

Cloudpath

Enrollment System

Configuring Cloudpath to Support Hotspot 2.0 Release 2 (Passpoint)

Software Release 5.1

May 2017

Summary: This document describes how to configure a Ruckus SmartZone controller and the Cloudpath system to support enrollment using Hotspot 2.0 Release 2 (Passpoint).

Document Type: Configuration

Audience: Network Administrator



Configuring Cloudpath to Support Hotspot 2.0 R2

Software Release 5.1

May 2017

Copyright © 2017 Ruckus Wireless, Inc. All Rights Reserved.

This document contains Ruckus Wireless confidential and proprietary information. It is not to be copied, disclosed or distributed in any manner, in whole or in part, without express written authorization of a Customer Advocacy representative of Ruckus Wireless, Inc. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing, RUCKUS WIRELESS PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

ZoneFlex™, BeamFlex™, MediaFlex™, ChannelFly™, and the Ruckus Wireless logo are trademarks of Ruckus Wireless, Inc. All other brands and product names are trademarks of their respective holders.

Copyright © 2017 Ruckus Wireless, Inc. All rights reserved.

Cloudpath Hotspot 2.0 R2 (Passpoint) Configuration Guide

Passpoint Overview

Hotspot 2.0 (HS 2.0), often referred to as Wi-Fi Certified Passpoint, is the new standard for Wi-Fi public access that automates and secures the connection.

Passpoint Release 1

Release 1 of HS 2.0 was based on the IEEE 802.11u standard and introduced new capabilities for automatic Wi-Fi network discovery, selection and 802.1X authentication based on the Access Network Query Protocol (ANQP).

Passpoint Release 2

Release 2 is largely focused on standardizing the management of the credentials; how they are provisioned, how they are stored on the device, how they are used in network selection, and how long they are valid. Some of these capabilities aren't applicable to cellular credentials (SIM/USIM), because those are provisioned by the home mobile network operator (MNO) and are themselves the stored credential.

In Release 2 mobile devices use Online Sign-Up (OSU) to accomplish registration and credential provisioning to obtain secure network access. Each Service Provider network has an OSU Server, an AAA Server, and access to a certificate authority (CA). The CA is known by two attributes: its name and its public key.

One of the requirements for a mobile device and the hotspot to trust each other is that OSU Server shall hold a certificate signed by a Certificate Authority whose root certificate is issued by one of the CAs authorized by Wi-Fi Alliance, and that these trust root CA certificates are installed on the mobile device.

All certificates for Release 2 of the Passpoint program are governed by the Hotspot 2.0 Online Sign-Up Certificate Policy Specification. An OSU server certificate should be obtained from any of the CAs authorized by Wi-Fi Alliance.

Prerequisites

To configure passpoint with your Cloudpath system, you need a Hotspot 2.0 WWW certificate with Common Language icon embedded, signed by a certified Hotspot 2.0 Root CA.

Devices That Support Passpoint

At the time of the Cloudpath 5.1 release, this device supported Hotspot 2.0 Release 2:

- Samsung Galaxy S5, running OS 4.4.2, kernel version 3.4.0-2727827eng, built number kltextx-eng 4.4.2 KOT49H G900FXXUTAMK6 test-keys.

Note >>

Reportedly, Windows 10 support Hotspot 2.0 R2, but it does not support the open browser command, and it only supports the PEAP EAP method. Therefore, Cloudpath 5.1 cannot support Windows 10 devices with a passpoint configuration.

Controller Configuration

Passpoint is supported on the Ruckus Virtual SmartZone (vSZ) controller, version 3.2.1.0.245.

Controller Configuration Summary

The following is a list of configuration steps on the vSZ controller:

- Configure AAA Services
- Configure Hotspot 2.0 Wi-Fi Operator Profile
- Configure Hotspot 2.0 Identity Provider
- Configure Guess Access Portal
- Configure Onboarding SSID
- Configure Hotspot 2.0 Profile
- Configure Secure SSID

Configure AAA Services

There are several places on the vSZ controller to configure AAA services. Be sure to configure them under Services.

