HP Client Security

Başlarken

Birinci Basım: Ağustos 2013

Belge Parça Numarası: 735339-141

İçindekiler

1 HP Client Security Manager'a giriş

HP Client Security; verilerinizi, aygıtınızı ve kimliğinizi koruma imkanı sunarak bilgisayarınızın güvenliğini artırır.

Bilgisayarınızda kullanılabilen yazılım modülleri, bilgisayarınızın modeline göre değişebilir.

HP Client Security yazılım modülleri önceden kurulmuş, önceden yüklenmiş olabileceği gibi HP web sitesinden de indirilebilir. Daha fazla bilgi için, bkz. http://www.hp.com.

NOT: Bu kılavuzda verilen yönergeler, ilgili HP Client Security yazılım modüllerini önceden yüklediğiniz varsayılarak yazılmıştır.

HP Client Security özellikleri

Aşağıdaki tabloda HP Client Security modüllerinin önemli özellikleri ayrıntılarıyla verilmiştir.

Modül	Önemli özellikler
HP Client Security Manager	Yöneticiler aşağıdakileri yapabilir: • Windows® başlamadan bilgisayarınızı koruyabilir • Güçlü kimlik doğrulama ile Windows hesabınızı koruyabilir • Web siteleri ve uygulamalar için kullandığınız oturum açma hesaplarınızı ve parolalarınızı yönetebilir • Windows işletim sistemi parolanızı kolayca değiştirebilir • Ekstra güvenlik ve kolaylık için parmak izi kullanabilir • Kimlik doğrulama işlemi için akıllı kart, temassız kart veya yakın alan kartı kullanabilir • Bluetooth telefonunuzu tanımlama yöntemi olarak kullanabilir • Kimlik doğrulama seçeneklerinizi genişletmek için bir PIN belirleyebilir • Oturum açma hesabı ve oturum ilkelerini yapılandırabilir • Program verilerinizi yedekleyebilir ve geri yükleyebilir • HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager ve HP Computrace gibi uygulamaları ekleyebilirsiniz Genel kullanıcılar aşağıdakileri yapabilir: • Şifreleme Durumu ve Device Access Manager'ın ayarlarını görüntüleyebilir. • Computrace'i etkinleştirebilir. • Tercihler, Yedekleme ve Geri Yükleme seçeneklerini yapılandırabilir.

Modül	Önemli özellikler
Password Manager	Genel kullanıcılar aşağıdakileri yapabilir: • Kullanıcı adları ve parolaları düzenleyip ayarlayabilir. • Eposta ve Web hesapları için gelişmiş hesap güvenliği sağlamak adına daha güçlü parolalar oluşturabilir. Password Manager bilgileri otomatik olarak girer ve gönderir. • Kullanıcı kimlik bilgilerini otomatik olarak anımsayıp uygulayan Çoklu Oturum Açma özelliğiyle oturum açma sürecini kolaylaştırabilir. • Bir hesabı riskli olarak işaretleyip benzer kimlik bilgisine sahip diğer hesap veya hesaplar için uyarılabilir. • Desteklenen bir tarayıcıdan oturum açma verilerini alabilir.
HP Drive Encryption (yalnızca belirli modellerde)	• Birimin tamamını kapsayan eksiksiz sabit sürücü şifrelemesi yapar. • Verinin şifresini çözmek ve veriye erişmek için önyükleme öncesi kimlik doğrulamasını zorunlu kılar. • Kendi kendini şifreleyen sürücüler özelliğini etkinleştirme seçeneği sunar (yalnızca belirli modellerde).
HP Device Access Manager	• IT yöneticilerinin aygıtlara erişimi kullanıcı profili temelinde denetlemesine olanak tanır. • Yetkisiz kullanıcıların harici depolama ortamı kullanarak veri almasını ve harici ortamdan sisteme virüs bulaştırmasını önler. • Yöneticilerin belirli kişiler veya kullanıcı grupları için iletişim aygıtlarına erişimi devre dışı bırakmalarına olanak sağlar.
HP Trust Circles	• Dosya ve belge güvenliği sağlar. • Kullanıcının belirlediği klasörlere konulan dosyaları şifreler ve onları bir güven çemberi (trust circle) içinde korur. • Dosyaların yalnızca güven çemberi üyeleri tarafından kullanılmasına ve paylaşılmasına izin verir.
Theft Recovery (Computrace, ayrıca satın alınır)	• Etkinleştirilecek izleme ve takip aboneliklerinin ayrıca satın alınmasını gerektirir. • Güvenli varlık izlemesi sağlar. • Donanım ve yazılım değişikliklerinin yanı sıra kullanıcı aktivitelerini de izler. • Sabit sürücü yeniden biçimlendirilse veya değiştirilse bile etkin kalmaya devam eder.

HP Client Security ürün açıklaması ve yaygın kullanım örnekleri

HP Client Security ürünlerinin çoğunda, parolaların kaybedilmesi, hazır bulunmaması, unutulması halinde veya kurumsal güvenlik için erişim gerektiğinde erişim sağlamak için hem kullanıcı kimlik doğrulaması (genellikle bir paroladır) hem de yönetici yedeği kullanılır.

NOT: Bazı HP Client Security ürünleri, veriye erişimi kısıtlayacak şekilde tasarlanmıştır. Kullanıcının, yetkisiz kişilerin eline geçmesindense onları kaybetmeyi tercih edeceği kadar önemli veriler şifrelenmelidir. Tüm verilerin güvenli bir konumda yedeklenmesi önerilir.

Password Manager

Password Manager kullanıcı adlarını ve parolaları depolar ve aşağıdakiler için kullanılabilir:

- Internet erişimi veya eposta için oturum açma adları ve parolaların kaydedilmesi.
- Kullanıcıların bir web sitesinde veya epostada otomatik olarak oturum açması.
- Kimlik doğrulamaların yönetilmesi ve düzenlenmesi.
- Bir Web veya ağ varlığının seçilerek bağlantıya doğrudan erişilmesi.
- Gerektiğinde adların ve parolaların görüntülenmesi.
- Bir hesabı riskli olarak işaretlenip benzer kimlik bilgisine sahip diğer hesap veya hesaplar için uyarıda bulunulması.
- Desteklenen bir tarayıcıdan oturum açma verilerinin alınması.

Örnek 1: Büyük bir üretici firmanın satın alma temsilcisi, kurumsal işlemlerin çoğunu Internet üzerinden gerçekleştirmektedir. Kendisi ayrıca oturum açma bilgisi gerektiren çok sayıda popüler web sitesini de sık sık ziyaret etmektedir. Güvenlik bilinci yüksek biri olarak her hesapta aynı parolayı kullanmamaktadır. Bu satın alma temsilcisi, Web bağlantılarını farklı kullanıcı adları ve parolalarla eşleştirmek için Password Manager kullanmaya karar verdi. Oturum açmak için bir web sitesine gittiğinde, Password Manager kimlik bilgilerini otomatik olarak sunuyor. Kullanıcı adlarını ve parolaları görmek istediğinde, Password Manager'ı bunu yapacak şekilde ayarlayabiliyor.

Password Manager, kimlik doğrulamaları yönetmek ve düzenlemek için de kullanılabilir. Bu araç, kullanıcının bir Web veya ağ varlığı seçip bağlantıya doğrudan erişmesine olanak sağlar. Kullanıcı ayrıca gerektiğinde kullanıcı adlarını ve parolaları görüntüleyebilir.

Örnek 2: Çalışkanlığının karşılığını terfi alarak gören bir çalışanın şimdi bütün muhasebe bölümünü yönetmesi beklenmektedir. Ekibin, her biri farklı oturum açma bilgisine sahip çok sayıda istemci Web hesabında oturum açması gerekmektedir. Bu oturum açma bilgisinin diğer çalışanlarla paylaşılması gerektiğinden gizlilik sorun olmaktadır. Bu çalışan, bütün Web bağlantılarını, şirket kullanıcı adlarını ve parolalarını Password Manager içinde düzenlemeye karar verir. İşlemi tamamlayan çalışan Password Manager'ı ekip üyelerine dağıtır. Ekip üyeleri Web hesaplarında çalışabilecek ancak kullanmakta oldukları oturum açma kimlik bilgilerini asla bilmeyeceklerdir.

HP Drive Encryption (yalnızca belirli modellerde)

HP Drive Encryption bilgisayar sabit sürücüsünün tamamında veya ikincil sürücüde bulunan verilere erişimi kısıtlamak için kullanılır. Drive Encryption kendi kendini şifreleyen sürücüleri yönetmek için de kullanılabilir.

Örnek 1: Bir doktor, bilgisayarındaki sabit sürücüde yer alan bilgilere yalnızca kendisinin erişebilmesini sağlamak istemektedir. Doktor, önyükleme öncesi kimlik doğrulaması gerektiren Drive Encryption'ı etkinleştirir. Kurulum gerçekleştirildikten sonra, işletim sistemi başlamadan önce parola sunulmadan sabit sürücüye erişilemez. Doktor, kendi kendini şifreleyen sürücü seçeneğiyle verileri şifrelemeyi tercih ederek sürücü güvenliğini daha da geliştirebilir.

Örnek 2: Bir hastane yöneticisi, yerel bilgisayarlarındaki verilere kişisel parolalar paylaşılmadan yalnızca doktorlar ve yetkili personel tarafından erişilebilmesini istemektedir. IT bölümü, yöneticiyi, doktorları ve yetkili tüm personeli Drive Encryption kullanıcıları olarak ekler. Artık yalnızca yetkili personel, kendi kişisel kullanıcı adlarını ve parolalarını kullanarak bilgisayarı veya etki alanını başlatabilir.

HP Device Access Manager (yalnızca belirli modellerde)

HP Device Access Manager bir yöneticinin donanıma erişimi kısıtlamasına ve yönetmesine olanak tanır. Device Access Manager, veri kopyalaması yapılabilen USB flash sürücülere yetkisiz erişimi engellemek için kullanılabilir. Bu modül ayrıca CD/DVD sürücülerine, USB aygıtlarının denetimine, ağ bağlantılarına ve daha birçok işleve erişimi engellemede kullanılabilir. Şirket bilgisayarlarına erişmesi gereken ancak verileri USB sürücüye kopyalaması engellenmek istenen kurum dışı satıcılar iyi bir örnek olabilir.

Örnek 1: Bir medikal tedarik şirketinin müdürü çalışırken kendi şirket bilgileriyle birlikte sık sık kişisel tıbbi kayıtları da kullanmak durumundadır. Çalışanların bu verilere erişmesi gerekir, ancak verilerin USB sürücü veya başka tür harici bir depolama ortamıyla bilgisayardan alınmaması son derece önemlidir. Ağ güvenlidir, ancak bilgisayarlarda verilerin kopyalanmasına veya çalınmasına olanak sağlayan CD yazıcılar ve USB bağlantı noktaları bulunmaktadır. Müdür, USB bağlantı noktalarını ve CD yazıcıları devre dışı bırakıp kullanılmaz hale getirmek için Device Access Manager'ı kullanır. USB bağlantı noktaları engellenmekte, ancak fare ve klavyeler çalışmaya devam etmektedir.

Örnek 2: Bir sigorta şirketi, çalışanlarının evden kişisel yazılımlar veya veriler yüklemesini istememektedir. Bazı çalışanların bütün bilgisayarlardaki USB bağlantı noktalarına erişmesi gerekmektedir. IT müdürü, bazı çalışanlara erişim izni verirken diğerlerinin harici erişimini engellemek için Device Access Manager'ı kullanır.

Computrace (ayrıca satın alınır)

Computrace (ayrıca satın alınır) çalınan bir bilgisayarın yerini, kullanıcı Internet'e eriştiğinde izleyebilen bir hizmettir. Computrace bilgisayarları uzaktan yönetmeye ve konumlarını belirlemeye yardımcı olmanın yanı sıra bilgisayar kullanımını ve uygulamaları da izleyebilir.

Örnek 1: Bir okul müdürü, IT bölümüne talimat vererek okuldaki bütün bilgisayarların takip edilmesini istemiştir. IT yöneticisi, bilgisayarın envanterini aldıktan sonra bütün bilgisayarları Computrace'e kaydederek çalınmaları durumunda izlenebilmelerini sağlamıştır. Geçtiğimiz günlerde okul, çok sayıda bilgisayarın kayıp olduğunu fark etmiş, IT yöneticisi de gerekli mercilere ve Computrace yetkililerine durumu bildirmiştir. Bilgisayarın konumu tespit edilmiş ve yetkililer tüm bilgisayarları okula teslim etmiştir.

Örnek 2: Bir gayrimenkul danışmanlığı şirketi, dünya genelindeki bilgisayarını yönetmek ve güncelleştirmek istemektedir. Her bilgisayara bir IT personeli göndermelerine gerek kalmaksızın bilgisayarı izlemek ve güncelleştirmek için Computrace'i kullanırlar.

Önemli güvenlik hedeflerine ulaşma

HP Client Security modülleri birlikte çalıştırılarak çeşitli güvenlik sorunlarına çözüm sağlanabilir. Önemli güvenlik hedeflerinden bazıları şunlardır:

- Hedef gözeterek yapılan hırsızlığa karşı koruma sağlama
- Hassas verilere erişimi kısıtlama
- Kurum içi veya kurum dışı konumlardan yetkisiz erişimi önleme
- Güçlü parola ilkeleri oluşturma

Hedef gözeterek yapılan hırsızlığa karşı koruma sağlama

Hedef gözeterek yapılan hırsızlığa örnek olarak, gizli veriler ve müşteri bilgileri içeren, bir havaalanı güvenlik kontrolü noktasındaki bilgisayarın çalınması verilebilir. Aşağıdaki özellikler, hedef gözeterek yapılan hırsızlığa karşı koruma sağlamaya yardımcı olur:

- Etkinleştirilmiş ise, önyükleme öncesi kimlik doğrulaması özelliği işletim sistemine erişimi engellemeye yardımcı olur.
  - HP Client Security—Bkz. HP Client Security sayfa 12.
  - HP Drive Encryption—Bkz. HP Drive Encryption (yalnızca belirli modellerde) sayfa 30.
- Şifreleme, sabit sürücü çıkarılıp güvenli olmayan başka bir sisteme takılsa bile verilere erişilememesine yardımcı olur.
- Computrace, hırsızlık sonrasında bilgisayarın konumunu izleyebilir.
  - Computrace—Bkz. Theft Recovery (yalnızca belirli modellerde) sayfa 54.

Hassas verilere erişimi kısıtlama

Bir sözleşme denetçisinin sahada çalışmakta olduğunu ve hassas finansal verileri incelemesi için bilgisayara erişim izni verildiğini düşünün. Denetçinin dosyaları yazdırmasını veya CD gibi yazılabilir bir aygıta kaydetmesini istemiyorsunuz. Aşağıdaki özellik veriye erişimi kısıtlamanıza yardımcı olur:

- HP Device Access Manager, IT yöneticilerinin iletişim aygıtlarına erişimi kısıtlamasına olanak sağlar. Böylece hassas bilgiler sabit sürücüden kopyalanamaz. Bkz. Sistem görünümü sayfa 44.

Kurum içi veya kurum dışı konumlardan yetkisiz erişimi önleme

Güvenliği sağlanmamış bir iş bilgisayarına yetkisiz erişim, finansal hizmetlerden, bir yöneticiden veya Araştırma Geliştirme ekibinden gelen kurumsal ağ bilgileri ya da hasta kayıtları veya kişisel mali kayıtlar gibi özel bilgiler açısından son derece gerçek bir risktir. Aşağıdaki özellikler yetkisiz erişimin önlenmesine yardımcı olur:

- Etkinleştirilmiş ise, önyükleme öncesi kimlik doğrulaması özelliği işletim sistemine erişimi engellemeye yardımcı olur. (bkz. HP Drive Encryption (yalnızca belirli modellerde) sayfa 30.
- HP Client Security, yetkisiz bir kullanıcının parolalara veya parola korumalı uygulamalara erişimini önlemeye yardımcı olur. Bkz. HP Client Security sayfa 12.
- HP Device Access Manager, IT yöneticilerinin yazılabilir aygıtlara erişimi kısıtlamasına olanak sağlar. Böylece hassas bilgiler sabit sürücüden kopyalanamaz. Bkz. HP Device Access Manager (yalnızca belirli modellerde) sayfa 43.

Güçlü parola ilkeleri oluşturma

Düzinelerce Web tabanlı uygulamaya ve veri tabanlarına erişilirken güçlü parola kullanılmasını gerektiren bir şirket politikası uygulamaya konulduğunda, Password Manager, parolalar için korumalı bir havuzla birlikte Çoklu Oturum Açma kolaylığı sağlar. Bkz. Password Manager sayfa 18.

Ek güvenlik unsurları

Güvenlik rolleri atama

Bilgisayar güvenliği yönetilirken (özellikle büyük organizasyonlarda) önemli uygulamalardan biri de sorumluluk ve hakların farklı türdeki yöneticilere ve kullanıcılara bölüştürülmesidir.

NOT: Küçük bir organizasyonda ya da bireysel kullanımda, bu rollerin hepsi bir kişide toplanabilir.

HP Client Security açısından güvenlik yükümlülükleri ve ayrıcalıklar aşağıdaki rollere ayrılabilir:

- Güvenlik görevlisi—Şirket veya ağ için güvenlik düzeyini tanımlar ve kullanılacak güvenlik özelliklerini (Drive Encryption gibi) belirler.

  NOT: HP Client Security'deki özelliklerin çoğu, HP ile işbirliği halinde güvenlik görevlisi tarafından özelleştirilebilir. Daha fazla bilgi için, bkz. http://www.hp.com.

- IT yöneticisi—Güvenlik görevlisi tarafından tanımlanan güvenlik özelliklerini uygular ve yönetir. Ayrıca bazı özellikleri etkinleştirip devre dışı bırakabilir. Örneğin, güvenlik görevlisi akıllı kart kullanılmasına karar vermişse, IT yöneticisi hem parola hem de akıllı kart modunu etkinleştirebilir.
- Kullanıcı—Güvenlik özelliklerini kullanır. Örneğin, güvenlik görevlisi ve IT yöneticisi, sistem için akıllı kartı etkinleştirmişse, kullanıcı akıllı kart PIN'ini belirleyip kimlik doğrulaması için kartı kullanabilir.

DİKKAT: Yöneticilerin son kullanıcı ayrıcalıklarını ve kullanıcı erişimini kısıtlarken "en iyi uygulamalar"ı takip etmesi önerilir.

Yetkisiz kullanıcılara yönetici ayrıcalıkları verilmemelidir.

HP Client Security Manager parolalarını yönetme

HP Client Security özelliklerinin çoğu parola korumalıdır. Aşağıdaki tabloda yaygın olarak kullanılan parolalar, parolaların belirlendiği yazılım modülü ve parola işlevi listelenmiştir.

Ayrıca, bu tabloda yalnızca IT yöneticileri tarafından belirlenen ve kullanılan parolalar verilmiştir. Diğer tüm parolalar normal kullanıcılar veya yöneticiler tarafından belirlenebilir.

HP Client Security parolası	Şu modülde ayarlanır	İşlev
Windows oturum açma parolası	Windows Denetim Masası veya HP Client Security	HP Client Security'nin çeşitli özelliklerine erişimde kimlik doğrulamak ve el ile oturum açmak için kullanılabilir.
HP Client Security Yedekleme ve Kurtarma parolası	HP Client Security, bireysel kullanıcı tarafından	HP Client Security Yedekleme ve Kurtarma dosyasına erişimi korur.
Akıllı kart PIN'i	Credential Manager	Çok etmenli kimlik doğrulama olarak kullanılabilir. Windows kimlik doğrulaması olarak kullanılabilir. Akıllı kart seçilmişse, Drive Encryption kullanıcılarının kimliğini doğrular.

Güvenli bir parola oluşturma

Parola oluştururken, öncelikle program tarafından öngörülmüş belirtimlere uymalısınız. Ancak genel olarak, güçlü parolalar oluşturmanıza ve parolaların yetkisiz kişilerce çalınma olasılığını düşürmenize yardımcı olan aşağıdaki ilkeleri göz önünde bulundurun:

- 6 karakterden fazla, tercihen 8 karakter içeren parolalar kullanın.
- Parola boyunca karışık olarak büyük/küçük harfler kullanın.
- Mümkünse harflerle sayıları birlikte kullanın ve parolanıza özel karakterler ve noktalama işaretleri koyun.
- Anahtar bir sözcükteki harflerin yerine özel karakterler veya sayılar kullanın. Örneğin I veya L harfi için 1 rakamını kullanabilirsiniz.
- 2 veya daha fazla dilden sözcükleri birleştirin.
- Bir sözcük veya tümceyi ortasından sayılar veya özel karakterlerle ayırın; örn. "Mary2-2Cat45."
- Sözlüklerde karşılaşılabilecek bir ifadeyi parola olarak kullanmayın.
- Parola olarak adınızı veya diğer kişisel bilgileri (örn. doğum tarihinizi, evcil hayvanınızın adını veya annenizin kızlık soyadını) tersten yazmış olsanız bile kullanmayın.
- Parolalarınızı düzenli olarak değiştirin. Artırılabilir nitelikte sadece birkaç karakteri değiştirmeniz yeterlidir.
- Parolanızı bir yere yazdıysanız, bu bilgiyi bilgisayarınıza çok yakın ve herkesin rahatça görebileceği bir yere bırakmayın.
- Parolayı eposta gibi bilgisayarınızdaki bir dosyaya kaydetmeyin.
- Hesap paylaşımı yapmayın ve parolanızı kimseye söylemeyin.

Kimlik bilgilerini ve ayarları yedekleme

HP Client Security'deki Backup and Recovery (Yedekleme ve Kurtarma) aracını, yüklü HP Client Security modüllerinden bazılarındaki güvenlik kimlik bilgilerini yedeklemek ve geri yüklemek için merkezî bir konum olarak kullanabilirsiniz.

