

Cloudpath End-User Experience for Linux Devices

Supporting Software Release 5.2

Copyright Notice and Proprietary Information

Copyright 2017 Brocade Communications Systems, Inc. All rights reserved.

No part of this documentation may be used, reproduced, transmitted, or translated, in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without prior written permission of or as expressly provided by under license from Brocade.

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. BROCADE and RUCKUS WIRELESS, INC. AND THEIR 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. BROCADE and RUCKUS RESERVE THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL BROCADE or 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.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and in other countries. Brocade, the B-wing symbol, MyBrocade, and ICX are trademarks of Brocade Communications Systems, Inc. in the United States and in other countries. Other trademarks may belong to third parties.

Contents

- Overview..... 4
 - Supported Versions.....4
- Cloudpath User Experience.....4
 - Enrollment User Prompts..... 4
 - Wizard Application User Experience..... 13

Overview

The Cloudpath Enrollment System (ES) automates WPA2-Enterprise configuration on any device that connects to the network and automatically connects the device to a secure SSID. This Automated Device Enablement (ADE) means authorized devices onboard simply and securely, with the appropriate level of access.

Cloudpath supports all operating systems including Windows, Mac OS X, iOS, Android, Linux, Chromebooks, and more.

This document provides an example of the end-user process for using Cloudpath to migrate a device running a Linux operating system to the secure network.

Supported Versions

Cloudpath supports the following Linux versions with automated configuration:

- Ubuntu version 12.04, and later
- Fedora version 18, and later

All earlier versions are supported with manual configuration.

Cloudpath User Experience

Cloudpath provides the prompts that guide the user through the sequence of steps that make up the enrollment workflow. During this process, the user enters information as requested, and makes selections about user type, device type, among others.

Enrollment User Prompts

This section displays the user prompts for a typical enrollment workflow. The sequence of steps for the enrollment can differ, depending on the selection that is made.

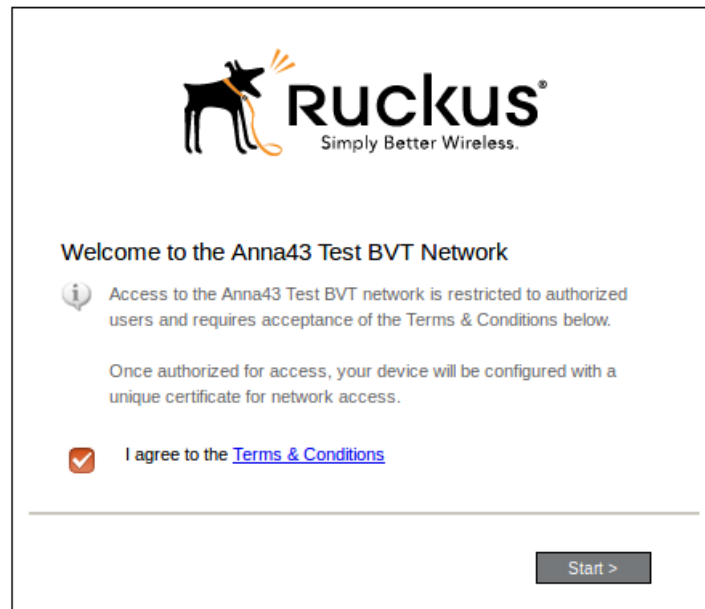
Welcome Screen With AUP

When the user enters the enrollment URL on their device, the **Login** (or **Welcome**) screen displays. The **login** screen is typically customized with the logo, colors, and text for the organization or institution. The screens in this example use the default look and feel of the application.

NOTE

If you have set up a captive portal, the user connects to onboarding SSID and is redirected to Cloudpath **Welcome** page to start the enrollment process.

