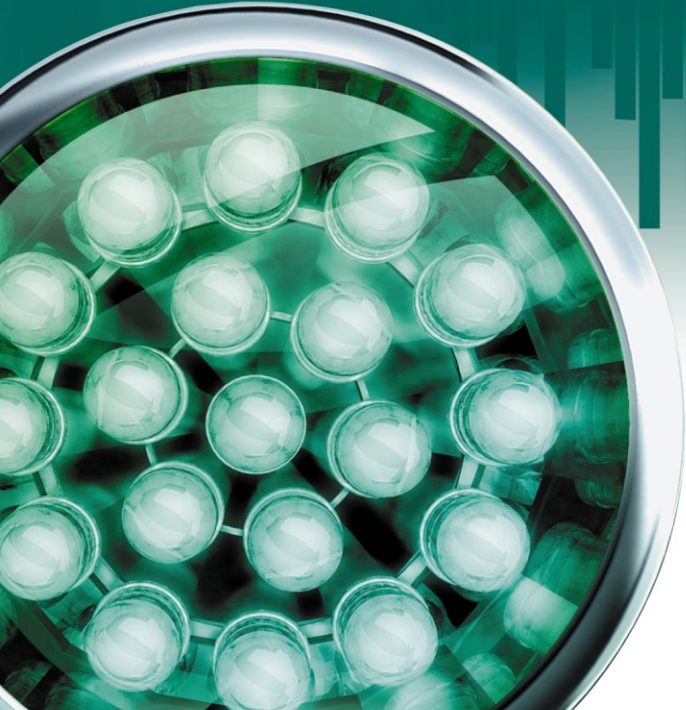


Kaspersky Security 8.0 for Microsoft Exchange Servers

YÜKLEME KILAVUZU

PROGRAM SÜRÜMÜ: 8.0



KASPERSKY lab

Sevgili Kullanıcılarımız!

Ürünümüzü seçtiğiniz için teşekkür ederiz. Umarız bu belge, işinizde size yardımcı olur ve sorularınızın büyük çoğunluğuna cevap sağlar.

Uyarı! Bu belge Kaspersky Lab'ın mülkünde olup, bu belgenin bütün hakları Rusya Federasyonu telif hakkı kanunları ve uluslararası anlaşmaları ile korunmaktadır. Bu belgenin veya bir kısmının kanun dışı olarak çoğaltılması ve dağıtılması, ilgili kanun gereğince hukuki, idari veya cezai sorumluluk doğuracaktır.

Çevrilmiş hali de dâhil olmak üzere, herhangi bir materyalin çoğaltılması veya dağıtılması sadece Kaspersky Lab'ın yazılı izni dâhilinde mümkündür.

Bu belge ve içinde bulunan grafiksel imgeler sadece, bilgilendirici, ticari olmayan veya kişisel amaçlar için kullanılabilir.

Bu belge üzerinde, önceden bildirilmeksizin değişiklikler yapılabilir. Son sürümü için, lütfen Kaspersky Lab'ın <http://www.kaspersky.com/docs> adresindeki internet sitesine bakın.

Kaspersky Lab, bu belge içinde kullanılmış herhangi bir materyalin içeriği, niteliği, ilişkisi veya doğruluğu için, üçüncü kişilere ait haklara veya bu tür materyallerin kullanımı ile ilgili potansiyel zararlara karşı hiç bir sorumluluk almamaktadır.

Bu belge, ayrı ayrı firmaların mülkiyetinde olan tescilli ticari markalar ve hizmet markaları içermektedir.

Revizyon tarihi: 06.05.2011

© 1997-2011 Kaspersky Lab ZAO. Tüm Hakları Saklıdır.

<http://www.kaspersky.com.tr>
<http://www.kaspersky.com.tr/destek>

İÇİNDEKİLER

BU KILAVUZ HAKKINDA	4
Bu belgede	4
BELGEDEKİ BİÇİMLER	5
EK BİLGİ KAYNAKLARI	6
Bağımsız arama İÇİN VERİ kaynakları	6
Kaspersky Lab uygulamalarının İNTERNET FORUMUNDA tartışılması	7
TEKNİK Dokümantasyon GELİŞTİRME Grubu İLE İLETİŞİM Kurma	7
KASPERSKY SECURITY 8.0 FOR MICROSOFT EXCHANGE SERVERS	8
Temel İŞLEVSELLİK	8
Dağıtım KİTİ	9
LİSANS anlaşması	9
Kayıtlı kullanıcılar İÇİN HİZMETLER	9
DONANIM VE YAZILIM GEREKSİNİMLERİ	10
YÜKLEME İÇİN HAZIRLIK	11
DAHA ÖNCEKİ BİR SÜRÜMDEN YÜKSELTME	12
UYGULAMA YÜKLEME PROSEDÜRÜ	13
Adım 1. GEREKLİ olan BİLEŞENLERİN YÜKLENMESİ	13
Adım 2. Selamlama ve LİSANS Anlaşması	14
Adım 3. yükleme türünün SEÇİLMESİ	14
Adım 4. Uygulama BİLEŞENLERİNİN SEÇİLMESİ	14
Adım 5. Microsoft SQL Sunucusuna bağlantının yapılandırılması	15
Adım 6. Dosyaların kopyalanması	16
BAŞLARKEN. UYGULAMA YAPILANDIRMA SİHİRBAZI	17
GÜNCELLEMELERİN yapılandırılması	17
LİSANS anahtarının kurulması	17
BİLDİRİM ayarları	18
Sunucu korumanın yapılandırılması	18
GÜVENLİK Sunucusuna bağlanması	19
Uygulama İŞLEVSELLİĞİNİN test EDİLMESİ	19
UYGULAMANIN YENİDEN YÜKLENMESİ	21
UYGULAMANIN KALDIRILMASI	22

BU KILAVUZ HAKKINDA

Kaspersky Lab ZAO ekibinden sevgiler (bundan sonra Kaspersky Lab olarak anılacaktır)! Umarız bu Yükleme Kılavuzu, Kaspersky Security 8.0 for Microsoft Exchange Servers'in (bundan sonra Exchange Servers için KS 8.0 veya Kaspersky Security olarak anılacaktır) yükleme prosedürünü, parametre ayarlarını ve temel çalışma prensiplerini anlamanıza yardımcı olacaktır. Bu belge, Kaspersky Security yazılımını posta sunucuları için koruyucu çözüm olarak seçmiş Microsoft Exchange Server 2007 veya 2010 (bundan sonra Microsoft Exchange Server olarak anılacaktır) kullanan posta sunucularının yöneticilerine yöneliktir.

Bu belgenin amacı şunlardır:

- Microsoft Exchange Server yöneticilerinin, uygulama bileşenlerini sunucuya yüklemelerine, sunucu korumasını etkinleştirmelerine ve mevcut görevlerin ışığında en uygun yapılandırmayı sağlamalarına yardımcı olmak;
- yükleme işlemiyle ilgili sorunlar hakkında hızlıca araştırılabilen bilgiler sunmak;
- uygulama ve teknik destek alma yöntemleri hakkında alternatif bilgi kaynakları sunmak.

