



Integration with LogPoint

Implementation Guide



This guide describes how to configure CyberArk Enterprise Password Vault (EPV) and Privileged Threat Analytics (PTA) to send syslog messages to LogPoint SIEM solution, and how to configure Logpoint to be able to receive and process these messages.

The guide is based on CyberArk EPV Version 9.95, CyberArk PTA Version 3.6 and Logpoint Version 6 and above

CyberArk EPV - Logpoint Integration

CyberArk EPV can send audit logs to LogPoint through the Syslog protocol and create a complete audit picture of privileged account activities in the LogPoint solution.

These audit logs include user and Safe activities in the Vault, which are transferred by the Vault to Logpoint.

The Vault uses any of the following protocols to send messages:

- ◆ Encrypted protocols
 - TLS
- ◆ Non-encrypted protocols
 - TCP
 - UDP
 - ◆ CyberArk's flexible configuration enables you to define multiple Syslog servers, specify dynamic format translators, and to filter the events that will be sent.
 - ◆ The Vault Syslog messages can be sent to multiple syslog servers in two different ways:
 - A single message can be sent to multiple servers by configuring a single XSLT file.
 - Multiple messages can be sent to different Syslog servers and formatted differently for each server by configuring multiple XSLT files, formats and code-message lists. The code-message lists must be matched, meaning they must contain the same number of items in the same order.



Forward of Syslog is controlled by the following parameters in DBParm.ini:

Parameter Name	Define or Select
SyslogServerIP	The IP address(es) or hostname(s) of the Syslog servers where messages will be sent. Separate multiple values with commas. Note: When using encrypted syslog, make sure that the IP address or hostname is identical to one of the following: • The CN specified in the certificate OR • The subject alternative name field in the certificate. If you specify the hostname, in the %WINDOWS%\System32\Drivers\Etc\hosts file, define the IP address and hostname of the syslog server to resolve the DNS name.
SyslogServerProtocol	Specifies the Syslog protocol(s) that will be used to send audit logs. Separate multiple values with commas. Valid values: TCP/UDP/TLS Default value: UDP Make sure that the order of the specified protocols corresponds to the order of the specified IP addresses or hostnames and ports..
SyslogServerPort	The port(s) used to connect to the Syslog server. Separate multiple values with commas. Default value: 514 Make sure that the order of the specified ports corresponds to the order of the specified IP addresses or hostnames and protocols.
SyslogMessageCodeFilter	Defines which message codes will be sent from the Vault to the SIEM application through Syslog protocol. You can specify message numbers and/or ranges of numbers, separated by commas. For example, to specify messages 1,2,3,30 and 5-10, specify the following value: 1,2,3,5-10,30. Specify multiple values with pipelines. By default, all message codes are sent for user and Safe activities. For a list of messages and codes, refer to the Privileged Account Security Reference Guide..
SyslogTranslatorFile	Specifies the XSL file used to parse CyberArk audit records data into Syslog protocol. Specify multiple values with commas.
UseLegacySyslogFormat	Controls the format of the syslog message, and defines whether it will be sent in a newer syslog format (RFC 5424) or in a legacy format. Default value: No. This enables the Vault to work with the



	newer syslog format.
--	----------------------

For more detailed instructions about Syslog integration, see **Integrating with SIEM Applications** in the *Privileged Account Security Implementation Guide*.

Configure CyberArk Vault to forward events to Logpoint:

1. From the installation package, copy Logpoint.xml to the Syslog subdirectory of the Vault installation folder. By default, the subdirectory is:
C:\Program Files (x86)\PrivateArk\Server\Syslog.
2. In the same server installation folder, by default **C:\Program Files (x86)\PrivateArk\Server**, open dbparm.ini and add the following lines:

```
[SYSLOG]
SyslogServerIP=<ip of Logpoint server>
SyslogServerProtocol=TCP
SyslogServerPort=514
SyslogMessageCodeFilter=0-999
SyslogTranslatorFile=Syslog\Logpoint.xml
UseLegacySyslogFormat=no
```

3. Save the file and close it.
4. Restart the Vault start the PrivateArk Server Service

Configure CyberArk Vault to forward events to multiple Syslog servers:

To forward Vault syslogs to multiple machines ,or instance both your Logpoint solution as well as to CyberArk PTA, you can specify multiple values for the following parameters and separate each value with a comma

```
[SYSLOG]
SyslogServerIP=<ip of Logpoint server>,<ip of PTA server>
SyslogServerProtocol=TCP,TCP
SyslogServerPort=514,514
SyslogMessageCodeFilter=0-999|295,308,7,428,361,372,373,359,436,412,411,300,302
SysLogTranslatorFile=Syslog\Logpoint.xml,Syslog\PTA.xml
UseLegacySyslogFormat=No,No
```

Configure Logpoint to receive CyberArk Vault events:

1. Install Logpoint Knowledge Base CyberArk packages by importing the CyberArk application.
2. Create a new repo for CyberArk EPV logs and assign this to a routing policy.
3. Create a new Normalization policy for CyberArk EPV and assign the CyberArk_EPV Compiled Normalizer package to it.



4. Create a processing policy and assign the Normalization Policy and the Routing Policy created above.

5. Create a new Log Collection policy for CyberArk EPV, and attach a Syslog collector to it, with a Syslog Parser, utf_8 as charset and the Routing Policy create above.
6. Create a new device for the CyberArk Vault and assign it to the CyberArk EPV Log Collection policy created.

CREATE DEVICE

DEVICE INFORMATION

Name:

CyberArk Vault

IP address(es):

10.10.10.20

Device Groups:

Log Collection Policy:

CyberArk_EPV

Distributed Collector:

Time Zone:

UTC TimeZone

RISK VALUES

Confidentiality:

Minimal

Integrity:

Minimal

Availability:

Minimal

Save

Cancel

CyberArk EPV - Logpoint Integration

PTA can send detected incidents as syslog messages to a SIEM solution.

This section describes how to configure integration of PTA with Logpoint SIEM solution.

When PTA detects an event, it sends a syslog record to Logpoint SIEM solution in real time using CEF/LEEF format.

The Syslog integration is controlled by `syslog_outbound` with the following parameters in `systemparm.properties`:

Parameter Name	Define or Select
host	Host name/IP address of the Logpoint SIEM Solution.
port	The port number through which the syslog records will be sent to Logpoint SIEM solution.
format	The format used to transfer the syslog records to the SIEM



	solution. Valid values: CEF
protocol	The protocol used to transfer the syslog records to Logpoint SIEM solution. Currently, PTA supports only udp
siem	Name of SIEM system -

Configure CyberArk PTA to send incidents to Logpoint:

1. Log on to PTA as root
2. Open `/opt/tomcat/diamond-resources/local/systemparm.properties` add the following line

```
syslog_outbound=[{"host": "<ip of Logpoint server>", "port": 514, "format": "CEF", "protocol": "UDP", "siem":"Logpoint"}]
```

3. Save the configuration file and close it.
4. Restart PTA

Configure Logpoint to receive CyberArk Vault events:

1. Install Logpoint Knowledge Base CyberArk packages by importing the CyberArk application.
2. Create a new repo for CyberArk PTA logs and assign this to a routing policy.
3. Create a new Normalization policy for CyberArk PTA and assign the CyberArkCEF Compiled Normalizer package to it.

CREATE NORMALIZATION POLICY

NORMALIZATION POLICY INFORMATION

Policy Name: CyberArk_PTA

Compiled Normalizer:

Available	Selected
CyberArkEPMCompiledNormalizer	CyberArkCEFCCompiledNormalizer
CyberArkEPVCompiledNormalizer	

Normalization Packages:

Available	Selected

View Signatures Submit Cancel

4. Create a processing policy and assign the Normalization Policy and the Routing Policy created above.

PROCESSING POLICY

PROCESSING POLICY

Policy Name: CyberArk_PTA

Normalization Policy: CyberArk_PTA

Enrichment Policy: None

Routing Policy: CyberArk_PTA

Submit Cancel

5. Create a new Log Collection policy for CyberArk PTA, and attach a Syslog collector to it, with a Syslog Parser, utf_8 as charset and the Routing Policy create above.
6. Create a new device for the CyberArk PTA and assign it to the CyberArk PTA Log Collection policy created.