

Cloudpath Enrollment System End-User Experience Guide For Supported Devices, 5.6

Supporting Cloudpath Software Release 5.6

Copyright, Trademark and Proprietary Rights Information

© 2019 CommScope, Inc. 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 CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope 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, COMMScope 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. CommScope 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. CommScope 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 CommScope 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 COMMScope, COMMScope 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 COMMScope 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, CommScope, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, Edgelron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface.....	7
Document Conventions.....	7
Notes, Cautions, and Warnings.....	7
Command Syntax Conventions.....	8
Document Feedback.....	8
Ruckus Product Documentation Resources.....	8
Online Training Resources.....	9
Contacting Ruckus Customer Services and Support.....	9
What Support Do I Need?.....	9
Open a Case.....	9
Self-Service Resources.....	9
Overview.....	11
End-User Experience for Windows Phones	13
Supported Windows Phones Versions.....	13
User Prompts.....	13
Welcome Screen With AUP.....	13
User Type.....	15
Device Type.....	15
Voucher Code.....	16
BYOD Policy.....	18
Windows Phone Configuration Instructions.....	18
Download CA Certificates.....	20
Start CA Certificate Installation.....	21
Install CA Certificate.....	22
CA Certificates installed.....	23
Download Your Certificates.....	24
Enter User Certificate Password.....	25
Install User Certificates.....	25
Certificates installed.....	27
Wi-Fi Configuration.....	28
Access Device Menu.....	28
Access Device Settings.....	29
Locate Wi-Fi Settings.....	30
Configure Wi-Fi Settings.....	31
Connected to Secure Network.....	33
Common Windows Phone Issues.....	33
Delete Network.....	34
Device Can't Connect.....	34
End-User Experience for Windows Devices.....	39
Supported Windows versions.....	39
User Experience.....	39
Enrollment User Prompts.....	39
Configuration Wizard.....	45
Wizard Application User Experience.....	48
Other Methods for Launching Application.....	51

End-User Experience for iOS Devices.....	55
Supported iOS Versions.....	55
User Prompts.....	55
Welcome Screen With AUP.....	55
User Type.....	57
User Credentials.....	58
Device Type.....	58
Install Profile.....	59
Connect to Secure Network.....	60
End-User Experience for MAC Devices.....	63
Supported MAC OS Versions.....	63
User Experience.....	63
Enrollment User Prompts.....	63
Configuration Wizard.....	69
Wizard Application User Experience.....	72
Install Network Profile to Configure Wi-Fi.....	77
End-User Experience for Linux Devices.....	83
Supported Linux Versions.....	83
Cloudpath User Experience.....	83
Enrollment User Prompts.....	83
Wizard Application User Experience.....	92
Configuring the Device.....	92
Connected to Secure Network.....	93
View Network Connection.....	93
End-User Experience for Blackberry Devices.....	95
Supported BlackBerry Versions.....	95
Cloudpath User Experience.....	95
Enrollment Steps.....	95
BlackBerry Configuration Instructions.....	101
Download Certificates.....	103
Import Certificates.....	108
Configure Wi-Fi Settings.....	120
End-User Experience for Chromebook Devices.....	129
Overview.....	129
Supported Chrome OS Devices.....	129
Cloudpath User Experience.....	129
Enrollment Workflow.....	129
Managed or Unmanaged Chromebooks.....	133
End-User Experience for Android Devices.....	139
Supported Android Versions.....	139
Cloudpath User Experience.....	139
Welcome Screen With AUP.....	139
User Type.....	141
User Credentials.....	142
Device Type.....	142
BYOD Policy.....	144
Android-Specific Configuration Instructions.....	144
Download and Install Application.....	145

Cloudpath Wizard User Experience.....	153
Troubleshooting.....	156
Common Android Issues.....	156
Retrieve Log Files.....	157
Passwords and Lock Screen PINs.....	157
Blank Certificate Field.....	158
Certificate Passwords.....	158
Android .netconfig File.....	158
Memory Card.....	158
Uninstalling the Application.....	158

Preface

- Document Conventions..... 7
- Command Syntax Conventions..... 8
- Document Feedback..... 8
- Ruckus Product Documentation Resources..... 8
- Online Training Resources..... 9
- Contacting Ruckus Customer Services and Support..... 9

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
monospace	Identifies command syntax examples	<code>device(config)# interface ethernet 1/1/6</code>
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the Start menu, click All Programs .
<i>italics</i>	Publication titles	Refer to the <i>Ruckus Small Cell Release Notes</i> for more information.

Notes, Cautions, and Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE

A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION

An ATTENTION statement indicates some information that you must read before continuing with the current action or task.



CAUTION

A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.



DANGER

A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
<i>italic text</i>	Identifies a variable.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ x y z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member[member...]</i> .
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Document Feedback

Ruckus is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to Ruckus at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- Ruckus SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

Ruckus Product Documentation Resources

Visit the Ruckus website to locate related documentation for your product and additional Ruckus resources.

Release Notes and other user documentation are available at <https://support.ruckuswireless.com/documents>. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a Ruckus Support Portal user account. Other technical documentation content is available without logging in to the Ruckus Support Portal.

White papers, data sheets, and other product documentation are available at <https://www.ruckuswireless.com>.

Online Training Resources

To access a variety of online Ruckus training modules, including free introductory courses to wireless networking essentials, site surveys, and Ruckus products, visit the Ruckus Training Portal at <https://training.ruckuswireless.com>.

Contacting Ruckus Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their Ruckus products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the Ruckus Support Portal using <https://support.ruckuswireless.com>, or go to <https://www.ruckuswireless.com> and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at <https://support.ruckuswireless.com/contact-us> and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The Ruckus Support Portal at <https://support.ruckuswireless.com> offers a number of tools to help you to research and resolve problems with your Ruckus products, including:

- Technical Documentation—<https://support.ruckuswireless.com/documents>

Preface

Contacting Ruckus Customer Services and Support

- Community Forums—<https://forums.ruckuswireless.com/ruckuswireless/categories>
- Knowledge Base Articles—<https://support.ruckuswireless.com/answers>
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—<https://support.ruckuswireless.com/security>

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

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 examples 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.

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 some generic screens and messaging, which might be different than what is displayed on the device.

End-User Experience for Windows Phones

- Supported Windows Phones Versions..... 13
- User Prompts..... 13
- Common Windows Phone Issues..... 33

Supported Windows Phones 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.

