Syslog fields information

Content field details

There are total 16 different log types (including both server and client logs). Following section gives details of the CONTENT for each log type. Fields are in the order of their appearance.

System logs

	Field	Significance
	Time Stamp	Time stamp of the record. If "Export logs to a dump file" is enabled.
	Severity	Log severity. All, Information, Warning or Error
	Site name	SEPM site name
	Server name	Name of the SEPM server.
	Event description	Description of the event. Usually, the first line of the description is treated as the summary.

Administrative logs

	Field	Significance
	Time Stamp	Time stamp of the record. If "Export logs to a dump file" is enabled.
	Severity	Log severity. If "Export logs to a dump file" is enabled.
	Site name	SEPM site name
	Server name	Name of the SEPM server.
	Domain name	SEPM Domain name
	Admin name	SEPM admin name
	Event description	Description of the event. Usually, the first line of the description is treated as the summary.

Policy logs

	Field	Significance

	Time Stamp	Time stamp of the record. If "Export logs to a dump file" is enabled.
	Site name	SEPM site name
	Server name	Name of the SEPM server.
	Domain name	SEPM domain name
	Admin name	SEPM admin name
	Event Id :Event description	The unique ID of the policy event: 0 = The policy was added. 1 = The policy was deleted. 2 = The policy was edited. 3 = Added a shared policy upon system installation. 4 = Add a shared policy upon a system upgrade. 5 = Add a shared policy upon domain creation.
	Policy name	Name of the policy

Agent Activity logs

	Field	**Significance**
	Time Stamp	Time stamp of the record. If "Export logs to a dump file" is enabled.
	Site name	SEPM site name
	Server name	Name of the SEPM server.
	Domain name	SEPM domain name
	Event description	The behavior that was blocked.
	Host name	The host name of the client computer.
	User name	User logged on to the machine.
	Domain name	Machine domain name.

Enforcer Activity logs

	Field	**Significance**
	Time Stamp	Time stamp of the record. If "Export logs to a dump file" is enabled.
	Site name	SEPM site name

	Server name	Name of the SEPM server.
	Enforcer name	Name of the Enforcer
	Event description	Description of the event. Usually, the first line of the description is treated as the summary

Agent System logs

	Field	**Significance**
	Event Time	Time stamp of the record. If "Export logs to a dump file" is enabled.
	Severity	Severity description. If "Export logs to a dump file" is enabled.
	Host name	The host name of the client computer.
	Category	Not used at this time.
	Event source	The data source, such as NETPORT, NATSRV, etc.
	Event description	Description of the event. Usually, the first line of the description is treated as the summary
	Following fields till GateWay IP 4 are present only if property **scm.syslog.agentinfo=ON** is defined	
	IP Address1	IP address of the machine
	MAC Address1	
	GATEWAY1	
	IP Address2	
	MAC Address2	
	GATEWAY2	
	IP Address3	
	MAC Address3	
	GATEWAY3	
	IP Address4	

	MAC Address4	
	GATEWAY4	
	Event time	This field is always logged.

Agent Security logs

	Field	Significance
	Event time	If "Export logs to a dump file" is enabled.
	Severity	Severity description. If "Export logs to a dump file" is enabled.
	Host name	The host name of the client computer.
	Event description	Description of the event. Usually, the first line of the description is treated as the summary.
	Local IP address	The IP address of the local computer (IPv4).
	Local MAC address	The MAC address of the local computer.
	Remote Host name	The host name of the remote computer. This field may be empty if the name resolution failed.
	Remote IP address	The IP address of the remote computer (IPv4).
	Remote MAC address	The MAC address of the remote computer.
	Traffic direction	The direction of traffic. (Unknown = 0; inbound = 1; outbound = 2)
	Network protocol	The protocol type. (OTHERS = 1; TCP = 2; UDP = 3; ICMP = 4)

