

Cloudpath Enrollment System for Mac OS X Devices End-User Guide, 5.4

Supporting Cloudpath Software Release 5.4

Copyright, Trademark and Proprietary Rights Information

© 2019 ARRIS Enterprises LLC. 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 ARRIS International plc and/or its affiliates ("ARRIS"). ARRIS reserves the right to revise or change this content from time to time without obligation on the part of ARRIS 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, ARRIS 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. ARRIS 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. ARRIS 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 ARRIS 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 ARRIS, ARRIS 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 ARRIS 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

ARRIS, the ARRIS logo, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, Edgelron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Overview	4
Supported Versions.....	4
User Experience	4
Enrollment User Prompts.....	4
Configuration Wizard.....	10
Wizard Application User Experience.....	13
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 10.10 and later with automated configuration. Manual configuration is not supported.

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

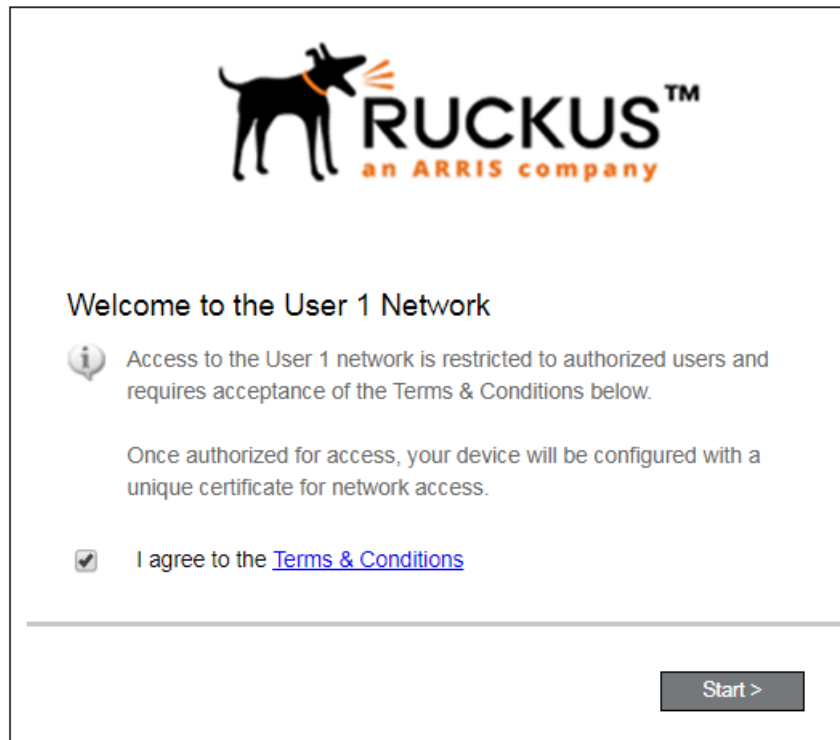
When the user enters the enrollment URL on their device, the Login (or Welcome) screen displays.

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 receive 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

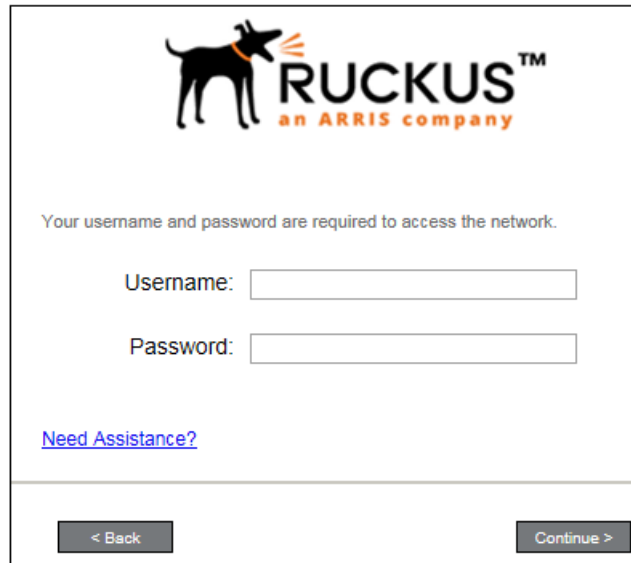


Select the user type to continue. This example follows the *Employee* workflow branch.

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



RUCKUS™
an ARRIS company

Your username and password are required to access the network.

Username:

Password:

[Need Assistance?](#)

