

# **McAfee Total Protection Service Kurulum Kılavuzu**

## TELİF HAKKI

Copyright © 2009 McAfee, Inc. Tüm hakları saklıdır.

Bu yayının hiç bir bölümü, McAfee, Inc. veya tedarikçileri veya iştiraklerinin yazılı izni olmadan hiç bir şekilde ve hiç bir yöntemle çoğaltılamaz, iletilemez, kopyalanamaz, bir erişim sisteminde depolanamaz veya herhangi bir dile tercüme edilemez.

## TİCARİ MARKA ÖZELLİKLERİ

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFFEE SECURITYALLIANCE EXCHANGE), MCAFFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN ve WEBSHIELD McAfee, Inc. ve ABD ve/veya diğer ülkelerdeki iştiraklerinin ticari markaları veya tescilli markalarıdır. McAfee'nin güvenlikle ilgili olarak kullandığı Kırmızı renk, McAfee markalı ürünlere özeldir. Burada yer alan tüm diğer tescilli ve tescilsiz ticari markalar kendi sahiplerine aittir.

## LİSANS BİLGİLERİ

### Lisans sözleşmesi

TÜM KULLANICILARIN DİKKATİNE: SATIN ALMIŞ OLDUĞUNUZ LİSANSIN, LİSANSLI YAZILIMIN KULLANIMINA İLİŞKİN GENEL ŞART VE KOŞULARI İÇEREN YASAL SÖZLEŞMESİNİ DİKKATLİCE OKUYUN. HANGİ LİSANS TÜRÜNÜ SATIN ALDIĞINIZI BİLMİYORSANIZ, YAZILIM PAKETİNİZLE BİRLİKTE VERİLEN VEYA SATIN ALMA İŞLEMİNİN BİR PARÇASI OLARAK AYRICA ALDIĞINIZ (BİR KİTAPÇIK, ÜRÜN CD'SİNDE BİR DOSYA VEYA YAZILIM PAKETİNİ İNDİRDİĞİNİZ WEB SİTESİNDE BULUNAN BİR DOSYA) SATIŞ, LİSANS VEYA SATIN ALMA SİPARİŞİ BELGELERİNE BAKINIZ. SÖZLEŞMEDE YER ALAN TÜM KOŞULLARI KABUL ETMİYORSANIZ, YAZILIMI YÜKLEMİYİN. MÜMKÜN OLMASI HALİNDE ÜRÜNÜ MCAFFEE'YE VEYA SATIN ALDIĞINIZ YERE İADE EDEBİLİRSİNİZ.

### Lisans özellikleri

Ürün sürüm notlarına bakınız.

# İçindekiler

<b>Total Protection Service'a Giriş</b> .....	<b>5</b>
Sipariş verdikten sonra .....	5
Birden çok siparişi veya hesabı birleştirme .....	5
Kurulum ortamı .....	6
Desteklenen işletim sistemleri .....	6
RAM gereksinimleri .....	8
E-posta koruması gereksinimleri .....	9
E-posta sunucusu koruması gereksinimleri .....	9
Gelişmiş ağ ortamları .....	10
Aktarma sunucuları kurulup kurulmayacağına karar verme .....	11
Güvenlik duvarı koruması Windows güvenlik duvarı ile nasıl etkileşir .....	11
Kurumsal güvenlik duvarı veya proxy sunucuları için destek .....	12
Terminal sunucu desteği .....	12
<b>İstemci Yazılımını Kurmaya Hazırlanma</b> .....	<b>13</b>
Etkin virüs koruma yazılımını kaldırma .....	13
Etkin güvenlik duvarı yazılımını kaldırma .....	13
Tarayıcınızı yapılandırma .....	14
Tek başına kurulum ajanını kurma .....	14
<b>Total Protection Service'ı Kurma</b> .....	<b>16</b>
Kurulum yöntemlerinin özeti .....	16
Standart kurulum işlemi .....	17
Standart kurulum gereksinimleri .....	17
Kullanıcılara kurulum URL'si gönderme .....	17
URL ile kurma .....	18
Sessiz kurulum işlemi .....	18
Sessiz kurulum gereksinimleri .....	19
Sessiz kurulum ile kurma .....	19
VSSETUP ile aktarma sunucusu atama .....	20
VSSETUP parametreleri .....	20
Zorla yükleme işlemi .....	21
Zorla yüklemeleri zamanlarken dikkat edilecek konular .....	23

Zorla yükleme gereksinimleri. ....	24
Yönetim bilgisayarını hazırlama. ....	24
Zorla yükleme ile kurma. ....	25
Push Install yardımcı programını kaldırma. ....	26
Önceden kurulmuş sürümler ve CD sürümleri için işlemler. ....	26
Önceden kurulmuş deneme sürümü ve tam abonelikler. ....	27
Bilgisayarı ilk açtığınızda. ....	27
Total Protection Service kopyasını etkinleştirme. ....	27
Tam abonelik satın alma veya yenileme. ....	28
Hesap kayıt anahtarını görüntüleme veya oluşturma. ....	28
Kurulumdan sonra lisans anahtarınızı etkinleştirme. ....	29
Kurulumu tamamlama. ....	29
Virüs korumasını test etme. ....	29
İstemci bilgisayarını tarama. ....	30
E-posta Gelen Kutusunu tarama. ....	30
<b>Sorun giderme ve destek. ....</b>	<b>31</b>
Sık sorulan sorular. ....	31
Kurulum hakkında sorular. ....	31
Önceden kurulmuş sürümler veya CD sürümleri hakkında sorular. ....	32
Hata iletileri. ....	33
Kurulumdaki hata iletileri. ....	33
Önceden kurulmuş sürümler ve CD sürümleri için hata iletileri. ....	36
Ürün destek hizmetlerine başvurma. ....	36

# Total Protection Service'a Giriş

Bu kılavuz, istemci bilgisayarlarda McAfee® Total Protection Service yazılımını kurmaya hazırlanmak ve kurmak için gerekli bilgileri içerir.

**NOT:** Total Protection Service tarafından yönetilen bazı koruma türleri istemci bilgisayarlarda yazılım olarak bulunmaz. Satın aldığınız ürün e-posta koruması veya e-posta sunucusu koruması içeriyorsa, sistem gereksinimleri bu kılavuza eklenmiştir, ancak bunları kurma yönergeleri için McAfee e-postalarına ve malzemelerine başvurmanız gerekir.

## İçindekiler

- ▶ Sipariş verdikten sonra
- ▶ Kurulum ortamı
- ▶ Gelişmiş ağ ortamları

## Sipariş verdikten sonra

Total Protection Service siparişi verdiğinizde, bir e-posta adresi verirsiniz ve hesabınız o e-posta adresiyle ilişkilendirilir. Siparişinizi verdikten sonra:

- 1 McAfee siparişinizi işler.
- 2 Üç e-posta alırsınız.

Bu e-postada...	Şu vardır...
Hoş geldiniz	Yükleme URL'si ile istemci yazılımı kurma, satın aldığınız korumayı etkinleştirip ayarlama, belgelere erişme ve müşteri destek hizmetlerine ulaşma yönergeleri.
Oturum açma kimlik bilgileri	McAfee SecurityCenter yönetim Web sitesinde oturum açmak ve parolanızı değiştirmek için yönergeler. SecurityCenter sayfasına erişmek için Microsoft Internet Explorer (sürüm 6.0 veya üzeri) ya da Mozilla Firefox (sürüm 2.0 veya üzeri) kullanmanız gerekir.
Lisans mektubu	Müşteri desteği için gerekli olan, siparişin lisans numarası.

**NOT:** Güvenliği sizin yerinize yöneten bir McAfee ortağından Total Protection Service satın alırsanız, bu e-postaları genellikle o ortak alır. Hangi e-postaları almanız gerektiği hakkında sorularınız varsa, ortak ile bağlantı kurun.

## Birden çok siparişi veya hesabı birleştirme

Farklı e-posta adreslerini kullanarak birden çok sipariş verdiyseniz, birden çok Total Protection Service hesabınız vardır.

Tüm güvenlik bilgilerinizin ve e-postalarınızın tek bir e-posta adresine gönderilebilmesi amacıyla ayrı hesapları birleştirmek için bu görevi kullanın.

## Görev

Seçenek tanımları için, arabirimde ? işaretini tıklatın.

- 1 Web tarayıcınızdan, SecurityCenter oturumunu açın. Oturum açma kimlik bilgileri, Total Protection Service ürününü satın aldığınız zaman Hoş Geldiniz e-postasında size gönderilmiştir.  
**NOT:** SecurityCenter sayfasında oturum açmak için Internet Explorer (sürüm 6.0 veya üzeri) ya da Firefox (sürüm 2.0 veya üzeri) kullanmanız gerekir.
- 2 Hesabım sayfasında, **Hesaplar ve Anahtarlar** sekmesini tıklatın.
- 3 Hesapları Yönet bölümünde, **Başka bir hesapla birleştir**'i seçin.
- 4 Ana hesabınızla birleştirmek istediğiniz hesabın e-posta adresini ve parolasını girin, sonra **İleri**'yi tıklatın. Ana hesap, tüm aboneliklerinizle ilgili durum e-postalarını ve iletilerini almak istediğiniz e-posta adresini kullanan hesaptır.
- 5 Hesap için listelenen lisansların ve bilgisayarların birleştirmek istedikleriniz olduğunu doğrulayın.
- 6 **Hesabı Birleştir**'i tıklatın.

## Kurulum ortamı

Total Protection Service, PC platformunda çalışan Microsoft Windows işletim sistemleri için tasarlanmıştır. İstemci yazılımı şu donanıma sahip bilgisayarlara kurulum ve çalıştırılır:

- Intel Pentium işlemci veya uyumlu bir mimari.
- Microsoft Internet Explorer 6.0 veya daha ileri sürümü.

Ek gereksinimler ve destek yönergeleri için şu konuları inceleyin:

- *Desteklenen işletim sistemleri*
- *RAM gereksinimleri*
- *E-posta koruması gereksinimleri*
- *E-posta sunucusu koruması gereksinimleri*

## Desteklenen işletim sistemleri

İstemci bilgisayarların desteklenen işletim sistemlerini çalıştırdığını doğrulamak için bu tabloyu kullanın. Bu tablo, yalnızca istemci bileşeninin kurulmasını gerektiren koruma türlerini içerir.

İşletim sistemi	Koruma		
	Virüs ve casus yazılım, güvenlik duvarı	Tarayıcı	İçerik filtreleme
<b>İstemci bilgisayarlar</b>			
Windows 2000 Professional Service Pack 3 veya daha ileri sürümü	X		
Windows XP Home Windows XP Professional Service Pack 2 veya daha ileri sürümü (32 bit ve 64 bit)	X	X	X

İşletim sistemi	Koruma		
	Virüs ve casus yazılım, güvenlik duvarı	Tarayıcı	İçerik filtreleme
Windows Vista (32 bit ve 64 bit)	X	X	X
Windows 7 (32 bit ve 64 bit)	X	X	X
<b>Sunucular</b>			
Windows 2000 Server Advanced Server Small Business Server Service Pack 3 veya daha ileri sürümü	X		
Windows 2003 Standard Server Enterprise Server Small Business Server (32 bit ve 64 bit)	X	X	X
Windows Server 2008 Standard Server Enterprise Server Small Business Server Essential Business Server (32 bit ve 64 bit)	X	X	X

### İşletim sistemini yükseltirken

İstemci bilgisayardaki işletim sistemini yükseltiyorsanız (örneğin, Windows 2000'den Windows XP'ye) ve yükseltme işlemi sırasında varolan dosya ve programlarınızı olduğu gibi korumak istiyorsanız, önce Total Protection Service ürününü kaldırmanız gerekir. Yükseltme tamamlandıktan sonra yeniden kurabilirsiniz.

## Windows Home Server Desteği

Total Protection Service istemci yazılımının farklı bir sürümü, Microsoft Windows Home Server çalıştıran bilgisayarlar için geliştirilmektedir. Windows Home Server yazılımını çalıştıran yöneticilerin, Total Protection Service istemci yazılımının Windows Home Server konsolu ile etkileşmesine izin verecek olan bu sürümü yüklemek için SecurityCenter erişimleri olacaktır. İki Total Protection Service sürümü arasındaki farklara lütfen dikkat edin:

- Windows Home Server konsoluyla etkileşim kurabilmek için, Windows Home Server çalıştıran bilgisayarlara kurulum bu kılavuzda açıklanandan farklı bir kurulum programı gerektirir.
- Kurulum programını SecurityCenter üzerindeki Yardımcı Programlar sayfasından yükleyin (program kullanılabilir olduğunda).
- Windows Home Server'in istemci yazılımı yalnızca virüs ve casus yazılımdan korunmayı destekler.
- Windows Home Server ürününe özel kurulum işlemini ve özellikleri açıklayan ayrı bir ürün kılavuzu, SecurityCenter üzerindeki Yardım sayfası aracılığıyla kullanıma sunulacaktır.

- Bu kılavuzda açıklanan kurulum yöntemleri, Windows Home Server çalıştıran bir bilgisayardaki istemci yazılımının desteklenen kurulum yöntemleri değildir.

## İşletim sistemi desteğinin sona ermesi

Windows 2000 işletim sistemi desteği sona ermek üzere zamanlanmıştır.

Total Protection Service çalıştıran bilgisayarlar varolan tehditlerden korunmaya devam ederler, ancak ürün güncellemelerini ve en son tehditlere karşı korumayla güncellenen DAT dosyalarını almazlar.

Windows 2000 desteği hakkında daha fazla bilgi için, şu adresi ziyaret edin:

[http://www.mcafee.com/us/small/support/customer\\_service/end\\_life.html](http://www.mcafee.com/us/small/support/customer_service/end_life.html)

## Desteğin ne zaman sona ereceğini kullanıcılara bildirme

Varsayılan olarak, Total Protection Service, kullanıcılara işletim sistemleriyle ilgili desteğin sona ermekte olduğunu anımsatmak için, istemci bilgisayarlarda bildirimler görüntüler. Bildirimler şu zaman görünür:

- Tarama motoru gibi ürün bileşenlerinin yükseltmeleri belirli bir tarihte veya 30 gün içinde sona erecek şekilde zamanlandığında.
- Algılama tanım (DAT) dosyalarının güncellemeleri sona erdiğinde veya 30 gün içinde sona ereceği zaman.

