epati

Rapor Ayarları

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı

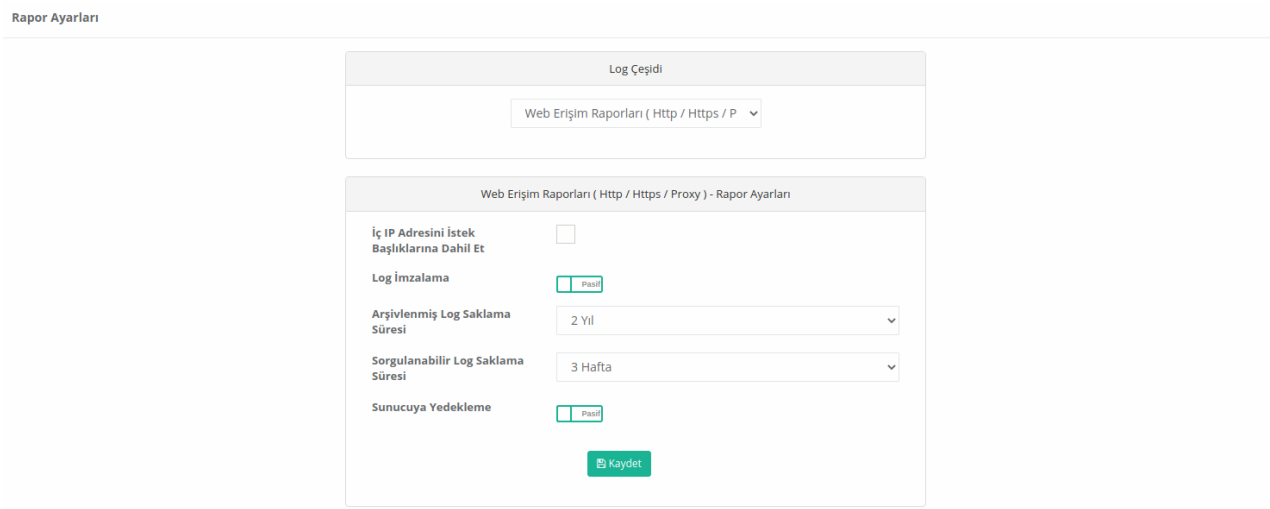
Kılavuzlar

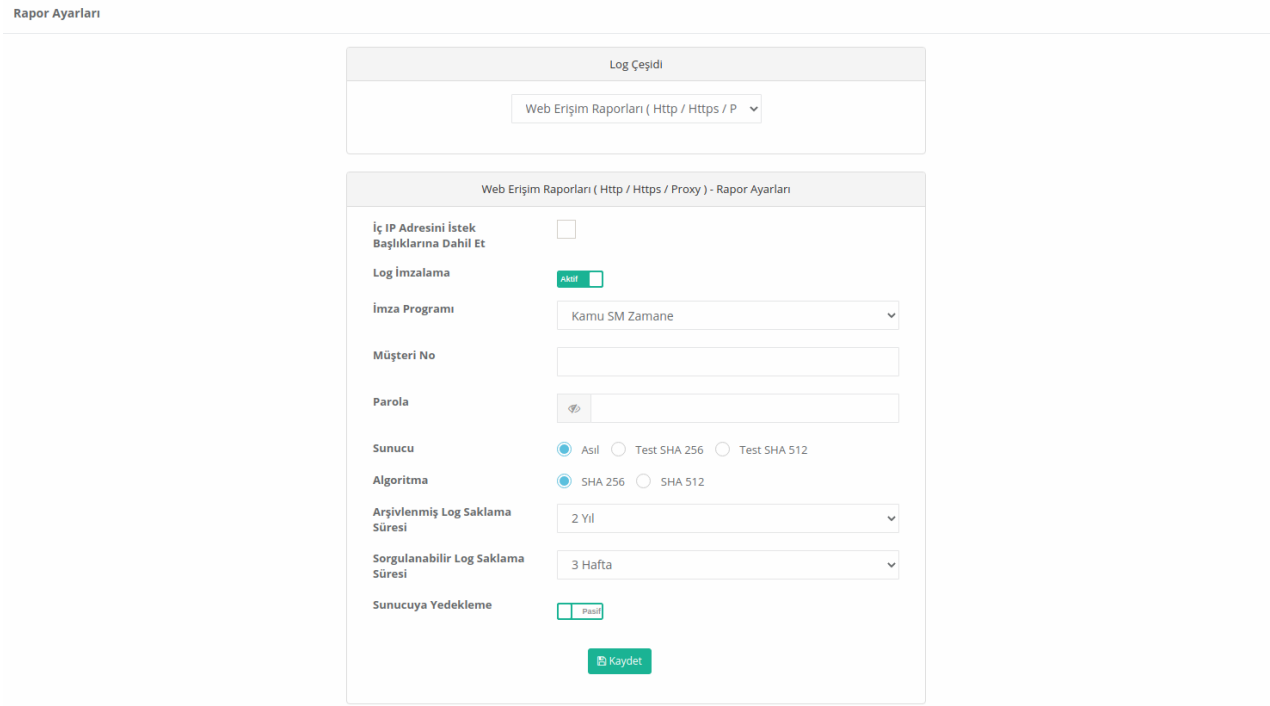
www.epati.com.tr

Rapor Ayarları

Logların imzalanması(Kamu SM Zamane veya Antikor Zaman Damgası) ve farklı bir sunucuya