SonicWall® SonicOS 6.5.1 Log Events

Reference Guide

SONICWALL®

1

Introduction to SonicOS Log Events

This reference guide lists and describes the SonicWall® SonicOS log event messages for SonicOS 6.5.1. 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 **INVESTIGATE | Logs | Event Logs** and **MANAGE | Logs & Reporting | Log Settings > Base Setup** pages and the **Enable Logging** option in the **Add** dialog on the **MANAGE | Policies | Rules > Access Rules** page in the SonicOS web based management interface.

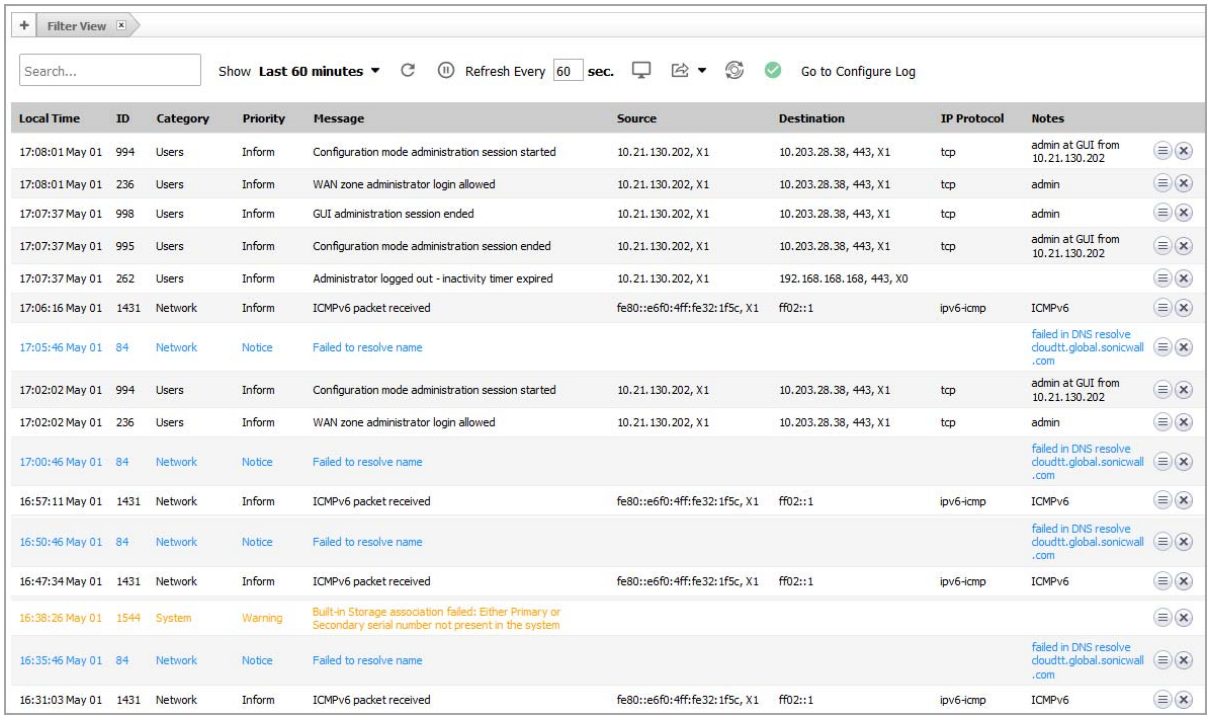
Topics:

Event Logs

The SonicWall security appliance maintains an Event log for tracking potential security threats. This log can be viewed by navigating to the **INVESTIGATE | Logs | Event Logs** page, or 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 configuring the **Event Logs** page, refer to the *SonicOS 6.5 Investigate* administration documentation.

Event Logs Page



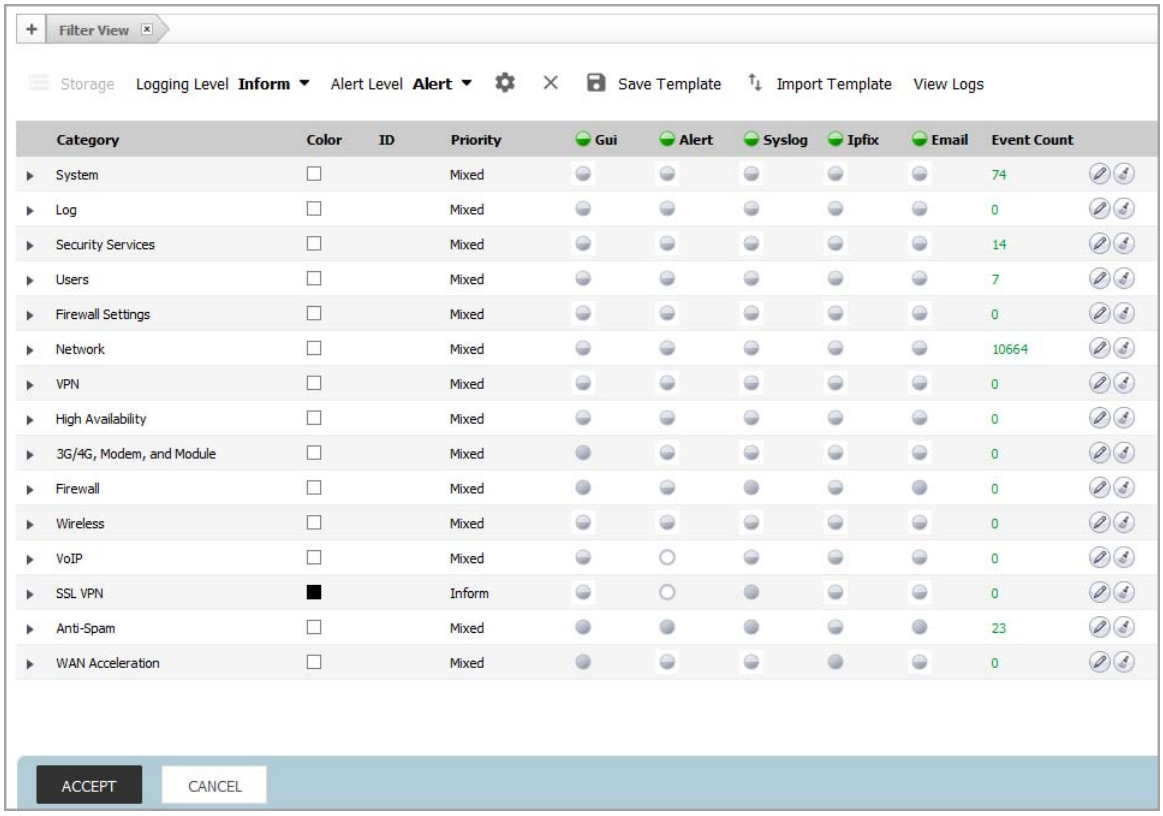
Local Time	ID	Category	Priority	Message	Source	Destination	IP Protocol	Notes
17:08:01 May 01	994	Users	Inform	Configuration mode administration session started	10.21.130.202, X1	10.203.28.38, 443, X1	tcp	admin at GUI from 10.21.130.202
17:08:01 May 01	236	Users	Inform	WAN zone administrator login allowed	10.21.130.202, X1	10.203.28.38, 443, X1	tcp	admin
17:07:37 May 01	998	Users	Inform	GUI administration session ended	10.21.130.202, X1	10.203.28.38, 443, X1	tcp	admin
17:07:37 May 01	995	Users	Inform	Configuration mode administration session ended	10.21.130.202, X1	10.203.28.38, 443, X1	tcp	admin at GUI from 10.21.130.202
17:07:37 May 01	262	Users	Inform	Administrator logged out - inactivity timer expired	10.21.130.202, X1	192.168.168.168, 443, X0		
17:06:16 May 01	1431	Network	Inform	ICMPv6 packet received	fe80::e6f0:4ff:fe32:1f5c, X1	ff02::1	ipv6-icmp	ICMPv6
17:05:46 May 01	84	Network	Notice	Failed to resolve name				failed in DNS resolve cloudtt.global.sonicwall.com
17:02:02 May 01	994	Users	Inform	Configuration mode administration session started	10.21.130.202, X1	10.203.28.38, 443, X1	tcp	admin at GUI from 10.21.130.202
17:02:02 May 01	236	Users	Inform	WAN zone administrator login allowed	10.21.130.202, X1	10.203.28.38, 443, X1	tcp	admin
17:00:46 May 01	84	Network	Notice	Failed to resolve name				failed in DNS resolve cloudtt.global.sonicwall.com
16:57:11 May 01	1431	Network	Inform	ICMPv6 packet received	fe80::e6f0:4ff:fe32:1f5c, X1	ff02::1	ipv6-icmp	ICMPv6
16:50:46 May 01	84	Network	Notice	Failed to resolve name				failed in DNS resolve cloudtt.global.sonicwall.com
16:47:34 May 01	1431	Network	Inform	ICMPv6 packet received	fe80::e6f0:4ff:fe32:1f5c, X1	ff02::1	ipv6-icmp	ICMPv6
16:38:26 May 01	1544	System	Warning	Built-in Storage association failed: Either Primary or Secondary serial number not present in the system				
16:35:46 May 01	84	Network	Notice	Failed to resolve name				failed in DNS resolve cloudtt.global.sonicwall.com
16:31:03 May 01	1431	Network	Inform	ICMPv6 packet received	fe80::e6f0:4ff:fe32:1f5c, X1	ff02::1	ipv6-icmp	ICMPv6

Log Settings Base Setup

The **MANAGE | Logs & Reporting | Log Settings > Base Setup** page allows you to categorize and customize the logging functions on your SonicWall security appliance for troubleshooting and diagnostics.

For more information on configuring and managing the **Log Settings > Base Setup** page, refer to the *SonicOS 6.5 Logs and Reporting* administration documentation.

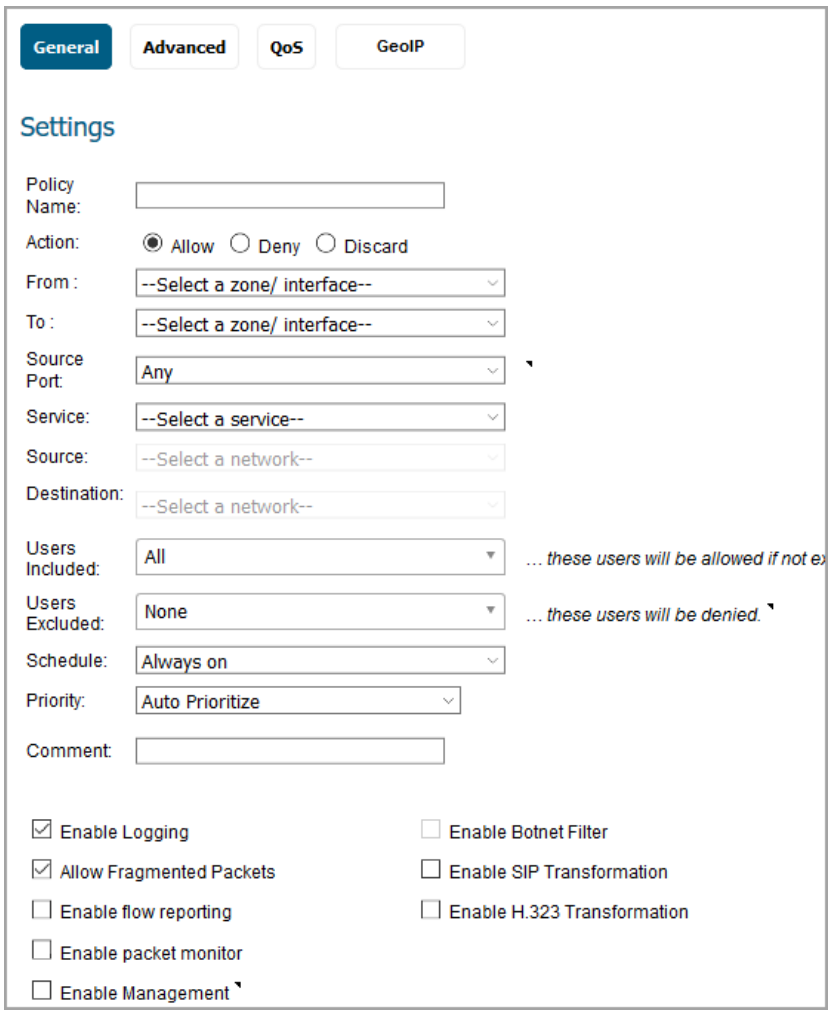
Log Settings > Base Setup Page



Access Rules Logging Control

The **Add Rule** dialog launched by clicking **Add** on the **MANAGE | Policies | Rules > Access Rules** page provides the **Enable Logging** checkbox. This option controls the policy logs; when the option is selected, event messages are logged for that policy, otherwise no messages are logged for it.

Add Rule Dialog with Enable Logging Option



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

Allowed vs Dropped Packets	Syslog ID	Event Message
Packet Allowed Messages:		
	526	Web Request Receiver
	1235	Packet Allowed
Packet Dropped Messages:		
	36	TCP Packets Dropped
	38	ICMP Packets Dropped

Policy Logs Controlled by Enable Logging Option in Access Rules

Allowed vs Dropped Packets	Syslog ID	Event Message
	41	Unknown Protocol Dropped
	173	LAN TCP Deny
	174	LAN UDP Deny
	175	LAN ICMP Deny
	522	Malformed IP Packet
	524	Web Request Drop
	533	ESP Drop
	534	AH Drop
	652	IPcomp Packet Drop
	1253	IPv6 Tunnel Dropped
	1254	LAN ICMPv6 Deny
	1257	ICMPv6 Packets Dropped
	1447	UDPv6 Packets Dropped

The Syslog event logs controlled by the **Enable Logging** option are listed in the Traffic Report Syslogs table. Traffic report Syslogs are generated for ***ALLOW*** policy matches.

Traffic Report Syslogs

Syslog 'c' Value	Syslog ID	Event Message	Comments
c=1024 This means Traffic Reporting, including bytes transferred.	97	Syslog Website Accessed	Has URL data
c=1024	537	Connection Closed	Non-URL traffic
c=1024	1153	SSL VPN Traffic	Statistics reported by SSL VPN
c=1024	1463	DPI-SSL Inspection Cleaned-up	Statistics reported by DPI-SSL
c=262144 This means *Connection Opened* (most probably zero bytes transferred).	98	Connection Opened	It is possible for some packets to trigger a *Connection Opened*, but later be dropped due to policy settings.

