FastNAC

CİHAZ PROFİLLEME

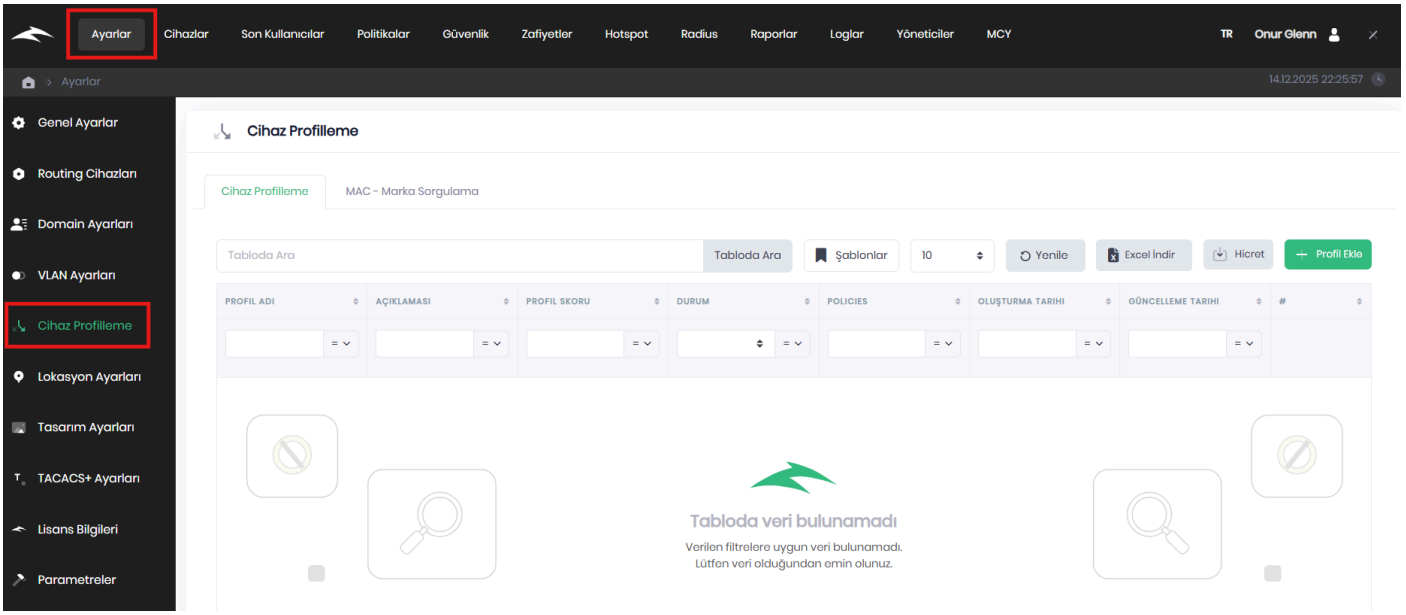
İçindekiler;

1. Başlangıç

FastNAC ile Network üzerinde bulunan IoT veya benzer cihazları, bir çok profilleme yöntemini aynı anda kullanarak sınıflandırma yapabilirsiniz. Cihazları;

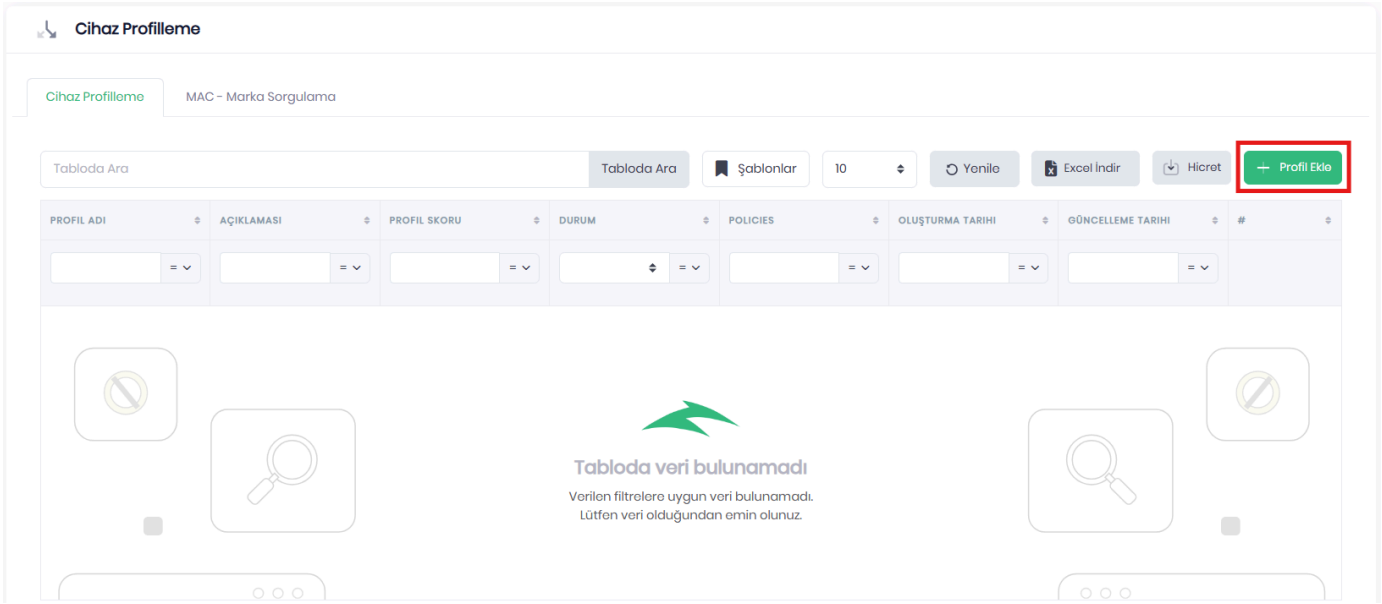
- MAC adresleri veya MAC üretici bilgisine göre,
- IP Adresi veya IP Bloklarına göre,
- Lokasyonuna veya Switch/Port bilgisine göre,
- Active Directory Öz Niteliklerine göre,
- HTTP/HTTPS yöntemi ile tarama yapıp içeriğe,
- Telnet/SSH ile komut çalıştırıp çıktısına göre,
- DHCP Fingerprint;
    - Üretici bilgisine göre,
    - Ana makine adına (hostname) göre,
    - Fingerprint parametrelerine göre
- TCP/UDP açık/kapalı/filtreli port durumlarına göre,
- SNMP isteği atarak gelen cevaba göre,
- Windows işletim sistemi için;
    - İşletim sistemi kontrolüne göre,
    - Windows içinde yüklü veya yüklü olmayan programa göre,
    - Windows içinde yüklü olan programın versiyon bilgisine göre,
    - Windows içinde çalışan/çalışmayan servislerin duruma göre,
- Linux işletim sistemi için;
    - İşletim sistemi kontrolüne göre,
    - Linux içinde yüklü veya yüklü olmayan programa göre,
    - Linux içinde yüklü olan programın versiyon bilgisine göre,
    - Linux içinde çalışan/çalışmayan servislerin duruma göre,
- İşletim sistemi içinde bulunan bir dosyanın yoluna göre,
- Oturum açılma süresine göre,
- NMAP taraması (özel parametreler kullanabilirsiniz) ile çıkan sonuca göre,

vb. yöntemleri kullanarak sınıflandırabilirsiniz. Cihaz Profilleme ayarlarına; **Ayarlar** -> **Cihaz Profilleme** menüsü altından ulaşabilirsiniz.



2. Profil Ekleme

Cihaz Profilleme ekranında bulunan “Profil Ekle” butonuna basarak yeni bir profil oluşturabilirsiniz.



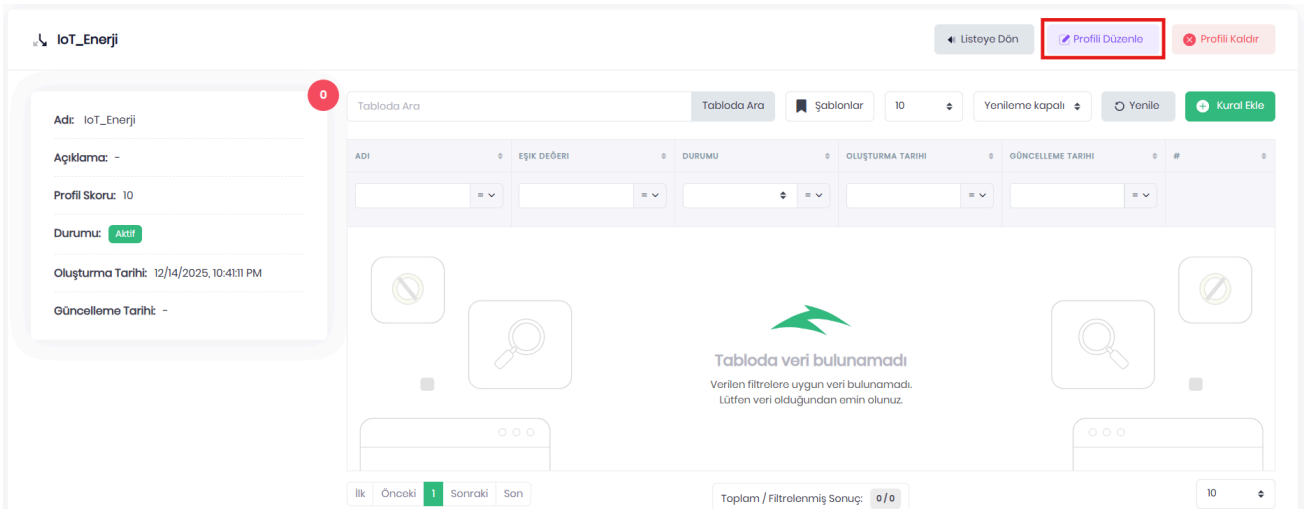
Açılan pencerede;

Oluşturmak istediğiniz profilin Adını, Açıklamasını (opsiyonel) ve Toplam Eşik Değeri Puanını belirtmelisiniz. Profili oluşturduğunuzda otomatik olarak detay sayfasına yönlendirileceksiniz.

Önemli: Toplam Eşik Değeri Puanı, profilin içine eklenecek kuralların toplam puanını ifade etmektedir. Burada vereceğiniz puan profilin içine eklenilen kurallara verdiğiniz puanların toplamı olmalıdır. "1.6) Profil Skor Sistemi ve Örnekler" konusunda bu bölüm daha detaylı anlatılmaktadır.

3. Profil Detay Sayfası

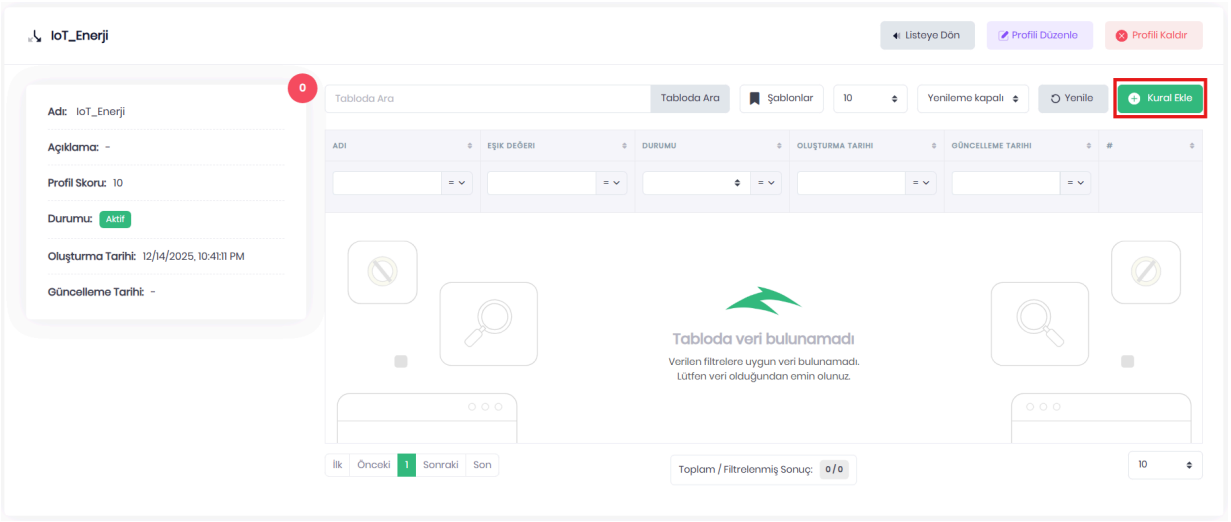
Profil detay sayfasına sağ üstte bulunan "Profil Düzenle" butonunu kullanarak ilgili profili düzenleyebilirsiniz;



Düzenleme ekranında Profilin Adını, Açıklamasını veya Toplam Eşik Değeri Puanını değiştirebilirsiniz.

4. Profil Kuralı Ekleme

Profil detay sayfasının sağında bulunan “Kural Ekle” butonuna basarak yeni bir kural ekleyebilirsiniz;



Kural eklerken;

Adı: Kural’a verebileceğiniz özel bir isim

Puanı: İlgili kuralın puanı (Profil skorunu etkiler)

Durumu: Kuralın aktif/pasif durumu

Kural Tipi: Profilleme sınıfı

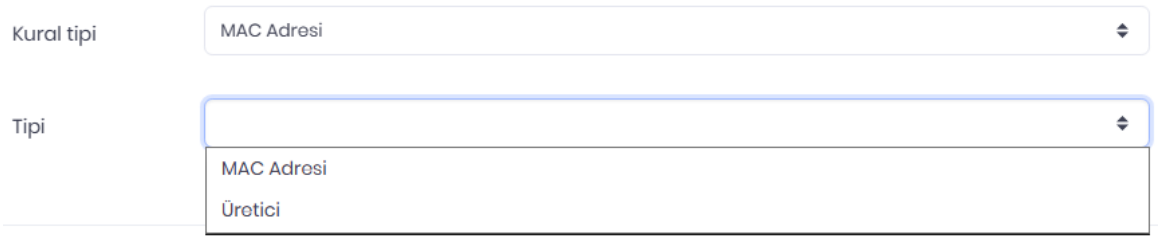
bilgilerini girerek yeni bir kural seti oluşturabilirsiniz.

Not: Kural tipini seç belirlediğinizde ilgili ekranda seçtiğiniz kural tipi için ekstra inputlar çıkmaktadır. Bunlar Kural Tipleri bölümünde anlatılmaktadır.

