



# Integration with Logpoint

## Implementation Guide



## About Logpoint

Logpoint SIEM solution extracts events and incidents from the billions of logs existing in any IT infrastructure of any size. You can quickly assess the status of your systems and applications through the solution's uniquely designed correlation and analysis layer.

The built-in log analysis engine automatically detects and notifies you of all critical incidents on your systems. The events monitored can be very diverse and can include: an ongoing attack, a compromised system, a system breakdown, user authentication issues and much more.

### **The raw log data from your systems can be used to:**

- Automate regulatory processes
- Improve efficiency in forensics investigations
- Increase troubleshooting turnaround time
- Improve your security position
- Gain visibility into the organization

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 receive and process these messages.

The guide is based on CyberArk EPV Version 9.95, CyberArk PTA Version 3.6 and Logpoint Version 6.7.3

## 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 the Vault transfers 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 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.

**Some of the benefits of the integration include:**

- Multi-layer correlation between log data and alerts from PTA, allows clients to perform in-depth analysis.
- Behavioral analysis identifying suspicious privileged user activity.
- Scores to the particular threat – so that customers can decide which incident poses the biggest threat.
- PTA alerts are to be included in dashboards and reporting.

- PTA alerts to be included in the general alerting and incident handling

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

| Parameter Name              | Define or Select                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SyslogServerIP</b>       | <p>The IP address(es) or hostname(s) of the Syslog servers where messages will be sent. Separate multiple values with commas.</p> <p><b>Note:</b> When using encrypted syslog, make sure that the IP address or hostname is identical to one of the following:</p> <ul style="list-style-type: none"> <li>• The CN specified in the certificate</li> </ul> <p>OR</p> <ul style="list-style-type: none"> <li>• The subject alternative name field in the certificate.</li> </ul> <p>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.</p> |
| <b>SyslogServerProtocol</b> | <p>Specifies the Syslog protocol(s) that will be used to send audit logs. Separate multiple values with commas.</p> <p>Valid values: TCP/UDP/TLS</p> <p>Default value: UDP</p> <p>Make sure that the order of the specified protocols corresponds to the order of the specified IP addresses or hostnames and ports..</p>                                                                                                                                                                                                                                                                                                                              |
| <b>SyslogServerPort</b>     | <p>The port(s) used to connect to the Syslog server. Separate</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |



|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                | <p>multiple values with commas.</p> <p>Default value: 514</p> <p>Make sure that the order of the specified ports corresponds to the order of the specified IP addresses or hostnames and protocols.</p>                                                                                                                                                                                                                                                                                                  |
| <b>SyslogMessageCodeFilter</b> | <p>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..</p> |
| <b>SyslogTranslatorFile</b>    | <p>Specifies the XSL file used to parse CyberArk audit records data into Syslog protocol. Specify multiple values with commas.</p>                                                                                                                                                                                                                                                                                                                                                                       |
| <b>UseLegacySyslogFormat</b>   | <p>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.</p> <p>Default value: <b>No</b>. This enables the Vault to work with the newer syslog format.</p>                                                                                                                                                                                                                                                           |

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 and start the PrivateArk Server Service

