

Cloudpath Enrollment System for Managed and Unmanaged Chromebooks 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 Devices.....	4
Cloudpath User Experience	4
Enrollment Workflow.....	4
Managed or Unmanaged Chromebooks.....	8

Overview

The Cloudpath Enrollment System (ES) extends the benefits of certificates to Chromebooks in environments with an existing Public Key Infrastructure (PKI).

The certificate is installed in the Trusted Platform Module (TPM), and can be used for certificate-based Wi-Fi (WPA2-Enterprise with EAP-TLS), web SSO authentication, web two-factor authentication and more.

Cloudpath can automatically distribute user and device certificates to both IT-managed and unmanaged (BYOD) Chromebooks.

- For IT-managed Chromebooks, Cloudpath deploys both user and device certificates via a Chrome extension provisioned through the Chromebook management console. Whether tied to the user or the device, the certificates are TPM-backed, which means they are burned into hardware for maximum protection.
- For unmanaged Chromebooks, Cloudpath provides a web portal for self-service and automated installation of the certificate along with configuration of related services, such as WPA2- Enterprise Wi-Fi using EAP-TLS.

Whether your network supports IT-managed, or unmanaged Chromebook devices (or both), Cloudpath provides a secure method for Automatic Device Enablement.

Supported Devices

Cloudpath supports all Chrome OS devices supported by Google. To see a list of devices currently supported by Google, consult the following URL:

<https://www.chromium.org/chromium-os/developer-information-for-chrome-os-devices>

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. The sequence of steps for the enrollment differ, depending on the selection that is made.

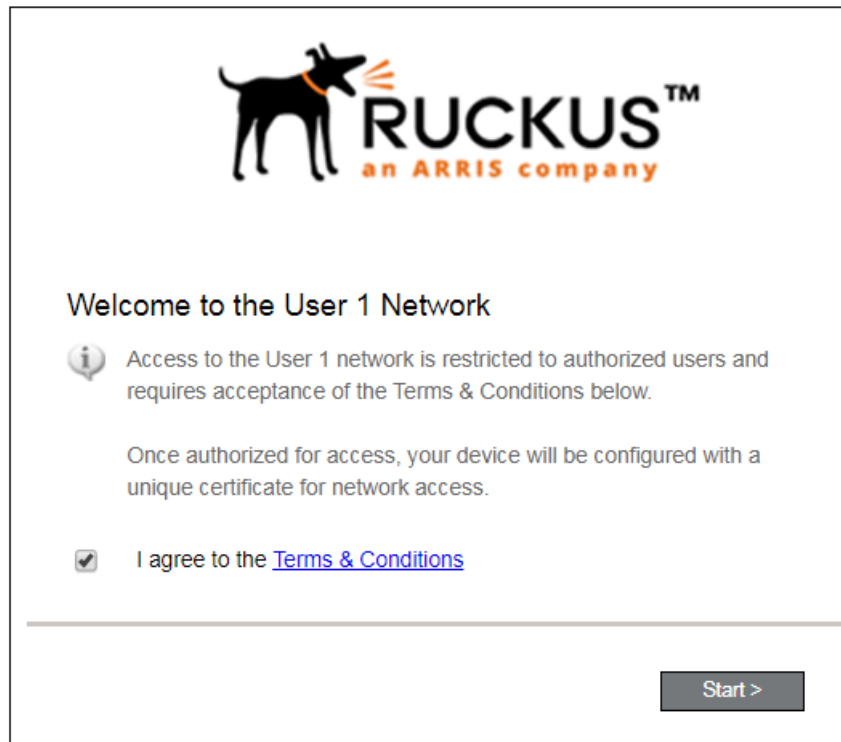
Enrollment Workflow

During enrollment, the Chrome OS is detected and Cloudpath provides Chrome OS-specific instructions for downloading the configuration file and installing it on the device manually, or automatically if extensions are configured. After the configuration file is installed, the user simply connects the secure network.

The following section provides an example of the Chromebook user experience.

1. The user connects to the deployment URL (either directly, or through a Captive Portal).
2. The Cloudpath Welcome screen displays.

