

CyberArk PAM

Configure the Vault to Forward syslog Messages to PTA

The system logger of the Vault must be configured to send logging data to the PTA machine for real-time data analysis.

	When PTA is configured with Vaults deployed in a distributed environment, configure the primary and satellite Vaults.
--	---

To Configure syslog on the Vault Machine (until Vault v10.4):

	1.	From the installation package, copy PTA.xsl 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]

SyslogTranslatorFile=Syslog\PTA.xsl

SyslogServerPort=<port number>

SyslogServerIP=<server IP>

SyslogServerProtocol=UDP

SyslogMessageCodeFilter=4,17,22,24,31,38,57,60,88,130,142,145,148,149,170,183,185,295,300,301,302,303,306,307,308,344,346,359,360,361,362,372,373,374,375,376,377,378,379,380,381,411,412,414,416,418,426,434,463

UseLegacySyslogFormat=No

Specify the following information:

Parameter Name	Define or Select
SyslogServerIP	The IP address(es) of the PTA machine where messages will be sent.

Parameter Name	Define or Select
SyslogServerPort	The port number through which the syslog will be sent. Specify 514 to send syslogs to the default PTA port.
SyslogServerProtocol	<div>The protocol used to transfer the syslog records. Specify: tcp or udp.<div><div></div><div>PTA does not support the SSL protocol.</div></div></div>

Parameter Name	Define or Select																																																																						
SyslogMessageCodeFilter	<p>Defines which message codes will be sent from the Vault Machine to PTA through Syslog protocol.</p> <p>You can specify message numbers, separated by commas. You can also specify range of numbers using '-'. Message codes are sent for the following events:</p> <table><tr><th>Code</th><th>Activity</th></tr><tr><td>4</td><td>User Authentication</td></tr><tr><td>17</td><td>Add Safe (Unauthorized)</td></tr><tr><td>22</td><td>CPM Verify Password</td></tr><tr><td>24</td><td>CPM Change Password</td></tr><tr><td>31</td><td>CPM Reconcile Password</td></tr><tr><td>38</td><td>CPM Verify Password Failure</td></tr><tr><td>57</td><td>CPM Change Password Failure</td></tr><tr><td>60</td><td>CPM Reconcile Password Failure</td></tr><tr><td>88</td><td>Set Password</td></tr><tr><td>130</td><td>CPM Disable Password</td></tr><tr><td>142, 145, 148, 149, 170</td><td>Delete Safe Failure</td></tr><tr><td>183</td><td>Delete Safe</td></tr><tr><td>185</td><td>Add Safe</td></tr><tr><td>295</td><td>Retrieve Password</td></tr><tr><td>300</td><td>PSM Connect</td></tr><tr><td>301</td><td>PSM Connect Failure</td></tr><tr><td>302</td><td>PSM Disconnect</td></tr><tr><td>303</td><td>PSM Disconnect Failure</td></tr><tr><td>306, 307, 308</td><td>Use Password</td></tr><tr><td>344</td><td>Privileged Command Initiated</td></tr><tr><td>346</td><td>Privileged Command Completed</td></tr><tr><td>359</td><td>PSM SQL Command</td></tr><tr><td>360</td><td>PSM SQL Command Failure</td></tr><tr><td>361</td><td>PSM Keystrokes</td></tr><tr><td>362</td><td>PSM Keystrokes Failure</td></tr><tr><td>372</td><td>Terminate session</td></tr><tr><td>373</td><td>Terminate session Failure</td></tr><tr><td>374</td><td>Start Monitor session</td></tr><tr><td>375</td><td>Start Monitor session Failure</td></tr><tr><td>376</td><td>End Monitor session</td></tr><tr><td>377</td><td>End Monitor session Failure</td></tr><tr><td>378</td><td>PSM Secure Connect Session Start</td></tr><tr><td>379</td><td>PSM secure Connect session start Failure</td></tr><tr><td>380</td><td>PSM Secure Connect Session End</td></tr></table>	Code	Activity	4	User Authentication	17	Add Safe (Unauthorized)	22	CPM Verify Password	24	CPM Change Password	31	CPM Reconcile Password	38	CPM Verify Password Failure	57	CPM Change Password Failure	60	CPM Reconcile Password Failure	88	Set Password	130	CPM Disable Password	142, 145, 148, 149, 170	Delete Safe Failure	183	Delete Safe	185	Add Safe	295	Retrieve Password	300	PSM Connect	301	PSM Connect Failure	302	PSM Disconnect	303	PSM Disconnect Failure	306, 307, 308	Use Password	344	Privileged Command Initiated	346	Privileged Command Completed	359	PSM SQL Command	360	PSM SQL Command Failure	361	PSM Keystrokes	362	PSM Keystrokes Failure	372	Terminate session	373	Terminate session Failure	374	Start Monitor session	375	Start Monitor session Failure	376	End Monitor session	377	End Monitor session Failure	378	PSM Secure Connect Session Start	379	PSM secure Connect session start Failure	380	PSM Secure Connect Session End
Code	Activity																																																																						
4	User Authentication																																																																						
17	Add Safe (Unauthorized)																																																																						
22	CPM Verify Password																																																																						
24	CPM Change Password																																																																						
31	CPM Reconcile Password																																																																						
38	CPM Verify Password Failure																																																																						
57	CPM Change Password Failure																																																																						
60	CPM Reconcile Password Failure																																																																						
88	Set Password																																																																						
130	CPM Disable Password																																																																						
142, 145, 148, 149, 170	Delete Safe Failure																																																																						
183	Delete Safe																																																																						
185	Add Safe																																																																						
295	Retrieve Password																																																																						
300	PSM Connect																																																																						
301	PSM Connect Failure																																																																						
302	PSM Disconnect																																																																						
303	PSM Disconnect Failure																																																																						
306, 307, 308	Use Password																																																																						
344	Privileged Command Initiated																																																																						
346	Privileged Command Completed																																																																						
359	PSM SQL Command																																																																						
360	PSM SQL Command Failure																																																																						
361	PSM Keystrokes																																																																						
362	PSM Keystrokes Failure																																																																						
372	Terminate session																																																																						
373	Terminate session Failure																																																																						
374	Start Monitor session																																																																						
375	Start Monitor session Failure																																																																						
376	End Monitor session																																																																						
377	End Monitor session Failure																																																																						
378	PSM Secure Connect Session Start																																																																						
379	PSM secure Connect session start Failure																																																																						
380	PSM Secure Connect Session End																																																																						

