

# Encrypt-Only & Do Not Forward Management

*Bu makalede, Azure Information Protection – Azure Rights Management (RMS) kapsamında E-mail Encryption yeteneklerinin **manuel** olarak kullanılması, uygulanması ve kullanılmayacağı senaryolarda ortamdan kaldırılması ile ilgili çalışmaları işleyeceğiz.*

İş hayatımızda iletişim dendiği zaman akla gelen ilk şey her zaman e-mail oluyor. E-mail kolay erişilebilir ve anlaşılabilir bir araç, ancak bu kolaylık içerisinde önemli datalarımızda bulunduğu unutmamak gerekiyor. Gizli verilerimizin yetkisiz kişilerce okunması, incelenmesi risklerini de yanında barındırıyor.

Microsoft Exchange ve M365 Exchange Online dünya çapında en çok kullanılan ve en çok gelişim gösteren platformdur. Kişisel bilgilerinizi yetkisiz erişime karşı korumanıza yardımcı olmak için e-postaların şifrelenmesi de dahil olmak üzere bir dizi araç ve özellik sağlamaktadır.

E-posta şifreleme, e-posta içeriğini ve hassas bilgileri yetkisiz erişime karşı korumaktadır . Bu, kişisel veya finansal bilgiler gibi hassas verilere sahip şirketler için özellikle önemli ve değerlidir. Şifrelenmemiş bu veriler siber saldırılara, kimlik hırsızlığına ve diğer ihlallere karşı savunmasız durumdadır. E-posta şifreleme ayrıca kuruluşların General Data Protection Regulation (GDPR), Kişisel Verilerin Korunması Konunu (KVKK) ve diğerleri gibi veri koruma düzenlemelerini karşılamalarına da yardımcı olur.

**Oluşturacağınız Etiketler ile bu operasyonları otomatize edebileceğiniz gibi, dilerseniz yeni bir mail oluşturma ekranı üzerinden de manuel şifreleme yapabilirsiniz.**

E-Posta Manuel Şifreleme Seçeneklerini İncelersek;

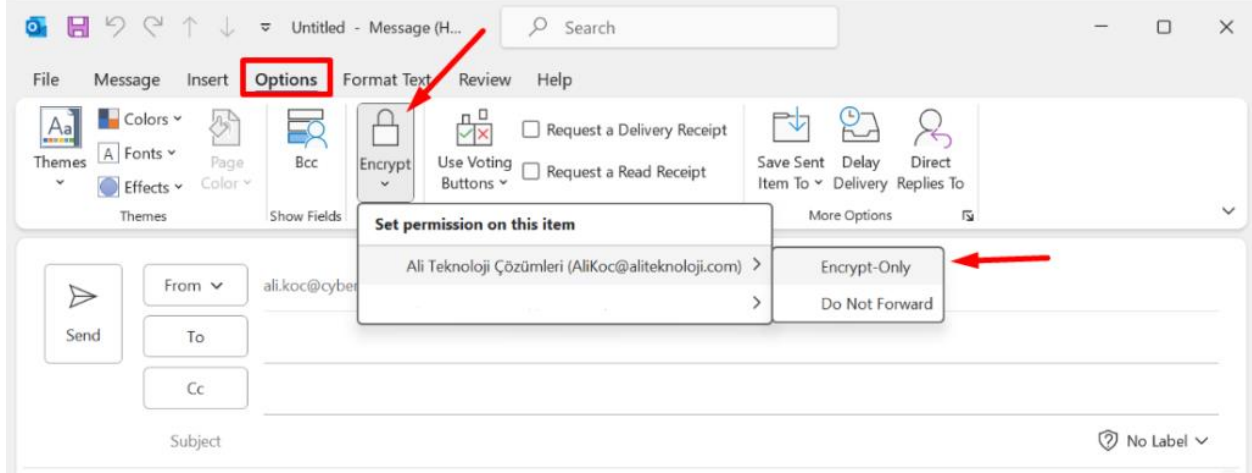
**Encrypt-Only** – İleti, tüm ekler dahil olmak üzere, alıcının posta kutusunda aktarım sırasında ve beklemedeyken şifrelenir. Alıcılar şifrelemeyi kaldıramaz, bu nedenle iletiye iletilen iletiler ve yanıtlar şifreli kalır. Yalnızca iletilmiş olan kişiler maili görüntüleyebilir. Görüntüleme yapmak isterkende kullanıcıdan credential ister.

