

# CT5760 Controller and Catalyst 3850 Switch Configuration Example



Document ID: 116342

Contributed by Antoine KMEID and Serge Yasmine, Cisco TAC Engineers.

Aug 13, 2013

## Contents

### Introduction

#### Prerequisites

Requirements

Components Used

#### Background Information for the Unified Access CT5760 Wireless Controller

#### Background Information for the Unified Access Catalyst 3850 Switches

#### 5760 WLC Initial Configuration

Configure

Setup Script

Required Configuration for Access Points to Join

Verify

Troubleshoot

#### 3850 Switch Initial Configuration

Configure

Setup Script

Required Configuration for Access Points to Join

Verify

Troubleshoot

## Introduction

This document describes the steps to install and prepare wireless services on the 5760 Wireless LAN Controller (WLC) and 3850 switch. This document covers initial configuration and the Access Point (AP) join process for both of the platforms.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on these software and hardware versions:

- Unified Access CT5760 Wireless Controller – Version 3.02.02SE
- Unified Access Catalyst 3850 Switch – Version 3.02.02SE

The information in this document was created from the devices in a specific lab environment. All of the

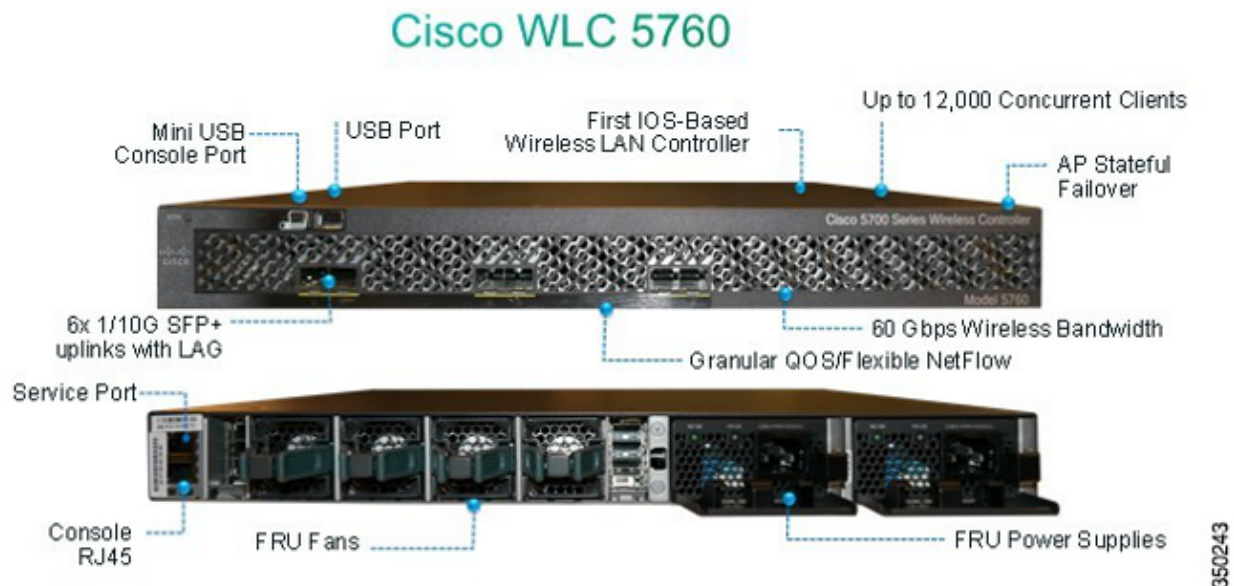
devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Background Information for the Unified Access CT5760 Wireless Controller

The CT5760 WLC is the first Cisco IOS–XE® software–based controller built with smart ASIC intended to be deployed as a centralized controller in the next–generation Unified wireless architecture. The platform also supports the new mobility functionality with Converged Access 3850 Series switches.

CT5760 controllers are typically deployed near the core. The uplink ports connected to the core switch can be configured as EtherChannel trunk ports to ensure port redundancy. This new controller is an extensible and high performance wireless controller, which can scale up to 1000 APs and 12,000 clients. The controller has six 10 Gbps data ports for a total capacity of 60 Gbps.