1. Navigate to *Configuration > Service and Profiles > Services* to configure AAA Authentication and Accounting Services
2. For the AAA Authentication server, use the IP address of the Cloudpath system and port 1812.
3. For the AAA Accounting server, use the IP address of the Cloudpath system and port 1813.
4. The Shared Secret must match the shared secret for the Cloudpath onboard RADIUS server. (*Configuration > Advanced > RADIUS Server*).
5. Leave the default values for the remaining fields, and *Apply* changes.

Configure Hotspot 2.0 Wi-Fi Operator Profile

FIGURE 1. Wi-Fi Operator Profile

The screenshot shows the configuration interface for a Wi-Fi Operator Profile. The title bar reads "Edit Hotspot 2.0 Wi-Fi Operator Profile: [Anna40 WiFiOperator]". The form contains the following sections:

- Name:** A text field containing "Anna40 WiFiOperator".
- Description:** An empty text field.
- Domain Names:** A section with a "Domain Name *" input field, "Add", and "Cancel" buttons. Below it is a table with one entry:

| Domain Name ▲ | |
|---------------|--|
| cloudpath.net | |
- Signup Security:** A checkbox labeled "Support Anonymous Authentication (OSEN)" which is checked.
- Certificate:** A dropdown menu showing "[?] * No data available" and a "Create New" button.
- Friendly Names:** A section with a "Language *" dropdown (set to "English") and a "Name *" input field, with "Add" and "Cancel" buttons. Below it is a table with one entry:

| Language ▲ | Name | |
|------------|-----------------------|--|
| English | Anna 40 Wi-Fi Service | |

At the bottom of the form are "Apply" and "Cancel" buttons.

1. Navigate to *Configuration > Service and Profiles > Service Profiles > Hotspot 2.0 Wi-Fi Operator*.
2. Enter a *Name* for the Wi-Fi Operator profile.
3. Add the *Domain Name* for the Cloudpath system.
4. Select a *Language*, and Add the *Friendly Name* for the Cloudpath system. You can enter multiple languages for the same Friendly Name.

Note >>

The Friendly Name in the vSZ controller must match the Friendly Name in the Hotspot 2.0 WWW certificate on the Cloudpath system.

5. Leave the default values for the remaining fields, and *Apply* changes.

Configure Hotspot 2.0 Identity Provider

Navigate to *Configuration > Service and Profiles > Service Profiles > Hotspot 2.0 Identity Provider*.

The Hotspot Identity Provider consists of the following information:

- Network Identifier
- Online Signup & Provisioning
- AAA Authentication
- AAA Accounting

Configure Network Identifier

FIGURE 2. Network Identifier

The screenshot shows the configuration interface for a Hotspot 2.0 Identity Provider. The title bar reads "Edit Hotspot 2.0 Identity Provider: [Anna40 Identity Provider]". Below the title bar is a navigation menu with tabs: "Network Identifier" (selected), "Online Signup & Provisioning", "Authentication", "Accounting", and "Review".

The main configuration area is divided into several sections:

- Name:** A text field containing "Anna40 Identity Provider".
- Description:** An empty text field.
- PLMNs:** Fields for "MCC *" and "MNC *". Below these is a table with columns "MCC" and "MNC".
- Realms:** A section containing:
 - Name:** A text field.
 - Encoding:** A dropdown menu set to "RFC-4282".
 - EAP Methods:** Four checkboxes labeled "#1", "#2", "#3", and "#4".
 - EAP Method:** A dropdown menu set to "N/A".
 - A table listing EAP methods:

| Name | Encoding | EAP Methods |
|---------------|----------|----------------------------------------------|
| cloudpath.net | RFC-4282 | #1: EAP-TLS #2: N/A #3: N/A #4: N/A |
- Home Ols:** Fields for "Name *", "Length *", and "Organization ID *". Below these is a table with columns "Name", "Length", and "Organization ID".

At the bottom of the form are "Next" and "Cancel" buttons.

1. On the *Network Identifier* tab, Enter a *Name* for the Identity Provider.
2. Enter the *Realm* for the Cloudpath system, and *EAP Method* for the Identity Provider. You can enter multiple EAP Methods for the same Realm.
3. Leave the default values for the remaining fields, and click *Next* to apply changes and continue with Online Signup & Provisioning.

