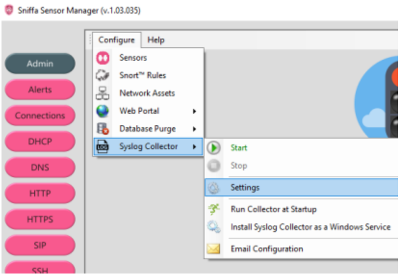
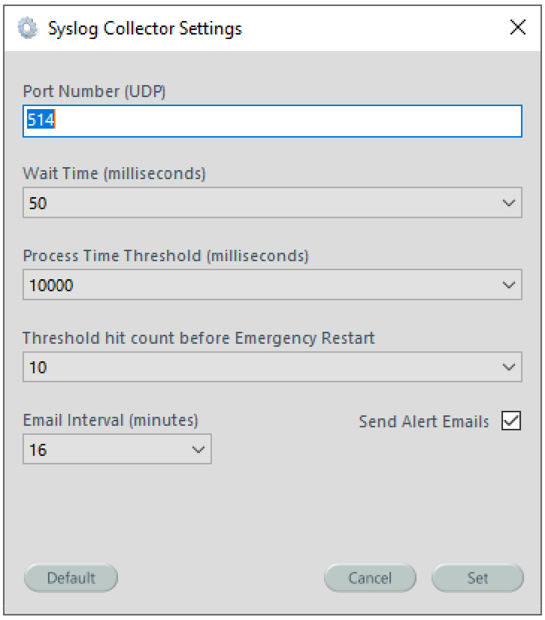
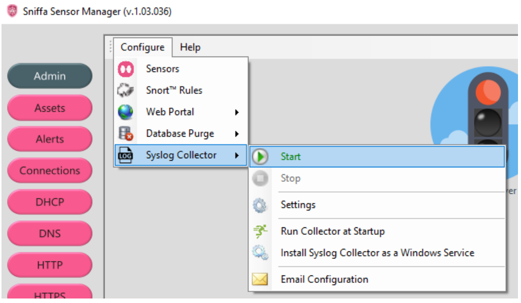
Sniffa Runbook
Running the Syslog Collector

Serial	Instruction
	Overview. 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. 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. *Note:* *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.* *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.*
1.	**Syslog Settings.** Go to the Admin panel. Select the 'Configure' menu item. Select the 'Syslog Collector' menu item. Select the 'Settings' menu item.  Sniffa Sensor Manager (v.1.03.035) Admin Alerts Connections DHCP DNS HTTP HTTPS SIP SSH Configure Help Sensors Snort™ Rules Network Assets Web Portal Database Purge Syslog Collector Start Stop Settings Run Collector at Startup Install Syslog Collector as a Windows Service Email Configuration
2.	Set the UDP Listening Port Number to the required value between 0 and 65353. Check or un-check the box marked 'Send Alert Emails', depending on your requirement and set the required email interval (in minutes). *Note: It is recommended to leave the other settings at the default value.* *Only change those settings with the guidance of the Sniffa Support Team.* To reset back to the default values, click on the button marked 'Default'. To save settings, click on the button marked 'Set'.  Syslog Collector Settings Port Number (UDP): 514 Wait Time (milliseconds): 50 Process Time Threshold (milliseconds): 10000 Threshold hit count before Emergency Restart: 10 Email Interval (minutes): 16 Send Alert Emails ☑

3. **Starting the Syslog Collector from the Application.**

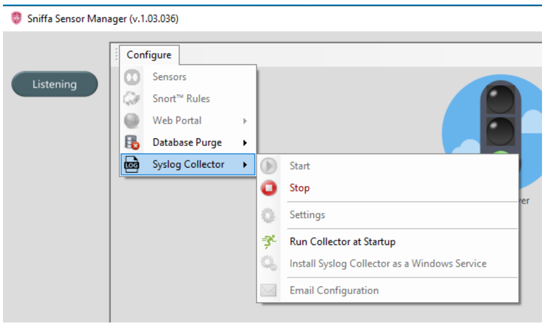
Go to the Admin panel.
Select the ‘Configure’ menu item.
Select the ‘Syslog Collector’ menu item.
Select the ‘Start’ menu item.

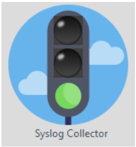


4. Whilst the Syslog Collector is running, you will notice that some of the menu items will be disabled and the protocol buttons on the left-hand side will be removed.

The traffic light image marked ‘Syslog Collector’ will show green.

