

Cloudpath Enrollment System for Hotspot 2.0 (Passpoint) Release 2 Configuration Guide, 5.12

Supporting Cloudpath Software Release 5.12

© 2023 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see <https://www.commscope.com/trademarks>. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

Passpoint Overview	5
Passpoint Release 1.....	5
Passpoint Release 2.....	5
Prerequisites.....	5
Devices That Support Passpoint.....	5
Controller Configuration	7
Controller Configuration Summary.....	7
Configure AAA Services.....	7
Configure Hotspot 2.0 Wi-Fi Operator Profile.....	8
Configure Hotspot 2.0 Identity Provider.....	8
Configure Network Identifier.....	9
Configure Online Signup & Provisioning.....	10
Authentication Services for Access WLAN.....	11
Accounting Services for Access WLAN.....	11
Review Identity Provider Configuration.....	12
Configure Guest Access Portal.....	12
Configure Onboarding SSID.....	13
Configure Hotspot 2.0 Profile.....	14
Configure Secure SSID.....	15
Cloudpath Configuration	17
Prerequisites.....	17
Cloudpath Configuration Summary.....	17
Enabling Passpoint on the Cloudpath System.....	17
Workflow for Passpoint Configuration.....	19
Device Configuration Passpoint Settings.....	19
Enable Passpoint for the Device Configuration.....	19
Configure Home Service Provider.....	20
Configure Subscription Server.....	21
Configure Policy Server.....	22
Additional Passpoint Settings.....	23
WLAN Settings.....	23
RADIUS Certificate Trust Settings.....	23
Certificate Template Settings.....	24
Testing the Passpoint Configuration	25
Troubleshooting the Cloudpath Passpoint Configuration	27
Hotspot 2.0 Root CA.....	27
Icon Embedded in the Certificate.....	27
Certificate Template EKU.....	27

Passpoint Overview

- [Passpoint Release 1](#)..... 5
- [Passpoint Release 2](#)..... 5
- [Prerequisites](#)..... 5
- [Devices That Support Passpoint](#)..... 5

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, build number kltexx-eng 4.4.2 KOT49H G900FXXUTAMK6 test-keys.

Passpoint Overview

Devices That Support Passpoint

NOTE

Reportedly, Windows 10 supports 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

- Controller Configuration Summary..... 7
- Configure AAA Services..... 7
- Configure Hotspot 2.0 Wi-Fi Operator Profile..... 8
- Configure Hotspot 2.0 Identity Provider..... 8
- Configure Guest Access Portal..... 12
- Configure Onboarding SSID..... 13
- Configure Hotspot 2.0 Profile..... 14
- Configure Secure SSID..... 15

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 Guest 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 Hotspot 2.0 Wi-Fi Operator Profile. The title bar reads 'Edit Hotspot 2.0 Wi-Fi Operator Profile: [Anna40 WiFiOperator]'. The form includes the following sections:

- Name:** A text input field containing 'Anna40 WiFiOperator'.
- Description:** An empty text input field.
- Domain Names:** A section with a 'Domain Name *' input field and '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 currently unchecked.
- Certificate:** A dropdown menu showing '[?] * No data available' and a 'Create New' button.
- Friendly Names:** A section with a 'Language *' dropdown menu (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 click **Apply**.

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 Configure Network Identifier

Edit Hotspot 2.0 Identity Provider: [Anna40 Identity Provider]

->
 ->
 ->
 ->

Name: *

Description:

PLMNs:

MCC * MNC *

MCC ▲	MNC

Realms: *

Name: *

Encoding: *

EAP Methods:

#1 #2 #3 #4

EAP Method:

Name ▲	Encoding	EAP Methods
cloudpath.net	RFC-4282	#1: EAP-TLS #2: N/A #3: N/A #4: N/A

Home Ols:

Name * Length * Organization ID *

Name ▲	Length	Organization ID

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

Edit Hotspot 2.0 Identity Provider: [Anna40 Identity Provider]

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

Enable Online Signup & Provisioning

Provisioning Options

Provisioning Service: Internal External Service URL: *

Provisioning Protocol: * OMA-DM SOAP-XML

Online Signup Options

OSU NAI Realm: *

Common Language Icon: *

OSU Service Description: *

Language *	Friendly Name *	Description	Icon	Format	Width	Height
English	Anna 40 Wi-Fi Service					

Whitelisted Domains:

Domain Name
cloudpath.net
google.com
www.google.com

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

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.