2

Index of Log Event Messages

This section contains the Log Event Message Index, which is a list of log event messages for the SonicOS 6.5.1 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 Category Name**—Displays category names as shown in the SonicOS **MANAGE | Logs & Reporting | Log Settings > Base Setup** page in the **Category** column of the table. The **INVESTIGATE | Logs | Event Logs** page also has the **Category** column, which can be displayed (if not already) by clicking the *Display Options* button  at the top and selecting the **Category** checkbox under **General** in the **Select Columns to Display** dialog.
- **SonicOS Group Name**—Displays group names as shown in the SonicOS **MANAGE | Logs & Reporting | Log Settings > Base Setup** page by expanding a category in the **Category** column of the table. The **INVESTIGATE | Logs | Event Logs** page displays the groups in the **Group** column, which can be displayed by clicking the *Display Options* button  at the top and selecting the **Group** checkbox under **General** in the **Select Columns to Display** dialog.
- **Syslog Legacy Category**—Displays the syslog category event type. This is the same category as Legacy Categories on page 99.
- **Priority Level**—Displays the level of urgency of the log event message. For additional information, see Priority Levels on page 100.
- **SNMP Trap Type**—Displays the SNMP Trap ID number of the log event message.
- **Event Name**—Displays a descriptive name for the log event, corresponding to the value in the **Event** column found in the **INVESTIGATE | Logs | Event Logs** page.
- **Log Event Message**—Displays the text of the log event message. Sometimes includes "%s", which is dynamically replaced by SonicOS with descriptive text in the actual log event message.

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
4	System	Status	Maintenance	ALERT	---	Activate Firewall	Network Security Appliance activated
5	Log	General	Maintenance	INFO	---	Clear Log	Log Cleared
6	Log	E-mail	Maintenance	INFO	---	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

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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	---	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	---	Fragmented Packet	Fragmented packet dropped
29	Users	Authentication Access	User Activity	INFO	---	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	---	Successful User Login	User login from an internal zone allowed
32	Users	Authentication Access	User Activity	INFO	---	Wrong User Password	User login denied due to bad credentials
33	Users	Authentication Access	User Activity	INFO	---	Unknown User Login Attempt	User login denied due to bad credentials
34	Users	Authentication Access	User Activity	INFO	---	Login Timeout	Pending login timed out
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	---	TCP Packets Dropped	TCP connection dropped
37	Network	UDP	UDP	NOTICE	---	UDP Packets Dropped	UDP packet dropped
38	Network	ICMP	ICMP	NOTICE	---	ICMP Packets Dropped	ICMP packet dropped due to Policy
41	Network	Network Access	Debug	NOTICE	---	Unknown Protocol Dropped	Unknown protocol dropped

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
43	VPN	VPN IPsec	Debug	DEBUG	---	IPsec Interrupt Error	IPsec connection interrupt
45	Network	ARP	Debug	DEBUG	---	ARP Failure	ARP Timeout
46	Network	Network Access	Debug	DEBUG	---	Broadcast Packets Dropped	Broadcast packet dropped
48	Network	TCP	Debug	DEBUG	---	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	---	ICMP Too Big	Received fragmented packet or fragmentation needed
65	VPN	VPN IPsec	User Activity	INFO	---	Illegal SPI	Illegal IPsec SPI
67	VPN	VPN IPsec	Attack	ERROR	508	IPsec Authenticate Failure	IPsec Authentication Failed
69	VPN	VPN IPsec	User Activity	INFO	---	Incompatible SA	Incompatible IPsec Security Association
70	VPN	VPN IPsec	Attack	ERROR	510	Illegal IPsec Peer	IPsec packet from or to an illegal host
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	---	Name Resolve Failed	Failed to resolve name
87	VPN	VPN IKE	User Activity	INFO	---	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)

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
89	VPN	VPN IKE	User Activity	INFO	---	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	GMS	Maintenance	INFO	---	GMS Heartbeat	Status
97	Log	Syslog	Connection Traffic	INFO	---	Syslog Website Accessed	Web site hit
98	Network	Network Access	Connection	INFO	---	Connection Opened	Connection Opened
99	Network	DHCP Client	Maintenance	INFO	---	DHCPC Retransmit Discover	Retransmitting DHCP DISCOVER.
100	Network	DHCP Client	Maintenance	INFO	---	DHCPC Retransmit Request	Retransmitting DHCP Request (Requesting).
101	Network	DHCP Client	Maintenance	INFO	---	DHCPC Retransmit Request Renew	Retransmitting DHCP Request (Renewing).
102	Network	DHCP Client	Maintenance	INFO	---	DHCPC Retransmit Request Rebind	Retransmitting DHCP Request (Rebinding).
103	Network	DHCP Client	Maintenance	INFO	---	DHCPC Retransmit Request Reboot	Retransmitting DHCP Request (Rebooting).
104	Network	DHCP Client	Maintenance	INFO	---	DHCPC Retransmit Request Verify	Retransmitting DHCP Request (Verifying).
105	Network	DHCP Client	Maintenance	INFO	---	DHCPC Discover	Sending DHCP DISCOVER.
106	Network	DHCP Client	Maintenance	INFO	---	DHCPC No Offer	DHCP Server not available. Did not get any DHCP OFFER.
107	Network	DHCP Client	Maintenance	INFO	---	DHCPC Offer Receive	Got DHCP OFFER. Selecting.
108	Network	DHCP Client	Maintenance	INFO	---	DHCPC Selecting	Sending DHCP Request.

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
109	Network	DHCP Client	Maintenance	INFO	---	DHCPC Request Failed	DHCP Client did not get DHCP ACK.
110	Network	DHCP Client	Maintenance	INFO	---	DHCPC Request NAK	DHCP Client got NACK.
111	Network	DHCP Client	Maintenance	INFO	---	DHCPC Request ACK	DHCP Client got ACK from server.
112	Network	DHCP Client	Maintenance	INFO	---	DHCPC Request Decline	DHCP Client is declining address offered by the server.
113	Network	DHCP Client	Maintenance	INFO	---	DHCPC Bound Rebind	DHCP Client sending Request and going to REBIND state.
114	Network	DHCP Client	Maintenance	INFO	---	DHCPC Bound Renew	DHCP Client sending Request and going to RENEW state.
115	Network	DHCP Client	Maintenance	INFO	---	DHCPC Request Renew	Sending DHCP Request (Renewing).
116	Network	DHCP Client	Maintenance	INFO	---	DHCPC Request Rebind	Sending DHCP Request (Rebinding).
117	Network	DHCP Client	Maintenance	INFO	---	DHCPC Request Reboot	Sending DHCP Request (Rebooting).
118	Network	DHCP Client	Maintenance	INFO	---	DHCPC Request Verify	Sending DHCP Request (Verifying).
119	Network	DHCP Client	Maintenance	INFO	---	DHCPC Verify Initiation Failed	DHCP Client failed to verify and lease has expired. Go to INIT state.
121	Network	DHCP Client	Maintenance	INFO	---	DHCPC Get New IP	DHCP Client got a new IP address lease.
122	Network	DHCP Client	Maintenance	INFO	---	DHCPC Send Release	Sending DHCP RELEASE.
123	Security Services	Anti-Virus	Maintenance	INFO	---	AV Access Without Agent	Access attempt from host without Anti-Virus agent installed
124	Security Services	Anti-Virus	Maintenance	INFO	---	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	---	PPPoE Start	Starting PPPoE discovery
128	Network	PPPoE	Maintenance	INFO	---	PPPoE Link Up	PPPoE LCP Link Up

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
129	Network	PPPoE	Maintenance	INFO	---	PPPoE Link Down	PPPoE LCP Link Down
130	Network	PPPoE	Maintenance	INFO	---	PPPoE Link Finish	PPPoE terminated
131	Network	PPPoE	Maintenance	INFO	---	PPPoE Network Up	PPPoE Network Connected
132	Network	PPPoE	Maintenance	INFO	---	PPPoE Network Down	PPPoE Network Disconnected
133	Network	PPPoE	Maintenance	INFO	---	PPPoE Discover Complete	PPPoE discovery process complete
134	Network	PPPoE	Maintenance	INFO	---	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	---	XAUTH Success	XAUTH Succeeded with VPN %s
140	VPN	VPN Client	User Activity	ERROR	---	XAUTH Failure	XAUTH Failed with VPN %s, Authentication failure
141	VPN	VPN Client	User Activity	INFO	---	XAUTH Timeout	XAUTH Failed with VPN client, Cannot Contact %s Server
142	Log	General	Debug	ERROR	---	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
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

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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	---	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	---	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	---	PPPoE Traffic Timeout	Disconnecting PPPoE due to traffic Timeout
169	Network	PPPoE	Maintenance	INFO	---	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
171	VPN	VPN IKE	User Activity	DEBUG	---	IPsec Dead Peer Detection	%s
173	Network	TCP	LAN TCP	NOTICE	---	LAN TCP Deny	TCP connection from LAN denied
174	Network	UDP	LAN UDP | LAN TCP	NOTICE	---	LAN UDP Deny	UDP packet from LAN dropped
175	Network	ICMP	LAN ICMP | LAN TCP	NOTICE	---	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	---	TCP FIN Drop	TCP FIN packet dropped

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
182	Network	ICMP	User Activity	INFO	---	Path MTU Receive	Received a path MTU ICMP message from router/gateway
188	Network	ICMP	User Activity	INFO	---	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	---	Admin Login From CLI	CLI administrator login allowed
200	Users	Authentication Access	User Activity	WARNING	---	Admin Password Error From CLI	CLI administrator login denied due to bad credentials
201	Network	L2TP Client	Maintenance	INFO	---	L2TP Tunnel Start	L2TP Tunnel Negotiation Started
202	Network	L2TP Client	Maintenance	INFO	---	L2TP Session Start	L2TP Session Negotiation Started
204	Network	L2TP Client	Maintenance	INFO	---	L2TP Tunnel Finish	L2TP Tunnel Established
205	Network	L2TP Client	Maintenance	INFO	---	L2TP Tunnel Disconect From Remote	L2TP Tunnel Disconnect from Remote
206	Network	L2TP Client	Maintenance	INFO	---	L2TP Session Success	L2TP Session Established
207	Network	L2TP Client	Maintenance	INFO	---	L2TP Session Disconnect From Remote	L2TP Session Disconnect from Remote
208	Network	L2TP Client	Maintenance	INFO	---	L2TP PPP Start	L2TP PPP Negotiation Started
210	Network	L2TP Client	Maintenance	INFO	---	L2TP PPP Up	L2TP PPP Session Up
211	Network	L2TP Client	Maintenance	INFO	---	L2TP Net Down	L2TP PPP Down
212	Network	L2TP Client	Maintenance	INFO	---	L2TP PPP Authenticate Failed	L2TP PPP Authentication Failed
215	Network	L2TP Client	Maintenance	INFO	---	L2TP Traffic Timeout	Disconnecting L2TP Tunnel due to traffic Timeout
217	Network	L2TP Client	Maintenance	INFO	---	L2TP PPP Down	L2TP PPP link down

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
222	VPN	DHCP Relay	Maintenance	INFO	---	DHCPR Remote Release	DHCP RELEASE relayed to Central Gateway
223	VPN	DHCP Relay	Maintenance	INFO	---	DHCPR Remote ACK	DHCP lease relayed to local device
224	VPN	DHCP Relay	Debug	INFO	---	DHCPR Central Release	DHCP RELEASE received from remote device
225	VPN	DHCP Relay	Debug	INFO	---	DHCPR Central ACK	DHCP lease relayed to remote device
226	VPN	DHCP Relay	Maintenance	INFO	---	DHCPR IP Conflict	DHCP lease to LAN device conflicts with remote device, deleting remote IP entry
227	VPN	DHCP Relay	Maintenance	INFO	---	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	---	DHCPR IP Drop	DHCP lease dropped. Lease from Central Gateway conflicts with Relay IP
229	VPN	DHCP Relay	Attack	ERROR	533	DHCPR IP Spoof	IP spoof detected on packet to Central Gateway, packet dropped
230	VPN	DHCP Relay	Maintenance	INFO	---	DHCPR Get Remote IP Table	Request for Relay IP Table from Central Gateway
231	VPN	DHCP Relay	Maintenance	INFO	---	DHCPR Get Central IP Table	Requesting Relay IP Table from Remote Gateway
232	VPN	DHCP Relay	Maintenance	INFO	---	DHCPR Send Remote IP Table	Sent Relay IP Table to Central Gateway
233	VPN	DHCP Relay	Maintenance	INFO	---	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

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
235	Users	Authentication Access	User Activity	INFO	---	Admin VPN Login	VPN zone administrator login allowed
236	Users	Authentication Access	User Activity	INFO	---	Admin WAN Login	WAN zone administrator login allowed
237	Users	Authentication Access	User Activity	INFO	---	User VPN Login	VPN zone remote user login allowed
238	Users	Authentication Access	User Activity	INFO	---	User WAN Login	WAN zone remote user login allowed
239	VPN	VPN IKE	User Activity	INFO	---	VPN Peer Behind NAT Device	NAT Discovery : Peer IPsec Security Gateway behind a NAT/NAPT Device
240	VPN	VPN IKE	User Activity	INFO	---	VPN Local Behind NAT Device	NAT Discovery : Local IPsec Security Gateway behind a NAT/NAPT Device
241	VPN	VPN IKE	User Activity	INFO	---	VPN No NAT Device Detected	NAT Discovery : No NAT/NAPT device detected between IPsec Security gateways
242	VPN	VPN IKE	User Activity	INFO	---	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	---	User Login Failed	User login denied - RADIUS authentication failure
244	Users	Radius Authentication	User Activity	WARNING	---	User Login Timeout	User login denied - RADIUS server Timeout
245	Users	Radius Authentication	User Activity	WARNING	---	User Login Error	User login denied - RADIUS configuration error
246	Users	Authentication Access	User Activity	INFO	---	User Login From Wrong Location	User login denied - User has no privileges for login from that location
247	VPN	VPN IPsec	Maintenance	INFO	---	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

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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	WARNING	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	WARNING	541	Tunnel Terminates Inside	IKE Responder: Tunnel terminates inside firewall but proposed local network is not inside firewall
256	VPN	VPN IKE	User Activity	WARNING	542	Tunnel Terminates DMZ	IKE Responder: Tunnel terminates on DMZ but proposed local network is on LAN
257	VPN	VPN IKE	User Activity	WARNING	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