FIGURE 1 Welcome Screen



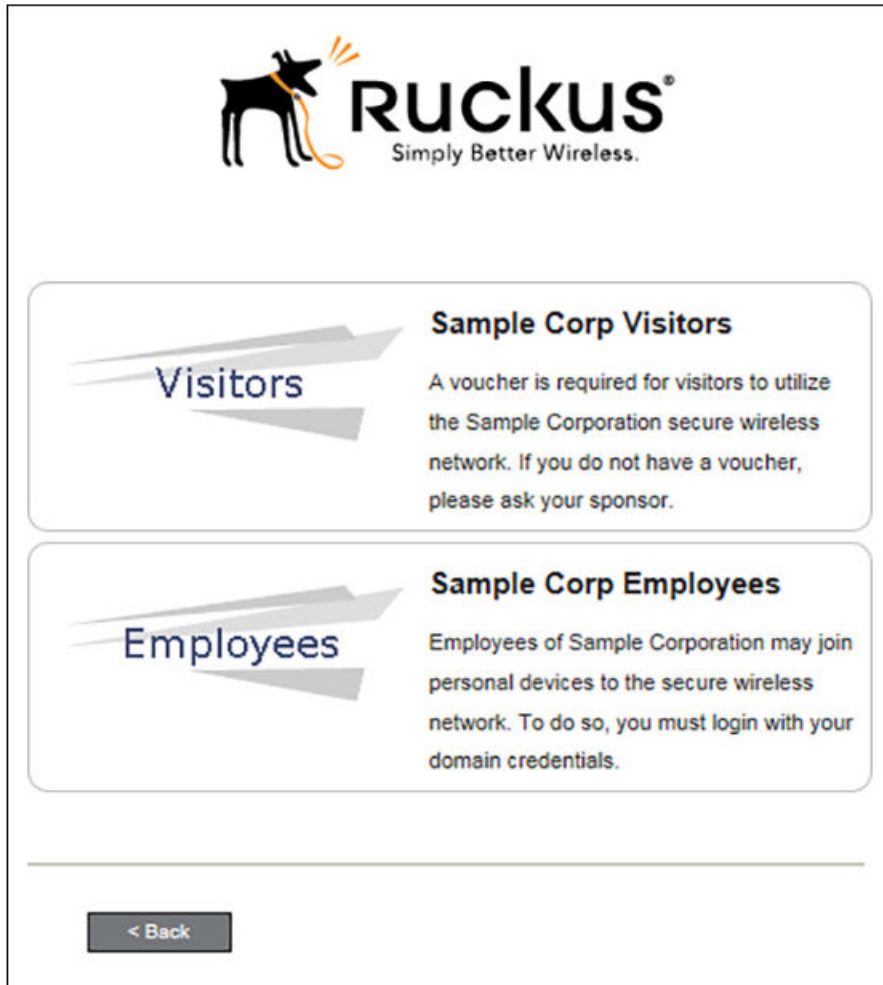
An acceptable use policy (AUP) prompt displays a message and requires that the user signal acceptance to continue. The **Welcome** page text and **Start** button may be customized.

Click **Start** to continue.

User Type

If required by the network, the user might see a User Type prompt. For example, an Employee might be required to enter domain credentials, and a Guest or Partner might be required to enroll using their social media credentials.

FIGURE 2 User Type Prompt

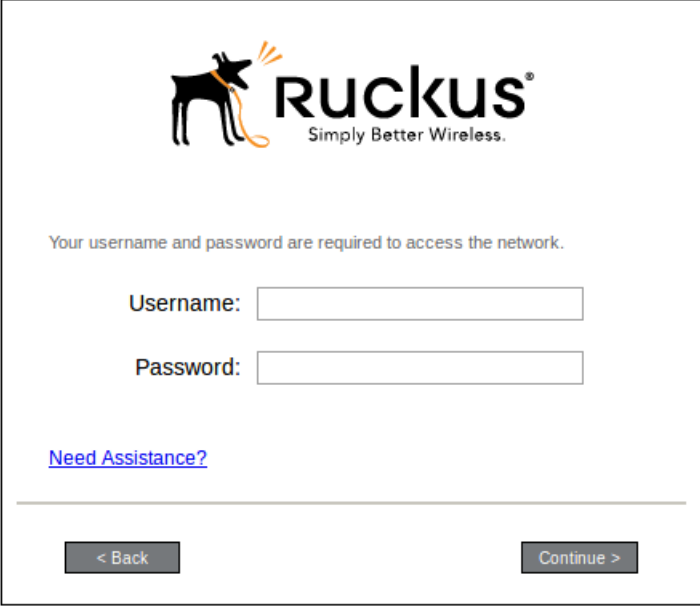


Select the **user type** to continue. This example follows the **Employees** workflow branch.

