

# **Cisco WLAN Passpoint™ Configuration Guide**

Last Updated: November, 2013

### **Overview**

The purpose of this document is to describe the necessary set-up procedures for demonstrating an automated network discovery and connection using WiFi Alliance Passpoint<sup>™</sup> Certified Access Point and client devices. Using this document's instructions, you will be able to configure Cisco APs/WLCs as Passpoint 1.0 certified system. Access Points (APs) and phone client devices that are certified for WiFi Alliance's Passpoint 1.0 specification are able to work together providing the functionality listed in this document. This is achieved by AP which supports IEEE 802.11u-based network information and the phone client device that gathers necessary information by using Access Network Query Protocol (ANQP) messages.

The 802.11u enabled phone client devices discover and select target AP based on the information gathered during the pre-association stage from an 802.11u-enabled AP/Wireless LAN Controller (WLC). A phone client device has pre-provisioned network information such as home OI Information, realm name and domain name, presented as configuration file inside the phone client device. In addition, the phone client device may obtain home network information using the IMSI data derived from the inserted SIM/USIM card.

The 802.11u AP provides various information listings that provide the HotSpot owner details, roaming partners, realm list, 3GPP cellular information, and domain name. The realm list also provides listings of the realm name and its associated EAP authentication type mappings. Knowing this information is essential for the phone client device so that correct EAP credential exchange may take place.

Currently, there are many WiFi Passpoint Certified devices, such as Samsung Galaxy-S4 and Intel Centrino 6230 WiFi chipset, and various types of phone client devices. This document uses Galaxy S4 (OS v4.2.2) as the device to demonstrate a "Wi-Fi CERTIFIED Passpoint<sup>™</sup>" device, as well as an iPhone 5 running iOS7 to demonstrate its configuration according to the Wi-Fi Alliance Hotspot 2.0 Specification.

The procedures described in this document provide a means of demonstrating the advantage of a seamless authentication process between the Passpoint supported phone client device and AP in an intraor inter-operator roaming environment. Through this hassle free process, an end user will experience the same ease of use regarding network connectivity as is present and expected with 3G or cellular-based services.



Cisco Systems, Inc. www.cisco.com One of the other benefits of Passpoint is hardened security from Rogue APs. During the network discovery process, the legitimacy of the service provider AP is identified preventing phone client devices from attaching to rogue APs. The information present in the validation process specific to the Passpoint device prevents inadvertent connection to rogue devices such as ad-hoc and other malicious APs broadcasting falsely labeled SSIDs. There are several other technics and methods introduced by Passpoint system to make WPA2-Enterprise security even stronger. GTK randomization is one such technic that is introduced to mitigate WPA2-"hole-196" vulnerability and for more wide usage of P2P blocking at the public WiFi hotspot.

The configuration described in this document lists in sequence the steps necessary to demonstrate and test the functionality. In this demonstration, through the WLAN configuration of the Wireless LAN Controller (WLC), single SSID and multiple SSID will be configured with necessary Passpoint information. This additional Passpoint information will be added on beacon or probe response information, so that Passpoint-enabled phone client device can detect and query AP to get further information. During the query process, standard protocol format called ANQP–Access Network Query Protocol–is followed. Here, the protocol describes the standard 2-way or 4-way handshake process to get enough information from the AP and ANQP server to determine the best AP that the phone client device can authenticate and associate with. This handshake process is called GAS–Generic Advertisement Service–protocol that is defined on IEEE 802.11u standard.

### Figure 1 Basic Passpoint behavior



Throughout the query process, the phone client device will gather information beyond just SSID, such as name of the actual venue, name of the actual HotSpot operator and realm name that can be used as the key element to identify its authentication eligibility. There are many other parameters and information that can be used as criteria to initiate auto connection from the phone client device. In this document, we will go through different use cases and configuration in detail.



The phone client device starts the auto discovery process by reading 802.11u information from the beacon or probe response of the 802.11u/HotSpot 2.0 capable AP. Once a phone client device recognizes and identifies neighboring AP's Passpoint capability, the phone client device starts an ANQP query to get the 3GPP Cellular Information (3GPP CI) or realm name and domain name information. The 3GPP CI & Realm name will reveal the list of service providers that the phone client device may initiate authentication request. The ANQP response also contains a domain name list. The domain name list will provide information if responding AP in the hotspot venue is operating as the home network or visitor (roaming) network. Once the phone client device gathers all of the required information, and if the phone client device successfully passes its own connection criteria, which is defined as Passpoint configuration file called "Cred.conf" in its user directory, the phone client device begins the 802.1x/EAP authentication process to establish a secure connection to the AP. In this example, the "Cred.conf" file name is unique to Samsung Galaxy S4. If there are any other Passpoint 1.0 certified devices, it can have a different name or format of the client configuration file

# Requirements

The following topics contain equipment matrices, drawings, configurations, and steps necessary to implement Passpoint configuration, using Cisco AP/WLC infrastructure.

### **Passpoint Tested Equipment**

Type of devices	Supported devices	Software	Notes			
Wireless LAN	CT5508	7.3.112 and	This document is based on			
controller	WISM2	above	7.5			
	CT8510					
	CT7510					
	CT2504					
	vWLC					
Access Point	LAP1042,	Same as above	Supports both Local mode			
	LAP1142,		as well as FlexConnect			
	CAP1602,		mode (connected mode)			
	CAP2600,					
	CAP3502,					
	CAP3602,					
	CAP1552					
Phone Client	Samsung	Default	Android OS 4.2.2			
Device	Galaxy-S4	shipping OS				

# **Systems Diagram**

The following are examples for the connectivity in the demonstration cases covered in this document.

### Visitor Network in International Roaming Case via Third Party Clearing House

Figure 2

Visitor network connection using Passpoint



In the case of visitor network, Passpoint-configured WLC at a hotspot has network information of its roaming partner network and this network information is provided in multiple ways.

Realm name is the most typical case that single SSID can include multiple realm name information up to 32 realm names. Each realm name is an indicator of available subscription from a user device. Similarly, if a user has a SIM or USIM card with active subscription, the user device can query 3GPP

Cellular information to retrieve its roaming partner using 3GPP carrier identifier, which is a combination of MCC (Mobile Country Code) and MNC (Mobile Network Code). In this type of user case, 802.11u IEs (Interworking Information element and Roaming Consortium Information elements) are mostly used.

### Domestic AP Auto Discovery and Connection (No Inter-WiFi Operator Roaming)



Passpoint connection is mainly useful for the best AP selection among multiple APs. This involves an AP selection process that provides most air capacity (less number of connected user, low amount of RF utilization), backhaul speed and capacity, and network service (IPsec, VoIP, VPN and so on) availability. In the above scenario, HS2.0 IE is mostly used.

# Configuration

### **Case 1–Third Party Clearing House**

### **Configuration Overview**

This configuration uses third party clearing house's private network address. Administrator may need to configure VPN network to connect third party hubbing network. For a quick start, see Initial WLC Configuration guide.

### WLC Configuration

Current Cisco's Passpoint certification is implemented in Controller-based Architecture, which uses WLC as central configuration and AP management hub. All Passpoint configuration is done at WLC or Cisco PI (Prime Infrastructure).

Configuration can be done via Console, ssh, telnet or GUI using Web Browser, as well as central NMS (using Cisco Prime Infrastructure 1.4 or above). In this guide, we will use CLI and Web-based interface from WLC to explain how to configure Cisco Wireless infrastructure to configure Passpoint setup.

#### Figure 4 Cisco Passpoint AP/WLC used in this guide



### WLC1

config wlan create 2 profile\_hs20 HS20\_TEST
//config wlan create <WLAN id> <profile name> <SSID>

config wlan hotspot dot11u enable 2
//Enables dot11u mode on WLAN 2

config wlan hotspot hs2 enable 2
//Enables hotspot 2.0 IE

config wlan hotspot dotllu 3gpp-info add 1 310090 2 //3gpp CIs for EAP-SIM authentication. Add MCC-MNCs for home and roaming partner networks on WLAN 2.

