

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from <https://www.audiocodes.com/library/technical-documents>.

This document is subject to change without notice.

Date Published: December-19-2023

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at <https://www.audiocodes.com/services-support/maintenance-and-support>.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at <https://online.audiocodes.com/documentation-feedback>.

Stay in the Loop with AudioCodes



Document Revision Record

LTRT	Description
40030	Initial document release.
40031	Updated to Ver. 1.44. Note added to indicate no support by MP-1xx for "Receiving Logs from Device's Web Interface"; Syslog format updated to indicate SID and BID contains serial number instead of MAC for Mediant Software and 9000; installation updated
40032	Added Configuring Syslog Listener with TLS section.
40033	Updated to Ver. 1.97.

LTRT	Description
40034	Updated to Ver. 2.5.

Table of Contents

1	Introduction	1
2	Installing Syslog Viewer	2
3	Starting Syslog Viewer	5
4	Getting Familiar with Syslog Viewer	6
	Areas of GUI	6
	Display Preferences	9
	Saving Window Size and Position	9
	Configuring Font Type and Size of Syslog Messages	9
	Customizing Appearance Theme	10
	Configuring Scrollback of Syslog Message Lines	10
	Freezing Syslog Messages Display	11
	Reconstructing New Lines for Syslog Messages	13
	Disabling Auto-Scroll in Syslog Messages	14
	Hiding or Showing Date in Syslog Messages	15
	Wrapping Syslog Message Lines	16
	Window Tabs	16
	Enabling Window Tabs per Device	17
	Configuring Labels for Window Tabs	17
	Displaying Window Tab for Syslog Messages of Single Device	18
	Clearing Existing Window Tabs when Opening Syslog File	19
	Sorting Window Tabs	19
	Detecting Missing and Out-Of-Order Logs	19
	Checking for Syslog Viewer Updates	20
5	Collecting Syslog Messages Methods	22
	Collecting Syslog Messages Directly from Devices	22
	Configuring Devices to Send Syslog Messages	22
	Configuring Syslog Server on Device	22
	Configuring Syslog Viewer's Listening Port and Interface	24
	Collecting Syslog Messages from Device's Web Interface	25
	Using Wireshark to Capture Packets for Syslog Viewer	27
	Realtime Monitoring of Syslog File by External Syslog Sever	28
6	Viewing Syslog Messages	30
	Viewing Real-time Collection of Syslog Messages	30
	Viewing Syslog Messages in External Text-Based Editor	32
	Viewing Syslog Messages of Saved Files	32
	Viewing Syslog Messages from Clipboard	33
	Clearing Display of Syslog Messages	33
	Viewing Supported File Formats	33
7	Writing Real-time Syslog Messages to File	35
	Rotating Written Syslog Files	35

Enabling Dedicated Syslog Files per Device	37
Creating Dedicated Folders per Device	37
8 Saving Displayed Syslog Messages	39
Saving Displayed Syslog Messages to File	39
Copying Displayed Syslog Messages to Clipboard	39
9 Searching Syslog Messages	40
Searching for Strings	40
Searching for a Syslog Message Line	40
10 Highlighting and Editing Syslog Messages	42
Highlighting Syslog Messages by Keywords	42
Marking Individual Syslog Message Lines	43
Highlighting SIDs in Syslog Messages	44
Editing Syslog Messages	44
11 Filtering Syslog Messages	46
Filtering Display of Syslog Messages	46
Filtering Incoming Syslog Messages by Severity Level	47
Filtering Incoming Syslog Messages by IP Address	48
Filtering Incoming Syslog Messages and Display by Content	48
12 Analyzing Syslog Messages	50
Syslog Message Types	50
SIP Call Session Logs	51
Board Logs	52
SNMP Alarms	53
Error Abbreviations in Syslog Messages	54
Severity Levels of Syslog Messages	56
Viewing SIP Flow Diagrams	56
Setting Preferences for SIP Flow Diagrams	61
Filtering Display by Session ID	62
Copying to Clipboard the SID, SIP URI From, or SIP URI To	63
13 Using the Command Line	64

1 Introduction

This document describes AudioCodes' Syslog Viewer utility. It includes installation, getting started, configuring preferences, and using Syslog Viewer.

Syslog is an event notification protocol that enables a device to send event notification messages across IP networks to event message collectors, also known as Syslog servers.

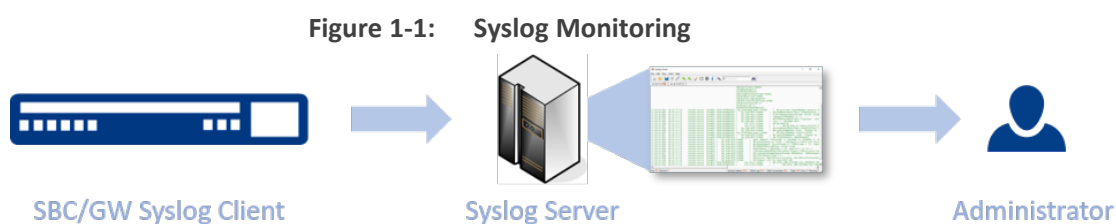
AudioCodes Session Border Controllers and Media Gateways (hereafter, referred to as device) contain an embedded Syslog client, which can be enabled to generate and send error reports and events to remote Syslog servers.

Syslog messages is a collection of error, warning, and system messages that records every internal operation of the device.

You can use AudioCodes Syslog Viewer for the following main tasks:

- Collect (record / capture) and display syslog messages sent from AudioCodes devices
- Analyze the collected syslog messages (using, for example, interactive SIP call flow diagrams)

The implementation of syslog monitoring is illustrated below:



2 Installing Syslog Viewer

This section describes how to install Syslog Viewer on your computer.

➤ **To install Syslog Viewer:**

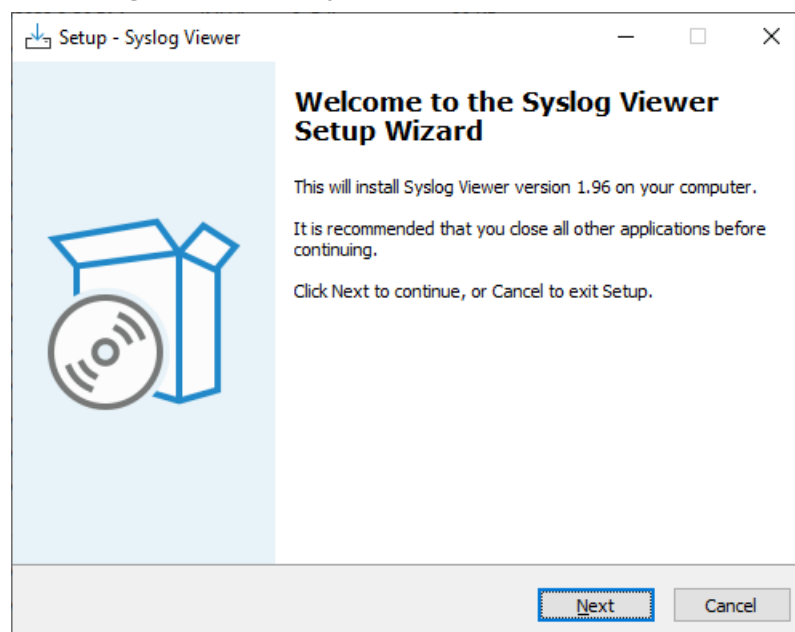
1. Download the Syslog Viewer installation file from AudioCodes website at <https://www.audiocodes.com/library/firmware>.



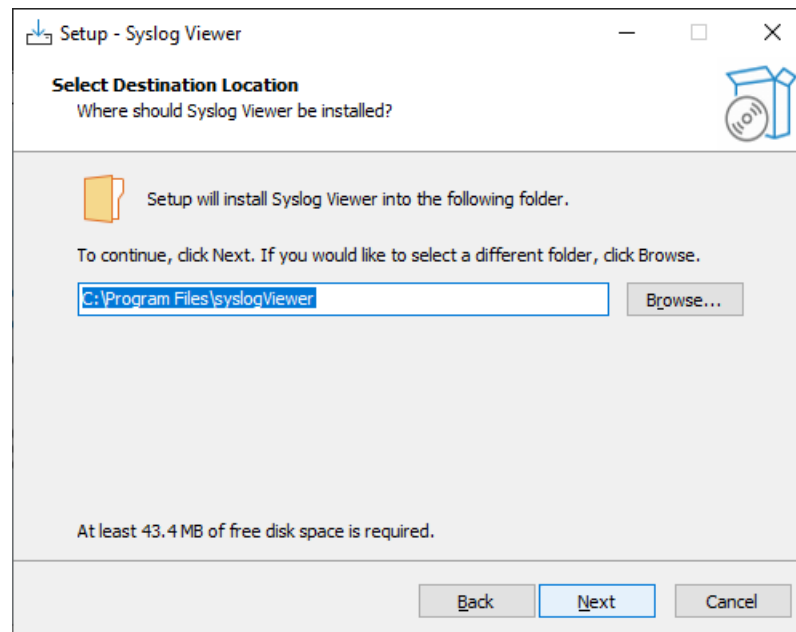
Once you have installed Syslog Viewer, whenever you start it, it checks online for a new software update. For more information, see [Detecting Missing and Out-Of-Order Logs](#) on page 19.

2. Click the *downloaded .exe* file; the installation wizard starts:

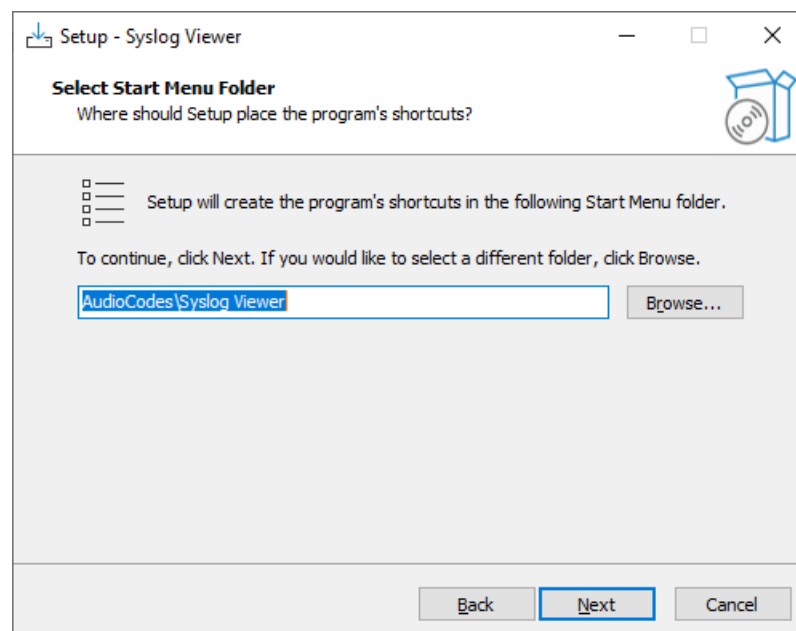
Figure 2-1: Setup Wizard - Welcome



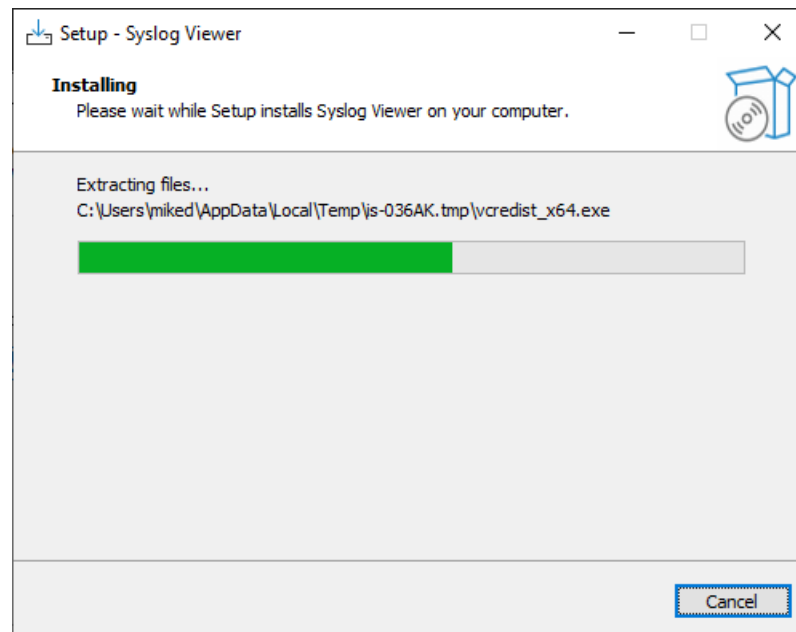
3. Click **Next**; the following appears:

Figure 2-2: Setup Wizard - Select Destination Location

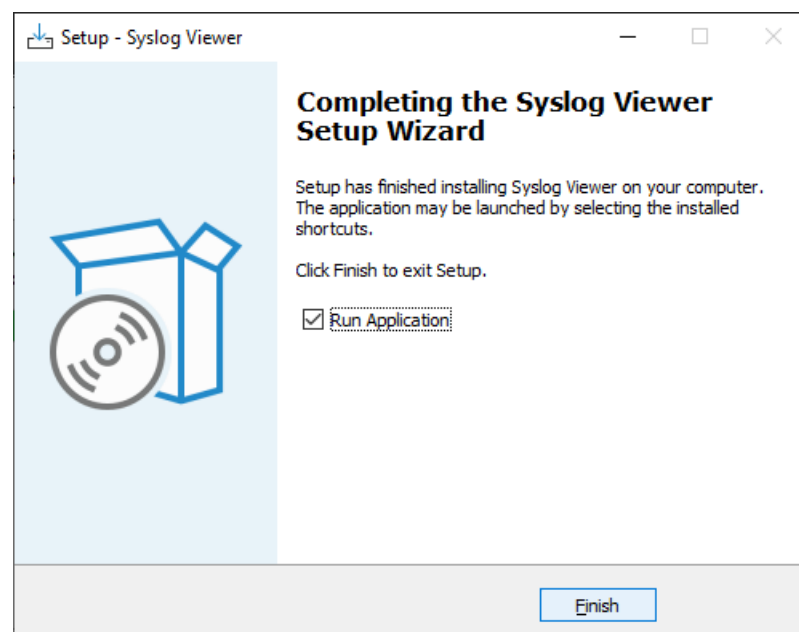
4. Select the location on your computer where you want to install Syslog Viewer, and then click **Next**; the following appears:

Figure 2-3: Setup Wizard - Select Start Menu Folder

5. Select where you want to add Syslog Viewer's shortcut menu, and then click **Next**; the application begins to install, displaying the installation progress bar:

Figure 2-4: Setup Wizard - Installing

When installation finishes, the following appears:


Figure 2-5: Setup Wizard - Complete**Figure 2-6:**

6. Click **Finish**; Syslog Viewer is installed and starts.

3 Starting Syslog Viewer

The procedure below describes how to start Syslog Viewer.

➤ **To start Syslog Viewer:**

On your Windows taskbar, click the **Start**  button, expand the **AudioCodes** folder, and then

click the **Syslog Viewer**  icon.



- You can open multiple instances of Syslog Viewer. This may be useful for analyzing multiple files.
- By default, when you start Syslog Viewer, it checks online for a new software update and if exists, it prompts you to update. For more information, see [Checking for Syslog Viewer Updates](#) on page 20.

4 Getting Familiar with Syslog Viewer

This section provides a description of the Syslog Viewer GUI.

Areas of GUI

The main areas of the Syslog Viewer GUI are shown below and described in the subsequent table.

Figure 4-1: Areas of Syslog Viewer GUI

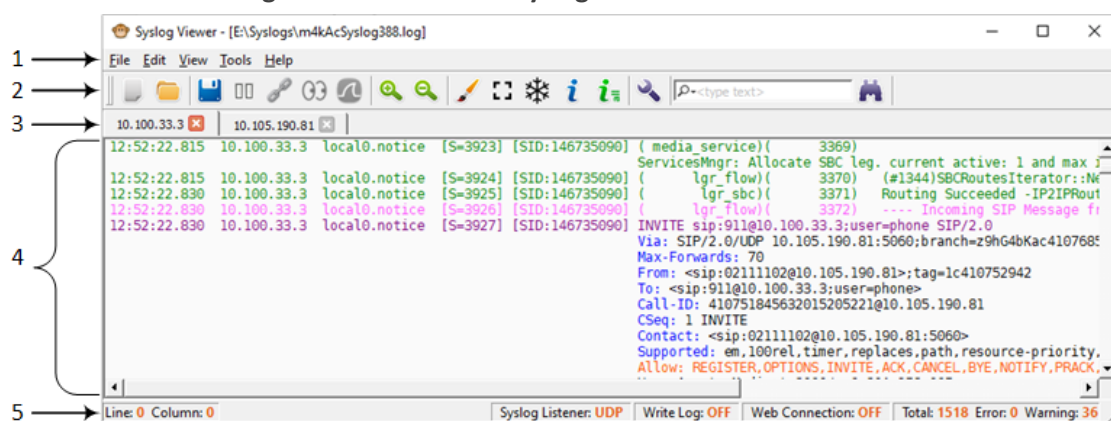















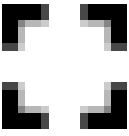







Table 4-1: Description of GUI Areas

Item #	Description		
1	Menu bar		
2	Toolbar with frequently required command icons:		
	Icon	Name	Description
		Clean	Clears the syslog messages in the window.
		Open	Open a syslog file saved on your computer.
		Write Log	Writes (saves) syslog messages to a file. For more information, see Writing Real-time Syslog Messages to File on page 35.
		Stop Writing Log	Stops writing syslog messages to a file. For more information, see Writing Real-time Syslog Messages to File on page 35.

Item #	Description		
		Pause	Pauses the receipt of syslog messages from the device. For more information, see Collecting Syslog Messages Methods on page 22.
		Resume	Resumes (after pausing) the receipt of syslog messages from the device. For more information, see Collecting Syslog Messages Methods on page 22.
		Connect To	Connects to the device's Web interface (over HTTP/S) from where it receives syslog messages. For more information, see Collecting Syslog Messages from Device's Web Interface on page 25.
		Disconnect from <IP address>	Disconnects from the device's Web interface from where it receives the syslog messages. For more information, see Collecting Syslog Messages from Device's Web Interface on page 25.
		File Monitor	Starts real-time display of syslog messages written to a file that are captured by an external syslog server. For more information, see Realtime Monitoring of Syslog File by External Syslog Sever on page 28.
		Stop File Monitor	Stops real-time display of syslog messages written to a file that are captured by an external syslog server. For more information, see Realtime Monitoring of Syslog File by External Syslog Sever on page 28.
		Network Capture (via Wireshark)	Starts capturing syslog messages on port 514 using Wireshark. For more information, see Using Wireshark to Capture Packets for Syslog Viewer on page 27.
		Stop Network Capture	Stops capturing syslog messages on port 514 using Wireshark. For more information, see Using Wireshark to Capture Packets for Syslog Viewer on page 27.
		Zoom In	Zooms in to the syslog messages window.