**Do not Forward** – İleti, aktarım sırasında ve ekleri de dahil olmak üzere alıcının posta kutusunda beklemedeyken şifrelenir. Alıcılar bu mesajı okuyabilir ancak içeriği iletmez, yazdıramaz veya kopyalayamaz. Konuşma sahibi, mesajlarına ve tüm yanıtlara tam erişim hakkına sahiptir.

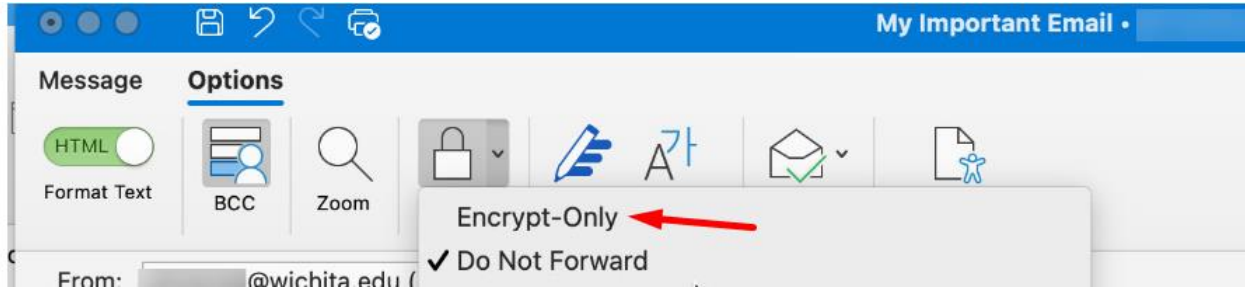
**Bir E-Posta nasıl şifrelenir ?**

**Encrypt-Only** seçeneği ile e-posta mesajını hem aktarım sırasında hem de alıcının posta kutusundaki bekleme durumunda, tüm ekler dahil olmak üzere şifreler. Alıcılar şifrelemeyi kaldıramaz. E-posta dizisinin tamamı şifreli kalacaktır.

**Windows:**



**Mac:**



Bir e-posta gönderirken Options > Encrypt seçeneği üzerinden maili şifreleyebilirsiniz.

Şifrelenmiş mail karşı tarafta aşağıdaki şekilde görüntülenecektir ve açılan mailde sizlerin credential girmenizi isteyecektir.

Test Gelen Kutusu x



Ali Koç (CYBERWISE)

Alici: ben ▼

Ali Koç (CYBERWISE) ([ali.koc@cyberwise.com.tr](mailto:ali.koc@cyberwise.com.tr)) has sent you a protected message.



Read the message

[Learn about messages protected by Microsoft Purview Message Encryption.](#)

[ali.koc@cyberwise.com.tr](mailto:ali.koc@cyberwise.com.tr) has sent you a protected message



