epati

SysLog Ayarları

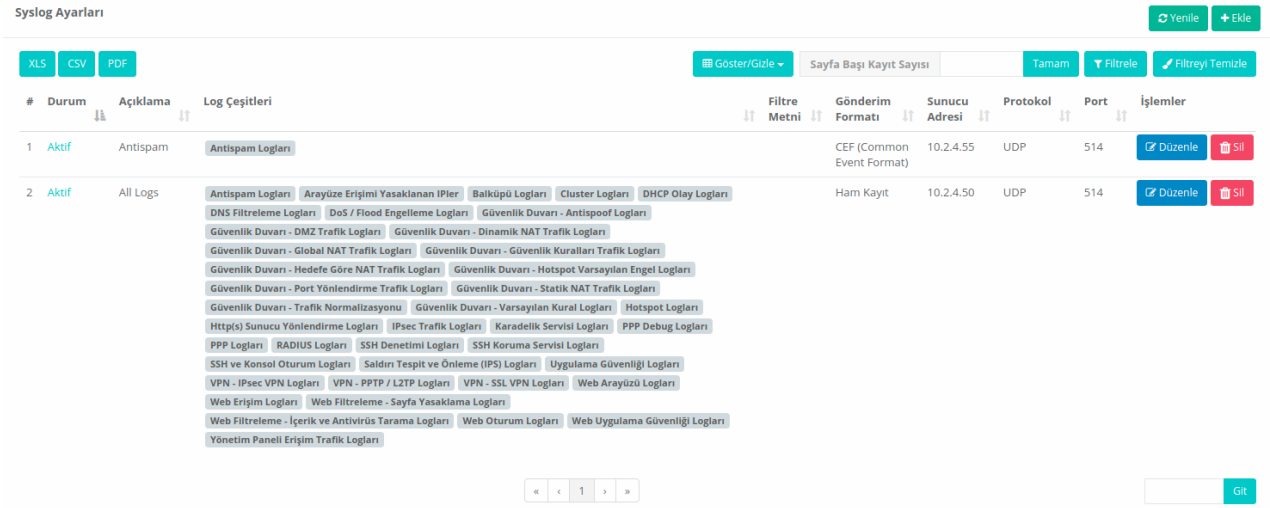
Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı

