

Cloudpath Enrollment System for Windows Phones 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
Cloudpath User Experience	4
User Prompts.....	4
Common Windows Phone Issues	25
Delete Network.....	26
Device Can't Connect.....	26

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 Windows Phone to the secure network.

Supported Versions

Cloudpath supports Windows Phone version 8.1 TLS and PEAP configurations.

Cloudpath supports Windows Phone version 8.0 for PEAP configurations.

NOTE

Windows Phone 8.0 does not support TLS.

This document provides an example of the prompts a user might see when using the Cloudpath application. Depending on the configuration set up by the network administrator, the device manufacturer, and operating system, the user prompts can vary.

Additionally, Cloudpath is a highly customizable application. Screen icons, color schemes, and messaging can all be customized by the network administrator. This guide provides examples with generic screens and messaging, which might be different than what is displayed on the device.

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.

User Prompts

This section displays the user prompts for a typical enrollment workflow.

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

Welcome Screen With AUP

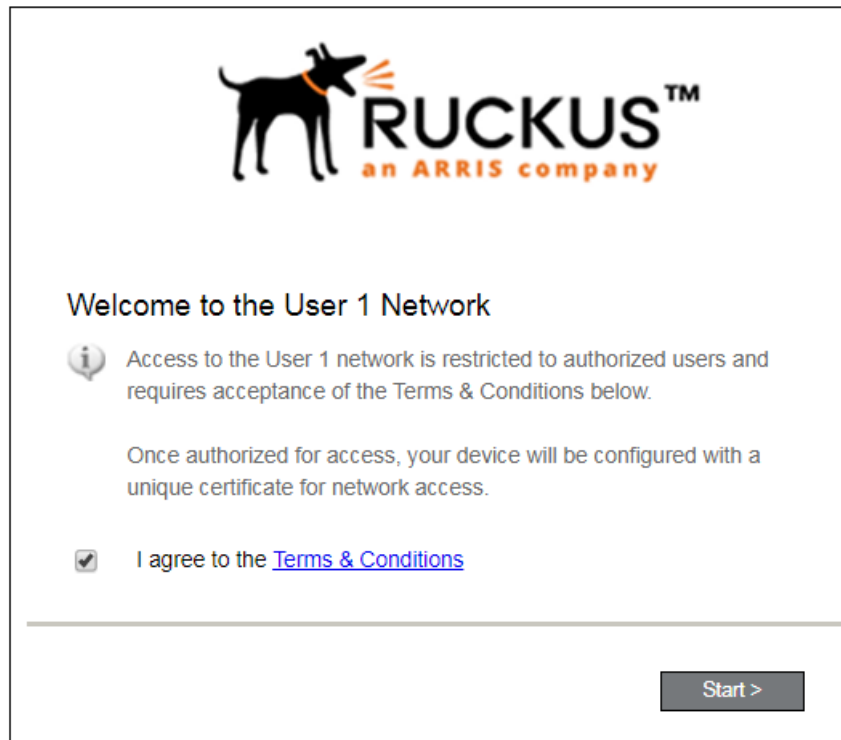
When the user enters the enrollment URL on their device, the Login (or Welcome) screen displays.

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

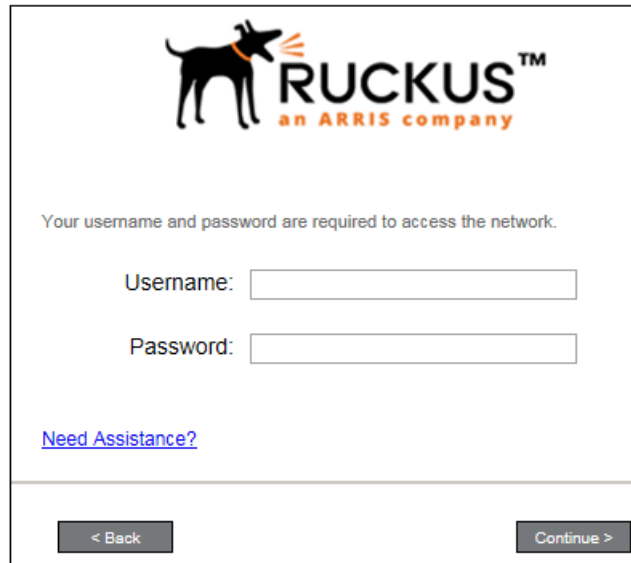


Select the user type to continue. This example follows the *Employee* workflow branch.

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 >

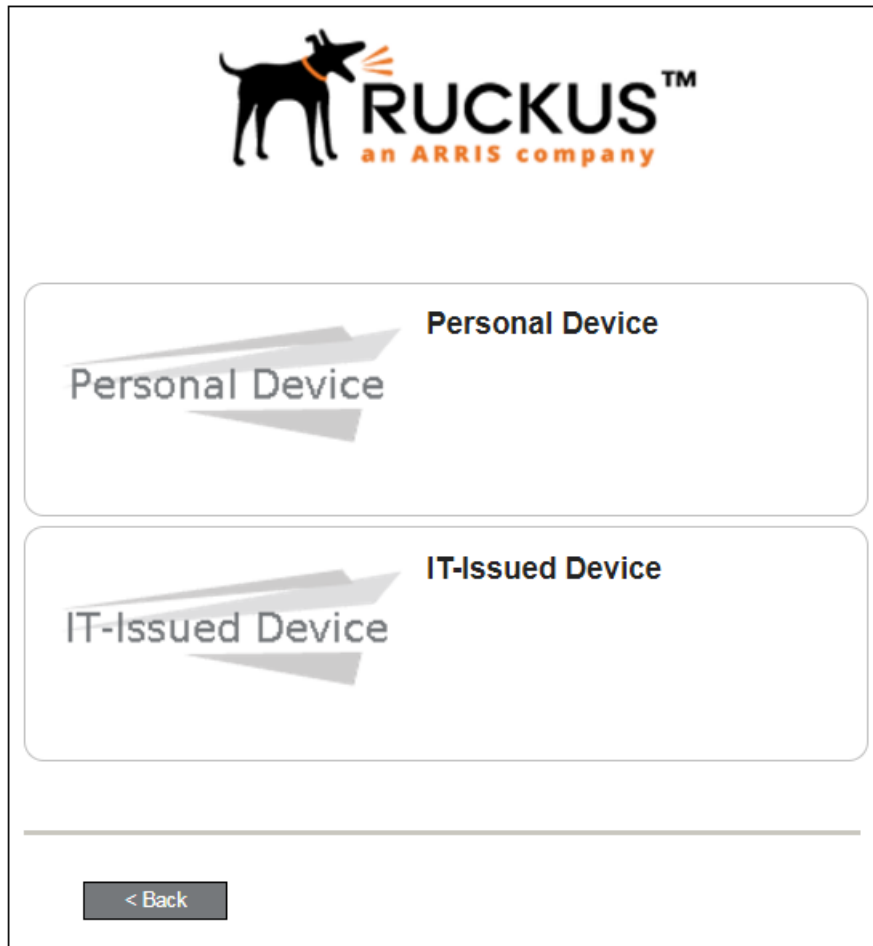
Enter the user credentials and click **Continue**.