2 Başlarken

HP Client Security'yi kimlik bilgilerinizle kullanmak üzere yapılandırmak için HP Client Security'yi aşağıdaki yöntemlerden biriyle başlatın. Sihirbaz adımları bir kullanıcı tarafından tamamlandıktan sonra, aynı kullanıcı tarafından tekrar başlatılamaz.

1. Başlangıç veya Uygulamalar ekranından **HP Client Security** uygulamasını tıklatın veya üzerine dokunun (Windows 8).

   – veya –

   Windows Masaüstünden **HP Client Security Gadget**'ı tıklatın veya üzerine dokunun (Windows 7).

   – veya –

   Windows masaüstünde, görev çubuğunun en sağında, bildirim alanında yer alan **HP Client Security** simgesine çift tıklatın veya çift dokunun.

   – veya –

   Windows masaüstünde bildirim alanındaki **HP Client Security** simgesini tıklatın veya üzerine dokunun, ardından **Open HP Client Security** (HP Client Security'yi Aç) seçimini yapın.

2. HP Client Security Kurulum sihirbazı Hoş Geldiniz sayfası görüntülenerek başlatılır.

3. Hoş Geldiniz ekranını okuyun, Windows parolanızı girerek kimliğinizi doğrulayın ve **İleri** düğmesini tıklatın veya üzerine dokunun.

   Henüz bir Windows parolası oluşturmamış olmanız durumunda bir parola oluşturmanız istenir. Windows hesabınıza izinsiz kişilerin erişimini önlemek ve HP Client Security özelliklerini kullanabilmek için bir Windows parolasına ihtiyaç vardır.

4. HP SpareKey sayfasında üç güvenlik sorusu seçin. Her soru için bir yanıt girdikten sonra **İleri**'yi tıklatın. Soruları özel olarak kendiniz de yazabilirsiniz. Daha fazla bilgi için, bkz. HP SpareKey—Parola Kurtarma sayfa 13.

5. Parmak İzleri sayfasında, gereken minimum sayıda veya daha fazla parmak izi girin ve **İleri**'yi tıklatın veya üzerine dokunun. Daha fazla bilgi için, bkz. Parmak İzleri sayfa 12.

6. Drive Encryption sayfasında şifrelemeyi etkinleştirin, şifreleme anahtarını yedekleyin ve **İleri**'yi tıklatın veya üzerine dokunun. Daha fazla bilgi için bkz. HP Drive Encryption yazılımı Yardım bölümü.

   NOT: Bu durum, kullanıcının yönetici olduğu ve HP Client Security Kurulum sihirbazının daha önce bir yönetici tarafından yapılandırılmadığı bir senaryo için geçerlidir.

7. Sihirbazın son sayfasında **Son**'u tıklatın veya üzerine dokunun.

   Bu sayfa özelliklerin durumunu ve kimlik bilgilerini belirtir.

8. HP Client Security Kurulum sihirbazı Tam Zamanında Kimlik Doğrulama ve File Sanitizer özelliklerinin etkinleşmesini sağlar. Daha fazla bilgi için bkz. HP Device Access Manager yazılımı Yardım bölümü ve HP File Sanitizer yazılımı Yardım bölümü.

   NOT: Bu durum, kullanıcının yönetici olduğu ve HP Client Security Kurulum sihirbazının daha önce bir yönetici tarafından yapılandırılmadığı bir senaryo için geçerlidir.

HP Client Security'yi Açma

HP Client Security uygulamasını aşağıdaki yöntemlerden biriyle açabilirsiniz:

NOT: HP Client Security uygulaması başlatılmadan önce HP Client Security Kurulum Sihirbazı tamamlanmış olmalıdır.

- Başlangıç veya Uygulamalar ekranından **HP Client Security** uygulamasını tıklatın veya üzerine dokunun.

  – veya –

  Windows masaüstünde **HP Client Security Gadget**'ı tıklatın veya üzerine dokunun (Windows 7).

  – veya –

  Windows masaüstünde, görev çubuğunun en sağında, bildirim alanında yer alan **HP Client Security** simgesine çift tıklatın veya çift dokunun.

  – veya –

  Windows masaüstünde bildirim alanındaki **HP Client Security** simgesini tıklatın veya üzerine dokunun, ardından **Open HP Client Security** (HP Client Security'yi Aç) seçimini yapın.

3 Küçük Ölçekli İşletmeler İçin Kolay Kurulum Kılavuzu

Bu bölüm, Küçük Ölçekli İşletmeler için HP Client Security'de en sık kullanılan ve en faydalı seçenekleri etkinleştirmeye yönelik temel adımları tanıtmak amacıyla hazırlanmıştır. Bu yazılımda tercihlerinizi ve erişim denetiminizi detaylı olarak ayarlamanıza olanak sağlayan çok sayıda araç ve seçenek vardır. Bu Kolay Kurulum Kılavuzunun odak noktası, kuruluma mümkün olan en az çaba ve zamanı harcayarak her bir modülü işler hale getirmektir. Daha fazla bilgi almak için, ilgilendiğiniz modülü seçtikten sonra **?** işaretini veya sağ üst köşedeki Yardım düğmesini tıklatın. Bu düğme, o anda görüntülenmekte olan pencereyle ilgili size yardım etmek için otomatik olarak bilgi görüntüler.

Başlarken

1. Windows masaüstünde, görev çubuğunun en sağında, bildirim alanında yer alan **HP Client Security** simgesini çift tıklatarak HP Client Security'yi açın.
2. Windows parolanızı girin veya bir Windows parolası oluşturun.
3. HP Client Security Kurulumunu tamamlayın.

HP Client Security'yi yalnızca Windows oturum açılışında bir kez kimlik doğrulaması yapacak şekilde ayarlamak için, bkz. Güvenlik Özellikleri sayfa 26.

Password Manager

Herkes oldukça fazla sayıda parola kullanıyor; özellikle de oturum açmayı gerektiren web sitelerini veya uygulamaları düzenli olarak kullananlar. Normal bir kullanıcı ya her uygulama ve web sitesi için aynı parolayı kullanır ya da yaratıcı olur fakat çok geçmeden hangi parolanın hangi uygulamaya ait olduğunu unutur.

Password Manager parolalarınızı otomatik olarak hatırlar ya da size hangi sitelerin hatırlanacağını hangilerinin göz ardı edileceğini seçme imkanı verir. Bilgisayarınızda oturum açıldığında, Password Manager, uygulamalara veya web sitelerine girebilmek için gereken parolaları veya kimlik bilgilerini sağlar.

Kimlik bilgisi isteyen herhangi bir uygulama veya web sitesine eriştiğinizde, Password Manager uygulamayı veya siteyi otomatik olarak tanır ve yazılımın bilgilerinizi hatırlamasını isteyip istemediğinizi size sorar. Bazı sitelerin hatırlanmasını istemiyorsanız, soruya olumsuz yanıt verebilirsiniz.

Web konumlarını, kullanıcı adlarını ve parolaları kaydetmeye başlamak için:

1. Örnek olarak, katılımcı bir web sitesine veya uygulamaya gidin ve Web sayfasının sol üst köşesinde bulunan Password Manager simgesini tıklatarak web kimlik doğrulamasını ekleyin.
2. Bağlantıya bir ad verin (isteğe bağlı), sonra da kullanıcı adı ve parolayı Password Manager'a girin.
3. İşlemi tamamladığınızda, **Tamam** düğmesini tıklatın.
4. Password Manager ayrıca ağ paylaşımları veya eşlenmiş ağ sürücülerindeki kullanıcı adlarınızı ve parolalarınızı kaydedebilir.

Kaydedilen kimlik doğrulama bilgilerini Password Manager'da görüntüleme ve yönetme

Password Manager merkezî bir konumdan kimlik doğrulama bilgilerinizi görmenize, yönetmenize, yedeklemenize ve başlatmanıza olanak sağlar. Password Manager ayrıca Windows'tan kaydedilen sitelerin başlatılmasını da destekler.

Password Manager'ı açmak için, Ctrl+Windows tuşu+h tuş birleşimini kullanın ve sonra da kaydedilen kısayolları başlatmak ve kimlik doğrulamasını yapmak için **Oturum Aç**'ı tıklatın.

Password Manager'ın **Düzenle** seçeneği, ad, oturum açma adı ve hatta parolaları görüntülemenize ve değiştirmenize olanak sağlar.

Küçük Ölçekli İşletmeler için HP Client Security bütün kimlik bilgilerinin ve ayarların başka bir bilgisayara yedeklemesini ve/veya kopyalanmasını sağlar.

HP Device Access Manager

Device Access Manager, verilerinizin sabit sürücünüzde güven içinde kalması ve işletmenizin sınırlarını terk etmemesi için, çeşitli dahili ve harici depolama aygıtlarının kullanımını kısıtlamak için kullanılabilir. Örnek olarak bir kullanıcının verilerinize erişmesine izin verebilir ancak bu verileri CD'ye, kişisel müzik çalara veya USB bellek aygıtına kopyalamasını engelleyebilirsiniz.

1. **Device Access Manager**'ı açın (bkz. Device Access Manager'ı açma sayfa 43).

   Geçerli kullanıcının erişimi görüntülenir.

2. Kullanıcılar, gruplar veya aygıtlar için erişimi değiştirmek için, **Değiştir**'e tıklatın veya dokunun. Daha fazla bilgi için, bkz. Sistem görünümü sayfa 44.

HP Drive Encryption

HP Drive Encryption, tüm sabit sürücünün şifrelenmesi yoluyla verilerinizin korunmasında kullanılır. Sabit sürücünüzdeki veriler, bilgisayarınızın çalınması ve/veya sabit sürücünüzün orijinal bilgisayardan sökülüp başka bir bilgisayara takılması durumunda güvende kalır.

Ek bir güvenlik özelliği olarak Drive Encryption, işletim sistemi açılmadan önce kullanıcı adı ve parola kullanarak kimlik doğrulaması yapmanızı gerektirir. Bu işleme, önyükleme öncesi kimlik doğrulaması denir.

İşinizi kolaylaştırmak adına çok sayıdaki yazılım modülü, parolaları (Windows kullanıcı hesapları, kimlik doğrulama etki alanları, HP Drive Encryption, Password Manager ve HP Client Security dahil) otomatik olarak senkronize eder.

HP Drive Encryption'ı HP Client Security kurulum sihirbazıyla ilk kurulumda ayarlamak için, bkz. Başlarken sayfa 8.

4 HP Client Security

HP Client Security Ana sayfası, HP Client Security özellikleri, uygulamaları ve ayarlarına kolay erişim sağlayan merkez konumdur. Ana sayfa üç bölüme ayrılmıştır:

- **DATA** (VERİ)—Veri güvenliğini yönetmek için kullanılan uygulamalara erişim sağlar.
- **DEVICE** (AYGIT)—Aygıt güvenliğini yönetmek için kullanılan uygulamalara erişim sağlar.
- **IDENTITY** (KİMLİK)—Kimlik doğrulama bilgilerinin kaydını ve yönetimini sağlar.

Uygulama açıklamasını görmek için imleci bir uygulama başlığının üzerine getirin.

HP Client Security, sayfanın alt kısmında kullanıcı ve yönetici ayarlarına bağlantı verebilir. HP Client Security, **Dişli** (ayarlar) simgesinin tıklatılması veya üzerine dokunulmasıyla Gelişmiş Ayarlara ve özelliklere erişim sağlar.

Kimlik özellikleri, uygulamaları ve ayarları

HP Client Security'nin sunduğu Kimlik özellikleri, uygulamaları ve ayarları dijital kimliğinizin çeşitli yönlerinin yönetimi için size yardımcı olur. HP Client Security Ana sayfasında aşağıdaki başlıklardan birini tıklatın veya üzerine dokunun ve Windows parolanızı girin:

- **Parmak izleri**—Parmak izi kimlik bilgilerinizi kaydeder ve yönetir.
- **SpareKey**—Diğer kimlik bilgilerinin kaybedilmesi durumunda bilgisayarınızda oturum açmak için kullanabileceğiniz HP SpareKey kimlik bilgisini ayarlar ve yönetir. Ayrıca unuttuğunuz parolayı sıfırlamanıza imkan verir.
- **Windows Parolası**—Windows parolanızı değiştirmeniz için kolay erişim sağlar.
- **Bluetooth Aygıtları**—Bluetooth aygıtlarını kaydetme ve yönetme imkanı sunar.
- **Kartlar**—Akıllı kart, temassız kart ve yakın alan kartlarını kaydetme ve yönetme imkanı sunar.
- **PIN**—PIN kimlik bilgisini kaydetme ve yönetme imkanı sunar.
- **RSA SecurID**—RSA SecurID kimlik bilgilerinizi kaydetme ve yönetme imkanı sunar (uygun kurulum varsa).
- **Password Manager**—Çevrimiçi hesaplar ve uygulamalar için parolaların yönetilmesini sağlar.

Parmak İzleri

HP Client Security Kurulum Sihirbazı parmak izlerinin kurulum veya "kaydetme" işleminde sizi yönlendirir.

Parmak izlerinizi Parmak İzleri sayfasında da kaydedebilir veya silebilirsiniz. Bu sayfaya erişmek için HP Client Security Ana sayfasında **Parmak İzleri** simgesini tıklatın veya üzerine dokunun.

1. Parmak İzleri sayfasında, parmak izi başarıyla kaydedilene kadar parmaklarınızdan birini kaydırın.

   Kaydedilmesi gereken parmak sayısı sayfada belirtilmiştir. İşaret veya orta parmağın kullanılması daha uygundur.

2. Önceden kaydedilmiş parmak izlerini silmek için **Sil**'i tıklatın veya üzerine dokunun.

3. Başka parmakları da kaydetmek için **Enroll an additional fingerprint** (Bir parmak izi daha kaydet) seçeneğini tıklatın veya üzerine dokunun.

4. Sayfadan ayrılmadan önce **Kaydet**'i tıklatın veya üzerine dokunun.

⚠ **DİKKAT:** Parmak izlerini sihirbazla kaydederken parmak izi bilgileri **İleri** seçeneği tıklatılana veya üzerine dokunulana kadar kaydedilmez. Bilgisayarda bir süre etkinlik göstermezseniz veya programı kapatırsanız yaptığınız değişiklikler **kaydedilmez**.

▲ Yöneticilerin kayıt, doğruluk ve diğer ayarları belirtebileceği Parmak İzleri Yönetici Ayarları bölümüne erişmek için **Administrative Settings**'i (Yönetici Ayarları) tıklatın veya üzerine dokunun (yönetici ayrıcalıkları gerektirir).

▲ Parmak izi tanıma görünümünü ve davranışını kontrol eden ayarları belirleyebileceğiniz Parmak İzleri Kullanıcı Ayarları bölümüne gitmek için **User Settings** (Kullanıcı Ayarları) seçeneğini tıklatın veya üzerine dokunun.

Parmak İzleri Yönetici Ayarları

Yöneticiler parmak izi okuyucusu için kayıt, doğruluk ve diğer ayarları belirleyebilir. Yönetici ayrıcalıkları gerekir.

▲ Parmak izi kimlik bilgisine yönelik Yönetici Ayarlarına erişmek için Parmak İzleri sayfasında **Administrative Settings** (Yönetici Ayarları) seçeneğini tıklatın veya üzerine dokunun.

- **User enrollment** (Kullanıcı kaydı)—Kullanıcının kaydedebileceği minimum ve maksimum parmak izi sayısını seçin.
- **Recognition** (Tanıma)—Parmağınızı kaydırdığınızda parmak izi okuyucunun ne kadar hassasiyet uygulayacağını ayarlamak için kaydırıcı çubukta ayarlama yapın.

  Parmak iziniz sürekli olarak tanınmıyorsa daha düşük bir tanıma ayarı seçmeniz gerekebilir. Ayar yükseldikçe parmak izi kaydırma işleminde değişkenlik hassasiyeti artar böylece hatalı kabul ihtimali azalır. **Orta-Yüksek** ayarı, iyi bir güvenlik ve kullanım kolaylığı kombinasyonu sunar.

Parmak İzleri Kullanıcı Ayarları

Parmak İzleri Kullanıcı Ayarlarında, parmak izi tanıma görünümü ve davranışını kontrol eden ayarları belirleyebilirsiniz.

▲ Parmak izi kimlik bilgisine yönelik Kullanıcı Ayarlarına erişmek için Parmak İzleri sayfasında **User Settings** (Kullanıcı Ayarları) seçeneğini tıklatın veya üzerine dokunun.

- **Enable sound feedback** (Sesli yanıtı etkinleştir)—HP Client Security varsayılan olarak, parmağınızı kaydırdığınızda sesli yanıt verir. Bu ses program olaylarına göre farklılık gösterir. Windows Denetim Masası'ndaki Ses ayarında bulunan Sesler sekmesine giderek bu olaylara yeni sesler atayabilirsiniz. Sesli yanıtı devre dışı bırakmak isterseniz onay kutusundaki işareti kaldırın.
- **Show scan quality feedback** (Tarama kalitesi yanıtını göster)—Kalite dikkate alınmaksızın tüm parmak kaydırma işlemlerini görüntülemek için onay kutusunu işaretleyin. Sadece iyi kalitedeki parmak kaydırma işlemlerini görüntülemek için onay kutusundaki işareti kaldırın.

HP SpareKey—Parola Kurtarma

HP SpareKey, üç güvenlik sorusunu yanıtlayarak bilgisayarınıza erişim elde etmenizi sağlar (desteklenen platformlarda).

HP Client Security, Kurulum Sihirbazıyla yapılan ilk kurulum sırasında kişisel HP SpareKey kurulumunu yapmanız için sizi yönlendirir.

HP SpareKey kurulumunuzu yapmak için:

1. Sihirbazın HP SpareKey sayfasında üç güvenlik sorusu seçip her soru için bir yanıt girin.

   Soruları belirli soruların bulunduğu listeden seçebilir veya kendi sorularınızı yazabilirsiniz.

2. **Kaydet**'i tıklatın veya üzerine dokunun.

HP SpareKey'inizi silmek için:

▲ **Delete your SpareKey** (SpareKey'inizi Silin) seçeneğini tıklatın veya üzerine dokunun.

SpareKey'iniz kurulduktan sonra, açılış kimlik doğrulaması oturum açma ekranından veya Windows Karşılama ekranından SpareKey'inizi kullanarak bilgisayarınıza erişebilirsiniz.

HP Client Security Ana sayfasının Parola Kurtarma bölümünden erişebileceğiniz SpareKey sayfasında farklı sorular seçebilir veya yanıtlarınızı değiştirebilirsiniz.

Yöneticinin HP SpareKey kimlik bilgilerine ilişkin ayarları belirleyebileceği HP SpareKey Ayarları sayfasına erişmek için **Ayarlar**'ı tıklatın (yönetici ayrıcalıkları gerekir).

HP SpareKey Ayarları

HP SpareKey Ayarları sayfasında HP SpareKey kimlik bilgisinin davranışını ve kullanımını kontrol eden ayarları belirleyebilirsiniz.

▲ HP SpareKey Ayarları sayfasını başlatmak için HP SpareKey sayfasında **Ayarlar**'ı tıklatın veya üzerine dokunun (yönetici ayrıcalıkları gerektirir).

Yöneticiler şu ayarları seçebilirler:

- HP SpareKey kurulumu sırasında her kullanıcıya sorulacak soruları belirleme.
- Kullanıcılara sunulan listeye üç adete kadar özel güvenlik sorusu ekleme.
- Kullanıcılara kendi güvenlik sorularını yazma izni verme veya vermeme.
- Hangi kimlik doğrulama ortamlarının (Windows veya Açılış kimlik doğrulaması) parola kurtarma için HP SpareKey kullanımına izin verdiğini belirleme.

Windows parolası

HP Client Security, Windows parolasını değiştirme işleminin Windows Denetim Masası'ndan yapılan işleme kıyasla daha kolay ve hızlı gerçekleştirilmesini sağlar.

Windows parolanızı değiştirmek için:

1. HP Client Security Ana sayfasından **Windows Parolası**'nı tıklatın veya üzerine dokunun.
2. **Current Windows password** (Geçerli Windows parolası) metin kutusuna geçerli parolanızı girin.
3. **New Windows password** (Yeni Windows parolası) metin kutusuna yeni bir parola yazdıktan sonra **Confirm new password** (Yeni parolayı onaylayın) kutusuna parolayı tekrar girin.
4. Geçerli parolanızı girmiş olduğunuz yeni parolayla hemen değiştirmek için **Değiştir**'i tıklatın veya üzerine dokunun.

Bluetooth Aygıtları

Yönetici kimlik doğrulama bilgisi olarak Bluetooth'u etkinleştirmişse, ekstra güvenlik için diğer kimlik bilgilerine ek olarak bir Bluetooth telefonu ayarlayabilirsiniz.

NOT: Sadece Bluetooth telefon aygıtları desteklenir.

1. Bilgisayarda Bluetooth işlevinin etkin, Bluetooth telefonun da keşif modunda olduğundan emin olun. Telefonun bağlanması için Bluetooth aygıtında otomatik olarak oluşturulan bir kod girmeniz gerekebilir. Bluetooth aygıtı yapılandırma ayarlarına bağlı olarak bilgisayarla telefon arasında eşleştirme kodlarının karşılaştırılması gerekebilir.
2. Telefonu kaydetmek için seçin ve **Kaydet**'i tıklatın veya üzerine dokunun.

Yöneticinin Bluetooth aygıtlarına ilişkin ayarları belirleyebileceği Bluetooth Aygıtları Ayarları sayfa 15 sayfasına erişmek için **Ayarlar**'ı tıklatın (yönetici ayrıcalıkları gerekir).

Bluetooth Aygıtları Ayarları

Yöneticiler Bluetooth Aygıtı kimlik bilgilerinin davranışını ve kullanımını kontrol eden aşağıdaki ayarları belirleyebilirler:

Sessiz Kimlik Doğrulama

- **Automatically use your connected enrolled Bluetooth Device during verification of your identity** (Kimliğinizin doğrulanması sırasında bağlı durumdaki kayıtlı Bluetooth Aygıtını otomatik olarak kullan)—Kullanıcıların kimlik doğrulama için kullanıcı eylemine gerek kalmadan Bluetooth kimlik bilgilerini kullanmasına izin vermek için onay kutusunu işaretleyin veya bu seçeneği devre dışı bırakmak için onay kutusundaki işareti kaldırın.

