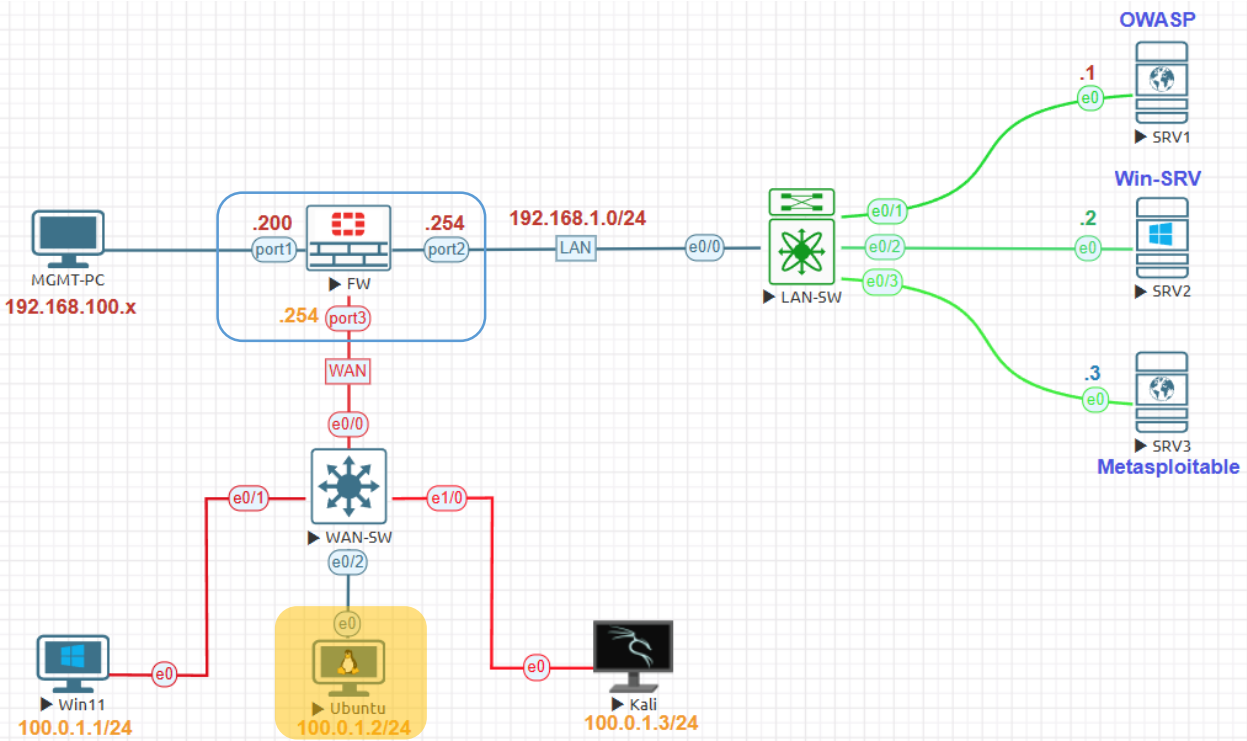
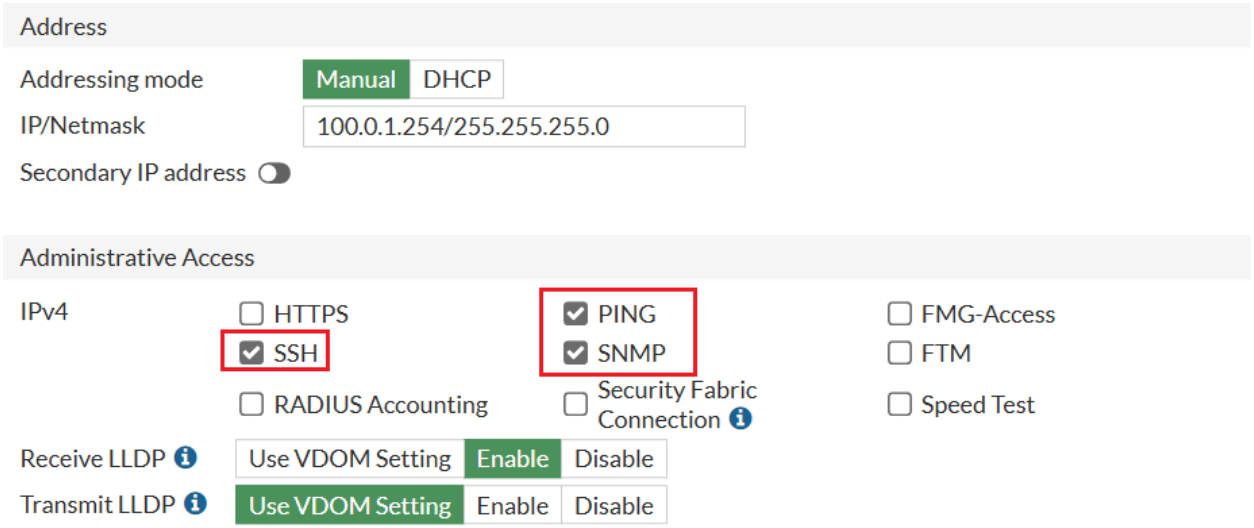
FortiGate Firewall Vulnerability Scan Lab:



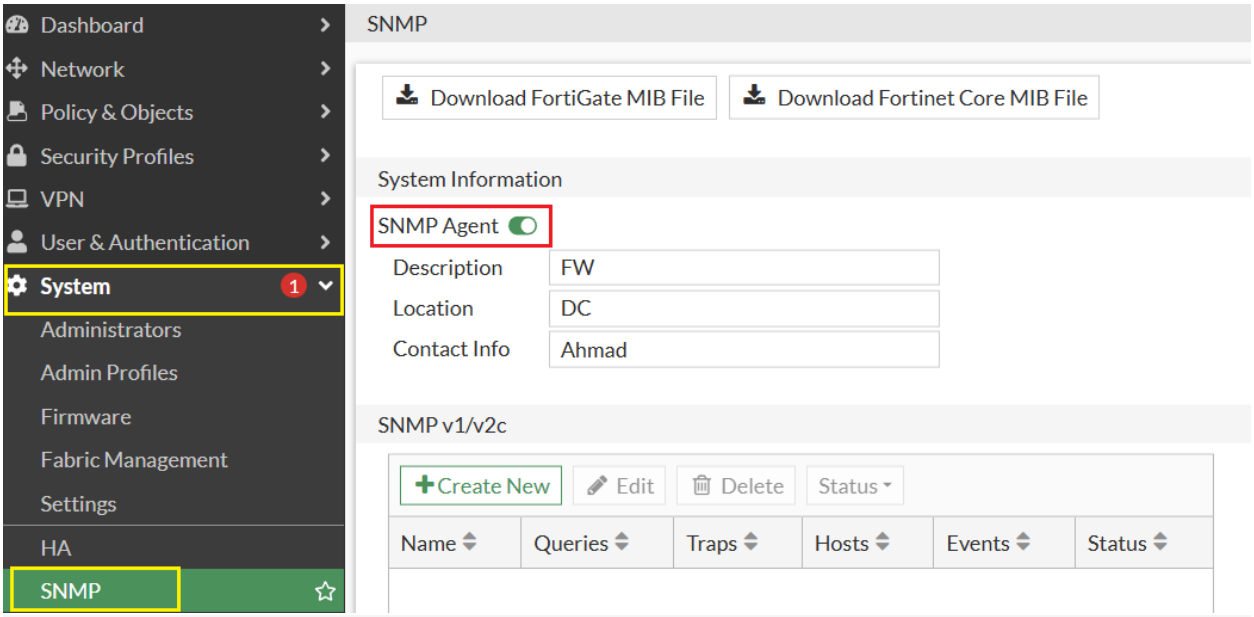
Management Subnet	192.168.100.0/24
FortiGate Management IP	192.168.100.200
Internal Servers Subnet	192.168.1.0/24
FortiGate Firewall External	100.0.1.0/24
FortiGate Firewall Internal IP	192.168.1.254
FortiGate Firewall External IP	100.0.1.254
SRV1 IP Address	192.168.1.1
SRV2 IP Address	192.168.1.2
SRV3 IP Address	192.168.1.3
External Win11 IP Address	100.0.1.1
External Ubuntu IP Address	100.0.1.2
External Kali IP Address	100.0.1.3