Configure Online Signup & Provisioning

FIGURE 3. Online Signup & Provisioning

Enable Online Signup & Provisioning

Provisioning Options

Provisioning Service: Internal External Service URL: * https://anna40.cloudpath.net/passpoint/Ann

Provisioning Protocol: * OMA-DM SOAP-XML

Online Signup Options

OSU NAI Realm: * cloudpath.net

Common Language Icon: * Anna 40 W-Fi Browse

OSU Service Description: * Language * Friendly Name * Description Icon Browse Add Cancel

| Language ▲ | Friendly Name | Description | Icon | Format | Width | Height | |
|------------|-----------------------|-------------|------|--------|-------|--------|----|
| English ▼ | Anna 40 Wi-Fi Service | | | | | | 🗑️ |

Whitelisted Domains: Domain Name * Add Cancel

| Domain Name ▲ | |
|----------------|----|
| cloudpath.net | 🗑️ |
| google.com | 🗑️ |
| www.google.com | 🗑️ |

Back Next Cancel

1. On the Online Signup & Provisioning tab, enable *Online Signup & Provisioning*.
2. Select External Provisioning Service and enter the Service URL. The Service URL on the controller must match the Passpoint OSU URL displayed on the Cloudpath system *Deploy* page (Configuration > Deploy).
3. Enter the *OSU NAI Realm* of the Cloudpath system.

Note>>

The Realm of the Cloudpath system should be consistent throughout the Identity Provider configuration.

4. Upload the *Common Language Icon*. This is the icon embedded in the Hotspot 2.0 WWW certificate on the Cloudpath system. Support file size = 64x64 pixels, file type = PNG.
5. Add one or more *Languages* for the *Friendly Name*. The Friendly Name must match the Friendly Name in the Hotspot 2.0 WWW certificate on the Cloudpath system.
6. Add one or more *Whitelisted Domains*. The domain of the Cloudpath system must be included.

7. Leave the default values for the remaining fields, and click *Next* to apply changes and continue with Authentication.

Authentication Services for Access WLAN

FIGURE 4. AAA Authentication Services

Edit Hotspot 2.0 Identity Provider: [Anna40 Identity Provider]

Network Identifier -> Online Signup & Provisioning -> **Authentication** -> Accounting -> Review

Authentication Services for Access WLAN

Realm * Auth Service * Dynamic VLAN ID

 No data available Add Cancel

| Realm | Protocol | Auth Service | Dynamic VLAN ID |
|---------------|----------|-----------------|----------------------|
| cloudpath.net | RADIUS | Anna40 AAA Auth | <input type="text"/> |
| No Match | RADIUS | Anna40 AAA Auth | <input type="text"/> |
| Unspecified | RADIUS | Anna40 AAA Auth | <input type="text"/> |

Note: If device onboarding was done with credential type 'remote', then map your 'realm' value to its respective authentication service PLUS define 'Unspecified' realm & map it to corresponding authentication service to properly handle legacy (non-Hotspot 2.0) devices.

Back Next Cancel

1. On the Authentication tab, add one or *Realms* for RADIUS authentication. Enter an authentication service for the Cloudpath system realm, for systems that do not match the Cloudpath realm, and for unspecified realms.
2. Specify the Authentication server previously configured in Authentication Services.
3. Specify the RADIUS protocol.
4. Leave the default values for the remaining fields, and click *Next* to apply changes and continue with Accounting.

Accounting Services for Access WLAN

FIGURE 5. AAA Accounting Services

Edit Hotspot 2.0 Identity Provider: [Anna40 Identity Provider]

Network Identifier -> Online Signup & Provisioning -> Authentication -> **Accounting** -> Review

Enable Accounting

Accounting Services for Access WLAN

Realm * Accounting Service *

 Add Cancel

| Realm | Accounting Service |
|---------------|--------------------|
| cloudpath.net | Anna40 AAA Acct |
| No Match | Anna40 AAA Acct |
| Unspecified | Anna40 AAA Acct |

Note: A realm to service mapping define the accounting service for each of the realm specified in this table. When the accounting service for a particular realm is 'NA', then accounting is disabled.