Bluetooth Yakınlığı

- **Kayıtlı Bluetooth aygıtınız bilgisayarınızın kapsama alanından çıktığında bilgisayarı kilitleyin**—Oturum açma sırasında bağlanan bir Bluetooth Aygıtı kapsam dışına çıktığında bilgisayarı kilitlemek için onay kutusunu işaretleyin veya bu seçeneği devre dışı bırakmak için onay kutusundaki işareti kaldırın.

NOT: Bu özellikten faydalanılabilmesi için bilgisayarınızdaki Bluetooth modülü bu özelliği destekliyor olmalıdır.

Kartlar

HP Client Security farklı türdeki kimlik kartlarını destekleyebilir. Bu kartlar üzerlerinde bilgisayar çipi bulunan küçük plastik kartlardır. Akıllı kartlar, temassız karlar ve yakın alan kartları desteklenmektedir. Bu kartlardan biri ve uygun kart okuyucu bilgisayara bağlanmışsa, yönetici ilgili üreticinin kart okuma sürücüsünü yüklemişse ve kartı bir kimlik doğrulama bilgisi olarak etkinleştirmişse kartı kimlik doğrulama bilgisi olarak kullanabilirsiniz.

Akıllı kartlar için üretici, HP Client Security'nin güvenlik algoritmasında kullanacağı bir güvenlik sertifikası ve PIN yöneticisi temin etmelidir. PIN olarak kullanılan karakterlerin sayısı ve tipi farklılık gösterebilir. Akıllı kartın kullanılmadan önce bir yönetici tarafından geçerli hale getirilmesi gerekir.

HP Client Security aşağıdaki akıllı kart biçimlerini destekler:

- CSP
- PKCS11

HP Client Security aşağıdaki temassız kart tiplerini destekler:

- Temassız HID iCLASS bellek kartları
- Temassız MiFare Classic 1k, 4k ve mini bellek kartları

HP Client Security aşağıdaki yakın alan kartlarını destekler:

- HID Yakın Alan Kartları

Bir akıllı kartı kaydetmek için:

1. Kartı, aygıta bağlı akıllı kart okuyucuya takın.
2. Kart tanındığında kartın PIN'ini girin ve **Kaydet**'i tıklatın veya üzerine dokunun.

Bir akıllı kartın PIN'ini değiştirmek için:

1. Kartı, aygıta bağlı akıllı kart okuyucuya takın.
2. Kart tanındığında kartın PIN'ini girin ve **Authenticate**'i (Kimliği doğrula) tıklatın veya üzerine dokunun.
3. **Change PIN** (PIN'i Değiştirme) seçeneğini tıklatın veya üzerine dokunun ve yeni PIN'i girin.

Temassız kart veya yakın alan kartının kaydı:

1. Kartı uygun okuyucunun üzerine veya yakınına yerleştirin:
2. Kart tanındığında **Kaydet**'i tıklatın veya üzerine dokunun.

Kayıtlı bir kartı silmek için:

1. Kartı okuyucuya gösterin.
2. Akıllı kartlar söz konusu olduğunda ise karta ait PIN'i girip **Authenticate**'i (Kimliği doğrula) tıklatın veya üzerine dokunun.
3. **Sil**'i tıklatın veya üzerine dokunun.

Kart kaydedildikten sonra karta ilişkin bilgiler **Enrolled Cards** (Kayıtlı Kartlar) altında görüntülenir. Bir kart silindiğinde listeden de kaldırılır.

Yöneticilerin kartla kimlik doğrulamaya ilişkin ayarları belirleyebileceği Yakın Alan Kartı, Temassız Kart veya Akıllı Kart Ayarlarına erişmek için **Ayarlar**'ı tıklatın veya üzerine dokunun (yönetici ayrıcalıkları gerekir).

Yakın Alan Kartı, Temassız Kart ve Akıllı Kart Ayarları

Bir kartın ayarlarına erişmek için listedeki kartı tıklatın veya üzerine dokunun, ardından çıkan oku tıklatın veya üzerine dokunun.

Bir akıllı kartın PIN'ini değiştirmek için:

1. Kartı okuyucuya gösterin
2. Karta ait PIN'i girip **Devam**'ı tıklatın veya üzerine dokunun.
3. Yeni PIN'i girip doğrulayın ve **Devam**'ı tıklatın veya üzerine dokunun.

Bir akıllı kartın PIN'ini geçerli hale getirmek için:

1. Kartı okuyucuya gösterin
2. Karta ait PIN'i girip **Devam**'ı tıklatın veya üzerine dokunun.

3. Yeni PIN'i girip doğrulayın ve **Devam**'ı tıklatın veya üzerine dokunun.
4. Geçerliliği onaylamak için **Evet**'i tıklatın veya üzerine dokunun.

Kart verilerini silmek için:

1. Kartı okuyucuya gösterin
2. Karta ait PIN'i girin (Akıllı kart söz konusuysa) ve **Devam**'ı tıklatın veya üzerine dokunun.
3. Silme işlemini onaylamak için **Evet**'i tıklatın veya üzerine dokunun.

PIN

Yönetici kimlik doğrulama bilgisi olarak bir PIN'i etkinleştirmişse, ekstra güvenlik için diğer kimlik bilgilerine ek olarak bir PIN ayarlayabilirsiniz.

Yeni bir PIN ayarlamak için:

▲ PIN'i girin, onaylamak için tekrar girin ve **Uygula**'yı tıklatın veya üzerine dokunun.

Bir PIN'i silmek için

▲ **Sil**'i tıklatın veya üzerine dokunun ve onaylamak için **Evet**'i tıklatın veya üzerine dokunun.

Yöneticilerin PIN kimlik doğrulama bilgilerine ilişkin ayarları belirleyebileceği PIN Ayarlarına erişmek için **Ayarlar**'ı tıklatın veya üzerine dokunun (yönetici ayrıcalıkları gerekir).

PIN Settings (BIOS Ayarları)

PIN Ayarları sayfasında PIN kimlik bilgisi için minimum ve maksimum uzunluğu tanımlayabilirsiniz.

RSA SecurID

Yönetici kimlik doğrulama bilgisi olarak RSA'yı etkinleştirmişse ve aşağıdaki koşullar da geçerliyse bir RSA SecurID kimlik bilgisini kaydedebilir veya silebilirsiniz.

NOT: Uygun kurulum gereklidir.

- Kullanıcı bir RSA Sunucusunda oluşturulmuş olmalıdır.
- Kullanıcı ve bilgisayara atanan RSA SecurID belirteci, RSA Sunucusu etki alanıyla birleştirilmiş olmalıdır.
- SecurID yazılımı bilgisayarda kuruludur.
- Doğru şekilde yapılandırılmış RSA Sunucusuna bir bağlantı bulunmaktadır.

Bir RSA SecurID kimlik bilgisini kaydetmek için:

▲ RSA SecurID kullanıcı adı ve geçiş kodunuzu girin (ortamınıza bağlı olarak RSA SecurID Belirteç kodu veya PIN+Belirteç kodu) ve ardından **Uygula**'yı tıklatın veya üzerine dokunun.

Kayıt başarılıysa “Your RSA SecurID credential has been successfully enrolled” (RSA SecurID kimlik bilginiz başarıyla kaydedildi) mesajı gösterilir ve Sil düğmesi etkinleşir.

Bir RSA SecurID kimlik bilgisini silmek için:

▲ **Sil**'i tıklatın ve çıkan iletişim kutusundaki “Are you sure you want to delete your RSA SecurID credential?” (RSA SecurID kimlik bilginizi silmek istediğinizden emin misiniz?) sorusu için **Evet**'i seçin.

Password Manager

Password Manager'ı kullandığınızda web sitelerinde ve uygulamalarda oturum açmak çok daha kolay ve güvenlidir. Not almanızı veya hatırlamanızı gerektirmeyen, daha güçlü parolalar oluşturabilir ve bir parmak izi, akıllı kart, yakın alan kartı, temassız kart, Bluetooth telefon, PIN, RSA kimlik bilgisi veya Windows parolanız ile kolayca ve hızlıca oturum açabilirsiniz.

NOT: Web'de oturum açma ekranlarının yapısı sürekli değiştiği için Password Manager her zaman her web sitesini destekleyemeyebilir.

Password Manager aşağıdaki seçenekleri sunar:

Password Manager sayfası

- Bir web sayfasını veya uygulamayı otomatik olarak başlatmak ve oturum açmak için bir hesabı tıklatın veya üzerine dokunun.
- Hesaplarınızı düzenlemek için kategorilerden faydalanın.

Parola Gücü

- Parolalarınızdan herhangi birinin güvenlik riski taşıyıp taşımadığını bir bakışta görün.
- Oturum açma verilerini eklerken web siteleri ve uygulamalar için kullanılan parolaların gücünü kontrol edin.
- Parola gücü kırmızı, sarı veya yeşil durum göstergeleriyle belirtilir.

Password Manager simgesi bir web sayfası veya uygulama oturum açma ekranının sol üst köşesinde görüntülenir. Bir web sitesi veya uygulama için oturum açma hesabı oluşturulmamışsa simgenin üzerinde bir artı işareti bulunur.

▲ Aşağıdaki seçeneklerden birini seçebileceğiniz bağlam menüsünü görüntülemek için **Password Manager** simgesini tıklatın veya üzerine dokunun:

- Add [somedomain.com] to Password Manager ([biralanadi.com.tr]'yi Password Manager'a ekle)
- Open Password Manager (Password Manager'ı aç)
- Simge Ayarları
- Yardım

Henüz oturum açma hesabının oluşturulmadığı web sayfaları veya programlar içindir

Bağlam menüsünde aşağıdaki seçenekler görüntülenir:

- **Add [somedomain.com] to the Password Manager** ([biralanadi.com.tr]'yi Password Manager'a ekle)—Mevcut oturum açma ekranı için oturum açma hesabı ekleme imkanı verir.
- **Open Password Manager** (Password Manager'ı aç)—Password Manager'ı başlatır.
- **Icon Settings** (Simge Ayarları)—**Password Manager** simgesinin görüntülendiği koşulları belirlemenize imkan verir.
- **Yardım**—HP Client Security Yardımını görüntüler.

Oturum açma hesabının oluşturulduğu web sayfaları veya programlar içindir

Bağlam menüsünde aşağıdaki seçenekler görüntülenir:

- **Fill in logon data** (Oturum açma verilerini doldur)—**Verify your identity** (Kimliğinizi doğrulayın) sayfası görüntüler. Kimlik doğrulama başarılı olursa oturum açma verileriniz oturum açma alanlarına yerleştirilir ve sayfa gönderilir (oturum açma hesabı oluşturulurken sayfa gönderme işlemi belirlenmişse).
- **Edit Logon** (Oturum Açma Hesabını Düzenle)—Bu web sitesine ilişkin oturum açma verilerinizi düzenleme imkanı verir.
- **Add Logon** (Oturum Açma Hesabı Ekle)—Password Manager'a bir hesap ekleme imkanı verir.
- **Open Password Manager** (Password Manager'ı aç)—Password Manager'ı başlatır.
- **Yardım**—HP Client Security Yardımını görüntüler.

NOT: Bu bilgisayarın yöneticisi, HP Client Security'yi kimliğinizi doğrularken birden fazla kimlik bilgisi gerektirecek şekilde yapılandırmış olabilir.

Oturum açma hesabı ekleme

Oturum açma bilgilerini bir defa girerek bir web sitesi veya program için oturum açma hesabı ekleyebilirsiniz. Bundan sonra, Password Manager bilgileri sizin yerinize otomatik olarak girer. Bu oturum açma bilgilerini web sitesi veya programa gittikten sonra kullanabilirsiniz.

Bir oturum açma hesabı eklemek için:

1. Bir web sitesi veya programın oturum açma ekranını açın.
2. **Password Manager** simgesini tıklatın veya üzerine dokunun, ardından oturum açma ekranının web sitesi veya program için mi olduğuna bağlı olarak aşağıdakilerden birini tıklatın veya üzerine dokunun:
   - Bir web sitesi için **Add [domain name] to Password Manager** ([biralanadi.com.tr]'yi Password Manager'a ekle) seçimini tıklatın veya üzerine dokunun.
   - Bir program için **Add this logon screen to Password Manager** (Bu oturum açma ekranını Password Manager'a ekle) seçimini tıklatın veya üzerine dokunun.
3. Oturum açma verilerinizi girin. Ekrandaki oturum açma alanları ve iletişim kutusundaki ilgili alanlar koyu turuncu kenarlıkla belirlenir.
   a. Bir oturum açma alanını biçimlendirilmiş seçeneklerden biriyle doldurmak için alanın sağındaki okları tıklatın veya üzerlerine dokunun.
   b. Bu oturum açma hesabında kullanılan parolayı görüntülemek için **Show password** (Parolayı göster) öğesini tıklatın veya üzerine dokunun.
   c. Oturum açma alanlarının doldurulmasını fakat bilgilerin gönderilmemesini istiyorsanız **Automatically submit logon data** (Oturum açma verilerini otomatik olarak doldur) onay kutusunu işaretlemeyin.

d. Kullanmayı istediğiniz kimlik doğrulama yöntemini (parmak izi, akıllı kart, yakın alan kartı, temassız kart, Bluetooth telefon, PIN veya parola) seçmek için **Tamam**'ı tıklatın veya üzerine dokunun ve seçili kimlik doğrulama yöntemiyle oturum açın.

Oturum açma hesabının oluşturulduğunu belirtmek için **Password Manager** simgesinin üzerindeki artı işareti kaldırılır.

e. Password Manager oturum açma alanlarını algılamıyorsa **More fields** (Daha fazla alan) seçimini tıklatın veya üzerine dokunun.

- Oturum açma için gereken her alandaki onay kutusunu işaretleyin, oturum açma için gerekli olmayan alanlar içinse onay kutusundaki işareti kaldırın.
- **Kapat**'ı tıklatın veya üzerine dokunun.

Web sitesine her eriştiğinizde veya programı açtığınızda, web sitesi veya program oturum açma sayfasının sol üst köşesinde, oturum açmak için kayıtlı kimlik doğrulama bilgilerinizi kullanabileceğinizi belirten **Password Manager** simgesi görüntülenir.

Oturum açma hesaplarını düzenleme

Bir oturum açma hesabını düzenlemek için:

1. Bir web sitesi veya programın oturum açma ekranını açın.
2. Oturum açma bilgilerinizi düzenlemenizi sağlayacak iletişim kutusunu açmak için **Password Manager** simgesini tıklatın veya üzerine dokunun, ardından **Edit Logon** (Oturum Açma Hesabını Düzenle) seçeneğini tıklatın veya üzerine dokunun.

   Ekrandaki oturum açma alanları ve iletişim kutusundaki ilgili alanlar koyu turuncu kenarlıkla belirlenir.

   Hesap bilgilerini Password Manager sayfasında da düzenleyebilirsiniz. Bunun için, düzenleme seçeneklerini görüntülemek üzere oturum açma hesabının adını tıklatın veya üzerine dokunun ve **Düzenle**'yi seçin.
3. Oturum açma bilgilerinizi düzenleyin.
   - **Account name** (Hesap adı) bölümünü düzenlemek için alana yeni bir ad girin.
   - **Kategori** adı eklemek veya düzenlemek için **Kategori** alanına bir ad girin veya alandaki adı değiştirin.
   - Bir **Kullanıcı adı** oturum açma alanını biçimlendirilmiş seçeneklerden biriyle doldurmak için alanın sağındaki aşağı yönlü oku tıklatın veya üzerine dokunun.

     Biçimlendirilmiş seçenekler sadece, Password Manager simgesi bağlam menüsünde bulunan Düzenle komutu üzerinden oturum açma hesabı düzenlendiğinde kullanılabilir.
   - Bir **Parola** oturum açma alanını biçimlendirilmiş seçeneklerden biriyle doldurmak için, alanın sağındaki aşağı yönlü oku tıklatın veya üzerine dokunun.

     Biçimlendirilmiş seçenekler sadece, Password Manager simgesi bağlam menüsünde bulunan Düzenle komutu üzerinden oturum açma hesabı düzenlendiğinde kullanılabilir.
   - Ekranda bulunan diğer alanları da oturum açma hesabı kaydına eklemek için **More fields** (Daha fazla alan) seçeneğini tıklatın veya üzerine dokunun.
   - Bu oturum açma hesabında kullanılan parolayı görüntülemek için **Show password** (Parolayı göster) simgesini tıklatın veya üzerine dokunun.

- Oturum açma alanlarının doldurulmasını fakat bilgilerin gönderilmemesini istiyorsanız **Automatically submit logon data** (Oturum açma verilerini otomatik olarak doldur) onay kutusunu işaretlemeyin.
- Bu oturum açma hesabındaki parolanın güvenliğinin aşıldığını belirtmek için **This password is compromised** (Bu parolanın güvenliği aşıldı) onay kutusunu işaretleyin.

  Değişiklikler kaydedildikten sonra, aynı parolayı paylaşan tüm oturum açma hesapları da güvenliği aşılmış olarak işaretlenir. Bunun ardından, etkilenen tüm hesapları tek tek açıp parolayı gereken şekilde değiştirebilirsiniz.

4. **Tamam**'ı tıklatın veya üzerine dokunun.

Password Manager Hızlı Bağlantılar menüsünü kullanma

Password Manager, oturum açma hesaplarına bağlı web sitelerini ve programları başlatmak için hızlı ve kolay bir yol sunar. Oturum açma ekranını açmak için **Password Manager Quick Links** (Password Manager Hızlı Bağlantılar) menüsünde veya HP Client Security'de bulunan Password Manager sayfasında bir programı veya web sitesini çift tıklatın veya üzerine iki kere dokunun.

Bir oturum açma hesabı oluşturduğunuzda bu hesap otomatik olarak Password Manager **Quick Links** (Hızlı Bağlantılar) menüsüne eklenir.

Quick Links (Hızlı Bağlantılar) menüsünü görüntülemek için:

▲ **Password Manager** kısayol tuşu birleşimine basın (Fabrika ayarı Ctrl+Windows tuşu+h'dir). Kısayol tuş birleşimini değiştirmek için HP Client Security Ana sayfasında **Password Manager**'ı tıklatın, ardından **Ayarlar**'ı tıklatın veya üzerine dokunun.

Oturum açma hesaplarını kategorilere ayırma

Oturum açma hesaplarınızı düzenli tutmak için bir veya daha fazla kategori oluşturun.

Bir kategoriye bir oturum açma hesabını atamak için:

1. HP Client Security Ana sayfasından **Password Manager**'ı tıklatın veya üzerine dokunun.
2. Bir hesap girişini tıklatın veya üzerine dokunun, ardından **Düzenle**'yi tıklatın veya üzerine dokunun.
3. **Kategori** alanında yeni bir kategori adı girin.
4. **Save** (Kaydet) seçeneğine dokunun veya tıklatın.

Bir kategoriden bir hesabı silmek için:

1. HP Client Security Ana sayfasından **Password Manager**'ı tıklatın veya üzerine dokunun.
2. Bir hesap girişini tıklatın veya üzerine dokunun, ardından **Düzenle**'yi tıklatın veya üzerine dokunun.
3. **Kategori** alanında kategori adını silin.
4. **Save** (Kaydet) seçeneğine dokunun veya tıklatın.

Bir kategoriyi yeniden adlandırmak için:

1. HP Client Security Ana sayfasından **Password Manager**'ı tıklatın veya üzerine dokunun.
2. Bir hesap girişini tıklatın veya üzerine dokunun, ardından **Düzenle**'yi tıklatın veya üzerine dokunun.

3. **Kategori** alanında kategori adını değiştirin.
4. **Save** (Kaydet) seçeneğine dokunun veya tıklatın.

Oturum açma yönetimi

Password Manager, kullanıcı adları, parolalar için oturum açma bilgilerinizi ve birden fazla oturum açma hesabını tek bir merkezi konumdan yönetmenizi kolaylaştırır.

Oturum açmalarınız, Password Manager sayfasında listelenir.

Oturum açmalarınızı yönetmek için:

1. HP Client Security Ana sayfasından **Password Manager**'ı tıklatın veya üzerine dokunun.
2. Mevcut bir oturum açmaya tıklatın veya dokunun ve sonra aşağıdaki seçeneklerden birini seçerek ekrandaki yönergeleri izleyin:
   - **Edit** (Düzenle)—Bir oturum açmayı düzenle. Daha fazla bilgi için, bkz. Oturum açma hesaplarını düzenleme sayfa 20.
   - **Log in** (Oturum aç)—Seçilen hesapta oturum aç.
   - **Delete** (Sil)—Seçilen hesap için oturum açmayı sil.

Bir web sitesi veya program için ilave bir oturum açma eklemek için:

1. Web sitesi veya program için oturum açma ekranını açın.
2. **Password Manager** simgesini tıklatarak içerik menüsünü görüntüleyin.
3. **Add Logon** (Oturum Açma Ekle) simgesine dokunun veya tıklatın ve sonra ekrandaki yönergeleri izleyin.

Parola gücünüzün değerlendirilmesi

Web sitelerinde ve programlarda oturum açmak için güvenlik düzeyi şifreler kullanmak, kimliğinizi korumak açısından önem taşır.

Password Manager, web sitelerinizde veya programlarınızda oturum açmak için kullandığınız parolaların her birinin güvenlik düzeyinin anında ve otomatik bir analizini yaparak güvenliğinizi izlemenizi ve iyileştirmenizi kolaylaştırır.