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 *

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.

1. On the Accounting tab, enable **Accounting**.

Controller Configuration

Configure Guest Access Portal

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 Guest Access Portal

Navigate to your AP Zone for Zone Configuration. 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 **Upload**

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

User Session

Session Timeout: * 1440 Minutes (2-14400)

Grace Period: * 60 Minutes (1-14399)

Apply **Cancel**

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: * Anna40 Onboarding
SSID: * Anna40 Onboarding
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 (OSEV)
 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: * Anna Guest Portal
Bypass CNA: Enable
Guest Authentication: * Guest
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: * No data available

Authentication Services

Service *	Credential Store *	Realm *	Local Credential Expiration	
No data available	Local	No data available	<input type="text" value=""/> Day	<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/Anna40TestEVT/Pro...	<input checked="" type="radio"/>	<input type="button" value="Delete"/>

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 HS2R2 Secure] of zone [KEVIN-H S2-ZONE]

General Options

Name: * Anna40 HS2R2 Secure
SSID: * Anna40 HS2R2 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 1 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

- Prerequisites..... 17
- Cloudpath Configuration Summary..... 17
- Enabling Passpoint on the Cloudpath System..... 17
- Workflow for Passpoint Configuration..... 19
- Device Configuration Passpoint Settings..... 19
- Additional Passpoint Settings..... 23

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

- Enable Passpoint on the Cloudpath System
- Workflow for Passpoint Configuration
- Device Configuration Passpoint Settings
- Additional Passpoint Settings

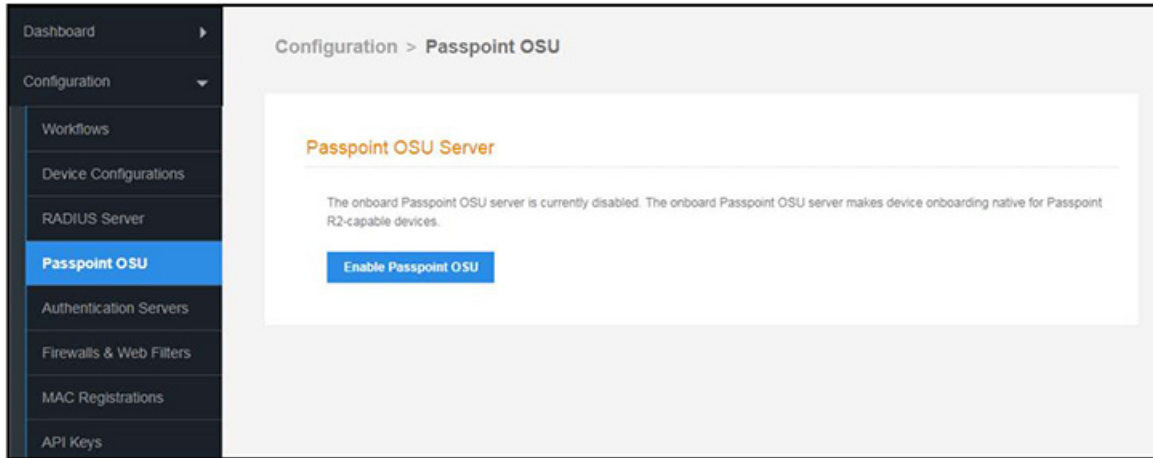
Enabling Passpoint on the Cloudpath System

Enable Passpoint from the left menu by selecting the **Configure > Passpoint OSU** tab.

