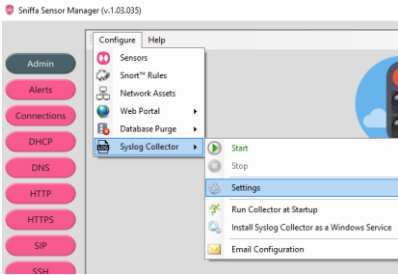
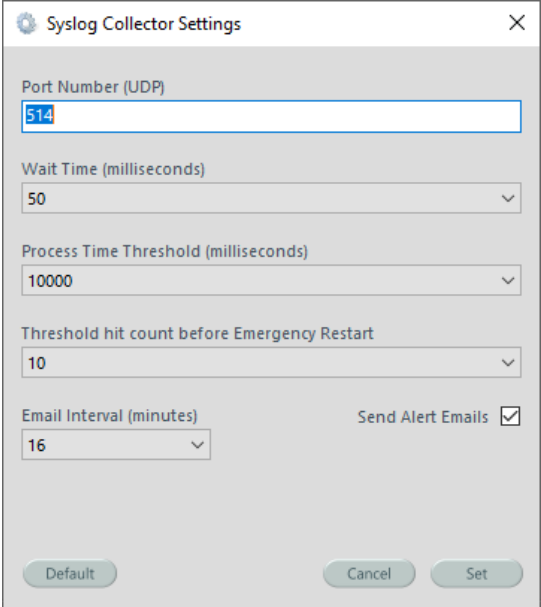
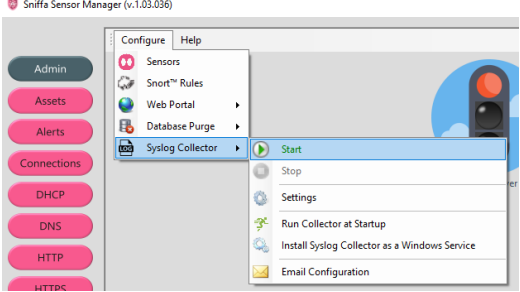
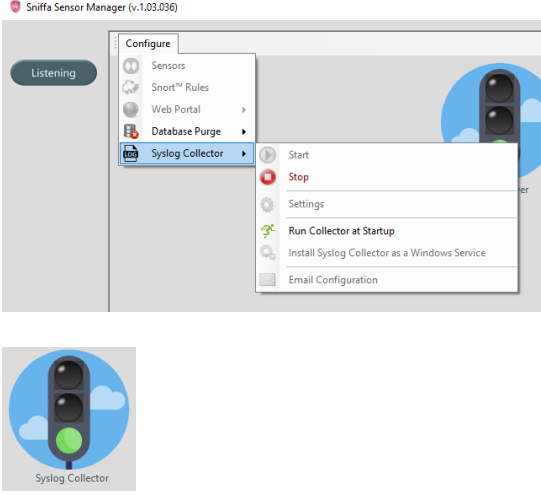
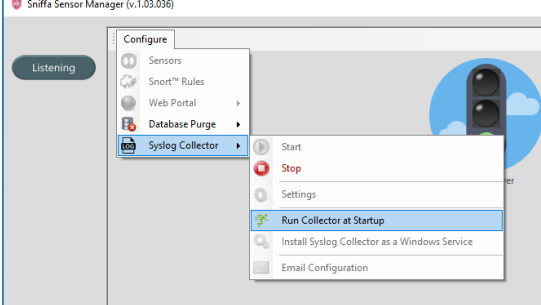
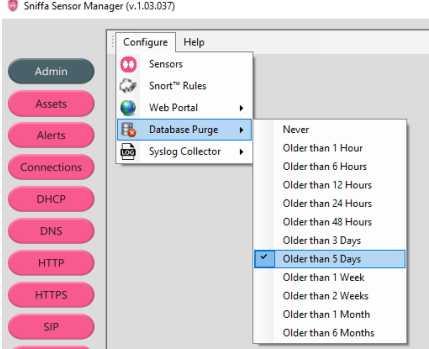