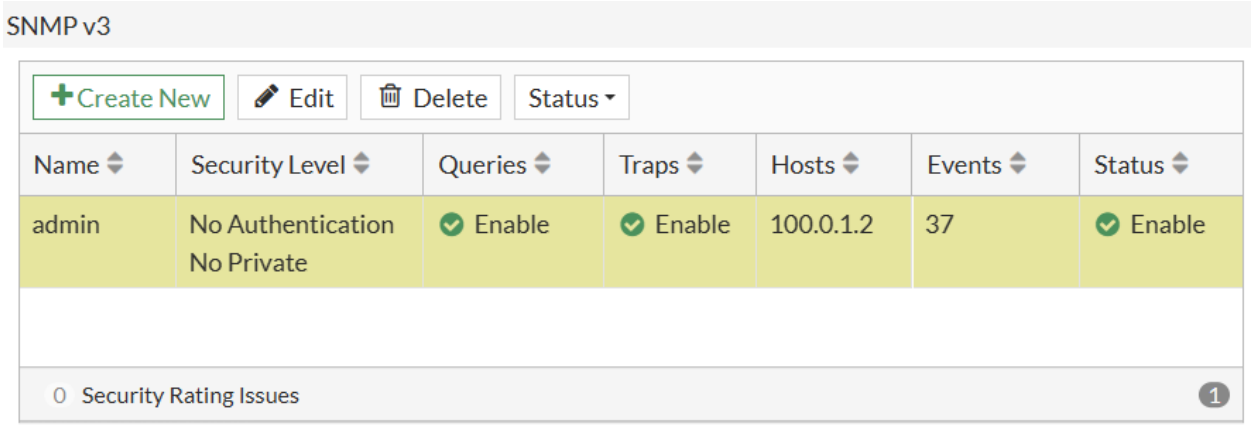
Devices	**Username**	**Password**
FortiGate 7.0.9	Admin	123
Linux Kali 2025.1c	kali	kali
Linux Ubuntu 22.04 Desktop	user	Test123
Windows 11 x64 SE	user(Administrator)	Test123
Linux Metasploitable 2.0	msfadmin	msfadmin
Linux-OWASP	root	owaspbwa
Windows Server 2012	Administrator	Test123

Before Start the scan enable PING,SNMP and SSH on WAN Interface of FortiGate Firewall.

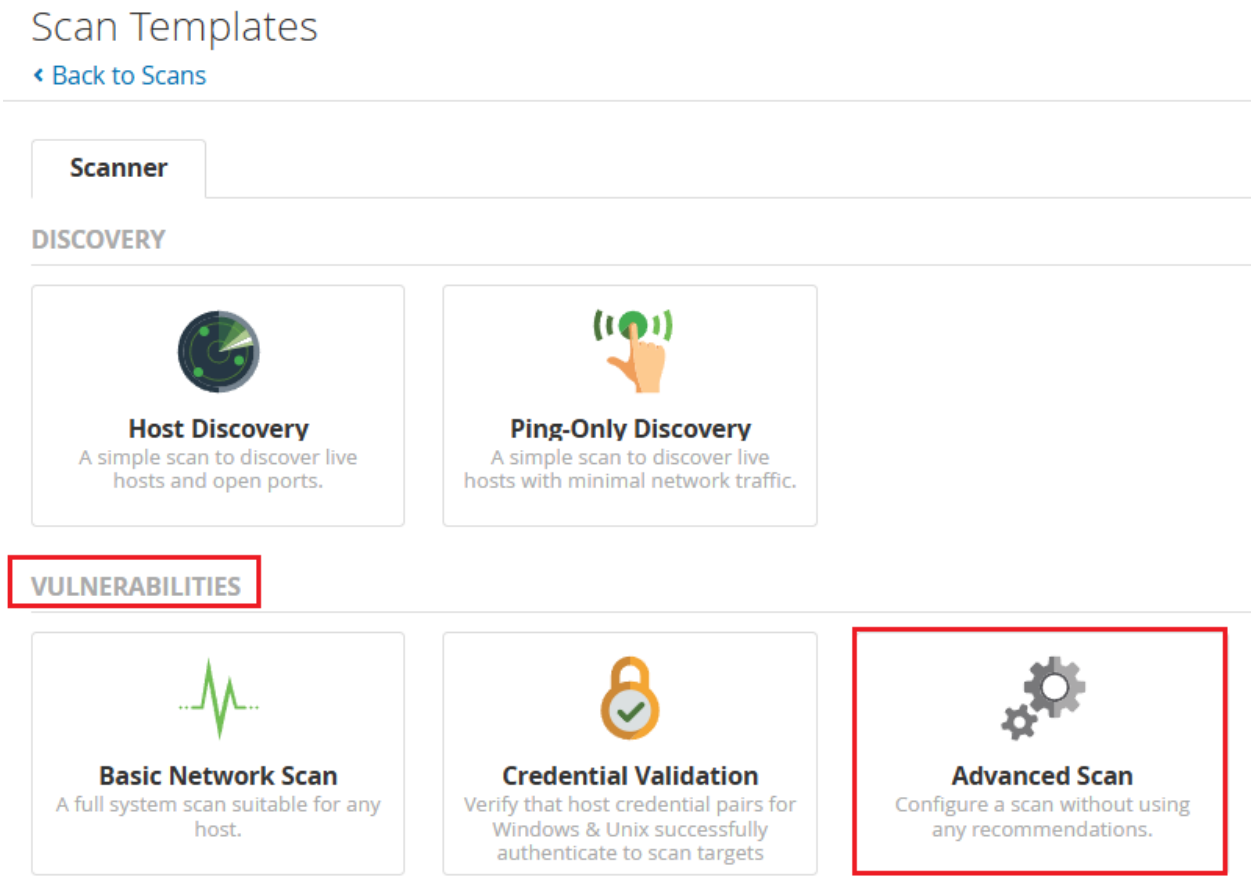


Enable SNMP Agent.