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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	---	Admin Logout	Administrator logged out
262	Users	Authentication Access	User Activity	INFO	---	Admin Logout - Timer Expire	Administrator logged out - inactivity timer expired
263	Users	Authentication Access	User Activity	INFO	---	User Logout	User logged out - %s
264	Users	Authentication Access	User Activity	INFO	---	User Logout - Max Session	User logged out - max session time exceeded
265	Users	Authentication Access	User Activity	INFO	---	User Logout - Timer Expire	User logged out - inactivity timer expired
266	VPN	VPN IPsec	Maintenance	INFO	---	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	---	CRL Request	Requesting CRL from
270	VPN	VPN PKI	User Activity	INFO	---	CRL Download Success	CRL loaded from
271	VPN	VPN PKI	User Activity	ALERT	---	CRL Download Failed	Failed to get CRL from
272	VPN	VPN PKI	User Activity	WARNING	---	CRL Failed - No Memory	Not enough memory to hold the CRL
273	VPN	VPN PKI	User Activity	ALERT	---	CRL Failed - Timeout	Connection timed out
274	VPN	VPN PKI	User Activity	ALERT	---	CRL Failed - No Connect	Cannot connect to the CRL server
275	VPN	VPN PKI	User Activity	ERROR	---	CRL Failed - No Reason	Unknown reason
276	VPN	VPN PKI	User Activity	ALERT	---	CRL Process Failed	Failed to Process CRL from
277	VPN	VPN PKI	User Activity	ALERT	---	CRL Bad Format	Bad CRL format
278	VPN	VPN PKI	User Activity	ALERT	---	CRL Wrong Issuer	Issuer match failed

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
279	VPN	VPN PKI	User Activity	ALERT	---	CRL Certificate Revoke	Certificate on Revoked list(CRL)
280	VPN	VPN PKI	User Activity	ALERT	---	No Certificate	No Certificate for
281	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	PPP Dial Up	PPP Dial-Up: Dialing: %s
282	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	PPP No Dialtone	PPP Dial-Up: No dial tone detected - check phone-line connection
283	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	PPP No Carrier	PPP Dial-Up: No link carrier detected - check phone number
284	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	PPP Peer Number Busy	PPP Dial-Up: Dialed number is busy
285	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	PPP No Answer	PPP Dial-Up: Dialed number did not answer
286	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	Start PPP	PPP Dial-Up: Connected at %s bps - starting PPP
287	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	PPP Failure	PPP Dial-Up: Unknown dialing failure
288	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	PPP Disconnect	PPP Dial-Up: Link carrier lost
289	Network	PPP	---	INFO	---	PPP Authenticate Success	PPP: Authentication successful
290	Network	PPP	---	INFO	---	PPP PAP Failed	PPP: PAP Authentication failed - check username / password
291	Network	PPP	---	INFO	---	PPP CHAP Failed	PPP: CHAP authentication failed - check username / password

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
292	Network	PPP	---	INFO	---	PPP MS-CHAP Failed	PPP: MS-CHAP authentication failed - check username / password
293	Network	PPP	---	INFO	---	PPP MS-CHAP Start	PPP: Starting MS-CHAP authentication
294	Network	PPP	---	INFO	---	PPP CHAP Start	PPP: Starting CHAP authentication
295	Network	PPP	---	INFO	---	PPP PAP Start	PPP: Starting PAP authentication
299	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	PPP IP Update	PPP Dial-Up: Received new IP address
300	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	PPP Link Establish	PPP Dial-Up: PPP link established
301	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	PPP Link Down	PPP Dial-Up: PPP link down
302	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	PPP Link Closing	PPP Dial-Up: Shutting down link
303	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	PPP Initialization	PPP Dial-Up: Initialization : %s
306	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	PPP Dial Cancel	PPP Dial-Up: Connect request canceled
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	---	L2TP Tunnel Establish	L2TP Server : L2TP Tunnel Established.
309	VPN	L2TP Server	Maintenance	INFO	---	L2TP Session Establish	L2TP Server : L2TP Session Established.
311	VPN	L2TP Server	Maintenance	INFO	---	L2TP Radius Authentication Failure	L2TP Server: RADIUS/LDAP reports Authentication Failure

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
312	VPN	L2TP Server	Maintenance	INFO	---	L2TP Local Authentication Failure	L2TP Server: Local Authentication Failure
318	VPN	L2TP Server	Maintenance	INFO	---	L2TP Local Authentication Success	L2TP Server: Local Authentication Success.
319	VPN	L2TP Server	Maintenance	INFO	---	L2TP Radius Authentication Success	L2TP Server: RADIUS/LDAP Authentication Success
321	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	PPP Manual Action Needed	PPP Dial-Up: Manual intervention needed. Check Primary Profile or Profile details
322	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	PPP Profile is Manual	PPP Dial-Up: Trying to failover but Primary Profile is manual
326	Network	Failover and Load Balancing	System Error	ALERT	637	Probe Failed	Probing failure on %s
327	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	PPP Max Connection Exceed	PPP Dial-Up: Maximum connection time exceeded - disconnecting
328	Users	Authentication Access	Maintenance	INFO	---	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
330	3G/4G, Modem, and Module	PPP Dial-Up	Maintenance	INFO	---	Disable VPN Network	PPP Dial-Up: The profile in use disabled VPN networking.
331	3G/4G, Modem, and Module	PPP Dial-Up	Maintenance	INFO	---	Enable VPN Network	PPP Dial-Up: VPN networking restored.
335	VPN	L2TP Server	Maintenance	INFO	---	L2TPS Tunnel Disconnect From Remote	L2TP Server: Tunnel Disconnect from Remote.
336	VPN	L2TP Server	Maintenance	INFO	---	L2TPS Tunnel Delete	L2TP Server : Deleting the Tunnel

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
337	VPN	L2TP Server	Maintenance	INFO	---	L2TPS Session Delete	L2TP Server : Deleting the L2TP active Session
338	VPN	L2TP Server	Maintenance	INFO	---	L2TPS Retransmissio n Timeout	L2TP Server : Retransmission Timeout, Deleting the Tunnel
339	Network	NAT	Debug	DEBUG	---	NAT Overwrite	NAT translated packet exceeds size limit, packet dropped
340	System	Administration	Maintenance	INFO	---	HTTP Port Change	HTTP management port has changed
341	System	Administration	Maintenance	INFO	---	HTTPS Port Change	HTTPS management port has changed
344	VPN	L2TP Server	Maintenance	INFO	---	L2TPS Authentication Local Failure	L2TP Server : User Name authentication Failure locally.
346	VPN	VPN IKE	User Activity	INFO	---	Quick Mode Started	IKE Initiator: Start Quick Mode (Phase 2).
347	Network	Network Access	TCP | UDP | ICMP	WARNING	---	Drop Clear Packet	Port configured to receive IPsec protocol ONLY; drop packet received in the clear
348	VPN	VPN IPsec	Maintenance	WARNING	---	VPN SA Import Invalid	Imported VPN SA is invalid - disabled
350	VPN	VPN IKE	User Activity	INFO	---	IKE SA Life Expired	IKE SA lifetime expired.
351	VPN	VPN IKE	User Activity	INFO	---	IKE Main Mode Started	IKE Initiator: Start Main Mode negotiation (Phase 1)
352	VPN	VPN IKE	User Activity	INFO	---	IKE Quick Mode Request Received	IKE Responder: Received Quick Mode Request (Phase 2)
353	VPN	VPN IKE	User Activity	INFO	---	Initial Main Mode Completed	IKE Initiator: Main Mode complete (Phase 1)
354	VPN	VPN IKE	User Activity	INFO	---	Initial Aggressive Mode Completed	IKE Initiator: Aggressive Mode complete (Phase 1).
355	VPN	VPN IKE	User Activity	INFO	---	Responder Main Mode Request Received	IKE Responder: Received Main Mode Request (Phase 1)

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
356	VPN	VPN IKE	User Activity	INFO	---	Responder Aggressive Mode Request Received	IKE Responder: Received Aggressive Mode Request (Phase 1)
357	VPN	VPN IKE	User Activity	INFO	---	Responder Main Mode Completed	IKE Responder: Main Mode complete (Phase 1)
358	VPN	VPN IKE	User Activity	INFO	---	Aggressive Mode Started	IKE Initiator: Start Aggressive Mode negotiation (Phase 1)
360	Security Services	Crypto Test	Maintenance	ERROR	---	DES Test Failed	Crypto DES test failed
361	Security Services	Crypto Test	Maintenance	ERROR	---	DH Test Failed	Crypto DH test failed
362	Security Services	Crypto Test	Maintenance	ERROR	---	HMAC-MD5 Test Failed	Crypto Hmac-MD5 test failed
363	Security Services	Crypto Test	Maintenance	ERROR	---	HMAC-SHA1 Test Failed	Crypto Hmac-Sha1 test failed
364	Security Services	Crypto Test	Maintenance	ERROR	---	RSA Test Failed	Crypto RSA test failed
365	Security Services	Crypto Test	Maintenance	ERROR	---	SHA1 Test Failed	Crypto Sha1 test failed
366	Security Services	Crypto Test	Maintenance	ERROR	---	Hardware DES Test Failed	Crypto hardware DES test failed
367	Security Services	Crypto Test	Maintenance	ERROR	---	Hardware 3DES Test Failed	Crypto hardware 3DES test failed
368	Security Services	Crypto Test	Maintenance	ERROR	---	Hardware DES-SHA Test Failed	Crypto hardware DES with SHA test failed
369	Security Services	Crypto Test	Maintenance	ERROR	---	Hardware 3DES-SHA Test Failed	Crypto Hardware 3DES with SHA test failed
371	VPN	VPN Client	User Activity	INFO	---	Client Policy Provisioned	VPN Client Policy Provisioning
372	VPN	VPN IKE	User Activity	INFO	---	IKE Initiator: Accept Proposal	IKE Initiator: Accepting IPsec proposal (Phase 2)
373	VPN	VPN IKE	User Activity	INFO	---	IKE Responder: Aggressive Mode Complete	IKE Responder: Aggressive Mode complete (Phase 1)
375	Network	PPTP	Maintenance	INFO	---	Start Control Connection Negotiation	PPTP Control Connection Negotiation Started

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
376	Network	PPTP	Maintenance	INFO	---	Start Session Negotiation	PPTP Session Negotiation Started
378	Network	PPTP	Maintenance	INFO	---	PPTP Control Establish	PPTP Control Connection Established
379	Network	PPTP	Maintenance	INFO	---	PPTP Remote Disconnect Tunnel	PPTP Tunnel Disconnect from Remote
380	Network	PPTP	Maintenance	INFO	---	PPTP Session Success	PPTP Session Established
381	Network	PPTP	Maintenance	INFO	---	PPTP Remote Disconnect Session	PPTP Session Disconnect from Remote
382	Network	PPTP	Maintenance	INFO	---	PPP Start	PPTP PPP Negotiation Started
384	Network	PPTP	Maintenance	INFO	---	PPP Up	PPTP PPP Session Up
385	Network	PPTP	Maintenance	INFO	---	PPP Down	PPTP PPP Down
388	Network	PPTP	Maintenance	INFO	---	PPTP User Diconnect	PPTP Disconnect Initiated by the User
389	Network	PPTP	Maintenance	INFO	---	PPTP Traffic Timeout	Disconnecting PPTP Tunnel due to traffic Timeout
390	Network	PPTP	Maintenance	INFO	---	PPTP User Connect	PPTP Connect Initiated by the User
392	Network	PPTP	Maintenance	INFO	---	PPTP CHAP Authentication	PPTP starting CHAP Authentication
393	Network	PPTP	Maintenance	INFO	---	PPTP PAP Authentication	PPTP starting PAP Authentication
396	Network	PPTP	Maintenance	INFO	---	PPTP Authentication ACK	PPTP PAP Authentication success.
398	Network	PPTP	Maintenance	INFO	---	PPTP PPP Link Up	PPTP PPP Link Up
399	Network	PPTP	Maintenance	INFO	---	PPTP PPP Link Down	PPTP PPP Link down
400	Network	PPTP	Maintenance	INFO	---	PPTP PPP Link Finish	PPTP PPP Link Finished
401	VPN	VPN IKE	User Activity	WARNING	---	No Proposal Chosen	Received notify. NO_PROPOSAL_CHOSEN
402	VPN	VPN IKE	User Activity	WARNING	---	Proposal Rejected	IKE Responder: IKE proposal does not match (Phase 1)

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
403	VPN	VPN IKE	User Activity	INFO	---	Negotiation Aborted	IKE negotiation aborted due to Timeout
404	VPN	VPN IKE	User Activity	WARNING	---	Decryption Failed: Key Mismatch	Failed payload verification after decryption; possible preshared key mismatch
405	VPN	VPN IKE	User Activity	WARNING	---	Payload Validation Failed	Failed payload validation
406	VPN	VPN IKE	User Activity	WARNING	---	Duplicate Packet Dropped	Received packet retransmission. Drop duplicate packet
408	Security Services	Anti-Virus	Maintenance	INFO	---	AV License Exceeded	Anti-Virus Licenses Exceeded
409	VPN	VPN IKE	User Activity	WARNING	---	Authentication Failed	Received notify: ISAKMP_AUTH_FAILED
410	VPN	VPN IKE	User Activity	WARNING	---	Hash Failed	Computed hash does not match hash received from peer; preshared key mismatch
411	VPN	VPN IKE	User Activity	WARNING	---	Notification on Malformed Payload	Received notify: PAYLOAD_MALFORMED
412	VPN	VPN IKE	User Activity	INFO	---	Receive IPsec Delete Request	Received IPsec SA delete request
413	VPN	VPN IKE	User Activity	INFO	---	Receive IKE Delete Request	Received IKE SA delete request
414	VPN	VPN IKE	User Activity	INFO	---	Invalid Cookies	Received notify: INVALID_COOKIES
415	VPN	VPN IKE	User Activity	INFO	---	Notification on Responder Lifetime	Received notify: RESPONDER_LIFETIME
416	VPN	VPN IKE	User Activity	INFO	---	Notification on Invalid SPI	Received notify: INVALID_SPI
419	Network	RIP	Maintenance	INFO	8401	LAN RIP Disable	RIP disabled on interface %s
420	Network	RIP	Maintenance	INFO	8402	LAN RIPv1 Enable	RIPv1 enabled on interface %s
421	Network	RIP	Maintenance	INFO	8403	LAN RIPv2 Enable	RIPv2 enabled on interface %s