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

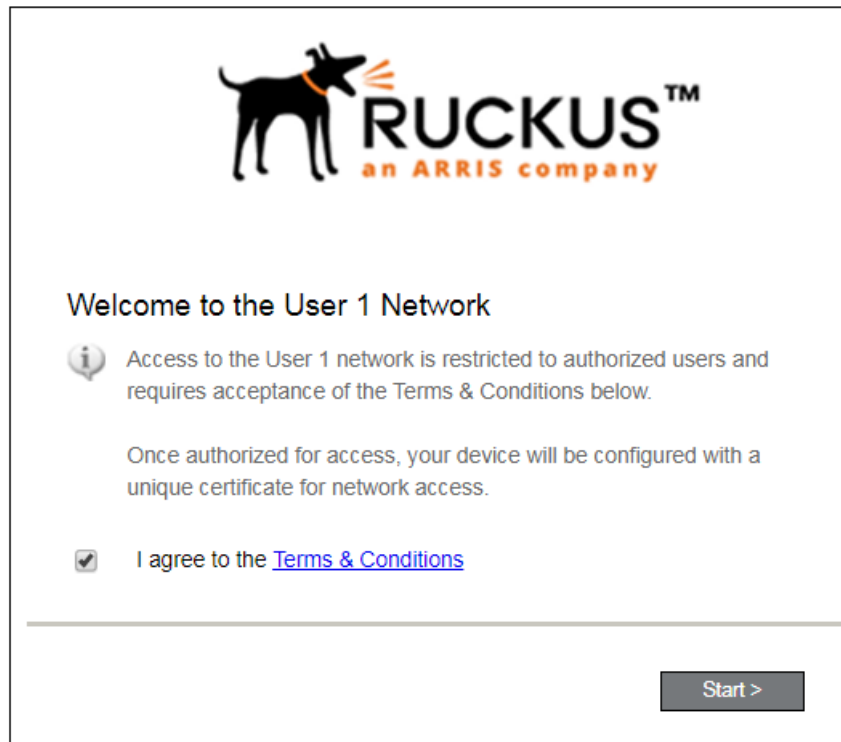
When the user enters the enrollment URL on their device, the Login (or Welcome) screen displays.

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



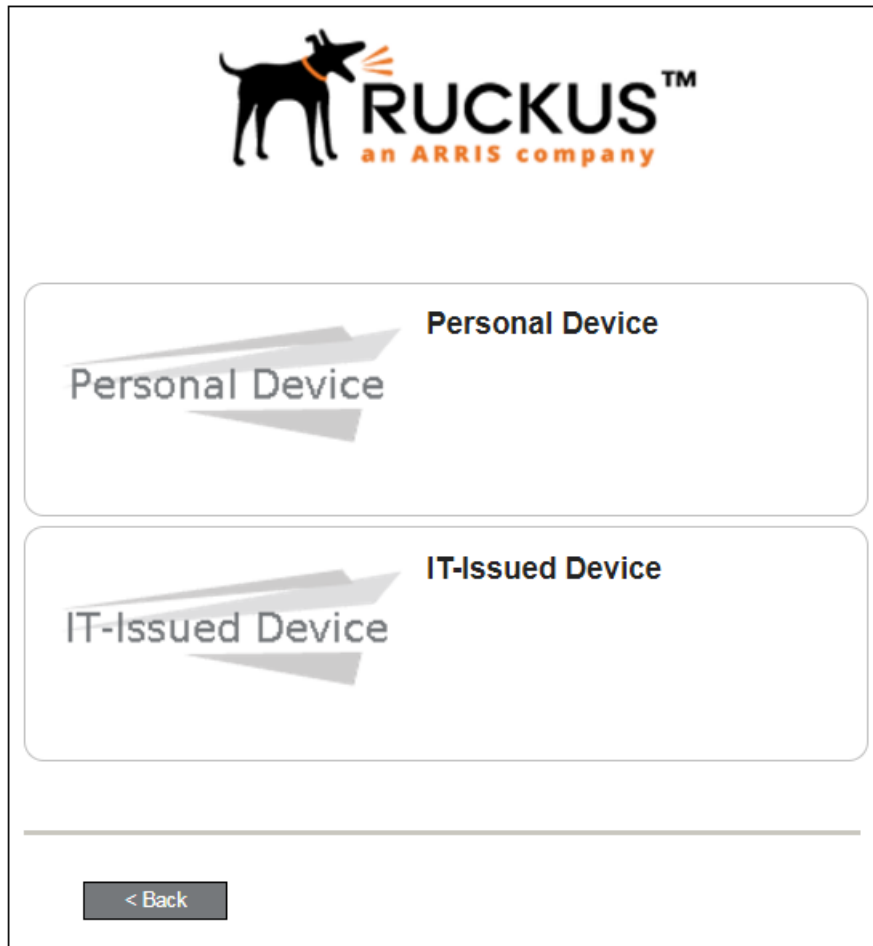
Select the user type to continue. This example follows the *Employee* workflow branch.

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 3 Device Type Prompt



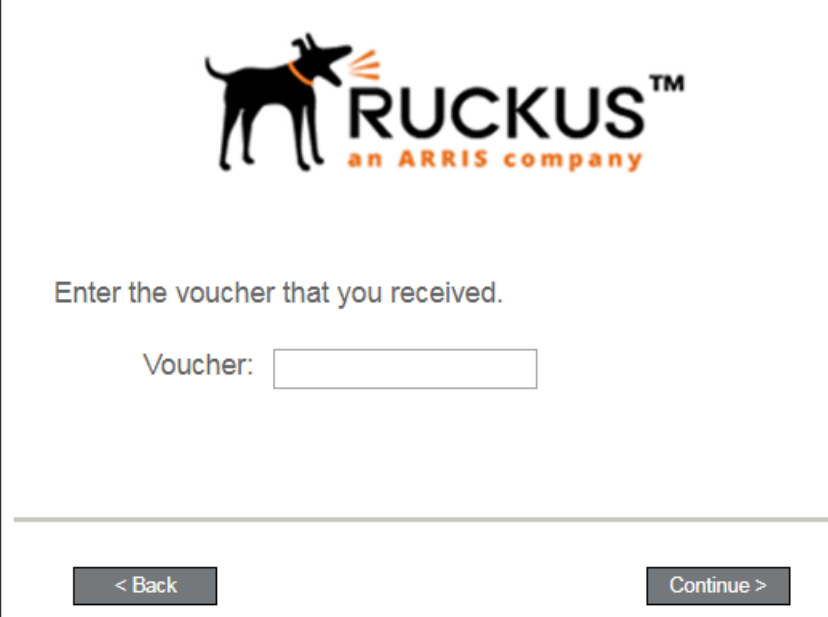
Select a device type to continue. This example follows the IT-Issued Device enrollment workflow.

