3. From the 'Recording Mode' drop-down list, select one of the following:
   - **All Physical Ethernet Ports**: The log filter for the IP trace is applied on packets received and sent (tagged and untagged) on all the physical Ethernet ports.
   - **Physical Ethernet Port**: The log filter for the IP trace is applied on packets received and sent on the specific Ethernet port selected in Step 4.
   - **VLAN ID**: The log filter for the IP trace is applied on packets received and sent on the specific VLAN (underlying Ethernet Device) selected in Step 5.
   - **Ethernet Group**: The log filter for the IP trace is applied on packets received and sent for a specific Ethernet Group selected in Step 6.
4. If you selected **Physical Ethernet Port** in Step 3, then from the 'Physical Ethernet Port' drop-down list, select the port. To view the device's Ethernet ports, see Configuring Physical Ethernet Ports on page 110.
5. If you selected **VLAN ID** in Step 3, then from the 'VLAN ID' drop-down list, select the VLAN. To configure VLANs (Ethernet Devices), see Configuring Underlying Ethernet Devices on page 115.

- The recording includes just packets of specific VLAN, but without the VLAN header.
- Untagged packets are not recorded.

6. f you selected **Ethernet Group** in Step 3, then from the 'Ethernet Group' drop-down list, select the Ethernet Group. To configure Ethernet Groups, see Configuring Ethernet Port Groups on page 112.
7. Click **Apply**.

Configuring Syslog

This section describes how to configure Syslog. To filter Syslog messages, see Configuring Log Filter Rules.

Syslog Message Format

The Syslog message is sent from the device to a Syslog server as an ASCII (American Standard Code for Information Interchange) message. Syslog uses UDP as its underlying transport layer mechanism. By default, UDP port 514 is assigned to Syslog, but this can be changed (see Enabling Syslog).

Syslog includes two types of log messages:

- **SIP Call Session Logs:** Logs relating to call sessions (e.g., call established). These logs are identified by a session ID ("SID"), described in detail in the table below. For example:

```
10:44:11.299 10.15.77.55 local0.notice [S=511941] [SID=50dcb2:31:12079]
(N 483455) ReleaseAddress. IPv4IF=1 IPv6IF=-1 Port=7500 [Time:10-
09@09:42:56.938]
```

- **Board Logs:** Logs relating to the operation of the device (infrastructure) that are non-call session related (e.g., device reset or Web login). These logs are identified by a board ID ("BID"), described in detail in the table below. For example:

```
11:58:30.820 10.15.77.55 local0.notice [S=534370] [BID=50dcb2:31] Activity
Log: WEB: User logout. User: Admin. Session: WEB (10.15.77.100) [Time:10-
09@10:57:16.360]
```

The format of the Syslog message is described in the following table:

Table 57-3: Syslog Message Format Description

Message Item	Description
Timestamp	When the Network Time Protocol (NTP) is enabled, a timestamp string [hour:minutes:seconds.msec] is added to all Syslog messages, for example (in bold): **10:44:11.299** 10.15.77.55 local0.notice [S=511941] [SID=50dcb2:31:12079] (N 483455) ReleaseAddress. IPv4IF=1 IPv6IF=-1 Port=7500 [Time:10-09@09:42:56.938]
IP Address	The device that generated the Syslog message, defined by IP address.
Severity Type	Each Syslog message is generated with a severity level in the format <*FacilityCode.Severity*>, for example: `10:44:11.299 10.15.77.55 local0.`**`notice`**` [S=511941] [SID=50dcb2:31:12079] (N 483455) ReleaseAddress. IPv4IF=1 IPv6IF=-1 Port=7500 [Time:10-09@09:42:56.938]` The severity level can be one of the following: ■ Error: Indicates that a problem has been identified that requires immediate handling. ■ Warning: Indicates an error that might occur if measures are not taken to prevent it. ■ Notice: Indicates that an unusual event has occurred. ■ Info: Indicates an operational message. ■ Debug: Messages used for debugging.

Message Item	Description
	Note: ■ The Info and Debug severity-level messages are required only for advanced debugging. By default, they are not sent by the device. ■ Syslog messages displayed in the Web interface (see Viewing Syslog Messages on page 1147) are color coded according to severity level.

Sequence Number [S=<number>]	By default, Syslog messages are sequentially numbered in the format *[S=<number>]*, for example, "[S=538399]". A skip in the number sequence of messages indicates a loss in message packets. The following example of a Syslog shows two missing messages (S=538402 and S=538403):
	`12:11:42.709 10.15.77.55 local0.notice [S=538399] [SID=50dcb2:31:12754] (N 508552) CAC: Remove SBC Outgoing Other, IPG 2 (Teams): 0, SRD 0 (DefaultSRD): 0, SipIF 1 (Teams): 0 [Time:10-09@11:10:28.848]`
	`12:11:42.709 10.15.77.55 local0.notice [S=538400] [SID=50dcb2:31:12754] (N 508553) States: (#2698)SBCCall[Deallocated] [Time:10-09@11:10:28.848]`
	`12:11:42.709 10.15.77.55 local0.notice [S=538401] [SID=50dcb2:31:12754] (N 508554) CAC: Remove SBC Incoming Other, IPG 2 (Teams): 0, SRD 0 (DefaultSRD): 0, SipIF 1 (Teams): 0 [Time:10-09@11:10:28.848]`
	`12:11:42.710 10.15.77.55 local0.notice [S=538404] [SID=50dcb2:31:12754] (N 508555) States: (#2699)SBCCall[Deallocated] [Time:10-09@11:10:28.848]`
	Note: To exclude the message sequence number from Syslog messages, configure the 'CDR Syslog Sequence Number' parameter to **Disable** (see Configuring Syslog).