5. Profil Kural Tipleri

5.1. MAC Bilgisine Göre

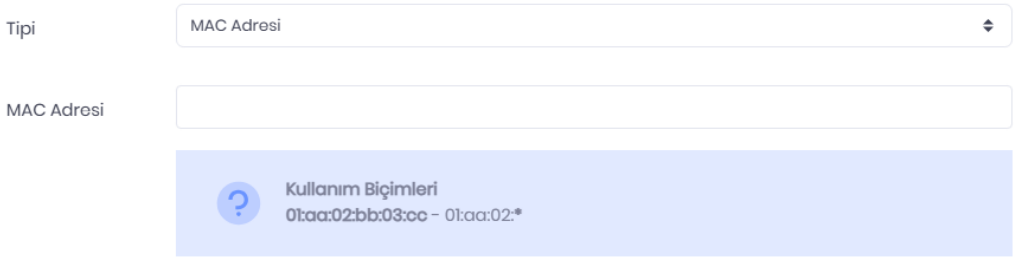
Kural tipi olarak "**MAC Adresi**" seçildiğinde;



MAC adresinin kendisi veya üretici bilgisine göre profil kuralı oluşturabilirsiniz**.**

5.1.1. MAC Adresi

Kural tipi olarak MAC adresi seçildiğinde;



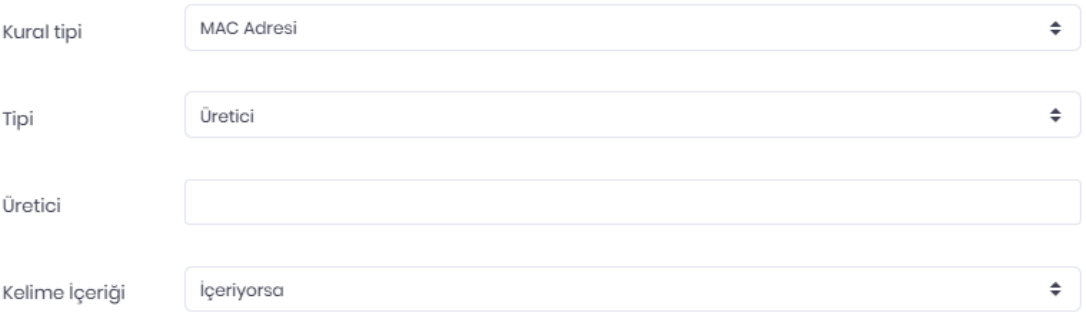
MAC adresinin tamamını veya :* regexini kullanarak ile başlıyorsa şeklinde kural oluşturabilirsiniz. Örneğin;

- Network'e erişmeye çalışan cihazın MAC adresi 01:aa:02:bb:03:cc ise
- Network'e erişmeye çalışan cihazın MAC adresi 01:aa:02:* ile başlıyorsa

şeklinde kural tanımı yapabilirsiniz.

5.1.2. MAC Üretici Bilgisi

MAC üretici bilgisi tipinde;



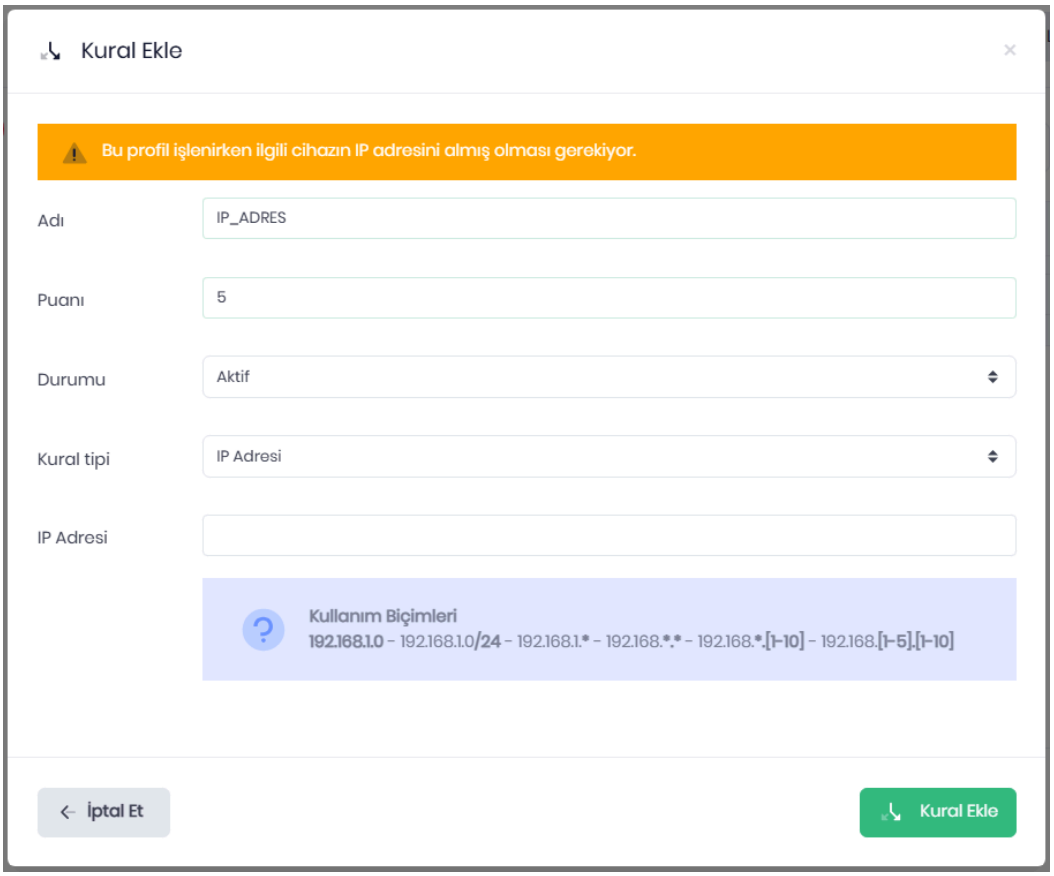
"**Üretici**" bilgisi girildikten sonra girdiğiniz "**Kelime İçeriği**" "**Eşitse**, **İçeriyorsa**, **ile Başlıyorsa**, **ile Bitiyorsa**" alt kural bilgisi seçilir. Örneğin üretici bilgisi olarak "**samsung**" ve kelime içeriği "**İçeriyorsa**" seçildiğinde;

- Network'e erişmeye çalışan cihazın MAC üretici bilgisi "**samsung**" içeriyorsa

şeklinde kural tanımı yapabilirsiniz.

5.2. IP Adresine Göre

Kural tipi olarak "**IP adresi**" seçildiğinde;



Network'e bağlanana cihazın IP adresinin tamamı, IP bloğu, IP adresinin son okteti, IP adresinin son iki okteti, IP adres aralıklarına göre kural tanımlaması yapılabilir. Örneğin;

- Network'e erişmeye çalışan cihazın IP adresi 192.168.1.10 ise,
- Network'e erişmeye çalışan cihazın IP adresi 192.168.1.0/24 ip bloğu içindeyse,
- Network'e erişmeye çalışan cihazın IP adresi 192.168.1. ile başlayıp 4.oktetinde herhangi bir rakam geliyorsa (Maksimum 254) (192.168.1.*),
- Network'e erişmeye çalışan cihazın IP adresi 192.168. ile başlayıp son 3. ve 4. oktetinde herhangi bir rakam geliyorsa (Maksimum 254) (192.168.*.*),
- Network'e erişmeye çalışan cihazın IP adresi 192.168. ile başlayıp 3.okteti herhangi bir rakam (Maksimum 254) ile başlayıp [1-10] arasında bir ip adresi alıyorsa (192.168.*.[1-10])
- Network'e erişmeye çalışan cihazın IP adresi 192.168. ile başlayıp 3.okteti [1-5] arasında bir rakam alıyorsa ve 4.okteti [1-10] arasında bir ip adresi alıyorsa (192.168.[1-5].[1-10])

şeklinde kural tanımları yapabilirsiniz.

Not: IP adresi tipinde kuralın eşleşebilmesi için networke bağlanan cihazın IP adresi almış olması gerekmektedir.

5.3. Lokasyona Göre

Kural tipi olarak "**Lokasyon**" seçildiğinde;

5.3.1. Lokasyon Bilgisi

Lokasyon tipinde;

FastNAC üzerinde oluşturulan lokasyonları seçerek kural tanımı yapabilirsiniz.

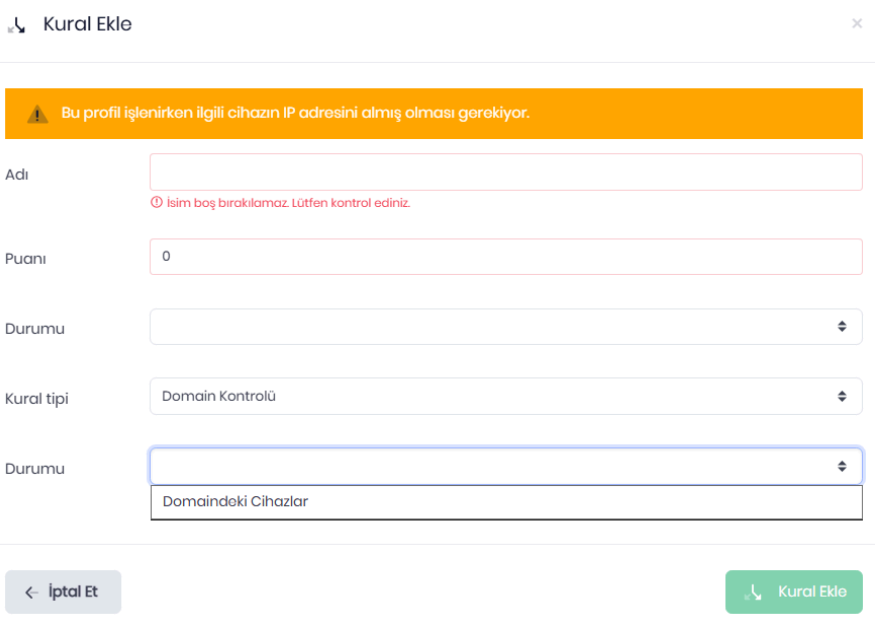
5.3.2. Switch/Port Bilgisi

Switch/Port Bilgisi Tipinde;

Inputlara yazılan Switch/Port bilgisine göre kural tanımı yapabilirsiniz.

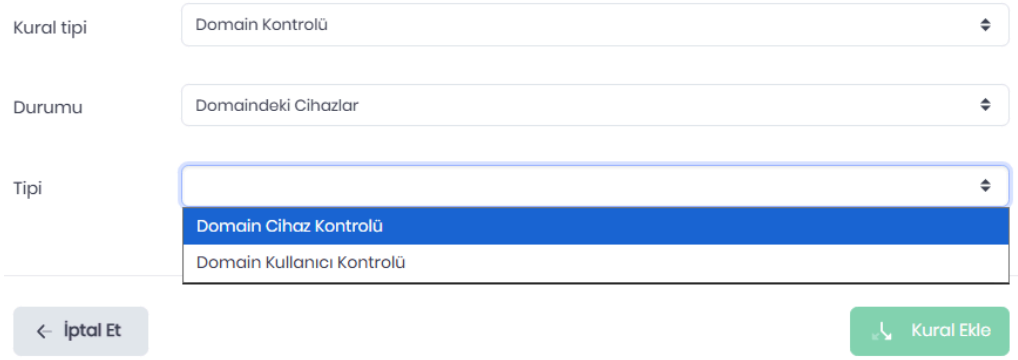
5.4. Domain Kontrolü

Kural tipi olarak "**Domain Kontrolü**" seçildiğinde;



5.4.1. Domain Cihaz Kontrolü

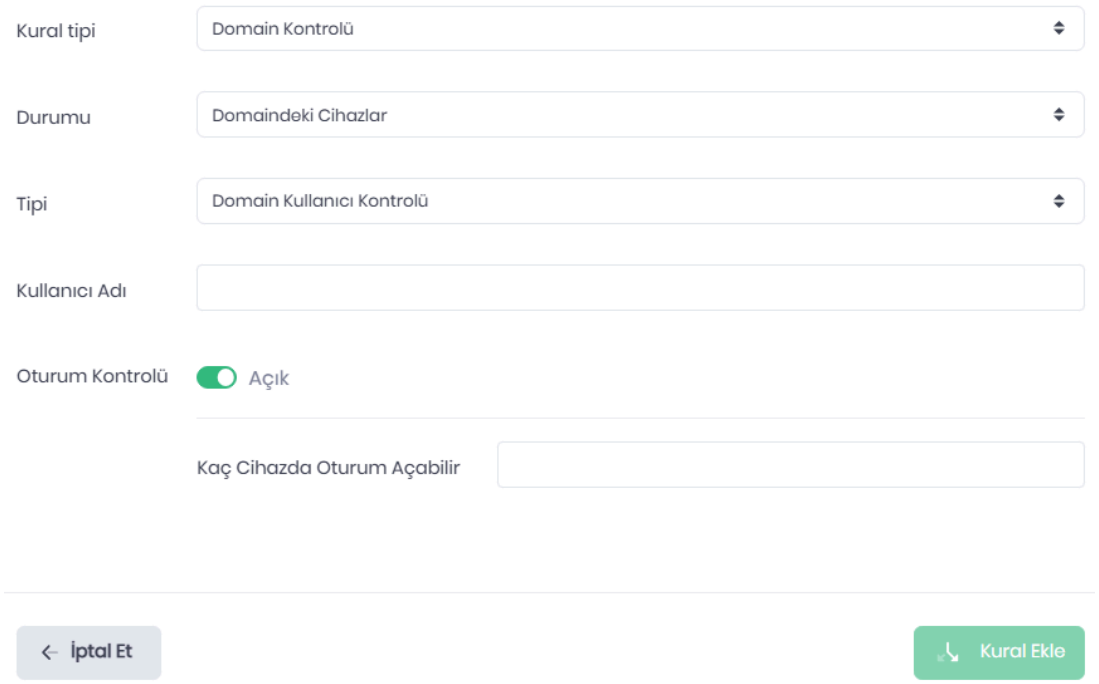
Varsayılan olarak gelen profil tipidir.



Parametre ayarlarına göre cihazınların domain kontrolünü sağlayan profildir.

5.4.2. Domain Kullanıcı Kontrolü

Domain Kullanıcı Kontrolü tipinde;



Domainde olan kullanıcılara özel profil tanımı yapabilirsiniz. Ayrıca kullanıcının kaç cihazda oturum açabileceğini "**Oturum Kontrolü**" ayarını açarak belirleyebilirsiniz. Örneğin;

- Network'e erişmeye çalışan cihazda "**onur**" kullanıcısı oturum açmışsa ve eğer oturum kontrolü açıksa ve herhangi bir cihazda 2.oturumu açmışsa (Kural tanımına uyması için inputun içine 3 yazılması gerekmektedir.)

şeklinde kural tanımı yapabilirsiniz.

