Intune ile Bitlocker Politikalarının Yönetimi

Endpoint Cihaz güvenliği birçok IT yöneticisinin ön planda tuttuğu konuların başında yer almaktadır. Kullanım esnasında birçok nedenden dolayı bilgisayarlar güvenlik açığı ile karşı karşıya kalabilir. Bitlocker, Windows işletim sistemi ile karşınıza çıkan, veri ve dosya güvenliği şifreleme desteği sunan bir sistemdir.

Bitlocker ile sabit diskleri ya da taşınabilir diskleri şifreleyerek güvenli hale getirebilirsiniz. Bu şifreleme işleminden sonra sürücülerin içinde bulunan ve sonradan oluşturulan dosyalarda şifrelenmiş olmakta. Sistem diskimiz ve diğer disklerimizi de şifreleme yaptığımızda 3rd parti kişiler tarafından Bitlocker ile şifrelenen diskimiz içerisindeki bilgilerimize erişilemez olacaklardır. Bitlocker bilgisayarın yeniden başlatılması sırasında bios ve açılış ayarlarında bir sorun algılar ise güvenlik şifresi girilmesini zorunlu kılmaktadır.

Intune ile Bitlocker politikalarının yaygınlaştırılmasını incelersek;

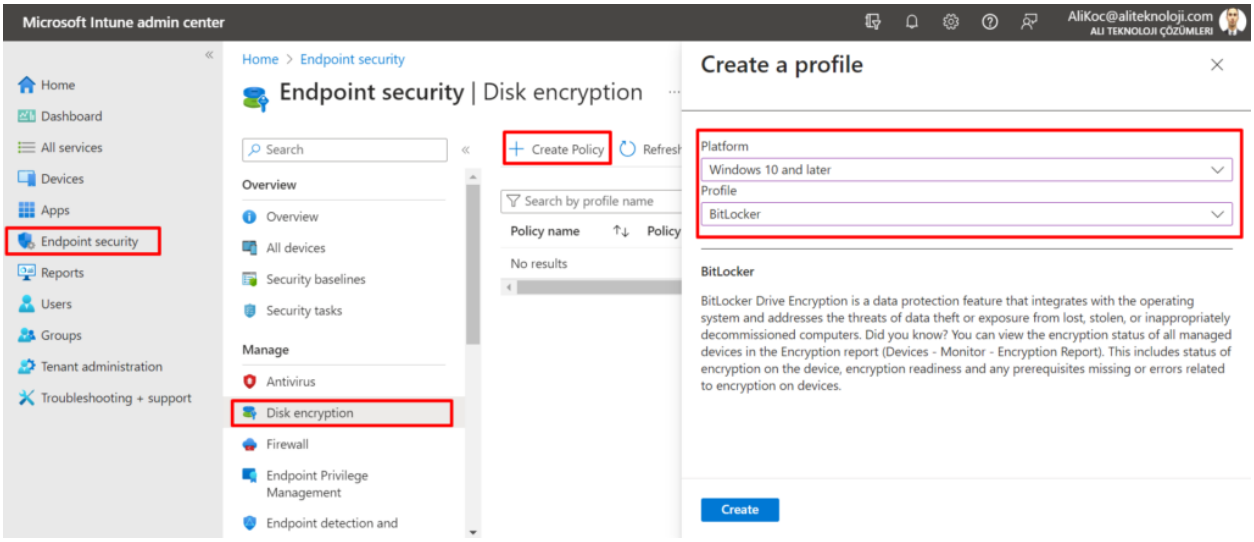
Gereksinimler:

- Intune License.
- Entra or Hybrid joined device.
- Windows 10/11.
- The device must have a TPM or Chip v. 1.2 or later (most new devices have 2.0).
- BIOS set to native EUFI.

BitLocker Yönetimi için Yetki Gereksinimleri:

- Global Admin.
- Intune Admin
- Helpdesk Operator.

İlk olarak Intune Admin Center’a giriş yapıyoruz, Sonrasında Endpoint Security> DiskEncryption> Create Policy “+” seçeneğini seçiyoruz.

