Dell Veri Koruma | Erişim Anasayfa

Dell Veri Koruma | Erişim Anasayfası bu uygulamanın özelliklerine erişmek için başlangıç noktasıdır. Bu pencereden aşağıdakilere erişebilirsiniz:

System Access Wizard
Erişim Seçenekleri
Self-Encrypting Drive
Gelişmiş Seçenekler

Pencerenin sağ alt köşesinde **gelişmiş** linki bulunmaktadır, buradan gelişmiş seçeneklere erişebilirsiniz.

Gelişmiş seçenekler'den anasayfaya dönmek pencerenin sağ alt köşesinde bulunan **anasayfa** linkine tıklayabilirsiniz.

System Access Wizard

Dell Veri Koruma | Erişim uygulaması ilk çalıştırıldığında System Access Wizard otomatik olarak çalışır. Bu sihirbaz sisteminizdeki güvenliğin tüm yönlerinin ayarlanması için size yardımcı olur, sistem oturumu açmayı nasıl (örn. sadece şifre veya parmak izi ve şifre) ve ne zaman (Windows, Windows öncesi veya her ikisi de) istediğinizi burada ayarlayabilirsiniz. Buna ek olarak eğer sisteminizde self-encrypting drive varsa bunu da sihirbaz ile yapılandırabilirsiniz.

Yönetici Fonksiyonları

Sistemde Windows yönetici ayrıcalıklarına sahip olan kullanıcılar **Dell Veri Erişim | Koruma** içinde standart kullanıcıların yapamayacağı aşağıdaki fonksiyonları gerçekleştirme hakkına sahiptirler:

- Sistem (Windows Öncesi) şifresi ayarlama / değiştirme
- Sabit Disk şifresi ayarlama / değiştirme
- Yönetici şifresi ayarlama / değiştirme
- TPM Sahip şifresi ayarlama / değiştirme
- ControlVault Yönetici şifresi ayarlama / değiştirme
- Sistem sıfırlama
- Tanıtımları arşivleme ve geri yükleme
- smartcard Yönetici PIN kodu ayarlama / değiştirme
- smartcard silme / sıfırlama
- Windows için Dell Güvenli oturum Açma etkinleştirme / devre dışı bırakma
- Windows oturumu açma ilkesi ayarlama
- Aşağıdakiler dahil self-encrypting drives yönetme:
    - Self-encrypting drive kilitleme etkin / devre dışı
    - Windows Şifre Senkronizasyonu (WPS) etkin / devre dışı
    - Single Sign On etkin / devre dışı (SSO)
    - Kriptografik silme gerçekleştirme

Uzaktan Yönetim

Organizasyonunuz **Dell Veri Koruma | Erişim** uygulamasının güvenlik fonksiyonlarını birden fazla platformda merkezi şekilde yönetilecek biçimde bir ortam oluşturabilir (örn. uzaktan yönetim). Bu durumda, **Dell Veri Koruma | Erişim** spesifik özelliklerini güvenle yönetmek için Aktif Dizin gibi Windows güvenlik alt yapısı kullanılabilir.

Bir bilgisayar uzaktan yönetildiğinde (örn. "sahibi" uzak yönetici olduğunda), **Dell Veri Koruma | Erişim** fonksiyonelliğinin lokal idaresi devre dışı kalacaktır; uygulamanın yönetim penceresine lokal olarak erişim mümkün olmayacaktır. Aşağıdaki fonksiyonlar uzaktan yönetilebilir:

- Trusted Platform Module (TPM)
- ControlVault
- Windows Öncesi Oturum Açma
- Sistem Sıfırlama
- BIOS Şifreleri
- Windows Oturum Açma ilkesi
- Self-Encrypting Drives
- Parmak izi ve Smartcard kaydı

Uzaktan yönetim amacıyla Wave Systems' EMBASSY® Remote Administration Server (ERAS) kullanma hakkında daha fazla bilgi istemek için lütfen Dell satış temsilcinizle görüşün veya dell.com adresine gidin.

Erişim Seçenekleri

Erişim Seçenekleri penceresinden, sisteminize nasıl erişeceğinizi ayarlayabilirsiniz.

Eğer ayarlanmış herhangi bir **Dell Veri Koruma | Erişim** seçeneği varsa, bunlar kullanılabilir seçeneklerle birlikte ana sayfada görüntülenir (örn., Windows öncesi oturum açma için şifre değiştirme). Kullanılabilir seçenekler üzerine tıklandığında belirli bir görevi yerine getirmek amacıyla sizi uygun pencereye taşıyan kısayollardır (örn., Windows öncesi şifreyi değiştirme veya başka bir parmak izi kaydetme).

Genel
Öncelikle ne zaman (Windows, Windows öncesi veya her ikisi de) ve nasıl (örn. parmak izi veya şifre) oturum açılacağını belirleyebilirsiniz. Nasıl oturum açılacağı ile ilgili olarak bir veya iki seçenek seçebilirsiniz; bunlar parmak izi, smartcard ve şifre kombinasyonları olabilir. Listelenen seçenekler ortamınızda uygulanan ve platformda desteklenen ilkelere dayanır.

Parmak izi
Eğer sisteminizde bir parmak izi okuyucu varsa, sistemde oturum açarken kullanmak amacıyla parmak izi kaydedebilir veya güncelleyebilirsiniz. Parmak izlerini kaydettiğinizde, sisteminize Windows, Windows öncesi veya her ikisinde de erişmek için sisteminizin parmak izi okuyucusundan kaydedilmiş parmak izlerini okutabilirsiniz (Genel Erişim Seçeneklerinde belirlenen şekilde). Daha fazla bilgi için Kullanıcı Parmak İzlerini Kaydetme bölümüne bakın.

Windows Öncesi Oturum Açma
Eğer kullanıcıların Windows öncesi oturum açmalarını belirlediyseniz, Windows öncesi erişim için Sistem Şifresi (bazen Windows öncesi şifre de denir) belirlemeniz gerekir. Bu ayarlandığında, yönetici şifreyi istediği zaman değiştirebilir.

Bu ekrandan Windows öncesi oturum açmayı devre dışı da bırakabilirsiniz; bunu yapmak için mevcut Sistem Şifresini girmeniz, şifrenin doğru olduğunu onaylamanız ve sonra **Devre dışı** düğmesine tıklamanız gereklidir.

Smartcard
Eğer kullanıcıların oturum açmak için smartcard kullanması gerektiğini belirttiyseniz, bir veya daha fazla geleneksel (temaslı) veya temassız smartcard kaydetmeniz gereklidir. Smartcard kayıt sihirbazını çalıştırmak için **Başka bir smartcard kaydet** linkine tıklayın. Kaydetmek oturum açmak için smartcard kullanımını ayarlamak demektir.

Smartcard kaydını tamamladığınızda, **Smartcard PIN değiştir veya ayarla** linki ile bu kart ile kullanım için PIN ayarlayabilir veya değiştirebilirsiniz.

