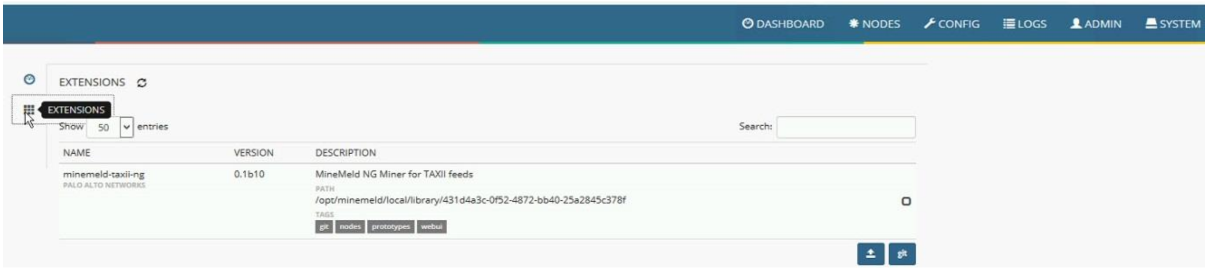
How-to ingest the SWIFT-ISAC TAXII feed
With PaloAltoNetwork MineMeld

Prerequisites:

- MineMeld installed
- Internet access from MineMeld host (e.g. Proxies, firewalls)

1. Login to the interface using and "admin" privileged account.

2. In the Top menu select "system" next select the "extensions" menu on the left (Figure 1)



NAME	VERSION	DESCRIPTION
minemeld-taxii-ng PALO ALTO NETWORKS	0.1b10	MineMeld NG Miner for TAXII feeds PATH /opt/minemeld/local/library/431d4a3c-0f52-4872-bb40-25a2845c378f TAGS git nodes prototypes webui

Figure 1: Extensions Menu

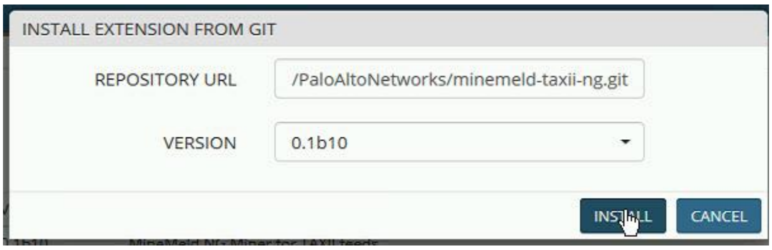
3. Install the "MineMeld NG Miner for TAXII feeds"

