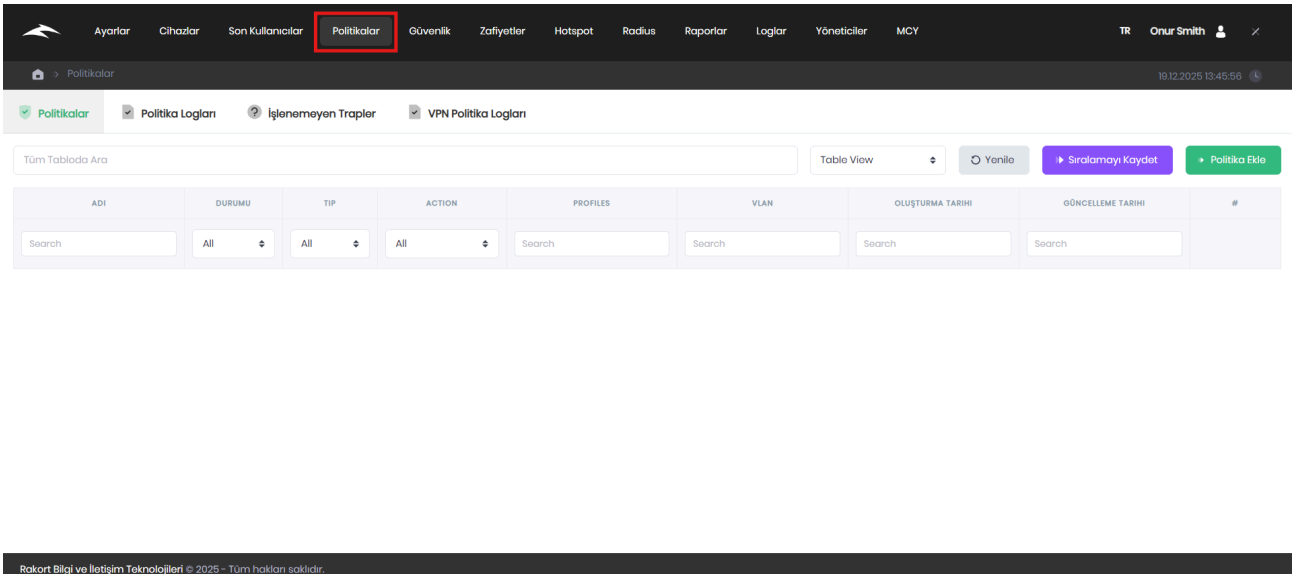
FastNAC

POLİTİKALAR

İçindekiler;

1.1) Başlangıç

Network'e bağlanan cihazlar ile ilgili alınacak aksiyon kararları ana menüde bulunan "**Politikalar**" bölümünden yapılmaktadır.



FastNAC üzerinde politikalar, aynı bir firewall kuralı gibi en üstten başlayarak kontrol edilir ve cihaz herhangi bir politikaya çarptığında, ilgili politikanın altındaki diğer politikalar kontrol edilmez. "**Politikalar**" sayfası üzerindeki tablonun içinde sürükle/bırak yaparak politika sıralamalarını değiştirebilirsiniz.

1.2) Politika Ekleme

"**Politikalar**" listesinde bulunan "**Politika Ekle**" butonuna basarak yeni bir politika oluşturabilirsiniz. Açılan pencerede;

Adı: Politikaya verilecek bir isim

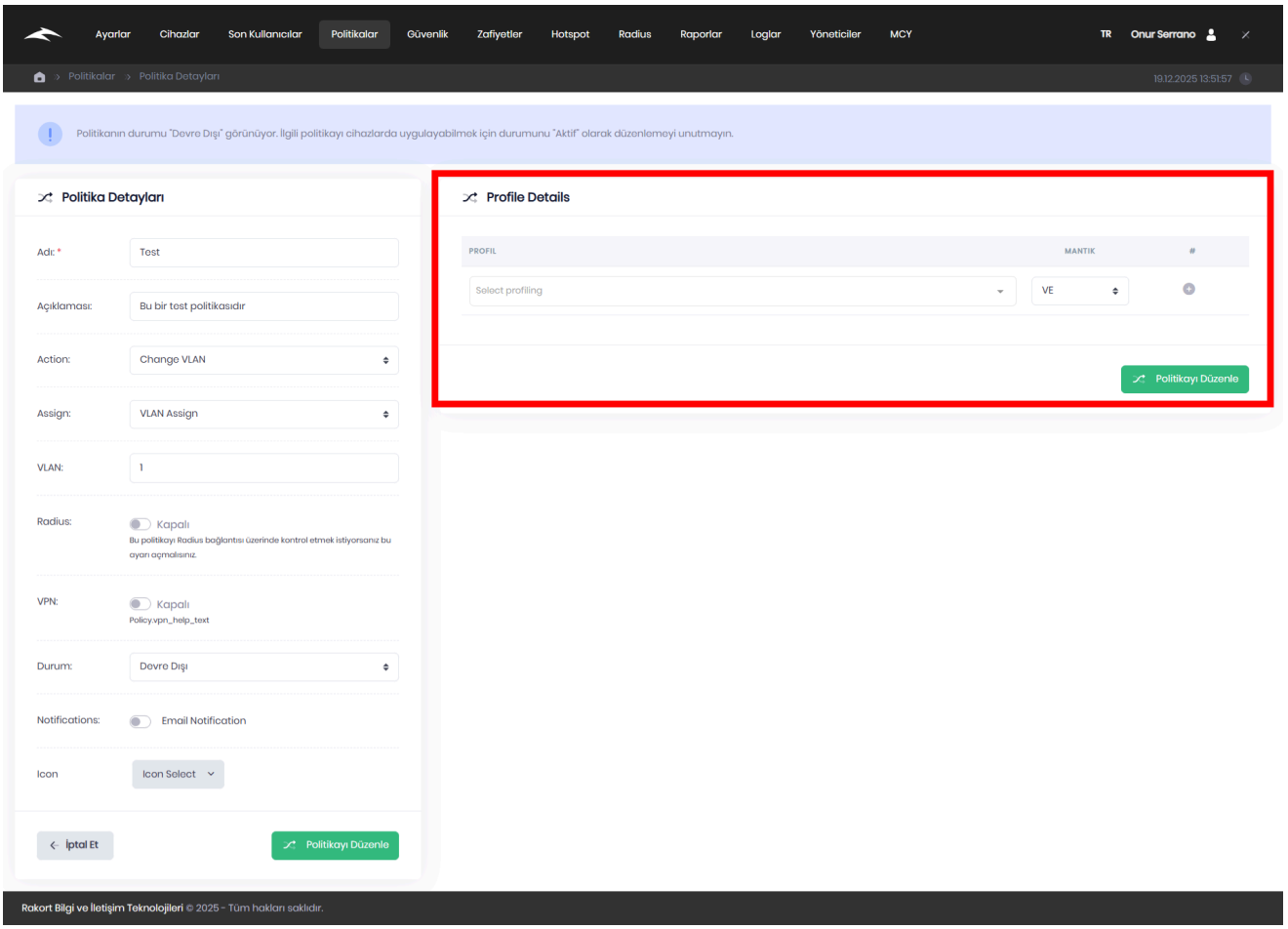
Açıklaması: Politikaya verilecek bir açıklama (Opsiyonel)

alanlarını doldurarak yeni bir politika oluşturabilirsiniz. Politika oluşturulduğunda sizleri direkt olarak politikanın detay sayfasına yönlendirmektedir.

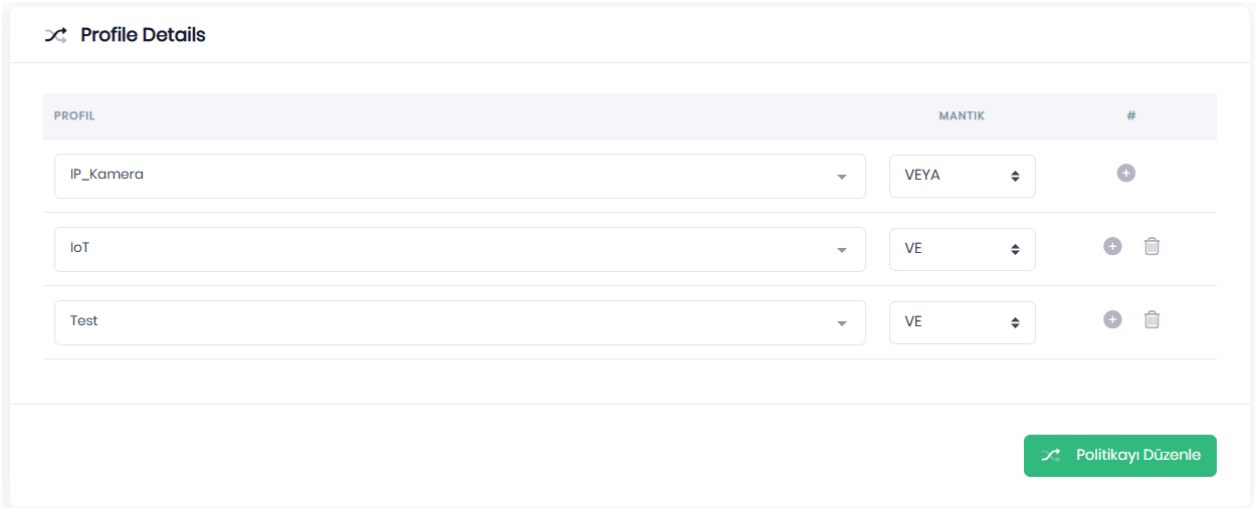
1.3) Politika Detay Sayfası

1.3.1) Profil Eklemek

Politika detay sayfasının sağ tarafında tarafında bulunan “**Profil Detayları**” bölümünden, ilgili politikaya, oluşturulan profiller bağlanabilir.



