Configuring Ruckus Cloud Wi-Fi with Cloudpath™ Enrollment System

‘How To’ Deployment Guide

Copyright Notice and Proprietary Information

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT, SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Ruckus Networks | 350 West Java Drive | Sunnyvale, CA 94089 USA | T: (650) 265-4200 | F: (408) 738-2065 ruckuswireless.com

Table of Contents

Table of Figures

Purpose of This Document

This document is aimed at IT administrators who want to deploy Cloudpath Enrollment System (Cloudpath ES) with Ruckus Cloud Wi-Fi in order to provide an additional level of network security for BYOD, guest users and IT-owned devices. In order to perform the steps provided in the document, admin privileges for the Ruckus Cloud Wi-Fi and Cloudpath ES software consoles are needed.

A high-level description of the workflows is given here, but a complete description of the configuration of the Cloudpath software is beyond the scope of this document. For more information on installation/configuration of the Cloudpath software, please refer to the Ruckus Support Site [1].

Introduction

The growing demand for Wi-Fi network access, driven by more users and more connected devices, creates opportunities for organizations but also challenges for IT. Users expect to be able to easily join a network, but they also expect their connections to be secure. Traditional methods of onboarding users and devices, like pre-shared key (PSK) and MAC authentication, fall short in preventing unauthorized access and can expose the network to security threats. Yet more secure alternatives have their own drawbacks. Without the proper platform in place, managing and distributing 802.1X certificates across devices located in multiple sites adds significant complexity for the IT teams.

Ruckus Networks offers solutions to IT administrators to radically simplify management, improve usability and increase security in their deployments. In this guide, we will discuss how the Ruckus Cloud Wi-Fi service together with Ruckus Cloudpath ES software streamlines onboarding and delivers secure connectivity for BYOD and guest users across multiple sites. Digital certificates and dynamic PSKs solve both the security and usability problems associated with default methods of network onboarding and authentication.

In the next section, we will describe individual components of the solution followed by configuration steps to build a solution.

Ruckus Cloud Wi-Fi and Cloudpath Enrollment System Solution Topology

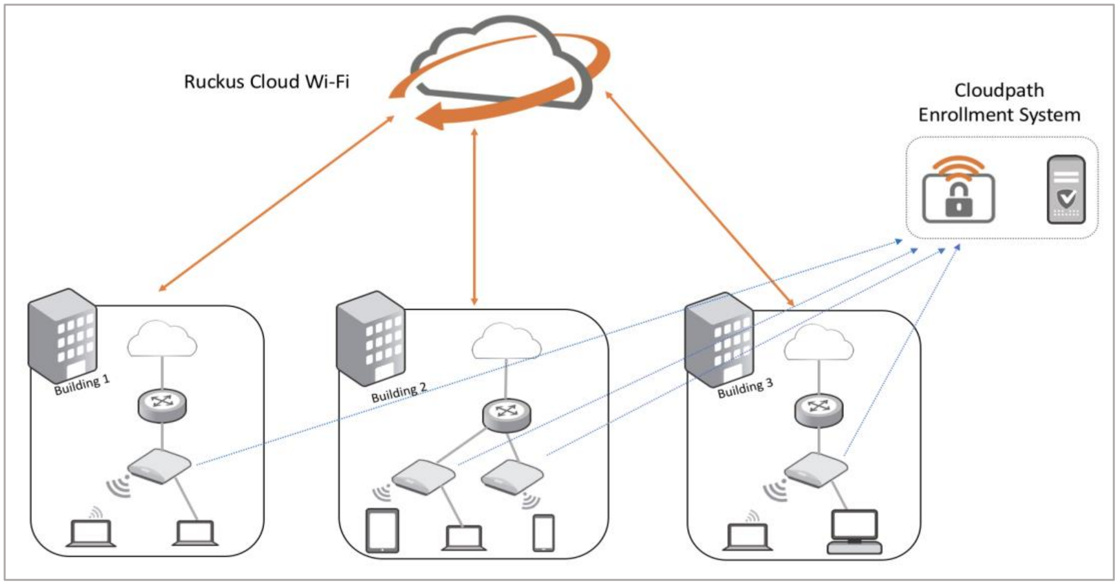


FIGURE 1 SOLUTION TOPOLOGY OVERVIEW

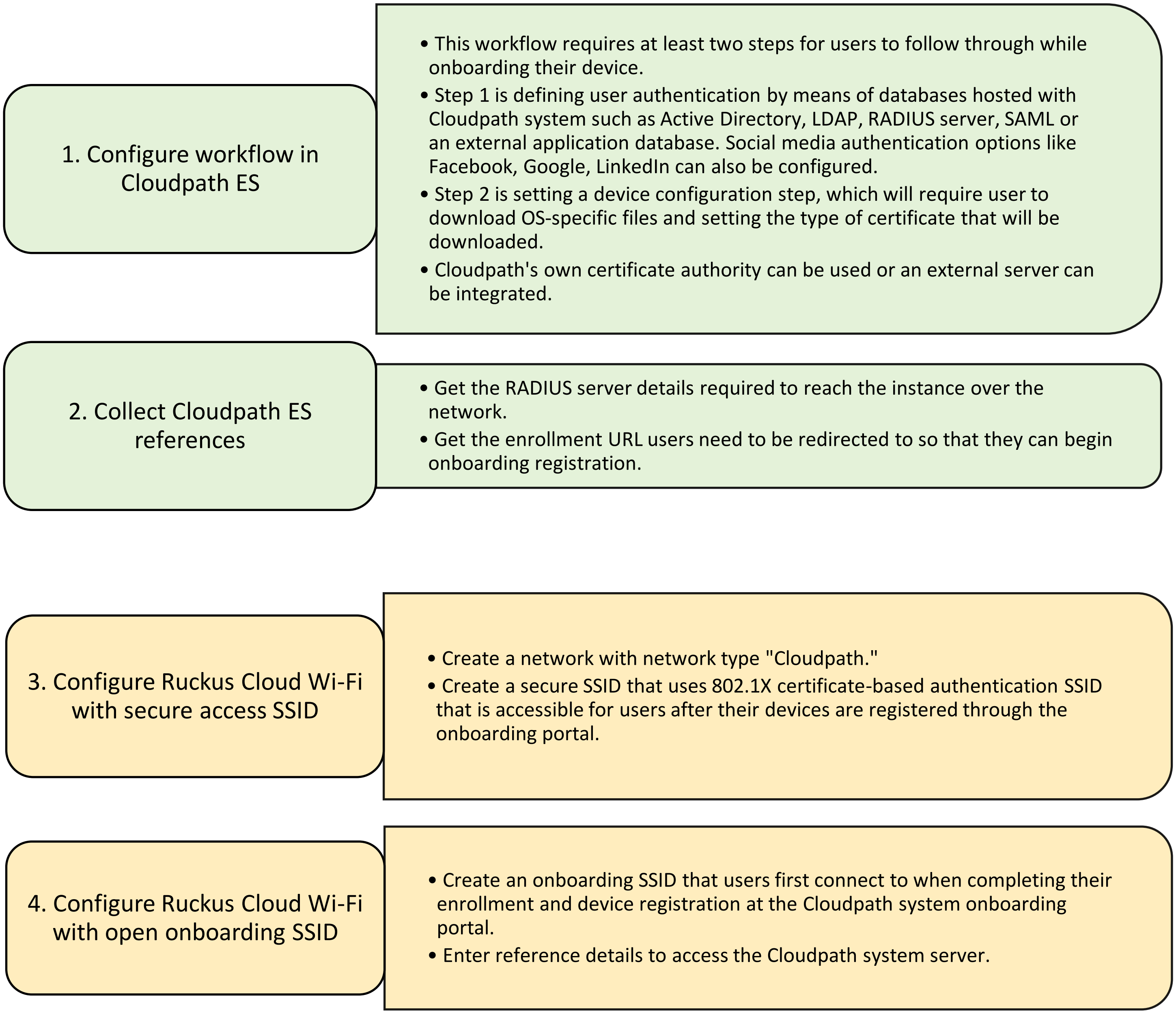
Ruckus Cloud Wi-Fi is cloud-managed Wi-Fi for simplified management of a distributed Wi-Fi network. With Ruckus Cloud Wi-Fi, even a small IT staff can keep up with the demands of deploying, monitoring and managing multiple sites. The solution's scalable architecture easily accommodates site and user growth.