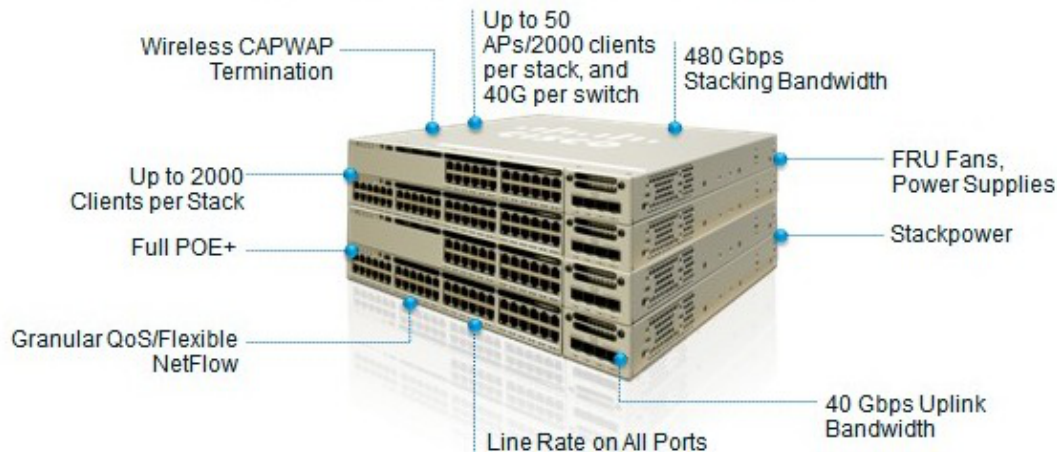
The 5760 Series works in conjunction with Cisco Aironet APs, Cisco Prime Infrastructure, and the Cisco Mobility Services Engine in order to support business–critical wireless data, voice, video, and location services applications.



## Background Information for the Unified Access Catalyst 3850 Switches

The Cisco Catalyst 3850 Series is the next generation of enterprise–class stackable access–layer switches that provide full convergence between wired and wireless on a single platform. Powered by IOS–XE software, wireless service is supported through the Control and Provisioning of Wireless Access Points (CAPWAP) protocol. Cisco's new Unified Access Data Plane (UADP) ASIC powers the switch and enables uniform wired–wireless policy enforcement, application visibility, flexibility, and application optimization. This convergence is built on the resilience of the new and improved Cisco StackWise–480. The Cisco Catalyst 3850 Series switches support full IEEE 802.3at Power over Ethernet Plus (PoE+), modular and field–replaceable network modules, redundant fans, and power supplies.

## NEW Catalyst 3850 Switch



350244

## 5760 WLC Initial Configuration

This section outlines the steps to successfully configure the 5760 WLC in order to host wireless services.

### Configure

#### Setup Script

```
--- System Configuration Dialog ---

Enable secret warning
-----
In order to access the device manager, an enable secret is required
If you enter the initial configuration dialog, you will be prompted for the
enable secret
If you choose not to enter the initial configuration dialog, or if you exit setup
without setting the enable secret,
please set an enable secret using the following CLI in configuration mode-
enable secret 0 <cleartext password>
-----

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

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '['].

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes

Configuring global parameters:

Enter host name [Controller]: w-5760-1

The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.
Enter enable secret: cisco
```

The enable password is used when you do not specify an enable secret password, with some older software versions, and some boot images.

Enter enable password: **cisco**

The virtual terminal password is used to protect access to the router over a network interface.

Enter virtual terminal password: **cisco**

Configure a NTP server now? [yes]:

Enter ntp server address : **192.168.1.200**

Enter a polling interval between 16 and 131072 secs which is power of 2:**16**

Do you want to configure wireless network? [no]: **no**

Setup account for accessing HTTP server? [yes]: **yes**

Username [admin]: **admin**

Password [cisco]: **cisco**

Password is UNENCRYPTED.

Configure SNMP Network Management? [no]: **no**

Current interface summary

Any interface listed with OK? value "NO" does not have a valid configuration

<b>Interface</b>	<b>IP-Address</b>	<b>OK?</b>	<b>Method</b>	<b>Status</b>	<b>Protocol</b>
Vlan1	unassigned	NO	unset	up	up
GigabitEthernet0/0	unassigned	YES	unset	up	up
Tel/0/1	unassigned	YES	unset	up	up
Tel/0/2	unassigned	YES	unset	down	down
Tel/0/3	unassigned	YES	unset	down	down
Tel/0/4	unassigned	YES	unset	down	down
Tel/0/5	unassigned	YES	unset	down	down
Tel/0/6	unassigned	YES	unset	down	down

