Configuration Note

Configuration of Cisco Autonomous Access Point with 802.1x Authentication for Avaya 3631 Wireless Telephone

Product Summary

Manufacturer: Cisco Systems: www.cisco.com
Access Point: Cisco Aironet 1130AG Series Access Point
Model: AIR-LAP1131AG-A-K9 Software version: 12.3(7) JA5
Radio: 2.4 and 5 GHz
Security: 802.1x

Assigning an IP address to a new AP

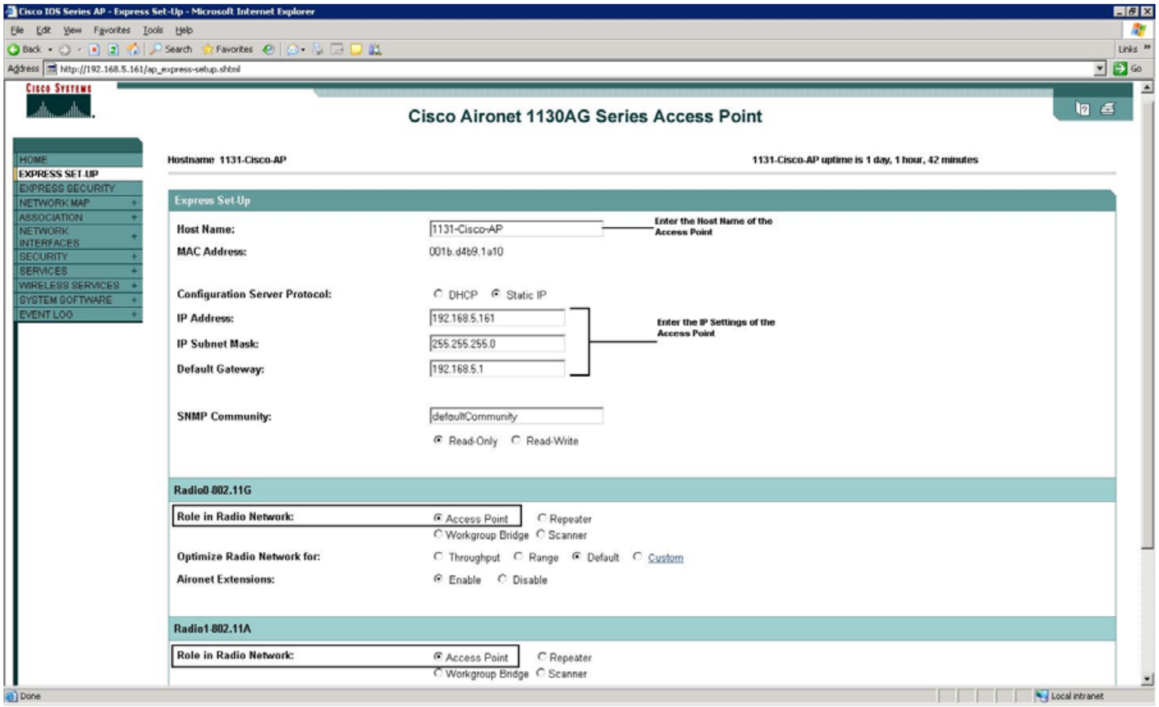
It is sometimes more convenient to assign an IP address to the access point using the command line interface (CLI). The steps are described below:

1. Connect the PC's serial port to the AP via the CLI cable. Open a terminal program, such as HyperTerminal. Configure the settings to 9600 baud, 8 data bits, no parity.
2. At the prompt, type **enable**.
3. Type in the password; default password is **Cisco**.
4. Type in the command **configure terminal**.
5. Type in the command **interface BVI 1**.
6. Type **ip address** **<**ip address**>** **<**net mask**>.**
7. Type **end** and then **write mem** to save configuration.

The rest of the configuration can easily be done through the browser interface.
Log into the AP via a Web browser, using the IP addresses assigned in the above step.

Connecting to the AP

Connect to the AP via Netscape or Internet Explorer by entering the URL: http://<IP_Addr> (where <IP_Addr> is the IP address of the AP).



