

# Cisco Unified Access CT5760 Controllers, Catalyst 3850 Switches IOS XE Software Release 3.2.2 Web GUI Deployment Guide

Last Updated: August, 2013



	1.1
	- difficulture
	· · · · · · · · · · · · · · · · · · ·
CONTRACTOR DESCRIPTION OF THE OWNER	
COLORED DESCRIPTION AND ADDRESS AND	



**Cisco Systems, Inc.** www.cisco.com

# Introduction

This document introduces the Maintenance Release 3.2.2 Web GUI functionality for the Cisco Converged Access CT5760 and Cat3850 products. This guide is designed to help you access, configure and monitor both products using the GUI Web interface.

#### CT5760 Controller

CT5760 is an innovative UADP ASIC based wireless controller deployed as a centralized controller in the next generation unified wireless architecture. CT5760 controllers are specifically designed to function as the Unified model central wireless controllers. They also support the newer Mobility functionality with Converged Access switches in the wireless architecture.



CT5760 controllers will be deployed behind a core switch/router. The core switch/router will be the only gateway into the network for the controller. The uplink ports connected to the core switch will be configured as EtherChannel trunk to ensure port redundancy.

This new controller is an extensible and high performing wireless controller, which can scale up to 1000 access points and 12000 clients. The controller has 6-10 Gbps data ports.

As a component of the Cisco Unified Wireless Network, the 5760 series works in conjunction with Cisco Aironet access points, the Cisco Prime infrastructure and the Cisco Mobility Services Engine to support business-critical wireless data, voice, and video applications.

### **Catalyst 3850 Controller**

Unified Access Catalyst 3850 switches are innovative UADP ASIC hardware that can support multiple protocols and has many advantages over the current hardware platform. CAT3850 switch has an integrated hardware based wireless support with CAPWAP and fragmentation. The CAT3850 switch has 40gig of uplink bandwidth with all port functioning at line rate.



The CAT3850 switches provide Open Service platform. It is a 4 core CPU to leverage the OS and to host various services. The CAT3850 hardware is the Next-Gen switching hardware.

UA CAT3850 switches have unified wired and wireless architecture. The wireless operating system is IOS based. UA CAT3850 switches provide uniform wired and wireless policies. The CAT3850 switch can manage 50 access points-802.11n and support 2000 clients per stack.

# **Getting Started**

Before you get started with enabling the WEB GUI on the Cat3850/CT5760, make sure you have the following:

- CLI access to the box. Console Access information is shown in the CLI/Console Access section below.
- 2. Have one of the Supported Browser Version as listed in the section.
- **3.** Go through Release 3.2.2 release notes located at:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2\_0\_se/release\_notes/OL28114.html#wp223882

4. Have access information such as Username/Password and networking access information.

#### Supported Browser Version

Below is a list of supported browser versions:

- Chrome Ver. 26.x
- Mozilla Ver. 20.x
- IE Ver. 8.x, 9.x and 10.x

### **CLI/Console Access**

Before you configure the switch or controller for basic operations, you must connect it to a PC that uses a VT-100 terminal emulator (such as HyperTerminal, ProComm, or Putty).

The controller has both EIA/TIA-232 asynchronous (RJ-45) and USB 5-pin mini Type B, 2.0 compliant serial console ports. The default parameters for the console ports are 9600 baud, eight data bits, one stop bit, and no parity. The console ports do not support hardware flow control. Choose the serial baud rate of 9600; if you have issues, try a baud rate of 115200. The figure below shows an example of a Mac Secure CRT; use similar configuration for PC/Windows Putty, and so on.





# Enabling WEB GUI on both the 5760 and 3850 Platforms

Both the Cat3850 and CT5760 currently ship with the first release labeled as 3.2.01. If you have an existing CAT3850/CT5760 and want to use GUI to configure/monitor your wireless network, please follow the steps below:

 Console to the 3850/5760 platform. Save your current configuration and upgrade to 3.2.2 release available on cisco.com. Upgrade procedure can be found in the link below: http://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2\_0\_se/system\_m anagement/appendix/swiosfs.html#wp1311040

Note

During the upgrade, firmware will be upgraded and therefore it will take few more additional minutes than the regular upgrade. Please do not turn off the unit during the upgrade.

- 2. After upgrading to 3.2.2 version, the web GUI functionality will be enabled. By default, https is enabled. You can access the web GUI through https but if you want to enable http access, you can do so by issuing the following command using IOS CLI command: Controller(config)#ip http server
- 3. Using IOS CLI, you will need to create a username and password to access the GUI. You can configure a local username by issuing the following command: Controller(config)#username admin privilege 15 password Cisco123. Or you can configure it to use credentials using an authentication server. Make sure the user has privilege 15 access level.

- **4.** In order to access the GUI, you can configure the out of band management port (GigE 0/0) or use existing reachable configured interfaces through the network.
- 5. Now you will be able to access the Web GUI interface. Open a browser and type your controller/switch IP address. Example: https://10.10.10.5/ . Please refer to the configuration examples below for additional Web GUI access information.

Note

If you have an out of the box or brand new 5760 or 3850, please console to the box and go through the Startup Wizard as outline in the deployment guide located at: http://www.cisco.com/en/US/docs/wireless/technology/5760\_deploy/Supported\_Features.html

# **Configuration Examples**

If you require additional information regarding any of the field while going through the deployment guide, please refer to the GUI online Help available after you have successfully accessed the GUI through the steps below.

#### GUI access for CT5760/3850 Example

Complete these steps:

**Step 1** For GUI access, open a browser and type your controller IP address. By default https is enabled, for example:

https://10.10.10.5

username: admin

Password: Cisco123

Note

You can setup username/password using the following CLI command: Controller(config) #username admin privilege 15 password Cisco123. This is an example and not the default username and password.

The server 10.10 password.	).10.5 at level_15	_or_view_acce	ess require	a usernam	e and
Warning: This s sent in an insec connection).	erver is requesti ure manner (bas admin eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee	ng that your u sic authenticat my credentia	Is sername a	nd passwor ut a secure <u>Pass</u> <u>Cisco</u> 1	d be
			ОК	Ca	ancel

Once you login, you will be directed to the following page:

#### **Cisco Systems**

#### Accessing Cisco AIR-CT5760 "Controller"



#### Help resources

1. CCO at www.cisco.com - Cisco Connection Online, including the Technical Assistance Center (TAC).

- 2. tac@cisco.com e-mail the TAC.
- 3. 1-800-553-2447 or +1-408-526-7209 phone the TAC.
- 4. cs-html@cisco.com e-mail the HTML interface development group.



🙆 Home Monitor 🔻	Configurat	ion   🔹 🛛	Administration   🔻			
System Summary		N		Rogue APs		
System Time	12:04:23	3.728 UTC	Wed Mar 27 2013	Active Rogue APs	0	Det
Software Version	03.09.45 ENGINE	S.RDP EARL	A WEEKLY BUILD	Active Rogue Clents	0	Det
System Name	Controlle	er		Adhoc Rogues	0	Det
System Model	AIR-CT5	760		Top WLANs		
Up Time	17 hours	s, 59 minut	es	Profile Name Number of Clie	ts	
Management IP Address	169.254	.1.1				
802.11 a/n Network State	Enabled					
802.11 b/g/n Network State	Enabled					
Software Activation	Detail					
Access Point Summary						
	Total	Up	Down			
802.11a/n Radios	0	0	0			
802.11b/g/n Radios	0	0	0			
All APs	0	0	0			

### **Basic Configuration for the CT5760/3850 Example**

In this section you will perform basic controller and management configuration using the GUI Wizard of the CT5760 or CAT 3850.