Destek bildirimlerinin görüntülenip görüntülenmeyeceğini bir ilke seçeneği belirler. Ancak bildirimler, desteğin önceden sona ermiş olduğu Windows sürümlerini çalıştıran bilgisayarlar için görüntülenmez.

Otomatik bildirimleri etkinleştirmek veya devre dışı bırakmak için bu görevi kullanın.

### Görev

Seçenek tanımları için, arabirimde ? işaretini tıklatın.

- Web tarayıcınızdan, SecurityCenter oturumunu açın. Oturum açma kimlik bilgileri, Total Protection Service ürününü satın aldığınız zaman Hoş Geldiniz e-postasında size gönderilmiştir.
- İlkeler sayfasında, yeni ilke oluşturmak için **İlke Ekle**'yi tıklatın veya varolan bir ilkeyi değiştirmek için **Düzenle**'yi tıklatın.
- İstemci Ayarları sekmesinde, **İstemci bilgisayarlarda destek bildirimleri göster**'i seçin veya seçimini kaldırın.
- Kaydet**'i tıklatın.

## RAM gereksinimleri

Total Protection Service kurmadan önce, istemci bilgisayarlara yeterli RAM takıldığından emin olmak için bu tabloyu kullanın.

İşletim sistemi	Tek koruma türü için minimum	Birden çok koruma türü için minimum	Önerilen
Windows 2000	512 MB	1 GB	1 GB
Windows XP	512 MB	1 GB	1 GB
Windows 2003	512 MB	1 GB	2 GB

İşletim sistemi	Tek koruma türü için minimum	Birden çok koruma türü için minimum	Önerilen
Windows Vista	1 GB	1 GB	2 GB
Windows 7	1 GB	1 GB	2 GB
Windows Server 2008	512 MB	1 GB	2 GB
Diğer Sunucular	512 MB	1 GB	2 GB

**NOT:** Gereken toplam RAM'i hesaplarken, istemci bilgisayarlarda çalışan diğer yazılım uygulamalarının bellek gereksinimlerini dikkate alın.

## E-posta koruması gereksinimleri

Aboneliğiniz e-posta koruması içeriyorsa, e-posta korumasını kurup çalıştırmak için ağınızın bu gereksinimleri karşıladığından emin olun:

- Kendi yerinizde veya ISS tarafından barındırılan özel bir e-posta sunucusu.
- Statik IP adresi olan bir e-posta etki alanı, örneğin etkialaniniz.com.

E-posta korumasını kurma yönergeleri McAfee'den gönderilen bir e-postada ve ürün kılavuzunda sağlanır, SecurityCenter üzerindeki Yardım sayfasından da bulunabilir.

## E-posta sunucusu koruması gereksinimleri

Aboneliğiniz e-posta sunucusu koruması içeriyorsa, e-posta sunucunuzun minimum gereksinimleri karşılayıp karşılamadığını doğrulamak için bu listeleri denetleyin. E-posta sunucusu korumasını kurma yönergeleri McAfee'den gönderilen e-postalarda ve malzemelerde sağlanır.

### Exchange İçin McAfee Security Service

Desteklenen Bileşen	Gereksinim
İşletim Sistemi	<ul style="list-style-type: none"><li>• Microsoft Windows 2000 Advanced Server Service Pack 4</li><li>• Microsoft Windows 2003 Standard/Enterprise Server (32 bit ve 64 bit)</li><li>• Microsoft Windows 2003 Standard/Enterprise Server R2 (32 bit)</li><li>• Microsoft Windows 2003 Small Business Server (32 bit)</li><li>• Microsoft Windows 2003 Datacenter Server (32 bit ve 64 bit)</li><li>• Microsoft Windows 2008 Standard/Enterprise Server (64 bit)</li><li>• Microsoft Windows 2008 Datacenter Server (64 bit)</li></ul>
Exchange Server	<ul style="list-style-type: none"><li>• Microsoft Exchange Server 2003 Service Pack 2</li><li>• Microsoft Exchange Server 2007</li></ul>
Tarayıcı	<ul style="list-style-type: none"><li>• Microsoft Internet Explorer 6.0 ve 7.0</li><li>• Mozilla Firefox 2.0 veya daha ileri sürümü</li></ul>

Desteklenen Bileşen	Gereksinim
	<ul style="list-style-type: none"><li>Netscape Navigator 9.0</li></ul>
İşlemci	<ul style="list-style-type: none"><li>Intel x86 mimarisi tabanlı işlemci (yalnızca Exchange Server 2003'te)</li><li>Intel Extended Memory 64 Teknolojisini destekleyen (Intel EM64T) Intel x64 mimarisi tabanlı işlemci</li><li>AMD x64 mimarisi tabanlı işlemci, AMD 64 bit teknolojili</li></ul>
Bellek	En düşük: 1 GB RAM (Önerilen: 2 GB RAM)
Disk alanı	En düşük: 740 MB
Ağ	10/100/1000Mbps Ethernet kartı
Ekran	1024 x 768

### McAfee GroupShield® for Lotus Domino, Windows sürümü

Desteklenen Bileşen	Gereksinim
İşletim Sistemi	<ul style="list-style-type: none"><li>Microsoft Windows 2000 Advanced Server Service Pack 4 veya daha ileri sürümü</li><li>Microsoft Windows 2003 Server (32 bit)</li><li>Microsoft Windows 2003 Enterprise Server Service Pack 2 veya daha ileri sürümü (32 bit).</li></ul>
Tarayıcı	Internet Explorer 6.x
İşlemci	Intel Pentium veya üzeri ve uyumlusu
Bellek	En düşük: 512 MB RAM (Önerilen: 1 GB RAM)
Disk alanı	En düşük: Bölüm başına 1 GB (Önerilen: bölüm başına en az 1,5 GB)
Disk takas alanı	Kullanılabilir fiziksel RAM'in iki katı
Lotus Domino	<ul style="list-style-type: none"><li>Lotus Domino sürüm 6.0.2</li><li>Lotus Domino sürüm 7.0.2</li><li>Lotus Domino sürüm 8.0</li></ul>
Ekran	1024 x 768 veya üzeri

## Gelişmiş ağ ortamları

Belirli özelliklere sahip ağlara Total Protection Service kurmadan önce birkaç konunun dikkate alınması uygun olabilir.

Ağınızda bu varsa...	Bu konuyu inceleyin
İnternet bağlantısı olmayan bir veya daha fazla bilgisayar	<i>Aktarma sunucuları kurulup kurulmayacağına karar verme</i>
Windows güvenlik duvarı çalıştıran bilgisayarlar	<i>Güvenlik duvarı koruması Windows güvenlik duvarı ile nasıl etkileşir</i>

Ağınızda bu varsa...	Bu konuyu inceleyin
Kurumsal güvenlik duvarı veya proxy sunucusu	<i>Kurumsal güvenlik duvarı veya proxy sunucuları için destek</i>
Hızlı kullanıcı değiştirme özelliğinin kullanıldığı terminal sunucular veya paylaşılan bilgisayarlar	<i>Terminal sunucu desteği</i>

## Aktarma sunucuları kurulup kurulmayacağına karar verme

Total Protection Service kurmadan önce, aktarma sunucuları kurmak isteyip istemediğinize ve hangi bilgisayarların aktarma sunucusu olacağına karar verin. Bu karar, bu bilgisayarlar için hangi kurulum yöntemlerini kullanabileceğinizi etkiler.

### Aktarma sunucuları ne zaman kurulmalı

Aktarma sunucularının kurulması gerekli değildir. Ancak, ağınızda Internet'e doğrudan bağlantısı olmayan bilgisayarlar varsa, bir veya daha fazla bilgisayarı aktarma sunucusu olarak atamayı düşünebilirsiniz.

### Aktarma sunucusu nedir?

Internet Bağımsız Güncelleme (IIU) özelliği, Internet bağlantısı olmayan kullanıcıların aktarma sunucusu olarak atanmış başka bir yerel bilgisayar aracılığıyla yazılım güncellemeleri almasını sağlar. Internet bağlantısı olan her bilgisayar, istemci yazılım kurulduğu sırada veya daha sonra aktarma sunucusu olarak ayarlanabilir. Aktarma sunucusu, diğer bilgisayarların güncellemeleri denetlemek için kendi bağlantısını kullanmasına izin vererek onlar için bir proxy işlevi görür.

### Aktarma sunucuları nasıl kurulur

Aktarma sunucularını aşağıdaki yöntemleri kullanarak belirtin:

- Sessiz kurulum — Aktarma sunucusunu kurulum sırasında belirtin veya bir istemci bilgisayarı aktarma sunucusu olarak istediğiniz zaman yeniden yapılandırmak için VSSETUP'ı çalıştırın.
- Zorla yükleme — Aktarma sunucusu olarak hizmet verecek bilgisayarlara ve aktarma sunucusu olmayacak bilgisayarlara dosyaları zorla yüklemek için ayrı ayrı zorla yükleme işlemi gerçekleştirin.

## Güvenlik duvarı koruması Windows güvenlik duvarı ile nasıl etkileşir

Ağınızdaki istemci bilgisayarlar Windows güvenlik duvarı çalıştırıyorsa ve Total Protection Service ile güvenlik duvarı koruması kurmayı planlıyorsanız, bu iki güvenlik duvarının nasıl etkileşeceği konusunda dikkatli olmanız gerekir.

Windows XP, Windows Vista veya Windows 7 çalıştıran bilgisayarlarda tam koruma sağlamak için, güvenlik duvarı koruması otomatik olarak Windows güvenlik duvarını devre dışı bırakır ve kendisini varsayılan güvenlik duvarı olarak yapılandırır. Bu sayede raporlama amacıyla Internet uygulamalarının iletişimlerini ve olayları izleyebilir.

Total Protection Service güvenlik duvarı etkinken Windows güvenlik duvarını yeniden etkinleştirmemeniz önerilir.

**DİKKAT:** İki güvenlik duvarı da etkin olduğunda, Total Protection Service güvenlik duvarı, Güvenlik Duvarı Tarafından Engellenen Gelen Olaylar raporunda engellenen IP adreslerinin yalnızca bir alt kümesini listeler. Windows güvenlik duvarı bu adreslerin bir bölümünü engeller; ancak, Windows güvenlik duvarında olay günlüğü kaydı varsayılan olarak devre dışı bırakıldığı

için bunları raporlamaz. Her iki güvenlik duvarı da etkin olduğunda, engellenen tüm IP adreslerinin listesini görebilmek için Windows güvenlik duvarı günlüğünü etkinleştirmeniz gerekir. Varsayılan Windows güvenlik duvarı günlüğü C:\Windows\pfirewall.log'dur. İki güvenlik duvarını da etkinleştirmek aynı zamanda çifte durum ve uyarı iletileri oluşmasına yol açar.

## Kurumsal güvenlik duvarı veya proxy sunucuları için destek

Total Protection Service, bileşenleri doğrudan McAfee sunucularından istemci bilgisayarlara yükler. Kurumsal güvenlik duvarı arkasındaysanız veya Internet'e proxy sunucu üzerinden bağlıysanız, hizmetinizin düzgün çalışması için ek bilgiler sağlamanız gerekebilir.

- Kimlik doğrulama desteği anonim kimlik doğrulama ile veya Windows etki alanı sınama/yanıt kimlik doğrulamasıyla sınırlıdır. Temel kimlik doğrulaması desteklenmez.
- Sessiz kurulum, zorla yükleme ve otomatik güncelleme CHAP veya NTLM proxy'sini desteklemez.

Total Protection Service kurulumu veya güncellemesi yaparken proxy sorularınız varsa, ürün destek hizmetlerine başvurun.

## Terminal sunucu desteği

Total Protection Service, çoğu durumda terminal sunucuları ve Windows hızlı kullanıcı değiştirme özelliğini şu sınırlamalarla destekler:

- Total Protection Service, sunucuya yerel yönetici hakları olan birisi tarafından yüklenmiş olmalıdır.
- Terminal sunucuda bir kurulum veya güncelleme gerçekleştiğinde, otomatik güncellemelere uygulanan kısıtlamalar için bir oturum birincil güncelleme oturumu olarak atanır.
- Tüm kullanıcı oturumlarında, kurulum veya güncelleme sırasında Total Protection Service simgesi sistem tepsisinden kaldırılır. Bu simge yalnızca birincil güncelleme oturumunda oturum açmış olan kullanıcı için yeniden başlatılır. Tüm kullanıcı oturumları korunur ve diğer kullanıcılar simgelerini el ile yeniden görüntüleyebilirler. (Simgeyi görüntüleme yönergeleri için ürün kılavuzuna veya istemci çevrimiçi yardımına bakın.)
- Hızlı kullanıcı değiştirme özelliği etkinleştirilmişse, algılama bildirimleri tüm bilgisayar kullanıcılarının masaüstünde görüntülenmez.

# İstemci Yazılımını Kurmaya Hazırlanma

Bu bölüm, istemci yazılımları kurmadan önce ağınızdaki bilgisayarları hazırlamayı açıklamaktadır.

## İçindekiler

- ▶ Etkin virüs koruma yazılımını kaldırma
- ▶ Etkin güvenlik duvarı yazılımını kaldırma
- ▶ Tarayıcınızı yapılandırma
- ▶ Tek başına kurulum ajanını kurma

## Etkin virüs koruma yazılımını kaldırma

Diğer virüs koruma yazılımları McAfee virüs korumasının gelişmiş özellikleriyle çakışabilir. Birden çok virüs tarama motoru bilgisayarınızdaki aynı dosyalara erişmeyi denediğinde, birbirleriyle etkileşirler. Total Protection Service virüs ve casus yazılım korumasını kurmadan önce varolan virüs koruma yazılımını kaldırmak için bu görevi kullanın. (Varolan bir Total Protection Service kurulumunun kaldırılması gerekmez.)

Total Protection Service, bazı virüs koruma yazılımlarını kurulum sırasında otomatik olarak algılar. Bu ürünlerin bazılarını kurulum sırasında kaldırabilir ve diğer ürünleri de sizden el ile kaldırmanız ister. Kurulum sırasında bir bilgisayarda virüs koruma yazılımı olduğundan bilgilendirilirsenez, Total Protection Service kurmadan önce onu kaldırmalısınız.