User Credentials

If required by the network, a prompt similar to the one below requires the user to enter network credentials.

FIGURE 3 User Credential Prompt



The image shows a user credential prompt window for Ruckus. At the top center is the Ruckus logo, which features a black silhouette of a dog with an orange leash and three orange curved lines above its head, followed by the word "RUCKUS" in a bold, black, sans-serif font and the tagline "Simply Better Wireless." below it. Below the logo, the text "Your username and password are required to access the network." is displayed. Underneath this text are two input fields: "Username:" followed by a white rectangular box, and "Password:" followed by a white rectangular box. Below the password field is a blue, underlined link that says "Need Assistance?". At the bottom of the window, there are two grey buttons: "< Back" on the left and "Continue >" on the right.

Enter the user credentials and click **Continue**.

Device Type

If required by the network, the user might see a Device Type prompt. For example, a Personal Device selection might add a prompt for a MAC address, and a IT-Issued Device would be allowed to bypass the MAC address prompt.

FIGURE 4 Device Type Prompt



Select a **device type** to continue. This example follows the **IT-Issued Device enrollment** workflow.

Voucher Code

Your network might require that you enter a voucher (one-time password) as an additional verification step. Vouchers are typically sent email or SMS from a network sponsor or administrator.

FIGURE 5 Voucher Code Prompt



Enter the voucher that you received.

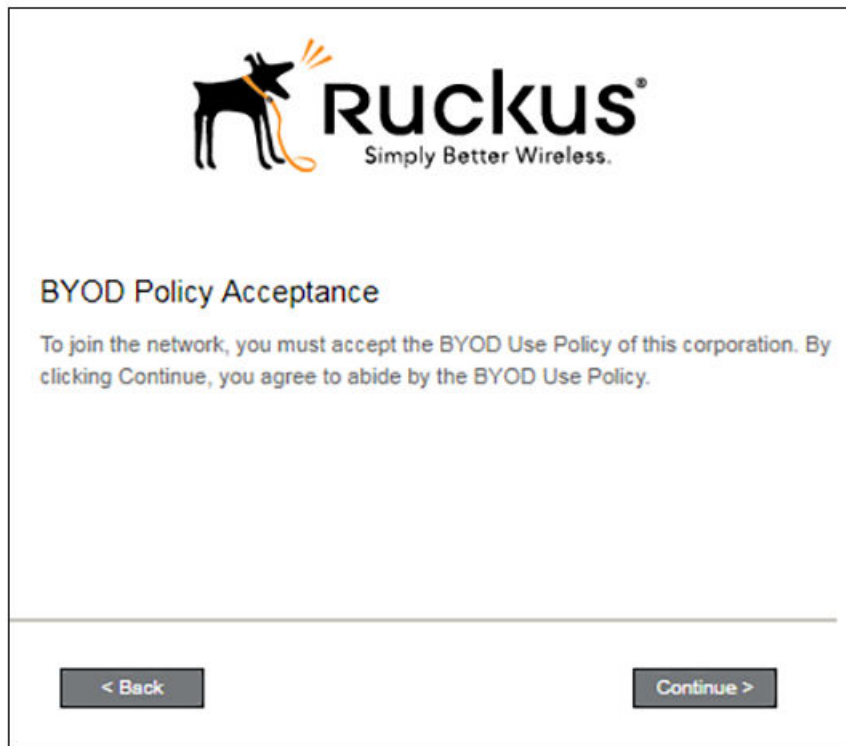
Voucher:

Enter the voucher code and click **Continue**.

BYOD Policy

Typically, you must agree to the terms and policies of the network before you can continue.

