epati

1.03. Kurulum Kılavuzu

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı

Kılavuzlar

www.epati.com.tr

1.03. Kurulum Kılavuzu

Online İnceleme

Antikor NGFW'ı online incelemek için tıklayınız.

Kullanıcı adı: demo

Parola: demo

Kurulumdan Önce Yapılması Gereken Adımlar

Ürün Doğrulama Prosedürleri

Alıcı tarafından doğrulama işlemi, alınan medyanın md5 toplamı ile karşılaştırılarak gerçekleştirilir.

• Müşteri, medyanın üzerinde bulunan Epati Siber Güvenlik Teknolojileri tarafından yapıştırılmış mührün zarar görüp görmediğini doğrular. Mührün zarar görmüş olması halinde kurulum gerçekleştirilmemelidir.

• Müşteri, ürünün adını ve sürümünü doğrular.

• Müşteri, medyanın md5 toplamını üretir ve resmi web sayfasındaki ISO md5 toplamı ile karşılaştırır.

• Hesaplanan md5 toplamı ve web sayfasında bulunan md5 toplamı aynı ise yükleme işlemi başlayabilir.

Fiziksel ve Mantıksal Güvenlik

1. Antikor kurulu donanım, güvenliği sağlanmış olan sistem odasında bulunmalıdır. Odaya giriş ve çıkışlar yalnızca yetkili kişiler tarafından olmalıdır.

2. Antikor'un yedekleri düzenli olarak alınarak saklanmalıdır.

3. Antikor kurulu donanım üzerinde USB portları bulunuyorsa devre dışı bırakılmalıdır.

4. Antikor kurulu donanımının güç kaynağı, ethernet kabloları vb. parçaların sağlamlığı kontrol edilmelidir.

5. Antikor'a erişim sağlayacak kişilerin parola bilgileri admin parolası ile aynı olmamalı ve yetkileri kısıtlanmalıdır.

6. Antikor'a erişim sağlayan kullanıcılar, belirli zaman dilimlerinde parola değişikliği yapmalıdır.

7. Antikor'a erişim sağlayan sistem yöneticilerinin kullanıcı adı ve parola bilgilerinin güvenliği kendilerine aittir. İlgili sistem yöneticisi, bu yazılımı kullanarak, kullanıcı adı ve parola bilgilerinin güvenliğinin korunması ile ilgili gerekli önemleri aldığını kabul etmiş sayılır. Epati Siber Güvenlik Teknolojileri kullanıcı adı ve parola bilgilerinin güvenliğinden kaynaklanabilecek doğrudan veya dolaylı bir zarar doğması halinde borç, sorumluluk ve mükellefiyet kabul etmemektedir.

Donanım İhtiyaçları

Bilgisayarlar en yavaş bileşene göre çalışırlar. Aşağıdaki yazılarda da görülebileceği üzere herbir bileşen kendi içerisinde çok parametre taşımaktadır. Güvenlik Duvarlarında en önemli bileşenler CPU, Ram Hızı, Ethernet, Disktir. Bu bileşenler cihazdan geçen internet trafiğini belirler. Güvenlik Duvarlarında Throughput'u cihaza girişten(ethernet), paketlerin işlendiği yer olan (CPU-Ram) değerleri hatta kendine bağlı switch ve İnternet Bant

Genişliğine kadar tüm çevre bileşenleri etkilidir.

Tümleşik Siber Güvenlik Sistemi Antikor için gereken bileşenler;

1. En az 8 Core Xeon (mantıksal çekirdekler hariç)

2. En az 32 GB DDR4 2133 Mhz Ram

3. Multi queue (çok kuyruklu) ethernet kartı

4. En az 256GB SSD

Ethernet (Ağ) Kartı

Güvenlik Duvarlarında Ethernet Kartları kesinlikle multi queue (çok kuyruklu) ethernet kartları olmak zorundadır. Bu sayede Ethernet driverları birden fazla core üzerine yayılabilmektedir.

Tavsiye edilen ethernet kartları aşağıdaki gibidir.

• Intel i210 ethernet kartı 2 port 1GBit/s (KOBİ lerde)
https://www.intel.com/content/dam/www/public/us/en/documents/datasheets/i210-ethernet-controller-datasheet.pdf

• Intel'in i350 ethernet kartı 4 port 1GBit/s olup, her bir portta 8 TX/RX yola sahip, bu da toplam 32 core'a kadar ethernet driverin yayılacağı anlamına gelir. (Orta büyüklükteki işletmelerde)
https://www.intel.com/content/www/us/en/products/sku/84805/intel-ethernet-server-adapter-i350t4v2/specifications.html

• Yine Intel'in başka 2 portlu Intel x540 modelleri 10 GBit/s olup her bir portu 128 kuyruğa dağıtabiliyor. (Büyük işletmelerde) http://www.intel.com/content/dam/www/public/us/en/documents/datasheets/ethernet-x540-datasheet.pdf

• Yine Intel'in başka 4 portlu Intel x710T modelleri 10 GBit/s (Büyük işletmelerde)
http://www.intel.com/content/www/us/en/support/network-and-i-o/ethernet-products/intel-10-gigabit-server-adapters/intel-ethernet-converged-network-adapter-x710-series/intel-ethernet-converged-network-adapter-x710-t4.html

Disk (Depolama)

Kullanılacak Programın Disk ile işi çok oluyorsa ve devamlı diskden okuma/yazma yapıyorsa Disklerin önemi çok büyüktür. Diskler de kendi içinde büyüklük ve hıza göre ayrılırlar. Disk çeşitleri olarak SATA Diskler, SAS Diskler, SSD Diskler, şimdi de SSD NVMe Diskler piyasadadır.

Sistem yöneticisi bir servisi veya sistemi devreye alırken disk'le ilgili ihtiyaçlarını düşünürken sadece kapasite öngörüsünde bulunurlar. Doğal olarak orta ve uzun vadede yük artıkça dar boğazlar oluşmaya ve performans kaybı gözlemlenir. Bunun yegâne sebebi sistemin ihtiyaç duyacağı toplam IOPS ve Throughput doğru öngörülememesi veya hiç hesaba katılmamasıdır.

Peki nedir bu değerler ve ne işe yararlar?

IOPS (Input/output operations per second) adından da anlaşılacağı gibi bir diskin saniyede yapabileceği maksimum yazma veya okuma sayısıdır. Throughput ise belli bir zaman aralığında yapılan işi temsil eder. Genelde 1 saniyede kaç MB yazdığı veya okuyabildiği değerdir. Örneğin kamera programı ise daha çok boyut önemlidir. Programın diske yazma hızı sabittir. Bu sunucunun toplam iş yükünün %10'i okuma, %90'si yazma gibi düşünebiliriz. Genelde kamera görüntüleri yazılır. Çekilmiş görüntülere bakacağımızda okuma işlemi olur.

Başka bir örnek olarak FTP dosya sunucumuzu ele alalım. Bu sunucunun toplam iş yükünün %80'i okuma, %20'si yazma gibi düşünebiliriz. Genelde insanlar dosya sunucusundan indirme yaptığı için okuma, biz dosya atarsak yazma işlemi olur.

Fonksiyonal IOPS = ((Toplam IOPS *yazma yüzdesi)/(Raid penalty))+(Toplam IOPS *okuma yüzdesi)

Not: Formülde RAID 0 Raid Penalty 1, RAID 1 Raid Penalty 2, RAID 5 Raid Penalty 4, RAID 6 Raid Penalty 6 olarak hesaplanır. Görüldüğü üzere aynı diskler farklı raid yapıları ve okuma ve yazma oranlarıyla tamamen farklı sonuçlar vermektedir. Antikor içerisinde Veritabanı işlemleri ve Loglama olduğundan kapasitesi en az 256GB olan SSD tercih edilmelidir.

1. Kurulumun gerçekleştirileceği cihaz için, network yapısına uygun olarak ethernet kartı takılmalıdır veya sanal kurulum gerçekleştirilecek ise ethernet kartları açılmalıdır . örneğin, WAN, LAN ve DMZ kullanılacak ise 3 portlu ethernet kartı veya 3 tane ayrı ethernet kartları takılmalıdır. Sanallaştırma üzerinden kurulum yapılacak ise 3 tane ethernet portu açılmalıdır. Kurulum tamamlandıktan sonra ethernet kartı eklenmesi veya çıkarılması yapılmamalıdır.

2. Kurulumun gerçekleştirileceği cihaz için **Last State** ayarı sürekli açık yapılmalıdır. Bunun için BIOS ayarları kontrol edilmelidir.

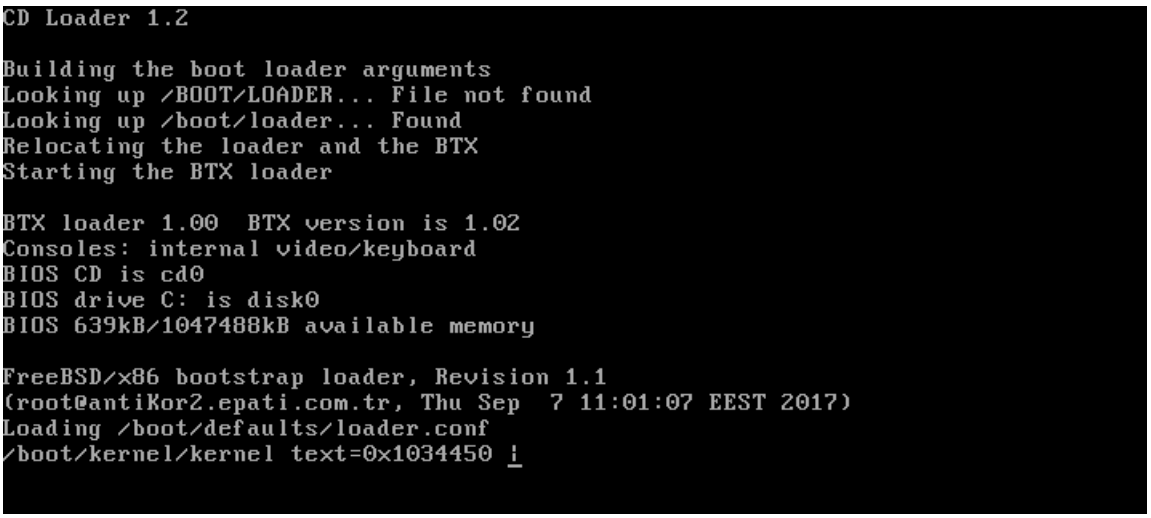
Not: Antikor'un kurulum yapılacağı ağ ortamda filtreleme yapan bir cihazın(firewall) arkasında ise; Antikor'un kurulu olduğu sunucu IP adresi için, 7001 ve 7002 portları lisans sunucusu ile haberleşebilmesi için açık olması gerekmektedir. Açık olmaması halinde lisans sunucusundan gelen paketler çekilmeyecek ve kurulum başarısız olacaktır. Bu portlar(7001 ve 7002) sadece Antikor lisans sunucu IP adresinin erişimi için de açılabilir. Lisans sunucu IP adresi için Teknik Destek Ekibi ile iletişime geçebilirsiniz.

Test için;

```
telnet lisans.epati.com.tr 7001
telnet lisans.epati.com.tr 7002
```

Kurulum Aşaması

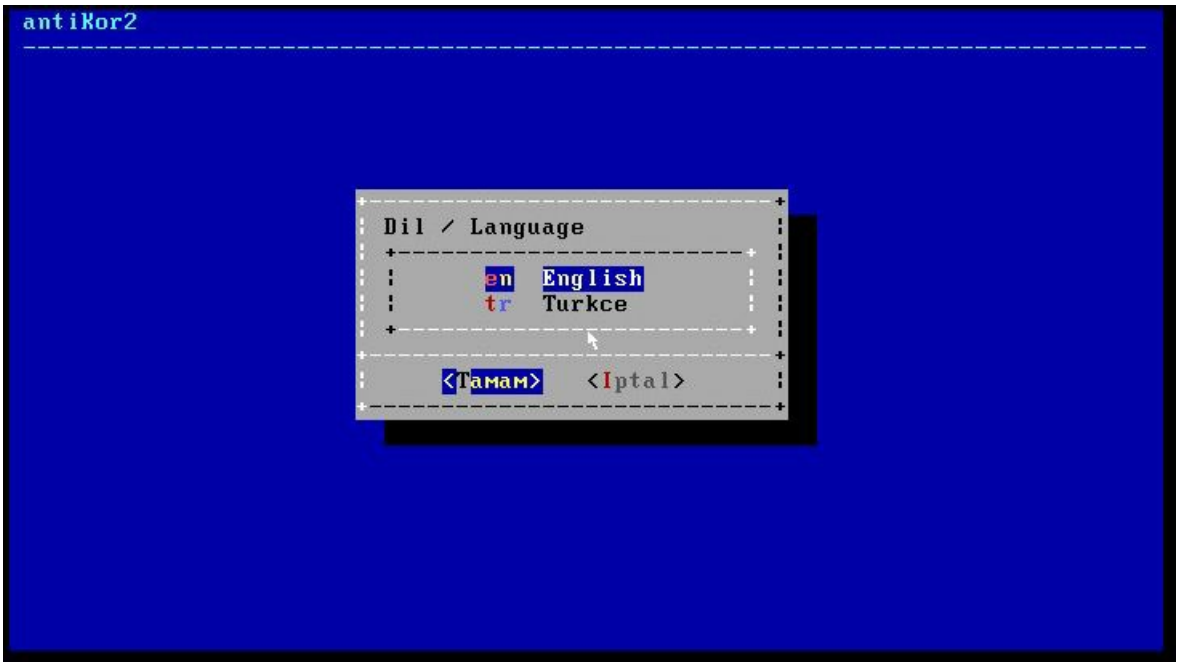
ISO dosyasını edinmek için tıklayınız.

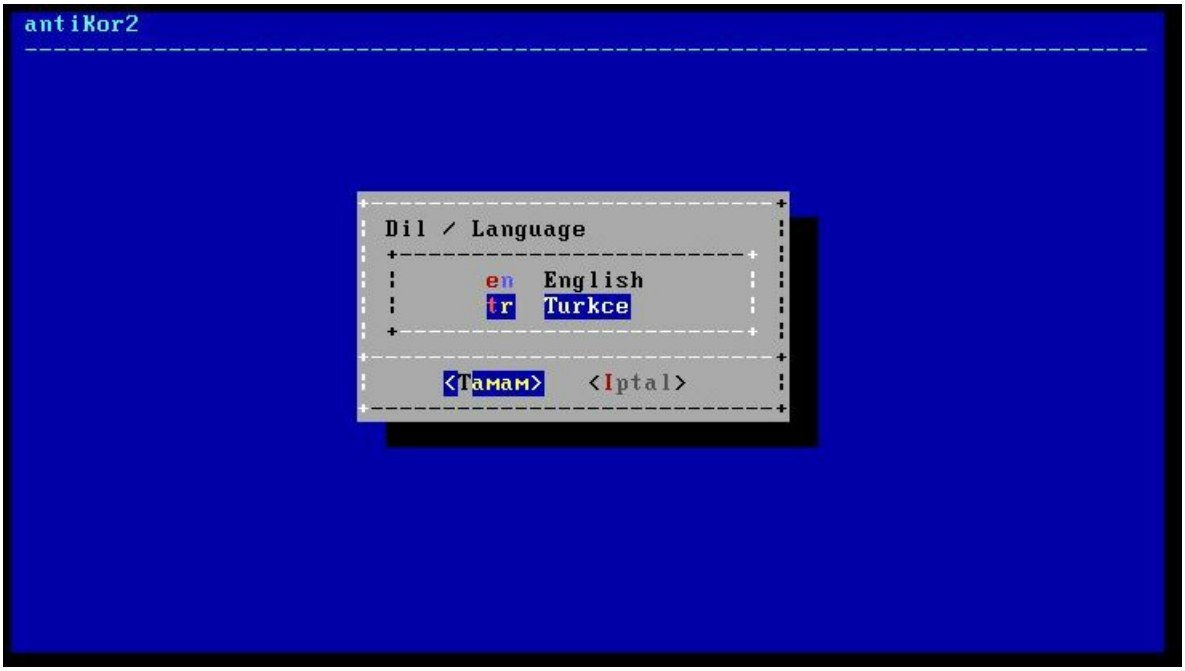


Yukarıdaki ekranda ilk satırda "CD Loader " yazdığında kurulum başladığını belirtmektedir.