Kurulum sırasında algılanan ve/veya kaldırılan yazılımların listesi için, [http://www.mcafeesap.com/downloads/uninstallinfo/detected\\_software\\_list.html](http://www.mcafeesap.com/downloads/uninstallinfo/detected_software_list.html) adresini ziyaret edin.

### Görev

- 1 Windows Denetim Masası'nda, **Program Ekle/Kaldır**'ı açın.
- 2 Program listesinden virüs koruma yazılımlarını bulun.
- 3 **Kaldır**'ı tıklayın.

## Etkin güvenlik duvarı yazılımını kaldırma

Güvenlik duvarı koruması kurmadan önce, diğer tüm güvenlik duvarı programlarını bilgisayarınızdan kaldırmanız önerilir. (Varolan bir Total Protection Service kurulumunun kaldırılması gerekmez.) Kaldırmak için güvenlik duvarı programınızın yönergelerini izleyin veya Windows Denetim Masası'nı kullanın.

Varolan güvenlik duvarı yazılımını Windows Denetim Masası'ndan kaldırmak için bu görevi kullanın.

### Görev

- 1 Windows Denetim Masası'nda, **Program Ekle/Kaldır**'ı açın.
- 2 Program listesinden güvenlik duvarı yazılımlarını bulun.
- 3 **Kaldır**'ı tıkklatın.

**NOT:** Windows güvenlik duvarı çalıştıran bilgisayarlarda, Total Protection Service kurulumu sırasında güvenlik duvarı otomatik olarak devre dışı bırakılır.

## Tarayıcınızı yapılandırma

Total Protection Service kurmak için kullanılan bilgisayarda Microsoft Internet Explorer 6.0 veya daha ileri sürümünün yüklü olması gerekir. Total Protection Service, Internet Explorer'da varsayılan güvenlik ayarlarıyla çalışır. Ayarlarınızdan emin değilseniz, onları doğrulayıp yapılandırmak için bu görevi kullanın.

**NOT:** Yönetim bilgisayarlarınızda veya istemci bilgisayarlarınızda genellikle Mozilla Firefox veya Opera gibi Microsoft olmayan bir tarayıcı kullanıyorsanız, Total Protection Service kurmadan önce Internet Explorer'ı kurmalısınız. Yazılım kurulduktan sonra, varsayılan Internet tarayıcınızı kullanmaya devam edebilirsiniz. Internet Explorer (sürüm 6.0 veya üzeri) ya da Firefox (sürüm 2.0 veya üzeri) ile SecurityCenter sayfasına erişebilirsiniz.

### Görev

- 1 Windows Denetim Masası'ndan, **İnternet Seçenekleri**'ni açın.
- 2 Güvenlik sekmesinde, Internet Explorer sürümünüze bağlı olarak güvenlik ayarlarınızı doğrulayın veya gerektiği şekilde değiştirin:
  - Internet Explorer 7.x — **Orta-yüksek**'i seçin.
  - Internet Explorer 6.x — **Özel Düzey**'i seçin, sonra **Özel ayarları sıfırla** alanında, **Orta**'yı seçin ve **Sıfırla** düğmesini tıkklatın.
- 3 **Tamam**'ı tıkklatın.

## Tek başına kurulum ajanını kurma

Yönetici hakları olmayan kullanıcıların URL yöntemini kullanarak istemci bilgisayarlara Total Protection Service kurmalarına izin vermek için, önce onların istemci bilgisayarına tek başına kurulum ajanı yüklemeniz gerekir.

**NOT:** Yönetici hakları olmayan kullanıcıların istemci yazılımları kurmasını istemediğiniz sürece, bu görev gerekli değildir.

Kurulum ajanını Microsoft Systems Management Server (SMS) yükleyicisi, Windows NT oturum komut dosyaları veya Tivoli IT Director gibi bir kuruluş aracını kullanarak ya da doğrudan istemci bilgisayarlara yükleyerek kurmak için, bu görevi kullanın. Bu dosyayı kurmak için istemci bilgisayarda yönetici haklarınızın olması gerekir. İstemci bilgisayara tek başına kurulum ajanı kurulduktan sonra, herhangi bir kullanıcı o bilgisayara Total Protection Service istemci yazılımını kurabilir.

## Görev

- 1 SecurityCenter Web sitesinden, **Yardım** sekmesini tıklatın, **Yardımcı Programlar**'ı seçin, sonra ajanın yürütülebilir kurulum dosyasını yüklemek için **kurulum ajanı**'nı tıklatın.
- 2 Kurulum dosyasını bellek çubuğu gibi bir taşınabilir ortama kopyalayın veya istemci bilgisayar kullanıcılarına e-posta ile gönderin (isteğe bağlı).
- 3 Ajanı, konunuza bağlı olarak şu yöntemlerden biriyle kurun:
  - Yönetim bilgisayarından — Her zamanki kurulum araçlarınızı kullanarak dosyayı istemci bilgisayarlara kurun ve çalıştırın.
  - İstemci bilgisayardan — Kurulum işlemini başlatmak için dosyayı çift tıklatın.

# Total Protection Service'ı Kurma

---

Bu bölümde, bilgisayarlara istemci yazılımının nasıl kurulacağı açıklanmaktadır.

## İçindekiler

- ▶ Kurulum yöntemlerinin özeti
- ▶ Standart kurulum işlemi
- ▶ Sessiz kurulum işlemi
- ▶ Zorla yükleme işlemi
- ▶ Önceden kurulmuş sürümler ve CD sürümleri için işlemler
- ▶ Kurulumu tamamlama

## Kurulum yöntemlerinin özeti

Total Protection Service istemci yazılımını kurmanın birisi standart ikisi gelişmiş olmak üzere üç yöntemi vardır.

### Standart kurulum

Her istemci bilgisayara Total Protection Service kurmak için URL kullanın.

- İstemci yazılımı bilgisayarınıza kurmak ve SecurityCenter Web sitesine erişmek için Hoş Geldiniz e-posta iletilisinde aldığınız URL'yi kullanın. Bu URL hesabınıza özeldir ve abone olduğunuz korumanın tamamını hesabınızın varsayılan dilinde yükler.
- İsteğe bağlı olarak, Koruma Kurma Sihirbazıyla SecurityCenter üzerinde özel URL oluşturabilirsiniz. Kurulacak özel koruma türlerini, istemci yazılımının dilini ve istemci bilgisayarın yerleştirileceği gruba belirtmek için bu özel URL'yi kullanın.

Kullanıcılara ister Hoş Geldiniz e-postasında aldığınız URL'yi ister özel URL'yi kurulum yönergeleriyle birlikte gönderin veya her istemci bilgisayarı ziyaret edin ve yazılımı kurmak için URL'yi kullanın.

### Gelişmiş kurulum seçenekleri

Yönetim bilgisayarından, SecurityCenter Web sitesini ziyaret edin ve yazılımı kullanıcı etkileşimi olmadan kurmak için gelişmiş bir kurulum yöntemini seçin.

- **Sessiz kurulum** — VSSETUP.EXE adlı programı yükleyin, istemci bilgisayarlara kurun, sonra her istemci bilgisayarda bir DOS penceresi açın ve komut satırından VSSETUP.EXE dosyasını çalıştırın. Bu yöntem üçüncü taraf bir kuruluş aracını, oturum açma komut dosyasını veya e-posta iletilisinde yürütülebilir dosyaya olan bir bağlantıyı gerektirir.
- **Zorla yükleme** — Push Install yardımcı programını edinin, sonra yazılımı doğrudan hizmet sağlayıcınızın Web sitesinden bir veya daha fazla istemci bilgisayara uzaktan kurun.

Bu tablo, gelişmiş kurulum yöntemleri arasındaki farkları özetler.

Yönetici...	Gelişmiş kurulum yöntemi	
	Sessiz	Zorla
Kurulumu şuradan gerçekleştirir	İstemci bilgisayardan	Yönetim bilgisayarından
SecurityCenter üzerinden bu dosyayı alır	VSSETUP.EXE	Push Install yardımcı programı
İstemci yazılımını şuraya kurar	Bir bilgisayara	Bir veya daha çok bilgisayara
Uzaktan kurar	Hayır	Evet
Aktarma sunucuları atayabilir (isteğe bağlı)	Evet	Evet (istemci bilgisayarlar ve aktarma sunucuları için ayrı kurulum gerektirir)

## Standart kurulum işlemi

URL kurulumu, en yaygın kurulum yöntemidir. İstemci yazılımı her bilgisayara tek tek yüklenir. Kullanıcılar istemci yazılımı şirkete özel bir URL'den bilgisayarlarına yükleyerek kurarlar.

### Standart kurulum nasıl işler

- 1 Yükleme URL'nizi Hoş Geldiniz e-posta iletinizden alın veya SecurityCenter üzerinden özel bir URL oluşturun.
- 2 URL'yi bir e-posta iletisi içinde yönergelerle birlikte (isteğe bağlı) kullanıcılara gönderin.
- 3 İstemci bilgisayardan, URL'yi bir tarayıcı penceresine girin.

## Standart kurulum gereksinimleri

Yükleme URL'si kullanarak istemci bilgisayara Total Protection Service kurmak için:

- İstemci bilgisayarın İnternet bağlantısı olması gerekir.
- İstemci bilgisayar kullanıcısının yerel yönetici haklarının olması gerekir.

**NOT:** Yönetici hakları varsayılan ayar değildir. Varsayılan Windows yapılandırmasını değiştirin veya istemci bilgisayara tek başına bir kurulum ajanı kurun (bkz. *Tek başına kurulum ajanını kurma*).

## Kullanıcılara kurulum URL'si gönderme

Yönetici olarak, şirkete özel kurulum URL'sini iki yoldan edinebilirsiniz:

- Total Protection Service kaydınızı yaptırdıktan sonra, şirketiniz için ayarlanmış kurulum URL'sini içeren bir e-posta iletisi alırsınız. Bu URL abone olduğunuz tüm koruma yazılımlarını kurar ve hesabınızın varsayılan grubuna hesabınızın varsayılan dilinde yerleştirir. Bu URL'yi bir e-posta iletisine kopyalayıp kullanıcılara gönderebilirsiniz.
- İstedığınız zaman, SecurityCenter oturumunuzu açabilir ve kullanıcılara yönelik özelleştirilmiş bir URL oluşturabilirsiniz. Bu onlara, seçilen koruma yazılımını belirlenen gruba belirlenen dilde kurma olanağı sağlar.

Özelleştirilmiş kurulum URL'si oluşturup kullanıcılara göndermek için bu görevi kullanın.

### Görev

Seçenek tanımları için, arabirimde ? işaretini tıklatın.

- 1 Web tarayıcınızda, SecurityCenter Web sitenizde oturum açın.
- 2 Bilgisayarlar sayfasından, **Bilgisayar Ekle**'yi tıklayın.
- 3 İstemci bilgisayarları yerleştirmek istediğiniz grubu seçin, kurulacak koruma türlerini ve yazılımın dilini de seçtikten sonra, **İleri**'yi tıklayın. Kullanıcılar için basit yönergelerle birlikte özelleştirilmiş URL görüntülenir.
- 4 **Metni Seç ve Panoya Kopyala**'yı tıklayın.
- 5 Yerel e-posta uygulamanızda, yeni bir ileti açın ve kopyaladığınız metni yapıştırın.
- 6 Gerektiğinde yönergeleri gözden geçirin, sonra yazılımı kurması gereken kullanıcılara e-postayı gönderin.

## URL ile kurma

Yükleme URL'si ile istemci bilgisayara Total Protection Service kurmak için bu görevi kullanın.

### Görev

Seçenek tanımları için, arabirimde ? işaretini tıklayın.

- 1 Hoş Geldiniz e-postasında aldığınız URL'yi kullanıcılara e-posta ile gönderin veya SecurityCenter oturumu açın, Kontrol ve yönetim ekranı sayfasında **Korumayı Kur**'u tıklayın ve özel bir URL oluşturup kullanıcılara e-posta ile göndermek üzere sihirbazdaki adımları izleyin.
- 2 İstemci bilgisayarda e-posta iletisini açın ve kurulum URL'sini tıklayın.
- 3 İstenirse, kurulacak koruma türlerini seçin, e-posta adresinizi **E-posta veya tanımlayıcı** alanına yazın ve **Devam**'ı tıklayın.

**NOT:** Buraya girilen bilgiler kurulumun yapılmakta olduğu bilgisayarı tanımlar. Raporlarda o bilgisayarı tanımlarken SecurityCenter bu bilgileri kullanır. Raporlar bilgisayardaki bir soruna işaret ediyorsa, kullanıcıyı bilgilendirmek için e-posta adresini kullanabilirsiniz. Kullanıcı e-posta adresi girmezse, güvenlik sorunları çıktığında kullanıcıyla nasıl iletişim kurulacağını bilmesi önemlidir.