Windows Öncesi Oturum Açma

Windows öncesi oturum açma ayarlandığında, sistem açıldığında Windows yüklenmeden önce kimlik doğrulama (şifre, parmak izi veya smartcard) sağlamanız gerekir. Windows öncesi oturum açma fonksiyonelliği sisteme ilave güvenlik sağlar, yetkisiz kullanıcıların Windows ve bilgisayara erişimlerini önler (örn. bilgisayar çalındığında).

Yöneticiler, Windows Öncesi Oturum Açma penceresinde Windows öncesi oturum açma ayarlayabilir veya Windows öncesi (Sistem) şifresi oluşturabilir ya da değiştirebilir; eğer bu şifre zaten oluşturulmuşsa, Windows öncesi oturum açmayı bu pencereden devre dışı bırakabilirsiniz. Windows öncesi oturum açmanın ayarlanması aşağıdakileri yapacak bir sihirbaz çalıştıracaktır:

- Sistem Şifresi: Windows öncesi erişim için Sistem Şifresi (Windows öncesi şifre de denir) oluşturun. Bu şifre kullanıcının ilave kimlik doğrulama faktörlerine sahip olması durumunda yedek olarak kullanılacaktır (örn. parmak izi okuyucunun sensörünün arızalanması).
- Parmak İzi veya Smartcard: Windows öncesi oturum açmada kullanmak için parmak izi veya smartcard ayarlayın ve bu kimlik doğrulama metodunun Windows öncesi şifrenin yerine mi yoksa onunla birlikte mi kullanılacağını belirleyin.
- Single Sign On: Varsayılan olarak Windows öncesi kimlik doğrulama (şifre, parmak izi veya smartcard) otomatik olarak Windows oturumu açmanız için de kullanılır (buna "Single Sign On" denir). Bu özelliği devre dışı bırakmak için "Windows oturumu açmak istiyorum" kutusunu işaretleyin.
- Eğer Windows öncesi şifreye ek olarak BIOS Sabit Disk şifresi ayarlandıysa, Sabit Disk şifresini değiştirme veya devre dışı bırakma seçeneğiniz olacaktır.

NOT: Windows öncesi kimlik doğrulama için tüm parmak izi okuyucular etkin değildir. Eğer okuyucunuz uyumlu değilse, sadece Windows oturumu açmak için parmak izi kaydedebilirsiniz. Belirli bir parmak izi okuyucunun uyumlu olup olmadığını öğrenmek için sistem yöneticinizle görüşün veya desteklenen parmak izi okuyucular için support.dell.com adresine gidin.

Windows Öncesi Oturum Açma Devre Dışı

Bu pencereden Windows öncesi oturum açmayı devre dışı da bırakabilirsiniz; bunu yapmak için mevcut Windows öncesi (Sistem) şifrenizi girmeniz, şifrenin doğru olduğunu onaylamanız ve sonra **Devre dışı** düğmesine tıklamanız gereklidir. Windows öncesi oturum açmayı devre dışı bıraktığınızda, kaydedilmiş parmak izleri veya smartcard'lar kayıtlı kalır.

Parmak İzlerini Kaydetme / Silme

Kullanıcılar Windows öncesi veya Windows oturumu açarken kimlik doğrulama amacıyla kullanılabilecek parmak izlerini kaydedebilirler veya güncelleyebilirler. Parmak izi sekmesinde eğer varsa el görüntüsü hangi parmakların izinin kayıtlı olduğunu gösterecektir. **Başka bir tane kaydet** linkine tıkladığınızda, Parmak İzi Kayıt sihirbazı çalışır, bu sihirbaz size kayıt işlemi sırasında yardımcı olacaktır. "Kayıt" oturum açmak için bir parmak izinin kaydedilmesi demektir. Parmak izi kaydedebilmek için için düzgün şekilde kurulmuş ve yapılandırılmış geçerli bir parmak izi okuyucunuz olmalıdır.

NOT: Windows öncesi kimlik doğrulama için tüm parmak izi okuyucular kullanılamaz. Eğer uyumsuz bir okuyucuyla Windows öncesi için kayıt yapmaya çalışırsanız bir hata mesajı görüntülenir. Cihazın uyumlu olup olmadığını öğrenmek için sistem yöneticinizle görüşün veya desteklenen parmak izi okuyucular için support.dell.com adresine gidin.

Bir parmak izi kaydedilirken sizden kimliğinizi doğrulamanız için Windows şifrenizi girmeniz istenecektir. Eğer sistem ilkeleri gerektiriyorsa Windows Öncesi (Sistem) şifresi de istenecektir. Windows Öncesi şifre parmak izi okuyucuda bir sorun olması durumunda sisteme erişim için kullanılabilir.

NOTLAR:

- Kayıt işlemi sırasında en az iki parmak izi kaydetmeniz tavsiye edilir.
- Parmak izi kimlik doğrulama özelliklerine etkinleştirmeden önce parmak izlerinin düzgün bir şekilde kaydedildiğinden emin olmalısınız.
- Eğer sistemdeki parmak izi okuyucuyu değiştirirseniz, parmak izlerini yeni okuyucu ile kaydetmelisiniz. İki farklı parmak izi okuyucu arasında geçiş yapılması tavsiye edilmemektedir.
- Eğer parmak izlerini kaydederken "sensör odağını yitirdi" mesajını sürekli görürseniz, bu bilgisayarın parmak izi okuyucuyu tanımadığı anlamına gelir. Eğer parmak izi okuyucu harici ise, parmak izi okuyucuyu çıkartmak ve sonra tekrar takmak genellikle sorunu çözer.

Kayıtlı Parmak İzlerini Silme
Kayıtlı parmak izlerini **Parmak izini sil** linkine tıklayarak veya Parmak İzi Kayıt Sihirbazında kayıtlı bir parmak izi üzerine tıklayarak (seçimi kaldırarak) silebilirsiniz.

Windows öncesi kimlik doğrulama için parmak izi kaydetmiş belirli bir kullanıcıyı silmek için yönetici bu kullanıcı için kaydedilmiş tüm parmak izlerinden seçimi kaldırabilir.

NOT: Eğer parmak izi kayıt işlemi sırasında hata olursa, ilave bilgi için wave.com/support/Dell adresine bakabilirsiniz.

Smartcard Kaydet

Dell Veri Koruma | Erişim size Windows oturumu açmak veya Windows öncesi kimlik doğrulama için geleneksel (temaslı) veya temassız smartcard kullanımı seçeneği verir. Smartcard sekmesinde, **Başka bir smartcard kaydet** linkine tıklayarak Smartcard Kayıt sihirbazını çalıştırın, bu sihirbaz size kayıt işlemi sırasında yardımcı olacaktır. "Kaydetmek" oturum açmak için smartcard kullanımını ayarlamak demektir.

Kayıt gerçekleştirebilmek için düzgün şekilde kurulmuş ve yapılandırılmış geçerli bir smartcard kimlik doğrulama aygıtınız olmalıdır.

NOT: Belirli bir aygıtın uyumlu olup olmadığını öğrenmek için sistem yöneticinizle görüşün veya desteklenen smartcard listesi için support.dell.com adresine gidin.

