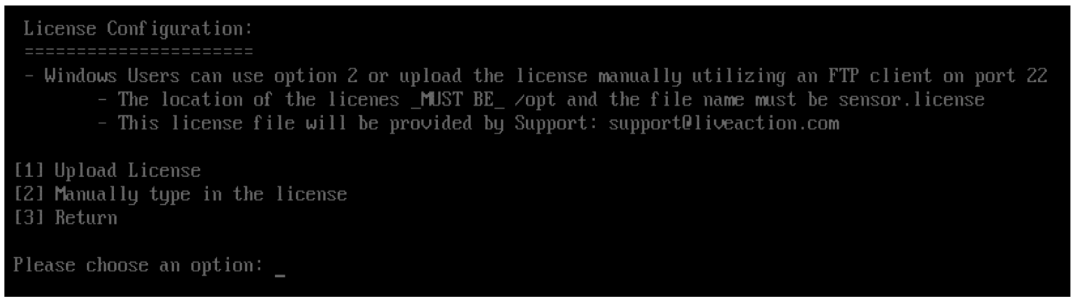
(http://communitylive.wpengine.com/wp-content/uploads/2016/09/Configuration-of-Live-Sensor.png)

1. Wait until the Live Sensor has finished booting and there will be a menu screen that shows you 6 options
   a. Static IP
   b. Install Sensor License
   c. Configure Sensor
   d. Restart Sensor
   e. Download Logs
   f. Reboot
2. For Static IP > 1

NOTE: The NIC configuration will be for eth0, eth1 will be your span port and will automatically be in promiscuous mode

a. Configure the Hostname
b. Configure the IP Address
c. Configure the NetMask
d. Configure the Gateway
e. Configure the 1st DNS
f. Configure the 2nd DNS
g. Configure NTP Server
h. Verify the settings are correct
i. There will be a check against a previous backup (Hostname and Network)
1. Type “y” or “Y” if you want to backup previous configuration.
2. Type “n” or “N” if you want to not backup the previous configuration.

j. An automatic reboot will be done to have the new configuration take effect

3. Install Sensor License > 2
4. 

(http://communitylive.wpengine.com/wp-content/uploads/2016/09/Install-Sensor-License.png)
    1. Upload License
        1. Uploading the license will require an ssh connection directly to the machine that contains the LiveSensor License
    2. Manually Type in the license
        1. This will require the license to be typed in manually, since it’s an alphanumeric hash, this maybe possible for offline activation
    3. Return
5. Configure Sensor > 3

(http://communitylive.wpengine.com/wp-content/uploads/2016/09/Configure-Sensor.png)

a. Configure the Target Server to receive flow
b. Configure the Target Server's Port to receive flow**i. NOTE: The target server will be LiveNX Server or LiveNX Node or LiveNX AIO**
c. The Sensor will restart the configured services and push you back to the splash screen

6. Reboot > 6
   a. This reboots LiveAction LiveSensor

(http://communitylive.wpengine.com/wp-content/uploads/2016/09/deploy-OVF.png)