Sign in to view the message



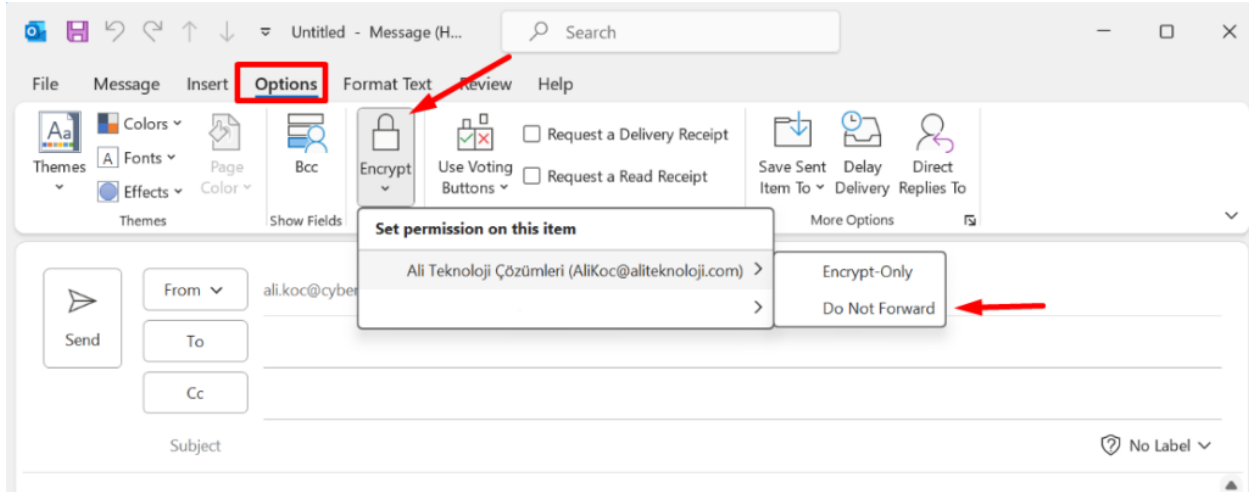
Sign in with a One-time passcode

[Need Help?](#)

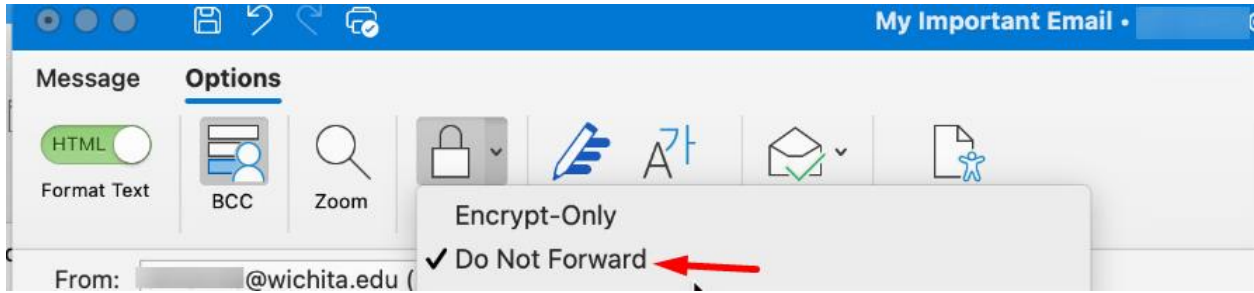
[Privacy Statement](#)

**Do Not Forward:** İleti, aktarım sırasında ve ekleri de dahil olmak üzere alıcının posta kutusunda beklemeyken şifrelenir. Alıcılar bu mesajı okuyabilir ancak içeriği iletemez, yazdıramaz veya kopyalayamaz. Konuşma sahibi, mesajlarına ve tüm yanıtlara tam erişim hakkına sahiptir.

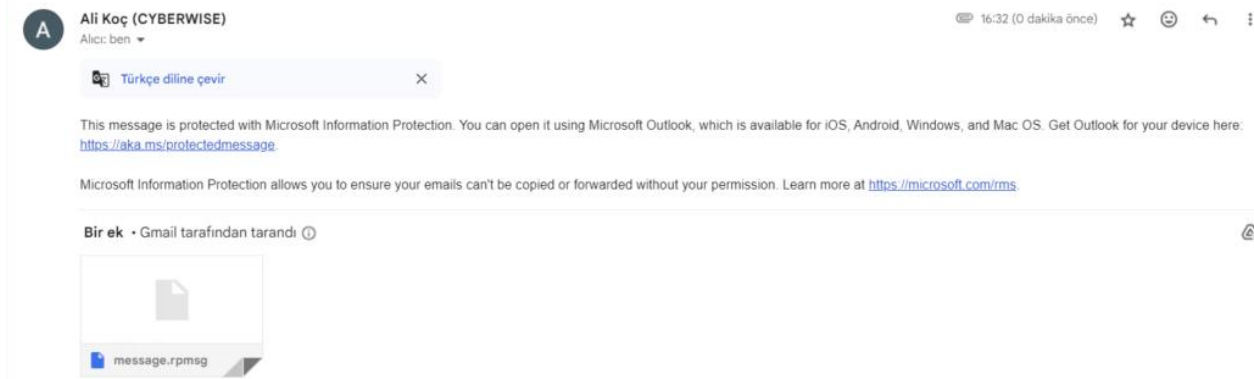
Windows:



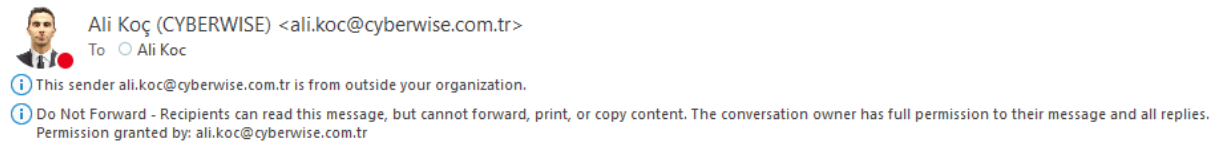
Mac:



Bir e-posta gönderirken Options > Encryption > Do Not Forward seçeneği üzerinden maili şifreleyebilir ve iletilmesini engelleyebilirsiniz.



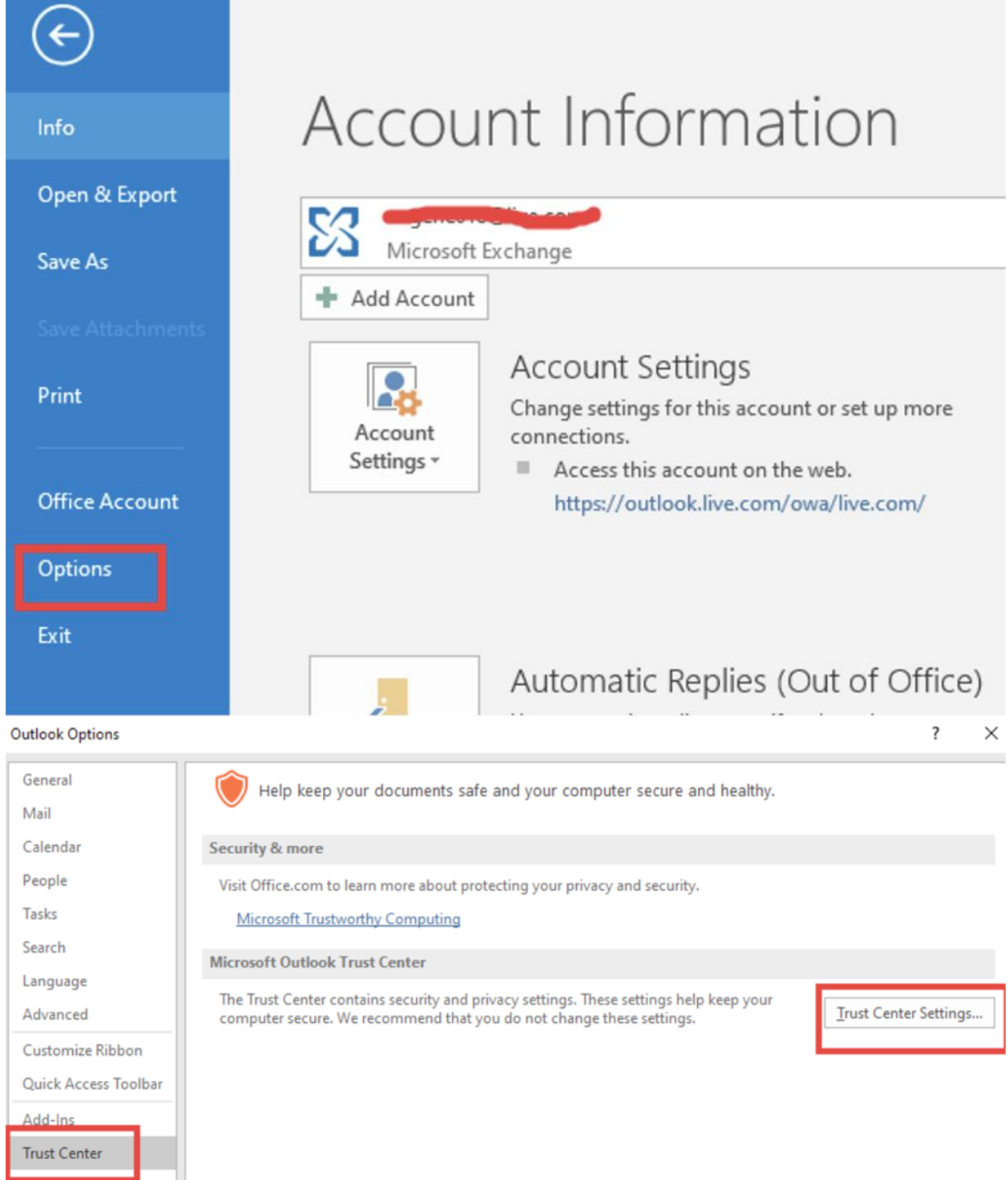
test



## Dışarıya Gönderilen Tüm Maillerin Encrypt Edilmesi

Outlook üzerinden yapılacak olan ayarlar ile tüm giden mesajları şifreleyecek şekilde ayarlayabilirsiniz.

” File” ya tıklayın , ardından “ Options” i seçin



- Trusted Publishers
- Privacy Options
- Email Security**
- Attachment Handling
- Automatic Download
- Macro Settings
- Programmatic Access

### Encrypted e-mail



- ☐ Encrypt contents and attachments for outgoing messages
- ☐ Add digital signature to outgoing messages
- ☒ Send clear text signed message when sending signed messages
- ☐ Request S/MIME receipt for all S/MIME signed messages

Default Setting:

[Settings...](#)

### Digital IDs (Certificates)



Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

[Publish to GAL...](#)

[Import/Export...](#)

[Get a Digital ID...](#)

### Read as Plain Text

Security Properties ✕

☐ Encrypt message contents and attachments

☐ Add digital signature to this message

☐ Send this message as clear text signed

☐ Request S/MIME receipt for this message

Security

Security setting:

<Automatic> ▼ Change Settings...

Security Label

Policy <None> ▼ Configure...

Classification ▼

Privacy Mark:

OK Cancel

#### Cihazlar Üzerinde Encrypt-Only veya Do Not Forward Özelliklerinin Kapatılması

Son kullanıcı cihazlarında olası bu özelliklerin kullanılmaması durumlarında, bu butonları pasife alabilirsiniz. Aşağıdaki registry kaydı ile bu özellikleri pasif moda alabilirsiniz.

Registry pathlerinin Office sürümüne göre farklı olacağını unutmayın.