Address: http://192.168.5.161/ap_express-setup.shtml

Cisco Aironet 1130AG Series Access Point

Hostname 1131-Cisco-AP

1131-Cisco-AP uptime is 1 day, 1 hour, 42 minutes

Express Set-Up

Host Name: 1131-Cisco-AP

MAC Address: 001b.d4b9.1a10

Configuration Server Protocol: ○ DHCP ● Static IP

IP Address: 192.168.5.161

IP Subnet Mask: 255.255.255.0

Default Gateway: 192.168.5.1

SNMP Community: defaultCommunity

● Read-Only ○ Read-Write

Radio0-802.11G

Role in Radio Network: ● Access Point ○ Repeater ○ Workgroup Bridge ○ Scanner

Optimize Radio Network for: ○ Throughput ○ Range ● Default ○ Custom

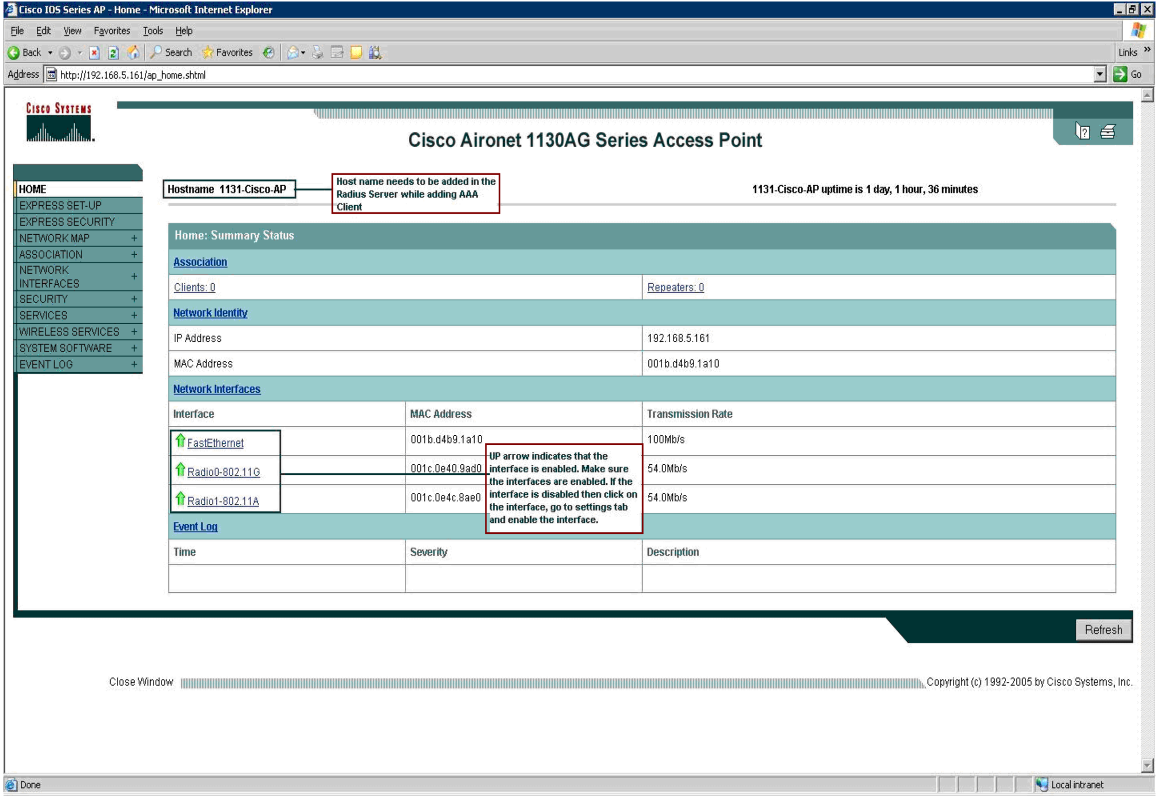
Aironet Extensions: ● Enable ○ Disable

Radio1-802.11A

Role in Radio Network: ● Access Point ○ Repeater ○ Workgroup Bridge ○ Scanner

1. Click on **Express Setup**.
2. Enter the **Host Name** and **IP Address** details for the Access Point.
3. **Role in Radio Network** should be set to Access Point.
4. Click **Apply** to save the settings.