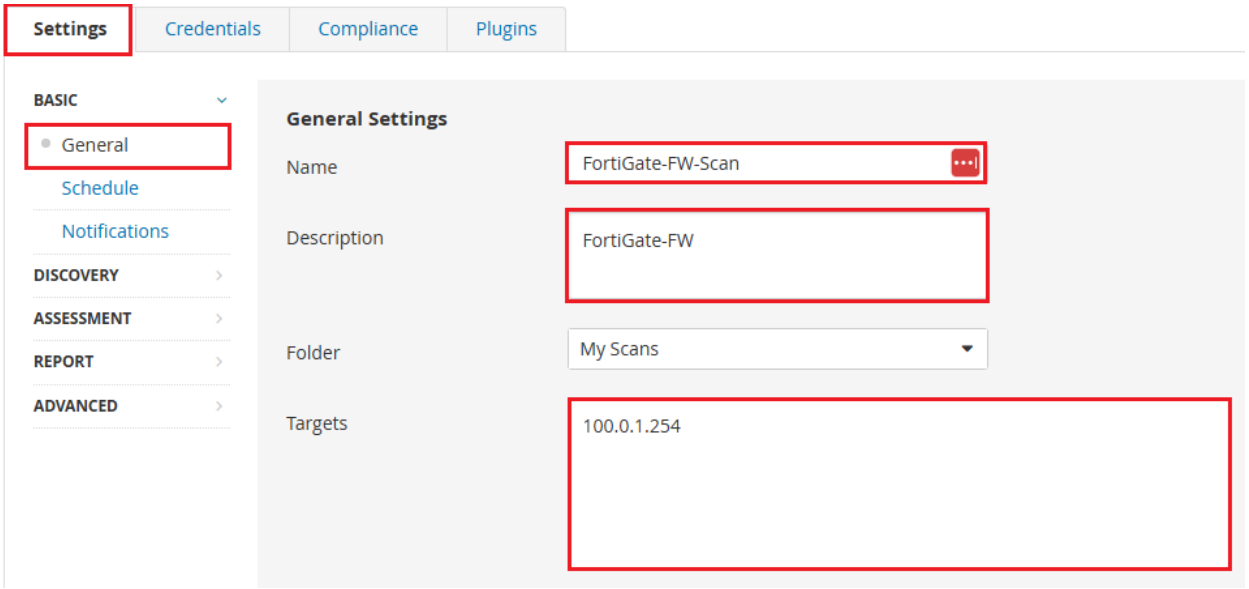




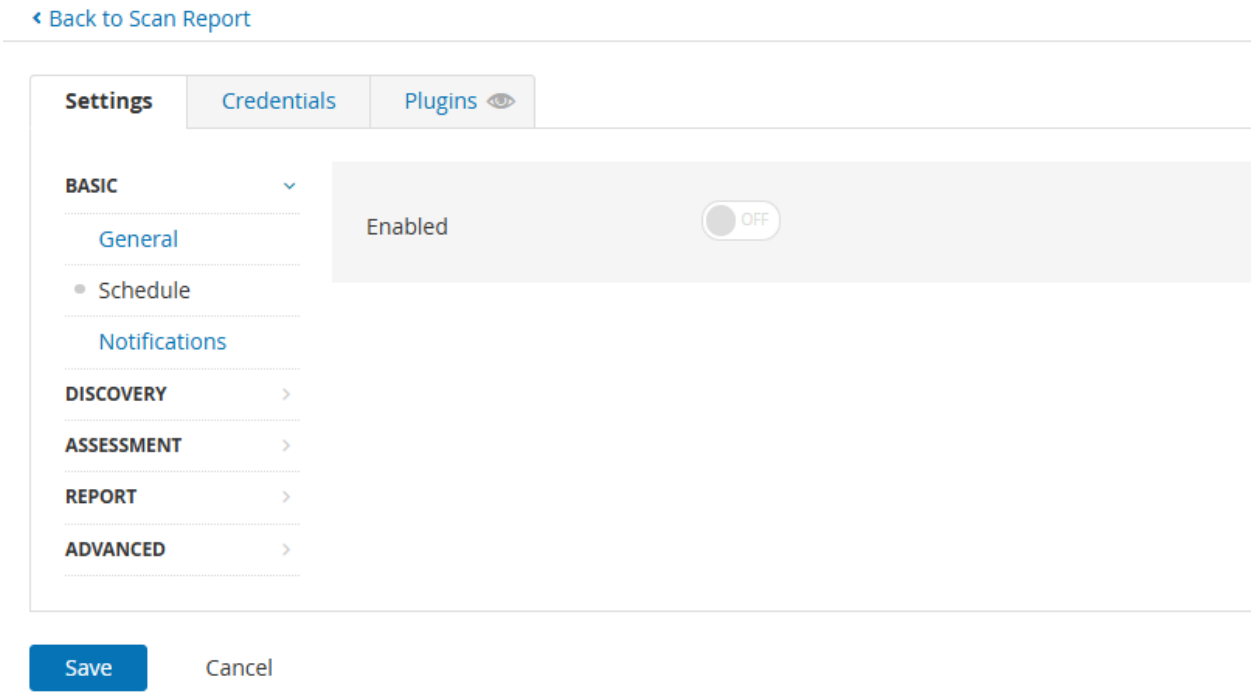
Go to Scans > New Scan. Choose Advanced Scan to open.



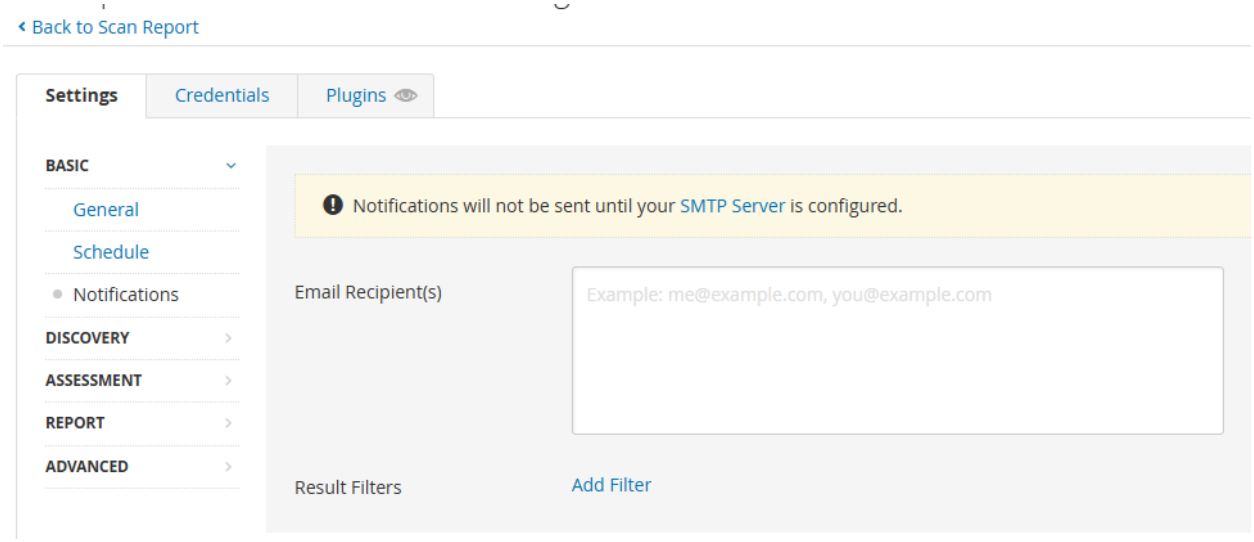
Name: FortiGate-FW-Scan. Targets: IP address of target 100.0.1.254 the IP Address of WAN Interface of FortiGate Firewall.



