İçerik

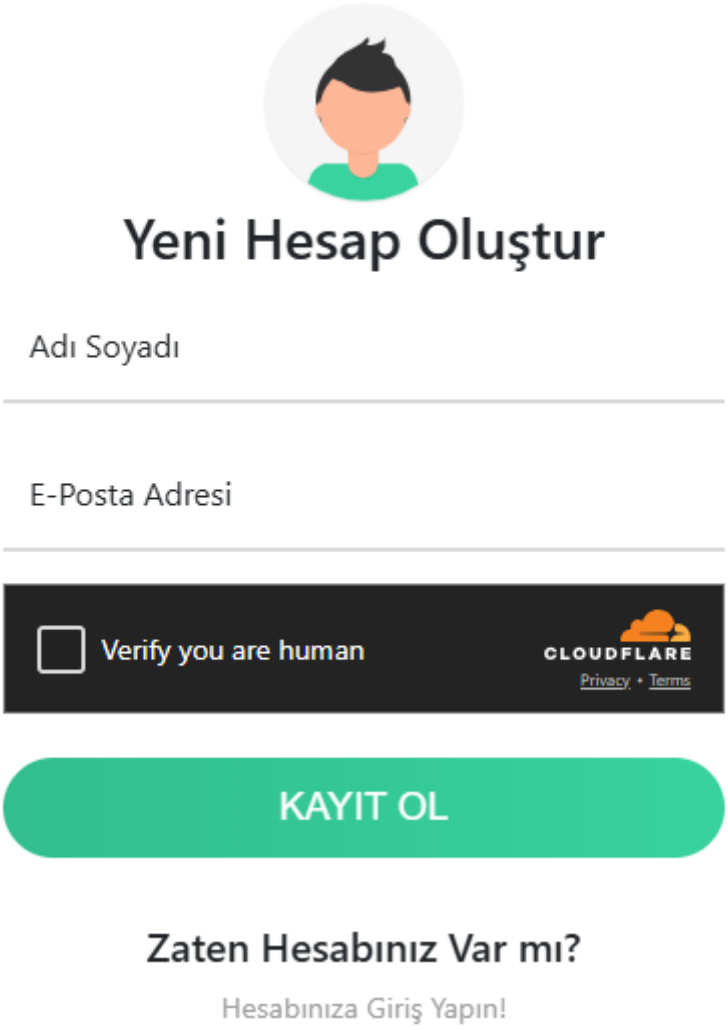
CyCastle'a Katılma ve Hesap Oluşturma 3
Hediye 100 Kredimi Nasıl Alabilirim? 5
Nasıl Şirket Oluşturabilirim? 6
ThreatChaser Ürün Anahtarını Nasıl Bulabilirim? 8
ThreatChaser Nasıl Kurulur? 9
1.VMWare Pro Ajan Kurulumu 10
2.VMWare ESXI Kurulumu 14
3.Hyper-V Ajan Kurulumu 18
Web Taraması İçin Nasıl Alan Adı Ekleyebilirim? 26
Alan Adımı Nasıl Doğrulayabilirim? 27
Nasıl Web Taraması Başlatabilirim ? 29
Web Tarama Sonuçlarımı Nasıl Görüntüleyebilirim? 31
CVE Zafiyetlerini Nasıl Görüntüleyebilirim ? 32
OVAS Zafiyetlerini Nasıl Görüntüleyebilirim ? 32
Zafiyet Raporumu Nasıl Görüntüleyebilirim? 33
Nasıl Ağ Taraması Başlatabilirim? 34
Ağ Tarama Sonuçlarını Nasıl Görüntüleyebilirim? 36
Siber Tehdit İstihbaratı (CTI) Nasıl Kullanabilirim ? 37
Alan Adlarımı Nasıl İzleyebilirim ? 37
Kişisel E-posta Hesaplarımı Nasıl İzleyebilirim? 38
Yeni E-posta Hesabı Nasıl Ekleyebilirim ? 38
Nasıl Alt Hesap Ekleyebilirim ? 39
Yeni Kullanıcı Nasıl Ekleyebilirim? 41
Şifremi Nasıl Değiştiririm? 42
Yeni Klasör Nasıl Oluştururum ve İçerisine Nasıl Şirket Ekleyebilirim? 45
Oturum Açma Aktivitelerimi Nasıl Görebilirim ? 46
Destek Kaydı Nasıl Oluşturabilirim ? 47
Beyaz Etiket (White Label) Ayarlarını ve Logonuzu Nasıl Özelleştirebilirsiniz? 50
5651 Loglama ve HotSpot Hizmetini Nasıl Aktif Edebilirim? 52
Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim? 56
Watchguard Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim? 56
FortiGate Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim? 58
Sophos Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim? 59
AIMdefense Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim? 61

Ruijie Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim? 64
Ruijie Reyee Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim? 66
Cloud Üzerinden Yönlendirme 66
Lokal Arayüz Üzerinden Yönlendirme 68
Cihazımdan HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim? 70
FortiGate API İşlemleri 70
FortiGate Cihazımdan HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim? 72
ThreatChaser Tarafındaki Ayarlamalar 72
Firewall Tarafındaki Ayarlamalar 75
Sophos Cihazımdanda HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim? 79
ThreatChaser Tarafındaki Ayarlamalar 79
Firewall Tarafındaki Ayarlamalar 81
AIMdefense Cihazımdanda HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim? 88
ThreatChaser Tarafındaki Ayarlamalar 88
Firewall Tarafındaki Ayarlamalar 90
Ruijie Cihazımdanda HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim? 96
ThreatChaser Tarafındaki Ayarlamalar 96
Firewall Tarafındaki Ayarlamalar 98
WatchGuard Cihazımdanda HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim? 104
ThreatChaser Tarafındaki Ayarlamalar 104
Firewall Tarafındaki Ayarlamalar 106
Ruijie Reyee Cihazımdanda HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim? 109
ThreatChaser Tarafındaki Ayarlamalar 109
Firewall Tarafındaki Ayarlamalar 111
SSL Kontrol Aracı Hizmetini Nasıl Aktif Edebilirim? 114
VPN Hizmetini Nasıl Aktif Edebilirim? 116
İki Faktörlü Doğrulamayı Nasıl Aktif Edebilirim? 118

CyCastle’a Katılma ve Hesap Oluşturma

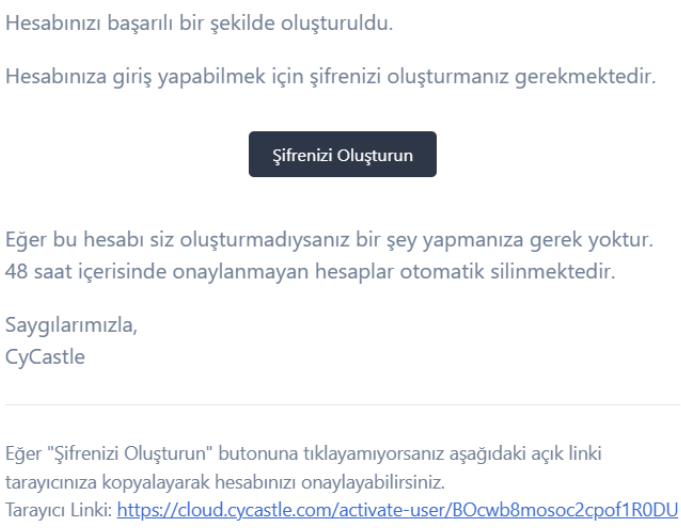
Hesap oluşturma sayfasına erişmek için aşağıdaki bağlantıya tıklayabilirsiniz:

https://cloud.cycastle.com/register

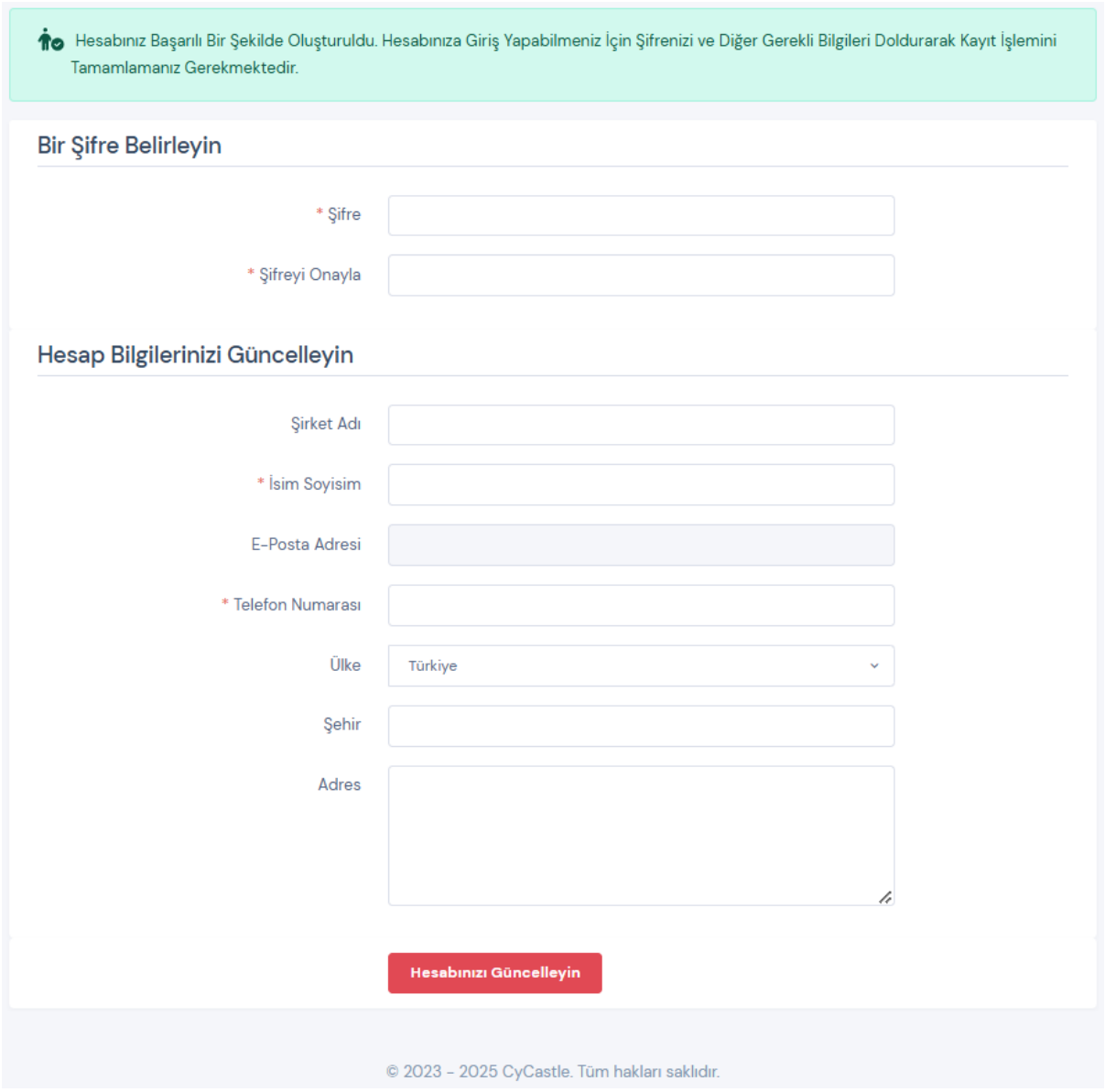


Adınızı ve soyadınızı girerek, robot olmadığınızı doğruladıktan sonra “**Kayıt Ol**” butonuna tıklayınız. Kayıt işleminin ardından e-posta adresinize bir onay mesajı iletilecektir. Gelen e-postada yer alan “**Şifrenizi Oluşturun**” butonuna veya bağlantıya tıklayarak, kayıt sürecinizi tamamlayabilirsiniz.

Eğer onay e-postası 24 saat içerisinde tarafınıza ulaşmazsa, **support@cycastle.com** adresine e-posta göndererek destek talebinde bulunabilirsiniz.

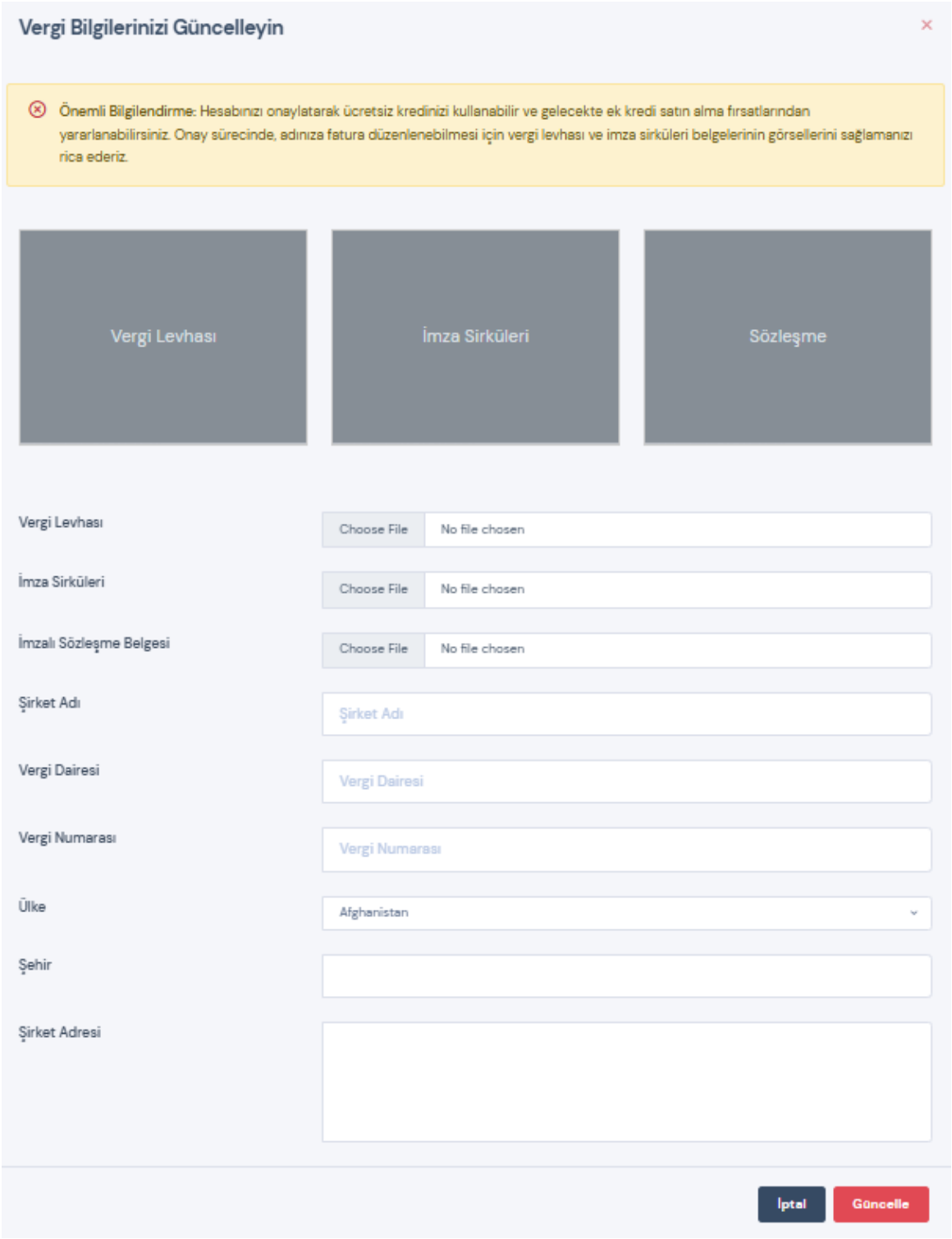


Gerekli bilgileri eksiksiz olarak doldurduktan sonra “**Hesabınızı Güncelleyin**” butonuna tıklayarak hesap oluşturma işlemini tamamlayabilirsiniz.



Hediye 100 Kredimi Nasıl Alabilirim?

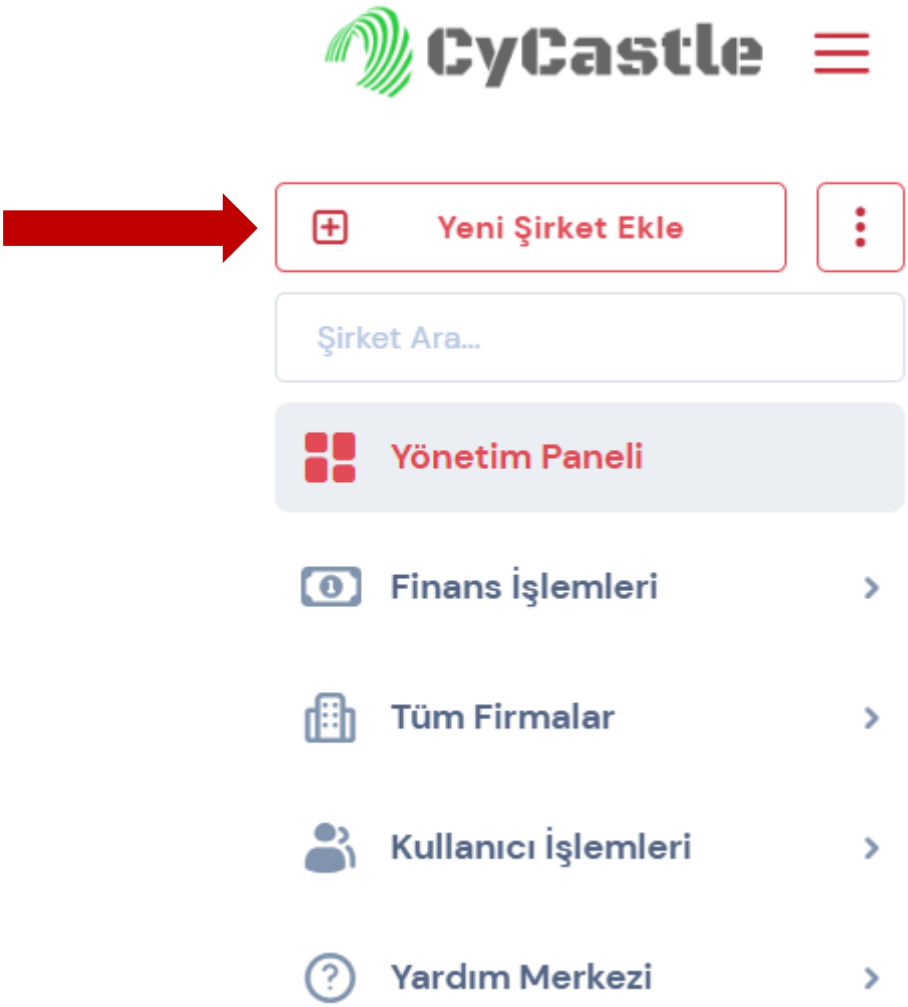
Yönetim Panelinde bulunan **“Bonus Kredinizi Aktif Edin”** butonuna tıklayarak hediye 100 kredinizi almak için başvuru yapabilirsiniz.



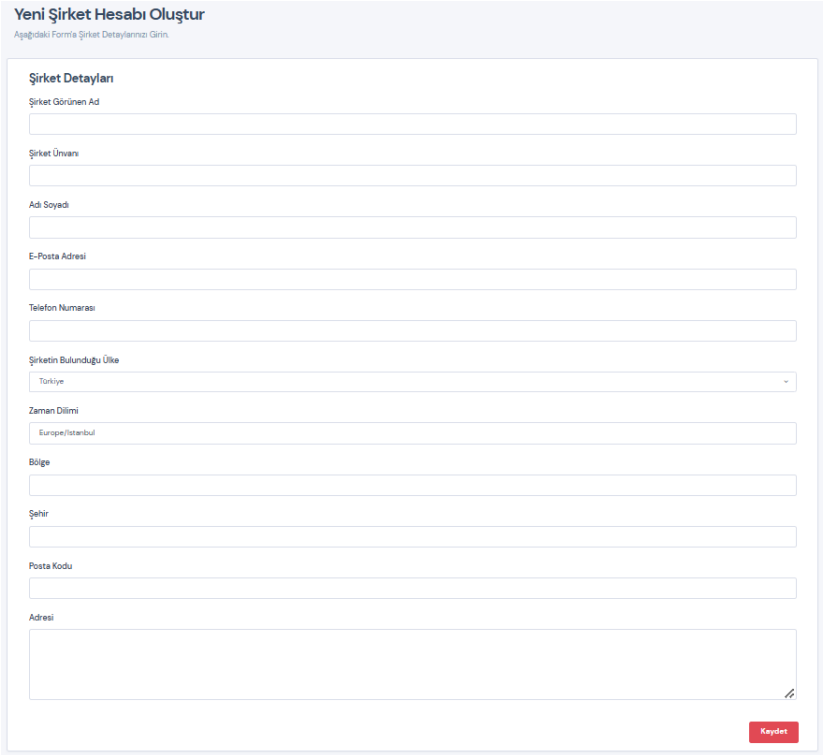
İletmiş olduğunuz bilgiler, onay sürecine alınacak olup, gerekli incelemelerin ardından hesabınıza 100 kredi tanımlanacaktır.

Nasıl Şirket Oluşturabilirim?

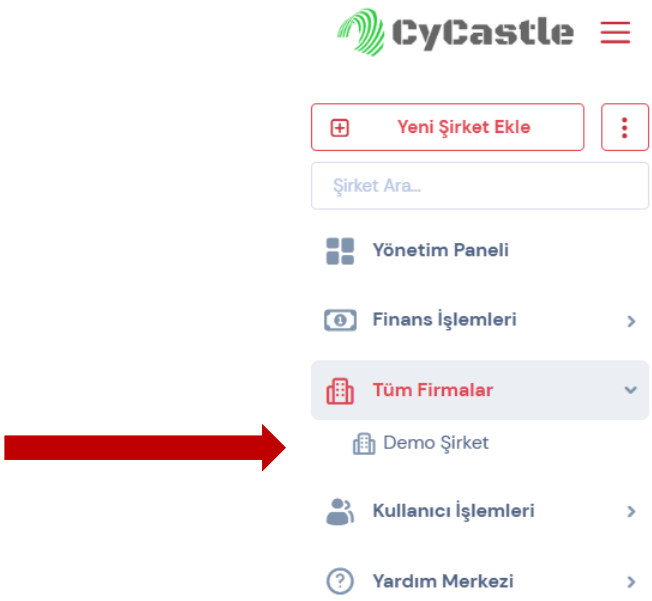
Menü üzerinden **“Yeni Şirket Ekle”** butonuna tıklayarak yeni bir şirket oluşturma sürecini başlatabilirsiniz.



Gerekli alanları eksiksiz şekilde doldurduktan sonra “**Kaydet**” butonuna tıklayarak işlemi tamamlayabilirsiniz.

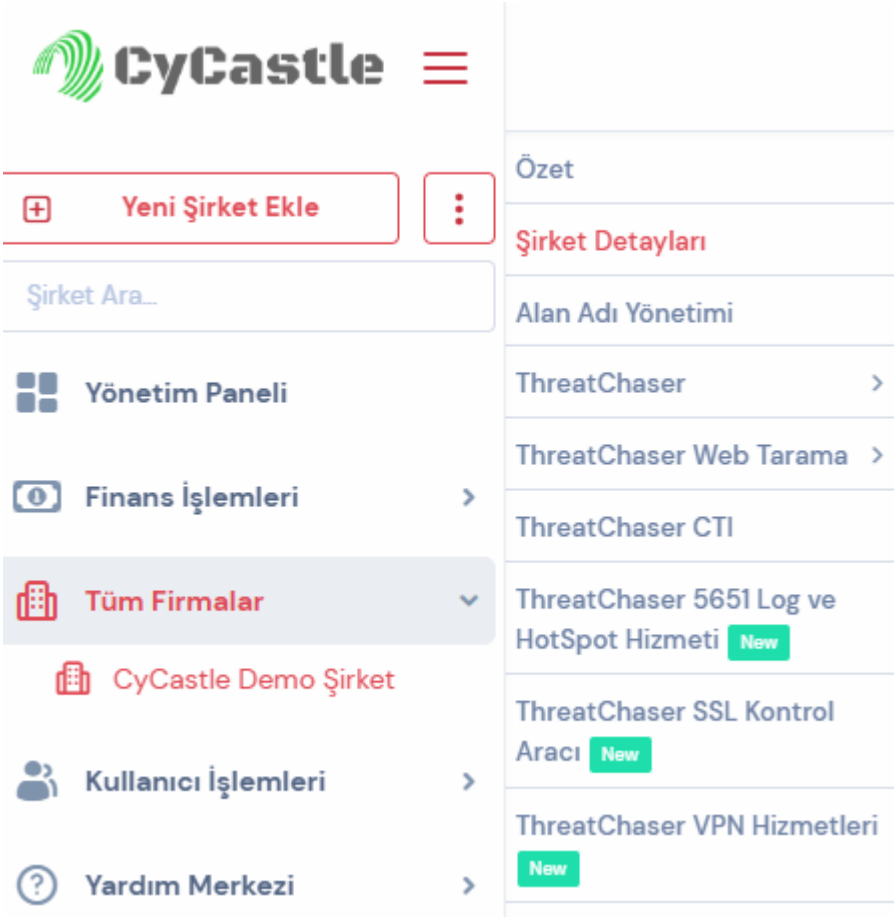


Oluşturduğunuz şirket, “**Tüm Firmalar**” menüsü altında listelenecektir.

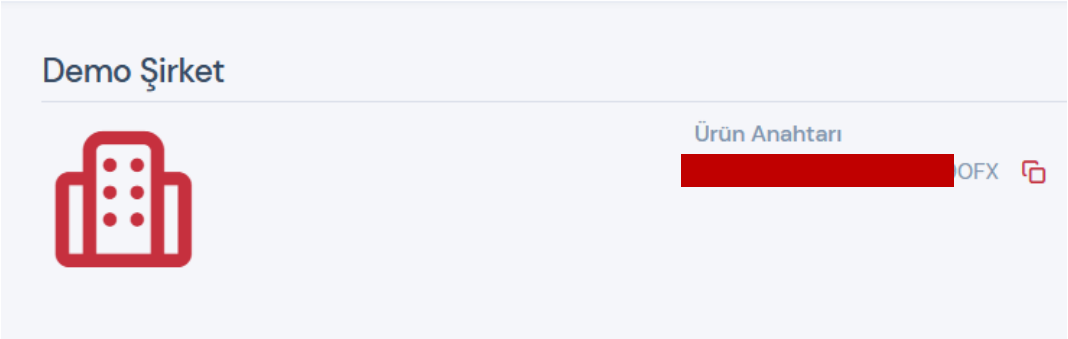


ThreatChaser Ürün Anahtarını Nasıl Bulabilirim?

Ürün anahtarınızı almak için, menüden ilgili şirketi seçin ve "**Şirket Detayları**" butonuna tıklayın.

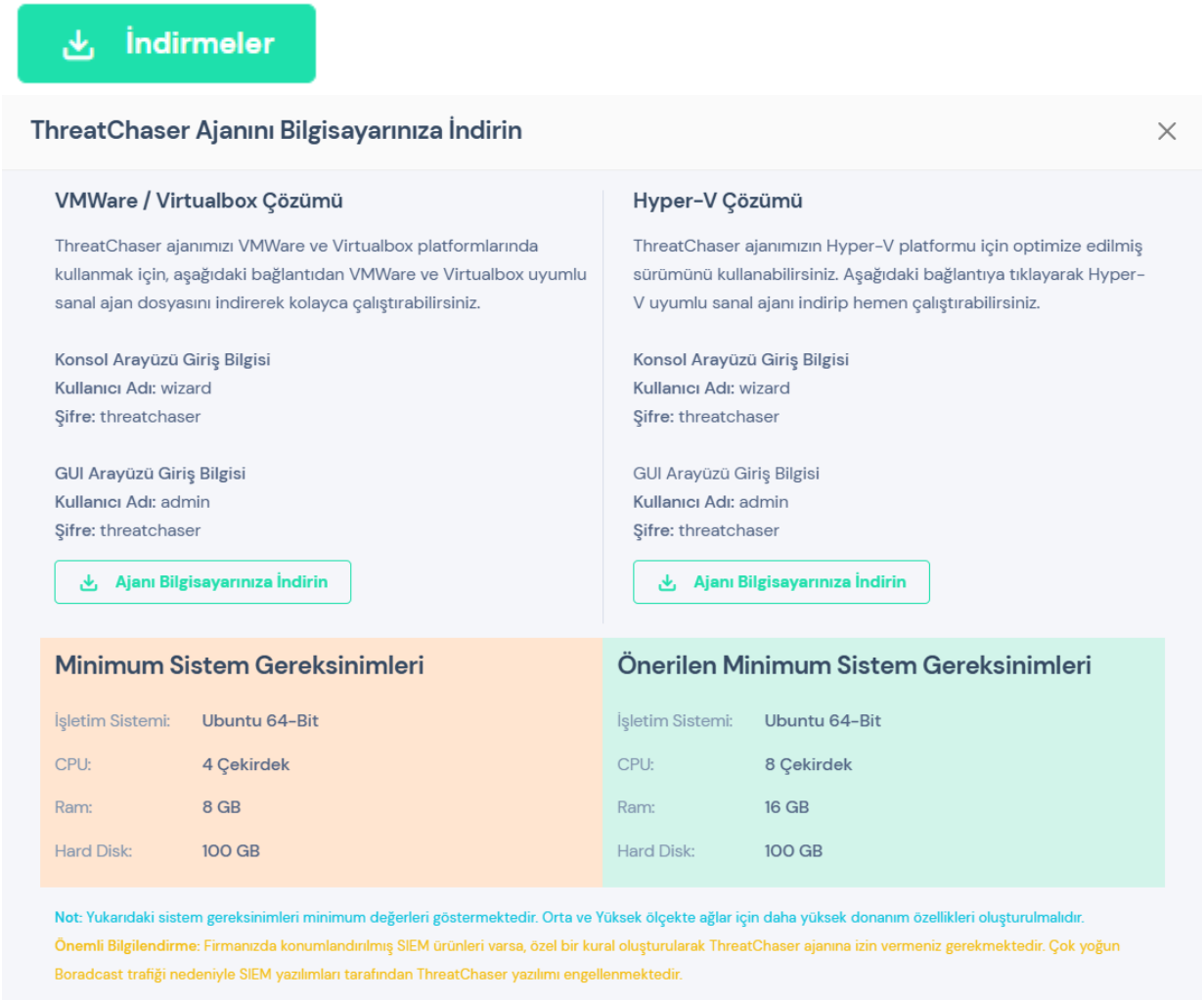


"**Şirket Detayları**" menüsünde ürün anahtarınızı bulabilirsiniz.



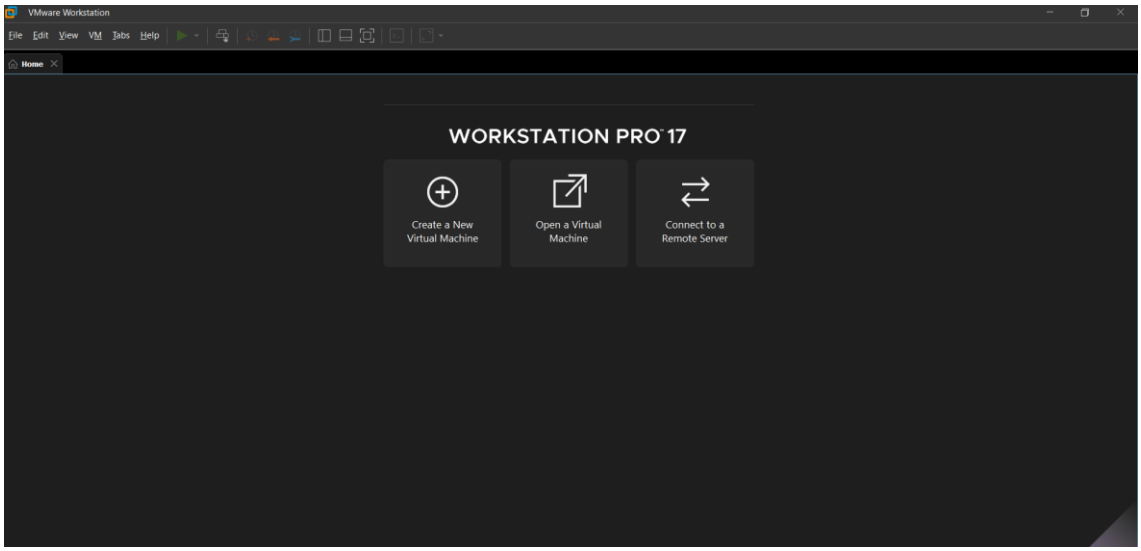
ThreatChaser Nasıl Kurulur?

Ekranın üst kısmında bulunan **“İndirmeler”** butonuna tıklayarak, açılan sayfadan size uygun sanallaştırma çözümünü indirip, sunucunuza kurabilirsiniz.

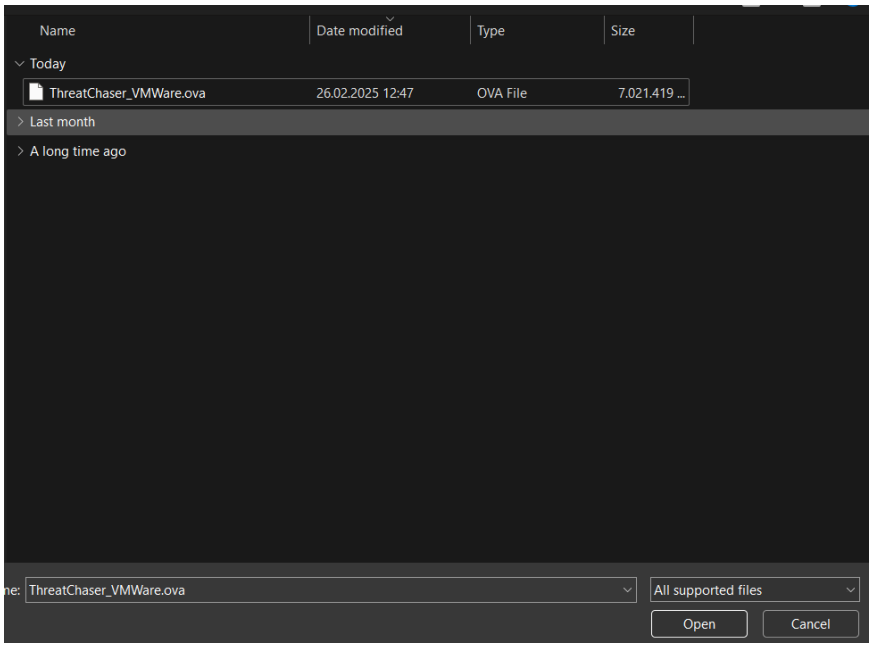


1.VMWare Pro Ajan Kurulumu

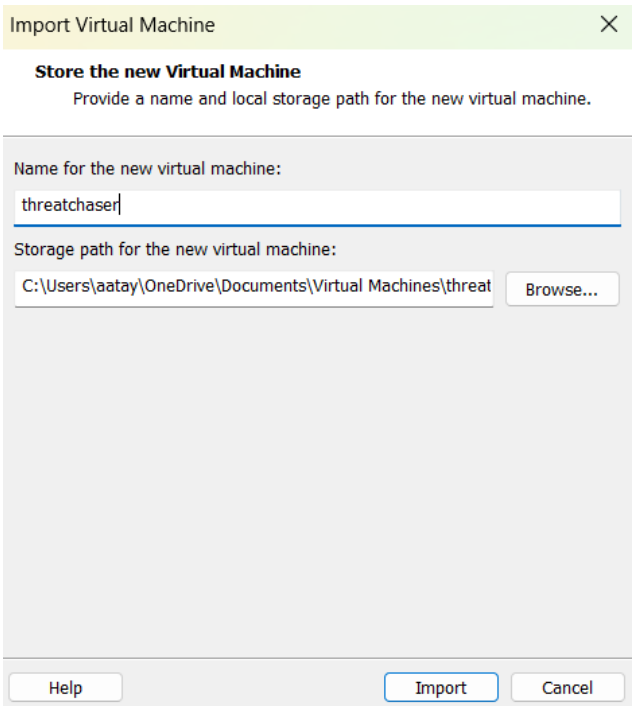
1.VMWare programını başlattıktan sonra sanal makineyi aç butonuna basıyoruz



2.Gelen pencerede ajanımızı seçip devam ediyoruz.



3.Sanal makinemize bir isim veriyoruz ve ilerliyoruz.



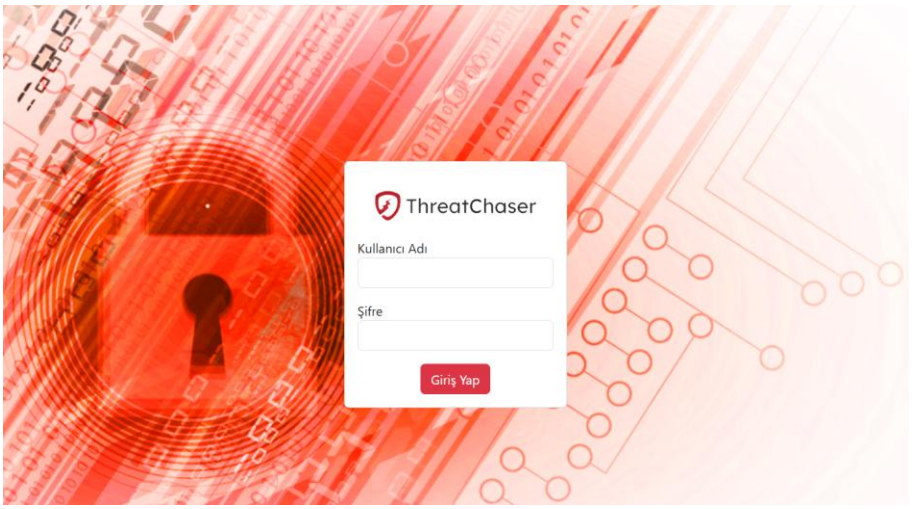
4.Açılan pencerede sanal makinemizi başlatıyoruz.

5.Açılan ekranda varsayılan değerler gözükecektir fakat dilerseniz değiştirmek için “Enter” tuşuna basabilirsiniz ve daha sonra Konsol Arayüzü Giriş bilgilerini girerek istediğiniz değerleri atayabilirsiniz (Eğer DHCP servisi tarafından ip sabitlemesi yapacaksanız bu adımı atlayın.)

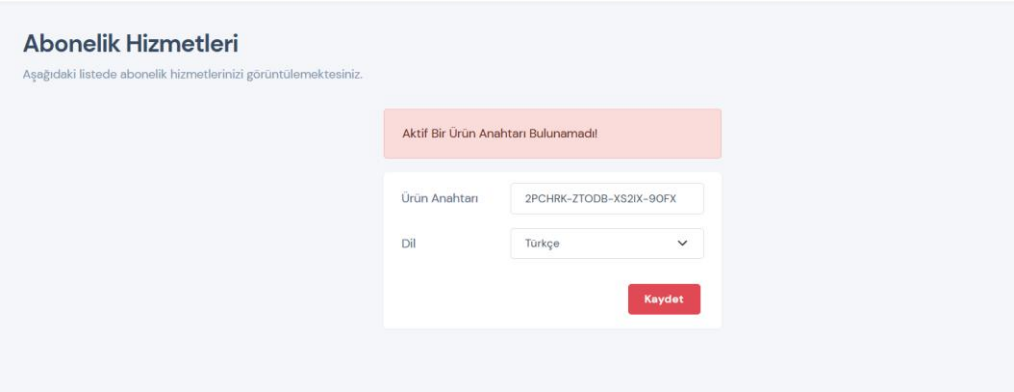
- wizard / threatchaser giriş bilgileri ile giriş yapın
- Network Konfigürasyonu için “1” değerini giriniz.
- Statik IP için “2” değerini giriniz ve gerekli ip bilgilerini girerek ip sabitleme işlemi tamamlayınız.

```
 _____ _                                  _     ____ _
|_   _| |__  _ __ ___  __ _| |_ / ___| |__   __ _ ___  ___ _ __
  | | | '_ \| '__/ _ \/ _` | __| |   | '_ \ / _` / __|/ _ \ '__|
  | | | | | | | |  __/ (_| | |_| |___| | | | (_| \__ \  __/ |
  |_| |_| |_|_|  \___|\__,_|\__|\____|_| |_|\__,_|___/\___|_|


Ağ Bilgileri:
IP Adresi: 192.168.100.116
Netmask: 255.255.255.0
Gateway: 192.168.100.1
Hostname: ThreatChaser

==============================
       Ana Menü
==============================
1) Network Konfigürasyonu
2) Kullanıcı Şifre Sıfırlama
3) Fabrika Ayarlarına Dön
4) Yeniden Başlat
5) Sistemi Kapat
==============================
Seçiminiz (1-5): 1
Ağ yapılandırma türünü seçin:
1) Dinamik IP (DHCP)
2) Statik IP
Seçiminiz (1/2): 2
IP adresini girin (Varsayılan: 192.168.100.116): 192.168.100.25
CIDR girin (0-32, Varsayılan: 24): 24
Gateway girin (Varsayılan: 192.168.100.1): 192.168.100.1
DNS girin (Varsayılan: 1.1.1.1): 1.1.1.1
Hostname girin (Varsayılan: ThreatChaser): ThreatChaser
```

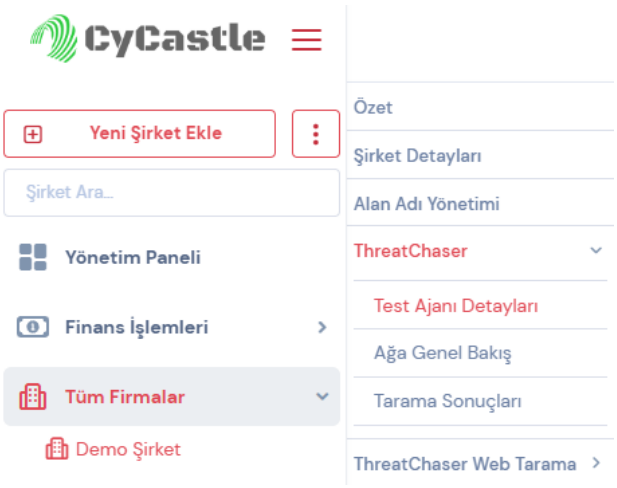
6.IP adresini tarayıcınızın arama barına girerek GUI arayüzüne ulaşabilirsiniz. Bu adımda GUI giriş bilgilerini girerek giriş yapabilirsiniz.

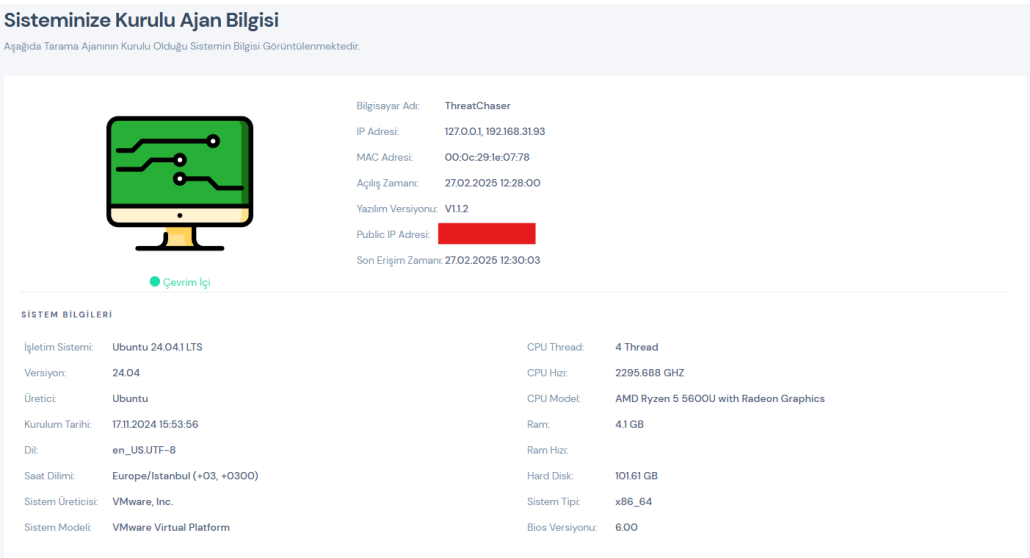


7.Giriş başarıyla gerçekleştikten sonra ürün anahtarımızı girerek lisansı aktif hale getiriyoruz.



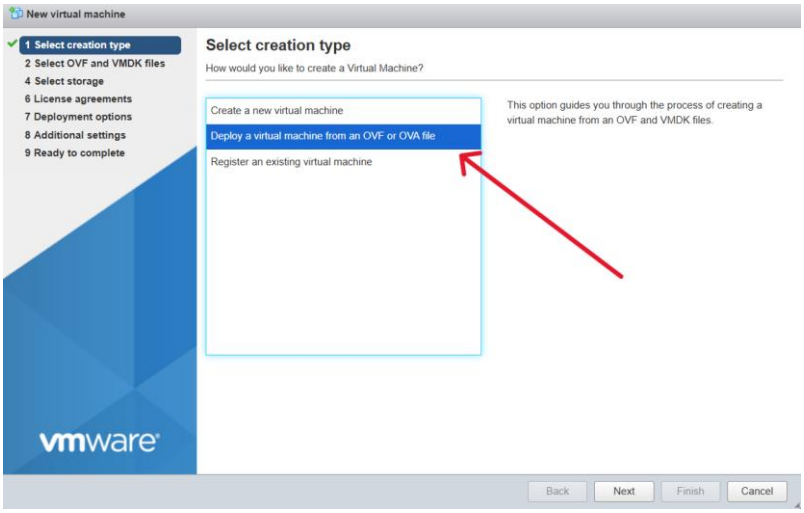
8.Yazılımı yüklediğiniz şirketin menüsünde Test Ajanı Detayları bölümüne giderek yazılımın aktif olup olmadığını kontrol edin.



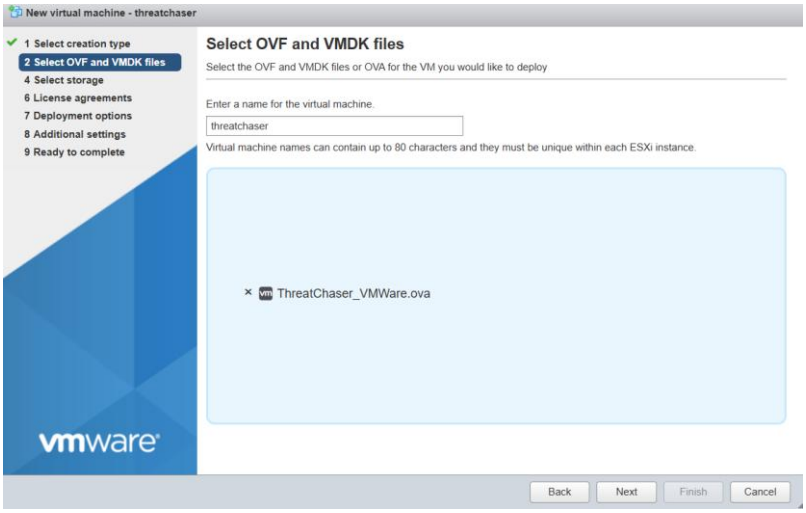


2.VMWare ESXI Kurulumu

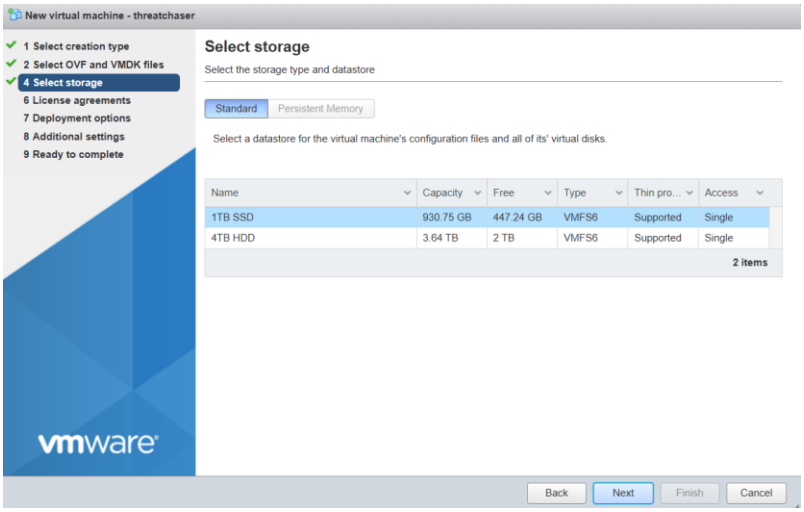
1.VMWare ESXI ekranında Virtual Machine > Create / Register VM butonuna tıkladıktan sonra aşağıdaki adımları takip ediniz.



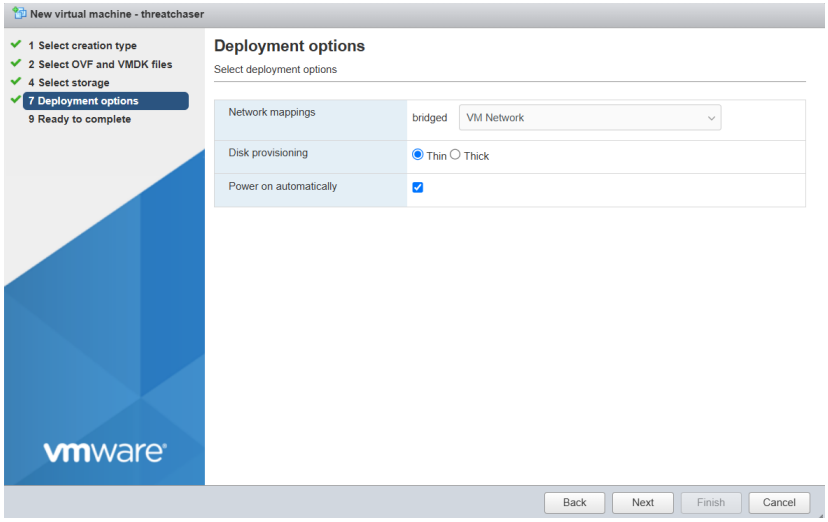
2.Gelen pencerede OVA dosyasını seçip ardından sanal makinenize bir isim veriniz



3.Kullanılacak disk alanını seçiniz.



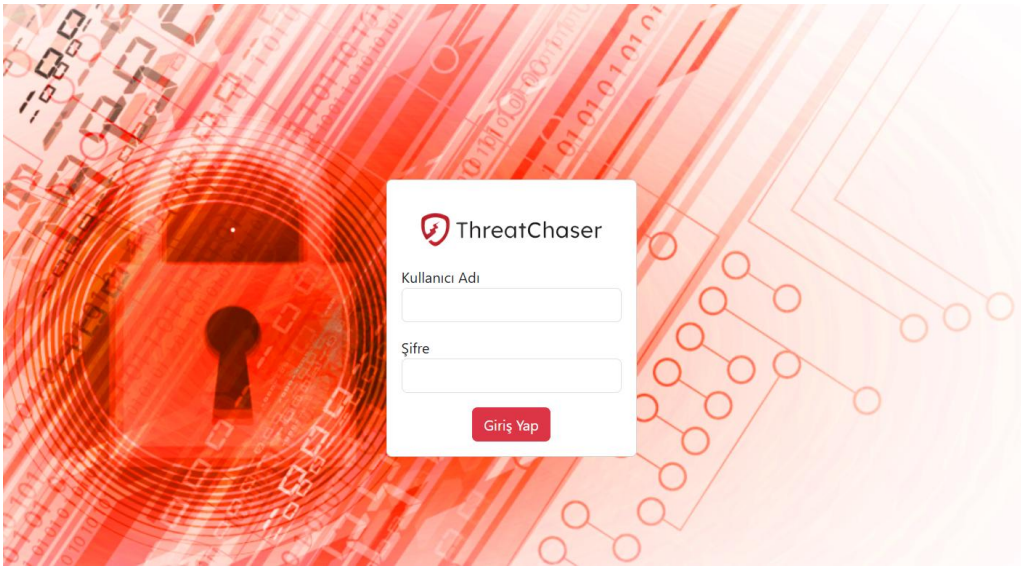
4.Dağıtım ayarımızı ayarladıktan sonra işlemi bitirerek sanal makinemizi başlatıyoruz.



