How to export Check Point logs to a Syslog server using CPLogToSyslog

Solution ID	sk115392
Product	Security Management, Multi-Domain Management / Provider-1
Version	R77, R77.10, R77.20, R77.30, R80, R80.10
OS	Gaia, SecurePlatform 2.6
Platform / Model	All
Date Created	06-Jan-2017
Last Modified	30-May-2018

Solution

Table of Contents:

Click Here to Show the Entire Article

Note: Log Exporter, an easy and secure method for exporting Check Point logs over syslog, is now available.

(1) Introduction

CPLogToSyslog is a tool that allows exporting Check Point FireWall and Audit logs from Security Management Server / Multi-Domain Security Management Server / Log Server to Syslog Servers over Syslog protocol.

Logs can be exported from one or more Log Servers, and sent to one or more SysLog servers.

The CPLogToSyslog tool allows the administrator (via the built-in policy file) to filter the Check Point log files by type, source, service, and other fields in the log. Logs can be collected from one or more Management Servers / Log Servers, and can be sent to one or more SysLog servers.

Action plan:

1. Install the CPLogToSyslog tool on the relevant Check Point Management Server / Log Server
2. Manually configure the CPLogToSyslog policy file (`$FWDIR/state/SEAM/local.cplogtosyslog_policy.C`) as described in section "(5) Configuration instructions"
3. Configure the automatic start of the CPLogToSyslog tool (if desired) as described in section "(9) Starting CPLogToSyslog"

(2) Supported versions

Deployment	• Security Management Server • Multi-Domain Security Management Server • Log Server
Version	• R80.10 • R80 • R77.30 • R77.20 • R77.10 • R77
Operating System	• Gaia OS • SecurePlatform OS

(3) Known Limitations

Show / Hide this section

(4) Installation instructions

Click Here to Show the Entire Section

The *CPLogToSyslog* package for Management Server / Log Server running *on Gaia OS* is provided directly in this article.

Note: In Management HA environment, this procedure must be performed on *both* Management Servers.

Version of Management Server [1]	Prerequisite [2]	CPUSE Identifier	CPUSE Offline
R80.10 on Gaia OS	R80.10 GA (Take 421) up to *Take 56* (including) of R80.10 Jumbo Hotfix	`Check_Point_CPLogToSyslog_R80.10_GA_jhf_T56_FULL.tgz`	(TGZ)
R80 on Gaia OS	R80 GA (Take 103)	`Check_Point_CPLogToSyslog_R80.tgz`	(TGZ)
	R80 GA (Take 132), or R80 GA (lower than Take 132) with *Take 76* of R80 Jumbo Hotfix	`Check_Point_CPLogToSyslog_R80_JUMBO_HF_T76.tgz`	(TGZ)
R77.30 on Gaia OS	R77.30 GA (Take 204)	`Check_Point_CPLogToSyslog_R77.30.tgz`	(TGZ)
	R77.30 GA with *Take 205* of R77.30 Jumbo Hotfix	`Check_Point_CPLogToSyslog_R77_30_Jumbo_HF_T205.tgz`	(TGZ)
	R77.30 GA with *Take 216* of R77.30 Jumbo Hotfix	`Check_Point_CPLogToSyslog_R77_30_Jumbo_HF_T216.tgz`	(TGZ)
R77.20 on Gaia OS	R77.20 GA (Take 124)	`Check_Point_CPLogToSyslog_R77.20.tgz`	(TGZ)
R77.10 on Gaia OS	R77.10 GA (Take 151)	`Check_Point_CPLogToSyslog_R77.10.tgz`	(TGZ)

Notes:

- For other supported versions, or for Management Server / Log Server running on *SecurePlatform OS*, contact Check Point Support to check if this package can be created for your environment.
  For faster resolution and verification, please collect CPInfo file from the Management Server / Log Server.
- These CPLogToSyslog packages can be installed *only* on the specified GA Releases (without any hotfixes) / specified Takes of Jumbo Hotfix Accumulators.
  For other Takes of Jumbo Hotfix Accumulator, contact Check Point Support to check if this package can be created for your environment.
  For faster resolution and verification, please collect CPInfo file from the Management Server / Log Server..

Instructions:

- Show / Hide instructions for installation in Gaia Portal - using CPUSE (Check Point Update Service Engine)

  For detailed installation instructions, refer to sk92449: CPUSE - Gaia Software Updates (including Gaia Software Updates Agent) - section "*(4) How to work with CPUSE*".

  - Online installation

    1. CPUSE Software Updates Policy should be configured to allow self-update of CPUSE Agent.

Otherwise, users should manually install the latest build of CPUSE Agent from sk92449.

2. Connect to the Gaia Portal on your Check Point machine and navigate to *Upgrades (CPUSE)* section - click on *Status and Actions*.
3. In the upper right corner, click on the *Add hotfixes from the cloud* button in the upper right corner.
4. Paste the CPUSE Identifier and start the search.
5. When the package is found, click on the link to add the package to the list of available packages.
6. Select the hotfix package - click on *More* button on the toolbar - click on *Verifier* (or right-click on the package and click on *Verifier*).
7. Select the package - click on *Install Update* button on the toolbar.
8. Manual restart of the Check Point services is required ('**cpstop ; cpstart**').