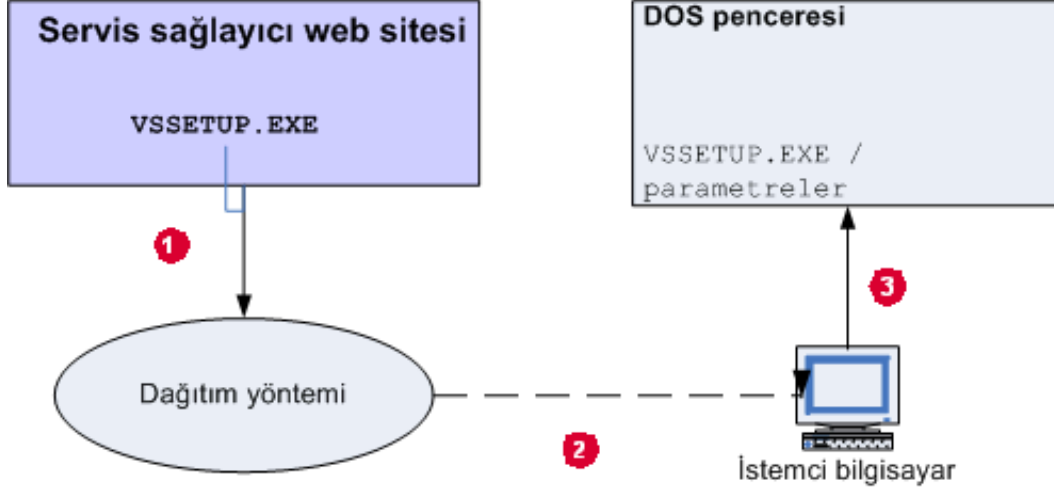
- 4 İstendiğinde, **Kur**'u tıklayın.
- 5 Dosya Yükleme iletişim kutusunda **Çalıştır**'ı tıklayın.  
Total Protection Service, kurulum için o an oluşturulan ve 24 saat sonra süresi sona eren bir tanımlama bilgisini kullanır. Kurulum dosyasını kaydeder ve 24 saat geçtikten sonra kurmayı denerseniz veya bu tanımlama bilgisini silerseniz, kurulum işlemine yeniden başlamanız istenir.
- 6 Kullanıcı Hesabı Denetimi iletişim kutusu görünürse, **Devam**'ı tıklayın.
- 7 Güvenlik duvarı desteği kuruyorsanız, istendiğinde **Yeniden Başlat**'ı seçin.

## Sessiz kurulum işlemi

Sessiz kurulum yöntemi, kullanıcı etkileşimi olmadan istemci bilgisayara Total Protection Service kurmak için VSSETUP yürütülebilir dosyasını kullanır. Bu kurulum yöntemi ağa özel değildir ve yazılımı herhangi bir Windows işletim sistemine kurar.

### Sessiz kurulum nasıl işler

- 1 VSSETUP'ı SecurityCenter üzerinden yükleyin.
- 2 İstemci bilgisayarı kurmak istediğiniz her bilgisayara kurun.
- 3 Bilgisayarda, bir DOS penceresi açın ve uygun parametreleri kullanarak VSSETUP komutunu çalıştırın.



### Sessiz kurulum gereksinimleri

Sessiz kurulum yöntemini kullanarak istemci bilgisayara Total Protection Service kurmak için:

- Ürünü kurmak için, bu programı yeterli haklara sahip bir hesabı kullanarak çalıştırmamız gerekir. Genellikle yerel yönetici izinleri gerekir ve bazı yöntemler uzaktan yürütme hakları olmasını gerektirir.
- Şirket anahtarınızı bilmeniz gerekir. Anahtarı bulmak için, şu konumlara bakın:
  - Kurulum URL'sinde, şundan sonraki karakter dizisine  
CK=
  - SecurityCenter üzerinde, Hesabım sayfasının **Hesaplar ve Anahtarlar** sekmesine.
- VSSETUP.EXE'yi kurmak için, ağ bilgisayarlarınıza yürütülebilir dosyaları kurmaya yönelik bir yönteminizin olması gerekir. Örnek:
  - Novell NAL, ZenWorks, Microsoft Systems Management Server (SMS) yükleyicisi veya Tivoli IT Director gibi üçüncü taraf bir kurulum aracı.
  - Oturum açma komut dosyası.
  - E-posta iletisi içinde bir yürütülebilir dosya bağlantısı.
  - CD veya bellek çubuğu gibi bir taşınabilir ortam.

### Sessiz kurulum ile kurma

Sessiz kurulum yöntemi ile Total Protection Service kurmak için bu görevi kullanın.

#### Görev

Seçenek tanımları için, arabirimde ? işaretini tıklatın.

- 1 Web tarayıcınızdan, SecurityCenter oturumunuzu açın.

- 2 Kontrol ve yönetim ekranı sayfasında, **Korumayı Kur**'u tıklayın.
- 3 İstemci bilgisayarları yerleştirmek istediğiniz grubu, kurulacak koruma türlerini ve yazılımın dilini seçtikten sonra, **İleri**'yi tıklayın.
- 4 Ek Kurulum Seçenekleri altından, **Gelişmiş kurulum yöntemlerini göster**'i seçin.
- 5 Yöntem 1 altından, VSSETUP.EXE dosyasını sabit sürücünüze kaydetmek için **VSSETUP**'ı tıklayın.
- 6 *Sessiz kurulum gereksinimleri* altında listelenenler gibi alıştığınız bir kurulum aracını kullanarak her istemci bilgisayara programı kurun.
- 7 Her istemci bilgisayarda, bir DOS penceresi açın ve aşağıdaki komutu çalıştırın.  
VSSETUP.EXE /CK=<şirket anahtarınız> /<parametreler>  
Bu örnekte gösterildiği gibi, şirket anahtarınızı (CK) parametre olarak eklemeniz gerekir. Komut satırınıza ekleyebileceğiniz isteğe bağlı parametrelerin listesi için *VSSETUP parametreleri* altına bakın.  
**NOT:** Şirket anahtarınız, Total Protection Service aboneliği aldığınız sırada verilen URL'de bulunur. Anahtar, URL'nin sonundaki  
CK=  
karakterlerinden sonraki onaltılı değerdir. Şirket anahtarınız, SecurityCenter üzerinde, Hesabım sayfasının **Hesaplar ve Anahtarlar** sekmesinde de listelenir.
- 8 Güvenlik duvarı koruması kuruyorsanız, istemci bilgisayarı yeniden başlatın.

## VSSETUP ile aktarma sunucusu atama

Bir bilgisayarın aktarma sunucusu işlevi görüp görmeyeceğini belirtmek için bu görevi kullanın.

### Görev

- Bir bilgisayarı aktarma sunucusu olarak belirtmek veya aktarma sunucusu belirtimini değiştirmek için VSSETUP parametresi kullanın.

Bunu yapmak için...	Bu parametreyi kullanın
Kurulum sırasında, bir bilgisayarı aktarma sunucusu olarak belirtin.	VSSETUP /RelayServer=1 <b>NOT:</b> Bu parametreyi belirtmezseniz, varsayılan 0'dır ve bilgisayar aktarma sunucusu olmaz.
Bir bilgisayarın aktarma sunucusu olduğunu belirtmek için varolan bir kurulumu değiştirin.	VSSETUP /SetRelayServerEnable=1
Bir bilgisayarın aktarma sunucusu olmadığını belirtmek için varolan bir kurulumu değiştirin.	VSSETUP /SetRelayServerEnable=0

## VSSETUP parametreleri

Sessiz kurulum için, bu komut satırını ve aşağıdaki parametrelerden herhangi birini kullanın (büyük-küçük harfe duyarlı değildir):

VSSETUP.EXE /CK=<şirket anahtarınız> /<parametreler>

Parametre	Açıklama
/CK=XYZ	Gerekli. Şirket anahtarını kullanarak Kurulum'u başlatır. Şirket anahtarınız SecurityCenter üzerinde, Hesabım sayfasının <b>Hesaplar ve Anahtarlar</b> sekmesinde listelenir.
/Email=x@y.com	Yönetim raporlarında kullanıcının e-posta adresini tanımlar. <b>NOT:</b> Adına karşın, email değişkeninin bir e-posta adresi olması gerekmez. Raporlarda hatalı görüntülenebileceği için, standart olmayan karakterler içeren bir dize kullanmayın.
/Uninstall	Total Protection Service ögesini kaldırır.
/SetRelayServerEnable=1	İnternet bağlantısı olan bir bilgisayarı aktarma sunucusu olarak belirler. Bilgisayar aktarma sunucusu olarak kullanılmıyorsa, 0'a ayarlayın.
/Reinstall	Önceki şirket anahtarı, e-posta adresi ve makine kimliği verilerini değiştirmeden olduğu gibi bırakarak Total Protection Service kurulumunu yeniden yapar.
/Groupid=[grup numarası]	Bilgisayarı oluşturmuş olduğunuz herhangi bir gruba yerleştirir. Bilgisayar Profilleri raporunu denetleyerek veya özel URL oluşturarak gruba ilişkilendirilmiş numarayı bulabilirsiniz. Grup kimliği, URL'nin sonunda G=xx biçimindedir. <b>NOT:</b> Olmayan bir grup atarsanız, kullanıcılar Varsayılan Gruba yerleştirilir.
/P=b /P=c /P=f /P=v	Kurulacak koruma türlerini seçer: <ul style="list-style-type: none"><li>• b — tarayıcı koruması</li><li>• c — web filtreleme</li><li>• f — güvenlik duvarı koruması</li><li>• v — virüs ve casus yazılım koruması</li></ul> <b>NOT:</b> /P parametresini atlarsanız, yalnızca virüs ve casus yazılım koruması kurulur.

## Örnekler

VSETUP.EXE /vfb /CK=abcd /Email=joe@example.com /Groupid=3

Virüs ve casus yazılım koruması, güvenlik duvarı koruması ve Web filtreleme kurulmuştur. Şirket anahtarı abcd'dir, kullanıcının raporlama amaçlı e-posta adresi joe@example.com'dur ve bu kullanıcı 3 rakamıyla temsil olunan varolan bir gruba yerleştirilmiştir. Doğru sayısal grup kimliğini bulmak için Bilgisayar Profilleri raporunu denetleyin.

VSETUP.EXE /CK=abcd /Email=joe@example.com

Yalnızca virüs ve casus yazılım koruması kurulmuştur. Şirket anahtarı abcd'dir ve kullanıcının raporlama amaçlı e-posta adresi joe@example.com'dur.

## Zorla yükleme işlemi

*Zorla yükleme*, ağdaki bir veya daha fazla bilgisayara uzaktan kurma anlamına gelir. Bu yöntem, istemci yazılımını servis sağlayıcısının Web sitesinden doğrudan ağınızdaki istemci bilgisayarlara kurmak için Push Install yardımcı programını kullanır. Zorla yükleme, üçüncü taraf kuruluş yazılımı veya kullanıcılarla etkileşim gerektirmez.

Zorla yükleme gerçekleştirmek için:

- 1 Push Install yardımcı programını yükleyip zorla yükleme işlemi başlatacağınız bir *yönetim bilgisayarını* belirleyin.
- 2 Ağınızdaki, yazılımı alacak istemci bilgisayarlar olan *hedef bilgisayarları* seçin.

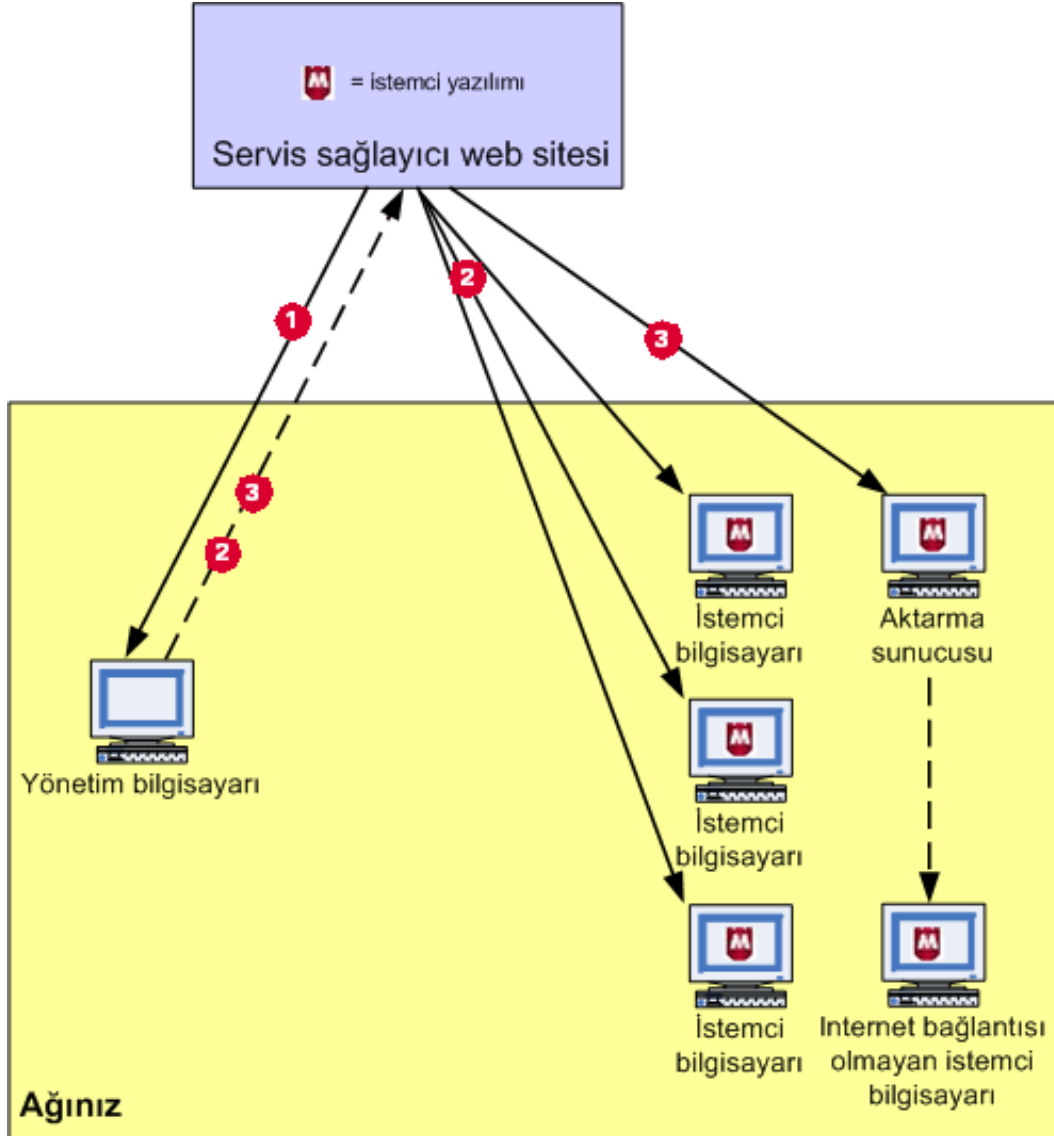
Push Install yardımcı programı, yönetim bilgisayarı üzerinde çalışan bir AciveX denetimidir. Zorla yükleme işlemi gerçekleştiğinde çevrimiçi olan tüm hedef bilgisayarlara istemci yazılımı yükler. Yeni ağ bilgisayarlarına istemci yazılımları yüklemek veya istemci yazılımlara sahip bilgisayarlara ek koruma türleri yüklemek için zorla yüklemeyi kullanın.