Kayıt
Bir smartcard kaydedilirken sizden kimliğinizi doğrulamanız için Windows şifrenizi girmeniz istenecektir. Eğer sistem ilkeleri gerektiriyorsa Windows Öncesi (Sistem) şifresi de istenecektir. Windows Öncesi şifre smartcard okuyucuda bir sorun olması durumunda sisteme erişim için kullanılabilir.

Kayıt sırasında eğer ayarlanmış ise sizden smartcard PIN istenecektir. Eğer ilkeniz PIN gerektiriyorsa ve bu ayarlanmamışsa, sizden bir tane oluşturmanız istenecektir.

NOTLAR:

- Kullanıcı Windows öncesi kullanım için smartcard kaydettiğinde, bu kullanıcı silinemez.
- Standart kullanıcılar smartcard PIN değiştirebilir, yöneticiler hem yönetici PIN hem de kullanıcı PIN değiştirebilir.
- Yönetici smartcard sıfırlaması da yapabilir; sıfırlama yapıldığında smartcard tekrar kaydedilene kadar Windows oturum açma veya Windows öncesinde kimlik doğrulama için kullanılamaz.

NOT: TPM sertifika kimlik doğrulaması için yöneticiler TPM sertifikalarını Microsoft Windows smartcard kayıt işlemi üzerinden kaydedebilir. Bu uygulamayla uyumluluk için yöneticiler Smartcard CSP yerine Kriptografik Servis Sağlayıcı olarak "Wave TCG-Etkin CSP" seçmelidir. Buna ek olarak istemci için uygun Kimlik Doğrulama Tipi İlkesi ile birlikte Dell Güvenli oturum açma etkin olmalıdır.

NOT: Eğer Smartcard Servisinin çalışmadığını bildiren bir hata oluşursa, aşağıdakileri yaparak servisi başlatabilir/tekrar başlatabilirsiniz:

- Denetim Masasından Yönetim Araçları penceresine gidin, Servis seçin sonra Smartcard üzerine sağ tıklayın ve Başlat veya Tekrar Başlat seçin.
- Eğer belirli bir hata ile ilgili olarak daha ayrıntılı bilgi isterseniz, wave.com/support/Dell adresine gidin.

Self-Encrypting Drive

Dell Veri Koruma | Erişim ; sürücü donanımında veri şifreleme özelliği gömülü olan self-encrypting drives donanım tabanlı güvenlik fonksiyonlarını yönetir. Bu fonksiyonellik (sürücü kilitleme etkinken) sadece yetkisi olan kullanıcıların şifrelenmiş veriye ulaşmalarını güvence altına alır.

Self-Encrypting Drive penceresine **Self-Encrypting Drive** alt sekmesine tıklayarak ulaşılır. Bu sekme sisteminizde bir veya daha fazla self-encrypting drives (SEDs) mevcutsa görüntülenir.

Self-Encrypting Drive kurulum sihirbazını başlatmak için **Kurulum** linkine tıklayın. Bu sihirbazda, Sürücü Yöneticisi şifresi oluşturacak, bu şifreyi yedekleyecek ve sürücü şifreleme ayarlarınızı uygulayacaksınız. Self-Encrypting Drive kurulum sihirbazına sadece sistem yöneticileri erişebilir.

Önemli! Sürücü bir kez ayarlandığında, veri koruma ve sürücü kilitleme "etkindir". Sürücü kilitlendiğinde aşağıdaki davranışlar geçerlidir:

- Sürücünün gücü kapatıldığında sürücü *kilitli* moda girer.
- Kullanıcı Windows öncesi oturum açma ekranında doğru kullanıcı adı ve şifresini girmedikçe sürücü yükleme yapmaz. Sürücü kilitlemenin etkinleşmesinden önce, sürücü üzerindeki verilere bilgisayardaki tüm kullanıcılar erişebilir.
- Sürücü ikinci sürücü olarak başka bir bilgisayara bağlansa bile hala güvenlidir; sürücüdeki veriye erişmek için kimlik doğrulama gereklidir.

Sürücü ayarlandığında Self-Encrypting Drive penceresi sürücüleri ve kullanıcıların sürücü şifresini değiştirmek için kullanacağı linki gösterir. Eğer sürücü yöneticisiyseniz, bu pencereden sürücü kullanıcılarını ekleyebilir veya çıkartabilirsiniz. Eğer ayarlanmış harici bir sürücü varsa, bu pencerede görüntülenir ve kilidi açılabilir.

NOT: ikincil, harici sürücü kilitlemek için, sürücü bilgisayardan bağımsız olarak kapatılmalıdır.

Sürücü yöneticisi sürücü ayarlarını **Gelişmiş>Aygıtlar** içinden yönetebilir. Daha fazla bilgi için, bkz. Aygıt Yönetimi - Self-Encrypting Drives.

Sürücü Ayarlama

Self-Encrypting Drive kurulum sihirbazı sürücülerinizi ayarlarken size yardımcı olur. Bu işlem sırasında aşağıdaki konseptleri akılda tutmakta yarar vardır.

Sürücü Yöneticisi
Sürücü erişimlerini ayarlayan (ve Sürücü Yöneticisi şifresini ayarlayan) sistem yöneticisi haklarına sahip ilk kullanıcı Sürücü Yöneticisi olur; sürücü erişimine değişiklik yapma hakkına sahip tek kullanıcı budur. İlk kullanıcının bilinçli şekilde sürücü yöneticisi olarak ayarlanması amacıyla işleme devam edebilmek için "Anlıyorum" kutusunun işaretlenmesi gereklidir.

Sürücü Yöneticisi Şifresi
Sihirbaz sizden Sürücü Yöneticisi şifresi oluşturmanızı ve şifreyi onaylamak için tekrar girmenizi ister. Sürücü Yöneticisi şifrenizi oluşturmadan önce kimliğinizi oluşturmanız için Windows şifrenizi girmelisiniz. Geçerli Windows kullanıcısı bu şifreyi oluşturmak için yönetici haklarına sahip olmalıdır.

Yedekleme Sürücü Tanıtımları
Bir konum girin veya bir konum seçmek için **Gözat** düğmesine tıklayın, sürücü yönetici tanıtımlarınızın bir kopyasını yedekleyin.

ÖNEMLİ!

- Bu tanıtımları yedeklemeniz önemle tavsiye edilir, bunları birincil sabit diskiniz dışında bir sürücüye yedeklemeniz önerilir (örn. çıkartılabilir ortam). Aksi takdirde, eğer sürücünüze erişiminizi kaybederseniz, yedeklerinize erişemezsiniz.
- Sürücü ayarlamayı tamamladıktan sonra, sistemin bir sonraki açılışında sisteme erişebilmek için tüm kullanıcılar doğru kullanıcı adı ve şifresini (veya parmak izi) girmek zorundadır.

Sürücü Kullanıcısı Ekle

Sürücü yöneticisi sürücü için geçerli Windows kullanıcısı olan diğer kullanıcıları ekleyebilir. Sürücüye diğer kullanıcıları eklerken, yönetici kullanıcılardan ilk oturum açışta şifrelerini sıfırlamalarını isteme seçeneğine sahiptir. Kullanıcı sürücü kilidi açılmadan önce Windows öncesi oturum açma ekranında şifresini sıfırlamalıdır.

