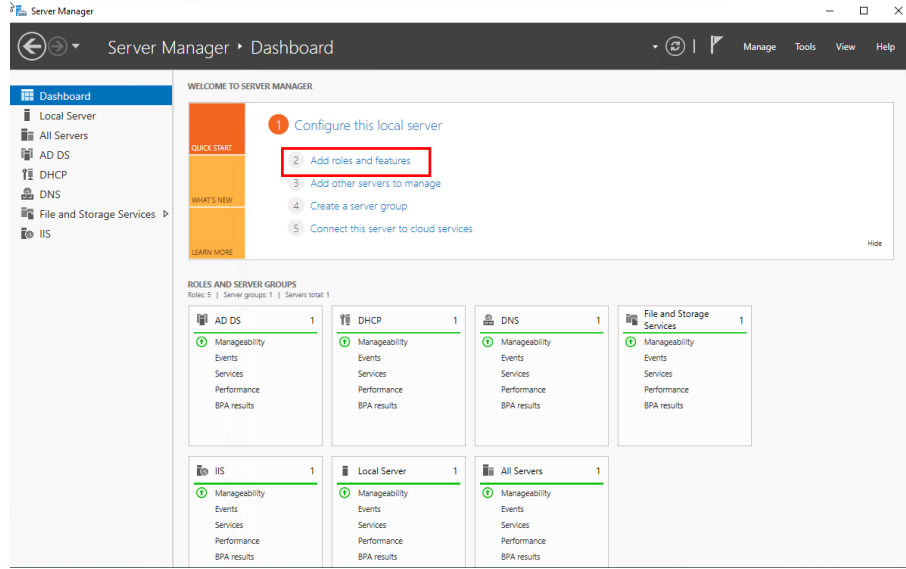


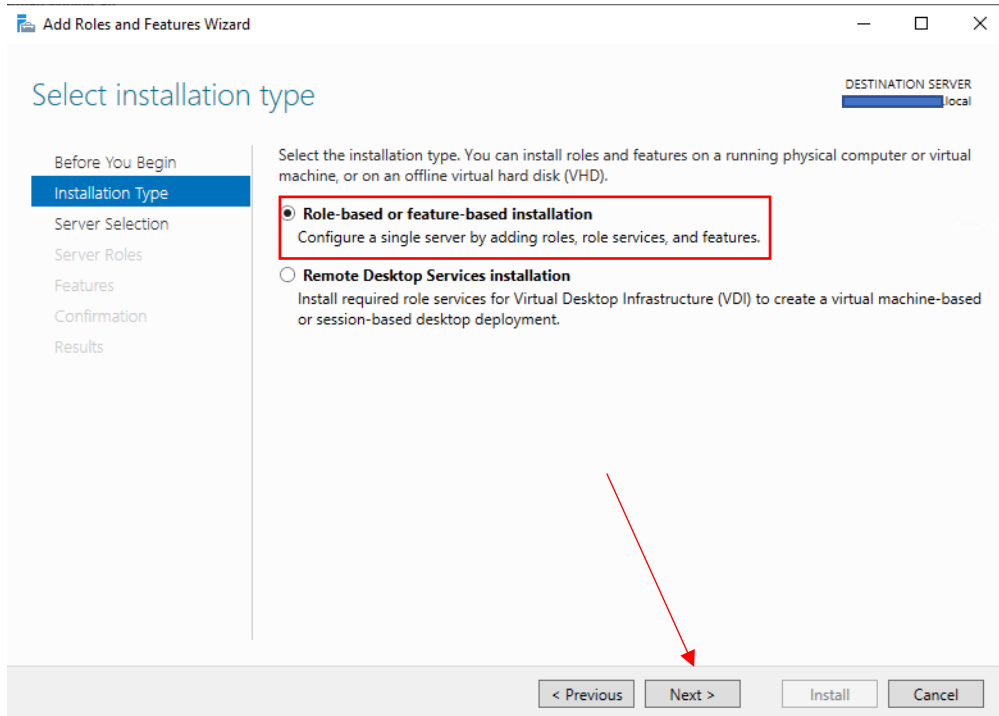
Senaryomuzda Mevcutta bulunan aces pointlerimizi kullanarak, domain de bulunan kullanıcılarımızın **RADIUS** sunucu üzerinden wifi network ağına kendi domain bilgileriyle nasıl logon olurlar anlatıyor olacağım.

Ben yapımda RADIUS sunucu çözümü olarak hem hazır olması açısından hemde maliyet açısından server rolü olan **Microsoft NPS (Network Policy and Access Services)** kullanacağım.

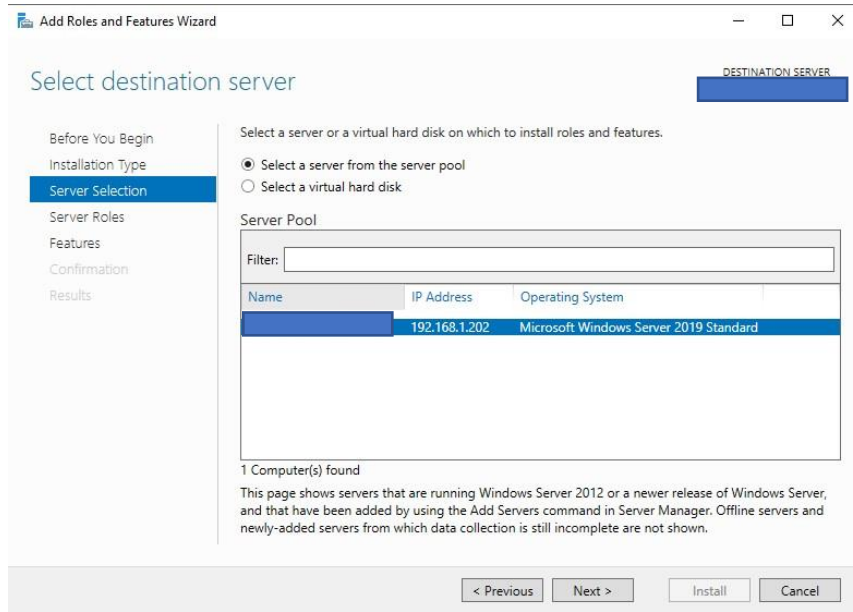
Öncelikler Rolü kurmak istediğim sunucuma giderek Server Manager üzerinden **Add roles and Feature** seçeneğine tıklıyorum. Sertifika servisim kurulu olduğu için tekrar kurmayacağım. Sizin mutlaka kurmanız gerekmektedir.



