HP ProtectTools
Kullanıcı Kılavuzu

Birinci Basım: Kasım 2009

Belge Parça Numarası: 593308-141

İçindekiler

1 Güvenlik konusuna giriş

HP ProtectTools Security Manager (HP ProtectTools Güvenlik Yöneticisi) yazılımı, bilgisayar, ağ ve kritik verilere yetkisiz erişime karşı koruma sağlamaya yardımcı olan güvenlik özellikleri sağlar. HP ProtectTools Security Manager (HP ProtectTools Güvenlik Yöneticisi) yazılımının yönetimi Administrative Console (Yönetim Konsolu) özelliğiyle sağlanır.

Yerel yönetici, HP ProtectTools Administrative Console'u kullanarak aşağıdaki görevleri gerçekleştirebilir:

- Güvenlik özelliklerini etkinleştirme veya devre dışı bırakma
- Kendilerinin ve bu bilgisayarın diğer kullanıcılarının parmak izlerini kaydetme
- Yüzden kimlik tanıma için bir veya daha fazla görünüm kaydetme
- Kimlik doğrulaması için akıllı kart ayarlama
- Kimlik doğrulaması için gerekli kimlik bilgilerini belirtme
- Bilgisayar kullanıcılarını yönetme
- Aygıta özel parametreleri ayarlama
- Yüklü Security Manager (Güvenlik Yöneticisi) uygulamalarını yapılandırma
- Diğer Security Manager (Güvenlik Yöneticisi) uygulamalarını ekleme

Genel kullanıcılar, Security Manager panosunu kullanarak aşağıdaki görevleri gerçekleştirebilir:

- Bir yönetici tarafından sağlanan seçenekleri yapılandırmak
- Bazı HP ProtectTools modüllerinin sınırlı denetimine izin vermek

Bilgisayarınızda kullanılabilecek yazılım modülleri bilgisayar modelinize göre değişir.

HP ProtectTools yazılım modülleri önceden yüklenebilir veya HP Web sitesinden indirilebilir. Daha fazla bilgi için http://www.hp.com adresini ziyaret edin.

NOT: Bu kılavuzdaki yönergelerde, uygun HP ProtectTools yazılım modüllerini bilgisayarınıza yüklemiş olduğunuz varsayılmaktadır.

HP ProtectTools özellikleri

Aşağıdaki tablo, HP ProtectTools modüllerinin anahtar özelliklerini ayrıntılı olarak belirtir.

Modül	Ana özellikler
HP ProtectTools Security Manager Administrative Console (yöneticiler için)	• Security Manager Kurulum Sihirbazı'nı kullanarak güvenlik düzeylerini ve güvenli oturum açma yöntemlerini ayarlayın ve yapılandırın. • Temel kullanıcılardan gizlenen seçenekleri yapılandırın. • Device Access Manager yapılandırmalarını ve kullanıcı erişimini yapılandırın. • Yönetici araçlarını kullanarak HP ProtectTools kullanıcıları ekleyip çıkarın ve kullanıcı durumunu görüntüleyin.
HP ProtectTools Security Manager (genel kullanıcılar için)	• Kullanıcı adlarını ve parolalarını düzenleyin, ayarlayın ve değiştirin. • Windows parolası ve Smart Card gibi kullanıcı kimlik bilgilerini yapılandırın ve değiştirin. • File Sanitizer Shred, Bleaching ve Settings ayarlarını yapılandırın ve değiştirin. • Device Access Manager ayarlarını görüntüleyin. • Preferences ve Backup and Restore seçeneklerini yapılandırın.
Credential Manager for HP ProtectTools (Password Manager)	• Adlarınızı ve parolalarınızı kaydedin, düzenleyin ve koruyun. • Web sitelerinin ve programların oturum açma ekranlarını hızlı ve güvenli erişim için ayarlayın. • Web sitesi kullanıcı adlarını ve parolalarını Password Manager'a girerek kaydedin. Bu siteyi sonraki ziyaretinizde, Password Manager bilgileri otomatik olarak doldurup gönderecektir. • Daha fazla hesap güvenliği için daha güçlü parolalar oluşturun. Password Manager bilgileri otomatik olarak doldurup gönderir.
HP ProtectTools için Drive Encryption (Sürücü Şifreleme) (yalnızca belirli modellerde)	• Eksiksiz, tüm birimi kapsayan sabit sürücü şifrelemesi sağlayın. • Veri şifrelemesini çözmek ve verilere erişmek için önyükleme öncesi kimlik doğrulamasını zorunlu kılın.
HP ProtectTools için Privacy Manager (Gizlilik Yöneticisi) (yalnızca belirli modellerde)	• E-posta, Microsoft® Office belgeleri veya anlık ileti (IM) iletişiminin kaynağını, doğruluğunu ve güvenliğini doğrulamak için gelişmiş oturum açma tekniklerini kullanın.
HP ProtectTools için File Sanitizer (Dosya Temizleyici)	• Bilgisayarınızdaki dijital varlıklarınızı (uygulama dosyaları, geçmiş veya Web'le ilişkili içerik dahil hassas bilgiler veya diğer gizli veriler) parçalayın ve sabit sürücüyü düzenli olarak temizleyin.
HP ProtectTools için Device Access Manager (Aygıt Erişim Yöneticisi) (yalnızca belirli modellerde)	• BT yöneticilerinin aygıtlara erişimi kullanıcı profilleri bazında denetlemesini sağlayın. • Yetkisiz kullanıcıların, harici depolama ortamı kullanarak verileri silmesini ve harici ortamdan sisteme virüs bulaştırmasını engelleyin. • Yöneticilerin, belirli şahısların veya kullanıcı gruplarının yazılabilir aygıtlara erişimini devre dışı bırakmasına imkan verin.

Ana güvenlik hedeflerine ulaşma

HP ProtectTools modülleri, aşağıdaki ana güvenlik hedefleri dahil, güvenlikle ilgili çok çeşitli sorunlara çözüm sunmak üzere birlikte kullanılabilir:

- Hırsızlığa karşı koruma
- Önemli verilere erişimi kısıtlama
- Dahili veya harici konumlardan yapılan izinsiz erişimleri engelleme
- Güçlü parola kuralları oluşturma

Hedefli hırsızlığa karşı koruma

Hedefli hırsızlığa örnek olarak, havaalanı güvenlik denetim noktasında bulunan ve gizli veriler ile müşteri bilgilerini içeren bir bilgisayarın çalınması verilebilir. Şu özellikler hedefli hırsızlığa karşı korunmaya yardımcı olur:

- Önyükleme kimlik doğrulaması özelliği etkinleştirildiğinde, işletim sistemine erişimi engellemeye yardımcı olur. Aşağıdaki yordamlara bakın:
  - Security Manager (Güvenlik Yöneticisi)
  - Drive Encryption (Sürücü Şifreleme)

Hassas verilere erişimi kısıtlama

Bir sözleşme denetçisi sahada çalışırken kendisine hassas finansal verileri incelemesi için bilgisayar erişimi veriliyor; ancak denetçinin dosyaları yazdırabilmesini veya CD gibi yazılabilir bir aygıta kaydetmesini istemiyorsunuz. Şu özellik veri erişiminin kısıtlanmasına yardımcı olur:

- HP ProtectTools için Device Access Manager (Aygıt Erişim Yöneticisi), hassas bilgilerin yazdırılamamasını veya sabit sürücüden çıkarılabilir medyaya kopyalanamamasını sağlamak için BT yöneticilerinin yazılabilir aygıtlara erişimi kısıtlamasına izin verir.

Dahili veya harici konumlardan yapılan izinsiz erişimleri engelleme

Güvenli olmayan iş bilgisayarına yetkisiz erişim, finans bölümlerinden, bir yöneticiden veya AR-GE grubundan gelen bilgiler gibi şirket ağı kaynakları ve hasta kayıtları veya kişisel mali kayıtlar gibi özel bilgiler için oldukça hassas bir risk oluşturur. Aşağıdaki özellikler izinsiz erişimi engellemeye yardımcı olur:

- Önyükleme kimlik doğrulaması özelliği etkinleştirildiğinde, işletim sistemine erişimi engellemeye yardımcı olur. Aşağıdaki yordamlara bakın:
  - Password Manager (Parola Yöneticisi)
  - Drive Encryption (Sürücü Şifreleme)
- Password Manager (Parola Yöneticisi), yetkisiz bir kullanıcının parolaları alamamasını veya parolayla korunan uygulamalara erişememesini sağlar.
- HP ProtectTools için Device Access Manager (Aygıt Erişim Yöneticisi), hassas bilgilerin sabit sürücüden kopyalanamamasını sağlamak için BT yöneticilerinin yazılabilir aygıtlara erişimi kısıtlamasına izin verir.

- File Sanitizer, kritik dosyaları ve klasörleri parçalayarak veya sabit sürücüyü temizleyerek (silinmiş ancak halen kurtarılabilir olan verilerin üzerine yazdırma) güvenli veri silmeye imkan verir.
- DriveLock, sabit sürücü çıkarılıp korumasız bir sisteme takılsa da verilere erişilememesini sağlar.

Güçlü parola oluşturma ilkeleri

Onlarca Web tabanlı uygulama ve veritabanı için güçlü parola kullanımı ilkesini gerekli kılan bir zorunluluk ortaya çıkarsa, Security Manager (Güvenlik Yöneticisi) parolalar için korunan bir depo ve Single Sign On (Tekli Oturum Açma) rahatlığı sağlar.

Ek güvenlik unsurları

Güvenlik rolleri atama

Bilgisayar güvenliğini yönetirken (özellikle büyük ölçekli şirketlerde), göz önünde tutulması gereken önemli bir nokta da sorumlulukları ve yetkileri çeşitli yönetici ve kullanıcı türleri arasında paylaştırmaktır.

NOT: Küçük ölçekli bir işletmede veya bireysel kullanımda bu rollerin tümü aynı kişi tarafından yönetilebilir.

HP ProtectTools uygulamasında güvenlikle ilgili görevler ve ayrıcalıklar şu rollere bölünebilir:

- Güvenlik yetkilisi — Şirketin veya ağın güvenlik düzeyini tanımlar ve dağıtılacak güvenlik özelliklerini (örneğin, Java™ Kartları, biyometrik okuyucular veya USB belirteçleri) belirler.

  NOT: HP ProtectTools uygulamasındaki birçok özellik, HP ile işbirliği içinde güvenlik yetkilisi tarafından özelleştirilebilir. Daha fazla bilgi için http://www.hp.com adresindeki HP Web sitesine bakın.

- Yönetici—Güvenlik personeli tarafından tanımlanmış güvenlik özelliklerini uygular ve yönetir. Ayrıca bazı işlevleri etkinleştirip devre dışı bırakabilir. Örneğin, güvenlik personeli Java Kartlarının dağıtılmasına karar vermişse, BT yöneticisi Java Kartı BIOS güvenlik modunu etkinleştirebilir.

- Kullanıcı — Güvenlik özelliklerini kullanır. Örneğin, güvenlik yetkilisi ve BT yöneticisi sistem için Java Kartları'nı etkinleştirmişse, kullanıcı Java Kartı PIN numarasını ayarlayabilir ve kimlik doğrulaması için kartı kullanabilir.

DİKKAT: Yöneticilerin, son kullanıcı ayrıcalıklarını kısıtlarken ve kullanıcı erişimini kısıtlarken "en iyi uygulamaları" izlemeleri önerilir.

Yetkisiz kullanıcılara yönetimsel ayrıcalıklar verilmemelidir.

HP ProtectTools parolalarını yönetme

HP ProtectTools Security Manager (HP ProtectTools Güvenlik Yöneticisi) özelliklerinin çoğu parolalarla korunur. Aşağıdaki tabloda yaygın şekilde kullanılan parolalar, parolanın ayarlandığı yazılım modülü ve parola işlevi listelenmiştir.

Bu tabloda yalnızca BT yöneticileri tarafından ayarlanan ve kullanılan parolalar belirtilmiştir. Diğer tüm parolalar normal kullanıcılar veya yöneticiler tarafından ayarlanabilir.

HP ProtectTools parolası	Aşağıdaki modülde ayarlanır	İşlev
Windows Oturum Açma parolası	Windows® Denetim Masası veya HP ProtectTools Security Manager (HP ProtectTools Güvenlik Yöneticisi)	Çeşitli Security Manager (Güvenlik Yöneticisi) özelliklerine erişmek üzere elle oturum açmak ve kimlik doğrulaması yapmak amacıyla kullanılabilir.
Security Manager Backup and Recovery (Güvenlik Yöneticisi Yedekleme ve Kurtarma) parolası	Security Manager (Güvenlik Yöneticisi), tek kullanıcı için	Security Manager Backup and Recovery (Güvenlik Yöneticisi Yedekleme ve Kurtarma) dosyasına erişimi korur.
Java™ Kartı PIN'i	Java Kartı Güvenliği	Java Kartı içeriğine erişimi korur ve Java Kartı kullanıcılarının kimlik doğrulamasını yapar. Açılış kimlik doğrulaması için kullanıldığında, Java Kartı PIN'i de

HP ProtectTools parolası	Aşağıdaki modülde ayarlanır	İşlev
		Computer Setup (Bilgisayar Kurulumu) yardımcı programına ve bilgisayar içeriğine erişimi korur. Java Kartı belirteci seçilmişse, Drive Encryption'ı (Sürücü Şifreleme) kullananların kimlik doğrulamasını yapar.

Güvenli parola oluşturma

Parola oluştururken, önce programın yönergelerini izlemelisiniz. Ancak genel olarak, tahmin edilmesi zor parolalar oluşturmanıza yardımcı olacak şu noktaları göz önünde bulundurun:

- 6 veya 8 karakterden daha uzun parolalar kullanın. Önerilen parolalar 8 karakterden uzun olanlardır.
- Parolada büyük ve küçük harf karışımlarını kullanın.
- Mümkünse alfasayısal karakterleri de kullanın, hatta özel karakterler ve noktalama işaretleri kullanın.
- Bir anahtar sözcükteki harfler için özel karakterleri veya sayıları kullanın. Örneğin, I veya L harfleri için 1 sayısını kullanabilirsiniz.
- 2 veya daha fazla dilden aldığınız sözcükleri birleştirin.
- Bir sözcüğün veya ifadenin arasına sayılar veya özel karakterler yerleştirin. Örneğin, “Mutlu2-2Kedi45.”
- Sözlükteki sözcükleri parola olarak kullanmayın.
- Tersten de yazacak olsanız, adınızı veya kişisel herhangi bir bilginizi (örneğin, doğrum tarihi, evcil hayvan adları veya anne kızlık soyadı) parola olarak kullanmayın.
- Parolanızı belirli aralıklarla değiştirin. Yalnızca birkaç karakterini de değiştirebilirsiniz.
- Parolanızı bir kağıda yazdıysanız, bilgisayara çok yakın olan ve görünen yerlerde tutmayın.
- Parolaları bilgisayarda e-posta gibi dosyalara kaydetmeyin.
- Hesaplarınızı başkalarıyla ortak kullanmayın veya parolanızı başkasına söylemeyin.

HP ProtectTools kimlik bilgilerini yedekleme ve geri yükleme

HP ProtectTools kimlik bilgisi verilerini ve ayarlarını, HP ProtectTools'un Backup and Restore özelliğini kullanarak seçebilir ve yedekleyebilirsiniz.

2 Kurulum Sihirbazı'na başlarken

HP ProtectTools Kurulum Sihirbazı, Security Manager'ın en sık kullanılan özelliklerinin kurulumunda size yol gösterir. Ancak, HP ProtectTools Administrative Console üzerinden kullanılabilen çok sayıda ek işlev vardır. Ek güvenlik özelliklerinin yanı sıra sihirbazda bulunan aynı ayarlar, Windows® Başlat menüsünden erişim sağlanan konsol üzerinden yapılandırılabilir. Bu ayarlar, bilgisayar ve bilgisayarı paylaşan tüm kullanıcılar için geçerlidir.

1. Bilgisayar kurulduktan bir hafta sonra, oturum açtığınızda veya yönetici haklarına sahip bir kullanıcı ilk kez parmağını parmak izi okuyucudan geçirdiğinde, Security Manager Kurulum Sihirbazı, programı yapılandırmaya yönelik temel adımlarda size yol göstermek üzere otomatik olarak başlayacaktır. Bilgisayarı kurmaya yönelik bir video eğitimi otomatik olarak başlar.

   – veya –

   Windows Kenar Çubuğu'ndaki **Araç** simgesinden veya görev çubuğunun en sağında yer alan bildirim alanındaki görev çubuğu simgesinden HP ProtectTools Security Manager'ı açın.

   

   Araç simgesinin üst çubuğunun rengi aşağıdaki durumlardan birini belirtir:

   - Kırmızı—HP ProtectTools ayarlanmamıştır veya ProtectTools modüllerinden birinde bir hata durumu söz konusudur.
   - Sarı—Yapılması gereken ayar değişiklikleri için Security Manager'da Applications Status sayfasını denetleyin.
   - Mavi—HP ProtectTools ayarlanmış ve düzgün çalışır durumdadır.

   NOT: Araç simgesi, Windows XP işletim sisteminde bulunmamaktadır.

   – veya –

Başlat'ı tıklatın, **Tüm Programlar**'ı tıklatın, ardından **HP ProtectTools Administrative Console**'u tıklatın.

2. “Welcome” (Hoş Geldiniz) ekranını okuduktan sonra **Next**'i (İleri) tıklatın.

NOT: Welcome (Hoş Geldiniz) ekranında, seçeneklerden birini belirleyerek sihirbazın artık görüntülenmemesini sağlayabilirsiniz.

3. Kurulum Sihirbazı sizden kimliğinizi doğrulamanızı ister.

   Windows parolanızı girin veya parmak izi okuyucu ile parmak izlerinizi taratın, sonra da **Next**'i (İleri) tıklatın.

   Parmak izi okuyucu veya akıllı kart yoksa, Windows parolanızı girmeniz istenir. İleride kimlik doğrulamasının gerektiği durumlarda bu parolayı kullanmalısınız.

   Henüz bir Windows parolası oluşturmadıysanız, bir tane oluşturmanız istenir. Windows parolası, Windows hesabınızı yetkisiz kişilerin erişiminden korumak ve HP ProtectTools Security Manager özelliklerini kullanmak için gereklidir.

4. Kurulum Sihirbazı, bilgisayarın tüm kullanıcıları için geçerli olan güvenlik özelliklerini ayarlama işleminde size yol gösterecektir:

   - Windows Logon Security, Windows hesaplarınızı, erişim için belirli kimlik bilgileri kullanımını gerektirerek korur.
   - Drive Encryption, uygun yetkiye sahip olmayanların bilgileri okuyamayacağı şekilde sabit sürücülerinizi şifreleyerek verilerinizi korur.
   - Pre-Boot Security, Windows başlatılmadan önce yetkisiz kişilerin erişimini yasaklayarak bilgisayarınızı korur.

     NOT: BIOS'unuz tarafından desteklenmiyorsa Pre-Boot Security kullanılamaz.

   Bir güvenlik özelliğini etkinleştirmek için, onay kutusunu seçin. Ne kadar çok özellik seçerseniz, bilgisayarınız o kadar güvenli hale gelir.

5. Sihirbazın son sayfasında **Finish**'i (Son) tıklatın.

   Security Manager panosu görüntülenir.

NOT: Sihirbazı tamamlamazsanız, otomatik olarak iki kez daha başlatılır. Bunun ardından, kurulum tamamlanana kadar sihirbaza görev çubuğunun en sağında, bildirim alanındaki bildirim balonundan erişebilirsiniz (devre dışı bırakmadıysanız).

3 HP ProtectTools Security Manager Administrative Console

HP ProtectTools Security Manager'ın yönetimi Administrative Console üzerinden sağlanır.

NOT: HP ProtectTools'un yönetimi, yönetici ayrıcalıkları gerektirir.

Konsol, aşağıdaki özellikleri sağlar:

- Güvenlik özelliklerini etkinleştirme veya devre dışı bırakma
- Bilgisayar kullanıcılarını yönetme
- Aygıta özel parametreleri ayarlama
- Security Manager uygulamalarını yapılandırma
- Diğer Security Manager uygulamalarını ekleme

▲ HP ProtectTools Security Manager uygulamalarını kullanmak için, Başlat menüsünden HP ProtectTools Security Manager'ı başlatın veya görev çubuğunun en sağında bulunan bildirim alanındaki Security Manager simgesini sağ tıklatın.

HP ProtectTools Administrative Console ve tüm uygulamaları bu bilgisayarı paylaşan tüm kullanıcılar tarafından kullanılabilir.

Administrative Console'u açma

Sistem ilkelerini ayarlama veya yazılımı yapılandırma gibi yönetim görevleri için, konsolu aşağıda anlatılan şekilde açın:

- **Başlat**'ı tıklatın, **Tüm Programlar**'ı tıklatın, **HP**'yi ve ardından **HP ProtectTools Administrative Console**'u tıklatın.

  – veya –

  Security Manager'ın sol panelinde **Administration**'ı (Yönetim) tıklatın.

Parmak izlerini kaydettirme veya Security Manager'ı kullanma gibi kullanıcı görevleri için, aşağıdaki yolu izleyerek konsolu açın:

- **Başlat**'ı tıklatın, **Tüm Programlar**'ı tıklatın, **HP**'yi ve ardından **HP ProtectTools Security Manager**'ı tıklatın.

  – veya –

  Görev çubuğunun en sağındaki bildirim alanında bulunan **HP ProtectTools Security Manager** simgesini çift tıklatın.

Administrative Console'u kullanma

HP ProtectTools Security Manager'ın yönetilmesi için merkezi konum Security Manager Administrative Console'dur.

Konsol şu bileşenlerden oluşur:

- **Tools** (Araçlar)—Bilgisayarınızda güvenliği yapılandırmak için şu kategorileri görüntüler:
  - **Home** (Giriş)—Gerçekleştirilecek güvenlik görevlerini seçmenize olanak tanır.
  - **System** (Sistem)—Güvenlik özelliklerini ve kullanıcılar ile aygıtlara yönelik yetkileri yapılandırmanıza olanak tanır.
  - **Applications** (Uygulamalar)—HP ProtectTools Security Manager ve Security Manager uygulamalarının genel ayarlarını görüntüler.
  - **Data** (Veri)—Verilerinizi koruyan Security Manager uygulamalarının bağlantılarını içeren genişleyen bir menü sağlar.
- **Management Tools** (Yönetim Araçları)—Ek araçlarla ilgili bilgiler sağlar. Panel şu tercihleri görüntüler:
  - **HP ProtectTools Security Manager Setup Wizard** (HP ProtectTools Security Manager Kurulum Sihirbazı)—HP ProtectTools Security Manager'ın kurulması sırasında size yol gösterir.
  - **Help** (Yardım)—Security Manager ile önceden yüklenmiş uygulamaları hakkında bilgi sağlayan bu Help (Yardım) dosyasını görüntüler. Ekleyebileceğiniz uygulamalara yönelik yardım, söz konusu uygulamaların içinde sağlanmıştır.
  - **About** (Hakkında)—HP ProtectTools Security Manager hakkında, sürüm numarası ve telif hakkı bildirimi gibi bilgileri sağlar.
- **Main area** (Ana alan)—Uygulamaya özel ekranları görüntüler.

4 Sisteminizi yapılandırma

System (Sistem) grubuna, HP ProtectTools Administrative Console (HP ProtectTools Yönetim Konsolu) ekranının sol tarafındaki Tools (Araçlar) menü panelinden erişilebilir. Bu gruptaki uygulamaları, bilgisayarın ilkelerini ve ayarlarını, kullanıcılarını ve aygıtlarını yönetmek üzere kullanabilirsiniz.

Şu uygulamalar System (Sistem) grubuna dahildir:

- **Security** (Güvenlik)—Özellikleri, kimlik doğrulamasını ve kullanıcıların bu bilgisayarla nasıl etkileşimde bulunduğunu belirleyen ayarları yönetin.
- **Users** (Kullanıcılar)—Bu bilgisayarın kullanıcılarını ayarlayın, yönetin ve kaydettirin.
- **Devices** (Aygıtlar)—Bilgisayardaki yerleşik veya bağlı güvenlik aygıtlarının ayarlarını yönetin.

Bilgisayarınız için kimlik doğrulamasını ayarlama

Authentication (Kimlik Doğrulaması) uygulaması içinde, bu bilgisayarda hangi güvenlik özelliklerinin uygulanması gerektiğini seçebilir, bilgisayar erişimini yöneten ilkeler belirleyebilir ve ek gelişmiş ayarlar yapılandırabilirsiniz. Windows'da oturum açma veya bir kullanıcı oturumu sırasında Web siteleri ve programlarda oturum açma işleminde her kullanıcı sınıfının kimlik doğrulamasını gerçekleştirmek için gerekli kimlik bilgilerini belirtebilirsiniz.

Bilgisayarınızda kimlik doğrulaması ayarlamak için:

1. Security (Güvenlik) panel menüsünde, **Authentication**'ı (Kimlik Doğrulaması) tıklatın.
2. Oturum açma kimlik doğrulamasını yapılandırmak için, **Logon Policy** (Oturum Açma İlkesi) sekmesini tıklatın, değişiklikleri yapın ve **Apply**'ı (Uygula) tıklatın.
3. Oturum kimlik doğrulamasını yapılandırmak için, **Session Policy** (Oturum İlkesi) sekmesini tıklatın, değişiklikleri yapın ve **Apply**'ı (Uygula) tıklatın.

Logon Policy (Oturum Açma İlkesi)

Windows'da oturum açarken bir kullanıcının kimlik doğrulamasını gerçekleştirmek için gereken kimlik bilgilerini yöneten ilkeleri tanımlamak için:

1. Tools (Araçlar) menüsünde, **Security**'yi (Güvenlik) ve ardından **Authentication**'ı (Kimlik Doğrulaması) tıklatın.
2. **Logon Policy** (Oturum Açma İlkesi) sekmesinde, bir kullanıcı kategorisini tıklatın.
3. Seçilen kullanıcı kategorisi için gereken kimlik doğrulaması kimlik bilgilerini belirtin. En az bir kimlik bilgisi belirtmeniz gerekir.
4. Bir kullanıcının kimlik doğrulamasını gerçekleştirmek üzere, belirtilen kimlik bilgilerinden HERHANGİ BİRİNİ (yalnızca birini) veya belirtilen kimlik bilgilerinin TÜMÜNÜ zorunlu kılmayı seçin. Herhangi bir kullanıcının bilgisayara erişimini de engelleyebilirsiniz.
5. **Apply**'ı (Uygula) tıklatın.

Session Policy (Oturum İlkesi)

Bir Windows oturumu sırasında HP ProtectTools uygulamalarına erişmek için gereken kimlik bilgilerini yöneten ilkeleri tanımlamak için:

1. Tools (Araçlar) menüsünde, **Security**'yi (Güvenlik) ve ardından **Authentication**'ı (Kimlik Doğrulaması) tıklatın.
2. **Session Policy** (Oturum İlkesi) sekmesinde, bir kullanıcı kategorisini tıklatın.
3. Seçilen kullanıcı kategorisi için gereken kimlik doğrulaması kimlik bilgilerini belirtin.
4. Bir kullanıcının kimlik doğrulamasını gerçekleştirmek üzere, belirtilen kimlik bilgilerinden BİRİNİ veya belirtilen kimlik bilgilerinin TÜMÜNÜ zorunlu kılmayı seçin. HP ProtectTools yazılımına erişmek için kimlik doğrulaması yapılmasını zorunlu kılmamayı da seçebilirsiniz.
5. **Apply**'ı (Uygula) tıklatın.

Ayarlar

Şu güvenlik ayarlarından birine veya daha fazlasına izin verebilirsiniz:

- **Allow One Step logon** (Tek Adımda oturum açmaya izin ver)—BIOS'ta veya şifreli disk düzeyinde kimlik doğrulaması gerçekleştirildiyse, bu bilgisayarın kullanıcılarının Windows oturum açma işlemini atlamasına izin verir.
- **Allow HP SpareKey authentication for Windows logon** (Windows oturum açma işlemi için HP SpareKey kimlik doğrulamasına izin ver)—Bu bilgisayarın kullanıcılarının, Security Manager (Güvenlik Yöneticisi) başka bir kimlik doğrulaması ilkesi gerektirse de Windows'da oturum açmak için HP SpareKey özelliğini kullanmasına izin verir.

Ayarları düzenlemek için:

1. Belirli bir ayarı etkinleştirmek veya devre dışı bırakmak için tıklatın.
2. Yaptığınız değişiklikleri kaydetmek için **Apply**'ı (Uygula) tıklatın.

Kullanıcıları yönetme

Users (Kullanıcılar) uygulaması içinde, bu bilgisayarın HP ProtectTools kullanıcılarını izleyebilir ve yönetebilirsiniz.

Tüm HP ProtectTools kullanıcıları, Security Manager (Güvenlik Yöneticisi) ile ayarlanan ilkelere göre listelenir ve doğrulanır; ayrıca bu ilkelere uymalarını sağlayan doğru kimlik bilgilerini kaydettirip kaydettirmedikleri de doğrulanır.

Kullanıcıları yönetmek için aşağıdaki ayarlardan birini seçin:

- Ek kullanıcı eklemek için **Add**'i (Ekle) tıklatın.
- Bir kullanıcıyı silmek için kullanıcıyı tıklatın, sonra da **Delete**'i (Sil) tıklatın.
- Kullanıcı için parmak izi kaydetmek veya ek kimlik bilgileri ayarlamak için, kullanıcıyı tıklatıp **Enroll**'u (Kaydet) tıklatın.
- Belirli bir kullanıcıya yönelik ilkeleri görüntülemek için kullanıcıyı seçin ve alt pencerenin alt kısmındaki ilkeleri görüntüleyin.

Aygıt ayarlarını belirtme

Device (Aygıt) uygulaması içinde, HP ProtectTools Security Manager'ın (HP ProtectTools Güvenlik Yöneticisi) tanıdığı herhangi bir yerleşik veya bağlı güvenlik aygıtının kullanılabilir ayarlarını belirtebilirsiniz.

Fingerprints (Parmak İzleri)

Fingerprints (Parmak İzleri) sayfasında üç sekme bulunur: Enrollment (Kayıt), Sensitivity (Duyarlılık) ve Advanced (Gelişmiş).

Enrollment (Kayıt)

Bir kullanıcının kaydetmesine izin verilen minimum ve maksimum parmak izi sayısını seçebilirsiniz.

Ayrıca, parmak izi okuyucudaki tüm verileri temizleyebilirsiniz.

△ **DİKKAT:** Parmak izi okuyucudaki tüm verileri temizlemek, yöneticiler de dahil olmak üzere tüm kullanıcıların tüm parmak izi verilerini siler. Oturum açma ilkesi yalnızca parmak izi gerektiriyorsa, tüm kullanıcıların bilgisayarda oturum açması engellenebilir.