Cloudpath Configuration

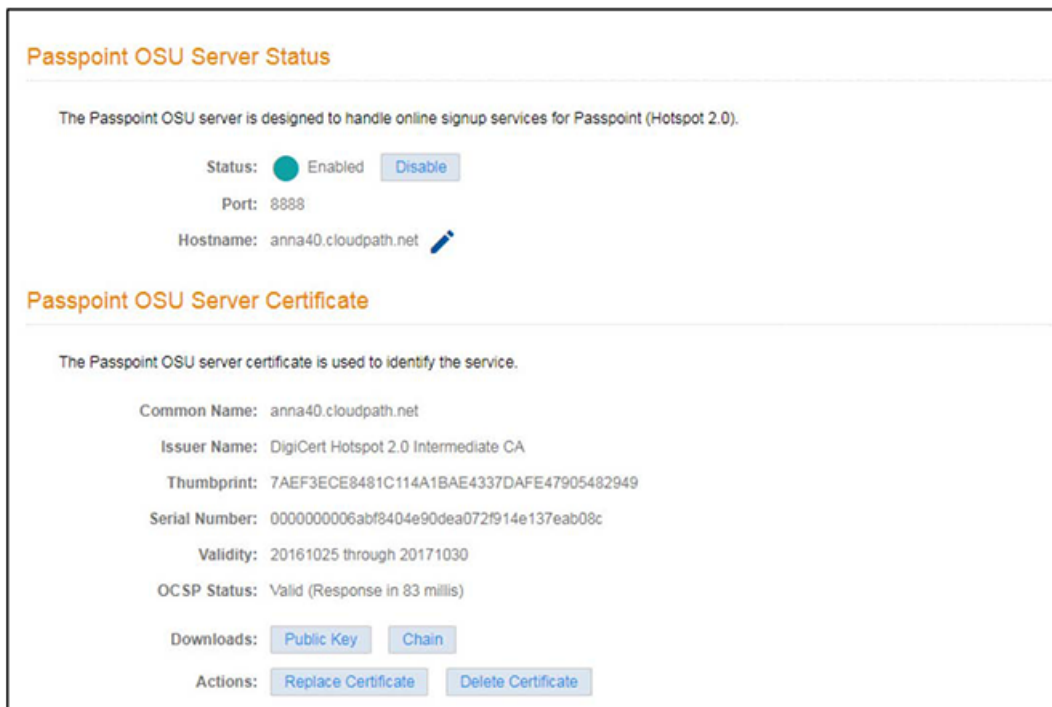
Enabling Passpoint on the Cloudpath System

FIGURE 10 Enable Passpoint OSU



Enabling Passpoint restarts the web server and displays the Passpoint Configuration page, which allows you to upload the Hotspot 2.0 WWW certificate and configure the Passpoint hostname and port.

FIGURE 11 Configure Passpoint server and certificate



The web server restarts after the Hotspot 2.0 WWW certificate has been uploaded.

NOTE

Enabling Passpoint on the system allows you to configure the server and upload the Hotspot 2.0 WWW certificate. However, you must also enable Passpoint for any device configuration that supports Passpoint. See [Device Configuration Passpoint Settings](#) on page 19.

Workflow for 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 12 Passpoint Workflow

Configuration > 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

Properties | **Enrollment Process** | Look & Feel | Snapshot(s) | Advanced

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...**

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

Device Configuration Passpoint Settings

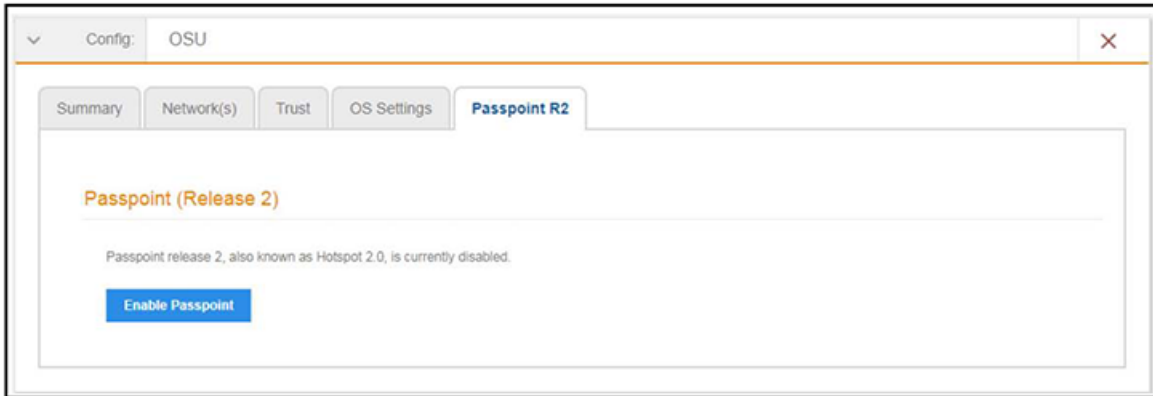
The passpoint settings include configuration for the Home Service Provider, the Subscription Server, and the Policy Server.