3.1 Press the "Git" button (Figure 1)

3.2 Repository URL: https://github.com/PaloAltoNetworks/minemeld-taxii-ng.git (Figure 2)

3.3 Press receive, next select the version you want to install (**0.1b10**) (Figure 2)

3.4 Press install to install the plugin (Figure 2)


INSTALL EXTENSION FROM GIT

REPOSITORY URL: /PaloAltoNetworks/minemeld-taxii-ng.git

VERSION: 0.1b10

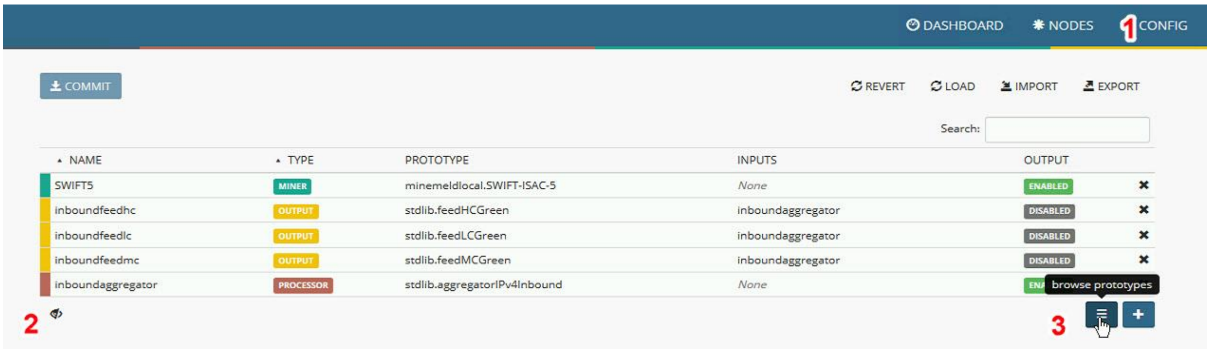
Figure 2: Install Extension from Git

4. Once completed create a new prototype for SWIFT-ISAC

4.1 Select the "Config" menu (1) (Figure 3)

4.2 Press the eye icon on the bottom left a new button will appear (2) (Figure 3)

4.3 Press the "Browse Prototypes" (3) (Figure 3)



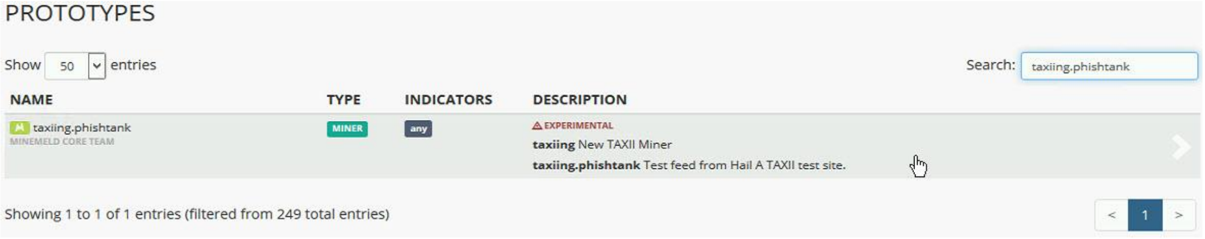
NAME	TYPE	PROTOTYPE	INPUTS	OUTPUT
SWIFT5	MINER	minemeldlocal.SWIFT-ISAC-5	None	ENABLED
inboundfeedhc	OUTPUT	stdlib.feedHCGreen	inboundaggregator	DISABLED
inboundfeedlc	OUTPUT	stdlib.feedLCGreen	inboundaggregator	DISABLED
inboundfeedmc	OUTPUT	stdlib.feedMCGreen	inboundaggregator	DISABLED
inboundaggregator	PROCESSOR	stdlib.aggregatorIPv4Inbound	None	ENA

Figure 3: How to activate the browse prototype menu

5. Finding the prototype we just installed

5.1 Using the search bar, search for “**Taxiing.phistank**” (Figure 4)

5.2 Select the Miner by pressing it as indicated on (Figure 4)



PROTOTYPES

Show 50 entries Search: taxiing.phishtank

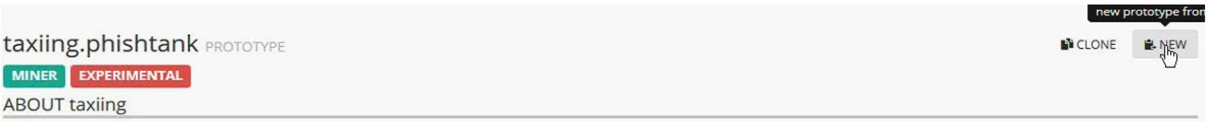
NAME	TYPE	INDICATORS	DESCRIPTION
taxiing.phishtank MINEMELD CORE TEAM	MINER	any	EXPERIMENTAL **taxiing** New TAXII Miner **taxiing.phishtank** Test feed from Hail A TAXII test site.

Showing 1 to 1 of 1 entries (filtered from 249 total entries)