**Step 3** Under the Configuration tab, choose the option **Wizard**.



**Step 4** Configure Admin username and password.

ſ



1

**Step 5** Configure SNMP information–SNMP trap can be configured in this section, give a **Location** and **Contact** and proceed to the next step.

cisco Wireless Cor	troller		Save Configuration   Refresh
😚 Home Monitor 🔻	Configuration   •	Administration 💌 Help	
Wizard	SNMP System St	nmary	Previous Next
I: Admin Users			1
2: SNMP System Summa	Location	bldg5	/
3: Port Management	Contact	tme	
4: Wireless Management	SNMP global trap	Disabled *	
S: RF Mobility and Count	SNMP logging	Disabled	
6: Mobility Configuration			
7: WLANs			
8: 802.11 Configuration			0
9: Set Time			136
Final : Save Wizard			6

Step 6 Management Interface Configuration–You can use the out of band Management Port to access the controller. Please enter the IP address/Netmask and proceed to the next screen for Wireless management configuration.

cisco Wireless Cor	ntroller		Save Configuration   Refresh
🏠 Home Monitor 🔻	Configuration 🛛 🔻	Administration 🔻 Help	
Wizard	Port Management		Previous Next
1: Admin Users	Interface:	GigabitEthernet 0/0	1
2: SNMP System Summa	IP Address	2.2.2.2	
3: Port Management	Netmask	255.255.255.0	
4: Wireless Management	IPV6 Address		
5: RF Mobility and Count	IPv4 DHCP Server	2.2.2.1	]
6: Mobility Configuration	IPv6 DHCP Server		]
7: WLANs			
8: 802.11 Configuration			
9: Set Time			
Final : Save Wizard			

**Step 7** Wireless Management Configuration–This is where you can configure Wireless Management interface on the 5760 and assign it for a specific VLAN. Please assign VLAN IP and default gateway.

cisco Wireless Controller				Save Configuration   Refresh
<ul> <li>Home Monitor ▼ Configu</li> <li>Wizard</li> </ul>	ration V Administration V Help			Previous Next
1.1 Admin Users     2: SNMP System Summary     3: Fork Management     4: Wireless Management     5: Fit Mobility and Country Code     6: Mobility Configuration     7: WLANs     8: 802.11 Configuration     9: Set Time     Final : Apply Wizard	Select Interface VLAN Id * IP Address * Netmask * IPv6 Address IPv4 DHCP Server IPv6 DHCP Server SwitchPort Configurations	VLAN	-	
	Available port Te1/0/2 Te1/0/4 Te1/0/4 Te1/0/5 Te1/0/6	Selected Trunk ports Te1/0/1 Selected Access ports		
	* fields are Mandatory			

**Step 8** RF Mobility and Country Code settings–This is where you can enter RF Mobility config and select a country code. As an example, enter **rfdemo** as the RF mobility name and choose **US** for Country Code.

Vizard	RF Mobility and Country Code	Previous New
🛚 1: Admin Users	-	1
2: SNMP System Summa	RF Mobility	
3: Port Management	RF Mobility rfdemo	
4: Wireless Management		
5: RF Mobility and Count	Country Code	
6: Mobility Configuration	Country Code US 💌	
I 7: WLANs	Note: On applying Country Code the 802.11a/n and 802.11 b/g/n will be disa	abled.
8: 802.11 Configuration		
9: Set Time		
Final : Save Wizard		

**Step 9** Mobility Configuration–Here you can change the Mobility Group Name and other Mobility timers. Please click Next and move to the next screen.

I

Wizard	Mobility Configuration		Previous Next
<ul> <li>1: Admin Users</li> <li>2: SNMP System Summa</li> <li>3: Port Management</li> <li>4: Wireless Managemeni</li> <li>5: RF Mobility and Couni</li> <li>5: RF Mobility Configuration</li> <li>7: WLANs</li> <li>8: 802.11 Configuration</li> <li>9: Set Time</li> </ul>	Mobility Role Mobility Protocol Port Mobility Group Name Mobility Oracle Enabled Mobility Oracle IP Address DTLS Mode Mobility Domain ID for 802.11r Mobility Keepalive Interval (1-30)sec	Mobility Controller 16666 rfdemo 0.0.0.0 Enabled 0xac34 10 2	

1

**Step 10** Creating a WLAN–You will be able to create a WLAN in this screen. It will be disabled by default. Create an 802.1x WLAN name. In this example, we will use (NGWC1-1x).

Wizard	WLANs		Previous Next
1: Admin Users     2: SNMP System Summe     3: Port Management     4: Wireless Management     5: RF Mobility and Count	WLAN ID 1 SSID NGWC1-1x Profile Name NGWC1-1x Note: WLAN created will have open au	Creating 802; 1x WLAN thentication and will be in disabled mode.	1
U 7: WLANs			
8: 802.11 Configuration			
9: Set Time			
Final : Save Wizard			

**Step 11** Enabling 802.11 Radios–Radios were disabled once we changed the country code in earlier steps. Click on the radio button to Enable the 802.11a/n and 802.11 b/g/n

lizard	802.11 Configura	ation		Previous Next
1: Admin Users     2: SNMP System Summe     3: Port Management     4: Wireless Management     5: RF Mobility and Count     6: Mobility Configuration     7: 3: MAN	802.11 a/n 802.11 b/g/n	<ul> <li>✓ Enabled</li> <li>✓ Enabled</li> </ul>	Click to enable radios	1
# 8: 802.11 Configuration				

**Step 12** Time Settings–You can choose between two modes: Manual and NTP. In this example: we are choosing NTP and using 10.10.10.1 as the NTP Server IP Address.

Vizard	Set Time		Previous
<ul><li>1: Admin Users</li><li>2: SNMP System Summary</li></ul>	Current Time		1
3: Port Management	Current Time	11:23:20.144 UTC Mon Apr 1 2013	
4: Wireless Management	Mode		
5: RF Mobility and Country C	Mode	NTP -	
6: Mobility Configuration	NTP Server		
7: WLANS	NTP Server	10 10 10 1	
8: 802.11 Configuration	(Hostname/IPv4 /IPv6)	10.10.10.1	

Step 13 Saving and Applying Wizard

I

Γ

Wizard	Save Wizard			Previous Apply	
<ul> <li>1: Admin Users</li> <li>2: SNMP System Summary</li> </ul>	Stan 1: ADMIN licer		Step 6: Mobility Configuration		
3: Port Management 4: Wireless Management 5: RF Mobility and Country Code 6: Mobility Configuration 7: NA Mathematical Statement	User Name Step 2: SNMP System Summary	P0D1	Mobility Mode Mobility Mode Oracle IP Address Step 7: WLANs	Mobility Controller Disabled 0.0.00 review info and Click Apply	
<ul> <li>Y: WLANS</li> <li>8: 802.11 Configuration</li> <li>9: Set Time</li> <li>Final : Save Wizard</li> </ul>	Location bidg5 Contact true SNMP Logging Disabled SNMP Global Trap Disabled Step 3: Port Management		WLAN ID 1 SSID NGWC1-1x Profile Name NGWC1-1x Note: WLAN created will have open authentication and will be in disabled i Step 8: 802.11 Configuration		
	IP Address Netmask IPv6 Address DHCP DHCP IPv6 Stan 4: Windows Management	22.22 255.255.255.0 - 22.2.1 -	802.11 a/n 802.11 b/g/n	Enabled Enabled	
	Jep 4. Micros Hanagement Interface IP Address IPv6 Address DHCP DHCP IPv6	VLAN 10 10.10.10.5 255.255.255.0 - 10.10.10.1 -	Mode Time NTP Server	NTP - 10.10.10.1	
	Step 5: RF Mobility and Country (	Code			

Step 14 Confirmation Message–After pressing apply, please wait few seconds until the configurations have been applied. You should see the success message below. Click OK and this should conclude the initial Wizard configuration.

Step 8- Success :802.11 configuration applied successfully Step 9- Success :Time Configuration set successfully OK	378
Step 1- Success :User name configuration applied successfully Step 2- Success :SNMP configuration applied successfully Step 3- Success :Port Management configuration applied successfully Step 4- Success :Wireless Management configuration applied successfully Step 5- Success :RF Mobility and Country Code configuration applied successfully. Step 6- Success :Mobility configurations submitted successfully Step 7- Success :Wireless Management configuration applied successfully.	

