

DEPLOYMENT GUIDE

FSM Nozomi CMDB Inbound Integration





FSM Nozomi CMDB Inbound Integration

Description	 3
High-level process	 3
Steps	 3

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:

🕱 FortiSIEM	🐠 DASHBOARD 🖮 ANALYTICS	A INCIDENTS	CASES 🔮 CMDB	Lini Res
O Setup	← All Settings > Integration			
⊟ Device Support	New Edit Delete Sched	ule Run Impor <mark>2</mark>	Export Search	
≡ Health	Instance	Vendor		
E License	Import Integration Poli	су		×
🛢 Data Update	3 Choose File No file chosen			
📽 Settings 🛛 ┨		Faura Cancal		
		save Cancel		

- 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.

← All Settings > Integration		
New Edit Delete Schedule	Run Import Export Se	rarch
Instance	Vendor	Туре
Nozomilitegration	Nozomi1	Device
Integration Policy Schedules	5	×
	2 4 14	NozomiIntegration Device Inbound 2
Time Range		
Start Time: 12:15:00	Local ¢ Europe/Paris ¢	
Recurrence Pattern		
Once OMinutely OHourly	3 Daily ○Weekly ○Monthly	
	4 Save Ca	ancel

• 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

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortiloare^{*}, FortiGate^{*}, FortiCare^{*} and FortiGuard^{*}, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Tortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet For absolute darity, any such warrants that the identified product will perform accertain to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute darity, any such warrants that the identified to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

June 9, 2021 8:40 PM