Enter interface name used to connect to the management network from the above interface summary: **vlan1**

Configuring interface Vlan1:

Configure IP on this interface? [yes]: **yes**

IP address for this interface: **192.168.1.20**

Subnet mask for this interface [255.255.255.0] : **255.255.255.0**

Class C network is 192.168.1.0, 24 subnet bits; mask is /24

Wireless management interface needs to be configured at startup  
It needs to be mapped to an SVI that's not Vlan 1 (default)

Enter VLAN No for wireless management interface: **120**

Enter IP address :**192.168.120.94**

Enter IP address mask: **255.255.255.0**

The following configuration command script was created:

```
w-5760-1
enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY^Q
enable password cisco
line vty 0 15
password cisco
ntp server 192.168.1.200 maxpoll 4 minpoll 4
username admin privilege 15 password cisco
no snmp-server
!
no ip routing
```

```

!
interface Vlan1
no shutdown
ip address 192.168.1.20 255.255.255.0
!
interface GigabitEthernet0/0
shutdown
no ip address
!
interface TenGigabitEthernet1/0/1
!
interface TenGigabitEthernet1/0/2
!
interface TenGigabitEthernet1/0/3
!
interface TenGigabitEthernet1/0/4
!
interface TenGigabitEthernet1/0/5
!
interface TenGigabitEthernet1/0/6
vlan 120
interface vlan 120
ip addr 192.168.120.94 255.255.255.0
exit
wireless management interface Vlan120
!
end

```

[0] Go to the IOS command prompt without saving this config.  
[1] Return back to the setup without saving this config.  
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2

Building configuration...

Compressed configuration from 2729 bytes to 1613 bytes[OK]

Use the enabled mode 'configure' command to modify this configuration.

Press RETURN to get started!

## Required Configuration for Access Points to Join

**Note:** Important – Ensure that the switch has the correct boot command under global configuration. If it has been extracted on the flash, then the *w-5760-1(config)#boot system flash:packages.conf* boot command is required.

### 1. Configure network connectivity.

Configure the TenGig interface connected to the backbone network where CAPWAP traffic flows inbound/outbound. In this example, the interface used is TenGigabitEthernet1/0/1. VLAN 1 and VLAN 120 are allowed.

```

interface TenGigabitEthernet1/0/1
switchport trunk allowed vlan 1,120
switchport mode trunk
ip dhcp relay information trusted
ip dhcp snooping trust

```

Configure the default route outbound:

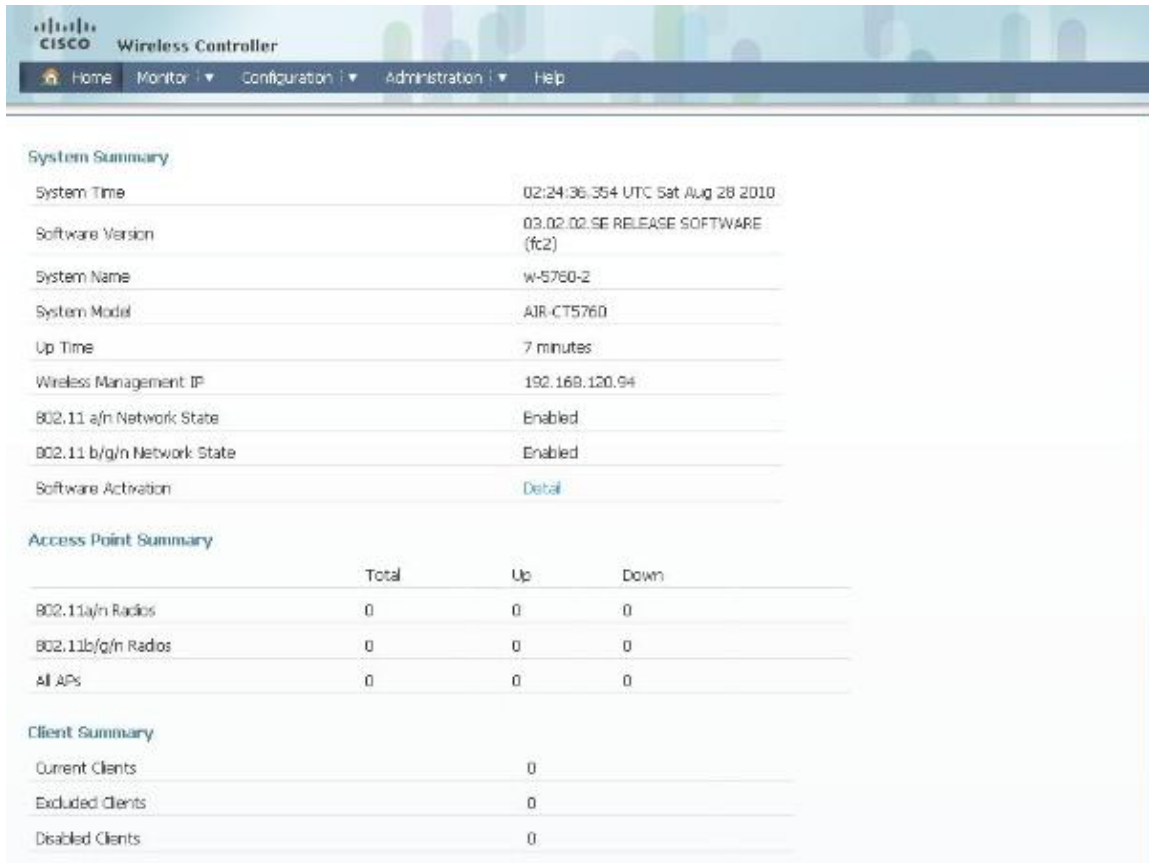
```
ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

2. Configure web access.

The GUI can be accessed via `https://<ipaddress>/wireless`

The logon credentials are already defined in the initial configuration dialog.