1



This concludes the Initial Wizard setup. Next section describes the AAA configuration.

# AAA Configuration for 802.1x WLAN Example

In this section you will setup AAA configuration.

Step 15 Configuring AAA settings for 802.1x WLAN–Under Configuration tab, choose Security.

cisco Wireless Contro	ller	
👩 Home Monitor 🔻 C	onfiguration 💌 Adminis	tration V Help
Wizard 1: Admin Users 2: SNMP System Summar 3: Port Management 4: Wireless Management 5: RF Mobility and Country Co 6: Mobility Configuration	Wizard Controller Wireless Security Commands	POD1 User name configuration applied successfully
7: WLANs	Step 2: SNMP Sys	tem Summary
<ul> <li>8: 802.11 Configuration</li> <li>9: Set Time</li> </ul>	Location	bldg5
Final : Save Wizard	SNMP Logging	Disabled se

This will take you to the AAA configuration page:

cisco Wireless Con	troller					Sive Con	guiadon ( Kenesh
👌 Home - Monitor 💌	Configuration 🔻	Administration	нер				
security	Authentication	1					
* AAA	New Remove					Show Quick Filter	- 16
Method LBIS     Server Groups     Server Groups     RADBUS     TACACS+ Servers     UDAP Servers     USers     WAC Fibering     A P Policy     Icroll EAP	Name	Type	Group1	Group2 No data availab	Group3	Group4	
Wireless Protection Policies     CIDS     ACL     Web Auth							

Step 16 Radius Server Configuration–Expand Radius Tab and Click New

cisco Wireless Cont	troller				0
👌 Home Monitor 🔻	Configuration	ation 🛛 🔻 Help			
ecurity	Radius Servers				
AAA	New Remove				
Method Lists	Server Name	Address	Auth Port	Acct Port	
Server Groups					
▼ RADIUS				No data available	
Servers					
Fallback					
TACACS+ Servers					
LDAP Servers					
Users					
MAC Filtering					
AP Policy					

Please enter the ISE/Radius server information as shown below. Once done, Click Apply.

Security	RADIUS Servers Radius Servers > New	Shared Secret is secret	Apply
* AAA			
<ul> <li>Method Lists</li> </ul>	Server Name	cisco	7
General	Server IP Address	10.10.200.60	
Authentication	Shared Secret		
Accounting	Confirm Shared Secret	•••••	
Authorization	Acct Port (0-65535)	1813	
Server Groups	Auth Port (0-65535)	1812 change ports number to	
▼ RADIUS	Server Timeout (1-1000)secs	1813 and 1812 as shown	
Servers	Retry Count (0-100)		
Fallback			

Γ

Radius server Configured successfully	
ОК	

Click **Ok** and you should see the following window.

cisco Wireless Con	ntroller			
🏠 Home 🛛 Monitor 🛛 🔻	Configuration	Administration	Help	
Security	Radius Servers			
▼ AAA	New Remove			
Method Lists	Server Name	Address	Auth Port	Acct Port
<ul> <li>Server Groups</li> </ul>				
<ul> <li>RADIUS</li> </ul>	Cisco	10.10.20	0.60 1812	1813
Servers				

351383

I

**Step 17** Server Group Creation–Go to **Server Group > Radius > New** 

Security	Radius Server Group Radius Server Group > New		Give cisco as name	Apply
<ul> <li>AAA</li> <li>Method Lists</li> <li>General</li> <li>Authentication</li> <li>Accounting</li> <li>Authorization</li> <li>Server Groups</li> </ul>	Name Group Type Servers In This Group	cisco radius Available Servers	Move cisco from Available servers to Assigned Servers	1

Once you click **Apply**, a confirmation pop-up appears:



Click **Ok** and confirm the server group cisco is created.

Step 18 Creating AAA Method Lists for Authentication/Accounting/Authorization–Go to AAA > Method Lists > Authentication > New



Once you click **Apply**, a confirmation pop-up appears:



Click **Ok** and confirm the server group cisco is created. Repeat the same Step for Accounting and Authorization:

I

#### Accounting

Security	Accounting Accounting > New	Apply
Add     Wethod Lists     W General     W Authentication     W Accounting     W Authorization     Server Groups     W Radus     W Tacacs+	Method Lat Name Type: © 60tlx 0 exec 0 identity 0 network Available Server Groups Groups In This Method * Method Lat Name can be 'default' or any User defined Name.	
illiifi CISCO Wireless Cont Rome Montor •	Configuration • Administration • Help	
Hanne Montor V	Cenfguration I Mathematication I Help	
Horne Montor      Montor	Notifier Configuration I • Help Accounting Here Remove Sho Hame Type Group1 Group2 Group3 Group4	w Quick Fitter •

1

#### Authorization

curity	Authorization					Apply
***	Authorization > New	<u>_</u>				1
Method Lists	Nethod List Name cisco					1
Authentication     Accounting	Group Type:  group	local     Server Ground     As	Contract Consume			
u Authorization	Available	^	40 Adver Groups	*		
Server Groups	Groups In This Method	< >				
W Radus		-		-		
# Tararsa						
- 10000	* Mathad List Name on he Matha	or you likes defined lines				
W Ldap	* Method List Name can be 'defau	' or any User defined Name.				
# Ldap	* Method Lat: Name can be 'defaul ller onfguration • Administration • Help Authorization	t or any User defined Name.		_		
U Ldap	* Method Lat: Name can be 'defau ller onfiguration	t or any User defined Name.			Show Quick Filter	•]
E Ldap     Under     Wireless Contre     Home Hontor      Montor      Markot Lats     Second	* Method Lat Name can be 'defaul ller onfguration	C or any User defined Name.	Group2	Group3	Show Quick Filter	•]
i i Ldap i L	* Method Lat Name can be 'defaul Iler onfiguration • Administration • Help Authorization Here Ramore Harme Type	C or any User defined Name.	Group2	Group3	Show Quick Fitter	•1

This will conclude Radius and AAA configuration. Next section is WLAN settings. Before moving on, please Save your configuration by clicking on **Save Configuration** in the upper right hand side of the GUI.

uluilu cisco Wireless C	ontroller				Save Config	uration   Refresh
👌 Home Monitor 🔹	Configuration	Administration	Help			
Security	Authorization					
* AAA	New Remove	e		Show	Quick Filter	- 8
<ul> <li>Method Lists</li> </ul>	Name	Туре	Group1	Group2	Group3	Grou
General						139
Authentication	Cisco	network	cisco	N/A	N/A	N/A S

# **801.1x WLAN Configuration Example**

I

In this section you will perform 802.1x WLAN configuration using ISE as a radius server

**Step 19** Enabling 802.1x on the entire system.

Under Configuration tab, navigate to Controller > System > General

Wizard Controller			
Wireless Security Commands	Type netwo	ork	
	Security Commands	Security Commands	Security Commands

Enable **Dot1x System Auth Control** and click **Apply**. Once you get a confirmation message, move to the next step.

Controller	General		Apply
▼ System ■ General ■ Multicast	Name AP Muticast Mode	Controler Uncast *	1
<ul> <li>Interfaces</li> <li>VLAN</li> </ul>	Fast SSID change AP Falback		
Internal DHCP Server     Management	RF group name	defaut defaut	
<ul> <li>Mobility Management</li> <li>Mobility Global Config</li> </ul>	Temperature Value	30 Degree Celsius	
Mobility Peer     Switch Peer Group	Temperature Status Dot1x System Auth Contr	GREEN	

#### Step 20 Edit WLAN Configuration and Assigning VLAN–Under Configuration tab, choose Wireless

1

cisco Wireless Cor	troller		
👌 Home Monitor 🔻	Configuration 💌 Admi	nistration 🔻 Help	
Controller • System	Wizard Controller		
<ul><li>General</li><li>Multicast</li></ul>	Wireless Security Commands	POD1-5760 Unicast V	
Interfaces     VLAN	AP Fallback Default Mobility Domain	↓ v rfdemo	e e
<ul> <li>Management</li> </ul>	RF group name	rfdemo	35139

Navigate to **Wireless > WLAN**, you should see the WLAN summary page:

cisco Wireles	s Controller				Save	Configuration   Refresh
👌 Home Monito	or 🔻 Configuration 💌 Administ	ration 🔻 Help				
Wireless	WLANs					
* WLAN	Mobility Anchor New Rem	iove		Show	Quick Filter	- 8
WLANs	Profile	ID	SSID	V	LAN	Status
<ul> <li>Access Points</li> </ul>						
<ul> <li>802.11a/n</li> <li>Network</li> </ul>	□ NGWC1-1x	1	NGWC1-1x	1		Disabled

Select WLAN NGWC1-1x and then you will be able to edit its settings.