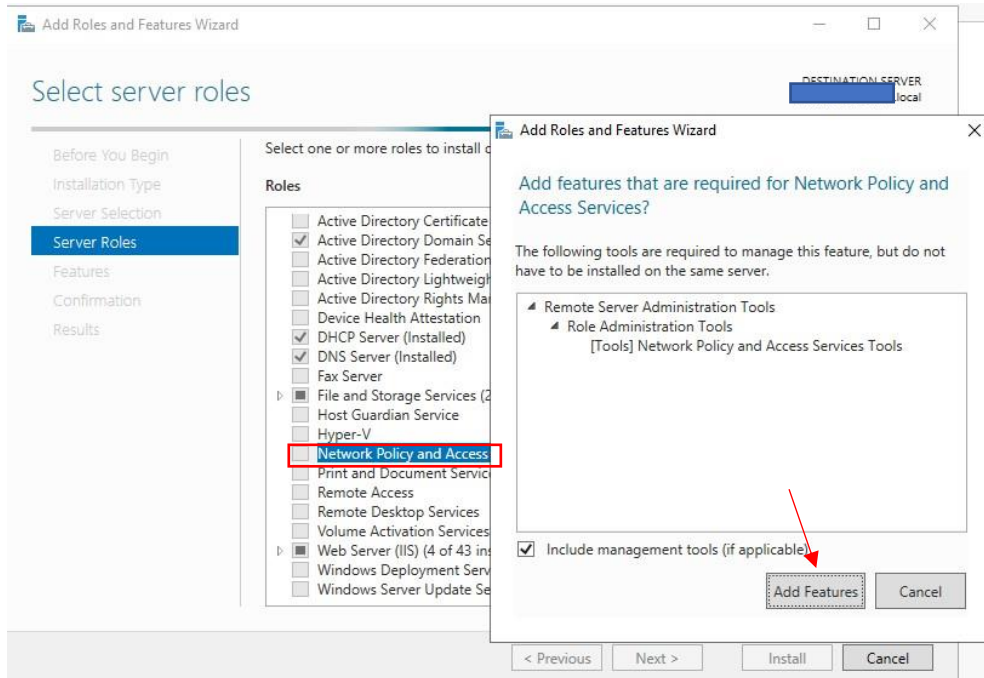
Karşıma gelen menüden **Role-based or feature-based installation** seçeneği seçiyor ve next diyerek ilerliyorum.



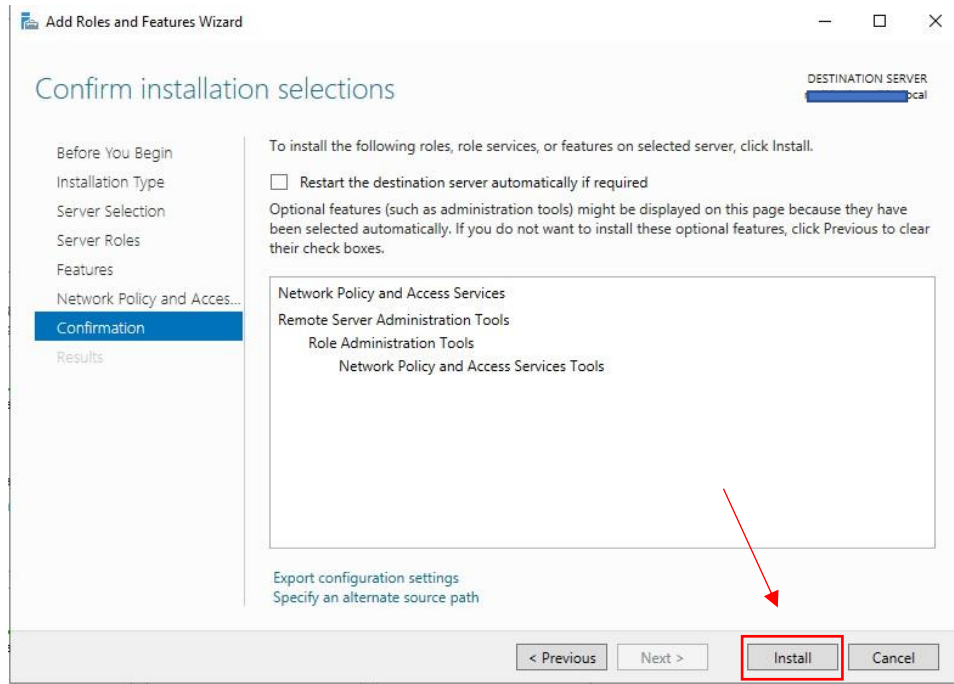
Karşıma gelen bir sonraki ekranımda Rolü hangi sunucuma kurmak isteğimi soruyor. Sunucumu seçerek next ile ilerliyorum.