```
username admin privilege 15 password cisco
```



The screenshot displays the Cisco Wireless Controller web interface. At the top, there is a navigation bar with 'Home', 'Monitor', 'Configuration', 'Administration', and 'Help' menus. Below this, the 'System Summary' section provides key system information:

Property	Value
System Time	02:24:36.354 UTC Sat Aug 28 2010
Software Version	03.02.02 SE RELEASE SOFTWARE (fc2)
System Name	w-5760-2
System Model	AIR-CT5760
Up Time	7 minutes
Wireless Management IP	192.168.120.94
802.11 a/n Network State	Enabled
802.11 b/g/n Network State	Enabled
Software Activation	<a href="#">Detail</a>

The 'Access Point Summary' section shows a table with columns for 'Total', 'Up', and 'Down' across different radio types:

Radio Type	Total	Up	Down
802.11a/n Radios	0	0	0
802.11b/g/n Radios	0	0	0
All APs	0	0	0

The 'Client Summary' section shows the following counts:

Client Type	Count
Current Clients	0
Excluded Clients	0
Disabled Clients	0

3. Ensure the wireless management interface is correctly configured.

```
wireless management interface Vlan120
```

```
w-5760-1#sh run int vlan 120
```

```
Building configuration...
```

```
Current configuration : 62 bytes
```

```
!  
interface Vlan120  
ip address 192.168.120.94 255.255.255.0  
end
```

```
w-5760-1#sh ip int br
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.20	YES	manual	up	up
Vlan120	192.168.120.94	YES	manual	up	up
GigabitEthernet0/0	unassigned	YES	unset	down	down
Te1/0/1	unassigned	YES	unset	up	up
Te1/0/2	unassigned	YES	unset	down	down
Te1/0/3	unassigned	YES	unset	down	down
Te1/0/4	unassigned	YES	unset	down	down
Te1/0/5	unassigned	YES	unset	down	down
Te1/0/6	unassigned	YES	unset	down	down
Capwap2	unassigned	YES	unset	up	up

w-5760-1#

4. Ensure an active license is enabled with the proper AP count.

**Note:** 1) The 5760 does not have activated license levels, the image is already ipservices. 2) The 5760 that acts as a Mobility Controller (MC) can support up to 1000 APs.

w-5760-1#*license right-to-use activate apcount <count> slot 1 acceptEULA*

5. Ensure the correct country code is configured on the WLC in compliance with the regulatory domain of the country the AP(s) are deployed in.

w-5760-1#*show wireless country configured*

```
Configured Country.....: US - United States
Configured Country Codes
  US - United States : 802.11a Indoor,Outdoor/ 802.11b / 802.11g
```

In order to modify the country code, enter these commands:

w-5760-1(config)#*ap dot11 24ghz shutdown*

w-5760-1(config)#*ap dot11 5ghz shutdown*

w-5760-1(config)#*ap country BE*

Changing country code could reset channel and RRM grouping configuration.

