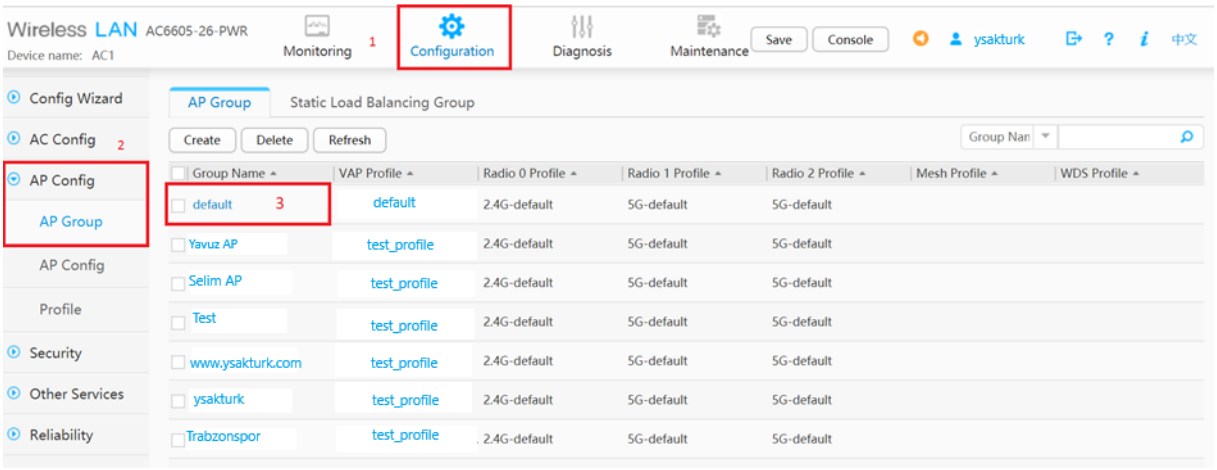
WIFI SSID Yayını

Var olan bir wireless network yapısında yeni bir SSID yayını yapılması istenildiğinde ne yapmamız gerekir? Hiç panik yapmaya gerek yok. İlk olarak Access Controller' ın web arayüzüne giriş yapılır.

Örneğin WAC mgmt ip adresi 192.168.100.1 olduğunu varsayalım.

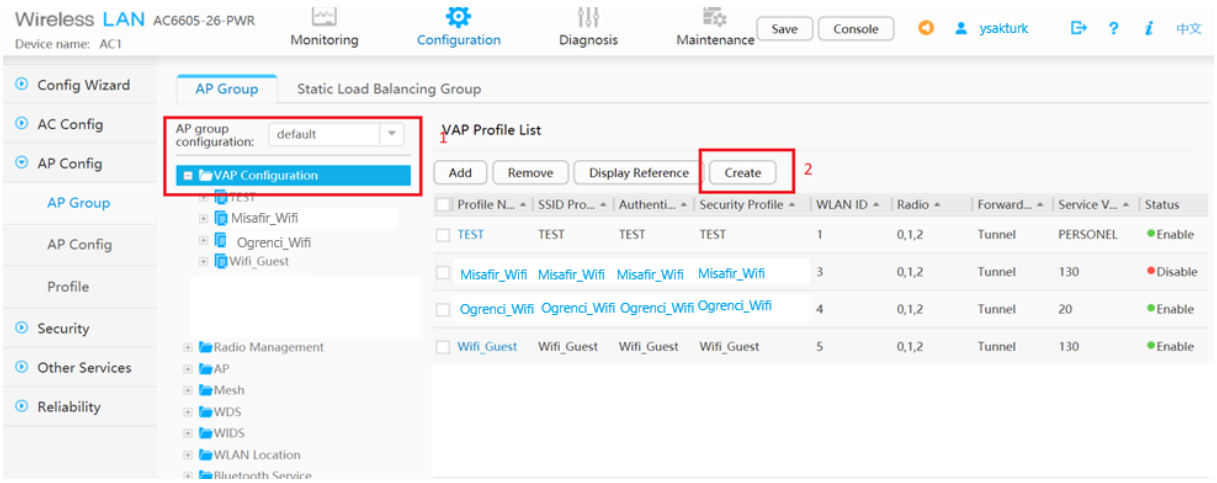
https://192.168.100.1/view/login.html

Açılan anasayfa ekranında; üst kısımda yer alan "Configuration" sekmesine giriş yapıp sonrasında sol kısımda yer alan "AP Config → AP Group" kısmına geçiş yapılır. AP Group altına girilince "default" yazan profili seçeriz.