BU BÖLÜMDE

Bu belgede	4
Belgedeki biçimler	5

BU BELGEDE

Kaspersky Security 8.0 for Microsoft Exchange Servers Yükleme Kılavuzu, aşağıdaki bölümlerden oluşmaktadır:

- Bu Kılavuz hakkında (sayfa [4](#)). Bu bölüm Yükleme Kılavuzunun yapısını açıklamaktadır.
- Ek bilgi kaynakları (sayfa [6](#)). Bu bölüm, Kaspersky Security'nin satın alınması, yüklenmesi ve kullanımı ile ilgili olarak çeşitli bilgi kaynaklarını açıklamaktadır.
- Kaspersky Security 8.0 for Microsoft Exchange Servers (sayfa [8](#)). Bu bölüm, uygulamanın başlıca özelliklerini açıklamaktadır.
- Donanım ve yazılım gereksinimleri (sayfa [10](#)). Bu bölüm, Kaspersky Security'nin donanım ve yazılım gereksinimlerini açıklamaktadır.
- Yükleme için hazırlık (sayfa [11](#)). Bu bölüm, uygulamayı kurmadan önce gerçekleştirilmesi gereken eylemleri açıklamaktadır.
- Daha önceki bir sürümden yükseltme (sayfa [12](#)). Bu bölüm, Kaspersky Security'nin önceki bir sürümünden nasıl yükseltme yapılacağını açıklamaktadır.
- Yükleme prosedürü (sayfa [13](#)). Bu bölüm, uygulamanın yüklenmesi için adım adım talimatları içermektedir.
- Başlarken.Başlangıç Yapılandırma Sihirbazı (bkz.bölüm "Başlarken.Başlangıç Yapılandırma Sihirbazı" sayfa [17](#)). Bu bölüm, yüklemeyi hemen sonra ana uygulama ayarlarının yapılandırılması için talimatları içermektedir.
- Uygulamanın yeniden yüklenmesi (sayfa [21](#)). Bu bölüm, programın çalışmasında herhangi bir hata olması durumunda programın geri yüklenmesi için kullanılacak yöntemler hakkında bilgi vermektedir.
- Uygulamanın kaldırılması (sayfa [22](#)). Bu bölüm, uygulama kaldırma prosedürü hakkında bilgi vermektedir.

BELGEDEKİ BİÇİMLER

Bu Kılavuz, aşağıdaki tabloda açıklanmış olan belge biçimlerini kullanmaktadır.

Table 1. Belgedeki biçimler

ÖRNEK METİN	BELGEDEKİ BİÇİMLERİN AÇIKLAMASI
Lütfen şunları göz önünde bulundurun:	Uyarılar, kırmızıyla işaretlenmiştir ve çerçeveye alınmıştır. Uyarılar, önemli bilgiler içermektedir, örnek olarak, bilgisayar güvenliği için önemli olan işlemlerle ilgili olan bilgiler gibi.
Şunu kullanmanız tavsiye edilmektedir:	Notlar, çerçeve içine alınmıştır. Notlarda, ek ve referans bilgileri bulunmaktadır.
Örnek: ...	Örnekler, "Örnek" başlığı altında sarı arka plan rengine sahip bölümler içinde verilmiştir.
Bir güncelleme ...	Yeni terimler, italik biçimde yazılmıştır.
ALT+F4	Klavye tuşlarının isimleri, büyük harfle ve kalın biçimde yazılmıştır. "Artı" işareti ile bağlantılı tuşların isimleri, tuş kombinasyonlarını belirtmektedir.
Etkinleştirme	Kullanıcı Arabirimindeki unsurlar, örnek olarak, giriş alanlarının isimleri, menü seçenekleri ve düğmeler, kalın şekilde yazılmıştır.
➔ Bir görev zaman çizelgesi yapılandırmak için, aşağıdaki adımları uygulayın:	Talimatların tanıtıcı ifadeleri, italik biçimde yazılmıştır.
yardım	Komut satırına girilen komutlar veya ekran üzerinde gösterilen iletiler, özel bir karakterle vurgulanmıştır.
<bilgisayarınızın IP adresi>	Değişkenler, açılı ayraçlar içinde verilmiştir. Her durumda ilgili değeri değişkenle yer değiştirmeniz gerekir; açılı ayraçlar çıkartılacaktır.

EK BİLGİ KAYNAKLARI

Kaspersky Security ürününün seçimi, satın alınması, yüklenmesi veya kullanımı ile ilgili herhangi bir sorunuz var ise hızlı bir şekilde yanıt alabilirsiniz.

Kaspersky Lab, uygulama ile ilgili olarak birçok bilgi kaynağı sağlar. Sorunuzun aciliyetine veya önem derecesine göre en uygun hizmeti seçebilirsiniz.

BU BÖLÜMDE

Bağımsız arama için veri kaynakları	6
Kaspersky Lab uygulamalarının internet forumunda tartışılması.....	7
Teknik Dokümantasyon Geliştirme Grubu ile İletişim Kurma.....	7

BAĞIMSIZ ARAMA İÇİN VERİ KAYNAKLARI

Uygulama ile ilgili olarak aşağıdaki bilgi kaynaklarına başvurabilirsiniz:

- Kaspersky Lab internet sitesindeki Anti-Virüs sayfası;
- Teknik Destek internet sitesindeki uygulama sayfası (Bilgi Tabanında);
- çevrimiçi yardım sistemi;
- dokümantasyon.

Kaspersky Lab internet sitesindeki Anti-Virüs sayfası

<http://www.kaspersky.com/business>

Bu sayfada, Kaspersky Security, özellikleri ve Kaspersky Security ile çalışmanın ayrıntıları hakkında genel bilgiler bulabilirsiniz.

Teknik Destek internet sitesindeki uygulama sayfası (Bilgi Tabanında)

<http://support.kaspersky.com/exchange>

Bu sayfa, Teknik Destek uzmanları tarafından yayınlanan makaleler içerir.

Bu makaleler, faydalı bilgiler, kılavuzlar ve Kaspersky Security'nin işletimi ile ilgili sık sorulan sorulara yanıtlar içermektedir.

Çevrimiçi yardım sistemi

Çevrimiçi yardım sistemi, program bileşenlerinin ayarlanması ile ilgili bilgilerin yanı sıra uygulama yönetimi ile ilgili talimatlar ve öneriler içerir. Çevrimiçi yardım sistemine erişmek için, Yönetim Konsolunun Eylemler menüsünde Yardım ögesini seçin.

Kaspersky Security'de bulunan belirli bir pencere veya sekme ile ilgili bir sorunuz var ise içeriksel yardımı kullanabilirsiniz.

İçeriksel yardımı açmak için, sizi ilgilendiren pencereyi veya sekmeyi açın ve **F1** tuşuna basın.

Dokümantasyon

Kaspersky Security'nin Yükleme Kılavuzu, uygulamayı kurmak için gerekli olan tüm bilgileri içerir ve uygulama paketine dahildir.

