



**Cisco Support Community** Presents

# Tech-Talk Series

## Cisco Office Extend Access Point OEAP-600

With,

**Sharath K.P.**

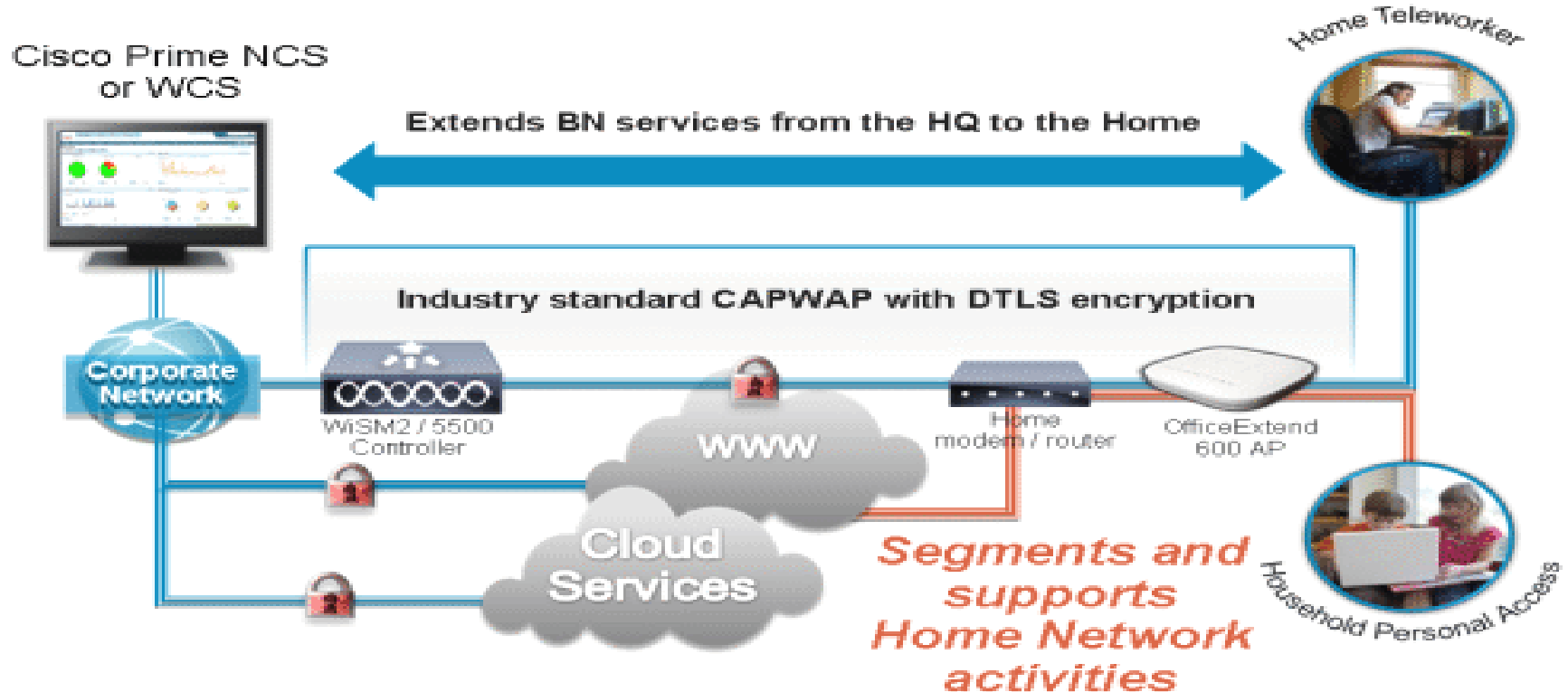
Customer Support Engineer, Cisco TAC

# Session Objectives

Introduction to OEAP  
OEAP -600 Series AP  
Controller Settings  
AP configuration

# OEAP Solution

## How does the Office Extend solution work?



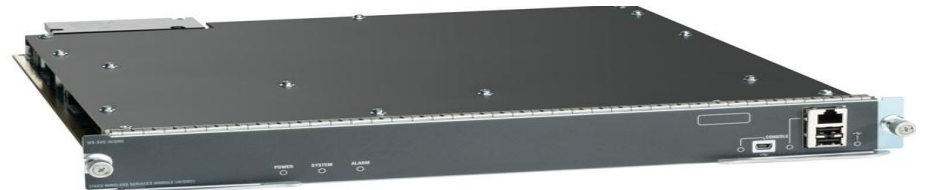
# OEAP Solution

## Cisco OfficeExtend Features and Benefits

Feature	Benefits
<b>Performance</b>	<ul style="list-style-type: none"><li>• Dual-band, 802.11n AP provides at least six times the throughput of existing 802.11a/g networks.</li><li>• Supports 2.4-GHz &amp; 5-GHz radio, avoid congestion</li></ul>
<b>Simplified Operations and Management</b>	<ul style="list-style-type: none"><li>• Extends corporate services to remote workers w/o local configuration.</li><li>• Same management as that of the HQ WLAN.</li><li>• User plugs 600 OEAP into home router – zero touch.</li></ul>
<b>Robust Security</b>	<ul style="list-style-type: none"><li>• Secure (DTLS) connection between the OEAP &amp; corporate WLC to offer remote WLAN connectivity using the same security profile as at the corporate office.</li><li>• Segmentation of home &amp; corporate traffic nullifies security risks to corporate assets.</li></ul>
<b>End-to-end Voice Services</b>	<ul style="list-style-type: none"><li>• Supports UC for improved collaboration.</li><li>• Supports all Cisco unified Wireless IP Phones (cost-effective real-time voice services)</li><li>• No need to user cellular phone to place calls.</li></ul>

# 600 Series AP

- Dual band 802.11n AP for the homes .
- Supported by **5508**, **WiSM2**, **2500** series WLC's .
- Supported from **7.0.116** onwards .
- The controller's Management Interfaces need to be on a routable IP network.





▲ [Up to Discussions in Other Wireless - Mobility Subjects](#)

## Discussions

This Question is **Answered**

225 Views 2 Replies Latest reply: Sep 12, 2011 9:33 PM by George Stefanick



**Rafael Jimenez** 291 posts since Feb 12, 2007  
**Cisco Partner**

Sep 12, 2011 9:05 PM

## OfficeExtend and WLC

Whats it "OfficeExtend support" in the 5500 WLC datasheet?  
I dont see nothing about this in the WLC configuration guide release v7.0.116.0..

