Lab00 Index&PreconfLab

LAB ACCESS INFORMATION

SYSTEM	FABRIC NAME	METHOD	USERNAME	PASSWORD	IP
FortiPAM	FortiPAM	HTTPS SSH	admin	Fortinet123#	10.20.0.3
FortiGate	FortiGate	HTTPS SSH	admin	Fortinet123#	Port3:10.20.0.254 Port6:192.168.60.254
FortiNDR	FortiNDR	HTTPS SSH	admin	Fortinet123#	10.20.0.5
FortiAnalyzer	FAZ + FAI	HTTPS SSH	admin	Fortinet123#	10.20.0.4
FortiSwitch	Switch_Internal	SSH	Admin	Fortinet123#	10.20.0.200
Windows Server 2016	WindowsServer	Display	Administrator	Fortinet123#	10.20.0.100
FortiSOAR	FortiSOAR	HTTPS SSH/Display	csadmin csadmin	Fortinet123# changeme	10.20.0.8
Windows10	Victim (GAMMA)	Display	fortixperts	Fortinet123#	192.168.60.13
Kali Linux	Attack	Display	Kali	kali	192.168.60.20

BELOW YOU CAN FIND A BRIEF EXPLANATION OF EACH LAB

LABORATORY 1: Ways for integrating FortiGate with FortiNDR: We will explore the different methods of integrating FortiNDR with our operational architectures to get the most out of the solution and different ways to enhance our customers' security posture with FortiNDR.

LABORATORY 2: Internal Suspicious Activities: We will run several network probing tools, typically used by attackers during the reconnaissance phase. These tools will include network scanning, port scanning, vulnerability scanning, and others.

This is to generate anomalous traffic that will be recorded by FortiGate in FortiAnalyzer, allowing us to conduct investigations with FortiAI.

LABORATORY 3: Anomaly Detection with FortiAI and Automatic Response: We will use FortiAI from FortiAnalyzer to generate forensic investigations, demonstrating how easy it is to conduct these investigations with the support of FortiAI.

Additionally, we will configure an automated response layer for the automatic blocking of suspicious IPs, configuring the FortiAnalyzer with its event management capability; "Event

Handler", and the execution of automated responses from FortiGate with its "Automations Stitch".

LABORATORY 4: Anomaly Detection by FortiNDR: We will perform several activities that an attacker would commonly carry out on the internal network, such as copying a malicious file to a file server integrated with FortiNDR, hoping that FortiNDR will detect it and move it to a quarantine folder.

Additionally, we will configure the FortiGate AV module to send malicious files to FortiNDR so we can execute automatic blocks.

Finally, we will analyze the NetFlow ML module and how it alerts us to suspicious traffic outside the ML baseline.

LABORATORY 5: Automated response with FortiSOAR: We will integrate FortiNDR with FortiAnalyzer and the FortiAnalyzer with the FortiSOAR and simulate a kind of internal network attack. FortiNDR will notify to FortiAnalyzer (As data lake) and the FortiAnalyzer will inform to FortiSOAR of this event, which will then execute a response on the FortiGate (As a quarantine) and the FortiSOAR from the FortiGate will obtain the MAC address of the victim, then use this MAC address to go to the “Switch_Internal” to find the port where the victim is connected and will shut down the port, simulating automatic isolation of the victim.

Bonus LABORATORY 6: Centralized management of privileged accounts: We will integrate FortiPAM with FortiGate to demonstrate the procedure and essence of FortiPAM credential management.

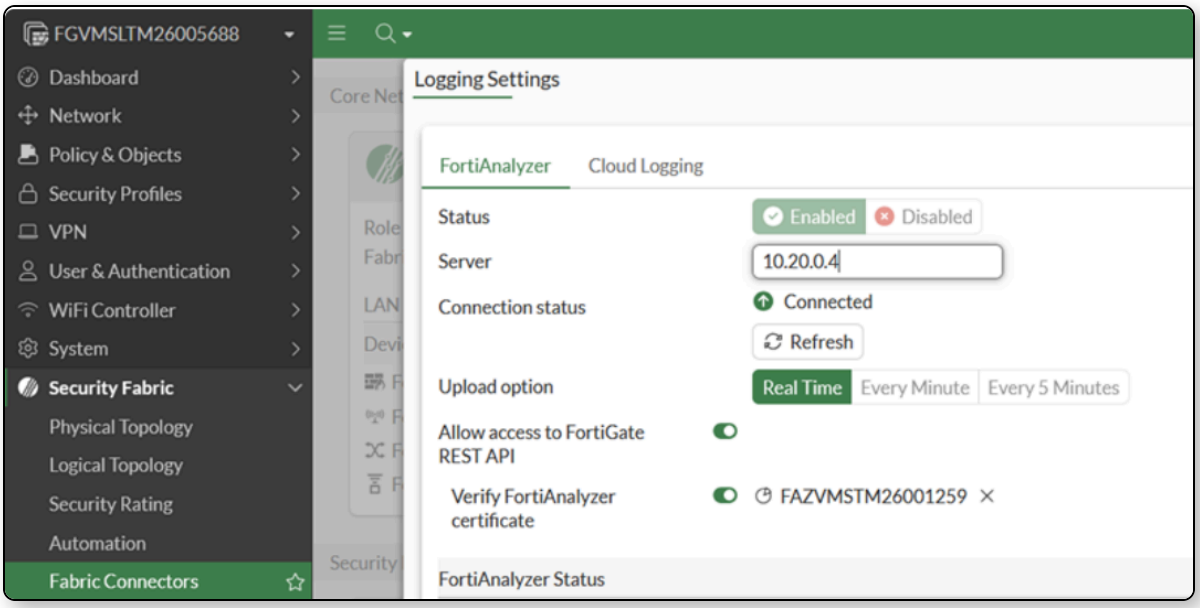
Then we will integrate FortiAnalyzer with FortiPAM and explain the access approval process.

Finally, we will integrate FortiPAM with a Windows server and use AutoIT to execute customized application tasks. This will demonstrate the advantages of using a PAM solution in a corporate security posture.

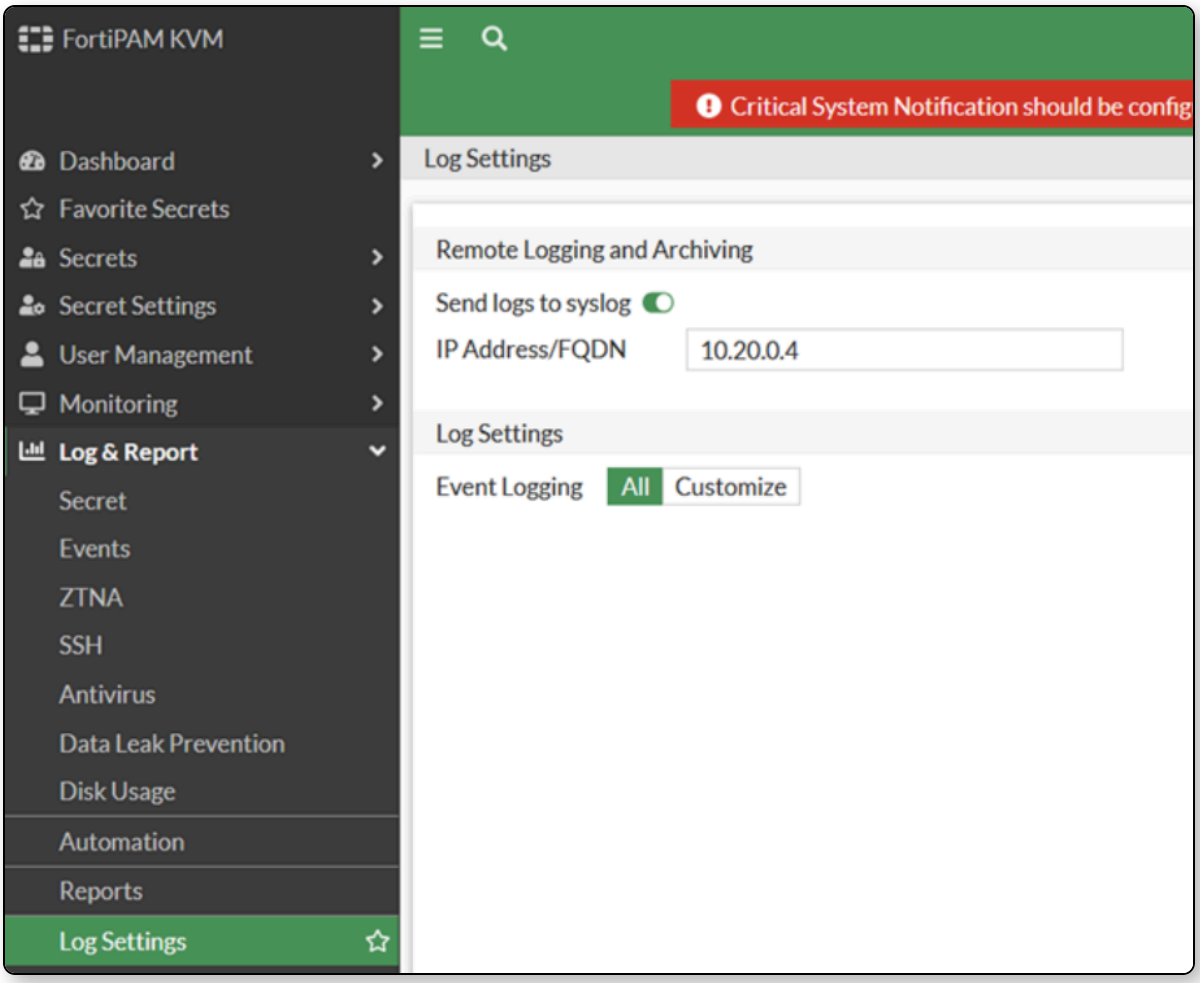
PRE-CONFIGURATION LAB

We need to do the next configurations before star to execute each lab.

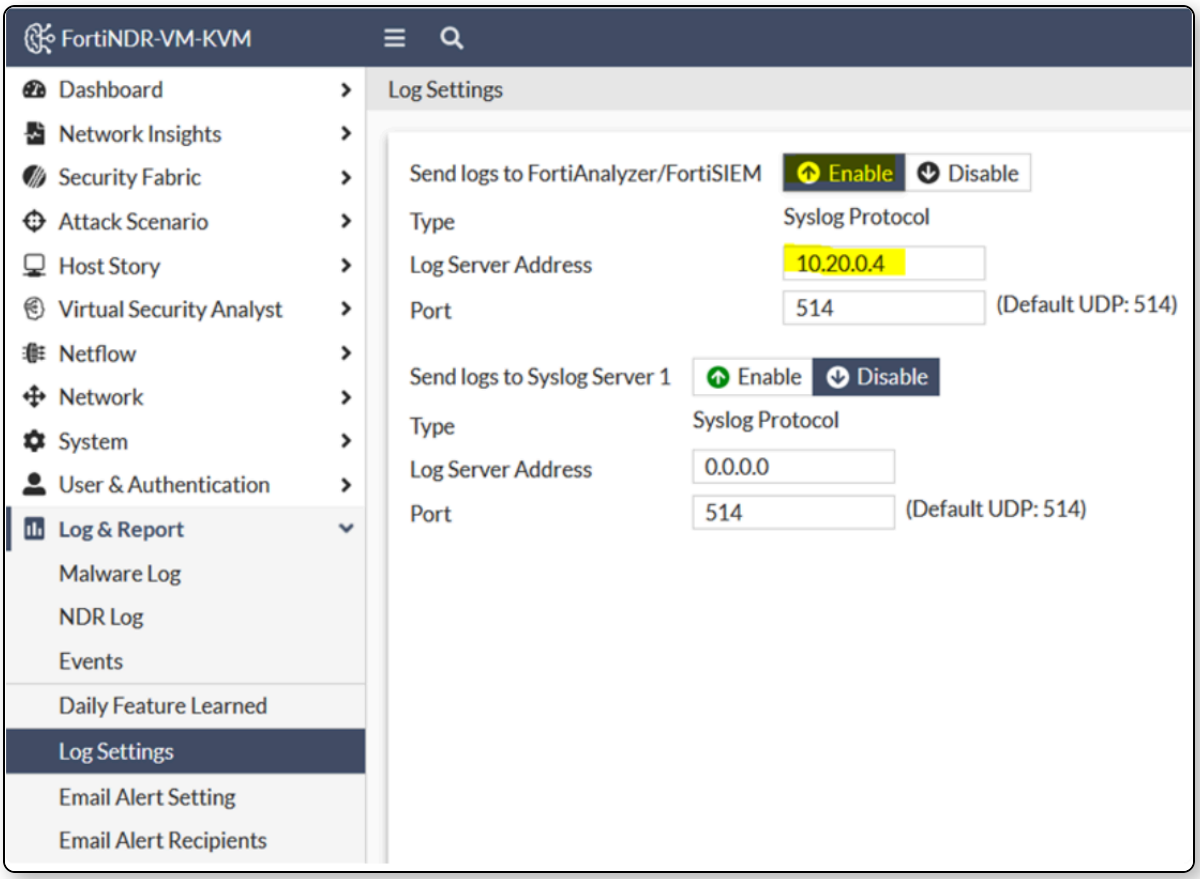
a) Integrate FortiGate with FortiAnalyzer via Security Fabric.



b) Integrate FortiPam with FortiAnalyzer via Security Fabric.



c) Integrate FortiNDR with FortiAnalyzer via Security Fabric.



Lab01 Ways to integrate FGT and FNDROnPremise

LABORATORY 1: Different ways of integrating FortiGate with FortiNDR:

We will integrate FortiGate with FortiNDR via Netflow and, using a "one-arm" interface (We will have more visibility), explore integration alternatives to gain complete visibility of my network, not only at the perimeter level but also down to lower network layers.

a) Integration of FortiGate with FortiSwitch “Switch_Internal” via “One Arm Interface” and “Port Sniffer”.

```
- We should configure the “Port11” in the “Swtich_Internal” as a “Port Mirror”.
- Accessing via “Display” to the “Switch_Internal” and we need to do the next
configuration:
```

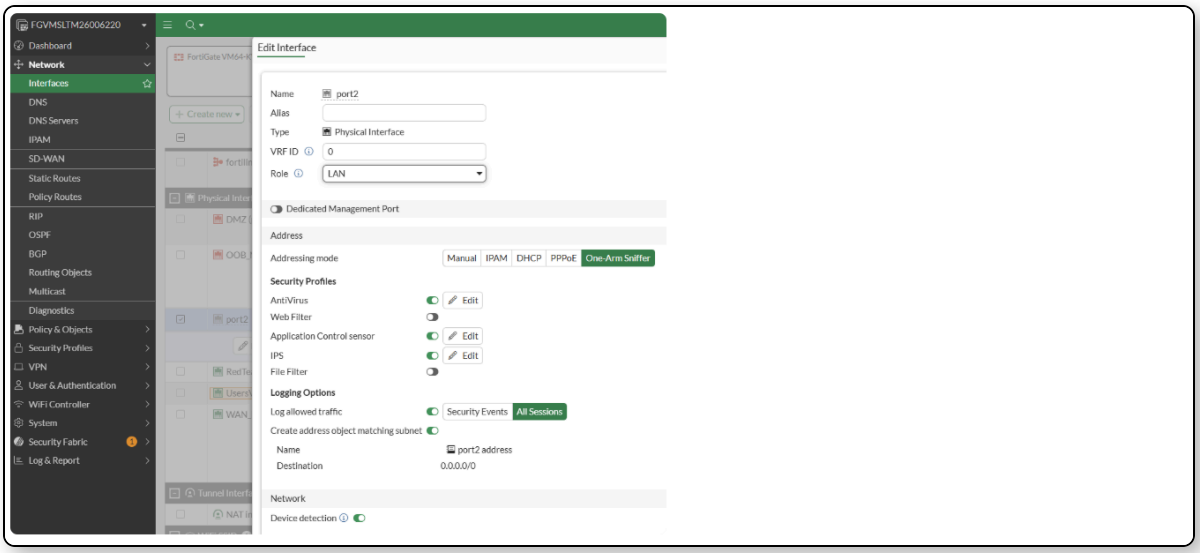
```
FS24VM02RRD3I046 #
FS24VM02RRD3I046 # config switch mirror

FS24VM02RRD3I046 (mirror) # edit MirrorToFortiGate

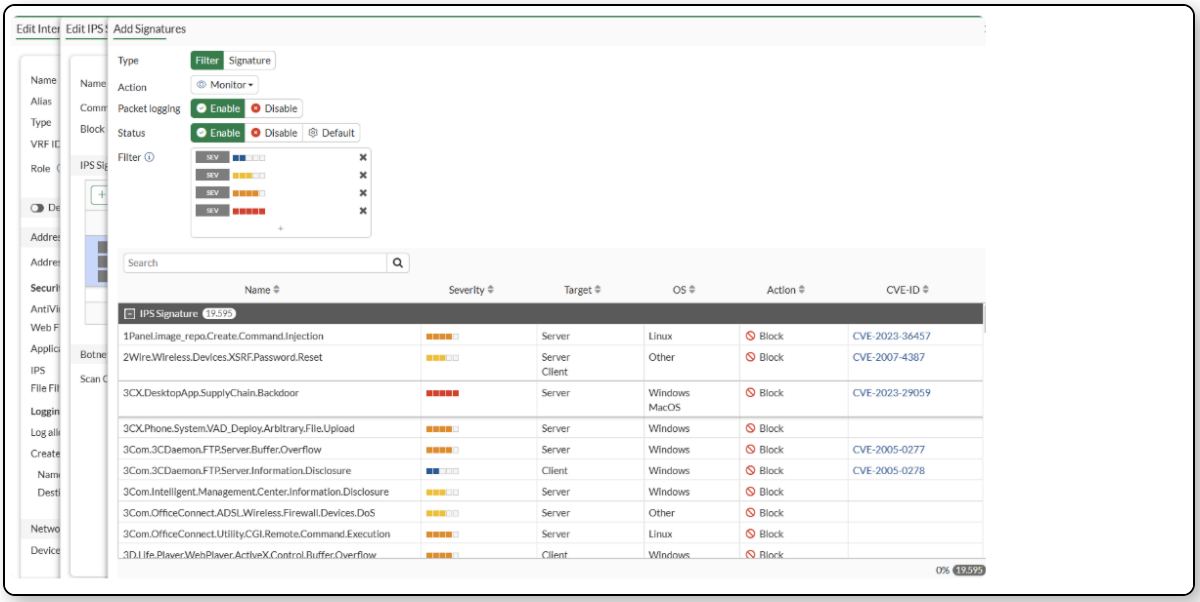
FS24VM02RRD3I046 (MirrorToFortiGate) # show
config switch mirror
    edit "MirrorToFortiGate"
        set status active
        set dst "port11"
        set src-ingress "port3"
        set src-egress "port3"
    next
end

FS24VM02RRD3I046 (MirrorToFortiGate) # _
```

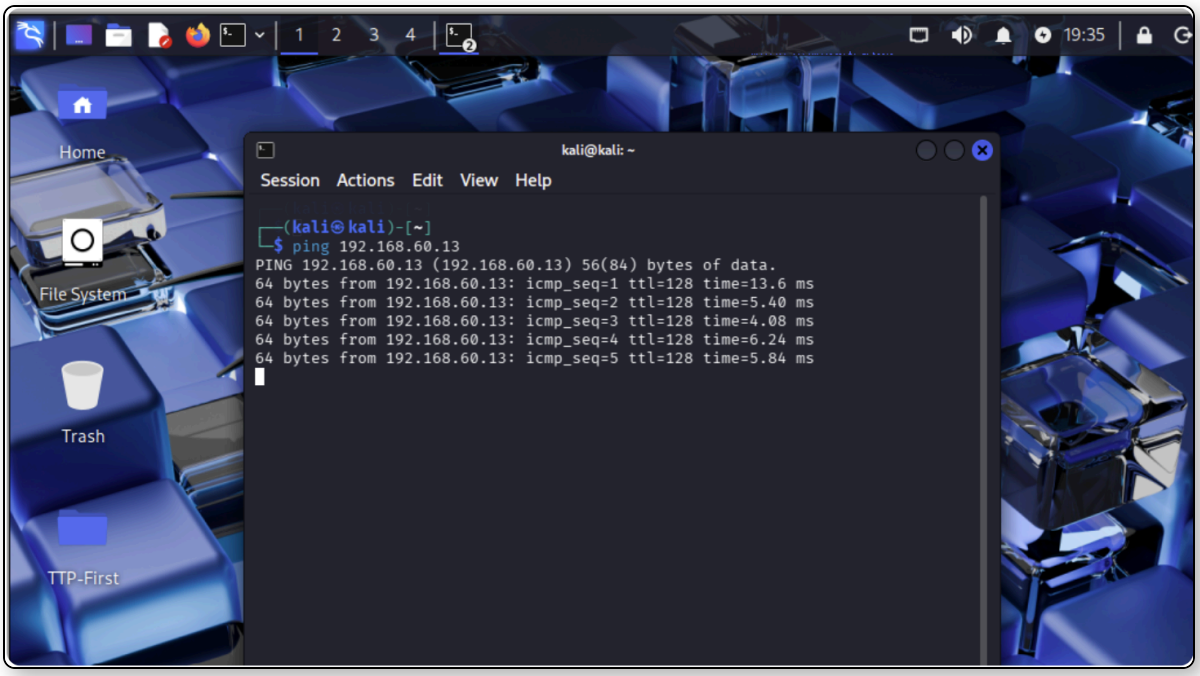
```
- In the Switch´s “port3” is connected the “Victim” client. And the “port11” is
connected the FortiGate´s “port2”
- We should configure the FortiGate´s “Port2” as a “One-Arm Sniffer” interface.
Accessing via HTTPS to FortiGate and we should be the next configuration:
```

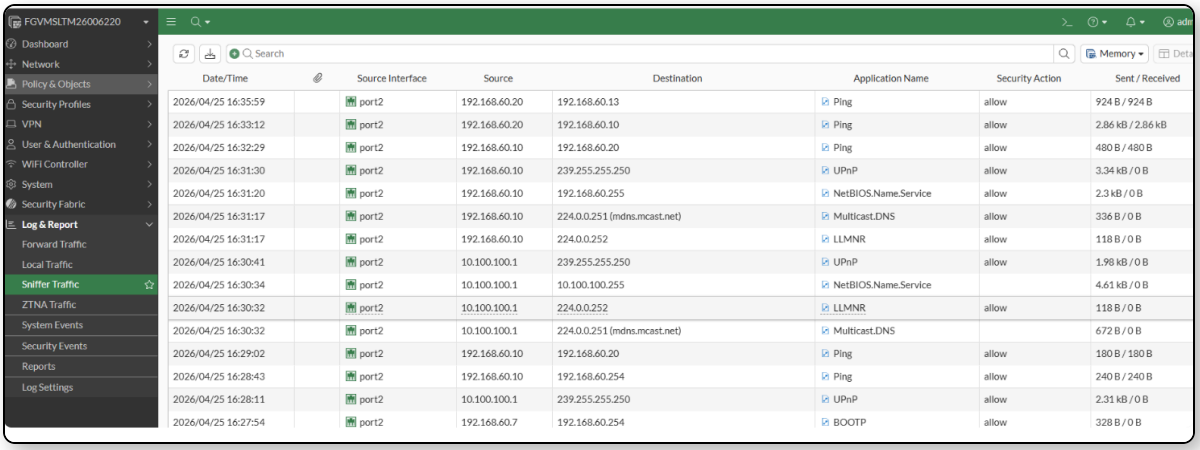


- Plaese make sure that all of the security profiles assigned in the "One Arm" interface are only "Monitoring", recomended the IPS with this configuration.



- You can validate if the port mirror is working well using a “Sniffer packet” in the FortiGate via SSH. We need to do a PING from “Attacker” device to “Victim” client:





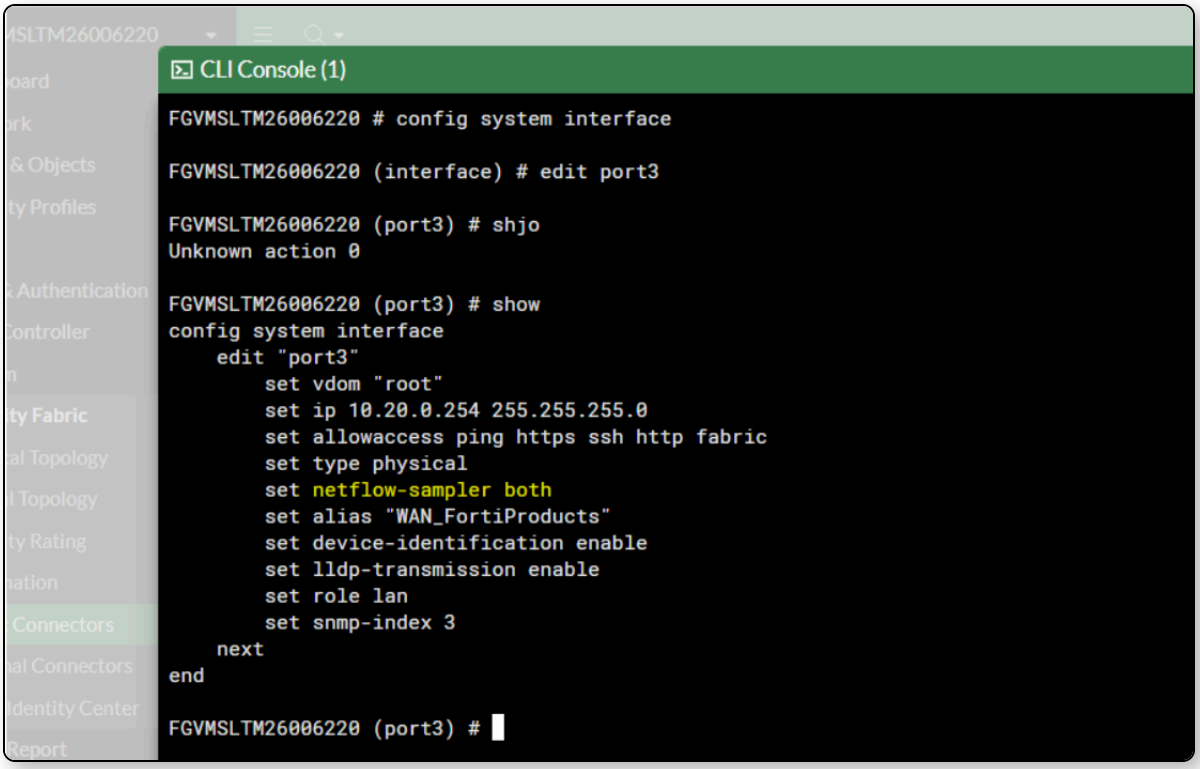
b) Integration from FortiGate with FortiNDR via NetFlow.

```
- Accessing FortiGate via SSH and we are going to activate and configure Netflow
integration with the FortiNDR:
```

```
FGVMSLTM26006220 (netflow) # show
config system netflow
    set active-flow-timeout 60
    set template-tx-timeout 60
    config collectors
        edit 5
            set collector-ip "10.20.0.5"
            set source-ip "10.20.0.254"
        next
    end
end

FGVMSLTM26006220 (netflow) #
```

- We need to activate the Netflow in every interface that we want to monitor using the next command: "set netflow-sampler both".
- We are going to activate the Netflow in the FortiGate “Port3” & "Port6" (Netflow does not send sniffer paquets)



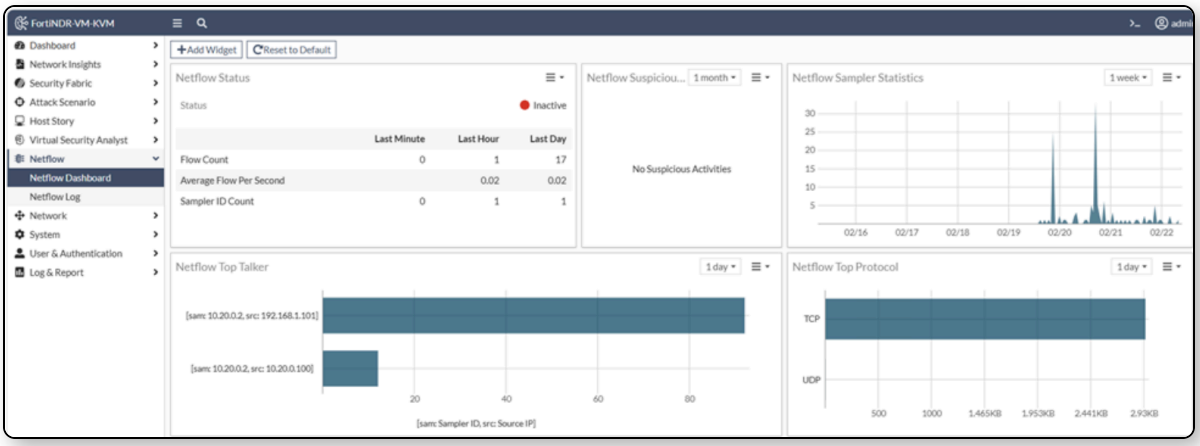
CLI Console (1)

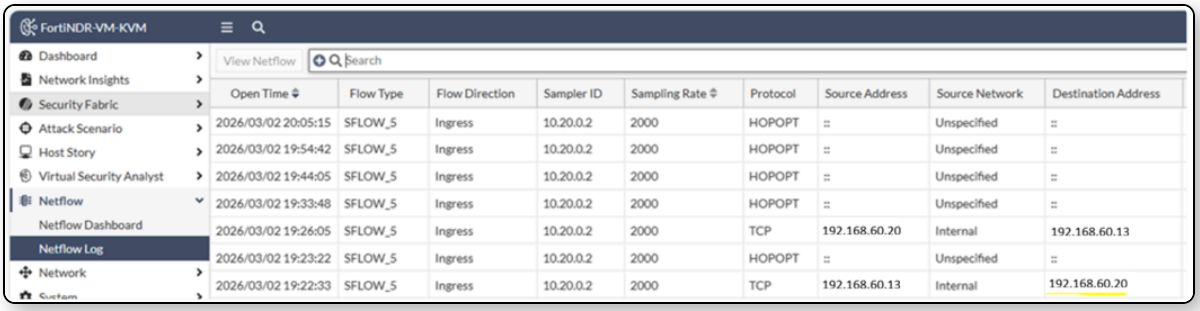
```
        set snmp-index 4
    next
    edit "port5"
        set vdom "root"
        set ip 192.168.100.254 255.255.255.0
        set allowaccess ping
        set type physical
        set alias "UsersVM"
        set device-identification enable
        set snmp-index 5
    next
    edit "port6"
        set vdom "root"
        set ip 192.168.60.254 255.255.255.0
        set allowaccess ping
        set type physical
        set netflow-sampler both
        set alias "RedTeamUsers"
        set device-identification enable
        set lldp-transmission enable
        set role lan
        set snmp-index 6
    next
```

- We need to activate the Netflow in the FortiNDR with the next command:



- After this configuration we can see NetFlow traffic in the FortiNDR:



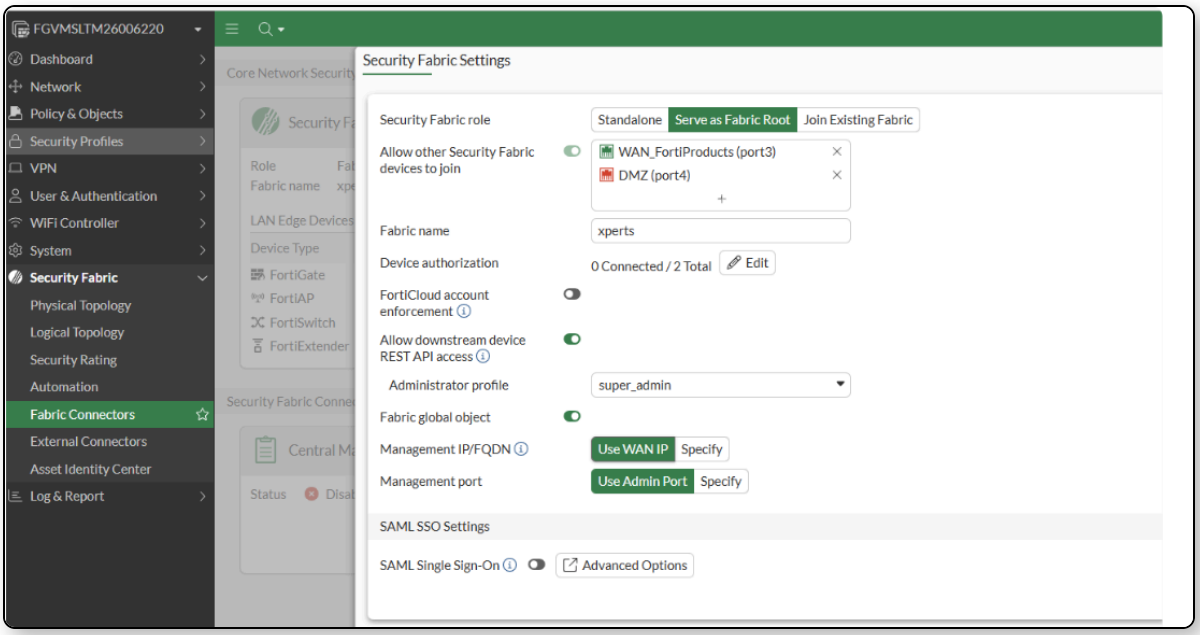


c) Integration from FortiGate with FortiNDR via Security Fabric.

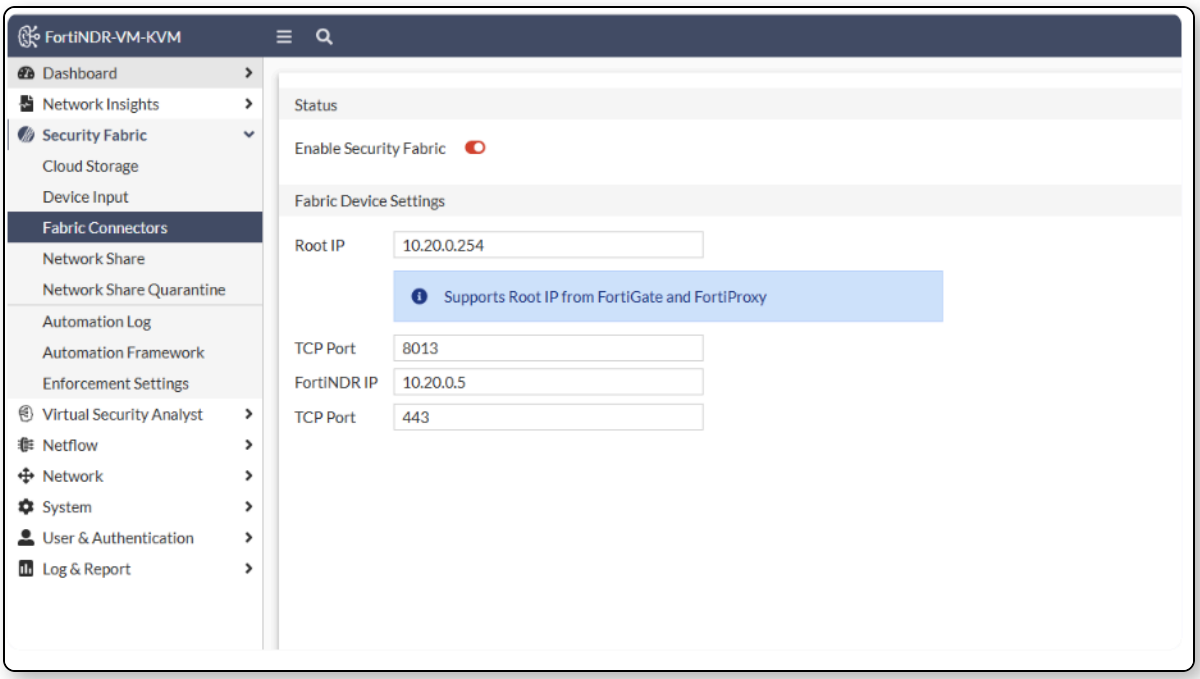
This integration is supported only via “Security Fabric”. We need to configure “Security Fabric” in a FortiGate and integrate the FortiGate Root with FortiNDR.

```
- Important NOTE: In an infrastructure Fortinet with several FortiGates, we need
to configure a "Security Fabric" due we can only integrate one only FortiGate
with the FortiNDR.

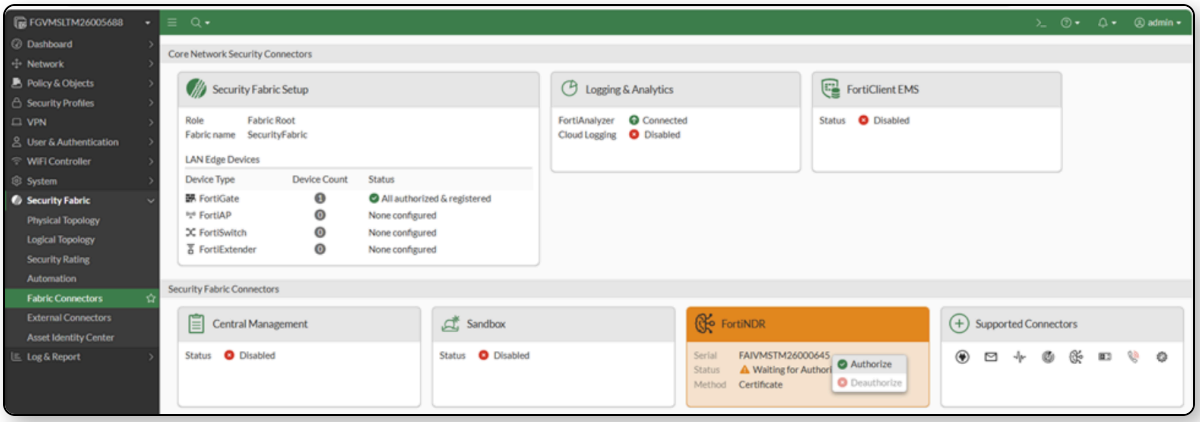
- Let´s configure “Security Fabric” in FortiGate. We are going to access via
HTTPS in FortiGate and let´s do the next configuration.
```



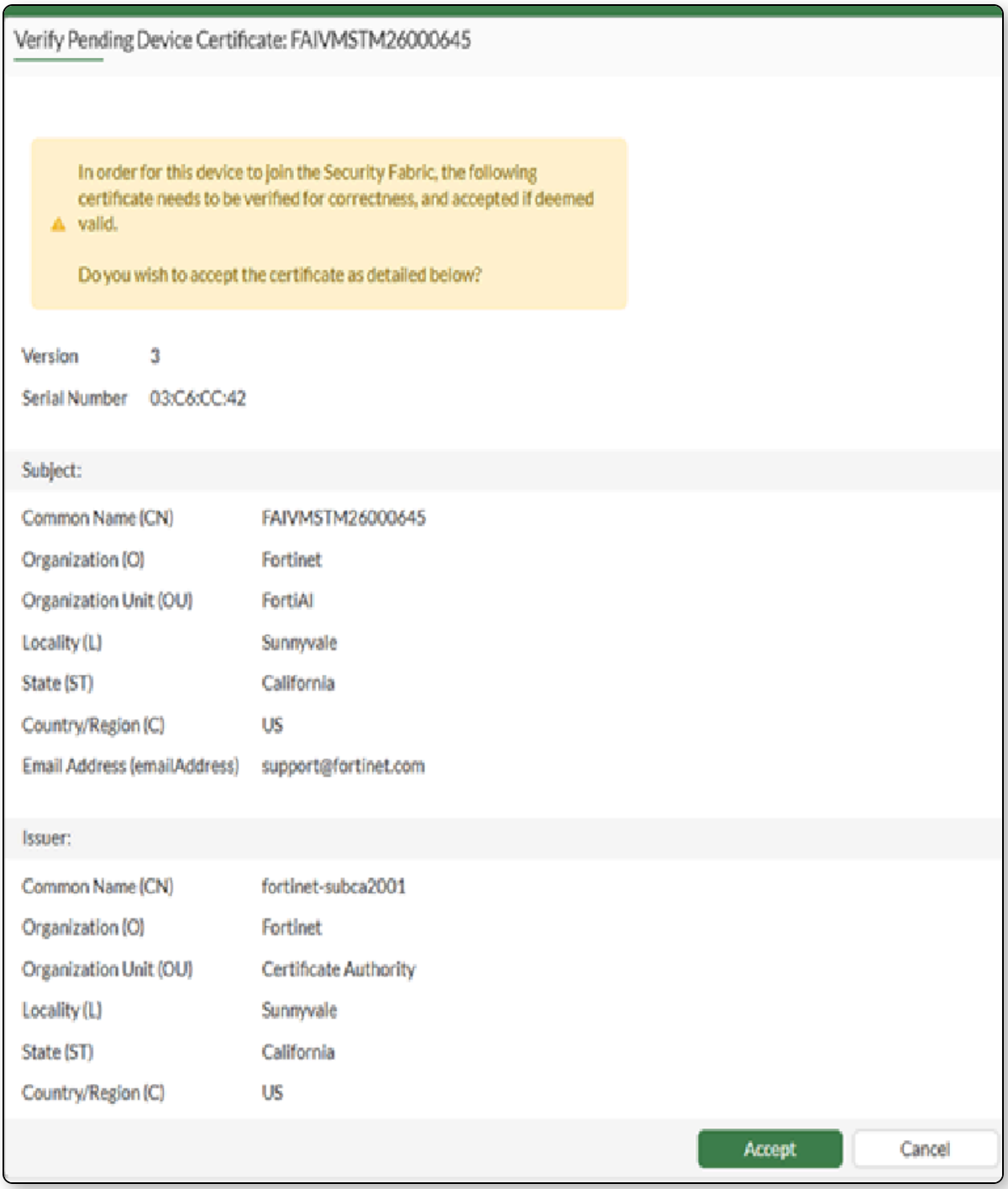
- Let´s go to FortiNDR and we access via HTTPS and let´s activate and configure Fabric Connector in “Security Fabric”.



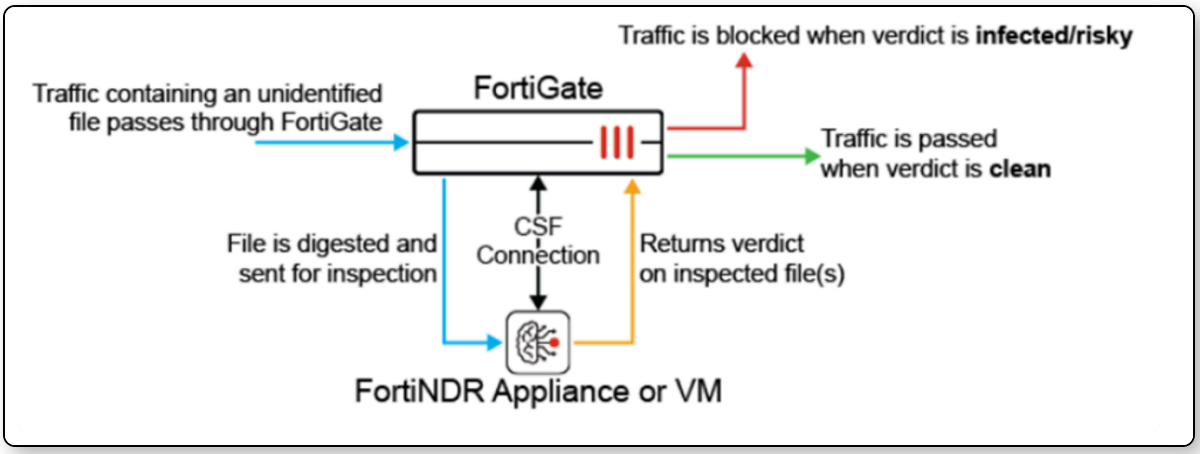
- We need to authorize join this FortiNDR in Security Fabric in the FortiGate. Make sure the “Security Fabric” is allowed in “Port1”.



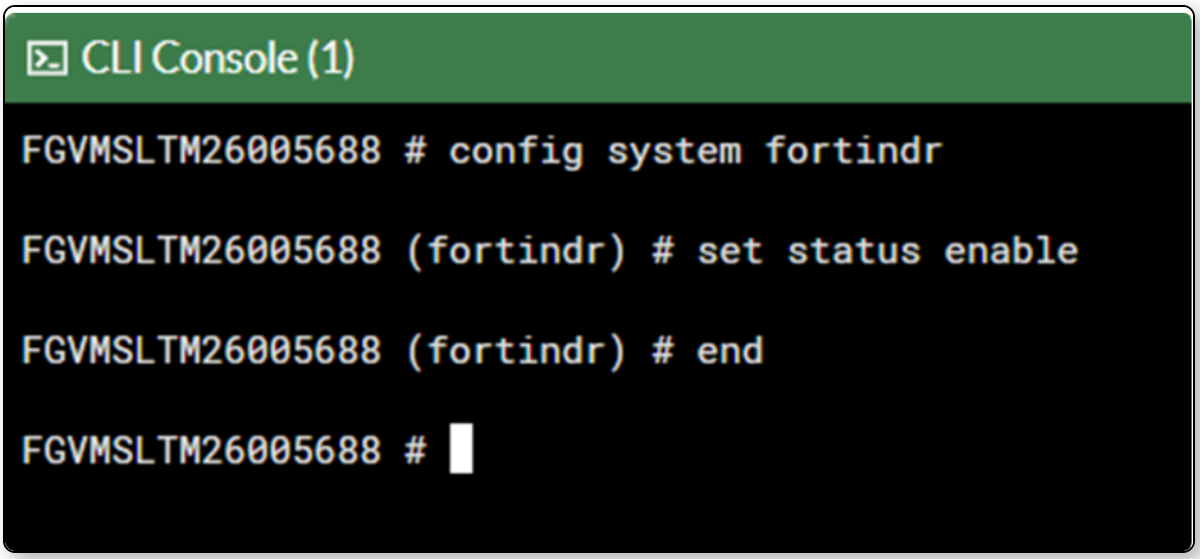
- Accept the certificate.


Verify Pending Device Certificate: FAIVMSTM26000645
In order for this device to join the Security Fabric, the following certificate needs to be verified for correctness, and accepted if deemed valid.
Do you wish to accept the certificate as detailed below?
Version 3
Serial Number 03:C6:CC:42
Subject:
Common Name (CN) FAIVMSTM26000645
Organization (O) Fortinet
Organization Unit (OU) FortiAI
Locality (L) Sunnyvale
State (ST) California
Country/Region (C) US
Email Address (emailAddress) support@fortinet.com
Issuer:
Common Name (CN) fortinet-subca2001
Organization (O) Fortinet
Organization Unit (OU) Certificate Authority
Locality (L) Sunnyvale
State (ST) California
Country/Region (C) US
Accept
Cancel

- Activation FortiNDR Inspection in FortiGate AV Profile. FortiNDR can be used with antivirus profiles in proxy inspection mode (flow mode is currently not supported).
- FortiNDR inspects high-risk files and issues a verdict to the firewall based on how close the file features match those of malware.
- When enabled, FortiNDR can log, block, ignore, or monitor (allow) the file based on the verdict.



- On the FortiOS, enable inline inspection:



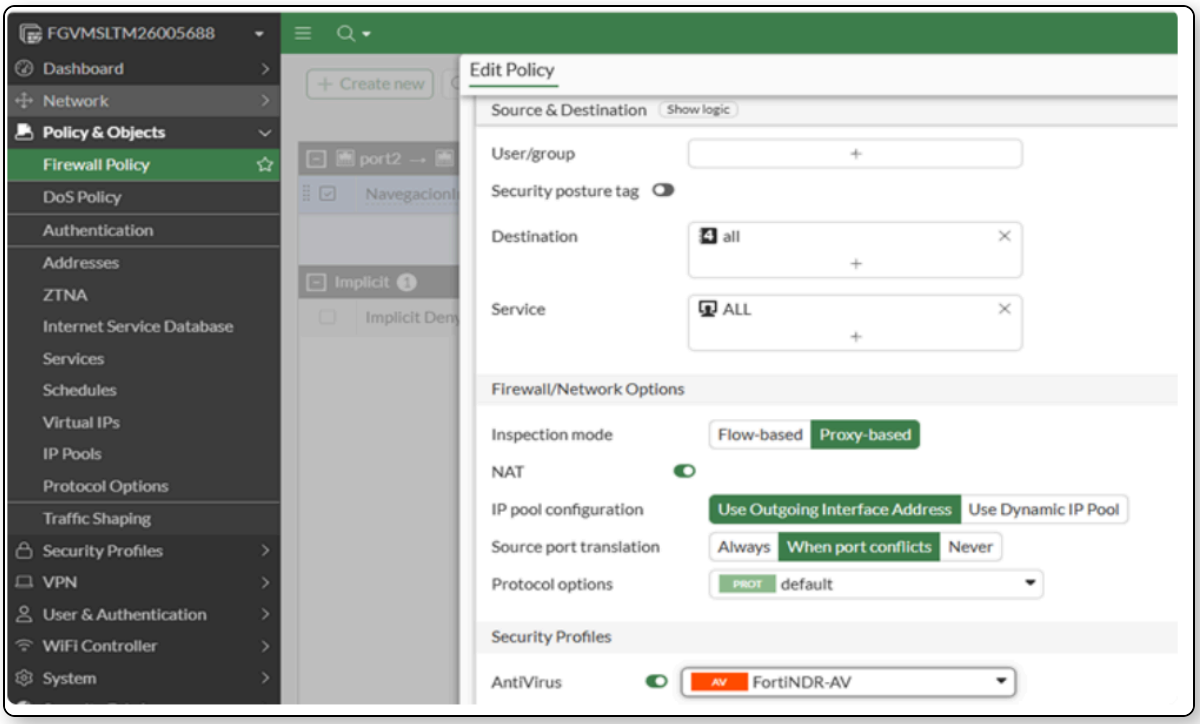
- Configure an antivirus profile to use inline inspection and block detected infections:

```
FGVMSLTM26005688 # config antivirus profile

FGVMSLTM26005688 (profile) #
FGVMSLTM26005688 (profile) # edit FortiNDR-AV

FGVMSLTM26005688 (FortiNDR-AV) # show
config antivirus profile
    edit "FortiNDR-AV"
        set feature-set proxy
        config http
            set fortindr block
        end
        config ftp
            set fortindr block
        end
        config imap
            set fortindr block
        end
        config pop3
            set fortindr block
        end
        config smtp
            set fortindr block
        end
        config mapi
            set fortindr block
        end
        config nntp
            set fortindr block
        end
        config cifs
            set fortindr block
        end
        config ssh
            set fortindr block
        end
    next
end
```

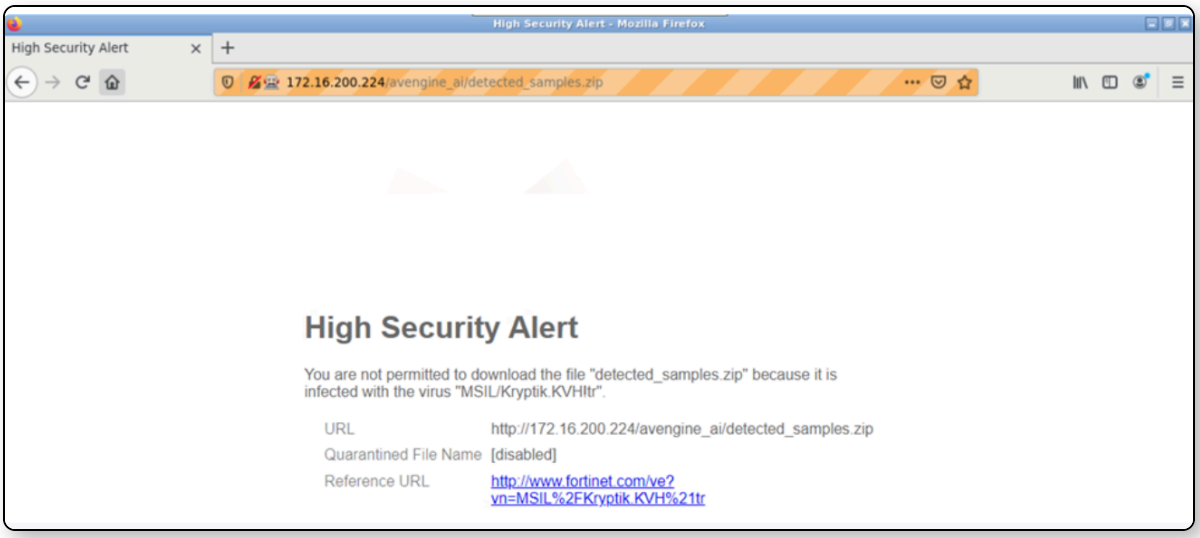
- Config the “set fortindr-error-action block” in the antivirus profile. It is a secure recomendation.
- Add the antivirus profile to a firewall policy that permit traffic between "Victim" and "FileServer".
- If the policy does not exist, please create the policy.



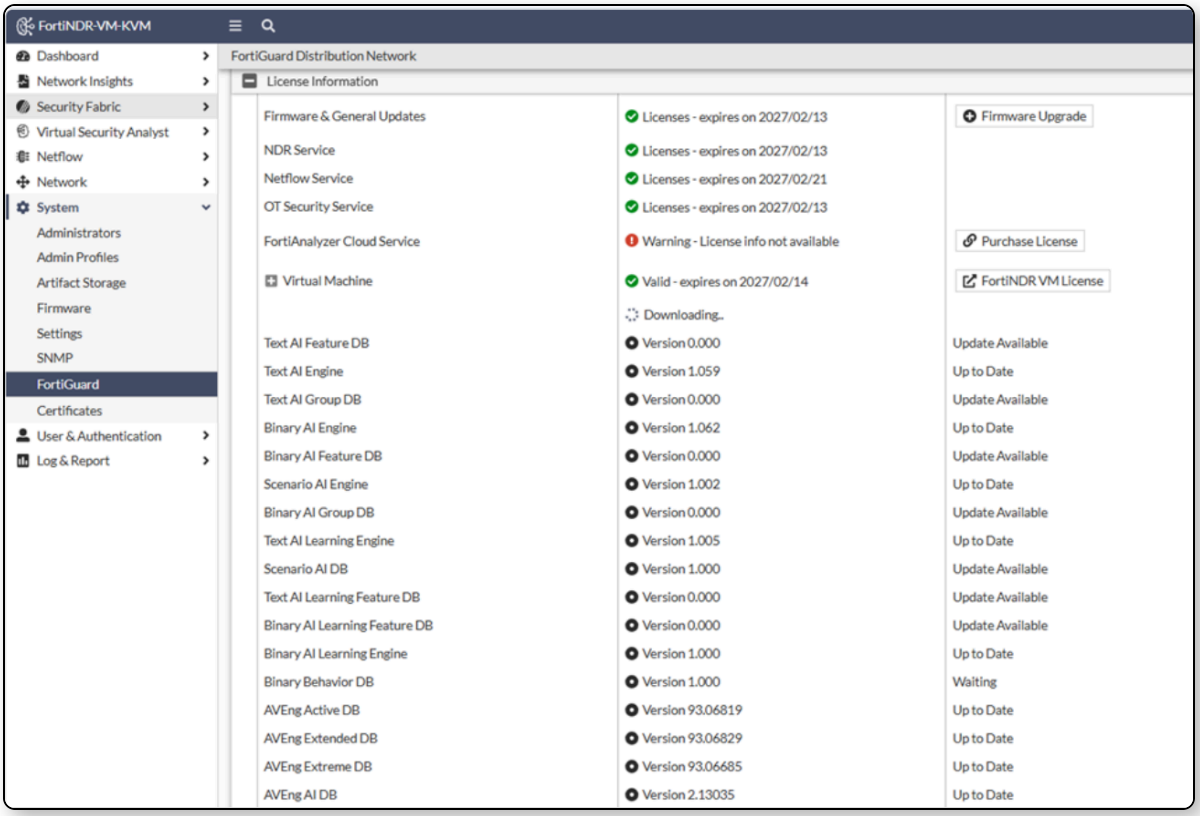
- The next image shows all the kind of files supported for FortiNDR´s inspection.

7Z	HTML	RTF
ARJ	JS	TAR
BZIP	LZH	VBA
BZIP2	LZW	VBS
CAB	MS Office documents (XML and non-XML)	WinPE (EXE)
ELF	PDF	XZ
GZIP	RAR	ZIP

- When potential infections are blocked by FortiNDR inline inspection, a replacement message appears. An infection blocked over HTTP looks similar to the following:

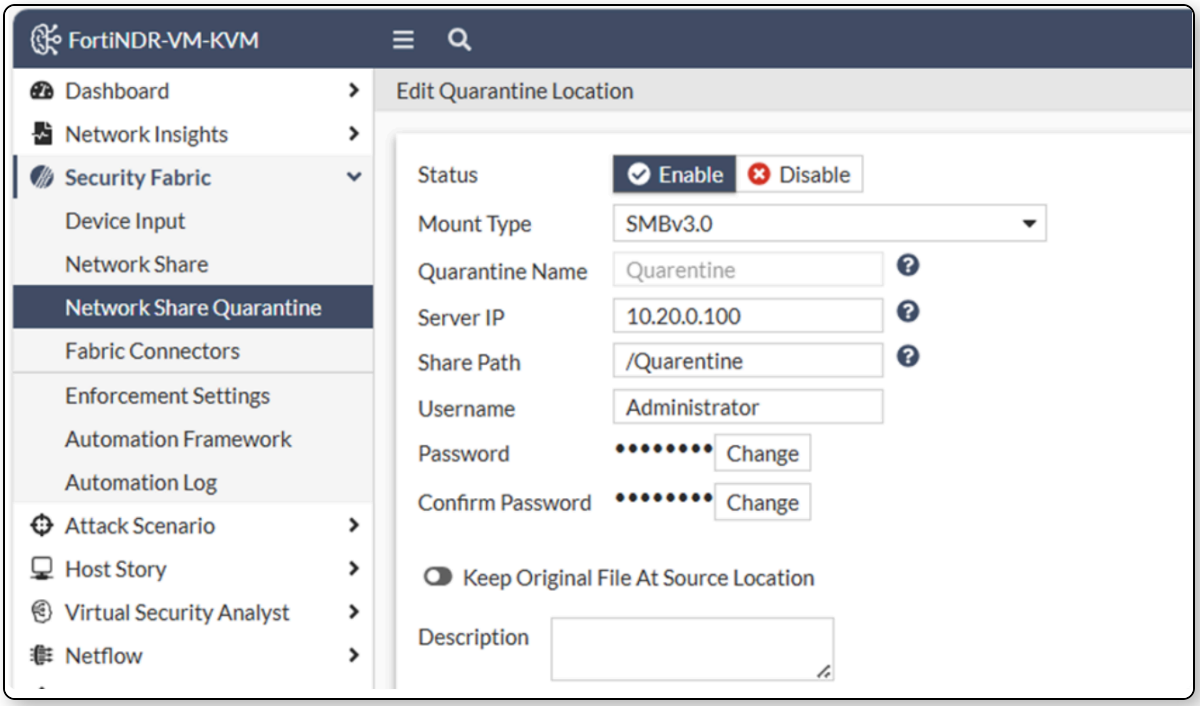


- Please review that the FortiNDR's data base segurity is updated:



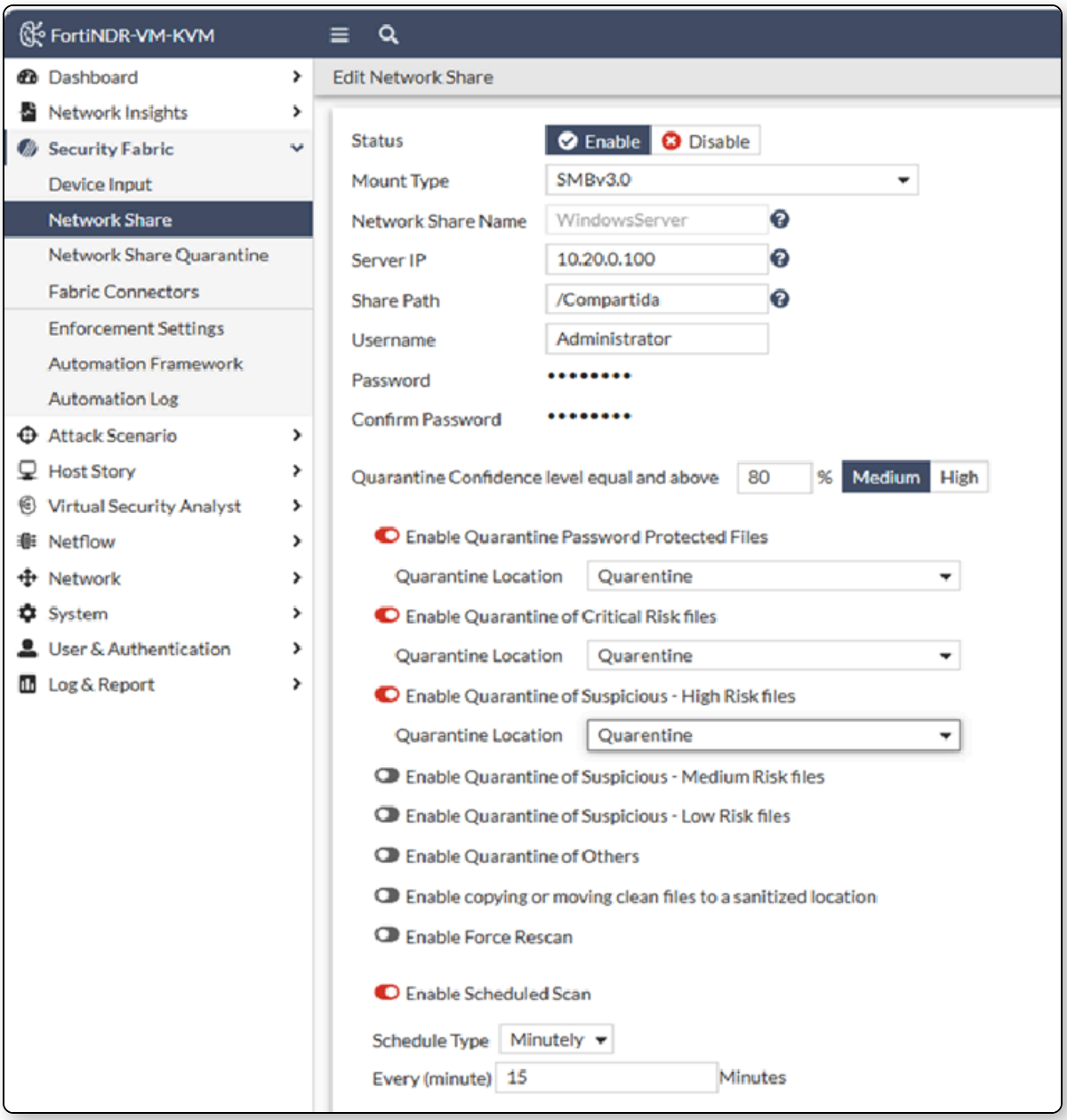
d) FortiNDR Integration with File Server to Advance Analysis of files shares.

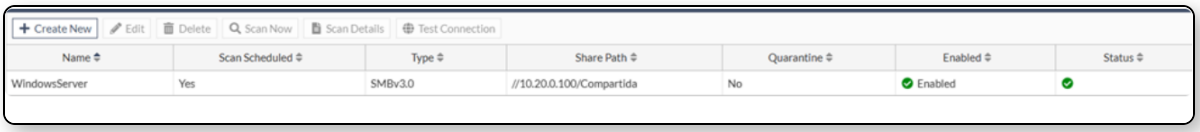
- We need to create and connect the FortiNDR with the quarantine Folder. Where FortiNDR will move suspicious files:





- We need to connect the FortiNDR with the folder that we want to protect. We can do this with the next configuration.


FortiNDR-VM-KVM
Dashboard
Network Insights
Security Fabric
Device Input
Network Share
Network Share Quarantine
Fabric Connectors
Enforcement Settings
Automation Framework
Automation Log
Attack Scenario
Host Story
Virtual Security Analyst
Netflow
Network
System
User & Authentication
Log & Report
Edit Network Share
Status
Enable
Disable
Mount Type
SMBv3.0
Network Share Name
WindowsServer
Server IP
10.20.0.100
Share Path
/Compartida
Username
Administrator
Password
Confirm Password
Quarantine Confidence level equal and above
80
%
Medium
High
Enable Quarantine Password Protected Files
Quarantine Location
Quarantine
Enable Quarantine of Critical Risk files
Quarantine Location
Quarantine
Enable Quarantine of Suspicious - High Risk files
Quarantine Location
Quarantine
Enable Quarantine of Suspicious - Medium Risk files
Enable Quarantine of Suspicious - Low Risk files
Enable Quarantine of Others
Enable copying or moving clean files to a sanitized location
Enable Force Rescan
Enable Scheduled Scan
Schedule Type
Minutely
Every (minute)
15
Minutes


Create New
Edit
Delete
Scan Now
Scan Details
Test Connection
Name
Scan Scheduled
Type
Share Path
Quarantine
Enabled
Status
WindowsServer
Yes
SMBv3.0
//10.20.0.100/Compartida
No
Enabled

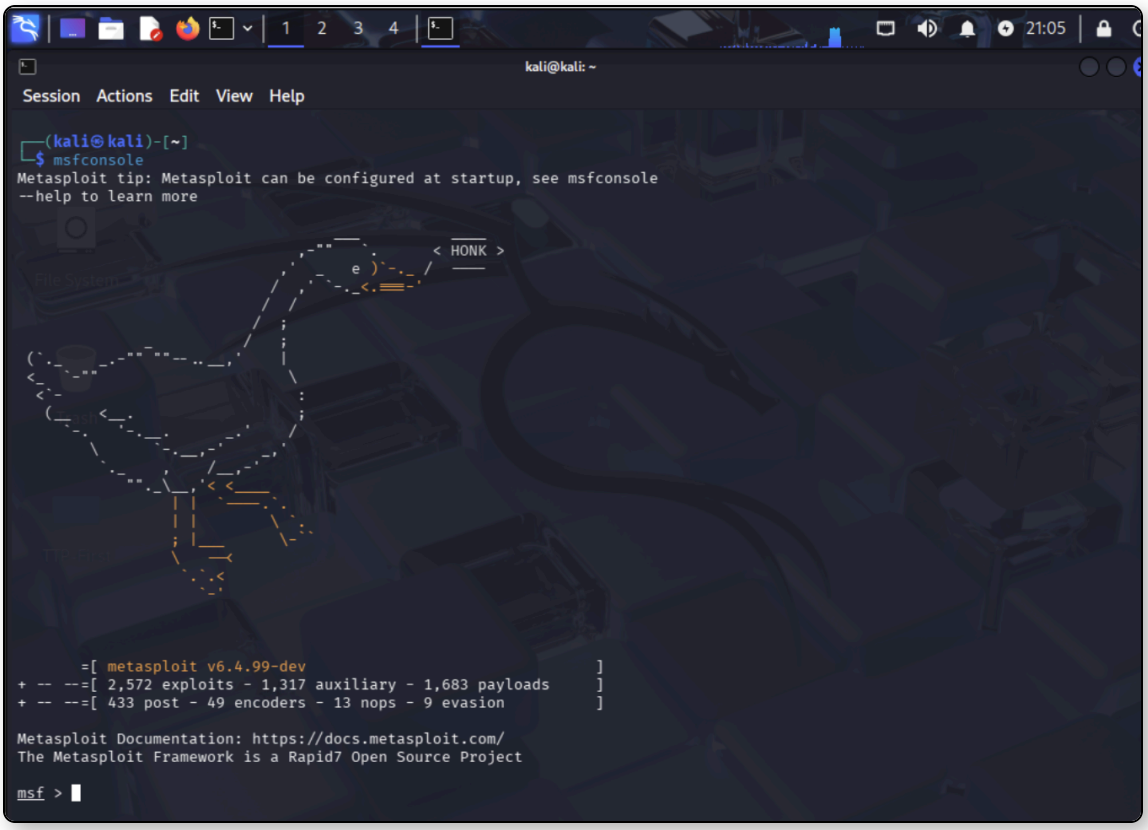
Lab02 Internal Suspicious Activities

LABORATORY 2: Internal Suspicious Activities:

In this lab, we will perform several activities like those an attacker would carry out on the internal network. The goal is to generate traffic and detections by security solutions for later use in the lab, either as a response from FortiSOAR or for analysis by FortiAnalyzer.

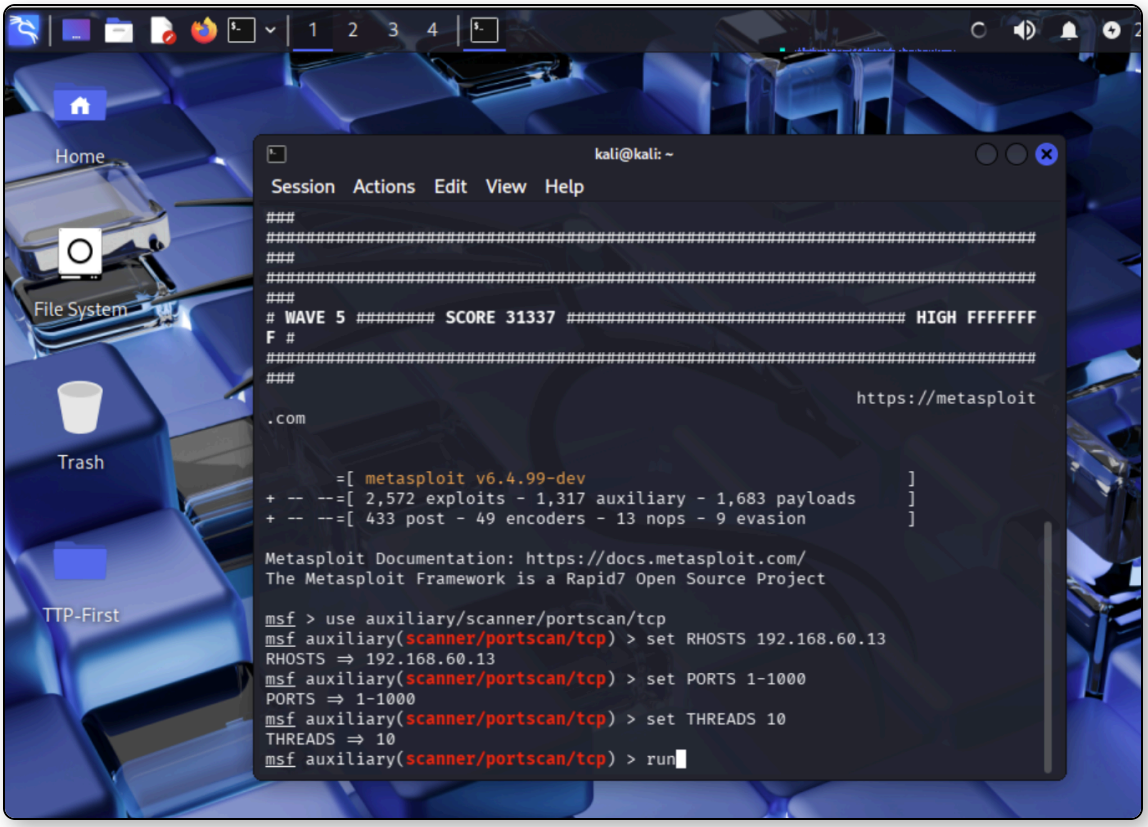
a) Internal Port Scan.

- We need to access in the “Attack” devices (Kali Linux or Debian) via “Display”.
- We should open “Metasploit” executing the next command in a terminal application: "msfconsole"



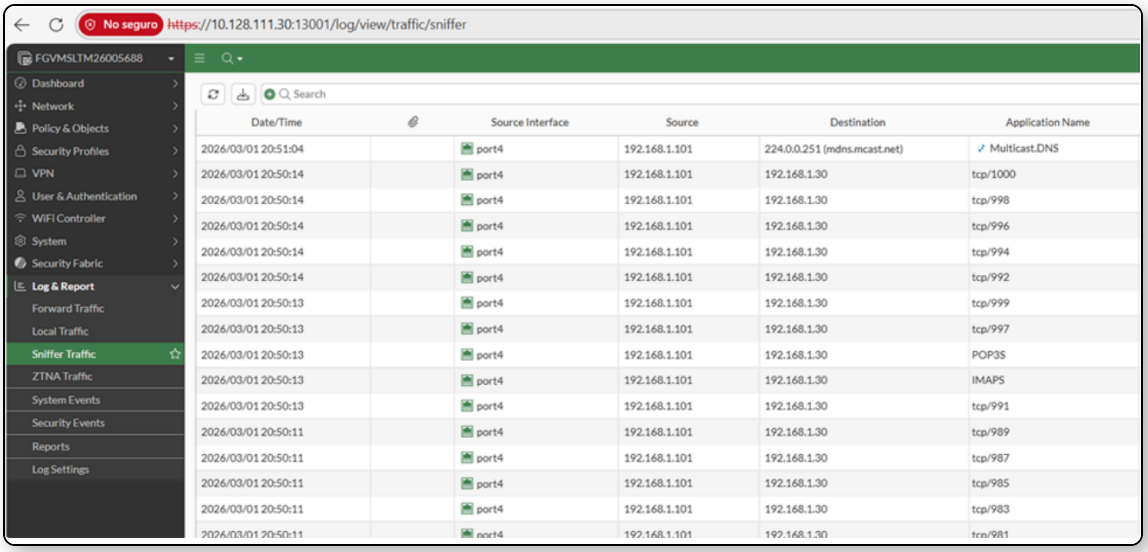
- Let´s go to use the Auxiliary modulo “Portscan” to execute a port scan to “ClienteWindows” with IP 192.168.60.13.
- We need to configure the module with the next commands:

    - use auxiliary/scanner/portscan/tcp
    - set RHOST 192.168.60.13
    - set PORTS 1-1000
    - set THREADS 10
- For execute this modulo, we need to lunch the next command: "run"



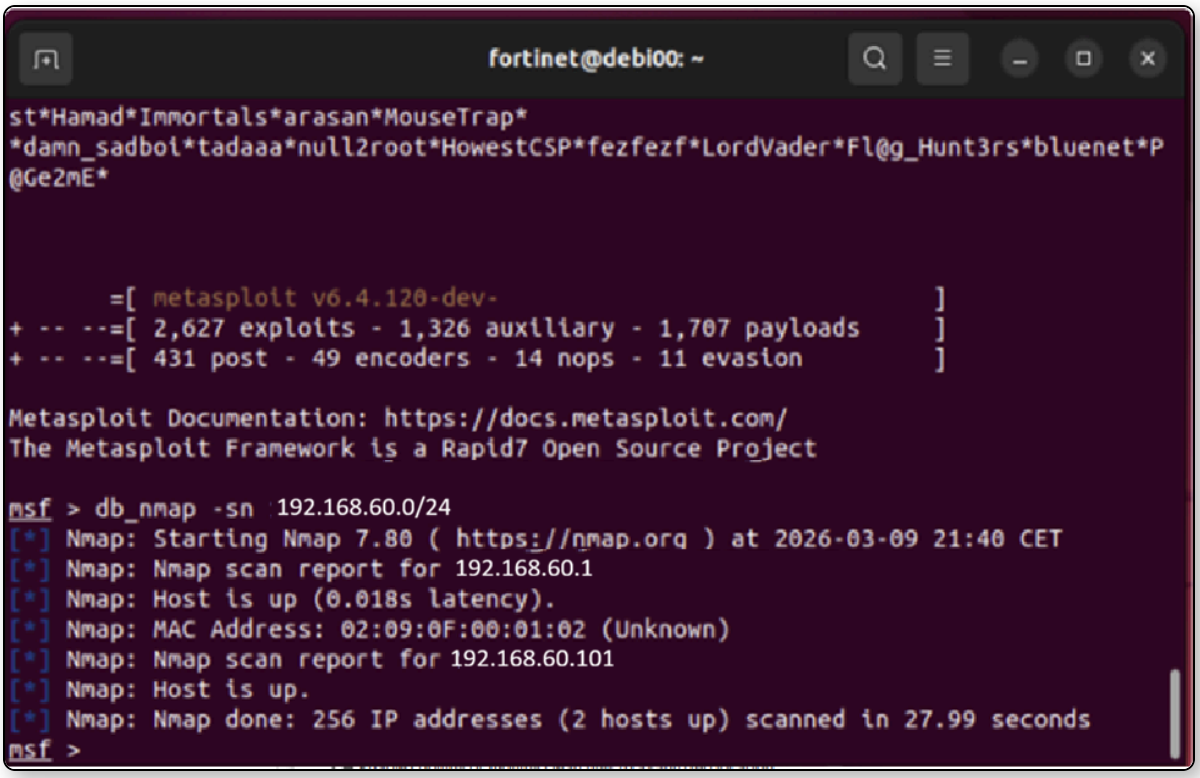
- You can observe sniffed traffic similar to that shown in the following image.

- Your IP addressing must be associated with the 192.168.60.0/24 segment.



b) Network scan with Nmap.

In the “msfconsole” we can use “Nmap” to do a network scan executing the next command: "db_nmap -sn 192.168.60.0/24"

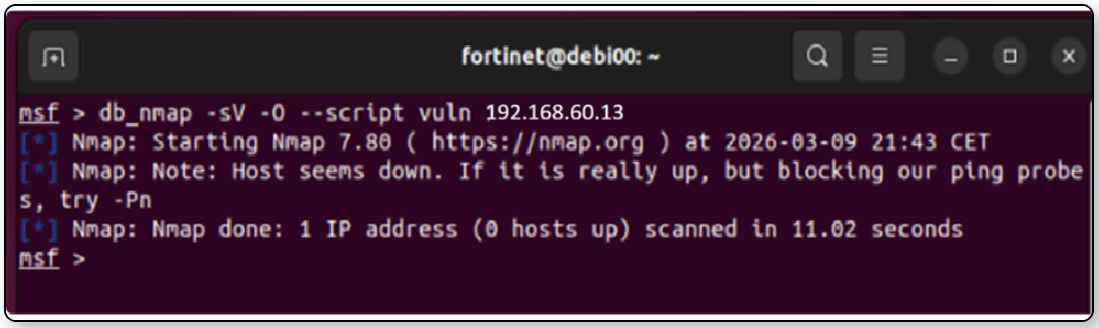


If you has issues with database connet, try the next: - sudo msfdb delete - sudo msfdb init - sudo msfconsole

c) Vulnerability Analysis with Metasploit.

Let's perform a scan with db_nmap (the most common method). Metasploit allows you to use Nmap directly to detect services and versions. By using the db_ prefix, the results are saved to the internal database, allowing you to query potential vulnerabilities later.

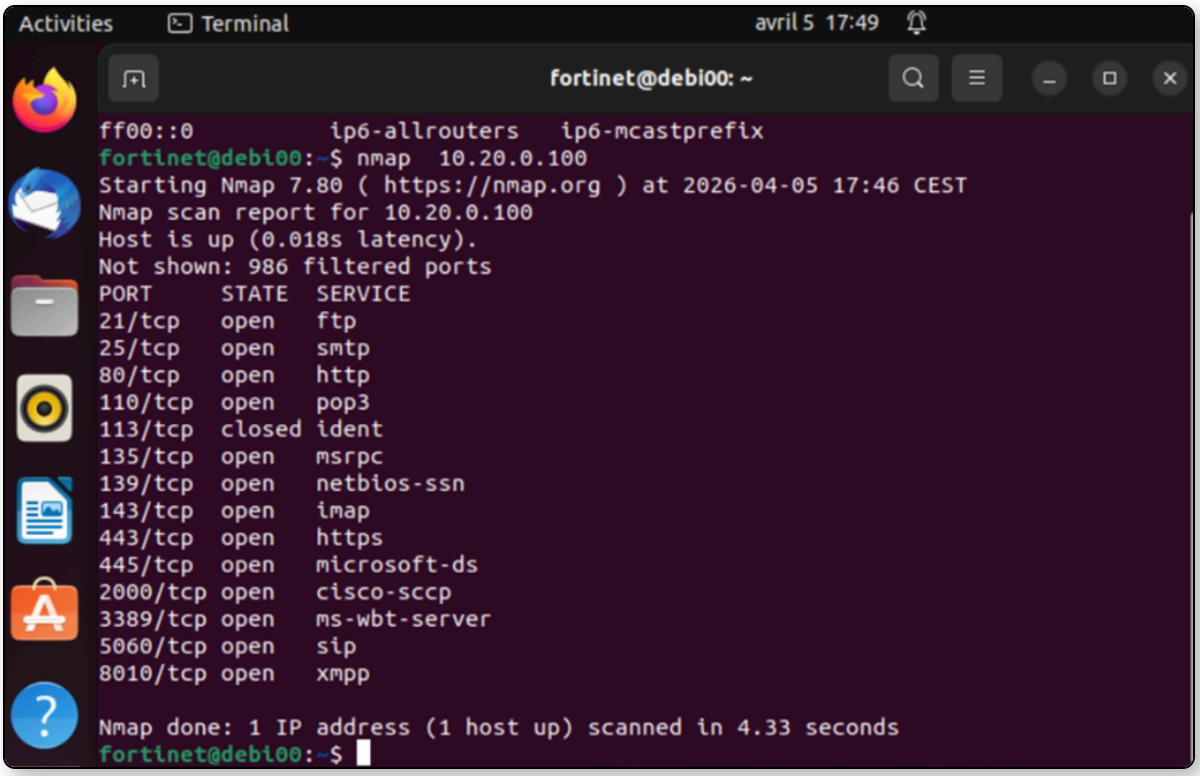
- The command that we need to use is: "db_nmap -sV -O --script vuln 192.168.60.13"
  - sV: Detects service versions.
  - -O: Attempts to identify the operating system.
  - --script vuln: Runs specific Nmap scripts to scan for known vulnerabilities.
  - We need to execute this command in root privileges.