Item #	Description		
		Zoom Out	Zooms out of the syslog messages window.
		External Viewer	Displays syslog messages in an external, text-based editor (e.g., Notepad). For more information, see Viewing Syslog Messages in External Text-Based Editor on page 32.
		Disable Auto Scroll	Disables auto-scroll in syslog messages window. For more information, see Freezing Syslog Messages Display on page 11.
		Freeze Display	Freezes current display in syslog messages window (but continues writing to file). For more information, see Freezing Syslog Messages Display on page 11.
		SIP Flow Diagram	Opens the SIP Flow Diagram window, displaying a SIP flow diagram of the currently displayed syslog messages window. For more information, see Viewing SIP Flow Diagrams on page 56.
		SIP Flow Diagram for All Tabs	Opens the SIP Flow Diagram window, displaying the SIP flow diagram of the currently displayed syslog messages window (tab), and listing the sessions of all the syslog messages windows (tabs). For more information, see Viewing SIP Flow Diagrams on page 56.
		Options	Opens the Options dialog box for configuring various preferences.
		Find Next	Searches for a string.
3	Tab bar, displaying window tabs. For more information, see Window Tabs on page 16.		
4	Window displaying syslog messages.		
5	Status bar, displaying various status information: <ul style="list-style-type: none"> ■ 'Line': Displays the number of the line where your cursor is currently located. The first line (top of window) is 0. ■ 'Column': Displays the number of the column where your cursor is currently 		

Item #	Description
	located.
■	'Syslog Listener': Displays if Syslog Viewer is currently listening on the port for incoming syslog messages from the device ("UDP" or "TCP"), or not ("OFF").
■	'Write Log': Displays if the syslog messages are being saved to a file ("OFF" or "ON").
■	'Web Connection': Displays if Syslog Viewer is collecting syslog messages from the device's Web interface (over HTTP/S). If yes, the device's IP address is displayed. If no, "OFF" is displayed.
■	'Total': Displays the total number of lines in the syslog file.
■	'Errors': Displays the total number of errors in the syslog file.
■	'Warning': Displays the total number of warnings in the syslog file.


Display Preferences

This section describes how to configure various global preferences for Syslog Viewer.

Saving Window Size and Position

You can save the Syslog Viewer's window size and position on your screen. When you start Syslog Viewer, it opens with the same window size and in the same position as when previously used.

➤ To save window size and position:

1. On the toolbar, click the **Options**  icon; the Options dialog box appears.
2. Under the Viewer group, select the 'Save Window Position' check box.
3. Click **OK**.


Configuring Font Type and Size of Syslog Messages

You can change the font type and size of the displayed syslog messages. The default font type is Bitstream Vera Sans Mono with font size 9.



AudioCodes recommends using monospaced fonts.

➤ To configure display font type and size:


1. On the toolbar, the **Options**  icon; the Options dialog box appears.
2. Under the Viewer group, do the following:

- a. From the 'Font' drop-down lists, select the desired font type.
 - b. From the 'Size' drop-down list, select the desired font size.
3. Click **OK**.

Customizing Appearance Theme

By default, Syslog Viewer appears in a light theme (gray). You can change the appearance to a dark theme.

➤ To change appearance theme:

1. On the toolbar, click the **Options**  icon; the Options dialog box appears.
2. Under the Viewer group, select the 'Dark Theme' check box.
3. Click **OK**; you are prompted to restart Syslog Viewer.
4. Click **OK** to restart Syslog Viewer; Syslog Viewer closes.
5. Start Syslog Viewer; it now appears in the dark theme.

Configuring Scrollback of Syslog Message Lines

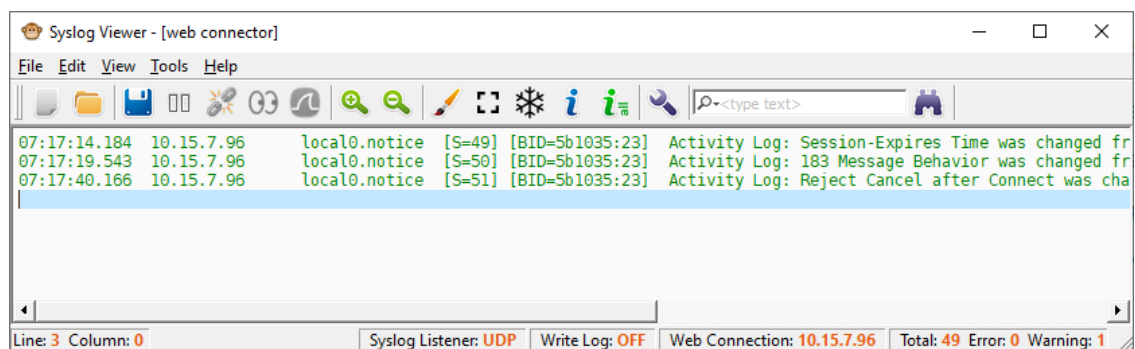
You can configure the maximum number of logged lines (scrollback) that Syslog Viewer displays in the window. When the maximum number of lines is reached and Syslog Viewer receives a new syslog message, it hides the oldest currently displayed syslog message line to accommodate for the new syslog message line.



If you are writing syslog messages to file (see [Writing Real-time Syslog Messages to File](#) on page 35), even though the syslog messages become hidden from display because of line scrollback, they're still saved to file.

The default line scrollback is 10,000 lines. You can change it to any value from 1 to 100,000 lines.


The maximum number of lines that Syslog Viewer displays is the line scrollback value plus 1. For example, if you configure scrollback to 2, a maximum of 3 lines are displayed, as shown in the following example:





- Increasing the line scrollbar to many lines may reduce performance.
- Total counters on the status bar in the bottom-right corner display total statistics for Syslog Viewer output; the total data statistics may be greater than what is displayed on the screen (which is acceptable).

➤ **To configure line scrollbar:**

1. On the toolbar, click the **Options**  icon; the Options dialog box appears.
2. Under the Viewer group, in the 'Lines of scrollbar' field, enter the maximum number of lines that you want displayed.
3. Click **OK**.

Freezing Syslog Messages Display

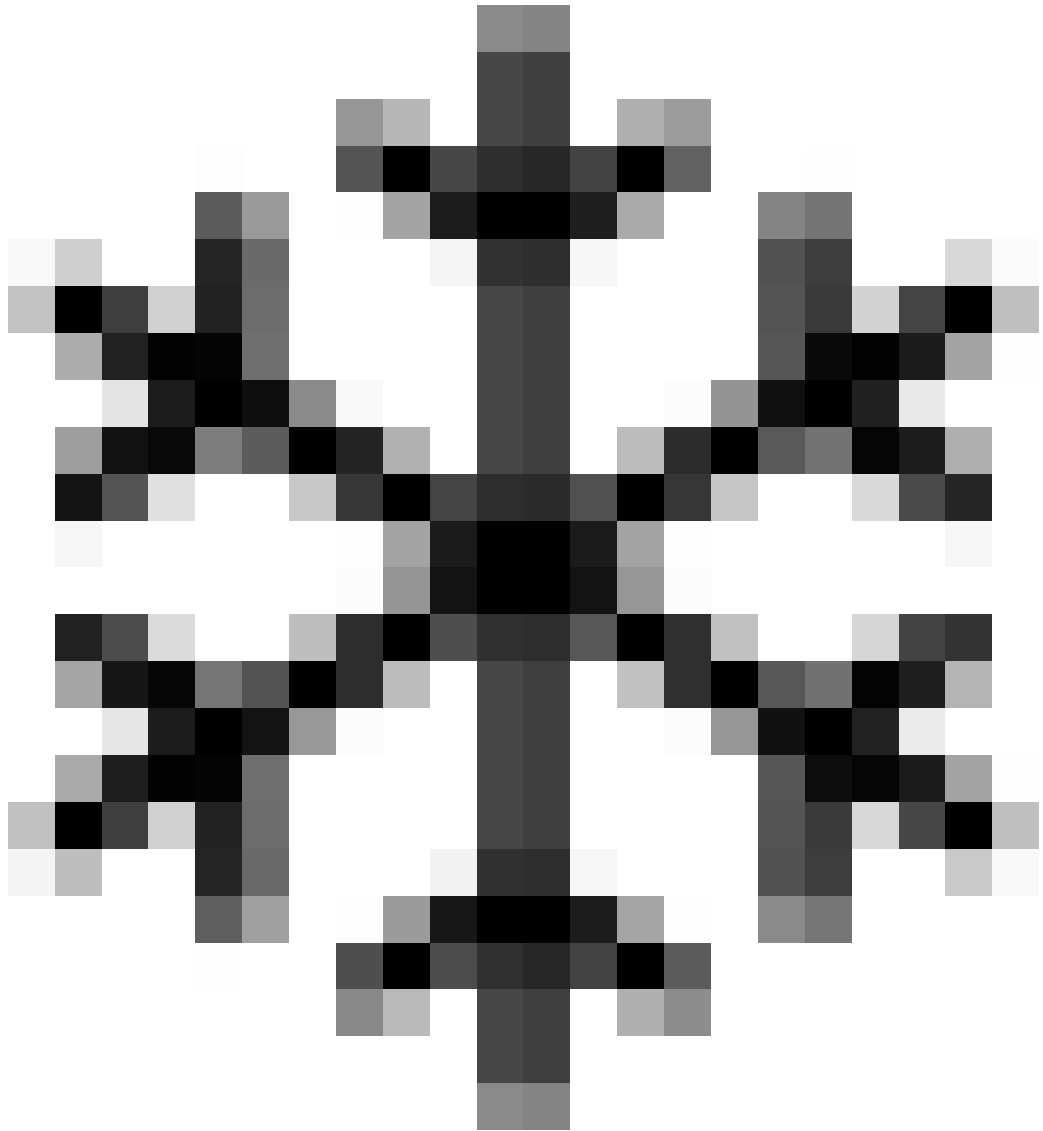
You can freeze the display of syslog messages, preventing newly received syslog messages from being displayed in the window. This may be useful if you need time to read the logged information.



When you freeze the display, Syslog Viewer continues to accept new syslog messages from the device; it simply doesn't display them.

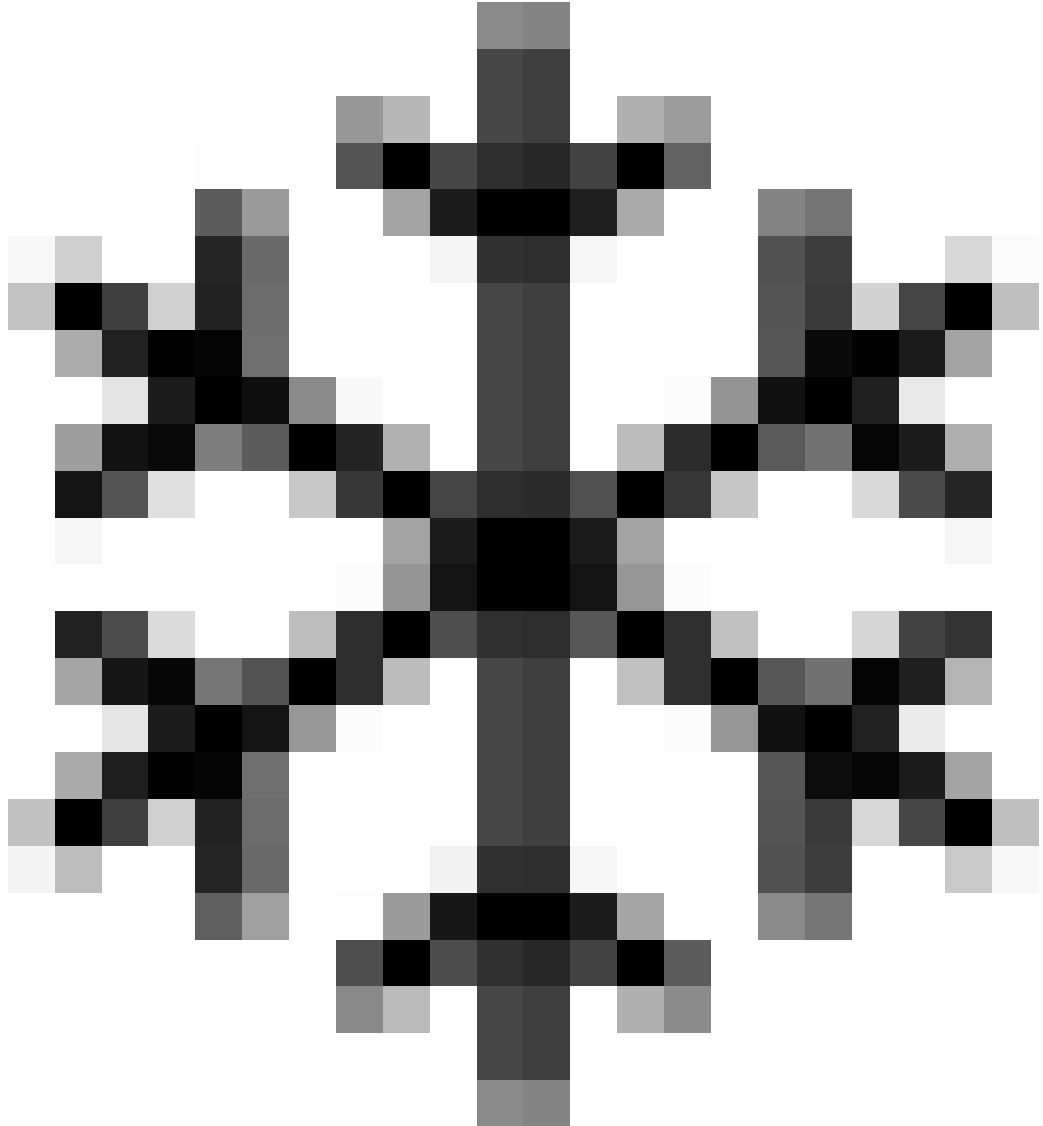
➤ **To freeze syslog messages display:**

1. On the toolbar, click



; the display freezes and no more messages are added to it.

2. To unfreeze the display and show new messages, click



again.

Reconstructing New Lines for Syslog Messages

Typically, syslog messages include new line characters (`\n`) that indicate the end of lines. However, unlike AudioCodes devices, some third-party syslog servers create syslog messages without new line characters. In such cases, Syslog Viewer tries to re-construct new lines, by identifying where each line ends, and then splitting the lines accordingly.

The following example shows received syslog messages that don't include new line characters. The first figure shows when this feature is disabled (i.e., no splitting onto new lines); the second figure shows when it's enabled (i.e., split onto new lines):

- Splitting lines disabled:

Syslog Viewer - [E:\backup\documents\SBC & Gateways\Complementary\Utilities\Syslog Viewer\pics\fujitsu_10.30.33.241_syslog.log]

File Edit View Tools Help

07/15 09:35:23.951 10.30.33.241 local0.notice [S=225] [SID=be36b7:18:38] (N 43) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:23.952 10.30.33.241 local0.notice [S=226] [SID=be36b7:18:38] (N 44) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:23.953 10.30.33.241 local0.notice [S=228] [SID=be36b7:18:38] (N 45) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:26.765 10.30.33.241 local0.notice [S=229] [SID=be36b7:18:38] (N 46) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:26.766 10.30.33.241 local0.notice [S=230] [SID=be36b7:18:38] (N 47) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:26.767 10.30.33.241 local0.notice [S=231] [SID=be36b7:18:38] (N 48) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:26.826 10.30.33.241 local0.notice [S=233] [SID=be36b7:18:40] (N 49) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:26.827 10.30.33.241 local0.notice [S=234] [SID=be36b7:18:40] (N 48) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:26.829 10.30.33.241 local0.notice [S=235] [SID=be36b7:18:40] (N 48) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:26.829 10.30.33.241 local0.notice [S=236] [SID=be36b7:18:40] (N 48) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:31.706 10.30.33.241 local0.notice [S=237] [SID=be36b7:18:41] (N 49) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:31.707 10.30.33.241 local0.notice [S=238] [SID=be36b7:18:41] (N 49) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

Line: 1 Column: 43 Syslog Listener: OFF Write Log: OFF Web Connection: OFF Total: 286 Error: 0 Warning: 5

■ Splitting lines enabled:

Syslog Viewer - [E:\backup\documents\SBC & Gateways\Complementary\Utilities\Syslog Viewer\pics\fujitsu_10.30.33.241_syslog.log]

File Edit View Tools Help

07/15 09:35:23.951 10.30.33.241 local0.notice [S=225] [SID=be36b7:18:38] (N 43) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:23.952 10.30.33.241 local0.notice [S=226] [SID=be36b7:18:38] (N 44) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:23.953 10.30.33.241 local0.notice [S=228] [SID=be36b7:18:38] (N 45) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:26.765 10.30.33.241 local0.notice [S=229] [SID=be36b7:18:38] (N 46) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:26.766 10.30.33.241 local0.notice [S=230] [SID=be36b7:18:38] (N 47) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:26.767 10.30.33.241 local0.notice [S=231] [SID=be36b7:18:38] (N 48) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:26.826 10.30.33.241 local0.notice [S=233] [SID=be36b7:18:40] (N 49) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:26.827 10.30.33.241 local0.notice [S=234] [SID=be36b7:18:40] (N 48) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:26.829 10.30.33.241 local0.notice [S=235] [SID=be36b7:18:40] (N 48) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399


07/15 09:35:26.829 10.30.33.241 local0.notice [S=236] [SID=be36b7:18:40] (N 48) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:31.706 10.30.33.241 local0.notice [S=237] [SID=be36b7:18:41] (N 49) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

07/15 09:35:31.707 10.30.33.241 local0.notice [S=238] [SID=be36b7:18:41] (N 49) ---- Incoming SIP Message from 10.30.33.241:5060;transport=udp SIP/2.0 200 OK Via: SIP/2.0/UDP 10.30.32.101:5060;branch=z9hG4bK-10.30.33.241;tag=24399

Line: 1 Column: 66 Syslog Listener: OFF Write Log: OFF Web Connection: OFF Total: 286 Error: 0 Warning: 5

➤ To enable new line breaks:

1. On the toolbar, click the **Options**  icon; the Options dialog box opens.
2. Under the Miscellaneous group, from the 'Split lines without EOL' drop-down list, select one of the following:
 - **Enable:** (Default) Syslog Viewer tries to identify the end of lines and splits them accordingly.
 - **Disable:** Syslog Viewer displays the syslog as is.
3. Click **OK**.

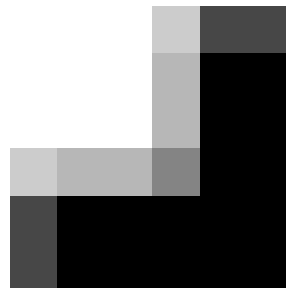
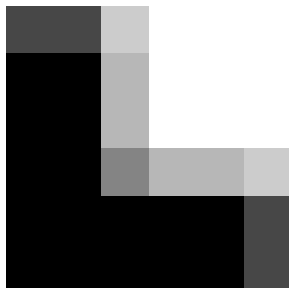
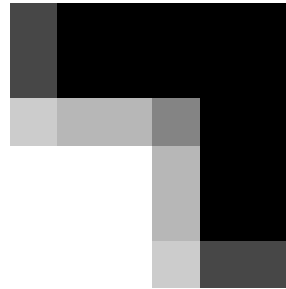
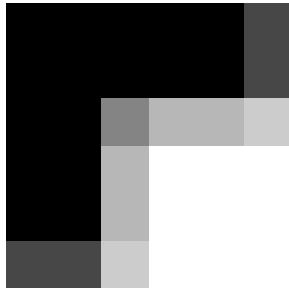
Disabling Auto-Scroll in Syslog Messages

By default, Syslog Viewer automatically scrolls to the most recently added syslog message (bottom of list). This allows you to view the latest message quickly and easily, without having to scroll down.

However, you may want to disable this feature to stay on a specific syslog message line instead of viewing the latest messages. When disabled, Syslog Viewer continues adding newly received syslog messages to the window.