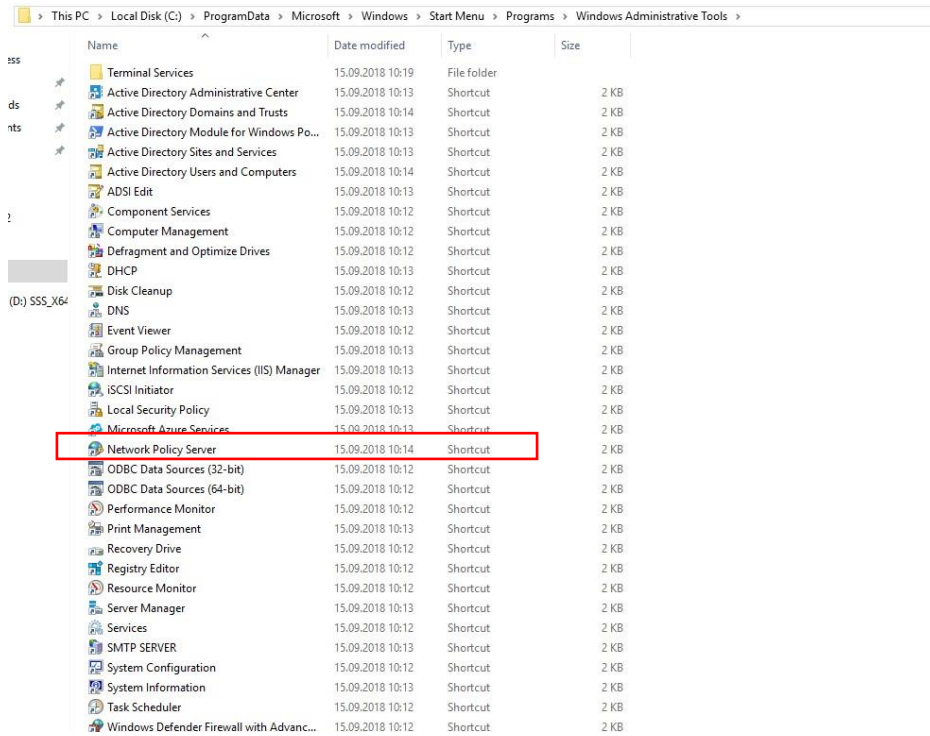
Bir sonraki adımda Server rolü kuracağım menü karşıma geliyor. Seçeneklerden Network Policy and Access Policy seçeneği onaylayıp Add Features butonuna tıklıyorum.



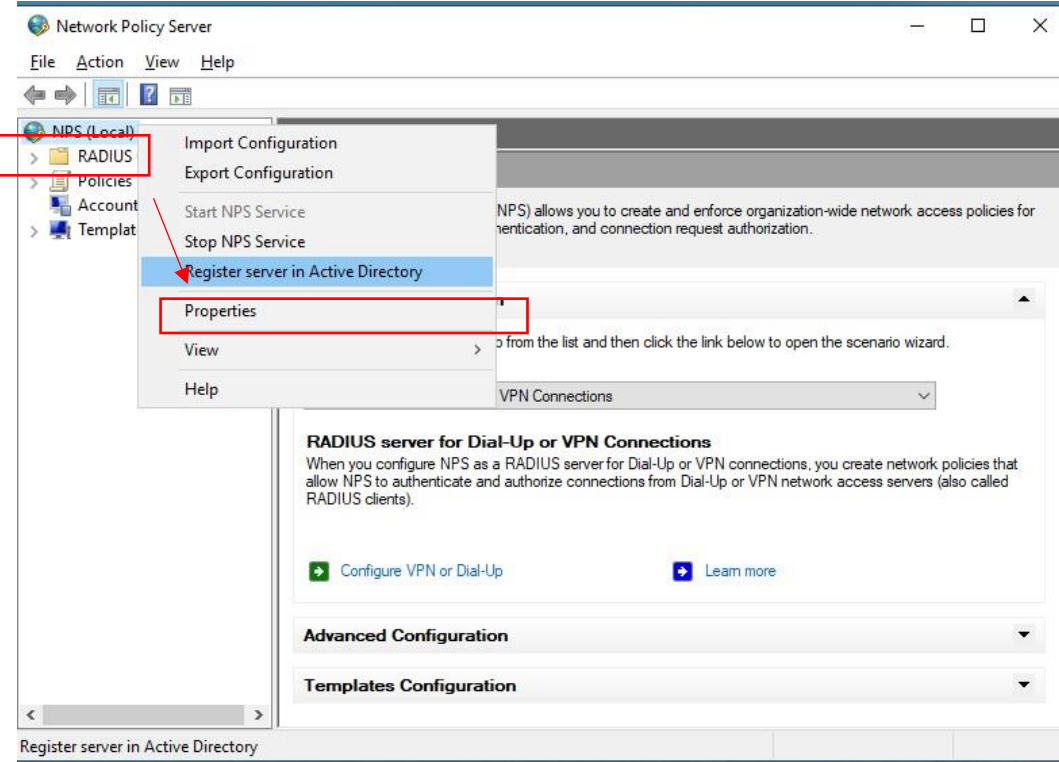
Karşıma gelen menüden ekstra bir servis kurmayacağım için next diyerek **install** menüsü gelene kadar onaylıyor ve install butonuna basarak kurulumu başlatıyorum.