5.5. Active Directory

Kural tipi olarak "**Active Directory**" seçildiğinde;

Active Directory kullanıcıları üzerinde bulunan Özniteliklere göre (Custom Attribute) profil tanımı yapabilirsiniz. Öznitelik(Attribute) adı, Active Directory üzerinde bulunan öznitelik ismiyle aynı olmalıdır. Karşılığındaki değere göre kural tanımı belirleyebilirsiniz. Örneğin;

Attribute Adı: **department**

Değer: **Bilgi İşlem**

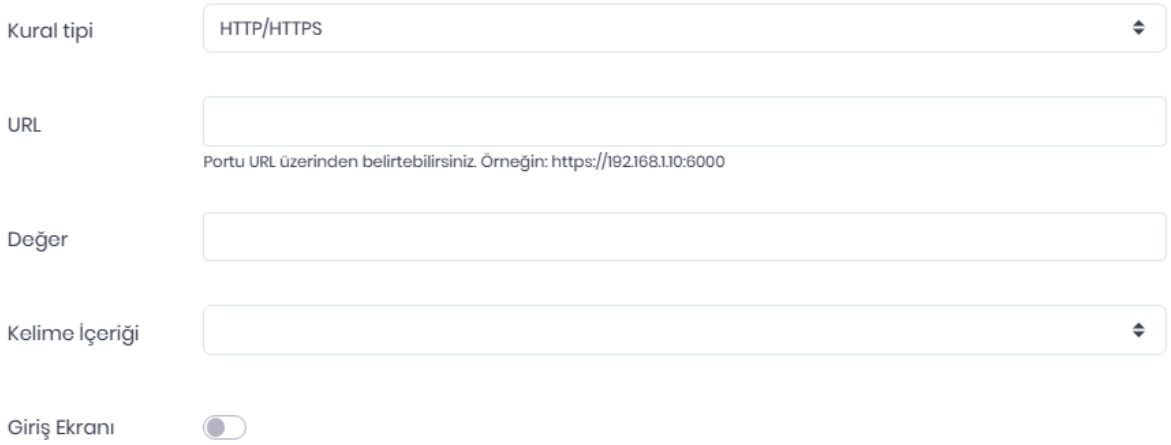
Kelime İçeriği: **Eşitse**

- Network'e erişmeye çalışan cihazda "**onur**" kullanıcısı oturum açmışsa ve "**onur**" kullanıcısının department özniteliği "**Bilgi İşlem**" yazısına eşitse

şeklinde kural tanımı yapabilirsiniz.

5.6. HTTP/HTTPS

Kural tipi olarak "**HTTP/HTTPS**" seçildiğinde ilgili cihazın eğer web arayüzü varsa (80/443), arayüzü tarayıp içeriğinde geçen kelimelere göre profil tanımlaması yapabilirsiniz.



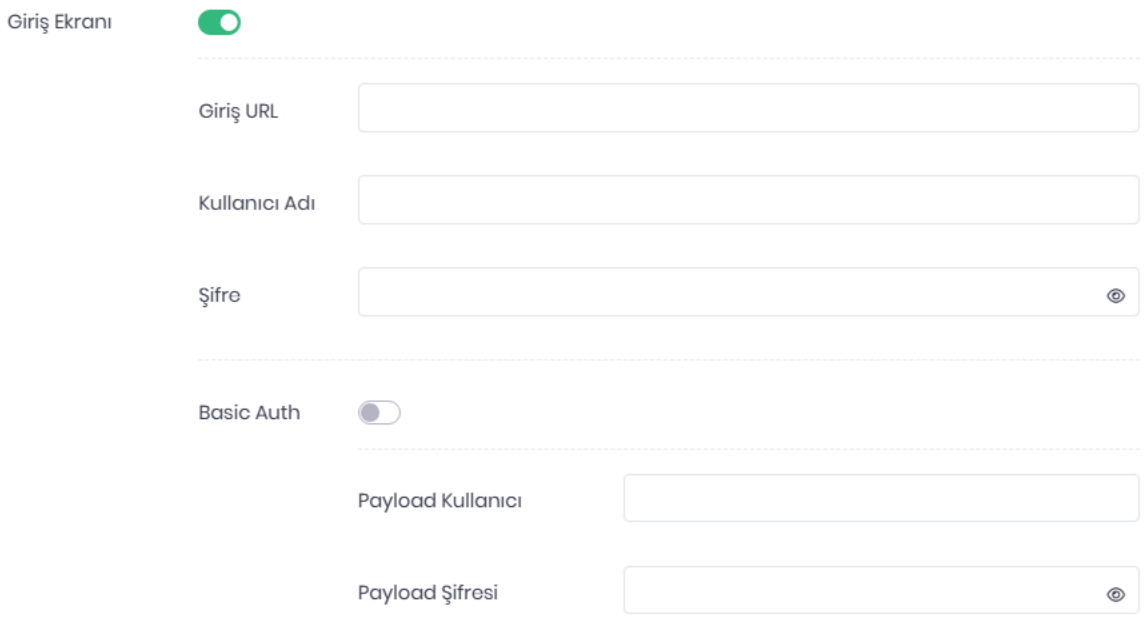
URL: Eğer profillemek istediğiniz cihazın özel bir URL adresi varsa buraya girebilirsiniz. Eğer yoksa "/" girmeniz yeterli olacaktır.

Değer: Web arayüz tarandıktan sonra aranmak istenen değer buraya girilir.

Kelime İçeriği: Yine Eşitse, İçeriyorsa, ile Başlıyorsa, ile Bitiyorsa alt kural seçilmelidir.

Giriş Ekranı: Açık/Kapalı

Taranmak istenen web arayüzüne Kullanıcı Adı ve Şifre ile giriş yapıldıktan sonra işlemlere devam edilmesi gerekiyorsa "Giriş Ekranı" bölümünü açıp aşağıdaki ayarları yapabilirsiniz;



Giriş URL: Kullanıcı girişi yapılacak URL (Örneğin: login.php)

Kullanıcı Adı: Sayfaya giriş yapacak Kullanıcı Adı

Şifre: Sayfaya giriş yapacak Şifre

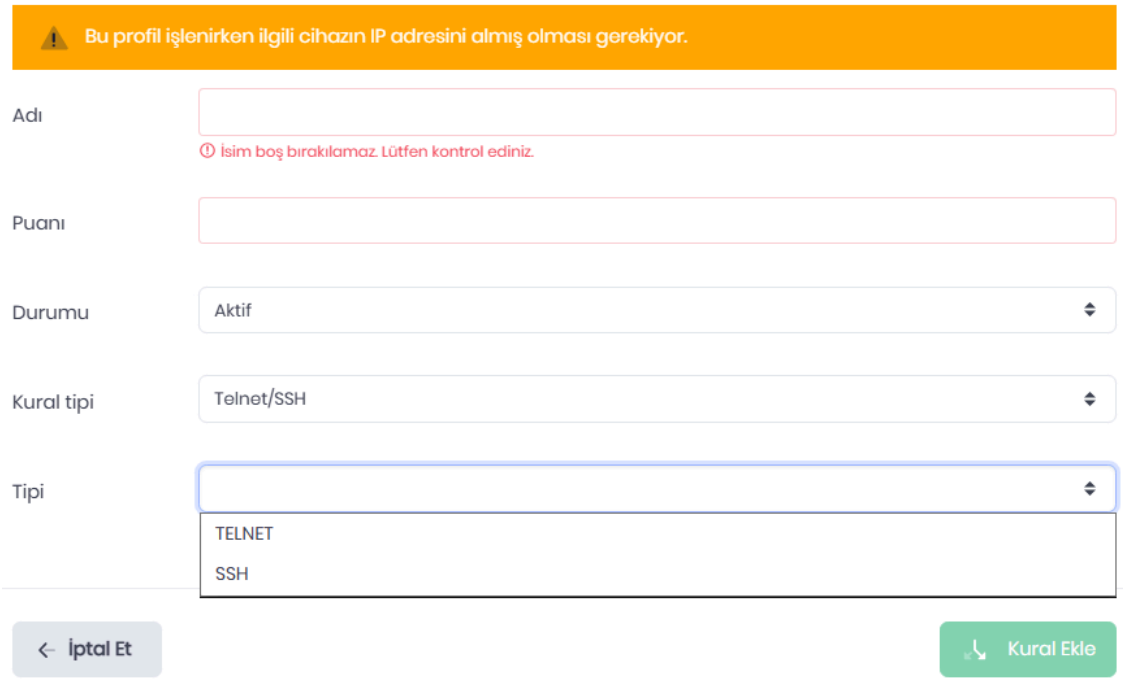
Basic Auth: Açık/Kapalı

Basic Authentication, HTTP protokolünde kullanılan en basit kimlik doğrulama yöntemlerinden biridir. Eğer taranmak istenen web arayüzü Basic Authentication kullanıyorsa bu ayarı açtığınızda form üzerinde bulunan Kullanıcı Adı ve Şifre kullanılarak Basic Authentication denemesi yapılır.

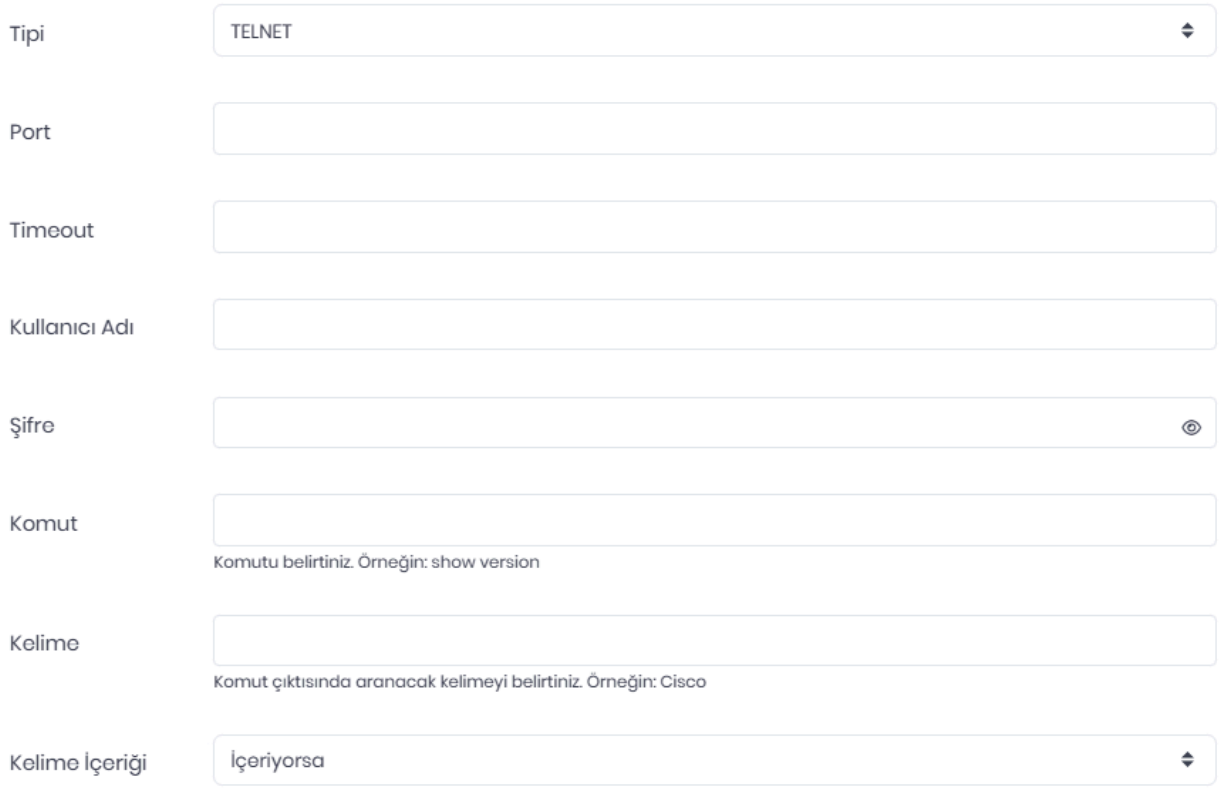
Eğer Basic Authtentication yoksa ilgili ayar Kapalı duruma getirilir. Sayfaya giriş yapılacak kullanıcı bilgileri Payload Username ile Payload Password bölümüne yazılması gerekir.

5.7. Telnet/SSH

Kural tipi olarak "**Telnet/SSH**" seçildiğinde;



5.7.1. Telnet



Port: Telnet port bilgisi (Varsayılan port 23'tür.)

Timeout: Bağlantı zaman aşımı süresi (Belirtilmezse 30 saniyedir)

Kullanıcı Adı: Telnet bağlantısı için gerekli kullanıcı adı

Şifre: Telnet bağlantısı için gerekli şifre

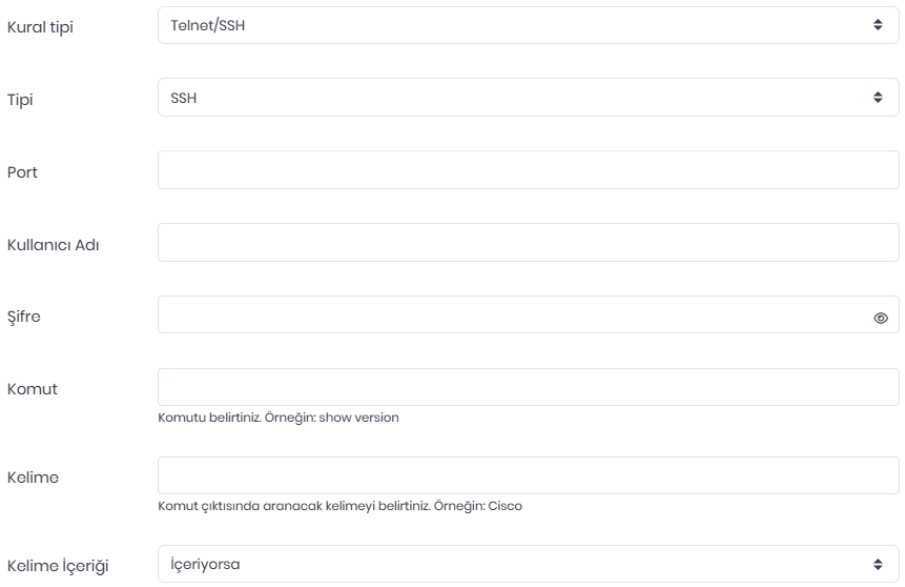
Komut: Telnet bağlantısı yapıldıktan sonra çalıştırılacak komut

Kelime: Çalıştırılan komut sonrasında aranan çıktı

Kelime İçeriği: Yine Eşitse, İçeriyorsa, ile Başlıyorsa, ile Bitiyorsa alt kural seçilmelidir.

Çalışma mantığı; ilgili cihaza verilen bilgilerle telnet üzerinden erişerek belirtilen komutun çıktısı sonucunda aranan kelimeye göre kural yazabilirsiniz.

5.7.2. SSH



Port: Telnet port bilgisi (Varsayılan portu 22'dir)

Timeout: Bağlantı zaman aşımı süresi (Belirtilmezse 30 saniyedir)

Kullanıcı Adı: Telnet bağlantısı için gerekli kullanıcı adı

Şifre: Telnet bağlantısı için gerekli şifre

Komut: Telnet bağlantısı yapıldıktan sonra çalıştırılacak komut

Kelime: Çalıştırılan komut sonrasında aranan çıktı

Kelime İçeriği: Yine Eşitse, İçeriyorsa, ile Başlıyorsa, ile Bitiyorsa alt kural seçilmelidir.