Note: 802.11A Radio is not supported by Avaya 3631 Wireless Telephone.



Cisco Aironet 1130AG Series Access Point

Hostname 1131-Cisco-AP

Host name needs to be added in the Radius Server while adding AAA Client

1131-Cisco-AP uptime is 1 day, 1 hour, 36 minutes

Home: Summary Status

Association

Clients: 0	Repeaters: 0

Network Identity

IP Address	192.168.5.161
MAC Address	001b.d4b9.1a10

Network Interfaces

Interface	MAC Address	Transmission Rate
FastEthernet	001b.d4b9.1a10	100Mb/s
Radio0-802.11G	001c.0e40.9ad0	54.0Mb/s
Radio1-802.11A	001c.0e4c.8ae0	54.0Mb/s

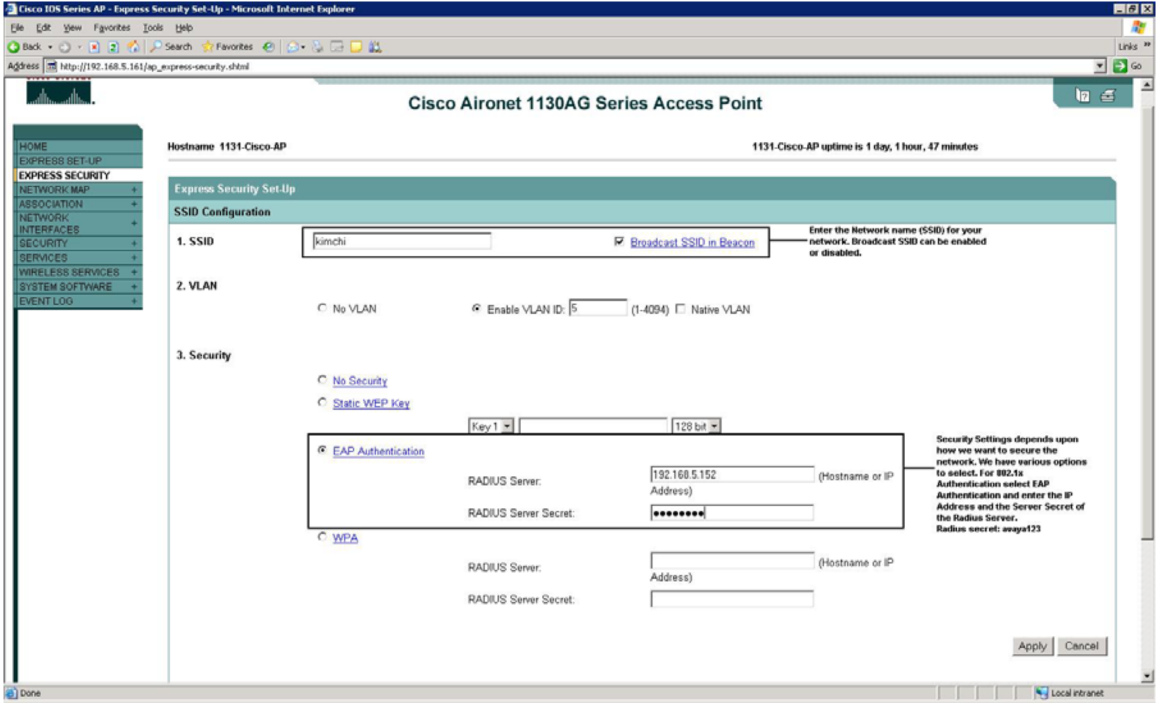
UP arrow indicates that the interface is enabled. Make sure the interfaces are enabled. If the interface is disabled then click on the interface, go to settings tab and enable the interface.