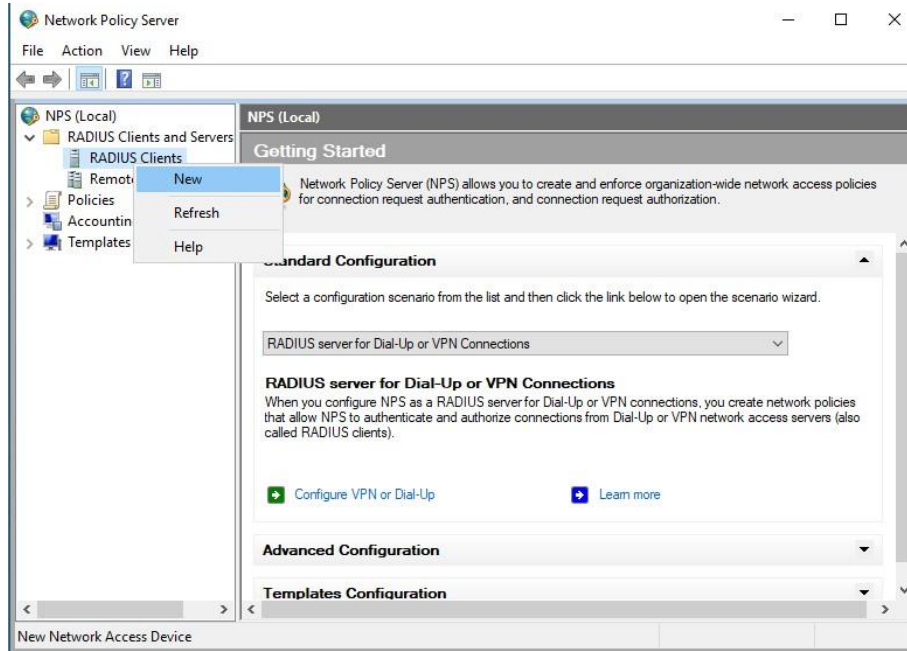
Kurulumu tamamlandığını teyit ediyorum.



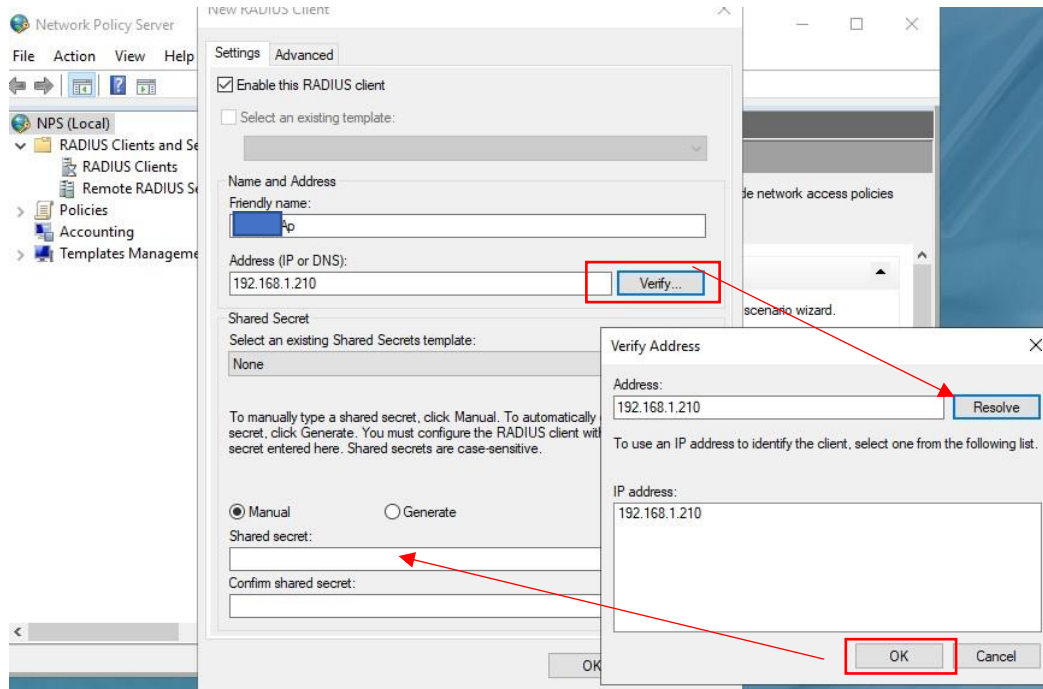
Sonraki adımlarımda NPS servisinin yapılandırmasını yapacağım. Bu nedenle servisi açıyorum ve ilk olarak Active Directory'e register işlemini tamamlamak için **NPS** sekmesine sağ tuş ile **Register server in Active Directory** seçeneğine tıklıyorum. Karşıma gelen uyarılara ok diyerek işlemi tamamliyorum.



