Step 1 Installing Ubuntu And Necessary Files

You can do this by going to -> <https://ubuntu.com/download/desktop> and install the ova

You need to setup docker compose which can be found here ->

https://docs.docker.com/engine/install/ubuntu/

And also necessary tools including python3

Step 2 Installing and configuring .yml file containing Thehive, Cortex, MISP

First Download this file <https://github.com/ls111-cybersec/thehive-cortex-misp-docker-compose-lab11update/blob/main/docker-compose.yml>

And you need to open the docker-compose.yml and find this environment:

- MYSQL\_HOST=misp\_mysql

- MYSQL\_DATABASE=mispdb

- MYSQL\_USER=mispuser

- MYSQL\_PASSWORD=misppass

- MISP\_ADMIN\_EMAIL=mispadmin@lab.local

- MISP\_ADMIN\_PASSPHRASE=mispadminpass

- MISP\_BASEURL=localhost

- TIMEZONE=Europe/London

- "INIT=true"

- "CRON\_USER\_ID=1"

- "REDIS\_FQDN=redis"

- "HOSTNAME=https://10.0.2.10" ->> You need to change this to your current IP so the misp javascript/Function will load

Now you done it run For newer docker version docker compose up for old docker-compose up

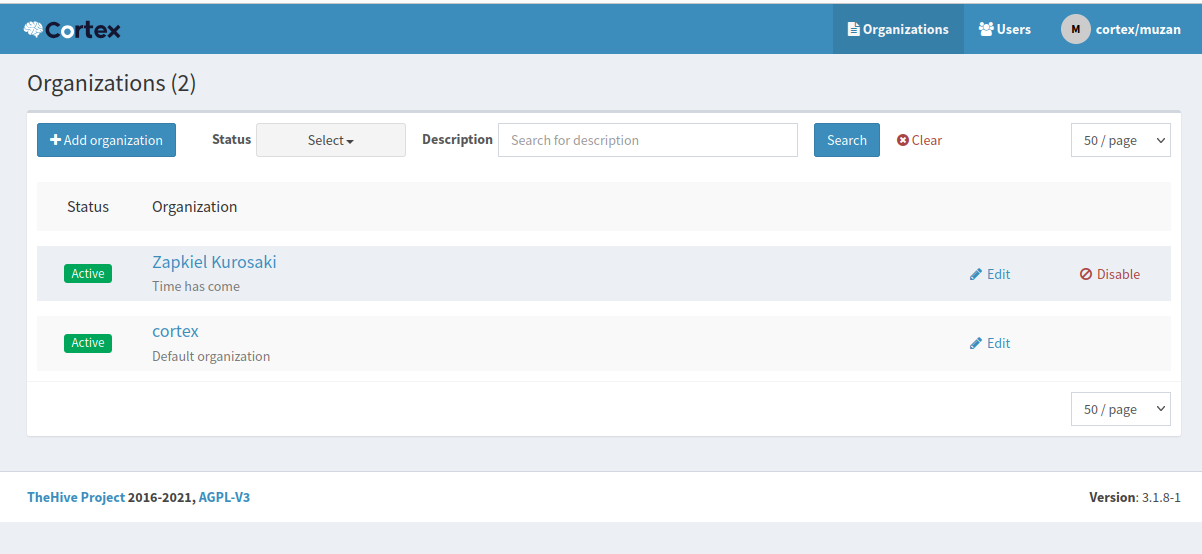
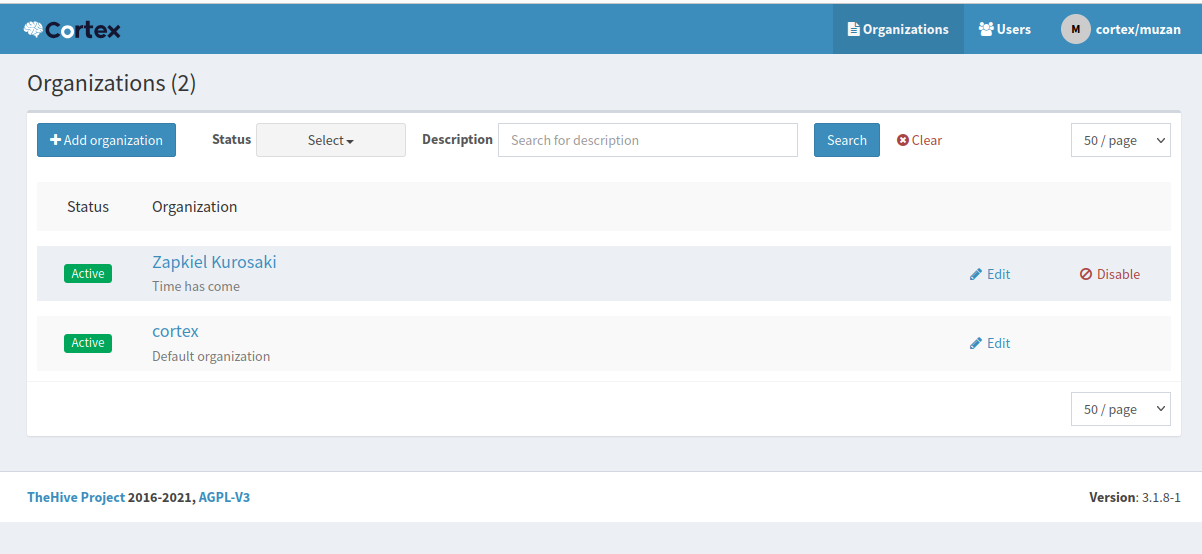
To run it with ease after installing run docker compose up -d

