USER GUIDE

Cloudpath End-User Experience for Mac OS X Devices

Supporting Software Release 5.2

Part Number: 800-71669-001
Publication Date: 08 September 2017

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
User Experience 4
Enrollment User Prompts 4
Configuration Wizard 10
Wizard Application User Experience 12
Install Network Profile to Configure Wi-Fi 18

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 Mac OS X to the secure network.

Supported Versions

Cloudpath supports Mac OS X version 10.7, and later, with automated configuration. Versions 10.5 and 10.6 are supported with manual configuration.

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.

Based on the information provided from the enrollment prompts, the Cloudpath wizard (or network profile) contains the wireless configuration to allow the device on the secure network.

Enrollment User Prompts

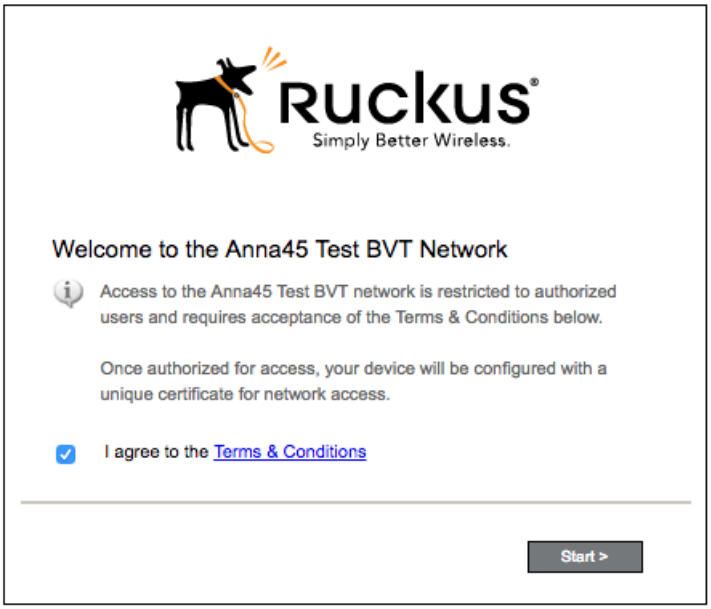
This section displays the user prompts for a typical enrollment workflow. The sequence of steps for the enrollment can differ, depending on the selection that is made.

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 the 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 text and **Start** button can 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 **Employee** workflow branch.

User Credentials

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

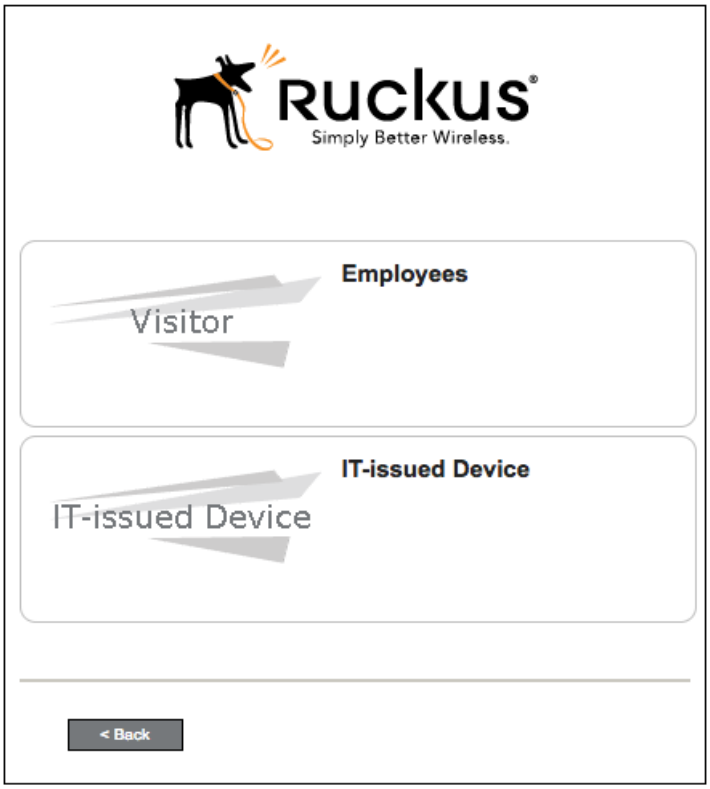
FIGURE 3 User Credential Prompt

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

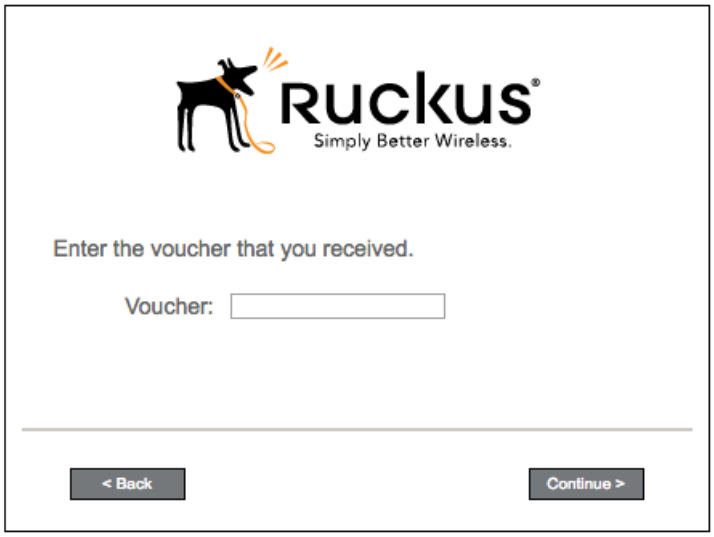


Select a **device type** to continue. This example follows the **IT-Issued Device** enrollment workflow.