Sniffa Runbook

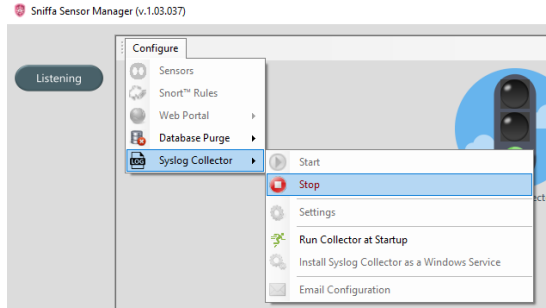
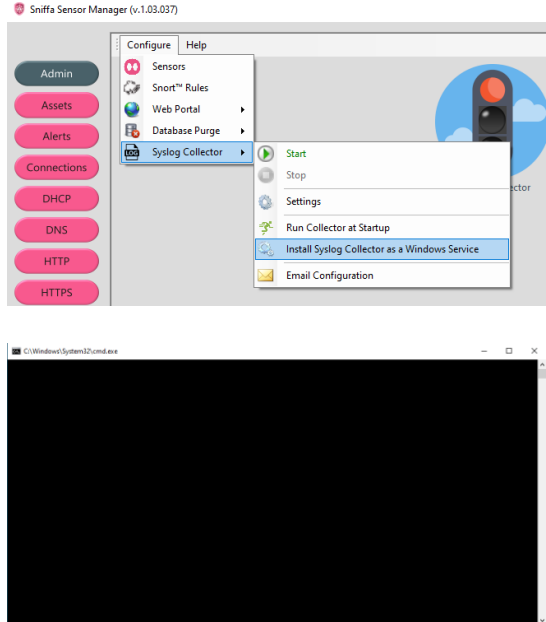
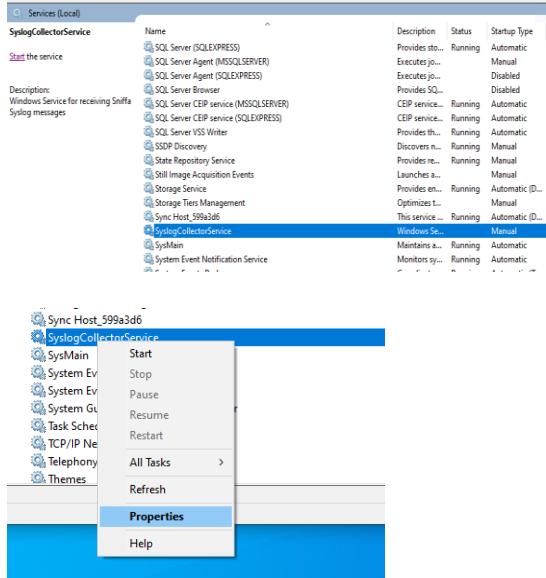
Running the Syslog Collector

Serial	Instruction
	<p>Overview.</p> <p>The Sensor Manager Application will receive log and alert messages from the remote Sensors using the Syslog Protocol. The messages are collected by the Sensor Manager Application and fed into the database to form an ordered and structured dataset.</p> <p>The Syslog Collector operation can be run directly from the Sensor Manger Application or it can be installed and run as a Microsoft™ Windows Service. The advantage of having the Syslog Collector running as a Microsoft™ Windows Service, is that it can operate in the background and be configured to re-start automatically at the same time as the local host machine. This might be referred to as running in ‘Headless’ mode.</p> <p><i>Note:</i> <i>Only a single instance of the Syslog Collector can be running on a host computer at any one time and the Syslog Collector Service will only feed a single database at any one time.</i></p> <p><i>However, you can have several Syslog Collectors feeding a single database, or you can run several Syslog Collectors that will feed multiple databases at the same time. The deployment architecture can be flexible to fit your environment.</i></p>
<p>1.</p>	<p>Syslog Settings.</p> <p>Go to the Admin panel. Select the ‘Configure’ menu item. Select the ‘Syslog Collector’ menu item. Select the ‘Settings’ menu item.</p> 
<p>2.</p>	<p>Set the UDP Listening Port Number to the required value between 0 and 65353.</p> <p>Check or un-check the box marked ‘Send Alert Emails’, depending on your requirement and set the required email interval (in minutes).</p> <p><i>Note: It is recommended to leave the other settings at the default value.</i></p> <p><i>Only change those settings with the guidance of the Sniffa Support Team.</i></p> <p>To reset back to the default values, click on the button marked ‘Default’.</p> <p>To save settings, click on the button marked ‘Set’.</p> 

