



Coriol				
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 can be grouped into a rules policy in 4 ways: Automatically on rules import, based on the rules file name. Automatically on rules import, based upon the metadata tags within a rule. Automatically on rules import, based upon the date/time of import. Manually from the rules table from within the Snort[™] Rules Manager panel (this runbook). 			
	This runbook includes the tasks to be completed, to add Snort™ rules manually to a policy in the Sensor Manager Application.			
1.	Go to the Admin panel. Select the 'Configure' menu item. Select the 'Snort™ Rules' menu item. Admin Alerts DNS DNS HTTP Syslog Collector →			
2.	Select the rules to add to a Policy. Right Click the selected rules and select the 'Group into a Policy' menu item. Store July Jet 300 Store Jet 30			

support@sniffa.uk





Sniffa Runbook Adding Snort[™] Rules to a Policies in the Sensor Manager Application

2	Add Using on clusted another Deline	
3.	Add Using an aiready created Policy.	Group rules into a Policy X
	Chose a policy from the drop down list.	Policy Name Adware
	Click on the button marked (Croup)	Create a new Policy name
	Click on the button marked Group .	Cancel Group
4.	Add Using a New Policy.	Group rules into a Policy ×
	Check the box marked 'Create a new Policy name'.	Policy Name
		Create a new Policy name
	Add a unique name for the new policy in the text	Cancel Group
	box marked Folicy Name .	
	Click on the button marked 'Group'.	
5.	Check for confirmation window.	×
		11 Rule(s) have been Grouped.
		ОК
C	To Domente miles from a Dollar	6969 SEXTER
б.	To Remove rules from a Policy.	5401:5402 SEXTERI
	Select the rules to remove from a Policy.	
	Dight Click the colorted rules and colort the	Clone
	'Ungroup from a Policy' menu item.	O Enable
		Disable
		Copy
		Sensor Whitelist
		Group into a Policy
		Ungroup from a Policy
		Signature Info
		Export Rules to File (.rules)





Sniffa Runbook Adding Snort™ Rules to a Policies in the Sensor Manager Application

7.	Chose a policy from the drop down list.	👔 Un-Group rules from a Policy 🛛 🗙
	Click on the button marked 'Un-Group'.	Policy Name Adware Cancel Un-Group
8.	Click on the button marked 'Yes' to proceed. Note: Click on the button marked 'No' to cancel.	Confirm Un-Group × ? Are you sure you want to remove the selected rules from the Policy Adware? Yes No
9.	Check for confirmation window.	K 6 Rule(s) have been Un-Grouped.
10.	End of Runbook.	