	Hack type	If event ID = 209, Host Integrity failed (TSLOG_SEC_NO_AV), the reason for the failure If Event ID = 206, Intrusion Prevention System(Intrusion Detected, TSLOG_SEC_INTRUSION_DETECTED), the intrusion ID If event ID = 210, Host Integrity passed(TSLOG_SEC_AV), additional information Possible reasons are as follows: Process is not running - Bit0 is 1 Signature is out of date - Bit1 is 1 Recovery was attempted - Bit2 is 1
	Begin time in yyyy-MM-dd HH:mm:ss	The start time of the security issue.
	End time in yyyy-MM-dd HH:mm:ss	The end time of the security issue. This field is an optional field because the exact end time of traffic may not be detected; for example, as with UDP traffic. If the end time is not detected, it is set to equal the start tim
	No. of occurrences	The number of attacks. Sometime, when a hacker launches a mass attack, it may be reduced to one event by the log system, depending on the damper period.
	Application name	The full path of the application involved. This field may be empty if an unknown application is involved, or no application is involved. For example, the ping of death DoS attack does not have an application name because it attacks the OS itself.
	Location name	The location used when the event occured.
	User name	The logon user name.
	Domain name	The logon domain name.
	Local port no.	The local port.
	Remote port no.	The remote port.
	CIDS signature ID	The signature ID.
	CIDS signature string	The signature name.
	CIDS signature sub ID	The signature sub ID.
	Intrusion URL	The URL from the detection.

	Intrusion payload URL	The URL that hosted the payload.	
	Following fields till GateWay IP 4 are present only if property **scm.syslog.agentinfo=ON** is defined		
	IP Address1	IP Address of the machine.	
	MAC Address1		
	GATEWAY1		
	IP Address2		
	MAC Address2		
	GATEWAY2		
	IP Address3		
	MAC Address3		
	GATEWAY3		
	IP Address4		
	MAC Address4		
	GATEWAY4		

Agent Traffic logs

	Field	**Significance**
	Event time	If "Export logs to a dump file" is enabled.
	Severity	Severity description. If "Export logs to a dump file" is enabled.
	Host name	The host name of the client computer.
	Local IP address	The IP address of the local computer (IPv4).
	Local port	The TCP/UDP port of the local computer (host byte-order). It is only valid on TSE_TRAFFIC_TCP and TSE_TRAFFIC_UDP. For other events, it is always zero.
	Local MAC address	The MAC address of the local computer.

	Remote IP address	The IP address of the remote computer (IPv4).
	Remote Host name	The host name of the remote client computer.
	Remote port	The TCP/UDP port of the remote computer (host byte-order). It is only valid on TSE_TRAFFIC_TCP and TSE_TRAFFIC_UDP. For other events, it is always zero.
	Remote Mac address	The MAC address of the remote computer.
	Network protocol	Localized string for Others/ TCP/ UDP/ ICMP
	Traffic direction	Localized strings for Unknown/ Inbound / Outbound
	Begin time in yyyy-MM-dd HH:mm:ss	The start time of the security issue.
	End time in yyyy-MM-dd HH:mm:ss	The end time of the security issue. This field is an optional field because the exact end time of traffic may not be detected; for example, as with UDP traffic. If the end time is not detected, it is set to equal the start time.
	No. of occurrences.	The number of attacks. Sometime, when a hacker launches a mass attack, it may be reduced to one event by the log system, depending on the damper period.
	Application name	The full path of application involved. It may be empty if an unknown application is involved or if no application is involved. For example, the ping of death DoS attack does not have AppName because it attacks the operating system itself.
	Rule name	The name of the rule that was triggered by the event. If the rule name is not specified in the security rule, then this field is empty. Having the rule name can be useful for troubleshooting. You may recognize a rule by the rule ID, but rule name can help you recognize it more quickly.
	Location name	The location used when the event occured.
	User Name	The logon user name.
	Domain name	The logon domain name.

	Following fields till GateWay IP 4 are present only if property **scm.syslog.agentinfo=ON** is defined	
	IP Address1	IP address of the machine.
	MAC Address1	
	GATEWAY1	
	IP Address2	
	MAC Address2	
	GATEWAY2	
	IP Address3	
	MAC Address3	
	GATEWAY3	
	IP Address4	
	MAC Address4	
	GATEWAY4	
	Action	Action description

Agent Packet logs

	Field	**Significance**
	Event time	If "Export logs to a dump file" is enabled.
	Host name	The host name of the client computer.
	Local IP address	The IP address of the local computer (IPv4).
	Local port	The TCP/UDP port of the local computer (host byte-order). It is only valid on TSE_TRAFFIC_TCP and TSE_TRAFFIC_UDP. For other events, it is always zero.
	Remote IP address	The IP address of the remote computer (IPv4).
	Remote Host name	The host name of the remote client computer.