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 4 Voucher Code Prompt



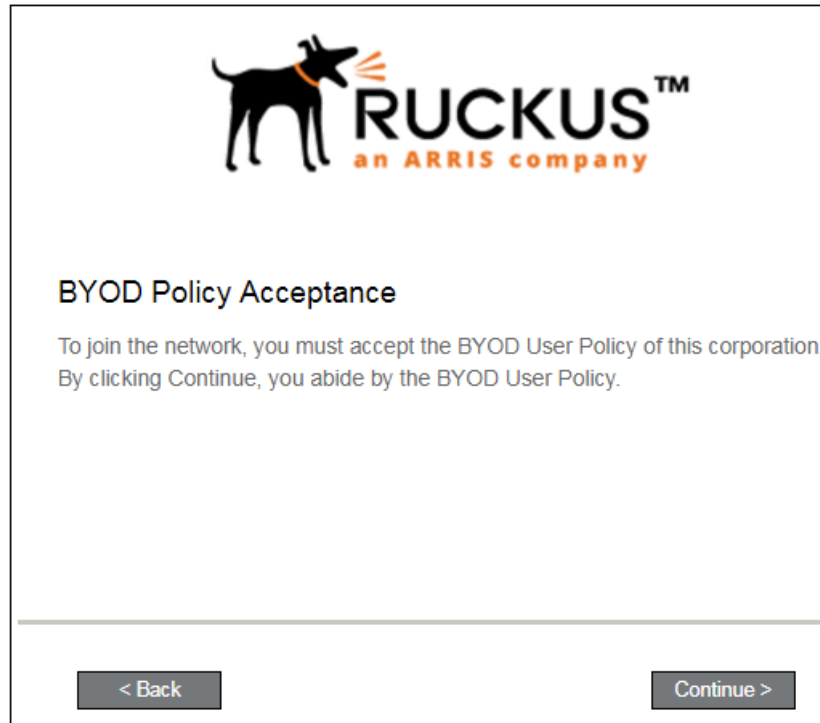
The image shows a user interface for entering a voucher code. At the top center is the RUCKUS logo, which features a black silhouette of a dog with an orange collar and three orange lines radiating from its head, followed by the text "RUCKUS™" in black and "an ARRIS company" in orange below it. Below the logo, the text "Enter the voucher that you received." is displayed. Underneath this text is the label "Voucher:" followed by a rectangular text input field. At the bottom of the screen, there are two buttons: a grey button on the left with the text "< Back" and a grey button on the right with the text "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 5 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 6 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

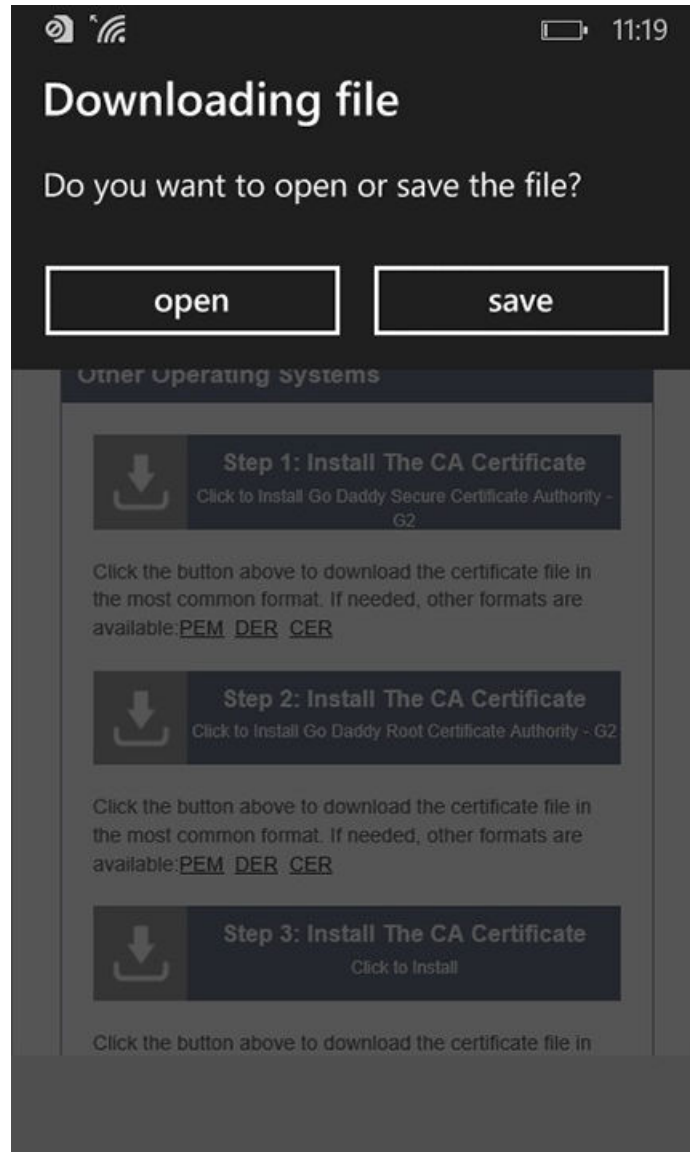
The certificate information is not populated on the configuration step until the certificates have been downloaded.

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 7 Download File



Tap **Save** to continue.

Start CA Certificate Installation

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

FIGURE 8 Tap Screen to Open

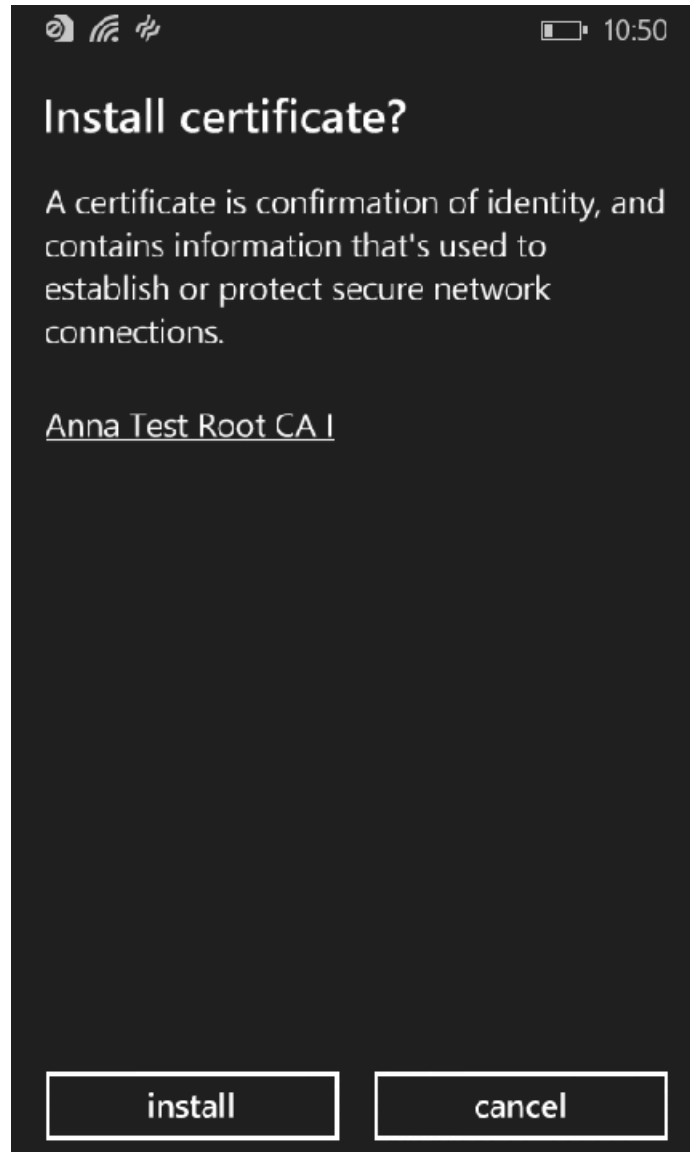


Continue with the certificate installation.