Is this the same as OEAP?.

Is the OfficeExtended (or OEAP) supported on the 1140 APs?. If so where can I get a guide to configure this?.

Thanks.

**Correct Answer** by George Stefanick on 12 Sep, 2011 9:14 PM

### Actions

- Edit discussion
- Lock discussion
- Move discussion
- Delete discussion
- Receive email notifications
- Send as email
- Report abuse
- Convert discussion to document
- View as PDF
- View print preview
- Add to featured content
- Bookmark this

Announcing  
the First



## ^ Up to Discussions in Getting Started with Wireless

### Discussions

This Question is **Answered**

184 Views 2 Replies Latest reply: Mar 31, 2011 8:01 AM by Leo Laohoo



**Jason Jones** 19 posts since Jan 16, 2007  
**Cisco Partner**

Mar 30, 2011 9:13 PM

## 4400 and 5508

I have a 4402 and a 5508 both running v7 code, are the controllers compatible if used as primary and secondary?.

Thanks,

Jason

**Correct Answer** by Stephen Rodriguez on 30 Mar, 2011 10:01 PM



Yes, running the same code they are compatible, depending on what features you are using.

For example CEAP is not supported on the 5508 as any CEAP would not support the 4400...

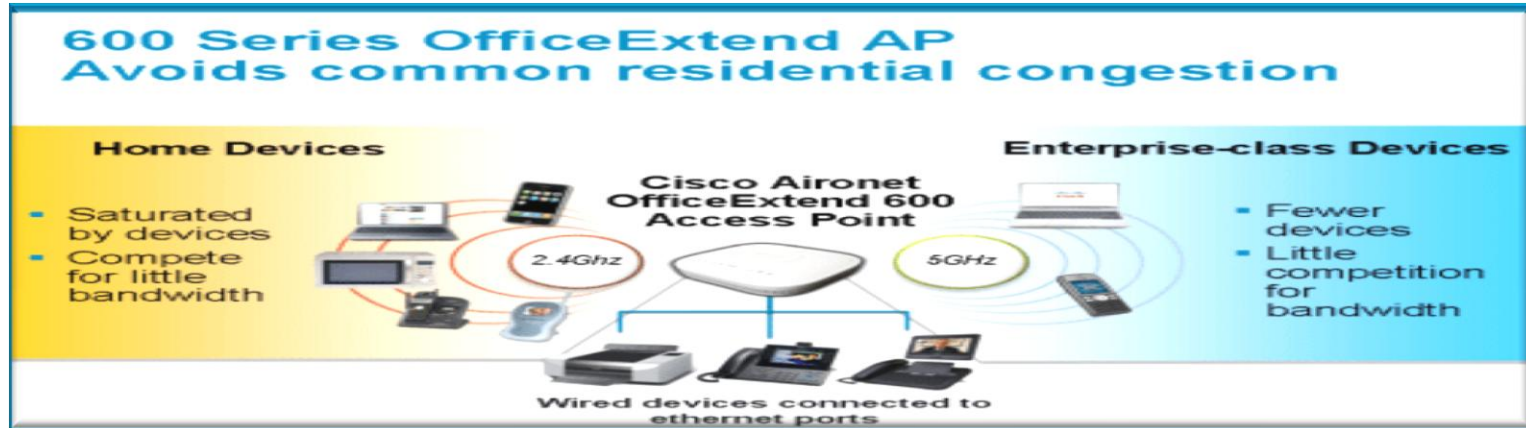
### Actions

- Edit discussion
- Lock discussion
- Move discussion
- Delete discussion
- Receive email notifications
- Send as email
- Report abuse
- Convert discussion to document
- View as PDF
- View print preview
- Add to featured content
- Bookmark this

### Announcing the First

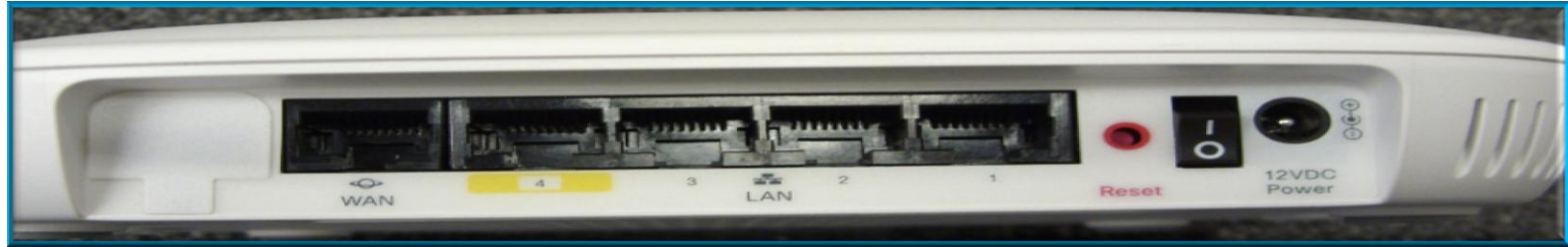
# Functionality

- Corporate access to employee over centrally configured SSID
  - ✓ Supports *up to 2 corporate SSIDs*
  - ✓ Supports *up to 4 wired corporate devices*
- Family Internet access over a locally configured SSID
- Supports up to 15 wireless clients





# Mechanicals – OEAP 600



# Installing the Office Extend Solution

## STEPS

User is given an AP 'primed' with the IP addresses & name of the controllers with public IP addresses

