

## Sniffa Runbook Importing Snort™ Rules into the Sensor Manager Application

Serial	Instruction		
	Overview. Snort <sup>™</sup> 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. Snort <sup>™</sup> 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. This runbook includes the tasks needed to be completed, to configure the import scheduler to import Snort <sup>™</sup> into the Sensor Manager Application at a regular time every 24 hours.		
1.	Go to the Admin panel. Select the 'Configure' menu item. Select the 'Sensors' menu item.	<ul> <li>Sniffa Sensor Manager (v.1.02.004)</li> <li>Admin</li> <li>Alerts</li> <li>Connections</li> <li>DNS</li> <li>HTTP</li> <li>Collector</li> </ul>	
2.	Right click on a Sensor. Select 'SSH to Sensor' menu item.	Hostname     Alias       Sniffa-Set     SSH to Sensor       Sniffa-Set     Iransfer Files to/from Sensor       Image: Sensor Settings     Edit Sensor Settings	
3.	Run Commands. # snort -V Take a note of the Snort <sup>™</sup> version that is installed on the Sensor.	<pre>     root@sniffa-sensor-u:/var/log# snort -V     root@sniffa-sensor-u:/var/log# snort -V     ","*&gt; Snort! &lt;**     ","*&gt; 7.0 GEE (Build 149)     "''' By Martin Boesch &amp; The Snort Tram: http://www.anort.org/contact#         Copyright (C) 2014 Cinco and/or tht tgf:/lintes. All rights reser         Copyright (C) 2014 Cinco and/or tht tgf:/lintes. All rights reser         Copyright (C) 2014 Cinco and/or tht tgf:/lintes. All rights reser         Copyright (C) 2014 Cinco and/or tht tgf:/lintes. All rights reser         Copyright (C) 2014 Cinco and/or tht tgf:/lintes. All rights reser         Copyright (C) 2014 Cinco and/or tht tgf:/lintes. All rights reser         Copyright (C) 2014 Cinco and/or tht tgf:/lintes. All rights reser         Copyright (C) 2014 Cinco and/or tht tgf:/lintes. All rights reser         Copyright (C) 2014 Cinco and/or tht tgf:/lintes. All rights reser         Copyright (C) 2014 Cinco and/or tht tgf:/lintes. All rights reser         Copyright (C) 2014 Cinco and/or tht tgf:/lintes. All rights reser         Copyright (C) 2014 Cinco and/or tht tgf:/lintes. All rights reser         Copyright (C) 2014 Cinco and/or tht tgf:/lintes. All rights reser         Copyright (C) 2014 Cinco and/or tht tgf:/lintes. All rights reser         Copyright (C) 2014 Cinco and/or the tgf:/lintes. All rights reser         Copyright (C) 2014 Cinco and/or the tgf:/lintes.         Copyright (C)</pre>	× ^





## Sniffa Runbook Importing Snort™ Rules into the Sensor Manager Application

4.	Go to the Admin panel. Select the 'Configure' menu item. Select the 'Snort™ Rules' menu item.	<ul> <li>Sniffa Sensor Manager (v.1.02.001)</li> <li>Admin         <ul> <li>Alerts</li> <li>Connections</li> <li>DNS</li> </ul> </li> <li>Final Alert Messages</li> <li>Database Purge</li> </ul>
5.	Select 'Options' menu item. Select 'Rules Import and Deploy Scheduler' menu item.	Shiffa Sensor Manager (v:1.02.004)          Admin       Back       Options       View         Admin       Add New Rule Signature ID       Protoc         Alerts       Signatu       Wew Quarentined Rules Signature ID       Protoc         Intro       Disinatu       Wew Quarentined Rules       top         Intro       Disinatu       Wew Quarentined Rules       top         Intro       Load Filter       top       top         Intro       Rules Import and Deploy Scheduler       top       top         Intro       Rules Import and Deploy Scheduler       top       top         Intro       Intro       Intro       top
6.	Set the scheduled time for importing rules. Note: To import Snort™ rules immediately, set the import time to 'Import Now'. 'Import Now' is a one off task and will stop once all rules have been imported.	Import Time 23:00 hrs



## Sniffa Runbook Importing Snort™ Rules into the Sensor Manager Application

7.	Set to import from a local directory.	Import Directory - Add .tar.gz or .rules files
	Click on the Directory icon to open the local file import directory.	
	Paste in any .rules files that need to be imported.	ers → import → rules v ७
	Paste in any .tar.gz files that need to be imported.	Image: Second
	Note: Ensure the Snort™ version matches that noted in serial 3.	Bit operation         Bit operation         Bit operation           Bit operation         01/12/2021 1.         01/12/2021 1.
	Check to add Phishing Rules (optional).	image: browser-other.rules         01/12/2021 1.           image: browser-plugins.rules         01/12/2021 1.           image: browser-webkit.rules         01/12/2021 1.
	Check to build SSL Blacklist Rules (optional).	
	Check to download Talos™ IP Blacklist (optional).	Build Phishing Rules     Build SSL Blacklist Rules     Download IP Blacklist
	Check all rules import options as required.	
		<ul> <li>Only overwrite those that are different.</li> </ul>
		When overwriting, keep status of old rule.
		<ul> <li>Mark an rules as Disabled on hipport.</li> <li>Create Policies based on File Names.</li> </ul>
		Create Policies based on Meta-data in rule.
		Create Policies for New and Updated Rules.
8.	Click on the Start button to start the Import	
9.	Click on the Pause button to stop the Import Scheduler Service at any time.	
10.	Go to the Admin panel.	
	Check the status of the Snort™ Import traffic light.	
	Note: Green light means Import Timer is running. <mark>Red light</mark> means Import Timer is stopped.	Snort <sup>™</sup> Import
11.	End of Runbook.	