- We can execute this command to evaluate the file server with IP 10.20.0.100: "db_nmap -sV -O --script vuln 10.20.0.100".

d) Execute a nmap with Linux

Exit from Metasploit and in a CMD in linux we can execute a nmap to file server.



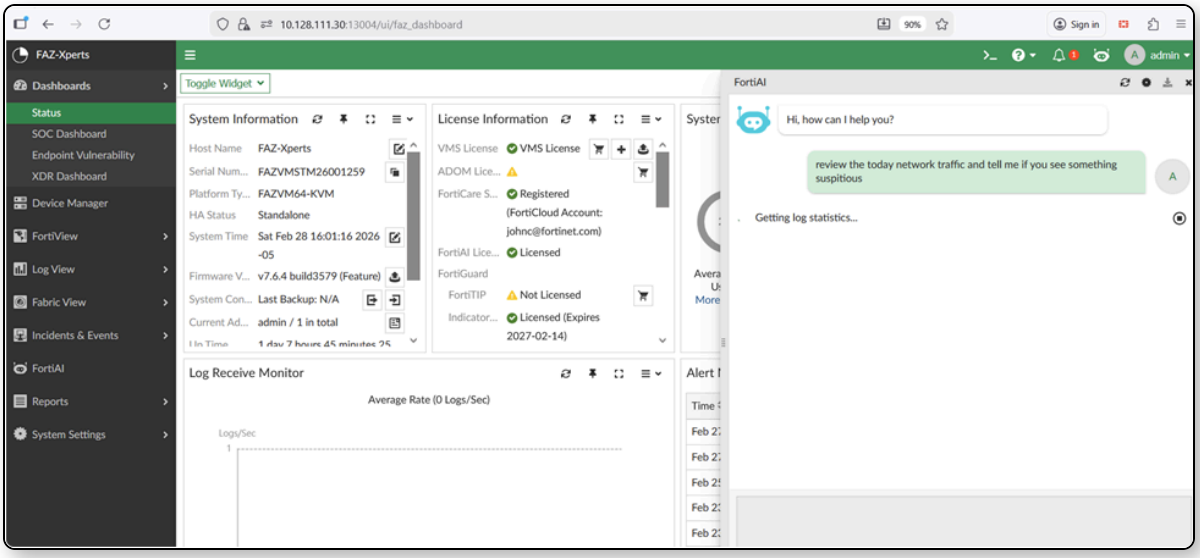
Lab03 Analysis of Anomalies Supported by FortiAI

LABORATORY 3: Investigation of anomalies Supported by FortiAI.

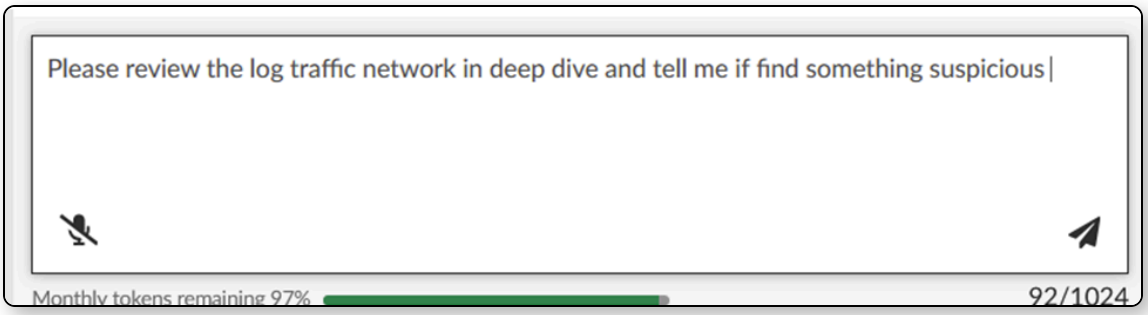
We will use FortiAI from FortiAnalyzer to generate forensic investigations, demonstrating how easy it is to conduct these investigations with the support of FortiAI.

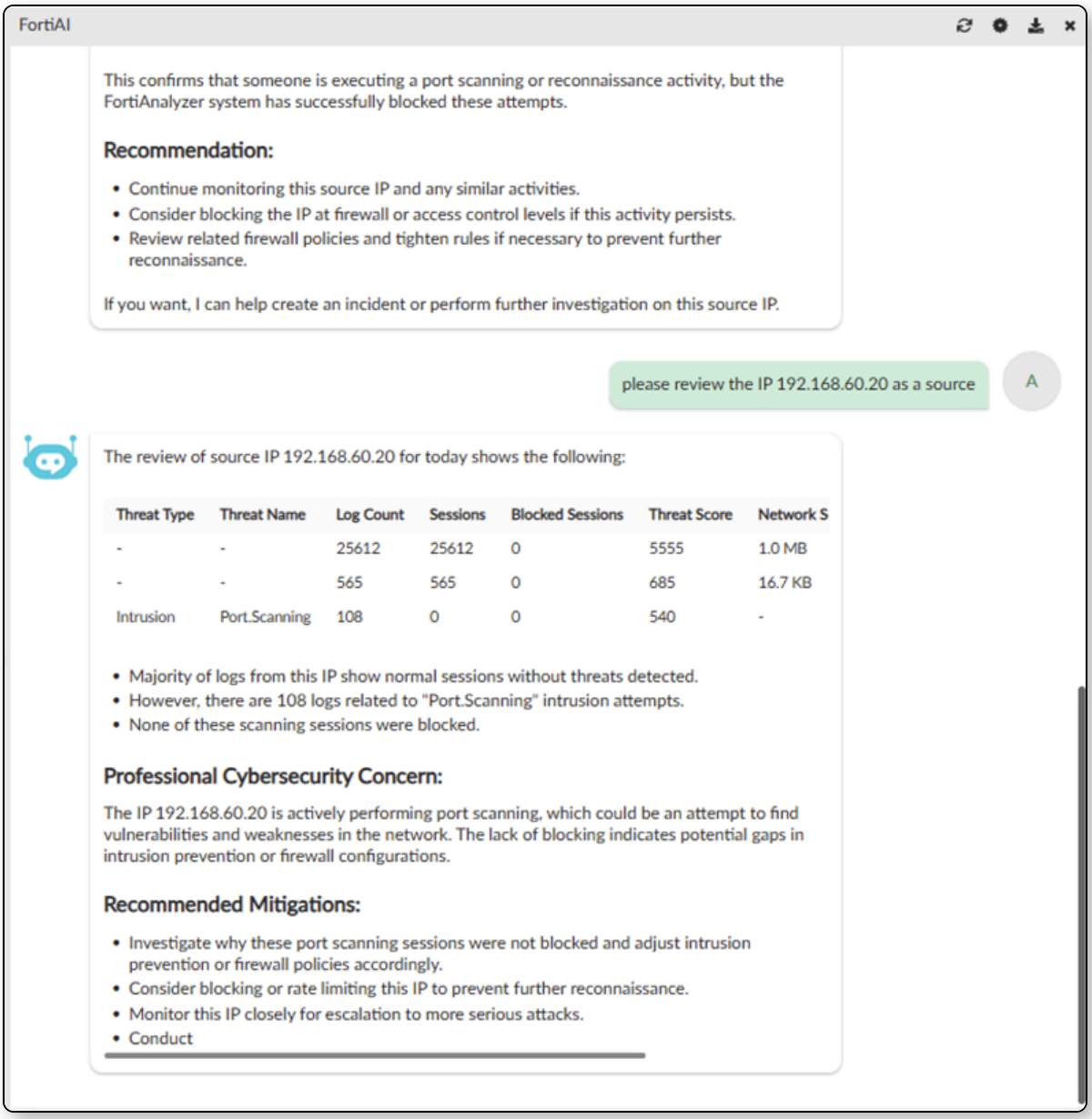
a) Let´s do an investigation supported by FortiAI about suspicious traffic.

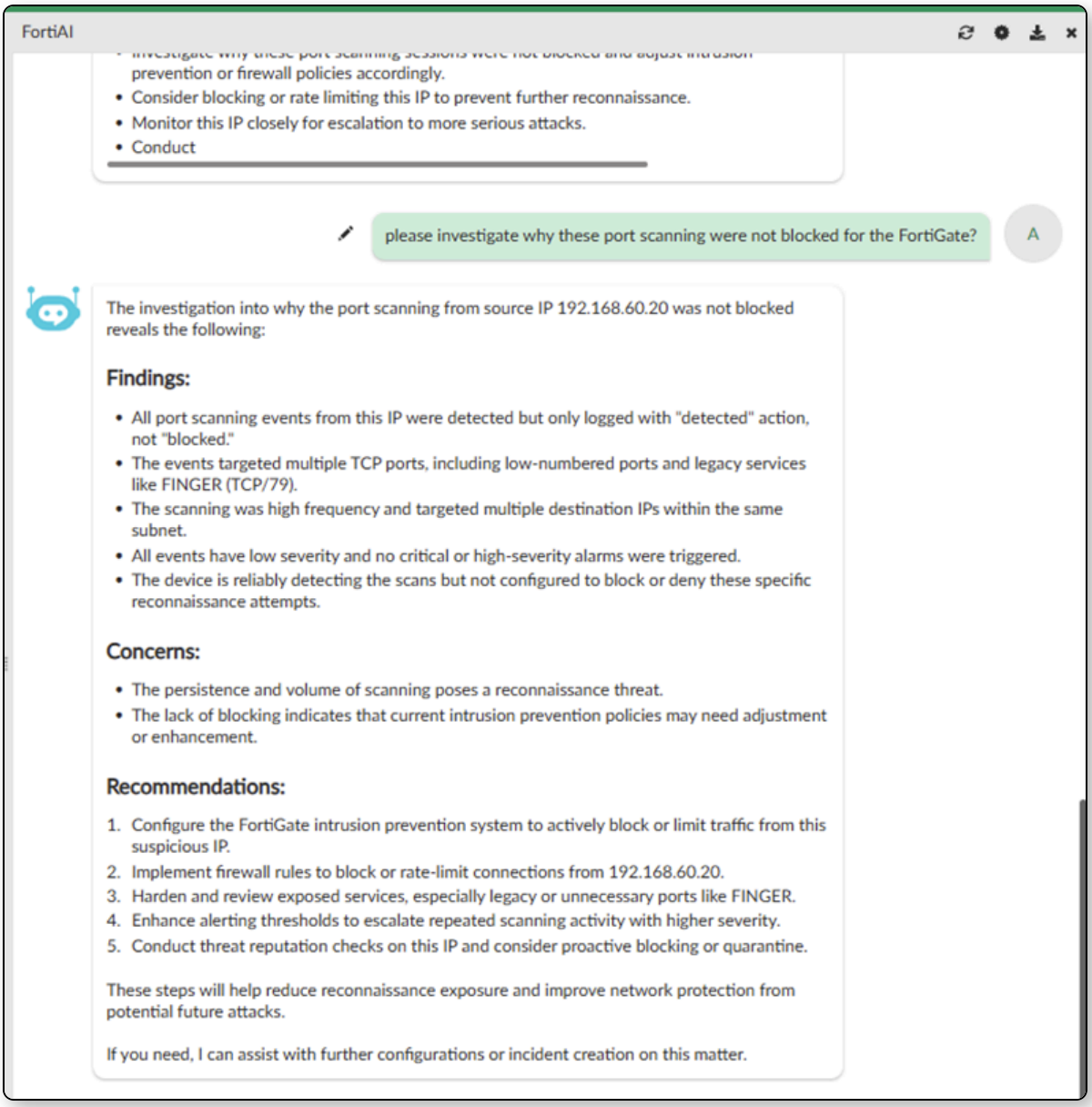
We are going to the FortiAnalyzer (Via HTTPS) and do click in FortiAI, let´s do ask for suspicious network traffic.



- We should review the information that FortiAI give us, and we ask to review deep dive.




FortiAI
This confirms that someone is executing a port scanning or reconnaissance activity, but the FortiAnalyzer system has successfully blocked these attempts.
Recommendation:
• Continue monitoring this source IP and any similar activities.
• Consider blocking the IP at firewall or access control levels if this activity persists.
• Review related firewall policies and tighten rules if necessary to prevent further reconnaissance.
If you want, I can help create an incident or perform further investigation on this source IP.
please review the IP 192.168.60.20 as a source
A
The review of source IP 192.168.60.20 for today shows the following:
Threat Type Threat Name Log Count Sessions Blocked Sessions Threat Score Network S
- - 25612 25612 0 5555 1.0 MB
- - 565 565 0 685 16.7 KB
Intrusion Port.Scanning 108 0 0 540 -
• Majority of logs from this IP show normal sessions without threats detected.
• However, there are 108 logs related to "Port.Scanning" intrusion attempts.
• None of these scanning sessions were blocked.
Professional Cybersecurity Concern:
The IP 192.168.60.20 is actively performing port scanning, which could be an attempt to find vulnerabilities and weaknesses in the network. The lack of blocking indicates potential gaps in intrusion prevention or firewall configurations.
Recommended Mitigations:
• Investigate why these port scanning sessions were not blocked and adjust intrusion prevention or firewall policies accordingly.
• Consider blocking or rate limiting this IP to prevent further reconnaissance.
• Monitor this IP closely for escalation to more serious attacks.
• Conduct



- FortiAI suggest analyzing internal endpoint (The IP could be different for others lab), we can say yes. The result is:

FortiAI

Review of the IP 192.168.1.101 shows:

- The security reputation check returned no data, which means no clear threat intel on this IP in the current reputation system.
- Network traffic from this IP today targeted multiple destination IPs internally and externally.

Top destination IPs accessed from 192.168.1.101 include:

Destination IP	Log Count	Sessions	Blocked Sessions	Ne
192.168.1.30 (internal?)	2004	2002	0	5.8
8.8.8.8	316	283	0	22.
224.0.0.251	40	20	0	3.9
Several others with fewer connections but consistent activity	Various	Various	0	Sm

Concerns:

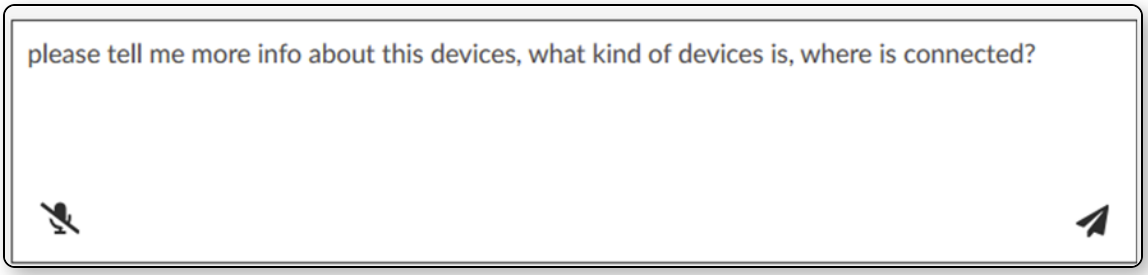
- This source IP is involved in many connection attempts to varied destinations, mostly without blockage.
- The predominance of session counts to an internal-looking IP 192.168.1.30 suggests possible internal reconnaissance or lateral movement attempts.
- Lack of blocked sessions from this IP indicates possible gaps in prevention or policy configuration.

Recommendations:

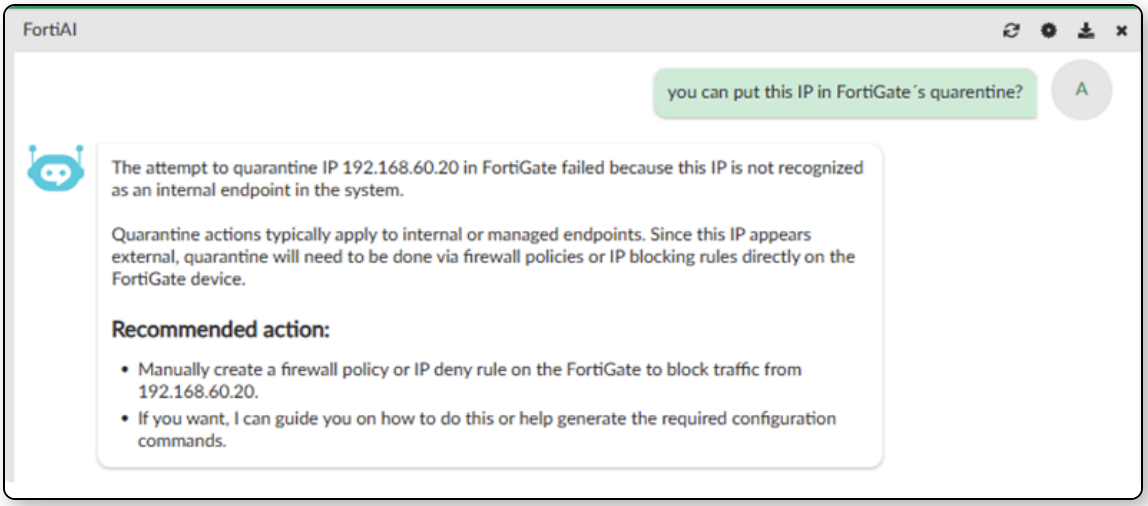
- Immediately block or quarantine the source IP 192.168.1.101 to halt ongoing suspicious activity.
- Conduct endpoint investigation on internal server at 192.168.1.30 for signs of compromise or intrusion.
- Review firewall and IPS rules to ensure this behavior is monitored and mitigated.
- Consider enabling stricter access policies and anomaly detection around these endpoints.

If you want, I can help you create a security incident report or proceed to quarantine the suspicious IP.

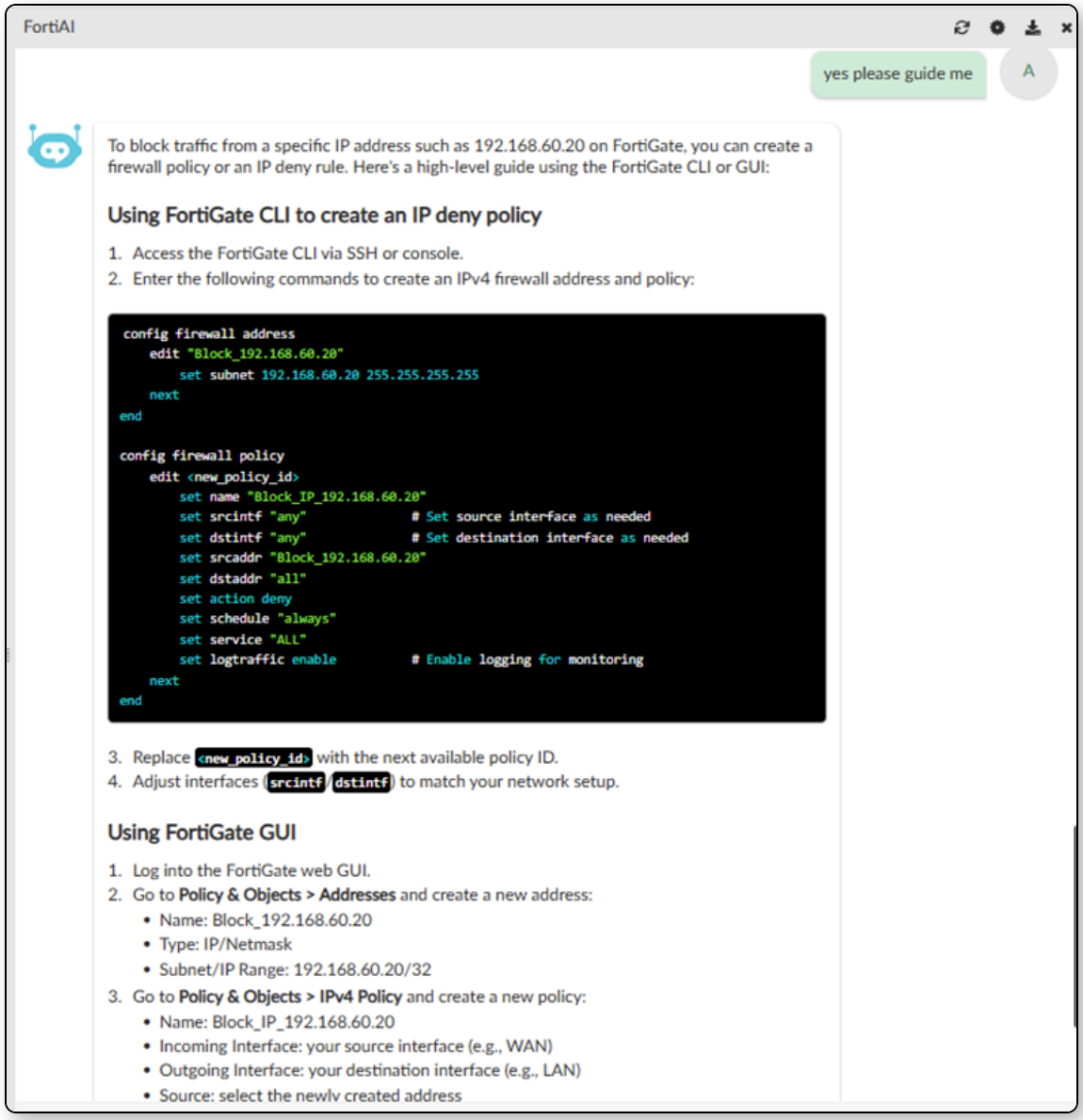
- We can ask for more details!!



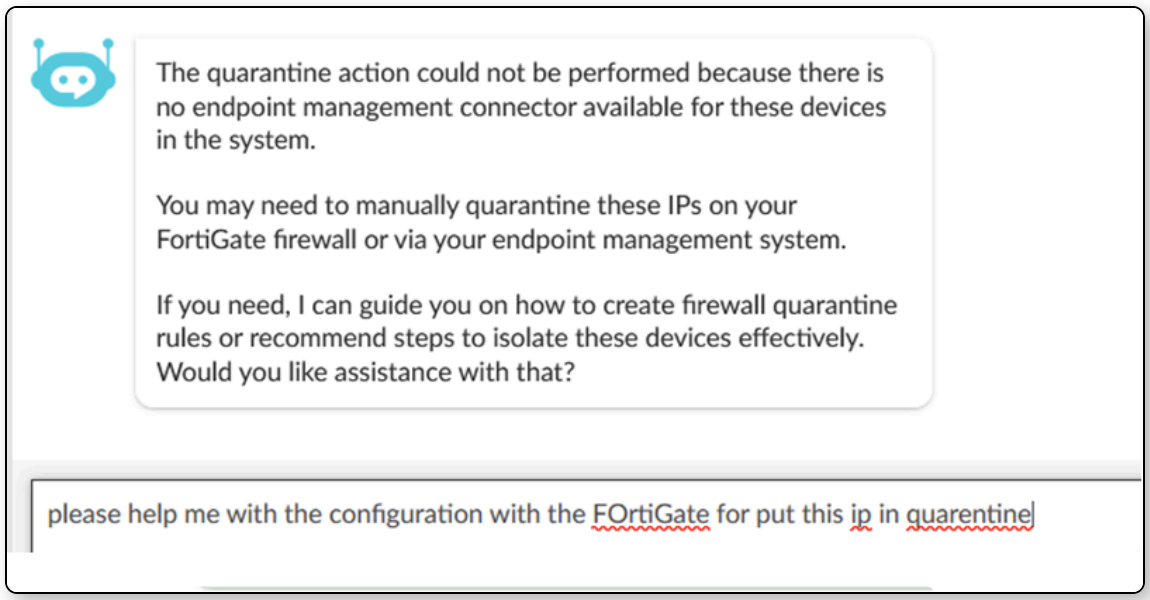
- We can ask for put this suspicious device in quarantine in the FortiGate:



- You can ask to FortAI to guide you as quarentine this IP:



- We need some configurations to do this, if we do not have this, FortiAI can help us:



To quarantine or block specific IP addresses on FortiGate firewall, you typically create a firewall policy or address object to block or restrict traffic from/to those IPs.

Here is a high-level CLI example to block IP 192.168.1.101 and 192.168.1.30 on FortiGate:

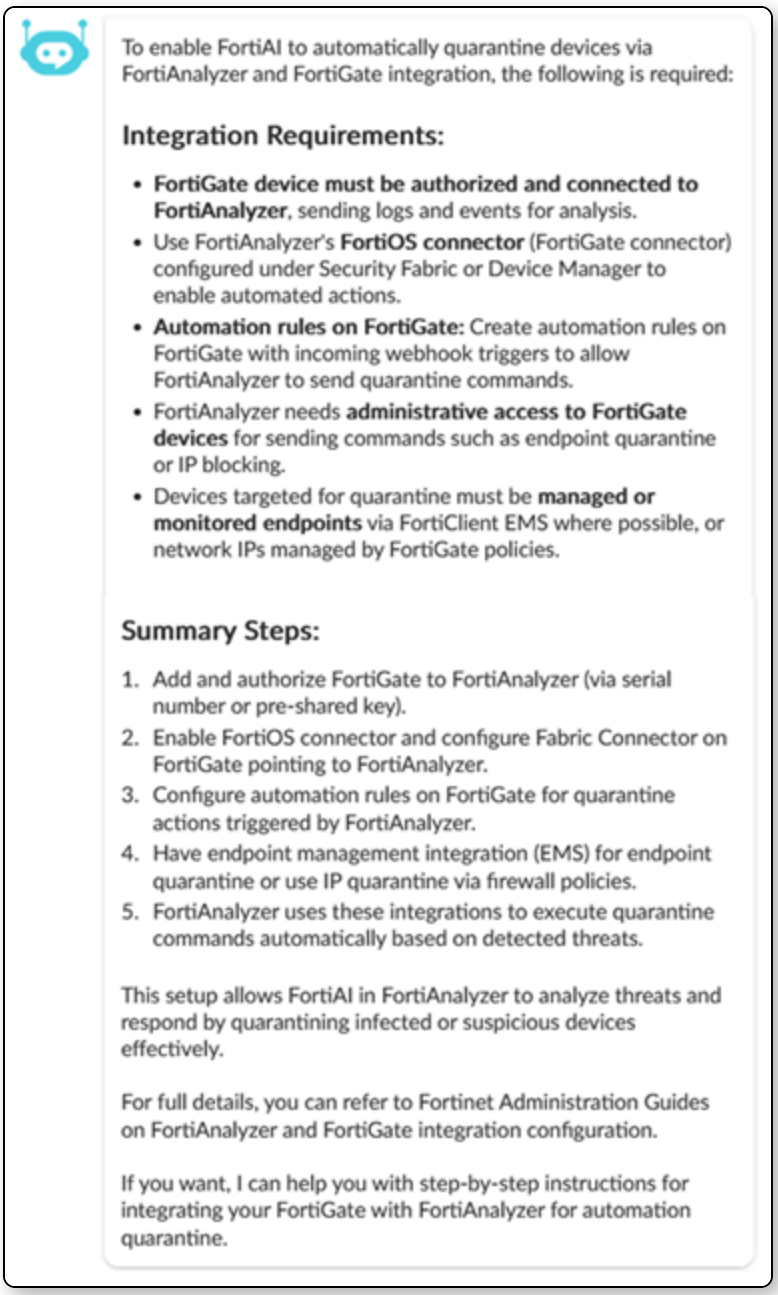
```
# Configure IP address objects for quarantine
config firewall address
    edit "quarantine-198-182-19-109"
        set subnet 192.168.1.101 255.255.255.255
    next
    edit "quarantine-198-182-19-119"
        set subnet 192.168.1.30 255.255.255.255
    next
end

# Create firewall policy to deny traffic from these addresses (
config firewall policy
    edit 0
        set name "block_suspicious_ips"
        set srcintf "any"
        set dstintf "any"
        set srcaddr "quarantine-198-182-19-109" "quarantine-198
        set action deny
        set schedule "always"
        set service "ALL"
        set logtraffic all
```

- We can ask for more help.

What integration between FortiAnalyzer and FortiGate do I need to do for you FortiAI can do this quarantine?

- For these automations you can use “Automations Stich”. If you have time, you can do it!!



To enable FortiAI to automatically quarantine devices via FortiAnalyzer and FortiGate integration, the following is required:

Integration Requirements:

- **FortiGate device must be authorized and connected to FortiAnalyzer**, sending logs and events for analysis.
- Use FortiAnalyzer's **FortiOS connector** (FortiGate connector) configured under Security Fabric or Device Manager to enable automated actions.
- **Automation rules on FortiGate:** Create automation rules on FortiGate with incoming webhook triggers to allow FortiAnalyzer to send quarantine commands.
- FortiAnalyzer needs **administrative access to FortiGate devices** for sending commands such as endpoint quarantine or IP blocking.
- Devices targeted for quarantine must be **managed or monitored endpoints** via FortiClient EMS where possible, or network IPs managed by FortiGate policies.

Summary Steps:

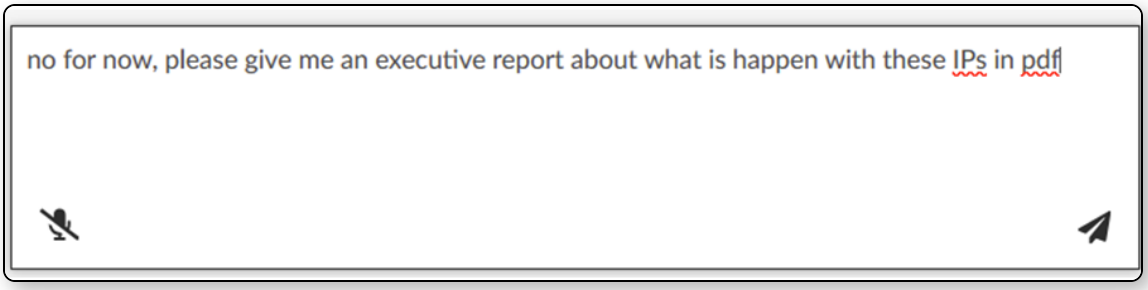
1. Add and authorize FortiGate to FortiAnalyzer (via serial number or pre-shared key).
2. Enable FortiOS connector and configure Fabric Connector on FortiGate pointing to FortiAnalyzer.
3. Configure automation rules on FortiGate for quarantine actions triggered by FortiAnalyzer.
4. Have endpoint management integration (EMS) for endpoint quarantine or use IP quarantine via firewall policies.
5. FortiAnalyzer uses these integrations to execute quarantine commands automatically based on detected threats.

This setup allows FortiAI in FortiAnalyzer to analyze threats and respond by quarantining infected or suspicious devices effectively.

For full details, you can refer to Fortinet Administration Guides on FortiAnalyzer and FortiGate integration configuration.

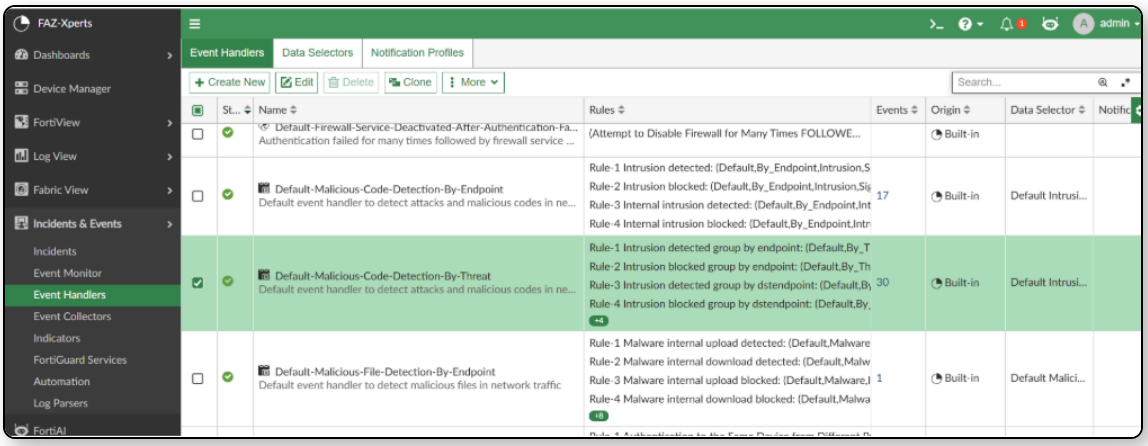
If you want, I can help you with step-by-step instructions for integrating your FortiGate with FortiAnalyzer for automation quarantine.

- We can ask for a executive report in PDF format!!

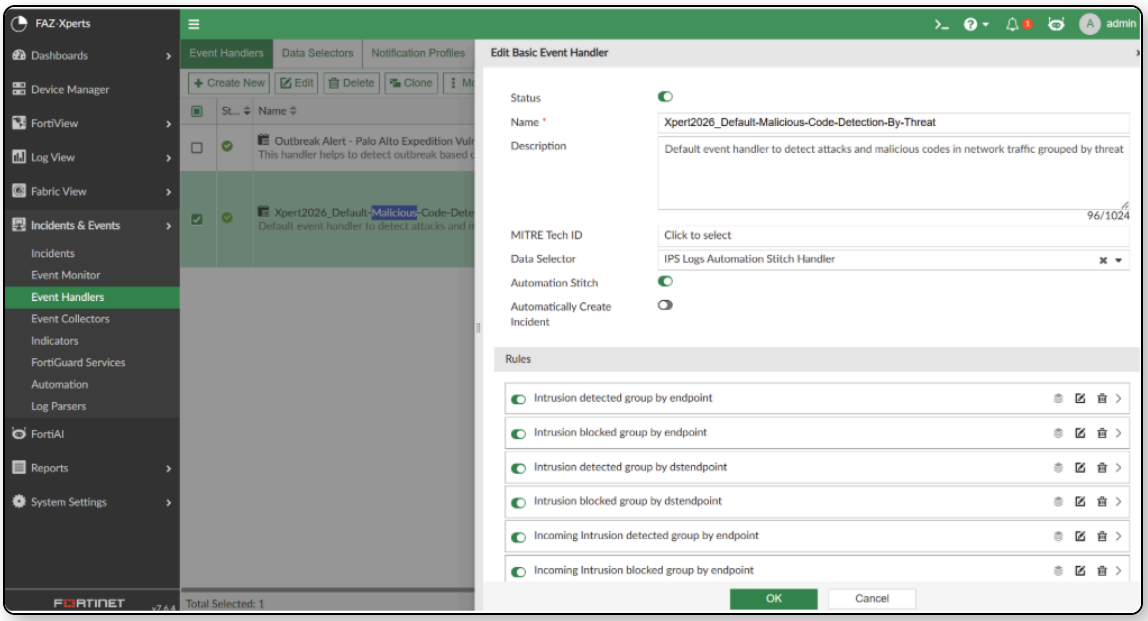


b) Let’s do a create an Automatic Response between FortiGate & FortiAnalyzer.

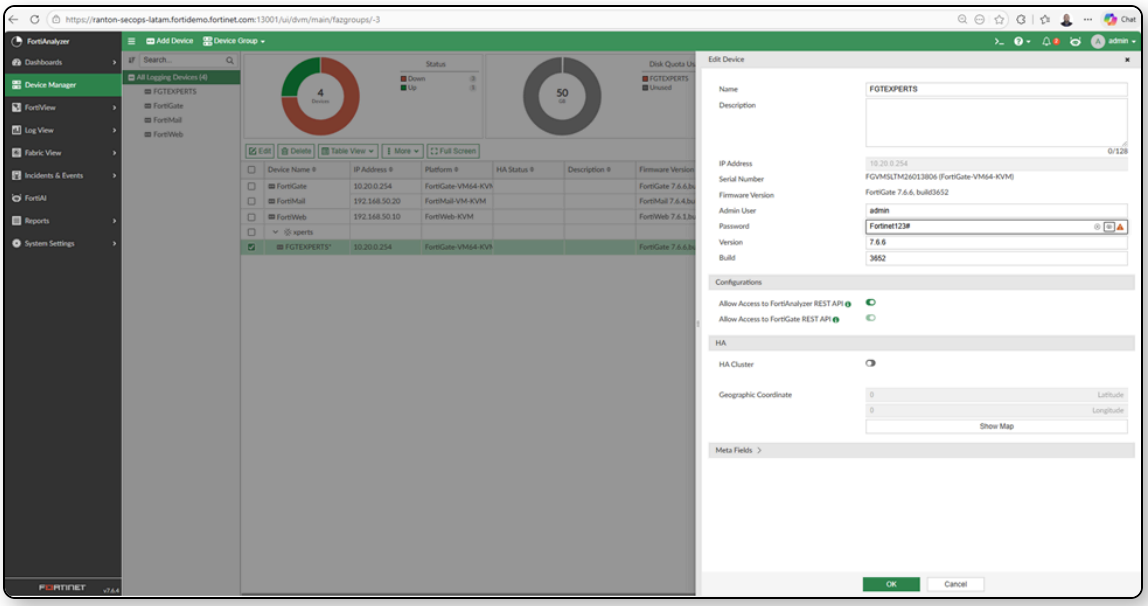
- First, in the FortiAnalyzer go to “Incident & Events → Event Handler” and search for “Default-Malicious-Code-Detection-By-Threat”.



- Select the handler “Default-Malicious-Code-Detection-By-Threat” and click in “Clone”.
- We can put the name “Xpert2026-Malicious-Code-Detection-By-Threat” (Without blanks), activate the toggle “Automation Stitch” (That we can integrated with FortiGate).
- In "Data Selector" select "IPS Logs Automation Stitch Handler" and click in “OK”.

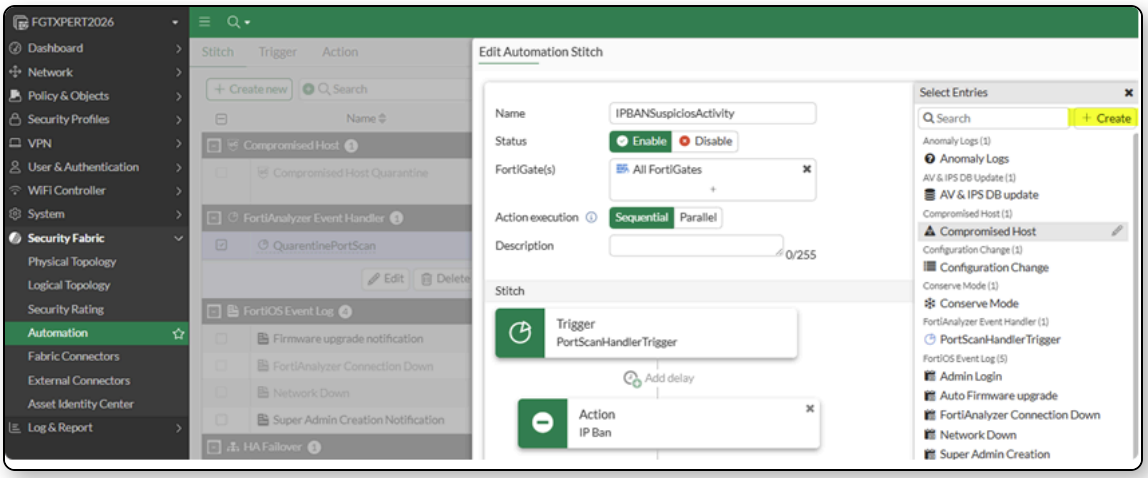


- In the FortiAnalyzer please make sure in "Device Manager" the FortiGate has the correct credentials:

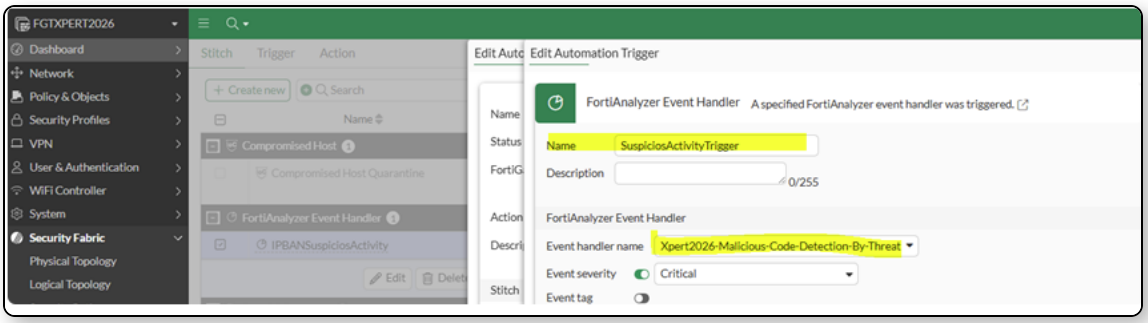


c) Let’s go to the FortiGate to create the “Automation Stitch”.

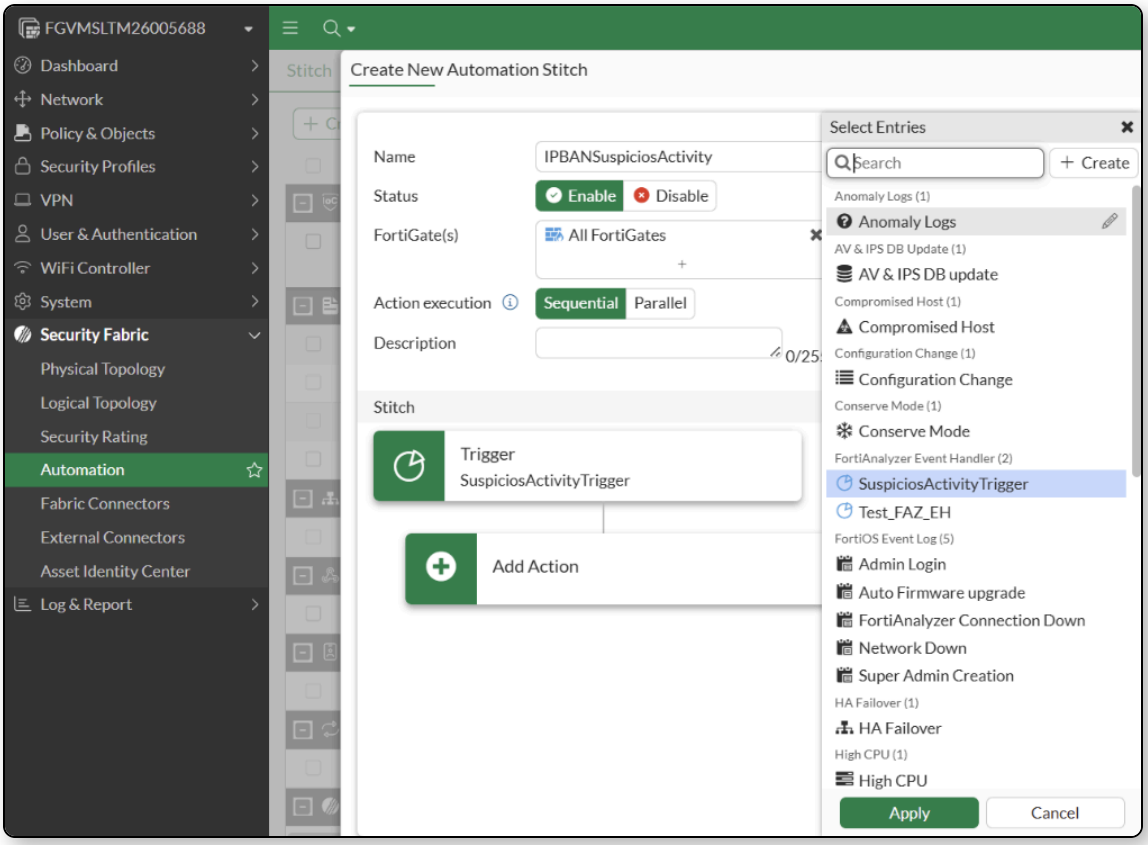
- Ingress to the FortiGate via HTTPS and go to “Security Fabric → Automation” and click in “Create new”.
- Put the name “IPBANSuspiciosActivity” and select “Add Trigger” and click in “Create”.



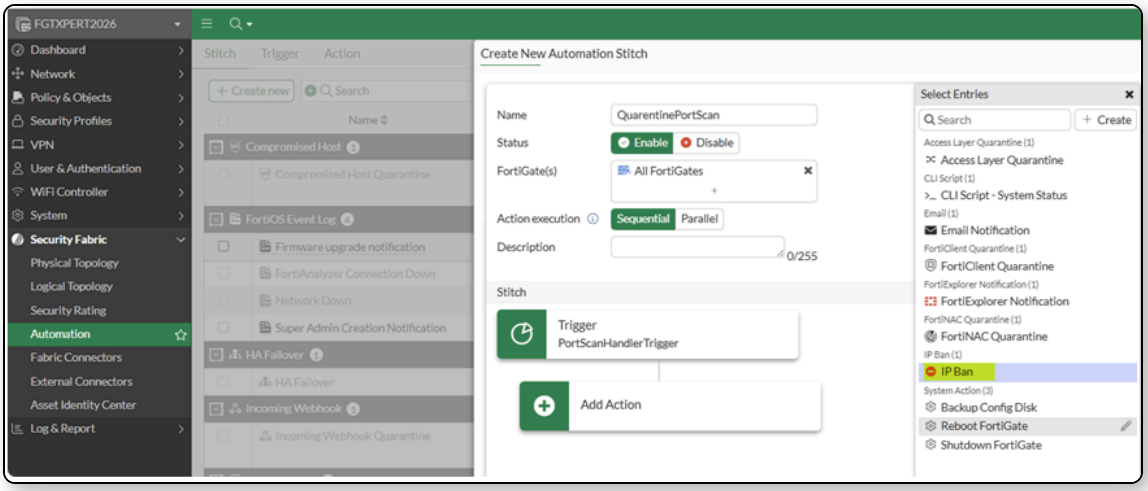
- Select “FortiAnalyzer Event Handler” put the name “SuspiciosActivityTrigger”.
- In the field “Event handler name” select “Xperts2026-Risky-Destination-Detection-By-Threat”, click in “OK”.



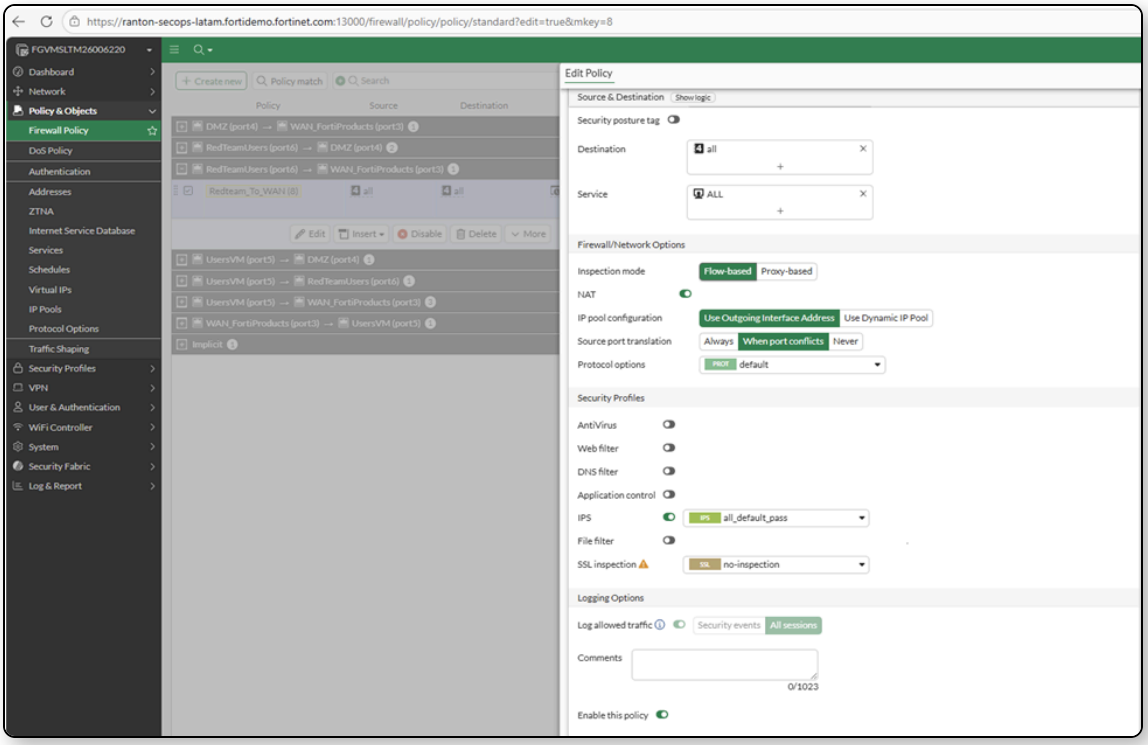
- Select “SuspiciosActivityTrigger” and click in “Apply”.



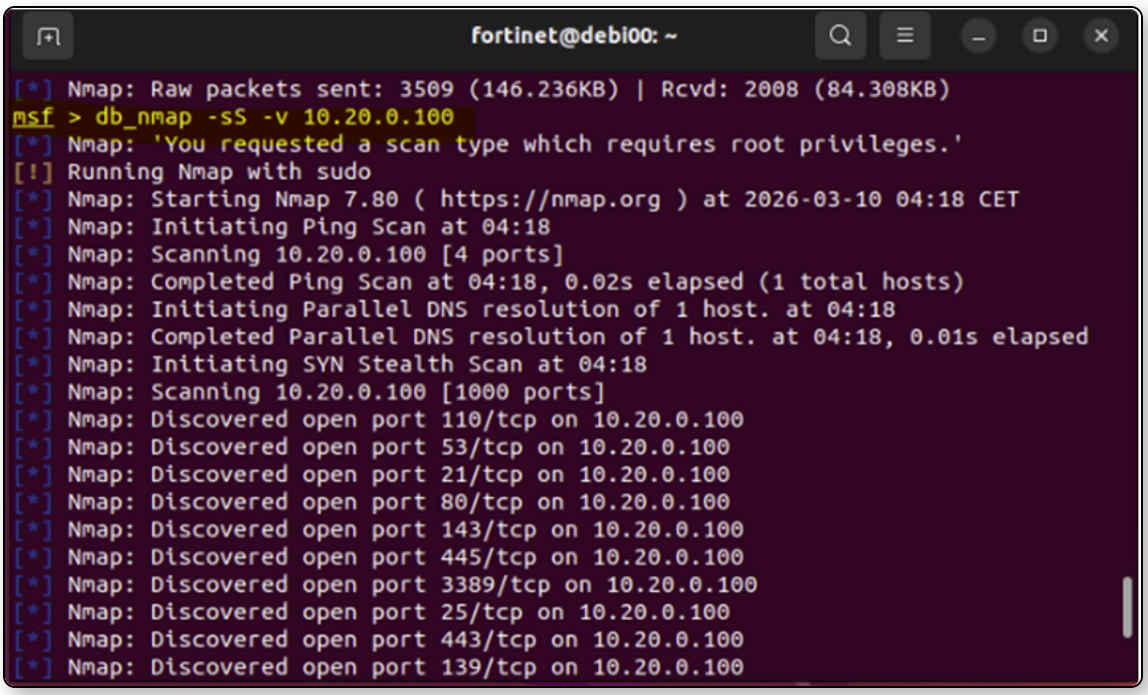
- Click in “Add Action”, select “IP Ban”, click in “Apply” and click in “OK”.



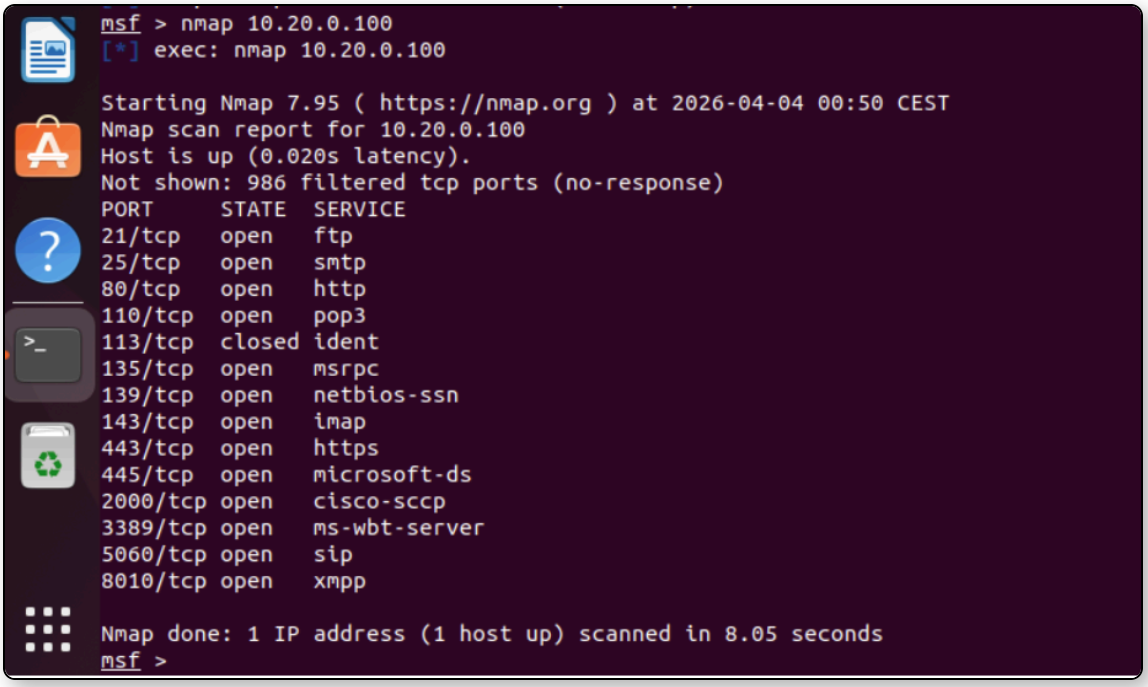
- Please validate that the Policy that allow traffic between "Attack" and "File Server" has an IPS profile "All Default Pass":



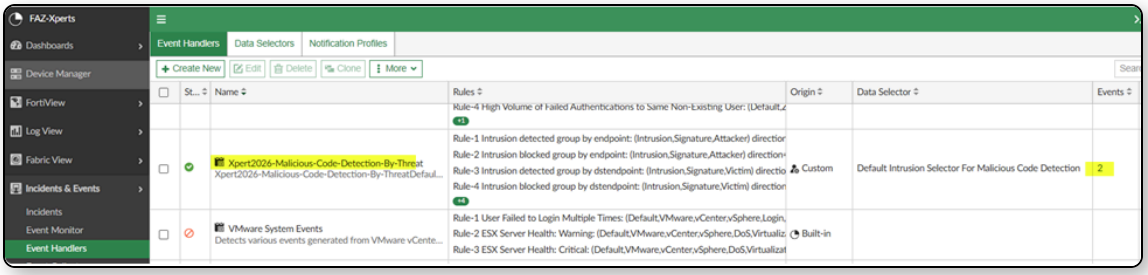
- Ingress to “Attack” device via “Display” and let’s do a “NetworkScan”.



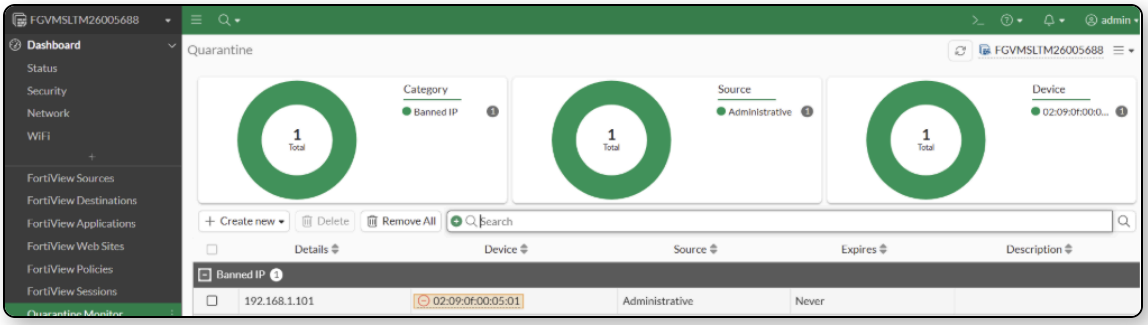
- Execute the next command in the "Attack" device "nmap 10.20.0.100":



- We can see “Events” triggers in the FortiAnalyzer.



- Now, we can go to FortiGate to review the automatic response:



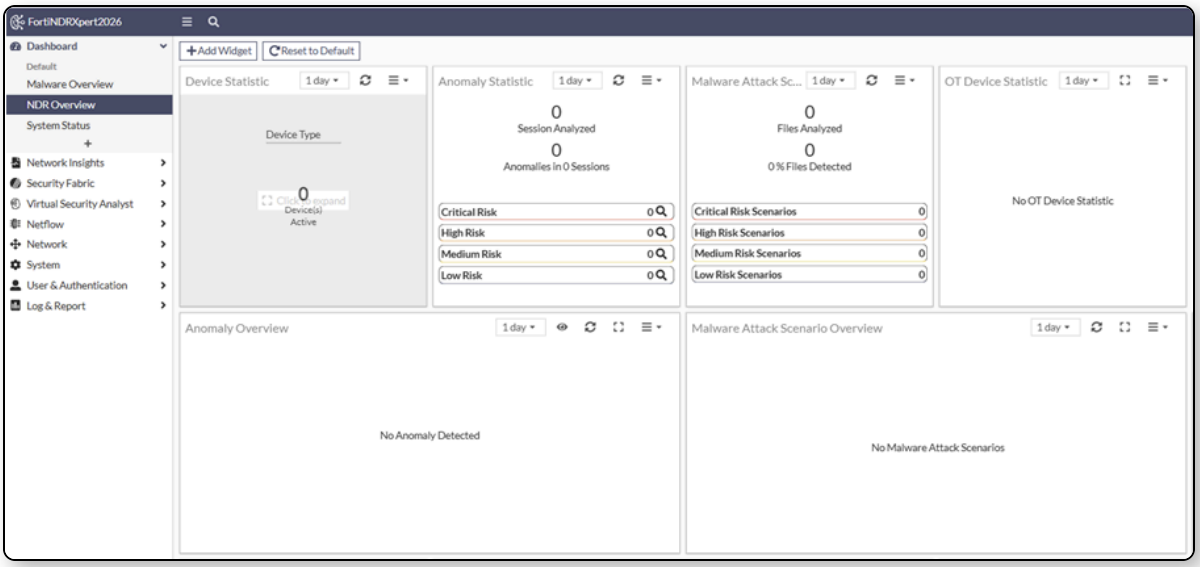
- If you do not see "Quarantine" add in "Dashboard" a widget that show this information.
- If you stich does not work, reboot the FortiAnalyzer. This is a issue identify in "Fabric Studio".

Lab04 Advance Anomaly Detection with FortiNDR

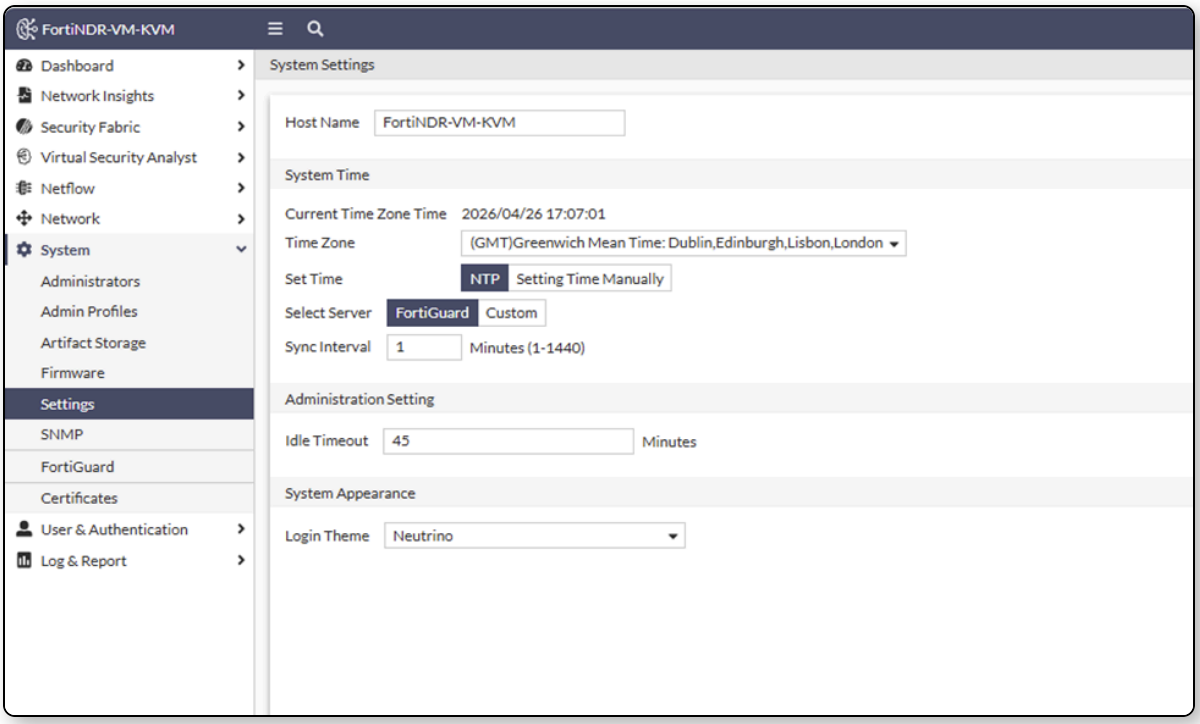
LABORATORY 4: Advance Anomaly Detection with FortiNDR:

a) Initial setup of FortiNDR

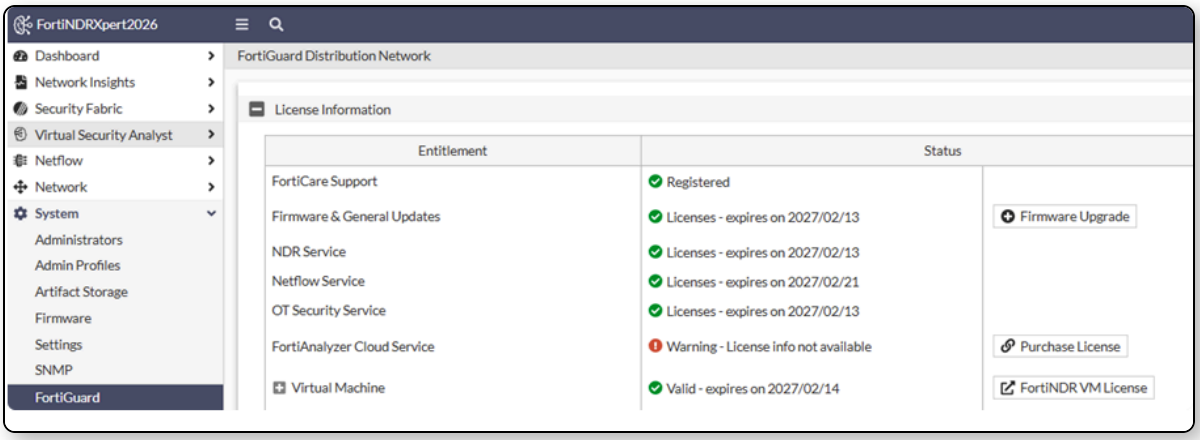
- Login in the FortiNDR via HTTPS, and review the next information:



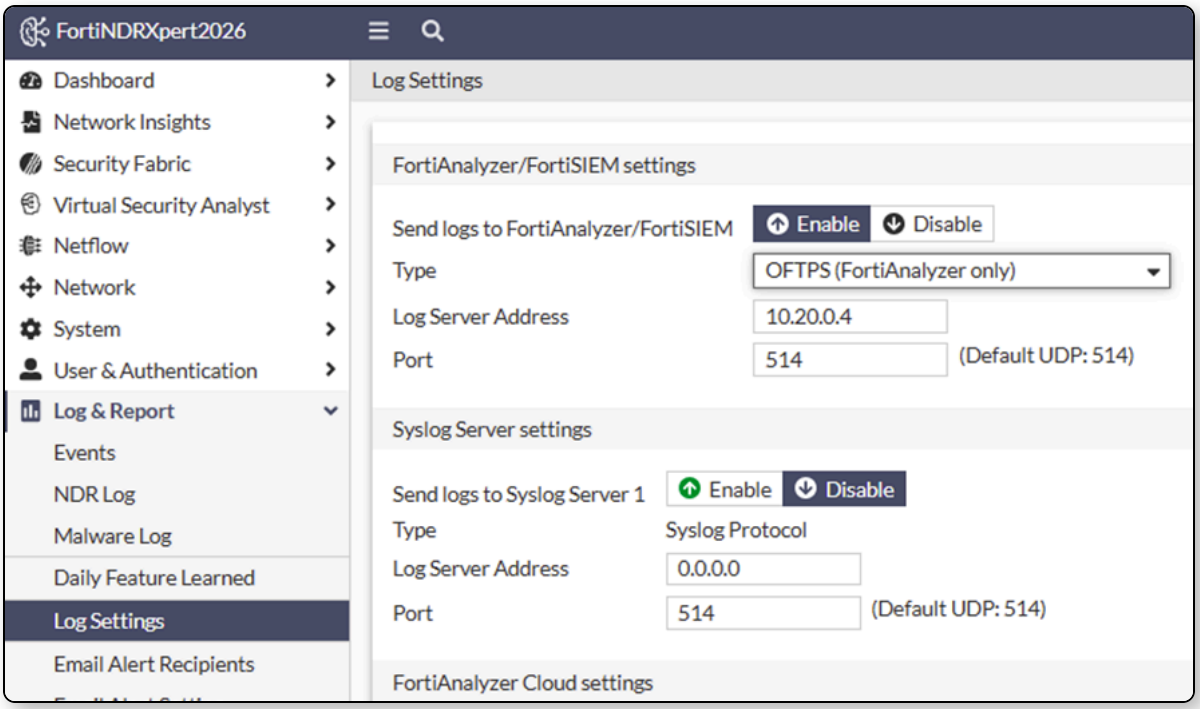
- Check the time zone (Should be GMT Greenwich). System → Settings → System Time:



- Check the license and Fortiguard updates: System → Fortiguard. Update if it necesary.
- **Important:** Netflow & OT Security Services is licensed separately.



- Check the setup remote logging configuration to the FortiAnalyzer server:



- Optionally, you can change the theme of the FortiNDR GUI, to do that you can connect to FortiNDR via SSH and run the command:

```
config system admin
  edit admin
  set theme <theme_name>
end
```

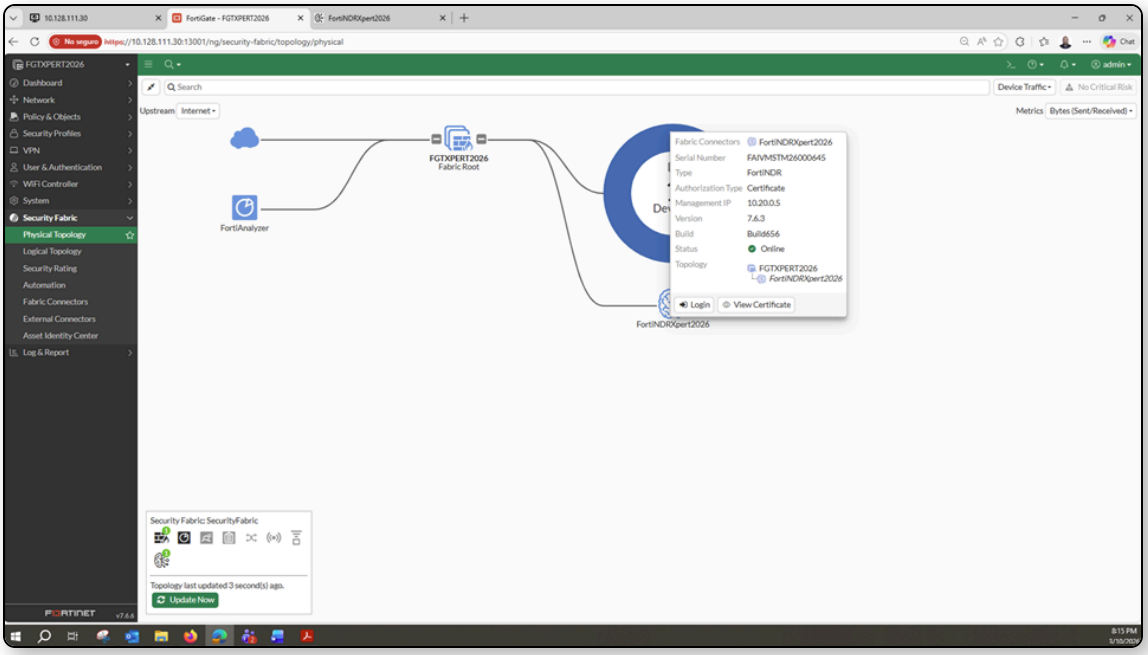
- Where “theme_name” must be replaced by one of the following options:

```
{Neutrino| Jade | Mariner | Graphite | Melongene | Onyx | Dark_Matter | Eclipse |
Cloud_App_Light | Cloud_App_Dark}
```

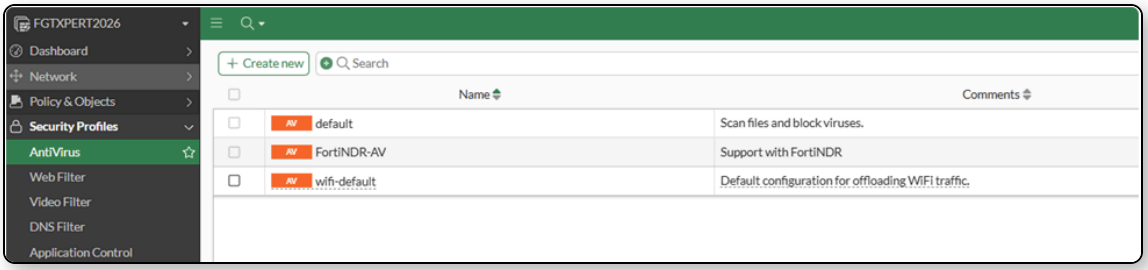
b) Check Fabric Integration

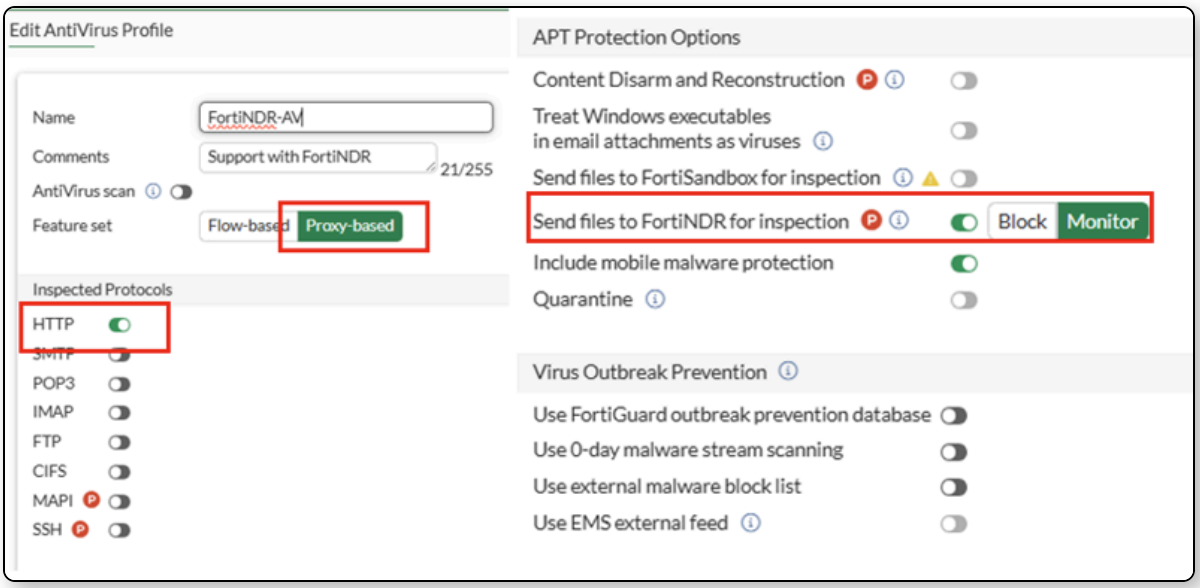
- We need to validate the connection between the FortiGate and FortiNDR is working (We do this integration in Lab 1).
- Login in the FortiGate via HTTPS and go to “Security Fabric → Physical Topology” section and move the mouse over the FortiNDR section, the status should be

“connected”.



- Now, go to “Security Profiles → AntiVirus” we are going to check the security AntiVirus Profile created in Lab 1; FortiNDR-AV, please modify the profile in the next way.





- Click “Ok” and open the Fortigate CLI to run the following commands:

```
FGTXPERT2026 # config antivirus profile

FGTXPERT2026 (profile) # edit FortiNDR-AV

FGTXPERT2026 (FortiNDR-AV) # set fortindr-error-action block

FGTXPERT2026 (FortiNDR-AV) # set fortindr-timeout-action block

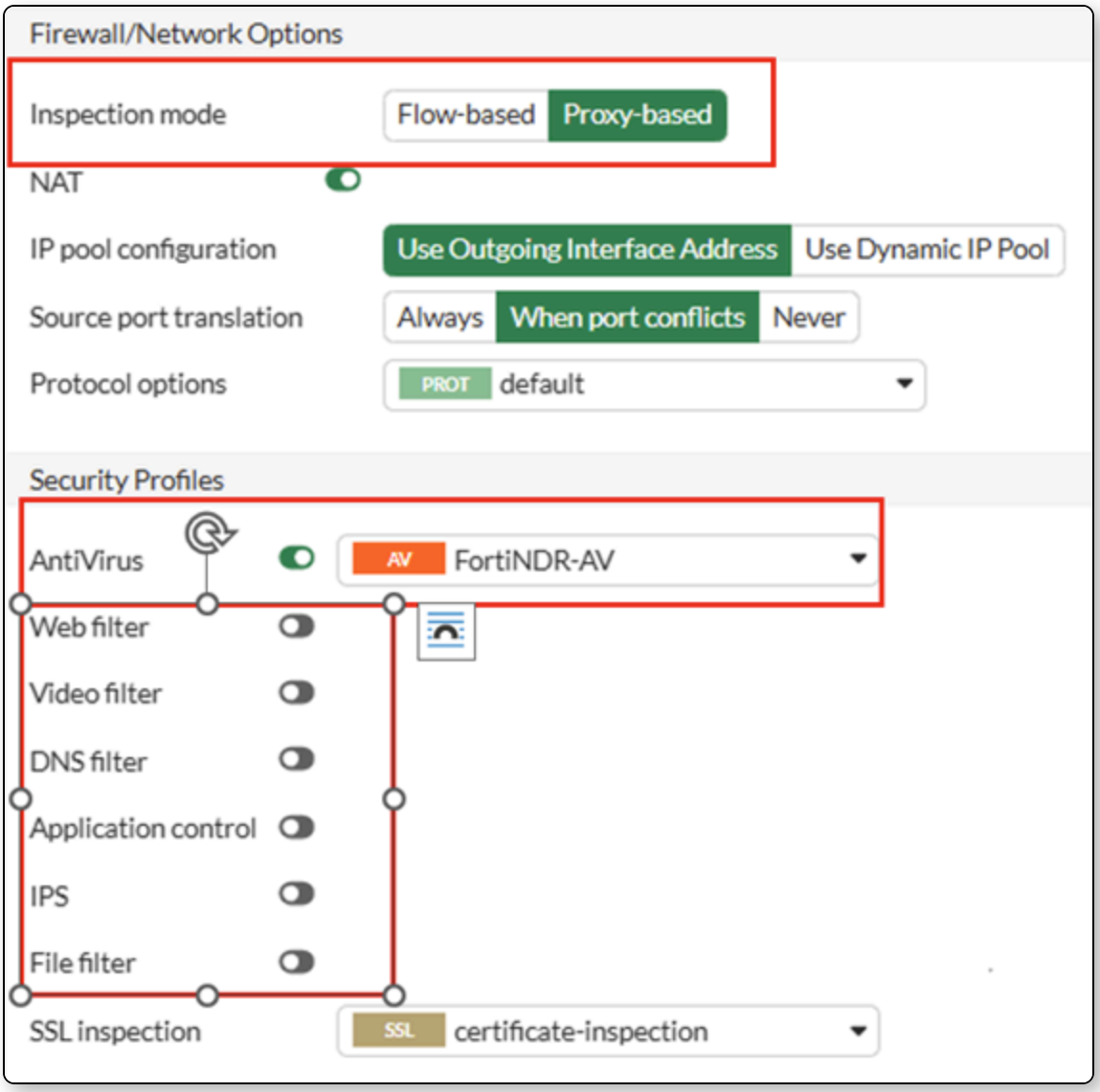
FGTXPERT2026 (FortiNDR-AV) # set av-virus-log enable

FGTXPERT2026 (FortiNDR-AV) # set extended-log enable

FGTXPERT2026 (FortiNDR-AV) # end

FGTXPERT2026 #
```

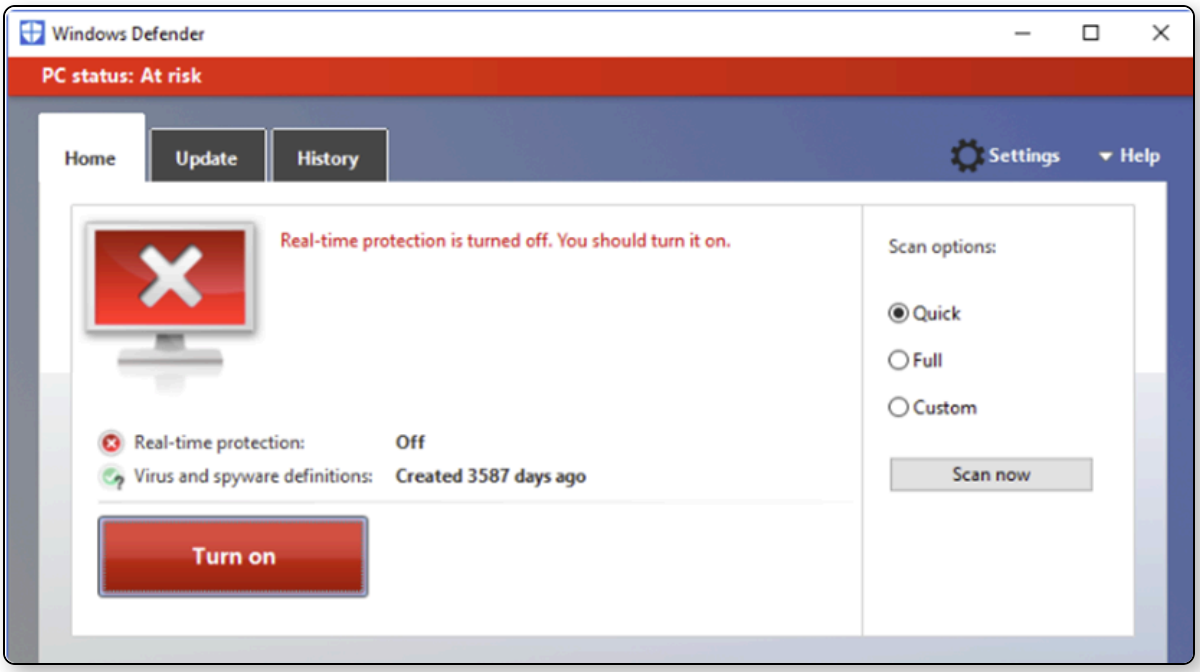
- We need to check this profile is assigned in a Firewall Policy.
- Go to “Policy & Objects → Firewall Policy” → Edit “ConexionRedServidores” policy.
- We need to validate this configuration:



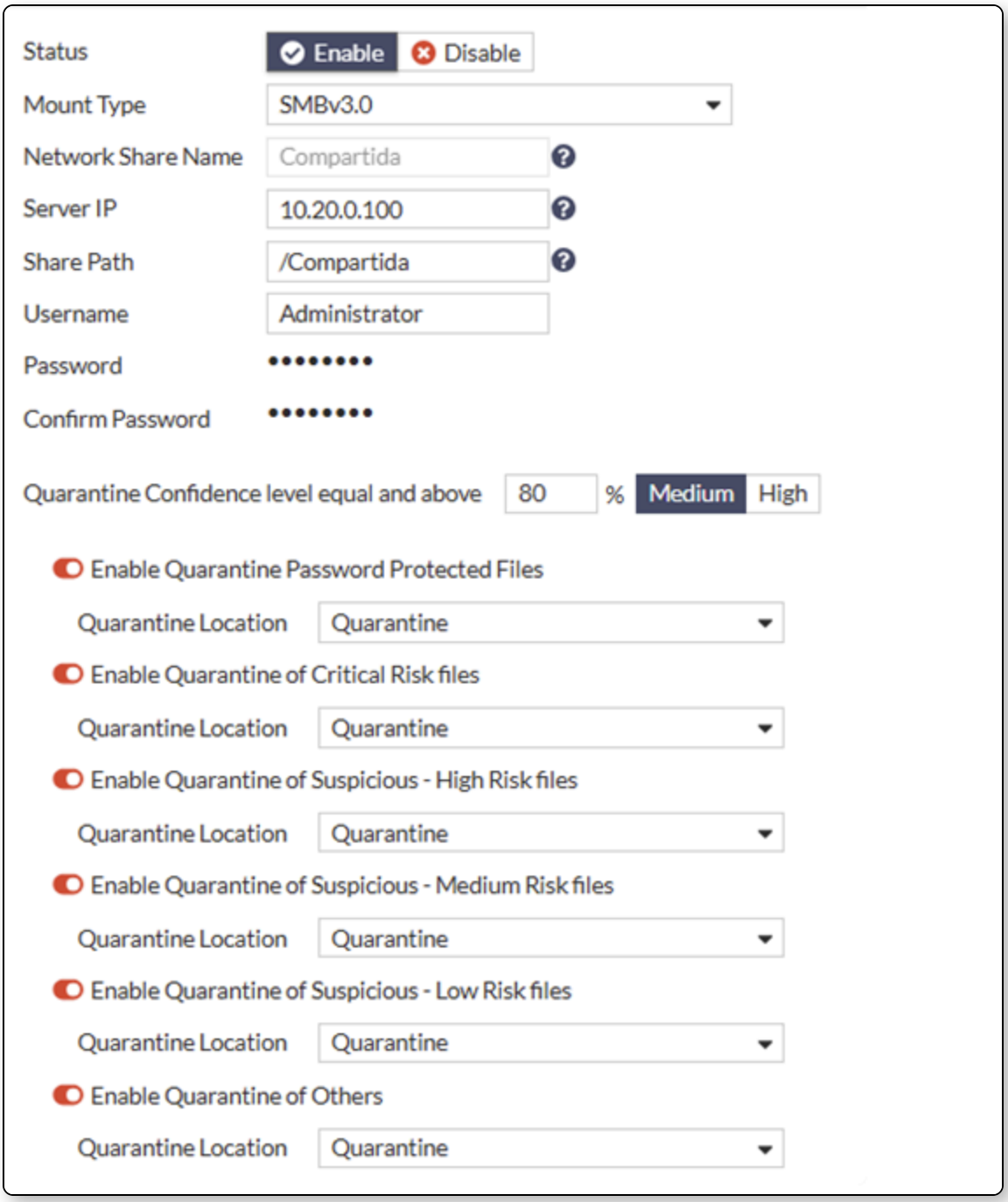
c) File share inspection for FortiNDR

In the Lab 1, we have integrated FortiNDR with a “Network Share”, now for test the file FortiNDR File inspection we are going to copy a malware file to folder integrated with FortiNDR and we hope the FortiNDR detects this malware and move it to Quarantine Folder.