Dil Seçimi

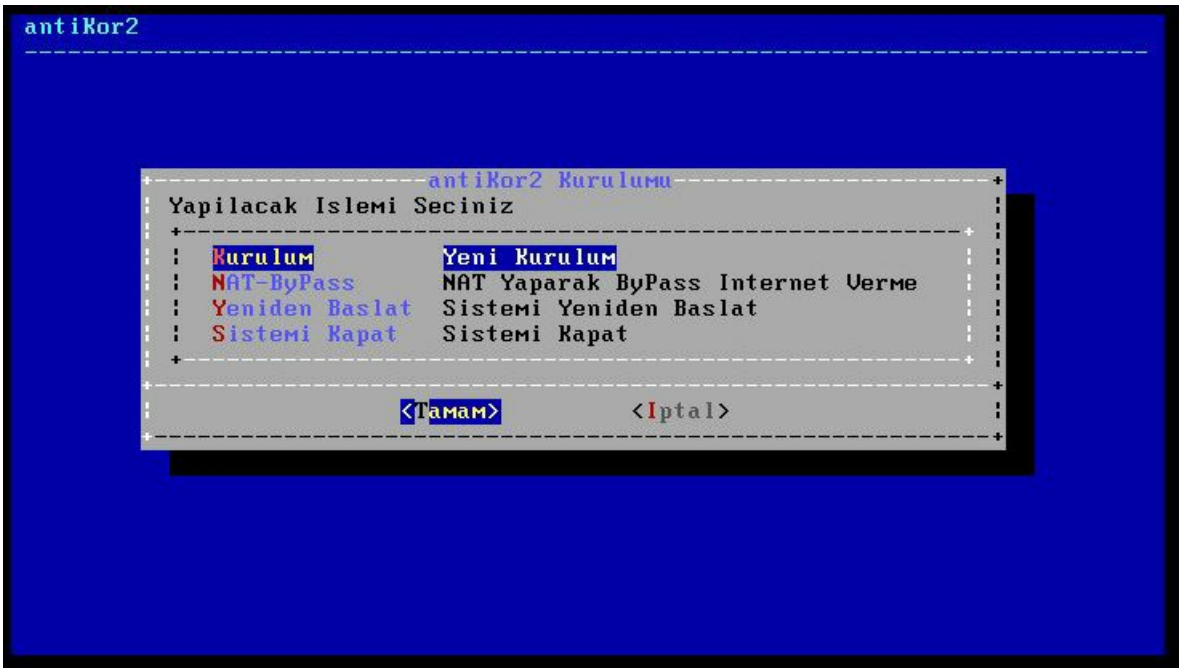
CD başarılı bir şekilde çalıştırılır ise, kuruluma başlama adımı karşımıza gelecektir.





İstenilen dil seçilerek **Tamam**'a tıklanır.

Kurulum

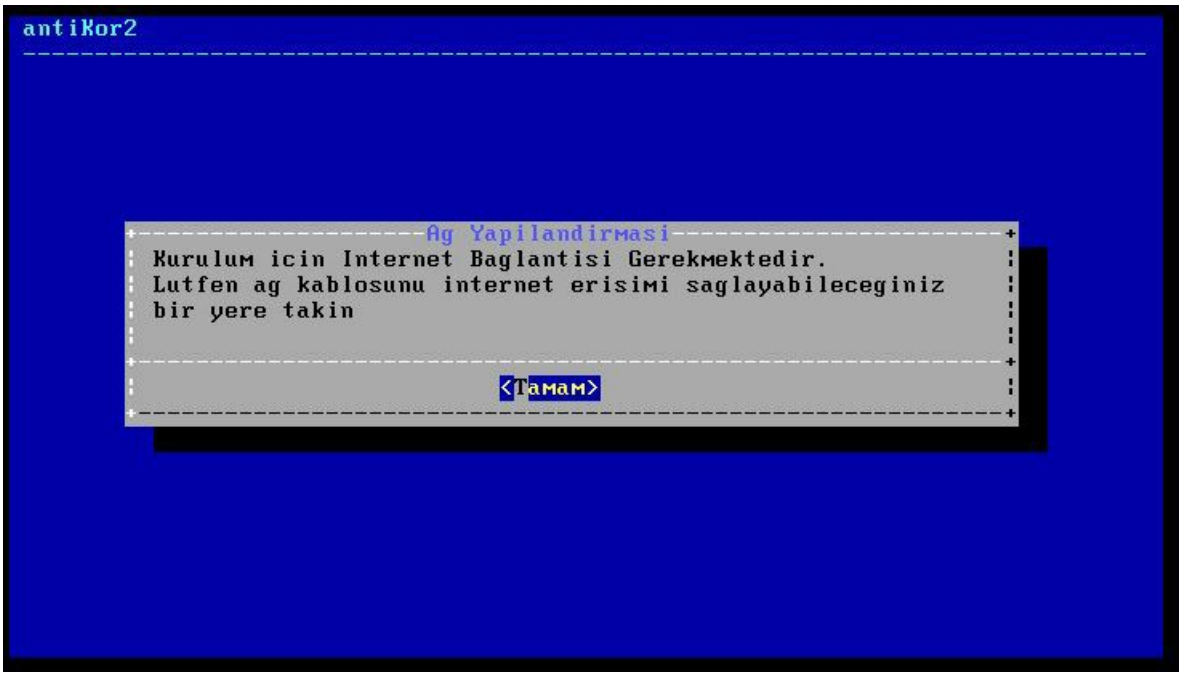


Yukarıdaki ekranda;

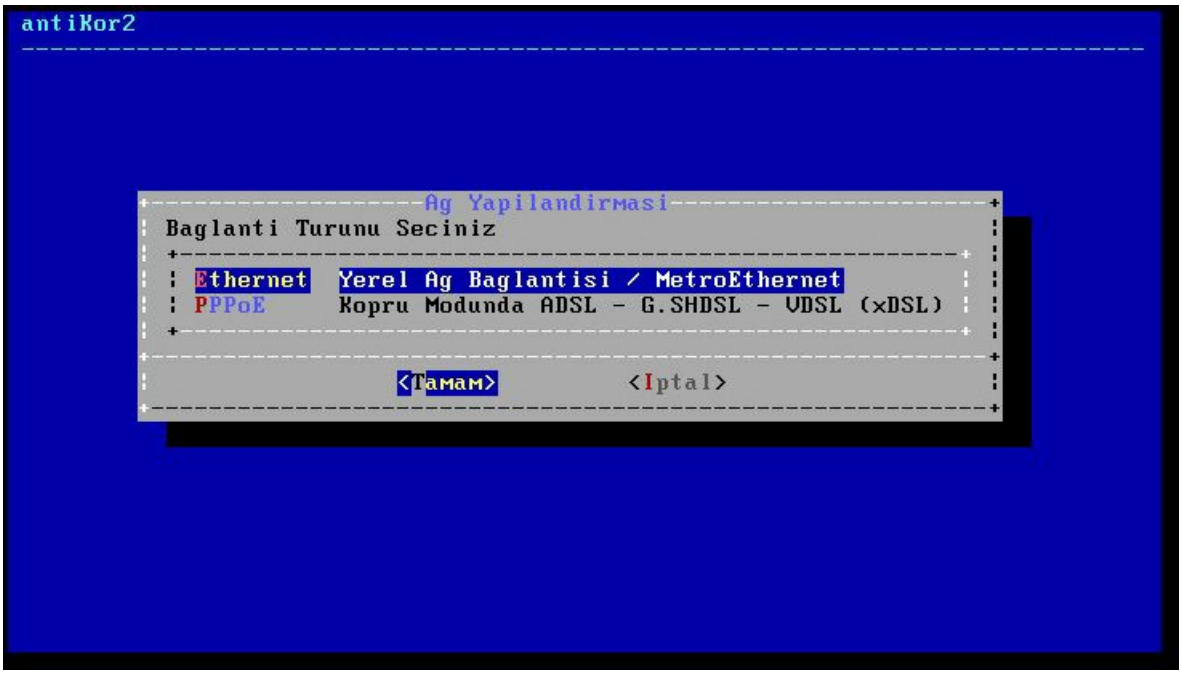
- `Kurulum` seçeneği yeni Antikor kurulumun başlatılması istendiğinde seçilmelidir.
- `Nat-Bypass` seçeneği kurulumu yapılmış Antikor'un bypass yapılarak internete çıkarılması için kullanılmalıdır.
- `Yeniden Başlat` seçeneği kurulumun tekrardan başlatılması için kullanılmalıdır.
- `Sistemi Kapat` seçeneği sistemin gücünü kapatmasını sağlamaktadır.

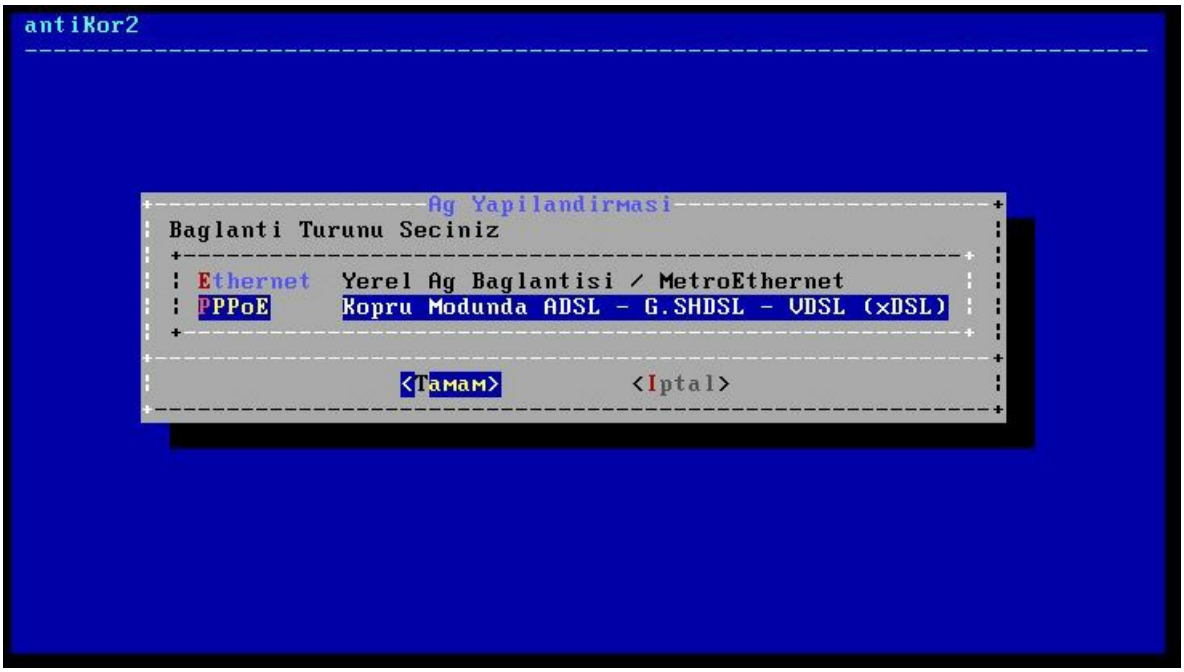
Yeni kurulum yapılması için, "Kurulum" seçilerek devam edilmelidir.

Ağ Yapılandırması

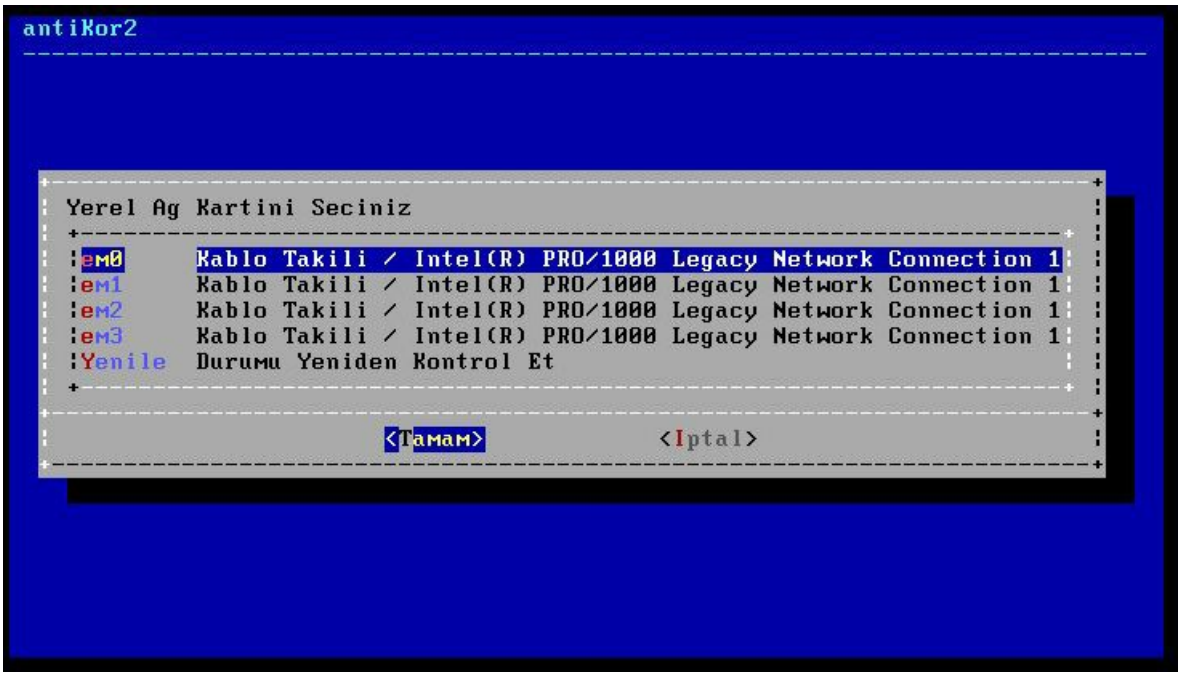


Kurulum için internet bağlantısı gerekmektedir.