FIGURE 6 BYOD Policy



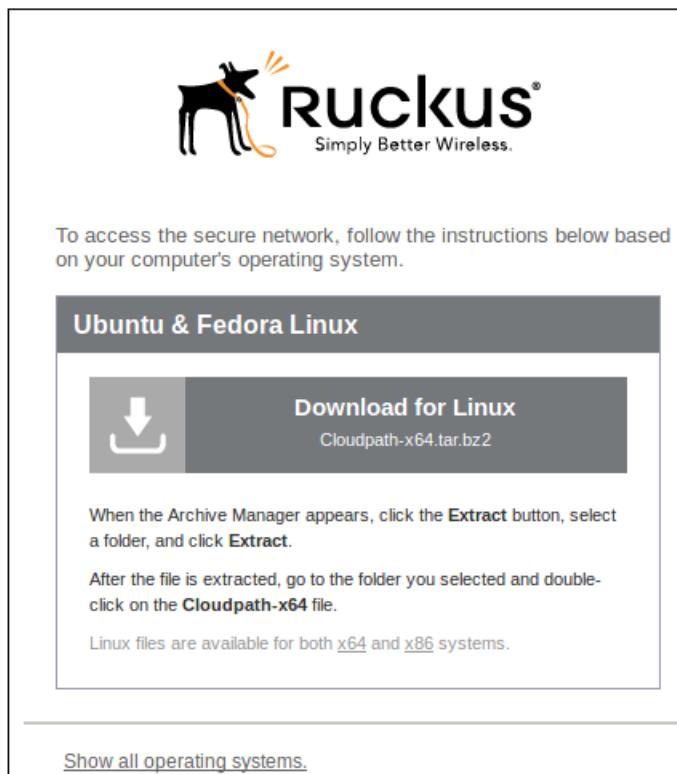
Click **Continue** to continue.

After the enrollment prompts, the user will download and run the configuration Wizard to migrate the device to the secure network.

Linux Download Page

The application detects the user agent for a Fedora or Ubuntu operating system and provides the correct configuration instructions. This screen includes the steps to install the application and to configure the device.

FIGURE 7 Linux Download Page

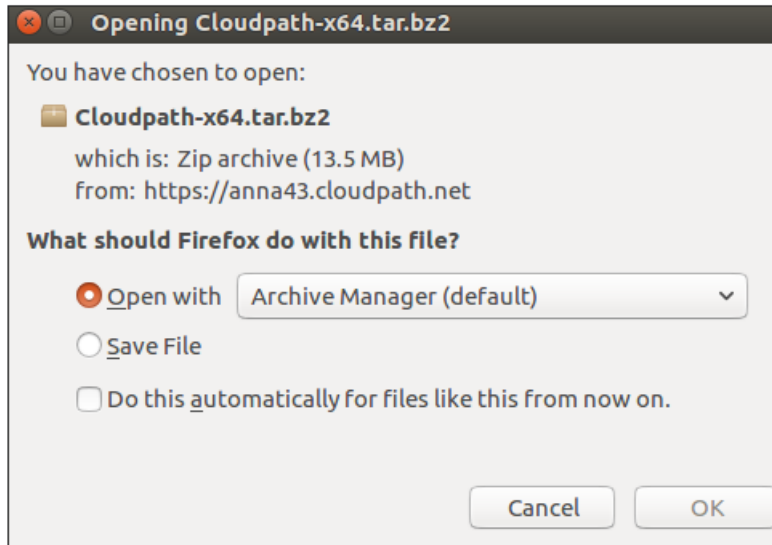


Click the **down arrow** to download the tar file, which contains the application files.

Open Downloaded Files

You can either **Open** with Archive Manager or **Save** to the Downloads folder. The Archive Manager automatically opens the files to extract. You must double-click the tar file in the Downloads folder to open and extract them.

FIGURE 8 Open Download File

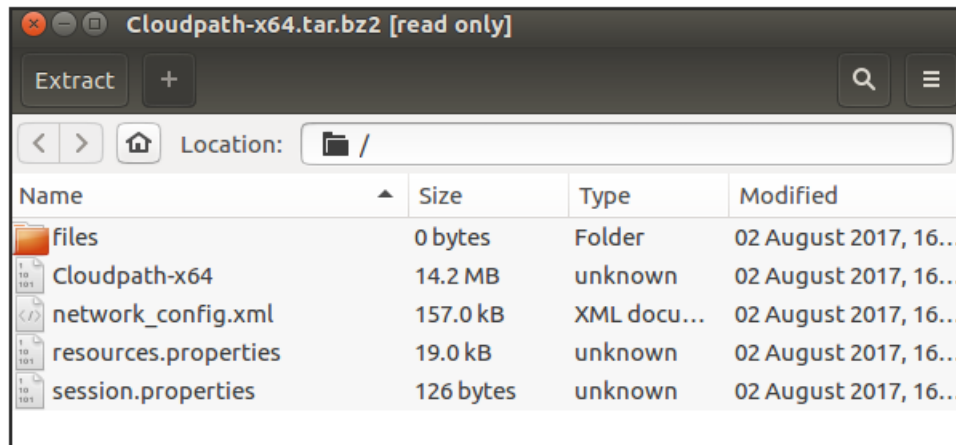


Click **OK** to continue.