KASPERSKY LAB UYGULAMALARININ İNTERNET FORUMUNDA TARTIŞILMASI

Sorunuz acil bir yanıt gerektirmiyor ise, sorunuzu <http://forum.kaspersky.com/index.php?showforum=218> adresinde bulunan forumumuzda Kaspersky Lab uzmanları ve diğer kullanıcılar ile tartışabilirsiniz.

Bu forumda mevcut konu başlıklarını görebilir, yorumlarda bulunabilir, yeni konu başlıkları oluşturabilir ve arama motorunu kullanabilirsiniz.

TEKNİK DOKÜMANTASYON GELİŞTİRME GRUBU İLE İLETİŞİM KURMA

Dokümantasyon ile ilgili sorunuz varsa, bir hata bulduysanız veya geri bildirimde bulunmak istiyorsanız, Teknik Dokümantasyon Geliştirme Grubu ile iletişim kurabilirsiniz.

Bilgisayarınızda varsayılan e-posta istemcisini açmak için Yardım penceresinin sağ üst tarafında bulunan **Geri bildirim bırak** bağlantısına tıklayın. Görüntülenen pencere otomatik olarak Dokümantasyon Geliştirme grubunun adresini (docfeedback@kaspersky.com) ve "Kaspersky Yardım Geri Bildirimi: Kaspersky Security" ileti konusunu içerecektir. Geri bildiriminizi yazın ve konuyu değiştirmeden e-posta gönderin.

KASPERSKY SECURITY 8.0 FOR MICROSOFT EXCHANGE SERVERS

Kaspersky Security 8.0 for Microsoft Exchange Servers , Microsoft Exchange Server'a baęlı posta sunucuları için virüslere, Trojan yazılımına ve e-posta aracılığıyla iletilebilecek dięer tehlike türlerine karşı koruma için tasarlanan bir uygulamadır.

Kötü amaçlı yazılım ciddi hasara neden olabilir; bu programlar verileri çalmak, bloke etmek, deęiřtirmek veya yok etmek için özellikle tasarlanmış olup bilgisayarların ve bilgisayar ağlarının çalışmasını sekteye uğratırlar. Büyük çaplı virüs postalama, hem çalışan sunucuları hem de iş istasyonlarını devre dışı bırakarak kurumsal ağlara hızla yayılabilir ve istenmeyen aksama süreleri ve kayıplarla sonuçlanır. Ayrıca virüs saldırıları, işinizi ve ortaklarınızın işini olumsuz etkileyebilecek veri kayıplarına da neden olabilir.

Kaspersky Security, kurumsal posta sunucunuz üzerinde istenmeyen posta önlemesi sağlayarak, çalışanlarınızı istenmeyen postaları el ile silme zahmetinden kurtarır.

BU BÖLÜMDE

Temel işlevsellik	8
Dağıtım Kiti	9

TEMEL İŞLEVSELLİK

Kaspersky Security, posta kutularını, ortak klasörleri ve Microsoft Exchange Server'dan aktarılan posta trafiğini kötü amaçlı yazılımlara ve istenmeyen postalara karşı korur. Uygulama, korunan Microsoft Exchange Server'dan geçen tüm e-posta trafiğini tarar.

Kaspersky Security, aşağıdaki işlemleri gerçekleştirebilir:

- Gelen ve giden postaların yanı sıra Microsoft Exchange Server'da depolanan iletileri (ortak klasörler dâhil) kötü amaçlı yazılımlar için tarar. Tarama sırasında uygulama tüm iletiyi ve ekli nesnelere işler. Uygulama, seçilen ayarlara baęlı olarak tespit edilen zararlı nesnelere temizler veya kaldırır ve kullanıcılara bunlar hakkında tam bilgi sağlar.
- Teklifiiz postaları (istenmeyen postalar) posta trafiğinden filtreler. İstenmeyen Posta bileşeni, posta trafiğinde istenmeyen posta olup olmadığını tarar. Ayrıca İstenmeyen Posta, gönderici adreslerinin beyaz ve kara listelerinin oluşturulmasını sağlar ve istenmeyen posta analiz yoğunluğunun esnek bir şekilde yapılandırılmasını destekler.
- Nesnelere (ekler veya ileti metinleri) ve istenmeyen posta iletilerinin temizlenmeden veya silinmeden önce gerektiğinde geri yüklenebilmelerini sağlamak amacıyla kopyalarını yedekler, böylece veri kaybı riskini önler. Yapılandırılabilir filtreler, saklanan bağımsız nesnelere yerini kolaylıkla bulmanızı sağlar.
- Göndereni, alıcıyı ve sistem yöneticisini, kötü amaçlı nesnelere içeren iletiler hakkında bilgilendirir.
- Olay günlükleri tutar, uygulama etkinliği ile ilgili istatistikler toplar ve düzenli raporlar oluşturur. Uygulama, bir çizelgeye veya isteğe göre otomatik olarak raporlar oluşturabilir.
- Uygulama ayarlarını, aktarılan trafiğin hacmine ve türüne uygun olacak şekilde yapılandırır, özellikle taramayı optimize etmek için bağlantı zaman aşımını tanımlar.
- Kaspersky Security veritabanılarını otomatik olarak veya manuel modda günceller. Güncellemeler Kaspersky Lab'ın FTP veya HTTP sunucularından, en son güncellemeler grubunu içeren yerel / ağ klasöründen veya kullanıcı tanımlı FTP veya HTTP sunucularından indirilebilir.

- İletileri, çizelgeye uygun olarak yeni virüsler açısından yeniden tarayın. Bu görev arka plan taraması olarak gerçekleştirilir ve posta sunucusunun performansı üzerinde fazla etkisi olmaz.
- Depolama düzeyi üzerinde Anti-Virüs'ü yönetin ve korunan depolama alanlarının bir listesini oluşturun.
- Lisansların yönetilmesi. Kullanıcı hesapları için değil, belirli sayıdaki posta kutuları için lisans verilir.

DAĞITIM KİTİ

Kaspersky Security'yi ortaklarımızdan veya <http://www.kaspersky.com.tr> adresinin e-Mağaza kısmı gibi internet mağazalarından çevrimiçi satın alabilirsiniz. Kaspersky Security, Kaspersky Security for Mail Servers (http://www.kaspersky.com/kaspersky_security_mail_server) veya Kaspersky Open Space Security ürünlerinin bir parçası olarak (http://www.kaspersky.com/open_space_security) Kaspersky Enterprise Space Security ve Kaspersky Total Space Security çözümleri içine dâhil edilmiştir. Kaspersky Security için bir lisans satın aldıktan sonra, uygulamayı Kaspersky Lab internet sitesinden indirmek amacıyla ya içinde bir bağlantı ve lisans etkinleştirme için bir anahtar dosyası bulunan bir e-posta ya da ürün dağıtım paketi bulunan bir yükleme CD'si alacaksınız. Yükleme diskini zarfı üzerindeki mührü açmadan önce, Son Kullanıcı Lisans Anlaşmasını dikkatlice okuyun.

