Cisco Catalyst 9800 WLC Entegrasyon Rehberi

Bu rehber, **Cisco Catalyst 9800** serisi kablosuz denetleyici (WLC, sanal 9800-CL dahil) ile Useroam Cloud arasındaki misafir hotspot entegrasyonunu adım adım anlatır. Misafir, WLC'nin şifresiz misafir ağına bağlanır; telefonunda Useroam karşılama sayfası açılır (SMS, WhatsApp, oda numarası ve diğer giriş yöntemleri); kimlik doğrulaması RADIUS ile Useroam'da yapılır ve misafir internete çıkar.

> **Başlamadan önce:** WLC web arayüzüne yönetici erişimi, WLC'nin internete çıktığı **genel (dış) IP adresi** ve IOS-XE 17.x sürümü gerekir. Bu rehberdeki ekranlar 17.15 sürümünden alınmıştır; diğer 17.x sürümlerinde menü adları aynıdır.

> **Useroam sunucu adresi her yerde 104.247.174.120'dir.** RADIUS sunucusu, giriş sayfası adresi ve giriş öncesi izin listesi (ACL) bu IP ile yazılır. Başka bir adres kullanmayın.

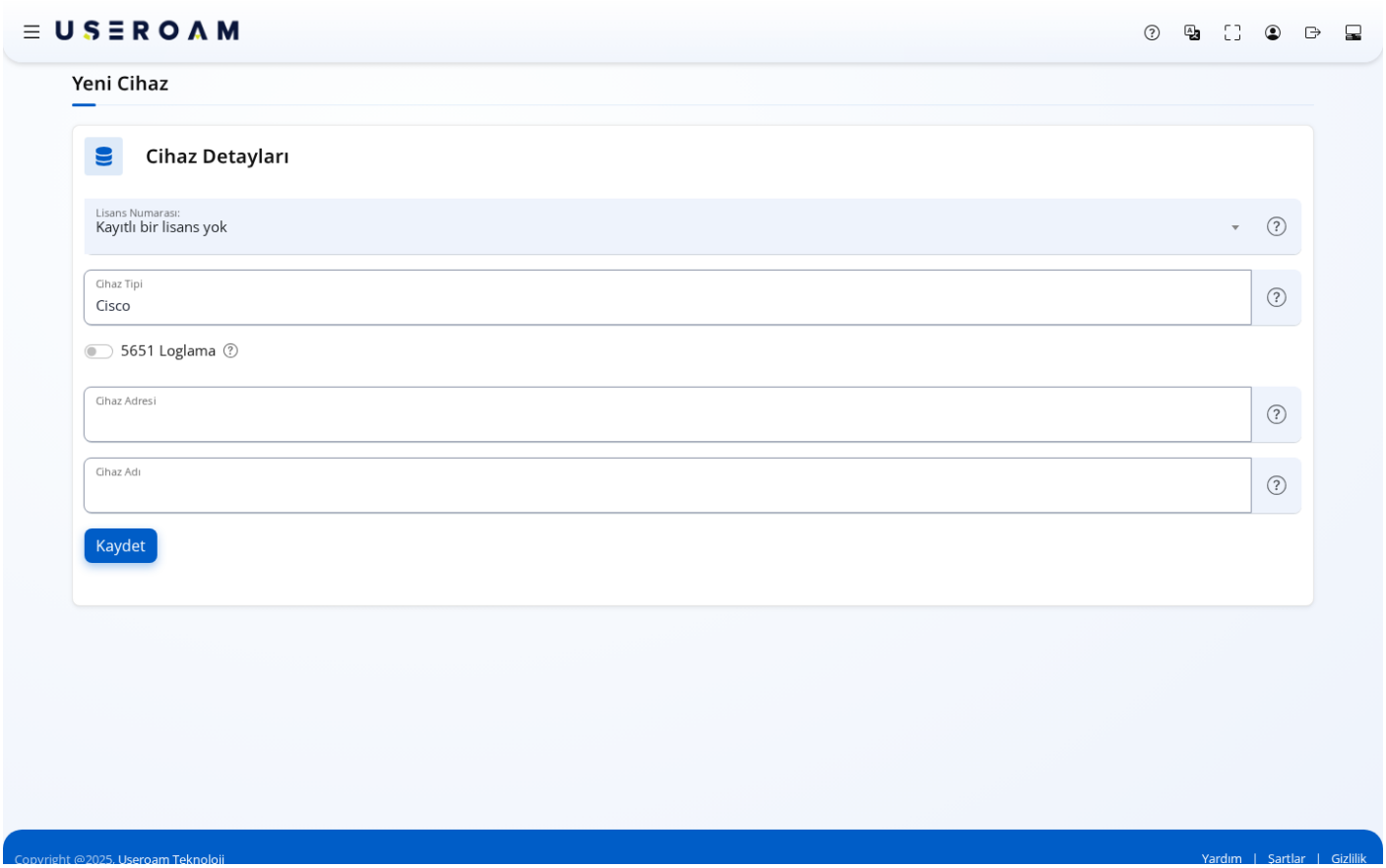
> **Controller bir firewall'un arkasında mı?** Misafir girişini FortiGate, Sophos gibi bir firewall yapacaksa WLC'de bu rehberdeki ayarlara gerek yoktur; WLC yalnızca açık bir SSID yayınlar.
>
> Bu durumda ilgili firewall rehberini izleyin: FortiGate, Sophos.

1 - Useroam Paneline Cihaz Ekleme

panel.useroam.com adresinden panelinize giriş yapıp **Yeni Cihaz** ekranını açın.

- **Cihaz Tipi:** `Cisco` seçin.
- **5651 Loglama:** internet çıkışını yapan cihaz (firewall veya router) loglarını Useroam'a gönderiyorsa açın.
- **Cihaz Adresi: [KRİTİK ADIM]** WLC'nin internete çıktığı genel (dış) IP adresini yazın. WLC bir NAT arkasındaysa NAT'ın çıkış IP'si yazılır. Useroam cihazı bu IP'den tanır; RADIUS istekleri de bu IP'den gelmelidir. WLC'nin iç IP'sini (192.168.x.x, 10.x.x.x) yazmayın.
- **Cihaz Adı:** panelde göreceğiniz ad (ör. "Otel WLC").

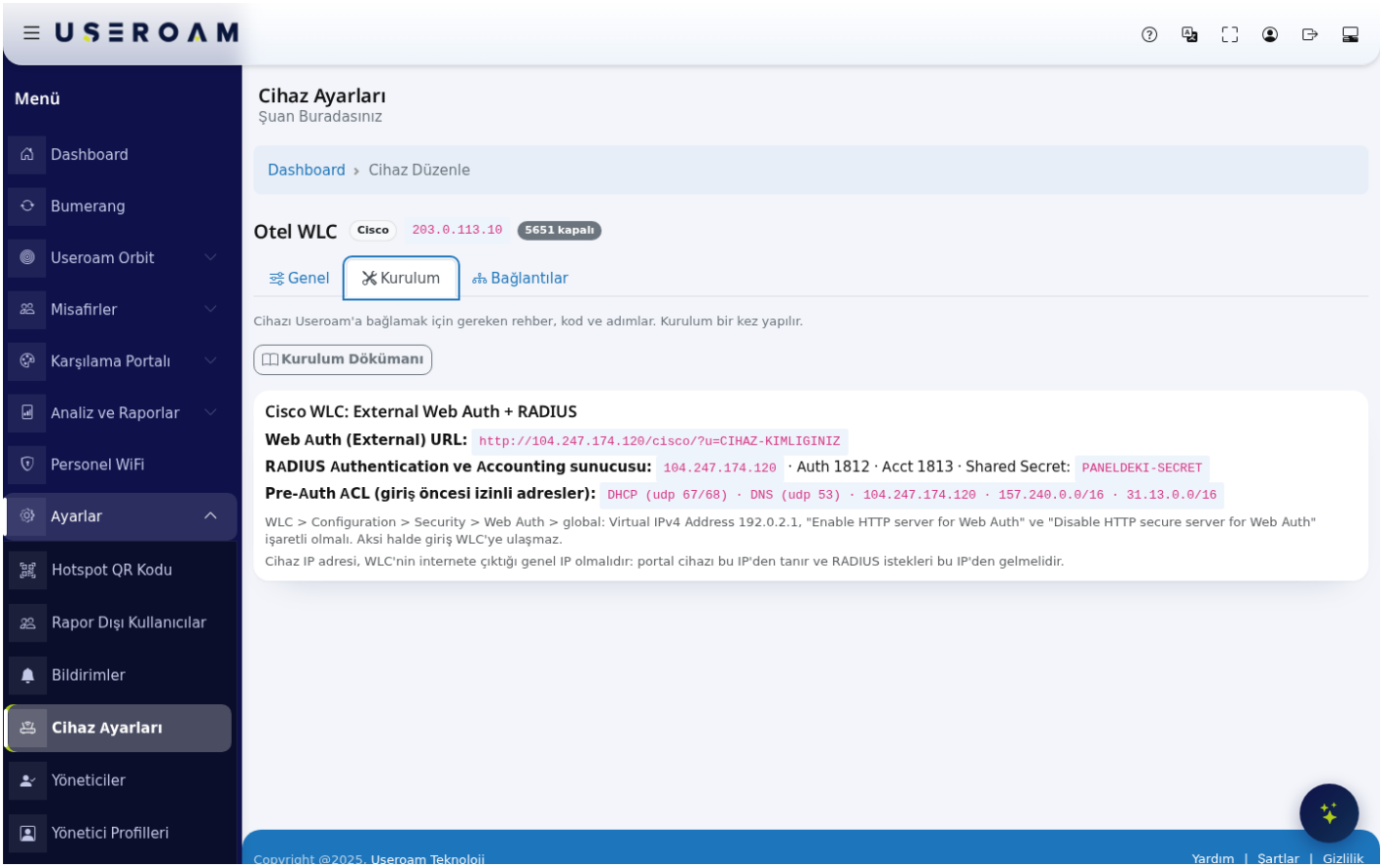
Kaydet düğmesine basın.