Extract Downloaded Files

Extract the application files that were downloaded.

FIGURE 9 Select Files to be Extracted



Select all files and click **Extract**. Choose a location for the extracted files and click **OK**.

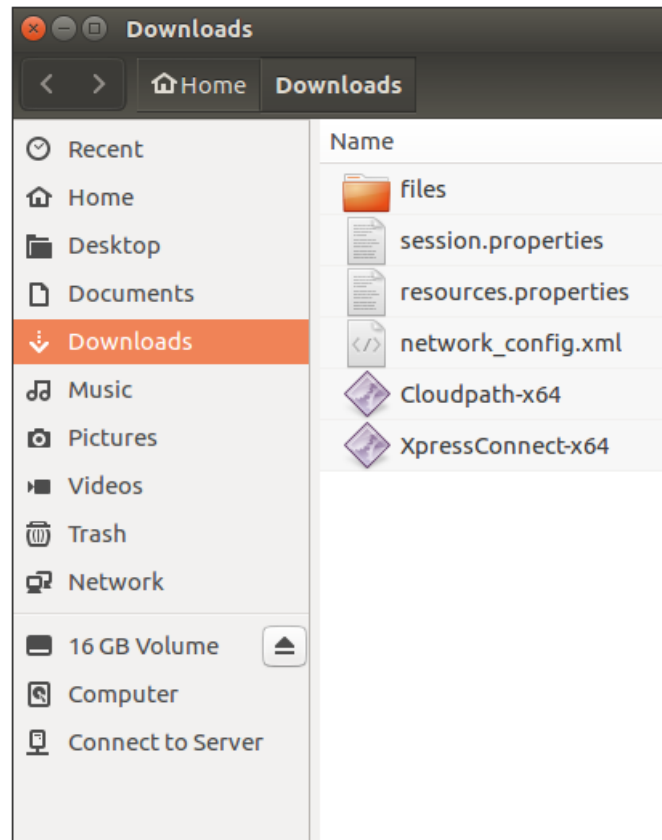
Open Application File

Double-click the **Cloudpath-x64** file to start the application.

NOTE

If you are running a 32-bit OS, run the **Cloudpath-x86** file.

FIGURE 10 Open Application File



The Wizard runs through the configuration and migration process.