LİSANS ANLAŞMASI

Son Kullanıcı Lisans Anlaşması, siz ve Kaspersky Lab arasında, satın almış olduğunuz yazılımın kullanımı hakkındaki şartları ayrıntılarıyla belirten, yasal bir anlaşmadır.

Son Kullanıcı Lisans Anlaşmasını dikkatlice okuyun!

Lisans anlaşmasının şartlarını ve koşullarını kabul etmezseniz, ürünü iade edebilir ve paranızı geri alabilirsiniz. Lütfen yükleme CD'sinin bulunduğu zarfın mühürlü olması gerektiğini göz önünde bulundurun.

Mühürlü yükleme diskini açtığınızda, Son Kullanıcı Lisans Anlaşmasındaki koşulların tamamını kabul etmiş olursunuz.

KAYITLI KULLANICILAR İÇİN HİZMETLER

Kaspersky Lab ZAO, Kaspersky Security'nin yasal kayıtlı kullanıcıları için uygulamanın performansını attırmalarına olanak sağlayan kapsamlı bir hizmet paketi sunmaktadır.

Bir lisans satın aldıktan sonra, kayıtlı bir kullanıcı olursunuz ve lisans süreniz boyunca, aşağıdaki hizmetlerden yararlanırsınız:

- düzenli uygulama veritabanı güncellemeleri ve yazılım paketi güncelleştirmeleri;
- satın alınan yazılım ürününün yüklenmesi, yapılandırılması ve kullanımı ile ilgili konularda telefon veya e-posta aracılığıyla destek;
- yeni Kaspersky Lab ürünleri ve tüm dünyada meydana çıkan yeni virüsler hakkında bilgiler. Bu hizmet, Teknik Destek Servisi internet sitesi(<http://support.kaspersky.com/subscribe/>) üzerindeki Kaspersky Lab haber postasına kayıt yaptıran kullanıcılar için mevcuttur.

İşletim sistemlerinin, üçüncü tarafa ait yazılımların veya Kaspersky olmayan teknolojilerin performansı ve kullanımları ile ilgili sorunlar için destek verilmez.

DONANIM VE YAZILIM GEREKSİNİMLERİ

Donanım gereksinimleri

Kaspersky Security'nin donanım gereksinimleri Microsoft Exchange Server'ın gereksinimleri ile aynıdır. Uygulama ayarlarına ve işletim moduna bağlı olarak Yedek depolama ve diğer hizmet klasörleri için kayda değer oranda disk alanı gerekebilir (varsayılan ayarları kullanırken Yedek depolama klasörü 5120 MB'a kadar bir alanı tutabilir).

Uygulama ile birlikte kurulan Yönetim Konsolu donanım gereksinimleri aşağıdaki gibidir:

- Intel Pentium 400 MHz veya daha hızlı bir işlemci (1000 MHz önerilir);
- 256 MB boş RAM;
- Uygulama dosyaları için 500 MB disk alanı.

Yazılım gereksinimleri

Kaspersky Security'nin yüklenebilmesi için aşağıdaki işletim sistemlerinden biri gereklidir:

Microsoft Small Business Server 2008 Standard / Microsoft Small Business Server 2008 Premium / Microsoft Essential Business Server 2008 Standard / Microsoft Essential Business Server 2008 Premium / Microsoft Windows Server 2008 x64 R2 Enterprise Edition / Microsoft Windows Server 2008 x64 R2 Standard Edition / Microsoft Windows Server 2008 x64 Enterprise Edition Service Pack 1 / Microsoft Windows Server 2008 x64 Enterprise Edition Service Pack 2 / Microsoft Windows Server 2008 x64 Standard Edition Service Pack 1 / Microsoft Windows Server 2008 x64 Standard Edition Service Pack 2 / Microsoft Windows Server 2003 x64 R2 Enterprise Edition Service Pack 2 / Microsoft Windows Server 2003 x64 R2 Standard Edition Service Pack 2 / Microsoft Windows Server 2003 x64 Enterprise Edition Service Pack 2 / Microsoft Windows Server 2003 x64 Standard Edition Service Pack 2.

Yükleme için aşağıdaki bileşenler gerekir:

- Şu rollerden en az birinde konuşlandırılan Microsoft Exchange Server 2007 x64 Service Pack 1 veya Microsoft Exchange Server 2010: Hub Aktarımı veya Posta Kutusu;
- MS SQL Server 2005 Express Edition, MS SQL Server 2005 Standard Edition, MS SQL Server 2005 Enterprise Edition, MS SQL Server 2008 Express Edition, MS SQL Server 2008 Standard Edition, MS SQL Server 2008 Enterprise Edition;
- Microsoft .NET Framework 3.5 Service Pack 1.

Yönetim Konsolu yüklemesi aşağıdaki işletim sistemlerinden birini gerektirir:

Microsoft Small Business Server 2008 Standard / Microsoft Small Business Server 2008 Premium / Microsoft Essential Business Server 2008 Standard / Microsoft Essential Business Server 2008 Premium / Microsoft Windows Server 2008 / Microsoft Windows Server 2003 x64 Service Pack 2 / Microsoft Windows Server 2003 x64 R2 Standard Edition / Microsoft Windows Server 2003 x64 R2 Enterprise Edition / Microsoft Windows XP x64 Service Pack 2 / Microsoft Windows Vista x64 / Microsoft Windows Server 2003 R2 Standard Edition / Microsoft Windows Server 2003 R2 Enterprise Edition / Microsoft Windows Vista / Microsoft Windows Server 2003 Service Pack 2 / Microsoft Windows XP Service Pack 3 / Windows 7 Professional / Windows 7 Enterprise / Windows 7 Ultimate.

yükleme için aşağıdaki bileşenler gerekir:

- Microsoft Management Console 3.0;
- Microsoft .NET Framework 3.5 Service Pack 1.

YÜKLEME İÇİN HAZIRLIK

Kaspersky Security'nin kurulması için, etki alanı yöneticisinin ayrıcalıklarına sahip olmanız gerekecektir. Bundan başka, aşağıdaki gerekli olan bileşenlerin kurulması için bir internet bağlantısı gereklidir:

- .NET Framework 3.5 SP1;
- Microsoft Management Console 3.0;
- Microsoft SQL Server 2005 / 2008 (Standard, Express, Enterprise).

Bir SQL sunucu üzerinde veritabanı oluşturmak için, Kaspersky Security'nin kurulacağı bilgisayarın yerel erişim haklarına ve SQL sunucunun yönetici ayrıcalıklarına sahip olmanız gerekecektir. Eğer SQL sunucusu etki alanı denetleyicisi üzerinde çalışıyorsa, Enterprise Admins ve / veya Domain Admins grup üyesi olmanız gerekir.

DAHA ÖNCEKİ BİR SÜRÜMDEN YÜKSELTME

Kaspersky Security, daha önceki sürümlerden yükseltmeleri desteklemez. Kaspersky Security yüklemesinden önce bilgisayara yüklenmiş olan daha eski bir sürüm varsa kaldırılması gerekir. Daha önceki sürüme ait veriler ve ayarlar saklanmayacaktır.

