SonicWall SonicOS/X 7.0.1 Log Events

Reference Guide

SONIC**WALL**®

Contents

Introduction to SonicOS/X Log Events

This reference guide lists and describes the SonicWall SonicOS and SonicOSX (SonicOS/X) log event messages for the SonicOS/X 7.0.1 release on SonicWall NS*sp*, NS*a*, NS*v*, and TZ network security appliances. The Log Event Message Index table lists all events by event ID number. The Syslog Tags table lists and describes all available Syslog tags which contain additional information specific to the log event.

This section provides a basic overview of the **MONITOR | Logs > System Logs** and **DEVICE | Log > Settings** pages and the **Logging** option in the **Adding Rule** dialog on the **POLICY | Rules and Policies > Access Rules** page in the SonicOS web based management interface.
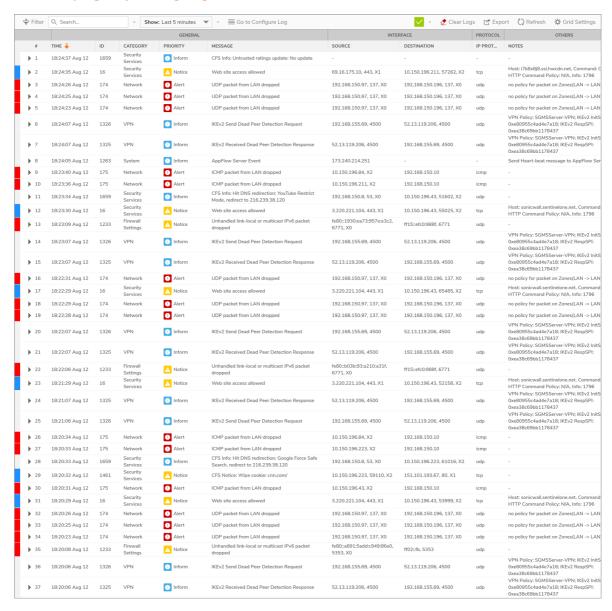
Topics:

Logs > System Logs

The SonicWall security appliance maintains a log of events on the firewall for tracking potential security threats. This log can be viewed by navigating to the **MONITOR | Logs > System Logs** page and it can be exported to a CSV file, text file, or sent to an email address for convenience and archiving. The log is displayed in a table and can be sorted by clicking on any of the column headings.

For more information about viewing, filtering and displaying event details on the **System Logs** page, refer to the *SonicOS/X 7 Monitor Logs* administration guide, available on the SonicWall Technical Documentation portal at https://www.sonicwall.com/support/technical-documentation.

Filter | Search... | Show: Last 5 minutes | Go to Configure Log | Clear Logs | Export | Refresh | Grid Settings

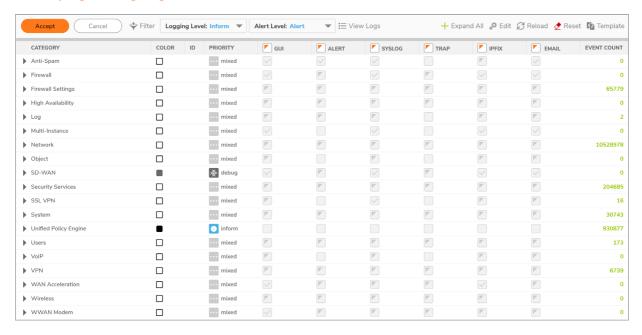| #	TIME	ID	CATEGORY	PRIORITY	MESSAGE	SOURCE	DESTINATION	IP PROT...	NOTES
1	18:24:37 Aug 12	1659	Security Services	Inform	CFS Info: Untrusted ratings update: No update	-	-	-	-
2	18:24:35 Aug 12	16	Security Services	Notice	Web site access allowed	69.16.175.10, 443, X1	10.150.196.211, 57262, X2	tcp	Host: i7k8x8j8.ssl.hwcdn.net, Command: C HTTP Command Policy: N/A, Info: 1796
3	18:24:26 Aug 12	174	Network	Alert	UDP packet from LAN dropped	192.168.150.97, 137, X0	192.168.150.196, 137, X0	udp	no policy for packet on Zones(LAN -> LAN
4	18:24:25 Aug 12	174	Network	Alert	UDP packet from LAN dropped	192.168.150.97, 137, X0	192.168.150.196, 137, X0	udp	no policy for packet on Zones(LAN -> LAN
5	18:24:23 Aug 12	174	Network	Alert	UDP packet from LAN dropped	192.168.150.97, 137, X0	192.168.150.196, 137, X0	udp	no policy for packet on Zones(LAN -> LAN
6	18:24:07 Aug 12	1326	VPN	Inform	IKEv2 Send Dead Peer Detection Request	192.168.155.69, 4500	52.13.119.206, 4500	udp	VPN Policy: SGMSServer-VPN; IKEv2 InitS 0xe80955c4ad4e7a18; IKEv2 RespSPI: 0xea38c69bb1178437
7	18:24:07 Aug 12	1325	VPN	Inform	IKEv2 Received Dead Peer Detection Response	52.13.119.206, 4500	192.168.155.69, 4500	udp	VPN Policy: SGMSServer-VPN; IKEv2 InitS 0xe80955c4ad4e7a18; IKEv2 RespSPI: 0xea38c69bb1178437
8	18:24:05 Aug 12	1263	System	Inform	AppFlow Server Event	173.240.214.251	-	-	Send Heart-beat message to AppFlow Ser
9	18:23:40 Aug 12	175	Network	Alert	ICMP packet from LAN dropped	10.150.196.84, X2	192.168.150.10	icmp	-
10	18:23:36 Aug 12	175	Network	Alert	ICMP packet from LAN dropped	10.150.196.211, X2	192.168.150.10	icmp	-
11	18:23:34 Aug 12	1659	Security Services	Inform	CFS Info: Hit DNS redirection: YouTube Restrict Mode, redirect to 216.239.38.120	192.168.150.8, 53, X0	10.150.196.43, 51602, X2	udp	-
12	18:23:30 Aug 12	16	Security Services	Notice	Web site access allowed	3.220.221.104, 443, X1	10.150.196.43, 55025, X2	tcp	Host: sonicwall.sentinelone.net, Command HTTP Command Policy: N/A, Info: 1796
13	18:23:09 Aug 12	1233	Firewall Settings	Notice	Unhandled link-local or multicast IPv6 packet dropped	fe80::1930:ea73:957e:e3c2, 6771, X0	ff15::efc0:988f, 6771	udp	-
14	18:23:07 Aug 12	1326	VPN	Inform	IKEv2 Send Dead Peer Detection Request	192.168.155.69, 4500	52.13.119.206, 4500	udp	VPN Policy: SGMSServer-VPN; IKEv2 InitS 0xe80955c4ad4e7a18; IKEv2 RespSPI: 0xea38c69bb1178437
15	18:23:07 Aug 12	1325	VPN	Inform	IKEv2 Received Dead Peer Detection Response	52.13.119.206, 4500	192.168.155.69, 4500	udp	VPN Policy: SGMSServer-VPN; IKEv2 InitS 0xe80955c4ad4e7a18; IKEv2 RespSPI: 0xea38c69bb1178437
16	18:22:31 Aug 12	174	Network	Alert	UDP packet from LAN dropped	192.168.150.97, 137, X0	192.168.150.196, 137, X0	udp	no policy for packet on Zones(LAN -> LAN
17	18:22:29 Aug 12	16	Security Services	Notice	Web site access allowed	3.220.221.104, 443, X1	10.150.196.43, 65485, X2	tcp	Host: sonicwall.sentinelone.net, Command HTTP Command Policy: N/A, Info: 1796
18	18:22:29 Aug 12	174	Network	Alert	UDP packet from LAN dropped	192.168.150.97, 137, X0	192.168.150.196, 137, X0	udp	no policy for packet on Zones(LAN -> LAN
19	18:22:28 Aug 12	174	Network	Alert	UDP packet from LAN dropped	192.168.150.97, 137, X0	192.168.150.196, 137, X0	udp	no policy for packet on Zones(LAN -> LAN
20	18:22:07 Aug 12	1326	VPN	Inform	IKEv2 Send Dead Peer Detection Request	192.168.155.69, 4500	52.13.119.206, 4500	udp	VPN Policy: SGMSServer-VPN; IKEv2 InitS 0xe80955c4ad4e7a18; IKEv2 RespSPI: 0xea38c69bb1178437
21	18:22:07 Aug 12	1325	VPN	Inform	IKEv2 Received Dead Peer Detection Response	52.13.119.206, 4500	192.168.155.69, 4500	udp	VPN Policy: SGMSServer-VPN; IKEv2 InitS 0xe80955c4ad4e7a18; IKEv2 RespSPI: 0xea38c69bb1178437
22	18:22:06 Aug 12	1233	Firewall Settings	Notice	Unhandled link-local or multicast IPv6 packet dropped	fe80::b03b:93:a210:a31f, 6771, X0	ff15::efc0:988f, 6771	udp	-
23	18:21:29 Aug 12	16	Security Services	Notice	Web site access allowed	3.220.221.104, 443, X1	10.150.196.43, 52158, X2	tcp	Host: sonicwall.sentinelone.net, Command HTTP Command Policy: N/A, Info: 1796
24	18:21:07 Aug 12	1325	VPN	Inform	IKEv2 Received Dead Peer Detection Response	52.13.119.206, 4500	192.168.155.69, 4500	udp	VPN Policy: SGMSServer-VPN; IKEv2 InitS 0xe80955c4ad4e7a18; IKEv2 RespSPI: 0xea38c69bb1178437
25	18:21:06 Aug 12	1326	VPN	Inform	IKEv2 Send Dead Peer Detection Request	192.168.155.69, 4500	52.13.119.206, 4500	udp	VPN Policy: SGMSServer-VPN; IKEv2 InitS 0xe80955c4ad4e7a18; IKEv2 RespSPI: 0xea38c69bb1178437
26	18:20:34 Aug 12	175	Network	Alert	ICMP packet from LAN dropped	10.150.196.84, X2	192.168.150.10	icmp	-
27	18:20:33 Aug 12	175	Network	Alert	ICMP packet from LAN dropped	10.150.196.223, X2	192.168.150.10	icmp	-
28	18:20:33 Aug 12	1659	Security Services	Inform	CFS Info: Hit DNS redirection: Google Force Safe Search, redirect to 216.239.38.120	192.168.150.8, 53, X0	10.150.196.223, 61016, X2	udp	-
29	18:20:32 Aug 12	1461	Security Services	Notice	CFS Notice: Wipe cookie: cnn.com/	10.150.196.223, 59110, X2	151.101.193.67, 80, X1	tcp	-
30	18:20:31 Aug 12	175	Network	Alert	ICMP packet from LAN dropped	10.150.196.43, X2	192.168.150.10	icmp	-
31	18:20:29 Aug 12	16	Security Services	Notice	Web site access allowed	3.220.221.104, 443, X1	10.150.196.43, 53999, X2	tcp	Host: sonicwall.sentinelone.net, Command HTTP Command Policy: N/A, Info: 1796
32	18:20:26 Aug 12	174	Network	Alert	UDP packet from LAN dropped	192.168.150.97, 137, X0	192.168.150.196, 137, X0	udp	no policy for packet on Zones(LAN -> LAN
33	18:20:25 Aug 12	174	Network	Alert	UDP packet from LAN dropped	192.168.150.97, 137, X0	192.168.150.196, 137, X0	udp	no policy for packet on Zones(LAN -> LAN
34	18:20:23 Aug 12	174	Network	Alert	UDP packet from LAN dropped	192.168.150.97, 137, X0	192.168.150.196, 137, X0	udp	no policy for packet on Zones(LAN -> LAN
35	18:20:08 Aug 12	1233	Firewall Settings	Notice	Unhandled link-local or multicast IPv6 packet dropped	fe80::a891:5add:c949:86e0, 5353, X0	ff02::fb, 5353	udp	-
36	18:20:06 Aug 12	1326	VPN	Inform	IKEv2 Send Dead Peer Detection Request	192.168.155.69, 4500	52.13.119.206, 4500	udp	VPN Policy: SGMSServer-VPN; IKEv2 InitS 0xe80955c4ad4e7a18; IKEv2 RespSPI: 0xea38c69bb1178437
37	18:20:06 Aug 12	1325	VPN	Inform	IKEv2 Received Dead Peer Detection Response	52.13.119.206, 4500	192.168.155.69, 4500	udp	VPN Policy: SGMSServer-VPN; IKEv2 InitS 0xe80955c4ad4e7a18; IKEv2 RespSPI: 0xea38c69bb1178437

Log > Settings

The **DEVICE | Log > Settings** page allows you to categorize and customize the logging functions on your SonicWall security appliance for troubleshooting and diagnostics. The page displays logging settings in a series of columns and allows you to configure the logging and alert levels, edit attributes of categories, groups, and events, and reset event counts. You can filter the entries to limit the data display to only those events of interest. You can select storage options on appliances with built-in or flexible storage components, and you can import and save logging templates.

For more information on configuring the **DEVICE | Log > Settings** page, refer to the *SonicOS/X 7 Device Log* administration guide.

DEVICE | Log > Settings Page

Traffic Report Syslogs

The Traffic Report Syslog event messages, their 'c' values, Syslog IDs, and location in the table on the **DEVICE | Log > Settings** page are listed in the Traffic Report Syslogs table.

Traffic Report Syslogs

Event Message	Syslog 'c' Value	Syslog ID	Location in Log > Settings	Comments
Syslog Website Accessed	**c=1024**	97	Category: Log Group: Syslog Event: Syslog Website Accessed	This means Traffic Reporting, including bytes transferred. Has URL data
Connection Closed	**c=1024**	537	Category: Network Group: Network Access Event: Connection Closed	Non-URL traffic
SSL VPN Traffic	**c=1024**	1153	Category: SSL VPN Group: General Event: SSL VPN Traffic	Statistics reported by SSL VPN

Traffic Report Syslogs

Event Message	Syslog 'c' Value	Syslog ID	Location in Log > Settings	Comments
DPI-SSL Inspection Cleaned-up	**c=1024**	1463	Category: Security Services Group: DPI-SSL Event: DPI-SSL Inspection Cleaned-up	Statistics reported by DPI-SSL
Connection Opened	**c=262144**	98	Category: Network Group: Network Access Event: Connection Opened	This means Connection Opened (most probably zero bytes transferred). It is possible for some packets to trigger a Connection Opened, but later be dropped due to policy settings.

The Traffic Report Syslogs are generated only if those messages are enabled in the **Log > Settings** page with the desired **Frequency Filter Interval**, normally 0, which means do not filter. They are always generated on Connection Closed events.

The Connection Closed event is represented by two different messages, id=97 and id=537. The Syslog Website Accessed (97) contains URL data while Connection Closed (537) does not.

On the **Log > Settings** page, expand the item in the **Category** column to display the group names and then expand the group to display the events in that group. For example, expand **Log**, then expand **Syslog** to display the **Syslog Website Accessed** event.

Events Displayed in Expanded Table

Click the Edit button in the row for the event to open the **Edit Event** dialog.

Edit Button

CATEGORY	COLOR	ID
▼ Log	☐	
▶ AWS	■	
▶ Configuration Auditing	■	
▶ E-mail	☐	
▶ FTP	☐	
▶ General	☐	
▼ Syslog	☐	
Syslog Website Accessed	■	97
Maximum Syslog Data Rate Exceeded	■	655
Syslog Server Unreachable	■	657

Edit this profile

You can then view or enable/disable the **Report Events via Syslog** option and configure its **Frequency Filter Interval**. A value of zero for the **Frequency Filter Interval** means to log every event (no filtering).

Edit Event Dialog

Edit Event 'Syslog Website Accessed'

	Enable	Frequency Filter Interval	
Event Priority		inform ▼	
Display Events in Log Monitor	☐	Multiple Values	seconds
Send Events as Email Alerts	☐	Multiple Values	seconds
Report Events via Syslog	☑	0	seconds
Use This Syslog Server Profile			ⓘ
Include Events in Log Digest	☐		
Report Events via SNMP Trap	☐	Multiple Values	seconds
SNMP OID Name(Trap Type)		swFwTrapEnhNetworkTraffic(7401)	
Send Alerts to E-mail Address			
Leave color settings unchanged	⬤ ■ = current color (click button to change)		

Cancel   Save

Access Rules Logging Control

In SonicOS, the **Adding Rule** dialog launched by clicking **+Add** on the **POLICY | Rules and Policies > Access Rules** page provides the **Logging** toggle button. This option controls the policy logs – when the **Logging** option is enabled, event messages are logged for that policy, otherwise no messages are logged for it.

ⓘ | **NOTE:** The **Logging** option is only available on firewalls running SonicOS (Classic mode), but not on firewalls running SonicOSX (Policy mode).

Logging Option on Adding Rule > Logging Screen

The associated policy log events are listed in the Policy Logs Controlled by Enable Logging Option in Access Rules table.

Policy Logs Controlled by Enable Logging Option in Access Rules

Syslog ID	Event Message	Packets Allowed or Dropped
526	Web Request Receiver	Allowed
1235	Packet Allowed	Allowed
36	TCP Packets Dropped	Dropped
38	ICMP Packets Dropped	Dropped
41	Unknown Protocol Dropped	Dropped
173	LAN TCP Deny	Dropped
174	LAN UDP Deny	Dropped
175	LAN ICMP Deny	Dropped
522	Malformed IP Packet	Dropped
524	Web Request Drop	Dropped
533	ESP Drop	Dropped
534	AH Drop	Dropped
652	IPcomp Packet Drop	Dropped
1253	IPv6 Tunnel Dropped	Dropped
1254	LAN ICMPv6 Deny	Dropped

Policy Logs Controlled by Enable Logging Option in Access Rules

Syslog ID	Event Message	Packets Allowed or Dropped
1257	ICMPv6 Packets Dropped	Dropped
1447	UDPv6 Packets Dropped	Dropped

Index of Log Event Messages

This section contains the Log Event Message Index, which is a list of log event messages for the SonicOS/X 7.0.1 firmware.

Each log event message described in the table provides the following log event details:

- **Event ID**—Displays the ID number of the log event message.

- **SonicOS/X Category Name**—Displays category names as shown in the **DEVICE | Log > Settings** page in the **Category** column of the table. The **MONITOR | Logs > System Logs** page also has the **Category** column, which can be displayed (if not already) by clicking **Grid Settings** at the top and selecting the **Category** checkbox under **General** in the **Column Selection** screen of the **Grid Settings** dialog.

- **SonicOS/X Group Name**—Displays group names as shown in the **DEVICE | Log > Settings** page by expanding a category in the **Category** column of the table. The **MONITOR | Logs > System Logs** page displays the groups in the **Group** column, which can be displayed by clicking **Grid Settings** at the top and selecting the **Group** checkbox under **General** in the **Column Selection** screen of the **Grid Settings** dialog.

- **Syslog Legacy Category**—Displays the Syslog category event type. This is the same category as Legacy Categories on page 109.

- **Priority Level**—Displays the level of urgency of the log event message. The table shows the factory default value of **Event Priority** for the event. The field is displayed as the **Priority** column found in **DEVICE | Log > Settings** and in **MONITOR | Logs > System Logs** (if **Priority** column is enabled). For additional information, see Priority Levels on page 110.

- **SNMP Trap Type**—Displays the SNMP Trap ID number of the log event message. In order for an SNMP Trap to be generated for the event, the **Send Events as Email Alerts** checkbox needs to be enabled for the event with the desired **Frequency Filter Interval**, normally 0, which means do not filter. Also, SNMP settings must be configured.

  To edit settings for an event, go to the **DEVICE | Log > Settings** page, expand the item in the **Category** column to display the group names and then expand the group to display the events in that group. To open the **Edit Event** dialog, click the Edit button in the row for the event.

  The values in this column are defined in the SONICWALL-FIREWALL-TRAP-MIB released with each firmware.

- **Event Name**—Displays a descriptive name for the log event, corresponding to the event row label in **DEVICE | Log > Settings** (after expanding both **Category** and **Group**) and can be shown in the **MONITOR | Logs > System Logs** page by enabling the **Event** column in the **Grid Settings**.

- **Log Event Message**—Displays the text of the log event message. Sometimes includes "%s", which is dynamically replaced by SonicOS/X with descriptive text in the actual log event message.

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
4	System	Status	Maintenance	ALERT	5201	Activate Firewall	Network Security Appliance activated
5	Log	General	Maintenance	INFO	5601	Clear Log	Log Cleared
6	Log	E-mail	Maintenance	INFO	5602	E-mail Log	Log successfully sent via E-mail
10	Security Services	General	System Error	ERROR	602	Setting Error on Load	Problem loading the URL List; check Filter settings
12	Log	E-mail	System Error	WARNING	604	E-mail Check Error on Load	Problem sending log E-mail; check log settings
14	Security Services	Content Filter	Blocked Sites	ERROR	701	Website Blocked	Web site access denied
16	Security Services	Content Filter	Blocked Sites	NOTICE	703	Website Accessed	Web site access allowed
22	Security Services	Attacks	Attack	ALERT	501	Ping of Death Blocked	Ping of death dropped
23	Security Services	Attacks	Attack	ALERT	502	IP Spoof Detected	IP spoof dropped
24	Users	Authentication Access	User Activity	INFO	4201	User Disconnect Detected	User logged out - user disconnect detected
25	Firewall Settings	Flood Protection	Attack	WARNING	503	Possible SYN Flood	Possible SYN flood attack detected
27	Security Services	Attacks	Attack	ALERT	505	Land Attack	Land attack dropped
28	Network	IP	TCP | UDP | ICMP	NOTICE	7001	Fragmented Packet	Fragmented packet dropped
29	Users	Authentication Access	User Activity	INFO	4202	Successful Admin Login	Administrator login allowed
30	Users	Authentication Access	Attack	ALERT	560	Wrong Admin Password	Administrator login denied due to bad credentials
31	Users	Authentication Access	User Activity	INFO	4204	Successful User Login	User login from an internal zone allowed
32	Users	Authentication Access	User Activity	INFO	4205	Wrong User Password	User login denied due to bad credentials
33	Users	Authentication Access	User Activity	INFO	4206	Unknown User Login Attempt	User login denied due to bad credentials
34	Users	Authentication Access	User Activity	INFO	4207	Login Timeout	Pending login timed out

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
35	Users	Authentication Access	Attack	ALERT	506	Admin Login Disabled	Administrator login denied from %s; logins disabled from this interface
36	Network	TCP	TCP	NOTICE	7209	TCP Packets Dropped	TCP connection dropped
37	Network	UDP	UDP	NOTICE	7210	UDP Packets Dropped	UDP packet dropped
38	Network	ICMP	ICMP	NOTICE	7211	ICMP Packets Dropped	ICMP packet dropped due to Policy
41	Network	Network Access	Debug	NOTICE	7214	Unknown Protocol Dropped	Unknown protocol dropped
43	VPN	VPN IPsec	Debug	DEBUG	7216	IPsec Interrupt Error	IPsec connection interrupt
45	Network	ARP	Debug	DEBUG	7002	ARP Failure	ARP Timeout
46	Network	Network Access	Debug	DEBUG	7217	Broadcast Packets Dropped	Broadcast packet dropped
48	Network	TCP	Debug	DEBUG	7218	Out of Order Packets Dropped	Out-of-order command packet dropped
53	System	Status	System Error	ERROR	607	Connection Cache Full	The cache is full; %s open connections; some will be dropped
58	Network	Interfaces	System Error	ERROR	608	Too Many IP on LAN	License exceeded: Connection dropped because too many IP addresses are in use on your LAN
61	VPN	VPN IPsec	System Error	ERROR	609	Out of Memory	Diagnostic Code E
63	Network	ICMP	Debug	DEBUG	7003	ICMP Too Big	Received fragmented packet or fragmentation needed
65	VPN	VPN IPsec	User Activity	INFO	9603	Illegal SPI	Illegal IPsec SPI
67	VPN	VPN IPsec	Attack	WARNING	508	IPsec Authenticate Failure	IPsec Authentication Failed
69	VPN	VPN IPsec	User Activity	INFO	9607	Incompatible SA	Incompatible IPsec Security Association
70	VPN	VPN IPsec	Attack	WARNING	510	Illegal IPsec Peer	IPsec packet from or to an illegal host

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
81	Security Services	Attacks	Attack	ALERT	520	Smurf Attack	Smurf Amplification attack dropped
82	Security Services	Attacks	Attack	ALERT	521	Port Scan Possible	Possible port scan detected
83	Security Services	Attacks	Attack	ALERT	522	Port Scan Probable	Probable port scan detected
84	Network	DNS	Maintenance	NOTICE	7004	Name Resolve Failed	Failed to resolve name
87	VPN	VPN IKE	User Activity	INFO	9401	IPsec Proposal Accepted	IKE Responder: Accepting IPsec proposal (Phase 2)
88	VPN	VPN IKE	User Activity	WARNING	523	IPsec Proposal Rejected	IKE Responder: IPsec proposal does not match (Phase 2)
89	VPN	VPN IKE	User Activity	NOTICE	9403	IPsec SA Added	IKE negotiation complete. Adding IPsec SA. (Phase 2)
93	System	Restart	System Error	ERROR	611	Suspend Reboot	Diagnostic Code A
94	System	Restart	System Error	ERROR	612	Deadlock Reboot	Diagnostic Code B
95	System	Restart	System Error	ERROR	613	Low Memory Reboot	Diagnostic Code C
96	System	NSM	Maintenance	INFO	6001	NSM Heartbeat	Status
97	Log	Syslog	Connection Traffic	INFO	7401	Syslog Website Accessed	Web site hit
98	Network	Network Access	Connection	INFO	7402	Connection Opened	Connection Opened
99	Network	DHCP Client	Maintenance	INFO	4801	DHCPC Retransmit Discover	Retransmitting DHCP DISCOVER.
100	Network	DHCP Client	Maintenance	INFO	4802	DHCPC Retransmit Request	Retransmitting DHCP Request (Requesting).
101	Network	DHCP Client	Maintenance	INFO	4803	DHCPC Retransmit Request Renew	Retransmitting DHCP Request (Renewing).
102	Network	DHCP Client	Maintenance	INFO	4804	DHCPC Retransmit Request Rebind	Retransmitting DHCP Request (Rebinding).
103	Network	DHCP Client	Maintenance	INFO	4805	DHCPC Retransmit Request Reboot	Retransmitting DHCP Request (Rebooting).

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
104	Network	DHCP Client	Maintenance	INFO	4806	DHCPC Retransmit Request Verify	Retransmitting DHCP Request (Verifying).
105	Network	DHCP Client	Maintenance	INFO	4807	DHCPC Discover	Sending DHCP DISCOVER.
106	Network	DHCP Client	Maintenance	INFO	4808	DHCPC No Offer	DHCP Server not available. Did not get any DHCP OFFER.
107	Network	DHCP Client	Maintenance	INFO	4809	DHCPC Offer Receive	Got DHCP OFFER. Selecting.
108	Network	DHCP Client	Maintenance	INFO	4810	DHCPC Selecting	Sending DHCP Request.
109	Network	DHCP Client	Maintenance	NOTICE	4811	DHCPC Request Failed	DHCP Client did not get DHCP ACK.
110	Network	DHCP Client	Maintenance	INFO	4812	DHCPC Request NAK	DHCP Client got NACK.
111	Network	DHCP Client	Maintenance	INFO	4813	DHCPC Request ACK	DHCP Client got ACK from server.
112	Network	DHCP Client	Maintenance	INFO	4814	DHCPC Request Decline	DHCP Client is declining address offered by the server.
113	Network	DHCP Client	Maintenance	INFO	4815	DHCPC Bound Rebind	DHCP Client sending Request and going to REBIND state.
114	Network	DHCP Client	Maintenance	INFO	4816	DHCPC Bound Renew	DHCP Client sending Request and going to RENEW state.
115	Network	DHCP Client	Maintenance	INFO	4817	DHCPC Request Renew	Sending DHCP Request (Renewing).
116	Network	DHCP Client	Maintenance	INFO	4818	DHCPC Request Rebind	Sending DHCP Request (Rebinding).
117	Network	DHCP Client	Maintenance	INFO	4819	DHCPC Request Reboot	Sending DHCP Request (Rebooting).
118	Network	DHCP Client	Maintenance	INFO	4820	DHCPC Request Verify	Sending DHCP Request (Verifying).
119	Network	DHCP Client	Maintenance	NOTICE	4821	DHCPC Verify Initiation Failed	DHCP Client failed to verify and lease has expired. Go to INIT state.
121	Network	DHCP Client	Maintenance	NOTICE	4823	DHCPC Get New IP	DHCP Client got a new IP address lease.