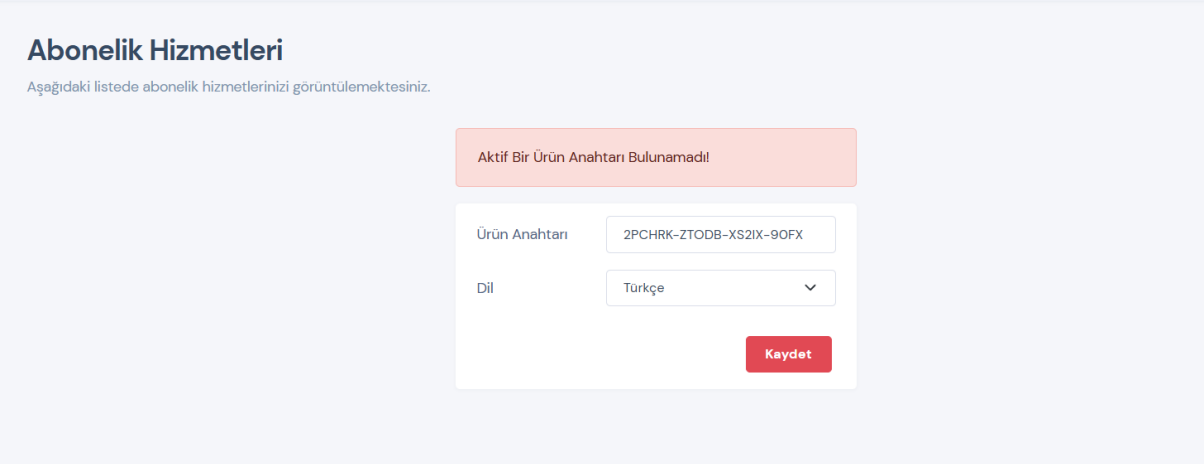
5.Açılan ekranda varsayılan değerler gözükecektir fakat dilerseniz değiştirmek için "**Enter**" tuşuna basabilirsiniz ve daha sonra Konsol Arayüzü Giriş bilgilerini girerek istediğiniz değerleri atayabilirsiniz (Eğer DHCP servisi tarafından ip sabitlemesi yapacaksanız bu adımı atlayın.)

- wizard / threatchaser giriş bilgileri ile giriş yapın
- Network Konfigürasyonu için "1" değerini giriniz.
- Statik IP için "2" değerini giriniz ve gerekli ip bilgilerini girerek ip sabitleme işlemi tamamlayınız.

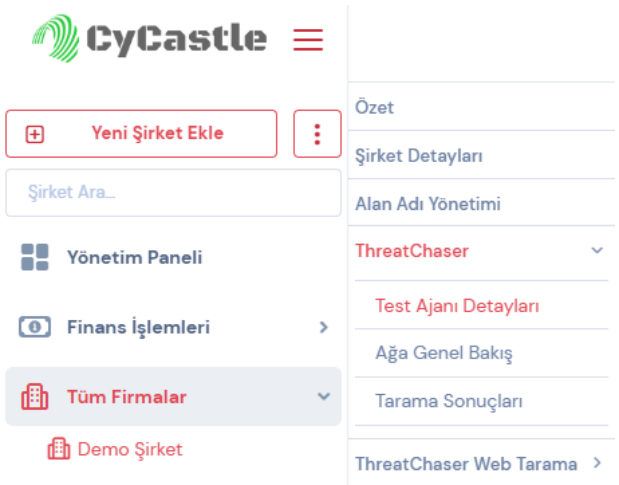
6.IP adresini tarayıcınızın arama barına girerek GUI arayüzüne ulaşabilirsiniz. Bu adımda GUI giriş bilgilerini girerek giriş yapabilirsiniz.



7.Giriş başarıyla gerçekleştikten sonra ürün anahtarımızı girerek lisansı aktif hale getiriyoruz.



8.Yazılımı yüklediğiniz şirketin menüsünde “**Test Ajanı Detayları**” bölümüne giderek yazılımın aktif olup olmadığını kontrol edin.



Sisteminize Kurulu Ajan Bilgisi

Aşağıda Tarama Ajanının Kurulu Olduğu Sistemin Bilgisi Görüntülenmektedir.

Çevrim İçi

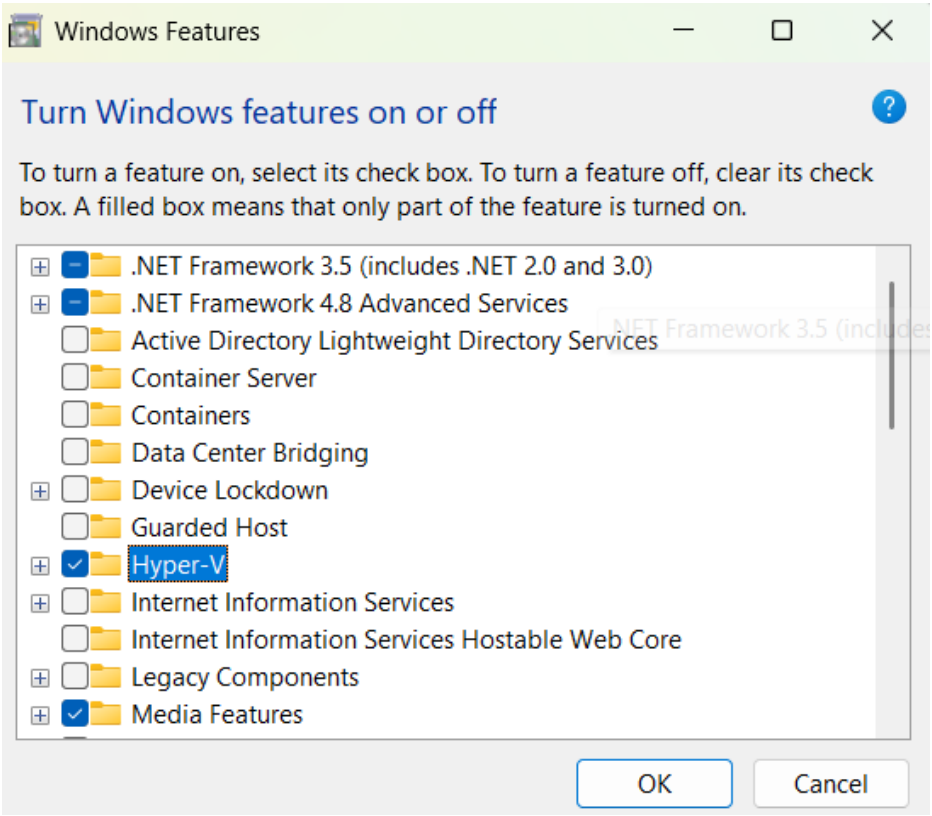
Bilgisayar Adı:	ThreatChaser
IP Adresi:	127.0.0.1, 192.168.31.93
MAC Adresi:	
Açılış Zamanı:	27.02.2025 12:28:00
Yazılım Versiyonu:	V1.1.2
Public IP Adresi:	
Son Erişim Zamanı:	27.02.2025 12:30:03

SİSTEM BİLGİLERİ

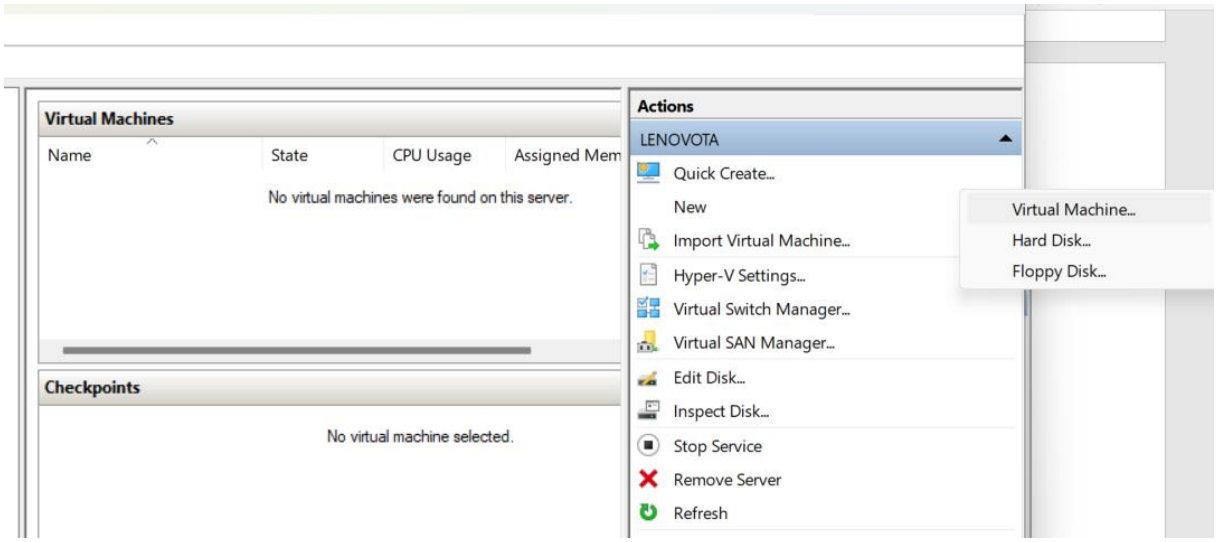
İşletim Sistemi:	Ubuntu 24.04.1 LTS	CPU Thread:	4 Thread
Versiyon:	24.04	CPU Hızı:	2295.688 GHZ
Üretici:	Ubuntu	CPU Model:	AMD Ryzen 5 5600U with Radeon Graphics
Kurulum Tarihi:	17.11.2024 15:53:56	Ram:	4.1 GB
Dil:	en_US.UTF-8	Ram Hızı:	
Saat Dilimi:	Europe/Istanbul (+03, +0300)	Hard Disk:	101.61 GB
Sistem Üreticisi:	VMware, Inc.	Sistem Tipi:	x86_64
Sistem Modeli:	VMware Virtual Platform	Bios Versiyonu:	6.00

3.Hyper-V Ajan Kurulumu

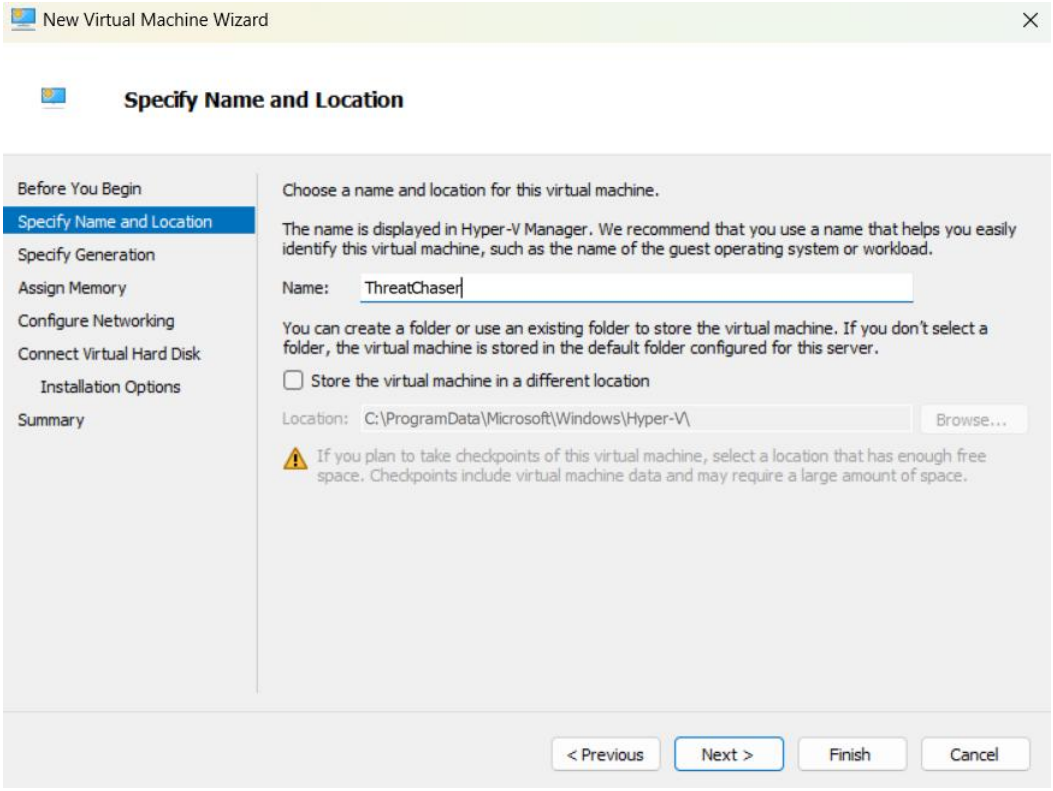
1.Denetim masasında “Programlar” kısmına gelindikten sonra “Windows Özelliklerini Aç / Kapat” kısmına tıklıyoruz. Açılan pencerede Hyper-V kutucuğuna tıklayıp OK (Tamam) butonuna tıklayabilirsiniz.



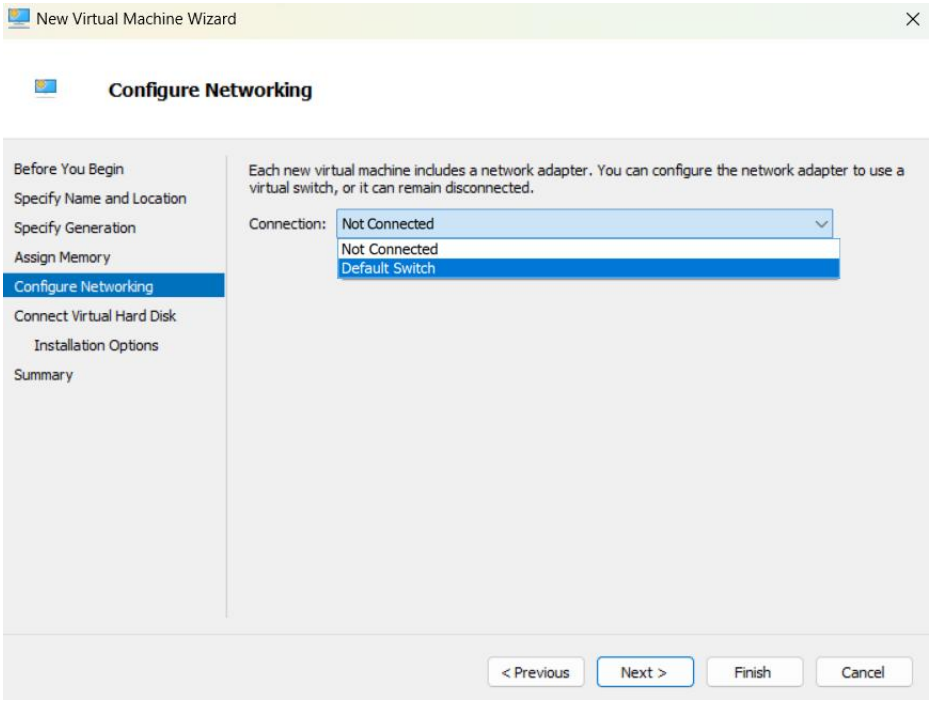
2.”New” diyerek “Virtual Machine” kısmına tıklıyoruz.



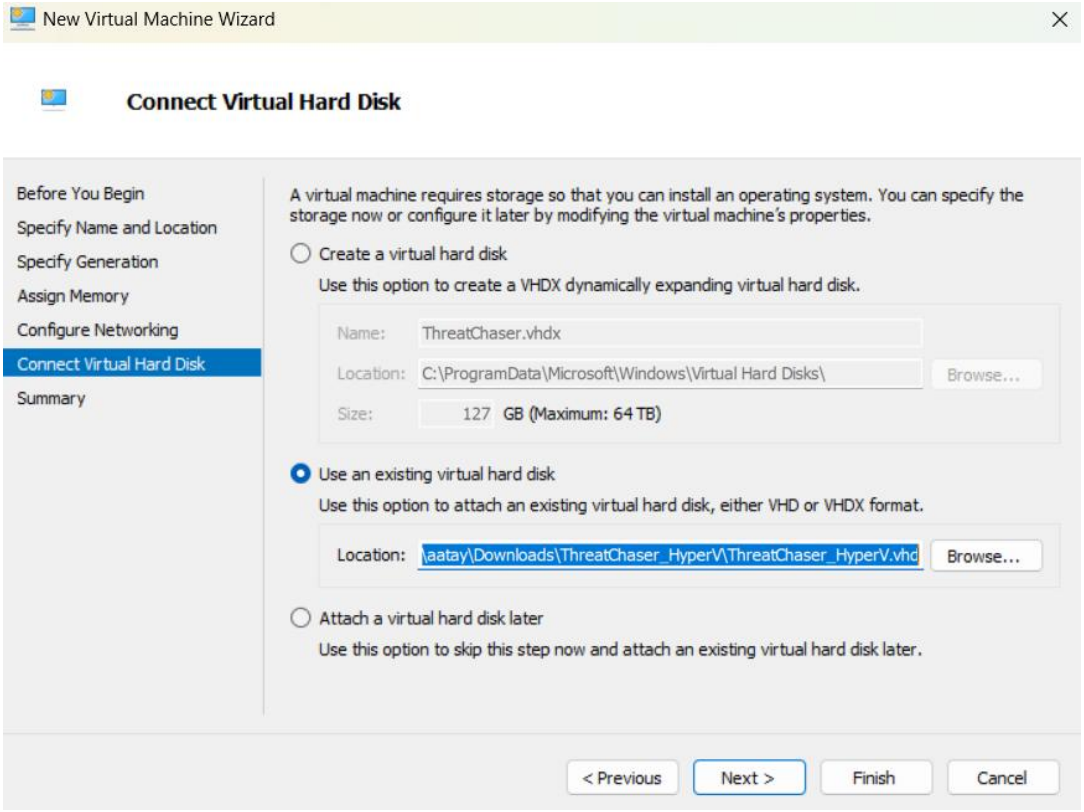
3.Açılan pencerede sanal makinemize isim veriyoruz.



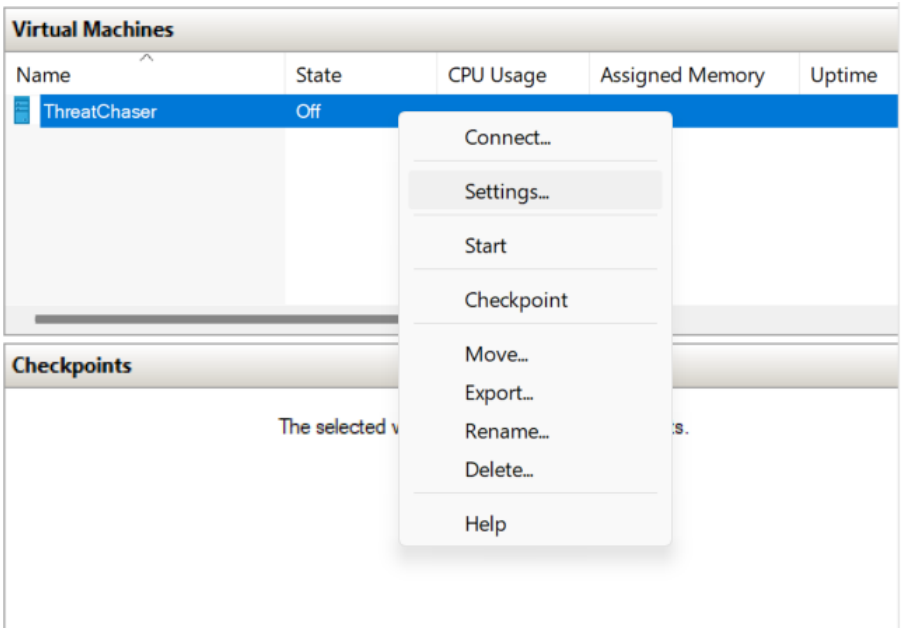
4.Ağ konfigürasyon kısmında “Default Switch” seçeneğini seçip devam ediyoruz.



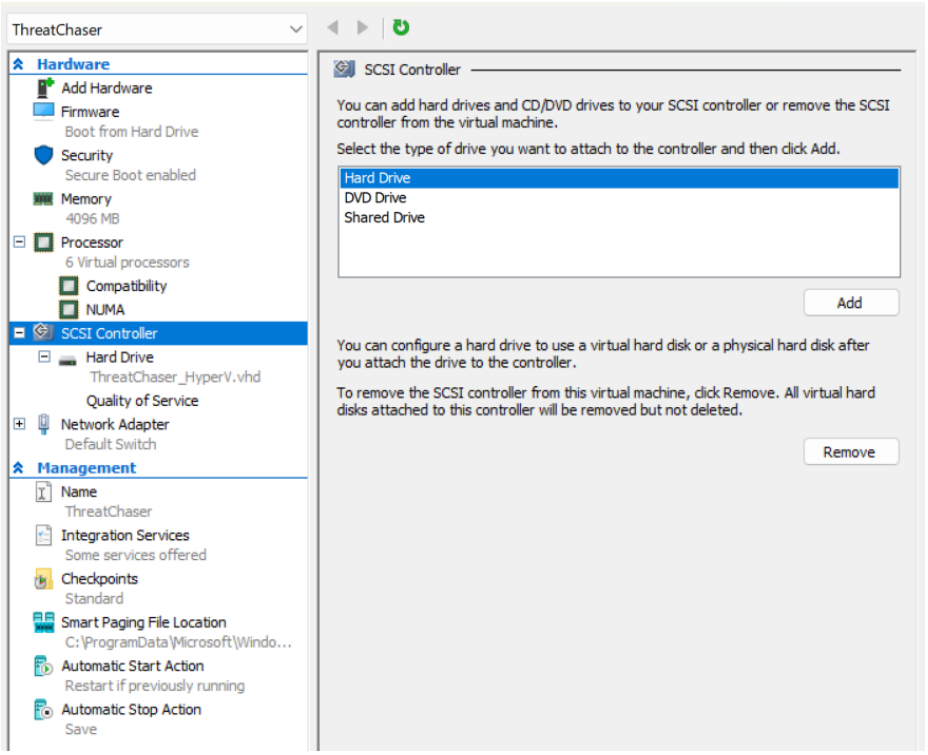
5.Öncesinde indirdiğimiz zip dosyasında çıkarttığımız “ThreatChaser_Hyper.vhd” dosya konumunu var olan sanal hard diskler kısmından ekliyoruz ve devam ediyoruz.



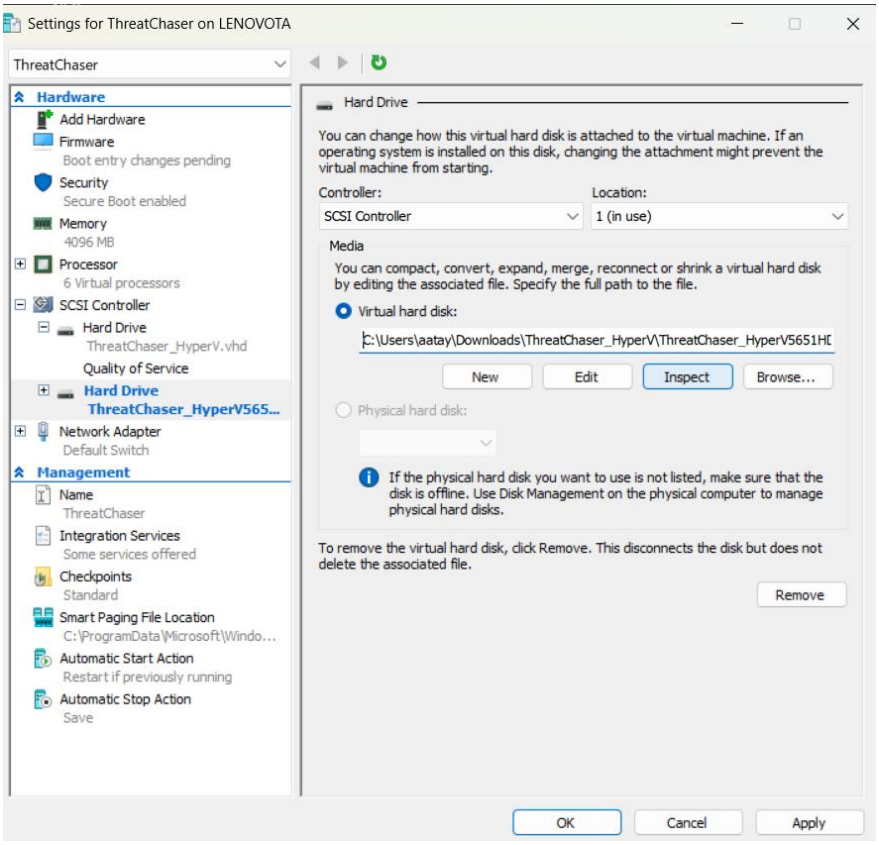
6. Oluşan sanal makinemizin üstüne gelip sağ tıklayarak açılan sekmelerde Settings (Ayarlar) kısmına tıklıyoruz.



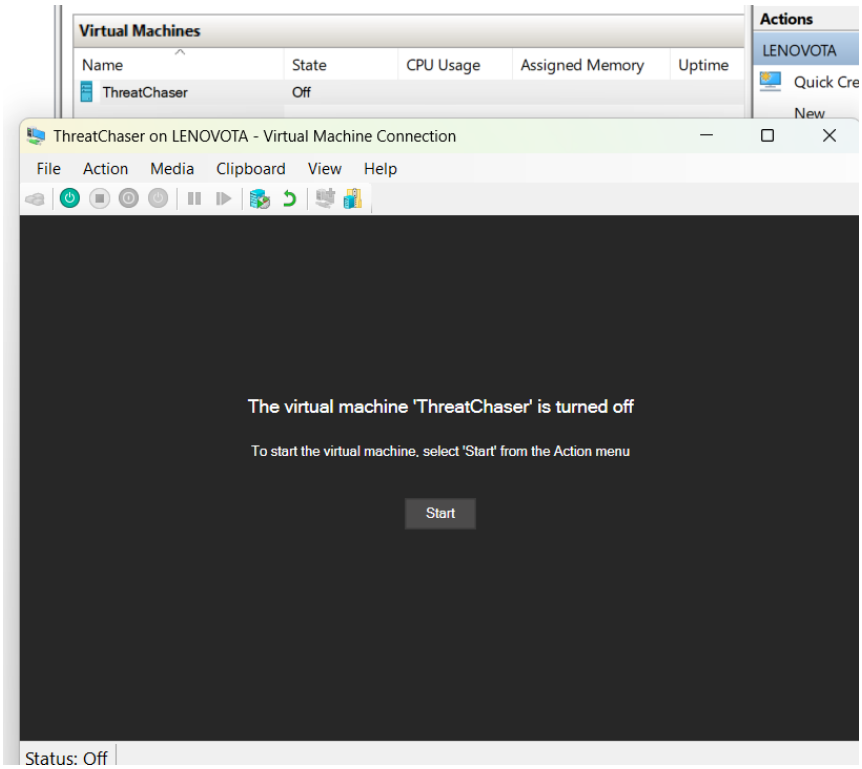
7.SCSI Controller kısmına gelip Hard Drive seçiliyken “Add” butonuna basıp ilerliyoruz.



8.Daha sonra önceden indirdiğimiz dosyamızın içindeki “ThreatChaser_HyperV5651HDD.vhd” diskimizin dosya yolunu ekliyoruz



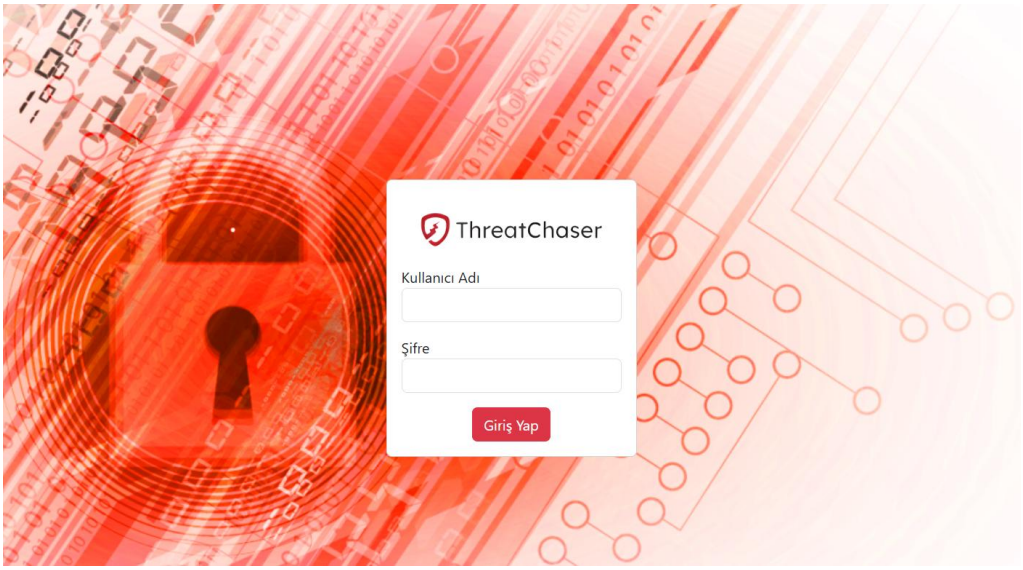
9.Diskler başarıyla eklendikten sonra makinemizin üstüne gelerek “Connect” kısmını seçiyoruz ve ardından açılan pencerede “Start” diyerek sanal makinemizi başlatıyoruz.



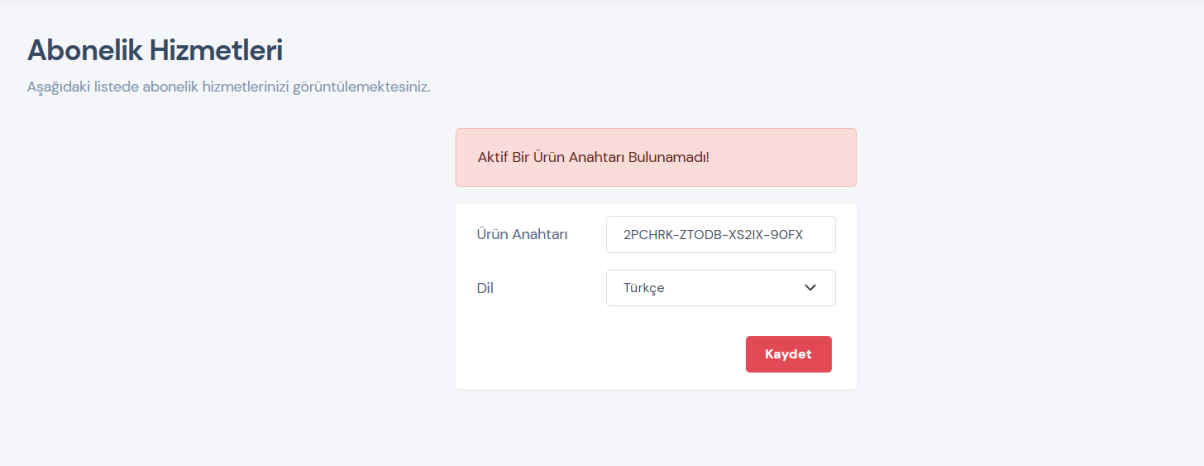
10.Açılan ekranda varsayılan değerler gözükecektir fakat dilerseniz değiştirmek için “**Enter**” tuşuna basabilirsiniz ve daha sonra Konsol Arayüzü Giriş bilgilerini girerek istediğiniz değerleri atayabilirsiniz (Eğer DHCP servisi tarafından ip sabitlemesi yapacaksanız bu adımı atlayın.)

- wizard / threatchaser giriş bilgileri ile giriş yapın
- Network Konfigürasyonu için “1” değerini giriniz.
- Statik IP için “2” değerini giriniz ve gerekli ip bilgilerini girerek ip sabitleme işlemi tamamlayınız.

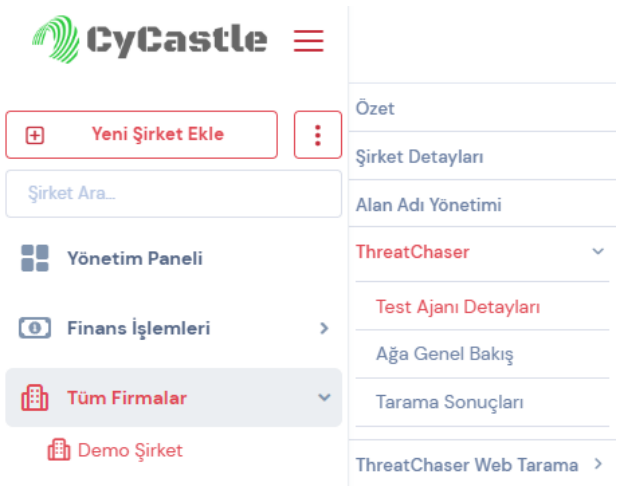
11.IP adresini tarayıcınızın arama barına girerek GUI arayüzüne ulaşabilirsiniz. Bu adımda GUI giriş bilgilerini girerek giriş yapabilirsiniz.



12.Giriş başarıyla gerçekleştikten sonra ürün anahtarımızı girerek lisansı aktif hale getiriyoruz.



13.Yazılımı yüklediğiniz şirketin menüsünde “**Test Ajanı Detayları**” bölümüne giderek yazılımın aktif olup olmadığını kontrol edin.



Sisteminize Kurulu Ajan Bilgisi

Aşağıda Tarama Ajanının Kurulu Olduğu Sistemin Bilgisi Görüntülenmektedir.

Çevrim İçi

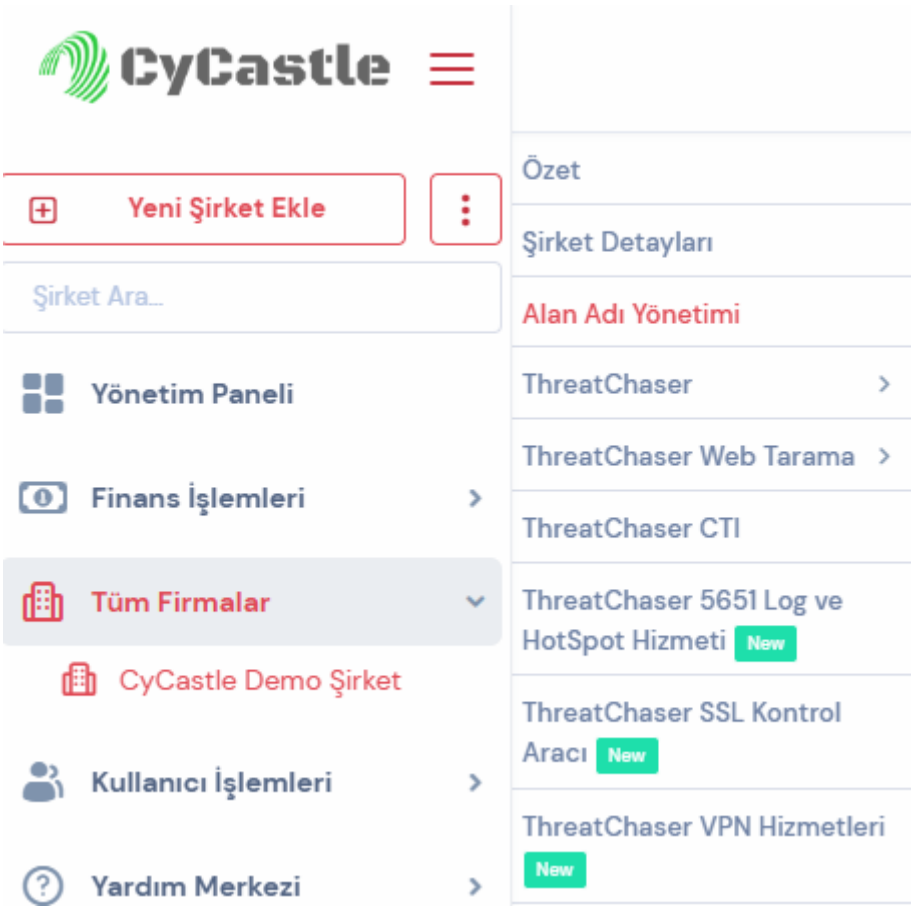
Bilgisayar Adı:	ThreatChaser
IP Adresi:	127.0.0.1, 192.168.31.93
MAC Adresi:	
Açılış Zamanı:	27.02.2025 12:28:00
Yazılım Versiyonu:	V1.1.2
Public IP Adresi:	
Son Erişim Zamanı:	27.02.2025 12:30:03

SİSTEM BİLGİLERİ

İşletim Sistemi:	Ubuntu 24.04.1 LTS	CPU Thread:	4 Thread
Versiyon:	24.04	CPU Hızı:	2295.688 GHZ
Üretici:	Ubuntu	CPU Model:	AMD Ryzen 5 5600U with Radeon Graphics
Kurulum Tarihi:	17.11.2024 15:53:56	Ram:	4.1 GB
Dil:	en_US.UTF-8	Ram Hızı:	
Saat Dilimi:	Europe/Istanbul (+03, +0300)	Hard Disk:	101.61 GB
Sistem Üreticisi:	VMware, Inc.	Sistem Tipi:	x86_64
Sistem Modeli:	VMware Virtual Platform	Bios Versiyonu:	6.00

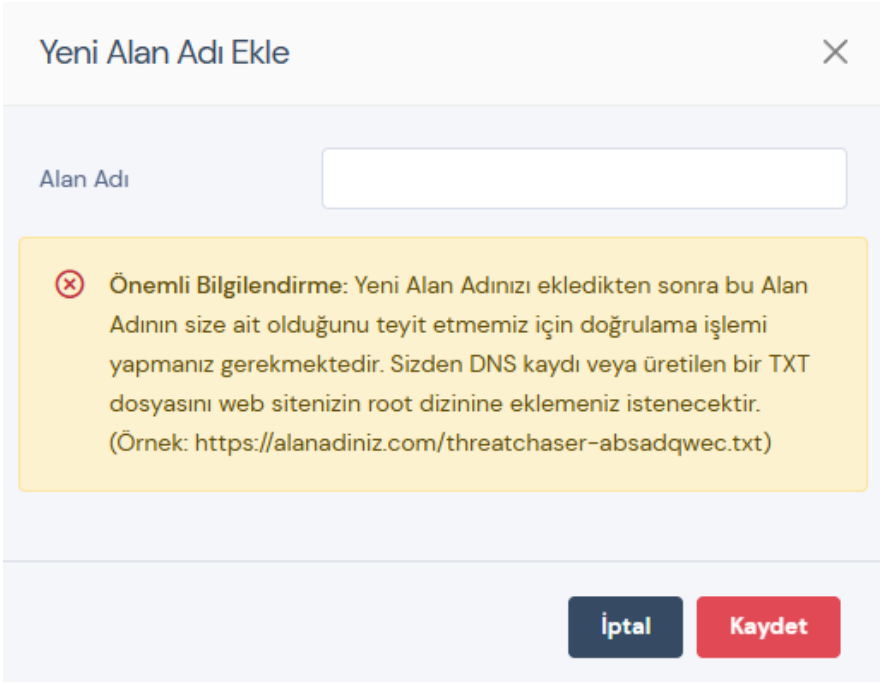
Web Taraması İçin Nasıl Alan Adı Ekleyebilirim?

Domain eklemek istediğiniz şirketin menüsünde "**Alan Adı Yönetimi**" bölümüne gidin.



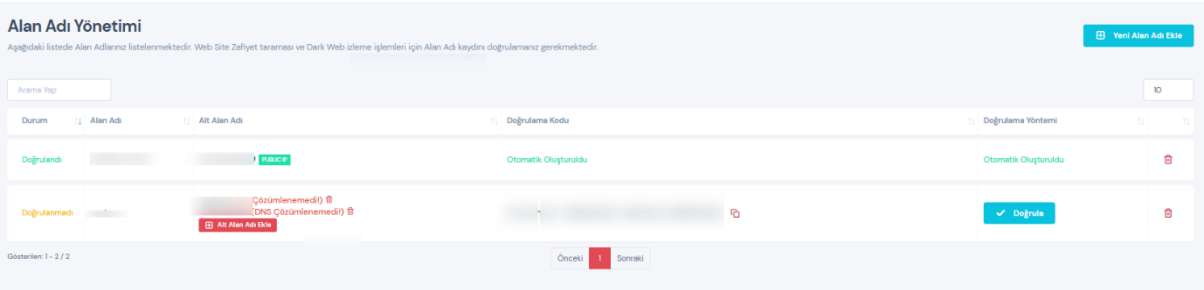
"Yeni Alan Adı Ekle" Butonuna Tıklayın

Alan adınızı yazın ve "**Kaydet**" butonuna tıklayarak işlemi tamamlayın.



Alan Adımı Nasıl Doğrulayabilirim?

Eklediğiniz alan adının yanında yer alan “**Doğrula**” butonuna tıklayarak doğrulama sürecini başlatabilirsiniz.

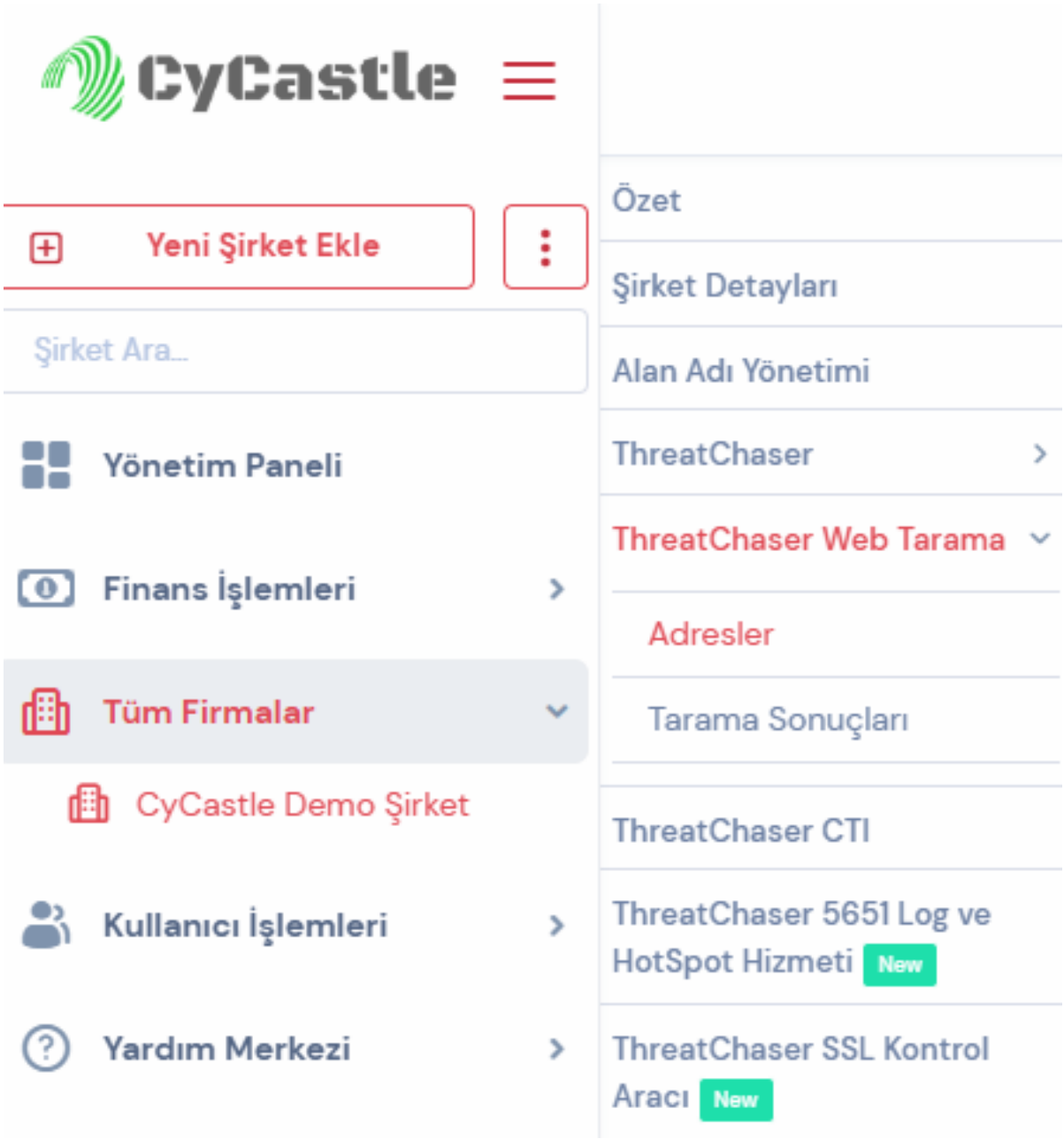


Açılan penceredeki adımları takip ederek işlemi tamamlayabilirsiniz.

Adımları uyguladıktan sonra menüdeki “**Doğrula**” butonuna tıklayarak işlemi tamamlayın.

Nasıl Web Taraması Başlatabilirim ?

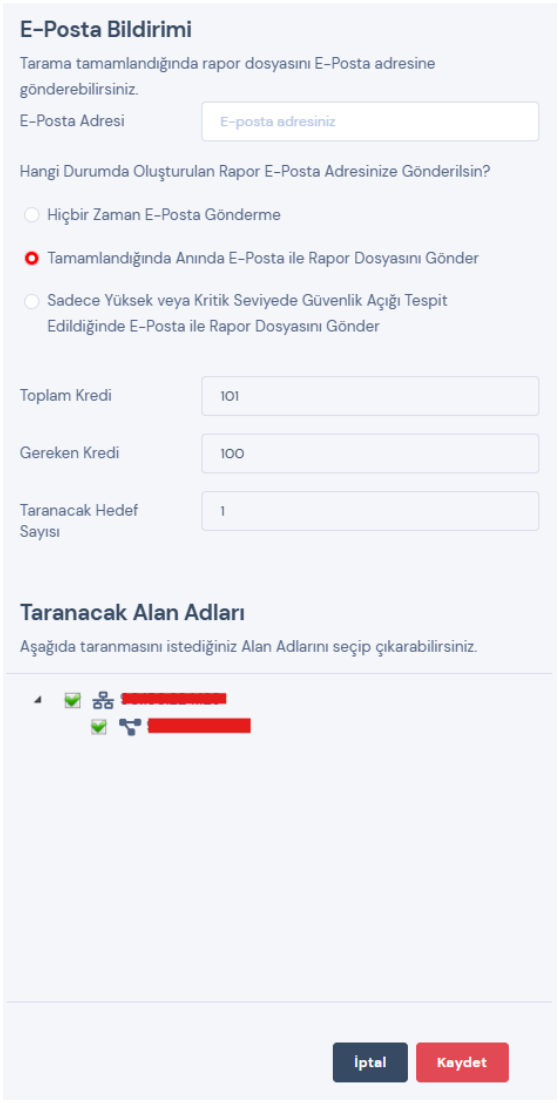
Web taraması başlatmak istediğiniz şirketin menüsünde yer alan “**Web Siteleri**” bölümüne gidiniz ve taramak istediğiniz alan adlarını seçiniz.



“Seçilen Web Sitelerini Tara” butonuna tıklayarak tarama işlemini başlatabilirsiniz.

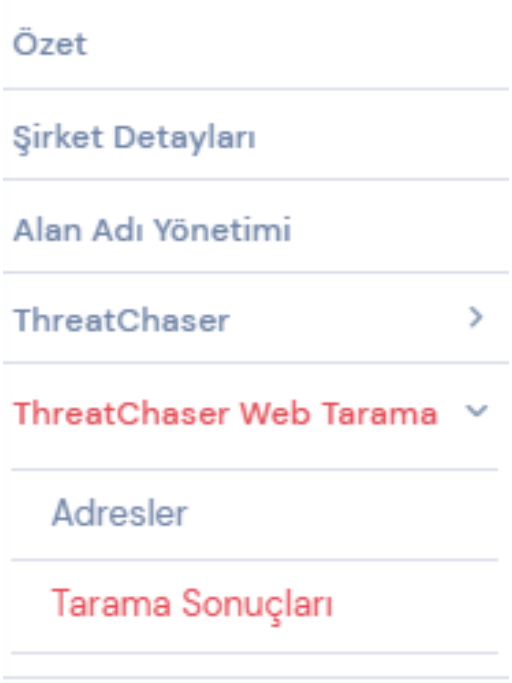
Not: Tarama hızı ve sayısı, ağ trafiğinizin yoğunluğunu etkileyebilir. Özellikle yoğun ağ trafiği olan sistemlerde, bu değerlerin çok yüksek tutulması önerilmez.

Taranacak Alan adlarını seçip “**Kaydet**” diyerek devam ediniz.

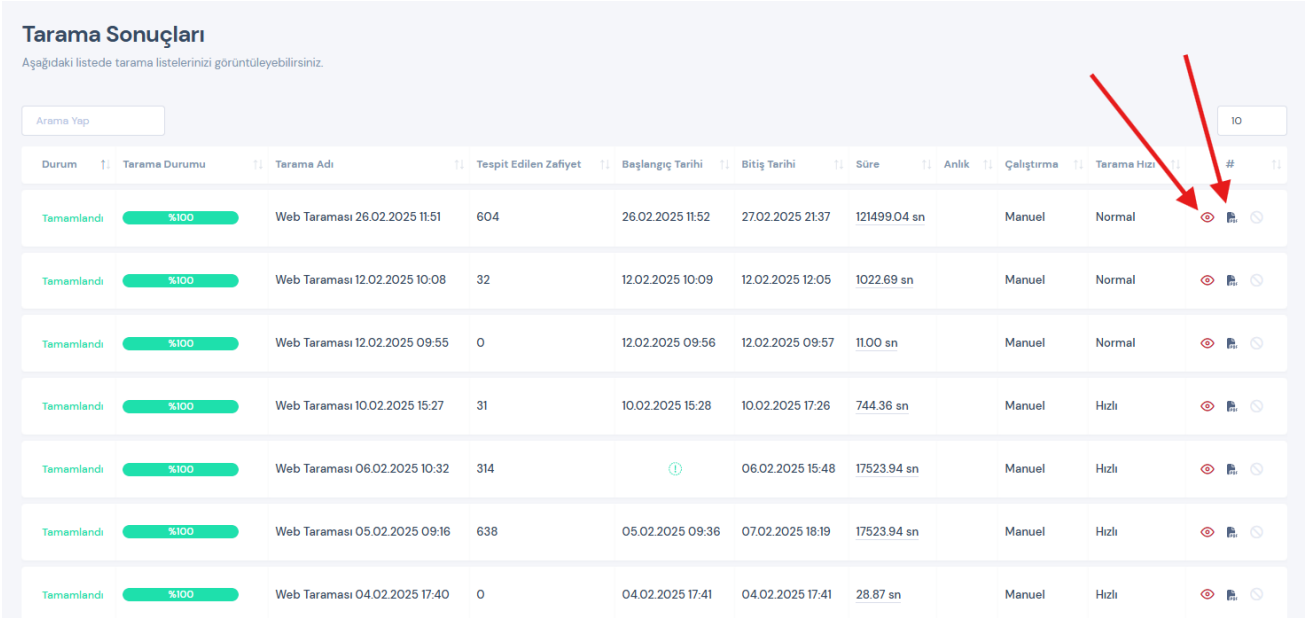


Web Tarama Sonuçlarımı Nasıl Görüntüleyebilirim?

"**ThreatChaser Web Tarama**" sekmesine tıklayıp ardından "**Tarama Sonuçları**" kısmına tıklayabilirsiniz.

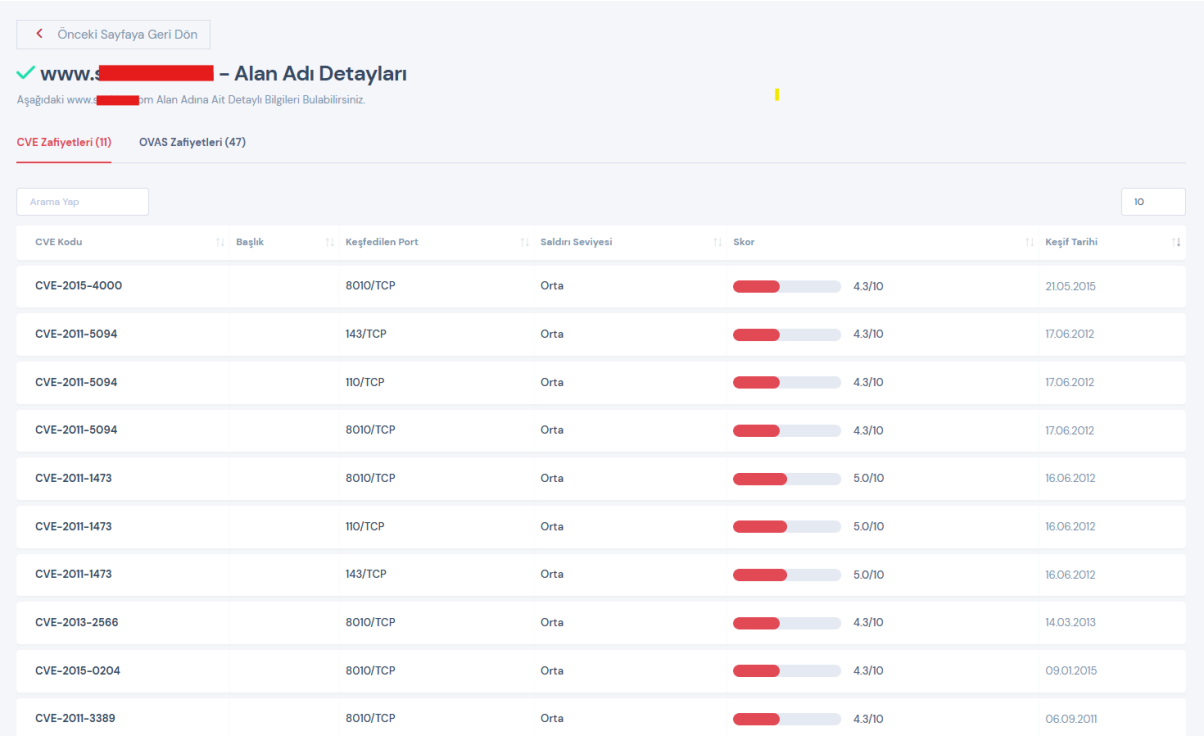


Açılan sayfada okla gösterilen butonlara tıklayarak detaylı şekilde zafiyetleri görüntüleyebilir veya sizin için hazırlanan zafiyet raporunu görüntüleyebilirsiniz.