Session ID (SID)	The SID is a unique SIP call session and device identifier. The device identifier facilitates debugging by clearly identifying the specific device that sent the log message, which is especially useful in deployments consisting of multiple devices. In addition, the benefit of unique numbering is that it enables you to filter information (such as SIP, Syslog, and media) according to device or session ID. The syntax of the session and device identifiers is as follows:

Message Item	Description
	[SID=<last 6 characters (3 lower bytes) of Serial Number>:<number of times device has reset>:<unique SID counter indicating the call session, which increments consecutively for each new session and resets to 1 after a device reset>] For example: `10:44:11.299 10.15.77.55 local0.notice [S=511941] [`**`SID=50dcb2736502:31:12079`**`] (N 483455) ReleaseAddress. IPv4IF=1 IPv6IF=-1 Port=7500 [Time:10-09@09:42:56.938]` Where: ■ *736502* is the device's Serial Number. ■ *31* is the number of times the device has reset. ■ *12079* is a unique SID session number (in other words, this is call session 12,079 since the last device reset). ✔ 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.
Board ID (BID)	The BID is a unique non-SIP session related (e.g., device reset) and device identifier. The BID value is similar to the SID (above), except that it doesn't contain the session ID. The device identifier facilitates debugging by clearly identifying the specific device that sent the log message, which is especially useful in deployments consisting of multiple devices. In addition, the benefit of unique numbering is that it enables you to filter information according to device. The syntax of the BID is as follows: *[BID=<last 6 characters (3 lower bytes) of Serial Number>:<number of times device has reset>]* For example: `11:58:30.820 10.15.77.55 local0.notice [S=534370] [`**`BID=736502:31`**`] Activity Log: WEB: User logout. User: Admin. Session: WEB (10.15.77.100) [Time:10-09@10:57:16.360]` Where: ■ *736502* is the device's Serial Number. ■ *31* is the number of times the device has reset.
Message Body	Describes the message. For example, the body (shown in bold) of the

Message Item	Description
	following Syslog message indicates that the user logged out of the Web interface: `11:58:30.820 10.15.77.55 local0.notice [S=534370] [BID=50dcb2:31]` **`Activity Log: WEB: User logout. User: Admin. Session: WEB (10.15.77.100)`** `[Time:10-09@10:57:16.360]`

Event Representation in Syslog Messages

The device denotes events in Syslog message 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]
```

For Syslog messages sent for packet loss events, see Packet Loss Indication in Syslog on page 1152.

Table 57-4: Syslog Error Event 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
CE	Invalid Cell Coder Code
CS	Command Sequence Error
ES	8 sec Timeout Before Disconnect

Error Abbreviation	Error Name Description
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
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
UF	Unrecognized Fax Relay Command

Syslog Fields for Answering Machine Detection (AMD)

The Syslog message can include information relating to the Answering Machine Detection (AMD) feature. AMD is used to detect whether a human (including a fax machine), an answering machine, silence, or answering machine beeps have answered the call on the remote side.

- AMDSignal – the field can acquire one of the following values:
  - voice (V)
  - answer machine (A)
  - silence (S)
  - unknown (U)
- AMDDecisionProbability – probability (in %) success that correctly detects answering type

Below is an example of such a Syslog message with AMD information:

```
CallMachine:EVENT_DETECTED_EV - AMDSignal = <type - V/A/S/U>,
AMDDecisionProbability = <percentage> %
```

If there is no AMD detection, the AMDSignal field is shown empty (i.e. AMDSignal =).

For more information on the AMD feature, see Answering Machine Detection (AMD).

SNMP Alarms in Syslog Messages

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 >.

  If additional information exists in the alarm, then these are also added: Additional Info1:/ Additional Info2:/ Additional Info3

  The Messages' Severity is as follows:

Table 57-5: Syslog Message Severity

ITU Perceived Severity (SNMP Alarm's Severity)	AudioCodes Syslog Severity
Critical	RecoverableMsg
Major	RecoverableMsg
Minor	RecoverableMsg
Warning	Notice
Indeterminate	Notice
Cleared	Notice

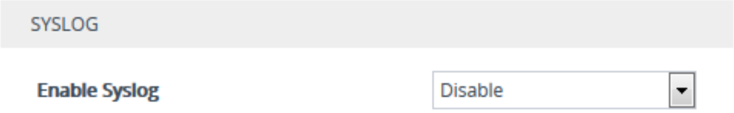
- **Cleared Alarms:** CLEAR-ALARM: <Alarm Name>; Textual Description: <Textual Description>; Severity <Alarm Severity>; Source <Alarm Source>; Unique ID: <Alarm Unique ID >; If exists Additional Info1:/ Additional Info2:/ Additional Info3:

Enabling Syslog

To use Syslog, you first need to enable it.

➢ To enable Syslog:

1. Open the Logging Settings page (**Troubleshoot** menu > **Troubleshoot** tab > **Logging** folder > **Logging Settings**).
2. From the 'Enable Syslog' drop-down list, select **Enable**.



SYSLOG

Enable Syslog: Disable

3. Click **Apply**.

Configuring the Syslog Server Address

The device sends the Syslog messages to the Syslog server's address.

➢ To configure the Syslog server address:

1. Open the Logging Settings page (**Troubleshoot** menu > **Troubleshoot** tab > **Logging** folder > **Logging Settings**).
2. In the 'Syslog Server IP' field [SyslogServerIP], enter the IP address of the Syslog server.
3. In the 'Syslog Server Port' field, enter the port of the Syslog server.

Syslog Server IP: 0.0.0.0

Syslog Server Port: 514

4. Click **Apply**.

Configuring Syslog Message Severity Level

You can configure the minimum severity level of messages that you want to include in Syslog messages that are generated by the device. The severity levels are described in the following table.

Severity Level (Highest to Lowest)	Syslog String	Description
Fatal	emerg	A panic condition (system is

Severity Level (Highest to Lowest)	Syslog String	Description
		unstable).
Alert	alert	A problem has been identified and an action must be taken immediately.
Critical	crit	A problem has been identified that is critical.
Error	error	An error has been identified.
Warning	warning	An error that might occur if measures are not taken to prevent it.
Notice	notice	An unusual event has occurred.
Informational	info	An operational message.
Debug	debug	Debug message.

The specified severity level and all higher severity levels are included in the Syslog message. For example, if you configure the parameter to **Alert**, the Syslog includes messages with **Alert** severity level and messages with **Fatal** severity level.

When viewing Syslog messages in the Web interface (see Viewing Syslog Messages on page 1147), each severity level is displayed in a different color.

➢ To configure the minimum message severity level to include in Syslog:

1. Open the Logging Settings page (**Troubleshoot** menu > **Troubleshoot** tab > **Logging** folder > **Logging Settings**).
2. From the 'Log Severity Level' [SyslogLogLevel] drop-down list, select the severity level.

Log Severity Level • Critical

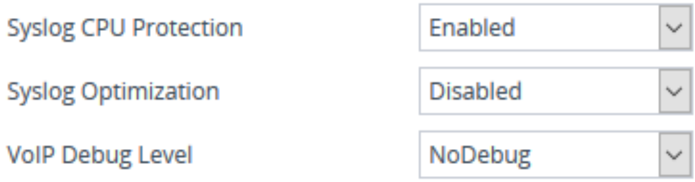
3. Click **Apply**.

Configuring Syslog Debug Level

You can configure the amount of information (debug level) to include in Syslog messages. You can also enable the device to send multiple Syslog messages bundled into a single packet, and enable a protection mechanism that automatically lowers the debug level when the device's CPU resources become low, ensuring sufficient CPU resources are available for processing voice traffic.

➢ To configure the Syslog debug level:

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



Syslog CPU Protection: Enabled

Syslog Optimization: Disabled

VoIP Debug Level: NoDebug

2. From the 'VoIP Debug Level' [GwDebugLevel] drop-down list, select the debug level of Syslog messages:
   - **No Debug:** Disables Syslog and no Syslog messages are sent.
   - **Basic:** Sends debug logs of incoming and outgoing SIP messages.
   - **Detailed:** Sends debug logs of incoming and outgoing SIP message as well as many other logged processes.
3. From the 'Syslog Optimization' [SyslogOptimization] drop-down list, select whether you want the device to accumulate and bundle multiple debug messages into a single UDP packet before sending it to a Syslog server. The benefit of the feature is that it reduces the number of UDP Syslog packets, thereby improving (optimizing) CPU utilization. The size of the bundled message is configured by the [MaxBundleSyslogLength] parameter.
4. From the 'Syslog CPU Protection' [SyslogCpuProtection] drop-down list, select whether you want to enable the protection feature for the device's CPU resources during debug reporting, ensuring voice traffic is unaffected. If CPU resources drop (i.e., high CPU usage) to a critical level (user-defined threshold), the device automatically lowers the debug level to free up CPU resources that were required for the previous debug-level functionality. When CPU resources become available again, the device increases the debug level to its' previous setting. For example, if you set the 'Debug Level' to **Detailed** and CPU resources decrease to the defined threshold, the device automatically changes the level to **Basic**, and if that is not enough, it changes the level to **No Debug**. Once CPU resources are returned to normal, the device automatically changes the debug level back to its' original setting (i.e., **Detailed**). The threshold is configured by the [DebugLevelHighThreshold] parameter.
5. Click **Apply**.

Reporting Management User Activities

The device can report operations (activities) performed in the device's management interfaces (e.g., Web and CLI) by management users, in Syslog messages. You can also view the logged user activities in the Web interface (see Viewing Web User Activity Logs).

The Syslog message indicates these logs with the string "Activity Log". Each logged user activity includes the following information:

- Username (e.g., "Admin") of the user that performed the action
- IP address of the client PC from where the Web user accessed the management interface
- Protocol used for the session (e.g., SSH or HTTP)

The following example shows a Web-user activity log (indicating a login action) with the above-mentioned information:

```
14:07:46.300 : 10.15.7.95 : Local 0  :NOTICE  : [S=3149] [BID=3aad56:32]
Activity Log: WEB: Successful login at 10.15.7.95:80. User: Admin. Session:
HTTP (10.13.22.54)
```

The device can report the following user activities:

- Modifications of individual parameters, for example:

  ```
  14:33:00.162 : 10.15.7.95 : Local 0  :NOTICE  : [S=3403] [BID=3aad56:32]
  Activity Log: Max Login Attempts was changed from '3' to '2'. User: Admin.
  Session: HTTP (10.13.22.54)
  ```

- Modifications of table fields, and addition and deletion of table rows, for example:

  ```
  14:42:48.334 : 10.15.7.95 : NOTICE  : [S=3546] [BID=3aad56:32]  Activity Log:
  Classification - remove line 2. User: Admin. Session: HTTP (10.13.22.54)
  ```

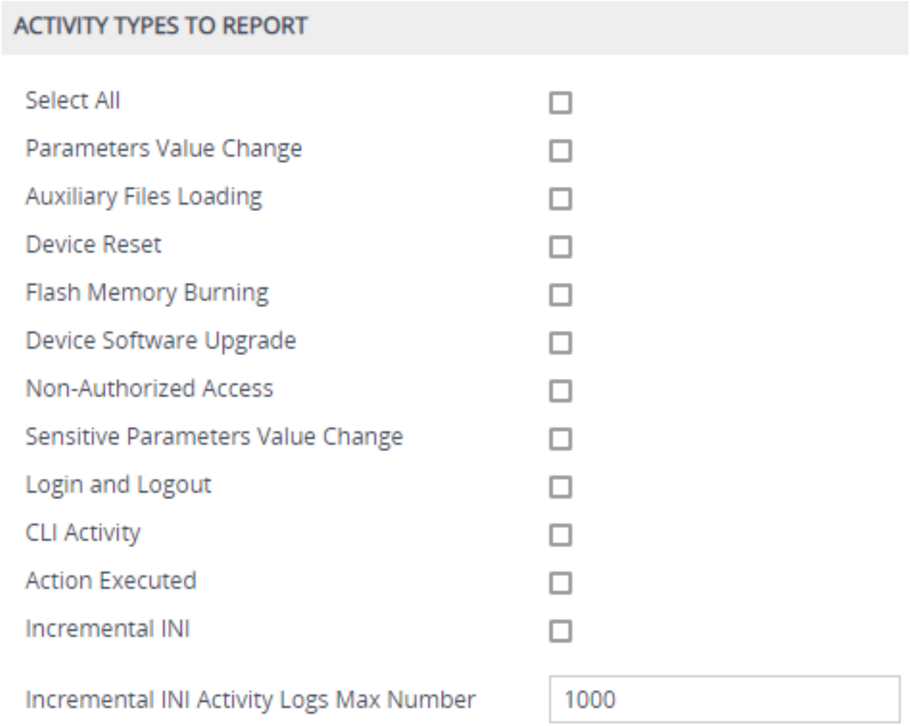
- Modifications of parameters due to an incremental ini file upload. If you choose this option, you can also define the maximum number of lines of parameters to log from the ini file, using the 'Incremental INI Activity Logs Max Number' parameter.
- Entered CLI commands (modifications of security-sensitive commands are logged without the entered value).
- Configuration file upload (reported without per-parameter notifications).
- Auxiliary file upload and software update.
- Device reset and burn to flash memory.
- Access to unauthorized Web pages according to the Web user's access level.
- Modifications of "sensitive" parameters.
- Log in and log out.
- Actions not related to parameter changes (for example, file uploads, file delete, lock-unlock maintenance actions, LDAP clear cache, register-unregister, and start-stop trunk). In the Web, these actions are typically done by clicking a button (e.g., the LOCK button).

For more information on each of the above listed options, see Syslog, CDR and Debug Parameters.

The following procedure describes how to configure management user activity logging through the Web interface. You can also configure it through ini file [ActivityListToLog] or CLI (`configure troubleshoot > activity-log`).

➢ To configure reporting of management user activities:

1. Open the Logging Settings page (**Troubleshoot** tab > **Troubleshoot** menu > **Logging** folder > **Logging Settings**).
2. Under the Activity Types to Report group, select the actions to report to the Syslog server. To select (or deselect) all activity types, click the 'Select All' check box.



ACTIVITY TYPES TO REPORT

Select All	☐
Parameters Value Change	☐
Auxiliary Files Loading	☐
Device Reset	☐
Flash Memory Burning	☐
Device Software Upgrade	☐
Non-Authorized Access	☐
Sensitive Parameters Value Change	☐
Login and Logout	☐
CLI Activity	☐
Action Executed	☐
Incremental INI	☐
Incremental INI Activity Logs Max Number	1000

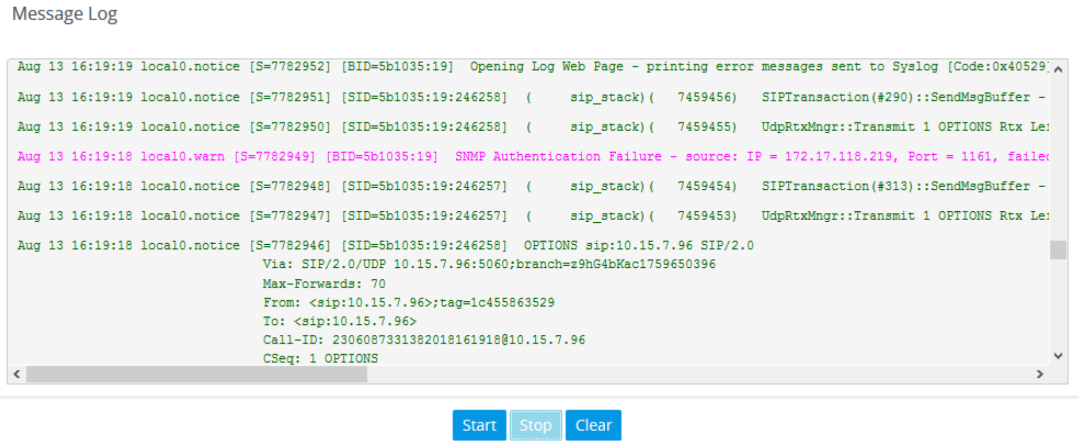
3. Click **Apply**.

- Logging of CLI commands can only be configured through CLI or ini file.
- You can configure the device to send an SNMP trap each time a user performs an action. For more information, see Enabling SNMP Traps for Web Activity on page 81.
- If you enable or enforce password obscurity (obscure-password-mode on or enforce-password-complexity) and a password is configured for a new management user (successfully or not) or the password of an existing user is modified (in the Local Users table), the password is not shown in the Activity Log.

Viewing Syslog Messages

You can view Syslog messages generated by the device using any of the following Syslog server types:

- **Device's Web Interface:** The device provides an embedded Syslog server, which is accessed through the Web interface (**Troubleshoot** tab > **Troubleshoot** menu > **Message Log** ⌂). You can select the Syslog messages displayed on the page, and then copy-and-paste them into a text editor such as Notepad. This text file (*txt*) can then be sent to AudioCodes support team for diagnosis and troubleshooting.



Message Log