Push Install yardımcı programı, Internet bağlantısı olan bir veya daha fazla ağ bilgisayarının aktarma sunucusu olarak belirtilmesini sağlar. Aktarma sunucuları ile aktarma sunucusu olmayan sunuculara aynı anda zorla yükleme yapılamayacağı için, bunun ayrı bir zorla yükleme işleminde yapılması gerekir. Daha fazla bilgi için *Aktarma sunucuları belirlenip belirlenmeyeceğine karar verme* konusuna bakın.

### **Zorla yükleme nasıl işler**

- 1 SecurityCenter üzerinden, aşağıdaki konumlardan birinden Push Install yardımcı programını edinin:
  - Koruma Kurma sihirbazının parçası olarak.
  - Yardımcı Programlar sayfasından.
- 2 Bir veya daha fazla istemci bilgisayara zorla yükleme başlatın.

3 Bir veya daha fazla aktarma sunucusuna zorla yükleme başlatın (*isteğe bağlı*).



## Zorla yüklemeleri zamanlarken dikkat edilecek konular

Zorla yüklemeleri zamanlarken:

- **Diğer ağ görevlerini dikkate alın.** Çok sayıda bilgisayara aynı anda zorla yükleme yapmak yüksek hacimde bir ağ trafiği oluşturabileceği için, zorla yüklemeleri diğer ağ görevlerini etkilemeyeceği saatlere zamanlayın.
- **Hedef bilgisayarların açık olduğundan emin olun.** Push Install yardımcı programı, istemci yazılımları, zorla yükleme gerçekleştiği sırada çevrimiçi ve açık olan hedef bilgisayarlara kurar.
- **Kullanıcıların hedef bilgisayarları kullanmadığından emin olun.** Zorla yükleme devam ederken bir istemci bilgisayarın yeniden başlatılması bilgisayarın kararsızlaşmasına neden olabileceği için, zorla yükleme işlemlerini kullanıcıların bilgisayarlarını kullanmayacağı saatlere zamanlayın.

Zorla yüklemenin gece yarısına zamanlanması ve kullanıcılara bilgisayarlarını gece açık bırakmalarını isteyen bir e-posta gönderilmesini öneririz.

## Zorla yükleme gereksinimleri

Zorla yükleme yöntemini kullanarak istemci bilgisayarlara Total Protection Service kurmak için bu sistem gereksinimlerini karşılamamız gerekir.

### Hedef bilgisayarlar için gereksinimler

- Tüm hedef bilgisayarların aynı Microsoft Windows etki alanında yönetici olarak oturum açmaları gerekir.

### Yönetim bilgisayarları için gereksinimler

- Yönetim bilgisayarının Windows 2000, Windows XP Professional, Windows Vista veya Windows 7 işletim sistemini çalıştırıyor olması gerekir.

**NOT:** Microsoft Windows XP Home Edition bir Active Directory etki alanında oturum açmadığı için, zorla yükleme yöntemi Windows XP Home Edition'da desteklenmez.

- Yönetim bilgisayarının, ActiveX etkinleştirilmiş olarak Internet Explorer 6.0 veya üzerini çalıştırması gerekir.
- Yönetim bilgisayarında, kurulmakta olan etki alanı için etki alanı yöneticisi ayrıcalıklarıyla oturum açmanız gerekir.
- SecurityCenter yönetim Web sitesinde oturum açmak için kimlik bilgilerinizin elinizde olması gerekir. Bu bilgileri, sipariş verdikten sonra Hoş Geldiniz e-postasında aldınız.
- Windows güvenlik duvarı ile Windows XP Professional, Windows Vista veya Windows 7'yi çalıştıran yönetim bilgisayarlarının, güvenlik duvarının Özel Durumlar listesine Dosya ve Yazıcı Paylaşımı'nı eklemesi gerekir.

## Yönetim bilgisayarını hazırlama

Windows XP Professional, Windows Vista veya Windows 7 üzerinde Windows güvenlik duvarı çalıştıran yönetim bilgisayarlarının, güvenlik duvarının Özel Durumlar listesine Dosya ve Yazıcı Paylaşımı'nı eklemesi gerekir.

Push Install yardımcı programını çalıştırmadan önce yönetim bilgisayarını hazırlamak için bu görevi kullanın.

### Görev

- 1 **Windows Denetim Masası**'nı açın.
- 2 **Windows Güvenlik Duvarı**'nı veya **Windows Güvenlik Merkezi**'ni çift tıklatın.
- 3 Özel Durumlar sekmesinde, Programlar ve Hizmetler altında **Dosya ve Yazıcı Paylaşımı**'ni seçin.
- 4 **Tamam**'ı tıklatın.

## Zorla yükleme ile kurma

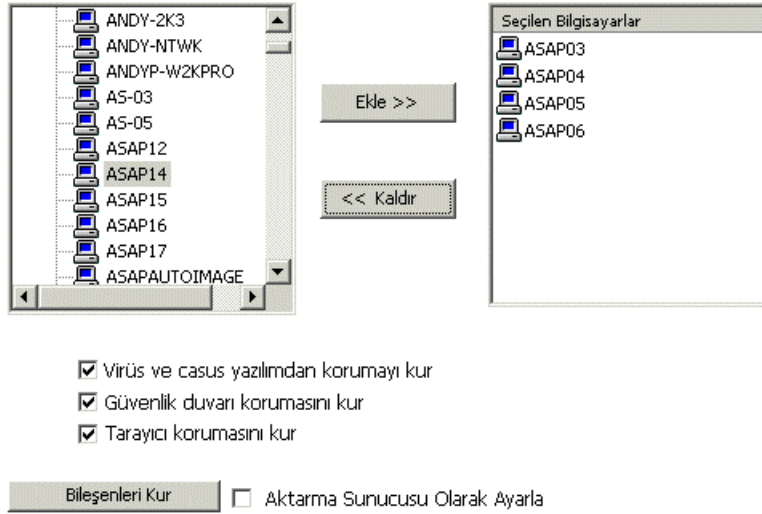
Push Install yardımcı programını kullanarak Total Protection Service istemci yazılımını kurmak için bu görevi kullanın.

**DİKKAT:** Zorla yazılım yüklemeyen önce kritik sunucularınızdaki tüm önemli verileri yedekleyin.

### Görev

Seçenek tanımları için, arabirimde ? işaretini tıklatın.

- 1 Yönetim bilgisayarında, Internet Explorer'ı açın, SecurityCenter oturumunu açın, ardından **Korumayı Kur**'u tıklatın.
- 2 Yazılımın kurulacağı bilgisayarların türünü seçin, sonra **İleri**'yi tıklatın.
- 3 Yeni bilgisayarlara kuruyorsanız (şu an Total Protection Service kurulu olmayan bilgisayarlara), bilgisayarları atamak istediğiniz gruba seçin.
- 4 Kurulacak koruma türlerini seçin, dili seçin, sonra **İleri**'yi tıklatın.
- 5 Ek Kurulum Seçenekleri altından, **Gelişmiş kurulum yöntemlerini göster**'i seçin.
- 6 Yöntem 2 altından, **Push Install yardımcı programını çalıştır**'ı tıklatın. Bir pencere, etki alanınızda görünen bilgisayarları listeler.



- 7 Sol bölmeden hedef bilgisayarları seçin, sonra **Ekle**'yi tıklatın.
- 8 İsteğe bağlı olarak, tüm seçili bilgisayarları ağdaki diğer bilgisayarlara güncelleme dağıtabilen aktarma sunucuları olarak yapılandırmak için **Aktarma Sunucusu Olarak Ayarla**'yı seçin.
- 9 Kurulacak koruma türlerini seçin, sonra **Bileşenleri Kur**'u tıklatın. Kurulum tamamlandıktan sonra, her hedef bilgisayar için bir durum görüntülenir.
- 10 Geçerli oturumun durumunu gösteren günlük dosyasını Microsoft Not Defterinde açmak için **Günlüğü Görüntüle**'yi tıklatın. Push Install yardımcı programını kapattığınızda veya başka bir zorla yükleme gerçekleştirdiğinizde, günlük dosyasının içeriği silinir.

**NOT:** İletişim kutusu ve günlük dosyası yalnızca dosyaların hedef bilgisayarlara zorla yüklenip yüklenmediğini gösterir. Dosyaların yüklendiğinden ve bilgisayarların başarıyla güncellendiğinden emin olmak için, SecurityCenter üzerindeki raporların incelenmesi veya istemci bilgisayarların denetlenmesi önemlidir.

- 11 Günlük dosyasını kaydedin veya isteğe bağlı olarak, önceki ekrana dönüp daha fazla bilgisayara zorla yükleme yapmak için **Geri**'yi tıklayın.
- 12 Güvenlik duvarı korumasını kurduysanız, istemci bilgisayarları yeniden başlatın.

## Push Install yardımcı programını kaldırma

Total Protection Service kurulumunu yaptıktan sonra yardımcı programı yönetim bilgisayarından kaldırmak için bu görevi kullanın.

### Görev

- 1 Windows Denetim Masası'nda, **Program Ekle/Kaldır**'ı açın.
- 2 **McAfee PushInstall** seçeneğini işaretleyin.
- 3 **Kaldır**'ı tıklayın.

## Önceden kurulmuş sürümler ve CD sürümleri için işlemler

Yükleme URL'sini, sessiz kurulumu veya zorla yüklemeyi kullanarak bir Total Protection Service kopyası kurduğunuzda, otomatik olarak kopya etkinleşir ve geçerli lisans bilgileri uygulanır. Ancak, Total Protection Service bilgisayara üretici tarafından önceden kurulduğunda veya CD'den kurulduğunda, hesabı ayarlamak için ek adımlar gereklidir.

Kopyanız şu ise...	Bu işlemi izleyin
CD'den kurulmuş	<p>İlk kopyayı kurmak için:</p> <ol style="list-style-type: none"><li>1 CD kullanarak kurun.</li><li>2 Yazılımı etkinleştirin.</li><li>3 Etkinleştirme işlemi sırasında, ilk kopyayı kurmak ve hesap oluşturmak üzere lisans anahtarını girin.</li><li>4 Etkinleştirme tamamlandıktan sonra, Etkinleştirme Sihirbazı ile oluşturulan hesap kayıt anahtarını kaydedin. (Anahtar SecurityCenter üzerinde, Hesabım sayfasının <b>Hesaplar ve Anahtarlar</b> sekmesinde de bulabilirsiniz.)</li></ol> <p>Ek bilgisayarlara yüklemek için:</p> <ol style="list-style-type: none"><li>1 CD kullanarak kurun.</li><li>2 Yazılımı etkinleştirin.</li><li>3 Etkinleştirme işlemi sırasında, hesap kayıt anahtarını girin.</li></ol> <p>Daha fazla bilgi için CD ile birlikte gelen yönergelere bakın.</p>
Önceden kurulmuş	<ol style="list-style-type: none"><li>1 Total Protection Service kopyanızı etkinleştirin.</li><li>2 Etkinleştirme işlemi sırasında lisans anahtarı gerekirse, sisteminizle birlikte gönderilen McAfee lisans kartında bulunan lisans anahtarını girin. (Bazı bilgisayar üreticileri bir lisans anahtarı gerektirmez. Anahtar istenmezse, bu adımı atlayın.)</li><li>3 Etkinleştirme işlemi sırasında, istenirse hesap kayıt anahtarını girin.</li><li>4 Bu bir deneme aboneliği ise, deneme süresinin sonuna kadar tam abonelik satın alın.</li></ol>

## Önceden kurulmuş deneme sürümü ve tam abonelikler

Total Protection Service'in bir kopyası bilgisayarını aldığınız sırada önceden kurulmuşsa, bilgisayarınızı açtığınızda şu seçeneklerden biri görülür:

- Bir deneme süresi başlar. Deneme kopyasını etkinleştirin, koruma özelliklerini değerlendirin, sonra deneme süresinden sonra korumayı uzatmak için tam abonelik satın alın.
- Tam abonelik başlar. Aboneliği etkinleştirin, sonra aboneliği yenileme zamanı gelene dek koruma özelliklerini kullanın.

## Bilgisayarı ilk açtığınızda

Ağ ilk algılandığında, önceden kurulmuş olan Total Protection Service kopyası, tehditleri algılamada kullanılan algılama tanım (DAT) dosyalarını günceller. Sonra erişime bağlı tarama özelliği tüm dosyaları otomatik olarak erişildikçe taramaya başlar ve kullanıcılar bilgisayardaki tüm dosyaları tehditler açısından denetlemek için isteğe bağlı taramalar gerçekleştirebilir. Yeni tehditlerden koruyan güncellemeler almaya devam etmek için, Total Protection Service kopyasının etkinleştirilmesi gerekir.

Çoğu durumda, bir iletişim kutusu kullanıcılara etkinleştirme işlemi anımsatır. Etkinleştirme yapmazlarsa, Total Protection Service kopyaları etkinleştirme süresinin sonunda çalışmamaya başlar. Bir özelliğe erişmeyi denediklerinde, bir iletişim kutusu etkinleştirme süresinin sona erdiğini bildirir ve tam abonelik satın alma fırsatı sunar.

## Total Protection Service kopyasını etkinleştirme

En son tehditlere karşı koruma sağlayan algılama tanım (DAT) dosyasının güncellemelerini almaya devam etmek için her Total Protection Service kopyasını etkinleştirin. Etkinleştirilmiş bir kopya, güncellemeleri otomatik olarak düzenli aralıklarla denetler. Deneme sürümünü etkinleştirdikten sonra, kullanıcıların korumayı deneme süresinden sonra uzatan bir tam abonelik satın alma seçeneği de olur.

Yazılımı etkinleştirmek için bu görevi kullanın.

### Görev

- 1 İstemci bilgisayarda, sistem tepsisindeki Total Protection Service simgesini tıklatın, sonra **Etkinleştir**'i seçin veya bildirim iletişim kutusundaki **Etkinleştir** bağlantısını seçin.
- 2 Etkinleştirme sihirbazında, etkinleştirilecek hesabın türünü seçin.