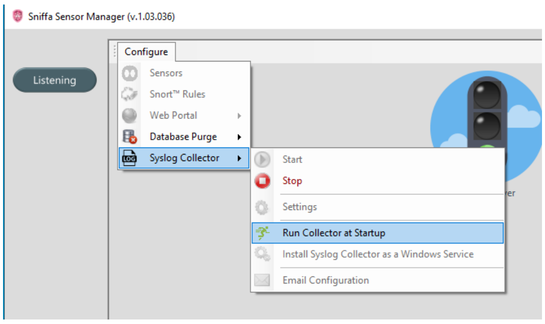
Note:
You will not be able to search the protocol tables or configure the IDS rules policies whilst the Syslog Collector is running.





5. 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.

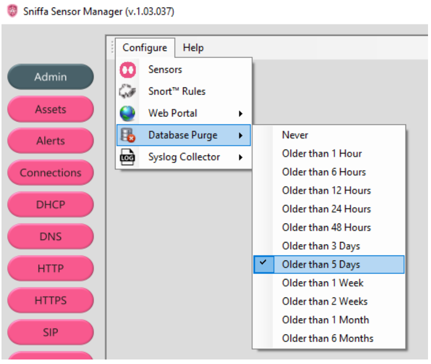
Go to the Admin panel.
Select the ‘Configure’ menu item.
Select the ‘Syslog Collector’ menu item.
Select the ‘Run Collector at Startup’ menu item.



6. You can configured the Syslog Collector to purge logs from the database, prior to a set point in time.

Note:
This will not include Alert logs, which can be archived and deleted manually from the Alerts Panel.

Go to the Admin panel.
Select the ‘Configure’ menu item.
Select the ‘Database Purge’ menu item.

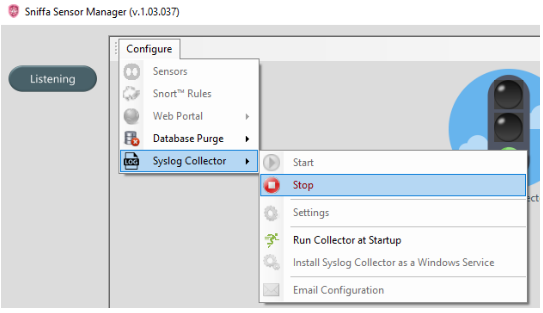


Sniffa Runbook
Running the Syslog Collector

7.

Stopping the Syslog Collector from the Application.

Go to the Admin panel.
Select the 'Configure' menu item.
Select the 'Syslog Collector' menu item.
Select the 'Stop' menu item.



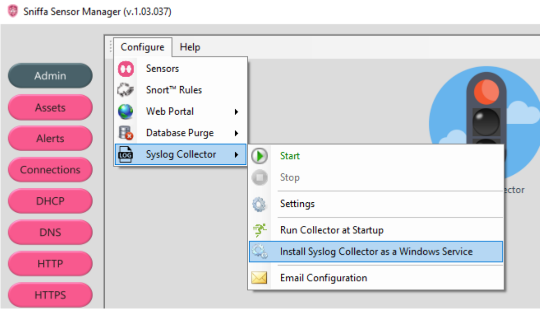
8.

Installing the Syslog Collector as a Service.

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.

You should see a command window pop-up briefly as the Windows Service is being installed onto the computer.

Note:
The Sensor Manager Application must be run with Administrator privileges for the Windows Service to be installed correctly.

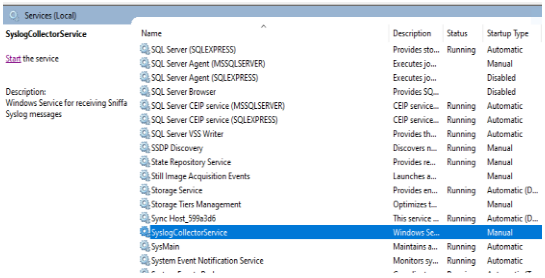


9.

After the Syslog Collector Service has been installed, you should see the 'Services' window appear on your screen.

Scroll down the page and ensure that you can see the 'SyslogCollectorService' in the list.

Right click on the 'SyslogCollectorService' and select the properties menu item.

