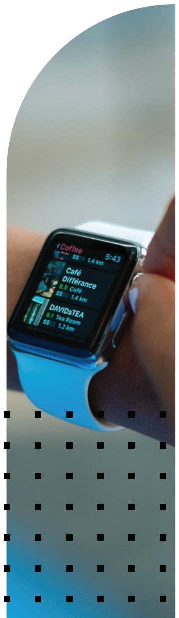
DEPLOYMENT GUIDE

FSM Nozomi CMDB Inbound Integration



FSM Nozomi CMDB Inbound Integration

Description:

This document describes the configuration process to automatically import Nozomi's CMC (Central Management Console) CMDB into FortiSIEM CMDB via inbound integration. The integration works via a pulling script which runs on cron periodically to fetch CMDB data from Nozomi CMC and stores it on FortiSIEM file system as a CSV file.

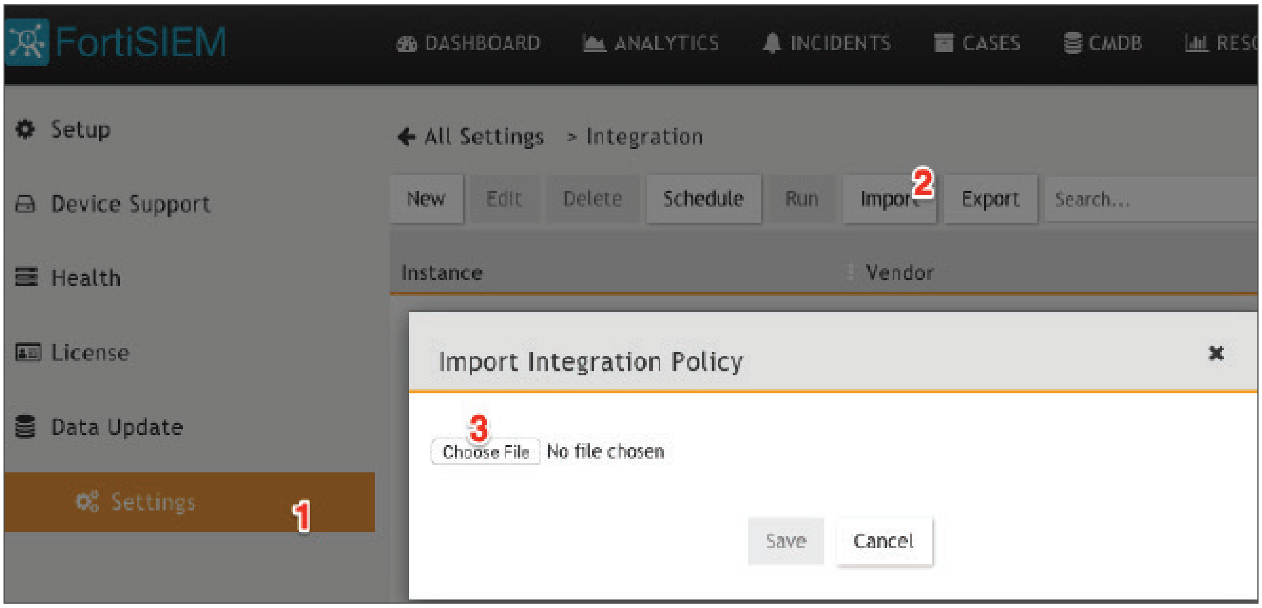
FortiSIEM Inbound Integration imports the CSV file to its CMDB via the integration scheduler:

The high-level process is:

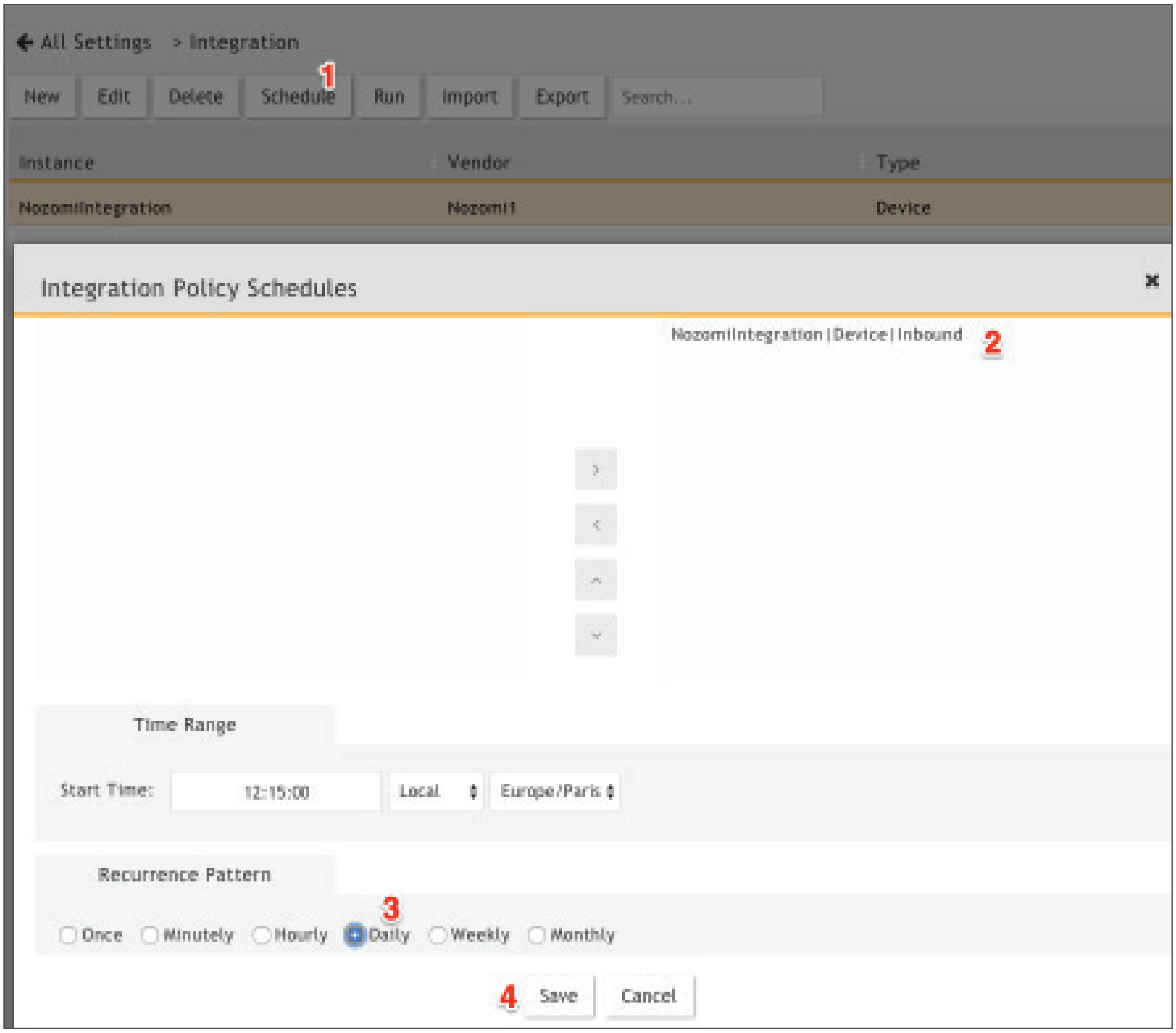
1. Download the Integration script and the integration XML definition
2. Add the script to FortiSIEM cron with the right credentials
3. Import the integration definition and schedule it

Steps:

1. Download the python script and the xml integration definition [https://github.com/ftntcse/ fsm_nozomi_cmdb_integration/archive/master.zip]
2. Copy **fetch_nozomi_cmdb.py to FortiSIEM /usr/local/bin/**
3. **chmod +x /usr/local/bin/ fetch_nozomi_cmdb.py**
4. Execute the script to make sure Nozomi CMC connectivity and credentials are correct
   - **fetch_nozomi_cmdb.py -h for arguments details**
5. If there are no error messages the CSV output file by default will be at /tmp/nozomi.csv
6. Schedule the script execution with **crontab -e** (each day is probably a good frequency)
7. Import FortiSIEM inbound integration:



- Go to Admin => Settings => Integration => Import and select the downloaded Integration definition (NozomiCSVIntegration.xml)
- Click "Run" to invoke the integration, you should see a number of devices imported in CMDB. Make sure /tmp/nozomi.csv is populated.



Instance	Vendor	Type
NozomiIntegration	Nozomi1	Device

Integration Policy Schedules

NozomiIntegration |Device| Inbound

Time Range

Start Time: 12:15:00 Local Europe/Paris

Recurrence Pattern

○ Once ○ Minutely ○ Hourly ● Daily ○ Weekly ○ Monthly

- Once imported click on Schedule, Select Nozomi-integration, set the schedule and click save.

At this point the integration script should be running periodically to create /tmp/nozomi.csv and FortiSIEM integration runs also periodically to import the devices found in this file.

www.fortinet.com

June 9, 2021 8:40 PM