	Remote port	The TCP/UDP port of the remote computer (host byte-order). It is only valid on TSE_TRAFFIC_TCP and TSE_TRAFFIC_UDP. For other events, it is always zero.
	Traffic direction	Localized strings for Unknown/ Inbound / Outbound
	Application name	The full path name of the application involved. It may be empty if an unknown application is involved or if no application is involved. For example, the ping of death DoS attack does not have an AppName because it attacks the operating system.
	Following fields till GateWay IP 4 are present only if property **scm.syslog.agentinfo=ON** is defined	
	IP Address1	IP address of the machine
	MAC Address1	
	GATEWAY1	
	IP Address2	
	MAC Address2	
	GATEWAY2	
	IP Address3	
	MAC Address3	
	GATEWAY3	
	IP Address4	
	MAC Address4	
	GATEWAY4	
	Action	Action description

Agent Behavior logs

	Field	**Significance**
	Event time	If "Export logs to a dump file" is enabled.

	Severity	Severity description. If "Export logs to a dump file" is enabled.
	Host name	The host name of the client computer.
	IP address	If **scm.syslog.agentinfo** is not defined or defined as **scm.syslog.agentinfo=OFF**
	Action description	The host name of the client computer.
	Event description	The behavior that was blocked.
	API name	API name that was blocked.
	Begin time in yyyy-MM-dd HH:mm:ss	The start time of the security issue.
	End time in yyyy-MM-dd HH:mm:ss	The end time of the security issue. This field is an optional field because the exact end time of traffic may not be detected; for example, as with UDP traffic. If the end time is not detected, it is set to equal the start time.
	Security Rule name	The name of the rule that was triggered by the event. If the rule name is not specified in the security rule, then this field is empty. Having the rule name can be useful for troubleshooting. You may recognize a rule by the rule ID, but rule name can help you recognize it more quickly.
	Caller process ID	The ID of the process that triggers the logging.
	Called process name	The full path name of the application involved. It may be empty if the application is unknown, or if OS itself is involved, or if no application is involved. Also, it may be empty if profile says, "don't log application name in raw traffic log".
	Caller return address	The return address of the caller. This field allows the detection of the calling module that makes the API call.
	Caller return module name	The module name of the caller. See CallerReturnAddress for more information.
	Parameters	Parameters that were used in the API call. Each parameter was converted to string format and separated by one space character. Double quotation mark characters within the string are escaped with a \ character.
	User name	Logon user name.

	Domain name	Logon windows domain name.
	Action type	The violation type that triggered the SymProtect event.
	File Size	The size of the file associated with the application control violation, in bytes.
	Device Id	The GUID of an external device (floppy disk, DVD, USB device, etc.)
	Following fields till GateWay IP 4 are present only if property **scm.syslog.agentinfo=ON** is defined	
	IP Address1	IP Address of the machine.
	MAC Address1	
	GATEWAY1	
	IP Address2	
	MAC Address2	
	GATEWAY2	
	IP Address3	
	MAC Address3	
	GATEWAY3	
	IP Address4	
	MAC Address4	
	GATEWAY4	

Agent Scan logs

	Field	**Significance**
	Time Stamp	Time stamp of the record. If "Export logs to a dump file" is enabled.
	Scan ID	The scan ID provided by the agent.
	Start date Time	The time that the scan started
	Stop date Time	The time that the scan stopped

	Status	Scan status as hard-coded English key:
		completed = Completed
		cancelled = Canceled
		started = Started