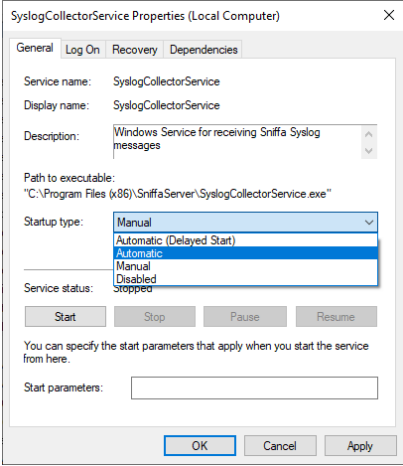
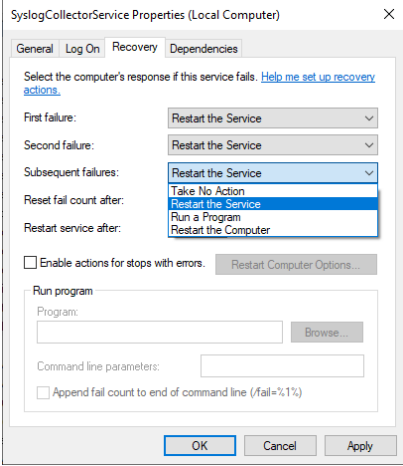
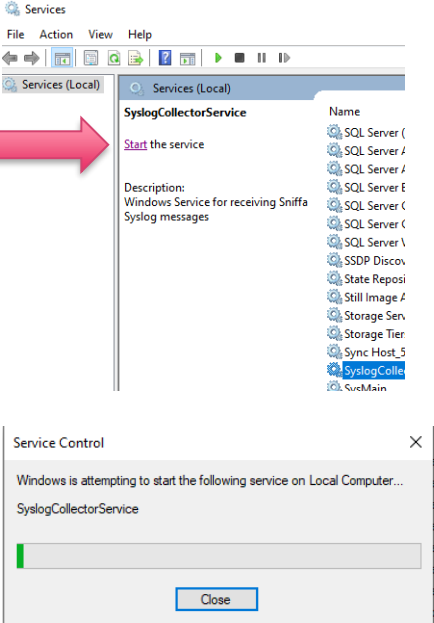
Sniffa Runbook Running the Syslog Collector

<p>3.</p>	<p>Starting the Syslog Collector from the Application.</p> <p>Go to the Admin panel. Select the 'Configure' menu item. Select the 'Syslog Collector' menu item. Select the 'Start' menu item.</p>	
<p>4.</p>	<p>Whilst the Syslog Collector is running, you will notice that some of the menu items will be disabled and the protocol buttons on the left-hand side will be removed.</p> <p>The traffic light image marked 'Syslog Collector' will show green.</p> <p><i>Note:</i> You will not be able to search the protocol tables or configure the IDS rules policies whilst the Syslog Collector is running.</p>	
<p>5.</p>	<p>The Syslog Collector can be configured to run immediately as the Sensor Manager Application opens. This is useful when an unexpected crash is encountered and the Sensor Manager Watchdog restarts the application.</p> <p>Go to the Admin panel. Select the 'Configure' menu item. Select the 'Syslog Collector' menu item. Select the 'Run Collector at Startup' menu item.</p>	
<p>6.</p>	<p>You can configured the Syslog Collector to purge logs from the database, prior to a set point in time.</p> <p><i>Note:</i> This will not include Alert logs, which can be archived and deleted manually from the Alerts Panel.</p> <p>Go to the Admin panel. Select the 'Configure' menu item. Select the 'Database Purge' menu item.</p>	

