DLP Nedir?

Data Loss Prevention'un (Veri Kaybı Önleme) kısaltması olan DLP veri güvenliğinizi sağlamak için standartlaştırılmaya çalışılan bir teknolojidir. KoruMail içerisindeki DLP modülü mime-type bazında dosya tipi kontrolü, e-posta içerisinde kredi kartı bilgileri, sosyal güvenlik numara bilgileri gibi verilerin dışarıya aktarılmasını önlemek gibi çok önemli bir görev gerçekleştirmektedir.

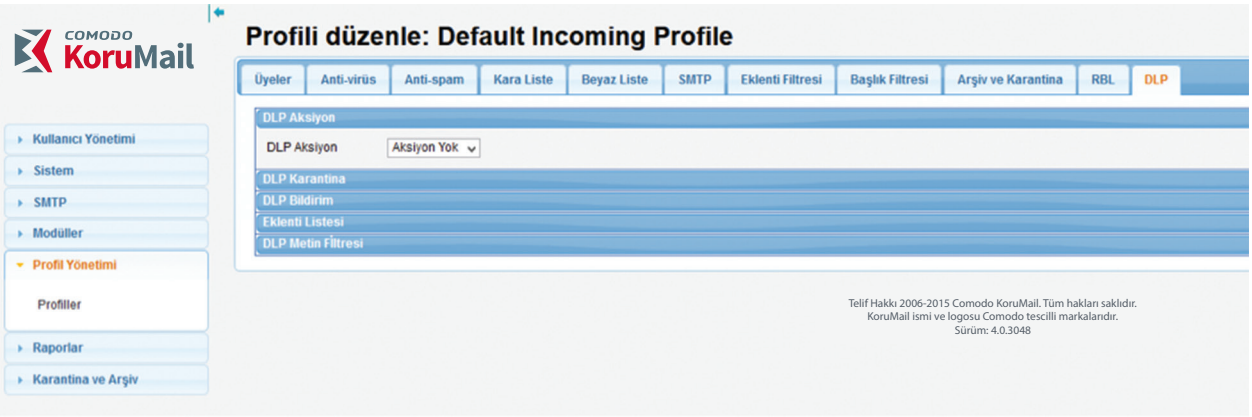
DLP temel olarak, belli politikalar üreterek kurum bilgilerinizin kötü niyetli kişiler tarafından dışarıya sızdırılmasını önlemek olarak açıklanabilir. Günümüzde, bilgi iletişiminde önemli bir yer tutan e-posta iletişimi de dışarı bilgi sızdırmak için kullanılan en yaygın yöntemlerdendir.

Firmanız içerisinden bilgi sızdırmaya çalışan kötü niyetli kişiler bazen siz ekli dosyalarda kontrol gerçekleştirseniz bile uzantıları değiştirerek dışarıya dosya gönderebilmektedir. KoruMail dosyanın mime-type kısmından kontrol gerçekleştirerek uzantısı değişse dahi dosyanın asıl olarak tipini tespit edebilmekte ve KoruMail DLP Profilinizde belirtmiş olduğunuz yasaklı uzantılar arasındaysa gönderimi engellemektedir. Ayrıca sahte e-postalarla kullanıcılardan kredi kartı ve sosyal güvenlik numarası gibi kişiye özel bilgileri elde etmeye çalışan kötü niyetli kişilere karşı önlem olarak e-posta içerisinde kredi kartı ve sosyal güvenlik numarası tespit edilirse bu e-postanın teslimi de engellenmektedir.

DLP Modülü Nasıl Etkinleştirilir?