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
422	Network	RIP	Maintenance	INFO	8404	LAN RIPv2c Enable	RIPv2 compatibility (broadcast) mode enabled on interface %s
427	VPN	VPN IPsec	VPN Tunnel Status	INFO	801	IPsec Tunnel Status Changed	IPsec Tunnel status changed
428	Firewall Settings	Advanced	Debug	WARNING	---	Drop Source Route Packet	Source routed IP packet dropped
429	Network	PPTP	Maintenance	INFO	---	PPTP Disconnect Echo Request	No response from server to Echo Requests, disconnecting PPTP Tunnel
430	Network	PPTP	Maintenance	INFO	---	PPTP Disconnect Control Connection Request	No response from PPTP server to control connection requests
431	Network	PPTP	Maintenance	INFO	---	PPTP Disconnect Session Request	No response from PPTP server to call requests
432	Network	PPTP	Maintenance	INFO	---	PPTP Disconnect Control Connection Reject	PPTP server rejected control connection
433	Network	PPTP	Maintenance	INFO	---	PPTP Disconnect Session Reject	PPTP server rejected the call request
434	Network	Failover and Load Balancing	User Activity	INFO	---	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	---	User Login Lockout Expired	Locked-out user logins allowed - lockout period expired

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
439	Users	Authentication Access	User Activity	INFO	---	User Login Lockout Clear	Locked-out user logins allowed by %s
440	Firewall	Access Rules	User Activity	INFO	---	Rule Added	Access rule added
441	Firewall	Access Rules	User Activity	INFO	---	Rule Modified	Access rule viewed or modified
442	Firewall	Access Rules	User Activity	INFO	---	Rule Deleted	Access rule deleted
444	Network	PPTP	Maintenance	INFO	---	PPTP Server Down	PPTP Server is not responding, check if the server is UP and running.
445	VPN	VPN IKE	User Activity	INFO	---	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	---	PKI Output Buffer Failure	PKI Failure: Output buffer too small
449	VPN	VPN PKI	Maintenance	ERROR	---	PKI Allocate Memory Failure	PKI Failure: Cannot alloc memory
450	VPN	VPN PKI	Maintenance	ERROR	---	PKI Certificate Failure	PKI Failure: Reached the limit for local certs, cant load any more
451	VPN	VPN PKI	Maintenance	ERROR	---	PKI Import Failure	PKI Failure: Import failed
452	VPN	VPN PKI	Maintenance	ERROR	---	PKI Bad Password	PKI Failure: Incorrect admin password
453	VPN	VPN PKI	Maintenance	ERROR	---	PKI CA Certificate Failure	PKI Failure: CA certificates store exceeded. Cannot verify this Local Certificate
454	VPN	VPN PKI	Maintenance	ERROR	---	PKI Import File Format Failure	PKI Failure: Improper file format. Please select PKCS#12 (*.p12) file
455	VPN	VPN PKI	Maintenance	ERROR	---	PKI Certificate ID Failure	PKI Failure: Certificate's ID does not match this Network Security Appliance
456	VPN	VPN PKI	Maintenance	ERROR	---	PKI Key Mismatch	PKI Failure: public-private key mismatch

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
457	VPN	VPN PKI	Maintenance	ERROR	---	PKI Local Certificate Name Duplicate	PKI Failure: Duplicate local certificate name
458	VPN	VPN PKI	Maintenance	ERROR	---	PKI Local Certificate Duplicate	PKI Failure: Duplicate local certificate
459	VPN	VPN PKI	Maintenance	ERROR	---	PKI No Certificate	PKI Failure: No CA certificates yet loaded
460	VPN	VPN PKI	Maintenance	ERROR	---	PKI Internal Error	PKI Failure: Internal error
461	VPN	VPN PKI	Maintenance	ERROR	---	PKI No Resource	PKI Failure: Temporary memory shortage, try again
462	VPN	VPN PKI	Maintenance	ERROR	---	PKI Certificate Chain Circular	PKI Failure: The certificate chain is circular
463	VPN	VPN PKI	Maintenance	ERROR	---	PKI Certificate Chain Incomplete	PKI Failure: The certificate chain is incomplete
464	VPN	VPN PKI	Maintenance	ERROR	---	PKI Certificate Chain No Root	PKI Failure: The certificate chain has no root
465	VPN	VPN PKI	Maintenance	ERROR	---	PKI Certificate Expire	PKI Failure: Certificate expiration
466	VPN	VPN PKI	Maintenance	ERROR	---	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	ERROR	---	PKI Certificate Corrupt	PKI Failure: The certificate or a certificate in the chain is corrupt
468	VPN	VPN PKI	Maintenance	ERROR	---	PKI Certificate Bad Signature	PKI Failure: The certificate or a certificate in the chain has a bad signature
469	VPN	VPN PKI	Maintenance	ERROR	---	PKI Certificate Not Verified	PKI Failure: Loaded but could not verify certificate

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
470	VPN	VPN PKI	Maintenance	ERROR	---	PKI Certificate Chain Not Verified	PKI Warning: Loaded the certificate but could not verify its chain
473	VPN	DHCP Relay	Debug	INFO	---	Remote: DHCP Request	DHCP REQUEST received from remote device
474	VPN	DHCP Relay	Debug	INFO	---	Remote: DHCP Discover	DHCP DISCOVER received from remote device
476	VPN	DHCP Relay	Debug	INFO	---	Server: DHCP Offer	DHCP OFFER received from server
477	VPN	DHCP Relay	Debug	INFO	---	Server: DHCP Nack	DHCP NACK received from server
481	3G/4G, Modem, and Module	PPP Dial-Up	Maintenance	INFO	---	PPP No Peer IP	PPP Dial-Up: No peer IP address from Dial-Up ISP, local and remote IPs will be the same
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	---	Invalid ID	Received notify: INVALID_ID_INFO
484	VPN	DHCP Relay	Maintenance	WARNING	---	DHCP Release Drop	DHCP lease dropped. Lease from Central Gateway conflicts with Remote Management IP
486	Users	Authentication Access	User Activity	INFO	---	WLAN User Login Deny	User login denied - User has no privileges for guest service
488	Wireless	Network Access	TCP | UDP | ICMP	WARNING	---	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	---	ISDN Update	ISDN Driver Firmware successfully updated

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
494	VPN	VPN Client	System Error	INFO	658	GVC License Exceed	Global VPN Client License Exceeded: Connection denied.
496	Security Services	General	Maintenance	WARNING	---	DEA Registration	Registration Update Needed, Please restore your existing security service subscriptions.
502	Network	Interfaces	Maintenance	INFO	---	WAN Not Ready	WAN not ready
505	VPN	VPN Client	System Error	ERROR	660	Blocked Quick Mode With Default Key ID	Blocked Quick Mode for Client using Default KeyId
506	Users	Authentication Access	Maintenance	INFO	---	VPN Disabled	VPN disabled by administrator
507	Users	Authentication Access	Maintenance	INFO	---	VPN Enabled	VPN enabled by administrator
508	Users	Authentication Access	Maintenance	INFO	---	WLAN Disabled	WLAN disabled by administrator
509	Users	Authentication Access	Maintenance	INFO	---	WLAN Enabled	WLAN enabled by administrator
518	Wireless	WLAN	802.11b Managemen t	INFO	---	WLAN 802.11 Management	802.11 Management
520	Users	Authentication Access	User Activity	INFO	---	Admin Logout From CLI	CLI administrator logged out
521	System	Status	Maintenance	INFO	---	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	---	No Match ICMP Drop	ICMP packet dropped no match
524	Network	Network Access	TCP	NOTICE	---	Web Request Drop	Web access Request dropped
526	Network	Network Access	User Activity	NOTICE	---	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.

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
529	VPN	VPN Client	System Error	INFO	643	GVC Not Authorized	Global VPN Client connection is not allowed. Appliance is not registered.
533	VPN	VPN IPsec	TCP | UDP | ICMP	NOTICE	---	ESP Drop	IPsec (ESP) packet dropped
534	VPN	VPN IPsec	TCP | UDP | ICMP	NOTICE	---	AH Drop	IPsec (AH) packet dropped
535	VPN	VPN IPsec	Debug	DEBUG	---	ESP Connection Drop	IPsec (ESP) packet dropped; waiting for pending IPsec connection
537	Network	Network Access	Connection Traffic	INFO	---	Connection Closed	Connection Closed
538	Firewall Settings	FTP	Attack	ALERT	557	FTP Data Port	FTP: Data connection from non default port dropped
542	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	Duration	PPP Dial-Up: Previous session was connected for %s
543	VPN	VPN IKE	User Activity	INFO	---	Negotiation on Second GW	IKE Initiator: Using secondary gateway to negotiate
544	VPN	VPN IKE	User Activity	INFO	---	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	INFO	---	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	INFO	---	WLAN Guest Limit	User login failed - Guest service limit reached

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
550	Users	Authentication Access	User Activity	INFO	---	WLAN Session Timeout	User Session Quota Expired
551	Users	Authentication Access	User Activity	INFO	---	WLAN Account Timeout	Guest Account Timeout
557	Users	Authentication Access	User Activity	INFO	---	WLAN Guest Already Login	Guest login denied. Guest '%s' is already logged in. Please try again later.
558	Users	Authentication Access	User Activity	INFO	---	WLAN Guest Create	Guest account '%s' created
559	Users	Authentication Access	User Activity	INFO	---	WLAN Guest Delete	Guest account '%s' deleted
560	Users	Authentication Access	User Activity	INFO	---	WLAN Guest Disable	Guest account '%s' disabled
561	Users	Authentication Access	User Activity	INFO	---	WLAN Guest Re-enable	Guest account '%s' re-enabled
562	Users	Authentication Access	User Activity	INFO	---	WLAN Guest Prune	Guest account '%s' pruned
564	Users	Authentication Access	User Activity	INFO	---	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
567	Network	Interfaces	Maintenance	INFO	---	Multi-Interface Shutdown	Interface IP Assignment changed: Shutting down %s
568	Network	Interfaces	Maintenance	INFO	---	Multi-Interface Bind Initiate	Interface IP Assignment : Binding and initializing %s
569	Network	Interfaces	Maintenance	INFO	---	Network Overlap	Network for interface %s overlaps with another interface.
570	Network	Interfaces	Maintenance	INFO	---	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

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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	---	WLB Spill-Over Start	WLB Spill-over started, configured threshold exceeded
582	Network	Failover and Load Balancing	Maintenance	WARNING	---	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
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	---	Header Verification Failed	Header verification failed
588	Network	DHCP Client	Maintenance	INFO	---	Offer Error	Received DHCP offer packet has errors
589	Network	DHCP Client	Maintenance	INFO	---	Request Response Error	Received response packet for DHCP request has errors
590	Network	Network Access	LAN UDP | LAN TCP	NOTICE	---	LAN IP Deny	IP type %s packet dropped
591	3G/4G, Modem, and Module	PPP Dial-Up	Attack	ERROR	566	Max Failed Dials	Maximum sequential failed dial attempts (10) to a single dial-up number: %s
592	3G/4G, Modem, and Module	PPP Dial-Up	Attack	ERROR	567	30 Mins Dial Delay	Regulatory requirements prohibit %s from being re-dialed for 30 minutes

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
593	Network	PPPoE	Maintenance	INFO	---	Receive PAD Offer	Received PPPoE Active Discovery Offer
594	Network	PPPoE	Maintenance	INFO	---	Receive PAD Conffirm	Received PPPoE Active Discovery Session_confirmation
595	Network	PPPoE	Maintenance	INFO	---	Sending PADR	Sending PPPoE Active Discovery Request
596	Network	PPTP	Debug	DEBUG	---	Decode Failure	PPTP decode failure
597	Network	ICMP	Debug	INFO	---	ICMP Allow	ICMP packet allowed
598	Network	ICMP	Debug	INFO	---	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	---	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	---	Received Unencrypted Packet	Received unencrypted packet in crypto active state
606	Security Services	Attacks	Attack	ALERT	568	Spank Attack	Spank attack multicast packet dropped
607	VPN	VPN IKE	Debug | UDP	INFO	---	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	---	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

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
616	VPN	VPN IKE	Debug	ERROR	---	Detail Error Log	Payload processing failed
617	Wireless	WLAN	Maintenance	INFO	---	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	---	Response to Remote Device	BOOTP server response relayed to remote device
619	Network	BOOTP	Maintenance	INFO	---	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	---	Response to Local Device	BOOTP reply relayed to local device
622	VoIP	Call	VoIP	INFO	---	Call Connect	VoIP Call Connected
623	VoIP	Call	VoIP	INFO	---	Call Disconnect	VoIP Call Disconnected
624	VoIP	H.323	VoIP	DEBUG	---	H.323/RAS Admission Reject	H.323/RAS Admission Reject
625	VoIP	H.323	VoIP	DEBUG	---	H.323/RAS Admission Confirm	H.323/RAS Admission Confirm
626	VoIP	H.323	VoIP	DEBUG	---	H.323/RAS Admission Request	H.323/RAS Admission Request
627	VoIP	H.323	VoIP	DEBUG	---	H.323/RAS Bandwidth Reject	H.323/RAS Bandwidth Reject
628	VoIP	H.323	VoIP	DEBUG	---	H.323/RAS Disengage Confirm	H.323/RAS Disengage Confirm
629	VoIP	H.323	VoIP	DEBUG	---	H.323/RAS Gatekeeper Reject	H.323/RAS Gatekeeper Reject
630	VoIP	H.323	VoIP	DEBUG	---	H.323/RAS Location Confirm	H.323/RAS Location Confirm
631	VoIP	H.323	VoIP	DEBUG	---	H.323/RAS Location Reject	H.323/RAS Location Reject