Sensitivity (Duyarlılık)

Parmak izi okuyucunun parmak izlerinizi okuma sırasındaki duyarlılığını ayarlamak için kaydırıcıyı hareket ettirin.

Parmak iziniz sürekli olarak tanınmıyorsa, daha düşük bir duyarlılık ayarı gerekli olabilir. Daha yüksek bir ayar, parmak izi taramalarındaki farklılıklara olan duyarlılığı artırarak hatalı kabul olasılığını azaltır. Medium-High (Orta-Yüksek) ayarı, güvenlik ve rahatlığı birlikte sağlayan bir ayardır.

Advanced (Gelişmiş)

Parmak izi okuyucuyu bilgisayar pil gücüyle çalışırken güç tasarrufu yapacak şekilde yapılandırabilirsiniz.

Smart card (Akıllı kart)

Bilgisayarı, akıllı kart çıkarıldığında otomatik olarak kilitlenecek şekilde yapılandırabilirsiniz. Ancak bilgisayar, yalnızca akıllı kartın Windows'da oturum açarken kimlik doğrulaması kimlik bilgisi olarak kullanıldığı durumlarda kilitlenir. Windows'da oturum açmak için kullanılmayan bir akıllı kartın çıkarılması bilgisayarı kilitlemez.

▲ Akıllı kart çıkarıldığında bilgisayarın kilitlenmesini etkinleştirmek veya devre dışı bırakmak için onay kutusunu seçin.

Yüz

Face Recognition (Yüz Tanıma) öğesinin güvenlik düzeyini, kolay kullanım ile bilgisayar güvenliğinin ihlal edilmesi arasında denge sağlayacak şekilde ayarlayabilirsiniz.

1. **Başlat**'ı tıklatın, **Tüm Programlar**'ı tıklatın, **HP**'yi ve ardından **HP ProtectTools Administrative Console**'u (HP ProtectTools Yönetim Konsolu) tıklatın.
2. **Devices**'ı (Aygıtlar), sonra da **Face**'i (Yüz) tıklatın.

3. Daha fazla kolaylık için, kaydırıcıyı tıklatıp sola oynatın veya daha fazla doğruluk için, kaydırıcıyı tıklatıp sağa doğru oynatın.

   - **Convenience** (Kolaylık)—Kayıtlı kullanıcıların marjinal durumlara erişim sağlamasını kolaylaştırmak için, kaydırma çubuğunu tıklatarak **Convenience** (Kolaylık) konumuna getirin.
   - **Balance** (Denge)—Güvenlik ile kullanışlılık arasında denge sağlamak istiyorsanız veya hassas bilgileriniz varsa ya da bilgisayarınız yetkisiz oturum açma girişimlerinin yaşanabileceği bir alandaysa, kaydırma çubuğunu tıklatarak **Balance** (Denge) konumuna getirin.
   - **Accuracy** (Doğruluk)—Kayıtlı görünümler veya mevcut aydınlatma koşulları normalin altındaysa ve yanlış onay gibi daha az olası bir durum gerçekleşirse, kaydırma çubuğunu tıklatıp **Accuracy** (Doğruluk) konumuna getirin.

NOT: Güvenlik düzeyi tüm kullanıcılar için geçerlidir

4. **Apply**'ı (Uygula) tıklatın.

Gelişmiş ayarlar

1. **Başlat**'ı tıklatın, **Tüm Programlar**'ı tıklatın, **HP**'yi ve ardından **HP ProtectTools Administrative Console**'u (HP ProtectTools Yönetim Konsolu) tıklatın.
2. **Devices**'ı (Aygıtlar), sonra da **Face**'i (Yüz) tıklatın.
3. **Advanced**'i (Gelişmiş) tıklatın.

   - **Windows oturumu açmak için kullanıcı adı isteme.**
     - Kullanıcıların kullanıcı adı olmaksızın Windows'da oturum açabilmesi için onay kutusunu seçin.
     - Oturum açmada kullanıcı adını zorunlu kılmak için onay kutusunu temizleyin.
   - **Enforce the use of PIN for face logon** (Yüzle oturum açmada PIN kullanımını zorunlu kıl)—Oturum açmak için her kullanıcının bir PIN (kişisel kimlik numarası) koymasını ve kullanmasını zorunlu kılmak için seçin.
     - **Minimum length allowed for PIN** (PIN için izin verilen minimum uzunluk)—PIN için gereken minimum karakter sayısını artırmak için yukarı, azaltmak için aşağı okunu tıklatın.
     - **Maximum length allowed for PIN** (PIN için izin verilen maksimum uzunluk)—PIN için izin verilen maksimum karakter sayısını artırmak için yukarı, azaltmak için aşağı oku tıklatın.
     - **Maximum retries allowed for PIN** (PIN için izin verilen maksimum deneme)—PIN'in yeniden girilebileceği maksimum deneme sayısını artırmak için yukarı, azaltmak için aşağı oku tıklatın.

4. **OK**'i (Tamam) tıklatın.

5 Uygulamalarınızı yapılandırma

Applications (Uygulamalar) grubuna, HP ProtectTools Administrative Console'un (HP ProtectTools Yönetim Konsolu) sol tarafındaki Security Applications (Güvenlik Uygulamaları) menü panelinden erişilebilir. Yüklü olan HP ProtectTools Security Manager (HP ProtectTools Güvenlik Yöneticisi) uygulamalarının davranışlarını özelleştirmek için Settings'i (Ayarlar) kullanabilirsiniz.

Uygulama ayarlarınızı düzenlemek için:

1. Tools (Araçlar) menüsünde, **Applications** (Uygulamalar) grubunda **Settings**'i (Ayarlar) tıklatın.
2. Belirli bir ayarı etkinleştirmek veya devre dışı bırakmak için tıklatın.
3. Yaptığınız değişiklikleri kaydetmek için **Apply**'ı (Uygula) tıklatın.

General (Genel) sekmesi

Aşağıdaki ayarlar General (Genel) sekmesinde bulunur:

- **Do not automatically launch the Setup Wizard for administrators** (Kurulum Sihirbazı'nı yöneticiler için otomatik olarak başlatma)—Oturum açılınca sihirbazın otomatik olarak açılmasını engellemek için bu seçeneği belirleyin.
- **Do not automatically launch the Getting Started wizard for users** (Başlarken sihirbazını kullanıcılar için otomatik olarak başlatma)—Oturum açılınca kullanıcı kurulumun otomatik olarak açılmasını engellemek için bu seçeneği belirleyin.

Applications (Uygulamalar) sekmesi

Burada görüntülenen ayarlar, Security Manager'a (Güvenlik Yöneticisi) yeni uygulamalar eklendiğinde değişebilir. Varsayılan olarak gösterilen en az sayıda ayar şu şekildedir:

- **Applications status** (Uygulama Durumu)—Tüm uygulamaların durumunun görüntülenebilmesini sağlar.
- **Password Manager** (Parola Yöneticisi)—Password Manager (Parola Yöneticisi) uygulamasını bilgisayarın tüm kullanıcıları için etkinleştirir.
- **Privacy Manager** (Gizlilik Yöneticisi)—Privacy Manager (Gizlilik Yöneticisi) uygulamasını bilgisayarın tüm kullanıcıları için etkinleştirir.
- **Enable the Discover more button** (Daha fazlasını keşfedin düğmesini etkinleştir)—Bu bilgisayarın tüm kullanıcılarının **[+] Discover more** ([+] Daha fazlasını keşfedin) düğmesini tıklatarak HP ProtectTools Security Manager'a (HP ProtectTools Güvenlik Yöneticisi) uygulama eklemesine olanak tanır.

Tüm uygulamaları fabrika ayarlarına döndürmek için **Restore Defaults** (Varsayılanları Geri Yükle) düğmesini tıklatın.

6 Yönetim araçları

Security Manager'a yeni yönetim araçları eklemek için ek uygulamalar mevcut olabilir. Bu bilgisayarın yöneticisi bu özelliği Settings (Ayarlar) uygulamasından devre dışı bırakabilir.

Ek yönetim araçları eklemek için, **[+] Management tools**'u ([+] Yönetim araçları) tıklatın.

Güncelleştirmeler ve Mesajlar

Internet bağlantısı varsa, yeni uygulamaları denetlemek için http://www.digitalpersona.com/ adresinden DigitalPersona Web sitesine erişebilir veya otomatik güncelleştirmeler için bir programlama ayarlayabilirsiniz.

1. Yeni uygulamalar ve güncelleştirmeler hakkında bilgi istemek için, **Keep me informed about new applications and updates** (Beni yeni uygulamalardan ve güncelleştirmelerden haberdar et) onay kutusunu seçin.
2. Otomatik güncelleştirmeler için bir zamanlama ayarlayın, gün sayısını seçin.
3. Güncelleştirmeleri denetlemek için, **Check Now**'ı (Şimdi Denetle) tıklatın.

7 HP ProtectTools Security Manager (HP ProtectTools Güvenlik Yöneticisi)

HP ProtectTools Security Manager (HP ProtectTools Güvenlik Yöneticisi) bilgisayarınızın güvenliğini önemli ölçüde artırmanıza olanak tanır.

Önceden yüklenmiş Security Manager (Güvenlik Yöneticisi) uygulamalarının yanı sıra, Web'den hemen indirebileceğiniz ek uygulamaları kullanabilirsiniz:

- Oturum açma verilerinizi ve parolalarınızı yönetin
- Windows® işletim sistemi parolanızı kolayca değiştirin
- Program tercihlerini ayarlayın
- Ek güvenlik ve rahatlık için parmak izlerini kullanın
- Kimlik doğrulaması için bir veya daha fazla görünüm kaydedin
- Kimlik doğrulaması için akıllı kart ayarlayın
- Program verilerinizi yedekleyin ve geri yükleyin
- Daha fazla uygulama ekleyin

HP ProtectTools Security Manager'ı açma

HP ProtectTools Security Manager'ı aşağıdaki yöntemlerden herhangi biriyle açabilirsiniz:

- **Başlat**'ı tıklatın, **Tüm Programlar**'ı tıklatın, **HP**'yi ve ardından **HP ProtectTools Security Manager**'ı tıklatın.
- Görev çubuğunun en sağındaki bildirim alanında yer alan **HP ProtectTools** simgesini çift tıklatın.
- **HP ProtectTools** simgesini sağ tıklatın ve **Open HP ProtectTools Security Manager**'ı (HP ProtectTools Security Manager'ı aç) tıklatın.
- Windows Kenar Çubuğu'ndaki **Security Manager ID Card** (Security Manager Kimlik Kartı) aracını tıklatın.
- Security Manager Quick Links (Security Manager Hızlı Bağlantılar) menüsünü açmak için ctrl +Windows+h kısayol tuşlarına basın.

Security Manager panosunu kullanma

Security Manager panosu, Security Manager özelliklerine, uygulamalarına ve ayarlarına kolay erişim için merkezi bir konumdur.

▲ Security Manager panosunu açmak için, **Başlat**'ı, **Tüm Programlar**'ı, **HP**'yi ve ardından **HP ProtectTools Security Manager**'ı tıklatın.

Pano şu bileşenlerden oluşur:

- **ID Card** (Kimlik Kartı)—Windows kullanıcı adını ve oturumu açık olan kullanıcı hesabını belirleyen seçilmiş bir resmi görüntüler.
- **Security Applications** (Güvenlik Uygulamaları)—Aşağıdaki güvenlik kategorilerini yapılandırmaya yönelik bağlantılardan oluşan genişleyen bir menü görüntüler.
  - **Credential Manager**
  - **My Data (Verilerim)**
- **Discover more** (Daha fazlasını keşfedin)—Kimliğinizin, verilerinizin ve iletişimlerinizin güvenliğini geliştirmek için ek uygulamalar bulabileceğiniz bir sayfa açar.
- **Main area** (Ana alan)—Uygulamaya özel ekranları görüntüler.
- **Administration** (Yönetim)—HP ProtectTools Administrative Console'u açar.
- **Help button** (Yardım düğmesi)—Geçerli ekran hakkında bilgiler görüntüler.
- **Advanced** (Gelişmiş)—Şu seçeneklere erişmenize olanak sağlar:
  - **Preferences** (Tercihler)—Security Manager ayarlarını özelleştirmenize olanak sağlar.
  - **Backup and Restore** (Yedekleme ve Geri Yükleme)—Verileri yedeklemenize veya geri yüklemenize olanak sağlar.
  - **About** (Hakkında)—Security Manager hakkındaki sürüm bilgilerini görüntüler.

Kurulum yordamları

Kimlik bilgilerini kaydetme

Çeşitli kimlik doğrulama yöntemlerinizi veya kimlik bilgilerinizi kaydettirmek için My Identity (Kimliğim) sayfasını kullanabilirsiniz. Kayıt işlemi bittikten sonra, Security Manager'da oturum açmak için bu yöntemleri kullanabilirsiniz.

Parmak izlerinizi kaydetme

Bilgisayarınızın yerleşik veya bağlı bir parmak izi okuyucusu varsa, HP ProtectTools Security Manager Kurulum Sihirbazı size parmak izlerinizi ayarlama veya “kaydetme” işlemi boyunca yol gösterir:

1. İki elin ana hatları görüntülenir. Önceden kaydedilmiş olan parmaklar yeşil renkle vurgulanır. Ana hat üzerindeki bir parmağı tıklatın.

   NOT: Daha önce kaydedilmiş bir parmak izini silmek için parmağı tıklatın.

2. Kaydetmek üzere bir parmak seçtiğinizde, parmak izi başarıyla kaydedilene kadar parmağı taramanız istenir. Kaydedilen bir parmak, ana hat üzerinde yeşil renkle vurgulanır.

3. En az iki parmak kaydetmeniz gerekir; işaret parmağı veya orta parmaklar tercih edilir. Başka bir parmak kaydetmek için 1'den 3'e kadar olan adımları tekrarlayın.

4. **Next**'i (İleri) tıklatın, sonra da ekrandaki yönergeleri izleyin.

NOT: Başlarken işlemiyle parmak izi kaydederken, parmak izi bilgileri siz **Next**'i (İleri) tıklatana kadar kaydedilmez. Bilgisayarda bir süre işlem yapmazsanız veya programı kapatırsanız, yaptığınız değişiklikler **kaydedilmez**.

Görünümleri kaydetme

Yüz oturumunu kullanmak için bir veya daha fazla görünümü kaydetmeniz gerekir.

HP ProtectTools Security Manager Kurulum Sihirbazı'ndan yeni bir görünüm kaydetmek için:

1. Ekranın en sağındaki kenar çubuğunda yer alan **HP ProtectTools Security Manager** (HP ProtectTools Güvenlik Yöneticisi) simgesini tıklatın.

2. Windows® parolanızı girin, sonra da **Next**'i (İleri) tıklatın.

3. **Enable security features** (Güvenlik özelliklerini etkinleştir) öğesi altında, **Windows Logon Security** (Windows Oturum Açma Güvenliği) onay kutusunu seçin, sonra da **Next**'i (İleri) tıklatın.

4. **Choose your credentials** (Kimlik bilgilerinizi seçin) öğesi altında, **Face** (Yüz) onay kutusunu seçin, sonra da **Next**'i (İleri) tıklatın.

5. **Enroll a new scene**'i (Yeni bir görünüm kaydet) tıklatın.

Başarıyla kaydettikten sonra, aşağıdaki koşulların bir veya daha fazlasının değişmesi nedeniyle oturum açarken zorluk yaşamanız halinde, yeni bir görünüm kaydetmeniz de mümkündür:

- Son kayıt sonrasında yüzünüzde önemli bir değişiklik olduysa.
- Aydınlatma önceki kayıtlarınızın tümünden önemli ölçüde farklıysa.
- Son kayıt sırasında gözlük takıyor (veya takmıyor) iseniz.

NOT: Görünüm kaydetmede zorluk yaşıyorsanız, web kamerasını yakınlaştırmayı deneyin. Aydınlatma ve karşıtlık, herhangi bir fotoğraf veya video türünde olduğu gibi son derece önemlidir. Oturumunuzda aydınlatmanın öncelikle arkaplanda değil önplanda olduğundan emin olun. Face Recognition'ın (Yüz Tanıma) kimliğinizi doğrulamaya hazır olmadığını görürseniz, görüntünüzü geliştirilmiş aydınlatma ile kaydetmek isteyebilirsiniz.

HP ProtectTools Security Manager'dan (HP ProtectTools Güvenlik Yöneticisi) yeni bir görünüm kaydetmek için:

1. **Başlat**'ı tıklatın, **Tüm Programlar**'ı tıklatın, **HP**'yi ve ardından **HP ProtectTools Security Manager**'ı (HP ProtectTools Güvenlik Yöneticisi) tıklatın.
2. **Credentials**'ı (Kimlik Bilgileri), sonra da **Face**'i (Yüz) tıklatın.
3. **Enroll a new scene**'i (Yeni bir görünüm kaydet) tıklatın.

Advanced User Settings (Gelişmiş Kullanıcı Ayarları)

1. **Başlat**'ı tıklatın, **Tüm Programlar**'ı tıklatın, ardından **HP ProtectTools Security Manager**'ı tıklatın.
2. **Set up your authentication credentials**'ı (Kimlik doğrulama bilgilerinizi ayarlayın), sonra da **Face**'i (Yüz) tıklatın.
3. **Advanced**'i (Gelişmiş) tıklatın, sonra da aşağıdaki seçenekler arasından seçim yapın.

   a. Yüzle oturum açmak için PIN kullanılmasını zorunlu tutmak üzere, **Create PIN**'i (PIN oluştur) tıklatın, Windows parolanızı girin, yeni PIN'i girin, sonra da yeni PIN yeniden girerek doğrulayın.

   b. İsterseniz, ilave ayarlar seçin. Bu ayarlar yalnızca mevcut kullanıcı için geçerlidir:

   - **Play sound on face recognition events (Yüz tanıma olaylarında ses çal)**
     - Yüz tanıma başarılı veya başarısız olduğunda bir ses çalmak için onay kutusunu seçin.
     - Bu seçeneği devre dışı bırakmak için onay kutusunu temizleyin.
   - **Prompt to update scenes when logon fails (Oturum açılamadığında görünümlerin güncellenmesini iste)**
     - Yüzle oturum açılamadığında kullanıcının görünümleri güncellemesine izin vermek için onay kutusunu seçin. Doğrulama “maybe” (belki) eşiğine ulaşırsa, kullanıcıdan “failed” (başarısız) oturumdaki canlı görüntüleri, sonraki oturumun başarıyla açılabilmesi şansını artırmak üzere mevcut görünüme ekleyip eklememeye karar vermesi istenir.
     - Bu seçeneği devre dışı bırakmak için onay kutusunu temizleyin.
   - **Prompt to enroll a new scene when logon fails (Oturum açılamadığında yeni bir görünüm kaydedilmesini iste)**
     - Oturum açılamadığında ve doğrulama “maybe” (belki) eşiğine ulaşmadığında kullanıcının yeni bir görünüm kaydetmesi için bir istem görüntülenmesi için onay kutusunu seçin. Bu sonraki oturumun başarıyla açılması şansını artırabilir.
     - Bu seçeneği devre dışı bırakmak için onay kutusunu temizleyin.

   c. Yeni bir görünüm kaydetmek için **Enroll a new scene**'i (Yeni bir görünüm kaydet) tıklatın, sonra da ekrandaki yönergeleri izleyin.

Windows parolanızı değiştirme

Security Manager (Güvenlik Yöneticisi), Windows parolanızı değiştirmeyi Windows Denetim Masası'ndan değiştirmekten daha basit ve hızlı hale getirir.

Windows parolanızı değiştirmek için şu adımları izleyin:

1. Security Manager (Güvenlik Yöneticisi) panosunda **Credentials**'ı (Kimlik Bilgileri), sonra da **Password**'ü (Parola) tıklatın.
2. **Current Windows password** (Geçerli Windows parolası) metin kutusuna geçerli parolanızı girin.

3. **New Windows password** (Yeni Windows parolası) metin kutusuna yeni bir parola yazın ve sonra parolayı **Confirm new password** (Yeni parolayı onaylayın) metin kutusuna tekrar yazın.

4. Geçerli parolanızı girdiğiniz yeni parolayla hemen değiştirmek için **Change**'i (Değiştir) tıklatın.

Akıllı kart ayarlama

Akıllı kart oturumunu seçtiyseniz ve bilgisayarınızda yerleşik veya bağlı bir akıllı kart okuyucu varsa, Security Manager Kurulum Sihirbazı sizden bir akıllı kart PIN'i (kişisel kimlik numarası) ayarlamanızı isteyecektir.

Akıllı kart PIN'i ayarlamak için:

1. **Set up smart card** (Akıllı kart ayarlama) öğesi altında, bir PIN girip onaylayın.

   PIN'inizi değiştirmeniz de mümkündür. Mevcut PIN'inizi girin, sonra da yeni bir PIN girin.

2. Devam etmek için **Next**'i (İleri) tıklatın, sonra da ekrandaki yönergeleri izleyin.

– veya –

▲ Security Manager (Güvenlik Yöneticisi) panosunda **Credentials**'ı (Kimlik Bilgileri), sonra da **Smart Card**'ı (Akıllı Kart) tıklatın.

- Bir akıllı kart PIN'i ayarlamak için—**Set up smart card** (Akıllı kart ayarlama) öğesi altında, bir PIN girip onaylayın.
- PIN'inizi değiştirmek için—İlk olarak geçerli PIN'inizi girin, sonra da yeni bir tane girip onaylayın.

Genel görevler

Bu gruptaki uygulamalar, dijital kimliğinizin çeşitli özelliklerini yönetmenize yardımcı olur.

- **Security Manager** (Güvenlik Yöneticisi)—Windows parolanızla, parmak izinizle veya bir akıllı kartla kimlik doğrulaması yaparak Web sitelerini ve programları başlatmanıza ve bunlarda oturum açmanıza olanak sağlayan Quick Links'i (Hızlı Bağlantılar) oluşturur ve yönetir.
- **Credentials** (Kimlik Bilgileri)—Windows parolanızı değiştirmek, parmak izlerinizi kaydetmek veya akıllı kart ayarlamak için kolay bir yol sunar.

Daha fazla uygulama eklemek için panonun sol alt köşesindeki [+] **Discover more** (Daha fazlasını keşfedin) düğmesini tıklatın. Bu düğme, yönetici tarafından devre dışı bırakılmış olabilir.

Password Manager (Parola Yöneticisi)

Windows'da, Web sitelerinde ve uygulamalarda oturum açmak, Password Manager (Parola Yöneticisi) ile daha kolay ve güvenlidir. Not almak veya hatırlamak zorunda olmadığınız daha güçlü parolalar oluşturmak için kullanabilir ve daha sonra parmak izi, akıllı kart veya Windows parolanızla kolay ve hızlı bir biçimde oturum açabilirsiniz.

Password Manager (Parola Yöneticisi), aşağıdaki seçenekleri sunar:

- Manage (Yönet) sekmesinde oturum açma verileri ekleme, düzenleme ve silme.
- Varsayılan tarayıcınızı başlatmak ve herhangi bir Web sitesinde veya programda kurulumun ardından oturum açmak için Quick Links'i (Hızlı Bağlantılar) kullanın.
- Quick Links'inizi (Hızlı Bağlantılar) kategorilere ayırarak düzenlemek için sürükleyip bırakın.
- Parolalarınızdan herhangi birinin bir güvenlik tehlikesi oluşturup oluşturmadığını tek bakışta görün ve yeni siteler için otomatik olarak karmaşık ve güçlü bir parola oluşturun.

Birçok Password Manager özelliği, bir Web sayfasına veya program oturum açma ekranına odaklanıldığında görüntülenen Password Manager simgesinden de kullanılabilir. Aşağıdaki seçenekler arasından seçim yapabileceğiniz bir bağlam menüsü görüntülemek için simgeyi tıklatın.

Oturum açma verileri henüz oluşturulmayan Web sayfaları ve programlar için

Bağlam menüsünde aşağıdaki seçenekler gösterilir:

- **Add [somedomain.com] to the Password Manager** ([etkialani.com] adresini Parola Yöneticisi'ne ekle)—Geçerli oturum açma ekranı için oturum açma verileri eklemenize olanak tanır.
- **Open Password Manager** (Parola Yöneticisi'ni aç)—Password Manager'ı (Parola Yöneticisi) başlatır.
- **Icon settings** (Simge ayarları)—Password Manager (Parola Yöneticisi) simgesinin görüntüleneceği durumları belirtmenize olanak sağlar.
- **Help** (Yardım)—Password Manager yazılımı Yardım'ı görüntüler.

Oturum açma verileri önceden oluşturulan Web sayfaları ve programlar için

Bağlam menüsünde aşağıdaki seçenekler gösterilir:

- **Fill in logon data** (Oturum açma verilerini doldur)—Oturum açma verilerinizi oturum açma alanlarına yerleştirir ve sayfayı gönderir (oturum açma verileri oluşturulduğunda veya son düzenlendiğinde gönderme eylemi belirtildiyse).
- **Edit logon** (Oturum açma verilerini düzenle)—Bu Web sitesi için oturum açma verilerinizi düzenlemenize olanak sağlar.
- **Add a New Account** (Yeni Hesap ekle)—Oturum açma verilerine hesap eklemenize olanak sağlar.
- **Open Password Manager** (Parola Yöneticisi'ni aç)—Password Manager (Parola Yöneticisi) uygulamasını başlatır.
- **Help** (Yardım)—Password Manager yazılımı Yardım'ı görüntüler.

NOT: Bu bilgisayarın yöneticisi, Security Manager'ı (Güvenlik Yöneticisi) kimliğinizi doğrularken birden fazla kimlik bilgisi gerektirecek şekilde ayarlamış olabilir.

Oturum açma verileri ekleme

Oturum açma bilgilerini bir kez girerek bir Web sitesi veya programın oturum açma verilerini kolayca ekleyebilirsiniz. Bundan sonra, Password Manager bu bilgileri sizin yerinize otomatik olarak girer. Bu oturum açma verilerini web sitesine veya programa gittikten sonra kullanabilir veya Password Manager'ın Web sitesini veya programı başlatarak oturumunuzu açmasını sağlamak üzere **Logons** (Oturum Açma Verileri) menüsünde oturum açma verilerini tıklatabilirsiniz.

Oturum açma verileri eklemek için:

1. Bir Web sitesinin veya programın oturum açma ekranını açın.
2. **Password Manager** (Parola Yöneticisi) simgesinin üzerindeki oku tıklatın ve ardından oturum açma ekranının bir Web sitesine veya programa yönelik oluşuna bağlı olarak aşağıdakilerden birini tıklatın:
   - Bir Web sitesi için, **Add [domain name] to Password Manager**'ı (Parola Yöneticisi'ne [etki alanı adı] adresini ekle) tıklatın.
   - Bir program için, **Add this logon screen to Password Manager**'ı (Parola Yöneticisi'ne bu oturum açma ekranını ekle) tıklatın.
3. Oturum açma verilerinizi girin. Ekrandaki oturum açma alanları ve iletişim kutusundaki ilgili alanlar, kalın bir turuncu kenarlıkla belirlenir. Ayrıca, **Password Manager Manage** (Password Manager Yönet) sekmesinde bulunan **Add Logon**'u (Oturum Açma Verileri Ekle) tıklatarak da bu iletişim kutusunu görüntüleyebilirsiniz. ctrl+Windows+h kısayol tuşunu kullanma, parmak izinizi tarama veya akıllı kart takma gibi bazı seçenekler, bilgisayara bağlı güvenlik aygıtlarına bağlıdır.
   a. Bir oturum açma alanını önceden biçimlendirilmiş seçeneklerden biriyle doldurmak için, alanın sağındaki okları tıklatın.
   b. Söz konusu oturum açma verilerine ait parolayı görüntülemek için **Show password**'ü (Parolayı göster) tıklatın.
   c. Oturum açma alanlarının doldurulması ancak gönderilmemesi için **Automatically submit logon data** (Oturum açma verilerini otomatik olarak gönder) onay kutusunu temizleyin.

d. **OK**'i (Tamam) tıklatın, kullanmak istediğiniz kimlik doğrulaması yöntemini tıklatın: **Fingerprints** (Parmak İzi), **Password** (Parola) veya **Face** (Yüz), ardından seçilen kimlik doğrulaması yöntemi ile oturum açın.

   Oturum açma verilerinizin oluşturulduğunu bildirmek amacıyla, artı işareti Password Manager (Parola Yöneticisi) simgesinden kaldırılır.

e. Password Manager (Parola Yöneticisi) oturum açma alanlarını algılamazsa, **More fields**'ı (Diğer alanlar) tıklatın.

   i. Oturum açmak için gerekli olan her bir alanın onay kutusunu seçin veya oturum açmak için gerekli olmayan alanların onay kutusunu temizleyin.

   ii. Password Manager (Parola Yöneticisi) oturum açma alanlarının tümünü algılayamazsa, devam etmek isteyip istemediğinizi soran bir mesaj görüntülenir. **Yes**'i (Evet) tıklatın.

   iii. Oturum açma alanlarınızın doldurulmuş olduğu bir iletişim kutusu görüntülenir. Her bir bölge için simgeyi tıklatıp uygun oturum açma alanına sürükleyin, sonra da Web sitesine giriş yapmak üzere düğmeyi tıklatın.

   NOT: Bir sitenin oturum açma verilerini girmek için manuel modu kullandıktan sonra, aynı sitede gelecekte oturum açmak için bu yöntemi kullanmaya devam etmeniz gerekir.

   NOT: Oturum açma bilgilerini manuel modda girmek, yalnızca Internet Explorer 8'de olan bir özelliktir.

   iv. **Close**'u (Kapat) tıklatın.

Bu Web sitesine her eriştiğinizde veya programı her açtığınızda, oturum açmak için kaydettirilen kimlik bilgilerinizi kullanabileceğinizi belirtmek üzere Password Manager (Parola Yöneticisi) simgesi görüntülenir.

Oturum açma verilerini düzenleme

Oturum açma verilerini düzenlemek için aşağıdaki adımları takip edin:

1. Bir Web sitesinin veya programın oturum açma ekranını açın.
2. Oturum açma bilgilerinizi düzenleyebileceğiniz bir iletişim kutusu görüntülemek için, **Password Manager** (Parola Yöneticisi) simgesindeki oku tıklatın ve daha sonra **Edit logon**'u (Oturum açma verilerini düzenle) tıklatın. Ekrandaki oturum açma alanları ve iletişim kutusundaki ilgili alanlar, kalın bir turuncu kenarlıkla belirlenir.