If running in RRM One-Time mode, reassign channels after this command.

Check customized APs for valid channel values after this command.

Are you sure you want to continue? (y/n)[y]: y

w-5760-1(config)#*no ap dot11 24ghz shut*

w-5760-1(config)#*no ap dot11 5ghz shut*

w-5760-1(config)#*end*

w-5760-1#*wr*

Building configuration...

Compressed configuration from 3564 bytes to 2064 bytes[OK]

w-5760-1#*show wireless country configured*

```
Configured Country.....: BE - Belgium
Configured Country Codes
  BE - Belgium : 802.11a Indoor,Outdoor/ 802.11b / 802.11g
```

6. Ensure that the APs are able to learn the IP address of the WLC ( 192.168.120.94 in this example) via DHCP option 43, Domain Name Services (DNS), or any other dicoverly mechanism in CAPWAP.

## Verify

In order to ensure that the APs has joined, enter the *show ap summary* command:

w-5760-1#*show ap summary*

Number of APs: 1

Global AP User Name: Not configured

Global AP Dot1x User Name: Not configured

AP Name	AP Model	Ethernet MAC	Radio MAC	State
APa493.4cf3.232a	1042N	a493.4cf3.232a	10bd.186d.9a40	Registered

## Troubleshoot

Useful debugs to troubleshoot AP join issues:

```
w-5760-1#debug capwap ap events  
capwap/ap/events debugging is on
```

```
w-5760-1#debug capwap ap error  
capwap/ap/error debugging is on
```

```
w-5760-1#debug dtls ap event  
dtls/ap/event debugging is on
```

```
w-5760-1#debug capwap ios event  
CAPWAP Event debugging is on
```

```
5760-1#debug capwap ios error  
CAPWAP Error debugging is on
```

## 3850 Switch Initial Configuration

This section includes the configuration required to host wireless services on the 3850.

### Configure

#### Setup Script

```
--- System Configuration Dialog ---  
  
Enable secret warning  
-----  
In order to access the device manager, an enable secret is required  
If you enter the initial configuration dialog, you will be prompted  
for the enable secret  
If you choose not to enter the initial configuration dialog, or if you  
exit setup without setting the enable secret,  
please set an enable secret using the following CLI in configuration mode-  
enable secret 0 <cleartext password>  
-----  
Would you like to enter the initial configuration dialog? [yes/no]: yes  
  
At any point you may enter a question mark '?' for help.  
Use ctrl-c to abort configuration dialog at any prompt.  
Default settings are in square brackets '['].  
  
Basic management setup configures only enough connectivity  
for management of the system, extended setup will ask you  
to configure each interface on the system  
  
Would you like to enter basic management setup? [yes/no]: yes  
Configuring global parameters:  
  
Enter host name [Switch]: sw-3850-1  
  
The enable secret is a password used to protect access to  
privileged EXEC and configuration modes. This password, after  
entered, becomes encrypted in the configuration.  
Enter enable secret: Cisco123  
  
The enable password is used when you do not specify an  
enable secret password, with some older software versions, and
```



some boot images.  
Enter enable password: **Cisco123**

The virtual terminal password is used to protect access to the router over a network interface.  
Enter virtual terminal password: **Cisco123**

Do you want to configure country code? [no]: **yes**

Enter the country code[US]:**US**

Note : Enter the country code in which you are installing this 3850 Switch and the AP(s). If your country code is not recognized, enter one that is compliant with the regulatory domain of your own country

Setup account for accessing HTTP server? [yes]: **yes**

Username [admin]: **admin**

Password [cisco]: **cisco**

Password is UNENCRYPTED.

Configure SNMP Network Management? [no]: **no**

Current interface summary

Any interface listed with OK? value "NO" does not have a valid configuration

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	NO	unset	up	down
GigabitEthernet0/0	unassigned	YES	unset	up	up
GigabitEthernet2/0/1	unassigned	YES	unset	down	down
GigabitEthernet2/0/2	unassigned	YES	unset	down	down
GigabitEthernet2/0/3	unassigned	YES	unset	down	down
...					
...					
...					
GigabitEthernet2/0/46	unassigned	YES	unset	down	down
GigabitEthernet2/0/47	unassigned	YES	unset	down	down
GigabitEthernet2/0/48	unassigned	YES	unset	up	up
GigabitEthernet2/1/1	unassigned	YES	unset	down	down
GigabitEthernet2/1/2	unassigned	YES	unset	down	down
GigabitEthernet2/1/3	unassigned	YES	unset	down	down
GigabitEthernet2/1/4	unassigned	YES	unset	down	down
Te2/1/1	unassigned	YES	unset	down	down
Te2/1/2	unassigned	YES	unset	down	down
Te2/1/3	unassigned	YES	unset	down	down
Te2/1/4	unassigned	YES	unset	down	down