Burada oluşturulan profilleri “VE - VEYA” mantığı ile birbirine bağlayabilir, dilediğiniz kadar profili tek bir politikada kullanabilirsiniz. Profiller tablosunda bulunan ⊕ ikonuna tıklayarak ikinci bir profili de politikaya ekleyip, iki profil arasındaki mantıksal bağlantıyı (VE - VEYA) belirleyebilirsiniz.

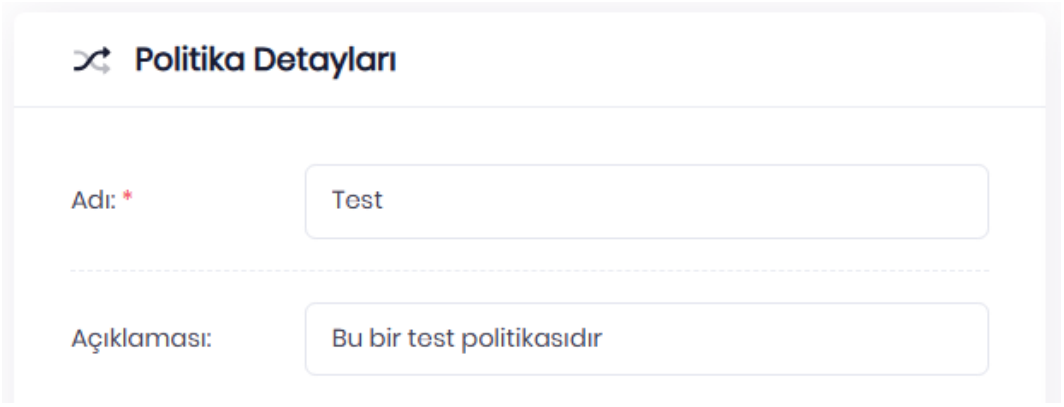


Yukardaki örnekte cihazın, "**IP_Kamera**" veya "**IoT**" ve "**Test**" profiline uyması gerektiğini söylemiş olduk. Mantıksal olarak: [**IP_Kamera** veya **IoT** (ikisinden bir tanesine uyuyorsa)] ve [**Test**] profiline uyuyorsa şeklinde yorumlanabilir.

Not: Bazı Aksiyon tiplerinde profil alanı değişmektedir. Aksiyon tipleri anlatılırken değişen kısımlar gösterilecektir.

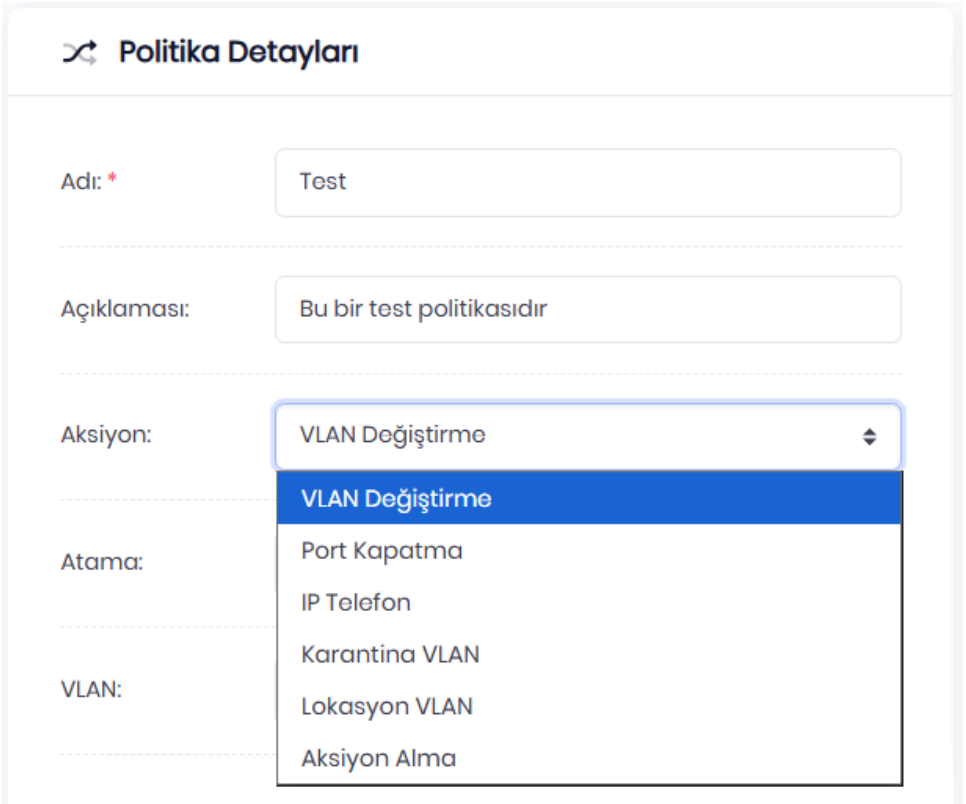
1.3.2) Temel Bilgiler

Politika detay sayfasının sol üst tarafında politikanın adını ve açıklamasını düzenleyebilirsiniz;



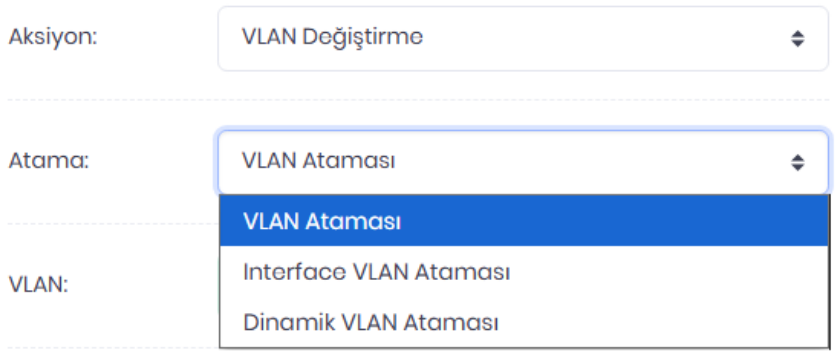
1.3.3) Aksiyon Tipleri

Politika detay sayfasının sol tarafında bulunan Aksiyon kısmından, seçilen profillere takılan cihazlara hangi aksiyonu alacağınızı seçebilirsiniz;



1.3.3.1) VLAN Değiştirme

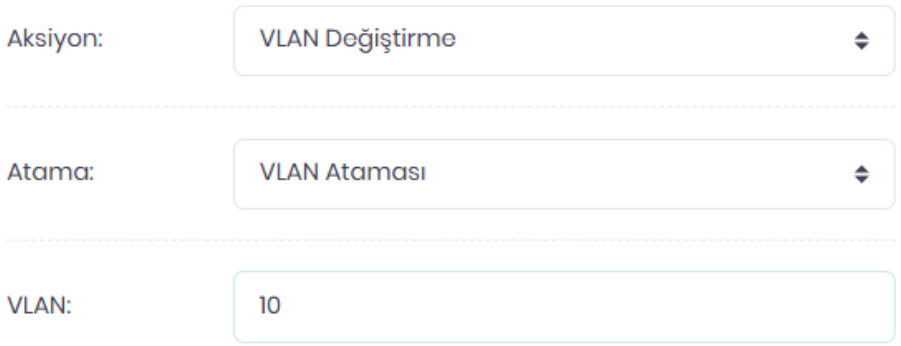
Seçilen profillere takılan bir cihazın VLAN numarasını değiştirmek isterseniz bu bölümden "**VLAN Değiştirme**" aksiyon tipini seçmeniz gerekmektedir.



VLAN Değiştirme aksiyonunda 3 farklı atama tipi bulunmaktadır. Bunlar;

1.3.3.1.1) VLAN Ataması

Atama olarak "VLAN Ataması" seçildiğinde;



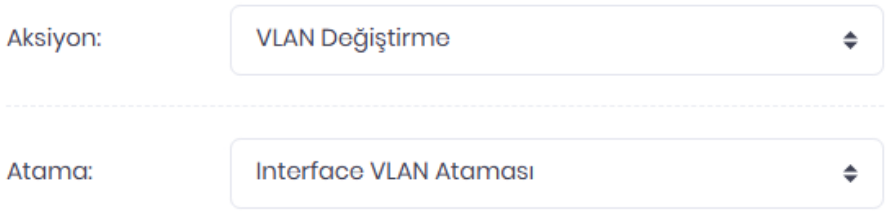
Atama bölümünün hemen altında yer alan "VLAN" inputu kısmına, ilgili profillere takılan cihazın atanacağı VLAN numarasını girebilirsiniz.