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

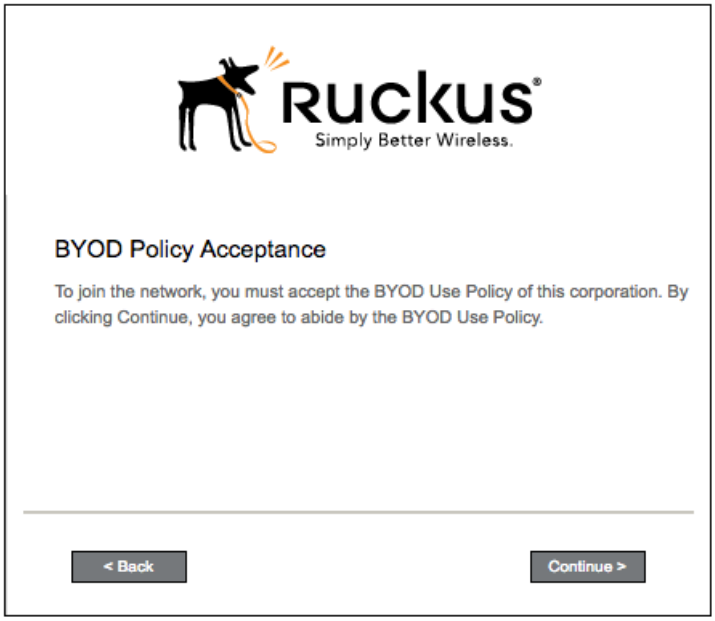


Enter the voucher code and click **Continue**.

BYOD Policy

If configured by the network administrator, you may be prompted to 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.

Configuration Wizard

The enrollment workflow for Mac OS X devices follows the same process as the other OSes. The user accepts the AUP, logs in with Active Directory or other credentials, then the configuration wizard runs to configure the device and migrate the user to the secure network.

The Wizard application can be set to start automatically or start manually from the download page. There is also an option for bypassing the Wizard application and using a network profile to configure the wireless network settings. These user experience options are set in the ES Admin UI, but the user experience can also vary depending on the Java version detected (if installed), the browser, or the OS version on the device.

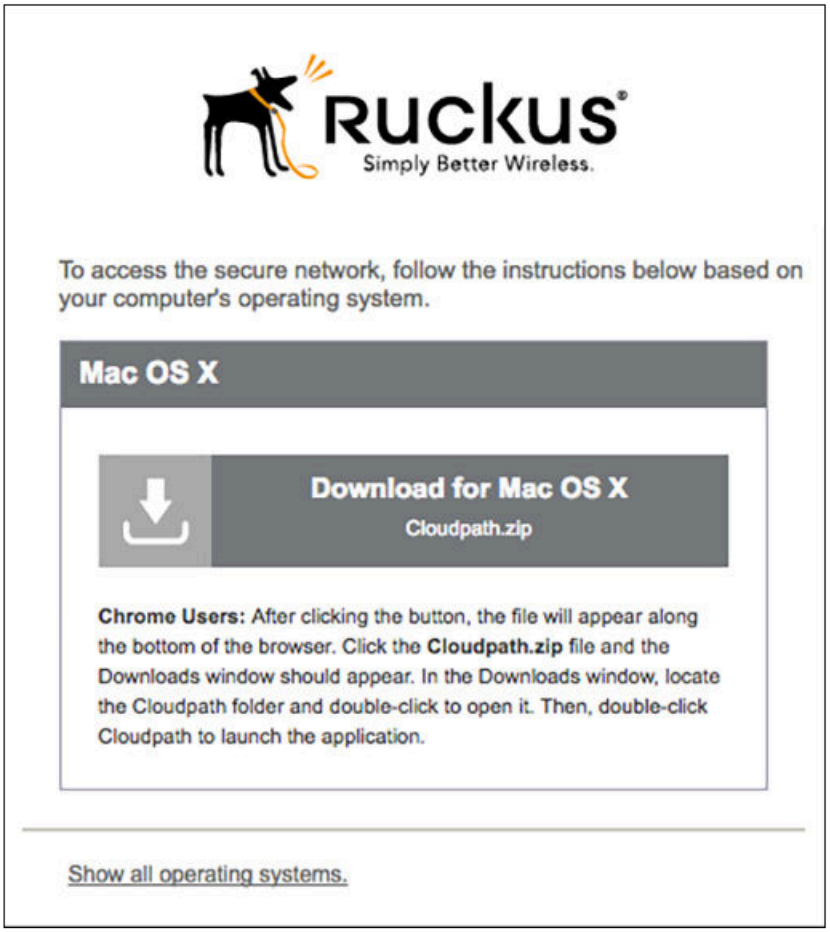
Download and Run Application

The default user experience setting for Mac OS X is to download the application to the user device, run the application to configure the wireless settings, and migrate the device to the secure network.

Download Page

The application detects the device user agent and displays the appropriate Mac OS X-specific download and configuration instructions.