< Back Continue >

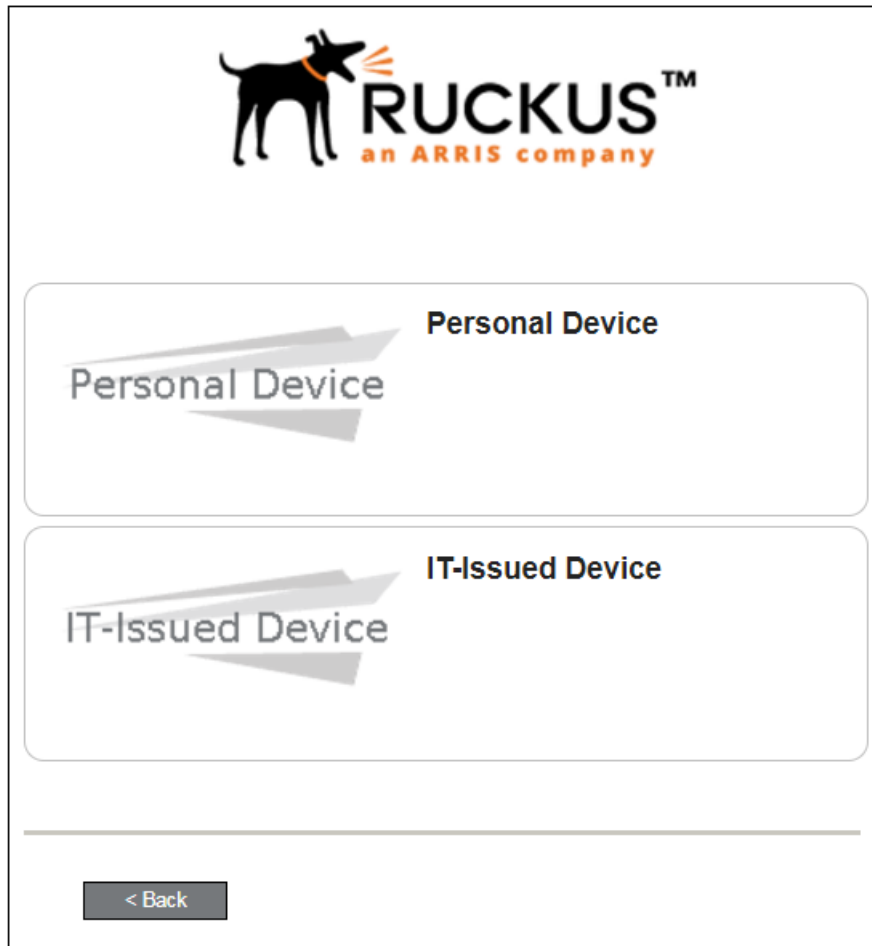
Enter the user credentials and click **Continue**.

Device Type

If required by the network, the user might receive a Device Type prompt.

An example is that a personal device selection might add a prompt for a MAC address, and an IT-Issued device would be allowed to bypass the MAC address prompt.

FIGURE 4 Device Type Prompt



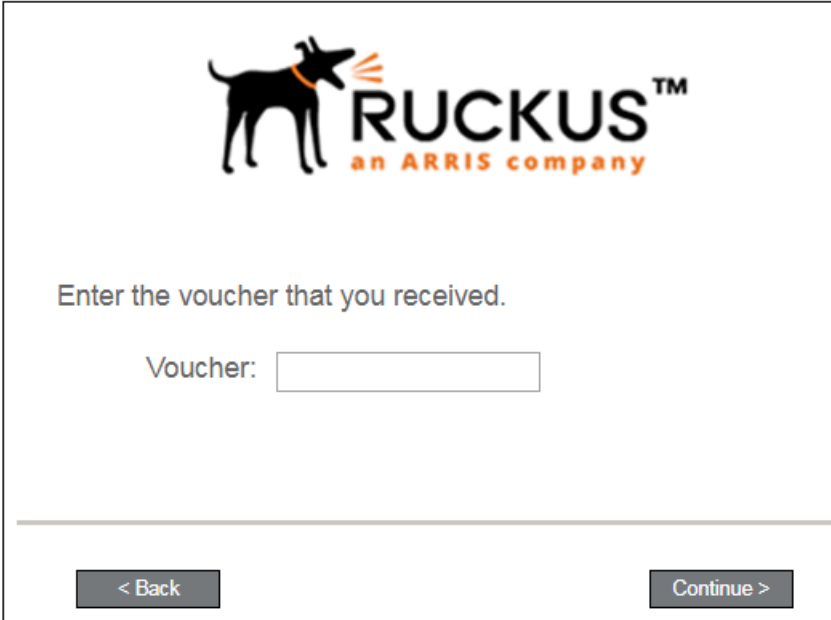
Select a device type to continue. This example follows the IT-Issued Device enrollment workflow.

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



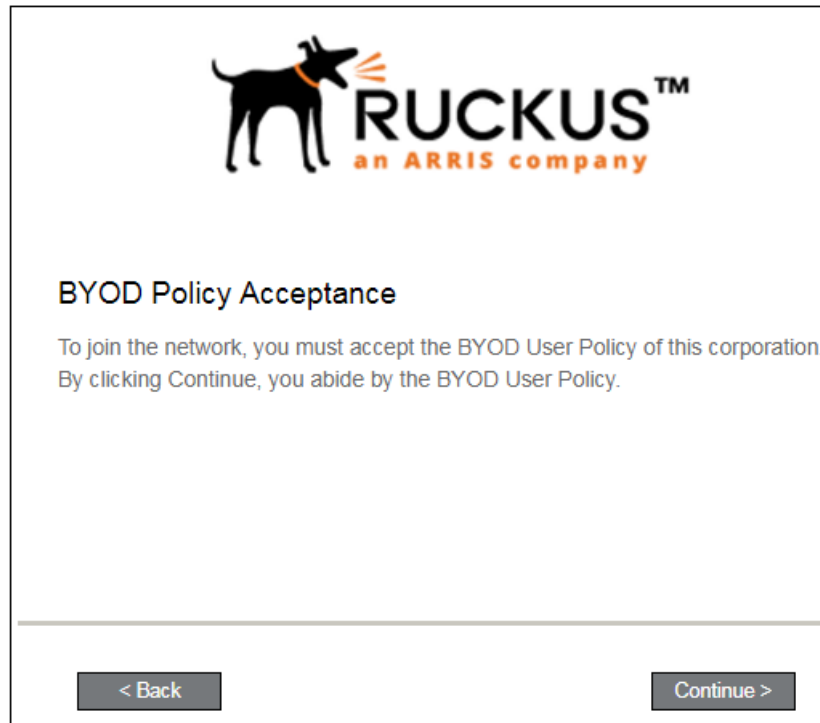
The screenshot shows a user interface for entering a voucher code. At the top center is the Ruckus logo, which consists of a black silhouette of a dog with an orange collar and three orange signal waves to its right. To the right of the dog, the word "RUCKUS" is written in a large, bold, black sans-serif font, with a trademark symbol (TM) to its upper right. Below "RUCKUS", the text "an ARRIS company" is written in a smaller, orange, lowercase sans-serif font. Below the logo, the text "Enter the voucher that you received." is displayed in a gray sans-serif font. Underneath this text, the word "Voucher:" is followed by a rectangular text input field. At the bottom of the screen, there is a horizontal line. Below this line are two gray buttons: one on the left labeled "< Back" and one on the right labeled "Continue >".