   Ayrıca, **Password Manager Manage** (Parola Yöneticisi Yönet) sekmesinde bulunan **Edit for the desired logon**'u (İstenen oturum açma verileri için düzenle) tıklatarak da bu iletişim kutusunu görüntüleyebilirsiniz.
3. Oturum açma bilgilerinizi düzenleyin.

   - Bir oturum açma alanını önceden biçimlendirilmiş seçeneklerden biriyle doldurmak için, alanın sağındaki okları tıklatın.
   - Oturum açma verilerinize ekrandan ek alanlar eklemek için, **More fields**'ı (Diğer alanlar) tıklatın.

- Oturum açma alanlarının doldurulması ancak gönderilmemesi için **Submit logon data** (Oturum açma verilerini gönder) onay kutusunu temizleyin.
- Söz konusu oturum açma verilerine ait parolayı görüntülemek için **Show password**'ü (Parolayı göster) tıklatın.

4. **OK**'i (Tamam) tıklatın.

Logons (Oturum Açma Verileri) menüsünü kullanma

Password Manager (Parola Yöneticisi), oturum açma verilerini oluşturduğunuz Web sitelerini ve programları başlatmak için hızlı ve kolay bir yol sunar. Oturum açma ekranını açmak için, **Logons** (Oturum Açma Verileri) menüsünde bir programa ya da Web sitesine ait oturum açma verilerini veya **Password Manager** (Parola Yöneticisi) içindeki **Manage** (Yönet) sekmesini çift tıklatın ve oturum açma verilerinizle doldurun.

Oturum açma verileri oluşturduğunuzda, bunlar otomatik olarak Password Manager Logons (Parola Yöneticisi Oturum Açma Verileri) menüsüne eklenir.

Logons (Oturum Açma Verileri) menüsünü görüntülemek için:

1. **Password Manager** kısayol tuşu bileşimine basın. ctrl+Windows+h fabrika ayarıdır. Kısayol tuşu bileşimini değiştirmek için, **Password Manager**'ı ve ardından **Settings**'i (Ayarlar) tıklatın.
2. Parmak izinizi tarayın (yerleşik veya bağlı parmak izi okuyucusu olan bilgisayarlarda).

Oturum açma verilerini kategorilere ayırarak düzenleme

Bir veya daha çok kategori oluşturarak, oturum açma verilerinizin düzenli kalmasını sağlamak üzere kategorileri kullanın. Ardından, oturum açma verilerinizi istediğiniz kategorilere sürükleyip bırakın.

Kategori eklemek için:

1. Security Manager (Güvenlik Yöneticisi) panosunda, **Password Manager**'ı (Parola Yöneticisi) tıklatın.
2. **Manage** (Yönet) sekmesini ve ardından **Add Category**'yi (Kategori Ekle) tıklatın.
3. Kategori için bir ad girin.
4. **OK**'i (Tamam) tıklatın.

Kategoriye oturum açma verileri eklemek için:

1. Fare imlecinizi istenen kategorinin üzerine getirin.
2. Sol fare düğmesini basılı tutun.
3. Söz konusu oturum açma verilerini kategori listesine sürükleyin. Siz fareyi üzerinde gezdirdiğinizde kategoriler vurgulanır.
4. İstenen kategori vurgulandığında fare düğmesini bırakın.

Oturum açma verileriniz seçilen kategoriye taşınmaz, yalnızca kopyalanır. Aynı oturum açma verilerini birden fazla kategoriye ekleyebilir ve tüm oturum açma verilerinizi **All**'u (Tümü) tıklatarak görüntüleyebilirsiniz.

Oturum açma verilerinizi yönetme

Password Manager (Parola Yöneticisi), kullanıcı adları, parolalar ve çoklu oturum açma hesapları için oturum açma verilerinizi tek bir merkezi konumdan kolayca yönetmenizi sağlar.

Oturum açma verileriniz Manage (Yönet) sekmesinde listelenir. Aynı web sitesi için birden fazla oturum açma verisi oluşturulduysa, her oturum açma verisi Web sitesi adının altında listelenir ve oturum açma verileri listesinde girintili olarak belirtilir.

Oturum açma verilerinizi yönetmek için:

Security Manager (Güvenlik Yöneticisi) panosunda, **Password Manager**'ı (Parola Yöneticisi) ve ardından **Manage** (Yönet) sekmesini tıklatın.

- **Add a logon** (Oturum açma verileri ekle)—**Add Logon**'u (Oturum Açma Verileri Ekle) tıklatın ve ekrandaki yönergeleri izleyin.
- **Edit a logon** (Oturum açma verilerini düzenle)—Bir oturum açma verisini tıklatın, **Edit**'i (Düzenle) tıklatın ve ardından oturum açma verilerini değiştirin.
- **Delete a logon** (Oturum açma verilerini sil)—Bir oturum açma verisini tıklatın ve ardından **Delete**'i (Sil) tıklatın.

Bir Web sitesi veya program için ek oturum açma verileri eklemek için:

1. Web sitesinin veya programın oturum açma ekranını açın.
2. Kısayol menüsünü görüntülemek için **Password manager** (Parola yöneticisi) simgesini tıklatın.
3. **Add additional logon**'u (Ek oturum açma verileri ekle) tıklatın ve ardından ekrandaki yönergeleri izleyin.

Parolanızın gücünü değerlendirme

Web sitelerinizde ve programlarınızda oturum açmak için güçlü parolalar kullanmak, kimliğinizi korumanın önemli bir noktasıdır.

Password Manager (Parola Yöneticisi), Web sitelerinizde ve programlarınızda oturum açmak için kullanılan parolaların her birine yönelik anında otomatik güç analizi ile güvenliğinizi izlemeyi ve geliştirmeyi kolay hale getirir.

Password Manager (Parola Yöneticisi) simgesi ayarları

Password Manager (Parola Yöneticisi), Web siteleri ve programlar için oturum açma ekranlarını belirleme girişiminde bulunur. Password Manager (Parola Yöneticisi), oturum açma verilerini oluşturmadığınız bir oturum açma ekranı algıladığında, Password Manager (Parola Yöneticisi) simgesini "+" işaretiyle görüntüleyerek ekran için oturum açma verileri eklemenize yönelik bir istem görüntüler.

Password Manager'ın (Parola Yöneticisi) olası oturum açma sitelerini ele alma biçimini özelleştirmek için simge okunu tıklatın ve ardından **Icon Settings**'i (Simge Ayarları) tıklatın.

- **Prompt to add logons for logon screens** (Oturum açma ekranları için oturum açma verileri ekleme istemi görüntüle)—Oturum açma verileri ayarlanmamış bir oturum açma ekranı görüntülendiğinde, Password Manager'ın (Parola Yöneticisi) oturum açma verileri eklemeniz için istem görüntülemesini sağlamak üzere bu seçeneği tıklatın.
- **Exclude this screen** (Bu ekranı hariç tut)—Password Manager'ın bu oturum açma ekranı için oturum açma verileri eklemek üzere tekrar istem görüntülememesi için bu onay kutusunu seçin.

Ek Password Manager (Parola Yöneticisi) ayarlarına erişmek için, **Password Manager**'ı (Parola Yöneticisi) ve ardından Security Manager (Güvenlik Yöneticisi) panosundaki **Settings**'i (Ayarlar) tıklatın.

Ayarlar

HP ProtectTools Security Manager'ı (HP ProtectTools Güvenlik Yöneticisi) kişiselleştirmek için ayarları belirtebilirsiniz.

1. **Prompt to add logons for logon screens** (Oturum açma ekranları için oturum açma verileri eklemek üzere istem görüntüle)—Bir Web sitesi veya program oturum açma ekranı algılandığında, bu ekran için oturum açma verilerini parola kasasına ekleyebileceğinizi belirtmek üzere artı işareti içeren bir Password Manager (Parola Yöneticisi) simgesi görüntülenir. Bu özelliği devre dışı bırakmak için **Icon Settings** (Simge Ayarları) iletişim kutusunda, **Prompt to add logons for logon screens** (Oturum açma ekranları için oturum açma verileri eklemek üzere istem görüntüle) öğesinin yanındaki onay kutusunu temizleyin.

2. **Open Password Manager with ctrl+Windows+H** (Password Manager'ı ctrl+Windows+H ile aç)—Password Manager Quick Links (Password Manager Hızlı Bağlantılar) menüsünü açan varsayılan kısayol tuşu ctrl+Windows+H'dir. Kısayol tuşunu değiştirmek için, bu seçeneği tıklatın ve yeni bir tuş bileşimi girin. Bileşimler aşağıdakilerden birini veya daha fazlasını içerebilir: ctrl, alt veya shift ve herhangi bir alfabetik ya da sayısal tuş.

3. Yaptığınız değişiklikleri kaydetmek için **Apply**'ı (Uygula) tıklatın.

Kimlik Bilgileri

Gerçekten kendiniz olduğunuzu doğrulamak için Security Manager (Güvenlik Yöneticisi) kimlik bilgilerinizi kullanırsınız. Bu bilgisayarın yerel yöneticisi, Windows hesabınızda, Web sitelerinde veya programlarda oturum açarken kimliğinizi doğrulamak için hangi kimlik bilgilerinin kullanılabileceğini ayarlayabilir.

Kullanılabilir kimlik bilgileri, bu bilgisayardaki yerleşik veya bağlı güvenlik aygıtlarına göre değişiklik gösterebilir. Desteklenen tüm kimlik bilgilerinin **My Identity, Credentials** (Kimliğim, Kimlik Bilgilerim) grubu altında bir girişi olacaktır.

Kullanılabilir kimlik bilgileri, gereksinimler ve geçerli durum listelenir ve aşağıdakileri içerebilir:

- Parmak izleri
- Parola
- Akıllı kart
- Yüz

Bir kimlik bilgisini kaydetmek veya değiştirmek için, bağlantıyı tıklatın ve ekrandaki yönergeleri izleyin.

Kişisel kimlik kartınız

Kimlik kartınız, adınızı ve seçtiğiniz bir resmi göstererek sizi benzersiz bir şekilde bu Windows hesabının sahibi olarak tanımlar. Bir Windows Kenar Çubuğu aracı olarak ve Security Manager (Güvenlik Yöneticisi) sayfalarının sol üst köşesinde belirgin bir şekilde görüntülenir.

Windows Kenar Çubuğu'nda Kimlik Kartınız'ı tıklatmak, Security Manager'a (Güvenlik Yöneticisi) hızlı bir şekilde erişmenin çok sayıda yolundan biridir.

Resmi ve adınızın görüntülenme şeklini değiştirebilirsiniz. Varsayılan olarak, Windows kurulumu sırasında seçtiğiniz tam Windows kullanıcı adınız ve resminiz gösterilir.

Görüntülenen adı değiştirmek için:

1. Security Manager (Güvenlik Yöneticisi) panosunda, sol üst köşede bulunan **ID Card** (Kimlik Kartı) simgesini tıklatın.
2. Windows'daki hesabınız için girdiğiniz adı görüntüleyen onay kutusunu tıklatın. Sistem bu hesap için Windows kullanıcı adınızı görüntüler.
3. Bu adı değiştirmek için, yeni adı yazın ve ardından **Save** (Kaydet) düğmesini tıklatın.

Görüntülenen resmi değiştirmek için:

1. Security Manager (Güvenlik Yöneticisi) panosunda, sol üst köşede bulunan **ID Card**'ı (Kimlik Kartı) tıklatın.
2. **Choose picture** (Resim seçin) düğmesini tıklatın, bir görüntüyü tıklatın ve ardından **Save** (Kaydet) düğmesini tıklatın.

Tercihlerinizi ayarlama

HP ProtectTools Security Manager ayarlarını kişiselleştirebilirsiniz. Security Manager panosunda **Advanced**'i (Gelişmiş) ve ardından **Preferences**'ı (Tercihler) tıklatın. Kullanılabilir ayarlar iki sekmede görüntülenir: General (Genel) ve Fingerprint (Parmak İzi).

General (Genel)

Aşağıdaki ayarlar General (Genel) sekmesinde bulunur:

Appearance (Görünüm)—**Show icon on taskbar** (Simgeyi görev çubuğunda göster)

- Simgenin görev çubuğunda görüntülenmesini etkinleştirmek için onay kutusunu seçin.
- Simgenin görev çubuğunda görüntülenmesini devre dışı bırakmak için onay kutusunu temizleyin.

Fingerprint (Parmak İzi)

Aşağıdaki ayarlar Fingerprint (Parmak İzi) sekmesinde bulunur:

- **Quick Actions** (Hızlı İşlemler)—Parmak izinizi tararken atanmış bir tuşu basılı tuttuğunuzda gerçekleştirilmesi gereken Security Manager görevini seçmek için Quick Actions'ı (Hızlı İşlemler) kullanın.

  Listelenen tuşların birine bir Quick Action (Hızlı İşlem) atamak için, bir **(Tuş) + Fingerprint** [(Tuş) + Parmak İzi] seçeneğini tıklatın ve ardından menüdeki kullanılabilir görevlerden birini seçin.

- **Fingerprint Scan Feedback** (Parmak İzi Tarama Geri Bildirimi)—Yalnızca kullanılabilir bir parmak izi okuyucu varsa görüntülenir. Bu ayarı, parmak izinizi taradığınızda oluşan geri bildirimi ayarlamak için kullanın.

  - **Enable sound feedback** (Sesli geri bildirimi etkinleştir)—Security Manager bir parmak izi tarandığında, belirli program olayları için farklı sesler çalarak sesli geri besleme sağlar. Windows Denetim Masası'ndaki Sesler sekmesinden bu olaylara yeni sesler atayabilir veya bu seçeneği temizleyerek sesli geri bildirimi devre dışı bırakabilirsiniz.

  - **Show scan quality feedback (Tarama kalitesi geri bildirimini göster)**

    Kalitesine bakmaksızın tüm taramaları görüntülemek için onay kutusunu seçin.

    Yalnızca kaliteli taramaları görüntülemek için onay kutusunun işaretini kaldırın.

Verilerinizi yedekleme ve geri yükleme

Security Manager (Güvenlik Yöneticisi) verilerinizi düzenli olarak yedeklemeniz önerilir. Ne sıklıkla yedeklediğiniz verilerin değişme sıklığına bağlıdır. Örneğin, günlük olarak yeni oturum açma verileri ekliyorsanız, verilerinizi günlük olarak yedeklemeniz mantıklı olacaktır.

Yedeklemeler, içe ve dışa aktarma olarak da bilinen bir bilgisayardan diğerine geçiş için de kullanılabilir.

NOT: Bu özellik ile yalnızca veriler yedeklenir.

Veriler yedekleme dosyasından geri yüklenmeden önce, yedeklenen verileri alacak tüm bilgisayarlara HP ProtectTools Security Manager (HP ProtectTools Güvenlik Yöneticisi) yüklenmiş olmalıdır.

Verilerinizi yedeklemek için:

1. Sol panelde, **Advanced**'i (Gelişmiş) ve ardından **Backup and Restore**'u (Yedekleme ve Geri Yükleme) tıklatın.
2. **Back up data**'yı (Verileri yedekle) tıklatın.
3. Yedeklemeye dahil etmek istediğiniz modülleri seçin. Çoğu durumda tümünü seçmek isteyeceksiniz.
4. Depolama dosyası için bir ad girin. Varsayılan olarak, dosya Documents (Belgeler) klasörünüze kaydedilecektir. Farklı bir konum belirtmek için **Browse**'ı (Gözat) tıklatın.
5. Dosyayı korumak için bir parola girin.
6. Kimliğinizi doğrulayın.
7. **Finish**'i (Son) tıklatın.

Verilerinizi geri yüklemek için:

1. Sol panelde, **Advanced**'i (Gelişmiş) ve ardından **Backup and Restore**'u (Yedekleme ve Geri Yükleme) tıklatın.
2. **Restore data**'yı (Verileri geri yükle) tıklatın.
3. Önceden oluşturulan depolama dosyasını seçin. Yolu, verilen alana girebilir veya **Browse**'ı (Gözat) tıklatabilirsiniz.
4. Dosyayı korumak için kullanılan parolayı girin.
5. Verilerini geri yüklemek istediğiniz modülleri seçin. Çoğu durumda bu, listelenen modüllerin tümü anlamına gelir.
6. **Finish**'i (Son) tıklatın.

Discover more (Daha fazlasını keşfedin)

Bu program için yeni özellikler sağlayan ek uygulamalar sunulabilir.

Security Manager panosunda ek uygulamalara göz atmak için **[+] Discover more**'u ([+] Daha fazlasını keşfedin) tıklatın.

NOT: Panonun sol alt kısmında **[+] Discover more** ([+] Daha fazlasını keşfedin) bağlantısı yoksa, bu bilgisayarın yöneticisi tarafından devre dışı bırakılmıştır.

Güncelleştirmeler ve Mesajlar

1. Yeni uygulamalar ve güncelleştirmeler hakkında bilgi istemek için, **Keep me informed about new applications and updates** (Beni yeni uygulamalardan ve güncelleştirmelerden haberdar et) onay kutusunu seçin.
2. Otomatik güncelleştirmeler için bir zamanlama ayarlayın, gün sayısını seçin.
3. Güncelleştirmeleri denetlemek için, **Check Now**'ı (Şimdi Denetle) tıklatın.

Güvenlik Uygulamaları Durumu

Security Manager Applications Status (Güvenlik Yöneticisi Uygulamaları Durumu) sayfası, yüklü güvenlik uygulamalarınızın genel durumunu görüntüler. Sayfa, kurulu olan uygulamaları ve her birinin kurulum durumunu gösterir. Özet, Security Manager (Güvenlik Yöneticisi) panosunu açıp **Check the status of the security applications**'ı (Güvenlik uygulamalarının durumunu denetle), **Security Applications**'ı (Güvenlik Uygulamaları) veya ekranın sağ tarafındaki Windows Kenar Çubuğu'nda bulunan **Gadget** (Araç) simgesi üzerindeki **Check Now**'ı (Şimdi Denetle) tıklattığınızda otomatik olarak görüntülenir.

8 HP ProtectTools için Drive Encryption (Sürücü Şifreleme) (yalnızca belirli modellerde)

△ **DİKKAT:** Drive Encryption (Sürücü Şifreleme) modülünü kaldırmaya karar verirseniz, önce tüm şifrelenen sürücülerin şifresini çözmeniz gerekir. Bunu yapmazsanız, Drive Encryption (Sürücü Şifreleme) geri yükleme hizmetine kayıt olmadığınız sürece şifrelenen sürücülerdeki verilere erişemezsiniz. Drive Encryption (Sürücü Şifreleme) modülünü yeniden yüklemeniz, şifrelenen sürücülere erişiminizi sağlamaz.

HP ProtectTools için Drive Encryption (Sürücü Şifreleme), bilgisayar sabit sürücünüzü şifreleyerek eksiksiz veri koruması sağlar. Drive Encryption (Sürücü Şifreleme) etkinleştirildiğinde, Windows® işletim sistemi başlatılmadan önce görüntülenen Drive Encryption (Sürücü Şifreleme) oturum açma ekranında oturum açmanız gerekir.

HP ProtectTools Setup Wizard (HP ProtectTools Kurulum Sihirbazı), Windows yöneticilerinin Drive Encryption'ı (Sürücü Şifreleme) etkinleştirmesine, şifreleme anahtarını yedeklemesine, kullanıcı ekleyip kaldırmasına ve Drive Encryption'ı (Sürücü Şifreleme) devre dışı bırakmasına olanak sağlar. Daha fazla bilgi için HP ProtectTools Security Manager (HP ProtectTools Güvenlik Yöneticisi) yazılım Yardımı'na başvurun.

Drive Encryption (Sürücü Şifreleme) ile şu görevler gerçekleştirilebilir:

- Encryption Management (Şifreleme Yönetimi)

  Sürücüleri tek tek şifreleme veya şifresini çözme

  NOT: Yalnızca dahili sabit sürücüler şifrelenebilir.

- Kurtarma
  - Yedekleme anahtarları oluşturma
  - Kurtarma işlemi gerçekleştirme

Kurulum yordamları

Drive Encryption'ı (Sürücü Şifreleme) açma

1. **Başlat**'ı tıklatın, **Tüm Programlar**'ı tıklatın, **HP**'yi ve ardından **HP ProtectTools Administrative Console**'u (HP ProtectTools Yönetim Konsolu) tıklatın.
2. Sol bölmede **Drive Encryption**'ı (Sürücü Şifreleme) tıklatın.

Genel görevler

Drive Encryption'ı (Sürücü Şifreleme) etkinleştirme

Drive Encryption'ı (Sürücü Şifreleme) etkinleştirmek için HP ProtectTools Setup Wizard'ı (HP ProtectTools Kurulum Sihirbazı) kullanın.

NOT: Sihirbaz ayrıca kullanıcı eklemek ve kaldırmak için de kullanılır.

– veya –

1. **Başlat**'ı tıklatın, **Tüm Programlar**'ı tıklatın, **HP**'yi ve ardından **HP ProtectTools Administrative Console**'u (HP ProtectTools Yönetim Konsolu) tıklatın.
2. Sol bölmede, **Security**'yi (Güvenlik) ve ardından **Features**'ı (Özellikler) tıklatın.
3. **Drive Encryption** (Sürücü Şifreleme) onay kutusunu seçip **Next**'i (İleri) tıklatın.
4. **Drives to be encrypted** (Şifrelenecek sürücüler) altında, şifrelemek istediğiniz sabit sürücünün onay kutusunu seçin.
5. Depolama aygıtını uygun yuvaya takın.

   NOT: Şifreleme anahtarını kaydetmek için, FAT32 biçiminde bir USB depolama aygıtı kullanmanız gerekir.
6. **External storage device on which to save encryption key** (Şifreleme anahtarının kaydedileceği harici depolama aygıtı) altında, şifreleme anahtarının kaydedileceği depolama aygıtının onay kutusunu seçin.
7. **Apply**'ı (Uygula) tıklatın.

   Sürücü şifreleme işlemi başlar.

Daha fazla bilgi için HP ProtectTools Security Manager (HP ProtectTools Güvenlik Yöneticisi) yazılımı Yardım bölümüne başvurun.

Drive Encryption'ı (Sürücü Şifreleme) devre dışı bırakma

Drive Encryption'ı (Sürücü Şifreleme) devre dışı bırakmak için HP ProtectTools Setup Wizard'ı (HP ProtectTools Kurulum Sihirbazı) kullanın. Daha fazla bilgi için HP ProtectTools Security Manager (HP ProtectTools Güvenlik Yöneticisi) yazılım Yardımı'na başvurun.

– veya –

1. **Başlat**'ı tıklatın, **Tüm Programlar**'ı tıklatın, **HP**'yi ve ardından **HP ProtectTools Administrative Console**'u (HP ProtectTools Yönetim Konsolu) tıklatın.
2. Sol bölmede, **Security**'yi (Güvenlik) ve ardından **Features**'ı (Özellikler) tıklatın.
3. **Drive Encryption** (Sürücü Şifreleme) onay kutusunu temizleyip **Apply**'ı (Uygula) tıklatın.

   Sürücü şifresini çözme işlemi başlar.

Drive Encryption (Sürücü Şifreleme) etkinleştirildikten sonra oturum açma

Drive Encryption (Sürücü Şifreleme) etkinleştirildikten ve kullanıcı hesabınız kaydedildikten sonra bilgisayarınızı açtığınızda, Drive Encryption (Sürücü Şifreleme) oturum açma ekranından oturum açmanız gerekir:

NOT: Windows yöneticisi HP ProtectTools Security Manager'da (HP ProtectTools Güvenlik Yöneticisi) Pre-Boot Security (Önyükleme Öncesi Güvenlik) özelliğini etkinleştirmişse, Drive Encryption (Sürücü Şifreleme) oturum açma ekranında oturum açmak yerine bilgisayar açıldığında bilgisayarda hemen oturum açarsınız.

1. Kullanıcı adınızı tıklatın ve Windows parolanızı veya Java™ Kartı PIN'inizi yazın ya da kayıtlı bir parmağınızı geçirin.
2. **OK**'i (Tamam) tıklatın.

NOT: Drive Encryption (Sürücü Şifreleme) oturum açma ekranında oturum açmak için bir kurtarma anahtarı kullanırsanız, Windows oturum açma ekranında ayrıca Windows kullanıcı adınızı seçmeniz ve parolanızı girmeniz istenecektir.

Sabit sürücünüzü şifreleyerek verilerinizi koruma

Sabit sürücünüzü şifreleyerek verilerinizi korumak için HP ProtectTools Setup Wizard'ı (HP ProtectTools Kurulum Sihirbazı) kullanın:

1. Security Manager'da, **Getting Started**'ı (Başlarken) ve ardından **Security Manager Setup** (Security Manager Kurulumu) simgesini tıklatın. Security Manager özelliklerini açıklayan bir tanıtım gösterisi başlar. (Security Manager'ı Drive Encryption (Sürücü Şifreleme) sayfasından da başlatabilirsiniz.)
2. Sol bölmede **Drive Encryption**'ı (Sürücü Şifreleme) ve daha sonra **Encryption Management**'ı (Şifreleme Yönetimi) tıklatın.
3. **Change Encryption** (Şifrelemeyi Değiştir) öğesini tıklatın.
4. Şifrelenecek sürücüyü veya sürücüleri seçin.

NOT: Sabit sürücüyü şifrelemeniz önemle önerilir.

Şifreleme durumunu görüntüleme

Kullanıcılar şifreleme durumunu HP ProtectTools Security Manager'dan (HP ProtectTools Güvenlik Yöneticisi) görüntüleyebilirler.

NOT: Sürücü şifreleme durumundaki değişiklikler, HP ProtectTools Administrative Console (HP ProtectTools Yönetim Konsolu) kullanılarak yapılmalıdır.

1. **HP ProtectTools Security Manager**'ı (HP ProtectTools Güvenlik Yöneticisi) açın.
2. **My Data** (Verilerim) altında, **Encryption Status**'ı (Şifreleme Durumu) tıklatın.

   Drive Encryption (Sürücü Şifreleme) etkinse, sürücü durumu aşağıdaki durum kodlarından birini görüntüler:

   - Active (Etkin)
   - Inactive (Etkin değil)

- Not encrypted (Şifrelenmemiş)
- Encrypted (Şifrelenmiş)
- Encrypting (Şifreleniyor)
- Decrypting (Şifre çözülüyor)

Sabit sürücüde şifreleme veya şifre çözme işlemi yapılıyorsa, bir ilerleme çubuğu tamamlanan yüzdeyi ve şifreleme ya da şifre çözme işleminin tamamlanması için kalan süreyi görüntüler.

Gelişmiş görevler

Drive Encryption'ı (Sürücü Şifreleme) (yönetici görevi) yönetme

Encryption Management (Şifreleme Yönetimi) sayfası, yöneticilerin Drive Encryption'ın (Sürücü Şifreleme) durumunu görüntüleyip değiştirmesine (etkin veya etkin değil) ve bilgisayardaki tüm sabit sürücülerin şifreleme durumunu görüntülemesine olanak sağlar.

- Durum Inactive (Etkin değil) ise, Drive Encryption (Sürücü Şifreleme) Windows yöneticisi tarafından HP ProtectTools Security Manager'da (HP ProtectTools Güvenlik Yöneticisi) henüz etkinleştirilmemiştir ve sabit sürücüyü korumuyordur. Drive Encryption'ı (Sürücü Şifreleme) etkinleştirmek için HP ProtectTools Security Manager Setup Wizard'ı (HP ProtectTools Güvenlik Yöneticisi Kurulum Sihirbazı) kullanın.
- Durum Active (Etkin) ise, Drive Encryption (Sürücü Şifreleme) etkinleştirilmiş ve yapılandırılmıştır. Sürücü aşağıdaki durumlardan birindedir:
  - Not encrypted (Şifrelenmemiş)
  - Encrypted (Şifrelenmiş)
  - Encrypting (Şifreleniyor)
  - Decrypting (Şifre çözülüyor)

Sürücüleri tek tek şifreleme veya şifresini çözme

Bilgisayardaki bir veya daha çok sabit sürücüyü şifrelemek veya önceden şifrelenmiş bir sürücünün şifresini çözmek için Change Encryption (Şifrelemeyi Değiştir) özelliğini kullanın:

1. **HP ProtectTools Administrative Console**'u (HP ProtectTools Yönetim Konsolu) açın, **Drive Encryption**'ı (Sürücü Şifreleme) ve ardından **Encryption Management**'ı (Şifreleme Yönetimi) tıklatın.
2. **Change Encryption** (Şifrelemeyi Değiştir) öğesini tıklatın.
3. Change Encryption (Şifrelemeyi Değiştir) iletişim kutusunda, şifrelemek veya şifresini çözmek istediğiniz her sabit sürücünün yanındaki onay kutusunu seçin veya temizleyin ve ardından **OK**'i (Tamam) tıklatın.

NOT: Sürücü şifrelenirken veya sürücünün şifresi çözülürken, ilerleme çubuğu geçerli oturum sırasında işlemin tamamlanması için kalan süreyi gösterir. Şifreleme işlemi sırasında bilgisayar kapatılırsa veya Uyku, Bekleme veya Hazırda Bekletme durumuna geçip yeniden başlatılırsa, Time Remaining (Kalan Süre) ekranı başlangıca sıfırlanır ancak asıl şifreleme işlemi durdurulduğu yerden devam eder. Kalan süre ve ilerleme ekranı, önceki ilerlemeyi yansıtmak için daha hızlı değişecektir.

Yedekleme ve kurtarma (yönetici görevi)

Recovery (Kurtarma) sayfası, yöneticilerin şifreleme anahtarlarını yedeklemesine ve kurtarmasına olanak sağlar.

Local Drive Encryption Key Backup (Yerel Sürücü Şifreleme Anahtarı Yedeklemesi)—Drive Encryption (Sürücü Şifreleme) etkinleştirildiğinde şifreleme anahtarlarını çıkarılabilir medyaya yedeklemenize olanak sağlar.

Yedekleme anahtarları oluşturma

Şifrelenmiş bir sürücünün şifreleme anahtarını çıkarılabilir bir depolama aygıtına yedekleyebilirsiniz:

△ **DİKKAT:** Parolanızı unutmanız veya Java Kartınız'ı kaybetmeniz durumunda sabit sürücünüze erişimi yalnızca bu aygıtla sağlayabileceğinizden, yedekleme anahtarını içeren depolama aygıtını güvenli bir yerde sakladığınızdan emin olun.

1. **HP ProtectTools Administrative Console**'u (HP ProtectTools Yönetim Konsolu) açın, **Drive Encryption**'ı (Sürücü Şifreleme) ve ardından **Recovery**'yi (Kurtarma) tıklatın.
2. **Backup Keys**'i (Yedekleme Anahtarları) tıklatın.
3. Select Backup Disk (Yedekleme Diskini Seçin) sayfasında, şifreleme anahtarınızı yedeklemek istediğiniz aygıtın onay kutusunu seçin ve ardından **Next**'i (İleri) tıklatın.
4. Görüntülenen sonraki sayfadaki bilgileri okuyun ve **Next**'i (İleri) tıklatın. Şifreleme anahtarı seçtiğiniz depolama aygıtına kaydedilir.
5. Onay iletişim kutusu açıldığında **Finish**'i (Son) tıklatın.