In order to protect the security and integrity of the network, users and devices need to be securely onboarded. To lessen the burden of having IT perform this task individually for each user and device, Cloudpath software provides an easy way for users to connect without IT intervention.

Ruckus Cloudpath Enrollment System is a software/SaaS that delivers secure network access to support any user and any device on any network. It streamlines network onboarding for BYOD, guest users and IT-owned device—including IoT devices. Cloudpath software increases security with powerful certificate-based encryption using WPA2-Enterprise, access policy management and up-front device posture assessment with remediation. Intuitive self-service workflows deliver a great end-user experience while dramatically reducing helpdesk tickets related to network access. Unlike leading competitors, Cloudpath software is available as either a cloud-based service or virtualized on-premises deployment.

Configure Cloudpath Software on Ruckus Cloud Wi-Fi

Configuration Overview



1. Configure workflow in Cloudpath ES

- This workflow requires at least two steps for users to follow through while onboarding their device.
- Step 1 is defining user authentication by means of databases hosted with Cloudpath system such as Active Directory, LDAP, RADIUS server, SAML or an external application database. Social media authentication options like Facebook, Google, LinkedIn can also be configured.
- Step 2 is setting a device configuration step, which will require user to download OS-specific files and setting the type of certificate that will be downloaded.
- Cloudpath's own certificate authority can be used or an external server can be integrated.

2. Collect Cloudpath ES references

- Get the RADIUS server details required to reach the instance over the network.
- Get the enrollment URL users need to be redirected to so that they can begin onboarding registration.

3. Configure Ruckus Cloud Wi-Fi with secure access SSID

- Create a network with network type "Cloudpath."
- Create a secure SSID that uses 802.1X certificate-based authentication SSID that is accessible for users after their devices are registered through the onboarding portal.

4. Configure Ruckus Cloud Wi-Fi with open onboarding SSID

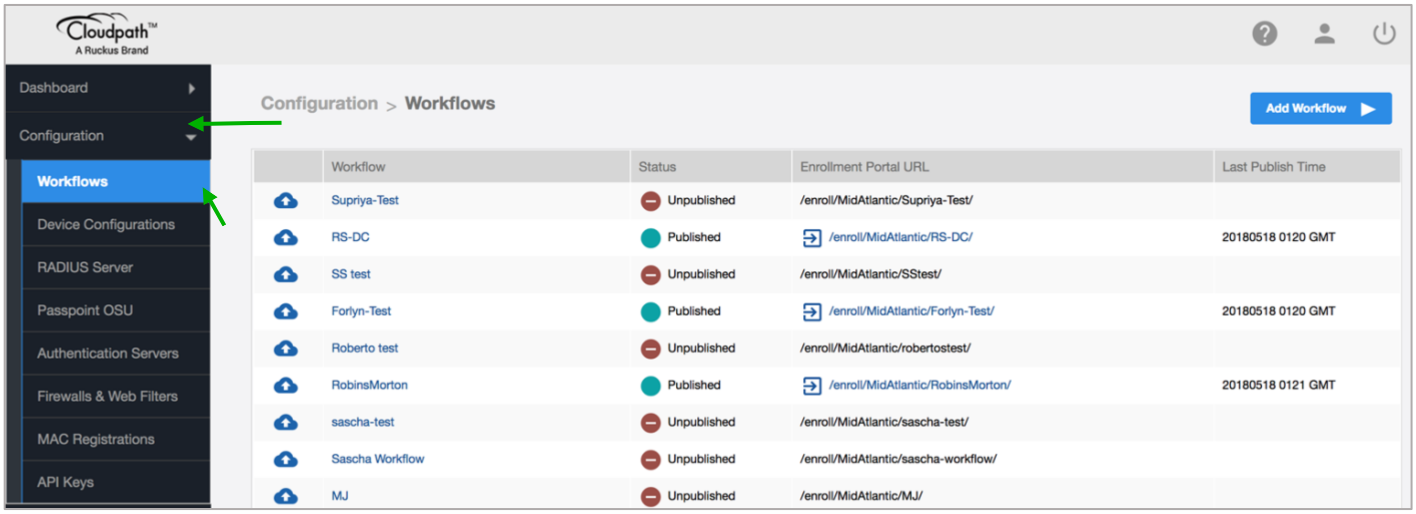
- Create an onboarding SSID that users first connect to when completing their enrollment and device registration at the Cloudpath system onboarding portal.
- Enter reference details to access the Cloudpath system server.

A high-level description of the workflows is given here, but a complete description of the configuration of Cloudpath workflows is beyond the scope of this document. Please refer to the appropriate documents for more details regarding configuring Cloudpath workflows on the Ruckus Support site [1].