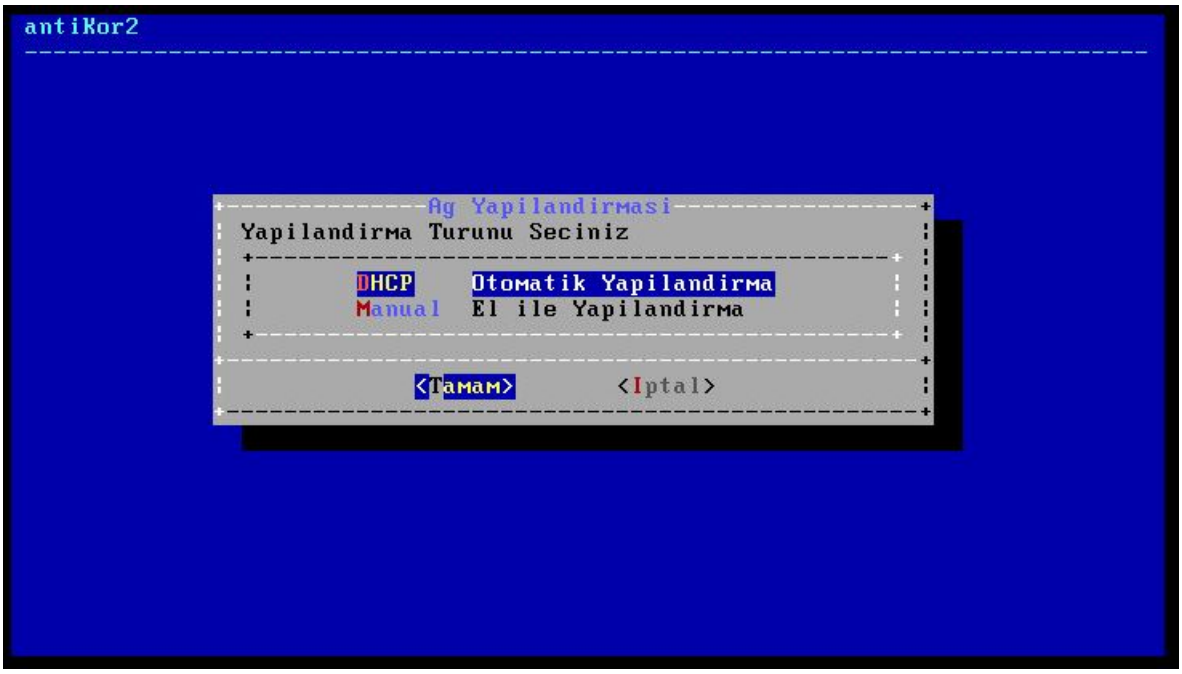
İnternet bağlantı türü seçimi yapılır.

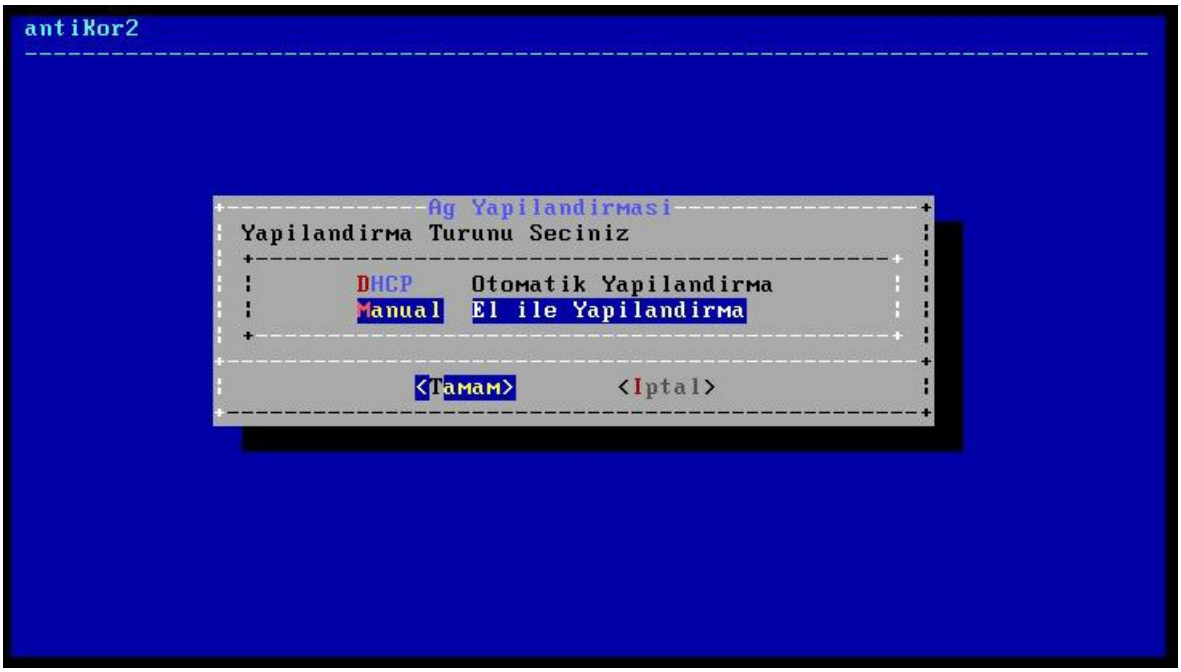


Bu ekranda 4 adet Intel Ethernet görülmektedir. Kurulum hangi Ethernet üzerinden yapılacaksa o Ethernet seçilerek kuruluma devam edilir.

Not: Ethernet kartları görünmediği takdirde, bağlantılar kontrol edilerek**Yenile Durumu Yeniden Kontrol Et** seçeneği seçilir.

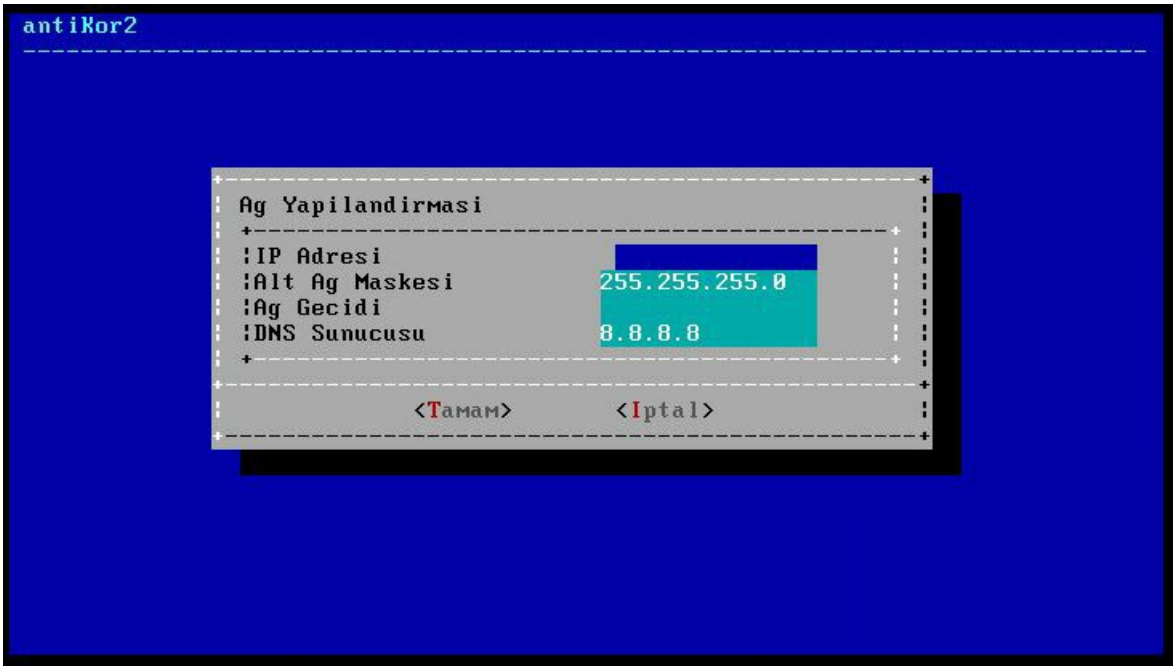
DHCP - Manuel Seçimi

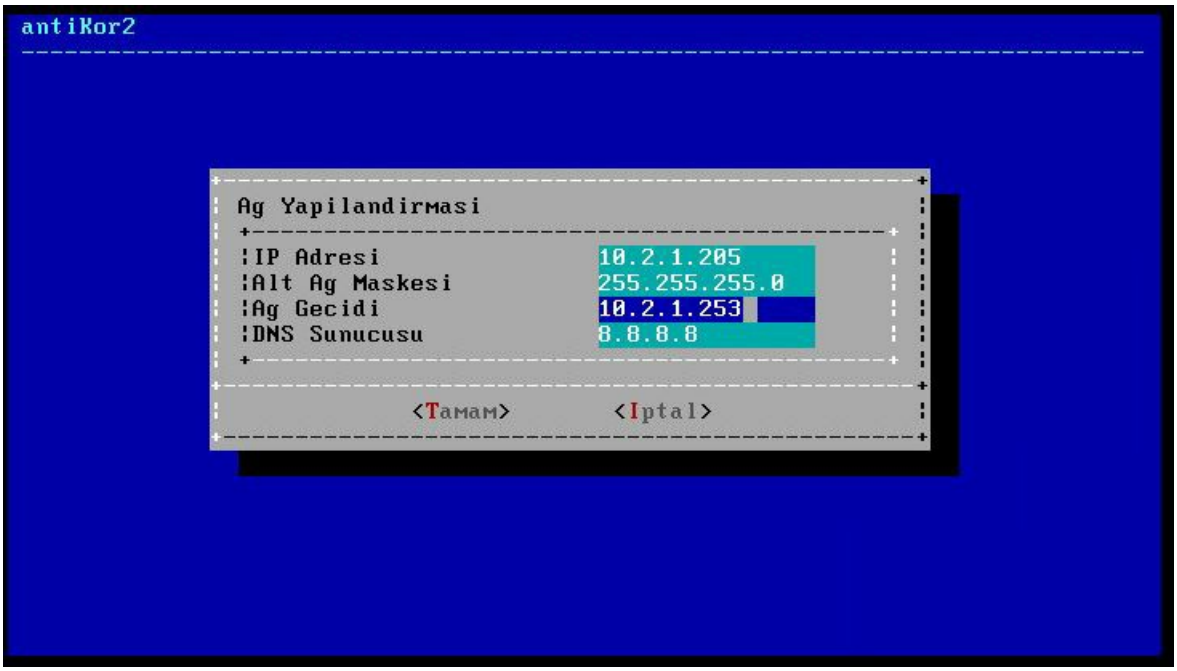


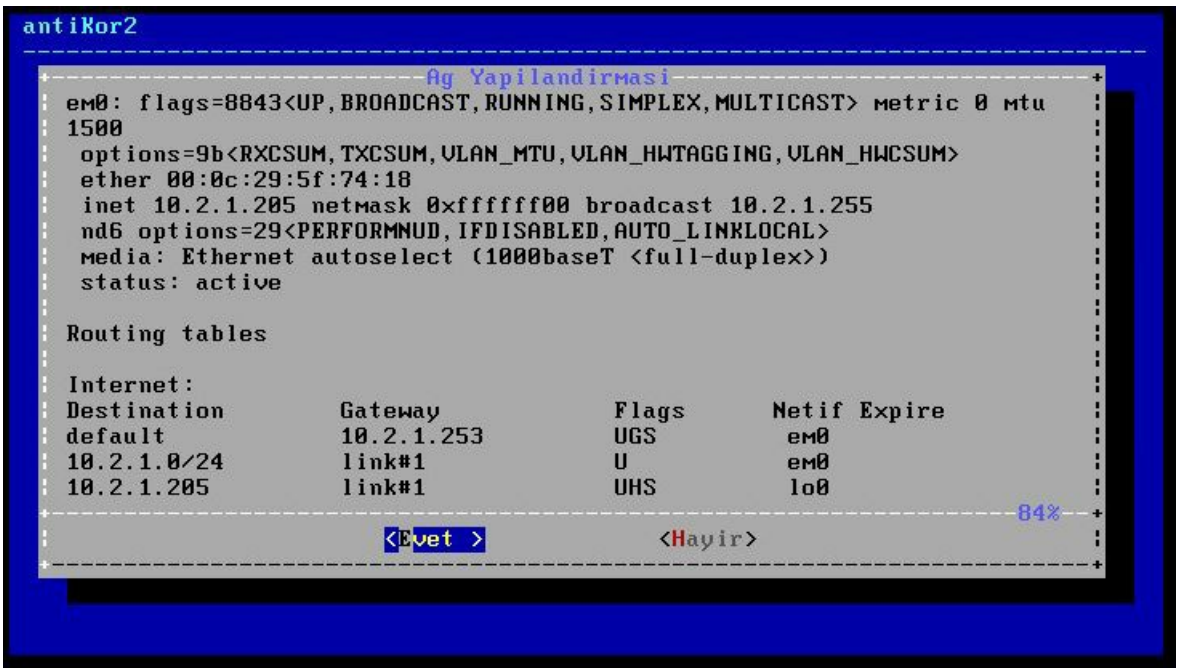


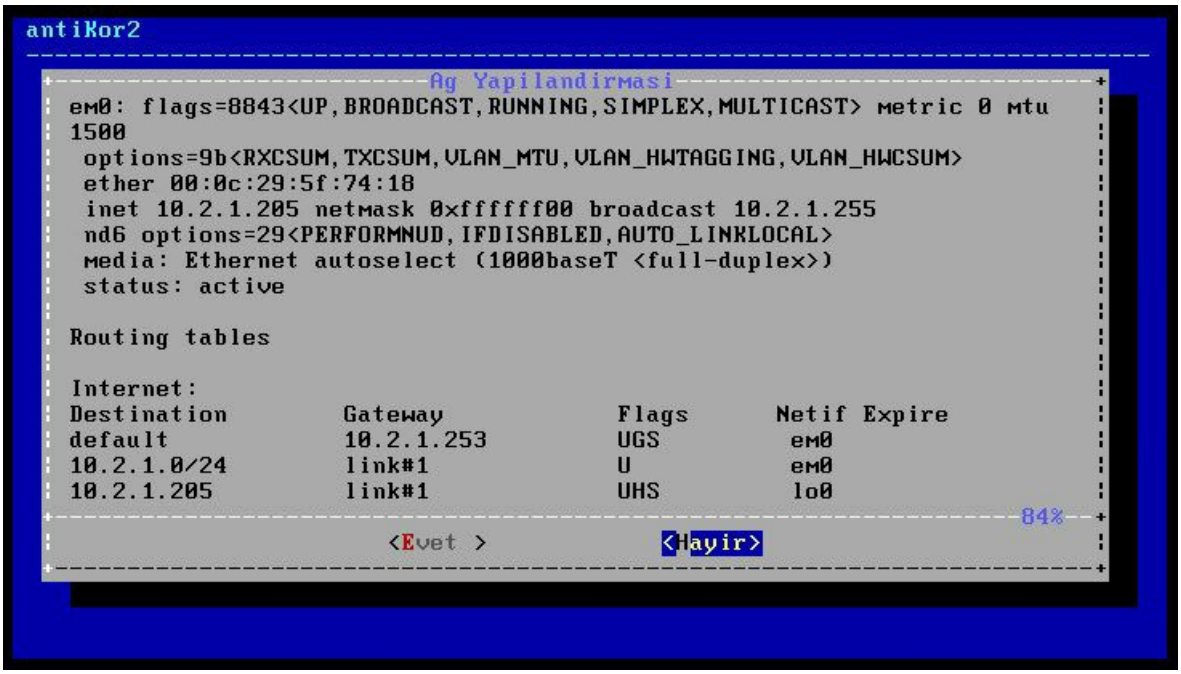
Seçilen ethernetten internete manuel IP verilerek veya DHCP seçilerek otomatik IP alınması gerekir. Fakat DHCP için IP dağıtan bir sisteminizin olması gerekmektedir. Eğer DHCP sunucu yoksa manuel IP verilerek devam edilir.

