

CISCO CATALYST 9800-CL WLC KURULUM & KONFIGÜRASYON DOKÜMANI

Kübra Yüksel

3) 9800-CL Software İçin Gerekli Ova Dosya Formatı

Cisco 9800-CL için gerekli OVA dosyasına aşağıdaki linkten ulaşabilirsiniz.

<https://software.cisco.com/download/home/286322605/type/282046477/release/Bengaluru-17.6.4>

Catalyst 9800-CL için OVA template (OVA) : *C9800-CL-universalk9.BLD_V***.ova*

Downloads Home / Wireless / Wireless LAN Controller / Standalone Controllers / Catalyst 9800 Wireless Controllers for Cloud / Catalyst 9800-CL Wireless Controller for Cloud / IOS XE Software - Bengaluru-17.6.4(MD)

Search...

Expand All Collapse All

Suggested Release

Bengaluru-17.6.4(MD)

Amsterdam-17.3.6(MD)

Latest Release

Dublin-17.11.1(ED)

Amsterdam-17.3.7(MD)

Cupertino-17.9.3(ED)

Bengaluru-17.6.5(MD)

All Release

17

16

Deferred Release

Catalyst 9800-CL Wireless Controller for Cloud

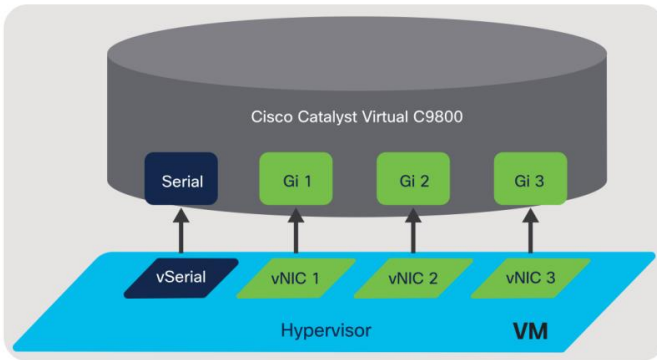
Release Bengaluru-17.6.4 MD [Related Links and Documentation](#)
[Release Notes for 9800-CL](#)

Cisco is aware of an issue affecting image validation at software upgrades or downgrades in the Cisco IW3702 Wave 1/IOS Access Points. We recommend following the workarounds mentioned in the bug CSCwd80290.

File Information	Release Date	Size	
Cisco Catalyst 9800 Wireless Controller for Cloud, C9800-CL-universalk9.17.06.04.SPA.bin Advisories	18-Aug-2022	1021.67 MB	
Cisco Catalyst 9800 Wireless Controller for Cloud - Hyper-V / ESXI / KVM C9800-CL-universalk9.17.06.04.iso Advisories	18-Aug-2022	1031.62 MB	
Cisco Catalyst 9800 Wireless Controller for Cloud - Hyper-V / ESXI / KVM C9800-CL-universalk9.17.06.04.ova Advisories	18-Aug-2022	1032.97 MB	

4) ESXI Üzerinde Cisco 9800-CL Kurulumu

4.1) Interface Arabirimleri



Catalyst 9800-CL, Gigabit Ethernet interfacelerini VM tarafından atanan logical vNIC adıyla eşleştirir. VM, logical vNIC adını fiziksel bir MAC adresine eşler. Catalyst 9800-CL ilk kez kurulurken, router interfaceleri VM oluşturulduğunda eklenen logical vNIC arabirimleriyle eşlenir.

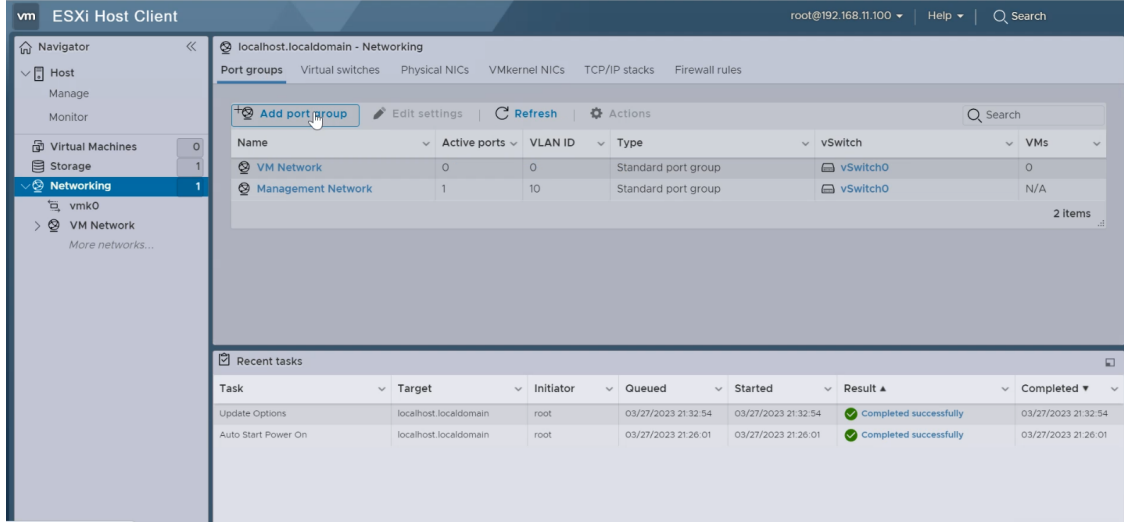
Üç adet interface vardır. Kurulum gerçekleştirirken aşağıdaki düzende seçmeliyiz.

- GigabitEthernet1: Device management interface
- GigabitEthernet2: Wireless management interface
- GigabitEthernet3: High Availability interface
- Eğer 9800-CL'de client'lar için farklı vlanlara izin vermek amacıyla farklı data paketlerini geçirecekseniz interfacelerin her biri kendi vSwitch'inde olmalıdır. Catalyst 9800 temelde kablosuz özelliklere sahip bir switchdir. Aynı vSwitch üzerinde bu interfacelerin birden fazlasının bulunması, port channel olmadan multiple link kullanarak iki switch'i birbirine bağlamak gibidir. Loop oluşmaması için iki interfacesi tek bir networke bağlamamalıyız.

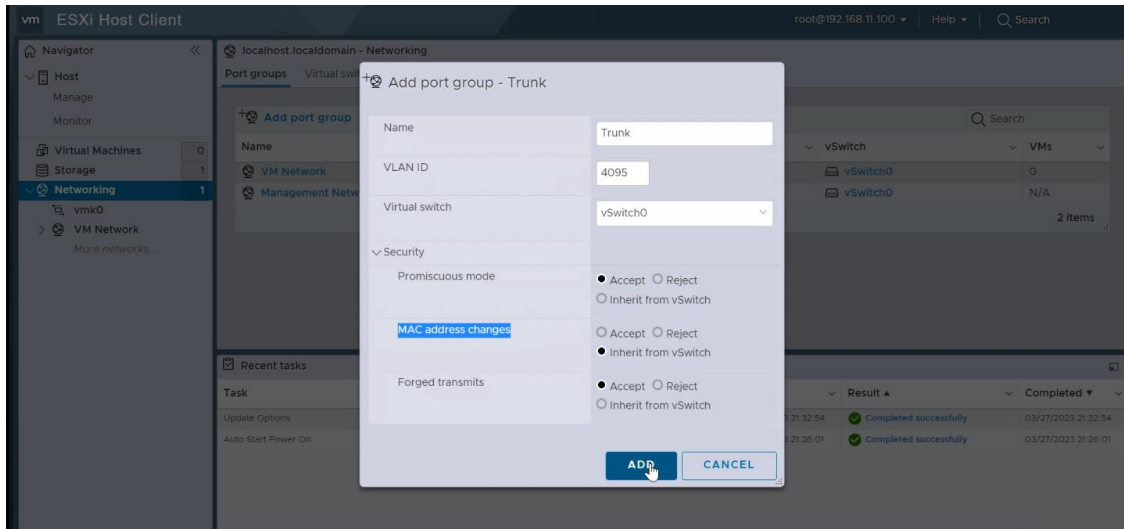
- Interfaceleri silecekseniz, bunu VM’i kurulum sonrası ilk kez çalıştırmadan önce yapmalısınız. Örneğin GigabitEthernet 2’yi silecekseniz kurulum esnasında gerçekleştirin ve VM’i öyle çalıştırın.