Step-by-Step

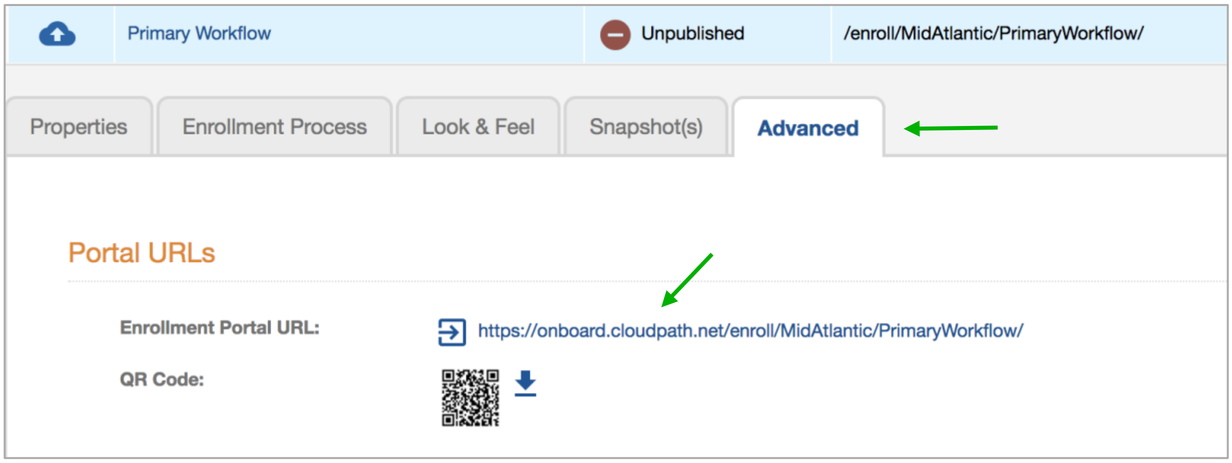
A. Cloudpath Enrollment System reference

1. Log in to Cloudpath ES and navigate to Configuration -> Workflow.
2. Click on the workflow to be deployed.
3. Click on the workflow's Advanced tab to get the enrollment portal URL.



Workflow	Status	Enrollment Portal URL	Last Publish Time
Supriya-Test	Unpublished	/enroll/MidAtlantic/Supriya-Test/	
RS-DC	Published	/enroll/MidAtlantic/RS-DC/	20180518 0120 GMT
SS test	Unpublished	/enroll/MidAtlantic/SStest/	
Forlyn-Test	Published	/enroll/MidAtlantic/Forlyn-Test/	20180518 0120 GMT
Roberto test	Unpublished	/enroll/MidAtlantic/robertostest/	
RobinsMorton	Published	/enroll/MidAtlantic/RobinsMorton/	20180518 0121 GMT
sascha-test	Unpublished	/enroll/MidAtlantic/sascha-test/	
Sascha Workflow	Unpublished	/enroll/MidAtlantic/sascha-workflow/	
MJ	Unpublished	/enroll/MidAtlantic/MJ/	

FIGURE 2 CLOUDPATH DASHBOARD NAVIGATION STEPS



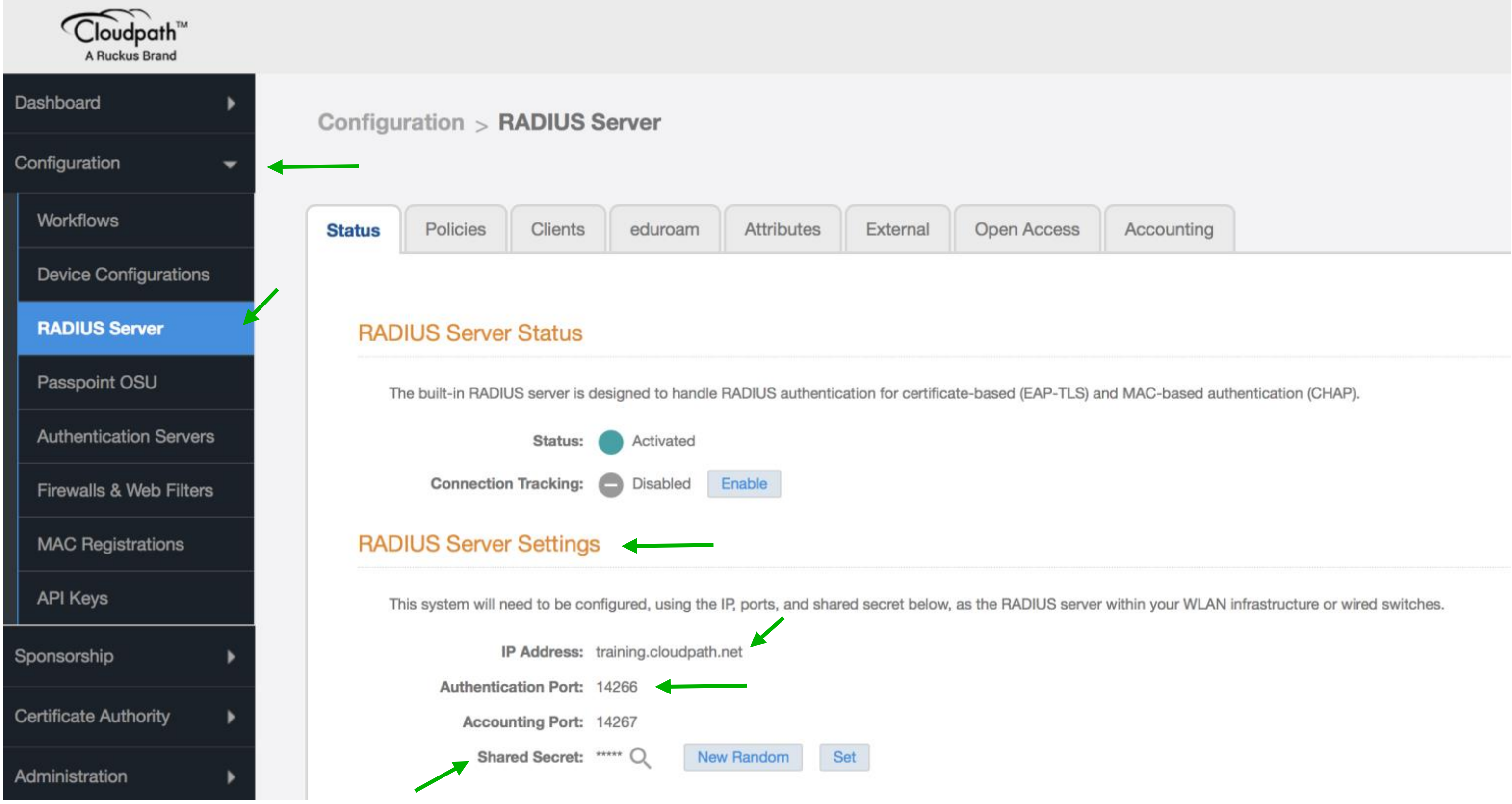
Primary Workflow | Unpublished | /enroll/MidAtlantic/PrimaryWorkflow/