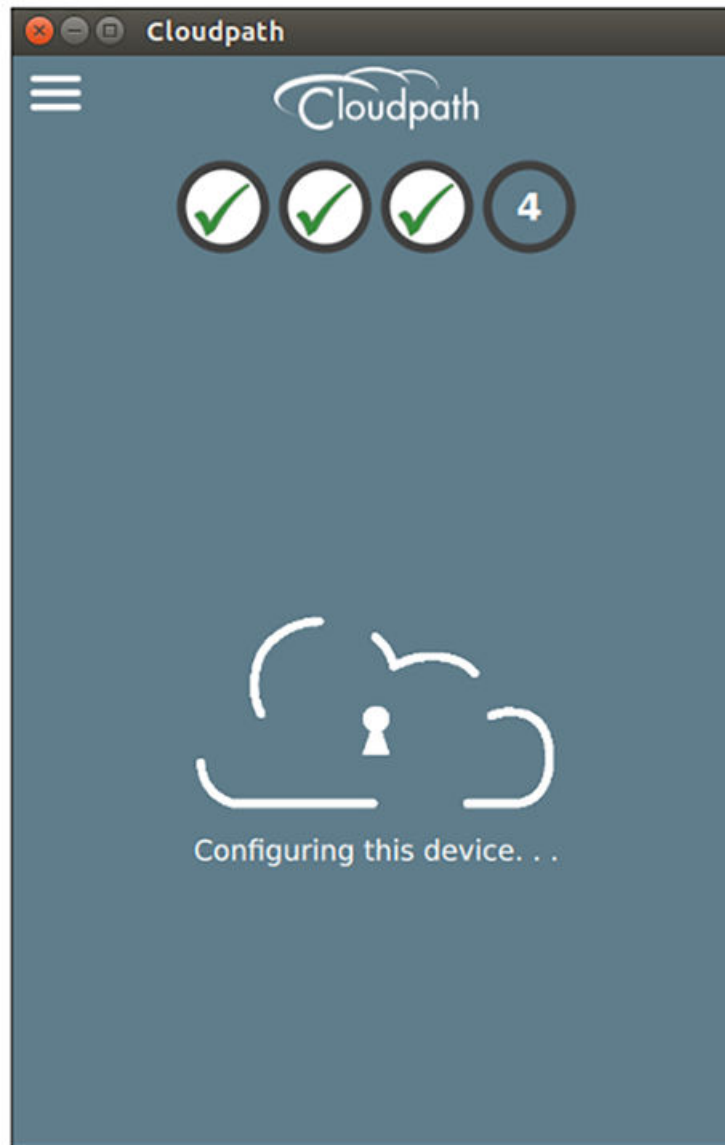
Wizard Application User Experience

After the user has gone through the enrollment prompts, the Wizard runs to configure the wireless network settings on the device.

Configuring the Device

The configuration process begins.

FIGURE 11 Configuring this Device

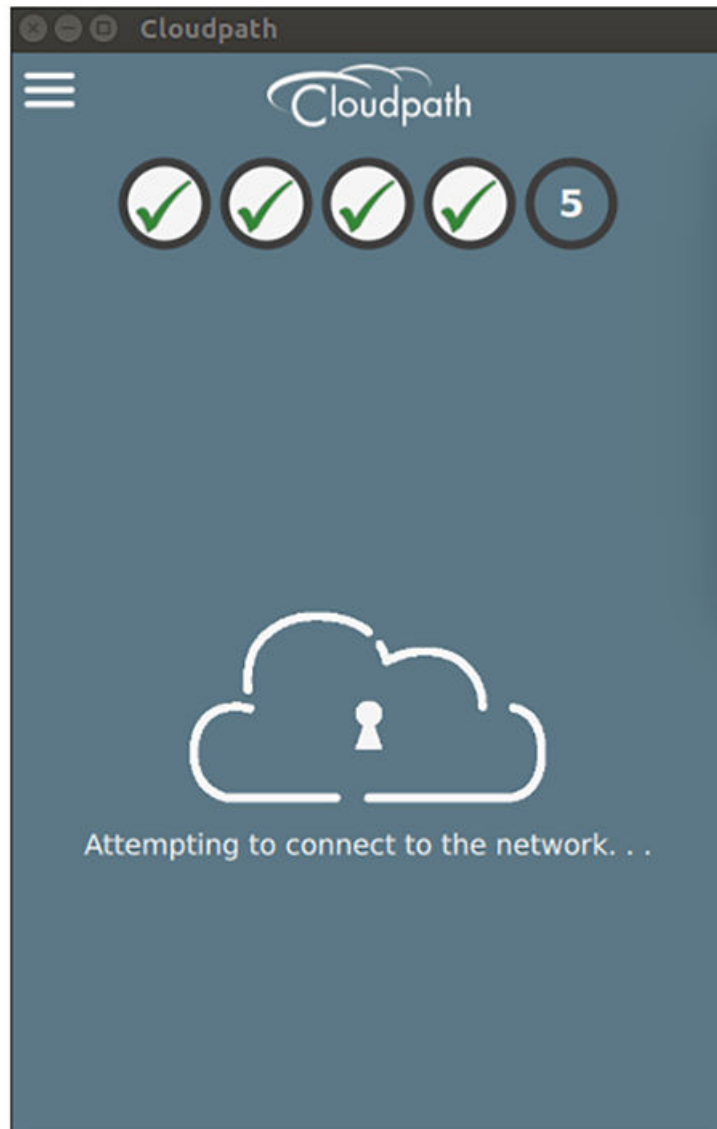


The application continues by attempting to associate to the wireless network.