Çalışma mantığı; ilgili cihaza verilen bilgilerle SSH üzerinden erişerek belirtilen komutun çıktısı sonucunda aranan kelimeye göre kural yazabilirsiniz.

5.8. DHCP Fingerprint

Kural tipi olarak "**DHCP Fingerprint**" seçildiğinde;

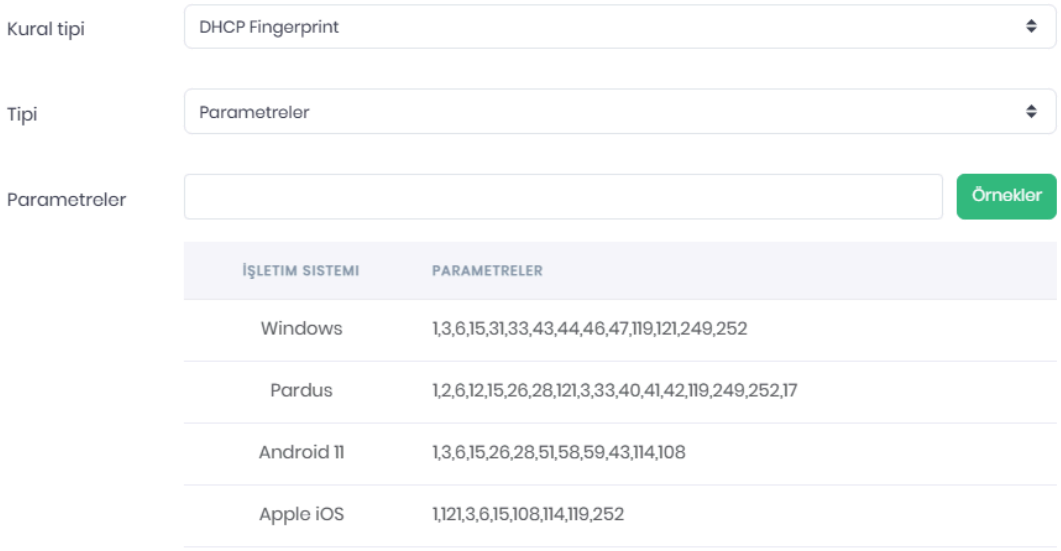
5.8.1. Üretici Bilgisi

DHCP Fingerprint çıktısındaki üretici bilgisine göre kural tanımı yapabilirsiniz.

5.8.2. Cihaz Adı (Hostname)

DHCP Fingerprint çıktısındaki cihaz adına (hostname) göre kural tanımı yapabilirsiniz.

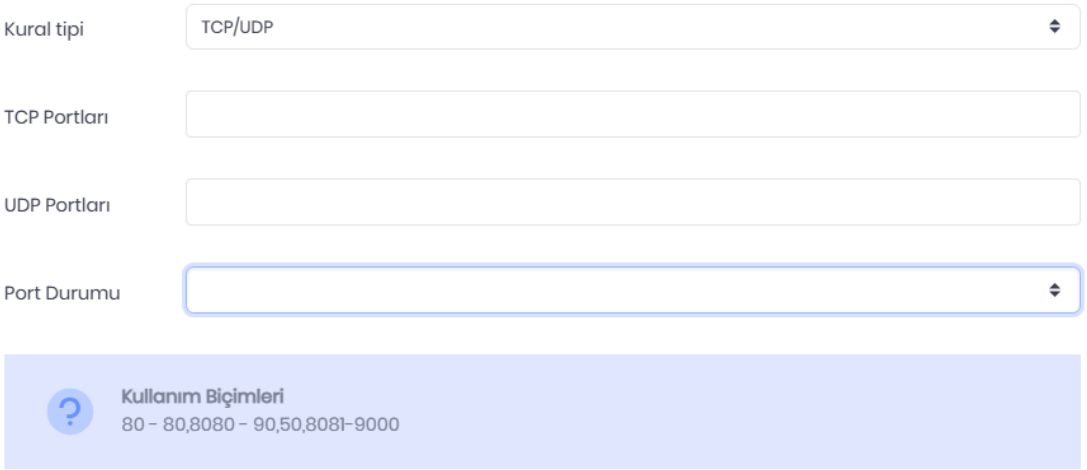
5.8.3. Parametreler



DHCP Fingerprint çıktısındaki parametrelere göre kural tanımı yapabilirsiniz.

5.9. TCP/UDP Port

Kural tipi olarak "**TCP/UDP Port**" seçildiğinde;



İlgili cihazın yukarda belirtilen TCP / UDP portlarının durumuna göre profil tanımı yapabilirsiniz. Port Durumları;

- Open (Açık)
- Closed (Kapalı)
- Open Filtered (Filtreli şekilde Açık)

Port tanımlamalarını yaparken tekil olarak port numarası (Örneğin: 80), birden fazla portta tarama yapmak için aralarında virgül ile (Örneğin: 80,8080), Port aralığını aramak için de arasına tire koyarak (Örneğin: 80-8080 arası) kural tanımlamasını yapabilirsiniz.

5.10. SNMP

Kural tipi olarak "**SNMP**" seçildiğinde;

Belirtilen SNMP OID'inin çıktısında gelen değerin içeriğine göre profil tanımı yapabilirsiniz. SNMPv1, SNMPv2c ve SNMPv3 desteği sunmaktadır. SNMPv3 için kabul edilen seçenekler;

Tip olarak noAuthNoPriv, authNoPriv, authPriv desteği sunulmaktadır.

Auth tip olarak: No Auth Protocol, MD5, SHA128, SHA256, SHA384, SHA512 desteği sunmaktadır.

Priv tip olarak: No Priv Protocol, DES, AES 128, AES 192, AES 256 desteği sunmaktadır.

Örneğin girilen SNMP bilgilerine göre 1.3.6.1.2.1.1.1 (SNMP sysdesrc OID) OID'ine atılan istek karşılığında eğer içeriğinde "Cisco" geçiyorsa şeklinde bir kural tanımı yapabilirsiniz.

Not: SNMP OID'lerine internet üzerinden arama yaparak ulaşabilirsiniz.

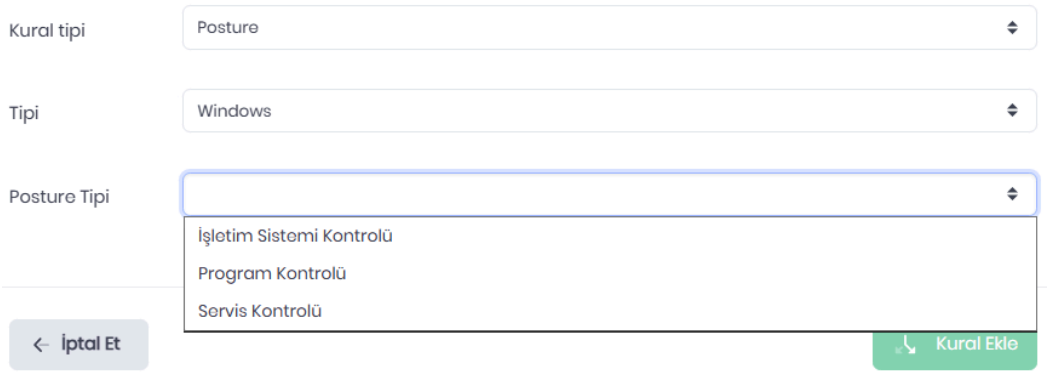
5.11. Posture

Kural tipi olarak "**Posture**" seçildiğinde;

Windows, Linux, Dosya Takibi, Oturum Takibi gibi özellikleri kullanarak kural tanımları gerçekleştirebilirsiniz.

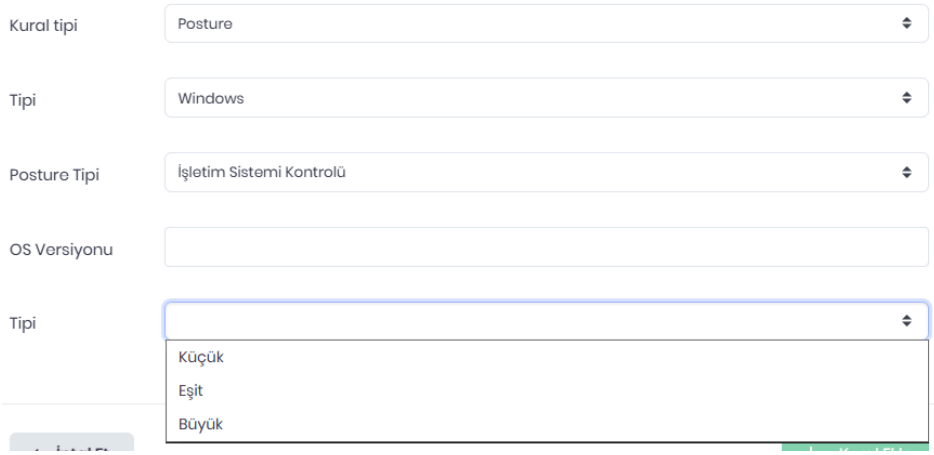
5.11.1. Windows

Kural tipi olarak "**Windows**" seçildiğinde;



5.11.1.1. İşletim Sistemi Kontrolü

Posture tipi olarak "**İşletim Sistemi**" Kontrolü seçildiğinde;



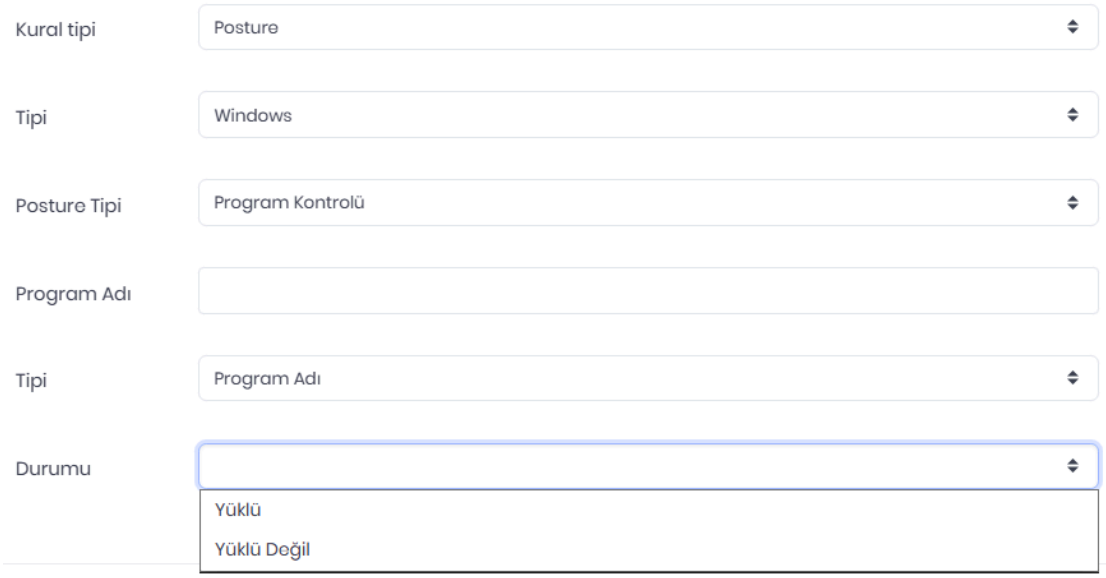
İşletim sistemi versiyonu "**OS Versiyonu**" inputuna yazdığınız versiyondan "**Küçük**, **Eşit**, **Büyük**" ise şeklinde kural tanımı yapabilirsiniz.

5.11.1.2. Program Kontrolü

Posture tipi olarak "**Program Kontrolü**" seçildiğinde;

5.11.1.2.1. Program Adı

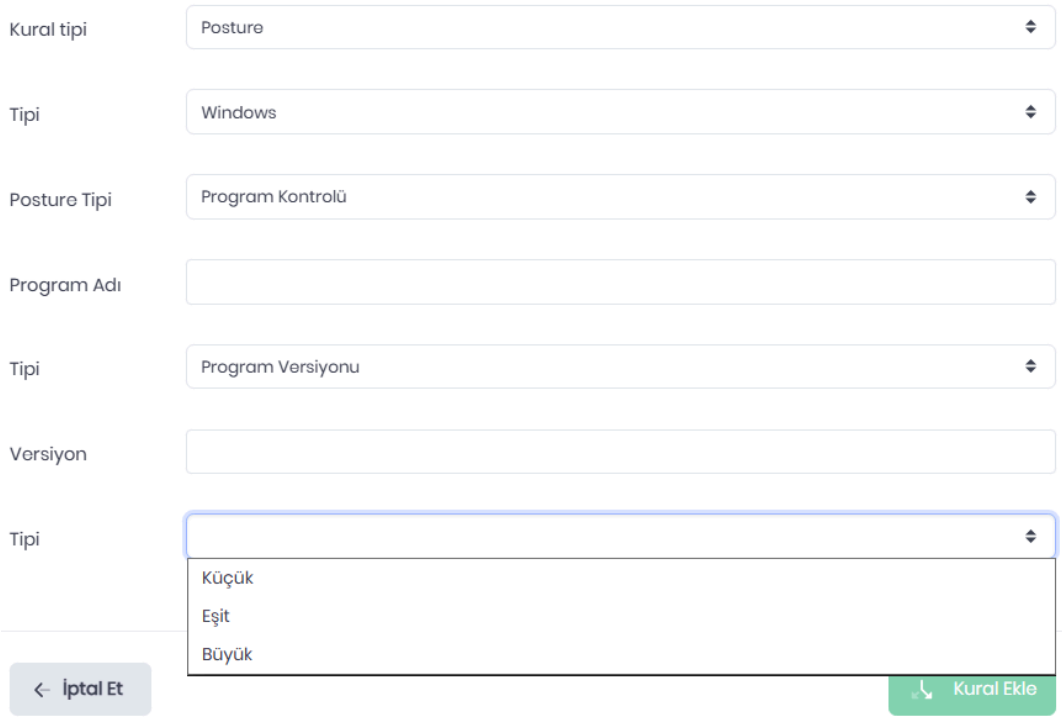
Alt kural tipi "**Program Adı**" olarak seçildiğinde;



"**Program Adı**" inputuna yazdığınız program kontrol edilen cihazda "**Yüklü**" veya "**Yüklü Değil**" şeklinde bir kural tanımı yapabilirsiniz.

5.11.1.2.2. Program Versiyonu

Alt kural tipi "**Program Versiyonu**" olarak seçildiğinde;



"**Program Adı**" inputuna yazılan programın versiyonu "**Versiyon**" inputuna yazacağınız değerden "**Küçük**, **Eşit**, **Büyük**" şeklinde kural tanımı yapabilirsiniz.