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



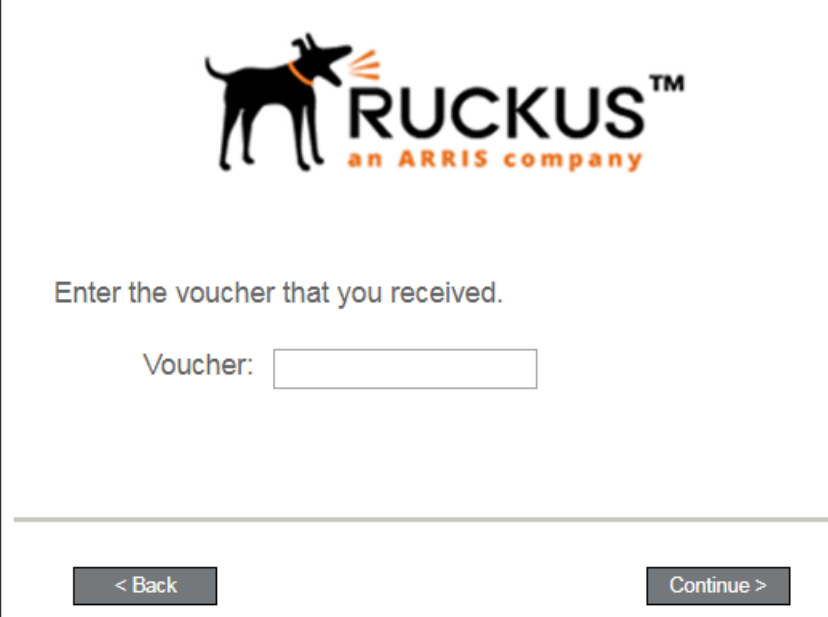
Select a device type to continue. This example follows the IT-Issued Device enrollment workflow.

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



Enter the voucher that you received.

Voucher:

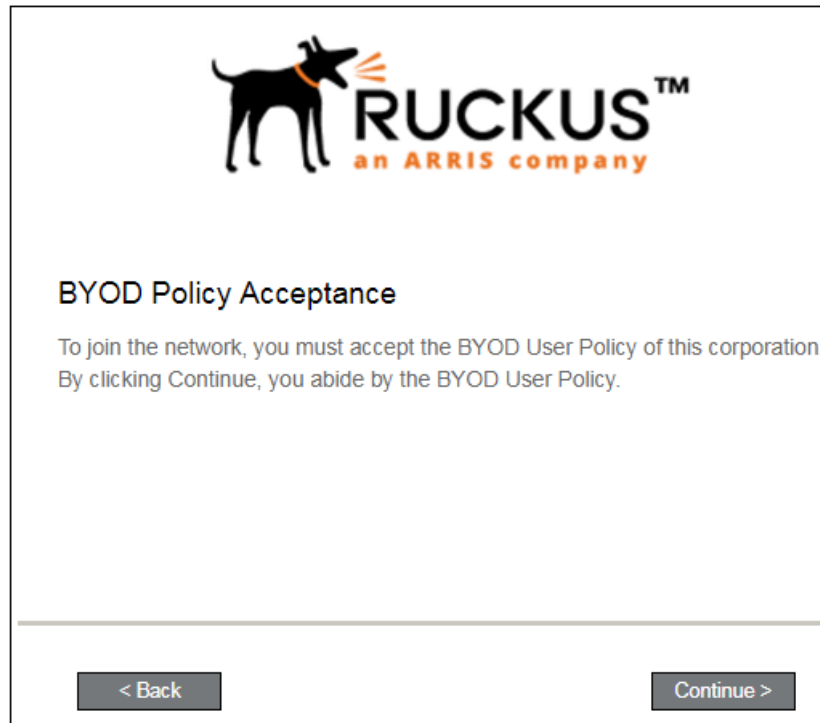
< Back Continue >

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.


Windows Phone Configuration Instructions

The application detects the user agent for a Windows Phone and provides the correct configuration instructions.


Windows Phone instructions are displayed on the Other Operating Systems tab.

FIGURE 7 Configuration for Windows Phones

Other Operating Systems


**Step 1: Install The CA Certificate**
Click to Install Anna Test Root CA I

Click the button above to download the certificate file in the most common format. If needed, other formats are available: [PEM](#) [DER](#) [CER](#)

**Step 2: Install Your Certificate**
Click to Install Your Certificate

Click the button above to download your certificate It will need imported into your device.

**** When prompted for a password while installing the certificate, enter the password you entered on the previous screen.**

**Step 3: Configure Wi-Fi**
Use The Information Below To Setup Wi-Fi

Wireless Name (SSID): R-DVES-Secure
Security Type: WPA2-Enterprise
Encryption Type: AES (CCMP)
EAP Method: EAP-TLS (or TLS)
Root CA Certificate(s): Anna Test Root CA I
Server Name: anna44.cloudpath.net
Client Certificate: <Download Above>
Username: <Download Above>

* Labels on fields will differ based on the operating system.

NOTE

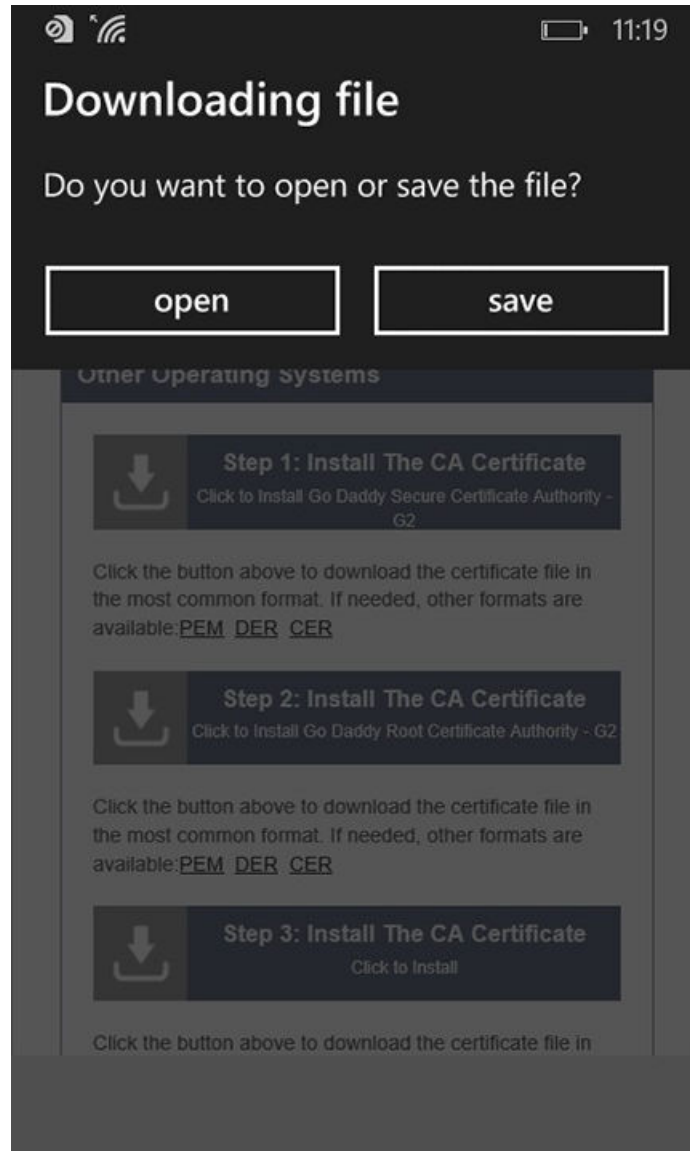
The certificate information is not populated on the configuration step until the certificates have been downloaded.

This screen includes the steps to install the certificates and to configure the device.

Download CA Certificates

The first step in the instructions prompts you to download the CA certificate.

FIGURE 8 Download File



Tap **Save** to continue.

Start CA Certificate Installation

Tap the certificate installation screen to start the CA certificate installation.