- Offline installation

  Note: Either get the offline package from the table above, or export the package from a source Gaia machine, on which this package was already downloaded / installed (for package export instructions, refer to sk92449 - section "*(4-D) "How to ..."*").

  1. Install the latest build of CPUSE Agent from sk92449.
  2. Connect to the Gaia Portal on your Check Point machine and navigate to *Upgrades (CPUSE)* section - click on *Status and Actions*.
  3. On the toolbar, click on the *More* button and select *Import Package*.
  4. In the *Import Package* window, click on *Browse...* - select the CPUSE package (either offline TGZ file, or exported TAR file) - click on *Upload*.
  5. Select the imported package - click on *More* button on the toolbar - click on *Verifier* (or right-click on the package and click on *Verifier*).
  6. Select the imported package - click on *Install Update* button on the toolbar.
  7. Manual restart of the Check Point services is required ('**cpstop ; cpstart**').

- Show / Hide instructions for installation in Gaia Clish - using CPUSE (Check Point Update Service Engine)
- Show / Hide instructions for installation on SecurePlatform OS - using Legacy CLI

(5) Configuration instructions

The following sections provide the detailed configuration instructions.

Before you begin, make sure you have this data:

- IP addresses of Security Management Server / Domain Log Server / Log Server, from which the logs are exported
- IP addresses of SysLog server(s), to which the exported logs are sent

Important Notes:

- Your SysLog server(s) must already be configured properly in order to get all / relevant logs.

  For example, it might be required to modify the */etc/syslog.conf* file on your SysLog server

  from

  ```
  *.info;mail.none;authpriv.none;cron.none                /var/log/messages
  ```

  to

  ```
  *.*                /var/log/messages
  ```

- If you make any changes in the Policy File, then you must restart the `CPLogToSyslog` (refer to the "(10) CPLogToSyslog process" section).
- On Multi-Domain Security Management Server, the Policy File must be configured in the context of the relevant Domain Management Server (`mdsenv <Name or IP of Domain Management Server>`).

Instructions:

Click Here to Show all subsections

- (5-A) Configuration instructions - Background

  Show / Hide this subsection

  - The CPLogToSyslog configuration is stored in the following policy file:

    $FWDIR/state/SEAM/local.cplogtosyslog_policy.C

    On Multi-Domain Security Management Server, this Policy File is located in the context of each Domain Management Server (`mdsenv <Name or IP of Domain Management Server>`).

    This is the default Policy File:

    ```
    (
       :customers ()
       :events_detectors (
          :Red_EventsDetector ("{01C36C58-35AF-4b65-A277-01F74E56E552}")
       )
       :data_types (
          :lea_audit_input_session ("{42296380-1671-4BA2-B66D-047D2B96E3BC}")
          :lea_log_input_session ("{42296380-1671-4BA2-B66D-047D2B96E3BC}")
    ```

```
)
:events_distributor (
   :CLSID ("{CD6872DE-10A2-4632-B9F3-714E3CE9A0A6}")
   :syslog_servers (
      : (
         :ip_addr ("192.168.100.1")
         :server_name ("syslog server control")
         :server_id (1)
         :port (514)
         :protocol (udp)
      )
      : (
         :ip_addr ("192.168.100.1")
         :server_name ("syslog server Log")
         :server_id (2)
         :port (514)
         :protocol (udp)
      )
   )
)
:jobs (
   :"All online jobs" ("{42DC9EE4-1529-4cb4-B4D9-E850AA328EDA}"
      :job_is_online (true)
      :job_is_canceled (false)
      :detectors_instances (
         :Red_EventsDetector ("{F42EE20C-CB81-4FDA-B6E8-AC916156C368}"
            :instance_is_online (true)
            :run_in_main_thread (true)
            :input_sessions (
               :lea_log_input_session ("{58281420-7DAA-47FD-BF27-6E64D0CAC844}"
                  :ip_addr (192.168.0.1)
                  :port (18184)
                  :logtrack (LEA_CURRENT_NORMAL_FILEID)
                  :iS_auth_port (true)
                  :mode (LEA_ONLINE)
                  :startat (LEA_AT_END)
                  :filename ()
                  :support_marker (false)
                  :save_marker_interval (600)
               )
            )
            :events_detecting_policy (
               :global_parameters (
                  :garbage_collector_interval (60)
                  :max_vm_size (1000000)
                  :time_mode (os_time)
               )
               :rulebase (
                  : (ctrl_type_filter
                     :ruleID ("{F0461B27-6D0F-43f9-A9BF-639454A8D971}")
                     :active (on)
                     :type ("single log event")
                     :category ()
                     :detection (
                        :source_data ()
                        :groupby ()
                        :analyze (
                           :type (resolution)
                           :resolution (0)
                        )
                        :parameters ()
                        :action ()
                        :filter (Equal
                           :field_name (Type)
                           :field_value (control)
                        )
                     )
                     :event_format (
                        :class_name (syslog_event_builder)
                        :severity (1)
                        :facility (2)
                        :add_time_stamp (true)
                        :host_name ("Control host")
                        :field_seperator (";")
                        :TAG ("CPLogToSyslog")
                        :event_name ("Control log type")
                        :server_id (1)
                     )
                     :create_for_all_detector_instances (false)
                  )
                  : (log_type_filter
                     :ruleID ("{F0461B27-6D0F-43f9-A9BF-639454A83973}")
                     :active (on)
                     :type ("single log event")
                     :category ()
                     :detection (
                        :source_data ()
                        :groupby ()
                        :analyze (
                           :type (resolution)
                           :resolution (0)
                        )
                        :parameters ()
                        :action ()
                        :filter (Equal
                           :field_name (Type)
```

```
                                        :field_value (log)
                                    )
                                )
                                :event_format (
                                    :class_name (syslog_event_builder)
                                    :severity (5)
                                    :facility (6)
                                    :add_time_stamp (true)
                                    :host_name ("Log host")
                                    :field_seperator (";")
                                    :TAG ("CPLogToSyslog")
                                    :event_name ("Log type log")
                                    :server_id (2)
                                )
                                :create_for_all_detector_instances (false)
                            )
                        )
                    )
                )
            )
        )
    )
```