The user plugs the AP into their home router

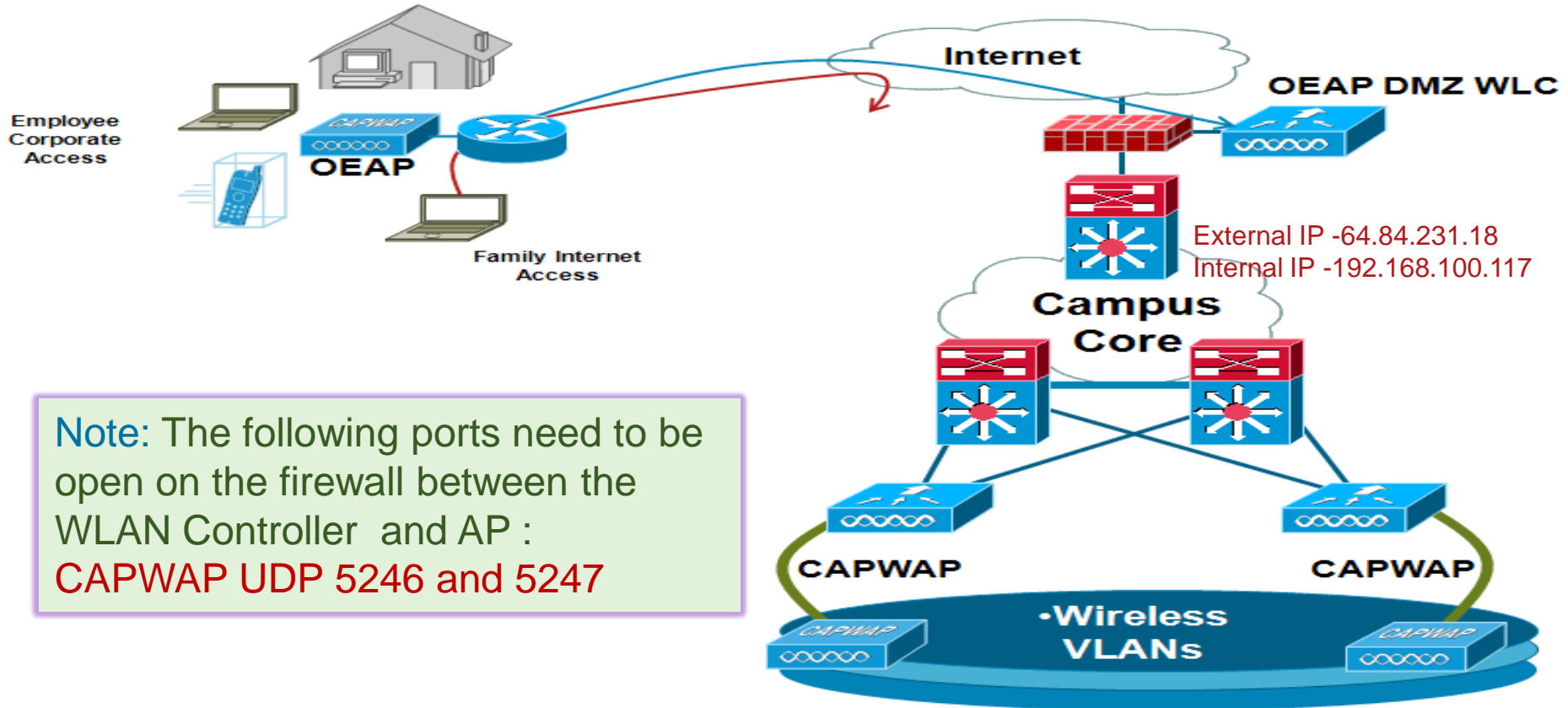
The AP gets an IP address from their home router, joins the primed controller and creates a secured tunnel

The AP advertises corporate SSID

The same security methods & services are thereby extended across the WAN to the user's home

The user can add his/her own local SSID

# OEAP controller in DMZ



Note: The following ports need to be open on the firewall between the WLAN Controller and AP :  
**CAPWAP UDP 5246 and 5247**

## ^ Up to Discussions in Security and Network Management

### Discussions

This Question is **Answered**

409 Views 13 Replies Latest reply: Dec 20, 2011 10:59 PM by Network Pro

share Tweet



**Network Pro** 235 posts since Mar 23, 2011  
Guest User

Dec 16, 2011 4:13 PM

## Officeextend suggestion?

Hi,

I have attached a diagram of the current topology. At present, we have two 5508 connected to our core. We also have a 4402 behind the firewall (DMZ) just purely for guest access. So the staff users connect to the access point which in turns connects to the Staff WLC 1 (if this fails then to Staff WLC2). any guest user connect to the access point which in turn connects to Staff WLC which anchors to Guest WLC which then provides access. Since the guest is behind the DMZ they can only access the internet and not out internal network.

Now we want to officeextend our network - we want our users to use 1132 AP's at home to access the Infrastructure. is there a way we can do this without disturbing the existing infrastructure.

On reading cisco website, i know the best practice is to use 2 5508 (one behind the firwall and the other anchored to this access the internet network ) i thought since we have a Cisco (dmz) switch (48 port) and only the 4402 (Guest WLC) is connected to it, maybe purchase another 5508 WLC and connect to the 48 port cisco (dmz) switch. will this work ?

### Actions

- Edit discussion
- Lock discussion
- Move discussion
- Delete discussion
- Receive email notifications
- Send as email
- Report abuse
- Convert discussion to document
- View as PDF
- View print preview
- Add to featured content
- Bookmark this

Announcing  
the First

Community  
**SPOTLIGHT**

# Controller setting – Enabling NAT

The screenshot shows the Cisco Controller configuration interface for the 'management' interface. The 'Enable NAT Address' checkbox is checked and circled in red. The NAT IP Address is set to 128.107.234.14. Other configuration details include the interface name 'management', MAC address '00:24:97:69:52:8f', and various address and physical settings.

General Information	
Interface Name	management
MAC Address	00:24:97:69:52:8f

Configuration	
Quarantine	<input type="checkbox"/>
Quarantine Vlan Id	0

NAT Address	
Enable NAT Address	<input checked="" type="checkbox"/>
NAT IP Address	128.107.234.14

Interface Address	
VLAN Identifier	0
IP Address	172.16.1.25
Netmask	255.255.255.0
Gateway	172.16.1.2