FIGURE 9 Tap Screen to Open

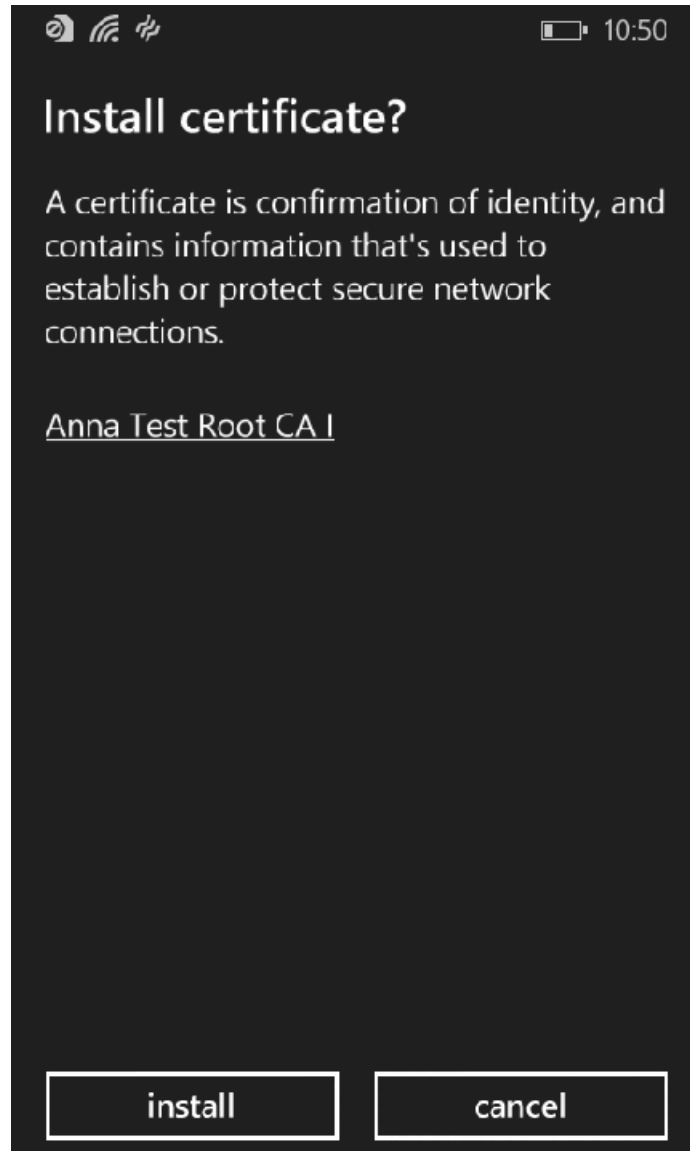


Continue with the certificate installation.

Install CA Certificate

After the CA certificate is downloaded, you are prompted to install the certificate on the device.

FIGURE 10 Install CA Certificate

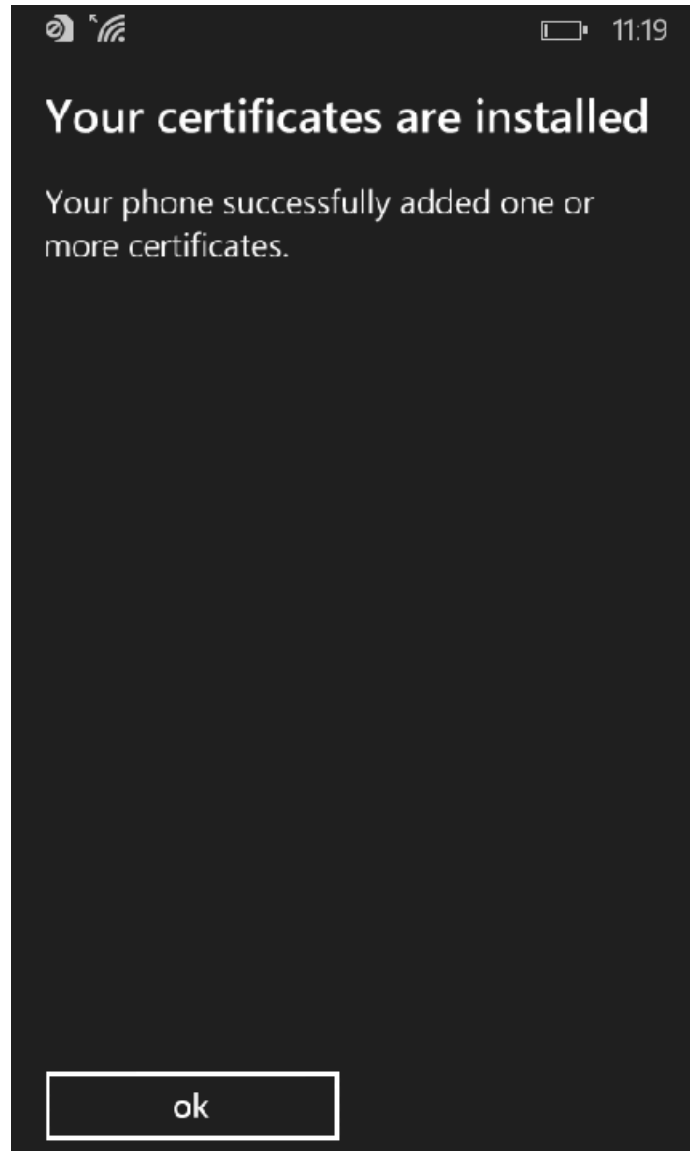


Tap **Install** to continue.

CA Certificates installed

The CA certificate has been downloaded and installed when you receive the confirmation screen.

FIGURE 11 Certificates are Installed



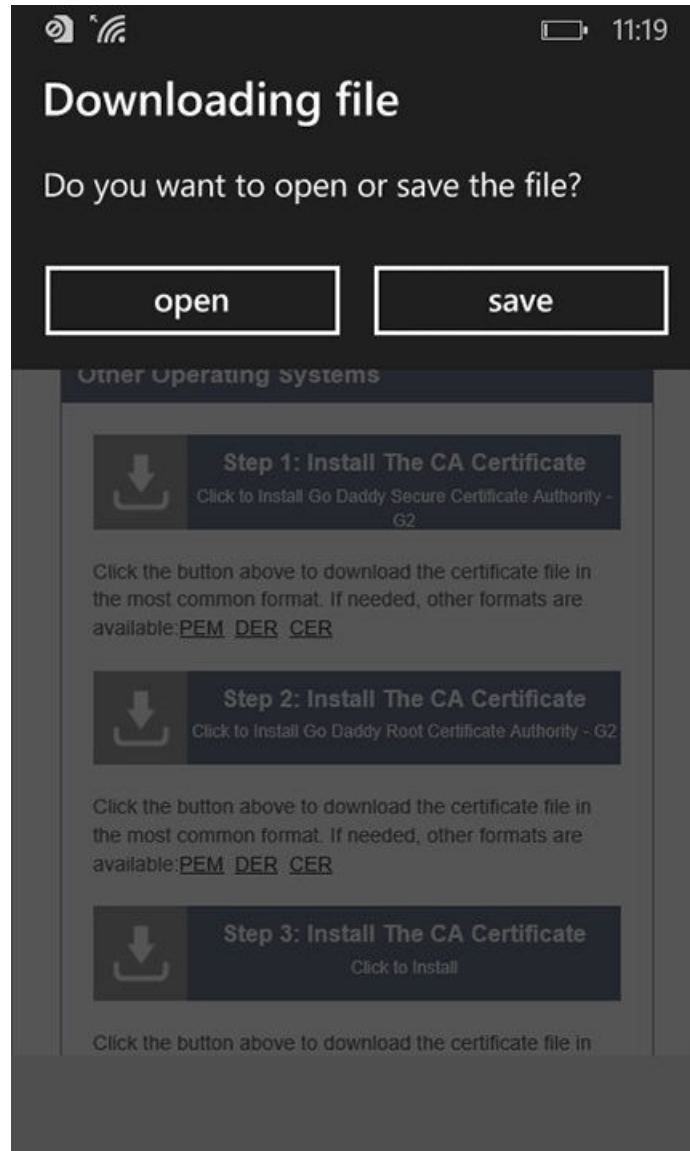
Tap the **ok** button.