FIGURE 7 Mac OS X Download Page

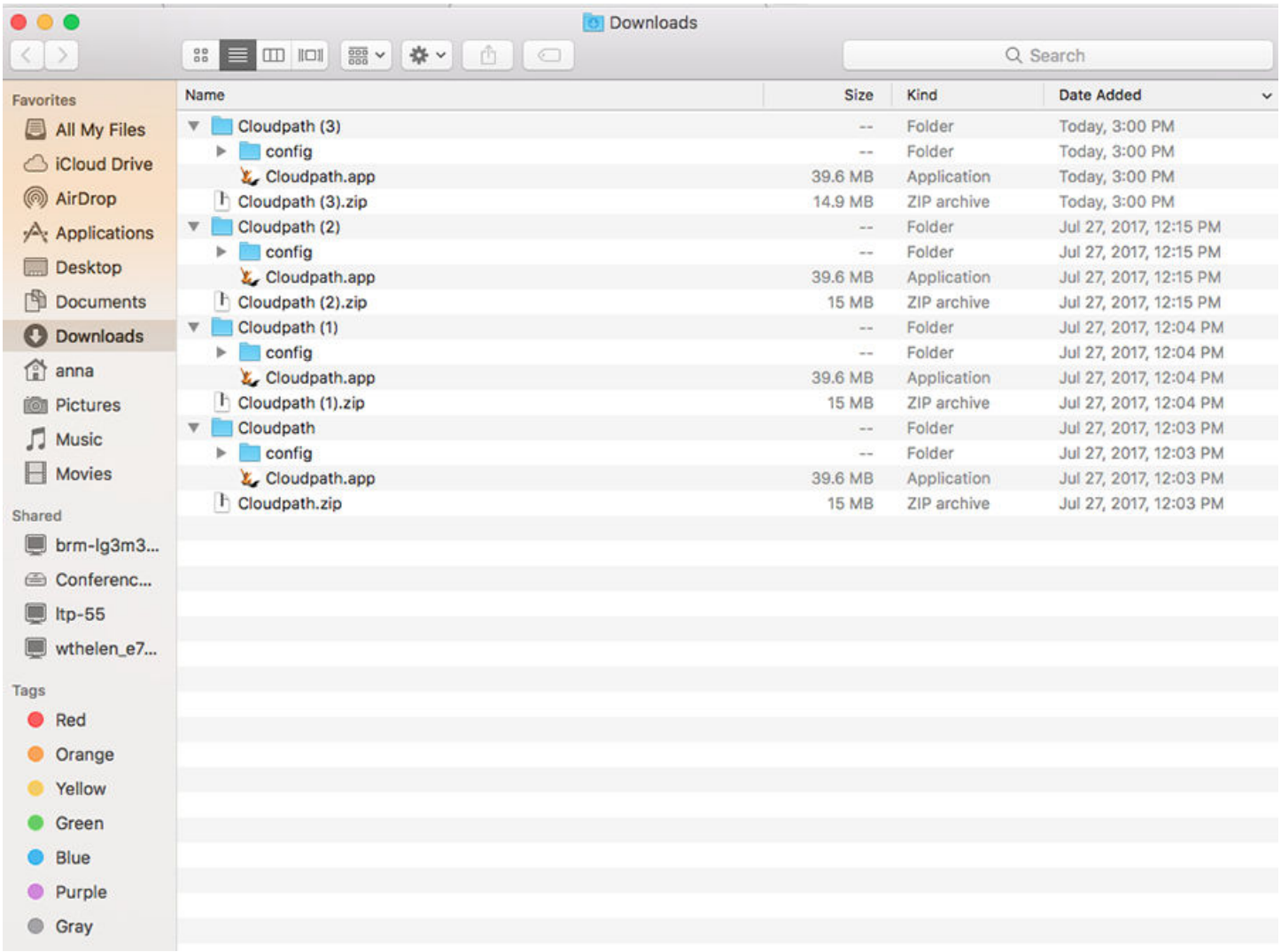


Click the **down arrow** to download the zip file, which contains the application files.

Open Downloaded Files

Browse to the Downloads folder, open the Cloudpath/config folder to locate the Cloudpath application file.

FIGURE 8 Open Download File

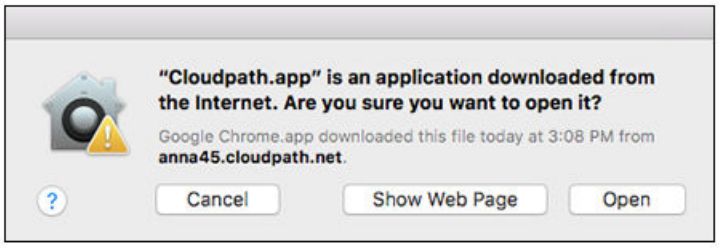


Double-click the Cloudpath application to start the Wizard, which runs through the configuration and migration process.

Confirm Open File

Your browser or operating system may prompt you to confirm that you want to open the application file.

FIGURE 9 Confirm Open File



Click **Open** to continue.