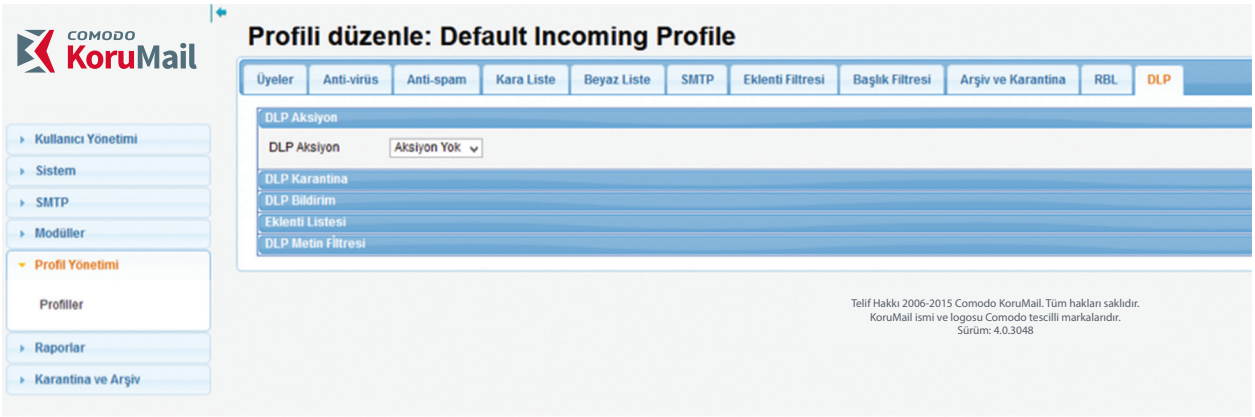
KoruMail üzerinde öncelikle Menü Altında "Modüller" – "DLP" sekmesinde modülü uygulamak istediğiniz Profili seçip kaydetmelisiniz. (Şekil 1)

Şekil 1



Bu işlem sonrası “Profil Yönetimi” – “Profiller” – “Uygulamak istediğiniz Profil” – “DLP” sekmesinde detaylı DLP ayarları gerçekleştirilebilmektedir. (Şekil 2)

Şekil 2



DLP Detaylı Ayarlar

DLP özelliğini kullanmak istediğimiz Profilimizde DLP sekmesinde Aşağıdaki sekmeler bizi karşılamaktadır. (Şekil - 2)

DLP Aksiyon

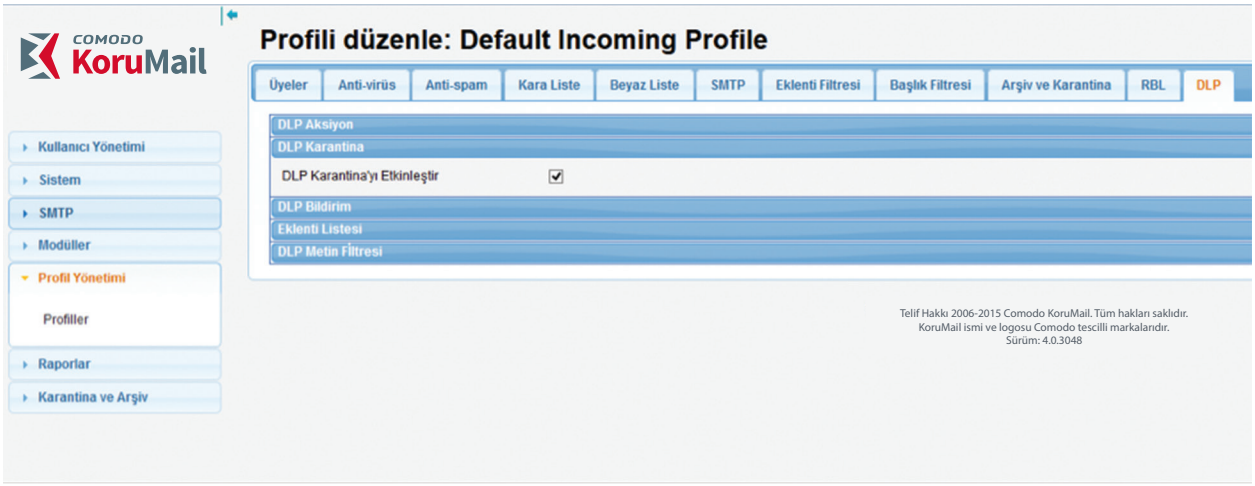
DLP tarafından tespit edilen maillerde uygulanacak işlemlerdir. Bu durumlar aşağıdaki gibidir.

- Reddet
- Yoksay
- Aksiyon yok

Bu seçeneklerden “Reddet” seçili durumda olduğu zaman DLP tarafından tespit edilen mailler reddedilir, “Yoksay” seçili durumda olduğu zaman DLP tarafından tespit edilen mailler karşı tarafa iletilir ve Sistem yöneticisine bilgi verilir. “Aksiyon Yok” seçili durumda olduğu zaman DLP pasif durumdadır.