4.2) ESXi Üzerinde Interface Ayarları

İlk adımda portlarımızı oluşturmalıyız. Management için ve Trunk için portlar create etmeliyiz. Portları oluştururken farklı vSwitch seçimi yapmalıyız. Çünkü birden fazla interface kullanacağız. Eğer tek bir interface kullanacak olsaydık tek bir vSwitch kullanmak yeterli olurdu.

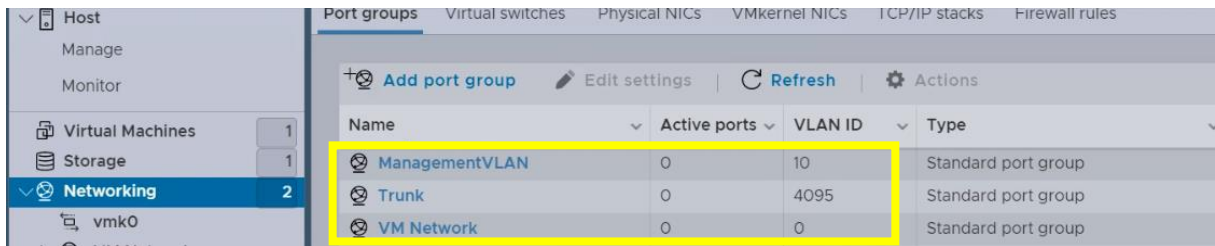


- Vlan ID: 4095 ile bütün vlanlara izin verdiğini belirttik.

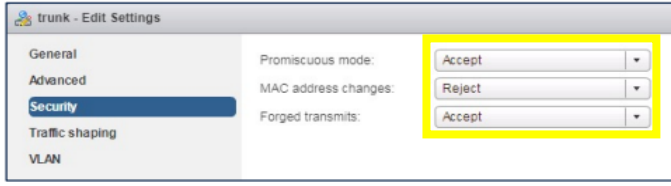


- Security de accep alanlarının ikisinde WLC'nin 802.1Q etiketlerini geçebilmesi için gereklidir

Oluşturduğumuz portları aşağıdaki gibi görebiliriz.

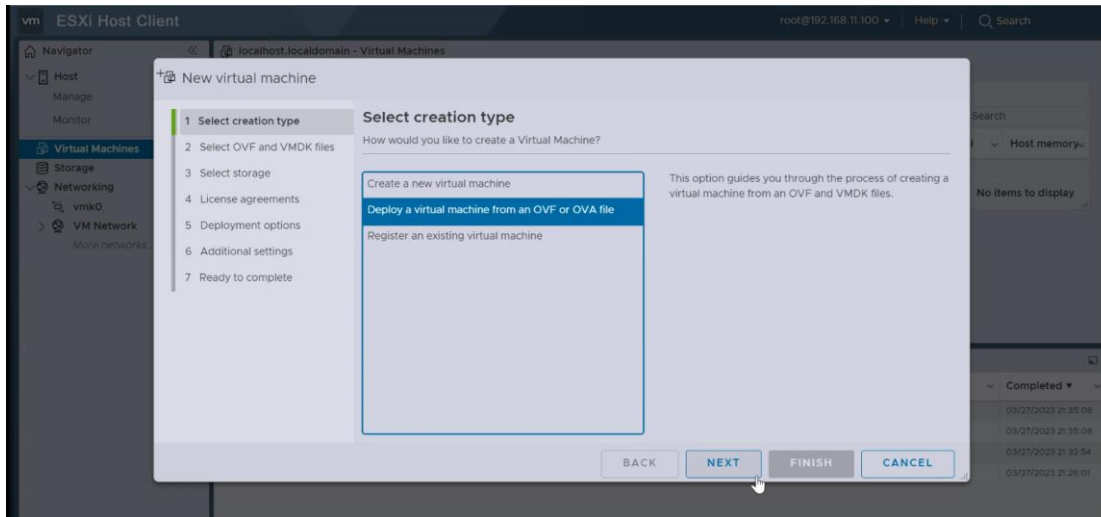
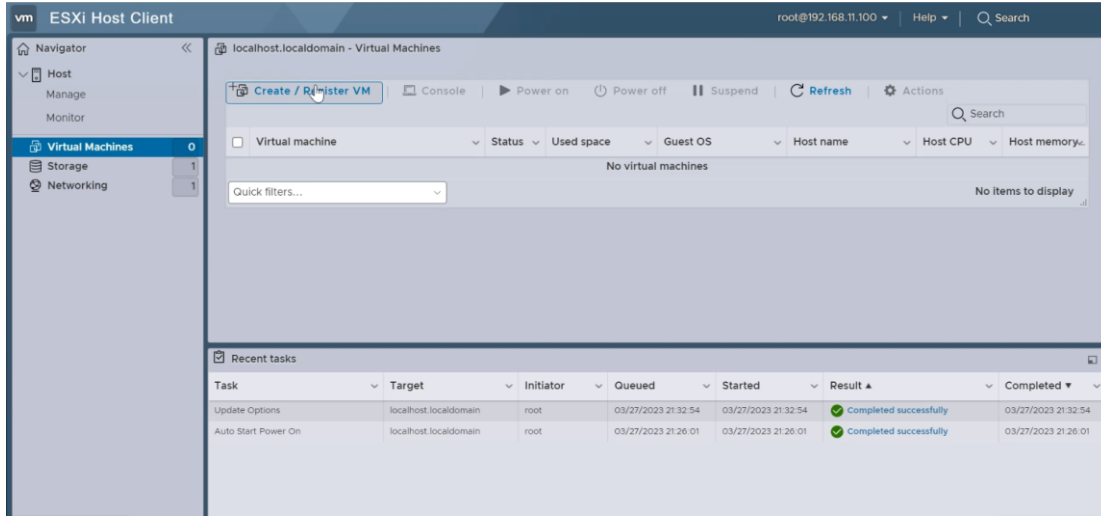


Trunk olsun ya da olmasın, portlar için ESX üzerinde aşağıdaki security ayarının muhakkak yapılması gerekmektedir.