UYGULAMA YÜKLEME PROSEDÜRÜ

Kaspersky Security, iki ana bileşenden oluşmaktadır: Güvenlik Sunucusu ve Yönetim Konsolu. Güvenlik Sunucusu, her zaman Yönetim Konsolu ile birlikte yüklenir. Yönetim Konsolu, Güvenlik Sunucusunun uzaktan yönetimi için bir başka bilgisayar üzerine ayrıca yüklenebilir. Kurumsal sunucunuzun mimarisine bağlı olarak mevcut üç yükleme değişkeninden birini seçebilirsiniz:

- Güvenlik Sunucusu, Microsoft Exchange Server'ı çalıştıran bilgisayar üzerine kurulacaktır. Yönetim Konsolu, aynı sunucu üzerine yüklenecektir.
- Güvenlik Sunucusu ve Yönetim Konsolu, Microsoft Exchange Server'ı çalıştıran bilgisayar üzerine yüklenecektir. Yönetim Konsolu, Güvenlik Sunucusunun uzaktan yönetimi için kurumsal ağınız dâhilindeki herhangi bir bilgisayara yüklenebilir.
- Güvenlik Sunucusu, Microsoft Exchange Server'ı çalıştıran sunucular kümesine kurulacaktır. Bu durumda Güvenlik Sunucusu ve Yönetim Konsolu kümenin her bir düğümüne birlikte kurulmalıdır.

Microsoft Exchange Server'ın bazı hizmetleri Kaspersky Security yüklemesinden sonra yeniden başlatılmalıdır.

Kaspersky Security yükleyici, prosedürün her bir adımı sırasında uygulamanız gereken işlemler hakkında bilgiler sunan bir sihirbaz olarak tasarlanmıştır. **Geri** ve **İleri** düğmeleri, herhangi bir zamanda yükleme ekranları (adımları) arasında gidip gelmek için kullanılabilir. **Çıkış** ve **İptal** düğmeleri, yükleyiciden çıkmanızı sağlar. **Bitir** düğmesi, yükleme prosedürünü tamamlar. yükleme prosedürü, setup_en.exe dosyası çalıştırıldığı zaman başlar. Kurulum Sihirbazı tarafından uygulanan adımlar hakkında daha ileride bahsedeceğiz.

BU BÖLÜMDE

Adım 1. Gerekli olan bileşenlerin kurulması	13
Adım 2. Selamlama ve Lisans Anlaşması	14
Adım 3. yükleme türünün seçilmesi	14
Adım 4. Uygulama bileşenlerinin seçilmesi	14
Adım 5. Microsoft SQL Sunucusuna bağlantının yapılandırılması	15
Adım 6. Dosyaların kopyalanması.....	16

ADIM 1. GEREKLİ OLAN BİLEŞENLERİN YÜKLENMESİ

Bu adım sırasında, aşağıdaki gerekli olan bileşenlerin bilgisayara yüklenmiş olduklarından emin olun:

- .NET Framework 3.5 SP1. **.NET Framework 3.5 SP 1 ögesini karşıdan yükle ve kur** düğmesine tıklayarak bu bileşeni kurabilirsiniz. .NET Framework 3.5 SP1 yüklemesi ardından, bilgisayarın yeniden başlatılması gerekir! Yeniden başlatmadan devam ederseniz, Kaspersky Security'nin çalışması sırasında sorunlar meydana gelebilir.
- Microsoft Windows Installer (MSI) 4.5. Bu bileşen, Microsoft SQL Server 2008 Express Edition kurmak için gereklidir. **Microsoft Windows Installer 4.5 ögesini karşıdan yükle ve kur** düğmesine tıklayarak bu bileşeni kurabilirsiniz.
- Microsoft SQL Server 2008 Express Edition veya başka bir SQL sunucu. Bileşeni kurmak için, **Microsoft SQL Server 2008 Express Edition ögesini kur** düğmesine tıklayın. Kaspersky Security ile çalışmak için, SQL Server programının sıfırdan yüklemesi tavsiye edilmektedir.

- Microsoft Management Console 3.0 (MMC 3.0). Microsoft Management Console 3.0 (MMC 3.0), Microsoft Windows Server 2003 R2 ve daha sonraki sürüm işletim sistemlerinin bir parçasıdır. Programı Microsoft Windows Server yazılımının daha önceki sürümlerine kurmak için, MMC'yi 3.0 sürümüne yükseltmeniz gerekir. Bunu yapmak için, **MMC 3.0 ögesini karşıdan yükle ve kur** düğmesine basın.

Kaspersky Security 8.0 for Microsoft Exchange Servers bağlantısına tıklayarak, bir sonraki yükleme adımına geçebilirsiniz.

Bundan başka, bir Yükleme Kılavuzunu karşıdan yüklemek ve kurmak için, **Yükleme Kılavuzu** düğmesine tıklayabilirsiniz.

ADIM 2. SELAMLAMA VE LİSANS ANLAŞMASI

Karşılama ekranı size, Kaspersky Security'nin bilgisayarınıza kurulmaya başladığını bildirir. **İleri** düğmesine tıklandığında Lisans Anlaşması penceresi açılır.

Lisans Anlaşması, uygulama kullanıcısı ile Kaspersky Lab arasındaki bir anlaşmadır. **Lisans Sözleşmesi şartlarını kabul ediyorum** kutusunun işaretlenmesi, Lisans Anlaşmasını okuduğunuz ve koşulları ve şartları kabul ettiğiniz anlamına gelmektedir.

ADIM 3. YÜKLEME TÜRÜNÜN SEÇİLMESİ

yükleme türü seçim ekranında iki adet düğme bulunur:

- **Normal.** Bu düğmeye tıklamak, çoğu kullanıcı için uygun olan standart bileşenlerin yükleme prosedürüne devam ettirecektir. Daha fazla talimat için lütfen Adım 5'e bakın.
- **Özel.** Bu düğmeye tıklamak, manuel olarak kurmak istediğiniz uygulama bileşenlerini seçmenize olanak sağlar. Özel yükleme modu, deneyimli kullanıcılar için tavsiye edilmektedir.

yükleme türü seçildikten sonra, Kurulum Sihirbazı bir sonraki adıma geçer.

ADIM 4. UYGULAMA BİLEŞENLERİNİN SEÇİLMESİ

Eğer **Özel** yükleme türünü seçmişseniz, yükleyici kurmak istediğiniz bileşenleri seçmeniz için size hatırlatma yapacaktır. yükleme için mevcut olan bileşenler dizisi, Microsoft Exchange Server'ın kurulup kurulmadığına ve ne şekilde yapılandırıldığına göre farklılık gösterecektir. Eğer Microsoft Exchange Server hem Posta Kutusu hem de Hub Aktarımı olarak çalışması için dağıtılmışsa, aşağıdaki bileşenler seçim ve yükleme için mevcut olacaktır:

- Yönetim Konsolu;
- İstenmeyen Posta önleme bileşeni;
- Posta Kutusu yapılandırması için Anti-Virüs.
- Hub Aktarımı ve Edge Aktarımı için Anti-Virüs.

