

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.areasecurity.com/sales/integrations/blob/master
/minemeld/area1_taxii.yml
```

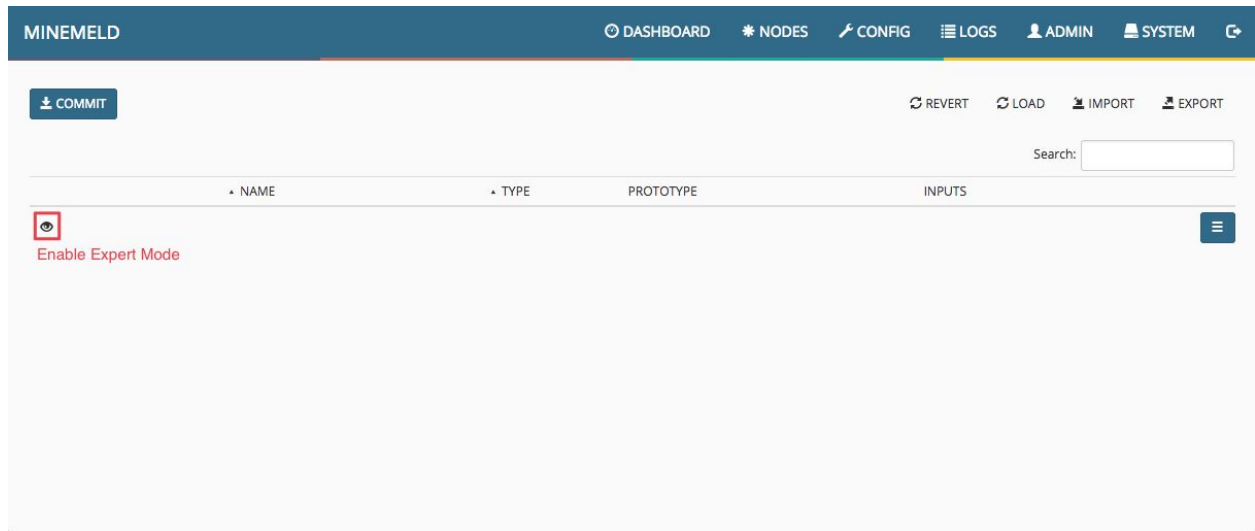
In order to use the TAXII feed, you will need to edit the feed configuration with your Area 1 credentials.

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

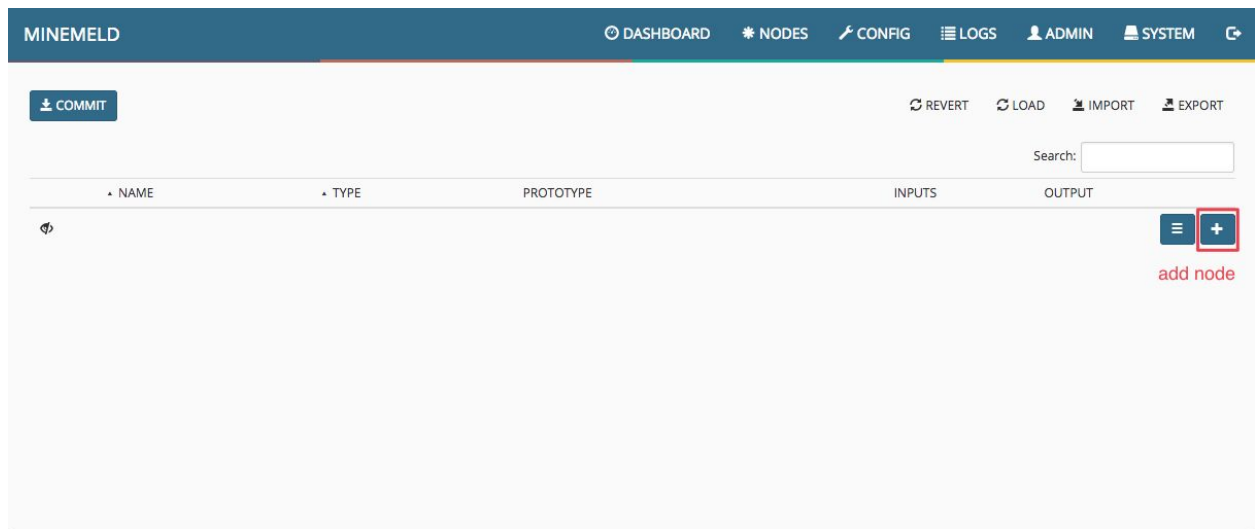
```
...
config:
  source_name: hailataxii.area1
  discovery_service: http://papillon.areasecurity.com/indicators/discovery
  username: [username]
  password: [password]
  collection: als.Indicators
  attributes:
    confidence: 30
    share_level: green
  age_out:
    sudden_death: false
    default: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