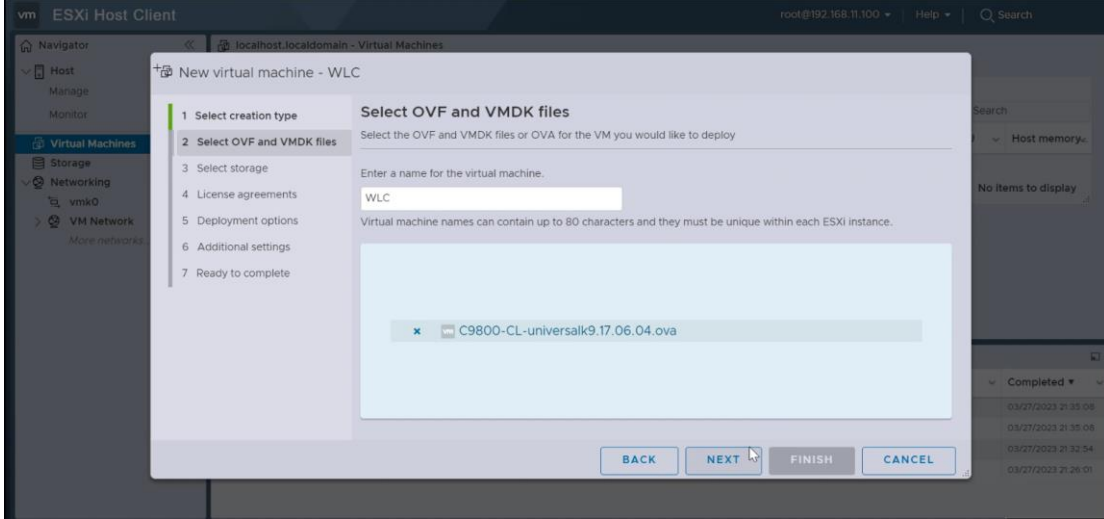


4.3) ESXI Üzerinde OVA Kurulumu

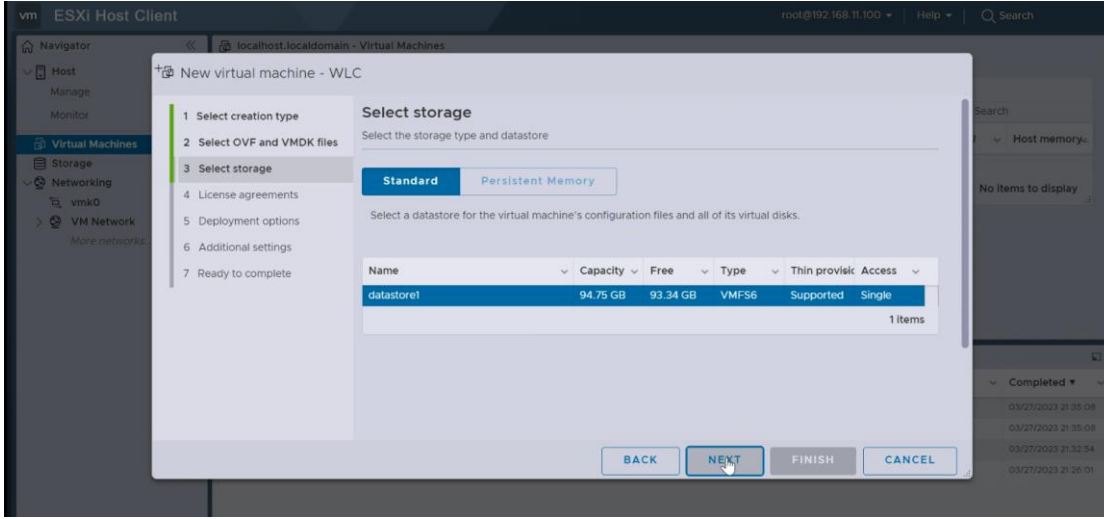
- Interfacelerimiz hazır. Şimdi Ova dosyasını deploy etmeye geçebiliriz. 'Create / Register VM' butonu ile kurulumu başlatıyoruz.



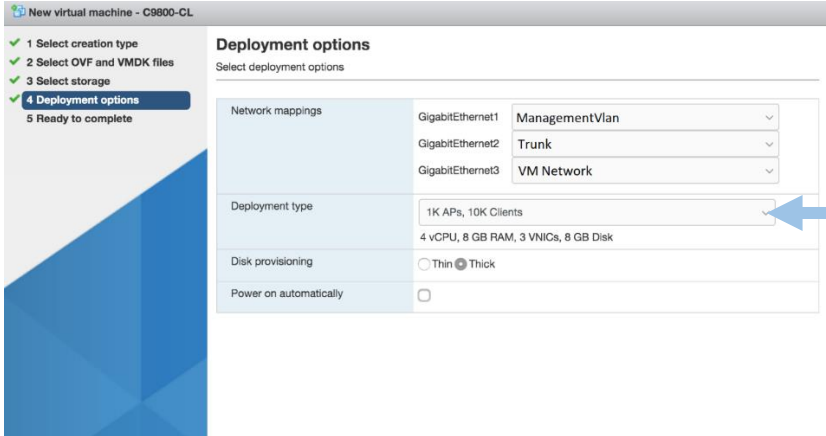
- Sanal Makineye isim verip, OVA dosyasını seçiyoruz.



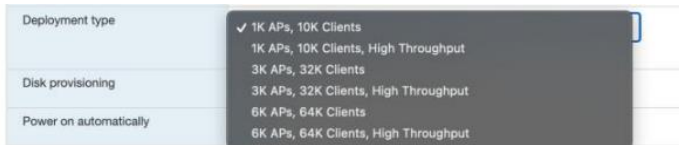
- Sanal makinenin bulunacağı Datastor'u seçiyoruz.



- Deployment opsiyonlarını (Network Mappings, Scale, Disk Provisioning, vb.) seçiyoruz.
- 'Power on automatically' seçeneğinin seçilmediğinden emin olalım.



AP ve Client
ölçeğini
seçelim



- Ayarları kontrol edip 'Finish' butonuna tıklayabiliriz.

Task	Target	Initiator	Queued	Started	Result	Completed
Upload disk - C9800-CL-universalk9_vga.17.05.01.iso (1...	C9800-CL-Deployment-Guide-ESXI	root	06/29/2021 11:00:31	06/29/2021 11:00:31		Running... 3 %
Upload disk - vmlc_harddisk.vmdk (2 of 2)	C9800-CL-Deployment-Guide-ESXI	root	06/29/2021 11:00:31	06/29/2021 11:00:31	Completed successfully	06/29/2021 11:00:32
Import VApp	Resources	root	06/29/2021 01:52:36	06/29/2021 01:52:36		Running... 2 %

New virtual machine - C9800-CL-Deployment-Guide-ESXI

Ready to complete

Review your settings selection before finishing the wizard

Product	Cisco C9800-CL Wireless Lan Controller
VM Name	C9800-CL-Deployment-Guide-ESXI
Files	vmlc_harddisk.vmdk C9800-CL-universalk9_vga.17.05.01.iso
Datastore	datastore1
Provisioning type	Thin
Network mappings	GigabitEthernet1: Lab Network,GigabitEthernet2: Trunk_9300,GigabitEthernet3: R edundancy
Guest OS Name	Cisco IOS-XE Software
Profile	4 vCPU, 8 GB RAM, 3 VNICS, 16 GB Disk

Do not refresh your browser while this VM is being deployed.

Back Next Finish Cancel

- Ayarlamaları tamamladıktan sonra 'power on' butonu ile çalıştırabiliriz.

Host Management Console

Virtual Machines

Virtual machine	Status	Used space	Guest OS	Host name	Host CPU	Host memory...
WLC	Nor...	Unknown	Other 3.x or later Lin...	Unknown	0 MHz	0 MB

Quick filters...

WLC

Guest OS: Other 3.x or later Linux (64-bit)