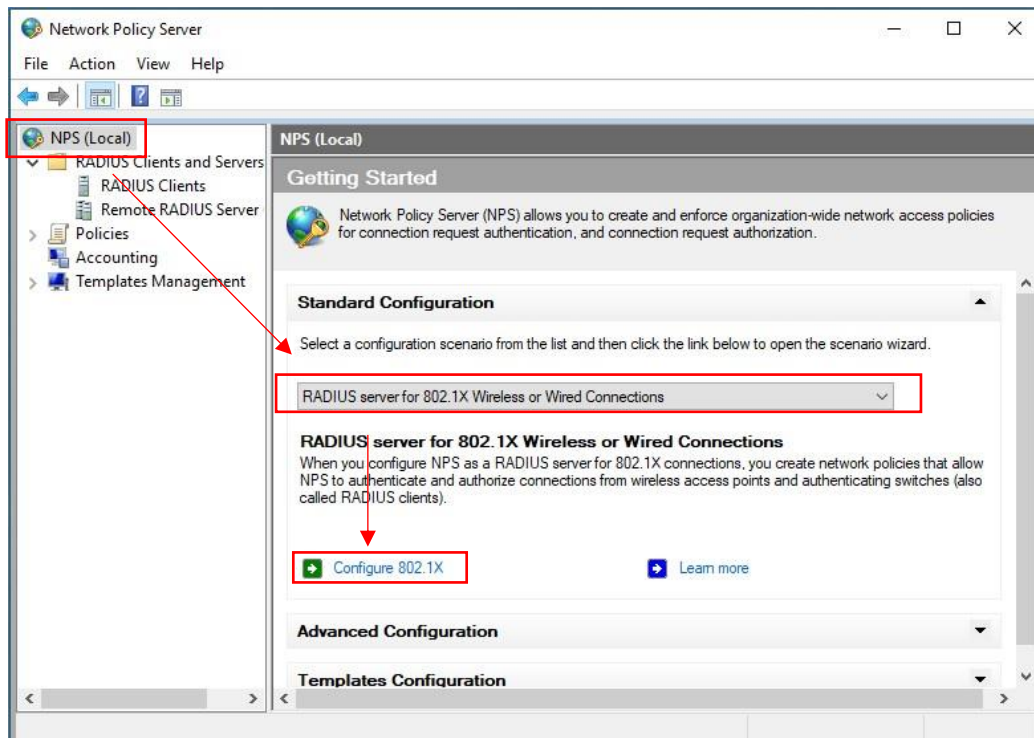
Bir sonraki adımda Radis Client and Serves sekmesinden RADIUS Client Sağ tıklayıp New diyerek Access pointleri ekleme işlemini yapacağım.



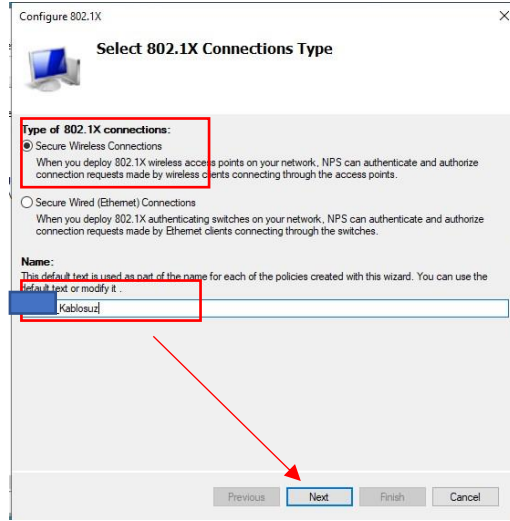
Karşıma gelen ekrandan Access pointlerimi eklemek için gerekli adımları tamamlayacağım. **Adress (IP or DNS)** kısmına AP ip bilgisini girerek **verify** ile doğruluyorum. Karşıma gelen ekrana ok deyip Ap'ler üzerinde RADIUS kısmında eşleştirme yapmak için **Shared select** kısmında bir şifre belirliyorum.



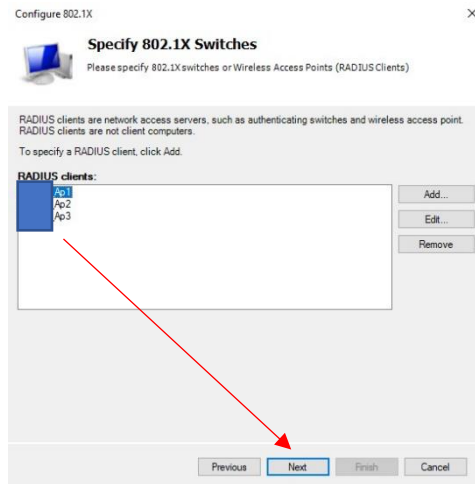
Ap ekleme işlemini tamamladıktan sonra yapılandırmama devam ediyorum. Bu nedenle tekrar **NPS (local)** sekmesine tıklıyorum. Karşıma gelen ekrandan Standart Configuration altından **RADIUS server for 802.1X Wireless or Wired Connections** seçip **Configure 802.1X** Butonuna tıklıyorum.



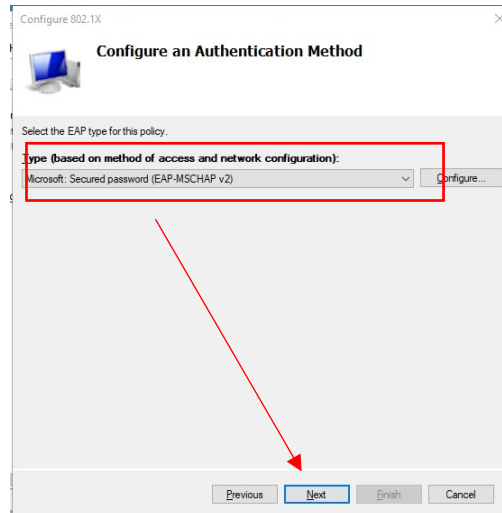
Karşıma gelen ekrandan **Secure Wireless Connections** seçeneğini seçip kuralıma bir isim vererek **next** diyerek bir sonraki adıma geçiyorum.



