

User Manual: NeoSyslog Collector

Version 2.0.0

	Author	Reviser
Name	Vincent Carpentier	
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.
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>

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
1.0.2	25/05/2020	Cyril Gambini	Added definition of 'Syslog server'
1.1.0	13/07/2020	Brice Freund	Update documentation for NeoSyslog 1.1
2.0.0	05/08/2026	Vincent Carpentier	Update documentation for NeoSyslog 2.0.0

CONTENTS

1	Purpose of This Document.....	5
2	General Description.....	5
2.1	Supported operating system	6
2.2	Firewall and network rules	6
3	Features	7
3.1	Live View	7
3.1.1	Live Table	7
3.1.2	Pause Tables button	8
3.1.3	Clear Tables button	8
3.1.4	Last Value Table (full license only)	8
3.1.4.1	Graph Widget (full license only)	10
3.2	History View (full license only)	12
3.3	Settings.....	12
3.3.1	About Window	15

1 Purpose of This Document

The purpose of this document is to describe how to use the NeoSyslog Collector application. It explains how to install, configure, operate, and use the software to collect, visualize, and analyze Syslog messages.

2 General Description

Syslog is a standard protocol used for message logging in computer systems. It separates the software or device generating the messages from the system responsible for storing, displaying, and analyzing them.

Syslog is commonly used for system monitoring, troubleshooting, security auditing, and general diagnostic purposes. A wide variety of devices and systems, including cRIOs, sbRIOs, printers, routers, servers, and other network-enabled equipment, can generate Syslog messages. This makes it possible to consolidate log data from different types of systems into a central repository.

When used over a network, Syslog typically follows a client-server architecture. Syslog clients generate and transmit messages, while a Syslog server listens for incoming messages and stores or processes them.

NeoSyslog Collector is a Syslog server designed to receive and collect messages compliant with the RFC 3164 and RFC 5424 specifications. It can receive messages from multiple Syslog clients simultaneously using UDP and/or TCP.

Each Syslog message includes a facility code, which identifies the type of system or application that generated the message, and a severity level, which indicates the importance of the event.

The main purpose of NeoSyslog Collector is to provide an intuitive interface for viewing received Syslog messages and efficiently filtering, searching, and analyzing the collected data.

NeoSyslog Collector is available under two license levels: Free and Paid. The differences between the two licenses are summarized 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	✗	✓

With the Paid license, Syslog messages are stored in a SQLite database, enabling post-processing and historical analysis by querying recorded messages from the History view. These features are described in more detail in the following sections.

Within the NI software ecosystem, Syslog client libraries capable of publishing RFC 3164- and RFC 5424-compliant messages are available through **VI Package Manager (VIPM)**.

2.1 Supported operating system

NeoSyslog Collector is designed to run on Windows platforms only, starting with Windows 10.

However, it can receive Syslog messages from devices or systems running any operating system, provided that the messages comply with the RFC 3164 or RFC 5424 formats.

2.2 Firewall and network rules

NeoSyslog Collector listens on UDP and TCP ports for incoming Syslog messages. By default, UDP port 514 and TCP port 601 are used. Additional UDP and TCP ports can also be configured as required.

Depending on your organization's IT security policies, the configured ports or the NeoSyslog Collector application itself may need to be added as exceptions in the Windows Firewall or other network security software.

If Syslog clients are sending messages to the server but no messages appear in the Live view, verify that the firewall configuration allows traffic on the configured Syslog ports.

Facility Code: Facility associated with the message. The facility identifies the type of system, service, or application that generated the message.

App-Name: Identifies the application that generated the message. This field is available with RFC 5424 messages. For RFC 3164 messages, this field is displayed as "-".

Process ID: Identifies the process associated with the message. The interpretation of this value is defined by the sending application. A change in the Process ID may indicate that the application or process generating the Syslog messages has restarted. This field is available with RFC 5424 messages. For RFC 3164 messages, this field is displayed as "-".

Message ID (Tag): Identifies the type or category of the message and is defined by the Syslog client. For example, messages generated during application initialization could use Init as their Message ID or tag.