FIGURE 1 Wizard Welcome Page



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.

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

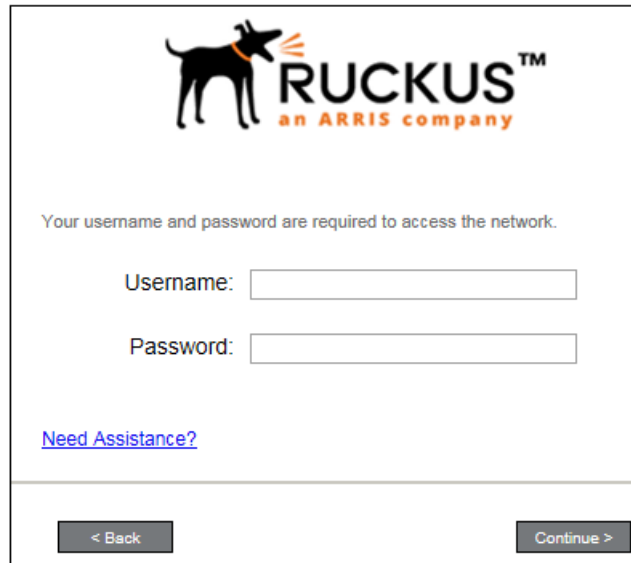


Select the user type to continue. This example follows the *Employee* workflow branch.

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 >

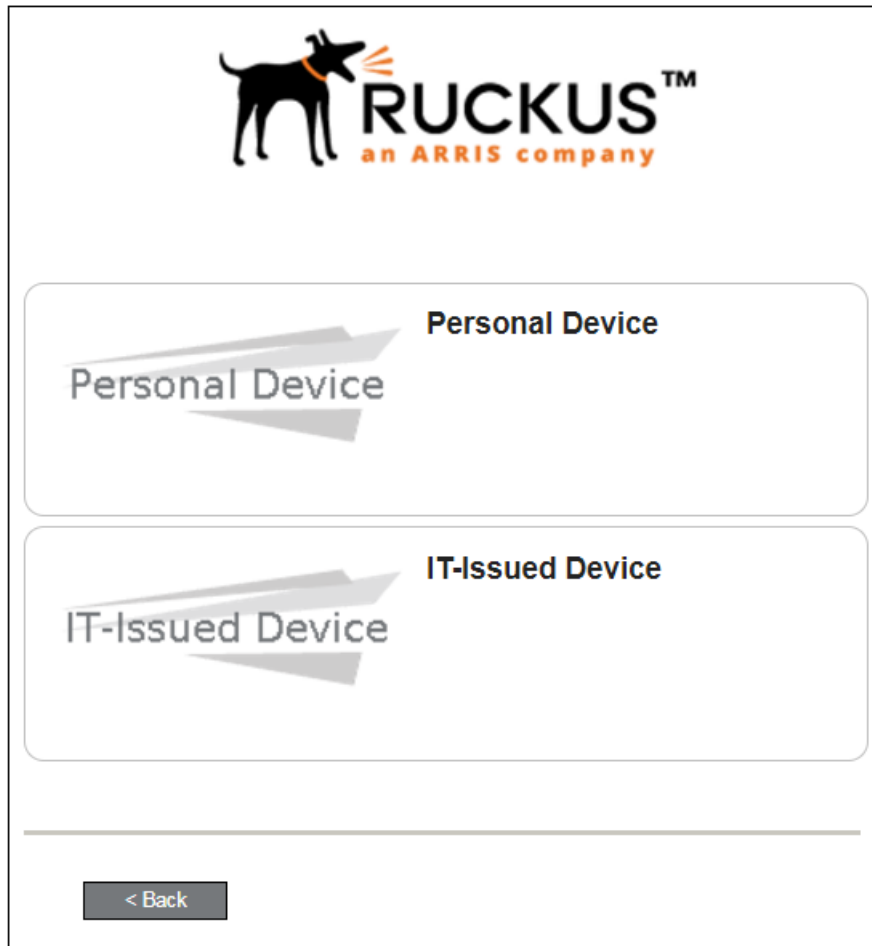
Enter the user credentials and click **Continue**.