```
Aug 13 16:19:19 local0.notice [S=7782952] [BID=5b1035:19]  Opening Log Web Page - printing error messages sent to Syslog [Code:0x40529]
Aug 13 16:19:19 local0.notice [S=7782951] [SID=5b1035:19:246258]  (     sip_stack)(   7459456)   SIPTransaction(#290)::SendMsgBuffer -
Aug 13 16:19:19 local0.notice [S=7782950] [SID=5b1035:19:246258]  (     sip_stack)(   7459455)   UdpRtxMngr::Transmit 1 OPTIONS Rtx Le
Aug 13 16:19:18 local0.warn [S=7782949] [BID=5b1035:19]  SNMP Authentication Failure - source: IP = 172.17.118.219, Port = 1161, faile
Aug 13 16:19:18 local0.notice [S=7782948] [SID=5b1035:19:246257]  (     sip_stack)(   7459454)   SIPTransaction(#313)::SendMsgBuffer -
Aug 13 16:19:18 local0.notice [S=7782947] [SID=5b1035:19:246257]  (     sip_stack)(   7459453)   UdpRtxMngr::Transmit 1 OPTIONS Rtx Le
Aug 13 16:19:18 local0.notice [S=7782946] [SID=5b1035:19:246258]  OPTIONS sip:10.15.7.96 SIP/2.0
                                Via: SIP/2.0/UDP 10.15.7.96:5060;branch=z9hG4bKac1759650396
                                Max-Forwards: 70
                                From: <sip:10.15.7.96>;tag=1c455863529
                                To: <sip:10.15.7.96>
                                Call-ID: 2306087331382018161918@10.15.7.96
                                CSeq: 1 OPTIONS
```

The displayed logged messages are color-coded based on message type:

- **"notice":** Dark green
- **"error", "crit", "alert", "emerg":** Red
- **"debug":** Black
- **"info":** Blue
- **"warn":** Magenta

The page provides various buttons to do the following actions:

Table 57-6: Buttons on Message Log Page

Button	Description
Start	Resumes the message log after it has been stopped (see the **Stop** button).
Stop	Stops the message log, allowing you to easily scroll through the messages to a specific message.