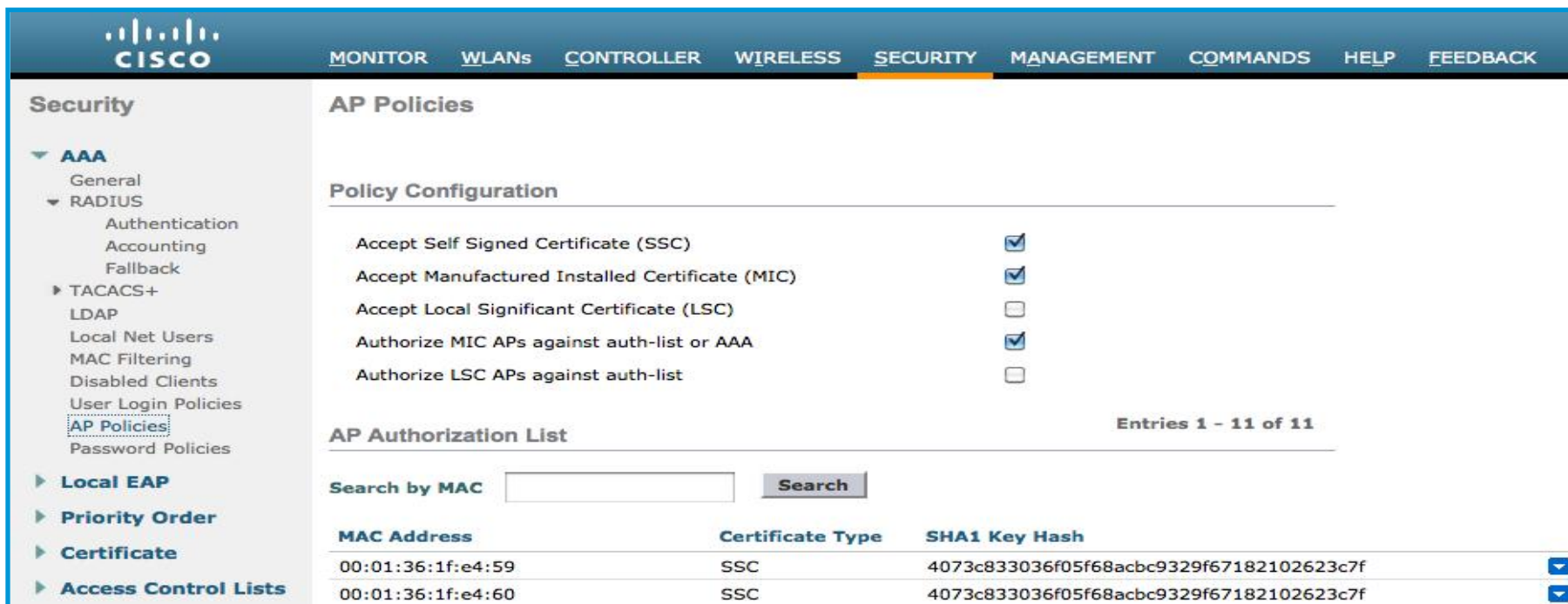
Physical Information	
The interface is attached to a LAG.	
Enable Dynamic AP Management	<input checked="" type="checkbox"/>

DHCP Information	
Primary DHCP Server	172.20.225.153
Secondary DHCP Server	0.0.0.0

# Controller – Adding MAC address of OEAP

- Add the MAC address of the OEAP 600 to the controller

**Note:** MAC filtering is ON by default



The screenshot shows the Cisco Controller's Security configuration page for AP Policies. The left sidebar contains a navigation menu with options like AAA, Local EAP, Priority Order, Certificate, and Access Control Lists. The main content area is titled 'AP Policies' and includes a 'Policy Configuration' section with several settings, each with a checkbox. Below this is an 'AP Authorization List' section with a search bar and a table of entries.

**Security**

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

**AP Policies**

**Policy Configuration**

- Accept Self Signed Certificate (SSC)
- Accept Manufactured Installed Certificate (MIC)
- Accept Local Significant Certificate (LSC)
- Authorize MIC APs against auth-list or AAA
- Authorize LSC APs against auth-list

**AP Authorization List** Entries 1 - 11 of 11

Search by MAC

MAC Address	Certificate Type	SHA1 Key Hash	
00:01:36:1f:e4:59	SSC	4073c833036f05f68acbc9329f67182102623c7f	<input checked="" type="checkbox"/>
00:01:36:1f:e4:60	SSC	4073c833036f05f68acbc9329f67182102623c7f	<input checked="" type="checkbox"/>

# How to enable the Office Extend AP

## Configuring the controller for the AP-1130 & AP-1140 Series

Configure the AP1130 /1140 in the HREAP mode

Enable OEAP option for the HREAP AP

All APs > Details for AP1140-2

**General** | Credentials | Interfaces | High Availability

**General**

AP Name	AP1140-2
Location	default location
AP MAC Address	00:22:90:90:ac:0f
Base Radio MAC	00:22:90:96:6a:10
Status	Enable
AP Mode	H-REAP

All APs > Details for AP1140-2

**General** | Credentials | Interfaces | High Availability

VLAN Support

Native VLAN ID  **VLAN Mappings**

HREAP Group Name Not Configured

**OfficeExtend AP**

Enable OfficeExtend AP

- Data Encryption is enabled automatically once we enable OEAP on an AP

# Office Extend AP

Wireless

- Access Points
  - All APs
  - Radios
    - 802.11a/n
    - 802.11b/g/n
  - Global Configuration
- Advanced
- Mesh
- HREAP Groups
- 802.11a/n
- 802.11b/g/n
- Media Stream
- Country
- Timers
- QoS

All APs > Details for Sujit-TME-Evora

General Interfaces High Availability Inventory Advanced

General

AP Name	Sujit-TME-Evora
Location	default location
AP MAC Address	c0:c1:c0:05:4a:2a
Base Radio MAC	00:22:bd:da:bd:80
Admin Status	Enable
AP Mode	local
AP Sub Mode	None
Operational Status	REG
Port Number	13

Versions

Primary Software Version	7.0.114.9
Backup Software Version	0.0.0.0
Boot Version	5.10.144.0
Mini IOS Version	7.0.112.34

IP Config

IP Address	192.168.0.5
------------	-------------

Time Statistics

UP Time	1 d, 17 h 33 m 38 s
Controller Associated Time	1 d, 17 h 32 m 04 s
Controller Association Latency	0 d, 00 h 01 m 33 s

All APs > Details for Sujit-TME-Evora

General Interfaces High Availability Inventory Advanced

	Name	Management IP Address
Primary Controller	Alpha Controller	171.70.35.131

**The OEAP-600 will connect to the WLC as a Local Mode Access Point.**



# REMOTE LAN

- Remote LAN is the network that is defined and ends being mapped as the “wired port #4” of the OEAP-600
- This is where that LAN is configured / enabled.