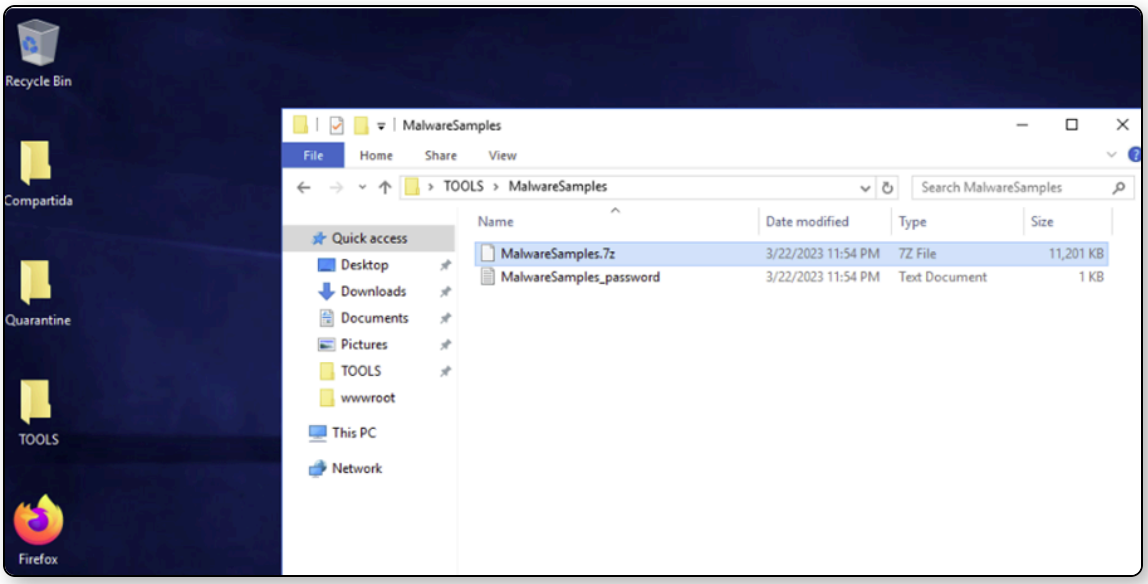
- First make sure the “WindowsServer” Windows Defender is in state “Off”.
- If Windows Defender is active, follow the next: execute gpedit.
- Next go "Administrative Templates → Windows Components → Windows Defender Antivirus and "Turn off Windows Defender Antivirus → Enabled"

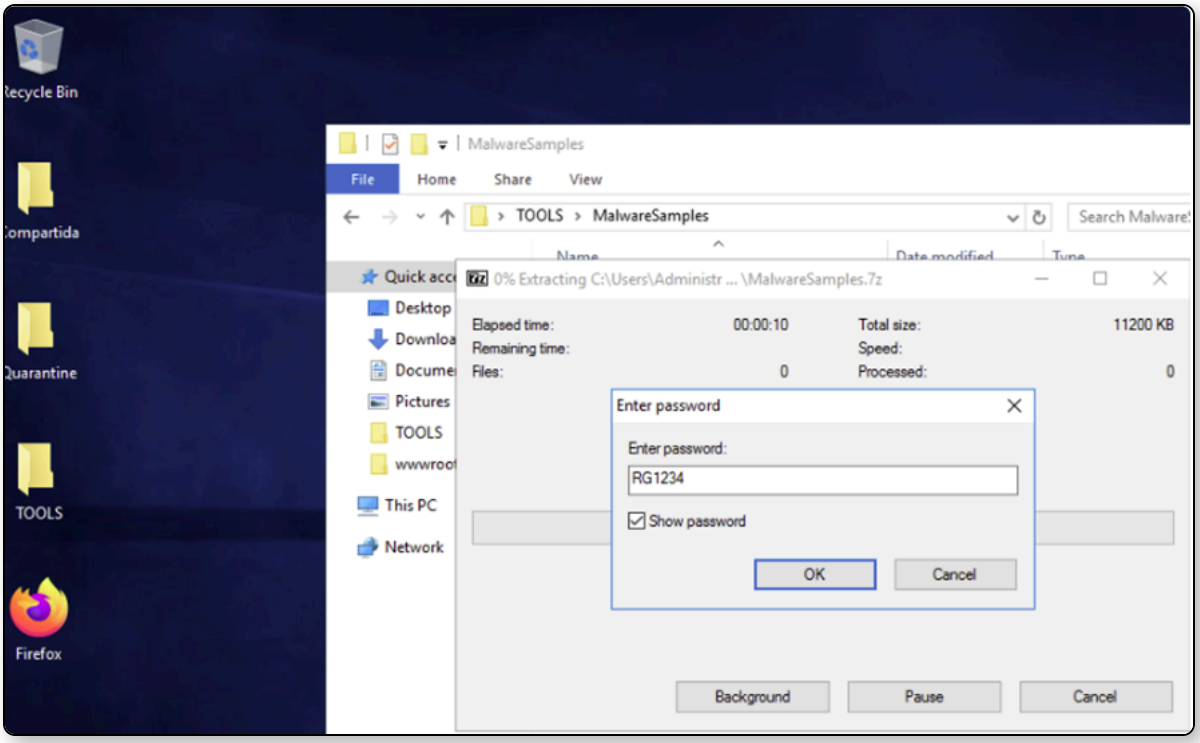


- We need to validate the “Network Share” configuration looks similar to this.
- Access to FortiNDR an go to “Security Fabric Network Share” and edit “Compartida”:

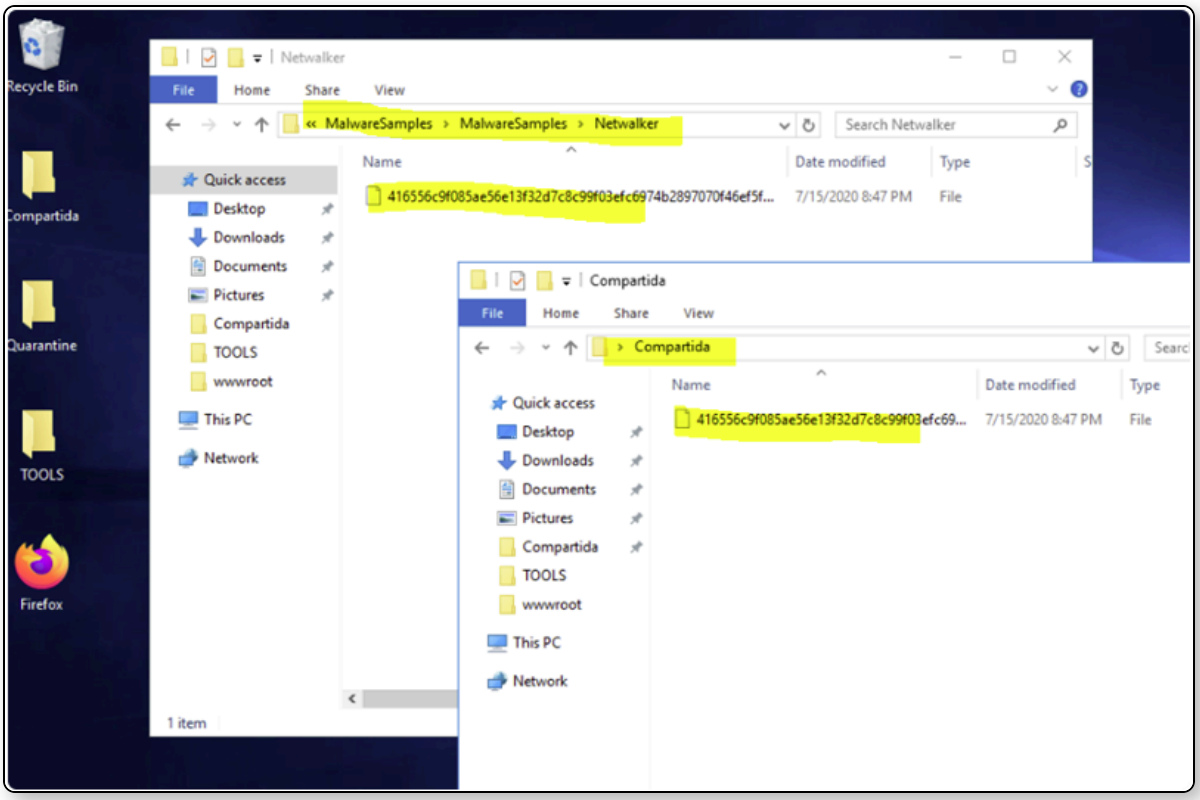


- Access to “WindowsServer” via “Display”, go to folder “TOOLS” in the desktop, unzip file “MalwareSamples.7z” to unzip folder “MalwareSamples.7z” (The unzip key is RG1234).

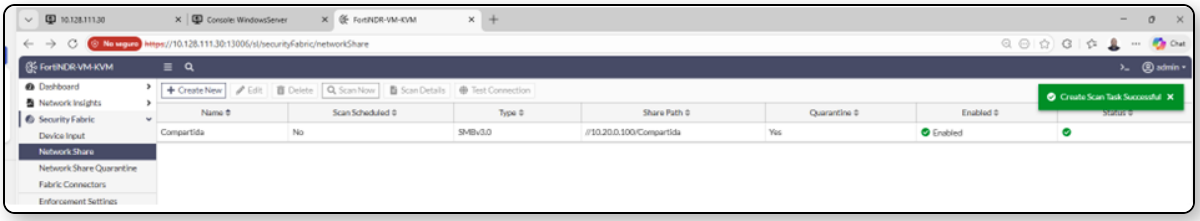




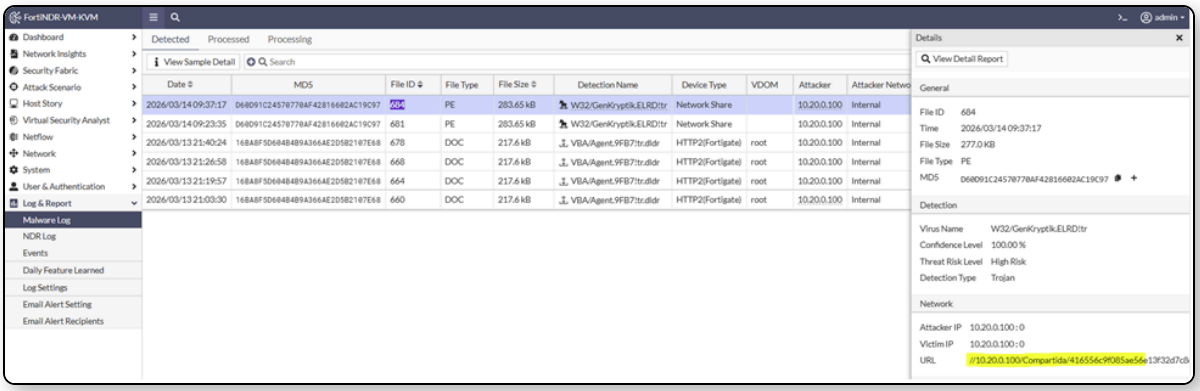
- Go to folder “Netwalker” and copy the file with name “416556c9f0.....” to the folder “Compartida”:



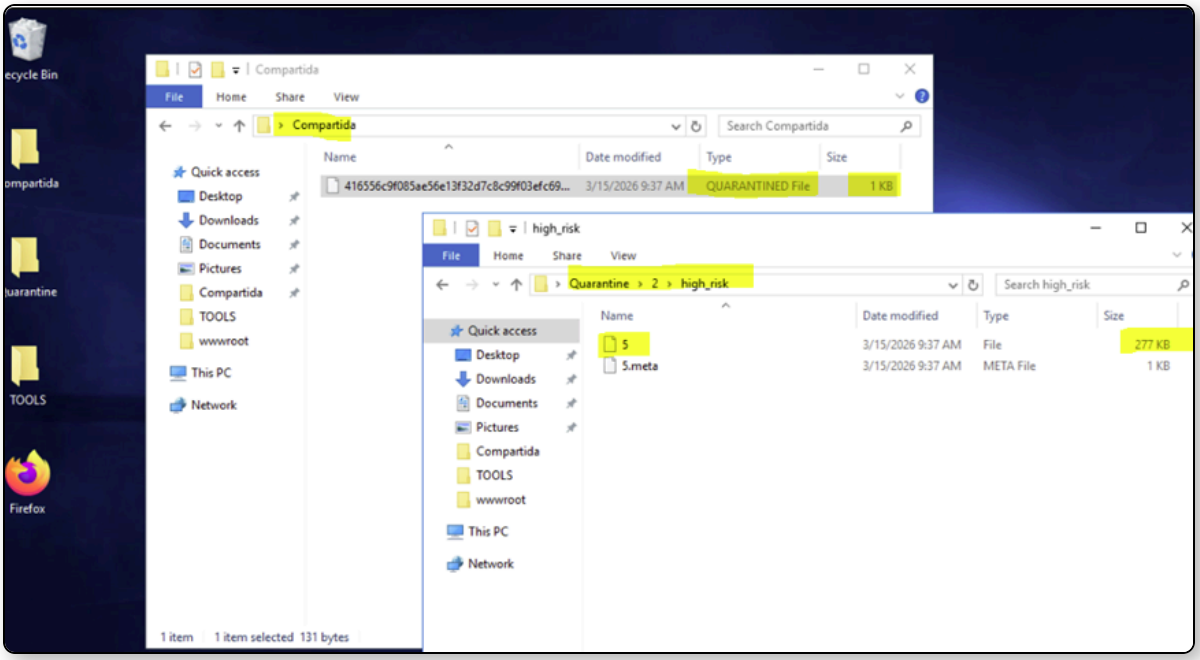
- Go to FortiNDR in “Security Frabric → Network Share” and select “Compartida” and click in “Scan Now”.
- With this we forced an scan now but in the configuration we can scheduled scan at least every 15 mins:



- You can go in the FortiNDR to “Log & Report → Malware Log” and see the detection log:



- Go to “WindowsServer” and you can see the file in “Compartida” folder has been deleted but we have a signal of “QUARANTINED File”.
- In “Quarantine” folder configured in FortiNDR has been copied the file:

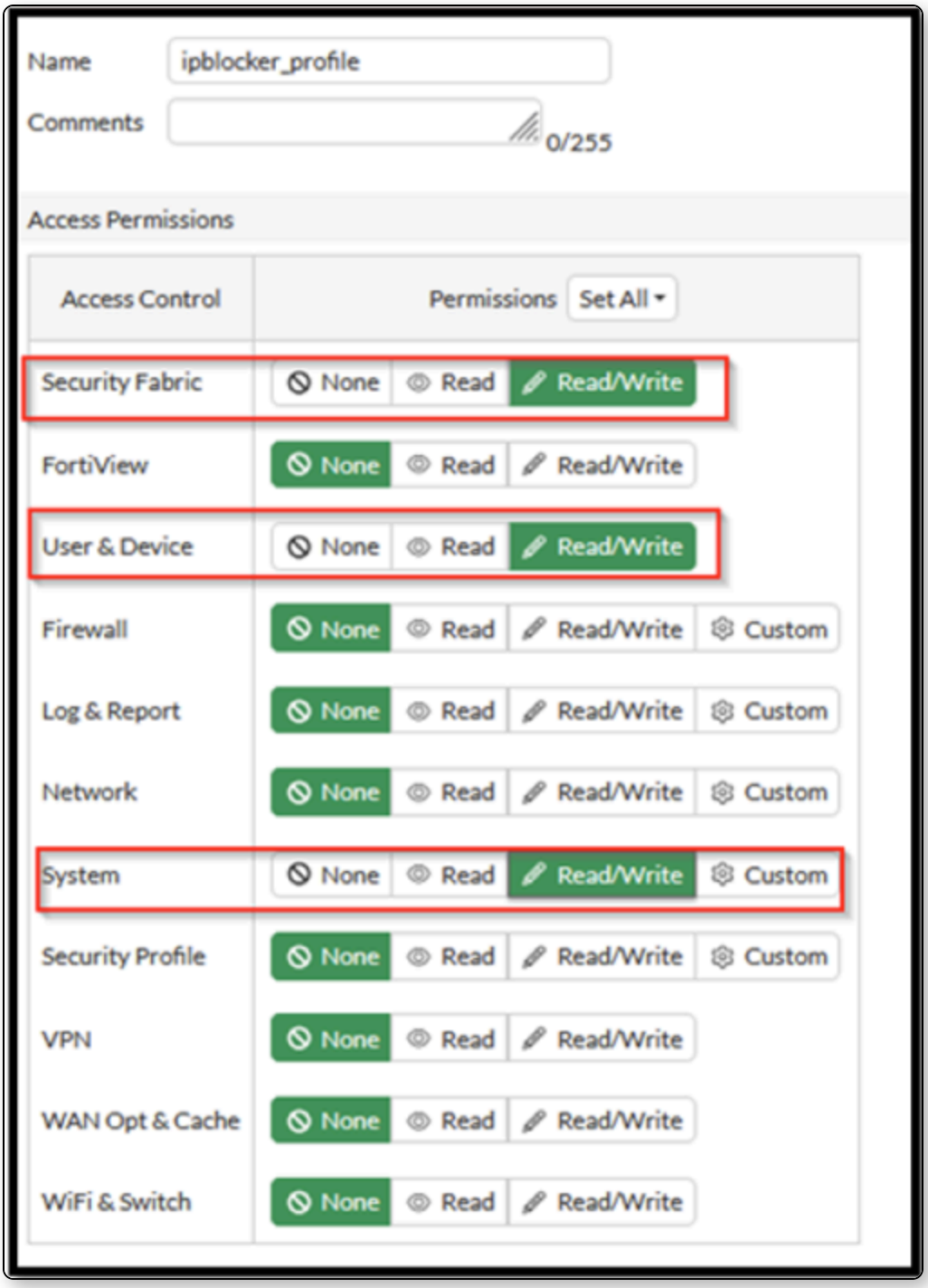


d) Fabric Response between FortiNDR and FortiGate

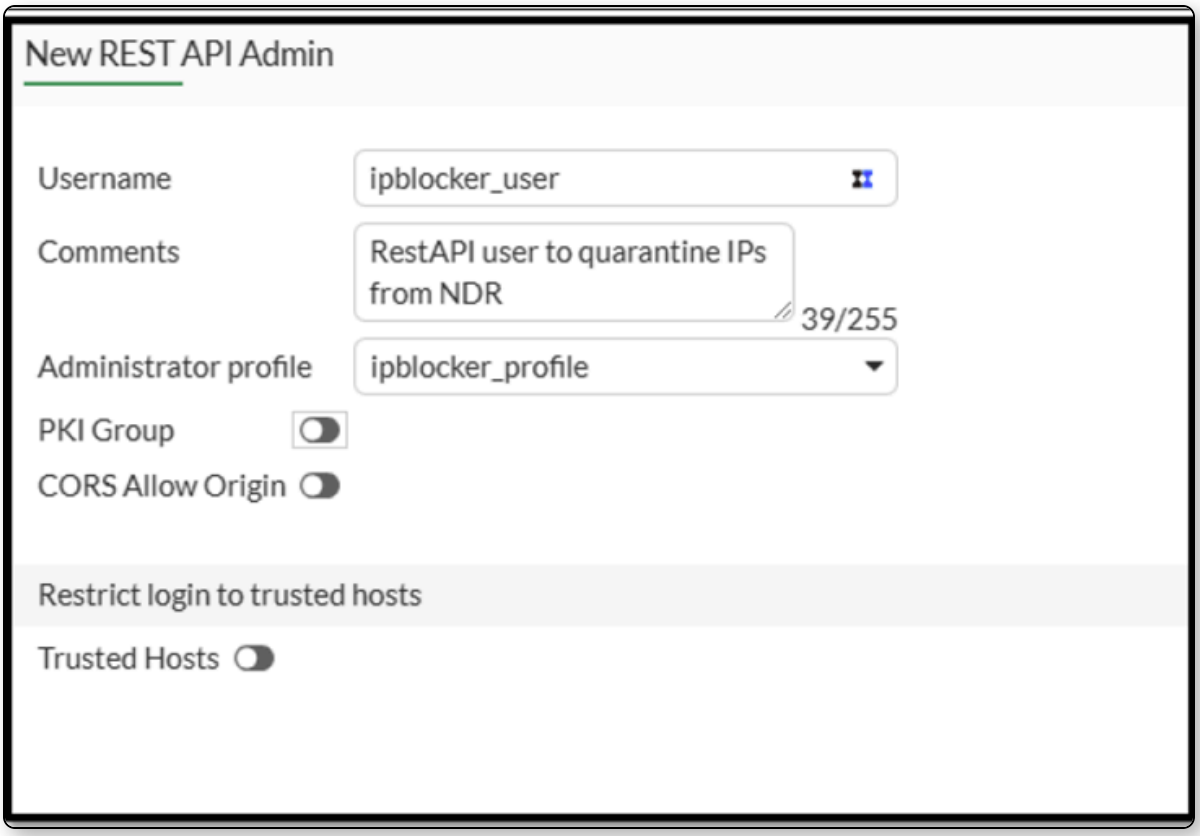
Now that the integration between Fortigate and NDR is configured and working correctly through the Security Fabric, we can go one step further and generate an automatic response when detecting an attack in the NDR.

- Fortigate - Automation config: In this section, we will configure the necessary resources within Fortigate to enable the automatic response from the NDR.
- Login to Fortigate via HTTPS and Go to “System → Admin Profiles → Create New”.

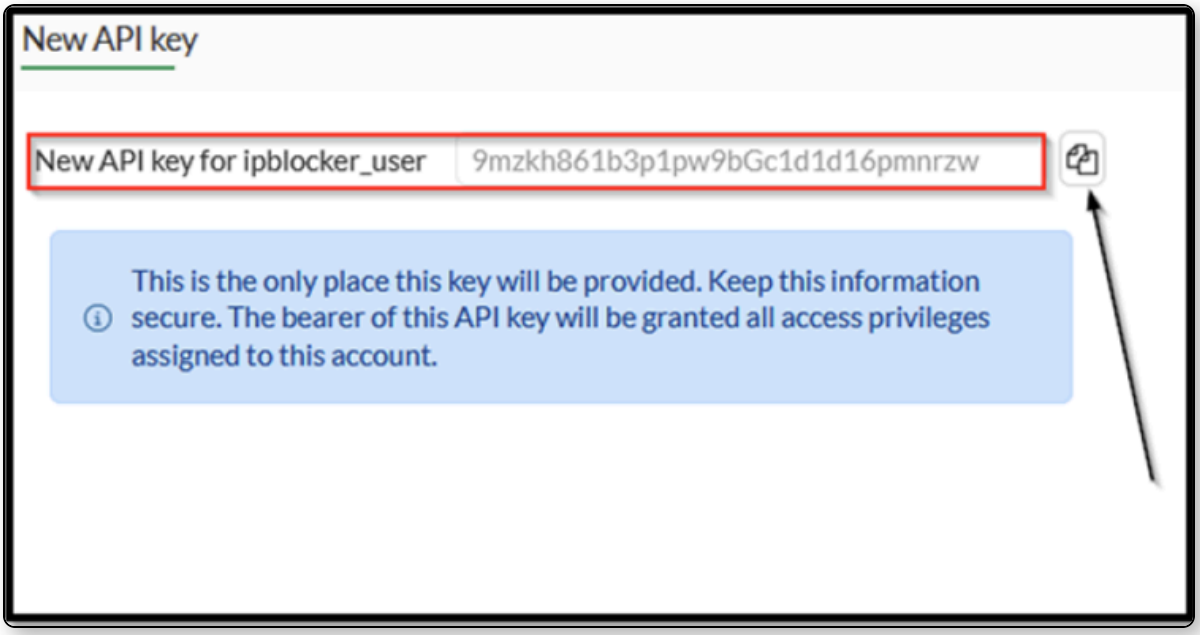
- Create a new profile admin with the next configuration and Click "Ok" to save changes:



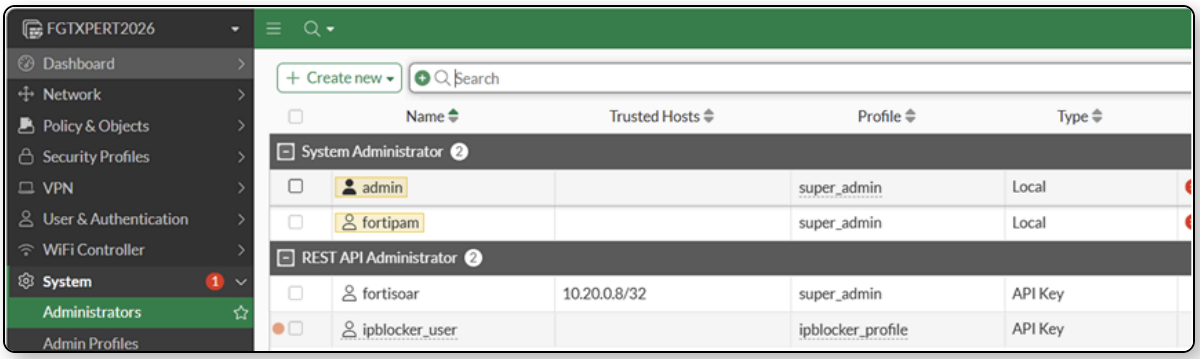
- Go to “System → Administrators → Create New → REST API” Admin to configure a new administrator:



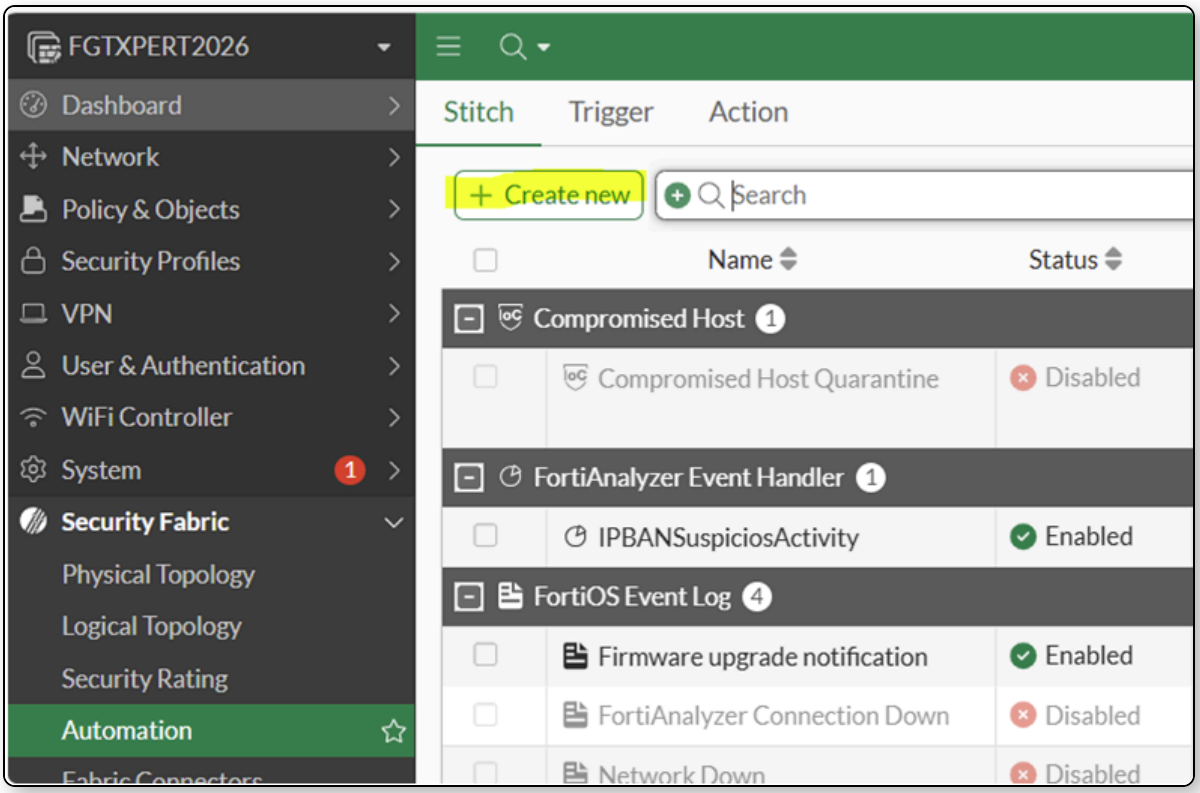
- Click "Ok" and [SAVE] the API key code in your notepad for later use:



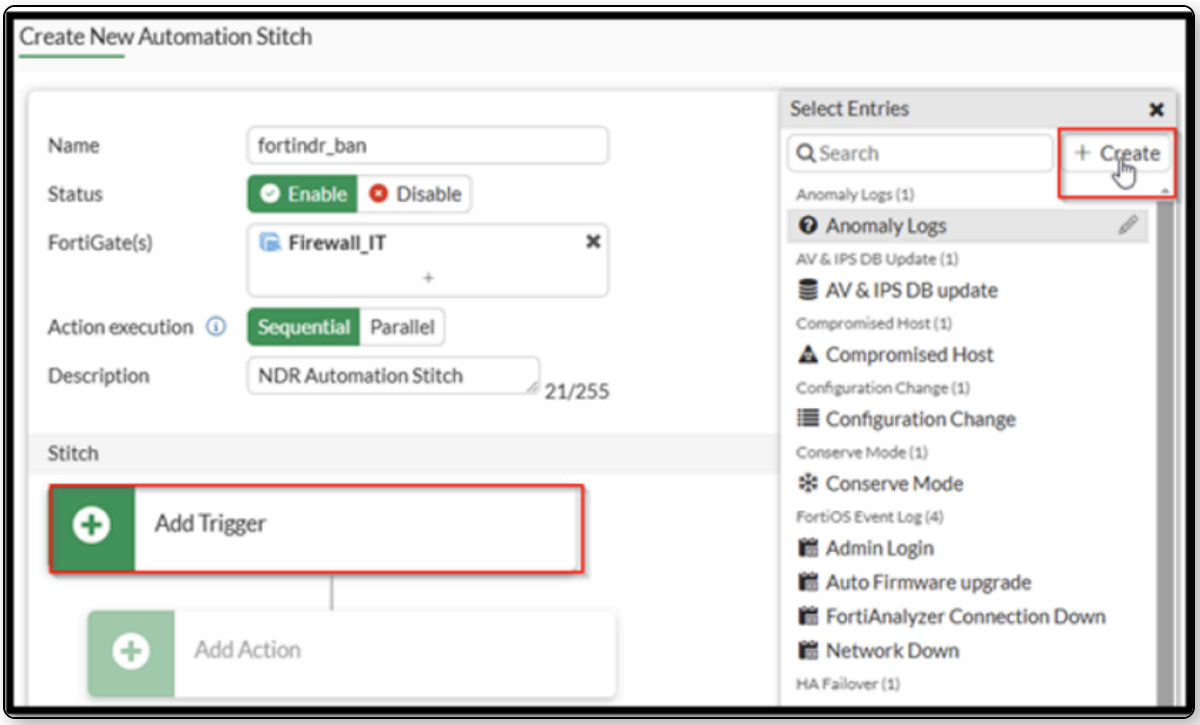
- Now you should see your new RestAPI user account:

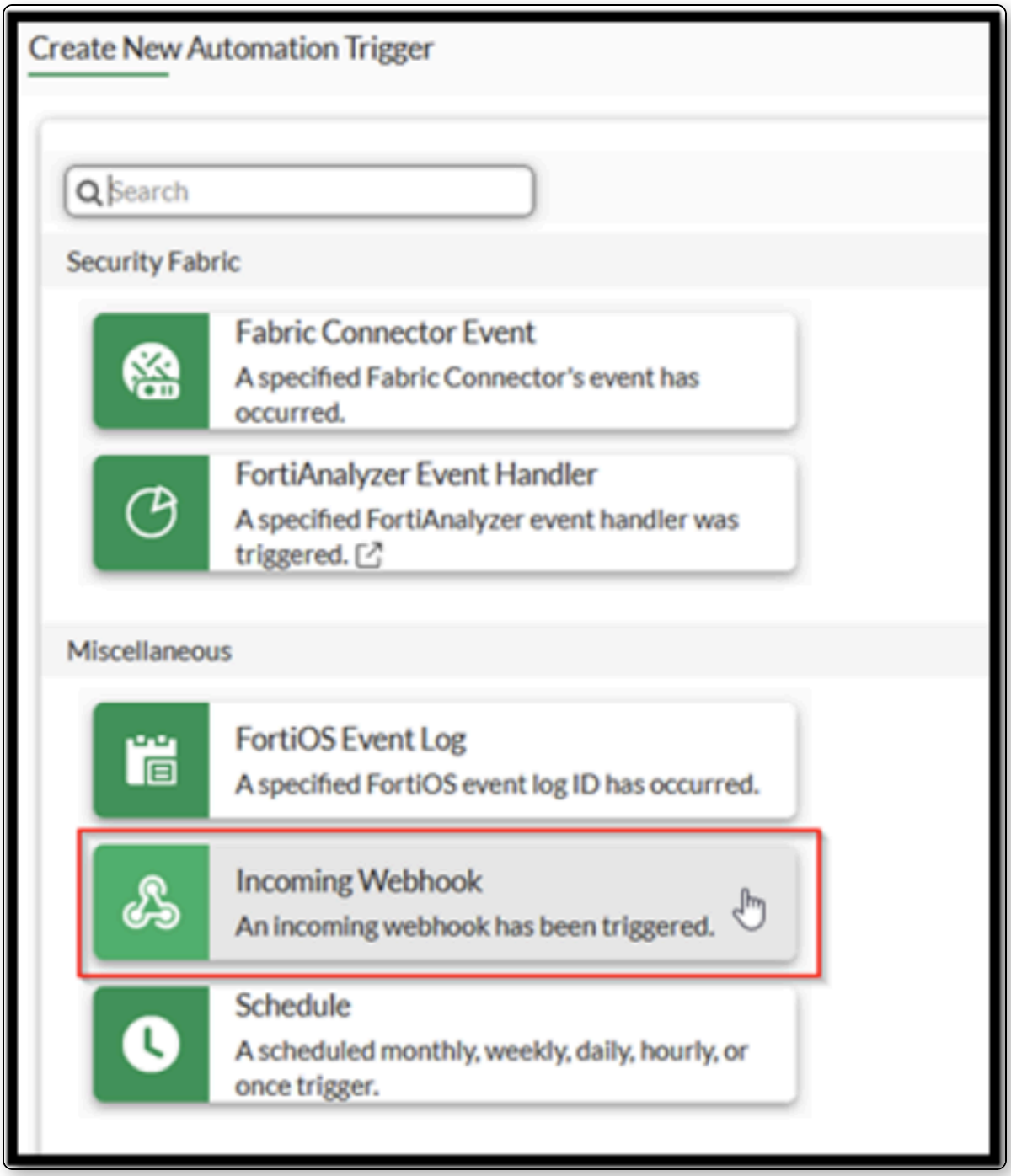


- Go to “Security Fabric → Automation → Stich → click on “Create new”:

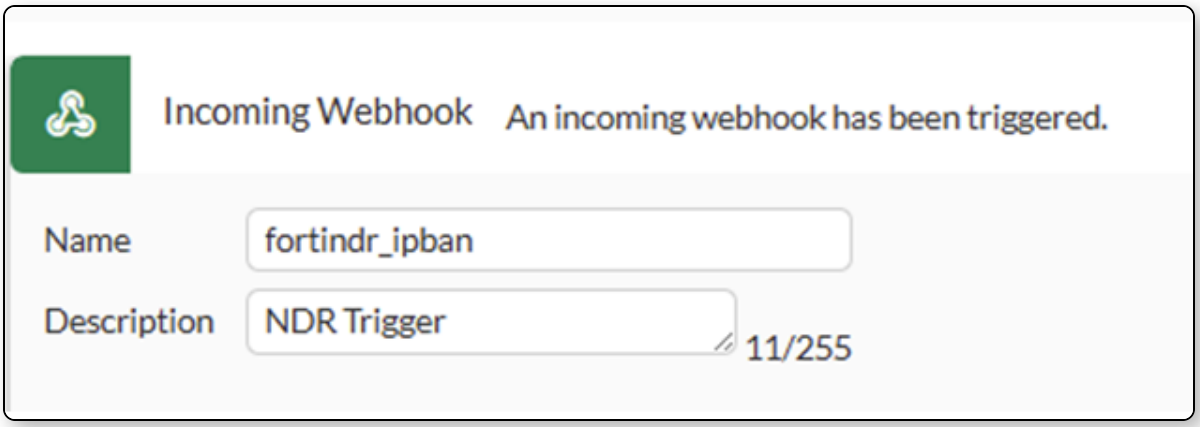


- Let´s go to create the next stitch “fortindr_ban” in “Add Trigger” click in “Create”:

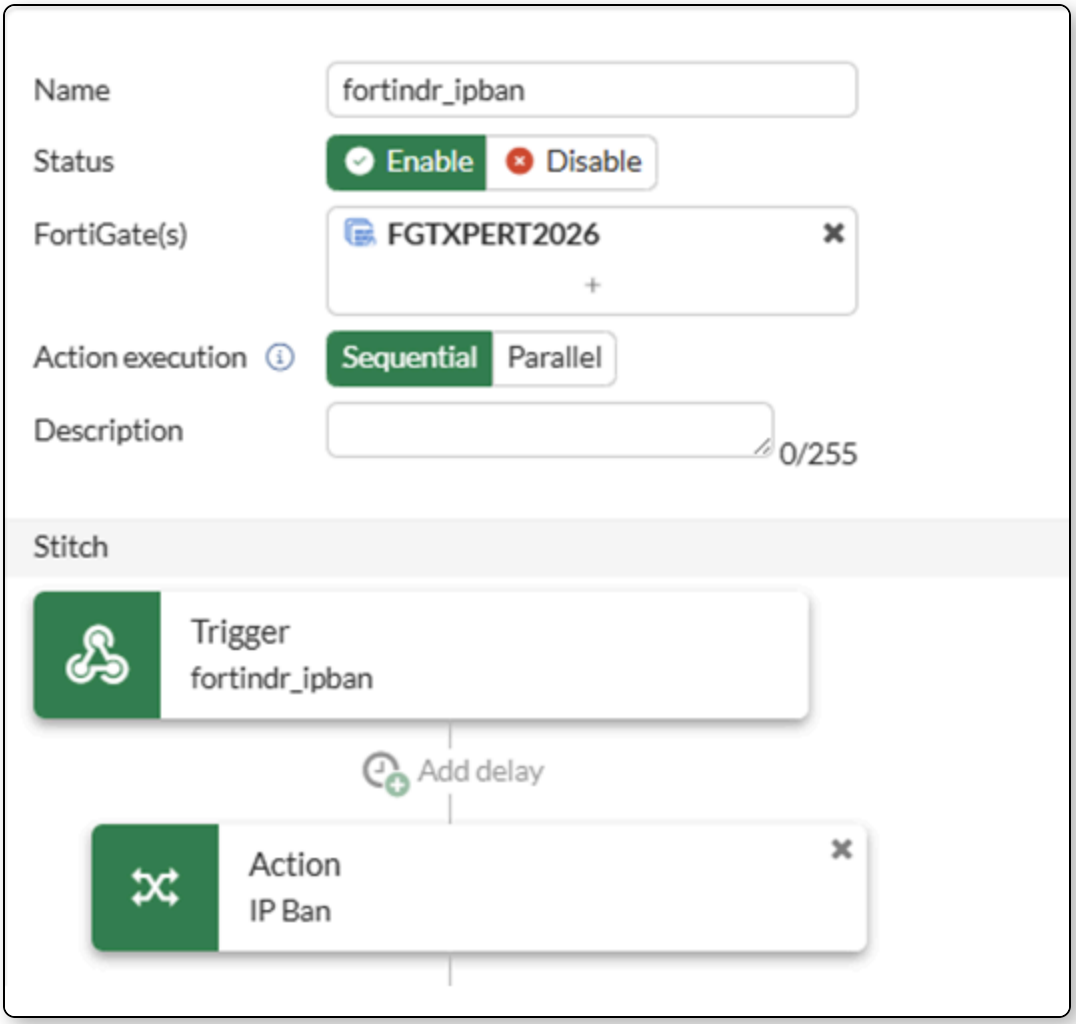

Create New Automation Stitch
Name
fortindr_ban
Status
Enable
Disable
FortiGate(s)
Firewall_IT
Action execution
Sequential
Parallel
Description
NDR Automation Stitch
21/255
Stitch
Add Trigger
Add Action
Select Entries
Search
Create
Anomaly Logs (1)
Anomaly Logs
AV & IPS DB Update (1)
AV & IPS DB update
Compromised Host (1)
Compromised Host
Configuration Change (1)
Configuration Change
Conserve Mode (1)
Conserve Mode
FortiOS Event Log (4)
Admin Login
Auto Firmware upgrade
FortiAnalyzer Connection Down
Network Down
HA Failover (1)



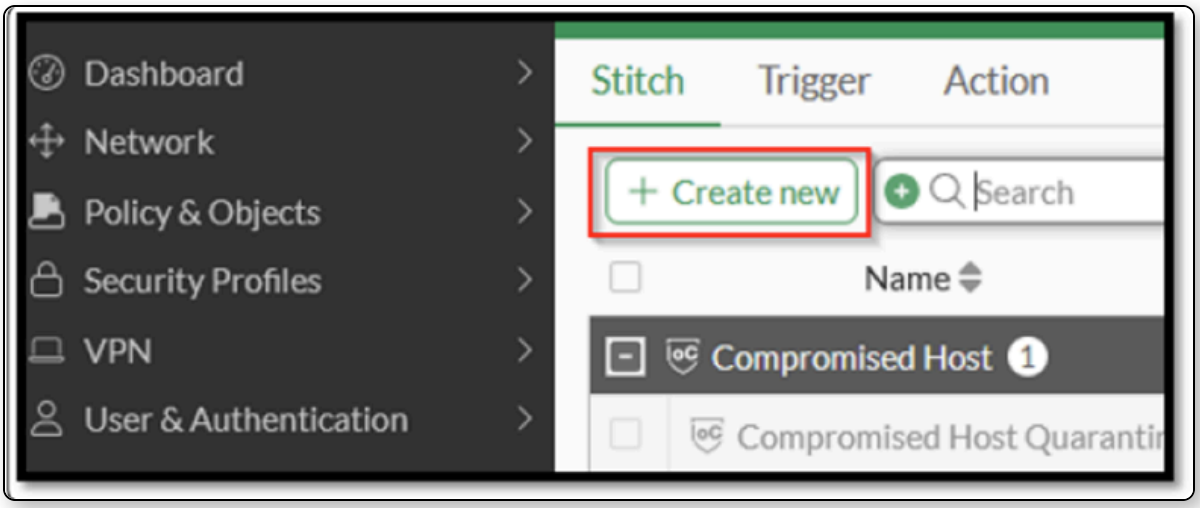
- Let´s go to configure the parameters with the next information and click in “OK”:



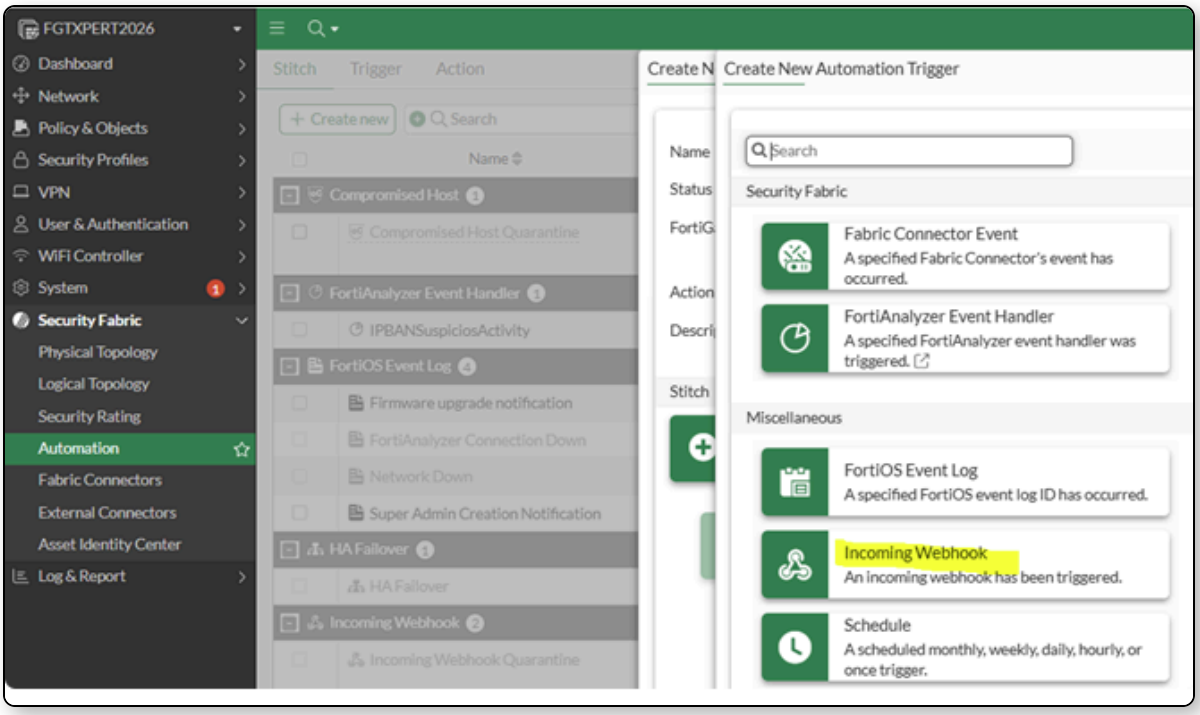
- Click "Ok", a dialog box with the explanation will appear. Click Ok; the newly created webhook will appear; click over it and Select it and Click "Apply".
- Select in “Trigger” = “fortindr_ipban” and in “Add Action” = “IP Ban” and click in apply.

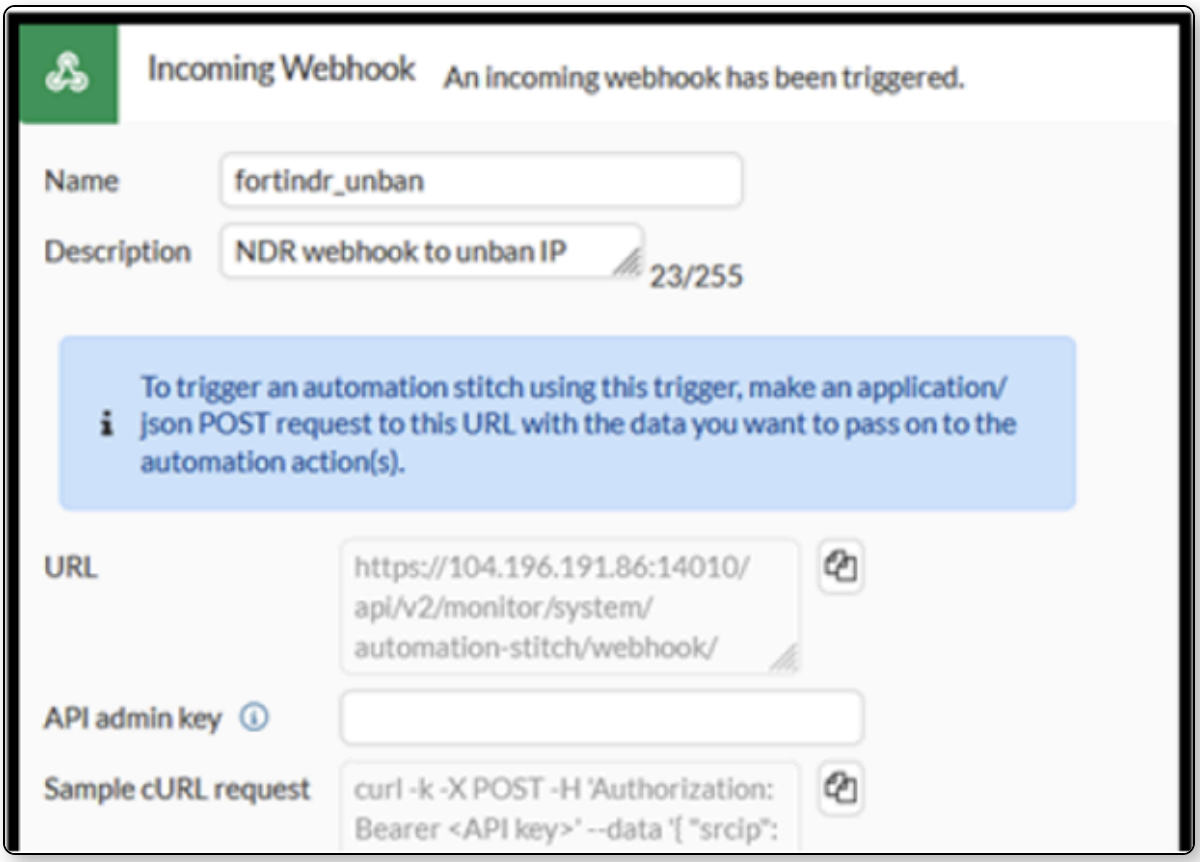


- Now, we are going to create another Stitch but to unband the IP directly from NDR So, click on “Create New” under “Security Fabric → Automation → Stich”.

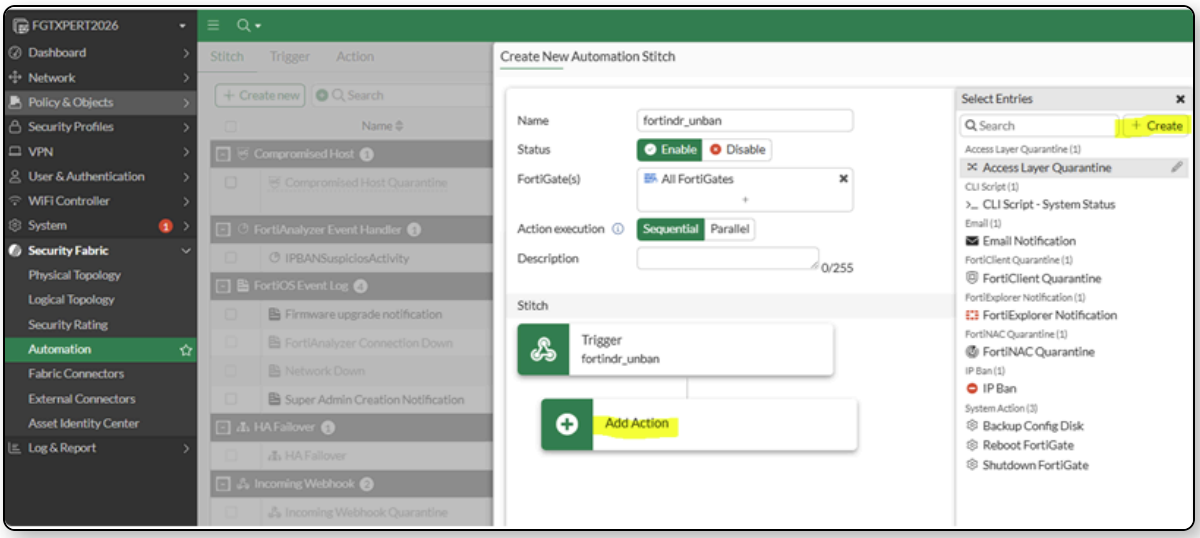


- Click on “Add Trigger”, then click on “Create” in the right pane, select “Incoming Webhook” to configure new webhook.

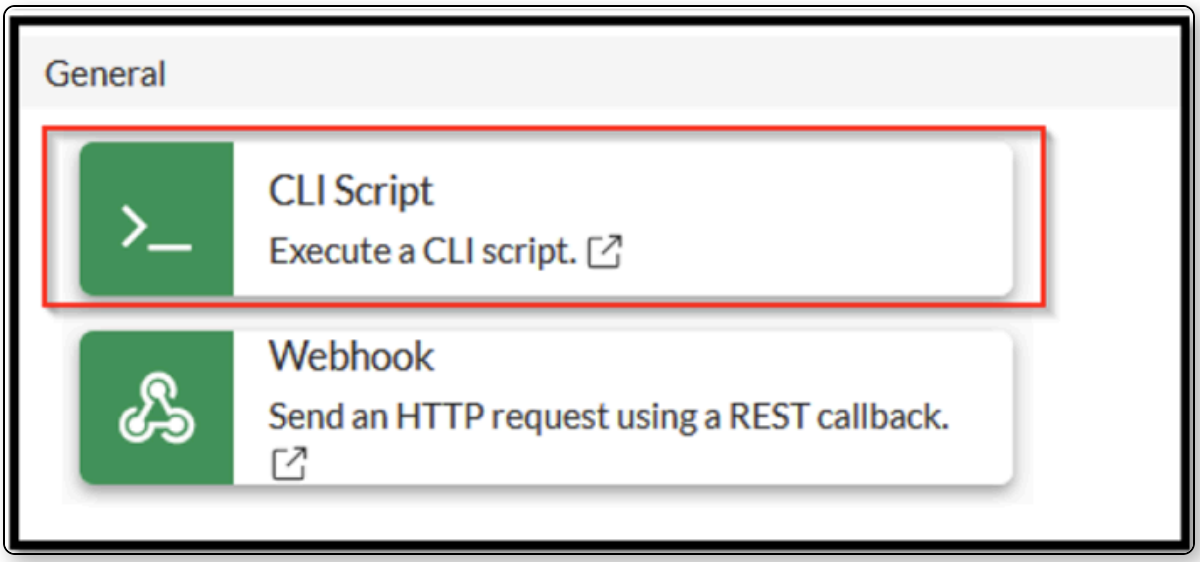




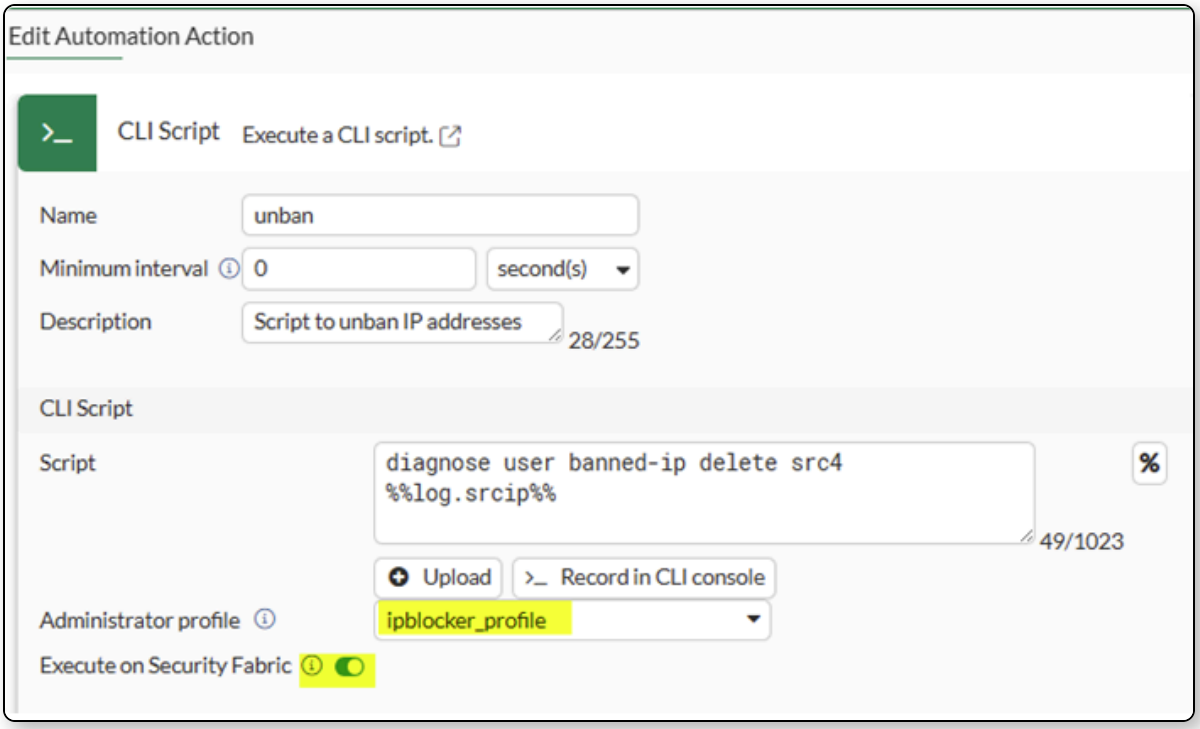
- Click on “OK”, then click in “OK”, last click on “Apply” selecting “fortindr_unban”.
- Let’s do “Add Action” to this Automation Stitch. Click in “Add Action” then click in “Create”:



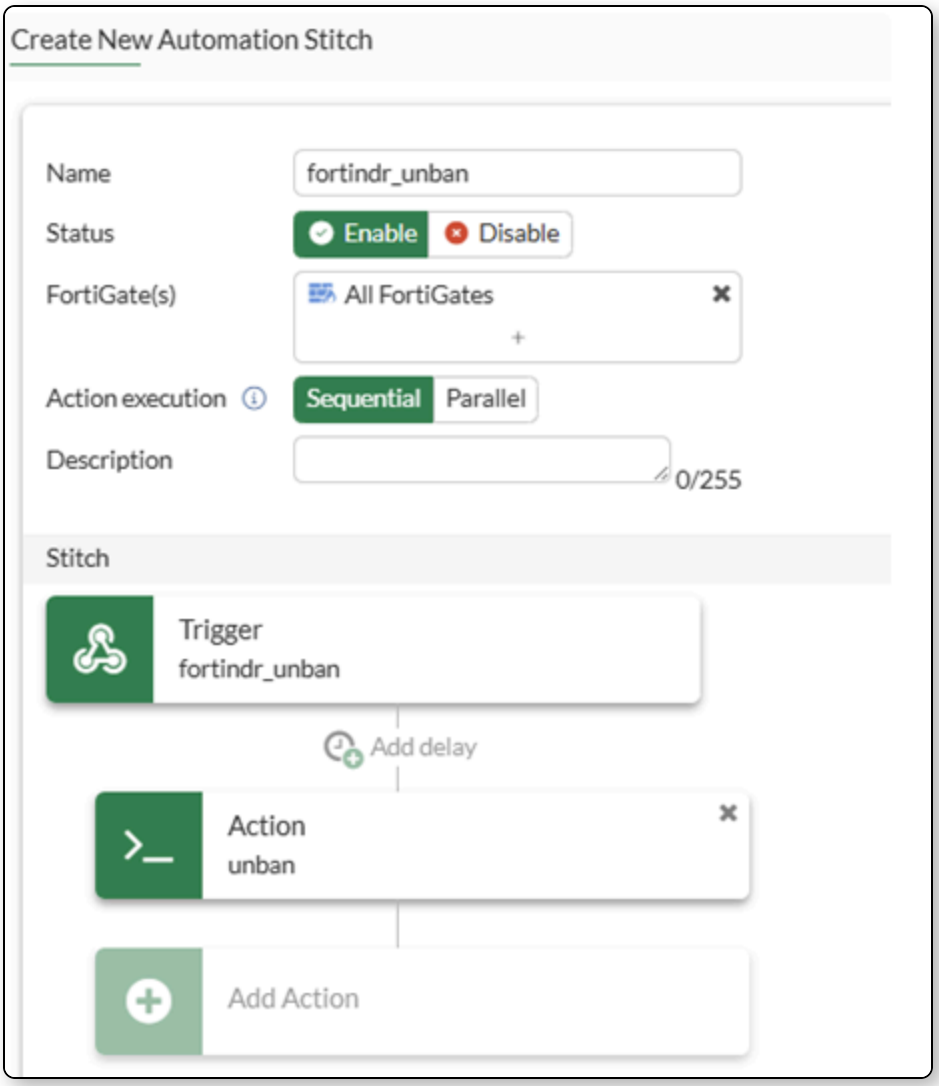
- Select “CLI Script”:



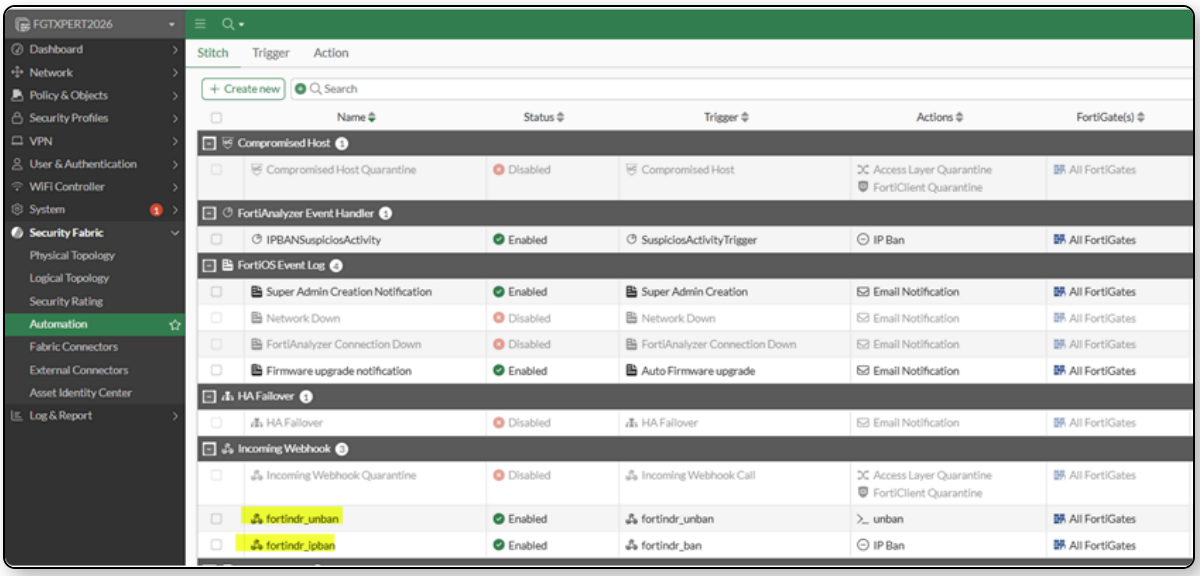
- Complete with the following information this action.



- Click “Ok” , click over “fortindr_unband” and “Apply” and check data:



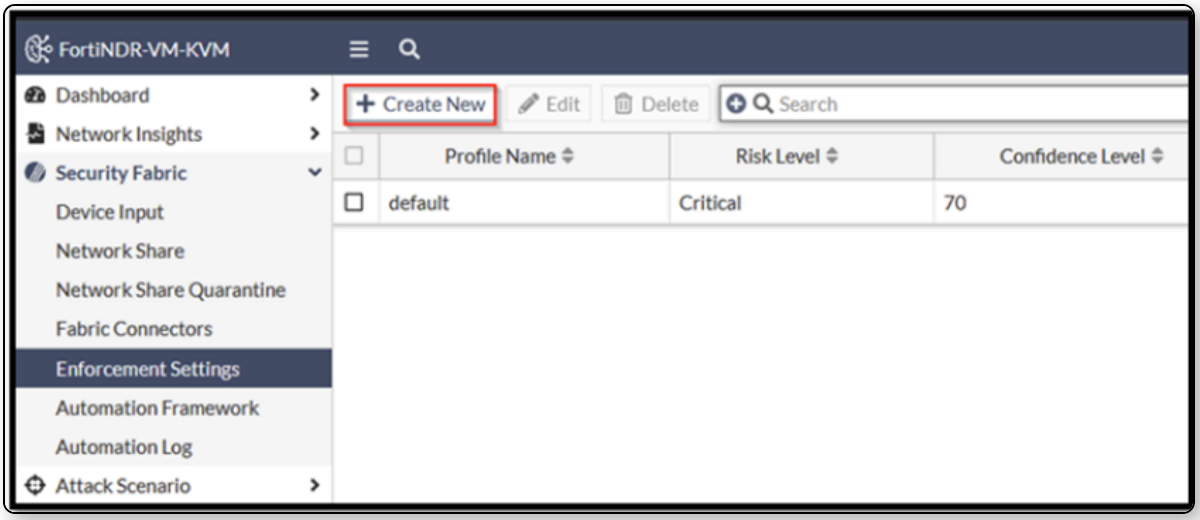
- Click “Ok” to save the Stich configuration.
- Refresh the screen, and you should see both incoming webhooks.
- Ensure the result matches the screenshot:



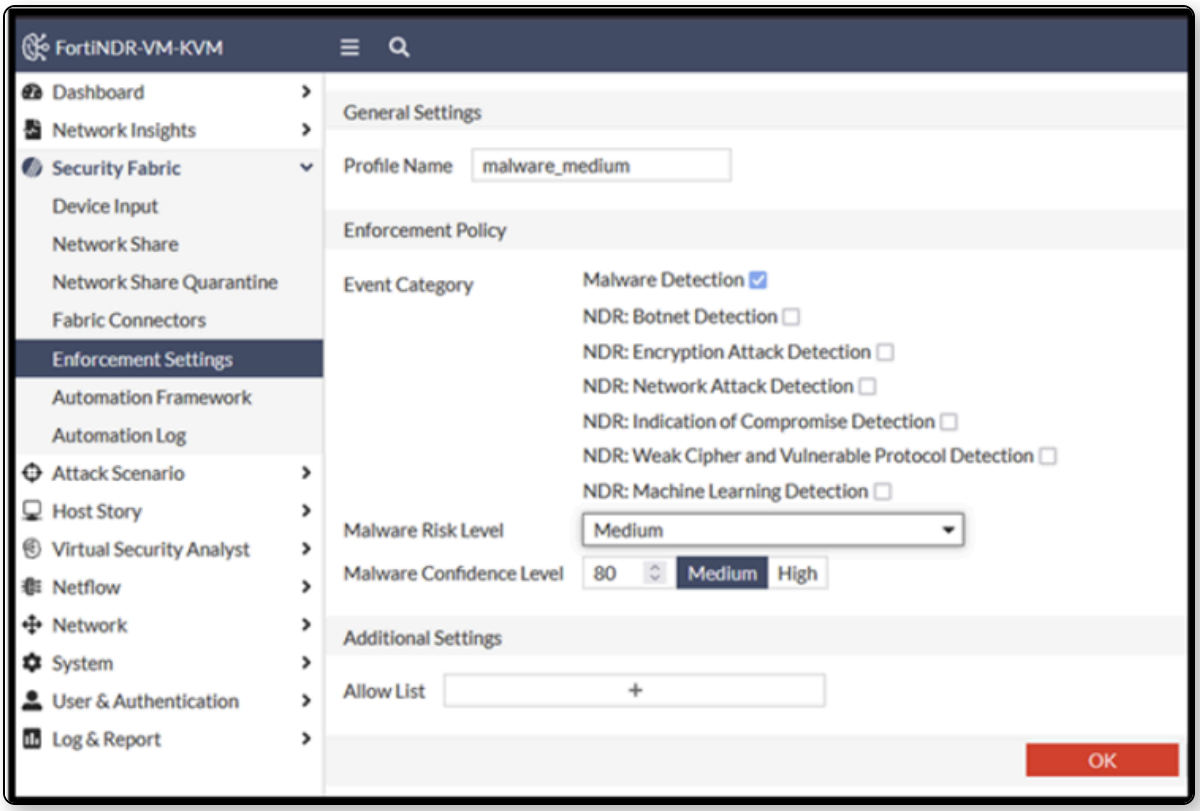
e) FortiNDR Automation Configuration.

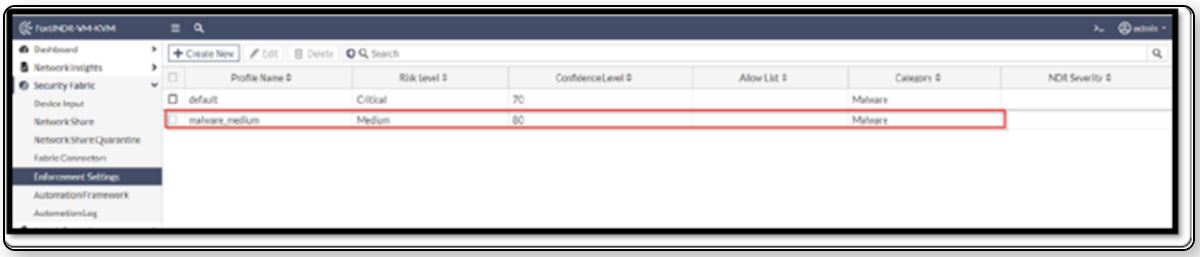
Now that we have configured everything necessary in Fortigate, we will configure the FortiNDR side to establish a remote connection requesting the blocking of an IP once the trigger is obtained.

- Login to FortiNDR via HTTPS and go to “Security Fabric → Enforment” Settings.
- Click on “Create New” to create the new enforcement.

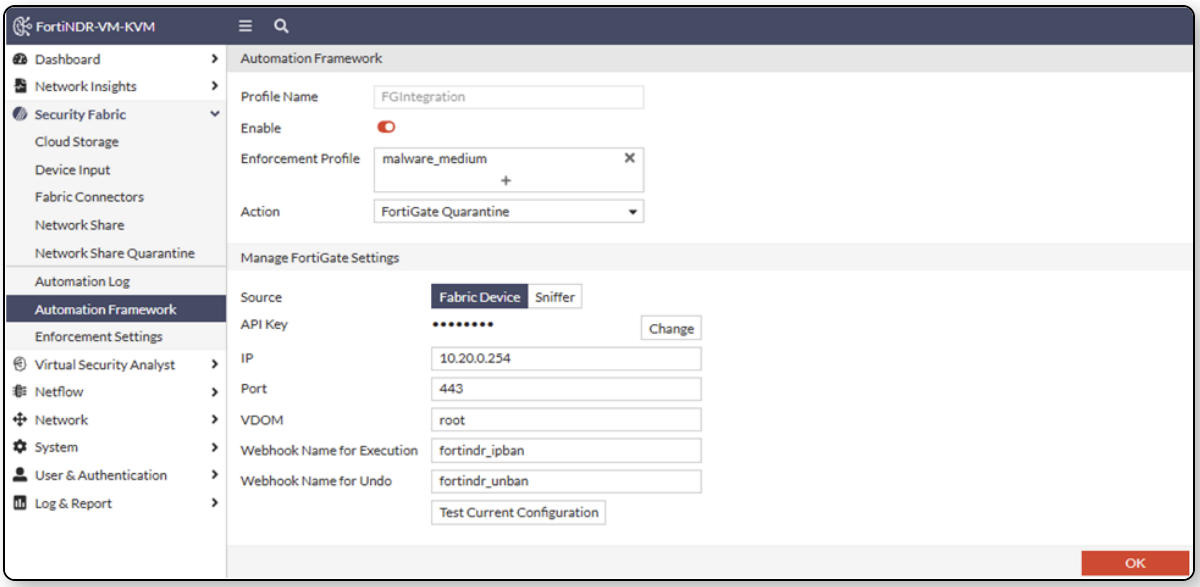


- Complete the following information and click “Ok”:

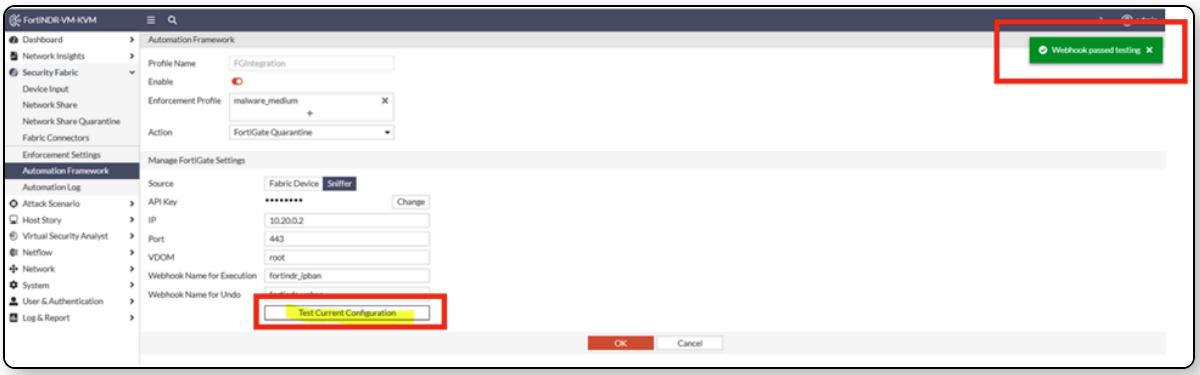




- Now, go to “Security Fabric → Automation Framework”, click “create new” and complete with the following information:



- Test this configuration. Go to “Security Fabric → Automation Framework”, select the newly created profile, click edit, and then “test the current configuration".



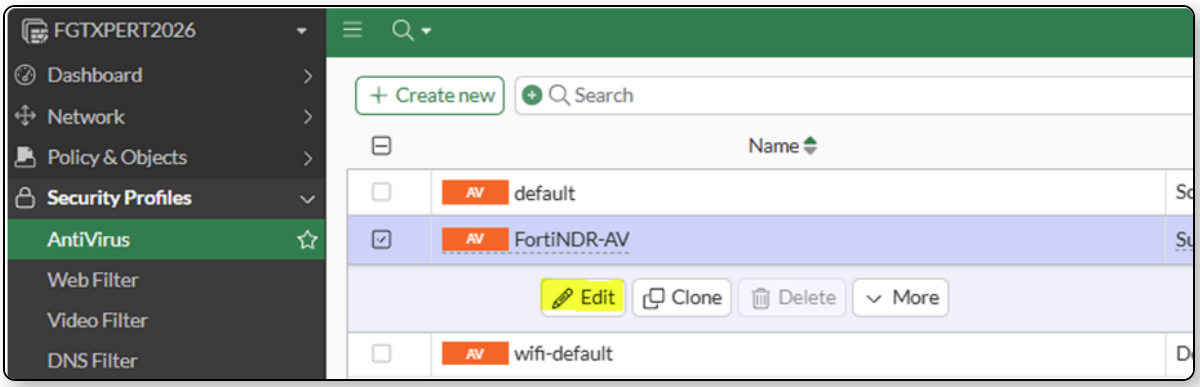
- Now, login to Fortigate via HTPPS and go to “Security Fabric → Automation → Stitch”.
- Type “ndr” in the search bar and ensure the result matches the screenshot, in particular, “Trigger Count” > 1 for both entries.



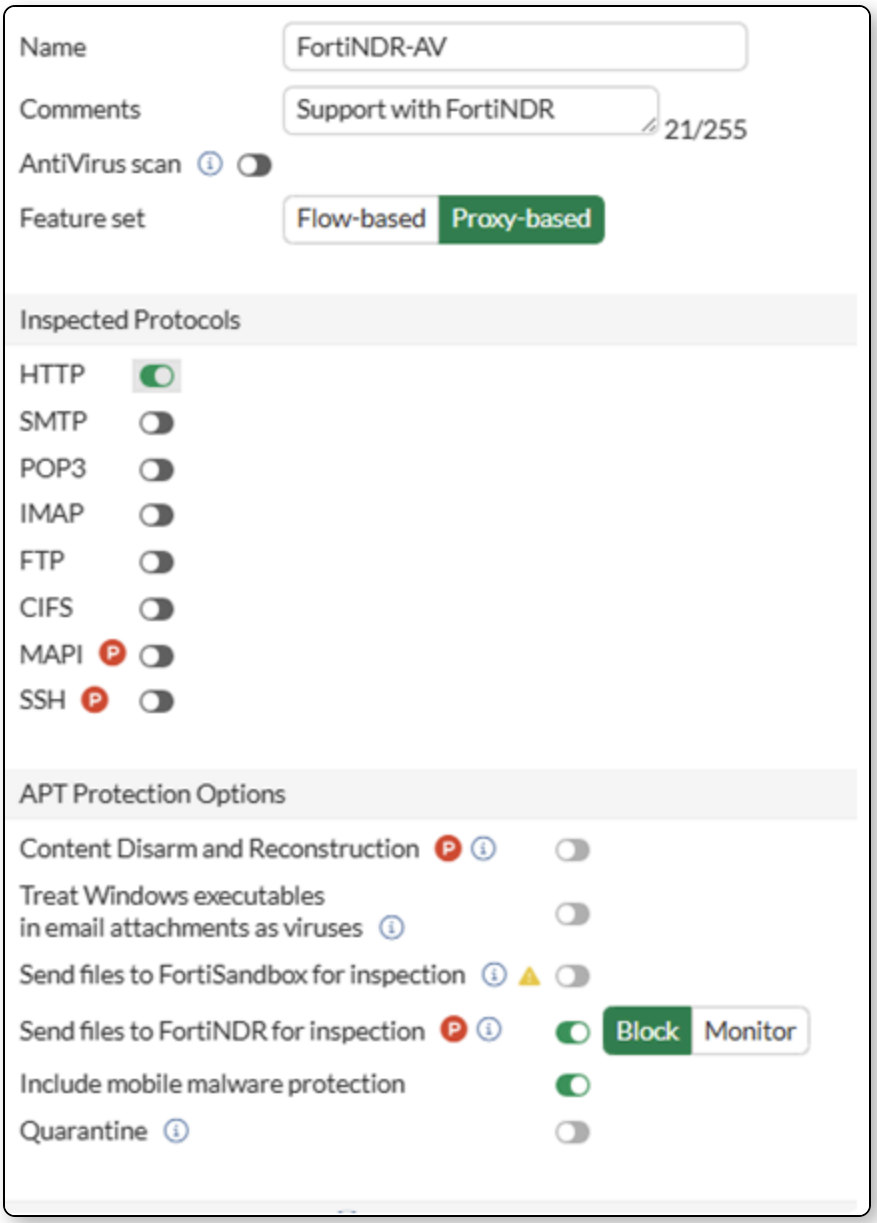
f) Malware Inline Blocking with FortiNDR.

Fortigate inline blocking was proposed to support very fast integration and veredict retrieval from FortiNDR which can scan the file in sub-seconds.

- First, we need to validate the AV Profile Configuration. Log in to FortiGate via HTTPS and go to “Security Profiles → Antivirus”, select “FortiNDR-AV” and edit:



- Change the option “Send files to FortiNDR for inspection” from “Monitor” to “Block” and click “Ok” to save the changes in the security profile.