Step 3 Integration Cortex

You first need to create your organization after thatYou need to Add user

As you can see after you make user you need to create API key

And after that your all see good to go to next level



Step 3 part2 Integration MISP

You first need to add organization which you can see here

You then need to add what name you want example uzer Piccolo in organization identifier

And generate uuid

After that you can go again to Administration on top select add user

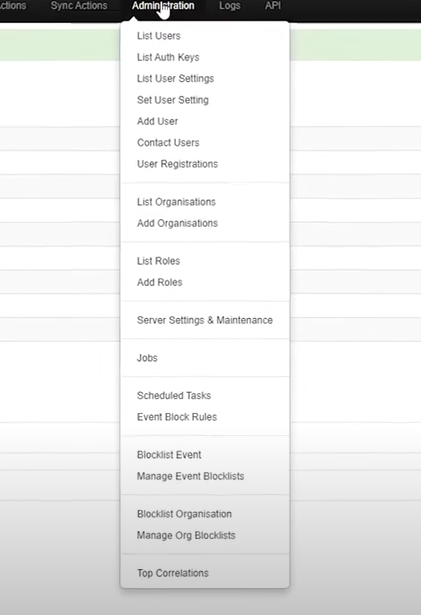
You need to Add what email you want example [labuser@up.local](mailto:labuser@up.local) And choose a password