Gelişmiş Ayarlar

- *Single Sign On* - Varsayılan olarak sürücü kimlik doğrulaması için Windows öncesinde girdiğiniz Self-Encrypting Drive şifresi otomatik olarak Windows oturumu açmak için kullanılacaktır (buna "Single Sign On" denir). Bu özelliği devre dışı bırakmak için sürücü ayarlarınızı yapılandırırken "Windows oturumu açmak istiyorum" kutusunu işaretleyin.
- *Parmak iziyle Oturum Açma* - Desteklenen platformlarda, self-encrypting drive kimlik doğrulamanızı şifre yerine parmak iziyle yapmak istediğinizi belirtebilirsiniz.
- *Uyku/Bekleme (S3) Desteği* (eğer platform destekliyorsa) - Etkin olduğunda self-encrypting drive güvenli şekilde Uyku/Bekleme moduna alınabilir (S3 modu da denir) Uyku/Bekleme modundan çıkmak için Windows öncesi kimlik doğrulama gerektirecektir.

NOTLAR:

- S3 Desteği etkinken sürücü şifreleme şifreleri var olabilecek BIOS şifre sınırlamalarına tabidir. Sistem için geçerli olabilecek tüm özel BIOS şifre kısıtlamaları hakkında daha fazla bilgi için lütfen sistem donanımı üreticinize başvurunuz.
- Tüm self-encrypting drives S3 modunu desteklemez. Sürücü ayarlama sırasında, sürücünün Bekleme/Uyku modunu destekleyip desteklemediği size bildirilecektir. Bu modu desteklemeyen sürücüler için, eğer hazırda bekleme modu etkinse Windows S3 istekleri otomatik olarak hazırda bekleme isteğine dönüştürülecektir (bilgisayarınızda hazırda bekleme modunu etkinleştirmeniz önemle tavsiye edilir).
- Single Sign On (SSO) seçeneği ayarlandıktan sonra ilk oturum açışınızda, işlem Windows oturum açma isteminde duraklayacaktır. Kullanıcının kendi Windows Kimlik Doğrulama biçimini girmesi istenir, bu bilgi daha sonraki Windows Oturum Açma girişimleri için güvenli bir şekilde kaydedilir. Sistemin sonraki başlatılmasında SSO Windows oturumunu otomatik olarak açacaktır. Aynı işlem kullanıcının Windows kimlik doğrulaması değiştiğinde de gereklidir (şifre, parmak izi, Smartcard PIN). Eğer bilgisayar bir etki alanı üzerindeyse, ve etki alanı Windows oturumu açmak için ctrl+alt+del tuşlarına basılmasını gerektiriyorsa, bu politikaya uyulacaktır.

DİKKAT! Eğer **Dell Veri Koruma | Erişim** uygulamasını kaldırırsanız, önce self-encrypting drive data korumasını kaldırmanız ve sürücü kilidini açmanız gereklidir.

Self-Encrypting Drive Kullanıcı Fonksiyonları

Self-encrypting drive yöneticileri sürücü güvenliği ve kullanıcılarla ilgili tüm yönetim görevlerini yerine getirirler. Yönetici olmayan sürücü kullanıcıları sadece aşağıdaki görevleri gerçekleştirebilirler:

- Kendi sürücü şifrelerini değiştirme
- Sürücü kilidini açma

Bu görevlere **Dell Veri Koruma | ErişimSelf-Encrypting Drive** sekmesinden ulaşılabilir.

Şifre Değiştir
Bu fonksiyon ile kullanıcı yeni bir sürücü kimliği doğrulama şifresi yaratabilir. Sürücü şifresi yenisi ile değiştirilmeden önce mevcut Self-Encrypting Drive şifrenizi girmeniz gereklidir.

NOTLAR:

- Uygulama Windows şifre uzunluğu ve Windows şifre karmaşıklık politikalarını, şayet bunlar etkinleştirilmişse, zorunlu kılar. Windows şifre politikaları etkinleştirilmemişse, bir Self Encrypting Drive şifresinin maksimum uzunluğu 32 karakterdir. Bu maksimum uzunluk eğer S3 (Uyku/Bekleme) etkin değilse 127 karakterdir.
- Kullanıcının Self-Encrypting Drive şifresi, kullanıcının Windows şifresinden ayrıdır. Windows Şifre Senkronizasyonu etkin olmadığı sürece, bir kullanıcının Windows şifresi değiştiğinde veya sıfırlandığında bu durumun kullanıcının sürücü şifresi üzerinde etkisi olmaz. Ayrıntılar için Aygıtlar: Self-Encrypting Drives bölümüne bakın.
- İngilizce dışı bazı klavyelerde, self-encrypting drive şifresi içinde kullanılamayacak kısıtlanmış karakterler seti bulunmaktadır. Windows Şifresi kısıtlanmış karakterlerden birini içeriyorsa ve Windows Şifre Senkronizasyonu etkinse, senkronizasyon başarısız olacak ve bir hata mesajı gösterilecektir.

Sürücü Kilidini Aç
Sürücü Kilidini Aç kayıtlı sürücü kullanıcısının kilitli sürücünün kilidini açmasını sağlar. Sürücü kilitleme devredeyken, bilgisayar güç girişi kapatıldığında sürücü kilitli moda geçer. Sisteme tekrar güç verildiğinde, Windows öncesi oturum açma ekranından şifrenizi girerek sürücü kimlik doğrulaması yapmanız gerekir.

NOTLAR:

- Eğer birden fazla self-encrypting drive kullanıcı hesabı bilgisayarda aktifse güç tasarruf moduna girememe (örn. Uyku/Bekleme Hazırda Beklet) durumu gerçekleşebilir.
- Windows öncesi kimlik doğrulama ekranında, uygulama sürümlerinde sürücü kullanıcı adları için geçici olarak "Kullanıcı 1", "Kullanıcı 2", vb kullanılmıştır, bu sürümler şu diller için yerelleştirilmiştir: Çince, Japonca, Korece ve Rusça.

Gelişmiş Seçenekler

Dell Veri Koruma | Erişim içindeki gelişmiş seçenekler yönetici ayrıcalıklarına sahip kullanıcının uygulamanın aşağıdaki yönlerini kontrol etmesini sağlar:

Bakım
Şifreler
Aygıtlar

NOT: Sadece yönetici ayrıcalıklarına sahip kullanıcılar Gelişmiş seçenekler içinde değişiklik yapabilir; standart kullanıcılar ayarları görebilir ancak değişiklik yapamazlar.

Bakım

Bakım penceresi yönetici tarafından Windows oturum açma tercihlerini ayarlamak, sistemi yeni amaca hazırlamak için sıfırlamak veya sistemin güvenlik donanımındaki kullanıcı tanıtımlarını arşivlemek ya da geri yüklemek için kullanılabilir. Ayrıntılar için aşağıdaki balıklara bakın:

Erişim Tercihleri
Sistem Sıfırlama
Tanıtımları Arşivle & Geri Yükle

Erişim Tercihleri

Erişim Tercihleri penceresi yöneticinin sistemin tüm kullanıcıları için Windows oturum açma tercihlerini belirlemesini sağlar.