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 with BYOD configuration.

FIGURE 6 BYOD Policy



Click **Start** 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.

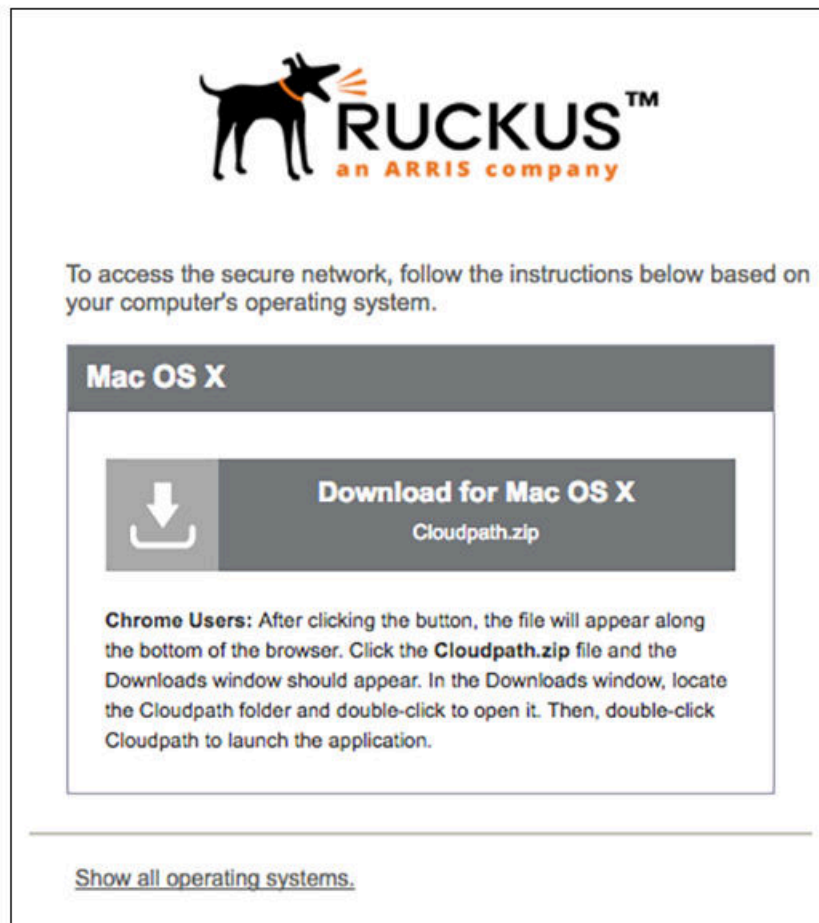
Download and Run Application

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

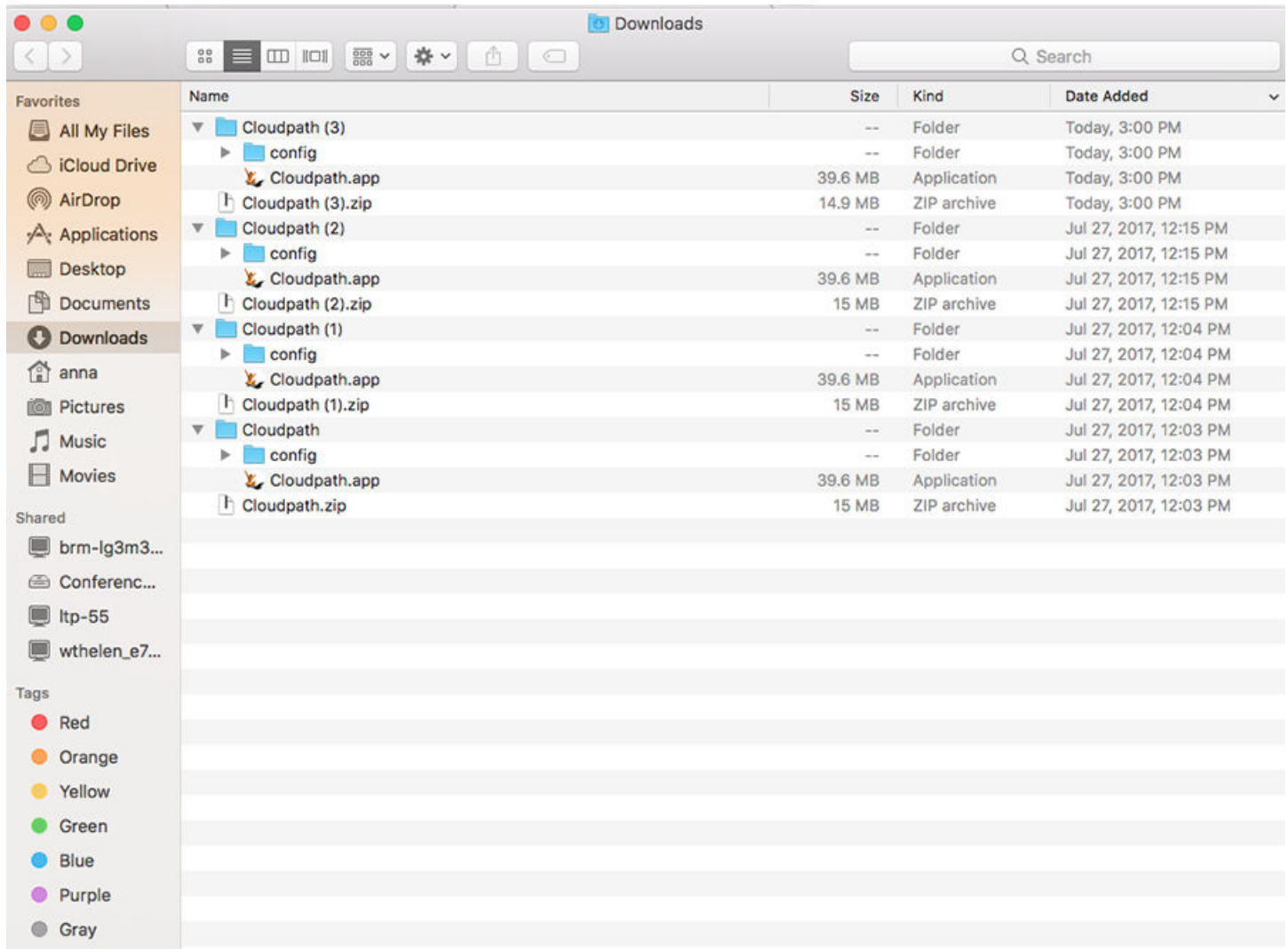


Click the **down arrow** to download the zip file, which contains the application files.

Open Downloaded Files

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

FIGURE 8 Open Download File

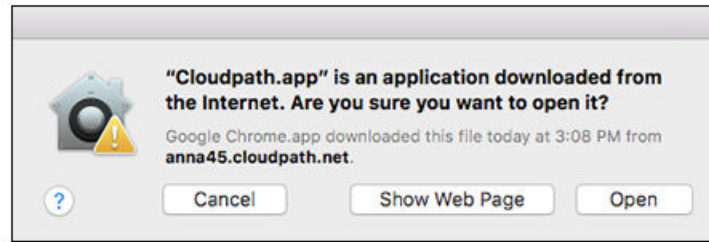