351

config wlan hotspot dotllu roam-oi add 2 1 004096 1 //Adds OI 004096 in the beacon and probe response on WLAN 2  $\!\!\!$ 

config wlan hotspot dot11u nai-realm add realm-name 2 1 realm.com
//Adds realm name "realm.com" for EAP-TLS & TTLS auth on WLAN 2, as realm index 1

config wlan hotspot dotllu nai-realm add eap-method 2 1 1 3 //Adds EAP-TLS as EAP-method in the realm name on WLAN 2

config wlan hotspot dotllu nai-realm add eap-method 2 1 2 6 //Adds EAP-TTLS as EAP-method type in the realm name on WLAN 2

config wlan hotspot dotllu nai-realm add auth-method 2 1 2 1 1 4 //Adds MS-CHAPv2 as auth-method of EAP-TTLS EAP-method in the realm name on WLAN 2

config wlan hotspot dotllu domain add 21 home.com //Adds domain name "home.com" as domain name for home operator on WLAN2 config wlan hotspot hs2 operator-name add 2 1 "ACME-operator" eng //Adds operator name "NGH-operator name" as operator name

config wlan enable 1
//Enables WLAN(indexed as 1)

config radius auth add 1 192.168.1.11 1812 ascii 12345678
//Adds RADIUS authentication server config radius auth add <index> <server\_ip\_address> port#
{ascii | hex} shared\_secret

config radius acct add 1 192.168.1.11 1813 ascii 12345678
//Adds RADIUS accounting server config radius acct add <index> <server\_ip\_address> port#
{ascii | hex} shared\_secret

Cisco WLAN infrastructure supports Passpoint certified 802.11u IEs and HotSpot 2.0 IEs. The current targeted phone client device checks the existence of .11u IE and hotspot 2.0 IE from the beacon or probe response to start further ANQP process. If .11u and hotspot 2.0 IE information in the beacon passes the device's auto connection criteria, the device can select an AP and go ahead to the 802.1x process without going to the ANQP process. For example, if common HESSID is used among single mobility domain, the device may not need to make ANQP query for every APs located in the same area.

### (Cisco Controller) >config wlan create 2 profile\_hs20 HS20\_TEST

This command will create a new WLAN that has "HS20\_TEST" as SSID. This new WLAN will be referred as WLAN index 2 for the future command. SSID "HS20\_TEST" will not be enabled or broadcasted until network administrator explicitly enables it by typing config wlan enable 2 or clicking the Web GUI interface, [] Enabled check box under WLANs > Edit.

#### (Cisco Controller) >config wlan hotspot dot11u enable 2

This command will enable 802.11u services in WLAN index 2. Dot11u service should be enabled as prerequisite of hotspot2 service.

(Cisco Controller) >config wlan hotspot hs2 enable 1

This command will enable HotSpot2 services in WLAN index 2.

### (Cisco Controller) >config wlan hotspot dot11u 3gpp-info add 1 310 090 2

This command will add 3GPP Cellular Information in WLAN index 2; in this example, 310 is used as MCC (Mobile Country Code) and 090 is mapped to MNC (Mobile Network Code). MCC and MNC is a unique value for each operator and is available from UICC Card in the phone client device. The phone client device will read the Home PLMN number from the UICC card, and extract MCC/MNC from PLMN. The phone client device will compare its MCC/MNC number with the AP's 3gpp cellular information using HotSpot 2.0 ANQP and select an AP to initiate EAP-SIM authentication.

If MNC consist of only two digits, use two digits instead of three in your configuration. For example, if MCC/MNC is 520/99, then use 99 in the MNC area. When the phone client device finds a match at the 3GPP-CI value, the phone client device will device either EAP-SIM or AKA based on its provisioned definition.

#### (Cisco Controller) >config wlan hotspot dot11u roam-oi add 2 1 004096 1

This command will add OI (Organizational Identifier) information to beacon and probe response. "004096" was used as an example and this will be also unique for an operator.

OI information will be registered from IEEE Registration Authority and can submit application from IEEE Home page (http://standards.ieee.org/develop/regauth/oui/public.html)

Having an OI value is not a mandatory condition; it is another AP selection criterion from the phone client device.

#### (Cisco Controller) >config wlan hotspot dot11u nai-realm add realm-name 2 1 realm.com

This command will add realm name information to the NAI Realm list. "realm.com" is used as an example here. Once the phone client device gathers the realm name from AP using ANQP, the phone client device will compare with its own provisioned realm name in the phone's HS2.0 profiles. Realm name is unique per operator and usually used in authentication as part of user identity field after an "@" delimiter. A single SSID can have multiple realms defined, the maximum is 32 realm names per SSID. The realm configuration doesn't separate home realm or roamed realm by the Realm list itself.

This Realm name will be sent along with EAP auth type as roaming consortium information element that will be defined from the next command.

#### (Cisco Controller) >config wlan hotspot dot11u nai-realm add eap-method 2 1 1 3

This command will add EAP authentication information, which will give information of the required EAP protocol per realm. This particular line of command describes adding EAP-TLS protocol as an EAP method in the second WLAN index, first realm index, as first EAP method.

#### (Cisco Controller) >config wlan hotspot dot11u nai-realm add eap-method 2 1 2 6

This command will add EAP authentication information, which will give information of the required EAP protocol per realm. This particular line of command describes adding EAP-TTLS protocol as an EAP method in the second WLAN index, first realm index, as second EAP method.

(Cisco Controller) >config wlan hotspot dot11u nai-realm add auth-method 2 1 2 1 1 4 This command will add Auth-Method information, which will give information of the required

authentication types per EAP protocol. This particular line of command describes MS-CHAPv2 auth.type in the second WLAN index, first realm index, EAP-TTLS as EAP method (2), as first auth-index, Non-EAP Inner Method(4).

### (Cisco Controller) >config wlan hotspot dot11u domain add 2 1 home.com

Adds domain name "home.com" as domain name for Home Service Provider. This is used to verify whether current AP connection is a home or roamed (visitor) network.

(Cisco Controller) >config wlan hotspot hs2 operator-name add 2 1 "ACME-operator" eng Adds operator name field on HotSpot 2.0 IE. If an administrator wants to add SPACE character, use double quotation mark to wrap the operator name field. Also language code can be 2 or 3 bytes.

(Cisco Controller) >config wlan enable 2 Finally, enables wlan to start service.

Same goal can be achieved using Cisco WLC's GUI. Complete the steps:

**Step 1** Access to 802.11u config screen in WLANs.

WLANs						Entries 1 - 1 of
WLAN ID	None	[Change Filter] [Change Filter]	wlan ssid	Create New :	Go Step1, Mouse ov Security Policies in left side	er to icon e.of WLAN listing
01	WLAN	profile_wba	WBA_NGH	Disabled	[WPA2][Auth(802.1X)]	Remove Mobility Anchors
					Select#22.11u	Foreign Maps Service Advertisements

Step 2 Enable 802.11u.

MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	
802.11u F	Paramet	ers			
WLAN S	SID	WBA_NGH	Click che	eck box	
802.11	Status	Enabled	2		2

Step 3 In 802.11u IE configuration screen, under 802.11u General Parameters, select [Network Type] and click Apply.

DNITOR WLANS	CONTROLLER WIRELESS SECURITY M	ANAGEMENT	COMMANDS	HELP	FEEDBACK	
2.11u Parameter	8					< Back Apply
WLAN SSID	WBA_NGH					2. Click [Apply]
802.11u Status	S Enabled					
802.11u General I	Parameters 1. Select Net	work Type	Realm List			
Internet Access	Enabled		Realm			Realm Index 1 : Add
Network Type	Free Public Network		Realm Inde	<	Realm	Name
Network Auth Type	Not Configured :					
HESSID	00:00:00:00:00:00		Cellular Ne	twork	Inforamation List	
IPv4 Type	Unknown :		Country Co	de	CellularIndex 1 :	Network Code Add
IPv6 Type	Unknown :		Cellular Ind	ex	Country Code	Network Code
OUI List						
OUI	Is Beacon 4 OUI Index 1 :	Add				
OUI Index	OUI Name Is Beacon					
Domain List						
Domain Name	Domain Index 1	+ Add				
Domain Index	Domain Name					
Foot Notes						

Step 4

Γ

Enter 3GPP CI, Realm name and Domain name and click **Apply**.