Event Log

Time	Severity	Description

5. Check if we have an UP Arrow under **Network Interfaces** on the main screen.
6. If we see a down arrow, then click on the respective interface, go to settings tab and enable the interface.

<u>Note:</u> Host Name needs to be added in the Radius Server while adding AAA Client.



Address: http://192.168.5.161/ap_express-security.shtml

Cisco Aironet 1130AG Series Access Point

Hostname 1131-Cisco-AP

1131-Cisco-AP uptime is 1 day, 1 hour, 47 minutes

Express Security Set-Up

SSID Configuration

1. SSID: kimchi ☑ Broadcast SSID in Beacon

Enter the Network name (SSID) for your network. Broadcast SSID can be enabled or disabled.

2. VLAN

○ No VLAN ● Enable VLAN ID: 5 (1-4094) ☐ Native VLAN

3. Security

○ No Security

○ Static WEP Key: Key 1, 128 bit

● EAP Authentication

RADIUS Server: 192.168.5.152 (Hostname or IP Address)

RADIUS Server Secret: ●●●●●●●●

○ WPA

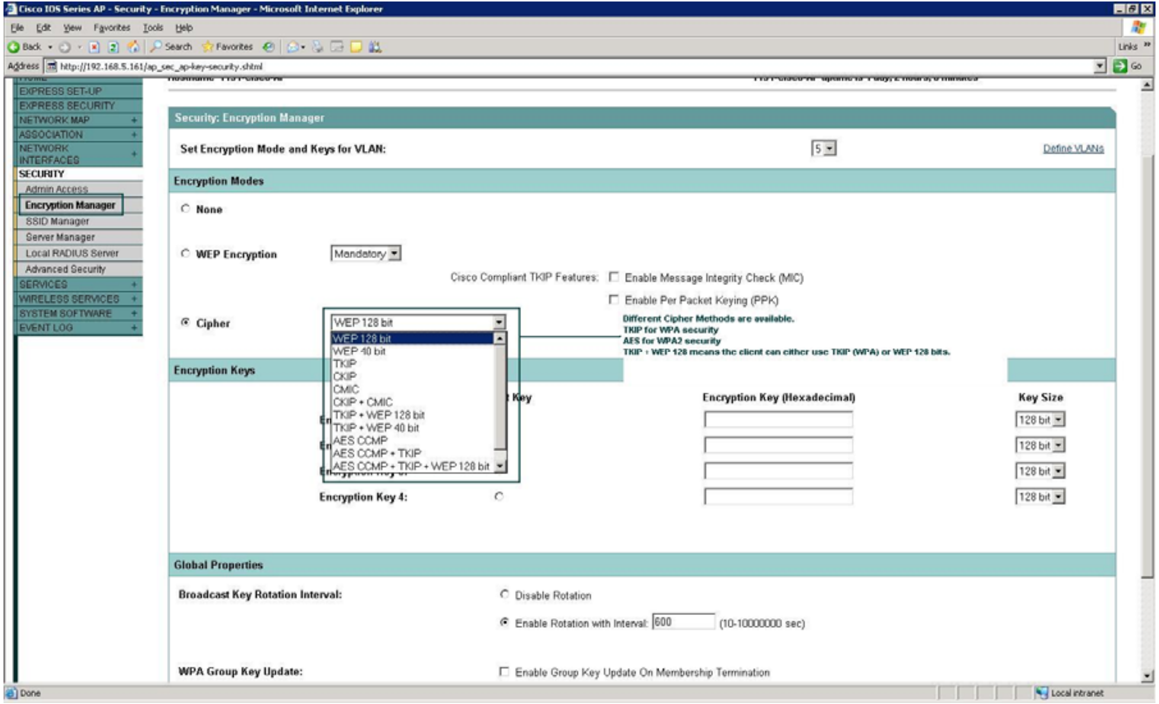
RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

Security Settings depends upon how we want to secure the network. We have various options to select. For 802.1x Authentication select EAP Authentication and enter the IP Address and the Server Secret of the Radius Server.
Radius secret: avaya123

7. Click on **Express Security**.
8. Enter the **SSID, for example "kimchi"**. **Broadcast SSID in Beacon** can be either enabled or disabled as per your network setup. For security reasons the broadcast is normally disabled.
9. Set the **VLAN ID** as per your network setup.
10. Enable **EAP Authentication**. Enter the **IP address** and the **Radius Server Secret** of the Radius Server.
11. Click **Apply** to save the settings.