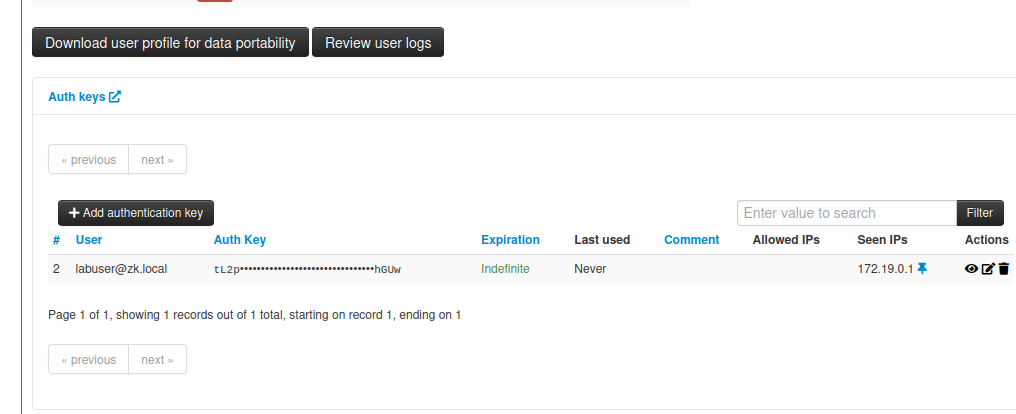
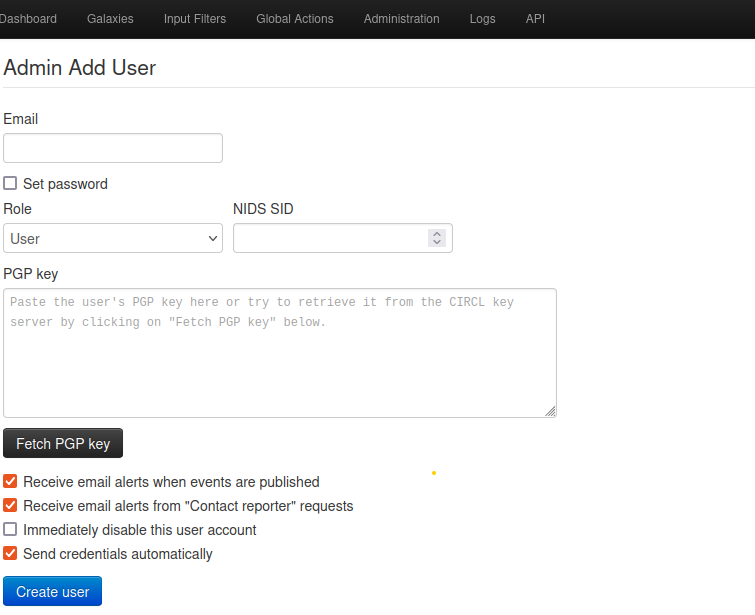
And select role org admin and then create user

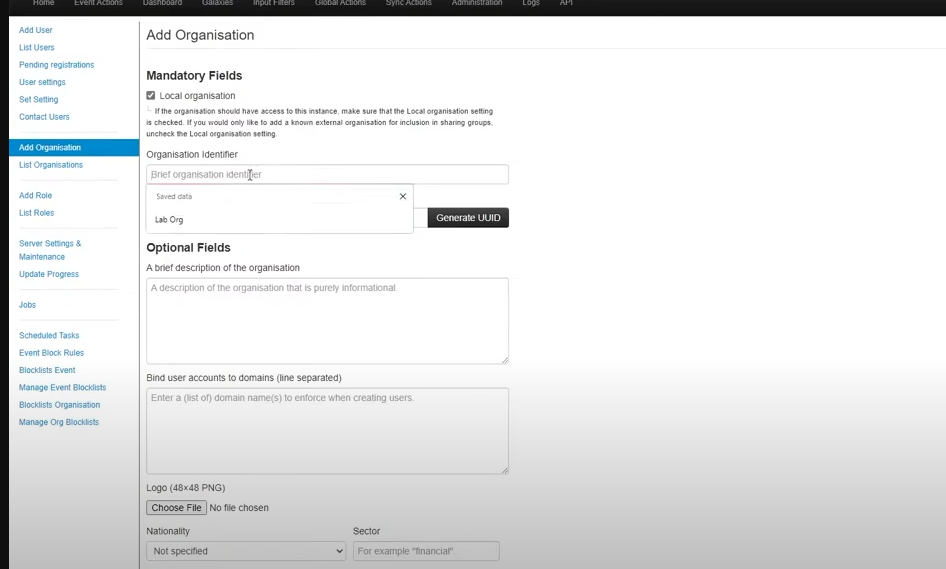
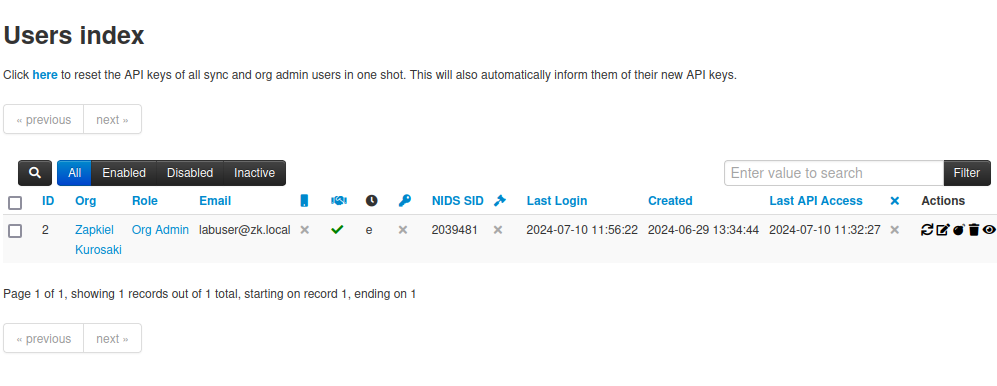
Now go again to administration drop down on top and select