2 - Kurulum Bilgilerini Panelden Alma

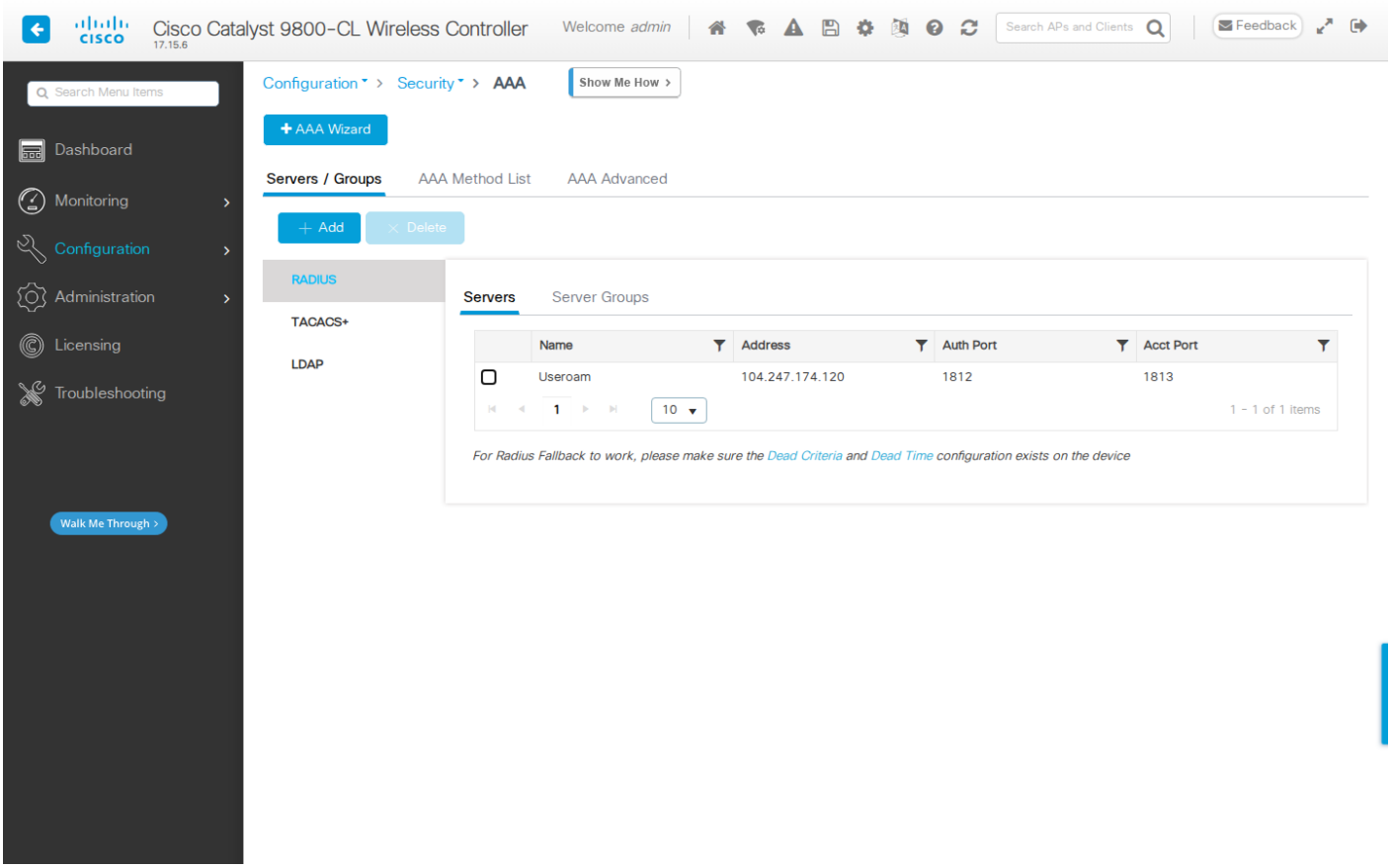
Cihaz kaydedildikten sonra **Ayarlar > Cihaz Ayarları** sayfasında **Kurulum** sekmesini açın. **Cisco WLC: External Web Auth + RADIUS** kartında sonraki adımlarda kullanacağınız üç bilgi yazar; bunları bir kenara not edin:

- **Web Auth (External) URL:** `http://104.247.174.120/cisco/?u=...` biçiminde, **cihazınıza özel** giriş sayfası adresi. `?u=` sonrasındaki kod cihazınızın kimliğidir; adresi olduğu gibi kopyalayın.
- **RADIUS sunucusu ve Shared Secret:** sunucu `104.247.174.120`, Auth 1812, Acct 1813 ve cihazınıza özel paylaşılan anahtar.
- **Pre-Auth ACL:** misafir giriş yapmadan önce erişebilmesi gereken adresler.



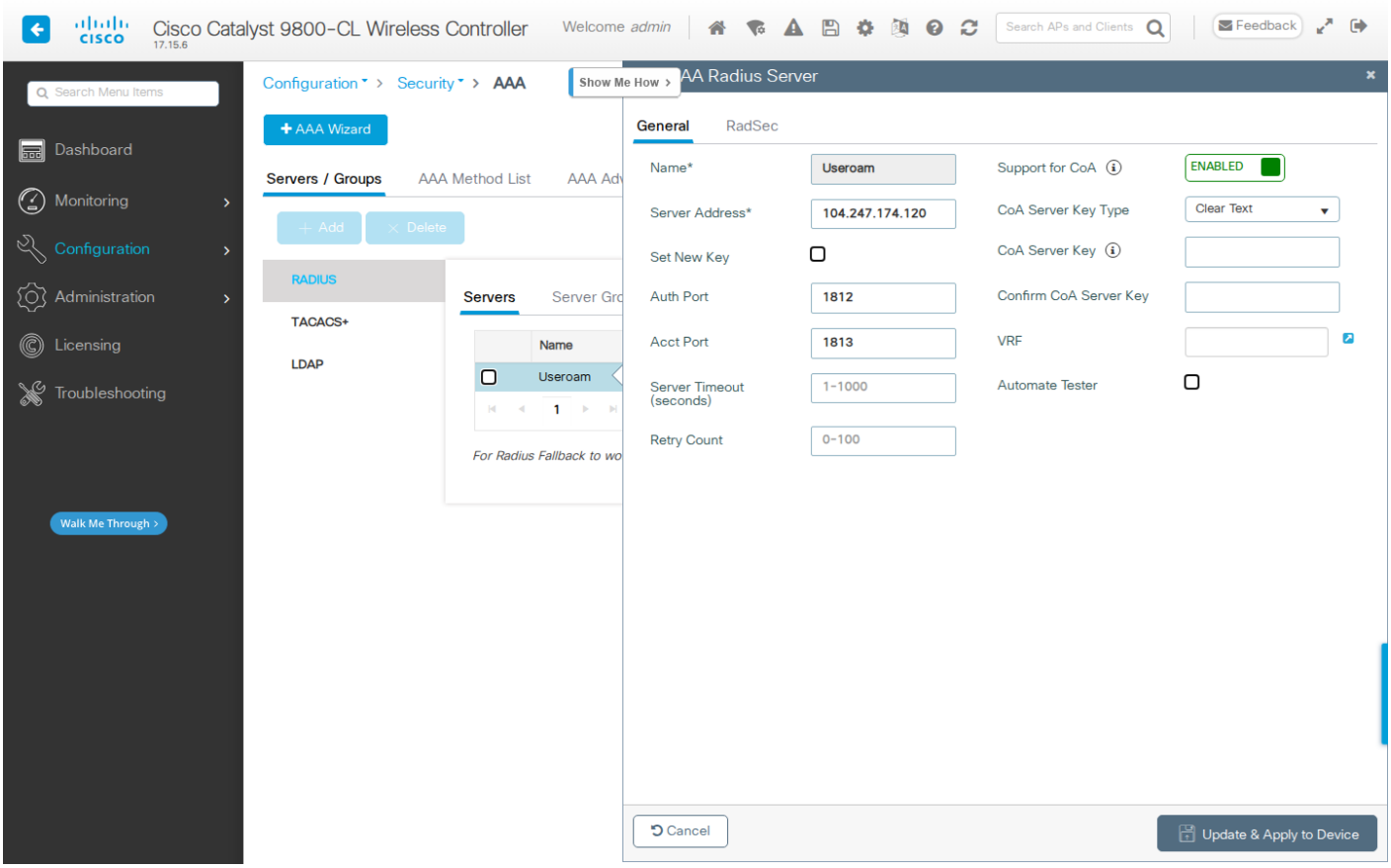
3 - RADIUS Sunucusunu Tanımlama

WLC web arayüzünde **Configuration > Security > AAA** yolunu izleyin. **Servers / Groups** sekmesinde sol listeden **RADIUS**, üstte **Servers** seçiliyken **+ Add** düğmesine basın.



- **Name:** `Useroam`
- **Server Address:** `104.247.174.120`
- **Key / Confirm Key:** paneldeki **Shared Secret** değeri (iki alana da aynısı).
- **Auth Port:** `1812`, **Acct Port:** `1813`
- **Support for CoA:** zorunlu değildir.

Apply to Device ile kaydedin.