📩 Home Monitor 🔻	Configuration	l▼ Help				
Wireless * WLAN	WLAN WLAN > Edit General Security QOS	Advanced				Apply 7
<ul> <li>Access Points</li> <li>III APs</li> <li>Radios</li> <li>802.11a/n</li> <li>802.11b/g/n</li> <li>III Global AP Configuration</li> <li>III AP Configuration</li> </ul>	Profile Name Type SSID Status Security Policies	ngwc1-1x WLAN ngwc1-1x [WPA2][Auth(802.1 (Modifications done of	Enable WL x)] under security t	LAN tab will appear after applying the c	tranges.)	
<ul> <li>R02.11a/n</li> <li>Network</li> <li>RRM</li> <li>General</li> </ul>	Radio Policy Interface/Interface Group(G) Broadcast SSID Multicast VLAN Feature	Al • VLAN0010 •	-	Choose your Client VLAN		

Step 21 Apply Security Settings–Under Security tab, Layer 2. Make sure WPA+WPA2 is selected as Layer 2 Security and 802.1x is selected as an Auth Key Mgmt

👌 Home Monito	r 🛛 🔻 Configuration 🗍 👻 Administration 🗍 💌 Help	
Wireless WLAN WLANs Access Points 802.11a/n 802.11b/g/n Media Stream	WLAN > Edit General Security QOS Advanced Layer2 Layer3 AMA Server Layer 2 Security WPA + WPA2 +	Apply
	WPA+WPA2 Parameters WPA Policy WPA2 Policy WPA2 Encryption AES TKIP Auth Key Mgmt 802.1x •	

Under **WLAN > Security > AAA Server**, type cisco as the Authentication and Accounting Methods that we have created earlier under AAA.

👌 Home 🛛 Monitor 🛛 🔻	Configuration    Administration    Help	
Wireless * WLAN = WLANs	WLAN WLW > Edit General Security QOS Advanced	Apply
<ul> <li>Access Points</li> <li>802.11a/n</li> <li>Network</li> <li>RRM</li> <li>Media Parameters</li> <li>Roaming Parameters</li> </ul>	Layer2     Layer3     AMA Server       Authentication Method     clsco     Enter cisco for auth and acct       Accounting Method     clsco     auth and acct       Local EAP Authentication	351400

Under WLAN > Advanced, Enable Allow AAA Override

Vireless VILAN	WLAN WLAN > Edit General Security Q	XOS Advanced	Enable AAA Override		Apply
Access Points 802.11a/n	Allow AAA Override		DHCP		Î
802.11b/g/n Media Stream	Coverage Hole Detection Session Timeout (secs) (0 - Infinity) Aironet IE Diagnostic Channel P2P Blocking Action Client Exclusion Timeout Value(secs) Max Allowed Client	♥ 1800 Disabled ▼ ♥ 60 0	DHCP Server override DHCP Address Assignment required DHCP Option 82 DHCP Option 82 Format DHCP Option 82 Ascil Mode DHCP Option 82 Rid Mode NAC	None *	

Now Click Apply to enable the WLAN and its settings.

ſ

Wireless	WLAN > Edit		Apply
WLANs	General Security QOS	Advanced	
Access Points	Profile Name	NGWC1-1x	Click Apply to enable the
* 802.11a/n	Type	WLAN	settings
Network     RRM	SSID	NGWC1-1x	
Media Parameters	Status		
Roaming Parameters	Security Policies	[WPA2][Auth(802.1x)] (Modifications done under securi	ty tab will appear after applying the changes.)
<ul> <li>CleanAir</li> <li>802.11b/g/n</li> </ul>	Radio Policy	All 💌	
Network	Interface/Interface Group(G)	VLAN0010 -	
► RRM	Broadcast SSID		

1

Once you click **Apply**, you will be prompted with the message below. Click **Ok**.

Changing WLAN parameters while it is enabled will cause the WLAN to be momentarily disabled and this may result in loss of connectivity for some clients. Press OK to continue.	
OK Cancel	351403

Confirmation message appears. Click Ok.

Configured the WLAN successfully	
ОК	351404

**Step 22** Saving Config–Once client verification is done, please save the configuration by selecting **Save Configuration** in the upper right hand side of the screen.

cisco y	reless Controller	ation   Refresh
💧 Home	Monitor 🕴 Configuration I 🖲 Administration I 🖲 Help	
Controller	General	51405
* System		

# Creating a Switch Peer Group (SPG) on Mobility Controller 5760 Example

In this section, you will be able to configure Switch Peer Group(SPG) and add members (Mobility Agent) to the Group on the Mobility Controller (MC).

Step 23 On the 5760 controller GUI, navigate to Configuration > Controller > Mobility Management

cisco Wireless Con	troller				0	
👌 Home Monitor   🔻	Configuration	Administration				
Controller	Wizard					
System	Controller	_		_		
Internal DHCP Server	Wireless		Controller	]		
<ul> <li>Management</li> </ul>	Security	st Mode	Unicast 👻			
• Mobility Management	Commanus	change				
Mobility Global Config	AP Fallba	ck.				
Mobility Peer	Default M	lobility Domain	default	]		
Switch Peer Group	RF group	name	default			
	User idle	timeout	300	]		
	Temperat	ture Value	29 Degree Celsius			9
	Temperat	ture Status	GREEN			140
	Dot1x Sys	stem Auth Contro				35

Step 24 Under Mobility Management tab, select Switch Peer Group tab. Click New and create a new Switch Peer Group (SPG1)

or Home Monitor ▼ Co	nfiguration    Administration    He	ip	_	
Controller	Mobility Switch Peer Groups			
<ul> <li>System</li> </ul>	New Remove			
General	Switch Peer Group Name	Switch Peer Group Member Count	Bridge Domain ID	Multicast IP Address
Multicast				
<ul> <li>Interfaces</li> </ul>			No data available	
▶ VLAN				
Internal DHCP Server				
Management				
Mobility Management				
Mobility Global Config				
Mobility Peer				
Switch Peer Group	-			

Step 25 Create new Switch Peer Group SPG1 and Click Apply

I







Step 27 Go to Switch Peer Group tab and Verify that SPG1 is created. Select SPG1

	Mobility Switch Deer Groups			
Controller	Probinty Switch Feel Groups			
<ul> <li>System</li> </ul>	New Remove			
General	Switch Peer Group Name	Switch Peer Group Member Count	Bridge Domain ID	Multicast IP Address
Multicast				
<ul> <li>Interfaces</li> </ul>	SPG1	0	0	0.0.0.0
▶ VLAN				
Internal DHCP Server				
<ul> <li>Management</li> </ul>				
<ul> <li>Mobility Management</li> </ul>				
Mobility Global Config	Pouble Click SPG1			
II Mobility Paar				
= Producty PCC				

Step 28 Add member in SPG1 by clicking new

uluulu CISCO Wireless Control	ler d			
& Home Monitor v Co	Administration V Switch Peer Group > SPG1 Switch Peer Group > SPG1	Help		
* System	New Remove			Show
<ul> <li>Multicast</li> </ul>	IP Address	Public IP Address	Control Link Status	Data Link Status
Interfaces				
VLAN			No data available	
Internal DHCP Server				
<ul> <li>Management</li> </ul>				
<ul> <li>Mobility Management</li> </ul>				
Mobility Global Config				
Mobility Peer				
u Switch Peer Group				







I



You can repeat this step to additional MA to the switch group or create a different SPG name. **Step 31** Go to **Switch Peer Group** tab and verify that Switch peer group Member Count is 1.

uliulu CISCO Wireless Control	ler		1	
Controller	Mobility Switch Peer Groups			
* System	New Remove			
<ul> <li>General</li> <li>Multicast</li> </ul>	Switch Peer Group Name	Switch Peer Group Member Count	Bridge Domain ID	Multicast IP Address
Interfaces     VI AN	SPG1	1 🔶	0	0.0.0.0
Internal DHCP Server				
Management				
<ul> <li>Mobility Management</li> </ul>				
Mobility Global Config				
Mobility Peer				
U Switch Peer Group				

Step 32 Click SPG1 and verify your MA address and control and data link status as Down. That's normal for now since you will be configuring the 3850 (MA) in the upcoming steps.