Back Next Cancel

1. On the Accounting tab, enable *Accounting*.
2. Add one or Realms for RADIUS accounting. Enter an accounting service for the Cloudpath system realm, for systems that do not match the Cloudpath realm, and for unspecified realms.
3. Specify the Accounting server previously configured in Accounting Services.
4. Leave the default values for the remaining fields, and click *Next* to apply changes and continue with Accounting.

Review Identity Provider Configuration

On the Review tab, verify the Identity Provider configuration and *Apply* changes.

Configure Guess Access Portal

Navigate to your AP Zone for Zone Configuration.

Configure Guest Access Portal

This the portal for iOS devices.

FIGURE 6. Guest Access Portal

Edit Guest Access Portal: [Anna Guest Portal] of zone [KEVIN-HS2-ZONE]

General Options

Portal Name: * Anna Guest Portal

Portal Description:

Language: * English

Redirection

Start Page:

After user is authenticated.

Redirect to the URL that user intends to visit.

Redirect to the following URL:

*

Guest Access

Guest Pass SMS Gateway: * Disabled

Terms and Conditions: Show Terms and Conditions

Terms of Use

By accepting this agreement and accessing the wireless network, you acknowledge that you are of legal age, you have read and understood, and agree to be bound by this agreement.
(*) The wireless network service is provided by the property owners and is completely at their discretion. Your access to the network may be blocked, suspended, or terminated at any time for any reason.
(*) You agree not to use the wireless network for any purpose that is unlawful or otherwise prohibited and you are fully responsible for your use.
(*) The wireless network is provided "as is" without warranties of any kind, either expressed or implied.

Web Portal Logo: Upload your logo to display it on the web portal pages. The recommended image size is 138 x 40 pixels and the maximum file size is 20KB. Select an image file to

Web Portal Title: Welcome to the Guest Access login page.

User Session

Session Timeout: * 1440 Minutes (2-14400)

Grace Period: * 60 Minutes (1-14399)

1. Enter a *Portal Name* and *Description*.
2. The *Start Page* must be *Redirect to the URL that the user intends to visit*.
3. Disable *Guest Pass SMS Gateway*.
4. Optional. Enter a *Web Portal Logo*.
5. Enter a *Web Portal Title*.
6. Leave the default values for the remaining fields, and *Apply* changes.

Configure Onboarding SSID

FIGURE 7. Onboarding SSID

Edit WLAN Config: [Anna40 Onboarding] of zone [KEVIN-HS2-ZONE]

General Options

Name:

SSID:

HESSID:

Description:

WLAN Usage

Access Network: Tunnel WLAN traffic through Ruckus GRE

Authentication Type: Standard usage (For most regular wireless networks)

Hotspot (WISPr)

Guest Access + Hotspot 2.0 Onboarding

Web Authentication

Hotspot 2.0 Access

Hotspot 2.0 Secure Onboarding (OSEN)

WeChat

Authentication Options

Method: Open 802.1x EAP MAC Address

Encryption Options

Method: WPA2 WPA-Mixed WEP-64 (40 bits) WEP-128 (104 bits) None

Guest Access Portal

Guest Portal Service:

Bypass CNA: Enable

Guest Authentication:

Guest Accounting: Use the controller as proxy

Online Signup/Onboarding Service

Hotspot 2.0 Online Signup: Hotspot 2.0 devices

Zero-IT Onboarding: Non-Hotspot 2.0 devices (i.e., legacy devices) and Hotspot Release 1 devices

Onboarding Portal: [Create New](#)

Authentication Services

| Service * | Credential Store * | Realm * [?] | Local Credential Expiration | |
|------------------------------------------------|-------------------------------------------|------------------------------------------------|-------------------------------|-----------------------------------|
| <input type="text" value="No data available"/> | <input type="text" value="Local"/> | <input type="text" value="No data available"/> | <input type="text" value=""/> | Day <input type="text" value=""/> |
| <input type="button" value="Add"/> | <input type="button" value="Create New"/> | <input type="button" value="Cancel"/> | | |
| Service ▲ | Protocol | Credential Store | Realm | Local Credential Expiration |
| | | | | |

Options

Wireless Client Isolation: Disable

Enable (Isolate wireless client traffic from all hosts on the same VLAN/subnet)

Priority: High Low

RADIUS Options

Advanced Options

1. Name the onboarding SSID.
2. Authentication Type must be *Guest Access + Hotspot 2.0 Onboarding*.
3. Authentication Method must be *Open*.
4. Encryption Method must be *None*.