	Duration	The length of the scan, in seconds
	User name 1	User who was logged in when scan started.
	User name 2	User who was logged in when scan stopped.
	Message 1	Scan message when scan started.
	Message 2	Scan message when scan ended.
	Command	Command sent from the SEPM. ScanNow_Full = Do a full scan. ScanNow_Quick = Do an Active Scan. ScanNow_Custom = Do a custom scan. Update_ScanNow_Full = Update content and then do a full scan. Update_ScanNow_Quick = Update content and do an Active Scan. Update_ScanNow_Custom = Update content and do a custom scan. CancelScan = Cancel the scan.
	No. of threats found	The number of threats that the scan found.
	No. of infected files found	The number of files that the scan found that were infected.
	No. of files scanned	The number of files scanned.
	No. of files omitted	The number of files that were omitted.
	Computer	Name of the machine on which the scan was run
	IP address	IP address of the machine on which the scan was run
	Domain name	Domain name to which the machine belongs

	Client Group name	Client group name in the SEPM
	Server name	Name of the server.
	Following fields till GateWay IP 4 are present only if property **scm.syslog.agentinfo=ON** is defined	
	IP Address1	IP address of the computer.
	MAC Address1	
	GATEWAY1	
	IP Address2	
	MAC Address2	
	GATEWAY2	
	IP Address3	
	MAC Address3	
	GATEWAY3	
	IP Address4	
	MAC Address4	
	GATEWAY4	

Agent Risk logs

	Field	**Significance**
	Time Stamp	Time stamp of the record. If "Export logs to a dump file" is enabled.

	Description of action taken on risk.	1 = Quarantined 2 = Renamed 3 = Deleted 4 = Left alone 5 = Cleaned 6 = Cleaned or macros deleted 7 = Saved 9 = Moved back 10 = Renamed back 11 = Undone 12 = Bad 13 = Backed up 14 = Pending repair 15 = Partially repaired 16 = Process termination pending restart 17 = Excluded 18 = Restart processing 19 = Cleaned by deletion 20 = Access denied 21 = Process terminated 22 = No repair available 23 = All actions failed 24 = RepairFailedPowerEraser. A Power Eraser scan is recommended. Symantec Endpoint Protection cannot remove or clean the threat. Symantec Endpoint Protection can only block the threat. 25 = RepairFailedPowerEraser2. A Power Eraser scan is recommended. Symantec Endpoint Protection cannot remove or clean the threat. Symantec Endpoint Protection cannot confirm that it blocked the threat. 98 = Suspicious 99 = Details pending 100 = IDS block. 101 = Firewall violation. 102 = Allowed by user. 110 = Detected by using the commercial application list. 111 = Forced detection by using the file name. 200 = Attachment stripped. 1000 = Forced detection by using the file hash. 500 = Not applicable.
	IP address of infected machine	IP address of the infected machines

	Computer name	Name of the host machine
	Scan source	Hard-coded English string that is used as a lookup key for scan types: "Scheduled Scan" "Manual Scan" "Real-Time Scan" "Integrity Shield" "Definition downloader" "System" "Startup Scan" "DefWatch" "Manual Quarantine" "Reboot Processing" "Heuristic Scan"
	Virus name	Name of virus / threat
	No. of viruses	Number of events for aggregated event record. This can be due to client-side aggregation, server-side compression, or both.
	File path	The file path of the attacked file.
	Event Description	Description of the event

	Actual action taken on the risk.	-1 = Action invalid 1 = Quarantined 2 = Renamed 3 = Deleted 4 = Left alone 5 = Cleaned 6 = Cleaned or macros deleted 7 = Saved 9 = Moved back 10 = Renamed back 11 = Undone 12 = Bad 13 = Backed up 14 = Pending repair 15 = Partially repaired 16 = Process termination pending restart 17 = Excluded 18 = Restart processing 19 = Cleaned by deletion 20 = Access denied 21 = Process terminated 22 = No repair available 23 = All actions failed 24 = RepairFailedPowerEraser. A Power Eraser scan is recommended. Symantec Endpoint Protection cannot remove or clean the threat. Symantec Endpoint Protection can only block the threat. 25 = RepairFailedPowerEraser2. A Power Eraser scan is recommended. Symantec Endpoint Protection cannot remove or clean the threat. Symantec Endpoint Protection cannot confirm that it blocked the threat. 98 = Suspicious 99 = Details pending 100 = IDS block. 101 = Firewall violation. 102 = Allowed by user. 110 = Detected by using the commercial application list. 111 = Forced detection by using the file name. 200 = Attachment stripped. 1000 = Forced detection by using the file hash. 500 = Not applicable.