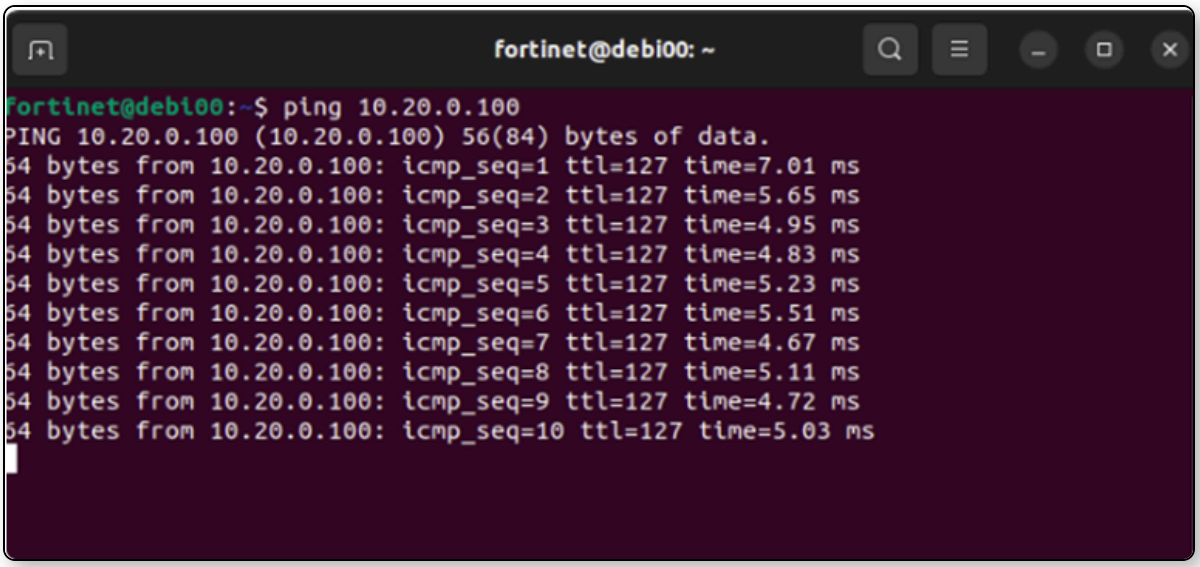
- It's that simple. We have configured Fortigate to retain the session until we receive a result from the NDR's analysis.
- FortiNDR timeout setting. Configuring the timeout time in the NDR for the fortigate is good practice. Log in to FNDR via SSH and execute the following command:
- config system fortigate settings set timeout 20 set block-risk-level low set block-confidence-level low end
- You could use the CLI option through the GUI as well.



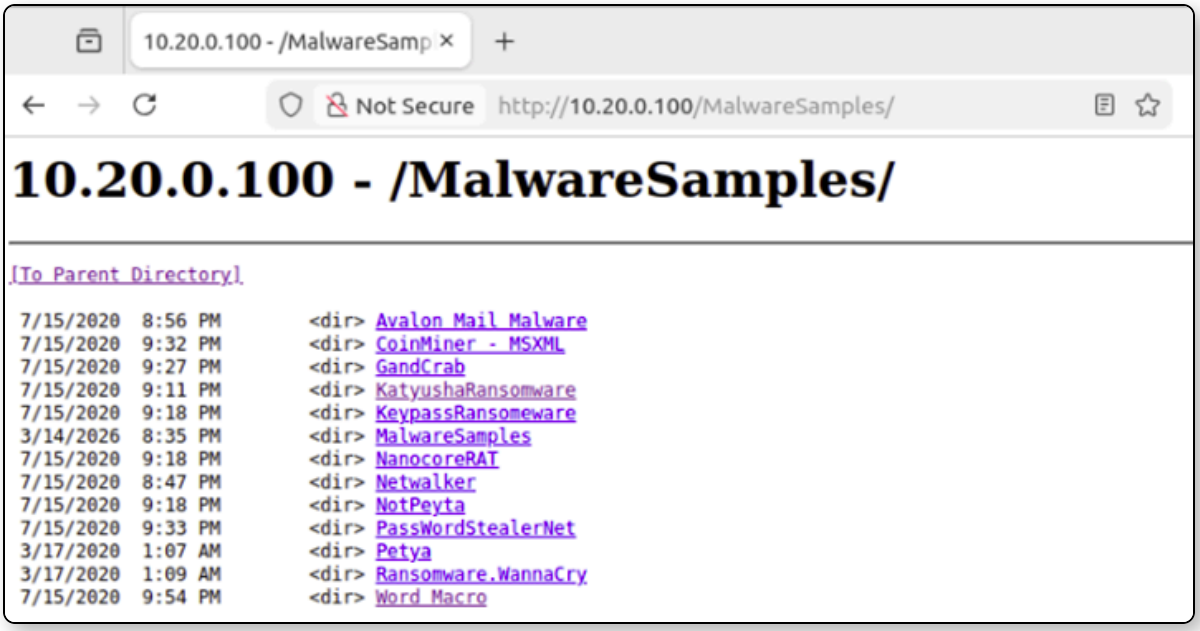
- You can execute “show” to review the configuration; you should see the following output:

```
FortiNDR-VM-KVM # show system fortigate settings
config system fortigate settings
  set timeout 20
  set block-risk-level low
  set block-confidence-level low
end
```

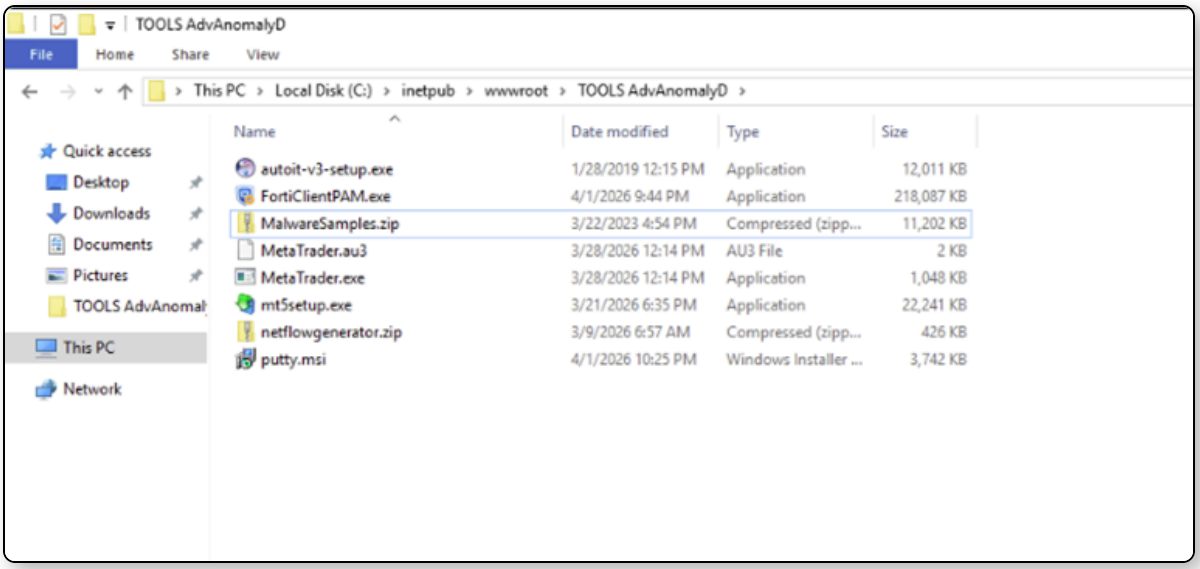
- HTTP/HTTPS Malware detection. Now that we have configured everything necessary, we will perform a test by downloading malware.
- Open and login to “Attack” VM, Open a terminal and run a ping to the IP 10.20.0.100.



- Now, Open Firefox and go to http://10.20.0.100.



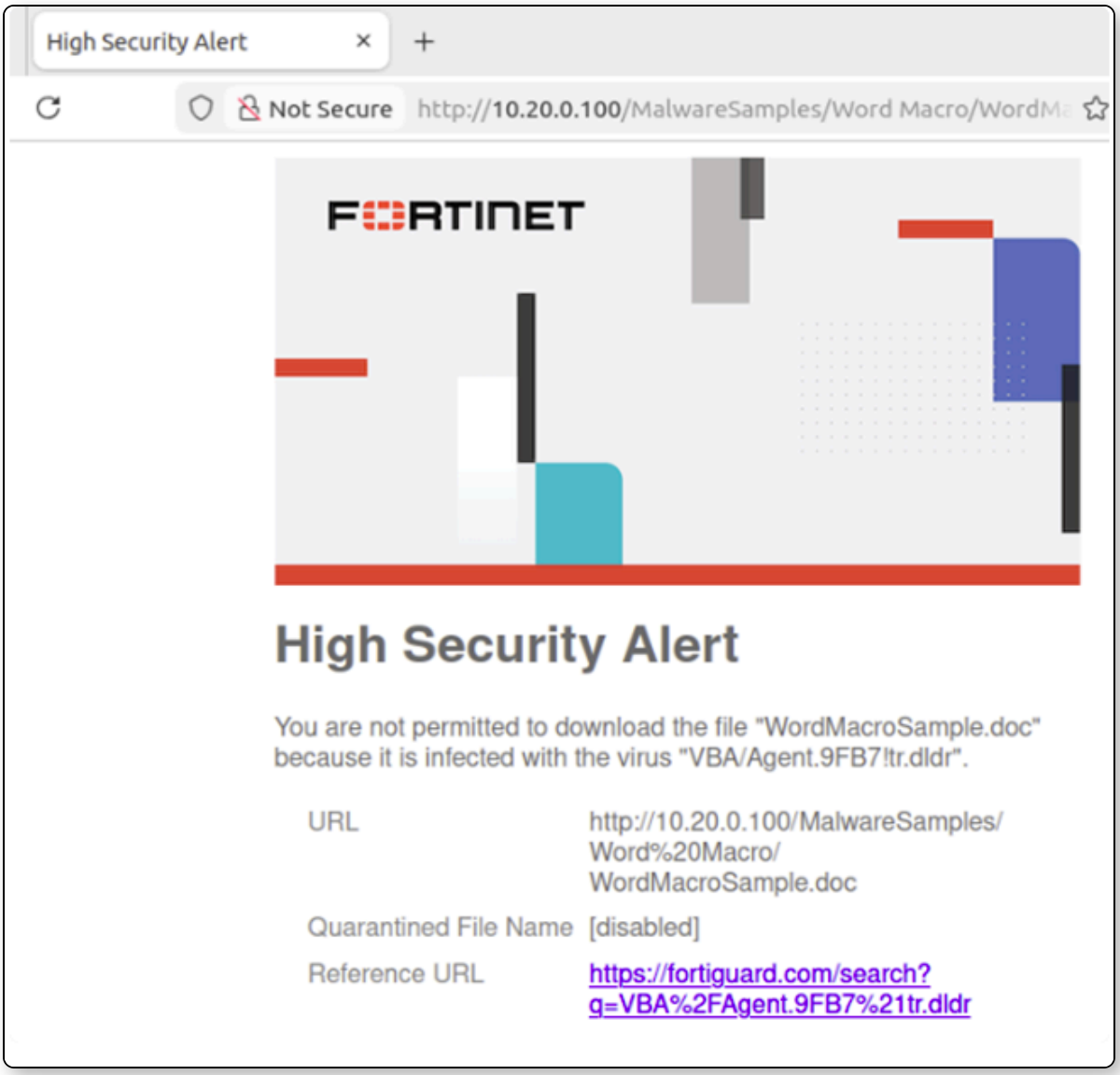
- You can go in "File Server" to the next path for unzip the malware samples.



- We can click in “Word Macro” folder and download “WordMacroSample.doc”.

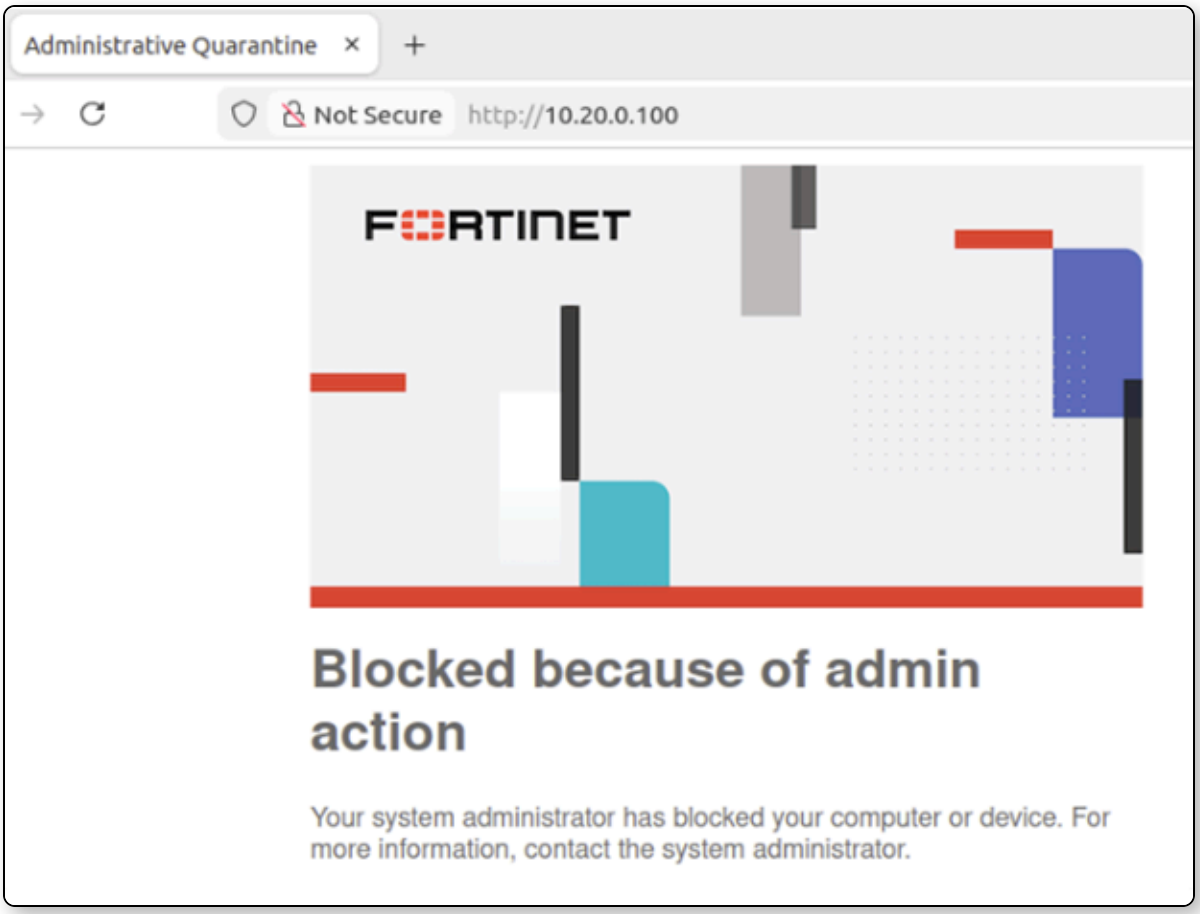


- You should get the following block page:



- Now, open a new TAB in the Firefox browser and try to go to http://10.20.0.100.

- You should get the following block message from the Fortigate.

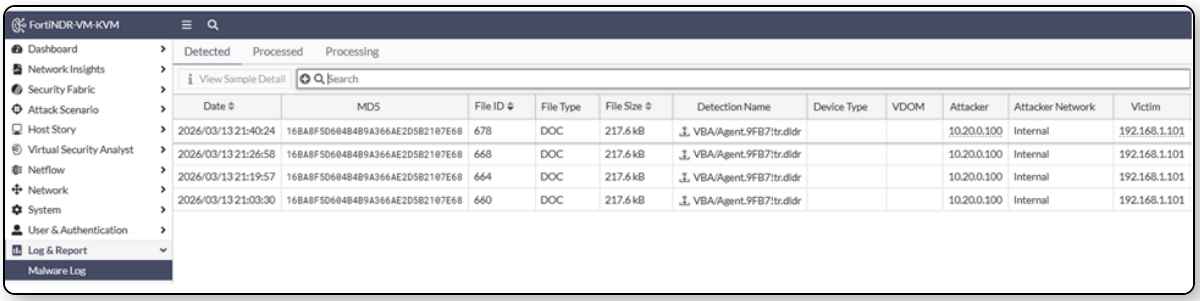


- Do you remember the ping that we left running? If you look again, you will realize that you no longer have a response from the IP 10.20.0.100.

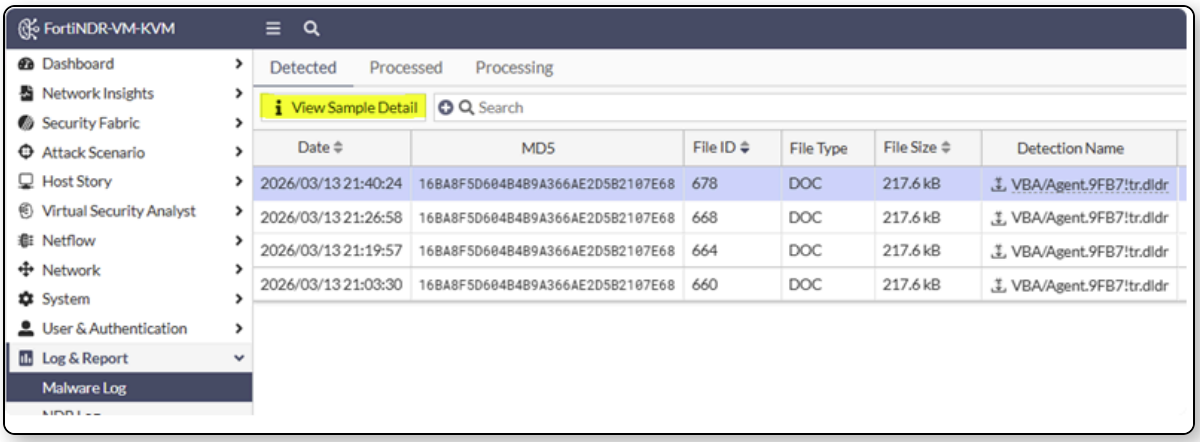
```
64 bytes from 10.20.0.100: icmp_seq=143 ttl=127 time=5.57 ms
64 bytes from 10.20.0.100: icmp_seq=144 ttl=127 time=4.94 ms
64 bytes from 10.20.0.100: icmp_seq=145 ttl=127 time=5.33 ms
64 bytes from 10.20.0.100: icmp_seq=146 ttl=127 time=6.16 ms
64 bytes from 10.20.0.100: icmp_seq=147 ttl=127 time=5.35 ms
64 bytes from 10.20.0.100: icmp_seq=148 ttl=127 time=124 ms
64 bytes from 10.20.0.100: icmp_seq=149 ttl=127 time=5.74 ms
64 bytes from 10.20.0.100: icmp_seq=150 ttl=127 time=4.83 ms
^C
--- 10.20.0.100 ping statistics ---
224 packets transmitted, 150 received, 33.0357% packet loss, time 224994ms
rtt min/avg/max/mdev = 4.116/12.878/268.604/34.060 ms
fortinet@debi00:~$
```

- FortiNDR Detection Review. As you could see from “Attack” VM we no longer have access to the IP 10.20.0.100.
- Now we are going to check what happened in the FortiNDR.

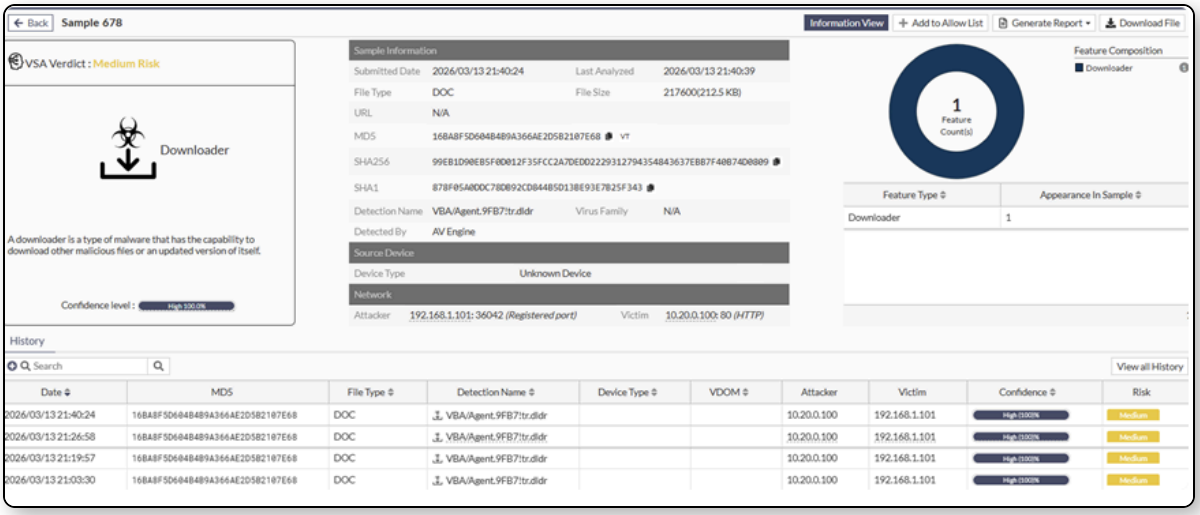
- Login to FNDR via HTTPS, and go to “Log & Report → Malware Log”. You should see a new event with the “VBA/Agent.9FB7!tr.dldr” Malware as a detection.



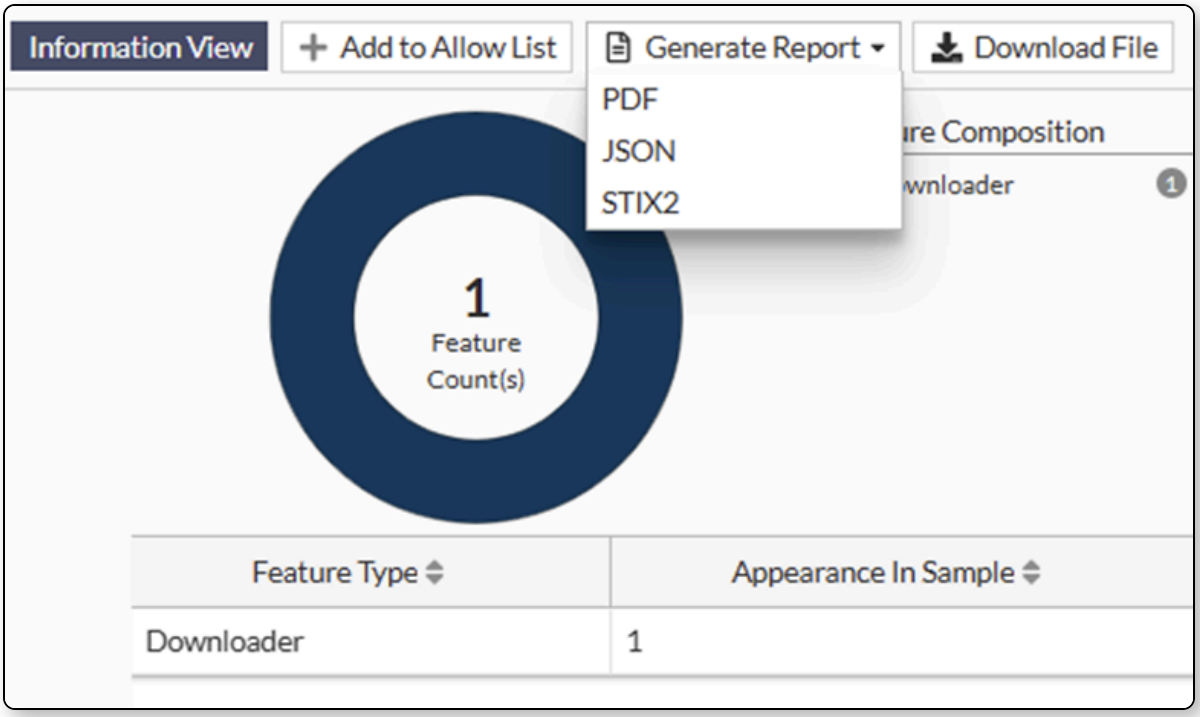
- Click over the event and click on “View Sample Detail”.



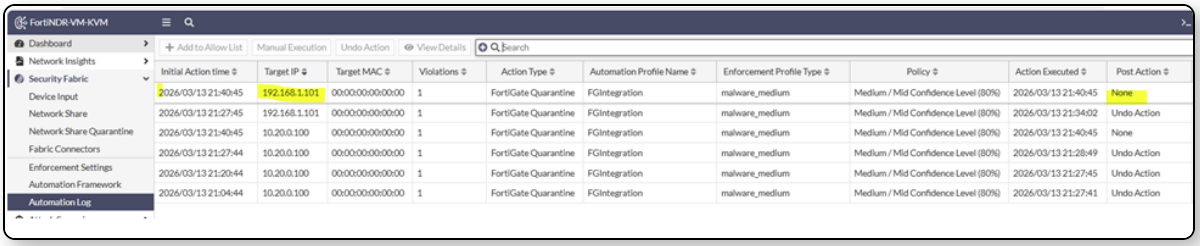
- The report contains a lot of good information from VSA (Virtual Security Analyst).
- Please take a moment to review all the information, such as the submitted Day, File Type, File Size, Hashes, Detection Name, etc.



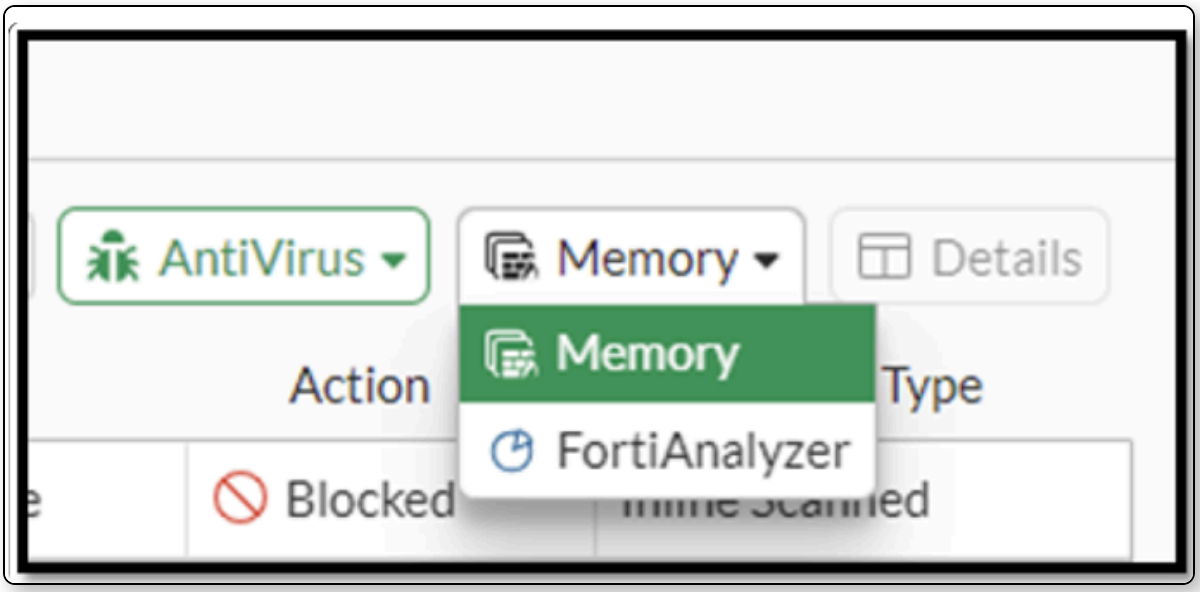
- You can export this report in a PDF, JSON or STIX format.



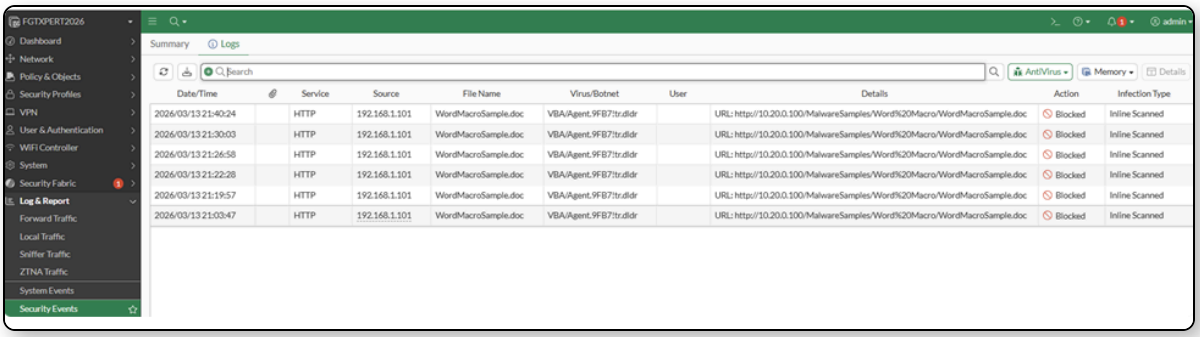
- Now, go to “Security Fabric → Automation Log”. You should see two lines for both IP addresses (Your Source IP should be 192.168.20.13):



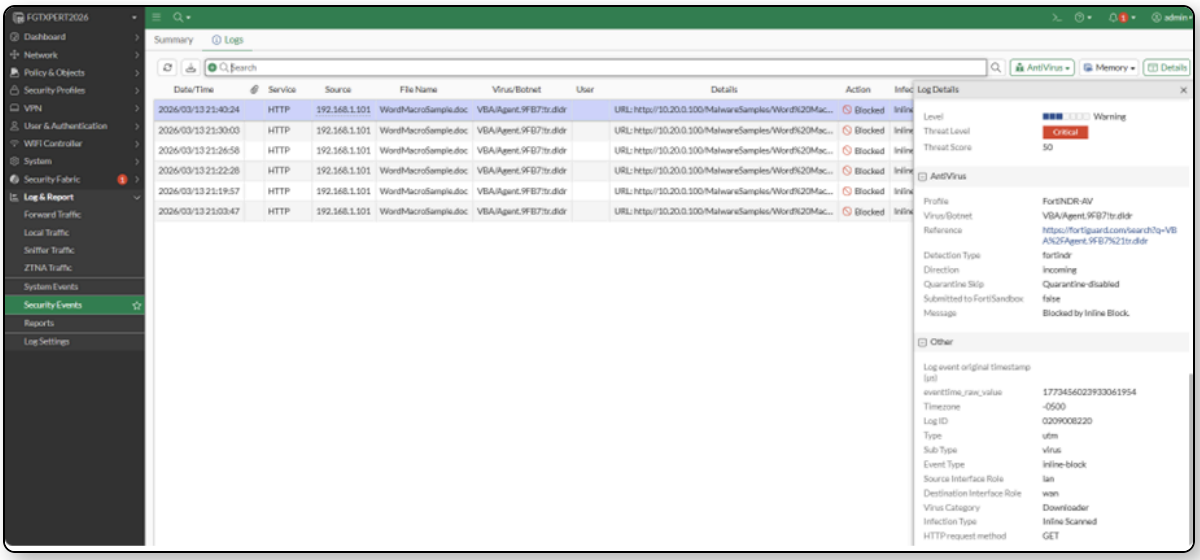
- FortiGate Detection Review. We are going to review the data in FortiGate.
- Login to FortiGate via HTTPS and go to “Log & Reports → Security Events → Select “Antivirus”” and “Memory” in the top right corner.



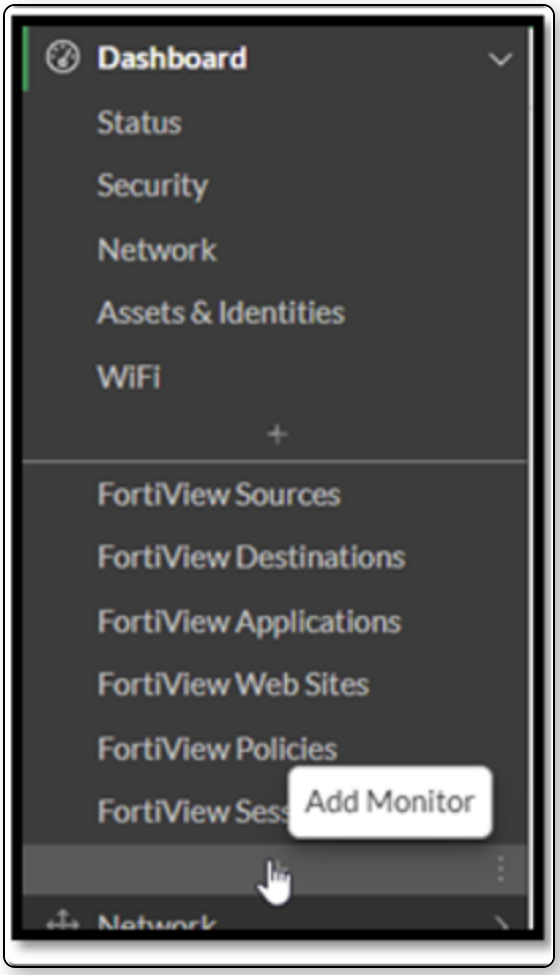
- You should see the security Antivirus event in the list:

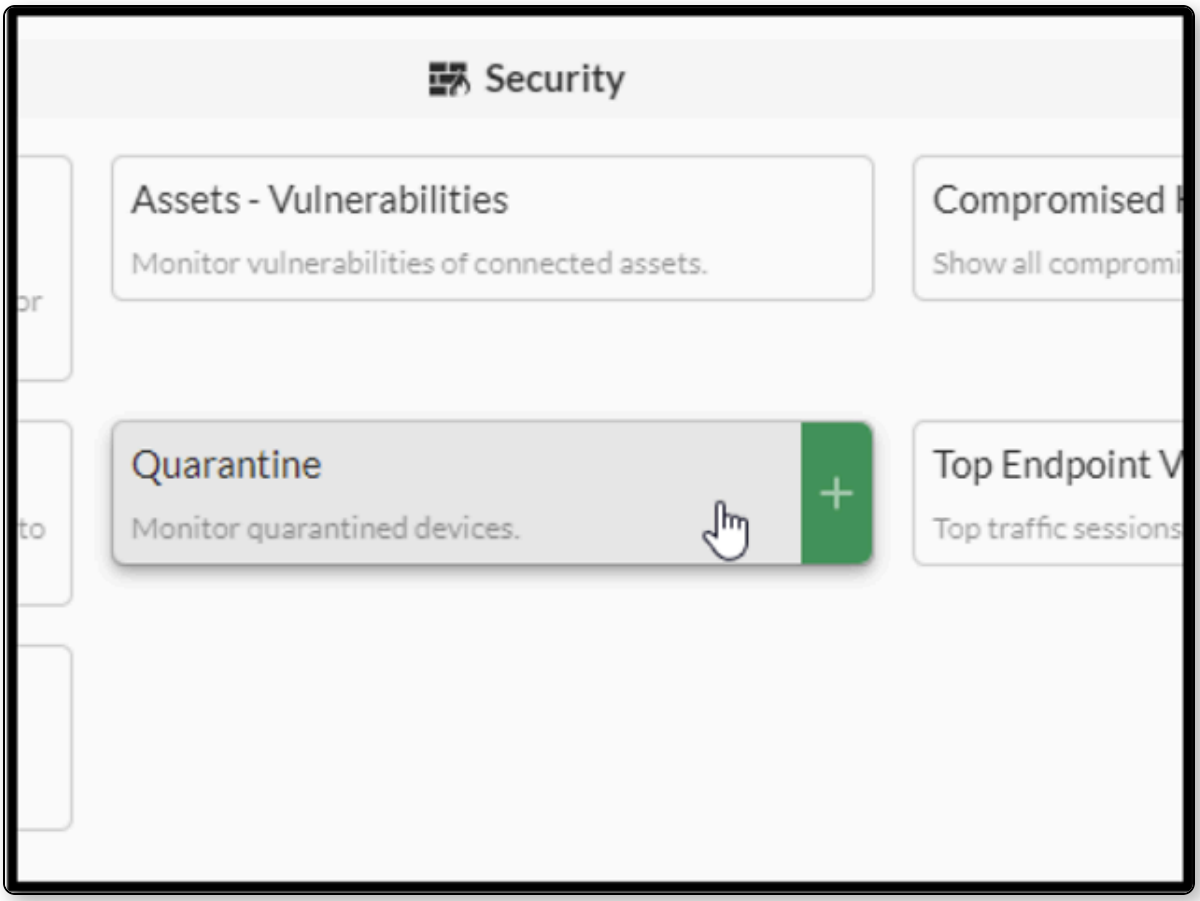


- Double-click on this event to review the details. As you can see the connection was blocked by the inline policy.

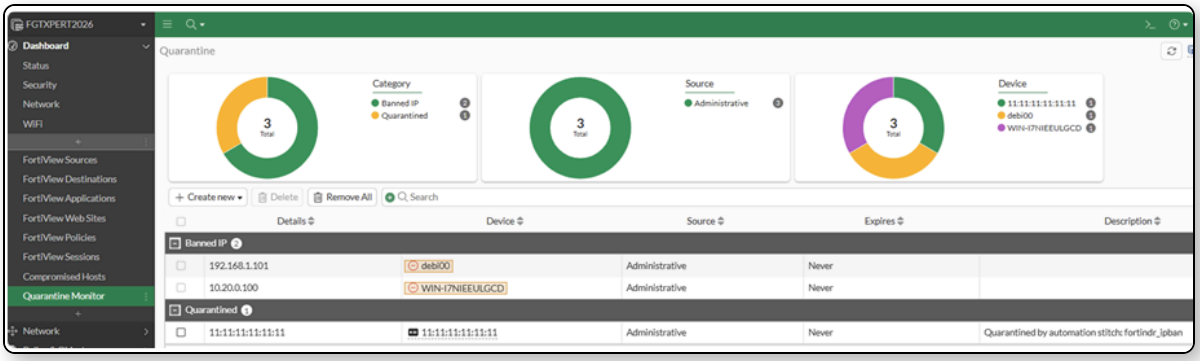


- Now, go to Dashboard → Click on “+” (add monitor) option Under “Security” select “Quarantine”.

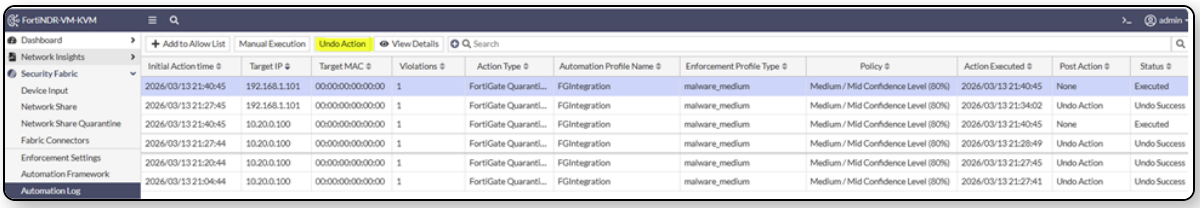




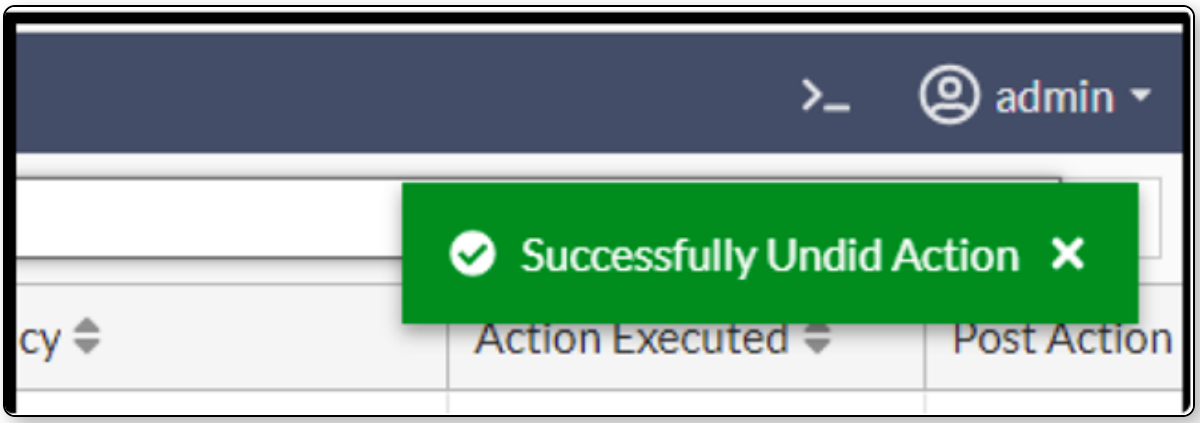
- Left default options and click “Ok”. You have now enabled the Quarantine monitor dashboard, and you should see the Banned IPs we use for NDR detection.



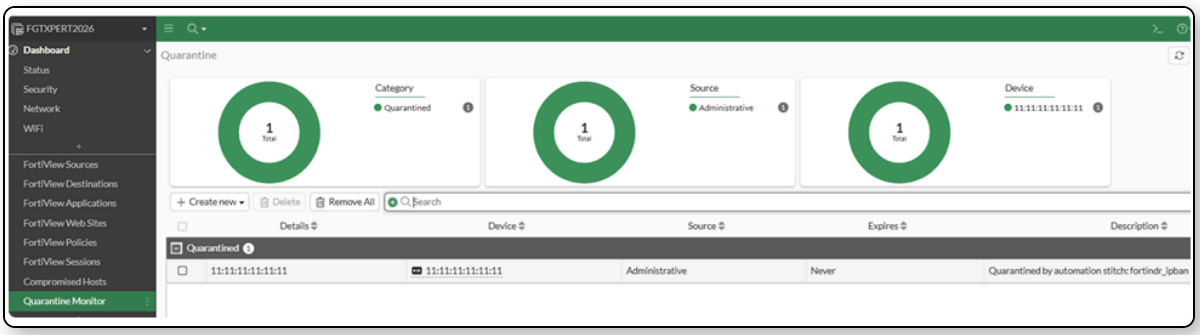
- Unblocking IP addresses from FortiNDR. Now, we will unlock the IPs to continue with the next lab.
- Login to FortiNDR and go to “Security Fabric → Automation Log”, Select the first line and click on “Undo Action”.



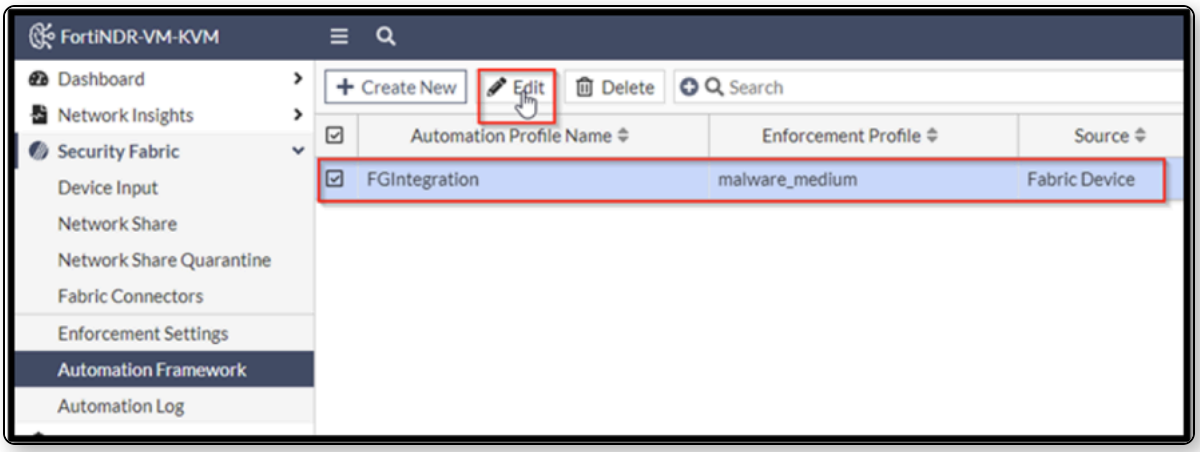
- Do the same for the second line, you should see a green box and a change to the “Post Action” field to “Undo Action”.



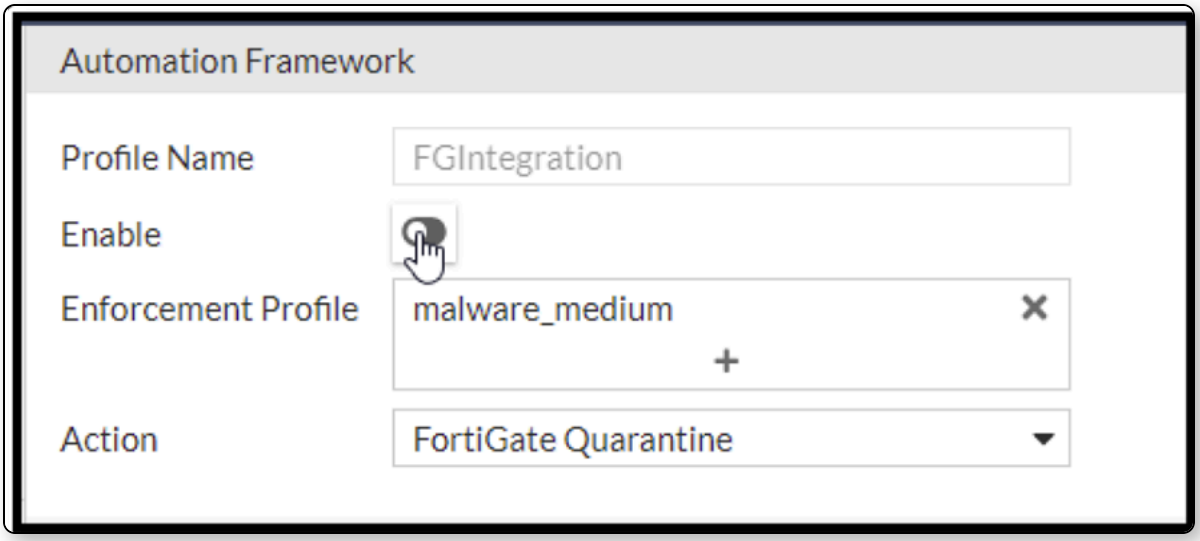
- Login to FortiGate via HTTPS and go to “Dashboard → Quarantine Monitor”.
- You should not see any crash logs, as we requested their removal from the NDR. If you see any logs, you can also remove them from Fortigate.



- Finally, we will disable the automatic response to not generate blockages in other laboratories.
- For this, go back and login to FortiNDR and go to “Security Fabric → Automation Framework”. Click on “FGIntegration” check box and click on “Edit”.



- Click the Enable checkbox to DISABLE the Automation Framework and click the “Ok” button to save changes.

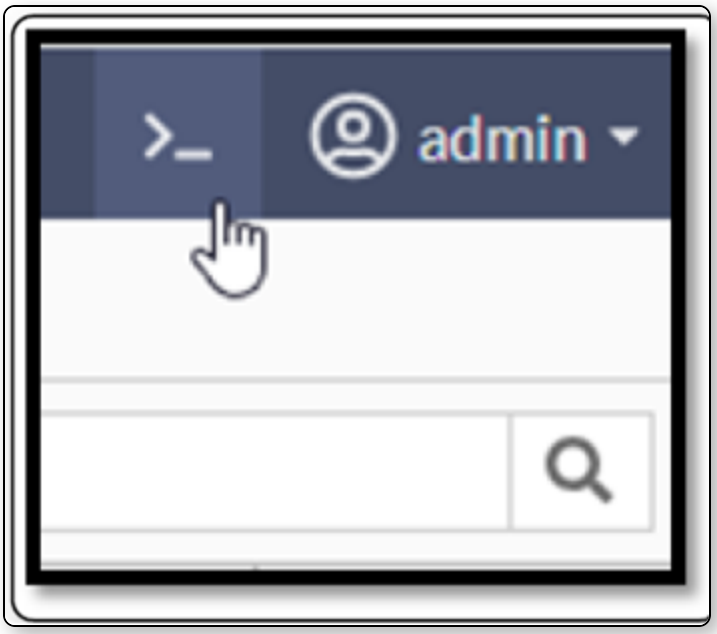




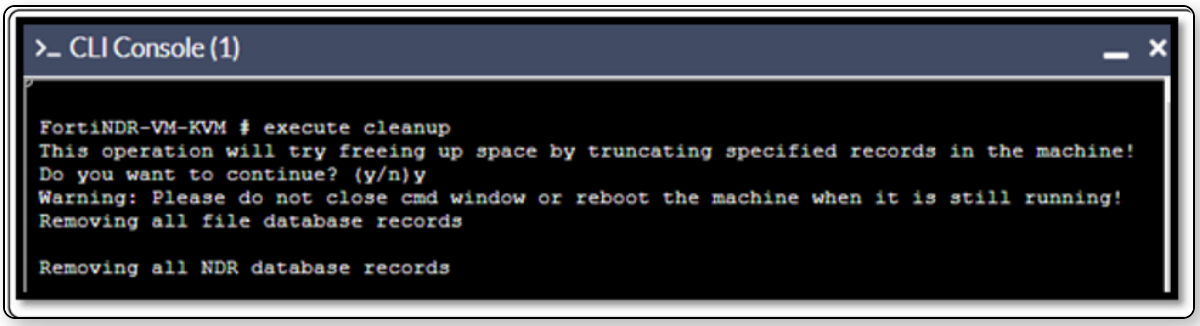
g) FortiNDR Machine Learning in Netflow.

We know that we will obtain the maximum detection capabilities of a FortiNDR when we implement it in SNIFER mode, connecting it directly to a network port or using protocols such as RSPAN (Remote Switched Port Analyzer). However, it's good to know that FortiNDR offers an integration alternative via NetFlow, which will allow us to identify Netflow botnet, Spam, Phishing, Tor, Proxy traffic detections and anomaly network behavior.

- Clean FortiNDR DB, Log In to FNDR, Open CLI console in the top right corner:



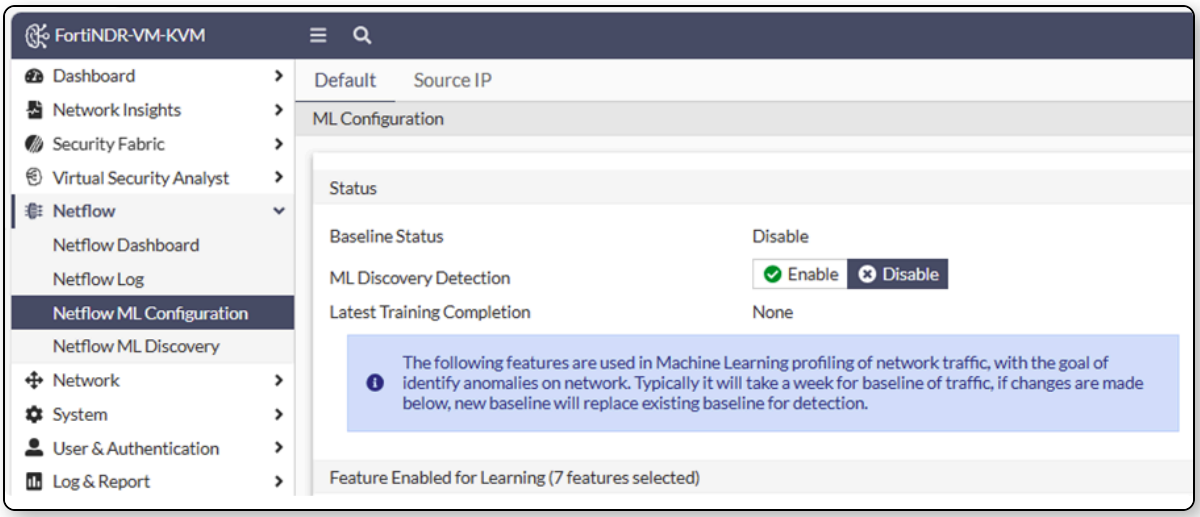
- Execute the command “execute cleanup” and confirm with “y”:
- Note: You can use this commando to restore the FortiNDR´s data base: "Execute db restore"



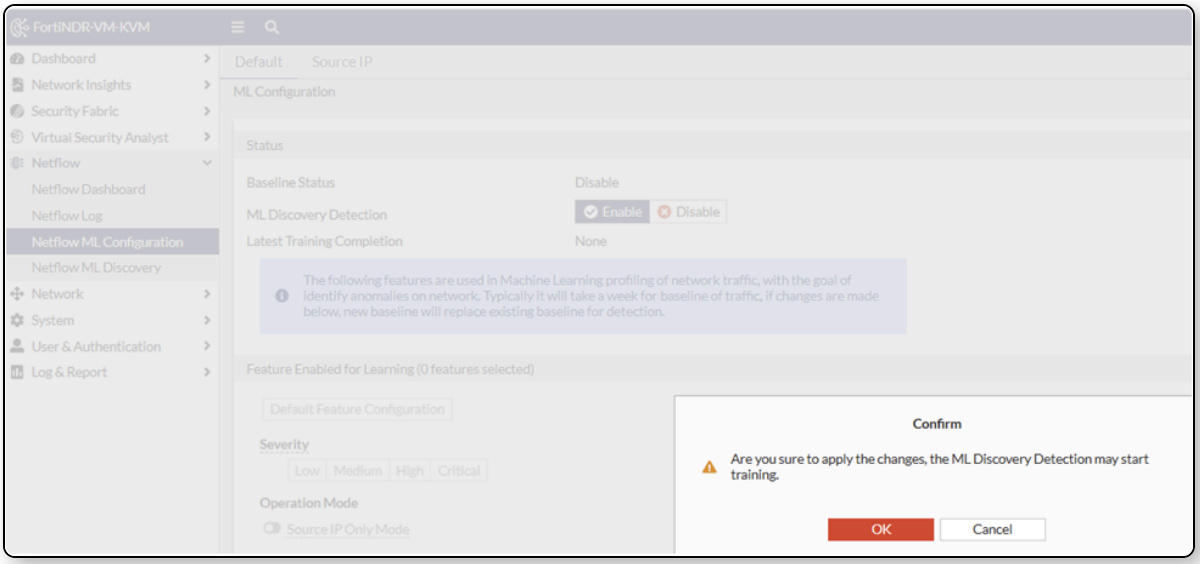
- You should get a message indicating the process has finished. The total space value may vary. After this close the CLI screen.



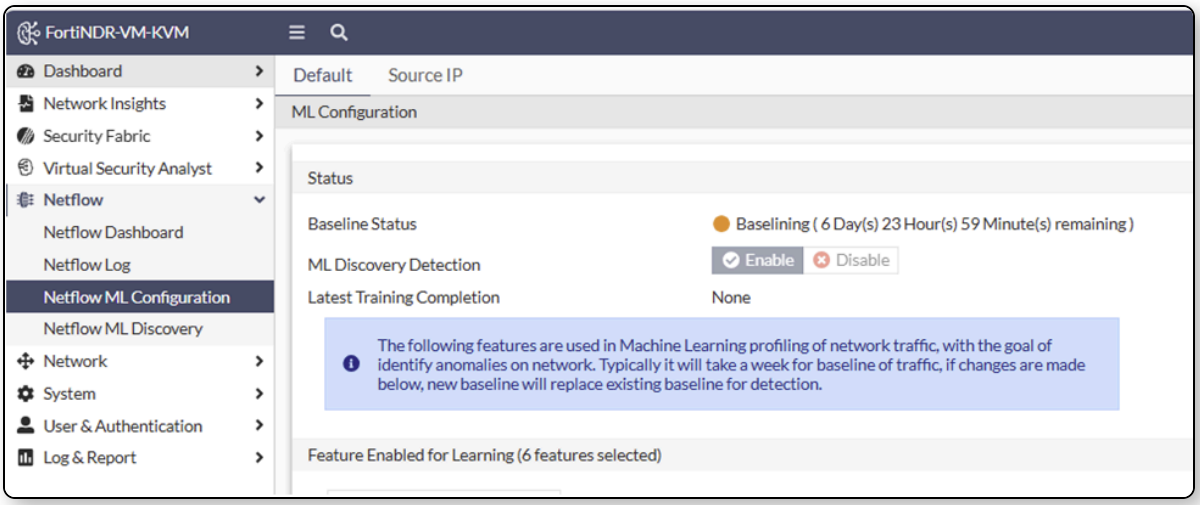
- Enable FortiNDR Netflow baseline. Configure the ML module to establish a baseline, allowing it to generate detections from that point forward.
- In the FortiNDR GUI console, go to “Netflow → Netflow ML Configuration”. Check the status for ML discovery detection; it should be disabled.



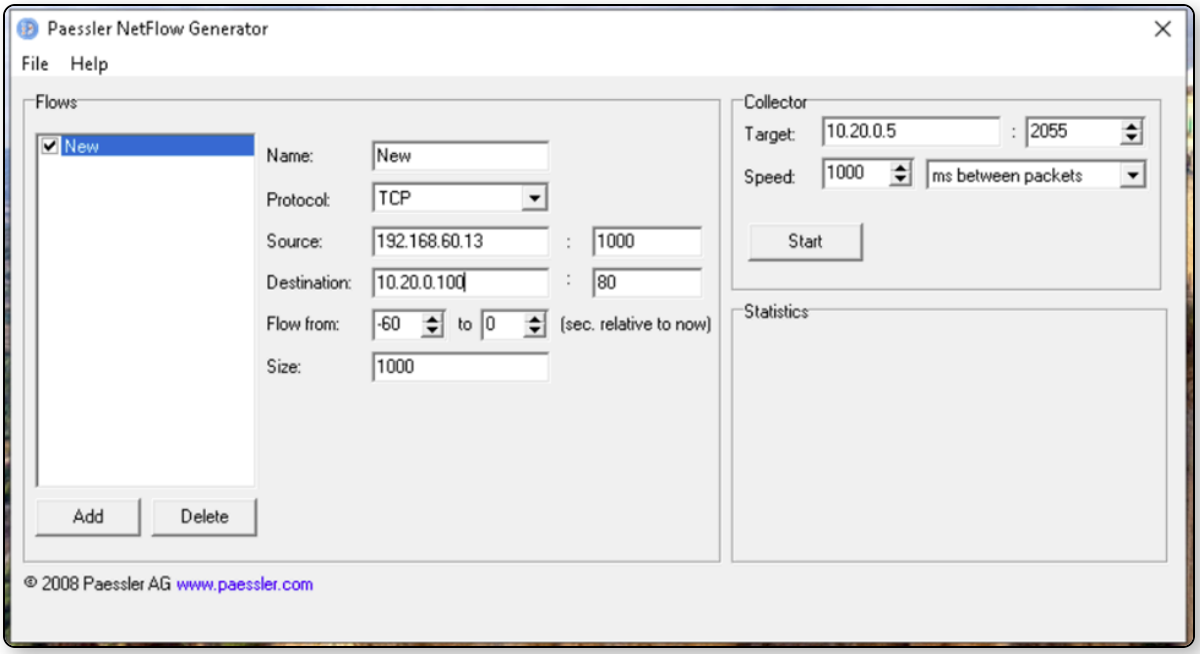
- Enable ML Discovery Detection and click apply. Click ok to confirm.



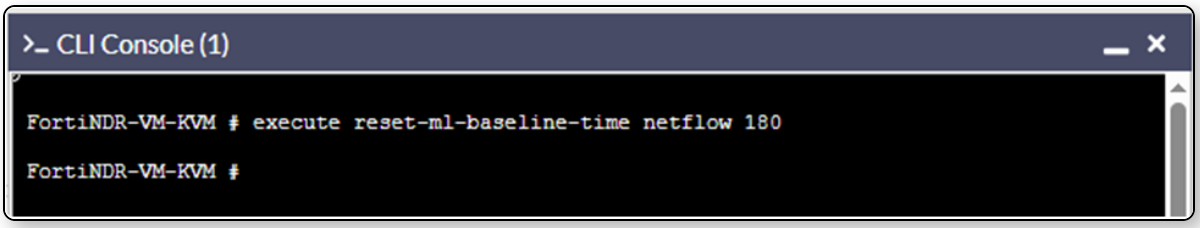
- Baseline status shows as “Initializing Training”:



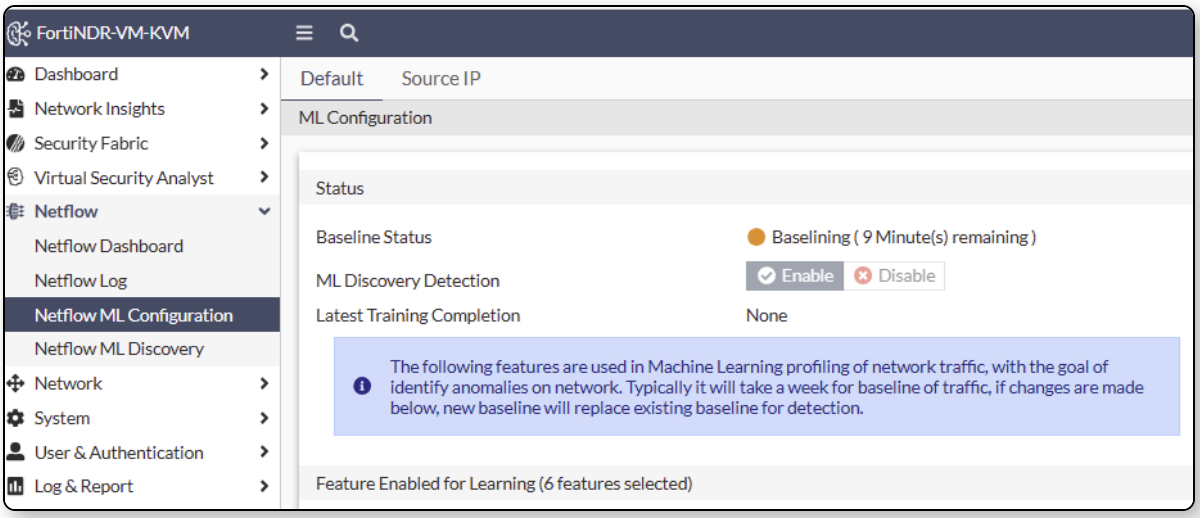
- Let's go to "Victim" devices and open "NetflowGenerator" in folder "Downloads".
- Configure the next parameter and click in "Start".



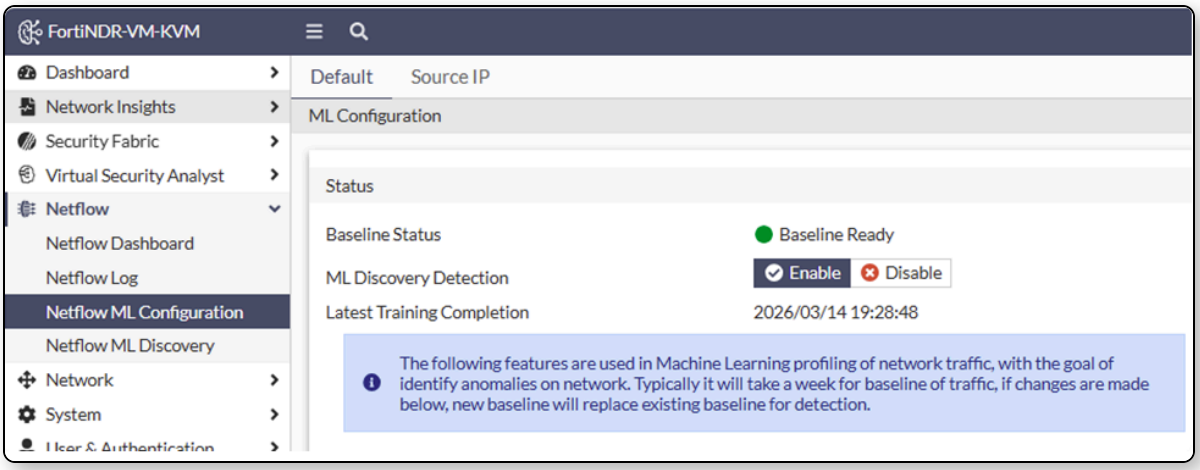
- **Reset baseline time.** Reset the learning time to just 180 seconds (3 min).
- This is very little time in a real environment, keep in mind at least 7 full days is default, but it will depend on the cycles of each company.
- On the NDR CLI console, Write the following command: "exec reset-ml-baseline-time netflow 180":



- Close CLI. Wait one minute and refresh the page.
- A new baseline message shows it will stay creating the baseline during the next two minutes.

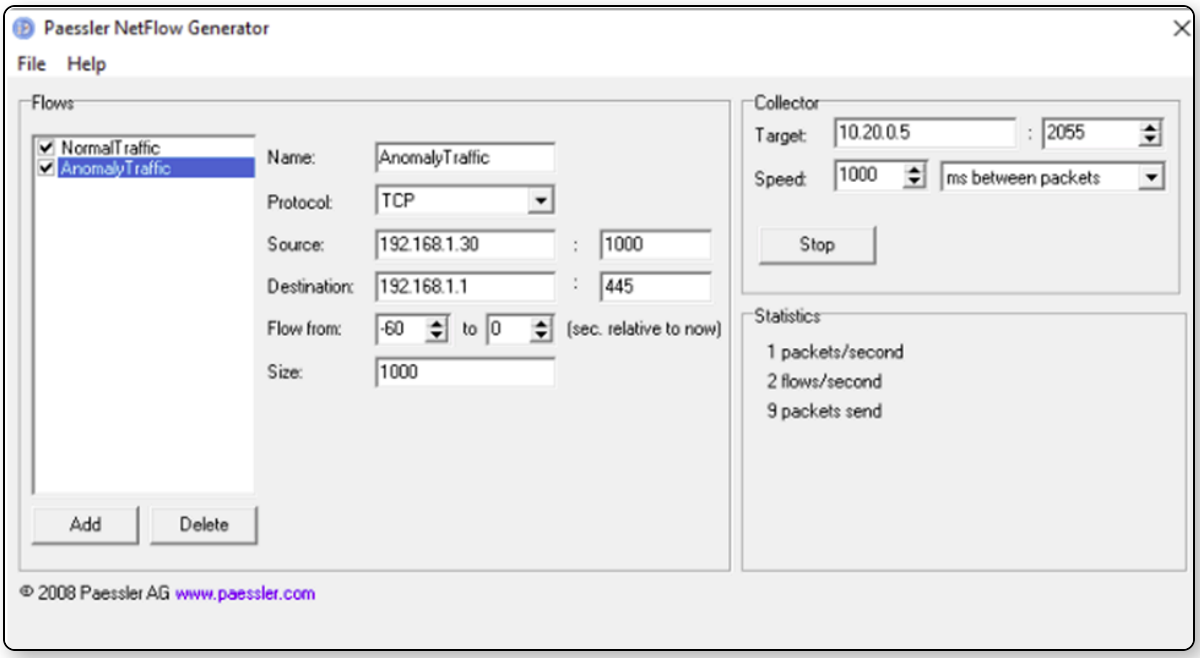


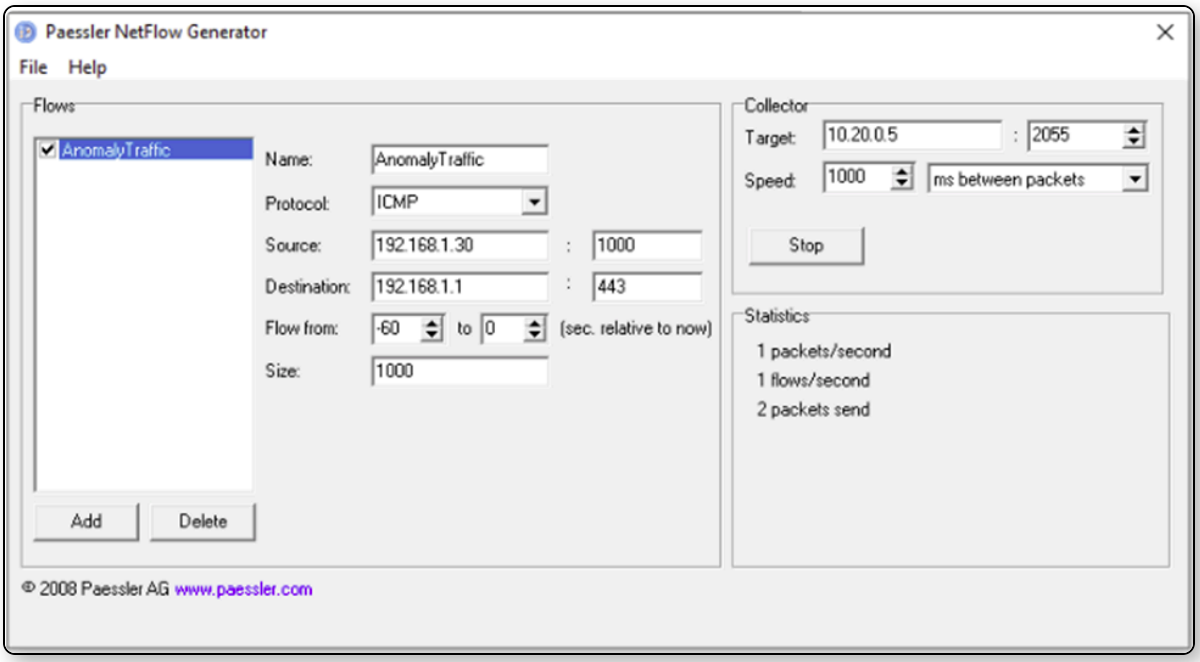
- Wait for a few minutes until “Netflow ML Configuration” is with “Baseline Ready”.
- When “Baseline Ready” stop the “Generator Flow”.



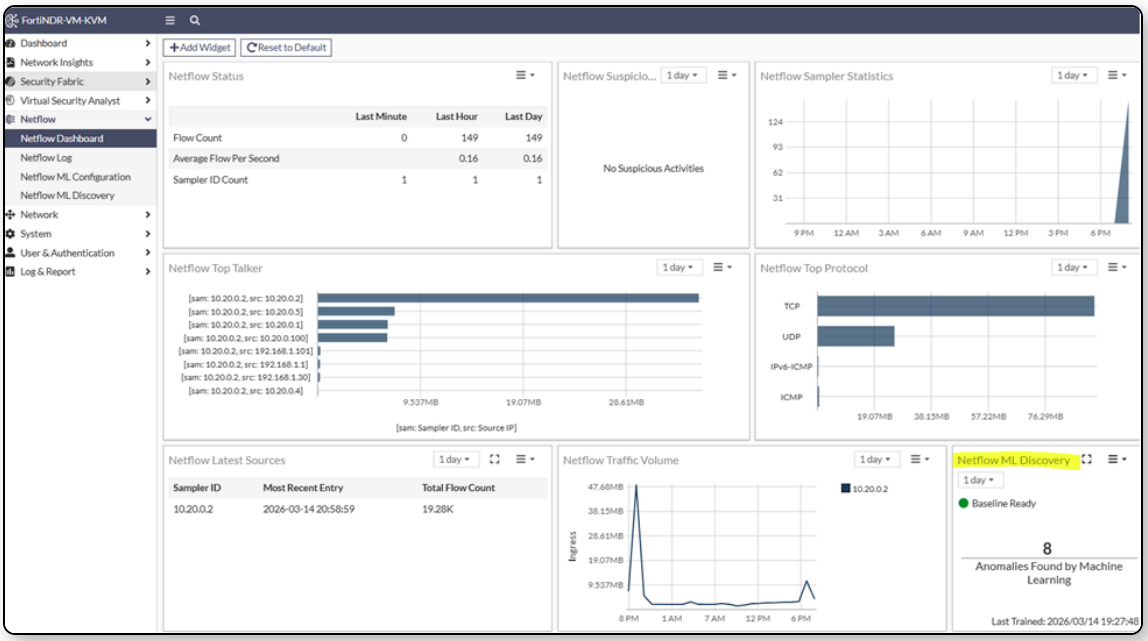
- Again, let’s go to “Victim” and execute “Netflow Generator” with the configuration “AnomalyTraffic” and click in “Start”.

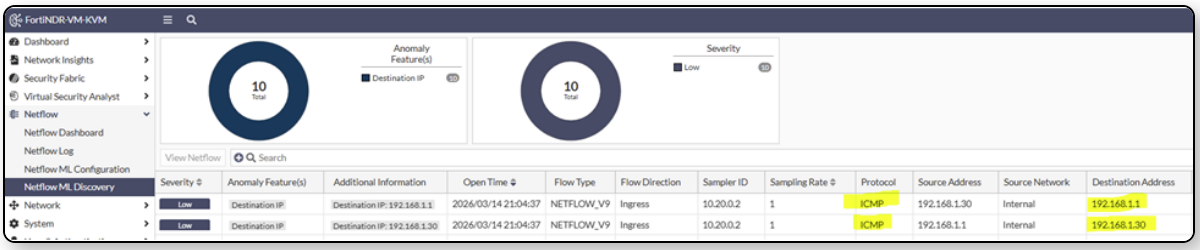
- You can generate a couple of different traffic.



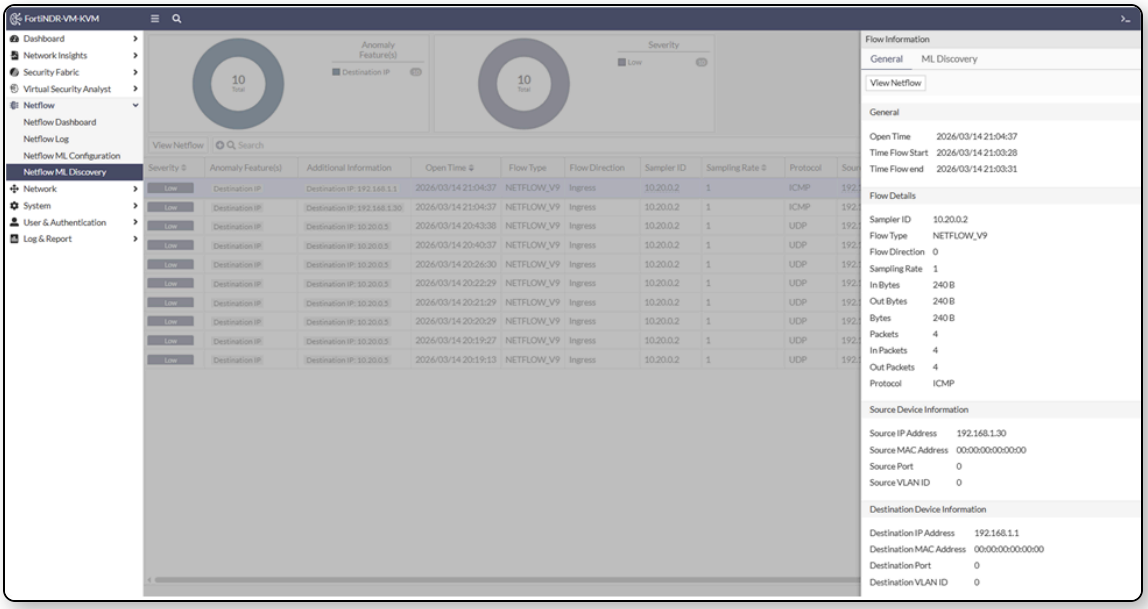


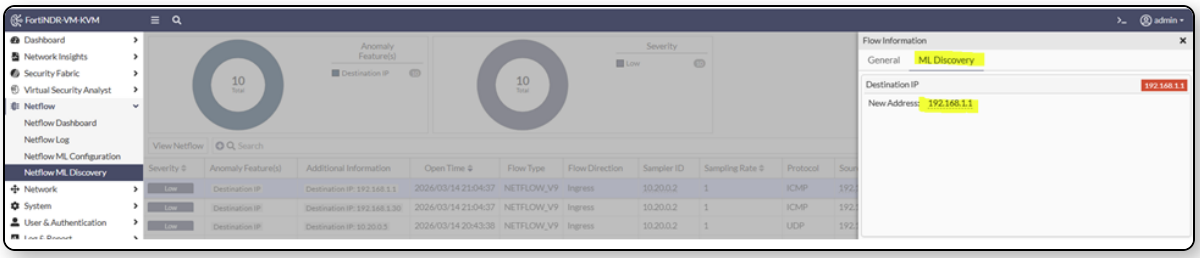
- This configuration allows to generate different traffic learning by “Netflow ML”. Wait a couple of minutes and “Stop” the “Netflow Generator”.
- Review ML Detections. The ML Discovery monitor displays a list of anomalies detected by Machine Learning configuration. Each row is based on a session.



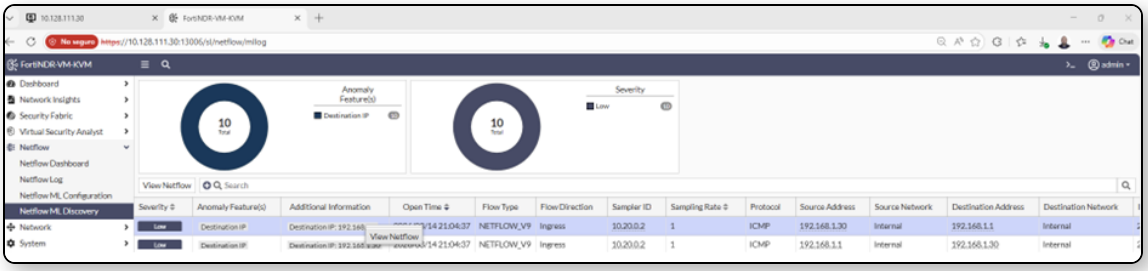


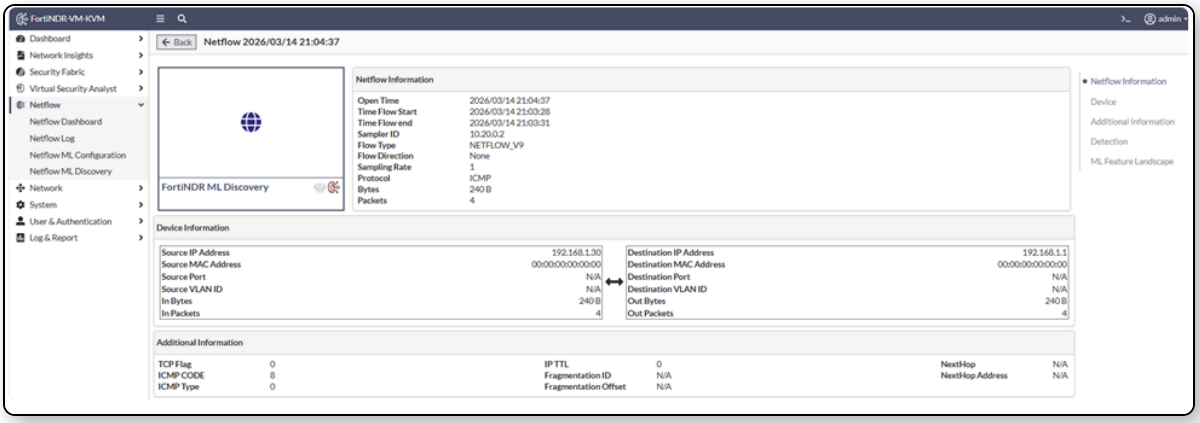
- Select one of the alerts and double-click on it. The alert was generated because the system detected a connection to a destination not seen during the learning stage.





- You can select an alert and click in “View Netflow”.





Lab05 Automated Response with FortiSOAR

LABORATORY 5: Automated response with FortiSOAR:

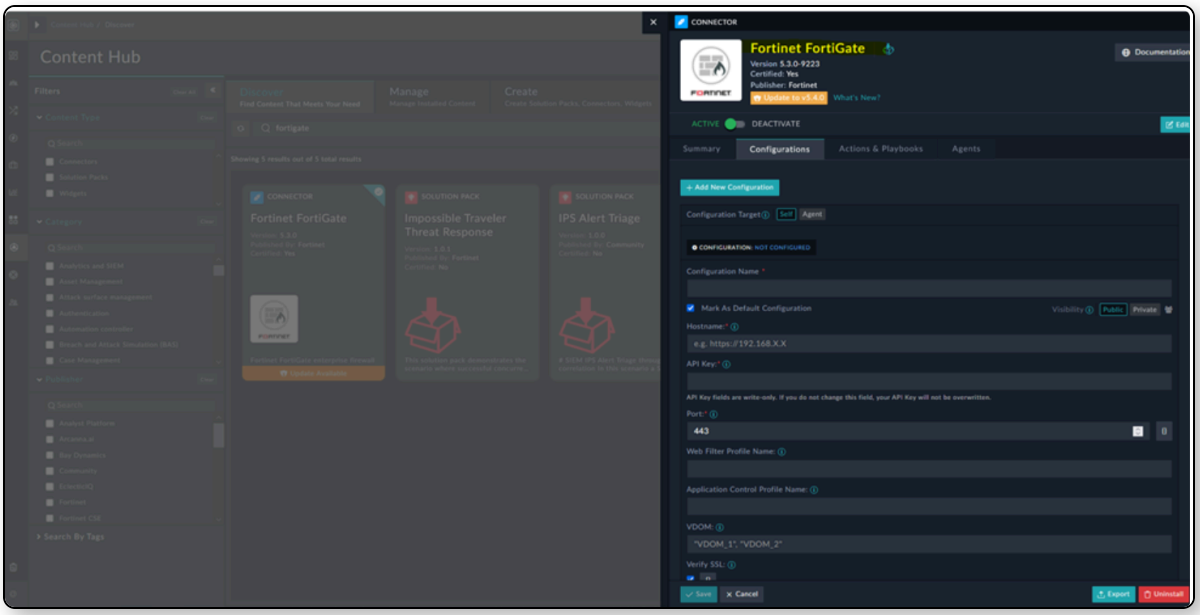
We will integrate FortiNDR with FortiAnalyzer and FortiAnalyzer as data ingest with FortiSOAR. We will simulate a kind of internal network attack (A malware download). FortiNDR will notify to FortiAnalyzer (As data lake) and the FortiAnalyzer will inform to FortiSOAR of this event, which will then execute a response on the FortiGate (will put the malware repository in quarantine) and in the “Switch_Internal” we will down the victim´s port.