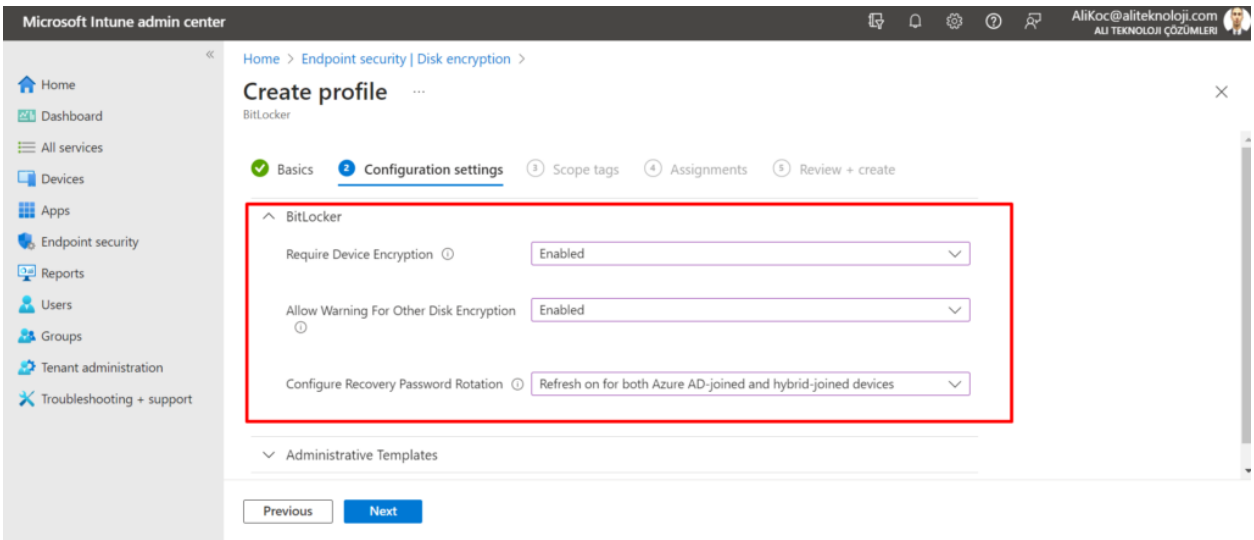


BitLocker Politikalarının Konfigurasyonu:

Require Device Encryption: Bu ilkeyi Devre Dışı Bırakırsanız, bu cihazdaki şifrelemeyi kapatmaz, ancak kullanıcıdan açmasını istemeyi durdurur. Ben etkinleştireceğim.

Allow Warning for Other Disk Encryption: Bu ilke =1 değerine ayarlıdır, bu nedenle kullanıcı varsayılan olarak uyarı işaretlerini görecektir, Devre Dışı Bırakırsanız , uyarı işaretleri görünmeyecektir.

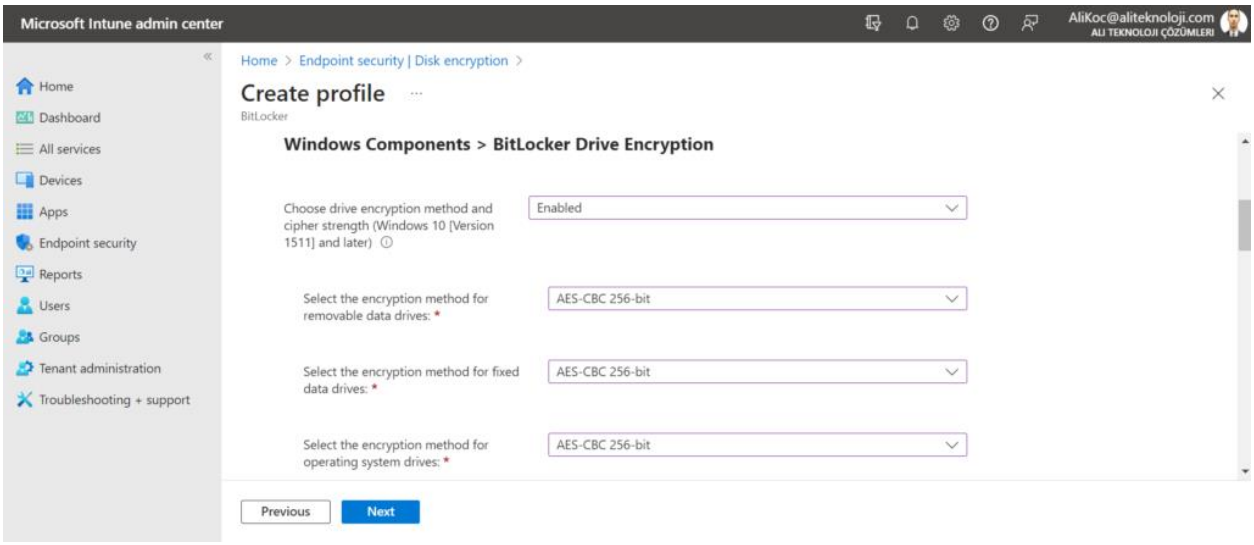
Allow Standard User Encryption: Diğer Disk Şifreleme için bu politika varsayılan olarak 0 değerinde ve yapılandırmayacak şekilde ayarlanmıştır, yani oturum açan kullanıcı yönetici olmayan biriyse, politika herhangi bir sürücüde şifrelemeyi etkinleştirmeye çalışmayacaktır, 1 değerini etkinleştirirseniz, oturum açan kullanıcı standart bir kullanıcı olsa bile politika tüm sabit sürücülerde şifrelemeyi etkinleştirmeye çalışacaktır.



Administrative Templets Seçenekleri

BitLocker Drive Encryption: Bu ilke ayarını Etkinleştirirseniz, sabit data sürücüleri, işletim sistemi sürücüleri ve çıkarılabilir data sürücüleri için ayrı ayrı bir şifreleme algoritması ve anahtar şifre gücü yapılandırabilirsiniz.

Bu ilke ayarını Devre Dışı Bırakırsanız veya yapılandırmazsanız, BitLocker aynı bit gücüne (128 bit veya 256 bit) sahip AES standartlarını kullanacaktır.