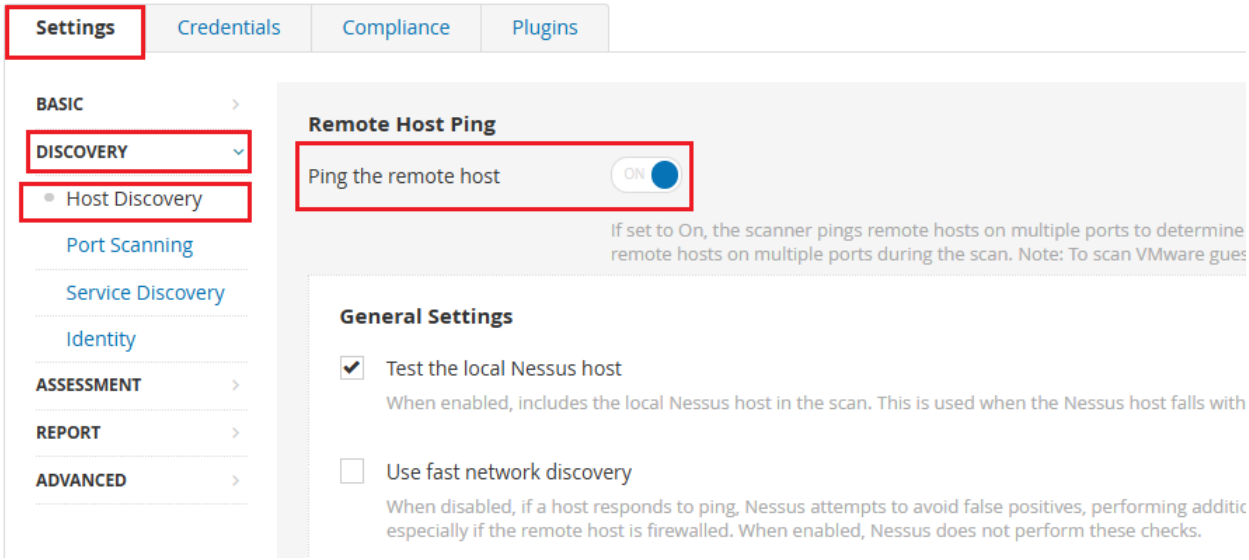
Basic>Schedule keep default disable.



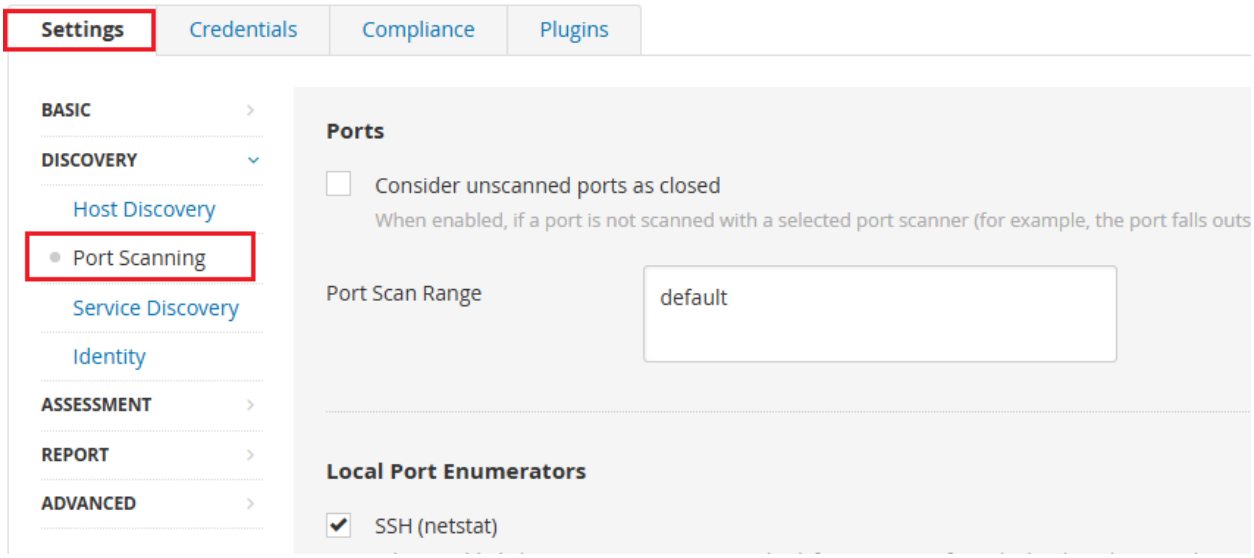
Basic>Notification keep default disable.



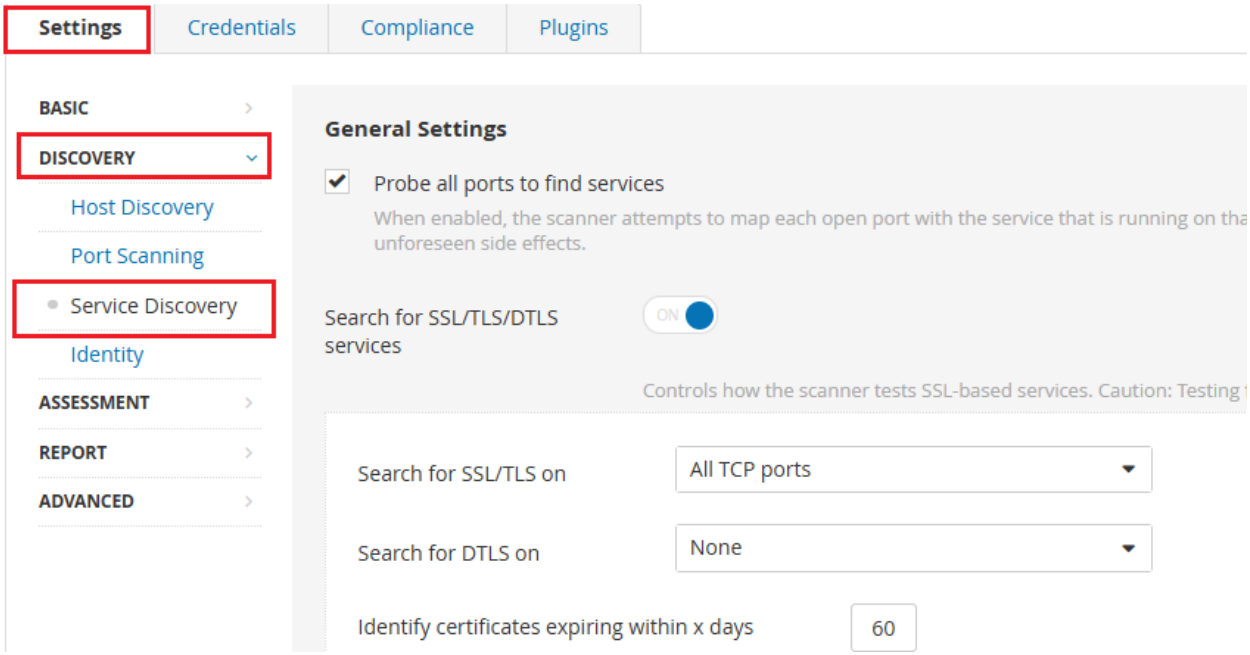
Basic>Discovery>Host Discovery keep default enable.