➤ **To enable and disable auto-scroll:**

1. In the syslog messages window, select a message line that you want to remain in view.
2. On the toolbar, click the **Auto-Scroll**



icon; the display remains

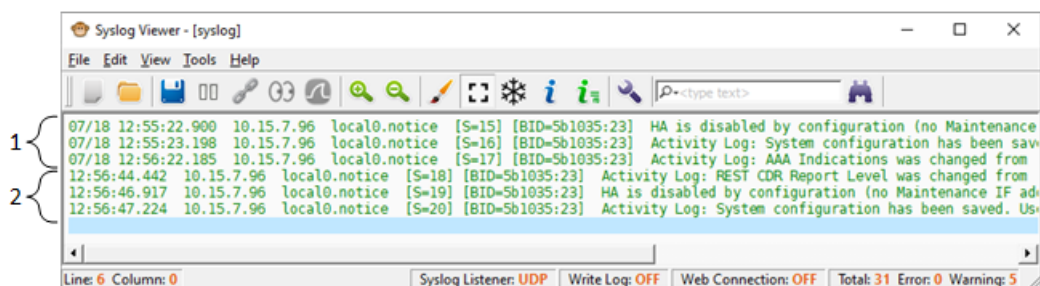
at your selected message even though new messages are added to the display.

3. To enable auto-scroll, click the icon again; Syslog Viewer automatically scrolls down to the most recently added syslog message.


Hiding or Showing Date in Syslog Messages

By default, Syslog Viewer displays the date when it received the syslog message from the device. However, you can hide the date from syslog messages.

For example, the following figure shows syslog messages with the date (#1) and syslog messages without the date (#2):



➤ **To hide or show date in syslog messages:**

1. On the toolbar, click the **Options**  icon; the Options dialog box appears.
2. Under the Syslog group, select or clear the 'Show date' check box to show or hide the date, respectively.
3. Click **OK**.

Wrapping Syslog Message Lines

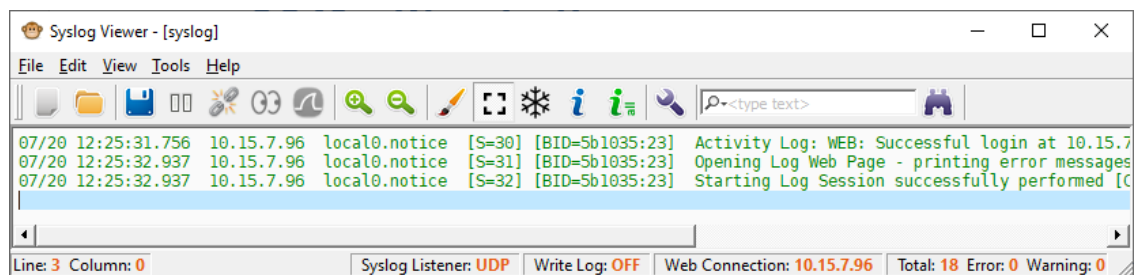
You can enable Syslog Viewer to wrap syslog message lines so that they fit into the current width of the window. When you resize the window, text is wrapped onto the next line so that they are always visible.

➤ **To enable or disable text wrapping:**

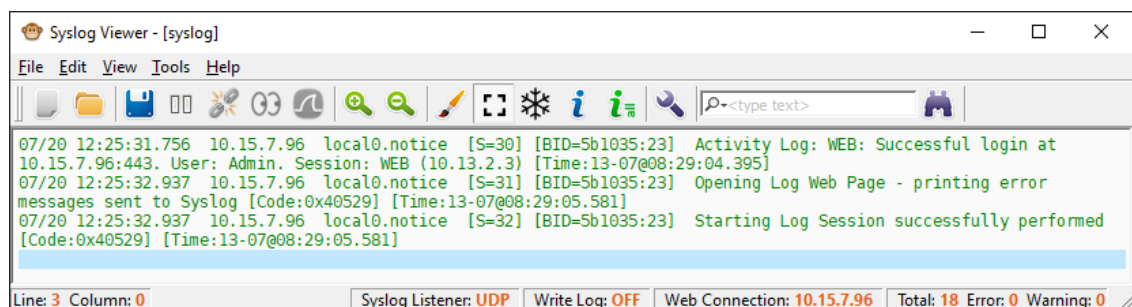
- From the View menu, choose **Line Wrap**.

The following shows an example of line wrapping:

■ **No line wrapping:**



■ **Line wrapping:**



Window Tabs

Syslog Viewer uses window tabs to allow you to easily identify syslog messages by device. It creates tabs when capturing syslog messages from multiple devices and when opening syslog files.



Syslog Viewer always creates tabs when you open syslog files.

Enabling Window Tabs per Device

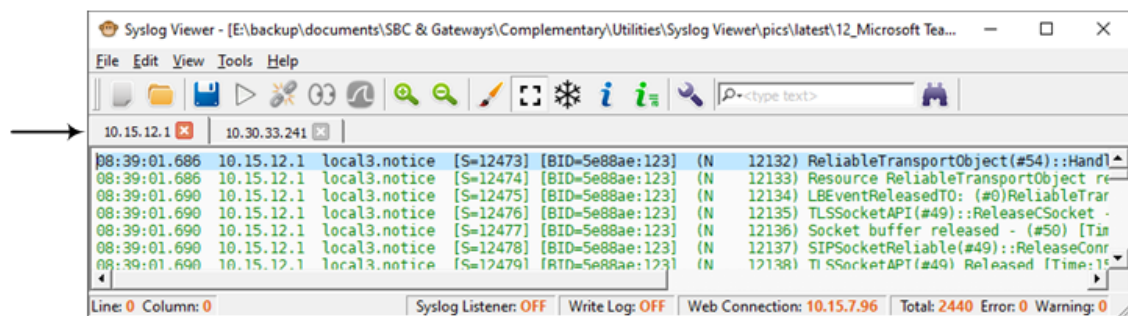
By default, Syslog Viewer uses window tabs to separate syslog messages captured from different devices (IP addresses). Each tab displays syslog messages captured from the specific device.

You can disable window tabs so that Syslog Viewer displays all syslog messages in a single window, even if they were captured from more than one device.


Using tabs can be useful, for example, in the following cases:

- Opening a syslog file that contains syslog messages captured from multiple devices.
- Capturing syslog messages from multiple devices.

The following figure shows an example of an opened syslog file that contains syslog messages captured from two devices - 10.15.12.1 and 10.30.33.241. Syslog Viewer creates a tab for each device and displays the syslog messages under the respective tab:



➤ To enable window tabs per connected device:

1. On the toolbar, click the **Options**  icon; the Options dialog box appears.
2. Under the Multiple Devices group, select the 'Use multiple tabs to separate between devices' check box.
3. Click **OK**.

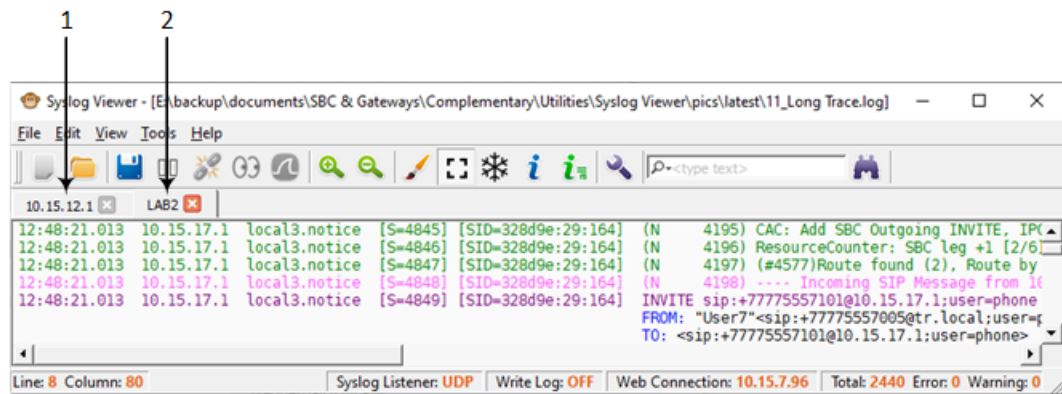


- For this feature to function, you must also disable clearing of tabs upon opening a file (see [Clearing Existing Window Tabs when Opening Syslog File](#) on page 19).
- When opening multiple syslog files, Syslog Viewer always creates a tab for each file.

Configuring Labels for Window Tabs

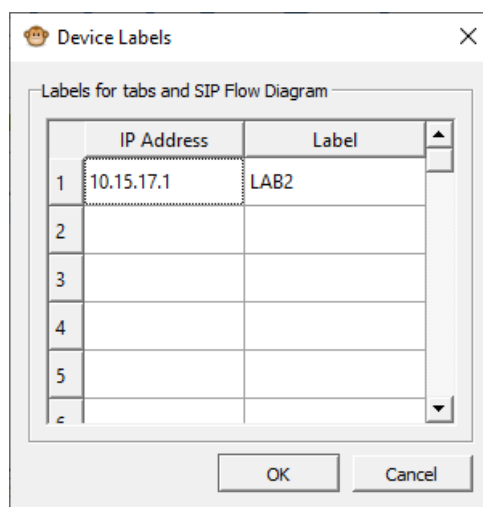
By default, Syslog Viewer displays the IP address of the device on the window tab. Instead of an IP address, you can configure any string label for a device (defined by IP address).

The following figure shows two window tabs, one displaying a device's IP address (#1) and another displaying a device's label (#2):



➤ **To configure window tab labels per device:**

1. From the Tools menu, choose **Device Labels**; the following dialog box appears:





2. Click the 'IP Address' field, and then enter the IP address of the device.
3. Click the corresponding 'Label' field, and then enter a label (string) for the device.
4. Click on any other row, and then click **OK**.

Displaying Window Tab for Syslog Messages of Single Device

By default, when you configure only one device to send syslog messages to Syslog Viewer, or only open one device's syslog file, the syslog messages are displayed in the window without a tab. If you want, you can enable Syslog Viewer to display a tab in such scenarios.

➤ **To display tab for single device:**

1. On the toolbar, click the **Clean**  icon to clear the syslog messages window.
2. On the toolbar, click the **Options**  icon; the Options dialog box appears.
3. Under the Multiple Devices group:

- a. Select the 'Use multiple tabs to separate between devices' check box.
 - b. Select the 'Always show device tab name' check box.
4. Click **OK**.




- For this feature, make sure that clearing tabs when opening a file is disabled (see [Clearing Existing Window Tabs when Opening Syslog File](#) below).
- Even if you enable this feature, Syslog Viewer creates additional tabs if necessary (e.g., syslog messages are received from an additional device, or you filter the display).

Clearing Existing Window Tabs when Opening Syslog File

By default, Syslog Viewer closes all existing window tabs when you open a syslog file. However, you can keep all existing tabs when opening a file.

➤ To enable / disable tab clearing upon opening file:


1. On the toolbar, click the **Options**  icon; the Options dialog box appears.
2. Under the Miscellaneous group, select the 'Clear tabs on file open' check box to clear existing tabs when opening a file, or clear the check box to keep existing tabs.
3. Click **OK**.

Sorting Window Tabs

You can enable Syslog Viewer to arrange (sort) multiple tabs in ascending order. For example, if you have open syslog files `syslog-sbc_10.15.7.97.txt`, `syslog-sbc_10.15.7.96.txt`, and `syslog-sbc_10.15.7.98.txt`, the tabs are also arranged in this order:

- `syslog-sbc_10.15.7.96.txt`
- `syslog-sbc_10.15.7.97.txt`
- `syslog-sbc_10.15.7.98.txt`

➤ To enable tab sort of opened files:

1. On the toolbar, click the **Options**  icon; the Options dialog box appears.
2. Under the Miscellaneous group, select the 'Sort opened files' check box.
3. Click **OK**.

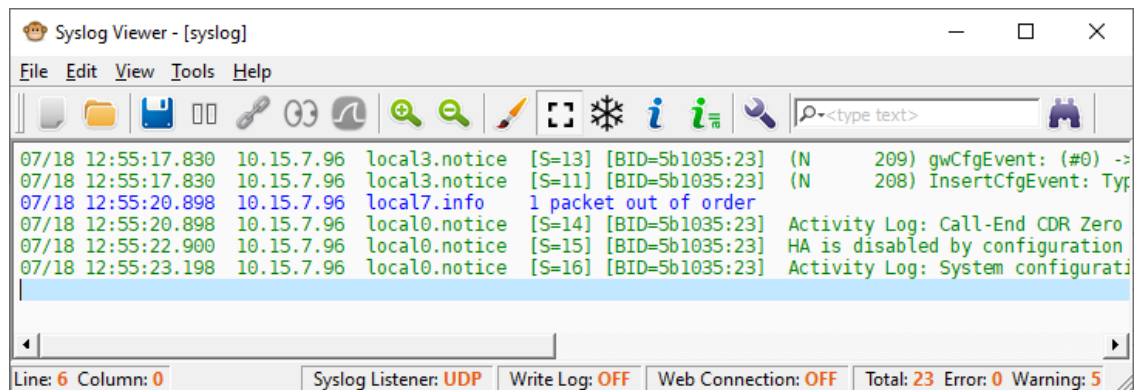
Detecting Missing and Out-Of-Order Logs

Syslog Viewer keeps track of sequence numbers for incoming syslog messages. If Syslog Viewer detects missing or out-of-order messages, it generates "syslog.error" errors, for example:

12:45:49.057 10.4.219.224 syslog.error 10 messages are missing


Syslog Viewer also automatically handles packet reordering, using a variation of jitter buffer algorithm. Packet reordering should function smoothly, except for the first few messages from the specific source.

The following figure shows an example of a packet order issue (S=13, then S=11, and then S=14):



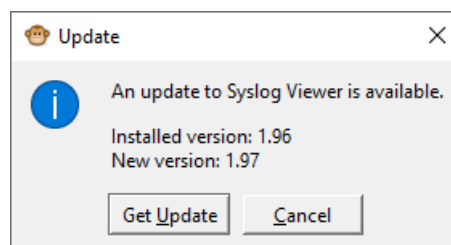
If you experience a degradation in the performance of Syslog Viewer, disable this feature.

➤ To disable packet recorder compensation mechanism:

1. On the toolbar, click the **Options**  icon; the Options dialog box appears.
2. Under the Syslog group, clear the 'Compensate for packet recorder' check box.
3. Click **OK**.

Checking for Syslog Viewer Updates

By default, whenever you start Syslog Viewer, it checks for a new software update. If there is an update, you are prompted to download and install it, as shown in the following example:




Simply click **Get Update** to download and install.



To enjoy the latest Syslog Viewer features, it's recommended to keep this feature enabled.

➤ **To enable or disable checking for updates:**

1. On the toolbar, click the **Options**  icon; the Options dialog box appears.
2. Under the Miscellaneous group, select or clear the 'Check new version' check box to enable or disable this feature, respectively.
3. Click **OK**.

5 Collecting Syslog Messages Methods

Syslog Viewer allows you to collect syslog messages in various ways:

- Collect syslog messages directly from AudioCodes devices – see [Collecting Syslog Messages Directly from Devices](#) below
- Use Wireshark to capture syslog messages - see [Using Wireshark to Capture Packets for Syslog Viewer](#) on page 27
- Collect syslog messages from a syslog file written in realtime ('tail -f' like) by a third-party Syslog server – see [Realtime Monitoring of Syslog File by External Syslog Sever](#) on page 28

Collecting Syslog Messages Directly from Devices

Syslog Viewer offers two methods for collecting syslog messages from devices:

- Configuring device to send syslog messages to Syslog Viewer (server) - see [Configuring Devices to Send Syslog Messages](#) below
- Connecting Syslog Viewer to device's web interface - see [Collecting Syslog Messages from Device's Web Interface](#) on page 25

Configuring Devices to Send Syslog Messages

The recommended method for collecting syslog messages from a device is to configure the device to send syslog messages to the computer on which Syslog Viewer is installed. This method uses the syslog protocol (e.g., over UDP).



- If communication isn't possible (i.e., not routable) between the device and the computer on which Syslog Viewer is installed (e.g., due to a firewall or NAT devices in the middle), you can use the Web Connect feature, whereby Syslog Viewer collects syslog messages from the device's Web interface (see [Collecting Syslog Messages from Device's Web Interface](#) on page 25).
- You can configure multiple devices to send syslog messages to Syslog Viewer.

Configuring Syslog Server on Device

The following procedure describes how to configure the device to send syslog messages to the computer on which Syslog Viewer is installed.

➤ Configuring syslog server on device:

1. Log in to the device's Web interface.
2. Enable syslog:
 - a. Open the Logging Settings page (**Troubleshoot** menu > **Troubleshoot** tab > **Logging** folder > **Logging Settings**).

- b. From the 'Enable Syslog' drop-down list, select **Enable**:

Enable Syslog • Enable ▼

- c. Click **Apply**.

3. Configure the syslog message debug level:

- a. Open the Logging Settings page (**Troubleshoot** menu > **Troubleshoot** tab > **Logging** folder > **Logging Settings**).

- b. From the 'VoIP Debug Level' drop-down list, select **Detailed**:

VoIP Debug Level • Detailed ▼

- c. Click **Apply**.

4. Configure the address of the computer on which Syslog Viewer is installed:

- a. Open the Syslog Servers page (**Troubleshoot** menu > **Troubleshoot** tab > **Logging** folder > **Syslog Servers**).

Syslog Servers - x

GENERAL	
Index	<input type="text" value="0"/>
Address	<input style="background-color: #ffffcc;" type="text" value="10.13.2.3"/>
Port	<input type="text" value="514"/>
Protocol	<div style="border: 1px solid #ccc; padding: 2px;">UDP ▼</div>
Interface	<div style="border: 1px solid #ccc; padding: 2px;">#0 [O+M+C] ▼ View</div>
Information Type	<div style="border: 1px solid #ccc; padding: 2px;">All ▼</div>
Severity Level	<div style="border: 1px solid #ccc; padding: 2px;">Notice ▼</div>
Mode	<div style="border: 1px solid #ccc; padding: 2px;">Enable ▼</div>

- b. Click **New**, and then do the following:

- ◆ In the 'IP Address' field, enter the IP address of the computer on which Syslog Viewer is installed.
- ◆ In the 'Port' field, enter the port that Syslog Viewer listens to for syslog messages (default is 514). You can change Syslog Viewer's listening port, as described in [Configuring Syslog Viewer's Listening Port and Interface](#) on the next page.
- ◆ From the 'Transport Protocol' drop-down list, select the listening port's transport protocol. You can define Syslog Viewer's transport protocol, as described in [Configuring Syslog Viewer's Listening Port and Interface](#) on the next page.
- ◆ From the 'Interface' drop-down list, select one of the device's local IP Interfaces through which it sends syslog.

- ◆ From the 'Severity Level' drop-down list, select the minimum severity level of messages that you want sent to Syslog Viewer.



It's recommended to leave the syslog severity level at default (i.e., **Notice**) to prevent excessive utilization of the device's resources. Changing severity level is typically done only by AudioCodes Support for debugging.

- ◆ From the 'Mode' drop-down list, select **Enable** to enable this syslog setting.

- c. Click **Apply**.

5. On the toolbar, click **Save** to save your settings to the device's flash memory.

Configuring Syslog Viewer's Listening Port and Interface

By default, Syslog Viewer listens on UDP port 514 of the computer or machine on which it's installed. By default, Syslog Viewer also listens on all interfaces if the computer or machine has more than one NIC, for example.

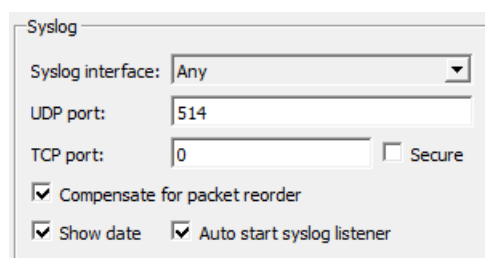
You can configure a secure syslog connection using TLS. By default, when TLS is enabled, Syslog Viewer uses the device's default self-signed certificate (TLS Context #0). However, if you want to use a non-default TLS certificate, you need to configure it on the device and on Syslog Viewer.