WLAN SSID	WBA_NGH				Finally, click [Apply]
802.11u Status	S Enabled				
802.11u General I	Parameters		Realm List		Add [Realm name] then click [Add]
Internet Access	S Enabled		Realm		Realm Index 2 :
Network Type	Free Public Network	:	Realm Index	Realm Name	
Network Auth Type	Not Configured	:	1	realm.com	
HESSID IPv4 Type	00:00:00:00:00:00		Cellular Netv	vork Inforamation List	Add [Country Code] and [Network Code] then click [Add]
IPv6 Type	Unknown ÷		Country Code	e CellularIndex 2	Network Code
OUTLINE			Cellular Index	Country Code	Network Code
OUTLIST			1	310	090
IUO	Is Beacon 4 💿 OUI Index	1 : Ad	b		
OUI Index	OUI Name Is Beac	on			
	Add (Domain Nat	nal than click [A	ddl		

1

**Step 5** Configure EAP per Realm.

Realm List		
Realm	Realm Index 2 ÷	Add
Realm Index	Realm Name Click [realm.com]	
1	realm.com	

**Step 6** Add EAP protocol and Auth type in the 802.11u GUI.

302.11u Para	meters > Eap Det	alls			
WLAN SSID V	VBA_NGH	Realm 7	tame realm.com	1	
	E	ap List			
Eap Method	Not Applicable	Eap Index	3 :	Add	
Eap Index	Eap Method				
	EAP-TLS				
1			-		

802.11u Parameters	> Auth Details							< Back	Apply
WLAN SSID WBA_NGH	Rea	im Name	realm.com		Eap Method	EAP-TTL	P-TTLS] Eap S 1	Method	
	A.	th Meth	od List		2 Select (MSCHAR)	2] as Auth P	aram	3. Click	[bbA]
Inner Auth Method	Non-EAP Inner Auth Method	1	Auth Param	MSCHAPV2	Auth Method	Index	1 0	Add	
Auth Method Index	Inner Auth Meth	bod	Aut	h Param					

### **Phone Devices**

The WFA Passpoint certified phone is recommended. In this configuration guide, we will use Samsung Galaxy-S4 stock device as the client machine. The device takes network information from two different locations:

The first location is the UICC (Universal Integrated Circuit Card) Card. The UICC card (SIM or USIM Card) has IMSI (International Mobile Subscriber Identity) information containing 15-digit long number that starts from MCC and MNC. This number will be extracted and used with 3GPP CI comparison. Optionally, an administrator can manually configure 3GPP-CI provision inside the phone's Passpoint configuration file. The second location is a static realm definition file, located at "/storage/emulated/0". It is not stored by default, the cred.conf file must be created separately using text editor or similar tools. Currently, auto creation of default profile is not supported.

Below is an example of a typical Passpoint/EAP-SIM based authentication configuration file "cred.conf" on SGS4,

```
cred={
imsi= "?"
eap=SIM
}
```

There are a couple of methods to create this "cred.conf" file and save it on /storage/emulated/0 folder.

### Method 1

A Windows PC is required to apply this method. You must connect the phone to your PC by using a USB cable. Configure the phone as removable disk. Once the phone is recognized, you will find a disk copy of "cred.conf" file in the root directory.



### Method 2

You can use the Text Editor available in Android and create a "cred.conf" file and save it directly in your phone device.

- 1. Go to Google "Play Store" and search for a text editor.
- 2. Download "Jota Text Editor" or a similar text editor.
- 3. Open Text Editor and type the below message as shown in the screenshot.
- 4. Save the file as "cred.conf" in /storage/emulated/0 folder.



### Method 3

1. Write a config file from a different machine, such as PC or MAC and save it as "cred.conf" file.

- 2. Send an email to the test phone with the "cred.conf" file attached.
- **3.** Open the default Gmail reader or Email reader and open the received email folder and click the attachment to save the file in the phone device. Use the default save location "/storage/emulated/0/Download".
- 4. Select the "My Files" App.



5. Go to All Files > Download and select "cred.conf".



6. Select the "=" icon on the top right corner of your phone screen or long press cred.conf file. Select the Copy or Move option.



7. Select the "/storage/emulated/0" folder



ſ

8. Click the "Paste here" (or "Move here") button to complete the copy (or move) process



### Method 4

- 1. Same as Method 3, an external editor is used to create the config file. Save the file name as "cred.conf".
- 2. Copy the file to an external memory card (microSD Card).
- 3. Insert the microSD card to the phone device.
- 4. Run the "My files" application.
- 5. Navigate to /extSdCard and confirm if the "cred.conf" file is available (copied into the external memory card at step 2).
- 6. Long key press "cred.conf" file until the Copy menu is displayed.
- 7. Select "Copy" and paste the file to the parent folder /sdcard0.

If Passpoint system is configured for EAP-TLS, CA certificate and User certificate must be copied using microSD card. The files can also be sent as emails because PKCS#12 SGS4 support multiple certificate encoding formats. ".p12" formatted certificate is generally recommended.

I

### Case 2–Standalone Demo Configuration Without using Third Party AAA Server

This topic does not cover cases where Operator is using third party AAA.

### AAA Configuration using Cisco CAR

### Add WLC as RADIUS Phone

### To add WLC as RADIUS phone:

### CAR

cd /radius/phones // cd to RADIUS phone section
add hs20wlc //Add WLC as RADIUS phone
cd hs20wlc/ //cd to WLC setup
IPAddress = 10.11.23.102 //WLC\_mgmt\_ip
Sharedsecret = cisco123 //WLC\_radius\_secret
save //Save configuration

### **Define ITP MAP Gateway as Remote Server**

To define ITP MAP Gateway as remote server:

```
CAR
```

cd /Radius/RemoteServers //cd to Remote AAA server - pointing to ITP MAP GW router
add itp1 //Add ITP MAP gateway. Name "itp1" as remote server
cd itp1/ //cd to itp1 setup
Protocol = map-gateway //Set the protocol as map-gateway
IPAddress = 10.11.24.11 //map-gateway IP address
Port = 12345
ReactivateTimerInterval = 300000
Sharedsecret = itpmap1
MaxTries = 3
Initial Timeout = 45000
save

### **Define EAP-SIM Service**

To define EAP-SIM service: CAR cd .. add eap-sim cd eap-sim set Type eap-sim cd RemoteServers/ add 1 itp1 save

### **Define Rule for EAP-SIM Realm Based Authentication**

To define rule for EAP-SIM realm based authentication:

### CAR

I

```
cd /radius/Rules//Navigates to Rules directoryadd sim-operator1.com//Add new rule name using the add commandset Script ExecRealmRule//Set ExecRealm Rulecd Attributes///Go to Attributes sub-directorySet Authentication-service eap-sim //Define eap-sim as authentication methodSet realm @sim-operator1.com// Set realm namesave// Save configuration
```

### **Define Policy for EAP-SIM Realm based Authentication**

To define policy for EAP-SIM Realm based authentication: CAR cd /radius/Policies add SelectPolicy // Added Policy Set Grouping sim-operator1.com //Set grouping to the name of rules save //save configuration

### **Define EAP-SIM Subscriber**

To define EAP-SIM subscriber:

### CAR

```
cd /Radius/UserLists/subscribers-local // cd to local subscriber
add 1102030405060708 // Add new user name based on IMSI with a prefix of 1
set AllowNullPassword TRUE // Allow Null password for EAP-SIM user
save // save configuration
```

Repeat the above steps for each user.

### **WLC Configuration**

Same as AAA Configuration using Cisco CAR but the IP address can be different per assigned local addressing.

### **Handset Configuration**

By default, the phone's Passpoint module is disabled. To enable it, go to [Settings] and in Connections Tab, select Wi-Fi option and Click Menu button (left side of home button) and enable Passpoint feature.