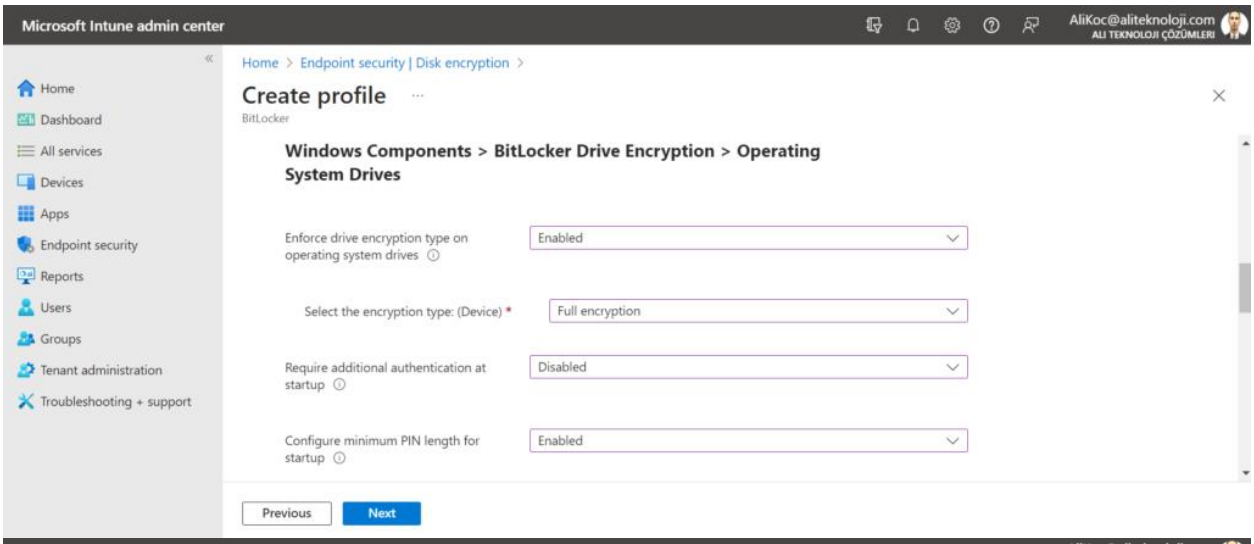


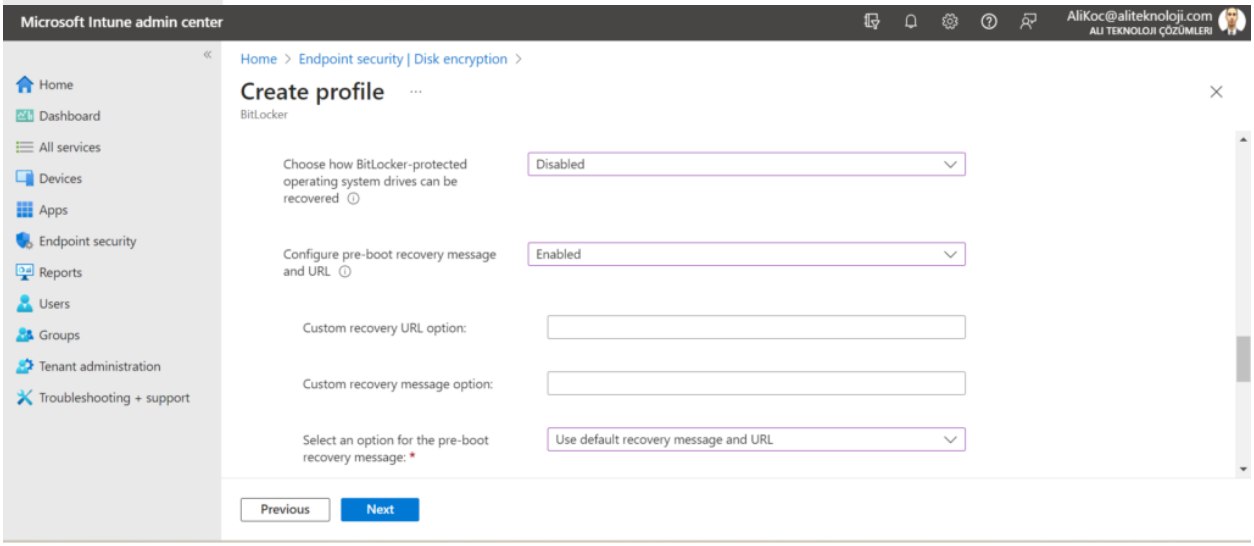
Operating System Drives: Bu politika ile, şifreleme türünü yapılandırabilirsiniz. Devre Dışı Bırakırsanız veya Yapılandırmazsanız, son kullanıcının şifreleme türünü seçmesine izin verecektir.

Etkinleştirirseniz, bu, kullanıcının Full encyrption veya space only seçeneklerinden birini seçmesine izin vererek şifreleme türünü seçmenize olanak tanır.