Structured-Data: Contains structured information associated with the message in a well-defined and machine-readable format. Structured-Data can contain one or more data elements and parameters that NeoSyslog Collector can extract and display in dedicated columns. This field is available with RFC 5424 messages.

Message Content: Contains the main text or payload of the Syslog message.

3.1.2 Pause Tables button

Pause Tables

This button pauses updates to the Live table. Syslog messages continue to be received while the display is paused and are shown when the button is clicked again.

3.1.3 Clear Tables button

Clear Tables

This button clears the data currently displayed in the tables. The data shown in the Last Value Table is also cleared. With the Paid license, clearing the displayed data does not delete the messages stored in the internal database.

3.1.4 Last Value Table (full license only)

This table displays the most recently received message for each unique set of selected criteria. These criteria can be based on Client IP, Host Name, Severity, Facility, Protocol, App-Name, Process ID, Tag, or values contained in the Structured-Data field.

The criteria used to identify unique messages can be configured from the Settings menu (see Section 3.2).

Each unique message combination appears as a separate row in the table, but only the most recently received message matching that combination is displayed. This provides a quick overview of the latest state or message from each client without requiring continuous monitoring of the Live Syslog table.

Data can also be displayed in a Graph Widget by right-clicking the corresponding row and selecting the appropriate option from the context menu.

Last Value Table							
IP Client	Timestamp	App-Name	Severity Code	Msg ID (Tag)	Message Content	temperature	interface
127.0.0.1	2026-08-05 14:30:02	kernel	critical	MEMORY100	NOTICE: Available memory dropped below recommended threshold		
127.0.0.1	2026-08-05 14:30:10	kernel	error	USB100	WARNING: USB device disconnected unexpectedly		
127.0.0.1	2026-08-05 14:30:18	rsyslogd	info	STATS100	INFO: Statistics report generated		
127.0.0.1	2026-08-05 14:29:40	systemd	notice	SERVICE	INFO: Started nginx.service - High Performance Web Server.		
127.0.0.1	2026-08-05 14:29:28	kernel	warning	THERMAL	CPU0: Core temperature above threshold, cpu clock throttled	101	

Figure 2 - Last Value Table

3.1.4.1 Graph Widget (full license only)

Selecting **Graph Widget** opens a new window displaying the selected data as a graph. The graph is automatically updated as new matching messages are received.