Enter interface name used to connect to the management network from the above interface summary: **vlan1**

Configuring interface Vlan1:

Configure IP on this interface? [yes]: **yes**

IP address for this interface: **192.168.1.2**

Subnet mask for this interface [255.255.255.0] : **255.255.255.0**

Class C network is 192.168.1.0, 24 subnet bits; mask is /24

This configuration command script was created:

```
hostname sw-3850-1
enable secret 4 vwcGVdcUZcRMCyxaH2U9Y/PTujsnQWPSbt.LFG8lhTw
enable password Cisco123
line vty 0 15
password Cisco123
ap dot11 24ghz shutdown
ap dot11 5ghz shutdown
```

```

ap country US
no ap dot11 24ghz shutdown
no ap dot11 5ghz shutdown

username admin privilege 15 password 0 cisco
no snmp-server
!
no ip routing

!
interface Vlan1
no shutdown
ip address 192.168.1.2 255.255.255.0
!
interface GigabitEthernet0/0
shutdown
no ip address
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/2
!
interface GigabitEthernet2/0/3
...
...
...
interface GigabitEthernet2/0/46
!
interface GigabitEthernet2/0/47
!
interface GigabitEthernet2/0/48
!
interface GigabitEthernet2/1/1
!
interface GigabitEthernet2/1/2
!
interface GigabitEthernet2/1/3
!
interface GigabitEthernet2/1/4
!
interface TenGigabitEthernet2/1/1
!
interface TenGigabitEthernet2/1/2
!
interface TenGigabitEthernet2/1/3
!
interface TenGigabitEthernet2/1/4
!
end

```

- [0] Go to the IOS command prompt without saving this config.
- [1] Return back to the setup without saving this config.
- [2] Save this configuration to nvram and exit.

```

Enter your selection [2]: 2
The enable password you have chosen is the same as your enable secret.
This is not recommended. Re-enter the enable password.
Changing country code could reset channel and RRM grouping configuration.
If running in RRM One-Time mode, reassign channels after this command.
Check customized APs for valid channel values after this command.
Are you sure you want to continue? (y/n)[y]: y
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

```

Building configuration...  
Compressed configuration from 4414 bytes to 2038 bytes[OK]  
Use the enabled mode 'configure' command to modify this configuration.

Press RETURN to get started!

## Required Configuration for Access Points to Join

**Note:** Important – Ensure that the correct boot command is configured under global configuration. If it has been extracted on the flash, then the *boot system switch all flash:packages.conf* command is required.

1. Configure wireless prerequisites.

In order to enable wireless services, the 3850 must run an *ipservices or ipbase* license.

2. Enable wireless on the switch.

**Note:** The APs need to be connected to access mode switchports in the same VLAN!

- ◆ Enable wireless management

```
sw-3850-1(config)#wireless management interface vlan <1-4095>
```

- ◆ Define the MC

An MC must be defined in order to allow APs to join.

- a. If this 3850 will be the MC, enter the *wireless mobility controller* command:

```
sw-3850-1(config)#wireless mobility controller
```

**Note:** This configuration change requires a reboot!

- b. If this 3850 operates as a Mobility Agent (MA), then point it to the MC IP address with this command:

```
sw-3850-1(config)#wireless mobility controller ip a.b.c.d
```

And on the MC, enter these commands:

```
3850MC(config)#wireless mobility controller peer-group <SPG1>
```

```
3850MC(config)#wireless mobility controller peer-group <SPG1> member ip w.x.y.z
```

3. Ensure license availability.

Ensure that active AP Licenses are available on the MC (the MA uses the licenses that are activated on the MC):

**Note:** 1) The 3850 must run ipservices or an ipbase license in order to enable wireless services on the 3850. 2) AP count licenses are applied at the MC, and are automatically provisioned and enforced at the MA. 3) The 3850 which acts as an MC can support up to 50 APs.

```
sw-3850-1#show license right-to-use summary
```