Tap the **Back** button (left arrow at the bottom on your phone) to return to the configuration instructions page. If there are more CA certificates, you will repeat the CA certificate installation. Otherwise, continue with the user certificate installation.

Download Your Certificates

After the CA certificates are installed, you are prompted to download the user certificates.

FIGURE 12 Download File

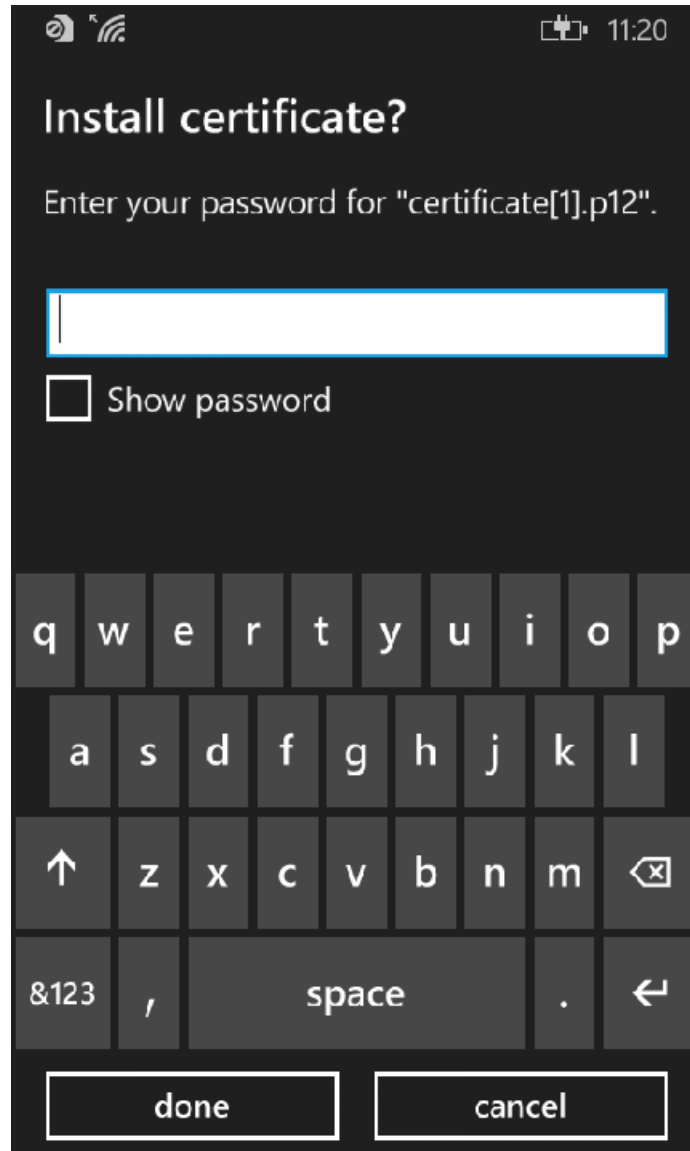


Tap **Save** to continue.

Enter User Certificate Password

The Windows Phone OS requires that you enter a password to import user certificates.

FIGURE 13 Enter User Certificate Password



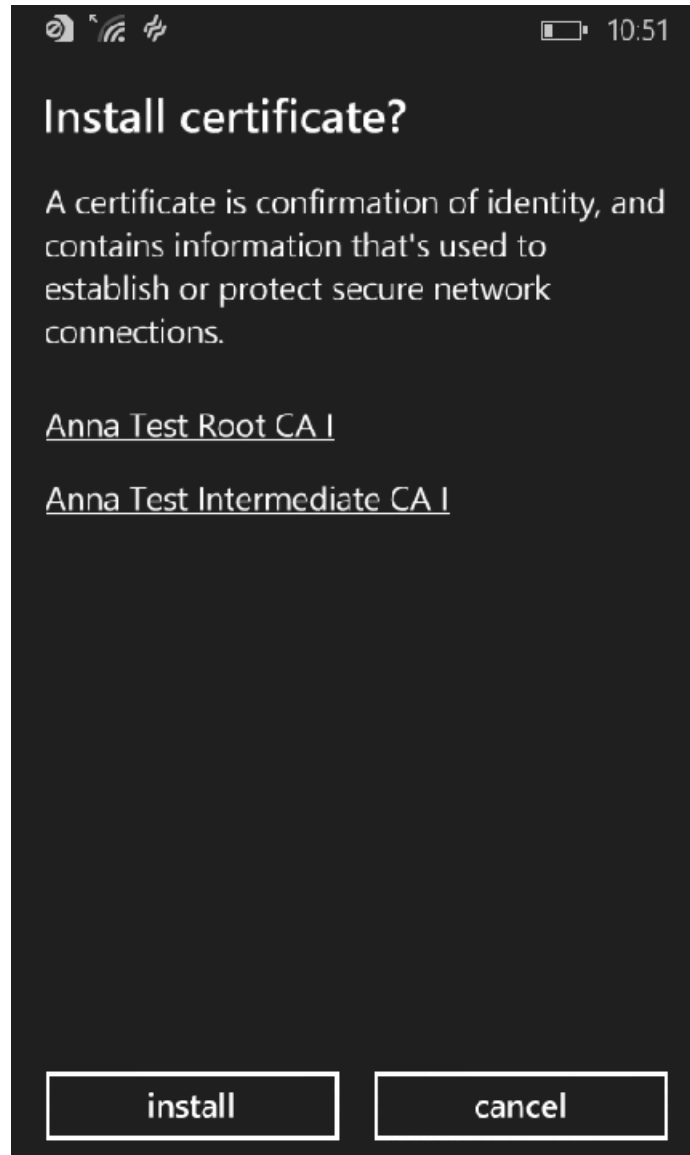
Enter the password from your user credentials. For example, if your user credentials are username=bob and password=bob1, then enter bob1 for the user certificate password.

Tap **done** to continue.

Install User Certificates

Install the user certificates provided for this device.

