User Manual: NeoSyslog Collector

Version 1.0

	Author	Reviser
Name	Dave Dufour	Cyril Gambini
Company	Neosoft Technologies	Neosoft Technologies

Confidentiality

This document prepared for the plugin users contains proprietary material and confidential information at Neosoft Technologies. Plugin users agree to treat this information confidentially and not disclose it to a third party.

Neosoft Technologies Inc.
1009 Route de l'Eglise, bureau 405
Québec, QC G1V 3V7

Neosoft Technologies Inc.
4800 rue de Rouen, suite 230
Montréal, QC H1V 3T4

Toll-free: 1-866-636-7381
Tel :(418) 948-8324
Fax : (418) 948-8325
https://www.neosoft.ca/en/home/

DOCUMENT HISTORY

Version	Date	Author	Modification
1.0.0	17/03/2020	Dave Dufour	Creation of the document
1.0.1	29/04/2020	Cyril Gambini	Added information about firewalls and supported OS

CONTENTS

1 Purpose of This Document 5
2 General Description 5
2.1 Supported operating system 5
2.2 Firewall and network rules 5
3 Features 6
3.1 Live Module 6
3.1.1 Live SysLog Table 6
3.1.2 Pause Live Table button 7
3.1.3 Clear Tables button 7
3.1.4 Last Value Table (paid license only) 7
3.1.4.1 Display Row 7
3.1.4.2 Graph Values 8
3.2 Post Mortem Module (paid license only) 9
3.3 Menu Bar 10
3.3.1 File 10
3.3.2 Preferences 10
3.3.3 Help 11

1 Purpose of This Document

The purpose of this document is to describe how to use NeoSyslog Collector application. It will be explained how to prepare, configure, parameterize, visualize and exploit the software.

2 General Description

The NeoSyslog Collector collects Syslog messages based on the specification RFC3164. It is a Syslog server (or collector) and can receive data from many clients. It is possible to receive data on UDP and/or TCP ports.

The purpose of the application is to provide an intuitive interface to clearly expose the received Syslog messages and efficiently process them.

Two licences are available on NeoSyslog Collector: the free one and the paid one. The differences between the two licences are highlighted in the following table.

Features	Free	Paid
Live monitoring	✓	✓
Access to the configurations	✓	✓
Last value monitoring	✗	✓
Database recording	✗	✓
Database reading	✗	✓
Database searching	✗	✓
Export data files	✗	✓
Import data files	✗	✓
Print data	✗	✓

With the paid licence, all the data is recorded in an internal database. This provides the ability to do post analysis by querying the database from Post-mortem interface.

Those features will be detailed below.

2.1 Supported operating system

NeoSyslog Collector is a software program intended to be used on Windows platforms only (Windows 7 and above).

However, it can receive Syslog messages from any targets running any OS as long as the messages are compliant to RFC3164 format.

2.2 Firewall and network rules

NeoSyslog Collector listen on UDP (default: 514) and TCP (default: 601) ports.

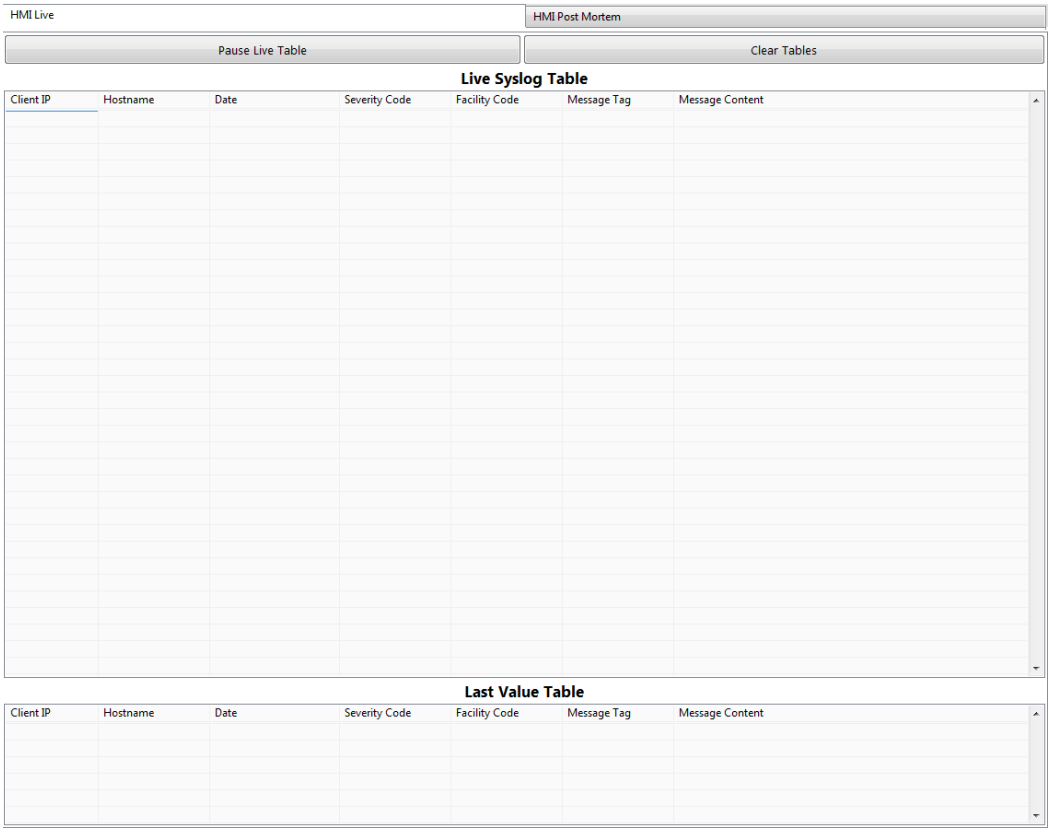
Therefore, according to you IT security rules, these ports or the entire application may be added as exceptions into your firewall settings.