Kurtarma işlemini gerçekleştirme

Parolanızı unutmanız durumunda bir kurtarma işlemi gerçekleştirmek için bu adımları izleyin:

1. Bilgisayarı açın.
2. Yedekleme anahtarınızı içeren çıkarılabilir depolama aygıtını takın.
3. HP ProtectTools için Drive Encryption (Sürücü Şifreleme) oturum açma iletişim kutusu açıldığında **Cancel**'ı (İptal) tıklatın.
4. Ekranın sol alt kısmındaki **Options**'ı (Seçenekler) tıklatın ve ardından **Recovery**'yi (Kurtarma) tıklatın.
5. Yedekleme anahtarınızı içeren dosyayı seçin veya dosyayı aramak için **Browse**'ı (Gözat) tıklatın ve ardından **Next**'i (İleri) tıklatın.
6. Onay iletişim kutusu görüntülendiğinde **OK**'i (Tamam) tıklatın.

   Bilgisayarınız başlatılır.

NOT: Kurtarma işlemi gerçekleştirmeden önce parolanızı sıfırlamanız önemle önerilir.

9 HP ProtectTools için Privacy Manager (Gizlilik Yöneticisi) (yalnızca belirli modellerde)

HP ProtectTools için Privacy Manager (Gizlilik Yöneticisi), e-posta, Microsoft® Office belgeleri veya anında mesajlaşma (IM) kullanırken iletişimin kaynağını, doğruluğunu ve güvenliğini doğrulamak için gelişmiş güvenlik oturum açma (kimlik doğrulaması) yöntemlerini kullanmanıza olanak sağlar.

Privacy Manager (Gizlilik Yöneticisi), aşağıdaki güvenlik oturum açma yöntemlerini içeren HP ProtectTools Security Manager (HP ProtectTools Güvenlik Yöneticisi) tarafından sağlanan güvenlik altyapısını geliştirir:

- Parmak izi kimlik doğrulaması
- Windows® parolası
- HP ProtectTools Java™ Kartı

Privacy Manager'da (Gizlilik Yöneticisi) yukarıdaki güvenlik oturum açma yöntemlerinden herhangi birini kullanabilirsiniz.

Privacy Manager (Gizlilik Yöneticisi) aşağıdakileri gerektirir:

- HP ProtectTools Security Manager (Güvenlik Yöneticisi) 5.00 veya üzeri
- Windows® 7, Windows Vista® veya Windows XP işletim sistemi
- Microsoft Outlook 2007 veya Microsoft Outlook 2003
- Geçerli e-posta hesabı

NOT: Güvenlik özelliklerine erişebilmeniz için, bir Privacy Manager (Gizlilik Yöneticisi) Sertifikası'nın istenmesi ve Privacy Manager (Gizlilik Yöneticisi) içinden yüklenmesi gerekir. Privacy Manager (Gizlilik Yöneticisi) Sertifikası istemeye yönelik bilgi için, bkz. Privacy Manager (Gizlilik Yöneticisi) Sertifikası isteme ve yükleme sayfa 48.

Kurulum yordamları

Privacy Manager'ı (Gizlilik Yöneticisi) açma

Privacy Manager'ı (Gizlilik Yöneticisi) açmak için:

1. **Başlat**'ı tıklatın, **Tüm Programlar**'ı tıklatın, **HP**'yi ve ardından **HP ProtectTools Security Manager**'ı (HP ProtectTools Güvenlik Yöneticisi) tıklatın.
2. **Privacy Manager**'ı (Gizlilik Yöneticisi) tıklatın.

– veya –

Görev çubuğunun en sağında, bildirim alanındaki **HP ProtectTools** simgesini sağ tıklatın ve **Privacy Manager**'ı (Gizlilik Yöneticisi) tıklatın, ardından **Configuration**'ı (Yapılandırma) tıklatın.

– veya –

Bir Microsoft Outlook e-posta iletisinin araç çubuğunda, **Send Securely**'nin (Güvenli Gönder) yanındaki aşağı oku tıklatın ve ardından **Certificates**'i (Sertifikalar) veya **Trusted Contacts**'i (Güvenilen Kişiler) tıklatın.

– veya –

Bir Microsoft Office belgesinin araç çubuğunda, **Sign and Encrypt**'in (İmzala ve Şifrele) yanındaki aşağı oku tıklatın ve ardından **Certificates**'i (Sertifikalar) veya **Trusted Contacts**'i (Güvenilen Kişiler) tıklatın.

Privacy Manager (Gizlilik Yöneticisi) Sertifikaları'nı yönetme

Privacy Manager (Gizlilik Yöneticisi) Sertifikaları, verileri ve iletileri ortak anahtar altyapısı (public key infrastructure - PKI) adı verilen bir şifreleme teknolojisi kullanarak korur. PKI, kullanıcıların şifreleme anahtarları ve bir sertifika yetkilisi (CA) tarafından verilen Privacy Manager (Gizlilik Yöneticisi) Sertifikası edinmesini gerektirir. Yalnızca periyodik olarak kimlik doğrulaması yapmanızı gerektiren çoğu veri şifreleme ve kimlik doğrulaması yazılımının aksine, Privacy Manager (Gizlilik Yöneticisi) bir şifreleme anahtarı kullanarak her e-posta veya Microsoft Office belgesi imzalayışınızda kimlik doğrulaması gerektirir. Privacy Manager (Gizlilik Yöneticisi), önemli bilgilerin kaydedilmesini ve gönderilmesini emniyetli ve güvenli hale getirir.

Aşağıdaki görevleri gerçekleştirebilirsiniz:

- Privacy Manager (Gizlilik Yöneticisi) Sertifikası isteme ve yükleme
- Privacy Manager (Gizlilik Yöneticisi) Sertifikası ayrıntılarını görüntüleme
- Privacy Manager (Gizlilik Yöneticisi) Sertifikaları'nı yenileme
- Birden çok sertifika kullanılabilir durumda olduğunda, Privacy Manager (Gizlilik Yöneticisi) tarafından kullanılmak üzere varsayılan bir Privacy Manager (Gizlilik Yöneticisi) Sertifikası ayarlama
- Privacy Manager (Gizlilik Yöneticisi) Sertifikası'nı silme veya iptal etme (gelişmiş)

Privacy Manager (Gizlilik Yöneticisi) Sertifikası isteme ve yükleme

Privacy Manager (Gizlilik Yöneticisi) özelliklerini kullanabilmeniz için geçerli bir e-posta adresi kullanarak bir Privacy Manager (Gizlilik Yöneticisi) Sertifikası isteyip yüklemeniz (Privacy Manager (Gizlilik

Yöneticisi) içinden) gerekir. E-posta adresi Privacy Manager (Gizlilik Yöneticisi) Sertifikası'nı istediğiniz bilgisayarda, Microsoft Outlook içindeki bir hesap olarak kurulmuş olmalıdır.

Privacy Manager (Gizlilik Yöneticisi) Sertifikası isteme

1. Privacy Manager'ı (Gizlilik Yöneticisi) açın ve **Certificates**'i (Sertifikalar) tıklatın.
2. **Request a Privacy Manager certificate**'i (Gizlilik Yöneticisi sertifikası iste) tıklatın.
3. Welcome (Hoş Geldiniz) sayfasındaki metni okuduktan sonra **Next**'i (İleri) tıklatın.
4. License Agreement (Lisans Sözleşmesi) sayfasında, lisans sözleşmesini okuyun.
5. **Check here to accept the terms of this license agreement** (Bu lisans sözleşmesinin şartlarını kabul etmek için burayı işaretleyin) öğesinin yanındaki onay kutusunun seçili olduğundan emin olun ve **Next**'i (İleri) tıklatın.
6. Your Certificate Details (Sertifika Ayrıntılarınız) sayfasında, gerekli bilgileri girin ve ardından **Next**'i (İleri) tıklatın.
7. "Certificate Request Accepted" (Sertifika İsteği Kabul Edildi) sayfasında **Finish**'i (Son) tıklatın.
8. Sertifikayı kapatmak için **OK**'i (Tamam) tıklatın.

Microsoft Outlook'da, Privacy Manager (Gizlilik Yöneticisi) Sertifikanız'ı içeren bir e-posta alacaksınız.

Önceden atanmış bir Privacy Manager (Gizlilik Yöneticisi) Şirket Sertifikası edinme

1. Outlook'ta, almış olduğunuz ve size önceden bir Şirket Sertifikası atandığını belirten e-postayı açın.
2. **Obtain**'i (Edinin) tıklatın.
3. Microsoft Outlook'da, Privacy Manager (Gizlilik Yöneticisi) Sertifikanız'ı içeren bir e-posta alacaksınız.
4. Sertifikayı yüklemek için bkz. Privacy Manager (Gizlilik Yöneticisi) Sertifikası yükleme sayfa 49

Privacy Manager (Gizlilik Yöneticisi) Sertifikası yükleme

1. Privacy Manager (Gizlilik Yöneticisi) Sertifikanız'ı içeren e-postayı aldığınızda, e-postayı açın ve Outlook 2007'de iletinin sağ alt köşesinde veya Outlook 2003'te sol üst köşesinde bulunan **Setup** (Kurulum) düğmesini tıklatın.
2. Seçtiğiniz güvenlik oturum açma yöntemini kullanarak kimlik doğrulaması yapın.
3. Certificate Installed (Sertifika Yüklendi) sayfasında, **Next**'i (İleri) tıklatın.
4. Certificate Backup (Sertifika Yedeklemesi) sayfasında, yedekleme dosyası için bir konum ve ad girin veya konum aramak için **Browse**'ı (Gözat) tıklatın.

△ **DİKKAT:** Dosyayı, sabit sürücünüzün dışındaki bir konuma kaydettiğinizden ve güvenli bir yerde sakladığınızdan emin olun. Bu dosya yalnızca sizin kullanımınız içindir ve Privacy Manager (Gizlilik Yöneticisi) Sertifikanız'ı ve ilişkili anahtarları geri yüklemeniz gereken durumlarda gereklidir.

5. Bir parola oluşturun ve onaylayın, ardından **Next**'i (İleri) tıklatın.

6. Seçtiğiniz güvenlik oturum açma yöntemini kullanarak kimlik doğrulaması yapın.

7. Güvenilen Kişi davet etme işlemine başlamayı seçerseniz, Microsoft Outlook kişilerini kullanarak Güvenilen Kişiler ekleme sayfa 53 konusunda adım 2'den başlayan ekrandaki talimatları izleyin.

   – veya –

   Cancel'ı (İptal) tıklatırsanız, daha sonra bir Güvenilen Kişi ekleme ile ilgili bilgiler için Güvenilen Kişi ekleme sayfa 52 konusuna bakın.

Privacy Manager (Gizlilik Yöneticisi) Sertifikası ayrıntılarını görüntüleme

1. Privacy Manager'ı (Gizlilik Yöneticisi) açın ve **Certificates**'i (Sertifikalar) tıklatın.
2. Bir Privacy Manager (Gizlilik Yöneticisi) Sertifikası'nı tıklatın.
3. **Certificate details**'ı (Sertifika ayrıntıları) tıklatın.
4. Ayrıntıları görüntülemeyi tamamladığınızda **OK**'i (Tamam) tıklatın.

Privacy Manager (Gizlilik Yöneticisi) Sertifikası'nı yenileme

Privacy Manager (Gizlilik Yöneticisi) Sertifikanız'ın süre dolum tarihi yaklaştığında, sertifikayı yenilemeniz gerektiği konusunda uyarılırsınız:

1. Privacy Manager'ı (Gizlilik Yöneticisi) açın ve **Certificates**'i (Sertifikalar) tıklatın.
2. **Renew certificate**'ı (Sertifikayı yenile) tıklatın.
3. Yeni bir Privacy Manager (Gizlilik Yöneticisi) Sertifikası satın almak için ekrandaki yönergeleri izleyin.

NOT: Privacy Manager (Gizlilik Yöneticisi) Sertifikası yenileme işlemi, eski Privacy Manager (Gizlilik Yöneticisi) Sertifikanız'ı değiştirmez. Yeni bir Privacy Manager (Gizlilik Yöneticisi) Sertifikası satın almanız ve Privacy Manager (Gizlilik Yöneticisi) Sertifikası isteme ve yükleme sayfa 48 ile aynı yordamı kullanarak yüklemeniz gerekir.

Varsayılan bir Privacy Manager (Gizlilik Yöneticisi) Sertifikası ayarlama

Bilgisayarınızda diğer sertifika yetkililerinin verdiği ek sertifikalar yüklü olsa da, Privacy Manager (Gizlilik Yöneticisi) içinden yalnızca Privacy Manager (Gizlilik Yöneticisi) Sertifikaları görülebilir.

Bilgisayarınızda Privacy Manager (Gizlilik Yöneticisi) içinden yüklenmiş birden fazla Privacy Manager (Gizlilik Yöneticisi) Sertifikası varsa, birini varsayılan sertifika olarak belirtebilirsiniz:

1. Privacy Manager'ı (Gizlilik Yöneticisi) açın ve **Certificates**'i (Sertifikalar) tıklatın.
2. Varsayılan olarak kullanmak istediğiniz Privacy Manager (Gizlilik Yöneticisi) Sertifikası'nı ve **Set default**'u (Varsayılan olarak ayarla) tıklatın.
3. **OK**'i (Tamam) tıklatın.

NOT: Varsayılan Privacy Manager (Gizlilik Yöneticisi) Sertifikanız'ı kullanmanız zorunlu değildir. Çeşitli Privacy Manager (Gizlilik Yöneticisi) işlevleri içinden, Privacy Manager (Gizlilik Yöneticisi) Sertifikalarınız'dan herhangi birini kullanmak için seçebilirsiniz.

Privacy Manager (Gizlilik Yöneticisi) Sertifikası'nı silme

Bir Privacy Manager (Gizlilik Yöneticisi) Sertifikası'nı silerseniz, bu sertifikayla şifrelediğiniz herhangi bir dosyayı açamaz veya veriyi görüntüleyemezsiniz. Bir Privacy Manager (Gizlilik Yöneticisi) Sertifikası'nı yanlışlıkla sildiyseniz, sertifikayı yüklediğinizde oluşturduğunuz yedekleme dosyasını kullanarak geri yükleyebilirsiniz. Daha fazla bilgi için bkz. Privacy Manager (Gizlilik Yöneticisi) Sertifikası'nı geri yükleme sayfa 51.

Bir Privacy Manager (Gizlilik Yöneticisi) Sertifikası'nı silmek için:

1. Privacy Manager'ı (Gizlilik Yöneticisi) açın ve **Certificates**'i (Sertifikalar) tıklatın.
2. Silmek istediğiniz Privacy Manager (Gizlilik Yöneticisi) Sertifikası'nı ve ardından **Advanced**'i (Gelişmiş) tıklatın.
3. **Delete**'i (Sil) tıklatın.
4. Onay iletişim kutusu açıldığında **Yes**'i (Evet) tıklatın.
5. **Close**'u (Kapat) ve ardından **Apply**'ı (Uygula) tıklatın.

Privacy Manager (Gizlilik Yöneticisi) Sertifikası'nı geri yükleme

Privacy Manager (Gizlilik Yöneticisi) sertifikanızın yüklemesi sırasında, sertifikanın yedekleme kopyasını oluşturmanız gerekir. Ayrıca, Migration (Geçiş) sayfasından da bir yedekleme kopyası oluşturabilirsiniz. Bu yedekleme kopyası, başka bir bilgisayara geçiş yaparken veya aynı bilgisayarda bir sertifikayı geri yüklemek için kullanılabilir.

1. Privacy Manager'ı (Gizlilik Yöneticisi) açın ve **Migration**'ı (Geçiş) tıklatın.
2. **Restore**'u (Geri yükle) tıklatın.
3. Migration File (Geçiş Dosyası) sayfasında, yedekleme işlemi sırasında oluşturduğunuz .dppsm dosyasını aramak için **Browse**'ı (Gözat) tıklatın ve daha sonra **Next**'i (İleri) tıklatın.
4. Yedeklemeyi oluşturduğunuzda kullandığınız parolayı girin ve ardından **Next**'i (İleri) tıklatın.
5. **Finish**'i (Son) tıklatın.
6. **OK**'i (Tamam) tıklatın.

Daha fazla bilgi için bkz. Privacy Manager (Gizlilik Yöneticisi) Sertifikası yükleme sayfa 49 veya Privacy Manager (Gizlilik Yöneticisi) Sertifikaları'nı ve Güvenilen Kişiler'i yedekleme sayfa 67.

Privacy Manager (Gizlilik Yöneticisi) Sertifikanız'ı iptal etme

Privacy Manager (Gizlilik Yöneticisi) Sertifikanız'ın güvenliğinin tehlikeye altında olduğunu düşünüyorsanız, kendi sertifikanızı iptal edebilirsiniz:

NOT: İptal edilmiş bir Privacy Manager (Gizlilik Yöneticisi) Sertifikası silinmez. Sertifika, hala şifrelenmiş dosyaları görüntülemek için kullanılabilir.

1. Privacy Manager'ı (Gizlilik Yöneticisi) açın ve **Certificates**'i (Sertifikalar) tıklatın.
2. **Advanced**'i (Gelişmiş) tıklatın.
3. İptal etmek istediğiniz Privacy Manager (Gizlilik Yöneticisi) Sertifikası'nı ve ardından **Revoke**'u (İptal Et) tıklatın.

4. Onay iletişim kutusu açıldığında **Yes**'i (Evet) tıklatın.
5. Seçtiğiniz güvenlik oturum açma yöntemini kullanarak kimlik doğrulaması yapın.
6. Ekranda görüntülenen yönergeleri izleyin.

Güvenilen Kişiler'i yönetme

Güvenilen Kişiler, karşılıklı olarak güvenli bir şekilde iletişim kurmanıza olanak sağlayacak şekilde Privacy Manager (Gizlilik Yöneticisi) Sertifikası alışverişinde bulunduğunuz kullanıcılardır.

Trusted Contacts Manager (Güvenilen Kişiler Yöneticisi) aşağıdaki görevleri gerçekleştirmenize olanak tanır:

- Güvenilen Kişi ayrıntılarını görüntüleme
- Güvenilen Kişiler'i silme
- Güvenilen Kişiler'in iptal durumunu denetleme (gelişmiş)

Güvenilen Kişiler ekleme

Güvenilen Kişiler ekleme, 3 adımdan oluşan bir işlemdir:

1. Bir Güvenilen Kişi alıcısına e-posta davetiyesi gönderirsiniz.
2. Güvenilen Kişi alıcısı e-posta'yı yanıtlar.
3. Güvenilen Kişi alıcısından gelen e-posta yanıtını alır ve **Accept**'i (Kabul Et) tıklatırsınız.

Güvenilen Kişi e-posta davetiyelerini bireysel olarak alıcılara veya Microsoft Outlook adres defterinizdeki tüm kişilere gönderebilirsiniz.

Güvenilen Kişiler eklemek için sonraki bölümlere bakın.

NOT: Güvenilen Kişi olma davetinize yanıt vermek için, Güvenilen Kişi alıcılarının bilgisayarında Privacy Manager (Gizlilik Yöneticisi) veya alternatif istemci yüklü olmalıdır. Alternatif istemciyi yüklemeye yönelik bilgiler için, http://DigitalPersona.com/PrivacyManager adresindeki DigitalPersona Web sitesine erişin.

Güvenilen Kişi ekleme

1. Privacy Manager'ı (Gizlilik Yöneticisi) açın, **Trusted Contacts Manager**'ı (Güvenilen Kişiler Yöneticisi) ve ardından **Invite Contacts**'i (Kişileri Davet Et) tıklatın.

   – veya –

   Microsoft Outlook'ta, araç çubuğunda bulunan **Send Securely** (Güvenli Gönder) öğesinin yanındaki aşağı oku ve ardından **Invite Contacts**'i (Kişileri Davet Et) tıklatın.
2. Select Certificate (Sertifika Seçin) iletişim kutusu açılırsa, kullanmak istediğiniz Privacy Manager (Gizlilik Yöneticisi) Sertifikası'nı ve ardından **OK**'i (Tamam) tıklatın.
3. Trusted Contact Invitation (Güvenilen Kişi Davetiyesi) iletişim kutusu açıldığında, metni okuyup **OK**'i (Tamam) tıklatın.

   Otomatik olarak bir e-posta oluşturulur.
4. Güvenilen Kişi olarak eklemek istediğiniz alıcılara ait bir veya daha fazla e-posta adresini girin.

5. Metni düzenleyin ve adınızla imzalayın (isteğe bağlı).

6. **Send**'i (Gönder) tıklatın.

NOT: Bir Privacy Manager (Gizlilik Yöneticisi) Sertifikası edinmediyseniz, bir ileti size Güvenilen Kişi isteği göndermek için Privacy Manager (Gizlilik Yöneticisi) Sertifikanız olması gerektiğini bildirir. Certificate Request Wizard'ı (Sertifika İsteme Sihirbazı) başlatmak için **OK**'i (Tamam) tıklatın. Daha fazla bilgi için bkz. Privacy Manager (Gizlilik Yöneticisi) Sertifikası isteme ve yükleme sayfa 48.

7. Seçtiğiniz güvenlik oturum açma yöntemini kullanarak kimlik doğrulaması yapın.

NOT: E-posta Güvenilen Kişi alıcısı tarafından alındığında, alıcı e-postayı açıp sağ alt köşesindeki **Accept** (Kabul Et) seçeneğini tıklatmalı ve ardından onay iletişim kutusu açıldığında **OK**'i (Tamam) tıklatmalıdır.

8. Güvenilen Kişi olma davetini kabul eden alıcıdan bir e-posta yanıtı aldığınızda, e-postanın sağ alt köşesindeki **Accept**'i (Kabul Et) tıklatın.

   Alıcının başarıyla Güvenilen Kişiler listenize eklendiğini onaylayan bir iletişim kutusu açılır.

9. **OK**'i (Tamam) tıklatın.

Microsoft Outlook kişilerini kullanarak Güvenilen Kişiler ekleme

1. Privacy Manager'ı (Gizlilik Yöneticisi) açın, **Trusted Contacts Manager**'ı (Güvenilen Kişiler Yöneticisi) ve ardından **Invite Contacts**'i (Kişileri Davet Et) tıklatın.

   – veya –

   Microsoft Outlook'ta, araç çubuğunda bulunan **Send Securely** (Güvenli Gönder) öğesinin yanındaki aşağı oku ve ardından **Invite All My Outlook Contacts**'i (Tüm Outlook Kişilerimi Davet Et) tıklatın.

2. Trusted Contact Invitation (Güvenilen Kişi Davetiyesi) sayfası açıldığında, Trusted Contacts (Güvenilen Kişi) olarak eklemek istediğiniz alıcıların e-posta adreslerini seçin ve ardından **Next**'i (İleri) tıklatın.

3. Sending Invitation (Davetiye Gönderiliyor) sayfası açıldığında, **Finish**'i (Son) tıklatın.

   Seçilen Microsoft Outlook e-posta adreslerini listeleyen bir e-posta otomatik olarak oluşturulur.

4. Metni düzenleyin ve adınızla imzalayın (isteğe bağlı).

5. **Send**'i (Gönder) tıklatın.

NOT: Bir Privacy Manager (Gizlilik Yöneticisi) Sertifikası edinmediyseniz, bir ileti size Güvenilen Kişi isteği göndermek için Privacy Manager (Gizlilik Yöneticisi) Sertifikanız olması gerektiğini bildirir. Certificate Request Wizard'ı (Sertifika İsteme Sihirbazı) başlatmak için **OK**'i (Tamam) tıklatın. Daha fazla bilgi için bkz. Privacy Manager (Gizlilik Yöneticisi) Sertifikası isteme ve yükleme sayfa 48.

6. Seçtiğiniz güvenlik oturum açma yöntemini kullanarak kimlik doğrulaması yapın.

NOT: E-posta Güvenilen Kişi alıcısı tarafından alındığında, alıcı e-postayı açıp sağ alt köşesindeki **Accept** (Kabul Et) seçeneğini tıklatmalı ve ardından onay iletişim kutusu açıldığında **OK**'i (Tamam) tıklatmalıdır.

7. Güvenilen Kişi olma davetini kabul eden alıcıdan bir e-posta yanıtı aldığınızda, e-postanın sağ alt köşesindeki **Accept**'i (Kabul Et) tıklatın.

   Alıcının başarıyla Güvenilen Kişiler listenize eklendiğini onaylayan bir iletişim kutusu açılır.

8. **OK**'i (Tamam) tıklatın.

Güvenilen Kişi ayrıntılarını görüntüleme

1. Privacy Manager'ı (Gizlilik Yöneticisi) açın ve **Trusted Contacts**'i (Güvenilen Kişiler) tıklatın.
2. Bir Güvenilen Kişi'yi tıklatın.
3. **Contact details**'ı (Kişi ayrıntıları) tıklatın.
4. Ayrıntıları görüntülemeyi tamamladığınızda **OK**'i (Tamam) tıklatın.

Güvenilen Kişi'yi silme

1. Privacy Manager'ı (Gizlilik Yöneticisi) açın ve **Trusted Contacts**'i (Güvenilen Kişiler) tıklatın.
2. Silmek istediğiniz Güvenilen Kişi'yi tıklatın.
3. **Delete contact**'i (Kişiyi sil) tıklatın.
4. Onay iletişim kutusu açıldığında **Yes**'i (Evet) tıklatın.

Bir Güvenilen Kişi'nin iptal durumunu denetleme

Bir Güvenilen Kişi'nin Privacy Manager (Gizlilik Yöneticisi) Sertifikası'nı iptal edip etmediğini öğrenmek için:

1. Privacy Manager'ı (Gizlilik Yöneticisi) açın ve **Trusted Contacts**'i (Güvenilen Kişiler) tıklatın.
2. Bir Güvenilen Kişi'yi tıklatın.
3. **Advanced** (Gelişmiş) düğmesini tıklatın.

   Advanced Trusted Contact Management (Gelişmiş Güvenilen Kişi Yönetimi) iletişim kutusu açılır.

4. **Check Revocation**'ı (İptal Durumunu Denetle) tıklatın.
5. **Close**'u (Kapat) tıklatın.

Genel görevler

Privacy Manager'ı (Gizlilik Yöneticisi) aşağıdaki Microsoft ürünleriyle kullanabilirsiniz:

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

Privacy Manager'ı (Gizlilik Yöneticisi) Microsoft Outlook'ta kullanma

Privacy Manager (Gizlilik Yöneticisi) yüklendiğinde, Microsoft Outlook araç çubuğunda bir Privacy (Gizlilik) düğmesi ve her Microsoft Outlook e-posta iletisinin araç çubuğunda bir Send Securely (Güvenli Gönder) düğmesi görüntülenir. **Privacy** (Gizlilik) veya **Send Securely**'nin (Güvenli Gönder) yanındaki aşağı oku tıklattığınızda, şu seçenekler arasından seçim yapabilirsiniz:

- Sign and Send (İmzala ve Gönder) (Yalnızca Send Securely (Güvenli Gönder) düğmesi))—Bu seçenek, e-postaya bir dijital imza ekler, e-postayı şifreler ve seçtiğiniz güvenlik oturum açma yöntemini kullanarak kimliğinizi doğrulamanızın ardından e-postayı gönderir.
- Seal for Trusted Contacts and Send (Güvenilen Kişiler için Mühürle ve Gönder) (Yalnızca Send Securely (Güvenli Gönder) düğmesi)—Bu seçenek, bir dijital imza ekler, e-postayı şifreler ve seçtiğiniz güvenlik oturum açma yöntemini kullanarak kimliğinizi doğrulamanızın ardından e-postayı gönderir.
- Invite Contacts (Kişileri Davet Et)—Bu seçenek, bir Güvenilen Kişi davetiyesi göndermenize olanak sağlar. Daha fazla bilgi için bkz. Güvenilen Kişi ekleme sayfa 52.
- Invite Outlook Contacts (Outlook Kişilerini Davet Et)—Bu seçenek, Microsoft Outlook adres defterinizdeki tüm kişilere Güvenilen Kişi davetiyesi göndermenize olanak sağlar. Daha fazla bilgi için bkz. Microsoft Outlook kişilerini kullanarak Güvenilen Kişiler ekleme sayfa 53.
- Open the Privacy Manager software (Gizlilik Yöneticisi yazılımını aç)—Certificates (Sertifikalar), Trusted Contacts (Güvenilen Kişiler) ve Settings (Ayarlar) seçenekleri, geçerli ayarları eklemek, görüntülemek ve değiştirmek için Privacy Manager (Gizlilik Yöneticisi) yazılımını açmanıza olanak sağlar. Daha fazla bilgi için bkz. Privacy Manager'ı (Gizlilik Yöneticisi) Microsoft Outlook için yapılandırma sayfa 55.

Privacy Manager'ı (Gizlilik Yöneticisi) Microsoft Outlook için yapılandırma

1. Privacy Manager'ı (Gizlilik Yöneticisi) açın, **Settings**'i (Ayarlar) ve ardından **E-mail** (E-posta) sekmesini tıklatın.

   – veya –

   Ana Microsoft Outlook araç çubuğunda, **Send Securely**'nin (Güvenli Gönder) (Outlook 2003'te **Privacy** (Gizlilik) olarak adlandırılır) yanındaki aşağı oku ve ardından **Settings**'i (Ayarlar) tıklatın.

   – veya –

   Bir Microsoft e-posta iletisinin araç çubuğunda, **Send Securely**'nin (Güvenli Gönder) yanındaki aşağı oku tıklatın ve ardından **Settings**'i (Ayarlar) tıklatın.

2. Güvenli e-posta gönderirken gerçekleştirmek istediğiniz eylemleri seçin ve **OK**'i (Tamam) tıklatın.

E-posta iletisini imzalama ve gönderme

1. Microsoft Outlook'ta, **New**'ı (Yeni) veya **Reply**'ı (Yanıtla) tıklatın.
2. E-posta iletinizi yazın.
3. **Send Securely**'nin (Güvenli Gönder) (Outlook 2003'te **Privacy** (Gizlilik) olarak adlandırılır) yanındaki aşağı oku tıklatın ve ardından **Sign and Send**'i (İmzala ve Gönder) tıklatın.
4. Seçtiğiniz güvenlik oturum açma yöntemini kullanarak kimlik doğrulaması yapın.

E-posta iletisini mühürleme ve gönderme

Dijital olarak imzalanan ve mühürlenen (şifrelenen) mühürlenmiş e-posta iletileri yalnızca Güvenilen Kişiler listenizden seçtiğiniz kişiler tarafından görüntülenebilir.