Wizard Application User Experience

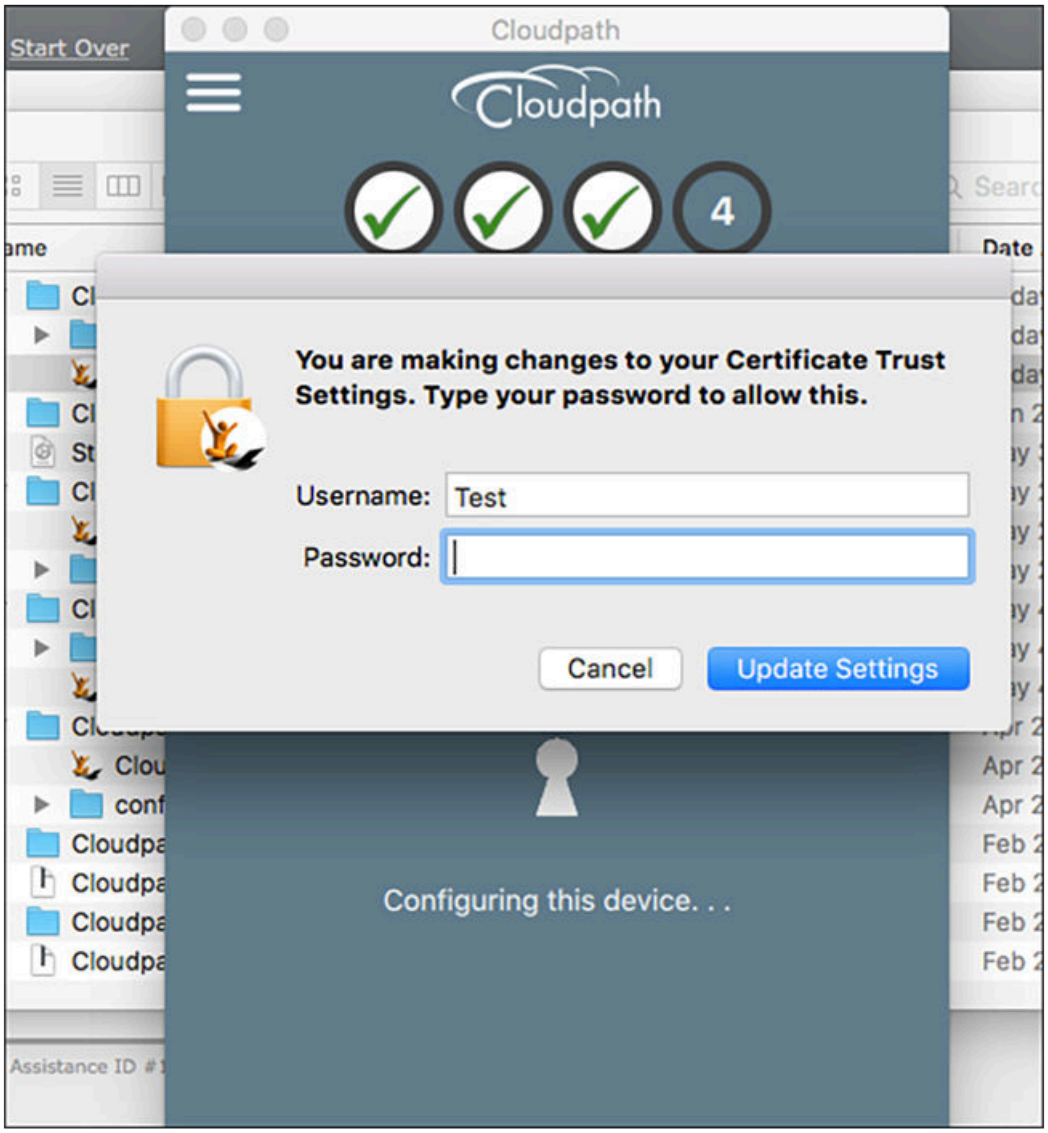
After the user has gone through the enrollment prompts, the Wizard runs to configure the wireless network settings on the device.

Administrator Credentials

The operating system requires elevated privileges to load certificates on the device. As the configuration process begins, you may be prompted multiple times to enter the administrator credentials for your device.

Certificate Trust Settings

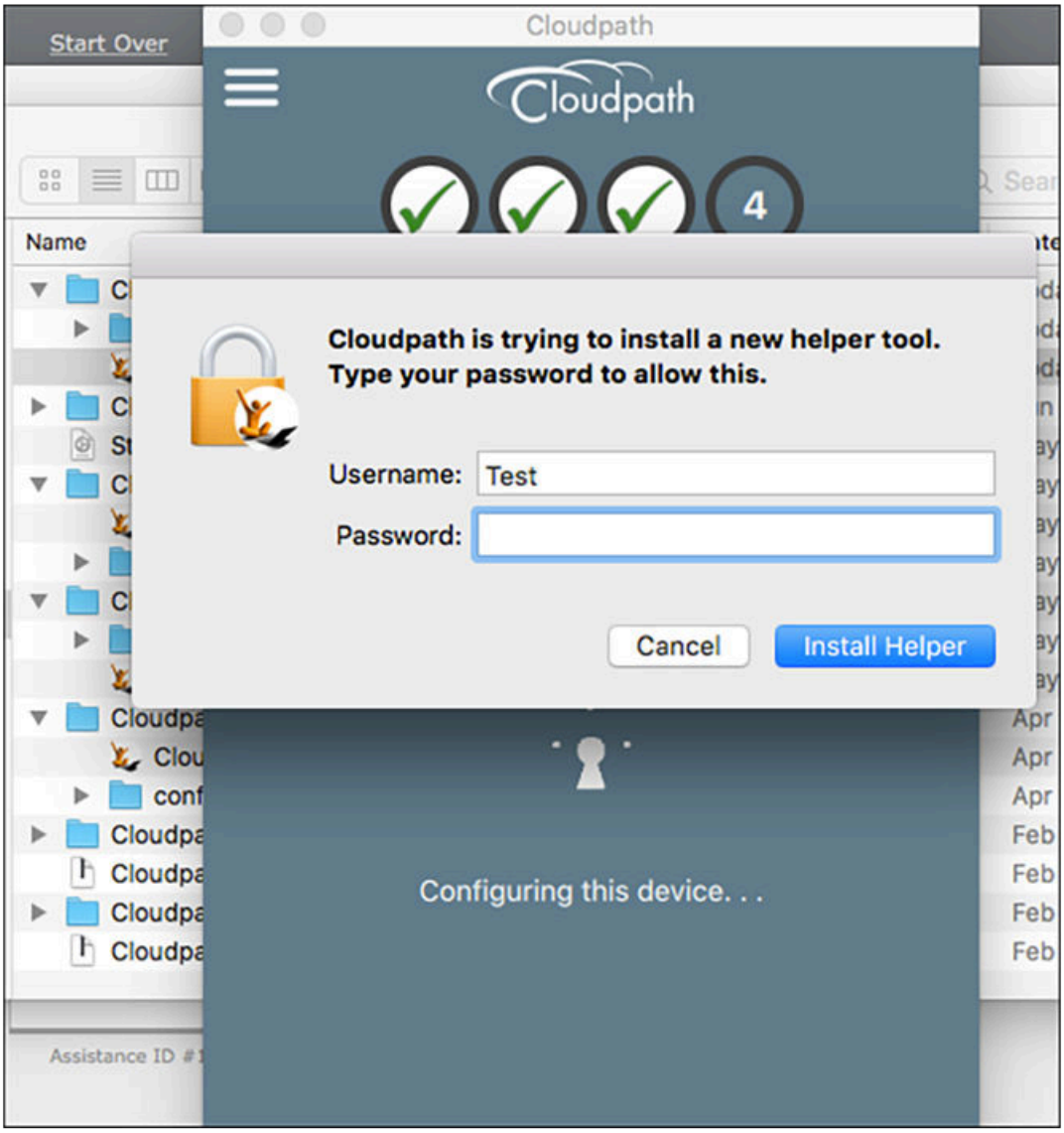
FIGURE 10 Enter Credentials for Certificate Trust Settings