Dell Güvenli oturum açma etkin
Standart Windows ctrl-alt-delete ekranını değiştirme seçeneği Windows erişimi için Windows şifresi dışında (veya buna ek olarak) farklı kimlik doğrulama faktörleri kullanmanızı mümkün kılar. Windows oturum açma işleminin güvenliğini artırmak için ikinci kimlik doğrulama faktörü olarak parmak izi ekleyebilirsiniz. Windows oturumu açmak için smartcard veya TPM sertifikası gibi ilave kimlik doğrulama faktörleri de eklenebilir.

NOTLAR:

- Dell Güvenli oturum açmayı etkinleştirmek sistemdeki tüm kullanıcıları etkiler.
- Bu seçeneğin kullanıcılar parmak izlerini veya smartcard'larını kaydettikten SONRA etkinleştirilmesi tavsiye edilir.
- Bu seçenek ayarlandıktan sonraki ilk oturum açışınızda, Windows kimlik doğrulamasını standart ilkeye göre yapmanız istenecek, daha sonra bir sonraki başlatma sırasında yeni kimlik doğrulama faktörlerini kullanmanız gerekecektir.

Dell Güvenli oturum açmayı devre dışı bırakma
Bu seçenek Windows oturumu açarken tüm **Dell Veri Koruma | Erişim** fonksiyonlarını devre dışı bırakır. Bu seçildiğinde standart Windows oturum açma ilkelerinize döneceksiniz.

NOTLAR:

- Eğer oturum açmaya çalışırken Güvenli Windows oturumu açma ile ilgili bir hata olursa, Dell Güvenli oturum açma seçeneğini devre dışı bırakın ve sonra tekrar etkinleştirin.
- Eğer belirli bir hata ile ilgili olarak daha ayrıntılı bilgi isterseniz, wave.com/support/Dell adresine gidin.

Sistem Sıfırlama

Sistem Sıfırlama fonksiyonu platformdaki tüm güvenlik donanımlarında bulunan tüm kullanıcı verilerini temizlemek için kullanılır; bu örneğin bir bilgisayarı farklı bir amaç için yapılandırmak amacıyla kullanılır. Bu seçenek Windows kullanıcı şifreleri dışında sistemdeki tüm şifreleri ve bunun yanında donanım cihazlarındaki tüm verileri siler (örn. ControlVault, TPM ve parmak izi okuyucular). Self-encrypting drives için bu fonksiyon veri korumasını devre dışı bırakır böylelikle sürücü halen kullanılabilir.

Sistemi sıfırladığınızı anladığınızı onaylamanız ve sonra **İleri** üstüne tıklamanız gereklidir. Sistemi sıfırlamak için eğer ayarlıysa her güvenlik aygıtının şifresini girmeniz istenecektir:

- TPM Sahibi
- ControlVault Yöneticisi
- BIOS Yöneticisi
- BIOS Sistem (Windows öncesi)
- Sabit Disk (BIOS)
- Self-Encrypting Drive Yöneticisi

NOT: Self-encrypting drives için sürücünün tüm kullanıcılarının şifreleri değil Sürücü Yönetici şifresi gereklidir.

Önemli! Sistemi sıfırladığınız zaman silinen verileri geri kurtarmanın tek yolu önceden kaydedilmiş arşivi geri yüklemektir. Eğer bir arşiviniz yoksa, bu veri geri kurtarılamaz. Self-encrypting drive için, sadece kurulum verisi silinir; sürücü üzerindeki kişisel hiç bir veri silinmez.

Tanıtım Arşivleme & Geri Yükleme

Tanıtımları Arşivle ve Geri Yükle özelliği ControlVault ve Trusted Platform Module (TPM) içinde kayıtlı tüm kullanıcı tanıtımlarını (oturum açma ve şifreleme bilgisi) yedeklemek ve geri yüklemek için kullanılır. Bu verinin yedeklenmesi bir bilgisayara yeniden provizyon sağlanması veya donanım arızası sırasında verinin kurtarılması açısından önemlidir. Bu durumda, tanıtımlarınızın tümünü kaydedilmiş arşiv dosyasından yeni bilgisayarınıza aktarabilirsiniz.

Tanıtımları arşivleme ve geri yüklemeyi tek bir kullanıcı için veya sistemdeki tüm kullanıcılar için seçebilirsiniz.

Kullanıcı tanıtımları kaydedilmiş parmak izleri ve smartcard verisi ve TPM içinde kayıtlı anahtarlar gibi Windows öncesi kullanıcı verilerinden oluşur. TPM güvenli uygulamalar tarafından istenen şekilde anahtarlar oluşturur; örneğin bir dijital sertifika oluşturma TPM içinde anahtarlar oluşturacaktır.

NOT: TPM anahtarlarının **Dell Veri Koruma | Erişim** içinde arşivlenip arşivlenemeyeceğini belirlemek için lütfen güvenlik uygulamalarının belgelerine başvurun. Genel olarak, anahtar oluşturmak için “Wave TCG Enabled CSP” kullanan uygulamalar desteklenmektedir.

Tanıtımları Arşivleme
Tanıtımları arşivlemek için aşağıdakileri yapmalısınız:

- Tanıtımları kendiniz için mi yoksa sistemdeki tüm kullanıcılar için mi arşivleyeceğinizi belirleyin.
- Sistem (Windows öncesi) şifresini, ControlVault Yönetici şifresini ve TPM Sahip şifresini girerek güvenlik donanımı için kimlik doğrulama sağlayın.
- Tanıtım yedekleme şifresi oluşturun.
- **Gözat** düğmesini kullanarak bir arşiv konumu belirleyin. Sabit disk hatalarına karşı koruma sağlamak için USB flash sürücü veya ağ sürücüsü gibi çıkartılabilir ortam olan bir arşiv konumu belirlemelidir.

Önemli Notlar:
- Lütfen arşiv konumunu not edin, kullanıcı tanıtım bilgilerini geri yüklemek için bu bilgilere ihtiyaç duyacaktır.
- Verinin geri yüklenebilmesi için tanıtım yedekleme şifresini not edin. Bu şifre kurtarılamadığından bu işlem çok önemlidir.
- Kullanıcı TPM Sahip Şifresini bilmiyorsa, lütfen sistem yöneticisiyle bağlantı kurun veya bilgisayarın TPM kurulum talimatlarına bakın.

Tanıtımları Geri Yükleme
Tanıtımları geri yüklemek için aşağıdakileri yapmalısınız:

- Tanıtımları kendiniz için mi yoksa sistemdeki tüm kullanıcılar için mi geri yükleyeceğinizi belirleyin.
- Arşiv konumunu bulun ve arşiv dosyasını seçin.
- Arşivi ayarladığınızda oluşturulan tanıtım yedekleme şifresini girin.
- Sistem (Windows öncesi) şifresini, ControlVault Yönetici şifresini ve TPM Sahip şifresini girerek güvenlik donanımı için kimlik doğrulama sağlayın.