- 1. Complete "cred.conf" file based on operator's roaming partnership and copy the file into the /storage/emulated/0 folder.
- 2. Use "cred.conf" file content in topic Phone Devices for EAP-SIM.
- **3.** EAP-TLS/TTLS will require pre-loaded certificate definition and user ID/password information inside of cred.conf, the file insertion method is the same.

Actual Importing of certificate can be done by manual certification copy and install or using Gmail in your phone to import the certificates.

### **Using Gmail in your Phone**

ſ

- a. Send certificate as attachment of an email to the phone's registered Gmail address.
- **b.** Open Gmail from your Android phone device and open the email where the certificate is attached.
- c. Click [View] button
- d. Type Password to Extract certificate if it has one



Installed Certificate can be verified from [Settings] > [More] > [Security] > [Trusted Credential] > Select [User] Tab

**e.** Administrator may be prompted to enable the security PIN or code to enable Certificate usage if it's the first time that the certificate is being inserted.

### Manual Certification File Copy using microSD Card.

This process can be done by using the external microSD card:

a. External microSD card can be accessed from the "MyFiles" app as "SD memory card"



- **b.** Select the EAP-TLS certificate and copy it under the root folder of [Device storage] /storage/emulated/0 folder.
- c. Navigate to [Settings] > [more] > [Security] > [Install from device storage]
- 4. Once all the settings have been configured, turn on WiFi interface. If the phone device discovers auto-connect eligible HotSpot 2.0 AP, it will automatically proceed to 802.1x authentication process that is included in "cred.conf" file, which matches with AP's 11u value where EAP auth type and realm name is defined. The phone device will not show any particular indicator for Passpoint-enabled SSID unless the user is successfully authenticated and connected.
- 5. At any time, if the user turns off the Passpoint feature, auto-connected SSID will be disconnected.
- **6.** If you click the [Passpoint] toggle menu from the advance menu, the phone device will display the scanned Passpoint APs.

I



Cisco WLAN Passpoint™ Configuration Guide

# **Configuration Guide per Test Case**

### Power Device with Wi-Fi Radio Turned On

### **Pre-Provisioned Case for EAP-SIM**

When configuring from a phone device, you must create "cred.conf" file as given in the below format:

cred={imsi= "mncmcc-simno"
eg.domain=home.com}
cred={imsi= "19454-simno"
domain=home.com}

"mncmcc" part is a combination of two or three digit MNC and three digit MCC. After MNCMCC number, add "–(dash)simno(string "simno"). Optionally, "cred.conf" file can have a domain definition which is used for validating roaming (Visitor) network by comparing domain name in ANQP response from AP and the phone's pre-configured information. If the domain name from AP (received by ANQP query result) is matched with cred.conf file's domain name, the AP will be considered as Home network. If imsi value is matched but is not a domain name, it will be considered as Visited (roamed) network. The sequence of MCC and MNC is reversed at the AP/WLC's 3GPP CI information tab.

### WLC

WLC must know the 3GPP CI information of the SIM Card which is being tested. To get this information, administrators must load the IMSI reader utility on the Phone. IMSI reader utility is downloadable from Google Play Store by searching the keyword "imsi" from the Play Store search text box. A list of result is displayed, select the "Know Your Phone" App.

· · · ·	 	-		
		)48 🍞 📶 🚺 17:16	्रम् 🕺 😤 🖉 🖉 🖓 🖓 🖓	7
( 🍞 Apps		<ul> <li>&lt;</li> </ul>	Know Your Phone	
Know Your Phone			YOUR Mobile No: +85	
YOUR PHONE MARK YANGCM		Install	IMEI: 351869	
			1M51: 45419p	
1471 214210204490177 0421 24420200449077 0421 325074172042040 0421 3250744412042040				
RANGE MOTOR FILE MARKE MOTOR			BRAND: samsung	
			MODEL: GT-19300	
			ANDROID RELEASE: 4.1.2	
				9
**** 13		May 15, 2011	Simple Apps, but always useful!	122
1,000+ downloads		93.10KB		35

In the above example, "454" is recognized as the Mobile Country Code(MNC) and "19" is recognized as the Mobile Network Code (MCC). This value will be loaded by the Passpoint module in the phone client device and will be used to compare 3GPP CI from WLC as ANQP query result.

WLC can be configured to have matching MCC and MNC value, you can do this by configuring MCC as 454 and MNC as 19 in the 3GPP CI section of 802.11u config screen.

Country Code	454	CellularIndex 1 ÷	Network Code 19	Add
Cellular Index		Country Code	Network Code	

### From CLI

Use the command: (Cisco Controller) >config wlan hotspot dotllu 3gpp-info add 1 454 19 1  $\,$ 

Once the phone client device is connected successfully, a message Connected (via Passpoint) is displayed.

1 T A A A A		iki 🍞 🕌 19:35
< 🔯 Wi-Fi	a 🕹 🕹	Scan 😭 Wi-Fi Direct
Wi-Fi networks		
WBA_NGH Connected(via passpoint)		() <del>,</del>
alpha Secured		( <del>)</del>
alpha_byod Secured		(c <del>3</del>
alpha_phone Secured		( <del>(</del> 7

### **Provisioned SIM for EAP-AKA**

### **Configuration from Phone**

EAP-AKA is not very different from EAP-SIM case. When configuring from phone, you must create "cred.conf" file as given in the below format:

```
cred={imsi= "mncmcc-simno"
eg. eap=AKA
domain=home.com}
cred={imsi= "19454-simno"
eap=AKA
domain=home.com}
```

"mncmcc" part is a combination of three digit MCC and two or three digit MNC. After MNCMCC number, add "–(dash)simno(string "simno"). The phone's IMSI sequence is MNC-MCC. WLC's 11u 3GPP CI sequence is MCC-MNC.

Similar to EAP-SIM, "cred.conf" file can optionally include domain definition which can be used for validating roaming (Visitor) network by comparing domain name in ANQP response from AP and phone's pre-configured information.

I

### EAP-TLS

#### **Configuration from the Phone**

The phone client device must have pre-provisioning certificates–CA certificate (if the testing environment uses private CA or Root CA that is not in the factory default certificate on android ), Server certificate, and a phone certificate.

Android OS 4.1.2 can support \*.p12, \*.pfx and \*.cer formatted certificate as importing certificate. A single \*.p12 file can package multiple certificates and key files.

The "Cred.conf" file must adopt different type of credentials:

```
cred={
username="user-name"
realm="realm.com"
domain="home.com" #mandatory for home identification
ca_cert="keystore://CACERT_certificate-name-installed"
phone_cert="keystore://USRCERT_certificate-name-installed"
private_key="keystore://USRPKEY_privatekey-name-used"
}
```

### **Configuration from the WLC**

Administrators can use the same configuration steps as WLC Configuration

### From GUI

Navigate to [WLANs][802.11u] Setup Screen

Realm List				WLAN SSID	WBA_NGH	Realm Nam	e realm.com	
Realm		Realm Index	2 ÷ Add		Eap	List		
				Eap Method	Not Applicable 🗧	Eap Index	2 ÷ Add	
Realm Index	Realm Name			Eap Index	Eap Method			
1	realm.com			1	EAP-TLS		3	

#### From CLI

(Cisco Controller) >config wlan hotspot dotllu nai-realm add realm-name 1 1 realm.com (Cisco Controller) >config wlan hotspot dotllu nai-realm add eap-method 1 1 1 3

### **EAP-TTLS**

### **Configuration from the Phone**

The phone client device must have pre-provisioning certificates–CA certificate (if the testing environment uses private CA or Root CA that is not in the factory default certificate on android ), Server certificate, User ID, and password.

```
cred={
username="user-name"
password="password"
realm="realm.com"
domain="home.com" #mandatory for home identification
ca_cert="keystore://CACERT_certificate-name-installed"
}
```

### **Configuration from the WLC**

Administrators can use the same configuration steps as WLC Configuration.