Install CA Certificate

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

FIGURE 9 Install CA Certificate

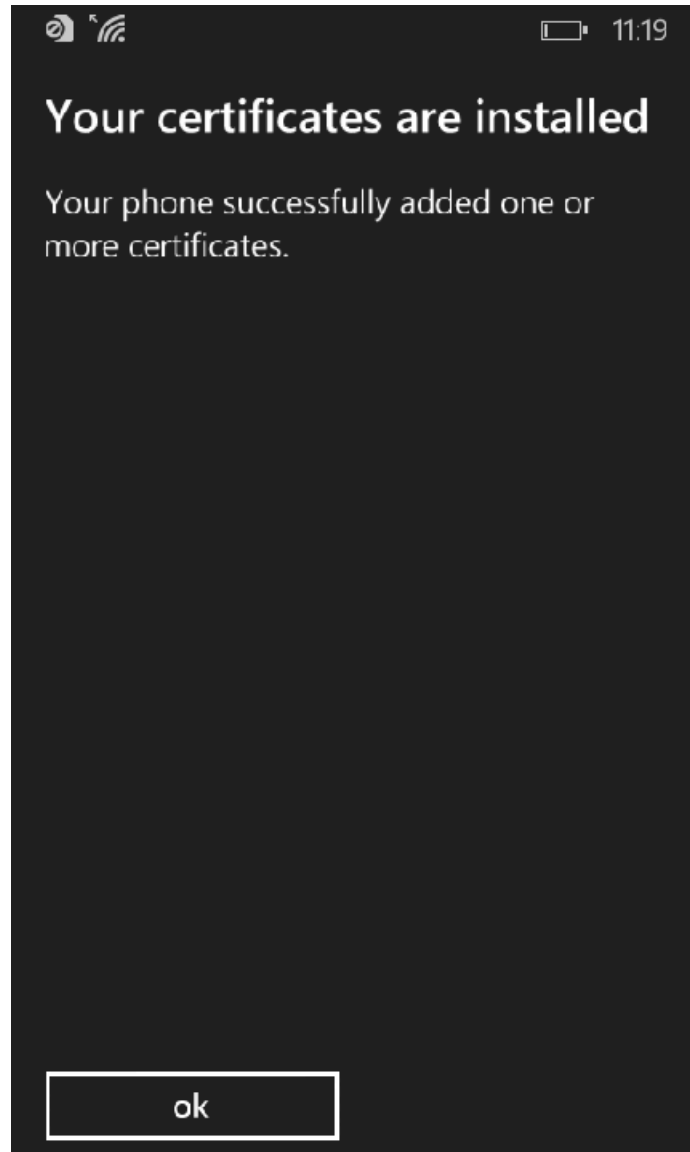


Tap **Install** to continue.

CA Certificates installed

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

FIGURE 10 Certificates are Installed



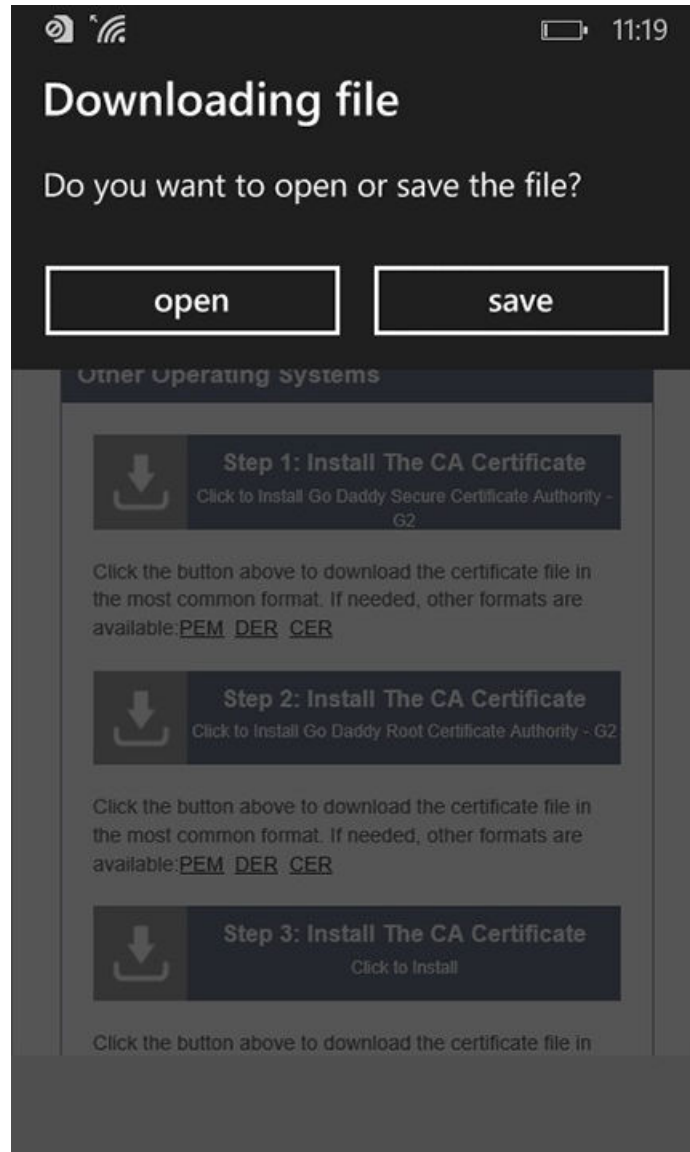
Tap the **ok** button.

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 11 Download File

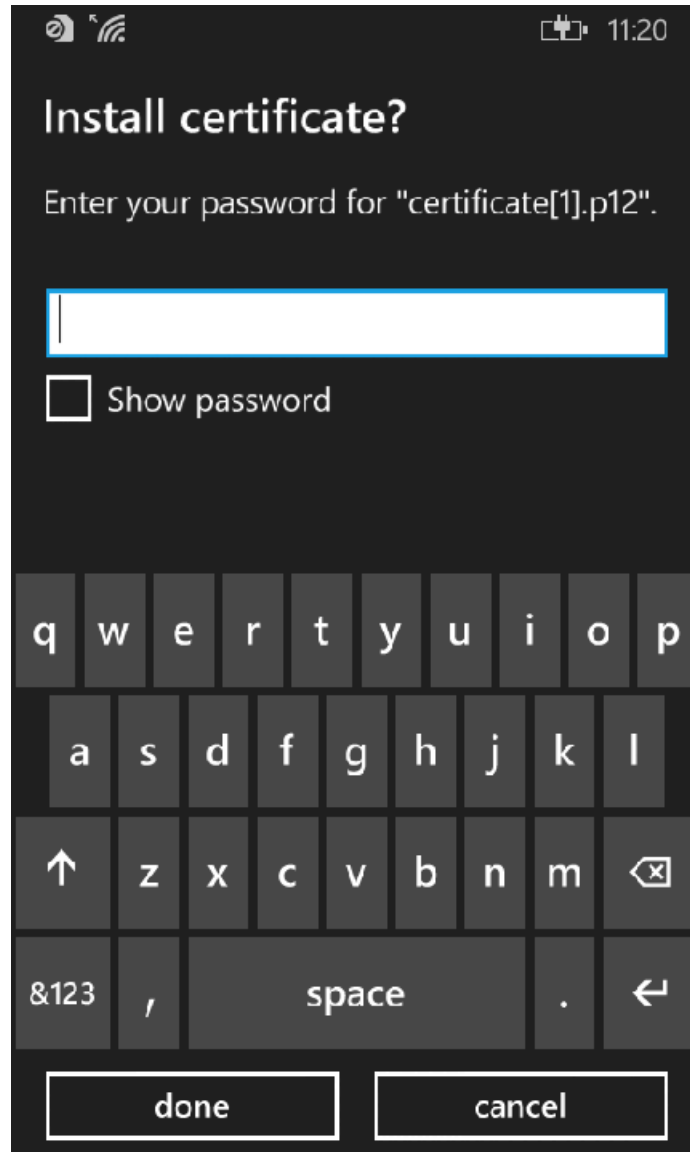


Tap **Save** to continue.