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
632	VoIP	H.323	VoIP	DEBUG	---	H.323/RAS Registration Reject	H.323/RAS Registration Reject
633	VoIP	H.323	VoIP	DEBUG	---	H.323/H.225 Setup	H.323/H.225 Setup
634	VoIP	H.323	VoIP	DEBUG	---	H.323/H.225 Connect	H.323/H.225 Connect
635	VoIP	H.323	VoIP	DEBUG	---	H.323/H.245 Address	H.323/H.245 Address
636	VoIP	H.323	VoIP	DEBUG	---	H.323/H.245 End Session	H.323/H.245 End Session
637	VoIP	SIP	VoIP	DEBUG	---	Endpoint Added	VoIP %s Endpoint added
638	VoIP	SIP	VoIP	DEBUG	---	Endpoint Removed	VoIP %s Endpoint removed
639	VoIP	SIP	VoIP	WARNING	---	Endpoint Deny	VoIP %s Endpoint not added - configured 'public' endpoint limit reached
640	VoIP	H.323	VoIP	DEBUG	---	H.323/RAS Unknown Message Response	H.323/RAS Unknown Message Response
641	VoIP	H.323	VoIP	DEBUG	---	H.323/RAS Disengage Reject	H.323/RAS Disengage Reject
642	VoIP	H.323	VoIP	DEBUG	---	H.323/RAS Unregistration Reject	H.323/RAS Unregistration Reject
643	VoIP	SIP	VoIP	DEBUG	---	SIP Request	SIP Request
644	VoIP	SIP	VoIP	DEBUG	---	SIP Response	SIP Response
645	VoIP	SIP	VoIP	WARNING	---	SIP Register Expire	SIP Register expiration exceeds configured Signaling inactivity time out
646	Firewall	Access Rules	System Error	ALERT	5238	Source IP Connection Limit	Packet dropped; connection limit for this source IP address has been reached
647	Firewall	Access Rules	System Error	ALERT	5239	Destination IP Connection Limit	Packet dropped; connection limit for this destination IP address has been reached

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
648	VPN	VPN IPsec	Attack	ERROR	572	Illegal Destination	Packet destination not in VPN Access list
651	Network	IPcomp	Debug	DEBUG	---	IPcomp Interrupt Error	IPcomp connection interrupt
652	Network	IPcomp	TCP | UDP | ICMP	NOTICE	---	IPcomp Packet Drop	IPcomp packet dropped
653	Network	IPcomp	Debug	DEBUG	---	IPcomp Packet Drop, Waiting	IPcomp packet dropped; waiting for pending IPcomp connection
654	Log	General	System Error	CRITICAL	---	Maximum Events Rate Exceeded	Maximum events per second threshold exceeded: %s
655	Log	Syslog	System Error	CRITICAL	---	Maximum Syslog Data Rate Exceeded	Maximum syslog data per second threshold exceeded: %s
656	Log	E-mail	System Error	WARNING	---	POP-Before-SMTP Authentication Failed	SMTP POP-Before-SMTP authentication failed
657	Log	Syslog	Maintenance	INFO	---	Syslog Server Unreachable	Syslog Server cannot be reached
658	VPN	VPN IKE	System Error	WARNING	---	Responder: IKE ID mismatch	IKE Responder: Proposed IKE ID mismatch
659	VPN	VPN Client	System Error	ERROR	---	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	ERROR	---	Responder: Static IP Not Allowed	IKE Responder: %s Policy does not allow static IP for Virtual Adapter.
661	VPN	VPN IKE	User Activity	ERROR	---	Invalid Payload	Received notify: INVALID_PAYLOAD
662	Wireless	SonicPoint	Attack	ERROR	6434	Non SonicPoint Traffic Drop	Drop WLAN traffic from non-SonicPoint devices
665	3G/4G, Modem, and Module	PPP Dial-Up	---	INFO	---	Dialing Not Allowed	PPP Dial-Up: Dialing not allowed by schedule. %s

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
666	3G/4G, Modem, and Module	PPP Dial-Up	---	INFO	---	Scheduled Disconnect	PPP Dial-Up: Connection disconnected as scheduled.
667	Wireless	SonicPoint	SonicPoint	INFO	10401	SonicPoint Status	SonicPoint Status
668	High Availability	State	Maintenance	INFO	---	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	ERROR	665	Reboot Signal From Secondary	Primary received reboot signal from Secondary
672	High Availability	State	System Error	ERROR	666	Reboot Signal From Primary	Secondary received reboot signal from Primary
674	High Availability	Monitoring	System Error	INFO	---	Probe Success	Success to reach Interface %s probe
675	High Availability	Monitoring	System Error	ERROR	6234	Probe Failed	Failure to reach Interface %s probe
676	Firewall Settings	Multicast	---	INFO	---	IGMPv2 Client Joined Multicast Group	IGMP V2 client joined multicast Group : %s
677	Firewall Settings	Multicast	---	INFO	---	IGMPv3 Client Joined Multicast Group	IGMP V3 client joined multicast Group : %s
682	Firewall Settings	Multicast	---	INFO	---	IGMP Leave Group Message	IGMP Leave group message Received on interface %s
683	Firewall Settings	Multicast	---	NOTICE	---	Wrong IGMP Checksum	IGMP packet dropped, wrong checksum received on interface %s
690	Firewall Settings	Multicast	---	NOTICE	---	UDP Packet Drop	Multicast UDP packet dropped, no state entry
694	Firewall Settings	Multicast	---	WARNING	---	RTP Stateful Failed	Multicast UDP packet dropped, RTP stateful failed

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
701	Firewall Settings	Multicast	---	DEBUG	---	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	---	TCP Invalid SEQ Number	TCP packet received with invalid SEQ number; TCP packet dropped
709	Network	TCP	Debug	DEBUG	---	TCP Invalid ACK Number	TCP packet received with invalid ACK number; TCP packet dropped
712	Network	TCP	Debug	DEBUG	---	TCP Connection Reject	TCP connection reject received; TCP connection dropped
713	Network	TCP	Debug	DEBUG	---	TCP Connection Abort	TCP connection abort received; TCP connection dropped
714	Network	Network Access	Debug	NOTICE	---	EIGRP Packet Drop	EIGRP packet dropped
719	VPN	VPN IPsec	System Error	ERROR	---	Bad SA Count	VPN policy count received exceeds the limit; %s
720	Network	PPPoE	Maintenance	INFO	---	Send LCP Echo Request	Sending LCP Echo Request
721	Network	PPPoE	Maintenance	INFO	---	Receive LCP Echo Request	Received LCP Echo Request
722	Network	PPPoE	Maintenance	INFO	---	Send LCP Echo Reply	Sending LCP Echo Reply
723	Network	PPPoE	Maintenance	INFO	---	Receive LCP Echo Reply	Received LCP Echo Reply
724	Wireless	Network Access	---	INFO	---	Guest Services Deny Network	Guest Services drop traffic to deny network
725	Wireless	Network Access	---	INFO	---	Guest Services Allow Network	Guest Services pass traffic to access allow network
726	Wireless	Network Access	---	INFO	---	WLAN Max User Reached	WLAN max concurrent users reached already
727	Wireless	SonicPoint	SonicPoint	INFO	10402	SonicPoint Provision	SonicPoint Provision

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
728	Users	Authentication Access	Maintenance	INFO	---	WLAN Disable By Schedule	WLAN disabled by schedule
729	Users	Authentication Access	Maintenance	INFO	---	WLAN Enabled By Schedule	WLAN enabled by schedule
732	Wireless	WLAN	TCP | UDP | ICMP	WARNING	---	WLAN SSL VPN Enforcement Check Drop	Packet dropped by WLAN SSL VPN enforcement check
733	SSL VPN	General	Maintenance	INFO	---	SSL VPN Enforcement	SSL VPN enforcement
734	Firewall	Access Rules	---	INFO	---	Source Connection Status	Source IP address connection status: %s
735	Firewall	Access Rules	---	INFO	---	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	---	RADIUS Communicatio n Problem	User login denied - RADIUS communication problem
745	Users	Radius Authentication	User Activity	INFO	---	LDAP Authentication Failure	User login denied - LDAP authentication failure
746	Users	Radius Authentication	User Activity	WARNING	---	LDAP Server Timeout	User login denied - LDAP server Timeout
747	Users	Radius Authentication	User Activity	WARNING	---	LDAP Server Error	User login denied - LDAP server down or misconfigured
748	Users	Radius Authentication	User Activity	WARNING	---	LDAP Communicatio n Problem	User login denied - LDAP communication problem
749	Users	Radius Authentication	User Activity	WARNING	---	LDAP Server Invalid Credential	User login denied - invalid credentials on LDAP server
750	Users	Radius Authentication	User Activity	WARNING	---	LDAP Server Insufficient Access	User login denied - insufficient access on LDAP server
751	Users	Radius Authentication	User Activity	WARNING	---	LDAP Schema Mismatch	User login denied - LDAP schema mismatch

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
752	Users	Radius Authentication	User Activity	WARNING	---	LDAP Server Certificate With Wrong Name	Allowed LDAP server certificate with wrong host name
753	Users	Radius Authentication	User Activity	WARNING	---	LDAP Server Name Resolution Failed	User login denied - LDAP server name resolution failed
754	Users	Radius Authentication	User Activity	WARNING	---	RADIUS Server Name Resolution Failed	User login denied - RADIUS server name resolution failed
755	Users	Radius Authentication	User Activity	WARNING	---	LDAP Server Certificate Invalid	User login denied - LDAP server certificate not valid
756	Users	Radius Authentication	User Activity	WARNING	---	LDAP TLS or Local Error	User login denied - TLS or local certificate problem
757	Users	Radius Authentication	User Activity	WARNING	---	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	---	TCP Handshake Violation Detected	TCP handshake violation detected; TCP connection dropped
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	---	DDNS Abuse	DDNS Failure: Provider %s
774	Network	Dynamic DNS	System Error	ERROR	---	DDNS Invalid	DDNS Failure: Provider %s
776	Network	Dynamic DNS	Maintenance	INFO	---	DDNS Update Success	DDNS Update success for domain %s
777	Network	Dynamic DNS	System Error	WARNING	---	DDNS Warning	DDNS Warning: Provider %s
778	Network	Dynamic DNS	Maintenance	INFO	---	DDNS Taken Offline	DDNS association %s taken Offline locally

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
779	Network	Dynamic DNS	Maintenance	INFO	---	DDNS Added	DDNS association %s added
780	Network	Dynamic DNS	Maintenance	INFO	---	DDNS Association Enable	DDNS association %s enabled
781	Network	Dynamic DNS	Maintenance	INFO	---	DDNS Association Disable	DDNS association %s disabled
782	Network	Dynamic DNS	Maintenance	INFO	---	DDNS Association On-line	DDNS Association %s put on line
783	Network	Dynamic DNS	Maintenance	INFO	---	Deleted All DDNS Association	All DDNS associations have been deleted
785	Network	Dynamic DNS	Maintenance	INFO	---	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
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	---	Outbound Connection Drop	Outbound connection to RBL-listed SMTP server dropped
798	Security Services	RBL Filter	---	NOTICE	---	Inbound Connection Drop	Inbound connection from RBL-listed SMTP server dropped
799	Security Services	RBL Filter	---	NOTICE	---	SMTP Server on RBL Blacklist	SMTP server found on RBL blacklist

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
800	Security Services	RBL Filter	---	ERROR	---	No Valid DNS Server on RBL	No valid DNS server specified for RBL lookups
805	System	GMS	---	INFO	---	Interface Statistics Report	Interface statistics report
806	System	GMS	---	INFO	---	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
811	3G/4G, Modem, and Module	PPP Dial-Up	Maintenance	INFO	---	Invalid DNS Server	PPP Dial-Up: Invalid DNS IP address returned from Dial-Up ISP; overriding using dial-up profile settings
815	Network	ARP	---	WARNING	---	Too Many Gratuitous ARPs Detected	Too many gratuitous ARPs detected
817	Users	Authentication Access	User Activity	INFO	---	Remote Dialup Received	Incoming call received for Remotely Triggered Dial-out session
818	Users	Authentication Access	User Activity	INFO	---	Remote Dialup Authentication Request	Remotely Triggered Dial-out session started. Requesting authentication
819	Users	Authentication Access	User Activity	INFO	---	Remote Dialup Authentication Password Error	Incorrect authentication received for Remotely Triggered Dial-out
820	Users	Authentication Access	User Activity	INFO	---	Remote Dialup Authentication Password Valid	Successful authentication received for Remotely Triggered Dial-out
821	Users	Authentication Access	User Activity	INFO	---	Remote Dialup Authentication Password Timeout	Authentication Timeout during Remotely Triggered Dial-out session

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
822	Users	Authentication Access	User Activity	INFO	---	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	---	License Expire to Shutdown Secondary	Secondary shut down because license is expired
825	High Availability	State	System Error	INFO	---	Secondary Active	Secondary active
826	High Availability	State	---	ERROR	---	HA Error	%s
829	High Availability	State	---	ALERT	---	HA Alert	%s
830	High Availability	State	---	NOTICE	---	HA Notice	%s
832	Network	DHCP Server	---	INFO	---	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	---	ARS Info	%s
841	Network	Advanced Routing	---	NOTICE	---	ARS Warning	%s
842	Network	Advanced Routing	---	DEBUG	---	ARS Debug	%s
847	Network	Interfaces	Maintenance	WARNING	---	IP Address Conflict	IP address conflict detected from Ethernet address %s
848	VPN	VPN PKI	User Activity	INFO	---	OCSP Send Request	OCSP sending request.
849	VPN	VPN PKI	User Activity	ERROR	---	OCSP Failed to Send Request	OCSP send request message failed.