Eğer Microsoft Exchange Server sadece Edge Aktarımı veya Hub Aktarımı olarak çalışması için dağıtılmışsa, aşağıdaki bileşenler seçim ve yükleme için mevcut olacaktır:

- Yönetim Konsolu;
- İstenmeyen Posta önleme bileşeni;
- Hub Aktarımı ve Edge Aktarımı için Anti-Virüs.

Eğer Microsoft Exchange Server sadece Posta Kutusu olarak çalışması için dağıtılmışsa, aşağıdaki bileşenler seçim ve yükleme için mevcut olacaktır:

- Yönetim Konsolu;
- Posta Kutusu yapılandırması için Anti-Virüs.

Diğer bütün durumlar için sadece, Yönetim Konsolu yükleme için mevcuttur.

Varsayılan yükleme klasörünün tam adı, pencerenin alt kısmında görüntülenir. Yükleme klasörünü değiştirmek için, **Gözet** düğmesine tıklayın ve başka bir konum belirleyin. Veri depolama klasörü, aşağıda görüntülenir. Veri depolama klasörü, aşağıdaki öğeleri içermektedir:

- Anti-Virüs veritabanı;
- İstenmeyen Posta veritabanı;
- karantina nesnelere.

Eğer klasörün seçilen sürücüde mevcut olan boş alandan daha fazla yer tutacağına inanıyorsanız, veri depolama klasörünün konumunu değiştirmek için, **Gözet** düğmesine tıklayabilirsiniz.

Yeniden ayarla düğmesine basılması, kullanıcı tanımlı bileşenlerin seçimini iptal eder ve varsayılan seçimleri geri yükler.

Disk kullanım düğmesi, seçilen bileşenlerin yerel sürücüler üzerinde yüklemesi için gerekli olan boş alanın kullanılabilirliği hakkında bilgilerin bulunduğu bir iletişim kutusu açar.

ADIM 5. MICROSOFT SQL SUNUCUSUNA BAĞLANTININ YAPILANDIRILMASI

Bu adımın amacı, bir SQL sunucusuna bir bağlantının yapılandırılmasıdır. Bir SQL sunucu üzerinde veritabanı oluşturmak için, Kaspersky Security'nin kurulacağı bilgisayarın yerel erişim haklarına ve SQL sunucunun yönetici ayrıcalıklarına sahip olmanız gerekecektir. Eğer SQL sunucusu etki alanı denetleyicisi üzerinde çalışıyorsa, Enterprise Admins ve / veya Domain Admins grup üyesi olmanız gerekir. Eğer SQL sunucusuna uzaktan bir bağlantı kullanıyorsanız, TCP/IP desteğin SQL Sunucu Yapılandırma Yöneticisinde etkinleştirildiğinden emin olun.

Microsoft SQL Sunucusuna bağlantının yapılandırılması

SQL sunucunun adı alanında, bilgisayarın adını (veya IP adresini) ve SQL sunucu oluşumunu belirleyin. Bu alanın yanında bulunan **Gözet** düğmesine basılması, mevcut ağ segmenti içindeki bir SQL sunucusu seçmenize olanak sağlar.

SQL sunucu üzerinde bir veritabanı oluşturmak için, SQL veritabanı oluşturmak için kullanılacak olan bir hesabı seçmek zorunda olacaksınız. Aşağıdaki seçenekler mevcuttur:

- **Etkin hesap.** Bu durumda, mevcut kullanıcı hesabı kullanılacaktır.
- **Diğer hesap.** Bu durumda, belirli bir kullanıcı hesabı için isim ve şifre girmelisiniz. Bir hesap seçmek için, **Gözet** düğmesine tıklayın.

SQL server tarayıcısının, SQL sunucusu çalıştıran bilgisayar üzerinde başlatılması gerekir. Aksi takdirde, ihtiyacınız olan SQL sunucunun oluşumunu göremezsiniz. Eğer Kaspersky Security, SQL sunucu bir etki alanı içinde çalışırken Edge Aktarım üzerine yüklendiye, SQL sunucusu bir bağlantı kurmanın hiçbir imkanı olmayacaktır. Bu durumda, yerel bir SQL sunucu oluşumunun kullanılması gerekir.

Uygulama hizmetinin çalışması için, bir hesap seçin.

Bir sonraki pencerede, SQL sunucuya bağlanmak için kullanılacak olan hesabı seçmeniz için bir hatırlatma yapılacaktır. Pencerede, iki seçenek bulunur:

- **Yerel Sistem Hesabı.** Bu durumda, yerel sistem hesabı, SQL sunucuya bağlantı kurmak için kullanılacaktır.
- **Hesap.** Bu durumda, SQL sunucuya bağlanmak amacıyla yeterli ayrıcalıklara sahip hesap için isim ve şifre belirlemeniz ve uygulama hizmetini başlatmanız gerekir.

ADIM 6. DOSYALARIN KOPYALANMASI

Yüklemeye devam etmek için, Kurulum Sihirbazı penceresindeki **Yükle** düğmesine basın. Bu, uygulama dosyalarının bilgisayara kopyalanmasını, bileşenlerin sistem içine kaydedilmesini, SQL sunucu üzerinde ilgili veritabanının oluşturulmasını başlatacak ve Microsoft Exchange Server'ın bazı hizmetlerinin yeniden başlatılmasını sağlayacaktır.

BAŞLARKEN. UYGULAMA YAPILANDIRMA SİHİRBAZI

Dosyalar kopyalandıktan ve bileşenler sisteme kaydedildikten sonra Kurulum Sihirbazı, uygulama yüklemesinin tamamlandığına dair bir bildirim görüntüler. Kurulum Sihirbazında **İleri** düğmesinin tıklanması Uygulama Yapılandırma Sihirbazını başlatacaktır. Uygulama Yapılandırma Sihirbazı, güncelleme ayarlarını yapılandırmada, lisansı yüklemeye ve uygulama işlevselliğini test etmede size yardımcı olacaktır. Uygulama Yapılandırma Sihirbazında, ürün yapılandırmasını başlatmak için **İleri** düğmesine tıklayın.

BU BÖLÜMDE

Güncellemelerin yapılandırılması	17
Lisans anahtarının kurulması	17
Bildirim ayarları	18
Sunucu korumanın yapılandırılması	18
Güvenlik Sunucusuna bağlanması	19
Uygulama işlevselliğinin test edilmesi	19

GÜNCELLEMELERİN YAPILANDIRILMASI

Kaspersky Security'nin güncelleme ayarlarını yapılandırmak için, Uygulama Yapılandırma Sihirbazının **Ayarları** **güncelleştir** penceresini kullanabilirsiniz.