FTP, SAMBA, NFS, SFTP, SCP dosya paylaşım türlerinden herhangi biri ile yedeklenmesi rapor ayarlarında yapılmaktadır.

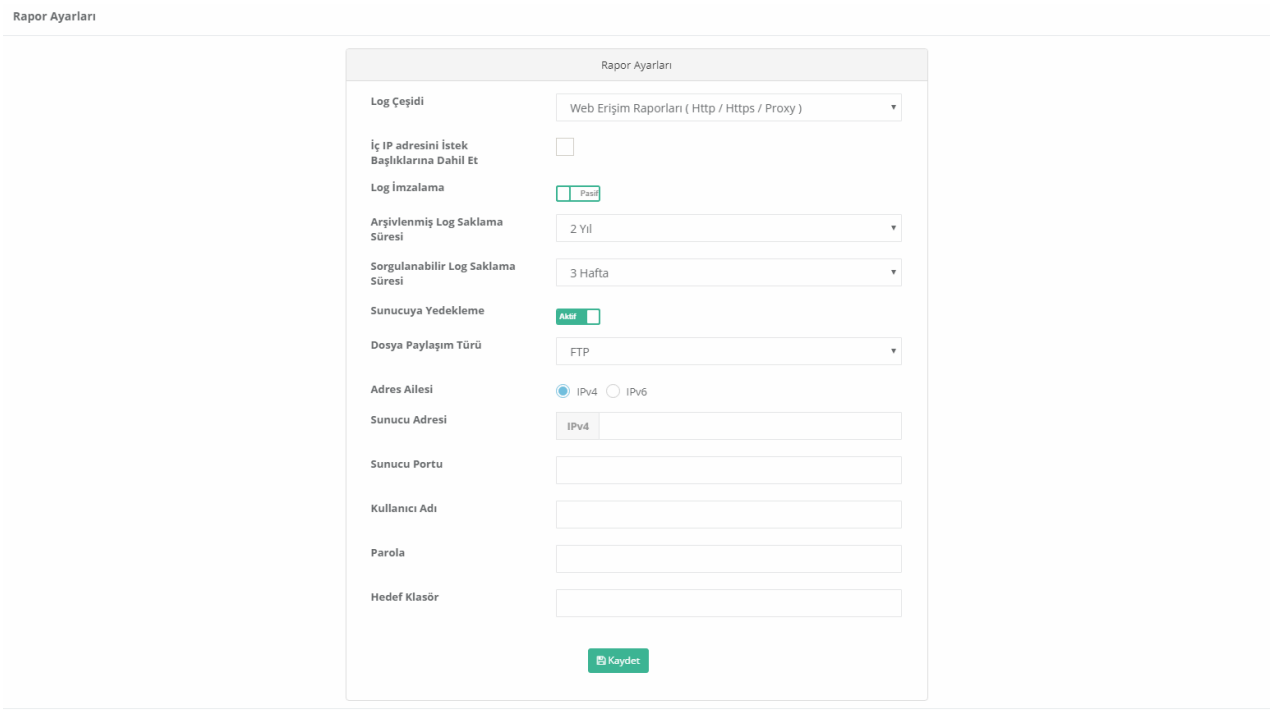
`Not:` Disk boyutuna göre imzalı logların `Arşivlenmiş Log Saklama Süresi` ve `Sorgulanabilir Log Saklama Süresi` seçilmelidir.