"**Profil Eklemek**" başlığında yaptığımız profilleri örnek olarak kullanacağız. Eğer network'e bağlanan cihaz;

[**IP_Kamera** veya **IoT** (ikisinden bir tanesine uyuyorsa)] ve [**Test**] profiline uyuyorsa yukardaki aksiyon tipinde ilgili cihaz **VLAN 10**'a atanacak şeklinde yorumlayabiliriz.

1.3.3.1.2) Interface VLAN Ataması

Atama olarak "Interface VLAN Ataması" seçildiğinde;



Atama bölümünün altındaki "VLAN" inputu kapanır. Bunun anlamı şudur;

İlgili switch FastNAC'a eklendiğinde, portların mevcut VLAN numaraları veritabanına kayıt edilir (Interface VLAN). Atama olarak "Interface VLAN Ataması" seçildiğinde mevcuttaki portun VLAN numarası kaçsa (Yani Interface VLAN neyse) ilgili VLAN numarasında bırakır.

Bir örnekle açıklayalım;

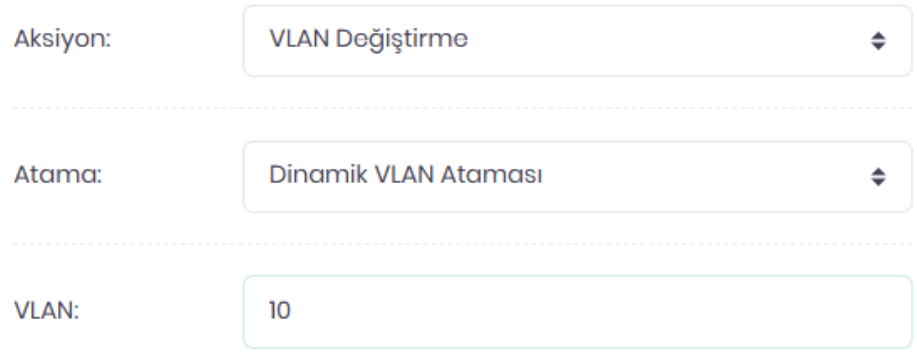
Öncelikle, 192.168.1.10 IP adresli Switch'in 5.portunun VLAN numarası 20 olsun. Biz bu switch'i FastNAC'a eklediğimizde 5.portun Interface VLAN'ının 20 olarak veritabanına kayıt ediyoruz. Daha sonrasında "**Profil Eklemek**" başlığında yaptığımız profilleri örnek olarak kullanacağız, Eğer network'e bağlanan cihaz;

[**IP_Kamera** veya **IoT** (ikisinden bir tanesine uyuyorsa)] ve [**Test**] profiline uyuyorsa "Interface VLAN Ataması" aksiyon tipinde ilgili cihazı VLAN 20'de bırakacak şeklinde yorumlanabilir.

Not: Interface VLAN tanımlamaları Switch'lerin detay sayfasından değiştirilebilir. Detayları switch_detaylari.docx dökümantasyonundan öğrenebilirsiniz.

1.3.3.1.3) Dinamik VLAN Ataması

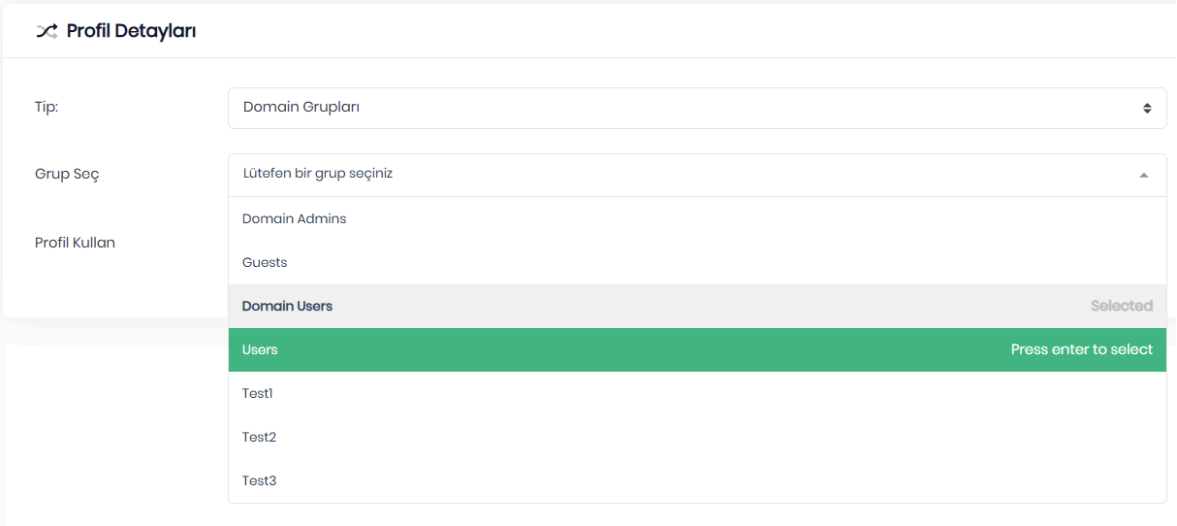
Dinamik VLAN ataması, domain içindeki OU'ya (Organization Units) veya domain kullanıcılarının gruplarına (memberOf) göre atama yapabilmek için kullanılmaktadır.



Bu atama tipi seçildiğinde sağ tarafta bulunan "**Profil Detayları**" kısmı değişmektedir. Atanacak OU veya domain grubu bu alandan seçilmektedir.

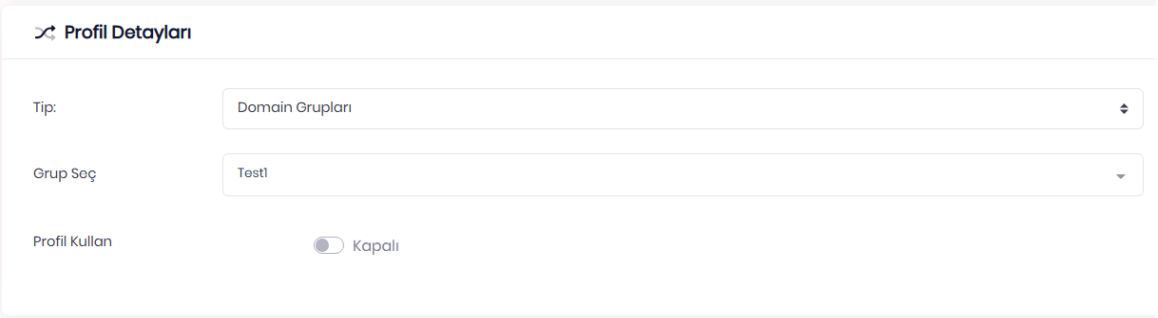
1.3.3.1.3.1) Domain Gruplarına göre Atama

Tip olarak "Domain Grupları" seçildiğinde,



"Grup Seç" inputu açıldığında domain üzerinde bulunan kullanıcı grupları listesi gelmektedir. Hangi grup için atama yapılacaksa ilgili ekrandan seçilmelidir.

Örnek olması açısından "**Test1**" kullanıcı grubunu seçiyoruz;

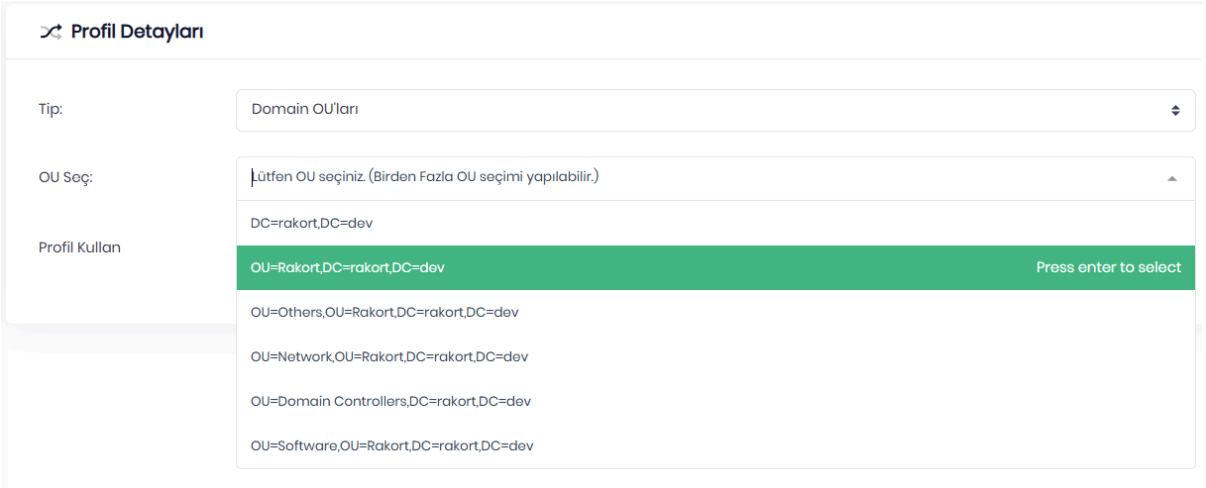


Ekranın sol tarafındaki atama kısmında seçtiğimiz "Dinamik VLAN Ataması" bölümünün altında yer alan VLAN inputu ise Test1 grubunda olan kullanıcıların atanacağı VLAN'ı temsil etmektedir.