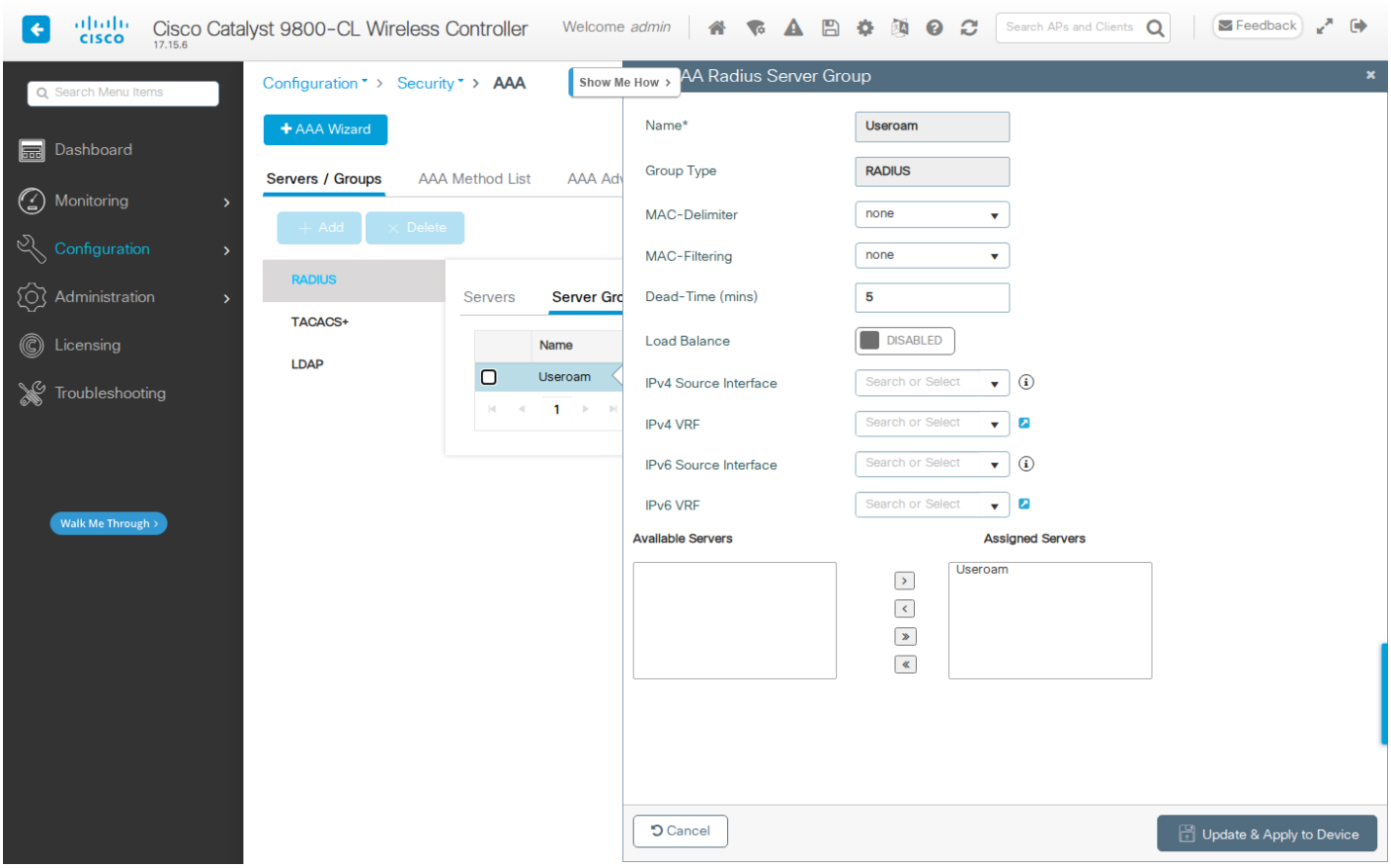


4 - RADIUS Sunucu Grubu Oluşturma

Aynı ekranda **Server Groups** sekmesine geçip **+ Add** düğmesine basın.

- **Name:** `Useroam`
- **Group Type:** `RADIUS`
- **Dead-Time (mins):** `5`
- **Available Servers** listesindeki `Useroam` sunucusunu **>** okuyla **Assigned Servers** listesine taşıyın.

Apply to Device ile kaydedin.

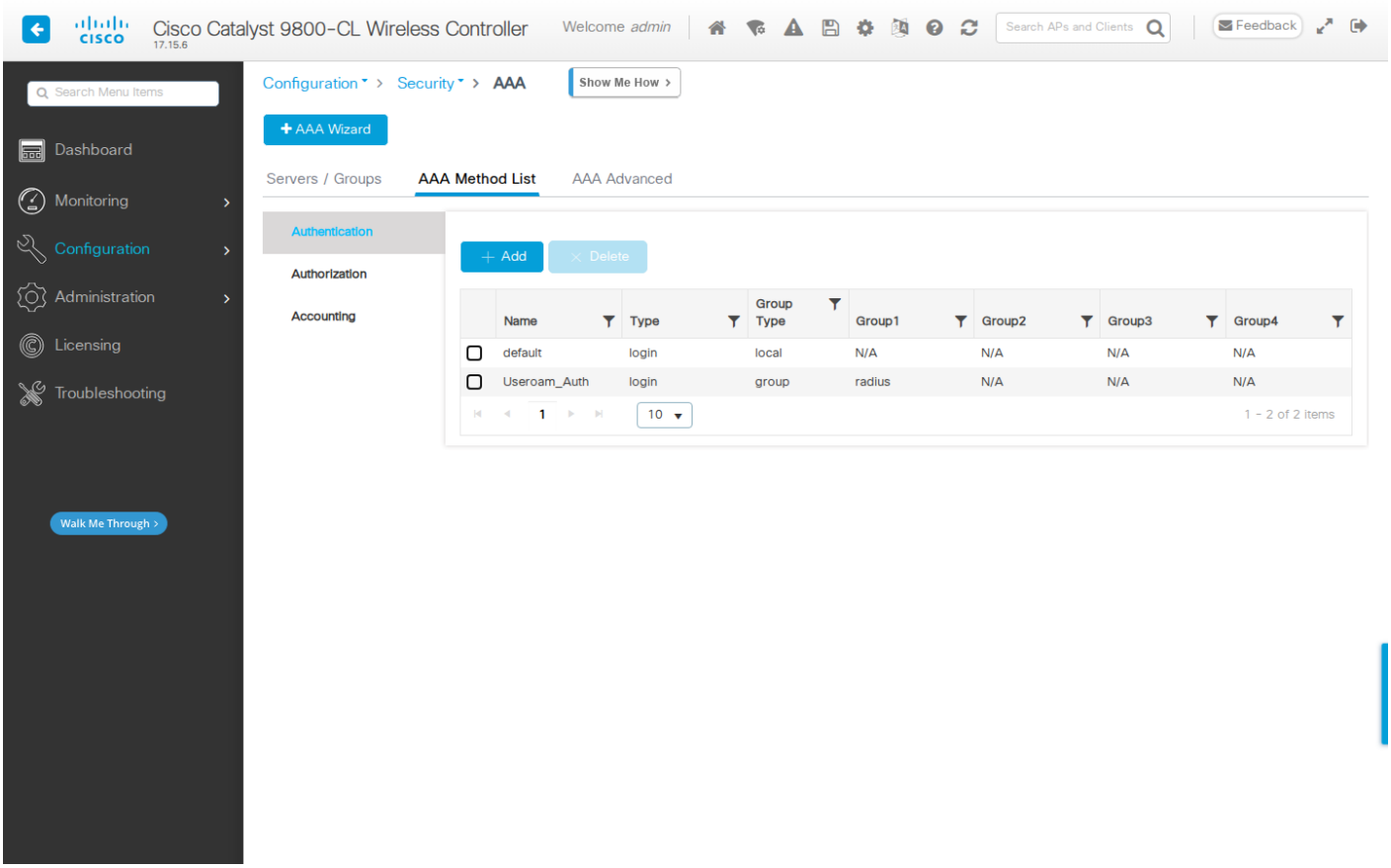


5 - Kimlik Doğrulama ve Accounting Yöntem Listeleri

AAA Method List sekmesine geçin.

Authentication bölümünde **+ Add**:

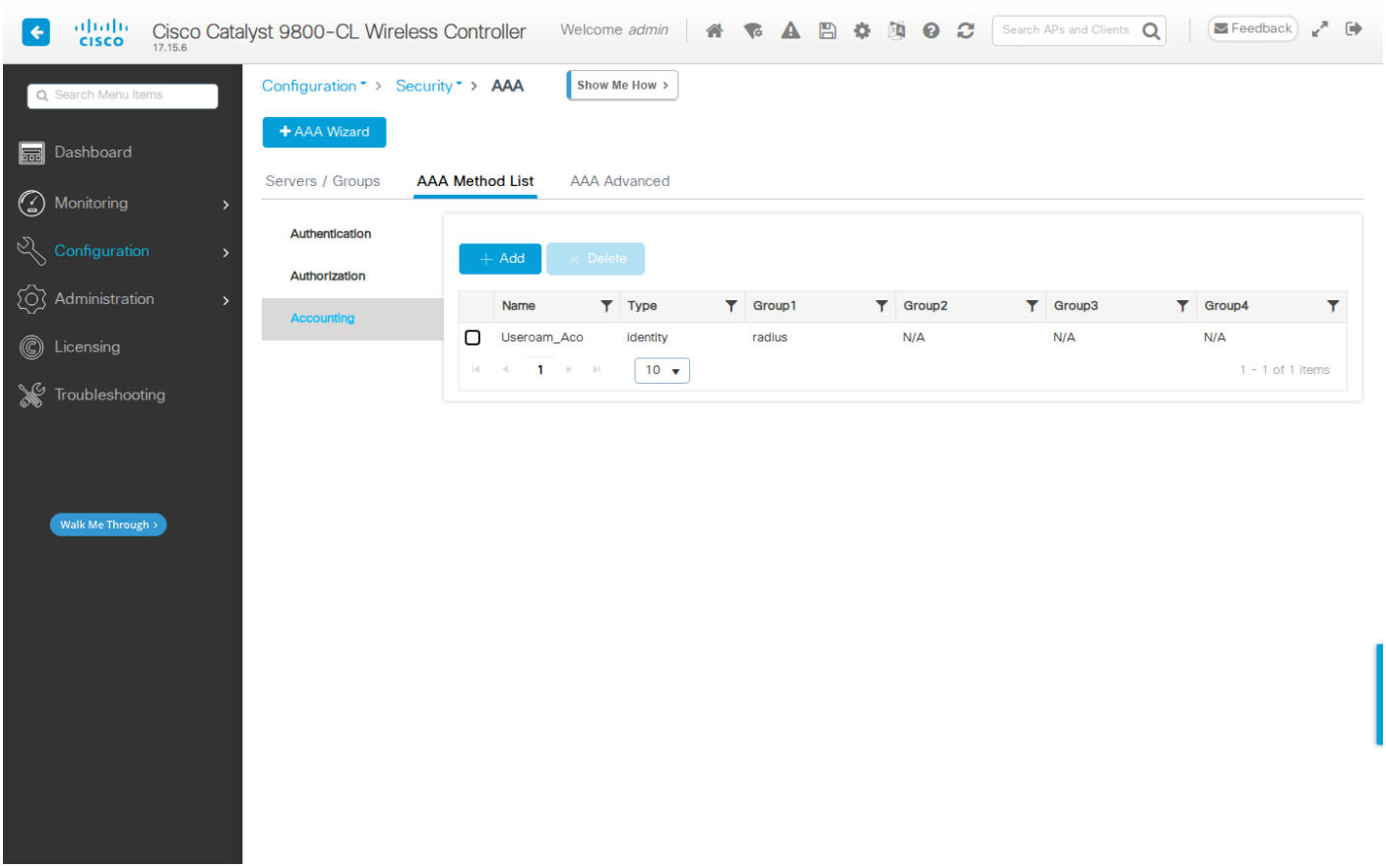
- **Method List Name:** `Useroam_Auth`
- **Type:** `login`
- **Group Type:** `group`
- **Assigned Server Groups:** `Useroam` grubunu taşıyın. (Görseldeki lab cihazında WLC'de başka RADIUS sunucusu olmadığı için genel `radius` grubu seçilidir; sizde başka sunucular da varsa mutlaka `Useroam` grubunu seçin.)