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
122	Network	DHCP Client	Maintenance	INFO	4824	DHCPC Send Release	Sending DHCP RELEASE.
123	Security Services	Anti-Virus	Maintenance	INFO	8605	AV Access Without Agent	Access attempt from host without Anti-Virus agent installed
124	Security Services	Anti-Virus	Maintenance	INFO	8606	AV Agent Out of Date	Anti-Virus agent out-of-date on host
125	Security Services	Anti-Virus	Maintenance	WARNING	524	AV Alert Receive	Received AV Alert: %s
127	Network	PPPoE	Maintenance	INFO	7801	PPPoE Start	Starting PPPoE discovery
128	Network	PPPoE	Maintenance	INFO	7802	PPPoE Link Up	PPPoE LCP Link Up
129	Network	PPPoE	Maintenance	INFO	7803	PPPoE Link Down	PPPoE LCP Link Down
130	Network	PPPoE	Maintenance	INFO	7804	PPPoE Link Finish	PPPoE terminated
131	Network	PPPoE	Maintenance	INFO	7805	PPPoE Network Up	PPPoE Network Connected
132	Network	PPPoE	Maintenance	INFO	7806	PPPoE Network Down	PPPoE Network Disconnected
133	Network	PPPoE	Maintenance	INFO	7807	PPPoE Discover Complete	PPPoE discovery process complete
134	Network	PPPoE	Maintenance	INFO	7808	PPPoE CHAP Authentication	PPPoE starting CHAP Authentication
138	Network	Interfaces	System Error	WARNING	636	WAN IP Change	Wan IP Changed
139	VPN	VPN Client	User Activity	INFO	9201	XAUTH Success	XAUTH Succeeded with VPN %s
140	VPN	VPN Client	User Activity	WARNING	9202	XAUTH Failure	XAUTH Failed with VPN %s, Authentication failure
141	VPN	VPN Client	User Activity	NOTICE	9203	XAUTH Timeout	XAUTH Failed with VPN client, Cannot Contact %s Server
142	Log	General	Debug	DEBUG	5206	Log Debug	Log Debug
144	High Availability	State	Maintenance	ALERT	6201	HA Active Primary	Primary firewall has transitioned to Active
145	High Availability	State	Maintenance	ALERT	6202	HA Active Secondary	Secondary firewall has transitioned to Active

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
146	High Availability	State	System Error	ALERT	6203	HA Standby Primary	Primary firewall has transitioned to Standby
147	High Availability	State	Maintenance	ALERT	6204	HA Standby Secondary	Secondary firewall has transitioned to Standby
148	High Availability	Synchronization	System Error	ERROR	615	HA Primary Missed Heartbeat	Primary missed heartbeats from Secondary
149	High Availability	Synchronization	System Error	ERROR	616	HA Secondary Missed Heartbeat	Secondary missed heartbeats from Primary
150	High Availability	State	System Error	ERROR	617	HA Primary Error Receive	Primary received error signal from Secondary
151	High Availability	State	System Error	ERROR	618	HA Secondary Error Receive	Secondary received error signal from Primary
153	High Availability	State	System Error	ERROR	620	HA Primary Preempt	Primary firewall preempting Secondary
157	High Availability	Synchronization	Maintenance	INFO	6214	HA Sync HA Peer	HA Peer Firewall Synchronized
158	High Availability	Synchronization	System Error	ERROR	662	HA Sync Error	Error synchronizing HA peer firewall (%s)
159	Security Services	Anti-Virus	Maintenance	WARNING	526	AV Expire message	Received AV Alert: Your Network Anti-Virus subscription has expired. %s
162	High Availability	Synchronization	Maintenance	INFO	6218	HA Packet Error	HA packet processing error
164	System	Restart	System Error	ERROR	621	HTTP Server Reboot	Diagnostic Code F
165	Security Services	E-mail Filtering	Attack	ALERT	527	Allow E-mail Attachment	Forbidden E-Mail attachment disabled
168	Network	PPPoE	Maintenance	INFO	7814	PPPoE Traffic Timeout	Disconnecting PPPoE due to traffic Timeout
169	Network	PPPoE	Maintenance	INFO	7815	PPPoE LCP Unack	No response from ISP Disconnecting PPPoE.
170	High Availability	State	System Error	ERROR	622	Secondary Active Preempt	Secondary going Active in preempt mode after reboot

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
171	VPN	VPN IKE	User Activity	DEBUG	9407	IPsec Dead Peer Detection	%s
173	Network	TCP	LAN TCP	NOTICE	7222	LAN TCP Deny	TCP connection from LAN denied
174	Network	UDP	LAN UDP | LAN TCP	NOTICE	7223	LAN UDP Deny	UDP packet from LAN dropped
175	Network	ICMP	LAN ICMP | LAN TCP	NOTICE	7224	LAN ICMP Deny	ICMP packet from LAN dropped
177	Security Services	Attacks	Attack	ALERT	528	TCP FIN Scan	Probable TCP FIN scan detected
178	Security Services	Attacks	Attack	ALERT	529	TCP Xmas Scan	Probable TCP XMAS scan detected
179	Security Services	Attacks	Attack	ALERT	530	TCP Null Scan	Probable TCP NULL scan detected
181	Network	TCP	Debug	DEBUG	7005	TCP FIN Drop	TCP FIN packet dropped
182	Network	ICMP	User Activity	INFO	7006	Path MTU Receive	Received a path MTU ICMP message from router/gateway
188	Network	ICMP	User Activity	INFO	7007	Path MTU ICMP	Received a path MTU ICMP message from router/gateway
191	High Availability	Synchronization	System Error	ERROR	629	HA Set Error	Error setting the IP address of the Secondary, please manually set to Secondary LAN IP
199	Users	Authentication Access	User Activity	INFO	4209	Admin Login From CLI	CLI administrator login allowed
200	Users	Authentication Access	User Activity	WARNING	4210	Admin Password Error From CLI	CLI administrator login denied due to bad credentials
201	Network	L2TP Client	Maintenance	INFO	6601	L2TP Tunnel Start	L2TP Tunnel Negotiation Started
202	Network	L2TP Client	Maintenance	INFO	6602	L2TP Session Start	L2TP Session Negotiation Started
204	Network	L2TP Client	Maintenance	INFO	6604	L2TP Tunnel Finish	L2TP Tunnel Established
205	Network	L2TP Client	Maintenance	NOTICE	6605	L2TP Tunnel Disconnect From Remote	L2TP Tunnel Disconnect from Remote
206	Network	L2TP Client	Maintenance	INFO	6606	L2TP Session Success	L2TP Session Established

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
207	Network	L2TP Client	Maintenance	NOTICE	6607	L2TP Session Disconnect From Remote	L2TP Session Disconnect from Remote
208	Network	L2TP Client	Maintenance	INFO	6608	L2TP PPP Start	L2TP PPP Negotiation Started
210	Network	L2TP Client	Maintenance	INFO	6610	L2TP PPP Up	L2TP PPP Session Up
211	Network	L2TP Client	Maintenance	NOTICE	6611	L2TP Net Down	L2TP PPP Down
212	Network	L2TP Client	Maintenance	NOTICE	6612	L2TP PPP Authenticate Failed	L2TP PPP Authentication Failed
215	Network	L2TP Client	Maintenance	INFO	6615	L2TP Traffic Timeout	Disconnecting L2TP Tunnel due to traffic Timeout
217	Network	L2TP Client	Maintenance	NOTICE	6617	L2TP PPP Down	L2TP PPP link down
222	VPN	DHCP Relay	Maintenance	INFO	5001	DHCPR Remote Release	DHCP RELEASE relayed to Central Gateway
223	VPN	DHCP Relay	Maintenance	INFO	5002	DHCPR Remote ACK	DHCP lease relayed to local device
224	VPN	DHCP Relay	Debug	INFO	5003	DHCPR Central Release	DHCP RELEASE received from remote device
225	VPN	DHCP Relay	Debug	INFO	5004	DHCPR Central ACK	DHCP lease relayed to remote device
226	VPN	DHCP Relay	Maintenance	INFO	5005	DHCPR IP Conflict	DHCP lease to LAN device conflicts with remote device, deleting remote IP entry
227	VPN	DHCP Relay	Maintenance	INFO	5006	DHCPR IP Conflict With Static IP	WARNING: DHCP lease relayed from Central Gateway conflicts with IP in Static Devices list
228	VPN	DHCP Relay	Maintenance	WARNING	5007	DHCPR IP Drop	DHCP lease dropped. Lease from Central Gateway conflicts with Relay IP
229	VPN	DHCP Relay	Attack	WARNING	533	DHCPR IP Spoof	IP spoof detected on packet to Central Gateway, packet dropped
230	VPN	DHCP Relay	Maintenance	INFO	5009	DHCPR Get Remote IP Table	Request for Relay IP Table from Central Gateway

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
231	VPN	DHCP Relay	Maintenance	INFO	5010	DHCPR Get Central IP Table	Requesting Relay IP Table from Remote Gateway
232	VPN	DHCP Relay	Maintenance	INFO	5011	DHCPR Send Remote IP Table	Sent Relay IP Table to Central Gateway
233	VPN	DHCP Relay	Maintenance	INFO	5012	DHCPR Receive Remote IP Table	Obtained Relay IP Table from Remote Gateway
234	VPN	DHCP Relay	System Error	WARNING	632	DHCPR Table Request Timeout	Failed to synchronize Relay IP Table
235	Users	Authentication Access	User Activity	INFO	4211	Admin VPN Login	VPN zone administrator login allowed
236	Users	Authentication Access	User Activity	INFO	4212	Admin WAN Login	WAN zone administrator login allowed
237	Users	Authentication Access	User Activity	INFO	4213	User VPN Login	VPN zone remote user login allowed
238	Users	Authentication Access	User Activity	INFO	4214	User WAN Login	WAN zone remote user login allowed
239	VPN	VPN IKE	User Activity	INFO	9409	VPN Peer Behind NAT Device	NAT Discovery : Peer IPsec Security Gateway behind a NAT/NAPT Device
240	VPN	VPN IKE	User Activity	INFO	9410	VPN Local Behind NAT Device	NAT Discovery : Local IPsec Security Gateway behind a NAT/NAPT Device
241	VPN	VPN IKE	User Activity	INFO	9411	VPN No NAT Device Detected	NAT Discovery : No NAT/NAPT device detected between IPsec Security gateways
242	VPN	VPN IKE	User Activity	NOTICE	9412	VPN Peer Does Not Support NAT	NAT Discovery : Peer IPsec Security Gateway doesn't support VPN NAT Traversal
243	Users	Radius Authentication	User Activity	INFO	8201	User Login Failed	User login denied - RADIUS authentication failure

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
244	Users	Radius Authentication	User Activity	WARNING	8202	User Login Timeout	User login denied - RADIUS server Timeout
245	Users	Radius Authentication	User Activity	WARNING	8203	User Login Error	User login denied - RADIUS configuration error
246	Users	Authentication Access	User Activity	INFO	8204	User Login From Wrong Location	User login denied - User has no privileges for login from that location
247	VPN	VPN IPsec	Maintenance	INFO	9610	Illegal Packet from IPsec Host	IPsec packet from an illegal host
248	Security Services	E-mail Filtering	Attack	ERROR	534	E-mail Attachment	Forbidden E-Mail attachment deleted
249	VPN	VPN IKE	User Activity	WARNING	535	Bad Tunnel Mode	IKE Responder: Mode %s - not tunnel mode
250	VPN	VPN IKE	User Activity	WARNING	536	Phase 1 ID Mismatch	IKE Responder: No matching Phase 1 ID found for proposed remote network
251	VPN	VPN IKE	User Activity	WARNING	537	Bad Remote Network	IKE Responder: Proposed remote network is 0.0.0.0 but not DHCP relay nor default route
252	VPN	VPN IKE	User Activity	WARNING	538	No Remote Network Match	IKE Responder: No match for proposed remote network address
253	VPN	VPN IKE	User Activity	WARNING	539	Default Gateway Not Match Proposal	IKE Responder: Default LAN gateway is set but peer is not proposing to use this SA as a default route
254	VPN	VPN IKE	User Activity	INFO	540	Tunnel Terminates Outside	IKE Responder: Tunnel terminates outside firewall but proposed local network is not NAT public address
255	VPN	VPN IKE	User Activity	INFO	541	Tunnel Terminates Inside	IKE Responder: Tunnel terminates inside firewall but proposed local network is not inside firewall

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
256	VPN	VPN IKE	User Activity	INFO	542	Tunnel Terminates DMZ	IKE Responder: Tunnel terminates on DMZ but proposed local network is on LAN
257	VPN	VPN IKE	User Activity	INFO	543	Tunnel Terminates LAN	IKE Responder: Tunnel terminates on LAN but proposed local network is on DMZ
258	VPN	VPN IKE	User Activity	WARNING	544	AH PFS Mismatch	IKE Responder: AH Perfect Forward Secrecy mismatch
259	VPN	VPN IKE	User Activity	WARNING	545	ESP PFS Mismatch	IKE Responder: ESP Perfect Forward Secrecy mismatch
260	VPN	VPN IKE	User Activity	WARNING	546	Algorithm or Key Mismatch	IKE Responder: Algorithms and/or keys do not match
261	Users	Authentication Access	User Activity	INFO	4215	Admin Logout	Administrator logged out
262	Users	Authentication Access	User Activity	INFO	4216	Admin Logout - Timer Expire	Administrator logged out - inactivity timer expired
263	Users	Authentication Access	User Activity	INFO	4217	User Logout	User logged out - %s
264	Users	Authentication Access	User Activity	INFO	4218	User Logout - Max Session	User logged out - max session time exceeded
265	Users	Authentication Access	User Activity	INFO	4219	User Logout - Timer Expire	User logged out - inactivity timer expired
266	VPN	VPN IPsec	Maintenance	INFO	9611	IPsec AH Does Not Support NAT	NAT device may not support IPsec AH pass-through
267	Security Services	Attacks	Attack	ALERT	547	TCP Xmas Tree Attack	TCP Xmas Tree dropped
269	VPN	VPN PKI	User Activity	INFO	9801	CRL Request	Requesting CRL from
270	VPN	VPN PKI	User Activity	INFO	9802	CRL Download Success	CRL loaded from
271	VPN	VPN PKI	User Activity	ALERT	9803	CRL Download Failed	Failed to get CRL from
272	VPN	VPN PKI	User Activity	ERROR	9804	CRL Failed - No Memory	Not enough memory to hold the CRL

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
273	VPN	VPN PKI	User Activity	WARNING	9805	CRL Failed - Timeout	Connection timed out
274	VPN	VPN PKI	User Activity	ERROR	9806	CRL Failed - No Connect	Cannot connect to the CRL server
275	VPN	VPN PKI	User Activity	ERROR	9807	CRL Failed - No Reason	Unknown reason
276	VPN	VPN PKI	User Activity	WARNING	9808	CRL Process Failed	Failed to Process CRL from
277	VPN	VPN PKI	User Activity	WARNING	9809	CRL Bad Format	Bad CRL format
278	VPN	VPN PKI	User Activity	WARNING	9810	CRL Wrong Issuer	Issuer match failed
279	VPN	VPN PKI	User Activity	WARNING	9811	CRL Certificate Revoke	Certificate on Revoked list(CRL)
280	VPN	VPN PKI	User Activity	WARNING	9812	No Certificate	No Certificate for
289	Network	PPP	---	INFO	11401	PPP Authenticate Success	PPP: Authentication successful
290	Network	PPP	---	NOTICE	11402	PPP PAP Failed	PPP: PAP Authentication failed - check username / password
291	Network	PPP	---	NOTICE	11403	PPP CHAP Failed	PPP: CHAP authentication failed - check username / password
292	Network	PPP	---	NOTICE	11404	PPP MS-CHAP Failed	PPP: MS-CHAP authentication failed - check username / password
293	Network	PPP	---	INFO	11405	PPP MS-CHAP Start	PPP: Starting MS-CHAP authentication
294	Network	PPP	---	INFO	11406	PPP CHAP Start	PPP: Starting CHAP authentication
295	Network	PPP	---	INFO	11407	PPP PAP Start	PPP: Starting PAP authentication
307	Network	Failover and Load Balancing	System Error	WARNING	639	WAN Mode	The network connection in use is %s
308	VPN	L2TP Server	Maintenance	INFO	6801	L2TP Tunnel Establish	L2TP Server : L2TP Tunnel Established.
309	VPN	L2TP Server	Maintenance	INFO	6802	L2TP Session Establish	L2TP Server : L2TP Session Established.

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
311	VPN	L2TP Server	Maintenance	INFO	6804	L2TP Radius Authentication Failure	L2TP Server: RADIUS/LDAP reports Authentication Failure
312	VPN	L2TP Server	Maintenance	INFO	6805	L2TP Local Authentication Failure	L2TP Server: Local Authentication Failure
318	VPN	L2TP Server	Maintenance	INFO	6811	L2TP Local Authentication Success	L2TP Server: Local Authentication Success.
319	VPN	L2TP Server	Maintenance	INFO	6812	L2TP Radius Authentication Success	L2TP Server: RADIUS/LDAP Authentication Success
326	Network	Failover and Load Balancing	System Error	ALERT	637	Probe Failed	Probing failure on %s
328	Users	Authentication Access	Maintenance	INFO	4220	Admin Name Change	Administrator name changed
329	Users	Authentication Access	Attack	ERROR	561	User Login Lockout	User login failure rate exceeded - logins from user IP address denied
335	VPN	L2TP Server	Maintenance	INFO	6815	L2TPS Tunnel Disconnect From Remote	L2TP Server: Tunnel Disconnect from Remote.
336	VPN	L2TP Server	Maintenance	INFO	6816	L2TPS Tunnel Delete	L2TP Server : Deleting the Tunnel
337	VPN	L2TP Server	Maintenance	INFO	6817	L2TPS Session Delete	L2TP Server : Deleting the L2TP active Session
338	VPN	L2TP Server	Maintenance	INFO	6818	L2TPS Retransmission Timeout	L2TP Server : Retransmission Timeout, Deleting the Tunnel
339	Network	NAT	Debug	DEBUG	7008	NAT Overwrite	NAT translated packet exceeds size limit, packet dropped
340	System	Administration	Maintenance	INFO	5212	HTTP Port Change	HTTP management port has changed
341	System	Administration	Maintenance	INFO	5213	HTTPS Port Change	HTTPS management port has changed

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
344	VPN	L2TP Server	Maintenance	INFO	6820	L2TPS Authentication Local Failure	L2TP Server : User Name authentication Failure locally.
346	VPN	VPN IKE	User Activity	INFO	9427	Quick Mode Started	IKE Initiator: Start Quick Mode (Phase 2).
347	Network	Network Access	TCP | UDP | ICMP	WARNING	7225	Drop Clear Packet	Port configured to receive IPsec protocol ONLY; drop packet received in the clear
348	VPN	VPN IPsec	Maintenance	WARNING	5214	VPN SA Import Invalid	Imported VPN SA is invalid - disabled
350	VPN	VPN IKE	User Activity	INFO	9428	IKE SA Life Expired	IKE SA lifetime expired.
351	VPN	VPN IKE	User Activity	INFO	9429	IKE Main Mode Started	IKE Initiator: Start Main Mode negotiation (Phase 1)
352	VPN	VPN IKE	User Activity	INFO	9430	IKE Quick Mode Request Received	IKE Responder: Received Quick Mode Request (Phase 2)
353	VPN	VPN IKE	User Activity	INFO	9431	Initial Main Mode Completed	IKE Initiator: Main Mode complete (Phase 1)
354	VPN	VPN IKE	User Activity	INFO	9432	Initial Aggressive Mode Completed	IKE Initiator: Aggressive Mode complete (Phase 1).
355	VPN	VPN IKE	User Activity	INFO	9433	Responder Main Mode Request Received	IKE Responder: Received Main Mode Request (Phase 1)
356	VPN	VPN IKE	User Activity	INFO	9434	Responder Aggressive Mode Request Received	IKE Responder: Received Aggressive Mode Request (Phase 1)
357	VPN	VPN IKE	User Activity	INFO	9435	Responder Main Mode Completed	IKE Responder: Main Mode complete (Phase 1)
358	VPN	VPN IKE	User Activity	INFO	9436	Aggressive Mode Started	IKE Initiator: Start Aggressive Mode negotiation (Phase 1)

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
360	Security Services	Crypto Test	Maintenance	ERROR	4602	DES Test Failed	Crypto DES test failed
361	Security Services	Crypto Test	Maintenance	ERROR	4603	DH Test Failed	Crypto DH test failed
362	Security Services	Crypto Test	Maintenance	ERROR	4604	HMAC-MD5 Test Failed	Crypto Hmac-MD5 test failed
363	Security Services	Crypto Test	Maintenance	ERROR	4605	HMAC-SHA1 Test Failed	Crypto Hmac-Sha1 test failed
364	Security Services	Crypto Test	Maintenance	ERROR	4606	RSA Test Failed	Crypto RSA test failed
365	Security Services	Crypto Test	Maintenance	ERROR	4607	SHA1 Test Failed	Crypto Sha1 test failed
366	Security Services	Crypto Test	Maintenance	ERROR	4608	Hardware DES Test Failed	Crypto hardware DES test failed
367	Security Services	Crypto Test	Maintenance	ERROR	4609	Hardware 3DES Test Failed	Crypto hardware 3DES test failed
368	Security Services	Crypto Test	Maintenance	ERROR	4610	Hardware DES-SHA Test Failed	Crypto hardware DES with SHA test failed
369	Security Services	Crypto Test	Maintenance	ERROR	4611	Hardware 3DES-SHA Test Failed	Crypto Hardware 3DES with SHA test failed
371	VPN	VPN Client	User Activity	INFO	9204	Client Policy Provisioned	VPN Client Policy Provisioning
372	VPN	VPN IKE	User Activity	INFO	9437	IKE Initiator: Accept Proposal	IKE Initiator: Accepting IPsec proposal (Phase 2)
373	VPN	VPN IKE	User Activity	INFO	9438	IKE Responder: Aggressive Mode Complete	IKE Responder: Aggressive Mode complete (Phase 1)
375	Network	PPTP	Maintenance	INFO	8001	Start Control Connection Negotiation	PPTP Control Connection Negotiation Started
376	Network	PPTP	Maintenance	INFO	8002	Start Session Negotiation	PPTP Session Negotiation Started
378	Network	PPTP	Maintenance	INFO	8004	PPTP Control Establish	PPTP Control Connection Established
379	Network	PPTP	Maintenance	NOTICE	8005	PPTP Remote Disconnect Tunnel	PPTP Tunnel Disconnect from Remote
380	Network	PPTP	Maintenance	INFO	8006	PPTP Session Success	PPTP Session Established

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
381	Network	PPTP	Maintenance	INFO	8007	PPTP Remote Disconnect Session	PPTP Session Disconnect from Remote
382	Network	PPTP	Maintenance	INFO	8008	PPP Start	PPTP PPP Negotiation Started
384	Network	PPTP	Maintenance	INFO	8010	PPP Up	PPTP PPP Session Up
385	Network	PPTP	Maintenance	NOTICE	8011	PPP Down	PPTP PPP Down
388	Network	PPTP	Maintenance	INFO	8014	PPTP User Diconnect	PPTP Disconnect Initiated by the User
389	Network	PPTP	Maintenance	INFO	8015	PPTP Traffic Timeout	Disconnecting PPTP Tunnel due to traffic Timeout
390	Network	PPTP	Maintenance	INFO	8016	PPTP User Connect	PPTP Connect Initiated by the User
392	Network	PPTP	Maintenance	INFO	8018	PPTP CHAP Authentication	PPTP starting CHAP Authentication
393	Network	PPTP	Maintenance	INFO	8019	PPTP PAP Authentication	PPTP starting PAP Authentication
396	Network	PPTP	Maintenance	INFO	8022	PPTP Authentication ACK	PPTP PAP Authentication success.
398	Network	PPTP	Maintenance	INFO	8024	PPTP PPP Link Up	PPTP PPP Link Up
399	Network	PPTP	Maintenance	INFO	8025	PPTP PPP Link Down	PPTP PPP Link down
400	Network	PPTP	Maintenance	INFO	8026	PPTP PPP Link Finish	PPTP PPP Link Finished
401	VPN	VPN IKE	User Activity	WARNING	9439	No Proposal Chosen	Received notify. NO_PROPOSAL_CHOSEN
402	VPN	VPN IKE	User Activity	WARNING	9440	Proposal Rejected	IKE Responder: IKE proposal does not match (Phase 1)
403	VPN	VPN IKE	User Activity	NOTICE	9441	Negotiation Aborted	IKE negotiation aborted due to Timeout
404	VPN	VPN IKE	User Activity	WARNING	9442	Decryption Failed: Key Mismatch	Failed payload verification after decryption; possible preshared key mismatch
405	VPN	VPN IKE	User Activity	WARNING	9443	Payload Validation Failed	Failed payload validation

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
406	VPN	VPN IKE	User Activity	WARNING	9444	Duplicate Packet Dropped	Received packet retransmission. Drop duplicate packet
408	Security Services	Anti-Virus	Maintenance	INFO	8617	AV License Exceeded	Anti-Virus Licenses Exceeded
409	VPN	VPN IKE	User Activity	WARNING	9446	Authentication Failed	Received notify: ISAKMP_AUTH_FAILED
410	VPN	VPN IKE	User Activity	WARNING	9447	Hash Failed	Computed hash does not match hash received from peer; preshared key mismatch
411	VPN	VPN IKE	User Activity	WARNING	9448	Notification on Malformed Payload	Received notify: PAYLOAD_MALFORMED
412	VPN	VPN IKE	User Activity	NOTICE	9449	Receive IPsec Delete Request	Received IPsec SA delete request
413	VPN	VPN IKE	User Activity	NOTICE	9450	Receive IKE Delete Request	Received IKE SA delete request
414	VPN	VPN IKE	User Activity	NOTICE	9451	Invalid Cookies	Received notify: INVALID_COOKIES
415	VPN	VPN IKE	User Activity	INFO	9452	Notification on Responder Lifetime	Received notify: RESPONDER_LIFETIME
416	VPN	VPN IKE	User Activity	INFO	9453	Notification on Invalid SPI	Received notify: INVALID_SPI
427	VPN	VPN IPsec	VPN Tunnel Status	INFO	801	IPsec Tunnel Status Changed	IPsec Tunnel status changed
428	Firewall Settings	Advanced	Debug	WARNING	6424	Drop Source Route Packet	Source routed IP packet dropped
429	Network	PPTP	Maintenance	INFO	8027	PPTP Disconnect Echo Request	No response from server to Echo Requests, disconnecting PPTP Tunnel
430	Network	PPTP	Maintenance	INFO	8028	PPTP Disconnect Control Connection Request	No response from PPTP server to control connection requests
431	Network	PPTP	Maintenance	INFO	8029	PPTP Disconnect Session Request	No response from PPTP server to call requests

