Configuring Palo Alto Minemeld with Area 1 STIX/TAXII

Step 1: Configuring the Area 1 Minemeld Prototype

Obtain the Area 1 minemeld prototype file (`area1_taxii.yml`) and copy it into the local prototype directory on your instance of Minemeld (`/opt/minemeld/local/prototypes/`):

> `[Probably Area 1 public GitHub Repo] (file: area1_taxii.yml)`
> `https://github.area1security.com/sales/integrations/blob/master/minemeld/area1_taxii.yml`

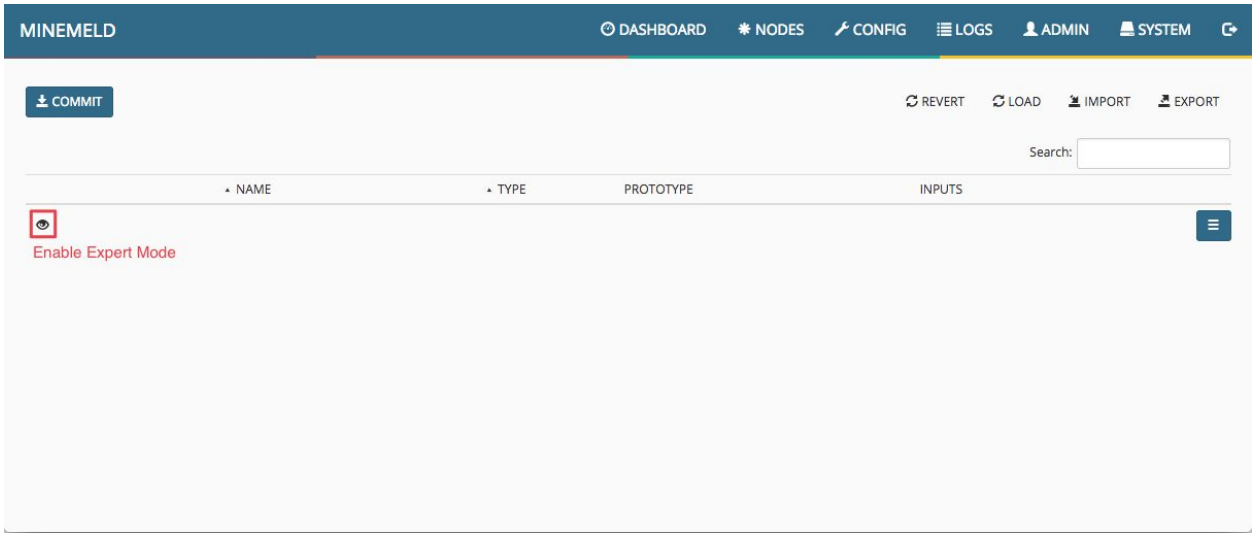
In order to use the TAXII feed, you will need to edit the feed configuration with your Area 1 credentials.

Modify the `[username]` and `[password]` entries in the `config:` section of the `area1_taxii.yml` prototype file:

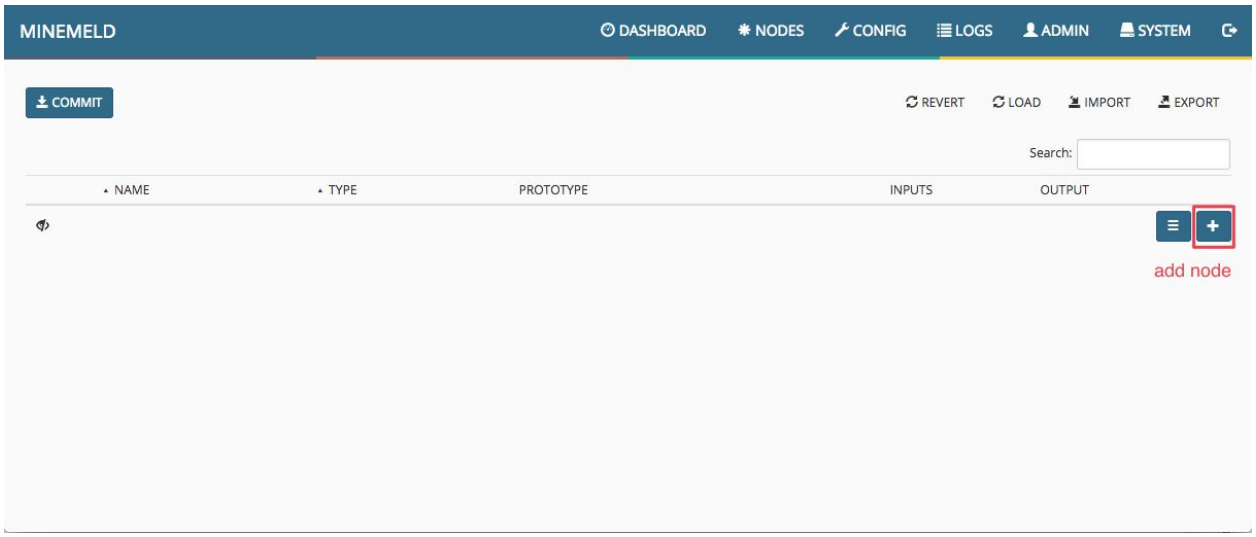
```
...
config:
   source_name: hailataxii.area1
   discovery_service: http://papillon.area1security.com/indicators/discovery
   username: [username]
   password: [password]
   collection: a1s.Indicators
   attributes:
       confidence: 30
       share_level: green
   age_out:
      sudden_death: false
      default: last_seen+30d
...
```

Step 2: Configuring the Area 1 STIX/TAXII Miner

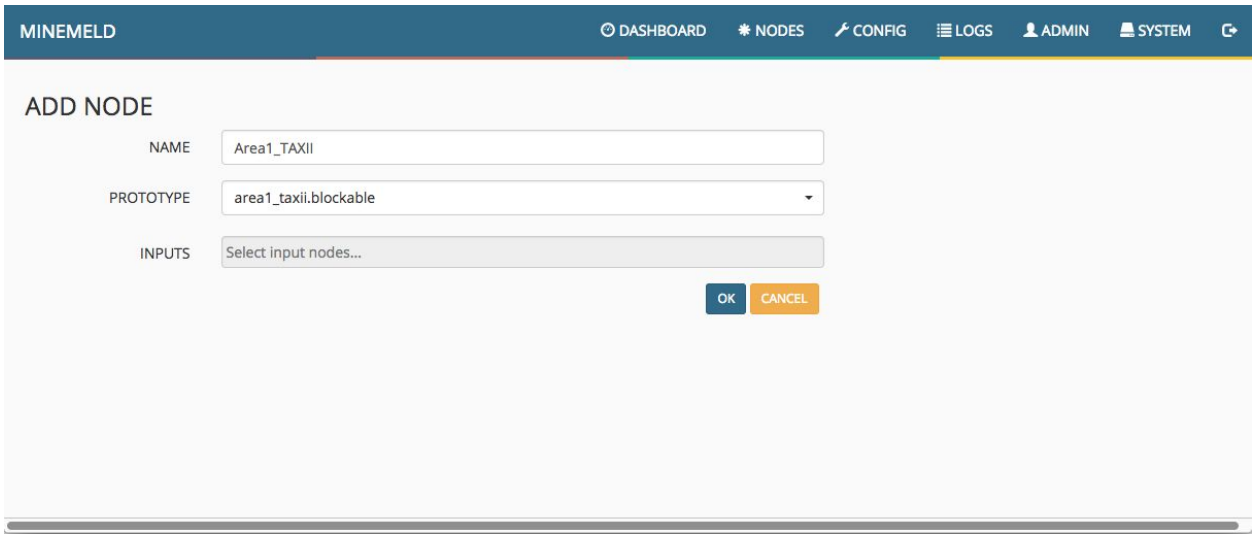
To configure a new miner, access the "CONFIG" section in the Minemeld GUI:



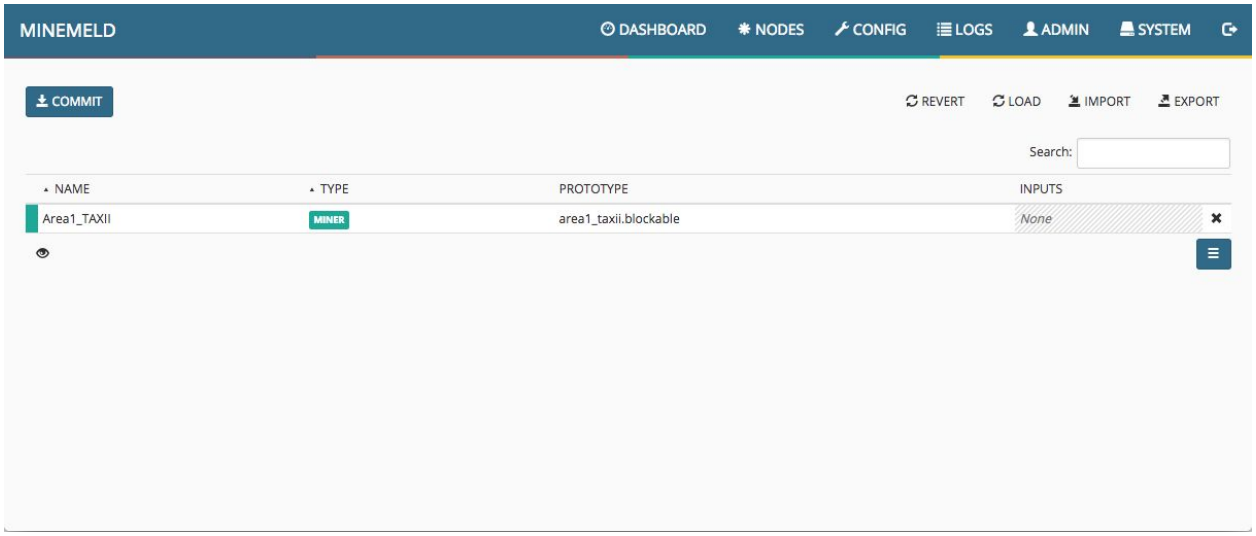
Click on the "Enable Expert Mode" icon and click on the "add node" button to add the new miner.



Create a new node, name it `Area1_TAXII`. If you have properly added the Area 1 Prototype in Step 1, you will be able to select the `area1_taxii.blockable` prototype from the dropdown list. Click the `"OK"` button to confirm the node creation:

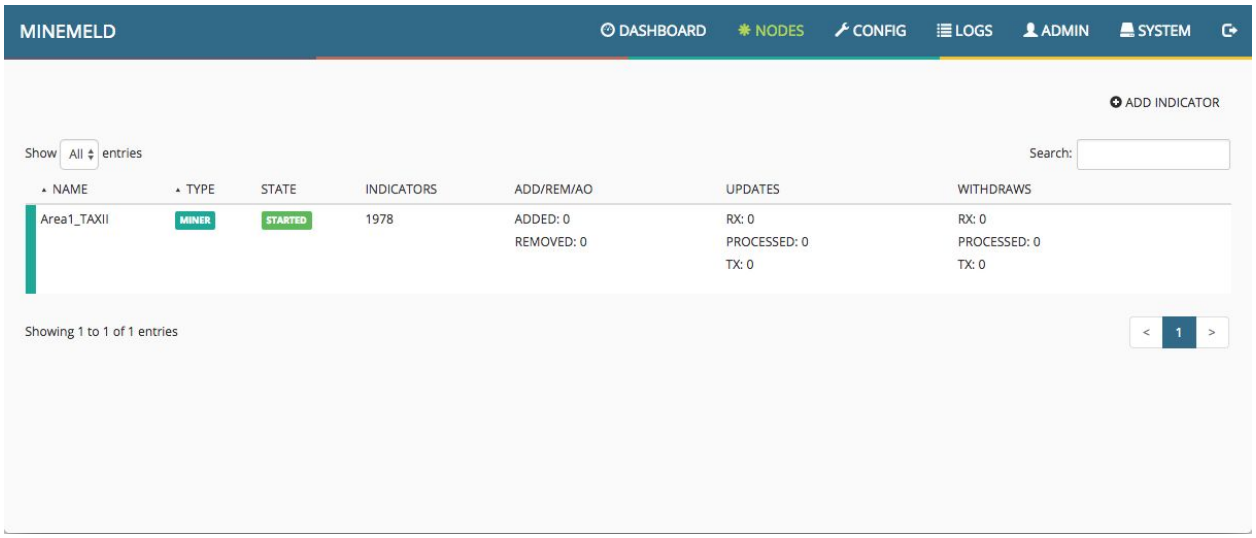


Once the new node has been created, click the `"Commit"` button to activate the new configuration:

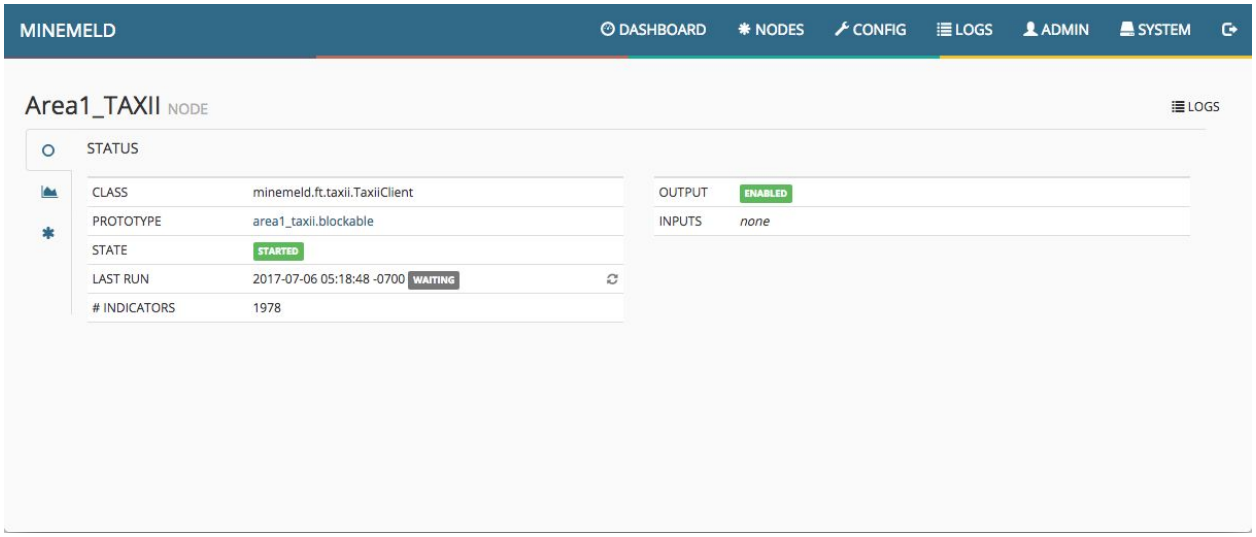


Once you click the `"COMMIT"` button, please wait a few minutes for the Minemeld engine to properly restart. You can check the status of the restarting process by access the `"SYSTEM"` section.

Once the Minemeld engine has restarted, you can click on the "NODES" section to see the status of the miner that was just added:



When you click on the miner, you will be able to see details regarding its status:



If the miner is in a "WAITING" mode, you can click the refresh button in the "LAST RUN" section to force a poll of the feed.

You can now add this new miner to your existing processors.