Step 2: Configuring the Area 1 STIX/TAXII Miner

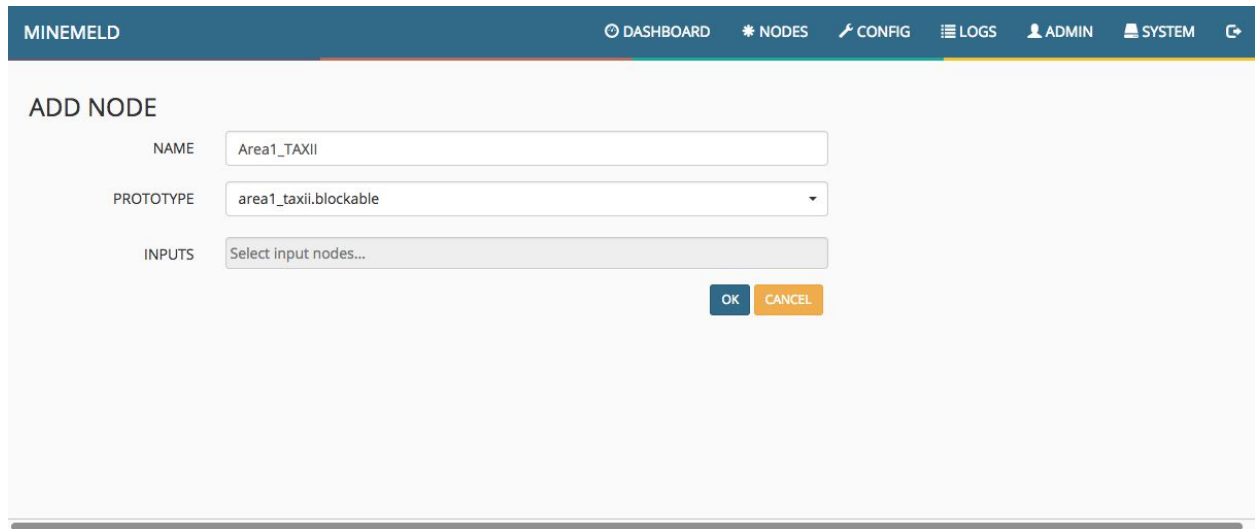
To configure a new miner, access the "CONFIG" section in the Minemeld GUI:



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:



MINEMELD DASHBOARD * NODES CONFIG LOGS ADMIN SYSTEM

ADD NODE

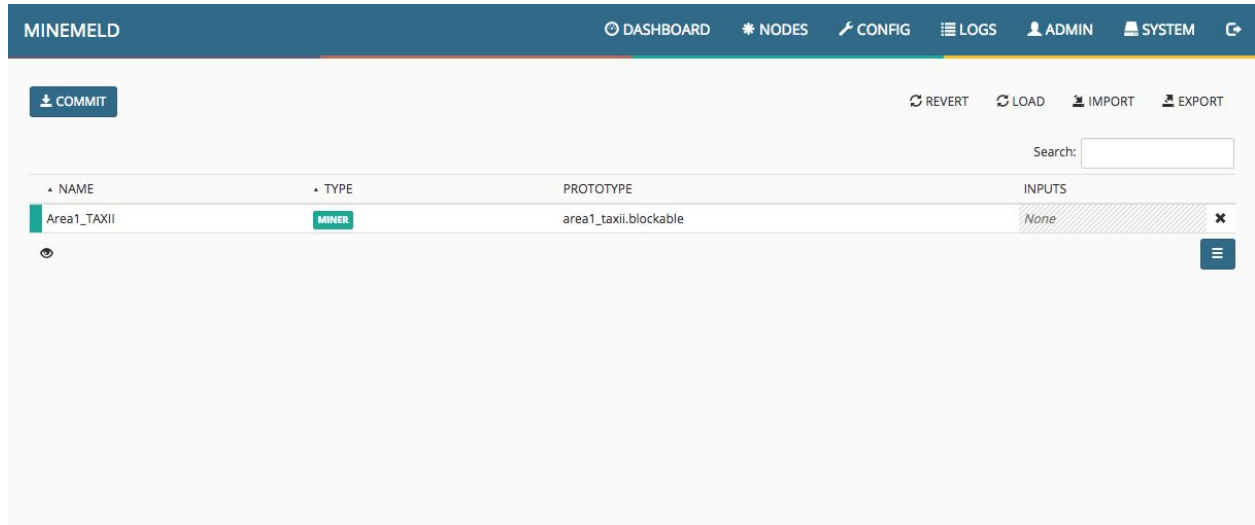
NAME

PROTOTYPE

INPUTS

OK CANCEL

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



MINEMELD DASHBOARD * NODES CONFIG LOGS ADMIN SYSTEM

COMMIT REVERT LOAD IMPORT EXPORT

Search:

NAME	TYPE	PROTOTYPE	INPUTS
Area1_TAXII	MINER	area1_taxii.blockable	None

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:

The screenshot shows the MINEMELD dashboard with the 'NODES' section selected. A table lists the nodes, with 'Area1_TAXII' highlighted in green. The table has columns for NAME, TYPE, STATE, INDICATORS, ADD/REM/AO, UPDATES, and WITHDRAWS. The 'Area1_TAXII' node is of type 'MINER' and has a 'STARTED' state. It has 1978 indicators and zero updates or withdrawals.

NAME	TYPE	STATE	INDICATORS	ADD/REM/AO	UPDATES	WITHDRAWS
Area1_TAXII	MINER	STARTED	1978	ADDED: 0 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 0	RX: 0 PROCESSED: 0 TX: 0

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

The screenshot shows the details for the 'Area1_TAXII' node. The node is in a 'WAITING' state. The details are as follows:

PROPERTY	VALUE
CLASS	minemeld.ft.taxii.TaxiiClient
PROTOTYPE	area1_taxii.blockable
STATE	STARTED
LAST RUN	2017-07-06 05:18:48 -0700 WAITING
# INDICATORS	1978
OUTPUT	ENABLED
INPUTS	none

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.