Bir hesap için bir Password Manager oturum açması oluştururken parola girişi yaptığınızda, parolanın alt kısmında parolanın gücünü belirten renkli bir çubuk görünür. Renkler, şu değerleri belirtir:

- **Kırmızı**—Zayıf
- **Sarı**—Orta
- **Yeşil**—Güçlü

Password Manager simge ayarları

Password Manager, web siteleri ve programlar için oturum açma ekranlarını tanımlamaya çalışır. Password Manager bir oturum açma oluşturmadığınız bir oturum açma ekranı tespit ettiğinde,

Password Manager simgesini bir artı işaretiyle birlikte görüntülenerek sizden ekran için bir oturum açma eklemeniz istenir.

1. Bu simgeye dokunun veya tıklatın ve sonra, Password Manager'ın olası oturum açma sitelerini nasıl yöneteceğini özelleştirmek için **Icon Settings** (Simge Ayarları)'na dokunun veya tıklatın.

   - **Prompt to add logons for logon screens** (Oturum açma ekranları için oturum açmalar ekleme istemi)—Password Manager'ın bir oturum açma ayarı yapılmamış bir oturum açma ekranı görüntülendiğinde sizden bir oturum açma eklemenizi istemesi için bu seçeneğe dokunun veya tıklatın.
   - **Exclude this screen** (Bu ekranı hariç tut)—Bu onay kutusunu işaretlediğinizde, Password Manager bu oturum açma ekranı için sizden bir daha bir oturum açma eklemenizi istemez.
   - **Do not prompt to add logons for logon screens** (Oturum açma ekranları için oturum açmalar eklenmesini isteme)—Radyo düğmesini seçin.

2. Daha önce hariç tutulan bir ekran için bir oturum açma eklemek için:

   a. Önceden hariç tutulan web sitesinde oturum açın.

   b. Password Manager'ın bu sitenin parolasını hatırlaması için, parolaları kaydetmesi ve ekran için bir oturum açma oluşturması için açılan iletişim kutusundan **Hatırla**'ya dokunun veya tıklatın.

3. Diğer Password Manager ayarlarına erişmek için, Password Manager simgesine dokunun veya tıklatın ya da **Open Password Manager** (Password Manager'ı Aç) seçeneğine dokunun veya tıklatın ve sonra Password Manager sayfasındaki **Settings** (Ayarlar) seçeneğine dokunun veya tıklatın.

Oturum açmaları alma ve verme

HP Password Manager Alma ve Verme sayfasından, bilgisayarınızdaki web tarayıcılarınızda kayıtlı olan oturum açmaları alabilirsiniz. Bir HP Client Security yedekleme dosyasından verileri almak ve bir HP Client Security yedekleme dosyasına verileri vermek de mümkündür.

▲ Alma ve verme sayfasını açmak için, Password Manager sayfasındaki **Import and export** (Al ve Ver) seçeneğine dokunun veya tıklatın.

Bir tarayıcıdaki parolaları almak için:

1. Kayıtlı parolalarını almak istediğiniz tarayıcıya dokunun veya tıklatın (sadece kurulu tarayıcılar görüntülenir).
2. Parolalarını almak istemediğiniz hesapların onay kutusundaki işareti kaldırın.
3. **Al** seçeneğine dokunun veya tıklatın.

Bir HP Client Security yedekleme dosyasından veriler almak ya da bir HP Client Security yedekleme dosyasına veriler vermek, Al ve ver sayfasında bulunan ilişkilendirilmiş bağlantılar aracılığıyla gerçekleştirilir (**Other Options** (Diğer Seçenekler) altında).

NOT: Bu özellik, sadece Password Manager verilerinin alınması ve verilmesi işlemleri içindir. Ek HP Client Security verilerinin yedeklenmesi ve geri yüklenmesi hakkında bilgi almak için bkz. Verilerinizi yedeklemek ve geri yüklemek sayfa 28.

Bir HP Client Security yedekleme dosyasından verilerin alınması:

1. HP Password Manager Al ve Ver sayfasından, **Import data from an HP Client Security backup file** (Bir HP Client Security yedekleme dosyasından veri al) üzerine dokunun veya tıklatın.
2. Kimliğinizi doğrulayın.
3. Daha önce oluşturulmuş olan bir yedekleme dosyasını seçin ya da verilen alana bir yol girin, sonra **Browse** (Araştır) seçeneğine dokunun veya tıklatın.
4. Dosyayı korumak için kullandığınız parolayı girin ve sonra **Next** (İleri) seçeneğine dokunun veya tıklatın.
5. **Restore** (Geri Yükle) öğesine dokunun veya tıklatın.

Bir HP Client Security yedekleme dosyasına verilerin verilmesi:

1. HP Password Manager Al ve Ver sayfasından, **Export data from an HP Client Security backup file** (Bir HP Client Security yedekleme dosyasına veri ver) üzerine dokunun veya tıklatın.
2. Kimliğinizi doğrulayın ve sonra **Next** (İleri) öğesine dokunun veya tıklatın.
3. Yedekleme dosyası için bir isim girin. Dosya, varsayılan olarak Belgelerim klasörünüze kaydedilir. Farklı bir konum belirlemek için **Browse** (Araştır) öğesine dokunun veya tıklatın.
4. Dosyayı korumak için bir parola girip onaylayın ve sonra **Save** (Kaydet) öğesine dokunun veya tıklatın.

Ayarlar

Password Manager'ı kişiselleştirmek için ayarlar yapabilirsiniz:

- **Prompt to add logons for logon screens** (Oturum açma ekranları için oturum açmalar ekleme istemi)—Bir web sitesi ya da program oturum açması tespit edildiğinde, bir artı simgesiyle birlikte **Password Manager** görüntülenir, böylece **Logons** (Oturum açmalar) menüsüne bu ekran için bir oturum açma ekleyebilirsiniz.

  Bu özelliği devre dışı bırakmak için, **Prompt to add logons for logon screens** (Oturum açma ekranları için oturum açmalar ekleme istemi) kutusundaki onayı kaldırın.

- **Open Password Manager with Ctrl+Win+h** (Ctrl+Win+h ile Password Manager'ı aç)—**Password Manager Quick Links** (Password Manager Hızlı Bağlantılar) menüsünü açan varsayılan kısayol tuş birleşimi Ctrl+Windows tuşu+h'dir.

  Bu kısayol tuşunu değiştirmek için bu seçeneğe dokunun veya tıklatın ve sonra yeni bir tuş birleşimi girin. Birleşimler, şunlardan bir veya birkaç tanesini içerebilir: ctrl, alt veya shift ve herhangi bir harf veya sayı tuşu.

  Windows veya Windows uygulamaları için ayrılmış birleşimler kullanılamaz.

- Ayarları varsayılan fabrika değerlerine döndürmek için **Restore defaults** (Varsayılanları geri yükle) seçeneğine dokunun veya tıklatın.

Gelişmiş Ayarlar

Yöneticiler, HP Client Security Ana sayfasından **Dişli** (ayarlar) simgesini seçerek şu seçeneklere ulaşabilir.

- **Administrator Policies** (Yönetici İlkeleri)—Yöneticiler için oturum açma ve oturum ilkelerini yapılandırmanızı sağlar.
- **Standard User Policies** (Standart Kullanıcı İlkeleri)—Standart kullanıcılar için oturum açma ve oturum ilkelerini yapılandırmanızı sağlar.
- **Security Features** (Güvenlik Özellikleri)—Güçlü kimlik doğrulama kullanarak ve/veya Windows başlatmasında kimlik doğrulamayı etkinleştirerek Windows hesabınızı korumak suretiyle bilgisayarınızın güvenliğini artırmanıza olanak tanır.
- **Users** (Kullanıcılar)—Kullanıcıları ve kullanıcıların kimlik bilgilerini yönetmenizi sağlar.
- **My Policies** (İlkelerim)—Kimlik doğrulama ilkelerinizi ve kayıt durumunuzu incelemenizi sağlar.
- **Backup and Restore** (Yedekleme ve Geri Yükleme)—HP Client Security verilerinizi yedeklemenizi veya geri yüklemenizi sağlar.
- **About HP Client Security** (HP Client Security Hakkında)—HP Client Security sürüm bilgilerini görüntüler.

Yönetici İlkeleri

Bu bilgisayarın yöneticileri için oturum açma ve oturum ilkelerini yapılandırabilirsiniz. Burada belirlenen oturum açma ilkeleri, bir yerel yöneticinin Windows'ta oturum açması için gereken kimlik bilgilerini yönetir. Burada belirlenen oturum ilkeleri, bir yerel yöneticinin bir Windows oturumu içinde kimlik doğrulaması yapması için gereken kimlik bilgilerini yönetir.

Varsayılan olarak, tüm yeni veya değiştirilmiş ilkeler **Apply** (Uygula) seçeneğine dokunulduktan ya da tıklatıldıktan hemen sonra uygulanır.

Yeni bir ilke eklemek için:

1. HP Client Security Ana sayfasından **Dişli** simgesine dokunun veya tıklatın.
2. Advanced Settings (Gelişmiş Ayarlar) sayfasından **Administrator Policies** (Yönetici İlkeleri) seçeneğine dokunun veya tıklatın.
3. **Add new policy** (Yeni ilke ekle) seçeneğine dokunun veya tıklatın.
4. Yeni ilke için birincil ve ikincil (opsiyonel) kimlik bilgilerini seçmek için aşağı okları tıklatın ve sonra **Add** (Ekle) seçeneğine dokunun veya tıklatın.
5. **Apply** (Uygula) seçeneğini tıklatın.

Yeni veya değiştirilmiş bir ilkenin uygulanmasını geciktirmek için:

1. **Enforce this policy immediately** (Bu ilkeyi hemen uygula) seçeneğine dokunun veya tıklatın.
2. **Enforce this policy on the specific date** (Bu ilkeyi belirli bir tarihte uygula) öğesini seçin.
3. Bu ilkenin ne zaman uygulanacağını seçmek için bir tarih girin ya da açılan takvimi kullanın.
4. Kullanıcılara yeni ilke hakkında ne zaman hatırlatma yapılacağını da eğer isterseniz seçebilirsiniz.
5. **Apply** (Uygula) seçeneğini tıklatın.

Standart Kullanıcı İlkeleri

Bu bilgisayarın standart kullanıcıları için oturum açma ve oturum ilkelerini yapılandırabilirsiniz. Burada belirlenen oturum açma ilkeleri, bir standart kullanıcının Windows'ta oturum açması için gereken kimlik bilgilerini yönetir. Burada belirlenen oturum ilkeleri, bir standart kullanıcının bir Windows oturumu içinde kimlik doğrulaması yapması için gereken kimlik bilgilerini yönetir.

Varsayılan olarak, tüm yeni veya değiştirilmiş ilkeler **Apply** (Uygula) seçeneğine dokunulduktan ya da tıklatıldıktan hemen sonra uygulanır.

Yeni bir ilke eklemek için:

1. HP Client Security Ana sayfasından **Dişli** simgesine dokunun veya tıklatın.
2. Advanced Settings (Gelişmiş Ayarlar) sayfasından **Standard User Policies** (Standart Kullanıcı İlkeleri) seçeneğine dokunun veya tıklatın.
3. **Add new policy** (Yeni ilke ekle) seçeneğine dokunun veya tıklatın.
4. Yeni ilke için birincil ve ikincil (opsiyonel) kimlik bilgilerini seçmek için aşağı okları tıklatın ve sonra **Add** (Ekle) seçeneğine dokunun veya tıklatın.
5. **Apply** (Uygula) seçeneğini tıklatın.

Yeni veya değiştirilmiş bir ilkenin uygulanmasını geciktirmek için:

1. **Enforce this policy immediately** (Bu ilkeyi hemen uygula) seçeneğine dokunun veya tıklatın.
2. **Enforce this policy on the specific date** (Bu ilkeyi belirli bir tarihte uygula) öğesini seçin.
3. Bu ilkenin ne zaman uygulanacağını seçmek için bir tarih girin ya da açılan takvimi kullanın.
4. Kullanıcılara yeni ilke hakkında ne zaman hatırlatma yapılacağını da eğer isterseniz seçebilirsiniz.
5. **Apply** (Uygula) seçeneğini tıklatın.

Güvenlik Özellikleri

Bu bilgisayarın izinsiz erişime karşı korumasına yardımcı olan HP Client Security Özelliklerini etkinleştirebilirsiniz.

Güvenlik özelliklerini ayarlamak için:

1. HP Client Security Ana sayfasından **Dişli** simgesine dokunun veya tıklatın.
2. Advanced Settings (Gelişmiş Ayarlar) sayfasından **Security Features** (Güvenlik Özellikleri) seçeneğine dokunun veya tıklatın.

3. Güvenlik özelliklerini etkinleştirmek için onay kutularını işaretledikten sonra **Apply** (Uygula) öğesine dokunun veya tıklatın. Ne kadar fazla özelliği seçerseniz, bilgisayarınız o kadar güvenli olur.

   Bu ayarlar tüm kullanıcılar için geçerli olacaktır.

   - **Windows Logon Security** (Windows Oturum Açma Güvenliği)—Windows hesaplarınızı, erişim için HP Client Security kimlik bilgilerinin kullanımı gerekli kılarak korur.
   - **Pre-Boot Security (Power-on authentication)** (Önyükleme öncesi güvenliği (Açılış kimlik doğrulaması))—Windows başlamadan önce bilgisayarınızı korur. Bu seçim, eğer BIOS desteklemiyorsa kullanılamaz.
   - **Allow One Step logon** (Tek adımlı oturum açmaya izin ver)—Bu ayar, eğer kimlik doğrulama işlemi Açılış kimlik doğrulaması ya da Drive Encryption seviyesinde gerçekleştirilmişse, Windows oturum açmasının atlanmasına izin verir.

4. **Users** (Kullanıcılar) öğesine dokunun veya tıklatın ve sonra kullanıcının kutucuğuna dokunun veya tıklatın.

Kullanıcılar

Bu bilgisayarın HP Client Security kullanıcılarını izleyebilir ve yönetebilirsiniz.

HP Client Security'e başka bir Windows kullanıcısı eklemek için:

1. HP Client Security Ana sayfasından **Dişli** simgesine dokunun veya tıklatın.
2. Advanced Settings (Gelişmiş Ayarlar) sayfasından **Users** (Kullanıcılar) seçeneğine dokunun veya tıklatın.
3. **Add another Windows user to HP Client Security** (HP Client Security'e başka bir Windows kullanıcısı ekle) seçeneğine dokunun veya tıklatın.
4. Eklemek istediğiniz kullanıcının adını girin ve **OK** (Tamam) seçeneğine dokunun veya tıklatın.
5. Kullanıcının Windows parolasını girin.

   Kullanıcı sayfasında, eklenen kullanıcı için bir kutucuk görüntülenir.

HP Client Security'den bir Windows kullanıcısını silmek için:

1. HP Client Security Ana sayfasından **Dişli** simgesine dokunun veya tıklatın.
2. Advanced Settings (Gelişmiş Ayarlar) sayfasından **Users** (Kullanıcılar) seçeneğine dokunun veya tıklatın.
3. Silmek istediğiniz kullanıcının ismine dokunun veya tıklatın.
4. **Delete User** (Kullanıcı Sil) öğesine dokunun veya tıklatın ve sonra **Yes** (Evet) ile onaylayın.

Bir kullanıcı için yürürlükte olan oturum açma ve oturum ilkelerinin bir özetini görüntülemek için:

▲ **Users** (Kullanıcılar) öğesine dokunun veya tıklatın ve sonra kullanıcının kutucuğuna dokunun veya tıklatın.

İlkelerim

Kimlik doğrulama ilkelerini ve kayıt durumunu görüntüleyebilirsiniz. User Policies (İlkelerim) sayfasında, Administrators Policies (Yönetici İlkeleri) ve Standard User Policies (Standart Kullanıcı İlkeleri) sayfalarına bağlantılar da bulunur.

1. HP Client Security Ana sayfasından **Dişli** simgesine dokunun veya tıklatın.
2. Advanced Settings (Gelişmiş Ayarlar) sayfasından **My Policies** (İlkelerim) seçeneğine dokunun veya tıklatın.

   O anda oturum açmış olan kullanıcı için oturum açma ve oturum ilkeleri görüntülenir.

My Policies (İlkelerim) sayfası ayrıca Yönetici İlkeleri sayfa 25 ve Standart Kullanıcı İlkeleri sayfa 26 için bağlantılar sunar.

Verilerinizi yedeklemek ve geri yüklemek

HP Client Security verilerinizi düzenli olarak yedeklemeniz önerilir. Yedeklemeyi ne sıklıkta yapacağınız, verilerin ne sıklıkta değiştiğine bağlıdır. Örneğin, günlük olarak yeni oturum açmalar ekliyorsanız, verilerinizi günlük olarak yedeklemeniz gerekir.

Yedeklemeler bir bilgisayardan başka bir bilgisayara aktarılabilir, buna alma ve verme denir.

NOT: Bu özellikle sadece Password Manager (Parola Yöneticisi) yedeklenir. Drive Encryption, bağımsız bir yedekleme yöntemidir. Device Access Manager (Aygıt Erişim Yöneticisi) ve parmak iziyle kimlik doğrulama bilgileri yedeklenmez.

Verilerin yedekleme dosyasından geri yüklenebilmesi için, yedeklenen verileri alacak bilgisayara HP Client Security önceden yüklenmiş olmalıdır.

Verilerinizi yedeklemek için:

1. HP Client Security Ana sayfasından **Dişli** simgesine dokunun veya tıklatın.
2. Advanced Settings (Gelişmiş Ayarlar) sayfasından **Administrator Policies** (Yönetici İlkeleri) seçeneğine dokunun veya tıklatın.
3. **Backup and Restore** (Yedekle ve Geri Yükle) öğesine dokunun veya tıklatın.
4. **Backup** (Yedekle) seçeneğine dokunun veya tıklatın ve kimliğini doğrulayın.
5. Yedeklemeye dahil edilmesini istediğiniz modülü seçin ve sonra **Next** (İleri) seçeneğine dokunun veya tıklatın.
6. Depolama dosyası için bir isim girin. Dosya, varsayılan olarak Belgelerim klasörünüze kaydedilir. Farklı bir konum belirlemek için **Browse** (Araştır) öğesine dokunun veya tıklatın.
7. Dosyayı korumak için bir parola girin ve onaylayın.
8. **Save** (Kaydet) seçeneğine dokunun veya tıklatın.

Verilerinizi geri yüklemek için:

1. HP Client Security Ana sayfasından **Dişli** simgesine dokunun veya tıklatın.
2. Advanced Settings (Gelişmiş Ayarlar) sayfasından **Administrator Policies** (Yönetici İlkeleri) seçeneğine dokunun veya tıklatın.
3. **Backup and Restore** (Yedekle ve Geri Yükle) öğesine dokunun veya tıklatın.
4. **Restore** (Geri Yükle) öğesini seçin ve kimliğini doğrulayın.
5. Daha önce oluşturulmuş olan depolama dosyasını seçin. Verilen alana yol girişini yapın. Farklı bir konum belirlemek için **Browse** (Araştır) öğesine dokunun veya tıklatın.
6. Dosyayı korumak için kullandığınız parolayı girin ve sonra **Next** (İleri) seçeneğine dokunun veya tıklatın.

7. Veri geri yüklemesi yapmak istediğiniz modülleri seçin.
8. **Restore** (Geri Yükle) öğesine dokunun veya tıklatın.

5 HP Drive Encryption (yalnızca belirli modellerde)

HP Drive Encryption, bilgisayarınızın verilerini şifreleyerek tam veri koruması sağlar. Drive Encryption etkinleştirildiğinde, Windows® işletim sistemi başlamadan önce görüntülenen Drive Encryption oturum açma penceresinde oturum açmanız gerekir.

HP Client Security Giriş Ekranı, Windows yöneticilerinin Drive Encryption'ı etkinleştirmesine, şifreleme anahtarını yedeklemesine ve sürücüler ve bölümleri şifreleme için seçmesine veya seçimlerini kaldırmasına olanak sağlamaktadır. Daha fazla bilgi için, HP Client Security yazılım yardımına bakın.

Aşağıdaki görevler, Drive Encryption ile gerçekleştirilebilir:

- Drive Encryption ayarlarının seçilmesi:
  - Yazılım şifrelemesi kullanarak farklı sürücü veya bölümlerin şifrelenmesi veya şifrelerinin çözülmesi
  - Donanım şifrelemesi kullanarak farklı kendi kendini şifreleyen sürücülerin şifrelenmesi veya şifrelerinin çözülmesi
  - Drive Encryption önyükleme kimlik doğrulamasının her zaman gerekli olmasını sağlamak için Uyku veya Beklemeyi devre dışı bırakarak ek güvenlik ekleme

NOT: Yalnızca dâhili SATA ve harici eSATA sabit sürücüleri şifrelenebilir.

- Yedekleme anahtarları oluşturma
- Yedekleme anahtarları ve HP SpareKey kullanarak şifrelenmiş bir bilgisayara erişimi kurtarma
- Bir parola, kayıtlı parmak dizi veya belirli akıllı kartlar için PIN kullanarak Drive Encryption önyükleme kimlik doğrulamasını etkinleştirme

Drive Encryption'ı açma

Yöneticiler, HP Client Security'yi açarak Drive Encryption'a erişebilir.

1. Başlat ekranından **HP Client Security** uygulamasına (Windows 8) tıklayın ya da dokunun.

   – veya –

   Windows masaüstünde, görev çubuğunun en sağında, bildirim alanında yer alan **HP Client Security** simgesine çift tıklatın veya çift dokunun.

2. **Drive Encryption** simgesine tıklayın veya dokunun.

Genel görevler

Standart sabit sürücüler için Drive Encryption'ı etkinleştirme

Standart sabit sürücüler, yazılım şifrelemesi kullanılarak şifrelenmektedir. Bir sürücüyü veya bir disk bölümünü şifrelemek için bu adımları izleyin:

1. **Drive Encryption**'ı başlatın. Daha fazla bilgi için, bkz. Drive Encryption'ı açma sayfa 30.
2. Şifrelemek istediğiniz sürücü veya bölümün onay kutusunu seçin ve ardından **Backup Key** (Anahtarı Yedekle) seçeneğine tıklayın veya dokunun.