Enter the password and click **Update Settings**. The application continues with the configuration process.

Helper tool

FIGURE 11 Enter Credentials for Helper Tool



Enter the password and click **Install Helper**. The application continues with the configuration process.

Configuration Profile Tool

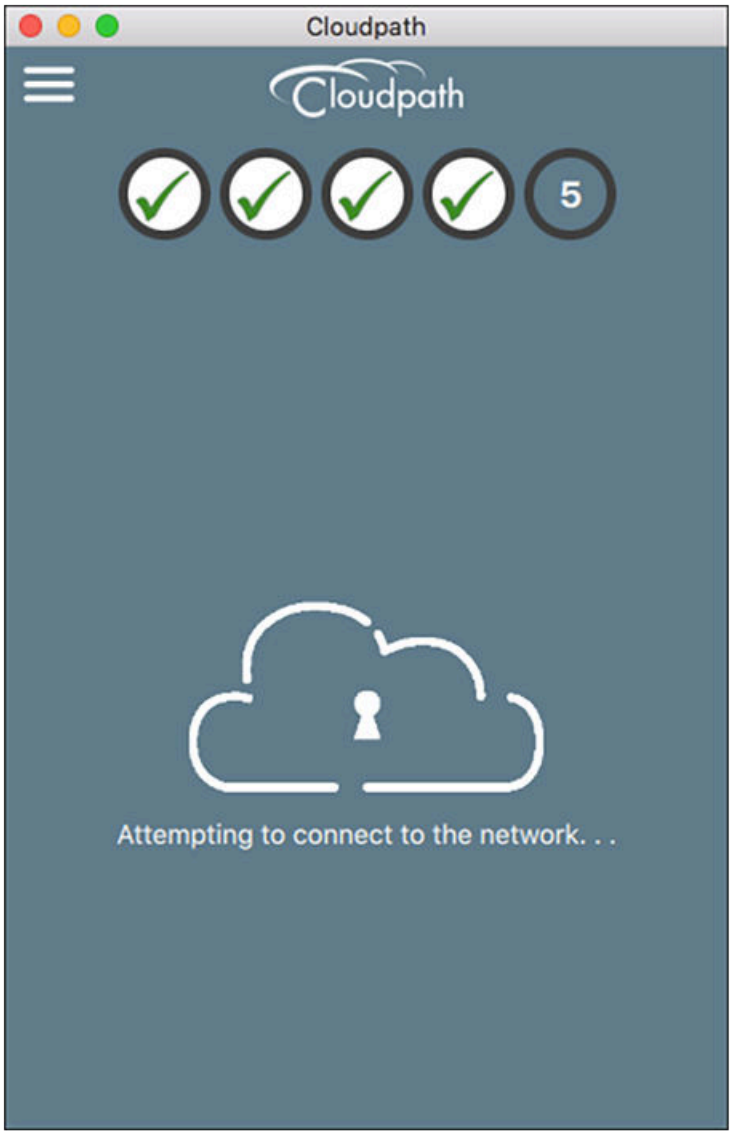
FIGURE 12 Enter Credentials for Configuration Profile Tool

Enter the password and click **OK**. The application continues.

Attempting to Connect to Secure Network

The application attempts to associate to the wireless network.

FIGURE 13 Attempting to Connect to Secure Network



The application continues with the validation process.