Note: The Server secret should match with the secret key on the Radius Server.



Security: Encryption Manager

Set Encryption Mode and Keys for VLAN: 5

Encryption Modes

○ None

○ WEP Encryption Mandatory

Cisco Compliant TKIP Features: □ Enable Message Integrity Check (MIC)

□ Enable Per Packet Keying (PPK)

● Cipher WEP 128 bit

Different Cipher Methods are available.
TKIP for WPA security
AES for WPA2 security
TKIP + WEP 128 means the client can either use TKIP (WPA) or WEP 128 bits.

Encryption Keys

Transmit Key	Encryption Key (Hexadecimal)	Key Size
		128 bit
		128 bit
		128 bit
Encryption Key 4: ○		128 bit

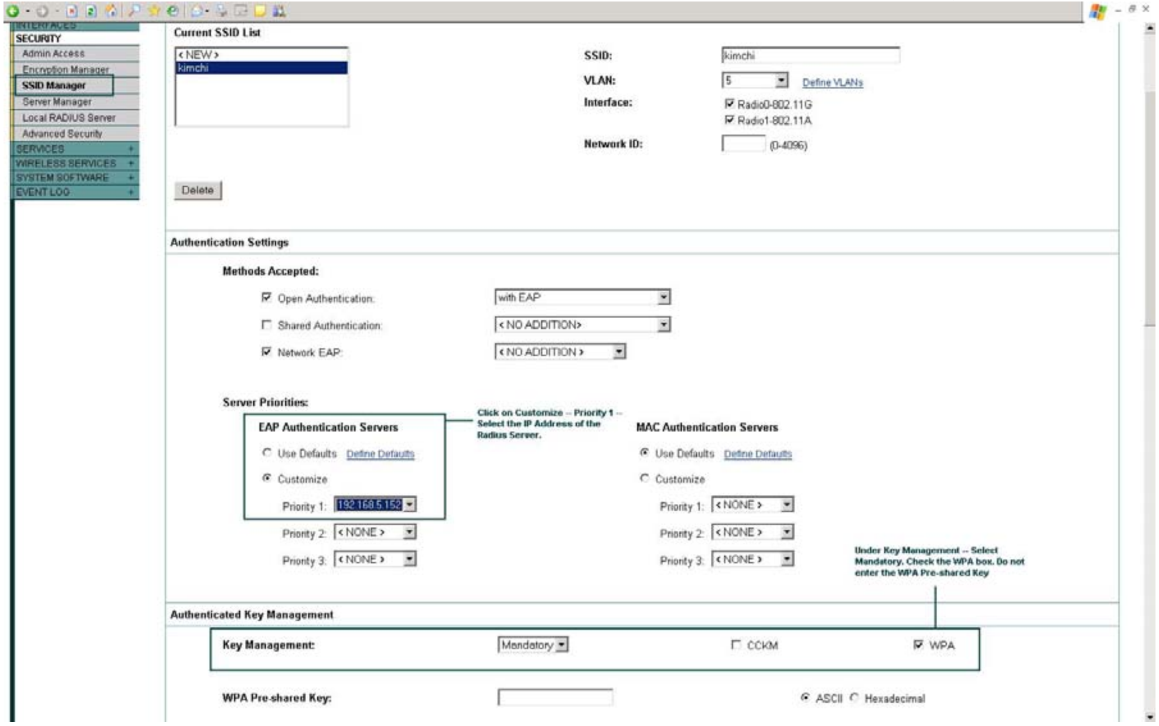
Global Properties

Broadcast Key Rotation Interval: ○ Disable Rotation

● Enable Rotation with Interval: 600 (10-10000000 sec)

WPA Group Key Update: □ Enable Group Key Update On Membership Termination

12. Click on **Security** and then **Encryption Manager**.
13. Different **Cipher** Methods are available. Select **TKIP** for **WPA** and **AES CCMP** for **WPA2**.
14. Click **Apply** to save the settings.