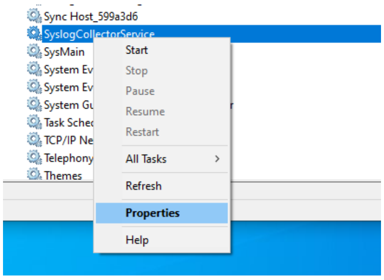


SyslogCollectorService

Start the service

Description:
Windows Service for receiving Sniffa Syslog messages

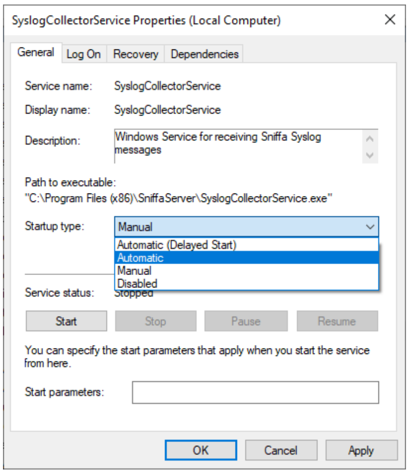
Name	Description	Status	Startup Type
SQL Server (SQLEXPRESS)	Provides sto...	Running	Automatic
SQL Server Agent (MSSQLSERVER)	Executes jo...		Manual
SQL Server Agent (SQLEXPRESS)	Executes jo...		Disabled
SQL Server Browser	Provides SQ...		Disabled
SQL Server CEIP service (MSSQLSERVER)	CEIP service...	Running	Automatic
SQL Server CEIP service (SQLEXPRESS)	CEIP service...	Running	Automatic
SQL Server VSS Writer	Provides th...	Running	Automatic
SSDP Discovery	Discovers n...	Running	Manual
State Repository Service	Provides re...	Running	Manual
Still Image Acquisition Events	Launches a...		Manual
Storage Service	Provides en...	Running	Automatic (D...
Storage Tiers Management	Optimizes t...		Manual
Sync Host_599a3d6	This service ...	Running	Automatic (D...
SyslogCollectorService	Windows Se...		Manual
SysMain	Maintains a...	Running	Automatic
System Event Notification Service	Monitors sy...	Running	Automatic



10.

Go to the ‘General’ tab.

Select the ‘Startup type’ setting from the drop down menu, depending on your requirements.



SyslogCollectorService Properties (Local Computer)

Service name: SyslogCollectorService

Display name: SyslogCollectorService

Description: Windows Service for receiving Sniffa Syslog messages

Path to executable:
"C:\Program Files (x86)\SniffaServer\SyslogCollectorService.exe"

Startup type: Manual

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

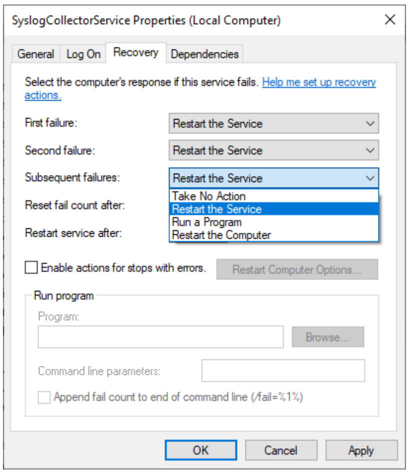
Start parameters:

11.

Go to the ‘Recovery’ tab.

Select the First, Second and Subsequent failure settings from the drop down menus, depending on your requirements.

Click on the button marked ‘OK’ to save your settings.



SyslogCollectorService Properties (Local Computer)

Select the computer's response if this service fails. Help me set up recovery actions.

First failure: Restart the Service

Second failure: Restart the Service

Subsequent failures: Restart the Service

Reset fail count after:

Restart service after:

☐ Enable actions for stops with errors.

Run program

Program:

Command line parameters:

☐ Append fail count to end of command line (/fail=%1%)

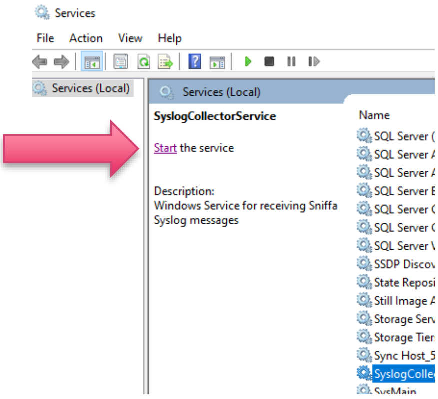
12.

Starting the Syslog Collector Service

Select the ‘SyslogCollectorService’ from the list.

Click on the button marked ‘Start’.

The service should take approximately 5 to 10 seconds to start.

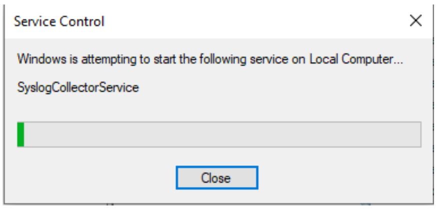


Services

SyslogCollectorService

Start the service

Description:
Windows Service for receiving Sniffa Syslog messages



Service Control

Windows is attempting to start the following service on Local Computer...