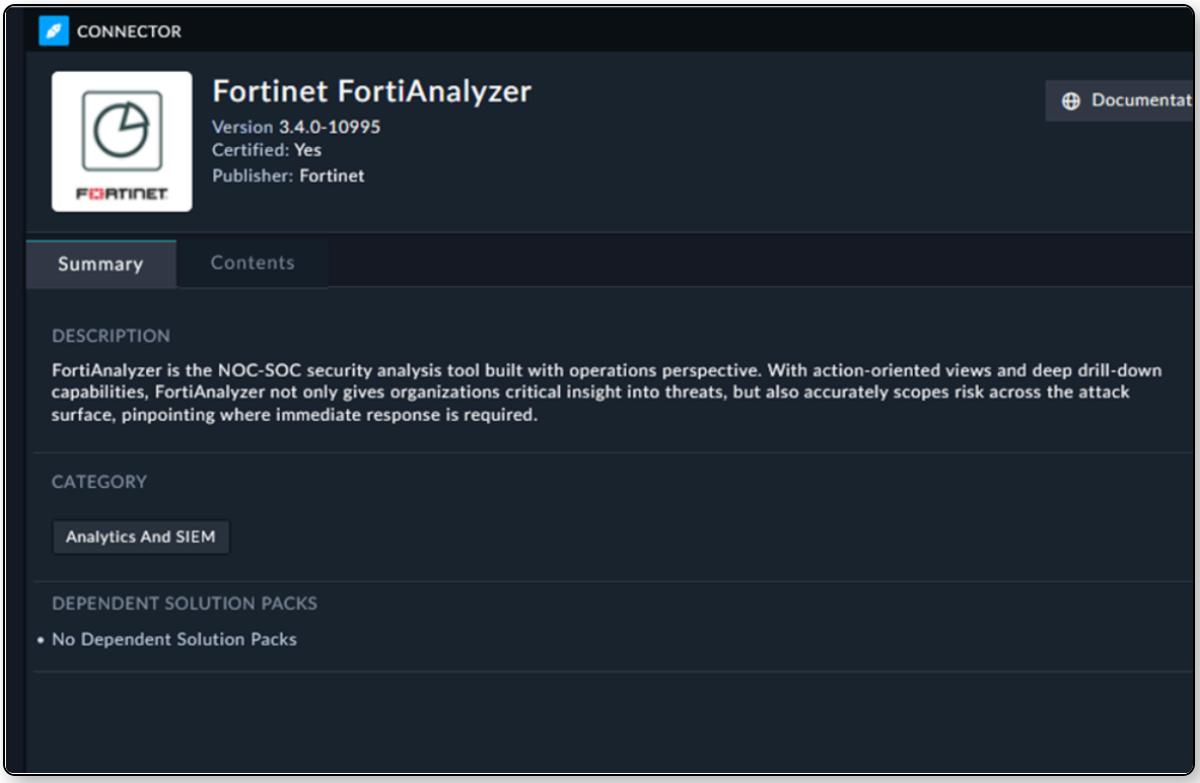
a) Important Notes:

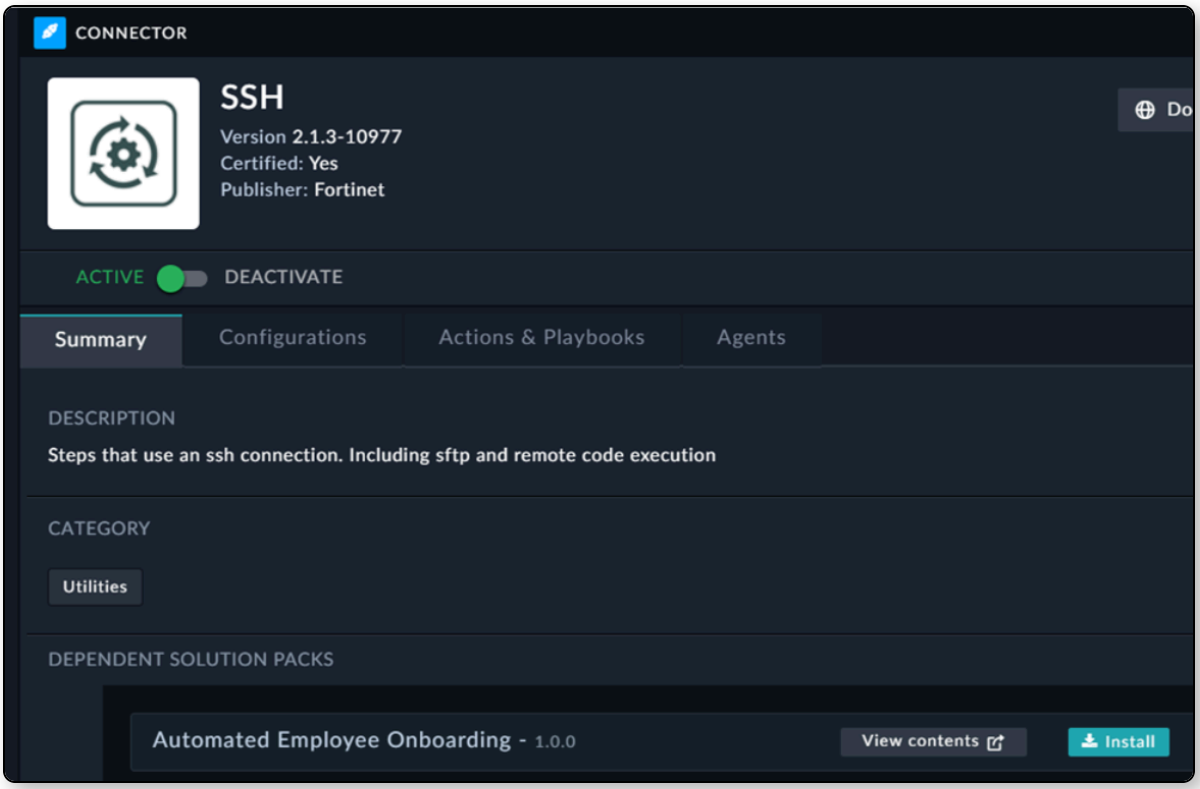
- The FortiAnalyzer´s Time should be configured in GMT similar to FortiSOAR´s TIME.
- Some times we need to restart the FortiAnalyzer for test automatically actions.
- Comand to change csadmin´s password via cli is ""sudo passwd csadmin"
- The command "sudo csadm services --restart", restart all FortiSOAR services.
- The command "sudo csadm package content-hub sync --force" syncronice internal content hub.
- Sometimes we need to restart our FortiAnalyzer lab.

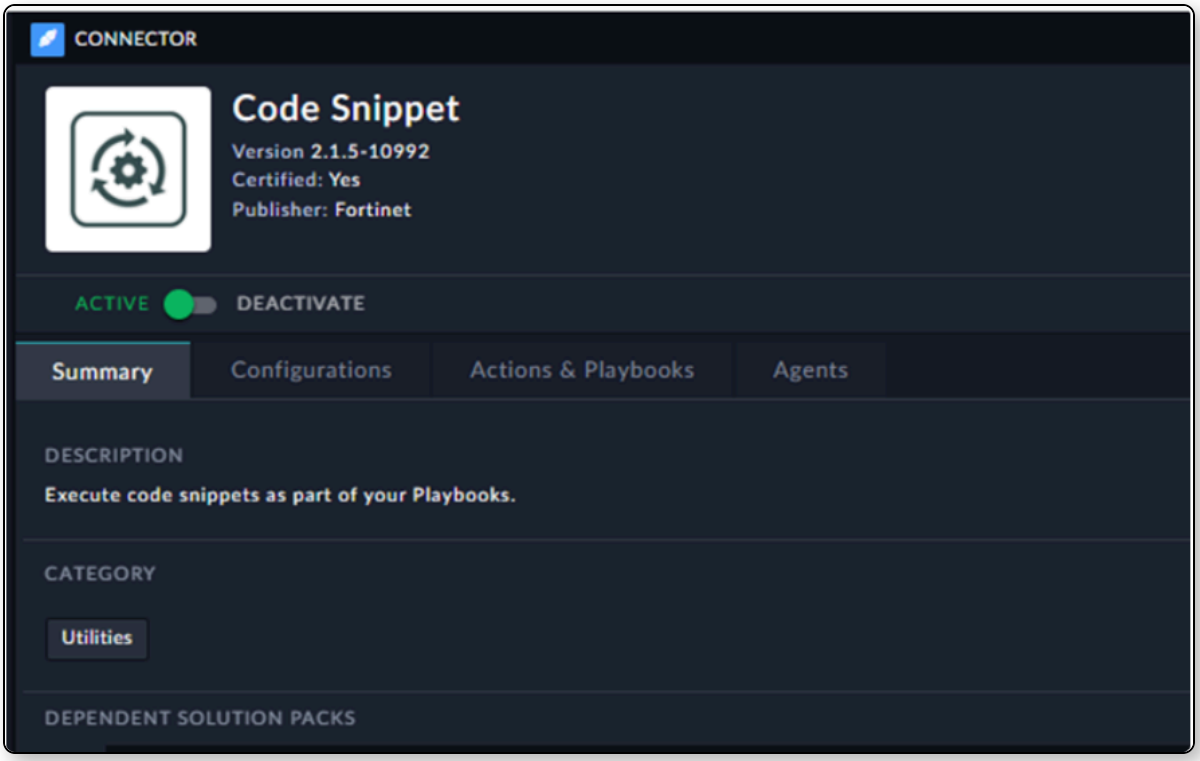
b) Let´s go to integrate the FortiSOAR to FortiGate, FortiNDR and FortiAnalyzer using the next Connectors.

- We need to install the next connectors on FortiSOAR: FortiGate, FortiAnalyzer, SSH Connector & Code Snippet. Let´s go to the FortiSOAR to “Content Hub”, looking for these connectors and we proceed to install everyone.


Content Hub
CONNECTOR
Fortinet FortiGate
Version 5.3.0-9223
Certified: Yes
Publisher: Fortinet
Documentation
ACTIVE
DEACTIVATE
Summary
Configurations
Actions & Playbooks
Agents
+ Add New Configuration
Configuration Target:
Self
Agent
CONFIGURATION: NOT CONFIGURED
Configuration Name *
Mark As Default Configuration
Visibility:
Public
Private
Hostname:*
e.g. https://192.168.X.X
API Key:*
API Key fields are write-only. If you do not change this field, your API Key will not be overwritten.
Port:*
443
Web Filter Profile Name:
Application Control Profile Name:
VDOM:
"VDOM_1","VDOM_2"
Verify SSL:
Save
Cancel
Export
Uninstall

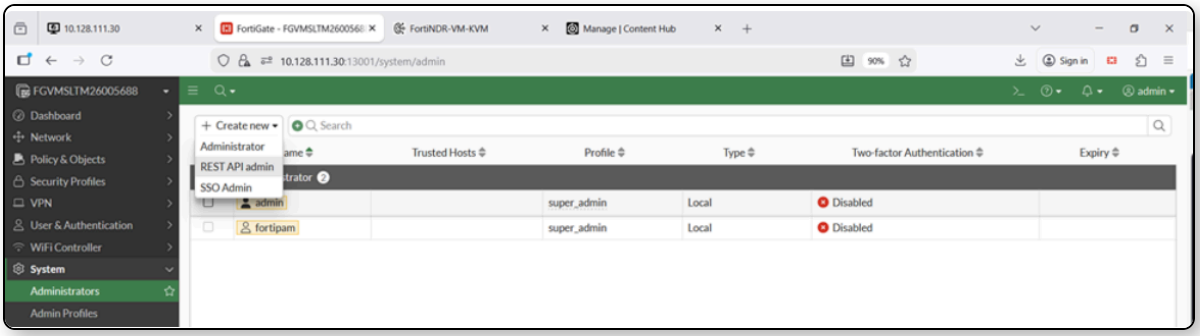

CONNECTOR
Fortinet FortiAnalyzer
Version 3.4.0-10995
Certified: Yes
Publisher: Fortinet
Documentat
Summary
Contents
DESCRIPTION
FortiAnalyzer is the NOC-SOC security analysis tool built with operations perspective. With action-oriented views and deep drill-down capabilities, FortiAnalyzer not only gives organizations critical insight into threats, but also accurately scopes risk across the attack surface, pinpointing where immediate response is required.
CATEGORY
Analytics And SIEM
DEPENDENT SOLUTION PACKS
• No Dependent Solution Packs

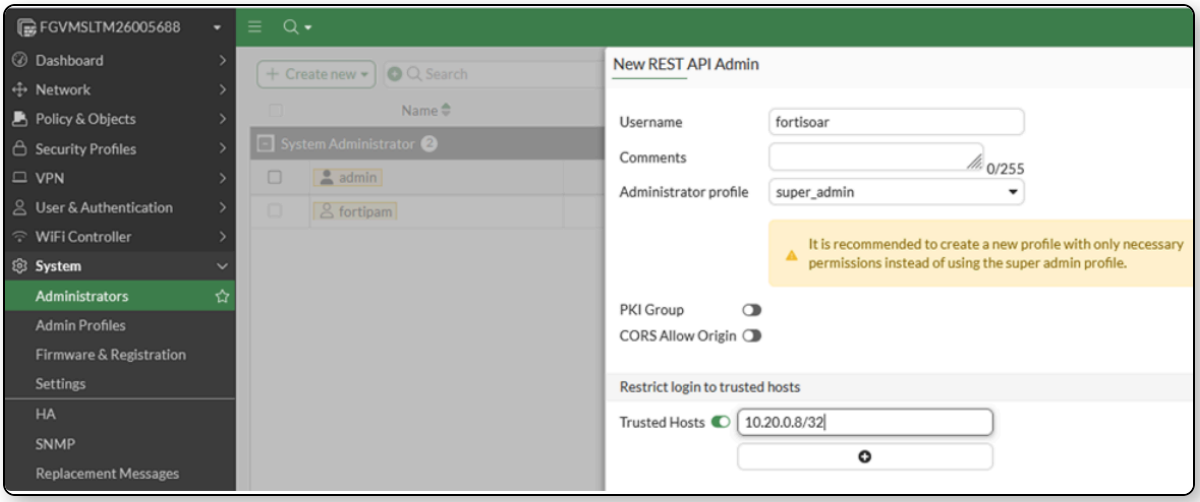




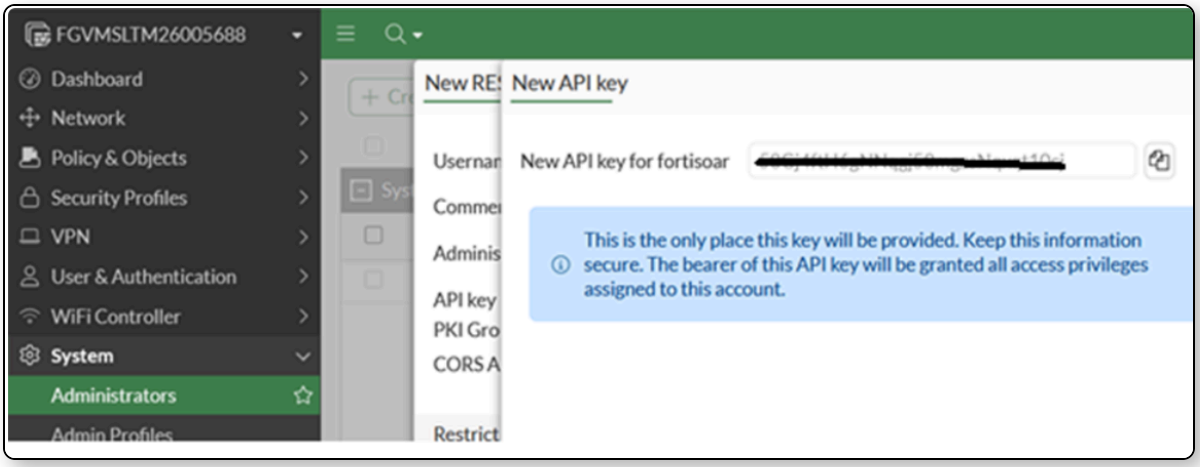
- We need to configure every connector in the next way. First, we are going to configure the FortiGate´s connector.

- We need to create an Admin API user in FortiGate.
- The trusted host is optional.

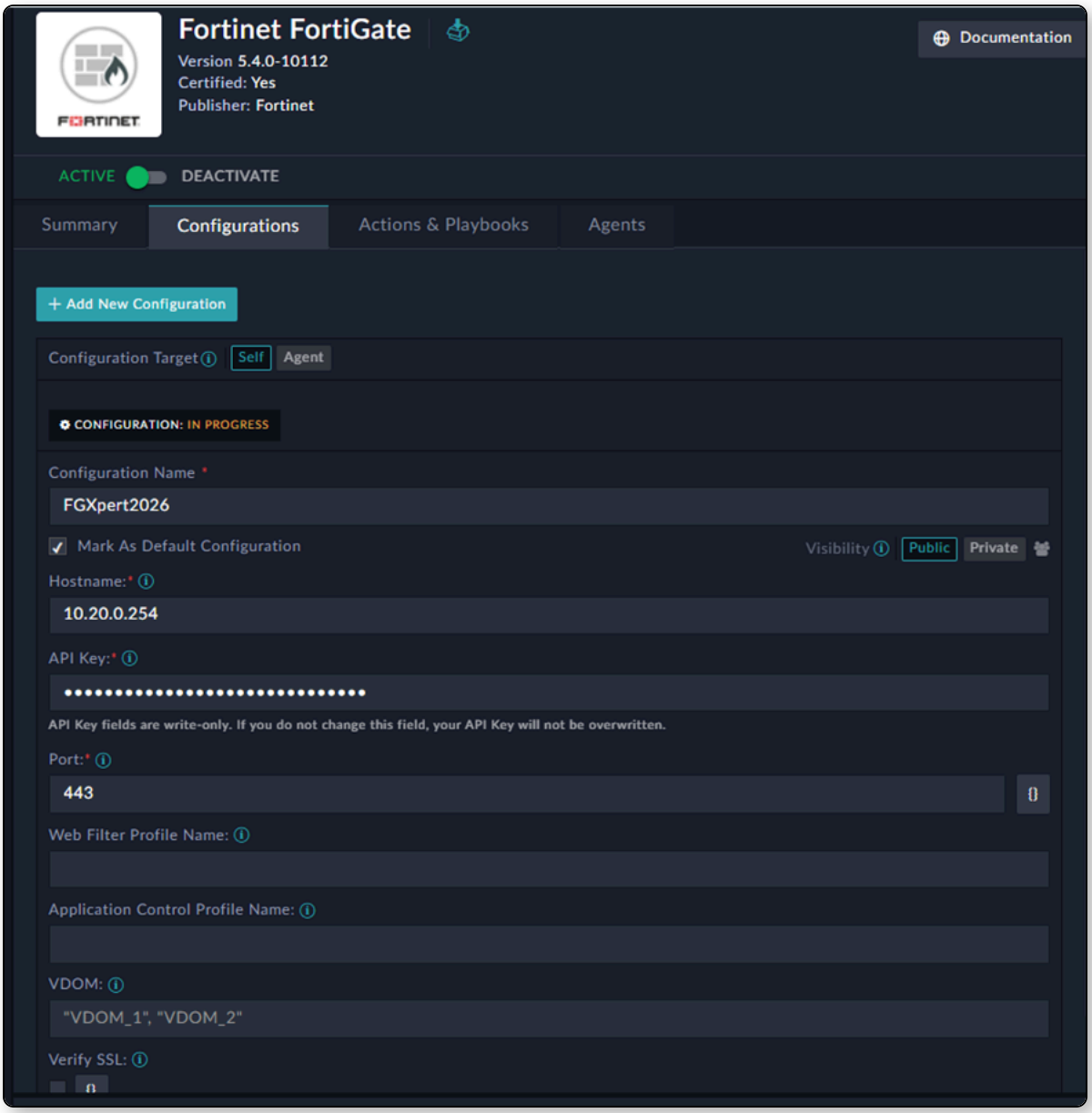




- Please be careful with the API Key and save it. There is no way to recovery this API key.

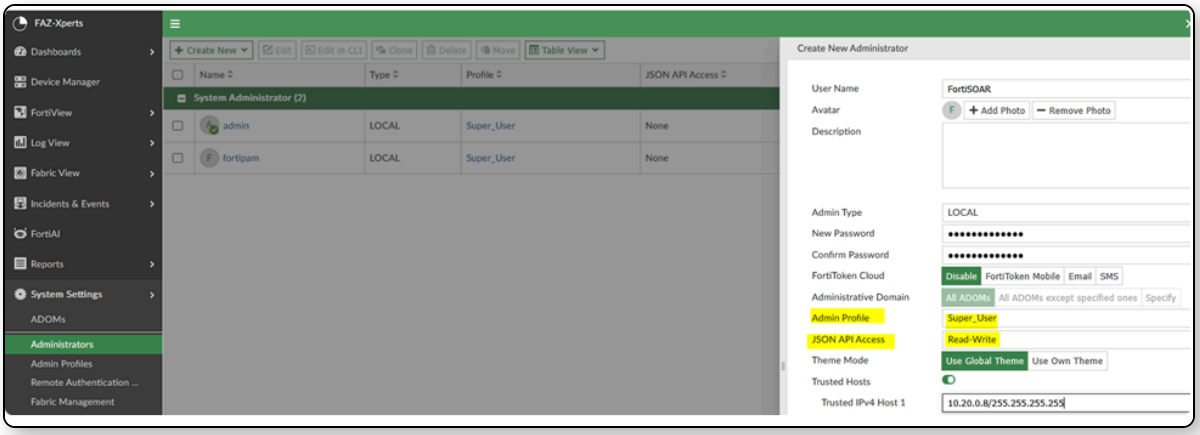


- Let´s go to the FortiSOAR and we are going to configure the “Fortinet Fortigate” connector with this information:

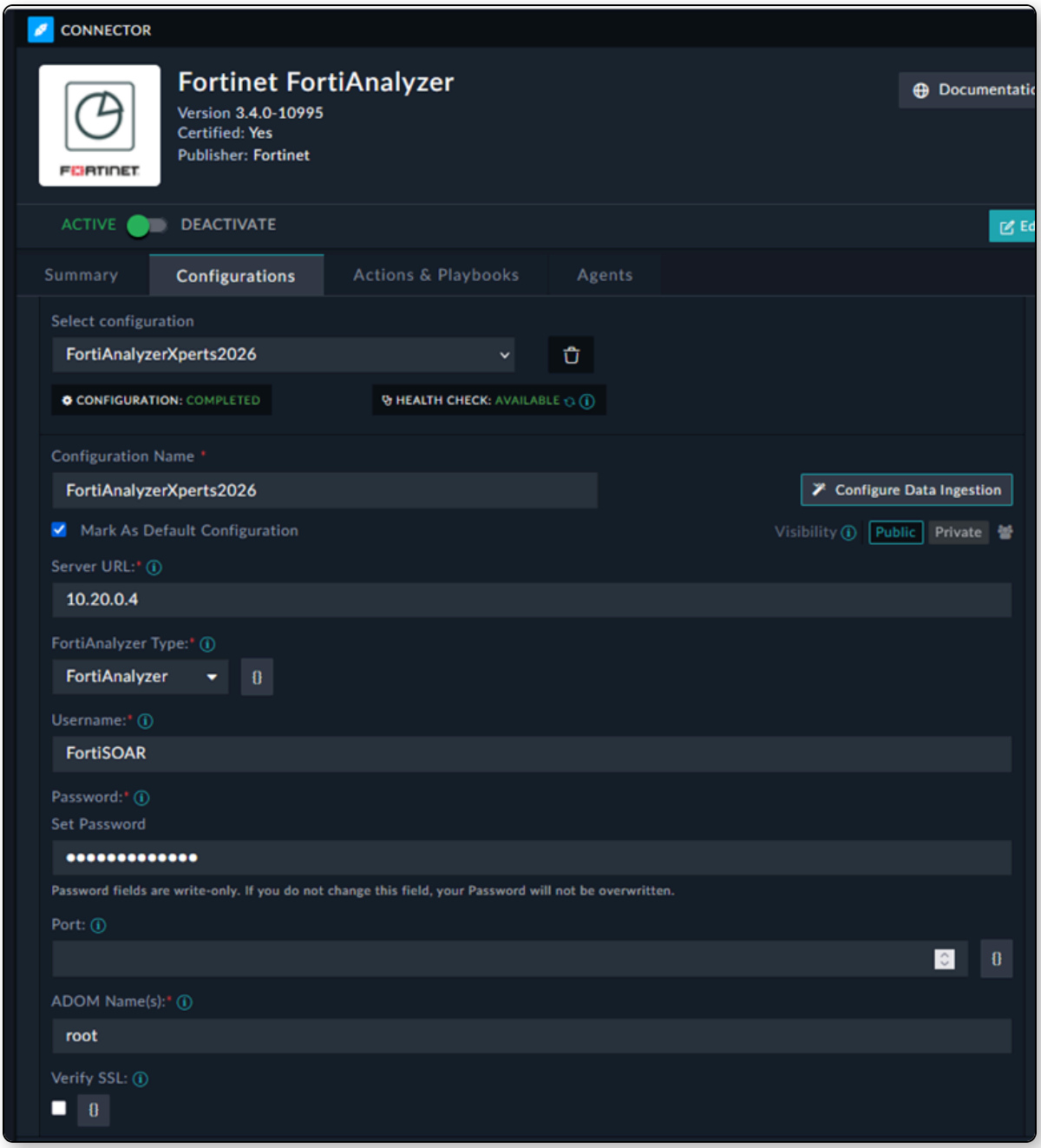

Fortinet FortiGate
Version 5.4.0-10112
Certified: Yes
Publisher: Fortinet
Documentation
ACTIVE
DEACTIVATE
Summary
Configurations
Actions & Playbooks
Agents
+ Add New Configuration
Configuration Target
Self
Agent
CONFIGURATION: IN PROGRESS
Configuration Name *
FGXpert2026
Mark As Default Configuration
Visibility
Public
Private
Hostname:*
10.20.0.254
API Key:*
••••••••••••••••••••••••••••••••
API Key fields are write-only. If you do not change this field, your API Key will not be overwritten.
Port:*
443
Web Filter Profile Name:
Application Control Profile Name:
VDOM:
"VDOM_1", "VDOM_2"
Verify SSL:

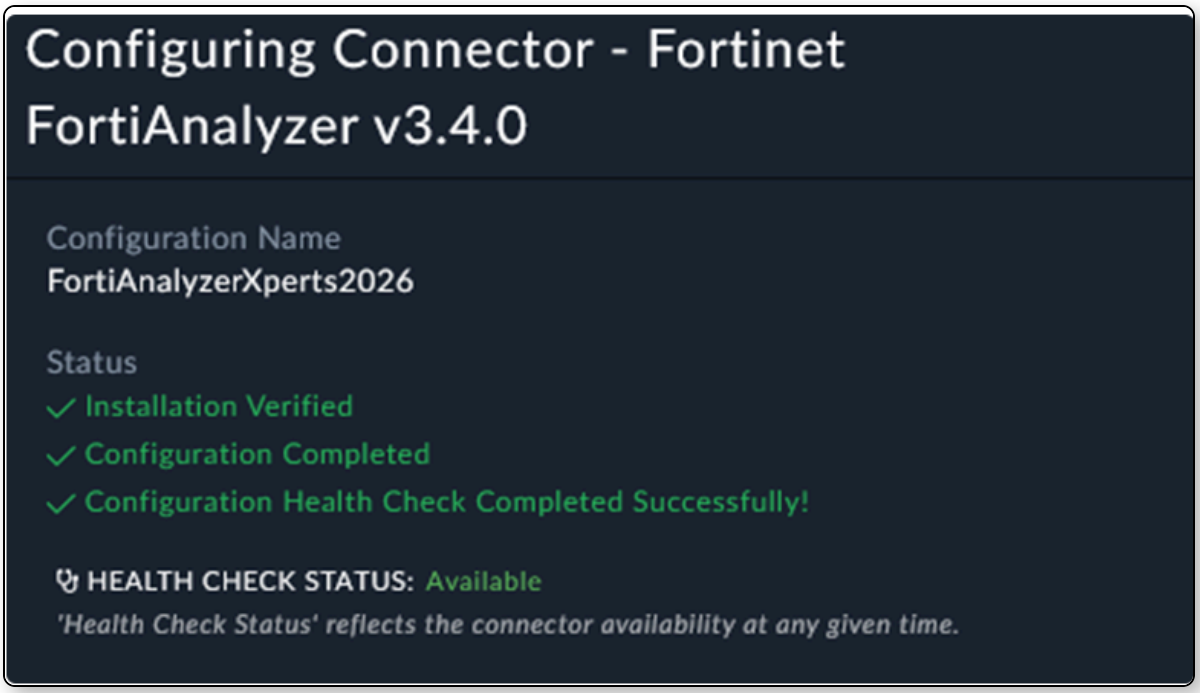


- We need to create a user admin in the FortiAnalyzer for use the FortiSOAR connector. This user needs to have admin profile as “Super-user” and JSON API Access as “Read-Write”.

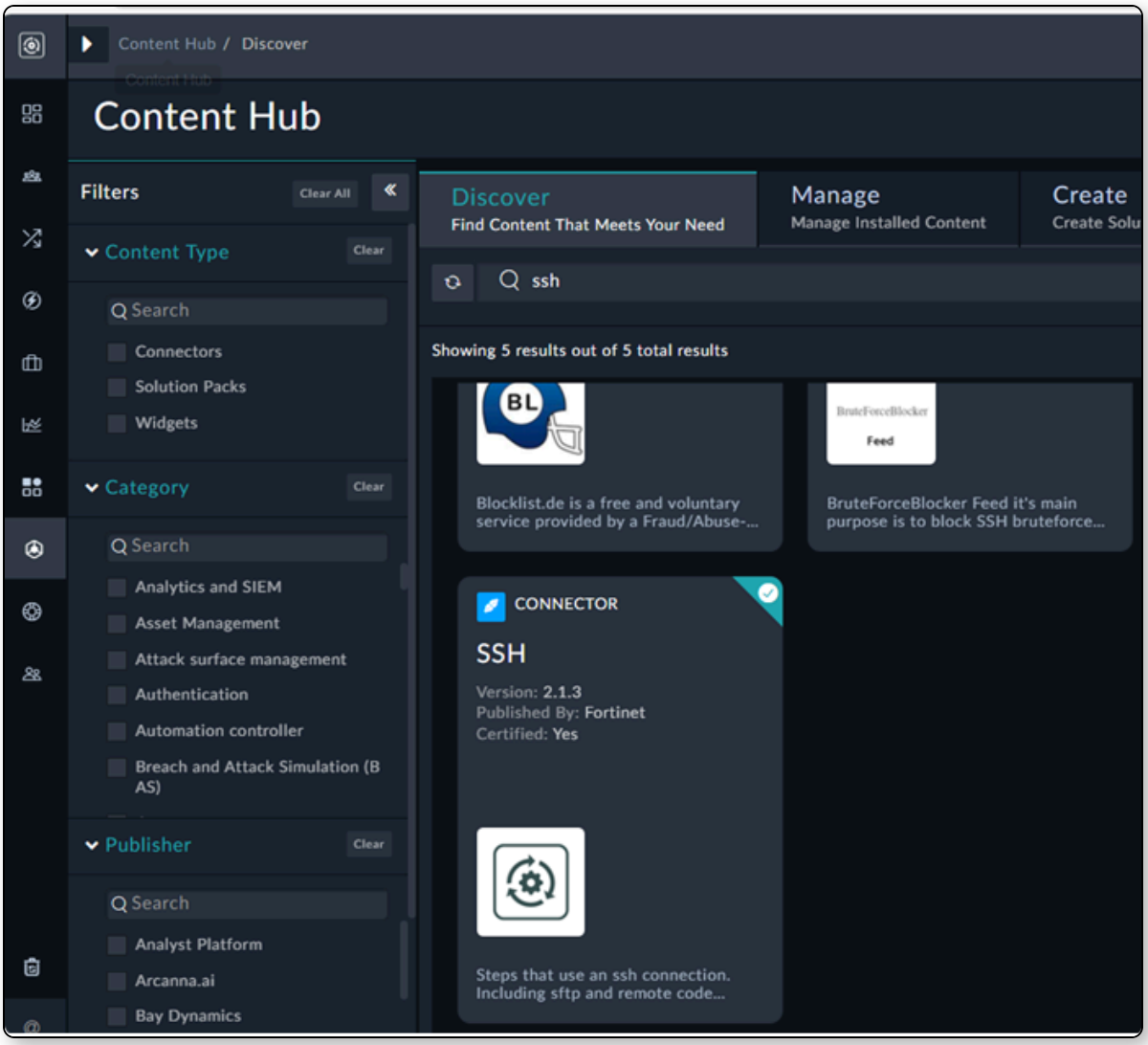


- Let´s go to the FortiSOAR and we will configure the FortiAnalyzer connector.

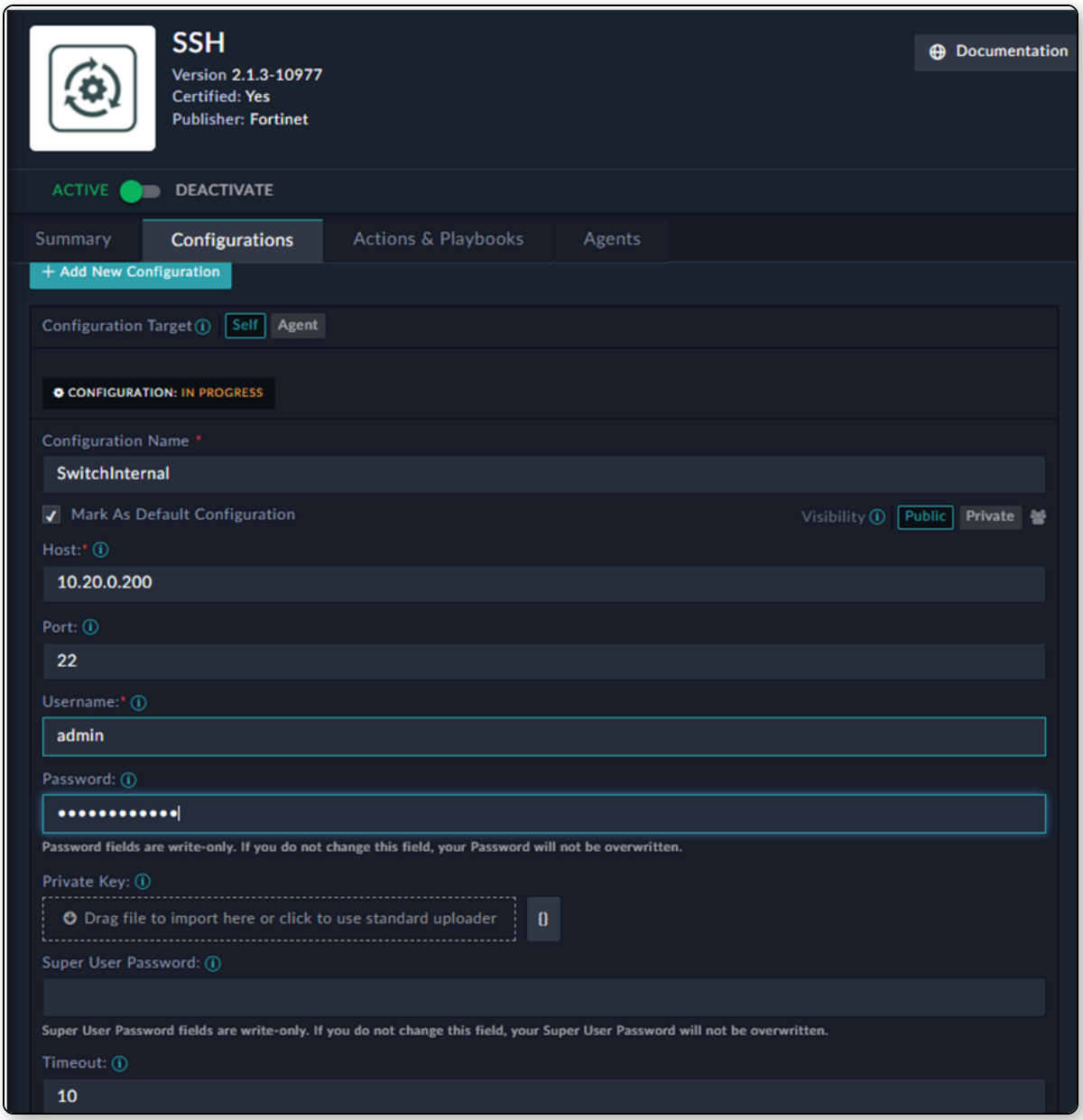

CONNECTOR
Fortinet FortiAnalyzer
Version 3.4.0-10995
Certified: Yes
Publisher: Fortinet
Documentatic
ACTIVE
DEACTIVATE
Summary
Configurations
Actions & Playbooks
Agents
Select configuration
FortiAnalyzerXperts2026
CONFIGURATION: COMPLETED
HEALTH CHECK: AVAILABLE
Configuration Name *
FortiAnalyzerXperts2026
Configure Data Ingestion
Mark As Default Configuration
Visibility
Public
Private
Server URL:*
10.20.0.4
FortiAnalyzer Type:*
FortiAnalyzer
Username:*
FortiSOAR
Password:*
Set Password
Password fields are write-only. If you do not change this field, your Password will not be overwritten.
Port:
ADOM Name(s):*
root
Verify SSL:



- Let’s go to install a generic connector as “SSH”, this connector we will use it to integrate with the “Switch_Internal” and try to execute some information commands.

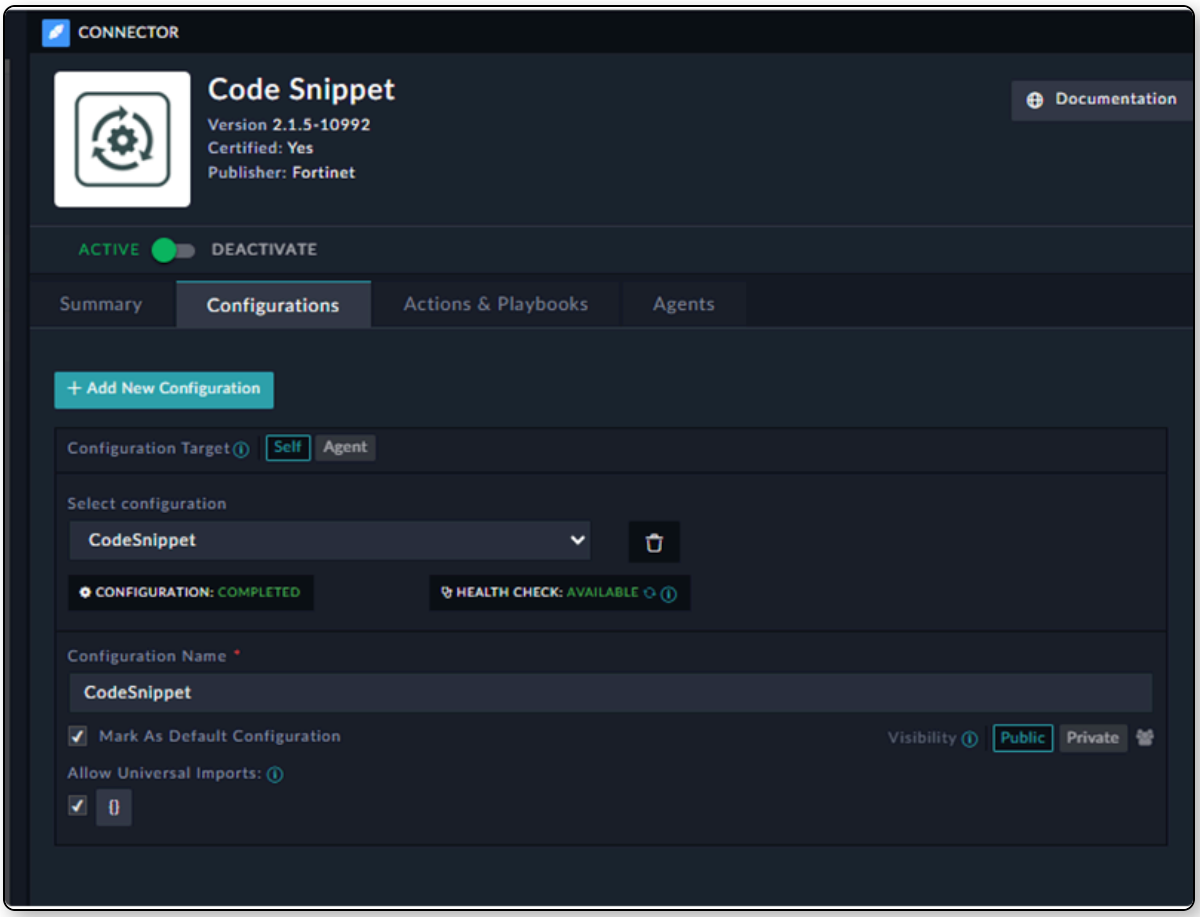


- Let’s go to configure this connector integrated with “SwitchInternal”:


SSH
Version 2.1.3-10977
Certified: Yes
Publisher: Fortinet
Documentation
ACTIVE
DEACTIVATE
Summary
Configurations
Actions & Playbooks
Agents
+ Add New Configuration
Configuration Target
Self
Agent
CONFIGURATION: IN PROGRESS
Configuration Name *
SwitchInternal
Mark As Default Configuration
Visibility
Public
Private
Host:*
10.20.0.200
Port:
22
Username:*
admin
Password:
Password fields are write-only. If you do not change this field, your Password will not be overwritten.
Private Key:
Drag file to import here or click to use standard uploader
{}
Super User Password:
Super User Password fields are write-only. If you do not change this field, your Super User Password will not be overwritten.
Timeout:
10

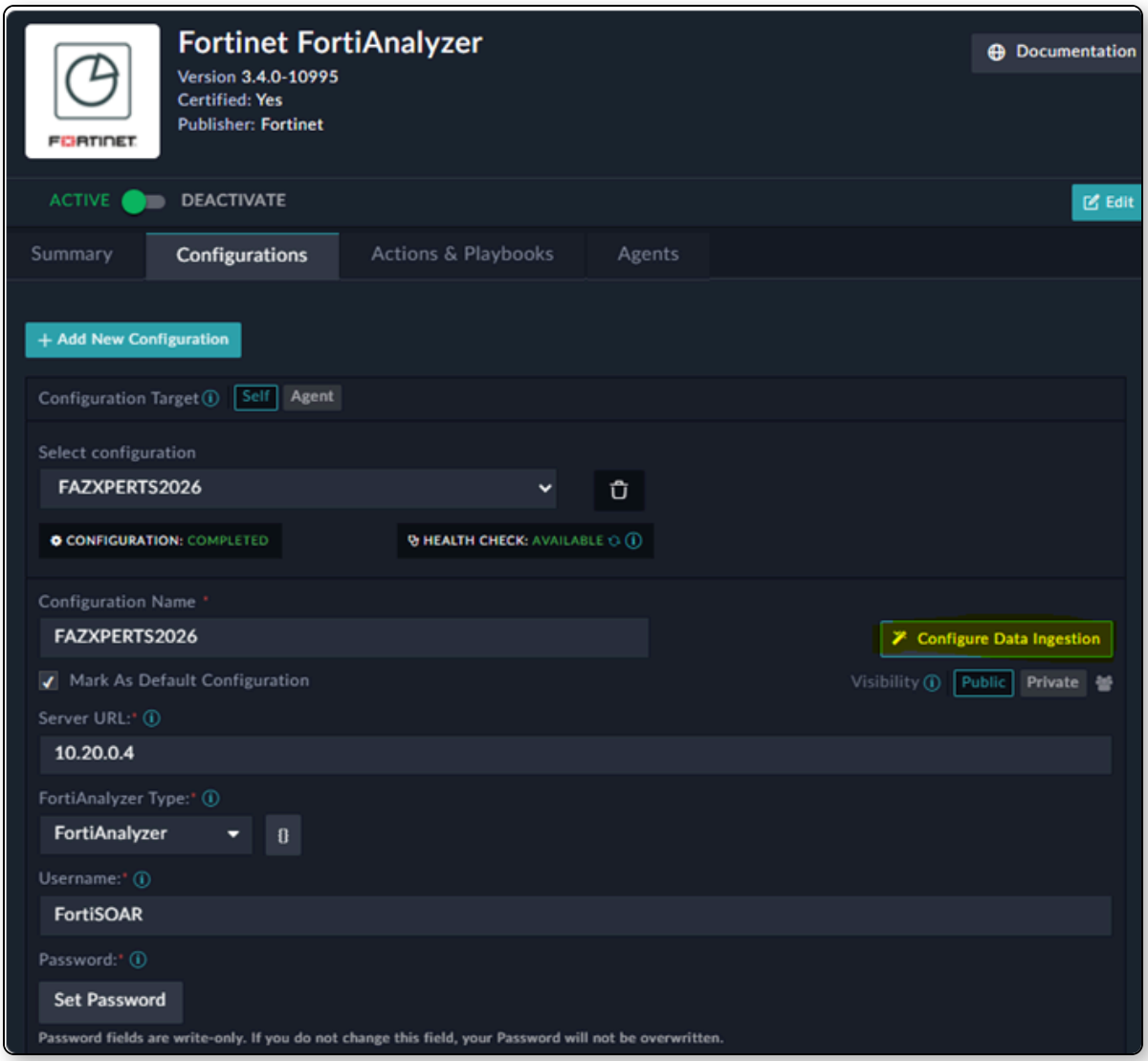


- Finally, we need to install the “Code Snippet” connector for use a script and execute a port shutdown in “Switch_Internal”.
- Let´s go to configure this connector with the next information:

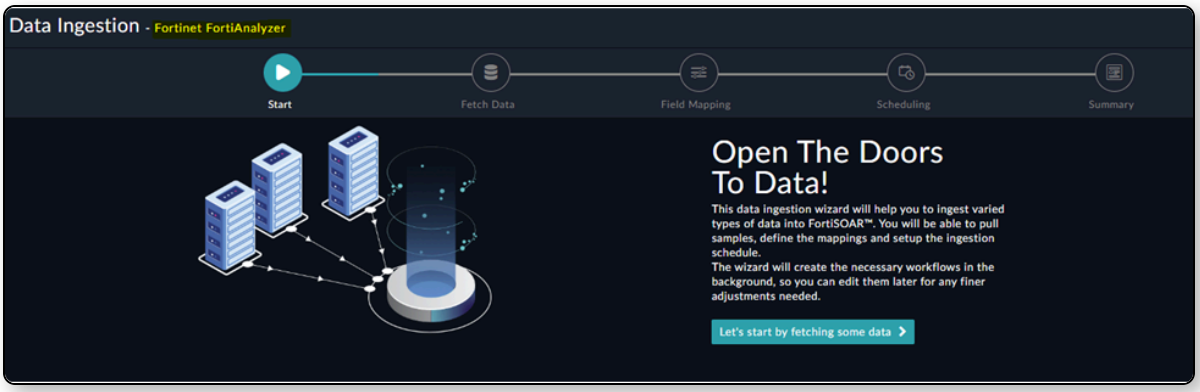


c) We are going to integrate FortiSOAR with FortiAnalyzer (As a Data Lake) to detect something suspicious in our network and execute an automatic response.

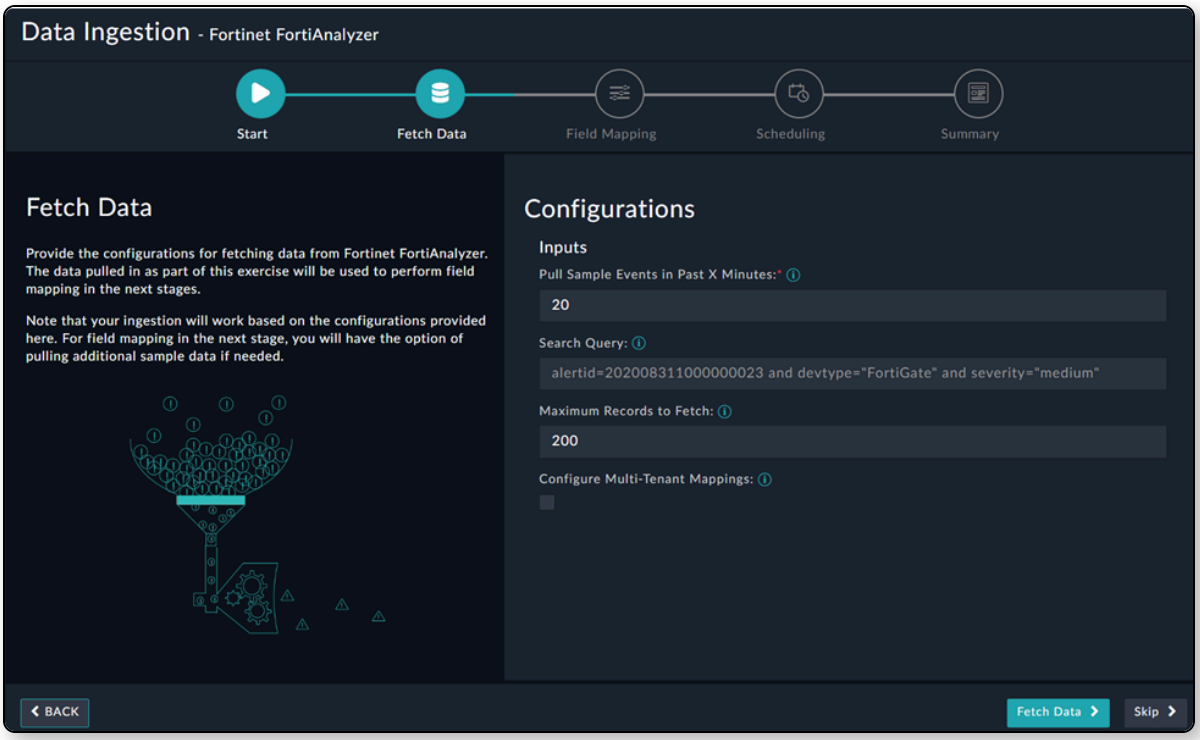
- We are going to use the “FortiAnalyzer´s Connector as a “Data Ingestion” as a principal events source:



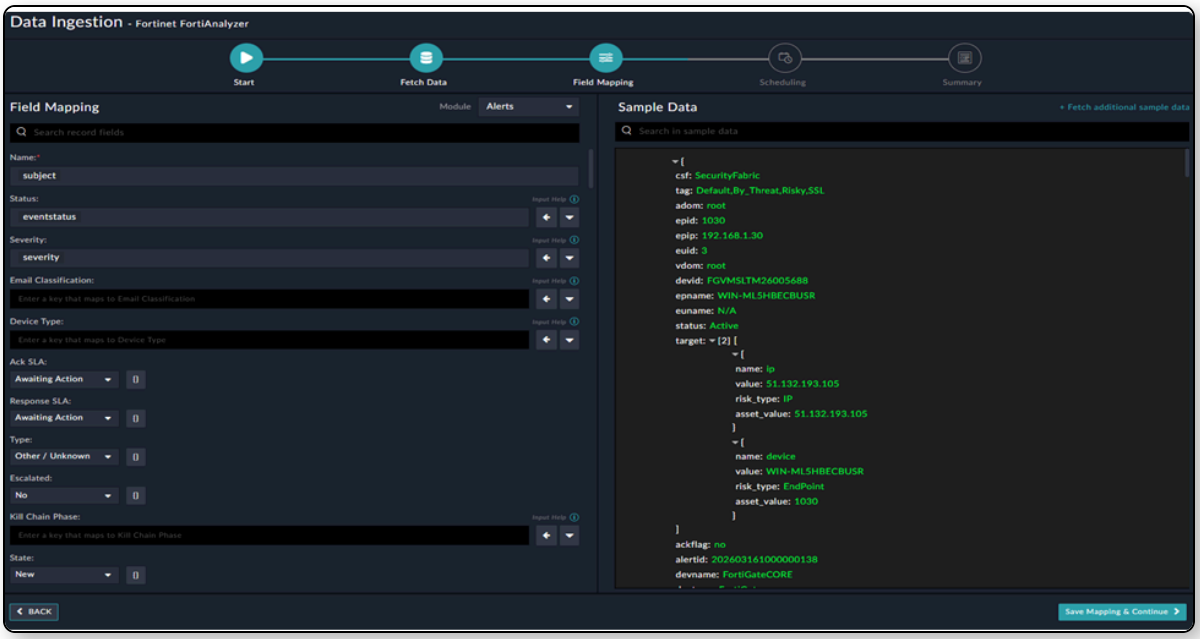
- Let’s go to follow the next steps:



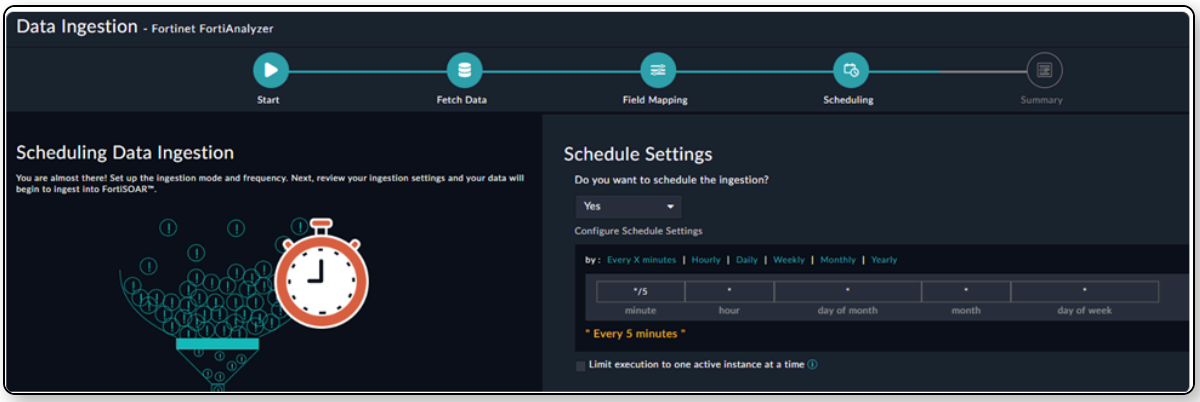
- In the next image click in “Fetch Data”



- Left the fields by default and click in “Save mapping & Continue”



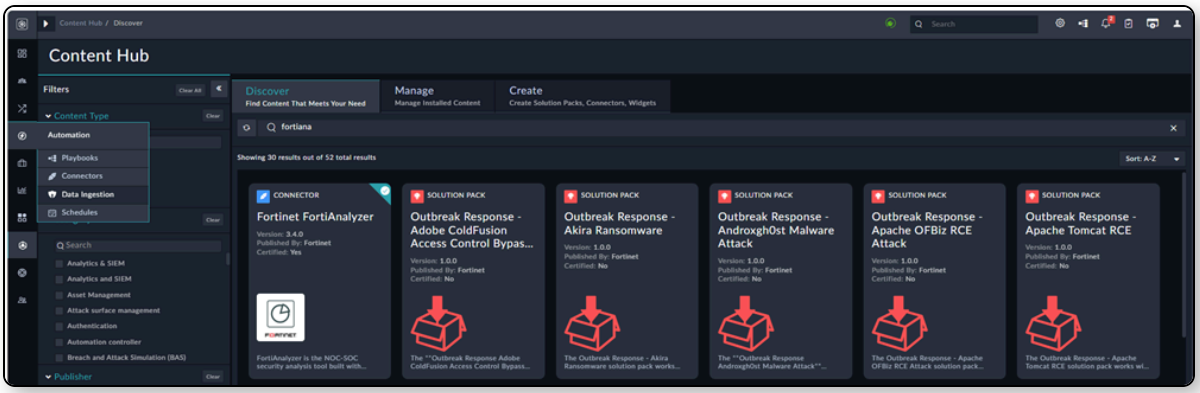
- Let’s configure “Do you want to schedule the ingestion” in “Yes”, and “Configure Schedule Setting” in “Every 5 minutes”. Click in “Save Settings & Continue”



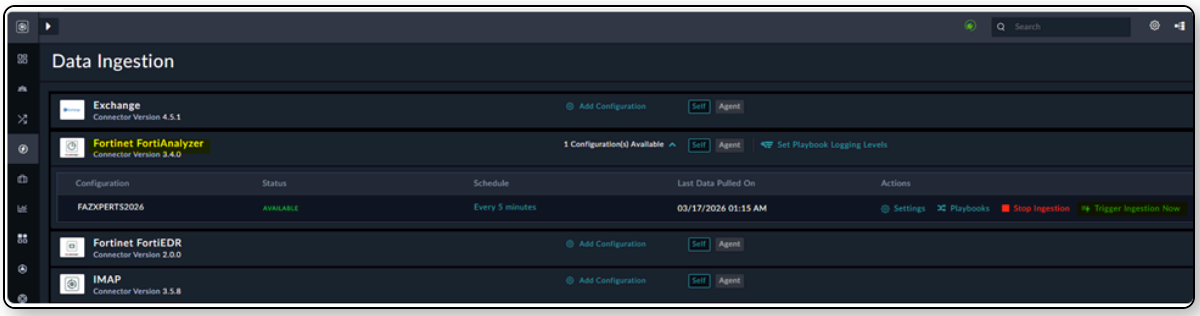
- At the end click in “Done”.



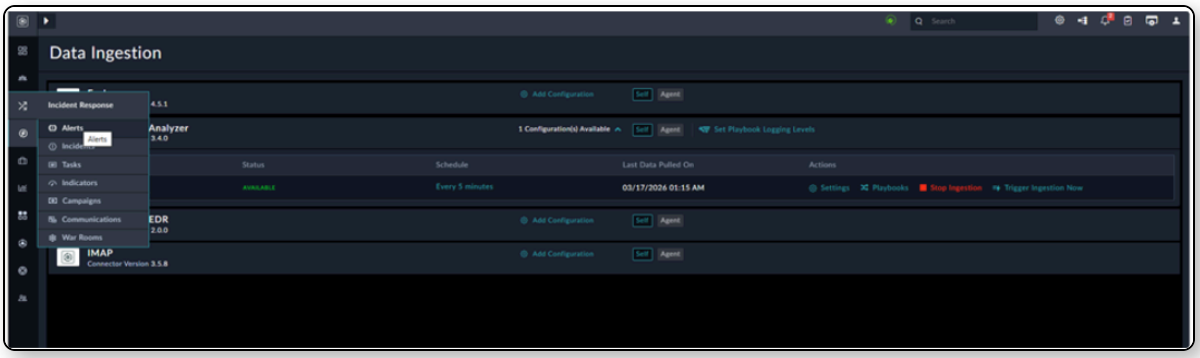
- Let’s go to “Automation Data Ingestion”:



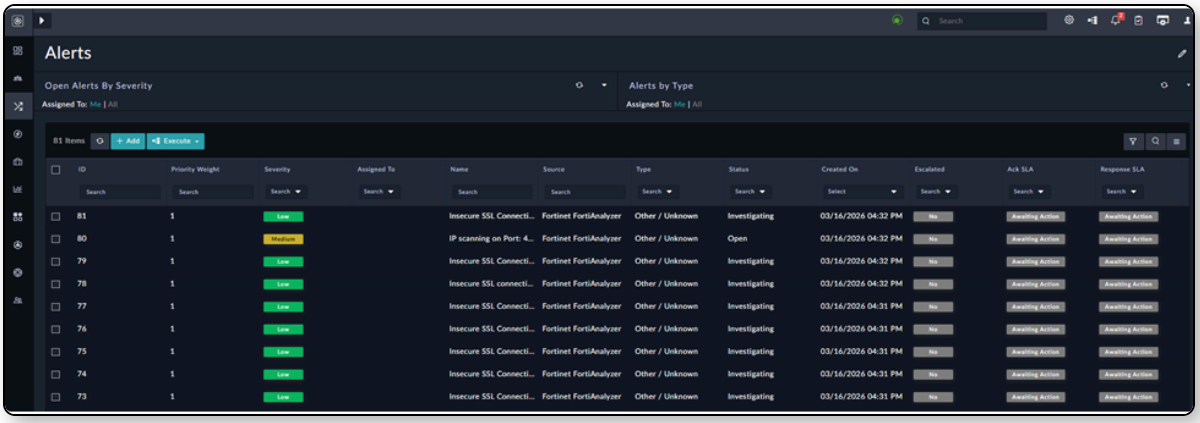
- Select “Fortinet FortiAnlyzer” and click in “Trigger Ingestion Now”:



- We can review if the “Ingestion Data” is working. Go to “Incidents & Response → Alerts”:

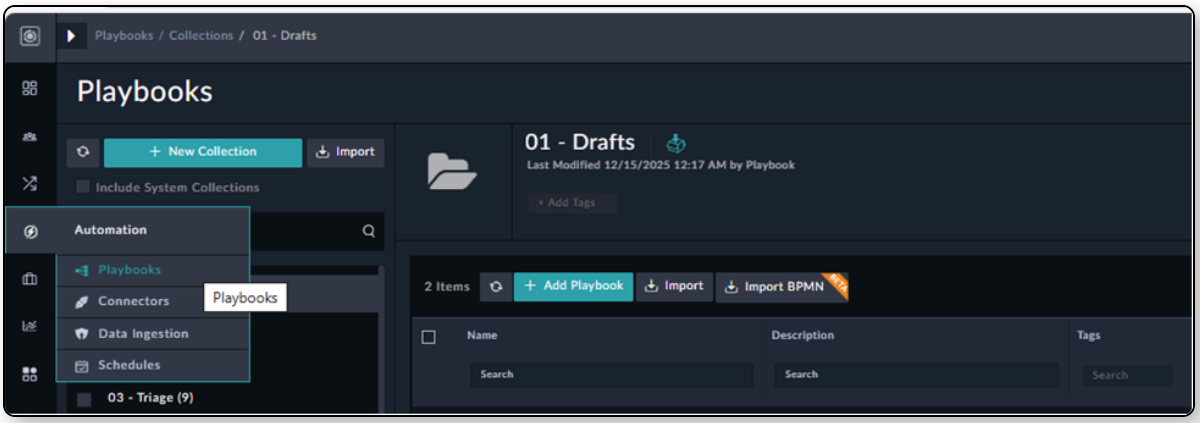


- Alerts from “FortiAnalyzer” are show:

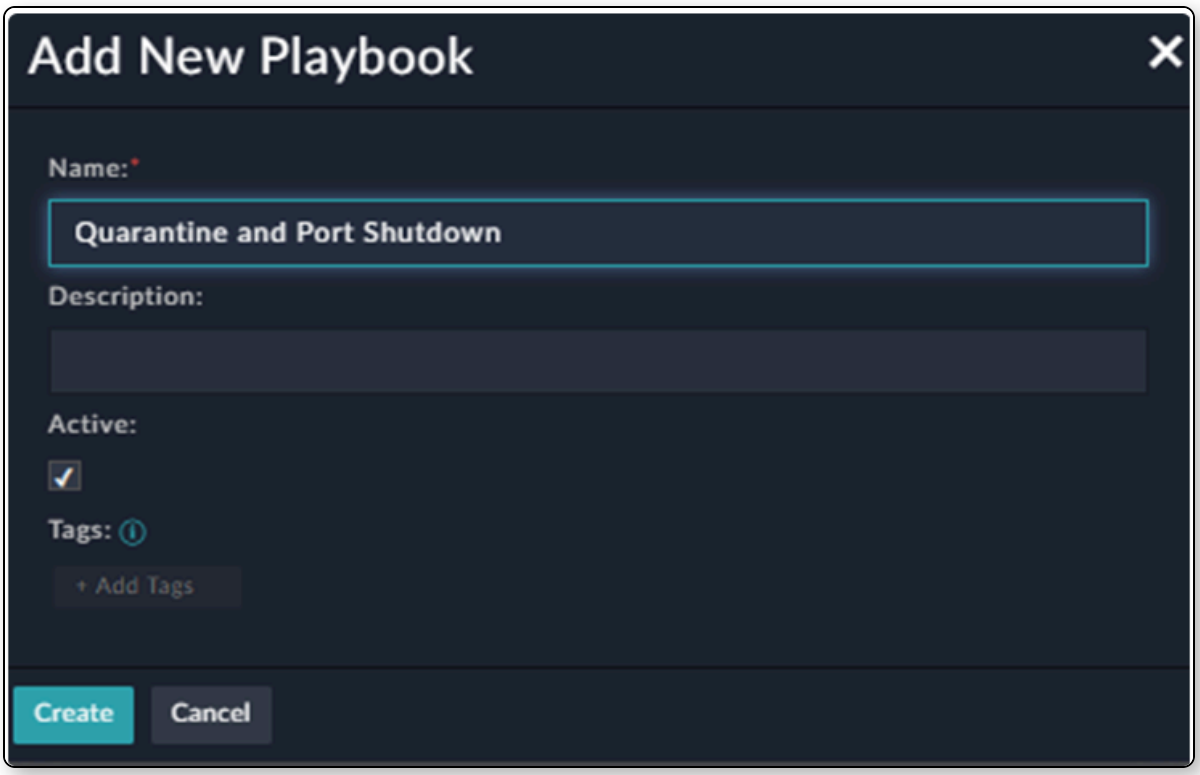


d) Let´s go to create a “Playbook” as an automated response task.

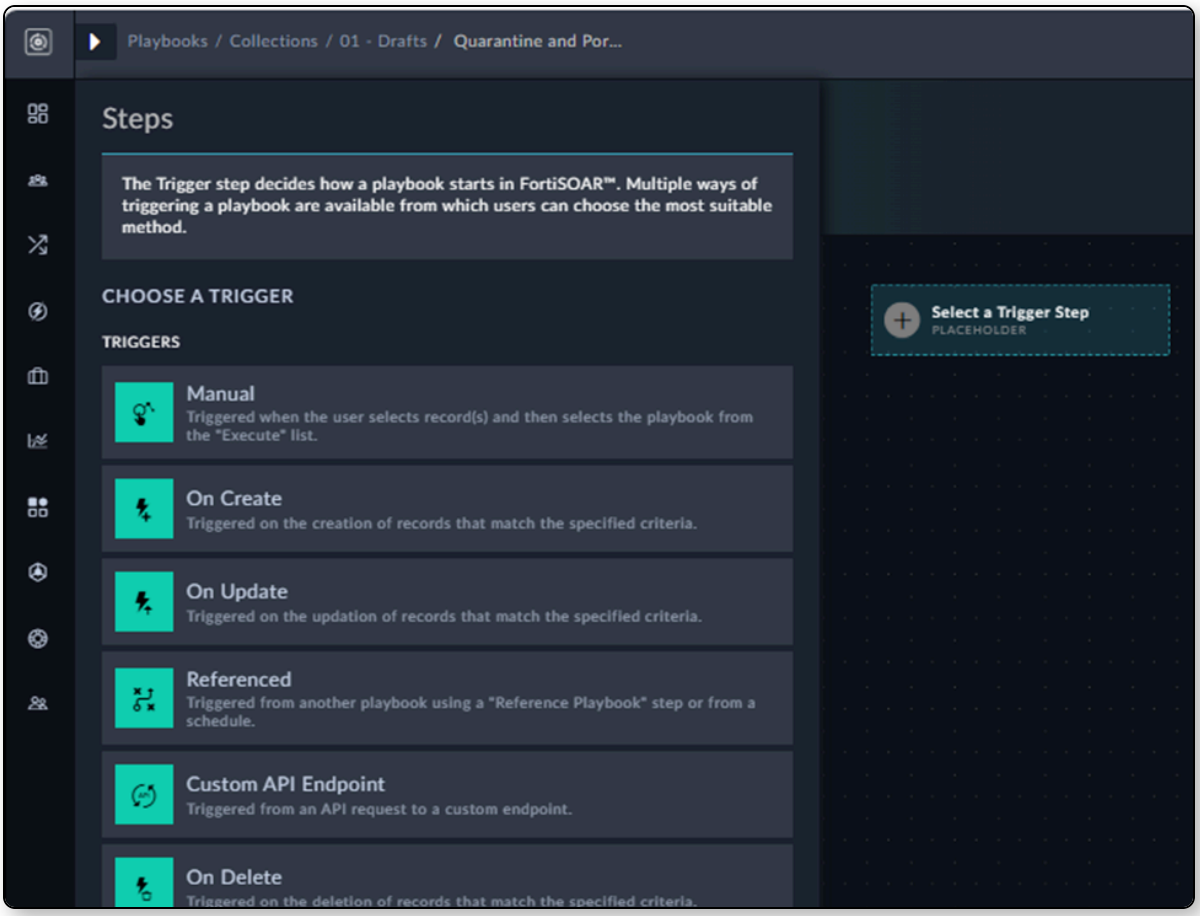
- In the FortiSOAR, go to “Automation Playbooks” and click in “Add Playbook”. You can left the ubication for this playbook in “Draft” folder.



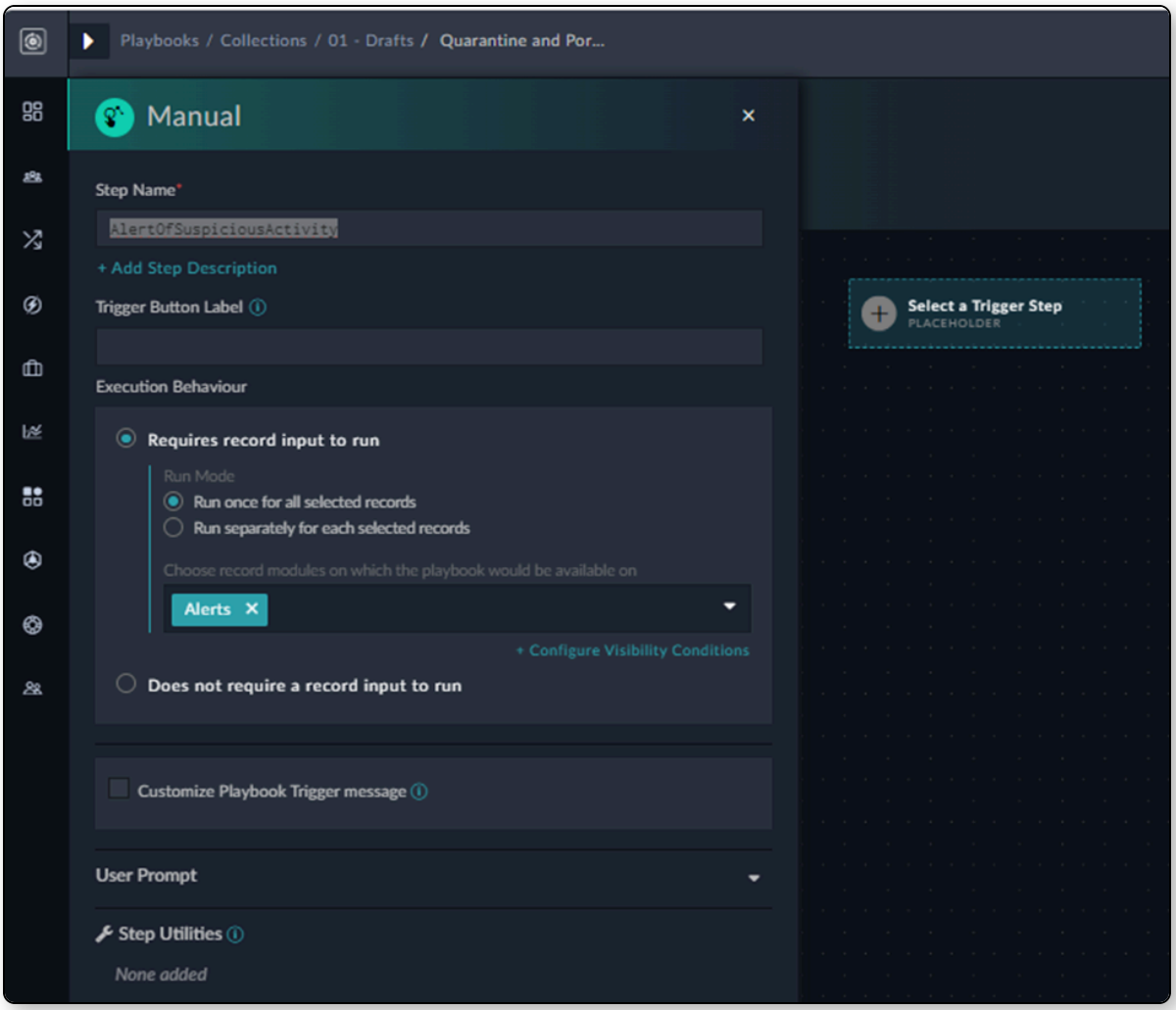
- Put a name to this playbook as “Quarantine and Port Shutdown” and click in “Create”.



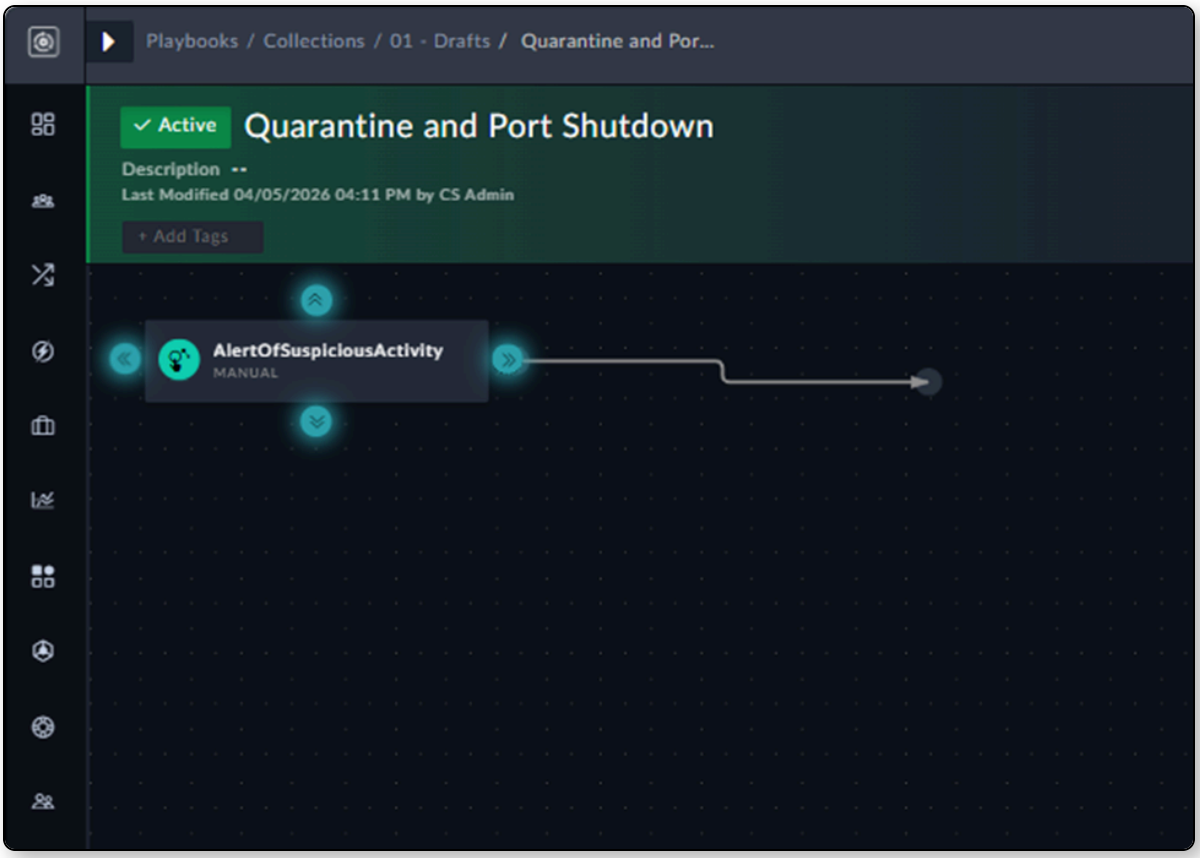
- Fort the “Trigger” we should select “Manual”:



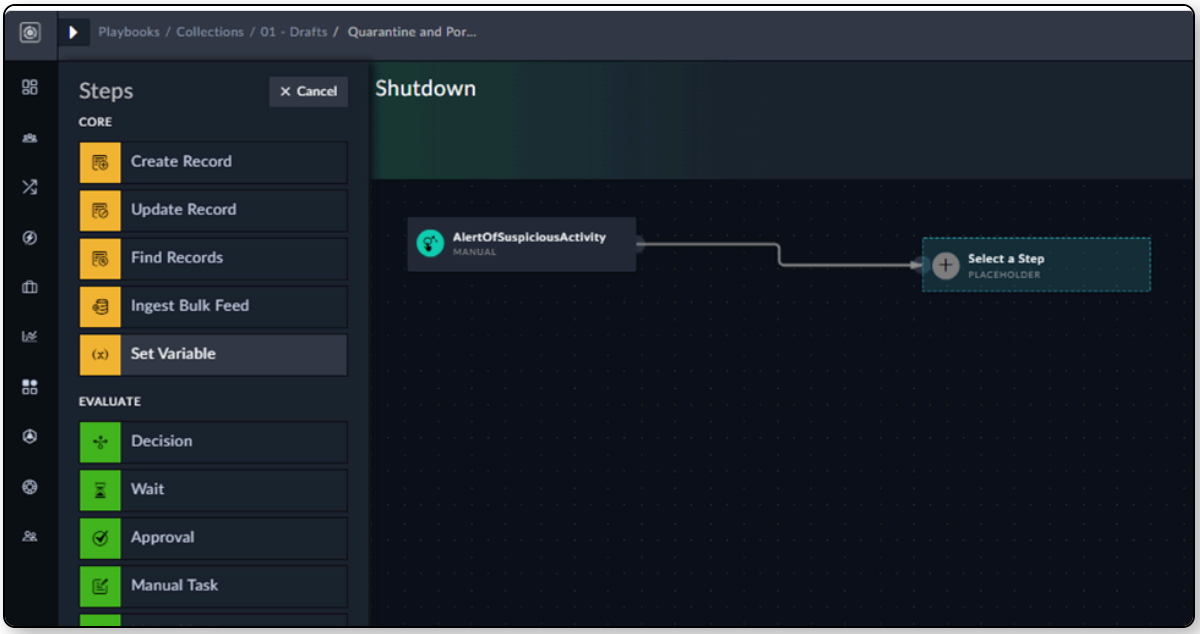
- Please configure a name as “AlertOfSuspiciousActivity” in “Requires record input to run” configure “Alerts” and click in “Save”.