Enable Passpoint for the Device Configuration

When Passpoint is enabled on the system, a Passpoint R2 tab is added for each device configuration.

You can enable Passpoint for only the device configurations that will support Passpoint.

FIGURE 13 Enable Passpoint for the Device Configuration



Enabling Passpoint for the device configuration allows you to configure Home Server Provider, Subscription, Policy, and Certificate settings.

Configure Home Service Provider

FIGURE 14 Home Service Provider Settings

A screenshot of a web-based configuration window titled 'Modify Home SP'. The window has 'Cancel' and 'Save' buttons in the top right corner. The main content area is divided into two sections. The first section, 'Home SP', contains the following fields: 'Friendly Name' (text input with value 'Anna 40 Wi-Fi Service'), 'FQDN' (text input with value 'anna40.cloudpath.net'), 'Realm' (text input with value 'cloudpath.net'), and 'EAP Method' (dropdown menu with value 'EAP-TLS'). The second section, 'Advanced Home SP Configuration', is expanded and contains: 'Network IDs' (table with columns 'SSID' and 'HESSID', a '+' icon below), 'Home OIs' (table with columns 'Home OI' and 'Required', a '+' icon below), 'Other Home Partners' (table with column 'FQDN', a '+' icon below), and 'Icon URL' (text input with value '[Automatic]').

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 15 Subscription Server Settings

The screenshot shows a 'Modify Subscription' dialog box with the following sections:

- Subscription Update Server**
 - Use this server.**
The end-user device will query this server for subscription updates.
Subscription Update Configuration:
 - Update Interval:** 10080 Minutes *
 - Restriction:** Unrestricted ▼
 - Use an external server.**
The end-user device will query an external server for subscription updates.
- Advanced Subscription Configuration**
 - 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 16 Policy Server Settings

The screenshot shows a 'Modify Policy' window with a 'Cancel' and 'Save' button in the top right. The main content is divided into two sections: 'Policy Update Server' and 'Advanced Policy Configuration'.

Policy Update Server

- Use this server.**
The end-user device will query this server for policy updates.
Policy Update Configuration:
 - Update Interval:** 10080 Minutes *
 - Restriction:** Unrestricted ▼
- 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:**

Match Type	FQDN Match	Priority	Country
+			
- Minimum Backhaul Threshold:**

Network Type	DL Bandwidth	UL Bandwidth
+		
- SP Exclusion List:**

SSID
+
- Required Protocol/Port:**

IP Protocol	Port Number
+	
- Maximum BSS Load Value:** [ex. 1]