Enrollment Portal URL: https://onboard.cloudpath.net/enroll/MidAtlantic/PrimaryWorkflow/

QR Code:

FIGURE 3 CLOUDPATH WORKFLOW DETAILS

4. Get the RADIUS server settings. On the main menu bar, navigate to Configuration -> RADIUS Server. Get the following information:
   - The IP address
   - Authentication port
   - The Shared Secret, which can be revealed by clicking on the magnifying glass



RADIUS Server Status

The built-in RADIUS server is designed to handle RADIUS authentication for certificate-based (EAP-TLS) and MAC-based authentication (CHAP).

Status: Activated

Connection Tracking: Disabled

RADIUS Server Settings

This system will need to be configured, using the IP, ports, and shared secret below, as the RADIUS server within your WLAN infrastructure or wired switches.

IP Address: training.cloudpath.net

Authentication Port: 14266

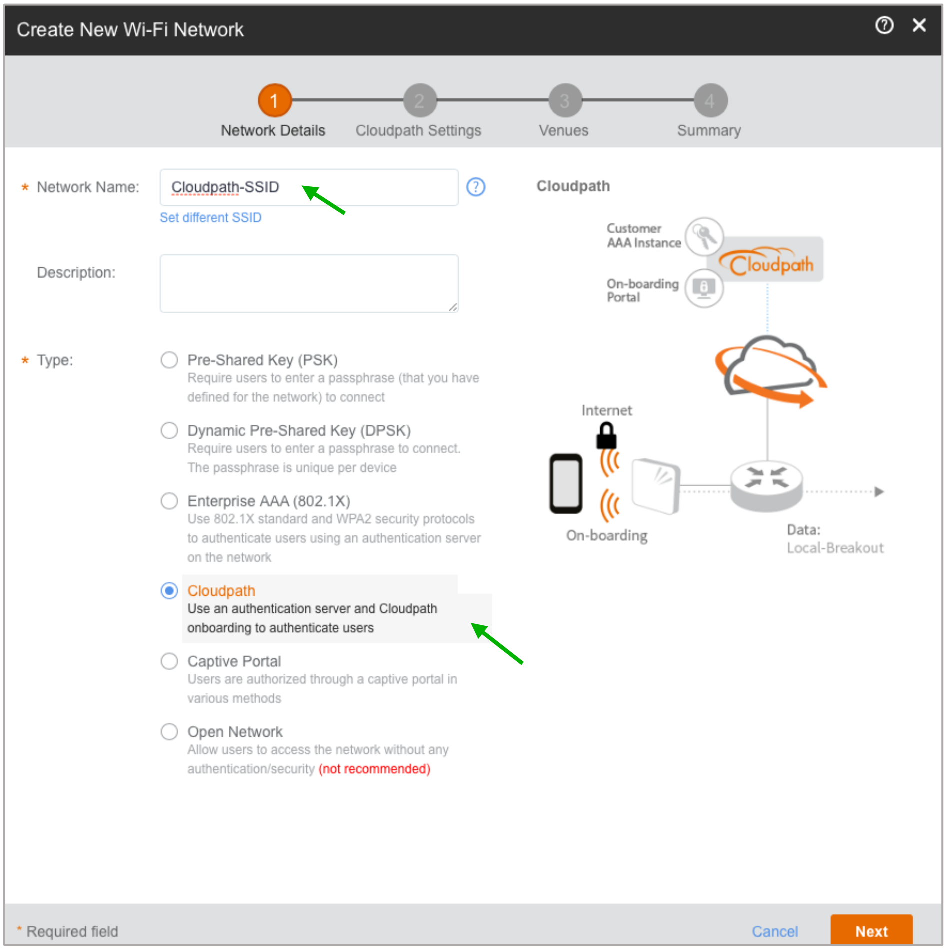
Accounting Port: 14267

Shared Secret: *****

FIGURE 4 RADIUS SERVER DETAILS CONFIGURED IN CLOUDPATH SOFTWARE

B. Ruckus Cloud Wi-Fi Configuration

5. Log in to Ruckus Cloud Wi-Fi and navigate to Networks -> Add Networks.
6. Create client access, secure SSID.
7. Select Cloudpath for network type.



Create New Wi-Fi Network

1 Network Details — 2 Cloudpath Settings — 3 Venues — 4 Summary

* Network Name: Cloudpath-SSID

Set different SSID

Description:

* Type:

○ Pre-Shared Key (PSK)
Require users to enter a passphrase (that you have defined for the network) to connect

○ Dynamic Pre-Shared Key (DPSK)
Require users to enter a passphrase to connect. The passphrase is unique per device

○ Enterprise AAA (802.1X)
Use 802.1X standard and WPA2 security protocols to authenticate users using an authentication server on the network

● Cloudpath
Use an authentication server and Cloudpath onboarding to authenticate users

○ Captive Portal
Users are authorized through a captive portal in various methods

○ Open Network
Allow users to access the network without any authentication/security (not recommended)