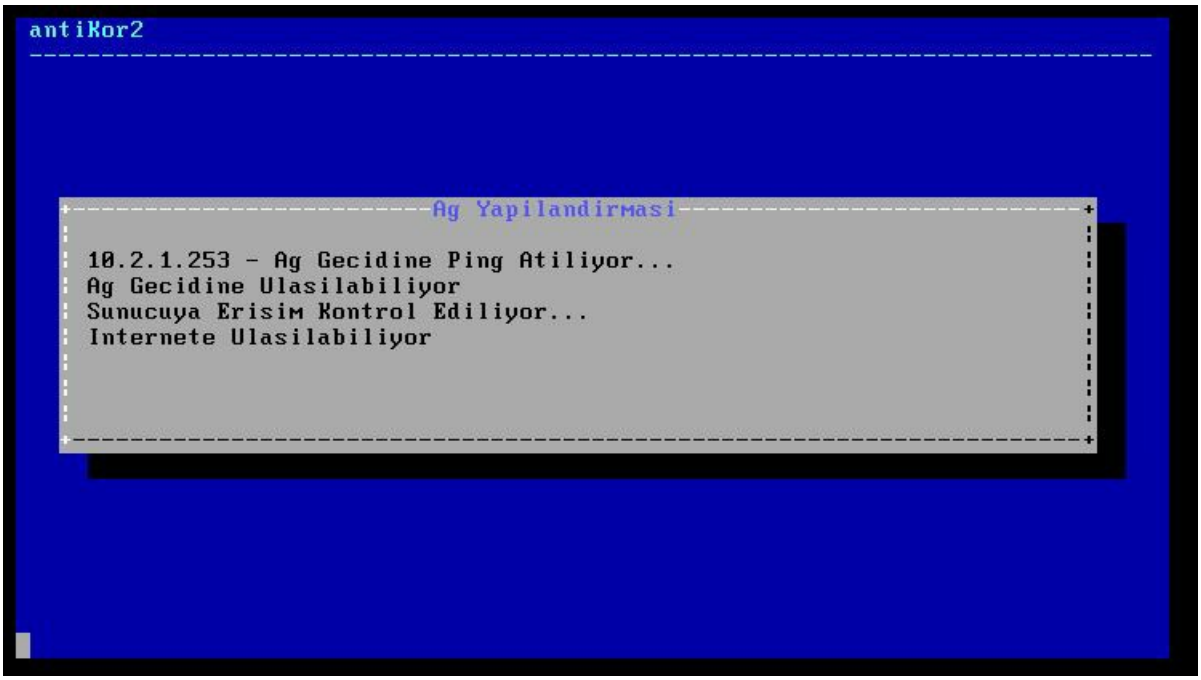
Aşağıda manuel IP verilerek kuruluma devam edilmiştir.



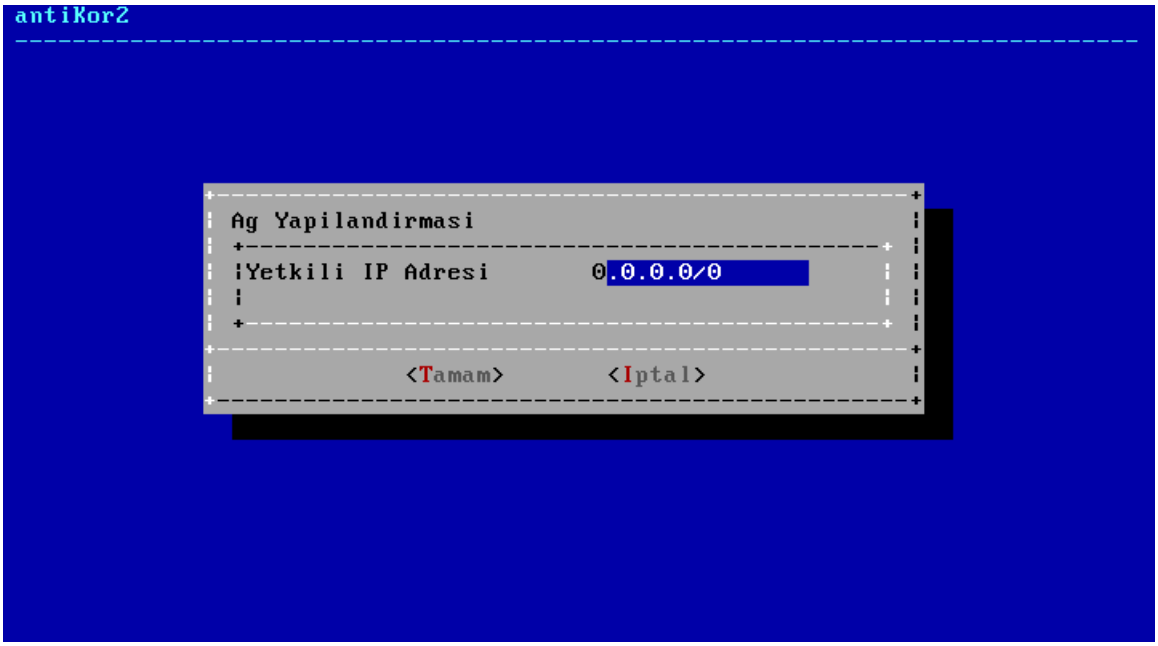

antiKor2
Ag Yapilandirmasi
IP Adresi
10.2.1.205
Alt Ag Maskesi
255.255.255.0
Ag Gecidi
10.2.1.253
DNS Sunucusu
8.8.8.8
<Tamam>
<Iptal>

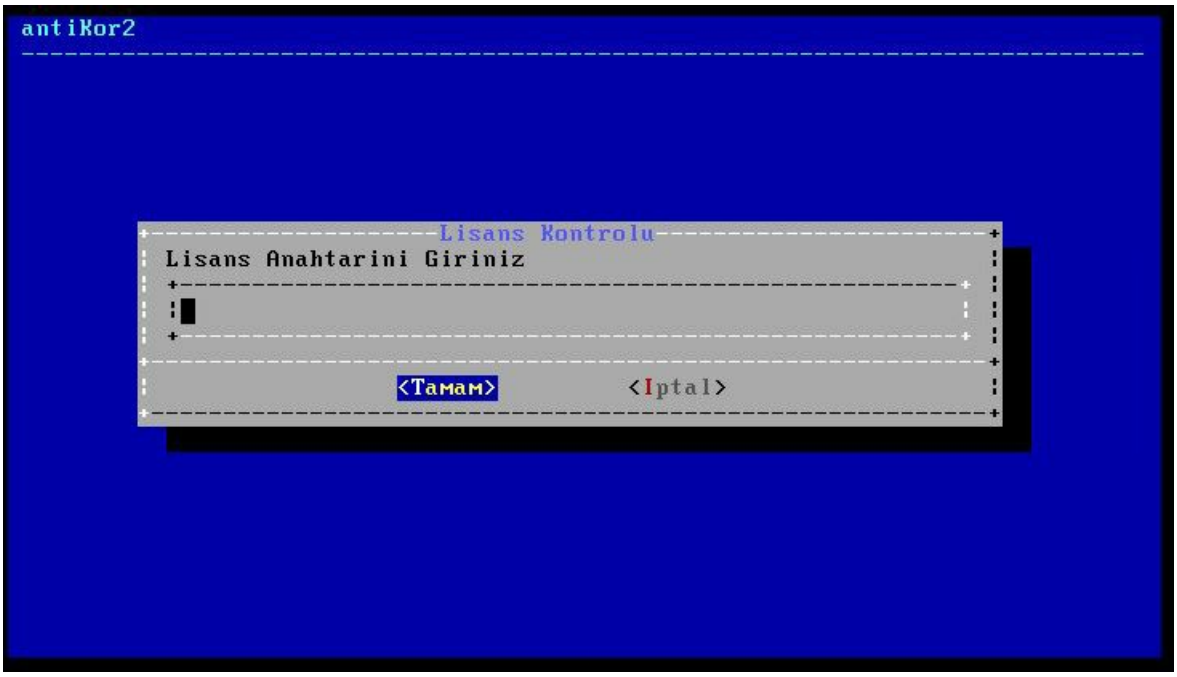

antiKor2
Ag Yapilandirmasi
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
ether 00:0c:29:5f:74:18
inet 10.2.1.205 netmask 0xffffff00 broadcast 10.2.1.255
nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
media: Ethernet autoselect (1000baseT <full-duplex>)
status: active
Routing tables
Internet:
Destination Gateway Flags Netif Expire
default 10.2.1.253 UGS em0
10.2.1.0/24 link#1 U em0
10.2.1.205 link#1 UHS lo0
84%
<Evet >
<Hayir>


antiKor2
Ag Yapilandirmasi
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
ether 00:0c:29:5f:74:18
inet 10.2.1.205 netmask 0xffffff00 broadcast 10.2.1.255
nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
media: Ethernet autoselect (1000baseT <full-duplex>)
status: active
Routing tables
Internet:
Destination Gateway Flags Netif Expire
default 10.2.1.253 UGS em0
10.2.1.0/24 link#1 U em0
10.2.1.205 link#1 UHS lo0
84%
<Evet >
<Hayir>

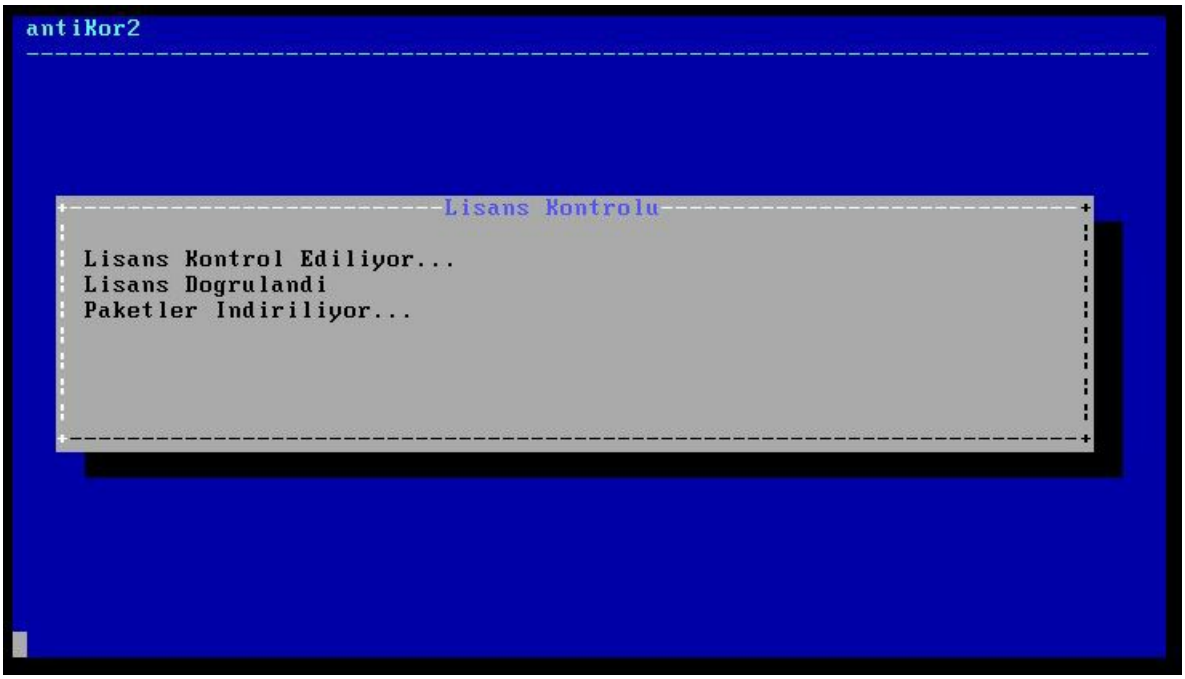


Antikor'a erişim sağlanması istenen IP adresi girilir. 0.0.0.0/0 seçilmesi durumunda her yerden erişim sağlanabilecektir.



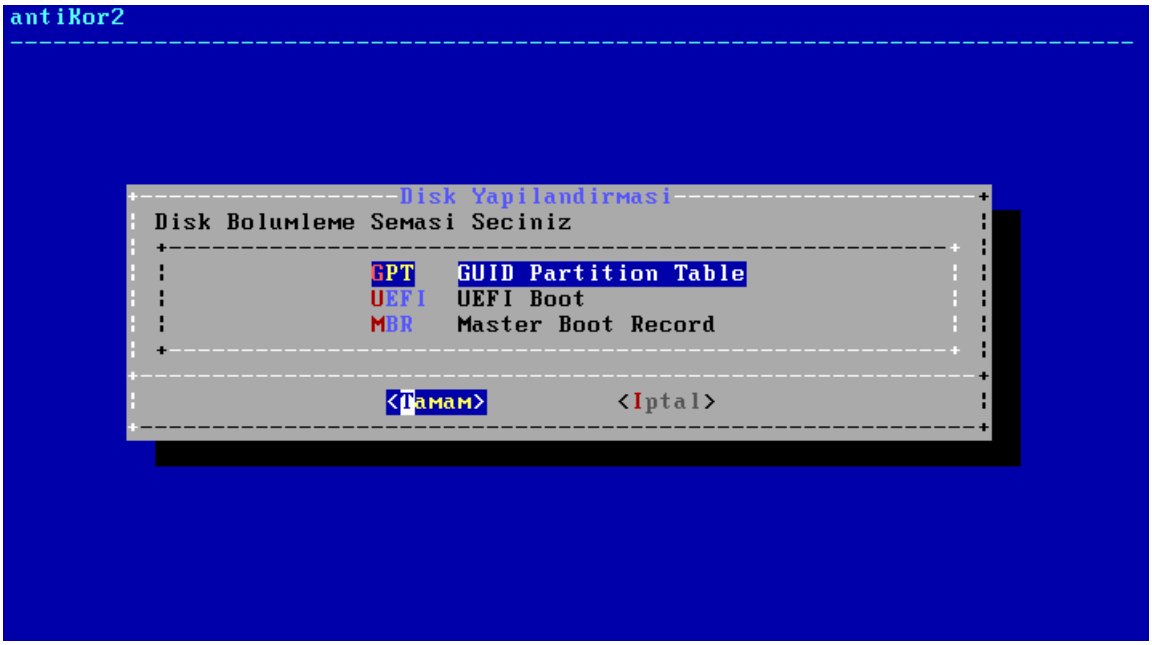


Epati Siber Güvenlik Teknolojileri tarafından sağlanan lisans anahtarı girilir.