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
432	Network	PPTP	Maintenance	INFO	8030	PPTP Disconnect Control Connection Reject	PPTP server rejected control connection
433	Network	PPTP	Maintenance	INFO	8031	PPTP Disconnect Session Reject	PPTP server rejected the call request
434	Network	Failover and Load Balancing	User Activity	INFO	10003	Manual Alternate Profile	PPP Dial-Up: Trying to failover but Alternate Profile is manual
435	Network	Failover and Load Balancing	System Error	ALERT	652	WLB Failback	WLB Failback initiated by %s
436	Network	Failover and Load Balancing	System Error	ALERT	638	WLB Probe Success	Probing succeeded on %s
437	Security Services	E-mail Filtering	Attack	ERROR	550	E-mail Fragment Dropped	E-Mail fragment dropped
438	Users	Authentication Access	User Activity	INFO	4222	User Login Lockout Expired	Locked-out user logins allowed - lockout period expired
439	Users	Authentication Access	User Activity	INFO	4223	User Login Lockout Clear	Locked-out user logins allowed by %s
440	Firewall	Access Rules	User Activity	INFO	5801	Rule Added	Access rule added
441	Firewall	Access Rules	User Activity	INFO	5802	Rule Modified	Access rule viewed or modified
442	Firewall	Access Rules	User Activity	INFO	5803	Rule Deleted	Access rule deleted
444	Network	PPTP	Maintenance	NOTICE	8032	PPTP Server Down	PPTP Server is not responding, check if the server is UP and running.
445	VPN	VPN IKE	User Activity	INFO	9455	IKE Initiator: Peer Lifetime Accept	IKE Initiator: Accepting peer lifetime. (Phase 1)
446	Firewall Settings	FTP	Attack	ERROR	551	FTP Passive Attack	FTP: PASV response spoof attack dropped
448	VPN	VPN PKI	Maintenance	ERROR	9815	PKI Output Buffer Failure	PKI Failure: Output buffer too small
449	VPN	VPN PKI	Maintenance	ERROR	9816	PKI Allocate Memory Failure	PKI Failure: Cannot alloc memory

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
450	VPN	VPN PKI	Maintenance	ERROR	9817	PKI Certificate Failure	PKI Failure: Reached the limit for local certs, cant load any more
451	VPN	VPN PKI	Maintenance	ERROR	9818	PKI Import Failure	PKI Failure: Import failed
452	VPN	VPN PKI	Maintenance	WARNING	9819	PKI Bad Password	PKI Failure: Incorrect admin password
453	VPN	VPN PKI	Maintenance	WARNING	9820	PKI CA Certificate Failure	PKI Failure: CA certificates store exceeded. Cannot verify this Local Certificate
454	VPN	VPN PKI	Maintenance	WARNING	9821	PKI Import File Format Failure	PKI Failure: Improper file format. Please select PKCS#12 (*.p12) file
455	VPN	VPN PKI	Maintenance	WARNING	9822	PKI Certificate ID Failure	PKI Failure: Certificate's ID does not match this Network Security Appliance
456	VPN	VPN PKI	Maintenance	WARNING	9823	PKI Key Mismatch	PKI Failure: public-private key mismatch
457	VPN	VPN PKI	Maintenance	WARNING	9824	PKI Local Certificate Name Duplicate	PKI Failure: Duplicate local certificate name
458	VPN	VPN PKI	Maintenance	WARNING	9825	PKI Local Certificate Duplicate	PKI Failure: Duplicate local certificate
459	VPN	VPN PKI	Maintenance	WARNING	9826	PKI No Certificate	PKI Failure: No CA certificates yet loaded
460	VPN	VPN PKI	Maintenance	ERROR	9827	PKI Internal Error	PKI Failure: Internal error
461	VPN	VPN PKI	Maintenance	WARNING	9828	PKI No Resource	PKI Failure: Temporary memory shortage, try again
462	VPN	VPN PKI	Maintenance	WARNING	9829	PKI Certificate Chain Circular	PKI Failure: The certificate chain is circular
463	VPN	VPN PKI	Maintenance	WARNING	9830	PKI Certificate Chain Incomplete	PKI Failure: The certificate chain is incomplete

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
464	VPN	VPN PKI	Maintenance	WARNING	9831	PKI Certificate Chain No Root	PKI Failure: The certificate chain has no root
465	VPN	VPN PKI	Maintenance	WARNING	9832	PKI Certificate Expire	PKI Failure: Certificate expiration
466	VPN	VPN PKI	Maintenance	WARNING	9833	PKI Certificate Invalid	PKI Failure: The certificate or a certificate in the chain has a validity period in the future
467	VPN	VPN PKI	Maintenance	WARNING	9834	PKI Certificate Corrupt	PKI Failure: The certificate or a certificate in the chain is corrupt
468	VPN	VPN PKI	Maintenance	WARNING	9835	PKI Certificate Bad Signature	PKI Failure: The certificate or a certificate in the chain has a bad signature
469	VPN	VPN PKI	Maintenance	WARNING	9836	PKI Certificate Not Verified	PKI Failure: Loaded but could not verify certificate
470	VPN	VPN PKI	Maintenance	WARNING	9837	PKI Certificate Chain Not Verified	PKI Warning: Loaded the certificate but could not verify its chain
473	VPN	DHCP Relay	Debug	INFO	5015	Remote: DHCP Request	DHCP REQUEST received from remote device
474	VPN	DHCP Relay	Debug	INFO	5016	Remote: DHCP Discover	DHCP DISCOVER received from remote device
476	VPN	DHCP Relay	Debug	INFO	5018	Server: DHCP Offer	DHCP OFFER received from server
477	VPN	DHCP Relay	Debug	INFO	5019	Server: DHCP Nack	DHCP NACK received from server
482	Security Services	Anti-Virus	Maintenance	WARNING	552	AV Expiration Warning	Received AV Alert: Your Network Anti-Virus subscription will expire in 7 days. %s
483	VPN	VPN IPsec	User Activity	WARNING	9613	Invalid ID	Received notify: INVALID_ID_INFO

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
484	VPN	DHCP Relay	Maintenance	WARNING	5023	DHCP Release Drop	DHCP lease dropped. Lease from Central Gateway conflicts with Remote Management IP
486	Users	Authentication Access	User Activity	INFO	4224	WLAN User Login Deny	User login denied - User has no privileges for guest service
488	Wireless	Wireless Access	TCP | UDP | ICMP	WARNING	10202	Guest Check	Packet dropped by guest check
491	Security Services	E-mail Filtering	Maintenance	WARNING	564	E-mail Filtering Expiration Warning	Received E-Mail Filter Alert: Your E-Mail Filtering subscription will expire in 7 days.
492	Security Services	E-mail Filtering	Maintenance	WARNING	565	E-mail Filtering Expiration Message	Received E-Mail Filter Alert: Your E-Mail Filtering subscription has expired.
493	Network	Interfaces	Maintenance	INFO	5215	ISDN Update	ISDN Driver Firmware successfully updated
494	VPN	VPN Client	System Error	NOTICE	658	GVC License Exceed	Global VPN Client License Exceeded: Connection denied.
496	Security Services	General	Maintenance	WARNING	8623	DEA Registration	Registration Update Needed, Please restore your existing security service subscriptions.
502	Network	Interfaces	Maintenance	INFO	5217	WAN Not Ready	WAN not ready
505	VPN	VPN Client	System Error	WARNING	660	Blocked Quick Mode With Default Key ID	Blocked Quick Mode for Client using Default KeyId
506	Users	Authentication Access	Maintenance	INFO	4225	VPN Disabled	VPN disabled by administrator
507	Users	Authentication Access	Maintenance	INFO	4226	VPN Enabled	VPN enabled by administrator
508	Users	Authentication Access	Maintenance	INFO	4227	WLAN Disabled	WLAN disabled by administrator
509	Users	Authentication Access	Maintenance	INFO	4228	WLAN Enabled	WLAN enabled by administrator

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
518	Wireless	WLAN	802.11b Management	INFO	---	WLAN 802.11 Management	802.11 Management
520	Users	Authentication Access	User Activity	INFO	4235	Admin Logout From CLI	CLI administrator logged out
521	System	Status	Maintenance	INFO	5218	Initializing	Network Security Appliance initializing
522	Network	IP	Debug	INFO	554	Malformed IP Packet	Malformed or unhandled IP packet dropped
523	Network	ICMP	ICMP	NOTICE	7227	No Match ICMP Drop	ICMP packet dropped no match
524	Network	Network Access	TCP	NOTICE	7228	Web Request Drop	Web access Request dropped
526	Network	Network Access	User Activity	NOTICE	7229	Web Request Receiver	Web management request allowed
527	Firewall Settings	FTP	Attack	ALERT	555	FTP Port Bounce Attack	FTP: PORT bounce attack dropped.
528	Firewall Settings	FTP	Attack	ALERT	556	FTP Passive Bounce Attack	FTP: PASV response bounce attack dropped.
529	VPN	VPN Client	System Error	NOTICE	643	GVC Not Authorized	Global VPN Client connection is not allowed. Appliance is not registered.
533	VPN	VPN IPsec	TCP | UDP | ICMP	NOTICE	9614	ESP Drop	IPsec (ESP) packet dropped
534	VPN	VPN IPsec	TCP | UDP | ICMP	NOTICE	9615	AH Drop	IPsec (AH) packet dropped
535	VPN	VPN IPsec	Debug	DEBUG	9616	ESP Connection Drop	IPsec (ESP) packet dropped; waiting for pending IPsec connection
537	Network	Network Access	Connection Traffic	INFO	7403	Connection Closed	Connection Closed
538	Firewall Settings	FTP	Attack	ALERT	557	FTP Data Port	FTP: Data connection from non default port dropped
543	VPN	VPN IKE	User Activity	INFO	9457	Negotiation on Second GW	IKE Initiator: Using secondary gateway to negotiate

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
544	VPN	VPN IKE	User Activity	NOTICE	9458	Initiator: Bound Scope Mismatch	IKE Initiator drop: VPN tunnel end point does not match configured VPN Policy Bound to scope
545	VPN	VPN IKE	User Activity	NOTICE	9459	Responder: Bound Scope Mismatch	IKE Responder drop: VPN tunnel end point does not match configured VPN Policy Bound to scope
546	Wireless	WLAN IDS	WLAN IDS	ALERT	901	Rogue AP or MitM AP Found	Found Rogue or MitM Access Point
548	Wireless	WLAN IDS	WLAN IDS	ALERT	903	WLAN Association Flood	Association Flood from WLAN station
549	Users	Authentication Access	User Activity	WARNING	4236	WLAN Guest Limit	User login failed - Guest service limit reached
550	Users	Authentication Access	User Activity	INFO	4237	WLAN Session Timeout	User Session Quota Expired
551	Users	Authentication Access	User Activity	INFO	4238	WLAN Account Timeout	Guest Account Timeout
557	Users	Authentication Access	User Activity	INFO	4239	WLAN Guest Already Login	Guest login denied. Guest '%s' is already logged in. Please try again later.
558	Users	Authentication Access	User Activity	INFO	4240	WLAN Guest Create	Guest account '%s' created
559	Users	Authentication Access	User Activity	INFO	4241	WLAN Guest Delete	Guest account '%s' deleted
560	Users	Authentication Access	User Activity	INFO	4242	WLAN Guest Disable	Guest account '%s' disabled
561	Users	Authentication Access	User Activity	INFO	4243	WLAN Guest Re-enable	Guest account '%s' re-enabled
562	Users	Authentication Access	User Activity	INFO	4244	WLAN Guest Prune	Guest account '%s' pruned
564	Users	Authentication Access	User Activity	INFO	4246	WLAN Idle Timeout	Guest Idle Timeout
565	Network	Interfaces	System Error	ALERT	646	Multi-Interface Link Up	Interface %s Link Is Up
566	Network	Interfaces	System Error	ALERT	647	Multi-Interface Link Down	Interface %s Link Is Down

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
567	Network	Interfaces	Maintenance	DEBUG	5222	Multi-Interface Shutdown	Interface IP Assignment changed: Shutting down %s
568	Network	Interfaces	Maintenance	DEBUG	5223	Multi-Interface Bind Initiate	Interface IP Assignment : Binding and initializing %s
569	Network	Interfaces	Maintenance	WARNING	5224	Network Overlap	Network for interface %s overlaps with another interface.
570	Network	Interfaces	Maintenance	INFO	5225	Invalid Network	Please connect interface %s to another network to function properly
573	System	Settings	System Error	WARNING	649	Preferences Too Big	The preferences file is too large to be saved in available flash memory
574	System	Settings	System Error	WARNING	650	Preferences Defaulted	All preference values have been set to factory default values
575	System	Hardware	System Environment	ERROR	101	Voltages Out of Tolerance	Voltages Out of Tolerance
576	System	Hardware	System Environment	ALERT	102	Fan Failure	Fan Failure
577	System	Hardware	System Environment	ALERT	103	Thermal Yellow	Thermal Yellow
578	System	Hardware	System Environment	ALERT	104	Thermal Red	Thermal Red
579	System	Hardware	System Environment	ALERT	105	Thermal Red Timer Exceeded	Thermal Red Timer Exceeded
580	Network	TCP	Attack	ALERT	558	TCP SYN/FIN Packet Drop	TCP SYN/FIN packet dropped
581	Network	Failover and Load Balancing	Maintenance	WARNING	10006	WLB Spill-Over Start	WLB Spill-over started, configured threshold exceeded
582	Network	Failover and Load Balancing	Maintenance	WARNING	10007	WLB Spill-Over Stop	WLB Spill-over stopped
583	Users	Authentication Access	Attack	ERROR	559	User Login Disable	User login disabled from %s
584	Network	Failover and Load Balancing	System Error	ALERT	651	WLB Failover	WLB Failover in progress

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
585	Network	Failover and Load Balancing	System Error	ALERT	653	WLB Resource Available	WLB Resource is now available
586	Network	Failover and Load Balancing	System Error	ALERT	654	WLB Resource Failed	WLB Resource failed
587	VPN	VPN IKE	User Activity	WARNING	9460	Header Verification Failed	Header verification failed
588	Network	DHCP Client	Maintenance	NOTICE	4826	Offer Error	Received DHCP offer packet has errors
589	Network	DHCP Client	Maintenance	NOTICE	4827	Request Response Error	Received response packet for DHCP request has errors
590	Network	Network Access	LAN UDP | LAN TCP	NOTICE	7232	LAN IP Deny	IP type %s packet dropped
593	Network	PPPoE	Maintenance	INFO	7817	Receive PAD Offer	Received PPPoE Active Discovery Offer
594	Network	PPPoE	Maintenance	INFO	7818	Receive PAD Conffirm	Received PPPoE Active Discovery Session_confirmation
595	Network	PPPoE	Maintenance	INFO	7819	Sending PADR	Sending PPPoE Active Discovery Request
596	Network	PPTP	Debug	DEBUG	8034	Decode Failure	PPTP decode failure
597	Network	ICMP	Debug	INFO	7233	ICMP Allow	ICMP packet allowed
598	Network	ICMP	Debug	INFO	7234	LAN ICMP Allow	ICMP packet from LAN allowed
599	System	Restart	System Error	ERROR	655	Stack Margin Reboot	Diagnostic Code G
600	System	Restart	System Error	ERROR	656	Delete Reboot	Diagnostic Code H
601	System	Restart	System Error	ERROR	657	Delete Stack Reboot	Diagnostic Code I
602	Network	DNS	Debug	INFO	7235	DNS Allow	DNS packet allowed
603	VPN	L2TP Server	System Error	ERROR	661	Problem Adding L2TP IP Pool	Adding L2TP IP pool Address object Failed.
605	VPN	VPN IKE	User Activity	WARNING	9461	Received Unencrypted Packet	Received unencrypted packet in crypto active state
606	Security Services	Attacks	Attack	ALERT	568	Spank Attack	Spank attack multicast packet dropped

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
607	VPN	VPN IKE	Debug | UDP	INFO	9462	ISAKMP Packet on Wrong Port	Received ISAKMP packet destined to port %s
608	Security Services	IPS	Attack	ALERT	569	IPS Detection Alert	IPS Detection Alert: %s
609	Security Services	IPS	Attack	ALERT	570	IPS Prevention Alert	IPS Prevention Alert: %s
610	Security Services	Crypto Test	Maintenance	ERROR	4614	Hardware AES Test Failed	Crypto Hardware AES test failed
614	Security Services	General	Maintenance	WARNING	571	IDP Expiration Message	Received IPS Alert: Your Intrusion Prevention (IDP) subscription has expired.
615	Wireless	WLAN IDS	WLAN IDS	WARNING	904	WLAN Probe Check	WLAN client null probing
616	VPN	VPN IKE	Debug	ERROR	9463	Detail Error Log	Payload processing failed
617	Wireless	WLAN	Maintenance	INFO	10207	WLAN Mode Not With DHCP	WLAN not in AP mode, DHCP server will not provide lease to clients on WLAN
618	Network	BOOTP	Debug	DEBUG	4401	Response to Remote Device	BOOTP server response relayed to remote device
619	Network	BOOTP	Maintenance	INFO	4402	Reply IP Conflict	BOOTP Client IP address on LAN conflicts with remote device IP, deleting IP address from remote table
620	Network	BOOTP	Maintenance	INFO	4403	Response to Local Device	BOOTP reply relayed to local device
622	VoIP	Call	VoIP	INFO	8801	Call Connect	VoIP Call Connected
623	VoIP	Call	VoIP	INFO	8802	Call Disconnect	VoIP Call Disconnected
624	VoIP	H.323	VoIP	DEBUG	8803	H.323/RAS Admission Reject	H.323/RAS Admission Reject
625	VoIP	H.323	VoIP	DEBUG	8804	H.323/RAS Admission Confirm	H.323/RAS Admission Confirm
626	VoIP	H.323	VoIP	DEBUG	8805	H.323/RAS Admission Request	H.323/RAS Admission Request

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
627	VoIP	H.323	VoIP	DEBUG	8806	H.323/RAS Bandwidth Reject	H.323/RAS Bandwidth Reject
628	VoIP	H.323	VoIP	DEBUG	8807	H.323/RAS Disengage Confirm	H.323/RAS Disengage Confirm
629	VoIP	H.323	VoIP	DEBUG	8808	H.323/RAS Gatekeeper Reject	H.323/RAS Gatekeeper Reject
630	VoIP	H.323	VoIP	DEBUG	8809	H.323/RAS Location Confirm	H.323/RAS Location Confirm
631	VoIP	H.323	VoIP	DEBUG	8810	H.323/RAS Location Reject	H.323/RAS Location Reject
632	VoIP	H.323	VoIP	DEBUG	8811	H.323/RAS Registration Reject	H.323/RAS Registration Reject
633	VoIP	H.323	VoIP	DEBUG	8812	H.323/H.225 Setup	H.323/H.225 Setup
634	VoIP	H.323	VoIP	DEBUG	8813	H.323/H.225 Connect	H.323/H.225 Connect
635	VoIP	H.323	VoIP	DEBUG	8814	H.323/H.245 Address	H.323/H.245 Address
636	VoIP	H.323	VoIP	DEBUG	8815	H.323/H.245 End Session	H.323/H.245 End Session
637	VoIP	SIP	VoIP	DEBUG	8816	Endpoint Added	VoIP %s Endpoint added
638	VoIP	SIP	VoIP	DEBUG	8817	Endpoint Removed	VoIP %s Endpoint removed
639	VoIP	SIP	VoIP	WARNING	8818	Endpoint Deny	VoIP %s Endpoint not added - configured 'public' endpoint limit reached
640	VoIP	H.323	VoIP	DEBUG	8819	H.323/RAS Unknown Message Response	H.323/RAS Unknown Message Response
641	VoIP	H.323	VoIP	DEBUG	8820	H.323/RAS Disengage Reject	H.323/RAS Disengage Reject
642	VoIP	H.323	VoIP	DEBUG	8821	H.323/RAS Unregistration Reject	H.323/RAS Unregistration Reject
643	VoIP	SIP	VoIP	DEBUG	8822	SIP Request	SIP Request

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
644	VoIP	SIP	VoIP	DEBUG	8823	SIP Response	SIP Response
645	VoIP	SIP	VoIP	INFO	8824	SIP Register Expire	SIP Register expiration exceeds configured Signaling inactivity time out
646	Firewall	Access Rules	System Error	WARNING	5238	Source IP Connection Limit	Packet dropped; connection limit for this source IP address has been reached
647	Firewall	Access Rules	System Error	WARNING	5239	Destination IP Connection Limit	Packet dropped; connection limit for this destination IP address has been reached
648	VPN	VPN IPsec	Attack	ERROR	572	Illegal Destination	Packet destination not in VPN Access list
651	Network	IPcomp	Debug	DEBUG	12401	IPcomp Interrupt Error	IPcomp connection interrupt
652	Network	IPcomp	TCP | UDP | ICMP	NOTICE	12402	IPcomp Packet Drop	IPcomp packet dropped
653	Network	IPcomp	Debug	DEBUG	12403	IPcomp Packet Drop, Waiting	IPcomp packet dropped; waiting for pending IPcomp connection
654	Log	General	System Error	CRITICAL	5605	Maximum Events Rate Exceeded	Maximum events per second threshold exceeded: %s
655	Log	Syslog	System Error	CRITICAL	5606	Maximum Syslog Data Rate Exceeded	Maximum syslog data per second threshold exceeded: %s
656	Log	E-mail	System Error	WARNING	5607	POP-Before-SMTP Authentication Failed	SMTP POP-Before-SMTP authentication failed
657	Log	Syslog	Maintenance	INFO	7009	Syslog Server Unreachable	Syslog Server cannot be reached
658	VPN	VPN IKE	System Error	WARNING	9464	Responder: IKE ID mismatch	IKE Responder: Proposed IKE ID mismatch

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
659	VPN	VPN Client	System Error	WARNING	9209	Responder: Duplicate Entry in Relay Table	IKE Responder: IP Address already exists in the DHCP relay table. Client traffic not allowed.
660	VPN	VPN Client	System Error	WARNING	9210	Responder: Static IP Not Allowed	IKE Responder: %s Policy does not allow static IP for Virtual Adapter.
661	VPN	VPN IKE	User Activity	WARNING	9465	Invalid Payload	Received notify: INVALID_PAYLOAD
662	Wireless	SonicPoint	Attack	ERROR	6434	Non SonicPoint Traffic Drop	Drop WLAN traffic from non-SonicPoint devices
667	Wireless	SonicPoint	SonicPoint	INFO	10401	SonicPoint Status	SonicPoint Status
668	High Availability	State	Maintenance	INFO	6227	HA Peer Firewall Reboot	HA Peer Firewall Rebooted
669	High Availability	State	System Error	ERROR	663	Error Rebooting HA Peer Firewall	Error Rebooting HA Peer Firewall
670	High Availability	General	System Error	ERROR	664	HA License Error	License of HA pair doesn't match: %s
671	High Availability	State	System Error	NOTICE	665	Reboot Signal From Secondary	Primary received reboot signal from Secondary
672	High Availability	State	System Error	NOTICE	666	Reboot Signal From Primary	Secondary received reboot signal from Primary
674	High Availability	Monitoring	System Error	INFO	6233	Probe Success	Success to reach Interface %s probe
675	High Availability	Monitoring	System Error	NOTICE	6234	Probe Failed	Failure to reach Interface %s probe
676	Firewall Settings	Multicast	---	INFO	10601	IGMPv2 Client Joined Multicast Group	IGMP V2 client joined multicast Group : %s
677	Firewall Settings	Multicast	---	INFO	10602	IGMPv3 Client Joined Multicast Group	IGMP V3 client joined multicast Group : %s
682	Firewall Settings	Multicast	---	INFO	10607	IGMP Leave Group Message	IGMP Leave group message Received on interface %s

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
683	Firewall Settings	Multicast	---	NOTICE	10608	Wrong IGMP Checksum	IGMP packet dropped, wrong checksum received on interface %s
690	Firewall Settings	Multicast	---	NOTICE	10615	UDP Packet Drop	Multicast UDP packet dropped, no state entry
694	Firewall Settings	Multicast	---	WARNING	10619	RTP Stateful Failed	Multicast UDP packet dropped, RTP stateful failed
701	Firewall Settings	Multicast	---	DEBUG	10626	IGMP Router Detected	IGMP querier Router detected on interface %s
706	Network	Network Monitor	---	ALERT	14005	Host Down	Network Monitor: Host %s is offline
707	Network	Network Monitor	---	ALERT	14006	Host Up	Network Monitor: Host %s is online
708	Network	TCP	Debug	DEBUG	7010	TCP Invalid SEQ Number	TCP packet received with invalid SEQ number; TCP packet dropped
709	Network	TCP	Debug	DEBUG	7011	TCP Invalid ACK Number	TCP packet received with invalid ACK number; TCP packet dropped
712	Network	TCP	Debug	DEBUG	7014	TCP Connection Reject	TCP connection reject received; TCP connection dropped
713	Network	TCP	Debug	DEBUG	7015	TCP Connection Abort	TCP connection abort received; TCP connection dropped
714	Network	Network Access	Debug	NOTICE	7236	EIGRP Packet Drop	EIGRP packet dropped
719	VPN	VPN IPsec	System Error	WARNING	9006	Bad SA Count	VPN policy count received exceeds the limit; %s
720	Network	PPPoE	Maintenance	INFO	7820	Send LCP Echo Request	Sending LCP Echo Request
721	Network	PPPoE	Maintenance	INFO	7821	Receive LCP Echo Request	Received LCP Echo Request
722	Network	PPPoE	Maintenance	INFO	7822	Send LCP Echo Reply	Sending LCP Echo Reply
723	Network	PPPoE	Maintenance	INFO	7823	Receive LCP Echo Reply	Received LCP Echo Reply

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
724	Wireless	Wireless Access	---	WARNING	7237	Guest Services Deny Network	Guest Services drop traffic to deny network
725	Wireless	Wireless Access	---	INFO	7238	Guest Services Allow Network	Guest Services pass traffic to access allow network
726	Wireless	Wireless Access	---	WARNING	7239	WLAN Max User Reached	WLAN max concurrent users reached already
727	Wireless	SonicPoint	SonicPoint	INFO	10402	SonicPoint Provision	SonicPoint Provision
728	Users	Authentication Access	Maintenance	INFO	4248	WLAN Disable By Schedule	WLAN disabled by schedule
729	Users	Authentication Access	Maintenance	INFO	4249	WLAN Enabled By Schedule	WLAN enabled by schedule
732	Wireless	WLAN	TCP | UDP | ICMP	WARNING	10210	WLAN SSL VPN Enforcement Check Drop	Packet dropped by WLAN SSL VPN enforcement check
733	SSL VPN	General	Maintenance	INFO	10211	SSL VPN Enforcement	SSL VPN enforcement
734	Firewall	Access Rules	---	WARNING	---	Source Connection Status	Source IP address connection status: %s
735	Firewall	Access Rules	---	WARNING	---	Destination Connection Status	Destination IP address connection status: %s
737	Log	E-mail	System Error	WARNING	---	SMTP Authentication Failed	SMTP authentication problem:%s
738	Network	PPPoE	Maintenance	INFO	---	Session Duration	PPPoE Client: Previous session was connected for %s
744	Users	Radius Authentication	User Activity	WARNING	8205	RADIUS Communication Problem	User login denied - RADIUS communication problem
745	Users	Radius Authentication	User Activity	INFO	8206	LDAP Authentication Failure	User login denied - LDAP authentication failure
746	Users	Radius Authentication	User Activity	WARNING	8207	LDAP Server Timeout	User login denied - LDAP server Timeout
747	Users	Radius Authentication	User Activity	WARNING	8208	LDAP Server Error	User login denied - LDAP server down or misconfigured