- Syslog Viewer (starting from Version 1.50) can collect syslog messages over TLS.
- You can receive syslog messages from the same IP address with two different transport protocols - one through UDP and the other through TCP/TLS. On the device, use the Syslog Servers table to configure two rows, one for UDP and one for TCP/TLS.

➤ To configure Syslog Viewer's listening port:

1. On the toolbar, click the **Options**  icon; the Options dialog box appears.



Syslog

Syslog interface: Any

UDP port: 514

TCP port: 0 ☐ Secure

☒ Compensate for packet reorder

☒ Show date ☐ Auto start syslog listener

2. Under the Syslog group, do the following:
 - a. From the 'Syslog interface' drop-down list, select the interface that Syslog Viewer listens to.

- b. In the 'UDP port' or 'TCP port' fields, enter the UDP or TCP port (respectively) that Syslog Viewer listens to.
 - c. If you want a secured (TLS) syslog connection, in the 'TCP port' field, enter the secured listening port, and then select the 'Secure' check box.
3. If you are using TLS and want to use a non-default TLS certificate, then after configuring the TLS port in Step 2.c, under the Secure group, do the following:

Secure Mode

Private key: ...

Certificate: ...

CA certificate: ...

- a. In the 'Private key' field, click the ellipsis (...) button, and then browse to and select the TLS private key file.
- b. In the 'Certificate' field, click the ellipsis (...) button, and then browse to and select the TLS certificate file.
- c. In the 'CA certificate' field, click the ellipsis (...) button, and then browse to and select the Certificate Authority (CA) file.



You must configure the device with a TLS Context that includes these non-default TLS certificates.

4. Click **OK**.

Collecting Syslog Messages from Device's Web Interface

Instead of configuring the device to send syslog messages, you can configure Syslog Viewer to connect to the device's Web interface and collect the messages from there.

This method is useful when Syslog Viewer is not routable from the device. For example, when the device is located behind NAT.

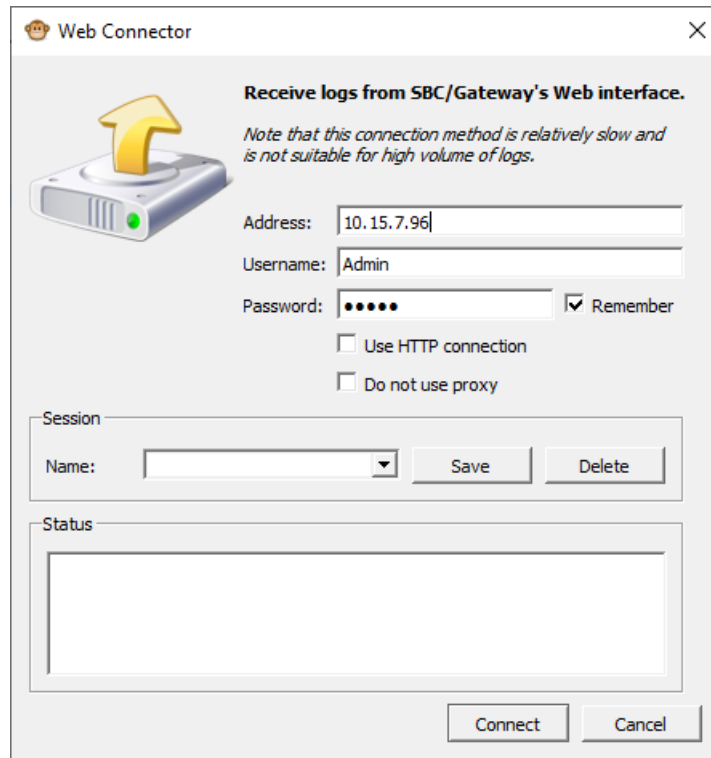
Syslog Viewer can connect to the device's Web interface using the device's IP address or hostname (if applicable). By default, Syslog Viewer connects over HTTPS (port 443), but you can change this to HTTP (port 80).



- This syslog collection method is not recommended and especially not suitable when the device sends a high volume of syslog messages. The recommended method is described in [Configuring Devices to Send Syslog Messages](#) on page 22.
- Collecting syslog messages from the Web interface is not supported by AudioCodes MP-1xx devices.
- No device configuration is required for this connection method.

➤ To connect Syslog Viewer to device's Web interface:

1. On the toolbar, click the **Connect To**  icon; the following dialog box appears:



The 'Web Connector' dialog box is titled 'Web Connector' and features a close button (X) in the top right corner. It contains a yellow arrow icon pointing upwards from a server icon. The main heading is 'Receive logs from SBC/Gateway's Web interface.' Below this is a note: 'Note that this connection method is relatively slow and is not suitable for high volume of logs.' The form includes fields for 'Address' (containing '10.15.7.96'), 'Username' (containing 'Admin'), and 'Password' (masked with dots). There is a 'Remember' checkbox which is checked. Below these are two unchecked checkboxes: 'Use HTTP connection' and 'Do not use proxy'. A 'Session' section contains a 'Name' field with a dropdown arrow, and 'Save' and 'Delete' buttons. A 'Status' section is a large empty text area. At the bottom are 'Connect' and 'Cancel' buttons.



The 'Do not use proxy' check box is reserved for future implementation.

2. In the 'Address' field, enter the device's address (IP address or FQDN).
3. In the 'Username' and 'Password' fields, enter the device's login credentials.
4. If you want Syslog Viewer to remember your settings, select the 'Remember' check box.
5. If you want to connect over HTTP instead of HTTPS, select the 'Use HTTP connection' check box.
6. If you want to save this specific connection setting for future use, under the Session group, in the 'Name' field, enter any easily identifiable name, and then click **Save**. The next time you want to use this connection setting, simply choose the name from the 'Name' drop-down list.
7. Click **Connect**; Syslog Viewer connects to the device's Web interface and the syslog window displays "connected to <device's address>". Syslog Viewer can now collect syslog messages from the device.



To disconnect Syslog Viewer from the device, on the toolbar, click the **Disconnect From** icon. The syslog window displays "disconnected by user".

Using Wireshark to Capture Packets for Syslog Viewer

You can use Wireshark (through Syslog Viewer) to capture syslog messages instead of (or in addition to) using Syslog Viewer to listen on the UDP/TCP port. Wireshark is used only to capture the syslog messages; everything else is done on Syslog Viewer (e.g., displaying and filtering messages).

Using Wireshark is useful because Syslog Viewer can't listen to the same UDP/TCP port (514) that a third-party syslog server (or another instance of Syslog Viewer) running on your computer is currently using to capture the syslog messages. In addition, you may have multiple people using the same computer and running multiple syslog server instances.

To overcome this, you can use Syslog Viewer as follows:


- Start two instances of Syslog Viewer, where one instance listens to port 514 "normally", and the other instance uses Wireshark to listen to the same port.
- Have a third-party syslog server listen to port 514, start Syslog Viewer and trigger it to use Wireshark to listen (capture) the messages on the same port.

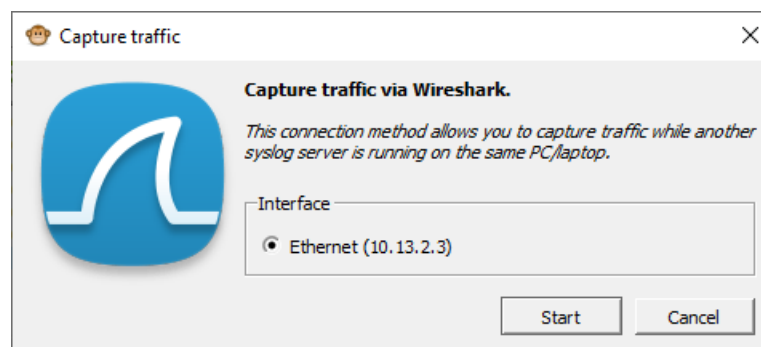
It also supports extracting logs from IP Trace debug capture stream (i.e., you can keep the device sending syslog to the "normal" destination (not your PC) and temporarily send IP Trace debug captures to your PC for some quick debugging.



You must have Wireshark installed on your computer.

➤ To view syslog messages in Wireshark:

1. On the toolbar, click the **Network Capture (via Wireshark)**  icon; the following appears:



2. Under the Interface group, select the interface (if more than one NIC exists on your computer).

3. Click **Start**; the 'Syslog Listener' field on the status bar displays "Wireshark". Wireshark starts capturing syslog messages and Syslog Viewer displays them.
4. To stop using Wireshark with Syslog Viewer, on the toolbar, click the **Stop Network**

Capture  icon.

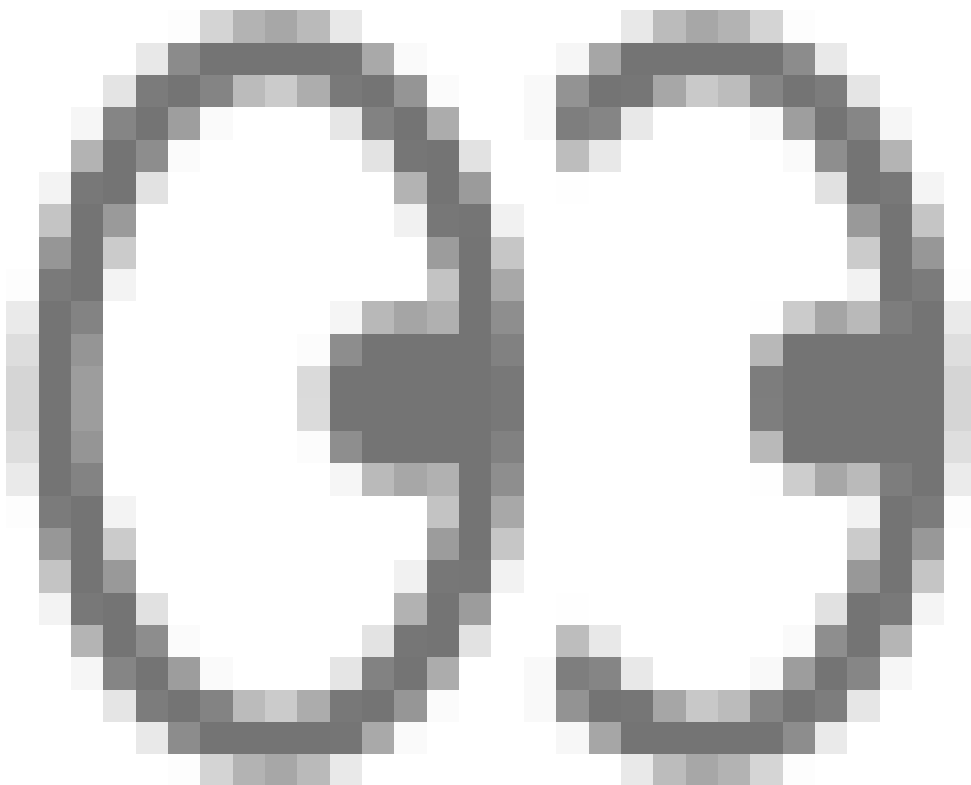
Realtime Monitoring of Syslog File by External Syslog Sever

Syslog Viewer's File Monitor feature is like Linux "tail -f" command. It's useful if you have an external syslog server running on your computer (e.g., NXLog) that writes syslog files, and you simply want to monitor them in real-time using Syslog Viewer.

Syslog Viewer opens the file, detects if any new syslog messages have been added and displays them. It also detects if the file gets rotated and opens the new written file (current file) to continue proper monitoring.

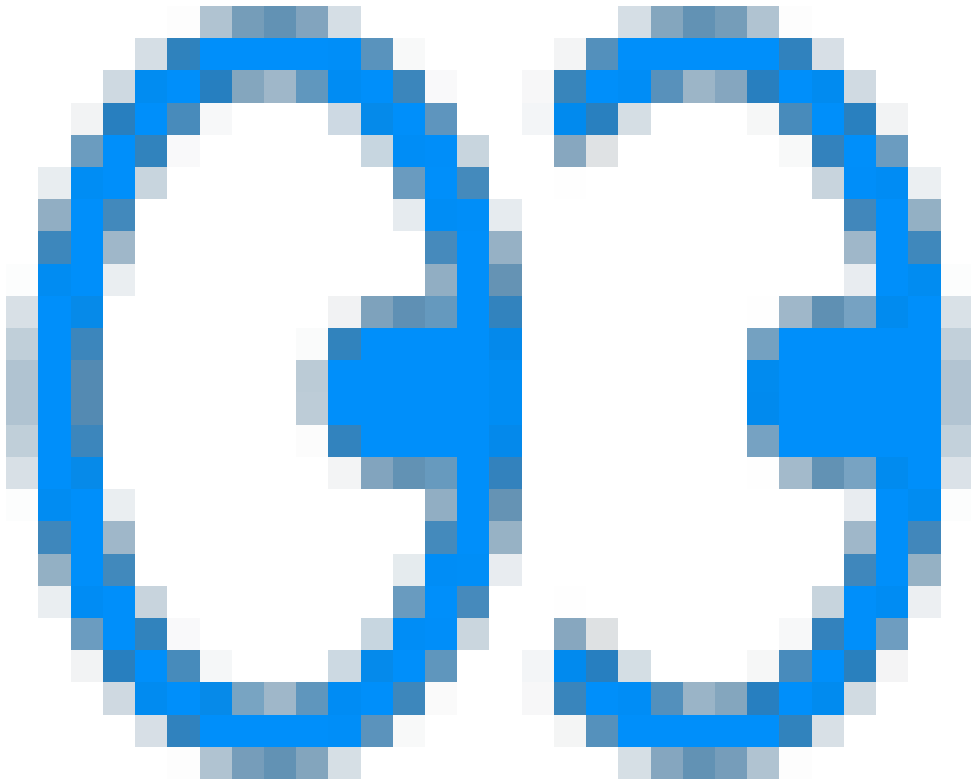
➤ To use file monitor:

1. On the toolbar, click the **File Monitor (tail -f)**



icon; an open file dialog box appears.

2. Browse to and select the syslog file written by the third-party syslog server; Syslog Viewer now displays the syslog messages of the selected file.
3. To stop the File Monitor, on the toolbar, click the **Stop File Monitor**



icon.

6 Viewing Syslog Messages



This section describes the ways you can view Syslog Messages in Syslog Viewer.

Viewing Real-time Collection of Syslog Messages

Once you have set up Syslog Viewer to collect syslog messages (see [Collecting Syslog Messages Methods](#) on page 22), syslog messages are automatically displayed in the window as they are sent by the device.

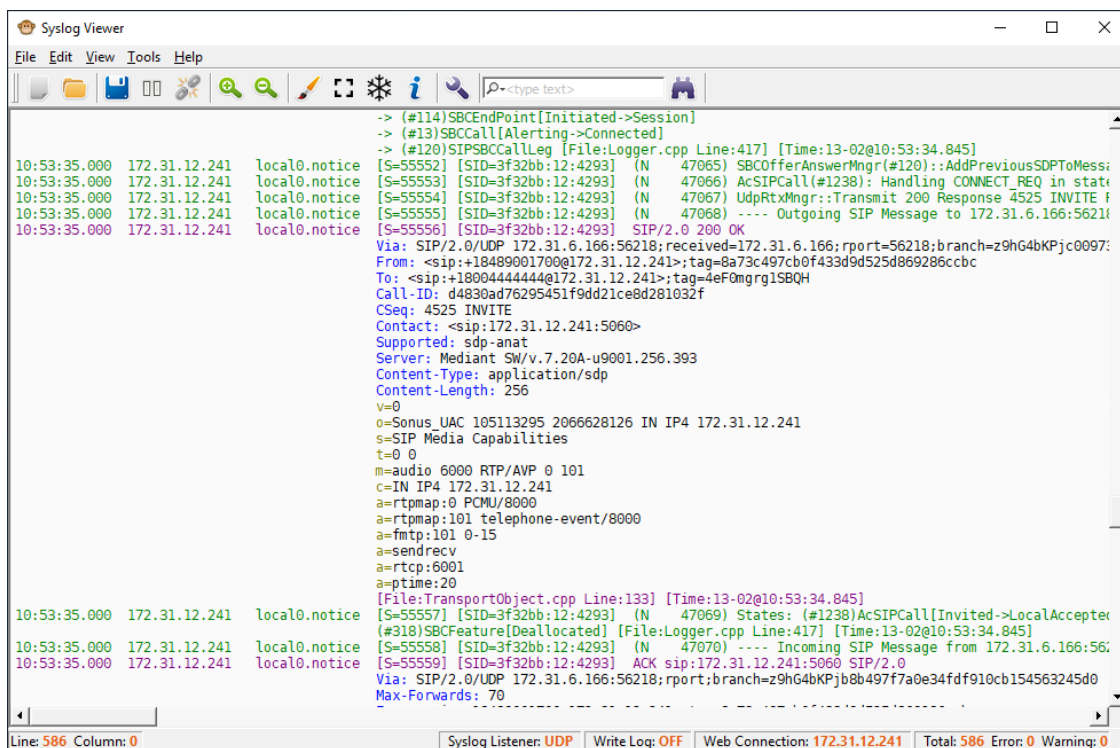
Syslog Viewer automatically formats the syslog messages for easy reading of SIP messages. Messages with warning severity level are displayed in magenta and messages with errors are displayed in red.

➤ To start and stop collecting syslog messages:

1. Make a few calls or perform configuration or management actions on the device. For example, configure a parameter or restart the device; Syslog Viewer collects and displays the syslog messages, including sent and received SIP messages. The 'Syslog Listener' field on the status bar displays "UDP" or "TCP", indicating the transport protocol over which the syslog messages are being collected.
2. To pause collection of syslog messages, on the toolbar, click the **Pause**  icon. The 'Syslog Listener' field on the status bar displays "OFF".
3. To resume collection of syslog messages, on the toolbar, click the **Play**  icon.