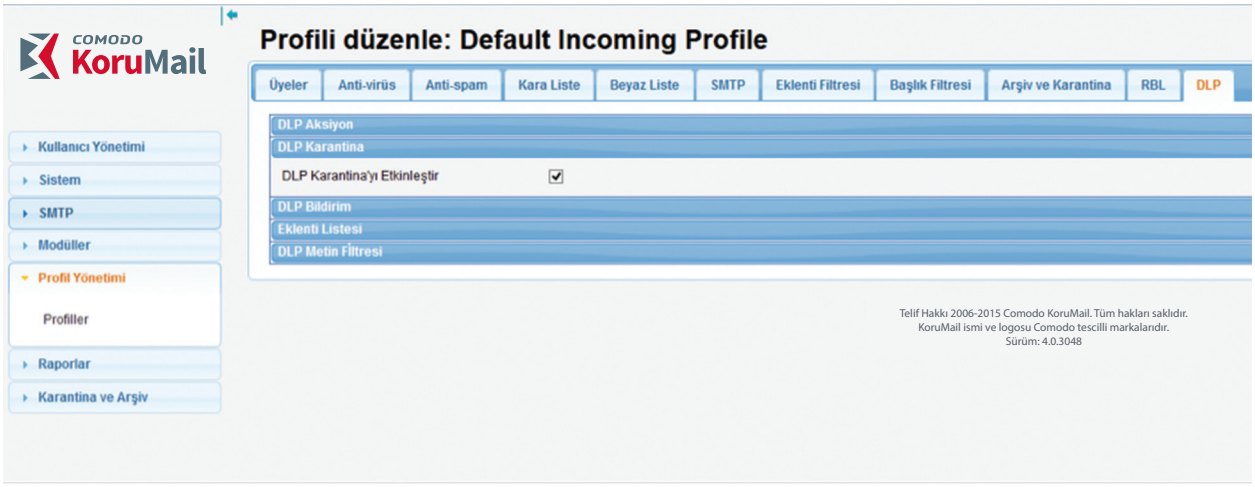
DLP Karantina

Şekil 3



DLP Karantina, Aksiyon durumu “Reddet” olduğu zaman Tespit edilen maillerin KoruMail Karantina bölgesine alınmasını sağlayan özelliktir. (Şekil 3)