## Configure CyberArk Vault to forward events to multiple Syslog servers:

To forward Vault Syslog to multiple machines or instances 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
```

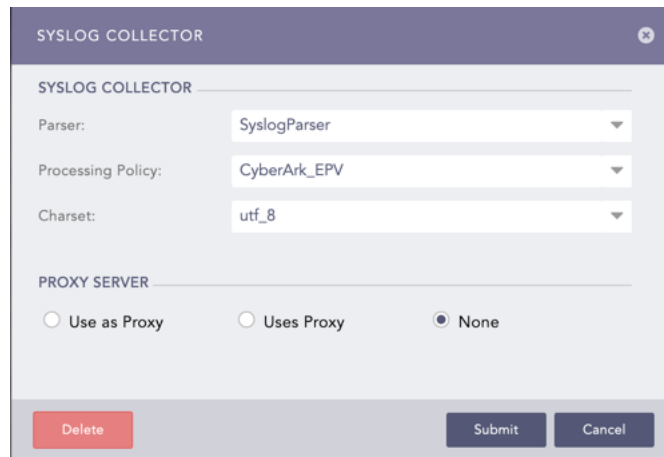


## Configure Logpoint to receive CyberArk Vault events:

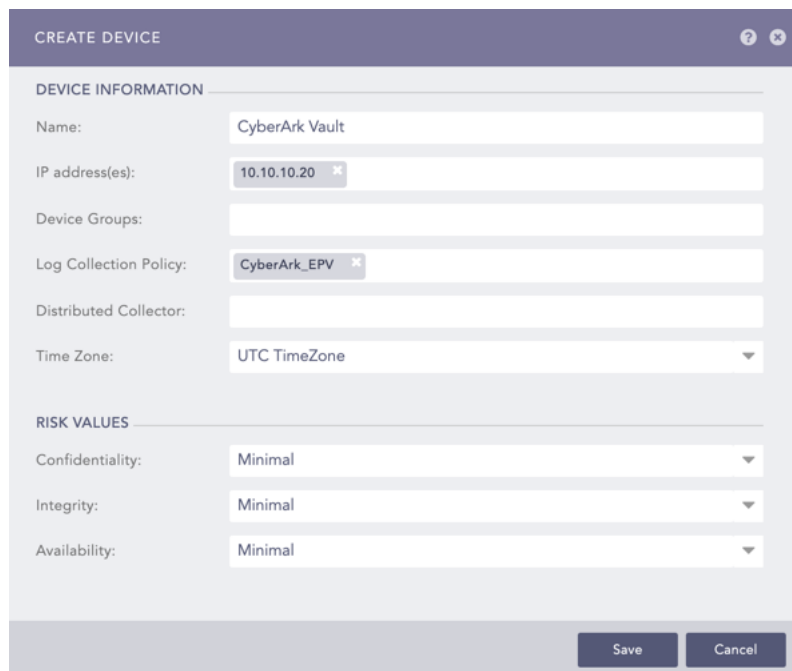
1. Install Logpoint Knowledge Base CyberArk packages by importing the Cyberark application package.
2. Create a new repo for **CyberArk EPV** logs.
3. Create a new Normalization policy for **CyberArk EPV** and assign the **CyberArkePVCompiledNormalizer** package to it.

The screenshot shows a 'CREATE NORMALIZATION POLICY' window. The 'NORMALIZATION POLICY INFORMATION' section has a text field containing 'CyberArk\_EPV'. Below this, the 'Compiled Normalizer' section features two lists: 'Available' (containing 'CyberArkCEFCCompiledNormalizer' and 'CyberArkEPMCompiledNormalizer') and 'Selected' (containing 'CyberArkePVCompiledNormalizer'). Between these lists are navigation arrows. The 'Normalization Packages' section also has two lists: 'Available' (empty) and 'Selected' (containing 'LP\_Cyberark'). At the bottom are buttons for 'View Signatures', 'Submit', and 'Cancel'.

4. Create a new **Log Collection** policy for CyberArk EPV and a **Syslog collector** to it, with a **Syslog Parser,utf\_8** as **charset** and the **Repo** and **Normalization Policy** created above.



5. Create a new device for the CyberArk Vault and assign it to the CyberArk EPV Log Collection policy created.



## CyberArk EPV - Logpoint Integration

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

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

When PTA detects an event, it sends a syslog record to the 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                                                                                                    |
|-----------------|---------------------------------------------------------------------------------------------------------------------|
| <b>host</b>     | Host name/IP address of the Logpoint SIEM Solution.                                                                 |
| <b>port</b>     | The port number through which the syslog records will be sent to Logpoint SIEM solution.                            |
| <b>format</b>   | The format used to transfer the Syslog records to the SIEM solution.<br><br>Valid values: CEF -or- LEEF             |
| <b>protocol</b> | The protocol used to transfer the syslog records to Logpoint SIEM solution.<br><br>Currently, PTA supports only udp |
| <b>siem</b>     | 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` and 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