FIGURE 14 Install User Certificates

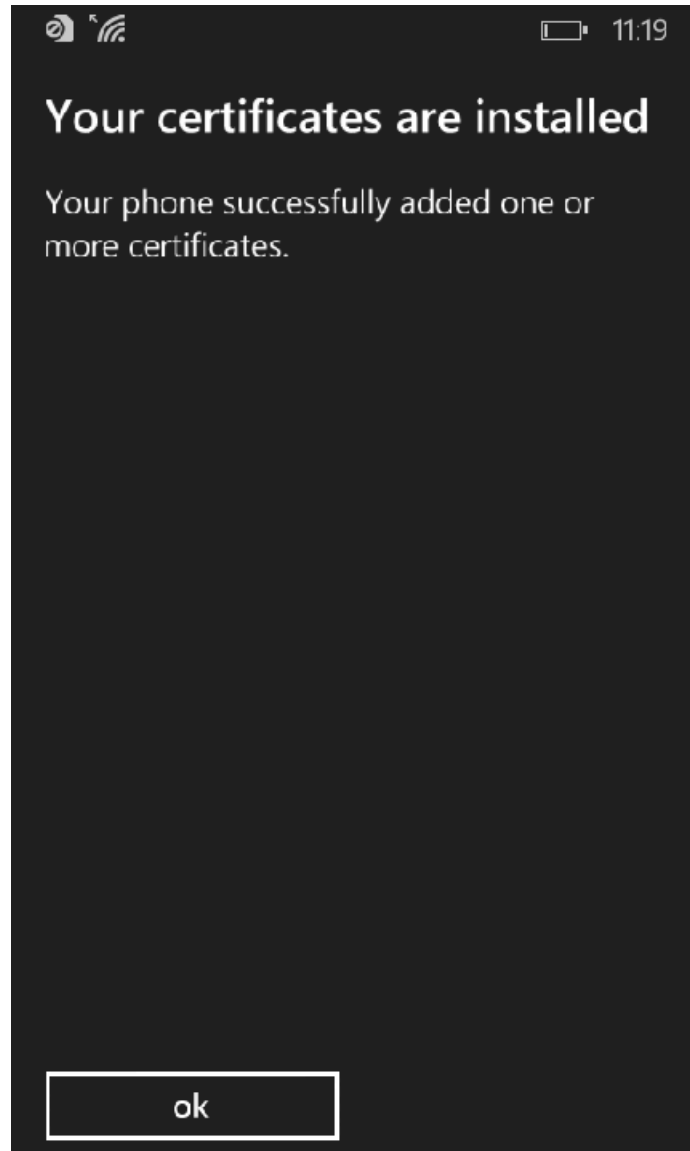


Tap **Install** to continue.

Certificates installed

The user certificate has been downloaded and installed when you receive the confirmation screen.

FIGURE 15 Certificates are Installed



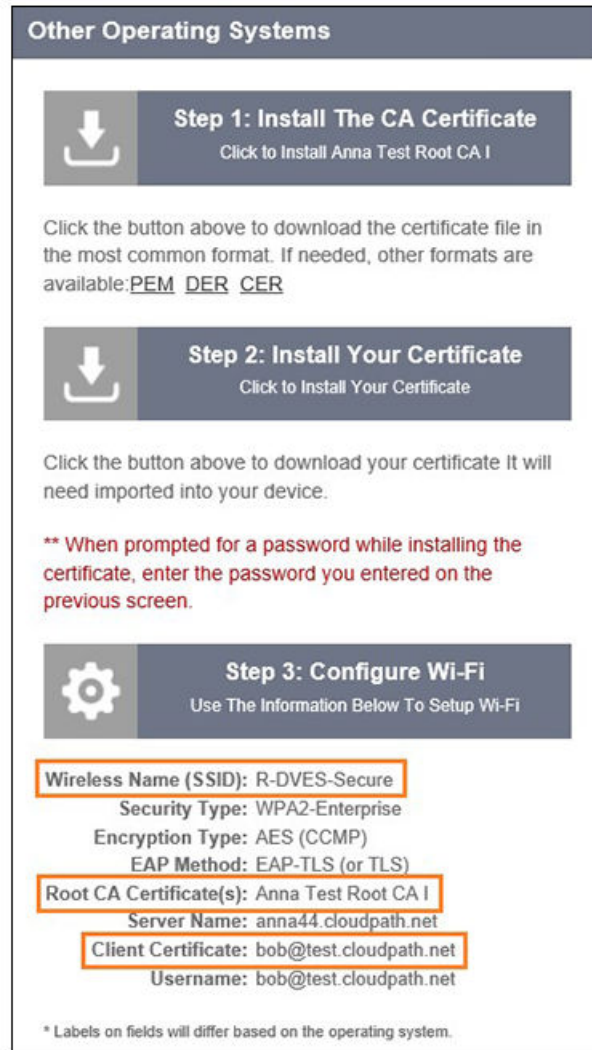
Tap the **ok** button.

Tap the **Back** button (left arrow at the bottom on your phone) to return to the configuration instructions page. Continue with the Wi-Fi Configuration.

Wi-Fi Configuration

After you download and install the certificates, make note of the Wireless Network Name, Root CA Certificate, and the Client Certificate. You need this information to connect to the secure network.

FIGURE 16 Wi-Fi Configuration



Other Operating Systems

Step 1: Install The CA Certificate
Click to Install Anna Test Root CA I

Click the button above to download the certificate file in the most common format. If needed, other formats are available: [PEM](#) [DER](#) [CER](#)

Step 2: Install Your Certificate
Click to Install Your Certificate

Click the button above to download your certificate It will need imported into your device.

**** When prompted for a password while installing the certificate, enter the password you entered on the previous screen.**

Step 3: Configure Wi-Fi
Use The Information Below To Setup Wi-Fi

Wireless Name (SSID): R-DVES-Secure
Security Type: WPA2-Enterprise
Encryption Type: AES (CCMP)
EAP Method: EAP-TLS (or TLS)

Root CA Certificate(s): Anna Test Root CA I
Server Name: anna44.cloudpath.net

Client Certificate: bob@test.cloudpath.net
Username: bob@test.cloudpath.net

* Labels on fields will differ based on the operating system.

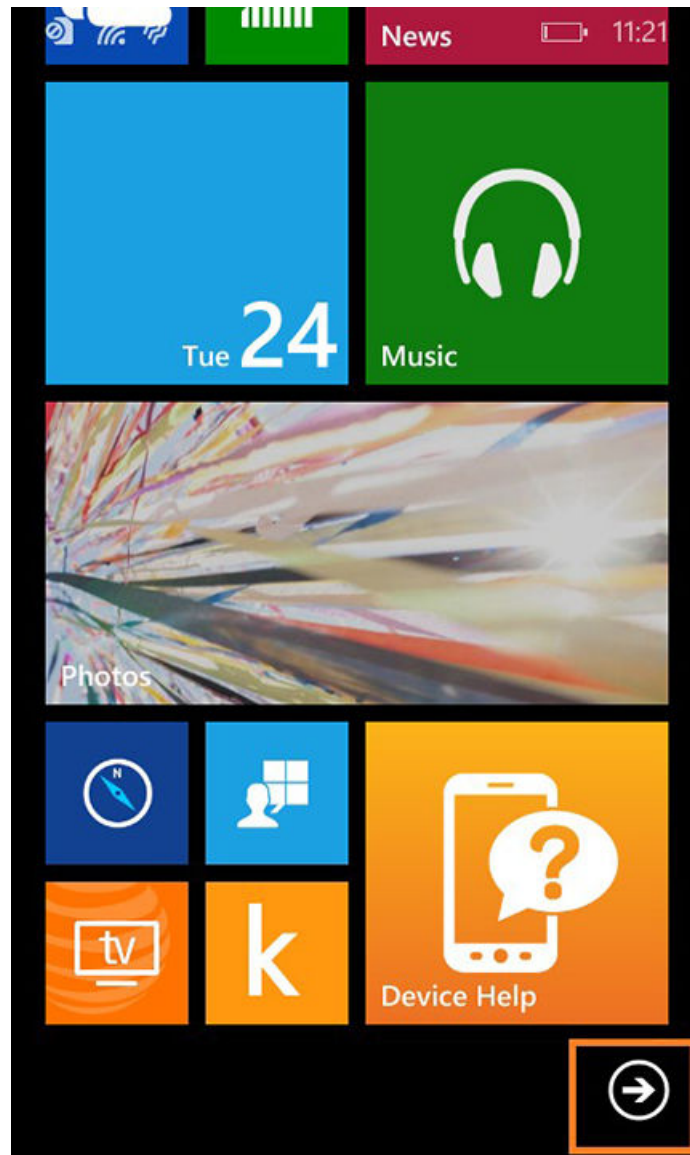
Continue to the next screen to configure Wi-Fi settings on the Windows Phone.