Attempting to Connect to Secure Network

The application attempts to associate to the wireless network.

FIGURE 12 Attempting to Connect



The application continues with the validation process.

Validating Connectivity

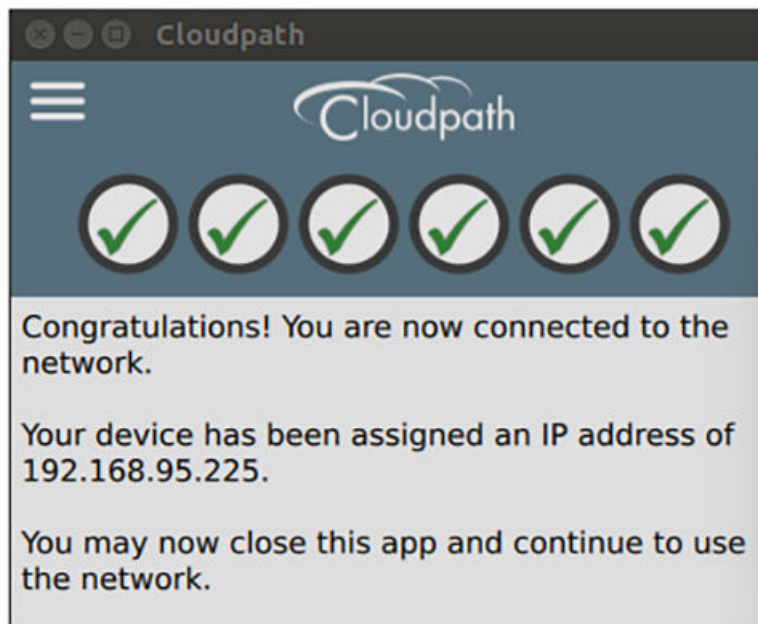
When the association with the secure network is successful, the application attempts to acquire a network address. A screen appears briefly to indicate that connectivity is being validated.

The application continues with the connection process.

Connected to Secure Network

When the application displays a message that you have received an IP address, you are connected to the secure network.

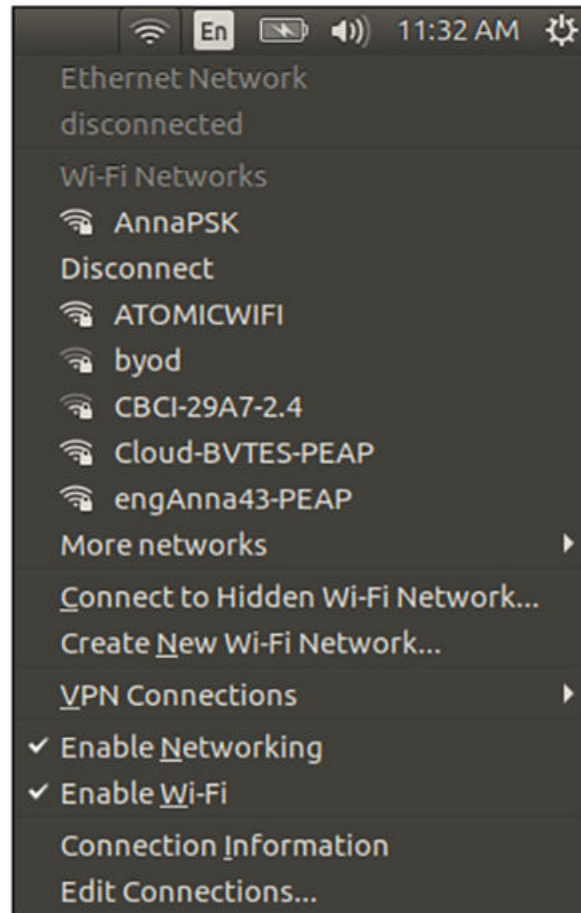
FIGURE 13 Connected to Secure Network



View Network Connection

View the wireless network to verify the Wi-Fi network name.

FIGURE 14 View Wireless Network



The Wi-Fi setting displays the secure network.



Copyright © 2006-2017. Ruckus Wireless, Inc.
350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com