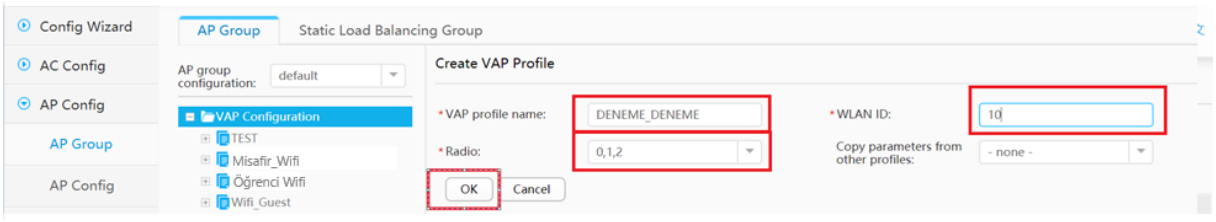


"default" seçtikten sonra açılan ekran içerisinde VAP Configuration içerisinde VAP Profile oluşturulması gerekmektedir. VAP Profile altında gereksinimlere göre SSID Profile, Security Profile, Authentication Profile ve Traffic Profile oluşturulabilir.

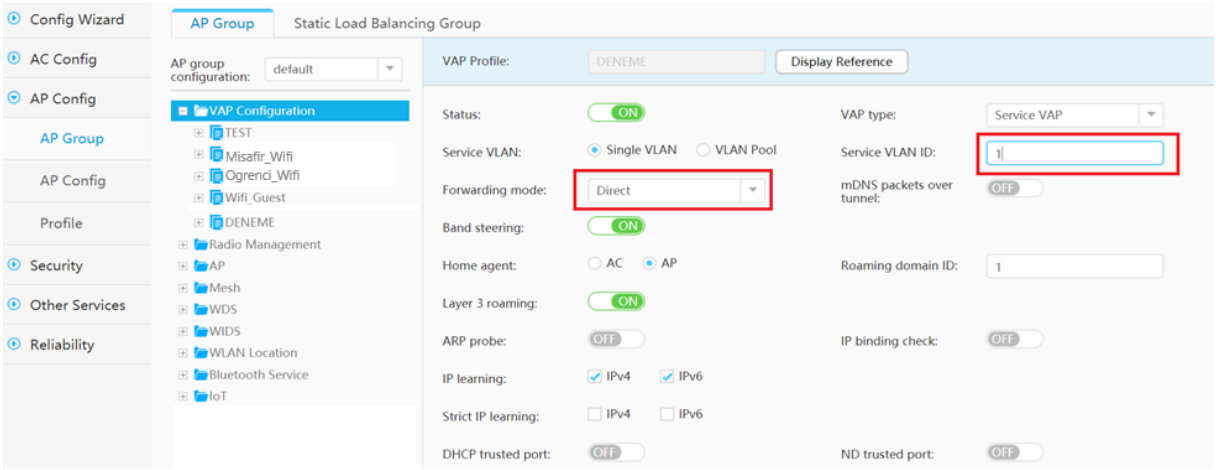
İlk olarak VAP Profile' a tıklanıp Create butonu seçilerek VAP profile oluştururuz.



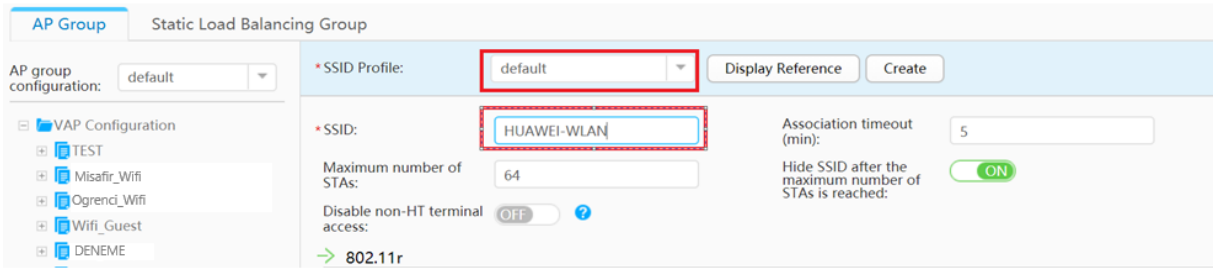
Create dedikten sonra açılan ekranda VAP Profile adı verilir ve bu profil içerisinde hangi wifi frekans kanalları çalışacak ise ilgili seçimler gerçekleştirilir. Seçenek olarak 0, 2.4 ve 5 GHz opsiyonları mevcuttur. Frekans kanallarından sonra son olarak WLAN ID seçiminin yapılması gerekir. Burada boş ya da uygun olan WLAN ID seçiminin yapılması gerekmektedir. Seçim yapıldıktan sonra OK denilip süreç tamamlanır ve VAP profile oluşmuş olur.