Accounting bölümünde **+ Add**:

- **Method List Name:** `Useroam_Aco`
- **Type:** `identity`
- **Group Type:** `group`, **Assigned Server Groups:** `Useroam`

Accounting, panelde **Aktif Misafirler** ve kullanım raporlarının dolması için gereklidir.



6 - Ara Accounting ve AP Bilgisi (Komut Satırı)

Aşağıdaki iki ayar web arayüzünde değil, komut satırında yapılır. **Administration > Command Line Interface** ekranından ya da SSH ile `configure terminal` modunda girin:

```
aaa accounting update newinfo periodic 5
radius-server attribute wireless accounting call-station-id ap-macaddress-ssid
```

- **Birinci satır:** açık oturumlar için her 5 dakikada bir kullanım güncellemesi gönderir; aktif kullanıcı sayısı ve veri kullanımı doğru görünür.
- **İkinci satır:** accounting kayıtlarına misafirin bağlı olduğu **AP'nin MAC adresi ve SSID** bilgisini ekler (hangi AP'den bağlandığı).

> Bu ayarlardan önce açılmış oturumlar eski biçimde kalır; yeni bağlanan misafirlerde geçerli olur.

7 - Giriş Öncesi İzin Listesi (Pre-Auth ACL)

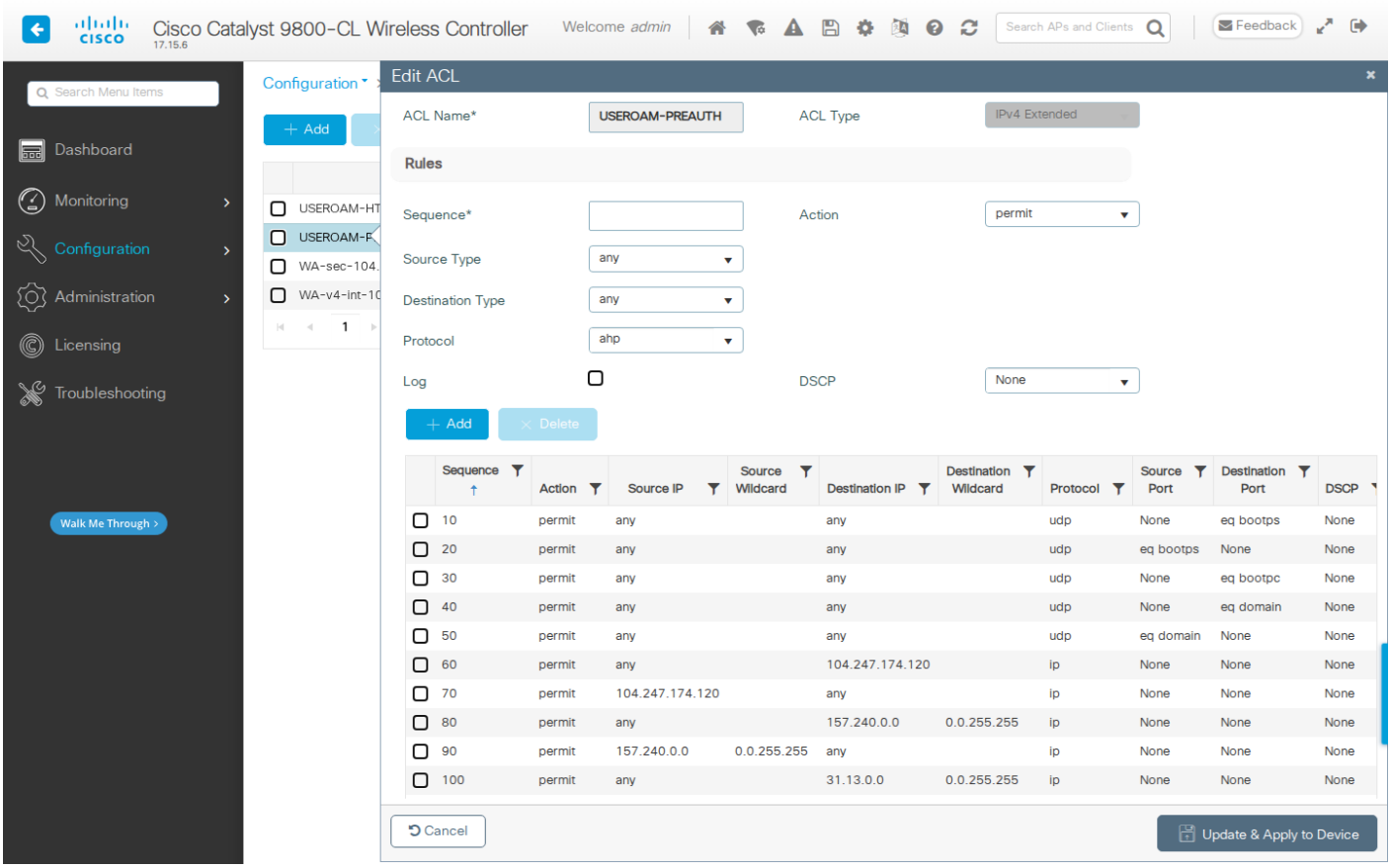
Misafir giriş yapmadan önce yalnızca IP adresi alabilmeli, isim çözebilmeli ve Useroam giriş sayfasına ulaşabilmelidir. **Configuration > Security > ACL** yolunda **+ Add** düğmesine basın.

- **ACL Name:** `USEROAM-PREAUTH`
- **ACL Type:** `IPv4 Extended`

Kuralları sırayla **Add** ile ekleyin:

Sıra	Action	Protokol	Kaynak	Hedef	Açıklama
10	permit	udp	any	any, port eq bootps	DHCP (IP alma)
20	permit	udp	any, port eq bootps	any	DHCP dönüşü
30	permit	udp	any	any, port eq bootpc	DHCP
40	permit	udp	any	any, port eq domain	DNS sorgusu
50	permit	udp	any, port eq domain	any	DNS cevabı
60	permit	ip	any	host 104.247.174.120	Useroam giriş sayfası
70	permit	ip	host 104.247.174.120	any	Useroam dönüşü
80	permit	ip	any	157.240.0.0 0.0.255.255	WhatsApp ile giriş
90	permit	ip	157.240.0.0 0.0.255.255	any	WhatsApp dönüşü
100	permit	ip	any	31.13.0.0 0.0.255.255	WhatsApp ile giriş
110	permit	ip	31.13.0.0 0.0.255.255	any	WhatsApp dönüşü

> 80 ile 110 arası kurallar, misafirin **WhatsApp ile giriş** yapabilmesi içindir (doğrulama mesajı giriş tamamlanmadan WhatsApp'tan gönderilir). Portalınızda WhatsApp girişi kapalıysa bu dört kuralı eklemeyebilirsiniz.



Komut satırıyla aynı liste:

```
ip access-list extended USEROAM-PREAUTH
 10 permit udp any any eq bootps
 20 permit udp any eq bootps any
 30 permit udp any any eq bootpc
 40 permit udp any any eq domain
 50 permit udp any eq domain any
 60 permit ip any host 104.247.174.120
 70 permit ip host 104.247.174.120 any
 80 permit ip any 157.240.0.0 0.0.255.255
 90 permit ip 157.240.0.0 0.0.255.255 any
 100 permit ip any 31.13.0.0 0.0.255.255
 110 permit ip 31.13.0.0 0.0.255.255 any
```

8 - Web Auth Genel Ayarı (global)

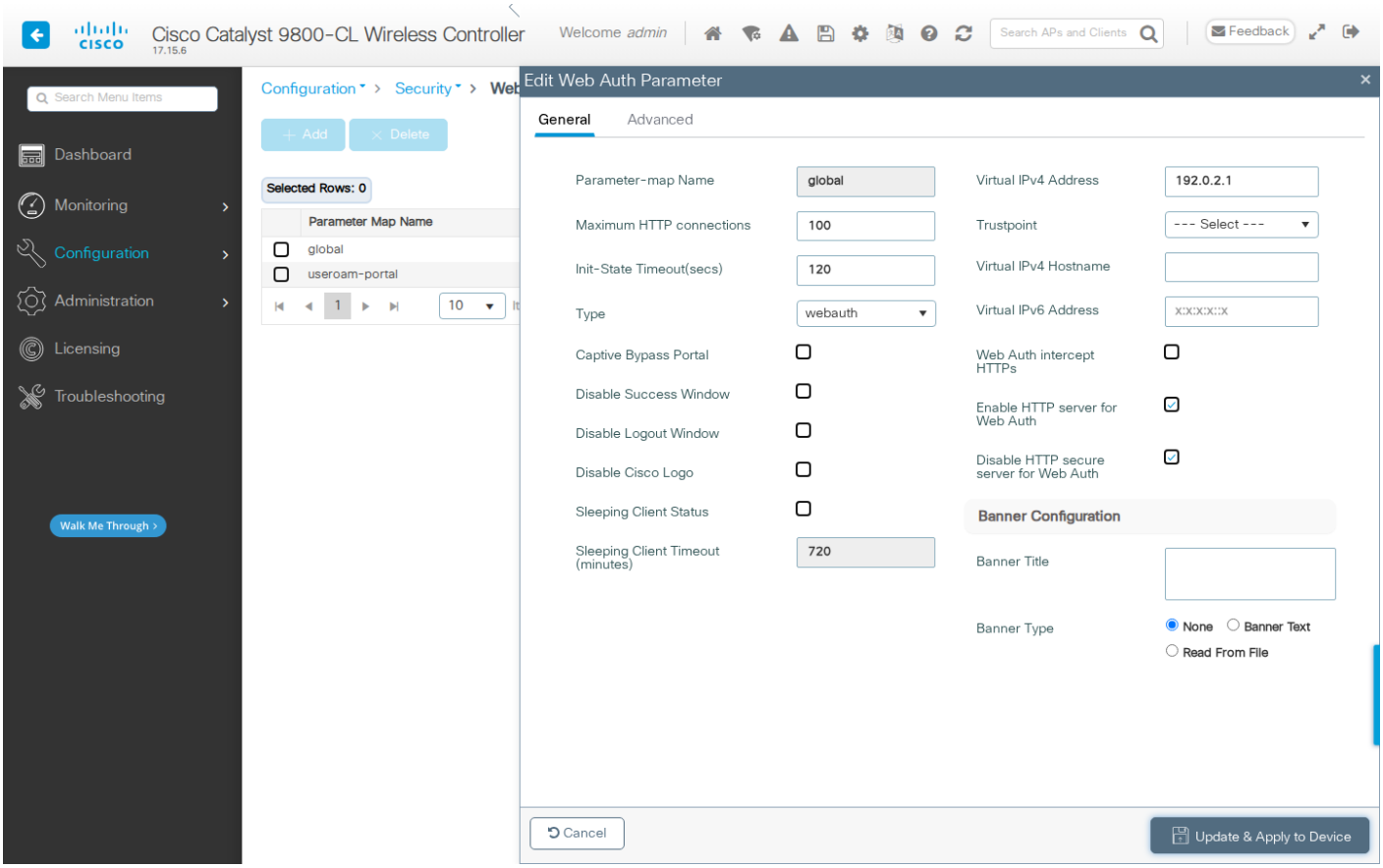
Configuration > Security > Web Auth listesinde **global** satırına tıklayın.