- Before making any changes in the policy file, you should back it up:

  [Expert@HostName:0]# cp -v $FWDIR/state/SEAM/local.cplogtosyslog_policy.C{,_ORIGINAL}

- To edit the policy file, use Vi editor (or any advanced text editor like Notepad++):

  [Expert@HostName:0]# vi $FWDIR/state/SEAM/local.cplogtosyslog_policy.C

  If you edited the policy file on Windows OS computer and transferred it to the Check Point machine, then make sure to convert the file from DOS format to UNIX format:
  `[Expert@HostName:0]# dos2unix $FWDIR/state/SEAM/local.cplogtosyslog_policy.C`

- It is recommended that you copy the default code provided in this section (5-A) and modify it as needed.

- (5-B) Configuration instructions - Log Input Session

  Show / Hide this subsection

- (5-C) Configuration instructions - Audit Input Session

  Show / Hide this subsection

  Part 1 - Default Audit Input Session

  Check Point Management Server / Log Servers generate these types of logs that can be exported to SysLog servers:

  - *Log* files show incoming and outgoing activities on the network.
  - *Audit* files show administrative activities.

  An *audit input session* in the policy defines how audit logs are read from a Management Server / Log Server.

  Notes:

  - The difference between an *audit* input session and a *log* input session definitions is in the *lea_audit_input_session* field and the *logtrack* field.
  - Refer to the following section at the top of the policy file:

    ```
    :data_types (
            :lea_audit_input_session ("{42296380-1671-4BA2-B66D-047D2B96E3BC}")
            :lea_log_input_session ("{42296380-1671-4BA2-B66D-047D2B96E3BC}")
    )
    ```

  This is the default audit input session:

  ```
  :input_sessions (
          :lea_audit_input_session ("{58281420-7DAA-47FD-BF27-6E64D0CAC844}"
                  :ip_addr (192.168.100.10)
                  :port (18184)
                  :logtrack (LEA_CURRENT_AUDIT_FILEID)
                  :is_auth_port (true)
                  :mode (LEA_ONLINE)
                  :startat (LEA_AT_END)
                  :filename ()
                  :support_marker (true)
                  :save_marker_interval (10)
                  )
  )
  ```

  Where:

Attribute	Description

`ip_addr`	Defines the IP address of Security Management Server / Domain Log Server / Log Server, from which the logs are exported
`support_marker`	Defines whether a persistent marker should be set (refer to the "(6) Setting Markers" section): ○ "`true`" - a persistent marker will be set ○ "`false`" - a temporary marker will be used
`save_marker_interval`	Defines the number of seconds, after which persistent markers are saved to the hard drive

Part 2 - Define your Audit Input Session

Copy the default code provided in Part 1 above and modify it as needed.

You can define multiple Audit Input sessions to export audit logs from multiple Management Servers / Log Servers.

This is an example of an Audit Input session:

```
:input_sessions (
        :lea_audit_input_session ("{58281420-7DAA-47FD-BF27-6E64D0CAC844}"
                :ip_addr (192.168.100.10)
                :port (18184)
                :logtrack (LEA_CURRENT_AUDIT_FILEID)
                :is_auth_port (true)
                :mode (LEA_ONLINE)
                :startat (LEA_AT_END)
                :filename ()
                :support_marker (true)
                :save_marker_interval (10)
                )
)
```

- (5-D) Configuration instructions - SysLog Servers

Show / Hide this subsection

Part 1 - Default SysLog Servers

This is the default configuration for SysLog Servers:

```
:syslog_servers (
        : (
                :ip_addr ("192.168.100.1")
                :server_name ("sysLog server control")
                :server_id (1)
                :port (514)
                :protocol (udp)
        )
        : (
                :ip_addr ("192.168.100.1")
                :server_name ("sysLog server Log")
                :server_id (2)
                :port (514)
                :protocol (udp)
        )
)
```

Note: You can define multiple such instances to export to multiple SysLog Servers.