CISCO Wireless Controll	er				Save Configuration   Refres
Controller > System	Switch Peer Group > SPG1 Switch Peer Group > SPG1				
<ul> <li>Internal DHCP Server</li> </ul>	New Remove			Show	Quick Filter 🗾 🏅
<ul> <li>Management</li> <li>Mobility Management</li> <li>Mobility Global Config</li> <li>Mobility Peer</li> <li>Switch Peer Group</li> </ul>	IP Address           10.10.10.2	Public IP Address       10.10.10.2	Control Link Status	Data Link Status	

# **Configuring Mobility between Mobility Agent (3850) and Mobility Controller** (5760) **Example**

Step 33 Follow the same steps outlined in the Basic Configuration for the CT5760/3850 Example to access and configure the 3850 switch. In this example, we will start with the Initial Wizard Configuration. Please note that there are differences between the 3850 and the 5760 Initial Wizard configuration.

Open a browser and type your 3850 IP address. For example:

https://10.10.10.2 Enter username: admin

nentreactori	Required	
?	A username and password are being requested by http://10.10.10.2. The site says: "level_15_or_view_access"	
Jser Name:	admin Pass: Cisco123	

Step 34 Landing Page for MA UA-C3850-24P. Select Wireless Web GUI

	▶ ③ 10.10.20.2	C ⊽ C
Ci	sco Systems	
Ace	cessing Cisco UA-C3850-24P "POD2-3850-sw"	
	Telnet - to the router.	
	<u>Show interfaces</u> - display the status of the interfaces. <u>Show diagnostic log</u> - display the diagnostic log. <u>Monitor the router</u> - HTML access to the command line interface at level 0.1.2.3.4.5.6.7.8.9.10.11.12.13.14.15	
	Show tech-support - display information commonly needed by tech support. Extended Ping - Send extended ping commands.	
1	<u>Wired Express Setup</u> - Configure basic connectivity on the Switch. <u>Wireless Web GUI</u> - Configure wireless on the Switch through the Web GUI interface.	
Helj	p resources	
1.2.3	CCO at www.cisco.com - Cisco Connection Online, including the Technical Assistance Center (TAC). tac@cisco.com - e-mail the TAC.	
4.	cs-html@cisco.com - e-mail the HTML interface development group.	

Step 35 Login to the Home page of the 3850 and verify the software version, System model and system name.

Γ

sco Wireless Cont	roller		20			
ome Monitor 🔻	Configur	ation i 🔻 🛛	Administration 🛛 🔻	p		
n Summary				Rogue APs		
em Time		12:02:33.6 2013	594 UTC Tue Apr 9	Active Rogue APs	200	Detail
ware Version		03.09.50.F		Active Rogue Clients	1	Detail
Name		POD1-3850		Top MI All-	,	Detail
n Model		UA-C3850-	48P 🔶	TOP WLANS		
ne		3 days, 19	hours, 27 minutes	Profile Name	Number of Clients	
ement IP Address		10.10.10.2	2	NGWC1-1x	1	
11 a/n Network State		Enabled		NGWC-WebGA	0	
11 b/g/n Network State		Enabled				
vare Activation		Detail				
s Point Summarv						
	Total	Up	Down			
a/n Radios	1	1	0			
b/g/n Radios	1	1	0			
°s	1	1	0			
Summary						
ant Clients		1				
ded Clients		D				
led Clients		D				

1

**Step 36** Under Configuration Tab, choose Wizard

cisco Wireless Cont	troller		
Wizard USCO Wireless Com Monitor View Wizard USCO Monitor View USCO MONITOR USCO MONITOR US	Vizard Configuration 🐨 Wizard Controller Wireless Security Commands	Administration V Help	
Final : Save Wizard			2514

**Step 37** Configure admin username and passwords

cisco Wireless Con	troller		Save Configuration   Refresh
👌 Home - Monitor 🔻	Configuration   •	Administration 🔻 Help	the second s
Wizard	ADMIN User		Next
■ 1: Admin Users	-		1
2: SNMP System Summa	UserName	POD1	
3: Port Management	Password	•••••	
4: Wireless Management	Confirm Password	•••••	
S: RF Mobility and Count			
6: Mobility Configuration			
7: WLANs			
8: 802.11 Configuration			
9: Set Time			420
Final : Save Wizard			551

**Step 38** You can configure SNMP trap in this section, give a Location and Contact to proceed to next step.

Home Monitor	Configuration	Administration V Help	
Wizard	SNMP System Su	mmary	Previous
1: Admin Users	-		1
2: SNMP System Summa	Location	bldg5	/
U 3: Port Management	Contact	tme	
4: Wireless Management	SNMP global trap	Disabled *	
S: RF Mobility and Count	SNMP logging	Disabled	
6: Mobility Configuration			
7: WLANs			
8: 802.11 Configuration			
9: Set Time			
Final : Save Wizard			

Step 39 Management Interface Configuration–You can use the out of band Management Port to access the switch. Please enter the IP address/Netmask shown in the screen below and proceed to next screen for Wireless management configuration.

🏠 Home Monitor 🔻 Config	uration   🔻 Administration	l▼ Help	
Wizard	Management Port		Previous
u 1: Admin Users	Interface:	Gigabit Ethernet 0/0	
2: SNMP System Summary	IP Address *	2.2.2.10	
3: Management Port	Netmask *	255.255.255.0	<i>"</i>
4: Wireless Management	IPV6 Address		
5: RF Mobility and Country Code	IPv4 DHCP Server	2.2.2.1	
6: Mobility Configuration	IPv6 DHCP Server		
7: WLANs			
8: 802.11 Configuration	* fields are Mandatory		
III 0: Sot Time			

Step 40 Wireless Management Configuration–This is where you can configure Wireless Management interface on the 3850 and assign it for a specific VLAN. Please assign VLAN IP and default gateway.

Note

I

AP is connected to Interface Gig1/0/3 marked as access port.

izard	Wireless Management	Previous Nex
u 1: Admin Users	Select Interface VLAN -	1
2: SNMP System Summary	VLAN Id * 10	
3: Management Port	IP Address * 10.10.10.2	-
4: Wireless Management	Netmask * 255.255.0	
5: RF Mobility and Country Code	IPv6 Address	
6: Mobility Configuration	IPv4 DHCP Server 10.10.10.1	
7: WLANs	IPv6 DHCP Server	
8: 802.11 Configuration		
9: Set Time	SwitchPort Configurations	
E Final : Apply Wizard	Avalable port Gg1/0/1 Gg1/0/2 Gg1/0/2 Gg1/0/5 Gg1/0/5 Gg1/0/6 Gg1/0/1 Gg1/0/10 Gg1/0/12	

1

Step 41 Enter RF mobility domain name as rfdemo and Country code US

Vizard	RF Mobility and Country Code	Previous Next
🛚 1: Admin Users	-	1
2: SNMP System Summa	RF Mobility	
3: Port Management	RF Mobility rfdemo	
4: Wireless Management		
S: RF Mobility and Count	Country Code	
6: Mobility Configuration	Country Code US 💌	
I 7: WLANs	Note: On applying Country Code the 802.11a/n and 802.11 b/g/n will be d	lisabled.
8: 802.11 Configuration		
9: Set Time		
Final : Save Wizard		

**Step 42** Enter Mobility configuration. Define Mobility role as Mobility Agent and enter Mobility Controller public and private IP Address as 10.10.10.5. This is where you point the MA to the MC.