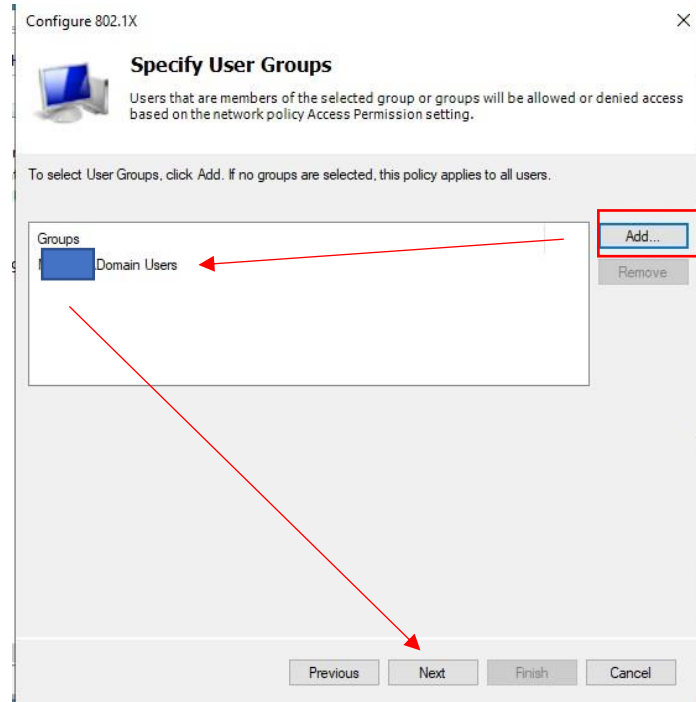
Karşıma gelen menüden AP mi seçip next diyerek ilerliyorum.



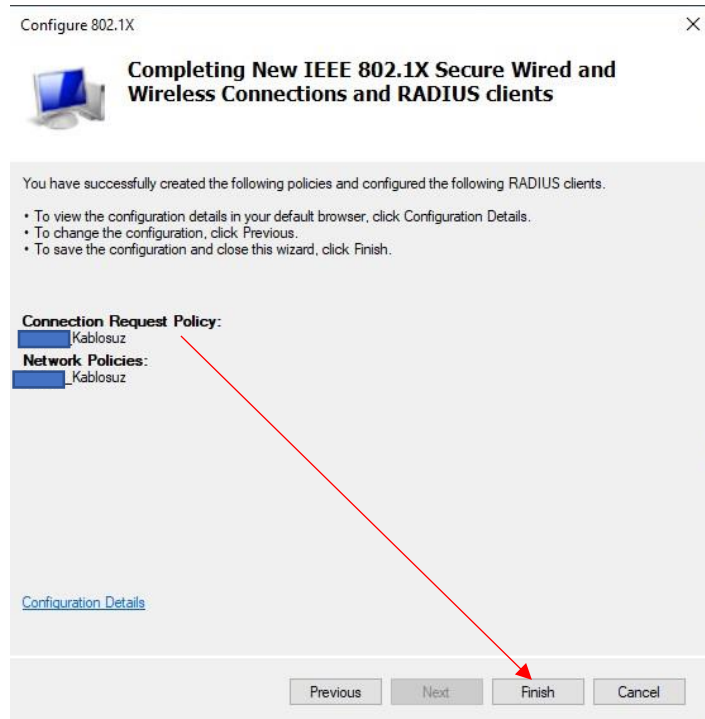
Karşıma gelen menüden Otantike metodunu seçmemi istiyor. **Microsoft Secured password (EAP-MSCHAP v2)** seçerek next diyerek ilerliyorum.



Bir sonraki adımda kuralımızı hangi gruba uygulamamız gerektiği soruluyor. Belirlemiş olduğum bir grubu seçiyorum. Ve next diyorum. .

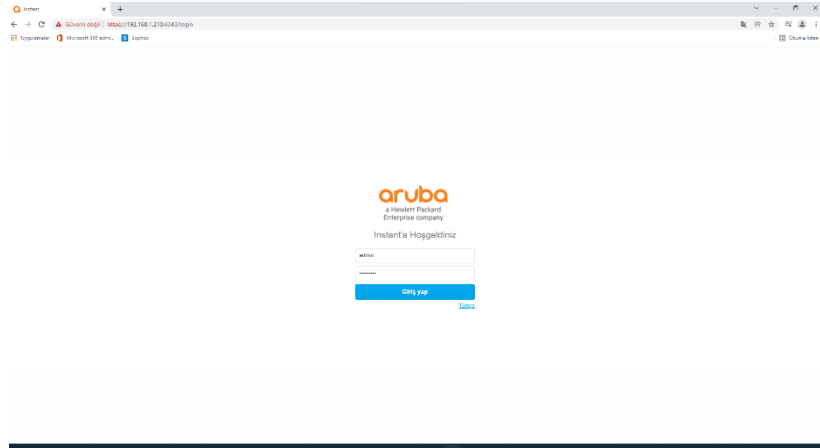


Karşıma gelen ekrandan Next ve finish diyerek işlemimi tamamlıyorum.