E-posta iletisini mühürlemek ve bir Güvenilen Kişi'ye göndermek için:

1. Microsoft Outlook'ta, **New**'ı (Yeni) veya **Reply**'ı (Yanıtla) tıklatın.
2. E-posta iletinizi yazın.
3. **Send Securely**'nin (Güvenli Gönder) (Outlook 2003'te **Privacy** (Gizlilik) olarak adlandırılır) yanındaki aşağı oku tıklatın ve ardından **Seal for Trusted Contacts and Send**'i (Güvenilen Kişiler için Mühürle ve Gönder) tıklatın.
4. Seçtiğiniz güvenlik oturum açma yöntemini kullanarak kimlik doğrulaması yapın.

Mühürlenmiş bir e-posta iletisini görüntüleme

Mühürlenmiş bir e-posta iletisini açtığınızda, güvenlik etiketi e-postanın başlık bölümünde görüntülenir. Güvenlik etiketi aşağıdaki bilgileri sağlar:

- E-postayı imzalayan kişinin kimliğini doğrulamak için hangi kimlik bilgilerinin kullanıldığı
- E-postayı imzalayan kişinin kimlik bilgilerini doğrulamak için kullanılan ürün

Privacy Manager'ı (Gizlilik Yöneticisi) bir Microsoft Office 2007 belgesinde kullanma

NOT: Privacy Manager (Gizlilik Yöneticisi), yalnızca Microsoft Office 2007 belgeleriyle kullanılabilir.

Privacy Manager (Gizlilik Yöneticisi) Sertifikanız'ı yükledikten sonra, tüm Microsoft Word, Microsoft Excel ve Microsoft PowerPoint belgelerinin araç çubuğunun sağ tarafında bir Sign and Encrypt (İmzala ve Şifrele) düğmesi görüntülenir. **Sign and Encrypt**'in (İmzala ve Şifrele) yanındaki aşağı oku tıklattığınızda, şu seçenekler arasından seçim yapabilirsiniz:

- Sign Document (Belgeyi İmzala)—Bu seçenek, dijital imzanızı belgeye ekler.
- Add Signature Line Before Signing (İmzalamadan Önce İmza Satırı Ekle) (Yalnızca Microsoft Word ve Microsoft Excel)—Varsayılan olarak, bir Microsoft Word veya Microsoft Excel belgesi imzalandığında veya şifrelendiğinde bir imza satırı eklenir. Bu seçeneği kapatmak için, onay işaretini kaldırmak üzere **Add Signature Line**'ı (İmza Satırı Ekle) tıklatın.
- Encrypt Document (Belgeyi Şifrele)—Bu seçenek, dijital imzanızı ekler ve belgeyi şifreler.

- Remove Encryption (Şifrelemeyi Kaldır)—Bu seçenek, belgenin şifrelemesini kaldırır.
- Open the Privacy Manager software (Gizlilik Yöneticisi yazılımını aç)—Certificates (Sertifikalar), Trusted Contacts (Güvenilen Kişiler) ve Settings (Ayarlar) seçenekleri, geçerli ayarları eklemek, görüntülemek ve değiştirmek için Privacy Manager (Gizlilik Yöneticisi) yazılımını açmanıza olanak sağlar. Daha fazla bilgi için bkz. Privacy Manager (Gizlilik Yöneticisi) Sertifikaları'nı yönetme sayfa 48, Güvenilen Kişiler'i yönetme sayfa 52 veya Privacy Manager'ı (Gizlilik Yöneticisi) Microsoft Office için yapılandırma sayfa 57.

Privacy Manager'ı (Gizlilik Yöneticisi) Microsoft Office için yapılandırma

1. Privacy Manager'ı (Gizlilik Yöneticisi) açın, **Settings**'i (Ayarlar) ve ardından **Documents** (Belgeler) sekmesini tıklatın.

   – veya –

   Bir Microsoft Office belgesinin araç çubuğunda, **Sign and Encrypt**'in (İmzala ve Şifrele) yanındaki aşağı oku tıklatın ve ardından **Settings**'i (Ayarlar) tıklatın.

2. Yapılandırmak istediğiniz eylemleri ve ardından **OK**'i (Tamam) tıklatın.

Microsoft Office belgesini imzalama

1. Microsoft Word, Microsoft Excel veya Microsoft PowerPoint'te bir belge oluşturup kaydedin.
2. **Sign and Encrypt**'in (İmzala ve Şifrele) yanındaki aşağı oku ve ardından **Sign Document**'ı (Belgeyi İmzala) tıklatın.
3. Seçtiğiniz güvenlik oturum açma yöntemini kullanarak kimlik doğrulaması yapın.
4. Onay iletişim kutusu açıldığında, metni okuyup **OK**'i (Tamam) tıklatın.

Daha sonra belgeyi düzenlemeye karar verirseniz, şu adımları izleyin:

1. Ekranın sol üst köşesindeki **Office** düğmesini tıklatın.
2. **Prepare**'i (Hazırla) ve daha sonra **Mark as Final**'ı (Son olarak İşaretle) tıklatın.
3. Onay iletişim kutusu açıldığında **Yes**'i (Evet) tıklatın ve çalışmaya devam edin.
4. Düzenlemeyi bitirdiğinizde, belgeyi tekrar imzalayın.

Bir Microsoft Word veya Microsoft Excel belgesini imzalarken imza satırı ekleme

Privacy Manager (Gizlilik Yöneticisi), bir Microsoft Word veya Microsoft Excel belgesini imzalarken bir imza satırı eklemenize olanak sağlar:

1. Microsoft Word veya Microsoft Excel'de bir belge oluşturup kaydedin.
2. **Home** (Giriş) menüsünü tıklatın.
3. **Sign and Encrypt**'in (İmzala ve Şifrele) yanındaki aşağı oku ve ardından **Add Signature Line Before Signing**'i (İmzalamadan Önce İmza Satırı Ekle) tıklatın.

NOT: Add Signature Line Before Signing (İmzalamadan Önce İmza Satırı Ekle) seçeneği belirlendiğinde, seçeneğin yanında bir onay işareti görüntülenir. Varsayılan olarak, bu seçenek etkinleştirilmiştir.

4. **Sign and Encrypt**'in (İmzala ve Şifrele) yanındaki aşağı oku ve ardından **Sign Document**'ı (Belgeyi İmzala) tıklatın.

5. Seçtiğiniz güvenlik oturum açma yöntemini kullanarak kimlik doğrulaması yapın.

Bir Microsoft Word veya Microsoft Excel belgesine önerilen imzalayanlar ekleme

Önerilen imzalayanlar atayarak belgenize birden fazla imza satırı ekleyebilirsiniz. Önerilen imzalayan, bir Microsoft Word veya Microsoft Excel belgesinin sahibi tarafından belgeye imza satırı eklemek üzere atanan bir kullanıcıdır. Önerilen imzalayanlar, siz veya belgenizi imzalamasını istediğiniz başka biri olabilir. Örneğin, departmanınızdaki tüm çalışanlar tarafından imzalanması gereken bir belge hazırlarsanız, belirli bir tarihe kadar imzalamaya yönelik yönergeler ile birlikte söz konusu kullanıcılar için belgenin son sayfasının en altına imza satırları ekleyebilirsiniz.

Bir Microsoft Word veya Microsoft Excel belgesine önerilen imzalayan eklemek için:

1. Microsoft Word veya Microsoft Excel'de bir belge oluşturup kaydedin.

2. **Insert** (Ekle) menüsünü tıklatın.

3. Araç çubuğundaki **Text** (Metin) grubunda, **Signature Line**'ın (İmza Satırı) yanındaki oku ve ardından **Privacy Manager Signature Provider**'ı (Gizlilik Yöneticisi İmza Sağlayıcısı) tıklatın.

   Signature Setup (İmza Ayarı) iletişim kutusu açılır.

4. **Suggested signer**'ın (Önerilen imzalayan) altındaki metin kutusuna önerilen imzalayanın adını girin.

5. **Instructions to the signer**'ın (İmzalayan için yönergeler) altındaki metin kutusuna bu önerilen imzalayan için bir ileti yazın.

   NOT: Bu ileti, başlık yerine görüntülenecek ve belge imzalandığında silinecek veya kullanıcının başlığıyla değiştirilecektir.

6. Tarihin gösterilmesini sağlamak için **Show sign date in signature line** (İmza satırında imzalama tarihini göster) onay kutusunu seçin.

7. Unvanın gösterilmesini sağlamak için **Show signer's title in signature line** (İmza satırında imzalayanın unvanını göster) onay kutusunu seçin.

   NOT: Önerilen imzalayanlar belgenin sahibi tarafından belgeye atandığından, **Show sign date in signature line** (İmza satırında imzalama tarihini göster) ve/veya **Show signer's title in signature line** (İmza satırında imzalayanın unvanını göster) onay kutuları seçilmediği takdirde, önerilen imzalayanın belge ayarları bu şekilde olsa dahi tarih ve/veya unvan imza satırında görüntülenmez.

8. **OK**'i (Tamam) tıklatın.

Önerilen imzalayanın imza satırını ekleme

Önerilen imzalayanlar belgeyi açtıklarında, imzalarının gerektiğini belirtecek şekilde, adlarını köşeli ayraç içinde görürler.

Belgeyi imzalamak için:

1. Uygun imza satırını çift tıklatın.

2. Seçtiğiniz güvenlik oturum açma yöntemini kullanarak kimlik doğrulaması yapın.

İmza satırı, belgenin sahibinin belirttiği ayarlara göre gösterilecektir.

Microsoft Office belgesini şifreleme

Siz ve Güvenilen Kişileriniz için bir Microsoft Office belgesini şifreleyebilirsiniz. Bir belgeyi şifreleyip kapattığınızda, siz ve listeden seçtiğiniz Güvenilen Kişi (veya Güvenilen Kişiler) belgeyi açmadan önce kimlik doğrulaması yapmalısınız.

Microsoft Office belgesini şifrelemek için:

1. Microsoft Word, Microsoft Excel veya Microsoft PowerPoint'te bir belge oluşturup kaydedin.
2. **Home** (Giriş) menüsünü tıklatın.
3. **Sign and Encrypt**'in (İmzala ve Şifrele) yanındaki aşağı oku ve ardından **Encrypt Document**'ı (Belgeyi Şifrele) tıklatın.

   Select Trusted Contacts (Güvenilen Kişileri Seçin) iletişim kutusu açılır.
4. Belgeyi açabilecek ve içeriğini görüntüleyebilecek Güvenilen Kişi'nin adını tıklatın.

NOT: Birden çok Güvenilen Kişi adı seçmek için, ctrl tuşunu basılı turun ve adları tek tek tıklatın.

5. **OK**'i (Tamam) tıklatın.

Daha sonra belgeyi düzenlemeye karar verirseniz, Bir Microsoft Office belgesinin şifrelemesini kaldırma sayfa 59 bölümündeki adımları izleyin. Şifreleme kaldırıldıktan sonra belgeyi düzenleyebilirsiniz. Belgeyi tekrar şifrelemek için bu bölümdeki adımları izleyin.

Bir Microsoft Office belgesinin şifrelemesini kaldırma

Bir Microsoft Office belgesinin şifrelemesini kaldırdığınızda, siz ve Güvenilen Kişileriniz artık belgeyi açmak ve içeriğini görüntülemek için kimlik doğrulaması yapmak zorunda kalmazsınız.

Bir Microsoft Office belgesinin şifrelemesini kaldırmak için:

1. Şifrelenmiş bir Microsoft Word, Microsoft Excel veya Microsoft PowerPoint belgesini açın.
2. Seçtiğiniz güvenlik oturum açma yöntemini kullanarak kimlik doğrulaması yapın.
3. **Home** (Giriş) menüsünü tıklatın.
4. **Sign and Encrypt**'in (İmzala ve Şifrele) yanındaki aşağı oku ve ardından **Remove Encryption**'ı (Şifrelemeyi Kaldır) tıklatın.

Şifrelenmiş bir Microsoft Office belgesi gönderme

Şifrelenmiş bir Microsoft Office belgesini, e-postanın kendisini imzalamadan veya şifrelemeden bir e-posta iletisine ekleyebilirsiniz. Bunu yapmak için, normalde ekli sıradan e-postalar için yaptığınız işlemleri yaparak, imzalanmış veya şifrelenmiş bir belge içeren bir e-posta oluşturun ve gönderin.

Ancak en iyi güvenlik için, imzalanmış veya şifrelenmiş bir Microsoft Office belgesi eklerken e-postayı şifrelemeniz önerilir.

Ek olarak imzalanmış ve/veya şifrelenmiş bir Microsoft Office belgesi içeren mühürlenmiş bir e-posta göndermek için, aşağıdaki adımları izleyin:

1. Microsoft Outlook'ta, **New**'ı (Yeni) veya **Reply**'ı (Yanıtla) tıklatın.
2. E-posta iletinizi yazın.
3. Microsoft Office belgesini ekleyin.
4. Ayrıntılı yönergeler için bkz. E-posta iletisini mühürleme ve gönderme sayfa 56.

İmzalanmış bir Microsoft Office belgesini görüntüleme

NOT: İmzalanmış bir Microsoft Office belgesini görüntülemek için bir Privacy Manager (Gizlilik Yöneticisi) Sertifikası'na ihtiyacınız yoktur.

İmzalanmış bir Microsoft Office belgesi açıldığında, belge penceresinin alt kısmındaki durum çubuğunda bir Digital Signature (Dijital İmza) simgesi görüntülenir.

1. Belgeyi imzalayan tüm kullanıcıların adını ve imzalama tarihini görüntüleyen Signatures (İmzalar) iletişim kutusunun görüntülenme durumunu değiştirmek için **Digital Signatures** (Dijital İmzalar) simgesini tıklatın.
2. Her imzayla ilgili ek ayrıntıları görüntülemek için, Signatures (İmzalar) iletişim kutusunda bir adı sağ tıklatıp Signature Details'ı (İmza Ayrıntıları) seçin.

Şifrelenmiş bir Microsoft Office belgesini görüntüleme

Başka bir bilgisayardaki şifrelenmiş bir Microsoft Office belgesini görüntülemek için, söz konusu bilgisayarda Privacy Manager (Gizlilik Yöneticisi) yüklü olmalıdır. Buna ek olarak, dosyayı şifrelemek için kullanılan Privacy Manager (Gizlilik Yöneticisi) Sertifikası'nı geri yüklemeniz gerekir.

Şifrelenmiş bir Microsoft Office belgesini görüntülemek isteyen bir Güvenilen Kişi'nin bir Privacy Manager (Gizlilik Yöneticisi) Sertifikası'na sahip olması ve Privacy Manager'ın (Gizlilik Yöneticisi) bilgisayarında yüklü olması gerekir. Ayrıca, Güvenilen Kişi, şifrelenmiş Microsoft Office belgesinin sahibi tarafından seçilmelidir.

Privacy Manager'ı (Gizlilik Yöneticisi) Windows Live Messenger'da kullanma

Privacy Manager (Gizlilik Yöneticisi), Windows Live Messenger'a aşağıdaki güvenli iletişim özelliklerini ekler:

- **Secure chat** (Güvenli sohbet)—İletiler XML protokolü üzerinden SSL/TLS (Secure Sockets Layer/ Transport Layer Security - Güvenli Yuva Katmanı/Aktarım Katmanı Güvenliği) kullanılarak iletilir. Bu, e-ticaret işlemlerinin güvenliğini sağlayan teknolojidir.
- **Recipient identification** (Alıcı tanımlama)—İleti göndermeden önce bir kişinin varlığını ve kimliğini doğrulayabilirsiniz.
- **Signed messages** (İmzalanmış iletiler)—İletilerinizi elektronik olarak imzalayabilirsiniz. Böylece, ileti kurcalanırsa, alıcı iletiyi aldığında geçersiz olarak işaretlenecektir.
- **Hide/show feature** (Gizle/göster özelliği)—Privacy Manager Chat (Gizlilik Yöneticisi Sohbet) penceresindeki iletilerin herhangi birini veya tümünü gizleyebilirsiniz. Ayrıca içeriğin gizli olduğu bir ileti de gönderebilirsiniz. Bir ileti görüntülenmeden önce kimlik doğrulaması gerekir.

- **Secure chat history** (Güvenli sohbet geçmişi)—Sohbet oturumlarınızın günlükleri, kaydedilmeden önce şifrelenir ve görüntülenmek için kimlik doğrulaması gerektirir.
- **Automatic locking/unlocking** (Otomatik kilitleme/kilit açma)—Privacy Manager Chat (Gizlilik Yöneticisi Sohbet) penceresini kilitleyip kilidini açabilir veya belirli bir süre işlem yapılaması durumunda otomatik olarak kilitlenecek şekilde ayarlayabilirsiniz.

Privacy Manager Chat (Gizlilik Yöneticisi Sohbet) oturumu başlatma

NOT: Privacy Manager Chat (Gizlilik Yöneticisi Sohbet) özelliğini kullanabilmek için, her iki tarafta Privacy Manager (Gizlilik Yöneticisi) ve bir Privacy Manager (Gizlilik Yöneticisi) Sertifikası yüklü olmalıdır. Privacy Manager (Gizlilik Yöneticisi) Sertifikası yüklemeye yönelik ayrıntılar için, bkz. Privacy Manager (Gizlilik Yöneticisi) Sertifikası isteme ve yükleme sayfa 48.

1. Windows Live Messenger'da Privacy Manager Chat'i (Gizlilik Yöneticisi Sohbet) başlatmak için aşağıdaki yordamlardan birini gerçekleştirin:

   a. Live Messenger'da çevrimiçi bir kişiyi sağ tıklatın ve ardından **Start an Activity**'yi (Etkinlik Başlat) tıklatın.

   b. **Start Chat**'i (Sohbet Başlat) tıklatın.

   – veya –

   a. Live Messenger'da çevrimiçi bir kişiyi çift tıklatın ve ardından **See a list of activities** (Etkinliklerin listesini gör) menüsünü seçin.

   b. **Action**'ı (Eylem) ve ardından **Start Chat**'i (Sohbet Başlat) tıklatın.

   – veya –

   a. Bildirim alanındaki **ProtectTools** simgesini sağ tıklatın, **Privacy Manager for HP ProtectTools**'u ve ardından **Start Chat**'i (Sohbet Başlat) tıklatın.

   b. Live Messenger'da **Actions: Start an Activity**'yi (Eylemler: Etkinlik Başlat) ve ardından **Privacy Manager Chat**'i (Gizlilik Yöneticisi Sohbet) seçin.

   NOT: Tüm kullanıcıların Live Messenger'da çevrimiçi olması ve birbirlerinin Live Messenger çevrimiçi penceresinde görüntülenmesi gerekir. Çevrimiçi bir kullanıcıyı seçmek için tıklatın.

   Privacy Manager (Gizlilik Yöneticisi), Privacy Manager Chat'i (Gizlilik Yöneticisi Sohbet) başlatmak için kişiye bir davetiye gönderir. Davet edilen kişi daveti kabul ettiğinde, Privacy Manager Chat (Gizlilik Yöneticisi Sohbet) penceresi açılır. Davet edilen kişinin Privacy Manager'ı (Gizlilik Yöneticisi) yoksa, karşıdan yüklemesi istenir.

2. Güvenli bir sohbete başlamak için **Start**'ı (Başlat) tıklatın.

Privacy Manager'ı (Gizlilik Yöneticisi) Windows Live Messenger için yapılandırma

1. Privacy Manager Chat'te (Gizlilik Yöneticisi Sohbet), **Settings** (Ayarlar) düğmesini tıklatın.

   – veya –

   Privacy Manager'da (Gizlilik Yöneticisi), **Settings**'i (Ayarlar) ve ardından **Chat** (Sohbet) sekmesini tıklatın.

   – veya –

   Privacy Manager Live Messenger History Viewer'da (Gizlilik Yöneticisi Live Messenger Geçmiş Görüntüleyici), **Settings** (Ayarlar) düğmesini tıklatın.

2. Oturumunuzu kapatmadan önce Privacy Manager Chat'in (Privacy Manager Sohbet) bekleyeceği süreyi belirlemek için, **Lock session after _ minutes of activity** (_ dakikalık etkinliğin ardından oturumu kilitle) listesinden bir sayı seçin.

3. Sohbet oturumlarınıza yönelik bir geçmiş klasörü belirtmek üzere bir klasör aramak için **Browse**'ı (Gözat) ve ardından **OK**'i (Tamam) tıklatın.

4. Oturumlarınızı kapattığınızda otomatik olarak şifreleyip kaydetmek için, **Automatically save secure chat history** (Güvenli sohbet geçmişini otomatik olarak kaydet) onay kutusunu seçin.

5. **OK**'i (Tamam) tıklatın.

Privacy Manager Chat (Gizlilik Yöneticisi Sohbet) penceresinde sohbet etme

Privacy Manager Chat'i (Gizlilik Yöneticisi Sohbet) başlattıktan sonra, Windows Live Messenger'da bir Privacy Manager Chat (Gizlilik Yöneticisi Sohbet) penceresi açılır. Privacy Manager Chat'i (Gizlilik Yöneticisi Sohbet) kullanmak, temel Windows Live Messenger'ı kullanmaya benzer, ancak Privacy Manager Chat (Gizlilik Yöneticisi Sohbet) penceresinde aşağıdaki ek özellikler kullanılabilir:

- **Save** (Kaydet)—Sohbet oturumunuzu, yapılandırma ayarlarınızda belirtilen klasöre kaydetmek için bu düğmeyi tıklatın. Privacy Manager Chat'i (Gizlilik Yöneticisi Sohbet), her oturumu kapatıldığında otomatik olarak kaydedecek şekilde de yapılandırabilirsiniz.
- **Hide all** (Tümünü gizle) ve **Show all** (Tümünü göster)—Secure Communications (Güvenli İletişim) penceresinde gösterilen iletileri genişletmek veya daraltmak için uygun düğmeyi tıklatın. İleti başlığını tıklatmak suretiyle iletileri tek tek gizlemeniz veya göstermeniz de mümkündür.
- **Are you there?** (Orada mısın?)—Kişinizden kimlik doğrulaması istemek için bu düğmeyi tıklatın.
- **Lock** (Kilitle)—Privacy Manager Chat (Gizlilik Yöneticisi Sohbet) penceresini kapatıp Chat Entry (Sohbet Girişi) penceresine dönmek için bu düğmeyi tıklatın. Secure Communications (Güvenli İletişim) penceresini tekrar görüntülemek için, **Resume the session**'ı (Oturumu sürdür) tıklatın, ardından seçilen güvenli oturum açma yönteminizi kullanarak kimlik doğrulaması yapın.
- **Send** (Gönder)—Kişinize şifrelenmiş bir ileti göndermek için bu düğmeyi tıklatın.
- **Send signed** (İmzalanmış olarak gönder)—İletilerinizi elektronik olarak imzalamak ve şifrelemek için bu onay kutusunu seçin. Böylece, ileti kurcalanırsa, alıcı iletiyi aldığında geçersiz olarak işaretlenecektir. Her imzalanmış ileti gönderişinizde, kimlik doğrulaması yapmanız gerekir.
- **Send hidden** (Gizli gönder)—Yalnızca ileti başlığını göstermek üzere bir iletiyi şifrelemek ve göndermek için bu onay kutusunu seçin. Kişinizin, iletinin içeriğini okumak için kimlik doğrulaması yapması gerekir.

Sohbet geçmişini görüntüleme

Privacy Manager Chat (Gizlilik Yöneticisi Sohbet): Live Messenger History Viewer (Live Messenger Geçmiş Görüntüleyici), şifrelenmiş Privacy Manager Chat (Gizlilik Yöneticisi Sohbet) oturum dosyalarını görüntüler. Oturumlar, Privacy Manager Chat (Gizlilik Yöneticisi Sohbet) penceresinde **Save** (Kaydet) tıklatılarak veya Privacy Manager'ın (Gizlilik Yöneticisi) Chat (Sohbet) sekmesinde otomatik kaydetme yapılandırılarak kaydedilebilir. Görüntüleyicide, her oturum (şifrelenmiş) Kişi Ekranı Adı'nı ve oturumun başladığı ve bittiği tarih ve saati gösterir. Varsayılan olarak oturumlar, kurduğunuz tüm e-posta hesapları için gösterilir. Görüntülemek üzere yalnızca belirli hesapları seçmek için **Display history for** (Geçmişi görüntüle:) menüsünü kullanabilirsiniz.

Görüntüleyici, aşağıdaki görevleri yapmanıza olanak sağlar:

- Tüm oturumları gösterme sayfa 63
- Belirli bir hesabın oturumlarını gösterme sayfa 63
- Oturum kimliğini görüntüleme sayfa 64
- Oturumu görüntüleme sayfa 64
- Belirli bir metni oturumlarda arama sayfa 64
- Oturumu silme sayfa 64
- Sütun ekleme ve kaldırma sayfa 65
- Görüntülenen oturumları filtreleme sayfa 65

Live Messenger History Viewer'ı (Live Messenger Geçmiş Görüntüleyici) başlatmak için:

▲ Görev çubuğunun en sağındaki bildirim alanında, **HP ProtectTools** simgesini sağ tıklatın, **Privacy Manager: for HP ProtectTools**'u (HP ProtectTools için Gizlilik Yöneticisi) ve ardından **Live Messenger History Viewer**'ı (Live Messenger Geçmiş Görüntüleyici) tıklatın.

– veya –

▲ Chat (Sohbet) oturumunda, **History Viewer**'ı (Geçmiş Görüntüleyici) veya **History**'yi (Geçmiş) tıklatın.

Tüm oturumları gösterme

Tüm oturumları göstermek, geçerli olarak seçili olan oturumun (oturumların) şifresi çözülmüş Kişi Ekran Adı'nı ve aynı hesaptaki tüm oturumları görüntüler.

Tüm kaydedilmiş sohbet geçmişi oturumlarınızı göstermek için:

1. Live Messenger History Viewer'da (Live Messenger Geçmiş Görüntüleyici) herhangi bir oturumu sağ tıklatın ve **Reveal All Sessions**'ı (Tüm Oturumları Göster) tıklatın.
2. Seçtiğiniz güvenlik oturum açma yöntemini kullanarak kimlik doğrulaması yapın.

   Kişi Ekran Adları'nın şifresi çözülür.
3. İçeriğini görmek için herhangi bir oturumu çift tıklatın.

Belirli bir hesabın oturumlarını gösterme

Bir oturumu göstermek, geçerli olarak seçili olan oturumun şifresi çözülmüş Kişi Ekran Adı'nı görüntüler.

Belirli bir sohbet geçmişi oturumunu göstermek için:

1. Live Messenger History Viewer'da (Live Messenger Geçmiş Görüntüleyici) herhangi bir oturumu sağ tıklatın ve **Reveal Session**'ı (Oturumu Göster) seçin.
2. Seçtiğiniz güvenlik oturum açma yöntemini kullanarak kimlik doğrulaması yapın.

   Kişi Ekran Adı'nın şifresi çözülür.
3. İçeriğini görmek için gösterilen oturumu çift tıklatın.

NOT: Aynı sertifikayla şifrelenen ek oturumlar, bu oturumlardan herhangi birini başka kimlik doğrulaması gerekmeden çift tıklatarak görüntüleyebileceğinizi belirtecek şekilde bir açık kilit simgesi gösterecektir. Farklı bir sertifikayla şifrelenen oturumlar, bu oturumların Kişi Ekran Adları'nı veya içeriği görüntüleyebilmek için ek kimlik doğrulaması gerektirdiğini belirtecek şekilde bir kapalı kilit simgesi gösterir.

Oturum kimliğini görüntüleme

Oturum kimliğini görüntülemek için:

- Live Messenger History Viewer'da (Live Messenger Geçmiş Görüntüleyici) gösterilen herhangi bir oturumu sağ tıklatın ve **View session ID**'yi (Oturum kimliğini görüntüle) seçin.

Oturumu görüntüleme

Oturumu görüntülemek, görüntüleme amacıyla dosyayı açar. Oturum önceden gösterilmediyse (şifresi çözülmüş Kişi Ekran Adı'nı görüntüleyecek şekilde), aynı anda bu da gösterilir.

Bir Live Messenger geçmişi oturumunu görüntülemek için:

1. Live Messenger History Viewer'da (Live Messenger Geçmiş Görüntüleyici) herhangi bir oturumu sağ tıklatın ve **View**'ı (Görüntüle) seçin.
2. İstenirse, seçtiğiniz güvenlik oturum açma yöntemini kullanarak kimlik doğrulaması yapın.

   Oturum içeriğinin şifresi çözülür.

Belirli bir metni oturumlarda arama

Yalnızca görüntüleyici penceresinde görüntülenen gösterilmiş (şifresi çözülmüş) oturumlarda metin arayabilirsiniz. Bunlar, Kişi Ekran Adı'nın düz metin biçiminde gösterildiği oturumlardır.

Sohbet geçmişi oturumlarında metin aramak için:

1. Live Messenger History Viewer'da (Live Messenger Geçmiş Görüntüleyici), **Search** (Ara) düğmesini tıklatın.
2. Arama metnini girin, istenen parametreleri yapılandırın ve ardından **OK**'i (Tamam) tıklatın.

   Metni içeren oturumlar, görüntüleyici penceresinde vurgulanır.

Oturumu silme

1. Bir sohbet geçmişi oturumu seçin.
2. **Delete**'i (Sil) tıklatın.

Sütun ekleme ve kaldırma

Varsayılan olarak, en çok kullanılan 3 sütun Live Messenger History Viewer'da (Live Messenger Geçmiş Görüntüleyici) görüntülenir. Ekrana ek sütunlar ekleyebilir veya sütunları ekrandan kaldırabilirsiniz.

Ekrana sütun eklemek için:

1. Herhangi bir sütun başlığını sağ tıklatın ve ardından **Add/Remove Columns**'u (Sütun Ekle/Kaldır) tıklatın.
2. Sol panelde bir sütun başlığı seçin ve sağ panele taşımak için **Add**'i (Ekle) tıklatın.

Sütunları ekrandan kaldırmak için:

1. Herhangi bir sütun başlığını sağ tıklatın ve ardından **Add/Remove Columns**'u (Sütun Ekle/Kaldır) tıklatın.
2. Sağ panelde bir sütun başlığı seçin ve sol panele taşımak için **Remove**'u (Kaldır) tıklatın.