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
748	Users	Radius Authentication	User Activity	WARNING	8209	LDAP Communication Problem	User login denied - LDAP communication problem
749	Users	Radius Authentication	User Activity	WARNING	8210	LDAP Server Invalid Credential	User login denied - invalid credentials on LDAP server
750	Users	Radius Authentication	User Activity	WARNING	8211	LDAP Server Insufficient Access	User login denied - insufficient access on LDAP server
751	Users	Radius Authentication	User Activity	WARNING	8212	LDAP Schema Mismatch	User login denied - LDAP schema mismatch
752	Users	Radius Authentication	User Activity	WARNING	8213	LDAP Server Certificate With Wrong Name	Allowed LDAP server certificate with wrong host name
753	Users	Radius Authentication	User Activity	WARNING	8214	LDAP Server Name Resolution Failed	User login denied - LDAP server name resolution failed
754	Users	Radius Authentication	User Activity	WARNING	8215	RADIUS Server Name Resolution Failed	User login denied - RADIUS server name resolution failed
755	Users	Radius Authentication	User Activity	WARNING	8216	LDAP Server Certificate Invalid	User login denied - LDAP server certificate not valid
756	Users	Radius Authentication	User Activity	WARNING	8217	LDAP TLS or Local Error	User login denied - TLS or local certificate problem
757	Users	Radius Authentication	User Activity	WARNING	8218	LDAP Directory Mismatch	User login denied - LDAP directory mismatch
758	Users	Radius Authentication	User Activity	WARNING	---	LDAP Server Not Allowing CHAP	LDAP server does not allow CHAP
759	Users	Authentication Access	User Activity	INFO	---	User Already Logged-In	User login denied - user already logged in
760	Network	TCP	---	NOTICE	7240	TCP Handshake Violation Detected	TCP handshake violation detected; TCP connection dropped

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
766	Security Services	General	Maintenance	WARNING	8628	Synchronize License Failed	Failed to synchronize license information with Licensing Server. %s
773	Network	Dynamic DNS	System Error	ERROR	11801	DDNS Abuse	DDNS Failure: Provider %s
774	Network	Dynamic DNS	System Error	ERROR	11802	DDNS Invalid	DDNS Failure: Provider %s
776	Network	Dynamic DNS	Maintenance	INFO	11804	DDNS Update Success	DDNS Update success for domain %s
777	Network	Dynamic DNS	System Error	WARNING	11805	DDNS Warning	DDNS Warning: Provider %s
778	Network	Dynamic DNS	Maintenance	INFO	11806	DDNS Taken Offline	DDNS association %s taken Offline locally
779	Network	Dynamic DNS	Maintenance	INFO	11807	DDNS Added	DDNS association %s added
780	Network	Dynamic DNS	Maintenance	INFO	11808	DDNS Association Enable	DDNS association %s enabled
781	Network	Dynamic DNS	Maintenance	INFO	11809	DDNS Association Disable	DDNS association %s disabled
782	Network	Dynamic DNS	Maintenance	INFO	11810	DDNS Association On-line	DDNS Association %s put on line
783	Network	Dynamic DNS	Maintenance	INFO	11811	Deleted All DDNS Association	All DDNS associations have been deleted
785	Network	Dynamic DNS	Maintenance	INFO	11813	Delete DDNS Association	DDNS association %s deleted
786	Network	Dynamic DNS	---	INFO	---	DDNS Updating	DDNS association %s updated
789	Security Services	IDP	Attack	ALERT	6435	IDP Detection Alert	IDP Detection Alert: %s
790	Security Services	IDP	Attack	ALERT	6436	IDP Prevention Alert	IDP Prevention Alert: %s
791	Security Services	DPI-SSL	---	INFO	---	DPI-SSL	DPI-SSL: %s
793	Firewall	Application Firewall	User Activity	ALERT	13201	Application Firewall Alert	Application Firewall Alert: %s
794	Security Services	Anti-Spyware	Attack	ALERT	6437	Anti-Spyware Prevention Alert	Anti-Spyware Prevention Alert: %s

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
795	Security Services	Anti-Spyware	Attack	ALERT	6438	Anti-Spyware Detection Alert	Anti-Spyware Detection Alert: %s
796	Security Services	Anti-Spyware	Maintenance	WARNING	8631	Anti-Spyware Service Expired	Anti-Spyware Service Expired
797	Security Services	RBL Filter	---	NOTICE	12001	Outbound Connection Drop	Outbound connection to RBL-listed SMTP server dropped
798	Security Services	RBL Filter	---	NOTICE	12002	Inbound Connection Drop	Inbound connection from RBL-listed SMTP server dropped
799	Security Services	RBL Filter	---	NOTICE	12003	SMTP Server on RBL Blacklist	SMTP server found on RBL blacklist
800	Security Services	RBL Filter	---	ERROR	12004	No Valid DNS Server on RBL	No valid DNS server specified for RBL lookups
805	System	NSM	---	INFO	6002	Interface Statistics Report	Interface statistics report
806	System	NSM	---	INFO	6003	SonicPoint Statistics Report	SonicPoint statistics report
809	Security Services	GAV	Attack	ALERT	8632	AV Gateway Alert	Gateway Anti-Virus Alert: %s
810	Security Services	GAV	Maintenance	WARNING	8633	AV Gateway Service Expire	Gateway Anti-Virus Service expired
815	Network	ARP	---	WARNING	7022	Too Many Gratuitous ARPs Detected	Too many gratuitous ARPs detected
817	Users	Authentication Access	User Activity	INFO	4250	Remote Dialup Received	Incoming call received for Remotely Triggered Dial-out session
818	Users	Authentication Access	User Activity	INFO	4251	Remote Dialup Authentication Request	Remotely Triggered Dial-out session started. Requesting authentication
819	Users	Authentication Access	User Activity	INFO	4252	Remote Dialup Authentication Password Error	Incorrect authentication received for Remotely Triggered Dial-out

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
820	Users	Authentication Access	User Activity	INFO	4253	Remote Dialup Authentication Password Valid	Successful authentication received for Remotely Triggered Dial-out
821	Users	Authentication Access	User Activity	INFO	4254	Remote Dialup Authentication Password Timeout	Authentication Timeout during Remotely Triggered Dial-out session
822	Users	Authentication Access	User Activity	INFO	4255	Remote Dialup Abort For Data	Remotely Triggered Dial-out session ended. Valid WAN bound data found. Normal dial-up sequence will commence
824	High Availability	General	System Error	ERROR	6236	License Expire to Shutdown Secondary	Secondary shut down because license is expired
825	High Availability	State	System Error	INFO	6237	Secondary Active	Secondary active
826	High Availability	State	---	ERROR	6238	HA Error	%s
829	High Availability	State	---	ALERT	6241	HA Alert	%s
830	High Availability	State	---	NOTICE	6242	HA Notice	%s
832	Network	DHCP Server	---	INFO	5237	DHCP Scopes Altered	DHCP Scopes altered automatically due to change in network settings for interface %s
833	Network	DHCP Server	System Error	WARNING	---	DHCP Lease File Corrupt	DHCP lease file in the storage is corrupted; read failed
834	Network	DHCP Server	System Error	WARNING	---	Failed to Write DHCP Leases to Storage	Failed to write DHCP leases to storage
835	Network	DHCP Server	Maintenance	INFO	---	DHCP Leases Written to Storage	DHCP leases written to storage
840	Network	Advanced Routing	---	INFO	12201	RIP Info	%s
841	Network	Advanced Routing	---	NOTICE	12202	RIP Notice	%s

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
842	Network	Advanced Routing	---	DEBUG	12203	RIP Debug	%s
843	Network	Advanced Routing	---	INFO	---	OSPF Info	%s
844	Network	Advanced Routing	---	DEBUG	---	OSPF Debug	%s
845	Network	Advanced Routing	---	INFO	---	BGP Info	%s
846	Network	Advanced Routing	---	DEBUG	---	BGP Debug	%s
847	Network	Interfaces	Maintenance	WARNING	7025	IP Address Conflict	IP address conflict detected from Ethernet address %s
848	VPN	VPN PKI	User Activity	INFO	9838	OCSP Send Request	OCSP sending request.
849	VPN	VPN PKI	User Activity	ERROR	9839	OCSP Failed to Send Request	OCSP send request message failed.
850	VPN	VPN PKI	User Activity	INFO	9840	OCSP Received Response	OCSP received response.
852	VPN	VPN PKI	User Activity	INFO	9842	OCSP Resolved Domain Name	OCSP Resolved Domain Name.
853	VPN	VPN PKI	User Activity	ERROR	9843	OCSP Failed to Resolve Domain Name	OCSP Failed to Resolve Domain Name.
854	VPN	VPN PKI	User Activity	ERROR	9844	OCSP Internal Error	OCSP Internal error handling received response.
856	Firewall Settings	Flood Protection	Attack	WARNING	6439	SYN Flood Watch Mode	SYN Flood Mode changed by user to: Watch and report possible SYN floods
857	Firewall Settings	Flood Protection	Attack	WARNING	6440	SYN Flood Trigger Mode	SYN Flood Mode changed by user to: Watch and proxy WAN connections when under attack
858	Firewall Settings	Flood Protection	Attack	WARNING	6441	SYN Flood Proxy Mode	SYN Flood Mode changed by user to: Always proxy WAN connections
859	Firewall Settings	Flood Protection	Attack	ALERT	6442	SYN Flood Proxy Trigger Mode	Possible SYN flood detected on WAN IF %s - switching to connection-proxy mode

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
860	Firewall Settings	Flood Protection	Attack	ALERT	6443	SYN Flood Detected	Possible SYN Flood on IF %s
861	Firewall Settings	Flood Protection	Attack	ALERT	6444	SYN Flood Proxy Mode Cancel	SYN flood ceased or flooding machines blacklisted - connection proxy disabled
862	Firewall Settings	Flood Protection	Attack	WARNING	6445	SYN Flood Blacklist On	SYN Flood blacklisting enabled by user
863	Firewall Settings	Flood Protection	Attack	WARNING	6446	SYN Flood Blacklist Off	SYN Flood blacklisting disabled by user
864	Firewall Settings	Flood Protection	Attack	ALERT	6447	SYN-Flooding Machine Blacklisted	SYN-Flooding machine %s blacklisted
865	Firewall Settings	Flood Protection	Attack	ALERT	6448	Machine removed from SYN Flood Blacklist	Machine %s removed from SYN flood blacklist
866	Firewall Settings	Flood Protection	Attack	WARNING	6449	Possible SYN Flood Continues	Possible SYN Flood on IF %s continues
867	Firewall Settings	Flood Protection	Attack	ALERT	6450	Possible SYN Flood Ceased	Possible SYN Flood on IF %s has ceased
868	Firewall Settings	Flood Protection	Attack	WARNING	6451	SYN Flood Blacklist Continues	SYN Flood Blacklist on IF %s continues
869	Firewall Settings	Flood Protection	Attack	DEBUG	6452	TCP SYN Receive	TCP SYN received
874	VPN	VPN PKI	User Activity	NOTICE	9845	CRL Expire	CRL has expired
875	VPN	VPN PKI	User Activity	WARNING	9846	Failed to Find Certificate	Failed to find certificate
876	VPN	VPN PKI	User Activity	WARNING	9847	CRL Missing	CRL missing - Issuer requires CRL checking.
877	VPN	VPN PKI	User Activity	WARNING	9848	CRL Validation Error	CRL validation failure for Root Certificate
878	VPN	VPN PKI	User Activity	WARNING	9849	Can't Validate Issuer Path	Cannot Validate Issuer Path
879	Wireless	RF Monitoring	---	WARNING	---	WLAN Radio Frequency Threat Detected	WLAN radio frequency threat detected

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
880	Network	Dynamic Address Objects	Maintenance	INFO	---	Failed to Resolve Dynamic Address Object	Unable to resolve dynamic address object
881	System	Time	---	NOTICE	5608	System Clock Manually Updated	System clock manually updated
882	Network	Network Access	TCP	DEBUG	7242	HTTP Drop	HTTP method detected; examining stream for host header
883	Firewall Settings	Checksum Enforcement	TCP|UDP	NOTICE	7243	IP Checksum Error	IP Header checksum error; packet dropped
884	Firewall Settings	Checksum Enforcement	TCP	NOTICE	7244	TCP Checksum Error	TCP checksum error; packet dropped
885	Firewall Settings	Checksum Enforcement	UDP	NOTICE	7245	UDP Checksum Error	UDP checksum error; packet dropped
886	Firewall Settings	Checksum Enforcement	UDP	NOTICE	7246	ICMP Checksum Error	ICMP checksum error; packet dropped
887	Network	TCP	Debug	DEBUG	7026	Invalid TCP Header Length	TCP packet received with invalid header length; TCP packet dropped
888	Network	TCP	Debug	DEBUG	7027	TCP Connection Does Not Exist	TCP packet received on non-existent/closed connection; TCP packet dropped
889	Network	TCP	Debug	DEBUG	7028	TCP Without Mandatory SYN Flag	TCP packet received without mandatory SYN flag; TCP packet dropped
890	Network	TCP	Debug	DEBUG	7029	TCP Without Mandatory ACK Flag	TCP packet received without mandatory ACK flag; TCP packet dropped
891	Network	TCP	Debug	DEBUG	7030	TCP Packet on Closing Connection	TCP packet received on a closing connection; TCP packet dropped
892	Network	TCP	Debug	INFO	7031	SYN Flag on Existing Connection	TCP packet received with SYN flag on an existing connection; TCP packet dropped

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
893	Network	TCP	Debug	DEBUG	7032	Invalid TCP SACK Option Length	TCP packet received with invalid SACK option length; TCP packet dropped
894	Network	TCP	Debug	DEBUG	7033	Invalid TCP MSS Option Length	TCP packet received with invalid MSS option length; TCP packet dropped
895	Network	TCP	Debug	DEBUG	7034	Invalid TCP Option Length	TCP packet received with invalid option length; TCP packet dropped
896	Network	TCP	Debug	DEBUG	7035	Invalid TCP Source Port	TCP packet received with invalid source port; TCP packet dropped
897	Firewall Settings	Flood Protection	Attack	INFO	7036	Invalid TCP SYN Flood Cookie	TCP packet received with invalid SYN Flood cookie; TCP packet dropped
898	Firewall Settings	Flood Protection	Attack	ALERT	6453	RST-Flooding Machine Blacklisted	RST-Flooding machine %s blacklisted
899	Firewall Settings	Flood Protection	Attack	WARNING	6454	RST Flood Blacklist Continues	RST Flood Blacklist on IF %s continues
900	Firewall Settings	Flood Protection	Attack	ALERT	6455	Machine Removed From RST Flood Blacklist	Machine %s removed from RST flood blacklist
901	Firewall Settings	Flood Protection	Attack	ALERT	6456	FIN-Flooding Machine Blacklisted	FIN-Flooding machine %s blacklisted
902	Firewall Settings	Flood Protection	Attack	WARNING	6457	FIN Flood Blacklist Continues	FIN Flood Blacklist on IF %s continues
903	Firewall Settings	Flood Protection	Attack	ALERT	6458	Machine Removed From FIN Flood Blacklist	Machine %s removed from FIN flood blacklist
904	Firewall Settings	Flood Protection	Attack	ALERT	6459	Possible RST Flood	Possible RST Flood on IF %s
905	Firewall Settings	Flood Protection	Attack	ALERT	6460	Possible FIN Flood	Possible FIN Flood on IF %s
906	Firewall Settings	Flood Protection	Attack	ALERT	6461	Possible RST Flood Ceased	Possible RST Flood on IF %s has ceased

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
907	Firewall Settings	Flood Protection	Attack	ALERT	6462	Possible FIN Flood Ceased	Possible FIN Flood on IF %s has ceased
908	Firewall Settings	Flood Protection	Attack	WARNING	6463	Possible RST Flood Continues	Possible RST Flood on IF %s continues
909	Firewall Settings	Flood Protection	Attack	WARNING	6464	Possible FIN Flood Continues	Possible FIN Flood on IF %s continues
910	Network	IP	Debug	NOTICE	7037	IP TTL Expire	Packet Dropped - IP TTL expired
911	Network	Dynamic Address Objects	Maintenance	INFO	---	Added Host Entry	Added host entry to dynamic address object
912	Network	Dynamic Address Objects	Maintenance	INFO	---	Removed Host Entry	Removed host entry from dynamic address object
913	VPN	VPN IKE	User Activity	WARNING	9466	Responder: Authentication Method Mismatch	IKE Responder: Phase 1 Authentication Method does not match
914	VPN	VPN IKE	User Activity	WARNING	9467	Responder: Encryption Algorithm Mismatch	IKE Responder: Phase 1 encryption algorithm does not match
915	VPN	VPN IKE	User Activity	WARNING	9468	Responder: Key Length Mismatch	IKE Responder: Phase 1 encryption algorithm keylength does not match
916	VPN	VPN IKE	User Activity	WARNING	9469	Responder: Hash Algorithm Mismatch	IKE Responder: Phase 1 hash algorithm does not match
917	VPN	VPN IKE	User Activity	WARNING	9470	Responder: Policy Has no User Name	IKE Responder: Phase 1 XAUTH required but Policy has no user name
918	VPN	VPN IKE	User Activity	WARNING	9471	Responder: Policy Has no Password	IKE Responder: Phase 1 XAUTH required but Policy has no user password
919	VPN	VPN IKE	User Activity	WARNING	9472	Responder: DH Group Mismatch	IKE Responder: Phase 1 DH Group does not match

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
920	VPN	VPN IKE	User Activity	WARNING	9473	Responder: AH Authentication Algorithm Mismatch	IKE Responder: AH authentication algorithm does not match
921	VPN	VPN IKE	User Activity	WARNING	9474	Responder: ESP Encryption Algorithm Mismatch	IKE Responder: ESP encryption algorithm does not match
922	VPN	VPN IKE	User Activity	WARNING	9475	Responder: ESP Authentication Algorithm Mismatch	IKE Responder: ESP authentication algorithm does not match
923	VPN	VPN IKE	User Activity	WARNING	9476	Responder: AH Authentication Key Length Mismatch	IKE Responder: AH authentication key length does not match
924	VPN	VPN IKE	User Activity	WARNING	9477	Responder: ESP Encryption Key Length Mismatch	IKE Responder: ESP encryption key length does not match
925	VPN	VPN IKE	User Activity	WARNING	9478	Responder: ESP Authentication Key Length Mismatch	IKE Responder: ESP authentication key length does not match
926	VPN	VPN IKE	User Activity	WARNING	9479	Responder: AH Authentication Key Rounds Mismatch	IKE Responder: AH authentication key rounds does not match
927	VPN	VPN IKE	User Activity	WARNING	9480	Responder: ESP Encryption Key Rounds Mismatch	IKE Responder: ESP encryption key rounds does not match
928	VPN	VPN IKE	User Activity	WARNING	9481	Responder: ESP Authentication Key Rounds Mismatch	IKE Responder: ESP authentication key rounds does not match
930	VPN	VPN IKE	User Activity	NOTICE	9483	Initiator: Peer Timeout - Retransmitting	IKE Initiator: Remote party Timeout - Retransmitting IKE Request.
931	VPN	VPN IKE	User Activity	NOTICE	9484	Responder: Peer Timeout - Retransmitting	IKE Responder: Remote party Timeout - Retransmitting IKE Request.

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
932	VPN	VPN IKE	User Activity	WARNING	9485	Responder: IPsec Protocol Mismatch	IKE Responder: IPsec protocol mismatch
933	VPN	VPN IKE	User Activity	WARNING	9486	Initiator: Proposed IKE ID Mismatch	IKE Initiator: Proposed IKE ID mismatch
934	VPN	VPN IKE	User Activity	WARNING	9487	Responder: Local Network Mismatch Peer's Destination Network	IKE Responder: Peer's local network does not match VPN Policy's [Destination]
935	VPN	VPN IKE	User Activity	WARNING	9488	Responder: Destination Network Mismatch Peer's Local Network	IKE Responder: Peer's destination network does not match VPN Policy's [Local Network]
936	VPN	VPN IKE	User Activity	WARNING	9489	Responder: Route Table Overrides VPN Policy	IKE Responder: Route table overrides VPN Policy
937	VPN	VPN IKE	User Activity	WARNING	9490	Initiator: IKE Proposal Mismatch	IKE Initiator: IKE proposal does not match (Phase 1)
938	VPN	VPN IKEv2	User Activity	INFO	9491	Initiator: Send IKE_SA_INIT Request	IKEv2 Initiator: Send IKE_SA_INIT Request
939	VPN	VPN IKEv2	User Activity	INFO	9492	Responder: Received IKE_SA_INIT Request	IKEv2 Responder: Received IKE_SA_INIT Request
940	VPN	VPN IKEv2	User Activity	INFO	9493	Initiator: Send IKE_AUTH Request	IKEv2 Initiator: Send IKE_AUTH Request
941	VPN	VPN IKEv2	User Activity	INFO	9494	Responder: Received IKE_AUTH Request	IKEv2 Responder: Received IKE_AUTH Request
942	VPN	VPN IKEv2	User Activity	INFO	9495	Authentication Successful	IKEv2 Authentication successful
943	VPN	VPN IKEv2	User Activity	INFO	9496	Accept IKE SA Proposal	IKEv2 Accept IKE SA Proposal
944	VPN	VPN IKEv2	User Activity	INFO	9497	Accept IPsec SA Proposal	IKEv2 Accept IPsec SA Proposal

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
945	VPN	VPN IKEv2	User Activity	INFO	9498	Initiator: Send CREATE_CHILD _SA Request	IKEv2 Initiator: Send CREATE_CHILD_SA Request
946	VPN	VPN IKEv2	User Activity	INFO	9499	Responder: Received CREATE_CHILD _SA Request	IKEv2 Responder: Received CREATE_CHILD_SA Request
947	VPN	VPN IKEv2	User Activity	INFO	9500	Send Delete IKE SA Request	IKEv2 Send delete IKE SA Request
948	VPN	VPN IKEv2	User Activity	INFO	9501	Received Delete IKE SA Request	IKEv2 Received delete IKE SA Request
949	VPN	VPN IKEv2	User Activity	INFO	9502	Send Delete IPsec SA Request	IKEv2 Send delete IPsec SA Request
950	VPN	VPN IKEv2	User Activity	INFO	9503	Received Delete IPsec SA Request	IKEv2 Received delete IPsec SA Request
951	VPN	VPN IKEv2	User Activity	INFO	9504	Responder: Destination Network Mismatch Peer's Local Network	IKEv2 Responder: Peer's destination network does not match VPN Policy's [Local Network]
952	VPN	VPN IKEv2	User Activity	INFO	9505	Responder: Peer Local Network Mismatch Peer's Destination Network	IKEv2 Responder: Peer's local network does not match VPN Policy's [Destination Network]
953	VPN	VPN IKEv2	User Activity	WARNING	9506	Payload Processing Error	IKEv2 Payload processing error
954	VPN	VPN IKEv2	User Activity	WARNING	9507	Initiator: Extra Payloads Present	IKEv2 Initiator: Negotiations failed. Extra payloads present.
955	VPN	VPN IKEv2	User Activity	WARNING	9508	Initiator: Missing Required Payloads	IKEv2 Initiator: Negotiations failed. Missing required payloads.
956	VPN	VPN IKEv2	User Activity	WARNING	9509	Initiator: Invalid Input State	IKEv2 Initiator: Negotiations failed. Invalid input state.

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
957	VPN	VPN IKEv2	User Activity	WARNING	9510	Initiator: Invalid Output State	IKEv2 Initiator: Negotiations failed. Invalid output state.
958	VPN	VPN IKEv2	User Activity	WARNING	9511	Payload Validation Failed	IKEv2 Payload validation failed.
959	VPN	VPN IKEv2	User Activity	WARNING	9512	Unable to Find IKE SA	IKEv2 Unable to find IKE SA
960	VPN	VPN IKEv2	User Activity	WARNING	9513	Decrypt Packet Failed	IKEv2 Decrypt packet failed
961	VPN	VPN IKEv2	User Activity	WARNING	9514	Out of Memory	IKEv2 Out of memory
962	VPN	VPN IKEv2	User Activity	NOTICE	---	Responder: Policy for Remote IKE ID Not Found	IKEv2 Responder: Policy for remote IKE ID not found
963	VPN	VPN IKEv2	User Activity	WARNING	9515	Process Message Queue Failed	IKEv2 Process Message queue failed
964	VPN	VPN IKEv2	User Activity	WARNING	9516	Invalid State	IKEv2 Invalid state
965	VPN	VPN IKE	System Error	WARNING	---	IKE Responder: No VPN Access Networks Assigned	IKE Responder: Client Policy has no VPN Access Networks assigned. Check Configuration.
966	VPN	VPN IKEv2	User Activity	WARNING	9517	Invalid SPI Size	IKEv2 Invalid SPI size
967	VPN	VPN IKEv2	User Activity	WARNING	9518	VPN Policy Not Found	IKEv2 VPN Policy not found
968	VPN	VPN IKEv2	User Activity	WARNING	9519	IPsec Proposal Mismatch	IKEv2 IPsec proposal does not match
969	VPN	VPN IKEv2	User Activity	WARNING	9520	IPsec Attribute Not Found	IKEv2 IPsec attribute not found
970	VPN	VPN IKEv2	User Activity	WARNING	9521	IKE Attribute Not Found	IKEv2 IKE attribute not found
971	VPN	VPN IKEv2	User Activity	WARNING	9522	Peer Not Responding	IKEv2 Peer is not responding. Negotiation aborted.
972	VPN	VPN IKEv2	User Activity	INFO	9523	Initiator: Retransmit IKEv2 Request Due to Remote Party Timeout	IKEv2 Initiator: Remote party Timeout - Retransmitting IKEv2 Request.