The screenshot displays the Cisco WLAN configuration interface. The main table lists three WLANs, with the third one, 'Remote LAN', highlighted by a red box. A 'WLANs > New' dialog box is open, showing the configuration for a new WLAN. The dialog box has a 'Type' dropdown set to 'WLAN', a 'Profile Name' field containing 'WLAN', an 'SSID' field containing 'Remote LAN', and an 'ID' dropdown set to '4'. The 'Create New' button is visible.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	Alpha	alpha	Enabled	[WPA + WPA2][Auth(802.1X)]
2	WLAN	AlphaPhone	alpha_phone	Enabled	[WPA + WPA2][Auth(802.1X)]
3	Remote LAN	Remote LAN	---	Enabled	None

# Configuring the controller

## Configuring the controller for the OEAP-600 Series

The 600 Series Supports at most two WLANs and one Remote LAN.



The screenshot shows the Cisco Controller configuration page for WLANs. The page title is "WLANs" and it displays a table of configured WLANs. The table has columns for WLAN ID, Type, Profile Name, WLAN SSID, Admin Status, and Security Policies. There are three entries: 1 (WLAN, EvoraData), 2 (WLAN, EvoraVoice), and 3 (Remote LAN, EthernetTunnel).

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	EvoraData	EvoraData	Enabled	[WPA2][Auth(802.1X)]
2	WLAN	EvoraVoice	Evora_Voice	Enabled	[WPA2][Auth(802.1X)]
3	Remote LAN	EthernetTunnel	---	Enabled	None

This means that the 600 OEAP needs to be placed into an AP-Group if there are more than two WLANs or more than one Remote LANs configured on the Controller.



The screenshot shows the Cisco Controller configuration page for AP Groups. The page title is "AP Groups" and it displays a table of configured AP Groups. The table has columns for AP Group Name and AP Group Description. There are two entries: EvoraOEAP (Group for EvoraOEAPs) and default-group.

AP Group Name	AP Group Description
EvoraOEAP	Group for EvoraOEAPs
default-group	

# Controller - WLANS

- Configure WLAN SSID profile and security for the OEAP 600
- Configure WLAN type as “Remote LAN” for wired port authentication in OEAP 600
- Only WLAN with ID 1-2 is automatically pushed to OEAP 600
- WLAN with ID 1 and 3 for example needs AP Group configuration

The screenshot displays the Cisco Controller's WLANS configuration interface. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WLANS' section is active, showing a 'Current Filter: None' and a 'Create New' button. Below this is a table of WLAN configurations:

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	Alpha	alpha	Enabled	[WPA + WPA2][Auth(802.1X)]
2	WLAN	AlphaPhone	alpha_phone	Enabled	[WPA + WPA2][Auth(802.1X)]
3	Remote LAN	Remote LAN	---	Enabled	None

# Configuring the controller

## Configuring the controller for the OEAP-600 Series

If the 600 series is entered into an AP Group, the same limits of two WLANs and one Remote LAN still applies for the configuration of the AP Group:

WLANs

- ▼ WLANs  
WLANs
- ▼ Advanced  
AP Groups

Ap Groups > Edit 'EvoraOEAP'

General | **WLANs** | APs

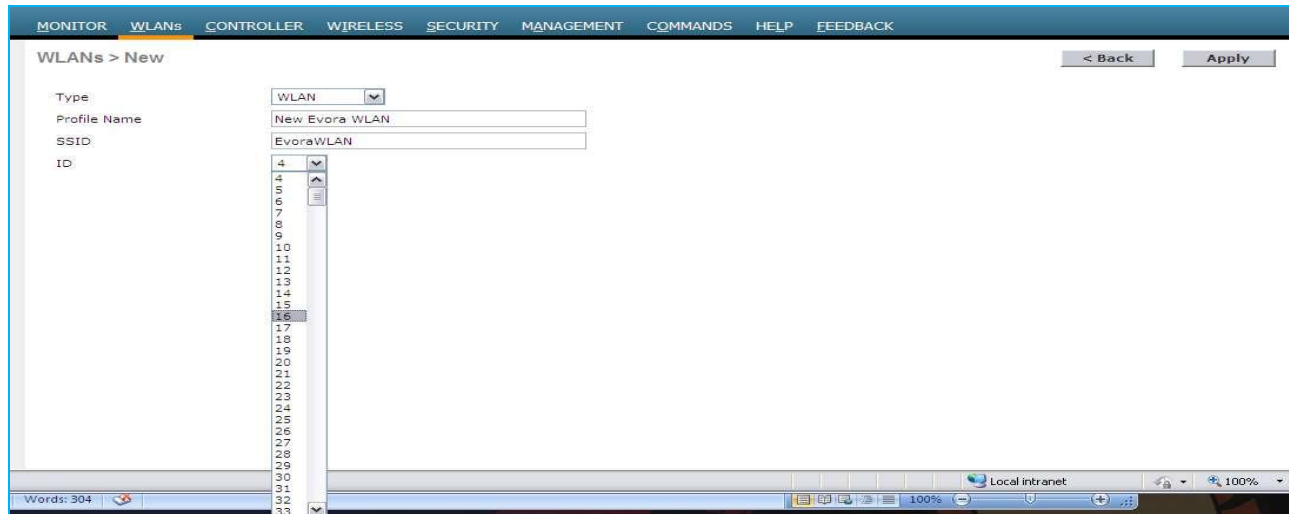
Add New

WLAN ID	WLAN SSID	Interface/Interface Group(G)	SNMP NAC State	
1	EvoraData	management	Disabled	<input checked="" type="checkbox"/>
2	Evora_Voice	management	Disabled	<input checked="" type="checkbox"/>
3	EthernetTunnel	management	Disabled	<input checked="" type="checkbox"/>

# Configuring the controller

## Configuring the controller for the OEAP-600 Series

- If the 600 OEAP is in the default-group, which means it is not in a defined AP-Group, the WLAN/Remote LAN IDs need to be set *as less than ID 8*. (note this may change).
- If additional WLANs or Remote-LANs are created with the intent of changing the WLANs or Remote-LAN being used by the 600 Series OEAP; disable the current WLANs or Remote-LAN that you are removing *before enabling* the new WLANs or Remote-LAN on the 600 Series.