Görüntülenen oturumları filtreleme

Live Messenger History Viewer'da (Live Messenger Geçmiş Görüntüleyici), tüm hesaplarınıza ait oturumların listesi görüntülenir. Ayrıca, görüntülenen oturumları aşağıdakilere yönelik olarak filtreleyebilirsiniz:

- Belirli hesaplar. Ayrıntılar için, bkz. Belirli bir hesabın oturumlarını görüntüleme sayfa 65.
- Tarih aralıkları. Ayrıntılar için, bkz. Bir tarih aralığındaki oturumları görüntüleme sayfa 65.
- Farklı klasörler. Ayrıntılar için, bkz. Varsayılan klasör dışında bir klasöre kaydedilen oturumları görüntüleme sayfa 65.

Belirli bir hesabın oturumlarını görüntüleme

▲ Live Messenger History Viewer'da (Live Messenger Geçmiş Görüntüleyici), **Display history for** (Geçmişi görüntüle:) menüsünden bir hesap seçin.

Bir tarih aralığındaki oturumları görüntüleme

1. Live Messenger History Viewer'da (Live Messenger Geçmiş Görüntüleyici), **Advanced Filter** (Gelişmiş Filtre) simgesini tıklatın.

   Advanced Filter (Gelişmiş Filtre) iletişim kutusu açılır.

2. **Display only sessions within specified date range** (Yalnızca belirtilen tarih aralığındaki oturumları görüntüle) onay kutusunu seçin.
3. **From date** (Başlangıç tarihi) ve **To date** (Bitiş tarihi) metin kutularına, günü, ayı ve/veya yılı girin ya da tarihleri seçmek için takvimin yanındaki oku tıklatın.
4. **OK**'i (Tamam) tıklatın.

Varsayılan klasör dışında bir klasöre kaydedilen oturumları görüntüleme

1. Live Messenger History Viewer'da (Live Messenger Geçmiş Görüntüleyici), **Advanced Filter** (Gelişmiş Filtre) simgesini tıklatın.
2. **Use an alternate history files folder** (Başka bir geçmiş dosyaları klasörü kullan) onay kutusunu seçin.

3. Klasör konumunu girin veya klasörü aramak için **Browse**'ı (Gözat) tıklatın.
4. **OK**'i (Tamam) tıklatın.

Gelişmiş görevler

Privacy Manager (Gizlilik Yöneticisi) Sertifikaları'nı ve Güvenilen Kişiler'i farklı bilgisayara geçirme

Privacy Manager (Gizlilik Yöneticisi) Sertifikalarınız'ı ve Güvenilen Kişileriniz'i güvenli bir şekilde başka bir bilgisayara taşıyabilir veya güvenli olarak saklamak için verilerinizi yedekleyebilirsiniz. Bunu yapmak için, verileri parola korumalı bir dosya olarak bir ağ konumuna veya herhangi bir çıkarılabilir depolama aygıtına yedekleyin ve daha sonra dosyayı yeni bilgisayara geri yükleyin.

Privacy Manager (Gizlilik Yöneticisi) Sertifikaları'nı ve Güvenilen Kişiler'i yedekleme

Privacy Manager (Gizlilik Yöneticisi) Sertifikalarınız'ı ve Güvenilen Kişileriniz'i parola korumalı bir dosyaya yedeklemek için, şu adımları izleyin:

1. Privacy Manager'ı (Gizlilik Yöneticisi) açın ve **Migration**'ı (Geçiş) tıklatın.
2. **Backup**'ı (Yedekle) tıklatın.
3. Select Data (Verileri Seçin) sayfasında, geçiş dosyasına dahil edilecek veri kategorilerini seçip **Next**'i (İleri) tıklatın.
4. Migration File (Geçiş Dosyası) sayfasında, bir dosya adı girin veya bir konum aramak için **Browse**'ı (Gözat) ve daha sonra **Next**'i (İleri) tıklatın.
5. Bir parola oluşturun ve onaylayın, ardından **Next**'i (İleri) tıklatın.

NOT: Geçiş dosyasını geri yükleyeceğiniz zaman ihtiyacınız olacağından, bu parolayı güvenli bir yerde depolayın.

6. Seçtiğiniz güvenlik oturum açma yöntemini kullanarak kimlik doğrulaması yapın.
7. Migration File Saved (Geçiş Dosyası Kaydedildi) sayfasında **Finish**'i (Son) tıklatın.

Privacy Manager (Gizlilik Yöneticisi) Sertifikaları'nı ve Güvenilen Kişiler'i geri yükleme

Privacy Manager (Gizlilik Yöneticisi) Sertifikalarınız'ı ve Güvenilen Kişileriniz'i geçiş işleminin parçası olarak farklı bir bilgisayara veya aynı bilgisayara geri yüklemek için şu adımları izleyin:

1. Privacy Manager'ı (Gizlilik Yöneticisi) açın ve **Migration**'ı (Geçiş) tıklatın.
2. **Restore**'u (Geri yükle) tıklatın.
3. Migration File (Geçiş Dosyası) sayfasında, dosyayı aramak için **Browse**'ı (Gözat) ve daha sonra **Next**'i (İleri) tıklatın.
4. Yedekleme dosyasını oluşturduğunuzda kullandığınız parolayı girin ve ardından **Next**'i (İleri) tıklatın.
5. Migration File (Geçiş Dosyası) sayfasında **Finish**'i (Son) tıklatın.

Privacy Manager'ın (Gizlilik Yöneticisi) merkezi yönetimi

Privacy Manager (Gizlilik Yöneticisi) yüklemeniz, yöneticiniz tarafından özelleştirilen merkezileştirilmiş bir yüklemenin bir parçası olabilir. Aşağıdaki özelliklerden biri veya daha fazlası etkinleştirilmiş veya devre dışı bırakılmış olabilir:

- **Certificate use policy** (Sertifika kullanım ilkesi)—Comodo tarafından verilen Privacy Manager (Gizlilik Yöneticisi) sertifikalarını kullanmakla kısıtlanmış olabilirsiniz veya diğer sertifika yetkililerinin verdiği dijital sertifikaları kullanmanıza izin veriliyor olabilir.
- **Encryption policy** (Şifreleme ilkesi)—Şifreleme özellikleri Microsoft Office veya Outlook'ta ve Windows Live Messenger'da tek tek etkinleştirilebilir veya devre dışı bırakılabilir.

10 HP ProtectTools için File Sanitizer (Dosya Temizleyici)

File Sanitizer (Dosya Temizleyici) bilgisayarınızdaki varlıkları (kişisel bilgiler veya dosyalar, geçmiş verileri veya Web ile ilgili veriler ya da diğer veri bileşenleri) güvenli bir şekilde parçalamanıza ve sabit sürücünüzü periyodik olarak temizlemenize olanak sağlayan bir araçtır.

NOT: File Sanitizer'ın (Dosya Temizleyici) bu sürümü yalnızca sistem sabit sürücüsünü desteklemektedir.

Parçalama

File Sanitizer'ı (Dosya Temizleyici) kullanarak bir varlığı parçaladığınızda, verileri anlaşılmaz hale getiren bir algoritma kullanılarak orijinal varlığın ele geçirilmesi neredeyse imkansız hale getirildiğinden, parçalama standart Windows® silme işleminden (File Sanitizer'da (Dosya Temizleyici) basit silme işlemi olarak adlandırılır) farklıdır. Windows'un basit silme işlemi, dosyayı (veya varlığı) sabit sürücüde tek parça halinde veya dosyayı (veya varlığı) kurtarmak için gelişmiş yöntemlerin kullanılabileceği bir durumda bırakabilir.

Bir parçalama profili (High Security (Yüksek Güvenlik), Medium Security (Orta Güvenlik) veya Low Security (Düşük Güvenlik)) seçtiğinizde, parçalama işlemi için varlıkların önceden tanımlı bir listesi ve bir silme yöntemi otomatik olarak seçilir. Ayrıca bir parçalama profilini, parçalama döngülerinin sayısını, hangi varlıkların parçalama işlemine dahil edileceğini, hangi varlıkların parçalama işleminden önce onaylanacağını ve hangi varlıkların parçalama işleminde hariç tutulacağını belirtmenize izin verecek şekilde özelleştirebilirsiniz. Daha fazla bilgi için, bkz. Bir parçalama profili seçme veya oluşturma sayfa 73.

Otomatik parçalama programı ayarlayabilir ve ayrıca varlıkları istediğiniz zaman el ile parçalayabilirsiniz. Daha fazla bilgi için, bkz. Parçalama programı ayarlama sayfa 72, Tek bir varlığı el ile parçalama sayfa 77 veya Tüm seçilen öğeleri el ile parçalama sayfa 77.

NOT: Bir .dll dosyası, yalnızca geri dönüşüm kutusuna gönderildiyse parçalanır ve sistemden kaldırılır.

Boş alan temizleme

Windows'da bir varlığı silmek, varlığın içeriğini sabit sürücünüzden tamamen kaldırmaz. Windows, yalnızca varlığa yönelik başvuruyu siler. Varlığın içeriği, başka bir varlık sabit sürücüdeki aynı alanın üzerine yeni bilgiler yazana kadar sabit sürücüde kalır.

Boş alan temizleme, kullanıcıların silinen varlığın orijinal içeriğini görüntülemesini engelleyecek şekilde, silinen varlıkların üzerine güvenli bir şekilde rastgele veriler yazmanıza olanak tanır.

NOT: Boş alan temizleme, Windows Geri Dönüşüm Kutusu'nu kullanarak veya el ile sildiğiniz varlıklar içindir. Boş alan temizleme, parçalanan varlıklar için ek güvenlik sağlamaz.

Otomatik boş alan temizleme programı ayarlayabilir veya görev çubuğunun en sağında bulunan bildirim alanındaki **HP ProtectTools** simgesini kullanarak boş alan temizlemeyi el ile etkinleştirebilirsiniz. Daha fazla bilgi için, bkz. Boş alan temizleme programı ayarlama sayfa 73 veya Boş alan temizlemeyi el ile etkinleştirme sayfa 78.

Kurulum yordamları

File Sanitizer'ı (Dosya Temizleyici) açma

File Sanitizer'ı (Dosya Temizleyici) açmak için:

1. **Başlat**'ı tıklatın, **Tüm Programlar**'ı tıklatın, **HP**'yi ve ardından **HP ProtectTools Security Manager**'ı (HP ProtectTools Güvenlik Yöneticisi) tıklatın.
2. **File Sanitizer**'ı (Dosya Temizleyici) tıklatın.

– veya –

▲ Masaüstünüzdeki **File Sanitizer** (Dosya Temizleyici) simgesini çift tıklatın.

– veya –

▲ Görev çubuğunun en sağında bulunan bildirim alanındaki **HP ProtectTools** simgesini sağ tıklatın ve **File Sanitizer**'ı (Dosya Temizleyici) ve ardından **Open File Sanitizer**'ı (Dosya Temizleyici'yi Aç) tıklatın.

Parçalama programı ayarlama

NOT: Önceden tanımlı bir parçalama profili seçme veya parçalama profili oluşturma ile ilgili bilgiler için Bir parçalama profili seçme veya oluşturma sayfa 73 bölümüne bakın.

NOT: Varlıkları el ile parçalama ile ilgili bilgiler için Tek bir varlığı el ile parçalama sayfa 77 bölümüne bakın.

1. File Sanitizer'ı (Dosya Temizleyici) açın ve **Shred**'i (Parçala) tıklatın.
2. Bir parçalama seçeneği belirleyin:
   - **Windows shutdown** (Windows kapatma)—Windows kapatıldığında tüm seçilen varlıkları parçalamak için bu seçeneği belirleyin.

     NOT: Bu seçenek belirlendiğinde, kapatma sırasında, seçilen varlıkları parçalamaya işlemiyle devam etme veya yordamı atlama arasında seçim yapmanızı isteyen bir iletişim kutusu görüntülenir. Yordamı atlamak isterseniz **Yes**'i (Evet) tıklatın veya parçalama işlemiyle devam etmek isterseniz **No**'yu (Hayır) tıklatın.
   - **Web browser open** (Web tarayıcısı açma)—Bir Web tarayıcısı açtığınızda, tarayıcı URL geçmişi gibi Web ile ilgili tüm seçilen varlıkları parçalamak için bu seçeneği belirleyin.
   - **Web browser quit** (Web tarayıcısından çıkma)—Bir Web tarayıcısını kapattığınızda, tarayıcı URL geçmişi gibi Web ile ilgili tüm seçilen varlıkları parçalamak için bu seçeneği belirleyin.
   - **Key sequence** (Tuş dizisi)—Bir tuş dizisi kullanarak parçalamayı başlatmak için bu seçeneği belirleyin.
   - **Scheduler** (Programlayıcı)—**Activate Scheduler** (Programlayıcıyı Etkinleştir) onay kutusunu seçin, bir Windows parolası ve ardından seçilen varlıkları parçalamak için bir gün ve saat girin.

   NOT: Bir .dll dosyası, yalnızca geri dönüşüm kutusuna gönderildiyse parçalanır ve sistemden kaldırılır.
3. **Apply**'ı (Uygula) ve ardından **OK**'i (Tamam) tıklatın.

Boş alan temizleme programı ayarlama

NOT: Boş alan temizleme, Windows Geri Dönüşüm Kutusu'nu kullanarak sildiğiniz veya el ile silinen varlıklar içindir. Boş alan temizleme, parçalanan varlıklar için ek güvenlik sağlamaz.

Boş alan temizleme programı ayarlamak için:

1. File Sanitizer'ı (Dosya Temizleyici) açın ve **Free Space Bleaching**'i (Boş Alan Temizleme) tıklatın.
2. **Activate Scheduler** (Programlayıcıyı Etkinleştir) onay kutusunu seçin, Windows parolanızı ve ardından sabit sürücünüzü temizlemek için bir gün ve saat girin.
3. **Apply**'ı (Uygula) ve ardından **OK**'i (Tamam) tıklatın.

NOT: Boş alan temizleme işlemi uzun sürebilir. Boş alan temizleme işlemi arka planda yapılsa da, bilgisayarınız artan işlemci kullanımı nedeniyle daha yavaş çalışabilir.

Bir parçalama profili seçme veya oluşturma

Önceden tanımlı bir profil seçerek veya kendi profilinizi oluşturarak bir silme yöntemi belirtebilir ve parçalanacak varlıkları seçebilirsiniz.

Önceden tanımlı bir parçalama profili seçme

Önceden tanımlı bir parçalama profili (High Security (Yüksek Güvenlik), Medium Security (Orta Güvenlik) veya Low Security (Düşük Güvenlik)) seçtiğinizde, önceden tanımlı bir silme yöntemi ve varlık listesi otomatik olarak seçilir. Parçalama için seçilen önceden tanımlı varlıkların listesini görüntülemek için **View Details** (Ayrıntıları Görüntüle) düğmesini tıklatabilirsiniz.

Önceden tanımlı bir parçalama profili seçmek için:

1. File Sanitizer'ı (Dosya Temizleyici) açın ve **Settings**'i (Ayarlar) tıklatın.
2. Önceden tanımlı bir parçalama profilini tıklatın.
3. Parçalama için seçilen varlıkların listesini görüntülemek için **View Details**'ı (Ayrıntıları Görüntüle) tıklatın.
4. **Shred the following** (Aşağıdakileri parçala) altında, parçalamadan önce onaylamak istediğiniz tüm varlıkların yanındaki onay kutusunu seçin.
5. **Apply**'ı (Uygula) ve ardından **OK**'i (Tamam) tıklatın.

Parçalama profilini özelleştirme

Bir parçalama profili oluşturduğunuzda, parçalama döngülerinin sayısını, hangi varlıkların parçalama işlemine dahil edileceğini, hangi varlıkların parçalama işleminden önce onaylanacağını ve hangi varlıkların parçalama işleminin dışında tutulacağını belirtirsiniz:

1. File Sanitizer'ı (Dosya Temizleyici) açın ve **Settings**'i (Ayarlar), **Advanced Security Settings**'i (Gelişmiş Güvenlik Ayarları) ve ardından **View Details**'ı (Ayrıntıları Görüntüle) tıklatın.
2. Parçalama döngülerinin sayısını belirtin.

NOT: Her bir varlık için gerçekleştirilmek üzere seçilen parçalama döngüsü sayısı. Örneğin 3 parçalama döngüsü seçerseniz, verileri belirsizleştiren bir algoritma 3 kez ayrı ayrı yürütülür. Daha yüksek güvenlikli parçalama döngüleri seçerseniz, parçalama oldukça uzun sürebilir; ancak belirttiğiniz parçalama döngüsü sayısı arttıkça, verilerin ele geçirilme olasılığı azalır.

3. Parçalamak istediğiniz varlıkları seçin:

   a. **Available shred options** (Kullanılabilir parçalama seçenekleri) altında bir varlığı ve ardından **Add**'i (Ekle) tıklatın.

   b. Özel bir varlık eklemek için, **Add Custom Option**'ı (Özel Seçenek Ekle) tıklatın ve ardından dosya adını veya klasörü gösteren yola göz atın veya yolu girin. **Open**'ı (Aç), ardından da **OK**'i (Tamam) tıklatın. **Available shred options** (Kullanılabilir parçalama seçenekleri) altında, özel varlığı ve ardından **Add**'i (Ekle) tıklatın.

NOT: Kullanılabilir parçalama seçeneklerinden bir varlığı kaldırmak için, varlığı tıklatın, sonra da **Delete**'i (Sil) tıklatın.

4. **Shred the following** (Aşağıdakileri parçala) altında, parçalamadan önce onaylamak istediğiniz tüm varlıkların yanındaki onay kutusunu seçin

NOT: Parçalama listesinden bir varlığı kaldırmak için, varlığı tıklatın, sonra da **Remove**'u (Kaldır) tıklatın.

5. Dosya veya klasörleri otomatik parçalamaya karşı korumak için, **Do not shred the following** (Aşağıdakileri parçalama) altında **Add**'i (Ekle) tıklatın, sonra da dosya adına veya klasöre giden yola göz atın veya yolu yazın. **Open**'ı (Aç), ardından da **OK**'i (Tamam) tıklatın.

NOT: Hariç tutulanlar listesinden bir varlığı silmek için, varlığı tıklatın, sonra da **Delete**'i (Sil) tıklatın.

6. Parçalama profilini yapılandırmayı tamamladığınızda, **Apply**'ı (Uygula) ve ardından **OK**'i (Tamam) tıklatın.

Bir basit silme profilini özelleştirme

Basit silme profili, parçalama yapmadan standart bir varlık silme işlemi gerçekleştirir. Bir basit silme profilini özelleştirdiğinizde, basit silme işlemine hangi varlıkların dahil edileceğini, basit silme işlemi yürütülmeden önce hangi varlıkların onaylanacağını ve basit silme işleminde hangi varlıkların hariç tutulacağını belirtebilirsiniz.

NOT: Basit sil seçeneğini kullanırsanız, el ile veya Windows Geri Dönüşüm Kutusu kullanılarak silinmiş varlıklar üzerinde zaman zaman boş alan temizleme işlemi gerçekleştirilebilir.

Bir basit silme profilini özelleştirmek için:

1. File Sanitizer'ı (Dosya Temizleyici) açın, **Settings**'i (Ayarlar), **Simple Delete Setting**'i (Basit Silme Ayarı) ve ardından **View Details**'ı (Ayrıntıları Görüntüle) tıklatın.

2. Silmek istediğiniz varlıkları seçin:

   a. **Available delete options** (Kullanılabilir silme seçenekleri) altında bir varlığı ve ardından **Add**'i (Ekle) tıklatın.

   b. Özel bir varlık eklemek için, **Add Custom Option**'ı (Özel Seçenek Ekle) tıklatın, bir dosya adı veya klasör adı girin ve ardından **OK**'i (Tamam) tıklatın. Özel varlığı ve daha sonra **Add**'i (Ekle) tıklatın.

NOT: Kullanılabilir silme seçeneklerinden bir varlığı silmek için, varlığı tıklatın, sonra da **Delete**'i (Sil) tıklatın.

3. **Delete the following** (Aşağıdakileri sil) altında, silmeden önce onaylamak istediğiniz tüm varlıkların yanındaki onay kutusunu seçin.

NOT: Silme listesinden bir varlığı kaldırmak için, varlığı tıklatın, sonra da **Remove**'u (Kaldır) tıklatın.

4. **Do not delete the following** (Aşağıdakileri silme) altında, parçalama işleminde hariç tutmak istediğiniz belirli varlıkları seçmek için **Add**'i (Ekle) tıklatın.

NOT: Hariç tutulanlar listesinden bir varlığı silmek için, varlığı tıklatın, sonra da **Delete**'i (Sil) tıklatın.

5. Basit silme profilini yapılandırmayı tamamladığınızda, **Apply**'ı (Uygula) ve ardından **OK**'i (Tamam) tıklatın.

Genel görevler

File Sanitizer'ı (Dosya Temizleyici) aşağıdaki görevleri gerçekleştirmek için kullanabilirsiniz:

- Use a key sequence to initiate shredding (Parçalamayı başlatmak için bir tuş dizisi kullan)—Bu özellik, parçalamayı başlatmak için bir tuş dizisi (ctrl+alt+s gibi) oluşturmanıza olanak tanır. Ayrıntılar için, bkz. Parçalamayı başlatmak için bir tuş dizisi kullanma sayfa 76.
- Use the File Sanitizer icon to initiate shredding (Parçalamayı başlatmak için Dosya Temizleyici simgesini kullan)—Bu özellik, Windows'daki sürükle bırak özelliğine benzer. Ayrıntılar için, bkz. File Sanitizer (Dosya Temizleyici) simgesini kullanma sayfa 77.
- Manually shred a specific asset or all selected assets (Belirli bir varlığı veya tüm seçilen varlıkları el ile parçala)—Bu özellikler, düzenli parçalama programının uygulanmasını beklemeden öğeleri el ile parçalamanıza olanak tanır. Ayrıntılar için, bkz. Tek bir varlığı el ile parçalama sayfa 77 veya Tüm seçilen öğeleri el ile parçalama sayfa 77.
- Manually activate free space bleaching (Boş alan temizlemeyi el ile etkinleştir)—Bu özellik, boş alan temizlemeyi el ile etkinleştirmenize olanak tanır. Ayrıntılar için, bkz. Boş alan temizlemeyi el ile etkinleştirme sayfa 78.
- Abort a shred or free space bleaching operation (Parçalama veya boş alan temizleme işlemini iptal et)—Bu özellik, parçalama veya boş alan temizleme işlemini durdurmanıza olanak tanır. Ayrıntılar için, bkz. Bir parçalama veya boş alan temizleme işlemini iptal etme sayfa 78.
- View the log files (Günlük dosyalarını görüntüle)—Bu özellik, son parçalama veya boş alan temizleme işlemindeki hataları veya bozuklukları içeren parçalama ve boş alan temizleme günlük dosyalarını görüntülemenize olanak tanır. Ayrıntılar için, bkz. Günlük dosyalarını görüntüleme sayfa 78.

NOT: Parçalama veya boş alan temizleme işlemi oldukça uzun sürebilir. Parçalama ve boş alan temizleme işlemi arka planda yapılsa da, bilgisayarınız artan işlemci kullanımı nedeniyle daha yavaş çalışabilir.

Parçalamayı başlatmak için bir tuş dizisi kullanma

Bir tuş dizisi belirtmek için aşağıdaki adımları takip edin:

1. File Sanitizer'ı (Dosya Temizleyici) açın ve **Shred**'i (Parçala) tıklatın.
2. **Key sequence** (Tuş dizisi) onay kutusunu seçin.
3. Metin kutusuna bir karakter girin.
4. **CTRL** onay kutusunu veya **ALT** onay kutusunu seçin ve ardından **SHIFT** kutusunu seçin.

   Örneğin, otomatik parçalamayı s tuşu ve ctrl+shift ile başlatmak için, metin kutusuna `s` karakterini girin ve ardından **CTRL** ile **SHIFT** onay kutularını seçin.

NOT: Yapılandırdığınız diğer tuş dizilerinden farklı bir tuş dizisi seçtiğinizden emin olun.

Parçalamayı bir tuş dizisi kullanarak başlatmak için:

1. Seçtiğiniz karaktere basarken, shift tuşunu ve ctrl tuşunu veya alt tuşunu (ya da hangi bileşimi belirttiyseniz) basılı tutun.
2. Onay iletişim kutusu açılırsa, **Yes**'i (Evet) tıklatın.

File Sanitizer (Dosya Temizleyici) simgesini kullanma

△ **DİKKAT:** Parçalanan varlıklar kurtarılamaz. El ile parçalama için hangi varlıkları seçeceğinize dikkatli bir şekilde karar verin.

1. Parçalamak istediğiniz belgeye veya klasöre gidin.
2. Varlığı, masaüstündeki **File Sanitizer** simgesine sürükleyin.
3. Onay iletişim kutusu açıldığında **Yes**'i (Evet) tıklatın.

Tek bir varlığı el ile parçalama

△ **DİKKAT:** Parçalanan varlıklar kurtarılamaz. El ile parçalama için hangi varlıkları seçeceğinize dikkatli bir şekilde karar verin.

1. Görev çubuğunun en sağında bulunan bildirim alanındaki **HP ProtectTools** simgesini sağ tıklatın ve **File Sanitizer**'ı (Dosya Temizleyici) ve ardından **Shred One**'ı (Birini Parçala) tıklatın.
2. Browse (Gözat) iletişim kutusu açıldığında, parçalamak istediğiniz varlığa gidin ve ardından **OK**'i (Tamam) tıklatın.

   NOT: Seçtiğiniz varlık tek bir dosya veya klasör olabilir.

3. Onay iletişim kutusu açıldığında **Yes**'i (Evet) tıklatın.

– veya –

1. Masaüstündeki **File Sanitizer** (Dosya Temizleyici) simgesini sağ tıklatın ve ardından **Shred One**'ı (Birini Parçala) tıklatın.
2. Browse (Gözat) iletişim kutusu açıldığında, parçalamak istediğiniz varlığa gidin ve ardından **OK**'i (Tamam) tıklatın.
3. Onay iletişim kutusu açıldığında **Yes**'i (Evet) tıklatın.

– veya –

1. File Sanitizer'ı (Dosya Temizleyici) açın ve **Shred**'i (Parçala) tıklatın.
2. **Browse** (Gözat) düğmesini tıklatın.
3. Browse (Gözat) iletişim kutusu açıldığında, parçalamak istediğiniz varlığa gidin ve ardından **OK**'i (Tamam) tıklatın.
4. Onay iletişim kutusu açıldığında **Yes**'i (Evet) tıklatın.

Tüm seçilen öğeleri el ile parçalama

1. Görev çubuğunun en sağında bulunan bildirim alanındaki **HP ProtectTools** simgesini sağ tıklatın ve **File Sanitizer**'ı (Dosya Temizleyici) ve ardından **Shred Now**'ı (Şimdi Parçala) tıklatın.
2. Onay iletişim kutusu açıldığında **Yes**'i (Evet) tıklatın.

– veya –

1. Masaüstündeki **File Sanitizer** (Dosya Temizleyici) simgesini sağ tıklatın ve ardından **Shred Now**'ı (Şimdi Parçala) tıklatın.
2. Onay iletişim kutusu açıldığında **Yes**'i (Evet) tıklatın.

– veya –

1. File Sanitizer'ı (Dosya Temizleyici) açın ve **Shred**'i (Parçala) tıklatın.
2. **Shred now** (Şimdi parçala) düğmesini tıklatın.
3. Onay iletişim kutusu açıldığında **Yes**'i (Evet) tıklatın.

Boş alan temizlemeyi el ile etkinleştirme

1. Görev çubuğunun en sağında bulunan bildirim alanındaki **HP ProtectTools** simgesini sağ tıklatın ve **File Sanitizer**'ı (Dosya Temizleyici) ve ardından **Bleach Now**'ı (Şimdi Temizle) tıklatın.
2. Onay iletişim kutusu açıldığında **Yes**'i (Evet) tıklatın.

– veya –

1. File Sanitizer'ı (Dosya Temizleyici) açın ve **Free Space Bleaching**'i (Boş Alan Temizleme) tıklatın.
2. **Bleach Now**'ı (Şimdi Temizle) tıklatın.
3. Onay iletişim kutusu açıldığında **Yes**'i (Evet) tıklatın.

Bir parçalama veya boş alan temizleme işlemini iptal etme

Bir parçalama veya boş alan temizleme işlemi devam ederken, bildirim alanındaki HP ProtectTools Security Manager (HP ProtectTools Güvenlik Yöneticisi) simgesinin üzerinde bir ileti görüntülenir. İleti, parçalama veya boş alan temizleme işlemi hakkında ayrıntılar (tamamlanma yüzdesi) verir ve size işlemi iptal etme seçeneği sunar.

İşlemi iptal etmek için:

▲ İşlemi iptal etmek için iletiyi ve ardından **Stop**'ı (Durdur) tıklatın.

Günlük dosyalarını görüntüleme

Bir parçalama veya boş alan temizleme işlemi her gerçekleştirildiğinde, hataları veya bozuklukları içeren günlük dosyaları oluşturulur. Günlük dosyaları her zaman en son parçalama veya boş alan temizleme işlemine göre güncelleştirilir.

NOT: Başarıyla parçalanan veya temizlenen dosyalar, günlük dosyalarında görünmez.

Parçalama işlemleri için ve boş alan temizleme işlemleri için birer farklı günlük dosyası oluşturulur. Her iki günlük dosyası da sabit sürücüde şu konumda yer alır:

- C:\Program Files\Hewlett-Packard\File Sanitizer*[Kullanıcı Adı]*_ShredderLog.txt
- C:\Program Files\Hewlett-Packard\File Sanitizer*[Kullanıcı Adı]*_DiskBleachLog.txt

11 HP ProtectTools için Device Access Manager (Aygıt Erişim Yöneticisi) (yalnızca belirli modellerde)

Windows® işletim sistemi yöneticileri, bir sistemdeki aygıtlara erişimi denetlemek ve yetkisiz erişime karşı koruma sağlamak için HP ProtectTools için Device Access Manager'ı (Aygıt Erişim Yöneticisi) kullanır.

- Her kullanıcı için, erişim izni verilen veya reddedilen aygıtları tanımlayan aygıt profilleri oluşturulur.
- Kullanıcılar, önceden tanımlı Device Administrator (Aygıt Yöneticisi) grubu gibi gruplar halinde düzenlenebilir veya gruplar Denetim Masası'nın Yönetimsel Araçlar bölümündeki Bilgisayar Yönetimi seçeneği kullanılarak tanımlanabilir.
- Aygıt erişimi, grup üyeliği esas alınarak verilebilir veya reddedilebilir.
- CD-ROM sürücüler veya DVD sürücüler gibi aygıt sınıfları için, okuma erişimi ve yazma erişimi izni ayrı ayrı verilebilir veya reddedilebilir.

Sınırlı kullanıcılara da aygıt erişim denetimi ilkesini okumak ve değiştirmek için izin verilebilir.