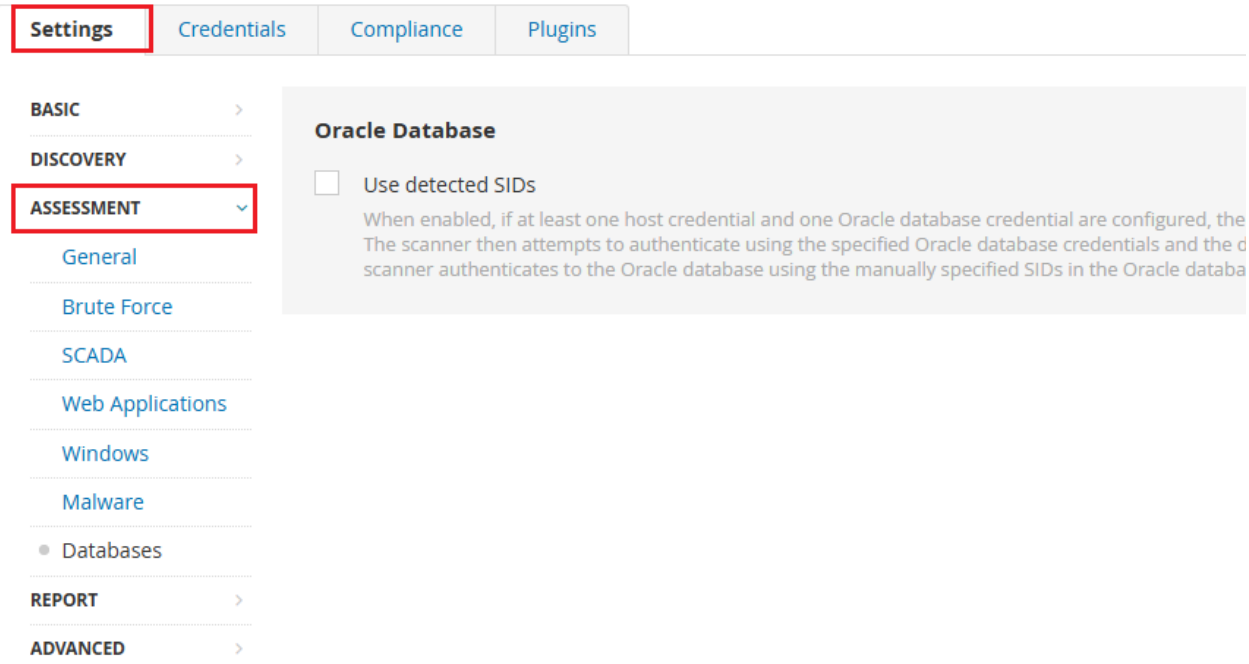
Basic>Discovery>Port Scanning keep default.



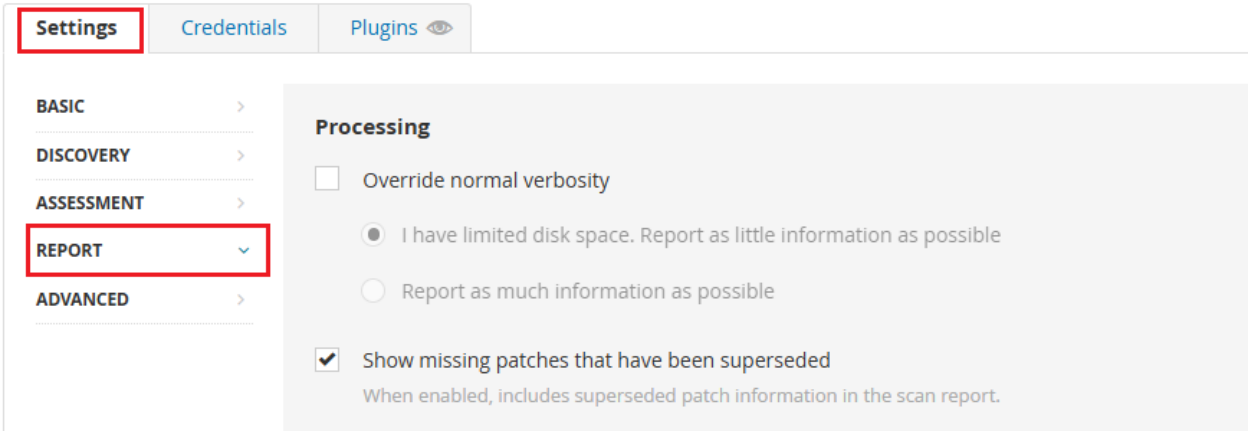
Basic>Discovery>Service Discovery keep default.



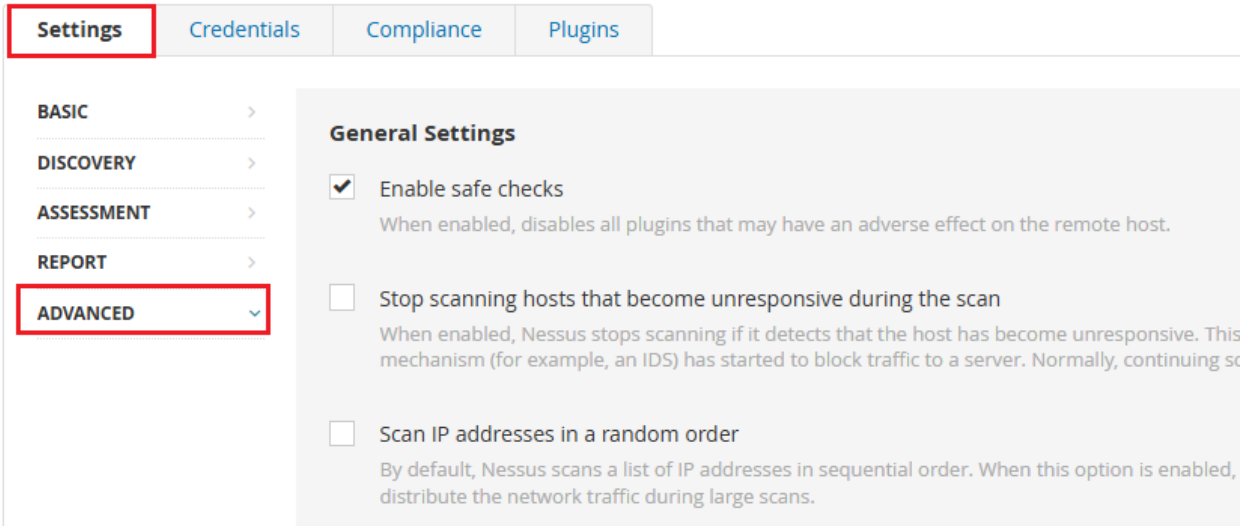
Basic>Assessment keep default.