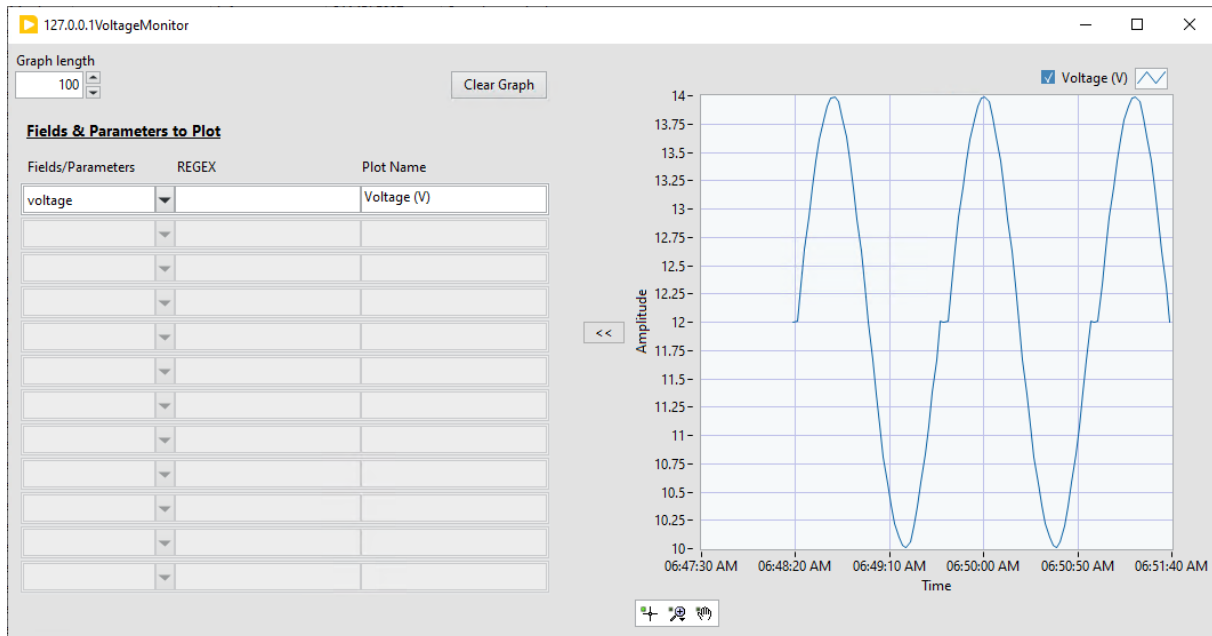


Figure 3 - Graph Widget

Graph settings can be modified by clicking the corresponding signal in the legend.

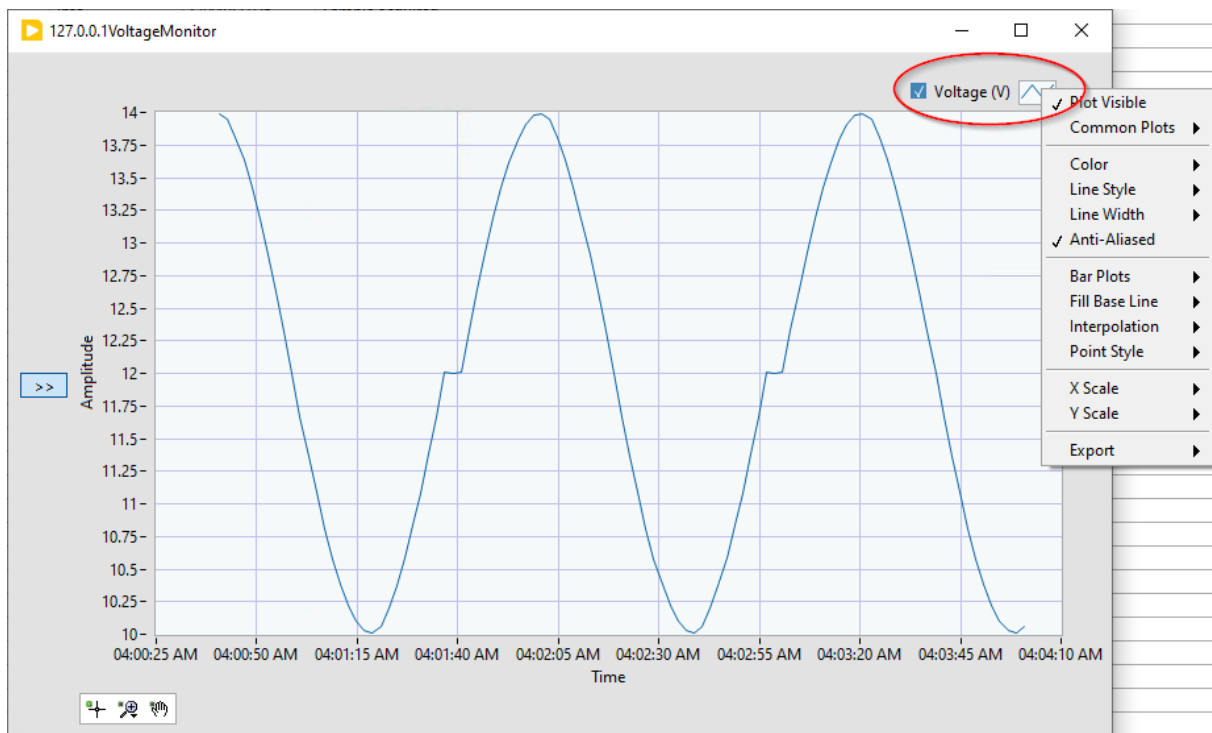


Figure 4 – Collapsed Graph Widget

The number of points displayed in the graph can also be configured directly from the interface, as shown in the previous figure.

Values plotted in the graph can be extracted from any field of the Syslog message. A regular expression (REGEX) can be defined to identify and extract the numeric value to be plotted.