# Configuring the controller

## WLAN security settings for the 600 series

When setting the security setting in the WLAN, there are specific elements that are not supported on the 600 series.

CCX is not supported on the 600 OEAP; elements related to CCX therefore are not supported.

**Note:** In the security do not select CCKM in WPA + WPA2 settings, only 802.1x or PSK should be selected.

**Note:** Security encryption settings need to be identical for WPA & WPA2 for TKIP and AES:



# Configuring the controller

## WLAN security settings for the 600 series

### Examples of incompatible settings for TKIP and AES:

WLANs > Edit

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security <sup>6</sup> WPA+WPA2  802.1X Filtering

**WPA+WPA2 Parameters**

WPA Policy	<input checked="" type="checkbox"/>		
WPA Encryption	<input type="checkbox"/> AES	<input checked="" type="checkbox"/> TKIP	
WPA2 Policy	<input checked="" type="checkbox"/>		
WPA2 Encryption	<input checked="" type="checkbox"/> AES	<input type="checkbox"/> TKIP	
Auth Key Mgmt			802.1X <input type="button" value="v"/>

WLANs > Edit

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security <sup>6</sup> WPA+WPA2  802.1X Filtering

**WPA+WPA2 Parameters**

WPA Policy	<input checked="" type="checkbox"/>		
WPA Encryption	<input type="checkbox"/> AES	<input checked="" type="checkbox"/> TKIP	
WPA2 Policy	<input checked="" type="checkbox"/>		
WPA2 Encryption	<input checked="" type="checkbox"/> AES	<input checked="" type="checkbox"/> TKIP	
Auth Key Mgmt			802.1X <input type="button" value="v"/>

[^ Up to Discussions in Other Wireless - Mobility Subjects](#)

## Discussions

This Question is **Answered**

235 Views 4 Replies Latest reply: Jan 30, 2012 8:54 PM by Vinay Sharma

**Hubert Kupper** 21 posts since Jan 18, 2011  
Cisco Customer

Dec 15, 2011 10:05 PM

## oep 600 can't connect to corporate SSIDs

Hi all,

I have setup an oep 600 and it joins the primary controller 5508. The corporate SSIDs are showed in the wlan client but the client cannot connect to the SSID.

The event\_log from the oep shows:

```
*Dec 15 16:14:30.807:
ADD_MOBILE from WLC,wmeEnabled=1,encrptPolicy=1

*Dec 15 16:14:30.807: ADD_MOBILE: client "client MAC", slot=0,vapid=1

*Dec 15 16:14:30.808: received assoc-rsp for wireless client, status=0000

*Dec 15 16:14:35.761: received de-auth for client "client MAC"
```

### Actions

- Edit discussion
- Lock discussion
- Move discussion
- Delete discussion
- Stop email notifications
- Send as email
- Report abuse
- Convert discussion to document
- View as PDF
- View print preview
- Add to featured content
- Bookmark this





# Configuring the controller

## WLAN security settings for the 600 series

### Examples of compatible settings:

WLANs > Edit

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security [e](#) WPA+WPA2  10MAC Filtering

**WPA+WPA2 Parameters**

WPA Policy	<input checked="" type="checkbox"/>	
WPA Encryption	<input checked="" type="checkbox"/> AES	<input checked="" type="checkbox"/> TKIP
WPA2 Policy	<input checked="" type="checkbox"/>	
WPA2 Encryption	<input checked="" type="checkbox"/> AES	<input checked="" type="checkbox"/> TKIP
Auth Key Mgmt		802.1X <input type="button" value="v"/>

WLANs > Edit

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security [e](#) WPA+WPA2  10MAC Filtering

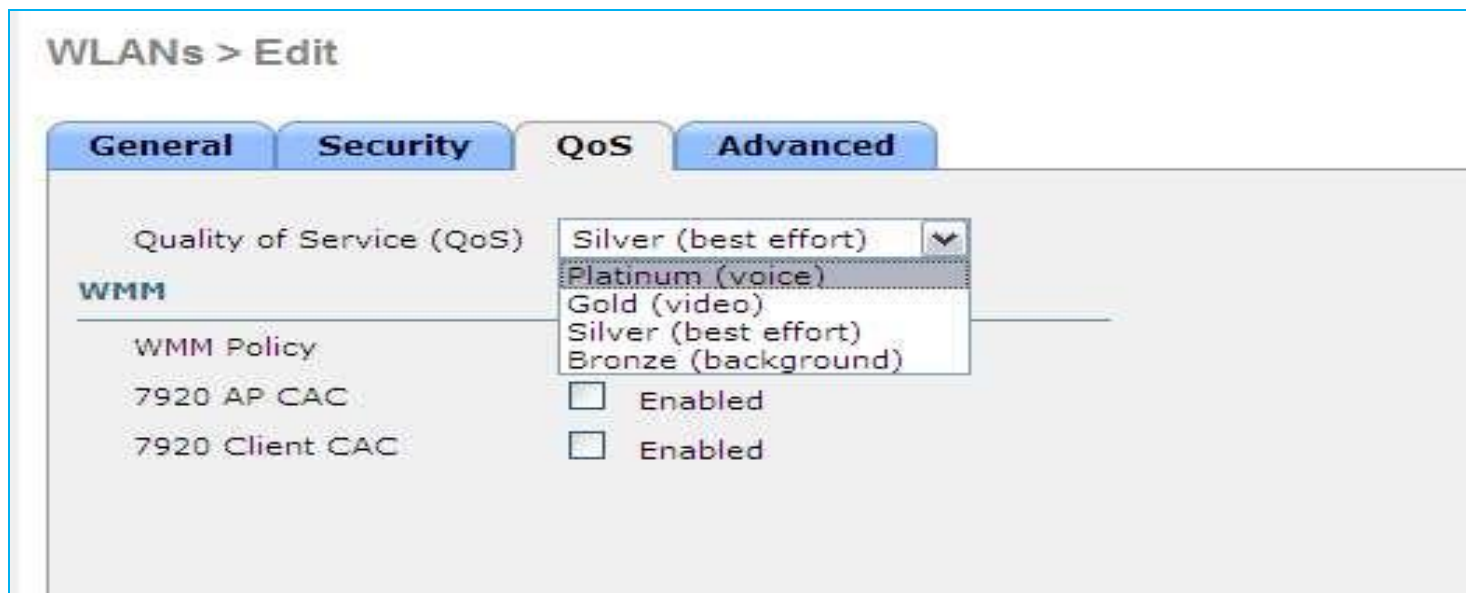
**WPA+WPA2 Parameters**

WPA Policy	<input checked="" type="checkbox"/>	
WPA Encryption	<input checked="" type="checkbox"/> AES	<input type="checkbox"/> TKIP
WPA2 Policy	<input checked="" type="checkbox"/>	
WPA2 Encryption	<input checked="" type="checkbox"/> AES	<input type="checkbox"/> TKIP
Auth Key Mgmt		802.1X <input type="button" value="v"/>