The following figure shows an example of a collected syslog message that's a SIP call:

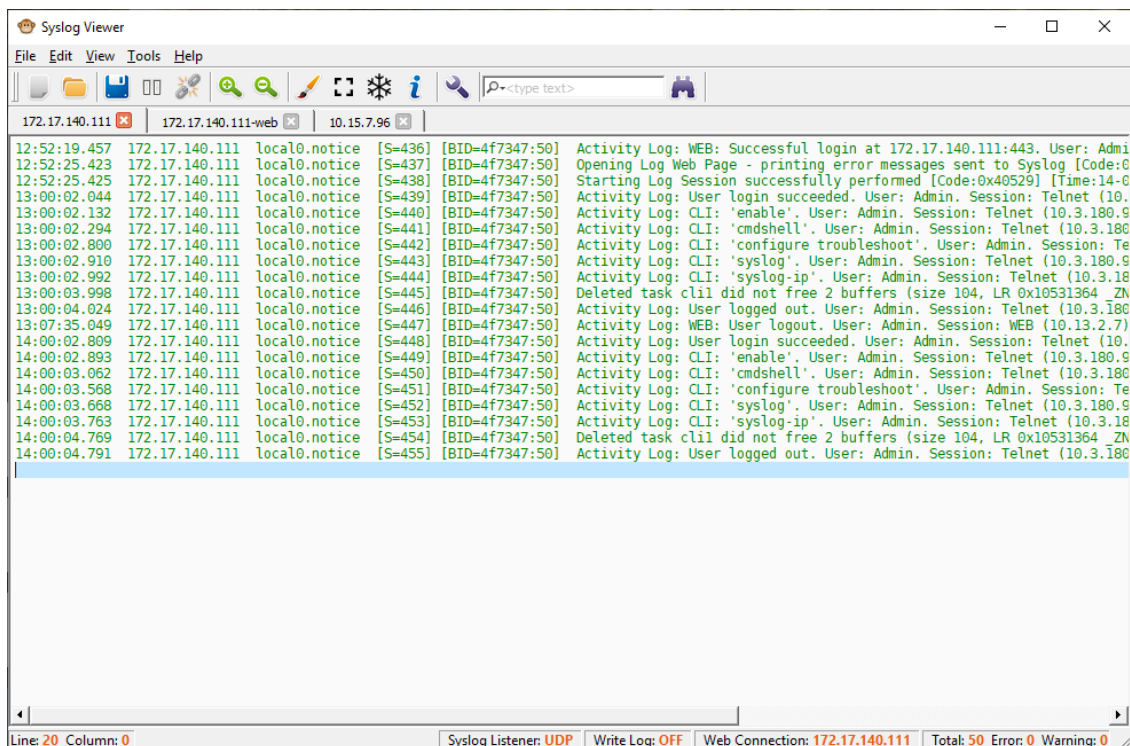
Figure 6-1: SIP Call



```
-> (#114)SBCEndPoint[Initiated->Session]
-> (#13)SBCCall[Alerting->Connected]
-> (#120)SIPSBCCallLeg [File:Logger.cpp Line:417] [Time:13-02@10:53:34.845]
10:53:35.000 172.31.12.241 local0.notice [S=55552] [SID=3f32bb:12:4293] (N 47065) SBCCofferAnswerMngr(#120)::AddPreviousSDPToMess;
10:53:35.000 172.31.12.241 local0.notice [S=55553] [SID=3f32bb:12:4293] (N 47066) AcSIPCall(#1238)::Handling CONNECT_REQ in state
10:53:35.000 172.31.12.241 local0.notice [S=55554] [SID=3f32bb:12:4293] (N 47067) UdpRtxMngr::Transmit 200 Response 4525 INVITE f
10:53:35.000 172.31.12.241 local0.notice [S=55555] [SID=3f32bb:12:4293] (N 47068) ---- Outgoing SIP Message to 172.31.6.166:56218
10:53:35.000 172.31.12.241 local0.notice [S=55556] [SID=3f32bb:12:4293] SIP/2.0 200 OK
Via: SIP/2.0/UDP 172.31.6.166:56218;received=172.31.6.166;rport=56218;branch=z9hG4bKPjc0097
From: <sip:+18489001700@172.31.12.241>;tag=8a73c497cb0f433d9d525d869286ccbc
To: <sip:+18004444444@172.31.12.241>;tag=4eF0mrg1SBQH
Call-ID: d4830ad76295451f9dd21ce8d281032f
CSeq: 4525 INVITE
Contact: <sip:172.31.12.241:5060>
Supported: sdp-anat
Server: Mediant SW/v.7.20A-u9001.256.393
Content-Type: application/sdp
Content-Length: 256
v=0
o=Sonus_UAC 105113295 2066628126 IN IP4 172.31.12.241
s=SIP Media Capabilities
t=0 0
m=audio 6000 RTP/AVP 0 101
c=IN IP4 172.31.12.241
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
a=rtp:6001
a=ptime:20
[File:TransportObject.cpp Line:133] [Time:13-02@10:53:34.845]
10:53:35.000 172.31.12.241 local0.notice [S=55557] [SID=3f32bb:12:4293] (N 47069) States: (#1238)AcSIPCall[Invited->LocalAccepte
(#318)SBCCFeature[Deallocated] [File:Logger.cpp Line:417] [Time:13-02@10:53:34.845]
10:53:35.000 172.31.12.241 local0.notice [S=55558] [SID=3f32bb:12:4293] (N 47070) ---- Incoming SIP Message from 172.31.6.166:56
10:53:35.000 172.31.12.241 local0.notice [S=55559] [SID=3f32bb:12:4293] ACK sip:172.31.12.241:5060 SIP/2.0
Via: SIP/2.0/UDP 172.31.6.166:56218;rport=56218;branch=z9hG4bKPjb8b497f7a0e34fdf910cb154563245d0
Max-Forwards: 70
```

The following figure shows an example of a collected syslog message that's a user activity event:

Figure 6-2: Activity Log



```
172.17.140.111 172.17.140.111-web 10.15.7.96
12:52:19.457 172.17.140.111 local0.notice [S=436] [BID=4f7347:50] Activity Log: WEB: Successful login at 172.17.140.111:443. User: Admin
12:52:25.423 172.17.140.111 local0.notice [S=437] [BID=4f7347:50] Opening Log Web Page - printing error messages sent to Syslog [Code:0
12:52:25.425 172.17.140.111 local0.notice [S=438] [BID=4f7347:50] Starting Log Session successfully performed [Code:0x40529] [Time:14-0
13:00:02.044 172.17.140.111 local0.notice [S=439] [BID=4f7347:50] Activity Log: User login succeeded. User: Admin. Session: Telnet (10.
13:00:02.132 172.17.140.111 local0.notice [S=440] [BID=4f7347:50] Activity Log: CLI: 'enable'. User: Admin. Session: Telnet (10.3.180.9
13:00:02.294 172.17.140.111 local0.notice [S=441] [BID=4f7347:50] Activity Log: CLI: 'cmdshell'. User: Admin. Session: Telnet (10.3.180
13:00:02.800 172.17.140.111 local0.notice [S=442] [BID=4f7347:50] Activity Log: CLI: 'configure troubleshoot'. User: Admin. Session: Te
13:00:02.910 172.17.140.111 local0.notice [S=443] [BID=4f7347:50] Activity Log: CLI: 'syslog'. User: Admin. Session: Telnet (10.3.180.9
13:00:02.992 172.17.140.111 local0.notice [S=444] [BID=4f7347:50] Activity Log: CLI: 'syslog-ip'. User: Admin. Session: Telnet (10.3.18
13:00:03.998 172.17.140.111 local0.notice [S=445] [BID=4f7347:50] Deleted task cli did not free 2 buffers (size 104, LR 0x10531364_ZN
13:07:35.049 172.17.140.111 local0.notice [S=446] [BID=4f7347:50] Activity Log: User logged out. User: Admin. Session: Telnet (10.3.180
13:07:35.049 172.17.140.111 local0.notice [S=447] [BID=4f7347:50] Activity Log: WEB: User logout. User: Admin. Session: WEB (10.13.2.7)
14:00:02.809 172.17.140.111 local0.notice [S=448] [BID=4f7347:50] Activity Log: User login succeeded. User: Admin. Session: Telnet (10.
14:00:02.893 172.17.140.111 local0.notice [S=449] [BID=4f7347:50] Activity Log: CLI: 'enable'. User: Admin. Session: Telnet (10.3.180.9
14:00:03.062 172.17.140.111 local0.notice [S=450] [BID=4f7347:50] Activity Log: CLI: 'cmdshell'. User: Admin. Session: Telnet (10.3.180
14:00:03.568 172.17.140.111 local0.notice [S=451] [BID=4f7347:50] Activity Log: CLI: 'configure troubleshoot'. User: Admin. Session: Te
14:00:03.668 172.17.140.111 local0.notice [S=452] [BID=4f7347:50] Activity Log: CLI: 'syslog'. User: Admin. Session: Telnet (10.3.180.9
14:00:03.763 172.17.140.111 local0.notice [S=453] [BID=4f7347:50] Activity Log: CLI: 'syslog'. User: Admin. Session: Telnet (10.3.180.9
14:00:04.769 172.17.140.111 local0.notice [S=454] [BID=4f7347:50] Deleted task cli did not free 2 buffers (size 104, LR 0x10531364_ZN
14:00:04.791 172.17.140.111 local0.notice [S=455] [BID=4f7347:50] Activity Log: User logged out. User: Admin. Session: Telnet (10.3.180
```



Viewing Syslog Messages in External Text-Based Editor

You can open the currently displayed syslog by Syslog Viewer in an external (third-party) text-based editor (e.g., Notepad). Before you can do this, you need to define the path on your computer to where the editor is located.



- The text-based editor only includes syslog messages that were displayed in Syslog Viewer when it was activated. Any subsequently received syslog messages aren't added to the text-based editor.
- By default, the text-based editor uses the filename syslog.txt.

➤ To view syslog messages in external text-based editor:

1. Define the editor:
 - a. On the toolbar, click the **Options**  icon; the Options dialog box appears.
 - b. Under the Miscellaneous group, click the 'External viewer' ellipsis button (...), and then browse to and select the location of the executable file of your editor (e.g., Notepad.exe).
 - c. Click **OK**.
2. On the toolbar, click the **External Editor**  icon; the text-based editor starts and displays the syslog messages.


Viewing Syslog Messages of Saved Files

You can open and view syslog files that were saved on the computer on which Syslog Viewer is running. When opening syslog files, Syslog Viewer creates a window tab for each opened file.



- The "Syslog Listener" automatically pauses when you open a file.
- Syslog files opened from disk are displayed in "full" view (i.e., display isn't limited by scroll buffer).
- It may take a few seconds to open and load large files. Make sure that the file is fully loaded by verifying that the "Total" counter on the status bar stabilizes.
- Syslog Viewer supports the following file formats:
 - ✓ Native file format (created by Syslog Viewer)
 - ✓ Legacy file format (created by ACSyslog)
 - ✓ PCAP files (Files are automatically converted based on .pcap or .pcapng file extensions. Wireshark must be installed in %PROGRAMFILES%.)
 - ✓ Third-party syslog file formats (based on Customer inputs)

➤ **To open a saved syslog file:**

- On the toolbar, click the **Open**  icon, and then browse to and select the syslog file.

--or--

- Drag-and-drop the syslog file into Syslog Viewer's window.

If the loaded file contains logs from multiple devices, Syslog Viewer creates a window tab for each device and displays the logs of each device under their respective window tab.

Viewing Syslog Messages from Clipboard

You can copy syslog messages from any application (e.g., email) to your clipboard, and then paste it directly into the Syslog Viewer window.



Prior to copying-and-pasting from clipboard, you must clean the buffer.


Clearing Display of Syslog Messages

You can clear the window of displayed syslog messages. If there are multiple window tabs, all the tabs and their syslog messages are cleared.



If you are capturing syslog messages from a device, clearing syslog messages doesn't pause the receipt of syslog messages. Once cleared, newly received syslog messages are displayed in the window.

➤ **To clear displayed syslog messages:**

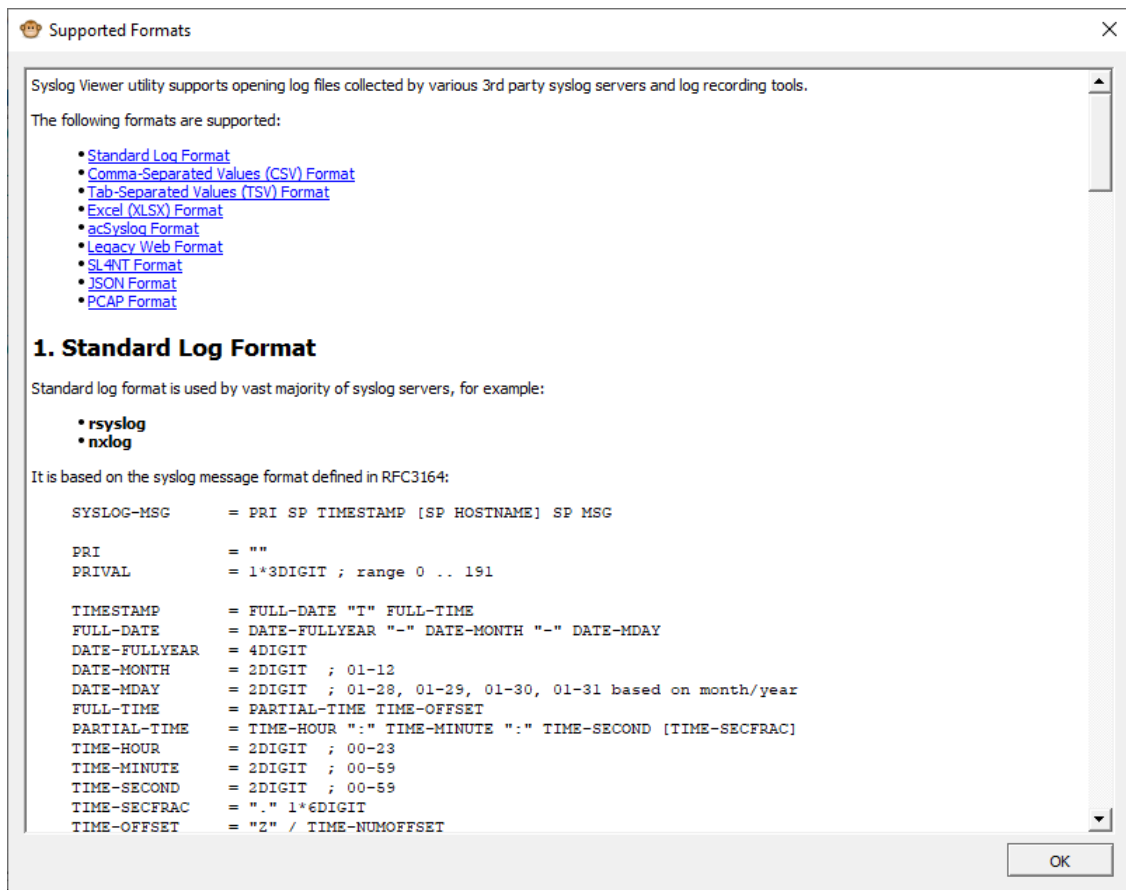
- On the toolbar, click the **Clean**  icon; all displayed syslog messages are removed from the window (and tabs, if exist).

Viewing Supported File Formats

Syslog Viewer allows you to open syslog files that were created in various file formats by third-party syslog servers and recording tools. This section describes how to check which file formats are supported and how to view examples of how Syslog Viewer displays the content of these different file formats.

➤ **To view supported file formats and display examples:**

1. From the Help menu, choose **Supported Formats**; the following pop-up window appears:



2. To view an example of how Syslog Viewer displays a file format, click the specific file type in the list.
3. Click **OK** to close the window.

7 Writing Real-time Syslog Messages to File

You can enable Syslog Viewer to write the syslog messages that are collected in realtime to a file on your computer (disk). As syslog messages are received, Syslog Viewer adds them to the file.


Before you start writing to file, Syslog Viewer prompts you for a filename. Once Syslog Viewer starts writing to the file, it implements file rotation, as described in see [Rotating Written Syslog Files](#) below.



- If you pause the syslog (see [Collecting Syslog Messages Methods](#) on page 22), even though Syslog Viewer doesn't display subsequently received syslog messages (until resumed), it continues writing them to the file.
- Writing to the file is persistent - if you quit Syslog Viewer while writing to the file, it automatically resumes writing when you next start it.

➤ To write syslog messages to file:




1. On the toolbar, click the  icon. you're prompted to define a file name and select a folder on your computer where you want it saved.
2. Click **Save**; the icon changes to red and received syslog messages are automatically written to the file.

➤ To stop writing logs to file:

- On the toolbar, click the **Stop Writing Log**  button. If you then click this button again, logs are written to the same location.



When you first click , you're prompted for the filename and directory. For all subsequent write stops and starts, you're no longer prompted because Syslog Viewer assumes that you are writing to the same file. If you want to change the file name and location, activate write logs from the File menu > **Write Log As**.

Rotating Written Syslog Files

When you write syslog messages to a file (see [Writing Real-time Syslog Messages to File](#) above), Syslog Viewer implements a file rotation mechanism.

In file rotation, when the file to which Syslog Viewer is currently writing (current file) reaches a user-defined size (in Mbytes), it stops writing to the file, saves it with a different name, and then immediately starts writing to a newly created file with the same original filename. Syslog Viewer renames rotated (old) files using a sequential index, which is added to the file's original name (<filename>_<seq. no.>.txt).

The following example explains file rotation and assumes that you have named the file `syslog-sbc.txt`:

1. First written (current) file: `syslog-sbc.txt`.
2. First file rotation: Syslog Viewer stops writing to `syslog-sbc.txt`, renames it `syslog-sbc_0000.txt`, and then starts writing to a newly created file called `syslog-sbc.txt`.
3. Second file rotation: Syslog Viewer stops writing to `syslog-sbc.txt`, renames it `syslog-sbc_0001.txt`, and then starts writing to a newly created file called `syslog-sbc.txt`.
4. Third file rotation: Syslog Viewer stops writing to `syslog-sbc.txt`, renames it `syslog-sbc_0002.txt`, and then starts writing to a newly created file called `syslog-sbc.txt`.
5. and so on ...


You can also define the maximum number of rotated files. When the total number of rotated files exists, Syslog Viewer performs file rotation from the beginning. For example, assume that you have configured the maximum number of files to 2 and the current file is `syslog-sbc.txt`:

1. First written (current) file: `syslog-sbc.txt`.
2. First file rotation: Syslog Viewer stops writing to `syslog-sbc.txt`, renames it `syslog-sbc_0000.txt`, and then starts writing to a newly created file called `syslog-sbc.txt`.
3. Second file rotation: Syslog Viewer stops writing to `syslog-sbc.txt`, renames it `syslog-sbc_0001.txt`, and then starts writing to a newly created file called `syslog-sbc.txt`.
4. Third file rotation: Syslog Viewer stops writing to `syslog-sbc.txt`, renames it `syslog-sbc_0000.txt` (overwriting `syslog_0000.txt` in Step 2, and then starts writing to a newly created file called `syslog-sbc.txt`.



The current file (to where syslog messages are currently written) always has the original filename that you specified (e.g., `syslog-sbc.txt`).

➤ **To configure log file rotation:**

1. On the toolbar, click the **Options**  icon; the Options dialog box appears.
2. Under the Log File group, configure the following:
 - In the 'File size' field, enter the size of the file (in Mbytes) after which file rotation occurs.



If you configure 'File size' to 0, file rotation is disabled and the current (initial) file increases endlessly.

- In the 'Number of files' field, enter the maximum number of rotated files.



If you configure 'Number of files' to 0, the number of rotated files is unlimited. Instead of a sequential index, a timestamp (YYYY-MM-DD_HH-MM-SS-MS, where MS is msec) is used in the filename (e.g., syslog-sbc_2023-07-27_14-40-25-843.txt).

- If you want the current file (e.g., syslog-sbc.txt) to be rotated whenever you click the



Write Log icon, select the 'Start with new file' check box.


3. Click **OK**.

Enabling Dedicated Syslog Files per Device

You can enable Syslog Viewer to write syslog messages of each device to dedicated files. The name of each file includes the device's IP address. For example, syslog files of devices 10.15.7.96 and 10.15.7.90 are named syslog-sbc_10.15.7.96.txt and syslog-sbc_10.15.7.90.txt, respectively.

If you have configured multiple devices to send syslog messages to your computer and you have disabled this feature, Syslog Viewer writes the syslog messages from all these devices to the same syslog file.

➤ To enable dedicated syslog files per device:

1. On the toolbar, click the **Options**  icon; the Options dialog box appears.
2. Under the Multiple Devices group, select the 'Create separate log files for each device' check box.
3. Click **OK**.

Creating Dedicated Folders per Device

You can enable Syslog Viewer to save written syslog files of each device in dedicated folders. Syslog Viewer automatically creates a folder for the device. The name of the folder is the IP address of the device. For example, syslog files of devices 10.15.7.96 and 10.15.7.90 are saved in folders "10.15.7.96" and "10.15.7.90", respectively.

➤ To enable dedicated folders per device:

1. On the toolbar, click the **Options**  icon; the Options dialog box appears.

2. Under the Multiple Devices group, select the 'Store logs of each device in separate directory' check box.
3. Click **OK**.

8 Saving Displayed Syslog Messages

This section describes how you can save or copy the displayed syslog messages.

Saving Displayed Syslog Messages to File

You can save the currently displayed syslog messages to a file on your computer. By default, Syslog Viewer names the file `syslog.txt`. Unlike writing to file where Syslog Viewer continuously adds new syslog messages to file as they are collected, saving syslog messages is a one-time operation.