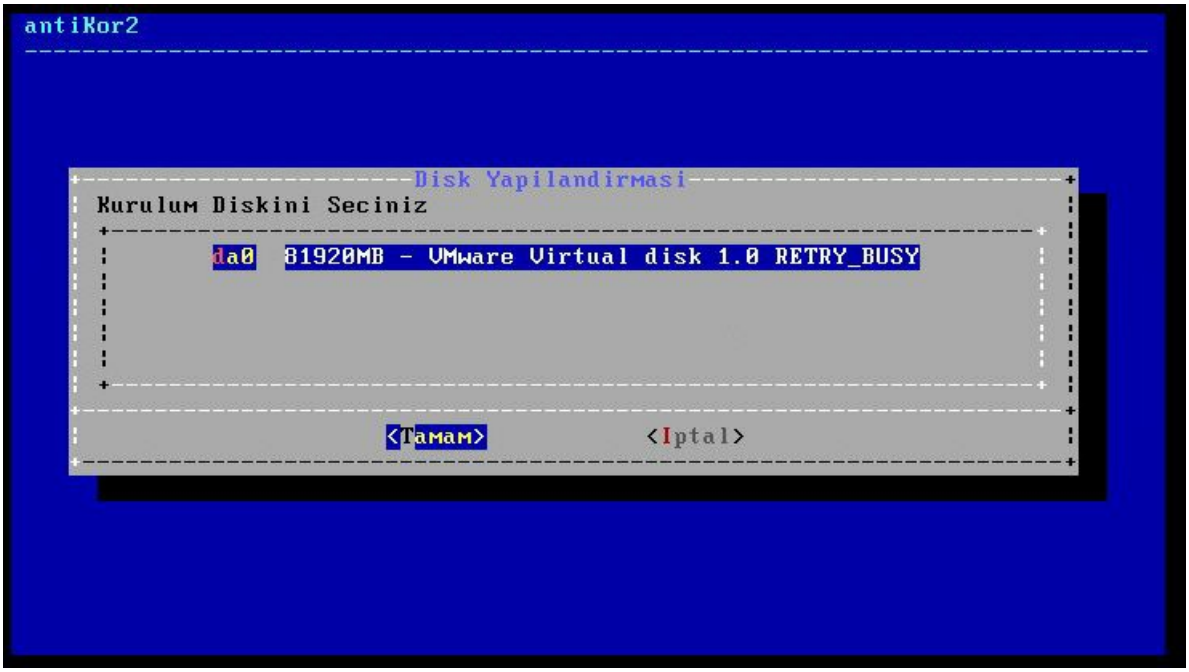


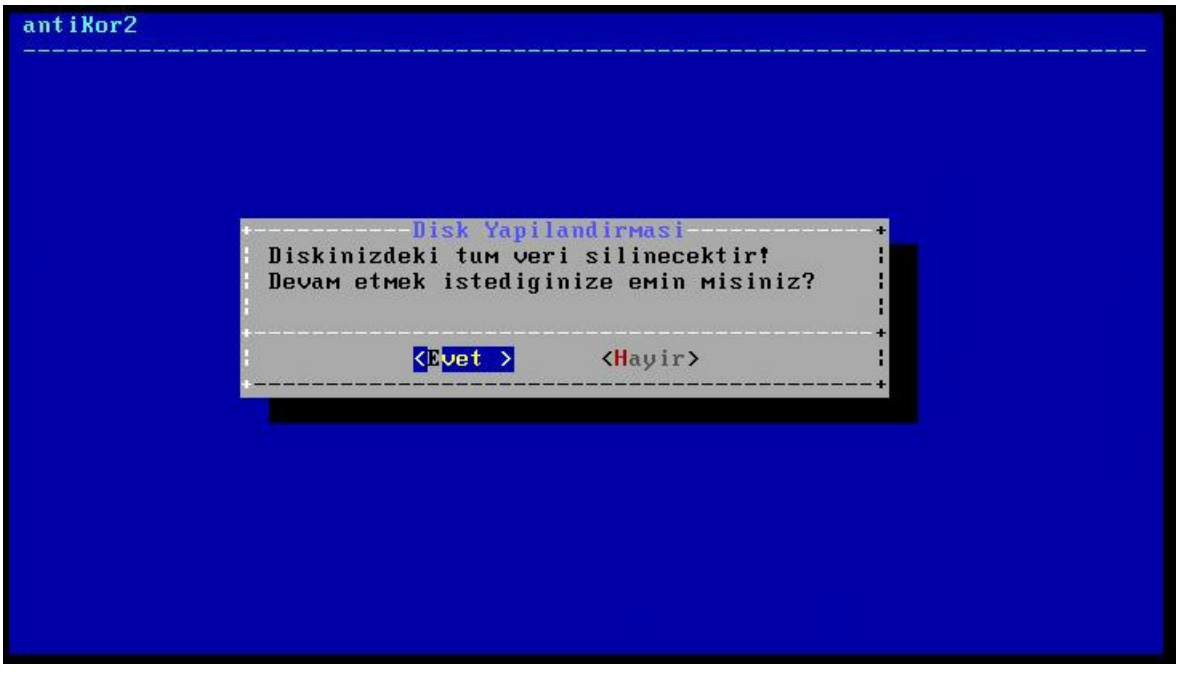
Disk Bölümleme

Sunucu üzerinde 2-3 farklı disk var ise, Antikor Yazılımı ve Logları 2 farklı diske kurulabilir. Tek disk var ise seçilen diske kurulum yapılacaktır.

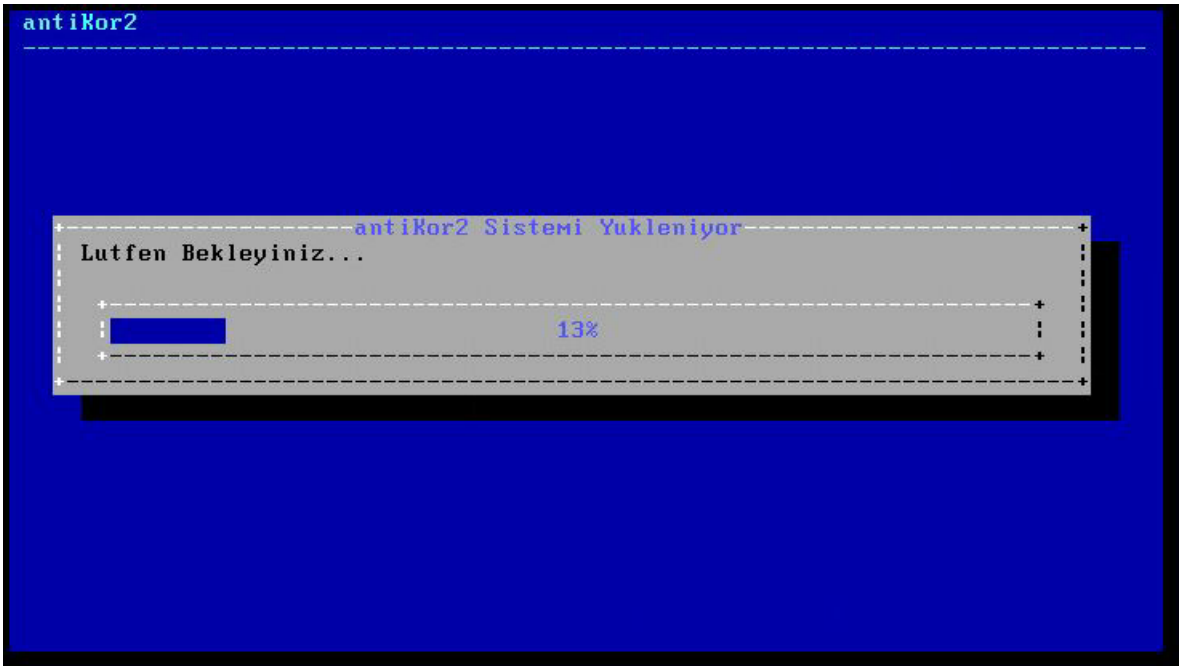


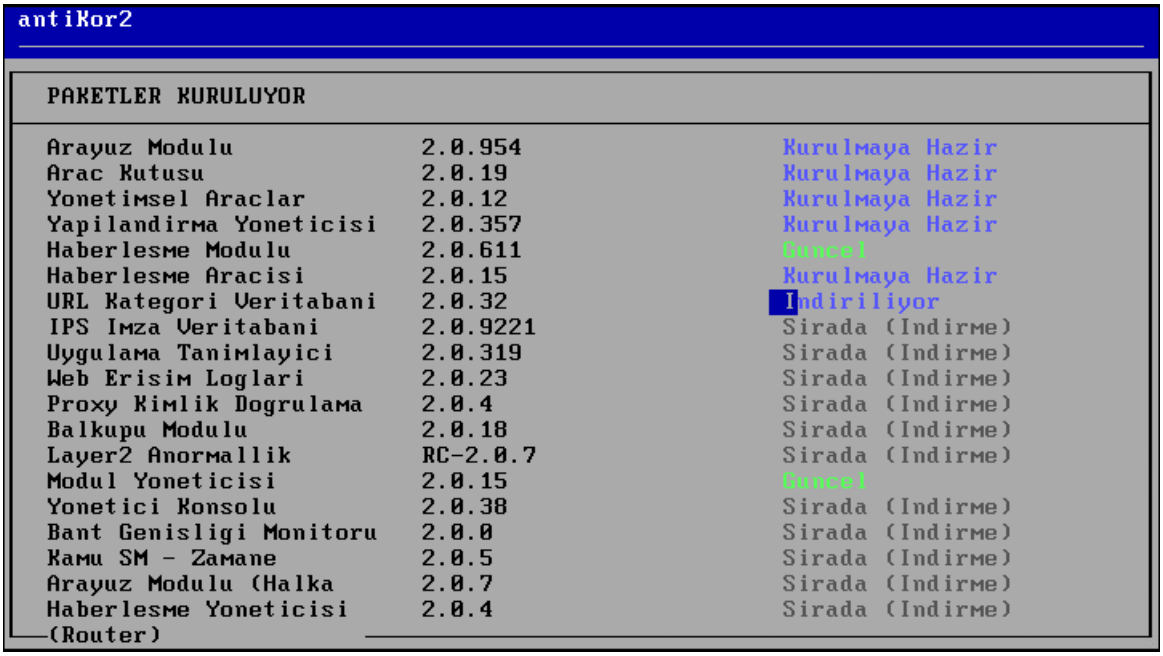
Diskinizin partition yapısına göre(GPT, UEFI, MBR) seçim yapılır. Disklerin bir çoğu GPT uyumludur.

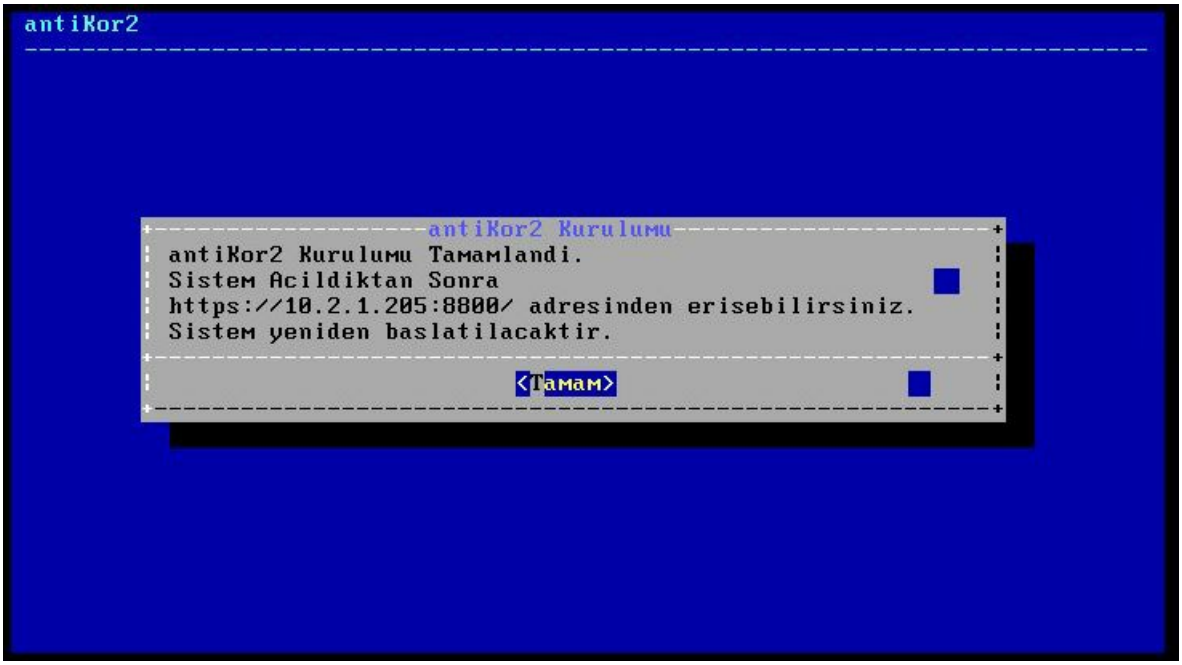




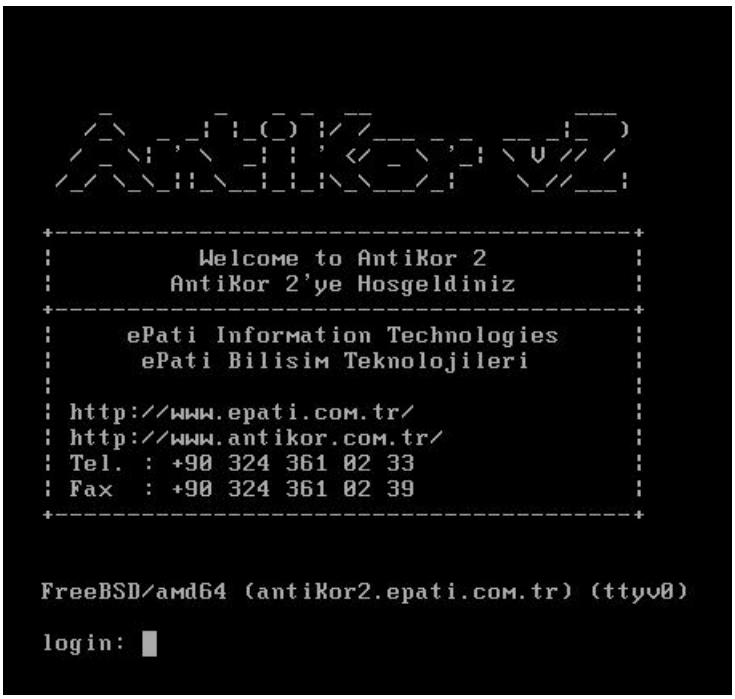
Kurulum için diskin biçimlendirilmesi gerekmektedir. Evet seçerek devam edilir.





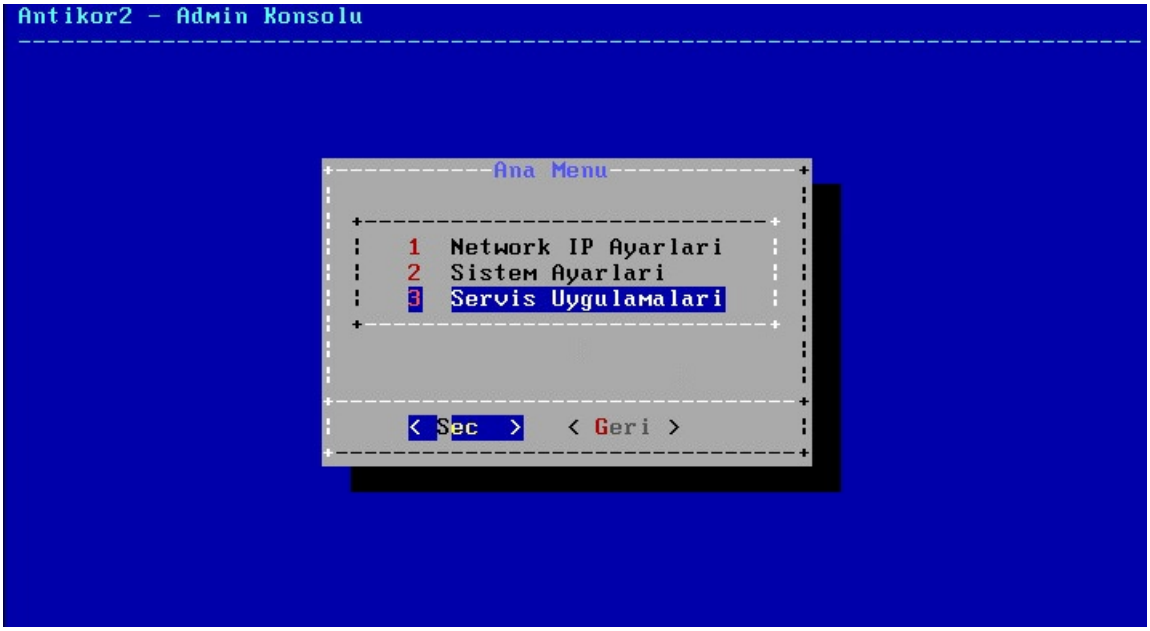


Bu aşamadan sonra kurulum tamamlanmıştır. Sunucu yeniden başlatılır. İlk başlatmadan sonra, ayarlar tamamlanır ve “login” ekranı gelir.