➔ *Güncelleme ayarlarını tanımlamak için aşağıdaki adımları gerçekleştirin:*

1. Uygulamanın belirtilen çizelgeye uygun olarak otomatik güncelleme yapmasını istiyorsanız **Otomatik güncellemeyi etkinleştir** kutusunu işaretli bırakın .
2. Proxy sunucu aracılığıyla Kaspersky Lab güncelleme sunucusuna bağlanmak için **Proxy sunucusu kullan** seçeneğini kullanın ve **Proxy sunucusu adresi** satırına şirket proxy sunucu adresini girin.
3. Giriş alanında proxy sunucusu bağlantı noktasını tanımlayın. Varsayılan olarak **8080** bağlantı noktası kullanılır.
4. Proxy sunucu ile kimlik doğrulamayı etkinleştirmek için, **Kimlik doğrulaması kullan** kutusunu işaretleyin ve **Hesap** ile **Parola** alanlarına seçilen kullanıcı hesabı ile ilgili bilgileri girin.
5. Güncellemeleri doğrudan yerel bir şirket sunucusundan indirmek istiyorsanız, **Yerel adresler için proxy sunucuyu atla** kutusunu işaretleyin.

LİSANS ANAHTARININ KURULMASI

Lisanslar penceresinde Kaspersky Security için bir lisans yükleyebilirsiniz.

➔ *Bir lisans yüklemek için aşağıdaki işlemleri gerçekleştirin:*

1. **Ekle** düğmesine basın.

2. Görüntülenen **Dosya adı** iletişim kutusunda anahtar dosyasına giden yolu belirtin (*.key uzantılı bir dosya) ve **Aç** düğmesine tıklayın.

Belirli bir süre boyunca Kaspersky Security ürününü limitsiz işlevsellik ile kullanmanızı sağlayan bir lisans yüklenecektir. Lisans etkin olduğunda geçerlilik süresinin tamamı boyunca Anti-Virüs ve İstenmeyen Posta veritabanı güncellemelerini indirebilir ve uygulamanın kullanımı ile ilgili tüm konular için Kaspersky Lab ile iletişim kurabilirsiniz.

Bir lisans anahtarının kaldırılması

Bir lisansı kaldırmak için **Kaldır** düğmesine tıklayın.

BİLDİRİM AYARLARI

Bildirim ayarları penceresi, e-posta ile gönderilen bildirimleri yapılandırmanızı sağlar. Bildirimleri kullanarak tüm Kaspersky Security olayları ile ilgili hemen bilgilendirilirsiniz.

► *Bildirim ayarlarını tanımlamak için aşağıdaki adımları gerçekleştirin:*

1. **İnternet hizmet adresi** alanında, iletileri Microsoft Exchange Server aracılığıyla postalamak için kullanılacak internet hizmetinin adresini belirleyin.

Varsayılan olarak Microsoft Exchange Server'da aşağıdaki adres bulunmaktadır:

`https://<client_access_server>/ews/exchange.asmx`

2. **Hesap** alanında, Microsoft Exchange Server üzerinde kaydedilmiş olan posta kutuları arasından bir hesap belirleyin.

Bunun için **Gözet** düğmesine tıklayın veya hesap adını el ile girin.

3. Seçilen hesabın parolasını **Parola** alanına girin.
4. **E-posta adresi** alanında, bildirimi alacak kişinin adresini belirtin.
5. Bir test iletisi göndermek için **Test** düğmesine basın.

Test iletisi belirtilen posta kutusuna ulaşmış ise bu bildirimlerin iletiminin doğru yapılandırıldığı anlamına gelir.

SUNUCU KORUMANIN YAPILANDIRILMASI

Koruma ayarları penceresinde Anti-Virüs ve istenmeyen posta önlemeyi yapılandırabilirsiniz. Anti-Virüs ve istenmeyen posta önleme varsayılan olarak etkinleştirilir.

► *Koruma ayarlarını tanımlamak için aşağıdaki adımları gerçekleştirin:*

1. Anti-Virüsü başlatmak için **Virüsten korunmayı etkinleştir** kutusunu işaretleyin.
2. İstenmeyen posta önlemesini başlatmak için, **İstenmeyen Posta Önlemeyi Etkinleştir** kutusunu işaretleyin.

Anti-Virüs ve istenmeyen posta önlemenin hemen çalışmaya başlamasını istemiyorsanız ilgili kutuların işaretlerini kaldırın. Yönetim konsolunu kullanarak korumayı daha sonra etkinleştirebilirsiniz.

3. Uygulama seçeneklerinin yüklemesini bitirmek için **İleri** düğmesine tıklayın.
4. Sihirbazdan çıkmak için, Uygulama Kurulum Sihirbazının son penceresinde **Bitir** düğmesine tıklayın.

Uygulama Yapılandırma Sihirbazı tamamlandığında Yönetim Konsolunu başlat kutusu işaretli bırakılır ise Yönetim Konsolu otomatik başlar.

GÜVENLİK SUNUCUSUNA BAĞLANILMASI

Kaspersky Security yüklemesinden sonra Yönetim Konsolu otomatik olarak Yerel Güvenlik Sunucusuna bağlanacaktır; Sunucu daha sonra Yönetim Konsolu ağacında görülecektir. Uzak bir bilgisayarda bulunan Güvenlik Sunucusuna bağlanmak için Kaspersky Security hizmetini, uzak bilgisayarın güvenlik duvarının güvenilir uygulamalar listesine eklemelisiniz veya RPC bağlantısına izin vermelisiniz.

► *Başka bir sunucuya bağlanmak için, aşağıdaki adımları gerçekleştirin:*

1. Aşağıdaki öğeleri seçerek Kaspersky Security'yi başlatın: **Başlat** → **Programlar** → **Kaspersky Security 8.0 for Microsoft Exchange Servers** → **Yönetim Konsolu**.
2. Konsol ağacında **Kaspersky Security 8.0 for Microsoft Exchange Servers** düğümünü seçin.
3. Ayrıntılar bölmesinde **Sunucu ekle** düğmesine tıklayın.
4. Görüntülenen pencereden **Diğer bilgisayar** seçeneğini seçin.
5. **Gözet**'a tıklayın ve bağlanmak istediğiniz sunucuyu belirtin.
6. **TAMAM** seçeneğine tıklayın.

Her bağlı sunucu için Kaspersky Security ayarlarını ayrı ayrı yapılandırabilirsiniz.

UYGULAMA İŞLEVSELLİĞİNİN TEST EDİLMESİ

Kaspersky Security yüklendikten ve yapılandırıldıktan sonra bir test "virüsünü" ve değişikliklerini kullanarak ayarlarını ve işletimini doğrulamanız önerilir.

Test "virüsü", Anti-Virüs ürünlerini test etmek için EICAR (Avrupa Bilgisayar Anti-Virüs Araştırmaları Enstitüsü) tarafından özel olarak tasarlanmıştır. Test "virüsü" kötü amaçlı bir program değildir ve bilgisayarınıza zarar verebilecek herhangi bir kod içermez. Bununla birlikte, birçok Anti-Virüs ürünü bunu virüs olarak tanımlar.

Test "virüsünü" EICAR'ın resmi internet sitesinden indirebilirsiniz: http://www.eicar.org/anti_virus_test_file.htm.