5. Select the *Guest Portal Service* previously configured.
6. Enable *Bypass CNA*.
7. Select *Hotspot 2.0 devices*.
8. Leave the default values for the remaining fields, and *Apply* changes.

Configure Hotspot 2.0 Profile

FIGURE 8. Hotspot 2.0

Edit Hotspot 2.0 WLAN Profile: [Anna40 Profile] of zone [KEVIN-HS2-ZONE]

Name: * Anna40 Profile

Description:

Operator: * Anna40 WiFiOperator

Identity Providers: * Identity Provider * No data available

You can configure Onboarding SSID when you add an identity provider which enable Online Signup & Provisioning

| Identity Provider | Online Signup Service | Default |
|--------------------------|-------------------------------------------------------------|----------------------------------|
| Anna40 Identity Provider | https://anna40.cloudpath.net/passpoint/Anna40TestBVT/Pro... | <input checked="" type="radio"/> |

Onboarding SSID: [?] * Anna40 Onboarding

1. *Name* the Hotspot 2.0 profile.
2. Select the previously configured *Wi-Fi Operator*.
3. Add the previously configured Identity Provider.
4. Select the previously configured *Onboarding SSID*.
5. Leave the default values for the remaining fields, and *Apply* changes.

Configure Secure SSID

FIGURE 9. Secure SSID

Edit WLAN Config: [Anna40 H52R2 Secure] of zone [KEVIN-H52-ZONE]

General Options

Name: * Anna40 H52R2 Secure
 SSID: * Anna40 H52R2 Secure
 HESSID:
 Description:

WLAN Usage

Access Network: Tunnel WLAN traffic through Ruckus GRE
 Authentication Type: * Standard usage (For most regular wireless networks)
 Hotspot (WISPr)
 Guest Access + Hotspot 2.0 Onboarding
 Web Authentication
 Hotspot 2.0 Access
 Hotspot 2.0 Secure Onboarding (OSEN)
 WeChat

Authentication Options

Method: * Open 802.1x EAP MAC Address

Encryption Options

Method: * WPA2 WPA-Mixed WEP-64 (40 bits) WEP-128 (104 bits) None
 Algorithm: * AES AUTO (TKIP+AES)
 802.11w MFP: * Disabled Capable Required

Hotspot 2.0 Profile

Hotspot 2.0 Profile: * Anna40 Profile
 Authentication Service: Enable RFC 5580 Location Delivery Support
 Accounting Service: * Send interim update every Minutes (0-1440)

Options

Wireless Client Isolation: * Disable
 Enable (Isolate wireless client traffic from all hosts on the same VLAN/subnet)
 Priority: * High Low
 Zero-IT Activation: Enable Zero-IT Activation (WLAN users are provided with a wireless configuration installer after they log on)

RADIUS Options

Advanced Options

Apply Cancel

1. Name the secure SSID.
2. Authentication Type must be *Hotspot 2.0 Access*
3. Authentication Method must be *802.1x EAP*.
4. Encryption Method must be *WPA2*.
5. Select the previously configured *Hotspot 2.0 Profile*.
6. Leave the default values for the remaining fields, and *Apply* changes.

Cloudpath Configuration

The Cloudpath configuration for passpoint consists of setting up the workflow, device configuration settings, certificate settings, and home service provider, subscriber, and policy settings.

Prerequisites

- The web server certificate must be signed by a Hotspot 2.0 Root CA and must contain the Common Language Icon. Icon size = 64 x 64 pixels. Icon file type = PNG.
- The RADIUS server certificate must also be signed by the Hotspot 2.0 Root CA.

Cloudpath Configuration Summary

- Workflow with Passpoint Configuration
- Passpoint Device Configuration
- Device Configuration Passpoint Settings

Workflow with Passpoint Configuration

Design a workflow for Passpoint.