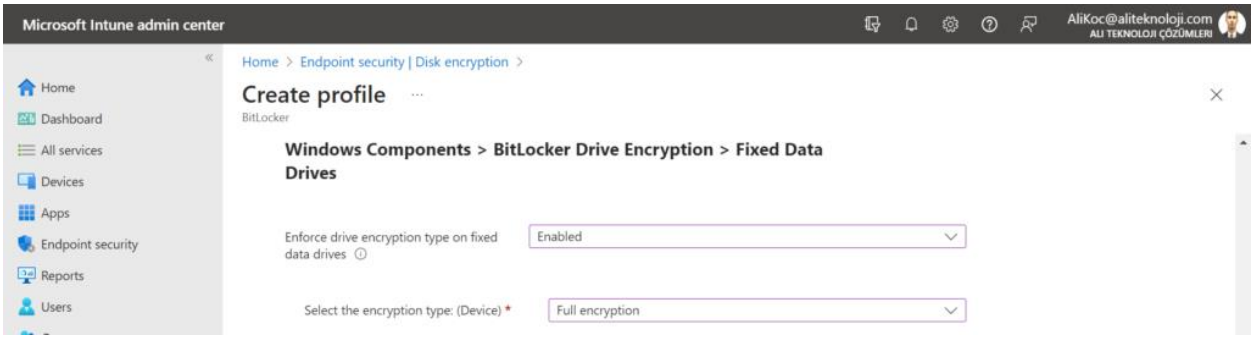
Require additional authentication at startup: Devre Dışı Bırakırsanız veya Yapılandırmazsanız, PIN, parola vb. gibi ek kimlik doğrulama gerektirmez. Etkinleştirilirse, kullanıcının başlangıçta bir PIN, Parola vb. girmesini gerektirir.

Configure pre-boot recovery message and URL: Bu ilke, kullanıcı BitLocker ile ilgili bir sorun yaşarsa veya Kurtarma Anahtarı isterse, son kullanıcılara help desk ekiplerine ulaşmaları için bazı ayrıntılar vermenizi sağlayacaktır.