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
850	VPN	VPN PKI	User Activity	INFO	---	OCSP Received Response	OCSP received response.
852	VPN	VPN PKI	User Activity	INFO	---	OCSP Resolved Domain Name	OCSP Resolved Domain Name.
853	VPN	VPN PKI	User Activity	ERROR	---	OCSP Failed to Resolve Domain Name	OCSP Failed to Resolve Domain Name.
854	VPN	VPN PKI	User Activity	ERROR	---	OCSP Internal Error	OCSP Internal error handling received response.
856	Firewall Settings	Flood Protection	Attack	WARNING	---	SYN Flood Watch Mode	SYN Flood Mode changed by user to: Watch and report possible SYN floods
857	Firewall Settings	Flood Protection	Attack	WARNING	---	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	---	SYN Flood Proxy Mode	SYN Flood Mode changed by user to: Always proxy WAN connections
859	Firewall Settings	Flood Protection	Attack	ALERT	---	SYN Flood Proxy Trigger Mode	Possible SYN flood detected on WAN IF %s - switching to connection-proxy mode
860	Firewall Settings	Flood Protection	Attack	ALERT	---	SYN Flood Detected	Possible SYN Flood on IF %s
861	Firewall Settings	Flood Protection	Attack	ALERT	---	SYN Flood Proxy Mode Cancel	SYN flood ceased or flooding machines blacklisted - connection proxy disabled
862	Firewall Settings	Flood Protection	Attack	WARNING	---	SYN Flood Blacklist On	SYN Flood blacklisting enabled by user
863	Firewall Settings	Flood Protection	Attack	WARNING	---	SYN Flood Blacklist Off	SYN Flood blacklisting disabled by user
864	Firewall Settings	Flood Protection	Attack	ALERT	---	SYN-Flooding Machine Blacklisted	SYN-Flooding machine %s blacklisted
865	Firewall Settings	Flood Protection	Attack	ALERT	---	Machine removed from SYN Flood Blacklist	Machine %s removed from SYN flood blacklist

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
866	Firewall Settings	Flood Protection	Attack	WARNING	---	Possible SYN Flood Continues	Possible SYN Flood on IF %s continues
867	Firewall Settings	Flood Protection	Attack	ALERT	---	Possible SYN Flood Ceased	Possible SYN Flood on IF %s has ceased
868	Firewall Settings	Flood Protection	Attack	WARNING	---	SYN Flood Blacklist Continues	SYN Flood Blacklist on IF %s continues
869	Firewall Settings	Flood Protection	Attack	DEBUG	---	TCP SYN Receive	TCP SYN received
872	Security Services	General	User Activity	NOTICE	---	Security Service Message	%s
874	VPN	VPN PKI	User Activity	ALERT	---	CRL Expire	CRL has expired
875	VPN	VPN PKI	User Activity	ALERT	---	Failed to Find Certificate	Failed to find certificate
876	VPN	VPN PKI	User Activity	ALERT	---	CRL Missing	CRL missing - Issuer requires CRL checking.
877	VPN	VPN PKI	User Activity	ALERT	---	CRL Validation Error	CRL validation failure for Root Certificate
878	VPN	VPN PKI	User Activity	ALERT	---	Can't Validate Issuer Path	Cannot Validate Issuer Path
879	Wireless	RF Monitoring	---	WARNING	---	WLAN Radio Frequency Threat Detected	WLAN radio frequency threat detected
880	Network	Dynamic Address Objects	Maintenance	INFO	---	Failed to Resolve Dynamic Address Object	Unable to resolve dynamic address object
881	System	Time	---	NOTICE	---	System Clock Manually Updated	System clock manually updated
882	Network	Network Access	TCP	DEBUG	---	HTTP Drop	HTTP method detected; examining stream for host header
883	Firewall Settings	Checksum Enforcement	TCP|UDP	NOTICE	---	IP Checksum Error	IP Header checksum error; packet dropped
884	Firewall Settings	Checksum Enforcement	TCP	NOTICE	---	TCP Checksum Error	TCP checksum error; packet dropped
885	Firewall Settings	Checksum Enforcement	UDP	NOTICE	---	UDP Checksum Error	UDP checksum error; packet dropped

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
886	Firewall Settings	Checksum Enforcement	UDP	NOTICE	---	ICMP Checksum Error	ICMP checksum error; packet dropped
887	Network	TCP	Debug	DEBUG	---	Invalid TCP Header Length	TCP packet received with invalid header length; TCP packet dropped
888	Network	TCP	Debug	DEBUG	---	TCP Connection Does Not Exist	TCP packet received on non-existent/closed connection; TCP packet dropped
889	Network	TCP	Debug	DEBUG	---	TCP Without Mandatory SYN Flag	TCP packet received without mandatory SYN flag; TCP packet dropped
890	Network	TCP	Debug	DEBUG	---	TCP Without Mandatory ACK Flag	TCP packet received without mandatory ACK flag; TCP packet dropped
891	Network	TCP	Debug	DEBUG	---	TCP Packet on Closing Connection	TCP packet received on a closing connection; TCP packet dropped
892	Network	TCP	Debug	INFO	---	SYN Flag on Existing Connection	TCP packet received with SYN flag on an existing connection; TCP packet dropped
893	Network	TCP	Debug	DEBUG	---	Invalid TCP SACK Option Length	TCP packet received with invalid SACK option length; TCP packet dropped
894	Network	TCP	Debug	DEBUG	---	Invalid TCP MSS Option Length	TCP packet received with invalid MSS option length; TCP packet dropped
895	Network	TCP	Debug	DEBUG	---	Invalid TCP Option Length	TCP packet received with invalid option length; TCP packet dropped
896	Network	TCP	Debug	DEBUG	---	Invalid TCP Source Port	TCP packet received with invalid source port; TCP packet dropped

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
897	Firewall Settings	Flood Protection	Attack	INFO	---	Invalid TCP SYN Flood Cookie	TCP packet received with invalid SYN Flood cookie; TCP packet dropped
898	Firewall Settings	Flood Protection	Attack	ALERT	---	RST-Flooding Machine Blacklisted	RST-Flooding machine %s blacklisted
899	Firewall Settings	Flood Protection	Attack	WARNING	---	RST Flood Blacklist Continues	RST Flood Blacklist on IF %s continues
900	Firewall Settings	Flood Protection	Attack	ALERT	---	Machine Removed From RST Flood Blacklist	Machine %s removed from RST flood blacklist
901	Firewall Settings	Flood Protection	Attack	ALERT	---	FIN-Flooding Machine Blacklisted	FIN-Flooding machine %s blacklisted
902	Firewall Settings	Flood Protection	Attack	WARNING	---	FIN Flood Blacklist Continues	FIN Flood Blacklist on IF %s continues
903	Firewall Settings	Flood Protection	Attack	ALERT	---	Machine Removed From FIN Flood Blacklist	Machine %s removed from FIN flood blacklist
904	Firewall Settings	Flood Protection	Attack	ALERT	---	Possible RST Flood	Possible RST Flood on IF %s
905	Firewall Settings	Flood Protection	Attack	ALERT	---	Possible FIN Flood	Possible FIN Flood on IF %s
906	Firewall Settings	Flood Protection	Attack	ALERT	---	Possible RST Flood Ceased	Possible RST Flood on IF %s has ceased
907	Firewall Settings	Flood Protection	Attack	ALERT	---	Possible FIN Flood Ceased	Possible FIN Flood on IF %s has ceased
908	Firewall Settings	Flood Protection	Attack	WARNING	---	Possible RST Flood Continues	Possible RST Flood on IF %s continues
909	Firewall Settings	Flood Protection	Attack	WARNING	---	Possible FIN Flood Continues	Possible FIN Flood on IF %s continues
910	Network	IP	Debug	WARNING	---	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

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
913	VPN	VPN IKE	User Activity	WARNING	---	Responder: Authentication Method Mismatch	IKE Responder: Phase 1 Authentication Method does not match
914	VPN	VPN IKE	User Activity	WARNING	---	Responder: Encryption Algorithm Mismatch	IKE Responder: Phase 1 encryption algorithm does not match
915	VPN	VPN IKE	User Activity	WARNING	---	Responder: Key Length Mismatch	IKE Responder: Phase 1 encryption algorithm keylength does not match
916	VPN	VPN IKE	User Activity	WARNING	---	Responder: Hash Algorithm Mismatch	IKE Responder: Phase 1 hash algorithm does not match
917	VPN	VPN IKE	User Activity	WARNING	---	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	---	Responder: Policy Has no Password	IKE Responder: Phase 1 XAUTH required but Policy has no user password
919	VPN	VPN IKE	User Activity	WARNING	---	Responder: DH Group Mismatch	IKE Responder: Phase 1 DH Group does not match
920	VPN	VPN IKE	User Activity	WARNING	---	Responder: AH Authentication Algorithm Mismatch	IKE Responder: AH authentication algorithm does not match
921	VPN	VPN IKE	User Activity	WARNING	---	Responder: ESP Encryption Algorithm Mismatch	IKE Responder: ESP encryption algorithm does not match
922	VPN	VPN IKE	User Activity	WARNING	---	Responder: ESP Authentication Algorithm Mismatch	IKE Responder: ESP authentication algorithm does not match
923	VPN	VPN IKE	User Activity	WARNING	---	Responder: AH Authentication Key Length Mismatch	IKE Responder: AH authentication key length does not match

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
924	VPN	VPN IKE	User Activity	WARNING	---	Responder: ESP Encryption Key Length Mismatch	IKE Responder: ESP encryption key length does not match
925	VPN	VPN IKE	User Activity	WARNING	---	Responder: ESP Authentication Key Length Mismatch	IKE Responder: ESP authentication key length does not match
926	VPN	VPN IKE	User Activity	WARNING	---	Responder: AH Authentication Key Rounds Mismatch	IKE Responder: AH authentication key rounds does not match
927	VPN	VPN IKE	User Activity	WARNING	---	Responder: ESP Encryption Key Rounds Mismatch	IKE Responder: ESP encryption key rounds does not match
928	VPN	VPN IKE	User Activity	WARNING	---	Responder: ESP Authentication Key Rounds Mismatch	IKE Responder: ESP authentication key rounds does not match
930	VPN	VPN IKE	User Activity	INFO	---	Initiator: Peer Timeout - Retransmitting	IKE Initiator: Remote party Timeout - Retransmitting IKE Request.
931	VPN	VPN IKE	User Activity	INFO	---	Responder: Peer Timeout - Retransmitting	IKE Responder: Remote party Timeout - Retransmitting IKE Request.
932	VPN	VPN IKE	User Activity	WARNING	---	Responder: IPsec Protocol Mismatch	IKE Responder: IPsec protocol mismatch
933	VPN	VPN IKE	User Activity	WARNING	---	Initiator: Proposed IKE ID Mismatch	IKE Initiator: Proposed IKE ID mismatch
934	VPN	VPN IKE	User Activity	WARNING	---	Responder: Local Network Mismatch Peer's Destination Network	IKE Responder: Peer's local network does not match VPN Policy's [Destination]

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
935	VPN	VPN IKE	User Activity	WARNING	---	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	---	Responder: Route Table Overrides VPN Policy	IKE Responder: Route table overrides VPN Policy
937	VPN	VPN IKE	User Activity	WARNING	---	Initiator: IKE Proposal Mismatch	IKE Initiator: IKE proposal does not match (Phase 1)
938	VPN	VPN IKEv2	User Activity	INFO	---	Initiator: Send IKE_SA_INIT Request	IKEv2 Initiator: Send IKE_SA_INIT Request
939	VPN	VPN IKEv2	User Activity	INFO	---	Responder: Received IKE_SA_INIT Request	IKEv2 Responder: Received IKE_SA_INIT Request
940	VPN	VPN IKEv2	User Activity	INFO	---	Initiator: Send IKE_AUTH Request	IKEv2 Initiator: Send IKE_AUTH Request
941	VPN	VPN IKEv2	User Activity	INFO	---	Responder: Received IKE_AUTH Request	IKEv2 Responder: Received IKE_AUTH Request
942	VPN	VPN IKEv2	User Activity	INFO	---	Authentication Successful	IKEv2 Authentication successful
943	VPN	VPN IKEv2	User Activity	INFO	---	Accept IKE SA Proposal	IKEv2 Accept IKE SA Proposal
944	VPN	VPN IKEv2	User Activity	INFO	---	Accept IPsec SA Proposal	IKEv2 Accept IPsec SA Proposal
945	VPN	VPN IKEv2	User Activity	INFO	---	Initiator: Send CREATE_CHILD_SA Request	IKEv2 Initiator: Send CREATE_CHILD_SA Request
946	VPN	VPN IKEv2	User Activity	INFO	---	Responder: Received CREATE_CHILD_SA Request	IKEv2 Responder: Received CREATE_CHILD_SA Request
947	VPN	VPN IKEv2	User Activity	INFO	---	Send Delete IKE SA Request	IKEv2 Send delete IKE SA Request
948	VPN	VPN IKEv2	User Activity	INFO	---	Received Delete IKE SA Request	IKEv2 Received delete IKE SA Request

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
949	VPN	VPN IKEv2	User Activity	INFO	---	Send Delete IPsec SA Request	IKEv2 Send delete IPsec SA Request
950	VPN	VPN IKEv2	User Activity	INFO	---	Received Delete IPsec SA Request	IKEv2 Received delete IPsec SA Request
951	VPN	VPN IKEv2	User Activity	INFO	---	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	---	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	---	Payload Processing Error	IKEv2 Payload processing error
954	VPN	VPN IKEv2	User Activity	WARNING	---	Initiator: Extra Payloads Present	IKEv2 Initiator: Negotiations failed. Extra payloads present.
955	VPN	VPN IKEv2	User Activity	WARNING	---	Initiator: Missing Required Payloads	IKEv2 Initiator: Negotiations failed. Missing required payloads.
956	VPN	VPN IKEv2	User Activity	WARNING	---	Initiator: Invalid Input State	IKEv2 Initiator: Negotiations failed. Invalid input state.
957	VPN	VPN IKEv2	User Activity	WARNING	---	Initiator: Invalid Output State	IKEv2 Initiator: Negotiations failed. Invalid output state.
958	VPN	VPN IKEv2	User Activity	WARNING	---	Payload Validation Failed	IKEv2 Payload validation failed.
959	VPN	VPN IKEv2	User Activity	WARNING	---	Unable to Find IKE SA	IKEv2 Unable to find IKE SA
960	VPN	VPN IKEv2	User Activity	WARNING	---	Decrypt Packet Failed	IKEv2 Decrypt packet failed
961	VPN	VPN IKEv2	User Activity	WARNING	---	Out of Memory	IKEv2 Out of memory