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.

Managed or Unmanaged Chromebooks

The final portion of the user experience differs, depending on if the certificate and Wi-Fi settings are set for delivery using the ONC file (unmanaged devices) or an extension (managed devices). See the following sections to continue with the user experience example for your configuration.

- Unmanaged Chromebook User Experience
- Managed Chromebooks With Extension User Experience

Unmanaged Chromebook User Experience

With an unmanaged Chromebook device, the user downloads and installs the ONC file, which contains configuration information required to access the secure network, including the certificate and Wi-Fi settings.

For unmanaged devices, the application detects the Chrome operating system and displays instructions for installing the Chrome configuration on the device.

FIGURE 5 Configuration Installation Instructions

The screenshot displays a Chrome OS interface with a dark header labeled "Chrome OS". Below the header, a list of instructions is provided: "If you are not logged in as the Chromebook owner, log out and log back in as the owner." This is followed by two main steps, each in a grey box with an icon: "Step 1: Download the Network File" (download icon) with the instruction "Simply download the file. Do not open it yet." and "Step 2: Import Network File" (gear icon) with the instruction "Import the Downloaded ONC File." Below Step 2, another list of instructions is shown: "Open a new tab in the browser." and "Type (or copy & paste) this address into the browser: chrome://net-internals/#chromeos". A screenshot of a browser window is included, showing the address bar with "chrome://net-internals/#chrome-os" and a red arrow pointing to the address. The page content shows an "Import ONC file" section with a "Choose File" button and "No file chosen" text, with a hand cursor pointing to the button. A final list of instructions follows: "Under Import ONC File, click Choose File", "Select the downloaded eng-Anna43.onc file and click Open.", "If an error is not reported, your device is now configured for the network.", and "To connect, select 'eng-Anna43' from the list of wireless networks."

Chrome OS

- If you are not logged in as the Chromebook owner, log out and log back in as the owner.

Step 1: Download the Network File
Simply download the file. Do not open it yet.

Step 2: Import Network File
Import the Downloaded ONC File.

- Open a new tab in the browser.
- Type (or copy & paste) this address into the browser:
chrome://net-internals/#chromeos

Import ONC file

Choose File No file chosen

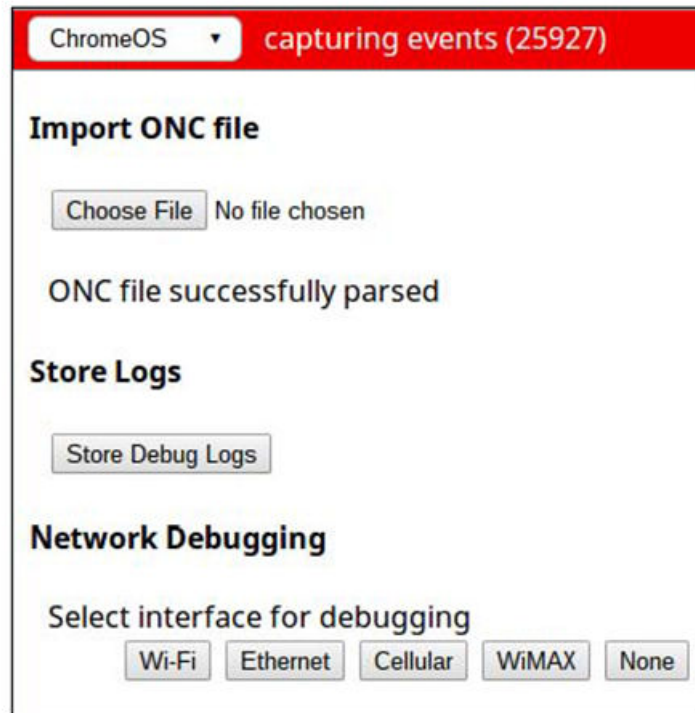
- Under **Import ONC File**, click **Choose File**
- Select the downloaded **eng-Anna43.onc** file and click **Open**.
- If an error is not reported, your device is now configured for the network.
- To connect, select 'eng-Anna43' from the list of **wireless networks**.