Double-click the Cloudpath application to start the Wizard, which runs through the configuration and migration process.

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

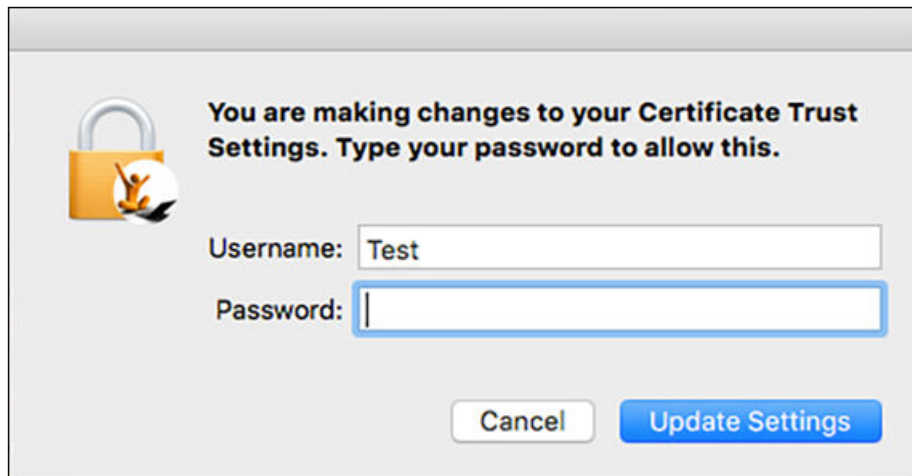
After the user has gone through the enrollment prompts, the Wizard runs to configure the wireless network settings on the device.

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

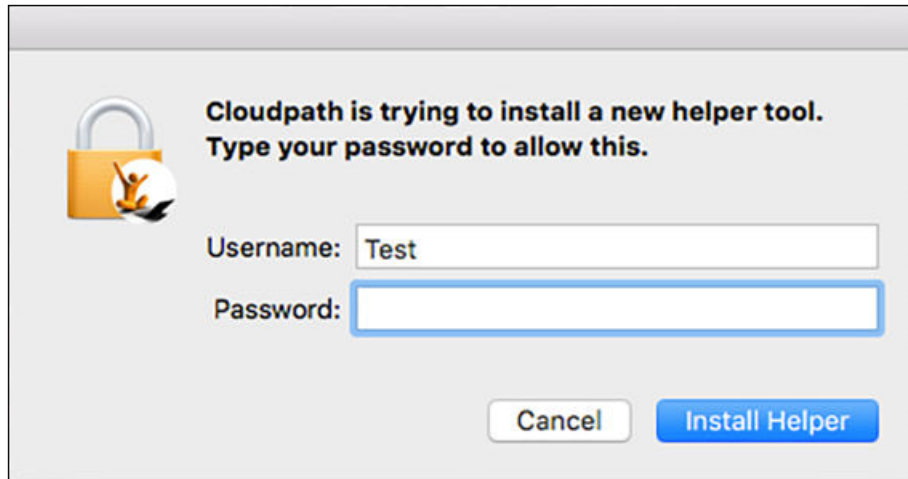
FIGURE 10 Enter Credentials for Certificate Trust Settings



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

Helper tool

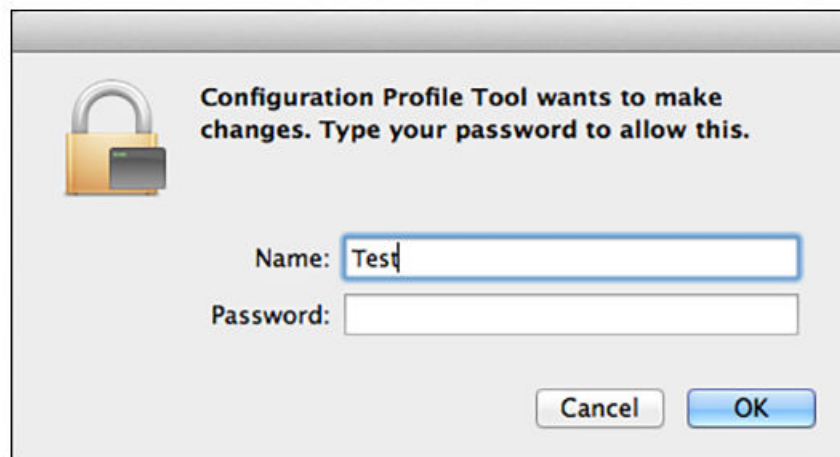
FIGURE 11 Enter Credentials for Helper Tool