Parameter Name	Define or Select
SyslogTranslatorFile	Specifies the XSL file used to parse Vault records data into Syslog protocol.
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. Required value: No. This enables the Vault to work with the newer syslog format.

	3.	To forward Vault syslogs to multiple machines (for instance to your SIEM solution as well as to PTA), you can specify multiple values for the following parameters and separate each value with a comma.
--	----	--

	■	This requires a CyberArk Vault version 7.2.5 or higher.
--	---	---

	■	All destinations must use the same port and protocol, which are specified in the SyslogServerPort and SyslogServerProtocol fields.
--	---	--

	■	The specified values will apply to all destinations configured in SyslogServerIP, using the translator files specified in SysLogTranslatorFile.
--	---	---

Parameter Name	Comments
SyslogServerIP	
SyslogTranslatorFile	
UseLegacySyslogFormat	
SyslogMessageCodeFilter	Separate multiple values with a comma, and separate sets of multiple values with a pipe-line, as shown in the example below.

The following example shows how to send different syslog messages to multiple syslog servers.

[SYSLOG]

SysLogTranslatorFile=Syslog\Arcsight.sample.xml,Syslog\QRadar.xml,Syslog\PTA.xml

SyslogServerPort=<port number>

SyslogServerIP=1.1.1.1,1.1.2.2,1.1.3.3

SyslogServerProtocol=UDP

UseLegacySyslogFormat=Yes,Yes,No

SyslogMessageCodeFilter=7,8,295|295-

296|295,308,7,24,31,428,361,372,373,359,436,412,411,300,302,294,427

	4.	Save the file and close it.
	5.	Restart the Vault.

For more detailed instructions about integrating SIEM applications, see [Security Information and Event Management Applications](#).

To Configure syslog on the Vault Machine (from Vault v10.5):

	1.	The PTA syslog parameters are available in the dbparm.sample.ini file. Copy the parameters to the dbparm.ini configuration file.
--	----	--

[SYSLOG]

SyslogTranslatorFile=Syslog\PTA.xml

SyslogServerPort=<port number>

SyslogServerIP=<server IP>

SyslogServerProtocol=UDP

SyslogMessageCodeFilter=295,308,7,24,31,428,361,372,373,359,436,412,411,300,302,294,427,471

UseLegacySyslogFormat=No

	2.	To forward Vault syslogs to multiple machines (for instance to your SIEM solution as well as to PTA), you can specify multiple values for the following parameters and separate each value with a comma.
--	----	--

	■	All destinations must use the same port and protocol, which are specified in the SyslogServerPort and SyslogServerProtocol fields.
--	---	--

	■	The specified values will apply to all destinations configured in SyslogServerIP, using the translator files specified in SysLogTranslatorFile.
--	---	---

Parameter Name	Comments
SyslogServerIP	
SyslogTranslatorFile	
UseLegacySyslogFormat	
SyslogMessageCodeFilter	Separate multiple values with a comma, and separate sets of multiple values with a pipe-line, as shown in the example below.

The following example shows how to send different syslog messages to multiple syslog servers.

[SYSLOG]

SysLogTranslatorFile=Syslog\Arcsight.sample.xsl,Syslog\QRadar.xsl,Syslog\PTA.xsl

SyslogServerPort=<port number>

SysLogServerIP=1.1.1.1,1.1.2.2,1.1.3.3

SyslogServerProtocol=UDP

UseLegacySyslogFormat=Yes,Yes,No

SyslogMessageCodeFilter=7,8,295|295-

296|295,308,7,24,31,428,361,372,373,359,436,412,411,300,302,294,427,471

	3.	To send secured syslog data to PTA, see Configure Vault Trusted Connection to PTA .
--	----	---

	4.	Save the file and close it.
--	----	-----------------------------

	5.	Restart the Vault.
--	----	--------------------

For more detailed instructions about integrating SIEM applications, see [Security Information and Event Management Applications](#).

Source: <https://docs.cyberark.com/pam-self-hosted/11.3/en/content/pta/configuring-vault-forward-syslog-messages.htm>

CyberArk PAM Integration Procedures

Please provide the following information to CyTech:

Requirements:Collect logs via syslog over UDP or TCP

- *Syslog Host-> Syslog Collector IP address where the Elastic-Agent is installed.
- *Syslog Port-> Port Number (Please identify if TCP or UDP)

If you need further assistance, kindly contact our support at support@cytechint.com for prompt assistance and guidance.