epati

Syslog Settings

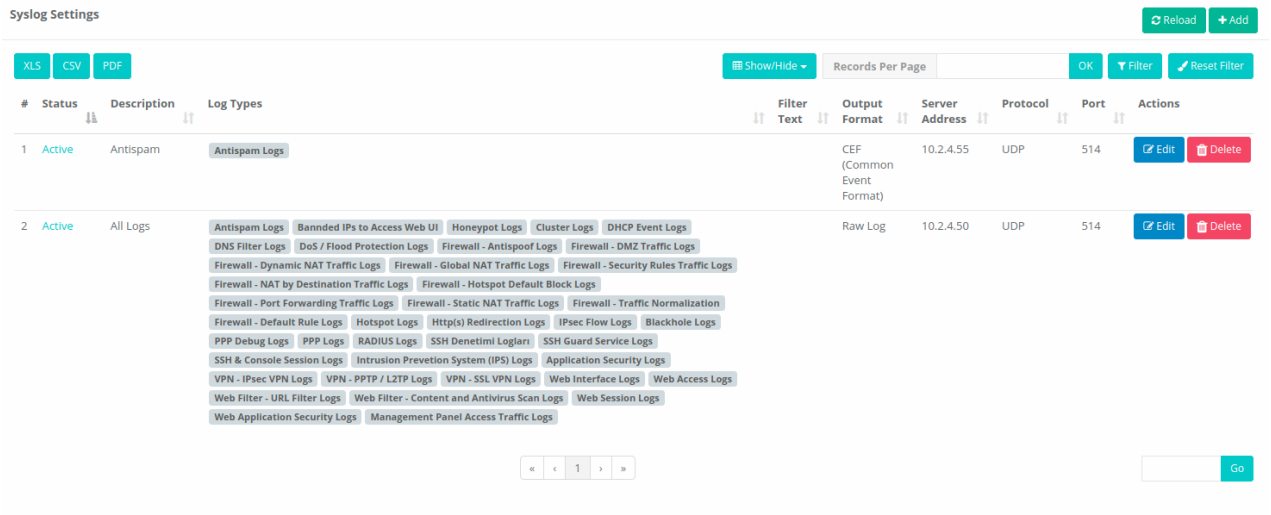
Product: Antikor v2 - Next Generation Firewall