	First action defined in the policy	First actions can be similar to action taken on the risk
	Secondary action defined in the policy	Secondary actions can be similar to action taken on the risk
	Time of event occurrence	The time that the event occurred.
	Time when event was inserted into database	The time that the event was inserted into the database.
	End of aggregated event time	Time at which event ended. This is the end of the aggregated event time.
	GMT time stamp	The time on the server when the event is logged into the system or updated in the system (GMT).
	Domain name	SEPM Domain name
	Client group name	SEPM client group
	Server name	Name of the server.
	User name	Logged in User.
	Source computer name	Computer name where this event occurred
	Source computer IP	IP address of the machine on which the event occurred.
	Following fields till GateWay IP 4 are present only if property **scm.syslog.agentinfo=ON** is defined	
	IP address 1	IP Address of the machine
	Mac address 1	
	Gateway IP 1	
	IP address 2	
	Mac address 2	
	Gateway IP 2	
	IP address 3	
	Mac address 3	
	Gateway IP 3	
	IP address 4	

	Mac address 4	
	Gateway IP 4	
	Reputation information	Good, Bad or message saying reputation was not used in this detection
	URL	The URL determined from where the image was downloaded from. Default is "". This field belongs to creator for dropper application The creator process of the dropper threat. Default is "".
	Web domain	The web domain.
	Downloader	The creator process of the dropper threat. Default is "".
	Information on no. of users have seen this file	0: Unknown. 1-50: Very low 51-100: Low 101-150: Moderate 151-200: High 201-255: Very high > 255: Very high Default is 0
	Confidence level	High, low, bad, trustworthy etc.
	CIDS status	On, off, not installed, off by policy, malfunctioning etc.
	No. of days since the first time this file was seen	The first seen date for the convicted application Default is 0.
	Engine sensitivity that produced this detection	Between 0 to 100
	Reason for white listing	Not on the permitted application list / Symantec permitted application list / Administrator permitted application list / User permitted application list
	Application hash	The hash for this application.
	Hashing type	MD5, SHA1 or SHA2
	Company name	The company name

	Application name	The application name
	Application version	Version of the application
	Type	Trojan Worm, Key logger or Remote control
	File size	File size of application
	Risk Detection Type	Localized strings for Heuristic / Cookie / Admin Black List / BPE / System Change / N/A
	Translation	The translated name.
	Location name	The location used when the event occurred

Agent Proactive Detection logs (SONAR)

	Field	**Significance**
	Time Stamp	Time stamp of the record. If "Export logs to a dump file" is enabled.
	Description of action taken on risk.	This will be related to SONAR and the list can be found in Agent Risk logs section.
	Computer name	Name of the host machine
	IP address	If **scm.syslog.agentinfo** is not defined or defined as **scm.syslog.agentinfo=OFF**
	Detection type	Detection type: 0 = heuristic 1 = commercial application
	When was this first seen?	The first seen date for the convicted application Default is 0.
	Application name	The application name
	Application type	Trojan, key logger etc.
	Application version	The application version
	Application hash type	MD5, SHA1, SHA256 etc.
	Application hash	The hash for this application.
	Company name	The company name.
	File size	File size

	Sensitivity	Engine sensitivity setting that produced the detection.
	Detection score	Score of detection.
	COH engine version	TruScan engine version
	Recommendation	Recommendation in the form of YES or NO on whether to submit this detection to Symantec or not.
	White list reason	Not on the permitted application list / Symantec permitted application list / Administrator permitted application list / User permitted application list
	Disposition	Good / Bad / Unknown / Not available.
	URL	The URL determined from where the image was downloaded from. Default is "". This field belongs to creator for dropper application The creator process of the dropper threat. Default is "".
	Web domain	The web domain.
	Downloader	The creator process of the dropper threat. Default is "".
	Prevalence	No. of users seen this. 0: Unknown. 1-50: Very low 51-100: Low 101-150: Moderate 151-200: High 201-255: Very high > 255: Very high Default is 0
	Reputation	If disposition is good, this will have more fine level information such as how is reputation. Whether it is high, medium, low, bad, worst etc.