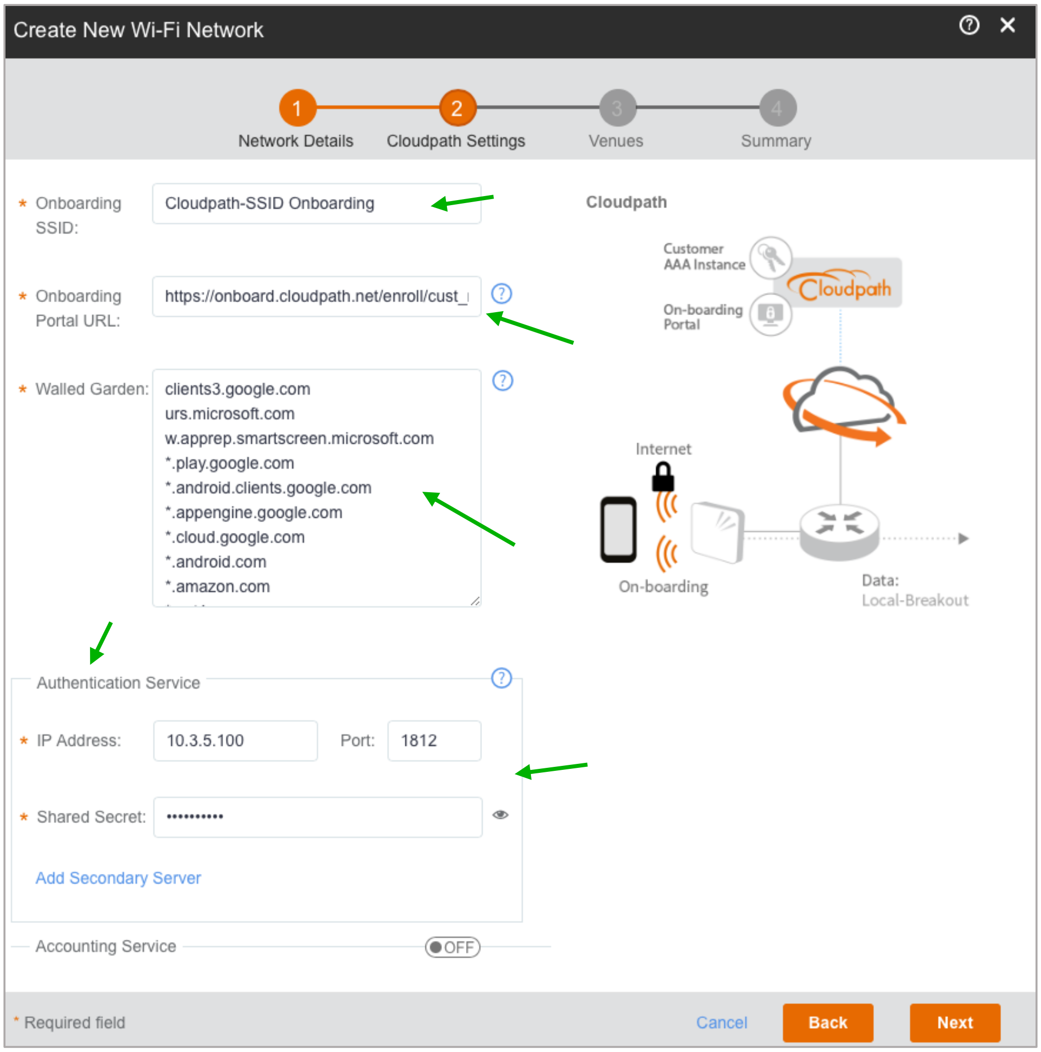
* Required field

Cancel Next

FIGURE 5 CREATE CLOUDPATH TYPE NETWORK ON CLOUD WI-FI

Caveat with device configuration template and client access secure SSID: It is required that the administrator match the SSID name in the Cloudpath system while setting up a device configuration template for certificate-based authentication with the one in Cloud Wi-Fi while creating the secure SSID. In case of mismatch, the device will not get secure network access even after a successful enrollment process.

8. Add the workflow settings collected from the Cloudpath system:
   - Enter the RADIUS IP, port and shared secret.
   - Enter the enrollment URL (Default: https://onboard.cloudpath.net/enroll/customer_name/location_name/redirect).
9. Create the open onboarding SSID.
10. Include relevant domains/URL/IP address details in the Walled Garden list.



Create New Wi-Fi Network

1 Network Details — 2 Cloudpath Settings — 3 Venues — 4 Summary

* Onboarding SSID: Cloudpath-SSID Onboarding

* Onboarding Portal URL: https://onboard.cloudpath.net/enroll/cust_

* Walled Garden:
clients3.google.com
urs.microsoft.com
w.apprep.smartscreen.microsoft.com
*.play.google.com
*.android.clients.google.com
*.appengine.google.com
*.cloud.google.com
*.android.com
*.amazon.com

Authentication Service

* IP Address: 10.3.5.100 Port: 1812

* Shared Secret: ••••••••••

Add Secondary Server

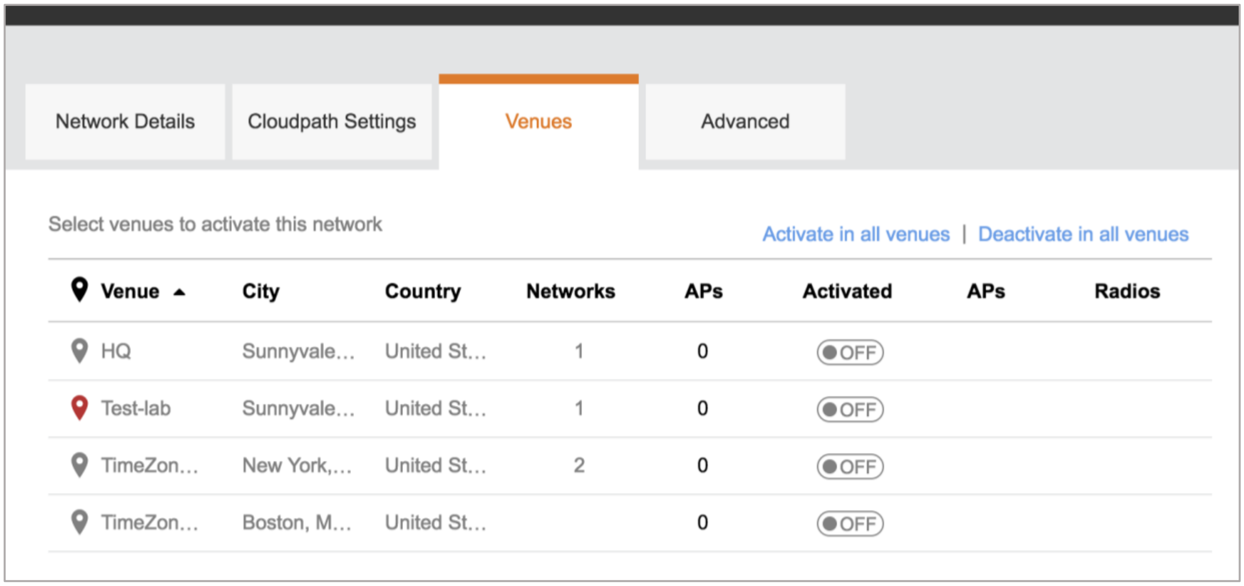
Accounting Service OFF

* Required field

FIGURE 6 CLOUDPATH SERVER SETTINGS CONFIGURED INTO CREATION OF NETWORK

Caveat with Walled Garden setting: Administrator must enter the correct set of IP addresses and URLs for allowing the user to be re-directed for social media login pages or custom authentication pages. Without proper entries, the user registration cannot be completed. The list of working IP addresses, domains and URLs can be found in the Ruckus Support site [2].