### From GUI

Navigate to [WLANs][802.11u] Setup Screen

				802.11u Par	ameters > Eap Details				
Realm List				WLAN SSID	WBA_NGH	Realm I	Name realm	.com	
Realm		Realm Index	2 ÷ Add		Eap	List		In the local division of the local divisiono	
Realm Index	Realm Name			Eap Method	Not Applicable : Eap Method	Eap Index	3 :	Add	
1	realm.com			1 2	EAP-TLS EAP-TTLS				

802.11u Paramete	rs > Auth Details								< Back	Apply
WLAN SSID WBA_N	GH Re	alm Name	realm.com			Eap Method	EAP-TTLS	:		
		Auth Meth	od List							
Inner Auth Method	Non-EAP Inner Auth Method	1.1	Auth Param	Reserved	1	Auth Method I	Index	2 1	Add	
Auth Method Index	Inner Auth Method	Aut	h Param							
1	Non EAP Inner Auth	MSC	CHAPV2							

### From CLI

Follow the same configuration steps as WLC Configuration.

(Cisco Controller) >config wlan hotspot dotllu nai-realm add eap-method 1 1 2 6 //Adds EAP-TTLS as EAP-method type in the realm name.

(Cisco Controller) >config wlan hotspot dotllu nai-realm add auth-method 1 1 2 1 1 4 //Add MS-CHAPv2 as auth-method of EAP-TTLS EAP-method in the realm name.

### **Non-Provisioned EAP-SIM**

### **Configuration from the Phone**

In the assumed SIM card case, the phone client device reads the 3GPP Cellular Information (3GPP CI) on the SIM card and automatically populates the necessary MCC/MNC information. The phone client device will then use the SIM card's information and make comparison with AP's 3GPP CI ANQP query result. There is no explicit or pre-defined IMSI information required at the phone client device's configuration file. If the AP responds with identical 3GPP CI values, the phone client device will make an automatic EAP-SIM connection. Since there is no home domain definition, every auto connection is considered as roaming network.

Currently, the phone client device does not generate the default "cred.conf" file from the off-the-shelf package. Manual creation of the minimum skeleton config is still required.

Here is the required "cred.conf" file content.

```
cred={
imsi= "?"
eap=SIM
}
```

### **Configuration from the WLC**

Same as first test case -WLC Configuration.

### **Non-Provisioned EAP-AKA**

ſ

EAP-AKA is not different from EAP-SIM case, except for the eap type definition given below:

```
cred={
imsi= "?"
eap=AKA
}
```

**Result Screen for Home Network Connection** 



### **Result Screen for Roamed Network Connection**



# Home Network Prioritization over Visited Network (No Pre-Provisioning of Realms)

### **Configuration of Phone**

Since there is no pre-provisioning of realms, connection should be done over 3GPP CI using pre-provisioned domain name field to validate HSP or Visited Network.

### **Configuration of WLC:**

Create two Passpoint-enabled SSIDs and configure the same 3GPP CI on both SSID. You must define "home.com" domain name in one SSID and leave other as no domain name. SSID that has "home.com" domain name IE will become HSP and the other with no domain name becomes a Visited Network.

WLANs				Entries 1	- 2 of 2
Current Filter: No	ne [Change Filter] [Clear Filter]	el .	Create New :	io	
WLAN ID Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
1 WLAN	profile_wba	WBA_NGH	Enabled	[WPA2][Auth(802.1X)]	
2 WLAN	profile_visited	NGH_Visited	Enabled	[WPA2][Auth(802.1X)]	

As the current handset's observation, the phone client device does not break the current established connection on Visited Network even if HSP network comes back online.

I

# Debug

### **Debug from the Controller**

Use the following commands to debug from the controller:

(Cisco Controller) >debug hotspot event enable //Displays HS 2.0 event debug information.

(Cisco Controller) >debug hotspot packet enable //Displays HS 2.0 packet debug information.

# **Configuring Hotspot 2.0 on iOS7**

With the release of the new version of the iOS7 Operating System, Apple announced support for the "Wi-Fi Alliance Hotspot 2.0 Specification" on their recent products such as iPhone 5, iPad mini, and later iDevices. Because only those products that have completed and passed Wi-Fi certification to the Hotspot 2.0 test plan may use the Passpoint<sup>TM</sup> name; in Apple's iDevice context, the term used will be "Hotspot 2.0" or HS2.0, but not "Passpoint<sup>TM</sup>".

The key strength of Apple's HS2.0 implementation is integrating it into their existing and proven framework of "Configuration Profiles" (previously known as "iPhone Configuration Profiles").

A configuration profile is simply an XML file containing a number of settings, including:

- Wi-Fi settings (HS2.0 settings were introduced to this section)
- Credentials and keys
- Restrictions on device features
- VPN settings
- Email server settings
- Exchange settings
- LDAP directory service settings
- CalDAV calendar service settings
- Web clips

By leveraging a method already familiar to network administrators around the world, Apple was able to scale the adoption of HS2.0 from day one. The scalability of Configuration Profiles has been proven over the years. Distributing Configuration Profiles can be done via any of the following five ways:

- Using Apple Configurator (iOS only)
- In an email message
- On a web page
- Over-the-Air Profile Delivery and Configuration
- Over the air using a Mobile Device Management Server

In this document, we will be using the "Apple Configurator" to illustrate the minimum required steps to create and push a HS2.0 Configuration Profile. The profile we create will demonstrate authentication using EAP-TLS and EAP-SIM on an iPhone 5.

The Apple Configurator app is available for free from the App Store (currently, only available for MAC OS). Apple Configurator version 1.4.2 or later is recommended.

For more information on the Apple Configurator, we recommend watching the instructional video at http://www.apple.com/education/tutorials/#introduction-to-apple-configurator and for a reference on Configuration Profiles refer to

https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html



On the WLC side, the minimum configuration required is as follows:

- 1. Create a WLAN with default L2 security settings (WPA2, 802.1x), and define the external RADIUS handling the EAP-TLS and/or EAP-SIM in our example.
- 2. Enable the 802.11u for the WLAN, set the Network type to any value.

ı. cısco			TROLLER W	IRELESS SECUR	ity m <u>a</u> nag	EMENT COMMANDS	HELP FEEDE	Sa <u>v</u> e	Configuration <u>P</u> ing Logout <u>R</u> efresh
WLANs	WLANs							A. Se	lect WLAN's
✓ WLANS WLANS	Current Filter	n None	[Change	Filter] [Clear Filter]			Create New	: 60 802	2.11u option
Advanced	WLAN ID	Туре	Profile Name		WLAN SS	ID	Admin Status	Security Policies	
	01	WLAN	WBA22_Cisco		Cisco Ho	tSpot 2.0	Enabled	[WPA2][Auth(802.1X)]	
	2	WLAN	admin		adminnet		Enabled	[WPA2][Auth(PSK)]	
	0 2	WLAN	profile_wba		WBA_NG	E.	Disabled	[WPA2][Auth(802.1X)]	Remove Select
								Mouse over to the blue icon beside the WLAN you want to configure	Mobility Anchor 802.110 Foreign Maps Service Advertisements Hotspot 2.0
				MONITOR	<u>W</u> LANs		R W <u>I</u> REL	ESS <u>S</u> ECURITY	
MONITOR WLANS	ONTROLLER	WIRELESS	SECURITY	802.11u	B. Ena	able 802.11	u Status		n <u>Ping Logout R</u> efresh
802.11u Parameters	5			WLAN S	SID	WBA_NGH	Click	check box	< Back Apply
WLAN SSID	ONGH_HOME			000 11	Chathan	- Enabled			
802.11u Status	Senabled			802.110	u Status	Enabled			D. Apply
802.11u General F	arameters		_			Realm List			
Internet Access	🗹 Enabled	C. Se	lect Ne	twork Typ	be	Realm		Realm Index	1 : Add
Network Type	Chargeable P	ublic Network	: •			Realm Index		Realm Name	
Network Auth Type HESSID	Not Configur	ed 00:00	\$			Cellular Network In	nforamation L	ist	
IPv4 Type	Unknown		۵			Country Code	CellularInde	x 1 : Network Code	Add
ІРv6 Туре	Unknown	٠				Cellular Index	Country C	Code Network (	Code

**3.** Define at least one Domain Name in the **Domain List** to match that set for the iDevice (more details will be provided in later sections).