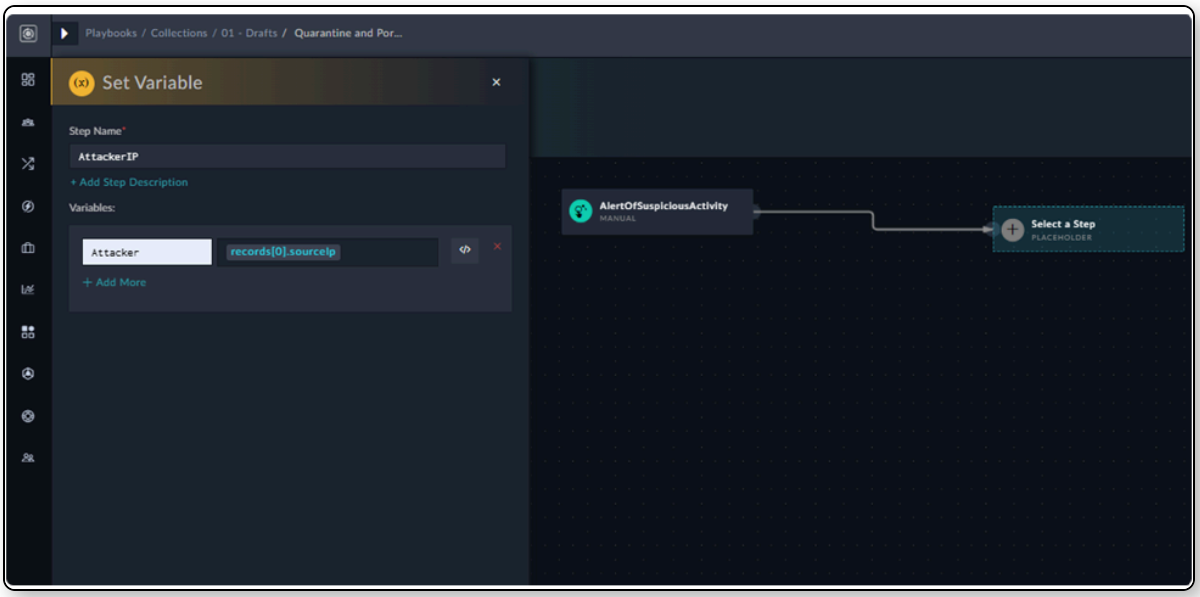
- Drag and drop any highlighted connector with a click held and finally a click:



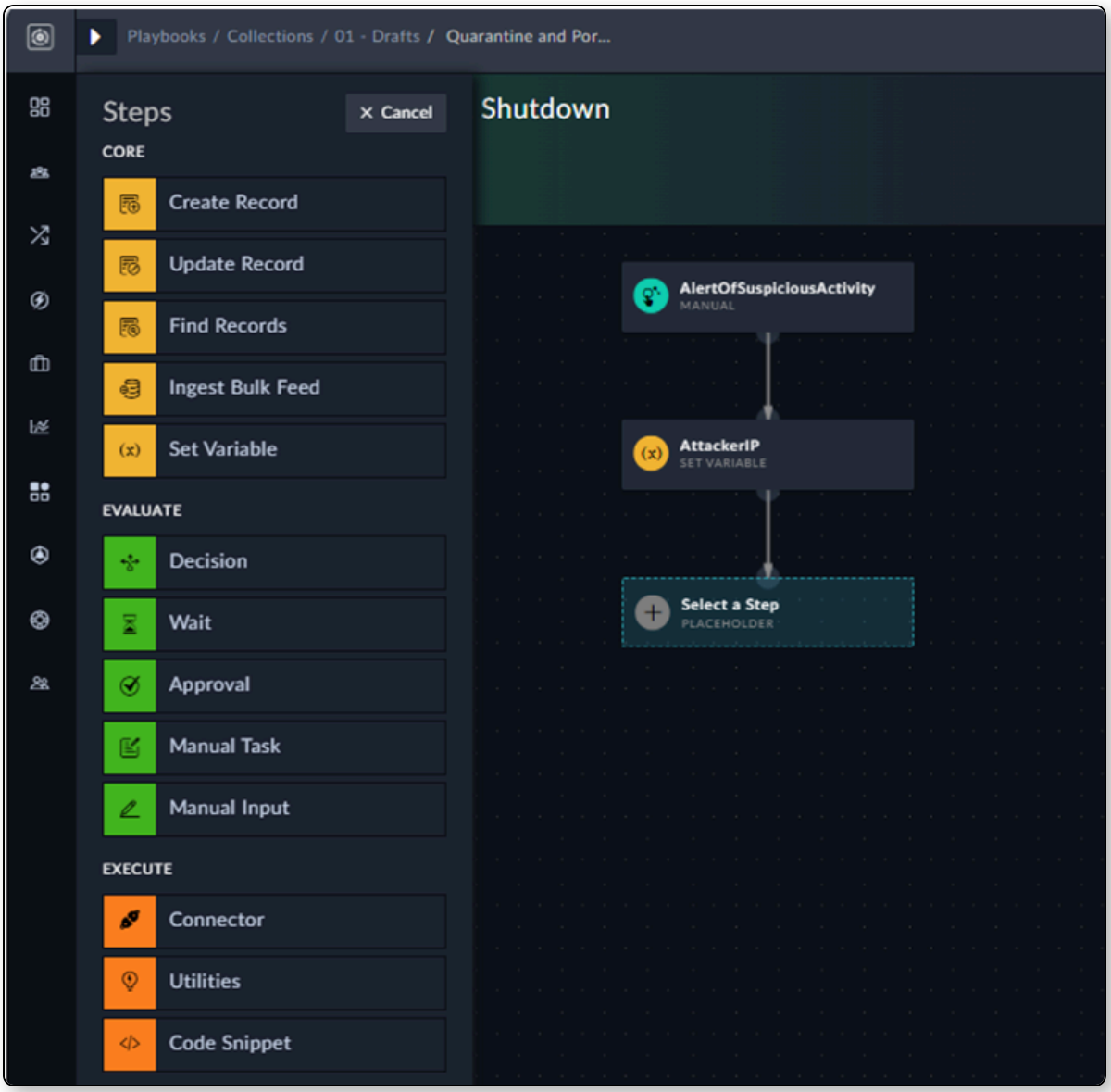
- Select a “Set Variable”:



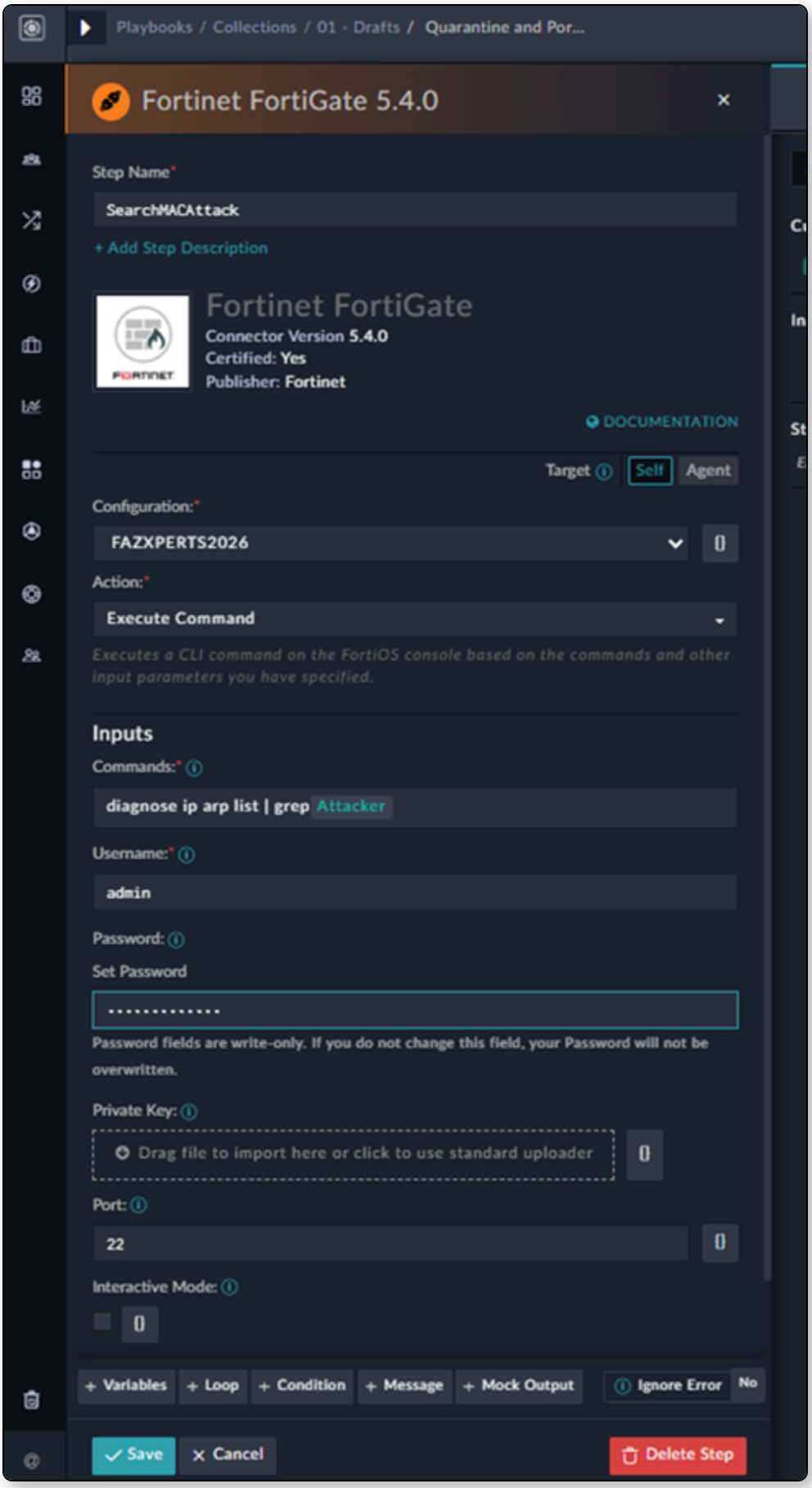
- Set the next parameter: “Step name”, in “Variables” set “Attacker” and in value select “Source IP” and click in “Save” (Save Playbook too).



- Drag and drop any highlighted in “AttackerIP” connector with a click held and finally a click and select “Connector”:



- Search and select the FortiGate connector and set this configuration.
- In Commands set “diagnose ip arp list | grep ” and the end select the custom variable “Attacker”.
- Make sure left a space. Set the user “Admin” and her password, click in “Save”.


Playbooks / Collections / 01 - Drafts / Quarantine and Por...
Fortinet FortiGate 5.4.0
Step Name*
SearchMACAttack
+ Add Step Description
Fortinet FortiGate
Connector Version 5.4.0
Certified: Yes
Publisher: Fortinet
DOCUMENTATION
Target
Self
Agent
Configuration:*
FAZXPERTS2026
Action:*
Execute Command
Executes a CLI command on the FortiOS console based on the commands and other input parameters you have specified.
Inputs
Commands:*
diagnose ip arp list | grep Attacker
Username:*
admin
Password:
Set Password
Password fields are write-only. If you do not change this field, your Password will not be overwritten.
Private Key:
Drag file to import here or click to use standard uploader
Port:
22
Interactive Mode:
+ Variables
+ Loop
+ Condition
+ Message
+ Mock Output
Ignore Error
No
Save
Cancel
Delete Step

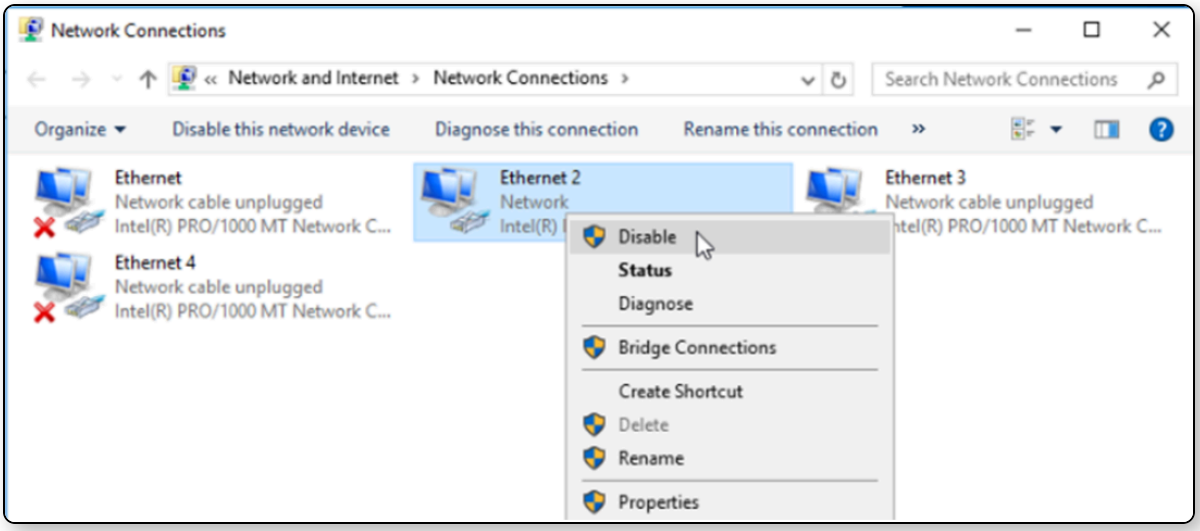
Lab06 Central Management Privileged Account FortiPAM

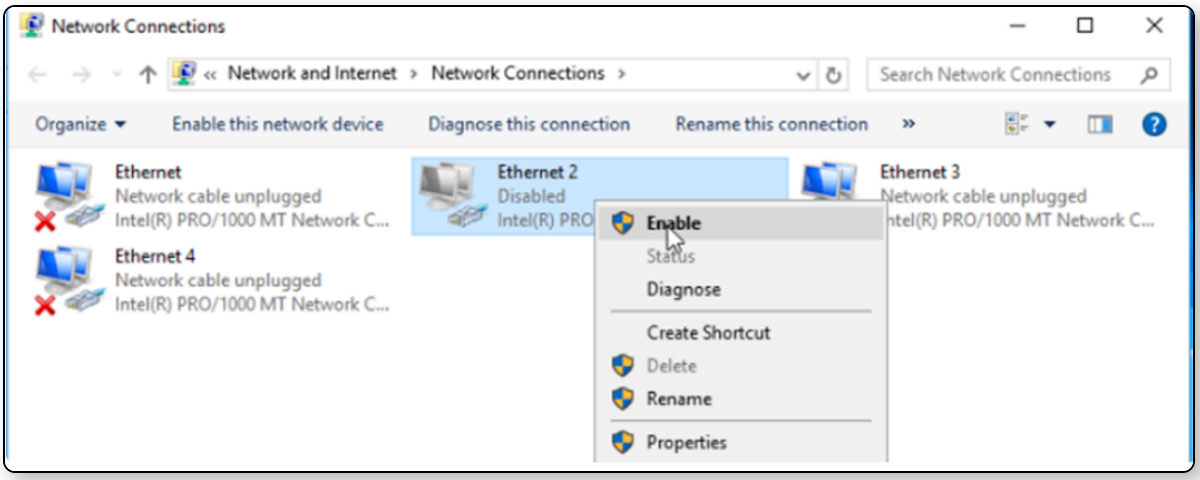
LABORATORY 6: Centralized management of privileged accounts:

We will integrate FortiPAM with some Fortinet solutions such as FortiGate and FortiAnalyzer, we will see how to block SSH commands, record session and the approved process. Also, we will include a Windows server, and we will use AutoIT to execute customized application tasks. This will demonstrate the advantages of using a PAM solution in a corporate security posture.

a) Some lab´s issues to keep in mind.

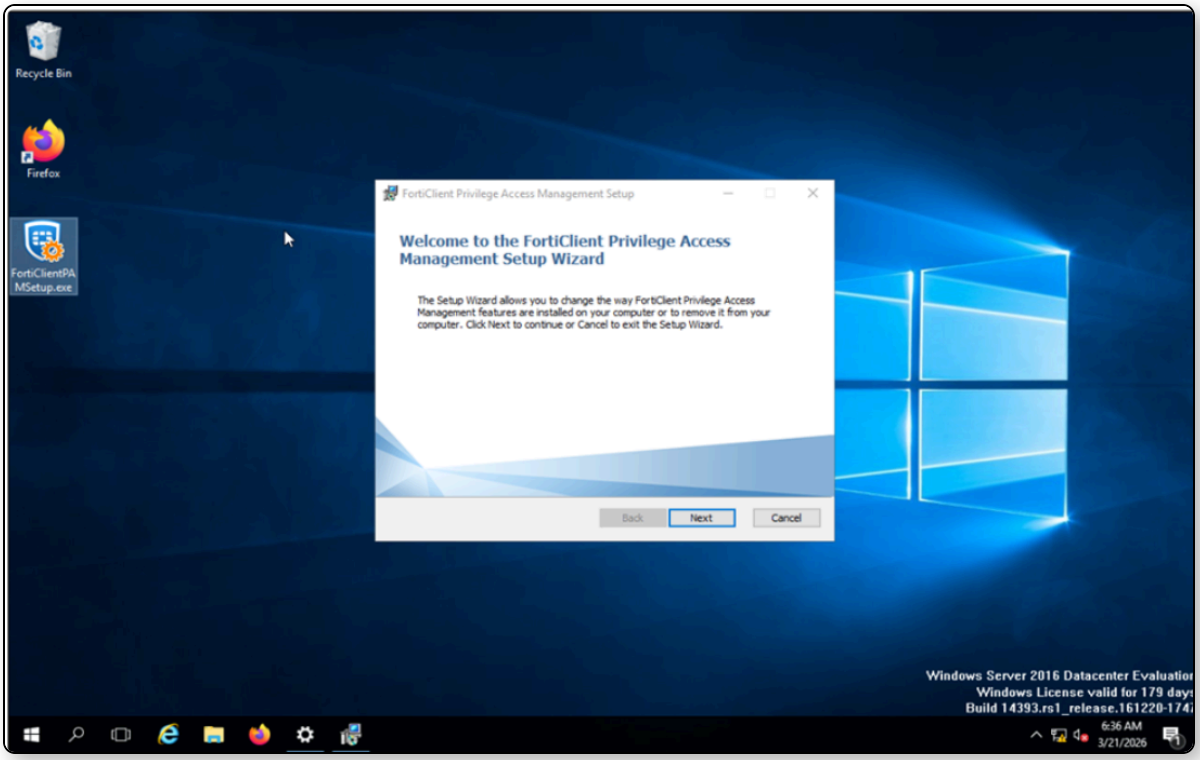
- The “Victim” device shows an alert about network interface. We advise is disable and enable the interface: 





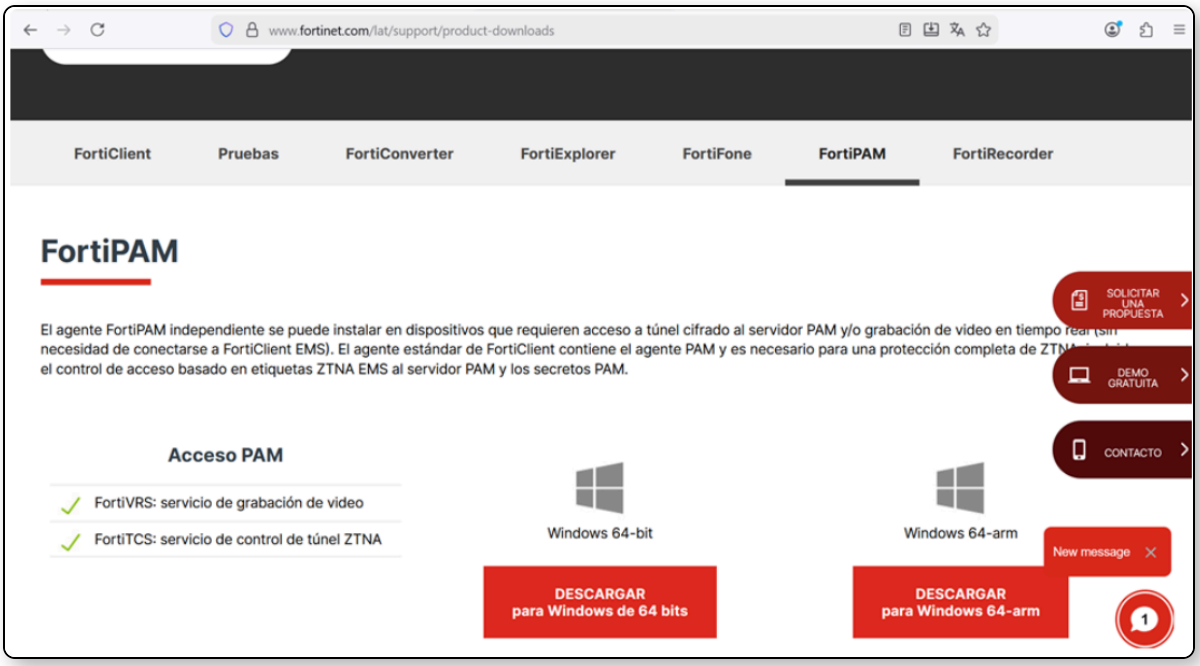
b) Preparing the FortiPAM´s client device

Let´s go to access in “Victim” device via “Display” and we need to install “FortiClientPAM.exe”. Please follow the installation procedure and accept the terms.

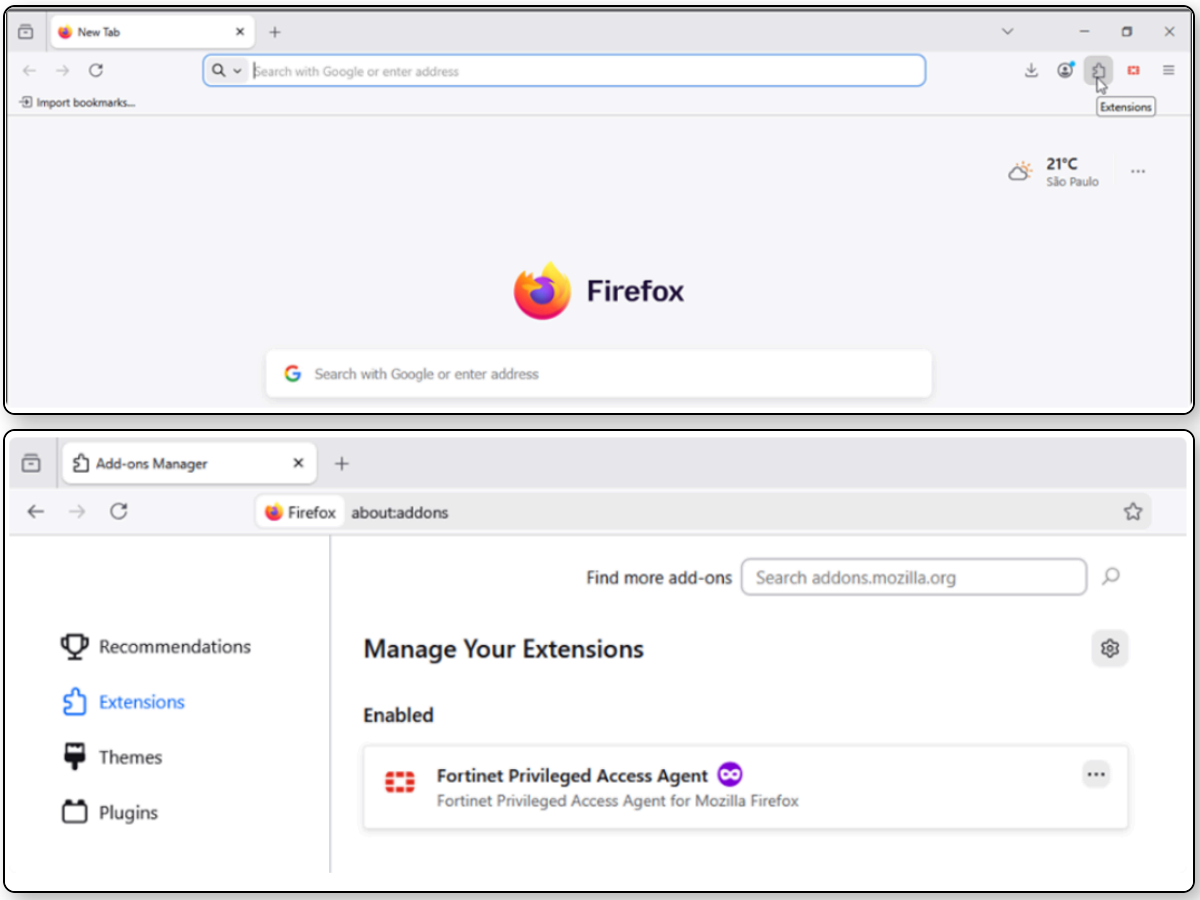


Remember these couple of things:

- The FortiPAM´s installer you can get in the official Fortinet web portal when we download the FortiClient: • https://www.fortinet.com/lat/support/product-downloads



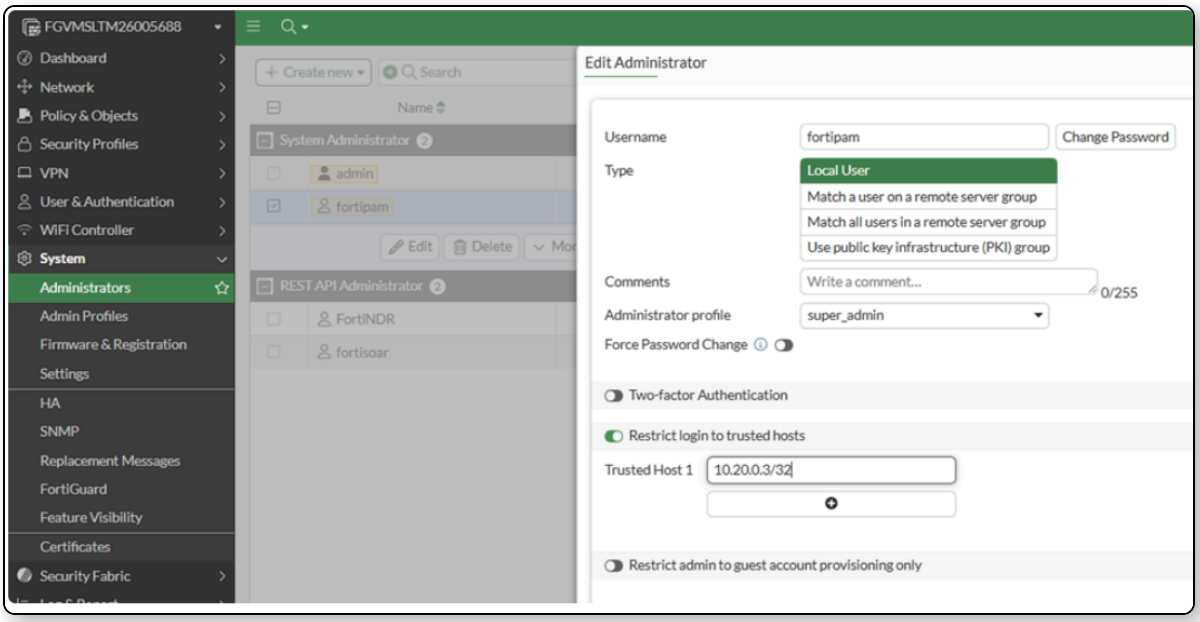
- FortiClient´s PAM does not coexist with any FortiClient´s product free.
- In addition to FortiClient´s PAM, we recommend installing the browser´s extension.
- In this case we are going to use “Firefox”. Open Firefox, go to “Extensions”, search “Fortinet Privileged Access Agent” and proceed to install.



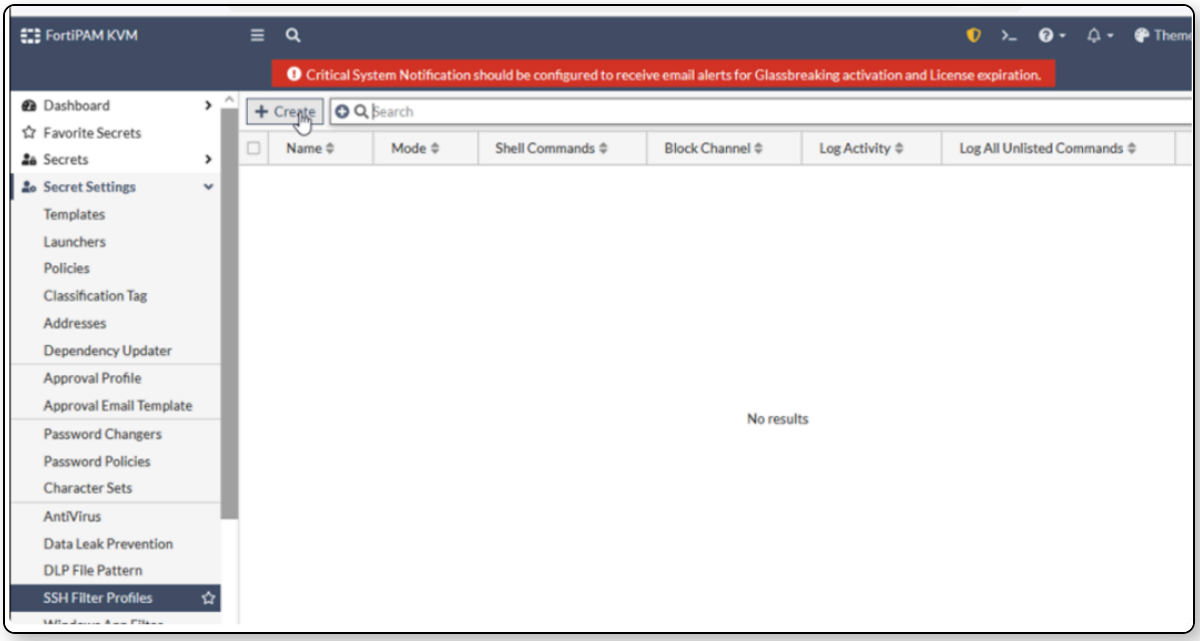
- Now we have the client ready to work with FortiPAM.

c) Integration FortiGate with FortiPAM

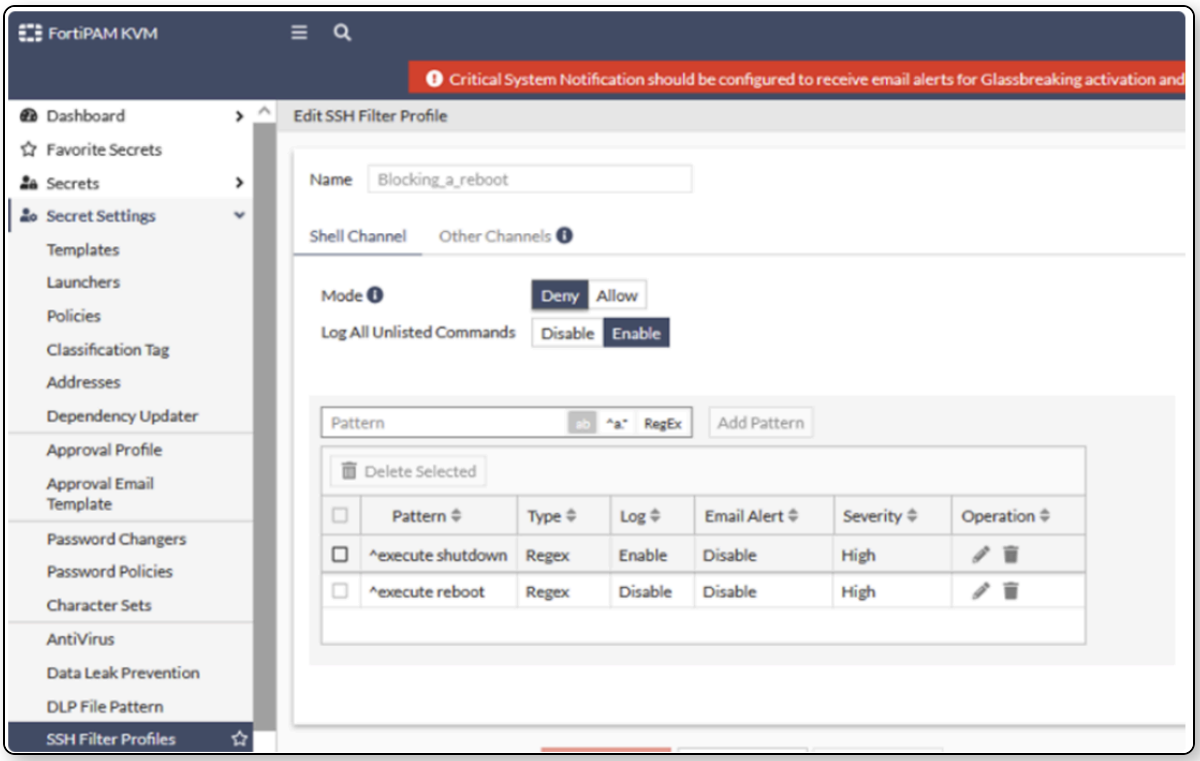
- First, let´s go to access FortiGate via HTTPS. We should create an Admin user to integrate FortiGate with FortiPAM.
- In this way if we have some issue with FortiPAM we will have other admin user as “Access emergency”. The “Access emergency” should be guarded with caution.
- Let´s go to create a new Administrator user called “fortipam” with “super_admin” as administrator profile. We suggest this user should have “Restrict login to trusted hosts” with the FortiPAM´s address.



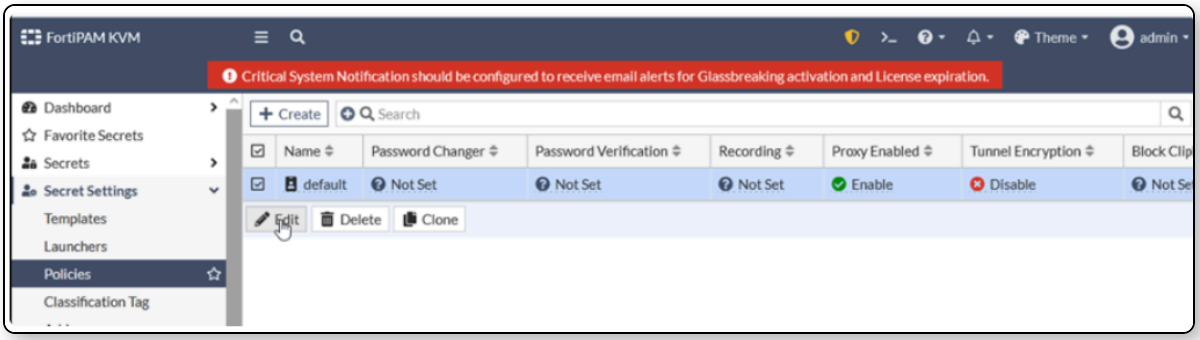
- In the “Victim” device let´s open a browser and go to access FortiPAM throw https://10.20.0.3 with the user “admin”
- In “Secrets Settings → SSH Filter Profile” click in “Create”.



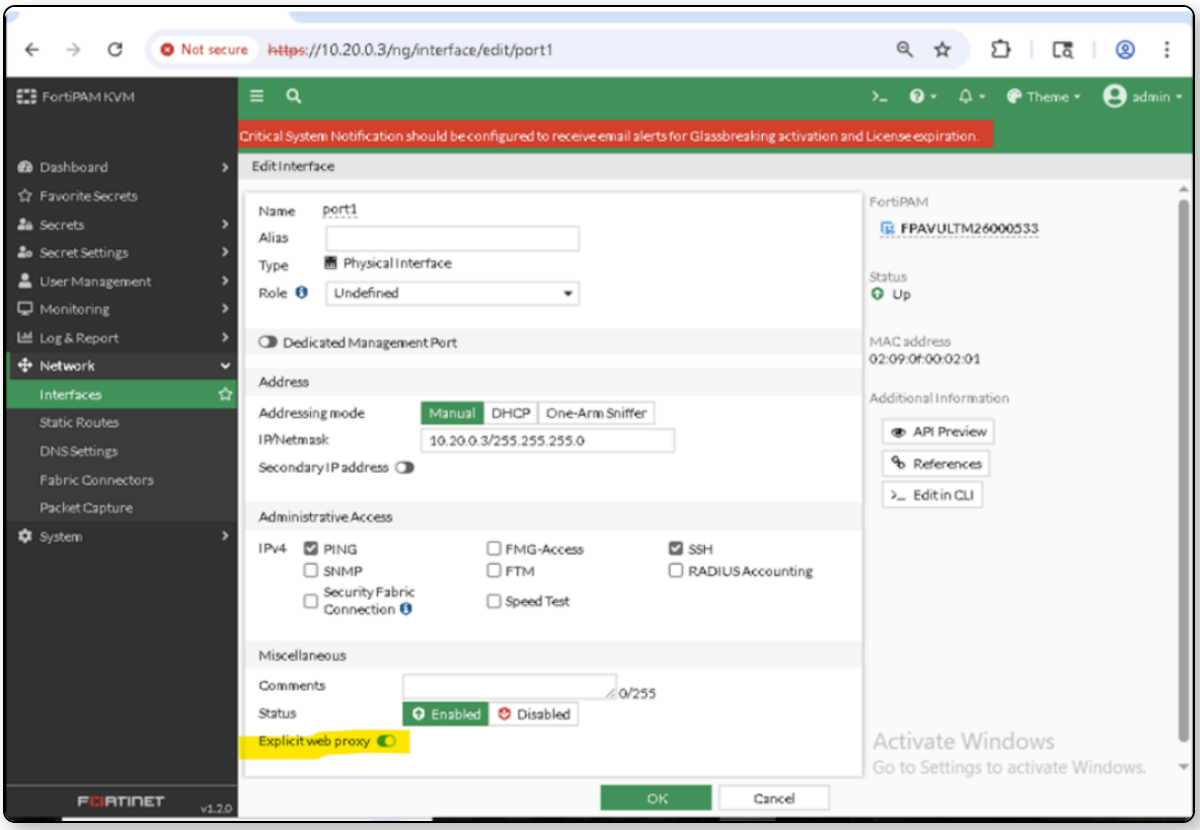
- Let´s go to create a “SSH Filter Profile” with the name “Blocking_a_reboot” in the next way and click in “Save”.



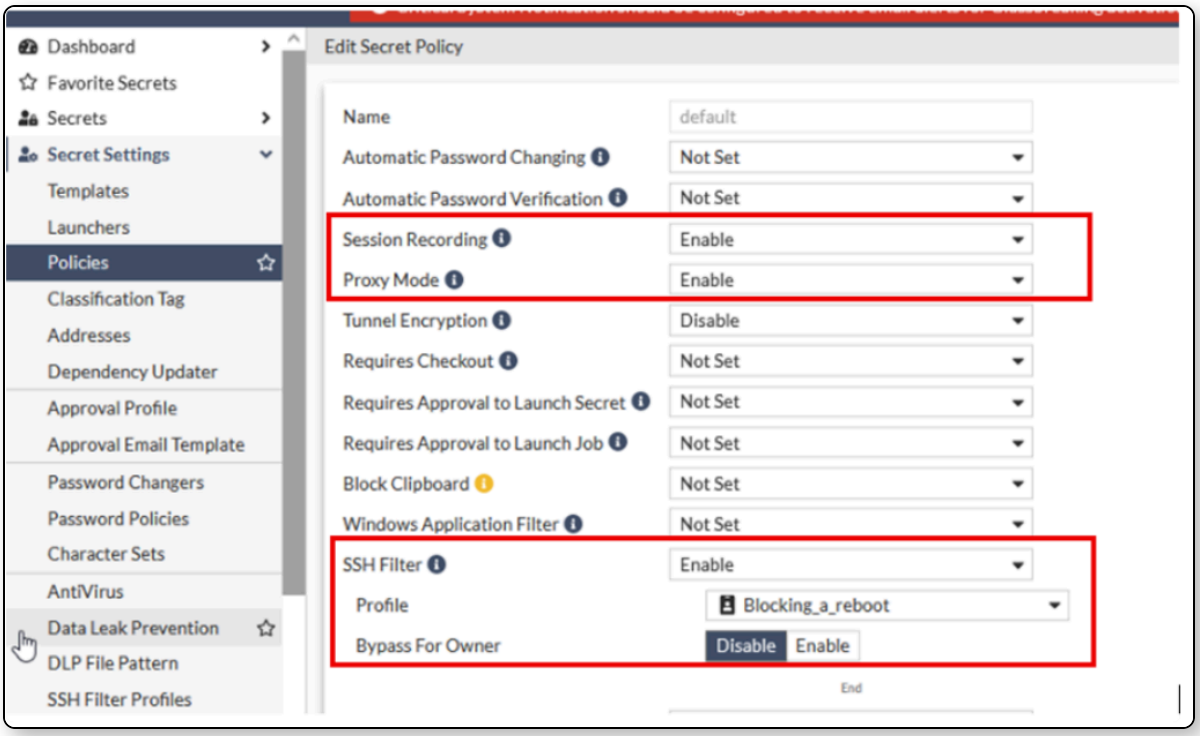
- In “Secrets Settings → Policies → default” we can see the default policy that apply a every device integrated in FortiPAM.
- We can edit this policy or create other to we need. Let´s to edit “default” policy:



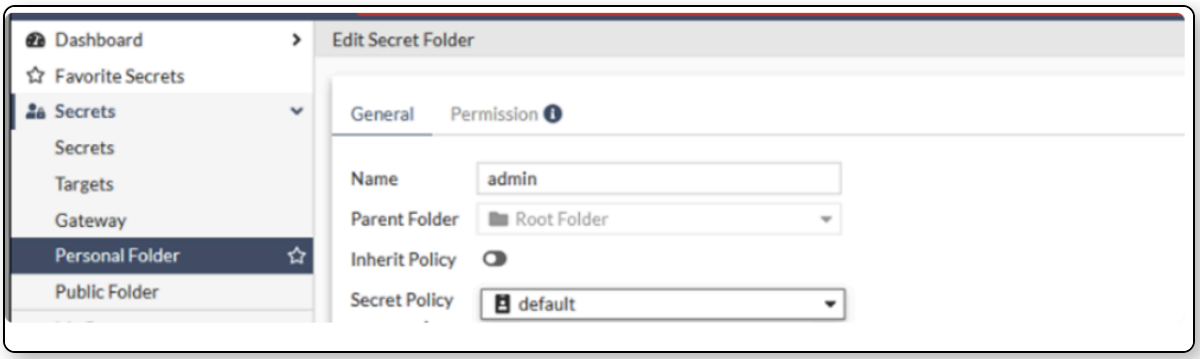
- You will need to activate "Explicit Web proxy" in FortiPAM´s port1:



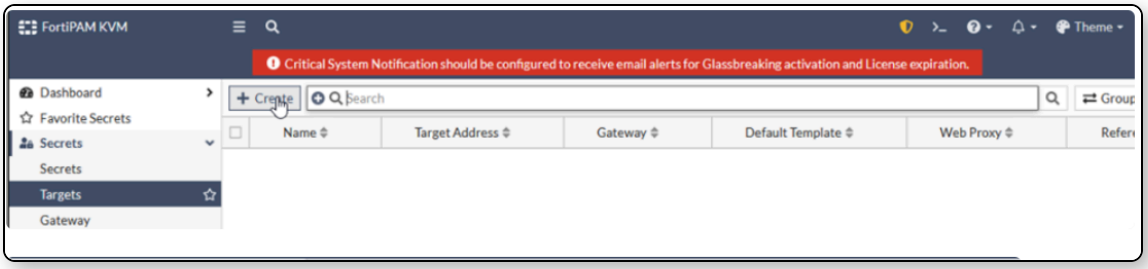
- We can edit this policy as the next image, leave the other field in default and click in “Save”.

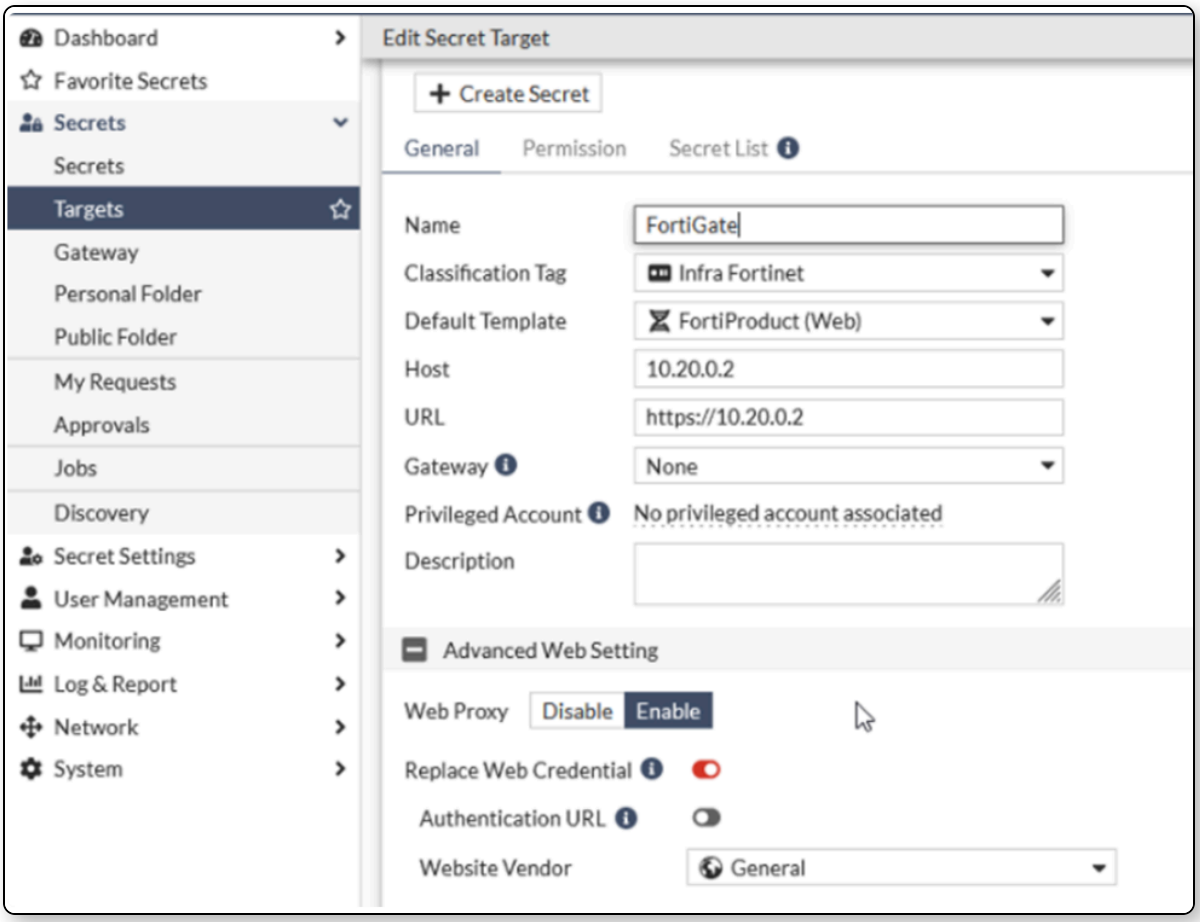


- Make sure the personal folder “Admin” has assigned in “Secret Policy” “default”. Go to “Secrets → Personal Folder → General”.

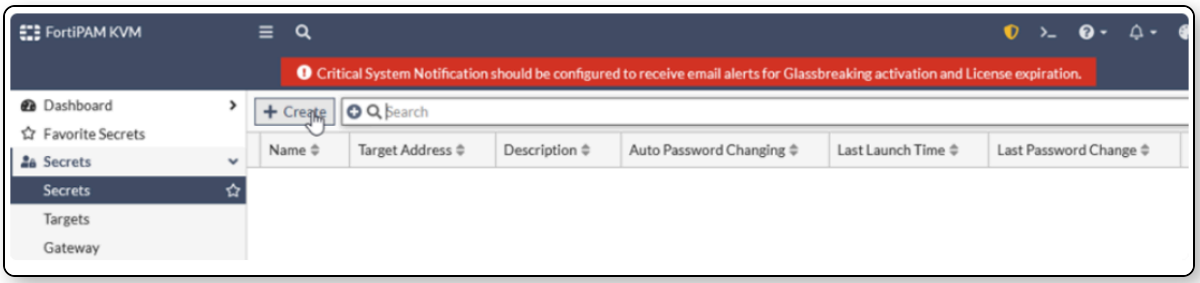


- Let´s go to create a “Target” associated to FortiGate. Go to “Secrets → Targets → Create”
- Remembe your FortiGate´s IP is 10.20.0.254.

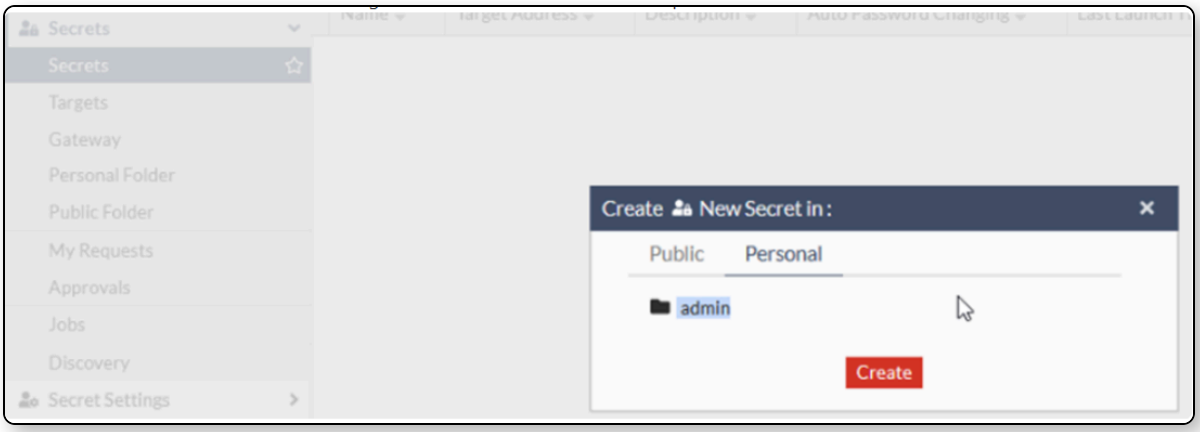




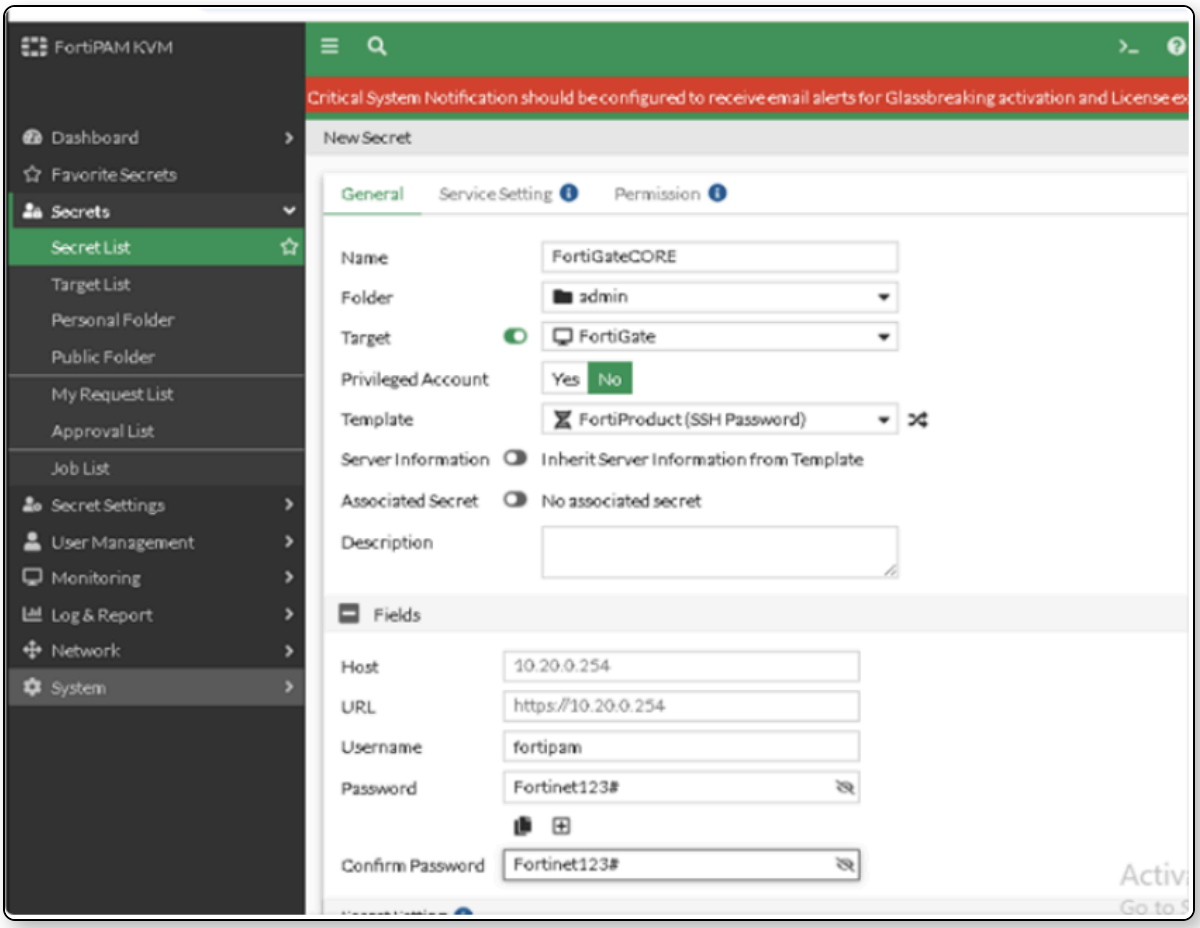
- Let´s go to create a “Secret” associated to “Target” created in the step before:



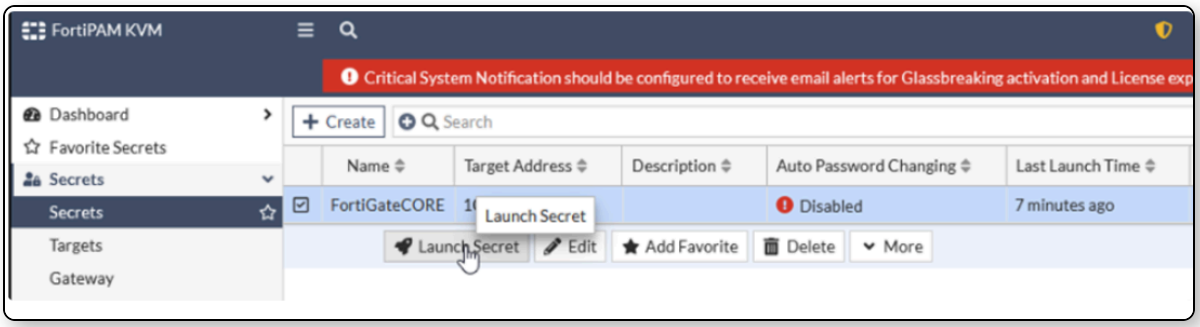
- Since we don't have custom folders to organize secrets, let's use the default personal admin folder.



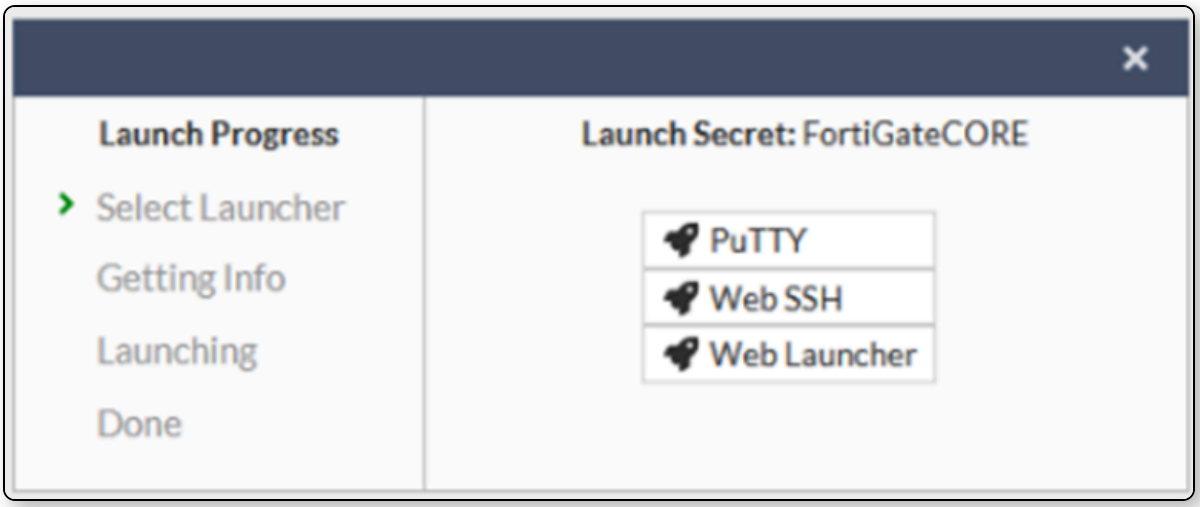
- Create the new “Secret” with the next configuration and click in “Submit”:



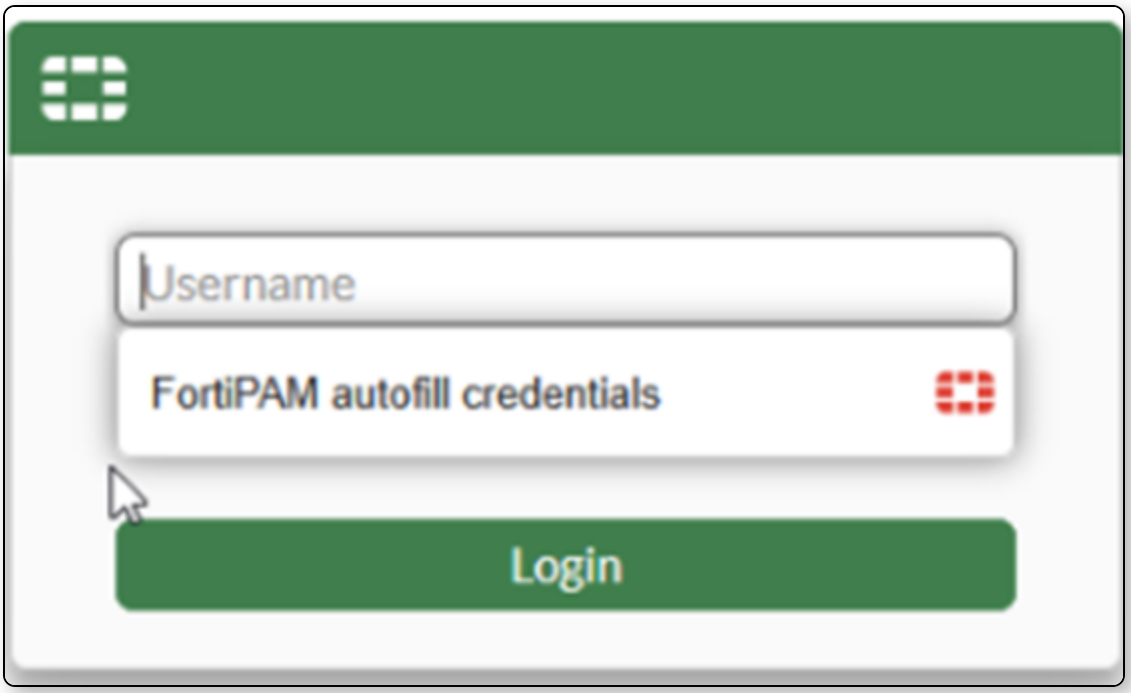
- Now we can test the access to FortiGate throw FortiPAM. In the FortiPAM Let´s go to “Secrets”. Go to “Secrets → FortiGateCORE” and click in “Launch Secret”.



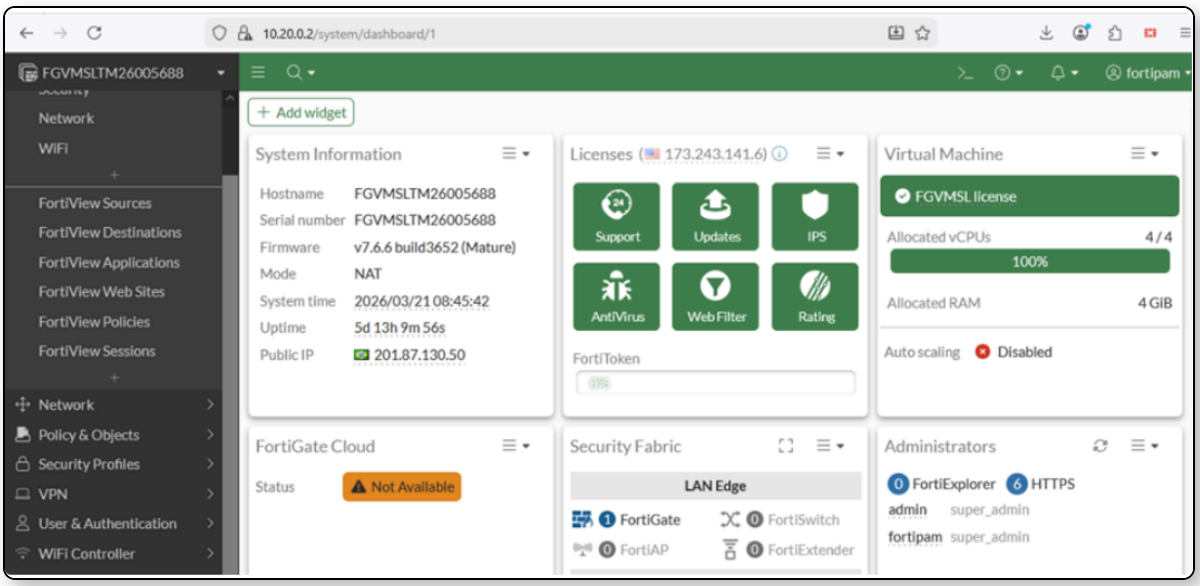
- Now, FortiPAM shows us 3 ways to connect to FortiGateCORE; PUTTY, Web SSH and Web Launcher.
- This launchers are associated to the “Default Template” selected for the “Target” configuration. Let´s go to try every connect way. Click in “Web Launcher”:



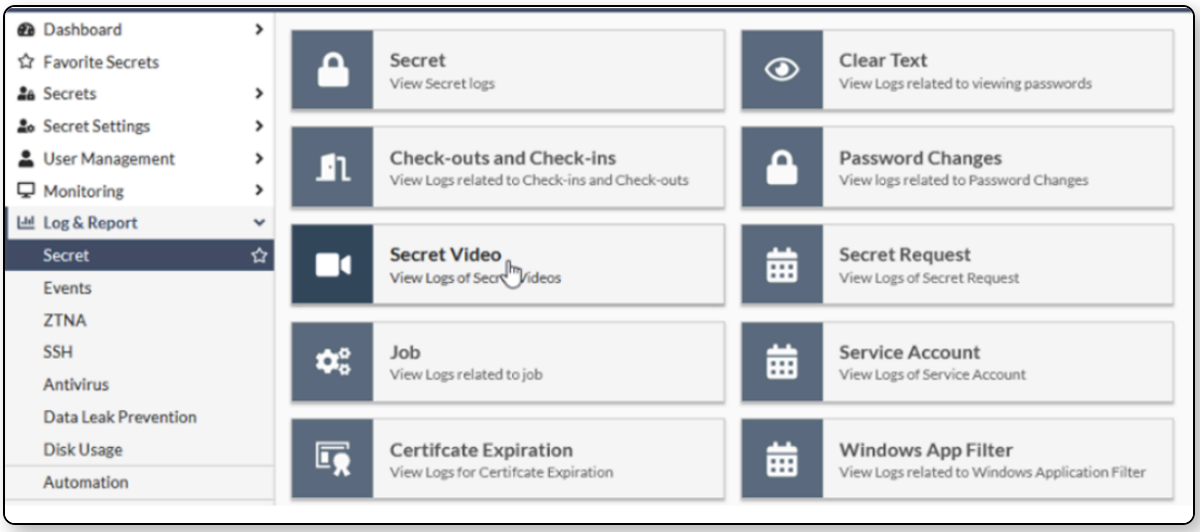
- We need to select “FortiPAM autofill credencials” and click in “Login”:



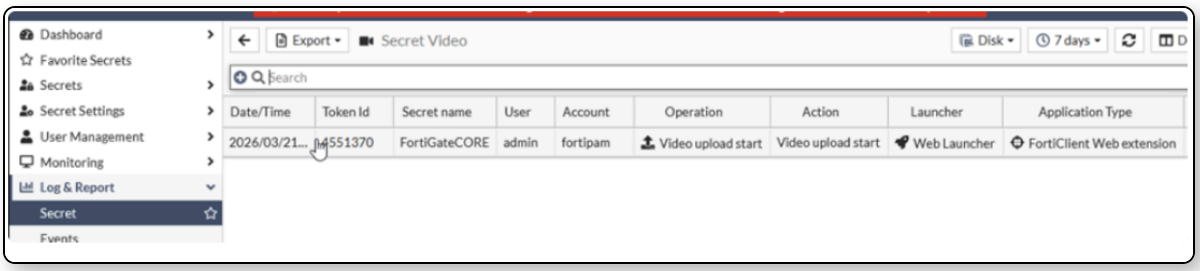
- We can access FortiGate without knowledge of the credentials access and every we do will be recorded.
- Please give us a little walkthrough in FortiGate. Remember, every thing will be recorded.

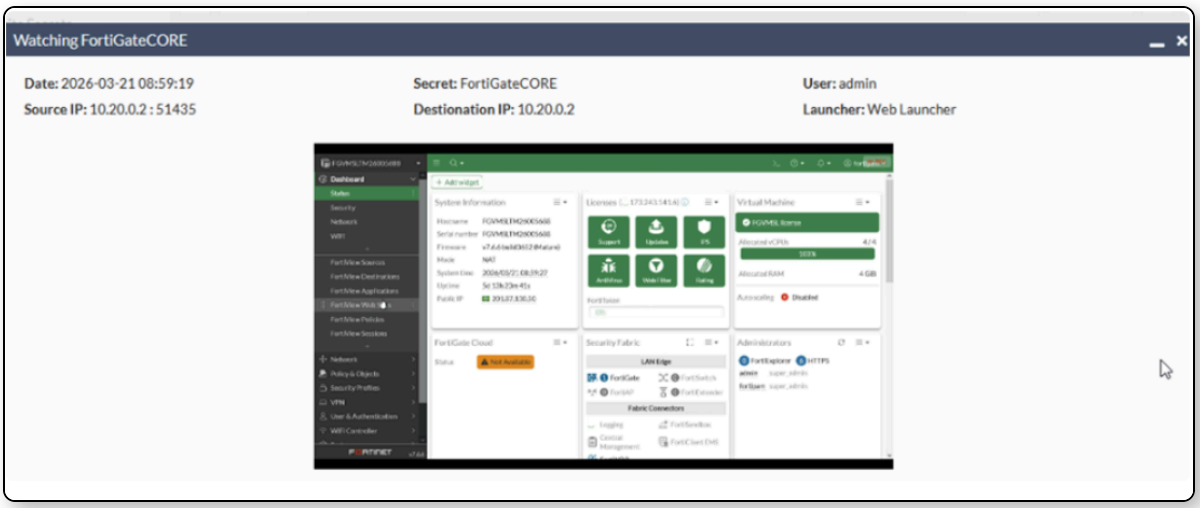


- After you close session, in the FortiPAM you can go to “Log & Report → Secret → Secret Video”:

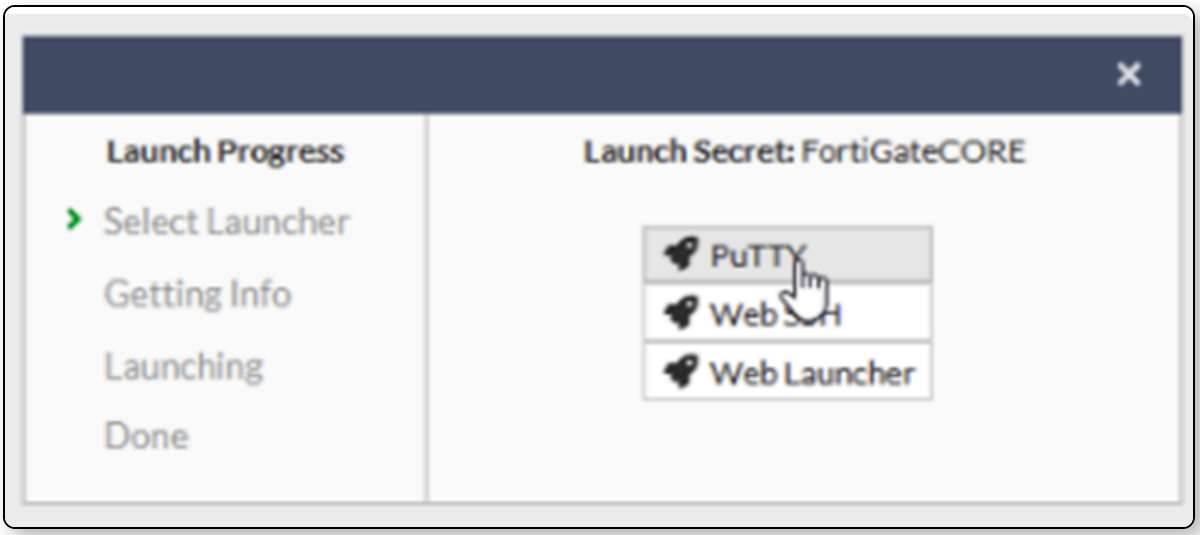


- Here you can see every session recorded. Plase open a video with a double click in every video that you want to see:

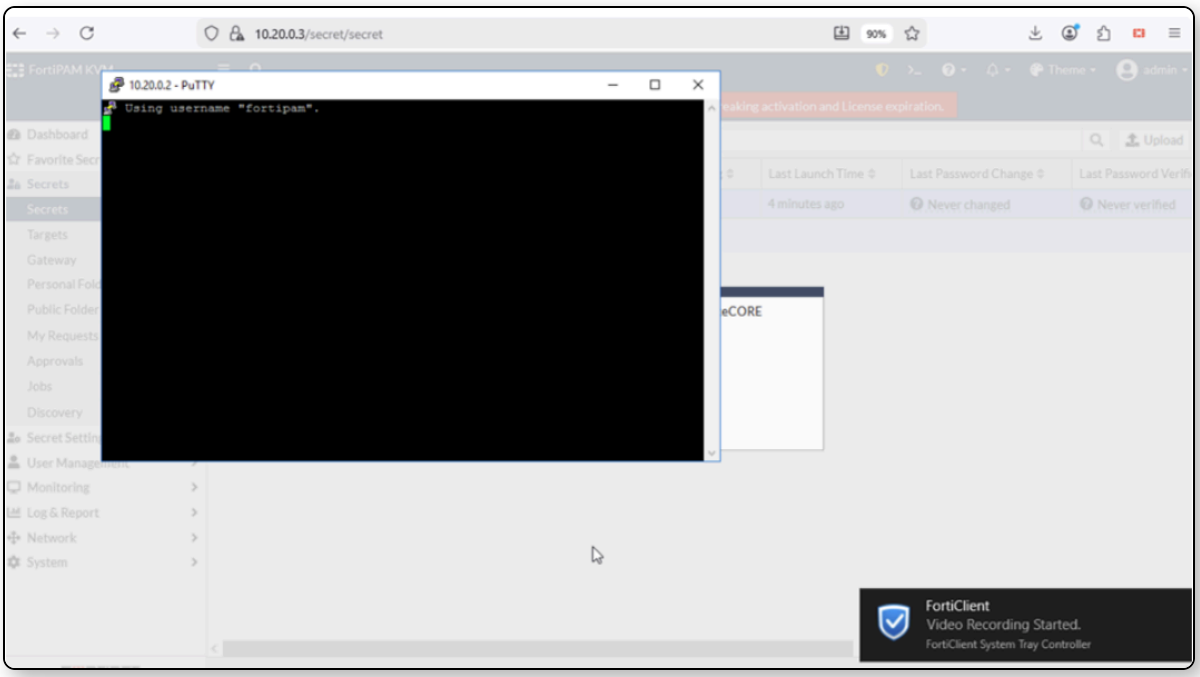




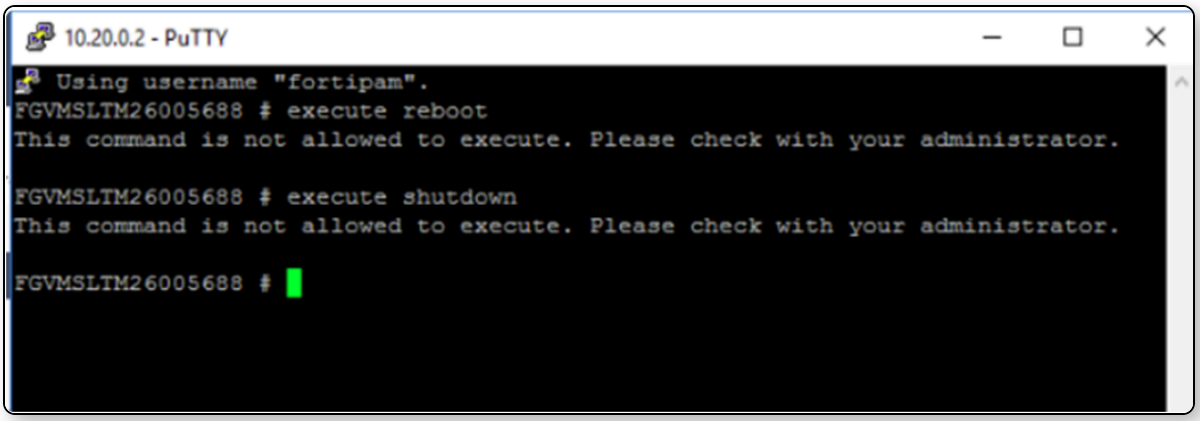
- We can test the “SSH Filter” launching a “PUTTY” connection and “Web SSH” connection. Let´s to open a “PUTTY”.



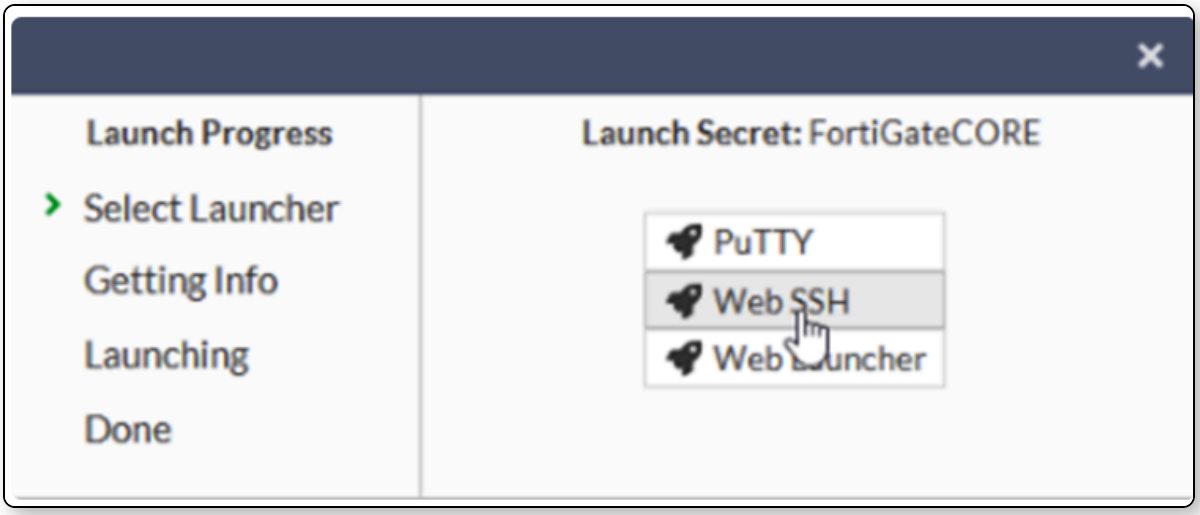
- The FortiClient PAM launch automatically the PUTTY and starts the record:

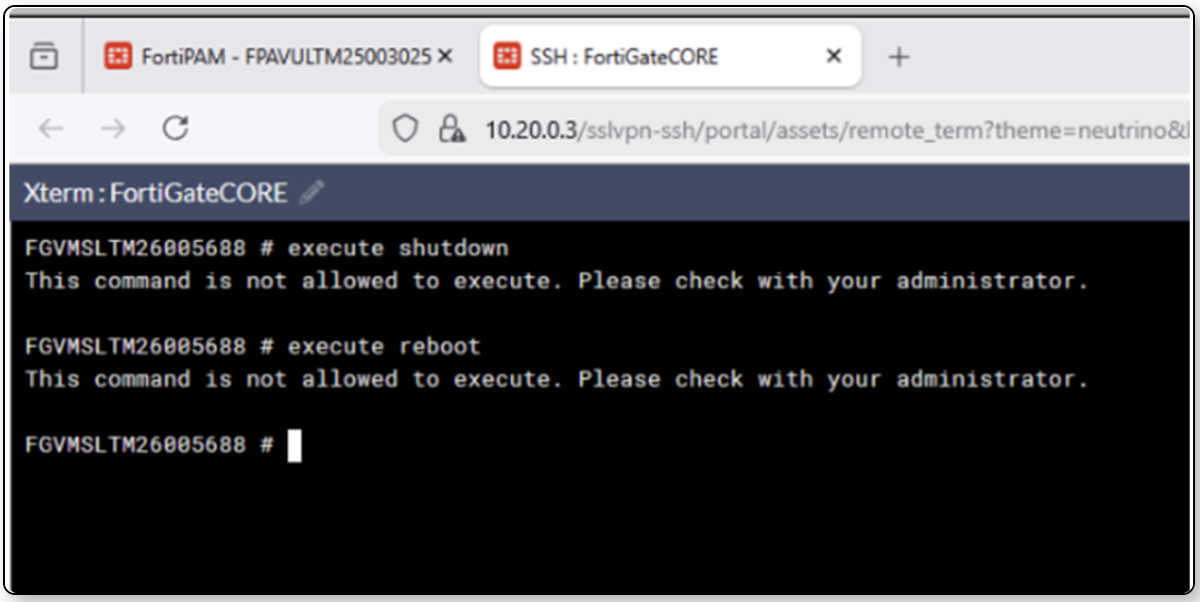


- Additional when we try a “Shutdown” or a “Reboot” these commands are blocked:

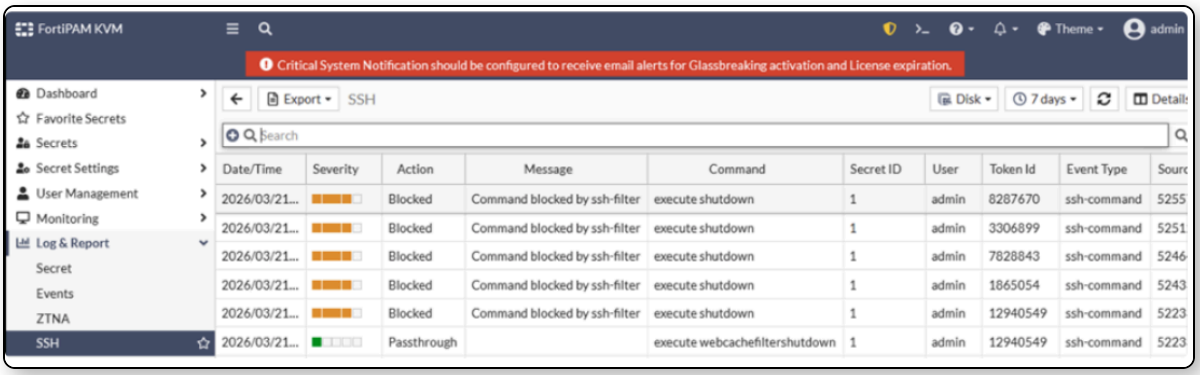


- We can test a “Web SSH” connection:





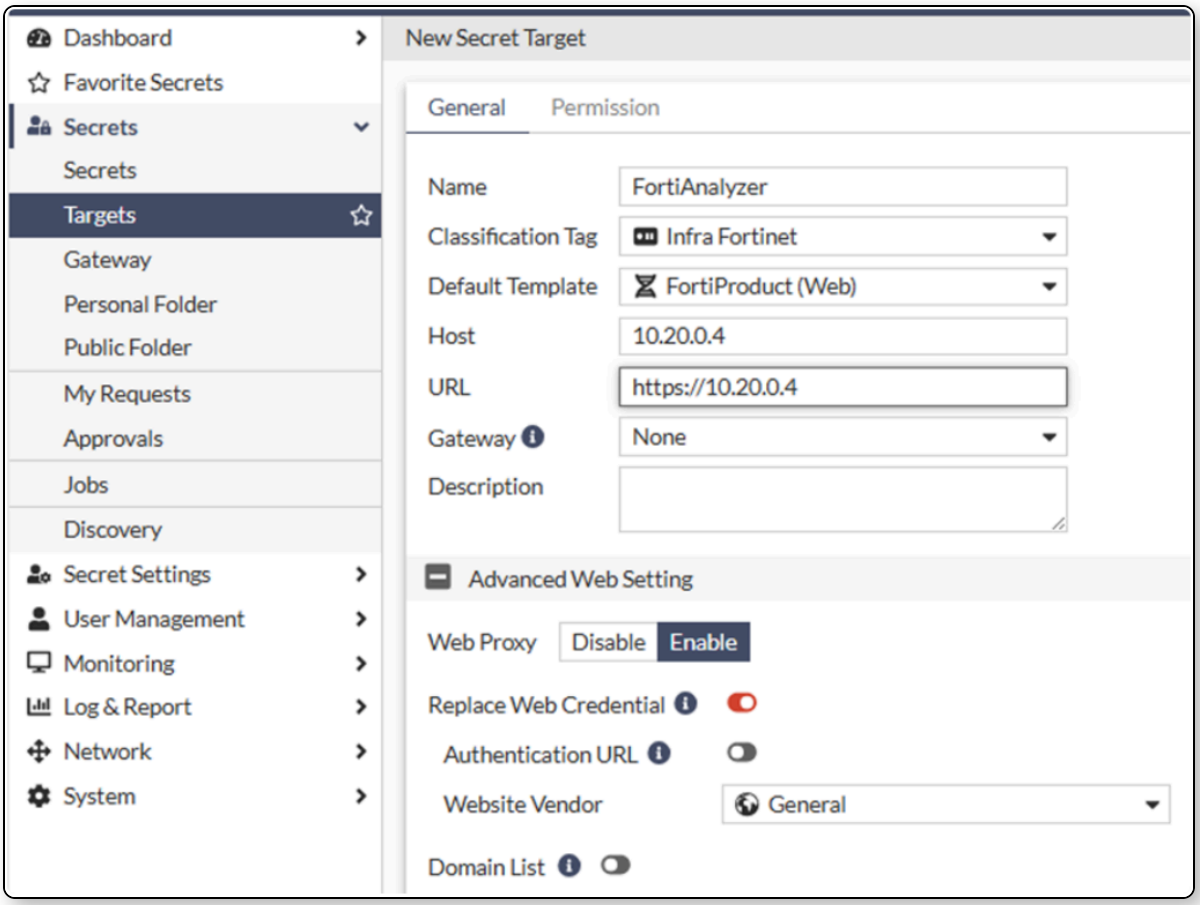
- We can review the logs generated in SSH connection, in FortiPAM go “Log & Report → SSH”:



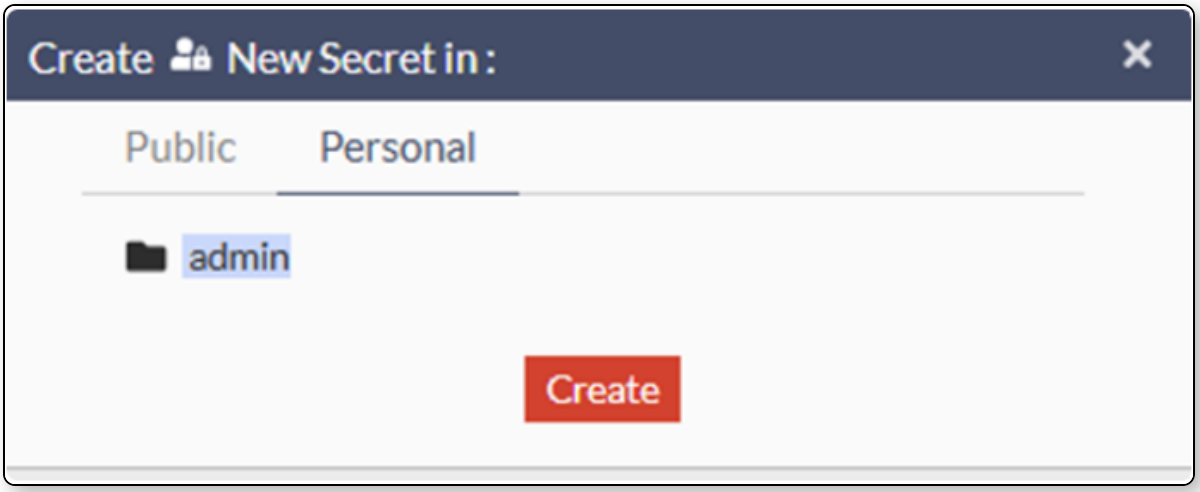
d) Integration of FortiAnalyzer and FortiPAM

In the same way that we integrated FortiGate, we are going to integrate FortiAnalyzer with FortiPAM. Please access to FortiPAM via HTTPS.