11. Activate the network on one or more venues.



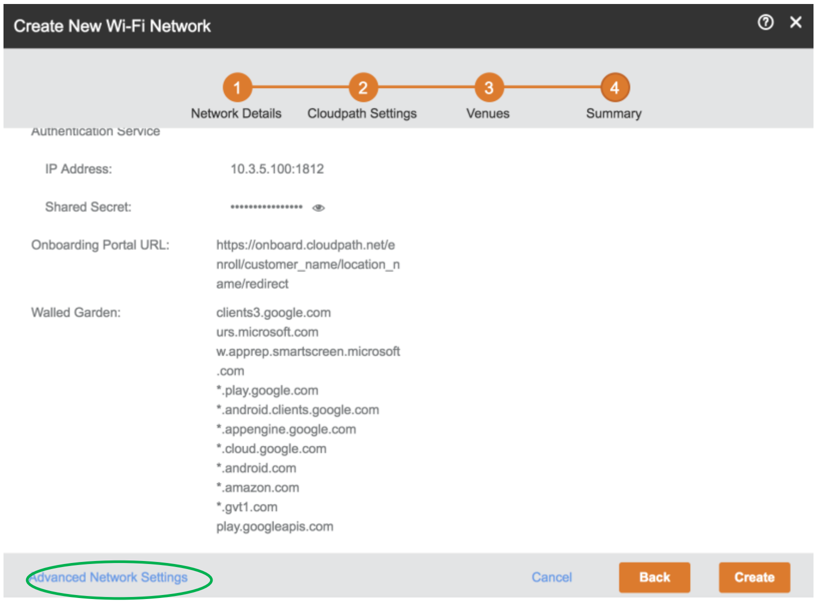
Select venues to activate this network

Activate in all venues | Deactivate in all venues

Venue ▲	City	Country	Networks	APs	Activated	APs	Radios
HQ	Sunnyvale…	United St…	1	0	OFF		
Test-lab	Sunnyvale…	United St…	1	0	OFF		
TimeZon…	New York,…	United St…	2	0	OFF		
TimeZon…	Boston, M…	United St…		0	OFF		

FIGURE 7 CLOUDPATH TYPE NETWORK ENABLED ON SELECTED VENUES

12. Enter appropriate onboarding VLAN ID under Advanced Network Settings.
    - Select Advanced Network Settings in the last step of Create Network.
    - It is advised not to have the same VLAN ID for the onboarding VLAN and management VLAN.
    - The onboarding VLAN should allow limited internet connectivity (app store in some cases) to the onboarding devices. However, it should not allow access to critical internal resources.



Authentication Service

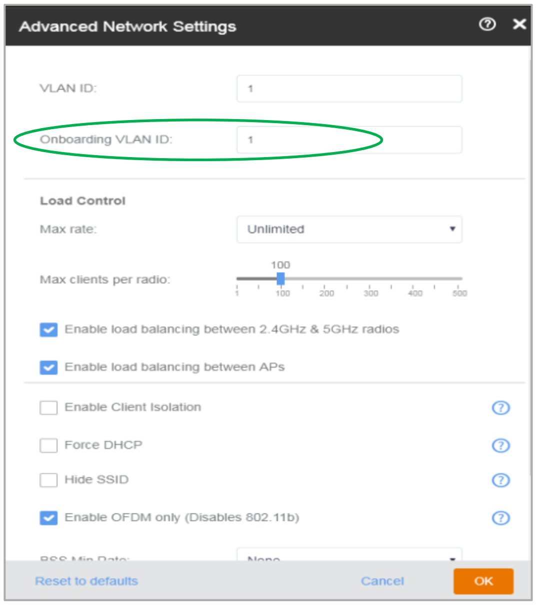
IP Address: 10.3.5.100:1812

Shared Secret: ••••••••••••••••

Onboarding Portal URL: https://onboard.cloudpath.net/enroll/customer_name/location_name/redirect

Walled Garden:
clients3.google.com
urs.microsoft.com
w.apprep.smartscreen.microsoft.com
*.play.google.com
*.android.clients.google.com
*.appengine.google.com
*.cloud.google.com
*.android.com
*.amazon.com
*.gvt1.com
play.googleapis.com

FIGURE 8 SELECT ADVANCED NETWORK SETTINGS



VLAN ID: 1

Onboarding VLAN ID: 1

Load Control

Max rate: Unlimited

Max clients per radio: 100

☑ Enable load balancing between 2.4GHz & 5GHz radios

☑ Enable load balancing between APs

□ Enable Client Isolation

□ Force DHCP

□ Hide SSID

☑ Enable OFDM only (Disables 802.11b)

BSS Min Rate: None

FIGURE 9 ENTER DIFFERENT ONBOARDING VLAN ID

With the completion of these steps, Ruckus Cloud Wi-Fi and Cloudpath Enrollment System are configured and two networks are set up.

1. Network 1: 802.1X secure SSID refers to the Cloudpath RADIUS server.
2. Network 2: Open SSID points to the Cloudpath system workflow URL.

It is useful to think of these two networks as a two-lane road where authorized and unauthorized users are separated and contained in their own lane. User separation is achieved by creating two networks and helps IT keep track of new users that are onboarding and move them to the secure network after successful enrollment.

Use Case: 802.1X Certificate-Based Authentication for secure network access

The challenges of implementing 802.1X certificate-based authentication are that it requires a certificate authority server such as RADIUS or Active Directory, and a means to manage it and distribute the certificates for authorized users and devices only. In a multi-site deployment scenario with many users and devices, implementation and distribution of 802.1X can become even more daunting. However, the combined Ruckus Cloud Wi-Fi and Cloudpath ES solutions can greatly simplify this process. Integration consists of only a few wizard-guided steps. In addition, the Cloudpath system provides the necessary backend for implementing 802.1X certificate management and policy definition for users and devices and Ruckus Cloud Wi-Fi provides the means for distributing it in the network.

This section describes the steps that users and devices go through for obtaining secure network access. The configuration and operation are the same for both Cloudpath software deployment options (on-premises and cloud).