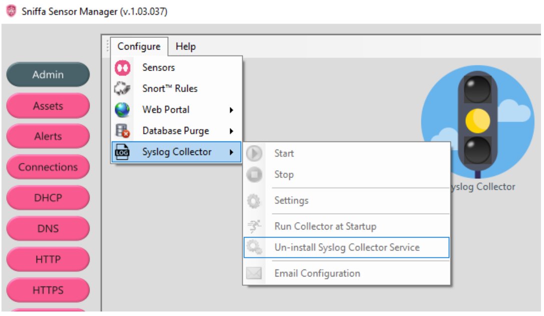
SyslogCollectorService

13.

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.

If you want to change any of the Syslog Collector settings, you will need to stop the Syslog Collector Windows Service first.

Note:
You will see an Amber Lamp showing on the traffic light whilst the Syslog Collector is running as a Windows Service.



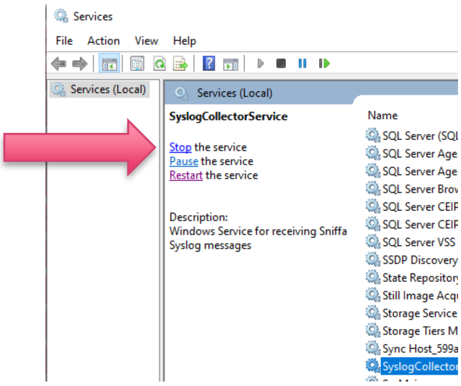
14.

Stopping the Syslog Collector Service

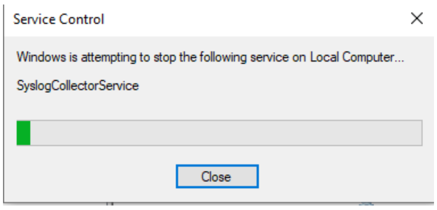
Select the ‘SyslogCollectorService’ from the list.

Click on the button marked ‘Stop’.

The service should take approximately 5 to 10 seconds to stop.



Description:
Windows Service for receiving Sniffa Syslog messages



Windows is attempting to stop the following service on Local Computer...

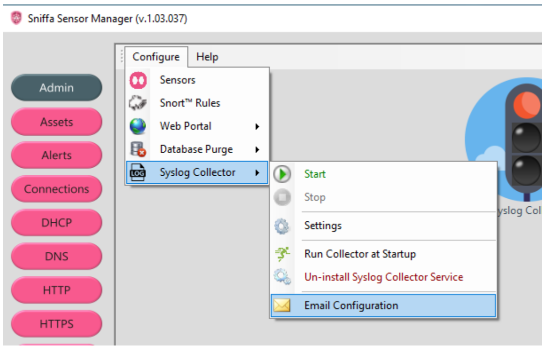
SyslogCollectorService

15.

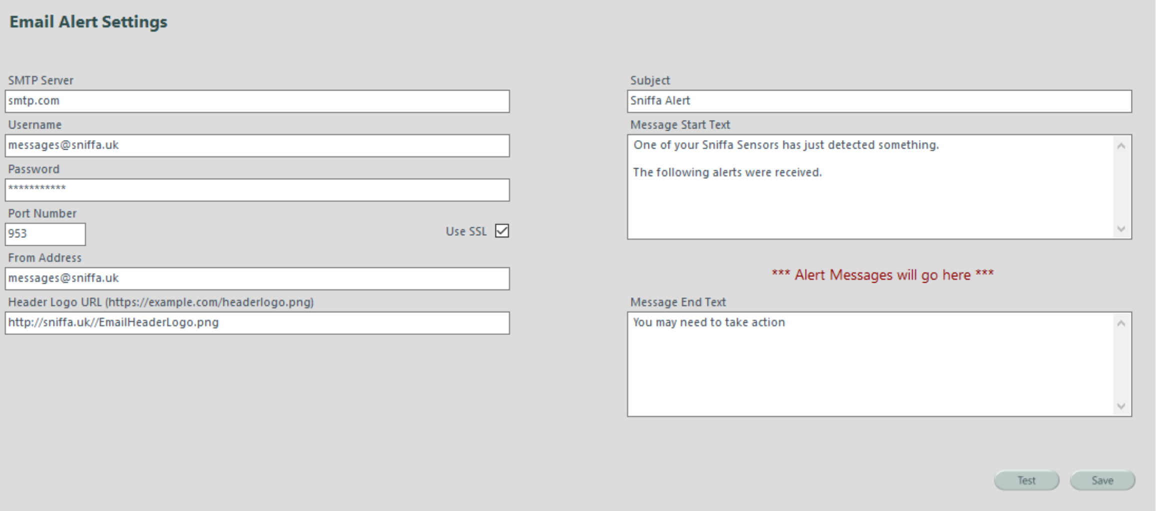
Email Settings.