NOT: Daha fazla güvenlik için, **Disable sleep mode for increased security** (Daha fazla güvenlik için uyku modunu devre dışı bırak) onay kutusunu seçin. Uyku modunu devre dışı bıraktığınızda, sürücünün kilidini kaldırmak için kullanılan kimlik bilgilerinin bellekte saklanma riski kesinlikle yoktur.

3. Yedekleme seçeneklerinden birini veya birden fazlasını seçin ve ardından **Backup** (Yedekle) seçeneğine tıklayın veya dokunun. Daha fazla bilgi için, bkz. Şifreleme anahtarlarını yedekleme sayfa 34.
4. Şifreleme anahtarı yedeklenirken çalışmaya devam edebilirsiniz. Bilgisayarınızı yeniden başlatmayın.

NOT: Bilgisayarınızı yeniden başlatmanız sizden istenir. Yeniden başlatma sonrasında, sürücü şifreleme önyükleme ekranı görüntülenir ve Windows'un başlaması öncesinde kimlik doğrulama ister.

Drive Encryption etkinleştirilmiştir. Seçilen sürücü bölümlerinin şifrelenmesi, bölümlerin sayısı ve boyutuna bağlı olarak birkaç saat sürebilmektedir.

Daha fazla bilgi için, HP Client Security yazılım yardımına bakın.

Kendi kendini şifreleyen sürücüler için Drive Encryption'ı etkinleştirme

Trusted Computing Group'un kendi kendini şifreleyen sürücü yönetimi konulu OPAL belirtimlerini karşılayan kendi kendini şifreleyen sürücüler, ya yazılım şifrelemesi ya da donanım şifrelemesi kullanılarak şifrelenebilir. Donanım şifrelemesi, yazılım şifrelemesinden çok daha hızlıdır. Ancak, hangi disk bölümlerinin şifreleneceğini seçemezsiniz. Her türlü disk bölümü de dâhil olmak üzere, diskin tamamı şifrelenmektedir.

Spesifik bölümleri şifrelemek için, yazılım şifrelemesi kullanmanız gerekir. **Only allow hardware encryption for Self-Encrypting Drives (SEDs)** (Kendi Kendini Şifreleyen Sürücüler (SED) için yalnızca donanım şifrelemesine izin ver) onay kutusunu temizlediğinizden emin olun.

Kendi kendini şifreleyen sürücüler için Drive Encryption'ı etkinleştirmeden önce bu adımları izleyin:

1. **Drive Encryption**'ı başlatın. Daha fazla bilgi için, bkz. Drive Encryption'ı açma sayfa 30.
2. Şifrelemek istediğiniz sürücünün onay kutusunu seçin ve ardından **Backup Key** (Anahtarı Yedekle) seçeneğine tıklayın veya dokunun.

NOT: Daha fazla güvenlik için, **Disable Sleep Mode for added security** (Daha fazla güvenlik için Uyku Modunu devre dışı bırak) onay kutusunu seçin. Uyku modunu devre dışı bıraktığınızda, sürücünün kilidini kaldırmak için kullanılan kimlik bilgilerinin bellekte saklanma riski kesinlikle yoktur.

3. Yedekleme seçeneklerinden birini veya birden fazlasını seçin ve ardından **Backup** (Yedekle) seçeneğine tıklayın veya dokunun. Daha fazla bilgi için, bkz. Şifreleme anahtarlarını yedekleme sayfa 34.

4. Şifreleme anahtarı yedeklenirken çalışmaya devam edebilirsiniz. Bilgisayarınızı yeniden başlatmayın.

NOT: Kendi kendini şifreleyen sürücüler için, bilgisayarı kapatmanız istenir.

Daha fazla bilgi için, HP Client Security yazılım yardımına bakın.

Drive Encryption'ı devre dışı bırakma

1. **Drive Encryption**'ı başlatın. Daha fazla bilgi için, bkz. Drive Encryption'ı açma sayfa 30.

2. Tüm şifrelenen sürücüler için onay kutusunu temizleyin ve ardından **Apply** (Uygula) seçeneğine tıklayın veya dokunun.

   Drive Encryption'ı devre dışı bırakma başlar.

NOT: Yazılım şifrelemesi kullanılmışsa, şifre çözme başlar. Şifrelenmiş sabit sürücü bölümlerinin boyutuna bağlı olarak, birkaç saat sürebilir. Şifreleme tamamlandığında, Drive Encryption devre dışı bırakılmaktadır.

Donanım şifrelemesi kullanılmışsa, sürücünün şifresi hemen çözülmekte ve birkaç dakika sonra Drive Encryption devre dışı bırakılmaktadır.

Drive Encryption devre dışı bırakılınca, sizden donanım şifresi varsa bilgisayarı kapatmanız, yazılım şifresi varsa da bilgisayarı yeniden başlatmanız istenecektir.

Drive Encryption etkinleştirildikten sonra oturum açma

Drive Encryption etkinleştirildikten ve kullanıcı hesabınız kaydedildikten sonra, Drive Encryption oturum açma ekranında oturum açmalısınız:

NOT: Uyku veya Beklemeden çıkışta, yazılım şifrelemesi veya donanım şifrelemesi için Drive Encryption önyükleme öncesi kimlik doğrulaması görüntülenmemektedir. Donanım şifrelemesi, etkinleştirildiğinde Uyku veya Beklemeyi önleyen **Disable sleep mode for increased security** (Daha fazla güvenlik için uyku modunu devre dışı bırak) seçeneğini sağlamaktadır.

Uyku veya Hazırda Bekletmeden çıkışta, hem yazılım şifrelemesi hem de donanım şifrelemesi için Drive Encryption önyükleme öncesi kimlik doğrulaması görüntülenmektedir.

NOT: Windows yöneticisi HP Client Security'de BIOS Önyükleme Öncesi Güvenliğini etkinleştirmişse ve One-Step Logon etkinleştirilmişse (varsayılan olarak), BIOS Önyükleme Öncesinde kimlik doğrulaması sonrasında, Drive Encryption oturum açma ekranında yeniden kimlik doğrulaması gerekmeksizin hemen bilgisayarda oturum açabilirsiniz.

Tek kullanıcı oturumunun açılması:

- **Logon** (Oturum açma) sayfasında, Windows parolanızı, akıllı kart PIN'inizi, SpareKey'inizi girin ya da kayıtlı bir parmağı çekin.

Çoklu kullanıcı oturumunun açılması:

1. **Select user to logon** (Oturumu açılacak kullanıcıyı seç) sayfasında, açılır listeden oturum açacak kullanıcıyı seçin ve ardından **Next** (İleri) seçeneğine tıklayın veya dokunun.

2. **Logon** (Oturum açma) sayfasında, Windows parolanızı, akıllı kart PIN'inizi, girin ya da kayıtlı bir parmağı çekin.

NOT: Aşağıdaki akıllı kartlar desteklenmektedir:

Desteklenen akıllı kartlar

- Gemalto Cyberflex Access 64k V2c

NOT: Drive Encryption oturum açma ekranında oturum açmak için kurtarma anahtarı kullanılıyorsa, kullanıcı hesaplarına erişmek için Windows oturumu açmada ek kimlik bilgileri gerekmektedir.

Ek sabit sürücüleri şifreleme

Sabit sürücünüzü şifrelemek suretiyle verilerinizi korumak için HP Drive Encryption kullanmanız kesinlikle önerilir. Etkinleştirme sonrasın oluşturulan her türlü eklenmiş sabit sürücü veya bölüm, aşağıdaki adımların izlenmesiyle şifrelenebilir:

1. **Drive Encryption**'ı başlatın. Daha fazla bilgi için, bkz. Drive Encryption'ı açma sayfa 30.
2. Yazılım şifrelemesi uygulanmış sürücüler için, şifrelenecek sürücü bölümlerini seçin.

NOT: Bu, bir veya daha fazla standart sabit sürücünün ve bir veya daha fazla kendi kendini şifreleyen sürücünün var olduğu karışık bir sürücü senaryosu için de geçerlidir.

– veya –

- Donanım şifrelemesi uygulanmış sürücüler için, şifrelenecek ek sürücüleri seçin.

Gelişmiş görevler

Drive Encryption'ı yönetme (yönetici görevi)

Yöneticiler, bilgisayardaki tüm sabit sürücülerin şifreleme durumunu görmek ve değiştirmek (Şifrelenmemiş veya Şifrelenmiş) için Drive Encryption kullanabilir.

- Durum Etkinleştirilmiş ise, Drive Encryption etkinleştirilmiş ve yapılandırılmıştır. Sürücü, aşağıdaki durumlardan birindedir:

Yazılım şifreleme

- Şifrelenmemiş
- Şifrelenmiş
- Şifreleniyor
- Şifre çözülüyor

Donanım şifreleme

- Şifrelenmiş
- Şifrelenmemiş (ek sürücüler için)

Farklı sürücü bölümlerini şifreleme veya şifresini çözme (yalnızca yazılım şifreleme)

Yöneticiler, bilgisayardaki bir veya daha fazla sabit sürücü bölümünü şifrelemek veya zaten şifrelenmiş olan tüm sürücü bölümlerinin şifresini çözmek için Drive Encryption kullanabilir.

1. **Drive Encryption**'ı başlatın. Daha fazla bilgi için, bkz. Drive Encryption'ı açma sayfa 30.
2. **Drive Status** (Sürücü Durumu) altında, şifrelemek veya şifresini çözmek istediğiniz sabit sürücü bölümlerinin yanındaki onay kutularını seçin ya d temizleyin ve ardından **Apply** (Uygula) seçeneğine tıklayın ya da dokunun.

NOT: Bir bölüm şifrelenirken ya da şifresi çözülürken, bir ilerleme çubuğu da şifrelenen bölüm yüzdesini görüntüler.

NOT: Dinamik bölümler desteklenmemektedir. Bölüm kullanılabilir olarak görüntüleniyorsa, ancak seçildiğinde şifrelenemiyorsa, bölüm dinamiktir. Dinamik bir bölüm, Disk Yönetimi altında yeni bir bölüm oluşturmak için bir bölümün sıkıştırılmasından doğmaktadır.

Bir bölüm dinamik bölüme dönüştürülecekse, bir uyarı görüntülenmektedir.

Disk yönetimi

- **Nickname** (Takma ad)—Daha kolay tanımlama için, sürücülerinize veya bölümlerinize ad verebilirsiniz.
- **Disconnected drives** (Bağlantısı kesilmiş sürücüler)—Drive Encryption, bilgisayardan kaldırılan diskleri takip edebilir. Bilgisayardan kaldırılan bir disk, otomatik olarak Bağlantısı Kesilmiş listesine taşınmaktadır. Disk sisteme geri dönüyorsa, bir kez daha Bağlanmış listesinde görünecektir.
- Bağlanmış sürücüyü artık takip etmiyor veya yönetmiyorsanız, bağlantısı kesilmiş sürücüyü Bağlantısı Kesilmiş listesinden kaldırabilirsiniz.
- Drive Encryption, tüm bağlı sürücüler temizlenene ve Bağlantısı Kesilmiş listesi boşalana dek etkinleştirilmiş kalır.

Yedekleme ve kurtarma (yönetici görevi)

Drive Encryption etkinleştirildiğinde, yöneticiler, kurtarılabilir ortamda şifreleme anahtarlarını yedeklemek ve bir kurtarma gerçekleştirmek için Şifreleme Anahtarı Yedekleme sayfasını kullanabilir.

Şifreleme anahtarlarını yedekleme

Yöneticiler, kaldırılabilir bir depolama aygıtındaki şifrelenmiş bir sürücünün şifreleme anahtarını yedekleyebilir.

DİKKAT: Yedekleme anahtarını içeren depolama aygıtını güvenli bir yerde tuttuğunuzdan emin olun, çünkü parolanızı unutursanız, akıllı kartınızı kaybederseniz veya parmağınız kayıtlı olmazsa, bu aygıt bilgisayara yegâne erişiminizi sağlar. Depolama yeri de güvenli olmalıdır, çünkü depolama aygıtı Windows'a erişimi mümkün kılar.

1. **Drive Encryption**'ı başlatın. Daha fazla bilgi için, bkz. Drive Encryption'ı açma sayfa 30.
2. Bir sürücünün onay kutusunu seçin ve ardından **Backup Key** (Yedekleme Anahtarı) seçeneğine tıklayın veya dokunun.

3. **Create HP Drive Encryption recovery key** (HP Drive Encryption kurtarma anahtarı oluştur) seçeneğinin altında, aşağıdaki seçeneklerden birini veya daha fazlasını seçin:

   - **Removable Storage** (Kaldırılabilir Depolama)—Onay kutusunu seçin ve ardından şifreleme anahtarının kaydedileceği depolama aygıtını seçin.
   - **SkyDrive**—Onay kutusunu seçin. İnternete bağlı olmanız gerekmektedir. Microsoft SkyDrive'da oturum açın ve ardından **Yes** (Evet) seçeneğine tıklayın ya da dokunun.

   NOT: SkyDrive üzerinde depolanan HP Drive Encryption yedekleme anahtarını kullanmak için, SkyDrive'dan kaldırılabilir bir depolama aygıtına indirmeli ve ardından depolama aygıtını bu bilgisayara takmalısınız.

   - **TPM** (yalnızca belirli modeller)—TPM parolanızı kullanarak verilerinizi kurtarmanıza olanak sağlar.

   DİKKAT: TPM temizlenir veya bilgisayar hasar görürse, yedeğe erişiminiz kaybolacaktır. Bu yöntem seçilirse, başka bir yedekleme yöntemi de seçilmelidir.

4. **Backup** (Yedekle) seçeneğine tıklayın veya dokunun.

   Şifreleme anahtarı, seçtiğiniz depolama aygıtına kaydedilir.

Yedekleme anahtarları kullanarak etkinleştirilmiş bir bilgisayara erişimi kurtarma

Yöneticiler, etkinleştirmede kurtarılabilir bir depolama aygıtında yedeklenmiş Drive Encryption anahtarını kullanarak ya da Drive Encryption'daki **Backup Key** (Anahtarı Yedekle) seçeneğini seçerek bir kurtarma gerçekleştirebilir.

1. Yedekleme anahtarınızı içeren kurtarılabilir depolama aygıtını takın.
2. Bilgisayarı açın.
3. HP Drive Encryption oturum açma diyalog kutusu açıldığında, **Recovery** (Kurtarma) seçeneğine tıklayın veya dokunun.
4. Yedekleme anahtarınızı içeren dosya yolunu ya da adını girin ve ardından **Recovery** (Kurtarma) seçeneğine tıklayın veya dokunun.
5. Onay diyalog kutusu açıldığında, **OK** (Tamam) seçeneğine tıklayın veya dokunun.

   Windows oturum açma ekranı görüntülenir.

NOT: Drive Encryption oturum açma ekranında oturum açmak için kurtarma anahtarı kullanılıyorsa, kullanıcı hesaplarına erişmek için Windows oturumu açmada ek kimlik bilgileri gerekmektedir. Bir kurtarma gerçekleştirdikten sonra kesinlikle parolanızı sıfırlamanız önerilir.

Bir HP SpareKey Kurtarma işlemi gerçekleştirme

Drive Encryption Önyükleme Öncesi sırasında SpareKey kurtarma, bilgisayara erişebilmek için güvenlik sorularına doğru yanıt vermenizi gerektirir. SpareKey Kurtarma kurulumu hakkında daha fazla bilgi için, HP Client Security yazılım yardımına bakın.

Parolanızı unutursanız HP SpareKey Kurtarma işlemi gerçekleştirmek için:

1. Bilgisayarı açın.
2. HP Drive Encryption sayfası görüntülendiğinde, kullanıcı oturum açma sayfasına gidin.

3. **SpareKey**'i tıklatın.

NOT: HP Client Security'de SpareKey başlatılmamışsa, **SpareKey** düğmesi kullanılamaz.

4. Görüntülenen sorulara doğru yanıtları yazın ve ardından **Logon** (Oturum aç) seçeneğini tıklatın.

   Windows oturum açma ekranı görüntülenir.

NOT: Drive Encryption oturum açma ekranında oturum açmak için SpareKey kullanılıyorsa, kullanıcı hesaplarına erişmek için Windows oturumu açmada ek kimlik bilgileri gerekmektedir. Bir kurtarma gerçekleştirdikten sonra kesinlikle parolanızı sıfırlamanız önerilir.

6 HP File Sanitizer (yalnızca belirli modellerde)

File Sanitizer, bilgisayarın dahili sabit sürücüsündeki varlıkları (örnek: kişisel bilgiler veya dosyalar, geçmiş veya web ile ilgili veriler ya da diğer veri bileşenleri) güvenli bir biçimde parçalamanıza ve bilgisayarın dahili sabit sürücüsünü periyodik olarak kaplamanıza izin vermektedir.

File Sanitizer, aşağıdaki sürücü tiplerini kaplamak için kullanılamaz.

- Bir SSD aygıtı yayan RAID birimleri de dâhil olmak üzere, katı hâl sürücüleri (SSD)
- USB, Firewire veya eSATA arayüzü ile bağlanan harici sürücüler

Bir SSD üzerinde bir parçalama veya kaplama işlemi deneniyorsa, bir uyarı iletisi görüntülenmekte ve işlem gerçekleştirilmemektedir.

Parçalama

Parçalama, standart Windows® silme işleminden farklıdır. File Sanitizer kullanarak bir varlığı parçaladığınız zaman, dosyaların üzerine anlamsız veriler yazılmakta ve özgün varlığın geri alınması neredeyse olanaksız hâle gelmektedir. Basit bir Windows silme işlemi, dosyayı (ya da varlığı) sabit sürücüde olduğu gibi ya da adli yöntemler kullanılarak kurtarılmasını mümkün kılacak bir hâlde bırakabilir.

Gelecekteki bir parçalama saatini zamanlayabilir ya da HP Client Security Home ekranında **File Sanitizer** simgesini seçerek ya da Windows masaüstündeki **File Sanitizer** simgesini kullanarak parçalamayı manuel olarak etkinleştirebilirsiniz. Daha fazla bilgi için, Bir parçalama zamanlaması ayarlama sayfa 39, Sağ tıkla parçalama sayfa 41 veya Bir parçalama işlemine manuel olarak başlama sayfa 41 seçeneklerine başvurun.

NOT: Bir .dll dosyası, yalnızca Geri Dönüşüm Kutusuna taşınmış olması durumunda parçalanarak sistemden kaldırılmaktadır.

Boş alan kaplama

Windows'ta bir varlığın silinmesi, varlığın içeriğini sabit sürücünüzden tamamen kaldırmamaktadır. Windows, yalnızca varlığa atıfı ya da sabit sürücüdeki yerini silmektedir. Varlığın içeriği, başka bir varlık sabit sürücüdeki aynı alana yeni bilgi ile yeniden yazılana dek sabit sürücüde kalmaktadır.

Boş alan kaplama, silinen varlıkların yerine rastgele verileri güvenli bir biçimde yazmanıza olanak sağlamakta ve kullanıcıların, silinen varlığın özgün içeriğini görmesini önlemektedir.

NOT: Boş alan kaplama, parçalanan varlıklar için ek güvenlik sağlamamaktadır.

Gelecekteki bir boş alan kaplama saati ayarlayabilir ya da HP Client Security Home ekranında **File Sanitizer** simgesini seçerek ya da Windows masaüstündeki **File Sanitizer** simgesini kullanarak önceden parçalanan varlıkların boş alan kaplamasını manuel olarak etkinleştirebilirsiniz. Daha fazla bilgi için, Bir boş alan kaplama zamanlaması ayarlama sayfa 40, Manuel olarak boş alan kaplamaya başlama sayfa 42 veya File Sanitizer simgesini kullanma sayfa 41 seçeneklerine başvurun.

File Sanitizer'ı açma

1. Başlat ekranından **HP Client Security** uygulamasına (Windows 8) tıklayın ya da dokunun.

   – veya –

   Windows masaüstünde, görev çubuğunun en sağında, bildirim alanında yer alan **HP Client Security** simgesine çift tıklatın veya çift dokunun.

2. **Data** (Veri) bölümünde **File Sanitizer**'a tıklayın ya da dokunun.

– veya –

▲ Windows masaüstünde **File Sanitizer** simgesine çift tıklayın ya da çift dokunun.

– veya –

▲ Windows masaüstündeki **File Sanitizer** simgesine sağ tıklayın ya da dokunarak basılı tutun ve ardından **Open File Sanitizer**'ı (File Sanitizer'ı Aç) seçin.

Kurulum işlemleri

Shredding (Parçalama)—File Sanitizer, seçilen varlık kategorilerini güvenli bir biçimde siler veya parçalar.

1. **Shredding** (Parçalama) bölümünde, parçalanacak dosya tipleri için onay kutularını seçin ya da bu dosyaları parçalamak istemiyorsanız, onay kutusunu temizleyin.
   - **Recycle Bin** (Geri Dönüşüm Kutusu)—Geri Dönüşüm Kutusu içindeki tüm öğeleri parçalar.
   - **Temporary system files** (Geçici sistem dosyaları)—Sistem geçici klasöründe bulunan tüm dosyaları parçalar. Aşağıdaki çevre değişkenleri, aşağıdaki sırayla aratılmıştır ve bulunan ilk yol da, sistem klasörü olarak görülmektedir:
     - TMP
     - TEMP
   - **Temporary Internet files** (Geçici internet dosyaları)—Daha hızlı görüntüleme için web tarayıcıları tarafından kaydedilen web sayfaları, resimler ve ortamların kopyalarını parçalar.
   - **Cookies** (Çerezler)—Oturum açma bilgileri gibi, tercihleri kaydetmek için web siteleri tarafından bir bilgisayarda saklanan tüm dosyaları parçalar.
2. Parçalamaya başlamak için, **Shred** (Parçala) seçeneğine tıklayın ya da dokunun.

Bleaching (Kaplama)—Alan boşaltmak için rastgele veriler yazar ve silinen öğelerin kurtarılmasını önler.