CISCO Wireless Controller				Save Configuration   Refresh
🏠 Home Monitor 🔽 Configu	ration 🛛 🔻 Administration 🕅 🔻 Help			
Wizard	Mobility Configuration			Previous Next
1: Admin Users				
2: SNMP System Summary	Mobility Role	Mobility Agent 💌		Γ
3: Management Port	Mobility Controller IP Address	10.10.10.5	MC IP	4
4: Wireless Management	Mobility Controller Public IP Address	10.10.10.5	Address	
5: RF Mobility and Country Code	Mobility Protocol Port	16666		
■ 6: Mobility Configuration	Mobility Switch Peer Group Name	SPG1		
U 7: WLANs	DTLS Mode	Enabled		
8: 802.11 Configuration	Mobility Domain ID for 802.11r	0xac34		
9: Set Time	Mobility Keepalive Interval (1-30)sec	10		
Final : Apply Wizard	Mobility Keepalive Count (3-20)	3		
	Mobility Control Message DSCP Value (0-63)	0		
	Switch Peer Group Members Configured	0		

**Step 43** Enter WLAN ID as 1 and SSID/Profile information as ngwc1-1x

Wizard	WLANs		Previous Next
1: Admin Users     2: SNMP System Summe     3: Port Management     4: Wireless Management     5: RF Mobility and Count	WLAN ID 1 SSID NGWC1-1x Profile Name NGWC1-1x Note: WLAN created will have open	Creating 802.1x WLAN	1
<ul> <li>7: WLANs</li> </ul>			
8: 802.11 Configuration			
9: Set Time			426
Final : Save Wizard			351

Step 44 Enable Radios as shown below and click Next

altalta CISCO Wireless Controller			Save Configuration   Refresh
The Monitor Configu	Ration  Administration 802.11 Configuration	• Help	Previous Net
= 1: Admin Users			<b>†</b>
2: SNMP System Summary	802.11 a/n	C Enabled	/
3: Port Management	802.11 b/g/n	· 🗹 Enabled	
4: Wireless Management			
S: RF Mobility and Country Code			
6: Mobility Configuration			
7: WLANs			
# 8: 802.11 Configuration			
# 9: Set Time			
Final : Save Wizard			

**Step 45** Set time as NTP or Manual

Γ

🚯 Home Monitor 🔻 Config	uration I 🔹 Administra	ston • Help	
Vizard	Set Time		Previous
I: Admin Users			
# 2: SNMP System Summary	Current Time		
B 3: Port Management	Current Time	*12:29:35.792 UTC Mon Apr 1 2013	
# 4: Wireless Management	Mode		
# 5: RF Mobility and Country Code	Mode	Manual v	
6: Mobility Configuration	Date	Manual	
# 7: WLANs	Vest	2013 *	
# 8: 802.11 Configuration	Hear	4012	
# 9: Set Time	Month	April *	
Final : Save Wizard	Dey	1 •	
	Time		
	Hour	12 -	
	Minute	29 *	
	Seconds	35 *	
	Time Zone		

Step 46 Enter NTP server as 10.10.10.1 as an example and click Next

CISCO Wireless Controller	aration I 🔻 Administration	I ▼ Help	Save Configuration   Refresh
Wizard	Set Time		Previous Next
<ul> <li>1: Admin Users</li> <li>2: SNMP System Summary</li> <li>3: Port Management</li> <li>4: Ministry Management</li> </ul>	Current Time	*12:29:35.792 UTC Mon Apr 1 2013	1
<ul> <li>+ Wretess Management</li> <li>5: RF Mobility and Country Code</li> <li>6: Mobility Configuration</li> <li>7: WLANs</li> <li>8: 802.11 Configuration</li> <li>9: Set Time</li> <li>Final : Save Wizard</li> </ul>	Mode NTP Server NTP Server (Hostname/IPv4/IPv6)	NTP v (10.10.10.1	

1

Step 47 At Save Wizard page verify Mobility Configuration, WLAN and Wireless Management configuration for your Network

Wizard	Save Wizard			Previous Apply	
1: Admin Users					
2: SNMP System Summary	Step 1: ADMIN User		Step 6: Mobility Configuration		
3: Port Management			Mobility Mode	Mobility Agent	
4: Wireless Management	User Name	POD1	Mobility Oracle	Disabled	
5: RF Mobility and Country Code			Oracle IP Address	undefined	
6: Mobility Configuration	Step 2: SNMP System Summary		Step 7: WLANs		
7: WLANs	Location	bldg5	WLAN ID	1	
8: 802.11 Configuration	Contact	tme	SSID	NGWC1-1x	
u 9: Set Time	SNMP Logging SNMP Global Trap	Disabled	Prome Name	NGWCI-IX	
■ Final : Save Wizard					
	Step 3: Port Management		Step 8: 802.11 Configuration		
	IP Address Netmask IPv6 Address DHCP DHCP IPv6	2.2.2 255.255.255.0 - 2.2.2.1 -	802.11 a/n 802.11 b/g/n	Enabled Enabled	
	Step 4: Wireless Management		Step 9: Set Time		
	Interface IP Address Netmask IPV6 Address DHCP DHCP IPV6 Step 5: RF Mobility and Country Code	VLAN 10 10.10.10.2 255.255.255.0 - 10.10.10.1 -	Mode Time NTP Server	NTP - 10.10.10.1	
	RF Mobility Country Code	rfdemo			

**Step 48** Apply Changes and verify that all the configurations are successfully applied.



**Note** It will take few seconds for the changes to be applied. Do not multiple click.



Step 49 The below screenshot displays the final success page where you can verify your configuration changes.

ſ

Wizard	Save Wizard				
🛙 1: Admin Users					
2: SNMP System Summary	Step 1: ADMIN User		Step 6: Mobility Configuration		
3: Port Management			Mobility Mode	Mobility Agent	
4: Wireless Management	User Name	POD1	Mobility Oracle	Disabled	
5: RF Mobility and Country Code	Success:	User name configuration applied successfully	Success:	Mobility configurations submitted successfully	
6: Mobility Configuration				······, ·····,	
7: WLANs	Step 2: SNMP System Summary		Step 7: WLANs		
8: 802.11 Configuration	Location	bldg5	WLAN ID SSID	1 NGWC1-1x	
9: Set Time	SNMP Logging	Disabled	Profile Name	NGWC1-1x	
□ Final : Save Wizard	SNMP Global Trap	Disabled	Success:	WLAN configuration applied successfully	
	Success:	SNMP configuration applied successfully	Note: WLAN created will have open authentication and will be in disabled mode.		
	Step 3: Port Management		Step 8: 802.11 Configuration		
	IP Address	2.2.2.2			
	Netmask	255.255.255.0	907 11 -/-	Fachlad	
	DHCP	2.2.2.1	802.11 b/g/n	Enabled	
	DHCP IPv6	-	Success:	802.11 configuration applied successfully	
	Success:	Port Management configuration applied successfully			
	Step 4: Wireless Management		Step 9: Set Time		
	Interface	VLAN10			
	IP Address	10.10.10.2	Mode	NTD	
	IPv6 Address	-	Time	-	
	DHCP	10.10.10.1	NTP Server	10.10.10.1	
	DHCP IPv6	-	Success:	Time Configuration set successfully	
	Success:	Wireless Management configuration applied successfully			
	Step 5: RF Mobility and Country Code				
	RF Mability Country Code	rfdemo US			

### Exercise – Verify New Mobility on MA 3850 and MC 5760

Step 50 Now on Mobility Agent 3850, navigate to Configuration > Controller > Mobility Management