# Configuring the controller

## QoS settings

QoS settings are supported, but CAC is not and should not be enabled



The screenshot shows the 'WLANs > Edit' configuration page. The 'QoS' tab is selected, and a dropdown menu is open for 'Quality of Service (QoS)'. The dropdown lists five options: Silver (best effort), Platinum (voice), Gold (video), Silver (best effort), and Bronze (background). Below the dropdown, the 'WMM' section is visible, with 'WMM Policy' set to '7920 AP CAC' and '7920 Client CAC'. Both '7920 AP CAC' and '7920 Client CAC' have checkboxes for 'Enabled', which are currently unchecked.

WLANs > Edit

General Security QoS Advanced

Quality of Service (QoS) Silver (best effort) ▼

Platinum (voice)

Gold (video)

Silver (best effort)

Bronze (background)

WMM

WMM Policy

7920 AP CAC  Enabled

7920 Client CAC  Enabled

# Configuring the controller

Advanced settings should also be managed

- Coverage Hole Detection should **not** be enabled
- Aironet IE should **not** be enabled
- MFP is also **not** supported, & should be disabled or optional
- Client Load Balancing & Client Band Select are **not** supported

The screenshot displays the 'WLANs > Edit' configuration page. The 'Advanced' tab is selected, showing various settings. Red circles highlight the 'Coverage Hole Detection' checkbox (which is checked), the 'Aironet IE' checkbox (which is checked), and the 'MFP Client Protection' dropdown menu (which is set to 'Optional'). A separate box below the main configuration shows the 'Load Balancing and Band Select' settings, with both 'Client Load Balancing' and 'Client Band Select' checkboxes unchecked.

Setting	Value
Allow AAA Override	<input type="checkbox"/> Enabled
Coverage Hole Detection	<input checked="" type="checkbox"/> Enabled
Enable Session Timeout	<input type="checkbox"/> Enabled
Aironet IE	<input checked="" type="checkbox"/> Enabled
Diagnostic Channel	<input type="checkbox"/> Enabled
IPv6 Enable Z	<input type="checkbox"/> Enabled
Override Interface ACL	None
P2P Blocking Action	Disabled
Client Exclusion	<input type="checkbox"/> Enabled
Maximum Allowed Clients	0
DHCP Server	<input type="checkbox"/> Override
DHCP Addr. Assignment	<input type="checkbox"/> Required
Management Frame Protection (MFP)	
MFP Client Protection	Optional
DTIM Period (in beacon interval)	
802.11a/n (1 - 255)	1
802.11b/g/n (1 - 255)	1
Client Load Balancing	<input type="checkbox"/>
Client Band Select	<input type="checkbox"/>

# Configuring the controller

## Authentication settings

- For authentication on the 600 series, **LEAP is not supported**. This configuration needs to be addressed on the clients and radius servers to migrate them to EAP-Fast, EAP-TTLS, EAP-TLS, or PEAP.
- If Local EAP is being utilized on the controller then the settings would also have to be modified not to utilize LEAP:



The screenshot shows the Cisco Controller's Security configuration page. The left sidebar is expanded to 'Local EAP' > 'Profiles'. The main content area displays a table of Local EAP Profiles. The table has columns for Profile Name, LEAP, EAP-FAST, EAP-TLS, PEAP, and an action menu. One profile named 'EvoraLocal' is listed with LEAP disabled and EAP-FAST, EAP-TLS, and PEAP enabled.

Profile Name	LEAP	EAP-FAST	EAP-TLS	PEAP	
<a href="#">EvoraLocal</a>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="v"/>

# Configuring the controller

## Remote LAN settings

- Only four clients are able to connect through the Remote LAN port on the 600 series.
- The Remote LAN client limit supports connecting a switch or hub to the Remote LAN port for multiple devices or connecting directly to a Cisco IP phone that is connected to that port.
- Remote LAN is configured in the same fashion that a WLAN and Guest LAN is configured on the controller:



The screenshot shows the 'WLANs > New' configuration page. The 'Type' dropdown menu is open, showing options: WLAN, Guest LAN, WLAN (highlighted), and Remote LAN. The 'Profile Name' and 'SSID' fields are empty. The 'ID' field is set to 4.

Type	WLAN
Profile Name	
SSID	
ID	4



Up to Discussions in Other Wireless - Mobility Subjects

## Discussions

This Question is **Answered**

952 Views 21 Replies Latest reply: Aug 31, 2011 1:41 AM by George Stefanick



**Tito Luna** 175 posts since Apr 28, 2009  
Cisco Customer

Aug 30, 2011 2:22 AM

## WLC 5508 Office extend - remote LAN

I'm confused as to how to setup the remote LAN portion of the office extend solution. Do I need to set up this remote LAN with a local interface and have it talk to the controller's internal DHCP server? Or can I set up this remote LAN and anchor it off to my internal controllers?

Thanks

**Correct Answer** by George Stefanick on 31 Aug, 2011 1:41 AM



For others who may be using this thread in the future. The issue after everything was configured was related to a bug:

You need to make sure you enable a mandatory data rate in 1,2,5.5 or 11 and NOT in the OFDM.

## Actions

- Edit discussion
- Lock discussion
- Move discussion
- Delete discussion
- Receive email notifications
- Send as email
- Report abuse
- Convert discussion to document
- View as PDF
- View print preview
- Add to featured content
- Bookmark this



# Configuring the controller

## Channel management settings

- The radios for the 600 series are controlled through the Local GUI on the 600 series & not through the Wireless LAN Controller.
- For the reasons stated above, RRM is not supported on the 600 series.