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
962	VPN	VPN IKEv2	User Activity	ERROR	---	Responder: Policy for Remote IKE ID Not Found	IKEv2 Responder: Policy for remote IKE ID not found
963	VPN	VPN IKEv2	User Activity	WARNING	---	Process Message Queue Failed	IKEv2 Process Message queue failed
964	VPN	VPN IKEv2	User Activity	WARNING	---	Invalid State	IKEv2 Invalid state
965	VPN	VPN IKE	System Error	ERROR	---	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	---	Invalid SPI Size	IKEv2 Invalid SPI size
967	VPN	VPN IKEv2	User Activity	WARNING	---	VPN Policy Not Found	IKEv2 VPN Policy not found
968	VPN	VPN IKEv2	User Activity	WARNING	---	IPsec Proposal Mismatch	IKEv2 IPsec proposal does not match
969	VPN	VPN IKEv2	User Activity	WARNING	---	IPsec Attribute Not Found	IKEv2 IPsec attribute not found
970	VPN	VPN IKEv2	User Activity	WARNING	---	IKE Attribute Not Found	IKEv2 IKE attribute not found
971	VPN	VPN IKEv2	User Activity	WARNING	---	Peer Not Responding	IKEv2 Peer is not responding. Negotiation aborted.
972	VPN	VPN IKEv2	User Activity	INFO	---	Initiator: Retransmit IKEv2 Request Due to Remote Party Timeout	IKEv2 Initiator: Remote party Timeout - Retransmitting IKEv2 Request.
973	VPN	VPN IKEv2	User Activity	INFO	---	Initiator: Received IKE_SA_INT Response	IKEv2 Initiator: Received IKE_SA_INT response
974	VPN	VPN IKEv2	User Activity	INFO	---	Initiator: Received IKE_AUTH Response	IKEv2 Initiator: Received IKE_AUTH response
975	VPN	VPN IKEv2	User Activity	INFO	---	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

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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	---	Negotiation Completed	IKEv2 negotiation complete
979	VPN	VPN IKEv2	User Activity	ERROR	---	Failed to Transmit Packet	IKEv2 Function sendto() failed to transmit packet.
980	VPN	VPN IKEv2	User Activity	WARNING	---	Initiator: Proposed IKE ID Mismatch	IKEv2 Initiator: Proposed IKE ID mismatch
981	VPN	VPN IKEv2	User Activity	WARNING	---	IKE Proposal Mismatch	IKEv2 IKE proposal does not match
982	VPN	VPN IKEv2	User Activity	INFO	---	Received Notify Status Payload	IKEv2 Received notify status payload
983	VPN	VPN IKEv2	User Activity	WARNING	---	Received Notify Error Payload	IKEv2 Received notify error payload
984	VPN	VPN IKEv2	User Activity	INFO	---	No NAT Device Detected	IKEv2 No NAT device detected between negotiating peers
985	VPN	VPN IKEv2	User Activity	INFO	---	NAT Device Detected Between Negotiating Peers	IKEv2 NAT device detected between negotiating peers
986	Users	Authentication Access	User Activity	INFO	---	Not Allowed by Policy Rule	User login denied - not allowed by Policy rule
987	Users	Authentication Access	User Activity	INFO	---	Not Found Locally	User login denied - not found locally
988	Users	SSO Agent Authentication	User Activity	WARNING	---	Timeout	User login denied - SSO agent Timeout
989	Users	SSO Agent Authentication	User Activity	WARNING	---	Configuration Error	User login denied - SSO agent configuration error
990	Users	SSO Agent Authentication	User Activity	WARNING	---	Communicatio n Problem	User login denied - SSO agent communication problem
991	Users	SSO Agent Authentication	User Activity	WARNING	---	Name Resolution Failed	User login denied - SSO agent name resolution failed

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
992	Users	SSO Agent Authentication	User Activity	WARNING	---	User Name Too Long	SSO agent returned user name too long
993	Users	SSO Agent Authentication	User Activity	WARNING	---	Domain Name Too Long	SSO agent returned domain name too long
994	Users	Authentication Access	User Activity	INFO	---	Configuration Mode Administration Session Started	Configuration mode administration session started
995	Users	Authentication Access	User Activity	INFO	---	Configuration Mode Administration Session Ended	Configuration mode administration session ended
996	Users	Authentication Access	User Activity	INFO	---	Read-only Mode GUI Administration Session Started	Read-only mode GUI administration session started
997	Users	Authentication Access	User Activity	INFO	---	Non-Config Mode GUI Administration Session Started	Non-config mode GUI administration session started
998	Users	Authentication Access	User Activity	INFO	---	GUI Administration Session End	GUI administration session ended
999	Firewall Settings	SSL Control	Blocked Sites	INFO	---	Website Found in Blacklist	SSL Control: Website found in blacklist
1000	Firewall Settings	SSL Control	Blocked Sites	INFO	---	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	---	Certificate With Invalid Date	SSL Control: Certificate with invalid date
1003	Firewall Settings	SSL Control	Blocked Sites	INFO	---	Self-Signed Certificate	SSL Control: Self-signed certificate
1004	Firewall Settings	SSL Control	Blocked Sites	INFO	---	Weak Cipher Being Used	SSL Control: Weak cipher being used
1005	Firewall Settings	SSL Control	Blocked Sites	INFO	---	Untrusted CA	SSL Control: Untrusted CA
1006	Firewall Settings	SSL Control	Blocked Sites	INFO	---	Certificate Chain Incomplete	SSL Control: Certificate chain not complete

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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	---	Bind to LDAP Server Failed	Bind to LDAP server failed
1010	Users	Radius Authentication	System Error	ALERT	---	Using LDAP Without TLS	Using LDAP without TLS - highly insecure
1011	Users	Radius Authentication	System Error	WARNING	---	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	---	Responder: Send CREATE_CHILD_SA Response	IKEv2 Responder: Send CREATE_CHILD_SA response
1013	VPN	VPN IKEv2	User Activity	INFO	---	Send Delete IKE SA Response	IKEv2 Send delete IKE SA response
1014	VPN	VPN IKEv2	User Activity	INFO	---	Send Delete IPsec SA Response	IKEv2 Send delete IPsec SA response
1015	VPN	VPN IKEv2	User Activity	INFO	---	Received Delete IKE SA Response	IKEv2 Received delete IKE SA response
1016	VPN	VPN IKEv2	User Activity	INFO	---	Received Delete IPsec SA Response	IKEv2 Received delete IPsec SA response
1017	3G/4G, Modem, and Module	3G/4G and Modem	System Environment	INFO	---	3G/4G Device Detected	3G/4G %s device detected
1018	Network	PPP	---	INFO	---	PPP Message	PPP message: %s
1019	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	Chat Start	Chat started
1020	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	Chat Completed	Chat completed
1021	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	Chat Wrote Message	Chat wrote '%s'

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1022	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	Chat Message	Chat %s
1023	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	INFO	---	Chat Failed	Chat failed: %s
1024	3G/4G, Modem, and Module	PPP Dial-Up	System Error	ERROR	---	Unable to Send Message to Dial-Up Task	Unable to send message to dial-up task
1026	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	ALERT	---	Data Usage Watermark Reached	3G/4G Dial-up: %s.
1027	3G/4G, Modem, and Module	PPP Dial-Up	User Activity	ALERT	7643	Data Usage Limit Reached	3G/4G Dial-up: data usage limit reached for the '%s' billing cycle. Disconnecting the session.
1028	3G/4G, Modem, and Module	PPP Dial-Up	System Error	ALERT	---	Auto-Dial Failed	%s auto-dial failed: Current Connection Model is configured as Ethernet Only
1029	Network	TCP	Debug	DEBUG	---	Non-Permitted Option TCP Packet	TCP packet received with non-permitted option; TCP packet dropped
1030	Network	TCP	Debug	DEBUG	---	Invalid TCP Window Scale Option Length	TCP packet received with invalid Window Scale option length; TCP packet dropped
1031	Network	TCP	Debug	DEBUG	---	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	ERROR	---	Responder: IKE Phase 1 Exchange Mismatch	IKE Responder: IKE Phase 1 exchange does not match

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1037	3G/4G, Modem, and Module	PPP Dial-Up	---	INFO	---	Starting PPP	PPP Dial-Up: Starting PPP
1038	3G/4G, Modem, and Module	PPP Dial-Up	---	INFO	---	Traffic Generated	Dial-up: Traffic generated by '%s'
1039	3G/4G, Modem, and Module	PPP Dial-Up	---	INFO	---	Session Initiated by Data Packet	Dial-up: Session initiated by data packet
1040	Network	DHCP Server	---	ALERT	---	DHCP Server IP Conflict Detected	DHCP Server: IP conflict detected
1041	Network	DHCP Server	---	ALERT	---	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
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
1053	3G/4G, Modem, and Module	3G/4G and Modem	---	ALERT	5418	PC Card Removed	PC Card removed.

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1054	3G/4G, Modem, and Module	3G/4G and Modem	---	ALERT	5419	PC Card Inserted	PC Card inserted.
1055	3G/4G, Modem, and Module	3G/4G and Modem	---	ALERT	---	3G/4G: No SIM Detected	3G/4G: 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	INFO	---	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	---	CRITICAL	---	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
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

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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	---	INFO	13803	Service Enable	Anti-Spam service is enabled by administrator.
1085	Anti-Spam	General	---	INFO	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
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

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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
1108	Anti-Spam	E-mail	---	INFO	---	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

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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
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

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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
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

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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
1148	Network	Interfaces	Advanced Switching	INFO	---	Advanced Switching	%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	Connection Traffic	INFO	---	SSL VPN Traffic	SSL VPN Traffic
1154	Firewall	Application Control	---	ALERT	15001	Application Control Detection Alert	Application Control Detection Alert: %s
1155	Firewall	Application Control	---	ALERT	15002	Application Control Prevention Alert	Application Control Prevention Alert: %s

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1156	Network	DNS	---	ERROR	---	Syslog/GMS Name Resolution Failure	Name Resolution for Syslog or GMS 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
1162	High Availability	Synchronization	System Error	ALERT	---	HA Module Mismatched	Modules attached to HA units do not match: %s
1163	3G/4G, Modem, and Module	E1-T1 Module	---	INFO	---	E1-T1 No Signal	E1_T1 Layer 1 status: No signal
1164	3G/4G, Modem, and Module	E1-T1 Module	---	INFO	---	E1-T1 No Frame	E1_T1 Layer 1 status: No frame synchronization
1165	3G/4G, Modem, and Module	E1-T1 Module	---	INFO	---	E1-T1 No Multiframe	E1_T1 Layer 1 status: No multiframe synchronization
1166	3G/4G, Modem, and Module	E1-T1 Module	---	INFO	---	E1-T1 Remote Alarm	E1_T1 Layer 1 status: Remote alarm detected
1167	3G/4G, Modem, and Module	E1-T1 Module	---	INFO	---	E1-T1 Slip	E1_T1 Layer 1 status: Controlled slip
1168	3G/4G, Modem, and Module	E1-T1 Module	---	INFO	---	E1-T1 OK	E1_T1 Layer 1 status: OK

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1169	WAN Acceleration	Local WXA Appliance	---	INFO	---	WXA Appliance Found	WAN Acceleration device %s found
1170	WAN Acceleration	Local WXA Appliance	---	ALERT	---	WXA Appliance Operational	WAN Acceleration device %s is operational
1171	WAN Acceleration	Local WXA Appliance	---	ALERT	---	WXA Appliance Not Operational	WAN Acceleration device %s is no longer operational
1172	WAN Acceleration	Local WXA Appliance	---	ALERT	---	WXA Appliance Used	WAN Acceleration device %s is being used
1173	WAN Acceleration	Local WXA Appliance	---	ALERT	---	WXA Appliance Not Used	WAN Acceleration device %s is no longer being used
1174	WAN Acceleration	Remote WXA Appliance	---	WARNING	---	WXA Appliance Not Responding	Remote WAN Acceleration device stopped responding to probes
1175	WAN Acceleration	Remote WXA Appliance	---	WARNING	---	WXA Appliance Responding	Remote WAN Acceleration device started responding to probes
1176	WAN Acceleration	Local WXA Appliance	---	WARNING	---	WAN Acceleration Software License Expired	Your WAN Acceleration Service subscription has expired.
1177	Network	DNS	Debug	ALERT	---	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

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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.
1185	3G/4G, Modem, and Module	DSL Module	---	ALERT	---	DSL Device Up	DSL: %s Device Up
1186	3G/4G, Modem, and Module	DSL Module	---	ALERT	---	DSL Device Down	DSL: %s Device Down
1187	3G/4G, Modem, and Module	DSL Module	---	ALERT	---	DSL WAN Up	DSL: %s WAN is connected
1188	3G/4G, Modem, and Module	DSL Module	---	ALERT	---	DSL WAN down	DSL: %s WAN is initializing
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
1193	Users	Radius Authentication	---	INFO	---	LDAP Mirror Deleted Member	Removed a member from an LDAP mirror user group
1194	High Availability	Monitoring	---	ERROR	---	HA Monitor Probe Interface Mismatched	Monitoring probe out interface mismatch %s

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1195	Security Services	Botnet Filter	Security Services	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	ALERT	---	HA Peer MultiInterface Link Up	On HA peer firewall, Interface %s Link Is Up
1206	High Availability	State	System Error	ALERT	---	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.
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.

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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	---	DEBUG	---	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	---	WARNING	---	Invalid SNMPv3 Packet	Invalid SNMP packet
1221	System	SNMP	---	WARNING	---	Invalid SNMPv3 Engine ID	Invalid SNMPv3 engineID
1222	System	SNMP	---	WARNING	---	Invalid SNMPv3 User	Invalid SNMPv3 User

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1223	System	SNMP	---	WARNING	---	Invalid SNMPv3 Time Window	Invalid SNMPv3 Time Window
1225	System	SNMP	---	INFO	---	SNMP Packet Drop	SNMP Packet Dropped
1226	Network	Network Access	---	INFO	---	HTTPS Handshake	HTTPS Handshake: %s
1227	Users	Authentication Access	User Activity	INFO	---	Guest Traffic Quota Exceeded	User Traffic Quota Exceeded
1229	Wireless	Network 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	---	WARNING	---	Endpoint Anomaly Lockout Started	%s

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1242	VoIP	Anomaly	---	WARNING	---	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	---	NOTICE	---	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	---	NOTICE	---	ICMPv6 Packets Dropped	ICMPv6 packet dropped due to policy
1258	Network	Network Access	---	DEBUG	---	TCP/IP Stack	%s
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

Event ID	SonicOS Category Name	SonicOS 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	Firewall	NOTICE	---	Firmware Update Failed	Firmware Update Failed
1269	System	Settings	Firewall	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 Category Name	SonicOS 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.