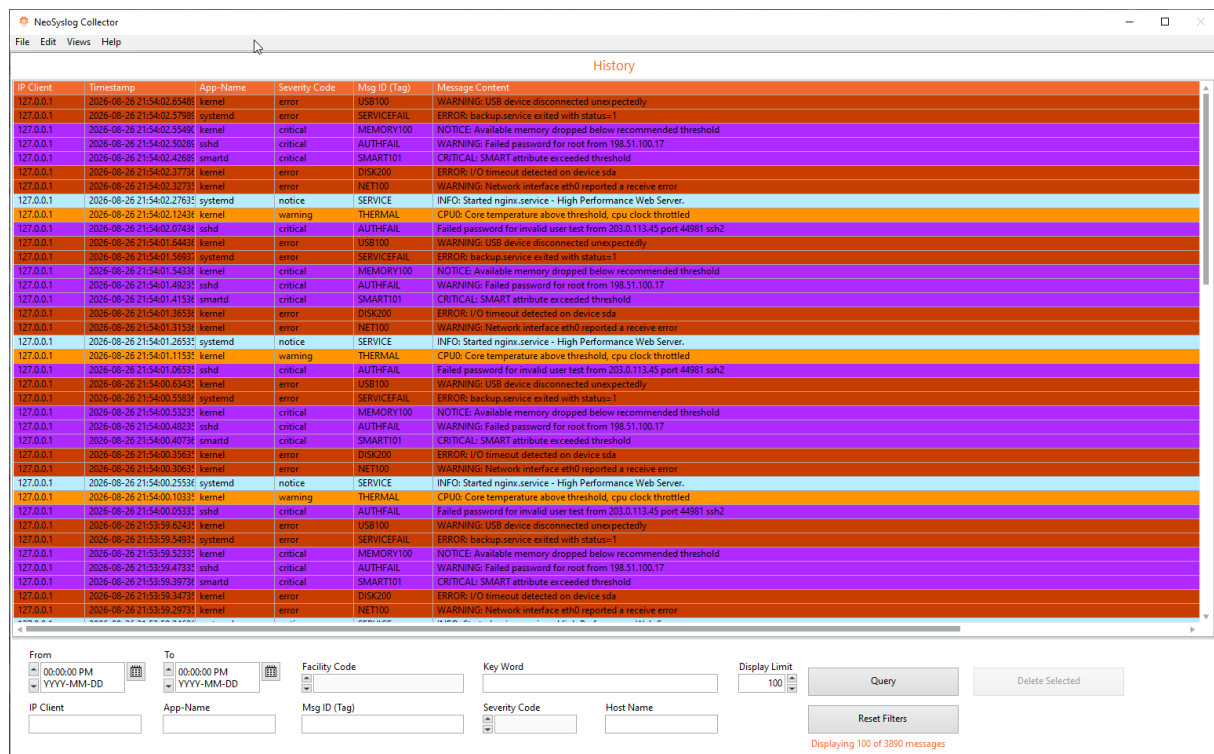
Note: If no REGEX pattern is specified, the first numeric value found in the selected message field, if any, is extracted and plotted.
For example, for the following message:

Measure values: 12.02154 V; 2.014 A

only 12.02154 is extracted and plotted.

3.2 History View (full license only)

The History view displays Syslog messages stored in the database. It provides access to previously received messages and allows the displayed data to be filtered using different search criteria.