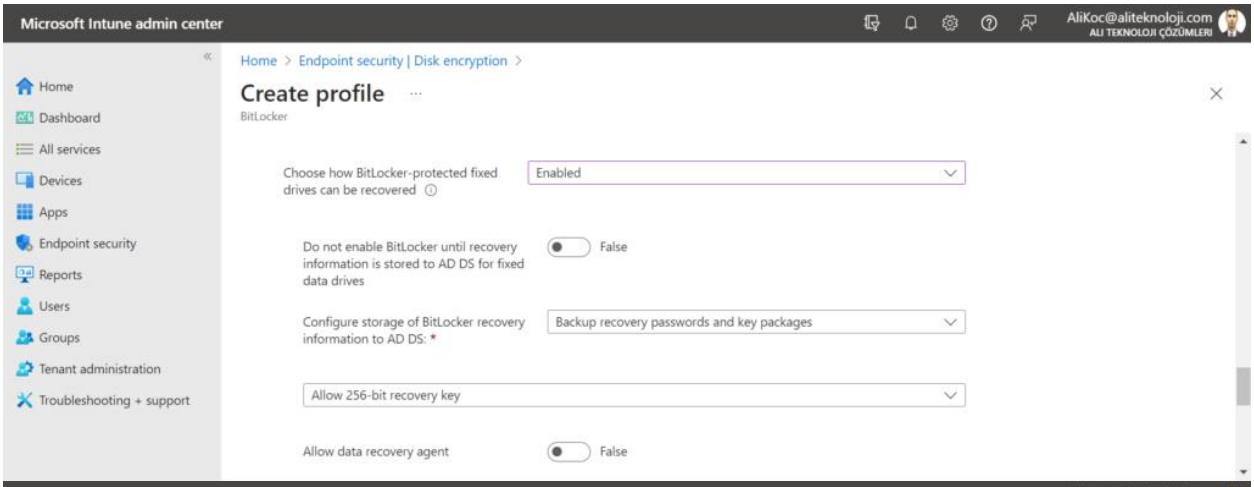


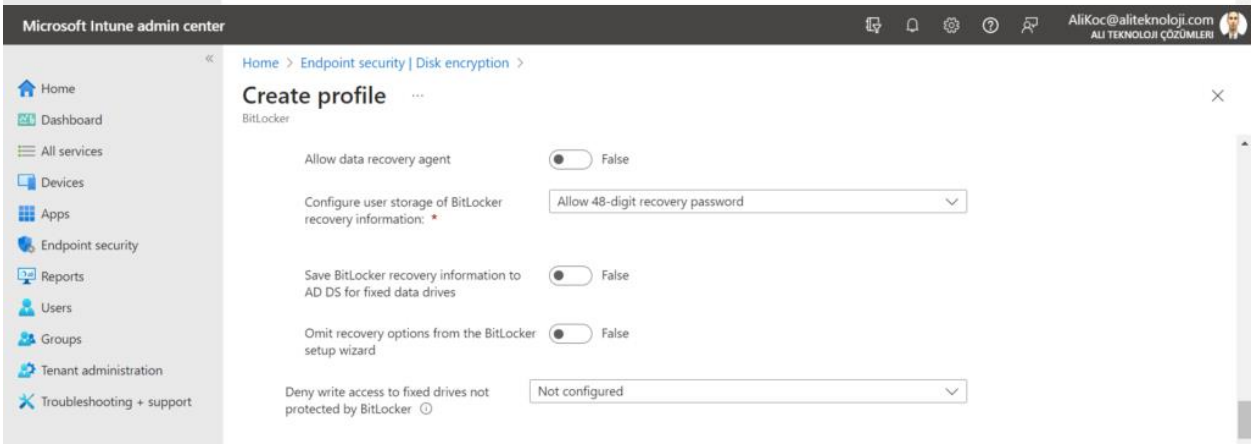


Fix Data Drives

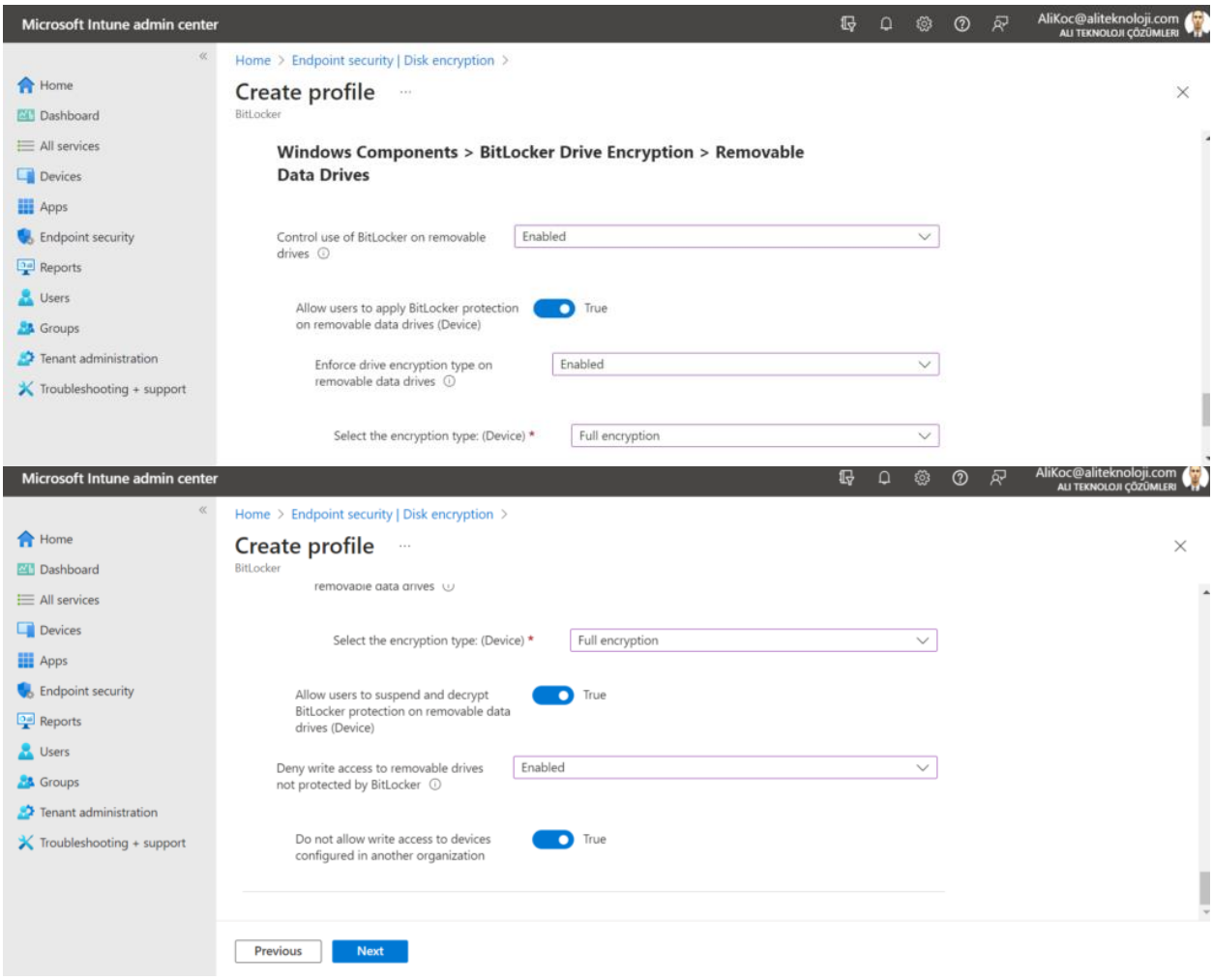


Enforce drive encryption type on fixed data drives: Bu politika işletim sistemi politikasına benzer, bu ilke ayarını etkinleştirirseniz BitLocker'ın sürücüleri şifrelemek için kullanacağı şifreleme türü bu politika tarafından tanımlanır ve BitLocker kurulum ekranında şifreleme türü seçeneği sunulmaz. Bu politika ayarını devre dışı bırakır veya yapılandırmazsanız, BitLocker kurulum sihirbazı BitLocker'ı açmadan önce kullanıcıdan şifreleme türünü seçmesini isteyecektir.