Compatibility: Yes

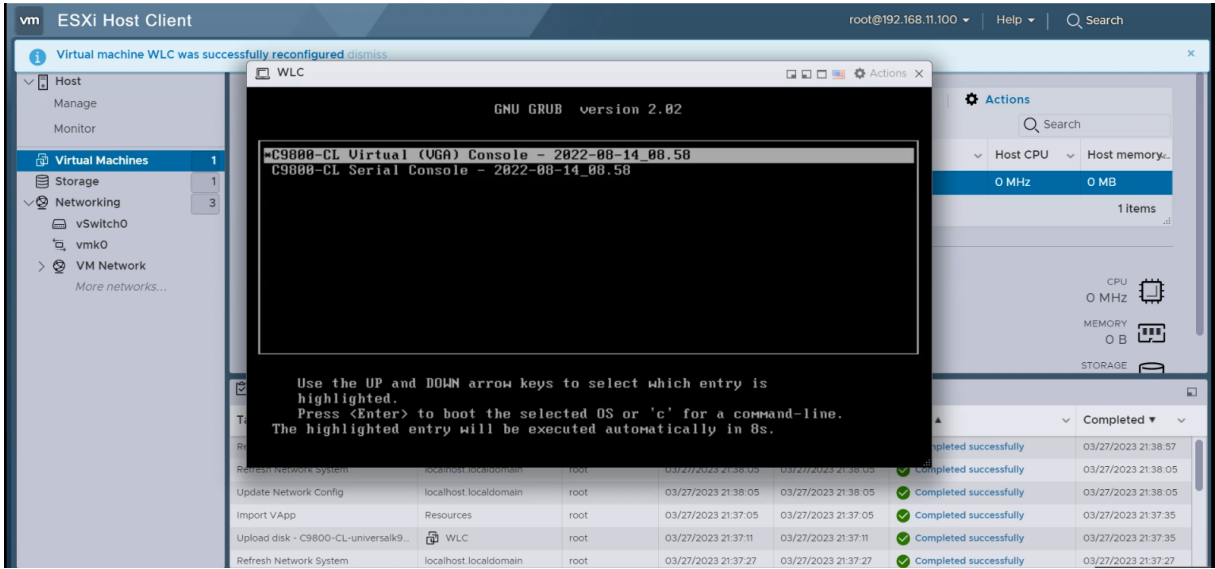
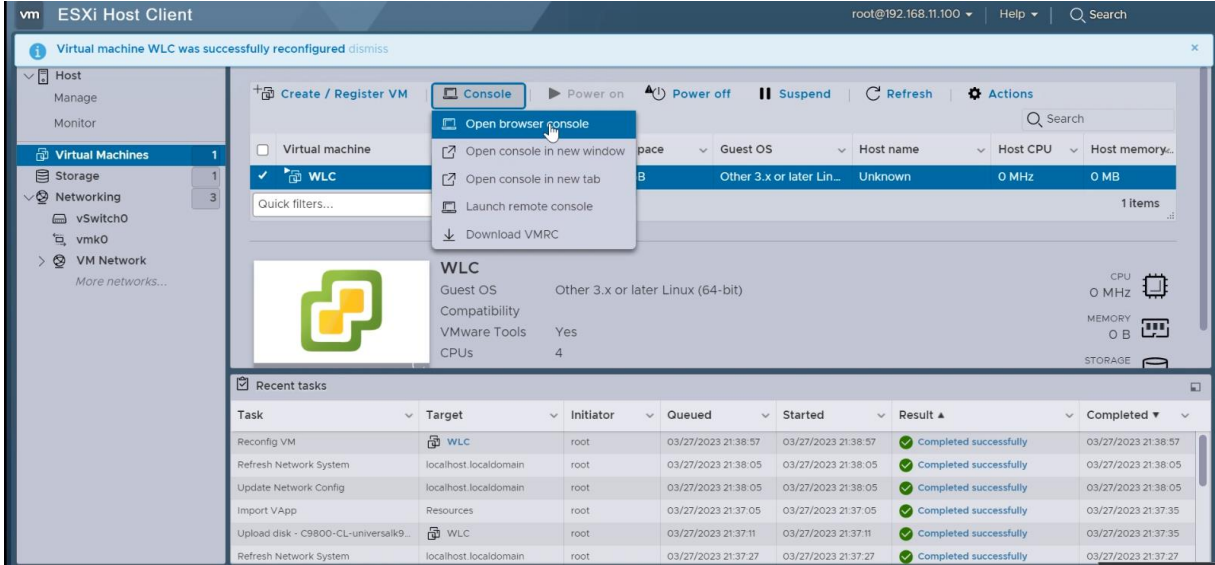
VMware Tools: Yes

CPUs: 4

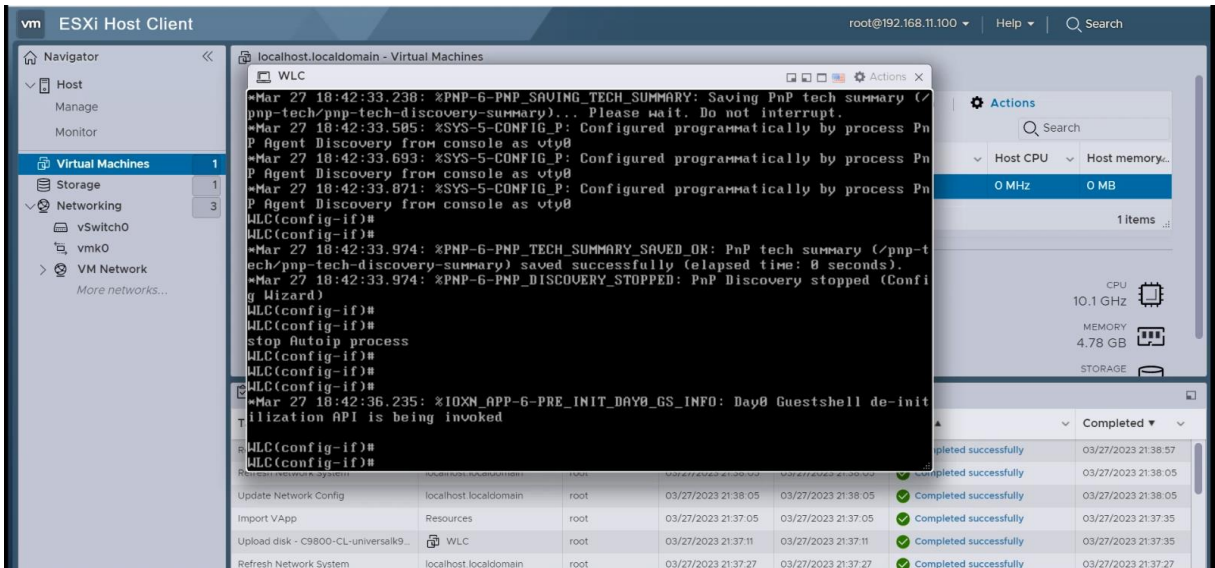
CPU: 0 MHz

MEMORY: 0 B

STORAGE: 0 B



Burada CLI ekranı üzerinden interface'e ip verme, vlan create etme gibi işlemler gerçekleştirebiliriz.



Görüldüğü gibi, Cisco 9800 WLC üzerinde 17.06.04 software'ı çalışmaktadır.

Ova dosyası kurduğunuz sistemde VCenter varsa aşağıda yer alan bilgiler kurulum esnasında gelecektir. Biz sadece ESXI 7.0 versiyonunu kurduk ve bu bilgileri istemediği için bir sonraki adımda CLI ekranı üzerinden management interface'imize ip adresi vererek kurulumu tamamlayıp web arayüzüne ulaşacağız.

Deploy OVF Template

1. Basic Management Setup 2 settings

1.1 Hostname Hostname of this wireless lan controller
C9800-CL

1.2 Enable Password Password for privileged (enable) access. WARNING: While this password will be stored securely within IOS, the plain-text password will be recoverable from the OVF descriptor file.
Password: *****
Confirm Password: *****

2. Device Management/Service Interface Configuration 4 settings

2.1 Device Management/Service Interface Management interface (such as "GigabitEthernet1")
GigabitEthernet1

2.2 Device Management/Service Interface IPv4 Address/Netmask IPv4 address and mask for management interface (such as "192.0.2.100/24" or "192.0.2.100 255.255.255.0"), or "dhcp" to configure via DHCP
10.0.0.24

2.3 Device Management/Service Interface IPv4 Gateway IPv4 gateway address (such as "192.0.2.1") for management interface, or "dhcp" to configure via DHCP
10.0.0.1

2.4 Remote Device Management/Service Network Route/Netmask This will add a route to the remote network where you want to manage your device from (Hint: To add the default route enter 0.0.0.0)
0.0.0.0

3. User login Configuration 2 settings

3.1 Login Username Username for remote login
admin

3.2 Login Password Password for remote login. WARNING: While this password will be stored securely within IOS, the plain-text password will be recoverable from the OVF descriptor file.
Password: *****
Confirm Password: *****

Vcenter ile kurulum için detaylara 8 No'lu bölümdeki kaynaklardan detaylara ulaşabilirsiniz.

5) Web Arayüzüne Erişim

WLC için kullanacağımız Management IP: 192.168.11.3 'tür. Initial config işlemlerini tamamladıktan sonra ' <https://192.168.11.3> ' adresi ile web üzerinden erişim sağlayabiliriz.

- CLI aracılığıyla 9800-CL Konfigürasyonu : Initial Konfigürasyon

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

```
Would you like to terminate autoinstall? [yes]: yes
```

```
WLC(config)#user admin privilege 15 password A123456!
```

- Açılan CLI ekranı üzerinden Management interface olan GigabitEthernet 1'e ip adresi veriyoruz.

```
WLC(config)# interface GigabitEthernet 1
```

```
WLC(config-if)#no switchport
```

```
WLC(config-if)#ip address 192.168.11.3 255.255.255.0
```

- Web arayüzüne erişmek için default route yazalım.

```
WLC(config)# ip route 0.0.0.0 0.0.0.0 192.168.11.1
```

Wireless yönetimi için management interface'i belirtmeniz, sertifika oluşturmanız ve sertifika kurulumunu doğrulamanız gerekir. Sertifika noktası yapılandırmasını atlarsanız AP'ler register olamaz. Ancak, GUI'ye gidebilir ve istenen sertifikayı alarak yapılandırabilirsiniz.