List user there you can see a eye icon click it and scroll down

You can see auth keys **Image below**





Step 3 part3 Integration TheHive

Finally after long configuration we’re almost done

You then need to login to your thehive what you need to do is make an organization

-Task Sharing Rule = Autoshare --> you can choose which you want

-Observable sharing rule = autoshare --> you can choose which you want

After that you can fill the user you need to add user

**Cortex**

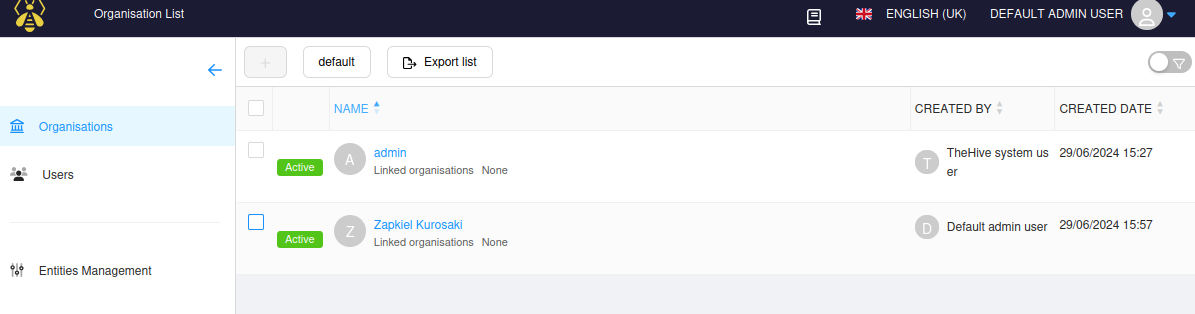
You then need to go to platform Management and find Cortex you can see there {Server}