If Syslog clients are pushing messages to the server but nothing appears in the live view, ensure that the firewall settings are correct.

3 Features

3.1 Live Module

This is the main module of the application. In this interface, the user will be able to see all the messages sent by the Syslog client(s) in real time (live).



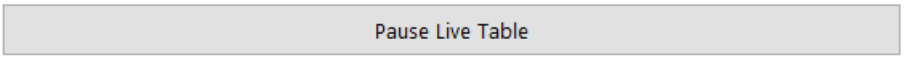
3.1.1 Live SysLog Table

This table contains all messages received by the collector in real time. Those messages are parse and shown by column to help the user see the information.

Here is a description of each column:

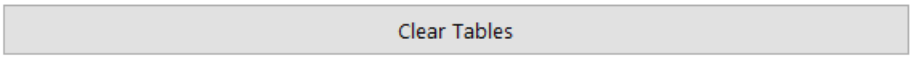
Client IP: IP address of the client sending the message
Hostname: Hostname of the client sending the message
Date: Date of the message in this format: Year Month Day HH:MM:SS. It is also possible to include milliseconds depending of the Syslog client library used.
Severity Code: Severity of the message sent. Per the Syslog standard, when sending the message, the client can specify the message's severity and NeoSyslog Collector will parse that information to display it appropriately.
Facility Code: The facility code specifies the program that is sending the message.
Message Tag: Represents the tag of the message. It can be anything and is defined by the client sending the Syslog message. For example, if the user wants to send a message during the initialization, the tag could be name "Init".
Message Content: Represents the content of the Syslog message. It can be anything the user wants it to be **but needs to be within a message size of less than 5 000 bytes (client's IP address and hostname included).**

3.1.2 Pause Live Table button



With this button, the user can pause the live table update while still receiving messages that will be later displayed after the button is click again.

3.1.3 Clear Tables button

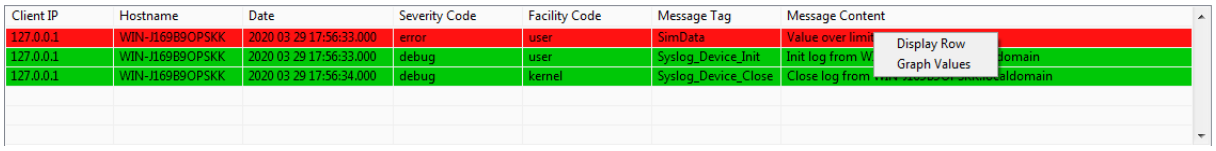


With this button, the user can clear the table's data. The data showed in the "Last Value Table" will also be deleted. It you have the paid licence; all the data remains saved in the internal database.

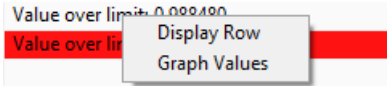
3.1.4 Last Value Table (paid license only)

This table contains the last message received that has the same IP, Host Name, Severity, Facility and Tag. Every unique message will appear in this table, but only the last one will be shown. That way, the user is able to clearly see the most recent messages of a client without having to monitor the Live Syslog table. It is also possible to right click on the row to show a sub-menu that lets a user choose to display the data in a graph or a row.