Bu seçeneği belirleyin...	Amacınız...
<b>Yeni hesap oluşturun</b>	Bu, etkinleştirdiğiniz veya satın aldığınız ilk Total Protection Service kopyasıysa, yeni bir hesap oluşturun. Total Protection Service için birden çok lisans satın aldıysanız, bu hesaba başka bilgisayarlar ekleyebilir ve tümünün güvenliğini yönetebilirsiniz.
<b>Varolan bir hesaba katılın</b>	Zaten kurulmuş olan bir hesaba katılın. Hesap kayıt anahtarı gereklidir. Bu anahtar hesap kurulduğu sırada sağlanmıştır. Hesap kayıt anahtarını görüntüleyin veya SecurityCenter üzerinde Hesabım sayfasındaki <b>Hesaplar ve Anahtarlar</b> sekmesinden yeni bir anahtar oluşturun.

- 3 Etkinleştirme sihirbazındaki yönergeleri izleyerek, hesabı tanımlayan bilgileri girin.

- 4 Yeni hesap oluştururken, diğer bilgisayarlara Total Protection Service kurulurken kullanılacak hesap kayıt anahtarını kaydedin. Diğer bilgisayarlara Total Protection Service kurarken kullanmak için kurulum URL'sini içeren bir e-posta da alırsınız.

**NOT:** Lisans anahtarını girmeniz istenirse ve anahtarınız yoksa, deneme hesabı oluşturabilir ve ardından lisans anahtarını etkinleştirip asıl anahtarı aldıktan sonra tam hesaba dönüştürebilirsiniz.

## Tam abonelik satın alma veya yenileme

Deneme sürümü aboneliği etkinleştirildikten sonra, deneme süresinde tam abonelik satın alarak bilgisayarınızın korumasını uzatabilirsiniz. Tam abonelik güncellemeleri almaya devam etmenizi ve Internet'e gözetip araştırırken isteğe bağlı taramalar, gelen e-posta ve eklerin otomatik taranması, gelen iletişimlerin şüpheli etkinlik açısından izlenmesi ve en güncel güvenlik raporları gibi özelliklere erişiminizi sürdürmenizi sağlar.

Tam aboneliğin süresi sona ermeye yaklaştığında, kesintisiz koruma sağlamak için yenileyebilirsiniz.

Abonelik satın almak veya yenilemek için bu görevi kullanın.

### Görev

- 1 İstemci bilgisayarda, sistem tepsisindeki Total Protection Service simgesini tıklattıktan sonra, **Satın Al**'ı veya **Bu aboneliği yenile**'yi seçin. (Bu seçenekleri bildirim iletişim kutusundan da seçebilirsiniz.)
- 2 İstendiğinde, iletişim ve ödeme bilgilerinizi girin.

**NOT:** Bir deneme sürümünün veya tam aboneliğin süresi sona erdiğinde, Total Protection Service artık bilgisayarınızı korumaz. Kullanıcılar bir özelliğe erişmeyi denediklerinde, bir iletişim kutusu kopyalarının süresinin sona erdiğini bildirir ve tam abonelik satın alma veya aboneliği yenileme fırsatı sunar.

## Hesap kayıt anahtarını görüntüleme veya oluşturma

Hesap kayıt anahtarı, hesabınıza yeni Total Protection Service kurulumları eklemenizi sağlayan bir benzersiz tanımlayıcıdır. Yedi gün süreyle geçerli kalır.

Hesap kayıt anahtarı ilk olarak, önceden kurulmuş bir Total Protection Service kopyası veya CD sürümü için yeni bir hesap etkinleştirdiğinizde oluşturulur. Bu anahtar şunlar için gereklidir:

- Önceden kurulmuş yeni Total Protection Service kopyalarını hesabınız altından etkinleştirmek.
- Hesabınıza yeni CD kurulumları eklemek.

Anahtarınızın süresi sona erer veya başkasının eline geçerse, anında etkinleşen yeni bir anahtar oluşturun.

Hesap kayıt anahtarını görüntülemek veya oluşturmak için bu görevi kullanın.

### Görev

Seçenek tanımları için, arabirimde ? işaretini tıklatın.

- 1 SecurityCenter üzerinde Hesabım sayfasında, **Hesaplar ve Anahtarlar** sekmesini tıklatın.
- 2 Hesap Kayıt Anahtarı bölümünde varolan anahtara bakın.

- Geçerli bir anahtar listelenmiyorsa, **Yeni anahtar oluştur**'u tıklatın. Sayfada yeni bir anahtar görüntülenir.

## Kurulumdan sonra lisans anahtarınızı etkinleştirme

Total Protection Service kurulumu yaptığınızda geçerli bir lisans anahtarınız yoksa, lisans anahtarı edinene dek bilgisayarlarınızı korumak için bir deneme aboneliği oluşturabilirsiniz.

Deneme sürümünü kurmak için bu görevi kullanın, sonra lisans anahtarı edinip etkinleştirin.

### Görev

Seçenek tanımları için, arabirimde ? işaretini tıklatın.

- Etkinleştirme işlemi sırasında, **Deneme kullanıcısı olarak devam et**'i seçin.
- SecurityCenter üzerinde Hesabım sayfasında, **Hesaplar ve Anahtarlar** sekmesini tıklatın.
- Lisans Anahtarını Etkinleştir**'i seçin.
- Geçerli bir lisans anahtarı almak için satıcınıza veya McAfee ürün destek hizmetlerine başvurun.
- İstenen bilgiyi forma girin, sonra **İleri**'yi tıklatın.  
Lisans anahtarınızı etkinleştirdikten sonra, hesabınız lisanslı bir tam abonelik olur. Lisans bilgileri, hesabınız altında kurulu diğer bilgisayarlar için de otomatik olarak güncellenir.

## Kurulumu tamamlama

Total Protection Service kurulumunu yaptıktan sonra, yazılımın doğru çalıştığından ve bilgisayarın korunduğundan emin olmak için her bilgisayarda bu görevleri gerçekleştirin.

### Görevler

- ▶ [Virüs korumasını test etme](#)
- ▶ [İstemci bilgisayarı tarama](#)
- ▶ [E-posta Gelen Kutusunu tarama](#)

## Virüs korumasını test etme

İstemci bilgisayara EICAR Standart Virüs Koruma Test Dosyasını yükleyerek virüs ve casus yazılımdan korunmanın virüs algılama özelliğini test etmek için bu görevi kullanın. EICAR test dosyası virüs olarak algılanmak üzere tasarlanmış olmasına karşın, bir virüs değildir.

### Görev

- EICAR dosyasını aşağıdaki konumdan yükleyin:  
<http://www.eicar.org/download/eicar.com>  
Düzgün yüklenirse, virüs ve casus yazılım koruması yüklemeyi keser ve bir tehdit algılama bildirimi görüntüler.
- Tamam**'ı tıklatın ve ardından **İptal**'i seçin.  
**NOT:** Hatalı yüklenirse, virüs ve casus yazılımdan korunma, virüsü algılamaz veya yükleme işlemini yarıda kesmez. Bu durumda, istemci bilgisayardan EICAR test dosyasını silmek için

Windows Gezgini'ni kullanın, ardından Total Protection Service uygulamasını yeniden kurun ve yeni kurulumu test edin.

## İstemci bilgisayarını tarama

Virüs ve casus yazılımlardan korumayı ilk olarak kurduktan sonra, devam etmeden önce tüm istemci bilgisayar sürücülerinin isteğe bağlı taramasının yapılması önerilir. Bu tarama, dosyalardaki varolan tehditleri denetleyip temizler veya siler. Daha sonra dosyalar erişildiğinde, yüklendiğinde veya kaydedildiğinde taranır.

İstemci bilgisayardaki sürücülerini taramak için bu görevi kullanın.

### Görev

- 1 Sistem tepesinde Total Protection Service simgesini tıklatın ve **Konsolu Aç**'i seçin.
- 2 Eylem Menüsünden, **Bilgisayarı Tara**'yı seçin.
- 3 Tarama hedefini seçin.
  - **Tüm bilgisayarımı tara** — Tüm sürücülerini, klasörleri ve dosyaları tarayın.
  - **Belirli bir sürücü veya klasörü tara** — Tarama hedefinin tam yolunu ve adını yazın veya bulmak için gözetin.
- 4 **Taramayı Başlat**'i tıklatın. Virüs ve casus yazılımdan korunma taramasının ilerlemesini görüntüler.
- 5 Gerekirse, taramayı geçici olarak durdurmak için **Taramayı Duraklat**'i veya taramayı sona erdirmek için **Taramayı İptal Et**'i tıklatın. (İsteğe Bağlı)
- 6 Bir tarayıcı penceresi açarak tarama sonuçlarını görüntülemek için **Ayrıntılı raporu göster**'i tıklatın.

## E-posta Gelen Kutusunu tarama

Virüs ve casus yazılımlardan korumayı ilk olarak kurduktan sonra, devam etmeden önce isteğe bağlı e-posta taramasının yapılması önerilir. Bu tarama, istemcinin Microsoft Outlook Gelen Kutusu'nda önceden bulunan tehditleri denetler. Sonraki e-postalar Gelen Kutusu'na yerleştirilmeden önce taranır.

Gelen Kutusu'nun içeriğini taramak için bu görevi kullanın.

### Görev

- 1 Microsoft Outlook Gelen Kutusu'nda, sağ bölmedeki bir veya daha fazla iletiyi vurgulayın.
- 2 Araçlar altından, **Tehditleri Tara**'yı seçin. İsteğe Bağlı E-posta Taraması penceresi olan algılamaları görüntüler. Pencere boşsa, bir tehdit algılanmamıştır.

# Sorun giderme ve destek

---

Bu bölümde, Total Protection Service yazılımının kurulması ve etkinleştirilmesiyle ilgili sorunların çözülmesine yardımcı olan bilgiler sunulmaktadır.

## İçindekiler

- ▶ Sık sorulan sorular
- ▶ Hata iletileri
- ▶ Ürün destek hizmetlerine başvurma

## Sık sorulan sorular

Bu bölüm, Total Protection Service istemci yazılımının kurulması ve etkinleştirilmesiyle ilişkili olarak yöneticiler ve istemci bilgisayar kullanıcıları tarafından soruları içerir.

## Kurulum hakkında sorular

### Mozilla Firefox veya Opera gibi Microsoft olmayan bir tarayıcı kullanabilir miyim?

**Hayır.** İstemci yazılımın kurulabilmesi için istemci bilgisayarın Microsoft Internet Explorer 6.0 veya daha ileri sürümünü kullanması gerekir. Ancak, istemci yazılım kurulduktan sonra, varsayılan Internet tarayıcısı diğer amaçlar için kullanılabilir. Internet Explorer'ı veya Firefox'u kullanarak SecurityCenter ürününü görüntüleyebilirsiniz.

### Yönetici hakları olmayan kullanıcılar istemci yazılımı Internet URL'si ile nasıl kurabilir?

Yönetici hakları olmayan kullanıcıların istemci yazılımı kurmasına izin vermek için, önce onların istemci bilgisayarına tek başına kurulum ajanını kurmalısınız. Bkz. *Tek başına kurulum ajanını kurma.*

### İstemci yazılımı kurarken hangi e-posta adresini veya tanımlayıcıyı girdiğim önemli mi?

**Hayır.** Alana herhangi bir açıklama girilebilir veya boş bırakılabilir. Ancak, e-posta adresi sorumlu kullanıcının bilgisayarın güvenlik sorunları hakkında bilgilendirilmesi için bir bağlantı sağlar. Girilen bilgiler, yönetim raporlarında istemci bilgisayarları tanıtır.

### İstemci yazılımı yüklerken, kurulum işlemi yanıt vermiyor görünüyor.

Kurulumun tamamlanması birkaç dakika sürebilir. Ancak, durum çubuğu hareket etmezse ve kurulum penceresinde birkaç dakikadan fazla süredir hiçbir şey değişmemişse, pencereyi kapatın ve kurulum işlemine yeniden başlayın (örneğin, kurulum URL'sini tıklatarak).

### **Erişim koruması veya diğer uygulamalardaki davranış engelleme kuralları istemci yazılımının kurulumunu etkiler mi?**

**Evet.** Kullanıcılar istemci yazılımını yükleyemiyorsa ve ikili dosyaların Temp klasöründen yürütülmesini engelleyen kurallar gibi erişim koruması veya davranış engelleme kuralları tanımladıysanız, onları devre dışı bırakıp kurulumu yeniden deneyin.

### **İstemci bilgisayarındaki Windows işletim sistemini güncellemek istiyorum. Total Protection Service istemci yazılımını yeniden kurmam gerekir mi?**

**Evet.** İstemci bilgisayarın işletim sistemini yükseltiyorsanız (örneğin, Windows 2000'den Windows XP'ye) ve yükseltme işlemi sırasında varolan dosya ve programlarınızı olduğu gibi korumak istiyorsanız, önce istemci yazılımı kaldırmayı, ardından yükseltme tamamlandıktan sonra tekrar kurmanız gerekir.

## **Önceden kurulmuş sürümler veya CD sürümleri hakkında sorular**

### **Total Protection Service istemci yazılımının her kopyasını neden etkinleştirmem gerekiyor?**

Kullanıcı önceden kurulmuş Total Protection Service kopyasıyla bilgisayarını ilk kez açtığı anda veya CD'den Total Protection Service kurduğunda, bilgisayar en son algılama tanım (DAT) dosyalarıyla ve ürün bileşenleriyle güncellenir. Total Protection Service kopyası etkinleştirilene kadar başka güncelleme gerçekleşmez. Bilgisayarın en son tehditlere karşı her zaman korunduğundan emin olmak için, kopyayı en kısa sürede etkinleştirin.

### **Hesap kayıt anahtarım kaybolduğunda veya süresi sona erdiğinde nasıl başka bir tane alabilirim?**

SecurityCenter kopyasının Hesabım sayfasında, **Hesaplar ve Anahtarlar** sekmesini tıklatın, sonra varolan anahtarı görmek için Hesap Kayıt Anahtarı bölümüne bakın. Bir anahtar yoksa, **Yeni anahtar oluştur**'u seçin. Hesap kayıt anahtarları yedi gün süresince geçerli kalır.