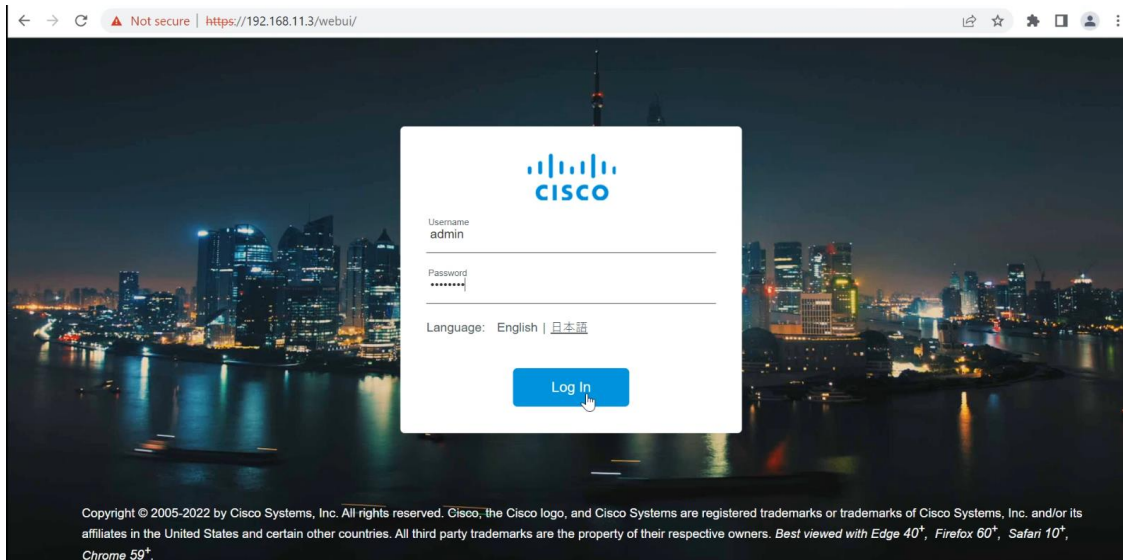
```
WLC(config)# wireless management interface GigabitEthernet 1
```

```
WLC(config)# exit
```

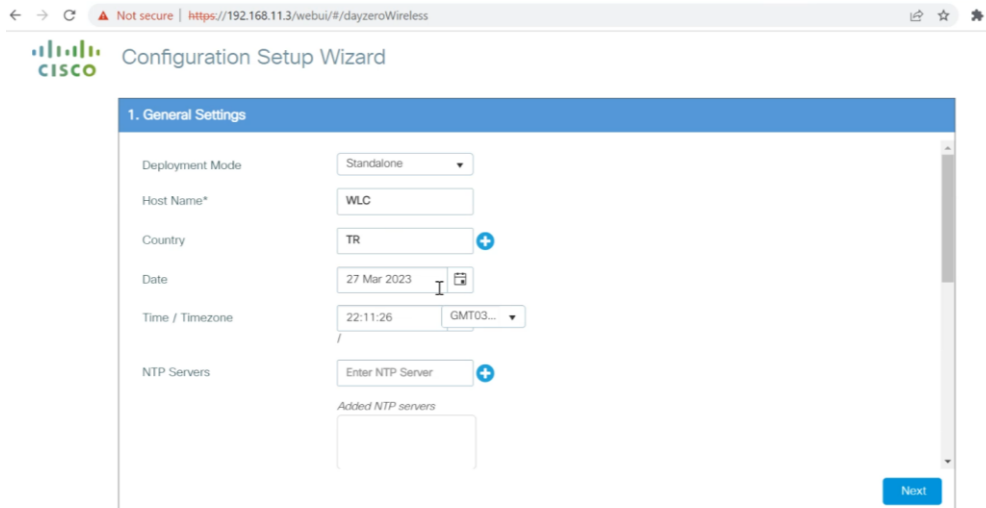
```
WLC# wireless config vwlc-ssc key-size 2048 signature-algo sha256 password 0 A123456!
```

```
WLC# show wireless management trustpoint
```

- Konfigürasyondan sonra <https://192.168.11.3> adresine giderek arayüzün gelip gelmediğini kontrol edelim.

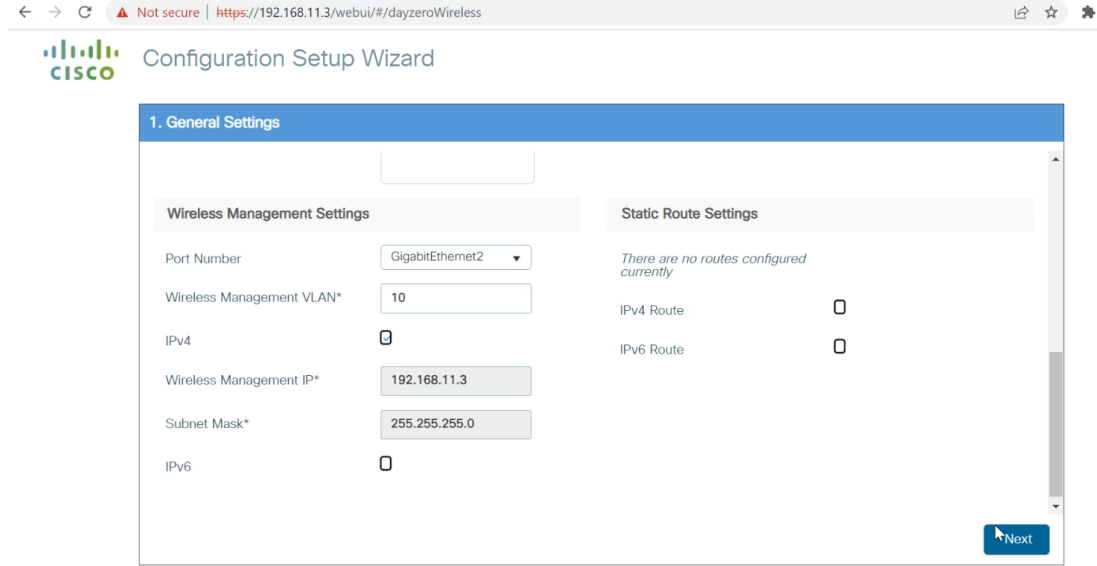


- CLI ekranı üzerinden oluşturduğumuz username ve password ile girişimizi gerçekleştirdikten sonra temel ayarlamaları yapıp, WLC'nin tamamen çalışır durumda olmasını sağlamak için Configuration Setup Wizard'ı tamamlamak gerekir.



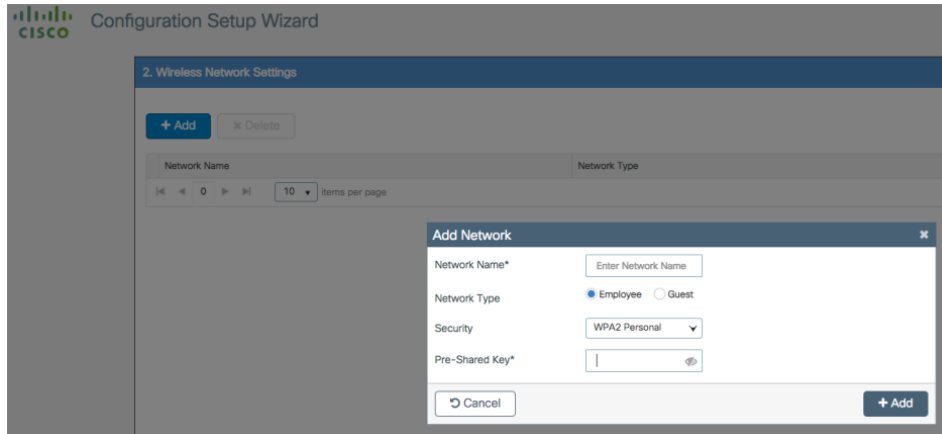
Burada Wireless Management Settings sekmesinde port number belirtirken GUI'ye erişmek için kullandığımız interface'den farklı bir interface seçmeliyiz. Bu durumda Gig1'i kullandığımız için burada Gig2 ya da Gig3'ü seçebiliriz. VLAN'ı, IP adresini ve subnet mask'ı seçerek interface'i yapılandırın. Böylelikle, şunlar otomatik olarak yapılandırılmış olur;

- Trunk Interface
- Wireless Management için SVI interface
- Subnet Mask



The screenshot shows the Cisco Configuration Setup Wizard, Step 1: General Settings. The page is divided into two main sections: Wireless Management Settings and Static Route Settings. The Wireless Management Settings section includes fields for Port Number (GigabitEthernet2), Wireless Management VLAN* (10), IPv4 (checkbox), Wireless Management IP* (192.168.11.3), Subnet Mask* (255.255.255.0), and IPv6 (checkbox). The Static Route Settings section shows a message: "There are no routes configured currently" and fields for IPv4 Route and IPv6 Route, both with checkboxes.