Validating Connectivity

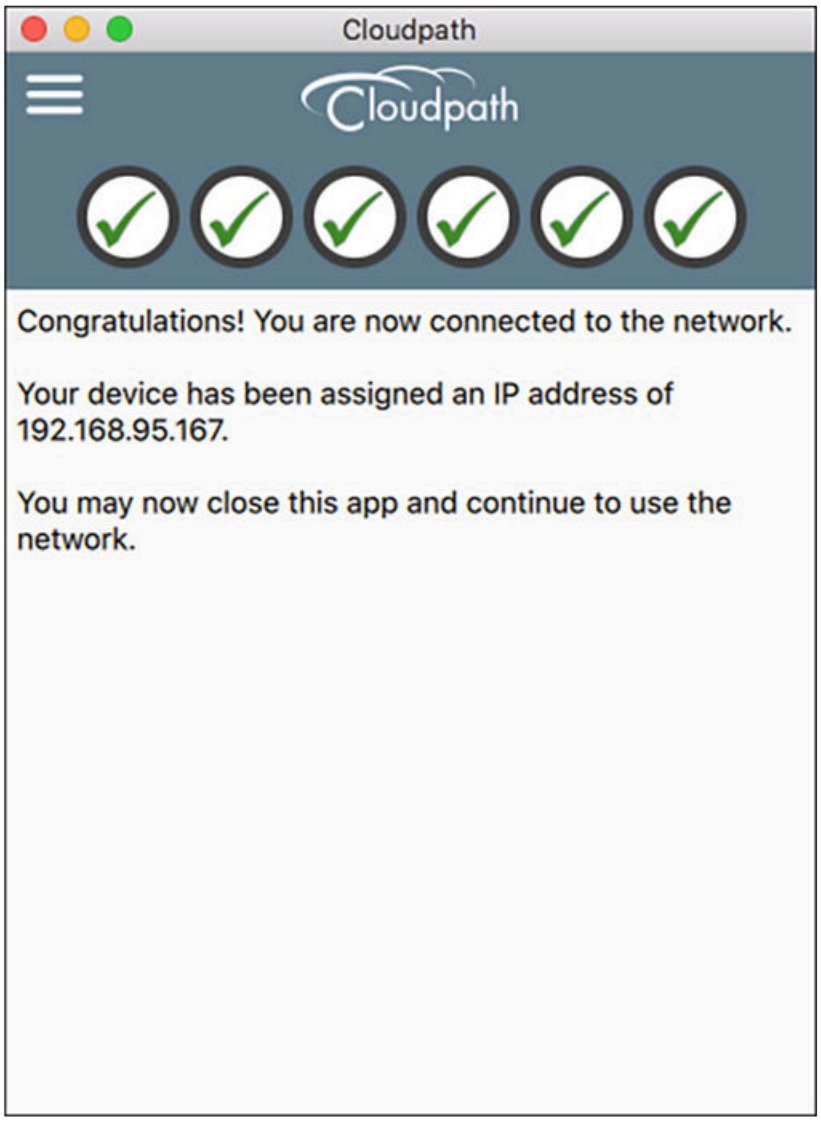
When the association with the secure network is successful, the application attempts to acquire a network address. A screen appears briefly to indicate that connectivity is being validated.

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.

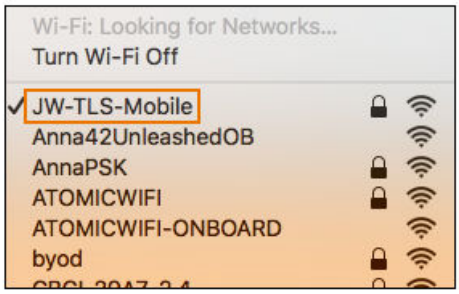
FIGURE 14 Connected to Secure Network



Verify Network Connection

Whether using the application to migrate the device, or manually connecting to the network, use the **airport** icon in the menu bar to verify the network to which you are connected.

FIGURE 15 Secure Network



A check mark indicates the network to which you are connected.

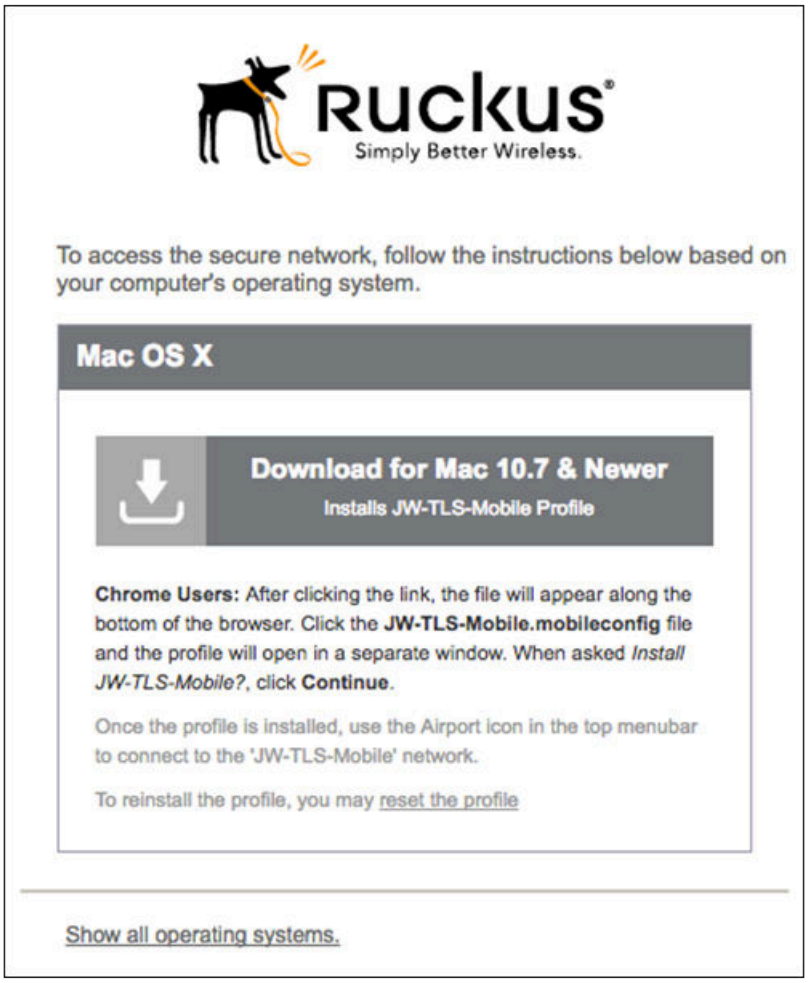
Install Network Profile to Configure Wi-Fi

Alternatively, the network administrator can set the Mac OS X user experience to download and configure the wireless settings on the device using a network profile.