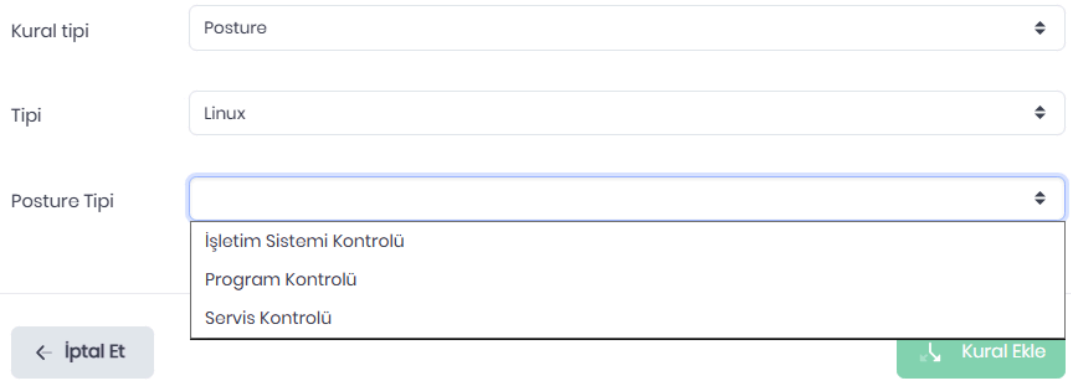
5.11.1.3. Servis Kontrolü

Posture tipi olarak "**Servis Kontrolü**" seçildiğinde;

"Servis Adı" yazan inputa yazacağınız servisin "Çalışıyor (Running)" veya "Çalışmıyor (Not Running)" durumuna göre kural tanımı yapabilirsiniz.

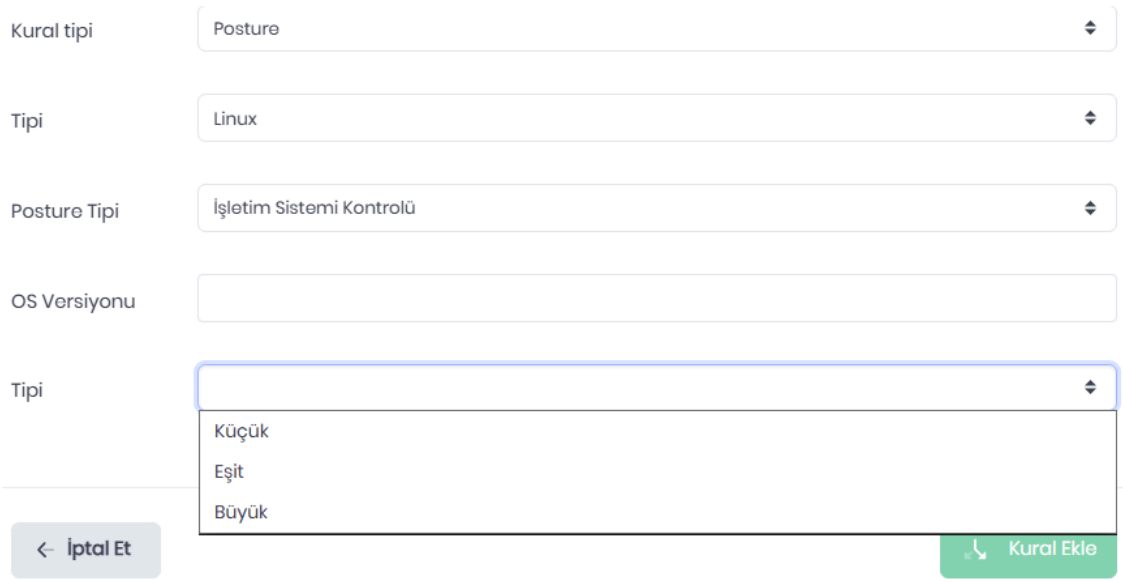
5.11.2. Linux

Kural tipi olarak "**Linux**" seçildiğinde;



5.11.2.1. İşletim Sistemi Kontrolü

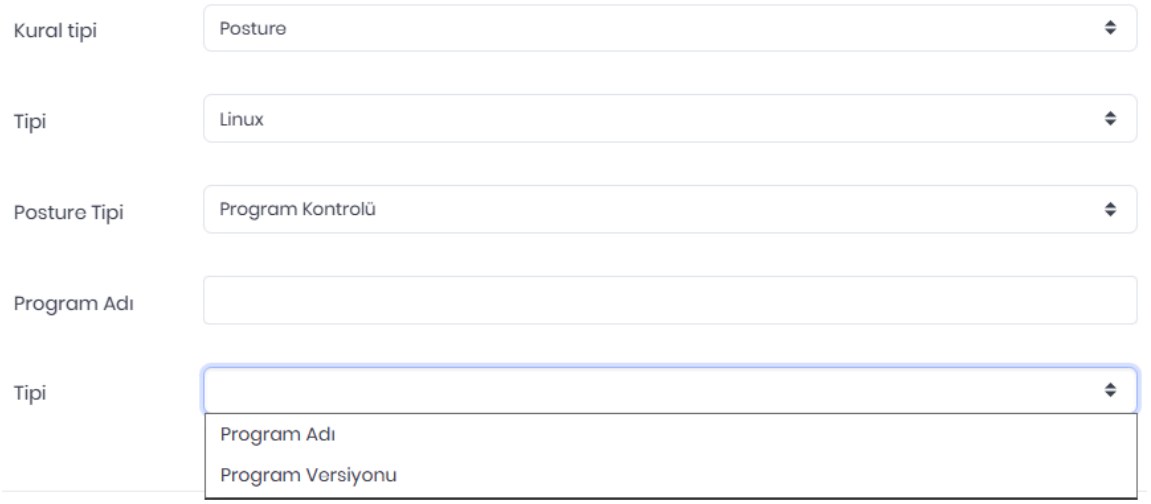
Posture tipi olarak "**İşletim Sistemi**" Kontrolü seçildiğinde;



İşletim sistemi versiyonu "**OS Versiyonu**" inputuna yazdığınız versiyondan "**Küçük**, **Eşit**, **Büyük**" ise şeklinde kural tanımı yapabilirsiniz.

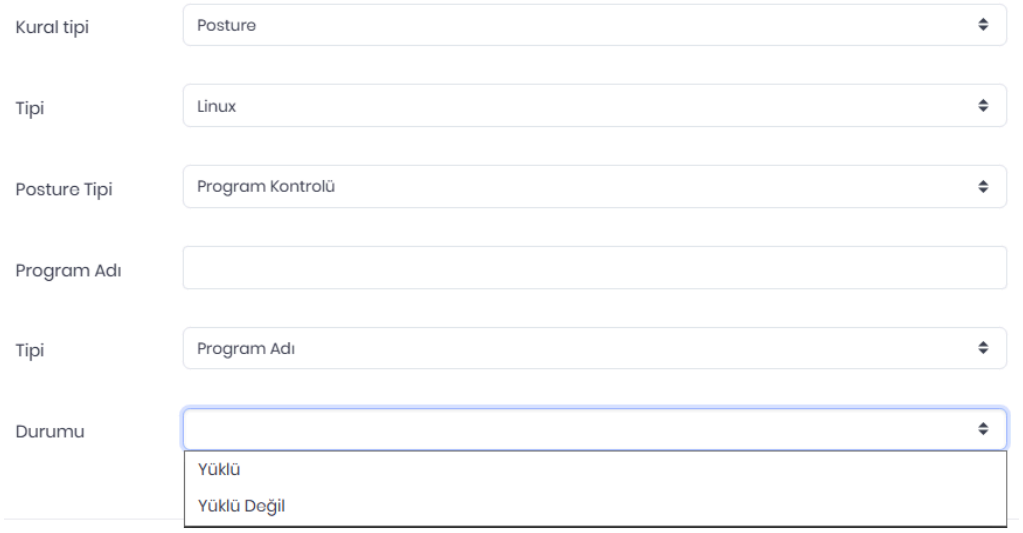
5.11.2.2. Program Kontrolü

Posture tipi olarak "**Program Kontrolü**" seçildiğinde;



5.11.2.2.1. Program Adı

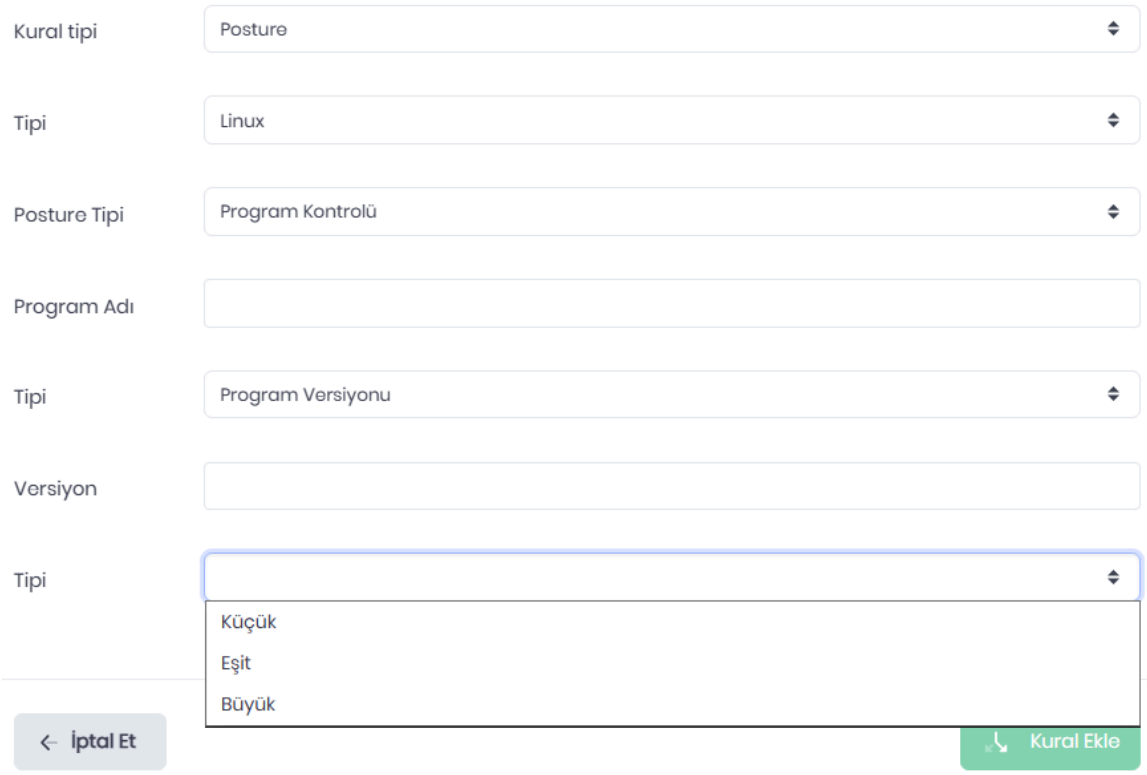
Alt kural tipi "**Program Adı**" olarak seçildiğinde;



"**Program Adı**" inputuna yazdığınız program kontrol edilen cihazda "**Yüklü**" veya "**Yüklü Değil**" şeklinde bir kural tanımı yapabilirsiniz.

5.11.2.2.2. Program Versiyonu

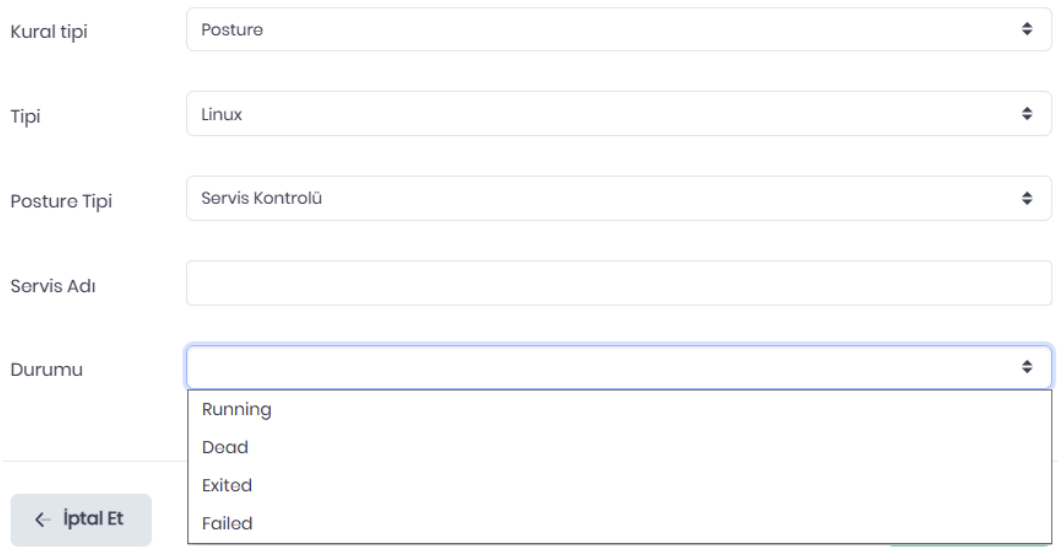
Alt kural tipi "**Program Versiyonu**" olarak seçildiğinde;



"**Program Adı**" inputuna yazılan programın versiyonu "**Versiyon**" inputuna yazacağınız değerden "**Küçük**, **Eşit**, **Büyük**" şeklinde kural tanımı yapabilirsiniz.

5.11.2.3. Servis Kontrolü

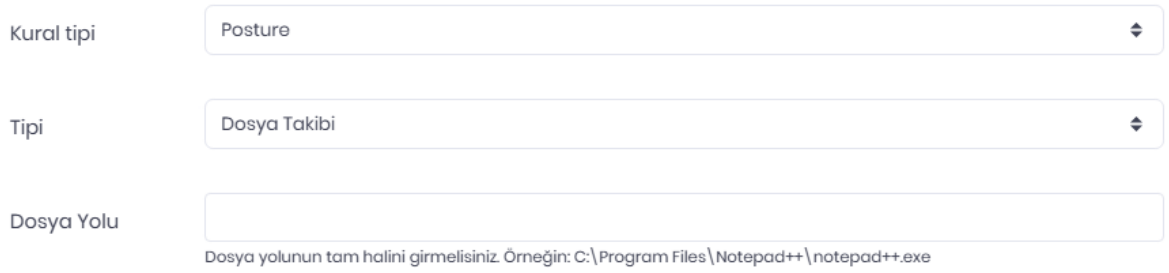
Posture tipi olarak "**Servis Kontrolü**" seçildiğinde;



"**Servis Adı**" yazan inputa yazacağınız servisin "**Çalışıyor** (**Running**)", "**Çalışmıyor** (**Dead**)", "**Çıkış Yaptı** (**Exited**)" ve "**Hatalı** (**Failed**)" durumuna göre kural tanımı yapabilirsiniz.