The screenshot shows the configuration page for a Cisco Office Extended Access Point. The 'Radio' section is expanded, and the 'Channel Selection' dropdown menu is highlighted with a red circle. The selected option is 'Auto'.

System	SSID	DHCP
<b>Login</b>		
Username	admin	
Password	•••••	
<b>Radio</b>		
Radio Interface	(2.4 GHz)	
Status	Enabled	
Channel Selection	Auto	
802.11 n-mode	Enabled	
Bandwidth	20 MHz	

The screenshot shows the configuration page for a Cisco Office Extended Access Point. The 'Radio' section is expanded, and the 'Channel Selection' dropdown menu is highlighted with a red circle. The selected option is 'Auto'.

System	SSID	DHCP
<b>Login</b>		
Username	admin	
Password	•••••	
<b>Radio</b>		
Radio Interface	(5 GHz)	
Status	Enabled	
Channel Selection	Auto	
802.11 n-mode	Enabled	
Bandwidth	40MHz	

# Local SSID on Office Extend AP

- Browse to local IP address of the OEAP to add the local SSID on the OEAP
- The local SSID will switch traffic locally and is useful for a home WLAN

The image shows a web browser window with the address bar containing `http://172.20.225.165/`. The main content area displays the Cisco Office Extend Access Point login page, which includes the Cisco logo, the text "Office Extend Access Point", and an "Enter" button. A Windows Security dialog box is overlaid on the page, displaying a warning: "The server 10.0.0.1 at Cisco Office Extend AP requires a username and password. Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection)." The dialog box contains two input fields, both containing the text "admin", and a checkbox labeled "Remember my credentials". The dialog box has "OK" and "Cancel" buttons at the bottom.



# Local Homepage of the Office Extend AP

| Refresh | Close Window



HOME CONFIGURATION EVENT LOG HELP

## Home: Summary

### General Information

AP Name	AP1	AP MAC Address	0022.9090.8f4e
AP IP Address	209.185.200.225	AP Uptime	1 day, 19 hours, 17 minutes
AP Mode	Remote	AP Status (Admin/Operational)	ADMIN_ENABLED/UP
AP Version	12.4(20090119:051918)	Software Version	6.0.75.0
Controller Name	5500		

### AP Statistics

Radio	Freq/Channel	Tx Power	Pkts In/Out	Bytes In/Out
Radio0-802.11N <sup>2.4</sup> GHz	2437 MHz/6	-20 dBm	459874/50945734	223261/206709119
Radio1-802.11N <sup>5</sup> GHz	5320 MHz/64	-17 dBm	386601/37115856	630268/511013585

### Association

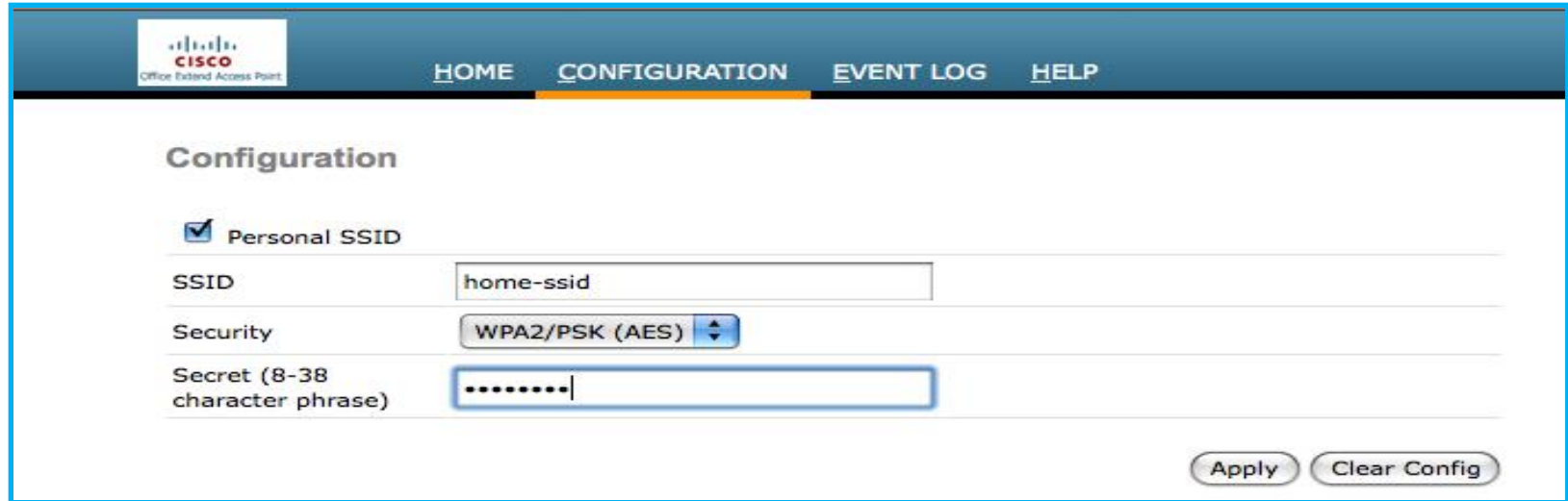


To remove 'Local Wireless Connection' association or modify settings, click on [Configuration](#).

Client MAC	Client IP/Name	Pkts In/Out	Bytes In/Out	Duplicates Rcvd/Data Retries	Decrypt Failed/RTS Retries
001c.58cd.3e13	0.0.0.0/NONE	1142/916	79751/52378	0/2	0/0

# Adding Local SSID on Office Extend AP

- Local SSID for personal use using Open, WPA or WPA2/PSK or 104 bit WEP key



The screenshot displays the configuration page for a Cisco Office Extend Access Point. The interface includes a navigation bar with 'HOME', 'CONFIGURATION', 'EVENT LOG', and 'HELP'. The 'CONFIGURATION' section is active, showing the 'Configuration' page. A checkbox for 'Personal SSID' is checked. Below this, there are three input fields: 'SSID' with the value 'home-ssid', 'Security' with a dropdown menu set to 'WPA2/PSK (AES)', and 'Secret (8-38 character phrase)' with a masked password field. At the bottom right, there are 'Apply' and 'Clear Config' buttons.

Field	Value
Personal SSID	<input checked="" type="checkbox"/>
SSID	home-ssid
Security	WPA2/PSK (AES)
Secret (8-38 character phrase)	.....



# Q&A

Thank you.