IP Client	Timestamp	App-Name	Severity Code	Msg ID (Tag)	Message Content
127.0.0.1	2026-08-26 21:54:02.6548	kernel	error	USB100	WARNING: USB device disconnected unexpectedly
127.0.0.1	2026-08-26 21:54:02.3789	systemd	error	SERVICEFAIL	ERROR: backup.service exited with status=1
127.0.0.1	2026-08-26 21:54:02.3549	kernel	critical	MEMORY100	NOTICE: Available memory dropped below recommended threshold
127.0.0.1	2026-08-26 21:54:02.5028	sshd	critical	AUTHFAIL	WARNING: Failed password for root from 198.51.100.17
127.0.0.1	2026-08-26 21:54:02.4268	smartd	critical	SMART101	CRITICAL: SMART attribute exceeded threshold
127.0.0.1	2026-08-26 21:54:02.3778	kernel	error	DISK200	ERROR: I/O timeout detected on device sda
127.0.0.1	2026-08-26 21:54:02.3273	kernel	error	NET100	WARNING: Network interface eth0 reported a receive error
127.0.0.1	2026-08-26 21:54:02.2763	systemd	notice	SERVICE	INFO: Started nginx.service - High Performance Web Server.
127.0.0.1	2026-08-26 21:54:02.1243	kernel	warning	THERMAL	CPU0: Core temperature above threshold, cpu clock throttled
127.0.0.1	2026-08-26 21:54:02.0743	sshd	critical	AUTHFAIL	Failed password for invalid user test from 203.0.113.45 port 44381 ssh2
127.0.0.1	2026-08-26 21:54:01.6448	kernel	error	USB100	WARNING: USB device disconnected unexpectedly
127.0.0.1	2026-08-26 21:54:01.5683	systemd	error	SERVICEFAIL	ERROR: backup.service exited with status=1
127.0.0.1	2026-08-26 21:54:01.5438	kernel	critical	MEMORY100	NOTICE: Available memory dropped below recommended threshold
127.0.0.1	2026-08-26 21:54:01.4923	sshd	critical	AUTHFAIL	WARNING: Failed password for root from 198.51.100.17
127.0.0.1	2026-08-26 21:54:01.4153	smartd	critical	SMART101	CRITICAL: SMART attribute exceeded threshold
127.0.0.1	2026-08-26 21:54:01.3653	kernel	error	DISK200	ERROR: I/O timeout detected on device sda
127.0.0.1	2026-08-26 21:54:01.3153	kernel	error	NET100	WARNING: Network interface eth0 reported a receive error
127.0.0.1	2026-08-26 21:54:01.2653	systemd	notice	SERVICE	INFO: Started nginx.service - High Performance Web Server.
127.0.0.1	2026-08-26 21:54:01.1153	kernel	warning	THERMAL	CPU0: Core temperature above threshold, cpu clock throttled
127.0.0.1	2026-08-26 21:54:01.0653	sshd	critical	AUTHFAIL	Failed password for invalid user test from 203.0.113.45 port 44381 ssh2
127.0.0.1	2026-08-26 21:54:00.6343	kernel	error	USB100	WARNING: USB device disconnected unexpectedly
127.0.0.1	2026-08-26 21:54:00.5583	systemd	error	SERVICEFAIL	ERROR: backup.service exited with status=1
127.0.0.1	2026-08-26 21:54:00.5323	kernel	critical	MEMORY100	NOTICE: Available memory dropped below recommended threshold
127.0.0.1	2026-08-26 21:54:00.4823	sshd	critical	AUTHFAIL	WARNING: Failed password for root from 198.51.100.17
127.0.0.1	2026-08-26 21:54:00.4073	smartd	critical	SMART101	CRITICAL: SMART attribute exceeded threshold
127.0.0.1	2026-08-26 21:54:00.3563	kernel	error	DISK200	ERROR: I/O timeout detected on device sda
127.0.0.1	2026-08-26 21:54:00.3063	kernel	error	NET100	WARNING: Network interface eth0 reported a receive error
127.0.0.1	2026-08-26 21:54:00.2553	systemd	notice	SERVICE	INFO: Started nginx.service - High Performance Web Server.
127.0.0.1	2026-08-26 21:54:00.1033	kernel	warning	THERMAL	CPU0: Core temperature above threshold, cpu clock throttled
127.0.0.1	2026-08-26 21:54:00.0533	sshd	critical	AUTHFAIL	Failed password for invalid user test from 203.0.113.45 port 44381 ssh2
127.0.0.1	2026-08-26 21:53:59.6243	kernel	error	USB100	WARNING: USB device disconnected unexpectedly
127.0.0.1	2026-08-26 21:53:59.5493	systemd	error	SERVICEFAIL	ERROR: backup.service exited with status=1
127.0.0.1	2026-08-26 21:53:59.5233	kernel	critical	MEMORY100	NOTICE: Available memory dropped below recommended threshold
127.0.0.1	2026-08-26 21:53:59.4733	sshd	critical	AUTHFAIL	WARNING: Failed password for root from 198.51.100.17
127.0.0.1	2026-08-26 21:53:59.3973	smartd	critical	SMART101	CRITICAL: SMART attribute exceeded threshold
127.0.0.1	2026-08-26 21:53:59.3473	kernel	error	DISK200	ERROR: I/O timeout detected on device sda
127.0.0.1	2026-08-26 21:53:59.2973	kernel	error	NET100	WARNING: Network interface eth0 reported a receive error