The manual download page shows the Chromebook instructions.

Step 1 provides the link to download the ONC file.

Step 2 provides instructions for importing the ONC file.

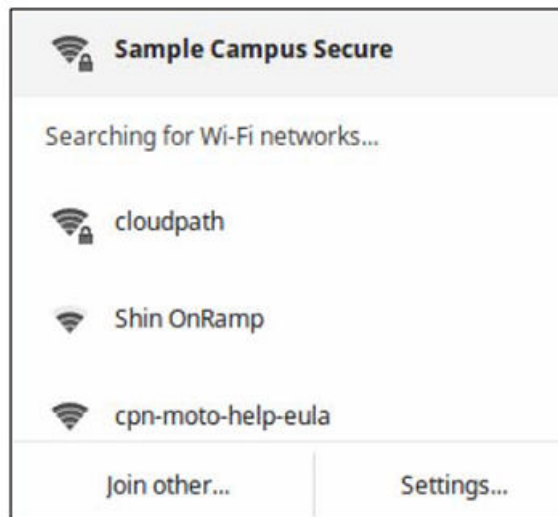
FIGURE 6 Import ONC File



- Copy the URL from the instructions.
- Paste the URL into a new browser window. The Chrome OS Import ONC File page displays.
- Click **Choose File** and browse to select the <NetworkName>.onc file.

After the ONC file installed, click the **Wi-Fi** icon in the bottom right corner of your screen and select the secure network.

FIGURE 7 Select Wi-Fi Network



Typically, user credentials are populated using the information passed during the enrollment process. Click **Connect**.

FIGURE 8 Enter User Credentials

The screenshot shows a 'Join Wi-Fi network' dialog box with the following fields and values:

- SSID: Sample Campus Secure
- EAP method: PEAP
- Phase 2 authentication: MSCHAPv2
- Server CA certificate: Cloudpath IT Root CA 1 [Cloudpath IT Root C
- Subject Match: (empty)
- User certificate: None installed
- Identity: (empty)
- Password: (empty)
- Anonymous identity: (empty)

At the bottom, there is a checked checkbox for 'Save identity and password' and two buttons: 'Connect' and 'Cancel'.

The user should now be connected to the secure network.

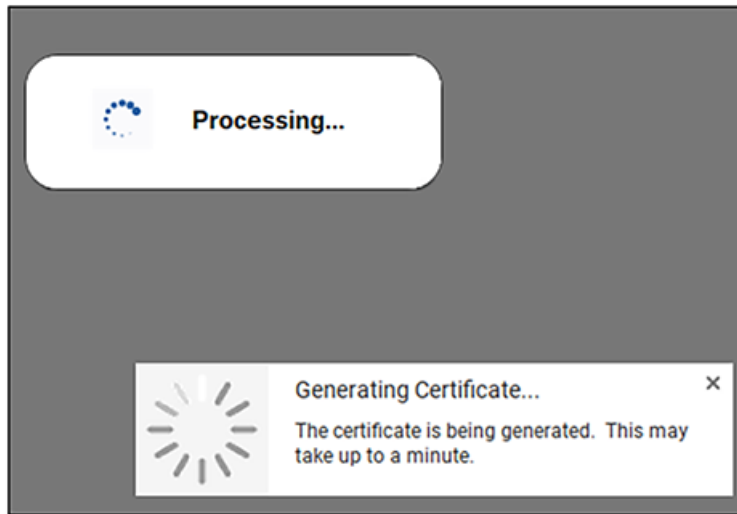
Managed Chromebooks With Extension User Experience

If managed Chromebooks are configured, the download page does not display.

When Cloudpath detects the Chrome OS during enrollment, the extension automatically generates and installs the CA certificate into the TPM.