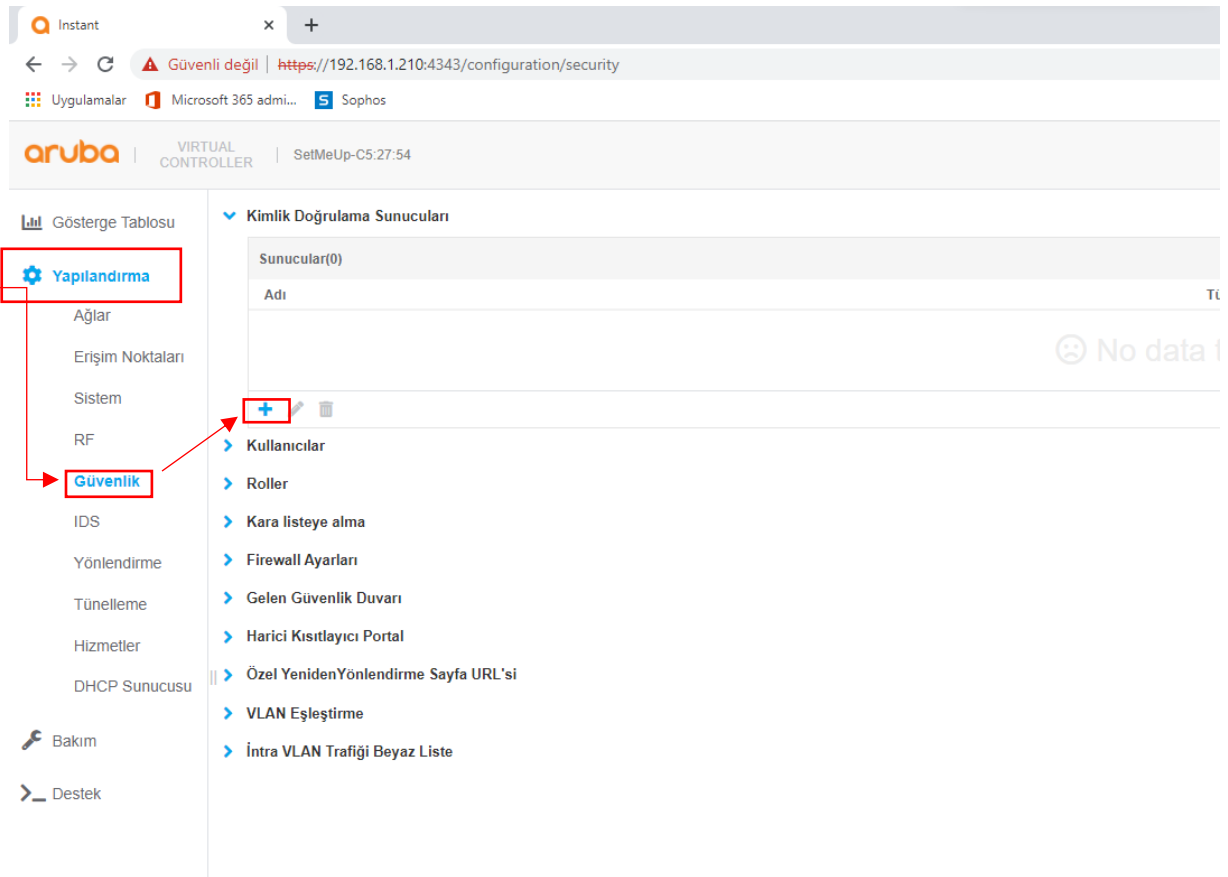




Sonraki adımlarımızda Access Pointler üzerinde yapılandırılmamı başlatmak için Ap ye login oluyorum.



Login olduktan sonra kaşıma gelen **dashboard** ekranından **Yapılandırma** sekmesinin altından **Güvenlik** tabına tıklayarak bir RADIUS doğrulama sunucusu oluşturacağım.





Karşıma gelen RADIUS sunucu menüsünden yapılandırmamı yapıyorum. Tür kısmından RADIUS seçip, Radius türüne bir isim belirliyorum. Ip adresi kısmına NPS rolünü kurduğum sunucumun Ip bilgilerine girip, paylaşılan anahtar kısmında da NPS yapılandırma tarafında vermiş olduğum şifremi girip Tamam diyerek yapılandırmayı tamamliyorum.

Yeni Kimlik Doğrulama Sunucusu

Tür

☒ RADIUS  
☐ LDAP  
☐ TACACS

RADIUS Türü

☐ Yalnız Dinamik Kimlik Doğrulama

Adı

rv

RadSec

☐

IP Adresi

192.168.1.202

Yetkilendirme portu

1812

Hesap tutma portu

1813

Paylaşılan anahtar

\*\*\*\*\*

Tekrar yazma anahtarı

\*\*\*\*\*

Zaman aşımı

5

saniye

İptal

Tamam

Bir sonraki adımda yeni bir ağ oluşturarak radius a entegra etmek için yapılandırma sekmesinden ağlar tabına tıklıyorum. Yeni bir ağ oluşturmak için + butonuna tıklıyorum.

aruba

VIRTUAL CONTROLLERS

SetMeUp-C5 27:54

Gösterge Tablosu

Genel Bakış

Ağlar

Erişim Noktaları

İstemciler

Örgü (Mesh) Cihazları

Yapılandırma

Ağlar

Erişim Noktaları

Sistem

RF

Güvenlik

IDS

Yönlendirme

Tünelleme

Hizmetler

DHCP Sunucusu

Bakım

Destek

Ağlar

	Tür	İstemciler
	wireless	2
	wireless	19
	wireless	4
	wired	0
	wired	0

+

Karşıma gelen menüden yeni ağıma bir isim aşağıdaki ayarları standart bırakıp sonraki diyerek, bir sonraki adıma geçiyorum.