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

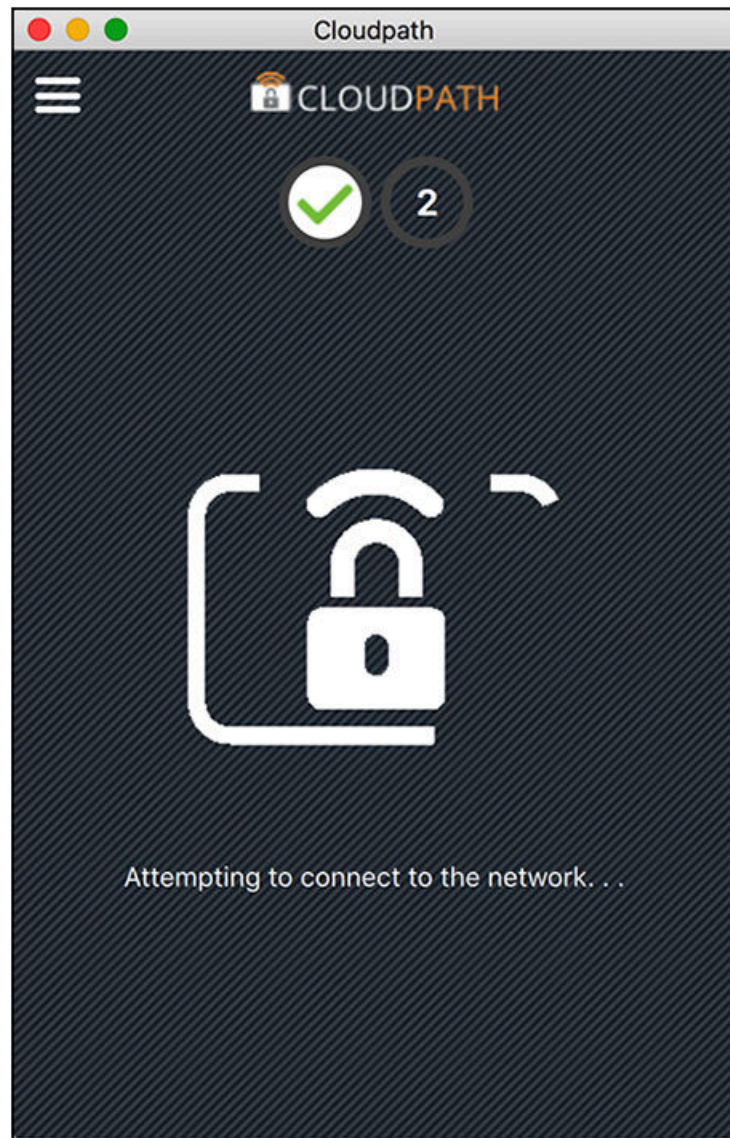


Enter the password and click **OK**. The application continues.

Attempting to Connect to Secure Network

The application attempts to associate to the wireless network.

FIGURE 13 Attempting to Connect to Secure Network

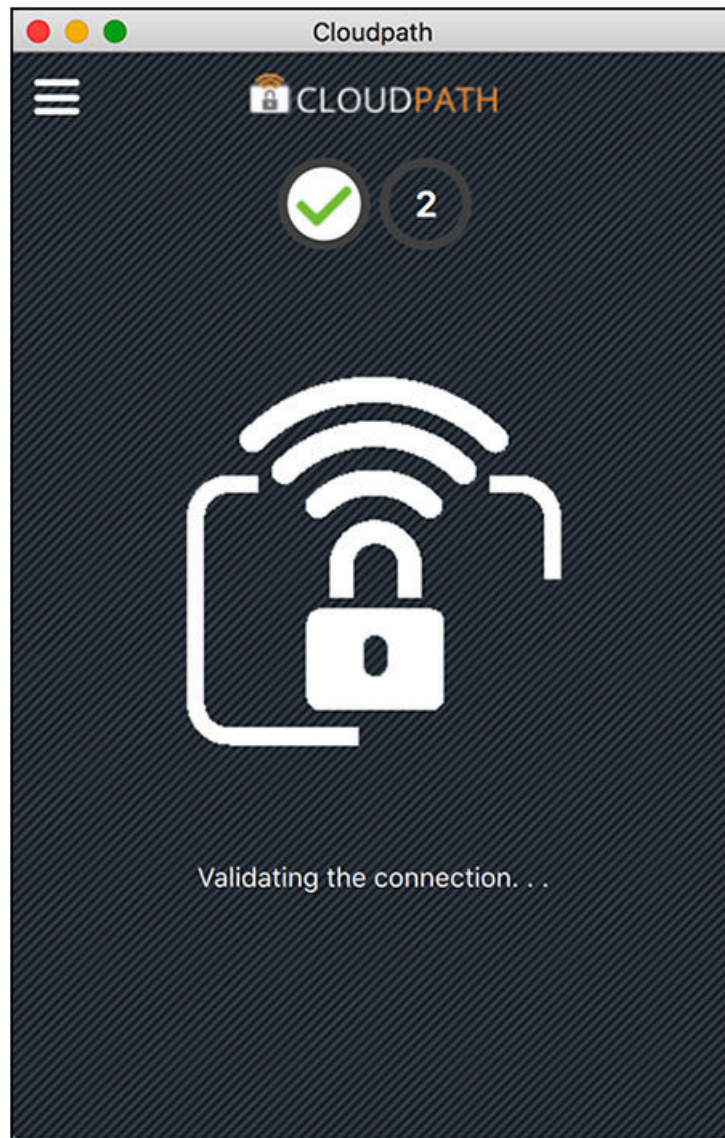


The application continues with the validation process.