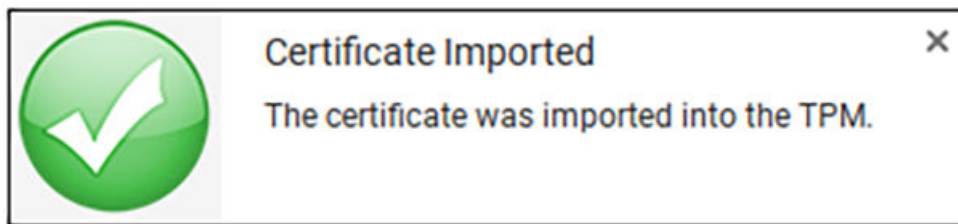
The extension generates the certificate.

FIGURE 9 Generating Certificate



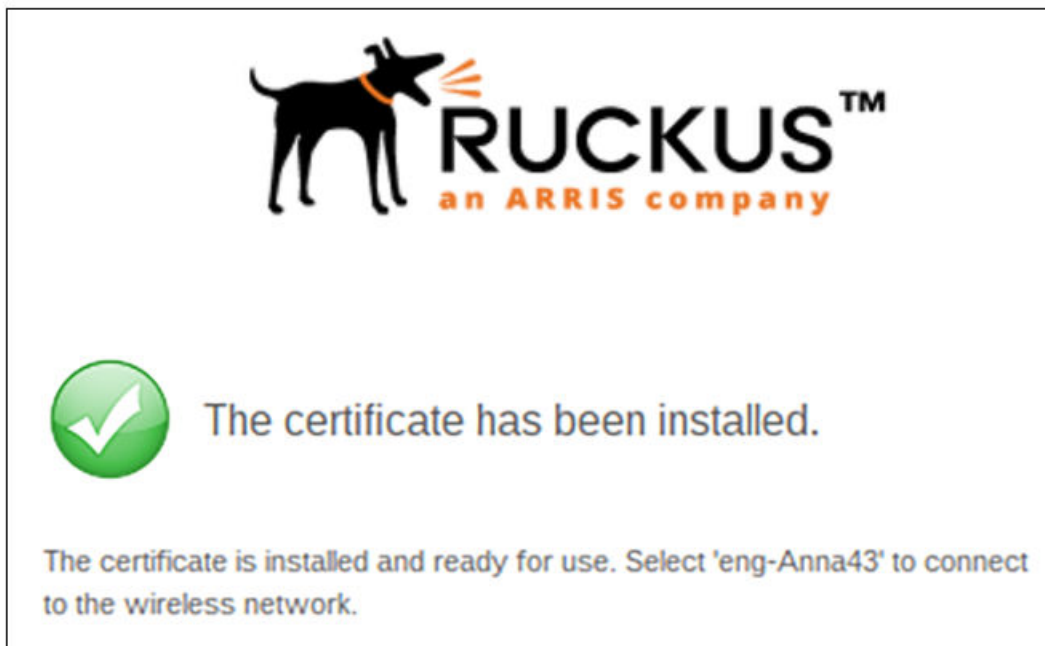
The extension imports the certificate into the TPM.

FIGURE 10 Certificate Imported



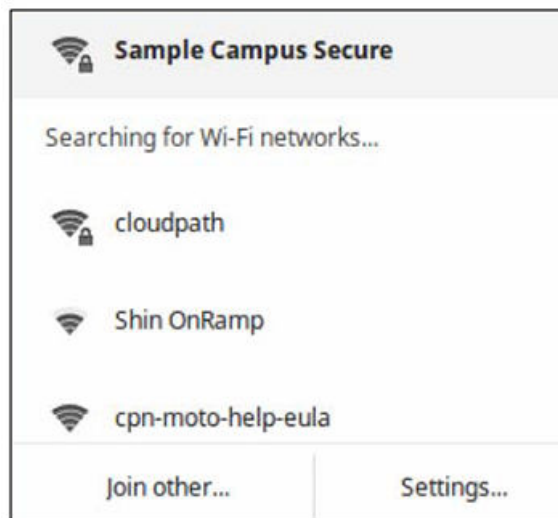
When the certificate installation is complete, a message displays indicating that the certificate is installed and ready for use.

FIGURE 11 Certificate Installed



If not automatically migrated, click the **Wi-Fi** icon in the bottom right corner of your screen and select the secure network.

FIGURE 12 Select Wi-Fi Network



The user should now be connected to the secure network.



© 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