➤ **To save displayed syslog messages to file:**

1. From the File menu, choose **Save As**.
2. Browse to the folder where you want to save the file, enter a file name, and save.

Copying Displayed Syslog Messages to Clipboard

You can easily select the entire syslog. This may be useful if you want to copy it to your clipboard for pasting it into another application (e.g., email).

➤ **To select entire log:**

1. In the syslog, right-click, and then from the shortcut menu, choose **Select All**.
2. Copy the syslog messages to your clipboard, by pressing the Ctrl+C key combination.
3. Paste the copied syslog messages into the desired application (e.g., email).


9 Searching Syslog Messages

Syslog Viewer provides you various tools for searching the syslog.

Searching for Strings


You can search for strings in the syslog. You can use various criteria such as case sensitive, whole words only, and regular expressions (regex).

➤ **To search for a string:**

1. On the toolbar, in the search field, click the magnifying glass  button, and then from the drop-down list, choose any of the following options:
 - **Case Sensitive:** Search string is case sensitive.
 - **Whole Words Only:** Searches for the whole string (not parts of it).
 - **Use Regular Expressions:** Searched string is a regex. For example, the regex "(Outgoing|Incoming) SIP" searches for all occurrences of "Outgoing SIP" and "Incoming SIP".
 - **Unfiltered Completion:** If not selected, when you start typing a search string, a drop-down list appears, offering you suggestions of previously typed search strings with the same typed letters, as shown in the following example:



If you select this option (check mark), regardless of what you type, the drop-down list includes all your previous search strings.

2. In the search field, enter the string or regex.
3. Click **Find Next**  icon (or Shift + F3 for find previous).

Searching for a Syslog Message Line

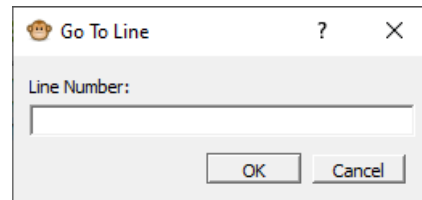
You can search for a specific line in the syslog. When you search for a line, Syslog Viewer automatically scrolls to the line and highlights it so that you can easily identify the line.



The first line in the Syslog is 0.

➤ **To search for a line:**

1. From the Edit menu, choose **Go To Line**; the following dialog box appears:



2. In the 'Line Number' field, enter the line that you want to search for.
3. Click **OK**.

10 Highlighting and Editing Syslog Messages

Syslog Viewer provides you with various tools to easily identify parts of the syslog, by highlighting them.

Highlighting Syslog Messages by Keywords

To easily identify specific strings in the syslog, you can configure keyword strings and assign each a color. The entire row in which the keyword occurs is highlighted in the assigned color. For example, if you want to easily identify SIP BYE messages, you can configure the keyword string "BYE" and assign it the color red.



You can also use regular expressions (regex) to define keywords. For example, the following regex-based keyword highlights rows containing "Incoming SIP Message" and rows containing "Outgoing SIP Message": (Incoming|Outgoing) SIP Message

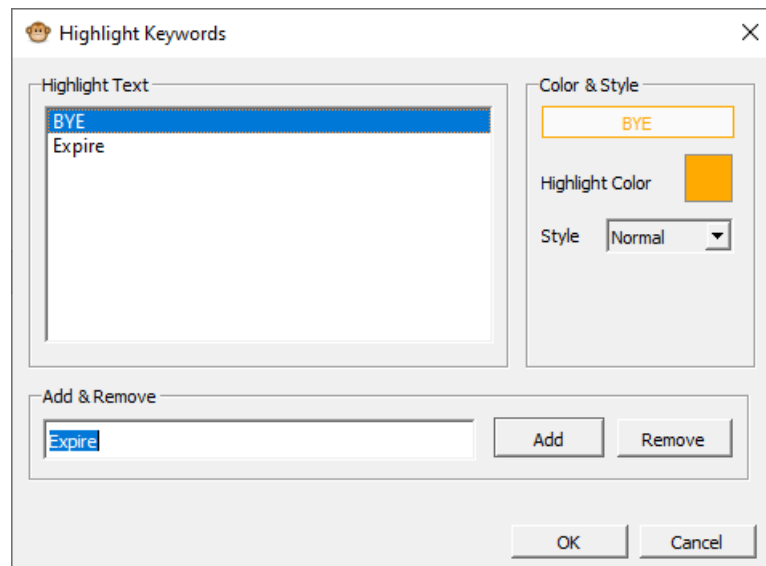
➤ To configure highlighted keywords:

1. From the Tools menu, choose **Highlight Keywords**; the Highlight Keywords dialog box opens.
2. In the 'Add & Remove' field, type the string (keyword) that you want highlighted, and then click **Add**; the string is listed under the Highlight Text group.
3. To add more keyword strings, repeat Step 2.



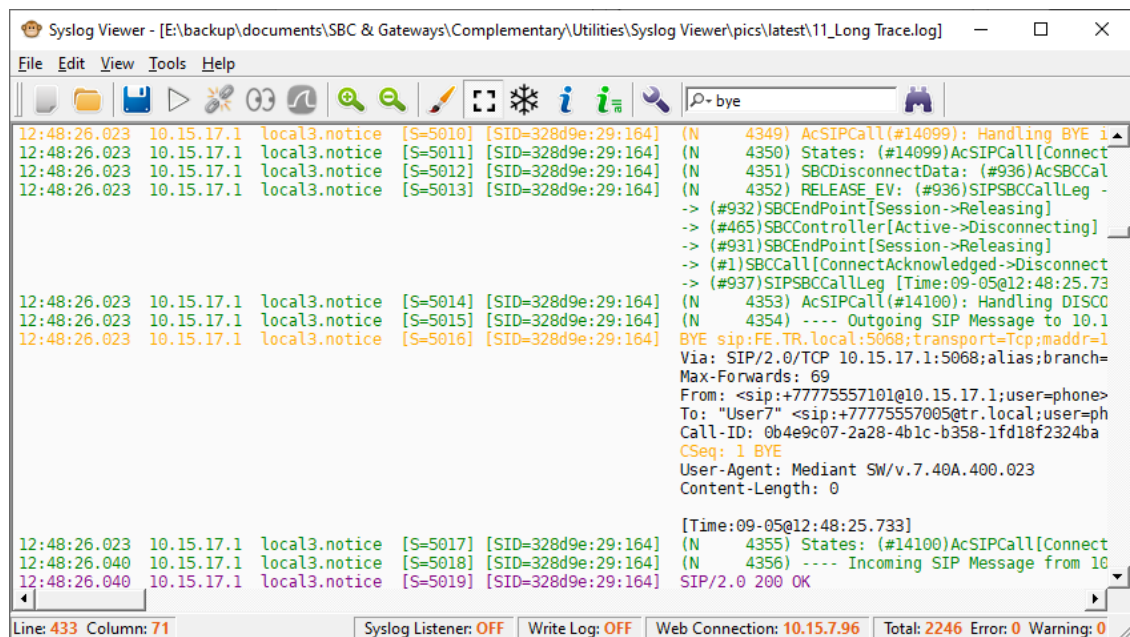
The keyword is case-sensitive.

4. In the Highlight Text list, select the string that you added.
5. Under the Color & Style group, click the 'Highlight Color' pallet, choose the desired color, and then click **OK**; the color is assigned to the keyword and a preview is displayed under the Color & Style group, as shown in the following example ("BYE"):



The 'Style' field is reserved for future implementation.

6. To assign highlight colors to more keyword strings that you added, repeat Step 4.
7. Click **OK**; all lines containing the keyword are highlighted in the assigned color, as shown in the following example ("BYE" in orange):



Marking Individual Syslog Message Lines

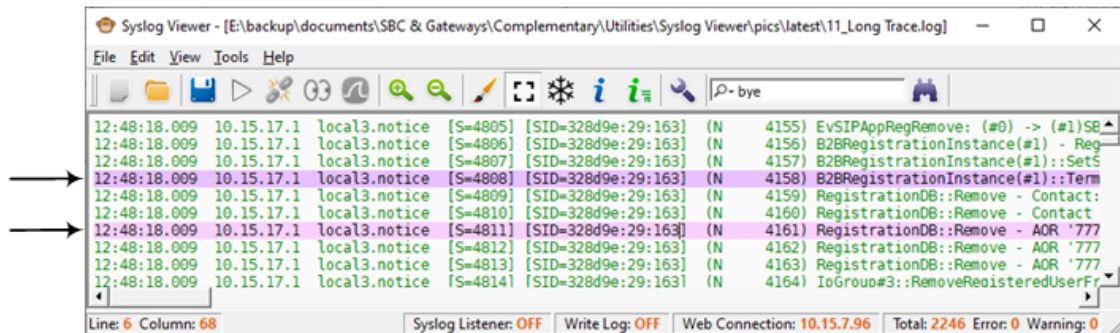
You can mark a selected line, which highlights it in purple. You can then easily navigate between marked lines.

➤ To mark lines and navigate between them:

1. In the syslog, select the line that you want to mark.

2. Right-click, and then from the shortcut menu, choose **Mark Line**.
3. To mark more lines, repeat steps 1 through 2.
4. To navigate between marked lines, right-click in the syslog, and then from the shortcut menu, choose **Next Mark** (F2) or **Previous Mark** (Shift + F2) to jump to the next mark or the previous mark, respectively.

An example of marked lines is shown in the following



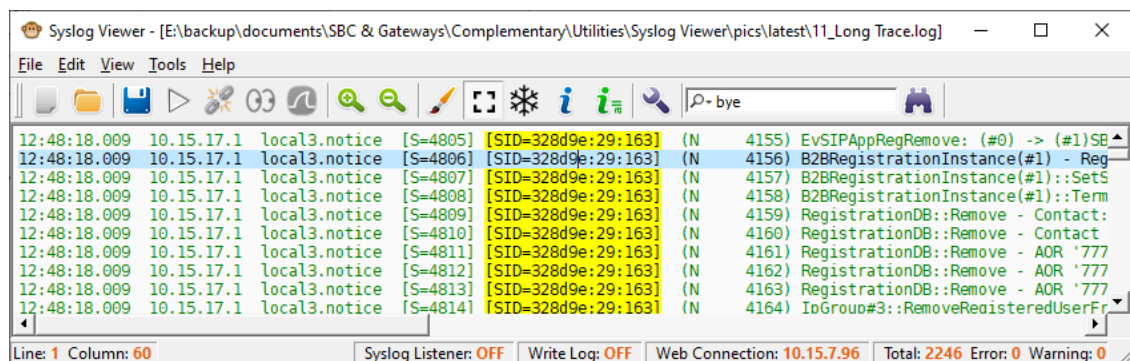
5. To unmark a line, right-click the line, and then choose **Unmark Line**.

Highlighting SIDs in Syslog Messages

You can easily highlight (in yellow) a specific Session ID (SID). The SID is highlighted wherever it is displayed in the syslog. This may be useful to easily identify lines belonging to a specific SID.

➤ To highlight an SID:

1. In the syslog, select the line that is related to the SID that you want to highlight.
2. Right-click, and then from the shortcut menu, choose **Highlight [SID of selected line]**; all occurrences of the SID is highlighted in the syslog, as shown in the following example:



3. To remove the highlights, right-click again, and then from the shortcut menu, choose **Clear Highlight**.

Editing Syslog Messages

Syslog Viewer provides an editing mode that allows you to edit the syslog messages. For example, you may want to remove unwanted strings or lines before saving or writing them to

file.

➤ **To edit syslog messages:**

1. From the Edit menu, choose **Enable Editing**; a check mark appears next to the command, indicating that you are in editing mode.
2. Make your changes as desired.
3. Disable editing - from the Edit menu, choose **Enable Editing**; the check mark no longer appears next to the command.

11 Filtering Syslog Messages

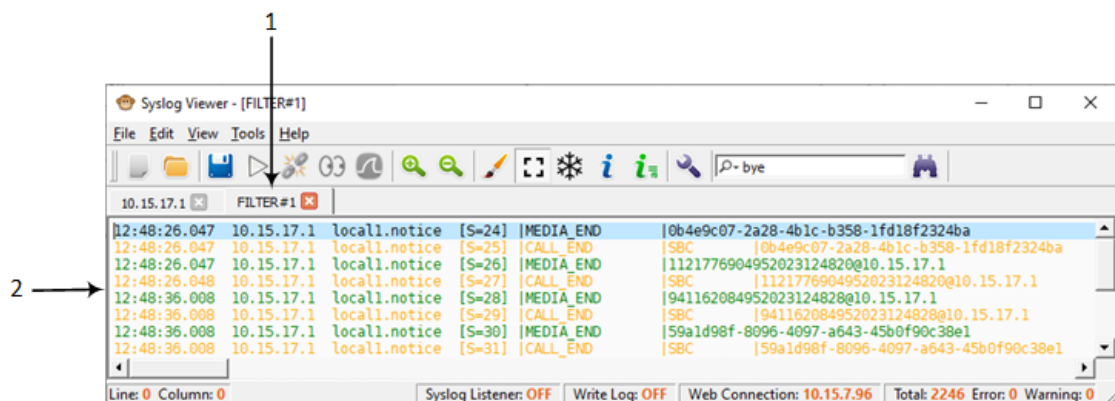
This section describes the different ways you can filter the syslog.

Filtering Display of Syslog Messages

You can filter the displayed syslog so that it displays only the following:

- CDR messages
- Messages relating to a specific session (SID)
- Messages that are non-call related (e.g., SIP REGISTER messages)
- Messages that are errors
- Messages that are warnings

When you filter the syslog, a new tab appears displaying the filtered syslog. The tag's title is in the format "FILTER#<filter number>". The following example shows a new filter tab (#1 in figure) with its filtered syslog by CDRs (#2 in figure):



You can also add a filter to an existing filter tab or create a new filter tab with both filters.

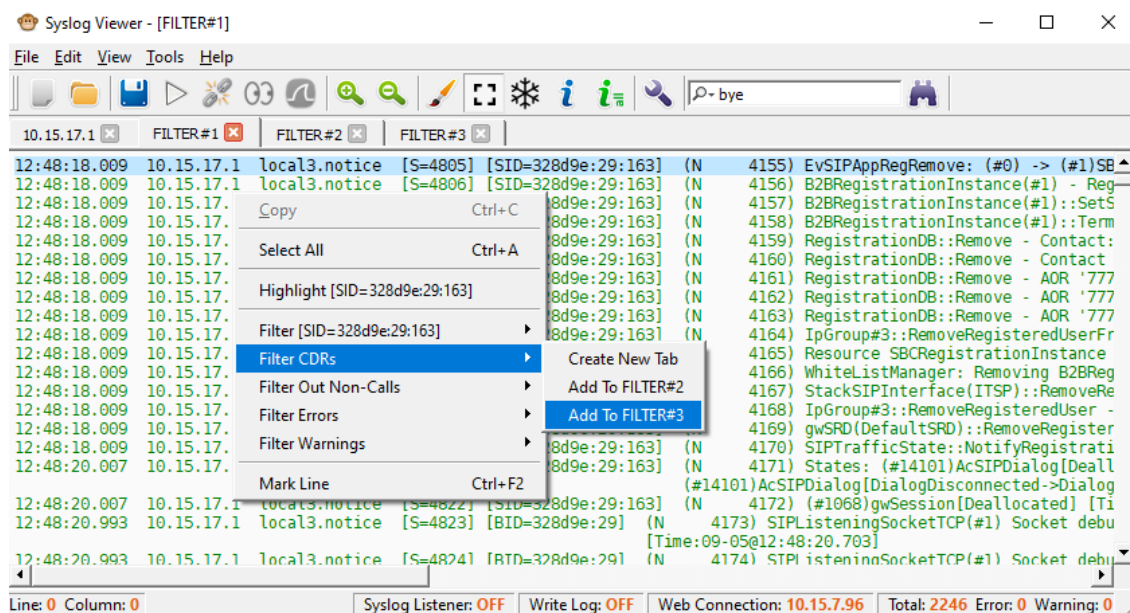
➤ To filter syslog messages:

1. In the main syslog, right-click a line; a shortcut menu appears:

Copy	Ctrl+C
Select All	Ctrl+A
Highlight [SID=328d9e:29:171]	
Filter [SID=328d9e:29:171]	
Filter CDRs	
Filter Out Non-Calls	
Filter Errors	
Filter Warnings	
Mark Line	Ctrl+F2

2. Choose one of the following options:


- **Filter [SID of selected line]:** Filters the log by the SID of the selected message. T
 - **Filter CDRs:** Filters the log by CDRs.
 - **Filter Out Non-Calls:** Filters the log by messages that are only call related.
 - **Filter Errors:** Filters the log by messages that are errors.
 - **Filter Warnings:** Filters the log by messages that are warnings.
3. You can add another filter to an existing filter tab, or create a new filter tab:
 - a. Right-click in the display; a shortcut menu appears.
 - b. From the shortcut menu, point to the desired filter, and then choose **Create New Tab** or **Add To FILTER#<filter tab>**:



Filtering Incoming Syslog Messages by Severity Level

You can filter incoming syslog messages by their severity level. For example, you can configure Syslog Viewer to accept only syslog messages with warning and emergency severity levels.

➤ To filter incoming syslog messages by severity level:

1. On the toolbar, click the **Options**  icon; the Options dialog box opens.
2. Under the Content Filter group, for 'Receive severities', select the check boxes of the corresponding syslog severity levels that you want to receive:


Receive severities: ☒ emerg ☒ alert ☒ crit ☒ error ☒ warn ☒ notice ☒ info ☒ debug

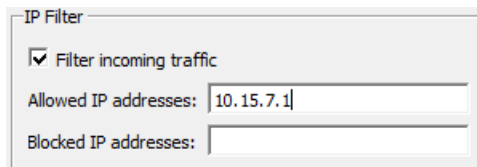
3. Click **OK**.

Filtering Incoming Syslog Messages by IP Address

You can filter incoming syslog messages by IP address(es). You can do this by defining allowed source IP addresses or blocked IP addresses.

➤ **To filter incoming traffic by IP address:**

1. On the toolbar, click the **Options**  icon; the Options dialog box opens.
2. In the IP Filter group, select the 'Filter incoming traffic' check box.
3. In the 'Allowed IP addresses' field, enter the source IP addresses that want to permit. Separate each IP address with a comma or space.
4. In the 'Blocked IP addresses' field, enter the IP addresses that you want to block. Separate each IP address with a comma or space.



IP Filter

☒ Filter incoming traffic

Allowed IP addresses: 10.15.7.1

Blocked IP addresses:

5. Click **OK**.



Define either allowed IP addresses or blocked IP addresses; not both.

Filtering Incoming Syslog Messages and Display by Content

You can filter syslog messages by the message content (i.e., not IP address, facility or severity).


You can filter I message content on the following two levels:

- Incoming traffic: Filter is applied to received syslog messages. This filter affects both the displayed log and content written to the log files.
- Log display: Filter affects only the displayed log.




You can also use regular expressions (regex) to define the message content filter. You can also use regex to match multiple lines (i.e., pattern1|pattern2).

➤ **To filter syslog messages by message content:**

1. On the toolbar, click the **Options**  icon; the Options dialog box opens.
2. Under the Content Filter group, configure the message content filters:
 - Incoming traffic:

- i. In the 'Receive filter' field, enter the message-content filter which is applied to incoming traffic.
 - ii. From the 'Mode' drop-down list, select **Allow** to allow only traffic according to your filter, or **Block** to block traffic according to your filter.
- Syslog Display:
 - i. In the 'Display filter' field, enter the message-content filter which is applied to the log display.
 - ii. From the 'Mode' drop-down list, select **Allow** to display syslog messages according to your filter, or **Block** to not display syslog messages according to your filter.