Özetlemek gerekirse, Test1 domain kullanıcı grubu içinde olan kullanıcılar Network'teki herhangi bir switch üzerinden bağlantı kurmak istediğinde VLAN 10 'a taşınacak şeklinde yorumlanabilir.

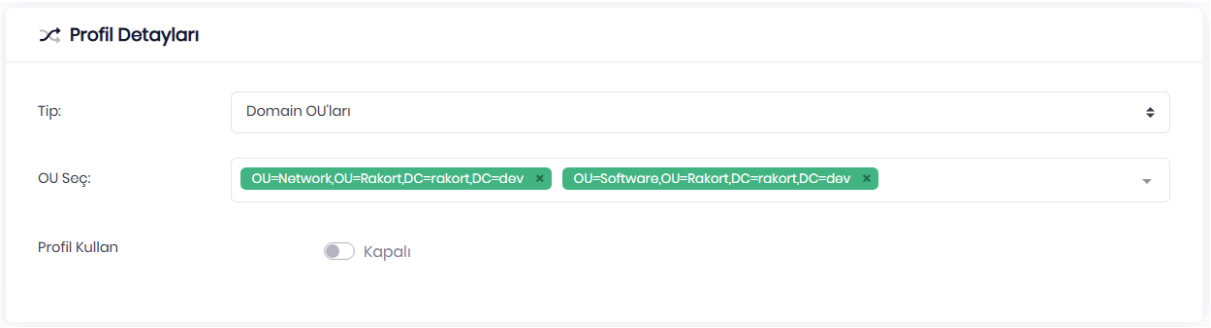
1.3.3.1.3.2) Domain OU'larına göre Atama

Tip olarak "Domain OU'ları" seçildiğinde,

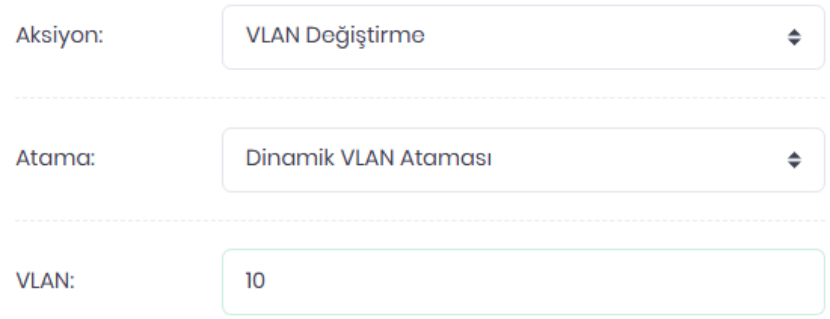


"OU Seç" inputunu açtığında domain üzerinde bulunan OU listesi gelmektedir. Hangi OU için atama yapılacaksa ilgili ekrandan seçilmelidir. Burada birden fazla OU seçimi yapılabilmektedir.

Örnek olması açısından "**OU=Network,OU=Rakort,DC=rakort,DC=dev**" ve "**OU=Software,OU=Rakort,DC=rakort,DC=dev**" OU'larını seçiyoruz;



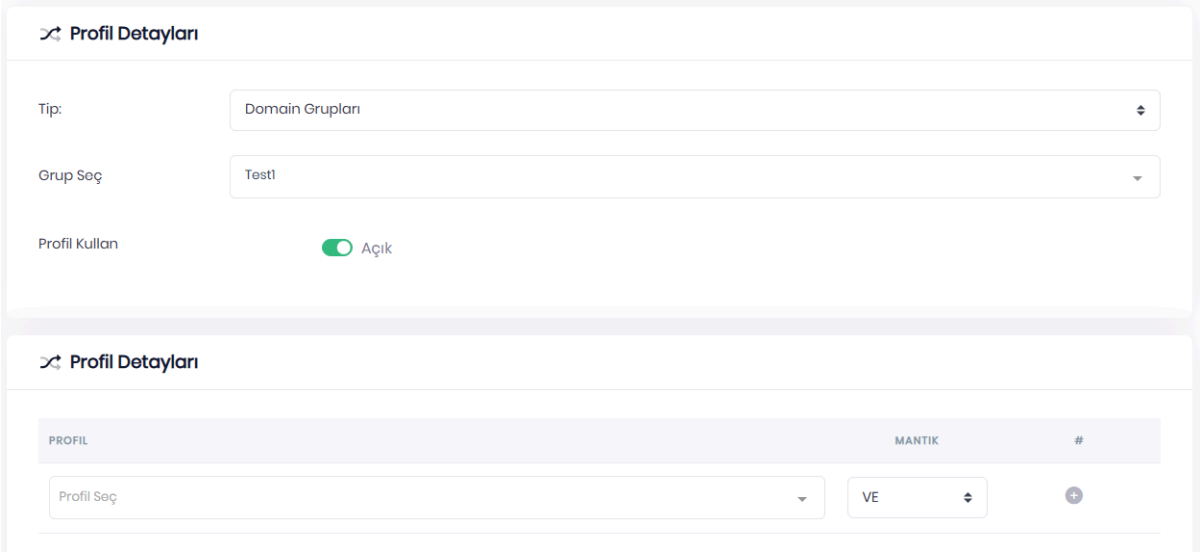
Ekranın sol tarafındaki atama kısmında seçtiğimiz "Dinamik VLAN Ataması" bölümünün altında yer alan VLAN inputu ise seçilen OU'ların atanacağı VLAN'ı temsil etmektedir.



Özetlemek gerekirse, domain kullanıcısı, "**OU=Network,OU=Rakort,DC=rakort,DC=dev**" veya "**OU=Software,OU=Rakort,DC=rakort,DC=dev**" OU'sunun içindeyse, Network'teki herhangi bir switch üzerinden bağlantı kurmak istediğinde VLAN 10 'a taşınacak şeklinde yorumlanabilir.

1.3.3.1.3.3) Dinamik VLAN ve Profil Kullanma

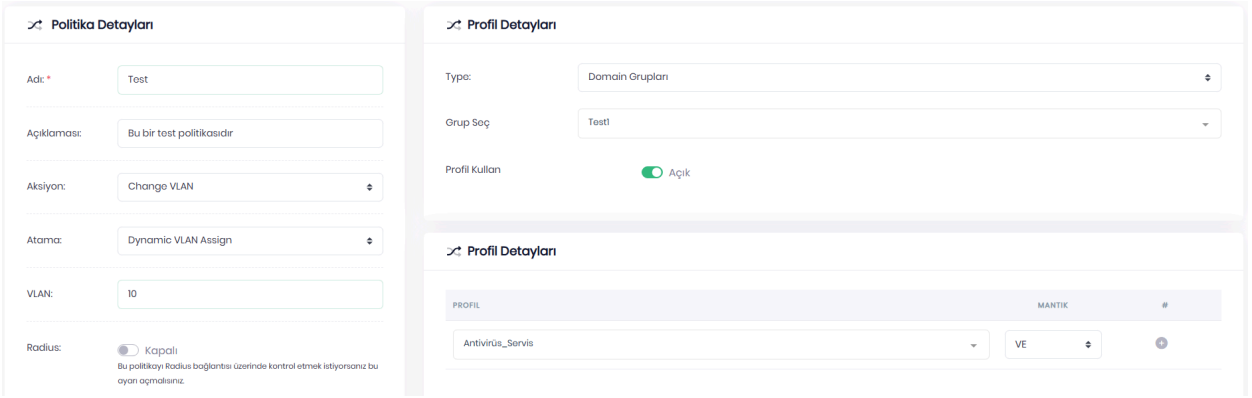
Dinamik VLAN atamasının yanında herhangi bir profili de kontrol etmek istiyorsanız "**Profil Kullan**" seçeneğini açmanız gerekmektedir. Bu ayarı açtığınızda ilgili ekranın hemen altında profil seçimleri yapabileceğiniz alan açılacaktır.



Burada aşağıdaki gibi bir senaryo kullanılabilir;

Öncelikle antivirüs servisinin çalışması gerektiği ile ilgili bir profil ekleyelim. (Profilleme ile ilgili detaylı bilgiye cihaz_profilleme.docx dökümantasyonundan ulaşabilirsiniz.) Daha sonrasında hem Dinamik VLAN ataması ile kullanıcı grubunu hem de antivirüs profilini beraber kontrol edelim.