Next dedikten sonra client'ların bağlanabilmesi için WLAN ekleyebilirsiniz. Bu tamamen optional'dır. İsterseniz next diyip geçebilir daha sonra ekleme yapabilirsiniz.



The screenshot shows the Cisco Configuration Setup Wizard, Step 2: Wireless Network Settings. The page features a table for Wireless Network Settings with columns for Network Name and Network Type. Below the table is an 'Add Network' dialog box with fields for Network Name* (Enter Network Name), Network Type (Employee/Guest), Security (WPA2 Personal), and Pre-Shared Key*.

- Sonraki sayfada RF parametre ve AP sertifika ayarlarını yapılandırabiliriz. Virtual IP adresini yazabiliriz.

← → ↻ Not secure | https://192.168.11.3/webui/#/dayzeroWireless

cisco Configuration Setup Wizard

3. Advanced Settings

Client Density

RF Group Name*

Traffic Type

Virtual IP Address

AP Certificate

Generate Certificate YES

RSA Key-Size

Signature Algorithm

- Trustpoint, dolaylı olarak güvenilen bir sertifika yetkilisidir. Bir trustpoint sertifikası kendinden imzalı bir sertifikadır, dolayısıyla başka birinin veya başka bir tarafın güvenine dayanmadığı için "trustpoint" adı verilir. Bir AP'nin 9800-CL'ye katılması için trustpoint gerekir. İlk kurulum sırasında otomatik olarak oluşturulabilir. Aksi takdirde burada Generate Certificate 'No' olarak seçilirse bu kurulum tamamlandıktan sonra AP'lerin katılması için bir sertifika yetkilisinin yapılandırılması gerekir.

← → ↻ Not secure | https://192.168.11.3/webui/#/dayzeroWireless

cisco Configuration Setup Wizard

3. Advanced Settings

Generate Certificate YES

RSA Key-Size

Signature Algorithm

Password*

Create New AP Management User (optional)

New AP Management User

Password

Secret

- Summary dedikten sonra yapılan config görünmektedir.

← → ↻ Not secure | https://192.168.11.3/webui/#/dayzeroWireless

cisco Configuration Setup Wizard

4. Summary

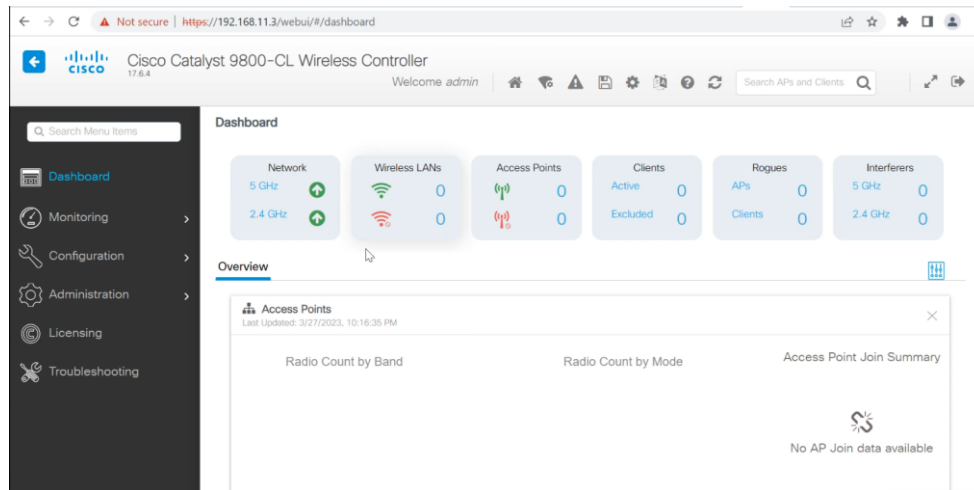
General Settings

Deployment Mode	standalone
Host Name	WLC
Country	TR
Date	27 Mar 2023
Time / Timezone	22:11:26 / GMT0300

Wireless Management Settings

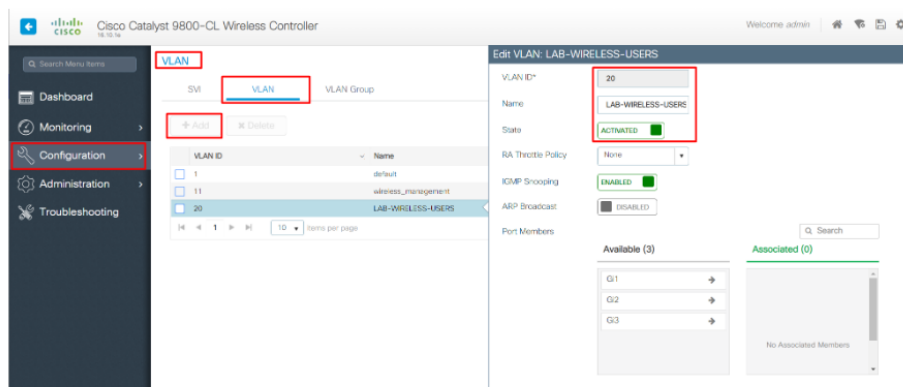
Port Number	GigabitEthernet2
Wireless Management VLAN	10
Wireless Management IP	192.168.11.3
Subnet Mask	255.255.255.0

- Finish dedikten sonra web arayüzümüze erişim sağlayabiliriz



6) Basic Wireless Konfigürasyonu ve Flex Mode

- SSID yayını yapmak için yapacağımız ilk adım Vlan create etmek olacaktır.

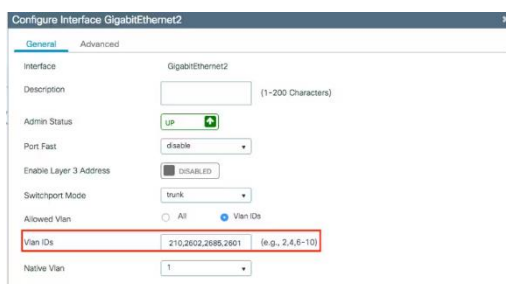


Add VLAN for wireless users

Vlan create ettikten sonra data interfacelerinin oluşturduğumuz Vlanlara izin verdiğini doğrulamalıyız.

Eğer port channel kullanıyorsak;

- Configuration> Interface> Logical> PortChannel name> General ayarına gidelim.
- Allowed Vlan = All yapılandırmasının olduğunu doğrulayalım.
- Eğer Allowed Vlan = Vlan ID ise izin verilmesi istenilen Vlan ID'leri kutucuğa ekleyelim.