Kurulum Yordamları

Device Access Manager'ı (Aygıt Erişim Yöneticisi) açma

Device Access Manager'ı (Aygıt Erişim Yöneticisi) açmak için aşağıdaki adımları uygulayın:

1. **Başlat**'ı tıklatın, **Tüm Programlar**'ı tıklatın, **HP**'yi ve ardından **HP ProtectTools Administrative Console**'u (HP ProtectTools Yönetim Konsolu) tıklatın.
2. Sol bölmede **Device Access Manager**'ı (Aygıt Erişim Yöneticisi) tıklatın.

Aygıt erişimini yapılandırma

HP ProtectTools için Device Access Manager (Aygıt Erişim Yöneticisi) üç görünüm sunar:

- Simple Configuration (Basit Yapılandırma) görünümü, Device Administrators (Aygıt Yöneticileri) grubunun üyeleri için aygıt sınıfları erişimine izin vermek veya erişimi reddetmek için kullanılır.
- Device Class Configuration (Aygıt Sınıfı Yapılandırması) görünümü, belirli kullanıcılar veya gruplar için aygıt türlerine veya belirli aygıtlara yönelik erişim vermek veya reddetmek için kullanılır.
- User Access Settings (Kullanıcı Erişim Ayarları) görünümü, hangi kullanıcıların Simple Configuration (Basit Yapılandırma) ve Device Class Configuration (Aygıt Sınıfı Yapılandırması) bilgilerini görüntüleyebileceğini veya değiştirebileceğini belirtmek için kullanılır.

Device administrators (Aygıt yöneticileri) grubu

Device Access Manager (Aygıt Erişim Yöneticisi) yüklendiğinde, bir Device Administrators (Aygıt Yöneticileri) grubu oluşturulur.

Sistem yöneticisi, bir kullanıcı güvenilir olarak sınıflandırılmamışsa (aygıt erişimi açısından), bir aygıt sınıfı kümesine erişimi reddederek basit bir aygıt erişim denetimi ilkesi uygulayabilir. "Aygıt için güvenilir" ve "aygıt için güvenilir olmayan" kullanıcıları ayırt etmenin önerilen yolu, tüm "aygıt için güvenilir" kullanıcıları Device Administrators (Aygıt Yöneticileri) grubunun bir üyesi yapmaktır. Böylece, Device Administrators (Aygıt Yöneticileri) grubunun öğelerine Simple Configuration (Basit Yapılandırma) ve Device Class Configuration (Aygıt Sınıfı Yapılandırması) görünümleri üzerinden aygıt erişimi vermek, "aygıt için güvenilir" kullanıcıların belirtilen aygıt sınıfı kümesine tam erişimi olmasını sağlayacaktır.

NOT: Bir kullanıcıyı Device Administrators (Aygıt Yöneticileri) grubuna eklemek, otomatik olarak kullanıcının aygıtlara erişmesini sağlamaz. Ancak "aygıt için güvenilir" kullanıcılara gerekli aygıt sınıfı kümesi erişimini vermek üzere Simple Configuration (Basit Yapılandırma) görünümü kullanılabilir.

Device Administrators (Aygıt Yöneticileri) grubuna kullanıcı eklemek için şu adımları izleyin:

- Windows 7, Vista veya XP Professional'da, standart “Yerel Kullanıcılar ve Gruplar” MMC ek bileşenini kullanın.
- Windows 7, Vista® veya XP'nin home sürümlerinde, ayrıcalıklı bir hesaptan, komut istemi penceresine şunu yazın:

```
c:\> net localgroup “Device Administrators” kullanıcıadı /ADD
```

Simple Configuration (Basit Yapılandırma)

Yöneticiler ve yetkili kullanıcılar, tüm Device Administrators (Aygıt Yöneticileri) dışı kullanıcılar için aşağıdaki aygıt sınıflarına erişimi değiştirmek için Simple Configuration (Basit Yapılandırma) görünümünü kullanabilirler.

NOT: Aygıt erişim bilgilerini okumak amacıyla bu görünümü kullanmak için, kullanıcıya veya gruba **User Access Settings** (Kullanıcı Erişim Ayarları) görünümünde "okuma" erişimi verilmiş olması gerekir. Aygıt erişim bilgilerini değiştirmek amacıyla bu görünümü kullanmak için, kullanıcıya veya gruba **User Access Settings** (Kullanıcı Erişim Ayarları) görünümünde "değiştirme" erişimi verilmiş olması gerekir.

- Tüm çıkarılabilir medyalar (disketler, USB flash sürücüler vb.)
- Tüm DVD/CD-ROM sürücüler
- Tüm seri ve paralel bağlantı noktaları
- Tüm Bluetooth® aygıtları
- Tüm kızılötesi aygıtları
- Tüm modem aygıtları
- Tüm PCMCIA aygıtları
- Tüm 1394 aygıtları

Device Administrators (Aygıt Yöneticileri) dışındaki tüm kullanıcıların bir aygıt sınıfına erişimine izin vermek veya erişimini reddetmek için şu adımları izleyin:

1. **HP ProtectTools Administrative Console**'un (HP ProtectTools Yönetim Konsolu) sol bölmesinde, **Device Access Manager**'ı (Aygıt Erişim Yöneticisi) ve ardından **Simple Configuration**'ı (Basit Yapılandırma) tıklatın.
2. Sağ bölmede, erişimi reddetmek için bir aygıt sınıfının veya belirli bir aygıtın onay kutusunu seçin. Bu aygıt sınıfına veya belirli bir aygıta erişime izin vermek için onay kutusunu temizleyin.

   Onay kutusu soluk görünüyorsa, erişim senaryosunu etkileyen değerler Device Class Configuration (Aygıt Sınıfı Yapılandırması) görünümünden değiştirilmiştir. Değerleri yeniden basit ayarlara sıfırlamak için, onay kutusunu temizlemek veya seçmek üzere tıklatın ve ardından onaylamak için **Yes**'i (Evet) tıklatın.
3. **Save** (Kaydet) simgesini tıklatın.

   NOT: Arka plan hizmeti çalışmıyorsa, başlatmak isteyip istemediğinizi soran bir iletişim kutusu açılır. **Yes**'i (Evet) tıklatın.
4. **OK**'i (Tamam) tıklatın.

Arka plan hizmetini başlatma

Aygıt profillerinin uygulanabilmesi için HP ProtectTools Security Manager (HP ProtectTools Güvenlik Yöneticisi), HP ProtectTools Device Locking/Auditing (HP ProtectTools Aygıt Kilitleme/Denetleme) arka plan hizmetini başlatmak isteyip istemediğinizi sormak üzere bir iletişim kutusu açar. **Yes**'i (Evet) tıklatın. Arka plan hizmeti başlatılır ve bundan böyle her sistem önyüklemesinde otomatik olarak başlatılacaktır.

NOT: Arka plan hizmeti istemi görüntülenmeden önce bir aygıt profili tanımlanmalıdır.

Yöneticiler de bu hizmeti başlatıp durdurabilir:

1. **Başlat**'ı ve ardından **Denetim Masası**'nı tıklatın.
2. **Yönetimsel Araçlar**'ı ve ardından **Hizmetler**'i tıklatın.
3. **HP ProtectTools Device Locking/Auditing** (HP ProtectTools Aygıt Kilitleme/Denetleme) hizmetini bulun.

Device Locking/Auditing (Aygıt Kilitleme/Denetleme) hizmetinin durdurulması, aygıt kilitlemeyi durdurmaz. Aygıt kilitlemeyi iki bileşen zorlar:

- Device Locking/Auditing (Aygıt Kilitleme/Denetleme) hizmeti
- DAMDrv.sys sürücüsü

Hizmetin başlatılması aygıt sürücüsünü başlatır, ancak hizmetin durdurulması sürücüyü durdurmaz.

Arka plan hizmetinin çalışıp çalışmadığını belirlemek için, bir komut istemi penceresi açın ve sc query flcdlock yazın.

Aygıt sürücüsünün çalışıp çalışmadığını belirlemek için, bir komut istemi penceresi açın ve sc query damdrv yazın.

Device Class Configuration (Aygıt Sınıfı Yapılandırması)

Yöneticiler ve yetkili kullanıcılar, aygıt sınıflarına veya belirli aygıtlara erişim izni verilen veya reddedilen kullanıcıların ve grupların listelerini görüntüleyebilir veya değiştirebilir.

NOT: Aygıt erişim bilgilerini okumak amacıyla bu görünümü kullanmak için, kullanıcıya veya gruba **User Access Settings** (Kullanıcı Erişim Ayarları) görünümünde "okuma" erişimi verilmiş olması gerekir. Aygıt erişim bilgilerini değiştirmek amacıyla bu görünümü kullanmak için, kullanıcıya veya gruba **User Access Settings** (Kullanıcı Erişim Ayarları) görünümünde "değiştirme" erişimi verilmiş olması gerekir.

Device Class Configuration (Aygıt Sınıfı Yapılandırması) aşağıdaki bölümleri içerir:

- **Device List** (Aygıt Listesi)—Sistemde yüklü olan veya daha önce sisteme yüklenmiş olabilecek tüm aygıt sınıflarını ve aygıtları gösterir.
  - Bir aygıt sınıfına genellikle koruma uygulanır. Seçilen bir kullanıcı veya grup, aygıt sınıfındaki herhangi bir aygıta erişebilecektir.
  - Belirli aygıtlara da koruma uygulanabilir.
- **User List** (Kullanıcı Listesi)—Seçilen aygıt sınıfı veya belirli bir aygıt için erişim izni verilen veya reddedilen tüm kullanıcıları ve grupları gösterir.
  - User List (Kullanıcı Listesi) girişi, belirli bir kullanıcı veya kullanıcının üyesi olduğu bir grup için oluşturulabilir.
  - User List'teki (Kullanıcı Listesi) bir kullanıcı veya grup girişi kullanılamıyorsa, ayar, Device List'teki (Aygıt Listesi) aygıt sınıfından veya Class (Sınıf) klasöründen devralınmıştır.
  - DVD ve CD-ROM gibi bazı aygıt sınıfları, okuma ve yazma işlemleri için ayrı ayrı izin verilerek veya reddedilerek daha ayrıntılı denetlenebilir.

    Diğer aygıtlar ve sınıflar için, okuma ve yazma erişim hakları devralınabilir. Örneğin, Read (Okuma) erişimi daha yüksek bir sınıftan devralınabilirken, Write (Yazma) erişimi bir kullanıcı veya grup için özel olarak reddedilebilir.

NOT: Read (Okuma) onay kutusu boşsa, erişim denetimi girişinin aygıta yönelik okuma erişimi üzerinde etkisi yoktur. Aygıta yönelik okuma izni vermez veya reddetmez.

Örnek 1—Bir kullanıcının veya grubun, bir aygıta veya aygıt sınıfına yönelik yazma erişimi reddedilirse:

Aynı kullanıcıya, aynı gruba veya aynı grubun bir üyesine, yalnızca aygıt hiyerarşisinde bu aygıtın altında olan bir aygıt için yazma erişimi veya okuma+yazma erişimi verilebilir.

Örnek 2—Bir kullanıcıya veya gruba, bir aygıta veya aygıt sınıfına yönelik yazma erişimi verilirse:

Aynı kullanıcının, aynı grubun veya aynı grubun bir üyesinin, yalnızca aynı aygıt için veya aygıt hiyerarşisinde bu aygıtın altında olan bir aygıt için yazma erişimi veya okuma+yazma erişimi reddedilebilir.

Örnek 3—Bir kullanıcıya veya gruba, bir aygıta veya aygıt sınıfına yönelik okuma erişimi verilirse:

Aynı kullanıcının, aynı grubun veya aynı grubun bir üyesinin, yalnızca aynı aygıt için veya aygıt hiyerarşisinde bu aygıtın altında olan bir aygıt için okuma erişimi veya okuma+yazma erişimi reddedilebilir.

Örnek 4—Bir kullanıcının veya grubun, bir aygıta veya aygıt sınıfına yönelik okuma erişimi reddedilirse:

Aynı kullanıcıya, aynı gruba veya aynı grubun bir üyesine, yalnızca aygıt hiyerarşisinde bu aygıtın altında olan bir aygıt için okuma erişimi veya okuma+yazma erişimi verilebilir.

Örnek 5—Bir kullanıcıya veya gruba, bir aygıta veya aygıt sınıfına yönelik okuma+yazma erişimi verilirse:

Aynı kullanıcının, aynı grubun veya aynı grubun bir üyesinin, yalnızca aynı aygıt için veya aygıt hiyerarşisinde bu aygıtın altında olan bir aygıt için yazma erişimi veya okuma+yazma erişimi reddedilebilir.

Örnek 6—Bir kullanıcının veya grubun, bir aygıta veya aygıt sınıfına yönelik okuma+yazma erişimi reddedilirse:

Aynı kullanıcıya, aynı gruba veya aynı grubun bir üyesine, yalnızca aygıt hiyerarşisinde bu aygıtın altında olan bir aygıt için okuma erişimi veya okuma+yazma erişimi verilebilir.

Bir kullanıcı veya grup için erişimi reddetme

Bir kullanıcının veya grubun bir aygıta veya aygıt sınıfına erişmesini engellemek için şu adımları izleyin:

1. **HP ProtectTools Administrative Console**'un (HP ProtectTools Yönetim Konsolu) sol bölmesinde, **Device Access Manager**'ı (Aygıt Erişim Yöneticisi) ve ardından **Device Class Configuration**'ı (Aygıt Sınıfı Yapılandırması) tıklatın.
2. Aygıt listesinde, yapılandırmak istediğiniz aygıt sınıfını tıklatın.
   - Device class (Aygıt sınıfı)
   - All devices (Tüm aygıtlar)
   - Individual device (Tek aygıt)
3. **User/Groups** (Kullanıcı/Gruplar) altında, erişimi reddedilecek olan kullanıcı veya grubu tıklatın.

4. Bir kullanıcının veya grubun yanındaki **Deny**'ı (Reddet) tıklatın.

5. **Save** (Kaydet) simgesini tıklatın.

NOT: Bir kullanıcı için reddet ve izin ver ayarları aynı aygıt düzeyinde belirlendiğinde, erişim reddetme, erişime izin vermeye kıyasla önceliğe sahiptir.

Bir kullanıcı veya grup için erişime izin verme

Bir kullanıcıya veya gruba bir aygıta veya aygıt sınıfına erişmek üzere izin vermek için şu adımları izleyin:

1. **HP ProtectTools Administrative Console**'un (HP ProtectTools Yönetim Konsolu) sol bölmesinde, **Device Access Manager**'ı (Aygıt Erişim Yöneticisi) ve ardından **Device Class Configuration**'ı (Aygıt Sınıfı Yapılandırması) tıklatın.

2. Aygıt listesinde aşağıdakilerden birini tıklatın:

   - Device class (Aygıt sınıfı)
   - All devices (Tüm aygıtlar)
   - Individual device (Tek aygıt)

3. **Add**'i (Ekle) tıklatın.

   Select Users or Groups (Kullanıcı veya Grup Seç) iletişim kutusu açılır.

4. Eklenecek kullanıcı veya grupları aramak için **Advanced**'i (Gelişmiş) ve ardından **Find Now**'ı (Şimdi Bul) tıklatın.

5. Mevcut kullanıcı ve grup listesine eklenecek kullanıcıyı veya grubu tıklatın ve ardından **OK**'i (Tamam) tıklatın.

6. Tekrar **OK**'i (Tamam) tıklatın.

7. Bu kullanıcı veya gruba erişim vermek için **Allow**'u (İzin ver) tıklatın.

8. **Save** (Kaydet) simgesini tıklatın.

Bir kullanıcı veya grup için erişimi kaldırma

Bir kullanıcının veya grubun bir aygıta veya aygıt sınıfına erişme iznini kaldırmak için şu adımları izleyin:

1. **HP ProtectTools Administrative Console**'un (HP ProtectTools Yönetim Konsolu) sol bölmesinde, **Device Access Manager**'ı (Aygıt Erişim Yöneticisi) ve ardından **Device Class Configuration**'ı (Aygıt Sınıfı Yapılandırması) tıklatın.

2. Aygıt listesinde, yapılandırmak istediğiniz aygıt sınıfını tıklatın.

   - Device class (Aygıt sınıfı)
   - All devices (Tüm aygıtlar)
   - Individual device (Tek aygıt)

3. **User/Groups** (Kullanıcı/Gruplar) altında, kaldırmak istediğiniz kullanıcıyı veya grubu tıklatın ve ardından **Remove**'u (Kaldır) tıklatın.

4. **Save** (Kaydet) simgesini tıklatın.

Gruptaki tek bir kullanıcı için bir aygıt sınıfına yönelik erişim izni verme

Bir kullanıcının grubundaki diğer tüm üyelerin bir aygıt sınıfına yönelik erişimini reddedip söz konusu kullanıcıya erişim izni vermek için şu adımları izleyin:

1. **HP ProtectTools Administrative Console**'un (HP ProtectTools Yönetim Konsolu) sol bölmesinde, **Device Access Manager**'ı (Aygıt Erişim Yöneticisi) ve ardından **Device Class Configuration**'ı (Aygıt Sınıfı Yapılandırması) tıklatın.
2. Aygıt listesinde, yapılandırmak istediğiniz aygıt sınıfını tıklatın.
   - Device class (Aygıt sınıfı)
   - All devices (Tüm aygıtlar)
   - Individual device (Tek aygıt)
3. **User/Groups** (Kullanıcı/Gruplar) altında, erişimi reddedilecek olan grubu seçin ve ardından **Deny**'ı (Reddet) tıklatın.
4. Gerekli sınıfın klasörünün altındaki klasöre gidin ve söz konusu kullanıcıyı ekleyin.
5. Bu kullanıcıya erişim vermek için **Allow**'ı (İzin ver) tıklatın.
6. **Save** (Kaydet) simgesini tıklatın.

Gruptaki tek bir kullanıcı için belirli bir aygıta yönelik erişim izni verme

Yöneticiler, sınıftaki tüm aygıtlar için gruptaki diğer üyelerin erişimini reddedip tek bir kullanıcıya belirli bir aygıta yönelik erişim verebilirler:

1. **HP ProtectTools Administrative Console**'un (HP ProtectTools Yönetim Konsolu) sol bölmesinde, **Device Access Manager**'ı (Aygıt Erişim Yöneticisi) ve ardından **Device Class Configuration**'ı (Aygıt Sınıfı Yapılandırması) tıklatın.
2. Aygıt listesinde, yapılandırmak istediğiniz aygıt sınıfını tıklatın ve altındaki klasöre gidin.
3. **Add**'i (Ekle) tıklatın. **Select Users or Groups** (Kullanıcı veya Grup Seç) iletişim kutusu açılır.
4. Kullanıcının sınıftaki tüm aygıtlara erişimi reddedilecek olan grubunu aramak için **Advanced**'i (Gelişmiş) ve ardından **Find Now**'ı (Şimdi Bul) tıklatın.
5. Grubu ve ardından **OK**'i (Tamam) tıklatın.
6. Aygıt sınıfı altında, kullanıcı için erişim izni verilecek belirli aygıta gidin.
7. **Add**'i (Ekle) tıklatın. **Select Users or Groups** (Kullanıcı veya Grup Seç) iletişim kutusu açılır.
8. Eklenecek kullanıcı veya grupları aramak için **Advanced**'i (Gelişmiş) ve ardından **Find Now**'ı (Şimdi Bul) tıklatın.
9. Erişim izni verilecek kullanıcıyı tıklatın ve **OK**'i (Tamam) tıklatın.
10. Bu kullanıcıya erişim vermek için **Allow**'ı (İzin ver) tıklatın.
11. **Save** (Kaydet) simgesini tıklatın.

Yapılandırmayı sıfırlama

△ **DİKKAT:** Yapılandırmanın sıfırlanması, yapılan tüm aygıt yapılandırma değişikliklerini yok sayar ve tüm ayarları fabrika değerlerine döndürür.

Yapılandırma ayarlarını fabrika değerlerine sıfırlamak için şu adımları izleyin:

1. **HP ProtectTools Administrative Console**'un (HP ProtectTools Yönetim Konsolu) sol bölmesinde, **Device Access Manager**'ı (Aygıt Erişim Yöneticisi) ve ardından **Device Class Configuration**'ı (Aygıt Sınıfı Yapılandırması) tıklatın.
2. **Reset** (Sıfırla) düğmesini tıklatın.
3. Onaylamak için **Yes**'i (Evet) tıklatın.
4. **Save** (Kaydet) simgesini tıklatın.

Gelişmiş görevler

Yapılandırma ayarlarına erişimi denetleme

User Access Settings (Kullanıcı Erişim Ayarları) görünümünde yöneticiler, Simple Configuration (Basit Yapılandırma) ve Device Class Configuration (Aygıt Sınıfı Yapılandırması) sayfalarını kullanmasına izin verilen grupları ve kullanıcıları belirtir.

NOT: User Access Settings (Kullanıcı Erişim Ayarları) görünümündeki ayarları değiştirmek için, bir kullanıcının veya grubun "Full User Administrator rights"a (Tam Kullanıcı Yönetici hakları) sahip olması gerekir.

- Simple Configuration (Basit Yapılandırma) ve Device Class Configuration (Aygıt Sınıfı Yapılandırması) bilgilerini görüntülemek için, bir kullanıcıya veya gruba User Access Settings (Kullanıcı Erişim Ayarları) görünümünde "View (Read-only) Configuration Settings" ((Salt-okunur) Yapılandırma Ayarlarını Görüntüleme) erişimi verilmelidir.
- Simple Configuration (Basit Yapılandırma) ve Device Class Configuration (Aygıt Sınıfı Yapılandırması) bilgilerini değiştirmek için, bir kullanıcıya veya gruba User Access Settings (Kullanıcı Erişim Ayarları) görünümünde "Change Configuration Settings" (Yapılandırma Ayarlarını Değiştirme) erişimi verilmelidir.

NOT: Administrators (Yöneticiler) grubunun üyelerine de, Simple Configuration (Basit Yapılandırma) ve Device Class Configuration (Aygıt Sınıfı Yapılandırması) görünümlerini görüntülemek için "okuma" erişimi; Simple Configuration (Basit Yapılandırma) ve Device Class Configuration (Aygıt Sınıfı Yapılandırması) görünümlerini kullanarak verileri değiştirmek için "değiştirme" erişimi verilmelidir.

NOT: Tüm kullanıcılar ve gruplar için erişim düzeyleri değerlendirildikten sonra bir kullanıcı için belirli bir erişim düzeyine yönelik olarak Allow (İzin ver) veya Deny (Reddet) ayarı seçilmemişse, kullanıcının erişimi tüm düzeylerde reddedilir.

Mevcut bir gruba veya kullanıcıya erişim verme

Mevcut bir gruba veya kullanıcıya yapılandırma ayarlarını görüntülemek veya değiştirmek üzere izin vermek için şu adımları izleyin:

1. **HP ProtectTools Administrative Console**'un (HP ProtectTools Yönetim Konsolu) sol bölmesinde, **Device Access Manager**'ı (Aygıt Erişim Yöneticisi) ve ardından **User Access Settings**'i (Kullanıcı Erişim Ayarları) tıklatın.
2. İzin verilecek grubu veya kullanıcıyı tıklatın.
3. **Permissions** (İzinler) altında, seçilen grup veya kullanıcıya verilecek her izin türü için **Allow**'ı (İzin ver) tıklatın:

NOT: Verilen izinler toplu niteliktedir. Örneğin, “Change Configuration Settings” (Yapılandırma Ayarlarını Değiştirme) izni verilen bir kullanıcıya otomatik olarak “View (Read-only) Configuration Settings” ((Salt-okunur) Yapılandırma Ayarlarını Görüntüleme) izni verilir. “Full User Administrator Rights” (Tam Kullanıcı Yönetici Hakları) verilen bir kullanıcıya, “Change Configuration Settings” (Yapılandırma Ayarlarını Değiştirme) ve “View (Read-only) Configuration Settings” ((Salt-okunur) Yapılandırma Ayarlarını Görüntüleme) izinleri de verilir.

- Full User Administrator Rights (Tam Kullanıcı Yönetici Hakları)
- Change Configuration Settings (Yapılandırma Ayarlarını Değiştirme)
- View (Read-only) Configuration Settings ((Salt-okunur) Yapılandırma Ayarlarını Görüntüleme)

4. **Save** (Kaydet) simgesini tıklatın.

Mevcut bir grubun veya kullanıcının erişimini reddetme

Mevcut bir grubun veya kullanıcının yapılandırma ayarlarını görüntüleme veya değiştirme iznini reddetmek için şu adımları izleyin:

1. **HP ProtectTools Administrative Console**'un (HP ProtectTools Yönetim Konsolu) sol bölmesinde, **Device Access Manager**'ı (Aygıt Erişim Yöneticisi) ve ardından **User Access Settings**'i (Kullanıcı Erişim Ayarları) tıklatın.
2. Erişimi reddedilecek grubu veya kullanıcıyı tıklatın.
3. **Permissions** (İzinler) altında, seçilen grup veya kullanıcıya yönelik olarak reddedilecek her izin türü için **Deny**'ı (Reddet) tıklatın:
   - Full User Administrator Rights (Tam Kullanıcı Yönetici Hakları)
   - Change Configuration Settings (Yapılandırma Ayarlarını Değiştirme)
   - View (Read-only) Configuration Settings ((Salt-okunur) Yapılandırma Ayarlarını Görüntüleme)
4. **Save** (Kaydet) simgesini tıklatın.

Yeni bir grup veya kullanıcı ekleme

Yeni bir gruba veya kullanıcıya yapılandırma ayarlarını görüntülemek veya değiştirmek üzere izin vermek için şu adımları izleyin:

1. **HP ProtectTools Administrative Console**'un (HP ProtectTools Yönetim Konsolu) sol bölmesinde, **Device Access Manager**'ı (Aygıt Erişim Yöneticisi) ve ardından **User Access Settings**'i (Kullanıcı Erişim Ayarları) tıklatın.
2. **Add**'i (Ekle) tıklatın. **Select Users or Groups** (Kullanıcı veya Grup Seç) iletişim kutusu açılır.
3. Eklenecek kullanıcı veya grupları aramak için **Advanced**'i (Gelişmiş) ve ardından **Find Now**'ı (Şimdi Bul) tıklatın.
4. Bir grubu veya kullanıcıyı tıklatın, **OK**'i (Tamam) tıklatın, ardından tekrar **OK**'i (Tamam) tıklatın.
5. Bu kullanıcıya erişim vermek için **Allow**'ı (İzin ver) tıklatın.
6. **Save** (Kaydet) simgesini tıklatın.

Grup veya kullanıcı erişimini kaldırma

Bir grubun veya kullanıcının, yapılandırma ayarlarını görüntülemeye veya değiştirmeye yönelik iznini reddetmek için şu adımları izleyin:

1. **HP ProtectTools Administrative Console**'un (HP ProtectTools Yönetim Konsolu) sol bölmesinde, **Device Access Manager**'ı (Aygıt Erişim Yöneticisi) ve ardından **User Access Settings**'i (Kullanıcı Erişim Ayarları) tıklatın.
2. Bir grubu veya kullanıcıyı tıklatın, sonra da **Remove**'u (Kaldır) tıklatın.
3. **Save** (Kaydet) simgesini tıklatın.

İlgili yönergeler

HP ProtectTools için Device Access Manager (Aygıt Erişim Yöneticisi), kurumsal ürün HP ProtectTools Enterprise Device Access Manager (HP ProtectTools Kurumsal Aygıt Erişim Yöneticisi) ile uyumludur. Kurumsal ürünle çalışırken, HP ProtectTools için Device Access Manager (Aygıt Erişim Yöneticisi) kendi özelliklerine yalnızca okuma erişimi için izin verir.

HP ProtectTools için Device Access Manager (Aygıt Erişim Yöneticisi) hakkında daha fazla bilgiye, Web'de http://www.hp.com/hps/security/products adresinden ulaşabilirsiniz.

12 LoJack Pro for HP ProtectTools

Absolute Software'in Computrace ürünleri, kullanıcıların HP bilgisayarlarını izlemelerini ve veri korumalarını geliştirmelerini sağlar. Computrace LoJack ürünleri ayrıca, makinenin kaybolma riskini azaltır ve çalınan makinelerin kurtarılmasına yardımcı olur.

Computrace ürününü etkinleştirmek için, şu yönergeleri izleyin:

1. **Başlat**'ı tıklatın, **Tüm Programlar**'ı tıklatın, ardından **HP ProtectTools Security Manager**'ı tıklatın.
2. **Theft Recovery**'yi (Hırsızlık Kurtarma) tıklatın, sonra da **Activate Now**'ı (Şimdi Etkinleştir) tıklatın.

   Varsayılan Web sunucunuz, HP ProtectTools ile birlikte kullanılabilen üç Computrace ürününden birini seçerek satın alabileceğiniz bir abonelik Web sitesi açar:

   - **Computrace Data Delete** (Computrace Veri Silme)—Uzaktan veri silme, aygıt dondurma ve temel varlık izlemesi ve raporlamasını içerir.
   - **Computrace LoJack Pro**—Uzaktan veri silme, aygıt dondurma ve temel varlık izlemesi ve raporlamasını ile yönetilen hırsızlık kurtarması içerir.
   - **Computrace LoJack Pro Premium**—Uzaktan veri silme, aygıt dondurma, gelişmiş varlık izlemesi ve raporları, mevki belirleme ve mevki koruma ile yönetilen hırsızlık kurtarması içerir.

Computrace Aracısı bilgisayar nakledilirken kapatılsa da, Aracı, HP iş bilgisayarlarının BIOS'una katıştırılmıştır. Aboneliğinizi satın aldıktan sonra, Aracı etkinleştirilebilir. Katıştırılmış Aracı, işletim sistemini yeniden yükleyebilir ve sabit sürücüleri yeniden biçimlendirebilir.

NOT: 1 ila 5 yıl arasında abonelik süreleri vardır. Daha fazla ayrıntı için lütfen Absolute Software abonelik sözleşmesine bakın. Kurtarma özelliği, coğrafi konumunuza bağlıdır. GPS izlemesi, WWAN seçeneğine sahip belirli modellerde desteklenmektedir.