Access Device Menu

After the Root CA certificate and user certificate have been installed on the device, you return to the home screen.

Swipe to the bottom of the home screen and tap the right-facing arrow.

FIGURE 17 Install From Amazon Market

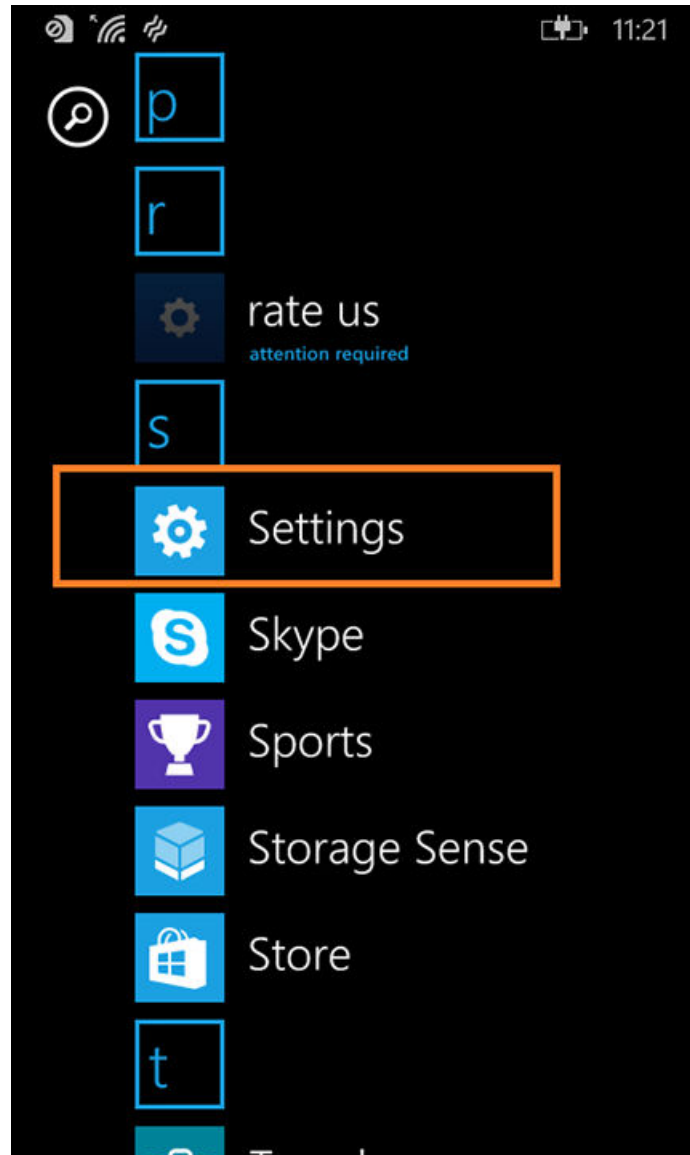


Continue to the next screen to locate the *Settings* on the Windows Phone.

Access Device Settings

Go to the device *Settings*.

FIGURE 18 Device Settings

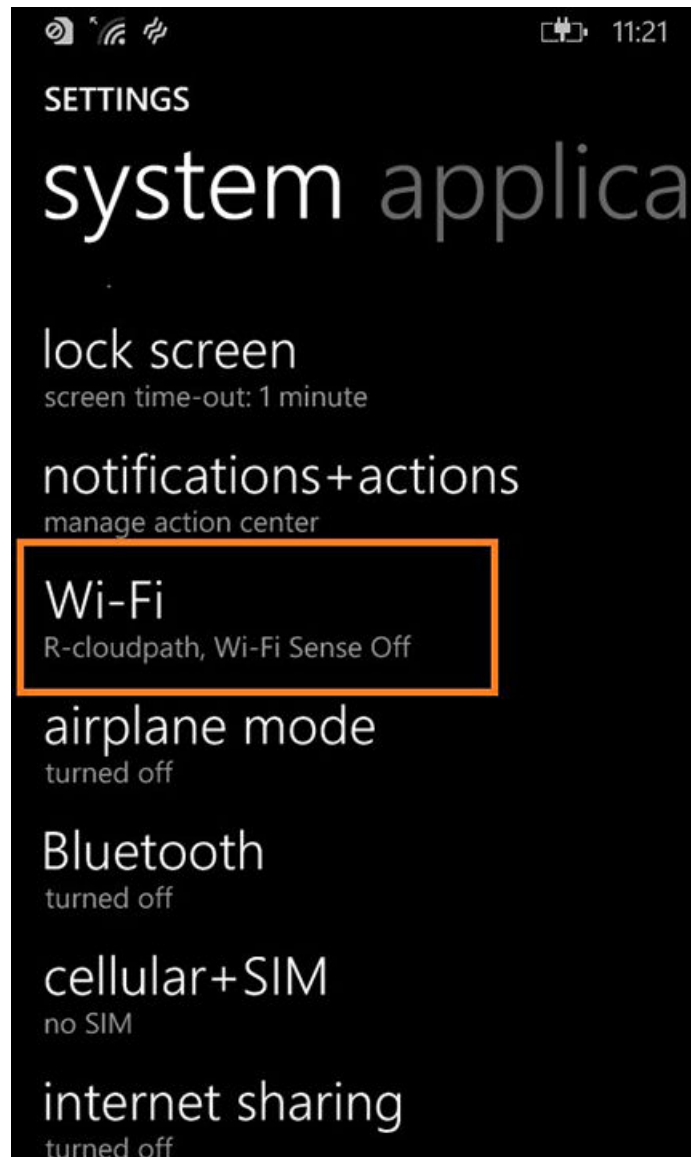


Tap **Settings** to continue.

Locate Wi-Fi Settings

Go to the *Wi-Fi* setting.

FIGURE 19 Wi-Fi Settings



Tap **Wi-Fi** to continue.

Configure Wi-Fi Settings

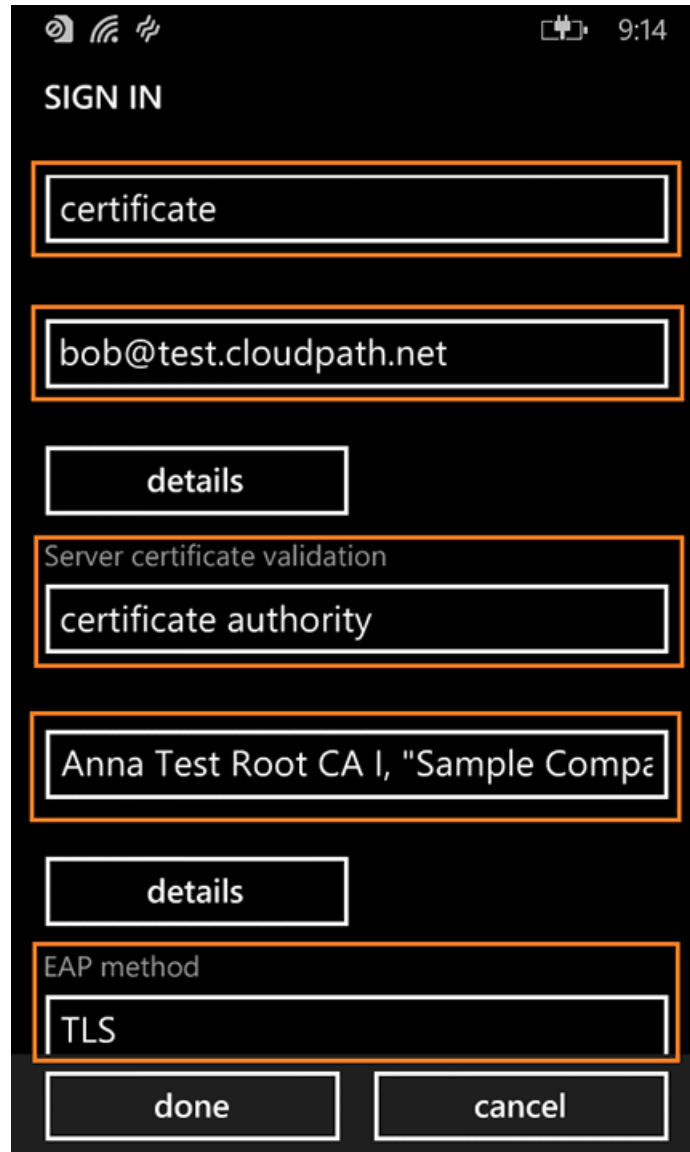
Tap the Wireless Network listed in the configuration instructions.