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.

Go to the Admin panel.
Select the ‘Configure’ menu item.
Select the ‘Syslog Collector’ menu item.
Select the ‘Email Configuration’ menu item.



16. Enter the details for your Email Server.



Email Alert Settings

SMTP Server: smtp.com

Username: messages@sniffa.uk

Password: ***********

Port Number: 953

Use SSL ☑

From Address: messages@sniffa.uk

Header Logo URL (https://example.com/headerlogo.png): http://sniffa.uk//EmailHeaderLogo.png

Subject: Sniffa Alert

Message Start Text: One of your Sniffa Sensors has just detected something.

The following alerts were received.

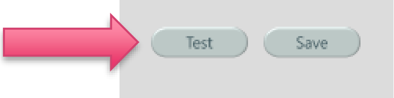
*** Alert Messages will go here ***

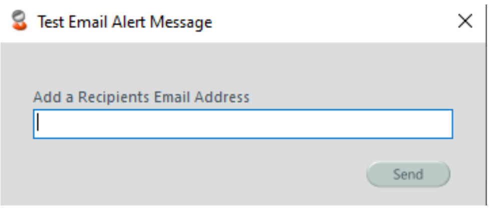
Message End Text: You may need to take action

17. To test your settings, click on the button marked ‘Test’.

Enter a valid email address and click on the button marked ‘Send’.

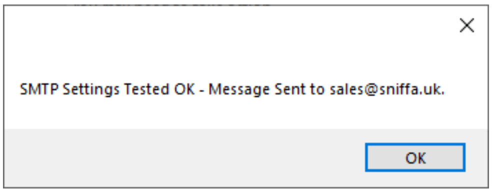
You should see a message to say the Test Message has been send correctly.





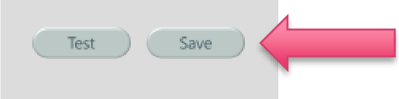
Test Email Alert Message

Add a Recipients Email Address



SMTP Settings Tested OK - Message Sent to sales@sniffa.uk.

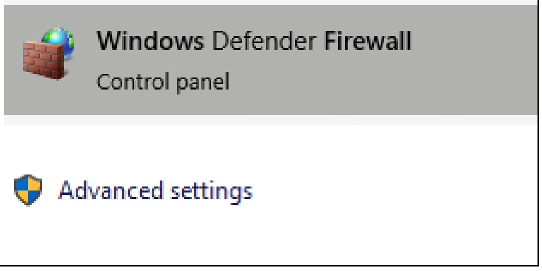
18. To save the Email Settings, click on the button marked ‘Save’.

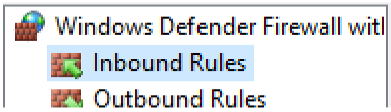
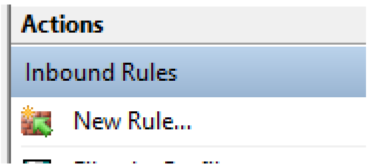
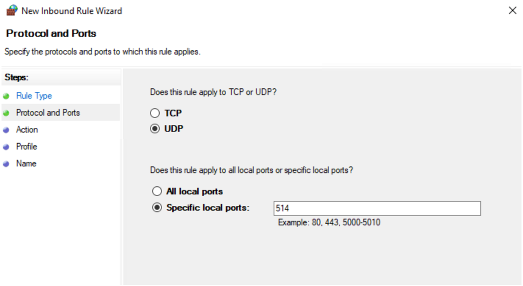


19. **Firewall Settings.**

Open Windows Defender Firewall from the Windows Start Menu.

Click on the Menu Item marked ‘Advance settings’ from the left hand menu.



20.	Select ‘Inbound Rules’ from the left hand menu. Select ‘New Rule…’ from the right hand menu.	 Windows Defender Firewall witl Inbound Rules Outbound Rules 
21.	Add a new rule to allow port UDP 514. Give the rule a unique name and click the button marked ‘Finish’ to save and enable the rule.	 New Inbound Rule Wizard **Protocol and Ports** Specify the protocols and ports to which this rule applies. Steps: Rule Type, Protocol and Ports, Action, Profile, Name Does this rule apply to TCP or UDP? ○ TCP ● UDP Does this rule apply to all local ports or specific local ports? ○ All local ports ● Specific local ports: 514 Example: 80, 443, 5000-5010
22.	End or Runbook.	