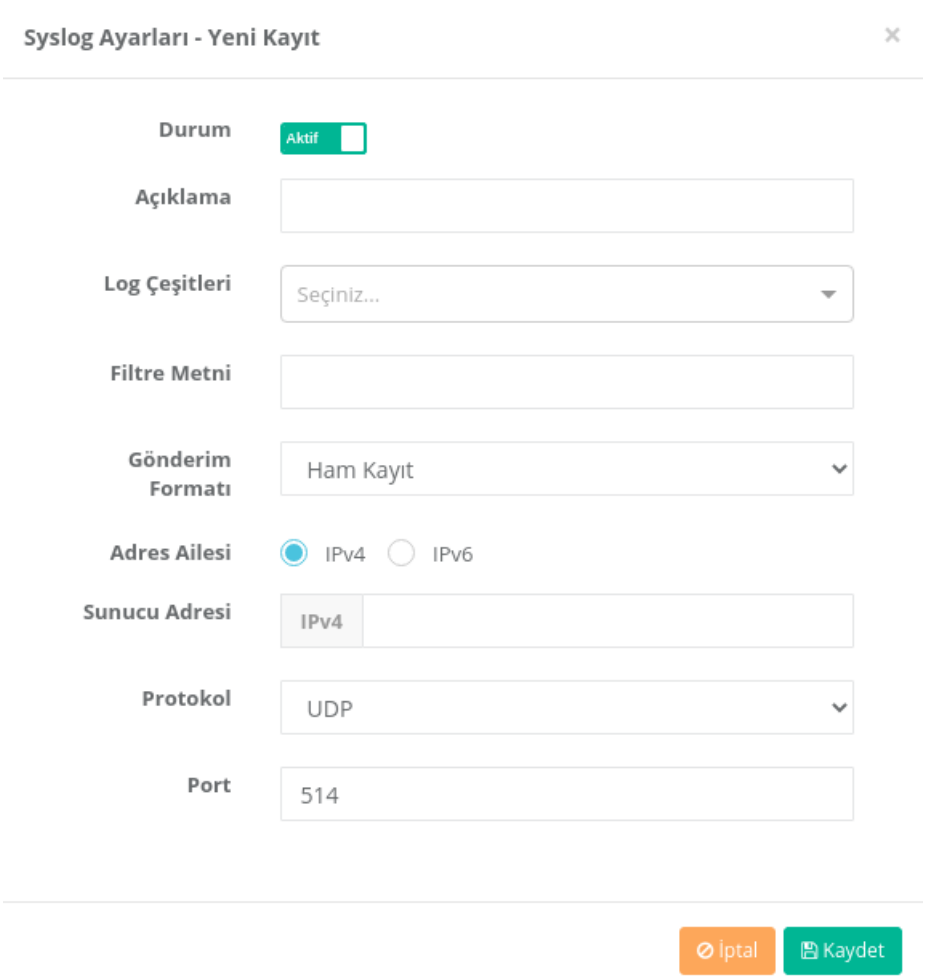
Kılavuzlar

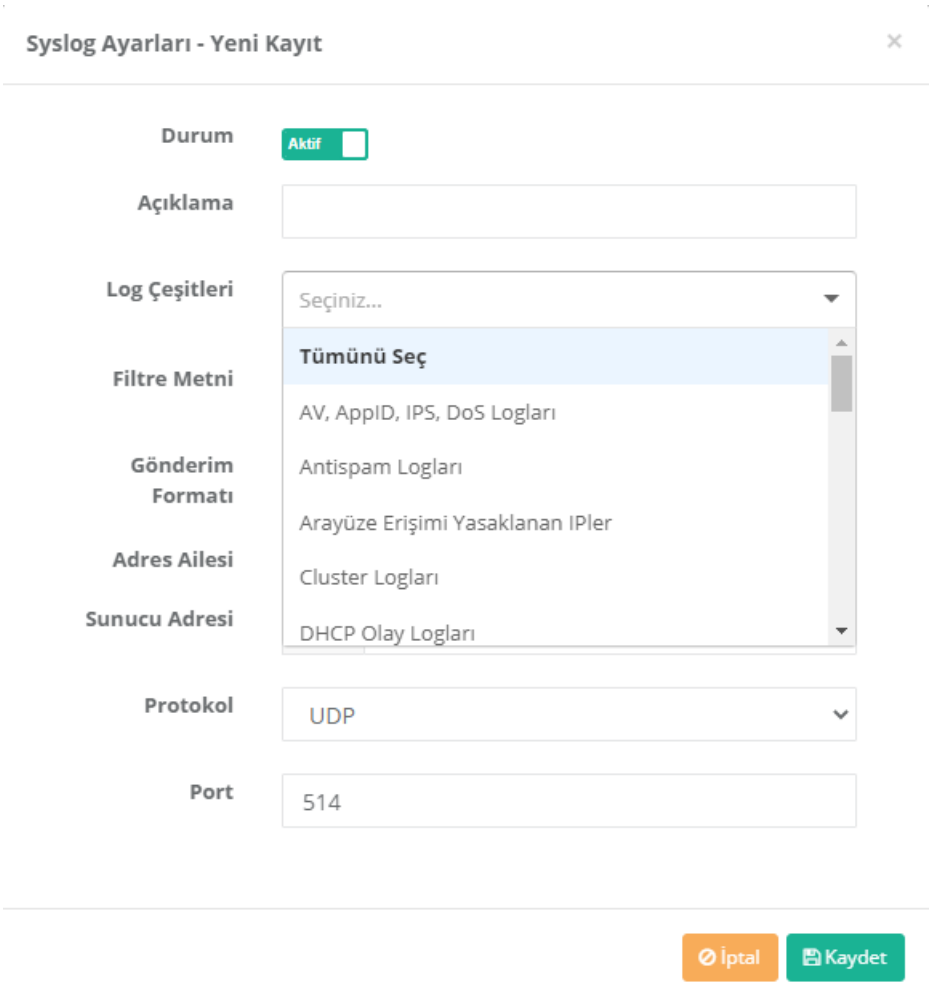
www.epati.com.tr

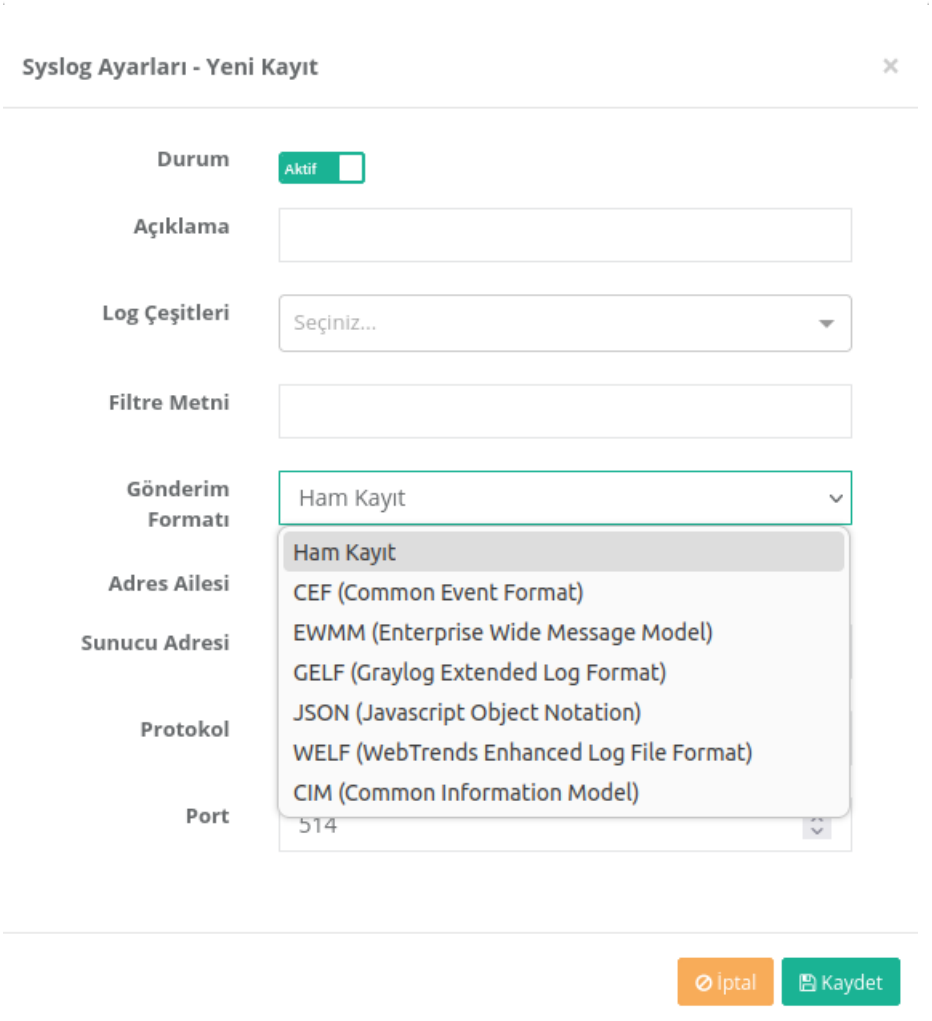
SysLog Ayarları

Sunucu sistem loglarının kayıt edileceği sunucunun/sunucuların eklendiği bölümdür. 26 farklı log çeşidi ve 7 farklı log formatını desteklemektedir. Tercih edilen ham veya yapısal log formatlarında kullanıcının sağlayacağı log toplayıcısına veya SIEM'e iletilebilmektedir.






