



Syslog Settings

Product: Antikor v2 - Next Generation Firewall
Guides

Syslog Settings

The server is the partition where the server/servers to register the system logs are added. It supports 40 different log types and 7 different log formats. It can be transmitted to the log collector or SIEM in the preferred raw or structural log formats.

Syslog Settings										Reload	Add
XLS CSV PDF			Show/Hide		Records Per Page		OK	Filter	Reset Filter		
#	Status	Description	Log Types	Filter Text	Output Format	Server Address	Protocol	Port	Actions		
1	Active	Antispam	Antispam Logs		CEF (Common Event Format)	10.2.4.55	UDP	514	Edit Delete		
2	Active	All Logs	Antispam Logs Banned IPs to Access Web UI Honeypot Logs Cluster Logs DHCP Event Logs DNS Filter Logs DoS / Flood Protection Logs Firewall - Antispoof Logs Firewall - DMZ Traffic Logs Firewall - Dynamic NAT Traffic Logs Firewall - Global NAT Traffic Logs Firewall - Security Rules Traffic Logs Firewall - NAT by Destination Traffic Logs Firewall - Hotspot Default Block Logs Firewall - Port Forwarding Traffic Logs Firewall - Static NAT Traffic Logs Firewall - Traffic Normalization Firewall - Default Rule Logs Hotspot Logs Http(s) Redirection Logs IPsec Flow Logs Blackhole Logs PPP Debug Logs PPP Logs RADIUS Logs SSH Denetimli Logları SSH Guard Service Logs SSH & Console Session Logs Intrusion Prevention System (IPS) Logs Application Security Logs VPN - IPsec VPN Logs VPN - PPTP / L2TP Logs VPN - SSL VPN Logs Web Interface Logs Web Access Logs Web Filter - URL Filter Logs Web Filter - Content and Antivirus Scan Logs Web Session Logs Web Application Security Logs Management Panel Access Traffic Logs		Raw Log	10.2.4.50	UDP	514	Edit Delete		
<div>« < 1 > »</div>										<div>Go</div>	

To choose log type, server IP, log port, priority, and application name to monitor logs click on Add button.

Syslog Settings - New Record

Status	<input checked="" type="checkbox"/> Active
Description	<input type="text"/>
Log Types	<div>Select...</div>
Filter Text	<input type="text"/>
Output Format	<div>Raw Log</div>
Address Family	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Server Address	<div>IPv4</div> <input type="text"/>
Protocol	<div>UDP</div>
Port	<input type="text" value="514"/>

Cancel

Save

Status

Active ☐

Description

Log Types

Select...

Filter Text

Output Format

Application Security Logs

Address Family

Banned IPs to Access Web UI

Server Address

Blackhole Logs

Protocol

UDP

Port

514

Cancel Save

Status

Active ☐

Description

Log Types

Select...

Filter Text

Output Format

Raw Log

Address Family

CEF (Common Event Format)

Server Address

EWMM (Enterprise Wide Message Model)

Protocol

GELF (Graylog Extended Log Format)

Port

JSON (Javascript Object Notation)

Port

WELF (WebTrends Enhanced Log File Format)

Port

CIM (Common Information Model)

Cancel Save

FIELD	DESCRIPTION
Status	Select status of the record. (Active or Passive)
Description	Description of Syslog Setting is written.
Log Types	The log type is selected and the selected log type is sent to the Syslog server.
Output Formats	There are 7 different output formats on the Antikor that can be output related to syslog. One of these log formats is selected.
Address Family	Select IPv4 or IPv6.
Server Address	Enter IP addresses of server where logs are stored.
Protocol	This is the field where the protocol used to send logs is selected.
Port	Enter port number to be used by the log.

Output Formats

FIELD	DESCRIPTION
Raw Log	It is the format in which the incoming data is sent raw without being processed.
CEF (Common Event Format)	The common event format (CEF) ArcSight is a log and control file format. It is an extensible, text-based format that is designed to solve multiple device types by providing the most needed information.
EWMM (Enterprise Wide Message Model)	It is a set of published enterprise-wide standards that allow organizations to send semantically precise messages across computer systems.
GELF (Graylog Extended Log Format)	The Graylog extended Log format (GELF) is a unique log format created to address all the shortcomings of the classic flat syslog. This enterprise feature lets you collect structured events from anywhere and then compress.
JSON (Javascript Object Notation)	JSON (JavaScript object representation) is a lightweight data interchange format. It's easy for people to read and write. Machines are easy to parse and produce.
WELF (WebTrends Enhanced Log File Format)	The WELF Reference defines the Webtrends industry standard log file interchange format.
CIM (Common Information Model)	The common information Model (CIM) is an open standard that defines how managed elements in an IT environment are represented as a common set of objects and relationships between them.