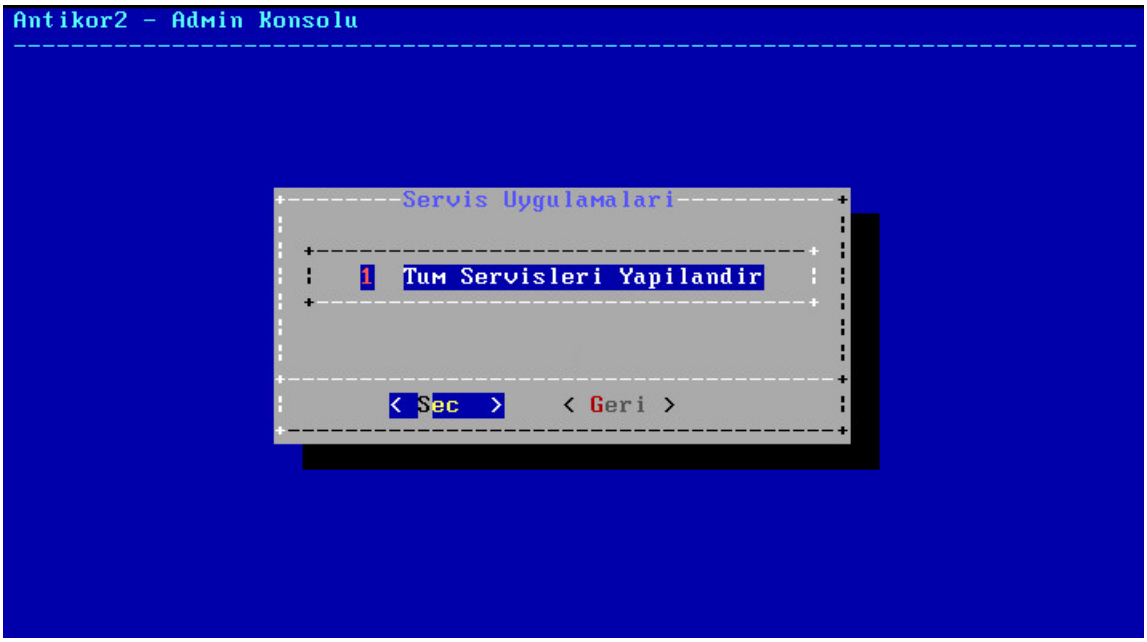


Kurulumdan Sonra Yapılması Gereken Adımlar

1. Servis Uygulamaları menüsüne girilir.



“Tüm Servisleri Yapılandır” butonuna tıklanır ve yapılandırmaların bitmesi gerekir.

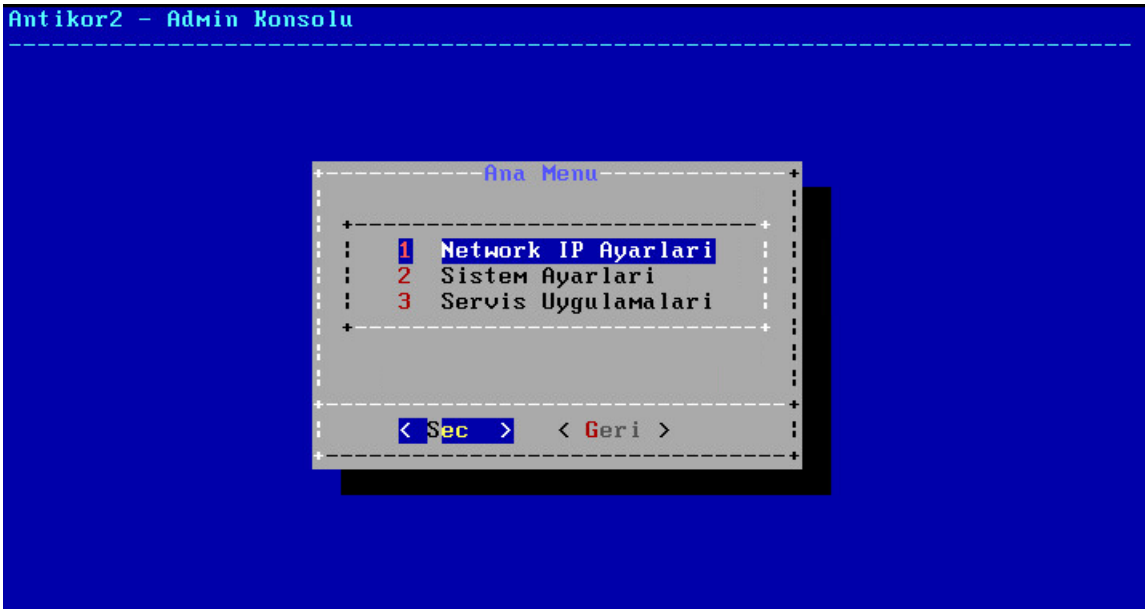


İşlem tamamlandıktan sonra Antikor bir defa yeniden başlatılır.

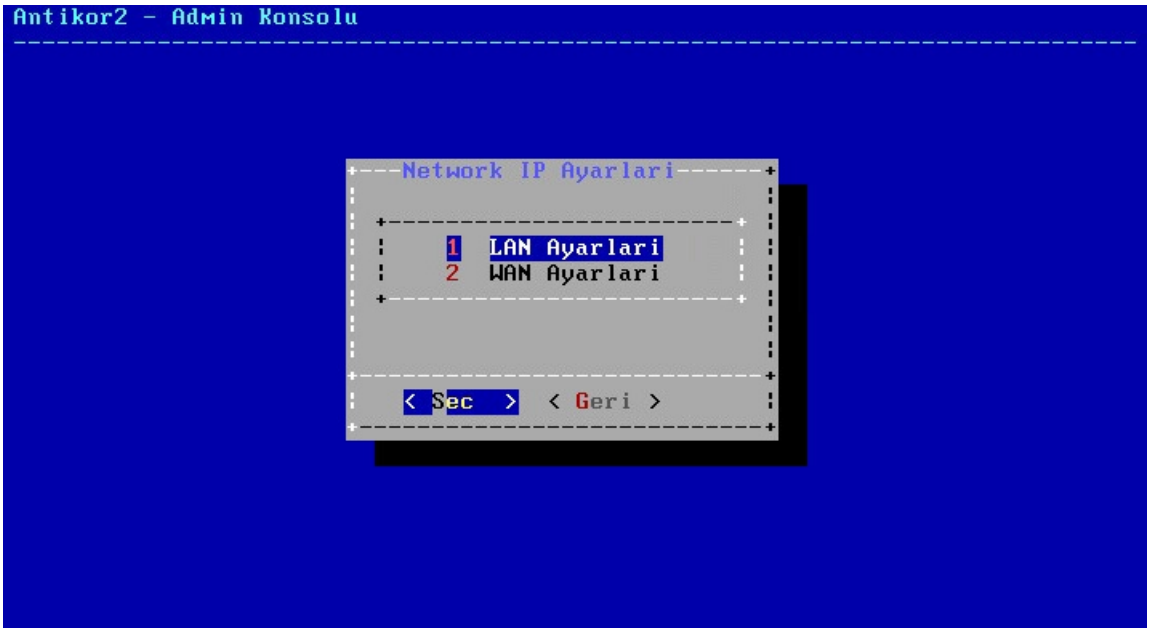
2. Admin konsolundan IP verilmesi gerekmektedir.

```
Kullanıcı adı: admin
Parola: antikor
```

İlk olarak yapılması gerekenler, Network & IP Ayarları menüsü açılır.



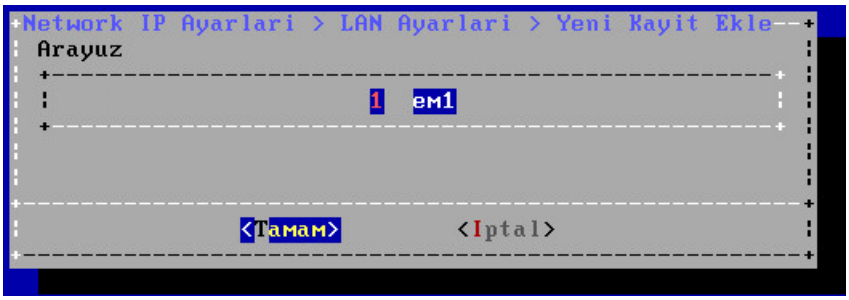
Düzenlenmesi istenilen ethernet bacağı seçilir.



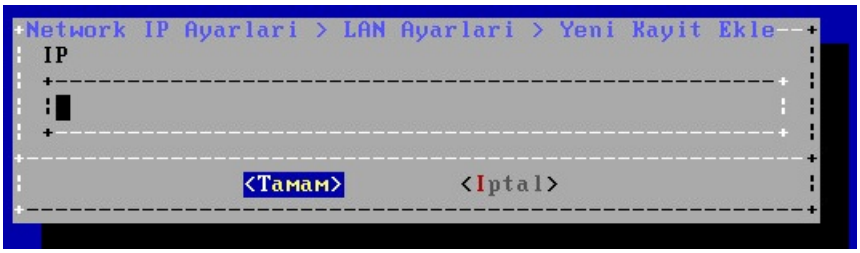
LAN Ayarları menüsünü açıldığında;

İki alt menü görülecektir. Hiç bir kayıt bulunmuyorsa, “Yeni Kayıt Ekleme Sihirbazı” seçilir.

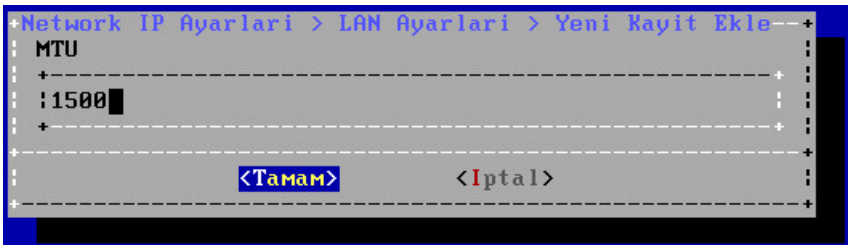
Yeni Kayıt Ekleme Sihirbazı seçildiğinde, cihazda bulunan ethernet portları görülecektir. LAN için kullanılacak ethernet portu seçilir.



IP alanına LAN IP bloğunda kullanılacak IP ve Alt Ağ Maskesi yazılır.



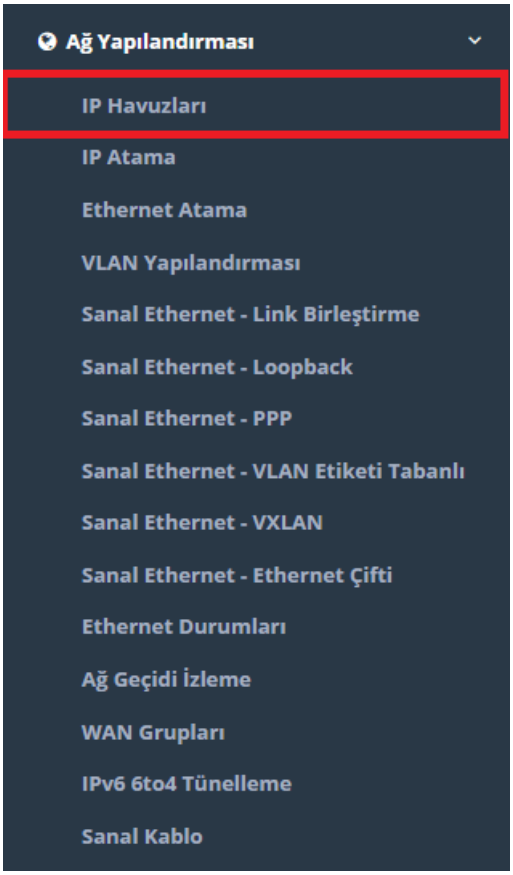
MTU değeri 1500 olarak bırakılır.



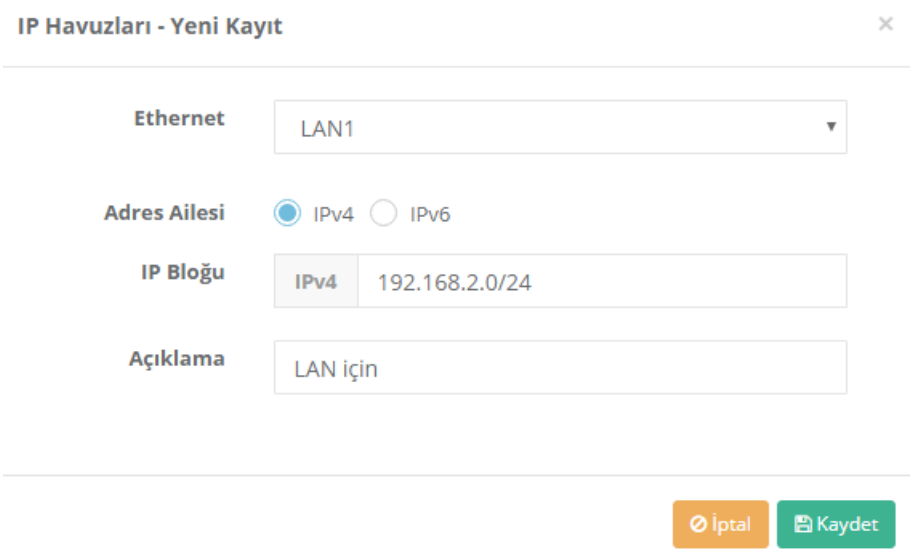
Bu işlemlerden sonra LAN bacağı için IP tanımlaması yapılmaktadır. Diğer ethernet bacakları için de aynı yol izlenerek IP adresleri verilebilir.

3. WEB arayüzüne girmek için LAN IP bloğunun kapsadığı bir IP'yi bilgisayara manuel olarak eklenebilir ve http://192.168.2.1:8800 IP adresi ile WEB arayüzüne ulaşılabilir.

4. Ağ Yapılandırması menüsü altında bulunan IP Havuzları sayfasına gidilir.

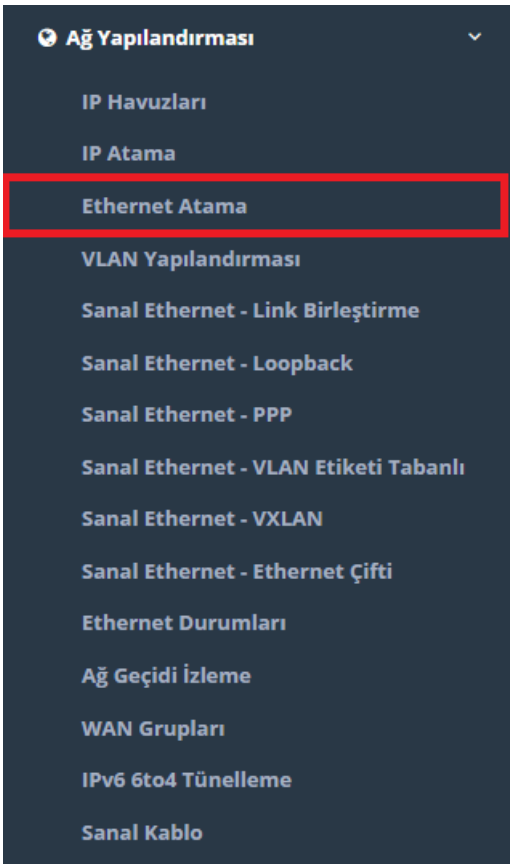


Ekle butonuna tıklandığında, LAN bloğu için IP Havuzu belirlenecektir.