- **Virtual IPv4 Address:** `192.0.2.1` (WLC'nin giriş sayfası için kullandığı sanal adres; ağınızda gerçek bir cihaza verilmemiş olmalıdır).

- **Enable HTTP server for Web Auth:** işaretli.
- **Disable HTTP secure server for Web Auth: işaretli**.
- **Web Auth intercept HTTPs:** işaretsiz.

> **Bu adım atlanırsa giriş çalışmaz.** Güvenli (https) web auth açıkken misafirin tarayıcısı, WLC'nin kendi imzaladığı sertifikayı kabul etmediği için giriş bilgisini WLC'ye hiç göndermez; misafir "giriş yapılıyor" ekranında kalır ve Useroam'a hiçbir RADIUS isteği gelmez.

Update & Apply to Device ile kaydedin.



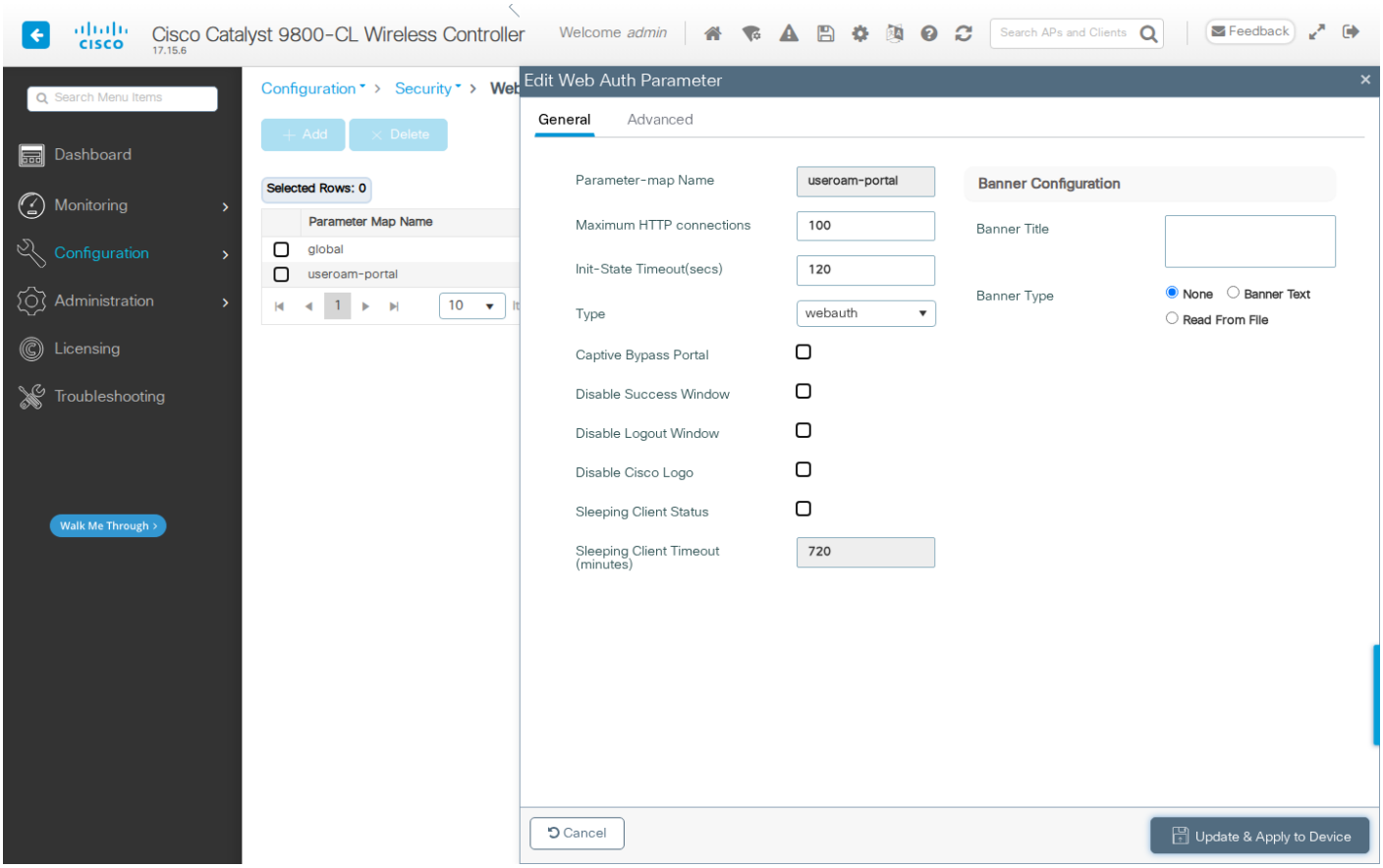
WLC'nin web sunucusu açık olmalıdır (komut satırında `ip http server`); kapalıysa misafir giriş sayfasına yönlendirilmez.

9 - Useroam Giriş Sayfası Parametre Haritası

Aynı **Web Auth** ekranında **+ Add** düğmesine basın.

- **Parameter-map Name:** `useroam-portal`
- **Type:** `webauth`

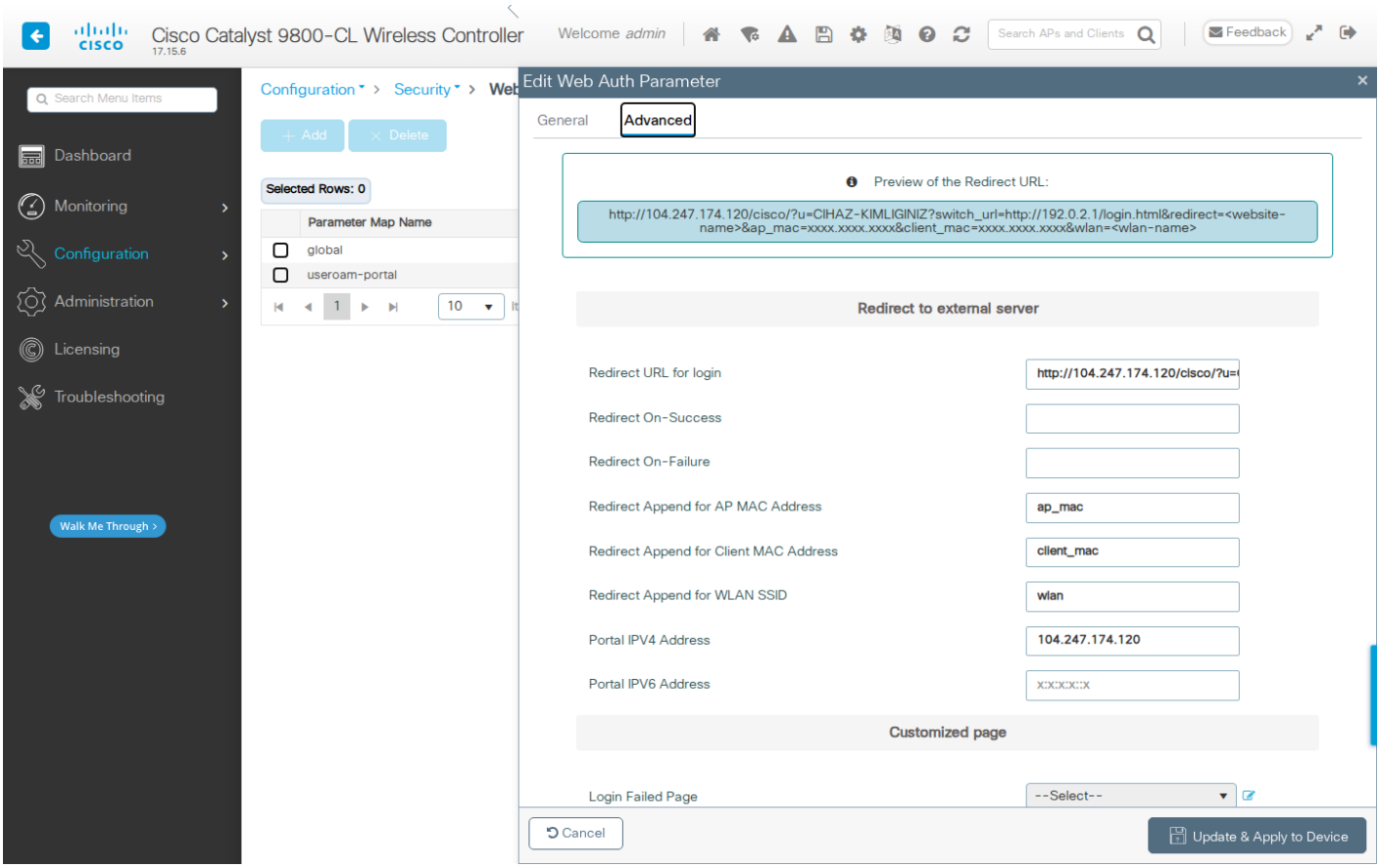
- Diğer alanlar varsayılan kalabilir (Maximum HTTP connections 100, Init-State Timeout 120).



Kaydettikten sonra `useroam-portal` satırına tıklayıp **Advanced** sekmesini açın:

- **Redirect URL for login:** paneldeki **Web Auth (External) URL** değerinin tamamı (`http://104.247.174.120/cisco/?u=...`).
- **Redirect On-Success / On-Failure:** boş bırakın (giriş sonrası sayfayı Useroam yönetir).
- **Redirect Append for AP MAC Address:** `ap_mac`
- **Redirect Append for Client MAC Address:** `client_mac`
- **Redirect Append for WLAN SSID:** `wlan`
- **Portal IPV4 Address:** `104.247.174.120`

Ekranın üstündeki **Preview of the Redirect URL** kutusunda, WLC'nin misafiri gönderdiği adresin önizlemesi görünür. Adresin `http://104.247.174.120/cisco/?u=` ile başladığını kontrol edin. WLC kendi parametrelerini ikinci bir `?` ile ekler; bu normaldir, Useroam bunu doğru okur.