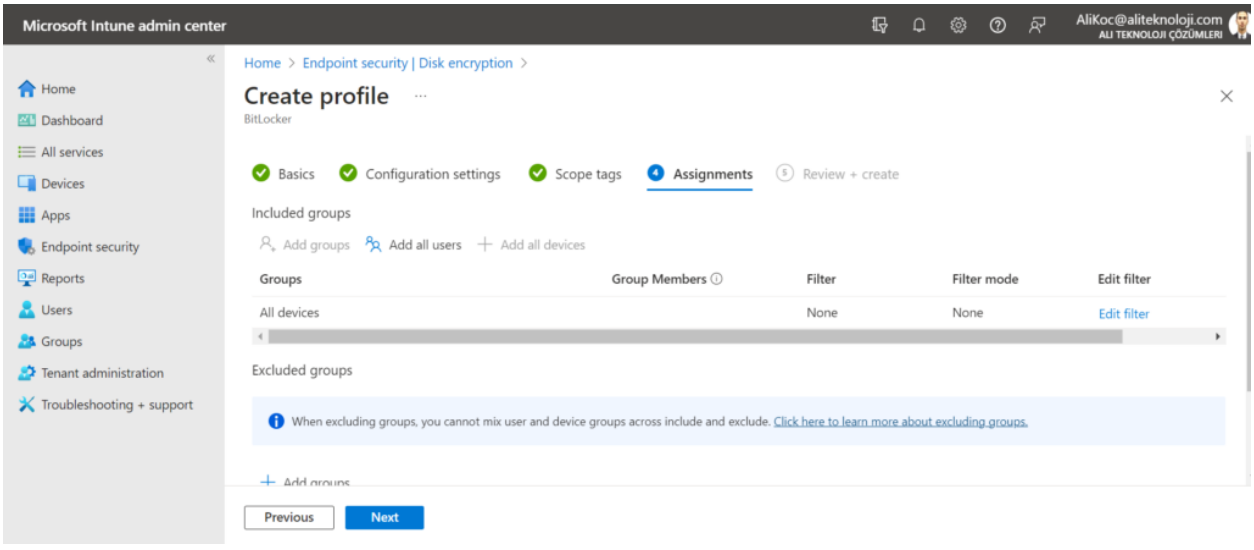




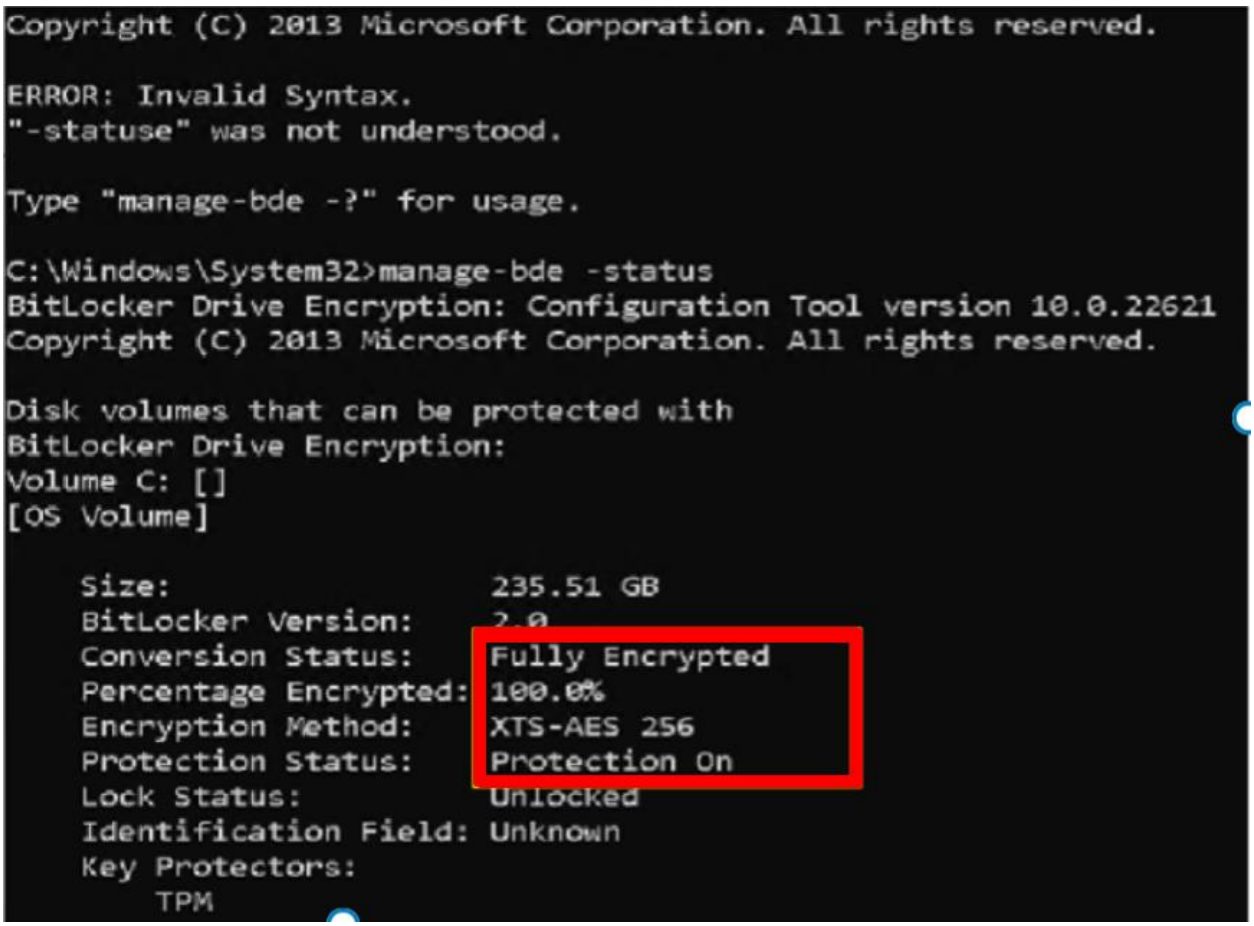
Choose how BitLocker-protected fixed drives can be recovered: Bu seçenek, recovery key'in nerede saklanmasını istediğinizi seçmek içindir. Bu politikayı etkinleştirirseniz, BitLocker korumalı sabit data sürücülerinden veri kurtarmak için kullanıcıların kullanabileceği yöntemleri kontrol etmenize olanak tanır. Ayrıca, AD DS'de nereye yedekleneceğini ve Parola ve Anahtar Paketlerinin veya bunlardan birinin yedekleneceğini kontrol edebilirsiniz. Devre Dışı veya Yapılandırılmamışsa, BitLocker kurtarma için varsayılan kurtarma seçenekleri desteklenir. Varsayılan olarak bir DRA'ya izin verilmekte ve kurtarma seçenekleri kurtarma parolası ve kurtarma anahtarı dahil olmak üzere kullanıcı tarafından belirtilebilir ve kurtarma bilgileri AD DS'ye yedeklenmez. Bizler Entra'da yedekliyoruz.