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
973	VPN	VPN IKEv2	User Activity	INFO	9524	Initiator: Received IKE_SA_INT Response	IKEv2 Initiator: Received IKE_SA_INT response
974	VPN	VPN IKEv2	User Activity	INFO	9525	Initiator: Received IKE_AUTH Response	IKEv2 Initiator: Received IKE_AUTH response
975	VPN	VPN IKEv2	User Activity	INFO	9526	Initiator: Received CREATE_CHILD _SA Response	IKEv2 Initiator: Received CREATE_CHILD_SA response
976	VPN	VPN IKEv2	User Activity	INFO	---	Responder: Send IKE_SA_INIT Response	IKEv2 Responder: Send IKE_SA_INIT response
977	VPN	VPN IKEv2	User Activity	INFO	---	Responder: Send IKE_AUTH response	IKEv2 Responder: Send IKE_AUTH response
978	VPN	VPN IKEv2	User Activity	INFO	9527	Negotiation Completed	IKEv2 negotiation complete
979	VPN	VPN IKEv2	User Activity	ERROR	9528	Failed to Transmit Packet	IKEv2 Function sendto() failed to transmit packet.
980	VPN	VPN IKEv2	User Activity	WARNING	9529	Initiator: Proposed IKE ID Mismatch	IKEv2 Initiator: Proposed IKE ID mismatch
981	VPN	VPN IKEv2	User Activity	WARNING	9530	IKE Proposal Mismatch	IKEv2 IKE proposal does not match
982	VPN	VPN IKEv2	User Activity	INFO	9531	Received Notify Status Payload	IKEv2 Received notify status payload
983	VPN	VPN IKEv2	User Activity	WARNING	9532	Received Notify Error Payload	IKEv2 Received notify error payload
984	VPN	VPN IKEv2	User Activity	INFO	9533	No NAT Device Detected	IKEv2 No NAT device detected between negotiating peers
985	VPN	VPN IKEv2	User Activity	INFO	9534	NAT Device Detected Between Negotiating Peers	IKEv2 NAT device detected between negotiating peers
986	Users	Authentication Access	User Activity	INFO	4256	Not Allowed by Policy Rule	User login denied - not allowed by Policy rule
987	Users	Authentication Access	User Activity	INFO	4257	Not Found Locally	User login denied - not found locally

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
988	Users	SSO Agent Authentication	User Activity	WARNING	12601	Timeout	User login denied - SSO agent Timeout
989	Users	SSO Agent Authentication	User Activity	WARNING	12602	Configuration Error	User login denied - SSO agent configuration error
990	Users	SSO Agent Authentication	User Activity	WARNING	12603	Communication Problem	User login denied - SSO agent communication problem
991	Users	SSO Agent Authentication	User Activity	WARNING	12604	Name Resolution Failed	User login denied - SSO agent name resolution failed
992	Users	SSO Agent Authentication	User Activity	WARNING	12605	User Name Too Long	SSO agent returned user name too long
993	Users	SSO Agent Authentication	User Activity	WARNING	12606	Domain Name Too Long	SSO agent returned domain name too long
994	Users	Authentication Access	User Activity	INFO	4258	Configuration Mode Administration Session Started	Configuration mode administration session started
995	Users	Authentication Access	User Activity	INFO	4259	Configuration Mode Administration Session Ended	Configuration mode administration session ended
996	Users	Authentication Access	User Activity	INFO	4260	Read-only Mode GUI Administration Session Started	Read-only mode GUI administration session started
997	Users	Authentication Access	User Activity	INFO	4261	Non-Config Mode GUI Administration Session Started	Non-config mode GUI administration session started
998	Users	Authentication Access	User Activity	INFO	4262	GUI Administration Session End	GUI administration session ended
999	Firewall Settings	SSL Control	Blocked Sites	INFO	7247	Website Found in Blacklist	SSL Control: Website found in blacklist
1000	Firewall Settings	SSL Control	Blocked Sites	INFO	7248	Website Found in Whitelist	SSL Control: Website found in whitelist
1001	Firewall Settings	SSL Control	Blocked Sites	INFO	---	Weak SSL Version	SSL Control: Weak SSL Version being used
1002	Firewall Settings	SSL Control	Blocked Sites	INFO	7250	Certificate With Invalid Date	SSL Control: Certificate with invalid date

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1003	Firewall Settings	SSL Control	Blocked Sites	INFO	7251	Self-Signed Certificate	SSL Control: Self-signed certificate
1004	Firewall Settings	SSL Control	Blocked Sites	INFO	7252	Weak Cipher Being Used	SSL Control: Weak cipher being used
1005	Firewall Settings	SSL Control	Blocked Sites	INFO	7253	Untrusted CA	SSL Control: Untrusted CA
1006	Firewall Settings	SSL Control	Blocked Sites	INFO	7254	Certificate Chain Incomplete	SSL Control: Certificate chain not complete
1008	Users	Authentication Access	User Activity	INFO	---	Logout Detected by SSO	User logged out - logout detected by SSO
1009	Users	Radius Authentication	System Error	ERROR	4263	Bind to LDAP Server Failed	Bind to LDAP server failed
1010	Users	Radius Authentication	System Error	ALERT	4264	Using LDAP Without TLS	Using LDAP without TLS - highly insecure
1011	Users	Radius Authentication	System Error	WARNING	4265	Non-Administrative Attempt to Change Password	LDAP using non-administrative account - VPN client user will not be able to change passwords
1012	VPN	VPN IKEv2	User Activity	INFO	9535	Responder: Send CREATE_CHILD_SA Response	IKEv2 Responder: Send CREATE_CHILD_SA response
1013	VPN	VPN IKEv2	User Activity	INFO	9536	Send Delete IKE SA Response	IKEv2 Send delete IKE SA response
1014	VPN	VPN IKEv2	User Activity	INFO	9537	Send Delete IPsec SA Response	IKEv2 Send delete IPsec SA response
1015	VPN	VPN IKEv2	User Activity	INFO	9538	Received Delete IKE SA Response	IKEv2 Received delete IKE SA response
1016	VPN	VPN IKEv2	User Activity	INFO	9539	Received Delete IPsec SA Response	IKEv2 Received delete IPsec SA response
1017	WWAN Modem	General	System Environment	INFO	5422	WWAN Device Detected	WWAN %s device detected
1018	Network	PPP	---	INFO	11408	PPP Message	PPP message: %s
1026	WWAN Modem	General	User Activity	ALERT	7642	Data Usage Watermark Reached	WWAN: %s.

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1027	WWAN Modem	General	User Activity	ALERT	7643	Data Usage Limit Reached	WWAN: data usage limit reached for the '%s' billing cycle. Disconnecting the session.
1029	Network	TCP	Debug	DEBUG	7038	Non-Permitted Option TCP Packet	TCP packet received with non-permitted option; TCP packet dropped
1030	Network	TCP	Debug	DEBUG	7039	Invalid TCP Window Scale Option Length	TCP packet received with invalid Window Scale option length; TCP packet dropped
1031	Network	TCP	Debug	DEBUG	7040	Invalid TCP Window Scale Option Value	TCP packet received with invalid Window Scale option value; TCP packet dropped
1033	Users	Authentication Access	User Activity	WARNING	---	Group Membership Retrieval Failed	Problem occurred during user group membership retrieval
1035	Users	Authentication Access	User Activity	INFO	---	Password Expire	User login denied - password expired
1036	VPN	VPN IKE	User Activity	WARNING	---	Responder: IKE Phase 1 Exchange Mismatch	IKE Responder: IKE Phase 1 exchange does not match
1040	Network	DHCP Server	---	ALERT	5240	DHCP Server IP Conflict Detected	DHCP Server: IP conflict detected
1041	Network	DHCP Server	---	NOTICE	5241	DHCP Server Received DHCP Decline	DHCP Server: Received DHCP decline from client
1043	System	Hardware	---	ERROR	5425	Power Supply Without Redundancy	Power supply without redundancy
1044	High Availability	State	---	INFO	---	Discover HA Firewall	Discovered HA %s Firewall
1046	System	Restart	---	INFO	---	Diagnostic Auto-Restart Canceled	Diagnostic Auto-restart canceled
1047	System	Restart	---	INFO	---	Diagnostic Auto-Restart	As per Diagnostic Auto-restart configuration Request, restarting system

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1048	Users	Authentication Access	---	INFO	---	Password doesn't meet constraints	User login denied - password doesn't meet constraints
1049	System	Settings	---	INFO	---	System Setting Imported	System Setting Imported
1050	VPN	VPN IPsec	User Activity	INFO	---	VPN Policy Added	VPN policy %s is added
1051	VPN	VPN IPsec	User Activity	INFO	---	VPN Policy Deleted	VPN policy %s is deleted
1052	VPN	VPN IPsec	User Activity	INFO	---	VPN Policy Modified	VPN policy %s is modified
1055	WWAN Modem	General	---	ALERT	5420	WWAN: No SIM Detected	WWAN: No SIM detected
1058	High Availability	State	---	INFO	---	Primary Firewall Reboot from Active to Standby	Primary firewall rebooting itself as it transitioned from Active to Standby while Preempt
1059	High Availability	State	---	INFO	---	Secondary Firewall Reboot from Active to Standby	Secondary firewall rebooting itself as it transitioned from Active to Standby while Preempt
1060	Security Services	Crypto Test	---	ERROR	---	DRNG KAT Test Failed	Crypto SHA1 based DRNG KAT test failed
1065	System	Settings	Maintenance	INFO	---	Remote Backup Succeeded	Successfully sent %s file to remote backup server
1066	System	Settings	Maintenance	ALERT	---	Remote Backup Failed	Failed to send file to remote backup server, Error: %s
1068	Network	DHCP Server	---	WARNING	---	Multiple DHCP Servers Detected	Multiple DHCP Servers are detected on network
1070	Network	DNS	---	INFO	---	Invalid DNS Server	Invalid DNS Server will not be accepted by the dynamic client
1071	Network	DHCP Server	---	INFO	---	DHCP Server Sanity Check Pass	DHCP Server sanity check passed %s
1072	Network	DHCP Server	---	CRITICAL	---	DHCP Server Sanity Check Failed	DHCP Server sanity check failed %s
1073	Users	SSO Agent Authentication	User Activity	WARNING	---	Agent Error	SSO agent returned error

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1074	Network	L2TP Client	---	INFO	---	Tunnel Negotiation	L2TP Tunnel Negotiation %s
1075	Users	SSO Agent Authentication	User Activity	ALERT	---	Agent Down	SSO agent is down
1076	Users	SSO Agent Authentication	User Activity	ALERT	---	Agent Up	SSO agent is up
1077	Wireless	SonicPoint/SonicWave	---	INFO	13601	SonicPoint/SonicWave Status	%s Status
1078	Wireless	SonicPoint/SonicWave	---	INFO	13602	SonicPoint/SonicWave Provision	%s Provision
1079	SSL VPN	General	---	INFO	---	SSL VPN	%s
1080	Users	Authentication Access	---	INFO	---	Successful SSL VPN User Login	SSL VPN zone remote user login allowed
1081	Firewall Settings	SSL Control	Blocked Sites	INFO	---	Certificate Blocked Weak Digest	SSL Control: Certificate with Weak Digest Signature Algorithm
1082	Anti-Spam	Probe	---	WARNING	13801	Entity Operational	%s is operational.
1083	Anti-Spam	Probe	---	WARNING	13802	Entity Unreachable	%s is unavailable.
1084	Anti-Spam	General	---	NOTICE	13803	Service Enable	Anti-Spam service is enabled by administrator.
1085	Anti-Spam	General	---	NOTICE	13804	Service Disable	Anti-Spam service is disabled by administrator.
1086	Anti-Spam	General	---	WARNING	13805	Service Subscription Expire	Your Anti-Spam Service subscription has expired.
1087	Anti-Spam	E-mail	---	WARNING	13806	SMTP Connection Expire	SMTP connection limit is reached. Connection is dropped.
1088	Anti-Spam	General	---	WARNING	13807	Startup Failure	Anti-Spam Startup Failure - %s
1089	Anti-Spam	General	---	WARNING	13808	Teardown Failure	Anti-Spam Teardown Failure - %s
1090	Network	DHCP Server	---	NOTICE	---	DHCP Message From Untrusted Relay Agent	DHCP Server: Received DHCP message from untrusted relay agent

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1091	Anti-Spam	GRID	---	NOTICE	13809	Outbound Connection Drop	Outbound connection to GRID-listed SMTP server dropped
1092	Anti-Spam	GRID	---	NOTICE	13810	Inbound Connection Drop	Inbound connection from GRID-listed SMTP server dropped
1093	Anti-Spam	GRID	---	NOTICE	13811	SMTP Server Found on Reject List	SMTP server found on Reject List
1094	Anti-Spam	GRID	---	ERROR	13812	No Valid DNS Server	No valid DNS server specified for GRID lookups
1095	Anti-Spam	E-mail	---	INFO	13813	Unprocessed E-mail From MTA	Unprocessed E-mail received from MTA on Inbound SMTP port
1097	VPN	VPN PKI	---	NOTICE	---	SCEP Client	SCEP Client: %s
1098	Network	DNS	---	ALERT	6465	DNS Rebind Attack Detected	Possible DNS rebind attack detected
1099	Network	DNS	---	ALERT	6466	DNS Rebind Attack Blocked	DNS rebind attack blocked
1100	Network	Network Monitor	---	ALERT	14001	Policy Status is Up	Network Monitor: Policy %s status is UP
1101	Network	Network Monitor	---	ALERT	14002	Policy Status is Down	Network Monitor: Policy %s status is DOWN
1102	Network	Network Monitor	---	ALERT	14003	Policy Status is Unknown	Network Monitor: Policy %s status is UNKNOWN
1103	Network	Network Monitor	---	ALERT	14004	Host Status is Unknown	Network Monitor: Host %s status is UNKNOWN
1104	Network	Network Monitor	---	INFO	---	Policy Added	Network Monitor Policy %s Added
1105	Network	Network Monitor	---	INFO	---	Policy Deleted	Network Monitor Policy %s Deleted
1106	Network	Network Monitor	---	INFO	---	Policy Modified	Network Monitor Policy %s Modified
1107	System	Status	System Error	ALERT	---	System Alert	%s

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1108	Anti-Spam	E-mail	---	NOTICE	---	E-mail Message Blocked	Message blocked by Real-Time E-mail Scanner
1109	VPN	VPN PKI	---	INFO	---	CSR Generation	CSR Generation: %s
1110	Network	DHCP Server	---	INFO	---	Assigned IP Address	Assigned IP address %s
1111	Network	DHCP Server	---	INFO	---	Released IP Address	Released IP address %s
1112	Firewall Settings	FTP	---	DEBUG	---	FTP Server Accepted Connection	Ftp server accepted the connection
1113	Firewall Settings	FTP	---	DEBUG	---	FTP Client Username Sent	Ftp client user name was sent
1114	Firewall Settings	FTP	---	DEBUG	---	FTP Client User Login	Ftp client user logged in successfully
1115	Firewall Settings	FTP	---	DEBUG	---	FTP Client User Login Failed	Ftp client user logged in failed
1116	Firewall Settings	FTP	---	DEBUG	---	FTP Client User Logout	Ftp client user logged out
1117	Users	Authentication Access	User Activity	WARNING	---	SSO Probe Failed	User login denied - SSO probe failed
1118	Users	Authentication Access	User Activity	INFO	---	SMTP Server Not Configured	User login denied - Mail Address(From/to) or SMTP Server is not configured
1119	Users	Authentication Access	User Activity	INFO	---	RADIUS User Cannot Use One Time Password	RADIUS user cannot use One Time Password - no mail address set for equivalent local user
1120	Users	Authentication Access	User Activity	WARNING	---	TSA Timeout	User login denied - Terminal Services agent Timeout
1121	Users	Authentication Access	User Activity	WARNING	---	TSA Name Resolution Failed	User login denied - Terminal Services agent name resolution failed
1122	Users	Authentication Access	User Activity	WARNING	---	No Name Received from TSA	User login denied - No name received from Terminal Services agent

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1123	Users	Authentication Access	User Activity	WARNING	---	TSA Communication Problem	User login denied - Terminal Services agent communication problem
1124	Users	Authentication Access	User Activity	INFO	---	TSA User logout	User logged out - logout reported by Terminal Services agent
1125	High Availability	General	User Activity	INFO	---	Dial Up Device Unsupported in HA	High Availability has been enabled, Dial-Up device(s) are not supported in High Availability processing.
1126	High Availability	Monitoring	User Activity	ERROR	---	Bad Monitoring IP	The High Availability monitoring IP configuration of Interface %s is incorrect.
1127	VPN	VPN IKE	User Activity	WARNING	---	IPsec Tunnel Mode Mismatch	IKE Responder: ESP mode mismatch Local - Tunnel Remote - Transport
1128	VPN	VPN IKE	User Activity	WARNING	---	IPsec Transport Mode Mismatch	IKE Responder: ESP mode mismatch Local - Transport Remote - Tunnel
1131	Anti-Spam	Probe	---	DEBUG	---	Anti-Spam Probe Response Success	Probe Response Success - %s
1132	Anti-Spam	Probe	---	DEBUG	---	Anti-Spam Probe Response Failure	Probe Response Failure - %s
1133	Network	PPPoE	---	INFO	---	PPPoE Overview	%s
1134	Network	PPTP	Maintenance	INFO	---	PPTP Overview	%s
1135	Network	L2TP Client	Maintenance	INFO	---	L2TP Overview	%s
1138	Anti-Spam	GRID	---	DEBUG	---	Anti-Spam Unauth GRID Response	Received unauthenticated GRID response
1139	Anti-Spam	GRID	---	DEBUG	---	Anti-Spam Invalid Key in GRID Response	Invalid key or serial number used for GRID response

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1140	Anti-Spam	GRID	---	DEBUG	---	Anti-Spam Invalid Key Version in GRID Response	Invalid key version used for GRID response
1141	Anti-Spam	GRID	---	DEBUG	---	Anti-Spam Host Not GRID List	Host IP address not in GRID List
1142	Anti-Spam	General	---	DEBUG	---	Anti-Spam No Response From DNS Server	No response received from DNS server
1143	Anti-Spam	GRID	---	DEBUG	---	Anti-Spam Not Blacklisted	Not blacklisted as per configuration
1144	Anti-Spam	GRID	---	DEBUG	---	Anti-Spam Default Not Blacklisted	Default to not blacklisted
1145	Anti-Spam	GRID	---	DEBUG	---	Anti-Spam Insert Entry Failed	Failed to insert entry into GRID result IP cached table
1146	Anti-Spam	General	---	DEBUG	---	Anti-Spam Resolved Cloud Address	Resolved ES Cloud - %s
1147	Anti-Spam	General	---	DEBUG	---	Anti-Spam Cloud Address Updated	Updated ES Cloud Address - %s
1149	High Availability	Cluster	---	WARNING	---	VRRP Expiration Message	Your Active/Active Clustering subscription has expired.
1150	Users	SSO Agent Authentication	User Activity	ALERT	---	Terminal Services Agent is Down	Terminal Services agent is down
1151	Users	SSO Agent Authentication	User Activity	ALERT	---	Terminal Services Agent is Up	Terminal Services agent is up
1152	High Availability	Cluster	---	ERROR	---	VRRP Cluster No license	Active/Active Clustering license is not activated on the following cluster units: %s
1153	SSL VPN	General	---	INFO	---	SSL VPN Session	%s
1154	Security Services	Application Control	---	ALERT	15001	Application Control Detection Alert	Application Control Detection Alert: %s

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1155	Security Services	Application Control	---	ALERT	15002	Application Control Prevention Alert	Application Control Prevention Alert: %s
1156	Network	DNS	---	ERROR	---	Syslog/NSM Name Resolution Failure	Name Resolution for Syslog or NSM failed.
1157	Users	Authentication Access	User Activity	INFO	---	User Account Expired	User account '%s' expired and disabled
1158	Users	Authentication Access	User Activity	INFO	---	User Account Pruned	User account '%s' expired and pruned
1159	Security Services	General	---	WARNING	---	Visualization Control Expire Message	Received Alert: Your Visualization Control subscription has expired.
1160	System	Settings	Maintenance	DEBUG	---	Failed to Ping Remote Backup Server	Attempt to contact Remote backup server for upload approval failed
1161	System	Settings	Maintenance	DEBUG	---	Failed to Upload Remote Backup Server	Backup remote server did not approve upload Request
1169	WAN Acceleration	Local WXA Appliance	---	INFO	---	WXA Appliance Found	WAN Acceleration device %s found
1170	WAN Acceleration	Local WXA Appliance	---	ALERT	16001	WXA Appliance Operational	WAN Acceleration device %s is operational
1171	WAN Acceleration	Local WXA Appliance	---	ALERT	16002	WXA Appliance Not Operational	WAN Acceleration device %s is no longer operational
1172	WAN Acceleration	Local WXA Appliance	---	ALERT	16003	WXA Appliance Used	WAN Acceleration device %s is being used
1173	WAN Acceleration	Local WXA Appliance	---	ALERT	16004	WXA Appliance Not Used	WAN Acceleration device %s is no longer being used
1174	WAN Acceleration	Remote WXA Appliance	---	WARNING	16005	WXA Appliance Not Responding	Remote WAN Acceleration device stopped responding to probes

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1175	WAN Acceleration	Remote WXA Appliance	---	WARNING	16006	WXA Appliance Responding	Remote WAN Acceleration device started responding to probes
1176	WAN Acceleration	Local WXA Appliance	---	WARNING	16007	WAN Acceleration Software License Expired	Your WAN Acceleration Service subscription has expired.
1177	Network	DNS	Debug	NOTICE	---	Malformed DNS Packet	Malformed DNS packet detected
1178	Users	SSO Agent Authentication	User Activity	ALERT	---	High SSO Packet Count	A high percentage of the system packet buffers are held waiting for SSO
1179	Users	SSO Agent Authentication	User Activity	ALERT	---	High SSO User Connection	A user has a very high number of connections waiting for SSO
1180	Firewall Settings	Flood Protection	---	ALERT	---	DOS Protection on WAN Begin	DOS protection on WAN begins %s
1181	Firewall Settings	Flood Protection	---	WARNING	---	DOS Protection on WAN In-Progress	DOS protection on WAN %s
1182	Firewall Settings	Flood Protection	---	ALERT	---	DOS Protection on WAN Stopped	DOS protection on WAN %s
1183	VPN	VPN IKE	---	DEBUG	---	Deleting IPsec SA	Deleting IPsec SA. (Phase 2)
1184	Network	DHCP Server	---	WARNING	---	Invalid Scope Deleted	Delete invalid scope because port IP in the range of this DHCP scope.
1189	VPN	VPN IKE	---	WARNING	---	Network Mismatched	IKE Responder: Peer's proposed network does not match VPN Policy's Network
1190	Users	Radius Authentication	---	INFO	---	LDAP Mirror Added	Added new LDAP mirror user group: %s
1191	Users	Radius Authentication	---	INFO	---	LDAP Mirror Deleted	Deleted LDAP mirror user group: %s
1192	Users	Radius Authentication	---	INFO	---	LDAP Mirror Added Member	Added a new member to an LDAP mirror user group

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1193	Users	Radius Authentication	---	INFO	---	LDAP Mirror Deleted Member	Removed a member from an LDAP mirror user group
1194	High Availability	Monitoring	---	NOTICE	---	HA Monitor Probe Interface Mismatched	Monitoring probe out interface mismatch %s
1195	Security Services	Botnet Filter	---	WARNING	---	Botnet Filter Subscription Expired	Received Alert: Your Firewall Botnet Filter subscription has expired.
1196	System	Status	Maintenance	ALERT	---	Firewall Limit Reached	Product maximum entries reached - %s
1197	Network	NAT	---	NOTICE	---	Connection NAT Mapping	NAT Mapping
1198	Security Services	Geo-IP Filter	---	ALERT	---	Geo IP Initiator Blocked	Initiator from country blocked: %s
1199	Security Services	Geo-IP Filter	---	ALERT	---	Geo IP Responder Blocked	Responder from country blocked: %s
1200	Security Services	Botnet Filter	---	ALERT	---	Botnet Initiator Blocked	Suspected Botnet initiator blocked: %s
1201	Security Services	Botnet Filter	---	ALERT	---	Botnet Responder Blocked	Suspected Botnet responder blocked: %s
1202	Users	Authentication Access	User Activity	INFO	---	User Log Audit Trail	%s
1203	Users	Authentication Access	User Activity	WARNING	---	User Log Audit Trail Warning	%s
1204	Users	Authentication Access	User Activity	ERROR	---	User Log Audit Trail Error	%s
1205	High Availability	State	System Error	INFO	---	HA Peer MultiInterface Link Up	On HA peer firewall, Interface %s Link Is Up
1206	High Availability	State	System Error	INFO	---	HA Peer MultiInterface Link Down	On HA peer firewall, Interface %s Link Is Down
1207	High Availability	State	Maintenance	INFO	---	HA Peer Link Status Bad for Failover	Peer firewall has reduced link status. In event of failover, it will operate with limited capability.

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1208	High Availability	State	Maintenance	INFO	---	HA Peer Link Status Good for Failover	Peer firewall has equivalent link status. In event of failover, it will operate with equal capability.
1209	Network	MAC-IP Anti-Spoof	Attack	ALERT	---	MAC-IP Anti-Spoof Check Enforced For Hosts	MAC-IP Anti-spoof check enforced for hosts
1210	Network	MAC-IP Anti-Spoof	Attack	ALERT	---	MAC-IP Anti-Spoof Cache Not Found For Router	MAC-IP Anti-spoof cache not found for this router
1211	Network	MAC-IP Anti-Spoof	Attack	ALERT	---	MAC-IP Anti-Spoof Cache Not Router	MAC-IP Anti-spoof cache found, but it is not a router
1212	Network	MAC-IP Anti-Spoof	Attack	ALERT	---	MAC-IP Anti-Spoof Cache Blacklisted Device	MAC-IP Anti-spoof cache found, but it is blacklisted device
1213	Firewall Settings	Flood Protection	Attack	ALERT	---	UDP Flood Detected	Possible UDP flood attack detected
1214	Firewall Settings	Flood Protection	Attack	ALERT	---	ICMP Flood Detected	Possible ICMP flood attack detected
1215	VPN	DHCP Relay	Debug	INFO	---	Remote: DHCP Inform	DHCP INFORM received from remote device
1216	VPN	VPN IKE	---	INFO	---	IP Pool of VPN Policy is Full	IP Pool of the VPN Policy is Full
1217	VPN	VPN IKE	---	DEBUG	---	IP Pool of VPN Policy Not Configured	IP Pool of the VPN Policy is Not Configured
1218	VPN	VPN IKE	---	INFO	---	Mobile IKE Update Peer Gateway IP	MOBIKE: Update Peer Gateway IP
1219	VPN	VPN IKE	---	INFO	---	IP Address Allocated For Client	IP Address is allocated for Client
1220	System	SNMP	---	NOTICE	---	Invalid SNMPv3 Packet	Invalid SNMP packet
1221	System	SNMP	---	NOTICE	---	Invalid SNMPv3 Engine ID	Invalid SNMPv3 engineID

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1222	System	SNMP	---	NOTICE	---	Invalid SNMPv3 User	Invalid SNMPv3 User
1223	System	SNMP	---	NOTICE	---	Invalid SNMPv3 Time Window	Invalid SNMPv3 Time Window
1225	System	SNMP	---	DEBUG	---	SNMP Packet Drop	SNMP Packet Dropped
1226	Network	Network Access	---	INFO	---	HTTPS Handshake	HTTPS Handshake: %s
1227	Users	Authentication Access	User Activity	WARNING	---	Guest Traffic Quota Exceeded	User Traffic Quota Exceeded
1229	Wireless	Wireless Access	TCP | UDP | ICMP	WARNING	---	Wireless Advance IDP	Packet dropped by wireless Advanced IDP
1230	System	Time	---	NOTICE	---	NTP Update Failure	Failed on updating time from NTP server
1231	System	Time	---	NOTICE	---	NTP Update Successful	Time update from NTP server was successful
1232	System	Time	---	NOTICE	---	NTP Request Sent	NTP Request sent
1233	Firewall Settings	Multicast	Debug	NOTICE	---	Link-Local/Multicast IPv6 Packet	Unhandled link-local or multicast IPv6 packet dropped
1235	Network	Network Access	---	INFO	---	Packet Allowed	Packet allowed: %s
1236	Security Services	RBL Filter	---	DEBUG	---	RBL Received Blacklist Directive	Received Blacklisted Directive from - %s
1237	Security Services	RBL Filter	---	DEBUG	---	RBL Not Blacklisted by Domain	Not Blacklisted by domain - %s
1238	Security Services	RBL Filter	---	DEBUG	---	RBL No Response to Domain	No DNS response to domain - %s
1239	Security Services	RBL Filter	---	DEBUG	---	RBL DNS Response With Error Reply Code	RBL DNS server responded with error code - %s
1240	VoIP	Anomaly	---	INFO	---	Endpoint Anomaly Detected	%s
1241	VoIP	Anomaly	---	INFO	---	Endpoint Anomaly Lockout Started	%s