Syslog Ayarları - Yeni Kayıt
Durum
Aktif
Açıklama
Log Çeşitleri
Seçiniz...
Filtre Metni
Gönderim Formatı
Adres Ailesi
Sunucu Adresi
Protokol
Port
Tümünü Seç
AV, AppID, IPS, DoS Logları
Antispam Logları
Arayüze Erişimi Yasaklanan IPler
Cluster Logları
DHCP Olay Logları
UDP
514
İptal
Kaydet


Syslog Ayarları - Yeni Kayıt
Durum
Aktif
Açıklama
Log Çeşitleri
Seçiniz...
Filtre Metni
Gönderim Formatı
Ham Kayıt
Adres Ailesi
Sunucu Adresi
Protokol
Port
Ham Kayıt
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
İptal
Kaydet

ALAN	AÇIKLAMA
Açıklama	Syslog ayarının açıklaması yazılır.
Log Çeşitleri	Log çeşitleri seçilir ve seçilen log çeşitleri Syslog sunucuya gönderilir.
Filtre Metni	Gönderilecek loglara uygulanacak filtrelerin yazıldığı alandır.
Gönderim Formatı	Desteklenen 7 farklı log formatından biri seçilerek log toplayıcısına veya SIEM'e iletilebilmektedir.
Adres Ailesi	IPv4 ya da IPv6 adres ailesi seçilir.
Server Adresi	Logların tutulacağı sunucuya ait IP adresi yazılır.
Protokol	Logların gönderilmesinde kullanılacak protokolün seçildiği alandır.
Port	Log'un hangi port numarasını kullanacağı yazılır.

Gönderim Formatı

ALAN	AÇIKLAMA
Ham Kayıt	Gelen veriler işlenmeden ham olarak gönderildiği formattır.
CEF (Common Event Format)	Ortak olay biçimi (CEF) ArcSight bir günlük ve denetim dosya biçimidir. En gerekli bilgileri sunarak birden fazla cihaz türlerini çözmek için tasarlanmıştır genişletilebilir, metin tabanlı bir formattır.
EWMM (Enterprise Wide Message Model)	Kuruluşların bilgisayar sistemleri arasında semantik olarak kesin mesajlar göndermesine izin veren yayınlanmış kurumsal çapında standartlar kümesidir.
GELF (Graylog Extended Log Format)	Graylog Genişletilmiş Günlük Biçimi (GELF), klasik düz Syslog'un tüm eksikliklerini gidermek için oluşturulmuş benzersiz bir günlük biçimidir. Bu kurumsal özellik, yapılandırılmış olayları her yerden toplamanızı ve ardından bunları göz açıp kapayıncaya kadar sıkıştırmanızı ve parçalamanızı sağlar.
JSON (Javascript Object Notation)	JSON (JavaScript nesne gösterimi) hafif bir veri değişim biçimidir. İnsanların okuması ve yazması kolaydır. Makinelerin ayrıştırılması ve üretilmesi kolaydır.
WELF (WebTrends Enhanced Log File Format)	WELF Başvurusu, WebTrends endüstri standardı günlük dosyası değişim biçimini tanımlar.
CIM (Common Information Model)	Ortak Bilgi Modeli (CIM), bir BT ortamındaki yönetilen öğelerin ortak bir nesne kümesi ve bunlar arasındaki ilişkiler olarak nasıl temsil edildiğini tanımlayan açık bir standarttır.

Teknopark İdari Binası Kat: 4 No: 411
Posta Kodu: 33343 Yenişehir / MERSİN
+90 324 361 02 33
+90 324 361 02 39