1

1

Home Monitor	Configuration 🖹	Administration	- Help								
reless	Wizard	Radios									
Access Points	Controller ┥	-							Show Quick Filb	er	•
	Wireless Security		Base Radio MAC	Admin State	Operation State	Channel	Power Level	Oean-Air Admi	Clean-Air Oper	Clean-Air Capa	
	Commande			Freddard	11.		70/#1	Easthlad	D	Max	

Step 51 Select Mobility Global Config and verify the Mobility role as Mobility Agent and Mobility Controller IP address as your MC 10.10.10.5

CISCO Wireless Controller	ration   V Administration   V Help		Save Configuration   Refresh
Controller	Mobility Agent Configuration		Apply
<ul> <li>System</li> <li>Internal DHCP Server</li> <li>Management</li> <li>Mobility Management</li> <li>Mobility Global Config</li> <li>Mobility Peer</li> <li>Switch Peer Group</li> </ul>	Mobility Role Mobility Controller IP Address Mobility Controller Public IP Address Mobility Protocol Port Mobility Switch Peer Group Name DTLS Mode Mobility Domain ID for 802.11r Mobility Keepalive Interval (1-30)sec Mobility Keepalive Count (3-20) Mobility Control Message DSCP Value (0-63) Switch Peer Group Members Configured	Mobility Agent       10.10.10.5       10.10.10.5       16666       SPG1       Enabled       0xac34       10       3       0       0       0	

Step 52 Now switch back to you Mobility Controller https://10.10.10.5

ſ

Step 53 Go to Configuration > Controller > Mobility Management > Switch Peer Group and then Click SPG1



Step 54 Check you MA IP Address 10.10.10.2 and verify that control link status and data link status is UP. If link is still showing down then refresh page. It usually takes around a minute for the link to show as Up.

uration    ▼ Administration    ▼ He	Нр			Save Con	figuration   Refresh
Switch Peer Group > SPG1 switch Peer Group > SPG1				Show Quick Filter	
IP Address 10.10.10.2	Public IP Address       10.10.10.2	Control Link Status	Data Link Status		
	vration <ul> <li>Administration</li> <li>He</li> </ul> <ul> <li>Switch Peer Group &gt; SPG1</li> <li>Switch Peer Group &gt; SPG1</li> <li>New Remove</li> <li>IP Address</li> <li>10.10.10.2</li> </ul> <ul> <li>Interview</li> </ul> <ul> <li>Interview</li> <li>Interview</li></ul>	Indiana     Indiana     Switch Peer Group > SPG1     Switch Peer Group > SPG1     New Remove     IP Address     IP Address     ID 10.10.10.2     10.10.10.2	Image: synth stration       Velocity         Switch Peer Group > SPG1         Switch Peer Group > SPG1         New Remove         IP Address       Control Link Status         10.10.10.2       UP         OP MA IP = 10.10.X0.2       Where X = POP Number	Institution       Image: Market Peer Group > SPG1         Switch Peer Group > SPG1         New Remove         Image: Problem Peer Group > SPG1         Image: Pr	Save Con       Initiatization (Initiatization (Initiatio) (Initiation (Initiation (

I

1

#### Step 55 Now go to Monitor > Controller > Mobility > Mobility Statistics



**Step 56** Verify Mobility statistics

ontroller	Mobility Statistics			Clear Stats
System	<ul> <li>Global Mobility Statistics</li> </ul>	<ul> <li>Mobility Agent Statistics</li> </ul>		
Ports	Rx Total 1	Rx Total	0	
Security	Tx Total 1	Rx Errors	o 🛻	
Mobility	Resource Allocation 2	Protocol Rx Errors	0	
Mobility Statistics	Resource Free 2	Protocol Tx Errors	0	
Mobility Oracle Summary	Rx Errors 0	Messages Retransmitted	0	
Management	Tx Errors 0	State Transitions Disallowed	0	
Statistics	Resource Unavailable 0	Total clients	0	
W AP Join		Local clients	0	
CDP	W Malife Control of Control of	Anchored clients	0	
	<ul> <li>Mobility Controller Statistics</li> </ul>	Foriegned clients	0	
		Initiator Statistics		
	KK Emors 0	Handoff Requests Sent	0	
	Protocol Rx Errors 0	Handoff Replies Received	0	
	Protocol Tx Errors 0	Handoff as Local Received	0	
	Messages Retransmitted 0	Handoff as Foreign Received	0	
	Handoff Requests Received 0	Inter-group Handoff Received	0	
	Handoff Completes Received 0	Intra-group Handoff Received	0	
	Client Delete Received 0	Handoff Denys Received	0	
	Handoff Requests Forwarded 0	Anchor Request Sent	0	
	Handoff Completes Forwarded 0	Anchor Deny Received	0	
	Client Delete Forwarded 0	Anchor Grant Received	0	
		Responder Statistics		
		Handoff Requests Received	0	
		Handoff Requests Ignored	0	
		Ping Pong Handoff Requests Dropped	0	

# **Monitoring: Verify AP Registration Example**

In this section, you monitor and verify AP and Client connectivity.

Step 57

Γ

Go to **Monitor > Wireless > Access Points** 

10 Home	Monitor 🗶 Con	guration v Administratio	• Hep	
ontroller	Controller	General		Apply
System Internal DHC Management Mobility Mana	Windess Interferers Rogues Clients	Name AP Multicast Mode Fast SSID change RF group name User idle timeout Temperature Value Temperature Status Dot1x System Auth Cor	POD2-3850-ow Unicast • default 300 28 Degree Celsius GatEN ol	



reless 802.11a/n Radios	
Jonar Deinte	Filter •
W 802.11a/n statistics AP name Base Radio MAC Admin State Operation St Channel Power Level Clean-Air Admi Clean-Ar Opr	Gean-Air Capa

I

1

Click the AP and you can check the radio stats, Channel assignment and RF Parameters

kozes Points W 862.112/n statistics W 862.113/g/n statistics	▼ General Details           Number of Sists         2           AP Name         AP5000           MAC Address         6C-201-56-A6:34:72           Sist ID         0           Radio Type         802.11b/g           Subband Type         All	Load Profile Passed     Raceive Utilization (%) 0     Transmit Utilization (%) 2     Channel Utilization (%) 74
	Coverage Information     Coverage Profile Passed     Interference Profile Failed	Channel Assignment Information     Channel Change Count S     Lat Channel Change Time Tue May 28 54:55:22 2013     Recommended Best Channel 11

# Monitoring: Verify Client Connectivity Example

**Step 59** Connecting a Client to your 802.1x WLAN–Go to **Monitor > Clients** and check that the client is connected.

🚯 Home 🛛 Me	onitor 🛛 🔻	Configuration 🔻 Admini	stration 🔻 Help			
ients	R	Clients				
Client Details					Show Quick Filter	- 5

1100				
Client Details	Cient > Detail			
Uients	<ul> <li>Client Properties</li> </ul>		<ul> <li>AP Properties</li> </ul>	
	Mac Address	64:A3:CB:4C:D6:8C	AP Address	54:78:1A:BF:B1:20
	IPv4 Address	10.10.10.153	AP Name	AP3600
	IPv6 Address	None	АР Туре	802.11n
	User Name	None	Wlan Profile	testbeta
	Port Number	1	Status	Associated
	Interface	VLAN0010	Association ID	1
	Vlan ID	10	802.11 Authentication	Open System
	CCX Version	No CCX support	Reason Code	1
	E2E Version	No E2E support	Status Code	0
	Mobility Role	Local	CF Pollable	Not implemented
	Policy Manager State	RUN	CF Pollable Request	Not implemented
	Management Frame Protection	n Disabled	Short Preamble	Not implemented
	Uptime(sec)	50	PBCC	Not implemented
	Power Save Mode	ON	Channel Agility	Not implemented
	Current TxRateSet	m7	Re-Authentication Timeout	N/A

### Configure Mobility Oracle, Mobility Peer and Verify Statistics on MC 5760 Example

Step 60 Now login back to Mobility Controller 5760 GUI using https://10.10.10.5 and navigate to Configuration > Controller > Mobility Management and enable Mobility Oracle as shown below. Click Apply.