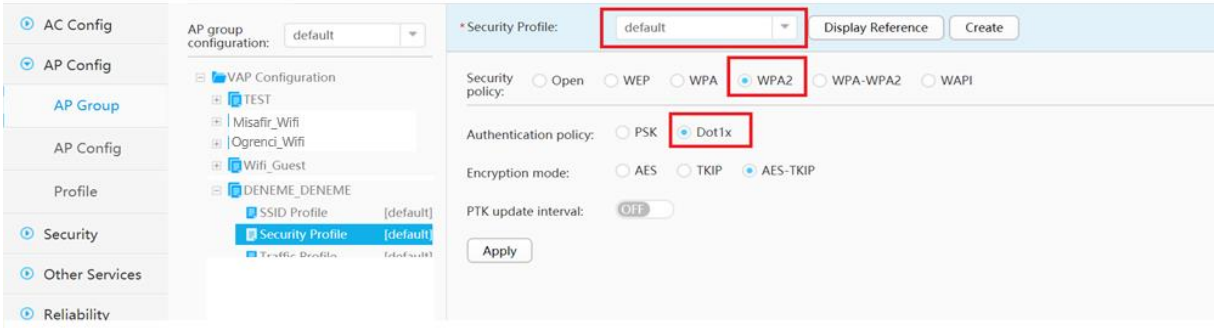
Oluşturulan VAP Profil ve Service Vlan bilgisi ile ”Forwarding Mode Direct” seçilir ve böylelikle kullanıcı data trafiği CAPWAP tunnel içerisinden geçmeyip doğrudan destination yani hedef adrese yönlendirilir. Tunnel modda, data paketleri Access Controller’ a ulaşıp sonrasında hedefe doğru yoluna devam eder. Fakat management data paketleri her zaman ve her koşulda daima CAPWAP tunnel içerisinden geçerek hedefe doğru ilerler. Hangi modda olduğunun bir önemi yoktur.



Daha sonraki adımda; DENEME isimli VAP Profilinin içerisine girilerek SSID Profile adı ve yayınlanacak olan SSID ismi belirlenir. SSID yayını gizli yapılacaksa yani SSID name görünmeyecek ise “others” kısmından aktif ya da pasif duruma çekilebilir.

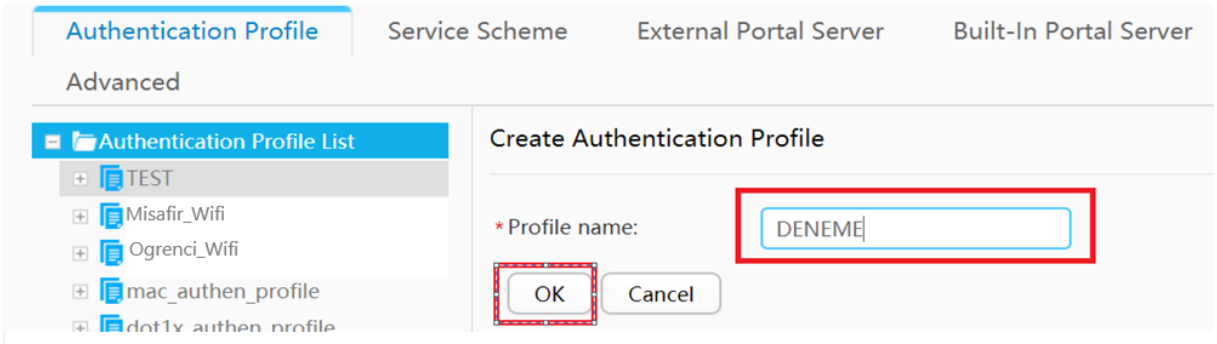


Yine DENEME VAP Profili altından Security Profile ekranına girerek kullanıcı kimlik doğrulamasının yöntemi seçilebilir. WPA2 seçilir ise ve authentication policy pre shared key aktif edilirse burada şifre ile kimlik doğrulama yöntemi aktif edilmiş olur. Dot1x doğrulama yöntemi kullanılacak ise yine WPA1 seçilip authentication policy dot1x aktif edilerek uygulanabilir. En son Apply denilerek konfig kaydedilir ve işlem gerçekleştirilmiş olur.