Last Value Table

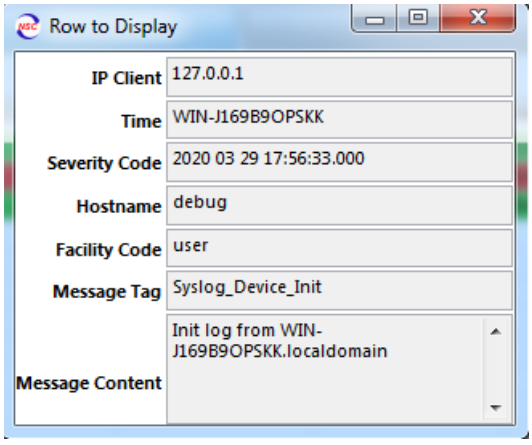


A zoom on the right-click sub-menu is shown here:



3.1.4.1 Display Row

Selecting "Display Row" will open a new window where the user will be able to see the whole message in a separate window to make it easier to see the message content.

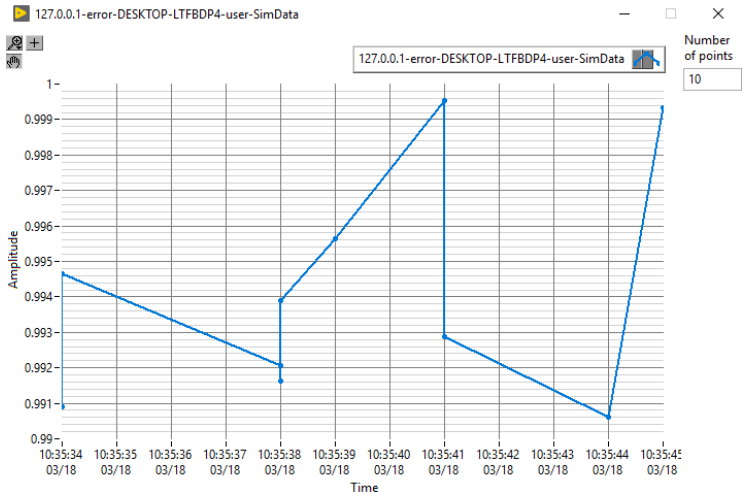


3.1.4.2 Graph Values

Selecting "Graph Values" will open a new window with a graph that shows the data and will update the graph as new messages are received. **Note that the Collector must be running!**

It is possible to change the settings of the graph by clicking on the signal legend.

Also, the number of points to graph can be set directly from the interface as shown on this next image.

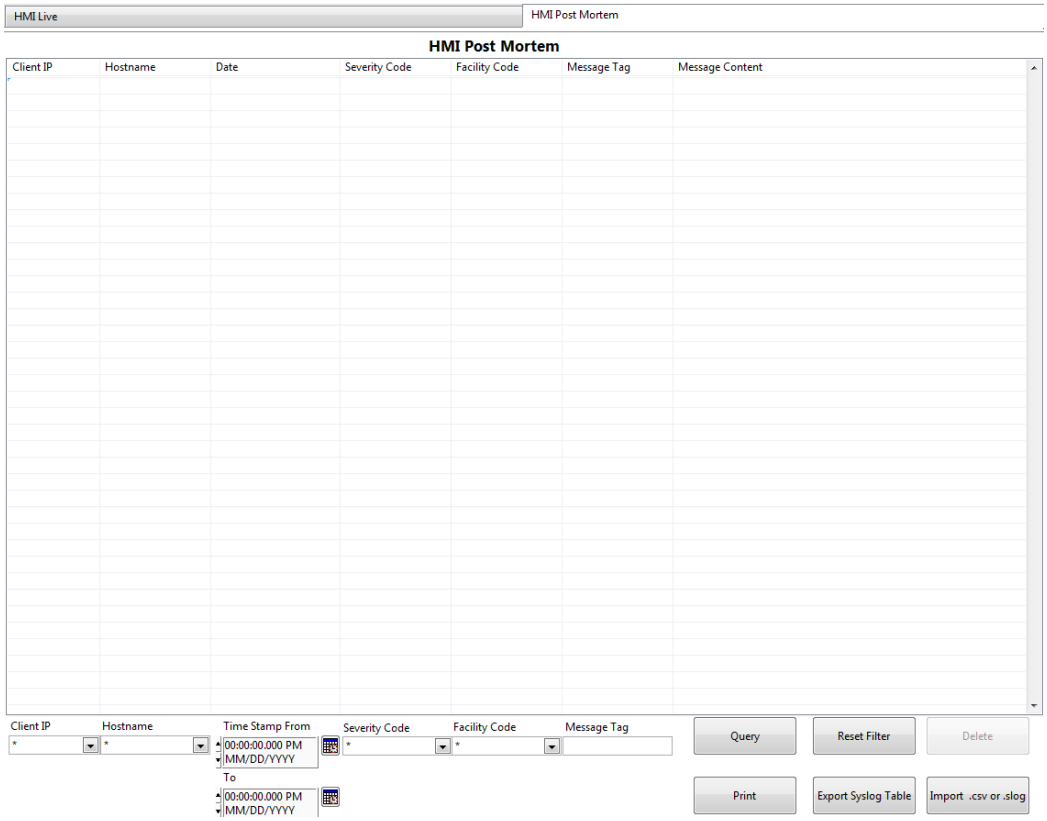


Value graphed is extracted from the message. The first "numeric chain" found in the message is extracted and plotted. It allows publishing a message like "measure voltage: 12.02154V" and the collector will analyze the message and extract the "12.02154" value and plot it.