Configure Wi-Fi for the secure network. Be sure to select the certificate configuration settings to match the configuration instructions:

- Connect using certificate.
- Choose a certificate and select the Client Certificate from the configuration instructions.
- For Server certificate validation, select certificate authority.
- Choose a certificate and select the Root CA Certificate from the configuration instructions.

- For EAP method, select TLS.

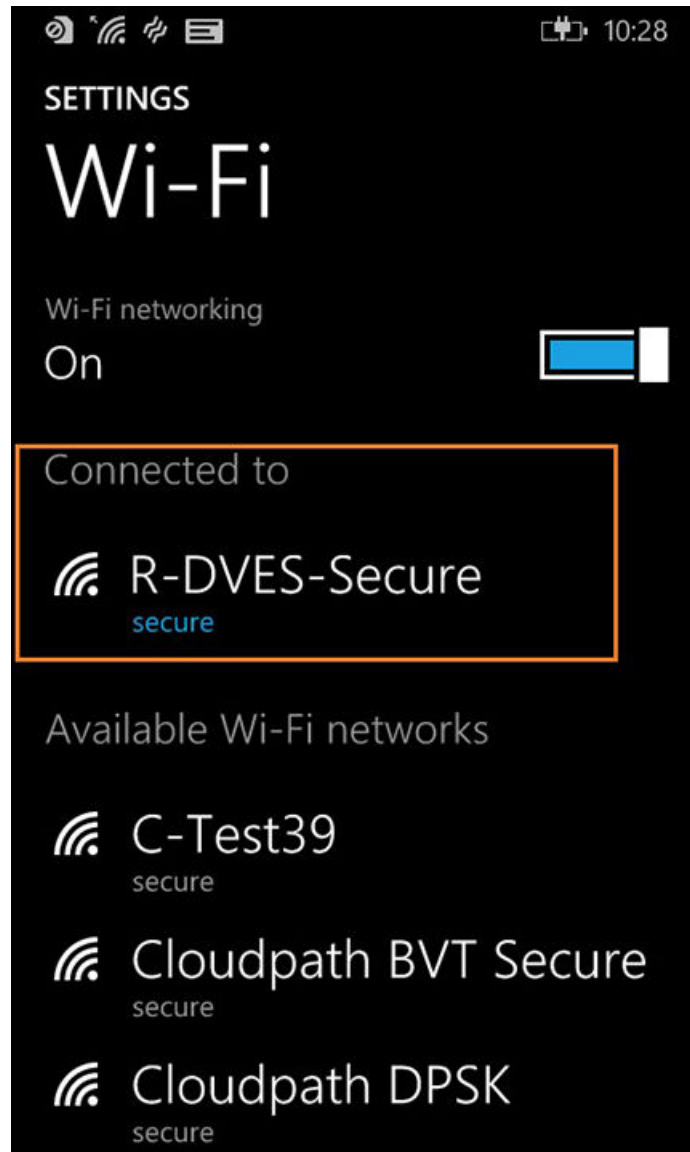
FIGURE 20 Configure Wi-Fi Settings



Tap done to continue.

Connected to Secure Network

FIGURE 21 Secure



You should be connected to the secure network.

Common Windows Phone Issues

If you encounter certain issues with enrollments on your Windows Phone, you may need to contact the network help desk.

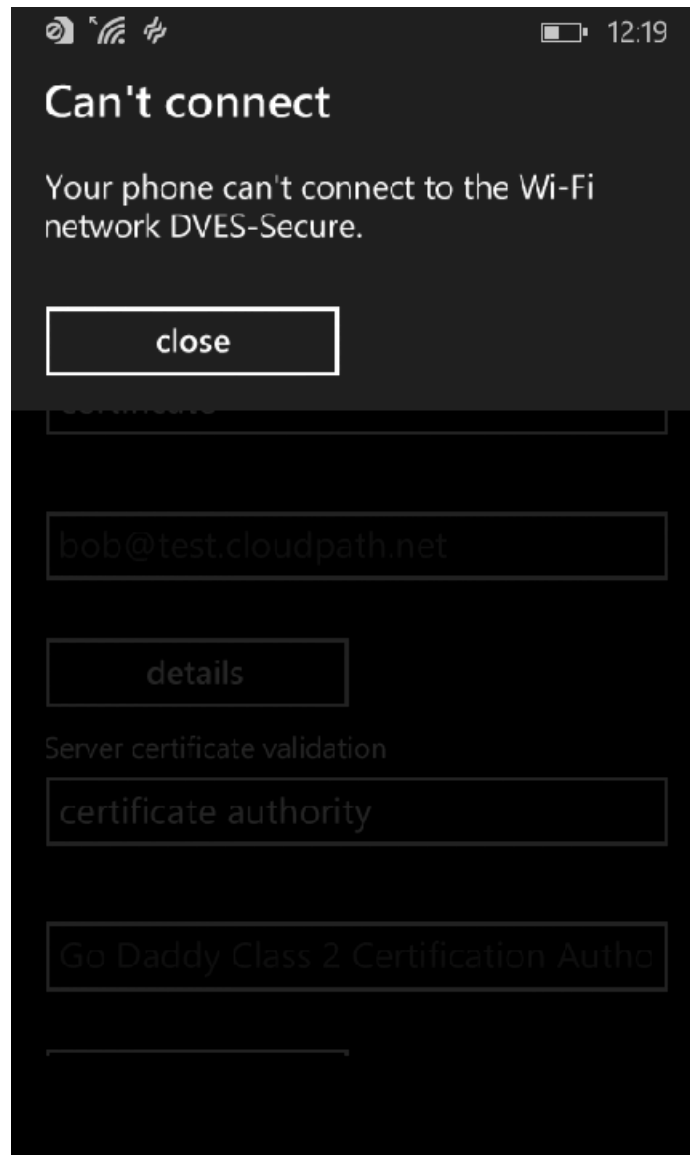
Delete Network

Sometimes, the SSID retains old settings. You might try deleting the network and reconfiguring it. To delete the network, tap and hold the network name, then tap **delete**.

Device Can't Connect

If you receive a message that the phone cannot connect the secure network, this typically means that there is a problem with your configuration.