Figure 4: Finding the correct Miner

6. Creating a new miner with the “taxiing.phishtank” miner.

6.1 Press the “**new**” button (Figure 5)



taxiing.phishtank PROTOTYPE

Figure 5: Creating a new miner 1/2

7. Creating the configuration

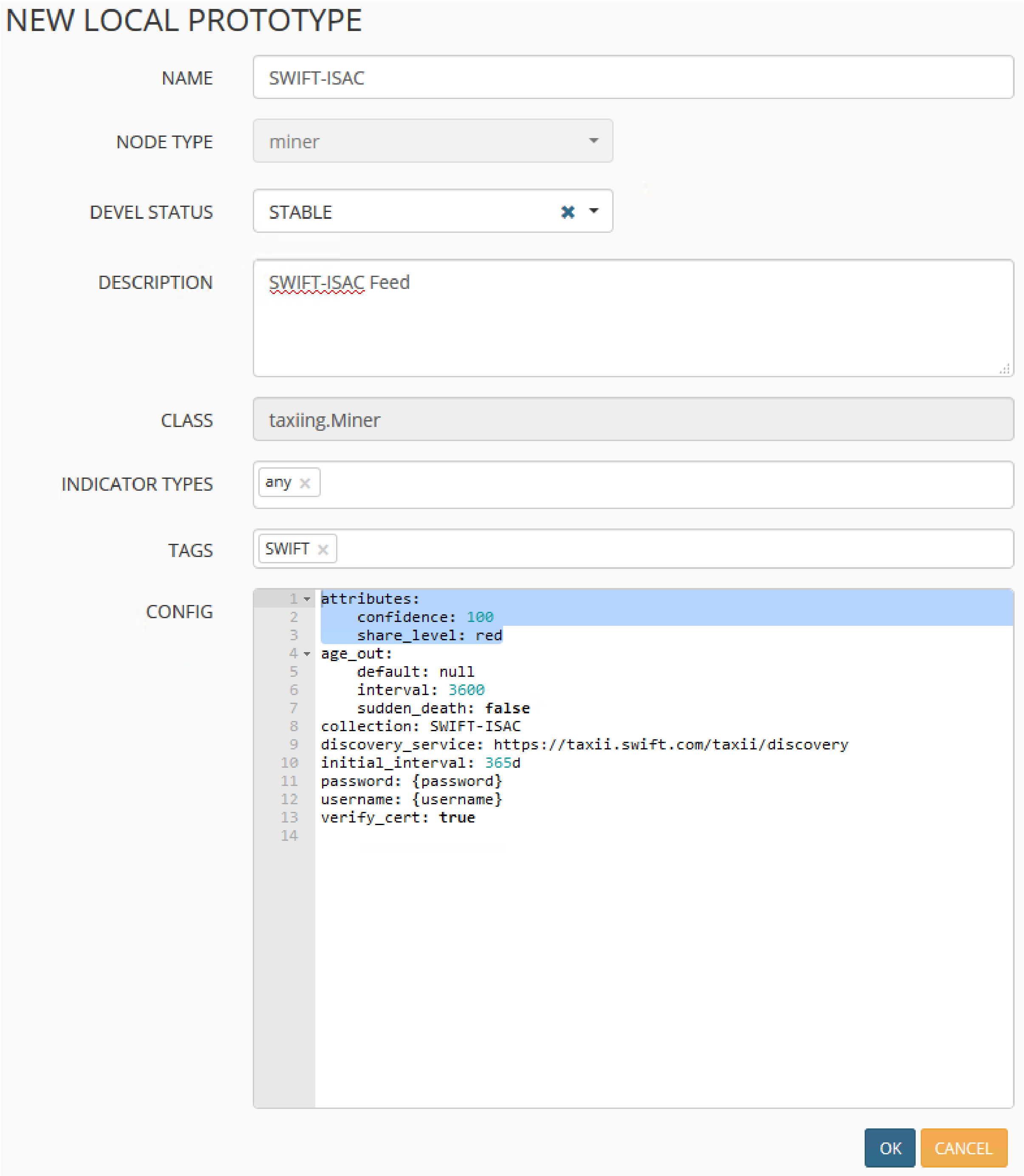
Name:	SWIFT-ISAC
Devel-status:	Stable
Description:	SWIFT-ISAC Feed
Indicator type:	Any
Tag:	SWIFT

Config: Please keep in mind that this is written in YML,
Formatting is important and could give problems if not done correctly.

7.1 Fill in your username and password as provided by SWIFT.

```
attributes:
    confidence: 100
    share_level: red
age_out:
    default: null
    interval: 3600
    sudden_death: false
collection: SWIFT-ISAC
discovery_service:
https://taxii.swift.com/taxii/discovery
initial_interval: 365d
password: {password}
username: {username}
verify_cert: true
```

Configuration example, see Figure 6.



NEW LOCAL PROTOTYPE

NAME: SWIFT-ISAC

NODE TYPE: miner

DEVEL STATUS: STABLE

DESCRIPTION: SWIFT-ISAC Feed

CLASS: taxiing.Miner

INDICATOR TYPES: any

TAGS: SWIFT

CONFIG:

```
attributes:
    confidence: 100
    share_level: red
age_out:
    default: null
    interval: 3600
    sudden_death: false
collection: SWIFT-ISAC
discovery_service: https://taxii.swift.com/taxii/discovery
initial_interval: 365d
password: {password}
username: {username}
verify_cert: true
```

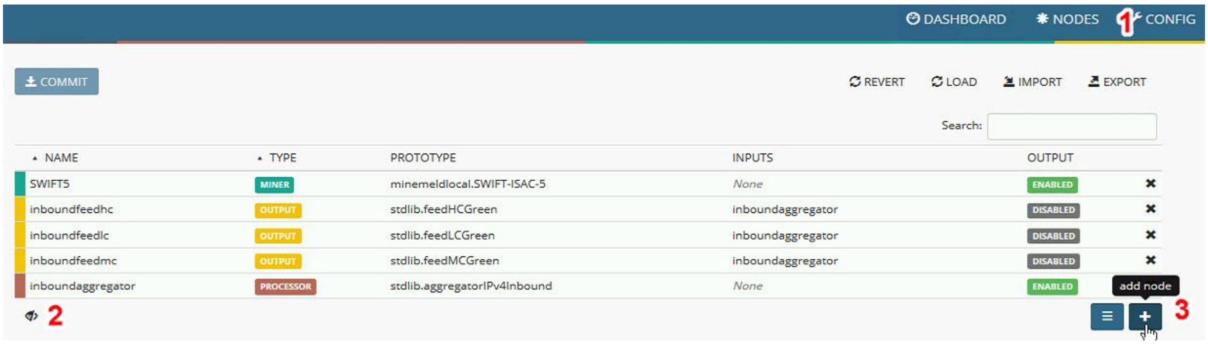
Figure 6: Creating a new miner 2/2 – Example configuration (Configuration is different than the ones in previous step)