### **Ek lisanslar satın alırken bir bilgisayarı nasıl koruyabilirim?**

Total Protection Service kopyasını deneme sürümü olarak kurun. Sonra ek lisansları satın alın ve deneme hesabını ana hesabınızla birleştirin.

### **Lisans anahtarımı bulamazsam veya anahtar geçerli değilse ne olur?**

Total Protection Service kurduğunuzda geçerli lisans anahtarınız yoksa, bir tane alıp daha sonra kaydettirebilirsiniz. Lisans anahtarını alana kadar bilgisayarın korunmasını sağlamak için Total Protection Service kopyasını deneme sürümü olarak kurun, sonra lisans anahtarını etkinleştirin.

### **Yeni Total Protection Service kurulumlarının hesabımla birleştirildiğini nasıl anlarım? Onlar için herhangi bir kurulum görevi gerçekleştirmem gerekli mi?**

Yeni bilgisayarların eklendiğini size bildirmek için SecurityCenter ürününün Kontrol ve yönetim ekranı sayfasında bir uyarı görüntülenir. Varsayılan olarak, yeni bilgisayarlar Varsayılan Gruba yerleştirilir ve McAfee Default ilkesi atanır. Bu ayarları değiştirmek istiyorsanız, yönergeleri görüntülemek için uyarının çözüm düğmesini tıklatın. Bu ayarları değiştirmek istemiyorsanız, **Uyarıyı Bırak**'ı seçin.

## Hata iletileri

Bu bölüm, Total Protection Service istemci yazılımının kurulması ve etkinleştirilmesiyle ilişkili hata iletilerini içermektedir. Nedeni ve çözümleri hakkındaki ayrıntıları görmek için bir hata iletisi bulun.

### Kurulumdaki hata iletileri

**Yazılımı kurmak için gereken bir dosya kullanılamıyor. Kurulum işlemine yeniden başlamak için lütfen kurulum URL'sini tıklatın.**

Kullanıcı kurulum dosyasını yüklemek üzere kurulum URL'sini tıklattığında, bir tanımlama bilgisi oluşturulur. Tanımlama bilgisinin geçerliliği 24 saat sonra sona erer. Kullanıcı kurulum dosyasını kaydeder ve 24 saat geçtikten sonra kurmayı dener veya tanımlama bilgisini silerse, o kullanıcının yeniden dosyayı yükleyip kurulum işlemine başlaması gerekir.

**Uzaktan paylaşımlı dizin bulunamıyor.**

Başarısız zorla yükleme sırasında bu hata görülür. Hedef bilgisayarlar aşağıdaki koşullardan birini veya birkaçını karşılamamıştır:

- Dosya ve Yazıcı Paylaşımı etkinleştirilmiş olmalıdır.
- Kullanıcı düzeyinde erişim denetimi yapılandırılmalıdır.
- Windows NT Etki Alanı oturumlarını desteklemeyen Microsoft Windows XP Home Edition çalıştırılmıyor olmalıdır.
- Zorla yüklemeyi başlatan kişinin etki alanı yöneticisi hakları olmalıdır.

Zorla yükleme yaptığınız istemci bilgisayarda gerekli paylaşımların etkin olup olmadığını ve o bilgisayara zorla yükleme yapmak için gerekli yönetici haklarınızın olup olmadığını denetleyin. Denetlemek için:

- 1 İstemci bilgisayarda **Başlat | Çalıştır**'ı seçin.
- 2 **Aç** metin kutusunda, \\CPUNAME\ADMIN\$ yazın (burada CPUNAME, zorla yükleme yaptığınız bilgisayarın adıdır); sonra **Tamam**'ı tıklatın.

Zorla yükleme yapmaya çalıştığınız bilgisayarın \Windows dizininin görüntülenmesi gerekir. O bilgisayar için yeterli yönetici izinleriniz yoksa veya o bilgisayarda gerekli kullanıcı düzeyi erişimi ve paylaşım etkin değilse, **Ağ yolu bulunamadı** hata iletisi kutusu görünür.

- 3 Ağ yönetimi ayarlarınızı düzeltme hakkında bilgi için, Windows ağ belgelerinize bakın.

**Önemli bir ajan bileşenini kabul etmemeyi seçtiğiniz için kurulum devam edemiyor....**

Hata iletisinin tam metni, "Önemli bir ajan bileşenini kabul etmemeyi seçtiğiniz için kurulum devam edemiyor, makinenizde yönetim haklarınız yok veya başka sorunlar oluştu" şeklindedir. Bu hata iletisine birkaç farklı sorun neden olabilir:

- **Tarayıcının güvenlik düzeyi çok yüksektir.** Tarayıcının güvenlik düzeyini Orta veya Orta-Yüksek olarak ayarlayın.
- **Kullanıcının yönetim hakları yoktur.** Kullanıcıların istemci bilgisayarlara koruma yükleyebilmeleri için yönetici hakları olmalıdır. Yoksa, tek başına kurulum ajanı kurulması gerekir.
- **Bir kayıt defteri dosyası eksiktir.** Regedit.exe sistem dosyası eksik olabilir. İstemci bilgisayarın Windows klasöründe o dosyayı arayın. Dosya eksikse, orijinal Windows kurulum

ortamını kullanarak dosyayı değiştirin veya aynı işletim sistemini çalıştıran başka bir bilgisayardan kopyalayın.

- **Tarayıcı ön belleği doludur.** Internet Explorer ön belleğini boşaltın:

#### **sürüm 6.0**

- 1 Internet Özellikleri iletişim kutusunu açın ve şunlardan birini yapın:
  - Masaüstünde Internet Explorer simgesini sağ tıklayın ve **Özellikler**'i seçin.
  - Windows Denetim Masası'ndan, **Internet Seçenekleri**'ni açın.
- 2 Temporary Internet Files altından, **Dosya Sil**'i tıklayın.
- 3 **Tüm çevrimdışı içeriği sil**'i seçin ve **Tamam**'ı tıklayın. Dosyalar silinirken bir kum saati görünür.
- 4 Temporary Internet Files altından, **Ayarlar**'ı tıklayın, sonra **Dosya Görüntüle**'yi tıklayın.
- 5 **Düzen | Tümünü Seç**'i seçin.
- 6 **Dosya | Sil**'i seçin. Tüm dosyaların silinmesi biraz zaman alabilir. Silme işlemleri tamamlandığında, Internet Özellikleri iletişim kutusuna geri dönersiniz.
- 7 **Tamam**'ı tıklayın.

#### **sürüm 7.0**

- 1 Internet Özellikleri iletişim kutusunu açın ve şunlardan birini yapın:
  - Masaüstünde Internet Explorer simgesini sağ tıklayın ve **Özellikler**'i seçin.
  - Windows Denetim Masası'ndan, **Internet Seçenekleri**'ni açın.
- 2 Gözetme geçmişi altından, **Sil**'i tıklayın.
- 3 Temporary Internet Files altından, **Dosya sil**'i tıklayın.

### **Kurulum Reddedildi.**

Bu ileti, başarısız bir Total Protection Service kurulumundan veya kaldırma işleminden sonra görünebilir. Kalmış ürün dosyalarının istemci bilgisayardan kaldırılması gerektiğine işaret eder. MVSUninstall temizleme yardımcı programını kurulum gerektiren bilgisayara yükleyip çalıştırarak bu bileşenleri kaldırın. Bu yardımcı program SecurityCenter ürününün Yardımcı Programlar sayfasındadır.

### **Kurulum Engellendi.**

Genel nedenler ve çözümleri:

- Kurulum başladığınızda, Internet Explorer, Total Protection Service'ı kurmak isteyip istemediğinizi doğrulamanızı isteyen bir iletişim kutusu görüntüler. **Evet**'i tıklamalısınız.
- Kullanıcıların istemci bilgisayarlara koruma hizmetleri yükleyebilmeleri için yönetici hakları olmalıdır. Yoksa, tek başına kurulum ajanı kurulması gerekir.
- Sistem sürücüsünde yeterli boş alan olduğundan emin olmak için sürücüyü kontrol edin. Birden çok koruma türü kurarken, maksimum 50 MB gerekli olabilir.
- Windows sistem dosyası Regedit.exe Windows dizininde bulunmalıdır. Orada yoksa, orijinal Windows kurulum ortamını kullanarak dosyayı değiştirin veya aynı işletim sistemini çalıştıran başka bir bilgisayardan kopyalayın.

### **Geçersiz Yetkilendirme Hatası.**

E-posta iletinizdeki kurulum URL'si eksik veya hatalı biçimlendirilmiş olabilir. URL'yi bütün olarak ve boşluksuz kullandığınızdan ve URL'nin sonundaki şirket anahtarının eksiksiz olduğundan emin

olun. (Şirket anahtarı CK= karakterlerinden sonraki değerdir. Şirket anahtarınızın doğru olduğunu SecurityCenter üzerindeki Hesabım sayfasındaki **Hesaplar ve Anahtarlar** sekmesinde doğrulayabilirsiniz.) URL'yi e-posta iletinizden seçemiyorsanız, Web tarayıcınıza yapıştırmanız gerekebilir.

Bu hata aynı zamanda, deneme değerlendirme süresinin veya aboneliğin sona erdiğini ya da satın aldığınız lisansın daha fazla sayıda bilgisayara koruma kurmayı denediğinizi gösterebilir. Abonelik ve lisanslarınızın durumu hakkında bilgi için SecurityCenter ürününü denetleyin.

### **MyASUtil.SecureObjectFactory hata iletisi.**

SecureObjectFactory Class programı bozulmuş olabilir. Bunu doğrulamak için, SecureObjectFactory Class program dosyasının durumunu denetleyin.

- 1 İnternet Explorer'ı başlatın.
- 2 Araçlar menüsünden **İnternet Seçenekleri**'ni seçin.
- 3 İletişim kutusunun Temporary İnternet Files bölümünde, Ayarlar iletişim kutusunu görüntülemek için **Ayarlar**'ı tıklatın.
- 4 Downloaded Program Files klasörünü açmak için **Nesne Görüntüle**'yi tıklatın.
- 5 SecureObjectFactory Class girdisini bulun. Durum ve Oluşturma Tarihi sütunlarındaki bilgileri not edin:
  - Durum ve tarihler **Bilinmiyor** olarak listelenmişse, SecureObjectFactory Class program dosyasını silin. Dosyayı yeniden yüklemek için Total Protection Service kopyasını kaldırıp tekrar kurun.
  - Durum geçerli tarihlerle birlikte **Yüklü** olarak listeleniyorsa, dosya sağlamdır.
  - Durum sütununda başka bir açıklama varsa, o bilgiyle birlikte ürün destek hizmetlerine başvurun.

**NOT:** Durum sütununu görmüyorsanız, görünüm seçeneklerinizi **Ayrıntılar** olarak değiştirin.

### **MyINX Hatası.**

Yükleyici, bilgisayar üzerinde kaldırılması gereken başka virüs koruma yazılımları algılamıştır.

- 1 Windows Denetim Masası'ndan, **Program Ekle/Kaldır**'ı açın.
- 2 Program listesinden virüs koruma yazılımlarını bulun (Total Protection Service dışındakileri), sonra **Kaldır**'ı tıklatın.
- 3 Kurulum işlemine yeniden başlayın.

Total Protection Service kopyasını kaldırmanıza karşın bu hatayı almaya devam ediyorsanız, kurulum yalnızca kısmen tamamlandığından bazı bileşenler kurulmuş ancak görünmüyor olabilir. MVSUninstall temizleme yardımcı programını kurulum gerektiren bilgisayara yükleyip çalıştırarak bu bileşenleri kaldırın. Bu yardımcı program SecurityCenter ürününün Yardımcı Programlar sayfasındadır.

### **Cab Yükleyici Nesnesi oluşturulamıyor.**

Olası bir neden, MyAgtSvc.exe hizmetinin artık bilgisayarda çalışmamasıdır. Elle yeniden başlatılması gerekir.

- 1 **Başlat | Çalıştır**'ı seçin.
- 2 MyAgtSvc.exe dosyasının yolunu yazın (dosyayı bulmak için **Gözet**'i kullanabilirsiniz) ve /start seçeneğini ekleyin. Örnek: C:\winnt\mycio\agent\myagtsvc.exe /start
- 3 **Tamam**'ı tıklatın.

Bu sorunu çözmezse, ürün destek hizmetlerine başvurun.

**NOT:** Bu bir Microsoft Internet Explorer hatasıdır ve bir Microsoft düzeltme ekinin yüklenmesini gerektirebilir.

## Önceden kurulmuş sürümler ve CD sürümleri için hata iletileri

### Yazılımınızı etkinleştirin.

Total Protection Service kopyanızı etkinleştirmediniz. Etkinleştirilene kadar en son tehditlere karşı güncellemeleri alamazsınız. Etkinleştirmek için, sistem tepeşisindeki Total Protection Service simgesini tıkladın, sonra **Etkinleştir**'i seçin veya bildirim iletişim kutusundaki **Etkinleştir** bağlantısını seçin.

### Yazılımınız güncel değil. En son güncelleştirmeyi almak için lütfen etkinleştirin.

Total Protection Service kopyanızı etkinleştirmediniz. Etkinleştirilene kadar en son tehditlere karşı güncellemeleri alamazsınız. Etkinleştirmek için, sistem tepeşisindeki Total Protection Service simgesini tıkladın, sonra **Etkinleştir**'i seçin veya bildirim iletişim kutusundaki **Etkinleştir** bağlantısını seçin.

### Aboneliğiniz sona erdi, Deneme süreniz doldu, Yazılımınızı yeniden etkinleştirmek için aboneliğinizi yenileyin veya Yazılımınızı yeniden etkinleştirmek için abonelik satın alın.

Önceden kurulmuş bir Total Protection Service kopyası kullanıyorsanız, etkinleştirilmiş deneme sürümünüzün veya önceden kurulmuş aboneliğinizin süresi sona erdi. Sistem tepeşisindeki Total Protection Service simgesini tıkladın ve sonra **Satın Al**'ı veya **Aboneliğinizi yenileyin**'i seçin ya da bildirim iletişim kutusundaki bu bağlantılardan birini seçin.