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:

FIGURE 14 Validating Connectivity

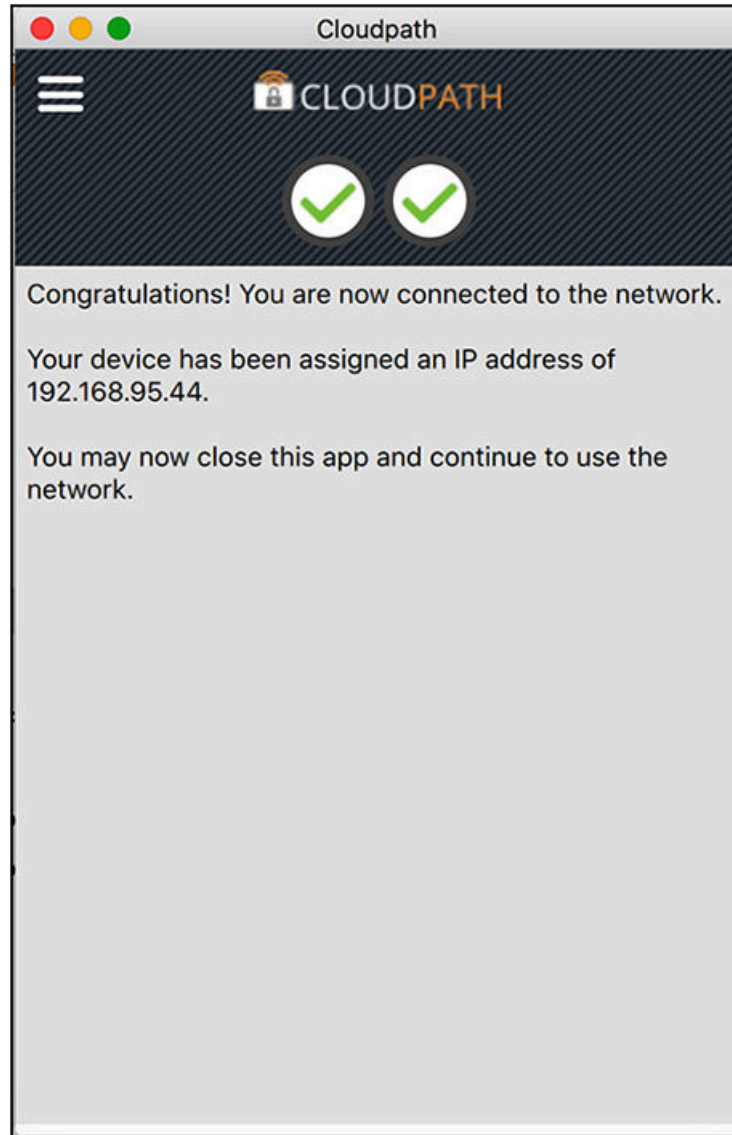


The application continues with the connection process.

Connected to Secure Network

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

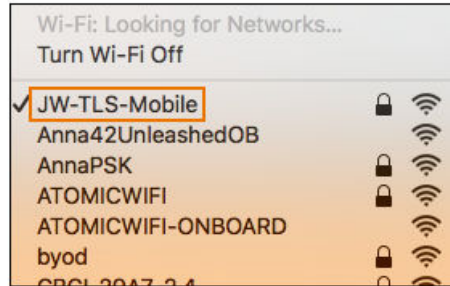
FIGURE 15 Connected to Secure Network



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 16 Secure Network



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

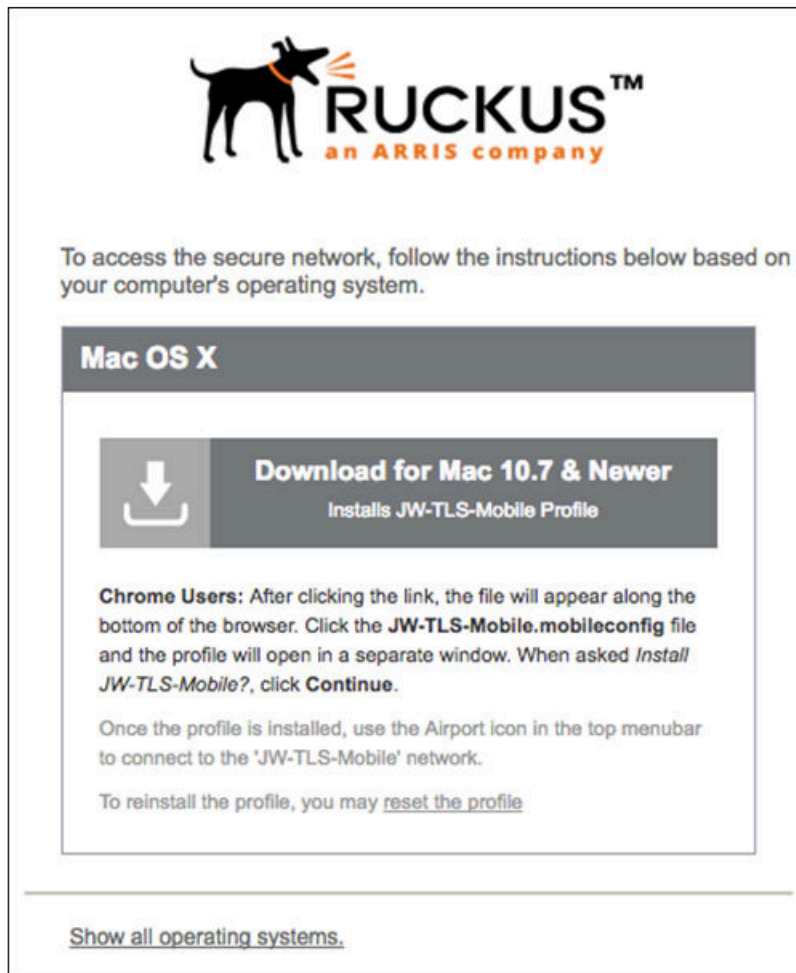
Install Network Profile to Configure Wi-Fi