Sunucuya yedekleme özelliği aktive edilince aşağıdaki KVKK uyarısı ile karşılaşılmaktadır.

Yukarıdaki uyarıyı okuyup onayladığınız takdirde sunucu bilgilerinizi girip, loglar o sunucuya FTP, SAMBA, NFS, SFTP, SCP ile gönderilebilmektedir.



ALAN	AÇIKLAMA
Log Çeşidi	11 farklı log çeşidi için log tutulabilmektedir.
İç IP adreslerini istek başlıklarına dahil et	Evet / Hayır
Log İmzalama	Aktif / Pasif
Arşivlenmiş Log Saklama Süresi	6 aydan 5 yıla kadar log tutabilmektedir.
Sorgulanabilir Log Saklama Süresi	1 Hafta ile 3 yıla kadar log tutabilmektedir.
Sunucuya Yedekleme	Aktif / Pasif

Log Çeşidi

ALAN	AÇIKLAMA
Web Erişim Raporları(HTTP / HTTPS / Proxy Logları	HTTP / HTTPS / Proxy erişim raporlarının loglarını tutar.
Hotspot Logları	Hotspot kullanıcılarının loglarını tutar.
DHCPV4 Logları	DHCPv4 raporlarının loglarını tutar.
DHCPV6 Logları	DHCPv6 raporlarının loglarını tutar.
Kullanıcı Hareket Logları	Web arayüzü kullanıcılarının loğlarını tutar.
Sistem Logları	Sistem raporlarının loglarını tutar.
Performans Logları	Antikor'un kurulu olduğu sunucuda bulunan RAM, CPU ve Bellek loglarını tutar.
Saldırı Tespit Logları	Tespiti yapılan saldırıların loglarını tutar.
VPN - SSL VPN Logları	IPSec ,L2TP/PPTP, SSL ve Site to Site VPN loglarını tutar.
Güvenlik Duvarı Logları	Güvenlik duvarı loglarını tutar.(Güvenlik Kuralları, DMZ, Global NAT, Port yönlendirme, Statik NAT, Hedefe göre NAT, Dinamik NAT, Antispoof, Yönetim Paneli, Güvenlik duvarı, Varsayılan Kural Logları)
Uygulama Güvenliği ve IPS Logları	Uygulama güvenliği ve IPS loglarını tutar.

Log İmzalama

ALAN	AÇIKLAMA
İmza Programı	Kamu SM Zamane / Antikor Zaman Damgası
Müşteri No	Kamu SM'den alınan Müşteri No girilir
Parola	Kamu SM'den alınan Parola girilir

Not: İmza programı olarak Kamu SM Zamane seçildiğinde Müşteri No ve Parola ile Tübitak Bilgem kamu sertifikasyon merkezi sunucularından zaman damgası(time stamp) çekmektedir. Antikor Zaman Damgası seçildiği takdirde Antikor sunucularından zaman damgası(time stamp) çekmektedir.(Bu işlem için kullanıcı adı ve şifre gerekmemektedir.) Kullanıcılar logları iki yöntemle de imzalayıp sunucuda tutabilirler. İmzalanmış loglar **Raporlar** menüsü altında **Rapor Arşivi** sayfasından görüntülenebilmektedir.