The 'Content Filter' dialog box contains two sections. The first section, 'Receive filter', has a text input field and a 'Mode' dropdown menu set to 'Allow'. The second section, 'Display filter', has a text input field and a 'Mode' dropdown menu set to 'Block'. Between these sections is a row of checkboxes for 'Receive severities' with the following labels: emerg, alert, crit, error, warn, notice, info, and debug. All these checkboxes are checked.

3. Click **OK**.

12 Analyzing Syslog Messages

The device sends syslog messages to the Syslog server as an ASCII message. All Syslog messages are indicated with a sequential number, including the time the message was received and the source IP address. The following figure describes the different types of information displayed in the syslog message.

Figure 12-1: Basic Message Format

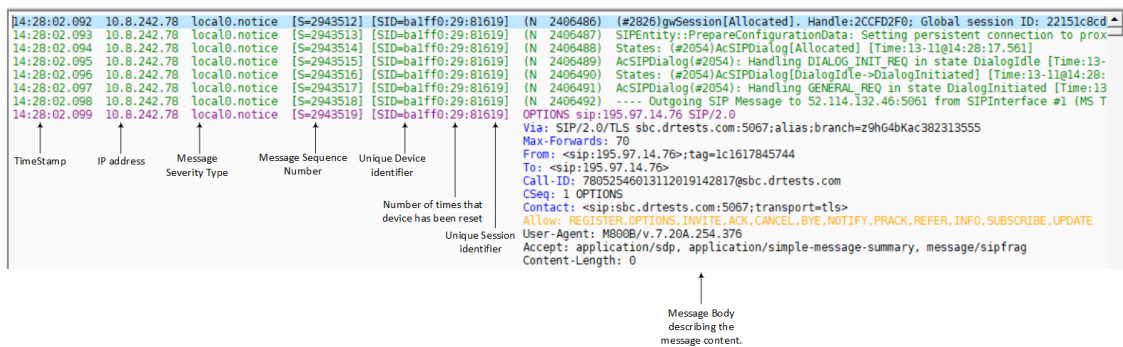


Table 12-1: Syslog Message Components

Component	Description
Timestamp	Time the event was sent to syslog.
IP address	IP address of the managed device.
Message Sequence Number	Sequence number of the message. This number increments for each consecutive message that is sent to syslog for the managed device.
Unique SIP Call Session and device identifier	ID of the call session (MAC address).
Message Body	-

Syslog Message Types

Syslog sends two types of log messages:

- **SIP Call Session Logs:** Logs relating to call sessions (e.g., call established).
- **Board Logs:** Logs relating to the operation of the device (infrastructure) that are non-call session related (e.g., device restart or Web login).
- **SNMP Alarms:** logs including the SNMP information from the alarms raised on the managed device.

SIP Call Session Logs

These logs are identified by a session ID ("SID"). The following shows an example of a SIP-session related Syslog message:

```
13:10:57.811 : 10.13.4.12 : NOTICE : [S=235][SID:2ed1c8:96:5] (lgr_flow)(63)
UdpTransportObject#0- Adding socket event for address 10.33.2.42:5060 [Time:
04-19-2012@18:29:39]
```

The SID is a unique SIP call session and device identifier for the following types of SIP calls:

- **Gateway application:** A call session is either a Tel-to-IP or an IP-to-Tel leg, where each leg is assigned a unique session number.
- **SBC application:** A session includes both the outgoing and incoming legs, where both legs share the same session number.
- **Forked legs and alternative legs** share the same session number.

The device identifier facilitates debugging by clearly identifying the specific device that sent the log message. Unique numbering enables filtering the information (SIP, Syslog, and media) according to device or session ID

Syntax of the session and device identifiers: **[SID=<last 6 characters of device's MAC address>:<number of times device has reset>:<unique SID counter indicating the call session; increments consecutively for each new session; resets to 1 after a device reset>]**

Example:

```
14:32:52.028: 10.33.8.70: NOTICE: [S=9369] [SID=2ed1c8:96:5] (lgr_psbrdex)
(274) recv <-- OFF_HOOK Ch:4
```

Where:

- **2ed1c8** is the device's MAC address
- **96** is the number of times the device has reset
- **5** is a unique SID session number (in other words, this is the fifth call session since the last device reset)



For later software versions of Mediant Software and Mediant 9000, instead of MAC address, the SID contains the serial number.

- **Example of an event in syslog that includes a SIP message with OPTIONS:**

```
11:36:54.582 10.15.45.49 local0.notice [S=12614840] [SID=50e91b:74:353424]
OPTIONS sip:195.189.192.135 SIP/2.0
```



```

Via: SIP/2.0/TLS
sbc11.AUDCTrunk.aceducation.info:5061;alias;branch=z9hG4bKac1026719750
Max-Forwards: 70
From:
<sip:195.189.192.135>;tag=1c942573283
To: <sip:195.189.192.135>
Call-ID:
286566002172202093652@sbc11.AUDCTrunk.aceducation.info
CSeq: 1 OPTIONS
Contact:
<sip:sbc11.AUDCTrunk.aceducation.info:5061;transport=tls>
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,
SUBSCRIBE,UPDATE
User-Agent: M800B/v.7.20A.254.604
Accept: application/sdp,
application/simple-message-summary, message/sipfrag
Content-Length: 0

```

■ **Example of outgoing SIP message:**

```

11:36:18.833 10.15.45.49 local0.notice [S=12614761] [SID=50e91b:74:353422]
(N 11900023) ---- Outgoing SIP Message to 52.114.75.24:5061 from SIPInterface
#2 (Teams) TLS TO(#206) SocketID(10518) ---- [Time:17-02@09:36:17.003]

```

■ **Example of successful classification of an IP Group entity:**

```

11:36:18.949 10.15.45.49 local0.notice [S=12614774] [SID=50e91b:74:353423]
(N 11900034) Classification Succeeded - Source IP Group #2 (Teams) [Time:17-
02@09:36:17.093]

```

Board Logs

These logs are identified by a board ID ("BID"). Example of a board Syslog message:

```

10:21:28.037 : 10.15.7.95 : NOTICE : [S=872] [BID=3aad56:32] Activity Log: WEB:
Successful login at 10.15.7.95:80. User: Admin. Session: HTTP (10.13.22.54)

```

Unique non-SIP session related (e.g., device reset or a Trunk alarm) and device identifier

The device identifier facilitates debugging by clearly identifying the specific device that sent the log message, especially useful in deployments consisting of multiple devices.

In addition, the benefit of unique numbering is that it enables you to filter the information according to device.

Syntax of the BID: [BID=<last 6 characters in MAC>:<number of times device has reset>]

Example:

```
14:32:52.062: 10.33.8.70: WARNING: [S=9399] [BID=2ed1c8:96] invalid Physical index
```

Where:

- **2ed1c8** is the device's MAC address.
- **96** is the number of times the device has reset.



For later software versions of Mediant Software and Mediant 9000, instead of MAC address, the BID contains the serial number.

Example: Event in syslog indicating a TLS socket debug message:

```
11:36:55.220 10.15.45.49 local0.notice [S=12614860] [BID=50e91b:74] (N 11900116) TLSSocketAPI(#67) Socket debug message: CTcpClientSocket::HandleSocketEvent socket close/resetSocketName: SIPTcpChild, FileDesc: 75 [Time:17-02@09:36:
```

SNMP Alarms

SNMP alerts are sent to the Syslog server using the following formats:

- Raised Alarms:

```
RAISE-ALARM: <Alarm Name>; Textual Description: <Textual Description>; Severity <Alarm Severity>; Source <Alarm Source>; Unique ID: <Alarm Unique ID >
```

- Cleared Alarms:

```
CLEAR-ALARM: <Alarm Name>; Textual Description: <Textual Description>; Severity <Alarm Severity>; Source <Alarm Source>; Unique ID: <Alarm Unique ID >
```

- If additional information exists in the alarm, these are added:

```
Additional Info1: ; Additional Info2: ; Additional Info3
```

■ SNMP alarm severity:

- Critical
- Major
- Minor
- Warning
- Indeterminate
- Cleared

The following shows an example of an alarm sent when a device is reset.

Figure 12-2: Reset Alarm

```
11:22:44.192 172.17.140.111 local0.info connected to 172.17.140.111
08:06:07.000 172.17.140.111 local0.notice [5=579] [810=4f7347:49] Deleted task c11 did not free 2 buffers (size 104, IP 0x0531364 -ZNBac:infral307611), DummyId 159 [Code:0x20042] [Time:14-02@08:06:07.137]
08:06:07.000 172.17.140.111 local0.notice [5=579] [810=4f7347:49] Activity Log: User logged out. User: Admin, Session: Telnet (10.3.180.99) [Time:14-02@08:06:07.162]
08:26:51.000 172.17.140.111 local0.notice [5=583] [810=4f7347:49] Activity Log: Web: Successful login at 172.17.140.111:80. User: Admin, Session: WEB (10.13.2.7) [Time:14-02@08:26:51.271]
08:27:04.000 172.17.140.111 local0.notice [5=583] [810=4f7347:49] Opening Log Web Page - printing error messages sent to Syslog [Code:0x40529] [Time:14-02@08:27:03.575]
08:27:04.000 172.17.140.111 local0.notice [5=583] [810=4f7347:49] Starting Log Session successfully performed [Code:0x40529] [Time:14-02@08:27:04.295]
08:27:05.000 172.17.140.111 local0.notice [5=583] [810=4f7347:49] Opening Log Web Page - printing error messages sent to Syslog [Code:0x40529] [Time:14-02@08:27:04.459]
08:27:05.000 172.17.140.111 local0.notice [5=583] [810=4f7347:49] Starting Log Session successfully performed [Code:0x40529] [Time:14-02@08:27:04.459]
08:29:04.000 172.17.140.111 local0.notice [5=583] [810=4f7347:49] Activity Log: Syslog Server IP was changed from '172.17.114.22' to '10.13.2.7'. User: Admin, Session: WEB (10.13.2.7) [Time:14-02@08:29:04.272]
08:30:42.000 172.17.140.111 local0.notice [5=583] [810=4f7347:49] Activity Log: Web: Successful login at 172.17.140.111:80. User: Admin, Session: WEB (10.13.2.7) [Time:14-02@08:30:42.154]
08:30:42.000 172.17.140.111 local0.notice [5=583] [810=4f7347:49] Opening Log Web Page - printing error messages sent to Syslog [Code:0x40529] [Time:14-02@08:30:42.154]
08:31:16.000 172.17.140.111 local0.notice [5=583] [810=4f7347:49] Starting Log Session successfully performed [Code:0x40529] [Time:14-02@08:30:46.145]
08:31:16.000 172.17.140.111 local0.notice [5=583] [810=4f7347:49] Activity Log: Device Reset. User: Admin, Session: WEB (10.13.2.7) [Time:14-02@08:31:16.147]
08:31:16.000 172.17.140.111 local0.notice [5=583] [810=4f7347:49] Activity Log: Device Reset. User: public, Session: WEB (172.17.140.84) [Time:14-02@08:31:16.147]
08:31:16.000 172.17.140.111 local0.warn [5=593] [810=4f7347:49] Managed Objects: Force Lock Module. [Time:14-02@08:31:16.148]
08:31:16.000 172.17.140.111 local0.warn [5=593] [810=4f7347:49] False Alarm: Invalid Object: Device is resetting. Severity:critical, Source:Internal, Message ID:41 [Time:14-02@08:31:16.148]
08:31:16.000 172.17.140.111 local0.notice [5=593] [810=4f7347:49] (N 10) SNMP new Admin State: FORCE. Restrict connections: False Current Calls: 0 [Time:14-02@08:31:16.150]
11:23:19.475 172.17.140.111 local0.warn disconnected
```

Error Abbreviations in Syslog Messages

The device denotes events in syslog messages using unique abbreviations, as listed in the following table. For example, if an invalid payload length event occurs, the syslog message uses the abbreviated event string "IP":

Apr 4 12:00:12 172.30.1.14 IP:5 [Code:0x5004] [CID:3294] [Time: 20:17:00]

Table 12-2: Syslog Error Abbreviations

Error Abbreviation	Error Name Description
AA	Invalid Accumulated Packets Counter
AC	Invalid Channel ID
AL	Invalid Header Length
AO	Invalid Codec Type
AP	Unknown Aggregation Payload Type
AR	Invalid Routing Flag Received
AT	Simple Aggregation Packets Lost
CC	Command Checksum Error

Error Abbreviation	Error Name Description
CE	Invalid Cell Coder Code
CS	Command Sequence Error
ES	8 sec Timeout Before Disconnect
HO	Host Received Overrun
IA	Invalid AMR Payload
IC	Invalid CID Error
IG	Invalid G723 Code
IP	Invalid payload length
IR	Invalid RTCP Packet
IS	Invalid SID Length
LC	Transmitter Received Illegal Command
LF	Lost Fax Frames In High Speed Mode
LM	Lost Modem Frames In High Speed Mode
MI	Misalignment Error
MR	Modem Relay Is Not Supported
PD	RTP Packet Duplicated
OR	DSP JB Overrun
PH	Packet Header Error
PL	RTP Packet Loss
RB	Counts the number of BFI Frames Received From The Host
RD	No Available Release Descriptor
RO	RTP Reorder
RP	Unknown RTP Payload Type
RS	RTP SSRC Error

Error Abbreviation	Error Name Description
UF	Unrecognized Fax Relay Command

Severity Levels of Syslog Messages

The following table shows the type of syslog messages that are generated based on message severity.

Table 12-3: Message Severity Levels

Severity Level (Highest to Lowest)	Syslog String (Color in Web Interface)	Description
Fatal	emergency (red)	A panic condition (system is unstable)
Alert	alert (red)	A problem has been identified and an action must be taken immediately
Critical	critical (red)	A problem has been identified that is critical
Error	error (red)	An error has been identified
Warning	warning (magenta)	An error that might occur if measures are not taken to prevent it
Notice	notice (dark green)	An unusual event has occurred
Informational	info (blue)	An operational message
Debug	debug (black)	Debug message


Viewing SIP Flow Diagrams

You can view the SIP call flow of SIP sessions (calls) included in your syslog. The SIP flow displays the SIP session in SIP ladder diagram format. This is useful for analyzing the SIP messages of calls.




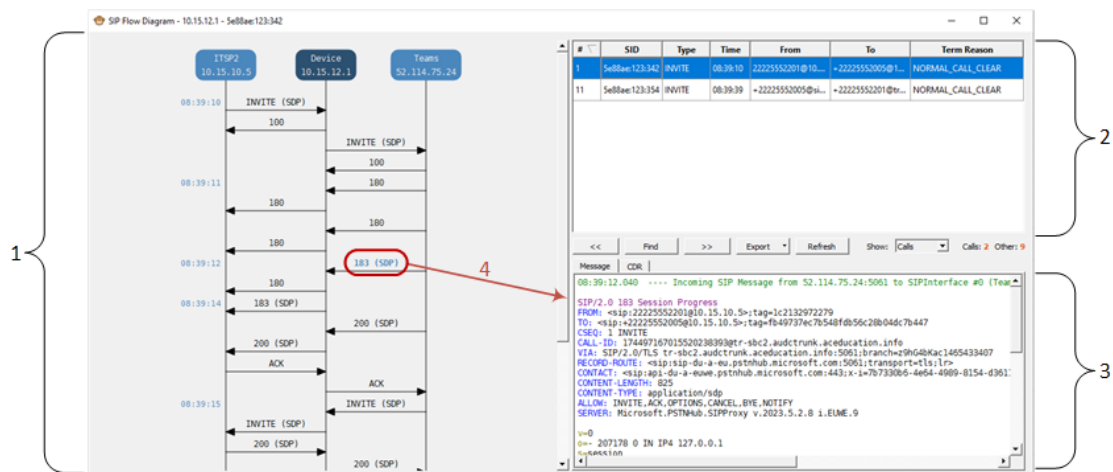
SIP flow currently supports the following call flows: Mediant SBCs, Mediant Gateways (analog and digital), SmartTAP 360° and IP Phones.

➤ To analyze calls using SIP flow:

1. On the toolbar, click the **SIP Flow Diagram**  icon (or from the Tools menu, choose **SIP Flow Diagram**); the SIP Flow Diagram window appears, as shown in the following example:



If you have multiple window tabs, you can view SIP call flow diagrams of all the tabs, by clicking the **SIP Flow Diagram for All Tabs**  icon.



Legend:

- **#1:** SIP Flow diagram.
 - **#2:** Session pane, listing all the SIP sessions in the syslog (e.g., INVITE, OPTIONS, and REGISTER messages).
 - **#3:** Message details pane with the Message tab selected by default, displaying the content of the selected SIP request or response in the SIP Call flow diagram. It also displays the CDR of the SIP session if you select the CDR tab.
 - **#4:** Selected SIP response (e.g., "183 (SDP)") in the SIP Call Flow diagram, whose content is displayed in the Message details pane.
2. In the Session pane (#2 in figure), select the SIP session type whose SIP flow you want to view. The Session pane provides the following tools:
 - **Filter by SIP Message Type:** From the 'Show' drop-down list, select the SIP message type, for example, **Options**, as shown below:

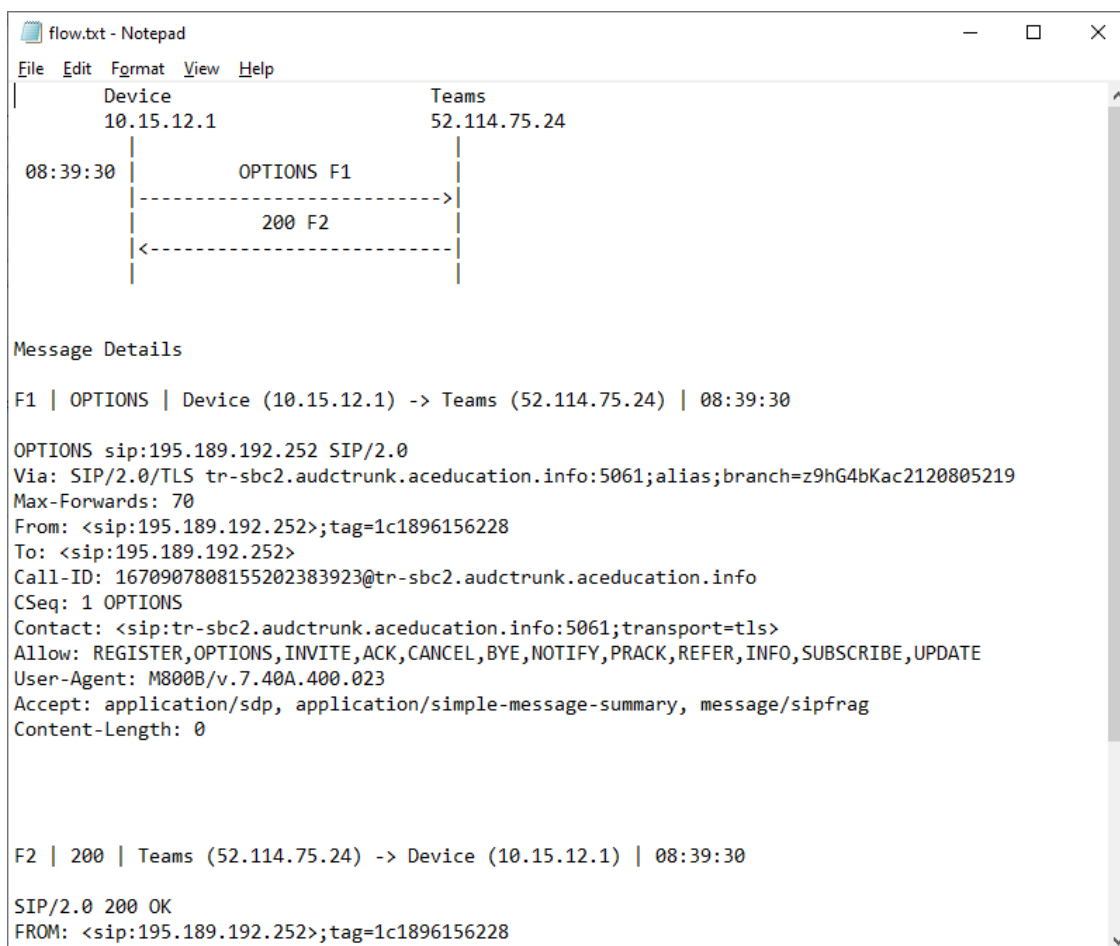
#	SID	Type	Time	From	To	Term Reason
2	5e88ae:123:345	OPTIONS	08:39:30	195.189.192.252	195.189.192.252	
3	5e88ae:123:346	OPTIONS	08:39:30	195.189.192.252	195.189.192.252	
4	5e88ae:123:347	OPTIONS	08:39:30	195.189.192.252	195.189.192.252	
5	5e88ae:123:348	OPTIONS	08:39:30	sip-du-a-...	195.189.192.252	
6	5e88ae:123:349	OPTIONS	08:39:31	sip-du-a-...	195.189.192.252	
7	5e88ae:123:350	OPTIONS	08:39:31	sip-du-a-...	195.189.192.252	
8	5e88ae:123:351	OPTIONS	08:39:34	10.15.12.1	10.15.12.1	
9	5e88ae:123:352	OPTIONS	08:39:34	10.15.12.1	10.15.12.1	