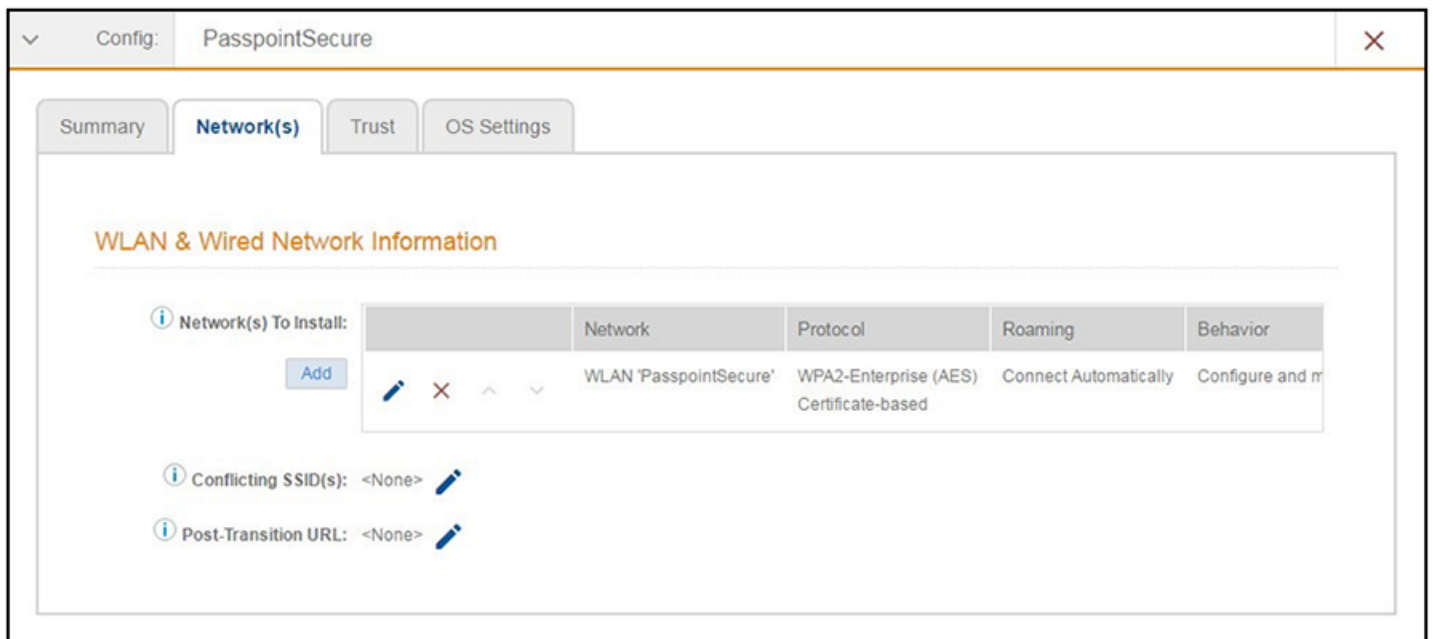
Additional Passpoint Settings

In addition to device configuration settings, you must specify the correct EAP Method in the WLAN settings, RADIUS server Trust settings, and Certificate Template settings.

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 17 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 18 RADIUS Certificate Trust Settings

Device Configuration: Trust Settings

Wi-Fi Trust

Trusted RADIUS Server(s): **Onboard RADIUS Server**

When connecting to the network, the end-user's device will compare the server certificate presented by the RADIUS server to the information specified here, including both the common name of the RADIUS server certificate and the chain of the issuing CA. On some operating systems, including Mac OS X, this value is case-sensitive.

Trusted Common Name:

Trusted RADIUS Chain:

⬇	Root CA:	Hotspot 2.0 Trust Root CA - 03	51501F...CC1FDF	20431208	
⬇	Intermediate CA:	DigICert Hotspot 2.0 Intermediate CA	102B55...2F8B5C	20231209	Hotspot 2.0 Trust Root CA - 03
⬇	Server Certificate:	anna40.cloudpath.net	7AEF3E...482949	20171030	DigICert Hotspot 2.0 Intermediate CA

Web Browser Trust

Install Additional CAs:

Certificate Template Settings

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

FIGURE 19 Certificate Template Settings

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

Common Name:

CA Type:

CA Reference Name:

CA Common Name:

Chain:

	Name	Notes	Expires
🔍	Anna40 Test BVT Intermediate CA 1		20361107
🔍	Anna40 Test BVT Root CA 1		20361107

Notifications:

SCEP Keys:

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 kltext-eng 4.4.2 KOT49H G900FXXUTAMK6 test-keys.

To test your configuration, use these example enrollment steps:

1. Enable Passpoint on the device.

The device should display **New Passpoint available. Click to subscribe**

2. Tap to subscribe. You should see the **Friendly Name** of the Cloudpath system previously configured.
3. Tap the Cloudpath system Friendly Name.

The device connects to the onboarding SSID, which redirects to the Cloudpath enrollment portal.

4. Run through the enrollment process, which includes, in this example, an AD login step.

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 do not match exactly, 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 20 Modify Certificate Template

Policy - RADIUS Attributes

Allow Authentication via RADIUS :



Login By Certificate
bob@byod.sample.com

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.

RADIUS Policies
ex. VLAN: 50

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:

<input checked="" type="checkbox"/> EKUs:	
<input checked="" type="checkbox"/>	Hotspot 2.0 Auth-1.3.6.1.4.1.40808.1.1.2
<input type="checkbox"/>	Hotspot 2.0 Server and Client Authentication
<input checked="" type="checkbox"/>	Microsoft Client ECU-1.3.6.1.5.5.7.3.2

▶ **Cleanup**



© 2023 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
<https://www.commscope.com>