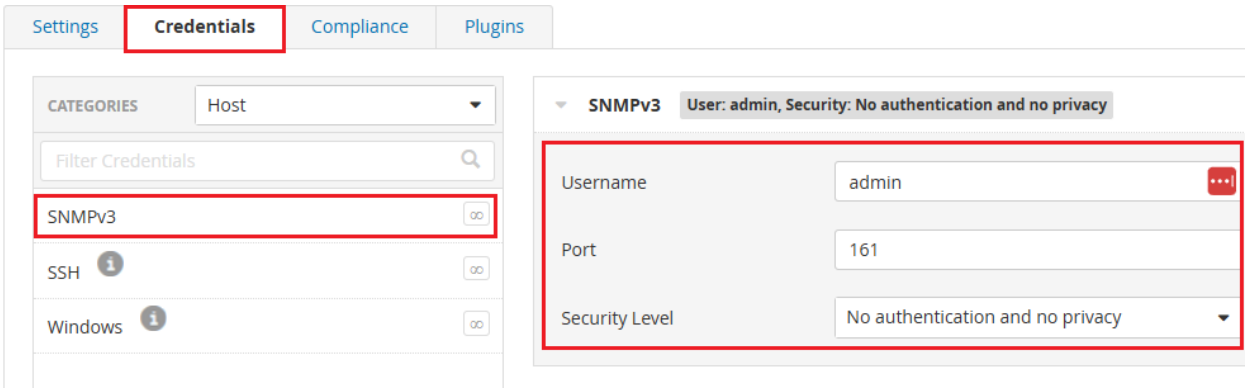
Settings>Reports keep default no changes.



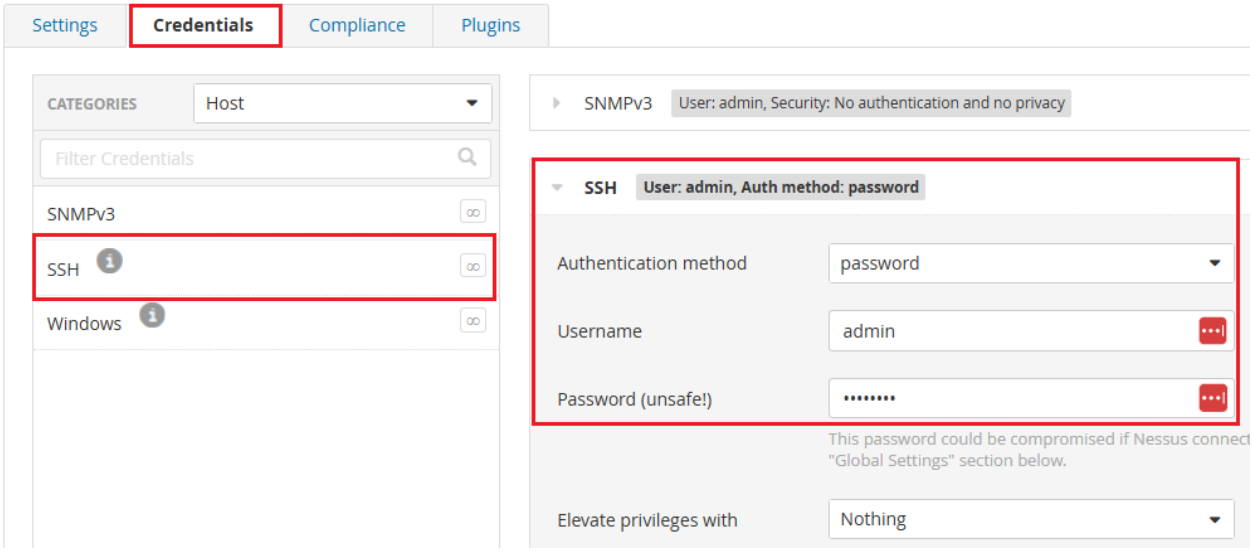
Settings>Advanced keep default no changes.



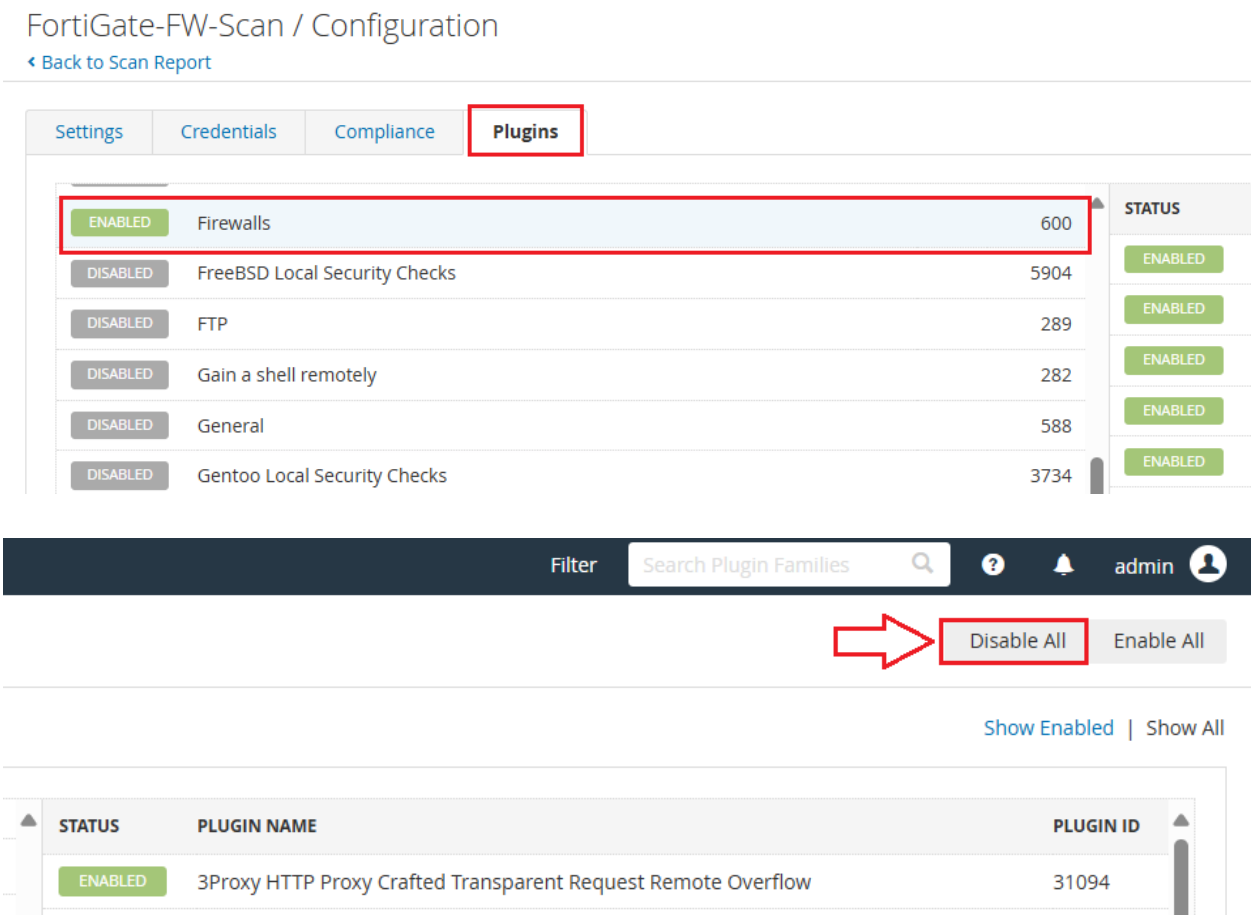
Under Credentials Tab. Choose SSH and SNMP3 authentication methods. In SNMP enter Username: admin keep the default Port:161 Security Level: No authentication and no privacy