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1242	VoIP	Anomaly	---	INFO	---	Endpoint Anomaly Lockout Ended	%s
1243	Users	Authentication Access	User Activity	INFO	---	Sending OTP Failed	User login Failed - An error has occurred while sending your one-time password
1244	Users	Radius Authentication	---	WARNING	---	LDAP Mirror User Group Add Failure	Failed to add an LDAP mirror user group
1245	Users	Radius Authentication	---	WARNING	---	LDAP Mirror User Group Member Add Failure	Failed to add a member to an LDAP mirror user group
1246	Users	Radius Authentication	---	WARNING	---	LDAP User Group Nesting Not Being Mirrored	An LDAP user group nesting is not being mirrored
1252	VPN	VPN IKE	---	INFO	---	IPv6 IPsec Tunnel Mode Mismatch	IPv6 VPN only support IKEv2 mode
1253	Network	IPv6 Tunneling	---	NOTICE	---	IPv6 Tunnel Dropped	IPv6 Tunnel packet dropped
1254	Network	ICMP	---	INFO	---	LAN ICMPv6 Deny	ICMPv6 packet from LAN dropped
1255	Network	ICMP	---	INFO	---	LAN ICMPv6 Allow	ICMPv6 packet from LAN allowed
1256	Network	ICMP	---	INFO	---	ICMPv6 Allow	ICMPv6 packet allowed
1257	Network	ICMP	---	INFO	---	ICMPv6 Packets Dropped	ICMPv6 packet dropped due to policy
1259	Network	DHCPv6 Server	---	WARNING	---	DHCPv6 Lease File Corrupt	DHCPv6 lease file in the storage is corrupted; read failed
1260	Network	DHCPv6 Server	---	WARNING	---	Failed To Write DHCPv6 Leases to Storage	Failed to write DHCPv6 leases to storage
1261	Network	DHCPv6 Server	---	INFO	---	DHCPv6 Leases Written to Storage	DHCPv6 leases written to storage
1263	System	AppFlow	Maintenance	INFO	---	AppFlow Server	AppFlow Server Event

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1264	WAN Acceleration	Remote WXA Appliance	---	WARNING	---	WXA Configuration	WLAN HTTP traffic not being sent to WXA WebCache; zone conflict
1265	Wireless	SonicPoint	---	WARNING	---	SonicPoint Association Post Request Failed	SonicPoint association request to License Manager failed: %s
1266	Wireless	SonicPoint	---	INFO	---	SonicPoint Association Post Request Success	SonicPoint association posted successfully to License Manager
1267	VPN	VPN IPsec	User Activity	DEBUG	---	Phase2 Dead Peer Detection	%s
1268	System	Settings	---	NOTICE	---	Firmware Update Failed	Firmware Update Failed
1269	System	Settings	---	NOTICE	---	Firmware Update Succeeded	Firmware Update Succeeded %s
1270	Security Services	Crypto Test	Maintenance	INFO	---	DH Test Success	Crypto DH test success
1271	Security Services	Crypto Test	Maintenance	INFO	---	HMAC-MD5 Test Success	Crypto Hmac-MD5 test success
1272	Security Services	Crypto Test	Maintenance	INFO	---	Hardware DES Test Success	Crypto hardware DES test success
1274	Security Services	Crypto Test	---	INFO	---	DRNG KAT Test Success	Crypto SHA1 based DRNG KAT test success
1275	Security Services	Crypto Test	Maintenance	INFO	---	HMAC-SHA1 Test Success	Crypto Hmac-Sha1 test success
1276	Security Services	Crypto Test	Maintenance	INFO	---	Hardware 3DES Test Success	Crypto hardware 3DES test success
1277	Security Services	Crypto Test	Maintenance	INFO	---	DES Test Success	Crypto DES test success
1278	Security Services	Crypto Test	Maintenance	ERROR	---	AES CBC Test Failed	Crypto AES CBC test failed
1279	Security Services	Crypto Test	Maintenance	INFO	---	AES CBC Test Success	Crypto AES CBC test success
1280	Security Services	Crypto Test	Maintenance	INFO	---	DRBG Test Success	Crypto DRBG test success
1281	Security Services	Crypto Test	Maintenance	ERROR	---	DRBG Test Failed	Crypto DRBG test failed
1282	Security Services	Crypto Test	Maintenance	INFO	---	HMAC-SHA256 Test Success	Crypto Hmac-Sha256 test success

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1283	Security Services	Crypto Test	Maintenance	ERROR	---	HMAC-SHA256 Test Failed	Crypto Hmac-Sha256 test failed
1284	Security Services	Crypto Test	Maintenance	INFO	---	RSA Test Success	Crypto RSA test success
1285	Security Services	Crypto Test	Maintenance	INFO	---	SHA1 Test Success	Crypto Sha1 test success
1286	Security Services	Crypto Test	Maintenance	INFO	---	SHA256 Test Success	Crypto Sha256 test success
1287	Security Services	Crypto Test	Maintenance	ERROR	---	SHA256 Test Failed	Crypto Sha256 test failed
1288	Security Services	Crypto Test	Maintenance	INFO	---	Hardware AES Test Success	Crypto hardware AES test success
1289	Security Services	Crypto Test	Maintenance	INFO	---	Hardware DES-SHA Test Success	Crypto hardware DES with SHA test success
1290	Security Services	Crypto Test	Maintenance	INFO	---	Hardware 3DES-SHA Test Success	Crypto hardware 3DES with SHA test success
1299	Security Services	Crypto Test	Maintenance	ALERT	---	Self Test Passed	Ndpp SelfTest write/read encrypt/decrypt successsfully
1300	Security Services	Crypto Test	Maintenance	ALERT	---	Self Test Failed	Ndpp SelfTest write/read encrypt/decrypt failure
1301	Network	IP	Debug	ALERT	---	IPv6 Packet Dropped With Reserved IP	Source or Destination IPv6 address is reserved by RFC 4291. Packet is dropped
1302	Network	IP	Debug	ALERT	---	IPv6 Packet Dropped With Unspecified Destination IP	Destination IPv6 address is unspecified. Packet is dropped
1303	Network	IP	Debug	ALERT	---	IPv6 Packet Dropped With Unspecified Source IP	Source IPv6 address is unspecified but this packet is not Neighbor Solicitation message for DAD. Packet is dropped
1304	Network	Network Access	Debug	ALERT	---	Packet Dropped Due to NDPP Rules	Packet is dropped due to NDPP rules.

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1305	VPN	VPN IKE	User Activity	WARNING	---	IKE Responder: No VPN Policy found for IKE ID	IKE Responder : VPN Policy for IKE ID not found
1306	VPN	VPN IKE	User Activity	WARNING	---	IKE Responder: No VPN Policy found for Gateway	IKE Responder : VPN Policy for gateway address not found
1307	VPN	VPN IKE	User Activity	WARNING	---	IKE Initiator: No VPN Policy found for IKE ID	IKE Initiator : VPN Policy for IKE ID not found
1308	VPN	VPN IKE	User Activity	WARNING	---	IKE Initiator: No VPN Policy found for Gateway	IKE Initiator : VPN Policy for gateway address not found
1309	High Availability	General	---	WARNING	---	HA Association Posted Failed	HA association request to License Manager failed: %s
1310	High Availability	General	---	INFO	---	HA Association Posted Success	HA association posted successfully to License Manager
1311	Network	DHCP Server	---	NOTICE	---	DHCP Resources of this Pool Ran Out	DHCP Server: Resources of this pool ran out. Client Info: %s
1312	VPN	VPN IKEv2	---	INFO	---	IP Version of Traffic Selector Mismatch	IKEv2: Peer's IP Version of Traffic Selector does not match with ours
1313	Network	NAT Policy	---	INFO	---	NAT Policy Add	NAT policy added
1314	Network	NAT Policy	---	INFO	---	NAT Policy Modify	NAT policy modified
1315	Network	NAT Policy	---	INFO	---	NAT Policy Delete	NAT policy deleted
1316	Network	ARP	---	ALERT	---	ARP Attack Detected	Possible ARP attack from MAC address %s
1324	VPN	VPN IKEv2	User Activity	INFO	---	Received Dead Peer Detection Request	IKEv2 Received Dead Peer Detection Request
1325	VPN	VPN IKEv2	User Activity	INFO	---	Received Dead Peer Detection Response	IKEv2 Received Dead Peer Detection Response
1326	VPN	VPN IKEv2	User Activity	INFO	---	Send Dead Peer Detection Request	IKEv2 Send Dead Peer Detection Request

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1327	VPN	VPN IKEv2	User Activity	INFO	---	Send Dead Peer Detection Response	IKEv2 Send Dead Peer Detection Response
1328	VPN	VPN IKEv2	User Activity	INFO	---	Send Invalid SPI Request	IKEv2 Send Invalid SPI Request
1329	VPN	VPN IKEv2	User Activity	INFO	---	Received Invalid SPI Request	IKEv2 Received Invalid SPI Request
1330	VPN	VPN IKEv2	User Activity	INFO	---	Send Invalid SPI Response	IKEv2 Send Invalid SPI Response
1331	VPN	VPN IKEv2	User Activity	INFO	---	Received Invalid SPI Response	IKEv2 Received Invalid SPI Response
1332	System	Status	Maintenance	ALERT	---	NDPP Mode Change	NDPP mode is changed to %s
1333	Users	Authentication Access	User Activity	INFO	---	Create a User	%s
1334	Users	Authentication Access	User Activity	INFO	---	Edit a User	%s
1335	Users	Authentication Access	User Activity	INFO	---	Delete a User	%s
1336	System	Settings	---	INFO	---	Change Certification	Certification %s
1337	System	Settings	---	INFO	---	User Password Changed by Administrators	%s
1338	System	Settings	---	INFO	---	User Change Password	User %s password is changed
1339	System	Settings	---	INFO	---	Change Password Rule	Password rule %s is changed
1340	System	Settings	---	INFO	---	Change User Inactive time out	User Inactive timeout is changed to %s
1341	Users	Authentication Access	User Activity	INFO	---	Edit Customize Login Pages	%s
1342	Users	Authentication Access	User Activity	INFO	---	Edit user lockout params	Update administrator/user lockout params - %s
1343	VPN	VPN IPsec	User Activity	INFO	---	VPN Policy Enabled/Disabled	VPN Policy %s
1344	Network	Interfaces	System Error	INFO	---	Interface Configure	%s
1345	Security Services	Crypto Test	---	INFO	---	SHA384 Test Success	Crypto Sha384 test success

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1346	Security Services	Crypto Test	---	ERROR	---	SHA384 Test Failed	Crypto Sha384 test failed
1347	Security Services	Crypto Test	---	INFO	---	SHA512 Test Success	Crypto Sha512 test success
1348	Security Services	Crypto Test	---	ERROR	---	SHA512 Test Failed	Crypto Sha512 test failed
1349	Security Services	Crypto Test	---	INFO	---	Ikev1 Test Success	Crypto Ikev1 test success
1350	Security Services	Crypto Test	---	ERROR	---	Ikev1 Test Failed	Crypto Ikev1 test failed
1351	Security Services	Crypto Test	---	INFO	---	Ikev2 Test Success	Crypto Ikev2 test success
1352	Security Services	Crypto Test	---	ERROR	---	Ikev2 Test Failed	Crypto Ikev2 test failed
1353	Security Services	Crypto Test	---	INFO	---	SSH Test Success	Crypto SSH test success
1354	Security Services	Crypto Test	---	ERROR	---	SSH Test Failed	Crypto SSH test failed
1355	Security Services	Crypto Test	---	INFO	---	SNMP Test Success	Crypto SNMP test success
1356	Security Services	Crypto Test	---	ERROR	---	SNMP Test Failed	Crypto SNMP test failed
1357	Security Services	Crypto Test	---	INFO	---	TLS 1.0/1.1/1.2 Test Success	Crypto TLS 1.0/1.1/1.2 test success
1358	Security Services	Crypto Test	---	ERROR	---	TLS 1.0/1.1/1.2 Test Failed	Crypto TLS 1.0/1.1/1.2 test failed
1359	Security Services	Crypto Test	---	INFO	---	HMAC-SHA384 Test Success	Crypto Hmac-Sha384 test success
1360	Security Services	Crypto Test	---	ERROR	---	HMAC-SHA384 Test Failed	Crypto Hmac-Sha384 test failed
1361	Security Services	Crypto Test	---	INFO	---	HMAC-SHA512 Test Success	Crypto Hmac-Sha512 test success
1362	Security Services	Crypto Test	---	ERROR	---	HMAC-SHA512 Test Failed	Crypto Hmac-Sha512 test failed
1363	Wireless	WLAN	802.11b Management	ALERT	---	WLAN 802.11 Flood	Wireless Flood Attack
1364	VPN	VPN PKI	---	WARNING	---	Cert Payload processing failed	Cert Payload processing failed

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1365	Security Services	DPI-SSL	---	NOTICE	---	DPI-SSL Memory Check	DPI-SSL: %s
1366	Firewall Settings	Flood Protection	Attack	ALERT	---	TCP-Flooding Machine Blacklisted	TCP-Flooding machine %s blacklisted
1367	Firewall Settings	Flood Protection	Attack	WARNING	---	TCP Flood Blacklist Continues	TCP Flood Blacklist on IF %s continues
1368	Firewall Settings	Flood Protection	Attack	ALERT	---	Machine Removed From TCP Flood Blacklist	Machine %s removed from TCP flood blacklist
1369	Firewall Settings	Flood Protection	Attack	ALERT	---	Possible TCP Flood	Possible TCP Flood on IF %s
1370	Firewall Settings	Flood Protection	Attack	ALERT	---	Possible TCP Flood Ceased	Possible TCP Flood on IF %s has ceased
1371	Firewall Settings	Flood Protection	---	WARNING	---	Possible TCP Flood Continues	Possible TCP Flood on IF %s continues
1372	Users	Radius Authentication	---	WARNING	---	LDAP Mirroring Overflow	LDAP mirroring overflow: too many user groups
1373	Security Services	Attacks	Attack	ALERT	---	IPv6 fragment size is less than minimum (<1280)	IPv6 fragment dropped, invalid length (<1280 Bytes)
1374	Security Services	Attacks	Attack	ALERT	---	IP Reassembly : Incomplete IGMP fragment	IGMP packet dropped, incomplete fragments
1375	Security Services	Attacks	Attack	ALERT	---	UDP fragmented datagram is too big (>65535)	UDP fragment dropped, exceeds maximum IP datagram size (>65535)
1376	Security Services	Attacks	Attack	ALERT	---	Nestea/Teardrop Attack	Nestea/Teardrop attack dropped
1377	Anti-Spam	General	---	ALERT	---	SHLO verification failed	SHLO verification failed with this client IP - %s
1378	Anti-Spam	General	---	ALERT	---	SHLO replay attack	Possible replay attack with this client IP - %s
1379	WAN Acceleration	Local WXA Appliance	---	WARNING	---	WXA association request failed	WXA association request to License Manager failed: %s

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1380	WAN Acceleration	Local WXA Appliance	---	INFO	---	WXA association succeeded	WXA association posted successfully to License Manager
1381	Security Services	General	---	WARNING	15003	Application Control Expiration Message	Received App-Control Alert: Your Application Control subscription has expired.
1382	Log	Configuration Auditing	User Activity	INFO	5609	Configuration Change Succeeded	Configuration succeeded: %s
1383	Log	Configuration Auditing	User Activity	INFO	5610	Configuration Change Failed	Configuration failed: %s
1384	Network	TCP	Debug	DEBUG	---	Invalid TCP Timestamps Option Length	TCP packet received with invalid Timestamps option length; TCP packet dropped
1385	Network	TCP	Debug	DEBUG	---	TCP Sequence Number Wrapped	TCP packet received with wrapped sequence number; TCP packet dropped
1387	Security Services	Attacks	Attack	ALERT	---	TCP Null Flag Attack	TCP Null Flag dropped
1388	VPN	VPN IPsec	Attack	DEBUG	---	Vpn Decryption Failed	IPSec VPN Decryption Failed
1389	Security Services	Client CF	Maintenance	INFO	---	Client CF Access Without Agent	Access attempt from host without Client CF agent installed
1390	Security Services	Client CF	Maintenance	INFO	---	Client CF Agent Out of Date	Client CF agent out-of-date on host
1391	Security Services	General	Attack	DEBUG	---	Raw Data	Packet Data
1392	System	Restart	Maintenance	ALERT	5243	SonicOS up	SonicOS up:%s
1393	System	Restart	Maintenance	ALERT	5244	SonicOS down	SonicOS down:%s
1394	WAN Acceleration	Local WXA Appliance	---	ERROR	---	Startup Failure	WXA Startup Failure - %s
1395	WAN Acceleration	Local WXA Appliance	---	WARNING	---	Get Failure	WXA Get Failure - %s
1396	WAN Acceleration	Local WXA Appliance	---	NOTICE	---	Parse Failure	WXA Parse Failure - %s

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1397	WAN Acceleration	Local WXA Appliance	---	NOTICE	---	Register Failure	WXA Register Failure - %s
1398	WAN Acceleration	Local WXA Appliance	---	NOTICE	---	Unregister Failure	WXA Unregister Failure - %s
1399	WAN Acceleration	Local WXA Appliance	---	NOTICE	---	Probe Failure	WXA Probe Failure - %s
1400	WAN Acceleration	Local WXA Appliance	---	ALERT	---	Create Failure	WXA Create Failure - %s
1401	WAN Acceleration	Local WXA Appliance	---	WARNING	---	Set Failure	WXA Set Failure - %s
1402	WAN Acceleration	Local WXA Appliance	---	ERROR	---	Delete Failure	WXA Delete Failure - %s
1403	WAN Acceleration	Local WXA Appliance	---	INFO	---	Enable Service	WXA Enable - %s
1404	WAN Acceleration	Local WXA Appliance	---	INFO	---	Disable Service	WXA Disable - %s
1405	WAN Acceleration	Local WXA Appliance	---	WARNING	---	Request Failure	WXA Request Failure - %s
1406	Network	DHCPv6 Client	---	INFO	---	General DHCPv6 Client Info	General DHCPv6 Client Information [%s]
1407	Network	DHCPv6 Client	---	DEBUG	---	DHCPv6 Client Send Message	DHCPv6 Client sent message [%s]
1408	Network	DHCPv6 Client	---	DEBUG	---	DHCPv6 Client Get Message	DHCPv6 Client received message [%s]
1409	Network	DHCPv6 Client	---	DEBUG	---	DHCPv6 Client DAD	DHCPv6 Client Duplicate Address Detection [%s]
1410	Network	DHCPv6 Client	---	DEBUG	---	DHCPv6 Client Timeout	DHCPv6 Client waiting reply timeout [%s]
1411	Network	DHCPv6 Client	---	DEBUG	---	DHCPv6 Client Get RA Flags	Router Advertisement flags [%s]
1412	Network	DHCPv6 Client	---	INFO	---	DHCPv6 Client Get New Lease	DHCPv6 Client got a new lease [%s]

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1413	Network	DHCPv6 Client	---	INFO	---	DHCPv6 Client Release Lease	DHCPv6 Client released lease [%s]
1414	Network	DHCPv6 Server	---	INFO	---	DHCPv6 Server Assign Lease	DHCPv6 Server assigned lease %s
1415	Network	DHCPv6 Server	---	INFO	---	DHCPv6 Server Release Lease	DHCPv6 Server released lease %s
1416	Network	DHCPv6 Server	---	INFO	---	DHCPv6 Server Receive Decline	DHCPv6 Server received DHCPv6 Decline from client %s
1417	Network	DHCPv6 Server	---	WARNING	---	DHCPv6 Server Resources of this Pool Ran Out	DHCPv6 Server: Resources of this pool ran out. Client Info: %s
1418	Network	DHCPv6 Server	---	INFO	---	Add DHCPv6 Server Scope	DHCPv6 Server: Add a new scope (%s)
1419	Network	DHCPv6 Server	---	INFO	---	Delete DHCPv6 Server Scope	DHCPv6 Server: Delete scope (%s)
1420	Network	DHCPv6 Server	---	DEBUG	---	DHCPv6 Server Get Message	DHCPv6 Server received message (%s)
1421	Network	DHCPv6 Server	---	DEBUG	---	DHCPv6 Server Send Message	DHCPv6 Server sent message (%s)
1422	Network	Interfaces	---	WARNING	---	IPv6 Address Conflict	IPv6 address conflict detected from Ethernet address %s
1423	Network	Interfaces	---	WARNING	---	Exceed Max NDP Size	Dropped NDP message:%s
1424	Security Services	DPI-SSL	---	ALERT	14601	DPI-SSL Connection Check	DPI-SSL Connection: %s
1426	Wireless	SonicPoint/SonicWave	---	WARNING	13603	SonicPoint/SonicWave Unexpected Reboot	%s unexpected reboot. Please check whether input power is adequate and ethernet connection is secured. (SonicWave/SonicPoint AC/NDR requires 802.3at PoE+)
1428	SSL VPN	General	---	DEBUG	---	Not in use	%s

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1429	Network	IP	Debug	ALERT	---	IPv6 Packet Dropped With Site Local IP	Source or Destination IPv6 address is site-local unicast address. Packet is dropped
1430	Network	IP	Debug	INFO	---	IPv6 Packet with Ext Header	IPv6 Packet with extension header received
1431	Network	ICMP	---	INFO	---	ICMPv6 Packets Received	ICMPv6 packet received
1432	System	Settings	---	INFO	---	Configuration Change	Configuration changed: %s
1433	Network	ICMP	---	NOTICE	---	NDP Packets Dropped	%s
1434	Network	Interfaces	---	NOTICE	---	Group-port Link Up	Interface %s up
1435	Network	Interfaces	---	ERROR	---	Group-port Link Down	Interface %s down
1436	Network	NAT	Debug	DEBUG	---	NAT Policy Dropped Packets	Packet dropped by NAT Policy, reason: %s
1437	Network	Default Address Objects	---	WARNING	---	Delete Default AO Failed	%s
1438	VPN	VPN PKI	---	INFO	---	CA Cert Added	CA Certificate %s Added.
1439	VPN	VPN PKI	---	NOTICE	---	Local Cert Added	Local Certificate %s Added.
1440	VPN	VPN PKI	---	NOTICE	---	CA Cert Deleted	CA Certificate %s Deleted.
1441	VPN	VPN PKI	---	NOTICE	---	Local Cert Deleted	Local Certificate %s Deleted.
1442	System	Hardware	System Environment	ALERT	---	USB Over Current	USB Over Current
1443	Firewall Settings	Flood Protection	Debug	WARNING	---	Control Plane Flood Protection Threshold Exceeded	Control Plane Flood Protection Threshold Exceeded: %s
1444	High Availability	State	Maintenance	ERROR	---	HA Reboot	Reboot occured (Reason :%s)
1445	WAN Acceleratio n	Local WXA Appliance	---	WARNING	---	Connection Exceed	WXA Warning - %s

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1446	Network	DHCP Server	---	NOTICE	---	Mask 31-Bit Scope Deleted	Delete invalid scope with mask of 31 bits [%s]
1447	Network	UDP	UDP	NOTICE	---	UDPv6 Packets Dropped	UDPv6 packet dropped
1448	Firewall Settings	Checksum Enforcement	UDP	NOTICE	---	UDPv6 Checksum Error	UDPv6 checksum error; packet dropped
1449	Firewall Settings	Checksum Enforcement	UDP	NOTICE	---	ICMPv6 Checksum Error	ICMPv6 checksum error; packet dropped
1450	Firewall Settings	Flood Protection	Attack	ALERT	---	UDPv6 Flood Detected	Possible UDPv6 flood attack detected
1451	Firewall Settings	Flood Protection	Attack	ALERT	---	ICMPv6 Flood Detected	Possible ICMPv6 flood attack detected
1452	Firewall Settings	Flood Protection	Attack	ALERT	---	Half Open TCP Connection Threshold Exceeded	Too many half-open TCP connections
1453	Network	Switch Network	Debug	INFO	---	Extended Switch Add	%s
1454	Network	Switch Network	Debug	INFO	---	Extended Switch Remove	%s
1455	Network	Switch Network	Debug	INFO	---	Extended Switch Port Speed Change	Extended Switch Port Status Change : %s
1456	Network	Switch Network	Debug	INFO	---	Extended Switch Port Duplex Mode Change	Extended Switch Port Status Change : %s
1457	Network	Switch Network	Debug	INFO	---	Extended Switch Port Link Status Change	Extended Switch Port Status Change : %s
1458	Network	ICMP	---	NOTICE	---	NDP Packets Received	%s
1459	Security Services	GAV	Maintenance	NOTICE	---	Capture ATP File Transfer Attempt	Gateway Anti-Virus Status: %s
1460	Security Services	GAV	Maintenance	NOTICE	---	Capture ATP File Transfer Result	Gateway Anti-Virus Status: %s
1461	Security Services	Content Filter	---	NOTICE	---	CFS Notice	CFS Notice: %s

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1462	Security Services	GAV	---	NOTICE	---	AV Gateway Inform	Gateway Anti-Virus Inform: %s
1463	Security Services	DPI-SSL	Connection Traffic	INFO	---	DPI-SSL Inspection Cleaned-up	DPI-SSL Inspection Cleaned-up
1471	Security Services	Attacks	Attack	ALERT	---	External IDS	External IDS: %s
1472	Log	General	System Error	INFO	---	Logs at 75% of maximum	Total current log entries is at 75% of maximum
1473	Firewall Settings	Advanced	Debug	INFO	---	Drop Source IP Subnet Broadcast	Source IP is a subnet broadcast address
1474	Security Services	Geo-IP Filter	---	ALERT	---	Custom Geo IP Initiator Blocked	Initiator from country blocked: %s, Source: Custom List
1475	Security Services	Geo-IP Filter	---	ALERT	---	Custom Geo IP Responder Blocked	Responder from country blocked: %s, Source: Custom List
1476	Security Services	Botnet Filter	---	ALERT	---	Custom Botnet Initiator Blocked	Suspected Botnet initiator blocked: %s, Source: Custom List
1477	Security Services	Botnet Filter	---	ALERT	---	Custom Botnet Responder Blocked	Suspected Botnet responder blocked: %s, Source: Custom List
1478	System	Vendor Name Resolution	Debug	INFO	---	Vendor Database Download Success	Vendor database downloaded successfully
1479	System	Vendor Name Resolution	Debug	INFO	---	Vendor Database Download Failed	Vendor database download failed
1480	Network	DNS	Maintenance	INFO	---	DNS Resolve Success	Success in DNS resolve
1481	Network	DNS Proxy	Maintenance	INFO	---	DNS Proxy Packet Send	Send DNS proxy query
1482	Network	DNS Proxy	Maintenance	INFO	---	DNS Proxy Packet Received	Receive DNS proxy reply
1483	Network	DNS Proxy	Maintenance	INFO	---	DNS Proxy Request Acked by Cache	DNS respond directly by firewall
1484	Network	DNS Proxy	Maintenance	INFO	---	DNS Proxy Add Cache	Add DNS cache

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1485	Network	DNS Proxy	Maintenance	INFO	---	DNS Proxy Delete Cache	Remove DNS cache
1486	Network	DNS Proxy	Maintenance	NOTICE	---	DNS Proxy Request Packet Drop	Drop DNS query packet
1487	Network	DNS Proxy	Maintenance	NOTICE	---	DNS Proxy Response Packet Drop	Drop DNS response packet
1490	Network	Network Access	User Activity	NOTICE	---	HTTP redirected	HTTP connection redirected
1491	Network	Network Access	User Activity	NOTICE	---	HTTPS redirected	HTTPS connection redirected
1492	Security Services	Crypto Test	Maintenance	INFO	---	ECDSA Test Success	Crypto ECDSA test success
1493	Security Services	Crypto Test	Maintenance	ERROR	---	ECDSA Test Failed	Crypto ECDSA test failed
1494	System	Settings	---	INFO	---	System Setting Exported	System Setting Exported
1495	System	Status	Maintenance	INFO	---	Firewall was Rebooted by Setting Import	Firewall was rebooted by setting import at %s
1496	System	Status	Maintenance	INFO	---	Firewall was Rebooted by Firmware	Firewall was rebooted by %s
1497	Network	Network Access	---	DEBUG	---	Packet Dissection Check	Packet Dissection Check -- %s
1506	Wireless	WLAN	802.11b Management	INFO	---	BandOver Event	BandOver event
1507	Network	IPv6 MAC-IP Anti-Spoof	Attack	ALERT	---	IPv6 MAC-IP Anti-Spoof Check Enforced For Hosts	IPv6 MAC-IP Anti-spoof check enforced for hosts
1508	Network	IPv6 MAC-IP Anti-Spoof	Attack	ALERT	---	IPv6 MAC-IP Anti-Spoof Cache Not Found For Router	IPv6 MAC-IP Anti-spoof cache not found for this router
1509	Network	IPv6 MAC-IP Anti-Spoof	Attack	ALERT	---	IPv6 MAC-IP Anti-Spoof Cache Not Router	IPv6 MAC-IP Anti-spoof cache found, but it is not a router