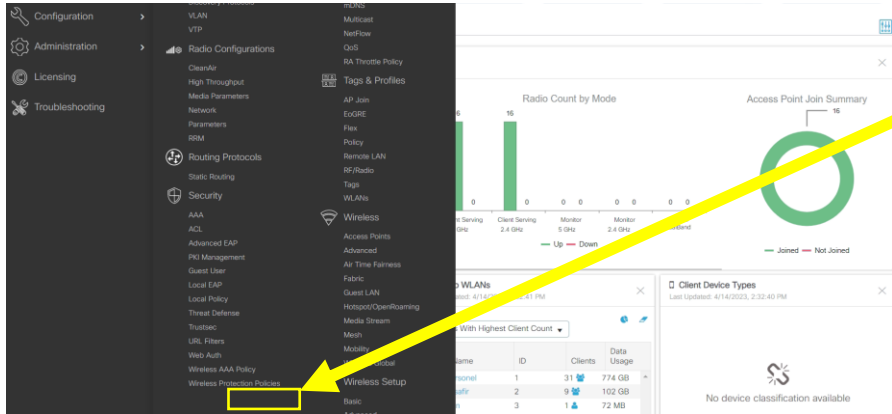


Port cahnnel kullanıyorsak;

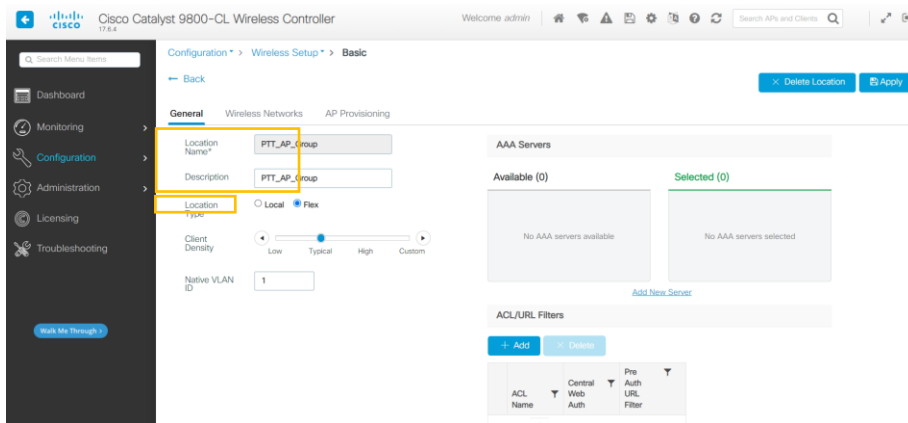
- Configuration> Interface> Ethernet> Interface Name> General ayarına gidelim.
- Allowed Vlan = All yapılandırmasının olduğunu doğrulayalım.
- Eğer Allowed Vlan = Vlan ID ise izin verilmesi istenilen Vlan ID'leri kutucuğa ekleyelim.

- Burada L3 Firewall üzerinde sonlanıyorsa Vlan create ettikten sonra SVI oluşturmaya gerek yoktur. Sadece Vlan create etmek yeterlidir. Kullanıcı VLAN'ları için herhangi bir SVI varsa, bunları silin, mdns veya dhcp relay ihtiyacınız olmadıkça, kullanıcı vlan'ları için herhangi bir SVI'ya ihtiyacınız yoktur.
- Vlan create ettikten sonra SSID yayını için aşağıda yer alan Tag&Profiles konfigürasyonunu gerçekleştirmek gerekir.

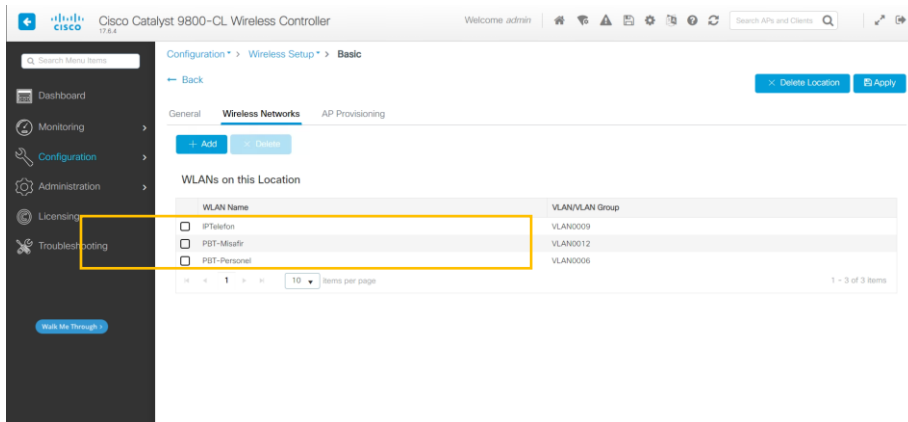
İlk olarak basic konfigürasyonumuzu gerçekleştirelim.



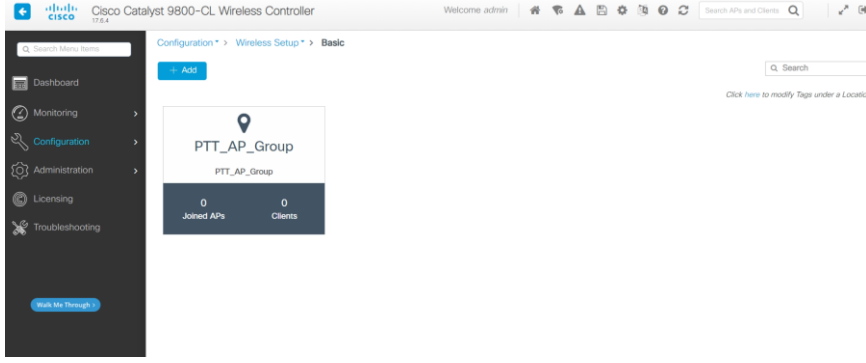
Step1:



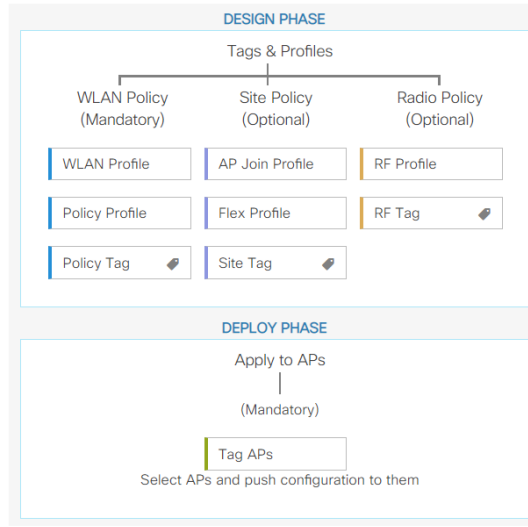
Step2:



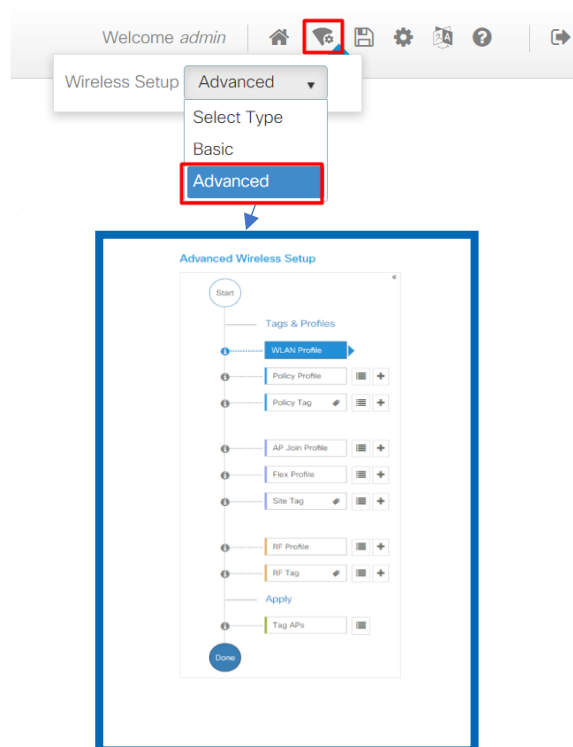
Gördüğümüz gibi apply ettiğimiz zaman wireless basic configuration tamamlamış olduk.



7) SSID Yayını Yapma İşlemi



- İlk olarak aşağıda yer alan sekmeden 'Advance' kısmı seçilmelidir. Seçimden sonra aşağıdaki 'Advanced Wireless Setup' menüsü açılır.



Yukarıdaki menüde yer alan bütün sekmelere sırasıyla konfigürasyon yapacağız. Aşağıdaki adımları takip edelim.