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 17 Download Profile Page

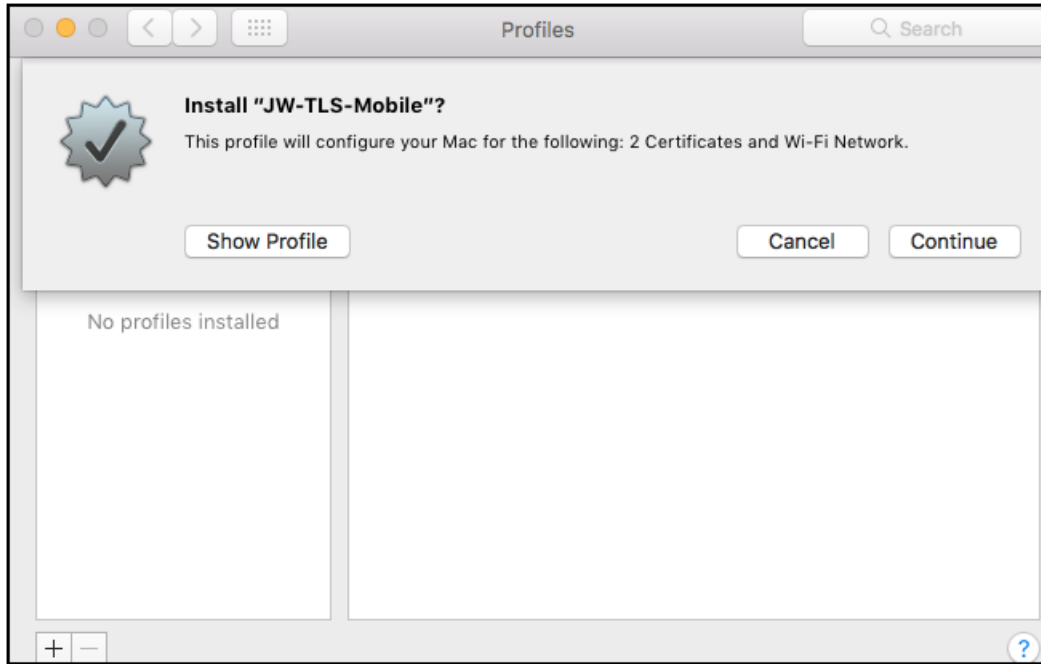


Click the **down arrow** to download the profile. If a profile has been previously installed, use the **Reset the Profile** link.

Install Profile

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

FIGURE 18 Install Profile

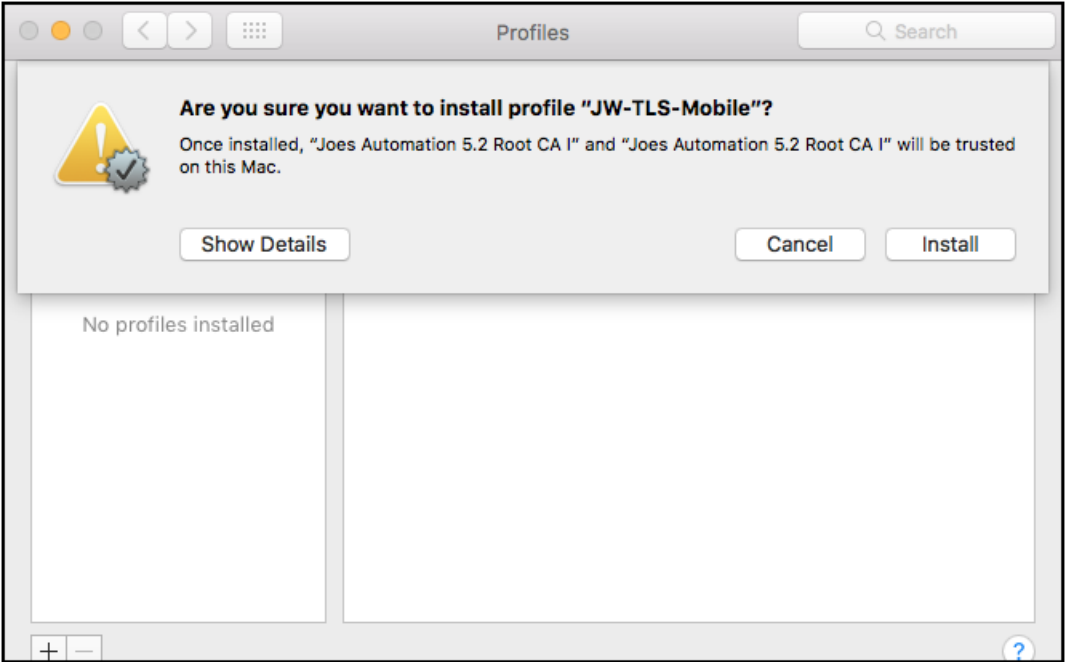


Click **Show Profile** to view profile details. Click **Continue** (or Install) to install the network profile.
Continue with profile installation.