NOTLAR:
- Tanıtımları geri yüklemenin başarısız olduğunu bildiren bir hata mesajı alırsanız ve geri yüklemeyi birden fazla kez denediyseniz, farklı bir arşivi geri yüklemeyi deneyin. Eğer bu başarılı olmazsa, başka bir tanıtım arşivi oluşturun ve bu yeni arşivi geri yüklemeyi deneyin.

- Eğer TPM anahtarlarının geri yüklenemediğini bildiren bir hata mesajı alırsanız, tanıtım arşivi oluşturun, sonra BIOS içinden TPM silin. TPM'i silin, bilgisayarınızı yeniden başlatın, yedeklemeyi başlatırken **F2** tuşuna basarak BIOS ayarlarına girin ve sonra Güvenlik>TPM Güvenlik içine girin. Daha sonra TPM sahipliğini yeniden oluşturun ve tanıtımları geri yüklemeyi tekrar deneyin.
- Eğer belirli bir hata ile ilgili olarak daha ayrıntılı bilgi isterseniz, wave.com/support/Dell adresine gidin.

Şifre Yönetimi

Yönetici Şifre Yönetimi penceresinden sisteminizdeki tüm güvenlik şifrelerini oluşturabilir veya değiştirebilir:

- Sistem (Windows Öncesi olarak da bilinir)*
- Yönetici*
- Sabit Disk*
- ControlVault
- TPM Sahibi
- TPM Ana
- TPM Şifre Kasası
- Self-Encrypting Drive

NOTLAR:

- Sadece mevcut platform konfigürasyonu için uygulanabilir şifreler gösterilecektir; bu yüzden bu pencere sistem konfigürasyonu ve durumuna göre değişecektir.
- Yukarıdaki şifrelerden yanlarında * olanlar BIOS şifreleridir ve sistem BIOS üzerinden de değiştirilebilirler.
- BIOS yöneticisi şifre değişikliklerini kabul etmediyse BIOS-seviye şifreleri oluşturulamaz veya değiştirilemez.
- Self-encrypting drive için **ayarla** linkine tıklanması Self-Encrypting Drive ayarlama sihirbazını çalıştırır; **yönet** üstüne tıklamak kullanıcının bir veya daha fazla Self-Encrypting Drive şifresini değiştirmesine izin verir.
- TPM Şifre Kasası için **yönet** linkine tıklamak TPM anahtarlarınızı koruyan şifreleri görüntüleyebileceğiniz veya değiştirebileceğiniz bir pencere açar. Şifre gerektiren bir TPM anahtarı oluşturulduğunda, şifre rasgele oluşturulur ve kasaya konur. TPM Ana şifre oluşturmadıkça TPM Şifre Kasasını yönetemezsiniz.

Windows Şifre Karmaşıklık Kuralları

Dell Veri Koruma | Erişim aşağıdaki şifrelerin makine için geçerli Windows şifre karmaşıklık kurallarına uygun olduğunu garanti eder:

- TPM Sahip şifresi

Bir makinenin Windows şifre karmaşıklığını belirlemek için şu adımları izleyin:

1. Denetim Masası'na gidin.
2. Yönetimsel Araçlar'a çift tıklayın.
3. Yerel Güvenlik Politikası'na çift tıklayın.
4. Hesap Politikaları'nı genişletin ve Şifre Politikası'nı seçin.

Aygıtlar

Aygıtlar penceresi yönetici tarafından sisteme bağlı tüm güvenlik aygıtlarının yönetilmesi amacıyla kullanılır. Her aygıt için durumu ve firmware sürümü gibi bilgileri görüntüleyebilirsiniz. Her aygıt için bilgileri görüntülemek için **göster** üstüne veya bu bölümü gizlemek için **gizle** üstüne tıklayın. Platformunuzda hangilerinin bulunduğuna bağlı olarak yönetilebilecek aygıtlar şunlardır:

Trusted Platform Module (TPM)
ControlVault®
Self-Encrypting Drive(s)
Kimlik Doğrulama Aygıt Bilgisi

Trusted Platform Module (TPM)

Dell Veri Koruma | Erişim ile TPM içindeki gelişmiş özelliklerin kullanılabilmesi için TPM güvenlik çipi etkin olmalı ve TPM sahipliği oluşturulmuş olmalıdır.

Aygıt Yönetimi içindeki Trusted Platform Module penceresi sadece sisteminizde TPM algılandığında gösterilir.

TPM Yönetimi

Bu fonksiyonlar sistem yöneticisinin sistemdeki TPM'i yönetmesini sağlar.

Durum

TPM için *aktif* veya *inaktif* durumunu gösterir. "Aktif" durumunun anlamı TPM'in BIOS içinde etkinleştirildiği ve ayarlama için hazır olmasıdır (örn. sahiplik alınabilir). TPM aktif (etkin) değilse TPM yönetilemez ve güvenlik özelliklerine erişilemez.

Eğer sistemde TPM algılandıysa ama aktif değilse (etkin), sistem BIOA'a girmeden bu penceredeki **aktifleştir** linkine tıklayarak etkinleştirebilirsiniz. TPM etkinleştirildikten sonra bilgisayarın yeniden başlatılması gereklidir. Yeniden başlatma sırasında bazı durumlarda değişiklikleri kabul edip etmediğiniz sorulabilir.

NOT: Bu uygulamanın içinde TPM etkinleştirme (aktifleştirme) tüm platformlarda desteklenmeyebilir. Eğer desteklenmiyorsa, sistem BIOS içinden etkinleştirmelisiniz. Bunu yapmak için sisteminizi yeniden başlatın, Windows yüklenmeden önce **F2** tuşuna basarak BIOS ayarlarına girin sonra Güvenlik>TPM Güvenlik içine girin ve TPM'i aktifleştirin.

Ayrıca buradan TPM'i *deaktive* de edebilirsiniz , bunun için **deaktive et** linkine tıklayın; TPM'i deaktive etmek gelişmiş güvenlik özellikleri için kullanılamamasına sebep olur. Bununla birlikte deaktive etmek TPM ayarlarını değiştirmez veya silmez ya da TPM içinde saklı bilgileri veya anahtarları değiştirmez.

Sahipli

sahipliği durumunu gösterir (örn. "sahipli") ve TPM sahibi oluşturmanıza ya da değiştirmenize izin verir. Güvenlik özelliklerinin kullanılabilmesi için TPM sahipliği oluşturulmalıdır. Sahiplik oluşturulmadan önce, TPM etkin (aktifleştirilmiş) olmalıdır.

Sahiplik oluşturma işlemi kullanıcının (yönetici ayrıcalıklarına sahip olmalıdır) TPM Sahip şifresi oluşturmasından oluşur. Bu şifre tanımlandıktan sonra sahiplik oluşturulmuştur ve TPM kullanıma hazırdır.

NOT: TPM Sahip şifresi sisteminizin Windows şifre karmaşıklık kurallarına uygun olmalıdır.

Önemli! TPM Sahip şifresini unutmamanız veya kaybetmemeniz önemlidir, çünkü bu şifre **Dell Veri Koruma | Erişim** içinde TPM gelişmiş güvenlik fonksiyonları için gereklidir

Kilitli

TPM için *kilitli* veya *kilit açık* durumunu gösterir. "Kilitleme" TPM'in güvenlik özelliğidir; TPM belirlenen sayıda yanlış TPM sahip şifresi girişi yapıldıktan sonra kilitli duruma geçer. TPM sahibi TPM kilidini buradan açabilir; TPM Sahip şifresinin girilmesi gereklidir.