رابیاب cısco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT
WLANs	802.11u Parameter	rs			
<ul> <li>✓ WLANS</li> <li>WLANS</li> <li>▶ Advanced</li> </ul>	WLAN SSID 802.11u Status	Pod-07-Passpoir	nt		
	802.11u General	Parameters			
	Internet Access	Enabled	the billion of the		
	Network Type	Acceptance of te	erms and cond	÷ ditions ¢	
	HESSID	00:00:00:00:00	0:00		
	IPv6 Type	Unknown	:		
	OUI List				
	OUI	Is Beacon 1	OUI In	dex 1	÷ Add
	OUI Index	OUI Name	Is B	eacon	_
	Domain List				
	Domain Name			Domain Index	2 ÷ Add
	Domain Index	Domain Name			_
	1	nome-u7.com			<u> </u>
	Foot Notes	can be configured	with 'Is Bead	on' enabled	

4. Enable the check mark for "Hotspot 2.0" (the default settings are sufficient).

### **The Apple Configuration**

ſ

No configuration is required on the device itself (ex: the iPhone). All Hotspot 2.0 configuration will be done on the Apple Configurator App.



Open the Apple Configurator App and choose **Supervise** from the top menu. In the new screen, under the **Profiles** list, click the "+" button to create a new Profile.

1

00	Apple Cont	figurator	
	Prepare Superv	rise Assign	
SUPERVISED DEVICES	All iPhones (1)		Settings Apps
All Devices	iPhone	Name:	iPhone
li∉ USB Connected	16 GB iPhone		Number sequentially starting at 1
		Update IOS:	When update is available
		Restore:	Don't restore backup \$
		Lock to App:	None    Options
		Profiles:	EAP-SIM
			Passpoint
2. Choo.	se Create Net	w Profile -	1. Click on the "+" • - C Import Profile Create New Profile
	(42) Refra		

The **General** settings tab will open. Enter the Profile information as you would like it to be displayed on the iDevice.

<u>[</u> ]	General Mandatory	G	eneral
P	Passcode Not configured		Name
<u>î</u>	Restrictions Not configured	Enter a Profile na	MyHotSpot2.0
١	Global HTTP Proxy Not configured	and	Name of the organization for the profile
G,	Web Content Filter Not configured	Organizat	Description Brief explanation of the contents or purpose of the profile
(	Wi-Fi Not configured		[optional]
	VPN Not configured		
•	AirPlay Not configured		Consent Message A message that will be displayed during profile installation
=	AirPrint Not configured		[optional]
	Mail		

Notice all the various configuration options to the left of the menu; in this guide we will only be using the **Wi-Fi** tab and then later on the **Certificates** tab to add the required certificates for EAP-TLS.



In the **Wi-Fi** configuration menu, the default **Network Type** is **Standard** (for example, entering an SSID value is mandatory as indicated by the small arrow shown in the screenshot).

To access the full "Hotspot 2.0" configuration options, from the **Network Type** drop-down list, choose **Hotspot 2.0**.

Note

I

You can add, mix, and match multiple Wi-Fi configuration instances (Payloads) within the same configuration profile by clicking the "+" button at the top right-hand side of the Wi-Fi configuration screen.

Mandatory	wi-ri Notice that an SSID is mandatory
Passcode Not configured	for a non-HS2.0 Network Service Set Identifier (SSID)
Restrictions	[required]
Global HTTP Proxy Not configured	Hidden Network Enable if target network is not open or broadcasting Auto Join
Web Content Filter	Automatically join this wireless Network Proxy Setup
Wi-Fi 1 Payload Configured	Configures proxies to be used with this network None
Not configured	Security Type Wireless network encryption to use when connecting
AirPlay Not configured	Network Type Configures network to appear as legacy or Hotspot 2.0
AirPrint Not configured	Standard Legacy Hotspot
Mail	

Notice that the SSID field is now disabled, and new configuration options pertaining to HS2.0 have now become available. Apple's Hotspot 2.0 implementation requires both the **Displayed Operator Name** and **Domain Name** to be configured.

1

	ĴØ.	General Mandatory	Wi-	Fi The SSID field is disabled for HS2.0 Networks
	2	Passcode Not configured		Service Set Identifier (SSID) Identification of the wireless network to connect to
	6	Restrictions Not configured		Hidden Network
	٩	Global HTTP Proxy Not configured		Enable if target network is not open or broadcasting
-	G.	Web Content Filter Not configured		Proxy Setup Configures proxies to be used with this network
10	(îr	Wi-Fi 1 Payload Configured	2	None ÷
		VPN Not configured		Wreless network encryption to use when connecting WPA2 Enterprise
		AirPlay Not configured		Enterprise Settings Configuration of protocols, authentication, and trust
	-	AirPrint Not configured		Protocols Trust Accepted EAP Types
		Mail Not configured		Authentication protocols supported on target network TLS LEAP EAP-FAST EAP-AKA TTLS PEAP EAP-SIM
	EX	Not configured		Network Type Configures network to appear as legacy or Hotspot 2.0
	@	Not configured		Hotspot 2.0
		Not configured		And of the Hotspot 2.0 service provider
		Not configured	Operator & D	Domain Name Domain name of the Hotspot 2.0 service provider Omain names are both mandatory in
	<b></b>	Not configured	Apple's imple	Reaming Consortium Ols
	*	Not configured		Roaming Consortium Organization Identifiers
	F	Not configured		
		Not configured	Scroll down	+ - NAI Realm Names
		Not configured	more to see the MCC/MNC	Network Access Identifier Realm Names
	<b>a</b>	Not configured	section	
	2 valida	ation errors	2 T-800-87	Cancel

The **Displayed Operator Name** is simply the value displayed below the SSID's name on the iDevice as shown in the following screenshot of an iPhone 5.

●●●○○ Sprint 1x	6:06 AM	<b>1</b> ∦ ■D
Settings	Wi-Fi	
Wi-Fi		
CHOOSE A NET	WORK	
adminnet		🔒 🗢 🚺
HS2.0 Cisco Hotspo	t2.0	<b>₽</b> ╤ (j)
Love	below the SSID	a 🗢 🤅
"Displa Other	ayed Operator N	ame"
Ask to Join N	etworks	$\bigcirc$
Known networks If no known networks have to manually	s will be joined vorks are avail y select a netw	automatically. able, you will rork.
		351982

Γ

Note

The **Domain Name** value set in the Apple Configuration Profile must match at least one of the configured domains advertised by the WLC as set in the 802.11u configuration screen for that WLAN.

1

،،ا،،،ا،، cısco	MONITOR WLANS C	ONTROLLER WIR	ELESS SECURITY	MANAGEMENT C
WLANs	802.11u Parameters	8		
VLANs WLANs	WLAN SSID	HS2.0		
Advanced	802.11u Status	S Enabled		
	802.11u General P	arameters		
	Internet Access	Senabled		
	Network Type	Chargeable Public Ne	twork ‡	
	Network Auth Type	Not Configured	\$	
	HESSID	00:00:00:00:00:00		
	IPv4 Type	Unknown	\$	
	IPv6 Type	Unknown ‡		
At least one Domain Name from	OUI List			
this list must	OUI	Is Beacon 1	OUI Index 1	\$ Add
match the value configured in the	OUI Index	OUI Name	Is Beacon	
Apple Profile before	Domain List			
attempt joining the	Domain Name		Domain Index	3 ‡ Add
WLAN	Domain Index D	omain Name		
		<u>ia.com</u>		8
	-	252752111		-
	Foot Notes 1 Only 3 OUI entries of	an be configured with	'Is Beacon' enabled	

Next, select the EAP types for this profile, in our case we will select EAP-TLS and EAP-SIM.

Notice that upon selecting the EAP-TLS check box, the **Identity Certificate** configuration option becomes available (marked with a red arrow). However, the drop-down list is currently empty because no certificates are defined for the Profile that we have just created. So, the next step is to click the **Certificates** tab on the left menu to define the **Identity Certificate**, and if required the certificate(s) for the Trusted server(s).



ſ

In the **Certificates** menu, add the Identity Certificate to be used by this device and then click the "+" button at the top-right-hand side of the screen to add the Trusted Servers as needed. Once done, we can now return to the Wi-Fi tab where these certificates will now be available to use for our EAP-TLS configuration.