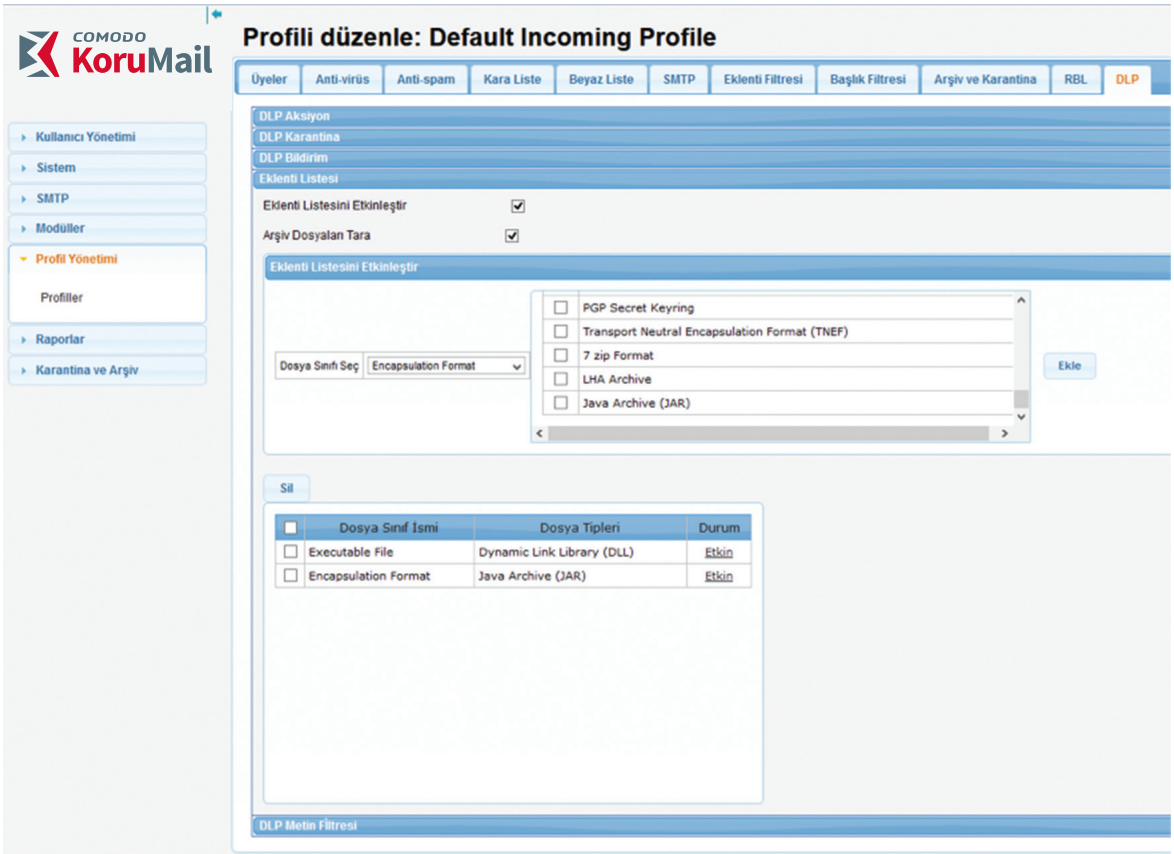
Şekil 4



DLP Aksiyon Durumu “Reddet” ve “Yoksay” olduğu durumlarda DLP tarafından algılanan maillerin Sistem Yöneticisine bilgi verilmesini sağlayan özelliktir. (Şekil 4) DLP aktif Durumda ise mutlaka açık olması tavsiye edilir.