Clear	Clears the message log. The button can only be clicked after you have stopped the message log (see the **Stop** button). **Note:** If you navigate away from the Message Log page to another page, the Message Log is stopped and cleared.

> ⚠
> - It's not recommended to keep a Message Log session open for a prolonged period. This may cause the device to overload. For prolonged (and detailed) debugging, use an external Syslog server.
> - The Message Log page provides limited Syslog server functionality.

- **Device's CLI:** The device sends error messages (e.g., Syslog messages) to the CLI as well as to the configured destination.
  - To start debug recording:

    ```
    debug log
    ```

  - To stop debug recording:

    ```
    no debug log
    ```

  - To stop all debug recording:

    ```
    no debug log all
    ```

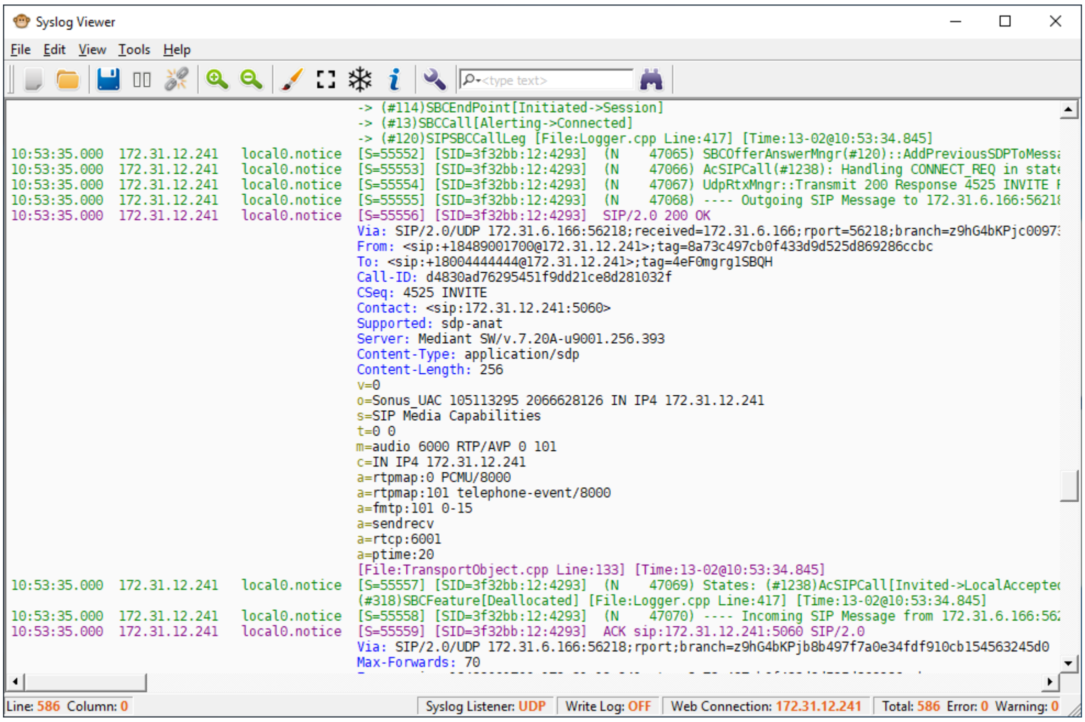
- Persistent Logging Storage on the Device: For more information, see Viewing Persistent-Logging Storage.
- **Wireshark:** Third-party, network protocol analyzer (http://www.wireshark.org).

> ⚠ When debug recording is enabled and Syslog messages are also included in the debug recording, to view Syslog messages using Wireshark, you must install AudioCodes' Wireshark plug-in (acsyslog.dll). Once the plug-in is installed, Syslog messages are decoded as "AC SYSLOG" and displayed using the "acsyslog" filter (instead of the regular "syslog" filter). For more information on debug recording, see Debug Recording.

- **AudioCodes Syslog Viewer:** This utility can be used for two major tasks:
  - Recording and displaying syslog messages from the device
  - Analyzing recorded logs (including support for interactive SIP ladder diagrams)

  To obtain the Syslog Viewer installation file, download it from https://www.audiocodes.com/library/firmware.

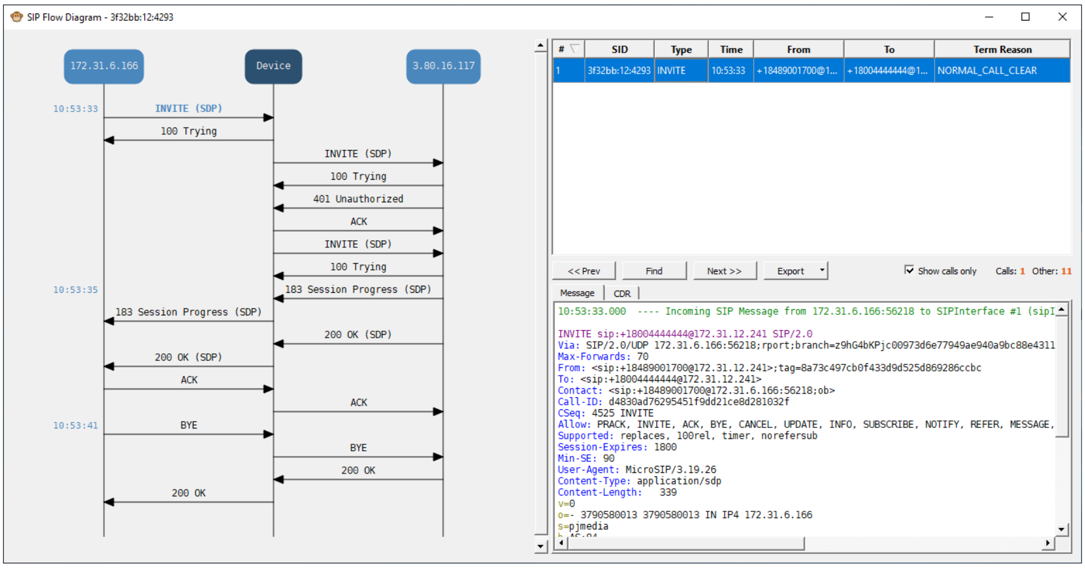
Figure 57-1: Example of Syslog Messages in Syslog Viewer