Network'e erişmek isteyen kullanıcı "Test" domain kullanıcı grubu içindeyse ve Antivirüs servisi çalışıyorsa şeklinde bir politika yazalım;

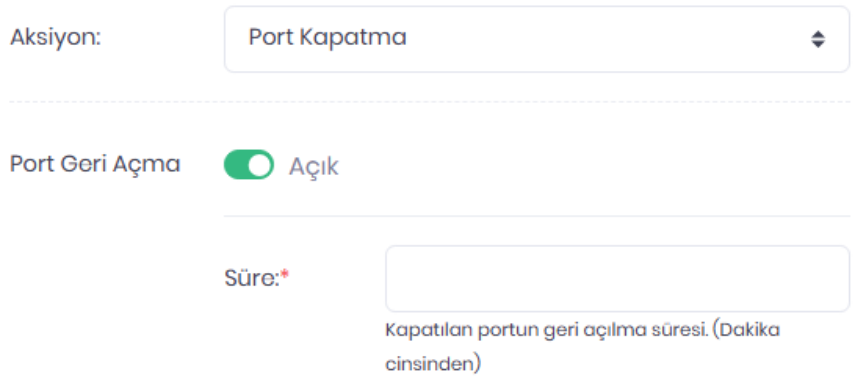


Yukardaki örnekte eğer domain kullanıcısı "Test1" domain grubunun içindeyse ve bilgisayarında antivirüs servisi çalışıyorsa, Network'teki herhangi bir switch üzerinden bağlantı kurmak istediğinde VLAN 10 'a taşınacak şeklinde yorumlanabilir.

Bu şekilde hem Dinamik VLAN ataması hem de kapsamlı bir şekilde profil kontrollerini aynı anda gerçekleştirebilirsiniz.

1.3.3.2) Port Kapatma (Disable Port)

Aksiyon tipi "Port Kapatma" olarak seçildiğinde,



İlgili seçilen profillere takılan cihazın bağlı olduğu portu kapatma aksiyonu alır. (Shutdown veya Disabled) "**Port Geri Açma**" süresini açarak ve Süre (dakika cinsinden) belirterek, kapatılan portun otomatik olarak tekrar açılmasını sağlayabilirsiniz. Port geri açıldığında eğer cihaz hala bağlıysa politika tekrar kontrol edilir ve koşullar hala sağlanıyorsa tekrar kapatılır.

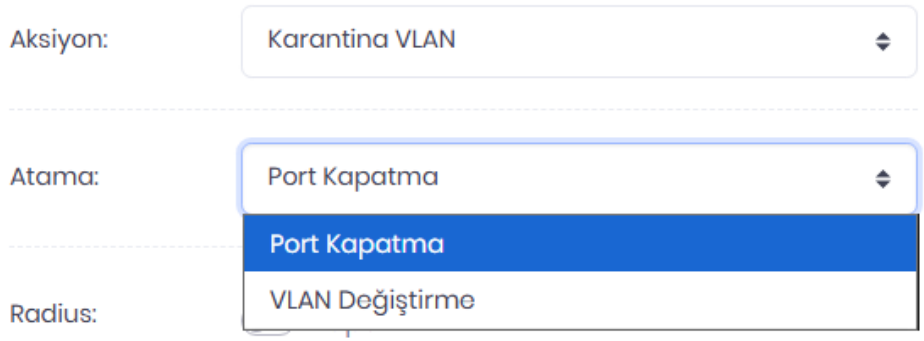
1.3.3.3) IP Telefon Tipi

Aksiyon tipi "IP Telefon" olarak seçildiğinde,

İlgili seçilen profillere takılan cihaza herhangi aksiyon alınmaz. Bu özel bir profildir. FastNAC, IP telefonların çalıştığı Ses VLAN'larına (Voice VLAN) karışmaz. Eğer network'te IP telefon kullanımı varsa ve cihazlar IP telefon arkasından network'e erişiyorsa, IP telefonların kendisi için muhakkak bu aksiyon tipi seçilmelidir.

1.3.3.4) Karantina VLAN

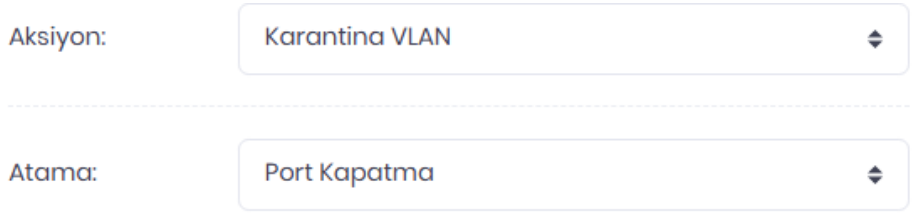
Aksiyon tipi olarak "Karantina VLAN" seçildiğinde;



Bu aksiyon tipi herhangi bir politikaya uymayan cihazlar için kullanılması gereken aksiyondur. 2 farklı atama tipi kullanılabilir;

1.3.3.4.1) Port Kapatma

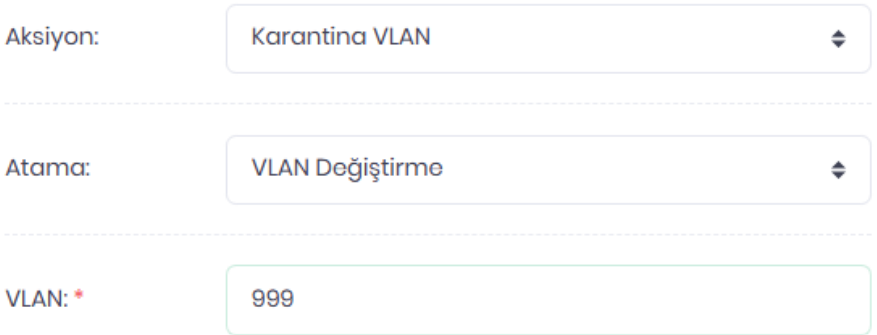
Atama olarak "Port Kapatma" seçildiğinde;



Cihazın bağlı olduğu switch portunu kapatma aksiyonu alır. (Shutdown veya Disabled)

1.3.3.4.2) VLAN Değiştirme

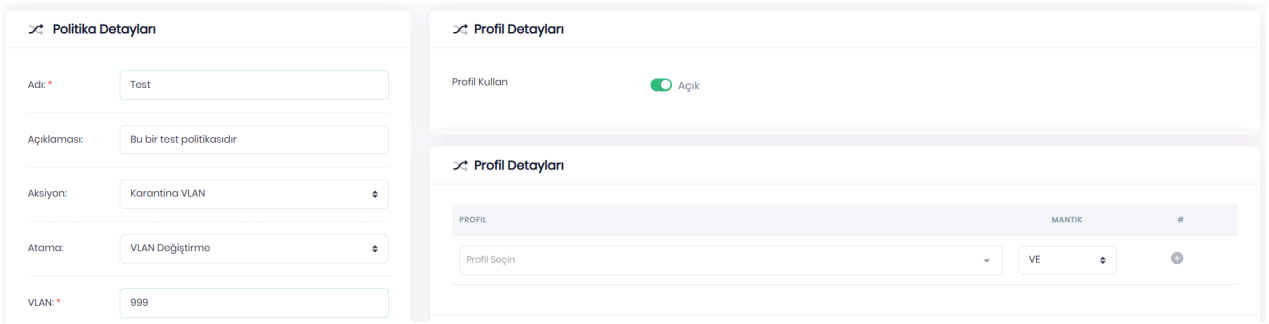
Atama olarak "VLAN Değiştirme" seçildiğinde;



Cihazın bağlı olduğu switch portunu "VLAN" bölümünde yazılan VLAN numarasına taşır.

1.3.3.4.3) Karantina ve Profil Kullanma

Karantina VLAN atamasının yanında herhangi bir profili de kontrol etmek istiyorsanız "**Profil Kullan**" seçeneğini açmanız gerekmektedir. Bu ayarı açtığınızda ilgili ekranın hemen altında profil seçimleri yapabileceğiniz alan açılacaktır.



1.3.3.4.4) Karantina ile ilgili Genel Kullanım

FastNAC üzerinde Karantina VLAN tanımı yapmak zorunlu değildir. Fakat genel kullanım açısından bu politikayı oluşturup, politika listesinin en altında tutmak sistemin çalışması açısından daha doğru olacaktır.

"**1.1) Başlangıç**" bölümünde belirtiği gibi FastNAC, politikaları yukarıdan aşağıya doğru sıralı bir şekilde kontrol eder. Eğer cihaz, herhangi bir politikaya takılırsa, takıldığı politikanın altındaki diğer politikalar kontrol edilmez. Bu sebeple Karantina VLAN aksiyonundaki politika listenin en altında olmalıdır. Örneğin, 5 tane politikamız var diyelim. Bunlar;

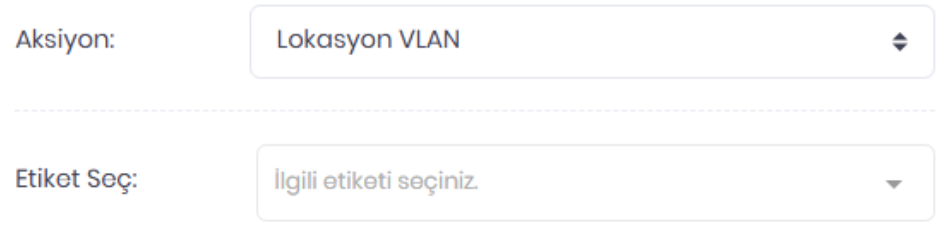
Politika Adı	Politika Tipi	Aksiyon
IP_Telefon	IP_Telefon	-
Yazıcılar	VLAN Değiştirme	20
IP_Kameralar	VLAN Değiştirme	30
Domain_Kontrolu	Interface VLAN	-
Karantina	Karantina VLAN -> VLAN Değiştirme	999

Yukardaki tablo örneğinde, Network'e bağlanan bir cihaz üzerinde sırayla "**IP_Telefon**" -> "**Yazıcılar**" -> "**IP_Kameralar**" -> "**Domain_Kontrolu**" politikaları kontrol edilecek. Eğer hiçbir politikaya uymuyorsa en son "**Karantina**" politikasına takılacak ve VLAN 999 'a atanacak.

