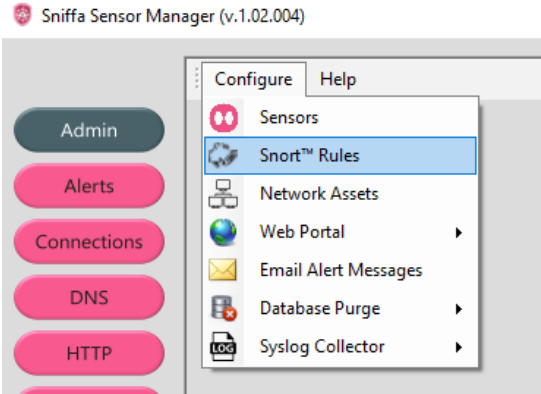
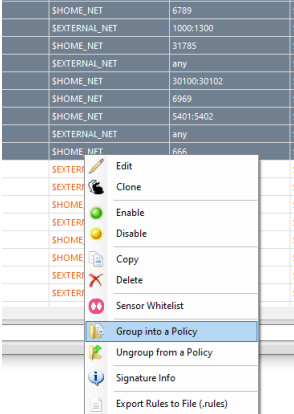


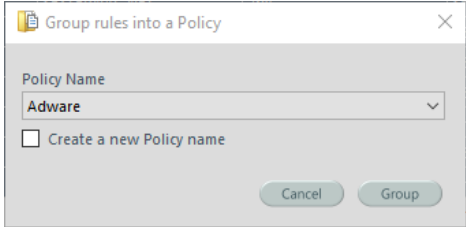
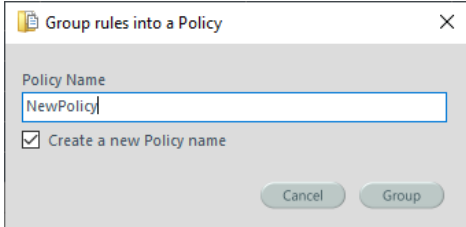
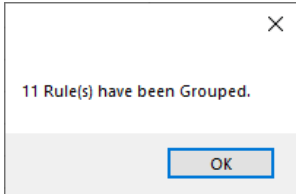
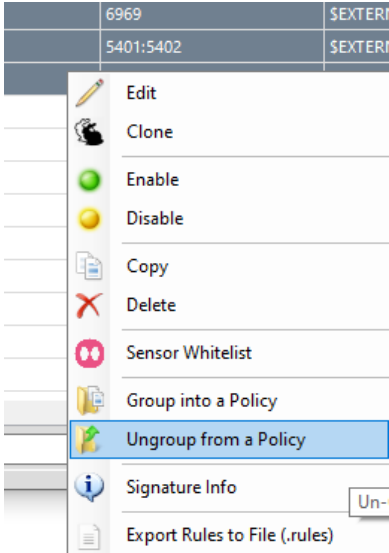
Sniffa Runbook

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

Serial	Instruction
	<p>Overview.</p> <p>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.</p> <p>1 or more Snort™ rules policies can be added to a Sensor’s configuration file and stored in the Sensor Manager Application database.</p> <p>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.</p> <p>Snort™ rules can be grouped into a rules policy in 4 ways:</p> <ul style="list-style-type: none"> • 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). <p>This runbook includes the tasks to be completed, to add Snort™ rules manually to a policy in the Sensor Manager Application.</p>
<p>1.</p>	<p>Go to the Admin panel. Select the ‘Configure’ menu item. Select the ‘Snort™ Rules’ menu item.</p> 
<p>2.</p>	<p>Select the rules to add to a Policy.</p> <p>Right Click the selected rules and select the ‘Group into a Policy’ menu item.</p> 

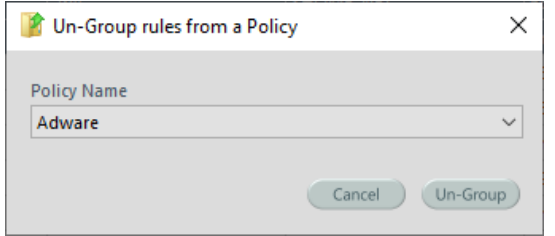
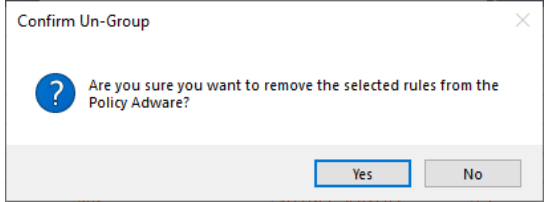
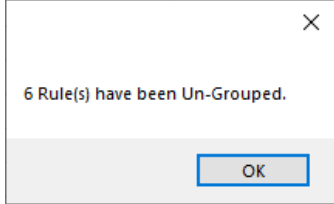
Sniffa Runbook

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

<p>3.</p>	<p>Add Using an already created Policy.</p> <p>Chose a policy from the drop down list.</p> <p>Click on the button marked 'Group'.</p>	
<p>4.</p>	<p>Add Using a New Policy.</p> <p>Check the box marked 'Create a new Policy name'.</p> <p>Add a unique name for the new policy in the text box marked 'Policy Name'.</p> <p>Click on the button marked 'Group'.</p>	
<p>5.</p>	<p>Check for confirmation window.</p>	
<p>6.</p>	<p>To Remove rules from a Policy.</p> <p>Select the rules to remove from a Policy.</p> <p>Right Click the selected rules and select the 'Ungroup from a Policy' menu item.</p>	

Sniffa Runbook

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

<p>7.</p>	<p>Chose a policy from the drop down list.</p> <p>Click on the button marked 'Un-Group'.</p>	
<p>8.</p>	<p>Click on the button marked 'Yes' to proceed.</p> <p><i>Note:</i> Click on the button marked 'No' to cancel.</p>	
<p>9.</p>	<p>Check for confirmation window.</p>	
<p>10.</p>	<p>End of Runbook.</p>	