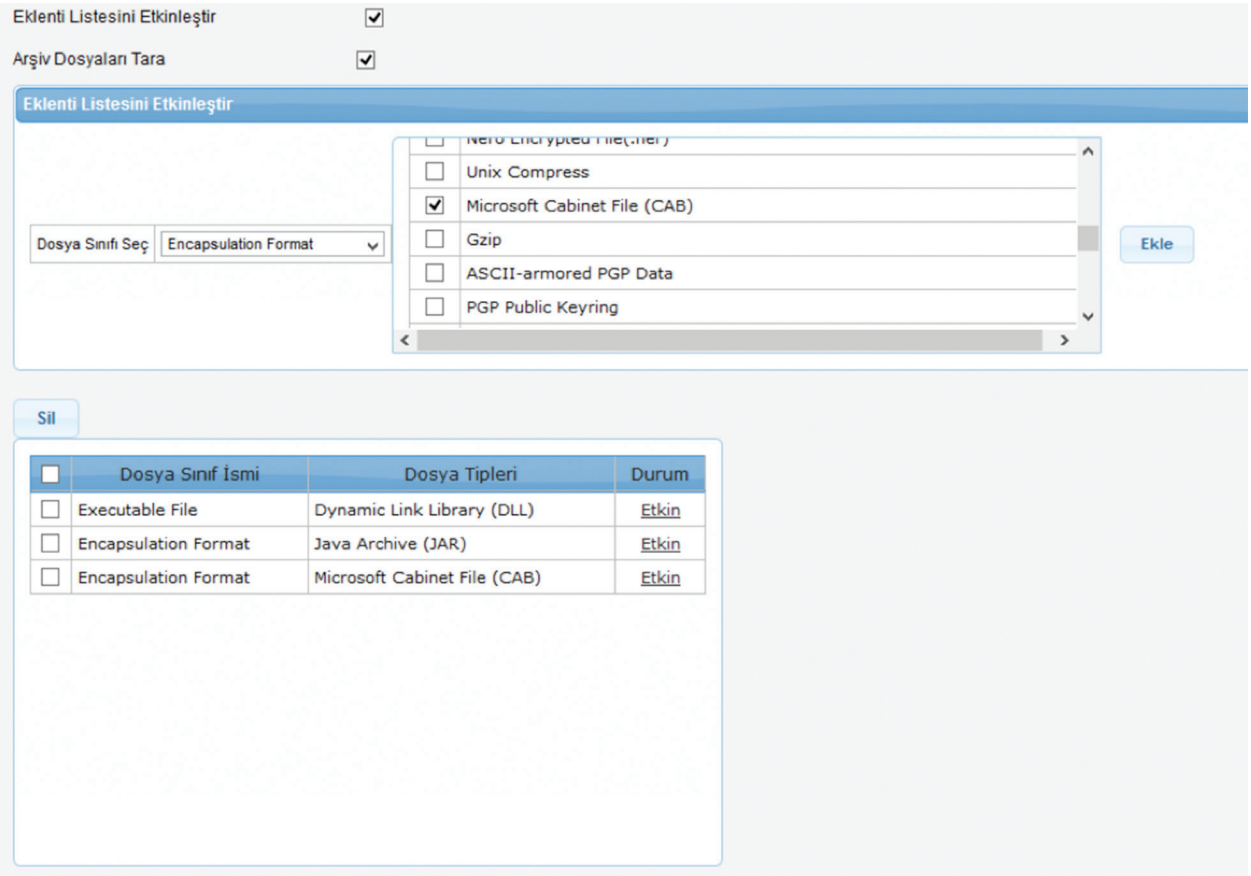
DLP Eklenti Listesi

Şekil 5



Engellemek istediğimiz eklentileri seçmek için öncelikle “Eklenti Listesini Etkinleştir” işaretlenmelidir. Mail içeriğindeki eklenti Arşiv dosyası (zip, rar, tar, jar vb.) ise içeriğinin taranması için “Arşiv Dosyaları Tara” etkin olmalıdır. (Şekil 5)

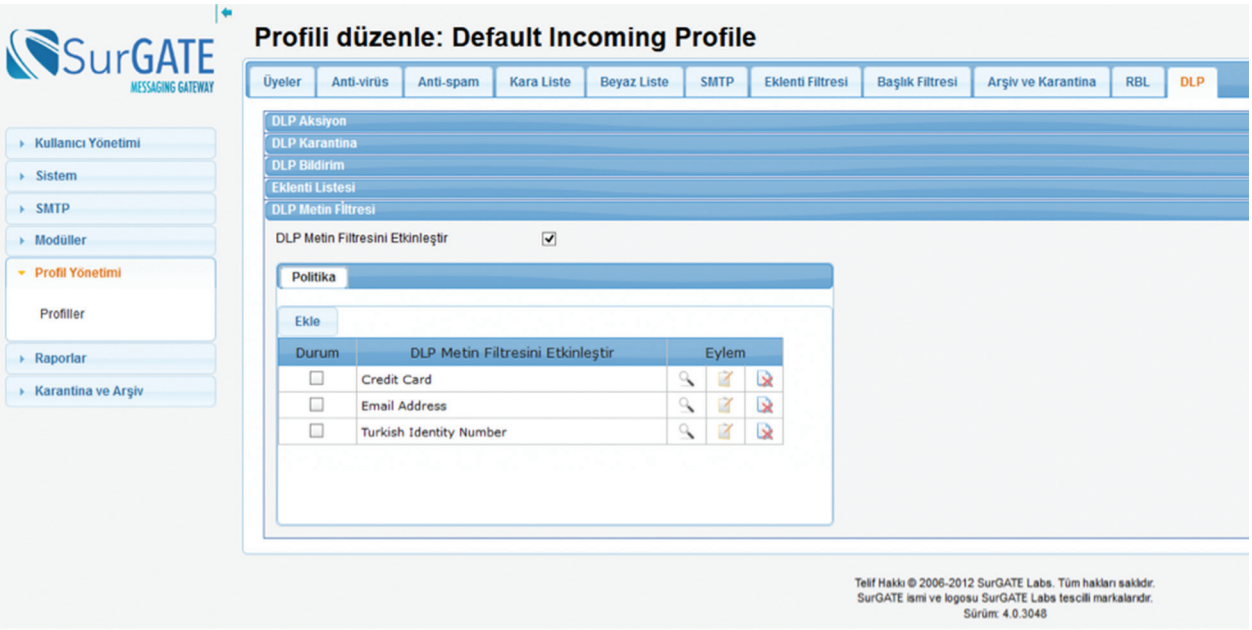
Şekil 6



Eklenti Listesini Etkinleştir sekmesinde “Dosya Sınıfı Seç” bölümünde ilgili dosyanın Sınıfını seçiyoruz ve sağ taraftaki “Dosya Tipleri” menüsü içinde dosya sınıfına ait dosya tipleri listeleniyor. Bu listeden engellemek istediğimiz dosya tipini seçip “Ekle” butonu ile Engellenecek dosya listemize ekliyoruz. (Şekil 6) Eklenti kuralları için mime-type bazında engelleme sağlandığı için, Uzantısı değişse dahi eklenti engellenecektir.