Where:

Attribute	Description
`ip_addr`	Defines the IP address of SysLog Server, to which the logs are sent
`server_name`	Used for server's identification only
`server_id`	Defines a unique number between 1 and 1000 that identifies this SysLog server in CPLogToSyslog. The same ID must be used to refer to the SysLog server in the "(5-E) Configuration instructions - Rulebase" section.
`port`	Defines the port on the SysLog server, to which the logs are sent (default is 514)
`protocol`	Defines over which protocol (UDP / TCP) the logs are sent. Follow sk109016 - CPLogToSyslog processes stop running after a few minutes.

Part 2 - Define your SysLog Servers

Modify the default code provided in Part 1 as needed.

You can define multiple such instances to export to multiple SysLog Servers.

This is an example of Syslog Servers configuration:

```
:syslog_servers (
        : (
                :ip_addr ("192.168.100.1")
                :server_name ("SysLog server Control")
                :server_id (1)
                :port (514)
```

```
                :protocol (udp)
        )
        : (
                :ip_addr ("192.168.100.2")
                :server_name ("SysLog server Log")
                :server_id (2)
                :port (514)
                :protocol (udp)
        )
)
```

- (5-E) Configuration instructions - Rulebase

  Show / Hide this subsection

  Part 1 - Default Rule

  These rules define the type of logs to export, to which SysLog server they should be sent, and how to send them.

```
:rulebase (
        : (ctrl_type_filter
                :ruleID ("{F0461B27-6D0F-43f9-A9BF-639454A8D971}")
                :active (on)
                :type ("single log event")
                :category ()
                :detection (
                        :source_data ()
                        :groupby ()
                        :analyze (
                                :type (resolution)
                                :resolution (0)
                        )
                        :parameters ()
                        :action ()
                        :filter (Equal
                                :field_name (Type)
                                :field_value (control)
                        )
                )
                :event_format (
                        :class_name (syslog_event_builder)
                        :sevirity (1)
                        :facility (2)
                        :add_time_stamp (true)
                        :host_name ("Control host")
                        :field_seperator (";")
                        :TAG ("CPLogToSyslog")
                        :event_name ("Control log type")
                        :server_id (1)
                )
                :create_for_all_detector_instances (false)
        )
```

  Note: You can define multiple such rules (each with its unique name and unique ID) to export multiple log types.

  Where:

Attribute	Description
`ctrl_type_filter`	Placeholder for the unique name of this rule (a string without white spaces)
`ruleID`	Defines unique rule ID. You must use a GUID Generator (e.g., https://www.guidgenerator.com).
`active`	Defines whether this rule is active (`on`), or not (`off`)
`filter`	Defines the filter (case-sensitive) - "`Equal`", "`And`", "`Or`": ○ Use "`Equal`" to name specific fields, with the given value ○ Use "`And`" or "`Or`" to define criteria to match field names and values Note: Multiple filters can be defined within each rule.
`field_name`	Defines the log field name to be exported (case-sensitive). It must match a SmartView Tracker / SmartLog log field name as listed in section "(8) Mapping of log field names between SmartView Tracker / SmartLog and Check Point Log". You can refer to some examples in subsection "*Part 3 - Define your Log Filters*" below.
`field_value`	Defines the exact value for logs you want to export (case-sensitive).
`severity`	Defines the severity of the log - refer to the "(7-A) Syslog Indicators - Severity Indicators" section
`facility`	Defines the facility of the log - refer to the "(7-B) Syslog Indicators - Facility Indicators" section
`host_name`	Defines the name to identify the host computer
`event_name`	Defines the description of the rule
`server_id`	Defines a unique number between 1 and 1000 that identifies this SysLog server in CPLogToSyslog. The same ID must be used to refer to the SysLog server in the "(5-D) Configuration instructions - SysLog Servers" section.

The export log format is based on the standard parts of a syslog message.
This is an example of a syslog message:

```
<16>Sun Mar 23 10:33:53 Log host CPLogToSyslog: 10:33:53 16386 accept 192.168.100.10 >vmxnet0
rule: 1; rule_uid: {CBA1863B-2B4F-4E59-A257-4CCFD6146C4C}; service_id: nbdatagram; src:
192.168.100.1; dst: 192.168.100.255; proto: 17; aba_customer: Default; date: 23Mar2012; hour:
10:33:53; type: log; Interface: < vmxnet0; product: VPN & FireWall; service: 138; s_port:
138;
```

The parts of a Syslog message that are reflected in the CPLogToSyslog rules are:

- PRI - Priority, with numbers to show Facility and Severity - refer to the "[7] Syslog Indicators" section
- Header - Time when the message is sent, and indication of a hostname
- MSG:
  - TAG - Name of the Check Point product that generated the message
  - Content: Details of the message, and timestamp of when the message was logged

Part 2 - Define your Rule Names and GUIDs

Copy the default code provided in Part 1 above and modify it as needed.

You can define multiple rules (each with its unique name and unique ID) to export multiple log types.