The Result step must include a device configuration that includes the secure SSID configured on the controller, and the certificate template must include the Common Name Pattern with the same realm as configured in the controller.

FIGURE 10. Passpoint Workflow

The screenshot shows the 'Configuration > Workflows' page. At the top right is an 'Add Workflow' button. Below is a table listing workflows:

| Workflows | Status | Enrollment Portal URL | Last Publish Time |
|---------------|-----------|--------------------------------------|-------------------|
| Passpoint | Published | /enroll/Anna42TestBVT/Passpoint/ | 20170504 1316 MDT |
| NewProduction | Published | /enroll/Anna42TestBVT/NewProduction/ | 20170504 1316 MDT |

Below the table are tabs for 'Properties', 'Enrollment Process', 'Look & Feel', 'Snapshot(s)', and 'Advanced'. The 'Enrollment Process' tab is active, showing a sequence of steps:

- Step 1: Require the user to accept the AUP **Welcome Message and AUP**
- Step 2: All matches in: Employees, Visitors, **Passpoint**
- Step 3: **Prompt the user** for credentials from **Anna42 Test BVT AD**
- Result: Move user to **PasspointSecure** and assign certificate using **username@passpoint.c...**

A tooltip is visible over the result text, showing certificate details:

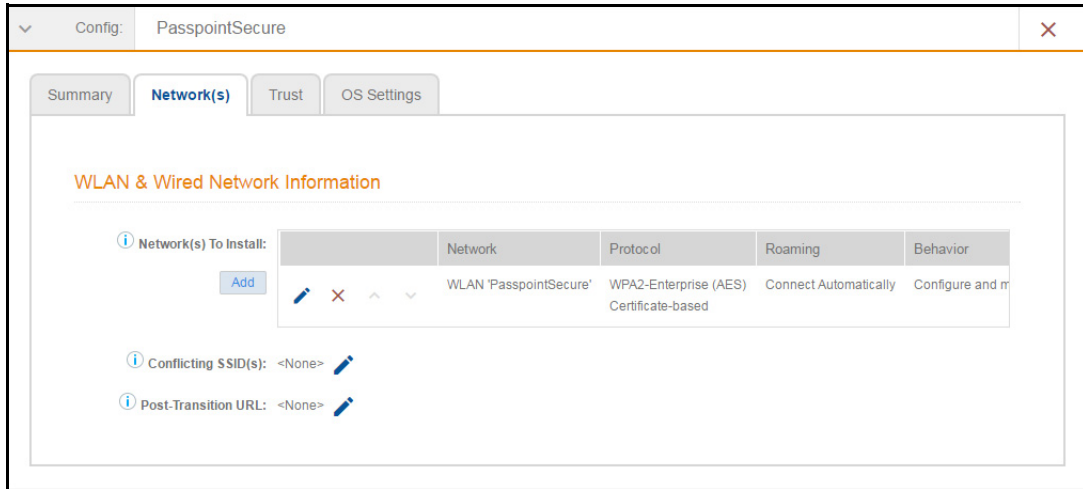
- Name: username@passpoint.company.com
- Issuing CA: Anna42 Test BVT
- Intermediate CA 1
- CN Pattern: \${USERNAME}@passpoint.company.com
- Valid Until: +1 Years

Passpoint Device Configuration

WLAN Settings

The WLAN settings for the device configuration must match the EAP Method specified in the controller Identity Profile, and include a Traditional SSID Type.