Enter User Certificate Password

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

FIGURE 12 Enter User Certificate Password



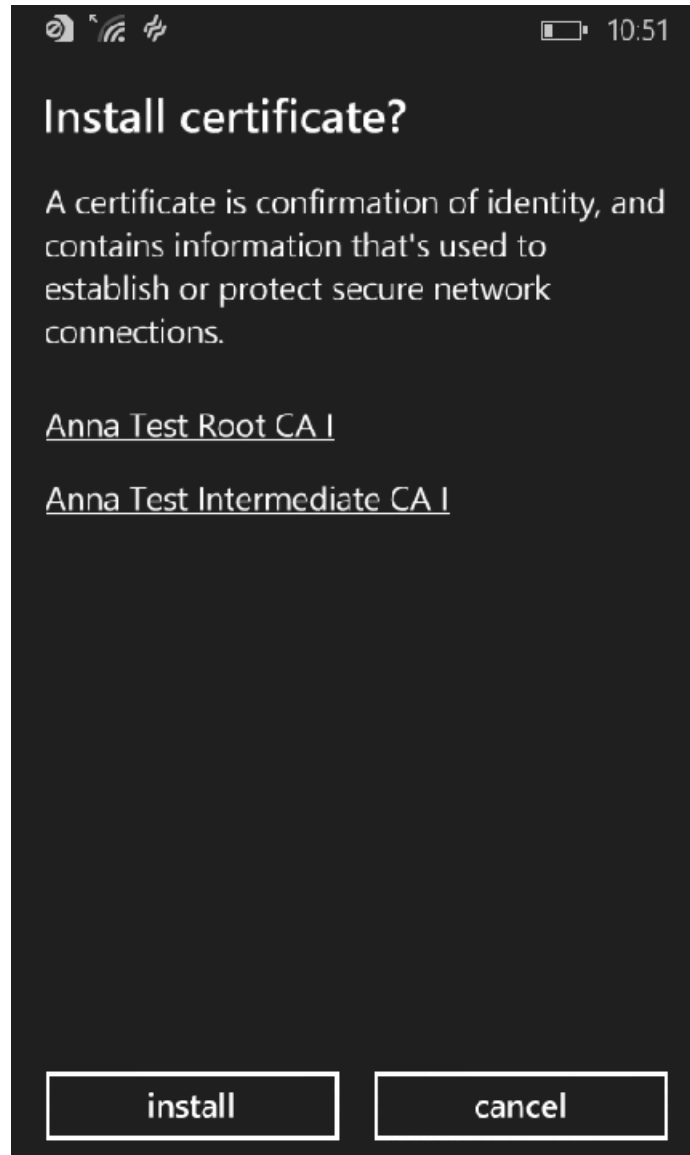
Enter the password from your user credentials. For example, if your user credentials are username=bob and password=bob1, then enter bob1 for the user certificate password.

Tap **done** to continue.

Install User Certificates

Install the user certificates provided for this device.

FIGURE 13 Install User Certificates

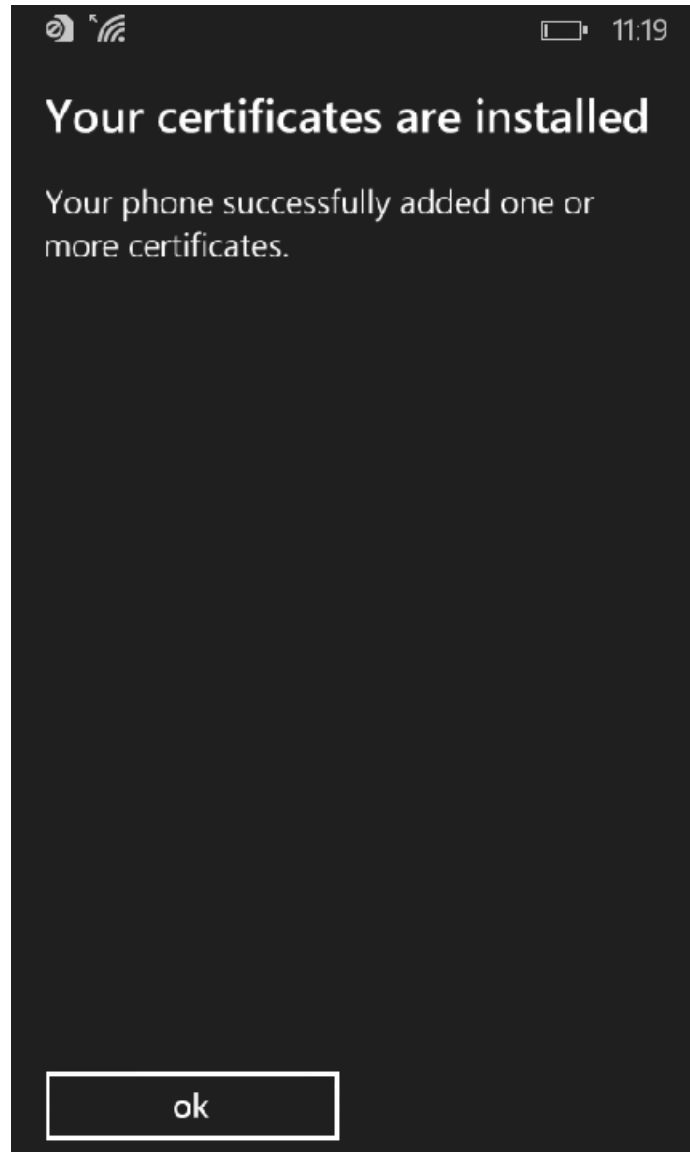


Tap **Install** to continue.