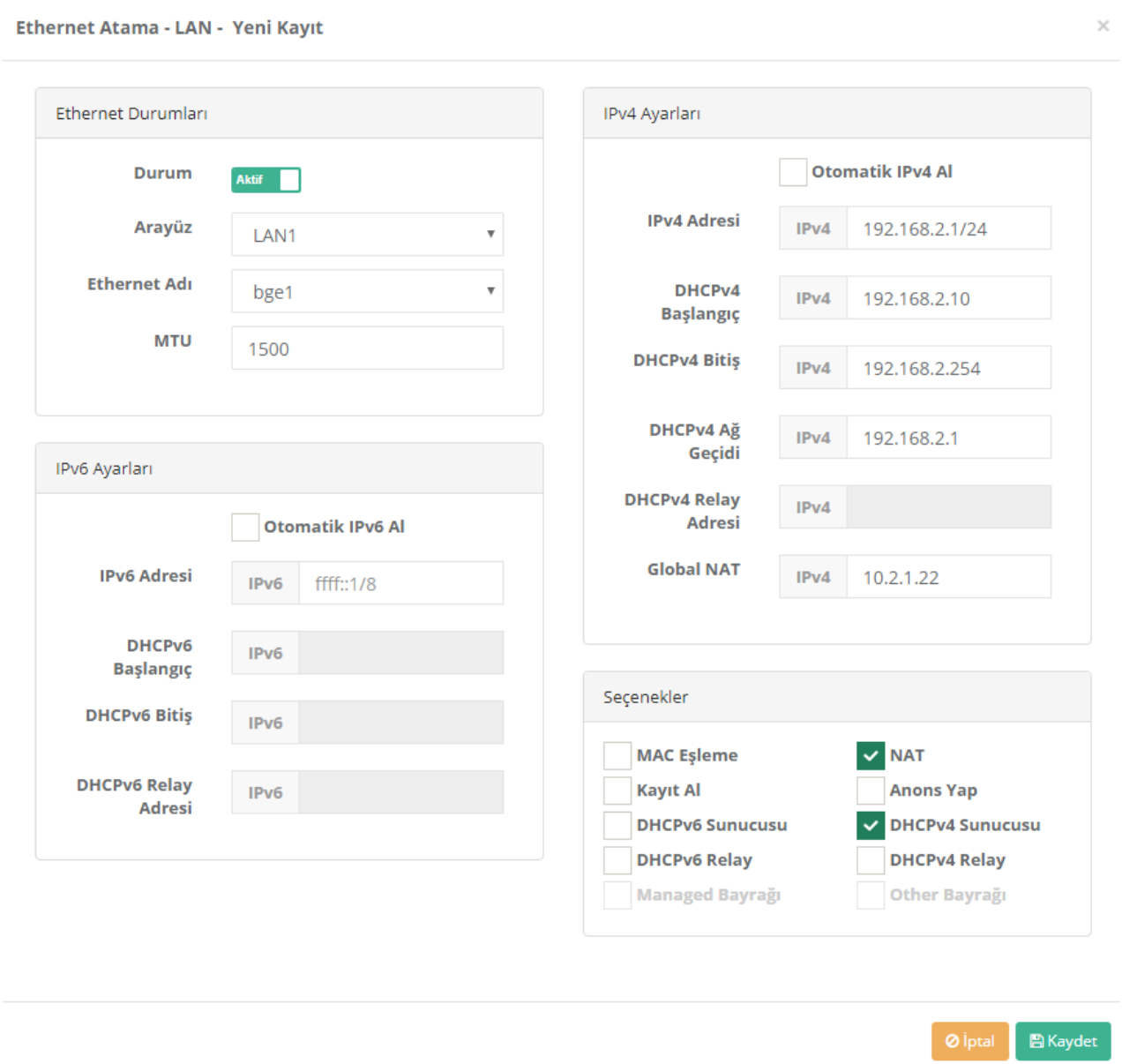
Kaydet butonuna tıklanarak LAN bacağı için IP Havuzu belirlenmiş olur. Diğer ethernet bacakları için de aynı yol izlenerek IP Havuzları verilebilir.

5. Ağ Yapılandırması menüsü altında bulunan Ethernet Atama sayfasına gidilir.



LAN Ekle butonuna tıklanarak, LAN Ethernet Ataması gerçekleştirilir.

LAN bacağı için ilgili ayarlar girilmiştir. Diğer ethernet bacakları içinde aynı yol izlenerek Ethernet Atama işlemi gerçekleştirilebilir.

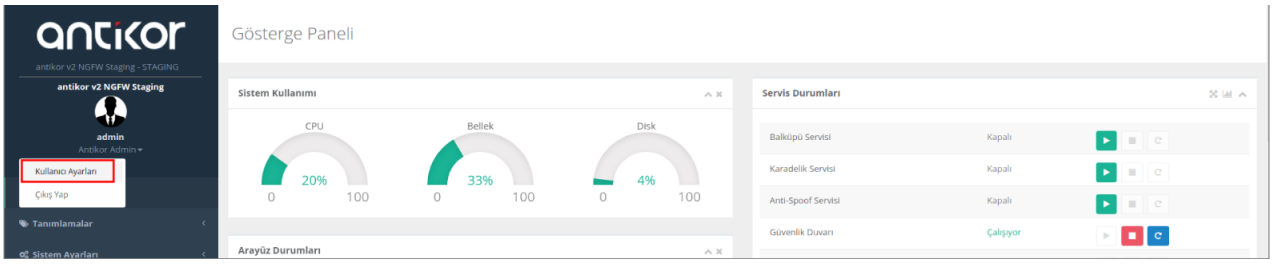


Ethernet atama işlemi yapılırken seçenekler bölümünde “DHCPv4 Sunucusu” işaretlenmiş ise; gösterge panelinde servis durumlarının altında bulunan DHCPv4 Servisi başlatılmalıdır.

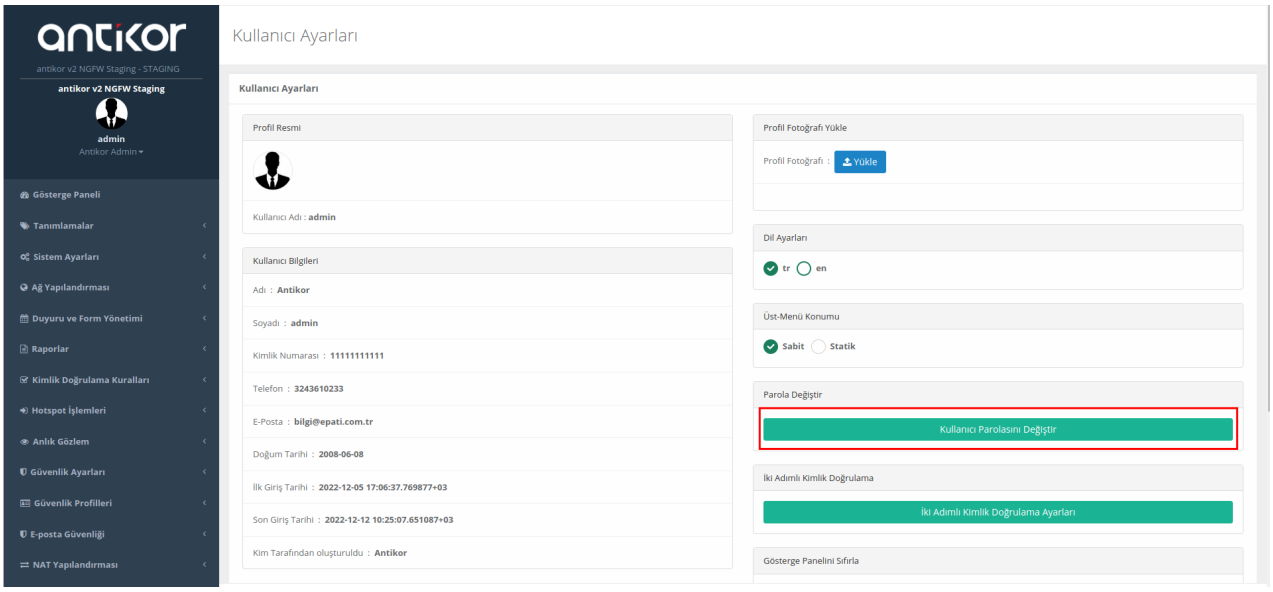
`Not:` Kurulum gerçekleştikten sonra ethernet kartı eklenmemelidir ve çıkarılmamalıdır.

6. admin kullanıcısının varsayılanda gelen şifresinin(antikor) değiştirilmesi gerekmektedir.

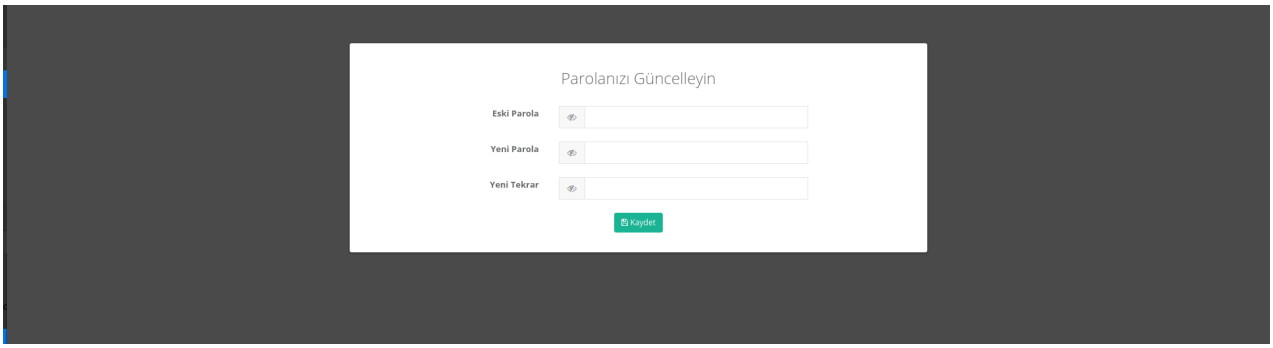
- Kullanıcı Ayarları sayfasına gidilir.

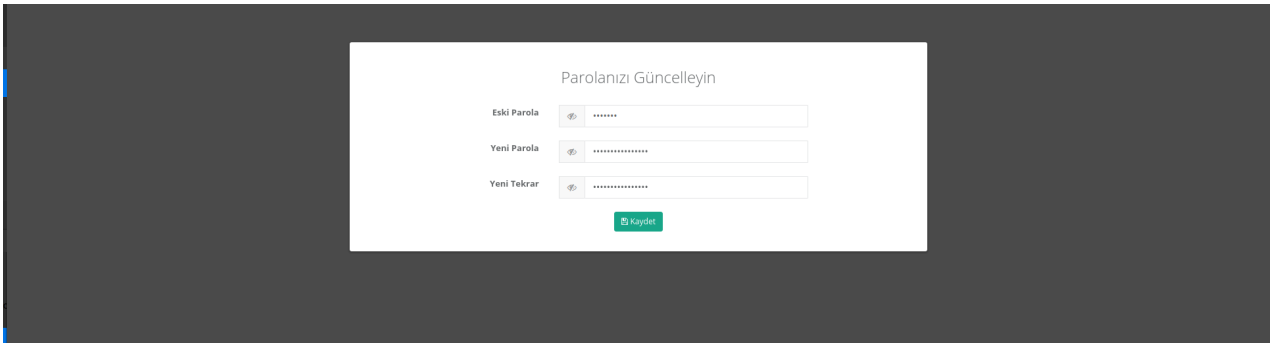


- Kullanıcı Ayarları sayfasında **Kullanıcı Parolasını Değiştir** butonuna tıklanır.

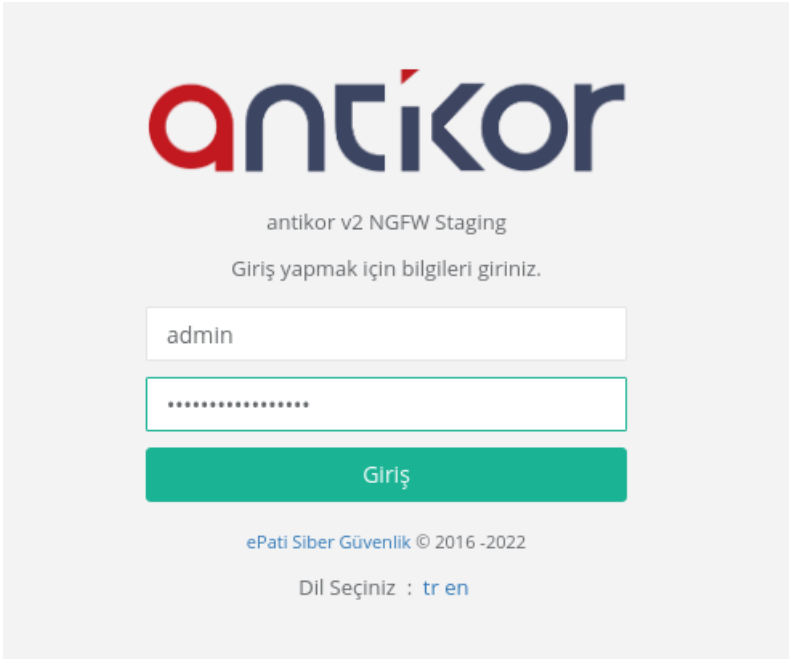


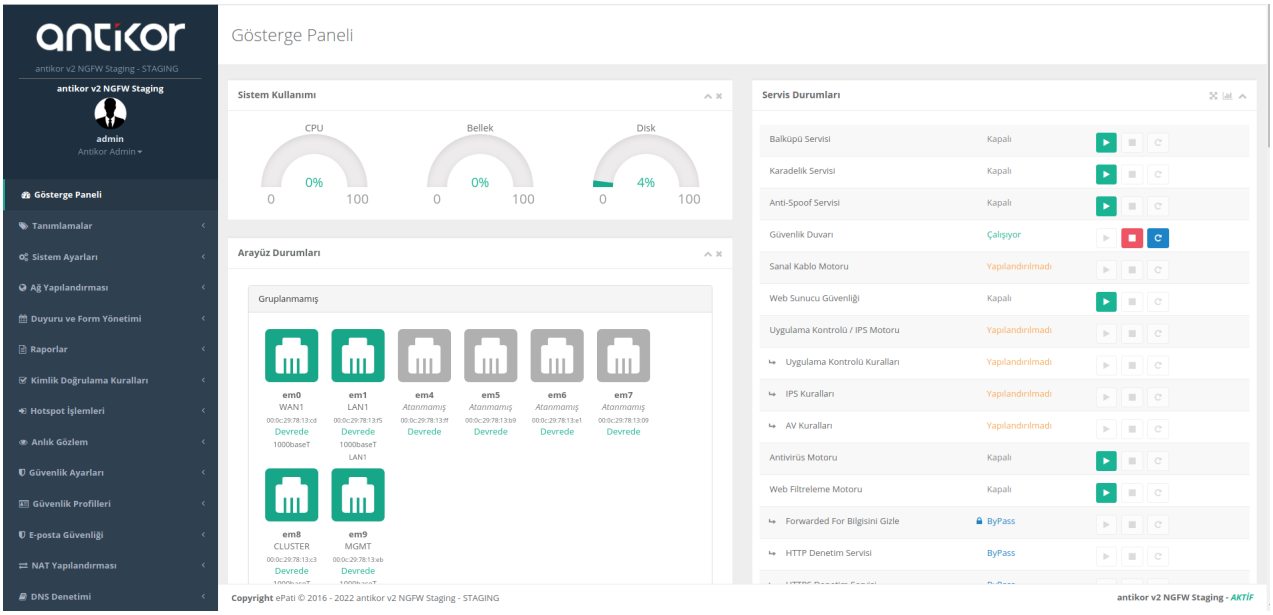
- Parola değiştirilir.





- Parola değiştirildikten sonra admin kullanıcısına atanmış yeni parola ile giriş yapılır.