Eğer Karantina tipinde bir politika yazılmazsa, ilgili cihaz politika kontrolleri sonucu herhangi bir politikaya çarpmazsa, herhangi bir aksiyon alınmaz ve cihaz, portun mevcut VLAN'ınında bırakılır.

1.3.3.5) Lokasyon VLAN

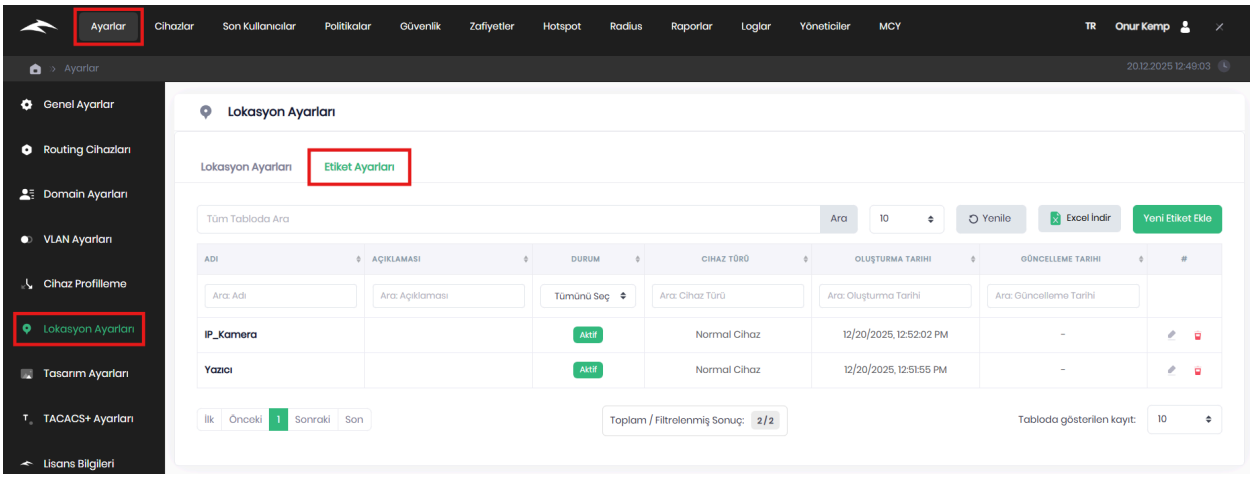
Aksiyon tipi olarak "Lokasyon VLAN" seçildiğinde;



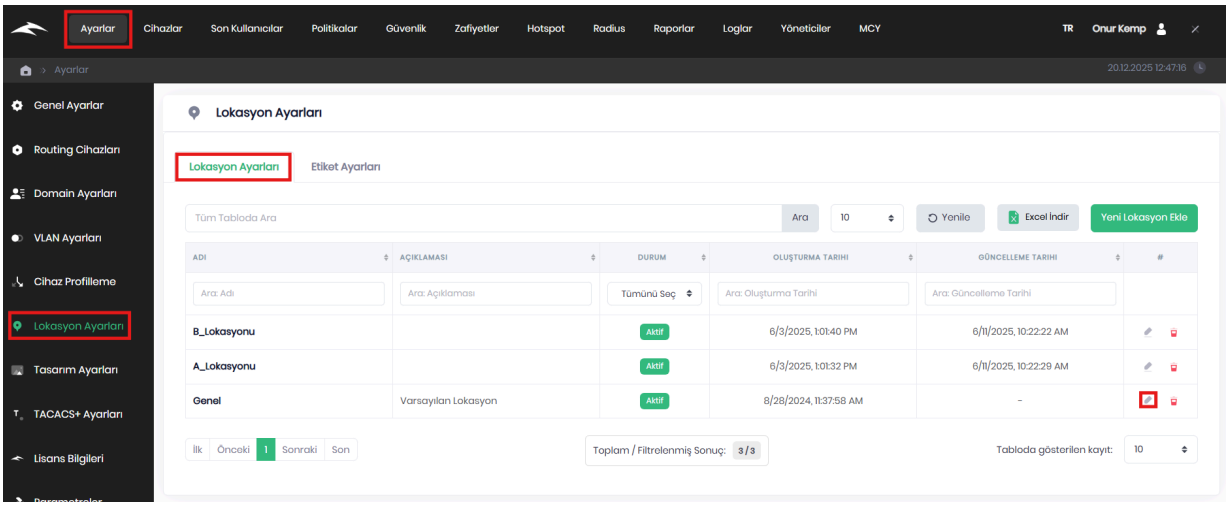
Aksiyon bölümünün altında "**Etiket Seç**" inputu açılmaktadır. Burada seçilen etiket'in belirtilen VLAN numarasına göre VLAN taşıma işlemi yapılmaktadır.

Lokasyon VLAN tipinde herhangi bir atama seçimi yapılmaz. Seçilen profillere göre alınacak aksiyon işlemleri etiketler üzerinden gerçekleştirilmektedir.

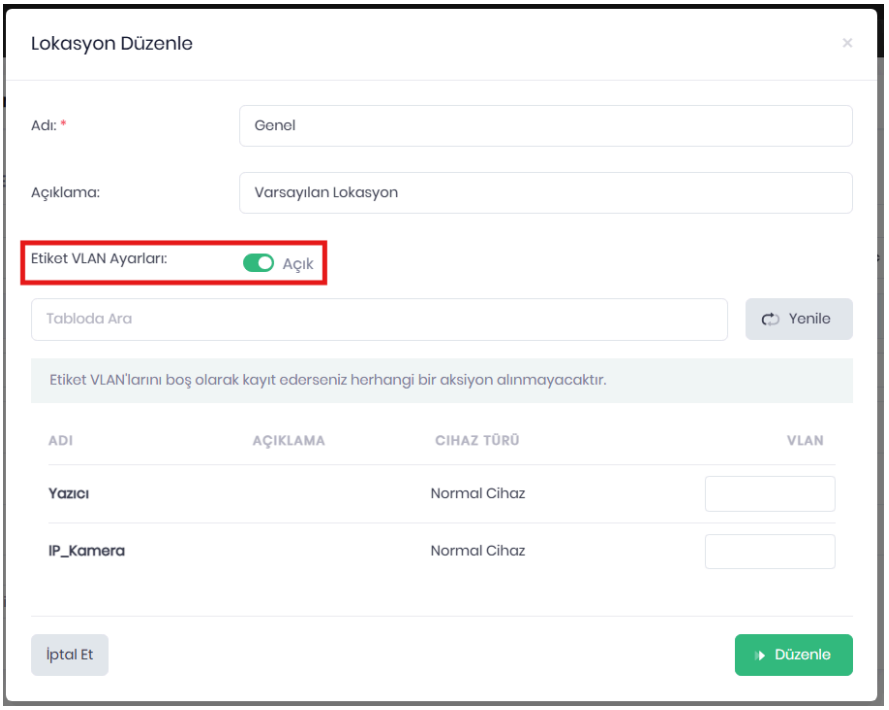
Etiket VLAN ayarlamaları için "**Ayarlar**" -> "**Lokasyon Ayarları**" -> "**Etiket Ayarları**" bölümünden etiketleri kontrol edebilirsiniz;



Oluşturduğunuz etiketlere VLAN numarası tanımlamak içinde "**Ayarlar**" -> "**Lokasyon Ayarları**" bölümünündeki lokasyonları düzenleyebilirsiniz;

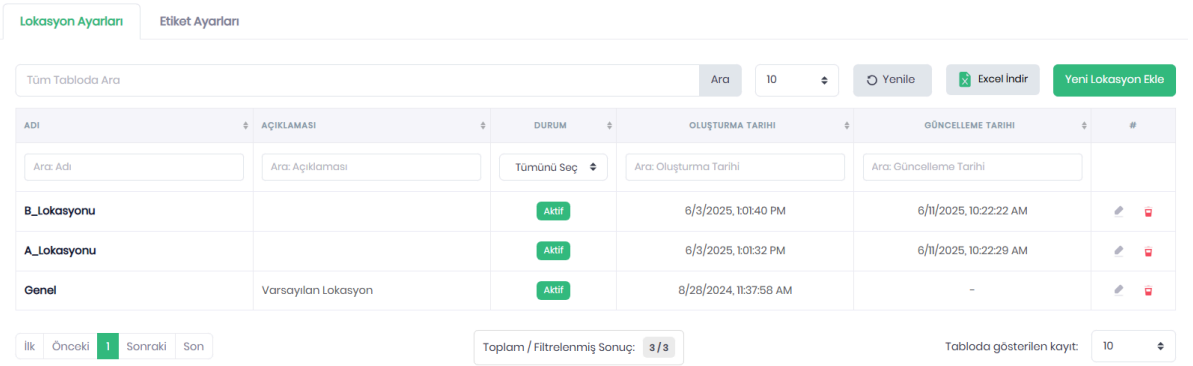


Lokasyon düzenleme ekranında "**Etiket VLAN Ayarları**" kısmını açtığında, oluşturduğunuz etiketlere VLAN tanımlamalarını girebilirsiniz;