- In the place of the "`ctrl_type_filter`", enter the unique name of this rule.
- In the "`ruleID`", enter the unique rule ID - you must use a GUID Generator (e.g., https://www.guidgenerator.com).

This is an example section of a custom rule:

```
: (This_is_My_Rule_1
        :ruleID ("{D81EC45E-09F4-46BB-A4F4-B4C211EF2405}")
        :active (on)
        :type ("single log event")
        :category ()
        :detection (
                :source_data ()
                :groupby ()
                :analyze (
                        :type (resolution)
                        :resolution (0)
                )
                ... ...
```

Part 3 - Define your Log Filters

Copy the default code provided in Part 1 above and modify it as needed.

Note: Multiple filters can be defined within each rule.

This is an example section of a custom rule:

```
: (This_is_My_Rule_1
        :ruleID ("{D81EC45E-09F4-46BB-A4F4-B4C211EF2405}")
        :active (on)
        :type ("single log event")
        :category ()
        :detection (
                :source_data ()
                :groupby ()
                :analyze (
                        :type (resolution)
                        :resolution (0)
                )
                :parameters ()
                :action ()
                :filter (Equal
                        :field_name (Product)
                        :field_value ("Firewall")
                )
                :filter (Or
                        : (Equal
                                :field_name (Src)
                                :field_value (192.168.0.1)
                        )
                        : (Equal
                                :field_name (Dst)
                                :field_value (192.168.0.1)
                        )
                )
                :filter (And
                        : (Equal
                                :field_name (Src)
                                :field_value (192.168.0.1)
                        )
                        : (Equal
                                :field_name (Dst)
                                :field_value (192.168.0.2)
                        )
                        : (And
                                : (Equal
                                        :field_name (service)
```

```
                                        :field_value (80)
                                )
                                : (Equal
                                        :field_name (Proto)
                                        :field_value (6)
                                )
                        )
                )
                ... ...
```

Part 4 - Define How Logs are Sent

Copy the default code provided in Part 1 above and modify it as needed.

Note: Multiple filters can be defined within each rule.

This is an example of a custom rule:

```
: (This_is_My_Rule_1
        :ruleID ("{D81EC45E-09F4-46BB-A4F4-B4C211EF2405}")
        :active (on)
        :type ("single log event")
        :category ()
        :detection (
                :source_data ()
                :groupby ()
                :analyze (
                        :type (resolution)
                        :resolution (0)
                )
                :parameters ()
                :action ()
                :filter (Equal
                        :field_name (Product)
                        :field_value ("Firewall")
                )
                :filter (Or
                        : (Equal
                                :field_name (Src)
                                :field_value (192.168.0.1)
                        )
                        : (Equal
                                :field_name (Dst)
                                :field_value (192.168.0.1)
                        )
                )
                :filter (And
                        : (Equal
                                :field_name (Src)
                                :field_value (192.168.0.1)
                        )
                        : (Equal
                                :field_name (Dst)
                                :field_value (192.168.0.2)
                        )
                        : (And
                                : (Equal
                                        :field_name (service)
                                        :field_value (80)
                                )
                                : (Equal
                                        :field_name (Proto)
                                        :field_value (6)
                                )
                        )
                )
        :event_format (
                :class_name (syslog_event_builder)
                :severity (1)
                :facility (2)
                :add_time_stamp (true)
                :host_name ("Control host")
                :field_seperator (";")
                :TAG ("CPLogToSyslog")
                :event_name ("Control log type")
                :server_id (1)
        )
        :create_for_all_detector_instances (false)
)
```

(6) Setting Markers

When you define input sessions, you can configure markers (refer to section "(5-B) Configuration instructions - Log Input Session" and to section "(5-C) Configuration instructions - Audit Input Session").

Markers show when the Security Management Server / Domain Log Server / Log Server has last exported logs to the SysLog server.

Click Here to Collapse the Entire Section

- (6-A) Setting Markers - Temporary Markers

Show / Hide this subsection

- (6-B) Setting Markers - Persistent Markers

  Show / Hide this subsection

(7) Syslog Indicators

Click Here to Show the Entire Section

- (7-A) Syslog Indicators - Severity (Priority) Indicators

  Show / Hide this subsection

- (7-B) Syslog Indicators - Facility Indicators

  Show / Hide this subsection

(8) Mapping of log field names between SmartView Tracker / SmartLog and Check Point Log

Show / Hide this section

The table below provides the mapping of log field names between how they appear in the SmartView Tracker / SmartLog GUI and how they appear in the Check Point Log itself.

This information is required to define correctly the '`field_name`' attribute in the Default Rule of the Policy File as mentioned in section "(5-E) Configuration instructions - Rulebase".

Note: The table is sorted by the *leftmost* column in the alphabetical ascending order.