Certificates installed

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

FIGURE 14 Certificates are Installed



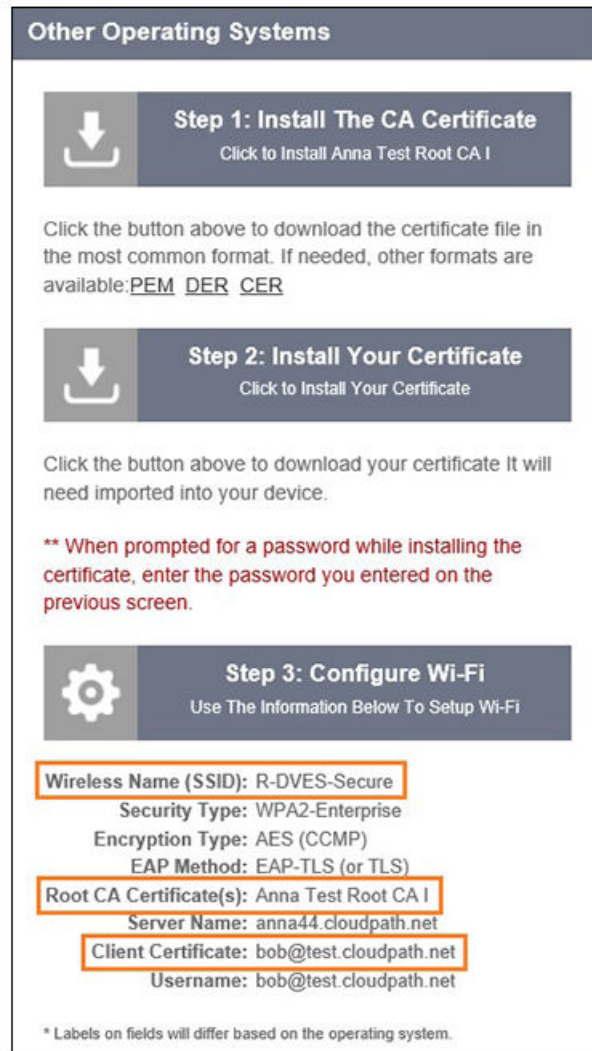
Tap the **ok** button.

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 15 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.

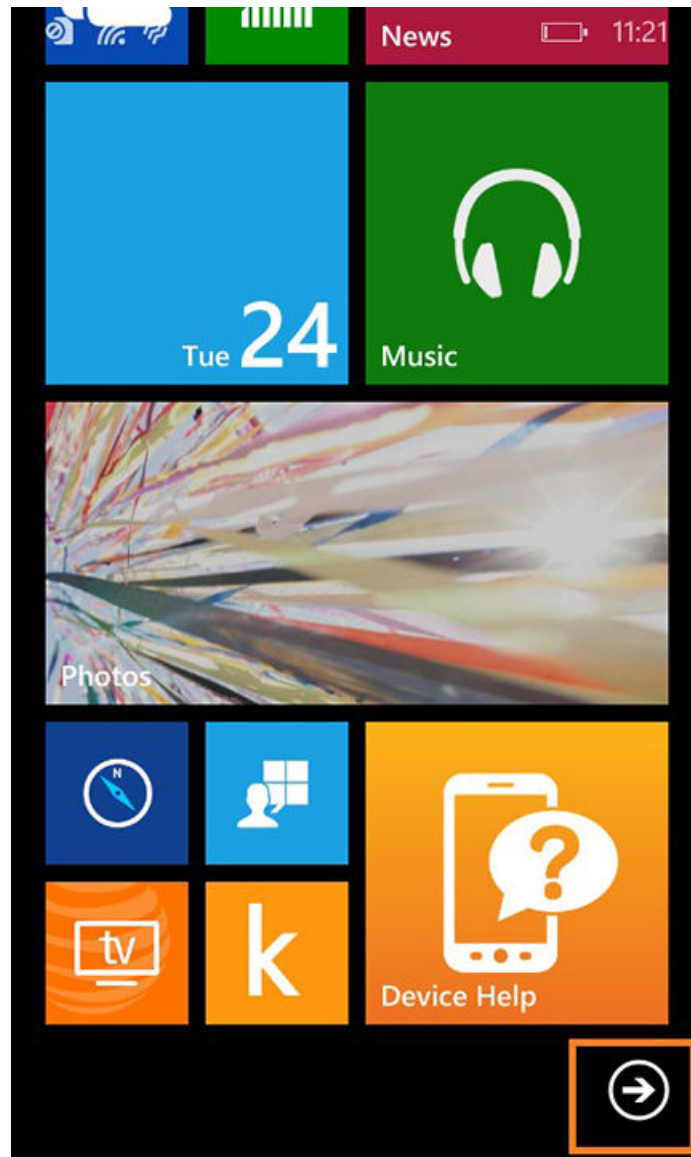
Continue to the next screen to configure Wi-Fi settings on the Windows Phone.

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 16 Install From Amazon Market

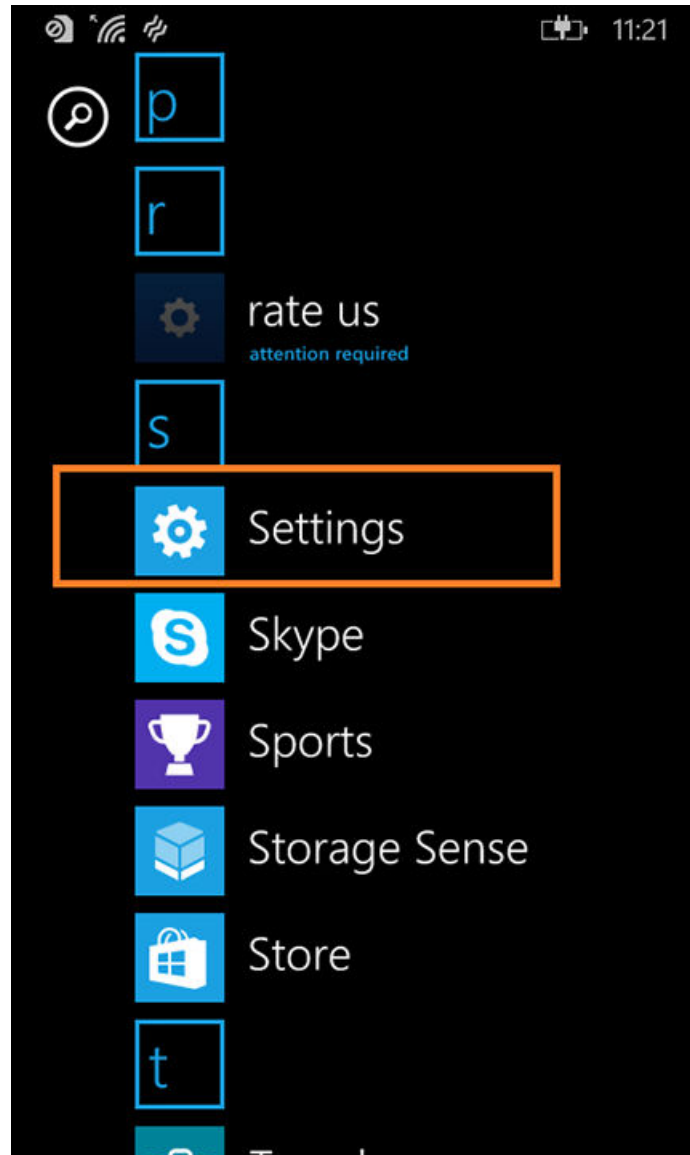


Continue to the next screen to locate the *Settings* on the Windows Phone.