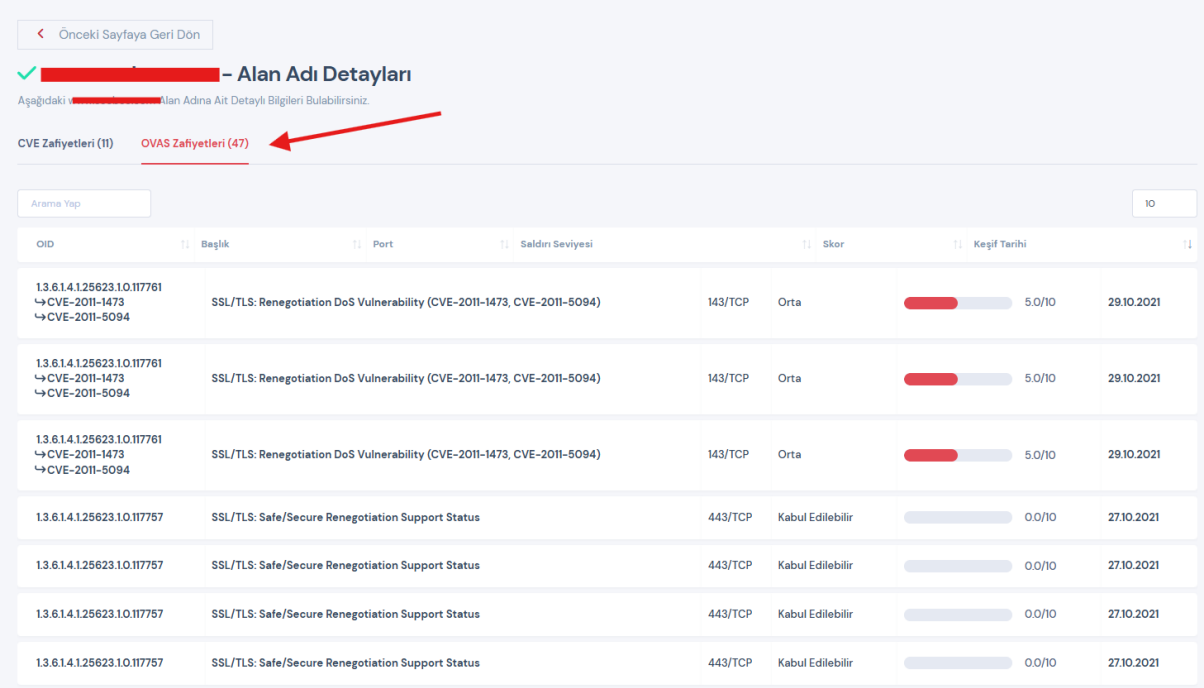
CVE Zafiyetlerini Nasıl Görüntüleyebilirim ?

Görüntüleme (Göz) ikonuna tıkladıktan sonra açılan sayfada görüntülemek istediğiniz alan adına tıkladığınızda, açılacak ekranda CVE zafiyetlerini görüntüleyebilirsiniz.



OVAS Zafiyetlerini Nasıl Görüntüleyebilirim ?

CVE kısmının hemen yanındaki OVAS Zafiyetleri kısmına tıklayarak görüntüleyebilirsiniz.

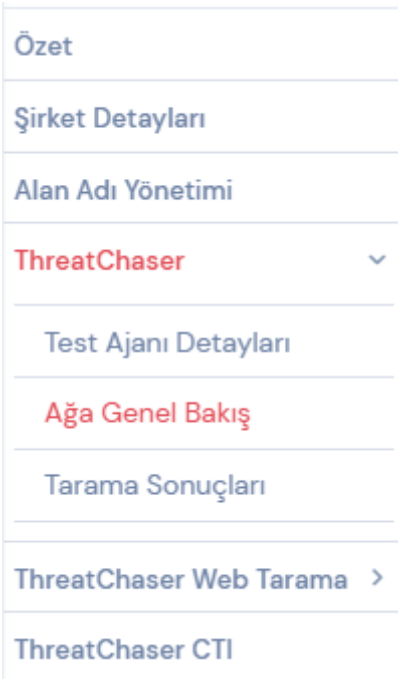


Zafiyet Raporumu Nasıl Görüntüleyebilirim?

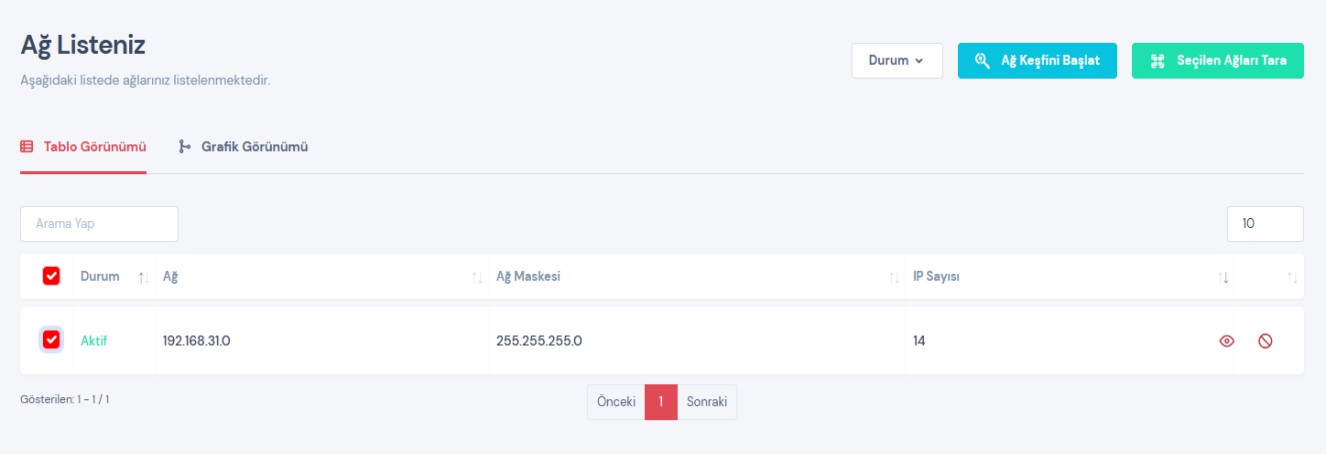
Tarama sonuçlar kısmındaki  ikonuna tıklayarak raporunuzu görüntüleyebilirsiniz.

Nasıl Ağ Taraması Başlatabilirim?

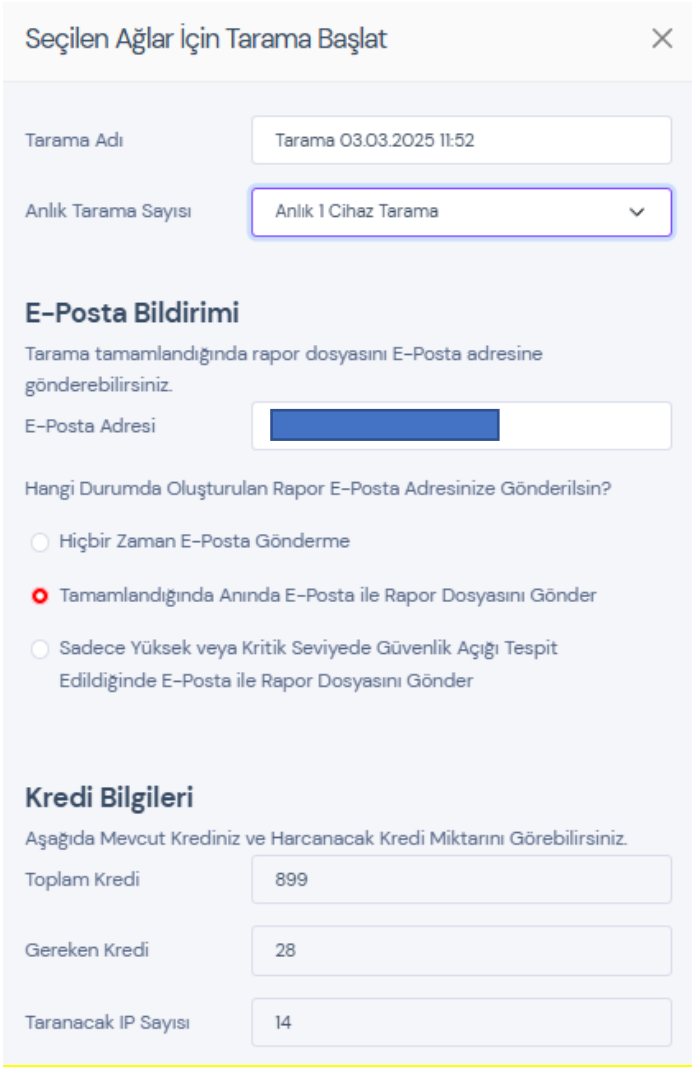
Ağ taraması başlatmak istediğiniz şirketin menüsünde “**Ağa Genel Bakış**” bölümüne giderek taramak istediğiniz ağı veya ağları seçiniz.



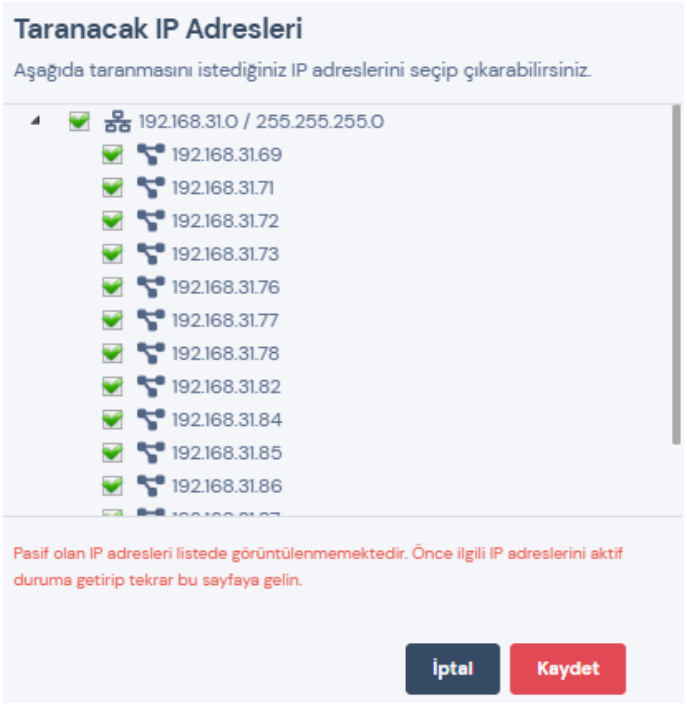
Taramak istediğiniz ağı veya ağları seçin. "**Seçilen Ağları Tara**" butonuna tıklayarak taramayı başlatın.



Tarama sayısını artırmak, ağınızdaki trafik yoğunluğunu yükseltebilir. Özellikle yoğun trafiğe sahip ağlarda bu sayıyı fazla artırmamanız önerilir.

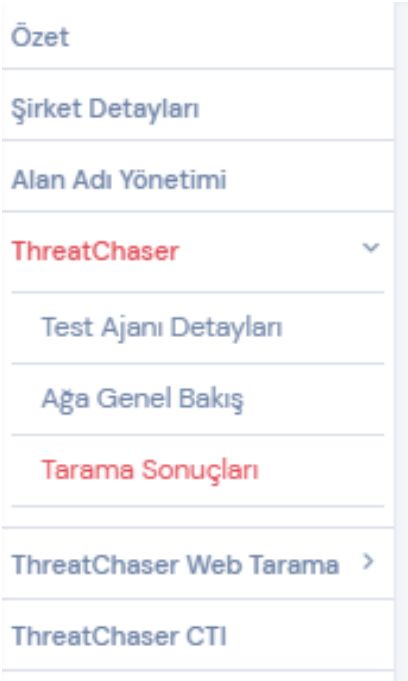


Taranacak IP Adreslerinizi Seçip “**Kaydet**” Butonuna tıklayarak devam ediniz

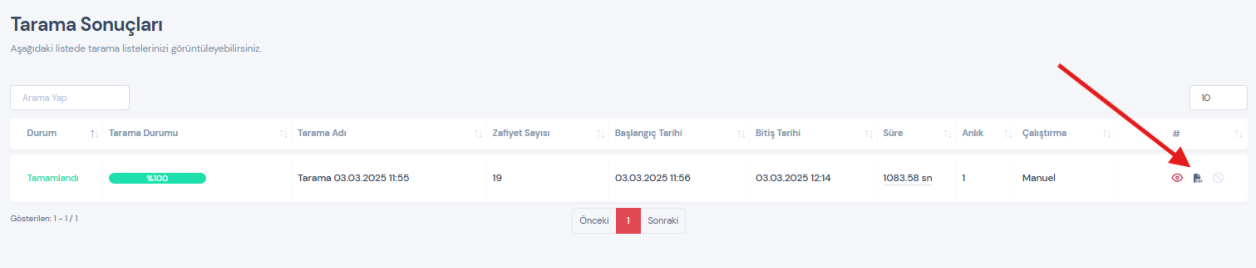


Ağ Tarama Sonuçlarını Nasıl Görüntüleyebilirim?

Ağ tarama sonuçlarını görmek istediğiniz şirketin menüsünde “**Tarama Sonuçları**” bölümüne giderek tarama sonuçlarınızı görüntüleyebilirsiniz

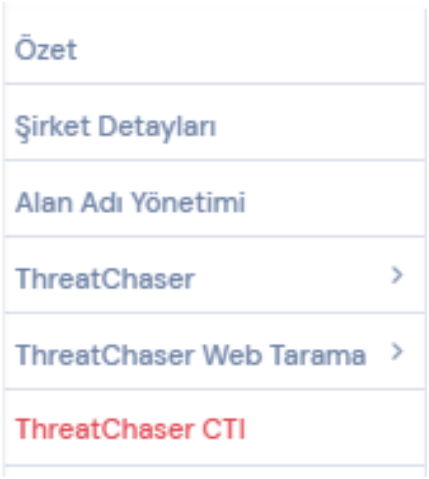


Görüntülemek istediğiniz tarama raporunun “**PDF**” butonuna tıklayarak raporu görüntüleyebilirsiniz



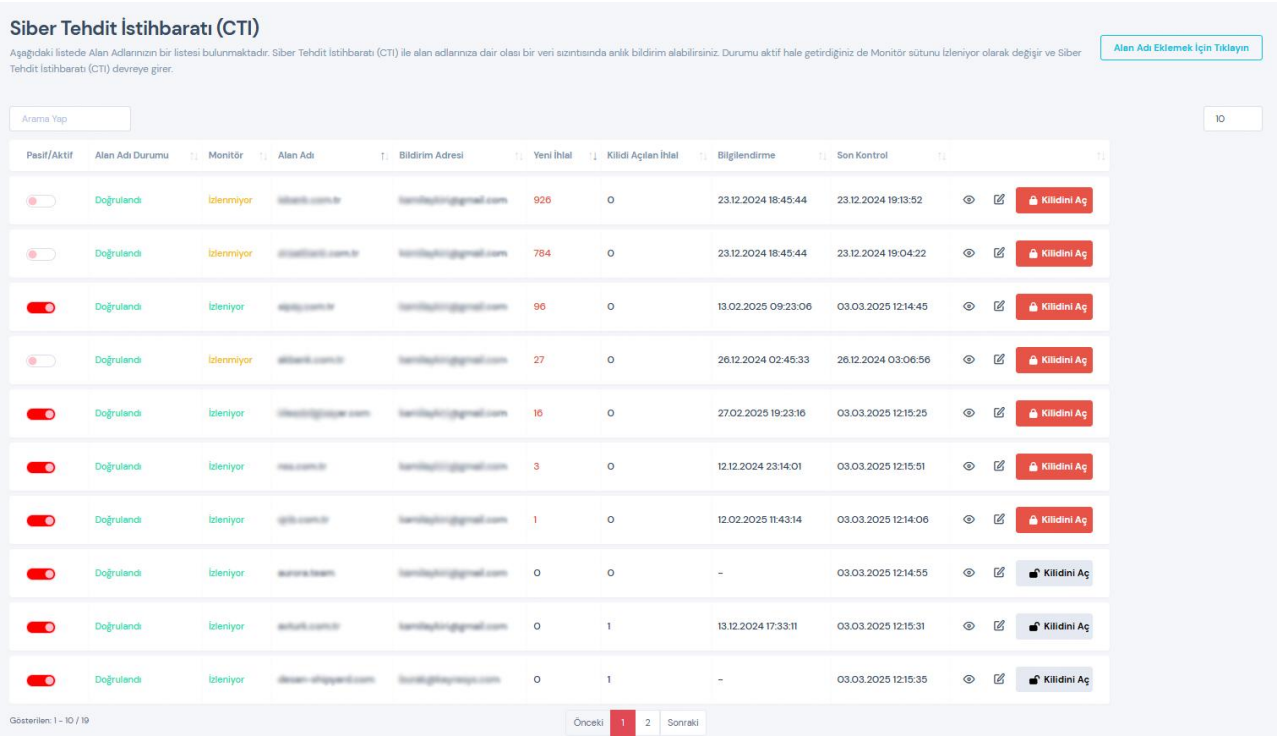
Siber Tehdit İstihbaratı (CTI) Nasıl Kullanabilirim ?

“ThreatChaser CTI“ bölümüne giderek Alan Adlarınızı veya Kişisel E-posta hesaplarınızı izleyebilirsiniz.



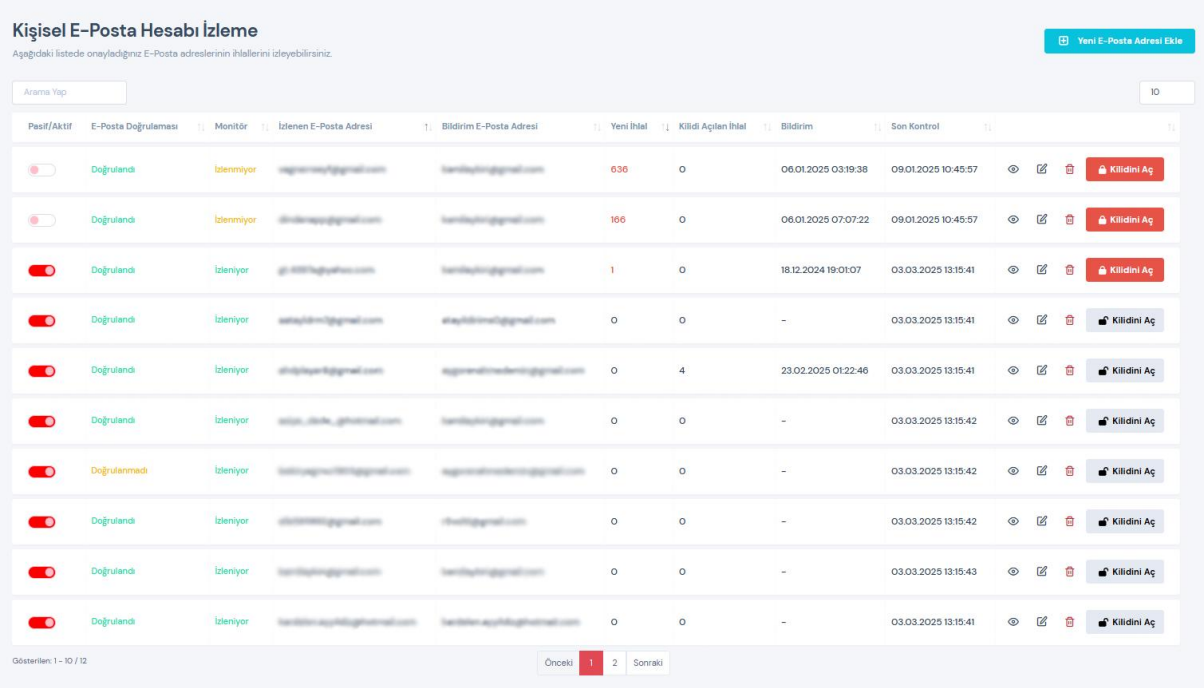
Alan Adlarımı Nasıl İzleyebilirim ?

Aşağıdaki listede Alan Adlarınızın bir listesi bulunmaktadır. **Siber Tehdit İstihbaratı (CTI)** ile alan adlarınıza dair olası bir veri sızıntısında anlık bildirim alabilirsiniz. Durumu aktif hale getirdiğiniz de Monitör sütunu İzleniyor olarak değişir ve Siber Tehdit İstihbaratı (CTI) devreye girer.



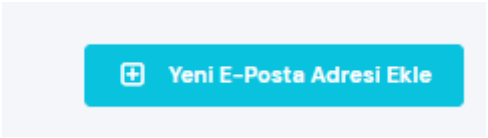
Kişisel E-posta Hesaplarımı Nasıl İzleyebilirim?

“**ThreatChaser CTI**” sayfasında sayfayı aşağıya kaydırıp listede onayladığınız E-Posta adreslerinin ihlallerini izleyebilirsiniz.

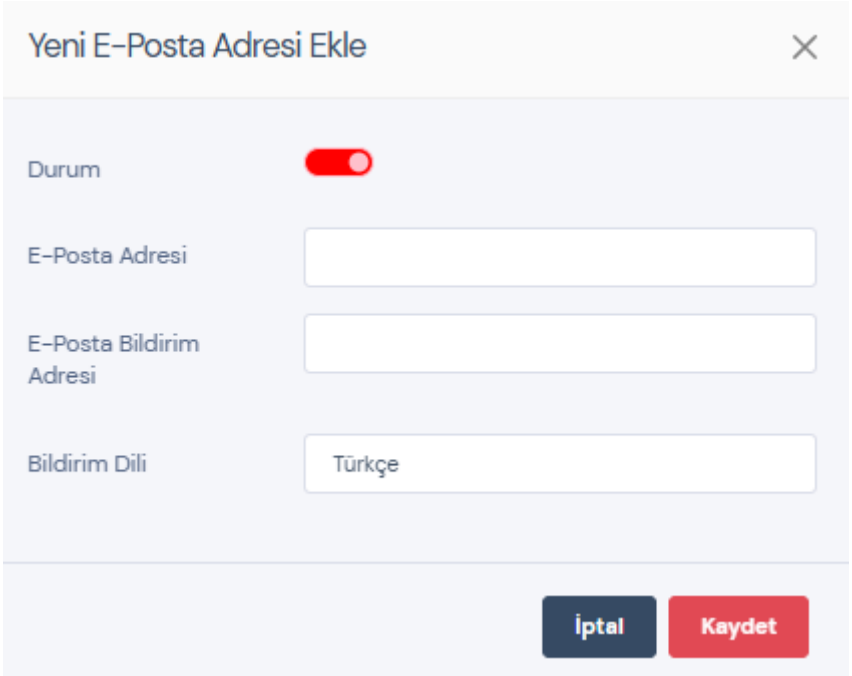


Yeni E-posta Hesabı Nasıl Ekleyebilirim ?

Kişisel e-posta hesabı izleme kısmında bulunan “**Yeni E-Posta Adresi Ekle**” butonuna tıklayın.

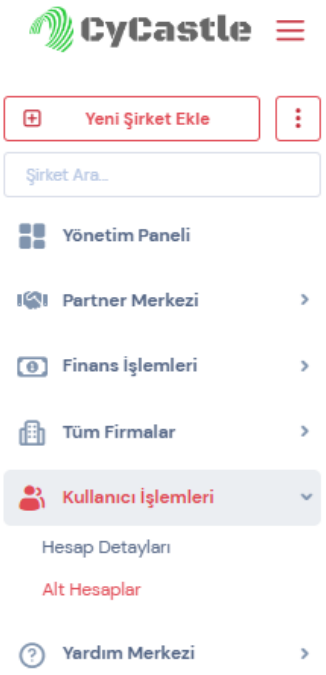


Açılan pencerede izlemek istenen kişisel e-postanızı girerek kaydet tuşuna basabilirsiniz.

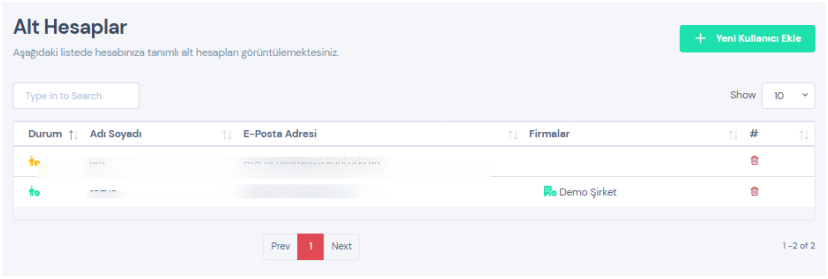


Nasıl Alt Hesap Ekleyebilirim ?

Menüden “**Kullanıcı İşlemleri**” kısmını açarak alt menülerden “**Alt Hesaplar**” kısmını seçiniz.

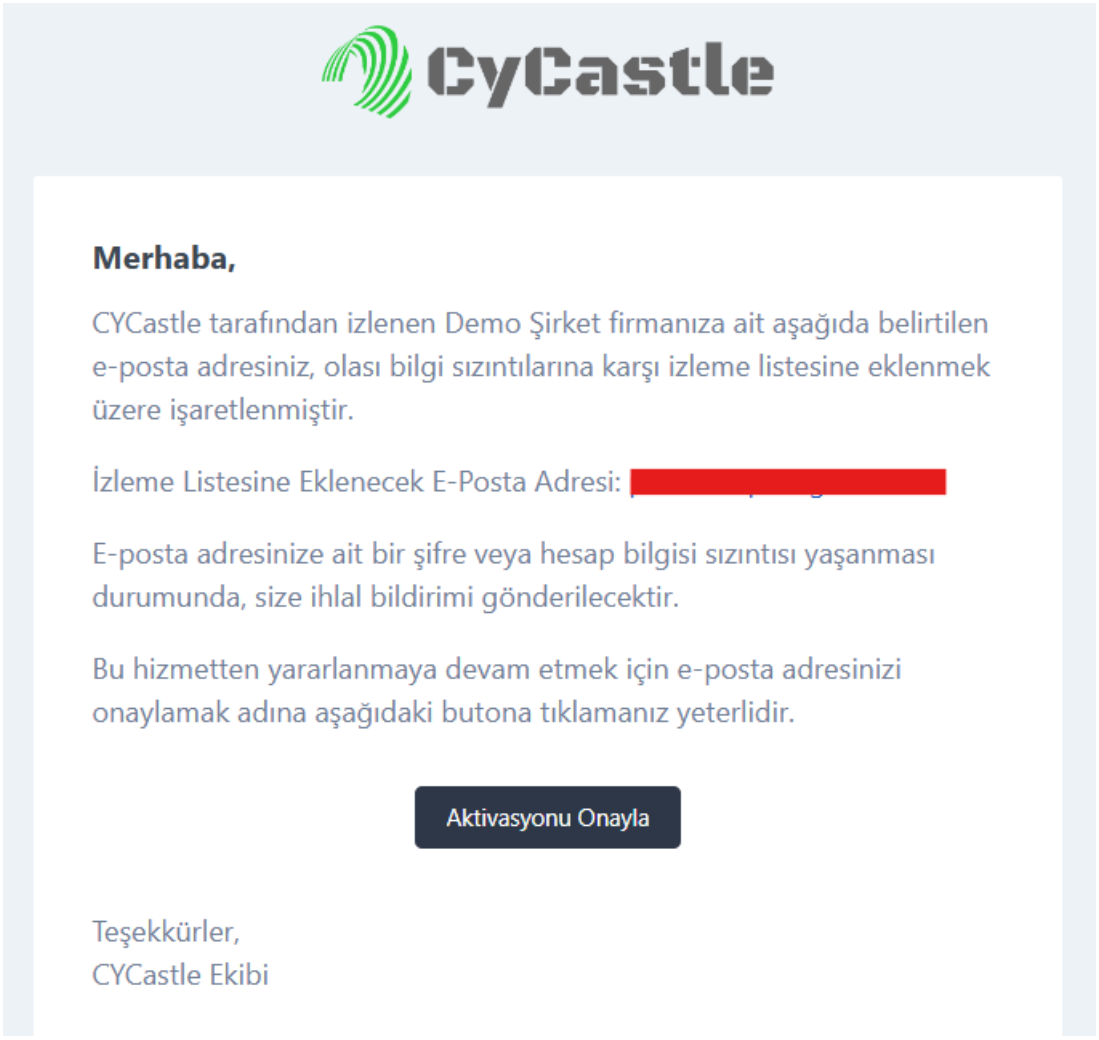


Alt Hesaplar sayfasında ekranın sağında bulunan “**Yeni Kullanıcı Ekle**” butonuna tıklayın.



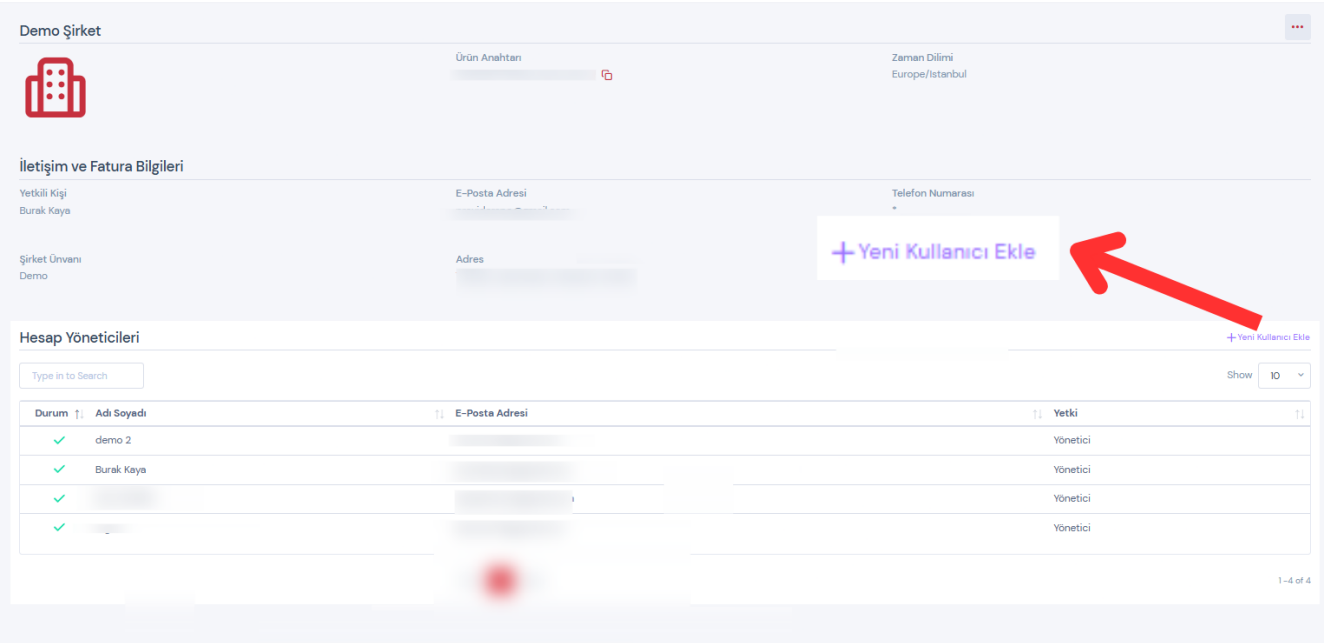
Açılan pencerede gerekli alanları doldurduktan sonra e-postanıza gelen doğrulama işlemini başarıyla gerçekleştirdiğinizde alt kullanıcı hesabınız başarıyla eklenmiş olacaktır.

Ardından mailinize gelen aktivasyonu onaylayarak işlemi tamamlayabilirsiniz.

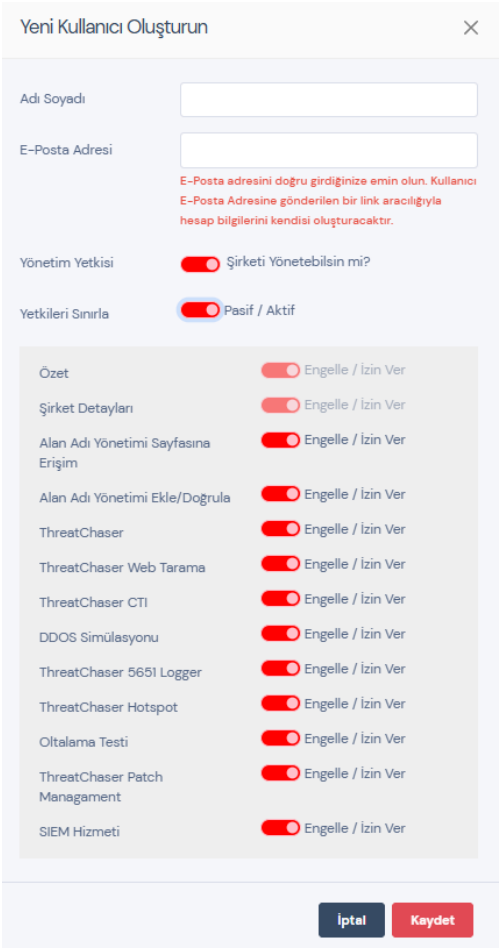


Yeni Kullanıcı Nasıl Ekleyebilirim?

Menümüzdeki “**Şirket Detayları**” kısmına tıkladıktan sonra açılan pencerede ekranın sağında bulundan “**Yeni Kullanıcı Ekle**” butonuna tıklayınız.



Sonrasında açılan pencerede kullanıcı bilgilerini girerek istenilen özellikleri aktif edebilirsiniz.



Şifremi Nasıl Değiştiririm?

1. Yol:

En kısa yoldan sayfaya ulaşmak için aşağıdaki linke tıklayın,

Parola ve Güvenlik Ayarları

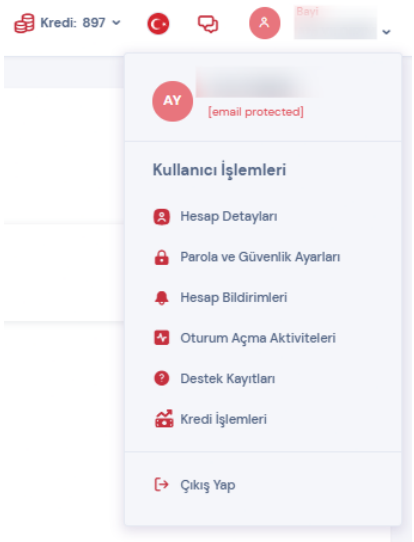
Açılan sayfada Şifre Değiştir butonuna tıklayın.

Karşınıza açılır pencere çıkacak, bu form alanında şu anki şifrenizi, yeni şifrenizi, doğrulamak için tekrar yeni şifrenizi girmeniz gerekmektedir. Tüm alanları eksiksiz doldurmanız durumunda şifrenizi başarılı bir şekilde güncelleyebilirsiniz.

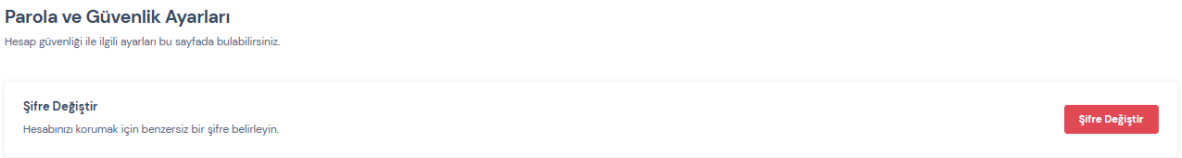
2. Yol:

Sitenin en üstünde bulunan Header Toolbar alanında "**Profil**" alanına tıklayın,

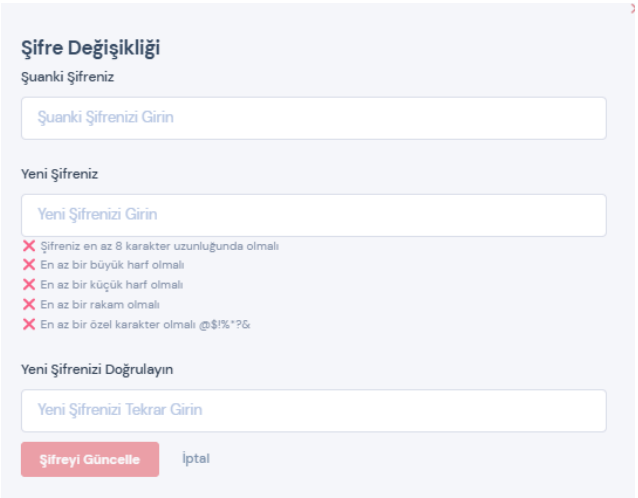
Aşağıya doğru açılan menüde "**Parola ve Güvenlik Ayarları**" linkine tıklayın.



Açılan sayfada "**Şifre Değiştir**" butonuna tıklayın.



Karşınıza açılır pencere çıkacak, bu form alanında şu an ki şifrenizi, yeni şifrenizi, doğrulamak için tekrar yeni şifrenizi girmeniz gerekmektedir.

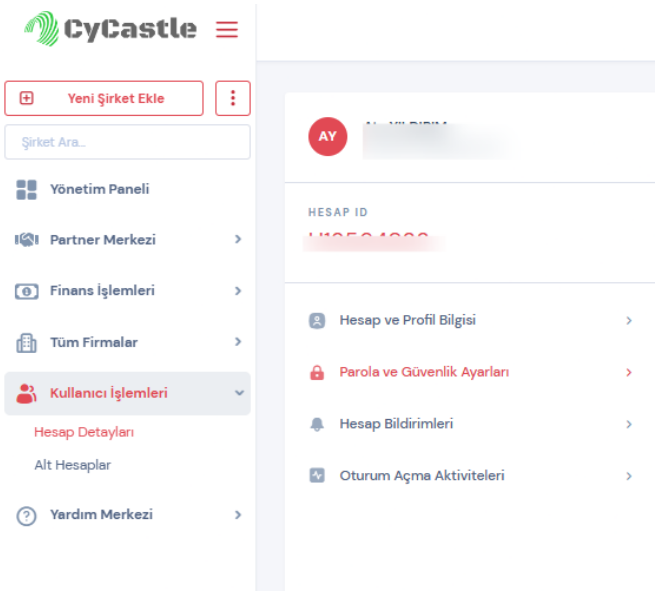


Tüm alanları eksiksiz doldurmanız durumunda şifrenizi başarılı bir şekilde güncelleyebilirsiniz.

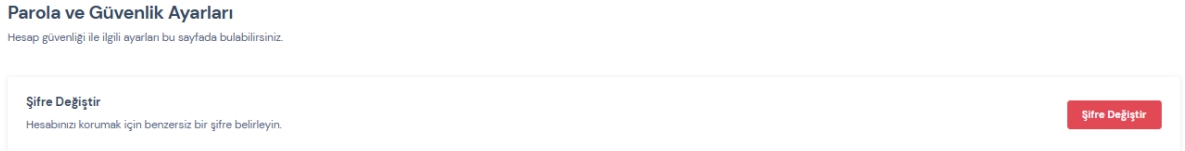
3. Yol:

Şifrenizi değiştirmek için sol taraftaki menüde “**Kullanıcı İşlemleri > Hesap Detayları**” linkine tıklayın.

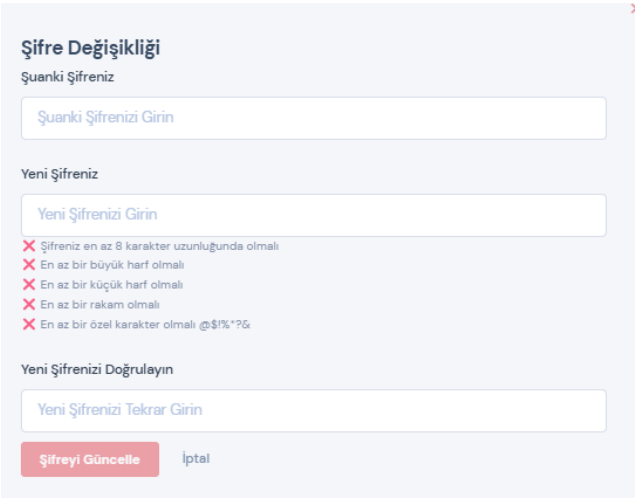
Açılan sayfada alt menü de “**Parola ve Güvenlik Ayarları**” linkine tıklayın.



Açılan sayfada “**Şifre Değiştir**” butonuna tıklayın.



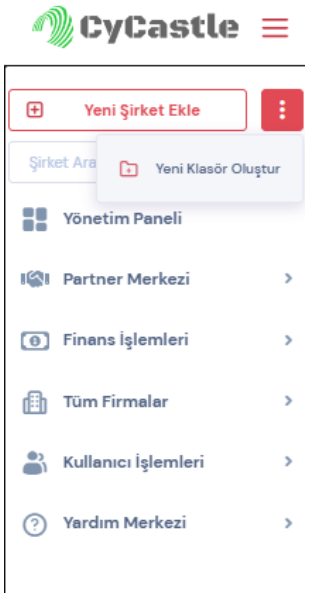
Karşınıza açılır pencere çıkacak, bu form alanında şu an ki şifrenizi, yeni şifrenizi, doğrulamak için tekrar yeni şifrenizi girmeniz gerekmektedir.



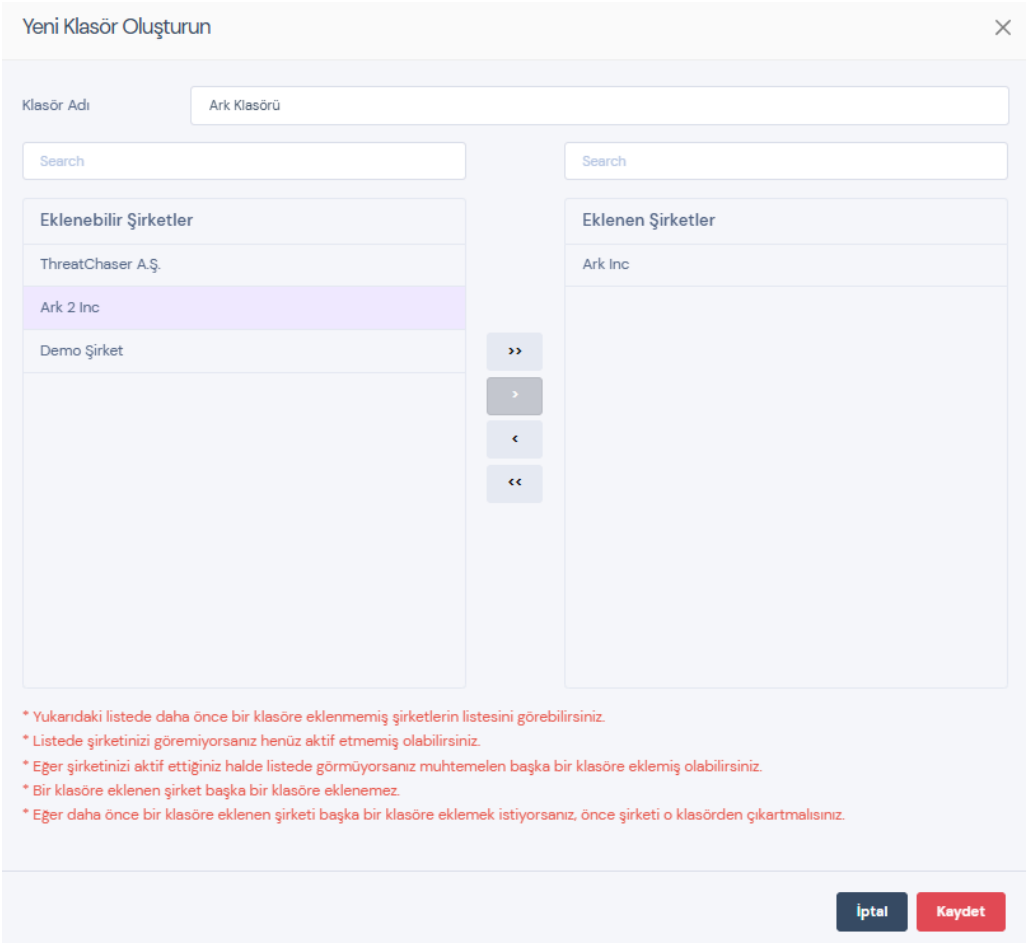
Tüm alanları eksiksiz doldurmanız durumunda şifrenizi başarılı bir şekilde güncelleyebilirsiniz.

Yeni Klasör Nasıl Oluştururum ve İçerisine Nasıl Şirket Ekleyebilirim?

Sol tarafta bulunan menü üzerindeki üç noktaya tıkladıktan sonra açılan "**Yeni Klasör Oluştur**" kısmına tıklıyoruz.



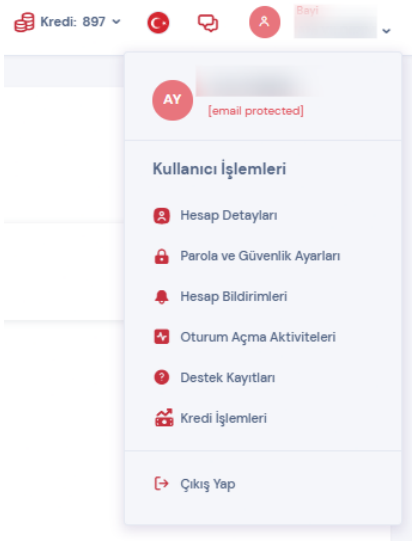
Açılan pencerede klasör adı belirttikten sonra eklemek istediğiniz şirketleri seçerek ortadaki butonlarla ekleyip çıkartabilirsiniz. Dilerseniz eklemek istediğiniz şirketi sürükleyip eklenen şirketler kısmına bırakabilirsiniz.



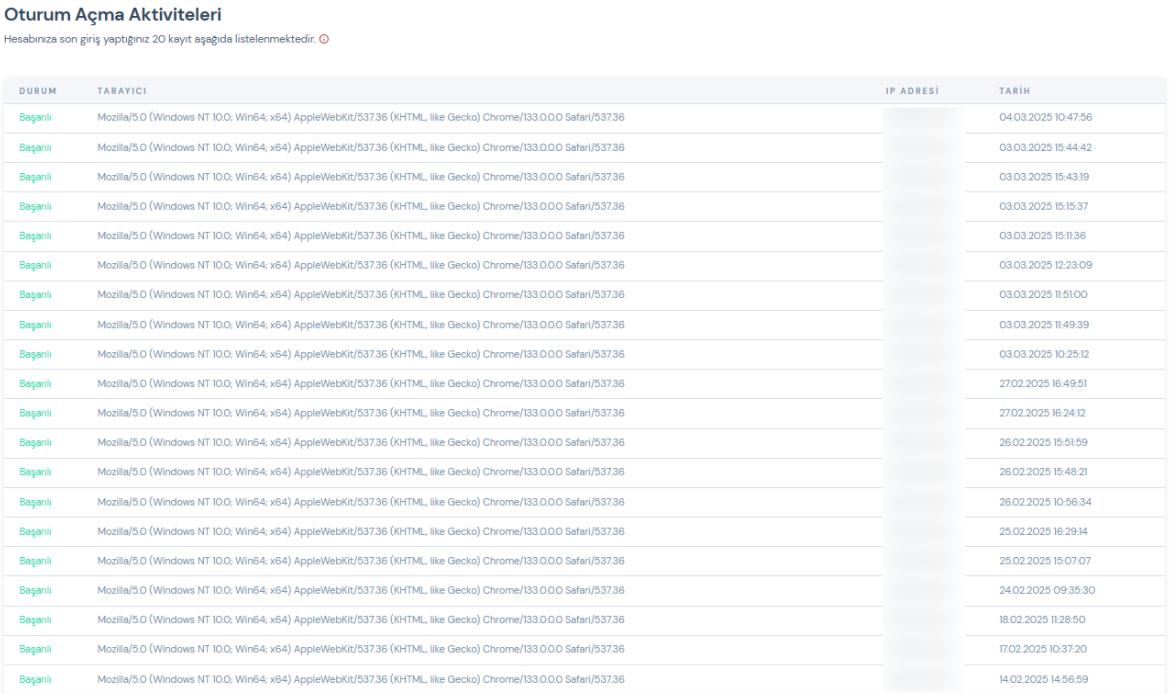
Oturum Açma Aktivitelerimi Nasıl Görebilirim ?

Sitenin en üstünde bulunan Header Toolbar alanında “**Profil**” linkine tıklayın,

Aşağıya doğru açılan menüde “**Oturum Açma Aktiviteleri**” linkine tıklayın.



Açılan pencerede hesabınızla yapılmış oturum açma girişimlerini görüntüleyebilirsiniz.



Oturum Açma Aktiviteleri

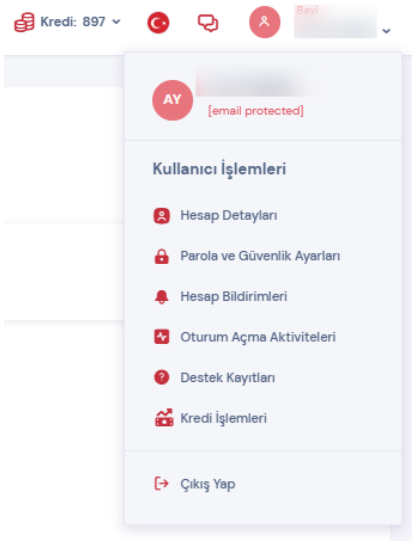
Hesabınıza son giriş yaptığınız 20 kayıt aşağıda listelenmektedir.

DURUM	TARAYICI	IP ADRESİ	TARİH
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		04.03.2025 10:47:56
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		03.03.2025 15:44:42
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		03.03.2025 15:43:19
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		03.03.2025 15:15:37
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		03.03.2025 15:11:36
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		03.03.2025 12:23:09
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		03.03.2025 11:51:00
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		03.03.2025 11:49:39
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		03.03.2025 10:25:12
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		27.02.2025 16:49:51
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		27.02.2025 16:24:12
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		26.02.2025 15:51:59
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		26.02.2025 15:48:21
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		26.02.2025 10:56:34
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		25.02.2025 16:29:14
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		25.02.2025 15:07:07
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		24.02.2025 09:35:30
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		18.02.2025 11:28:50
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		17.02.2025 10:37:20
Başarılı	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		14.02.2025 14:56:59

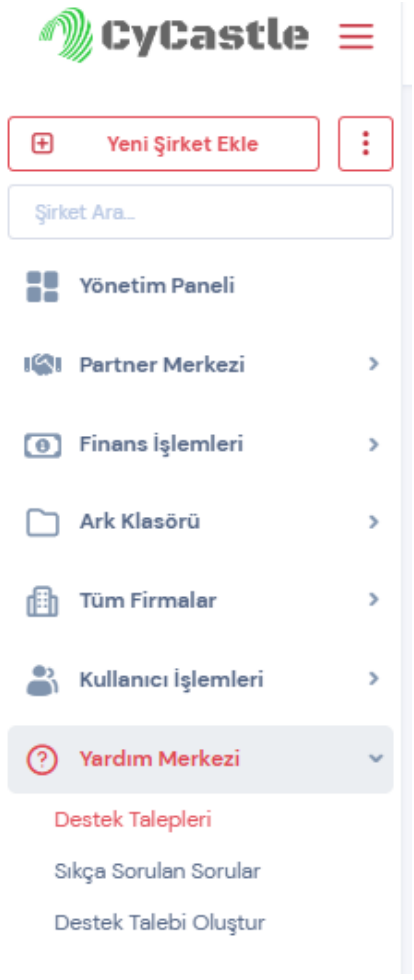
Destek Kaydı Nasıl Oluşturabilirim ?

Sitenin en üstünde bulunan Header Toolbar alanında “**Profil**” linkine tıklayın,

Aşağıya doğru açılan menüde “**Destek kayıtları**” linkine tıklayın.