13 Sorun Giderme

HP ProtectTools Security Manager (HP ProtectTools Güvenlik Yöneticisi)

Kısa açıklama	Ayrıntılar	Çözüm
Akıllı kartlar ve USB belirteçleri, Security Manager (Güvenlik Yöneticisi) yüklemesinden sonra yüklendiyse, Security Manager'da (Güvenlik Yöneticisi) kullanılamıyor.	Akıllı kartları ve USB belirteçlerini Security Manager'da (Güvenlik Yöneticisi) kullanmak için, destek yazılımlarının (sürücüler, PKCS#11 sağlayıcıları vb.) Security Manager (Güvenlik Yöneticisi) yüklemesinden önce yüklenmesi gerekir. Security Manager (Güvenlik Yöneticisi) zaten yüklü durumdaysa, akıllı kart veya belirteç destek yazılımını yükledikten sonra şu adımları izleyin:	Password Manager'da (Parola Yöneticisi) oturum açın. HP ProtectTools Security Manager'da (HP ProtectTools Güvenlik Yöneticisi), **Password Manager**'ı (Parola Yöneticisi), **Credentials**'ı (Kimlik Bilgileri) ve **Smart Card**'ı (Akıllı Kart) tıklatın. İstenirse bilgisayarı yeniden başlatın.
Bazı uygulama Web sayfaları kullanıcıların bazı işleri yapmalarını veya tamamlamalarını engelleyen hatalar veriyor.	Bazı Web tabanlı uygulamalar, Single Sign On (Tekli Oturum Açma) yönteminin devre dışı bırakma işlevselliği nedeniyle çalışmaz ve hata verir. Örneğin, sarı renkli bir üçgen içinde **!** işareti görünür, bir hata oluştuğunu belirtir.	Security Manager Single Sign On (Güvenlik Yöneticisi Tekli Oturum Açma) özelliği, tüm yazılım Web arabirimlerini desteklemez. Single Sign On (Tekli Oturum Açma) desteğini kapatarak söz konusu Web sitesinin Single Sign On (Tekli Oturum Açma) desteğini devre dışı bırakın. Security Manager (Güvenlik Yöneticisi) yazılım Yardım dosyalarında bulunan, Single Sign On (Tekli Oturum Açma) ile ilgili tüm yönergelere bakın. Belirli bir uygulama için belirli bir Single Sign On (Tekli Oturum Açma) işlemi devre dışı bırakılamıyorsa, HP teknik desteğini arayın ve HP Servis sözleşmeniz uyarınca 3. düzey desteği isteyin.
Oturum açma işleminde **Browse for Virtual Token (Sanal Belirteç Ara)** seçeneği görüntülenmiyor.	Güvenlik tehlikelerini azaltmak için göz atma seçeneği kaldırıldığından, kullanıcı Password Manager'da (Parola Yöneticisi) kayıtlı bir sanal belirtecin konumunu değiştiremez.	Arama seçeneği, kullanıcı olmayanların dosyaları silmesine, yeniden adlandırmasına ve Windows'un denetiminin başkalarının eline geçmesine olanak verdiği için kaldırılmıştır.
Etki alanı yöneticileri yetkileri olsa dahi Windows parolasını değiştiremiyor.	Bu, bir etki alanı yöneticisi, etki alanı ve yerel bilgisayar üzerinde Yönetici haklarına sahip bir hesapla bir etki alanında oturum açıp etki alanı kimliğini Password Manager'a (Parola Yöneticisi) kaydettirdikten sonra gerçekleşir. Etki alanı yöneticisi, Password Manager (Parola Yöneticisi) içinden Windows parolasını değiştirmeyi denerse, bir hatalı giriş hatası alır: **User account**	Password Manager (Parola Yöneticisi), **Change Windows password** (Windows parolasını değiştir) üzerinden bir etki alanı kullanıcısının hesap parolasını değiştiremez. Security Manager (Güvenlik Yöneticisi) yalnızca yerel bilgisayar hesabı parolalarını değiştirebilir. Etki alanı kullanıcısı, **Windows security** (Windows güvenlik) özelliğinin **Change password** (Parola değiştir) seçeneği üzerinden parolasını değiştirebilir, ancak etki alanı kullanıcısı yerel bilgisayarda fiziksel bir hesaba sahip olmadığından,

Kısa açıklama	Ayrıntılar	Çözüm
	restriction (Kullanıcı hesabı kısıtlaması).	Password Manager (Parola Yöneticisi) yalnızca oturum açmada kullanılan parolayı değiştirebilir.
Password Manager (Parola Yöneticisi), Corel WordPerfect 12 parolası GINA ile uyumsuzluk sorunları yaşıyor.	Kullanıcı Password Manager'da (Parola Yöneticisi) oturum açar, WordPerfect'te bir belge oluşturur ve parola korumasıyla kaydederse, Password Manager (Parola Yöneticisi) el ile veya otomatik olarak GINA parolasını algılayamaz veya tanıyamaz.	HP, gelecekteki ürün geliştirmeleri için bir çözüm araştırmaktadır.
Password Manager (Parola Yöneticisi) ekrandaki **Connect** (Bağlan) düğmesini tanımıyor.	Uzak Masaüstü Bağlantısı (RDP) için Single Sign On (Tekli Oturum Açma) kimlik bilgileri **Bağlan** olarak ayarlanmışsa, Single Sign On (Tekli Oturum Açma) yeniden başlatıldığında her zaman **Bağlan** yerine **Farklı Kaydet**'i verir.	HP, gelecekteki ürün geliştirmeleri için bir çözüm araştırmaktadır.
Yalnızca Windows XP Service Pack 1'de Bekleme modundan Hazırda Bekletme'ye geçildikten sonra, kullanıcı Password Manager'da oturum açamaz.	Yönetici veya kullanıcı sistemin hazırda bekletme ve uyku moduna geçmesine izin verdikten sonra Password Manager'da (Parola Yöneticisi) oturum açamaz ve Windows oturum açma ekranı hangi oturum açma kimlik bilgisinin (parola, parmak izi veya Java Kartı) seçildiğine bakılmaksızın görüntülenmeyi sürdürür.	Windows Update ile Windows'u Service Pack 2'ye güncelleştirin. Sorunun nedeniyle ilgili daha fazla bilgi için http://www.microsoft.com adresindeki Microsoft bilgi makalesi 813301'e bakın. Oturum açmak için, kullanıcının Password Manager'ı (Parola Yöneticisi) seçmesi ve oturum açması gerekir. Password Manager'da (Parola Yöneticisi) oturum açtıktan sonra, oturum açma işlemini tamamlaması için kullanıcıdan Windows'da oturum açması (kullanıcının Windows oturum açma seçeneğini belirlemesi gerekebilir) istenir. Kullanıcı ilk önce Windows'da oturum açarsa, Password Manager'da (Parola Yöneticisi) el ile oturum açması gerekir.
Güvenlik **Kimliği Geri Yükle** işleminin sanal belirteçle ilişkisi kayboluyor.	Kullanıcı kimliği geri yüklediğinde, Password Manager (Parola Yöneticisi) sanal belirtecin oturum açma ekranındaki yeri ile olan ilişkisini kaybedebilir. Password Manager (Parola Yöneticisi) sanal belirteci kaydetmiş olsa da, kullanıcının ilişkiyi geri yüklemek için belirteci yeniden kaydettirmesi gerekir.	Şu anda bu işleyiş biçimi normaldir. Security Manager'ı (Güvenlik Yöneticisi) kimlikleri saklamadan kaldırdığınızda, belirtecin sistem (sunucu) bölümü yok edilir; böylece, belirtecin istemci bölümü kimlik geri yükleme işlemiyle geri yüklense de belirteç artık oturum açmak için kullanılamaz. HP, çözüm için uzun vadeli seçenekler araştırmaktadır.

HP ProtectTools için Device Access Manager (Aygıt Erişim Yöneticisi)

Kullanıcıların Device Access Manager'daki (Aygıt Erişim Yöneticisi) aygıtlara erişimi reddedildi, ancak aygıtlar hala erişilebilir durumda.

- **Açıklama**—Kullanıcıların aygıtlara erişimini reddetmek için, Device Access Manager (Aygıt Erişim Yöneticisi) içinden Simple Configuration (Basit Yapılandırma) ve/veya Device Class Configuration (Aygıt Sınıfı Yapılandırması) kullanıldı. Erişimleri reddedilse de, kullanıcılar aygıtlara erişmeye devam ediyor.
- **Çözüm:**
  - HP ProtectTools Device Locking (HP ProtectTools Aygıt Kilitleme) hizmetinin başlatıldığını doğrulayın.
  - Bir yönetici kullanıcı olarak, **Denetim Masası**'nı ve **Sistem ve Bakım**'ı tıklatın. Yönetimsel Araçlar penceresinde, **Hizmetler**'i tıklatın ve **HP ProtectTools Device Locking/Auditing** (HP ProtectTools Aygıt Kilitleme/Denetleme) hizmetini arayın. Hizmetin başlatıldığından ve başlangıç türünün **Automatic** (Otomatik) olduğundan emin olun.

Bir kullanıcının beklenmedik bir şekilde bir aygıta erişimi var veya bir kullanıcının beklenmedik bir şekilde bir aygıta erişimi reddediliyor.

- **Açıklama**—Kullanıcıların bazı aygıtlara erişimini reddetmek ve diğer aygıtlara erişimine izin vermek için Device Access Manager (Aygıt Erişim Yöneticisi) kullanıldı. Kullanıcı sistemi kullanırken, Device Access Manager (Aygıt Erişim Yöneticisi) tarafından engellendiğini düşündükleri aygıtlara erişebiliyor ve Device Access Manager (Aygıt Erişim Yöneticisi) tarafından izin verilmesi gerektiğini düşündükleri aygıtlara erişimi reddediliyor.
- **Çözüm:**
  - Kullanıcının aygıt ayarlarını incelemek için Device Access Manager (Aygıt Erişim Yöneticisi) içinden Device Class Configuration'ı (Aygıt Sınıf Yapılandırması) kullanın.
  - **Security Manager**'ı (Güvenlik Yöneticisi), **Device Access Manager**'ı (Aygıt Erişim Yöneticisi) ve ardından **Device Class Configuration**'ı (Aygıt Sınıfı Yapılandırması) tıklatın. Device Class (Aygıt Sınıfı) ağacındaki düzeyleri genişletin ve bu kullanıcı için geçerli olan ayarları inceleyin. Kullanıcı veya Users (Kullanıcılar) ya da Administrators (Yöneticiler) gibi üyesi olduğu herhangi bir Windows Grubu için ayarlanmış olabilecek “Deny” (Reddet) izinlerini arayın.

İzin ver ve reddet. Hangisi önceliğe sahiptir?

- **Açıklama**—Device Class Configuration (Aygıt Sınıfı Yapılandırması) içinden, aşağıdaki yapılandırma ayarlanmıştır:
  - Allow (İzin ver) izni bir Windows grubuna (örn. BUILTIN\Administrators) ve Deny (Reddet) izni aygıt sınıfı hiyerarşisinde aynı düzeyde olan (örn. DVD/CD-ROM Drives (DVD/CD-ROM Sürücüler)) başka bir Windows grubuna (örn. BUILTIN\Users) verildi.
  - Bir kullanıcı bu gruplardan her ikisinin de üyesi ise (örn. Yönetici), hangisi önceliğe sahiptir?
- **Çözüm:**
  - Kullanıcının aygıta erişimi reddedilir. Deny (Reddet), Allow (İzin ver) üzerinde önceliğe sahiptir.
  - Windows'un aygıt için etkin izni yürütme biçiminden dolayı, erişim reddedilir. Bir grup reddedilir ve diğer gruba izin verilir, ancak kullanıcı her iki grubun da üyesidir. Erişimi reddetme, erişime izin verme üzerinde önceliğe sahip olduğundan, kullanıcı reddedilir.
  - Geçici bir çözüm, DVD/CD-ROM Drives (DVD/CD-ROM Sürücüler) düzeyinde Users (Kullanıcılar) grubunu reddetmek ve DVD/CD-ROM Drives (DVD/CD-ROM Sürücüler) düzeyinin altındaki düzeyde Administrators (Yöneticiler) grubuna izin vermektir.
  - Başka bir geçici çözüm ise, DVD/CD erişimine izin vermek için bir grup, DVD/CD erişimini reddetmek için başka bir grup olmak üzere belirli Windows grupları oluşturmaktır. Daha sonra, belirli kullanıcılar uygun gruba eklenebilir.

Simple Configuration (Basit Yapılandırma) görünümü, bir aygıt erişimi denetim ilkesini tanımlamak için kullanıldı, ancak yönetici kullanıcılar aygıtlara erişemiyor.

- **Açıklama**—Simple Configuration (Basit Yapılandırma), Users (Kullanıcılar) ve Guests (Konuklar) için erişimi reddediyor ve Device Administrators (Aygıt Yöneticileri) için erişim izni veriyor.
- **Çözüm:** Yönetici kullanıcıyı Device Administrators (Aygıt Yöneticileri) grubuna ekleyin.

Çeşitli

İlgili Yazılım—Kısa açıklama	Ayrıntılar	Çözüm
Security Manager (Güvenlik Yöneticisi)—Alınan uyarı: **HP Protect Tools Security Manager (Güvenlik Yöneticisi) yüklenene kadar güvenlik uygulaması yüklenemiyor**.	Java Card Security (Java Kartı Güvenliği) ve biyometri gibi tüm güvenlik uygulamaları, Security Manager (Güvenlik Yöneticisi) arabirimine yönelik genişletilebilir eklentilerdir. HP onaylı bir güvenlik eklentisinin yüklenebilmesi için, Security Manager'ın (Güvenlik Yöneticisi) yüklenmiş olması gerekir.	Bir güvenlik eklentisinin yüklenebilmesi için önce Security Manager (Güvenlik Yöneticisi) yazılımı yüklenmelidir.
HP ProtectTools Security Manager (HP ProtectTools Güvenlik Yöneticisi)—Security Manager (Güvenlik Yöneticisi) arabirimi kapatılırken ara sıra bir hata oluşuyor.	Tüm eklenti uygulamaların yüklenmesi bitmeden önce Security Manager'ı (Güvenlik Yöneticisi) kapatmak üzere ekranın sağ üst tarafındaki kapatma düğmesi kullanıldığında ara sıra (12'de 1) hata oluşuyor.	Bu, Security Manager (Güvenlik Yöneticisi) kapatılırken ve yeniden başlatılırken eklenti hizmetleri yükleme işlemleri ile ilgili bir zamanlama bağlantısıyla ilişkilidir. PTHOST.exe başka uygulamaları (eklentileri) içeren bir kabuk olduğundan, eklentinin yükleme süresini tamamlayabilmesine bağımlıdır (hizmetler). Eklenti yükleme işlemini tamamlamadan önce kabuğun kapatılması ana sebeptir. Security Manager'ın (Güvenlik Yöneticisi) hizmetlerin yüklendiğini bildiren iletinin görüntülenmesine (Security Manager (Güvenlik Yöneticisi) penceresinin üst kısmında görüntülenir) ve tüm eklentileri soldaki sütunda listelenmiş halde görene kadar bekleyin. Hatanın olmaması için, ilgili eklentilerin yüklenmesine izin verecek makul bir süre bekleyin.
HP ProtectTools—Sınırsız erişim veya denetimsiz yönetici ayrıcalıkları güvenlik açısından tehlikeler oluşturuyor.	İstemci bilgisayarına sınırsız erişim çeşitli tehlikeleri de beraberinde getirir: • PSD'nin silinmesi • Kullanıcı ayarlarında zararlı değişikliklerin yapılması • Güvenlik ilkelerinin ve işlevlerinin devre dışı bırakılması	Yöneticilerin, son kullanıcı ayrıcalıklarını kısıtlarken ve kullanıcı erişimini kısıtlarken "en iyi uygulamaları" izlemeleri önerilir. Yetkisiz kullanıcılara yönetimsel ayrıcalıklar verilmemelidir.

Sözlük

acil durum kurtarma arşivi Temel kullanıcı anahtarlarının bir platform sahibi anahtarından diğerine tekrar şifrelenmesine olanak veren korumalı depolama alanı.

açılış kimlik doğrulaması Bilgisayar başlatıldığında bir tür kimlik doğrulaması (örneğin, Java Kartı, güvenli yonga veya parola) gerektiren güvenlik özelliği.

ağ hesabı Yerel bir bilgisayarda, bir çalışma grubunda veya bir etki alanında bulunan Windows kullanıcı veya yönetici hesabı.

akıllı kart Boyut ve şekil olarak kredi kartına benzeyen, sahibi ile ilgili kimlik bilgilerini barındıran küçük bir donanım. Sahip kimliğini bilgisayara doğrulamak için kullanılır.

arka plan hizmeti Uygulanacak aygıt erişim denetimi ilkeleri için çalışması gereken HP ProtectTools Device Locking/Auditing (HP ProtectTools Aygıt Kilitleme/Denetleme) arka plan hizmeti. Denetim Masası'ndaki Yönetimsel Araçlar altında bulunan Hizmetler uygulaması içinden görüntülenebilir. Çalışmıyorsa, aygıt erişim denetimi ilkeleri uygulandığında HP ProtectTools Security Manager (HP ProtectTools Güvenlik Yöneticisi) bu hizmeti başlatmayı dener.

ATM Ağ yöneticilerine sistemi BIOS düzeyinde uzaktan yönetme imkanı veren Otomatik Teknoloji Yöneticisi.

aygıt erişim denetimi ilkesi Bir kullanıcının erişimine izin verilen veya erişimi reddedilen aygıtların listesi.

aygıt sınıfı Sürücüler gibi, belirli bir türdeki tüm aygıtlar.

basit silme Bir varlığın Windows başvurusunu silme. Varlık içeriği, boş alan temizleme işlemiyle belirsizleştirme verisi ile üzerine yazılana kadar sabit sürücüde kalır.

belirteç Bkz. güvenlik oturum açma yöntemi.

biometrik Kullanıcıyı tanımlamak için parmak izi gibi fiziksel bir özellik kullanan kimlik doğrulaması bilgileri kategorisi.

boş alan temizleme Silinen varlıkların içeriğini bozmak için silinen varlıklar üzerine rasgele verileri güvenle yazma.

dijital imza Materyali göndereni ve dosyanın imzalandıktan sonra değiştirilmediğini doğrulayan, dosyayla birlikte gönderilen veri.

dijital sertifika Dijital sertifika sahibini dijital bilgileri imzalamak için kullanılan elektronik anahtar çiftine bağlayarak bir kişi veya kurumun kimliğini onaylayan elektronik kimlik bilgileri.

Drive Encryption (Sürücü Şifreleme) Bilgileri uygun yetkiye sahip olmayanlar tarafından okunamaz hale getirmek üzere sabit sürücünüzü (sürücülerinizi) şifreleyerek verilerinizi korur.

Drive Encryption (Sürücü Şifreleme) oturum açma ekranı Windows başlatılmadan önce bir oturum açma ekranı görüntülenir. Kullanıcıların Windows kullanıcı adlarını ve parolalarını veya Java Kartı PIN'lerini girmesi

gerekir. Birçok durumda, Drive Encryption (Sürücü Şifreleme) oturum açma ekranına doğru bilgilerin girilmesi, Windows'a, Windows oturum açma ekranında tekrar oturum açmaksızın erişmeye imkan verir.

DriveLock Sabit sürücüyü kullanıcıya bağlayan ve bilgisayar başladığında kullanıcıdan DriveLock parolasını doğru yazmasını isteyen güvenlik özelliği.

el ile parçalama Otomatik parçalama zamanlamasını atlayarak varlığın veya seçili varlıkların hemen parçalanması.

etki alanı Bir ağın parçası olan veya ortak dizin veritabanını paylaşan bilgisayar grubu. Etki alanları benzersiz olarak adlandırılır ve her birinin genel kural ve yordamları vardır.

etkinleştirme Drive Encryption (Sürücü Şifreleme) özelliklerinden herhangi birinin erişilebilir olması için tamamlanması gereken görev. Drive Encryption (Sürücü Şifreleme), HP ProtectTools Setup Wizard (HP ProtectTools Kurulum Sihirbazı) kullanılarak etkinleştirilir. Drive Encryption (Sürücü Şifreleme) yalnızca bir yönetici tarafından etkinleştirilebilir. Etkinleştirme işlemi, yazılımı etkinleştirme, sürücüyü şifreleme, bir kullanıcı hesabı oluşturma ve çıkarılabilir bir depolama aygıtında ilk yedekleme şifreleme anahtarını oluşturma aşamalarından oluşur.

geçiş Privacy Manager (Gizlilik Yöneticisi) Sertifikaları'nı ve Güvenilen Kişiler'i yönetme, geri yükleme ve aktarma olanağı sağlayan görev.

geri yükleme Program bilgilerini daha önce kaydedilmiş bir yedekleme dosyasından bu programa kopyalayan bir işlem.

Gizlilik Yöneticisi belgesi Microsoft Office belgelerini ve e-posta iletilerini imzalama ve şifreleme gibi şifreleme işlemleri için her kullandığınızda doğrulama gerektiren dijital sertifika.

görünüm Kayıtlı bir kullanıcının kimlik doğrulaması için kullanılacak bir fotoğrafı.

gösterme Kullanıcının, bir veya daha fazla sohbet geçmişi oturumunu, Kişi Ekran Adı'nı düz metin olarak görüntüleyerek ve oturumun görünmesini sağlayarak, şifresini çözmesine olanak sağlayan görev.

grup Bir aygıt sınıfına veya belirli bir aygıta yönelik olarak aynı erişim veya ret düzeyinde olan bir grup kullanıcı.

Güvenilen Kişi Güvenilen Kişi davetini kabul eden kişi.

Güvenilen Kişi alıcısı Güvenilen Kişi daveti alan kişi.

Güvenilen Kişi daveti Güvenilen Kişi olması istenen kişiye gönderilen e-posta.

Güvenilen Kişi listesi Güvenilen Kişiler'in listesi.

güvenilen kişiler için mühürle Dijital imza ekleyen, e-postayı şifreleyen ve seçtiğiniz güvenlik oturum açma yöntemini kullanarak doğruladıktan sonra e-postayı gönderen görev.

güvenilir gönderen İmzalanmış ve/veya şifrelenmiş e-postalar ve Microsoft Office belgeleri gönderen Güvenilen Kişi.

güvenilir IM iletişimi Güvenilir göndericiden Güvenilen Kişi'ye güvenilir mesajların gönderildiği iletişim oturumu.

güvenilir mesaj Güvenilir göndericiden Güvenilen Kişi'ye güvenilir mesajların gönderildiği iletişim oturumu.

güvenlik oturum açma yöntemi Bilgisayarda oturum açmak kullanılan yöntem.

HP SpareKey Sürücü şifreleme kilidinin yedek kopyası.

imza satırı Dijital imzanın görsel görüntülenmesi için yer tutucu. Bir belge imzalandığında, imzalayan kişinin adı ve doğrulama yöntemi görüntülenir. İmzalama tarihi ve imzalayanın başlığı da dahil edilir.

İmzala ve Şifrele düğmesi Microsoft Office uygulamalarının araç çubuğunda görüntülenen yazılım düğmesi. Düğmeyi tıklatma, Microsoft Office belgesini imzalamanıza, şifrelemenize veya şifreyi kaldırmanıza olanak sağlar.

iptal parolası Kullanıcı, dijital sertifika istediğinde oluşturulan parola. Kullanıcı, dijital sertifikasını iptal etmek istediğinde parola sorulur. Bu, yalnızca kullanıcının sertifikayı iptal etmesini garantiler.

Java Kartı Bilgisayara takılan çıkarılabilir kart. Oturum açma tanımlama bilgilerini içerir. Drive Encryption (Sürücü Şifreleme) oturum açma ekranında Java Kartı ile oturum açma, Java Kartı'nı takmanızı ve kullanıcı adınız ile Java Kartı PIN'ini yazmanızı gerektirir.

kimlik HP ProtectTools Security Manager'da (HP ProtectTools Güvenlik Yöneticisi), belirli bir kullanıcı için, hesap veya profil gibi kullanılan bir grup kimlik bilgisi ve ayar.

kimlik bilgileri Kullanıcının kimlik doğrulaması işleminde belirli bir görev için yetkisinin bulunduğunu kanıtlamak üzere kullandığı yöntem.

kimlik doğrulaması Kullanıcının, bilgisayara erişme, belirli programın ayarlarını değiştirme veya güvenli verileri görme gibi belirli görevleri gerçekleştirme yetkisinin olup olmadığını doğrulama işlemidir.

Kimlik kartı Kullanıcı adınız ve seçtiğiniz resimle masaüstünüzü görsel olarak tanımlamaya yarayan bir Windows Kenar Çubuğu aracı. HP ProtectTools Administrative Console'u (HP ProtectTools Yönetim Konsolu) açmak için kimlik kartını tıklatın.

konsol HP ProtectTools Administrative Console'daki (HP ProtectTools Yönetim Konsolu) özellik ve ayarlara erişebileceğiniz ve bunları yönetebileceğiniz merkezi bir konum.

kullanıcı Drive Encryption'da (Sürücü Şifreleme) kayıtlı herhangi biri. Drive Encryption'da (Sürücü Şifreleme) yönetici olmayan kullanıcılar sınırlı haklara sahiptir. Yalnızca kaydolup (yönetici onayı ile) oturum açabilirler.

Live Messenger History Viewer (Live Messenger Geçmiş Görüntüleyici) Şifreli sohbet geçmişi oturumlarını aramanıza ve görmenize olanak sağlayan Privacy Manager Chat (Gizlilik Yöneticisi Sohbet) bileşeni.

otomatik parçalama Kullanıcının File Sanitizer'da (Dosya Temizleyici) ayarladığı programlanmış parçalama işlemi.

oturum açma verisi Security Manager (Güvenlik Yöneticisi) içinde, Web sitelerinde ve diğer programlarda oturum açmak için kullanılabilen, bir kullanıcı adı ve paroladan (ve büyük olasılıkla seçilen diğer bilgilerden) oluşan bir nesne.

önerilen imzalayan Microsoft Word veya Microsoft Excel belgesinin sahibi tarafından belgeye imza satırı eklemek üzere atanan kişi.

pano HP ProtectTools için Security Manager'daki (Güvenlik Yöneticisi) özellik ve ayarlara erişebileceğiniz ve bunları yönetebileceğiniz merkezi bir konum.

parçalama Bir varlığın içindeki verileri belirsizleştiren algoritmayı yürütme.

parçalama döngüsü Parçalama algoritmasının her varlıktaki yürütülme sayısı. Ne kadar yüksek parçalama döngüsü sayısı seçerseniz, bilgisayarınız da o kadar güvende olur.

parçalama profili Belirlenen silme yöntemi ve varlıkların listesi.

parmak izi Parmak izi görüntünüzün dijital çıkarımı. Gerçek parmak izi görüntünüz, Security Manager (Güvenlik Yöneticisi) tarafından asla depolanmaz.

PIN Kişisel kimlik numarası.

PKI Sertifika ve şifreleme işlemi anahtarlarının oluşturulması, kullanılması ve yönetimi için kullanılan arabirimleri tanımlayan Genel Anahtar Altyapısı standardı.

PSD Kişisel güvenlik sürücüsü, önemli bilgiler için korumalı bir depolama alanı sağlar.

sanal belirteç Java Kartı'na ve kart okuyucusuna çok benzer biçimde çalışan güvenlik özelliği. Güvenlik anahtarı bilgisayarın sabit sürücüsüne veya Windows kayıt defterine kaydedilir. Sanal güvenlik anahtarıyla oturum açtığınızda, doğrulamayı tamamlamak için sizden bir kullanıcı PIN'i istenir.

SATA aygıt modu Bilgisayar ile sabit sürücüler ve optik sürücüler gibi toplu depolama aygıtları arasında veri aktarım modu.

Send Security (Güvenlik Gönder) düğmesi Microsoft Outlook e-posta iletilerinin araç çubuğunda görüntülenen yazılım düğmesi. Düğmeyi tıklatma Microsoft Outlook e-posta iletisini imzalamanıza ve/veya şifrelemenize olanak sağlar.

sertifika yetkilisi Bir genel anahtar altyapısını çalıştırmak için gereken sertifikayı yayınlayan hizmet.

Single Sign On (Tekli Oturum Açma) Internet'e ve parola doğrulaması gerektiren Windows uygulamalarına erişmek için Security Manager'ı (Güvenlik Yöneticisi) kullanmanıza olanak veren ve kimlik doğrulaması bilgilerini depolayan özellik.

sohbet geçmişi oturumu Sohbet oturumundaki her iki tarafın görüşmelerinin kaydını içeren şifreli dosya.

şifre çözme Şifrelenmiş veriyi düz metne dönüştürmek için şifrelemede kullanılan yordamlar.

şifre işlemleri Verilerin yalnızca belirli kişiler tarafından okunabilmesi için şifreleme ve şifre çözme işlemi.

şifreleme İstenmeyen kişilerin verileri okumasını önlemek için düz metni şifreli metne dönüştürmek üzere şifre işlemlerinde kullanılan bir yordam (örneğin, algoritma kullanma). Birçok veri şifreleme biçimi mevcut olup bunlar, ağ güvenliğinin temelini oluşturur. En sık kullanılan türler içerisinde, Veri şifreleme Standardı ve genel anahtar şifrelemesi bulunmaktadır.

Şifreleme Dosya Sistemi (EFS) Seçilen klasördeki tüm dosyaları ve alt klasörleri şifreleyen sistem.

şifreleme hizmet sağlayıcısı (CSP) Belirli şifreleme işlevlerini uygulamak için iyi tanımlanmış bir arabirimde kullanılabilen şifreleme algoritmaları sağlayıcısı veya kitaplığı.

tuş dizisi Basıldığında otomatik parçalamayı başlatan ctrl+alt+s gibi belirli tuşların birleşimi.

TXT Güvenilir Yürütme Teknolojisi.

USB belirteci Kullanıcının tanımlama bilgilerini depolayan güvenlik aygıtı. Java Kartı ve biyometri okuyucusu gibi, bilgisayarın sahibini doğrulamak için kullanılır.

varlık Kişisel bilgiler veya dosyalar, geçmiş ve Web'le ilişkili veriler vb içeren, sabit sürücüde yer alan veri bileşeni.

Windows kullanıcı hesabı Bir ağda veya bilgisayarda oturum açma izni olan kişinin profili.

Windows Oturum Açma Güvenliği Windows hesabınızı (hesaplarınızı), erişim için belirli kimlik bilgilerinin kullanılmasını gerektirerek korur.

Windows yöneticisi İzinleri değiştirmek ve diğer kullanıcıları yönetmek için tüm hakları olan kullanıcı.

yedekleme Önemli program bilgilerinin bir kopyasını, programın dışındaki bir konuma kaydetmek için yedekleme özelliğini kullanma. Böylece, sonraki bir tarihte bu bilgileri aynı bilgisayara veya başka bir bilgisayara geri yüklemek için kullanılabilir.

yeniden başlatma Bilgisayarı yeniden başlatma işlemi.

yetkili kullanıcı Simple Configuration (Basit Yapılandırma) veya Device Class Configuration (Aygıt Sınıfı Yapılandırması) görünümünde yapılandırma ayarlarını görüntülemek veya değiştirmek için, User Access Settings (Kullanıcı Erişim Ayarları) görünümünde kendisine izin verilen bir kullanıcı.

yönetici Windows yöneticisine *başvurun*.

Dizin