

Sniffa Runbook Adding Policies to a Sensor in the Sensor Manager Application

Serial	Instruction			
	Overview. Rules Policies consist of 1 or more Snort [™] rules that are grouped together based upon a common attribute, e.g. Application, Protocol, Attack Type, etc.			
	1 or more Snort™ rules policies can be added to a Sensor's configuration file and stored in the Sensor Manager Application database.			
	All of the Snort™ rules that are included in a Sensor's configuration file, will be deployed out to the network Sensor at deployment time.			
	Snort™ rules policies can be added to Sensors in 2 ways:			
	 Via the Rules Management Panel (serial 1 onwards). Via the Sensor Management Panel (serial 10 onwards). 			
	This runbook includes the tasks to be completed, to add Sensor Manager Application.	Snort™ rules policies to a Senso	or in the	
1.	Adding policies via the Rules Management Panel.			
	Go to the Admin panel. Select the 'Configure' menu item. Select the 'Snort™ Rules' menu item.	Admin Alerts Connections DNS HTTP Configure Configure Configure Admin Configure Configure Metwork Metwork	ages ,	
2.	Select the 'Options' menu item. Select the 'Rule Policies' menu item.	Sniffa Sensor Manager (v.1.02.007) Admin Alerts Options View Alerts DNS HTTP HTTP HTTP Sign 12 Save Filter 118 119 121 Export Displayed Rules 1 141 142 144 10	ture ID	



Sniffa Runbook



3.	Adding multiple polices to a single Sensor. Highlight one Sensor from the list in the left-hand table, using the left mouse button.	Sniffs Sensor Manager (v. 1.02.007) Admin Add Policies to Sensor Aderst Onnections DNS HTTP HTTPS
4.	Highlight 1 or more of the Rule Policies from the right-hand table, using the left mouse button. <i>Note:</i> <i>Use the 'Shift' or 'Ctrl' button in conjunction with the</i> <i>left mouse button to select multiple polices.</i>	Policy(s) on Selected Sensor Policy(s) on Selected Sensor Add Policies from the list Add Policies from the list
5.	Click on the button marked with the left arrow, to add the selected polices to the selected Sensor. Selected policies should appear in the middle table.	Policy(s) on Selected Sensor Add Policies from 1 Adobe_Flash Adwind Adwind Adwind ActiveAgent_NDV Adbe_Coldfusion Adobe_Flash Adobe_Flash Adobe_Coldfusion Adobe_Clash
6.	Adding a single policy to multiple Sensors. Select the 'Options' menu item. Select the 'Switch View' menu item.	 Sniffa Sensor Manager (v.1.02.007) Admin Alerts Connections Sniffa-Sensor-C Sniffa-Sensor-U





Sniffa Runbook Adding Policies to a Sensor in the Sensor Manager Application

7.	Highlight one Policy from the list in the left-hand table, using the left mouse button.	 Sniffa Sensor Manager (v.1.02.007) Admin Add Sensor to Policy Alerts Select a Policy ActiveAgent ActiveAgent<
8.	Highlight 1 or more of the Sensor from the right- hand table, using the left mouse button. Note: Use the 'Shift' or 'Ctrl' button in conjunction with the left mouse button to select multiple Sensors.	Add a Sensor from list Add a Sensor-C Sniffa-Sensor-U
9.	Click on the button marked with the left arrow, to add the selected Sensors to the selected Policy. Selected Sensors should appear in the middle table.	Sensor with Selected Policy Added Sensor-C Sensor-C Sindfa-Sensor-C Sindfa-Sensor-U Sindfa-Sensor-U
10.	Adding policies via the Sensor Management Panel. Go to the Admin panel. Select the 'Configure' menu item. Select the 'Sensors' menu item.	 Sniffa Sensor Manager (v.1.02.007) Admin Alerts Connections DNS HTTP Syslog Collector



Sniffa Runbook Adding Policies to a Sensor in the Sensor Manager Application

11.	Right click on a Sensor and select 'Snort™' and then select the 'Policies' menu item.	Hostname Alias IP Address Status Sniffa-Senor-11 Sniffa-Sensor-11 192.168.1.9 ONLIN Sniffa-Sen SSH to Sensor 192.168.1.8 ONLIN Sniffa-Sen Restart Sensor (shutdown and restart) istatus Settist Sensor Settings Clone Sensor Settings Clone Sensor Settings istatus Sont** Policies Sont** Settist Get Configuration File Dumpcap** Get Rules File Get Rules File Packet Capture Probe Appliance Get IP Blacklist Get IP Whitelist
12.	Highlight 1 or more policies from the left-hand table, using the left mouse button. <i>Note:</i> <i>Use the 'Shift' or 'Ctrl' button in conjunction with the</i> <i>left mouse button to select multiple Sensors.</i>	Sensor Policies set for Sniffa-Sensor-U - X All Policies All Policies All Policies ActiveAgent ActiveA
13.	Click on the button marked with the right arrow, to add the selected policies to the Sensor. Selected policies should appear in the right-hand table.	All Policies set for Sniffa-Sensor-U - × All Policies Adobe_Flash Adobe_Flash 1xxbot Adobe_Flash Adobe_Flash ACBeckdoor Adobe_Flash Oday ActiveX Adobe_Flash Adobe_Flash Adobe_Flash Adobe_Flash Adobe_Flash
14.	Click on the cross at the top right-hand corner to close the policies window.	- X
15.	End of Runbook.	