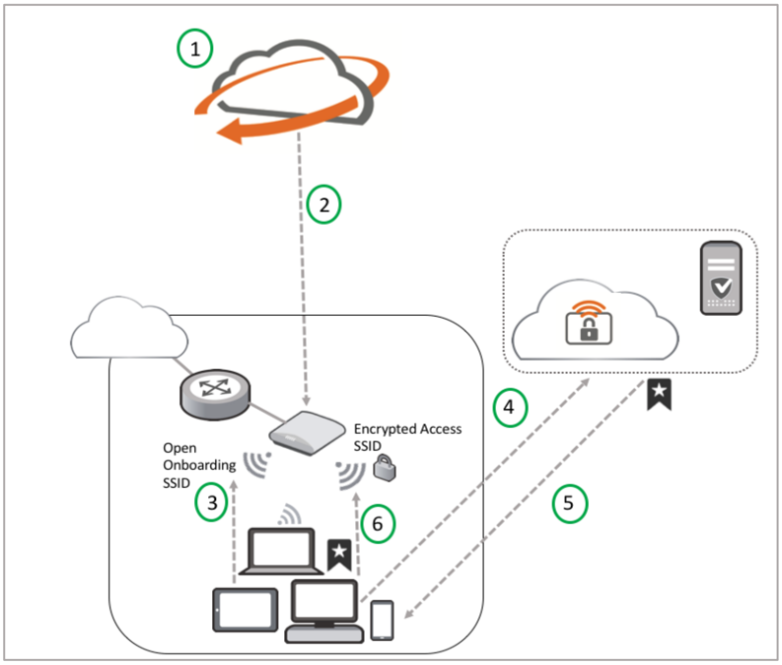


FIGURE 10 ONBOARDING STEPS FOR A CLOUD/ON-PREM INSTANCE OF CLOUDPATH SOFTWARE

Onboarding Steps

A. Administrator:
1. A Ruckus Cloud Wi-Fi network is configured as a Cloudpath type with necessary references to the enrollment system. This network is activated on one venue or multiple venues.
2. All APs in the selected venues are provisioned with this network.

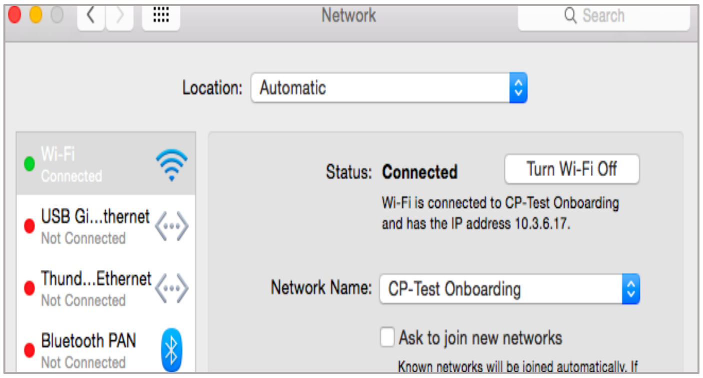
B. End-user:

3. Clients connect to the open onboarding SSID advertised by the AP.
4. Clients are redirected by the AP to go through a portal for registration.
5. On successful enrollment, user is asked to download a digital certificate.
6. Certificate is used to authenticate user and authorize device for secure network access.

The end-user steps are completed only once per user and device. A new device for the same user still goes through the same onboarding steps. For repeat users and devices with enrollment already in place, the certificate in the device is used for authentication and will be authorized for secure network access.

End-User View of Onboarding Steps

Unauthorized user and device beginning to onboard



Location: Automatic

Wi-Fi Connected

USB Gi...thernet Not Connected

Thund...Ethernet Not Connected

Bluetooth PAN Not Connected

Status: Connected

Wi-Fi is connected to CP-Test Onboarding and has the IP address 10.3.6.17.

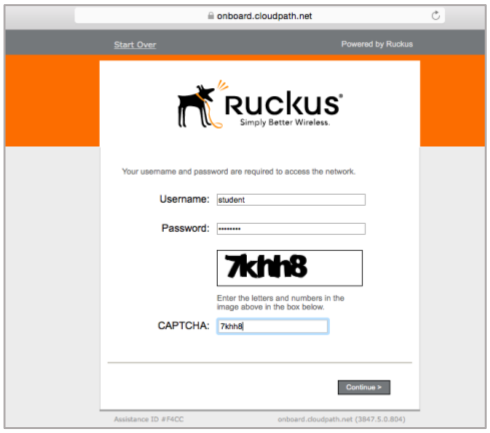
Network Name: CP-Test Onboarding

□ Ask to join new networks

Known networks will be joined automatically. If

FIGURE 11 USER CONNECTS DEVICE TO ONBOARDING SSID

User authentication using Active Directory



Your username and password are required to access the network.

Username: student

Password: ••••••••

Enter the letters and numbers in the image above in the box below.

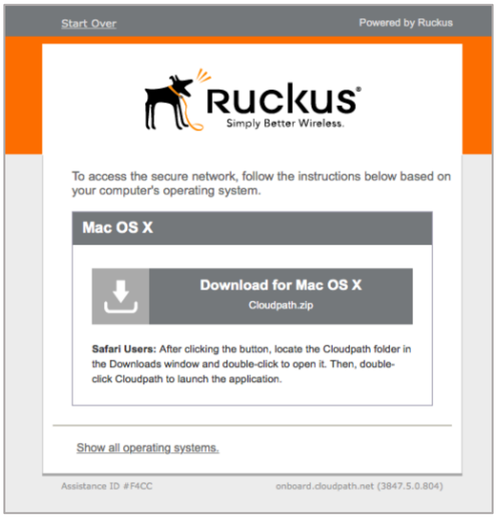
CAPTCHA: 7khh8

Assistance ID #F4CC

onboard.cloudpath.net (3847.5.0.804)

FIGURE 12 USER RE-DIRECTED TO ONBOARDING PORTAL FOR AUTHENTICATION

Download certificate to authenticate for secure network access



To access the secure network, follow the instructions below based on your computer's operating system.

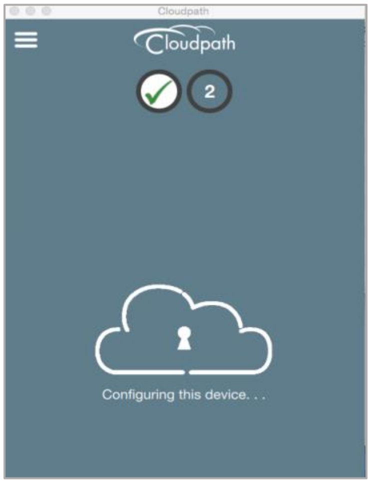
Mac OS X

Safari Users: After clicking the button, locate the Cloudpath folder in the Downloads window and double-click to open it. Then, double-click Cloudpath to launch the application.