Install Profile Confirmation

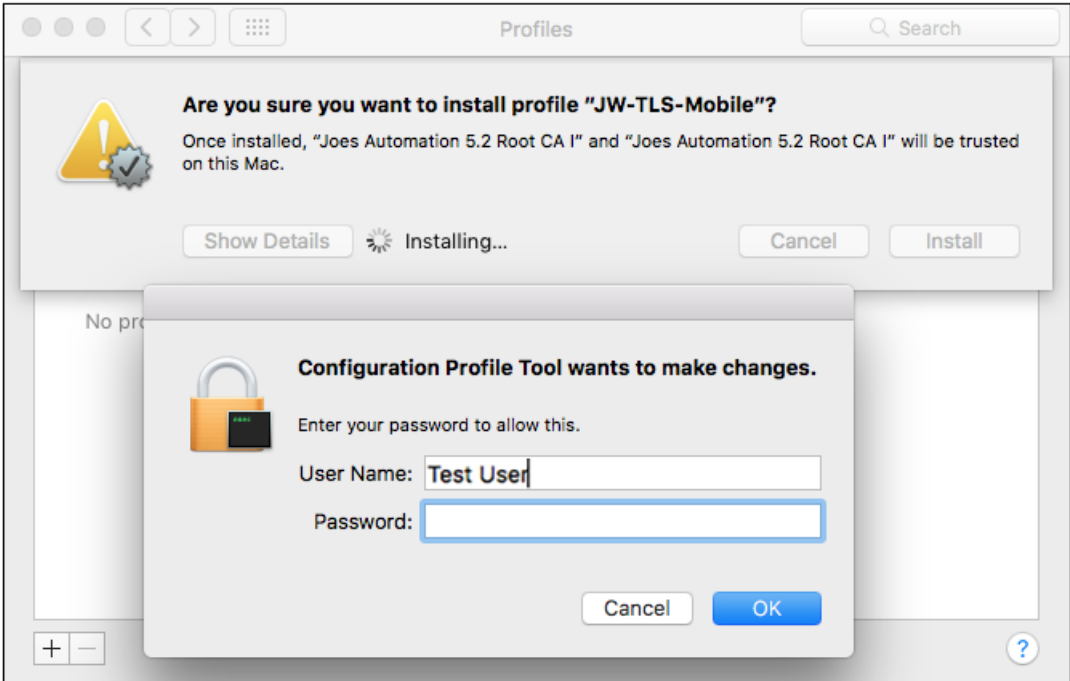
You are prompted to confirm that you want to install the network profile on the device.

FIGURE 19 Install Profile Confirmation Prompt



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

FIGURE 20 Enter Credentials for Configuration Profile Tool

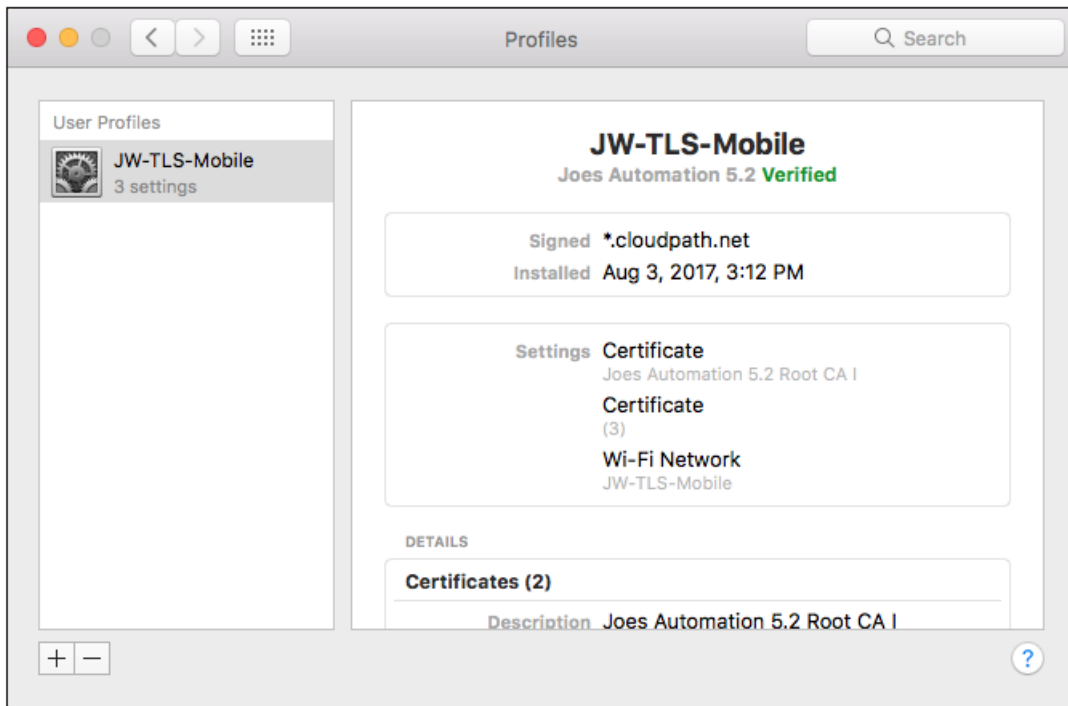


Enter the password and click **OK**.

Profile installed

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

FIGURE 21 Profile Installed

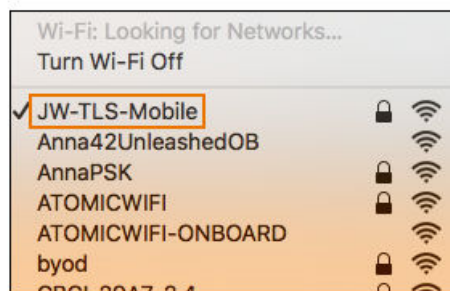


Close this page and proceed with connecting to the wireless network.

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 22 Secure Network



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



© 2019 ARRIS Enterprises LLC. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com