1

Proceeding       All the certificates as needed         Proceeding       Restrictions         Not configured       Mane of accipiton of the certificate         Proceeding       Configured         Proceeding       Configured         Proceeding       Proceeding         Proce Proceeding       Proceeding <th>.8.</th> <th>General Mandatory</th> <th>Certificate 1. Click the "+" button to add</th>	.8.	General Mandatory	Certificate 1. Click the "+" button to add
Not configured   Not		Passcode	all the certificates as needed
Restrictions   Not configured   Not con	~	Not configured	Certificate Name Name or description of the certificate
Not configured   Not	90	Restrictions	WiFi-Intermediate-CA-sta
Wiscanfigured   Wisc configured   Wiscanfigured   Wiscanfigured <t< th=""><th></th><th>Clobal HTTP Provid</th><th>Certificate or Identity Data</th></t<>		Clobal HTTP Provid	Certificate or Identity Data
Web Content Filter   Not configured     Wi-Fi   Not configured   Not configured <td< th=""><th>٧</th><th>Not configured</th><th>PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device</th></td<>	٧	Not configured	PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device
<ul> <li>Not configured</li> <li>Wi-Fi</li> <li>Payload Configured</li> <li>Ventificate was signed by an untrusted issuer</li> <li>Ventificate antonion</li> <li></li></ul>		Web Content Filter	Certificate WiFi-Intermediate-CA-sta
Wi-Fi       1 Payload Configured         Wi-Fi       1 Payload Configured         Wi Not configured       2. Once done, go back to the Wi-Fi tab to continue with the configuration         Wi Not configured       2. Once done, go back to the Wi-Fi tab to continue with the configuration         Wi Not configured       2. Once done, go back to the Wi-Fi tab to continue with the configuration         Wi Not configured       Certificate         Wi Not configured       Certificate Name         Not configured       Mail         Not configured       Certificate Name         Not configured       Not configured         Not configured	<b>∽</b> ₽	Not configured	Expires: Tuesday, December 31, 2024 at
VPN > Details   Wot configured 2. Once done, go back to the Wi-Fi tab to continue with the configuration   With an in the configured With the configured   Wot configured Certificate Name   Wot configured Certificate CA-srv   Wot configured WiFi-Intermediate-CA-srv   Wot configured Thermediate-Ca-srv   Wot configured Thermediate certificate authority   Wot configured Thermediate-Ca-srv   Wot configured Thermediate was signed by an untrusted issuer   Wot configured Certificate Name   Wot configured Name or description of the certificate   Wot configured Mifiuse-pl2   Mot configured Certificate or identity	1	Wi-Fi 1 Payload Configured	© This certificate was signed by an
Not configured       2. Once done, go back to the wirking of the continue with the continue with the configuration         Image: State of the configured       Image: State of the configured         Image: State of the configured       Image: State of the configured         Image: State of the configured       Image: State of the configured         Image: State of the configured       Image: State of the configured         Image: State of the configured       Image: State of the configured         Image: State of the configured       Image: State of the configured         Image: State of the configured       Image: State of the configured         Image: State of the configured       Image: State of the configured         Image: State of the configured       Image: State of the configured         Image: State of the configured       Image: State of the configured         Image: State of the configured       Image: State of the configured         Image: State of the configured       Image: State of the configured         Image: State of the configured       Image: State of the configured         Image: State of the configured       Image: State of the configured         Image: State of the configured       Image: State of the configured         Image: State of the configured       Image: State of the configured         Image: State of the configured       Image: State of the contificate <th>A</th> <th>VPN</th> <th>Untrusted issuer     Details</th>	A	VPN	Untrusted issuer     Details
AirPlay       with the configured         Wat configured       (Certificate Name)         Wat configured       (Certificate CA-srv)         Wat configured       (Certificate authority)         Wat configured       (Certificate authority)         Wat configured       (Certificate authority)         Wat configured       (Certificate Name)         Wat configu		Not configured 2. Once	done, go back to
AirPrint Not configured <ul> <li>Mail Not configured</li> <li>Mail Not configured</li> <li>Cathada ActiveSync Not configured</li> <li>LDAP Not configured</li> <li>Calendar Not configured</li> <li>Calendar Not configured</li> <li>Calendar Not configured</li> <li>Contacts Not configured</li> <li>Subscribed Calendars Not configured</li> <li>Subscribed Calendars Not configured</li> <li>Configured</li> </ul> <ul> <li>Configured</li></ul>		AirPlay the WI-F	configuration
<ul> <li>For Configured</li> <li>Mail Not configured</li> <li>Mail Not configured</li> <li>Change ActiveSync Not configured</li> <li>ChAP Not configured</li> <li>Chandar Not configured</li> <li>Catendar Not configured</li> <li>Contacts Not configured</li> <li>Contacts Not configured</li> <li>Subscribed Calendars Not configured</li> <li>Post configured</li> <li>Configured</li> <li>Contacts</li> <li>Contacts</li></ul>		AirPrint	Certificate - •
Mail Not configured       Name or description of the certificate         Image: Subscription of the certificate Name       Name or description of the certificate         Image: Not configured       Image: Not configured         Image: N		Not configured	
With-Intermediate-CA-srv         Image: Configured         Image: Contacts         Mot configured         Image: Contacts         Image: Contacts         Mot configured         Image: Contacts         Image: Contacts         Image: Contacts         Mot configured         Image: Contacts         Image: Contacts         Image: Contacts         Image: Contacts         Image: Configured         Image: Configured         Image: Configured         Image: Configured         Image: Configured         Image:	1	Mail Not configured	Certificate Name Name or description of the certificate
I contingured       Certificate or identity Data         I configured       PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device         I configured       Image: PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device         I configured       Image: PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device         I configured       Image: PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device         I configured       Image: PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device         I configured       Image: PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device         I configured       Image: PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device         I configured       Image: PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device         I configured       Image: PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device         I configured       Image: PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device         I configured       Image: PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device         I configured       Image: PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device         I configured       Image: PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device         I configured       Image: PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device         I configured       Image: PKCS1 (.cer, etc)		Exchange ActiveSunc	WiFi-Intermediate-CA-srv
LDAP Not configured       PKCS1 (cer, etc) or PKCS12 (p12) files for inclusion on device         WiFi-Intermediate certificate authority Depries: Tuesday, December 31, 2024 at 4:00:00 PM Pacific Standard Time © This certificate was signed by an untrusted issuer         Wob Clips Not configured       This certificate was signed by an untrusted issuer         Web Clips Not configured       Certificate         Point Not configured       Certificate Name         Certificates 4 Payloads Configured       Certificate Name         Scep Not configured       Certificate or identify Data PKCS1 (cer, etc) or PKCS12 (p12) files for inclusion on device         PN Not configured       Prisonal Information Exchange	Eß	Not configured	Certificate or Identity Data
Not configured         WiFi-Intermediate -CA-srv         Intermediate certificate authority         Not configured	0	LDAP	PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device
Calendar       Expires: Tuesday, December 31, 2024 at 400:00 PM Pacific Standard Time         Contacts       Prins certificate was signed by an untrusted issuer         Subscribed Calendars       Image: Contact on figured         Not configured       Certificate was signed by an untrusted issuer         Not configured       Image: Certificate was signed by an untrusted issuer         Not configured       Certificate was signed by an untrusted issuer         Image: Not configured       Certificate was signed by an untrusted issuer         Image: Not configured       Certificate was signed by an untrusted issuer         Image: Not configured       Certificate was signed by an untrusted issuer         Image: Not configured       Certificate was signed by an untrusted issuer         Image: Not configured       Certificate was signed by an untrusted issuer         Image: Not configured       Certificate Name         Image: Not configured       Certificate or dentity Data         Image: Not configured       Personal Information Exchange         Image: Not configured       Certificate or dentity Data         Image: Not configured       Personal Information Exchange		Not configured	Certificate Intermediate certificate authority
Contacts Not configured       O This certificate was signed by an untrusted issuer         Subscribed Calendars Not configured       ► Details         Not configured       ► Certificate was signed by an untrusted issuer         Not configured       ► Certificate was signed by an untrusted issuer         Not configured       ● ① ①         Not configured       ● ①         Certificates 4 Payloads Configured       ● ①         Not configured       Certificate or identity Data PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device         Image: APN Not configured       Personal Information Exchange	æ	Calendar Not configured	Expires: Tuesday, December 31, 2024 at
Wot configured     ► Details       Subscribed Calendars Not configured     ► Details       Image: Subscribed Calendars     Certificate       Not configured     Certificate       Not configured     Certificate Name       Not configured     Certificate Name       Not configured     Certificate Name       Not configured     Certificate Name       Scep     Arayloads Configured       Not configured     Certificate or Identity Data       PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device       Not configured     Certificate or Identity Data       PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device	20	Contacts	This certificate was signed by an
Subscribed Calendars         Not configured         Image: Subscribed Calendars         Not configured         Image: Source Certificates         Image: A Payloads Configured         Image: Scep         Image: Not configured         Image: Scep         Image: Not configured         Image: Not conf		Not configured	Details
Web Clips Not configured       Certificate       ● ●         Font Not configured       Certificate Name       ■         Certificates 4 Payloads Configured       Name or description of the certificate       ●         Mot configured       Wiftuser.p12       ■         Not configured       Certificate or identity Data PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device         Mot configured       Experiment       Personal Information Exchange	1	Subscribed Calendars Not configured	
Not configured       Certificate         Image: Pont Not configured       Certificate Name         Image: Certificates Apply       Name or description of the certificate         Image: Certificates Apply       Minuser.pl2         Image: Certificate Apply       Certificate or Identity Data         PN       Prisonal Information Exchange		Web Clips	
Font Not configured       Certificate Name         Image: Certificates of the certificate of the certificate       Name or description of the certificate         Image: Certificates of the certificate of the certificate of the certificate of the certificate       Name or description of the certificate         Image: Certificates of the certificate of	34.4	Not configured	Certificate 😑 🕀
Certificates       Name or description of the certificate         Vertificates       Vertificate or description of the certificate         Vertificates       Vertificate or dentity Data         Provide       Provide or PKCS1 (cert, etc) or PKCS12 (p12) files for inclusion on device         Vertificate       Personal Information Exchange	F	Font Not configured	
		Certificates	Certificate Name Name or description of the certificate
SCEP         Certificate or identity Data           Not configured         PKCS1 (.cer, etc) or PKCS12 (.p12) files for inclusion on device           APN         Resonant Presonal Information Exchange           Not configured         Certificate		4 Payloads Configured	wifiuser.p12
APN Not configured  PRCS1 (cer, etc) or PRCS12 (p12) miles for inclusion on device  Personal Information Exchange  Concel  Sum		SCEP Not configured	Certificate or Identity Data
Not configured Centification Personal Information Exchange		APN	FRC51 (.cer, etc) of FRC512 (.p12) files for inclusion on device
Cancel Saue		Not configured	Certificate Control
Calcel			Cancel