Field Short Name in SmartView Tracker / SmartLog	Field Long Name in SmartView Tracker / SmartLog	Field Name in Check Point Log
__policy_id_tag	__policy_id_tag	__policy_id_tag
Access	Access	access_status
Act.	Action	Action
Activity	Activity	activity
Admin.	Administrator	Administrator
Anti Virus	Anti Virus	Anti_Virus_type
Anti-Spyware Action	Anti-Spyware Action	spyware_action
Anti-Spyware Status	Anti-Spyware Status	spyware_status
APN	APN	apn
App. Byte/Sec in	Application Byte/Sec in	app_byte_ps_in
App. Byte/Sec Out	Application Byte/Sec Out	app_byte_ps_out
App. Dst.IP	Application Destination IP	application_ip
App. Name	Application Name	app_name
App. Packet/Sec in	Application Packet/Sec in	app_pack_ps_in
App. Packet/Sec Out	Application Packet/Sec Out	app_pack_ps_out
App. Port	Application Port	application_port
Application	Application	cvpn_resource
Application	Application	ProductNameInAuditMode
Attack	Attack	attack
Attack Info.	Attack Information	Attack Info
Auth Domain	Auth Domain	auth_domain
Auth. Method	Authentication	Method auth_method
Auth. Status	Authentication	Status auth_status
AV Mail Recipient	Integrity AV Mail Recipient	integrity_av_email_to
BW Loss Threshold%	BW Loss Threshold%	bw_loss_threshold
BW Loss%	BW Loss%	bw_loss
Bytes	Bytes	bytes

Categories	Categories	categories
Category	Category	cvpn_category
Changes	Changes	FieldsChanges
CIR Bps	CIR Bps	cir
CIR Threshold Bps	CIR Threshold Bps	cir_threshold
Client	Client	Machine
Client Bytes In	Client Inbound Bytes	client_inbound_bytes
Client Bytes Out	Client Outbound Bytes	client_outbound_bytes
Client DiffServ In	Client Inbound DiffServ	client_inbound_diffserv
Client DiffServ Out	Client Outbound DiffServ	client_outbound_diffserv
Client In rule match	Client In rule match	fg-1_client_in_rule_name
Client Interface In	Client Inbound Interface	client_inbound_interface
Client Interface Out	Client Outbound Interface	client_outbound_interface
Client Out rule match	Client Out rule match	fg-1_client_out_rule_name
Client Packets In	Client Inbound Packets	client_inbound_packets
Client Packets Out	Client Outbound Packets	client_outbound_packets
Comment	Comment	comment
Community	Community	Community
Compliance Action	Compliance Action	compliance_action
Compliance Rule	Compliance Rule	compliance_name
Compliance Type	Compliance Type	compliance_type
Conn. ID	Connection ID	command:
Container Changes	Container Changes	ContainerChanges
Curr. Rule No.	Current Rule Number	normalized_rule_num
Date	Date	Date
Description	Description	description
Display Name	Display Name	d_name
Domain	Domain	domain_name
Dst GW	Destination Gateway	dst_gw
Dst.	Destination	Dst
Dst. IP-phone	Destination IP-phone	dst phone number
DstKeyId	Destination Key ID	dstkeyid
E2E Enc.	End to End Encryption	e2e_enc_desc
Elapsed	Elapsed	active_conn_elapsed
Elapsed	Elapsed	elapsed
Enc Scheme	Encryption Scheme	scheme:
Enc. Methods	Encryption Methods	methods:
Enc. Type	Encryption Type	enc_desc
End User fw.	End User Firewall	End_User_Firewall_type
Endpoint ID	Endpoint ID	endpoint_id
Endpoint IP	Endpoint IP	endpoint_ip
Endpoint Name	Endpoint Name	endpoint_addr
Estimation	Estimation	estimation
EU IP	End User IP Address	end_user_address
EU IPv6	End User IPv6 Address	end_user_address_ipv6
Event Count	Event Count	event_count
Event Type	Event Type	event_type
File Direction	File Direction	scan direction
File Name	File Name	file_name
File Origin	File Origin	data origin

File Type	File Type	file_type
FS Protocol	FS Protocol	fs_proto
General Info.	General Information	Additional Info
GGSN Signal	GGSN for Signal	ggsn_signal
GGSN Traffic	GGSN for Traffic	ggsn_traffic
GTP Msg. Type	GTP Message Type	signal_type
GTP Version	GTP Version	gtp_ver
Headers in/out	Headers inserted/removed	wa_headers
ICS Access Status	ICS Access Status	ICS_access_status
ICS Scan	ICS Scan	user_ics
ICS Scan ID	ICS Scan ID	ICS_scan_id
ICS Scan Status	ICS Scan Status	ICS_scan_status
ID Source	ID Source	id_src
IKE CookieI	IKE Initiator	Cookie CookieI
IKE CookieR	IKE Responder	Cookie CookieR
IKE Phase2 MsgID	IKE Phase2 Message ID	msgid
IM Event	IM Event	im_event
IM Protocol	IM Protocol	im_protocol
IM User	IM User	im_userid
IMEI-SV	International Mobile Equipment Identifier	imei
Info.	Information	Info
Integrity AV Mail Sender	Integrity AV Mail Sender	integrity_av_email_from
Integrity AV Scan Type	Integrity AV Scan Type	integrity_av_invoke_type
Integrity Scan Event	Integrity Scan Event	integrity_av_event
Inter.	Interface	interface
IPv6 Dst.	IPv6 Destination	ipv6_dst
IPv6 Src.	IPv6 Source	ipv6_src
ISB	ISB	user_isb
Linked NSAPI	Linked NSAPI	linked_nsapi
Malware Name	Malware Name	spyware_name
Malware Type	Malware Type	spyware_type
MCC	Mobile Country Code	mobile_country_code
Media Type	Media Type	media type
MNC	Mobile Network Code	mobile_network_code
MS Time Zone	Mobile Subscriber Time Zone	time_zone
MSIN	MS Identification Number	mobile_subscriber_code
MS-ISDN	MS-ISDN	ms_isdn
NAT add. rule num.	NAT additional rule number	NAT_addtnl_rulenum
NAT rule num.	NAT rule number	NAT_rulenum
No.	Number	num
NSAPI	NSAPI	nsapi
Object Tbl.	Object Table	ObjectTable
Object Type	Object Type	ObjectType
Op. Num.	Operation Number	Operation Number
Operation	Operation	Operation
Operation	Operation	ua_operation
Orig.	Origin	Origin
Out. URL	Outgoing URL	outgoing_url
Packets	Packets	packets
Partner	Partner	partner