5.11.3. Dosya Takibi

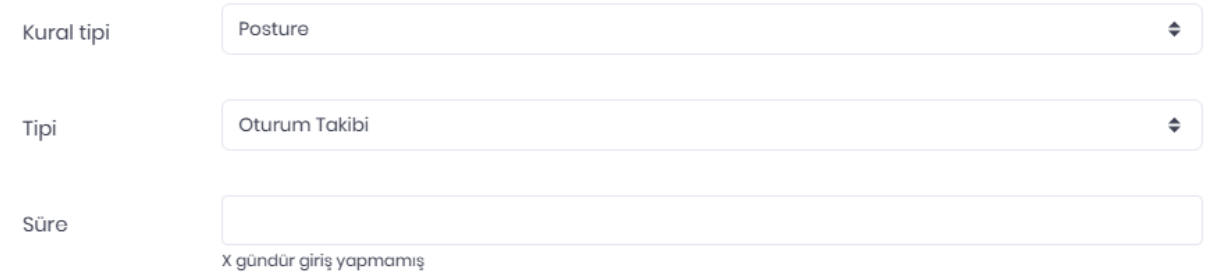
Kural tipi olarak "**Dosya Takibi**" seçildiğinde;



"**Dosya Yolu**" inputunda belirtilen dosyanın var olup olmadığını cihaz üzerinde kontrol et şeklinde kural tanımı yapabilirsiniz.

5.11.4. Oturum Takibi

Kural tipi olarak "**Oturum Takibi**" seçildiğinde;



Cihazda "**Süre**" inputunda belirtilen gün sayısına göre oturum açılmamışsa şeklinde kural tanımı yapabilirsiniz.

5.12. NMAP

Kural tipi olarak "**NMAP**" seçildiğinde;

cihazda "**Parametre**" bölümüne yazılan NMAP parametreleri kullanarak bir tarama başlatır ve "**Kelime**" inputuna yazılan çıktıyı arar. Örneğin Parametre inputuna "**-Pn -O**" yazdım ve Kelime inputuna da "**Windows**" yazdım;

- İlgili cihazda belirtilen parametrelerle NMAP taraması başlat ve çıktısında "**Windows**" yazısı geçiyorsa

şeklinde kural tanımı yapabilirsiniz.

6. Profil ve Skor Sistemi ve Örnekler

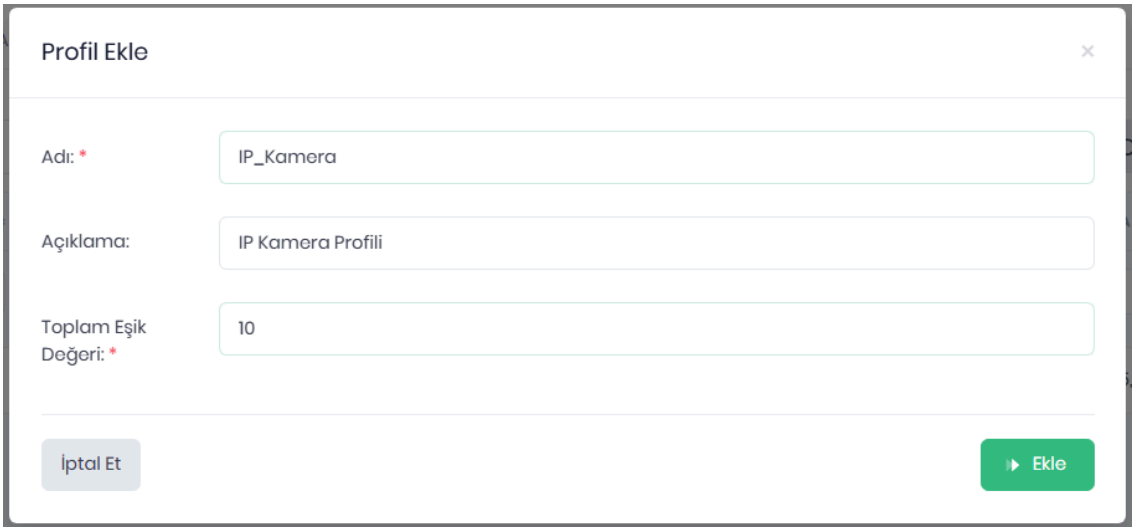
Yeni bir profil oluşturulduğunda sizden Toplam Eşik Değeri (Profil Skoru) istenmektedir;

Bu Profil Skoru, profilin detayına eklenilen profil kurallarının puan toplamına eşit veya üzeri şeklinde ayarlanmalıdır. Aşağıdaki verilen örnek kuralların detayları "**1.5 Profil Kural Tipleri**" başlığı altında detaylı bir şekilde anlatılmaktadır.

6.1. Örnek IP_Kamera Profili

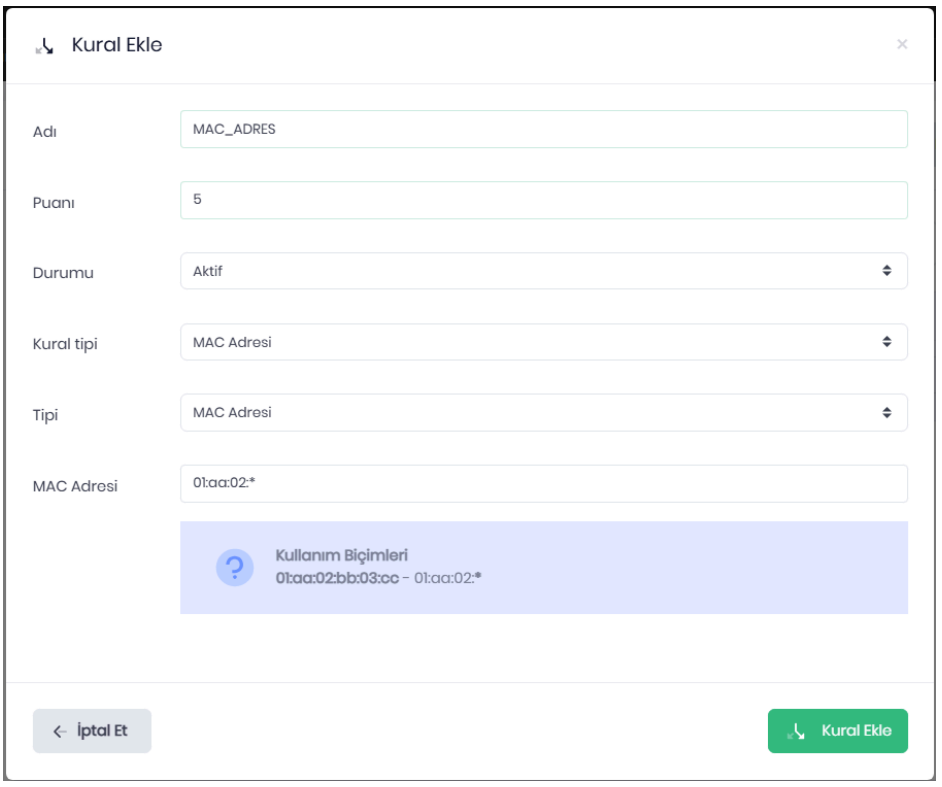
Profil Skor sistemini daha ayrıntılı anlamak için bir profil oluşturalım.

"**IP_Kamera**" adında Yeni bir Profil ekliyoruz ve Toplam Eşik Değeri puanını **10** olarak belirliyoruz;



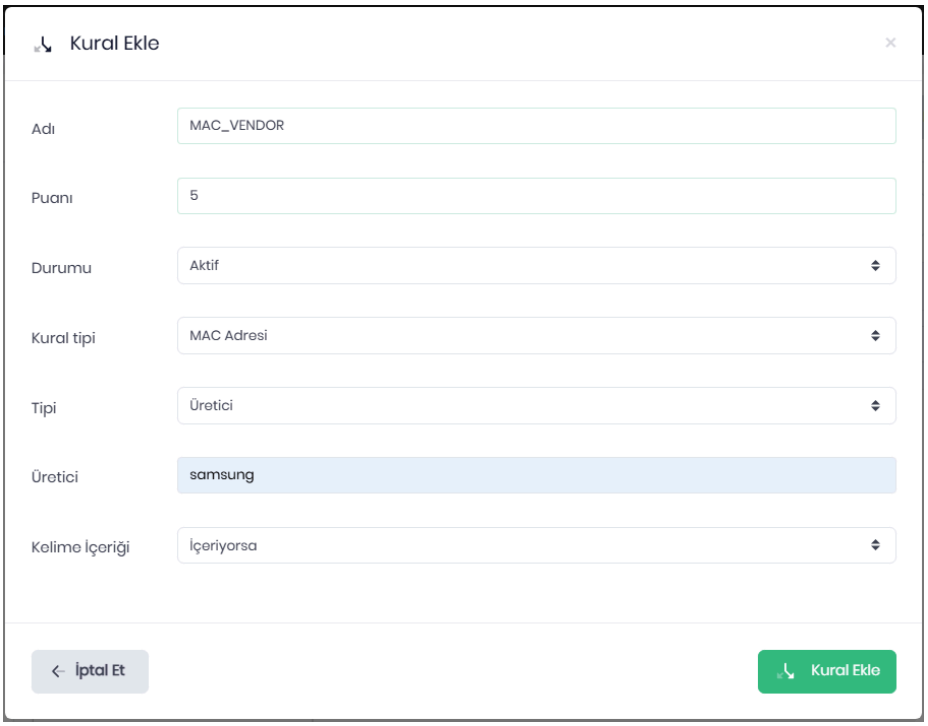
Şimdi oluşturduğumuz bu profile kural setleri ekleyerek Toplam Eşik Değeri puanını yakalamamız gerekiyor.

İlk kural olarak regex'li bir MAC adresi kural seti oluşturalım;



Yukardaki örneğe göre cihazın MAC adresi "**01:aa:02:***" ile başlıyorsa bu kural setinden 5 puan alacak şekilde yorumlanır.

Daha sonrasında yeni bir kural seti daha oluşturarak bu sefer Üretici seçelim;



Yukardaki örneğe göre cihazın MAC üretici bilgisi "**samsung**" içeriyorsa bu kural setinden 5 puan daha alacak şekilde yorumlanır.

"**IP_Kamera**" profilinin Profil skorunu **10** olarak belirlemiştik. Eğer yukarda yazdığımız 2 kural setine çarpan bir cihaz olursa ilgili cihaza artık "**IP_Kamera**" profiline uyan bir cihaz diyebiliriz. Yorumlamak gerekirse;

Network'e erişmeye çalışan cihazın;

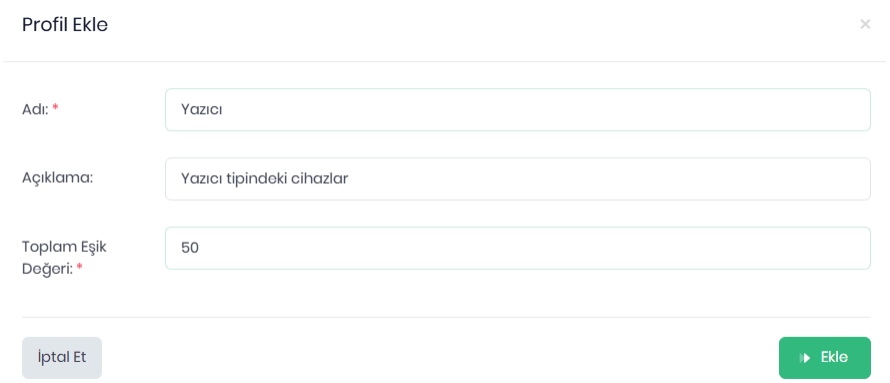
- MAC adresi "**01:aa:02:***" ile başlıyorsa 5 puan,
- MAC üretici bilgisi "**samsung**" içeriyorsa 5 puan daha alacak.

Yani toplamda kural setlerinden **10** puan'a sahip olacak ve "**IP_Kamera**" profiline uyan bir cihaz olacak.

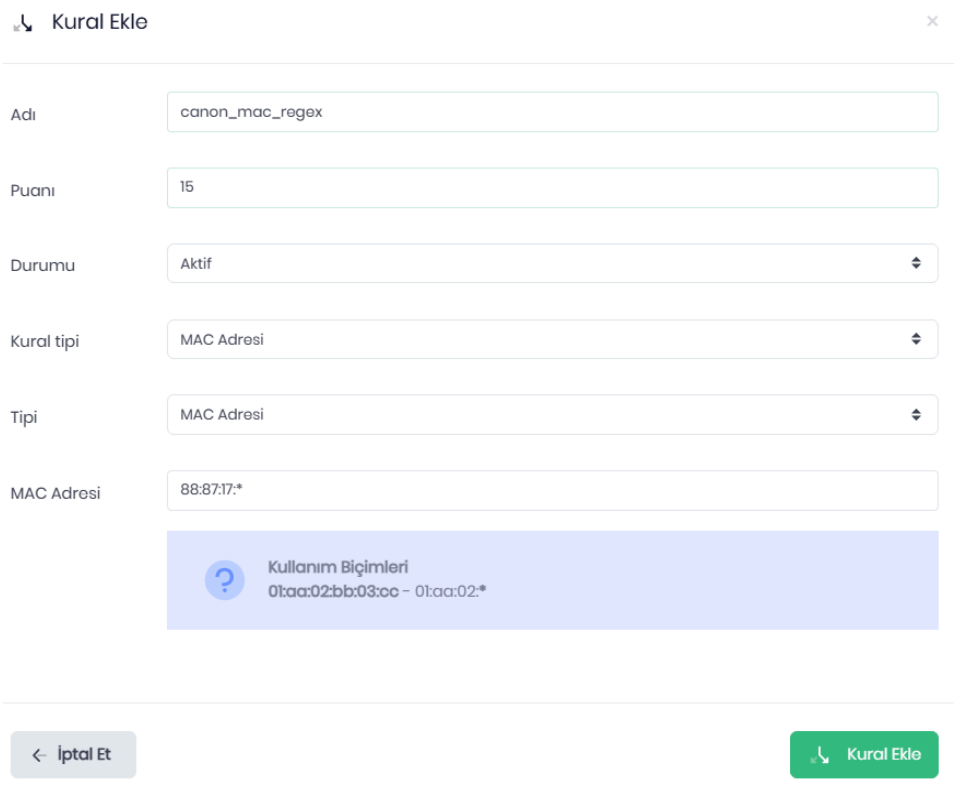
6.2. Örnek Yazıcı Profili

Bir örnek daha yaparak bu sefer bir Yazıcı profili oluşturalım.