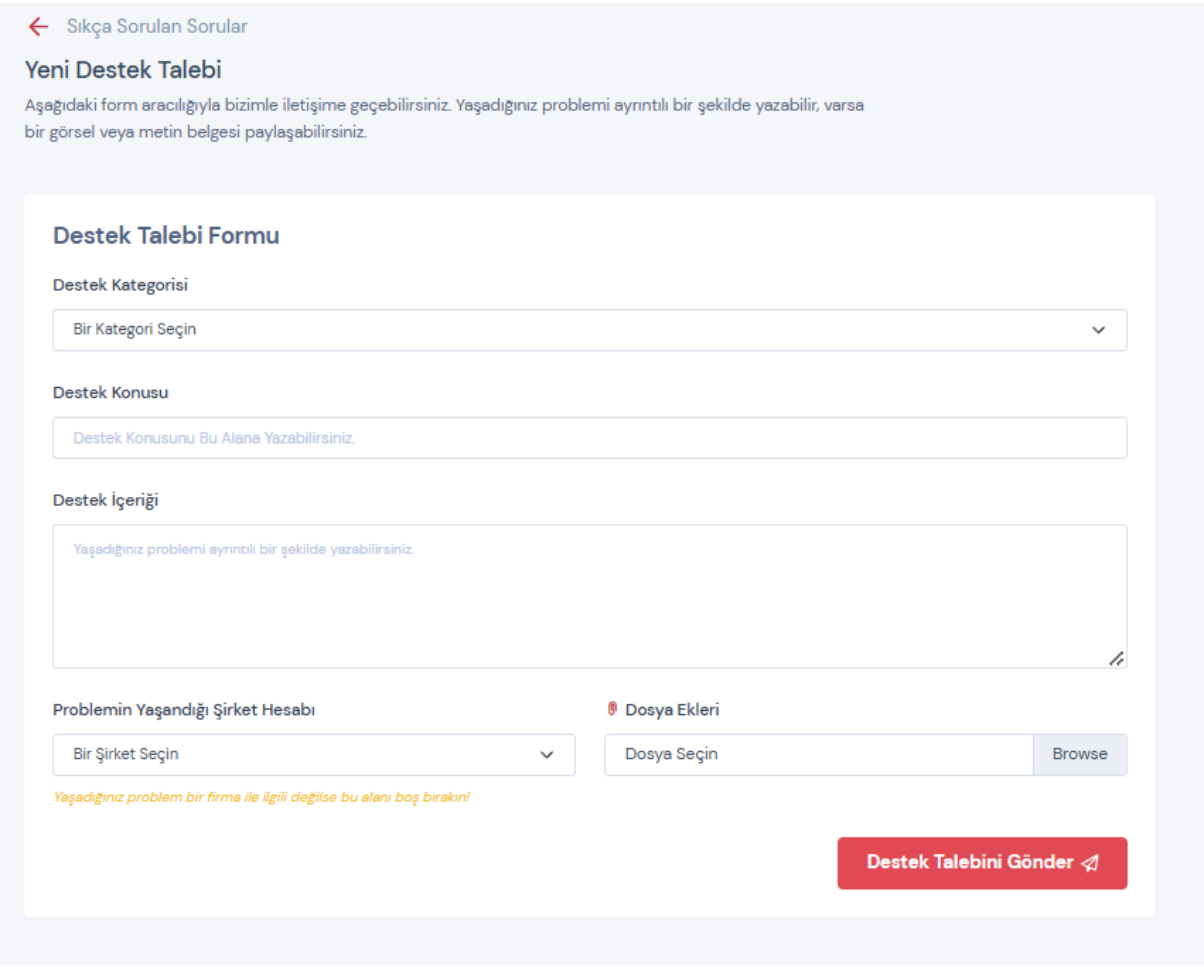


Diğer bir yol ise sol menüdeki “**Yardım Merkezi**” altındaki “**Destek Talepleri**” kısmına tıklamanız.

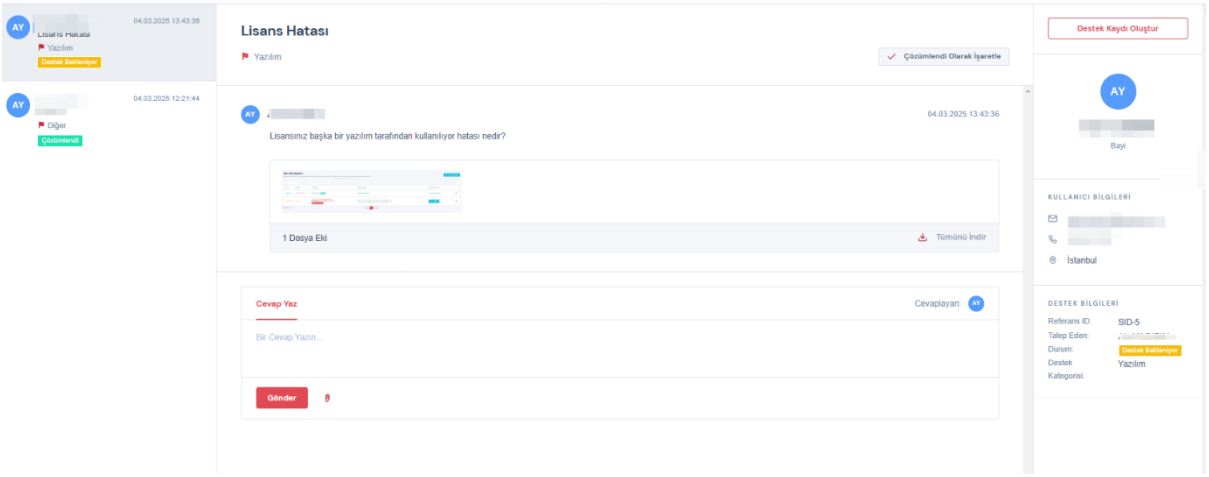


Açılan ekranda “**Yeni Bir Destek Talebi Oluştur**” butonuna tıklayınız.

Formdaki gerekli alanları doldurduktan sonra gönderme butonuna basarak işleminizi tamamlayabilirsiniz.



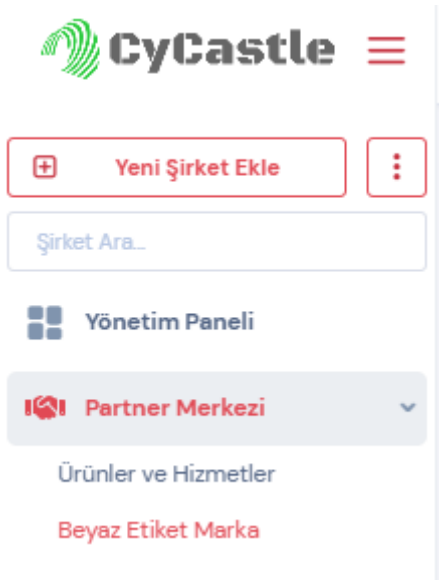
Destek taleplerinizi yine aynı sayfadan görüntüleyebilirsiniz.



Beyaz Etiket (White Label) Ayarlarını ve Logonuzu Nasıl Özelleştirebilirsiniz?

Bilgilendirme : Whitelabel hizmeti sadece bayilerimiz tarafından kullanılabilir.

Sol tarafta bulunan menüde “Partner Merkezi” altındaki “Beyaz Etiket Marka” kısmına tıklayınız.



Ekranınızın sağ üstünde bulunan “Düzenle” butonuna tıklayarak markanızı özelleştirmeye başlayabilirsiniz.

Dikkat Edilmesi Gerekenler :

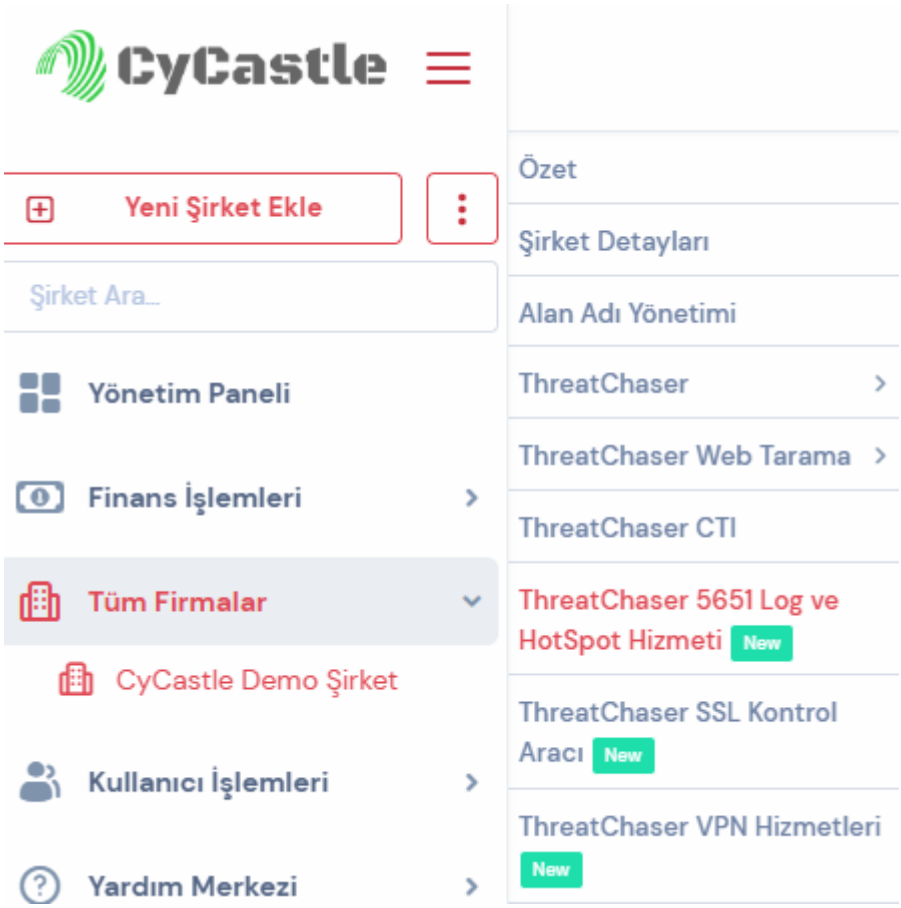
- Logo ve favicon eklemeniz durumunda, firmanıza ait logo tüm alanlarda görüntülenecektir.
- Logonun maksimum genişliği 175px olmalıdır. Yükseklik isteğinize göre değişebilir, ancak 50px'i geçmemesi tavsiye edilir.
- Favicon dosyanız .ico formatında olmalıdır. Eğer farklı bir formatta görseliniz varsa, online ico converter araçlarını kullanarak uygun formata dönüştürebilirsiniz.
- Alan adı kayıtlarının root DNS sunucuları arasında dağıtılması bazen 48 saate kadar sürebilir. Yukarıdaki alan adı için CNAME kayıtlarını doğru şekilde yönlendirdiğinizden emin olun.
- Alan adı kayıtları düzenli olarak kontrol edilmektedir. DNS kayıtları doğru yapılandırıldığında, sistem otomatik olarak aktif hale gelir.
- Alan adı kaydı tamamlandıktan sonra, ilgili alan adı için ücretsiz SSL sertifikası oluşturulacaktır.
- Eğer alan adınız Cloudflare, Amazon AWS gibi proxy hizmetleri tarafından korunuyorsa, proxy özelliğini devre dışı bırakmanız gerekir. Aksi durumda, CNAME kaydı doğrulanamaz.
- Cloudflare proxy ve DNS hizmeti kullanan müşterilerimizin durumu bize bildirmesi gerekmektedir. Cloudflare politikaları gereği, birden fazla hesaptan iç içe yönlendirme yapılması durumunda, sizinle ek olarak paylaşacağımız DNS kayıtlarını sisteme eklemeniz gerekecektir.
- Sunucularımız Cloudflare koruması altındadır.

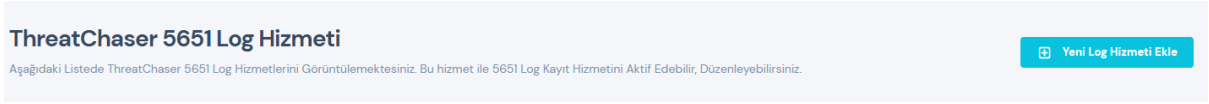
Gerekli düzenlemeleri yaptıktan sonra “Kaydet” butonuna tıklayarak işlemi gerçekleştirebilirsiniz.

5651 Loglama ve HotSpot Hizmetini Nasıl Aktif Edebilirim?

Her bir 5651 loglama hizmeti için bir adet hotspot kullanım hakkınız bulunmaktadır.

Web taraması başlatmak istediğiniz şirketin menüsünde yer alan “**ThreatChaser 5651 Log ve HotSpot Hizmeti**” bölümüne gidiniz “**Yeni Log Hizmeti Ekle**” Butonuna tıklayın.





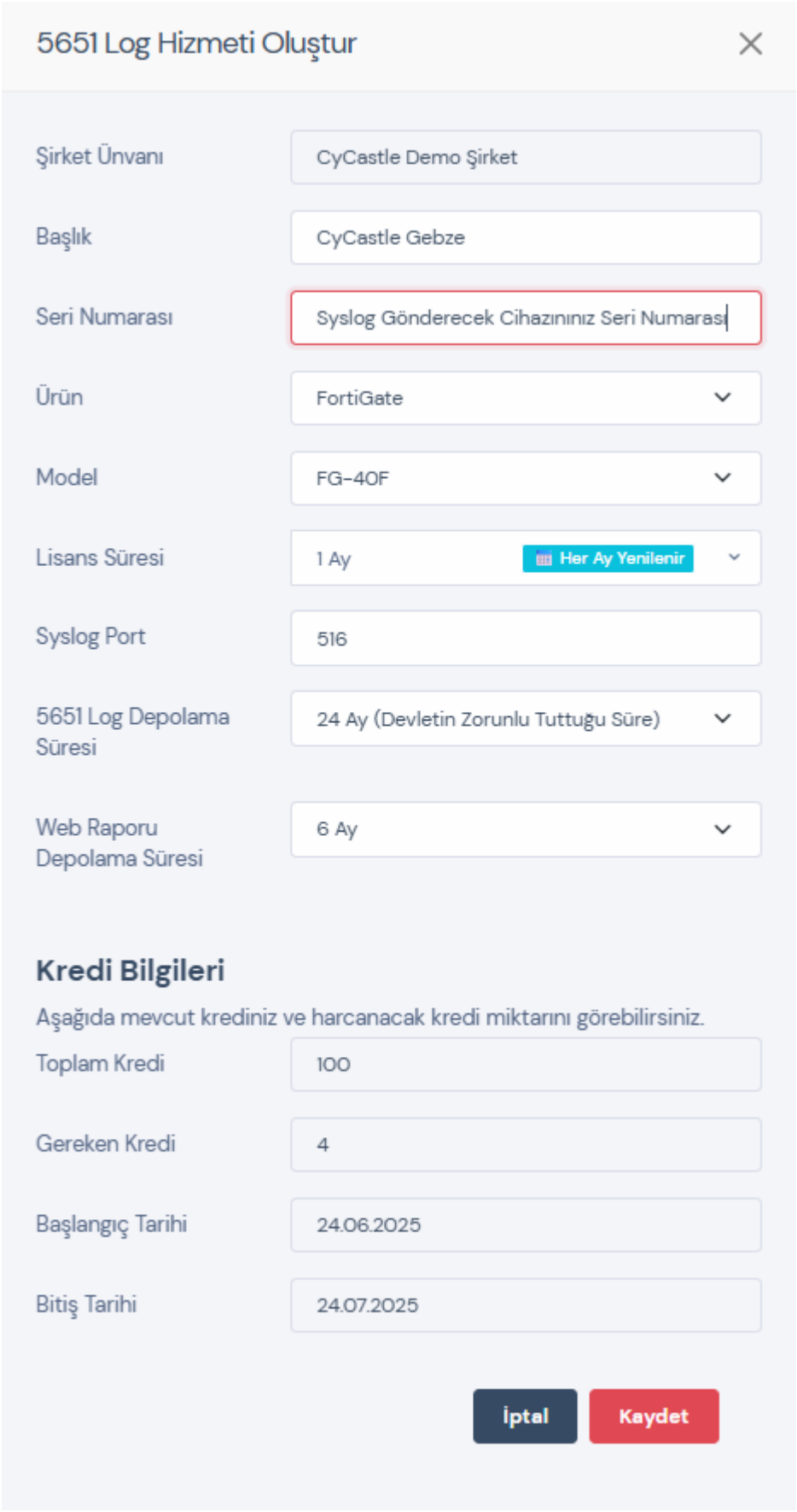
Başlık: 5651 Log Hizmetinin Adı

Seri Numarası: Syslog gönderecek cihazın seri numarasını giriniz.

Ürün: 5651 Logunu tutmak istediğiniz ürünü seçiniz.

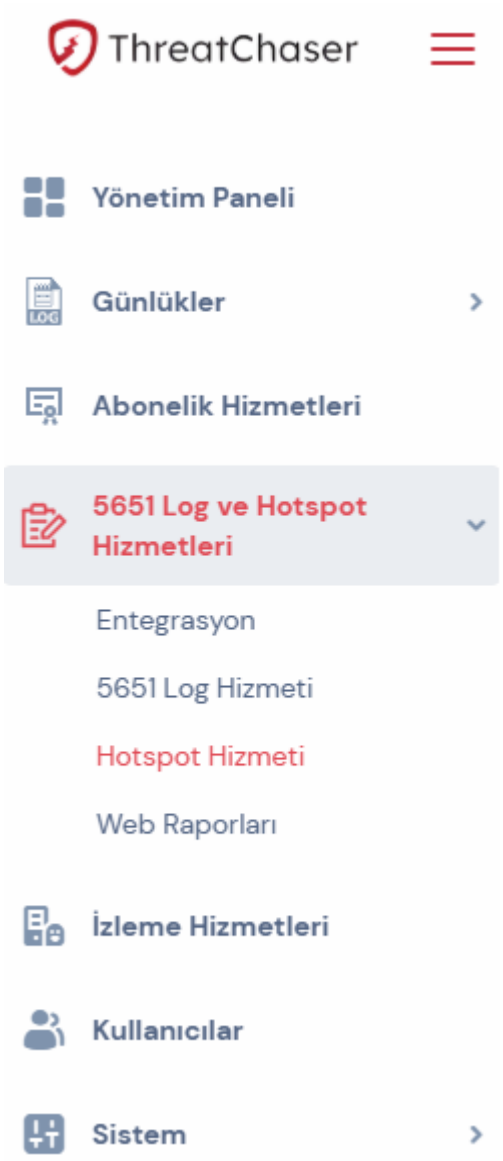
Model: 5651 Logunu tutacağınız ürünün modelini belirtiniz.

Syslog Portu: Syslog gönderen cihazda tanımlı portu giriniz.



Hotspot Hizmetini Aktif hale getirmek için ThreatChaser'ın web arayüzüne giriş yapınız

5651 Log ve Hotspot Hizmetleri -> Hotspot Hizmeti



“Yeni Hostpot Hizmeti Ekle“ Butonuna tıklayınız

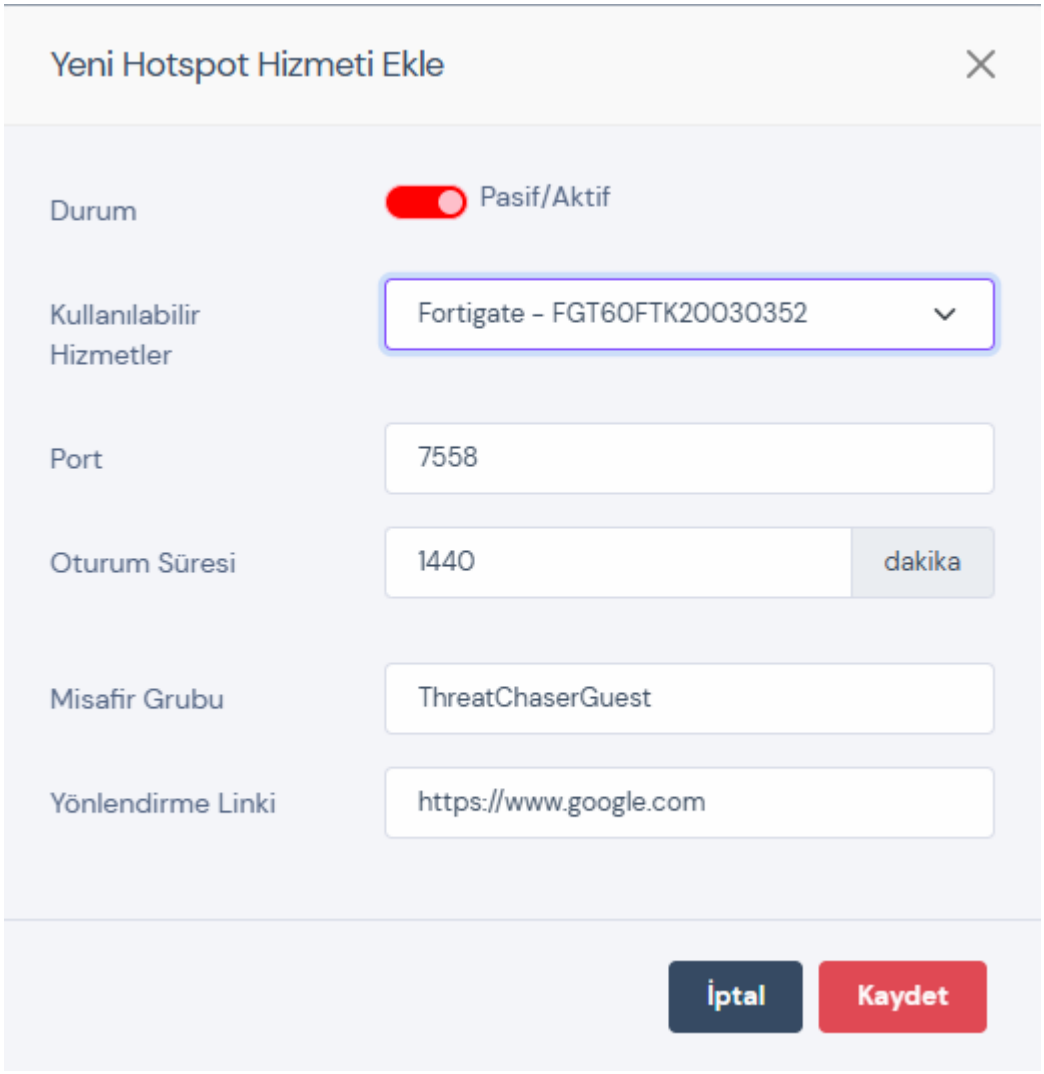
Kullanılabilir hizmetler arasından hotspot yayını yapmak istediğiniz cihazı seçiniz

HotSpot yayını yapmak istediğiniz port numarasını belirtiniz

HotSpot oturum süresini belirtiniz

FortiGate tarafında oluşturduğunuz Misafir Grubu ismini giriniz

Yönlendirme linkini belirtiniz


Yeni Hotspot Hizmeti Ekle
Durum
Pasif/Aktif
Kullanılabilir Hizmetler
Fortigate - FGT60FTK20030352
Port
7558
Oturum Süresi
1440
dakika
Misafir Grubu
ThreatChaserGuest
Yönlendirme Linki
https://www.google.com
İptal
Kaydet

Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim?

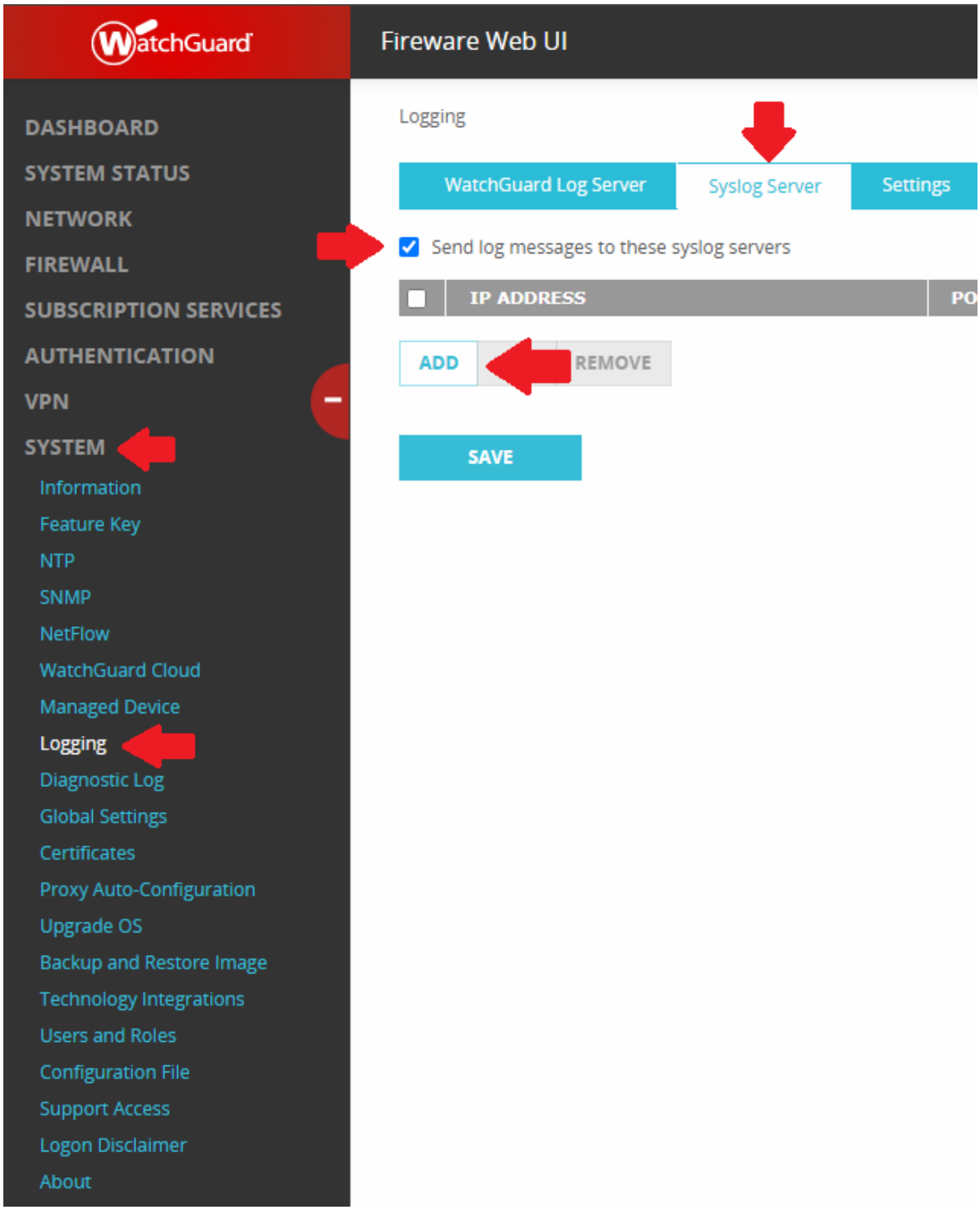
Watchguard Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim?

Watchguard Cihazınıza Web Arayüzü üzerinden giriş yapın

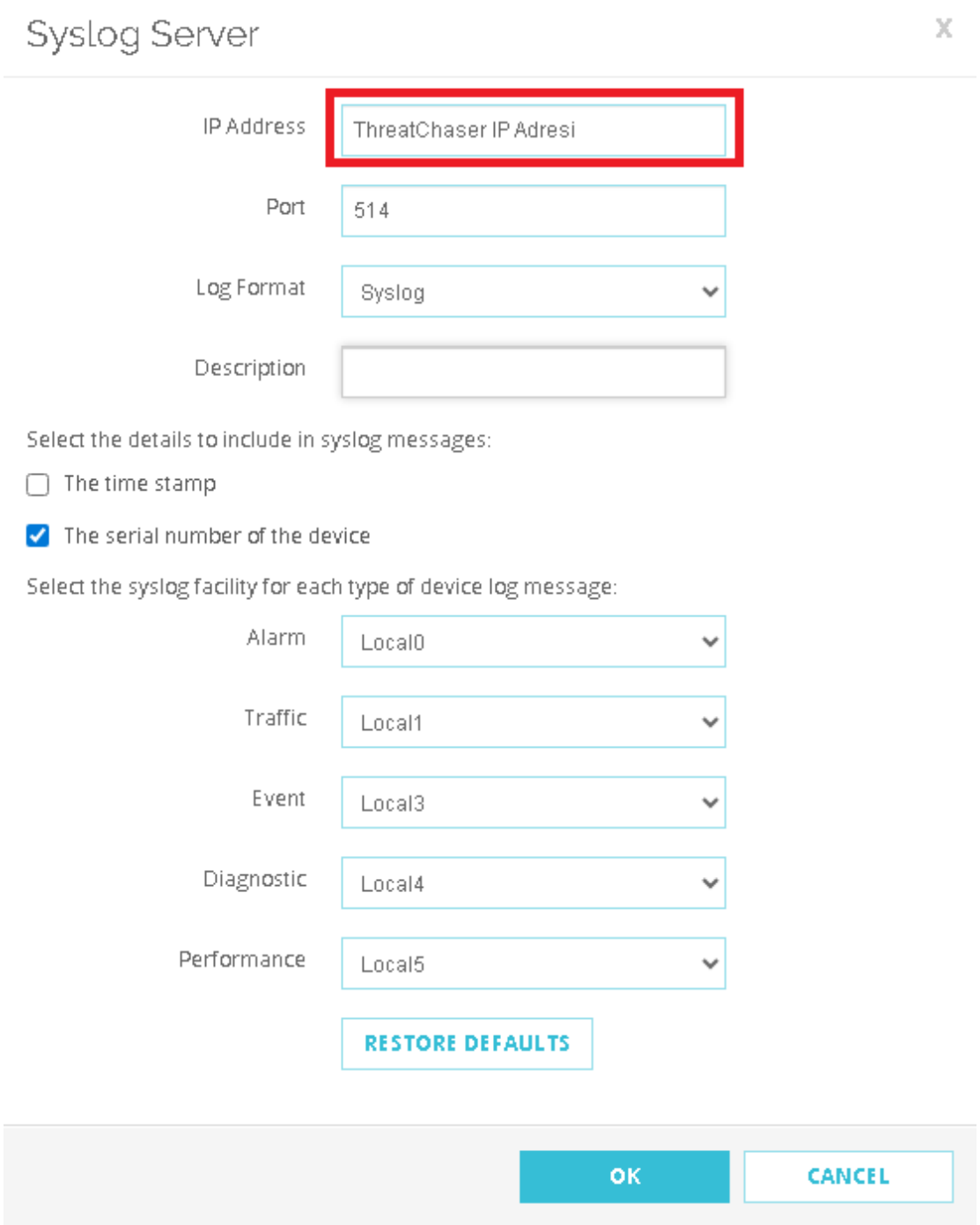
System -> Logging -> Syslog Server menüsüne gidin

“Send log messages to these Syslog servers” kutucuğunu işaretleyin

“Add” Butonuna Tıklayınız



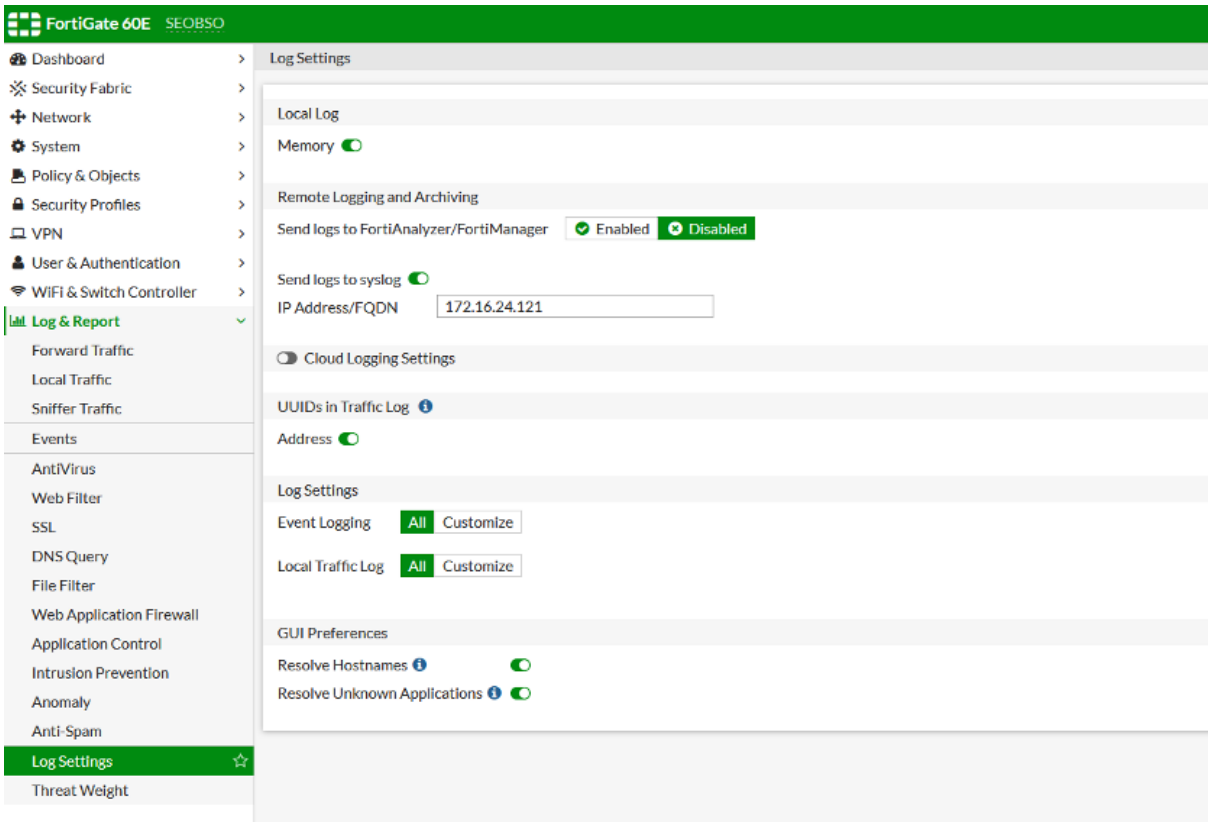
“IP Address” bölümüne ThreatChaser’ın ip adresini giriniz



FortiGate Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim?

FortiGate Cihazınıza Web Arayüzü üzerinden giriş yapın

Log & Report > Log Settings sayfasına gidin.



“Send logs to Syslog” aktif edilir ve ThreatChaser ip adresi bu alana girilir.

Event Logging “All” seçilir.

Local Traffic Log “All” seçilir.

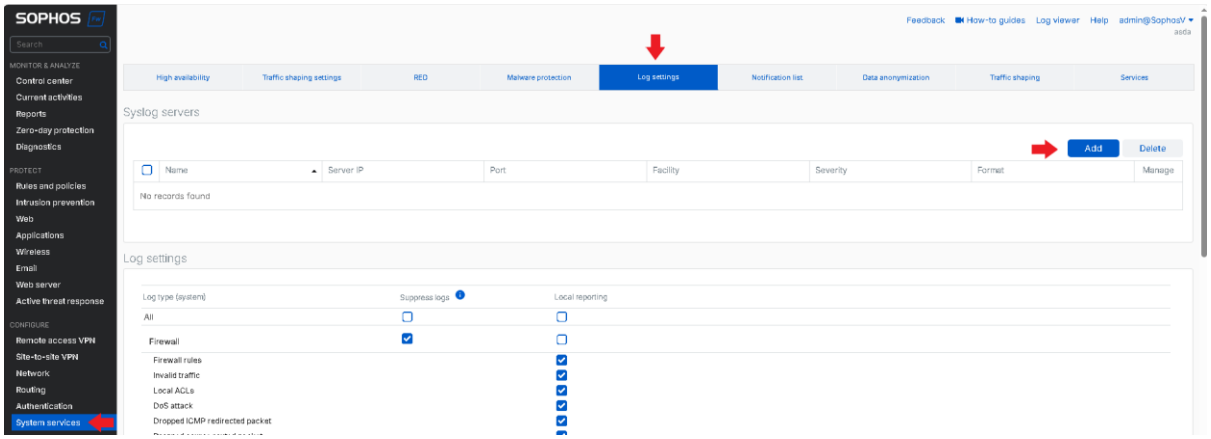
“Apply” butonuna basılarak bu işlem bitirilir.

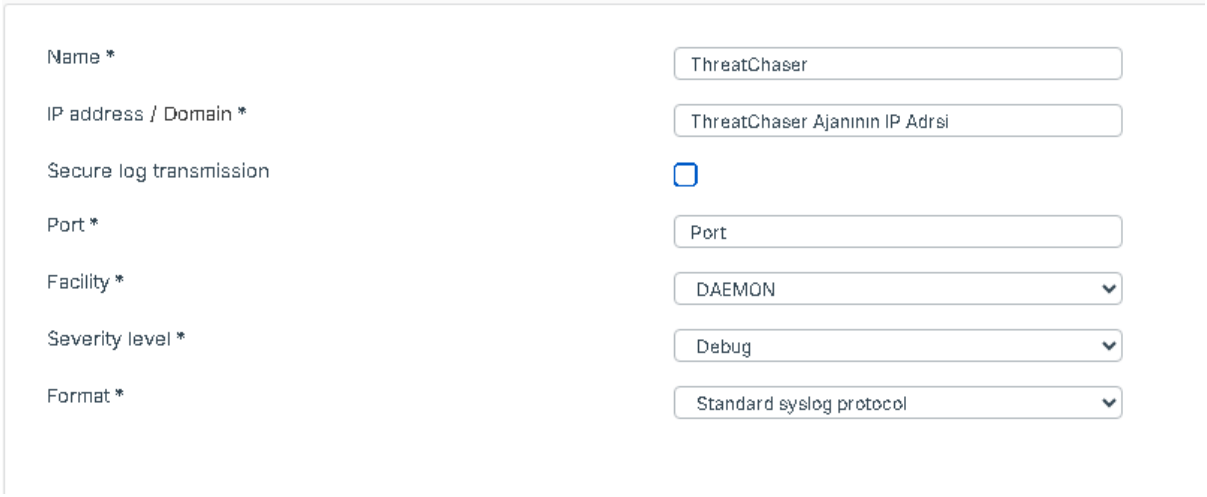
Sophos Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim?

Sophos Cihazınıza Web Arayüzü üzerinden giriş yapın

CONFİGURE & System services > Log settings sayfasına gidin.

“Add” Butonuna tıklayın





“IP Address” bölümüne ThreatChaser’ın ip adresini giriniz.

“PORT” bölümüne cloud.cycastle.com üzerinden belirlediğiniz port numarasını giriniz.

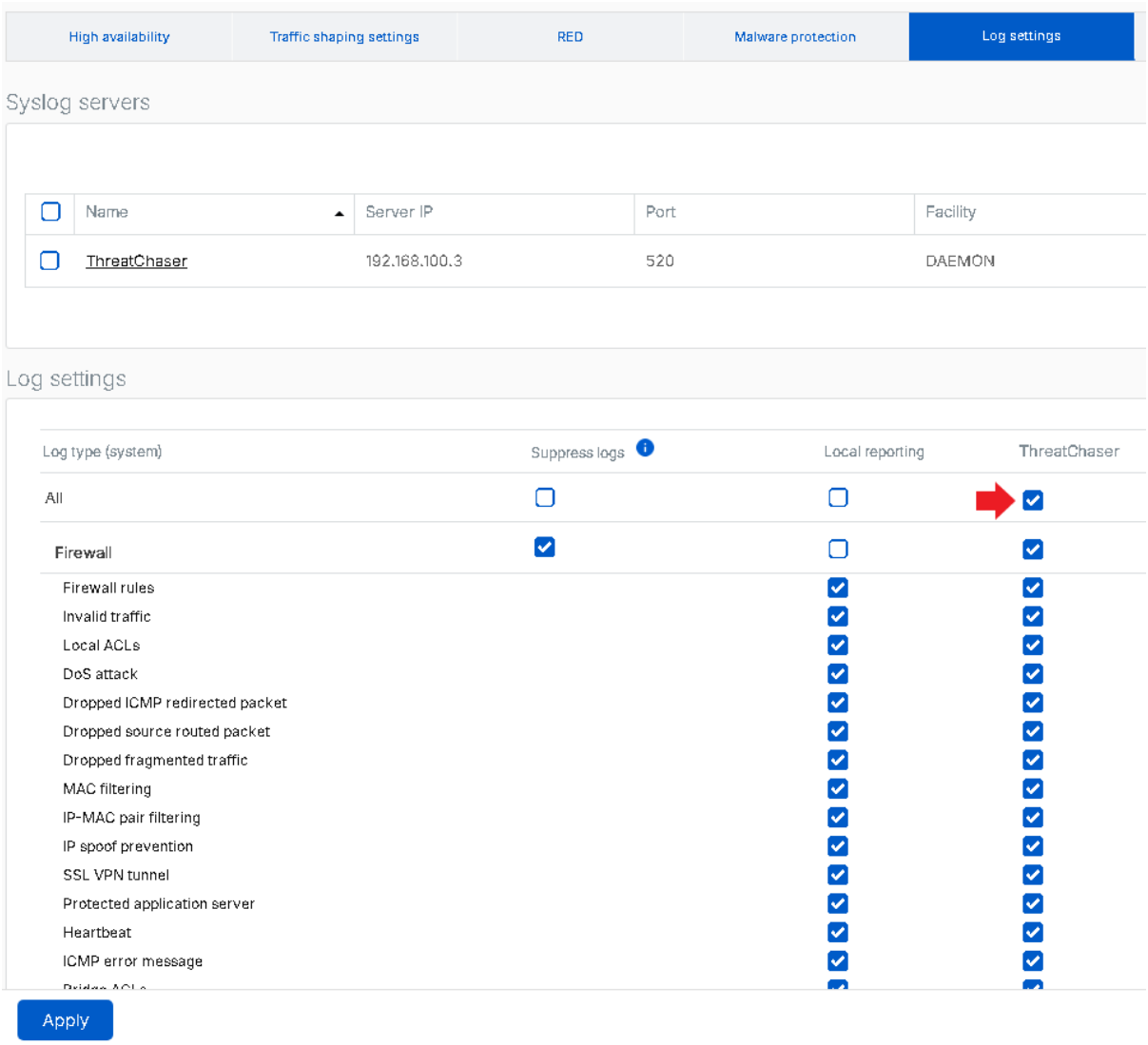
“Facility” bölümünde DAEMON seçeneğini işaretleyiniz.

“Severity “Level bölümünde Debug seçeneğini işaretleyiniz.

“Format” bölümünde Standart Syslog Protocol seçeneğini işaretleyiniz.

Tüm ayarları yaptıktan sonra Save butonuna basarak işlemi tamamlayınız.

CONFİGURE & System services > Log settings sayfasından eklediğiniz Syslog sunucusunda “All” seçeneğini işaretleyerek tüm logların gönderilmesini sağlayınız.

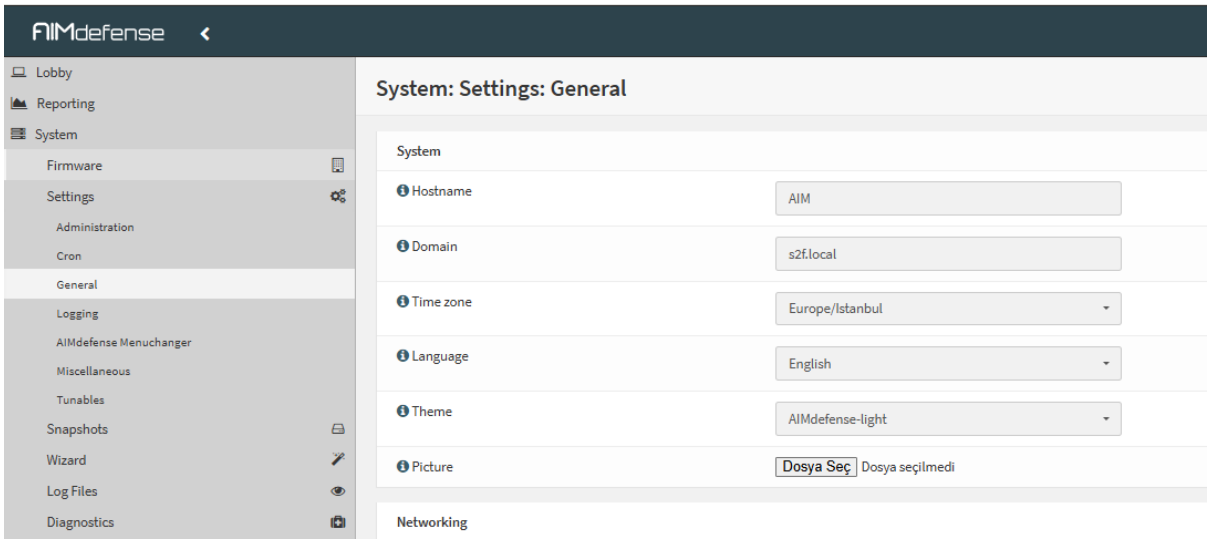

High availability
Traffic shaping settings
RED
Malware protection
Log settings
Syslog servers
Name
Server IP
Port
Facility
ThreatChaser
192.168.100.3
520
DAEMON
Log settings
Log type (system)
Suppress logs
Local reporting
ThreatChaser
All
Firewall
Firewall rules
Invalid traffic
Local ACLs
DoS attack
Dropped ICMP redirected packet
Dropped source routed packet
Dropped fragmented traffic
MAC filtering
IP-MAC pair filtering
IP spoof prevention
SSL VPN tunnel
Protected application server
Heartbeat
ICMP error message
Apply

AIMdefense Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim?

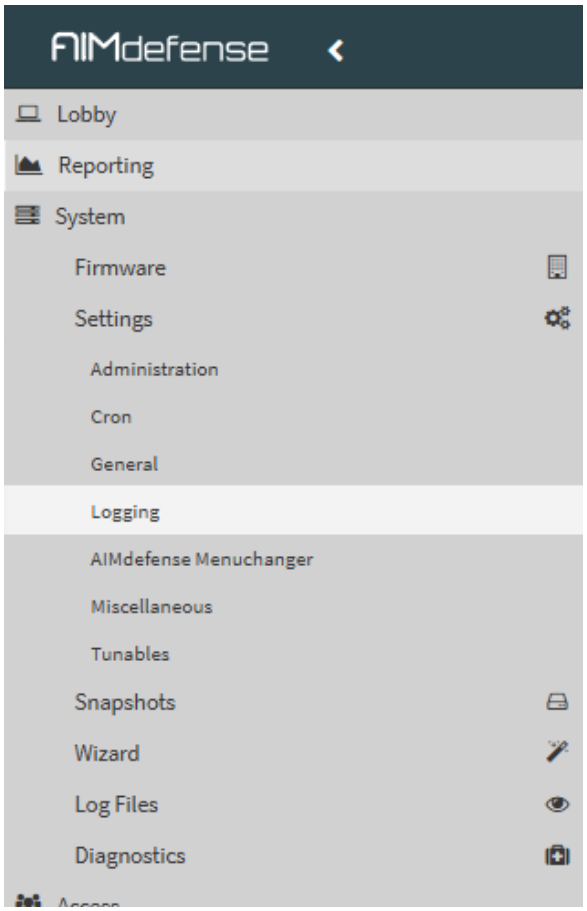
AIM Defence Cihazınıza Web Arayüzü üzerinden giriş yapın

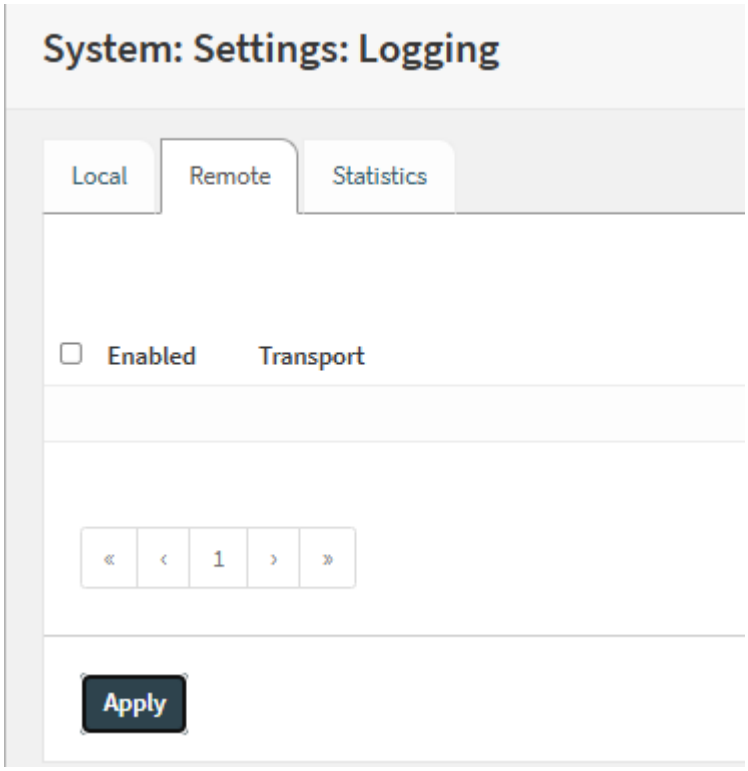
System -> Settings -> General Sayfasına gidin.

“Time Zone” bölümünden bulunduğunuz bölgeyi seçiniz

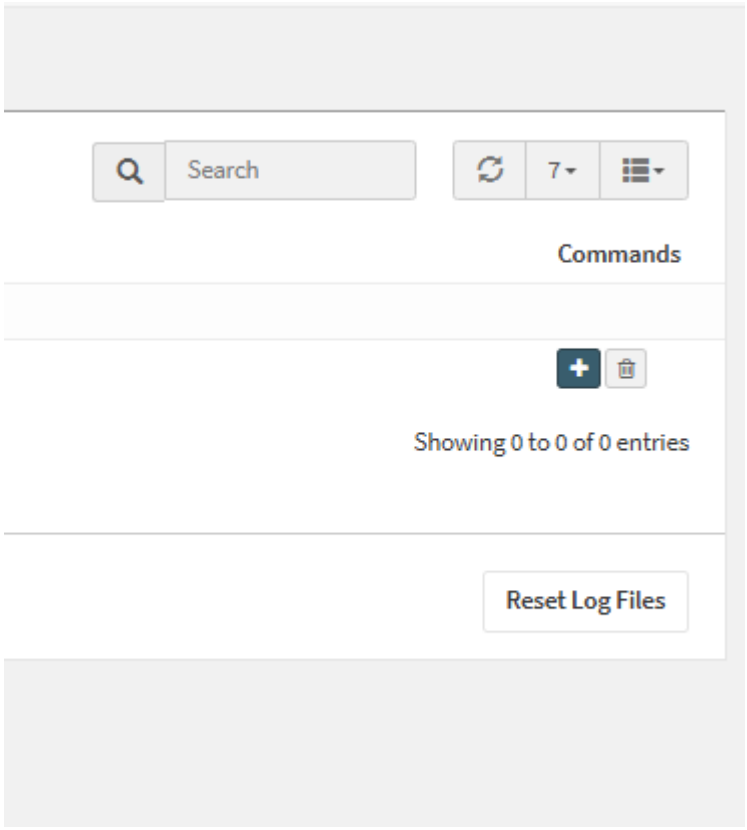


System > Logging > Remote sayfasına gidin.





“+” Butonuna Tıklayın

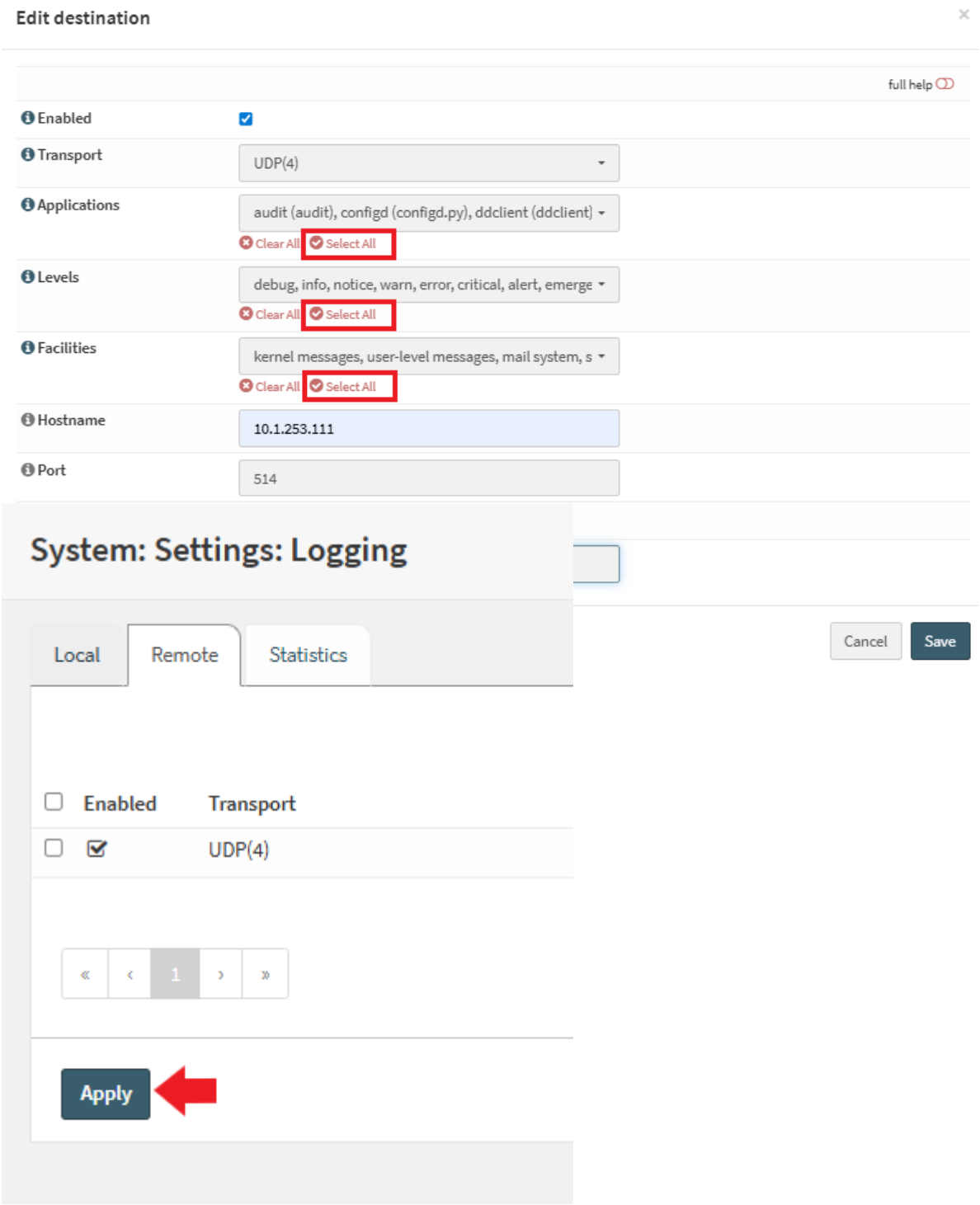


Applications, Levels ve Facilities bölümlerinde “Select All” seçeneğini seçiniz

“Hostname” bölümüne ThreatChaser’ın ip adresini giriniz.