▲ Kaplamaya başlamak için, **Bleach** (Kapla) seçeneğine tıklayın ya da dokunun.

File Sanitizer Options (File Sanitizer Seçenekleri)—Aşağıdaki seçenekleri etkinleştirmek için onay kutusunu seçin ya da bir seçeneği devre dışı bırakmak için onay kutusunu temizleyin:

- **Enable Desktop icon** (Masaüstü simgesini etkinleştir)—Windows Masaüstündeki File Sanitizer simgesini görüntüler.
- **Enable right-click** (Sağ tıklamayı etkinleştir)—Bir varlığa sağ tıklamanızı veya dokunarak basılı tutmanızı ve ardından **HP File Sanitizer – Shred** (HP File Sanitizer - Parçala) seçeneğini seçmenizi mümkün kılar.

- **Ask for Windows password before manual shredding**(Manuel parçalam öncesinde Windows parolası iste)—Bir öğeyi manuel olarak parçalamadan önce Windows parolası ile kimlik doğrulama gerektirir.
- **Shred Cookies and Temporary Internet Files on browser close** (Tarayıcı kapandığında çerezleri ve geçici internet dosyalarını parçala)—Bir web tarayıcısını kapattığınız zaman, tarayıcının URL geçmişi gibi web ile ilgili seçilmiş tüm varlıkları parçalar.

Bir parçalama zamanlaması ayarlama

Parçalamayı otomatik olarak gerçekleştirmek için bir zaman planlayabilir ya da istediğiniz zaman manuel olarak varlık parçalayabilirsiniz. Daha fazla bilgi için Kurulum işlemleri sayfa 38 bölümüne bakın.

1. File Sanitizer'ı açın ve ardından **Settings** (Ayarlar) seçeneğine tıklayın veya dokunun.
2. Seçilen varlıkları parçalamak için gelecekte bir zaman planlamak için, **Shred Schedule** (Parçalama Zamanlaması) altında **Never** (Asla), **Once** (Bir Kez), **Daily** (Günde Bir), **Weekly** (Haftada Bir) veya **Monthly** (Ayda Bir) seçin ve ardından bir gün ve saat seçin:
   a. Saat, dakika veya AM/PM alanına tıklayın veya dokunun.
   b. İstenen değer diğer alanlarla aynı düzeyde görüntülenene dek kaydırın.
   c. Saat ayarı alanlarını çevreleyen beyaz alana tıklayın ya da dokunun.
   d. Doğru zamanlama seçilene dek her alan için yineleyin.
3. Aşağıdaki dört varlık tipi listelenmiştir:
   - **Recycle Bin** (Geri Dönüşüm Kutusu)—Geri Dönüşüm Kutusu içindeki tüm öğeleri parçalar.
   - **Temporary system files** (Geçici sistem dosyaları)—Sistem geçici klasöründe bulunan tüm dosyaları parçalar. Aşağıdaki çevre değişkenleri, aşağıdaki sırayla aratılmıştır ve bulunan ilk yol da, sistem klasörü olarak görülmektedir:
     - TMP
     - TEMP
   - **Temporary Internet files** (Geçici internet dosyaları)—Daha hızlı görüntüleme için web tarayıcıları tarafından kaydedilen web sayfaları, resimler ve ortamların kopyalarını parçalar.
   - **Cookies** (Çerezler)—Oturum açma bilgileri gibi, tercihleri kaydetmek için web siteleri tarafından bir bilgisayarda saklanan tüm dosyaları parçalar.

   İşaretlenmesi durumunda, bu varlıkları planlanan zamanda parçalanmaktadır.
4. Parçalanacak ek özel varlıklar seçmek için:
   a. **Scheduled Shred List** (Zamanlanan Parçalama Listesi) altında, **Add folder** (Klasör ekle) seçeneğine tıklayın veya dokunun ve ardından dosya veya klasöre gidin.
   b. **Open** (Aç) seçeneğine tıklayın veya dokunun ve ardından **OK** (Tamam) seçeneğine tıklayın veya dokunun.

   Planlanan Parçalama Listesinden bir varlığı kaldırmak için, varlığın onay kutusunu kaldırın.

Bir boş alan kaplama zamanlaması ayarlama

Boş alan kaplama, parçalanan varlıklar için ek güvenlik sağlamamaktadır.

1. File Sanitizer'ı açın ve ardından **Settings** (Ayarlar) seçeneğine tıklayın veya dokunun.
2. Sabit sürücünüzü kaplamak için gelecekte bir zaman planlamak için, **Bleach Schedule** (Kaplama Zamanlaması) altında **Never** (Asla), **Once** (Bir Kez), **Daily** (Günde Bir), **Weekly** (Haftada Bir) veya **Monthly** (Ayda Bir) seçin ve ardından bir gün ve saat seçin:
   a. Saat, dakika veya AM/PM alanına tıklayın veya dokunun.
   b. İstenen zaman diğer alanlarla aynı düzeyde görüntülenene dek kaydırın.
   c. Saat ayarı alanlarını çevreleyen beyaz alana tıklayın ya da dokunun.
   d. Doğru zamanlama seçilene dek yineleyin.

NOT: Boş alan kaplama işlemi uzun sürebilir. Bilgisayarınızın AC güç kaynağına bağlı olduğundan emin olun. Boş alan kaplama arka planda gerçekleşse de, artan işlemci kullanımı bilgisayarınızın performansını etkileyebilir. Boş alan kaplama, mesai saatleri dışında ya da bilgisayar kullanımda olmadığında gerçekleştirilebilir.

Dosyaları parçalanmadan koruma

Dosyaları veya klasörleri parçalanmadan korumak için:

1. File Sanitizer'ı açın ve ardından **Settings** (Ayarlar) seçeneğine tıklayın veya dokunun.
2. **Never Shred List** (Parçalanmayacaklar Listesi) altında, **Add folder** (Klasör ekle) seçeneğine tıklayın veya dokunun ve ardından dosya veya klasöre gidin.
3. **Open** (Aç) seçeneğine tıklayın veya dokunun ve ardından **OK** (Tamam) seçeneğine tıklayın veya dokunun.

NOT: Bu listedeki dosyalar, listede kaldıkları sürece korunmaktadır.

İstisnalar listesinden bir varlığı kaldırmak için, varlığın onay kutusunu kaldırın.

Genel görevler

Aşağıdaki görevleri gerçekleştirmek için File Sanitizer'ı kullanın:

- **Use the File Sanitizer icon to initiate shredding** (Parçalamayı başlatmak için File Sanitizer simgesini kullan)—Dosyaları Windows masaüstündeki **File Sanitizer** simgesine sürükleyin. Daha fazla bilgi için, File Sanitizer simgesini kullanma sayfa 41 seçeneğine başvurun.
- **Manually shred a specific asset or all selected assets** (Spesifik bir varlığı ya da seçilen tüm varlıkları manuel olarak parçala)—Planlanan parçalama zamanını beklemeden öğeleri istediğiniz zaman parçalayın. Ayrıntılar için, Sağ tıkla parçalama sayfa 41 veya Bir parçalama işlemine manuel olarak başlama sayfa 41 seçeneğine başvurun.
- **Manually activate free space bleaching** (Boş alan kaplamayı manuel olarak etkinleştir)—Boş alan kaplamayı istediğiniz zaman etkinleştirin. Daha fazla bilgi için, Manuel olarak boş alan kaplamaya başlama sayfa 42 seçeneğine başvurun.
- **View the log files** (Günlük dosyalarını gör)—Son parçalama ya da boş alan kaplama işleminden kalan tüm hata ve arızaları içeren parçalama ve boş alan kaplama günlük dosyalarını görün. Daha fazla bilgi için, şuraya başvurun: Günlük dosyalarını görme sayfa 42.

NOT: Parçalama veya boş alan kaplama işlemi uzun bir süre alabilir. Parçalama ve boş alan kaplama arka planda gerçekleşse de, artan işlemci kullanımı bilgisayarınızın performansını etkileyebilir.

File Sanitizer simgesini kullanma

DİKKAT: Parçalanan varlıklar kurtarılamaz. Manuel parçalama için hangi öğeleri seçeceğinizi dikkatli düşünün.

Manuel olarak bir parçalama işlemine başladığınızda, File Sanitizer görünümündeki standart parçalama listesi parçalanmaktadır (bkz: Kurulum işlemleri sayfa 38).

Manuel olarak bir parçalama işlemine aşağıdaki yollardan birini izleyerek başlayabilirsiniz:

1. File Sanitizer'ı açın (bkz: File Sanitizer'ı açma sayfa 38) ve ardından **Shred** (Parçala) seçeneğine tıklayın veya dokunun.
2. Onay diyalog kutusu açıldığında, parçalamak istediğiniz varlıkların işaretlenmiş olduğundan emin olun ve ardından **OK** (Tamam) seçeneğine tıklayın veya dokunun.

– veya –

1. Windows masaüstündeki **File Sanitizer** simgesine sağ tıklayın veya dokunarak basılı tutun ve ardından **Shred Now** (Şimdi Parçala) seçeneğine tıklayın veya dokunun.
2. Onay diyalog kutusu açıldığında, parçalamak istediğiniz varlıkların işaretlenmiş olduğundan emin olun ve ardından **Shred** (Parçala) seçeneğine tıklayın veya dokunun.

Sağ tıkla parçalama

DİKKAT: Parçalanan varlıklar kurtarılamaz. Manuel parçalama için hangi öğeleri seçeceğinizi dikkatli düşünün.

File Sanitizer görünümünde **Enable right-click shredding** (Sağ tıklamayla parçalamayı etkinleştir) seçilmişse, bir varlığı şu şekilde parçalayabilirsiniz:

1. Parçalamak istediğiniz belge veya klasöre gidin.
2. Dosya veya klasöre sağ tıklayın veya dokunarak basılı tutun ve ardından **HP File Sanitizer – Shred** (HP File Sanitizer - Parçala) seçeneğini seçin.

Bir parçalama işlemine manuel olarak başlama

DİKKAT: Parçalanan varlıklar kurtarılamaz. Manuel parçalama için hangi öğeleri seçeceğinizi dikkatli düşünün.

Manuel olarak bir parçalama işlemine başladığınızda, File Sanitizer görünümündeki standart parçalama listesi parçalanmaktadır (bkz: Kurulum işlemleri sayfa 38).

Manuel olarak bir parçalama işlemine aşağıdaki yollardan birini izleyerek başlayabilirsiniz:

1. File Sanitizer'ı açın (bkz: File Sanitizer'ı açma sayfa 38) ve ardından **Shred** (Parçala) seçeneğine tıklayın veya dokunun.
2. Onay diyalog kutusu açıldığında, parçalamak istediğiniz varlıkların işaretlenmiş olduğundan emin olun ve ardından **OK** (Tamam) seçeneğine tıklayın veya dokunun.

– veya –

1. Windows masaüstündeki **File Sanitizer** simgesine sağ tıklayın veya dokunarak basılı tutun ve ardından **Shred Now** (Şimdi Parçala) seçeneğine tıklayın veya dokunun.
2. Onay diyalog kutusu açıldığında, parçalamak istediğiniz varlıkların işaretlenmiş olduğundan emin olun ve ardından **Shred** (Parçala) seçeneğine tıklayın veya dokunun.

Manuel olarak boş alan kaplamaya başlama

Manuel olarak bir kaplama işlemine başladığınızda, File Sanitizer görünümündeki standart parçalama listesi kaplanmaktadır (bkz. Kurulum işlemleri sayfa 38).

Manuel olarak bir kaplama işlemine aşağıdaki yollardan birini izleyerek başlayabilirsiniz:

1. File Sanitizer'ı açın (bkz: File Sanitizer'ı açma sayfa 38) ve ardından **Bleach** (Kapla) seçeneğine tıklayın veya dokunun.
2. Onay iletişim kutusu açıldığında, **OK** (Tamam) seçeneğine tıklayın veya dokunun.

– veya –

1. Windows masaüstündeki **File Sanitizer** simgesine sağ tıklayın veya dokunarak basılı tutun ve ardından **Bleach Now** (Şimdi Kapla) seçeneğine tıklayın veya dokunun.
2. Onay iletişim kutusu açıldığında, **Bleach** (Kapla) seçeneğine tıklayın veya dokunun.

Günlük dosyalarını görme

Her parçalama veya boş alan kaplama işlemi gerçekleştirildiğinde, tüm hata ve arızaların günlük dosyaları oluşturulmaktadır. Günlük dosyaları, her zaman en son parçalama veya boş alan kaplama işlemine göre güncellenmektedir.

NOT: Başarıyla parçalanan veya kaplanan dosyalar, günlük dosyalarında görünmemektedir.

Parçalama işlemleri için bir günlük dosyası oluşturulmuştur ve boş alan kaplama işlemleri için başka bir günlük dosyası oluşturulmaktadır. Her iki günlük dosyası da, sabit sürücüdeki şu klasörlerde yer almaktadır:

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

64 bitlik sistemler için, günlük dosyaları, sabit sürücüdeki şu klasörlerde yer almaktadır:

- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[Kullanıcı Adı]*_ShredderLog.txt
- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[Kullanıcı Adı]*_DiskBleachLog.txt

7 HP Device Access Manager (yalnızca belirli modellerde)

HP Device Access Manager, veri aktarım aygıtlarını devre dışı bırakarak verilere erişimi kontrol etmektedir.

NOT: Fare, Dokunmatik Yüzey ve parmak izi okuyucu gibi bazı insan arabirim/giriş aygıtları, Device Access Manager tarafından kontrol edilmemektedir. Daha fazla bilgi için, bkz. Yönetilmeyen aygıt sınıfları sayfa 46.

Windows® işletim sistemi yöneticileri, bir sistem üzerindeki aygıtlara erişimi kontrol etmek ve yetkisiz erişime karşı korumak için HP Device Access Manager kullanmaktadır:

- Erişim yetkisine sahip oldukları ya da erişim izninin verilmediği aygıtları tanımlama amacıyla, her kullanıcı için aygıt profilleri oluşturulmaktadır.
- Just In Time Authentication (JITA), aksi halde erişilemeyecek aygıtlara erişmek amacıyla önceden tanımlanmış kullanıcıların kimlik doğrulamasına olanak tanımaktadır.
- Yöneticiler ve güvenilir kullanıcılar Aygıt Yöneticileri grubuna eklenerek, aygıta erişimde Device Access Manager tarafından uygulanan kısıtlamaların dışında bırakılabilirler. Bu grup üyeliği Gelişmiş Ayarlar kullanılarak yönetilir.
- Aygıta erişim izni, grup üyeliği veya ayrı ayrı kullanıcı temelinde verilebilir veya reddedilebilir.
- CD-ROM sürücüleri ve DVD sürücüleri gibi aygıt sınıflarında, yazma erişimi ve okuma erişimi ayrı ayrı verilebilir veya reddedilebilir.

HP Device Access Manager, HP Client Security Kurulum Sihirbazının tamamlanması sırasında aşağıdaki ayarlar ile otomatik olarak yapılandırılmaktadır:

- Tam Zamanında Kimlik Doğrulaması (JITA) Çıkarılabilir Ortam, Yöneticiler ve Kullanıcılar için etkinleştirilir.
- Aygıt ilkesi, diğer aygıtlara tam erişime izin verir.

Device Access Manager'ı açma

1. Başlat ekranından **HP Client Security** uygulamasına (Windows 8) tıklayın ya da dokunun.

   – veya –

   Windows masaüstünde, görev çubuğunun en sağında, bildirim alanında yer alan **HP Client Security** simgesine çift tıklatın veya çift dokunun.

2. **Device** (Aygıt) bölümünde **Device Permissions** (Aygıt İzinleri) seçeneğine tıklayın ya da dokunun.

   - Standart kullanıcılar, güncel aygıt erişimlerini görebilirler (bkz: Kullanıcı görünümü sayfa 44).
   - Yöneticiler **Change** (Değiştir) seçeneğine tıklayarak veya dokunarak ve ardından Yönetici parolasını girerek bilgisayar için yapılandırılmış durumda olan aygıt erişimini görebilir ve değişiklik yapabilir (bkz: Sistem görünümü sayfa 44).

Kullanıcı görünümü

Device Permissions (Aygıt İzinleri seçildiğinde, Kullanıcı görünümü görüntülenir. İlkeye bağlı olarak, standart kullanıcılar ve yöneticiler, bu bilgisayardaki aygıt sınıfları veya bireysel aygıtlar için kendi erişimlerini görebilirler.

- **Current user** (Güncel kullanıcı)—Hâlihazırda oturum açmış olan kullanıcının adı görüntülenir.
- **Device Class** (Aygıt Sınıfı)—Aygıt tipleri görüntülenir.
- **Access** (Erişim)—Hâlihazırda yapılandırılmış aygıt tiplerine ya da spesifik aygıtlara erişiminiz görüntülenir.
- **Duration** (Süre)—CD/DVD-ROM sürücülerine veya çıkarılabilir disk sürücülerine erişiminiz için süre sınırı görüntülenir.
- **Settings** (Ayarlar)—Yöneticiler, hangi sürücülerin Device Access Manager tarafından kontrol edilen erişime sahip olduğunu değiştirebilir.

Sistem görünümü

Sistem görünümünde, yöneticiler Kullanıcılar grubu veya Yöneticiler grubu için bu bilgisayardaki aygıtlara erişime izin verebilir ya da reddedebilir.

▲ Yöneticiler, **Change** (Değiştir) seçeneğine tıklayarak veya dokunarak, bir Yönetici parolası girerek ve ardından aşağıdaki seçenekler arasında seçim yaparak Sistem görünümüne erişebilir:

- **Device Access Manager** (Aygıt Erişim Yöneticisi)—Tam Zamanında Kimlik Doğrulama ile HP Device Access Manager'ı açmak veya kapamak için, **On** (Açık) veya **Off** (Kapalı) seçeneğine tıklayın veya dokunun.
- **Users and groups on this PC** (Bu PC'deki kullanıcılar ve gruplar)—Seçilen aygıt sınıflarına erişim yetkisi verilen ya da reddedilen Kullanıcılar Grubu veya Yöneticiler grubunu görüntüler.
- **Device Class** (Aygıt Sınıfı)—Sistemde yüklü olan veya önceden sisteme yüklenmiş olabilecek aygıt sınıflarını ve aygıtları görüntüler. Listeyi genişletmek için, **+** simgesine tıklayın. Bilgisayara bağlı tüm aygıtlar gösterilir ve Yöneticiler ve Kullanıcılar grubu da, ilişkinin gösterilmesi için genişletilir. Aygıtların listesini yenilemek için, yuvarlak ok (yenile) simgesine tıklayın.
  - Koruma, genellikle bir aygıt sınıfı için uygulanmaktadır. Eğer erişim **Allow** (İzin Ver) olarak ayarlanırsa, seçilen kullanıcı veya grubun aygıt sınıfındaki her türlü aygıta erişim olanağı olacaktır.
  - Koruma, spesifik aygıtlara da uygulanabilir.
  - Seçilen kullanıcıların kendi kimlik doğrulamalarını yaparak DVD/CD-ROM sürücülerine veya çıkarılabilir disk sürücülerine erişmesine izin verecek şekilde Tam Zamanında Kimlik Doğrulamasını (JITA) yapılandırın. Daha fazla bilgi için, bkz. JITA yapılandırması sayfa 45.
  - Çıkarılabilir ortam (USB flash sürücüler gibi), seri ve paralel bağlantı noktaları, Bluetooth® aygıtları, modern aygıtlar, PCMCIA/ExpressCard aygıtları, 1394 aygıtları, parmak izi okuyucu ve akıllı kart okuyucu gibi diğer aygıt sınıflarına erişime izin verin ya da reddedin. Parmak izi okuyucu ve akıllı kart okuyucu reddedilirse, kimlik doğrulama bilgisi olarak kullanılabilirler, ancak Oturum ilke düzeyinde kullanılamazlar.

    NOT: Bluetooth aygıtları kimlik doğrulama bilgisi olarak kullanılırsa, Device Access Manager ilkesinde Bluetooth aygıtı erişiminin kısıtlanması gerekir.

  - Grup veya Aygıt Sınıfı düzeyinde bir ayar seçtiğiniz ve size ayarı alt nesnelere uygulamak isteyip istemediğiniz sorulduğu zaman:

Yes (Evet)—Ayar yayılacaktır.

No (Hayır)—Ayar yayılmayacaktır.

- DVD ve CD-ROM gibi bazı aygıt sınıfları, okuma ve yazma işlemleri için erişime ayrı ayrı izin verilmesi veya reddedilmesi ile de kontrol edilebilir.

NOT: Yöneticiler grubu, Kullanıcı Listesine eklenemez.

- **Access** (Erişim)—Aşağı oka tıklayın veya basın ve ardından erişim izni vermek ya da reddetmek için aşağıdaki erişim tiplerinden birini seçin:
  - **İzin Ver - Tam Erişim**
  - **İzin Ver - Salt Okunur**
  - **Allow – JITA Required** (İzin Ver - JITA Gerekli)—Daha fazla bilgi için, JITA yapılandırması sayfa 45 seçeneğine bakınız.

    Bu erişim tipi seçilirse, **Duration** (Süre) altında bir süre sınırı seçmek için aşağı oka tıklayın veya dokunun.
  - **Reddet**
- **Duration** (Süre)—CD/DVD-ROM sürücülerine ya da çıkarılabilir disk sürücülerine erişim için bir süre sınırı seçme amacıyla aşağı oka tıklayın veya dokunun (bkz: JITA yapılandırması sayfa 45).

JITA yapılandırması

JITA Yapılandırması, yöneticiye Tam Zamanında Kimlik Doğrulama (JITA) kullanarak aygıtlara erişmeye izni olan kullanıcılar ve grupların listesini görme ve değiştirme izni verir.

JITA etkinleştirilmiş kullanıcılar, **Device Class Configuration** (Aygıt Sınıfı Yapılandırması) görünümünde oluşturulmuş ilkelerin kısıtlanmış olduğu bazı aygıtlara erişebilecektir.