Assistance ID #F4CC
onboard.cloudpath.net (3847.5.0.804)

FIGURE 13 CLIENT DIRECTED TO DOWNLOAD CONFIGURATION FILE

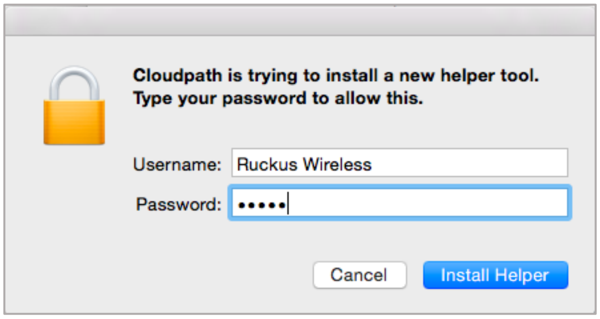
Device posturing based on configured workflow for client device



Configuring this device. . .

FIGURE 14 CONFIGURATION OF DEVICE ACCORDING TO CLOUDPATH WORKFLOW IN PROGRESS

Device remediation based on configuration in the Cloudpath software



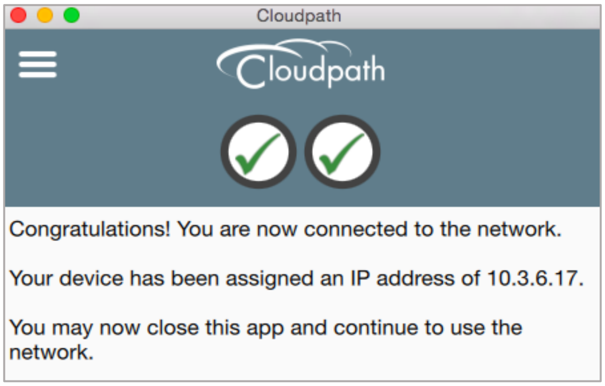
Cloudpath is trying to install a new helper tool. Type your password to allow this.

Username: Ruckus Wireless

Password: •••••

FIGURE 15 CLOUDPATH SOFTWARE DOWNLOADS RELEVANT FILES INTO THE REGISTERING DEVICE

Completion of enrollment with successful user authentication and device authorization



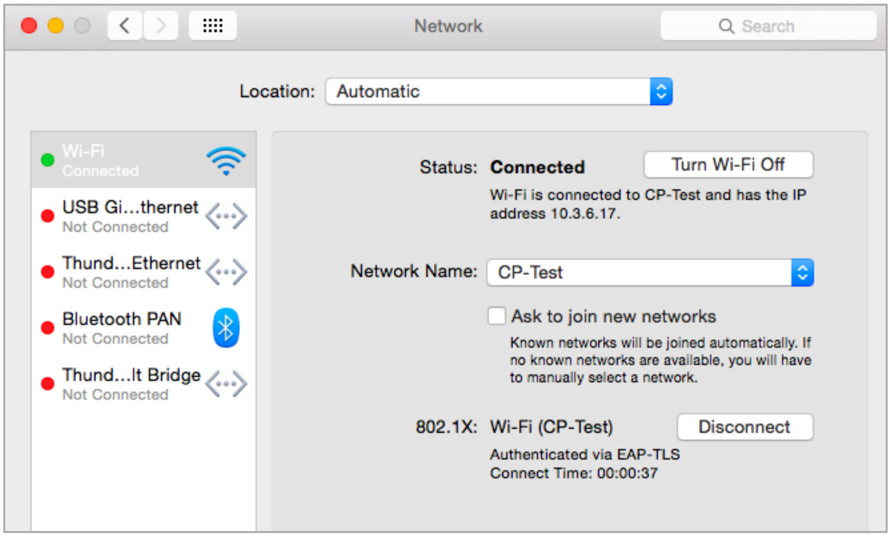
Congratulations! You are now connected to the network.

Your device has been assigned an IP address of 10.3.6.17.

You may now close this app and continue to use the network.

FIGURE 16 SUCCESSFUL CONFIGURATION OF DEVICE

Secure network access provided by validation of assigned certificate



Location: Automatic

Status: **Connected**

Wi-Fi is connected to CP-Test and has the IP address 10.3.6.17.

Network Name: CP-Test

☐ Ask to join new networks

Known networks will be joined automatically. If no known networks are available, you will have to manually select a network.

802.1X: Wi-Fi (CP-Test)

Authenticated via EAP-TLS
Connect Time: 00:00:37

FIGURE 17 SECURE ACCESS AFTER AUTHENTICATION

Summary

Configuration of Cloudpath Enrollment System and integration with Ruckus Cloud Wi-Fi takes minimal IT time and expertise. The step-by-step wizard allows administrators to quickly and easily deploy secure network access for a variety of devices while still maintaining a high level of control and visibility. 802.1X implementation is made easy even for multi-site deployments with multiple users and devices.

Cloudpath software's simplified 802.1X certificate management and Ruckus Cloud Wi-Fi's simplified deployment and management of a distributed Wi-Fi network reduce the burden on IT, while enhancing Wi-Fi network security and usability for users.

Appendix A: References

[1] Ruckus Support Site, [Online]: https://support.ruckuswireless.com/documents?filter=89#documents

[2] Ruckus Support Site, [Online]: https://support.ruckuswireless.com/answers/000005988

Appendix B: License SKUs

Ruckus Cloud Wi-Fi and Cloudpath Bundles	Descriptions
CLD-RKWF-1001 CLD-CLP1-4999	Cloud Wi-Fi 1 yr., 1 AP Cloudpath 1 yr. Cloud-hosted
CLD-RKWF-3001 CLD-CLP3-4999	Cloud Wi-Fi 3 yr., 1 AP Cloudpath 3 yr. Cloud-hosted
CLD-RKWF-5001 CLD-CLP5-4999	Cloud Wi-Fi 5 yr., 1 AP Cloudpath 5 yr. Cloud-hosted

About Ruckus Networks

Ruckus Networks enables organizations of all sizes to deliver great connectivity experiences. Ruckus delivers secure access networks to delight users while easing the IT burden, affordably. Organizations turn to Ruckus to make their networks simpler to manage and to better meet their users' expectations. For more information, visit www.ruckuswireless.com.

Ruckus Networks | 350 West Java Drive | Sunnyvale, CA 94089 USA | T: (650) 265-4200 | F: (408) 738-2065 ruckuswireless.com

About ARRIS

ARRIS International plc (NASDAQ: ARRS) is powering a smart, connected world. The company's leading hardware, software and services transform the way that people and businesses stay informed, entertained and connected. For more information, visit www.arris.com.

For the latest ARRIS news:

Check out our blog: ARRIS EVERYWHERE

Follow us on Twitter: @ARRIS