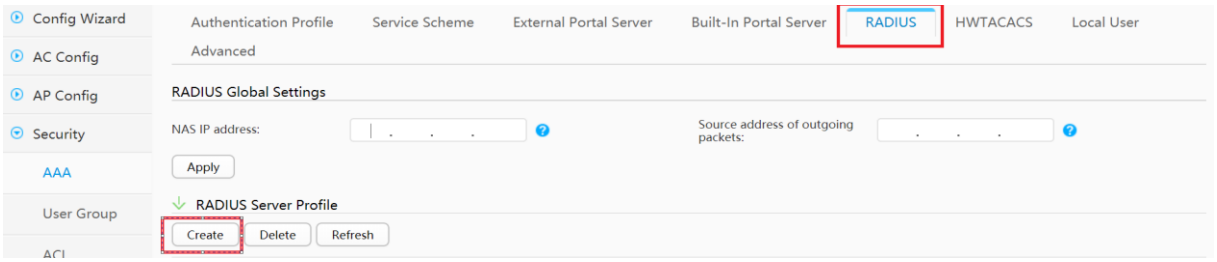
Öncelikle Authentication Profile oluşturmamız gerekir ve burada dot1x profile Radius profile authentication scheme profillerinin oluşturulması gerekir.

"Configuration→Security→AAA→Authentication Profile→Authentication Profile List→Create"

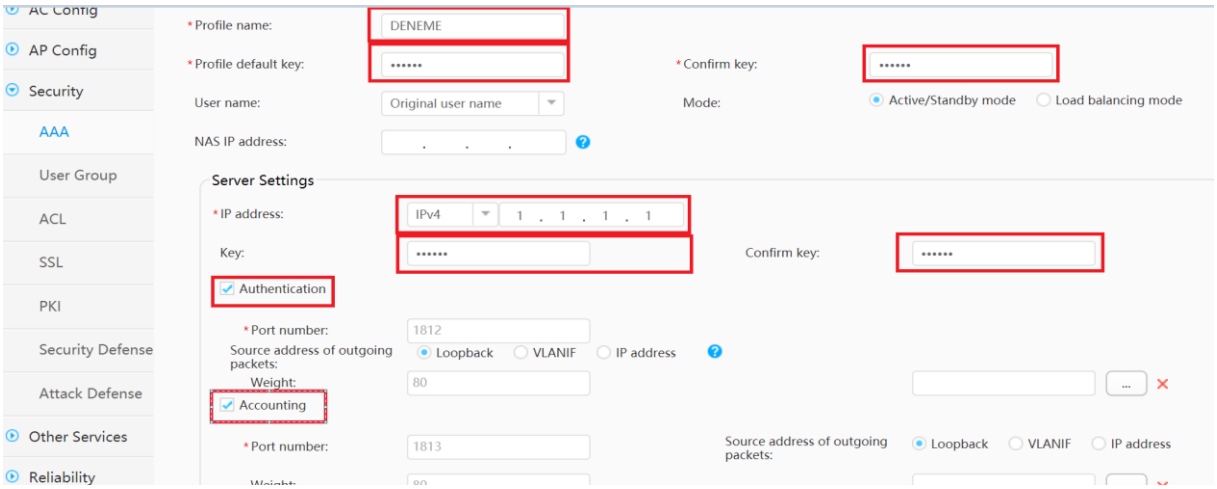


Authentication Profile oluştururken Radius Server tanımlamalarının da yapılması gerekir. Uygulanması gereken adım şu şekildedir:

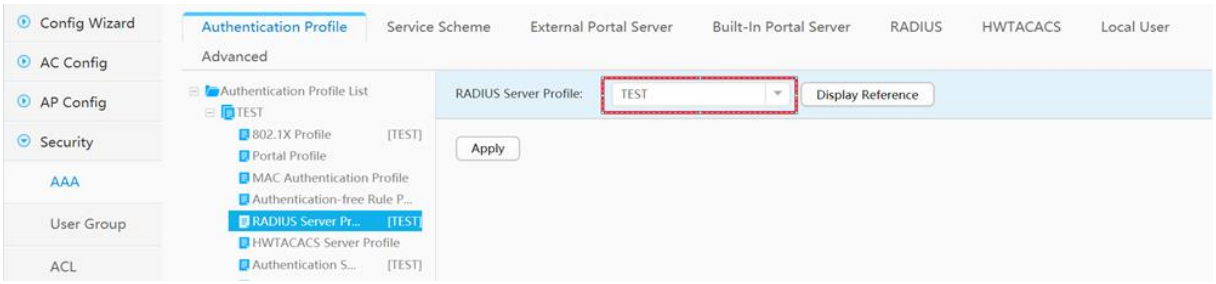
"Configuration→Security→AAA→RADIUS"