JITA dönemine belirli birkaç dakika için ya da Sınırsız izin verilebilir. Kimlik doğrulama anından sistem oturumunun kapatıldığı ana kadar sınırsız kullanıcının aygıta erişimi olacaktır.

Kullanıcıya sınırlı bir JITA süresi verilirse, JITA süresinin bitmesinden bir dakika önce, kullanıcıya erişimi uzatıp uzatmayacağı sorulur. Kullanıcı sistem oturumunu kapatıp başka bir kullanıcı oturum açtığında, JITA süresi sona erer. Kullanıcı bir kez daha oturup açıp JITA etkinleştirilmiş bir aygıta erişmeye çalıştığında, kimlik bilgilerini girme isteği görüntülenir.

Aşağıdaki aygıt sınıfları için JITA kullanılabilir:

- DVD/CD-ROM sürücüsü
- Çıkarılabilir Disk sürücüleri

Bir kullanıcı veya grup için bir JITA ilkesi oluşturma

Yöneticiler, Tam Zamanında Kimlik Doğrulama (JITA) kullanarak kullanıcılara veya gruplara aygıtlara erişim izni verebilmektedir.

1. **Device Access Manager**'ı başlatın ve ardından **Change** (Değiştir) seçeneğine tıklayın veya dokunun.
2. Kullanıcı veya grubu seçin ve ardından ya **Çıkarılabilir Disk sürücüleri** ya da **DVD/CD-ROM sürücüleri** için **Access** (Erişim) altından **Allow – JITA Required** (İzin Ver - JITA Gerekli) seçeneğini seçin.
3. **Duration** (Süre) altından, JITA erişimi için bir zaman seçmek için aşağı oka tıklayın veya dokunun.

Kullanıcı, yeni JITA ayarının geçerli olması için, oturumu kapatmalı ve ardından yeniden oturum açmalıdır.

Bir kullanıcı veya grup için bir JITA ilkesini devre dışı bırakma

Yöneticiler, Tam Zamanında Kimlik Doğrulama kullanarak kullanıcı veya gruba aygıt erişim izni verebilmektedir.

1. **Device Access Manager**'ı başlatın ve ardından **Change** (Değiştir) seçeneğine tıklayın veya dokunun.
2. Kullanıcı veya grubu seçin ve ardından ya **Çıkarılabilir Disk sürücüleri** ya da **DVD/CD-ROM sürücüleri** için **Access** (Erişim) altından **Deny** (Reddet) seçeneğini seçin.

Kullanıcı oturum açtığında ve aygıta erişmeye çalıştığında, erişim reddedilir.

Ayarlar

Settings (Ayarlar) görünümü, yöneticilere Device Access Manager tarafından kontrol edilen erişime sahip sürücüleri görme ve değiştirme izni verir.

NOT: Sürücü harfleri listesi yapılandırılırken Device Access Manager'ın etkinleştirilmesi gerekir (bkz: Sistem görünümü sayfa 44).

Yönetilmeyen aygıt sınıfları

HP Device Access Manager, aşağıdaki aygıt sınıflarını yönetmemektedir:

- Giriş/çıkış aygıtları
  - CD-ROM
  - Disk sürücüsü
  - Disket denetleyici (FDC)
  - Sabit disk denetleyici (HDC)
  - İnsan arabirim aygıtı (HID) sınıfı
  - Kızılötesi insan arabirim aygıtı
  - Fare
  - Çoklu bağlantı noktası seri
  - Klavye

- Tak ve Kullan (PnP) yazıcılar
- Yazıcı
- Yazıcı yükseltme

- Güç
  - Gelişmiş güç yönetimi (APM) desteği
  - Pil
- Çeşitli
  - Bilgisayar
  - Kod çözücü
  - Ekran
  - Intel® birleştirilmiş ekran sürücüsü
  - Legacard
  - Ortam sürücüsü
  - Ortam değiştirici
  - Bellek teknolojisi
  - Monitör
  - Çok işlevli
  - Net istemcisi
  - Net hizmeti
  - Net geçişi
  - İşlemci
  - SCSI bağdaştırıcısı
  - Güvenlik hızlandırıcı
  - Güvenlik aygıtları
  - Sistem
  - Bilinmeyen
  - Birim
  - Birim anlık görüntüsü

8 HP Trust Circles

Hp Trust Circles, klasör dosyası şifreleme ile kullanışlı bir güven çemberi belge paylaşım özelliğini bir araya getiren bir dosya ve belge güvenliği uygulamasıdır. Uygulama, kullanıcıların belirlediği klasörlere yerleştirilen dosyaları bir güven çemberinde koruyarak şifrelemektedir. Korunan dosyalar, yalnızca güven çemberindeki üyeler tarafından kullanılabilir ve paylaşılabilir. Korunan bir dosya üye olmayan bir kişi tarafından alınırsa, dosya şifreli kalır ve üye dışındakiler içeriğe erişemez.

Trust Circles'ı açma

1. Başlat ekranında, **HP Client Security** uygulamasına tıklayın ya da dokunun.

   – veya –

   Windows masaüstünde, görev çubuğunun en sağında yer alan bildirim alanındaki **HP Client Security** simgesine çift tıklayın.

2. **Data** (Veri) bölümünde **Trust Circies**'a tıklayın ya da dokunun.

Başlarken

E-posta daveti göndermenin ve bunlara yanıt vermenin iki yolu bulunmaktadır:

- **Using Microsoft® Outlook** (Microsoft® Outlook'u kullanma)—Microsoft Outlook ile Trust Circles kullanma, tüm Trust Circle davetlerinin ve diğer Trust Circle kullanıcılarından gelen yanıtların işlenmesini otomatikleştirir.
- **Using Gmail, Yahoo, Outlook.com or other email services (SMTP)** (Gmail, Yahoo, Outlook.com veya diğer e-posta servislerini kullanma (SMTP)—Adınızı, e-posta adresinizi ve parolanızı girdiğinizde, Trust Circles, güven çemberinize girmeleri için seçilen üyelere e-posta davetleri göndermek için e-posta servisinizi kullanır.

Temel profilinizi oluşturmak için:

1. Adınızı ve e-posta adresinizi girin ve ardından **Next** (İleri) seçeneğine tıklayın veya dokunun.

   Ad, güven çemberinize katılması için davet edilen tüm üyeler tarafından görülebilir. Davet göndermek, almak veya yanıtlamak için e-posta adresi kullanılır.

2. E-posta hesabı parolanızı girin ve ardından **Next** (İleri) seçeneğine tıklayın veya dokunun.

   E-posta ayarlarının doğru olduğundan emin olmak için, bir test e-postası gönderilir.

   NOT: Bilgisayar, bir ağa bağlı olmalıdır.

3. **Trust Circle Name** (Güven Çemberinin Adı) alanında güven çemberi için bir ad girin ve ardından **Next** (İleri) seçeneğine tıklayın veya dokunun.

4. Üye ve klasör ekleyin ve ardından **Next** (İleri) seçeneğine tıklayın veya dokunun. Güven çemberi, seçilen her türlü klasör ile oluşturulur ve seçilen üyelere e-posta davetleri gönderir. Herhangi bir nedenden dolayı bir davetin gönderilememesi durumunda, bir bildirim görüntülenir. Üyeler, **Your Trust Circles** (Güven Çemberleriniz) seçeneğine tıklanarak ve ardından güven çemberine çift tıklanarak veya çift dokunarak herhangi bir zamanda yeniden davet edilebilir. Daha fazla bilgi için, bkz. Trust Circles sayfa 49.

Trust Circles

E-posta adresinizi girdikten sonra ilk kurulum sırasında veya Trust Circle görünümde bir güven çemberi oluşturabilirsiniz:

▲ Trust Circle görünümünde, **Create Trust Circle** (Güven Çemberi Oluştur) seçeneğine tıklayın veya dokunun ve ardından güven çemberi için bir ad girin.

- Güven çemberine üye eklemek için, **Members** (Üyeler) seçeneğinin yanındaki **M+** simgesine tıklayın veya dokunun ve ardından ekrandaki yönergeleri izleyin.
- Güven çemberine klasör eklemek için, **Folders** (Klasörler) seçeneğinin yanındaki **+** simgesine tıklayın veya dokunun ve ardından ekrandaki yönergeleri izleyin.

Bir güven çemberine klasör ekleme

Yeni bir güven çemberine klasör ekleme:

- Yeni bir güven çemberinin oluşturulması sırasında, **Folders** (Klasörler) seçeneğinin yanındaki **+** simgesine tıklayarak veya dokunarak ve ardından ekrandaki yönergeleri izleyerek klasör ekleyebilirsiniz.

  – veya –

- Windows Gezgininde, bir güven çemberinin parçası olmayan bir klasöre sağ tıklayın veya dokunarak basılı tutun, **Trust Circle** (Güven Çemberi) seçeneğini seçin ve ardından **Create Trust Circle from Folder** (Klasörden Güven Çemberi Oluştur) seçeneğini seçin.

İPUCU: Bir veya daha fazla klasör seçebilirsiniz.

Var olan bir Güven Çemberine klasör ekleme:

- Trust Circle görünümünde, **Your Trust Circles** (Güven Çemberleriniz) seçeneğine tıklayın, güncel klasörleri görüntülemek için var olan güven çemberine çift tıklayın veya çift dokunun, **Folders** (Klasörler) seçeneğinin yanındaki **+** simgesine tıklayın veya dokunun ve ardından ekrandaki yönergeleri izleyin.

  – veya –

- Windows Gezgininde, bir güven çemberinin parçası olmayan bir klasöre sağ tıklayın veya dokunarak basılı tutun, **Trust Circle** (Güven Çemberi) seçeneğini seçin ve ardından **Add to existing Trust Circle from Folder** (Klasörden Var Olan Güven Çemberine Ekleme Yap) seçeneğini seçin.

İPUCU: Bir veya daha fazla klasör seçebilirsiniz.

Bir klasör bir güven çemberine eklendiğinde, Trust Circles klasörü ve içeriğini otomatik olarka şifrelemektedir. Tüm dosyalar şifrelenince, bir bildirim görüntülenir. Ek olarak, tüm şifrelenen klasör simgelerinde ve klasörlerdeki dosya simgelerinde yeşil bir kilit sembolü görüntülenir ve bunların tam koruma altında olduğunu gösterir.

Bir güven çemberine üye ekleme

Üyeleri bir güven çemberine eklemek için üç adım gereklidir:

1. **Invite** (Davet Et)—İlk olarak güven çemberinin sahibi üyeleri davet eder. Davet e-postası, birden fazla kullanıcıya ya da dağıtım listesine/gruba gönderilebilir.
2. **Accept** (Kabul Et)—Davet edilen kişi, daveti alır ve kabul mü ret mi edeceğini seçer. Davet edilen kişi daveti kabul ederse, davet eden kişiye bir e-posta yanıtı gönderilir. Davet bir gruba gönderilmişse, her üye bir davet alır ve kabül mü ret mi edeceğini seçer.
3. **Enroll** (Kaydet)—Davet eden kişi, üyeyi güven çemberine ekleyip eklememe kararını vermek için son bir fırsata sahiptir. Davet eden kişi üyeyi kabul etmeye karar verirse, davet eden kişiye yanıtı gösteren bir e-posta gönderilir. Davet eden ve edilen kişiler, isteğe bağlı olarak davet işleminin güvenliğini doğrulayabilirler. Davet edilen kişi için bir doğrulama kodu görüntülenir ve bunun telefonda davet eden kişiye okunması gerekir. Kod doğrulandıktan sonra, davet eden kişi son kabul e-postasını gönderebilir.

Yeni bir güven çemberine üye ekleme:

▲ Yeni bir güven çemberinin oluşturulması sırasında, **Members** (Klasörler) seçeneğinin yanındaki **+** simgesine tıklayarak veya dokunarak ve ardından ekrandaki yönergeleri izleyerek üye ekleyebilirsiniz.

- Outlook kullanıyorsanız, Outlook adres defterinden kişileri seçin ve ardından **OK** (Tamam) seçeneğine tıklayın
- Başka bir e-posta servisi kullanıyorlarsa, ya Trust Circle'a manuel olarak yeni adres ekleyin ya da Trust Circle'a kaydedilen e-posta adresinden bunları alabilirsiniz.

Var olan bir güven çemberine üye ekleme:

▲ Trust Circle görünümünde, **Your Trust Circles** (Güven Çemberleriniz) seçeneğine tıklayın, güncel üyeleri görüntülemek için var olan güven çemberine çift tıklayın veya çift dokunun, **Members** (Üyeler) seçeneğinin yanındaki **+** simgesine tıklayın veya dokunun ve ardından ekrandaki yönergeleri izleyin.

- Outlook kullanıyorsanız, Outlook adres defterinden kişileri seçin ve ardından **OK** (Tamam) seçeneğine tıklayın.
- Başka bir e-posta servisi kullanıyorlarsa, ya Trust Circle'a manuel olarak yeni adres ekleyin ya da Trust Circle'a kaydedilen e-posta adresinden bunları alabilirsiniz.

Bir güven çemberine dosya ekleme

Dosyaları aşağıdaki yollardan biriyle bir güven çemberine ekleyebilirsiniz:

- Dosyayı kopyalayarak var olan bir güven çemberi klasörüne taşıyın.

  – veya –

- Windows Gezgininde, şifrelenmemiş bir dosyaya sağ tıklayın veya dokunarak basılı tutun, **Trust Circle** (Güven Çemberi) seçeneğini seçin ve ardından **Encrypt** (Şifrele) seçeneğini seçin. Dosyanın ekleneceği güven çemberini seçmeniz istenecektir.

İPUCU: Bir veya daha fazla dosya seçebilirsiniz.

Şifrelenmiş klasörler

Bir güven çemberinin tüm üyeleri, o güven çemberine ait olan dosyaları görebilir ve düzenleyebilir.

NOT: Trust Circle Manager/Reader, üyeler arasında dosya senkronizasyonu yapmaz.

Dosyalar; e-posta, ftp veya bulut depolama sağlayıcıları gibi var olan yollardan paylaşılmalıdır. Bir güven çemberi klasörüne kopyalanan, taşınan veya burada oluşturulan dosyalar hemen korumaya alınmaktadır.

Bir güven çemberinden klasör kaldırma

Bir güven çemberinden klasör kaldırma, klasörün ve tüm içeriğinin şifresini çözer ve korumasını kaldırır.

- Trust Circle görünümünde, **Your Trust Circles** (Güven Çemberleriniz) seçeneğine tıklayın veya dokunun, güncel klasörleri görüntülemek için var olan güven çemberine çift tıklayın veya çift dokunun ve ardından o klasörün yanındaki **trash can** (çöp kutusu) simgesine tıklayın veya dokunun ve ardından ekrandaki yönergeleri izleyin.

  – veya –

- Windows Gezgininde, bir güven çemberinin parçası olan bir klasöre sağ tıklayın veya dokunarak basılı tutun, **Trust Circle** (Güven Çemberi) seçeneğini seçin ve ardından **Remove from trust circle** (Güven çemberinden kaldır) seçeneğini seçin.

İPUCU: Bir veya daha fazla klasör seçebilirsiniz.

Bir güven çemberinden dosya kaldırma

Bir güven çemberinden dosya kaldırmak için, Windows Gezgininde şifrelenmemiş olan bir dosyaya sağ tıklayın veya dokunarak basılı tutun, **Trust Circle** (Güven Çemberi) seçeneğini seçin ve ardından **Decrypt File** (Dosyanın Şifresini Çöz) seçeneğini seçin.

Bir güven çemberinden üye kaldırma

Tamamen kabul edilmemiş olan bir üye, bir güven çemberinden kaldırılamaz. Bir alternatif de, tüm diğer üyelerle yeni bir güven çemberi oluşturmak, tüm dosya ve klasörleri yeni güven çemberine taşımak ve ardından eski güven çemberini silmek olabilir. Bu, üyenin aldığı yeni dosyaların erişilebilir olmamasını sağlayacak, ancak önceden paylaşılmış olan her şey, eski güven çemberinin üyesi için erişilebilir olacaktır.

Bir üye tam olarak kabul edilmemişse (ya üye güven çemberine katılması için davet edilmiştir ya da güven çemberi davetini kabul etmemiştir), üyeyi şu yollardan birini izleyerek güven çemberinden kaldırabilirsiniz:

- Trust Circle görünümünde **Your Trust Circles** (Güven Çemberleriniz) seçeneğine tıklayın veya dokunun ve ardından güncel üye listesini görmek için güven çemberine çift tıklayın veya çift dokunun. Kaldırılacak üyenin adının yanındaki **trash can** (çöp kutusu) simgesine tıklayın veya dokunun.
- Trust Circle görünümünde, **Members** (Üyeler) seçeneğine tıklayın veya dokunun ve ardından üye oldukları güven çemberlerini göstermek için üyeye çift tıklayın veya çift dokunun. Üyeyi o güven çemberinden kaldırmak için bir güven çemberinin yanında bulunan **trash can** (çöp kutusu) simgesine tıklayın veya dokunun.

Bir güven çemberini silme

Bir güven çemberini silmek için, sahibi olmak gerekir.

▲ Trust Circle görünümünde, **Your Trust Circles** (Güven Çemberleriniz) seçeneğine tıklayın veya dokunun, silinecek güven çemberinin yanındaki **trash can** (çöp kutusu) simgesine tıklayın veya dokunun.

Bu, güven çemberini sayfadan kaldırır ve güven çemberinin tüm üyelerine e-posta göndererek onları güven çemberinin silinmiş olduğu konusunda bilgilendirir. Bu güven çemberine dâhil edilen tüm dosya veya klasörlerin şifresi çözülür.

Tercihleri ayarlama

Trust Circle görünümünden **Preferences** (Tercihler) seçeneğine tıklayın veya dokunun. Üç sekme görüntülenir.

- **E-Posta Ayarları**

Seçenek	Açıklama
Kullanıcı Adı	Şu anda kullanımda olan kullanıcı adı görüntülenir. Değiştirmek için, metin kutusuna yeni bir kullanıcı adı girin. Değişiklikler otomatik olarak kaydedilir.
E-Posta Adresi	Şu anda kullanılan e-posta hesabı görüntülenir. Değiştirmek için, **Change Email Settings** (E-Posta Ayarlarını Değiştir) seçeneğine tıklayın veya dokunun ve ardından ekrandaki yönergeleri izleyin.
Yeni Üye Onayı	Aşağıdaki seçeneklerden birini seçin: ◦ **Confirm Automatically** (Otomatik Onayla)—Davet edilen kişilerden kabul aldıktan sonra, bunlar manuel giriş olmadan güven çemberinde onaylanmakta ve davet edilenlere bir onay e-postası gönderilmektedir. ◦ **Confirm Manually** (Manuel Onayla)—Davet edilen kişilerden kabul aldıktan sonra, yeni üyeleri güven çemberine kabul etmek için manuel giriş gerekmekte ve ardından davet edilenlere bir onay e-postası gönderilmektedir. ◦ **Require Verification** (Doğrulama İster)—Davet edilen kişilerden kabul aldıktan sonra, davet edilenleri tam olarak kabul etmek için bir doğrulama kodu gerekmektedir. Güven çemberinin sahibi, davet edilen kişi ile irtibata geçmeli ve ondan doğrulama kodunu almalıdır. Doğru kodu girdikten sonra, onay e-postaları gönderilir.
Periyodik Kimlik Doğrulama	Periyodik kimlik doğrulama, kullanıcıların belirlenen zaman aşımı (dakika cinsinden kaydedilir) geçtikten sonra ve ayrıca hassas işlemler gerçekleştirirken Windows parolasını girmesini gerekli kılar. Bu ayar, kullanıcıların kimlik doğrulamayı açması veya kapamasına izin verir.
Kimlik Doğrulama Zaman Aşımı	Kimlik doğrulamayı gerektirecek belirlenmiş zaman aşımını (dakika cinsinden kaydedilir) seçin.
Onay mesajını gösterme	Onay mesajlarının görüntülenmesini devre dışı bırakmak için onay kutusunu seçin veya onay mesajlarını görüntülemek için onay kutusunu temizleyin.
Anonim kullanım izleme yoluyla HP Trust Circle'ın iyileştirilmesine yardımcı olmak isterim	Programa katılmak için onay kutusunu seçin veya katılmak istemiyorsanız onay kutusunu temizleyin.

- **Yedekleme/Geri Yükleme**

Seçenek	Açıklama
Yedekleme	Trust Circle Manager/Reader uygulama verilerinizi (ayarlar ve güven çemberleri) bir yedekleme dosyasına kopyalar. Bir çökme ya da sistem arızası durumunda, yeni Trust Circle yüklemenizi dosyada kaydedilen duruma geri yüklemek için bu dosyayı kullanabilirsiniz. **NOT:** Yalnızca Trust Circle uygulama verileriniz kaydedilmektedir (güven çemberleri, ayarlar ve üyeler). Güven çemberi klasörlerindeki esas dosyalar yedeklenmemektedir. Bu dosyalar, ayrı olarak yedeklenmelidir. Trust Circle ayarlarını ve kullanıcı verilerini yedeklemek için: **1.** **Backup** (Yedekle) seçeneğine tıklayın veya dokunun. **2.** Yedekleme dosyası için bir dosya adı veya dizin seçin ve ardından **Save** (Kaydet) seçeneğine tıklayın veya dokunun. **3.** Bir parola girin, onaylayın ve ardından **OK** (Tamam) seçeneğine tıklayın veya dokunun. Bu dosyayı geri yüklemek için bu parola gerekecektir.
Geri yükleme	Genellikle bir sistem çökmesi veya başka bir bilgisayara geçiş sonrasında bir yedekleme dosyasından ayarları ve güven çemberlerini geri yükler. Trust Circle Manager ayarlarını ve kullanıcı verilerini geri yüklemek için: **1.** **Restore** (Geri Yükle) seçeneğine tıklayın veya dokunun. **2.** Yedekleme dosyasının dizinine veya dosya adına gidin ve ardından **Open** (Aç) seçeneğine tıklayın veya dokunun. **3.** Yedekleme yapılırken belirlenen parolayı girin.