Figure 5 - History View

At the bottom of the interface, several filter parameters can be specified to refine the database query and display only matching messages.

Messages can be filtered by:

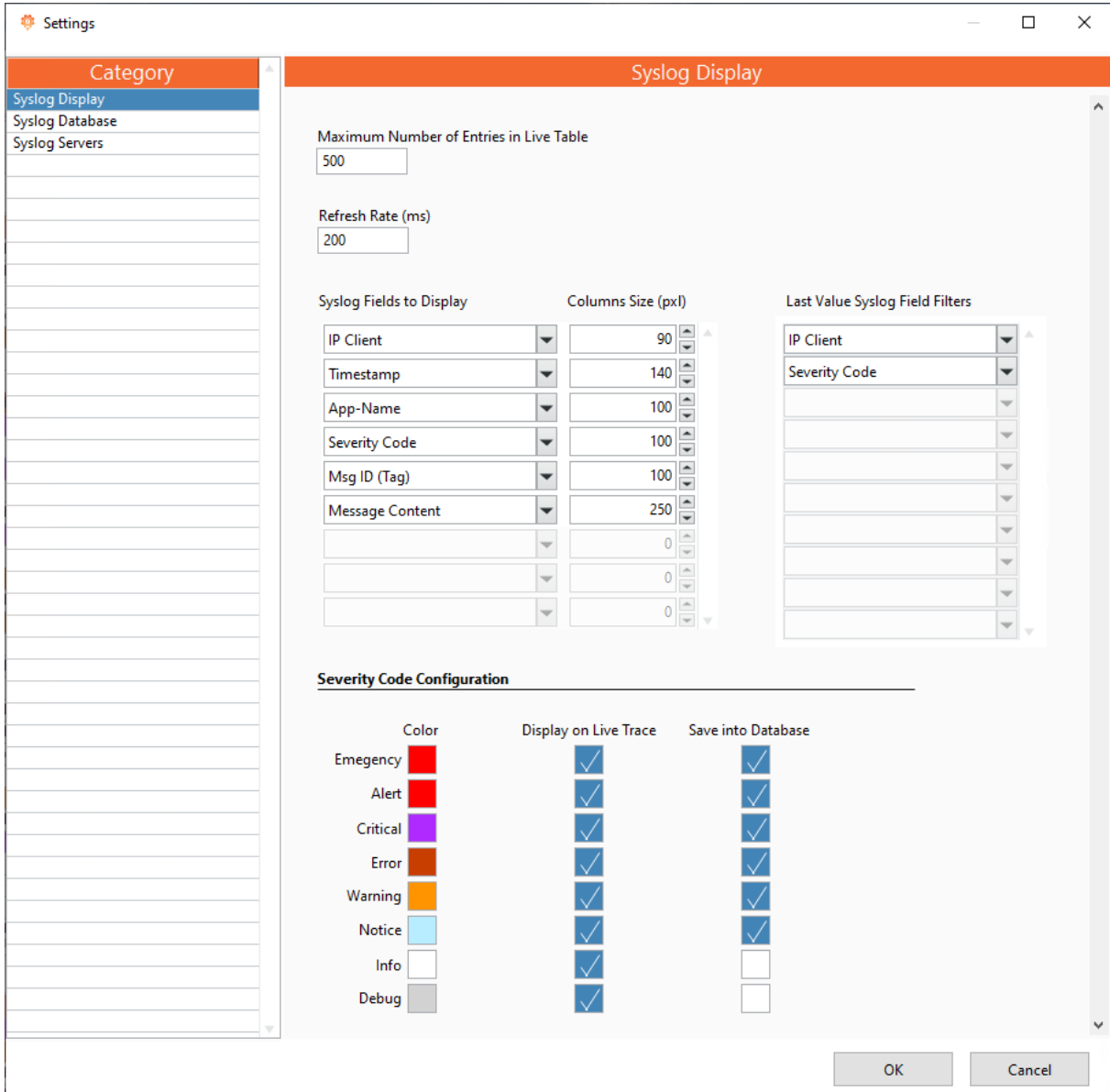
- Client IP
- Hostname
- Timestamp
- Severity Code
- Facility Code
- Protocol Version
- App-Name
- Process ID
- Message ID
-