8. Adding a new node to MineMeld

8.1 Select the “**config**” menu (1) (Figure 7)

8.2 Press the “**eye**” icon on the bottom left a new button will appear (2) (Figure 7)

8.3 Press the “**plus**” icon to add a new node to your configuration (Figure 7)



NAME	TYPE	PROTOTYPE	INPUTS	OUTPUT	
SWIFT5	MINER	minemeldlocal.SWIFT-ISAC-5	*None*	ENABLED	✖
inboundfeedhc	OUTPUT	stdlib.feedHCGreen	inboundaggregator	DISABLED	✖
inboundfeedlc	OUTPUT	stdlib.feedLCGreen	inboundaggregator	DISABLED	✖
inboundfeedmc	OUTPUT	stdlib.feedMCGreen	inboundaggregator	DISABLED	✖
inboundaggregator	PROCESSOR	stdlib.aggregatorIPv4Inbound	*None*	ENABLED	

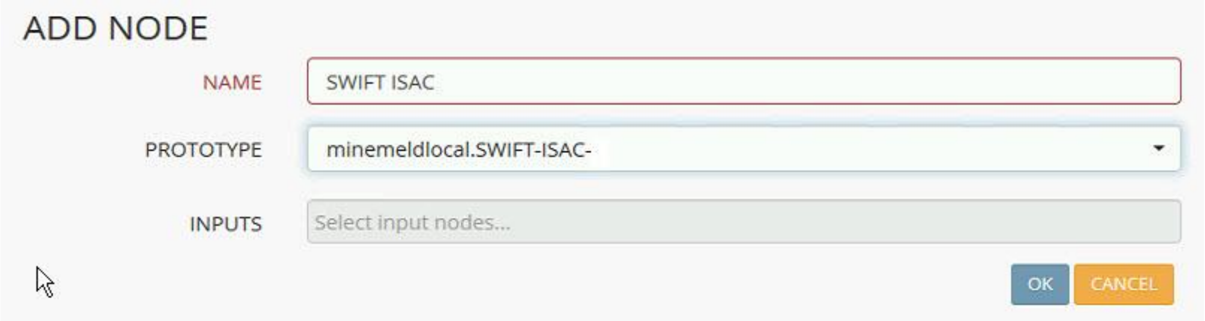
Figure 7: Adding the new node

9. Adding the node by selecting the prototype

9.1 Name: SWIFT-ISAC (Figure 8)

Prototype: “minemeldlocal.SWIFT-ISAC”

9.2 After pressing “**Ok**”, you will go back to the previous menu, Press “**Commit**” to save the node.



ADD NODE

NAME: SWIFT ISAC

PROTOTYPE: minemeldlocal.SWIFT-ISAC-

INPUTS: Select input nodes...

Figure 8: Adding a node

10. Wait, the first pull can take little while depending on your internet speed and setup, when completed it would look like this. (Figure 9)

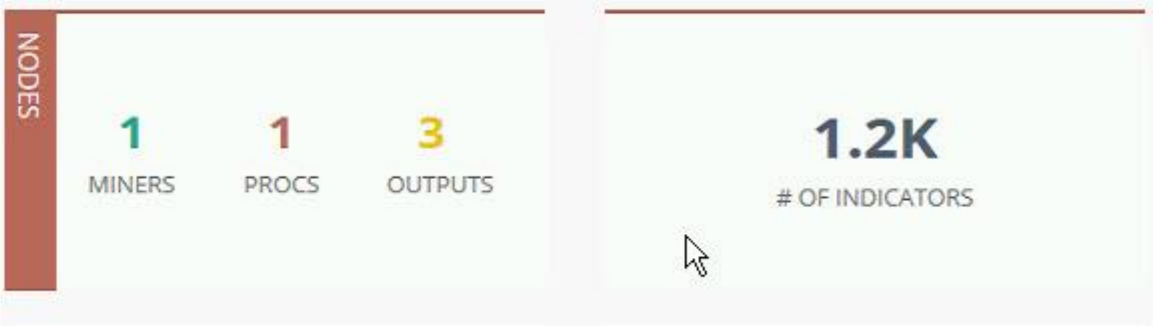


Figure 9: Configuration with 1 miner; and amount of indicators