“PORT” bölümüne cloud.cycastle.com üzerinden belirlediğiniz port numarasını giriniz.

Tüm ayarları tamamladıktan sonra “Save” butonuna basarak işlemi kaydediniz. Ardından, ayarların geçerli olabilmesi için “Apply” butonuna tıklayınız.

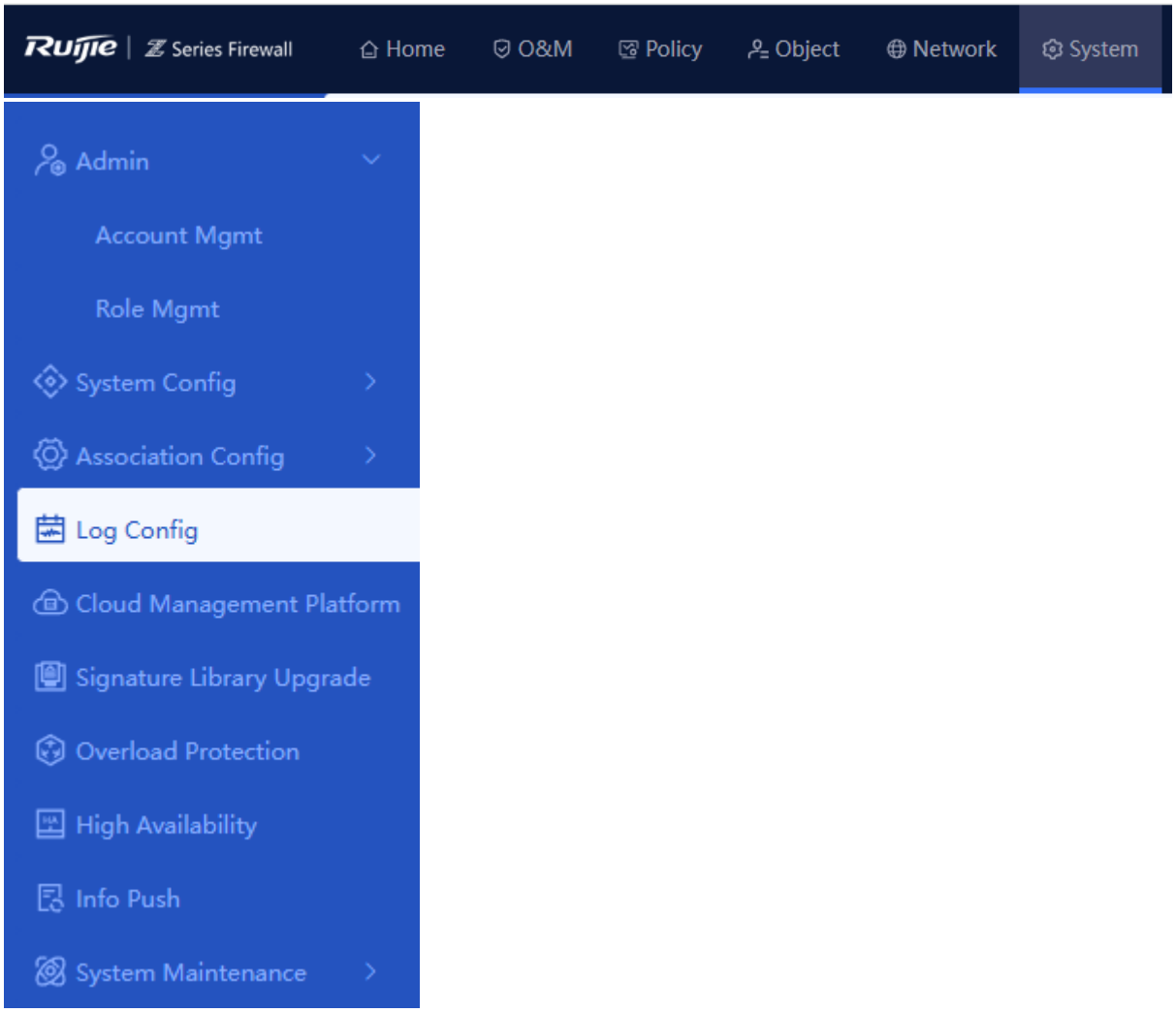


Ruijie Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim?

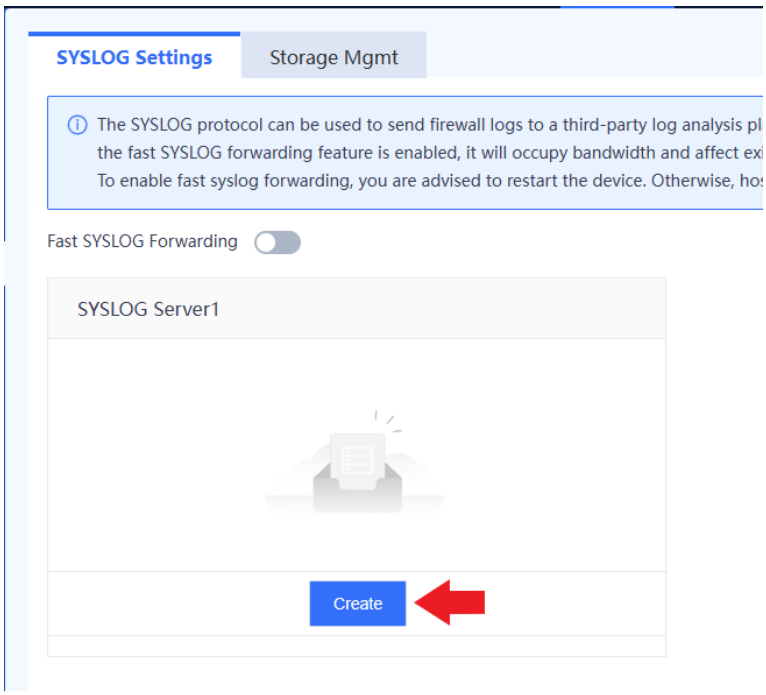
Ruijie Cihazınıza Web Arayüzü üzerinden giriş yapın

Cihazınızın en son sürümde olduğundan emin olun; sürümler arasındaki ekranlar farklılık gösterebilir.

System -> Log Config -> Syslog Settings menüsüne gidin



“Create” Butonuna Tıklayınız



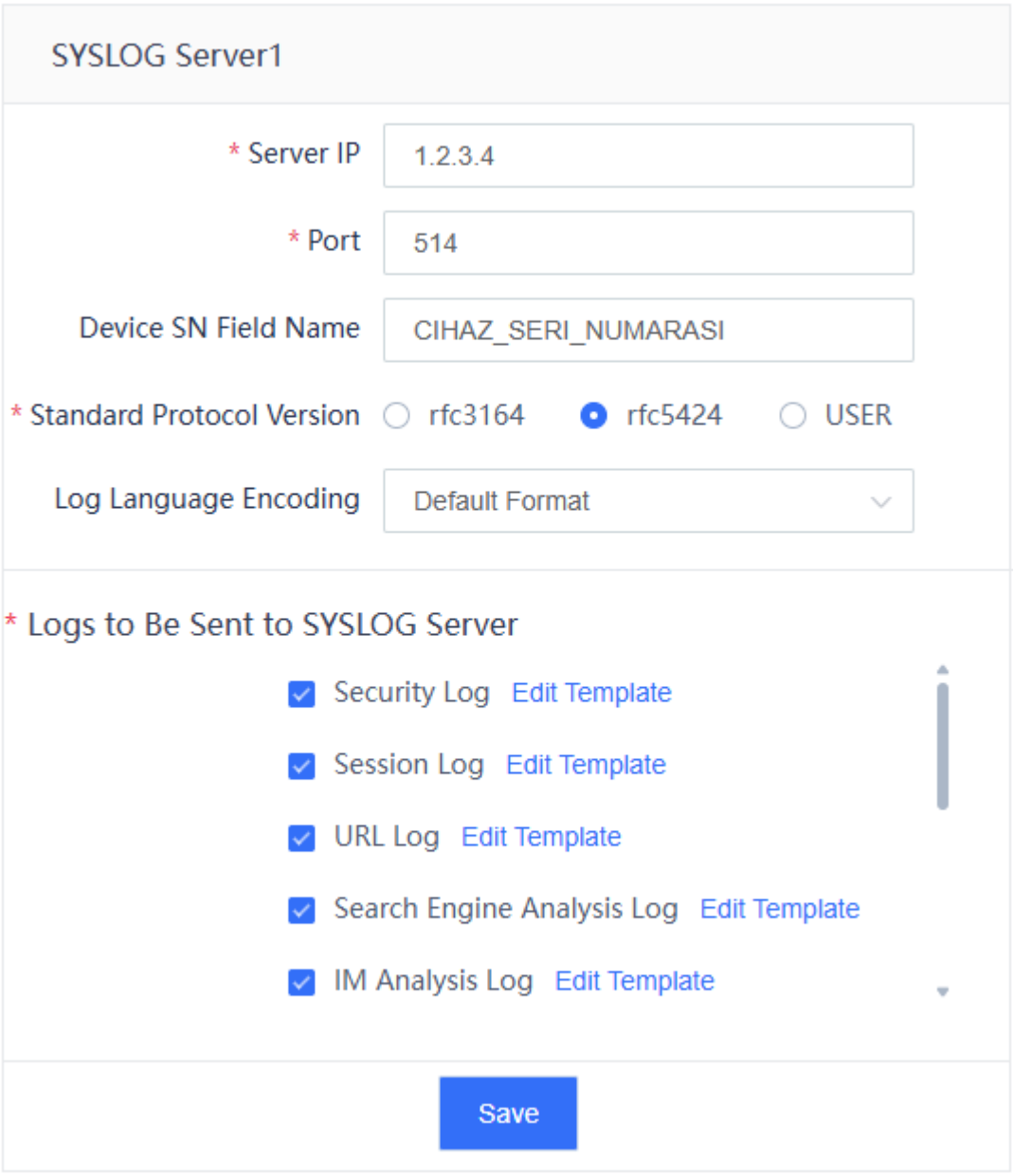
Server IP bölümüne ThreatChaser'ın ip adresini giriniz

Port bölümüne Syslog için kullanacağınız portu giriniz

Device SN Field Name bölümüne cihazınızın seri numarasını girin

Standart Protocol Version bölümünde rfc3164 ya da rfc5424'ü seçiniz

Logs to Be Sent to SYSLOG Server bölümündeki bütün seçenekleri işaretleyin

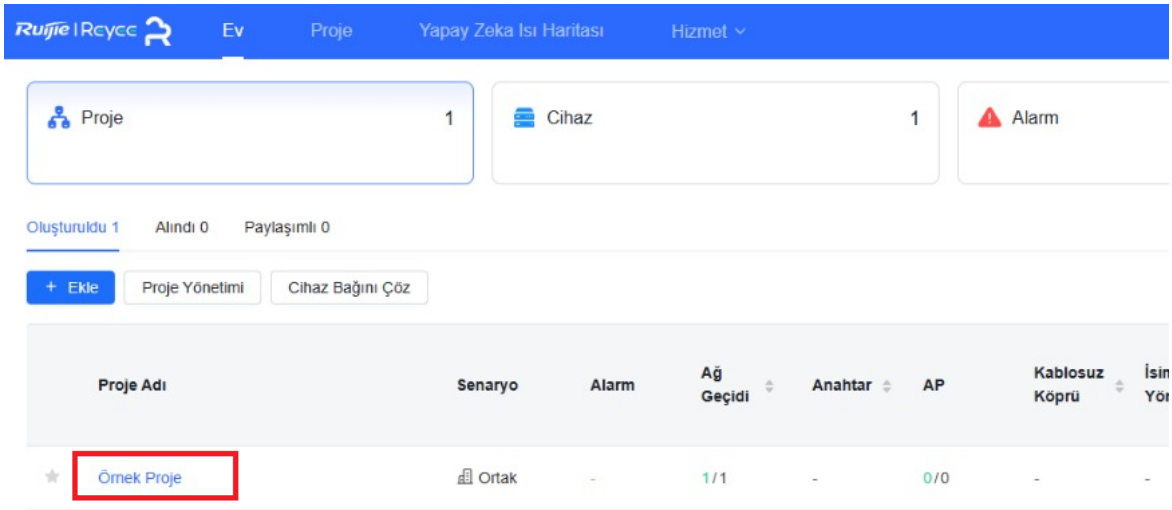


Ruijie Reyee Cihazımdan Syslog Yönlendirmesini Nasıl Gerçekleştirebilirim?

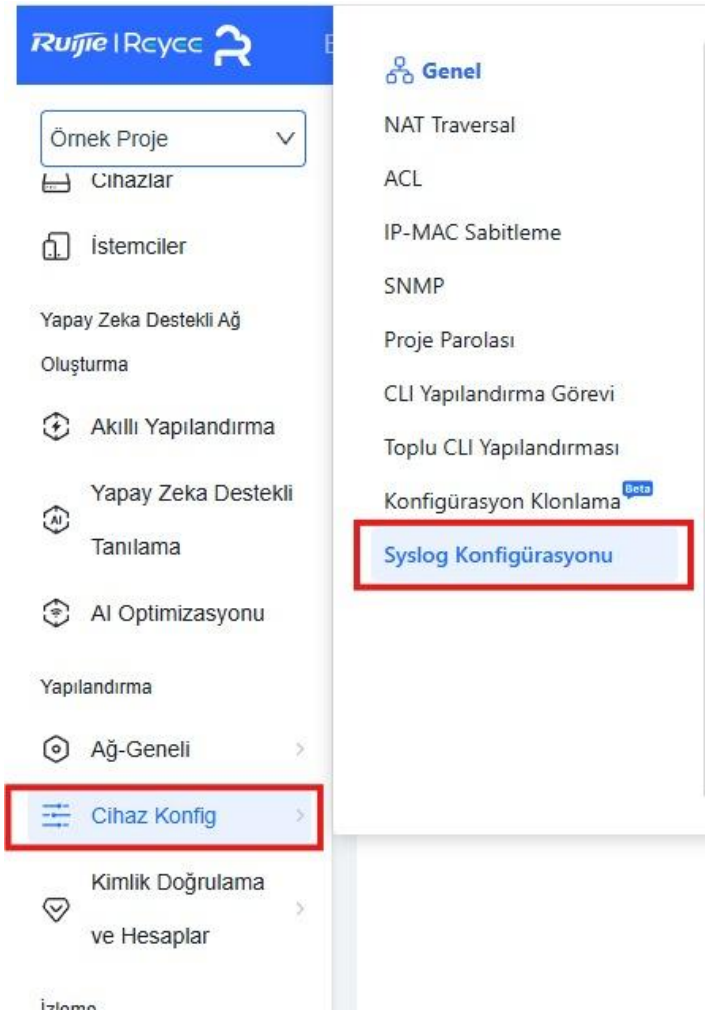
Cloud Üzerinden Yönlendirme

Yaptığınız işlemlerin geçerli olabilmesi için Ruijie Reyee cihazınızın bulut (cloud) entegrasyonunun tamamlanması gerekmektedir.

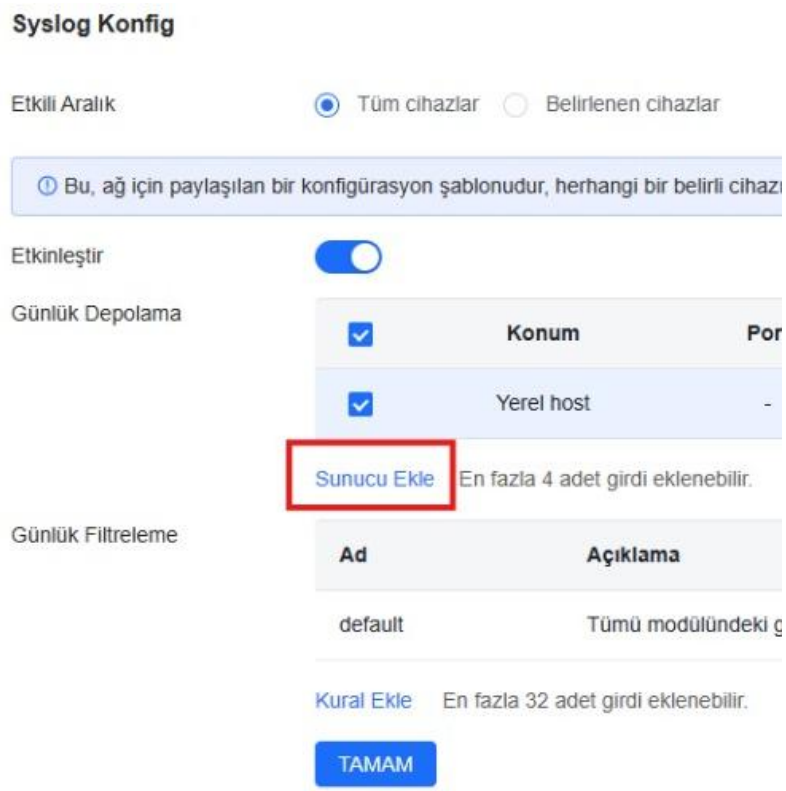
Daha önceden eklediğiniz Ruijie Reyee cihazınızı seçin



Cihaz Konfig -> Syslog Konfigürasyonu menüsüne gidin



Sunucu Ekle butonuna tıklayın

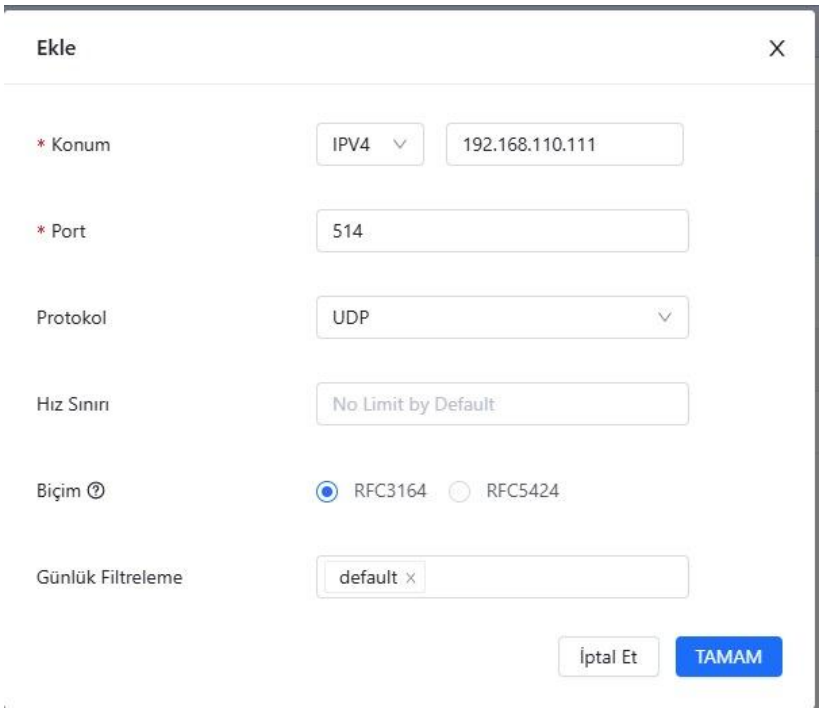


Konum bölümüne ThreatChaser'ın ip adresini giriniz

Port bölümüne Syslog için kullanacağınız portu giriniz

Biçim bölümünde rfc3164 ya da rfc5424'ü seçiniz

Günlük Filtreleme bölümünde default'u seçiniz



Lokal Arayüz Üzerinden Yönlendirme

Cihazınıza Web Arayüzü üzerinden giriş yapın

Gelişmiş -> Denetim Logu Sayfasına gidin

Etkinleştir seçeneğini seçin

Sunucu türü bölümünü varsayılan olarak seçin

Sunucu adresi bölümüne **ThreatChaser'ın ip adresini** girin

Port bölümüne Syslog için kullanacağınız portu giriniz

Log gönder Hızı bölümünü ağınızın büyüklüğüne göre değişiklik gösterebilir. Varsayılan ayarı 5000'dir

Log türü seçeneklerini aşağıdaki gibi olacak şekilde ayarlayınız

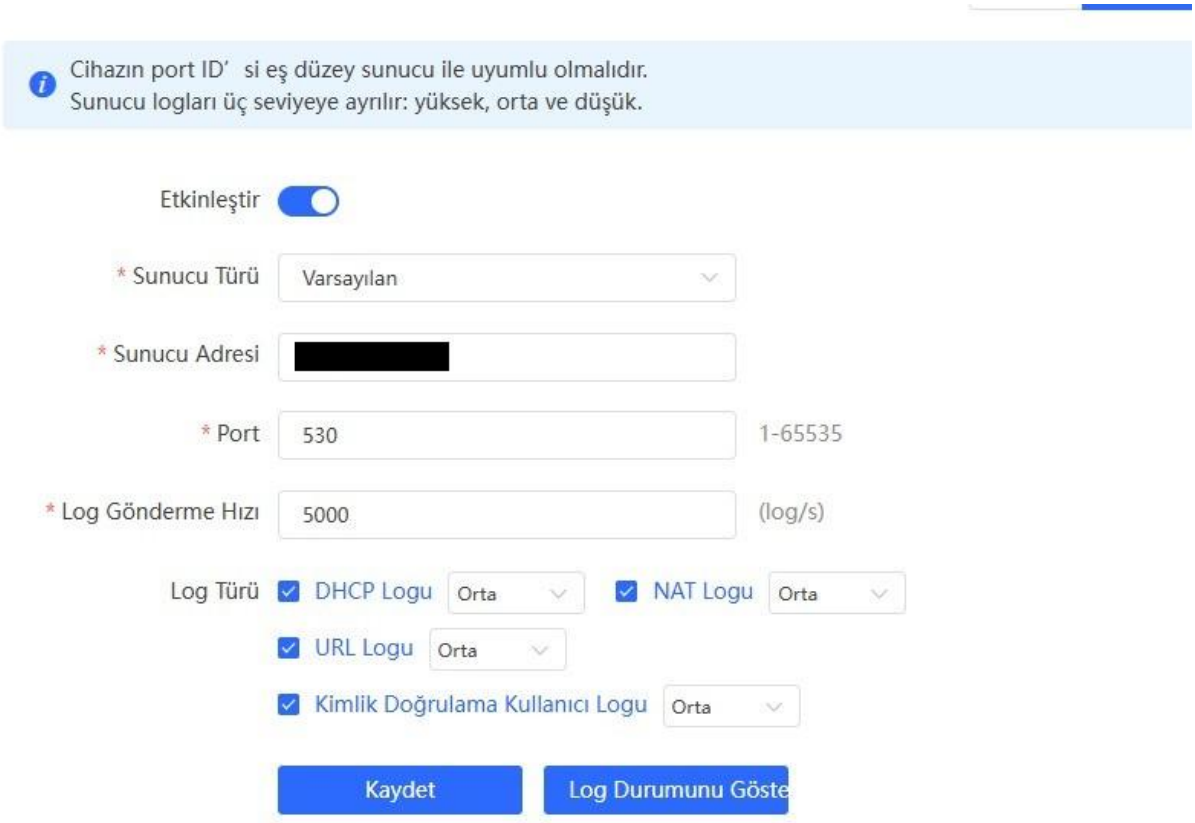
DHCP Logu Orta

URL Logu Orta

Nat Logu Orta

Kimlik Doğrulama Kulllanıcı Logu Orta

Tüm ayarları yaptıktan sonra **Kaydet** butonuna basarak işlemi tamamlayınız.

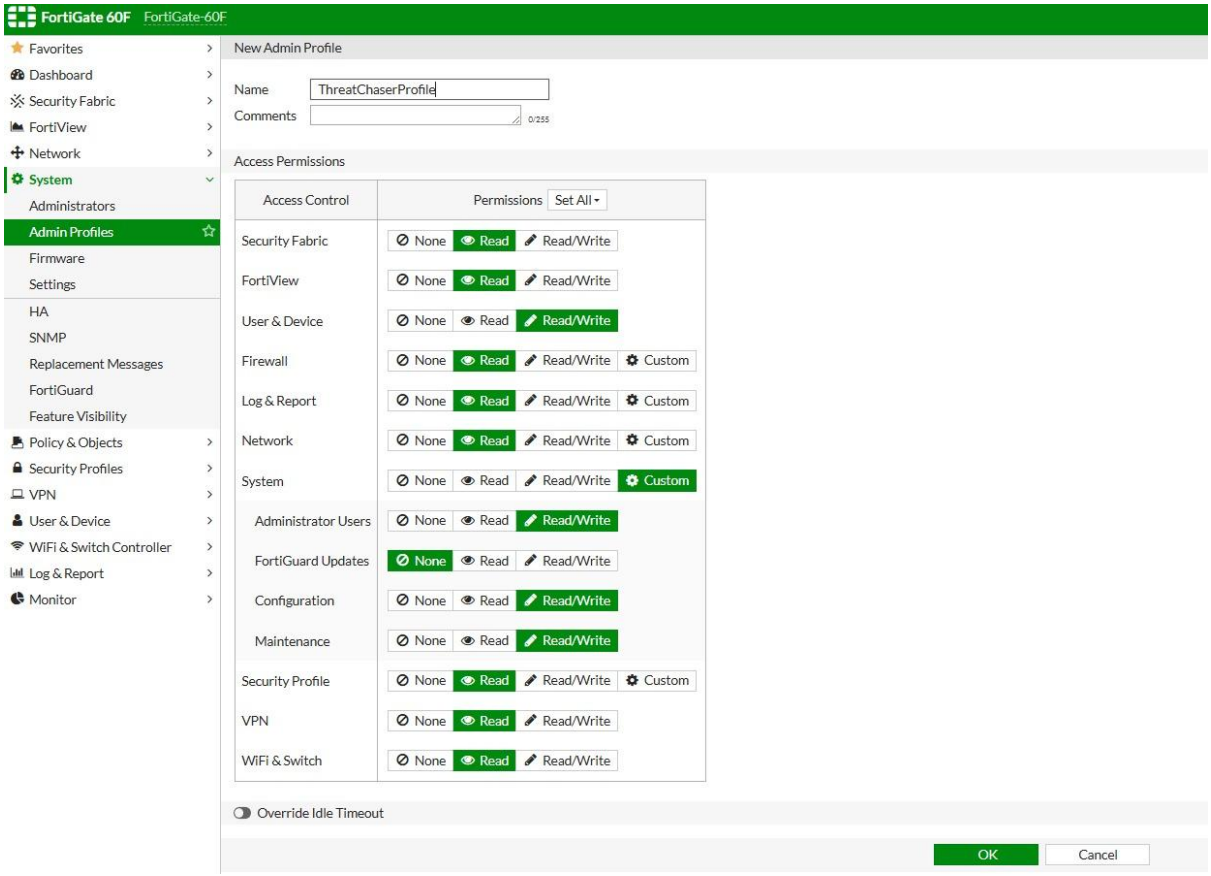


Cihazımdan HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim?

FortiGate API İşlemleri

API Kullanıcısı oluşturmak için System -> Admin Profile Sayfasına gidin

Aşağıdaki gibi bir profil oluşturunuz



System -> Administrators Sayfasına gidin

Create New -> REST API Admin butonuna tıklayınız

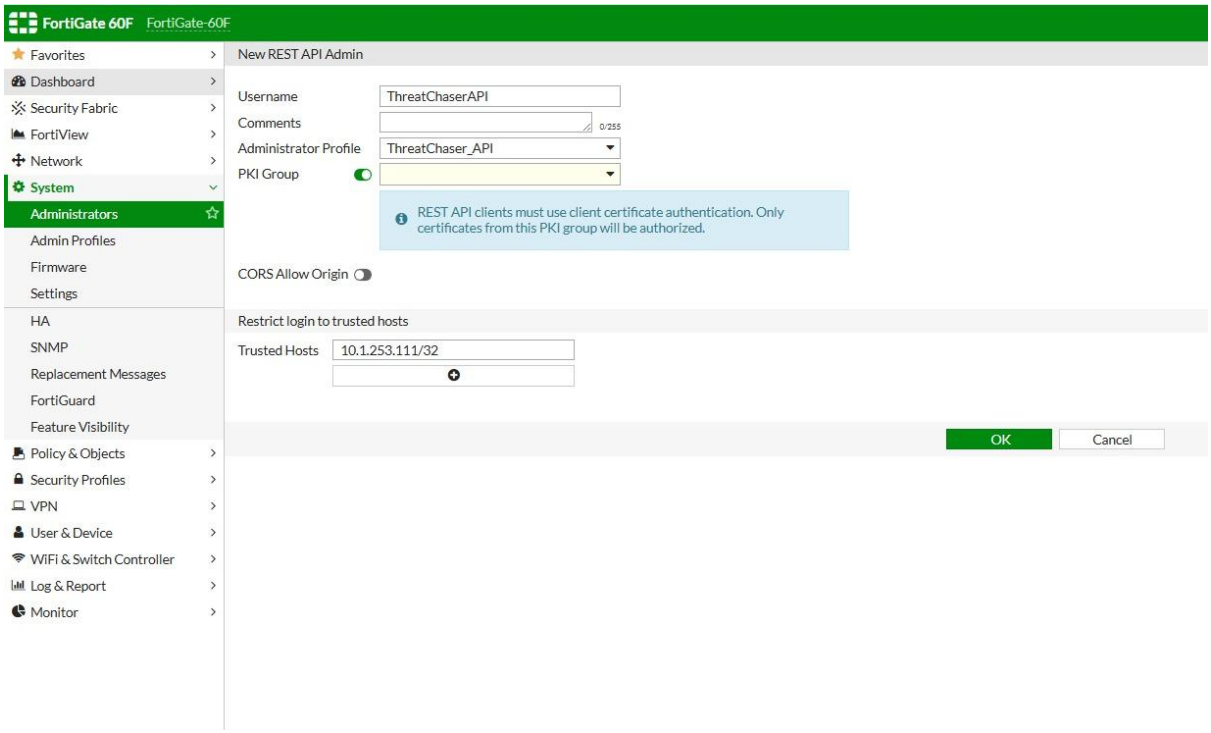
Açılan sayfada yeni bir API kullanıcısı oluşturuyoruz.

Kullanıcı Adını yazıyoruz

Administrator Profile kısmında oluşturduğumuz API profilini seçiyoruz.

Trusted Hosts kısmında ThreatChaser yazılımının IP adresini yazıyoruz.

Önemli Not: Burada bize verilen API key bilgisini ThreatChaser ayarlarına kayıt edeceğiz.

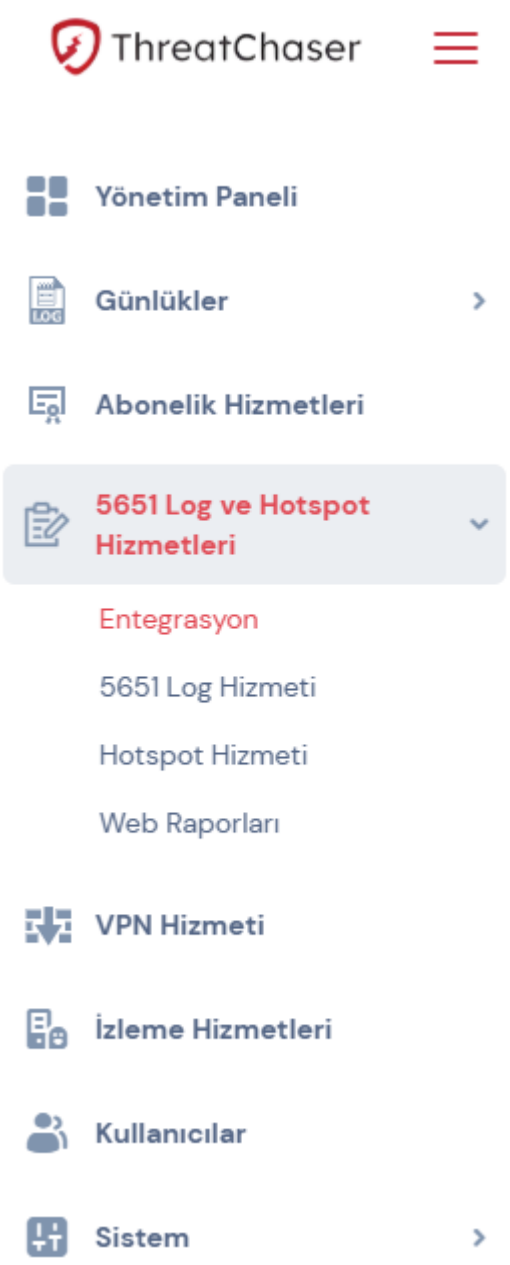


FortiGate Cihazımdan HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim?

ThreatChaser Tarafındaki Ayarlamalar

ThreatChaser'a web arayüzü üzerinden erişim sağlayınız

5651 Log ve Hotspot Hizmetleri -> Entegrasyon sayfasına gidin



Entegrasyon yapacağınız firewall için düzenleme simgesine tıklayınız.

“IP Adresi” bölümüne FortiGate’in ip adresini giriniz.

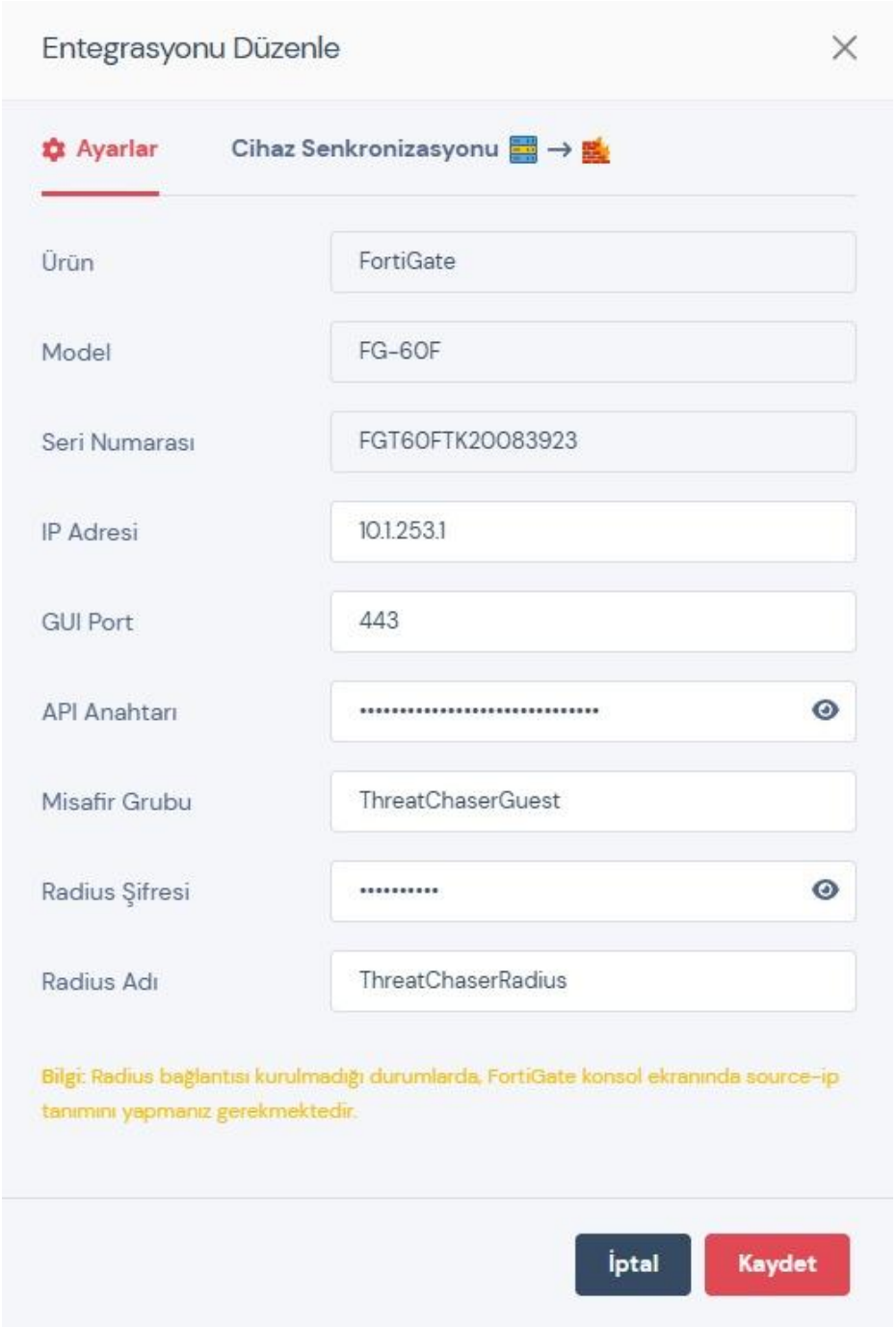
“GUI Port” bölümüne FortiGate’in port numarasını giriniz.

“API Anahtarı” bölümüne FortiGate’te oluşturduğunuz API Anahtarını giriniz.

“Misafir Grubu” Bu bölümün User Groups menüsüne eklediğiniz isimle aynı olması gerekiyor.

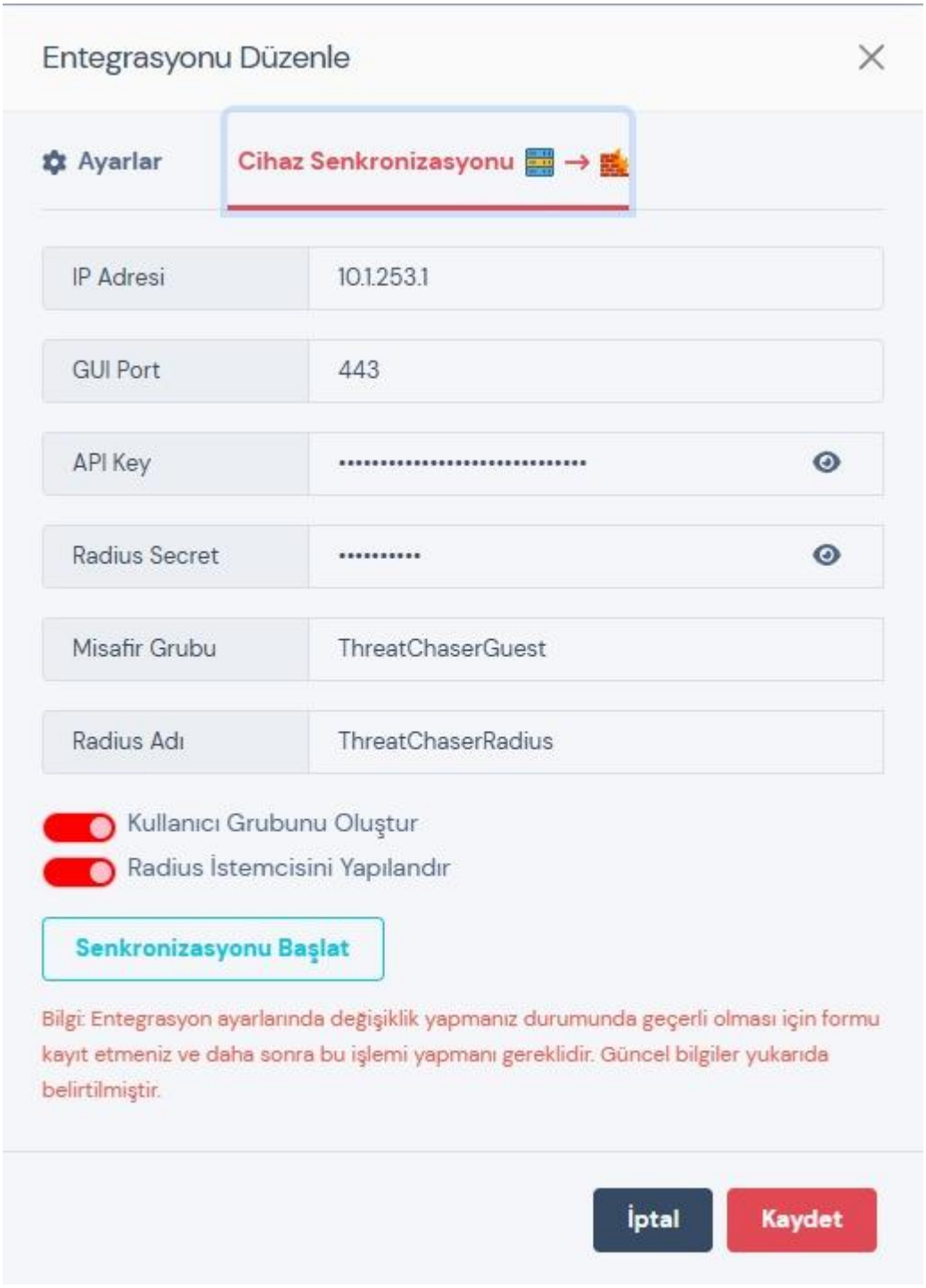
“Radius Şifresi” Bu bölüme FortiGate’in ThreatChaser ile iletişime geçebilmesi için bir şifre oluşturmanız gerekiyor.

“Radius Adı” Bu bölümün FortiGate tarafında Radius Server ismiyle aynı olması gerekiyor.



Eğer FortiGate tarafında kullanıcı grubunu oluşturmak ve RADIUS yapılandırmasını otomatik olarak yapmak istiyorsanız, bu işlemi Cihaz Senkronizasyonu üzerinden gerçekleştirebilirsiniz.

Not: Bu işlemi manuel yapmak istiyorsanız, bu adımı atlayabilirsiniz.



Firewall Tarafındaki Ayarlamalar

FortiGate Cihazınıza Web Arayüzü üzerinden giriş yapın

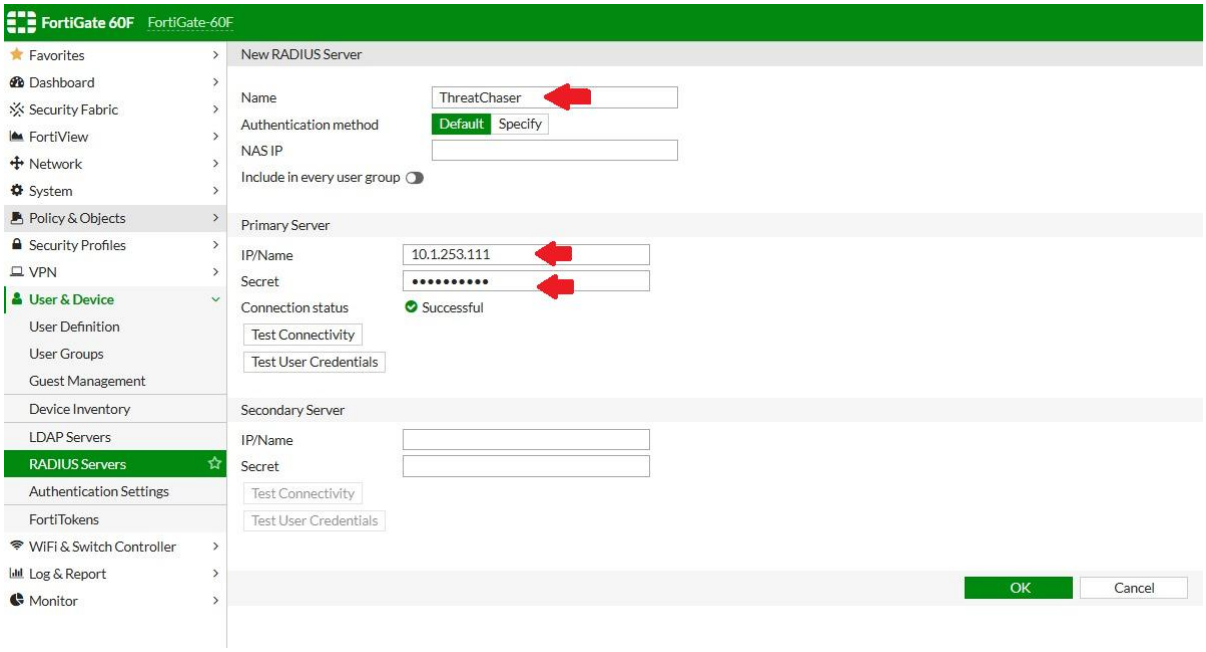
User & Device -> RADIUS Server menüsüne gidin

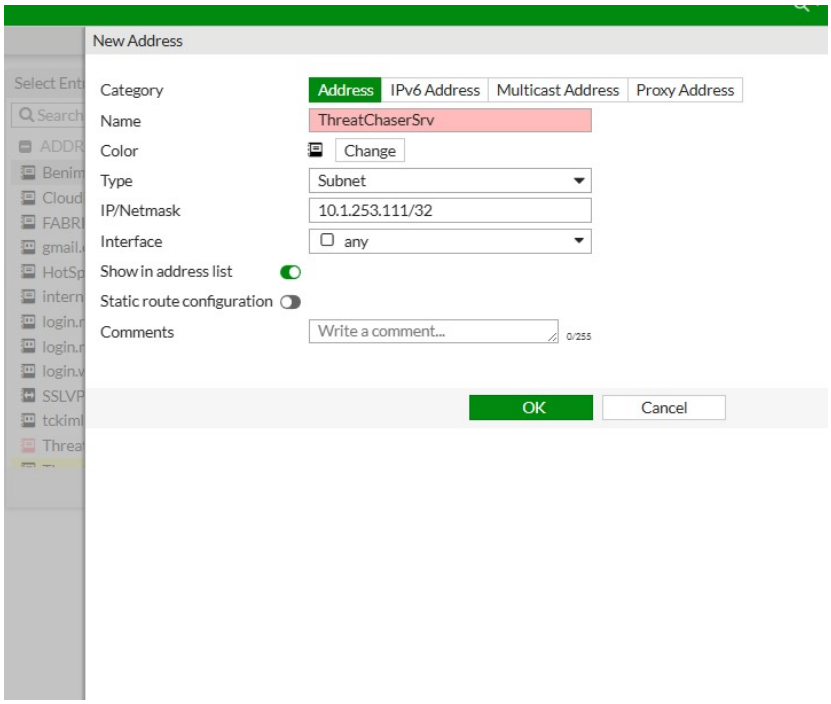
“Create New” Butonuna tıklayın

Name: Oluşturduğunuz RADIUS server’ına bir isim verin

IP Adresini kısmına ThreatChaser’ın ip adresini giriniz

ThreatChaser’ın Radius ile haberleşmesi için bir şifre oluşturun. Bu şifre ThreatChaser Entegrasyon bölümünde girdiğiniz Radius Şifresi ile aynı olması gerekmektedir.