License Name	Type	Count	Period left
-----			

ipservices	permanent	N/A	Lifetime
apcount	base	1	Lifetime
apcount	adder	49	Lifetime

-----

```
License Level In Use: ipservices
License Level on Reboot: ipservices
Evaluation AP-Count: Disabled
Total AP Count Licenses: 50
AP Count Licenses In-use: 1
AP Count Licenses Remaining: 49
```

In order to activate the AP count license on the 3850, enter this command with the required AP count on the MC:

```
sw-3850-1#license right-to-use activate apcount <count> slot <#> acceptEULA
```

4. Configure the AP discovery process.

In order for APs to join the controller, the switchport configuration *must be set as an access port* in the wireless management vlan:

If vlan 100 is used for the wireless management interface:

```
sw-3850-1(config)#interface gigabit1/0/10
sw-3850-1(config-if)#switchport mode access
sw-3850-1(config-if)#switchport access vlan 100
```

5. Configure web access.

The GUI can be accessed via <https://<ipaddress>/wireless>

The logon credentials are already defined in the initial configuration dialog.

```
username admin privilege 15 password 0 cisco ( username for Web access)
```

The screenshot shows the Cisco Wireless Controller web interface. The top navigation bar includes Home, Monitor, Configuration, Administration, and Help. The main content area is divided into three sections:

- System Summary:** A table with the following data:
 

System Time	02:24:36.354 UTC Sat Aug 28 2010
Software Version	03.02.02.SE RELEASE SOFTWARE (fc2)
System Name	w-5760-2
System Model	AIR-CT5760
Up Time	7 minutes
Wireless Management IP	192.168.120.94
802.11 a/n Network State	Enabled
802.11 b/g/n Network State	Enabled
Software Activation	<a href="#">Detail</a>
- Access Point Summary:** A table with columns Total, Up, and Down.
 

	Total	Up	Down
802.11a/n Radios	0	0	0
802.11b/g/n Radios	0	0	0
All APs	0	0	0
- Client Summary:** A table with the following data:
 

Current Clients	0
Excluded Clients	0
Disabled Clients	0

6. Ensure that the proper country code is configured on the switch in compliance with the regulatory domain of the country the AP(s) are deployed in.

```
sw-3850-1#show wireless country configured
```

```
Configured Country.....: US - United States
Configured Country Codes
US - United States : 802.11a Indoor,Outdoor/ 802.11b / 802.11g
```

In order to modify the country code, enter these commands:

```
sw-3850-1(config)#ap dot11 24ghz shutdown
```

```
sw-3850-1(config)#ap dot11 5ghz shutdown
```

```
sw-3850-1(config)#ap country BE
```

Changing country code could reset channel and RRM grouping configuration.

If running in RRM One-Time mode, reassign channels after this command.

Check customized APs for valid channel values after this command.

Are you sure you want to continue? (y/n)[y]: y

```
sw-3850-1(config)#no ap dot11 24ghz shut
```

```
sw-3850-1(config)#no ap dot11 5ghz shut
```

```
sw-3850-1(config)#end
```

```
sw-3850-1#wr
```

Building configuration...

Compressed configuration from 3564 bytes to 2064 bytes[OK]

```
sw-3850-1#show wireless country configured
```

```
Configured Country.....: BE - Belgium
```

```
Configured Country Codes
```

```
BE - Belgium : 802.11a Indoor,Outdoor/ 802.11b / 802.11g
```

## Verify

In order to ensure that the AP(s) has joined, enter the *show ap summary* command:

```
sw-3850-1#show ap summary
```

```
Number of APs: 1
```

```
Global AP User Name: Not configured
```

```
Global AP Dot1x User Name: Not configured
```

AP Name	AP Model	Ethernet MAC	Radio MAC	State
APa493.4cf3.232a	1042N	a493.4cf3.231a	10bd.186e.9a40	Registered

## Troubleshoot

Useful debugs to troubleshoot AP join issues:

```
sw-3850-1#debug capwap ap events  
capwap/ap/events debugging is on
```

```
sw-3850-1#debug capwap ap error  
capwap/ap/error debugging is on
```

```
sw-3850-1#debug dtls ap event  
dtls/ap/event debugging is on
```

```
sw-3850-1#debug capwap ios event  
CAPWAP Event debugging is on
```

```
sw-3850-1#debug capwap ios error  
CAPWAP Error debugging is on
```

---

Updated: Aug 13, 2013

Document ID: 116342

---