- **About** (Hakkında)—Trust Circle Manager/Reader yazılım sürümü görüntülenir. Trust Circle Manager'ı Pro sürümüne yükseltmenize olanak sağlamak ve HP gizlilik bildirimini görüntülemek için bağlantılar görüntülenir.

9 Theft Recovery (yalnızca belirli modellerde)

Computrace (ayrıca satın alınır) bilgisayarınızı uzaktan izlemenize, yönetmenize ve takip etmenize olanak sağlar.

Etkinleştirildikten sonra Computrace, Absolute Software Customer Center'dan yapılandırılır. Yönetici, Customer Center'da Computrace'i bilgisayarı izlemesi veya yönetmesi için yapılandırabilir. Sistem yer değiştirir veya çalınırsa, Customer Center, yerel mercilere bilgisayarın yerinin bulunması ve bilgisayarın ele geçirilmesi konusunda yardımcı olabilir. Gerektiği şekilde yapılandırılmışsa Computrace, sabit sürücü silinse veya yerinden çıkarılsa bile çalışmaya devam edebilir.

Computrace'i etkinleştirmek için:

1. Internet'e bağlanın.
2. HP Client Security'yi açın. Daha fazla bilgi için, bkz. HP Client Security'yi Açma sayfa 9.
3. **Theft Recovery**'yi tıklatın.
4. Computrace Activation Wizard'ı (Computrace Etkinleştirme Sihirbazı) başlatmak için **Get Started**'ı (Başlayın) tıklatın.
5. Kişisel bilgilerinizle birlikte kredi kartı ödeme bilgilerini girin ya da önceden satın aldığınız Ürün Anahtarını girin.

Etkinleştirme Sihirbazı işlemi güvenli bir biçimde gerçekleştirir ve Absolute Software Customer Center (Absolute Yazılım Müşteri Merkezi) web sitesinde kullanıcı hesabınızı oluşturur. İşlem tamamlandıktan sonra Customer Center (Müşteri Merkezi) hesap bilgilerinizin yer aldığı bir onay epostası alırsınız.

Computrace Etkinleştirme Sihirbazını önceden çalıştırmışsanız ve Customer Center kullanıcı hesabınız zaten varsa, HP hesap temsilcinizle iletişime geçerek ek lisanslar satın alabilirsiniz.

Customer Center'da (Müşteri Merkezi) oturum açmak için:

1. https://cc.absolute.com/ adresine gidin.
2. **Login ID** (Oturum Açma Kimliği) ve **Password** (Parola) alanlarına onay epostasında almış olduğunuz kimlik bilgilerini girin ve **Log in**'i (Oturum Aç) tıklatın.

Customer Center'ı (Müşteri Merkezi) kullanarak:

- Bilgisayarlarınızı izleyebilirsiniz.
- Uzaktan verilerinizi koruyabilirsiniz.
- Computrace tarafından korunan bilgisayarınızın çalındığını ihbar edebilirsiniz.

▲ Computrace hakkında daha fazla bilgi için **Learn More** (Daha Fazla Bilgi) seçeneğini tıklatın.

10 Yerelleştirilmiş parola istisnaları

Açılış kimlik doğrulaması seviyesinde ve HP Drive Encryption seviyesinde, parola yerelleştirmesi desteği kısıtlıdır. Daha fazla bilgi için, bkz. Windows IME'leri, Açılış kimlik doğrulaması seviyesinde ya da Drive Encryption seviyesinde desteklenmez sayfa 55.

Bir parola reddedildiğinde ne yapılmalıdır

Parolalar, şu nedenlerden dolayı reddedilebilir:

- Bir kullanıcı, desteklenmeyen bir IME kullanıyorsa. Bu, çift baytlık dillerde (Korece, Japonca, Çince) yalanan genel bir sorundur. Bu sorunu çözmek için:

  1. **Control Panel** (Denetim Masasını) kullanarak desteklenen bir klavye düzeni ekleyin (Çince Giriş Dili altına ABD/İngilizce klavyeleri ekleyin).
  2. Varsayılan giriş için desteklenen klavyeyi ayarlayın.
  3. HP Client Security'i çalıştırın ve sonra Windows parolasını girin.

- Bir kullanıcı, desteklenmeyen bir karakter kullanıyorsa. Bu sorunu çözmek için:

  1. Windows parolalarını, sadece desteklenen karakterleri kullanacak şekilde değiştirin. Desteklenmeyen karakterlerle ilgili daha fazla bilgi için bkz. Özel tuş işleme sayfa 56.
  2. HP Client Security'i çalıştırın ve sonra Windows parolasını girin.

Windows IME'leri, Açılış kimlik doğrulaması seviyesinde ya da Drive Encryption seviyesinde desteklenmez

Kullanıcı, Windows'ta standart bir batı klavyesi kullanarak Japonca veya Çince karakterler gibi karmaşık karakterler ve semboller girmek için bir IME (Giriş Yöntemi Düzenleyicisi) seçebilir.

IME'ler, Açılış kimlik doğrulaması veya Drive Encryption seviyesinde desteklenmez. Bir Windows parolası, Açılış kimlik doğrulaması veya HP Drive Encryption oturum açma sayfasında bir IME ile girilemez. Bunu yapmak, bir kilitlenme durumuyla sonuçlanabilir. Bazı durumlarda Microsoft®, kullanıcı parolayı girerken IME görüntülemez.

Bunun çözümü, klavye düzenini 00000411'e dönüştüren şu klavye düzenlerinden birine geçmektir:

- Japonca için Microsoft IME
- Japonca klavye düzeni
- Japonca için Office 2007 IME—Eğer Microsoft veya bir üçüncü taraf, IME terimini ya da giriş metodunu editörü kullanıyorsa, giriş metodu aslında bir IME olabilir. Bu karışıklığa neden olabilir ama yazılım on altılı kod temsilini okur. Bu yüzden, eğer bir IME, desteklenen bir klavye düzenine eşlemlenirse, HP Client Security yapılandırmayı destekleyebilir.

⚠ **UYARI!** HP Client Security uygulandığında, bir Windows IME ile girilen parolalar reddedilecektir.

Desteklenen bir klavye düzeni kullanılarak yapılan parola değişiklikleri

Eğer parola ilk olarak ABD İngilizce (409) gibi bir klavye düzeni kullanılarak ayarlanmışsa ve daha sonra kullanıcı Latin Amerika Dili (080A) gibi yine desteklenen farklı bir klavye düzenini kullanarak şifreyi değiştirirse, şifre değişimi HP Drive Encryption'da çalışır; ancak eğer kullanıcı ikinci klavye düzeninde olan ancak ilk klavye düzeninde olmayan karakterler (ē gibi) kullanırsa, parola BIOS'ta çalışmaz.

NOT: Yöneticiler bu sorunu, kullanıcıyı HP Client Security'den kaldırmak, işletim sisteminde istenilen klavye düzenini seçmek ve sonra HP Client Security Kurulum Sihirbazını aynı kullanıcı için tekrar çalıştırmak için HP Client Security Users (Kullanıcılar) sayfasını (Ana Sayfadaki **Dişli** simgesinden erişilir) kullanabilir. BIOS, istenilen klavye düzenini kaydeder ve bu klavye düzeni ile yazılan parolalar BIOS'ta sorunsuz bir şekilde ayarlanır.

Hepsi aynı karakterleri üretebilecek farklı klavye düzenlerinin kullanılması da başka bir potansiyel sorundur. Örneğin hem ABD Uluslararası klavye düzeni (20409) hem de Latin Amerika Dili klavye düzeni (080A) kullanıldığında, farklı bir tuş vuruşu sırası gerekebilecek olsa bile é karakteri üretilebilir. Eğer bir parola ilk olarak Latin Amerika Dili klavye düzeninde ayarlanmışsa, o zaman parola sonradan ABD Uluslararası klavye düzeni kullanılarak değiştirilmiş olsa bile BIOS'ta Latin Amerika Dili klavye düzeni ayarlanır.

Özel tuş işleme

- Çince, Slovakça, Kanada Fransızcası ve Çek Dili

  Kullanıcı önceki klavye düzenlerinden birini seçip bir parola girdiğinde (örneğin abcdef), aynı parolayı küçük harfler için shift tuşuna basılı tutarak ve büyük harfler içinse shift tuşuna ve caps lock tuşuna basılı tutarak açılış kimlik doğrulamasına ve HP Drive Encryption'a girmelidir. Rakamlardan oluşan parolalar, sayısal tuş takımı kullanılarak girilmelidir.

- Korece

  Kullanıcı desteklenen Korece bir klavye düzeni seçip bir parola girdiğinde, aynı parolayı küçük harfler için sağ taraftaki alt tuşuna basılı tutarak ve büyük harfler içinse sağ taraftaki alt tuşuna ve caps lock tuşuna basılı tutarak açılış kimlik doğrulamasına ve HP Drive Encryption'a girmelidir.

- Desteklenmeyen karakterler aşağıdaki tabloda listelenmiştir:

Language (Dil)	Windows	BIOS	Drive Encryption
Arapça	ﻷ ,ﻹ ve ﻵ tuşları iki karakter üretir.	ﻷ ,ﻹ ve ﻵ tuşları bir karakter üretir.	ﻷ ,ﻹ ve ﻵ tuşları bir karakter üretir.
Kanada Fransızcası	ç, è, à, ve é ile caps lock kullanıldığında Windows'ta Ç, È, À, ve É elde edilir.	ç, è, à, ve é ile caps lock kullanıldığında açılış kimlik doğrulamasında ç, è, à, ve é elde edilir.	ç, è, à, ve é ile caps lock kullanıldığında HP Drive Encryption'da ç, è, à, ve é elde edilir.

Language (Dil)	Windows	BIOS	Drive Encryption
İspanyolca	40a desteklenmez. Yine de çalışır çünkü yazılım onu c0a'ya dönüştürür. Ancak, klavye düzenleri arasındaki ince farklılıklardan dolayı İspanyolca konuşan kullanıcıların Windows klavye düzenlerini 1040a (İspanyolca Çeşit) ya da 080a (Latin Amerika Dili) olarak değiştirmeleri önerilir.	yok	yok
ABD uluslararası	◦ Üst satırdaki ¡, ¤, ‘, ’, ¥ ve × tuşları reddedilir. ◦ İkinci satırdaki å, ® ve Þ tuşları reddedilir. ◦ Üçüncü satırdaki á, ð ve ø tuşları reddedilir. ◦ Alt satırdaki æ tuşu reddedilir.	yok	yok
Çekçe	◦ ğ tuşu reddedilir. ◦ į tuşu reddedilir. ◦ ų tuşu reddedilir. ◦ ė, ı ve ż tuşları reddedilir. ◦ ģ, ķ, ļ, ņ ve ţ tuşları reddedilir.	yok	yok
Slovakca	ż tuşu reddedilir.	◦ š, ś ve ş tuşları, yazıldıklarında reddedilir ancak bunlar ekran klavyesi ile girildiklerinde kabul edilir. ◦ ţ konum atlatmayan tuşu, iki karakter üretir.	yok
Macarca	ż tuşu reddedilir.	ţ tuşu, iki karakter üretir.	yok
Slovence	żŻ tuşu Windows'ta reddedilir ve alt tuşu BIOS'ta bir konum atlatmayan tuş üretir.	ú, Ú, ů, Ů, ş, Ş, ś, Ś, š ve Š tuşları BIOS'ta reddedilir.	yok
Japonca	Kullanılabildiği durumlarda, Microsoft Office 2007 IME daha iyi bir seçimdir. IME adına rağmen bu aslında klavye düzeni 411'dir ve desteklenir.	yok	yok

Sözlük

acil durum kurtarma arşivi
Temel Kullanıcı Anahtarlarının bir platform sahibi anahtarından diğerine yeniden şifrelenmesine olanak tanıyan korumalı depolama alanı.

açılış kimlik doğrulaması
Bilgisayar açıldığında, akıllı kart, güvenlik yongası veya parola gibi bir tür kimlik doğrulama gerektiren güvenlik özelliği.

ağ hesabı
Yerel bir bilgisayarda, bir iş grubunda veya bir etki alanında bulunabilen bir Windows kullanıcı veya yönetici hesabı.

akıllı kart
Kimlik doğrulama için bir PIN ile birlikte kullanılabilecek bir donanım aygıtı.

Ana sayfa
HP Client Security'deki özelliklere ve ayarlara erişim sağlayabileceğiniz ve bunları yönetebileceğiniz merkezi bir konumdur.

aygıt erişim denetim ilkesi
Bir kullanıcının erişim izni ya da reddi aldığı aygıtların listesi.

aygıt sınıfı
Sürücüler gibi belli bir tipteki her türlü aygıt.

bağlı aygıt
Bilgisayar üzerindeki bir bağlantı noktasına bağlanmış bir donanım aygıtı.

Bluetooth
Bluetooth özellikli bilgisayarların, farelerin, cep telefonlarının ve diğer aygıtların kısa mesafeli kablosuz iletişim kurabilmesi için radyo transmisyonların kullanan teknoloji.

boş alan kaplama
Silinen varlıkların ve kullanılmayan alanın üzerine rastgele verilerin yazılması. Bu işlem, özgün varlığın kurtarılmasının daha güç olması için, silinen varlığın varlığını azaltmaktadır.

Çoklu Oturum Açma
Parola ile kimlik doğrulaması gerektiren Internet ve Windows uygulamalarına erişmek için HP Client Security'yi kullanmanıza olanak sağlayan ve kimlik doğrulama bilgilerini saklayan özellik.

donanım şifreleme
Anlık şifrelemeyi tamamlamak için Trusted Computing Group'un OPAL kendi kendini şifreleyen sürücü yönetimi konulu OPAL belirtimini karşılayan kendi kendini şifreleyen sürücülerin kullanımı. Donanım şifreleme anlıktır ve yalnızca birkaç dakika sürebilir, ancak yazılım şifreleme birkaç saat sürebilmektedir.

Drive Encryption
Sabit sürücünüzü veya sürücülerinizi şifreleyip bilgileri yetkisiz kişiler için okunulmaz hale getirerek verilerinizi korur.

Drive Encryption önyükleme öncesi kimlik doğrulaması
Windows başlamadan önce görüntülenen bir oturum açma ekranı. Kullanıcılar, Windows kullanıcı adlarını ve parolalarını veya akıllı kart PIN'lerini girmeli ya da kayıtlı bir parmağı çektirmelidir. Tek adımda oturum açma seçilirse, o zaman Drive Encryption oturum açma ekranında doğru bilgilerin girilmesi, Windows oturum açma ekranında yeniden oturum açma gerektirmeksizin Windows'a doğrudan erişime olanak sağlamaktadır.

DriveLock
Sabit sürücüyü bir kullanıcıyla bağdaştıran ve bilgisayar başlatıldığında kullanıcının DriveLock parolasını doğru girmesini isteyen bir güvenlik özelliği.

elle parçalama
Zamanlanan bir parçalamayı atlayan bir varlık veya seçilen varlıkların hemen parçalanması.

etki alanı
Bir ağın parçası olan ve ortak bir dizin veritabanı paylaşan bilgisayarlardan oluşan bir grup. Etki alanlarının her birinin adı farklıdır ve her birinin bir dizi ortak kuralları ve yordamları vardır.

etkinleştirme
Drive Encryption özelliklerine erişilmeden önce tamamlanması gereken görev. Yöneticiler, HP Client Security Kurulum Sihirbazı veya HP Client Security ile Drive Encryption'ı etkinleştirebilir. Etkinleştirme işlemi; yazılımın etkinleştirilmesi, sürünün şifrelenmesi ve kurtarılabilir bir depolama aygıtında ilk yedek şifreleme anahtarının oluşturulmasından oluşmaktadır.

geri yükleme
Program bilgilerini, daha önce kaydedilmiş bir yedekleme dosyasından bu programa kopyalama işlemi.

grup
Bir aygıt sınıfı veya spesifik bir aygıta aynı düzeyde erişim ya da redde sahip olan bir kullanıcı grubu.

güvenli oturum açma yöntemi
Bilgisayarda oturum açmak için kullanılan yöntem.

HP SpareKey Kurtarma
Güvenlik sorularına doğru yanıt vererek bilgisayarınıza erişebilme kabiliyeti.

Just In Time Authentication
Bkz. HP Aygıt Erişim Yöneticisi yazılımı Yardımı.

kimlik
HP Client Security'de, belirli bir kullanıcının hesabı veya profili gibi işlem gören bir grup kimlik bilgisi ve ayar.

kimlik bilgisi
Bir kullanıcının kimlik doğrulamasını yapmak için kullanılan özel bir bilgi parçası ya da donanım aygıtı.

kimlik doğrulaması
Windows parolanız, parmak iziniz, bir akıllı kart, bir temassız kart ya da bir yakın alan kartı gibi kimlik bilgilerini kullanarak, iddia ettiğiniz kişi olduğunuzu doğrulama işlemidir.

kimlik kartı
Masaüstünüzü görsel olarak kullanıcı adınız ve seçtiğiniz resimle tanımlamanızı sağlayan bir Windows masaüstü aracı.

kullanıcı
Drive Encryption'a kaydedilen herkes. Yönetici dışındaki kullanıcılar, Drive Encryption'da sınırlı haklara sahiptir. Yalnızca kayıt yapabilir (yönetici onayı ile) ve oturum açabilirler.

otomatik parçalama
File Sanitizer'da zamanladığınız parçalama.

oturum açma
Kullanıcı adı ve paroladan (ve diğer seçilmiş bilgilerden) oluşan ve web sitelerinde ve diğer programlarda oturum açmak için kullanılabilecek HP Client Security içindeki bir nesnedir.

parçalama
Anlamsız verilerle birlikte bir varlığın içinde bulunan verilerin üzerine yazan bir algoritmanın yürütülmesi.

parmak izi

Parmak izi resminizin dijital bir ayıklamasıdır. Gerçek parmak izi resminiz HP Client Security tarafından asla saklanmaz.

PIN
Kayıtlı bir kullanıcı için, kimlik doğrulama amacıyla kullanılacak kişisel bir tanımlama numarasıdır.

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

Sürücü Şifreleme oturum açma ekranı
Drive Encryption önyükleme öncesi kimlik doğrulamasına bakın.

şifre çözme
Şifreleme biliminde şifreli bir veriyi düz metne dönüştürmek için kullanılan bir yordam.

şifreleme
Yetkisiz alıcıların söz konusu verileri okumasını önlemek için, algoritmalar gibi şifreleme biliminde kullanılan yöntemlerle düz metni şifreli metne dönüştürme yordamıdır. Çok sayıda türü mevcut olan veri şifreleme, ağ güvenliğinin temelini oluşturur. Yaygın türleri arasında Veri Şifreleme Standardı ve ortak anahtar şifrelemesi bulunur.

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

temassız kart
Kimlik doğrulama için kullanılabilecek bir bilgisayar çipi içeren bir plastik kart.

Trust Circle
Tanımlı bir güvenilir kullanıcılar grubuna veri bağlayarak veri kapsama sağlar. Bu, verilerin kaza eseri ya da kasıtlı olarak yanlış ellere geçmesini önler. CryptoMill'in Zero Overhead Key Management teknolojisi ile güvence altına alınan veriler, kriptografik olarak bir güven çemberine bağlanır. Bu, belgelerin ve diğer hassas bilgilerin trust circle (güven çemberi) dışında şifre çözümüne uğramasını önler

Trust Circle klasörü
Bir güven çemberi tarafından korunan herhangi bir klasör.

Trust Circle Manager/Reader
Trust Circle Reader, yalnızca Trust Circle Manager kullanıcıları tarafından gönderilen davetleri kabul edebilir. Ancak Trust Circle Manager, güven çemberlerinin oluşturulmasına izin verir. Bir güven çemberine e-posta aracılığıyla birini davet etme ve başkalarından güven çemberi davetleri alma gibi özellikleri bulunur. Akranlar arasında bir güven çemberi oluşturulunca, bu güven çemberi tarafından korunan dosyalar da güvenli olarak paylaşılabilir.

Trusted Platform Module (TPM) katıştırılmış güvenlik yongası
TPM, şifreleme anahtarları, dijital sertifikalar ve parolalar gibi ana bilgisayar sistemine özel bilgileri depolayarak bir kullanıcıdan çok bir bilgisayarın kimlik doğrulamasını yapar. TPM, bilgisayardaki bilgilerin fiziksel olarak hırsızlık ya da dışarıdan bir hacker saldırısı ile tehlikeye girmesi olasılığını en aza indirir.

varlık
Sabit sürücüde yer alan ve kişisel bilgiler veya dosyalar, geçmiş ve web ile ilgili veriler vs. içeren bir veri bileşeni.

Windows kullanıcı hesabı
Bir ağda ya da bağımsız bir bilgisayarda oturum açma yetkisine sahip bir kullanıcı.

Windows Oturumu Açma Güvenliği
Erişim için belirli kimlik bilgilerinin kullanılmasını isteyerek Windows hesabınızı veya hesaplarınızı korur.

Windows yöneticisi
Diğer kullanıcıların izinlerini değiştirmek ve onları yönetmek için tüm haklara sahip bir kullanıcı.

yakın alan kartı
Ek güvenlik için diğer kimlik bilgileriyle birlikte kimlik doğrulama için kullanılabilecek bir bilgisayar çipi içeren bir plastik kart.

yazılım şifreleme
Sabit sürücüyü sektör sektör şifrelemek için yazılım kullanımı. Bu işlem, donanım şifrelemeden daha yavaştır

yedekleme
Önemli program bilgilerinin bir kopyasını, programın dışındaki bir konuma kaydetmek için yedekleme özelliğini kullanmaktır. Bunlar daha sonra aynı bilgisayara ya da başka bir bilgisayara bu bilgileri geri yüklemek için kullanılabilir.

yeniden başlatma
Bilgisayarı yeniden başlatma işlemi.

yönetici
*Windows yöneticisi*ne bakın.

Dizin