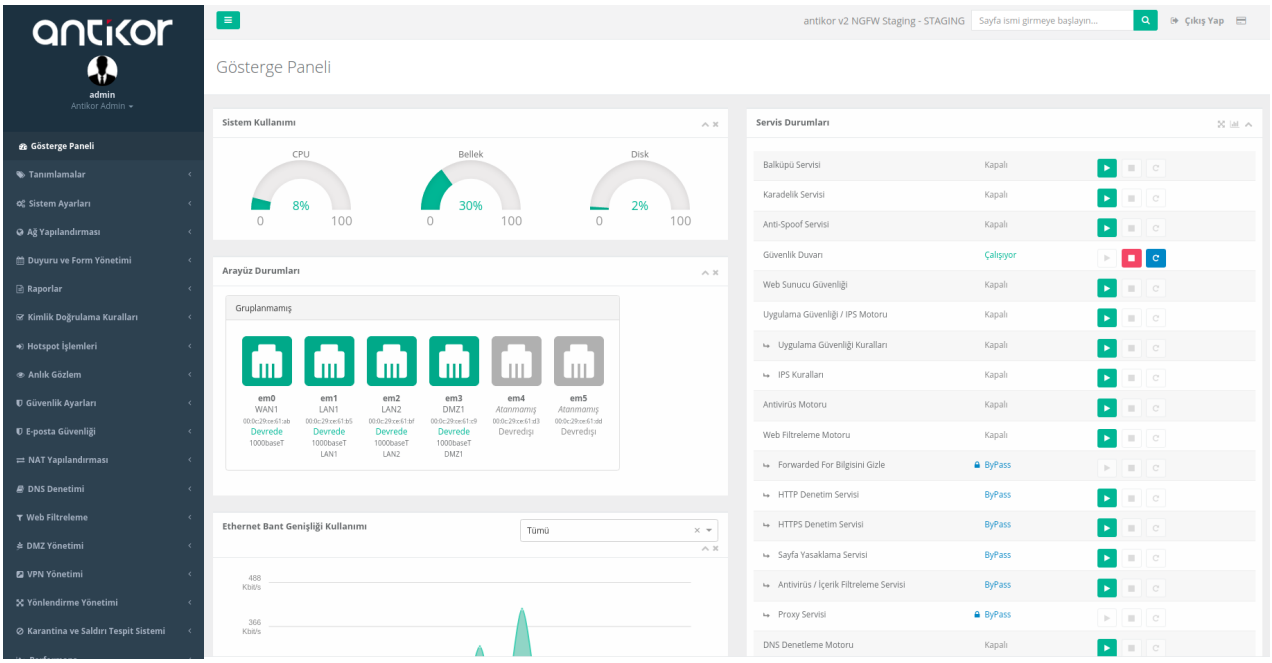


Antikor Güvenlik Duvarının WEB arayüzüne nasıl girilir?

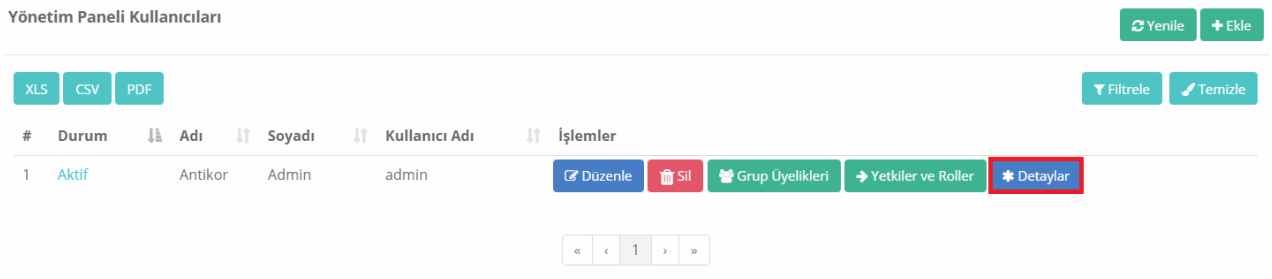
Bilgisayarda bulunan herhangi bir web tarayıcısı (Internet Explorer, Chrome, Firefox, vb.) ile cihaza erişip gerekli ayarlar yapılabilmektedir. Yazılım ayarlarını yapmadan önce yukarıdaki gibi Antikorun kurulum IP adreslerinin doğruluğundan ve kabloların takılı olduğundan emin olunuz. Antikor sunucusu açıldıktan sonra;

- Tarayıcının adres kısmına sunucuya verilmiş olan IP adresihttps://10.2.1.205:8800 girilir. Port 8800 olduğu için “https://” nin yazılması unutulmamalıdır.

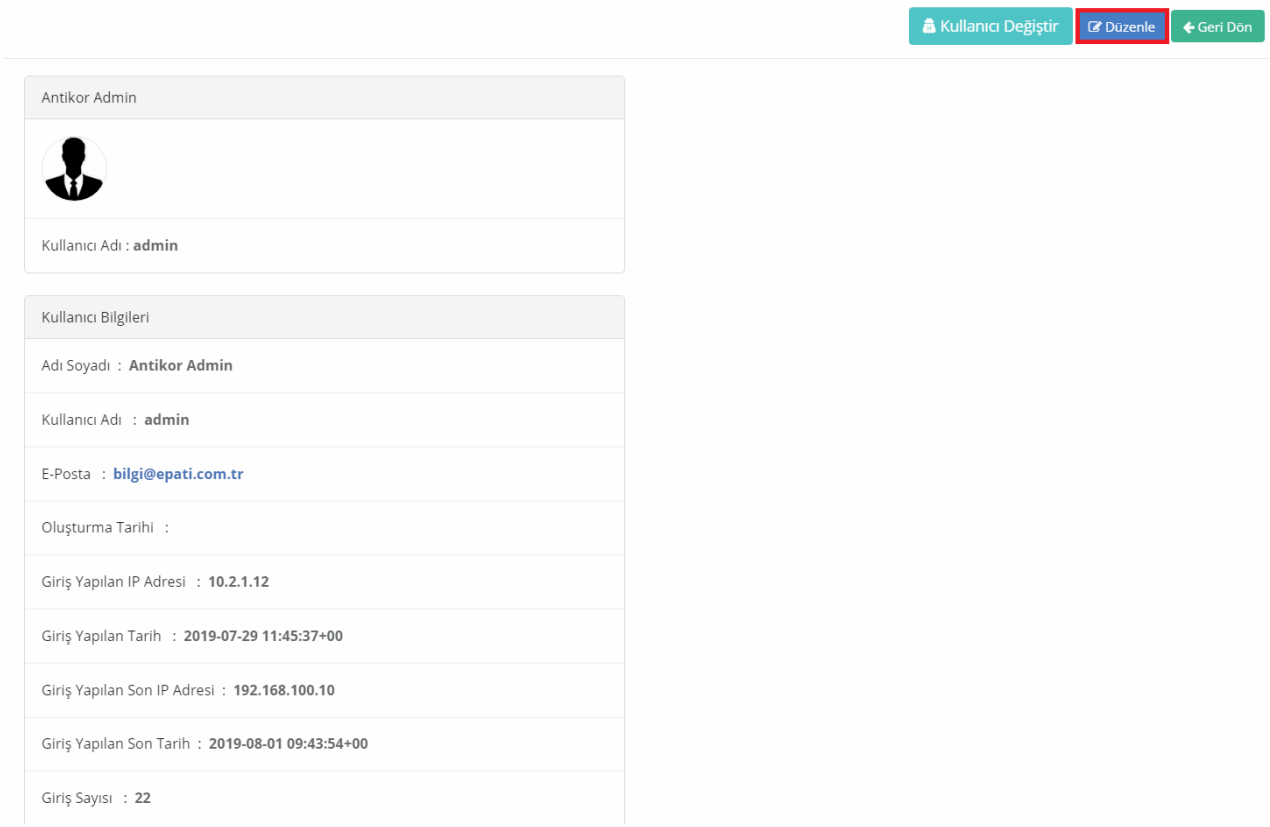
- Giriş ekranı gelecektir. Kullanıcı adı “admin” ve parolayı “antikor” yazarak`Giriş` butonuna tıklanır.



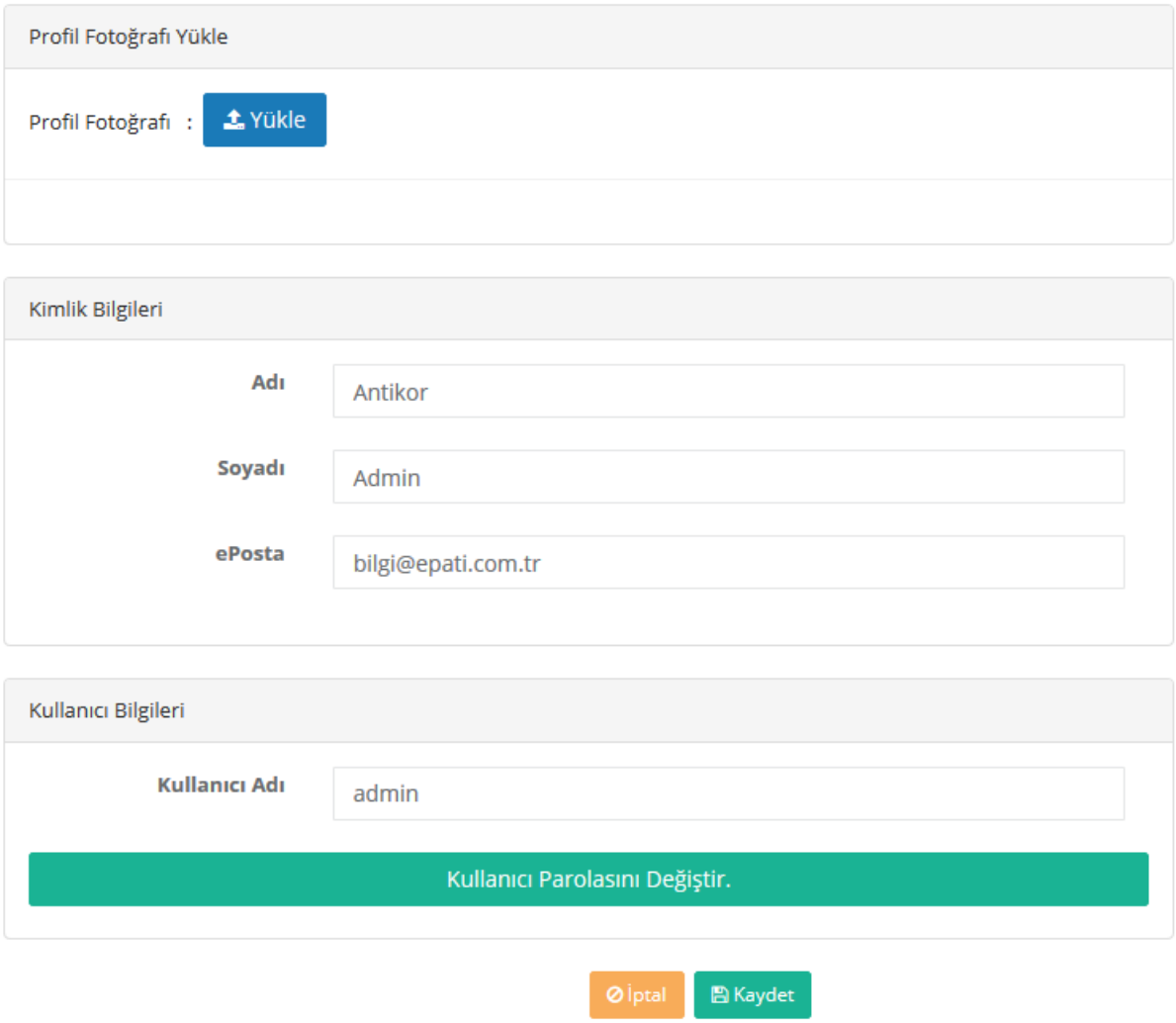
Arayüze giriş yapıldıktan sonra ilk adım olarak güvenlik amacı ile Parolanın değiştirilmesi gerekmektedir. Kullanıcı Yönetimi menüsü altında bulunan Yönetim Paneli Kullanıcıları sekmesine tıklanır.



Ardından “Detaylar” butonuna tıklanır.



Açılan sayfada “Düzenle” butonuna tıklanır.

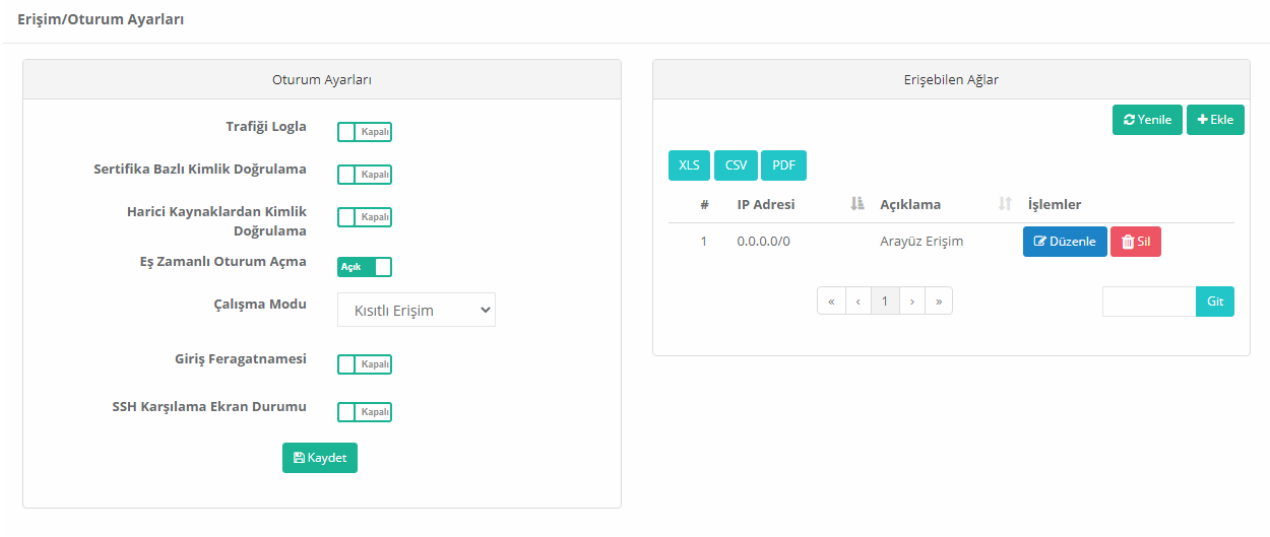


Kullanıcı Parola Günceleme

Kullanıcı bilgileri bölümünde yeni Parola belirlenerek “Kaydet” butonuna tıklanır.

Kurumsal Güvenlik Politikası

Kurulum tamamlandıktan sonra, kurulum sırasında `Yetkili IP Adresi` alanına girilen istemciden başka yetkili istemci var ise Antikor ürünü web arayüzünden bu yetkiler tanımlanmalıdır. Bunun için `Yönetim Paneli Ayarları` > Erişim / Oturum Ayarları menüsünden arayüze erişmeye yetkili diğer istemcilerin IP adresleri tanımlanabilir. Tanımlanan yetkili istemcilerin IP adreslerinin ağınızda kullanılan mimariye bağlı olarak değişmediğinden emin olunuz.



Güvenli Mod

Antikor kurulumu gerçekleştirildikten sonra RAM haricinde herhangi bir donanım(ethernet kartı, harddisk vb.) eklenildiği zaman, Antikor güvenlik amacıyla “Güvenli Moda” geçiş yapacak ve işlevini yerine getirmeyecektir. Bu durumda, Antikor’un Güvenli Moddan önceki işlevine devam edebilmesi için eklenilen donanım sökülmelidir. Eklenilen donanımın Antikorla uyumlu bir şekilde çalışabilmesi için yeniden kurulum yapılması gerekmektedir.

Sistemde Oluşan Bir Failure Sonrasında Gerçekleştirilecek Eylemler

Sistemde herhangi bir arıza yaşanması durumunda lütfen aşağıdaki adımları takip ediniz.

1. Yaşanan arıza ile ilgili olarak, arızanın ne zaman ve hangi işlemden sonra ortaya çıktığı, karşılaşılan detaylar ve varsa hata çıktısı ile birlikte teknik destek talep edilmelidir.

2. Yaşanan arıza sadece belli servisleri etkiliyorsa, ilgili servis kapatılmalıdır.

3. Yaşanan arıza tüm sistemi olumsuz etkiliyor ve yedek sistemin mevcut olması halinde yedek sistem devreye alınmalıdır.