**Minemeld Installation**

Minemeld Can be easily and directly installed with their Ansible playbook. more details in their [Minemeld Github] (https://github.com/PaloAltoNetworks/minemeld-ansible)

CentOS would be used for this demonstration and it is good to have root access for ease of installation.

$ Git clone https://github.com/PaloAltoNetworks/minemeld-ansible.git

$ sudo yum install -y wget git gcc python-devel libffi-devel openssl-devel zlib-dev sqlite-devel bzip2-devel

$ wget https://bootstrap.pypa.io/get-pip.py

$ sudo -H python get-pip.py

$ sudo -H pip install ansible

$ git clone https://github.com/PaloAltoNetworks/minemeld-ansible.git

$ cd minemeld-ansible

$ ansible-playbook -K -i 127.0.0.1, local.yml

$ usermod -a -G minemeld <your user> # add your user to minemeld group, useful for development

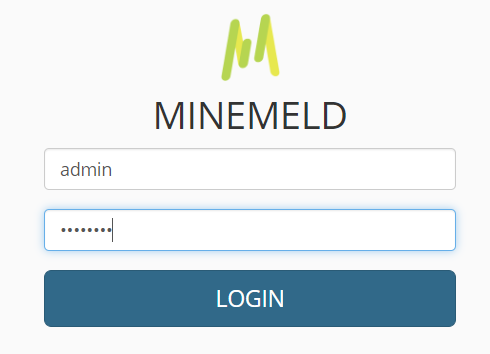
Upon complete Installation, Check if all services running.

```

$ sudo -u minemeld /opt/minemeld/engine/current/bin/supervisorctl -c /opt/minemeld/supervisor/config/supervisord.conf status

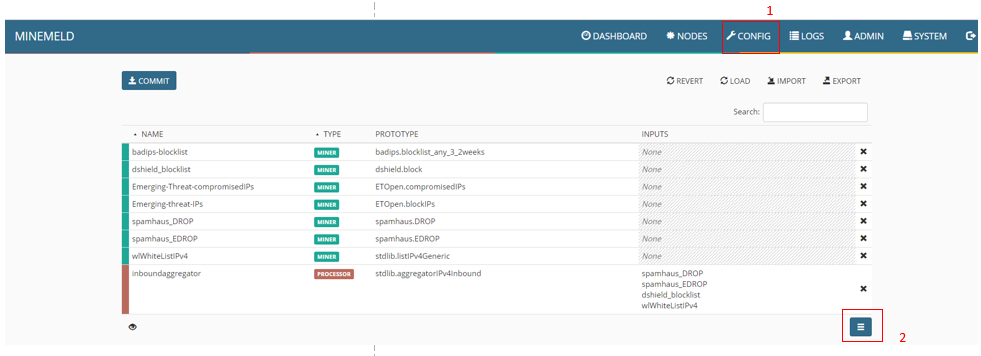
```

Minemeld Web UI is installed along with the core engine using above Ansible playbook. Access the web UI (http://[serverIP] ) with default credentials of “username: admin and password: minemeld”. Different users and authroisation can be configured within minemeld GUI dpending on your compliance needs.



**Minemeld - Threat Feed Configuration**

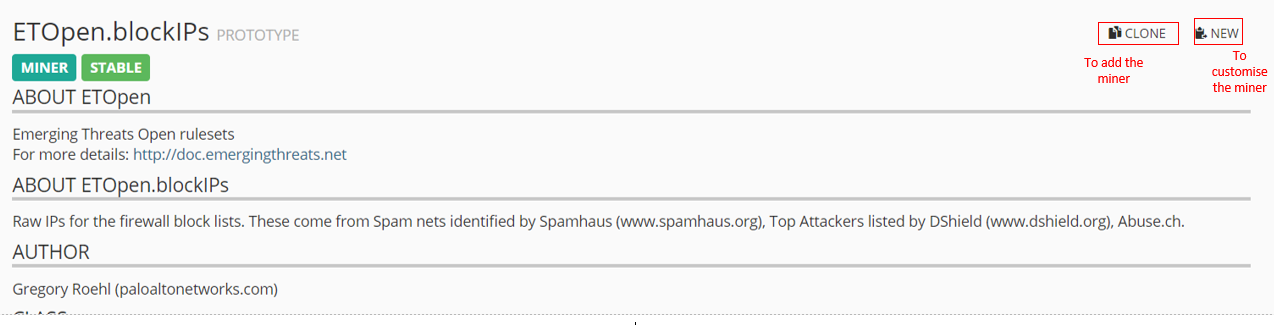
* Navigate to Config tab and view the list of prototypes that can be used.