Current SSID List: < NEW >, kimchi

SSID: kimchi

VLAN: 5

Interface: ☑ Radio0-802.11G ☑ Radio1-802.11A

Network ID: (0-4096)

Authentication Settings

Methods Accepted:

☑ Open Authentication: with EAP

☐ Shared Authentication: < NO ADDITION>

☑ Network EAP: < NO ADDITION >

Server Priorities:

EAP Authentication Servers

○ Use Defaults

● Customize

Priority 1: 192.168.5.152

Priority 2: < NONE >

Priority 3: < NONE >

Click on Customize -- Priority 1 -- Select the IP Address of the Radius Server.

MAC Authentication Servers

● Use Defaults

○ Customize

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

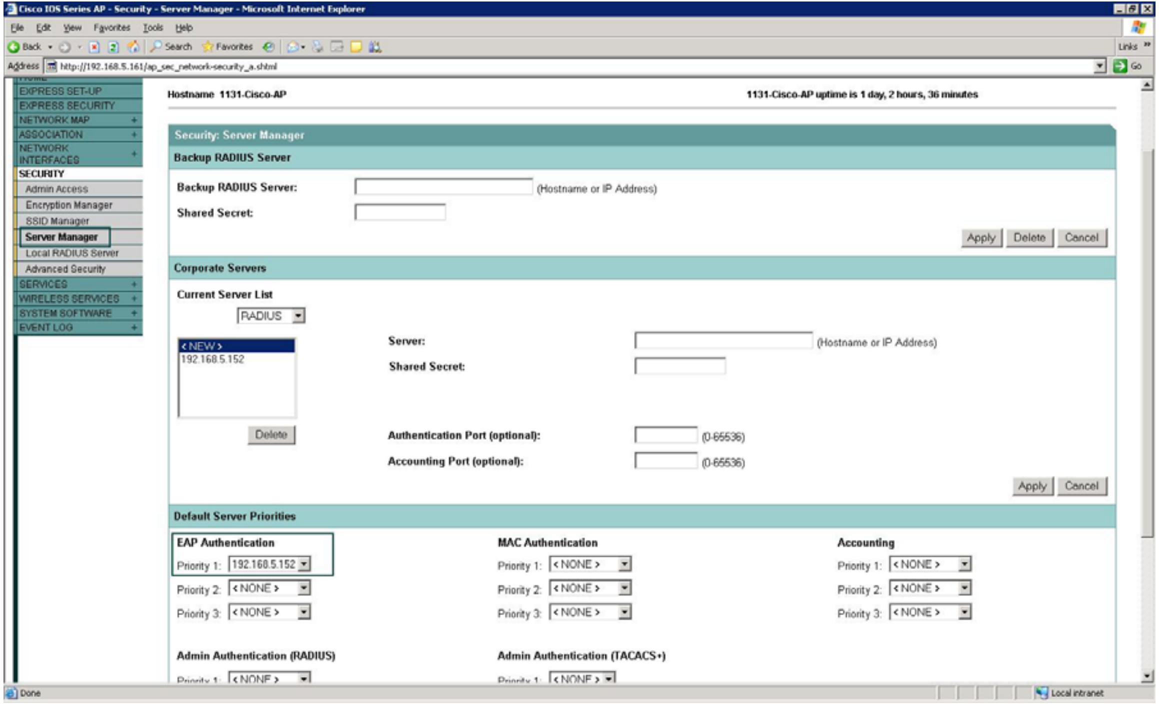
Under Key Management -- Select Mandatory. Check the WPA box. Do not enter the WPA Pre-shared Key