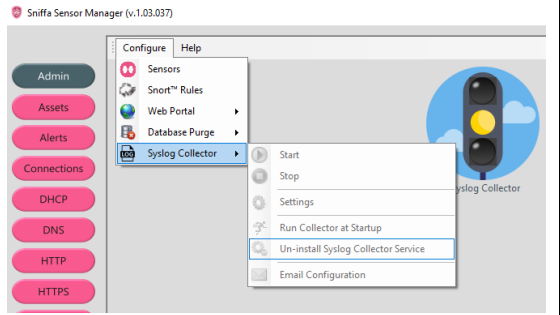
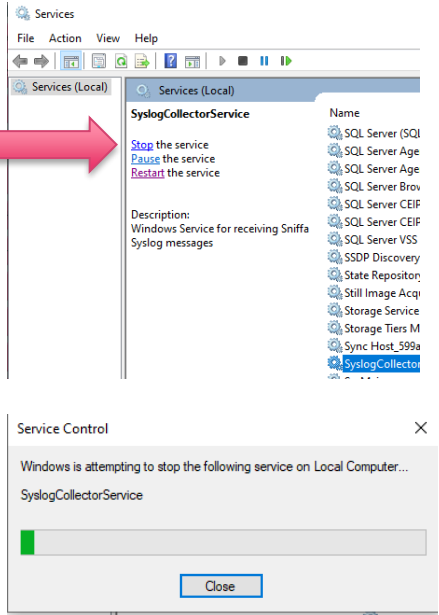
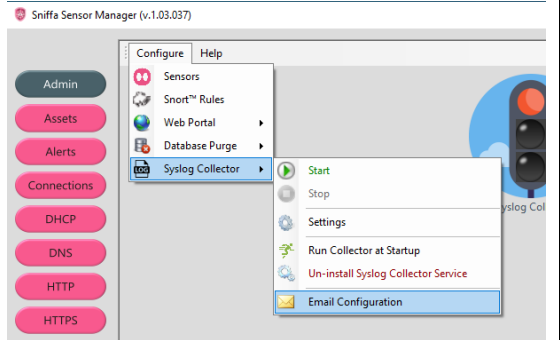
Sniffa Runbook Running the Syslog Collector

<p>7.</p>	<p>Stopping the Syslog Collector from the Application.</p> <p>Go to the Admin panel. Select the 'Configure' menu item. Select the 'Syslog Collector' menu item. Select the 'Stop' menu item.</p>	
<p>8.</p>	<p>Installing the Syslog Collector as a Service.</p> <p>Go to the Admin panel. Select the 'Configure' menu item. Select the 'Syslog Collector' menu item. Select the 'Install Syslog Collector as a Windows Service' menu item.</p> <p>You should see a command window pop-up briefly as the Windows Service is being installed onto the computer.</p> <p><i>Note:</i> <i>The Sensor Manager Application must be run with Administrator privileges for the Windows Service to be installed correctly.</i></p>	
<p>9.</p>	<p>After the Syslog Collector Service has been installed, you should see the 'Services' window appear on your screen.</p> <p>Scroll down the page and ensure that you can see the 'SyslogCollectorService' in the list.</p> <p>Right click on the 'SyslogCollectorService' and select the properties menu item.</p>	