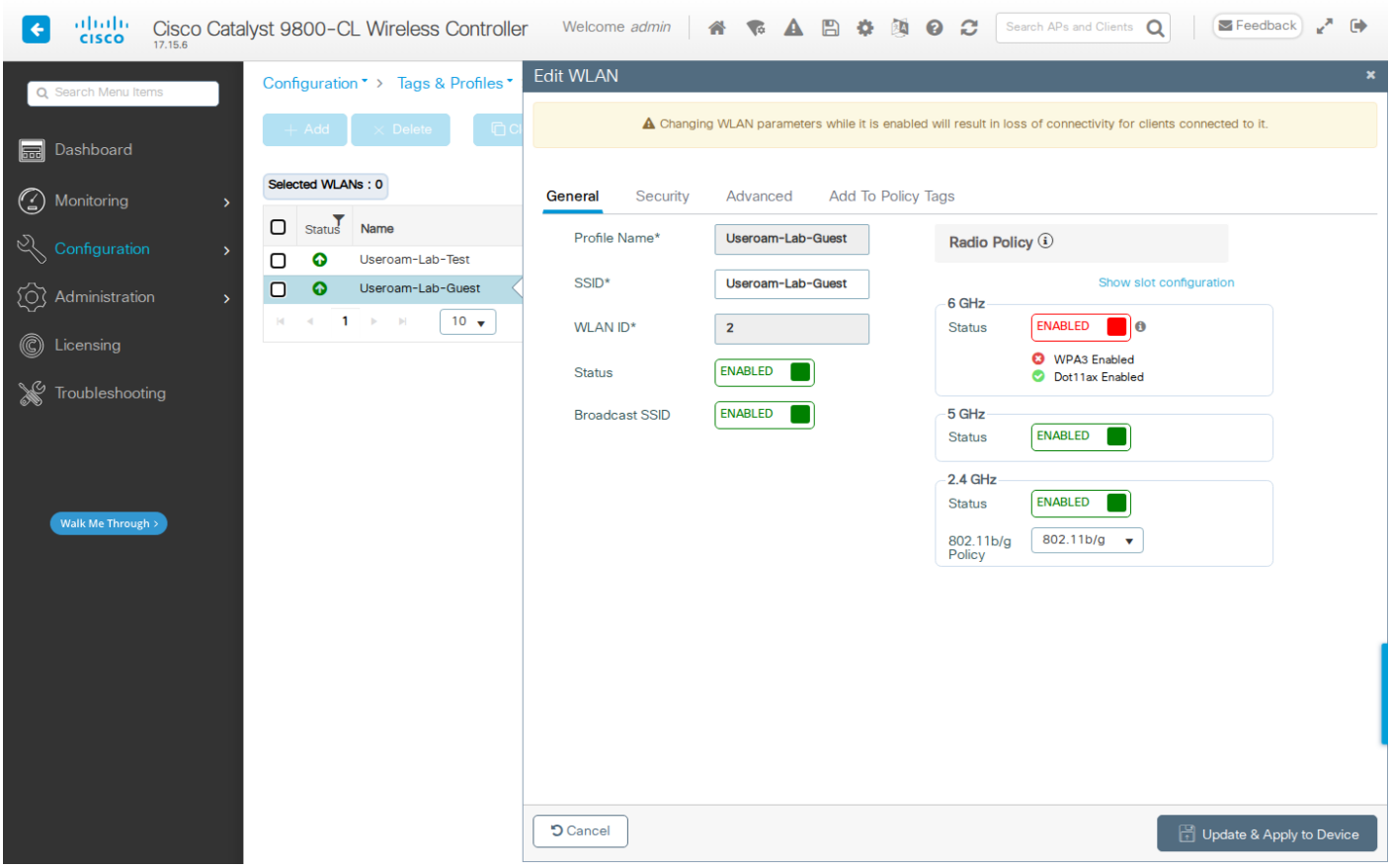


10 - Misafir WLAN'ı (SSID)

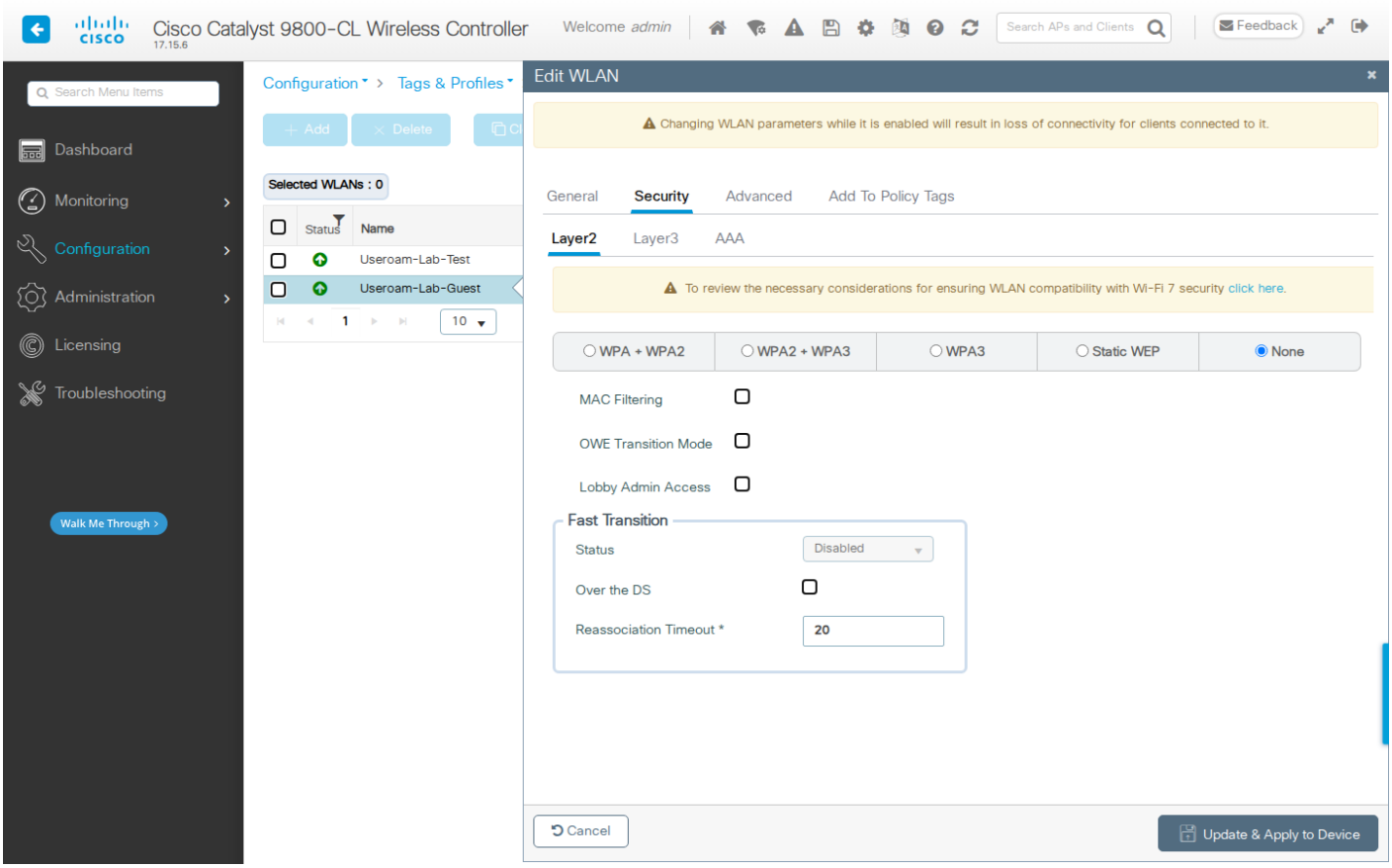
Configuration > Tags & Profiles > WLANs yolunda **+ Add** düğmesine basın.

General sekmesi:

- **Profile Name** ve **SSID:** misafirlerin göreceği ağ adı (ör. `Otel-Misafir`).
- **Status:** ENABLED, **Broadcast SSID:** ENABLED.



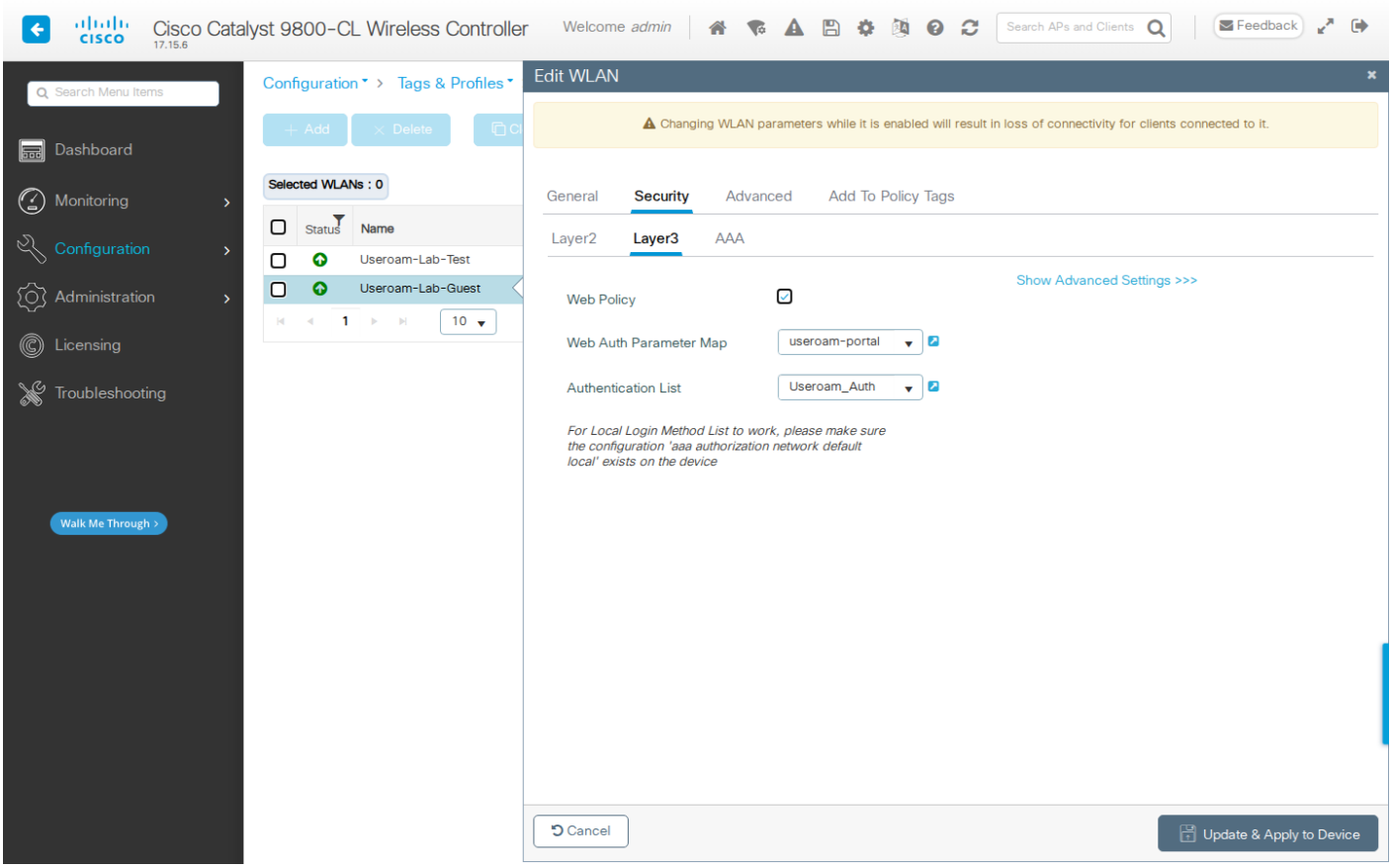
Security > Layer2 sekmesi: güvenlik türü **None** (şifresiz ağ; giriş Useroam sayfasıyla yapılır). **MAC Filtering** işaretsiz.