Sunucuya Yedekleme

ALAN	AÇIKLAMA
Dosya Paylaşım Türü	FTP / SAMBA / NFS / SFTP / SCP Tutulacak log dosyasının log tutulacak sunucuya hangi dosya paylaşım yolu ile bağlanılacağını belirler.

Dosya Paylaşım Türü FTP Seçilmiş ise

ALAN	AÇIKLAMA
Adres Ailesi	IPv4 / IPV6
Sunucu Adresi	Tutulacak log dosyasına ait log sunucusunun Adres Ailesinde seçilen IPv4 veya IPV6 adresi girilir.
Sunucu Portu	FTP Log sunucusunun port numarası girilir.
Kullanıcı Adı	Log sunucusunun kullanıcı adı girilir.
Parola	Log sunucusunun kullanıcı adına ait parolası girilir.
Hedef Klasör	Log sunucusunun hedef klasör yolu girilir.

Dosya Paylaşım Türü SAMBA Seçilmiş ise

ALAN	AÇIKLAMA
Adres Ailesi	IPv4 / IPV6
Sunucu Adresi	Tutulacak log dosyasına ait log sunucusunun Adres Ailesinde seçilen IPv4 veya IPV6 adresi girilir.
Kullanıcı Adı	Log sunucusunun kullanıcı adı girilir.
Parola	Log sunucusunun kullanıcı adına ait parolası girilir.
Hedef Klasör	Log sunucusunun hedef klasör yolu girilir.
Etki Alanı	SAMBA etki alanı girilir.

Dosya Paylaşım Türü NFS Seçilmiş ise

ALAN	AÇIKLAMA
Adres Ailesi	IPv4 / IPV6
Sunucu Adresi	Tutulacak log dosyasına ait log sunucusunun Adres Ailesinde seçilen IPv4 veya IPV6 adresi girilir.
Sunucu Portu	FTP Log sunucusunun port numarası girilir.
Hedef Klasör	Log sunucusunun hedef klasör yolu girilir.
Bağlama Yolu	Log sunucusunun bağlama yolu girilir.

Dosya Paylaşım Türü SFTP Seçilmiş ise

ALAN	AÇIKLAMA
Adres Ailesi	IPv4 / IPV6
Sunucu Adresi	Tutulacak log dosyasına ait log sunucusunun Adres Ailesinde seçilen IPv4 veya IPV6 adresi girilir.
Sunucu Portu	FTP Log sunucusunun port numarası girilir.
Kullanıcı Adı	Log sunucusunun kullanıcı adı girilir.
Parola	Log sunucusunun kullanıcı adına ait parolası girilir.
Hedef Klasör	Log sunucusunun hedef klasör yolu girilir.
Public Key	Log sunucusunun SSH Public Key girilir.

Dosya Paylaşım Türü SCP Seçilmiş ise

ALAN	AÇIKLAMA
Adres Ailesi	IPv4 / IPV6
Sunucu Adresi	Tutulacak log dosyasına ait log sunucusunun Adres Ailesinde seçilen IPv4 veya IPV6 adresi girilir.
Sunucu Portu	SCP Log sunucusunun port numarası girilir.
Kullanıcı Adı	Log sunucusunun kullanıcı adı girilir.
Parola	Log sunucusunun kullanıcı adına ait parolası girilir.
Hedef Klasör	Log sunucusunun hedef klasör yolu girilir.
Public Key	Log sunucusunun SSH Public Key girilir.