Controller	Mobility Controller Configuration		
▼ System			
U General	Mobility Role	Mobility Controller	
Multicast	Mobility Protocol Port	16666	
Interfaces	Mobility Group Name	default	
> VLAN	Mobility Oracle Enabled	Ø <b>4</b>	
Internal DHCP Server	Mobility Oracle IP Address	0.0.0	
Management	DTLS Mode	Enabled	
<ul> <li>Mobility Management</li> </ul>	Mobility Domain ID for 802.11r	0xac34	
u Mobility Global Config	Mobility Keepalive Interval (1-30)sec	10	
II Mobility Peer	Mobility Keepalive Count (3-20)	3	
Switch Peer Group	Mobility Control Message DSCP Value (0	63) 46	
- smarred drug	Mohility Domain Mamhar Count	1	

ſ



Step 62 Go to Mobility Peer tab and verify that only MC is showing and the link status is shown as UP

CISCO Wireless Controller	Iration   Y Help		Save Co	nfiguration   Refresh
Controller	Mobility Peer			
<ul> <li>System</li> </ul>	New Remove		Show Quick Filter	- 8
<ul> <li>Internal DHCP Server</li> <li>Management</li> <li>Mobility Management</li> <li>Mobility Global Config</li> <li>Mobility Peer</li> <li>Switch Peer Group</li> </ul>	IP Address Public IP	Address Group Name Multic	cast IP Control Link Status Data Link Status 1.0 UP UP UP Mobility Peer POP MG IP = 10.10 X 0.5 Where X = POP NO.	

Step 63 Now navigate to Monitor > Mobility > Mobility Oracle Summary and verify client count is showing as 1.

uluulu CISCO Wireles Controller			0.1		Save Configuration   Refresh
🛕 Home Monitor 🛛 Config	juration 🛛 🔻 Administration 🔍 H	elp Anno 10 mai a anno 10 mai an Anno 10 mai			
Controller	Mobility Oracle Summary				
<ul> <li>System</li> <li>Ports</li> <li>Consults</li> </ul>	Number of Mobility Controllers 1				Show Quick Filter
RADIUS Authentication     RADIUS Accounting     MFP	IP Address	Control Link Status	Client Count	]	=
<ul> <li>▼ Mobility</li> <li>■ Mobility Statistics</li> <li>■ Mobility Oracle Summary</li> </ul>					
<ul> <li>Management</li> <li>Statistics</li> <li>CDP</li> </ul>					

**Step 64** Click on IP address and verify your client details on MO as shown below:

I

Γ

CISCO Wireless Controller	uration i v Administration i v	Help		11	Save Configuration   Refresh
Controller  System Ports Seruity	Mobility Oracle Clients Mobility Oracle Clients > Details	10.10.10.5			
<ul> <li>Security</li> <li>RADIUS Authentication</li> <li>RADIUS Accounting</li> <li>MFP</li> <li>Mobility Statistics</li> <li>Mobility Oracle Summary</li> <li>Management</li> <li>Statistics</li> <li>CDP</li> </ul>	MAC Address OUF4.8916.F988	Anchor MC 10.10.10.5	Foreign MC	Association Time 0 d, 0 h, 1 m, 45 s	

### Managing CT5760/Cat3850 with Cisco Prime Infrastructure 2.0 Example

In this section you will:

- Configure SNMP on CT5760
- Add CT5760/Cat3850 to Cisco Prime Infrastructure.
- Manage basic CT5760/Cat3850 functions on Prime Infrastructure.

Step 65 SNMP strings Configurations - navigate to 5760 Web GUI: Configuration > Controller > Management > Protocol Management > SNMP > Communities



Configure SNMP strings for private and public

1 to 1	iome Monitor	Configuration	Administration 🔻 Help	
Controll	er	SNMP v1/v2c Co SNMP v1/v2c Community	nmunity > New	
<ul> <li>Interna</li> <li>Manag</li> <li>Prot</li> <li>SI</li> </ul>	al DHCP Server ement ocol Managemen	Community Name Access Mode	private Read/Write *	
	General			450
	Communities			351

Repeat the same step for a public Community

Controller	SNMP v1/v2c Community SNMP v1/v2c Community > New	Apply
System	K	
Internal DHCP Server	Community Name public	
* Management	Access Mode	
* Protocol Managemen	Access Hode Read Only +	
* SNMP		
General		5
Communities		

Step 66



Step 67

Navigate to **PI > Operate > Device Work Center.** 



Step 68 Click 'Add Device'.



**Step 69** Enter CT5760 parameters:

I

- a. IP address CT5760 mgt IP
- **b.** Read-Write SNMP string (private)
- c. Telnet credentials
- Username = admin

- User password = admin
- iEnable password = cisco
- HTTP credentials can be IGNORED

🔻 General Parameters		
IP Address	10.10.10.5	
C *DNS Name		
<ul> <li>SNMP Parameters</li> </ul>		
Version	v2c •	
* Retries	2	
* Timeout	10	(secs)
* Community	*****	]
<ul> <li>Telnet/SSH Parameters</li> </ul>		
Protocol	Telnet 🔹	
Timeout	60	(secs)
Username	admin	
Password	••••	]
Confirm Password	••••	]
Enable Password	••••	]
Confirm Enable Password	••••	]

**Step 70** Confirm Prime Infrastructure discovery of the CT5760 – if reachable and successful, the status will show as complete with the correct device type.

1

1

✓ Edit       X Delete       Sync       Groups & Sites <b>Q</b> Add Device             Bulk Import             Perice Varies               Collection Status        Show              All               Add Device               Add Device               Add Device               Add Device               Collection Status               Collection Time               Software Version             Credentia                 Device Name             A             Reachability             Controller             Perice             Reachable             10.10.10.5             Cisco 5760             Wireless             L             Managed             October 4, 2012 1             03.08.26.EMP3             Success              Finite             Au             Au	8	)   Total 1	Selected 0							
Device Name       Reachability       IP Address       Device Type       Collection Status       Collection Time       Software Version       Credentia         Controller       Image: Controler       Image: Controller	*	*	now All	Sł	y Credentials	: 📝 Export Device 🥠 Verif	dd Device 🔹Bulk Import،	Groups & Sites 🔻 👰 A	Sync	lit 🗙 Delete
🗌 Controller 🛛 Reachable 10.10.10.5 Cisco 5760 Wireless L Managed October 4, 2012 1 03.08.26.EMP3 Success	entia	Credentia	Software Version	Collection Time	Collection Status	Device Type	IP Address	Reachability		Device Name
	355	Success	03.08.26.EMP3	October 4, 2012 1	Managed	Cisco 5760 Wireless L	10.10.10.5	🗹 Reachable		Controller
							lcture.	Infrastru		

**Step 72** Explore Cisco Prime Infrastructure GUI in management of CT5760, e.g. client statistics, details, reports etc.

				Vii	rtual Domain ROOT-DOMAI	N   root	· [P.	
cisco Infrastructure	🏠 Home	e Design 🔻	Deploy 🔻 Op	erate 🔻 Report	<ul> <li>Administration</li> </ul>			P 1
Clients and Users Clients Search Results - Reset							Selecte	d 1   Total 1 😵 🕩
roubleshoot 🍐 Test 👻 Disable	Remove 🔊	More 👻 🚋 Tr	ack Clients 🛛 🕁 Identi	y Unknown Users				
MAC Address IP Address	IP Type	User Name	Type Vendor	Device Name	Location	VLAN	Status	Interface
• 74:e1:b6:ba:0e:47 10.10.10.237	IPv4	N/A	🥵 Apple	Controller	Root Area	10	Associated	VLAN0010
Client 74:e1:b6:ba:0e:47 (Refre	shed :2012-Oct-04	, 13:42:01 UTC	-)					No
Client 74:e1:b6:ba:0e:47 (Refree	shed :2012-Oct-04	, 13:42:01 UTC	:)					No
Client 74:e1:b6:ba:0e:47 (Refre Client Attributes General	shed :2012-Oct-04	, 13:42:01 UTC	:) ssion		Securit	y		No

L

Γ