Event ID	SonicOS Category Name	SonicOS 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 Category Name	SonicOS 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	Firewall	INFO	---	Change Certification	Certification %s
1337	System	Settings	Firewall	INFO	---	User Password Changed by Administrators	%s
1338	System	Settings	Firewall	INFO	---	User Change Password	User %s password is changed
1339	System	Settings	Firewall	INFO	---	Change Password Rule	Password rule %s is changed
1340	System	Settings	Firewall	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

Event ID	SonicOS Category Name	SonicOS 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 Test Success	Crypto TLS 1.0/1.1 test success
1358	Security Services	Crypto Test	---	ERROR	---	TLS 1.0/1.1 Test Failed	Crypto TLS 1.0/1.1 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	---	ALERT	---	Cert Payload processing failed	Cert Payload processing failed
1365	Security Services	DPI-SSL	---	NOTICE	---	DPI-SSL Memory Check	DPI-SSL: %s

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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
1380	WAN Acceleration	Local WXA Appliance	---	INFO	---	WXA association succeeded	WXA association posted successfully to License Manager

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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	ALERT	---	Raw Data	Packet Data
1392	System	Restart	Maintenance	ALERT	5243	Blade up	Blade up:%s
1393	System	Restart	Maintenance	ALERT	5244	Blade down	Blade 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
1397	WAN Acceleration	Local WXA Appliance	---	NOTICE	---	Register Failure	WXA Register Failure - %s

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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]
1413	Network	DHCPv6 Client	---	INFO	---	DHCPv6 Client Release Lease	DHCPv6 Client released lease [%s]

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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	---	INFO	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	---	INFO	---	SSL VPN Debug	%s
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

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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	Firewall	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	INFO	---	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	---	NOTICE	---	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	Advanced	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 Acceleration	Local WXA Appliance	---	WARNING	---	Connection Exceed	WXA Warning - %s
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

Log Event Message Index

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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	Network Access	Debug	INFO	---	Extended Switch Add	%s
1454	Network	Network Access	Debug	INFO	---	Extended Switch Remove	%s
1455	Network	Network Access	Debug	INFO	---	Extended Switch Port Speed Change	Extended Switch Port Status Change : %s
1456	Network	Network Access	Debug	INFO	---	Extended Switch Port Duplex Mode Change	Extended Switch Port Status Change : %s
1457	Network	Network Access	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	INFO	---	Capture ATP File Transfer Attempt	Gateway Anti-Virus Status: %s
1460	Security Services	GAV	Maintenance	INFO	---	Capture ATP File Transfer Result	Gateway Anti-Virus Status: %s
1461	Security Services	Content Filter	---	NOTICE	703	CFS Alert	CFS Alert: %s
1462	Security Services	GAV	---	INFO	---	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

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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	WARNING	---	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
1485	Network	DNS Proxy	Maintenance	INFO	---	DNS Proxy Delete Cache	Remove DNS cache
1486	Network	DNS Proxy	Maintenance	INFO	---	DNS Proxy Request Packet Drop	Drop DNS query packet

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1487	Network	DNS Proxy	Maintenance	INFO	---	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	---	INFO	---	Packet Dissection Check	Packet Dissection Check -- %s
1498	3G/4G, Modem, and Module	3G/4G and Modem	User Activity	INFO	---	WWAN Connecting	WWAN - Connecting %s
1499	3G/4G, Modem, and Module	3G/4G and Modem	User Activity	INFO	---	WWAN Start New Session	WWAN - Starting a new session
1500	3G/4G, Modem, and Module	3G/4G and Modem	User Activity	INFO	---	WWAN Connection Established	WWAN - Connection established
1501	3G/4G, Modem, and Module	3G/4G and Modem	User Activity	INFO	---	WWAN IP Update	WWAN - Received new IP address
1502	3G/4G, Modem, and Module	3G/4G and Modem	User Activity	INFO	---	WWAN Disconnected	WWAN - Link disconnected
1503	3G/4G, Modem, and Module	3G/4G and Modem	User Activity	INFO	---	WWAN Session Duration	WWAN - Previous session was connected for %s

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
1504	3G/4G, Modem, and Module	3G/4G and Modem	User Activity	INFO	---	WWAN Disconnecting	WWAN - Disconnecting
1505	3G/4G, Modem, and Module	3G/4G and Modem	User Activity	INFO	---	WWAN Profile is Manual	WWAN - Trying to failover but Primary Profile is manual
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
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	Firewall	INFO	---	Automatic Cloud Backup Successful	%s
1512	System	Cloud Backup	Firewall	INFO	---	Automatic Cloud Backup Failed	%s
1513	System	Cloud Backup	Firewall	INFO	---	Manual Cloud Backup Successful	%s
1514	System	Cloud Backup	Firewall	INFO	---	Manual Cloud Backup Failed	%s
1515	System	Cloud Backup	Firewall	INFO	---	Delete Cloud Backup Successful	%s
1516	System	Cloud Backup	Firewall	INFO	---	Delete Cloud Backup Failed	%s

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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	Suspected Botnet initiator blocked: %s, Source: Dynamic List
1519	Security Services	Botnet Filter	---	ALERT	---	Botnet Responder Blocked	Suspected Botnet responder blocked: %s, Source: Dynamic List
1520	System	Settings	Maintenance	INFO	---	Email SFR Success	Successfully sent SFR file by email
1521	System	Settings	Maintenance	INFO	---	Email SFR Failed	Failed to send SFR file by email, %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	---	INFO	---	SonicWave License Expired	SonicWave %s
1526	Wireless	SonicPoint/SonicWave	---	INFO	---	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
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

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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
1539	System	Global Search	Debug	DEBUG	---	Global Search Data Download Success	Global Search Data downloaded successfully
1540	System	Global Search	Debug	INFO	---	Global Search Data Download Failed	Global Search Data download failed
1541	System	Global Search	Debug	INFO	---	Global Search Data Incorrect Hash	Global Search Data Invalid Server Hash
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
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
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

Event ID	SonicOS Category Name	SonicOS Group Name	Syslog Legacy Category	Priority Level	SNMP Trap Type	Event Name	Log Event Message
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

3

Syslog Events

This section provides information about using the detailed logs created from Syslog events. Syslog settings are configured in the **MANAGE** view on the **Log Settings > SYSLOG** page in SonicOS.

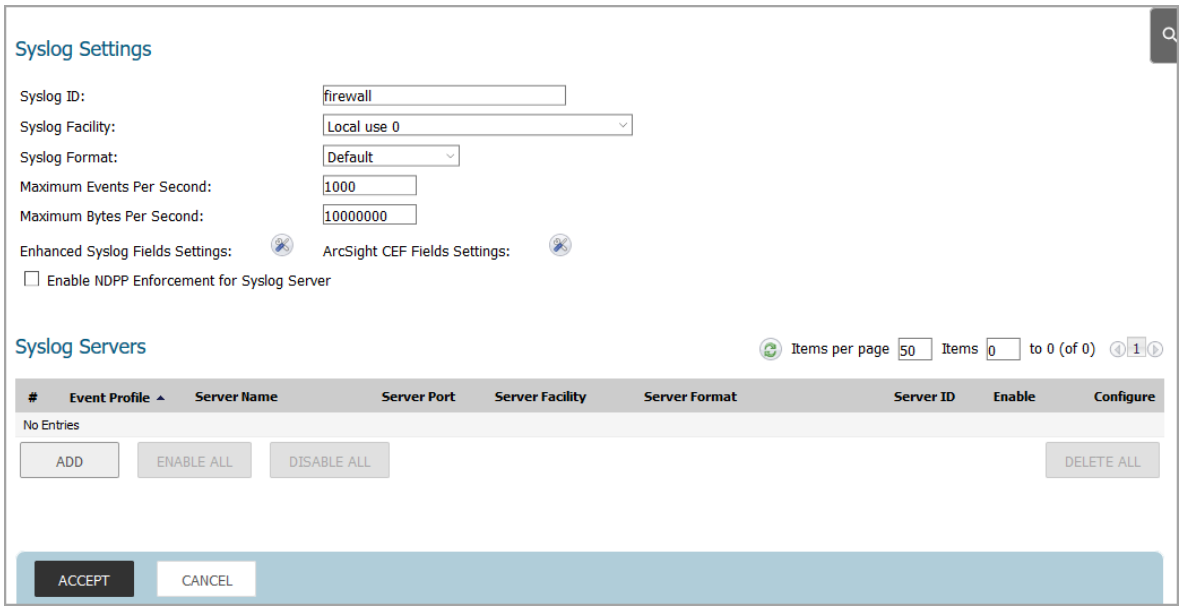
Topics:

Log Settings > 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 Analyzer or WebTrends Firewall Suite can be used to sort, analyze, and graph the Syslog data.

For more information on configuring the **Log Settings > SYSLOG** page, refer to the *SonicOS 6.5 Logs and Reporting* administration documentation.

Log Settings > SYSLOG Page



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 100. The value here is taken from the “Priority Level” column of the Index of Log Event Messages on page 7. For more information about the “c” Syslog Tag, see Legacy Categories on page 99.

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
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

Tag	Tags for Arc-Sight	Field	Description
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
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 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” 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
icmpCode	cn2	ICMP type and code	Indicates the ICMP code

Tag	Tags for Arc-Sight	Field	Description
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
	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
fwaction		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
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 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 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)
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 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
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

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 any packet analyzer application. Note that this is the Default Syslog Format.

```
<134>id=firewall sn=18B1690729A8 time="2016-07-07 21:34:52 UTC"
fw=10.205.123.15 pri=6 c=1 m=1460 msg="Gateway Anti-Virus Status:  File sent
to Capture ATP, receipt confirmed:
http://gsf-cf.softonic.com/99c/940/bf4a82884175db3ca674c4ad7cf6b41db1/
fdminst.exe?SD_used=0&channel=WEB&fdh=no&id_file=34870&instance=softonic_en
&type=PROGRAM&Expires=1467966751&Signatur"
fileid="b6a156a67658e2d22f04de5bd204bf86" filetxstatus=100 n=17
src=54.230.141.144:80:X1:server-54-230-141-144.sfo5.r.cloudfront.net
dst=192.168.168.10:64178:X0 proto=tcp/64178


<134>id=firewall sn=18B1690729A8 mgmtip=192.168.168.168 time="2016-08-19
00:21:40 UTC" fw=10.205.123.15 m=96 n=24789 i=60 lic=0 pt=8080.8443
usestandbysa=0 dyn=n.e ai=1 fwlan=192.168.168.168 conns=18


<134>id=firewall sn=18B1690729A8 time="2016-06-16 17:21:40 UTC"
fw=10.205.123.15 pri=6 c=1024 m=97 app=48 n=9 src=192.168.168.10:52589:X0
dst=69.192.240.232:443:X1:a69-192-240-232.deploy.akamaitechnologies.com
srcMac=98:90:96:de:f1:78 dstMac=ec:f4:bb:fb:f7:f6 proto=tcp/https op=1
sent=798 rcvd=12352 result=403 dstname=www.suntrust.com arg=/favicon.ico
code=20 Category="Online Banking"


<134>id=firewall sn=18B1690729A8 time="2016-08-19 17:15:19 UTC"
fw=10.205.123.15 pri=6 c=1024 m=537 msg="Connection Closed" app=44
n=1183392 src=10.205.122.22:514:X1 dst=10.205.123.15:514:X1
proto=udp/syslog sent=294 spkt=1


<134>id=firewall sn=18B1690729A8 fw=10.205.123.15 time="2016-08-19
18:05:44" pri=1 c=32 m=609 msg="IPS Prevention Alert: DNS named version
attempt" sid=143 ipscat=DNS ipspri=3 n=3 src=192.168.169.180:2907
dst=172.16.2.11:53
```

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.

```
MAR 20 2013 19:07:43 0017C5991784 CEF:0|SonicWall|NSA
2400|5.9.0.0-d_75o|97|Syslog Website Accessed|4|cat=1024 gcat=2 src=1.2.3.4
spt=5432 deviceInboundInterface=X0 cs1Label=1.2.4.5 snpt=1 dst=4.3.2.1
dpt=2345 deviceOutboundInterface=X1 cs2Label=5.4.3.2 dnpt=2 proto=tcp/2345
out=9876 in=6789 requestMethod=1 outcome=403
request=http://www.gui.log.eng.sonicwall.com reason=20 Category-"Online
Banking"


MAR 20 2013 19:07:49 0017C5991784 CEF:0|SonicWall|NSA
2400|5.9.0.0-d_75o|98|Syslog Connection Logged|4|cat=262144 gcat=2
src=192.168.168.1 spt=61693 deviceInboundInterface=X0 dst=192.168.168.168
dpt=443 deviceOutboundInterface=X0 susr="admin" proto=tcp/https out=52
cnt=1570


MAR 20 2013 19:07:52 0017C5991784 CEF:0|SonicWall|NSA
2400|5.9.0.0-d_75o|537|Syslog Close|4|cat=1024 gcat=2
smac=00:00:c5:b3:6b:e5 src=192.168.168.1 spt=61693
deviceInboundInterface=X0 cs3Label=Trusted dst=192.168.168.168 dpt=443
deviceOutboundInterface=X0 cs4Label=Trusted susr="admin" proto=tcp/https
out=1519 in=967 cn2Label=7 cn1Label=8 cn3Label=2333 cnt=3815


MAR 20 2013 19:07:43 0017C5991784 CEF:0|SonicWall|NSA
2400|5.9.0.0-d_75o|609|IDP Prevention Alert|9|cat=32 gcat=3 src=1.2.3.4
spt=5432 deviceInboundInterface=X0 cs1Label=1.2.4.5 snpt=1 dst=4.3.2.1
dpt=2345 deviceOutboundInterface=X1 cs2Label=5.4.3.2 dnpt=2 msg="IPS
Prevention Alert: P2P BitTorrent -- Peer Sync, SID: 1994, Priority: Low"
cnt=3


MAR 20 2013 19:07:43 0017C5991784 CEF:0|SonicWall|NSA
2400|5.9.0.0-d_75o|793|Application Firewall Alert|9|cat=16 gcat=10
src=1.2.3.4 spt=5432 deviceInboundInterface=X0 dst=4.3.2.1 dpt=2345
deviceOutboundInterface=X1 msg="Application Firewall Alert: Policy: foobar,
Action Type: Block SMTP E-Mail - Send Error Reply, Mail From: an unknown
string of unknown length" cnt=3
```

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 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.
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 Name for Syslog Tags. The value here is taken from the “Priority Level” column of the Log Event Message Index table, or the “pri” tag in Index of Syslog Tag Field Descriptions on page 90. 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

4

SonicWall Support

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

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 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.

SonicOS Log Events Reference Guide
Updated - June 2018
Software Version - 6.5.1
232-004342-00 Rev A