```
                                                  -> (#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) SBCOfferAnswerMngr(#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 172.31.6.166:5621
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=4eF0mgrglSBQH
                                                  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=rtcp: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)SBCFeature[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;branch=z9hG4bKPjb8b497f7a0e34fdf910cb154563245d0
                                                  Max-Forwards: 70
```

Line: 586 Column: 0 | Syslog Listener: UDP | Write Log: OFF | Web Connection: 172.31.12.241 | Total: 586 Error: 0 Warning: 0

Figure 57-2: Example of SIP Ladder Diagram in Syslog Viewer



#	SID	Type	Time	From	To	Term Reason
1	3f32bb:12:4293	INVITE	10:53:33	+18489001700@1...	+18004444444@1...	NORMAL_CALL_CLEAR

☑ Show calls only Calls: 1 Other: 11

```
10:53:33.000  ---- Incoming SIP Message from 172.31.6.166:56218 to SIPInterface #1 (sipI

INVITE sip:+18004444444@172.31.12.241 SIP/2.0
Via: SIP/2.0/UDP 172.31.6.166:56218;rport;branch=z9hG4bKPjc00973d6e77949ae940a9bc88e4311
Max-Forwards: 70
From: <sip:+18489001700@172.31.12.241>;tag=8a73c497cb0f433d9d525d869286ccbc
To: <sip:+18004444444@172.31.12.241>
Contact: <sip:+18489001700@172.31.6.166:56218;ob>
Call-ID: d4830ad76295451f9dd21ce8d281032f
CSeq: 4525 INVITE
Allow: PRACK, INVITE, ACK, BYE, CANCEL, UPDATE, INFO, SUBSCRIBE, NOTIFY, REFER, MESSAGE,
Supported: replaces, 100rel, timer, norefersub
Session-Expires: 1800
Min-SE: 90
User-Agent: MicroSIP/3.19.26
Content-Type: application/sdp
Content-Length:   339
v=0
o=- 3790580013 3790580013 IN IP4 172.31.6.166
s=pjmedia
```

- **Third-party, Syslog Server:** Any third-party, Syslog server program that enables filtering of messages according to parameters such as priority, IP sender address, time, and date.

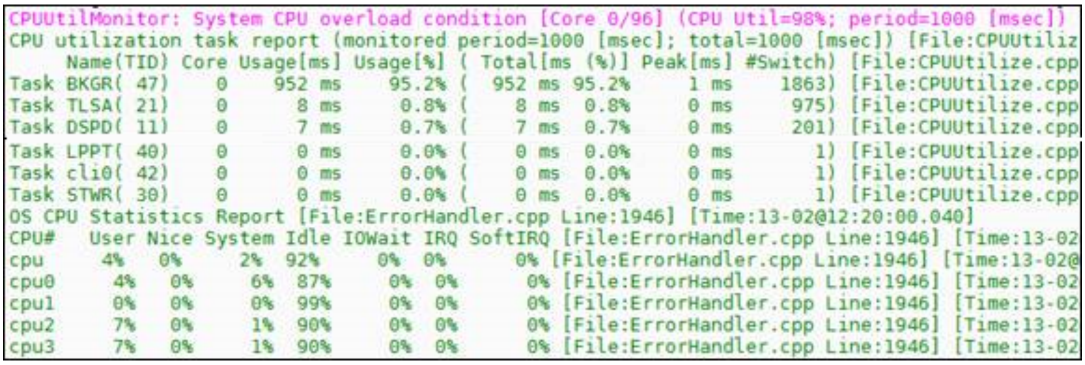
Syslog Message Description for CPU Overload

Whenever the device detects a CPU overload, it sends a Syslog message that shows CPU utilization of the different processes (tasks) per core. This information can help in identifying the cause of the overload. When the devicedetects a CPU overload, it sends a Syslog message every 10 seconds until it returns to normal state.

You can also view CPU utilization through the CLI, by using the following command:

```
show system utilization
```

The figure below shows an example of a Syslog message generated because of a CPU overload. CPU utilization information is shown under the "CPUUtilMonitor" section (shown in pink). The subsequent table describes the displayed information.