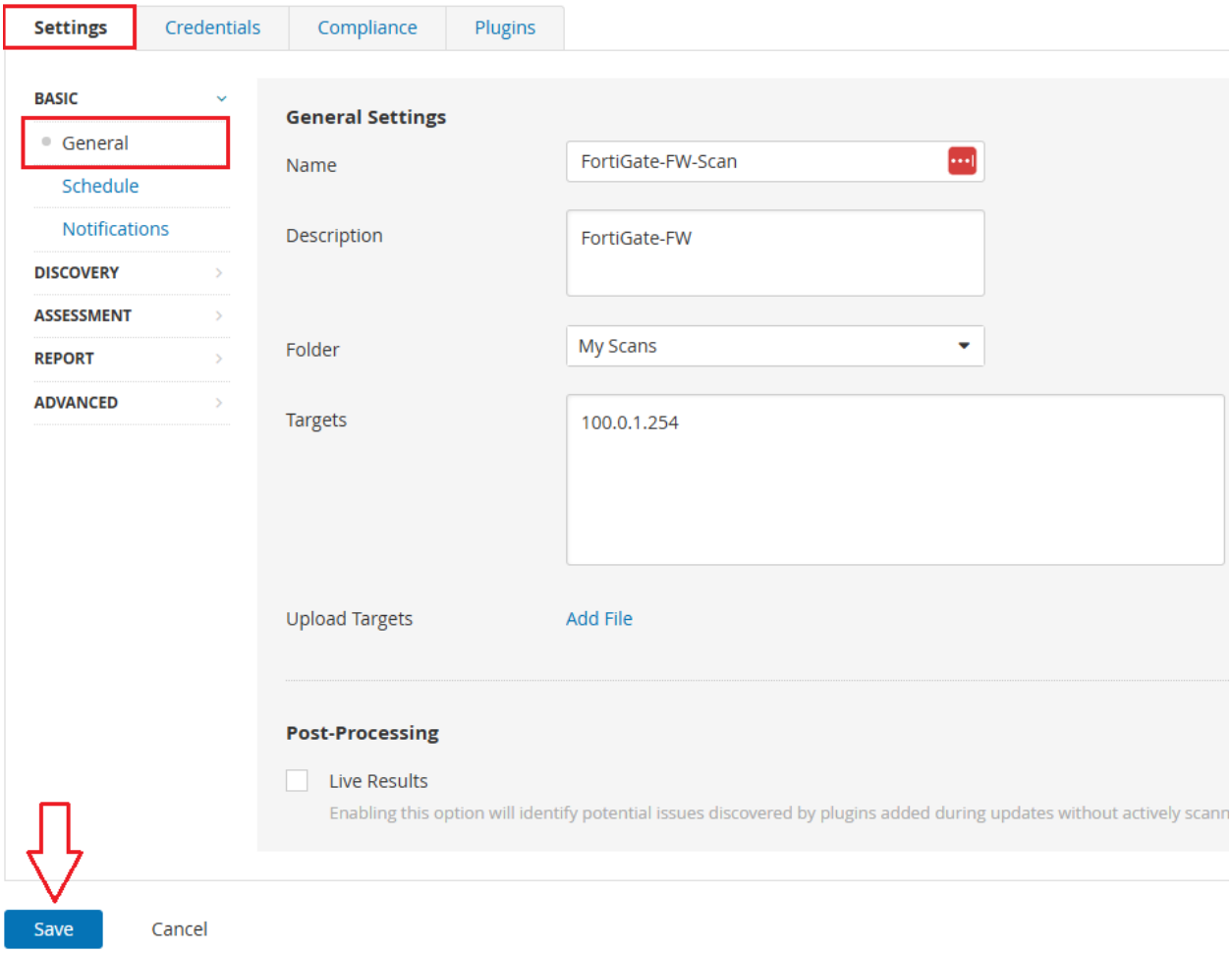
In SSH choose the Authentication method: Password enter username and password of FortiGate Firewall admin/123