## Ürün destek hizmetlerine başvurma

Total Protection Service hakkında daha fazla bilgi için ürün destek hizmetlerine başvururken bu görevi kullanın.

### E-posta ile

- Ürün destek hizmetlerine e-posta ile başvurmak için, siparişi verdiğiniz sırada aldığınız Hoş Geldiniz e-postasında servis sağlayıcınızın destek adresini bulun.

### Telefon ile

- Ürün destek hizmetlerinin geçerli telefon numarası listesine erişmek için şu adresi ziyaret edin: <http://www.mcafee.com/us/about/contact/index.html>

### Web üzerinden

- 1 Kullanıcı adı ve parolanızla SecurityCenter oturumu açın. Bunlar, Hoş Geldiniz e-postasında size gönderilmiştir.
- 2 **Yardım** sekmesini tıkladın.
- 3 Desteğe Başvur bölümünde, bir seçenek belirleyin:
  - **Çevrimiçi destek** — Sorununuzun açıklamasını destek temsilcisine gönderebileceğiniz bir formu görüntüler.

- **Telefonla Destek** — Hesabınız, lisans numaranız ve telefon numaranızla ilgili bilgileri görüntüler.

# Dizin

## A

- abonelikler, satın alma ve yenileme [28](#)
- aboneliklerin yenilenmesi [28](#)
- ActiveX denetimleri, zorla yükleme ve [21](#), [24](#)
- admin\$ paylaşımı [33](#)
- aktarma sunucuları
  - genel bakış [11](#)
  - sessiz kurulum ve [20](#)
  - zorla yükleme ve [25](#)

## B

- bildirimler, işletim sistemi desteği hakkında [8](#)
- birden çok hesap, birleştirme [5](#)

## C

- CHAP proxy'si [12](#)

## D

- davranış engelleme kuralları [31](#)
- deneme sürümü aboneliği
  - etkinleştirme [27](#)
  - gereksinimleri [27](#)
  - lisans anahtarı olmadığına oluşturma [29](#)
  - tam aboneliğe dönüştürme [28](#)
- deneme sürümünü tam aboneliğe dönüştürme [28](#)
- destek hizmetlerine başvurma [36](#)
- destek, başvurma [36](#)
- desteklenmesi
  - aktarma sunucuları [11](#)
  - işletim sistemleri [6](#)
  - işletim sistemleri, sona erme [8](#)
  - Windows güvenlik duvarı [11](#)
- disk alanı gereksinimleri [33](#)

## E

- e-posta adresleri
  - birden çok hesap ve [5](#)
  - kurulum sırasında girme [18](#)
  - raporlardaki iş istasyonlarını tanımak için [31](#)
  - sipariş verirken girme [5](#)
- e-posta koruması, kurulum gereksinimleri [9](#)
- e-posta sunucusu koruması, kurulum gereksinimleri [9](#)
- e-posta taramaları (virüs ve casus yazılımdan koruma), isteğe bağlı tarama [30](#)
- EICAR test virüsü [29](#)
- engelleme kuralları
  - davranış engelleme kuralları [31](#)
  - erişim koruma kuralları [31](#)
- erişim koruma kuralları [31](#)

## G

- gereksinimler
  - boş disk alanı [33](#)
  - CD sürümleri [26](#)
  - e-posta koruması [9](#)
  - e-posta sunucusu koruması [9](#)
  - işletim sistemi [6](#)
  - önceden kurulmuş yazılım [26](#)
  - RAM [8](#)
  - sessiz kurulum [19](#)
  - tarayıcı, SecurityCenter'ı görüntülemek için [5](#), [14](#)
  - tarayıcı, Total Protection Service kurmak için [6](#), [14](#)
  - URL kurulumu [17](#)
  - Windows güvenlik duvarı ve yönetim bilgisayarı [24](#)
  - zorla yükleme [24](#)
- GroupShield, bakınız: E-posta sunucusu koruması
- grup kimliği, konumu [20](#)
- güncellemeler
  - etkinleştirme ve [27](#)
  - ilk ağ algılaması ve [27](#)
  - proxy sunucu ve [12](#)
- güvenlik ayarları, Internet Explorer [14](#)
- güvenlik duvarı
  - devre dışı bırakma [11](#)
  - kurma [11](#)
  - kurumsal, destek [12](#)
  - varolan güvenlik duvarı yazılımını kaldırma [13](#)
  - varsayılan [11](#)
  - Windows 7 [11](#), [13](#), [24](#)
  - Windows ve yönetim bilgisayarı [24](#)
  - Windows Vista [11](#), [13](#), [24](#)
  - Windows XP [11](#), [13](#), [24](#)
- güvenlik duvarı koruması
  - varolan güvenlik duvarı yazılımını kaldırma [13](#)
  - Windows güvenlik duvarı ve [11](#), [24](#)

## H

- hata iletileri [33](#)
- hedef bilgisayarlar
  - tanımı [21](#)
  - zorla yükleme gereksinimleri [24](#)
  - zorla yüklemeyen sonra yeniden başlatma [25](#)
- hesap kayıt anahtarı
  - görüntüleme veya oluşturma [28](#)
  - tanımı [28](#)
- hesaplar
  - birden çok hesabı birleştirme [5](#)
  - varolan hesaba katılma [27](#)
  - yeni hesap oluşturma [27](#)
- hesapları ve siparişleri birleştirme [5](#)
- hızlı kullanıcı değiştirme, desteği [12](#)
- hoş geldiniz e-postası [5](#)

**I**

## Internet Explorer

- güvenlik ayarlarını yapılandırma 14
- önbellek, boşaltma 33

**İ**

## isteğe bağlı taramalar

- e-posta (virüs ve casus yazılımdan korunma) 30
- istemci bilgisayarlar 30

## istemci bilgisayarlar

- kurulumdan sonra Outlook Gelen Kutusu'nu tarama 30
- kurulumdan sonra tarama 30
- lisans anahtarı olmadığına koruma 29
- standart URL kurulumu gereksinimleri 17
- zorla yükleme gereksinimleri 24

## istemci bilgisayarlar için yeniden başlatma

- sessiz kurulumdan sonra 19
- zorla yüklemeyen sonra 25

## istemci işletim sistemi için yükseltmeler 6, 31

## istemci yazılımı

- kurulum yöntemleri 16
- kurulumunu test etme 29
- sessiz kurulumla kurma 18, 19
- zorla yükleyerek kurma 21, 25

## istemci yazılımını etkinleştirme

- avantajları 27
- yönergeleri 27

## iş istasyonlarının raporlarda tanınması 31

## işletim sistemleri

- admin\$ paylaşımı 33
- desteğin sona ermesi 8
- desteklenmesi 6
- Dosya ve Yazıcı Paylaşımı 33
- e-posta sunucusu koruması gereksinimleri 9
- Windows Home Server 7
- yükseltme 6, 31
- yükseltme, ve Total Protection Service 31
- zorla yükleme gereksinimleri 24

**K**

## kaldırılması

- önceki kurulumlardan dosyalar 33
- Push Install yardımcı programı 26
- varolan güvenlik duvarı yazılımı 13
- varolan virüs koruma yazılımı 13, 33

## kaldırma

- önceki kurulumlardan dosyalar 33
- Push Install yardımcı programı 26
- sorun giderme 33
- varolan güvenlik duvarı yazılımı 13
- varolan virüs koruma yazılımı 13, 33

## kimlik doğrulama, destek 12

## Kullanıcı Hesabı Denetimi iletişim kutusu 18

## kurulum

- boş disk alanı gerekli 33
- desteklenen tarayıcılar 14
- e-posta adresi girme 18
- gereksinimler 6
- Kullanıcı Hesabı Denetimi iletişim kutusu 18
- kurumsal ağ güvenlik duvarı ve 12
- lisans anahtarı olmadan 29
- önceden kurulmuş veya CD'deki yazılımlar için gereksinimler 26
- proxy sunucu ve 12
- sessiz, genel bakış 18
- tanımlama bilgileri ve 18

kurulum (*devamı*)

- tek başına kurulum ajanı 14
- test etme 29
- URL, genel bakış 17
- varolan güvenlik duvarı yazılımını kaldırma 13
- varolan virüs koruma yazılımını kaldırma 13
- Windows Home Server desteği 7
- yanıt vermiyor 31
- yönetici hakları 14
- yönetici hakları olmayan kullanıcılar 14
- yöntemleri 16
- zorla, genel bakış 21
- kurulum için tarayıcı yapılandırması 14
- kurulum URL'si, edinme 16
- kurulum araçları
  - sessiz kurulum için 19
  - tek başına kurulum ajanı için 14

**L**

## lisans anahtarı, etkinleştirme 29

## lisans numarası 5, 36

## lisanslar

- lisans satın alırken bilgisayarları koruma 29
- yenileme 28

## Lotus Domino 9

**M**

## Microsoft Exchange Server 9

## Microsoft olmayan tarayıcılar 14

## MVSUninst yardımcı programı 33

**N**

## NTLM proxy'si 12

**O**

## otomatik güncellemeler

- etkinleştirme ve 27
- proxy sunucular ve 12

## oturum açma kimlik bilgileri 5

## Outlook Gelen Kutusu, tarama 30

**Ö**

## önceden kurulmuş yazılım

- etkinleştirme 27
- gereksinimleri 26
- kurma 27

## özel URL, oluşturma 17

**P**

## Program Ekle/Kaldır

- diğer güvenlik duvarı programlarını kaldırma 13
- diğer virüs korumasını kaldırma 13, 33
- Push Install yardımcı programını kaldırma 26

## proxy sunucuları 12

## Push Install yardımcı programı

- edinme 25
- kaldırma 26

**R**

## RAM gereksinimleri 8

## raporlar, içinde bilgisayarları tanıma 18

## regedit.exe, sistem dosyası 33

**S**

- SecurityCenter
  - oturum açma kimlik bilgileri 5
  - tarayıcı gereksinimleri 5, 14
- sessiz kurulum
  - aktarma sunucuları etkinleştirme/devre dışı bırakma 20
  - genel bakış 16, 18
  - gereksinimleri 19
  - kuruluş araçları 19
  - proxy sunucu ve 12
  - şema 18
  - şirket anahtarı 19
  - VSETUP parametreleri 20
  - yordam 19
- siparişler, birden çoğunu birleştirme 5
- sorun giderme
  - boş disk alanı 33
  - ekleme, lisansları yenileme 32
  - engelleme kuralları ve kurulum 31
  - kurulum 31
  - önceki kurulumdan dosyaları kaldırma 33
  - regedit.exe, eksik sistem dosyası 33
  - varolan virüs koruma yazılımını kaldırma 33
  - yönetici hakları olmadan kurma 31
- sunucular
  - e-posta sunucusu koruması gereksinimleri 9
  - istemci yazılımı kurulumunun gereksinimleri 6

**Ş**

- şirket anahtarı
  - bulma 19
  - kurulum ve 19

**T**

- tam abonelik satın alma 28
- tanımlama bilgileri, kurulum için gereken 18
- taramalar
  - istemci bilgisayarlar, istemci yazılım kurulduktan sonra 30
  - Outlook Gelen Kutusu, istemci yazılım kurulduktan sonra 30
  - sonuçları görüntüleme 30
- tarayıcı
  - e-posta sunucusu koruması gereksinimleri 9
  - güvenlik ayarları 14
  - kurulum için yapılandırma 14
  - Microsoft olmayan 14
  - önbelleği temizleme 33
  - SecurityCenter'ı görüntüleme 5, 14
  - Total Protection Service kurma gereksinimleri 6
- tek başına kurulum ajanı
  - kurma 14
  - yükleme 14
- teknik destek, başvurma 36
- temizleme yardımcı programı 33
- temizleme, önceki kurulumlardaki dosyaları 33
- Temp dizini, sorun giderme 31
- terminal sunucular, desteği 12

**U**

- URL kurulumu
  - genel bakış 17
  - gereksinimleri 17
  - Kullanıcı Hesabı Denetimi iletişim kutusu 18
  - kullanıcılara URL gönderme 17

**URL kurulumu (devamı)**

- özel URL oluşturma 17
- sorun giderme 31
- tanımlama bilgileri ve 18
- URL'yi edinme 16
- yordam 18

**Ü**

- ürün destek hizmetleri, başvurma 36

**V**

- varolan hesaba katılma 27
- varsayılan güvenlik duvarı 11
- virüs koruma özelliğini test etme 29
- virüs koruma uygulamaları, kaldırılması 13
- virüs koruma uygulamaları, kaldırma 33
- virüs ve casus yazılımdan korunma
  - kurulumdan sonra istemci sürücülerini tarama 30
  - kurulumdan sonra Outlook Gelen Kutusu'nu tarama 30
  - varolan virüs koruma yazılımını kaldırma 13
  - virüs korumasını test etme 29
- VSETUP parametreleri 20
- VSETUP yardımcı programı
  - aktarma sunucuları etkinleştirme/devre dışı bırakma 20
  - gereksinimleri 19
  - komut satırı parametreleri 20
  - tanımı 18
  - yükleme 19

**Y**

- yardımcı programlar
  - MVSUninst 33
  - Push Install yardımcı programı 21, 25
  - tek başına kurulum ajanı, tanımı 14
  - temizleme yardımcı programı 33
  - VSETUP, tanımı 18
- yazılımın CD sürümü
  - etkinleştirme 27
  - gereksinimleri 26
- yeni hesap oluşturma 27
- yönetici hakları
  - istemci yazılımı kurulumu ve 14, 17, 19
  - terminal sunucular ve 12
- yönetici hakları, etki alanı, zorla yükleme ve 24
- yönetim bilgisayarları
  - Push Install yardımcı programını kaldırma 26
  - tanımı 21
  - zorla yükleme gereksinimleri 24
- yükleme URL'si, edinme 16

**Z**

- zorla yükleme
  - ActiveX denetimleri 21, 24
  - aktarma sunucularını etkinleştirme 25
  - genel bakış 16, 21
  - gereksinimler 24
  - hedef bilgisayarlar 21
  - proxy sunucu ve 12
  - sonrasında istemci bilgisayarları yeniden başlatma 25
  - şema 21
  - yordam 25
  - yönetim bilgisayarları 21
  - zamanlamada dikkat edilecekler 23