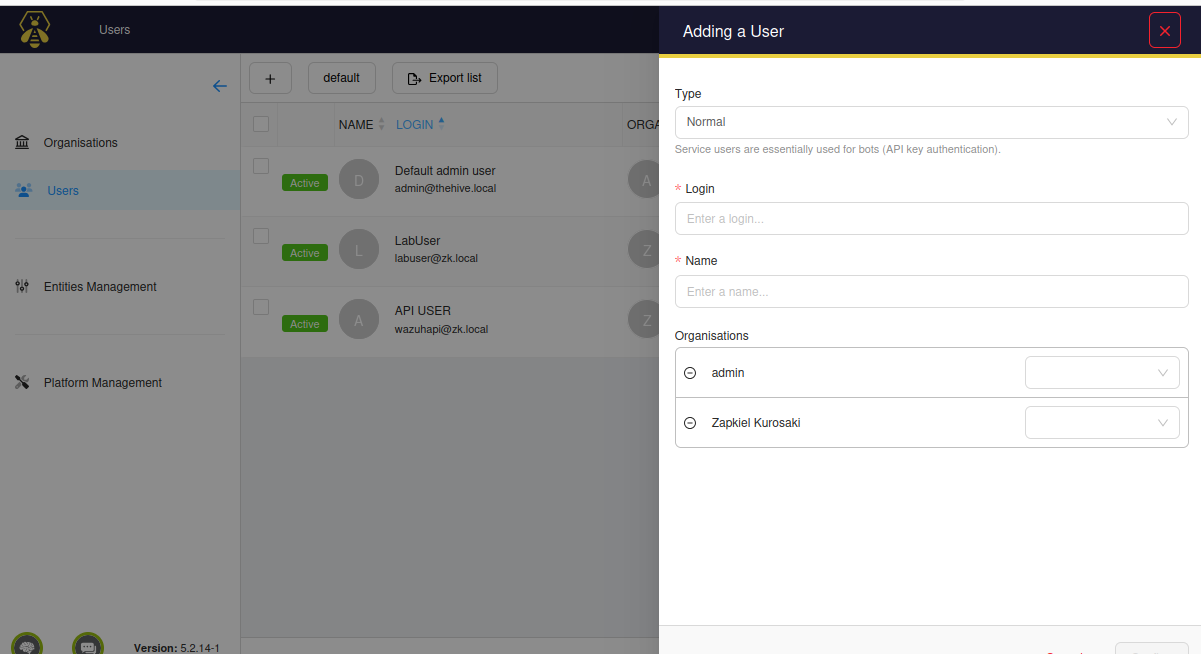
Click Cortext0 And then you need to fill the server url which url you use to access the cortex