Security > Layer3 sekmesi:

- **Web Policy:** işaretli.
- **Web Auth Parameter Map:** `useroam-portal`
- **Authentication List:** `Useroam_Auth`
- **Show Advanced Settings >>>** bağlantısına tıklayıp **Preauthentication ACL IPv4** alanında `USEROAM-PREAUTH` seçin.

Apply to Device ile kaydedin.

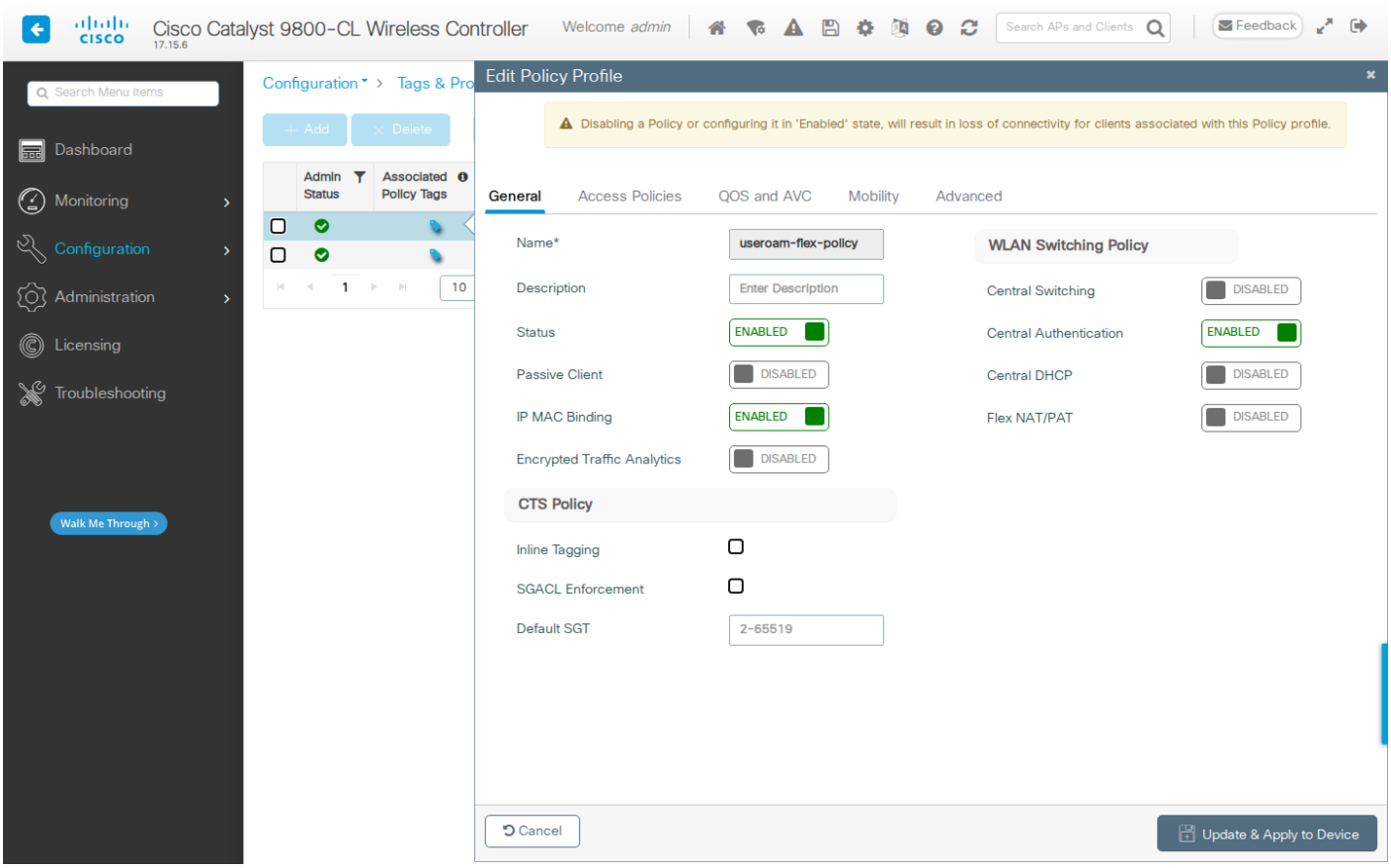


11 - Policy Profili

Configuration > Tags & Profiles > Policy yolunda **+ Add** düğmesine basın (var olan bir profili de kullanabilirsiniz).

General sekmesi:

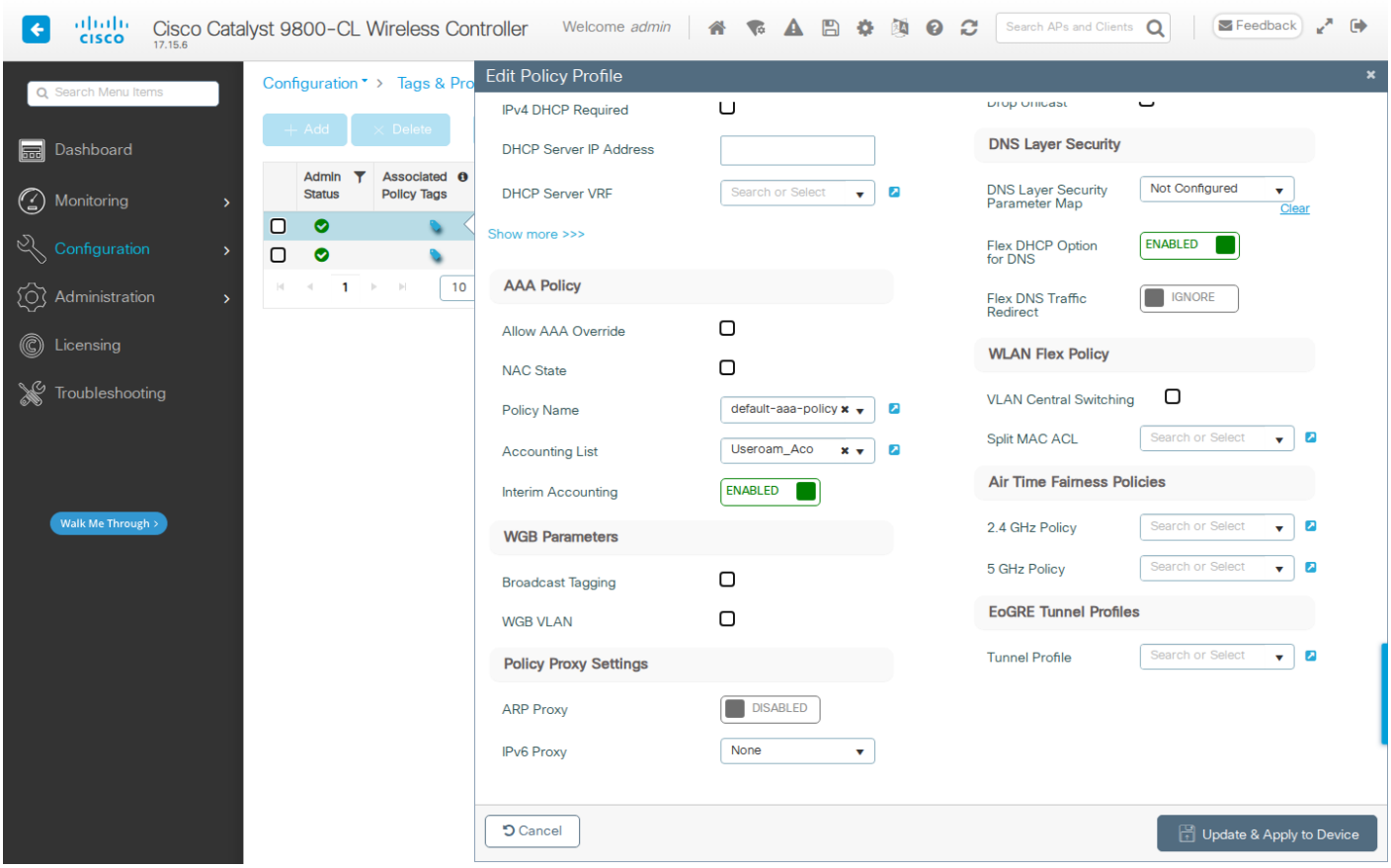
- **Name:** ör. `useroam-policy`, **Status:** ENABLED.
- **WLAN Switching Policy:** AP'leriniz uzak bir lokasyonda **FlexConnect** modundaysa (görseldeki lab gibi) **Central Switching** ve **Central DHCP** kapalı, **Central Authentication** açık olur. AP'ler WLC ile aynı yerde **Local** moddaysa Central Switching açık kalır.
- Misafir VLAN'ı **Access Policies** sekmesinde seçilir.