ThreatChaser için yeni bir adres oluşturunuz

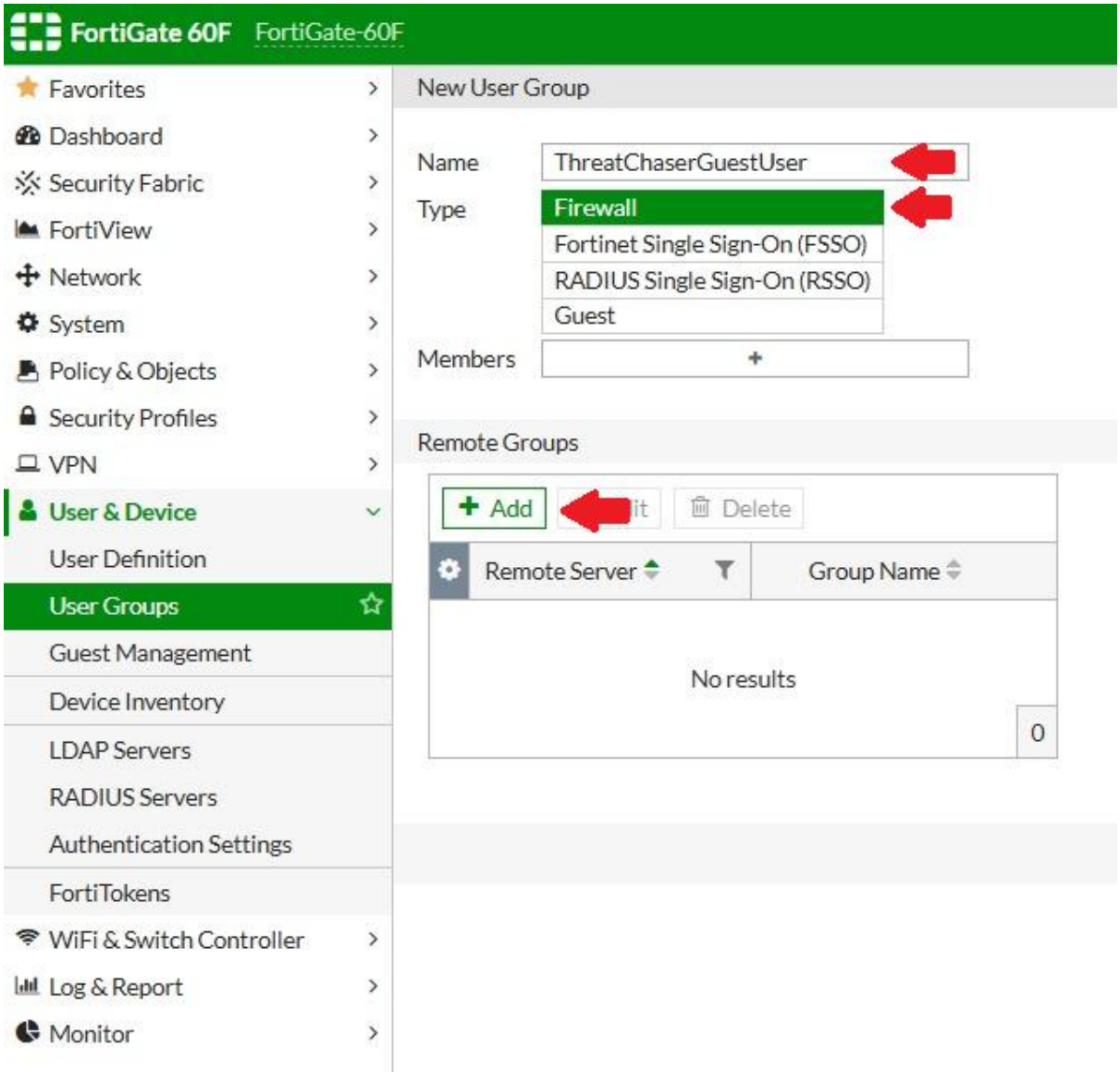
User & Devices -> User Groups menüsüne gidin

“Create New” butouna tıklayın

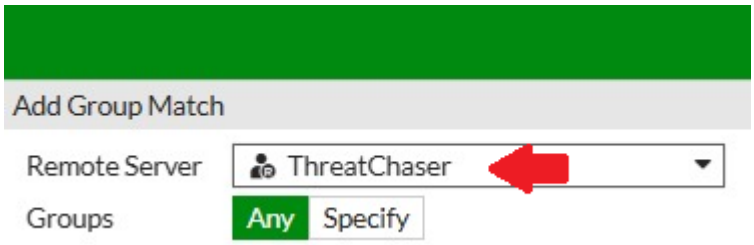
Name kısmına oluşturacağınız grup için bir isim belirleyiniz daha sonra bu ismi threatchaser ayarlarında belirtmeniz gerekecek

Type kısmını Firewall olarak seçiniz

Remote Groups başlığının altındaki “Add” butonuna tıklayınız



Sağ tarafta açılan sayfada oluşturduğunuz RADIUS Server'ı seçiniz



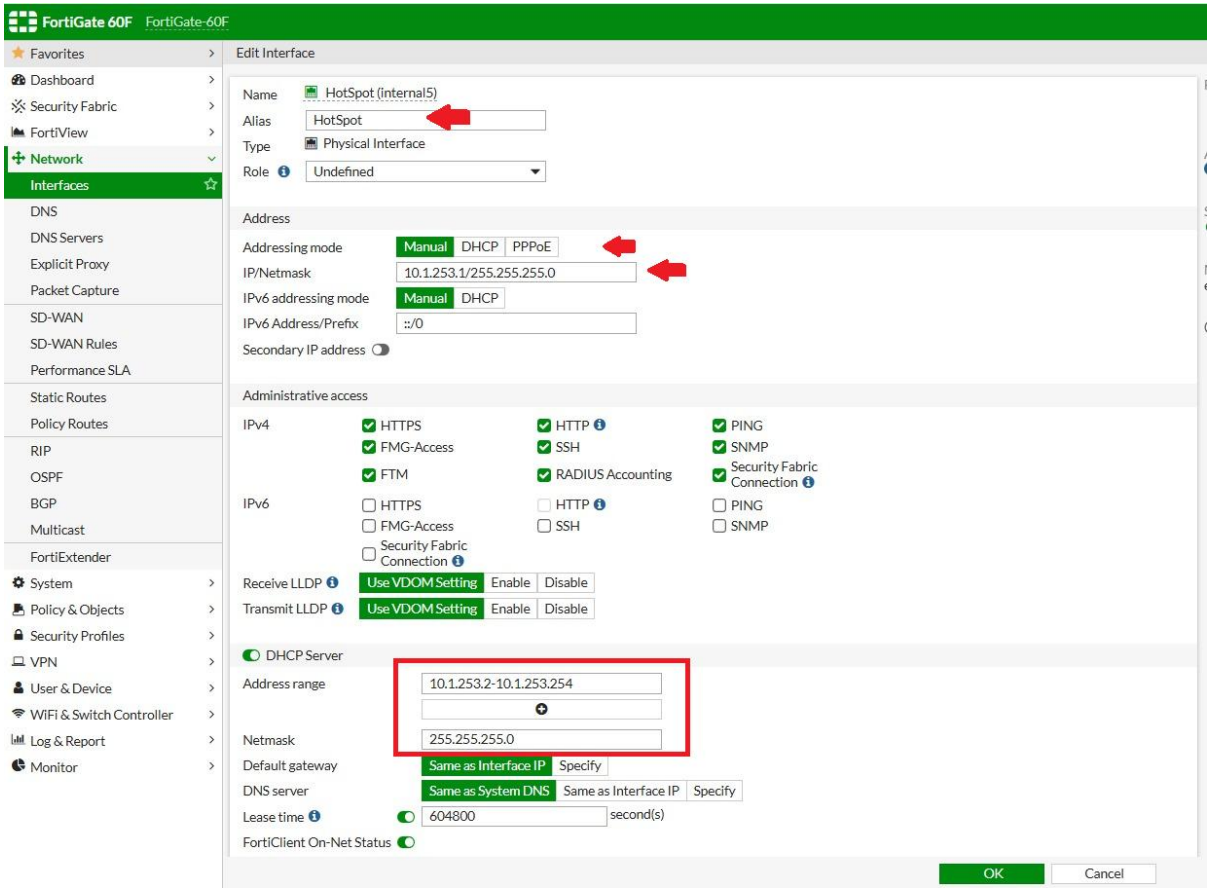
Network – Interface menüsüne gidin

HotSpot yayını yapacağınız interface'i düzenleyiniz

Alias bölümüne bir takma ad giriniz

Address bölümüne hotspot yayınında kullanmak istediğiniz ip ve netmask bilgilerini giriniz

DHCP Server bölümünde hotspot ip aralığınızı belirtiniz



Network kısmından

Security Mode'u aktif hale getirin ve Captive Portal'ı seçin

Authentication Portal'ı External olarak seçiniz

URL olarak http://ThreatChaserIPAdresi:PortNumarası/auth değerini giriniz

User Access'i Restricted to Groups olarak seçiniz

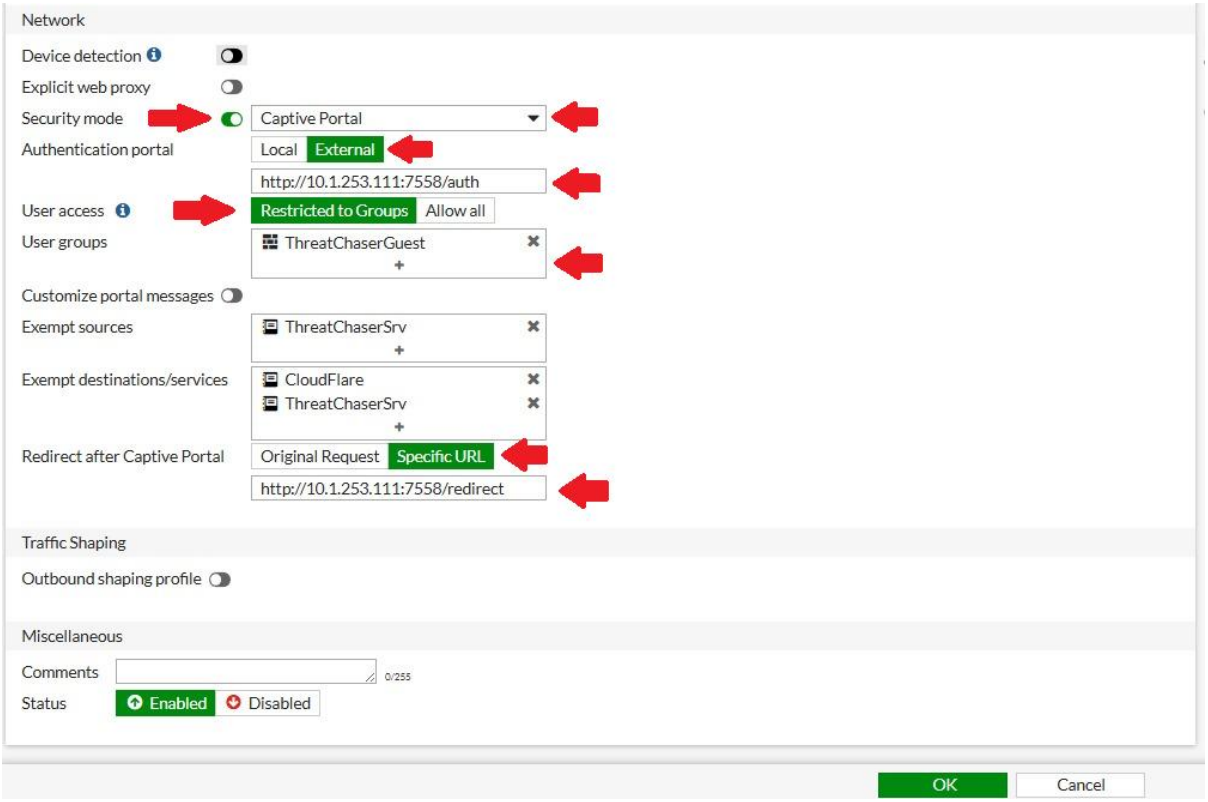
User Group kısmına daha önceden oluşturduğumuz grubu seçiniz

Exempt sources bölümünde threatchaser ürününün internete çıkabilmesi için izin verin

Exempt destinations/services ise eğer threatchaser ürünü farklı bir ağda ise hotspot ağındaki cihazların thraetchaser'a erişebilmesi için bu bölüme eklemeniz gerekmektedir

Redirect after Captive Portal kısmından "Specific URL" seçiniz

URL olarak http://ThreatChaserIPAdresi:PortNumarası/redirect değerini giriniz

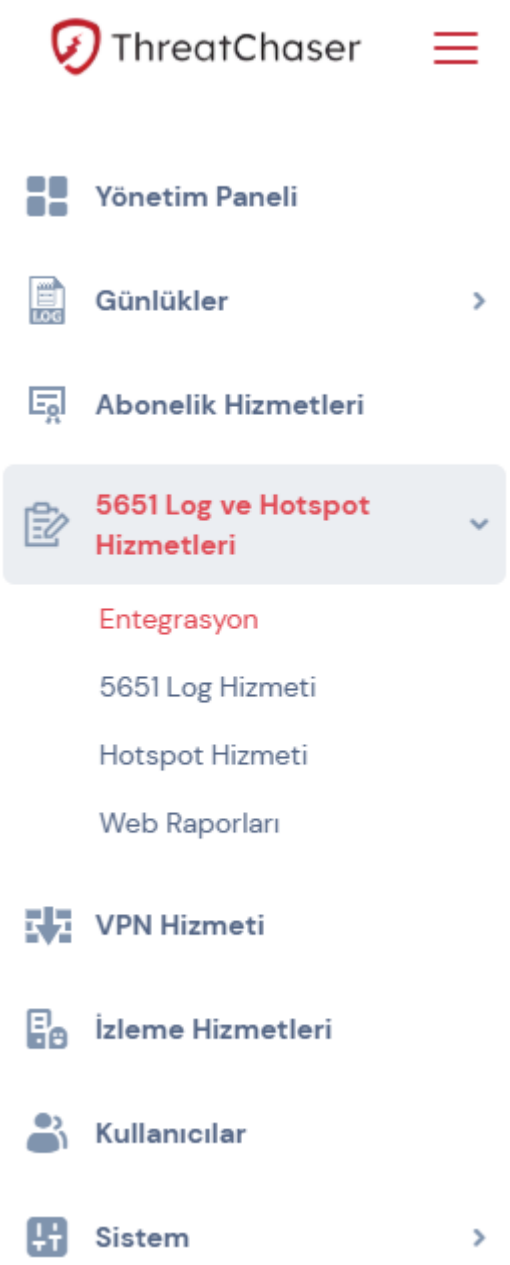


Sophos Cihazımdanda HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim?

ThreatChaser Tarafındaki Ayarlamalar

ThreatChaser'a web arayüzü üzerinden erişim sağlayınız

5651 Log ve Hotspot Hizmetleri -> Entegrasyon sayfasına gidin

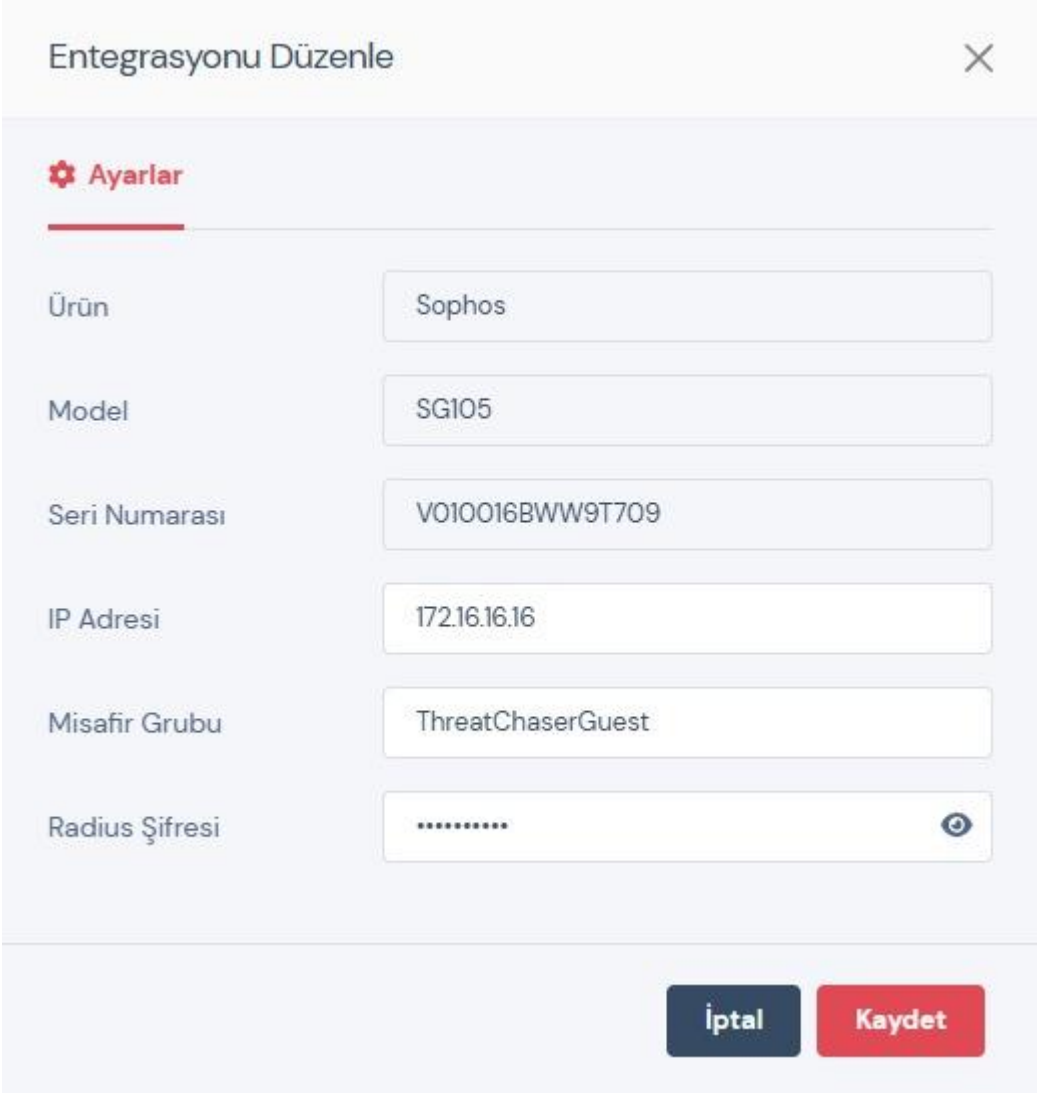


Entegrasyon yapacağınız firewall için düzenleme simgesine tıklayınız.

“IP Adresi” bölümüne Sophos’un ip adresini giriniz.

“Misafir Grubu” Bu bölümün Authentication -> Groups menüsüne eklediğiniz isimle aynı olması gerekiyor.

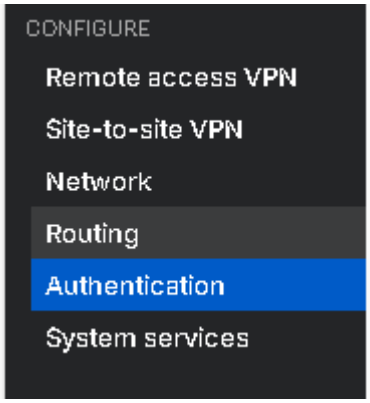
“Radius Şifresi” Bu bölüme Sophos’un ThreatChaser ile iletişime geçebilmesi için bir şifre oluşturmanız gerekiyor.



Firewall Tarafındaki Ayarlamalar

Sophos Cihazınıza Web Arayüzü üzerinden giriş yapın

Configure -> Authentication sayfasına gidin



“Add” Butonuna tıklayın

“Group Name” bölümüne ThreatChaser’da girdiğiniz misafir grubu adını girin.

“Group Type” bölümünü Normal olarak seçin

“Surfing quota” bölümünü “Unlimited Internet Access” olarak seçin. Eğer bir sınırlama yapmak isterseniz bu bölümden belirtebilirsiniz.

“Access time” bölümünü “Access Time” olarak seçin. Eğer bir sınırlama yapmak isterseniz bu bölümden belirtebilirsiniz.

“SSL VPN policy“ bölümünü “No policy applied” olarak seçin

“Clientless SSL VPN policy” bölümünü “No policy applied” olarak seçin

“L2TP” bölümünü “Disable” olarak seçin

“PPTP” bölümünü “Disable” olarak seçin

“Quarantine digest“ bölümünü “Enable” olarak seçin

“Quarantine digest” bölümünü “Any node” olarak seçin

Authentication

Servers | Services | Groups | Users | Multi

Group name *: ThreatChaserGuest

Description: Description

Group type *: Normal

Policies

Surfing quota *: Unlimited Internet Access

Access time *: Allowed all the time

Network traffic: None

Traffic shaping: None

VPN

SSL VPN policy *: No policy applied

Clientless SSL VPN policy *: No policy applied

L2TP *: Enable / Disable

PPTP *: Enable / Disable

Other settings

Quarantine digest *: Enable / Disable

MAC binding: Enable / Disable

IPsec remote access *: Enable / Disable

Save | Cancel

“**Authentication -> Servers**” sayfasına gidin

Add butonuna tıklayın

Server Type bölümünü **RADIUS Server** olarak seçin

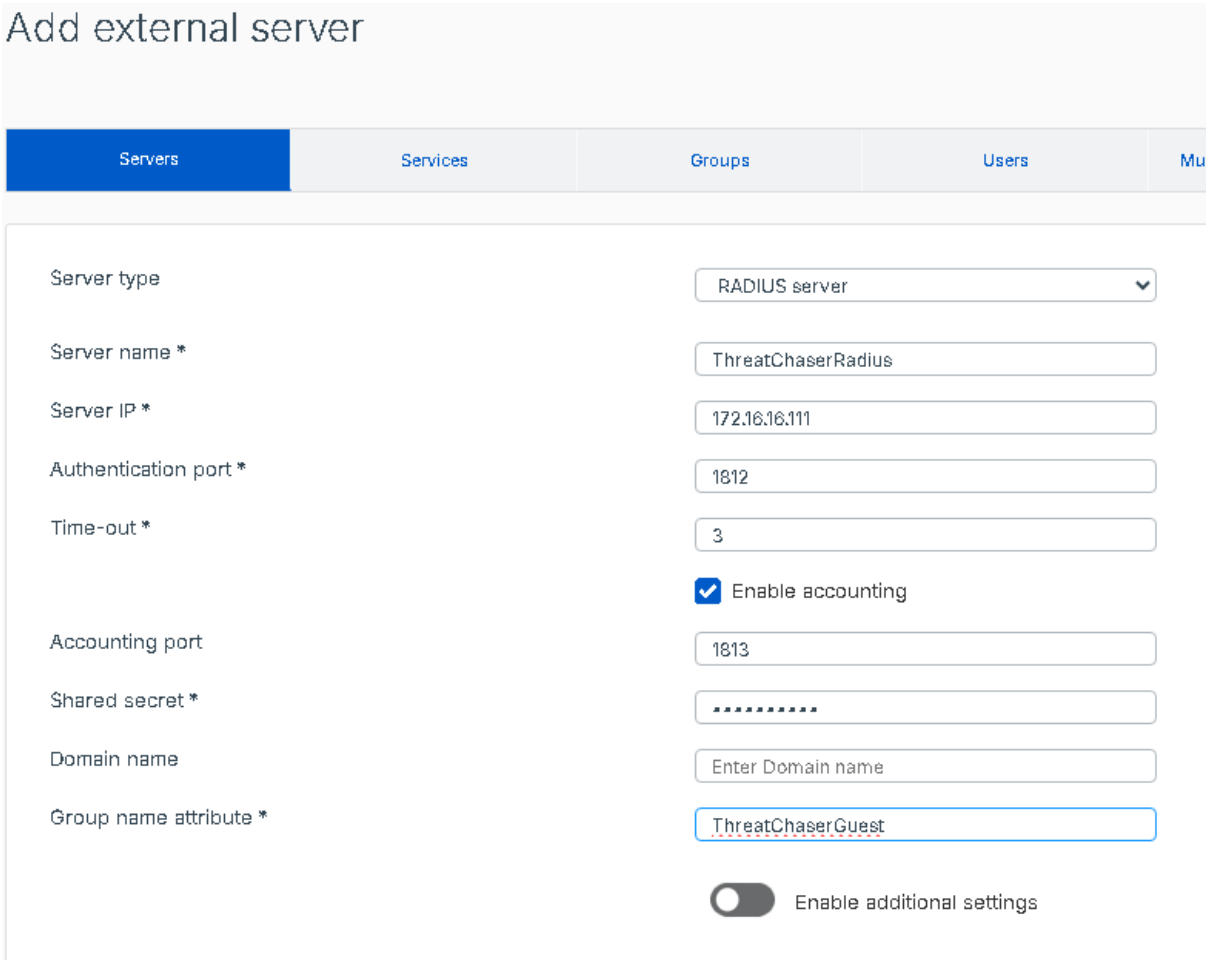
Server IP bölümüne **ThreatChaser’ın ip adresini** giriniz

Authentication port bölümünü **1812** olarak giriniz

Accounting Port bölümünü **1813** giriniz

Shared secret bölümünü **ThreatChaser’da girdiğiniz Radius şifresini** giriniz

Group name attributes bölümünü **ThreatChaser’da girdiğiniz Misafir Grubu Adı** ile aynı giriniz



“**Authentication -> Services**” sayfasına gidin

Oluşturduğunuz Radius Server’ı seçin

“**Authentication -> Web Authentication**” sayfasına gidin

“Show user portal link” ve “Show web page after sign-in” işaretini kaldırın

Captive portal appearance bölümünü **Custom HTML** olarak işaretleyin

Aşağıdaki metinde cihazın ip adresini ve portunu düzenleyerek **Custom HTML** sayfasına yapıştırınız