Yeni Ağ | SetMeUp-C5 27:54

Yeni Ağ 1 Temel 2 VLAN 3 Güvenlik 4 Erişim

İsim ve Kullanım

Adı RADIUS

Tür Kablosuz

Birinci kullanım Çalışan

Gelişmiş seçenekleri göster

İptal Sonraki

Bir sonraki ekranda Ayarlarımı standart bırakıyorum ve sonraki butonu tıklayarak ilerliyorum.

aruba | VIRTUAL CONTROLLER | SetMeUp-C5 27:54

Gösterge Tablosu

Yeni Ağ 1 Temel 2 VLAN 3 Güvenlik 4 Erişim

Genel Bakış

Ağlar

Erişim Noktaları

İstemciler

Organizasyon (Mesh) Cihazı

Yapılandırma

Ağlar

Erişim Noktaları

Sistem

RF

Güvenlik

IDS

Yönlendirme

Tünelleme

Hizmetler

DHCP Sunucusu

Bakım

Destek

İstemci IP'si ve VLAN Atama

İstemci IP ataması

Sanal Denetleyiciyle yönetilen

Ağ tarafından atanmış

İstemci VLAN atama

Varsayılan

Statik

Dinamik

İptal Geri Sonraki

Sonraki adımda karşıma gelen menüden ayarlarımı aşağıdaki gibi uyguluyorum. Kimlik doğrulama sunucusu kısmında Daha önce oluşturmuş olduğum sunucumu seçiyor ve sonraki butonuna tıklıyorum.

Aruba VIRTUAL CONTROLLER | SetMeUp-C5.27.54

Yeni Ağ | 1 Temel | 2 VLAN | 3 Güvenlik | 4 Erişim

Gösterge Tablosu | Genel Bakış | Ağlar | Erişim Noktaları | İstemciler | Örgü (Mesh) Cihazı

**Yapılandırma**

**Ağlar**

Erişim Noktaları

Sistem

RF

Güvenlik

IDS

Yönlendirme

Tünelleme

Hizmetler

DHCP Sunucusu

Bakım

Destek

**Güvenlik Düzeyi**

Güvenlik Düzeyi: Kurumsal

Anahtar yönetimi: WPA2-Kurumsal

**Kimlik Doğrulama sunucusu 1** (highlighted with a red box)

Kimlik Doğrulama sunucusu 2: -- Select Server --

EAP yük boşaltma: ☒

Yeniden kimlik doğrulama aralığı: 0 min

MAC kimlik doğrulaması: ☐ 802.1X öncesinde MAC kimlik doğrulaması gerçekleştirir ☐ MAC kimlik doğrulama fail-secure

Kara listeye alma: ☐

DHCP'yi zorla: ☐

**Hızlı Dolanışmada**

Opportunistic Key Caching(OKC): ☐

802.11r: ☐

802.11k: ☒

802.11v: ☒

İptal | Geri | **Sonraki** (highlighted with a red arrow)

Karşıma gelen ekrandan erişim kuralına herhangi bir kısıtlama uygulamayacağım için Son butonuna tıklayarak işlemimi tamamlıyorum.

Aruba VIRTUAL CONTROLLER | SetMeUp-C5.27.54

Yeni Ağ | 1 Temel | 2 VLAN | 3 Güvenlik | 4 Erişim

Gösterge Tablosu | Genel Bakış | Ağlar | Erişim Noktaları | İstemciler | Örgü (Mesh) Cihazı

**Yapılandırma**

**Ağlar**

Erişim Noktaları

Sistem

RF

Güvenlik

IDS

Yönlendirme

Tünelleme

Hizmetler

DHCP Sunucusu

Bakım

Destek

**Erişim Kuralları**

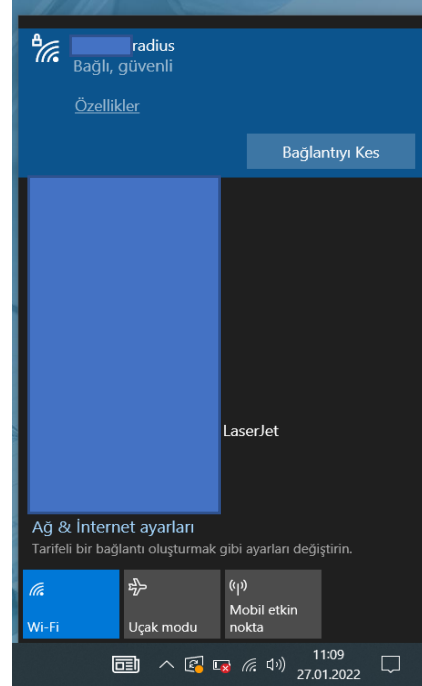
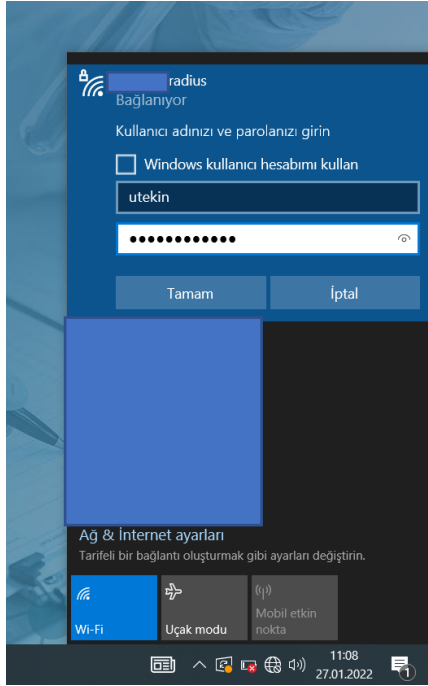
Erişim Kuralları: Kısıtlamalar

Rolleri indir: ☐

Hedef veya trafik türü bazı kısıtlama bulunmamaktadır

İptal | Geri | **Son** (highlighted with a red arrow)

Şimdi testlerimizi yapalım. Kablosuz bağlantı için ağıma seçiyor ve bağlan diyorum. Domain bilgilerimi girerek yapılandırmasını tamamladığı ağa başarılı şekilde bağlanmış oluyorum.



Aynı şekilde Ap dashboardan istemcimi kontrol ettiğimde istemcimi listede görüyorum.