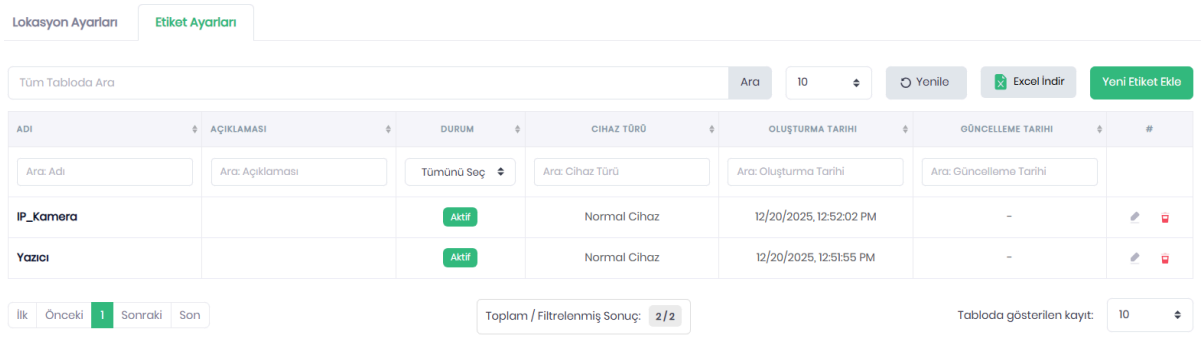


1.3.3.5.1) Lokasyon VLAN ile ilgili Genel Kullanım

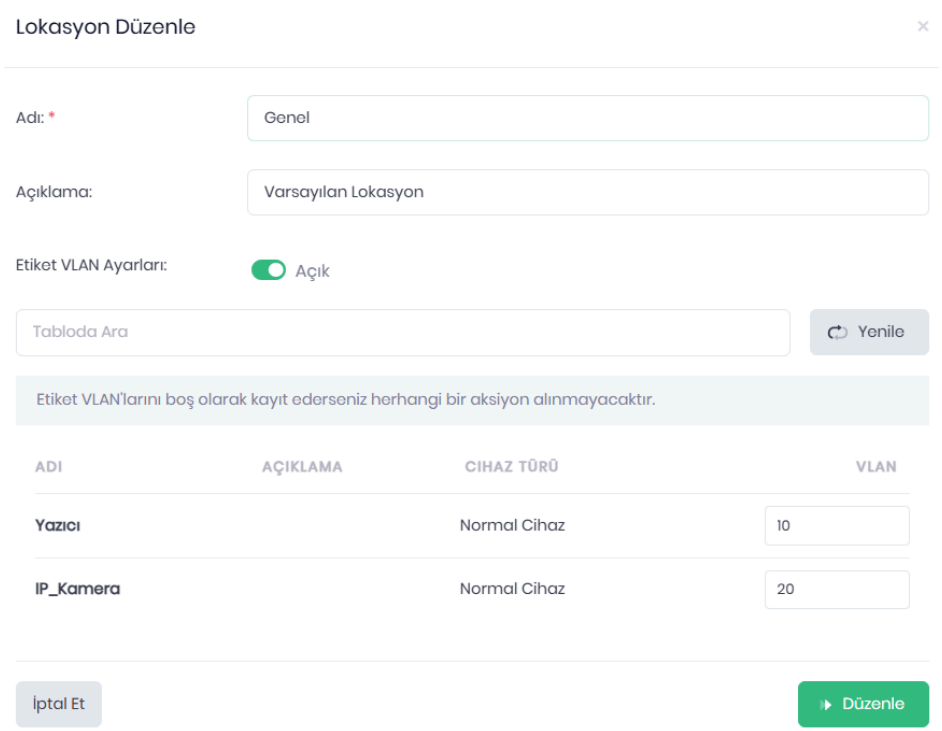
Lokasyon VLAN ile ilgili detaylı bir anlatım yapalım. Örneğin birden fazla lokasyonda switchleriniz var. Bu lokasyonları FastNAC'a ekliyoruz;



Örnek olması açısından "**Genel**", "**A_Lokasyonu**" ve "**B_Lokasyonu**" şeklinde 3 tane lokasyon ekledik. Sonra "**IP_Kamera**" ve "**Yazıcı**" şeklinde de 2 tane etiket ekliyoruz;

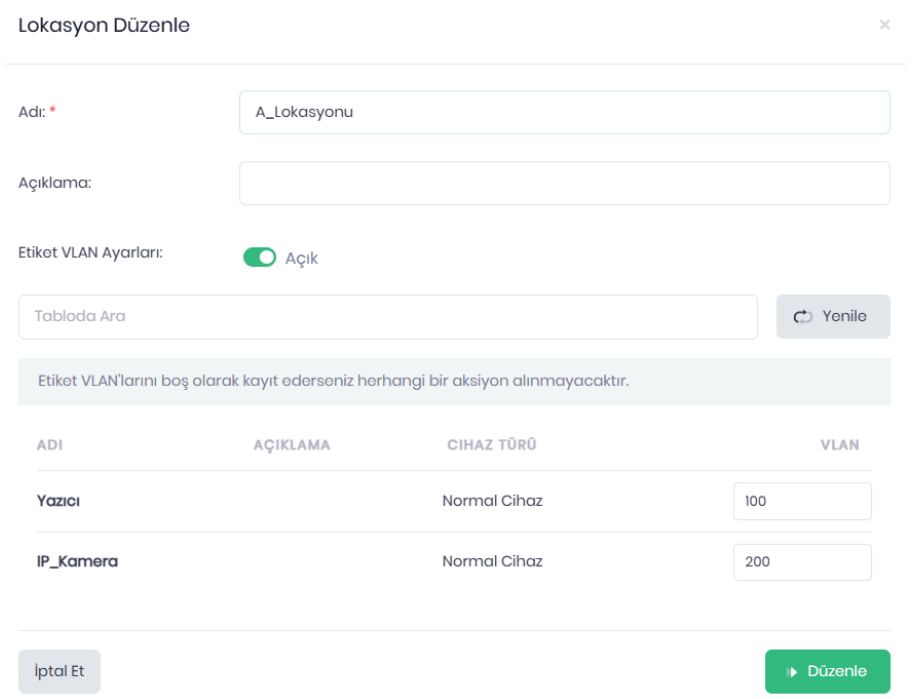


Tekrar "**Lokasyon**" bölümüne dönüyoruz. "**Genel**" lokasyonu düzenle kısmına geliyoruz ve "**Etiket VLAN Ayarı**" bölümünü açıyoruz.



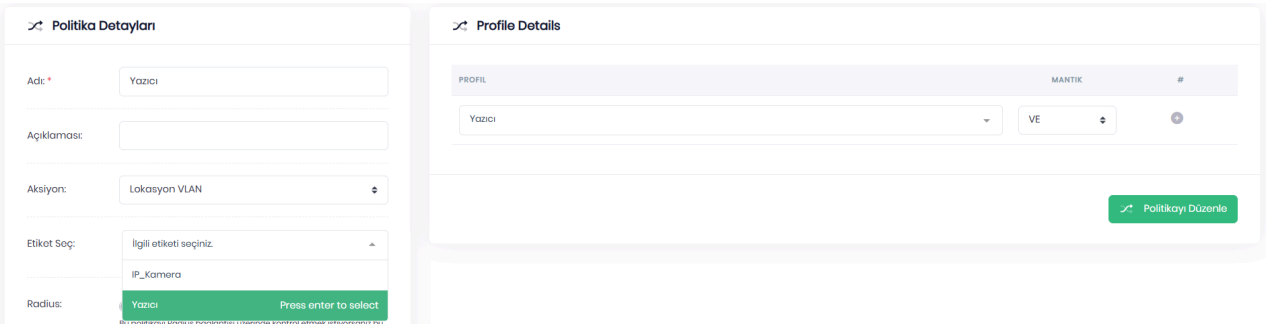
Bu ekranda oluşturduğumuz etiketleri görüyoruz. "**Genel**" lokasyonu içindeki "**IP_Kamera**" ve "**Yazıcı**" etiketleri için bir VLAN ataması yapıp "**Düzenle**" butonuna basıyoruz. (Yukardaki örnekte "**Yazıcı**" için VLAN 10, "**IP_Kamera**" için VLAN 20 belirlenmiştir.)

Daha sonrasında aynı işlemi "**A_Lokasyonu**" için yapıyoruz ve bu sefer "**Yazıcı**" için VLAN 100, "**IP_Kamera**" için VLAN 200 atama işlemlerini yapıyoruz;



Son olarak "**B_Lokasyonu**" içinde aynı işlemleri yapıyoruz ve bu sefer de "**Yazıcı**" için VLAN 500, "**IP_Kamera**" için VLAN 700 tanımı yapıyoruz.