Anti-Virüs işlevselliğinin test edilmesi

► *Test "virüsü" ile bir ileti göndermek için, aşağıdaki adımları uygulayın:*

1. Ekli EICAR test "virüsü" ile bir e-posta iletisi yaratın.
2. İletiyi, Kaspersky Security'nin kurulu ve Güvenlik Sunucusunun bağlı olduğu Microsoft Exchange Server aracılığıyla gönderin (bakınız "Güvenlik Sunucusuna Bağlanması" sayfa [19](#)).
3. İletilen iletinin virüs içermediğinden emin olmak için kontrol edin. Posta kutusu olarak çalışan bir sunucuda virüs algılanması durumunda silinen virüs bir metin dosyası ile değiştirilecektir. Hub Aktarımı olarak çalışan bir sunucuda virüs algılandığında uygulama, ileti konusuna `Kötü amaçlı nesne silindi` ön ekini ekler.

Virüs saptandıktan sonra, Başlangıç Yapılandırma Sihirbazının Bildirim Ayarları penceresinde (bakınız "Bildirimlerin yapılandırılması" bölümü sayfa [18](#)) belirttiğiniz posta kutusu, engellenen virüsle ilgili bir bildirim almalıdır.

► *Saptanan virüs ile ilgili uygulama raporunu görüntülemek için, aşağıdaki işlemleri gerçekleştirin:*

1. Aşağıdaki öğeleri seçerek Kaspersky Security'yi başlatın: **Başlat** → **Programlar** → **Kaspersky Security 8.0 for Microsoft Exchange Servers** → **Yönetim Konsolu**.
2. Soldaki konsol ağacında "virüs" içeren iletiyi işlemesi gereken sunucuya karşılık gelen düğümü seçin ve açın.

3. **Raporlar** düğümünü seçin.
4. Sağdaki ayrıntılar bölümünde **Hızlı Raporlar** ve / veya **Anti-Virüs raporu** bölümündeki **Rapor oluştur** ögesine tıklayın.
5. **Hazır raporlar** bölümünde oluşturulan raporu görüntüleyin. Bunun için istenen raporu açmak üzere raporun üzerine çift tıklayın.

Rapor EICAR virüsü ile ilgili bilgi içeriyorsa, uygulama doğru bir şekilde yapılandırılmıştır.

► *Raporları bir e-posta adresine almak için aşağıdaki işlemleri gerçekleştirin:*

1. **Hızlı raporlar** ve / veya **Virüsten korunma raporu** bölümlerindeki ayrıntılar bölümünde, Uygulama Yapılandırma Sihirbazının Bildirim Ayarları penceresinde belirtmiş olduğunuz adrese bildirim göndermeyi etkinleştirmek için, **Yönetici** kutusunu işaretleyin (bakınız "Bildirimlerin yapılandırılması" bölümü sayfa [18](#)).

Eğer Başlangıç Yapılandırma Sihirbazında bir e-posta belirlemediyseniz, bildirimleri ayarlamak için **E-posta gönderme ayarları** bağlantısına tıklayın (bakınız "Bildirimlerin yapılandırılması" bölümü sayfa [18](#)).

2. Raporların belirtilen posta kutusuna ulaştığından emin olmak için bir test iletisi göndermek amacıyla **Test** düğmesine tıklayın.


Uygulama varsayılan olarak Yedekte virüslü nesnenin bir kopyasını kaydeder.

► *Etkilenmiş bir nesnenin Yedekte kaydedilip kaydedilmediğini kontrol etmek için aşağıdaki işlemleri gerçekleştirin:*

1. Konsol ağacında **Yedek** düğümünü seçin.
2. Etkilenmiş nesnenin (ekte "virüslü" iletisi) ayrıntılar bölümünde görüldüğünden emin olmak için kontrol edin.

İstenmeyen Posta işlevselliğinin test edilmesi

► *İstenmeyen Posta bileşeninin normal işlevselliğini test etmek için aşağıdaki adımları uygulayın:*

1. **Başlat** → **Programlar** → **Kaspersky Security 8.0 for Microsoft Exchange Servers** → **Yönetim Konsolu** ögesini seçerek Kaspersky Security'yi başlatın.
2. Soldaki konsol ağacında test iletisini aktarmak için kullanılacak sunucuya karşılık gelen düğümü seçin ve açın.
3. **Sunucu koruması** düğümünü seçin.
4. Ayrıntılar bölümündeki **İstenmeyen posta önleme** sekmesini seçin.
5. **Beyaz ve kara liste ayarları** bölümünü açın.
6. **Gönderenin adresini kara listeye ekle** kutusunu işaretleyin.
7. Gönderenin e-posta adresini giriş satırına yazın.
8. Alanın sağındaki ekleme düğmesine  tıklayın.
9. **Tarama ayarları** bölümünü açın.
10. **Kara listede** alanında **İzin ver** seçeneğini seçin
11. Aynı alanda **Etiket ekle** kutusunu işaretleyin.
12. Korunan posta sunucusu aracılığıyla yöneticinin adresine bir iletisi gönderin.

İleti, başlığında **[Kara listede]** etiketi ile gelir ise, **İstenmeyen Posta** bileşeni doğru çalışmaktadır.

UYGULAMANIN YENİDEN YÜKLENMESİ

Uygulamanın çalışırken bir hata ile karşılaşması durumunda (örneğin, ikili modüllerinin zarar görmesi) yükleyicide verilen yeniden yükleme işlevselliğini kullanabilirsiniz. Yeniden yükleme sırasında yükleyici, seçilen ayarları ve bildirimler, Karantina veritabanına giden yollar vb.dâhil olmak üzere kullanıcı yapılandırmasını saklayacaktır.

◆ *Kaspersky Security'yi geri yüklemek için aşağıdaki işlemleri gerçekleştirin:*

1. setup_en.exe dosyasını başlatın.
2. **Kaspersky Security 8.0 for Microsoft Exchange Servers** bağlantısına tıklayın.
3. Başlangıç Kurulum Sihirbazının karşılama ekranında **İleri** düğmesine tıklayın.
4. **Uygulamayı değiştir, geri yükleme veya Kaldır** penceresinde **Geri yükle** düğmesine tıklayın.
5. **Geri yükleniyor** penceresinde, **Onar** düğmesine tıklayın.

Yapılandırma dosyaları hasarlı ise, uygulama yeniden yüklenemez. Bu durumda, uygulamanın kaldırılması ve yeniden kurulması tavsiye edilir.

UYGULAMANIN KALDIRILMASI

➔ *Kaspersky Security'yi bilgisayardan kaldırmak için aşağıdaki işlemleri gerçekleştirin:*

1. setup_en.exe dosyasını başlatın.
2. Kurulum Sihirbazını başlatmak için **Kaspersky Security 8.0 for Microsoft Exchange Servers** bağlantısına tıklayın ve daha sonra **İleri** ögesine tıklayın.
3. **Uygulamayı değiştir, geri yükleme veya Kaldır** penceresinde **Kaldır** düğmesine tıklayın.
4. **Kaldır** penceresinde **Kaldır** düğmesine tıklayın.

Ayrıca Microsoft Windows'ta standart yazılım yönetim araçlarını kullanarak uygulamayı kaldırabilirsiniz.

Kaspersky Security'nin kaldırılması sırasında Microsoft Exchange Server'ın bazı hizmetlerinin yeniden başlatılması gerekebilir.