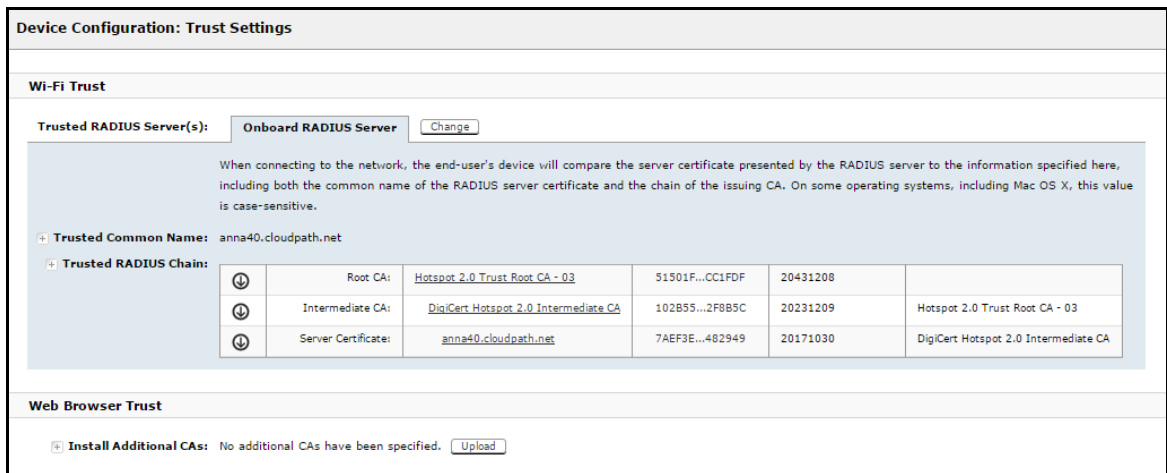
FIGURE 11. Device Configuration WLAN Settings



RADIUS Certificate Trust Settings

The RADIUS server certificate must be signed by the same Hotspot 2.0 Root CA that signs the web server certificate.

FIGURE 12. RADIUS Certificate Trust Settings



Certificate Template Settings

The certificate template Common Name must include the domain name that is specified in the Controller Realm setting.

Certificate Template Settings

Template 4: Onboard template `username@hs2r2.cloudpath.net`

Common Name: `${USERNAME}@hs2r2.cloudpath.net`
CA Type: Onboard
CA Reference Name: Anna40 Test BVT Intermediate CA I
CA Common Name: Anna40 Test BVT Intermediate CA I

Chain:

| | Name | Notes | Expires |
|---|-----------------------------------|-------|----------|
| 🔍 | Anna40 Test BVT Intermediate CA I | | 20361107 |
| 🔍 | Anna40 Test BVT Root CA I | | 20361107 |

Notifications: No notifications currently exist.

SCEP Keys: No SCEP keys currently exist.

Device Configuration Passpoint Settings

The passpoint settings include configuration for the Home Service Provider, the Subscription Server, and the Policy Server.

To configure passpoint settings on the Cloudpath system, select the *Passpoint* tab on the Hotspot 2.0 device configuration.

Configure Home Service Provider

FIGURE 13. Home Service Provider Settings

Modify Home SP

Home SP

Friendly Name:

FQDN:

Realm:

EAP Method:

Advanced Home SP Configuration

Network IDs:

+

Home OIs:

+

Other Home Partners:

+

Icon URL:

1. The Friendly Name must match the Friendly Name in the Hotspot 2.0 WWW certificate.
2. The FQDN of the Cloudpath system.
3. The Realm must match the realm of the Cloudpath system.
4. The EAP Method for the Hotspot 2.0 configuration.

Configure Subscription Server

FIGURE 14. Subscription Server Settings

The screenshot displays the 'Modify Subscription' configuration window. At the top right, there are 'Cancel' and 'Save' buttons. The main section is titled 'Subscription Update Server' and contains two radio button options:

- Use this server.** (Selected): The end-user device will query this server for subscription updates. Below this is a 'Subscription Update Configuration' box containing:
 - Update Interval:** 10080 Minutes *
 - Restriction:** Unrestricted (dropdown menu)
- Use an external server.** (Unselected): The end-user device will query an external server for subscription updates.

Below these options is a section titled 'Advanced Subscription Configuration' with the following fields:

- Type of Subscription:** [ex. Gold]
- Data Limit:** [ex. 1000] Megabytes
- Time Limit:** [ex. 86600] Minutes
- Usage Time Period:** [ex. 86600] Minutes

Configure Policy Server

FIGURE 15. Policy Server Settings

Modify Policy
Cancel Save

Policy Update Server

Use this server.
The end-user device will query this server for policy updates.

Policy Update Configuration:

+ **Update Interval:** **Minutes ***

+ **Restriction:**

Use an external server.
The end-user device will query an external server for policy updates.

Do not use a policy update server.
The end-user device will not query a server for policy updates.