Pressing **Reset Filters** clears all active filters and restores the default view.

3.3 Settings

The Settings screen can be accessed from the **Edit** menu.

From this screen, the HMI settings and NeoSyslog Collector connection parameters can be configured.



Settings

Category

- Syslog Display
- Syslog Database
- Syslog Servers

Syslog Display

Maximum Number of Entries in Live Table
500

Refresh Rate (ms)
200

Syslog Fields to Display

Syslog Fields to Display	Columns Size (pxl)
IP Client	90
Timestamp	140
App-Name	100
Severity Code	100
Msg ID (Tag)	100
Message Content	250
	0
	0
	0

Last Value Syslog Field Filters

Last Value Syslog Field Filters
IP Client
Severity Code

Severity Code Configuration

Severity Code	Color	Display on Live Trace	Save into Database
Emergency	Red	☒	☒
Alert	Red	☒	☒
Critical	Purple	☒	☒
Error	Brown	☒	☒
Warning	Orange	☒	☒
Notice	Light Blue	☒	☒
Info	White	☒	☐
Debug	Gray	☒	☐

OK Cancel

Figure 6 - Setting Window

The color associated with each severity code can be configured to make messages easier to distinguish in the different Syslog tables.

Severity codes can also be used to control whether messages are displayed in the Live Table and/or stored in the database. This can help reduce the number of stored messages, for example by excluding low-priority debugging messages that are not required for historical analysis.

The maximum number of messages retained in the Live Table can also be configured. Increasing this value requires additional memory and CPU resources. The value should therefore be selected according to the expected message volume and the performance of the computer running NeoSyslog Collector.

A similar setting is available for the History Table, allowing the maximum number of displayed messages to be limited. After changing this value, press Query to refresh the table using the new setting.

The columns displayed in the Syslog tables can also be configured. Changes to the column configuration are applied directly to all applicable tables. The content of the Last Value Table is controlled by the Last Value Criteria settings. One or more criteria can be selected to determine which messages are considered part of the same group. Only the most recently received message for each unique combination of the selected criteria is displayed.

If no criteria are selected, the Last Value Table displays only the most recently received Syslog message.

Changing the Last Value Criteria requires the existing table contents to be cleared to maintain consistency with the new configuration.

The TCP and UDP ports monitored for incoming Syslog messages can also be configured. This provides additional flexibility when the default ports are already in use by another application or when specific network configurations are required.

Note: Applying settings may clear the **Live Table** and **Last Value Table**. Messages removed from these tables are no longer available in the live interface. With the Paid license, messages already stored in the database remain available from the historical data.

3.4 SQLite Database

With the Paid license, received Syslog messages can be stored in an internal SQLite database. This provides persistent storage of the collected messages and allows previously received data to be reviewed and analyzed from the **History View**.

The **History View** queries the database and provides filtering capabilities based on several Syslog fields, such as Client IP, Hostname, Timestamp, Severity, Facility, Protocol Version, App-Name, Process ID, and Message ID.

Clearing messages from the **Live Table** or **Last Value Table** does not remove messages that have already been stored in the database. Stored messages remain available from the **History View**.

The location of the SQLite database file can be configured from the **Settings** window.

The SQLite database is managed automatically by NeoSyslog Collector and does not require a separate database server or additional database configuration.

3.5 About Window

The **About** window displays information about NeoSyslog Collector, including version information and support contact details.



Figure 7 - About Window