- 14.0 = 2010

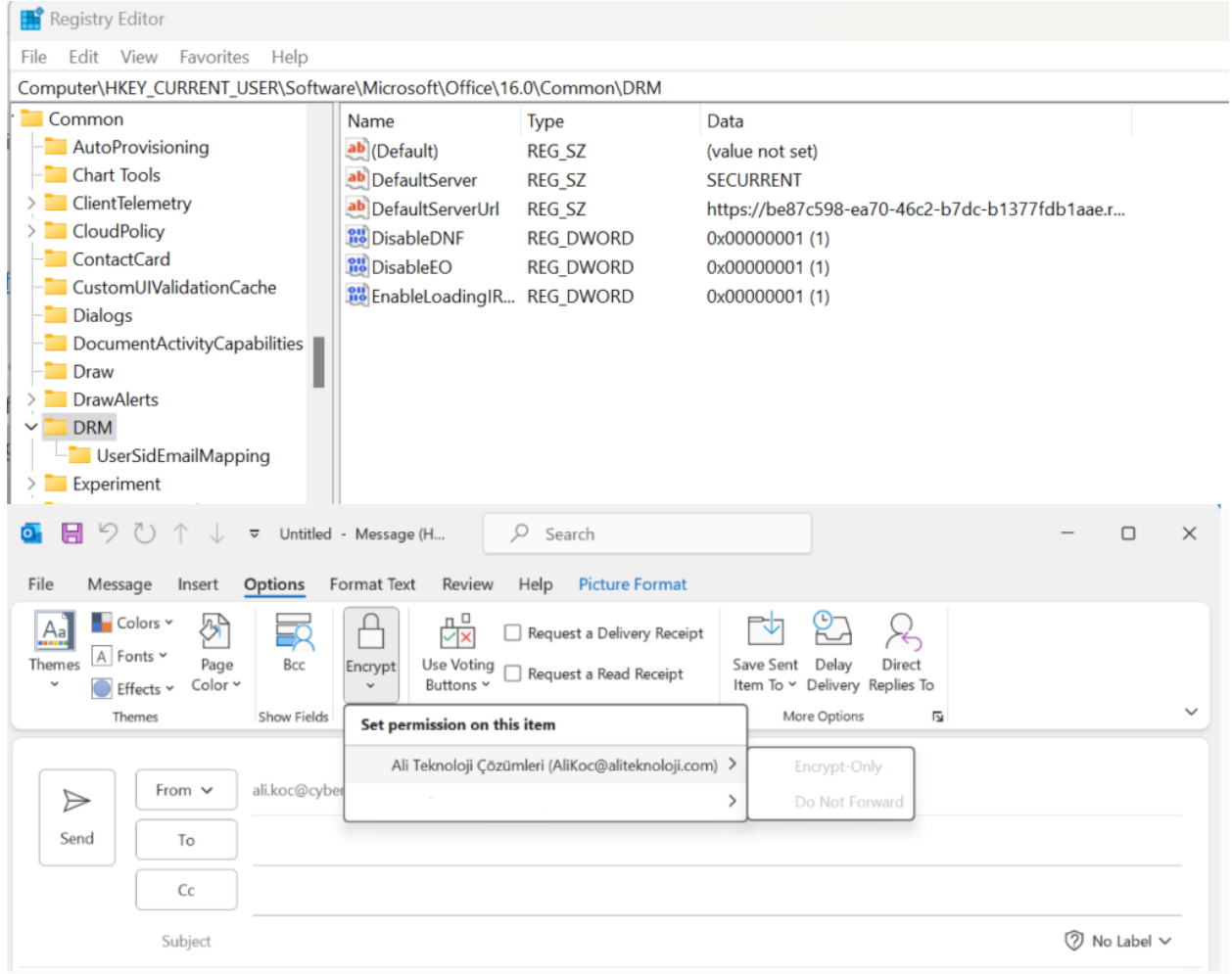
- 15.0 = 2013
- 16.0 = 2016

Registry Editörü açıyoruz (regedit)

**HKEY\_CURRENT\_USER\Software\Microsoft\Office\14.0\Common\DRM**

1. On the **Edit** menu, point to **New**, and then click **DWORD (32-bit) Value**.
2. Type **DisableDNF**, and then press ENTER.
3. In the **Details** pane, right-click **DisableDNF**, and then click **Modify**.
4. In the **Value data** box, type 1, and then click **OK**.
5. Exit Registry Editor.
6. If you previously disabled the **Do Not Forward** command by using a Group Policy setting, remove that policy setting.
7. and again right-click **DisableEO**, and then click **Modify**.
8. In the **Value data** box, type 1, and then click **OK**.
9. Exit Registry Editor.
10. If you previously disabled the **Encrypt-Only** command by using a Group Policy setting, remove that policy setting.





Tekrar aktif hale getirmek için registry kayıtlarını “0” değerine getirmeniz yeterli olacaktır.

Bir sonraki makalede görüşmek üzere.