Politika kısmında ise "**Yazıcı**" adında bir profil oluşturuyoruz ve Aksiyon olarak "**Lokasyon VLAN**" seçip, Etiket olarakta "**Yazıcı**" etiketini seçiyoruz;



Bu politikayı yorumlamak gerekirse;

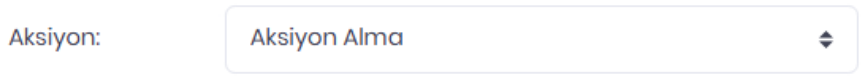
"**Yazıcı**" profiline takılan herhangi bir cihaz;

- Eğer "Genel" lokasyonunda ise etiket VLAN ataması olarak belirttiğimiz VLAN 10'a,
- Eğer "A_Lokasyonu" lokasyonunda ise etiket VLAN ataması olarak belirttiğiniz VLAN 100'e,
- Eğer "B_Lokasyonu" lokasyonunda ise etiket VLAN ataması olarak belirttiğimiz VLAN 500'e

atanacak şeklinde yorumlayabiliriz. Lokasyon VLAN aksiyonu, sizleri her lokasyon için ayrı profil/politika eklemek zorunda bırakmaz. Cihazları tek bir profil/politika üzerinden kontrol edebilirsiniz.

1.3.3.6) Aksiyon Alma (No Action)

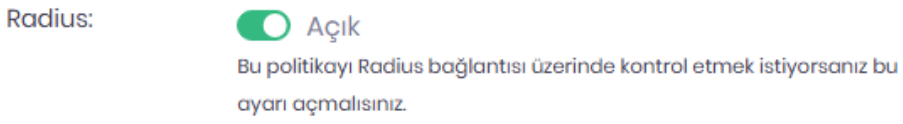
Aksiyon tipi olarak "**Aksiyon Alma**" seçildiğinde;



Seçilen profillere takılan cihazlara herhangi bir aksiyon alınmaz. Bazı özel durumlar için kullanılabilir. Örneğin "Profile takılan cihaza herhangi bir aksiyon alınmasın ama network'e giriş yapmak istediğinizde beni bilgilendirsin." şeklinde bir politikayı "**Aksiyon Alma**" ile oluşturabilirsiniz.

1.3.4) Radius

"Radius" seçeneği açıldığında;

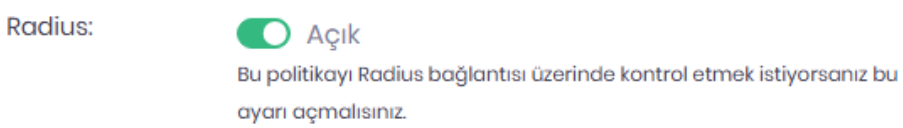


FastNAC üzerinde hem yeni nesil hem de geleneksel (Radius) yöntemi hibrit bir şekilde kullanarak politikalar oluşturulabilmektedir. İlgili politikanın Radius bağlantıları üzerinden kontrol edileceğini belirtmek için bu ayarı açmanız gerekmektedir.

"**Radius**" ayarı açıldığında Aksiyon tipi olarak "**VLAN Değiştirme**" ve "**Karantina VLAN**" gelmektedir. Bu Aksiyon tiplerinin detaylarını "**1.3.3) Aksiyon Tipleri**" başlığından bakabilirsiniz.

1.3.5) VPN

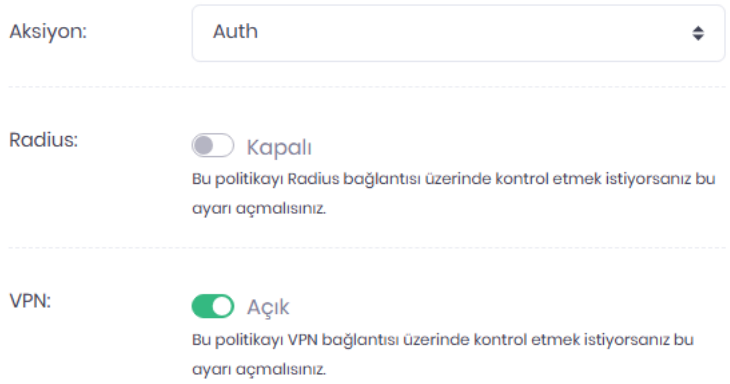
"**VPN**" seçeneği açıldığında;



İlgili politikanın VPN bağlantısı üzerinden bağlanan cihazlar için kontrol edileceğini belirtmiş oluyorsunuz. "**VPN**" ayarı açıldığında Aksiyon tipi olarak "**Auth**" ve "**Deauth**" gelmektedir.

1.3.5.1) Auth Tipi

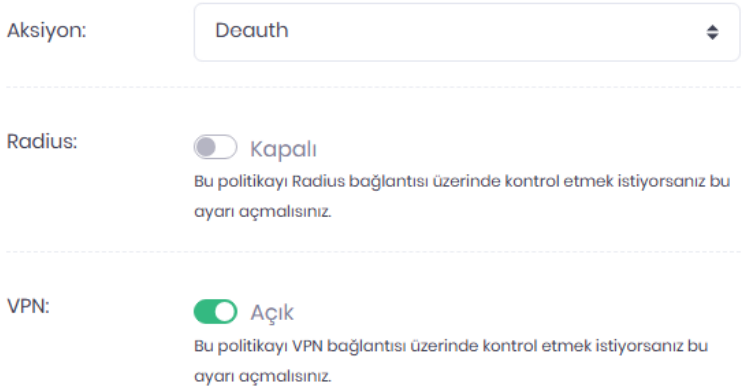
Aksiyon tipi olarak "**Auth**" seçildiğinde;



İlgili profillere takılan cihazı Yetkilendir ve Network'e erişmesine izin ver tanımı yapmış oluyorsunuz.

1.3.5.2) Deauth Tipi

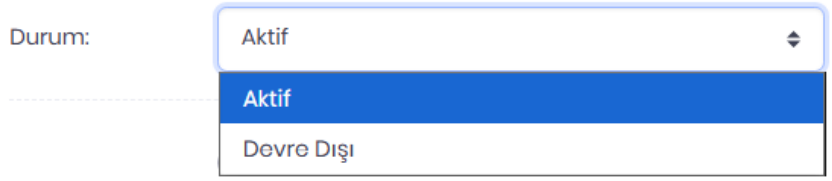
Aksiyon tipi olarak "**Deauth**" seçildiğinde;



İlgili profillere takılan cihazın VPN bağlantısı yapmasını engellemiş olursunuz.

1.3.6) Durum

"**Durum**" kısmında ise politikanın durumunu seçebilirsiniz;



- "**Aktif**" seçilirse, politika çalışmaya devam edecektir.
- "**Devre Dışı**" seçilirse, politika çalışmayacaktır.

1.3.7) Bildirimler

"**Bildirimler**" kısmında, ilgili politikaya takılan cihazlar için eposta bildirimlerini açabilirsiniz.

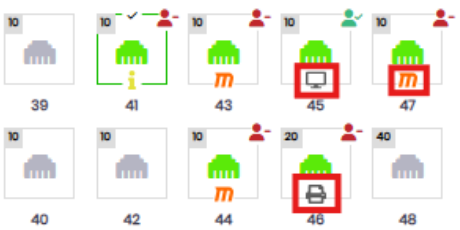
Eğer bir cihaz ilgili politikaya çarparsa, "**Ayarlar**" -> "**Genel Ayarlar**" -> "**Bildirim Ayarları**" -> "**Gönderim Adresleri**" bölümüne eklenen e posta adreslerine bilgilendirme e postası gönderir.

Not: Politikalarda e posta gönderimi için Genel Bildirim ayarının açık olması gerekmektedir. "**Ayarlar**" -> "**Genel Ayarlar**" -> "**Bildirim Ayarları**" -> "**Bildirim Özellikleri**" bölümünden "**Politikalar**" kısmının açık olduğunu kontrol etmeniz gerekmektedir.

1.3.8) Ikon (Port Görselleştirme)

İlgili profile takılan cihazlara ikon eklemek için seçim yapabilirsiniz;

Politika ikonları, switch detay sayfalarında portların altında gösterilmektedir. Switch detay sayfasına girildiğinde, hangi portta hangi cihazın bağlı olduğu anlık olarak görebilmektesiniz.



Bu ekrandaki ikonlar, politika bölümünden gelmektedir. Herhangi bir politikaya çarpan cihaz için seçtiğiniz ikon portun altına gelmektedir.

FastNAC'ta varsayılan olarak 16 tane ikon gelmektedir. Sisteme sizde ikon ekleyebilirsiniz. "**Ayarlar**" -> "**Tasarım Ayarları**" -> "**İkon Ayarları**" bölümündeki "**Yeni İkon Ekle**" butonunu kullanarak bilgisayarınızdan ikonlar yükleyebilirsiniz.

Not: Yüklemek istediğiniz ikon formatları; "**image/svg**", "**png**", "**jpeg**", "**jpg**" olmalıdır.