Performed On	Performed On	ObjectName
Policy	Policy	policy_name
Prd.	Product	ProductName
Proto.	Protocol	Proto
RAT	Radio Access Type	rat_type
Reason	Reason	reason
Redirect URL	Redirect URL	redirect_url
Redirection dst.	Redirection destination	r_dest
Reg. IP-phones	Registered IP-phones	Registered IP-phones
Reject ID	Reject ID	reject_id
Reject Reason	Reject Reason	reject_category
Request Result	Request Result	result_desc
Resource	Resource	resource
RTT ms	RTT ms	rtt
RTT Threshold ms	RTT Threshold ms	rtt_threshold
Rule	Rule	Rule
Rule Name	Rule Name	rule_name
Rule UID	Rule UID	rule_uid
Sample ID	Sample ID	sample_id
Scan Result	Scan Result	scan result
Scanned File name	Scanned File name	file name
Sel. Mode	Selection Mode	selection_mode
Server Bytes In	Server Inbound Bytes	server_inbound_bytes
Server Bytes Out	Server Outbound Bytes	server_outbound_bytes
Server DiffServ In	Server Inbound DiffServ	server_inbound_diffserv
Server DiffServ Out	Server Outbound DiffServ	server_outbound_diffserv
Server In rule match	Server In rule match	fg-1_server_in_rule_name
Server Interface In	Server Inbound Interface	server_inbound_interface
Server Interface Out	Server Outbound Interface	server_outbound_interface
Server Out rule match	Server Out rule match	fg-1_server_out_rule_name
Server Packets In	Server Inbound Packets	server_inbound_packets
Server Packets Out	Server Outbound Packets	server_outbound_packets
Session ID	Session ID	Session_Id
Session ID	Session ID	snid
SGSN Signal	SGSN for Signal	sgsn_signal
SGSN Traffic	SGSN for Traffic	sgsn_traffic
Signature Version	Signature Version	sig_ver
SLA Violation	SLA Violation	sla_violation
SmartDefense Profile	SmartDefense Profile	SmartDefense profile
Src GW	Source Gateway	src_gw
Src.	Source	Src
Src. IP-phone	Source IP-phone	src phone number
Src. Port	Source Port	SPort_Svc
SrcKeyId	Source Key ID	srckeyid
Srv.	Service	svc
SSO Type	SSO Type	sso_type_desc
Start Time	Start Time	start_time
Status	Status	Audit Status
Status	Status	status
Sub Service	Sub Service	fg-1_sub_service

Subject	Subject	Subject
Subproduct	Subproduct	fw_subproduct
Subscription Expiration	Subscription Expiration	subs_exp
TEID Sig Down	TEID Sig Down	teid_dnlink
TEID Sig Up	TEID Sig Up	teid_uplink
Ticket ID	Ticket ID	ticket_id
Time	Time	hour
Tunnel ID	Tunnel ID	tid
Type	Type	type
UA Auth result	UA Auth result	auth_result
UA Session Id	UA Session Id	ua_snid
Uid	Uid	Uid
Update Src	Update Source	update_src
Update Status	Update Status	Update Status
URL	URL	url
URL List Version	URL List Version	uf_sig_ver
User	User	User
User Dir.	User Directory	user_directory
User Group	Mobile Access User Group	group
User Group	User Group	user_group
User Location	Mobile User Location	user_location
User's IP	User's IP	uname4domain
Version	Version	version
Virtual Link	Virtual Link	vl
Virus Name	Virus Name	virus name
VPN Feature	VPN Feature	vpn_feature_name
VPN Peer Gateway	VPN Peer Gateway	peer gateway
Wire Byte/Sec in	Wire Byte/Sec in	wire_byte_ps_in
Wire Byte/Sec Out	Wire Byte/Sec Out	wire_byte_ps_out
Wire Packet/Sec in	Wire Packet/Sec in	wire_pack_ps_in
Wire Packet/Sec Out	Wire Packet/Sec Out	wire_pack_ps_out
XlateDPort	XlateDPort	XlateDPort_Svc
XlateDst	XlateDst	XlateDst
XlateSPort	XlateSPort	XlateSPort_Svc
XlateSrc	XlateSrc	XlateSrc

(9) Starting CPLogToSyslog

Show / Hide this section

After you configure and save the policy file, start the `CPLogToSyslog`.