NOTLAR:

- Eğer TPM sahipliğinin oluşturulamadığını belirten bir hata oluşursa, sistem BIOS içinden TPM'i silin ve sahipliği oluşturmayı tekrar deneyin. TPM'i silmek için, bilgisayarınızı yeniden başlatın, yedeklemeyi başlatırken **F2** tuşuna basarak BIOS ayarlarına girin ve sonra Güvenlik>TPM Güvenlik içine girin.

- Eğer TPM Sahip şifresinin değiştirilemediğini belirten bir hata oluşursa, TPM verisini arşivleyin (tanıtım arşivi), BIOS içinden TPM'i silin, TPM sahipliğini yeniden oluşturun ve TPM verisini geri yükleyin (tanıtımları geri yükleyin).
- Eğer belirli bir hata ile ilgili olarak daha ayrıntılı bilgi isterseniz, wave.com/support/Dell adresine gidin.

Dell ControlVault®

Dell ControlVault® (CV) Windows öncesi oturum açma (örn. kullanıcı şifreleri veya kaydedilmiş parmak izleri) süresince kullanılan kullanıcı tanıtımlarının saklanması için kullanılan güvenli bir donanımdır. **Aygıt Yönetimi** içindeki ControlVault penceresi sadece sisteminizde ControlVault algılandığında gösterilir.

ControlVault Yönetimi

Bu fonksiyonlar sistem yöneticisinin sistemdeki ControlVault'u yönetmesini sağlar.

Durum
ControlVault için *aktif* veya *inaktif* durumunu gösterir. "İnaktif" durumu ControlVault'un sisteminizde depolama için kullanılamayacağını gösterir. Sisteminizde ControlVault olup olmadığını belirlemek için Dell sistem dokümantasyonuna bakın.

Şifre
ControlVault Yönetici şifresinin ayarlanıp ayarlanmadığını gösterir, şifre oluşturmanıza veya değiştirmenize izin verir (eğer ayarlanmış bir şifre varsa). Sadece sistem yöneticileri bu şifreyi oluşturabilir veya değiştirebilir. Aşağıdakileri yapabilmek için ControlVault Yönetici şifresi oluşturulmalıdır:

- Tanıtım arşivleme veya geri yükleme gerçekleştirmek için.
- Kullanıcı verilerini silmek için (tüm kullanıcılar).

NOT: Eğer ControlVault Yönetici şifresi oluşturulmadan arşivleme veya geri yükleme denenirse, bir şifre oluşturması istenecektir (eğer yönetici iseler).

Kayıtlı Kullanıcılar
Herhangi bir kullanıcının ControlVault içinde kayıtlı kullanıcı tanıtımlarını (örn. şifreler, parmak izi veya smartcard verisi) kaydedip kaydetmediğini gösterir.

Kullanıcı Verisi Sil
ControlVault içindeki verinin bazı zamanlarda silinmesi gerekebilir; örneğin eğer kullanıcılar kimlik doğrulama için Windows öncesi tanıtımları kaydetmek veya kullanmakta sorun yaşıyorlarsa. ControlVault içindeki tüm veriler tek kullanıcı veya tüm kullanıcılar için bu pencereden silinebilir.

Platform içindeki tüm kullanıcı verilerinin silinmesi için ControlVault Yönetici şifresi girilmelidir. Eğer kayıtlı Windows öncesi tanıtım varsa, sizden Sistem (Windows öncesi) şifresini girmeniz de istenecektir. Tüm kullanıcı verilerini sildiğinizde, ControlVault Yönetici şifresi ve Sistem şifresi sıfırlanır; unutmayın ControlVault Yönetici şifresini silmenin tek yolu budur.

NOT: Tüm kullanıcı verilerini sildiğinizde, bizden bilgisayarınızı yeniden başlatmanız istenir. Sistemin düzgün çalışması için yeniden başlatmak gereklidir.

Tek kullanıcı tanıtımlarını silmek için ControlVault Yönetici şifresinin ayarlı olması gerekli değildir. **Kullanıcı verisini sil** üstüne tıkladığınızda, ControlVault tanıtımlarını silmek istediğiniz kullanıcıyı seçmeniz istenecektir. Bir kullanıcıyı seçtiğinizde, sizden Sistem şifresi istenir (sadece eğer Windows öncesi tanıtımlar kayıtlıysa).

NOTLAR:

- Eğer ControlVault Yönetici şifresinin oluşturulamadığını bildiren bir hata oluşursa, tanıtımlarınızı arşivlemeli, ControlVault içindeki tüm kullanıcı verilerini silmeli, bilgisayarınızı yeniden başlatmalı ve şifreyi oluşturmayı yeniden denemelisiniz.

- Tek bir kullanıcı için ControlVault içindeki tanıtımların silinemediğini bildiren bir hata oluşursa, tanıtımlarınızı arşivlemeli, tüm kullanıcı verilerini silmeyi denemeli ve sonra tek kullanıcı için veriyi silmeyi tekrar denemelisiniz.
- Eğer tüm kullanıcılar için tanıtımların ControlVault içinden silinemediğini bildiren bir hata oluşursa, sistem sıfırlama denemelisiniz. **Önemli!** Sıfırlama gerçekleştirmeden önce Sistem Sıfırlama yardım başlığını gözden geçirin, çünkü bu işlem TÜM kullanıcı güvenlik verilerini silecektir.
- Eğer ControlVault ve TPM verilerinin yedeklenemediğini bildiren bir hata oluşursa, sistem BIOS içinden TPM'i devre dışı bırakın. Bu bilgisayar yeniden başlatılarak, başlatma sırasında **F2** tuşuna basarak BIOS ayarlarına girilerek ve sonra Güvenlik>TPM Güvenlik içine girilerek yapılır. Sonra TPM'i tekrar etkinleştirin ve ControlVault verilerinizi arşivlemeyi tekrar deneyin.
- Eğer belirli bir hata ile ilgili olarak daha ayrıntılı bilgi isterseniz, wave.com/support/Dell adresine gidin.

Self-Encrypting Drives: Gelişmiş

Dell Veri Koruma | Erişim sürücü donanımında veri şifreleme özelliği gömülü olan self-encrypting drives donanım tabanlı güvenlik fonksiyonlarını yönetir. Bu yönetim sürücü kilitleme etkinken sadece yetkisi olan kullanıcıların şifrelenmiş veriye ulaşmalarını güvence altına alır.

Aygıt Yönetim içindeki Self-Encrypting Drive penceresi sadece sisteminizde bir veya daha fazla self-encrypting drives (SED) bulunduğunda görüntülenir.

Önemli! Sürücü bir kez ayarlandığında, self-encrypting drive veri koruma ve sürücü kilitleme "etkindir".