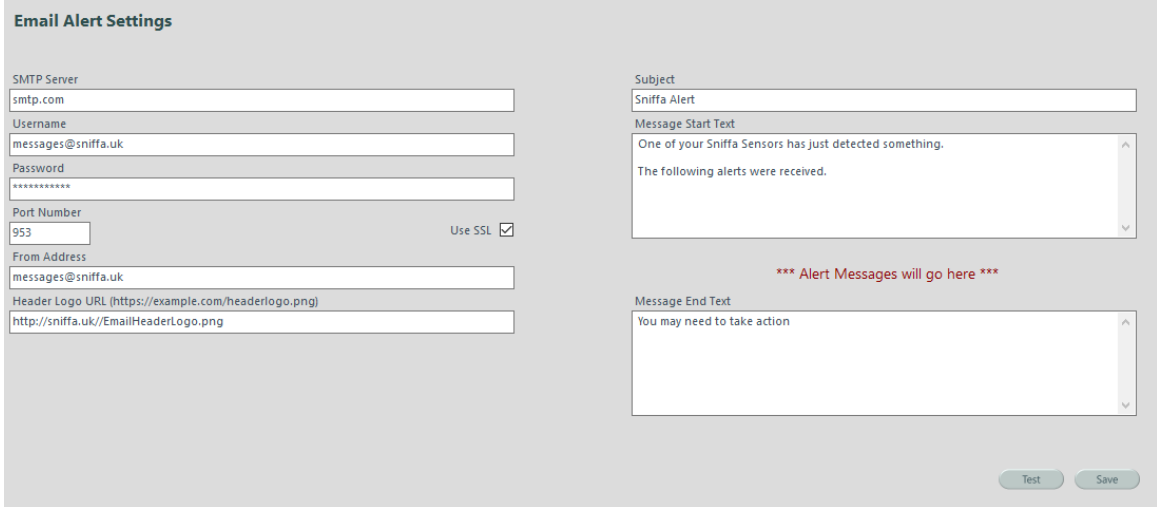

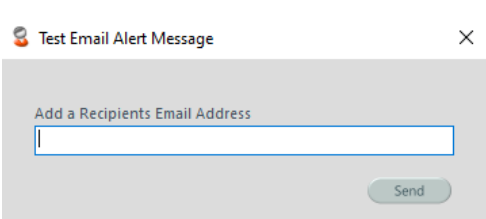
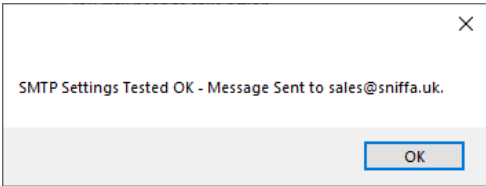

Sniffa Runbook Running the Syslog Collector

<p>10.</p>	<p>Go to the 'General' tab.</p> <p>Select the 'Startup type' setting from the drop down menu, depending on your requirements.</p>	
<p>11.</p>	<p>Go to the 'Recovery' tab.</p> <p>Select the First, Second and Subsequent failure settings from the drop down menus, depending on your requirements.</p> <p>Click on the button marked 'OK' to save your settings.</p>	
<p>12.</p>	<p>Starting the Syslog Collector Service</p> <p>Select the 'SyslogCollectorService' from the list.</p> <p>Click on the button marked 'Start'.</p> <p>The service should take approximately 5 to 10 seconds to start.</p>	

Sniffa Runbook Running the Syslog Collector

<p>13.</p>	<p>Whilst the Syslog Collector is running as a Windows Service, you will not be able to change any of the Syslog Collector settings from the Sensor Manager Application.</p> <p>If you want to change any of the Syslog Collector settings, you will need to stop the Syslog Collector Windows Service first.</p> <p><i>Note:</i> You will see an Amber Lamp showing on the traffic light whilst the Syslog Collector is running as a Windows Service.</p>	
<p>14.</p>	<p>Stopping the Syslog Collector Service</p> <p>Select the 'SyslogCollectorService' from the list.</p> <p>Click on the button marked 'Stop'.</p> <p>The service should take approximately 5 to 10 seconds to stop.</p>	
<p>15.</p>	<p>Email Settings.</p> <p>If you want to have Alerts sent by email whilst the Syslog Collector is running, you will need to configure an Email Server to send the messages first.</p> <p>Go to the Admin panel. Select the 'Configure' menu item. Select the 'Syslog Collector' menu item. Select the 'Email Configuration' menu item.</p>	

Sniffa Runbook Running the Syslog Collector

<p>16.</p>	<p>Enter the details for your Email Server.</p> 
<p>17.</p>	<p>To test your settings, click on the button marked 'Test'.</p>  <p>Enter a valid email address and click on the button marked 'Send'.</p> <p>You should see a message to say the Test Message has been send correctly.</p>  
<p>18.</p>	<p>To save the Email Settings, click on the button marked 'Save'.</p> 
<p>19.</p>	<p>End or Runbook.</p>