Authenticated Key Management

Key Management: Mandatory ☐ CCKM ☑ WPA

WPA Pre-shared Key: ● ASCII ○ Hexadecimal

15. Click on **SSID Manager**.
16. Select the SSID you want to configure from the **Current SSID List**.
17. Check the box **Open Authentication** and select **with EAP** from the dropdown menu.
18. Check the box **Network EAP**.
19. For **EAP Authentication Servers**, click on **Customize** and Select the IP Address of the Radius Server for **Priority 1**.
20. Set the **Key Management** as Mandatory for Authenticated Key Management. Check the box for **WPA**. Do not enter any **WPA Pre-shared Key**.
21. Click **Apply** to save the settings.



Hostname 1131-Cisco-AP

1131-Cisco-AP uptime is 1 day, 2 hours, 36 minutes

Security: Server Manager

Backup RADIUS Server

Backup RADIUS Server: (Hostname or IP Address)

Shared Secret:

Corporate Servers

Current Server List

RADIUS

< NEW >
192.168.5.152

Server: (Hostname or IP Address)

Shared Secret:

Authentication Port (optional): (0-65536)

Accounting Port (optional): (0-65536)

Default Server Priorities

EAP Authentication	MAC Authentication	Accounting
Priority 1: 192.168.5.152	Priority 1: < NONE >	Priority 1: < NONE >
Priority 2: < NONE >	Priority 2: < NONE >	Priority 2: < NONE >
Priority 3: < NONE >	Priority 3: < NONE >	Priority 3: < NONE >

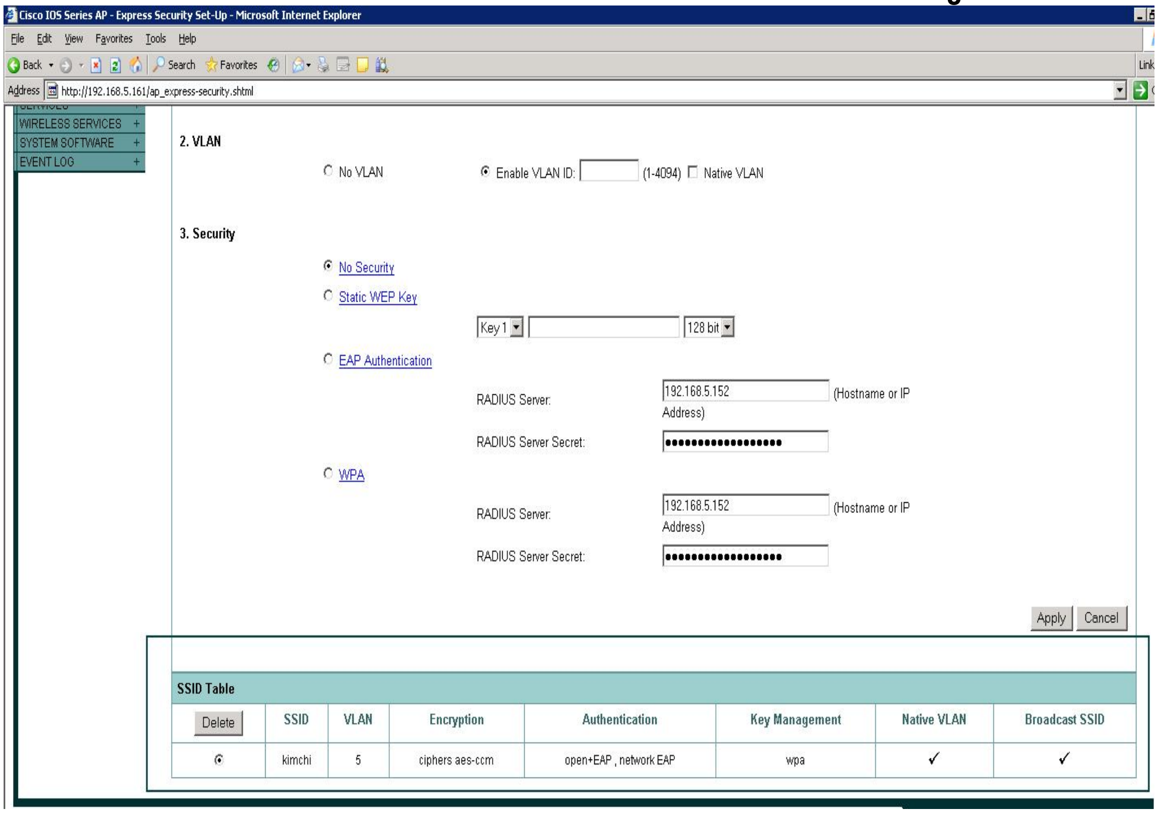
Admin Authentication (RADIUS)