Note: if the message contains several numeric data, it will only plot the first one. For example, if the message is "measure values: 12.02154V; 2.014A", only "12.02154" will be graphed.

3.2 Post Mortem Module (paid license only)

The interface displays the messages saved in the database. That way, it's possible for the user to search all received messages and filter them.



At the bottom of the interface, the user can specify different parameters to refine the query and display the resulting data only.

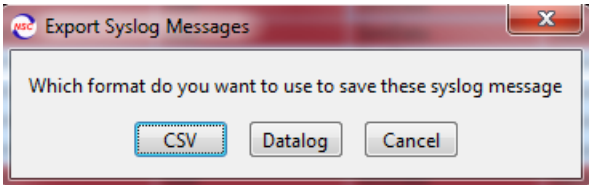
You can query the data by:

- Client IP
- Hostname
- Time Stamp
- Severity Code
- Facility Code
- Message Tag

To reset the filter, press the "Reset Filters" button.

If the recording of a message was is unwanted, it's possible to remove it from the database by pressing on the "Delete" button. It's also possible to delete multiple rows at the same time by selecting them before pressing on "Delete"

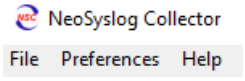
By pressing the "Export Syslog Table" button, it's possible to save the current table into a CSV or Datalog (slog) file. CSV files can be opened in software like Excel to perform other analysis. The Datalog (.slog) files save the data in less space than a CSV, but it is only readable by NeoSyslog Collector. This enables to free the internal database after doing the data export.



You can import data into the "post mortem table" by pressing on the "Import .csv or .slog" button. You will then be able to analyse the data. **Note:** The data imported that way won't be inserted and saved in the database.

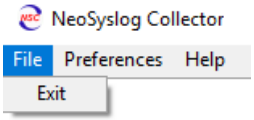
3.3 Menu Bar

This section covers the different options accessible in the menu bar.



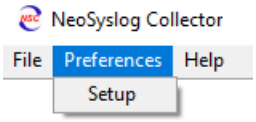
3.3.1 File

It's possible to exit the software by selecting File -> Exit

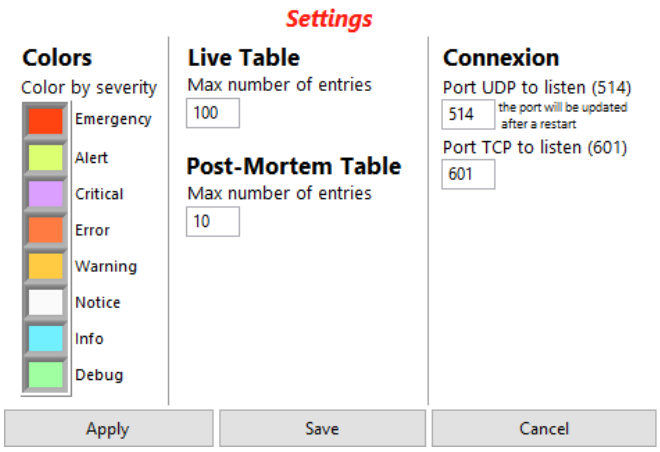


3.3.2 Preferences

The setup screen is accessible through the Preferences menu.



In the setup screen, the user is able to configure the HMI and the connexion parameters of the NeoSyslog Collector software.



It is possible to change the color for all severity code. It helps the user to better distinguish the messages received by severity.

It is also possible to change the number of messages retained into the "Live table". Rising the number of elements into the Live Table requires more memory and CPU. This number as to be set according to your usage and PC performance.

The same option is available for the "Post-Mortem Table". It's possible to limit the number of messages shown in the table.
To update the number of points in the table, the user must press on "Query" after changes have been applied in the setting page.

The last parameters that can be change are about the TCP and UDP ports to monitor for incoming messages. This provides more flexibility if another application is already utilizing the default ports. The change is applied only when saved and after restarting the program.

Note: Applying a setting makes it live in the current run of the collector. But it will not persist if the software program is restarted. To make the settings permanent they must be saved.

3.3.3 Help

This menu is used to show information about NeoSyslog Collector and support contacts. It also provides a link to display this user manual.