Step 1

The screenshot shows the 'Edit WLAN' configuration page with the 'General' tab selected. The following fields are visible:

Field	Value
Profile Name*	9800-PSK-Central
SSID	9800-PSK-Central
WLAN ID*	1
Status	ENABLED
Radio Policy	All
Broadcast SSID	ENABLED

WLAN Profile General tab

The screenshot shows the 'Edit WLAN' configuration page with the 'Security' tab selected. The following fields are visible:

Field	Value
Layer 2 Security Mode	WPA + WPA2
MAC Filtering	<input type="checkbox"/>
Protected Management Frame	<input type="checkbox"/>
PMF	Disabled
WPA Parameters	
WPA Policy	<input type="checkbox"/>
WPA2 Policy	<input checked="" type="checkbox"/>
WPA2 Encryption	AES(CCMP128) <input checked="" type="checkbox"/> CCMP256 <input type="checkbox"/> GCMP128 <input type="checkbox"/> GCMP256 <input type="checkbox"/>
Auth Key Mgmt	PSK
PSK Format	ASCII
Pre-Shared Key
Fast Transition	Disabled
Over the DS	<input checked="" type="checkbox"/>
Reassociation Timeout	20

WLAN Profile Security tab

Step 2

The screenshot shows the 'Edit Policy Profile' configuration page with the 'General' tab selected. A warning message is displayed at the top: "Configuring in enabled state will result in loss of connectivity for clients associated with this profile." The following fields are visible:

Field	Value
Name*	LAB-Policy-Profile-Cen
Description	Enter Description
Status	ENABLED
Passive Client	DISABLED
Encrypted Traffic Analytics	DISABLED
CTS Policy	
Inline Tagging	<input type="checkbox"/>
SGACL Enforcement	<input type="checkbox"/>
Default SGT	2-65519
WLAN Switching Policy	
Central Switching	<input type="checkbox"/>
Central Authentication	<input checked="" type="checkbox"/>
Central DHCP	<input type="checkbox"/>
Central Association	<input checked="" type="checkbox"/>
Flex NAT/PAT	<input type="checkbox"/>

Policy Profile - General Tab

Edit Policy Profile

General **Access Policies** QoS and AVC Mobility Advanced

WLAN Local Profiling

HTTP TLV Caching

RADIUS Profiling

DHCP TLV Caching

Local Subscriber Policy Name

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

VLAN

VLAN/VLAN Group

Multicast VLAN

Policy Profile – Access Policies Tab

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override

NAC State

Policy Name

Accounting List

Hotspot Server

User Defined (Private) Network

Status

Drop Unicast

DNS Layer Security

DNS Layer Security Parameter Map [Clear](#)

Flex DHCP Option for DNS **ENABLED**

Flex DNS Traffic Redirect **IGNORE**

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Step 3

Edit Policy Tag

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name*

Description

WLAN Profile	Policy Profile
<input type="checkbox"/> 9800-PSK-Central	LAB-Policy-Profile-Central

10 items per page 1 - 1 of 1 items

Map WLAN and Policy

WLAN Profile*

Policy Profile*

Policy Tag

Step 4

Add AP Join Profile

General Client CAPWAP AP Management Security iCap QoS

Name* OfficeExtend AP Configuration

Description Local Access

Country Code Link Encryption

LED State Rogue Detection

LAG Mode Provisioning SSID

NTP Server Antenna Monitoring

GAS AP Rate Limit Antenna Monitoring

USB Enable RSSI Fail Threshold(dB)*

Apphost Weak RSSI(dBm)*

Fallback to DHCP Detection Time(min)*

Add AP Join Profile

General Client CAPWAP AP Management Security iCap QoS

Device **User** Credentials CDP Interface

User Management

Username

Password Type

Password

Secret Type

Secret
Enter Secret

Wireless Password Policy is Disabled ⓘ

Although disabled, it is recommended to follow the following password rules

Do's:

- Password length range 8 - 120 characters
- At least one uppercase character
- At least one lowercase character
- At least one digit

Don'ts:

- Default passwords (Cisc0) and reverse passwords (0c\$1c) are not allowed
- Alphabets repeated more than twice in sequence (CCC)
- Digits repeated more than twice in sequence (666)
- Sequential digits are not allowed (234)
- Sequential characters are not allowed (lmn)

Step 5

Flex Profile Name	Description
<input type="checkbox"/> default-flex-profile	default flex profile

1 10 items per page 1 - 1 of 1 items

Edit Flex Profile

General Local Authentication Policy ACL VLAN DNS Layer Security

Name* PTT_AP_Group

Description Enter Description

Native VLAN ID 1

HTTP Proxy Port 0

HTTP-Proxy IP Address 0.0.0.0

CTS Policy

Inline Tagging

SGACL Enforcement

CTS Profile Name default-exp-profile

Fallback Radio Shut

Flex Resilient

ARP Caching

Efficient Image Upgrade

OfficeExtend AP

Join Minimum Latency

IP Overlap

mDNS Flex Profile Search or Select

Cancel Update & Apply to Device

Edit Flex Profile

General Local Authentication Policy ACL VLAN DNS Layer Security

+ Add - Delete

VLAN Name	ID	Ingress ACL	Egress ACL
<input type="checkbox"/> VLAN006	6		
<input type="checkbox"/> VLAN009	9		
<input type="checkbox"/> VLAN012	12		

10 Items per page 1 - 3 of 3 items

Cancel Update & Apply to Device

Cisco Catalyst 9800-CL Wireless Controller

Configuration > Tags & Profiles > Flex

+ Add - Delete

Flex Profile Name	Description
<input type="checkbox"/> PTT_AP_Group	
<input type="checkbox"/> default-flex-profile	default flex profile

10 Items per page 1 - 2 of 2 items

Dashboard Monitoring Configuration Administration Licensing Troubleshooting

Step 6

Edit Site Tag

Name* LAB-Site-Tag-Central

Description Enter Description

AP Join Profile AP-Join-Profile-Cen

Control Plane Name

Enable Local Site

Site Tag configuration

Step 7

Add RF Profile

General 802.11 RRM Advanced

Name* TEST_5

Radio Band 5 GHz Band

Status ENABLE

Description Enter Description

NDP Mode AUTO

Cancel Apply to Device

Add RF Profile

General 802.11 RRM Advanced

Name* TEST2

Radio Band 2.4 GHz Band

Status ENABLE

Description Enter Description

NDP Mode AUTO

Cancel Apply to Device

Step 8

Add RF Tag

Name* TEST [Show slot configuration](#)

Description Enter Description

5 GHz Band RF Profile TEST_5

2.4 GHz Band RF Profile TEST2

Cancel Apply to Device

Step 9

[+ Tag APs](#)

Number of APs: 1
Selected Number of APs: 1

<input type="checkbox"/>	AP Name	AP Model	AP MAC	AP Mode	Admin Status
<input checked="" type="checkbox"/>	LAB-AP-3702-FLO	AIR-CAP3702I-E-K9	d8b1.903b.84f0	Local	Enabled

1 10 Items per page

Tag APs

Tags

Policy LAB-Policy-Tag-Cer

Site LAB-Site-Tag-Centr

RF LAB-RF-Tag

Changing AP Tag(s) will cause associated AP(s) to reconnect

Cancel Save & Apply to Device

Apply tags to APs

- Kontrol sağladığımızda bir yayının geldiğini görmeliyiz.

8) FAYDALANILABİLECEK KAYNAKLAR

<https://www.wifireference.com/2019/08/24/cisco-catalyst-9800-cl-deployment-guide/>

<https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/9800/17-4/deployment-guide/c9800-webui-dg.pdf>

<https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-6/release-notes/rn-17-6-9800.html>

<https://wifininjas.net/2019/08/15/wn-blog-10-cisco-c9800-configuration-central-switching/>

<https://mrnciew.com/2023/01/21/9800-flexconnect-basics/>

<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213945-understand-flexconnect-on-9800-wireless.html>

<https://wifininjas.net/2019/08/15/wn-blog-10-cisco-c9800-configuration-central-switching/>

<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213911-understand-catalyst-9800-wireless-contro.html>

<https://www.wwt.com/article/demystifying-the-new-cisco-catalyst-9800>

<https://networkphil.com/2018/12/27/deploying-and-configuring-the-cisco-9800-virtual-wireless-controller-for-the-first-time/>