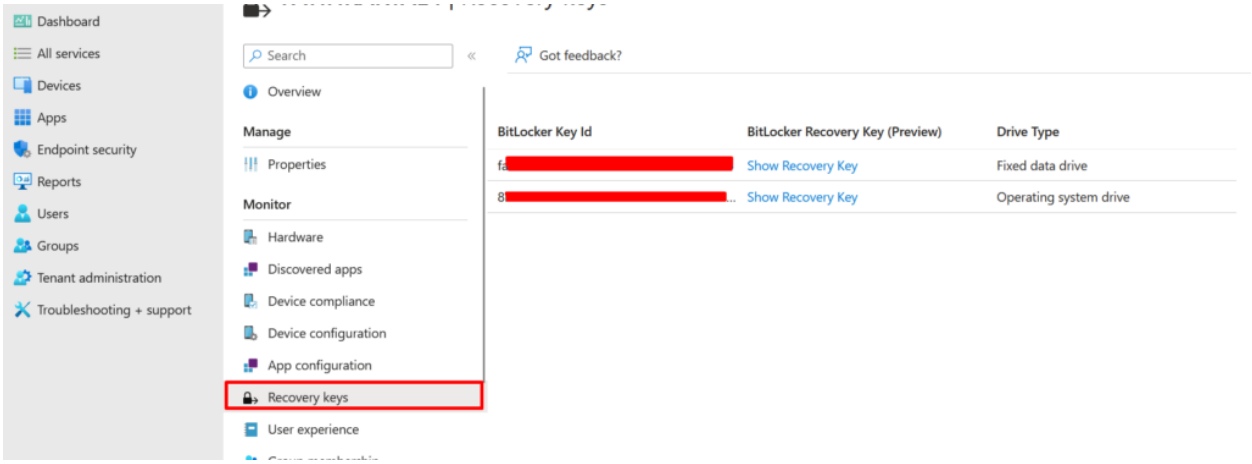
Daha sonra politikaları tüm cihazlara uygulayabiliriz.



Politika dağıtıldıktan sonra, cihazımıza “manage-bde -status” komutu ile mevcut encryption durumunu görüntüleyebiliriz.



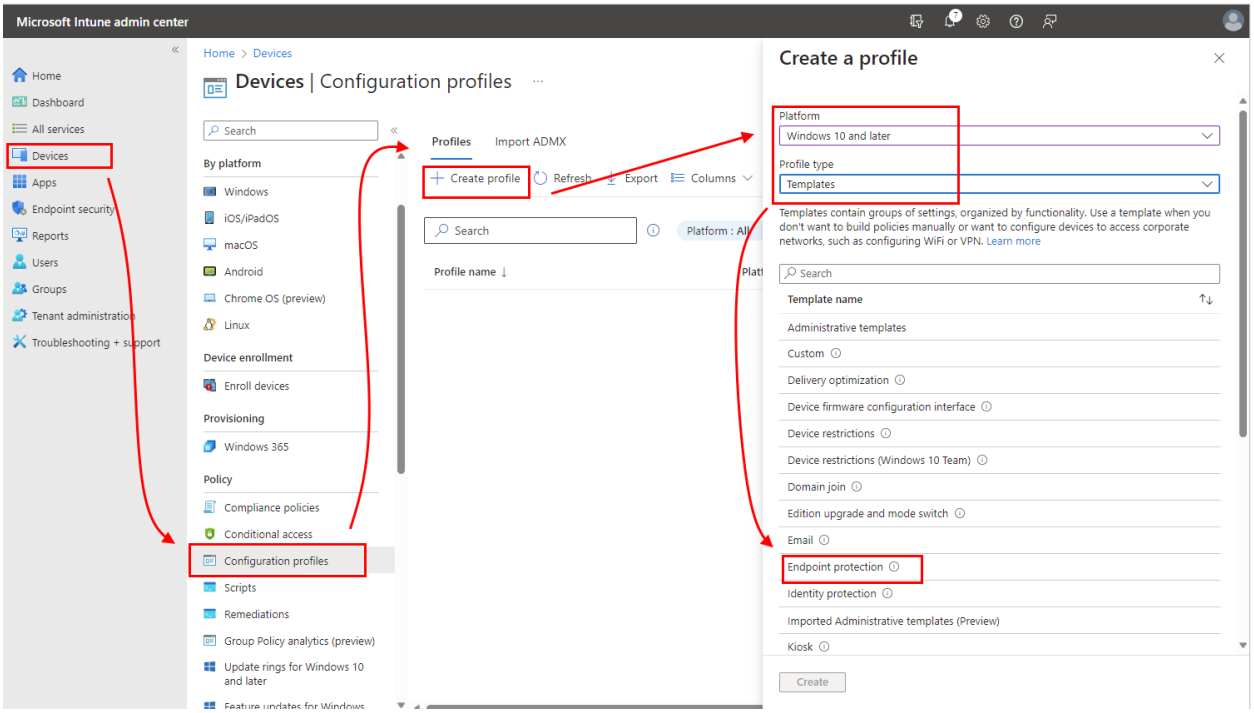
Intune > Cihazlar > Recovery Key ekranından, recovery key'i görüntüleyebilirsiniz. Olası bir sorun durumunda bu key ile diskleri recover edebilirsiniz.