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="pragma" content="no-cache" />
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta http-equiv="expires" content="-1" />
</head>
<body>
<h3>Yönlendiriliyorsunuz lütfen bekleyiniz...</h3>
   <script>location.href =
"http://172.16.16.111:7561/auth?post="+window.location.hostname</script>
</body>
</html>
```

“**Protect -> Rules and Policies**” sayfasına gidin

Add Firewall Rule -> New firewall rule butonuna tıklayın

Action bölümünü “Accept” olarak seçin

Rule Position bölümünü “Top” olarak seçin

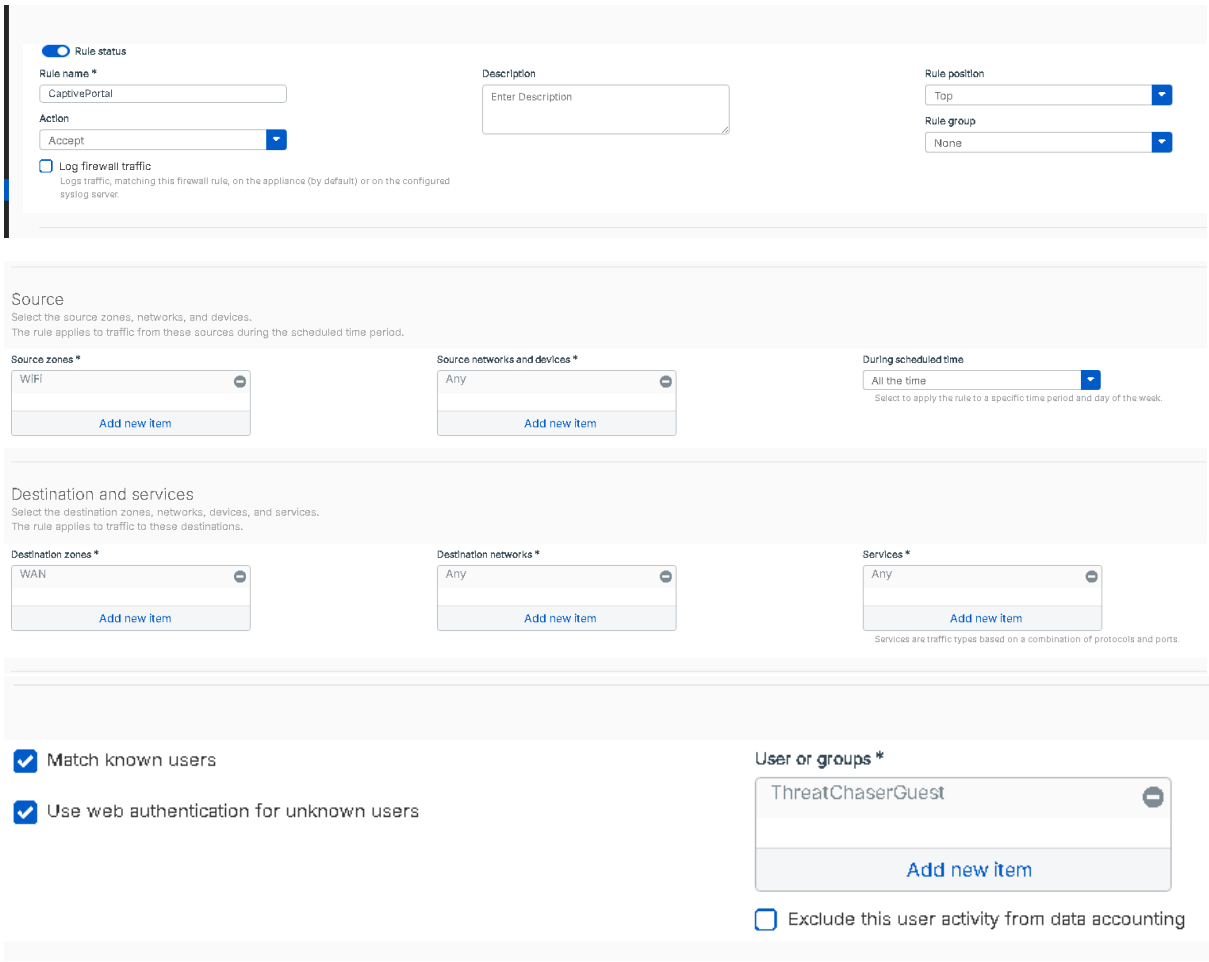
Source Zones Hotspot yayını yapacağınız interface’i seçin

Destination Zones hotspot interface’inin hangi internetten çıkmasını istiyorsanız onu seçiniz

Match known users bölümünü işaretleyin

Use web authentication for unkown users bölümünü işaretleyin

User or groups bölümüne ThreatChaser’da girdiğiniz misafir grubu adını girin.



“**Protect -> Rules and Policies**” sayfasına gidin

Add Firewall Rule -> New firewall rule butonuna tıklayın

Action bölümünü “Accept” olarak seçin

Rule Position bölümünü “Top” olarak seçin

Source Zones Hotspot yayını yapacağınız interface’i seçin

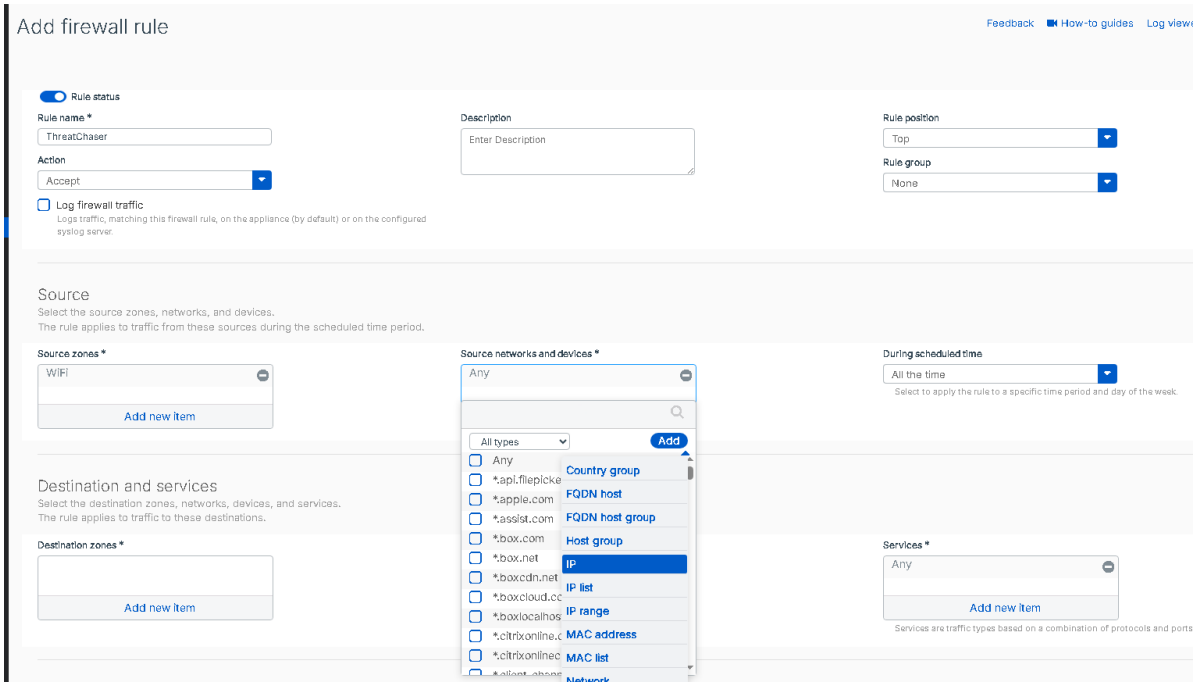
Source networks and devices bölümüne ThreatChaser’ın ip adresini girin

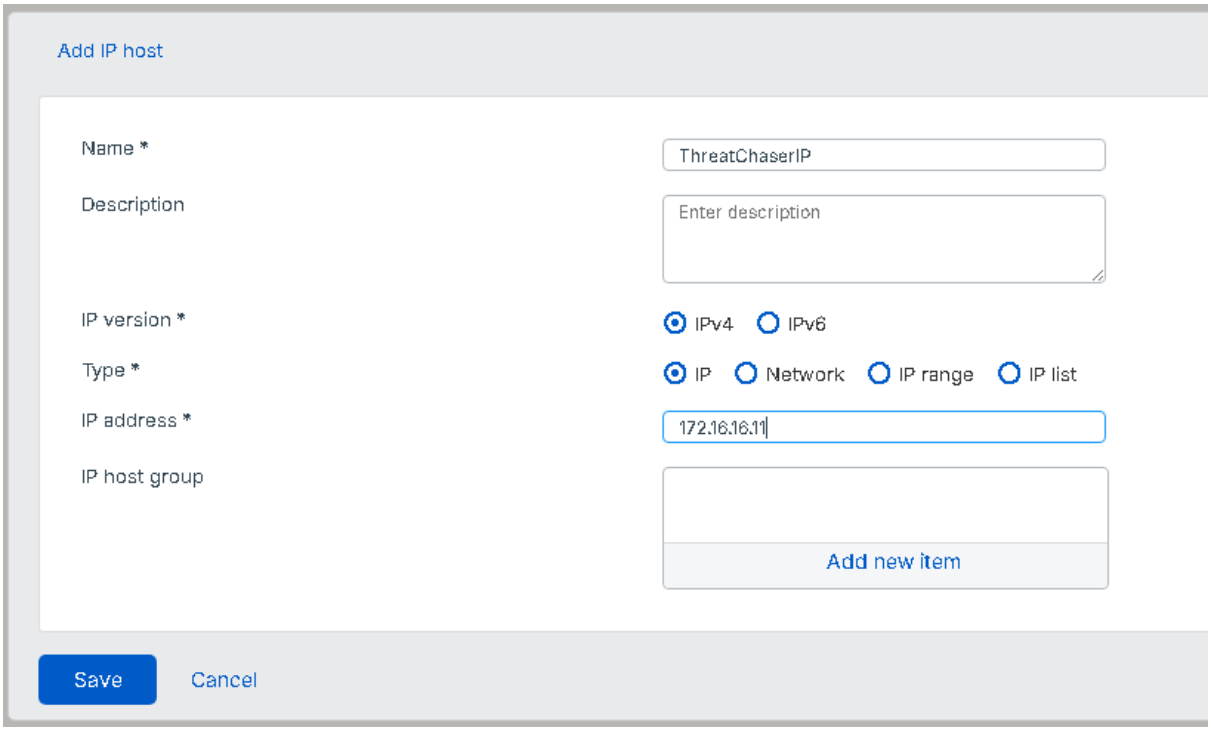
Destination Zones ThreatChaser’ın hangi internetten çıkmasını istiyorsanız onu seçiniz

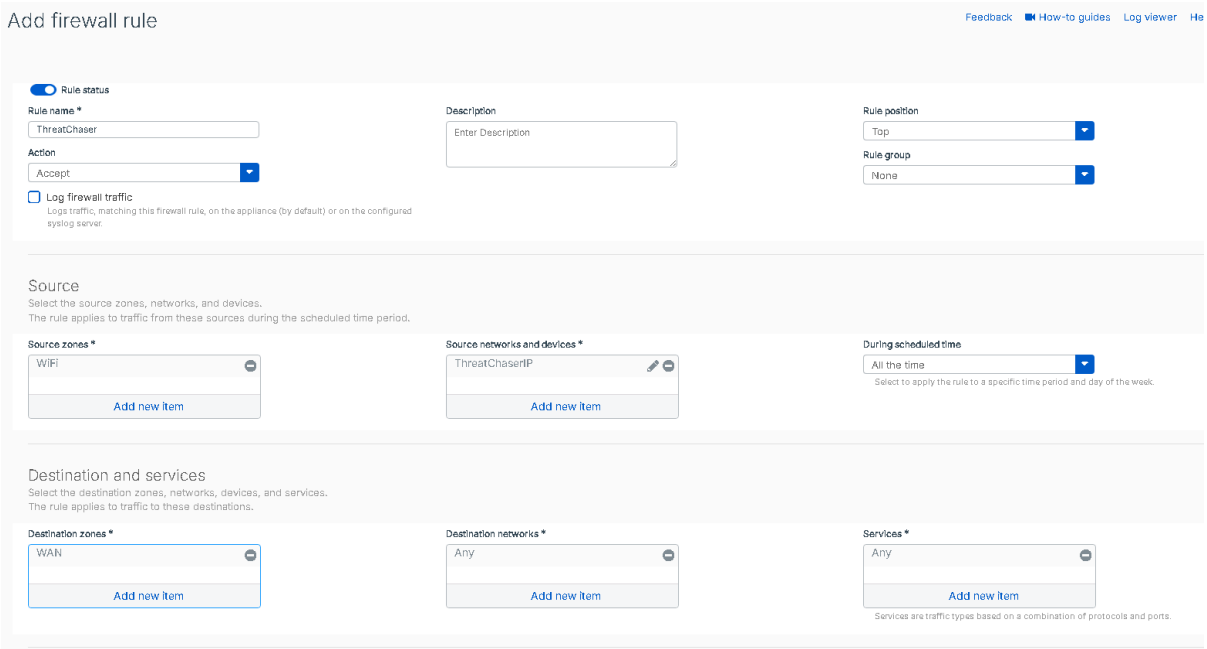
Match known users bölümünü işaretleyin

Use web authentication for unkown users bölümünü işaretleyin

User or groups bölümüne ThreatChaser’da girdiğiniz misafir grubu adını girin.




Add IP host
Name *
ThreatChaserIP
Description
Enter description
IP version *
IPv4
IPv6
Type *
IP
Network
IP range
IP list
IP address *
172.16.16.11
IP host group
Add new item
Save
Cancel

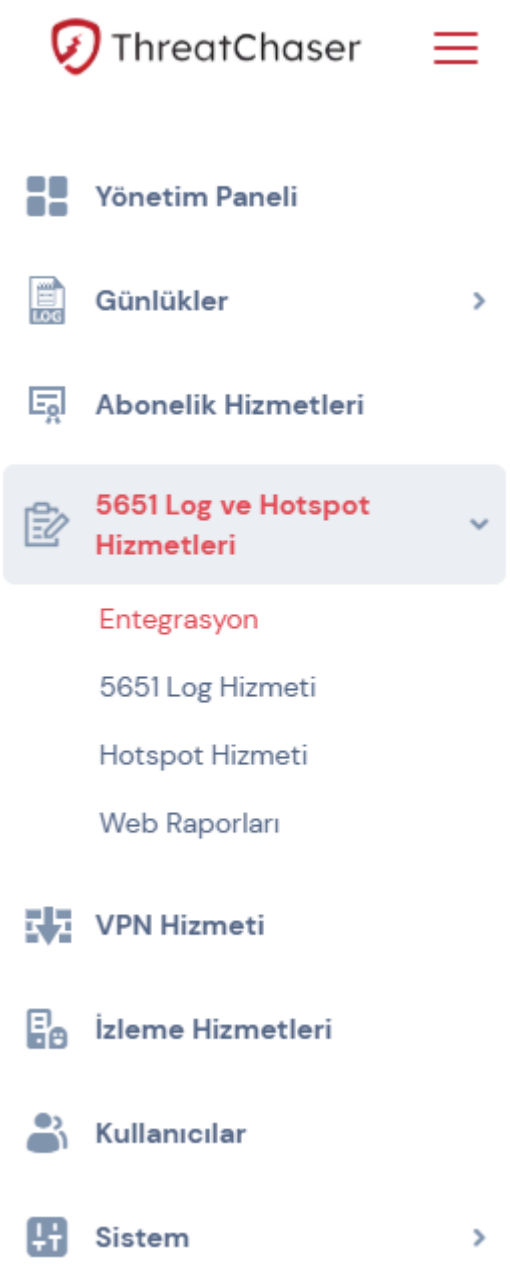

Add firewall rule
Feedback
How-to guides
Log viewer
Rule status
Rule name *
ThreatChaser
Action
Accept
Log firewall traffic
Logs traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.
Description
Enter Description
Rule position
Top
Rule group
None
Source
Select the source zones, networks, and devices.
The rule applies to traffic from these sources during the scheduled time period.
Source zones *
WiFi
Add new item
Source networks and devices *
ThreatChaserIP
Add new item
During scheduled time
All the time
Select to apply the rule to a specific time period and day of the week.
Destination and services
Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.
Destination zones *
WAN
Add new item
Destination networks *
Any
Add new item
Services *
Any
Add new item
Services are traffic types based on a combination of protocols and ports.

AIMdefense Cihazımdanda HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim?

ThreatChaser Tarafındaki Ayarlamalar

ThreatChaser'a web arayüzü üzerinden erişim sağlayınız

5651 Log ve Hotspot Hizmetleri -> Entegrasyon sayfasına gidin



Entegrasyon yapacağınız firewall için düzenleme simgesine tıklayınız.

IP Adresi bölümüne AIMdefense'ın ip adresini giriniz.

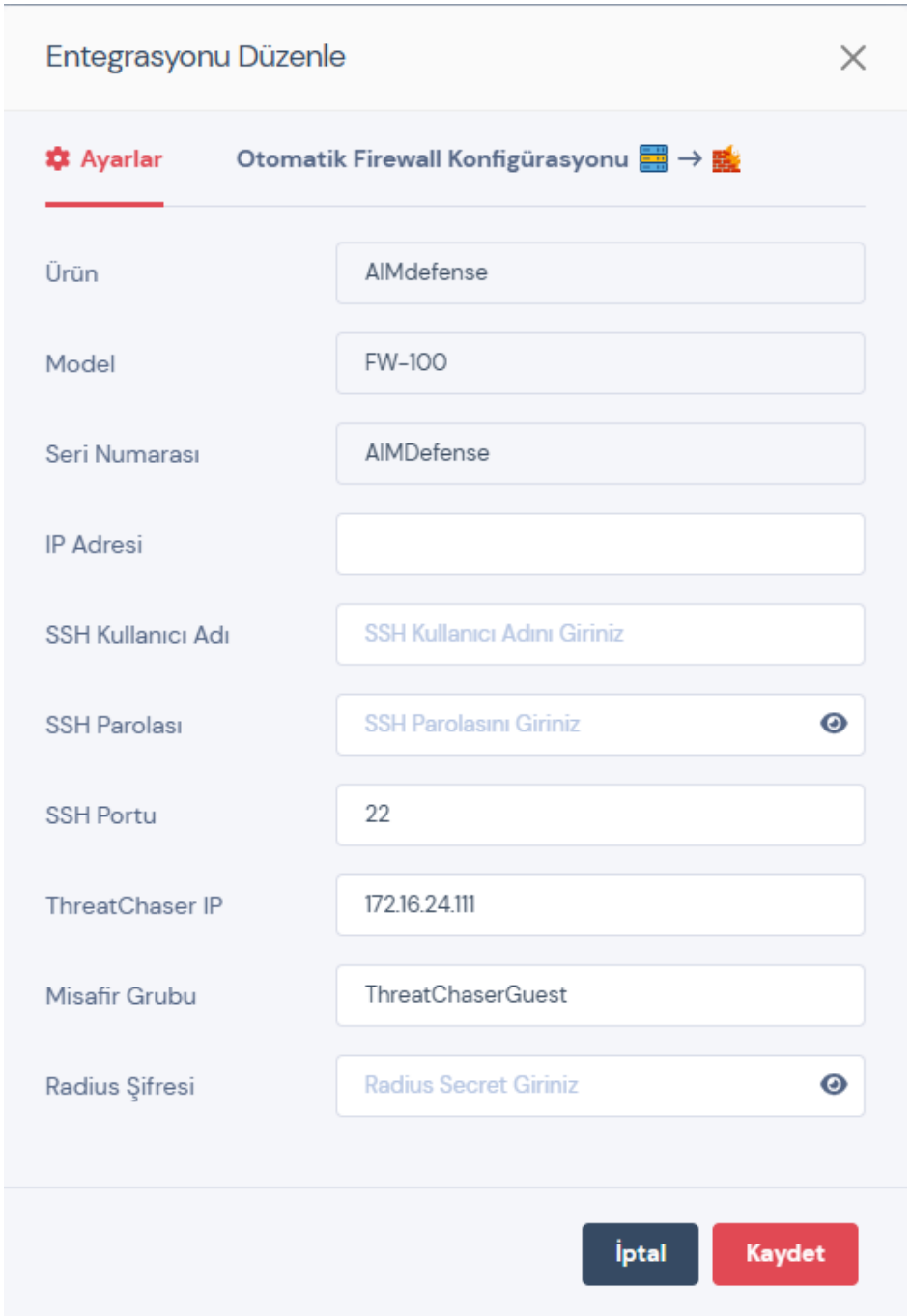
SSH Kullanıcı Adı bölümüne AIMdefense'ın SSH kullanıcı adını giriniz

SSH Parolası bölümüne AIMdefense'ın SSH parolasını giriniz

SSH Portu bölümüne AIMdefense'ın SSH portunu giriniz

ThreatChaser IP alanına, ThreatChaser'ın IP adresini giriniz. Eğer bulunduğunuz lokasyonda ürüne dışarıdan port yönlendirmesi ile erişiyorsanız, bu alana cihazın iç IP adresini yazmanız gerekmektedir.
Misafir Grubu Bu bölümün AIMdefense tarafında oluşturduğunuz grup ismi ile aynı olması gerekiyor

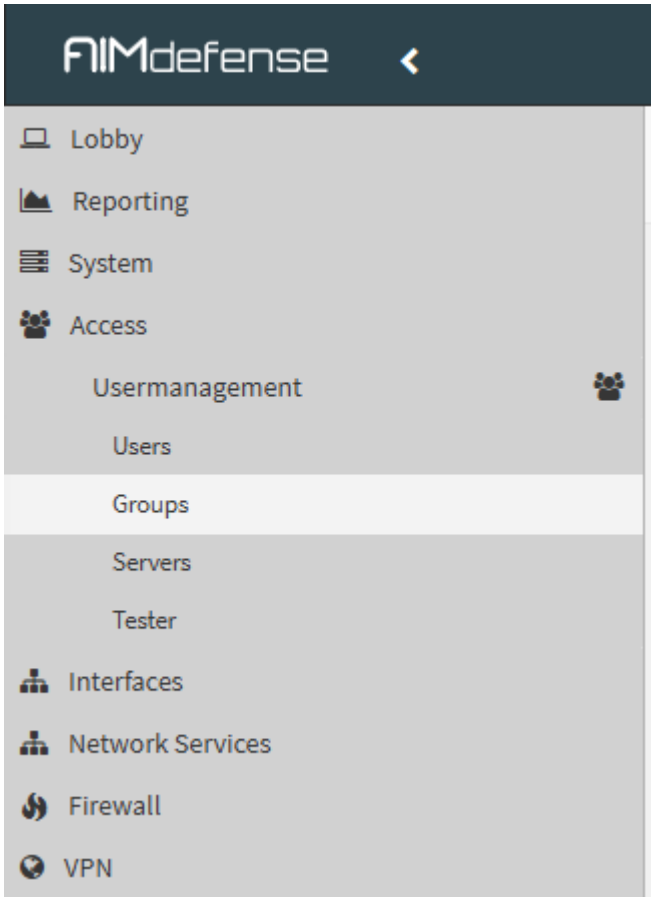
Radius Şifresi Bu bölüme AIMdefense'ın ThreatChaser ile iletişime geçebilmesi için bir şifre oluşturmanız gerekiyor.



Firewall Tarafındaki Ayarlamalar

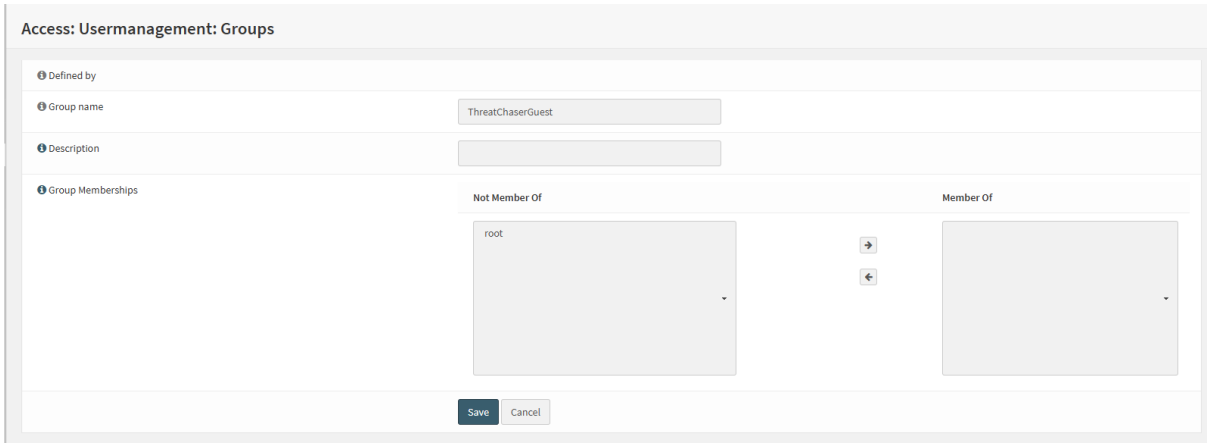
AIMdefense Cihazınıza Web Arayüzü üzerinden giriş yapın

Access -> Groups sayfasına gidin

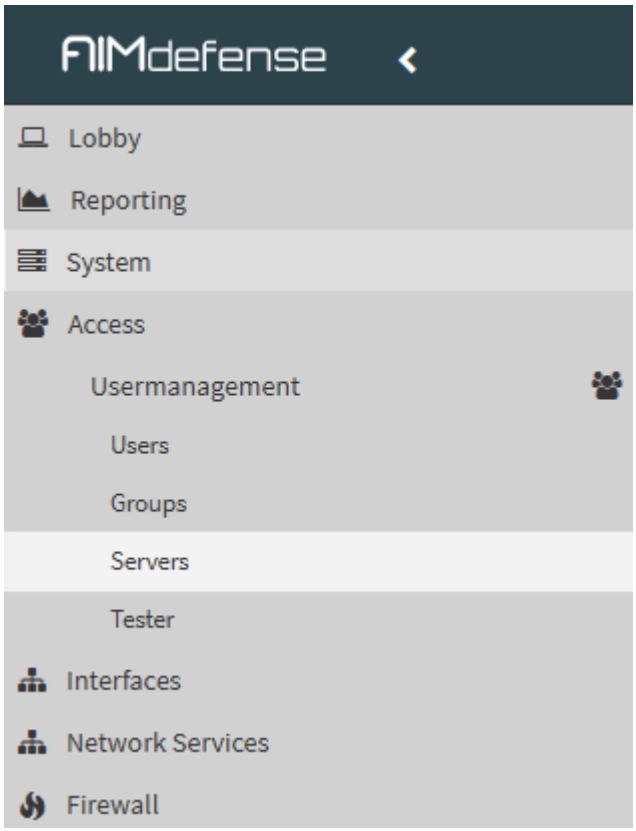


Add Butonuna tıklayın

Group Name bölümüne ThreatChaser'da girdiğiniz misafir grubu adını girin.



Access -> Servers sayfasına gidin



Add Butonuna tıklayın

Type bölümünü **RADIUS** olarak seçin

Hostname or IP Address bölümüne **ThreatChaser'ın ip adresini** giriniz

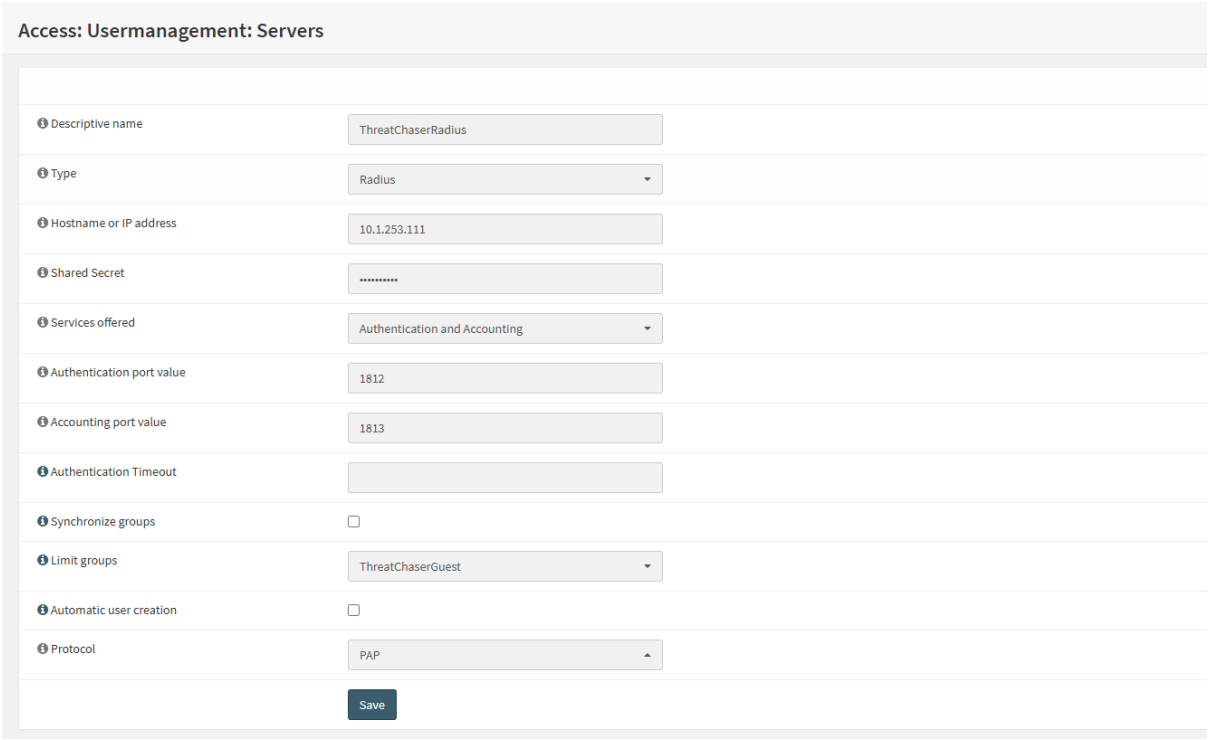
Shared secret bölümünü **ThreatChaser'da girdiğiniz Radius şifresini** giriniz

Authentication port value bölümünü **1812** olarak giriniz

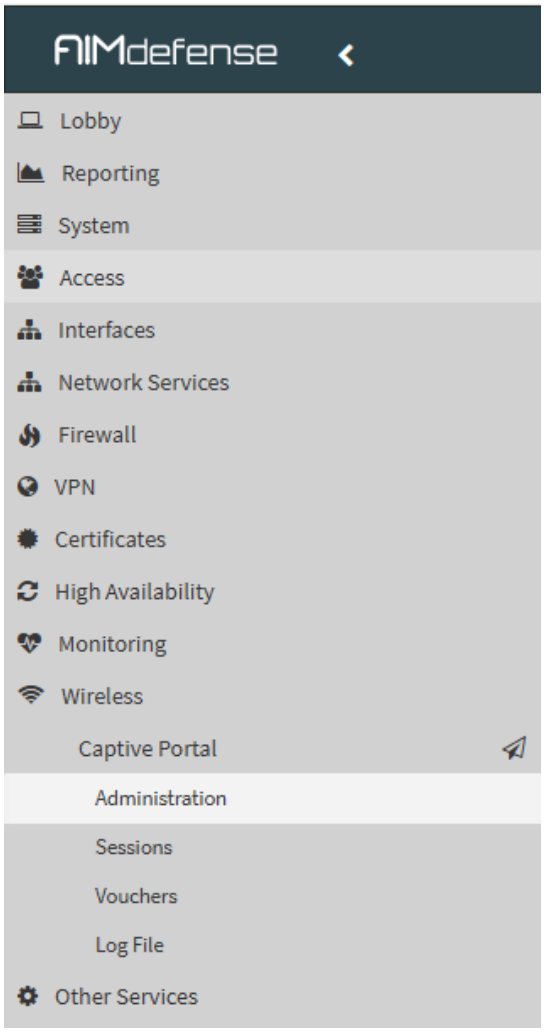
Accounting Port value bölümünü **1813** giriniz

Limit groups bölümünden **daha önceden oluşturduğunuz Radius grubunuzu** seçin

Protocol bölümünü **PAP** olarak seçiniz



Wireless -> Administration sayfasına gidin



Add Butonuna tıklayın

Enabled bölümünü **işaretleyin**

interface bölümünde **Misafir yayını yapmak istediğiniz ağ arayüzünü** giriniz

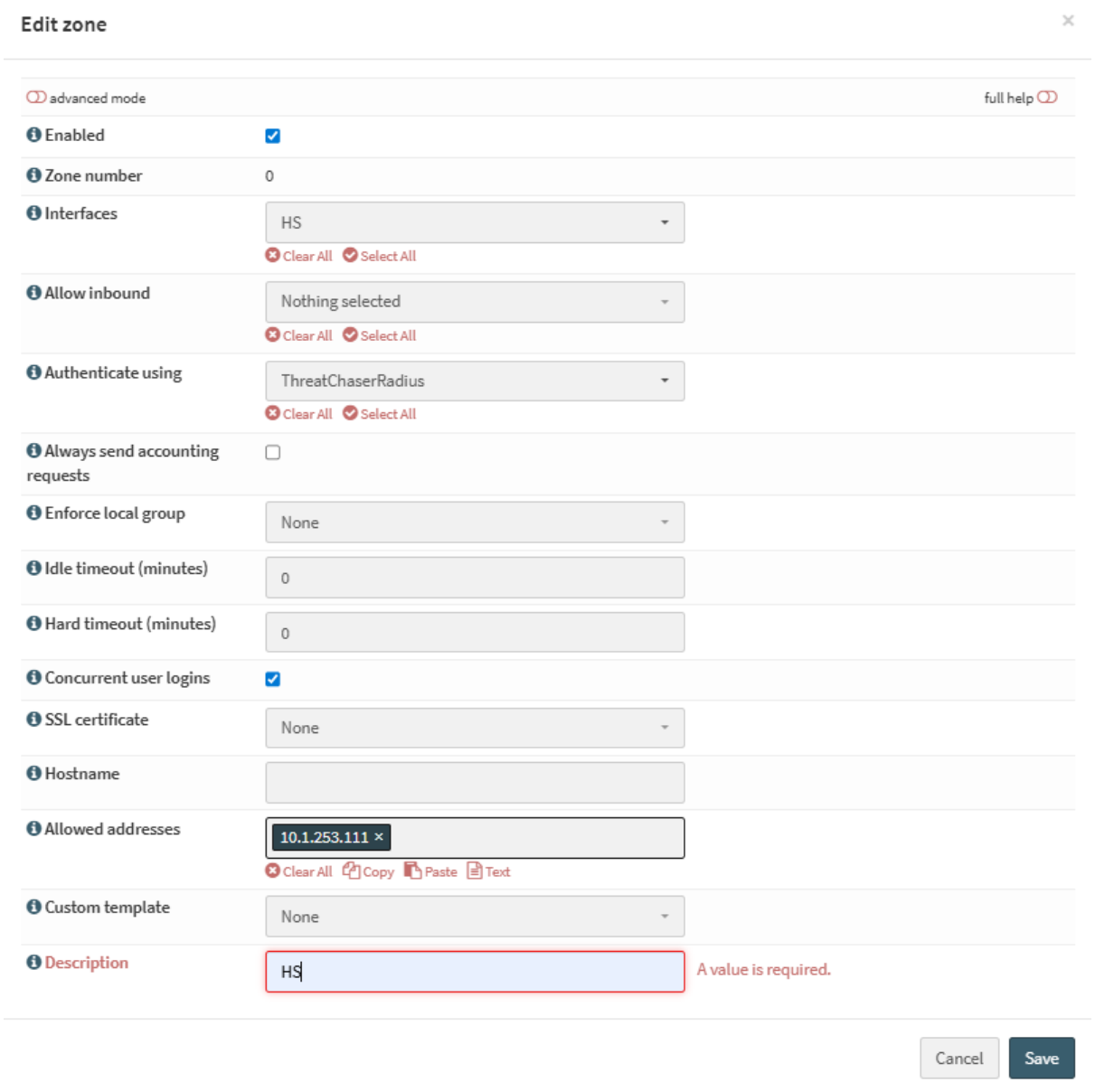
Authenticate using bölümünde **önceden oluşturduğunuz Radius server'ı** giriniz

Concurrent user logins bölümünü **işaretleyin**

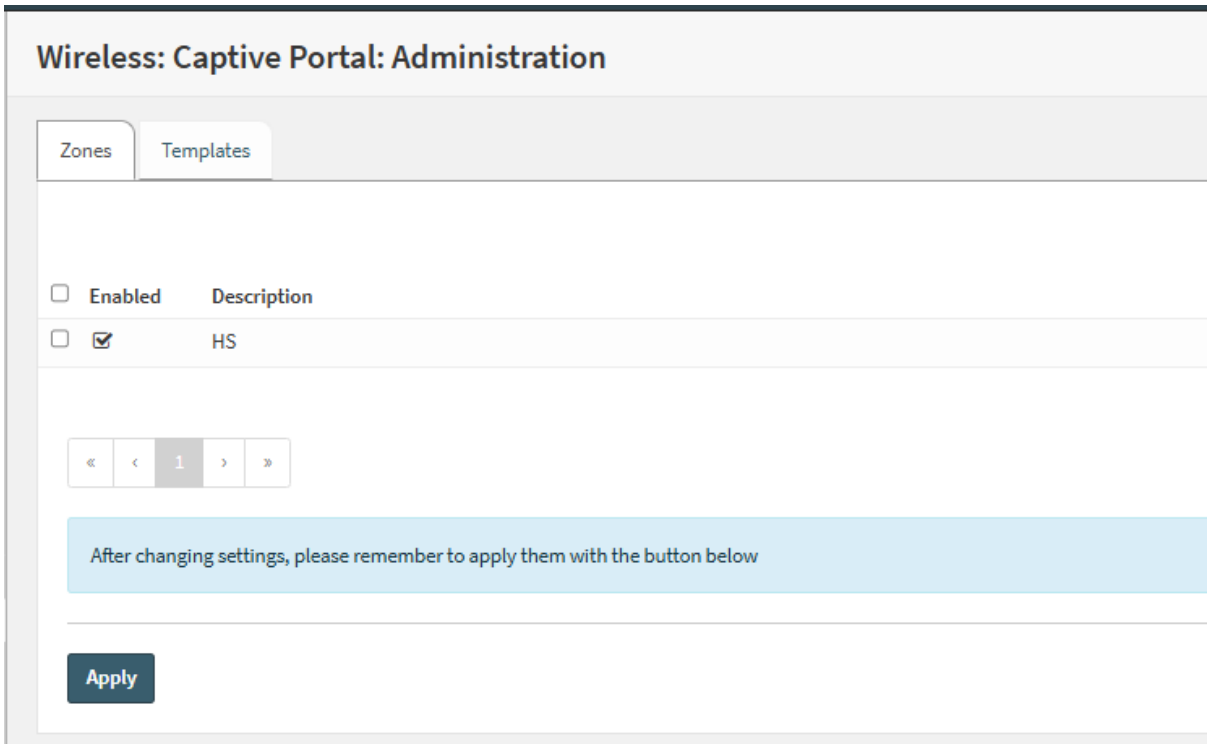
Allowed addresses bölümüne **ThreatChaser'ın ip adresini giriniz**

Description bölümünde Misafir yayınınıza isim verin

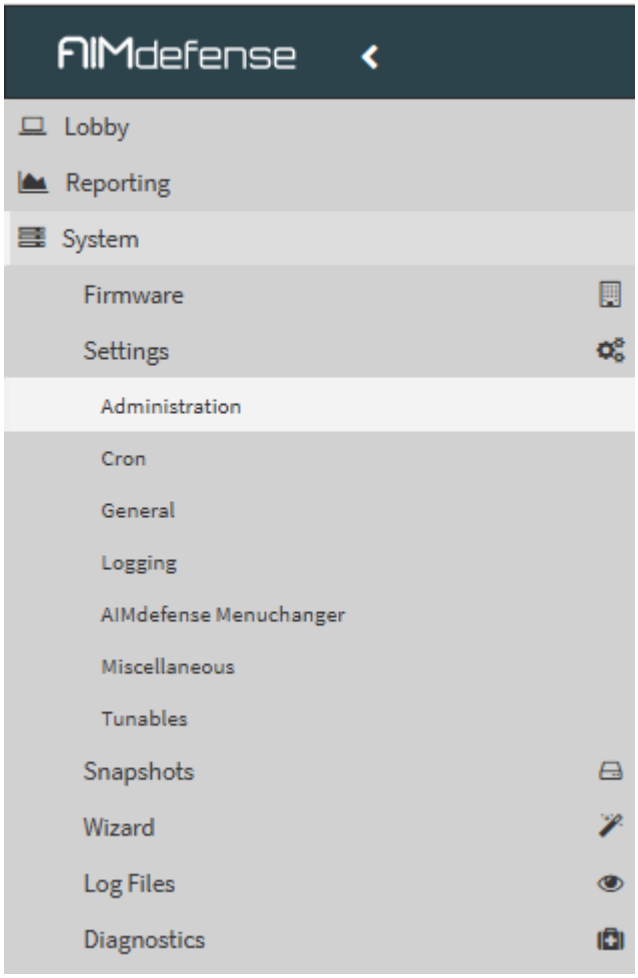
Save butonuna tıklayın



Apply diyerek ayarlarınızı kaydedin



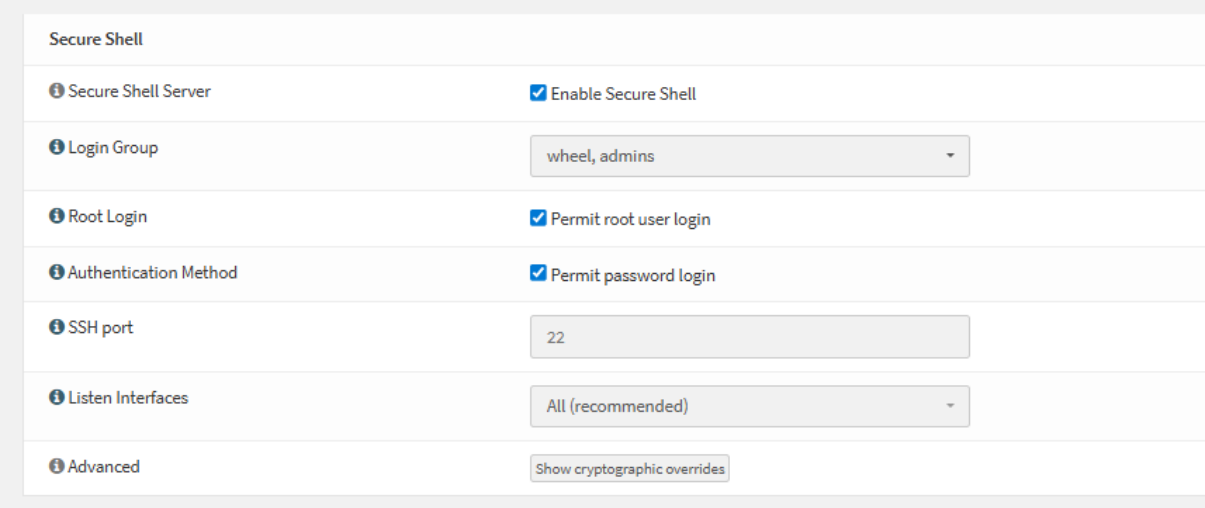
System -> Administration sayfasına gidin



Secure Shell Server bölümünü **işaretleyin**

Root Login bölümünde **Permit root user login'i** işaretleyin

Authentication Method bölümünden **Permit password login'i** işaretleyin

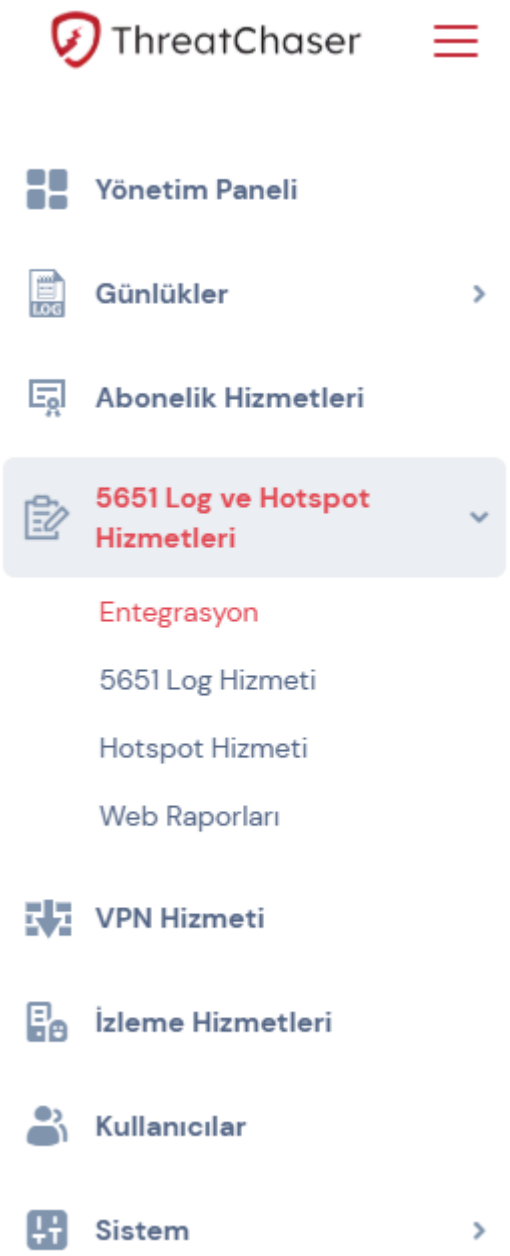


Ruijie Cihazımdanda HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim?

ThreatChaser Tarafındaki Ayarlamalar

ThreatChaser'a web arayüzü üzerinden erişim sağlayınız

5651 Log ve Hotspot Hizmetleri -> Entegrasyon sayfasına gidin

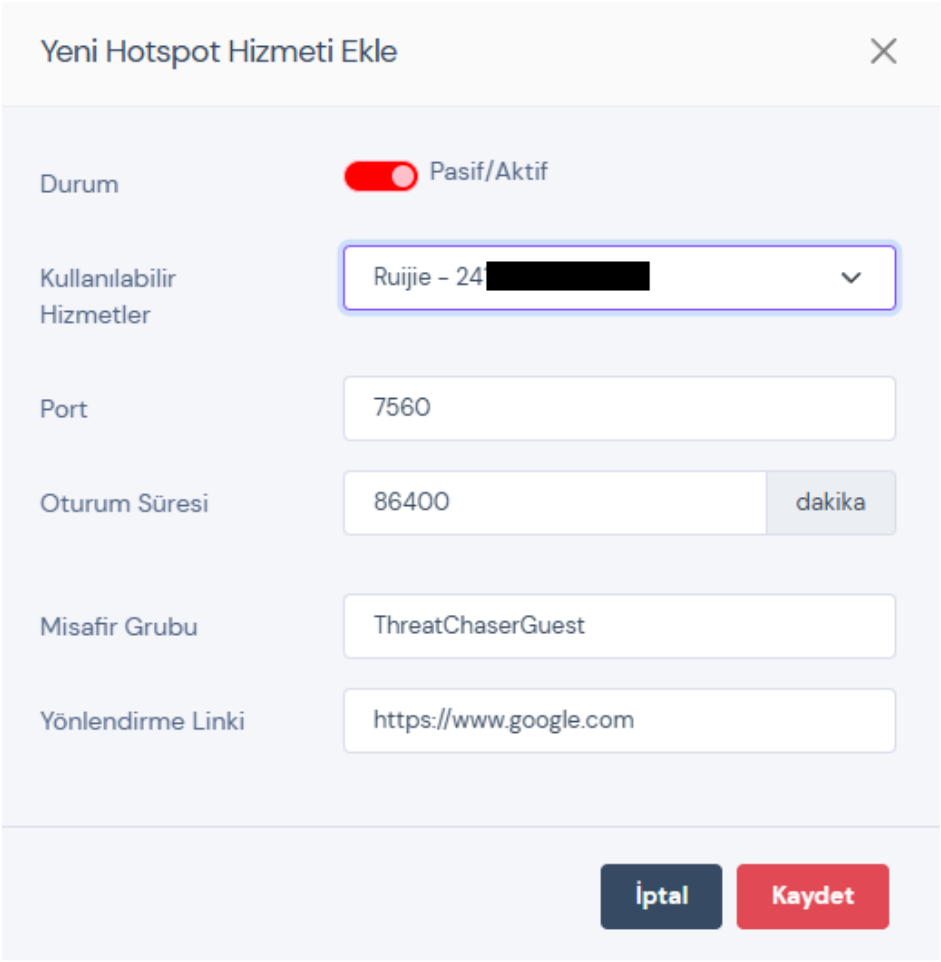


Entegrasyon yapacağınız firewall için düzenleme simgesine tıklayınız.

Misafir Grubu Bu bölümün Ruijie tarafında oluşturduğunuz grup ismi ile aynı olması gerekiyor

Port bölümüne HotSpot port numarasını giriniz.

Yönlendirme Linki bölümüne, giriş yaptıktan sonra kullanıcıların yönlendirilmesini istediğiniz adresi giriniz.

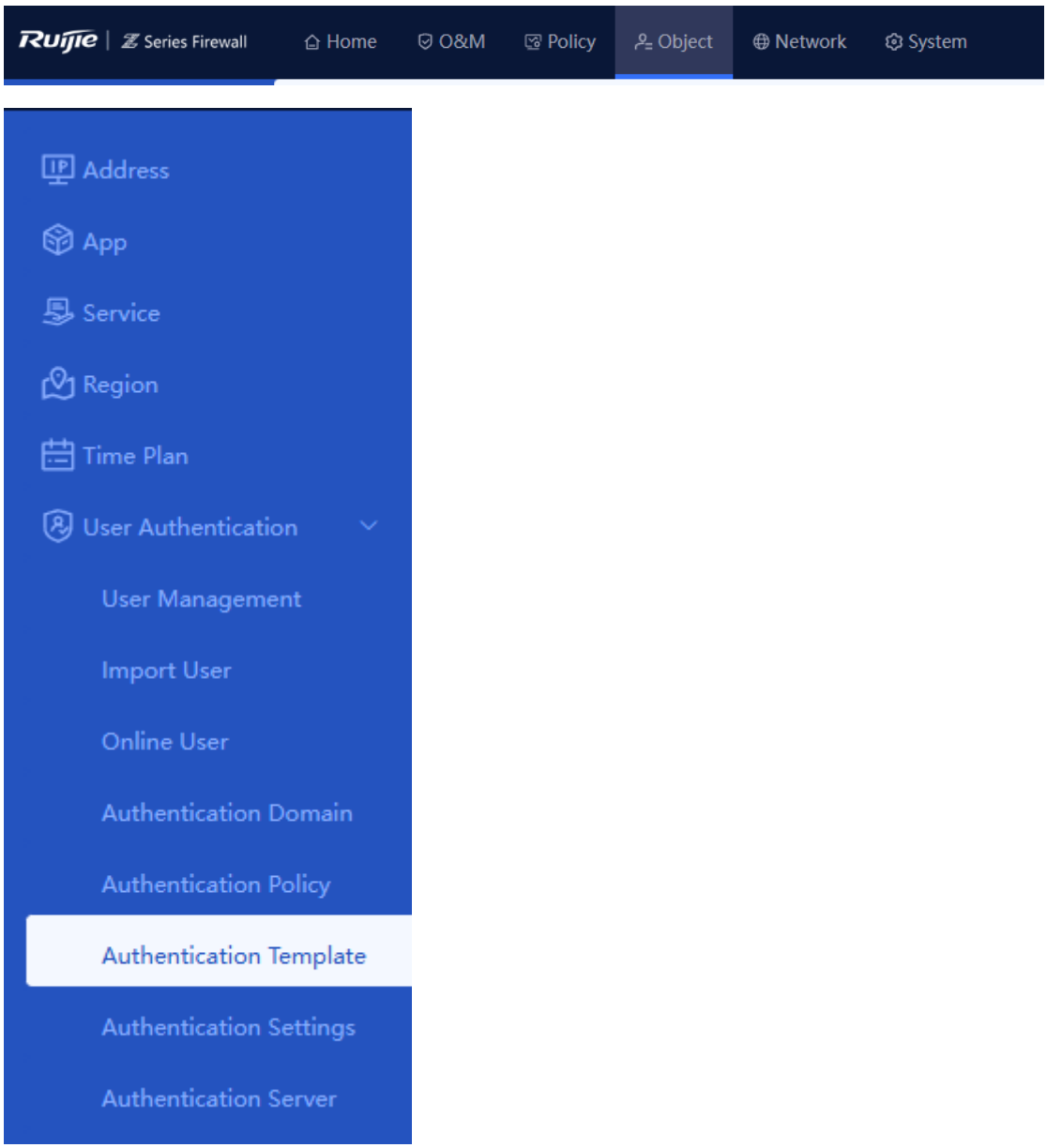


Firewall Tarafındaki Ayarlamalar

Ruijie Cihazınıza Web Arayüzü üzerinden giriş yapın

Cihazınızın en son sürümde olduğundan emin olun; sürümler arasındaki ekranlar farklılık gösterebilir.

Object -> Authentication Template sayfasına gidin



External Portal bölümünden **WiFiDog Authentication'ı** etkinleştirin

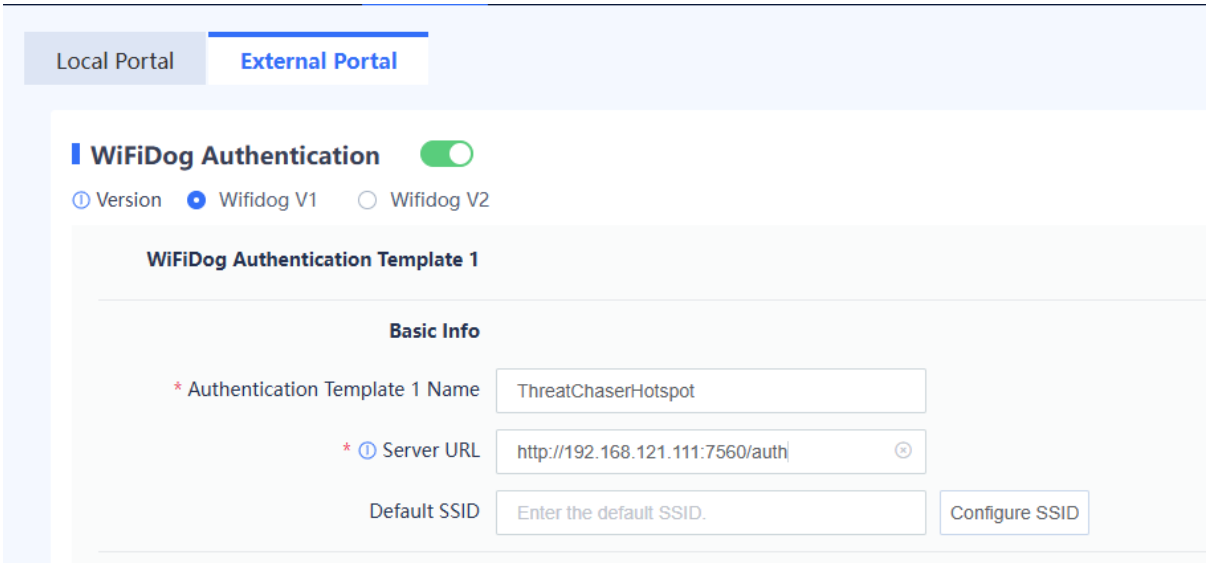
Wifidog V1'i seçin

Authentication Teplate bölümüne bir isim girin

Server URL bölümünde aşağıdaki örnekteki bilgileri kendi değerlerinizle değiştirerek giriniz

http://threatchaser_ip_adresi:threatchaser_hotspot_port_numarası/auth

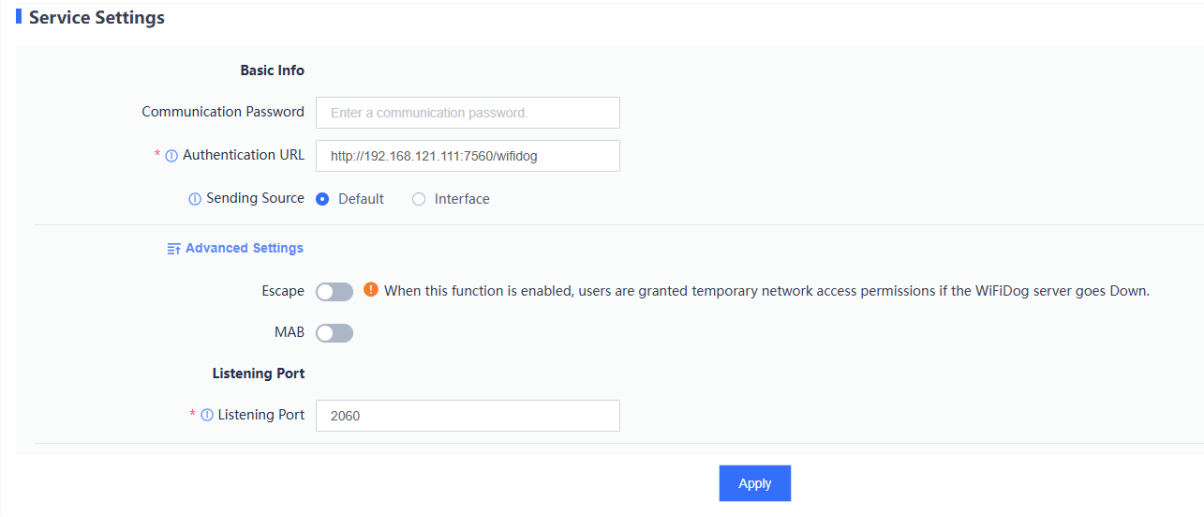
(Örn: http://192.168.1.111:7560/auth)



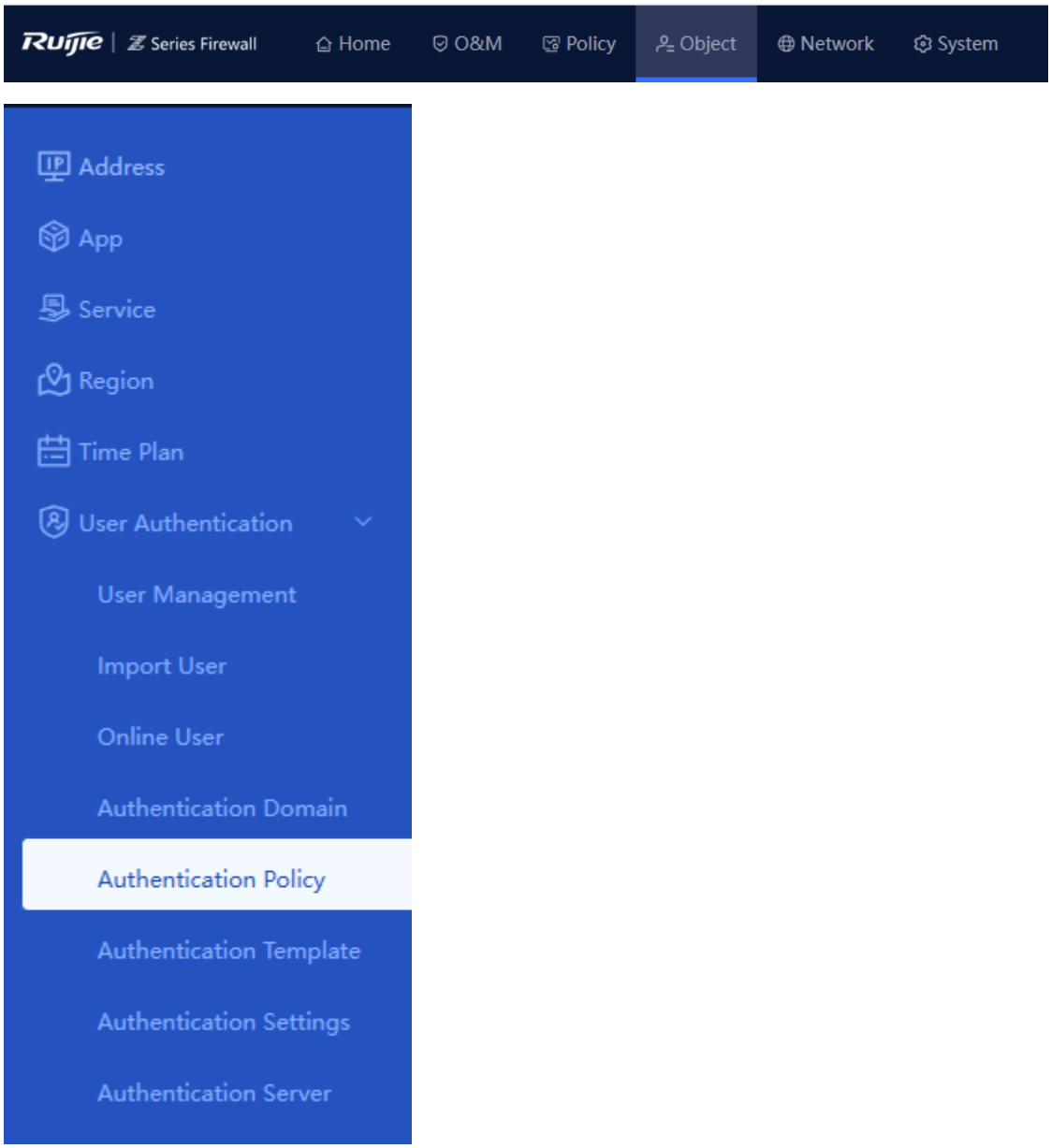
Authentication URL bölümünde aşağıdaki örnekteki bilgileri kendi değerlerinizle değiştirerek giriniz

http://threatchaser_ip_adresi:threatchaser_hotspot_port_numarası/wifidog

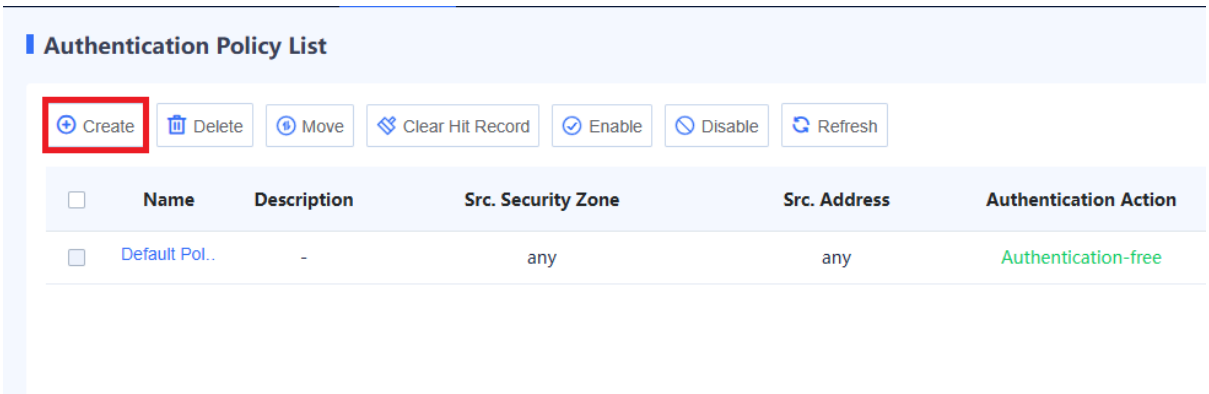
(Örn: http://192.168.1.111:7560/wifidog)



Object -> Authentication Policy sayfasına gidin



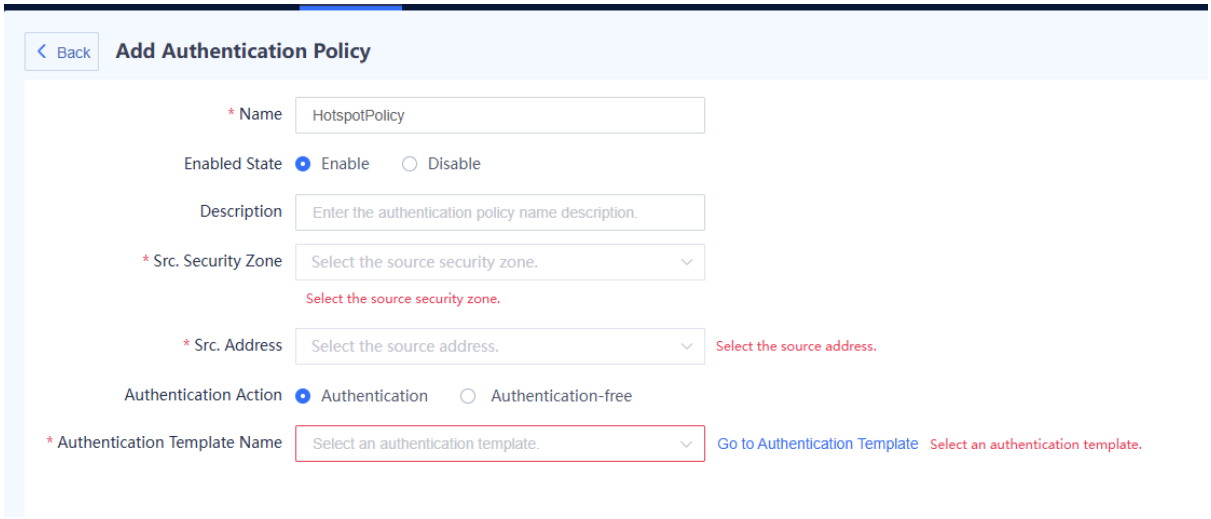