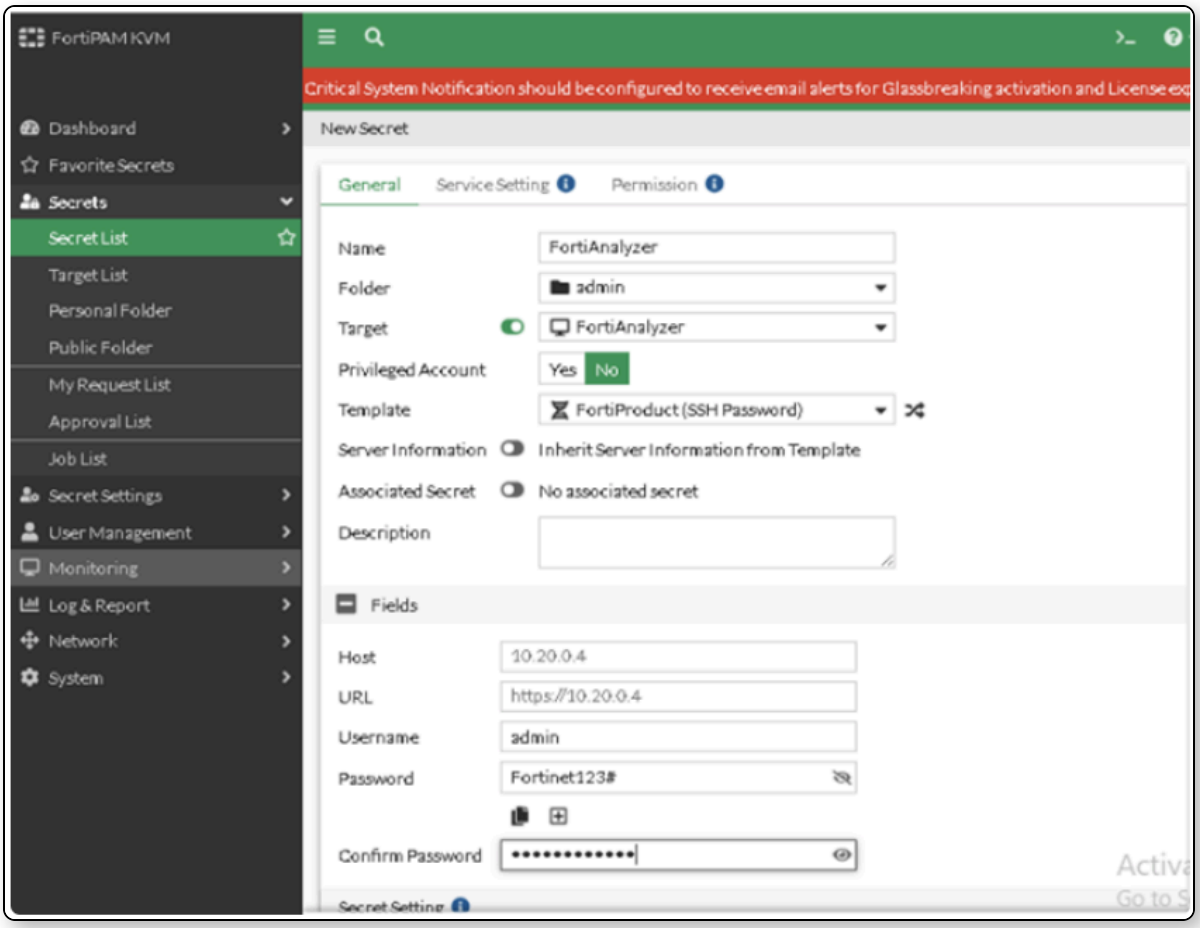
- In FortiPAM go to “Secrets → Targets” and click in “Create”. Let´s to create the next “Target”:



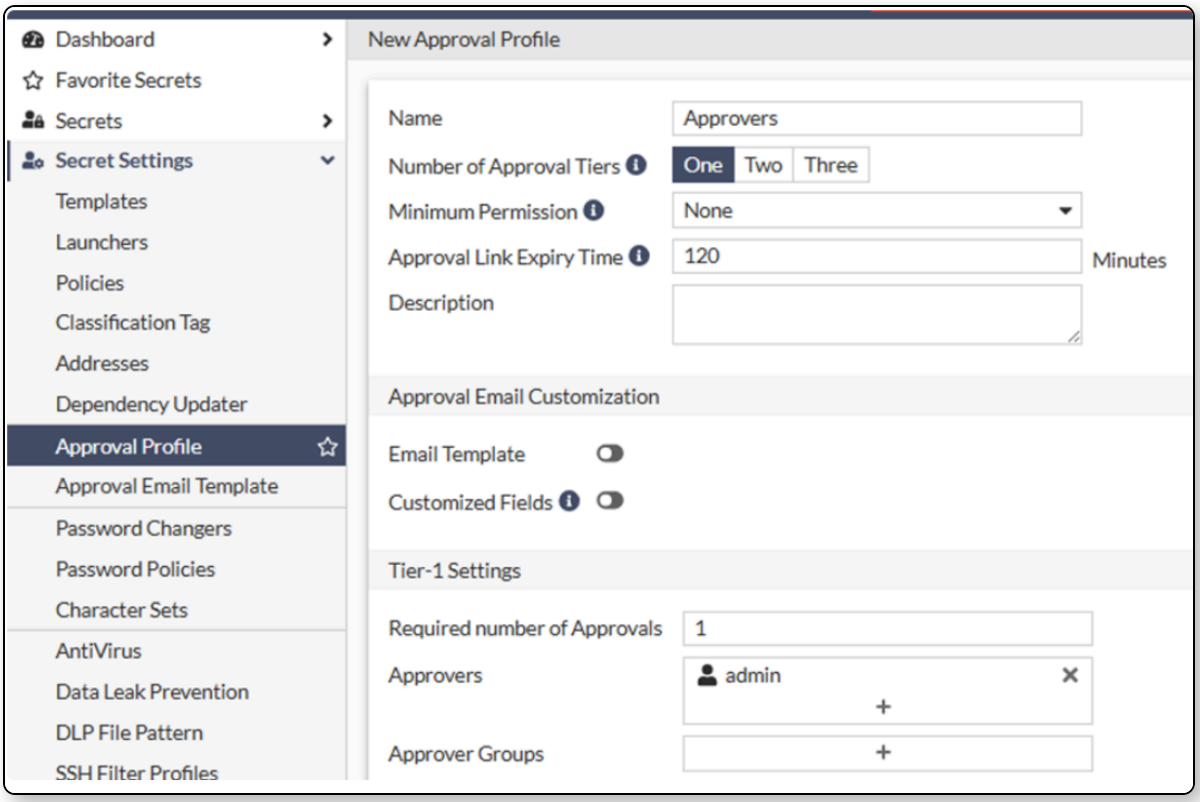
- Go to “Secrets → Secrets” and click in “Create”. Let´s go to create the “Secret” for FortiAnalyzer. Select “Create New Secret in” folder “Personal → admin”:



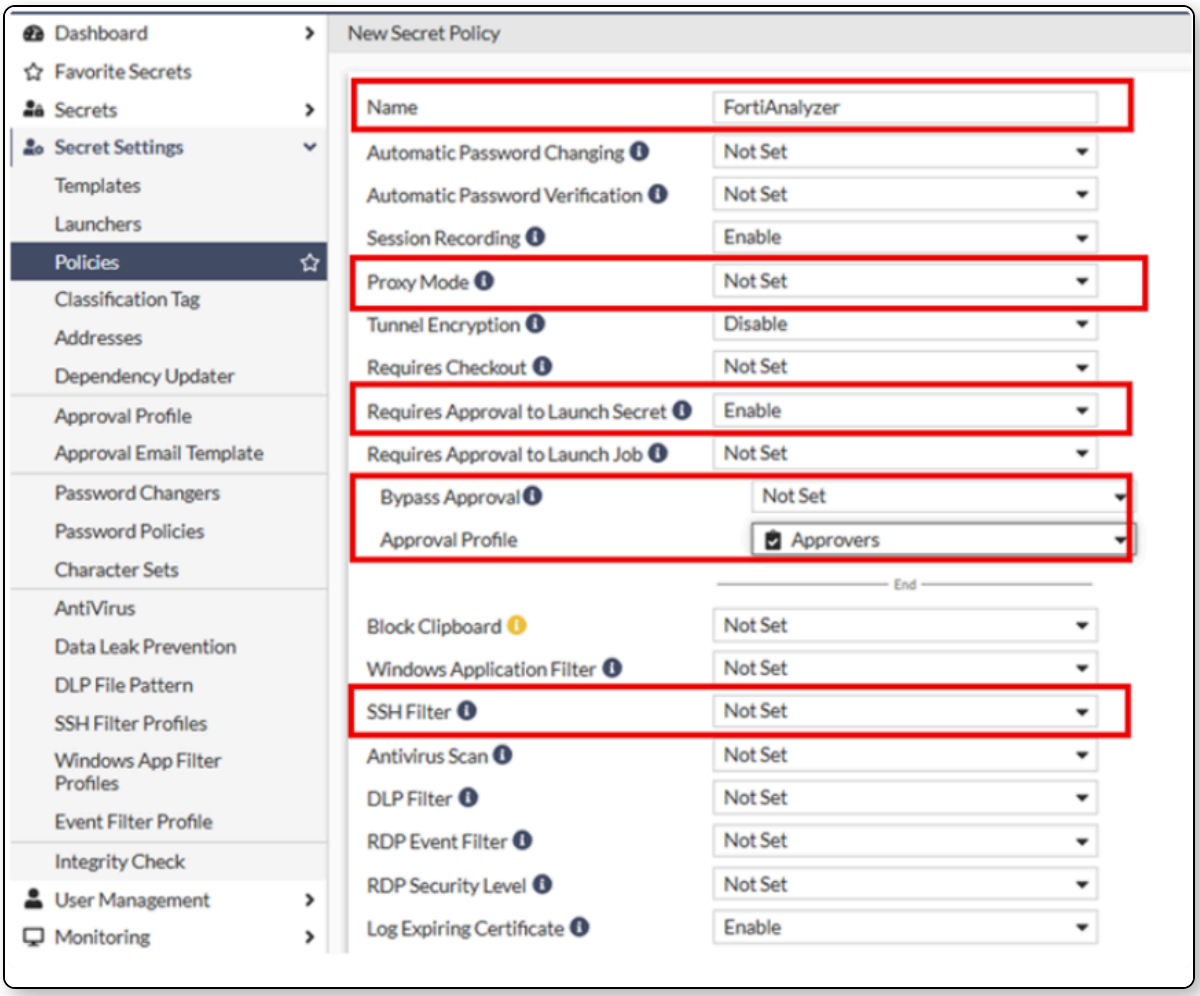
- Fill up the next information and click in “Submit”.



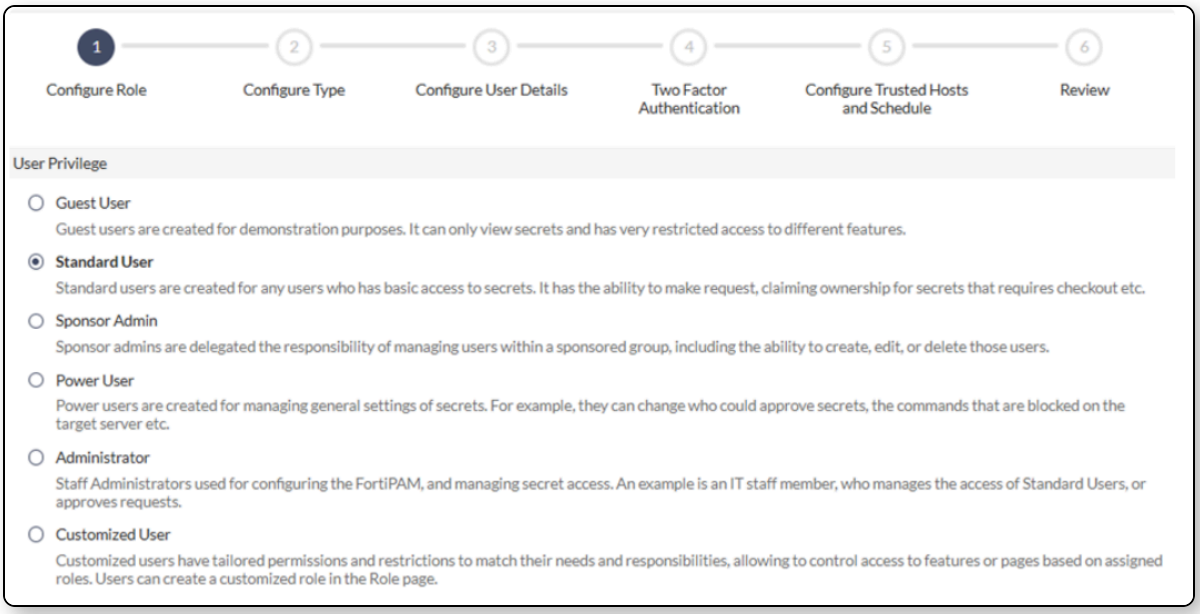
- Go to “Secret Settings → Approval Profile” and let´s to create the next profile:

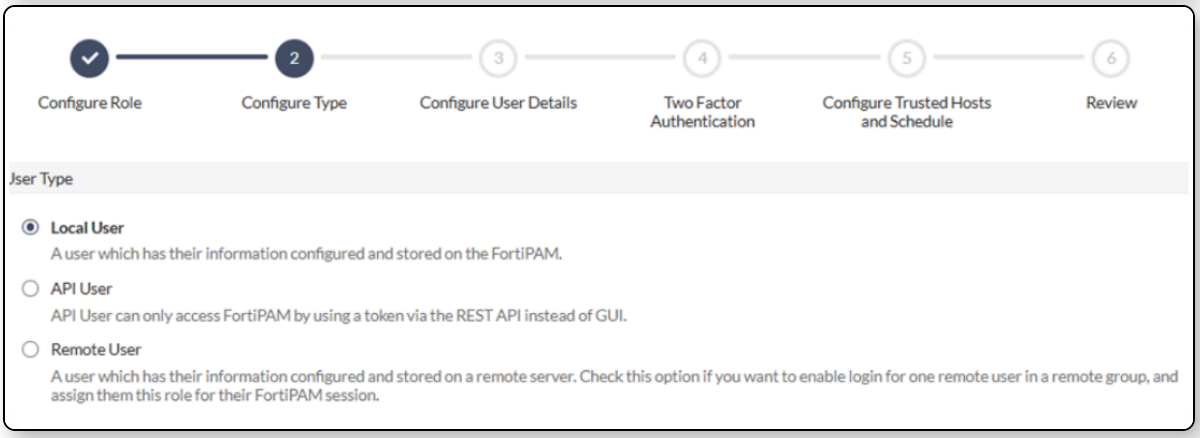


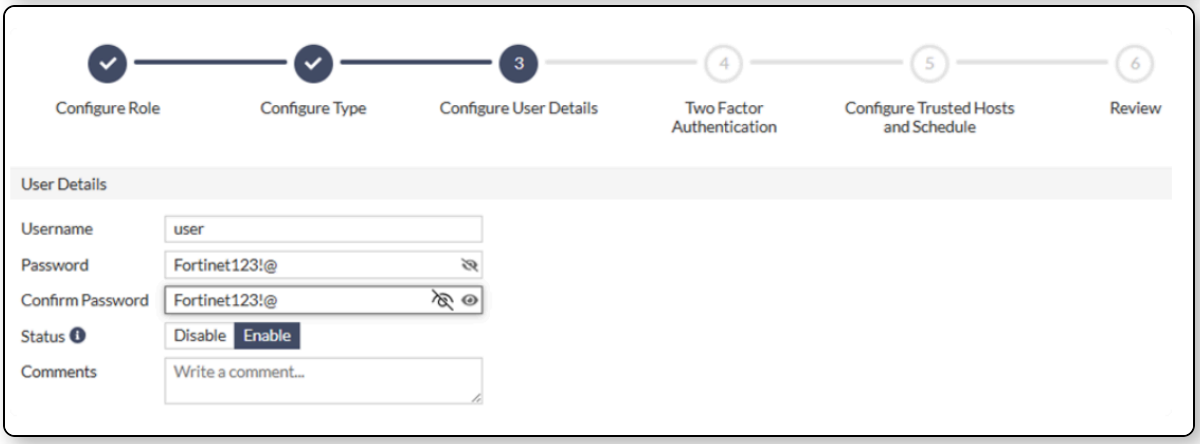
- Let´s to create a new “Secret Policy”. Go to “Secret Settings → Policies” and create the next policy:

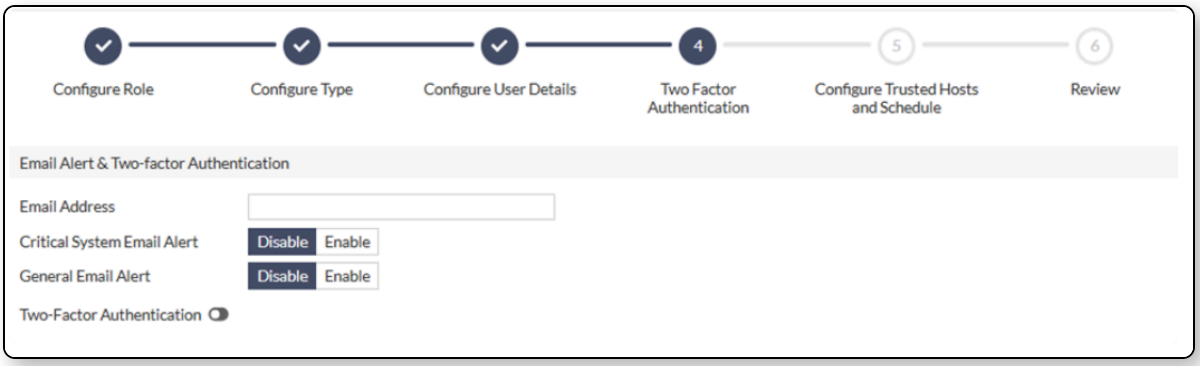


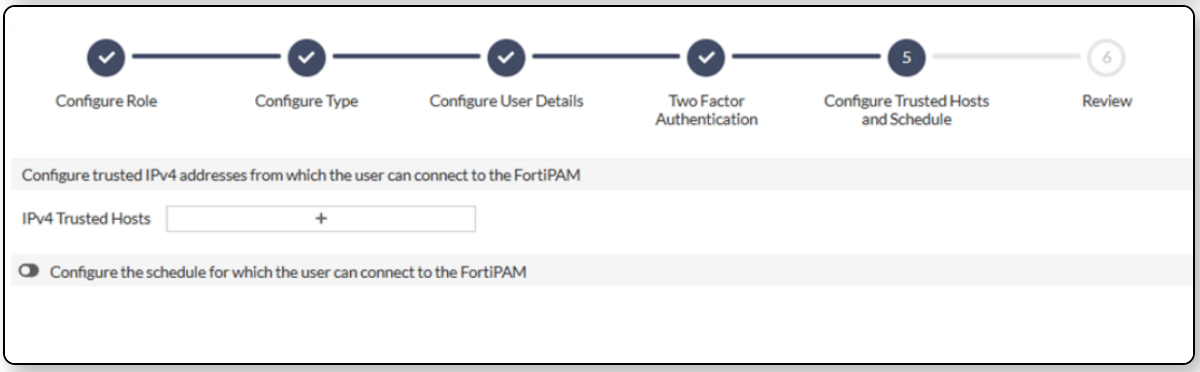
- You can see that this policy does not have “SSH Filter”, is not using “Proxy Mode” and needs approval to use the launcher.
- Let´s to create a new user. Go to “User Management → User List” and click in “Create” follow the next instructions and click in “Next”:

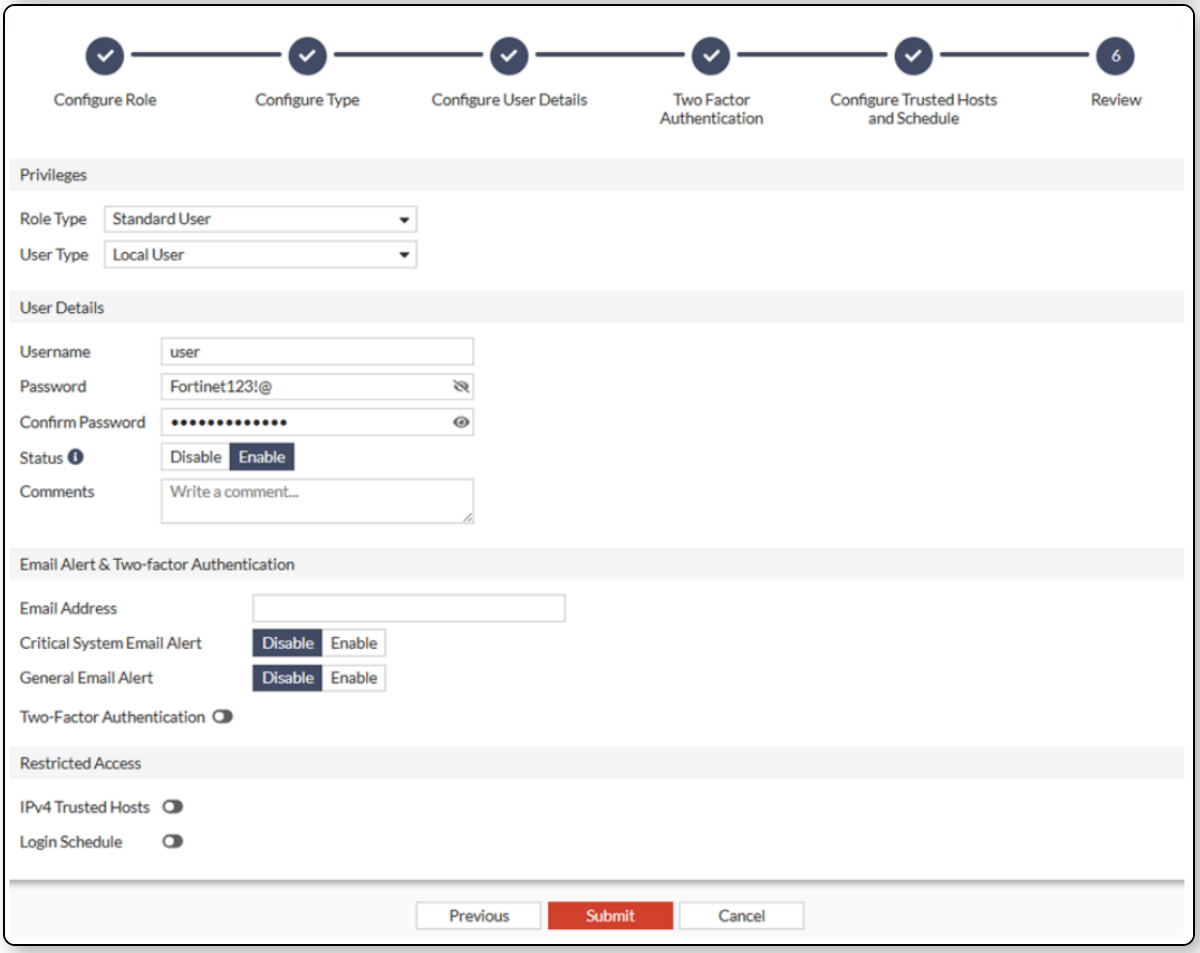

1 Configure Role
2 Configure Type
3 Configure User Details
4 Two Factor Authentication
5 Configure Trusted Hosts and Schedule
6 Review
User Privilege
Guest User
Guest users are created for demonstration purposes. It can only view secrets and has very restricted access to different features.
Standard User
Standard users are created for any users who has basic access to secrets. It has the ability to make request, claiming ownership for secrets that requires checkout etc.
Sponsor Admin
Sponsor admins are delegated the responsibility of managing users within a sponsored group, including the ability to create, edit, or delete those users.
Power User
Power users are created for managing general settings of secrets. For example, they can change who could approve secrets, the commands that are blocked on the target server etc.
Administrator
Staff Administrators used for configuring the FortiPAM, and managing secret access. An example is an IT staff member, who manages the access of Standard Users, or approves requests.
Customized User
Customized users have tailored permissions and restrictions to match their needs and responsibilities, allowing to control access to features or pages based on assigned roles. Users can create a customized role in the Role page.


Configure Role
2 Configure Type
3 Configure User Details
4 Two Factor Authentication
5 Configure Trusted Hosts and Schedule
6 Review
Jser Type
Local User
A user which has their information configured and stored on the FortiPAM.
API User
API User can only access FortiPAM by using a token via the REST API instead of GUI.
Remote User
A user which has their information configured and stored on a remote server. Check this option if you want to enable login for one remote user in a remote group, and assign them this role for their FortiPAM session.

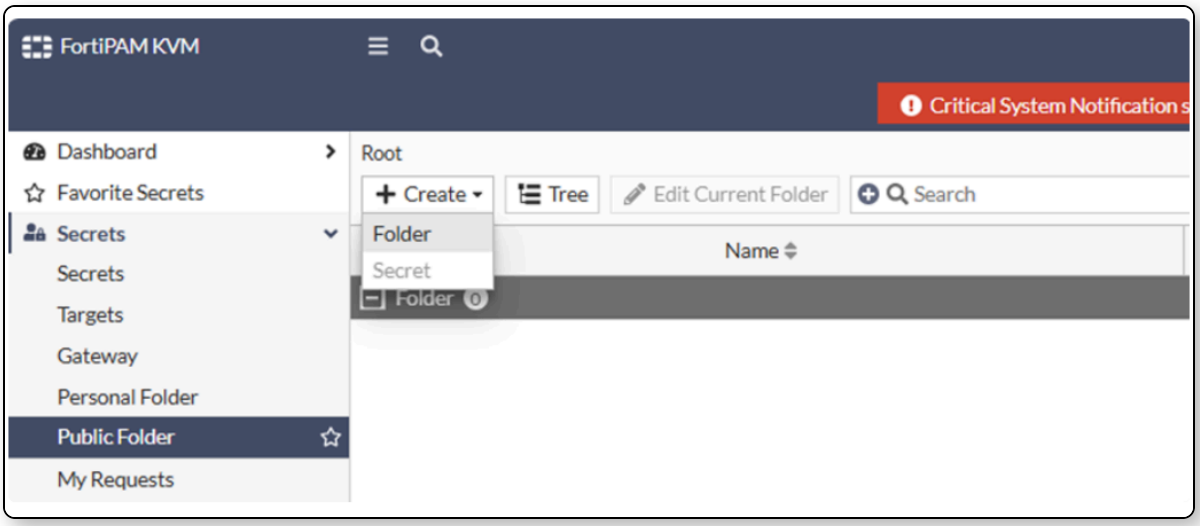

Configure Role
Configure Type
3 Configure User Details
4 Two Factor Authentication
5 Configure Trusted Hosts and Schedule
6 Review
User Details
Username
user
Password
Fortinet123!@
Confirm Password
Fortinet123!@
Status
Disable
Enable
Comments
Write a comment...

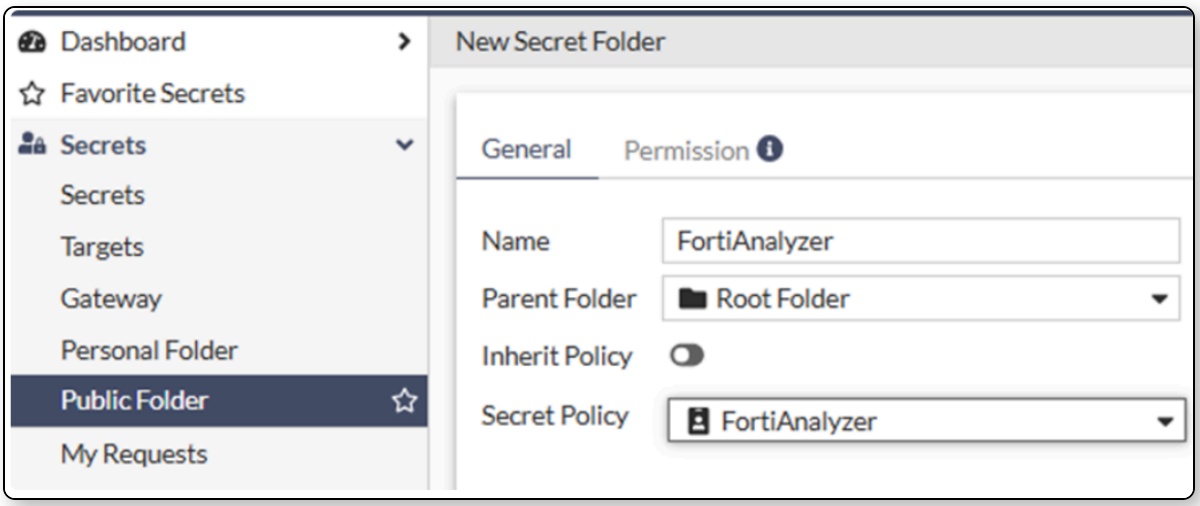

Configure Role
Configure Type
Configure User Details
4
Two Factor Authentication
5
Configure Trusted Hosts and Schedule
6
Review
Email Alert & Two-factor Authentication
Email Address
Critical System Email Alert
Disable
Enable
General Email Alert
Disable
Enable
Two-Factor Authentication


Configure Role
Configure Type
Configure User Details
Two Factor Authentication
5
Configure Trusted Hosts and Schedule
6
Review
Configure trusted IPv4 addresses from which the user can connect to the FortiPAM
IPv4 Trusted Hosts
+
Configure the schedule for which the user can connect to the FortiPAM

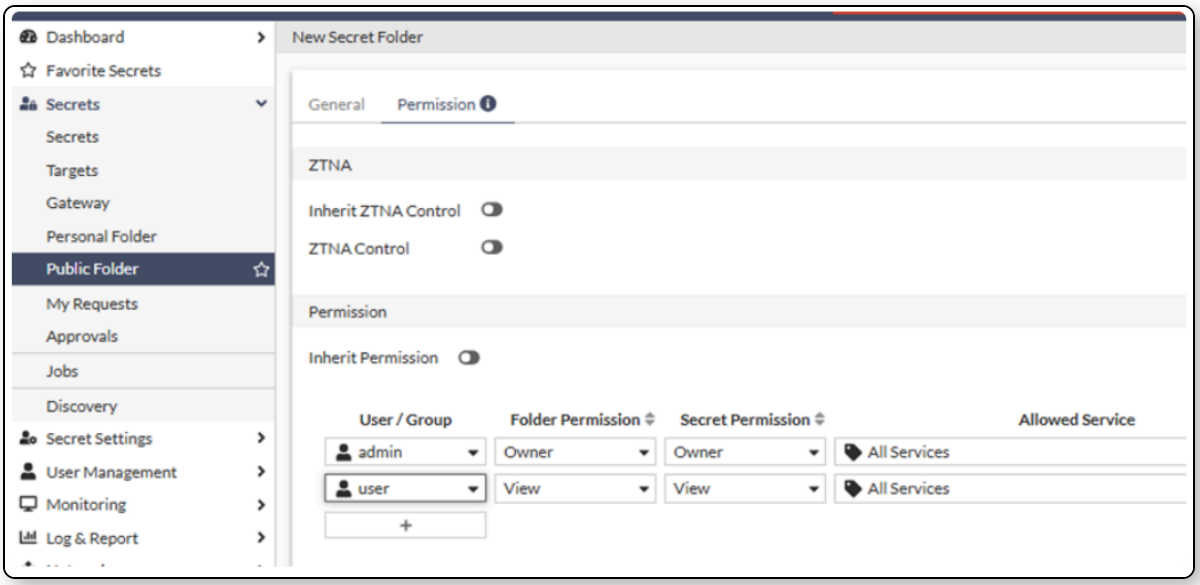

Configure Role
Configure Type
Configure User Details
Two Factor Authentication
Configure Trusted Hosts and Schedule
6
Review
Privileges
Role Type
Standard User
User Type
Local User
User Details
Username
user
Password
Fortinet123!@
Confirm Password
Status
Disable
Enable
Comments
Write a comment...
Email Alert & Two-factor Authentication
Email Address
Critical System Email Alert
Disable
Enable
General Email Alert
Disable
Enable
Two-Factor Authentication
Restricted Access
IPv4 Trusted Hosts
Login Schedule
Previous
Submit
Cancel

- Go to “Secret → Public Folder” and let´s to create a Folder for FortiAnalyzer with the new policy and the “user” can use.

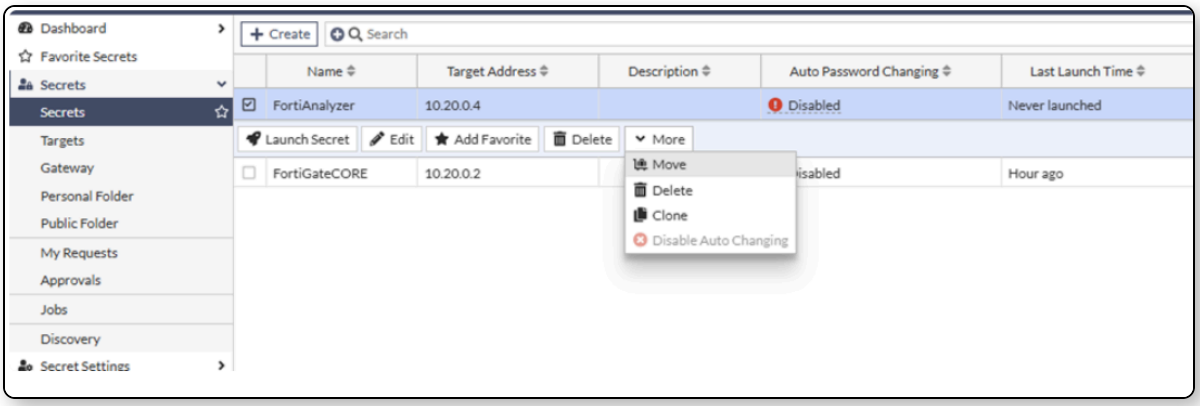


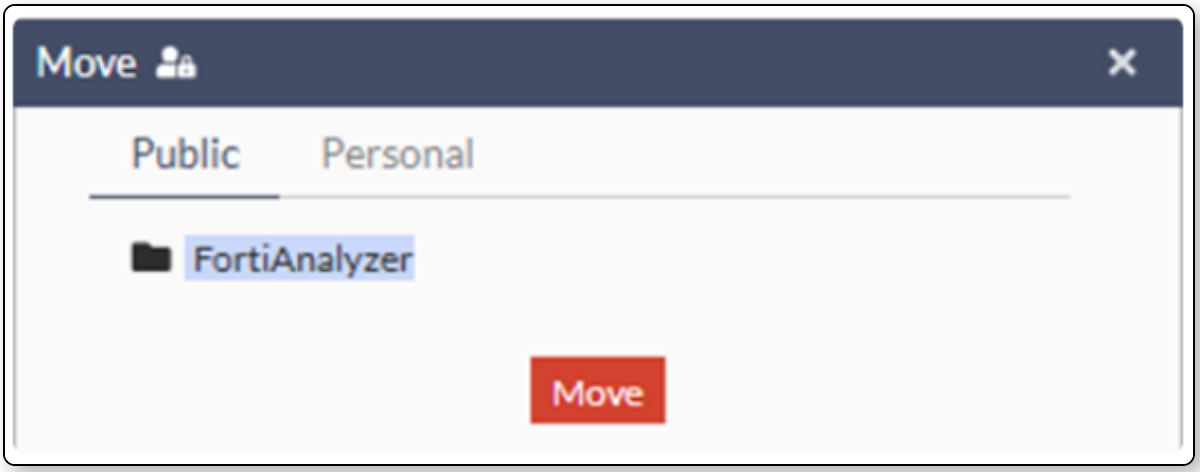


- In Folder´s “Permission”, select the user “user” and clic in “Submit”:

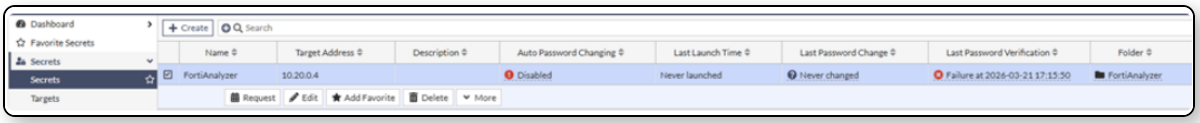


- In “Secrets → Secrets” select “FortiAnalyzer” and click in “More” and click in “Move”:

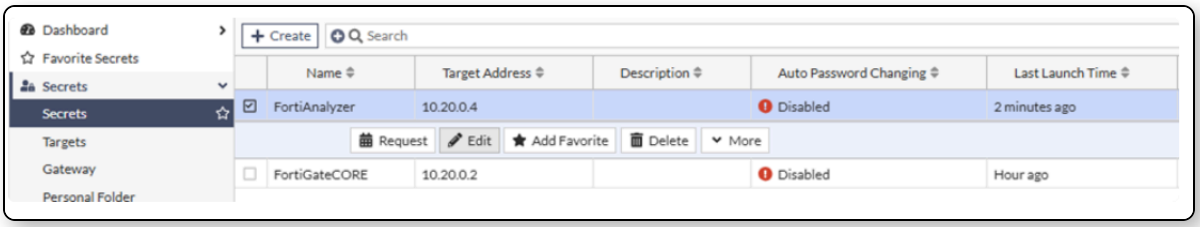




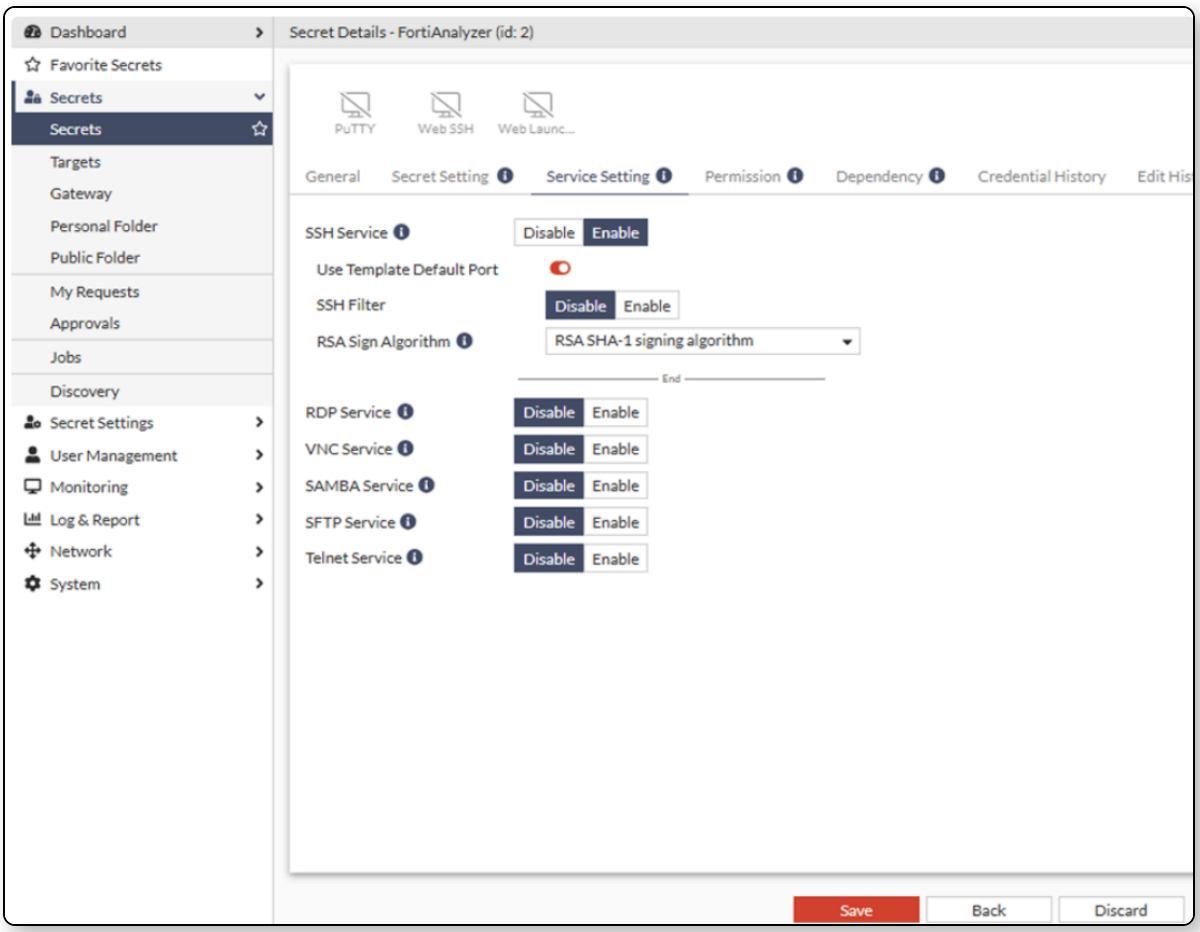
- You can see the “FortiAnalyzer´s Secret” is in “FortiAnalyzer” Folder:



- Review that the “SSH Filter” is not active in “FortiAnalyzer” secret. Got to the “FortiAnalyzer” secret and click in edit.

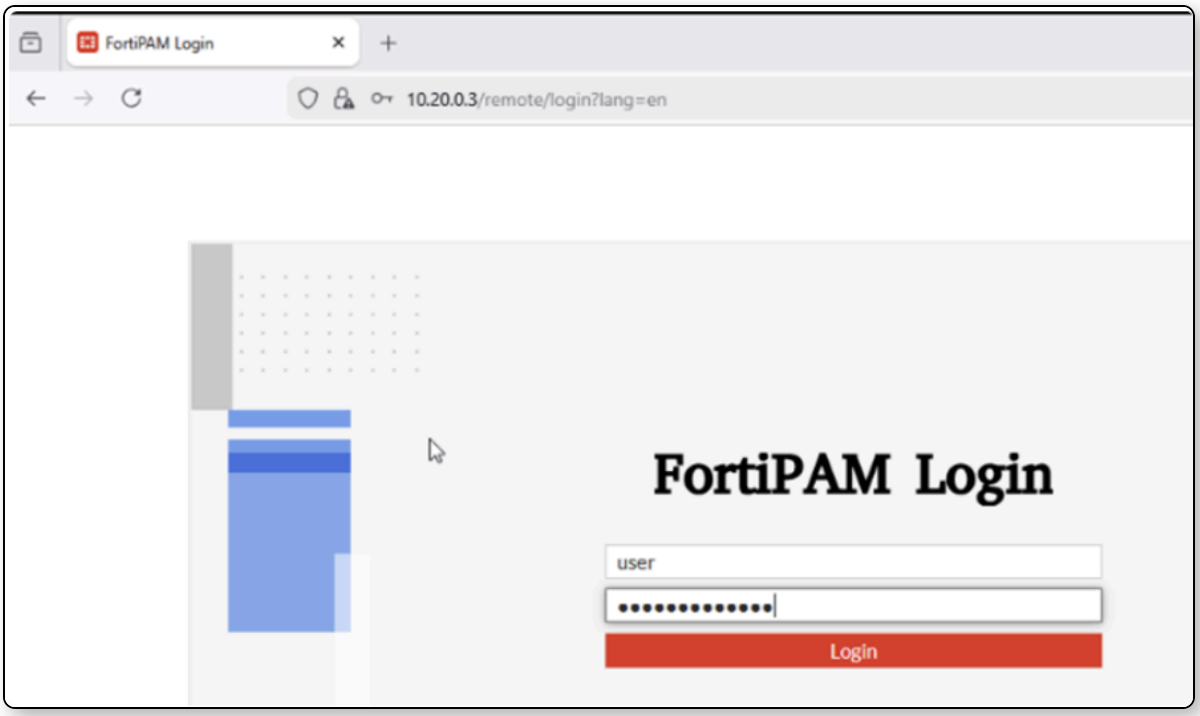


- Select “Service Setting” and disable “SSH FIlter” and click in “Save”.

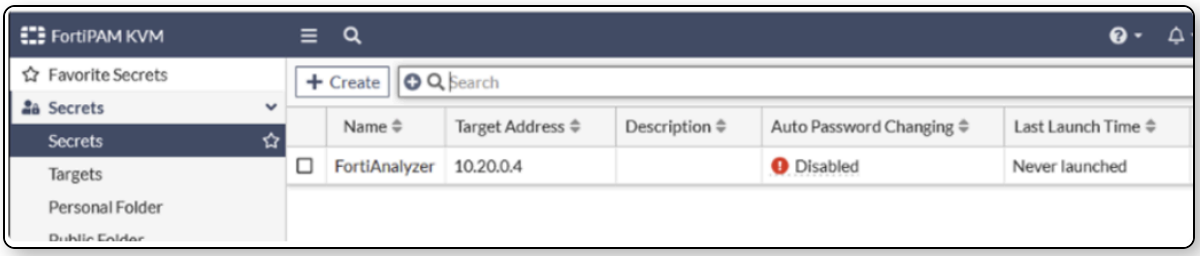


- In this way we have another central access with FortiAnalyzer. We can test all the launcher connections and how the policy applies.

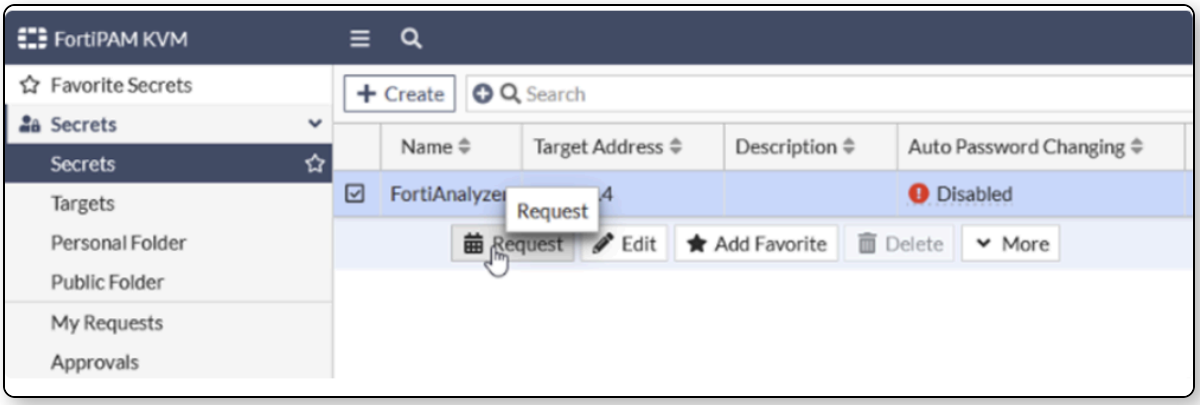
- Access in “Victim” device, open a browser and access to FortiPAM (https://10.20.0.3) with the “user” account:

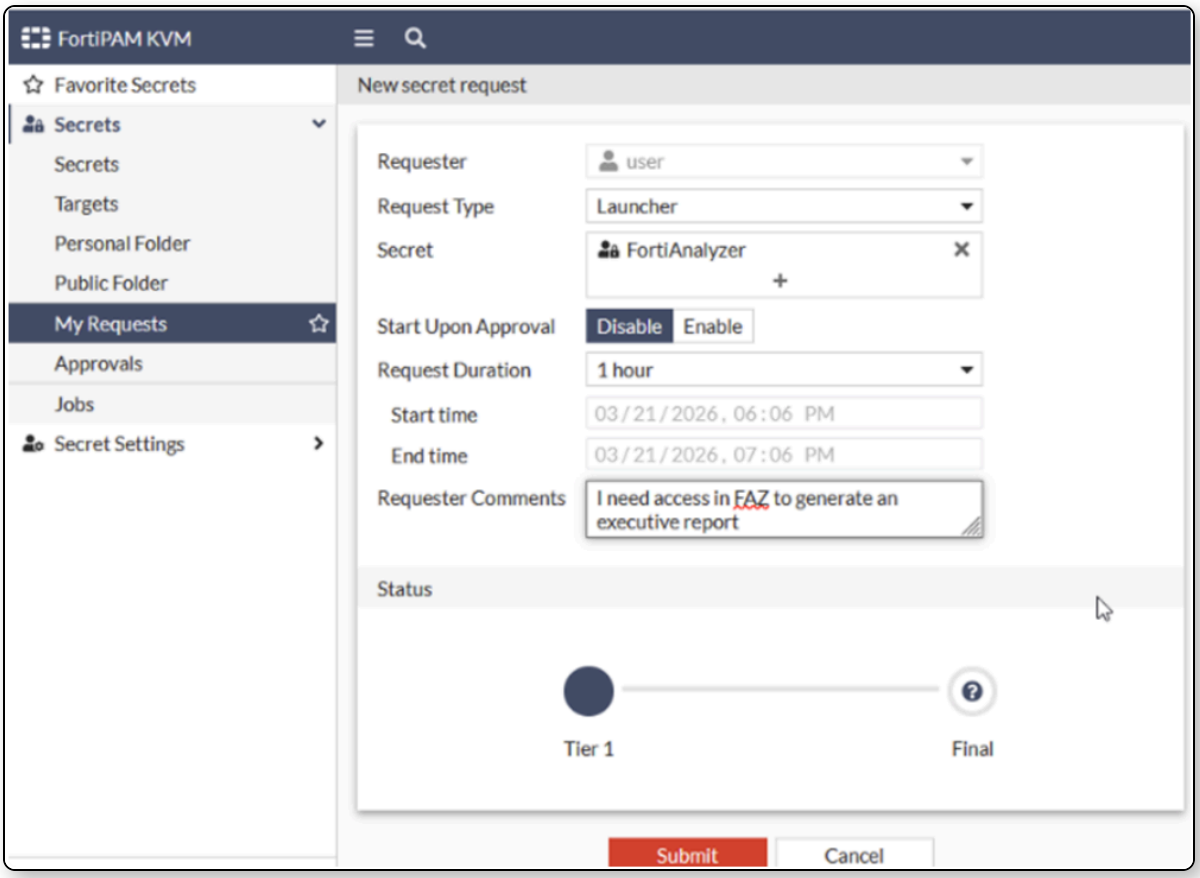


- This user has a limited panel and only can see the FortiAnalyzer:

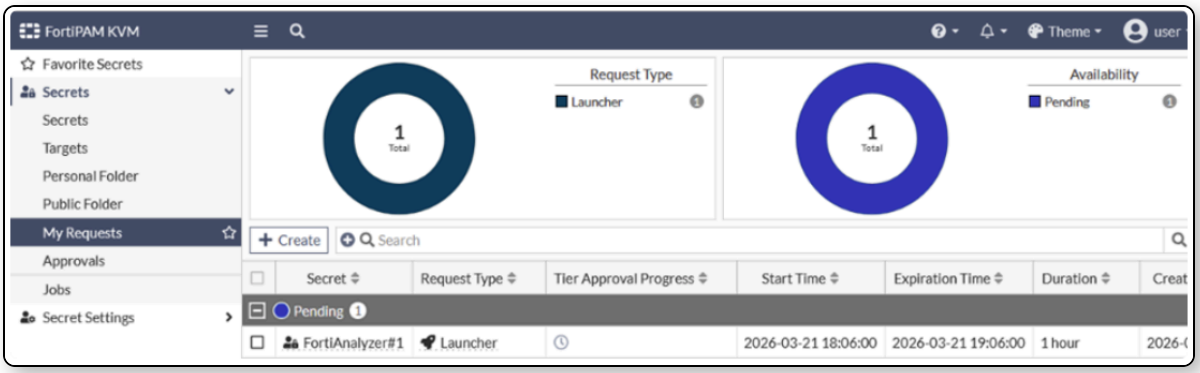


- Select “FortiAnalyzer” secret and click in “Request” and fill up with the next information:

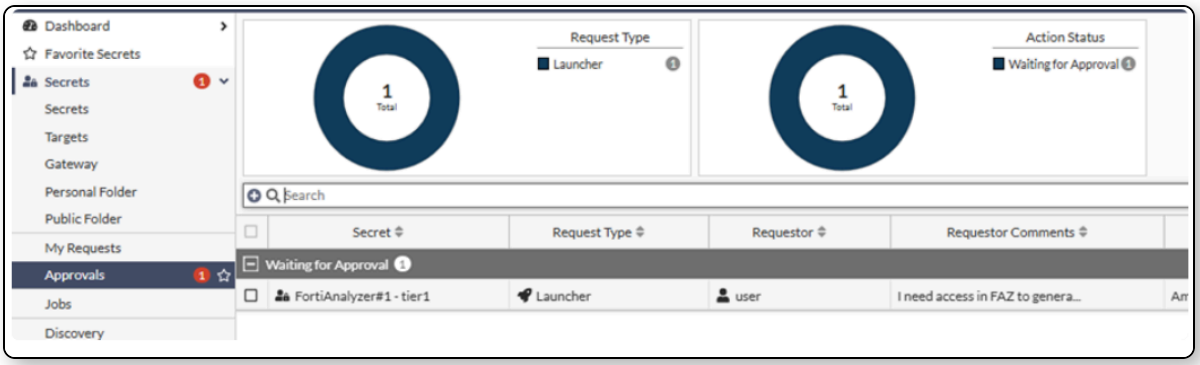




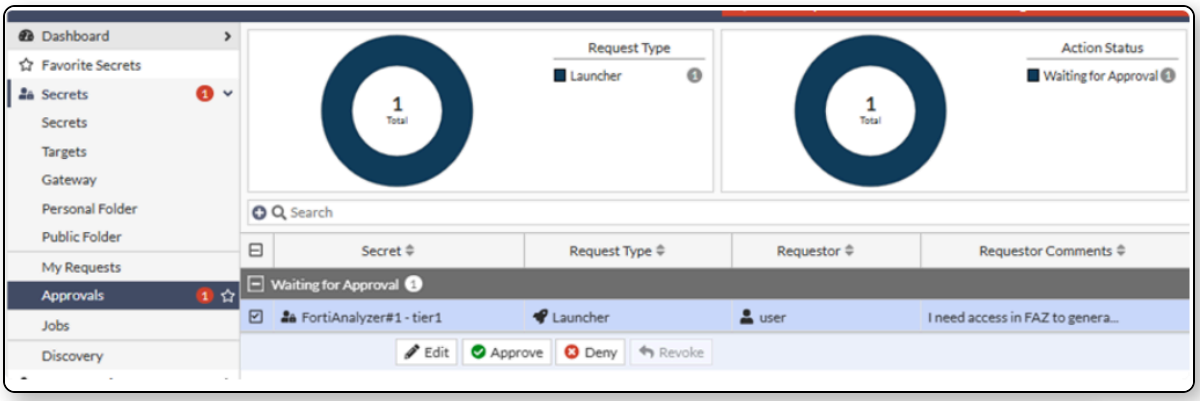
- You can see the status “Request” in “Secrets → My Requests”:

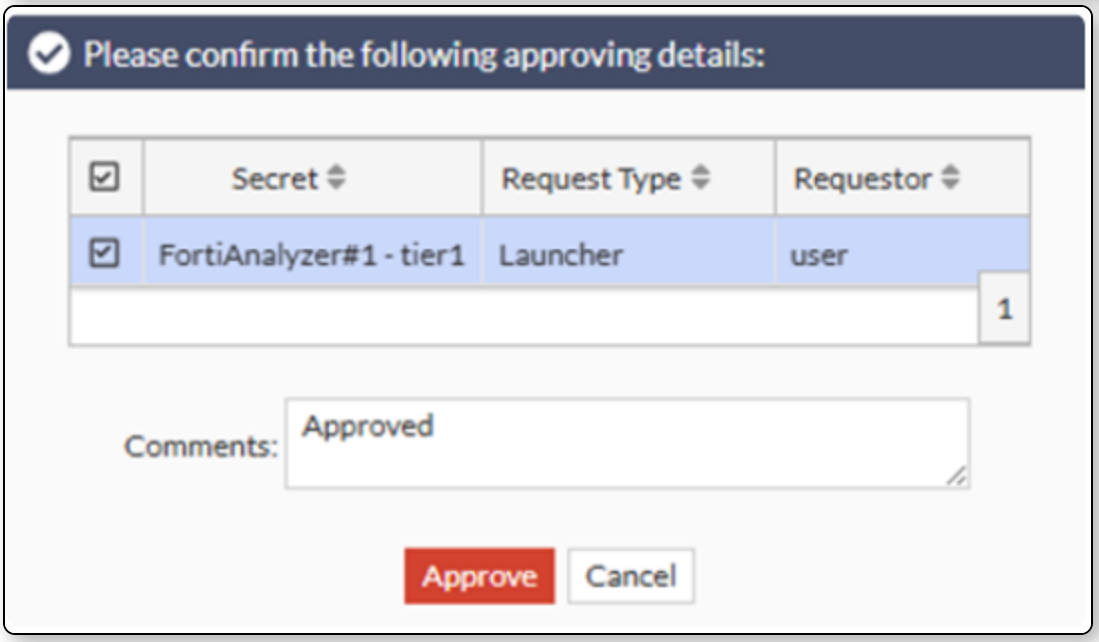


- Please access to “FortiPAM” via HTTPS in “Security Fabric” with the “admin” user to approve the user´s request.
- When you access you can see a notification in “Secrets → Approvals”:

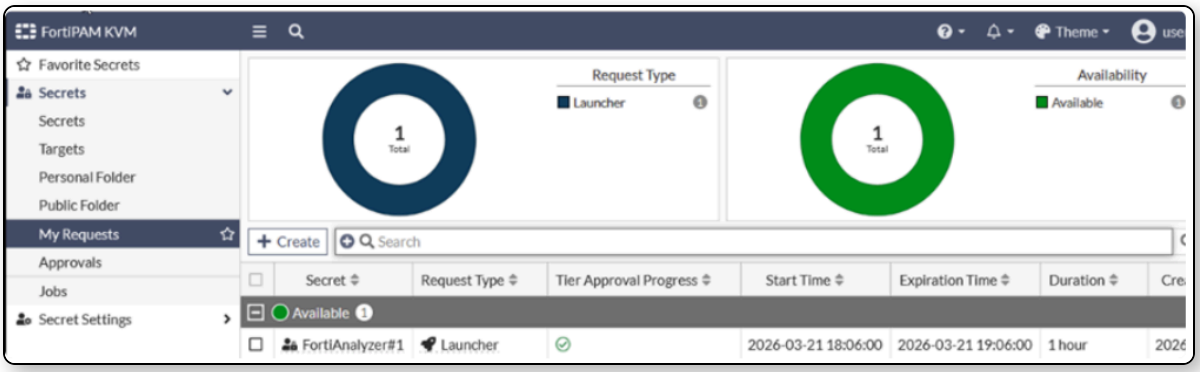


- Please select the pending request, click and “Approve”.

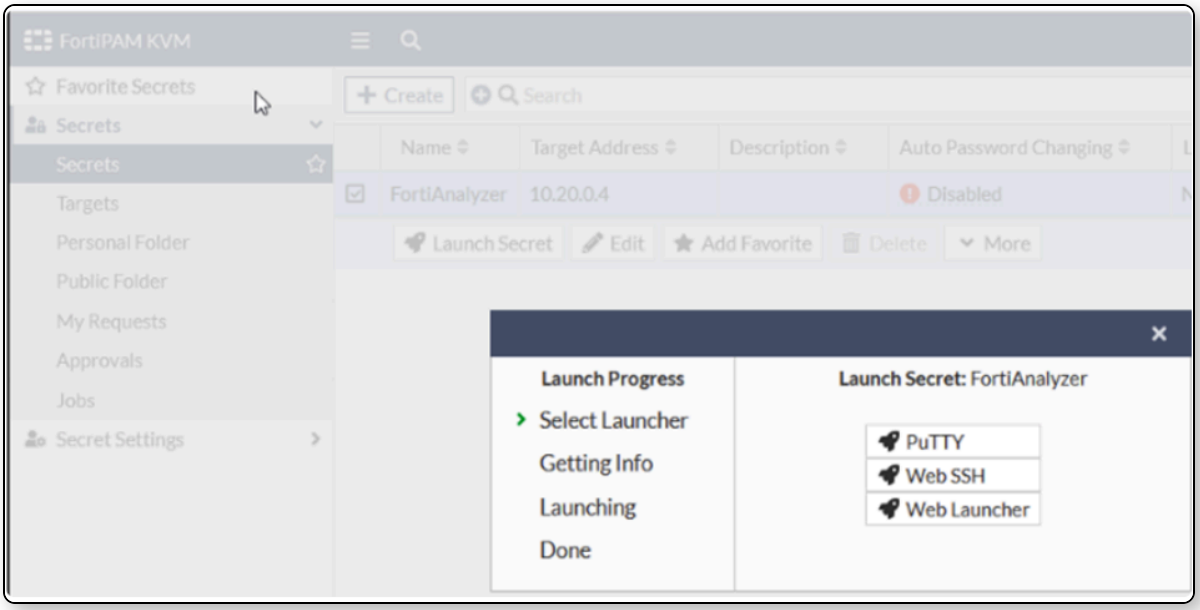




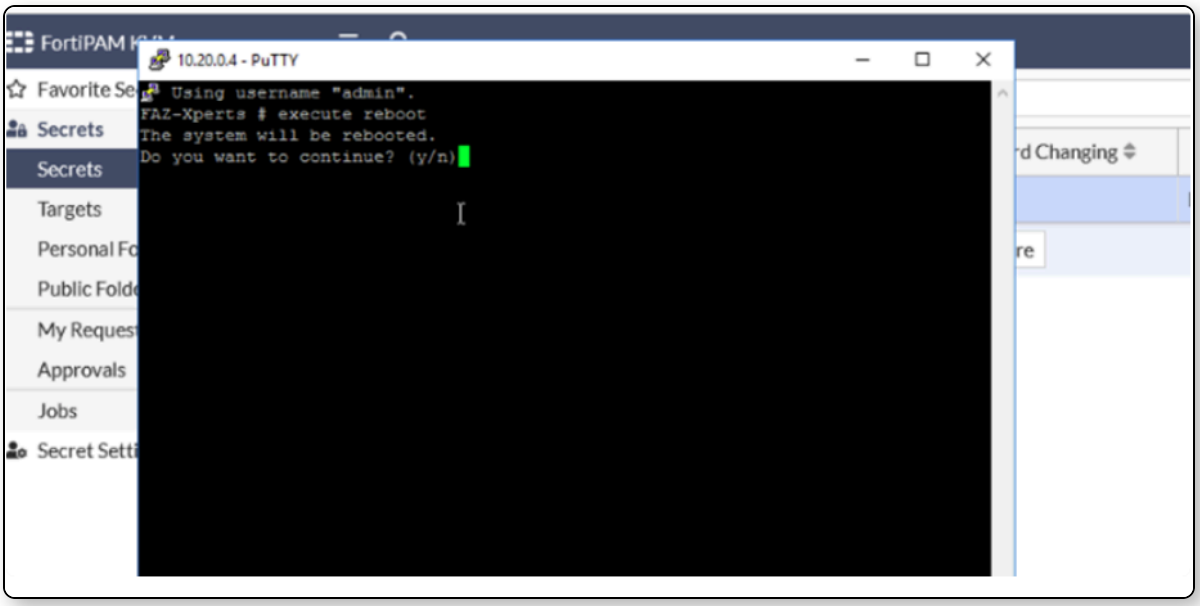
- Return to “Victim” device, update the browser and you can see your request approved and you can access to use the “FortiAnalyzer” secret.



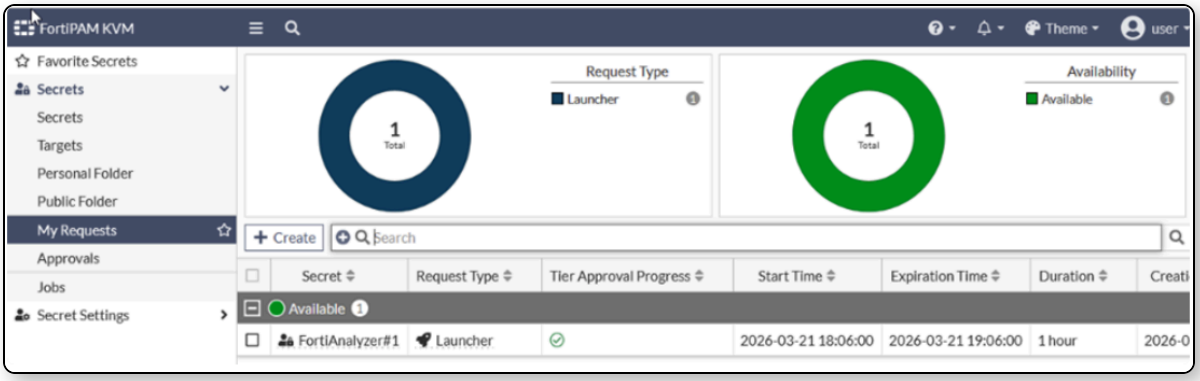
- Go to “Secrets → Secrets” select “FortiAnalyzer”. Now you can see the “Launch Secret” (Instead of Request). Select “PUTTY” connection.



- Now you are connected to FortiAnalyzer via PUTTY with the “admin” user and you can execute a “reboot” because your new policy permits it.



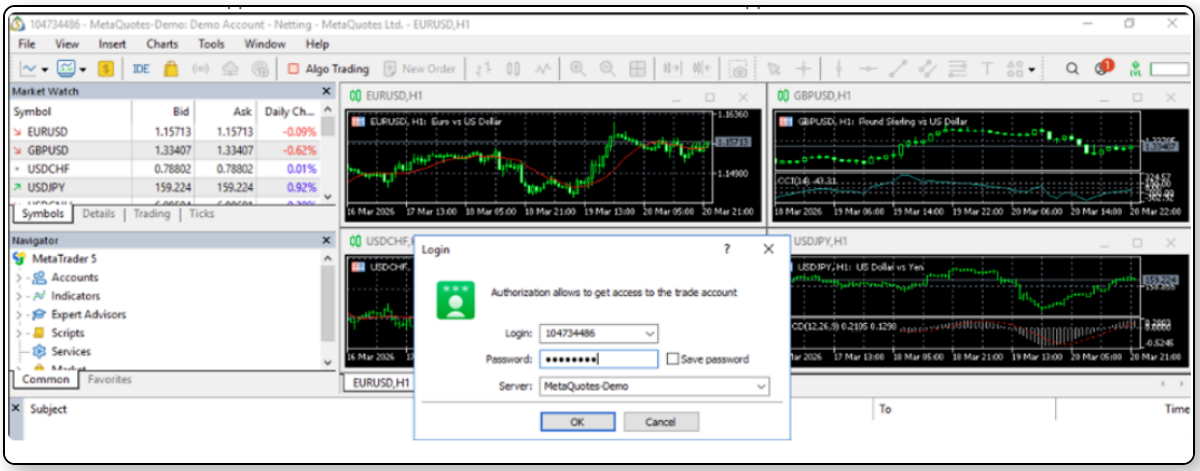
- You will have access to FortiAnalyzer for one hour. This parameter is configurable.



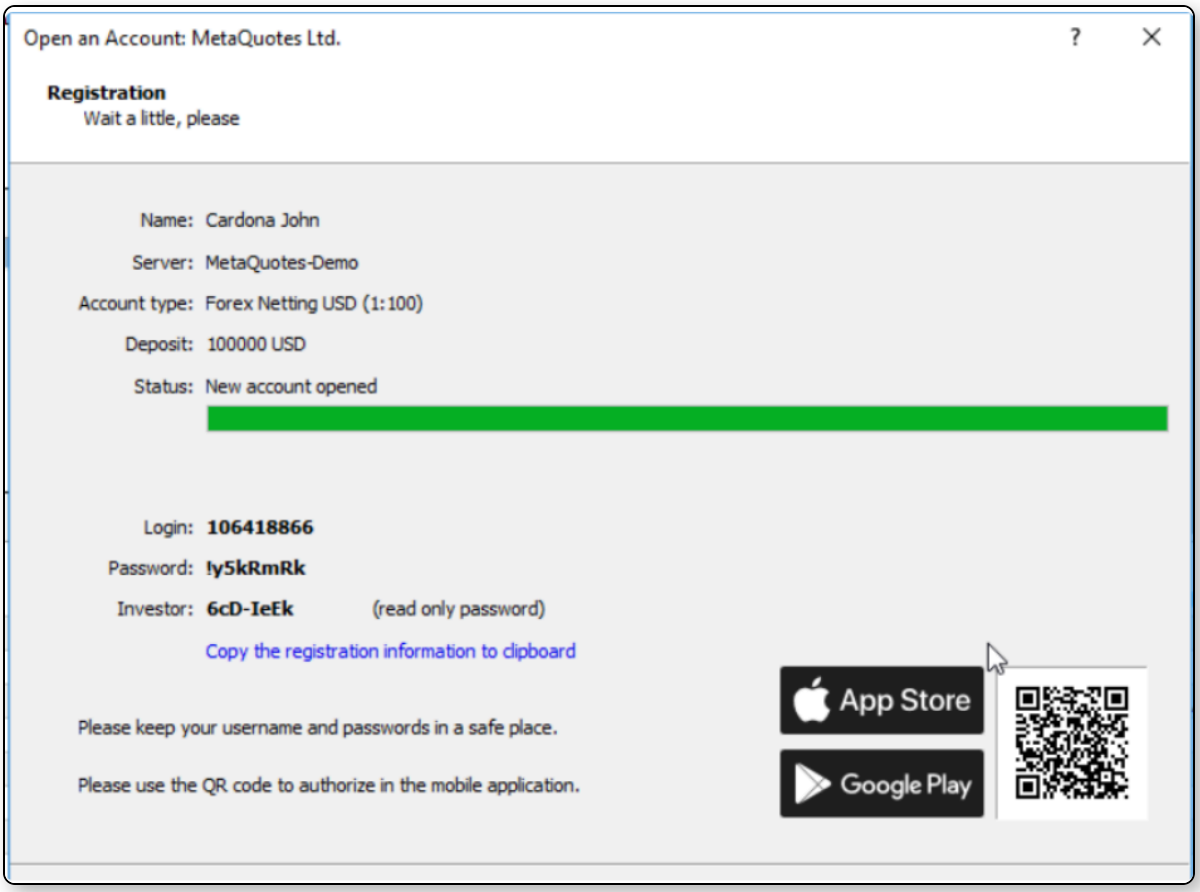
e) Integration Windows Server with FortiPAM via RDP using AutoIT for custom Apps access.

We will use AutoIt to customize the connection from the FortiPAM, run an application “MetaTrader 5”, and automate the startup and provision of credentials in that application.

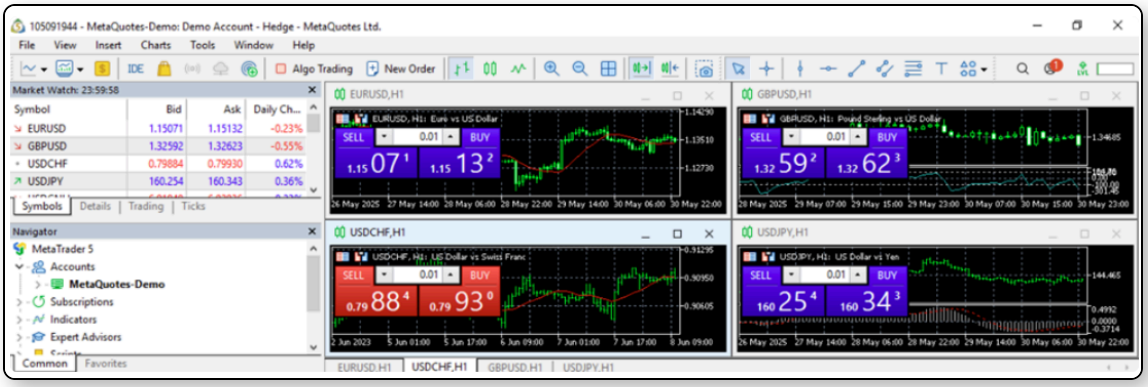
We will assume that the application is installed and an account is used to access said application.



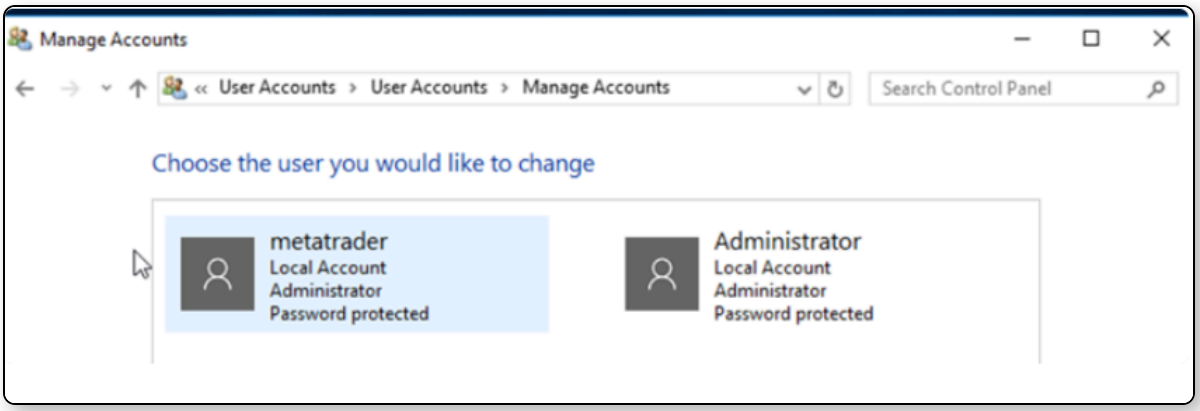
- The account information DEMO is the next:



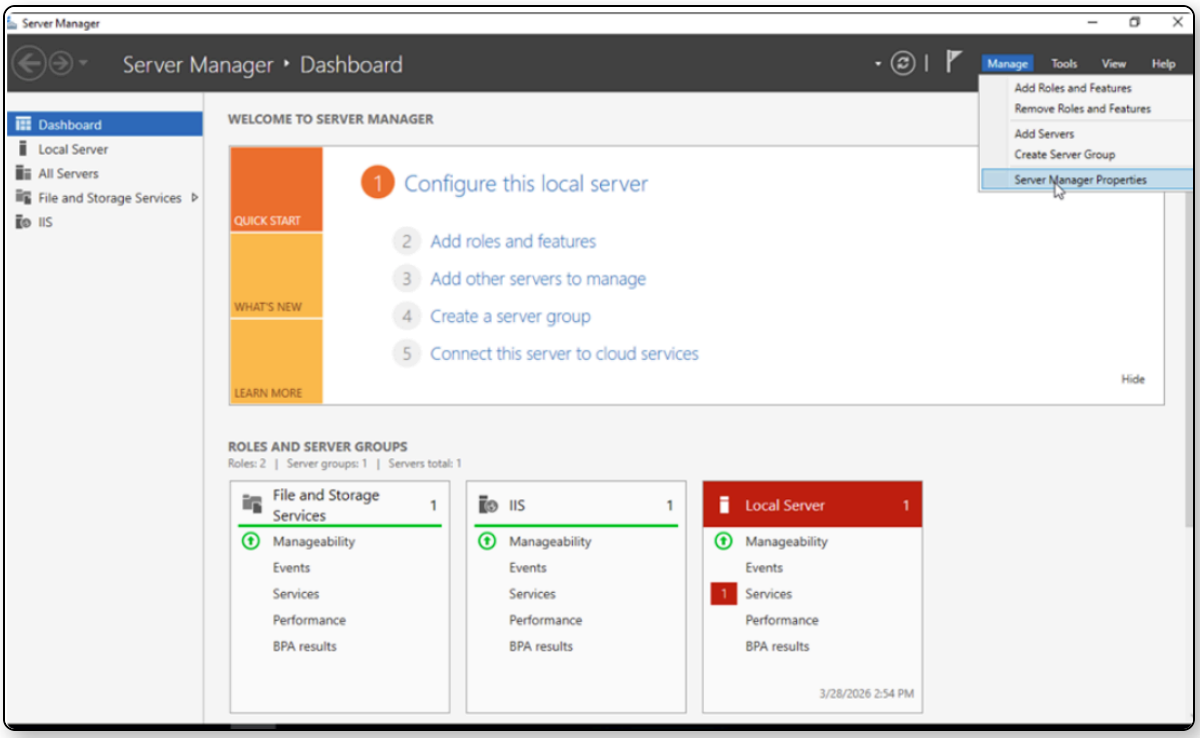
- This account works!

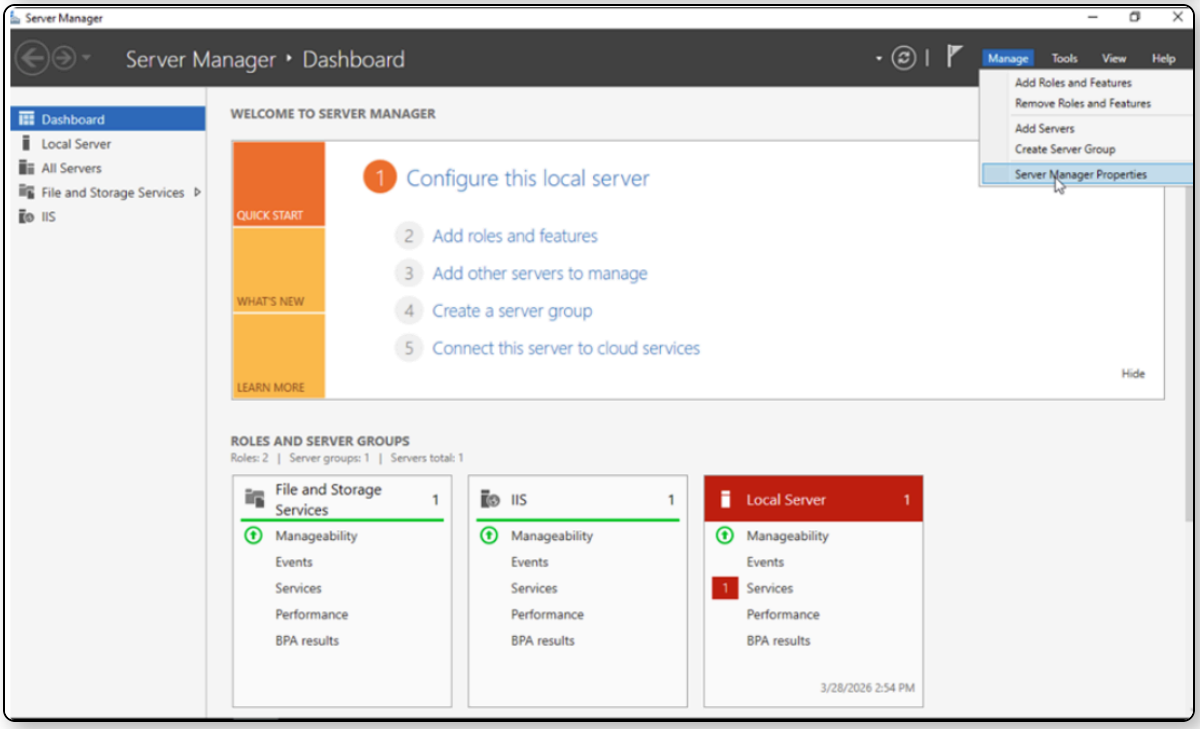


- Let´s go to integrate this application with FortiPAM to be able to safeguard the access account.
- First, we need to create a second administrator on Windows Server. Go to “Control Panel → User Accounts” and add a “metatrader” local account as a “Administrator” (Put the next password "Fortinet123!@").

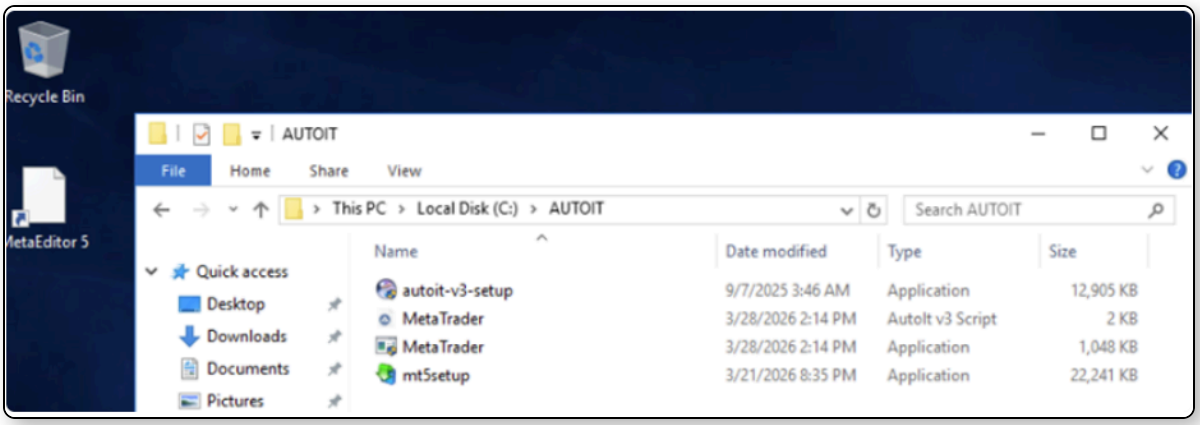


- Logoff in the server with “Administrator” account and login with the “metatrader” account.
- Let´s go to disable the open automatic of “Server Manager”, in “Server Manager” go to “Manage → Server Manager Properties” and click in “Do not start Server Manager automatically at logon”. Click and “OK” and close “Server Manger”.