And the Api you made in part 1 of integration cortex

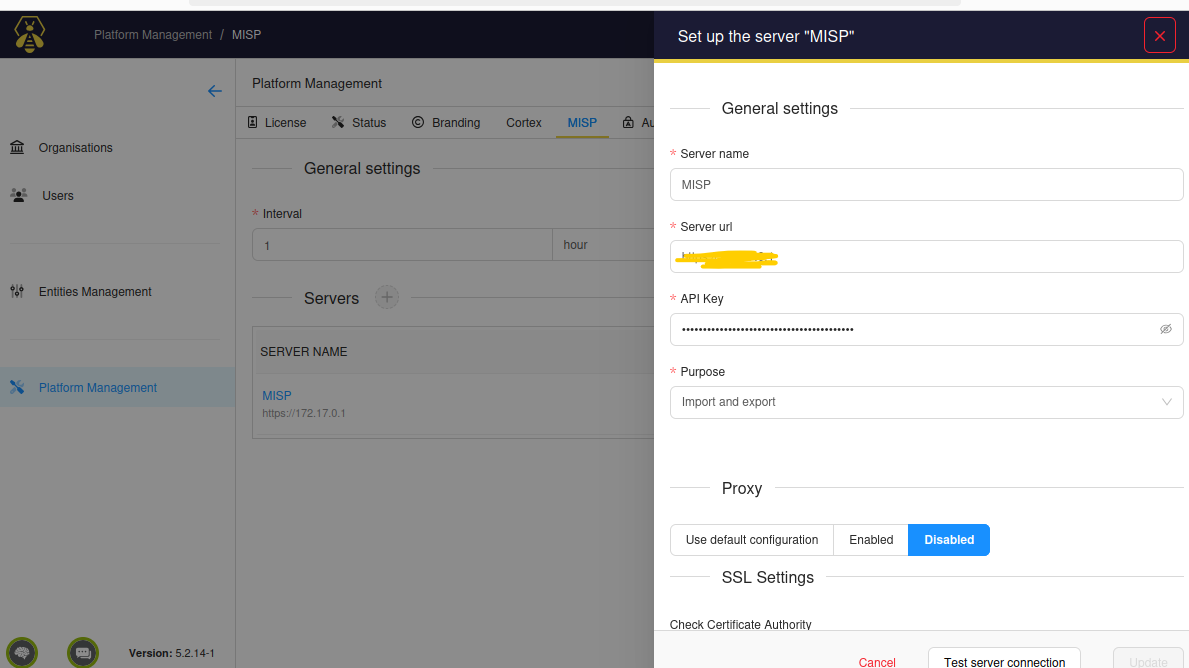
**MISP**

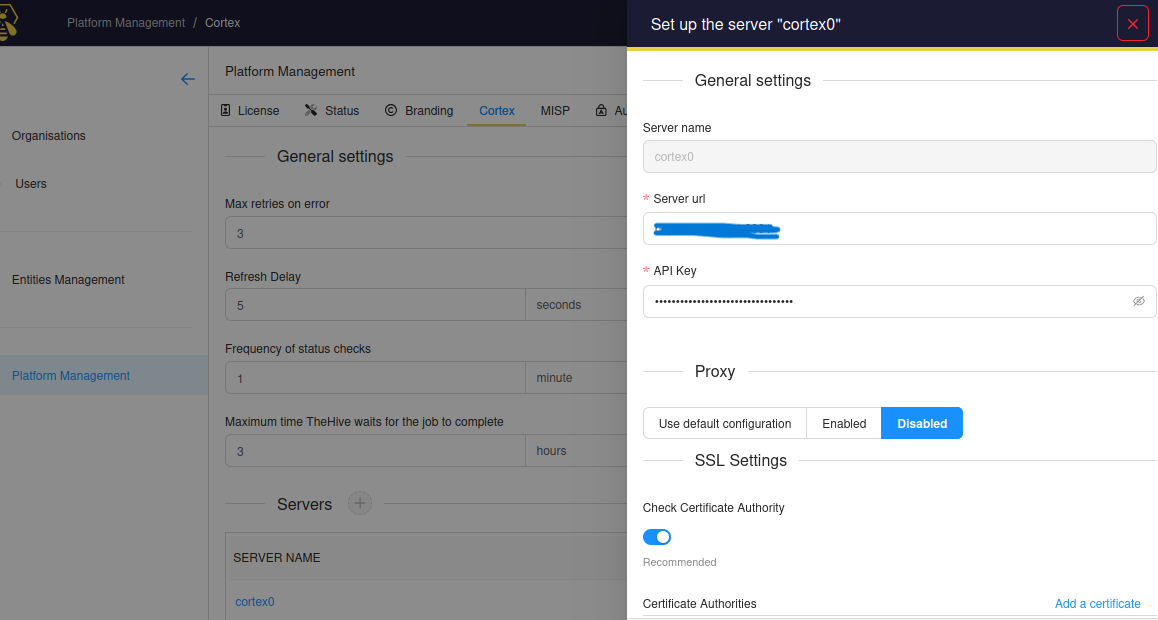
Now you are done configuring the cortex next is misp its also located in platform management next to cortex click add icon write your server name and the url you use to access MISP don’t put any port on the end example <http://127.0.0.1> what I mean is in cortex you have 127.0.0.1:9001





Cortex





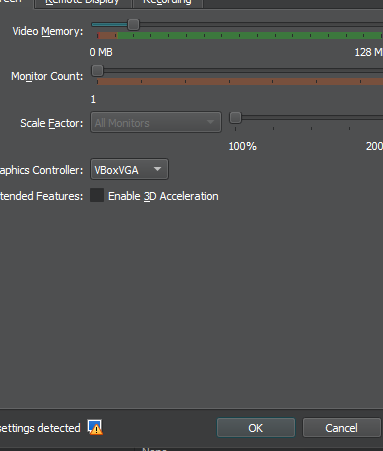
Part 4 Wazuh Installation&Integration

You can install wazuh to its official website ova In vmbox you will face an error which your screen will freeze to solve that change this graphics controller to VMSVGA

After Installing wazuh you can open it there you will be promted to enter password the user is wazuh-user and password is wazuh its also on top of it after that you need to install necessary tools

sudo yum update

sudo yum install python3

sudo /var/ossec/framework/python/bin/pip3 install thehive4py

Part 5 Integration to thehive

Visit this link for full documentation

https://wazuh.com/blog/using-wazuh-and-thehive-for-threat-protection-and-incident-response/

To be continued. . .