<< Find >> Export Refresh Show: Options Calls: 2 Other: 9

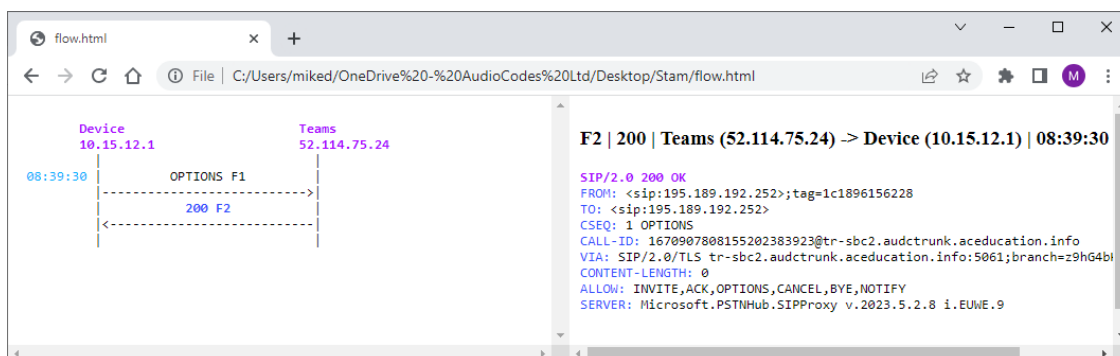
- **Refresh List of Sessions:** Click **Refresh**. Refreshing the list is important if Syslog Viewer is still receiving syslog messages from the device.
- **Export Sessions:** From the 'Export' drop-down list, select the following:
 - ◆ **Export sessions** - downloads the list of sessions to a .csv file (in CSV format).

#	A	B	C	D	E	F	G		
#	SID	Type	Time	From	To	Term Reason			
2	1	5e88ae:123:342	INVITE	8:39:10	22225552201@10.15.10.5	+22225552005@10.15.10.5	NORMAL_CALL_CLEAR		
3	2	5e88ae:123:345	OPTIONS	8:39:30	195.189.192.252	195.189.192.252			
4	3	5e88ae:123:346	OPTIONS	8:39:30	195.189.192.252	195.189.192.252			
5	4	5e88ae:123:347	OPTIONS	8:39:30	195.189.192.252	195.189.192.252			
6	5	5e88ae:123:348	OPTIONS	8:39:30	sip-du-a-eu.pstnhub.microsoft.com	195.189.192.252			
7	6	5e88ae:123:349	OPTIONS	8:39:31	sip-du-a-us.pstnhub.microsoft.com	195.189.192.252			
8	7	5e88ae:123:350	OPTIONS	8:39:31	sip-du-a-as.pstnhub.microsoft.com	195.189.192.252			
9	8	5e88ae:123:351	OPTIONS	8:39:34	10.15.12.1	10.15.12.1			
10	9	5e88ae:123:352	OPTIONS	8:39:34	10.15.12.1	10.15.12.1			
11	10	5e88ae:123:353	OPTIONS	8:39:36	10.15.10.5	10.15.10.5			
12	11	5e88ae:123:354	INVITE	8:39:39	+22225552005@sip.pstnhub.microsoft.com	+22225552201@tr-sbc2.audctrunk.aceducation.info	NORMAL_CALL_CLEAR		
13									
sessions									

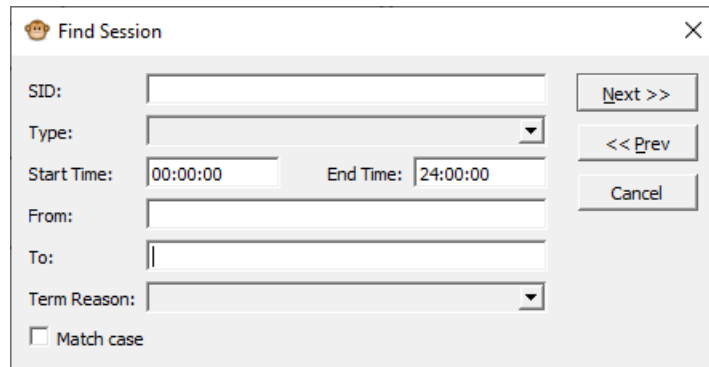
- ◆ **Export flow diagram as TXT** – downloads the SIP call flow of the selected session in text format (.txt file). The file includes the SIP call flow and the details of the entire message.



- ◆ **Export flow diagram as HTML** – downloads the SIP call flow of the selected session in HTML format (.html file). The file includes the SIP call flow and the details of the entire message. In the left pane, click a SIP request or response in the call flow to view its details in the right pane.



- **Search for SIP Sessions:**
 - Click **Find**; the following dialog box appears:



Find Session

SID:

Type:

Start Time: End Time:

From:

To:

Term Reason:

☐ Match case

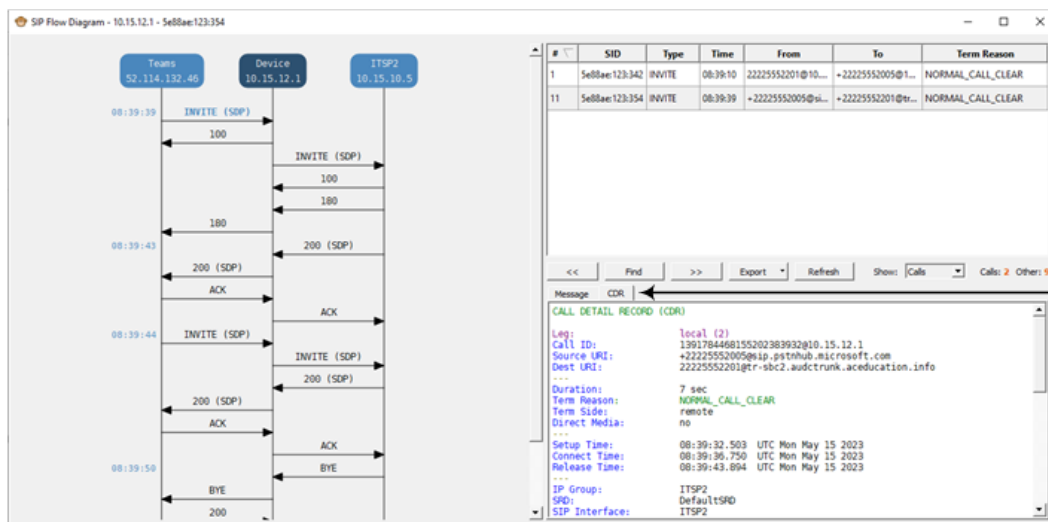
Next >> << Prev Cancel

ii. Fill in the desired search parameters:


- ◆ 'SID': Search for a specific Session ID.
- ◆ 'Type': Search for sessions of a specific SIP message request or response. The list only displays SIP message types that are available in the syslog.
- ◆ 'Start Time' and 'End Time': Search for sessions within a specific time range.
- ◆ 'From': Search for sessions with a specific SIP From header value.
- ◆ 'To': Search for sessions with a specific SIP To header value.
- ◆ 'Term Reason': Search for sessions with a specific call termination reason.

iii. Click **Next** or **Prev** to find sessions based on your search criteria.

3. In the SIP Flow diagram (#1 in figure), select the SIP request or response message of whose content you want to view. If you return to the Syslog Viewer's main window, your cursor is automatically located on the line in the syslog that corresponds to the selected SIP message.
4. In the Message details pane (#3 in figure), click the **Message** tab (default); the content of the message that you selected in Step 3 is displayed.
5. To view the CDR of the currently selected SIP session, in the Message details pane, click the **CDR** tab:






The **CDR** tab appears only if parsing of CDR records is enabled (default). To disable CDR parsing, click the **Options**  icon, clear the 'Parse CDR records' check box, and then click **OK**.

Setting Preferences for SIP Flow Diagrams

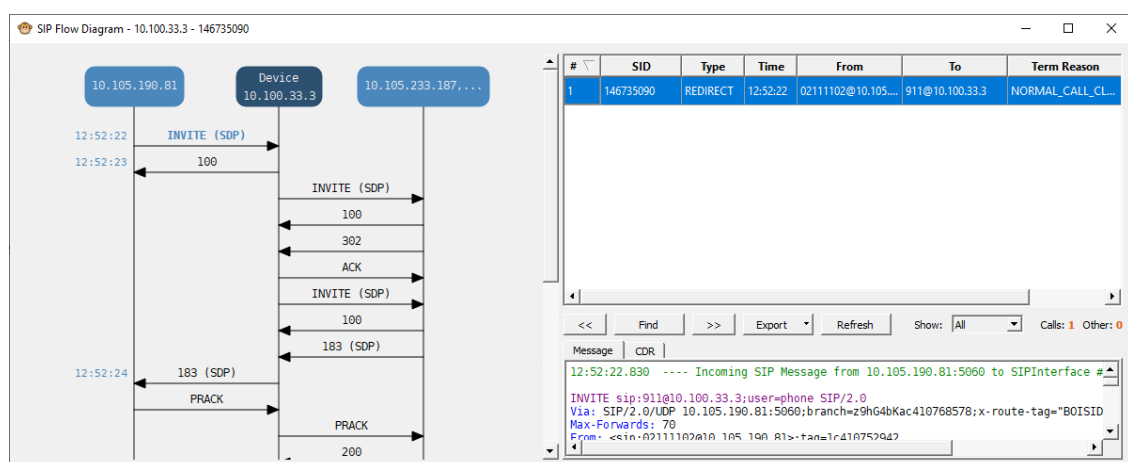
The following procedure describes how to set global preferences for SIP flow diagrams.

➤ To set preferences for SIP flow diagrams:

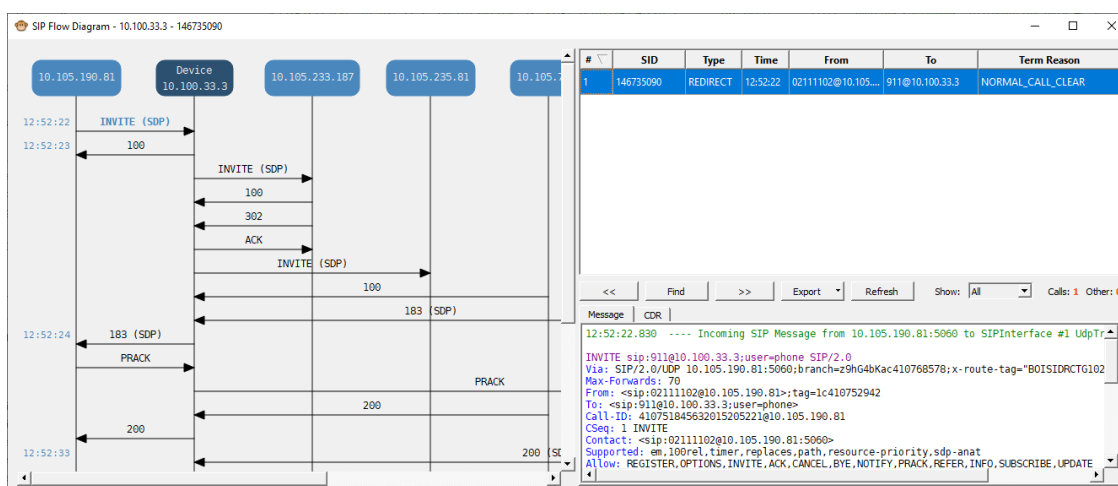
1. On the toolbar, click the **Options**  icon; the Options dialog box appears.
2. Under the SIP Flow Diagram group, configure the following preferences:
 - **'Group messages by':** Affects how vertical lines in SIP Flow Diagrams are calculated (see example below).
 - **'Merge sessions with identical Call-ID':** This option useful for earlier device software versions where the "[SID=]" element sometimes "switched" in the middle of the session (or even disappeared). Enabling this option merges the sessions based on SIP Call-ID.
 - **'Parse sessions without SID':** This option useful for earlier device software versions where the "[SID=]" element is sometimes not displayed at all in the Web interface's Message Log.
3. Click **OK**.

The following shows an example of the 'Group messages by' field:

■ 'Group messages by' configured to Call-ID:



■ 'Group messages by' configured to Call-ID + IP Address:

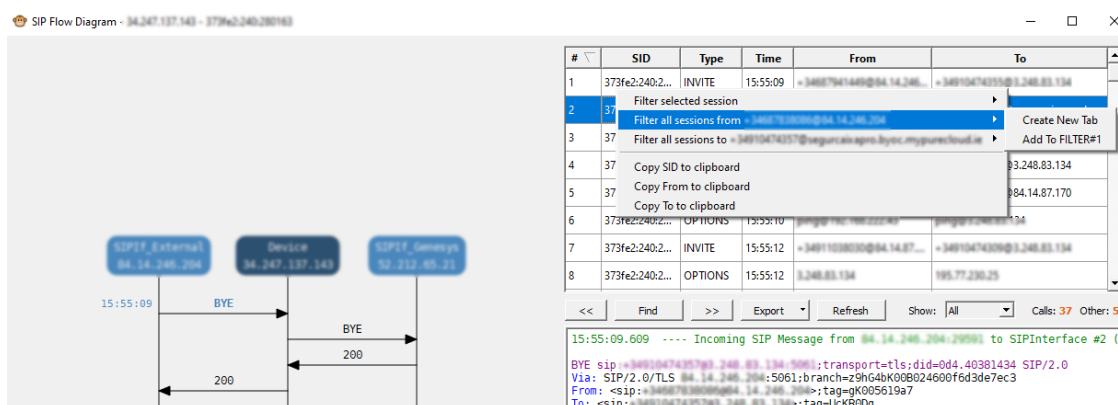


Filtering Display by Session ID

You can use the SIP Call Flow diagram to filter the syslog message window by session ID, SIP URI of From header, or SIP URI of To header.

➤ To filter syslog message window by session ID:

- In the Session pane of the SIP Flow Diagram window, right-click the desired SIP session row, and then from the pop-up menu, choose one of the following:
 - Filter selected session:** Filters the syslog message window according to the session ID (SID) of the selected row.
 - Filter all sessions from <SIP URI in From header>:** Filters the syslog message window according to the specific SIP URI of the From header.
 - Filter all sessions to <SIP URI in To header>:** Filters the syslog message window according to the specific SIP URI of the To header.



- When selecting the filter type (previous step), you can choose whether to create a new tab in the syslog message window for your filtered syslog messages, or add the filter to an existing tab.

Copying to Clipboard the SID, SIP URI From, or SIP URI To

In the SIP Flow Diagram window, you can copy to your clipboard the session ID (SID), SIP URI of the From header, or SIP URI of the To header. You can then paste these values in, for example, Notepad or an email.

➤ To copy to clipboard the SID, From SIP URI, or To SIP URI:

1. In the Session pane of the SIP Flow Diagram window, right-click the desired SIP session row, and then from the pop-up menu, choose one of the following:
 - **Copy SID to clipboard:** Copies to clipboard the session ID.
 - **Copy From to clipboard:** Copies to clipboard the SIP URI of the From header.
 - **Copy To to clipboard:** Copies to clipboard the SIP URI of the To header.

The screenshot shows the SIP Flow Diagram window. On the left, a sequence diagram illustrates a SIP session between 'SIP/2.0 External' (94.14.246.204), 'Device' (94.247.137.143), and 'SIP/2.0 Gateway' (92.237.95.21). The sequence includes a 'BYE' message from the Device to the Gateway, followed by a '200' response from the Gateway to the Device, and another 'BYE' message from the Device to the External interface, followed by a '200' response from the External interface to the Device.

On the right, the Session pane displays a table of SIP sessions. A right-click context menu is open over the second row (SID: 373fe2:2402...), showing options: 'Filter selected session', 'Filter all sessions from +349110474357@94.14.246.204', 'Filter all sessions to +34910474337@92.237.95.21', 'Copy SID to clipboard', 'Copy From to clipboard', and 'Copy To to clipboard'. The 'Copy SID to clipboard' option is highlighted.

#	SID	Type	Time	From	To
1	373fe2:2402...	INVITE	15:55:09	349110474357@94.14.246.204	34910474337@92.237.95.21
2	373fe2:2...				caixapro.b...
3	373fe2:2...				caixapro.b...
4	373fe2:2...				83.134
5	373fe2:2...				87.170
6	373fe2:2402...	OPTIONS	15:55:10	92.237.95.21	92.237.95.21
7	373fe2:2402...	INVITE	15:55:12	349110474357@94.14.246.204	34910474337@92.237.95.21
8	373fe2:2402...	OPTIONS	15:55:12	92.237.95.21	92.237.95.21

Below the table, the SIP message details for the selected session are shown:

```

15:55:09.609 ----- Incoming SIP Message from 94.14.246.204 (94.14.246.204) to SIPInterface #2 (92.237.95.21)
BYE sip:34910474337@92.237.95.21;transport=tls;did=0d4.40381434 SIP/2.0
Via: SIP/2.0/TLS 94.14.246.204:5060;branch=z9hG4bK00B024600f6d3de7ec3
From: <sip:349110474357@94.14.246.204>;tag=gK005619a7
To: <sip:34910474337@92.237.95.21>;tag=UcKR00dg
  
```

2. Paste the copied item into an application (e.g., Notepad or an email).

13 Using the Command Line

You can run Syslog Viewer from the command line and write to disk.

➤ **To run Syslog Viewer commands:**

1. Open a command shell.
2. Change to the directory where the Syslog Viewer is installed.
3. To run the Syslog Viewer:

```
syslogViewer.exe
```

4. To open an existing log file:

```
syslogViewer.exe D:\logs\sbc_lync.txt
```

5. To write logs to disk:

```
syslogViewer.exe --writeLog
```

6. To write logs to disk at specific location:

```
syslogViewer.exe --writeLog D:\logs\syslog.txt
```

This page is intentionally left blank.

International Headquarters

1 Hayarden Street,

Airport City

Lod 7019900, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd

Piscataway, NJ 08854, USA

Tel: +1-732-469-0880

Fax: +1-732-469-2298

Contact us: <https://www.audiocodes.com/corporate/offices-worldwide>

Website: <https://www.audiocodes.com/>

Documentation Feedback: <https://online.audiocodes.com/documentation-feedback>

©2023 AudioCodes Ltd.. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, and AudioCodes Room Experience are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-40034