Select the **Identity Certificate** and then click the **Trust** tab to select the trusted servers. This concludes the minimum required configuration for EAP-TLS.



ſ

For EAP-SIM, it is possible to define the MCC/MNC values for the operator(s) as shown in the following screen:

1

1 Payload Configured	Configures network to appear as legacy or Hotspot 2.0						
VPN Not configured	Hotspot 2.0 ÷						
Not compared	Displayed Operator Name						
AirPlay	Name of the Hotspot 2.0 service provider						
Not configured	Cisco Hostpot2.0						
AirPrint	Domain Name						
Not configured	Domain name of the Hotspot 2.0 service provider						
Mail	cisco.com						
Not configured	Roaming Consortium Ols						
Exchange ActiveSync	Roaming Consortium Organization Identifiers						
Not configured							
LDAP							
Not configured							
Calendar	+ -						
Not configured	NAI Pealm Names						
Contacts	Network Access Identifier Realm Names						
Not configured							
Subscribed Calendars							
Not configured							
Web Clips	+ -						
Not configured	MCC/MNCs						
Font	Mobile Country Code and Mobile Network Configuration						
Not configured	MCC MNC						
Certificates	310 120 <i>Click the "+" button to</i>						
4 Payloads Configured	add the MCC/MNC						
SCEP	value(s) as needed						
Not configured	+						
APN	Allow connecting to roaming partner networks						
Not configured							

On the WLC, the MCC/MNC values are defined under the 3GPP CI as shown in the following screen:

ululu cisco	MONITOR WLANS CO	NTROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Si FEEDBACK	a⊻e Configuration   <u>P</u> ing	Logout <u>R</u> efresh
WLANs	802.11u Parameters							< Back	Apply
VLANs WLANs	WLAN SSTD H	52.0							
Advanced	802.11u Status	Enabled							
	802.11u General Par	rameters			Realm L	list			
	Internet Access	Enabled		Realm Realm Index 1 =	1 : Add				
	Network Type	Chargeable Public Network	+		Realm In	ndex		Realm Name	
	Network Auth Type HESSID	Not Configured 0:00:00:00:00:00	\$		Cellular	Network	Inforamation Lis	st	
	IPv4 Type Unknown Country C	Country Code CellularIndex 3 : Network Code Add							
	IPv6 Type	Unknown =			Cellular	Index	Country Cod	le Network Co	de
	OUI List		1 310 410	410					
	IUO	Is Beacon 🕹 📄 🛛 OUI In	dex 1 :	Add	2		310	120	٥
	OUI Index 0	OUI Name Is B	eacon						
	Domain List								
	Domain Name		Domain Index	3 ÷ Add	I				
	Domain Index Don	nain Name							
	1 <u>usa</u>	.com							
	Foot Notes	he configured with 'Is Beau	on' coshied						

Finally, to import the Profile into the iPhone 5, you can use any of the five methods described earlier in this section. Two of the simplest methods available are via email or USB.

The following screenshot illustrates how to export the Profile created into an XML file, and then later email it to the device.



Below is an illustration of how to use a USB connection to push the Profile to an iPhone 5.



ſ

The imported Profiles on the device can be viewed from **Settings > General > Profile**. Once the Profile has been imported to the iPhone 5, and if no remembered user-defined Wi-Fi networks are in range, the general operation of an Apple device configured to auto join a HS2.0 wireless network is as follows:

- 1. The device performs an active scan.
- 2. BSSIDs with HS2.0 IE in the probe response are queried using ANQP.
- **3.** The device compiles a list of the BSSIDs for which it has credentials, then it authenticates the best candidate based on home operator versus roaming partner (NAI, 3GPP, or Roaming OI).
- 4. Within each category the device will make a decision similar to non HS2.0 legacy networks based on the band and RSSI.

Sprint 3G 1:07 AM 7 %      Settings General	Settings Wi-Fi	<b>-</b> 7 % <b></b> >				
Restrictions Off			✓ Wi-Fi	HS2.0		
	Wi-Fi		Note the missin option when au	g "Forget this Network" to-connected by HS2.0!		
Date & Time	HS2.0		IP ADDRESS			
Keyboard			DHOP	Boote Static		
International	CHOOSE A NETWORK		IP Address	10.11.23.24		
	adminnet	ê 🕈 🚺	Subnet Mask	255.255.255.0		
iTunes Wi-Fi Sync	Les	ê 🕈 🚺	Router	10.11.23.1		
VPN Not Connected	Love	ê 🗢 🚺	DNS	8.8.8.8		
Profile MyHotSpot2.0	Other		Search Domai	ins		
The Profile is installed			Client ID			
Reset	Ask to Join Networks	$\bigcirc$				
	Known networks will be joined If no known networks are avait have to manually select a networks	l automatically. lable, you will vork.	Renew Lease			
	1		HTTP PROXY			

<u>Note</u>

Unlike the Samsung implementation, the Apple device will not show a special icon indicating if the connection is to a home versus a roaming partner network. Furthermore, the only clues of the connection being connected via Hotspot 2.0 is the "Displayed Provider Name" message below the SSID, and lack of the "Forget the Wireless Network" option if the user displays the details of the connected WLAN.