FIGURE 22 Device Can't Connect

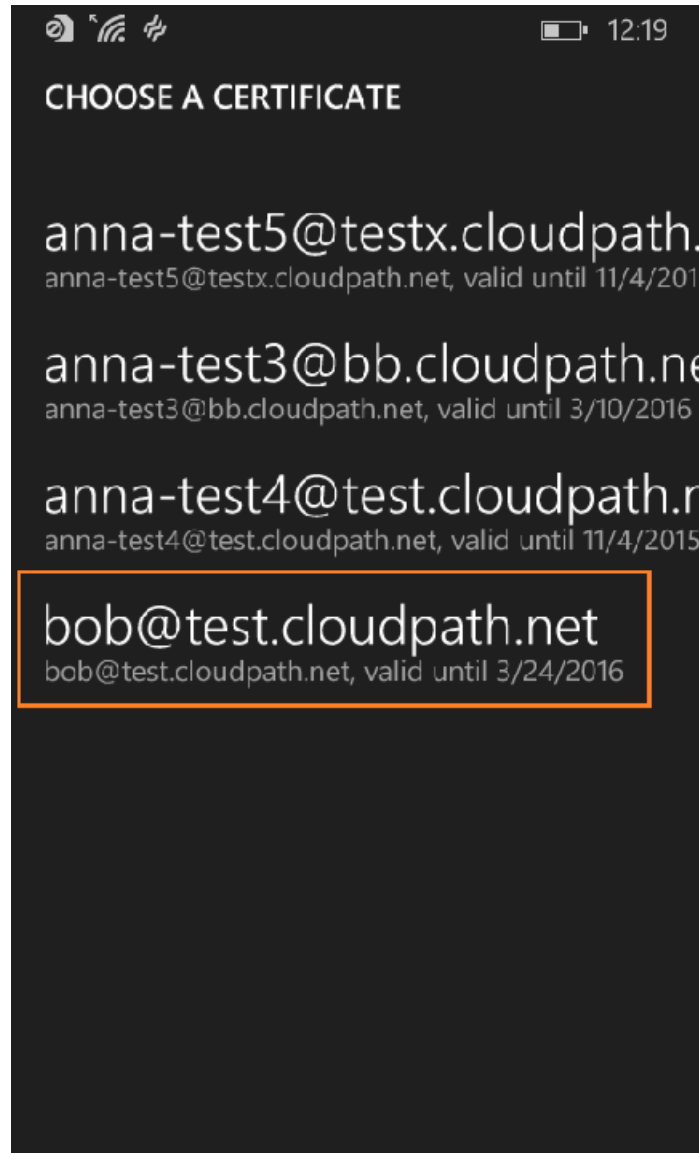


Be sure that your selections on the Wi-Fi configuration page match the settings provided on the Other Operating Systems tab. Refer to [Windows Phone Configuration Instructions](#) on page 10 for more information.

Use these settings:

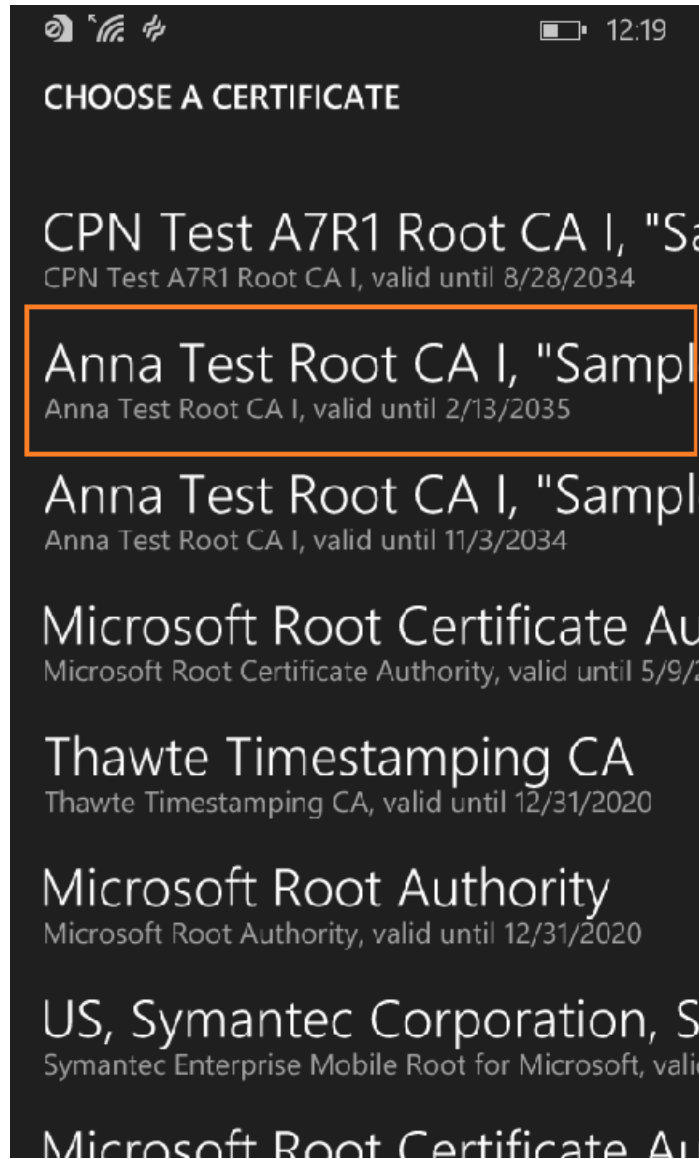
- Connect using **certificate**.
- Choose a certificate to match the **Client Certificate** in the configuration instructions.

FIGURE 23 Choose A User Certificate



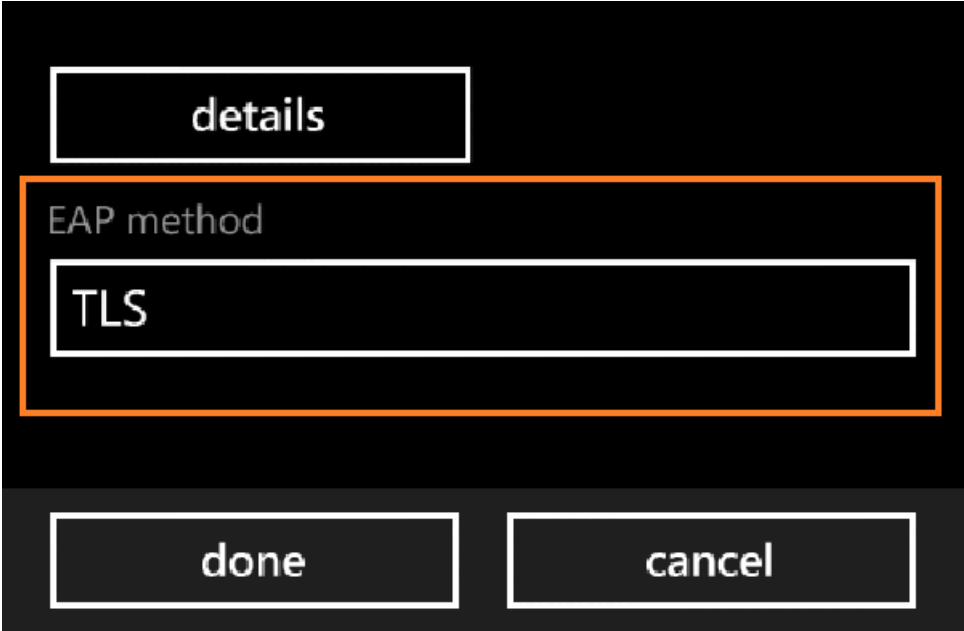
- Server Certificate Validation must be **certificate authority**.
- Choose the **Root CA Certificate** to match the configuration instructions.

FIGURE 24 Choose A Root CA Certificate



- Select **TLS** for the EAP method.

FIGURE 25 EAP Method





© 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