	CIDS on / off	Enabled state of CIDS 0 = off 1 = on 2 = not installed 127 = unknown.
	Risk level	The risk level (high, med, low) for the convicted threat. 0 -- Unknown 1 or 2 -- Low 3 -- Medium 4 -- High Default is 0.
	Risk type	Localized strings for Heuristic / Cookie / Admin Black List / BPE / System Change / N/A
	Source	Log risk action description
	Virus name	Name of virus / threat
	No. of viruses	Number of events for aggregated event record.
	File path for attacked file	File path
	Description	Description of the event
	Actual action taken	Actual action will be similar to the one see in Risk logs
	Requested action by policy	High Risk Detections: Log Remove Quarantine Low Risk Detections: Log Remove Quarantine Disabled DNS Changed detected, Host file change detected and Suspicious behavior detections: Ignore Prompt Block Log

	Secondary action requested by policy	None
	Time of events occurrences	The time that the event occurred.
	Time of events insertion into database	The time that the event was inserted into the database.
	Time of end of events	Time at which event ended. This is the end of the aggregated event time.
	Domain name	SEPM domain name
	Client group name	SEPM client group name
	Server name	Name of the server.
	User name	Logged in user name
	Source computer name	Computer name where this event occurred
	Source IP address	IP address of the machine on which the event occurred.
	Following fields till GateWay IP 4 are present only if property **scm.syslog.agentinfo=ON** is defined	
	IP address 1	IP address of the machine.
	Mac address 1	
	Gateway IP 1	
	IP address 2	
	Mac address 2	
	Gateway IP 2	
	IP address 3	
	Mac address 3	
	Gateway IP 3	
	IP address 4	
	Mac address 4	
	Gateway IP 4	

Enforcer System logs

	Field	Significance
	Event time	Time of event occurrence. If "Export logs to a dump file" is enabled.
	Severity	Log severity. If "Export logs to a dump file" is enabled.
	Enforcer type	Gateway / LAN / DHCP / Integrated / NAP / Peer To Peer
	Enforcer ID	The GUID of the Enforcer.
	Event description	Description of the event. Usually, the first line of the description is treated as the summary.

Enforcer Client Activity logs

	Field	Significance
	Event time	Time of event occurrence. If "Export logs to a dump file" is enabled.
	Enforcer type	Gateway / LAN / DHCP / Integrated / NAP / Peer To Peer
	Host name	If enforcer is of P2P, then host name, else enforcer Id.
	Event description	Description of the event. Usually, first line of the description is treated as the summary.
	Remote host	Remote host information.

	Action	The Enforcer's action on the client (a hard-coded English string that is used as lookup)
		
		Authenticated = Agent's UID is correct
		Rejected = Agent's UID is wrong or there's no agent running
		Disconnected = Agent disconnects from Enforcer or Enforcer service stops
		Passed = Agent has passed Host Integrity check
		Failed = Agent has failed Host Integrity check

Enforcer Traffic logs

	Field	Significance
	Event time	If "Export logs to a dump file" is enabled.
	Enforcer type	Gateway / LAN / DHCP / Integrated / NAP / Peer To Peer
	Enforcer ID	The GUID of the Enforcer
	Local IP address	The IP address of the local computer (IPv4).

	Local port	The TCP/UDP port on the local computer (host byte-order). It is only valid on TSE_TRAFFIC_TCP and TSE_TRAFFIC_UDP. For other events, it is always zero.
	Remote IP address	The IP address of the remote computer (IPv4)
	Remote port	The TCP/UDP port of the remote computer (host byte-order). It is only valid on TSE_TRAFFIC_TCP and TSE_TRAFFIC_UDP. For other events, it is always zero.
	Network protocol	Localized string for Others/ TCP/ UDP/ ICMP
	Traffic direction	Localized strings for Unknown/ Inbound / Outbound
	Begin time in yyyy-MM-dd HH:mm:ss	The start time of the Enforcer event.
	End time in yyyy-MM-dd HH:mm:ss	The end time of the Enforcer event.
	No. of occurrences.	The number of attacks. Sometime, when a hacker launches a mass attack, it may be reduced to one event by the log system, depending on the damper period.
	Action	Action description