Priority 1: < NONE >

Admin Authentication (TACACS+)

Priority 1: < NONE >

22. Click on **Server Manager** under **Security**.
23. Select the IP Address of your Radius Server under **EAP Authentication** for **Default Server Priorities**.


Cisco IOS Series AP - Express Security Set-Up - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.5.161/ap_express-security.shtml
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +

2. VLAN

○ No VLAN ● Enable VLAN ID: (1-4094) □ Native VLAN

3. Security

● No Security

○ Static WEP Key

Key 1 128 bit

○ EAP Authentication

RADIUS Server: 192.168.5.152 (Hostname or IP Address)

RADIUS Server Secret: ••••••••••••••••••

○ WPA

RADIUS Server: 192.168.5.152 (Hostname or IP Address)

RADIUS Server Secret: ••••••••••••••••••

Apply Cancel

SSID Table

Delete	SSID	VLAN	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID
●	kimchi	5	ciphers aes-ccm	open+EAP , network EAP	wpa	✓	✓

24. Click on **Express Security**.
25. Under **SSID Table** you will see the SSID along with the security settings.

Security Settings on Kimchi Phone

From the A Menu → Advanced → Admin Mode (Enter Admin Password) → Access Profile → Profile 1

Profile Name:	Enter any Profile Name (ex: WLAN1)
SSID:	for example "kimchi" (As set in the AP)
WMM Mode:	ON
Power Save Mode:	Depends on the capabilities of your access point – should not affect 802.1x security.
Security Type:	WPA2-802.1x or WPA-802.1x
Encryption Type:	AES (if Security type is WPA2-802.1x) or TKIP (if Security type is WPA-802.1x)
Encryption Key:	Leave it blank
WEP Key Index:	Not required for 802.1x
EAP Type:	for example "PEAP-MsCHAPv2" (Any method as per your Radius Server configuration)
EAP Identity:	for example "kimchi" (User created on your Active Directory/ Local user created in Cisco ACS)
EAP Username:	for example "kimchi" (User created on your Active Directory/ Local user created in Cisco ACS)
EAP Password:	for example "kimchi123" (password specified for the above user in Active Directory or Cisco ACS)
Use DHCP:	ON/OFF (as per your network setup)

Note: For more information regarding WPA-802.1x/WPA2-802.1x Setup on Avaya 3631 Phone, Certificate generation and uploading the certificate on the phone, refer to the document from the link below:

http://support.avaya.com/elmodocs2/3600/Avaya_3631_Wireless_Security_Configuration_Guide.pdf

Reference Documents

1. Release Notes for Cisco Aironet 1130AG, 1200, 1230AG, and 1240AG Series Access Points for Cisco IOS Release 12.3(7)JX can be found at: http://www.cisco.com/en/US/docs/wireless/access_point/ios/release/notes/b37jxrn.html#wp150990

2. Cisco Aironet 1130AG IEEE 802.11 A/B/G Access Point can be found at: http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6087/product_data_sheet0900aecd801b9058.html

3. Converting LWAPP to Autonomous AP: http://www.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html (Refer to section: Converting a Lightweight Access Point Back to Autonomous Mode)

4. For other assistance, contact Avaya's customer service at: http://support.avaya.com