```
CPUUtilMonitor: System CPU overload condition [Core 0/96] (CPU Util=98%; period=1000 [msec])
CPU utilization task report (monitored period=1000 [msec]; total=1000 [msec]) [File:CPUUtiliz
     Name(TID) Core Usage[ms] Usage[%] ( Total[ms (%)] Peak[ms] #Switch) [File:CPUUtilize.cpp
Task BKGR( 47)    0    952 ms    95.2% (  952 ms 95.2%     1 ms    1863) [File:CPUUtilize.cpp
Task TLSA( 21)    0      8 ms     0.8% (    8 ms  0.8%     0 ms     975) [File:CPUUtilize.cpp
Task DSPD( 11)    0      7 ms     0.7% (    7 ms  0.7%     0 ms     201) [File:CPUUtilize.cpp
Task LPPT( 40)    0      0 ms     0.0% (    0 ms  0.0%     0 ms       1) [File:CPUUtilize.cpp
Task cli0( 42)    0      0 ms     0.0% (    0 ms  0.0%     0 ms       1) [File:CPUUtilize.cpp
Task STWR( 30)    0      0 ms     0.0% (    0 ms  0.0%     0 ms       1) [File:CPUUtilize.cpp
OS CPU Statistics Report [File:ErrorHandler.cpp Line:1946] [Time:13-02@12:20:00.040]
CPU#   User Nice System Idle IOWait IRQ SoftIRQ [File:ErrorHandler.cpp Line:1946] [Time:13-02
cpu     4%   0%      2%  92%     0%  0%      0% [File:ErrorHandler.cpp Line:1946] [Time:13-02@
cpu0     4%   0%      6%  87%     0%  0%      0% [File:ErrorHandler.cpp Line:1946] [Time:13-02
cpu1     0%   0%      0%  99%     0%  0%      0% [File:ErrorHandler.cpp Line:1946] [Time:13-02
cpu2     7%   0%      1%  90%     0%  0%      0% [File:ErrorHandler.cpp Line:1946] [Time:13-02
cpu3     7%   0%      1%  90%     0%  0%      0% [File:ErrorHandler.cpp Line:1946] [Time:13-02
```

Table 57-7: CPU Overload Fields Description in Syslog Message

Field	Description
First line (shown in pink)	
“Core”	Index of the CPU core.
“CPU Util”	CPU utilization (in percentage).
“period”	Total period (in msec).
Second line	
“monitored period”	Duration (in msec) of CPU overload within the total monitored period.
“total“	Monitored period (in msec).
Statistics per task (process) in overloaded cores only **Note:** By default, the Syslog message only shows the five most used tasks in the last period.	
“Name (TID)”	Name of task (process).
“Core”	Index of the CPU core.
“Usage [ms]”	Total time (msec) of monitored period that the task utilized CPU.

Field	Description
“Usage [%]”	Percentage of time of monitored period that the task utilized CPU.
“Total [ms (%)]”	Total time (in msec) and percentage that task utilized CPU during entire period.
“peak [ms]”	Maximum lasting time (msec) that the task utilized CPU during the period.
“#Switch”	Context switch time - number of consecutive periods that were allocated for this task.
Statistics per CPU core	
"CPU#"	Index of the CPU core.
"User"	Percentage of CPU utilization that occurred while executing at the user level (application).
"Nice"	Percentage of CPU utilization that occurred while executing at the user level with nice priority (Linux systems).
"System"	Percentage of CPU utilization that occurred while executing at the system level (kernel).
"Idle"	Percentage of time that the CPU was idle (%) during which no tasks were using the CPU core.
"IOWait"	Percentage of time that the CPU was idle (5) during which tasks were using the CPU core.
"IRQ"	IRQ time (in percentage).
"SoftIRQ"	SoftIRQ time (in percentage%).

Packet Loss Indication in Syslog

The device reports packet loss (PL) of incoming (Rx) RTP media streams (calls) in 15-second intervals. The device obtains packet loss statistics from the RTCP of the RTP streams. When packet loss occurs in the 15-second interval, at the end of the interval the device sends a Syslog message with Warning severity level, indicating this packet loss. The Syslog indicates the number of calls that experienced packet loss per packet loss range (in percentage) during the interval. It also indicates the number of calls that didn't have packet loss. If no packet loss occurred in all the RTP streams in the 15-second interval, no Syslog message is sent.

Below shows an example of a Syslog message sent when packet loss occurred in the 15-second interval. This Syslog indicates that 6 calls were active during the interval. One call had no packet loss, 3 calls had 1 to 2% packet loss, and 2 calls had 5 to 100% packet loss:

```
16:47:13.921 192.168.8.70 local0.warn [S=2116] [BID=884772:92] Packets-Loss
report [PL range]=#media-legs: [No PL]=1, [up to 0.5%]=0, [0.5% - 1%]=0, [1% -
2%]=3, [2% - 5%]=0, [5% - 100%]=2 [[Time:28-12@00:40:18.550|time:28-
12@00:40:18.550]]
```

Below shows the default packet-loss ranges in the Syslog:

- [No PL]: Indicates the number of calls without packet loss.
- [up to 0.5%]: Indicates the number of calls with up to 0.5% packet loss. This packet loss typically has no effect on voice quality.
- [0.5% - 1%]: Indicates the number of calls with 0.5 to 1% packet loss. This packet loss typically has no effect on voice quality.
- [1% - 2%]: Indicates the number of calls with 1 to 2% packet loss. This packet loss may affect voice quality for calls using certain vocoders.
- [2% - 5%]: Indicates the number of calls with 2 to 5% packet loss. This packet loss affects voice quality and typically indicates a network problem.
- [5% - 100%]: Indicates the number of calls with 5 to 100% packet loss. This packet loss affects voice quality and typically indicates a network problem.

You can change these packet-loss ranges, using the [PLThresholdLevelsPerMille] parameter. For more information, see Syslog, CDR, SDR and Debug Parameters on page 1247.

- The packet loss report in the Syslog message should be carefully considered. For example, for calls that are opened and then closed during the 15-second interval, packet loss statistics may be misleading due to insufficient packets for accurate calculation. Therefore, if the Syslog message shows very few calls in the high packet-loss ranges, then you should probably ignore them as it might be due to this scenario. On the other hand, if there is a large number of calls falling into these high packet-loss ranges, then it probably indicates network problems.
- When the device is deployed in the cloud (e.g., Microsoft Azure), it is normal to see calls in the low packet-loss ranges. This is due to various network elements used in these networks.

Configuring Debug Recording

This section describes how to configure debug recording and how to collect debug recording packets.