Access Device Settings

Go to the device *Settings*.

FIGURE 17 Device Settings

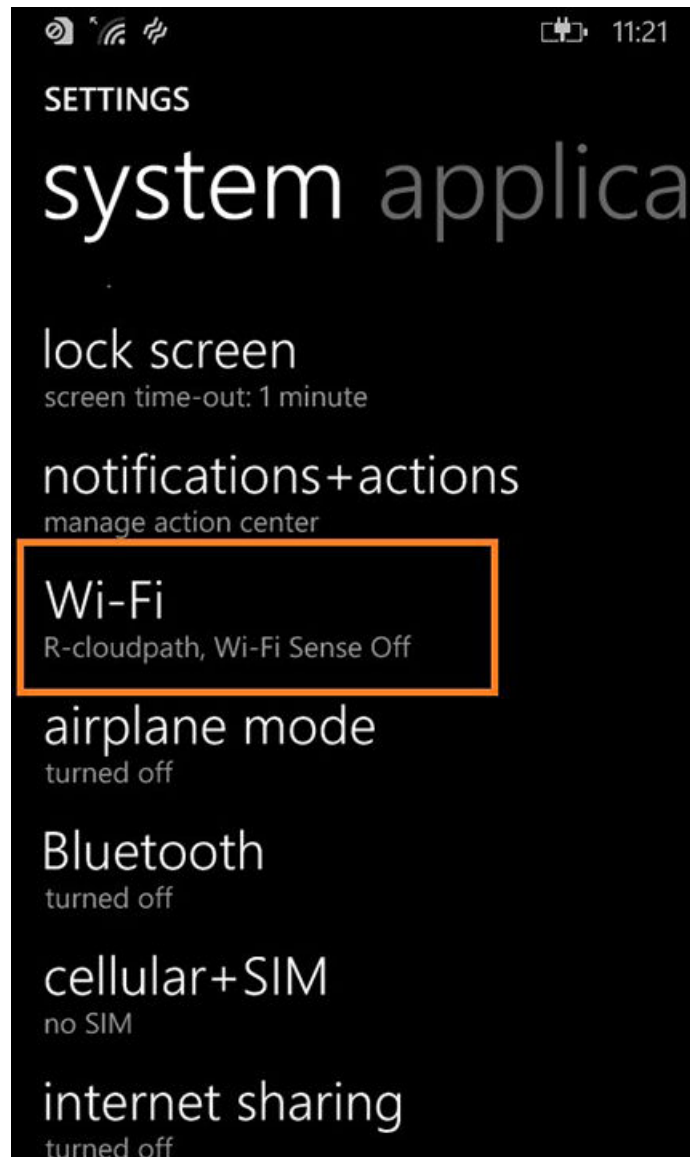


Tap **Settings** to continue.

Locate Wi-Fi Settings

Go to the *Wi-Fi* setting.

FIGURE 18 Wi-Fi Settings



Tap **Wi-Fi** to continue.

Configure Wi-Fi Settings

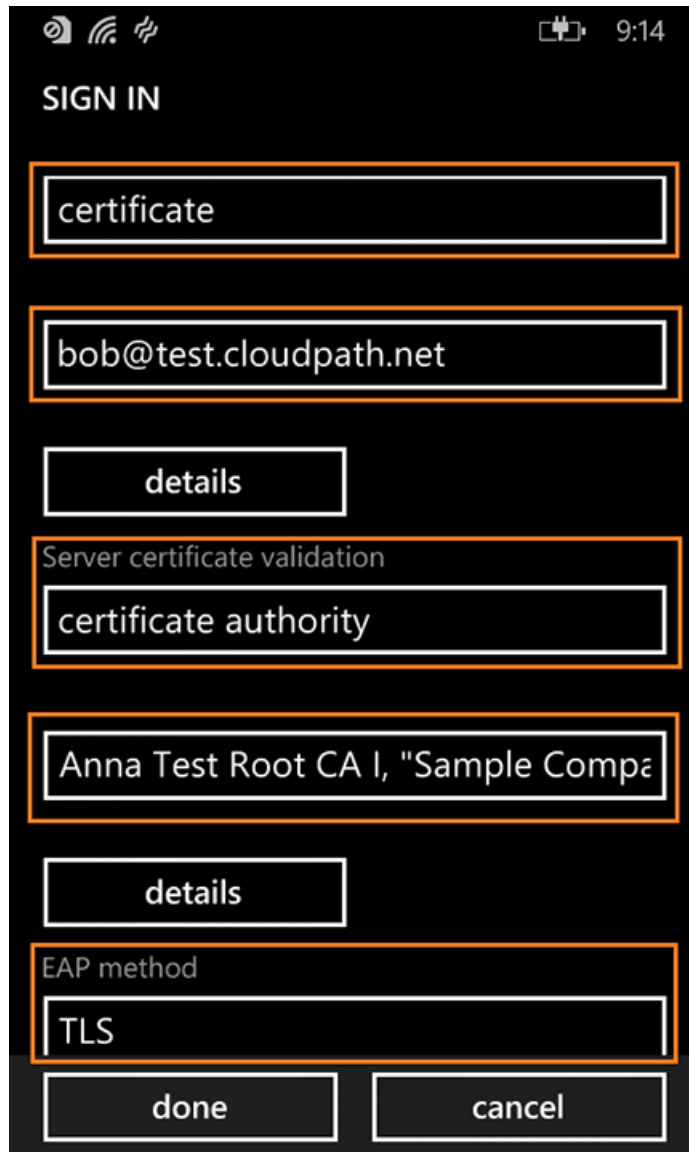
Tap the Wireless Network listed in the configuration instructions.

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 19 Configure Wi-Fi Settings



Tap done to continue.

Connected to Secure Network

FIGURE 20 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.