DLP Metin Filtresi

Şekil 7



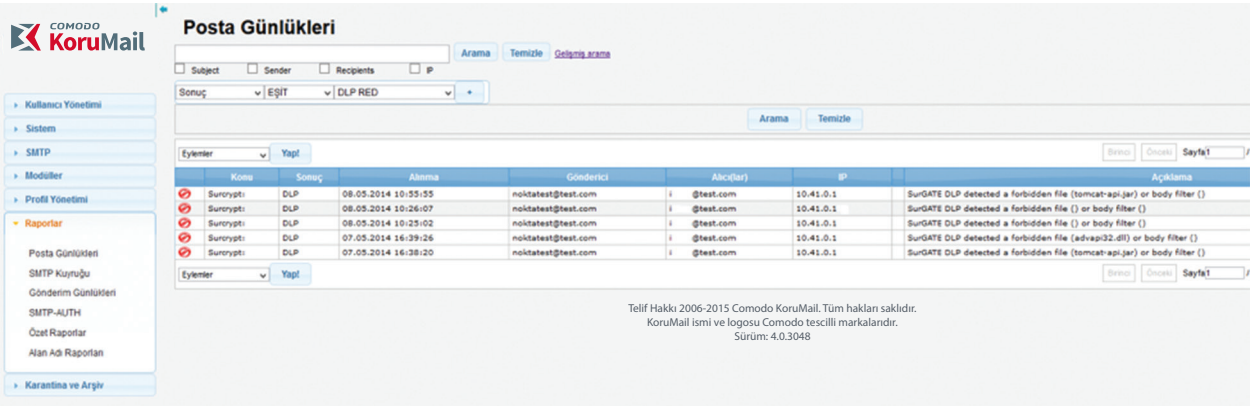
Sahteciliği önlemek için, kredi kartı ve sosyal güvenlik numarası gibi kişi veya kuruma özel olabilecek bilgilerin sahte e-postalarla dışarı sızdırılmasının engellenmesi için oluşturulmuş bir filtrelemedir.
DLP Metin Filtresini aktif etmek için “DLP Metin Filtresini Etkinleştir” karşısındaki kutucuğu işaretlememiz gerekmektedir. (Şekil 7)

Varsayılan olarak 3 şablon mevcuttur. Herhangi bir sablon üzerine tıklatıp göster dediğinizde içeriğini görebilirsiniz. Ekle kısmında ise kendiniz bir şablon oluşturarak bu tarz denetimleri fazlalaştırabilirsiniz. Şablon örnekleri için aşağıdaki adresten faydalanabilirsiniz.

- http://www.regexlib.com
- http://regex101.com/

KoruMail DLP Modülü açık iken modül tarafından engellenen maillerin bilgisini KoruMail arayüzünden "Raporlar" – "Posta Günlükleri" menüsünden "Gelişmiş Arama" linkini tıklayarak. (Şekil 8) Aşağıdaki örnekteki gibi filtreleyerek öğrenebilirsiniz.

Şekil 8



KoruMail Hakkında

İstanbul Yıldız Teknopark'ta faaliyet gösteren KoruMail; 2006 yılında e-posta konusundaki derin tecrübelerini Ar-Ge'ye aktararak ilk ürünü Secure Email Gateway çözümünü pazara sunmuştur. 35 kişilik genç ve dinamik kadrosuyla "E-posta ve Mesajlaşma" konusuna odaklanan KoruMail kendi geliştirdiği ürünlerle alanında lider global bir firma olmayı hedeflemektedir. KoruMail 2014 Eylül ayında Comodo Yazılım AŞ tarafından satın alınmış olup, Comodo bünyesinde faaliyetine devam etmektedir.

Adres: Yıldız Teknopark Atatürk Bulvarı İkitelli/İstanbul 1. Kat Ofis No:101

KoruMail bir COMODO firmasıdır.