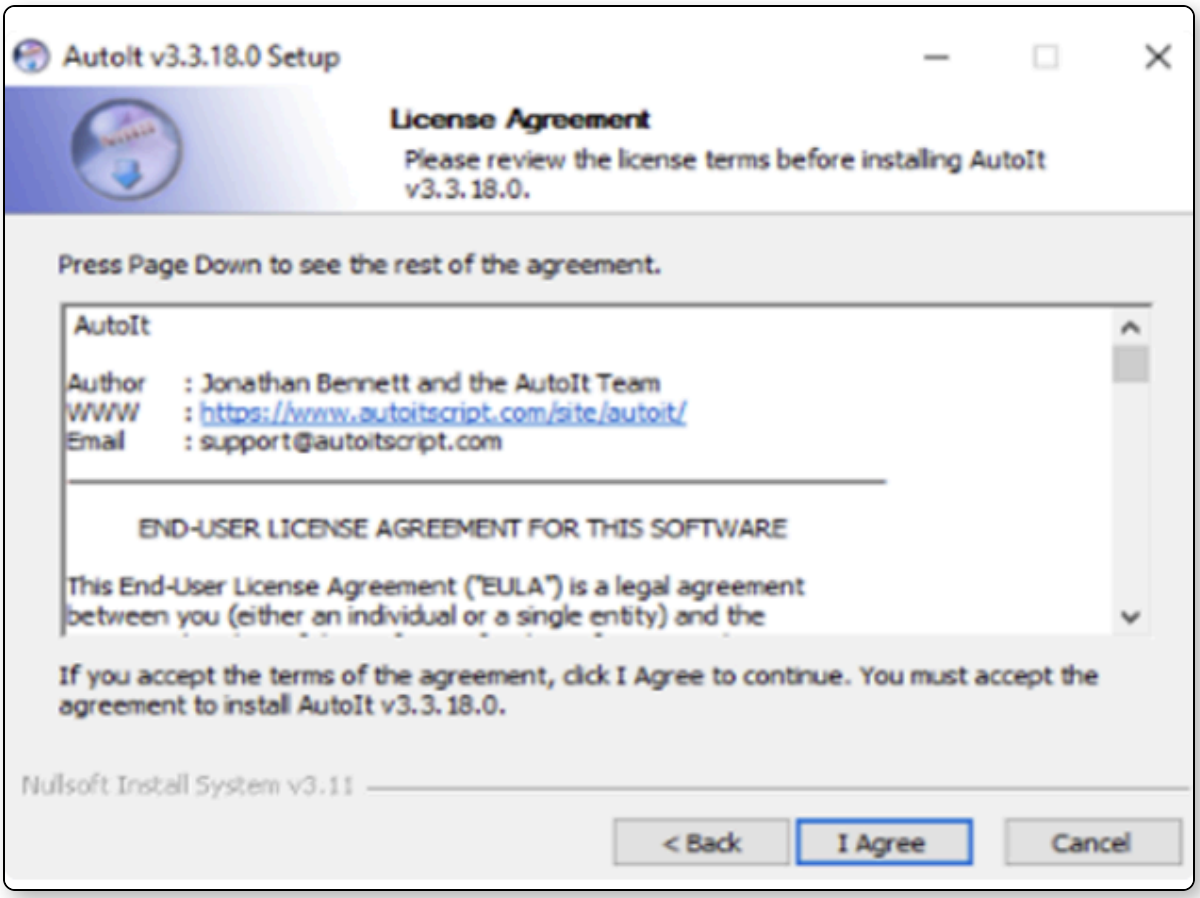
- let´s go to install “AutoIT” in this server. In the folder “AUTOIT” we can found “autoit-v3-setup.exe”:

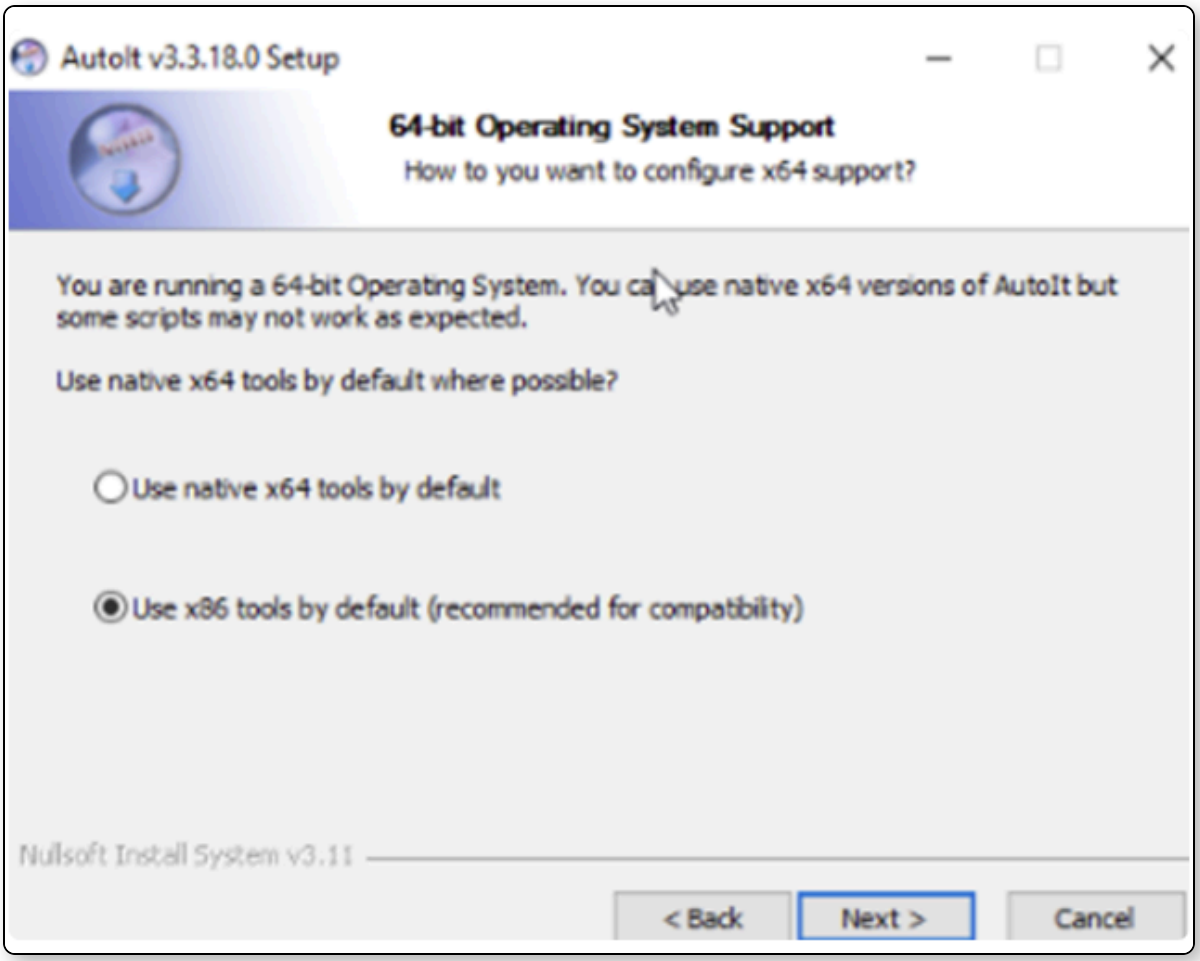


- Double click to “autoit-v3-setup.exe” and click in “Next”:

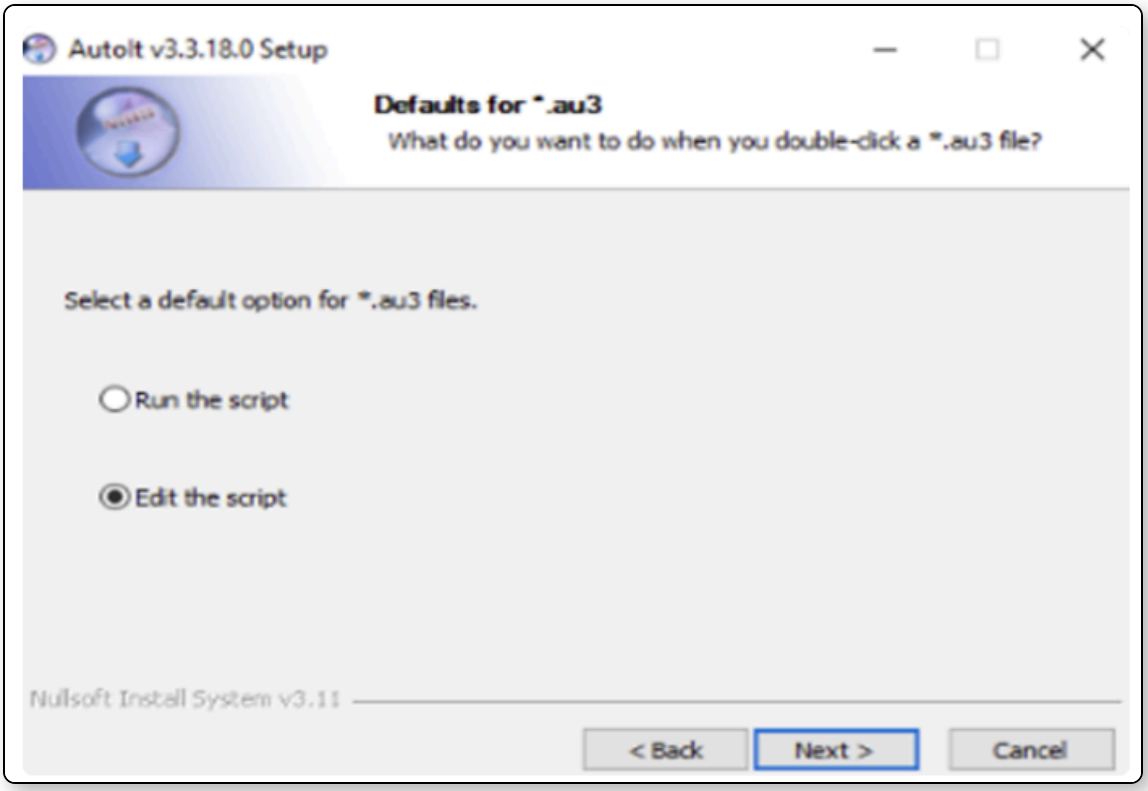


- Click in “I Agree” and select “Use x86 tools by default” and “Next”.

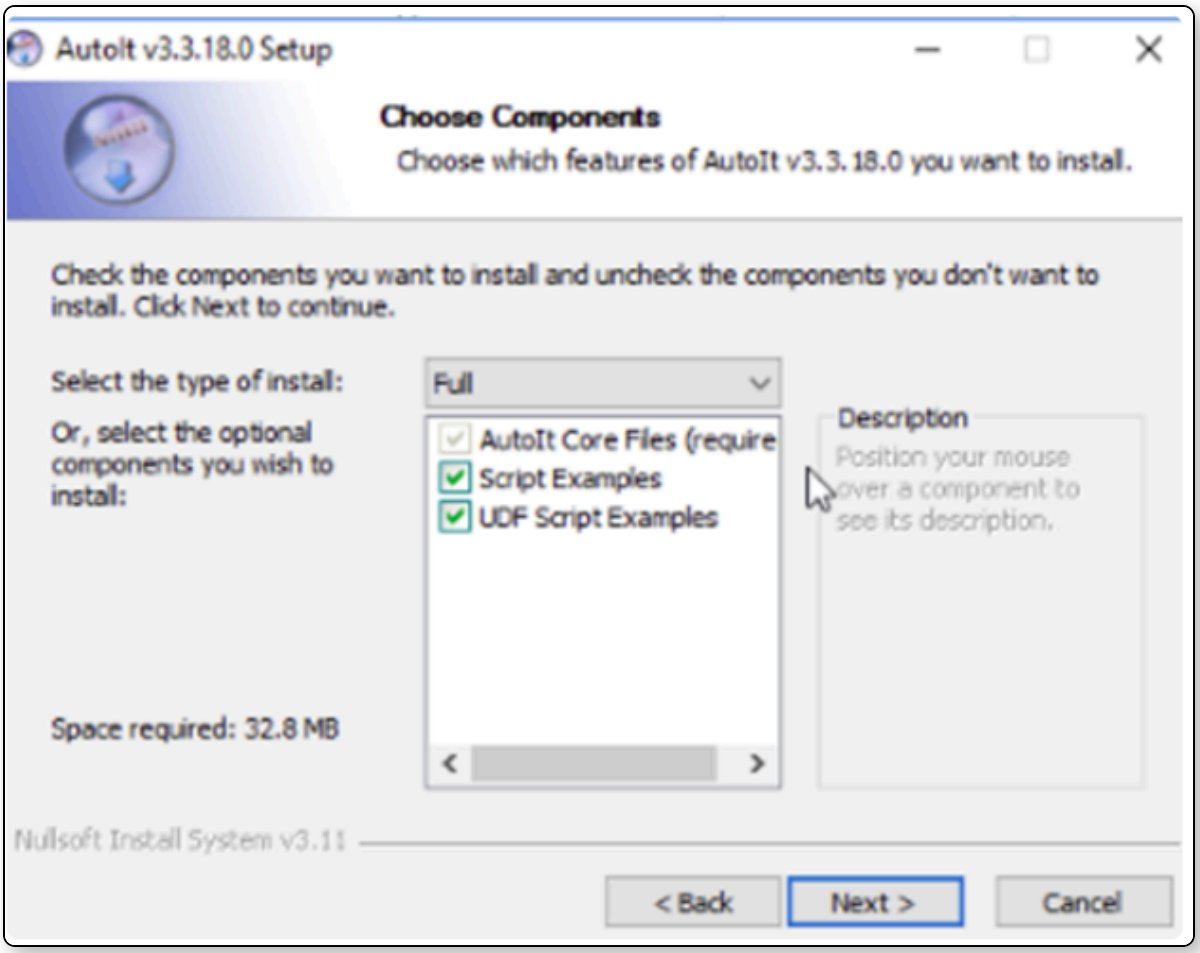

AutoIt v3.3.18.0 Setup
License Agreement
Please review the license terms before installing AutoIt v3.3.18.0.
Press Page Down to see the rest of the agreement.
AutoIt
Author : Jonathan Bennett and the AutoIt Team
WWW : https://www.autoitscript.com/site/autoit/
Email : support@autoitscript.com
END-USER LICENSE AGREEMENT FOR THIS SOFTWARE
This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and the
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install AutoIt v3.3.18.0.
Nullsoft Install System v3.11
< Back
I Agree
Cancel

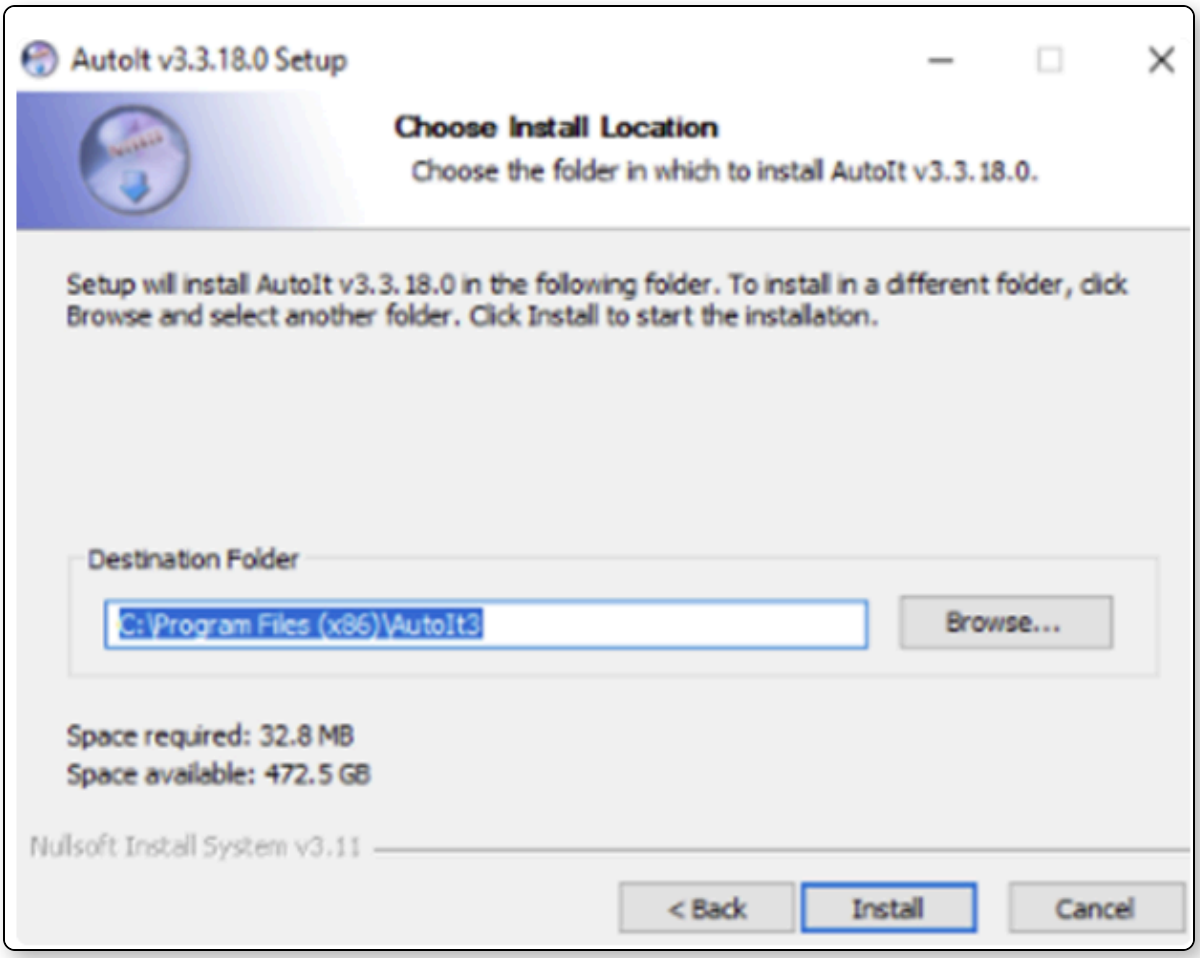

AutoIt v3.3.18.0 Setup
64-bit Operating System Support
How to you want to configure x64 support?
You are running a 64-bit Operating System. You can use native x64 versions of AutoIt but some scripts may not work as expected.
Use native x64 tools by default where possible?
Use native x64 tools by default
Use x86 tools by default (recommended for compatibility)
Nullsoft Install System v3.11
< Back
Next >
Cancel

- Select a default option for *.au3 files “Edit the script” and click in “Next”.

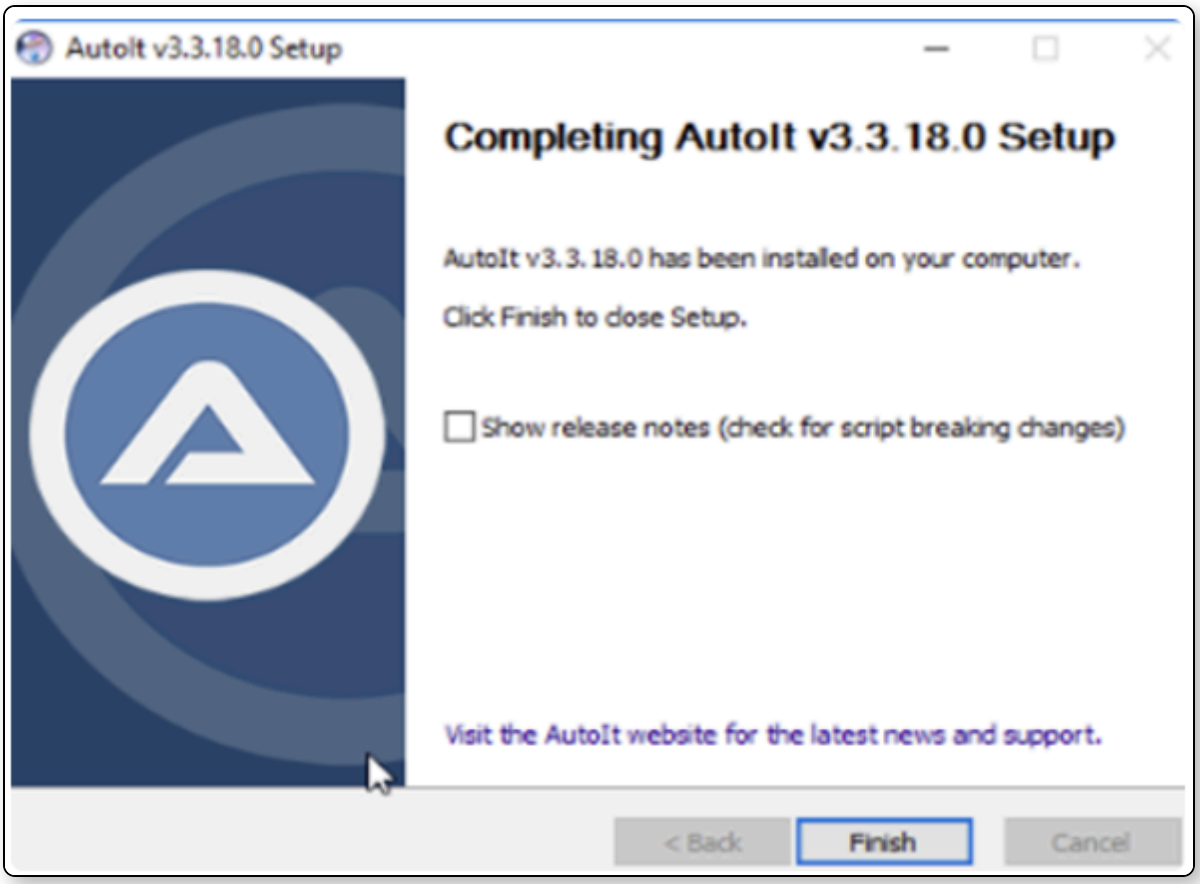


- Click in “Next” and “Install”.

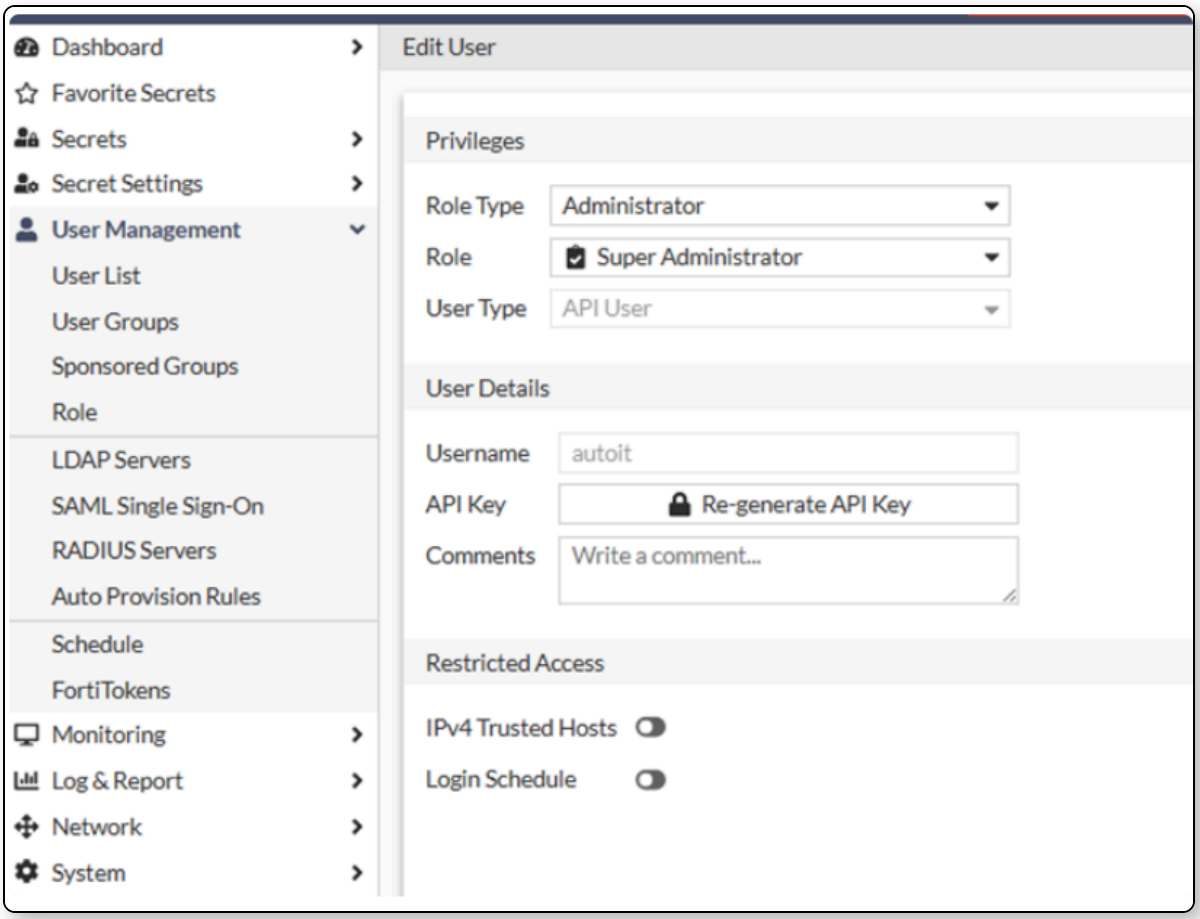

AutoIt v3.3.18.0 Setup
Choose Components
Choose which features of AutoIt v3.3.18.0 you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select the type of install:
Full
Or, select the optional components you wish to install:
AutoIt Core Files (require
Script Examples
UDF Script Examples
Description
Position your mouse over a component to see its description.
Space required: 32.8 MB
Nullsoft Install System v3.11
< Back
Next >
Cancel



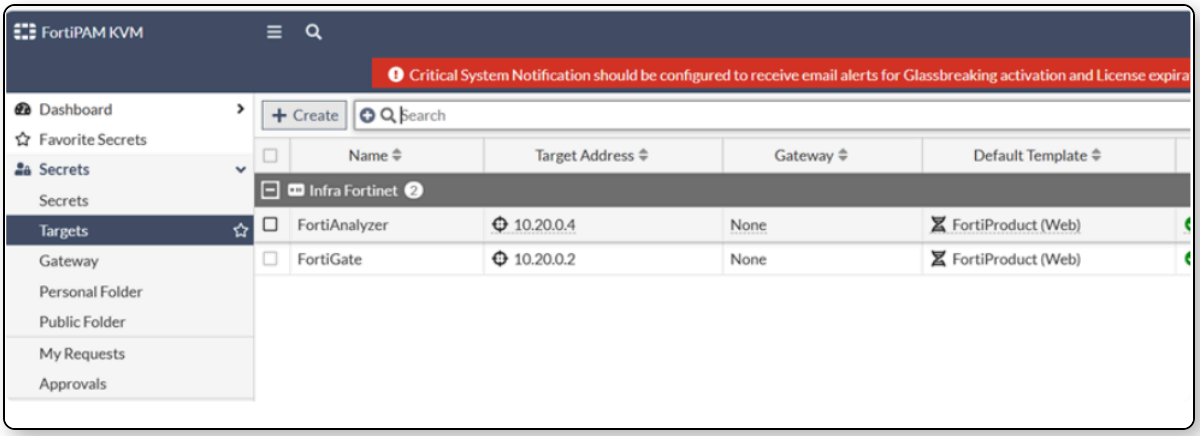
- Click in “Finish” to finish this installation.



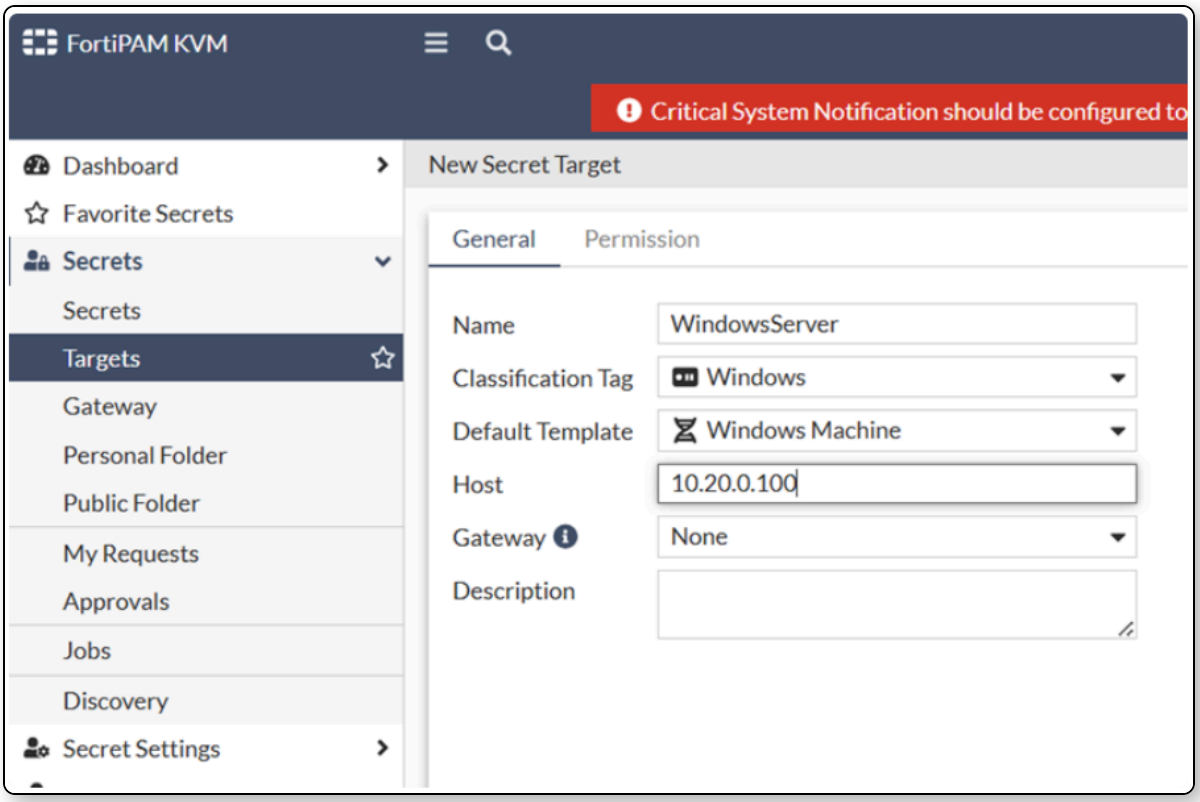
- Now go to FortiPAM via HTTPS and create the next admin API.
- Go to “User Management → User List” and click in “Create” follow the next steps. WARNING: Saved the API due this will be used later:



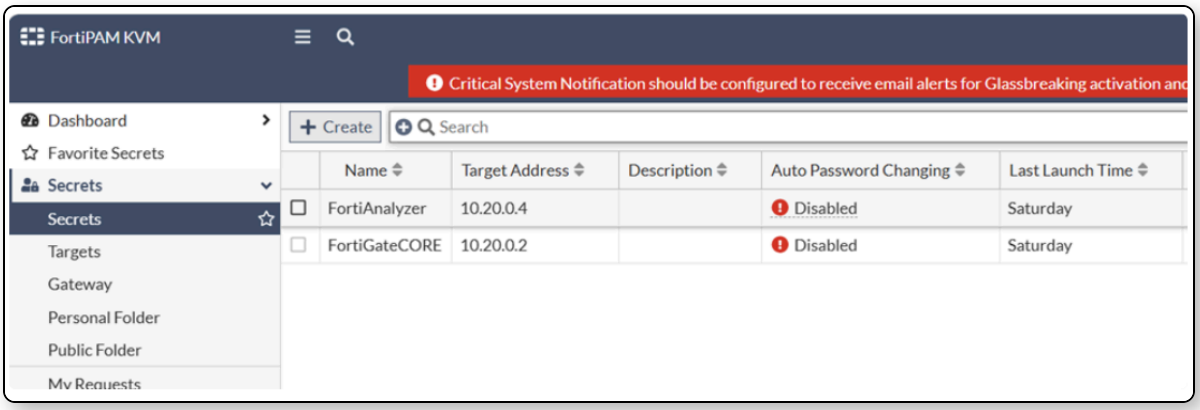
- Now we should go to FortiPAM via “HTTPS” and let´s go to add a “Windows Server”.
- Go to “Secret → Targets” and click in “Create”.



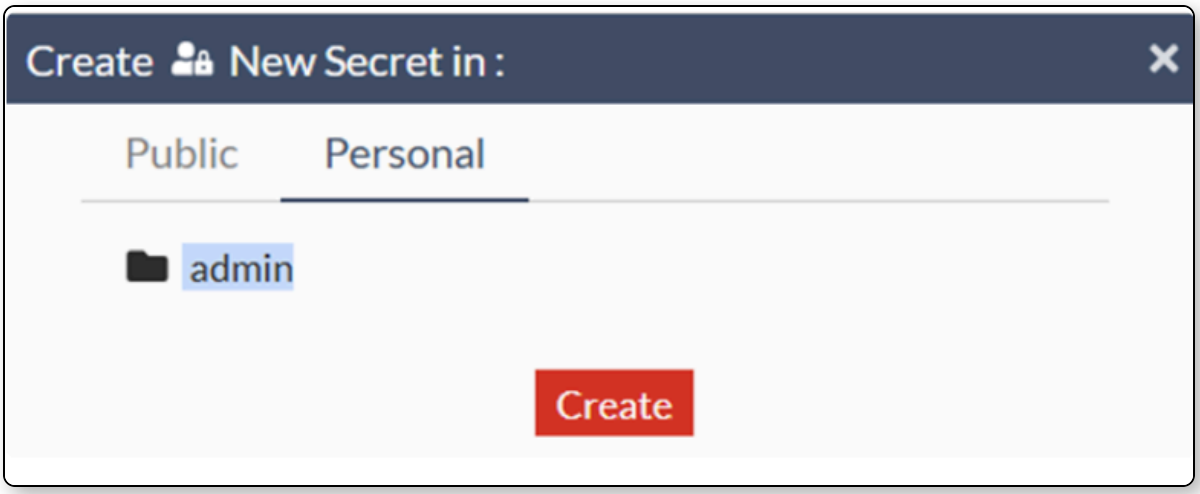
- Let´s go to create the next “Target”



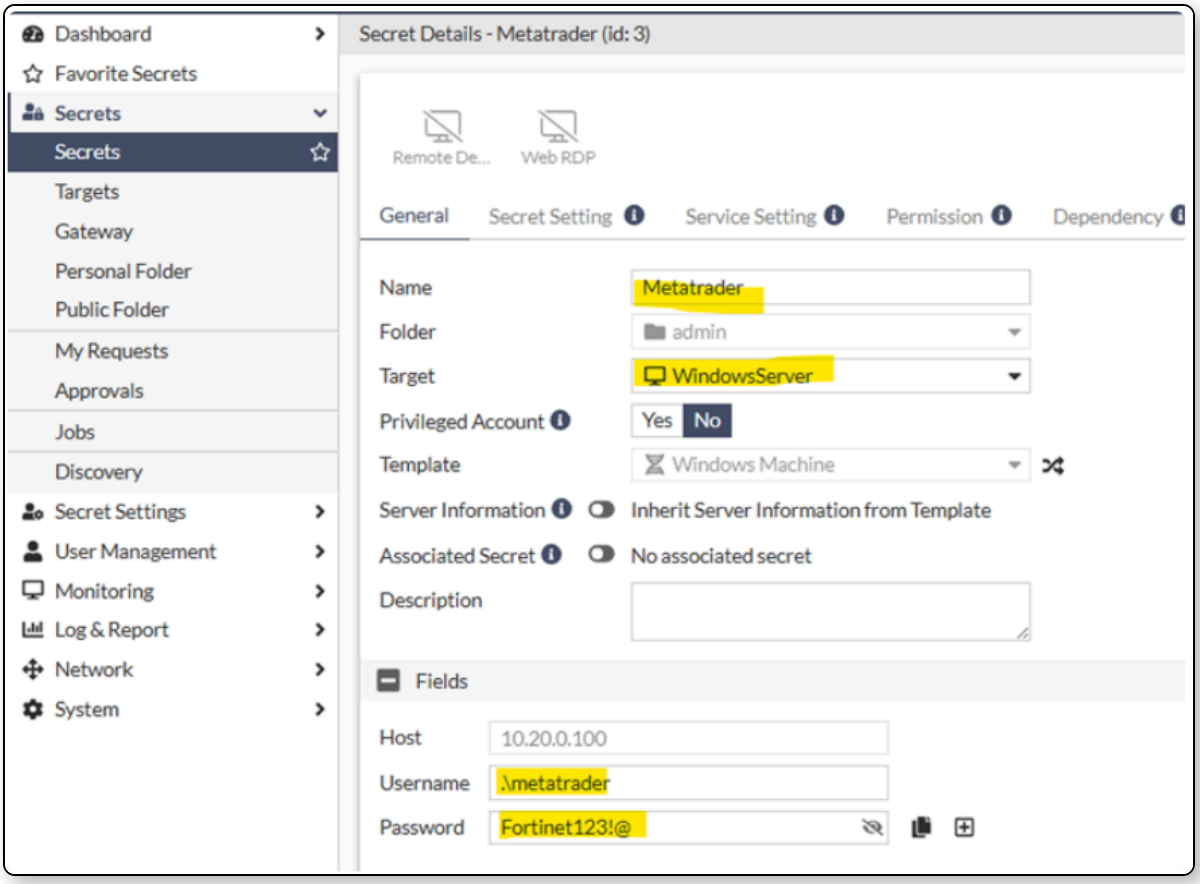
- Let´s go to create the "Secret". Go to "Secrets → Secrets" and click in "Create".



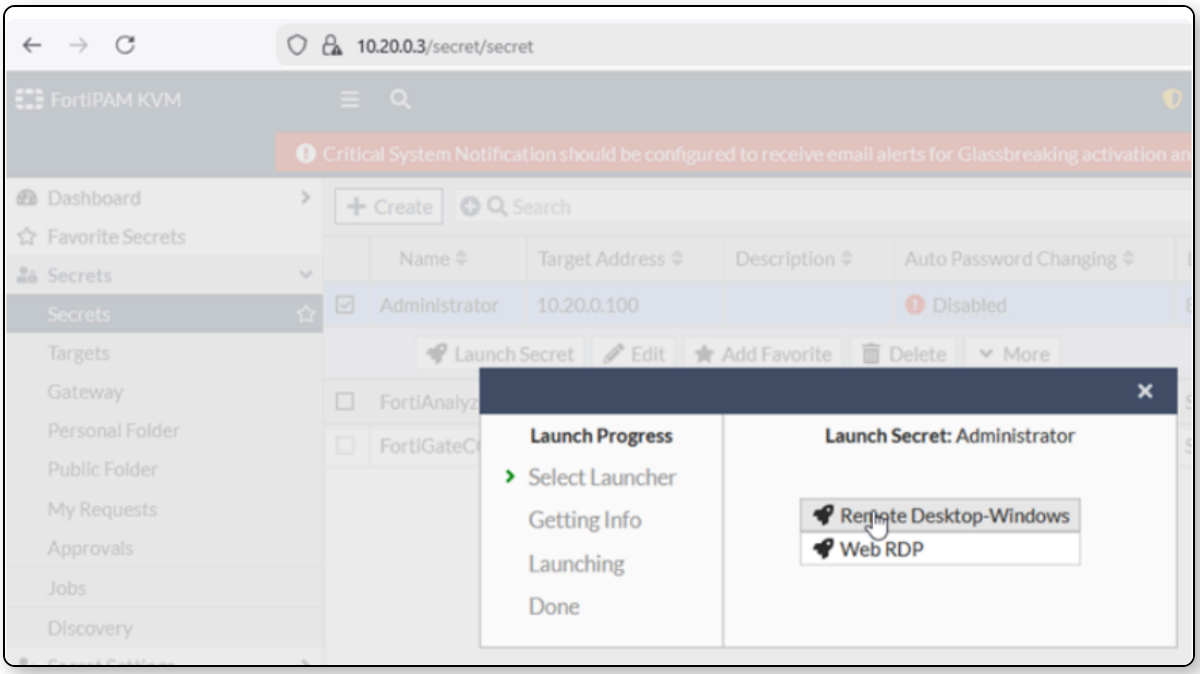
- Select the folder "Personal → admin".



- Go to create the secret with the next information and click in “Save”.



- We can test the RDP connection in FortiPAM. Go to “Victim” device via “Display” and in a browser open FortiPAM (https://10.20.0.3).
- Go to “Secrets → Secrets” and launch “WindowsServer” in any way.

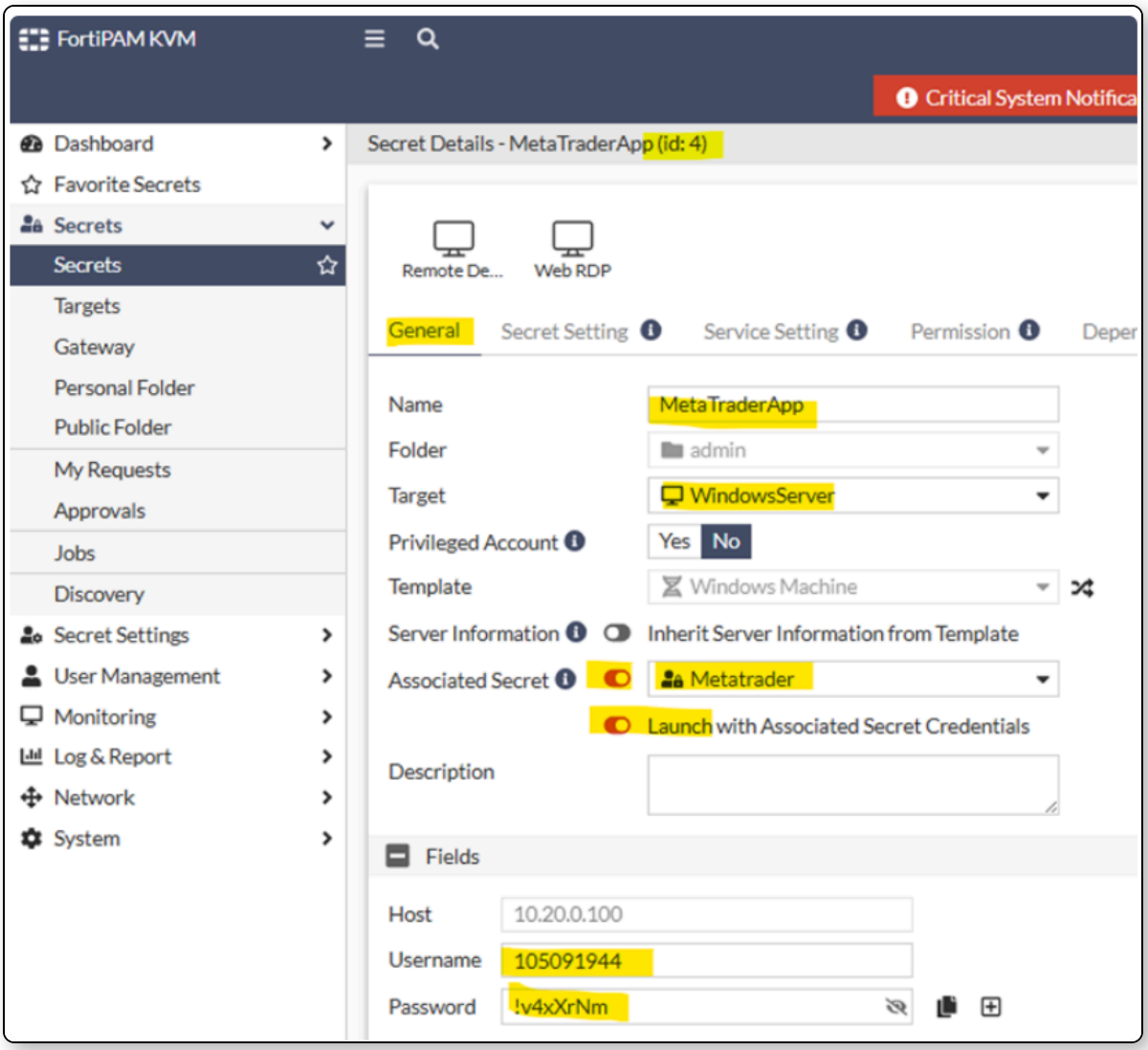


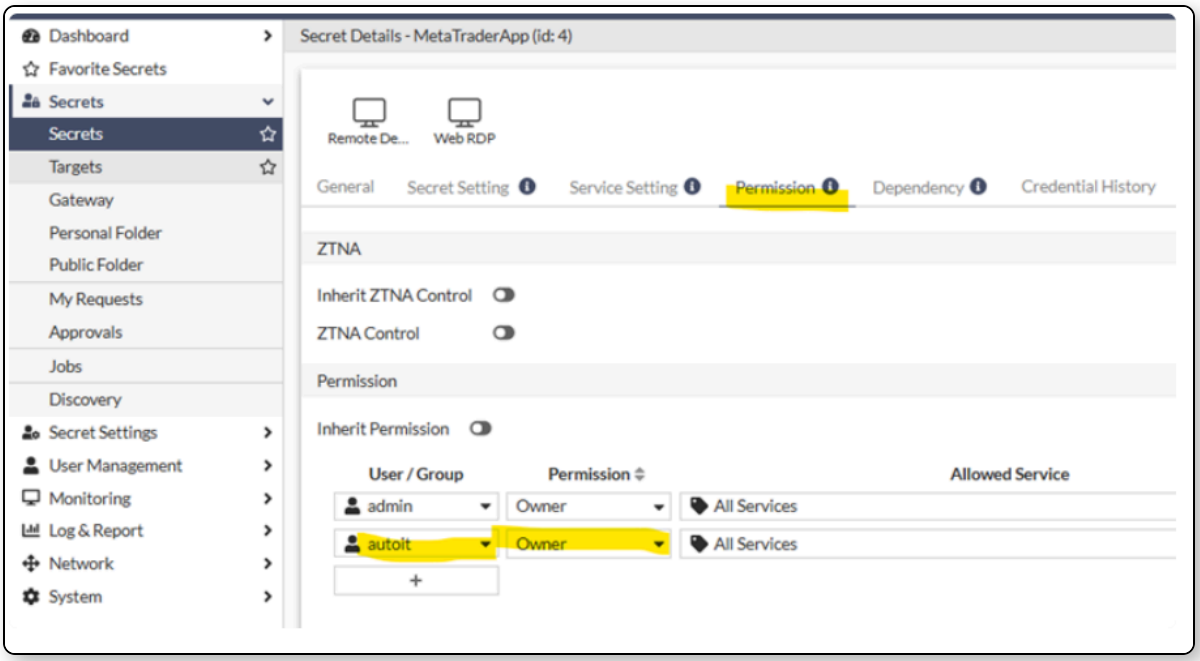
- The connection is established successfully:



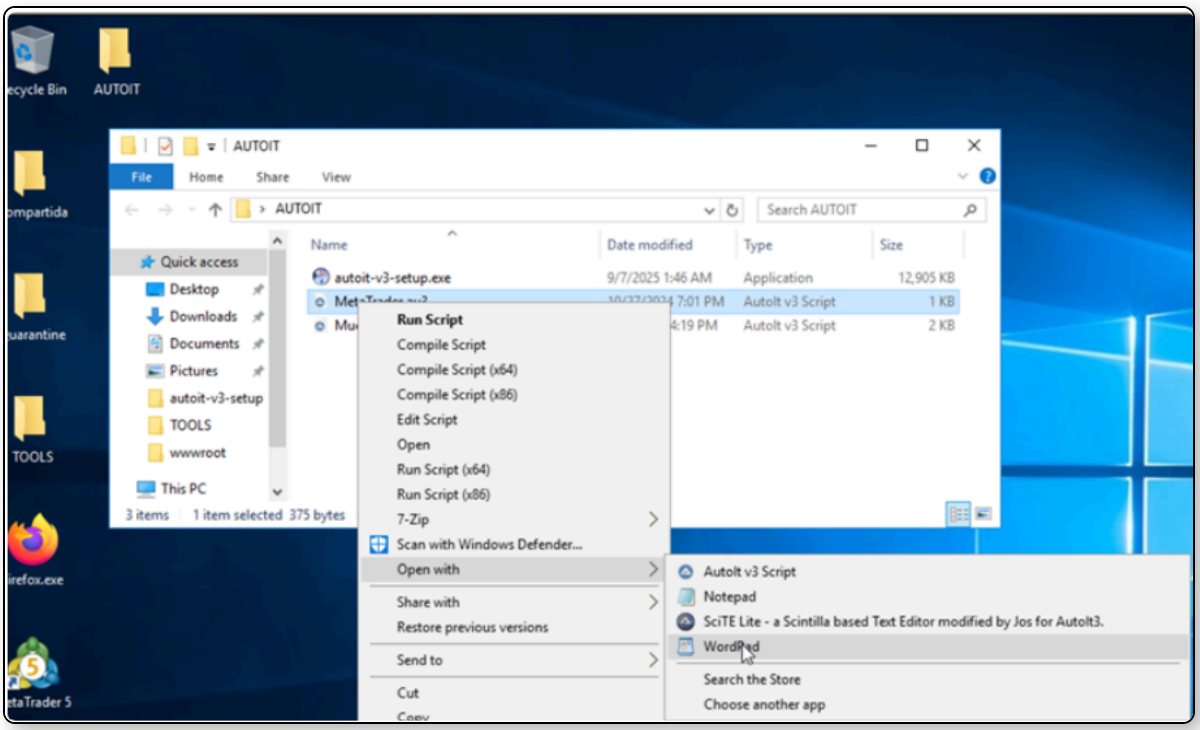
- We need to create a Secret for save our Metatrader´s credencial.

- In the FortiPAM go to “Secrets → Secret” and let´s to create a new secret with the next information:





- Save the secret. In this point we have and secret ID and an API Key.
- Got to “WindowsServer” and once the “AutoIT” installation has been finished, go to folder “AUTOIT” and open the file “MetaTrader.au3” with “Wordpad”:



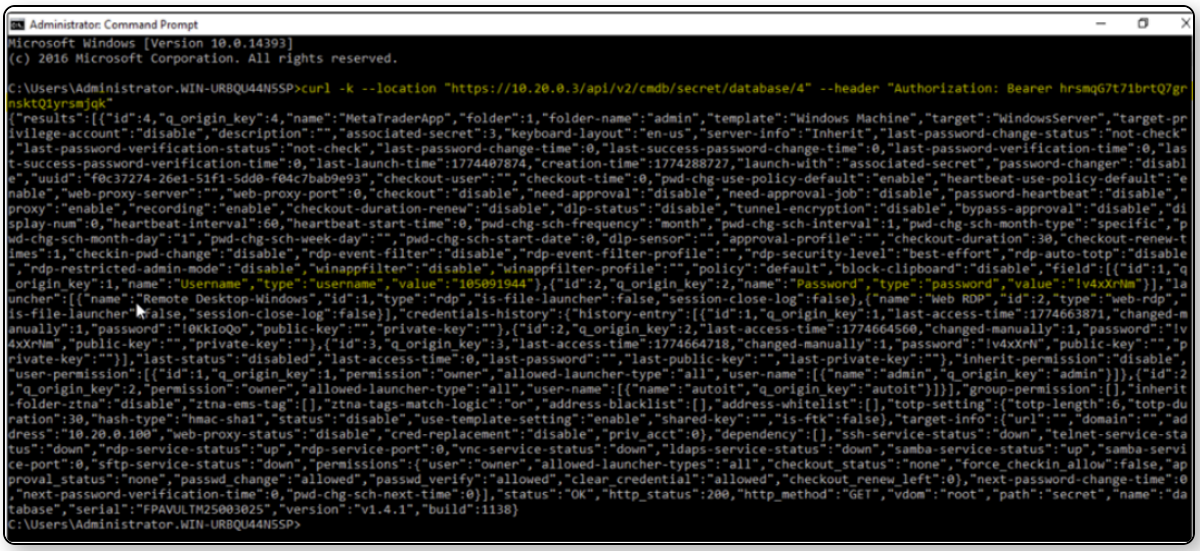
- You can see the script configuration. You will need change the next parameters: APY Key & Secret ID.

```
#RequireAdmin
#include <MsgBoxConstants.au3>
#include <MsgBoxConstants.au3>
#BlockInput(1)
Run("C:\terminal64.exe")
; --- Parámetros Extraídos de tu CURL Exitoso ---
Local $sUrl = "https://10.20.0.3/api/v2/cmdb/secret/database/1"
Local $sToken = "9tppkq0fqxN10x9s548c4khw1b3Qmf"
Local $sPassword = ""
; --- Petición ---
Local $oHTTP = ObjCreate("WinHttp.WinHttpRequest.5.1")
$oHTTP.Open("GET", $sUrl, False)
$oHTTP.Option(4) = 0x3300 ; Ignorar errores SSL (-k)
$oHTTP.SetRequestHeader("Authorization", "Bearer " & $sToken)
$oHTTP.Send()
; --- Response ---
Local $iStatus = $oHTTP.Status
Local $sResponse = $oHTTP.ResponseText
If $oHTTP.Status = 200 Then
    ; --- EXTRACCIÓN DEL PASSWORD ---
    ; Esta expresión busca donde dice "Password", salta el tipo y captura el "value"
    ; Estructura en tu JSON: "name":"Password","type":"password","value":"XxXxXxXxX"
    Local $aMatch = StringRegExp($sResponse, '"name":"Password".+?"value":"([^"]+)"', 1)

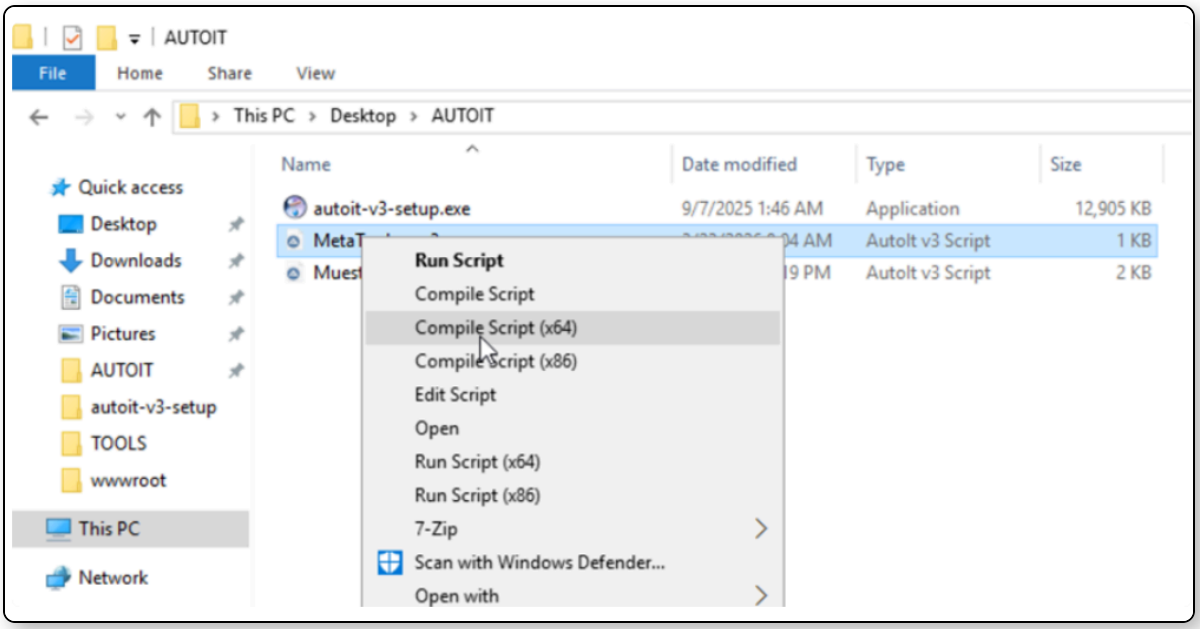
    If Not @error Then
        $sPassword = $aMatch[0] ; ¡Aquí se guarda el password

    Else
        MsgBox($MB_ICONERROR, "Error", "No se pudo encontrar el patrón del password en el JSON.")
    EndIf
Else
    MsgBox($MB_ICONERROR, "Error " & $oHTTP.Status, "No se pudo conectar al FortiPAM.")
EndIf
Sleep(35000)
Send($sPassword, 1)
Sleep(1000)
Send("{TAB}")
Send("{TAB}")
Sleep(1000)
Sleep(1000)
Send("{ENTER}")
BlockInput(0)
```

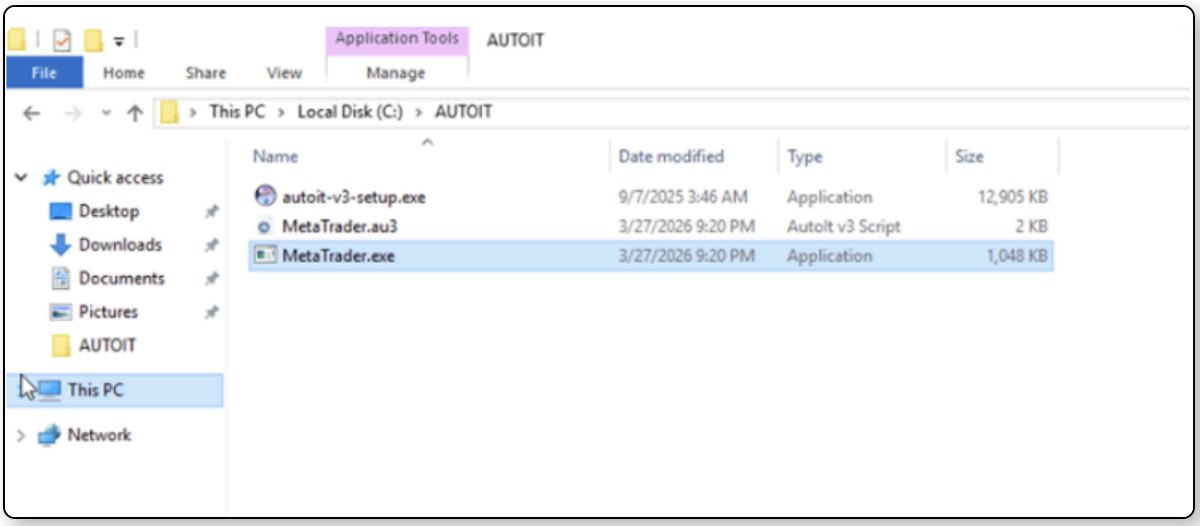
- You can edit and create your own custom script. You can use https://www.autoitscript.com/autoit3/docs/ the official documentation links about AutoIT.
- Curl is a great tool for test the calls API to FortiPam, in this way we can verify that the API works then we can use it in our own script:



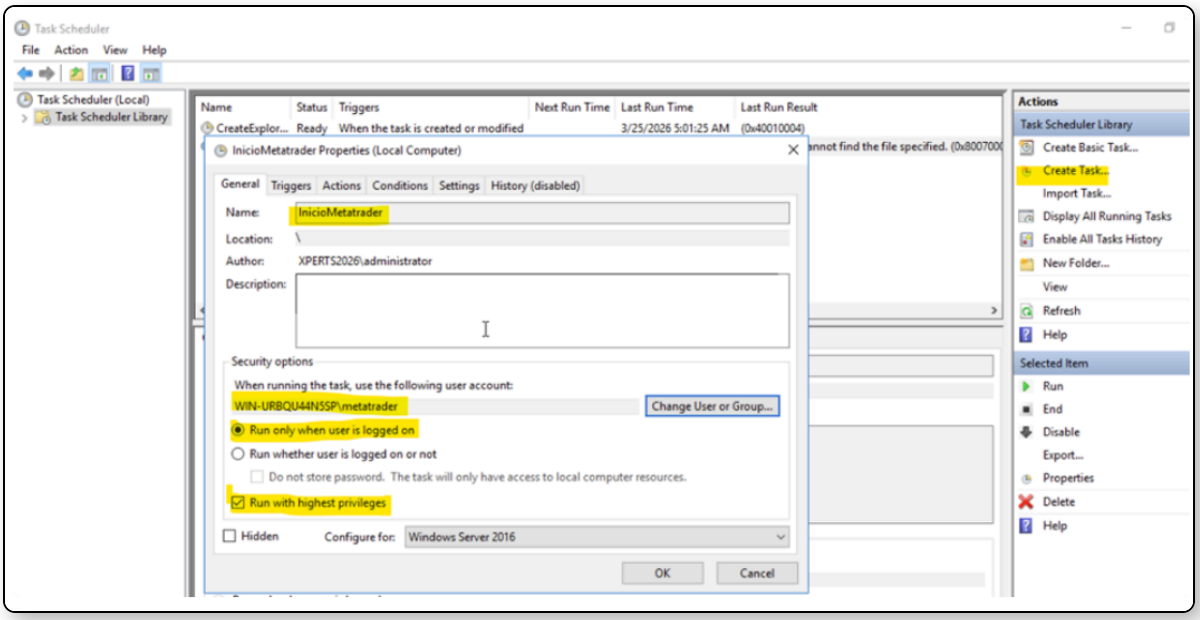
- And we can use the FortiPAM´s API official documentation: https://fndn.fortinet.net/index.php?/fortiapi/3047-fortipam/
- Please close the script and saved your changes. After this, we need to compile it.

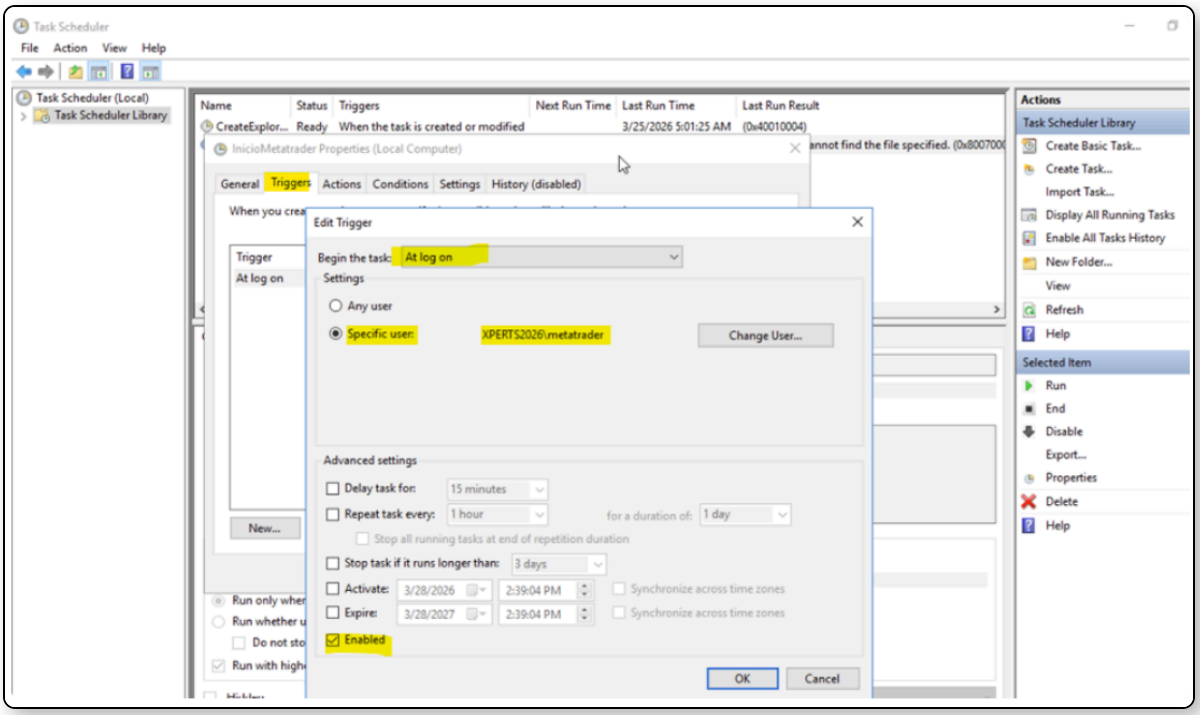


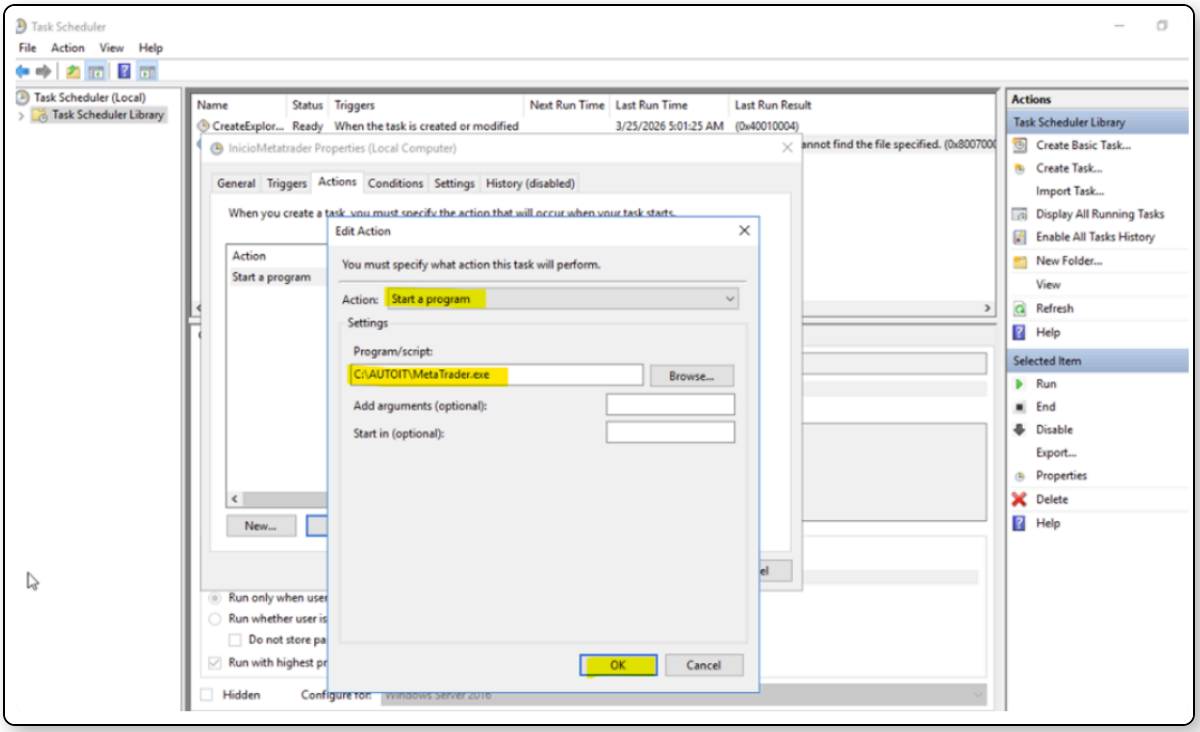
- We have already the .exe to invocate in the integration with FortiPAM.

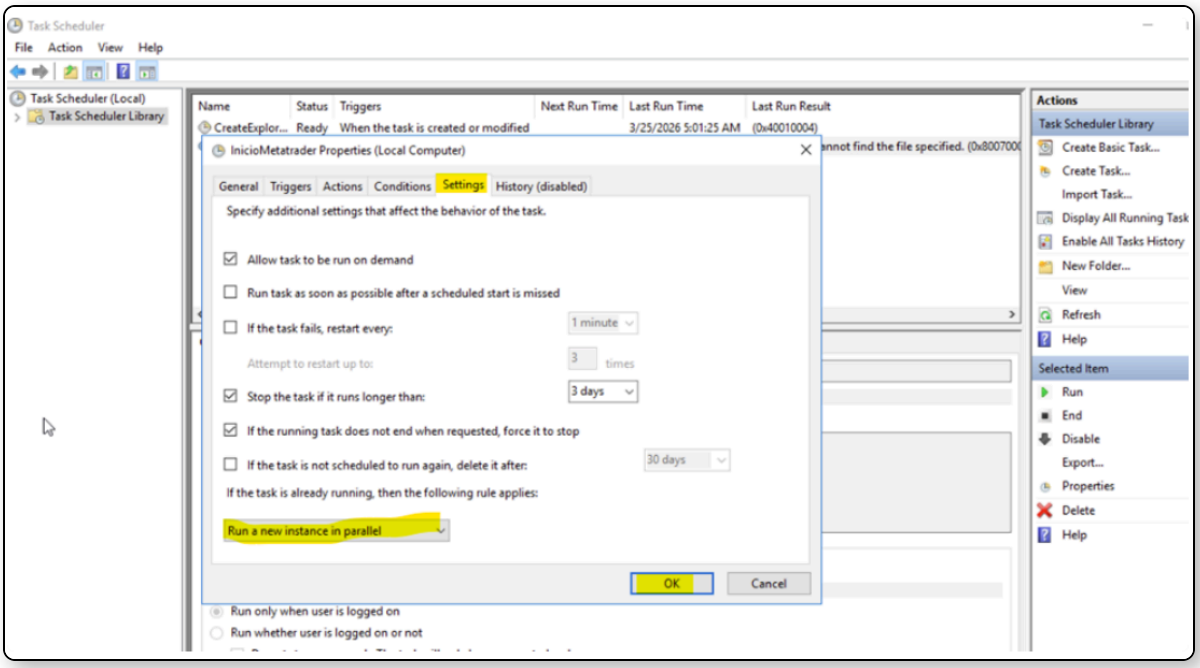


- We can test if this ".exe" works executing it with a double click.
- In the server, we will need make sure that this ".exe" is executed once there is a connection RDP. There are some ways to do this, but we will use a task schedule in “metatrader” logon.
- Press “Run” in the Windows Server, type “taskschd.msc” and press Enter. Click “Create Task” in the right panel follow the next instructions.

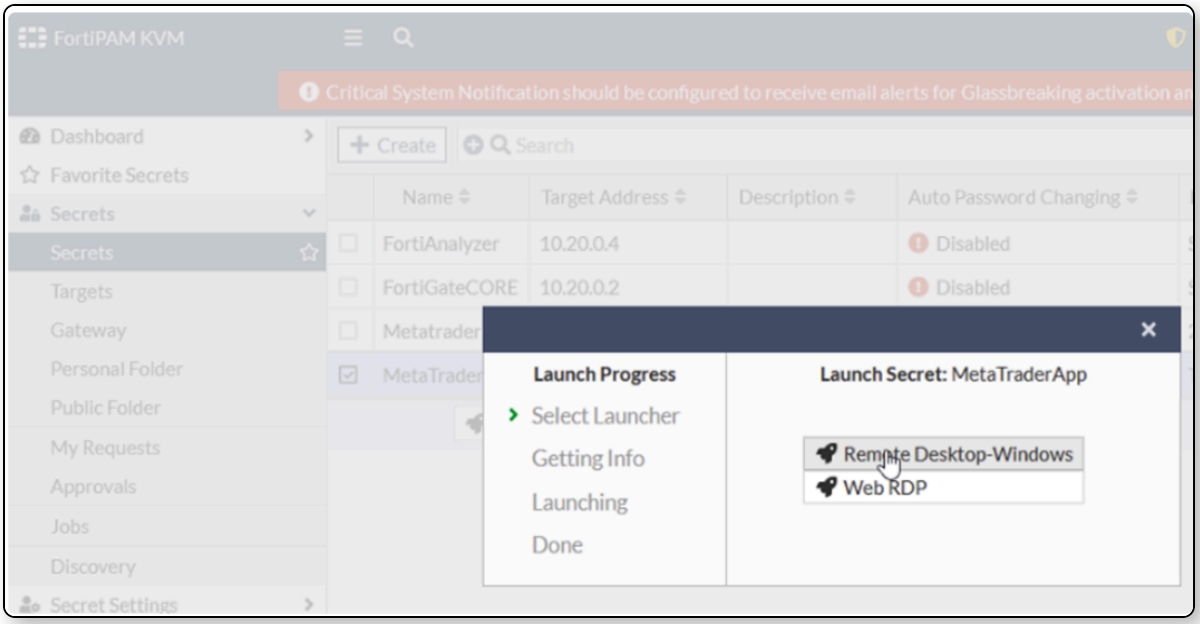


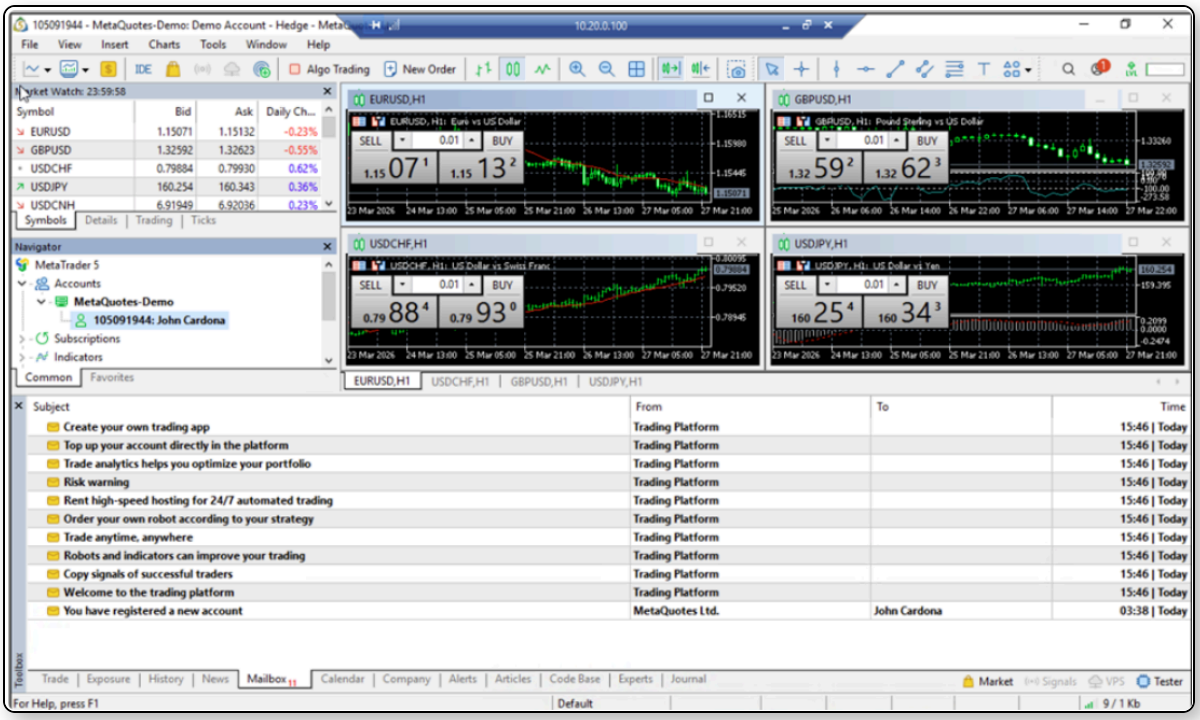

Task Scheduler
File Action View Help
Task Scheduler (Local)
Task Scheduler Library
Name Status Triggers Next Run Time Last Run Time Last Run Result
CreateExplor... Ready When the task is created or modified 3/25/2026 5:01:25 AM (0x40010004)
InicioMetatrader Properties (Local Computer)
General Triggers Actions Conditions Settings History (disabled)
Edit Trigger
Begin the task: At log on
Settings
Any user
Specific user: XPERTS2026\metatrader
Change User...
Advanced settings
Delay task for: 15 minutes
Repeat task every: 1 hour
for a duration of: 1 day
Stop all running tasks at end of repetition duration
Stop task if it runs longer than: 3 days
Activate: 3/28/2026 2:39:04 PM
Expire: 3/28/2027 2:39:04 PM
Synchronize across time zones
Enabled
OK
Cancel
Actions
Task Scheduler Library
Create Basic Task...
Create Task...
Import Task...
Display All Running Tasks
Enable All Tasks History
New Folder...
View
Refresh
Help
Selected Item
Run
End
Disable
Export...
Properties
Delete
Help


Task Scheduler
File Action View Help
Task Scheduler (Local)
Task Scheduler Library
Name Status Triggers Next Run Time Last Run Time Last Run Result
CreateExplor... Ready When the task is created or modified 3/25/2026 5:01:25 AM (0x40010004)
InicioMetatrader Properties (Local Computer)
General Triggers Actions Conditions Settings History (disabled)
When you create a task, you must specify the action that will occur when your task starts.
Edit Action
You must specify what action this task will perform.
Action: Start a program
Settings
Program/script: C:\AUTOIT\MetaTrader.exe
Browse...
Add arguments (optional):
Start in (optional):
OK
Cancel
Actions
Task Scheduler Library
Create Basic Task...
Create Task...
Import Task...
Display All Running Tasks
Enable All Tasks History
New Folder...
View
Refresh
Help
Selected Item
Run
End
Disable
Export...
Properties
Delete
Help



- In this way we already have a task that will be executed when a login in windows server with “metatrader” account es due.
- We can test that all this work. Go to “Victim” device, open FortiPAM via HTTPS and log in with “Admin” account.
- Select the secret "MetaTraderApp" and clic in lunch "Remote Desktop-Windows":




105091944 - MetaQuotes-Demo: Demo Account - Hedge - MetaTrader 5
10.20.0.100
File View Insert Charts Tools Window Help
Algo Trading New Order
Market Watch: 23:59:58
Symbol Bid Ask Daily Ch...
EURUSD 1.15071 1.15132 -0.23%
GBPUSD 1.32592 1.32623 -0.55%
USDCHF 0.79884 0.79930 0.62%
USDJPY 160.254 160.343 0.36%
USDCNH 6.91949 6.92036 0.23%
Symbols Details Trading Ticks
Navigator
MetaTrader 5
Accounts
MetaQuotes-Demo
105091944: John Cardona
Subscriptions
Indicators
Common Favorites
EURUSD,H1
GBPUSD,H1
USDCHF,H1
USDJPY,H1
EURUSD,H1 USDCHF,H1 GBPUSD,H1 USDJPY,H1
Subject From To Time
Create your own trading app Trading Platform 15:46 | Today
Top up your account directly in the platform Trading Platform 15:46 | Today
Trade analytics helps you optimize your portfolio Trading Platform 15:46 | Today
Risk warning Trading Platform 15:46 | Today
Rent high-speed hosting for 24/7 automated trading Trading Platform 15:46 | Today
Order your own robot according to your strategy Trading Platform 15:46 | Today
Trade anytime, anywhere Trading Platform 15:46 | Today
Robots and indicators can improve your trading Trading Platform 15:46 | Today
Copy signals of successful traders Trading Platform 15:46 | Today
Welcome to the trading platform Trading Platform 15:46 | Today
You have registered a new account MetaQuotes Ltd. John Cardona 03:38 | Today
Trade Exposure History News Mailbox 11 Calendar Company Alerts Articles Code Base Experts Journal
Market Signals VPS Tester
For Help, press F1
Default
9 / 1 Kb

Storytelling Agro Meals

THIS IS THE STORY OF “AGRO-MEALS”: FROM OPERATIONAL "BLIND SPOT" TO TOTAL RESILIENCE

THE CHALLENGE: Feeding the world blindly.

At the heart of Agro-Meals, operations never stop. With 10 processing plants and more than 50 farms, the protein that reaches thousands of tables depends on critical OT architecture where downtime is not an option.

THE PROBLEM was invisible but latent:

Being rural environments with high employee turnover, any contractor or employee could connect a device to the network without supervision. With no capacity for virtualization (VM) or space for new infrastructure on the farms, East-West traffic was a black hole: if a threat entered through one farm, it could spread laterally and paralyze a processing plant. Additionally, there was a need to provide remote access to third-party users for support, seeking to simplify the current VPN scenario.

THE SOLUTION:

Visibility, Intelligence, and automated response with easy integration into existing architecture. Agro-Meals needed its current infrastructure to be smarter. Leveraging their existing FortiGate devices in more than 60 locations and a FortiAnalyzer with an OT license, the strategy focused on three pillars:

1. Total Visibility and 24/7 response: FortiNDR VM16 was implemented and integrated as follows: - Via Netflow with all FortiGate devices, and we also used the port capacity as "One-Arm" to act as a network sniffer for lower network layers. - Via Fabric to the root FortiGate device to enhance the AV module of the FortiGate infrastructure. - Via SMB with file servers to inspect and detect malicious files.

2. Centralized secure remote access: FortiPAM was implemented as a remote access tool for third parties, allowing supervised access with privileged users to internal OT servers WITHOUT depending on and requiring the necessary support of a VPN client.

3. Agnostic Automated Response: FortiSOAR is implemented, which integrates with FortiAnalyzer and FortiNDR. These solutions generate the necessary detections for FortiSOAR to execute automated responses across virtually any integrated platform.

THE RESULT: A Secure Operation

Today, Agro-Meals not only processes food; it processes data securely. They have achieved complete visibility of internal traffic: east-west and north-south, with an immediate response capability that doesn't depend on an engineer traveling hours to a farm. The OT network is now a resilient asset, ready to scale regardless of who connects to it.

ARCHITECTURE OF SOLUTION