Download Page

If the user experience is set to use a network profile, the **Profile Download** page displays after the user has gone through the enrollment workflow steps.

FIGURE 16 Download Profile Page

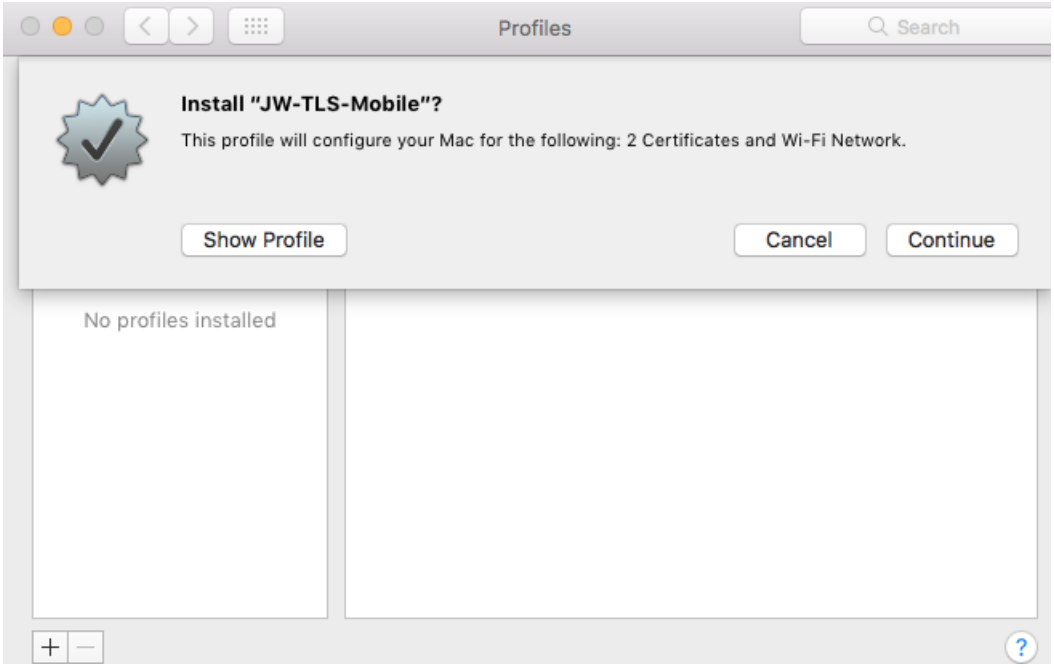


Click the **down arrow** to download the profile. If a profile has been previously installed, use the **Reset the Profile** link.

Install Profile

You are prompted to install the network profile on the device.

FIGURE 17 Install Profile



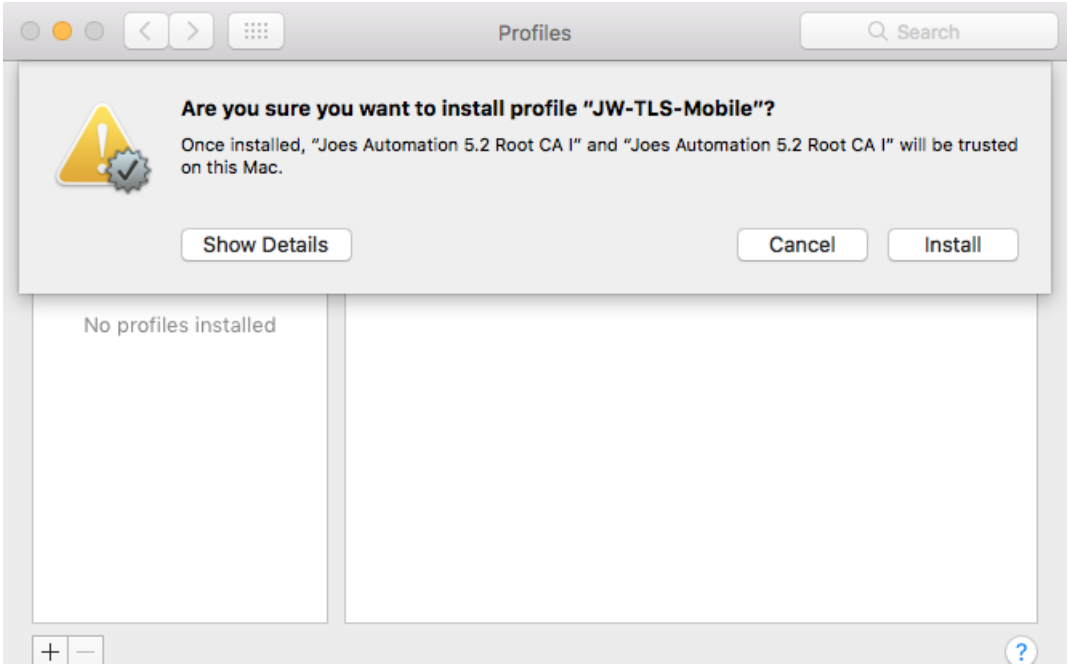
Click **Show Profile** to view profile details. Click **Continue** (or Install) to install the network profile.

Continue with profile installation.