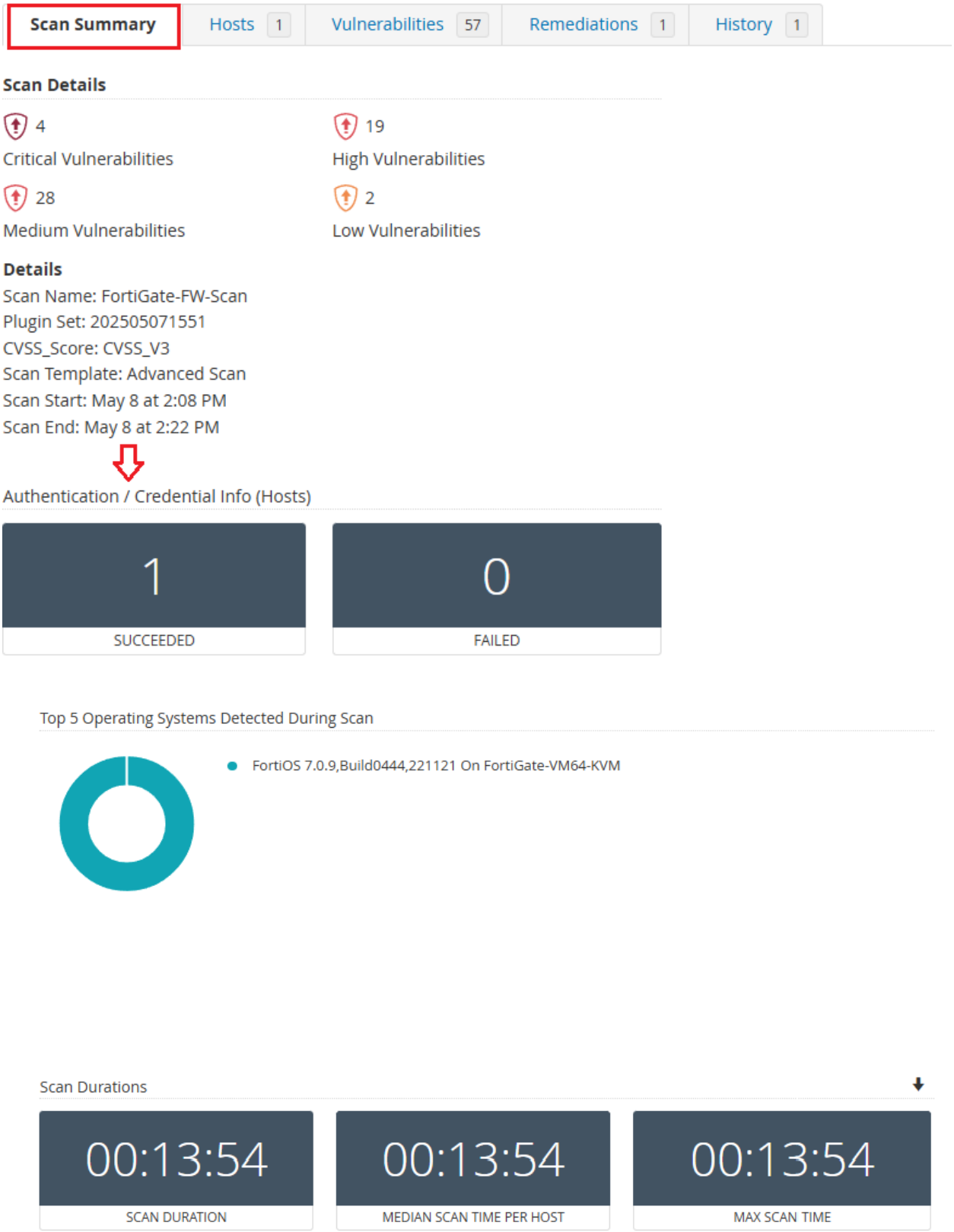
Plugins Tab disable all Plugins only enable Firewalls plugin.



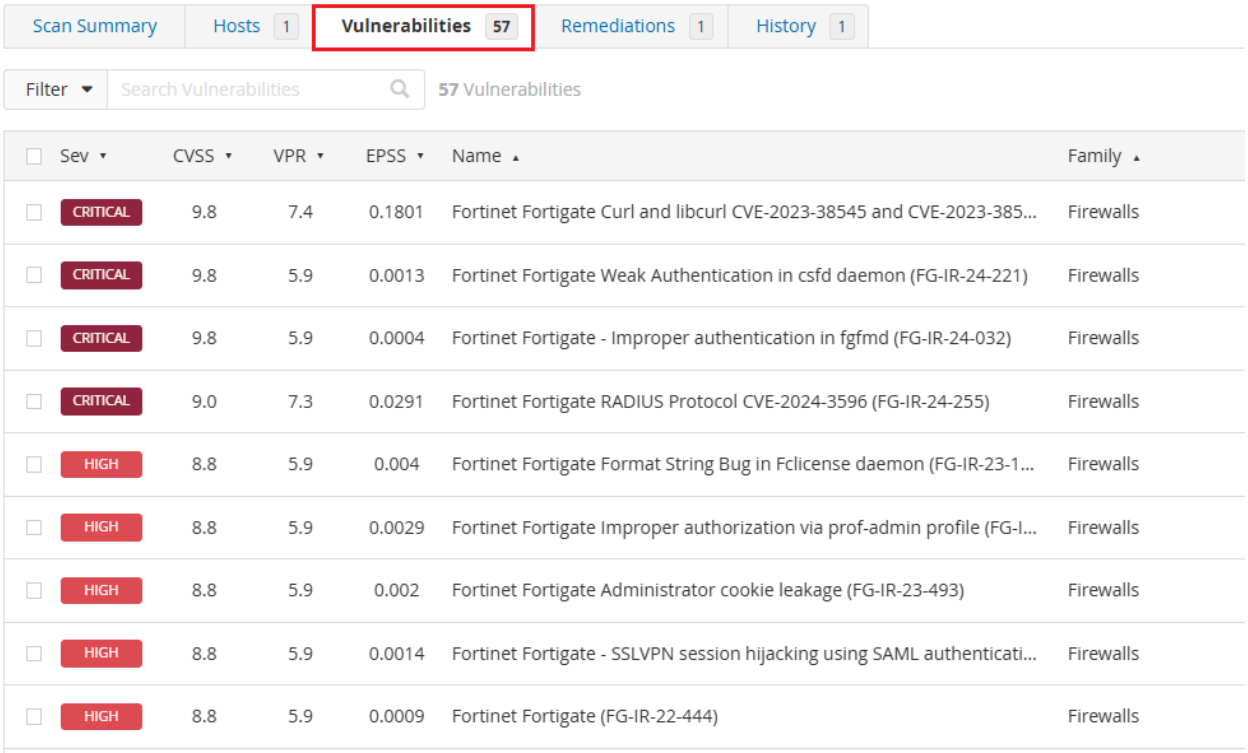
Click Save Then Launch. Wait for the scan to complete.

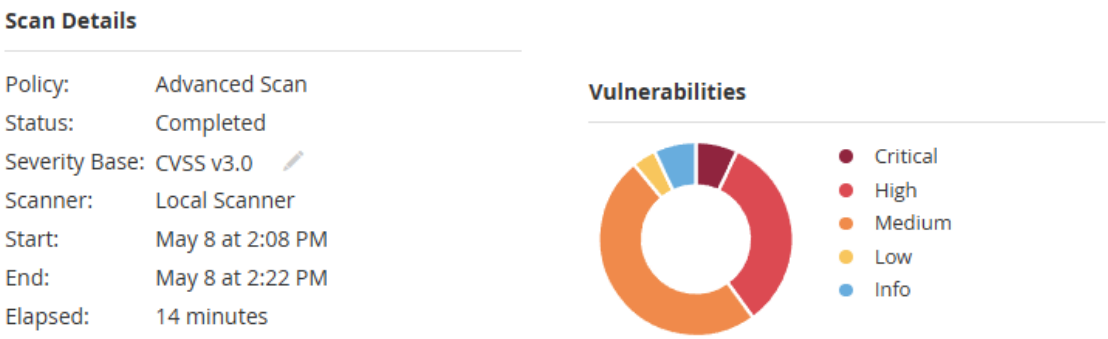


After complete the scan, Scan Summary Show Authentication / Credential info (Hosts) Succeeded.



Under Vulnerabilities Tab it shows almost 57





Under Remediation Tab