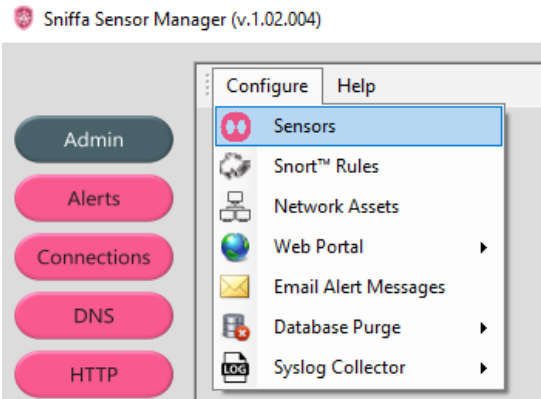
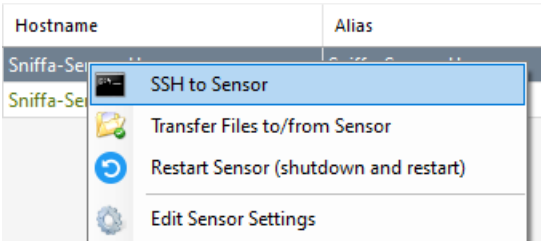
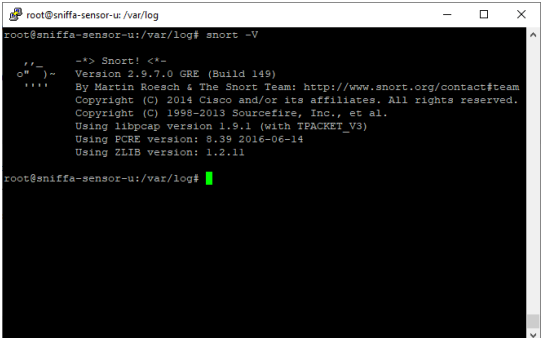
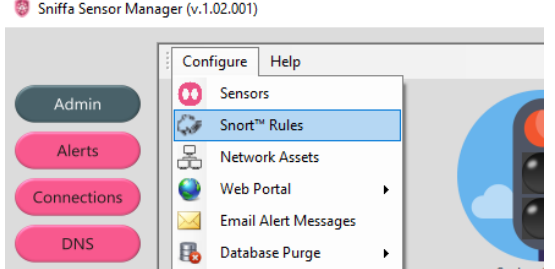
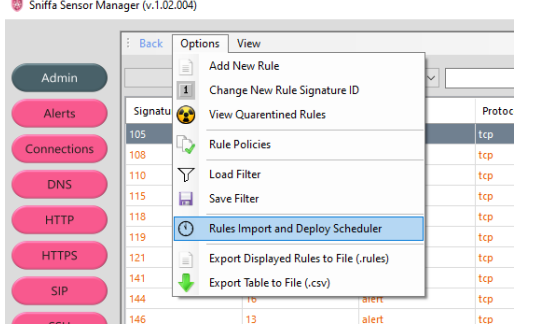
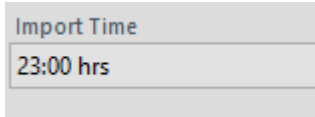


Sniffa Runbook Importing Snort™ Rules into the Sensor Manager Application

Serial	Instruction
	<p>Overview.</p> <p>Snort™ rules (.tar.gz) files can be imported from up to 3 remote locations using a valid Uniform Resource Locator (URL) and/or can be imported from a local rules directory on the host machine.</p> <p>Snort™ rules will be stored centrally in a database, ready to be added into rules policies and configured to be deployed to remote sensors on the network.</p> <p>This runbook includes the tasks needed to be completed, to configure the import scheduler to import Snort™ into the Sensor Manager Application at a regular time every 24 hours.</p>
<p>1.</p>	<p>Go to the Admin panel. Select the 'Configure' menu item. Select the 'Sensors' menu item.</p> 
<p>2.</p>	<p>Right click on a Sensor. Select 'SSH to Sensor' menu item.</p> 
<p>3.</p>	<p>Run Commands. <code># snort -V</code></p> <p>Take a note of the Snort™ version that is installed on the Sensor.</p> 

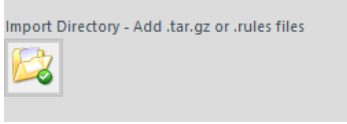
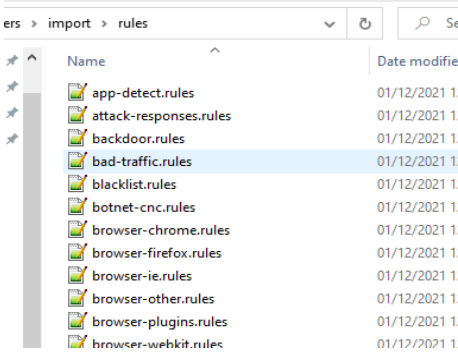
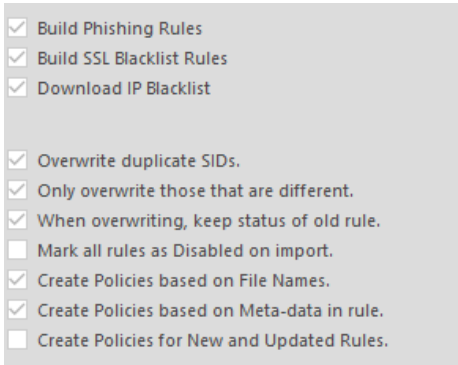


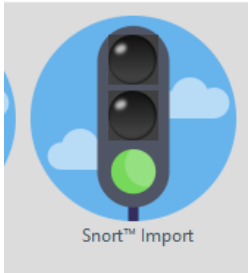
Sniffa Runbook

Importing Snort™ Rules into the Sensor Manager Application

<p>4.</p>	<p>Go to the Admin panel. Select the 'Configure' menu item. Select the 'Snort™ Rules' menu item.</p>	
<p>5.</p>	<p>Select 'Options' menu item. Select 'Rules Import and Deploy Scheduler' menu item.</p>	
<p>6.</p>	<p>Set the scheduled time for importing rules.</p> <p><i>Note:</i> To import Snort™ rules immediately, set the import time to 'Import Now'.</p> <p><i>'Import Now' is a one off task and will stop once all rules have been imported.</i></p>	

Sniffa Runbook

Importing Snort™ Rules into the Sensor Manager Application

<p>7.</p>	<p>Set to import from a local directory.</p> <p>Click on the Directory icon to open the local file import directory.</p> <p>Paste in any .rules files that need to be imported.</p> <p>Paste in any .tar.gz files that need to be imported.</p> <p><i>Note:</i> <i>Ensure the Snort™ version matches that noted in serial 3.</i></p> <p>Check to add Phishing Rules (optional).</p> <p>Check to build SSL Blacklist Rules (optional).</p> <p>Check to download Talos™ IP Blacklist (optional).</p> <p>Check all rules import options as required.</p>	  
<p>8.</p>	<p>Click on the Start button to start the Import Scheduler Service.</p>	
<p>9.</p>	<p>Click on the Pause button to stop the Import Scheduler Service at any time.</p>	
<p>10.</p>	<p>Go to the Admin panel.</p> <p>Check the status of the Snort™ Import traffic light.</p> <p><i>Note:</i> <i>Green light means Import Timer is running.</i> <i>Red light means Import Timer is stopped.</i></p>	
<p>11.</p>	<p>End of Runbook.</p>	