- To start the CPLogToSyslog automatically with all Check Point services:

  1. Connect to the command line on the Security Management Server / Multi-Domain Security Management Server.
  2. Log in to the Expert mode.
  3. On Multi-Domain Security Management Server, switch to the context of the relevant Domain Management Server:

     ```
     [Expert@HostName:0]# mdsenv <Name or IP address of Domain Management Server>
     ```

  4. Backup the current Check Point Registry:

     ```
     [Expert@HostName:0]# cp -v $CPDIR/registry/HKLM_registry.data{,_ORIGINAL}
     ```

  5. Register the CPLogToSyslog service:

     ```
     [Expert@HostName:0]# $CPDIR/bin/cpprod_util CPPROD_SetValue FW1 "CPLogToSysLog" 4 1 1
     ```

6. Verify:

```
[Expert@HostName:0]# grep CPLogToSysLog $CPDIR/registry/HKLM_registry.data
```

To disable this configuration:

1. UnRegister the CPLogToSyslog service:

```
[Expert@HostName:0]# $CPDIR/bin/cpprod_util CPPROD_SetValue FW1 "CPLogToSysLog" 4 0 1
```

2. Verify:

```
[Expert@HostName:0]# grep CPLogToSysLog $CPDIR/registry/HKLM_registry.data
```

- To start the CPLogToSyslog on demand:

1. Connect to the command line on the Security Management Server / Multi-Domain Security Management Server.
2. Log in to the Expert mode.
3. On Multi-Domain Security Management Server, switch to the context of the relevant Domain Management Server:

```
[Expert@HostName:0]# mdsenv <Name or IP address of Domain Management Server>
```

4. Manually start the CPLogToSyslog:

```
[Expert@HostName:0]# $FWDIR/bin/CPLogToSyslog &
```

5. Verify:

```
[Expert@HostName:0]# ps auxw | egrep "PID|CPLogToSyslog"
```

Note: The "**cpwd_admin list**" command shows the CPLogToSyslog process as "**CPLOGTOSYSLOG**".

(10) CPLogToSyslog process

Show / Hide this section

The following table contains the summary information about the CPLogToSyslog process.

Section	Information
Description	Exports Check Point logs from Security Management Server / Multi-Domain Security Management Server / Log Server based on the configured CPLogToSyslog policy to external Syslog Servers over Syslog protocol.
Path	*$FWDIR/bin/CPLogToSyslog*
Log file	*$FWDIR/log/cplogtosyslog.elg*
Policy file	*$FWDIR/state/SEAM/local.cplogtosyslog_policy.C*
Marker file	*$FWDIR/conf/CPLogToSyslog_lea_marker.C*
Notes	• "*cpwd_admin list*" command shows the process as "*CPLOGTOSYSLOG*" • If there is an issue with the policy file, it is automatically renamed to: *$FWDIR/state/SEAM/local.cplogtosyslog_policy.err*
To Stop	• With Check Point WatchDog: *$CPDIR/bin/cpwd_admin stop -name CPLOGTOSYSLOG >& /dev/null* • Otherwise, run: *$FWDIR/bin/fw kill CPLogToSyslog >& /dev/null*
To Start	• With Check Point WatchDog: *$CPDIR/bin/cpwd_admin start -name CPLOGTOSYSLOG -path $FWDIR/bin/CPLogToSyslog -command "CPLogToSyslog -udp" >& /dev/null* In addition, refer to sk109016 - CPLogToSyslog processes stop running after a few minutes. • Otherwise, run: *$FWDIR/bin/CPLogToSyslog &*
Debug	1. Switch to the context of the relevant Domain Management Server: *mdsenv <Domain_Name>* 2. Start debug:

fw debug CPLogToSyslog on TDERROR_ALL_ALL=5
fw debug CPLogToSyslog on OPSEC_DEBUG_LEVEL=3
3. Replicate the issue
4. Stop debug:
fw debug CPLogToSyslog off TDERROR_ALL_ALL=0
fw debug CPLogToSyslog off OPSEC_DEBUG_LEVEL=0
5. Analyze:
*$FWDIR/log/cplogtosyslog.elg**

(11) Troubleshooting

Show / Hide this section

(12) Related solutions

Show / Hide this section

(13) Revision history

Show / Hide the revision history

Applies To:

- 01998369 , 02398968 , 02388223
- 02504095
- 01240778 , 02448702 , 02445934 , 01681879 , 01612096 , 01804858 , 01644802 , 02484524 , 01693401 , 02301019 , 02427976 , 01295796 , 02663030
- 02156711 , 02158982 , 02301042 , 02174560

Give us Feedback Please rate this document [1=Worst,5=Best]

Comment Enter your comment here