"**Yazıcı**" adında Yeni bir Profil ekliyoruz ve Toplam Eşik Değeri puanını bu sefer **50** olarak belirliyoruz;



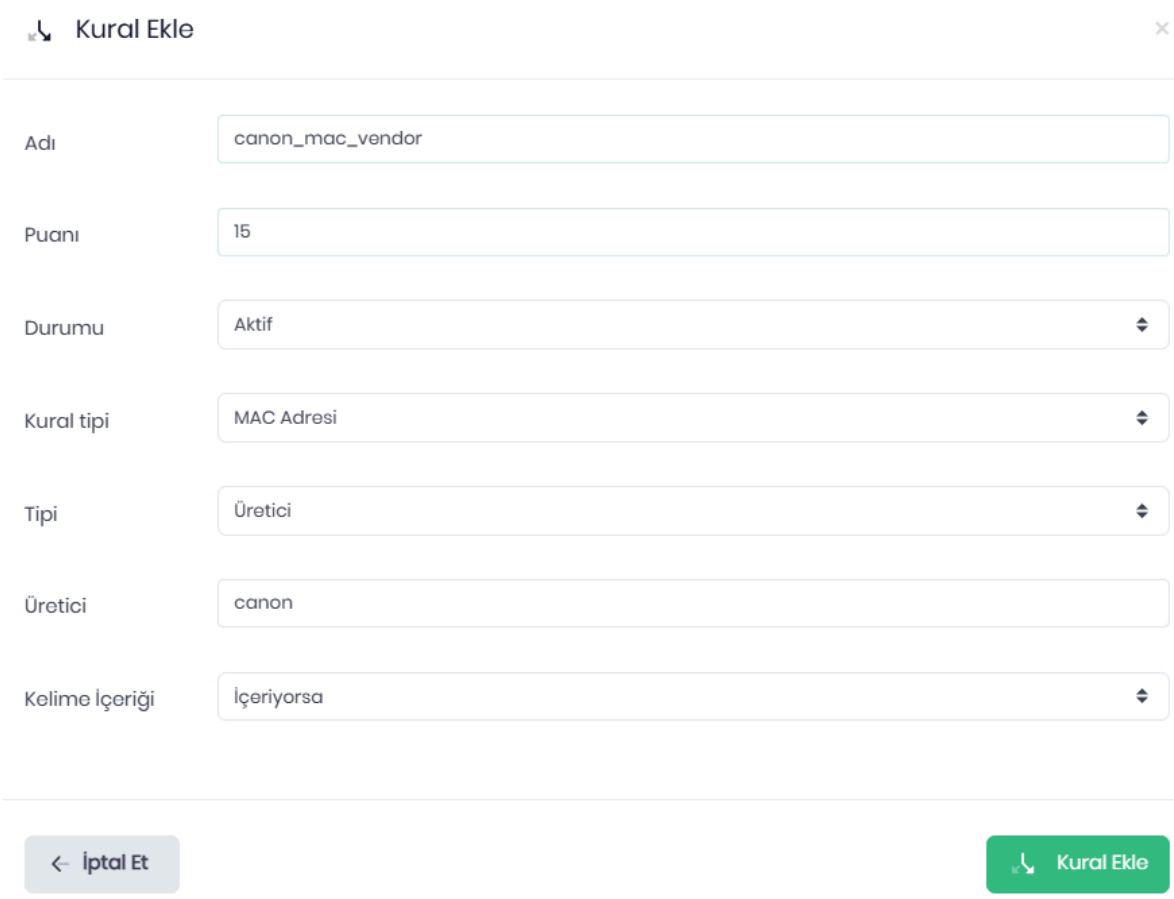
İlk kural olarak yine regex'li bir MAC adresi kural seti oluşturalım;



Eğer cihazın MAC adresi "**88:87:17:***" ile başlıyorsa kural setinden **15** puan alacak şeklinde yorumlayabiliriz.

Profil Skorunu **50** olarak belirtmiştik. Kuralımız işlerse cihaz **15** puan alacak ve cihaza **"Yazıcı"** profilindeki bir cihaz diyebilmemiz için **50-15=35** puanlık kural setleri daha gerekmektedir.

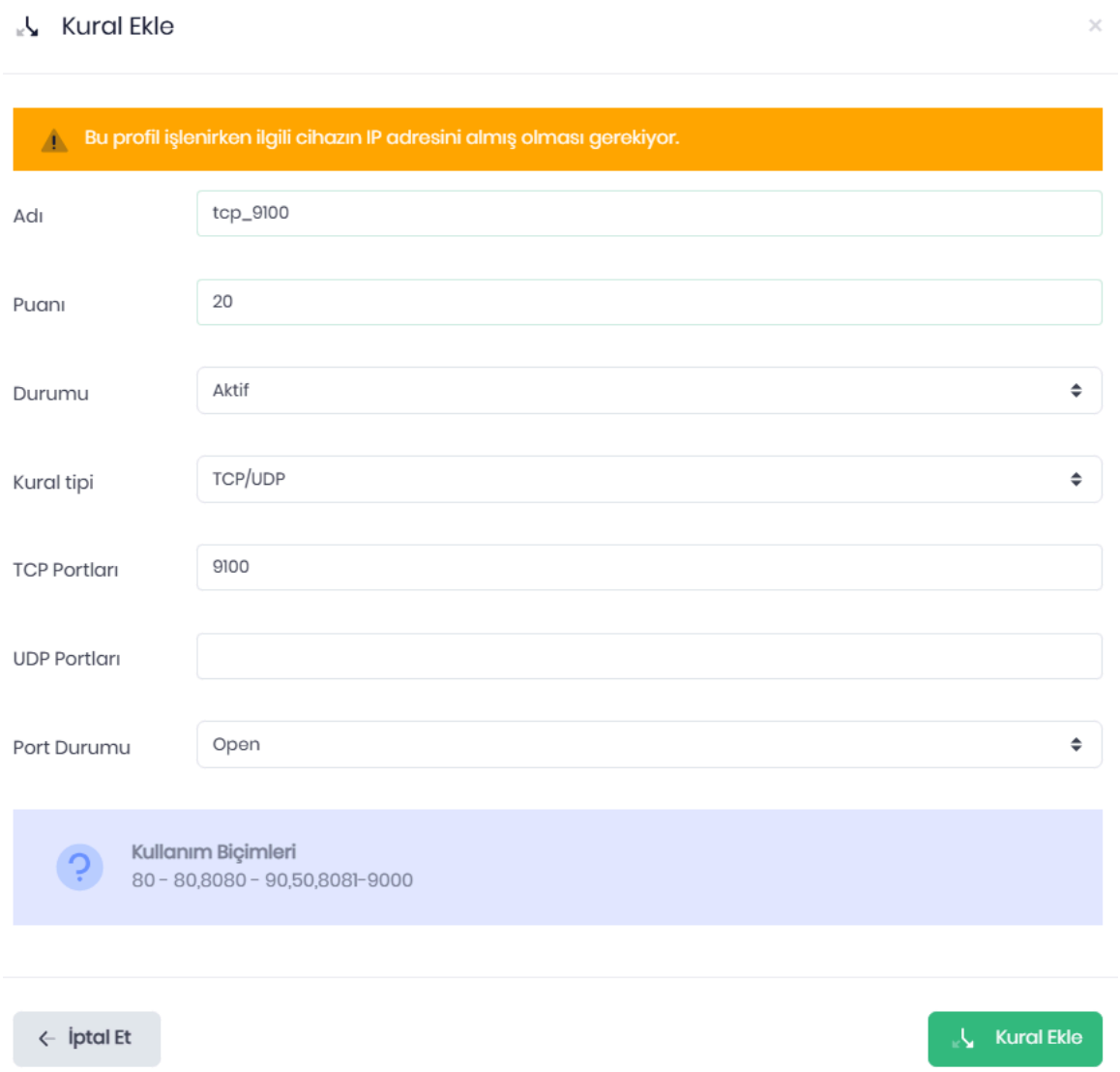
İkinci kural olarak MAC üretici bilgisi ekleyelim;



Eğer cihazın MAC üreticisi "**canon**" içeriyorsa kural setinden 15 puan alacak şeklinde yorumlayabiliriz.

Yine tekrar etmek gerekirse, Profil Skorunu **50** olarak belirtmiştik. Bize ilk kuralımız işlerse cihaz **15** puan alacak. İkinci kuralımızda işlerse **15** puan daha alacak ve toplamda **30** puan'a erişecek. Bizim **50** puana ihtiyacımız var ve **50-30=20** puanlık kural setleri daha gerekmektedir.

Devam edelim ve üçüncü kural olarak bu sefer TCP/UDP port bilgisi ekleyelim;



Eğer cihazın "**TCP 9100 portu açıksa**" (open) kural setinden de **20** puan alacak şeklinde yorumlayabiliriz.

Sonuç olarak Network'e erişmeye çalışan cihazın;

- MAC adresi "**88:87:17:***" ile başlıyorsa 15 puan,
- MAC üretici bilgisi "**canon**" içeriyorsa 15 puan,
- "**TCP 9100 portu açık**" ise 20 puan alacak.

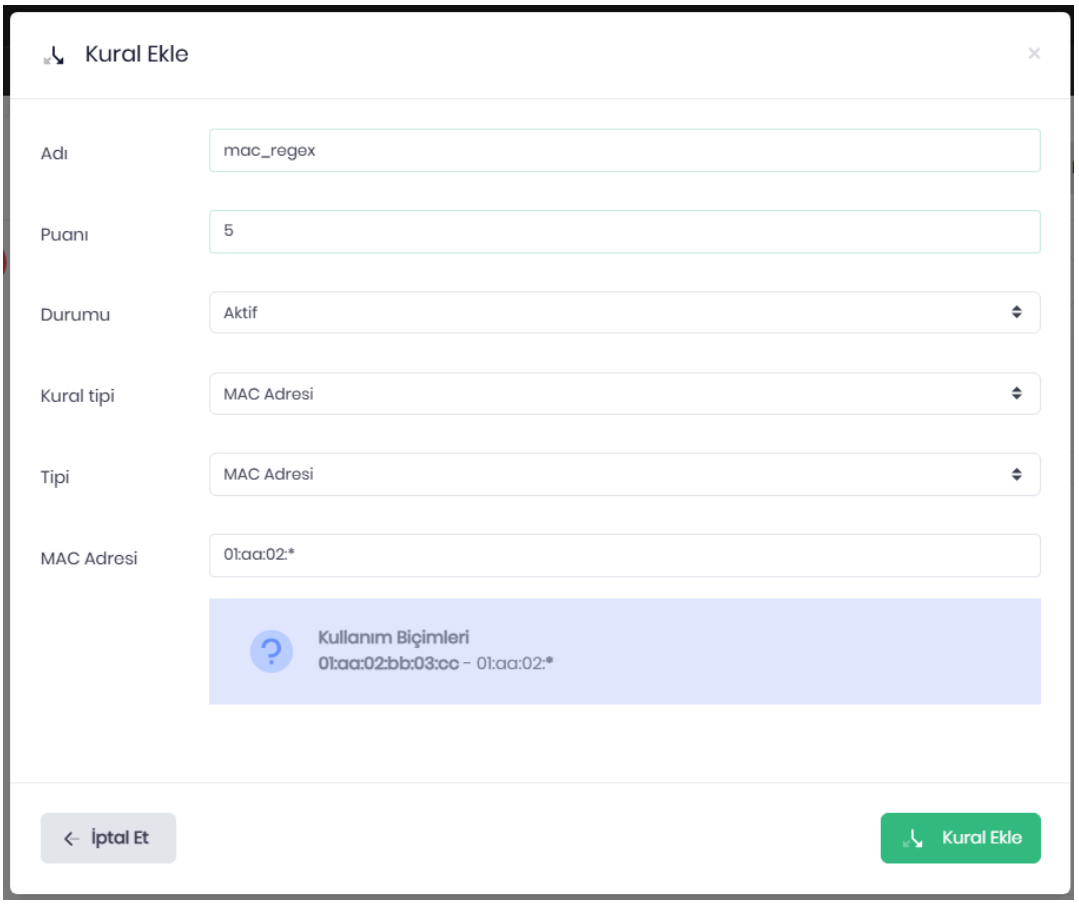
Toplamda **50** puana ulaşacak ve Yazıcı profiline uygun bir cihaz olarak tanımlanacaktır.

6.3. Örnek IoT Cihaz Profili

Bir örnek daha yaparak bu sefer daha kapsamlı ve sıkılaştırılmış bir profil oluşturalım.

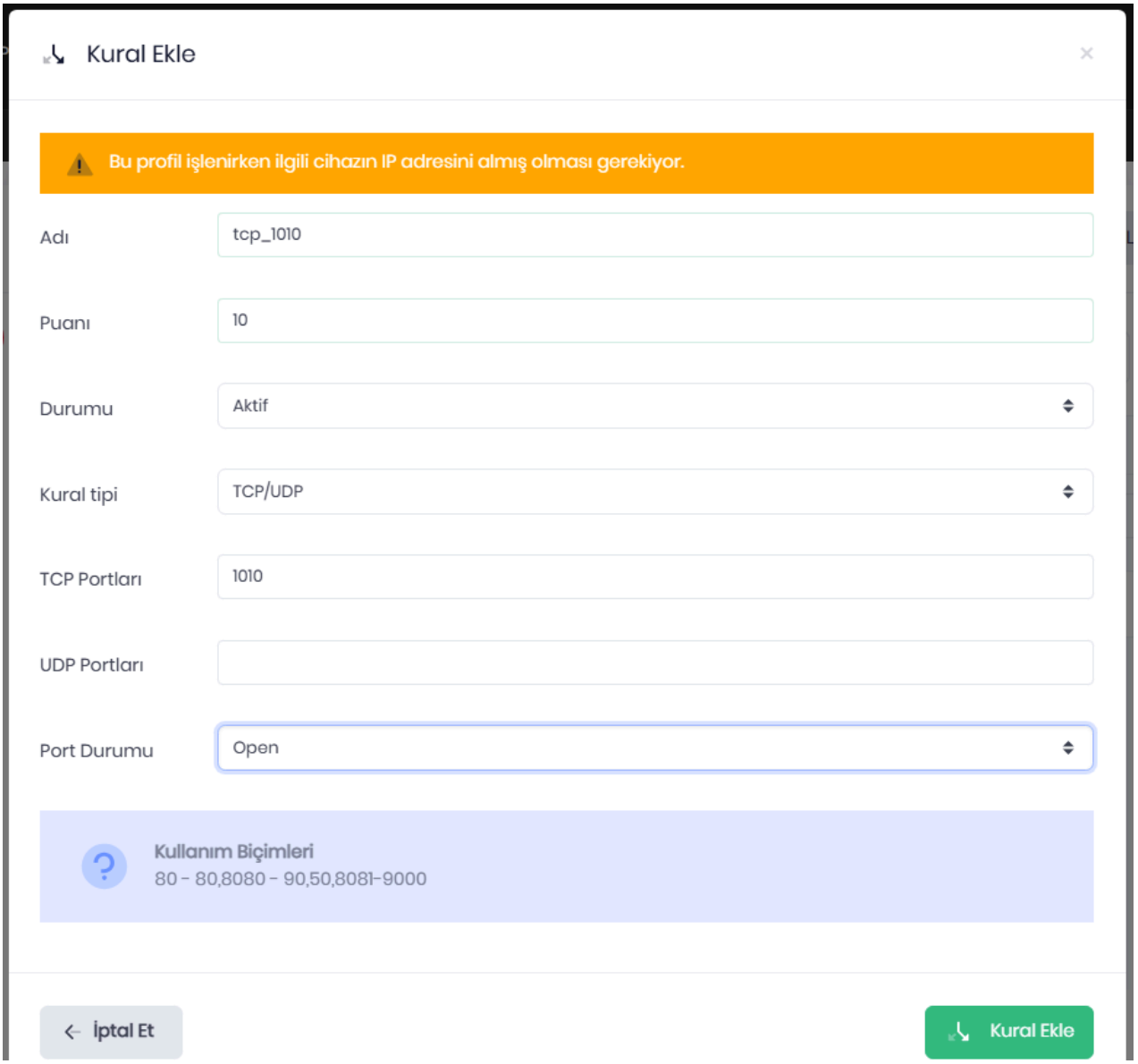
"**IoT**" adında Yeni bir Profil ekliyoruz ve Toplam Eşik Değeri puanını bu seferde **50** olarak belirliyoruz;