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1510	Network	IPv6 MAC-IP Anti-Spoof	Attack	ALERT	---	IPv6 MAC-IP Anti-Spoof Cache Blacklisted Device	IPv6 MAC-IP Anti-spoof cache found, but it is blacklisted device
1511	System	Cloud Backup	---	INFO	---	Automatic Cloud Backup Successful	%s
1512	System	Cloud Backup	---	INFO	---	Automatic Cloud Backup Failed	%s
1513	System	Cloud Backup	---	INFO	---	Manual Cloud Backup Successful	%s
1514	System	Cloud Backup	---	INFO	---	Manual Cloud Backup Failed	%s
1515	System	Cloud Backup	---	INFO	---	Delete Cloud Backup Successful	%s
1516	System	Cloud Backup	---	INFO	---	Delete Cloud Backup Failed	%s
1517	Users	Authentication Access	User Activity	INFO	---	User Name Invalid Symbol	User name invalid symbol: %s
1518	Security Services	Botnet Filter	---	ALERT	---	Botnet Initiator Blocked By Dynamic List	Suspected Botnet initiator blocked: %s, Source: Dynamic List
1519	Security Services	Botnet Filter	---	ALERT	---	Botnet Responder Blocked By Dynamic List	Suspected Botnet responder blocked: %s, Source: Dynamic List
1520	System	Settings	Maintenance	INFO	---	E-mail SFR Success	Successfully sent SFR file by E-mail
1521	System	Settings	Maintenance	INFO	---	E-mail SFR Failed	Failed to send SFR file by E-mail, %s
1522	Wireless	SonicPoint/SonicWave	---	INFO	---	SonicPoint 3G/4G/LTE WWAN Status	%s 3G/4G/LTE WWAN Status
1523	VPN	VPN PKI	---	INFO	---	Invalid Certificate Imported	Invalid certificate is imported: %s
1524	Wireless	SonicPoint/SonicWave	---	ALERT	---	SonicWave POE warning	%s POE Warning
1525	Wireless	SonicPoint/SonicWave	---	WARNING	---	SonicWave License Expired	SonicWave %s

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1526	Wireless	SonicPoint/SonicWave	---	WARNING	---	SonicWave License Invalid	SonicWave %s
1527	Security Services	Crypto Test	Maintenance	ERROR	---	AES GCM Test Failed	Crypto AES GCM test failed
1528	Security Services	Crypto Test	Maintenance	INFO	---	AES GCM Test Success	Crypto AES GCM test success
1529	Log	AWS	System Error	DEBUG	---	AWS Log export Failed	Failed export of logs to AWS: %s
1530	Log	AWS	System Error	DEBUG	---	AWS Log export Success	Logs successfully exported to AWS: %s
1531	Log	AWS	System Error	DEBUG	---	AWS AddressObject synchronization	AWS AddressObject Synchronization: %s
1532	Security Services	DPI-SSH	Users	ALERT	---	DPI-SSH PF User	DPI SSH Port Forward Alert: %s
1533	Security Services	DPI-SSH	---	INFO	---	DPI-SSH	DPI-SSH: %s
1534	Security Services	DPI-SSH	---	ALERT	---	DPI-SSH Connection Check	DPI-SSH Connection: %s
1535	Network	DNS	Maintenance	NOTICE	---	Receive DNS Reply With Truncated Flag Set	Truncated flag is set
1536	Network	DNS	Maintenance	INFO	---	DNS Query Over TCP Send	Send DNS query over TCP
1537	Network	DNS	Maintenance	INFO	---	DNS Response Over TCP Receive	Receive DNS response over TCP
1538	Network	DNS	Maintenance	INFO	---	DNS Response Over TCP Timeout	DNS response over TCP Timeout
1542	Security Services	Crypto Test	Maintenance	INFO	---	DSA Test Success	Crypto DSA test success
1543	Security Services	Crypto Test	Maintenance	ERROR	---	DSA Test Failed	Crypto DSA test failed
1544	System	Storage Module	---	WARNING	---	Storage Module Association Posted Failed	%s
1545	System	Storage Module	---	INFO	---	Storage Module Association Posted Success	%s

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1547	VPN	VPN IPsec	TCP | UDP | ICMP	INFO	---	Fragmented IPsec packet DF bit set dropped	Fragmented IPsec packet DF bit set dropped
1549	Network	DNS Security	Maintenance	NOTICE	---	Drop DNS Sinkhole Forged IP Packets	Drop DNS Sinkhole Forged IP Packets
1550	Network	DNS Security	Maintenance	NOTICE	---	Drop Hit DNS Sinkhole Malicious Database Packets	Drop Hit DNS Sinkhole Malicious Database Packets
1551	Wireless	WLAN	802.11b Management	INFO	---	RSSI Event	RSSI event
1552	Users	Tacacs Authentication	User Activity	INFO	---	User Login Failed	User login denied - TACACS+ authentication failure
1553	Users	Tacacs Authentication	User Activity	WARNING	---	User Login Timeout	User login denied - TACACS+ server Timeout
1554	Users	Tacacs Authentication	User Activity	WARNING	---	User Login Error	User login denied - TACACS+ configuration error
1555	Users	Tacacs Authentication	User Activity	WARNING	---	TACACS+ Communication Problem	User login denied - TACACS+ communication problem
1556	Users	Tacacs Authentication	User Activity	WARNING	---	TACACS+ Server Name Resolution Failed	User login denied - TACACS+ server name resolution failed
1557	Users	Authentication Access	User Activity	INFO	---	TACACS+ User Cannot Use One Time Password	TACACS+ user cannot use One Time Password - no mail address set for equivalent local user
1558	Log	General	Debug	ERROR	---	Log DB Deleted	Log DB Deleted due to data corruption
1559	Security Services	Next-Gen Anti-Virus	Maintenance	INFO	---	Next-Gen AV Access Without Agent	Access attempt from host without Next-Gen Anti-Virus agent installed
1560	Security Services	Next-Gen Anti-Virus	Maintenance	INFO	---	Next-Gen AV Agent Out of Date	Next-Gen Anti-Virus agent out-of-date on host

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1561	Security Services	Next-Gen Anti-Virus	Maintenance	WARNING	---	Next-Gen AV Expire message	Received Next-Gen AV Alert: Your Network Next-Gen Anti-Virus subscription has expired. %s
1562	Security Services	Next-Gen Anti-Virus	Maintenance	WARNING	---	Next-Gen AV Expiration Warning	Received Next-Gen AV Alert: Your Network Next-Gen Anti-Virus subscription will expire in 7 days. %s
1563	Security Services	DPI-SSL Enforcement	Maintenance	INFO	---	SSLE Access Without Agent	Access attempt from host without DPI-SSL Enforcement agent installed
1564	Security Services	DPI-SSL Enforcement	Maintenance	WARNING	---	SSLE Expire Message	Received DPI-SSL Enforcement Alert: Your Network DPI-SSL Enforcement subscription has expired. %s
1565	System	Settings	Maintenance	INFO	---	FTP Transfer Success	Successfully sent Flow Report file by FTP
1566	System	Settings	Maintenance	INFO	---	FTP Transfer Failed	Failed to send Flow Report file by FTP, %s
1567	System	Settings	Maintenance	INFO	---	E-mail Transfer Success	Successfully sent Flow Report file by E-mail
1568	System	Settings	Maintenance	INFO	---	E-mail Transfer Failed	Failed to send Flow Report file by E-mail, %s
1569	Network	SFP	---	INFO	---	Multi-Interface SFP Event	%s
1570	Users	Authentication Access	Attack	ERROR	---	User Account Lockout	%s.
1571	Users	Authentication Access	Attack	ERROR	---	User Account Unlocked	User %s account is unlocked.
1572	Users	Authentication Access	Attack	ERROR	---	User is currently locked out	User login failed because the user is currently locked out.

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1573	Firewall Settings	Advanced	Debug	INFO	---	Drop All IPv6 Traffic	IPv6 packet dropped due to IPv6 traffic processing is disabled on this firewall
1574	Firewall	Application Control	---	NOTICE	---	Filename Logging	Filename: %s
1575	Security Services	DPI-SSL	---	WARNING	---	DPI-SSL Default Exclusions	DPI-SSL Exclusions: Couldn't get DefaultExclusion definitions from the cloud
1576	Firewall Settings	Advanced	Debug	INFO	---	Drop Record Route Packet	Record routed IP packet dropped
1577	Object	Dynamic External Address Object	Maintenance	INFO	---	Dynamic External Address Group Added	Added Dynamic External Address Group %s
1578	Object	Dynamic External Address Object	Maintenance	INFO	---	Dynamic External Address Group Deleted	Deleted Dynamic External Address Group %s
1579	Object	Dynamic External Address Object	Maintenance	INFO	---	Dynamic External Address Group Edited	Edited Dynamic External Address Group %s
1580	Object	Dynamic External Address Object	Maintenance	INFO	---	Dynamic External Address Group Download New File Success	New file Download for Dynamic External Address Group %s successful
1581	Object	Dynamic External Address Object	Maintenance	INFO	---	Dynamic External Address Group Download File Success	Download for Dynamic External Address Group %s successful
1582	Object	Dynamic External Address Object	Maintenance	ALERT	---	Dynamic External Address Group Download Failed	Download Dynamic External Address Group %s failed
1583	Object	Dynamic External Address Object	Maintenance	INFO	---	Dynamic External Address Group Flush OK	Flush Dynamic External Address Group %s successful

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1584	Object	Dynamic External Address Object	Maintenance	INFO	---	Dynamic External Address Group Flush Failed	Flush Dynamic External Address Group %s failed
1585	Users	Authentication Access	User Activity	INFO	---	User Login Denied	User login denied - %s
1586	SD-WAN	Path Selection Profiles	---	DEBUG	18001	Path Available	SD-WAN PSP: %s
1587	SD-WAN	Path Selection Profiles	---	DEBUG	18002	All Paths Removed	SD-WAN PSP: %s
1588	SD-WAN	Path Selection Profiles	---	DEBUG	18003	Path Added	SD-WAN PSP: %s
1589	SD-WAN	Path Selection Profiles	---	DEBUG	18004	Path Removed	SD-WAN PSP: %s
1590	Firewall Settings	Advanced	Debug	INFO	---	Internal VLAN Configuration	%s
1591	Network	Advanced Routing	---	INFO	---	NSM Info	%s
1592	Network	Advanced Routing	---	DEBUG	---	NSM Debug	%s
1593	Network	DNS Security	Maintenance	NOTICE	---	DNS Tunnel Attack	Find DNS tunnel attack - %s
1594	Network	DNS Security	Maintenance	NOTICE	---	Drop DNS Packets Via Suspicious DNS Tunnel	Drop DNS Packets Via Suspicious DNS Tunnel - %s
1595	Wireless	SonicPoint/SonicWave	---	WARNING	---	SonicWave BLE warning	SonicWave %s
1596	Wireless	SonicPoint/SonicWave	---	INFO	---	SonicWave BLE Info	SonicWave %s
1597	Network	POE	---	INFO	---	POE Overview	%s
1598	Wireless	WLAN	802.11b Management	INFO	---	AutoChannel Event	AutoChannel event
1599	Security Services	Content Filter	User Activity	INFO	---	CFS Policy Added	CFS policy added
1600	Security Services	Content Filter	User Activity	INFO	---	CFS Policy Modified	CFS policy modified
1601	Security Services	Content Filter	User Activity	INFO	---	CFS Policy Deleted	CFS policy deleted
1602	System	API	---	INFO	---	Authentication	API Auth: %s
1603	System	API	---	DEBUG	---	Fetch Resource	API Fetch Resource: %s
1604	System	API	---	DEBUG	---	Configuration Change	API Configuration: %s

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1605	Log	FTP	Maintenance	INFO	---	Send Log to FTP	Log successfully sent via FTP
1606	Log	FTP	System Error	WARNING	---	FTP Check Error on Load	Problem sending log via FTP; check FTP settings
1607	Log	FTP	System Error	WARNING	---	FTP Transfer Failed	FTP transfer failed : %s
1608	SD-WAN	Performance Probes	---	DEBUG	18005	Probe Added	Performance Probe added : %s
1609	SD-WAN	Performance Probes	---	DEBUG	18006	Probe Deleted	Performance Probe deleted : %s
1610	SD-WAN	Performance Probes	---	DEBUG	18007	Probe Modified	Performance Probe modified : %s
1611	SD-WAN	Performance Class Objects	---	DEBUG	18008	Performance Class Object Added	Performance Class Object added : %s
1612	SD-WAN	Performance Class Objects	---	DEBUG	18009	Performance Class Object Deleted	Performance Class Object deleted : %s
1613	SD-WAN	Performance Class Objects	---	DEBUG	18010	Performance Class Object Modified	Performance Class Object modified : %s
1615	SD-WAN	Path Selection Profiles	---	DEBUG	18011	PSP Added	SD-WAN Path Selection Profile added : %s
1616	SD-WAN	Path Selection Profiles	---	DEBUG	18012	PSP Modified	SD-WAN Path Selection Profile modified : %s
1617	SD-WAN	Path Selection Profiles	---	DEBUG	18013	PSP Deleted	SD-WAN Path Selection Profile deleted : %s
1618	SD-WAN	SD-WAN Route	---	DEBUG	18014	Route Added	SD-WAN Route added : %s
1619	SD-WAN	SD-WAN Route	---	DEBUG	18015	Route Modified	SD-WAN Route modified : %s
1620	SD-WAN	SD-WAN Route	---	DEBUG	18016	Route Deleted	SD-WAN Route deleted : %s
1621	SD-WAN	SD-WAN Groups	---	DEBUG	18017	SD-WAN Group Added	SD-WAN Group added %s
1622	SD-WAN	SD-WAN Groups	---	DEBUG	18018	SD-WAN Group Modified	SD-WAN Group modified %s
1623	SD-WAN	SD-WAN Groups	---	DEBUG	18019	SD-WAN Group Deleted	SD-WAN Group deleted %s

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1624	SD-WAN	SD-WAN Groups	---	DEBUG	18020	SD-WAN Interface Added to Group	SD-WAN Group Member added %s
1625	SD-WAN	SD-WAN Groups	---	DEBUG	18021	SD-WAN Interface Deleted from Group	SD-WAN Group Member deleted %s
1626	SD-WAN	SD-WAN Groups	---	DEBUG	18022	SD-WAN Group Member Modified	SD-WAN Group Member modified %s
1627	Users	Authentication Access	User Activity	INFO	---	User Account Expired due to inactivity	User account '%s' expired and disabled due to inactivity
1628	Network	TCP	Debug	DEBUG	---	TCP SYN Packet With Data	TCP SYN packet received with data; TCP packet dropped
1629	Network	TCP	Debug	DEBUG	---	TCP Urgent Flag or Pointer	TCP packet received with Urgent flag or pointer; TCP packet dropped
1630	Log	E-mail	Maintenance	INFO	---	Email Audit Records	Audit Records from Network Security Appliance
1631	Security Services	GAV	Maintenance	NOTICE	---	Capture ATP Sandbox Verdict	Gateway Anti-Virus Status: %s
1632	Multi-Instance	Instance Status	---	NOTICE	---	Service Stopped	%s
1633	Multi-Instance	Instance Status	---	INFO	---	Service Started	%s
1634	Multi-Instance	Instance Status	---	NOTICE	---	Service Deleted	%s
1635	Multi-Instance	Instance Status	---	ERROR	---	Service Failed	%s
1636	System	Settings	---	INFO	---	Port Unreachable Received	Port Unreachable received from remote sender
1637	System	Settings	---	INFO	---	Port Unreachable Ignored	Port Unreachable from remote sender ignored
1638	Wireless	SonicPoint/SonicWave	---	INFO	---	SonicWave RRM Info	%s
1639	System	Cloud Platform	---	DEBUG	---	Cloud Platform API	%s

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1640	Unified Policy Engine	Policy Action	NGPE	INFO	---	Policy Matched	Policy Matched %s
1641	Unified Policy Engine	Policy Action	NGPE	INFO	---	Report Connection Opened	Connection Opened reporting %s
1642	Unified Policy Engine	Policy Action	NGPE	INFO	---	Report Connection Closed	Connection Closed reporting %s
1643	Multi-Instance	Instance Status	---	NOTICE	---	Service Added	%s
1644	Multi-Instance	Instance Status	---	NOTICE	---	Service Edited	%s
1645	Security Services	Endpoint Security	Maintenance	INFO	---	Endpoint Security Access Without Agent	Endpoint Security: Access attempt from host without %s agent installed.
1646	Security Services	Endpoint Security	Maintenance	WARNING	---	Endpoint Security Service Expire Message	Endpoint Security: %s subscription of your network has expired.
1647	Security Services	Endpoint Security	Maintenance	WARNING	---	Endpoint Security Expiration Warning	Endpoint Security: %s subscription of your network will expire in 7 days.
1649	Network	Switch Network	---	INFO	---	SonicWall Switch	%s
1650	Users	Authentication Access	System Error	ALERT	---	Recommend NSM upgrade	Using an old NSM which compromises the security of some functionality on this firewall. An upgrade of NSM is recommended.
1651	Users	Authentication Access	System Error	ALERT	---	NSM encryption type unknown	NSM wants to use an encryption method which this firewall does not support: %s

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1652	Users	Authentication Access	System Error	ALERT	---	Recommend management platform upgrade	Using an old SonicWall firewall management platform which compromises the security of some functionality on this firewall. An upgrade of the platform is recommended.
1653	Users	Authentication Access	System Error	ALERT	---	Management platform encryption type unknown	The SonicWall firewall management platform wants to use an encryption method which this firewall does not support: %s
1654	Firewall	Application Firewall	User Activity	DEBUG	---	Custom Match Applied	Custom Match applied %s
1655	Users	Authentication Access	Attack	ERROR	---	User is now locked out	User login failed, user is now locked out.
1656	WWAN Modem	General	User Activity	INFO	---	WWAN Attached	WWAN - Attached %s
1657	WWAN Modem	General	User Activity	INFO	---	WWAN Detached	WWAN - Detached %s
1658	Security Services	Content Filter	---	WARNING	---	CFS Warning	CFS Warning: %s
1659	Security Services	Content Filter	---	INFO	---	CFS Info	CFS Info: %s
1660	Security Services	GAV	Attack	NOTICE	---	Capture ATP Block Until Verdict	Gateway Anti-Virus: %s
1661	Network	Advanced Routing	---	INFO	---	RIPng Info	%s
1662	Network	Advanced Routing	---	NOTICE	---	RIPng Notice	%s
1663	Network	Advanced Routing	---	DEBUG	---	RIPng Debug	%s
1664	Network	Advanced Routing	---	INFO	---	OSPFv3 Info	%s
1665	Network	Advanced Routing	---	NOTICE	---	OSPFv3 Notice	%s
1666	Network	Advanced Routing	---	DEBUG	---	OSPFv3 Debug	%s

Log Event Message Index

Event ID	SonicOS/X Category Name	SonicOS/X Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1667	Network	Advanced Routing	---	NOTICE	---	NSM Notice	%s
1668	Network	Advanced Routing	---	NOTICE	---	OSPF Notice	%s
1669	Network	Advanced Routing	---	NOTICE	---	BGP Notice	%s
1670	Security Services	GAV	Maintenance	NOTICE	---	Capture ATP Sandbox Pending Response	Gateway Anti-Virus Status: %s
1671	Network	Network Access	---	ALERT	---	Extended Switch Unreachable	%s
1672	Users	Authentication Access	User Activity	WARNING	---	CLI Limit Admin Denied From WAN	CLI limit administrator login denied from WAN
1673	SSL VPN	General	---	DEBUG	---	SSL VPN Debug	%s
1674	Log	Configuration Auditing	User Activity	INFO	---	Chassis settings change	Chassis: %s
1675	Security Services	GAV	---	INFO	---	Capture Security Failover	CSa failover %s

Syslog Events

This section provides information about using the detailed logs created from Syslog events. Syslog settings are configured in the **DEVICE | Log > Syslog** page in SonicOS/X.

Topics:

Log > Syslog

In addition to the standard event log, the SonicWall security appliance can send a detailed log to an external Syslog server. The detailed log captures all log activity and includes every connection source and destination IP address, IP service, and number of bytes transferred. Syslog analyzers such as SonicWall Analytics, SonicWall Next Generation Analyzer or a product from another vendor such as Graylog, Solarwinds, or Fastvue can be used to sort, analyze, and graph the Syslog data.

The **DEVICE | Log > Syslog** page provides two screens: **Syslog Settings** and **Syslog Servers**. For more information on configuring settings and servers on the **DEVICE | Log > Syslog** page, refer to the *SonicOS/X 7 Device Log* administration guide.

DEVICE | Log > Syslog > Syslog Settings Screen

DEVICE | Log > Syslog > Syslog Servers Screen

Index of Syslog Tag Field Descriptions

This section provides an alphabetical listing of Syslog tags and the associated field description. For more information about the "pri" Syslog Tag, see Priority Levels on page 110. The value here is taken from the "Priority Level" column of the Index of Log Event Messages on page 10. For more information about the "c" Syslog Tag, see Legacy Categories on page 109.

Syslog Tags

Tag	Tags for Arc-Sight	Field	Description
<ddd>		Syslog message prefix	The beginning of each Syslog message has a string of the form <ddd> where ddd is a decimal number indicating facility and priority of the message
af_polid		Application Filter	Displays the Application Filter Policy ID
af_policy		Application Filter	Displays the Application Policy name

Tag	Tags for Arc-Sight	Field	Description
af_type		Application Filter	Displays the Application Policy type such as: • SMTP Client Request • HTTP Client Request • HTTP Server Response • FTP Client Request • FTP Client Upload File • FTP Client Download File • POP3 Client Request • POP3 Server Response • FTP Data Transfer • IPS Content • App Control Content • Custom Policy Type • CFS
af_service		Application Filter	Displays the Application Policy service name
af_action		Application Filter	Displays the Application Policy action such as: • HTTP Block Page • HTTP Redirect • Bandwidth Management • Disable E-Mail Attachment • FTP Notification Reply • Reset/Drop • Block SMTP E-Mail • Bypass DPI • CFS Block Page • Packet Monitor
af_object		Application policy object name	Displays the custom Application Policy object name
ai		Active Interface via GMS heartbeat	Displays the Active WAN Interface. Normally it is Primary WAN, but in a failover, it displays the value of the failover default outbound WAN interface, if there is more than one WAN. When there is only one WAN Interface, it is always Primary WAN regardless of the link state
app	app	Numeric application ID	Indicates the application for the applied Syslog. Only displays when Flow Reporting is enabled
appcat	appcat	Application Control	Display the application category when Application Control is enabled
appid	appid	Application ID	Display the application ID when Application Control is enabled

Tag	Tags for Arc-Sight	Field	Description
appName		Non-Signature Application Name	Indicates the non-signature Application Name that matches the Application ID "app" or "f" of the Syslog; Only displays when Flow Reporting is enabled
arg	arg	URL	Used to render a URL: arg represents the URL path name part
bcastRx	bcastRx	Interface statistics report	Displays the broadcast packets received
bcastTx	bcastTx	Interface statistics report	Displays the broadcast packets transmitted
bid	bid	Numeric Blade ID	Indicates the blade that originated the event and applies only to products with blade architecture
bytesRx	bytesRx	Interface statistics report	Displays the bytes received
bytesTx	bytesTX	Interface statistics report	Displays the bytes transmitted
c	cat	Message category (legacy only)	Indicates the legacy category number (Note: SonicOS/X does not currently send new category information)
category	category	Blocking code description	Applicable only when CFS is enabled, indicates the category of the blocked content such as "Gambling". This works in conjunction with "code" for the blocking code.
catid		Rule category	Indicates the category ID of the rule
cdur	cn3Label	Connection Duration	Displays the connection duration in milliseconds (ms) and only applies to m=537 "Connection Closed" Syslog
change	SWGMSchangeUrl	Configuration change webpage	Displays the basename of the firewall web page that performed the last configuration change
code	reason	Blocking code	Indicates the CFS block code
conns		Firewall status report via GMS heartbeat	Indicates the number of connections in use
contentObject		Application Filter	Indicates rule name
	cs4	Interface Statistics	Display interface statistics
	deviceOutboundInterface	Interface	Indicates interface on which the packet leaves the device
	deviceInboundInterface	Interface	Indicates interface on which the packet leaves the device

Tag	Tags for Arc-Sight	Field	Description
dpi		Numeric code	Indicates that a flow underwent inspection by Deep Packet Inspection. The dpi tag only applies to *Connection Closed* Syslog events with the message ID defined as either: • m=537 if the flow has no URL information, or if CFS was not enabled • m=97 if CFS was enabled and flow information includes URL Possible values for dpi are: • 1 = DPI inspection occurred • 0 = no DPI inspection
	dpt	Port	Display destination port
	dnpt	NAT'ed Port	Display NAT'ed destination port
dst	dst	Destination	Destination IP address, and optionally, port, network interface, and resolved name
dstMac	dmac	Destination MAC Address	Destination MAC Address
dstV6	dst	Destination	Destination IPv6 address, and optionally, port, network interface, and resolved name
dstname	request	URL	Displays the URL of accessed Websites and hosts
dstname	dstname	Notes	Indicates additional information such as description of forbidden/deleted email attachments
dstZone	cs4Label (destination)	Destination zone name	Displays destination zone
dur	cs6label	Numeric, session duration in seconds	Displays the connection duration in seconds; pertains to the activity time of an authenticated user session (such as logout messages)
dyn		Firewall status report via GMS heartbeat	Displays the HA and dialup connection state (rendered as "h.d" where "h" is "n" (not enabled), "b" (backup), or "p" (primary) and "d" is "1" (enabled) or "0" (disabled))
f	flowType	Numeric flow type	Indicates the flow type when Flow Reporting is disabled
fileid		URL or MD5 (long URLs may be truncated)	File identification or name, which may be in MD5 format or a URL. For example, Capture ATP uses this tag to indicate a file inspected by GAV or CloudAV.