* Select the protype you wish to add . let us start with Input protype. I will be adding Ipv4 indicators as miners that are not avialble by default

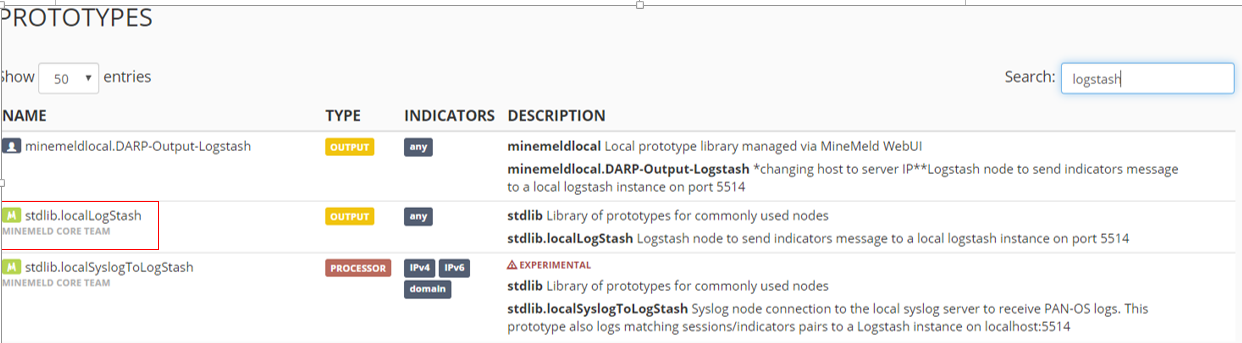
\*\* if you wish to add the Ipv4 miner – select clone and click ok

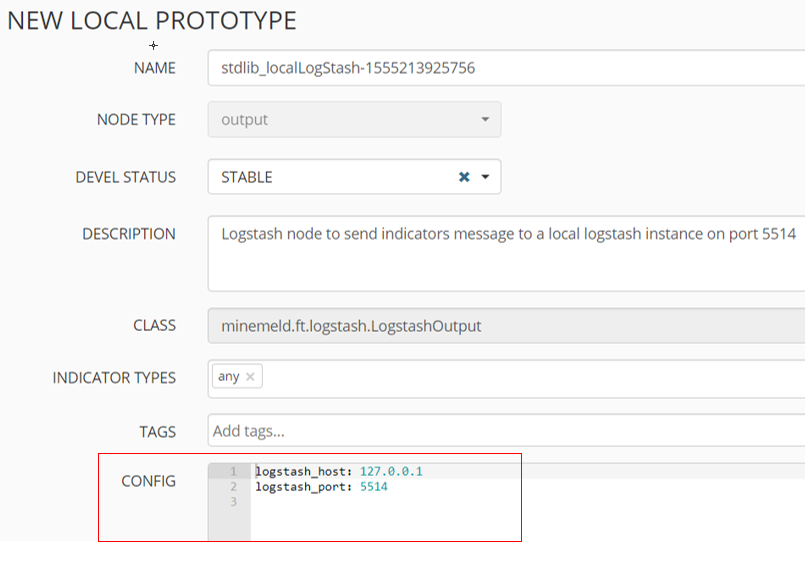
\*\* if you wish to customise the miner by adding your own data feed inputs – select new and edit the config



* Select Ipv4 processor protype if not available by default. Processor node can also be customised/renamed if needed.
* Select **Stdlib.local.Logstash** output prototpe to configure Logstash output node

\*\* **select new and edit the logstash host and port if you wish to cutomise from default**.





* Once the prortoypes configured , navigate to Config tab
* Select input field from Processor node and add the miners

Below example is a customised Ipv4 processor and logstash output config.