Guides

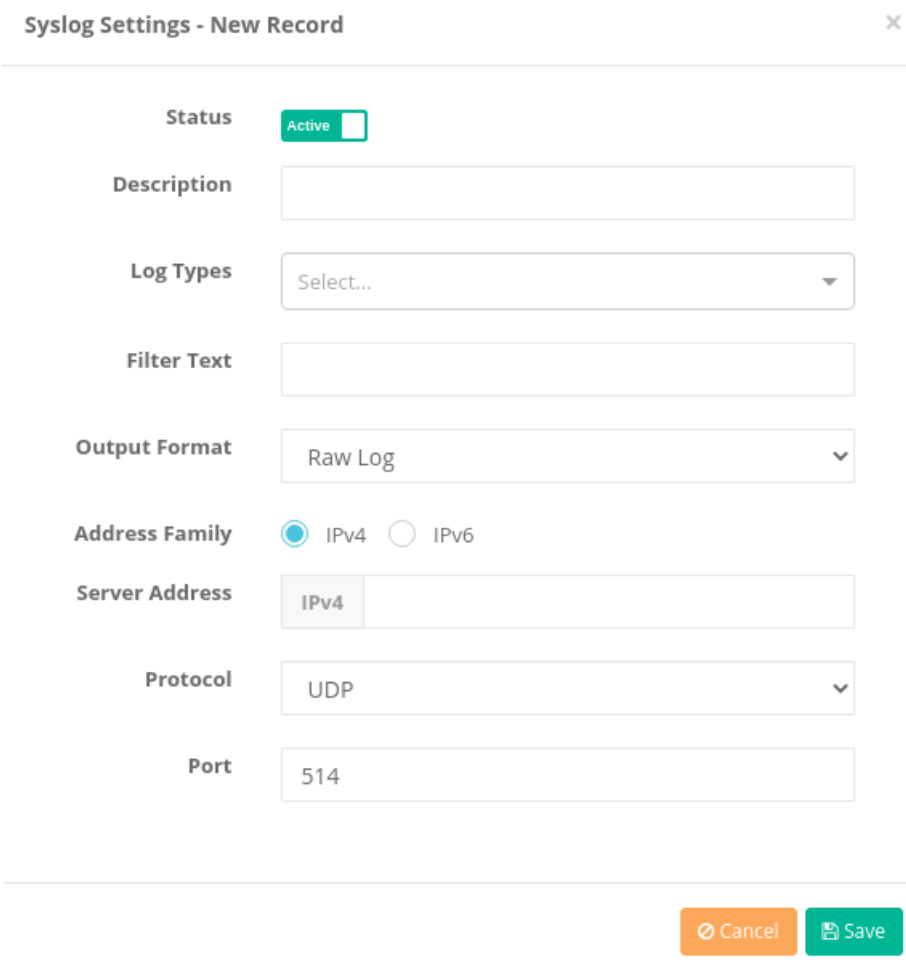
www.epati.com.tr

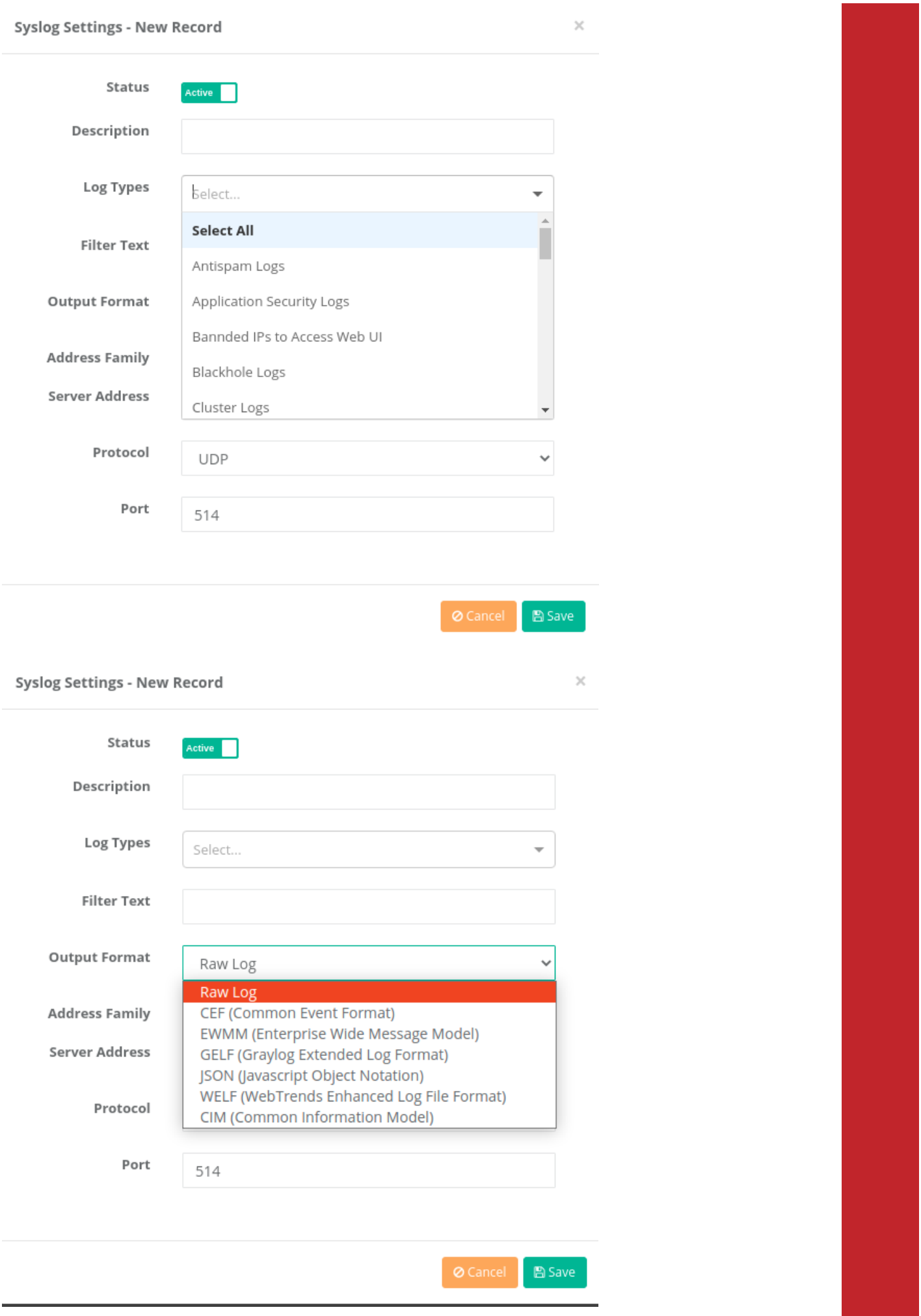
Syslog Settings

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.



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




Syslog Settings - New Record
Status
Active
Description
Log Types
Select...
Filter Text
Output Format
Address Family
Server Address
Protocol
Port
Select All
Antispam Logs
Application Security Logs
Bannded IPs to Access Web UI
Blackhole Logs
Cluster Logs
UDP
514
Cancel
Save
Syslog Settings - New Record
Status
Active
Description
Log Types
Select...
Filter Text
Output Format
Raw Log
Address Family
Server Address
Protocol
Port
Raw Log
CEF (Common Event Format)
EWMM (Enterprise Wide Message Model)
GELF (Graylog Extended Log Format)
JSON (Javascript Object Notation)
WELF (WebTrends Enhanced Log File Format)
CIM (Common Information Model)
514
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.