İlk kural olarak yine regex'li bir MAC adresi kural seti oluşturalım ve buna 5 puan verelim;



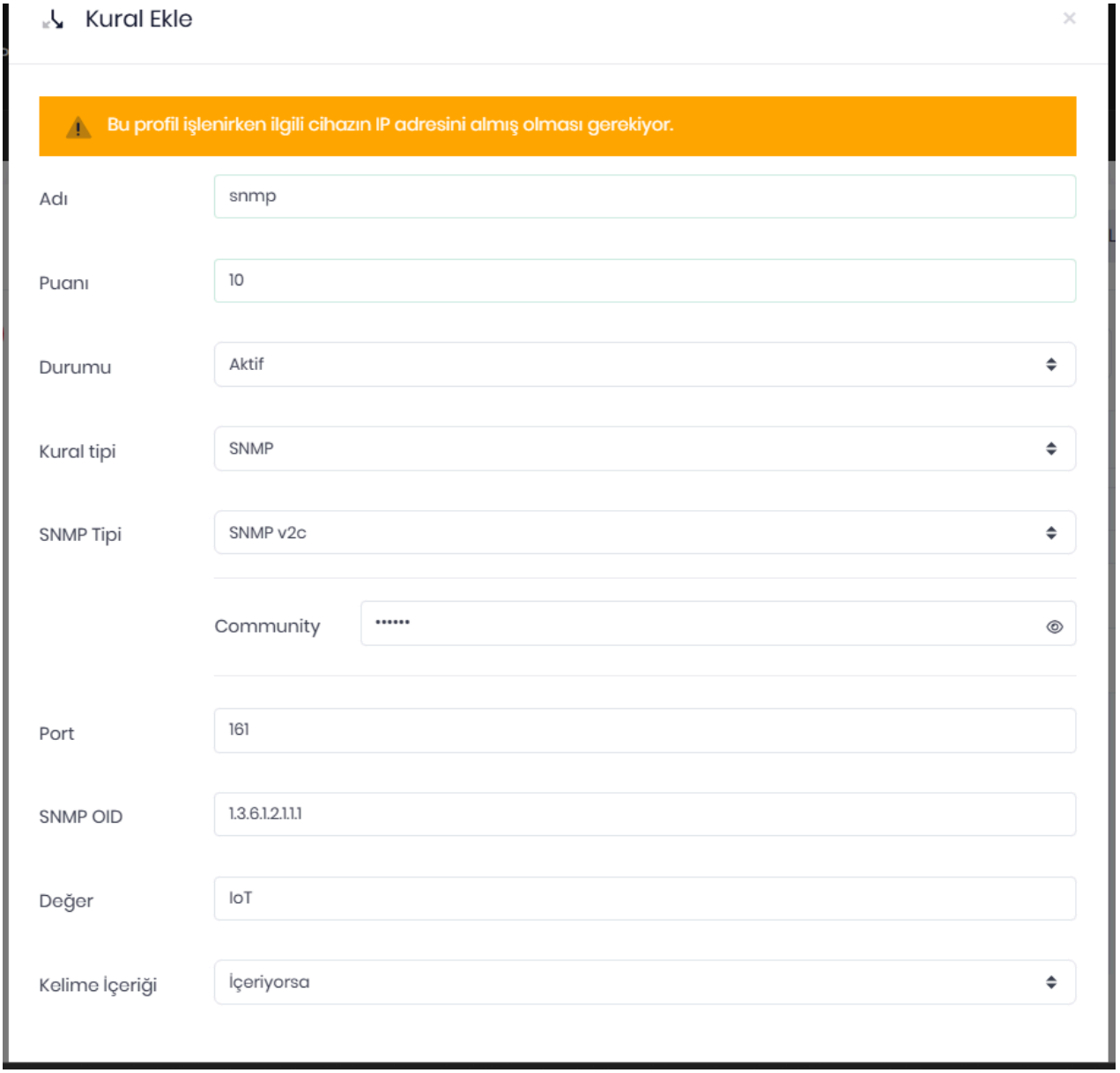
Cihazın MAC adresi "**01:aa:02:***" ile başlıyorsa 5 puan alacak.

Devam edelim ikinci kural olarak bu sefer **TCP 1010** portunun açık olması kuralını ekleyelim ve buna da 10 puan verelim;



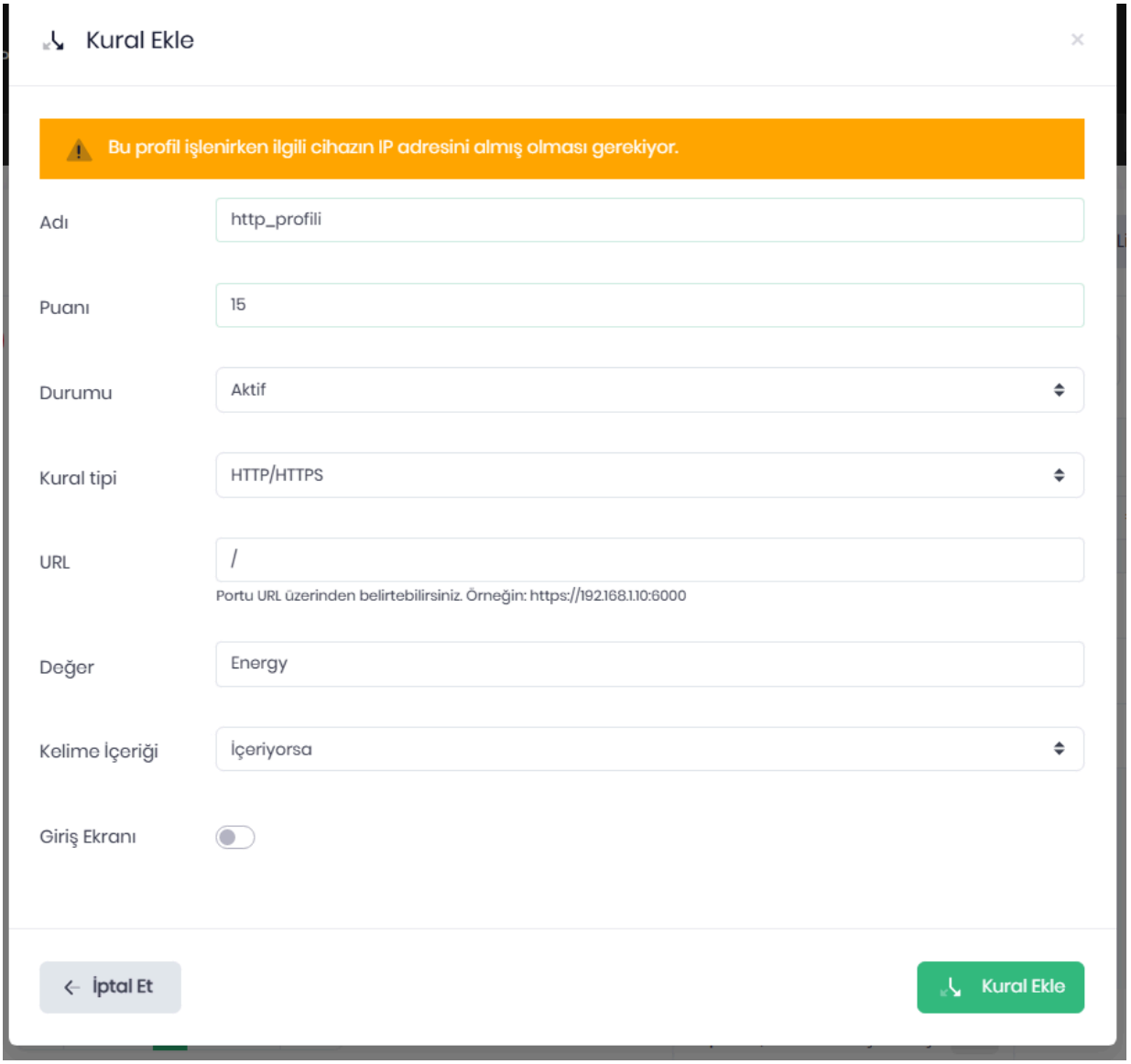
Cihazın **TCP 1010** portu açıksa buradan **10** puan alacak ve toplamda **15** puana erişecek.

Üçüncü kural olarakta bir SNMP kuralı yapalım ve buna da **10** puan verelim;



Cihaza **SNMPv2c** community ile **1.3.6.1.2.1.1.1** (SNMP sysdescr OID) istek atılacak ve cevabın içinde **IoT** geçiyorsa buradan da **10** puan alacak. Toplamda **25** puana erişecek.

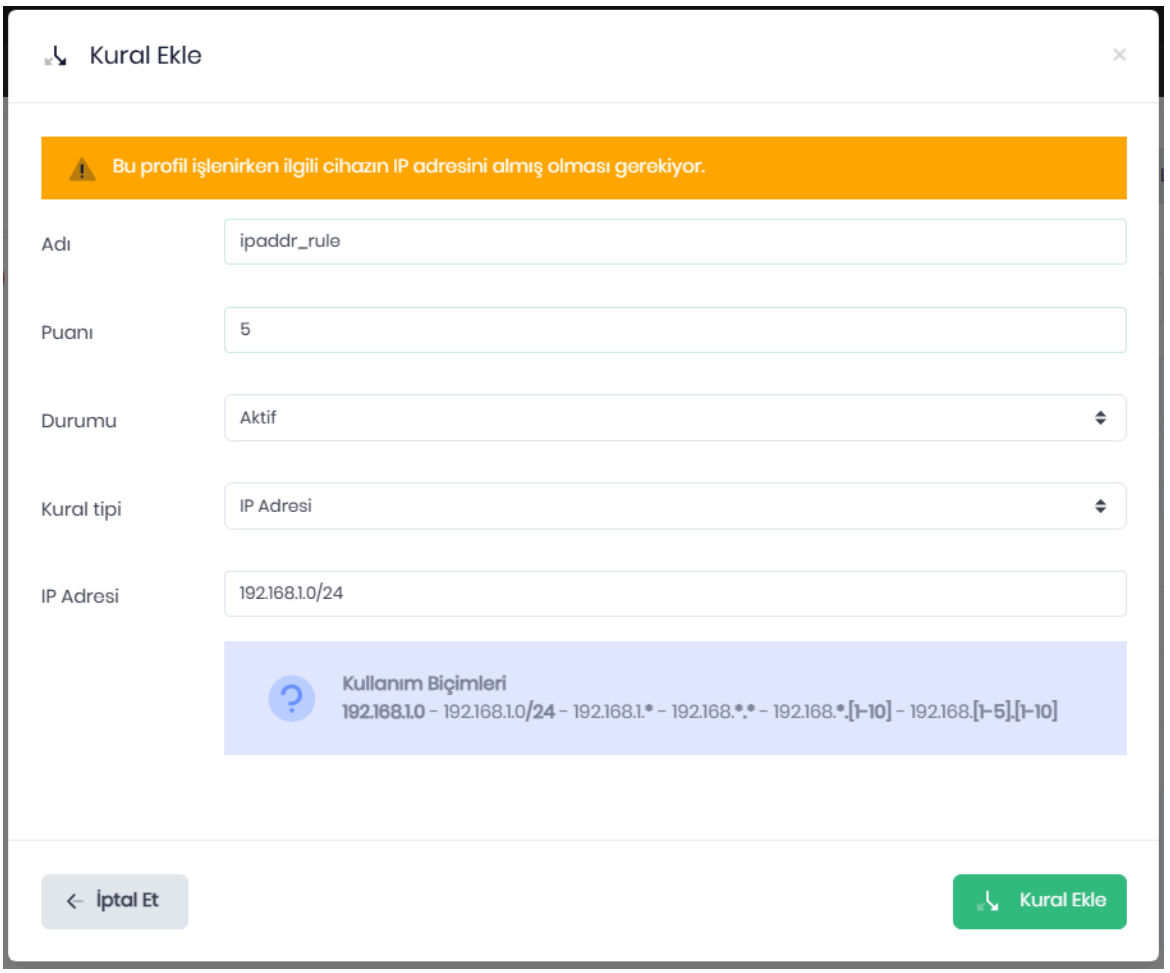
Unutmayın, profili eklerken **50** puan vermiştik. Şu an **25** puandayız. Devam edelim ve dördüncü kuralı HTTP/HTTPS olarak ekleyelim ve buna **15** puan verelim;



Cihazın web arayüzü taranacak ve içeriğinde "**Energy**" kelimesi geçiyorsa bu kuraldan da **15** puan daha alacak. Toplamda **45** puan'a ulaştık.

Cihaza IoT profilindeki bir cihaz diyebilmemiz için 5 puanlık kural setine ihtiyacımız kaldı.

Hemen beşinci kuralımızı ekleyelim. Bunun tipini de IP adresi olarak belirleyelim ve cihazın bir ip bloğunun içinde olması kuralını yapalım;



Cihazın IP adresi **192.168.1.0/24** network bloğu içindeyse bu kuraldan da **5** puan daha alacak. Toplamda **50** olacak.

Artık tüm kurallarımız hazır. Bir cihaza "**IoT**" profilinde diyebilmemiz için sıkı bir kural seti oluşturduk. Özetlemek gerekirse;

- Cihazın MAC adresi "**01:aa:02:***" ile başlıyorsa **5** puan,
- Cihazın "**TCP 1010 portu**" açıksa **10** puan,
- Cihazın **SNMPv2c** community ile "**1.3.6.1.2.1.1.1** (sysDescr)" SNMP OID'ine istek attığımızda gelen cevabın içinde "**IoT**" geçiyorsa **10** puan,
- Cihazın web arayüzü taranacak ve içeriğinde "**Energy**" kelimesi geçiyorsa **15** puan,
- Cihazın IP adresi "**192.168.1.0/24**" network bloğu içindeyse **5** puan alacak

toplamda **50** puana ulaşacak ve biz artık bu cihaza "**IoT**" profiline uygun bir cihaz olarak tanımlayacağız.

Cihaz profilleme ile ilgili tüm detayları öğrendik. Cihazlar profillendikten sonra aksiyon alma işlemi Politikalar üzerinden gerçekleşmektedir. Bunun için **politikalar.docx** dökümanını inceleyebilirsiniz.