Install Profile Confirmation

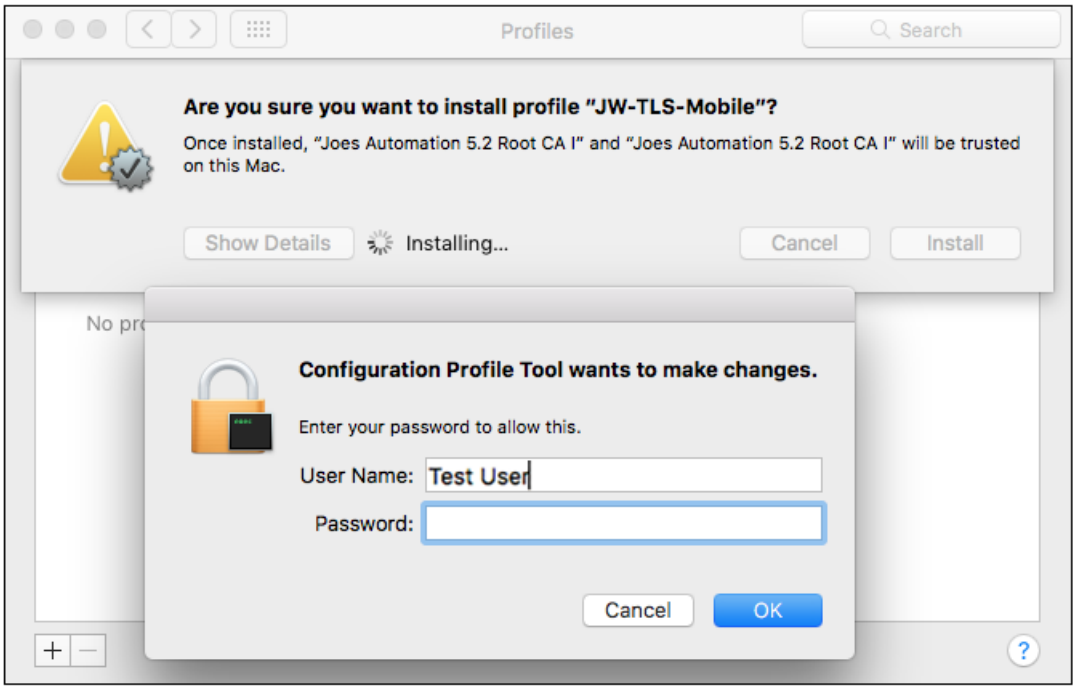
You are prompted to confirm that you want to install the network profile on the device.

FIGURE 18 Install Profile Confirmation Prompt



Click **Install** to continue. You may be prompted to again enter the administrator credentials for your device.

FIGURE 19 Enter Credentials for Configuration Profile Tool

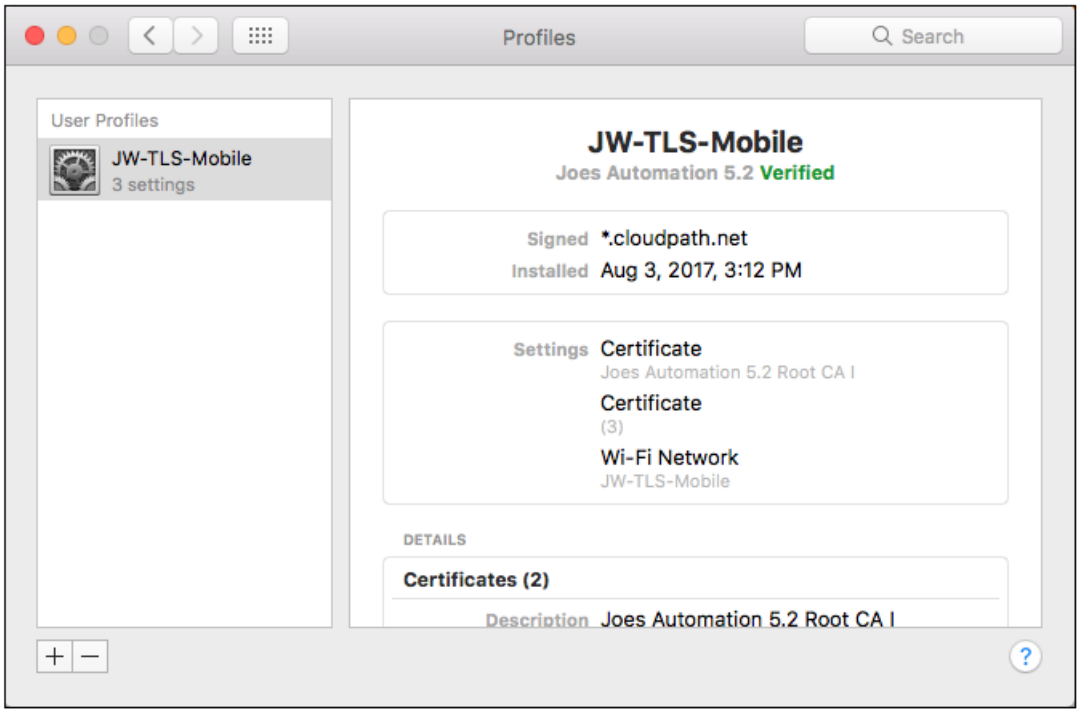


Enter the password and click **OK**.

Profile installed

The profile has been installed when you receive this confirmation page.

FIGURE 20 Profile Installed

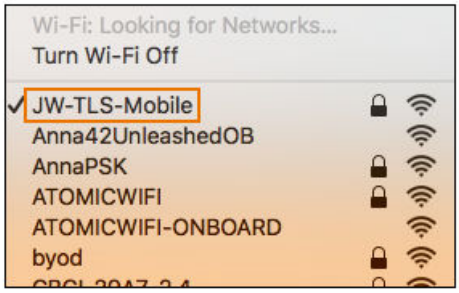


Close this page and proceed with connecting to the wireless network.

Join Wireless Network

When the wireless configuration is installed using a network profile, you must manually connect to the secure network. Use the **airport** icon in the top menu bar to select the specified network.

FIGURE 21 Secure Network



A check mark indicates the network to which you are connected.

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