▼ **Advanced Policy Configuration**

+ **Preferred Roaming Partner List:**

+

+ **Minimum Backhaul Threshold:**

+

+ **SP Exclusion List:**

+

+ **Required Protocol/Port:**

+

Maximum BSS Load Value:

Testing the Passpoint Configuration

This Hotspot 2.0 R2 configuration was tested on a Samsung Galaxy S5, running OS 4.4.2, kernel version 3.4.0-2727827eng, built number kltexx-eng 4.4.2 KOT49H G900FXXUTAMK6 test-keys.

To test your configuration, use these example enrollment steps:

1. Enable Passpoint on the device.
2. The device should display *New Passpoint available. Click to subscribe.*

3. Tap to subscribe. You should see the *Friendly Name* of the Cloudpath system previously configured.
4. Tap the Cloudpath system Friendly Name.
5. The device connects to the onboarding SSID, which redirects to the Cloudpath enrollment portal.
6. Run through the enrollment process, which includes, in this example, an AD login step.
7. The configuration is installed on the device, and the device connects to the secure SSID.

Troubleshooting the Cloudpath Passpoint Configuration

This section describes issues to consider when testing or troubleshooting Cloudpath servers that have been configured for Passpoint.

Hotspot 2.0 Root CA

Your Hotspot 2.0 root CA must be issued by one of the CAs authorized by Wi-Fi Alliance.

Note >>

Refer to the Wi-Fi Alliance website, <http://www.wi-fi.org/certification/certificate-authority-vendors>.

Each OSU Server has a certificate signed by a Certificate Authority whose root certificate is trusted by the connection manager of the mobile device. Passpoint Release 2 mobile devices possess the Trust Root certificates from all of the authorized Trust Root CAs. As such, mobile devices can properly validate an OSU server certificate and its metadata (friendly name and icon). This insures the integrity and security of the OSU process

Icon Embedded in the Certificate

The web server certificate for your Cloudpath system must use a Hotspot 2.0 WWW certificate with an embedded Common Language icon.

Use PNG-encoded icon images because the Hotspot 2.0 Release 2 specification mandates all mobile devices accept this format. Image sizes up to a maximum of 65,535 bytes are permitted, but we recommend using images having a small file size to conserve air time when delivering the image to a mobile device.

The exact same image file provided in the CSR is also provided to the Hotspot Operator. This is because the CA puts a hash of the icon file in the OSU server certificate and the mobile device computes the hash of the icon delivered by a Hotspot Operator's AP—if the hashes don't exactly match, the mobile device aborts the OSU process.


Certificate Template EKU

Be sure that the certificate template in your passpoint configuration has the Hotspot 2.0 Auth-1.3.6.1.4.1.40808.1.1.2 EKU setting checked.

FIGURE 16. Modify Certificate Template

Policy - RADIUS Attributes

Allow Authentication via RADIUS :



When a device authenticates using a certificate from this template, Cloudpath will return RADIUS attributes based on the information below.

These attributes may be used to apply a dynamic VLAN, an ACL, or other connection policies.

Reply Username: Certificate Common Name (Default) ▼

Allowed SSID(s): *

VLAN ID: 1

Filter ID: [ex. BYOD]

Class: [ex. BYOD]

Reauthentication: [ex. 86400] **Seconds**

+

▶ **Certificate Strength**

▶ **Organization Information**

▼ **Advanced Settings**

Certificate Type: User + Device ▼

Email Pattern: _____

SAN Other Name Pattern: _____

SAN RFC822 Pattern: _____

SAN DNS Name Pattern: _____

SAN URL Pattern: _____

SAN IP Pattern: _____

SAN RID Pattern: _____

Title Pattern: _____

| EKUs: | Status | EKU Name |
|-------------------------------------|-------------------------------------|------------------------------------------|
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Hotspot 2.0 Auth-1.3.6.1.4.1.40808.1.1.2 |
| <input type="checkbox"/> | <input type="checkbox"/> | Microsoft Server ECU-1.3.6.1.5.5.7.3.2 |
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Microsoft Client ECU-1.3.6.1.5.5.7.3.2 |

▶ **Cleanup**