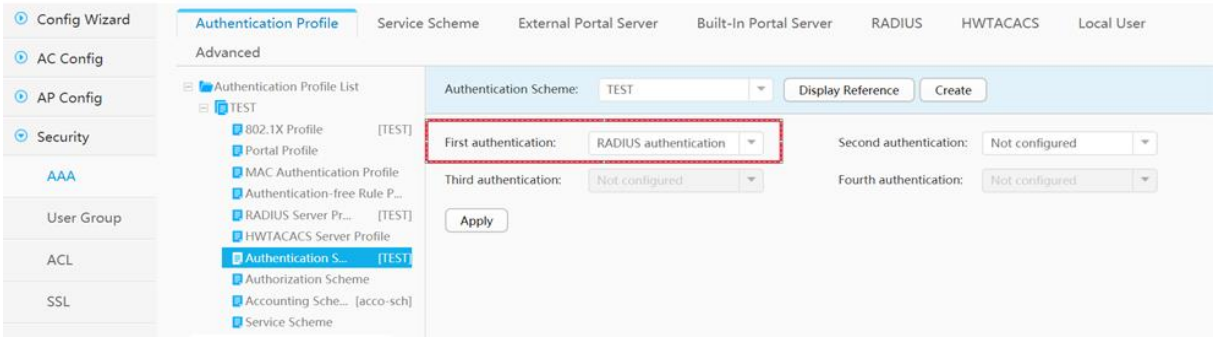
İlgili adım takip edilerek açılan ekranda Radius Server Profile oluşturularak profil name, Radius Server IP, Shared Key gibi bilgiler ilgili alanlara yazılır.

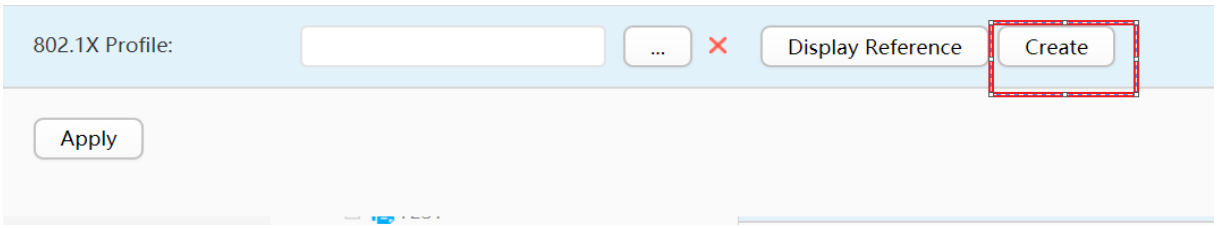


Oluşturulan Radius Profile, ilgili Authentication Profile bağlanır.

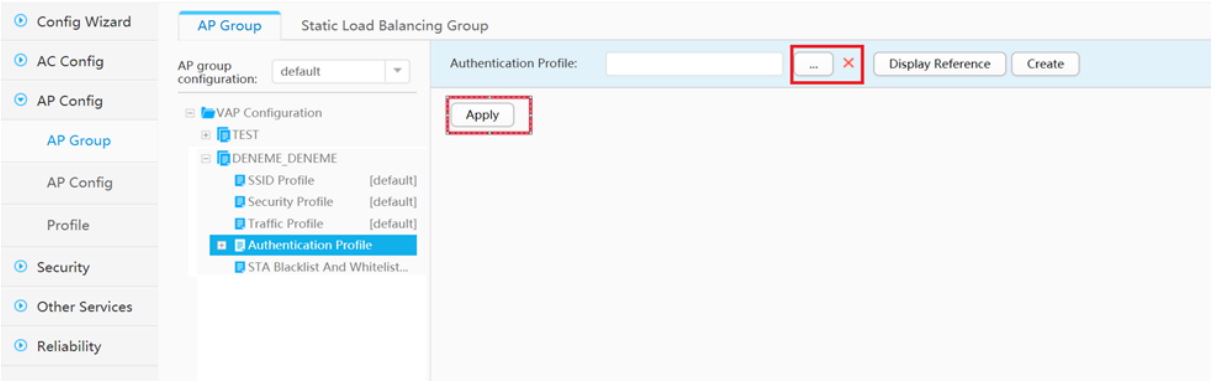


Daha sonrasında ise Authentication Scheme profili oluşturulur ve Authentication sürecinin nasıl olacağı yani Radius Authentication seçilir ve ardından Dot1x profile oluşturulur. Profile name belirlenir.





En son adım olarak da oluşturulan Authentication Profile, daha önce oluşturulmuş olan VAP Profile içerisine uygulanır.



İşlem bu kadar.. 😊