Tag	Tags for Arc-Sight	Field	Description
filetxstatus		Capture ATP: File transmission status	Result of file transmission as reported by Capture ATP. Possible values are:
			100 : CONFIRMED
			200 : TOO BIG
			210 : PENDING
			211 : GOOD
			212 : BAD
			213 : REQUEST SENT
			214 : UNKNOWN
			220 : CLOUDAV
			230 : GAV
			260 : SERVER COMMAND
			270 : EXCESSIVE PACKET LOSS
			280 : OUT OF MEMORY
			300 : AWAITING CONFIRM
			310 : CANT CONFIRM
			400 : LOW MEMORY
			410 : Files Per Hour EXCEEDED
			420 : TOO MANY CONCURRENT
fw		Firewall WAN IP	Indicates the WAN IP Address
fw_action		Firewall Action	The explicit action performed on network traffic (packets) encountered by the firewall based on built-in or user-configured policies that may allow or drop packets. For events that are not associated with specific packets, the value "Not Applicable" or "NA" is used. Possible values are:
			• **forward** - packet is forwarded due to a matching policy or rule set
			• **drop** - packet is dropped due to a matching policy or rule set
			• **mgmt** - packet is a management packet, management policy will be applied
			• **NA** - not associated with a packet, firewall action is Not Applicable
fwlan		Firewall status report via GS heartbeat	Indicates the LAN zone IP address
gcat	gcat	Group category	Display event group category when using Enhanced Syslog
goodRxBytes	goodRxBytes	SonicPoint statistics report	Indicates the well-formed bytes received
goodTxBytes	goodTxBytes	SonicPoint statistics report	Indicates the well-formed bytes transmitted

Tag	Tags for Arc-Sight	Field	Description
i		Firewall status report via GMS heartbeat	Displays the GMS message interval in seconds
icmpCode	cn2	ICMP type and code	Indicates the ICMP code
id=firewall		WebTrends prefix	Syntactic sugar for WebTrends (and GMS by habit)
if	if	Interface statistics report	Displays the interface on which statistics are reported
ipscat	ipscat	IPS message	Displays the IPS category
ipspri	ipspri	IPS message	Displays the IPS priority
lic		Firewall status report via GMS heartbeat	Indicates the number of licenses for firewalls with limited modes
m		Message ID	Provides the message ID number
mailFrom		Email sender	Originator of the email
msg	msg	Message	Displays the message which is composed of either or both a predefined message and a dynamic message containing a string %s or numeric %d argument
n	cnt	Message count	Indicates the number of times event occurs
natDst	cs2Label	NAT destination IP	Displays the NAT'ed destination IP address
natDstV6	cs2Label	NAT destination IPv6	Displays the NAT'ed destination IPv6 address
natSrc	cs1Label	NAT source IP	Displays the NAT'ed source IP address
natSrcV6	cs1Label	NAT source IPv6	Displays the NAT'ed source IPv6 address
note	cs6	Additional Information	Additional information that is application-dependent
npcs	cs5	URL	Applicable only when Network Packet Capture System (NPCS Solera) is enabled, displays URL of an NPCS object
op	requestMethod	HTTP OP code	Displays the value assigned by SonicOS/X Content Filtering based on its parsing of an HTTP packet's Method token for the Request message. Supported values are: • 0 = NO OPERATION • 1 = HTTP GET • 2 = HTTP POST • 3 = HTTP HEAD where GET/POST/HEAD are standard HTTP Methods and NO OPERATION is used by SonicOS/X to indicate that none of the other defined values apply.

Tag	Tags for Arc-Sight	Field	Description
packetdatId packetdatNum packetdatEnc		Raw Data used in Security Services Syslogs, disabled by default	Used in m=1391 (Raw Data) to indicate that Raw Data is available and transmission had been enabled. When enabled, Raw Data information is provided to SonicWall GMS when generating Security Service Syslogs: m=14, 16, 608, 609, 761, 789, 790, 793, 794, 795, 809, 1154, 1155
pri		Message priority	Displays the event priority level (0=emergency, 7=debug) Refer to Priority Levels on page 110
proto	proto	Protocol and service	Displays the protocol information (rendered as "proto=[protocol]" or just "[proto]/[service]")
pt		Firewall status report via GMS heartbeat	Displays the HTTP/HTTPS management port (rendered as "hhh.sss")
radio	radio	SonicPoint statistics report	Displays the SonicWave/SonicPoint radio on which event occurred
rcptTo		recipient	Indicates the email recipient
rcvd	in	Bytes received	Indicates the number of bytes received within connection
referer	referer	HTTP Referrer URI	When HTTP content is detected, this value distinguishes the referrer from the requested URL for website access
result	outcome	HTTP Result code	Displays the HTTP result code (200, 403, etc.) of Website hit
rpkt	cn1Label	Packet received	Display the number of packet received
rule	cs1	Rule ID	Used to identify a policy or a rule associated with an event
sent	out	Bytes sent	Displays the number of bytes sent within connection

Tag	Tags for Arc-Sight	Field	Description
sess	cs5Label	Pre-defined string indicating session type	Applies to Syslogs with an associated user session being tracked by the UTM. Determined by the Authentication mechanism and can be one of: • **None** - the starting session type when user authentication is still pending or just started • **Web** - identified as a Web browser session • **Portal** - SSL-VPN portal login • **l2tpc** - L2TP client session • **vpnc** - VPN client session • **sslvpnc** - SSL-VPN client session • **Auto** - Auto-logged in session, for example Single Sign On (SSO) • **Other** - none of the known types • **CLI** - indicates a CLI session
sid	sid	IPS or Anti-Spyware message	Provides either IPS or Anti-Spyware signature ID
sn		Firewall serial number	Indicates the device serial number
spkt	cn2Label	Packet sent	Display the number of packets sent
	spt	Port	Displays source port
spycat	spycat	Anti-Spyware message	Displays the Anti-Spyware category
spypri	spypri	Anti-Spyware message	Displays the Anti-Spyware priority
	snpt	NAT source port	Display NAT'ed source port
src	src	Source	Indicates the source IP address, and optionally, port, network interface, and resolved name
srcMac	smac	Source MAC Address	Source MAC Address
srcZone	cs3Label (source)	Source zone name	Displays source zone
station	station	SonicPoint statistics report	Displays the client (station) on which event occurred
time		Time	Reports the time of event
type	cn1	ICMP type and code	Indicates the ICMP type
ucastRx	ucastRx	Interface statistics report	Displays the unicast packets received
ucastTx	ucastTx	Interface statistics report	Displays the unicast packets transmitted
unsynched		Firewall status report via GMS heartbeat	Reports the time since last local change in seconds
usestandbysa		Firewall status report via GMS heartbeat	Displays whether standby SA is in use ("1" or "0") for GMS management
usr (or user)	susr	User	Displays the user name ("user" is the tag used by WebTrends)

Tag	Tags for Arc-Sight	Field	Description
uuid	uuid	Universally Unique Identifier	A universally unique identifier (UUID) is a 128-bit label that is unique within the SonicOS/X product platforms used to tag information objects. The SonicOS/X format uses the hyphenated hexadecimal notation compliant with Rec. ITU-T X.667	ISO/IEC 9834-8 and technically compatible with RFC 4122. Example SonicOS/X usage is: uuid="b63c4f43-8bd4-2063-0700-c0e ae488cfd2"
vpnpolicy	cs2 (source)	Source VPN policy name	Displays the source VPN policy name of event
vpnpolicyDst	cs3 (destination)	Destination VPN policy name	Displays the destination VPN policy name of event

Configuration Auditing Syslog Tags

Configuration auditing is a feature that automatically records any configuration changes that an administrator attempts from one of the available user interfaces, including web management (via HTTP and HTTPS), command line (via console or SSH), or SonicWall Network Security Manager (NSM). A configuration auditing records table on **MONITOR | Logs > Auditing Logs** records all attempted configuration changes, both successful and failed. Syslog events are also generated for configuration auditing. The following table identifies and defines the Configuration Auditing Syslog tags.

Configuration Auditing Syslog Tags

Tag	Description
auditId	Configuration Audit ID is used to identify a Configuration Auditing entry.
tranxId	Configuration Audit Transaction ID is used to determine entries pertaining to the same transaction or batch.
userMode	Configuration Audit User Mode distinguishes privileges bestowed to a user.
auditTime	Configuration Audit Timestamp indicates the time when a configuration was changed.
auditPath	Configuration Audit Path describes the logical location of the configuration setting.
grpName	Configuration Audit Group Name labels a group of data usually associated with a table. Scalar data have no group.
grpIndex	Configuration Audit Group Index identifies an instance of a data group.
oldValue	Configuration Audit Old Value is the previous value of an object.
newValue	Configuration Audit New Value is the new value of an object.

Syslog Group Category (gcat) Values

The following table defines the gcat values used in SonicOS/X Syslog events.

Syslog gcat Values

gcat Number	Value
1	System
2	Log
3	Security Services
4	Users
5	Firewall Settings
6	Network
7	VPN
8	High Availability
9	3G/4G, Modem, and Module
10	Firewall
11	Wireless
12	VoIP
13	SSL VPN
14	Anti-Spam
15	WAN Acceleration
16	SD-WAN
17	Multi-Tenancy

For example, **gcat=3** means "Security Services" category, and **gcat=6** means "Network" category in the following examples:

Intrusion Prevention (IPS) example:

```
Feb 26 22:53:50 10.8.139.192 FEB 26 2019 06:53:50 18B16989BF80 CEF:0|SonicWall|NSa
3650|6.5.4.1-25n|608|IPS Detection Alert|9|cat=32 gcat=3 src=180.97.33.107 spt=8
deviceInboundInterface=X1 dst=36.50.1.220 dpt=1 deviceOutboundInterface=X0 msg="IPS
Detection Alert: ICMP Echo Reply, SID: 316, Priority: low" msg="IPS Detection Alert:
ICMP Echo Reply" sid=316 ipscat="ICMP Echo Reply" ipspri=3 cnt=6 fw_action="NA"
```

IP Spoof Detection example:

```
Feb 26 22:53:52 10.8.139.192 FEB 26 2019 06:53:52 18B16989BF80 CEF:0|SonicWall|NSa
3650|6.5.4.1-25n|23|IP Spoof Detected|9|cat=32 gcat=3 smac=00:50:56:9f:88:86
src=10.8.138.215 spt=68 deviceInboundInterface=MGMT cs3Label=Unknown
dmac=ff:ff:ff:ff:ff:ff dst=255.255.255.255 dpt=67 deviceOutboundInterface=X0
cs4Label=LAN proto=udp/67 in=328 cnt=4 fw_action="drop"
```

IPv6 / ICMPv6 example:

```
Feb 26 22:54:05 10.8.139.192 FEB 26 2019 06:54:05 18B16989BF80 CEF:0|SonicWall|NSa
3650|6.5.4.1-25n|1430|IPv6 Packet with Ext Header|4|cat=512 gcat=6
smac=00:1c:57:66:00:00 srcV6=fe80::1 deviceInboundInterface=X1
dmac=33:33:00:00:00:01 dstV6=ff02::1 proto=0 in=76 cs6="Extention header: 0"
cnt=1401 fw_action="NA"
```

Examples of Standard Syslog Messages

The following examples show the content of the Syslog packet. This type of message can be viewed on the Syslog server or in any packet analyzer application. Note that this is the Default Syslog Format.

Connection Closed (with dpi tag) examples:

```
Feb 26 22:47:37 10.8.139.192 id=firewall sn=18B16989BF80 time="2019-02-26 06:47:37"
fw=10.8.139.192 pri=6 c=1024 m=537 msg="Connection Closed" app=9 n=2200
src=36.50.1.220:49196:X0 dst=216.58.195.67:80:X1 dstMac=00:1c:57:66:00:00
proto=tcp/http sent=152 spkt=3 dpi=0 cdur=40183 rule="9 (LAN->WAN)" fw_action="NA"

Jan 31 09:07:48 10.8.96.203  id=firewall sn=004010292F25 time="2019-01-30 18:17:17"
fw=10.8.96.203 pri=6 c=1024 m=537 msg="Connection Closed" app=9 n=1792
src=192.168.203.56:65440:X0 dst=10.8.96.159:80:X1 srcMac=00:50:56:a1:3e:5d
dstMac=00:0c:29:5b:4f:04 proto=tcp/1 sent=186 rcvd=94 spkt=4 rpkt=2 dpi=1 cdur=4983
rule="5 (LAN->WAN)" fw_action="NA"

Jan 31 09:07:48 10.8.96.203  id=firewall sn=004010292F25 time="2019-01-30 18:17:17"
fw=10.8.96.203 pri=6 c=1024 m=97 app=48 n=3 src=192.168.203.56:65439:X0
dst=10.8.96.159:80:X1 srcMac=00:50:56:a1:3e:5d dstMac=00:0c:29:5b:4f:04 proto=tcp/1
op=1 sent=1347 rcvd=2443 dpi=1 dstname=10.8.96.159 arg=/ code=64 Category="Not
Rated" note="Policy: CFS Default Policy, Info: 6148 " rule="5 (LAN->WAN)"
fw_action="NA"
```

Content Filtering (CFS) examples:

```
Feb 26 22:50:44 10.8.139.192  id=firewall sn=18B16989BF80 time="2019-02-26
06:50:44" fw=10.8.139.192 pri=6 c=1024 m=97 app=48 n=19 src=36.50.1.220:49312:X0
dst=10.8.8.200:80:X1 srcMac=00:50:56:b4:54:f5 dstMac=00:1c:57:66:00:00
proto=tcp/http op=1 sent=4775 rcvd=173391 dpi=0 dstname=10.8.8.200 arg=/ code=64
Category="Not Rated" note="Policy: CFS Default Policy, Info: 6148 " rule="9
(LAN->WAN)" fw_action="NA"

Feb 26 22:49:51 10.8.139.192  id=firewall sn=18B16989BF80 time="2019-02-26
06:49:51" fw=10.8.139.192 pri=3 c=4 m=14 msg="Web site access denied" app=9 n=1
src=36.50.1.220:49281:X0 dst=209.59.212.85:80:X1 srcMac=00:50:56:b4:54:f5
dstMac=18:b1:69:89:bf:80 proto=tcp/http dstname=www.gamble.com arg=/ code=11
Category="Gambling" rule="9 (LAN->WAN)" fw_action="drop"

Feb 26 22:50:50 10.8.139.192  id=firewall sn=18B16989BF80 time="2019-02-26
06:50:49" fw=10.8.139.192 pri=6 c=1024 m=97 app=48 n=20 src=36.50.1.220:49315:X0
dst=10.8.8.200:80:X1 srcMac=00:50:56:b4:54:f5 dstMac=00:1c:57:66:00:00
proto=tcp/http op=1 sent=643 rcvd=4546 dpi=0 dstname=10.8.8.200
arg=/virus/klez.h.bin code=64 Category="Not Rated" note="Policy: CFS Default Policy,
Info: 6148 Referer: http://10.8.8.200/virus.htm"
referer="http://10.8.8.200/virus.htm" rule="9 (LAN->WAN)" fw_action="NA"

Feb 26 22:49:41 10.8.139.192  id=firewall sn=18B16989BF80 time="2019-02-26
06:49:41" fw=10.8.139.192 pri=6 c=1024 m=97 app=48 n=18 src=36.50.1.220:49239:X0
dst=124.108.103.103:80:X1 srcMac=00:50:56:b4:54:f5 dstMac=00:1c:57:66:00:00
proto=tcp/http op=1 sent=626 rcvd=890 dpi=0 dstname=www.yahoo.com arg=/ code=29
Category="Search Engines and Portals" note="Policy: CFS Default Policy, Info: 6148 "
rule="9 (LAN->WAN)" fw_action="NA"
```

Capture ATP (Sandbox) example:

```
Feb 26 22:50:44 10.8.139.192  id=firewall sn=18B16989BF80 time="2019-02-26
06:50:44" fw=10.8.139.192 pri=6 c=1 m=1460 msg="Gateway Anti-Virus Status: GAV
Detection. File forwarding to Sandbox truncated for:
http://10.8.8.200/virus/klez.h.bin, filename: klez.h.bin."
fileid="10.8.8.200/virus/klez.h.bin" filetxstatus=230 dstname=10.8.8.200
```

```
arg=/virus/klez.h.bin n=1 src=10.8.8.200:80:X1 dst=36.50.1.220:49312:X0
proto=tcp/http fw_action="NA"
```

Gateway Anti-Virus (GAV) example:

```
Feb 26 22:50:44 10.8.139.192   id=firewall sn=18B16989BF80 time="2019-02-26
06:50:44" fw=10.8.139.192 pri=1 c=32 m=809 msg="Gateway Anti-Virus Alert:
Injected.AZ (Trojan) blocked." n=1 src=10.8.8.200:80:X1 dst=36.50.1.220:49312:X0
fw_action="NA"
```

Intrusion Prevention (IPS) example:

```
Feb 26 22:48:49 10.8.139.192   id=firewall sn=18B16989BF80 time="2019-02-26
06:48:49" fw=10.8.139.192 pri=1 c=32 m=608 msg="IPS Detection Alert: ICMP Echo
Reply" sid=316 ipscat="ICMP Echo Reply" ipspri=3   n=1 src=180.97.33.107:8:X1
dst=36.50.1.220:1:X0 fw_action="NA"
```

Detected scan attack examples:

```
Feb 26 22:49:44 10.8.139.192   id=firewall sn=18B16989BF80 time="2019-02-26
06:49:44" fw=10.8.139.192 pri=1 c=32 m=82 msg="Possible port scan detected" n=1
src=69.147.88.7:443:X1 dst=10.8.139.192:31894:X1 srcMac=00:1c:57:66:00:00
dstMac=18:b1:69:89:bf:81 proto=tcp/https note="TCP scanned port list, 42338, 28852,
6467, 55193, 47039" fw_action="NA"

Feb 26 22:49:45 10.8.139.192   id=firewall sn=18B16989BF80 time="2019-02-26
06:49:45" fw=10.8.139.192 pri=1 c=32 m=177 msg="Probable TCP FIN scan detected" n=1
src=69.147.88.7:443:X1 dst=10.8.139.192:11269:X1 srcMac=00:1c:57:66:00:00
dstMac=18:b1:69:89:bf:81 proto=tcp/https note="TCP scanned port list, 42338, 28852,
6467, 55193, 47039, 31894, 45687, 2228, 62490, 11269" fw_action="NA"
```

Examples of ArcSight Syslog Messages

The following examples show the content of the Syslog packet. This type of message can be viewed on the
Syslog server or any packet analyzer application.

Content Filtering (CFS) examples:

```
Feb 26 22:53:28 10.8.139.192 WAN)" app=48 requestMethod=1
request=10.8.8.200/virus/Macro.Word97.Melissa.c reason=64 Category-"Not Rated"
cs6="Policy: CFS Default Policy, Info: 6148 Referer: http://10.8.8.200/virus.htm"
cnt=21 fw_action="NA" dpi=0 referer="http://10.8.8.200/virus.htm"

Feb 26 22:53:39 10.8.139.192 WAN)" app=48 requestMethod=1
request=ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedc
ertstl.cab?c4091b107fb9006c reason=27 Category-"Information Technology/Computers"
cs6="Policy: CFS Default Policy, Info: 6148 " cnt=22 fw_action="NA" dpi=0
```

Intrusion Prevention (IPS) example:

```
Feb 26 22:53:50 10.8.139.192 FEB 26 2019 06:53:50 18B16989BF80 CEF:0|SonicWall|NSa
3650|6.5.4.1-25n|608|IPS Detection Alert|9|cat=32 gcat=3 src=180.97.33.107 spt=8
deviceInboundInterface=X1 dst=36.50.1.220 dpt=1 deviceOutboundInterface=X0 msg="IPS
Detection Alert: ICMP Echo Reply, SID: 316, Priority: low" msg="IPS Detection Alert:
ICMP Echo Reply" sid=316 ipscat="ICMP Echo Reply" ipspri=3   cnt=6 fw_action="NA"
```

IP Spoof Detection example:

```
Feb 26 22:53:52 10.8.139.192 FEB 26 2019 06:53:52 18B16989BF80 CEF:0|SonicWall|NSa
3650|6.5.4.1-25n|23|IP Spoof Detected|9|cat=32 gcat=3 smac=00:50:56:9f:88:86
src=10.8.138.215 spt=68 deviceInboundInterface=MGMT cs3Label=Unknown
dmac=ff:ff:ff:ff:ff:ff dst=255.255.255.255 dpt=67 deviceOutboundInterface=X0
cs4Label=LAN proto=udp/67 in=328 cnt=4 fw_action="drop"
```

IPv6 / ICMPv6 examples:

```
Feb 26 22:54:05 10.8.139.192 FEB 26 2019 06:54:05 18B16989BF80 CEF:0|SonicWall|NSa
3650|6.5.4.1-25n|1430|IPv6 Packet with Ext Header|4|cat=512 gcat=6
smac=00:1c:57:66:00:00 srcV6=fe80::1 deviceInboundInterface=X1
dmac=33:33:00:00:00:01 dstV6=ff02::1 proto=0 in=76 cs6="Extention header: 0"
cnt=1401 fw_action="NA"
```

```
Feb 26 22:54:05 10.8.139.192 FEB 26 2019 06:54:05 18B16989BF80 CEF:0|SonicWall|NSa
3650|6.5.4.1-25n|1431|ICMPv6 Packets Received|4|cat=0 gcat=6 smac=00:1c:57:66:00:00
srcV6=fe80::1 deviceInboundInterface=X1 dmac=33:33:00:00:00:01 dstV6=ff02::1
proto=ipv6-icmp cn1=130 cn2=0 in=76 cs6="ICMPv6" cnt=1559 fw_action="NA"
```

Anti-Spyware Detection example:

```
Feb 26 22:54:59 10.8.139.192 FEB 26 2019 06:54:58 18B16989BF80 CEF:0|SonicWall|NSa
3650|6.5.4.1-25n|795|Anti-Spyware Detection Alert|9|cat=32 gcat=3 src=10.8.8.200
spt=80 deviceInboundInterface=X1 dst=36.50.1.220 dpt=49451
deviceOutboundInterface=X0 msg="Anti-Spyware Detection Alert: Search_Miracle
Download x.cab (Adware), SID: 2648, Danger Level: low" msg="Anti-Spyware Detection
Alert: Search_Miracle Download x.cab (Adware)" sid=2648 spycat="Search_Miracle
Download x.cab (Adware)" spypri=3 cnt=1 fw_action="NA"
```

Gateway Anti-Virus (GAV) example:

```
Feb 26 22:55:08 10.8.139.192 FEB 26 2019 06:55:08 18B16989BF80 CEF:0|SonicWall|NSa
3650|6.5.4.1-25n|809|AV Gateway Alert|9|cat=32 gcat=3 src=10.8.8.200 spt=80
deviceInboundInterface=X1 dst=36.50.1.220 dpt=49451 deviceOutboundInterface=X0
msg="Gateway Anti-Virus Alert: Injected.AZ (Trojan) blocked." cnt=4 fw_action="NA"
```

Capture ATP File Transfer examples:

```
Feb 26 22:55:41 10.8.139.192 FEB 26 2019 06:55:41 18B16989BF80 CEF:0|SonicWall|NSa
3650|6.5.4.1-25n|1460|Capture ATP File Transfer Result|4|cat=1 gcat=3 src=10.8.8.200
spt=80 deviceInboundInterface=X1 dst=36.50.1.220 dpt=49388
deviceOutboundInterface=X0 proto=tcp/http in=1500
request=10.8.8.200/spyware/3gargs.exe.bin msg="Gateway Anti-Virus Status:  File sent
to Sandbox, but could not confirm receipt due to highly delayed acks. Time-wait
timer expired waiting for receipt confirmation:
http://10.8.8.200/spyware/3gargs.exe.bin, filename: 3gargs.exe.bin." cnt=4
fw_action="NA" fileid="64ab24d0e8b375cfba1cbcfe0ac614db" filetxstatus=310
```

```
Feb 26 22:55:48 10.8.139.192 FEB 26 2019 06:55:47 18B16989BF80 CEF:0|SonicWall|NSa
3650|6.5.4.1-25n|1460|Capture ATP File Transfer Result|4|cat=1 gcat=3 src=10.8.8.200
spt=80 deviceInboundInterface=X1 dst=36.50.1.220 dpt=49465
deviceOutboundInterface=X0 proto=tcp/http in=1500
request=10.8.8.200/spyware/3gargs.exe.bin msg="Gateway Anti-Virus Status:
GAV_BLOCK_REASON_SPYWARE. File forwarding to Sandbox truncated for:
http://10.8.8.200/spyware/3gargs.exe.bin, filename: 3gargs.exe.bin." cnt=5
fw_action="NA" fileid="10.8.8.200/spyware/3gargs.exe.bin" filetxstatus=230
```

Connection Opened/Closed (with dpi tag) examples:

```
Feb 26 22:53:14 10.8.139.192 FEB 26 2019 06:53:14 18B16989BF80 CEF:0|SonicWall|NSa
3650|6.5.4.1-25n|98|Connection Opened|4|cat=262144 gcat=6 src=36.50.1.220 spt=49385
deviceInboundInterface=X0 cs1Label=10.8.139.192 snpt=56339 dst=216.58.194.195
dpt=443 deviceOutboundInterface=X1 cs2Label=216.58.194.195 dnpt=443 proto=tcp/https
out=52 cnt=2764 fw_action="NA" dpi=0
```

```
Feb 26 22:53:16 10.8.139.192 FEB 26 2019 06:53:16 18B16989BF80 CEF:0|SonicWall|NSa
3650|6.5.4.1-25n|537|Connection Closed|4|cat=1024 gcat=6 src=10.8.139.192 spt=49153
deviceInboundInterface=X1 cs1Label=10.8.139.192 snpt=12830 dmac=00:1c:57:66:00:00
dst=10.190.202.200 dpt=53 deviceOutboundInterface=X1 cs2Label=10.190.202.200 dnpt=53
proto=udp/dns out=346 in=574 cn2Label=5 cn1Label=5 cn3Label=35750 app=2 cnt=2720
fw_action="NA" dpi=0
```

Legacy Categories

This section can be used as a reference for understanding different categories and their descriptions. The following table describes the Legacy categories shared in all SonicOS/X releases.

Legacy Category Values

ID (used in Syslog)	Name	Description
0		Event is not Legacy Category, not backward compatible.
1	System Maintenance	Logs general system activity, such as system activations.
2	System Errors	Logs problems with DNS or Email.
4	Blocked Web Sites	Logs Web sites or news groups blocked by the Content Filter List or by customized filtering.
8	Blocked Java Etc	Logs Java, ActiveX, and Cookies blocked by the SonicWall security appliance.
16	User Activity	Logs successful and unsuccessful log in attempts.
32	Attacks	Logs messages showing Denial of Service attacks, such as SYN Flood, Ping of Death, and IP Spoofing.
64	Dropped TCP	Logs blocked incoming TCP connections.
128	Dropped UDP	Logs blocked incoming UDP packets.
256	Dropped ICMP	Logs blocked incoming ICMP packets.
512	Network Debug	Logs NetBIOS broadcasts, ARP resolution problems, and NAT resolution problems. Also, detailed messages for VPN connections are displayed to assist the network administrator with troubleshooting problems with active VPN tunnels. Network Debug information is intended for experienced network administrators.
1024	Syslog Only - For Traffic Reporting	Used for Syslog only to report HTTP connections opened and closed, and bytes transferred.
2048	Dropped LAN TCP	Used for Syslog only to report that the TCP packet is dropped due to LAN management policy.
4096	Dropped LAN UDP	Used for Syslog only to report that the UDP packet is dropped due to LAN management policy.
8192	Dropped LAN ICMP	Used for Syslog only to report that the ICMP packet is dropped due to LAN management policy.
32768	Modem Debug	Logs Modem Debug activity.

Legacy Category Values

ID (used in Syslog)	Name	Description
65536	VPN Tunnel Status	Logs status information on VPN tunnels.
131072	802.11 Management	Logs WLAN IEEE 802.11 connections.
262144	Syslog Only - For Traffic Reporting	Used for Syslog only to report that the Network Traffic is logged when connection is open.
524288	System Environment	Logs system environment activity.
1048576	Expanded - VOIP Activity	Used for Syslog only to log VoIP H.323-RAS, H.323/H.225, and H.323/H.245 activity.
2097152	Expanded - WLAN IDS Activity	Used for Syslog only to log WLAN IDS activity.
4194304	Expanded - SonicPoint Activity	Used for Syslog only to log SonicPoint activity.

Priority Levels

The following table displays the Priority Number and Priority Name for Syslog tags. The value here corresponds to the **Priority Level** column of the Log Event Message Index table, or the **pri** tag in the Syslog Tags table. For example, a tag with "pri=0" means Emergency Priority.

Priority Level

Priority Number	Priority Name
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Info
7	Debug

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

About This Document

Legend

⚠ **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

△ **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

ⓘ **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.