Sürücü Yönetimi

Bu fonksiyonlar, sürücü yöneticisinin sürücü güvenlik ayarlarını yönetmesini mümkün kılar. Sürücü güvenlik ayarlarında yapılan değişiklikler, sürücü kapatıldıktan sonra etkili hale gelir.

Veri Koruma

Self-encrypting drive veri koruma için *etkin* veya *devre dışı* durumunu görüntüler. "Etkin" durumu sürücü güvenliğinin ayarlandığı anlamına gelir; bununla birlikte, sürücü *kilitleme* açılana kadar kullanıcılar sürücüye erişim için Windows öncesi kimlik doğrulama yapmak zorunda olmayacaktır.

Self-encrypting drive veri korumasını buradan devre dışı bırakabilirsiniz. Devre dışı bırakıldığında, self-encrypting drive tüm gelişmiş güvenlik fonksiyonları kapalı hale gelir ve sürücü standart sürücü gibi çalışır. Veri güvenliğini devre dışı bırakmak aynı zamanda sürücü yöneticilerinin ve sürücü kullanıcılarının tanıtımları da dahil olmak üzere tüm güvenlik ayarlarını siler. Bununla birlikte bu fonksiyon sürücüdeki hiçbir kullanıcı verisini değiştirmez veya silmez.

Kilitleme

Self-encrypting drive veri koruma için *etkin* veya *devre dışı* durumunu görüntüler. Kilitli sürücü davranışlarıyla ilgili bilgi için Self-Encrypting Drive başlığına bakın.

Sürücü kilitlemeyi geçici olarak devre dışı bırakmanız gerekebilir, bunu buradan yapabilirsiniz. Sürücü kilitleme devre dışı bırakıldığında sürücüye erişmek için hiç bir tanıtım gerekmeyeceğinden ve platformdaki tüm kullanıcılar sürücü verilerine ulaşabileceğinden bu önerilmez. Sürücü kilitlemeyi devre dışı bırakmak sürücü yöneticileri ve sürücü kullanıcıları tanıtımları da dahil hiç bir güvenlik ayarını silmez.

DİKKAT! Eğer **Dell Veri Koruma | Erişim** uygulamasını kaldırırsanız, önce self-encrypting drive data korumasını kaldırmanız ve sürücü kilidini açmanız gereklidir.

Sürücü Yöneticisi

Geçerli sürücü yöneticisini gösterir. Sürücü yöneticisi hangi kullanıcının sürücü yöneticisi olduğunu buradan değiştirebilir. Yeni yönetici yönetici ayrıcalıklarına sahip geçerli Windows kullanıcısı olmalıdır. Sistemde sadece bir sürücü yöneticisi olabilir.

Sürücü Kullanıcıları

Kayıtlı sürücü kullanıcılarını ve mevcut olarak kaydedilmiş kullanıcıların sayısını gösterir. Desteklenen maksimum kullanıcı sayısı self-encrypting drive ile ilişkilidir (şu anda Seagate sürücüler için 4 kullanıcı, Samsung sürücüler için 24 kullanıcıdır).

Windows Şifresi Senk
Windows şifresi senkronizasyonu (WPS) özelliği kullanıcıların Self-Encrypting Drive şifrelerinin Windows şifreleri ile aynı olmasını otomatik olarak sağlar. Bu fonksiyon sürücü yöneticisi için zorunlu değildir, sadece sürücü kullanıcıları için kullanılabilir. WPS fonksiyonelliği şifrelerin belirli sıklıkta değiştirilmesi gereken (örn. 90 günde bir) kurumsal ortamlarda kullanılabilir; bu seçenek etkin olduğunda tüm kullanıcıların self-encrypting drive şifreleri Windows şifreleri değiştirildiğinde otomatik olarak güncellenecektir.

NOT: Windows şifresi senkronizasyonu (WPS) etkin olduğunda, bir kullanıcının Self-Encrypting Drive şifresi değiştirilemez; sürücü şifresinin otomatik olarak güncellenmesi için Windows şifresinin değiştirilmesi gereklidir.

Son Kullanıcı Adını Hatırla
Bu seçenek etkin olduğunda, girilen son kullanıcı adı Windows öncesi oturum açma ekranının **Kullanıcı adı** alanında varsayılan olarak gösterilecektir.

Kullanıcı Adı Seçimi
Bu seçenek etkin olduğunda, kullanıcılar Windows öncesi oturum açma ekranının **Kullanıcı adı** alanında tüm sürücü kullanıcı adlarını görebilirler.

Kriptografik Sil
Bu seçenek self-encrypting drive üzerindeki tüm verinin "silinmesi" için kullanılabilir. Bu veriyi gerçekten silmez ancak veriyi şifrelemek için kullanılan anahtarları siler ve bu şekilde veriyi kullanılamaz hale getirir. Kriptografik silme sonrasında veriyi kurtarmanın yolu yoktur, ayrıca self-encrypting drive veri koruma devre dışı kalır ve sürücü yeniden yapılandırma için hazır hale gelir.

NOTLAR:

- Eğer self-encrypting drive yönetim fonksiyonları ile ilgili bir hata oluşursa, bilgisayarı tamamen kapatın (yeniden başlatma değil) ve yeniden başlatın.
- Eğer belirli bir hata ile ilgili olarak daha ayrıntılı bilgi isterseniz, wave.com/support/Dell adresine gidin.

Kimlik Doğrulama Aygıt Bilgisi

Aygıt Yönetim içindeki Kimlik Doğrulama Aygıt Bilgisi sisteme bağlı olan tüm kimlik doğrulama aygıtlarının bilgi ve durumlarını gösterir (örn. parmak izi okuyucu, geleneksel veya temassız smartcard okuyucu).

Teknik Destek

Dell Veri Koruma | Erişim yazılımı için teknik destek http://www.wave.com/support.dell.com adresinde bulunabilir.

Wave TCG Enabled CSP

Wave Systems Trusted Computing Group (TCG)-etkin Kriptografik Servis Sağlayıcı (CSP) **Dell Veri Koruma | Erişim** uygulamasına dahildir ve CSP ne zaman gerekirse kullanıma uygundur – ya uygulamada içinden doğrudan çağrılır ya da kurulu CSP'ler listesi içinden seçilebilir. Mümkün olduğunda, “Wave TCG-Enabled CSP” seçerek TPM'in anahtarları oluşturduğundan ve bunların şifrelerinin **Dell Veri Koruma | Erişim** tarafından yönetildiğinden emin olun.

Wave Systems TCG-enabled CSP uygulamaların TCG-uyumlu platformlardaki fonksiyonları doğrudan MSCAPI üzerinden kullanmasını mümkün kılar. TCG-etkin MSCAPI CSP modülü, TPM'de asimetrik anahtar işlevi sunar ve TPM tarafından sağlanan geliştirilmiş güvenliği Trusted Software Stack (TSS) sağlayıcısının üreticiye özel gerekliliklerinden bağımsız olarak artırır.

NOT: Eğer Wave TCG-enabled CSP tarafından oluşturulan TPM anahtarları şifre gerektiriyorsa ve kullanıcı TPM Ana şifre oluşturmuşsa, her bir anahtar şifresi rasgele şekilde oluşturulur ve TPM Password Vault içinde saklanır.