Advanced sekmesi:

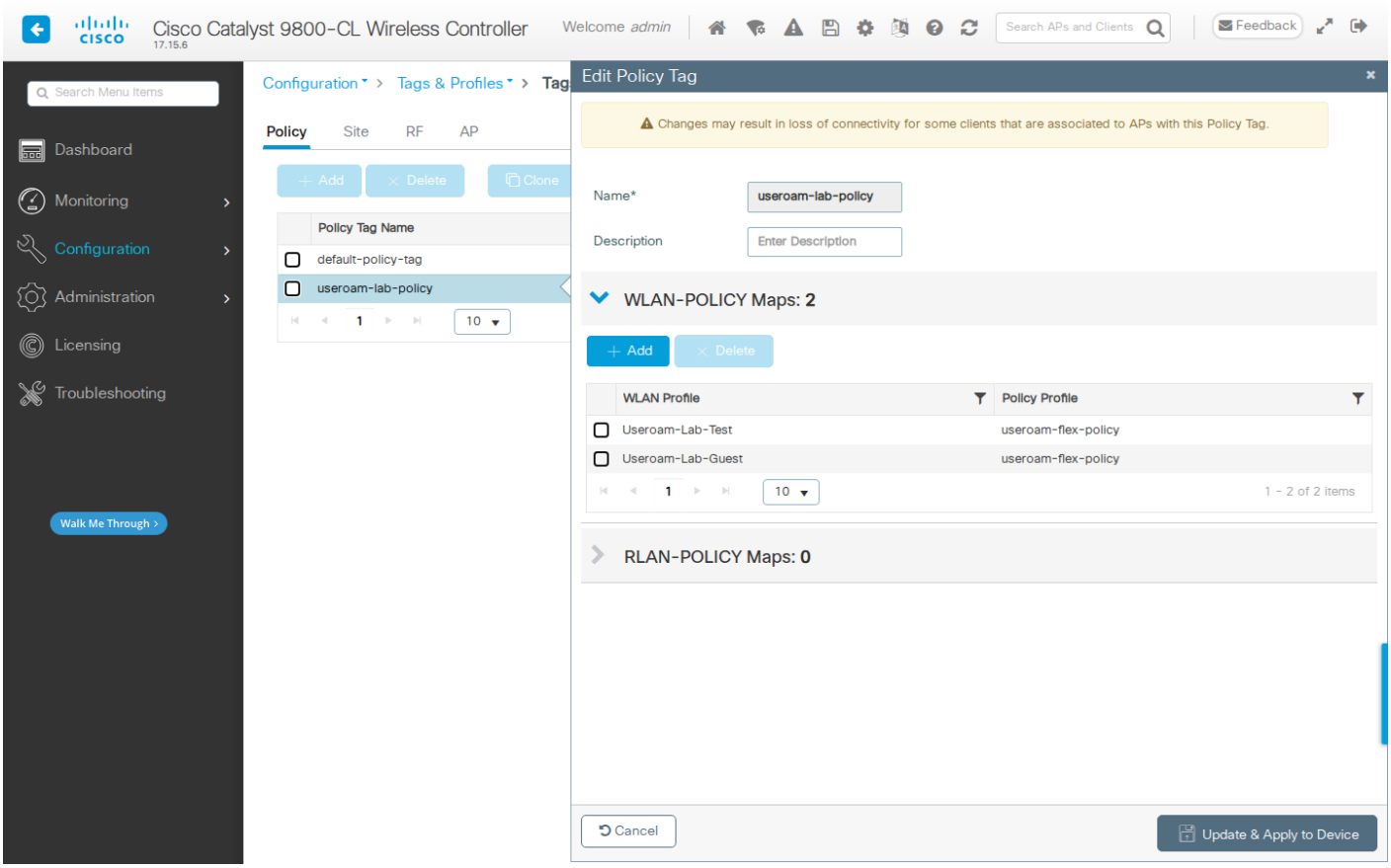
- **Session Timeout (sec):** misafir oturumunun en uzun süresi (ör. `86400` = 24 saat).
- **Idle Timeout (sec):** hareketsiz kalan misafirin düşme süresi (ör. `3600`).
- **AAA Policy > Accounting List:** `Useroam_Aco`
- **Interim Accounting:** ENABLED

Apply to Device ile kaydedin.

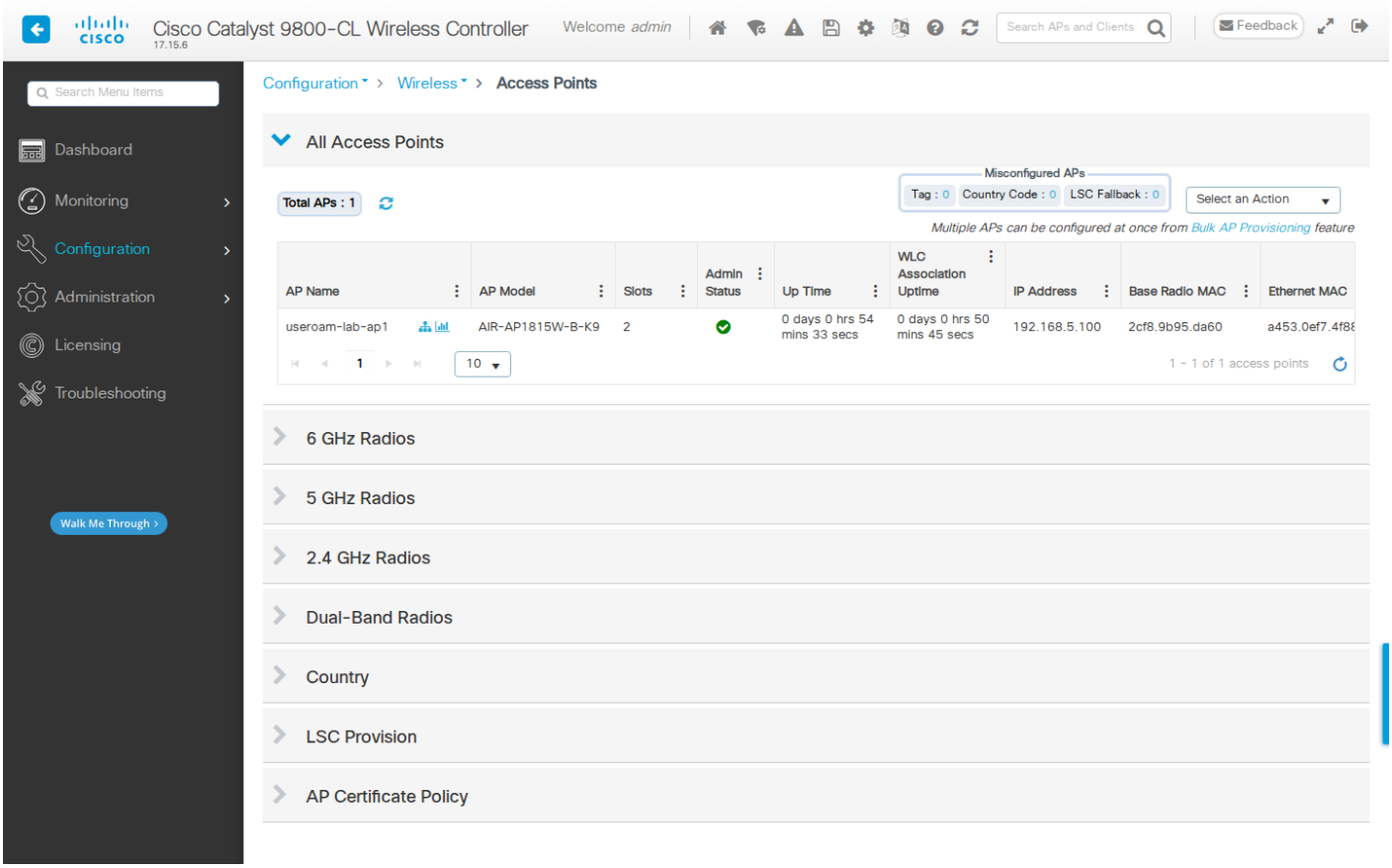


12 - Policy Tag ve AP'lere Atama

Configuration > Tags & Profiles > Tags yolunda **Policy** sekmesinde yeni bir tag ekleyin ya da AP'lerinizin kullandığı tag'i açın. **WLAN-POLICY Maps** bölümünde **+ Add** ile misafir WLAN'ınızı (10. adım) policy profilinizle (11. adım) eşleyin.



Bu tag'in misafir ağını yayınlayacak AP'lere atanmış olması gerekir: **Configuration > Wireless > Access Points** listesinde AP'ye tıklayıp **General > Tags > Policy** alanında tag'i seçin. Listedeki **Policy Tag** sütununda her AP'nin doğru tag'i aldığını kontrol edin.



> **Ayarları kalıcı yapın:** tüm adımlar bitince üst menüdeki **kaydet (disket)** simgesine basın ya da komut satırında `write memory` çalıştırın. Aksi halde WLC yeniden başladığında ayarlar kaybolur.

13 - Test ve Sorun Giderme

1. Telefonla misafir SSID'sine bağlanın. Useroam giriş sayfası kendiliğinden açılmalıdır. Açılmazsa tarayıcıda `http://neverssl.com` adresini açın.
2. SMS, WhatsApp veya portalınızda açık olan başka bir yöntemle giriş yapın.
3. Panelde **Misafirler > Aktif Misafirler** ekranında misafiri görün; WLC'de **Monitoring > Wireless > Clients** ekranında misafirin durumu **Run** olmalıdır.

Belirti	Kontrol edilecek
Giriş sayfası hiç açılmıyor	WLAN Layer3'te Web Policy ve `useroam-portal` seçili mi; ACL'de 104.247.174.120 ve DNS kuralları var mı; `ip http server` açık mı.
"Giriş yapılıyor" ekranında kalıyor	8. adım: Disable HTTP secure server for Web Auth işaretli mi, Virtual IPv4 Address 192.0.2.1 mi.
Tarayıcı "güvenli olmayan form" uyarısı veriyor	Redirect URL for login `http://104.247.174.120/cisco/?u=...` ile başlamalı; https panel adresi kullanılmamalı.
"Kullanıcı adı veya şifre hatalı"	RADIUS Key paneldeki Shared Secret ile aynı mı; paneldeki Cihaz Adresi WLC'nin internete çıktığı genel IP mi (RADIUS istekleri farklı bir IP'den çıkarsa Useroam cihazı tanımaz).
WLC RADIUS sunucusunu "dead" gösteriyor	Önünüzdeki firewall WLC'den 104.247.174.120'e UDP 1812 ve 1813 çıkışına izin veriyor mu. Komut satırından deneme: `test aaa group Useroam deneme 1234 legacy` (cevap "reject" gelirse bağlantı çalışıyordur).
Aktif kullanıcılar panelde görünmüyor	Policy profilinde Accounting List `Useroam_Aco` ve Interim Accounting açık mı; 6. adımdaki komutlar girildi mi.

Revizyon #2
tugay tarafından 5 Kasım 2026 11:01:50 oluşturuldu
tugay tarafından 5 Kasım 2026 11:02:06 güncellendi