Create Butonuna tıklayın

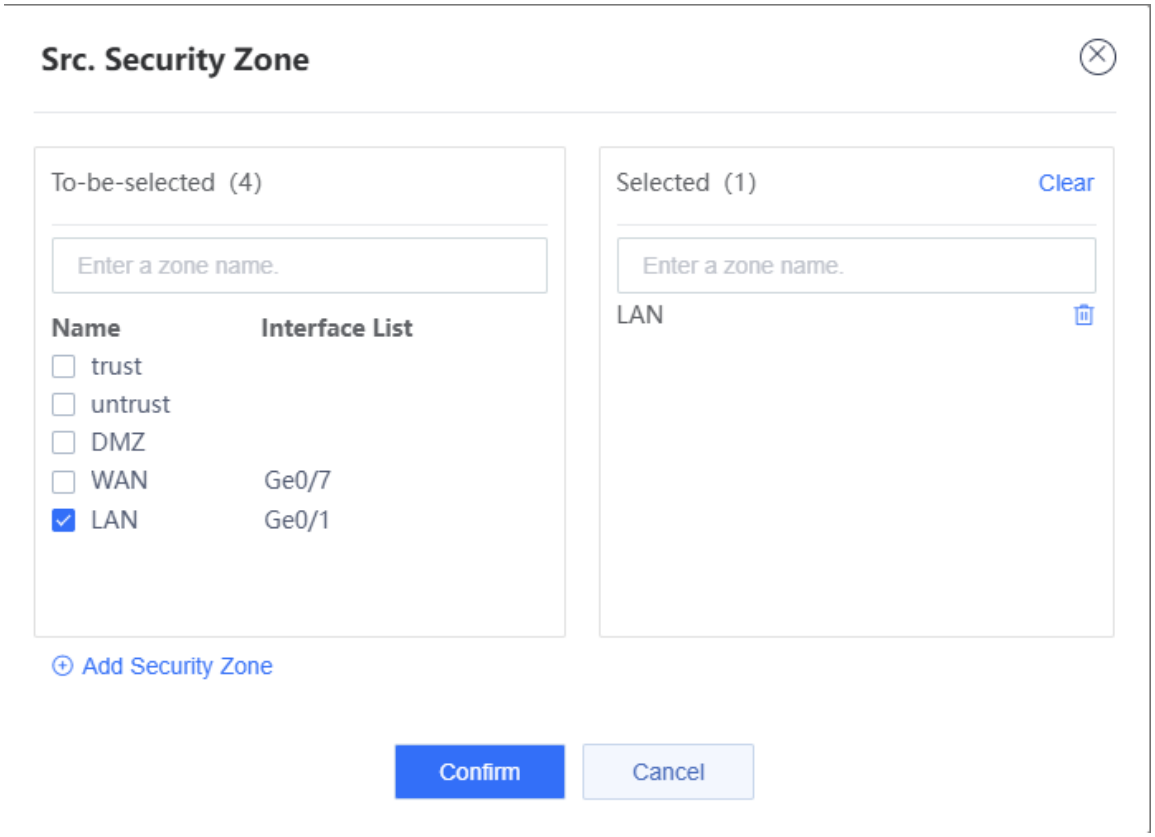


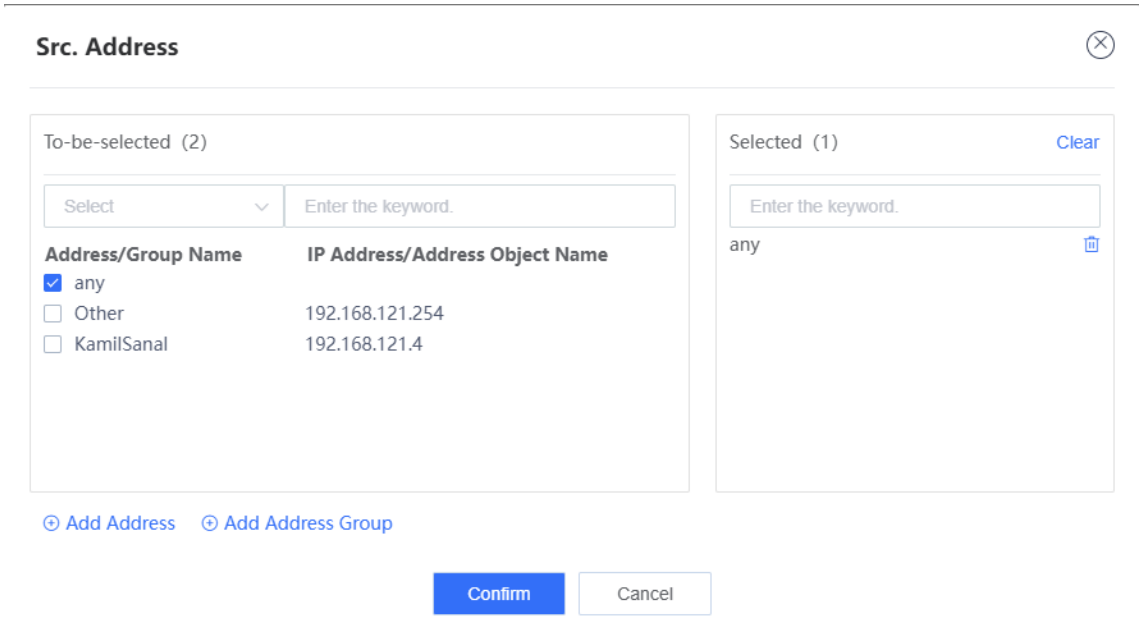
Src. Security Zone bölümünde hotspot yayını yapacağınız interface'i seçiniz

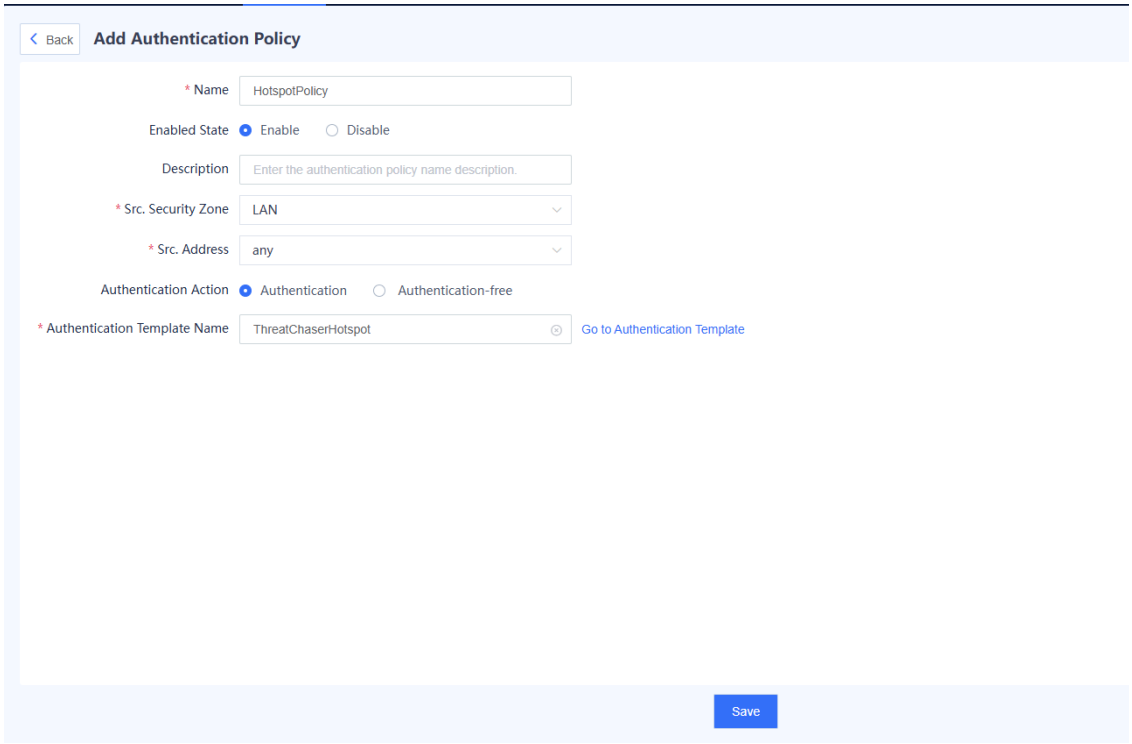
Src. Address bölümünde 'any' veya 'hotspot network' seçeneğini işaretleyiniz

Authentication Template Name Önceden oluşturduğunuz Authentication Template Name'i seçin

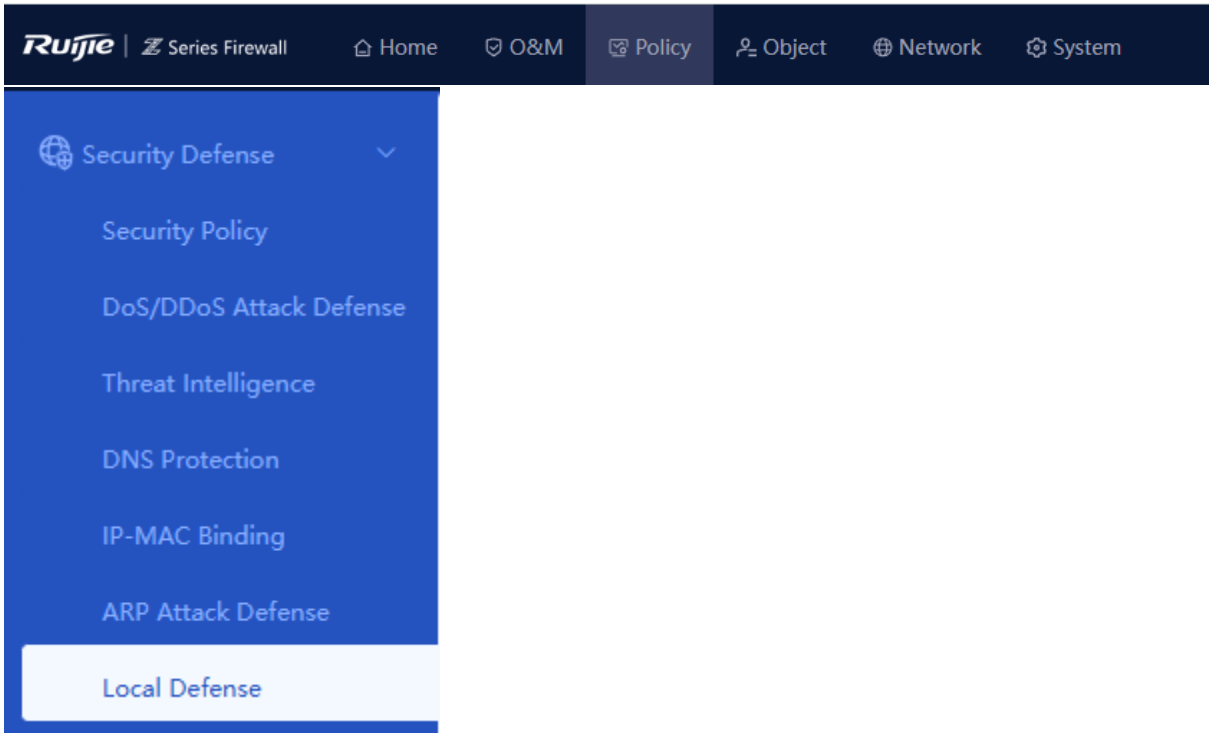




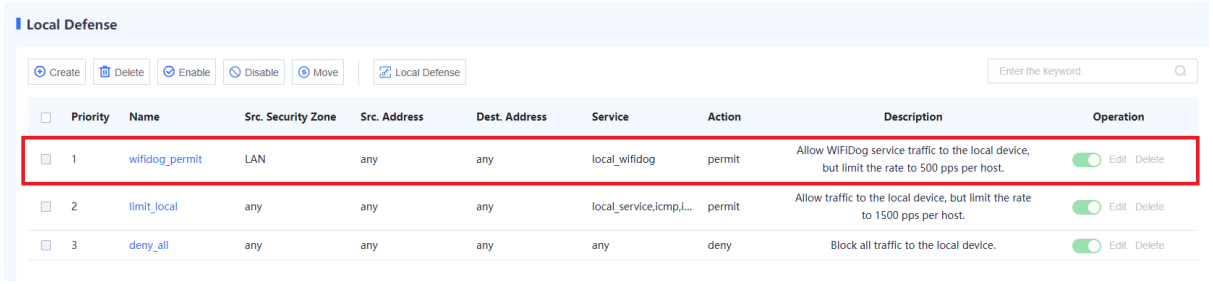

Src. Address
To-be-selected (2)
Select
Enter the keyword.
Address/Group Name
IP Address/Address Object Name
any
Other
192.168.121.254
KamilSanal
192.168.121.4
Selected (1)
Clear
Enter the keyword.
any
Add Address
Add Address Group
Confirm
Cancel


Back
Add Authentication Policy
* Name
HotspotPolicy
Enabled State
Enable
Disable
Description
Enter the authentication policy name description.
* Src. Security Zone
LAN
* Src. Address
any
Authentication Action
Authentication
Authentication-free
* Authentication Template Name
ThreatChaserHotspot
Go to Authentication Template
Save

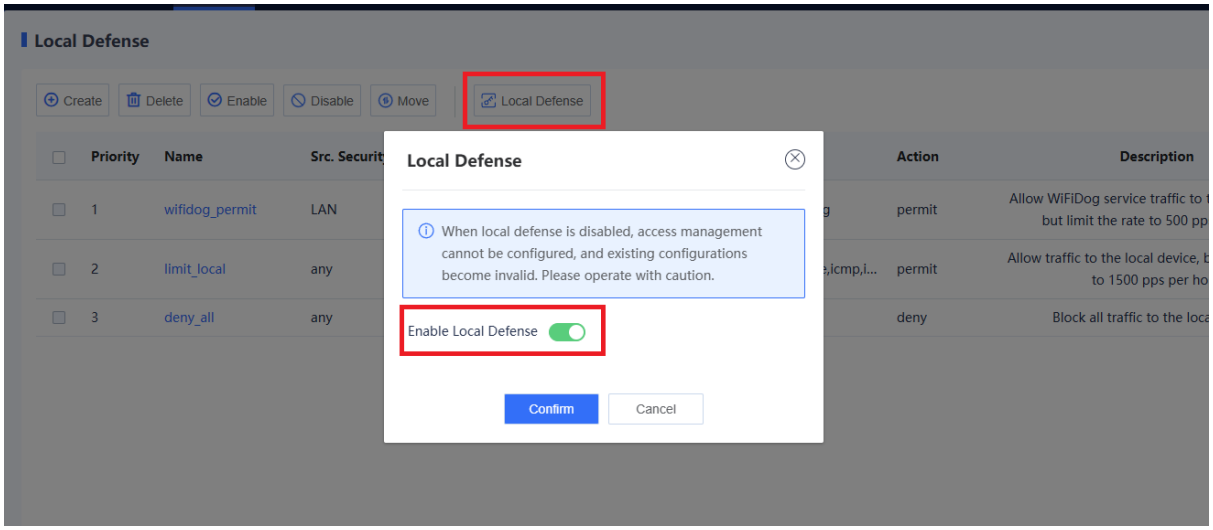
Policy -> Local Defense sayfasına gidin



Wifido_permit bölümü etkin değilse etkinleştirin



Local Defense özelliğini etkinleştirin

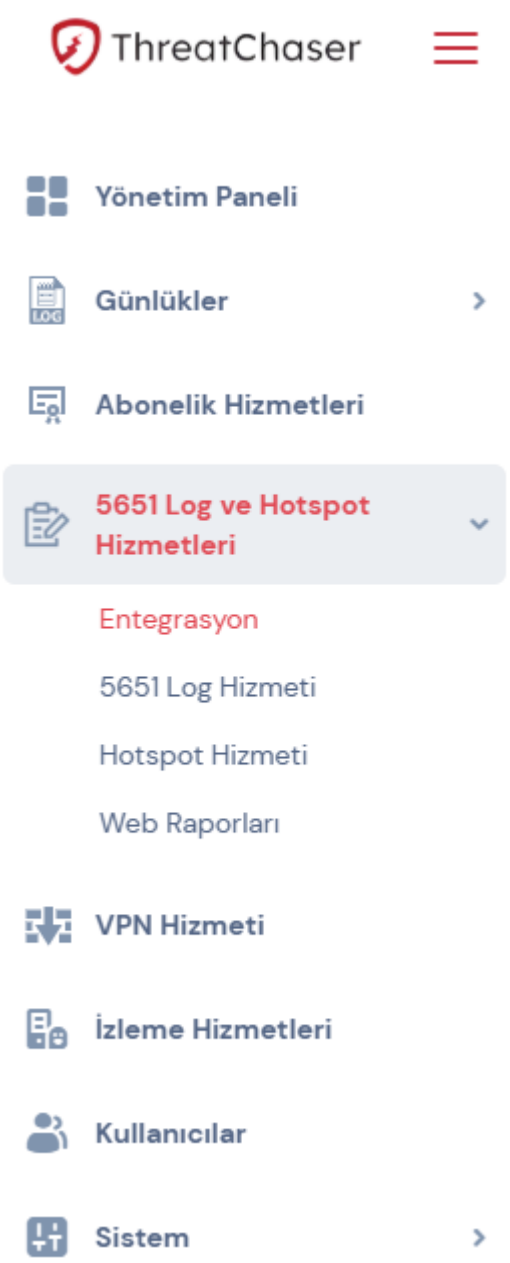


WatchGuard Cihazımdanda HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim?

ThreatChaser Tarafındaki Ayarlamalar

ThreatChaser'a web arayüzü üzerinden erişim sağlayınız

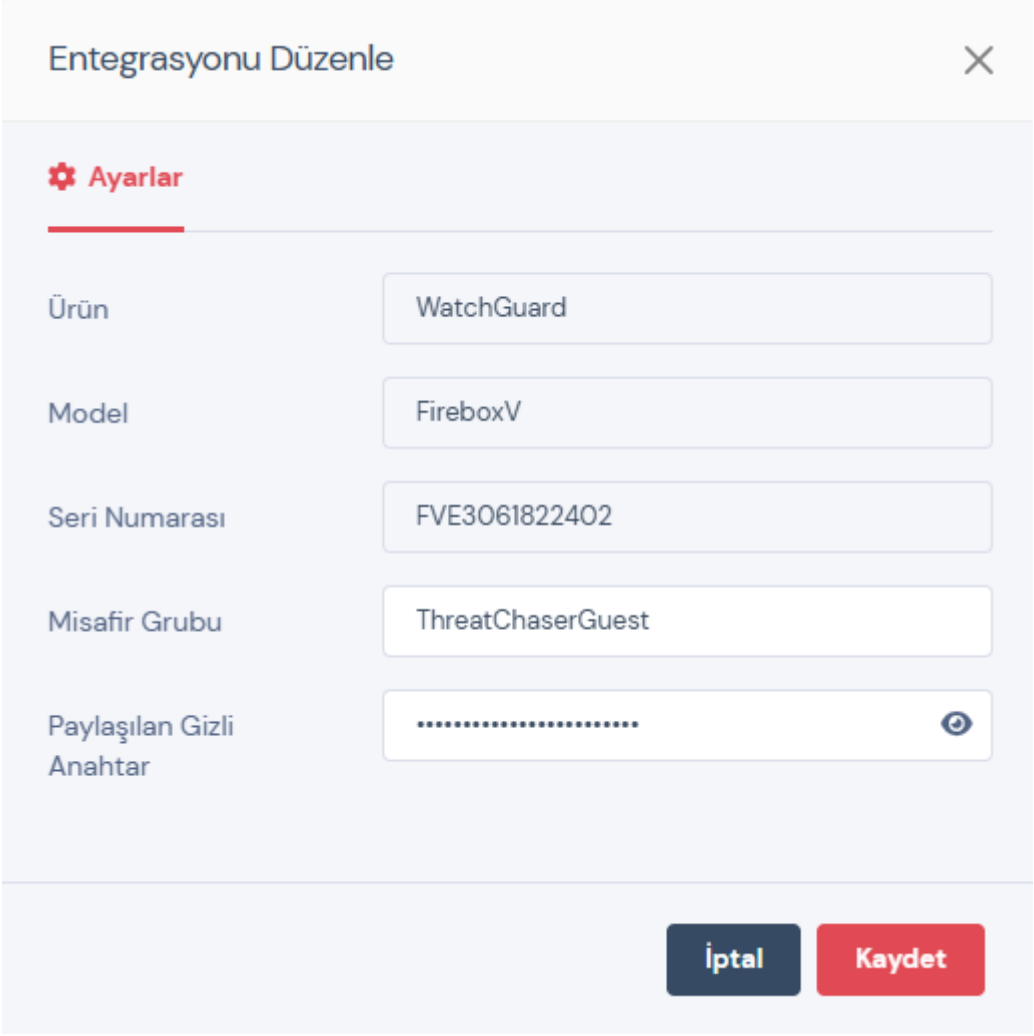
5651 Log ve Hotspot Hizmetleri -> Entegrasyon sayfasına gidin



Entegrasyon yapacağınız firewall için düzenleme simgesine tıklayınız.

Misafir Grubu Bu bölümün Ruijie tarafında oluşturduğunuz grup ismi ile aynı olması gerekiyor

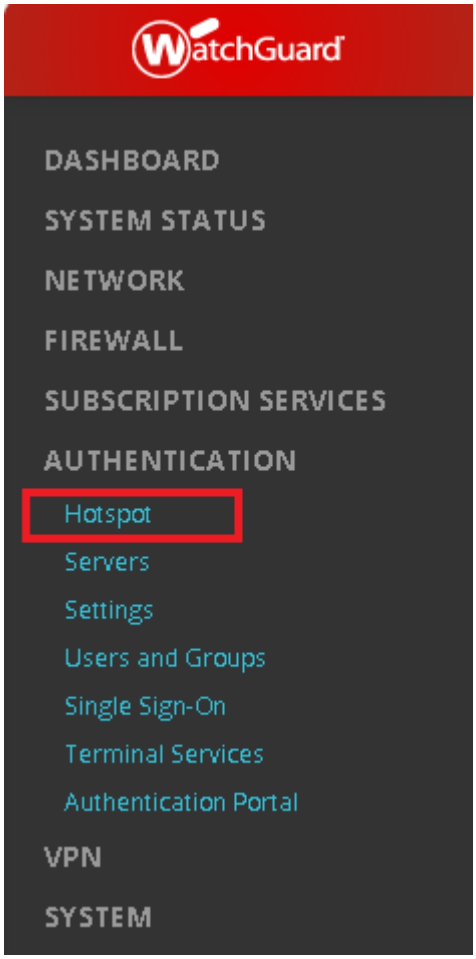
Paylaşılan Gizli Anahtar Bu bölüme WatchGuard'ın ThreatChaser ile iletişime geçebilmesi için bir şifre oluşturmanız gerekiyor.



Firewall Tarafındaki Ayarlamalar

WatchGuard Cihazınıza Web Arayüzü üzerinden giriş yapın

Authentication -> Hotspot -> External Guest Authentication sayfasına gidin



Enable External Guest Hotspot seçeneğini işaretleyin

Shared Secret ThreatChaser tarafında girdiğiniz **Paylaşılan Gizli Anahtar** şifresini giriniz

Authentication URL bölümünde aşağıdaki örnekteki bilgileri kendi değerlerinizle değiştirerek giriniz

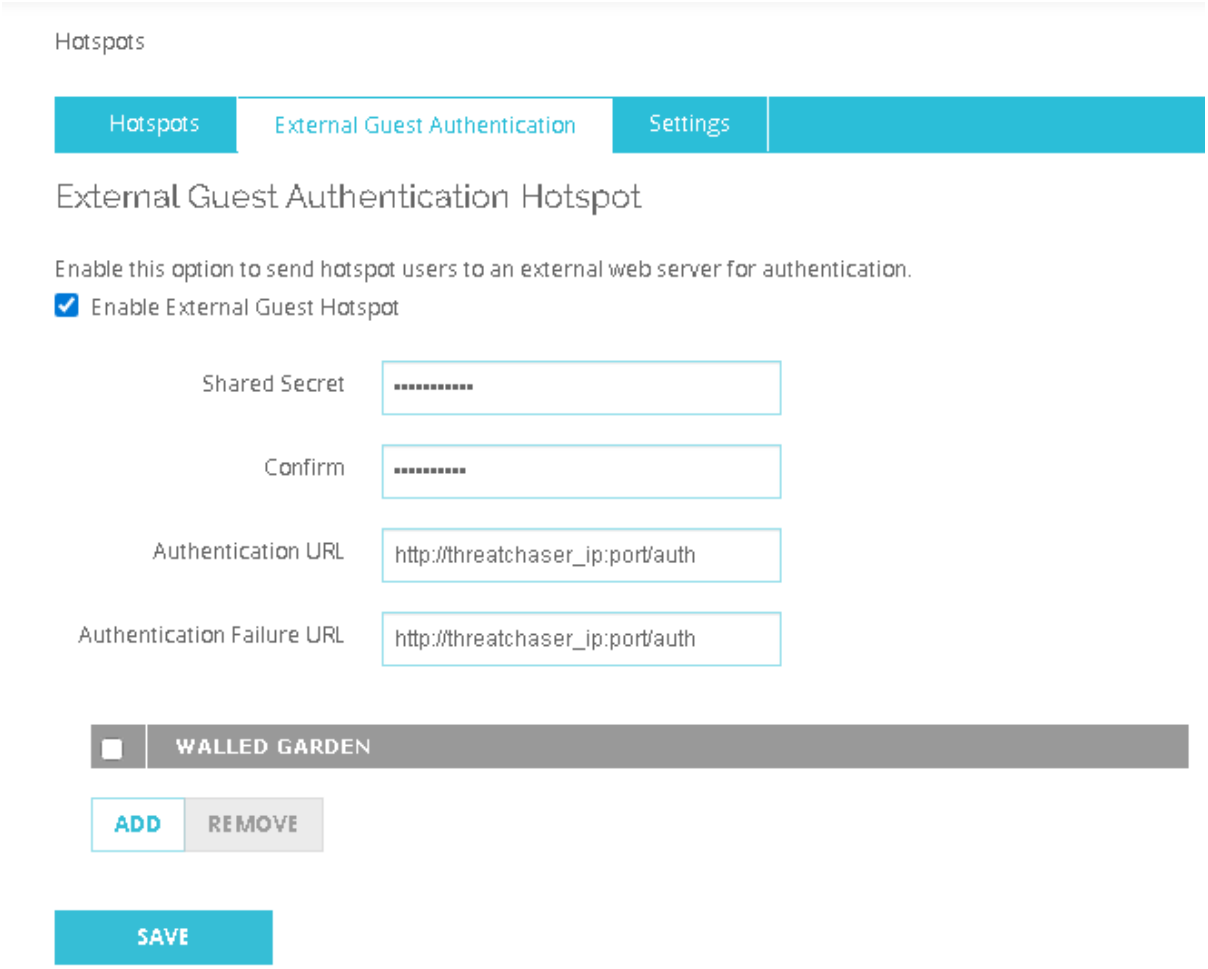
http://threatchaser_ip_adresi:threatchaser_hotspot_port_numarası/wifidog

(Örn: http://192.168.1.111:7560/auth)

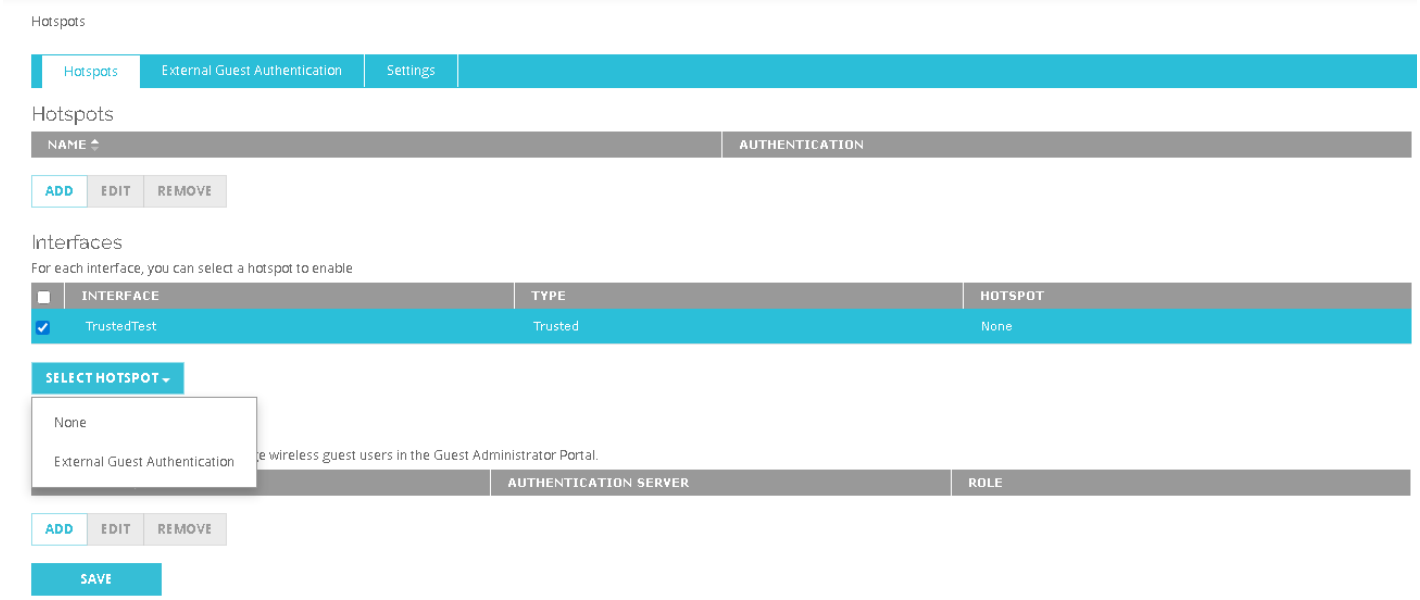
Authentication Failure URL bölümünde aşağıdaki örnekteki bilgileri kendi değerlerinizle değiştirerek giriniz

http://threatchaser_ip_adresi:threatchaser_hotspot_port_numarası/wifidog

(Örn: http://192.168.1.111:7560/auth)



Authentication -> Hotspot -> Hotspots sayfasına gidin



Interfaces bölümünden hotspot yayını yapmak istediğiniz interface'i seçiniz

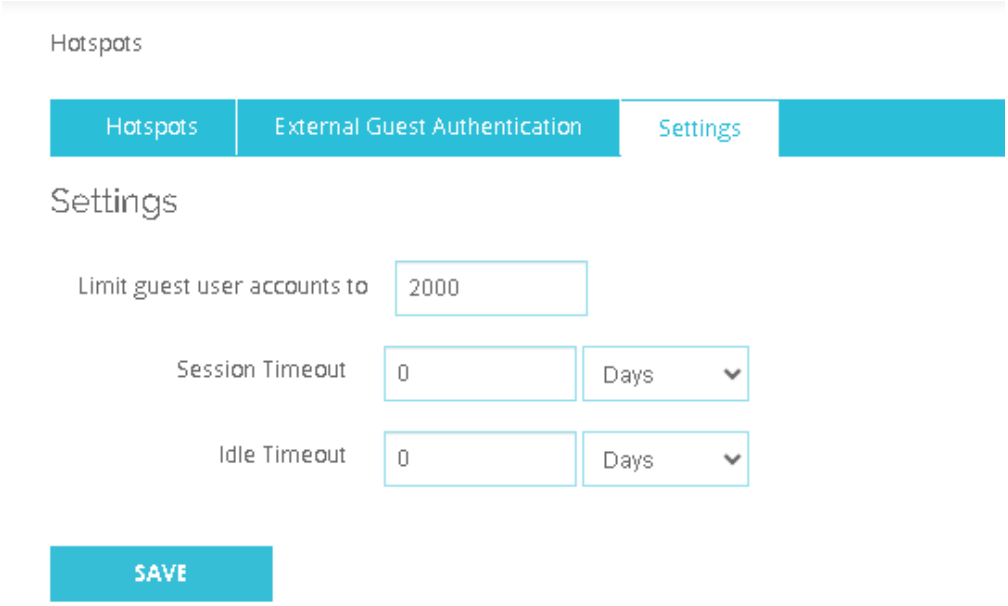
SELECT HOTSPOT bölümünden oluşturduğunuz External Guest Authentication'ı seçiniz

Authentication -> Hotspot -> Settings sayfasına gidin

Limit guest user accounts to bölümünü ağınızın büyüklüğüne göre belirleyin

Session Timeout bölümünü 0 olarak ayarlayınız

Idle Timeout bölümünü 0 olarak ayarlayınız

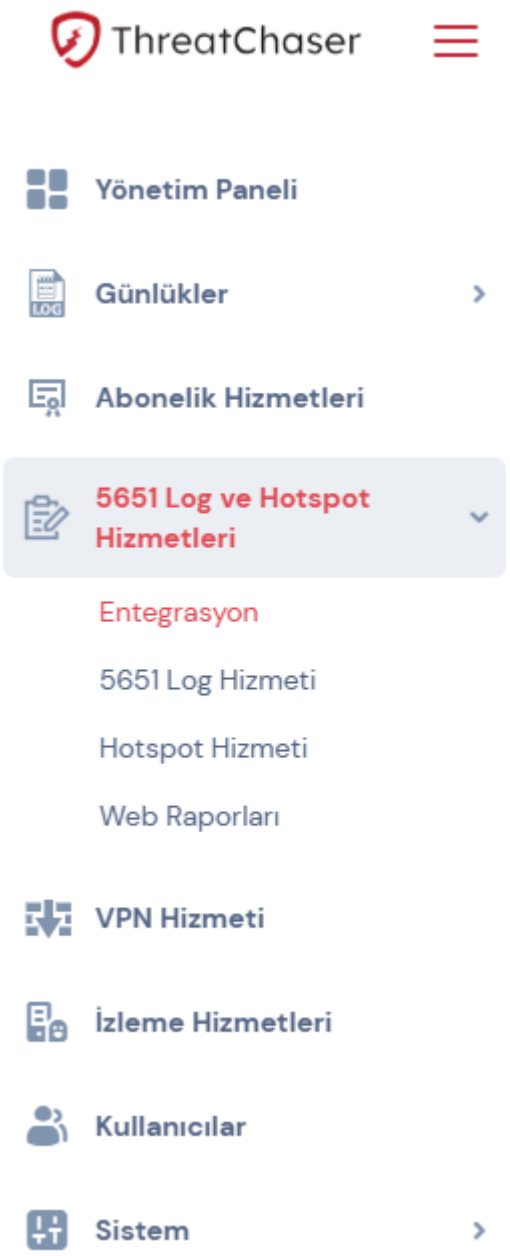


Ruijie Reyee Cihazımdanda HotSpot Hizmetini Nasıl Aktif Hale Getirebilirim?

ThreatChaser Tarafındaki Ayarlamalar

ThreatChaser'a web arayüzü üzerinden erişim sağlayınız

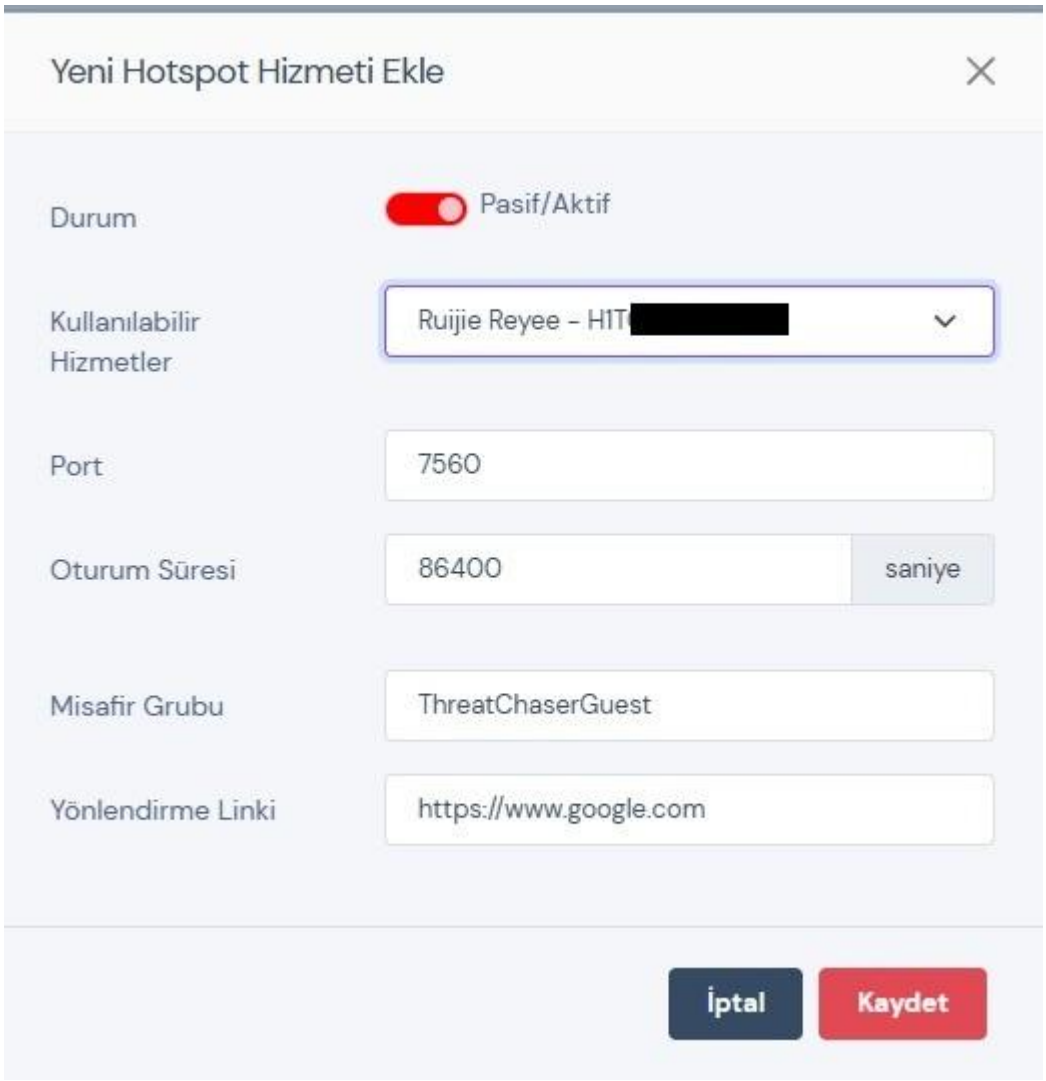
5651 Log ve Hotspot Hizmetleri -> Entegrasyon sayfasına gidin



Entegrasyon yapacağınız firewall için düzenleme simgesine tıklayınız.

Misafir Grubu ismini giriniz

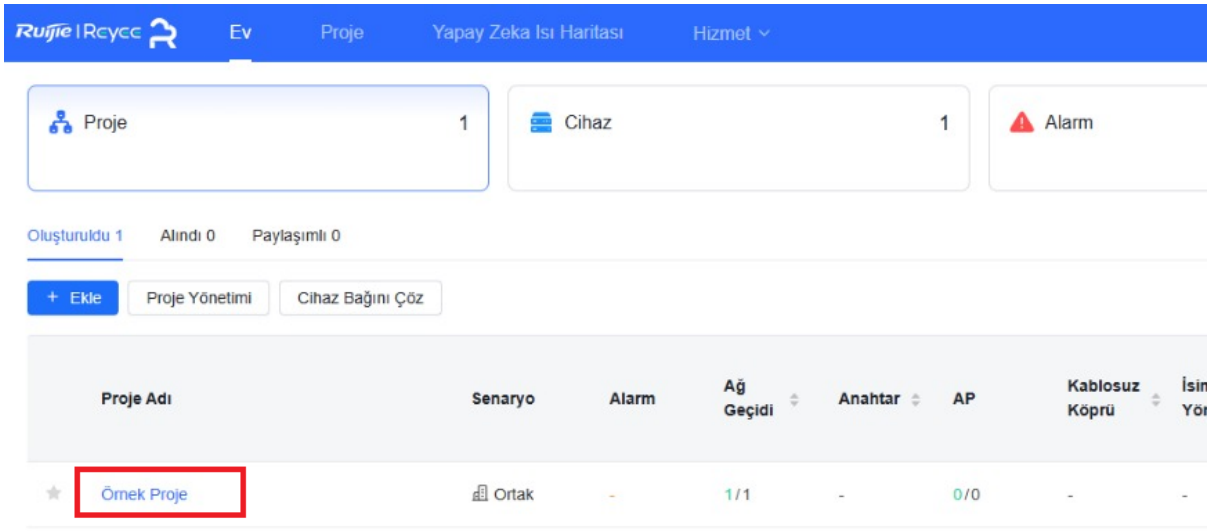
Yönlendirme linkini belirtiniz



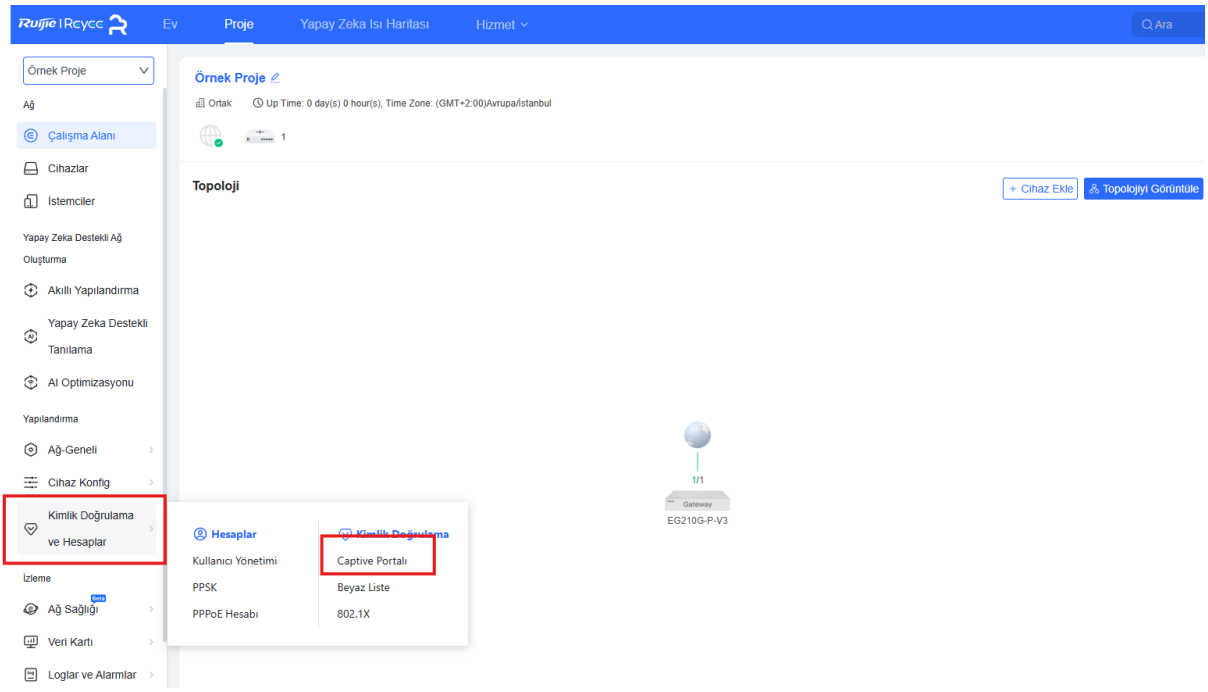
Firewall Tarafındaki Ayarlamalar

Yaptığınız işlemlerin geçerli olabilmesi için Ruijie Reyee cihazınızın bulut (cloud) entegrasyonunun tamamlanması gerekmektedir.

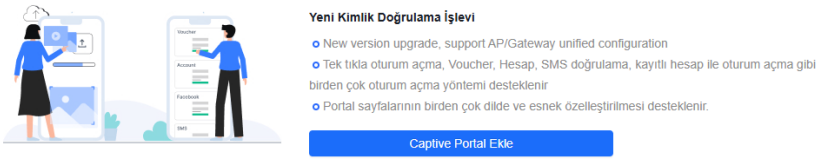
Daha önceden eklediğiniz Ruijie Reyee cihazınızı seçin



Kimlik Doğrulama ve Hesaplar -> Captive Portal sayfasına gidin



Captive Portal Ekle butonuna tıklayınız



Politika Adı bölümüne misafir yayınız için bir isim giriniz

Politika Modu bölümünü **Harici** olarak seçiniz

Kimlik Doğrulama Cihazı bölümünü **Reyee Ağ Geçidi** olarak seçiniz

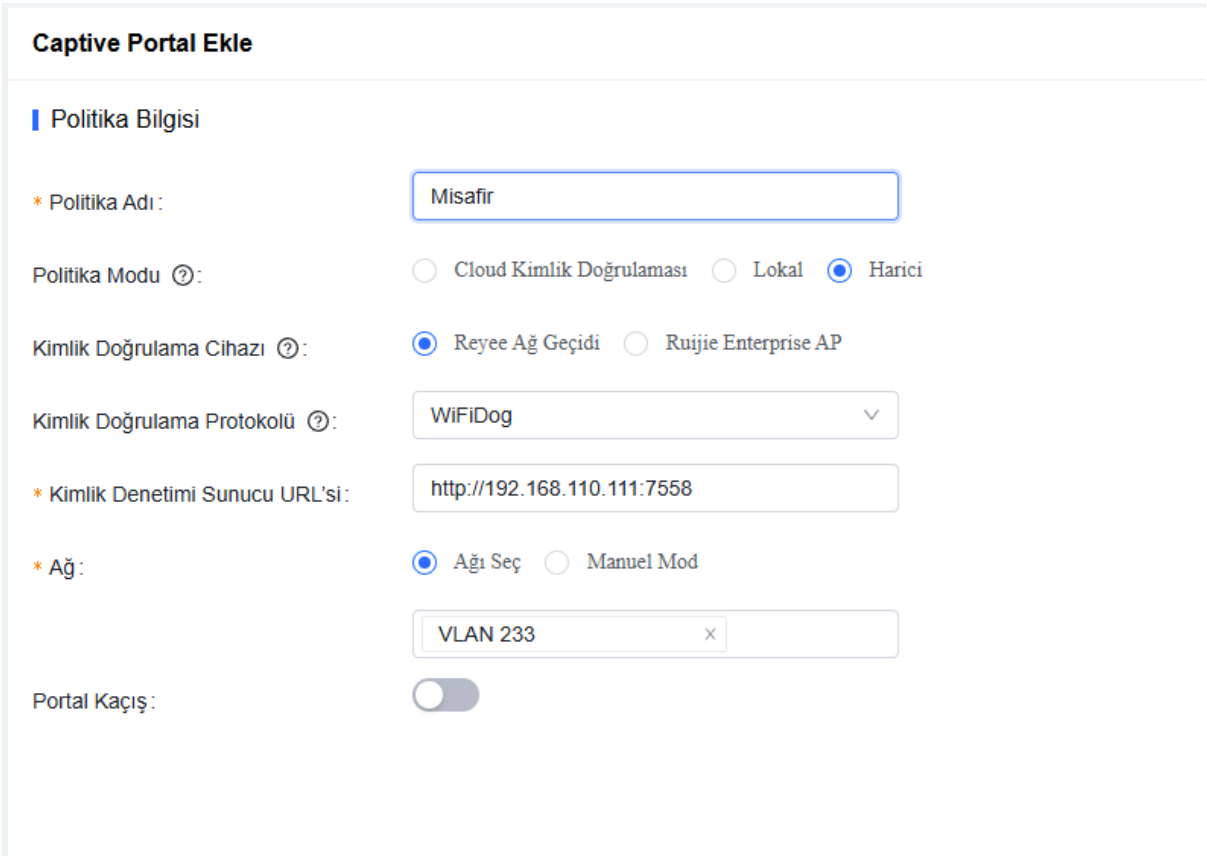
Kimlik Doğrulama Protokülü bölmünü **WIFIDog** olarak seçiniz

Kimlik Denetimi Sunucu URL'si bölümünde aşağıdaki örnekteki bilgileri kendi değerlerinizle değiştirerek giriniz

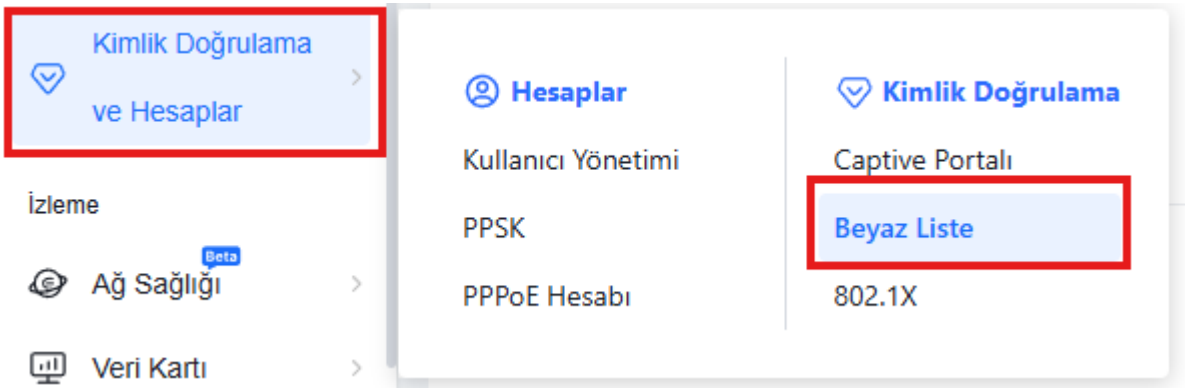
http://threatchaser_ip_adresi:threatchaser_hotspot_port_numarası/wifidog

(Örn: http://192.168.110.111:7558/auth)

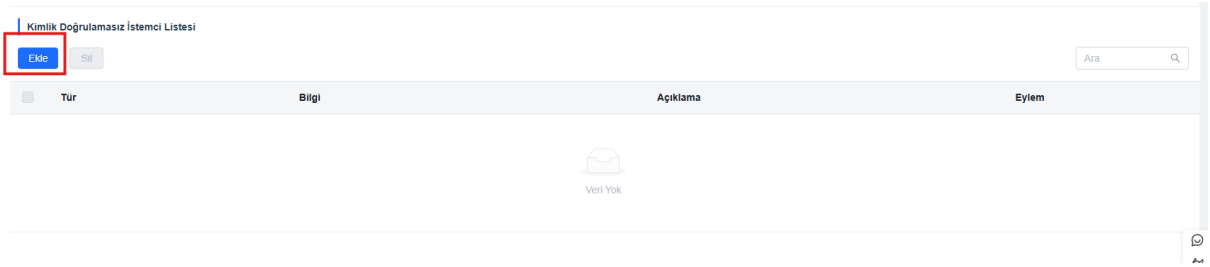
Ağ bölümünde misafir yayını yapmak istediğiniz ağı seçiniz



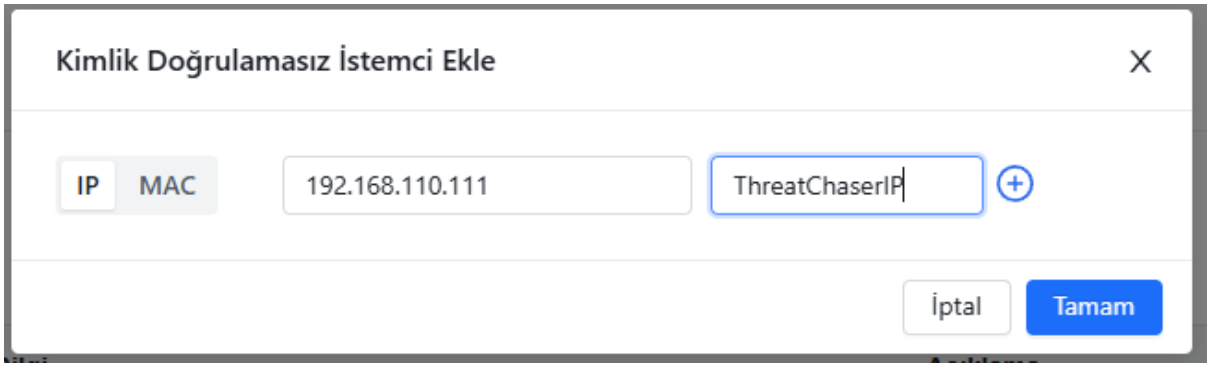
Kimlik Doğrulama ve Hesaplar -> Beyaz Liste sayfasına gidin



Ekle butonuna tıklayın

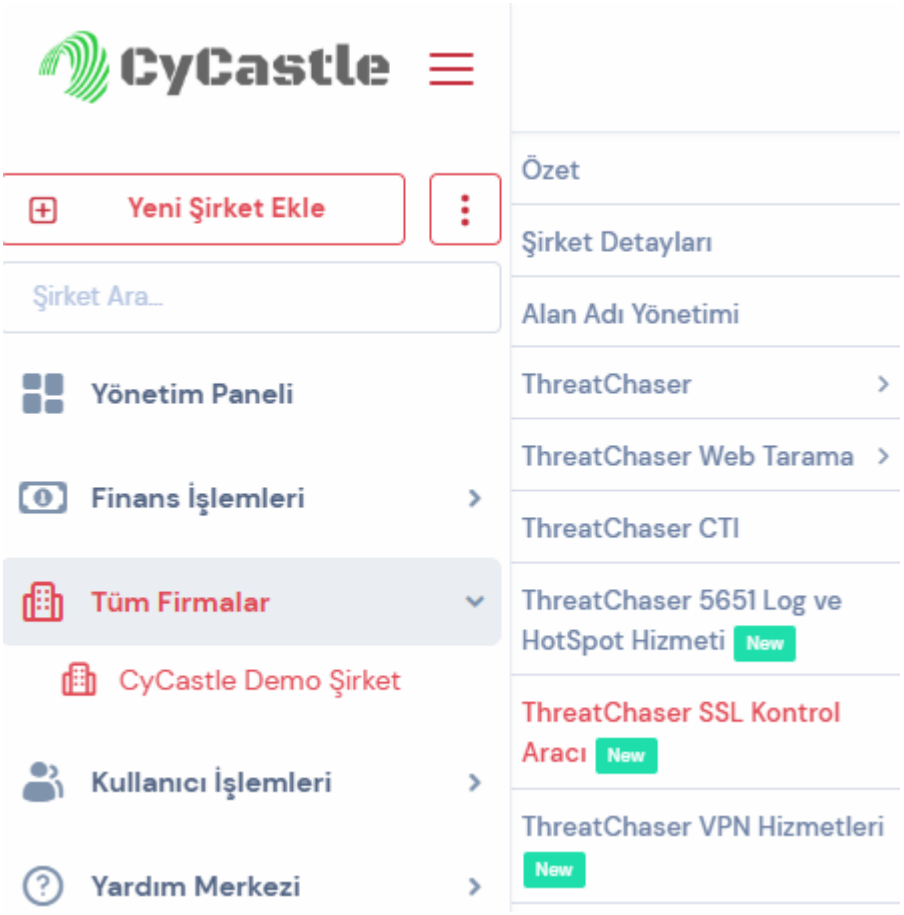


ThreatChaser'ın IP adresini girin ve kaydedin.

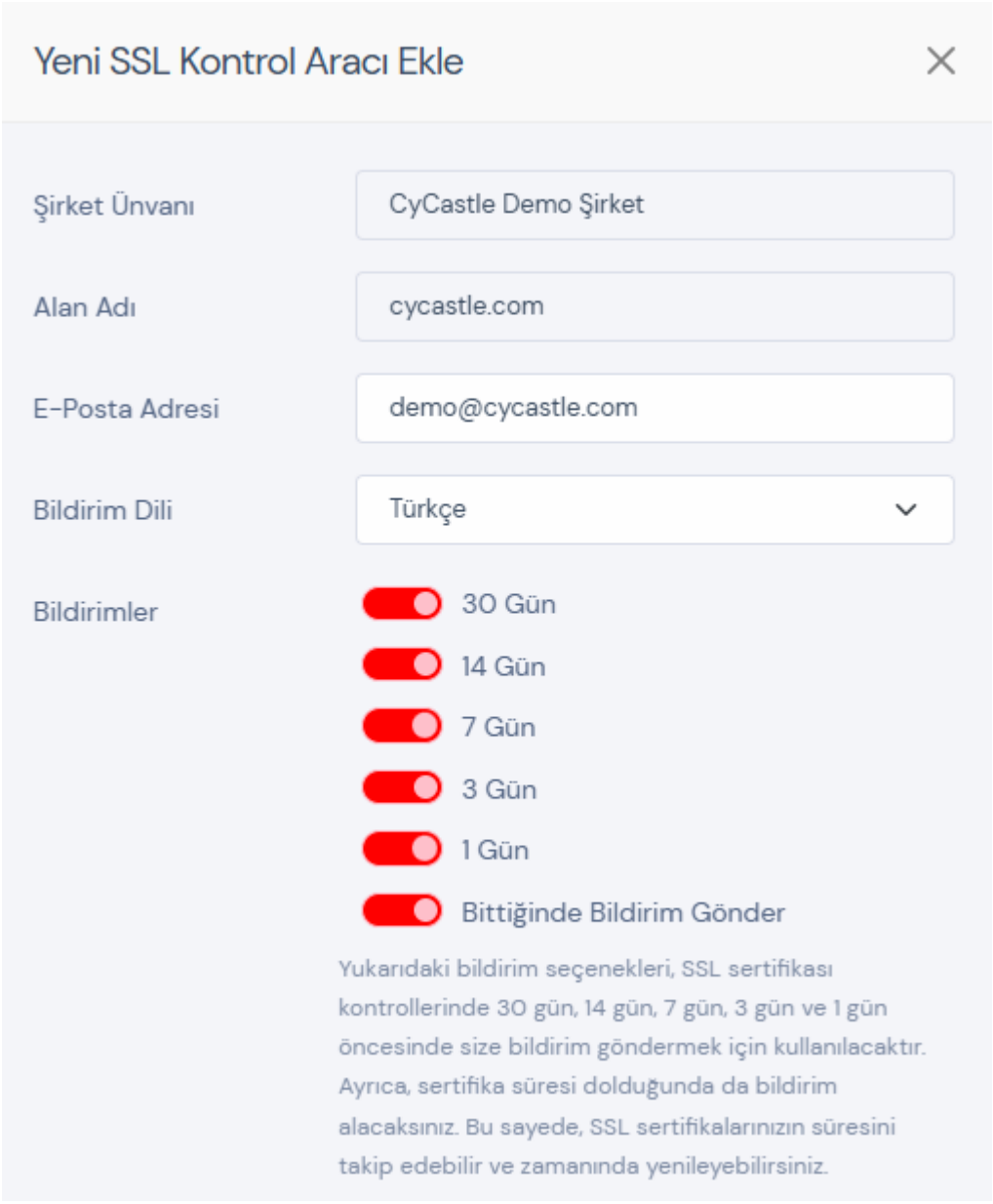


SSL Kontrol Aracı Hizmetini Nasıl Aktif Edebilirim?

Şirket menüsünde yer alan “**ThreatChaser SSL Kontrol Aracı**” bölümüne gidiniz



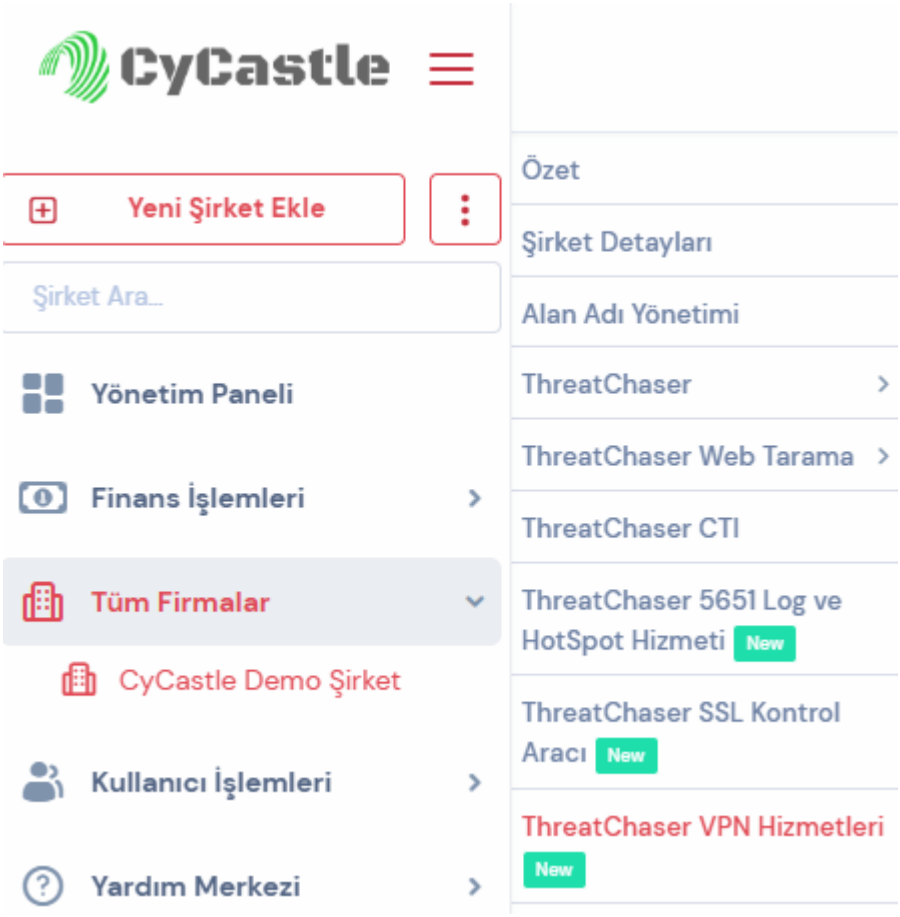
SSL kontrolünü etkinleştirmek istediğiniz domainin sol tarafında bulunan butonu aktif konuma getiriniz.



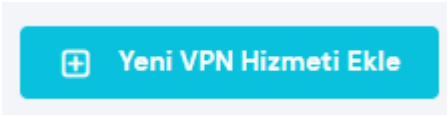
“Kaydet” butonuna tıklayarak işlemi sonlandırın.

VPN Hizmetini Nasıl Aktif Edebilirim?

Şirket menüsünde yer alan “**ThreatChaser VPN Hizmetleri**” bölümüne gidiniz



“Yeni VPN Hizmeti Ekle” Butonuna Tıklayınız

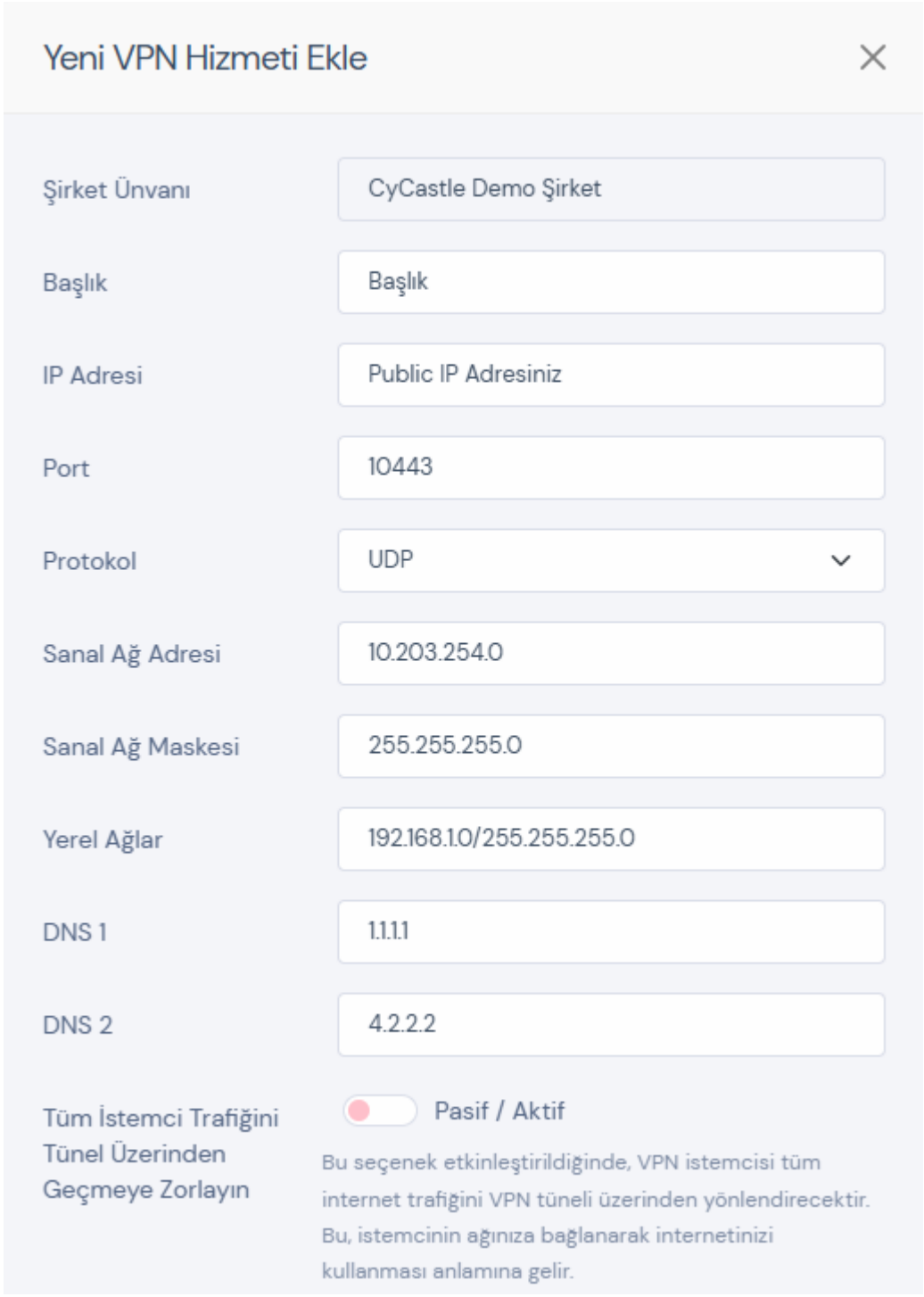


“IP Adresi” bölümüne public IP adresinizi girmeniz gerekmektedir. Kullanacağınız public IP adresinin statik olması zorunludur. Eğer firewall kullanıyorsanız VPN portu için yönlendirmeyi firewall üzerinden yapmanız gerekir, firewall kullanmıyorsanız bu işlemi modem üzerinden gerçekleştirmeniz gerekir.

Sanal Ağ Adresi ve Sanal Ağ Maskesi, VPN tüneli için kullanılmaktadır. Burada, hali hazırda kullanılmayan bir ağ adresi girmeniz gerekmektedir.

Yerel Ağlar, VPN üzerinden erişilmesini istediğiniz ağları ifade eder.

“**Tüm İstemci Trafiğini Tünel Üzerinden Geçmeye Zorlayın**” seçeneği etkinleştirildiğinde, tüm internet trafiği VPN tünelinden geçirilir. Böylece VPN’e bağlanan kullanıcılar internete firmanın dış IP adresi üzerinden erişmiş olur.



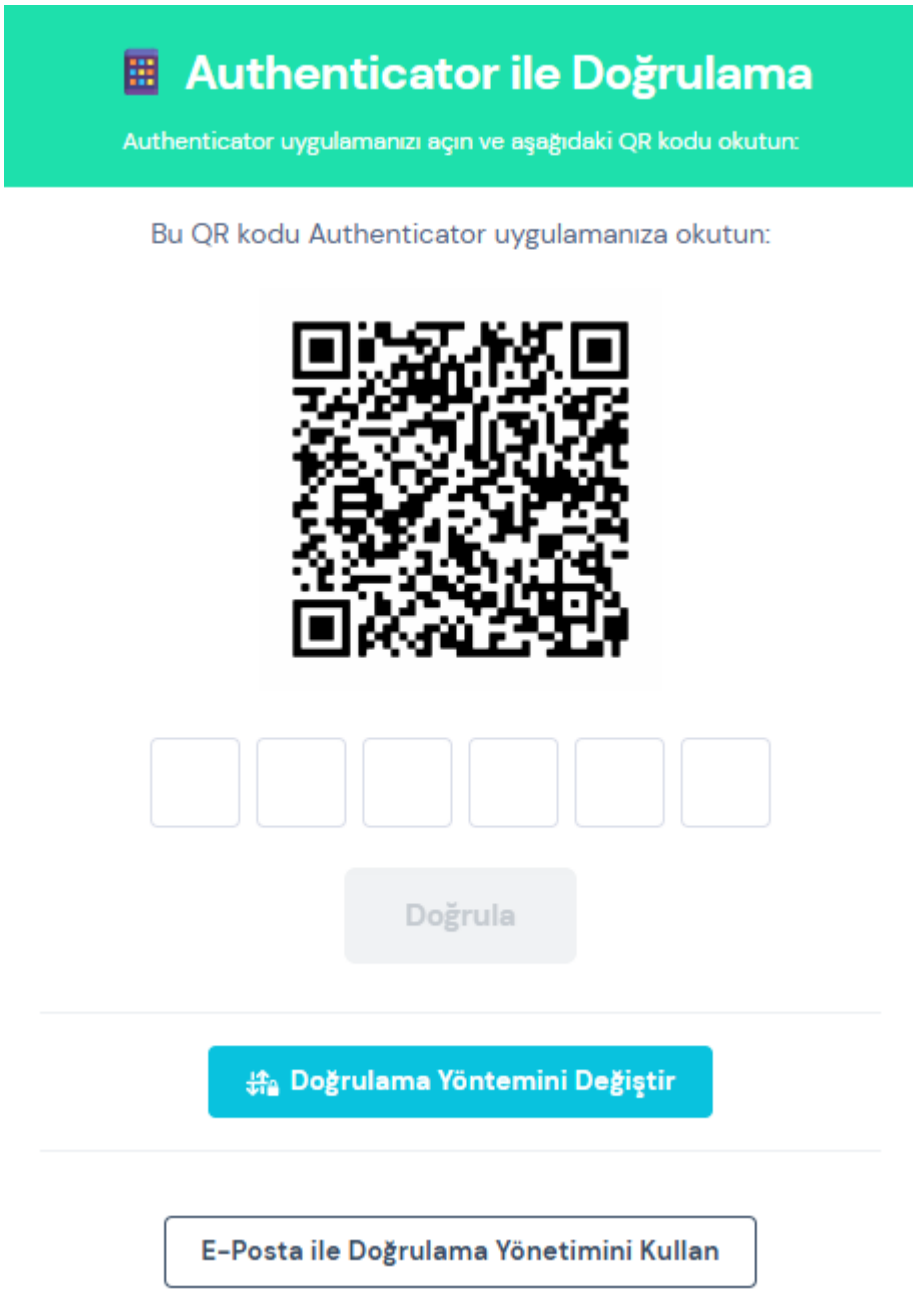
“Kaydet” butonuna tıklayarak işlemi sonlandırın.

İki Faktörlü Doğrulamayı Nasıl Aktif Edebilirim?

Yeni kayıt olduysanız ilk girişte, veya daha önceden kayıtlı olup iki faktörlü doğrulama aktif değilse, giriş yaptıktan sonra karşınıza aşağıdaki ekran gelecektir. Aktivasyon işlemini bu ekrandan gerçekleştireceğiz.

1. Yöntem E-Posta Doğrulaması
   Giriş yapmak istediğinizde, sistemde kayıtlı olan e-posta adresinize iki faktörlü doğrulama kodu gönderilecektir. Bu kodu kullanarak sisteme giriş yapabilirsiniz.

2. Authenticator ile Doğrulama



Ekranınıza gelen QR kodu Authenticator uygulamanıza okutun

QR kodunu okuttuktan sonra sistemdeki kodu aşağıdaki gibi girin

Authenticator ile Doğrulama

Authenticator uygulamanızı açın ve aşağıdaki QR kodu okutun:

Bu QR kodu Authenticator uygulamanıza okutun:

8 4 1 7 6 0

Doğrula

Doğrulama Yöntemini Değiştir

E-Posta ile Doğrulama Yönetimini Kullan