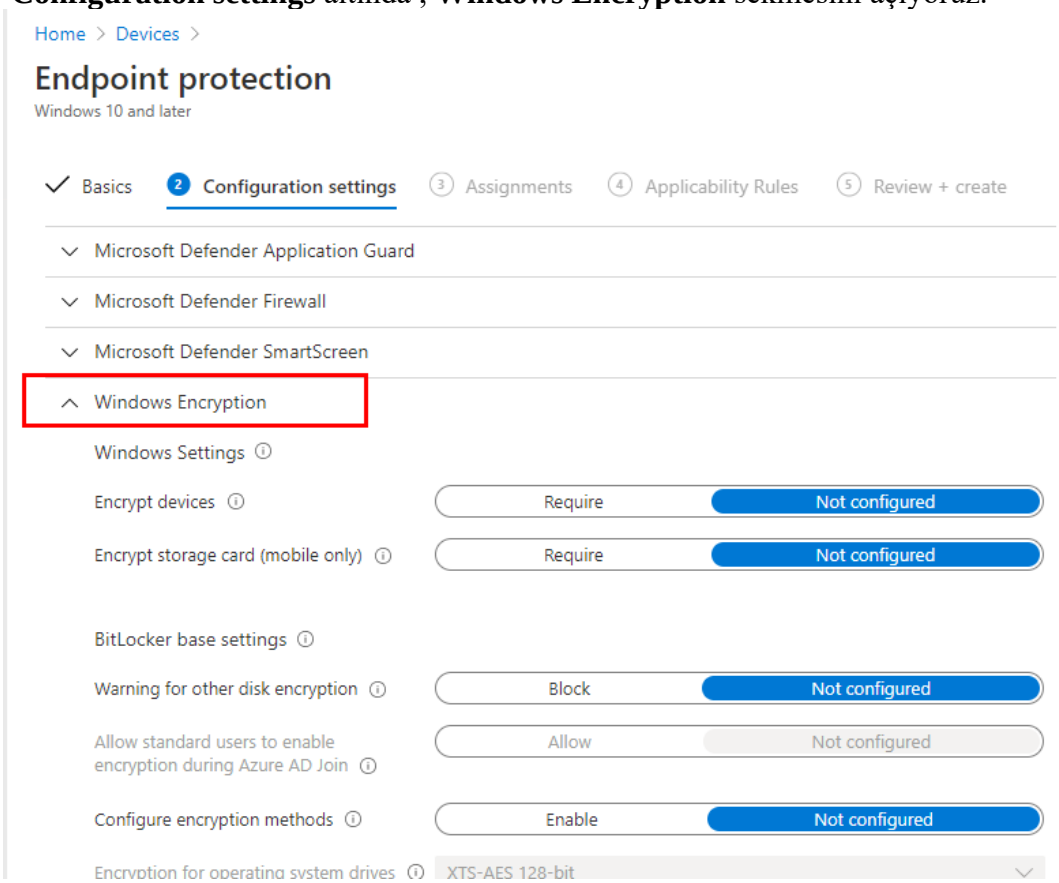
Ayrıca, Device Configuration Politikaları ile de aktif edebilirsiniz;

1. Microsoft Intune admin center 'a giriş yapıyoruz.
2. **Devices** > **Configuration** > On the *Policies* tab, **Create** seçeneğini seçiyoruz.
3. aşağıdaki adımları seçiyoruz:

1. **Platform**: **Windows 10 and laterProfile type**:
   > **Templates** > **Endpoint protection**, **Create** diyoruz.



Configuration settings altında , **Windows Encryption** sekmesini açıyoruz.



BitLocker ayarlarını gereksinimlerinizi karşılayacak şekilde yapılandırabiliriz.

Bir sonraki makalede görüşmek üzere.