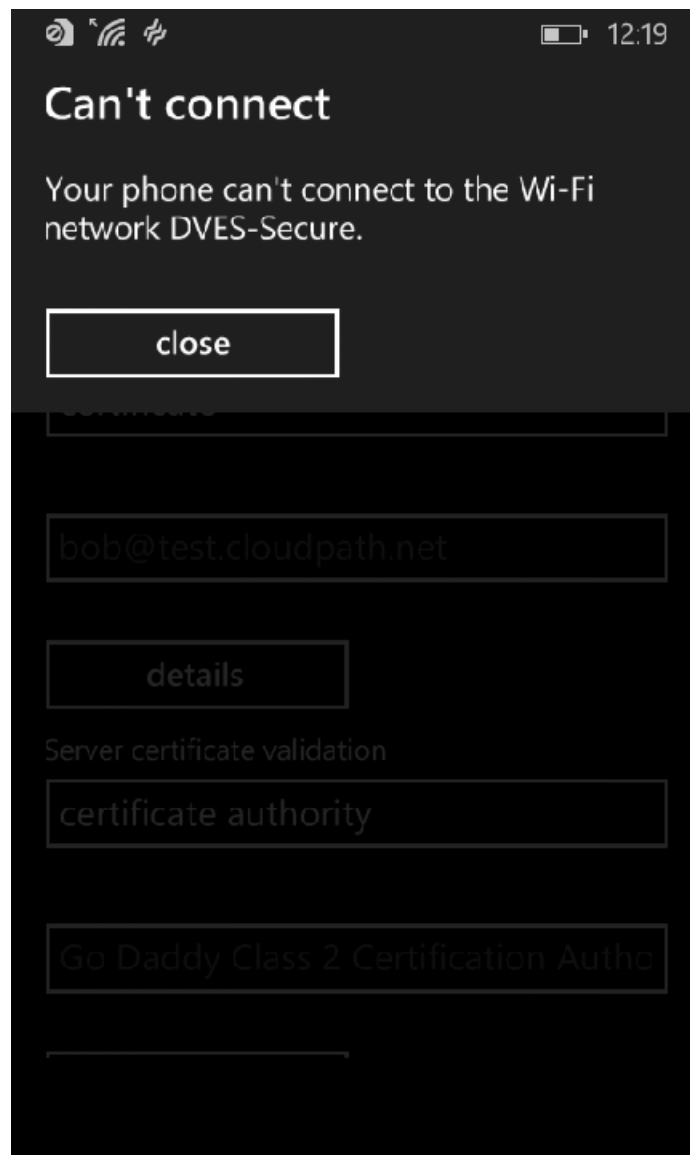
Delete Network

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 21 Device Can't Connect

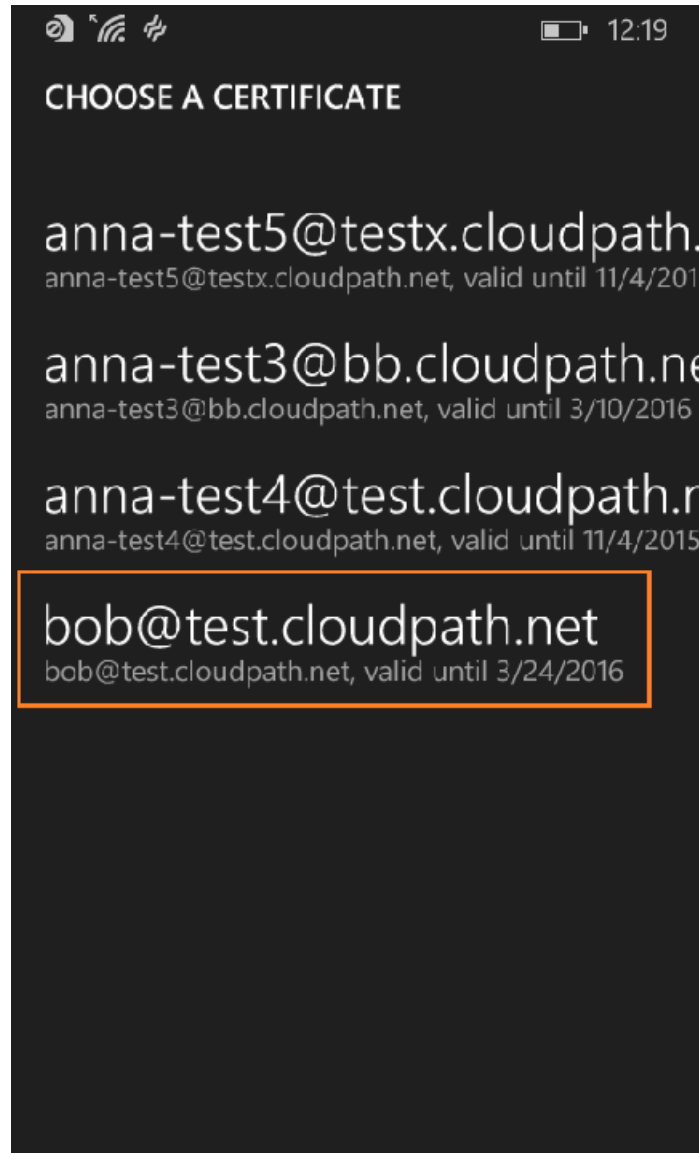


Be sure that your selections on the Wi-Fi configuration page match the settings provided on the Other Operating Systems tab. Refer to [Windows Phone Configuration Instructions](#) on page 18 for more information.

Use these settings:

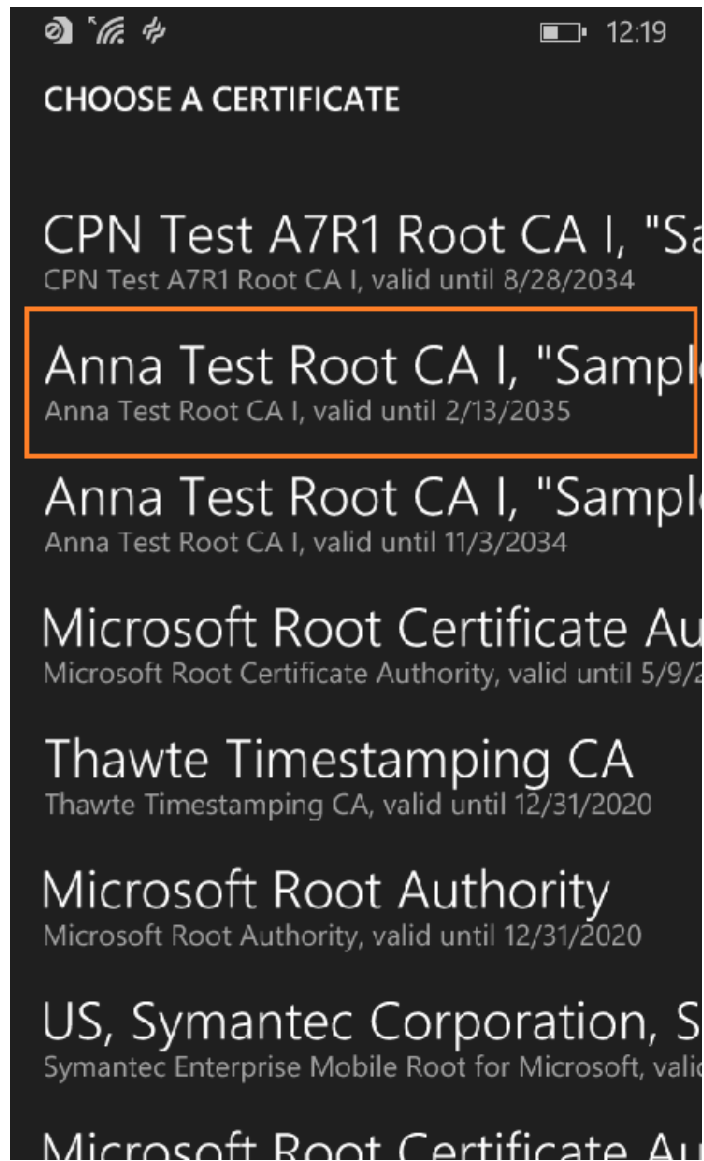
- Connect using **certificate**.
- Choose a certificate to match the **Client Certificate** in the configuration instructions.

FIGURE 22 Choose A User Certificate



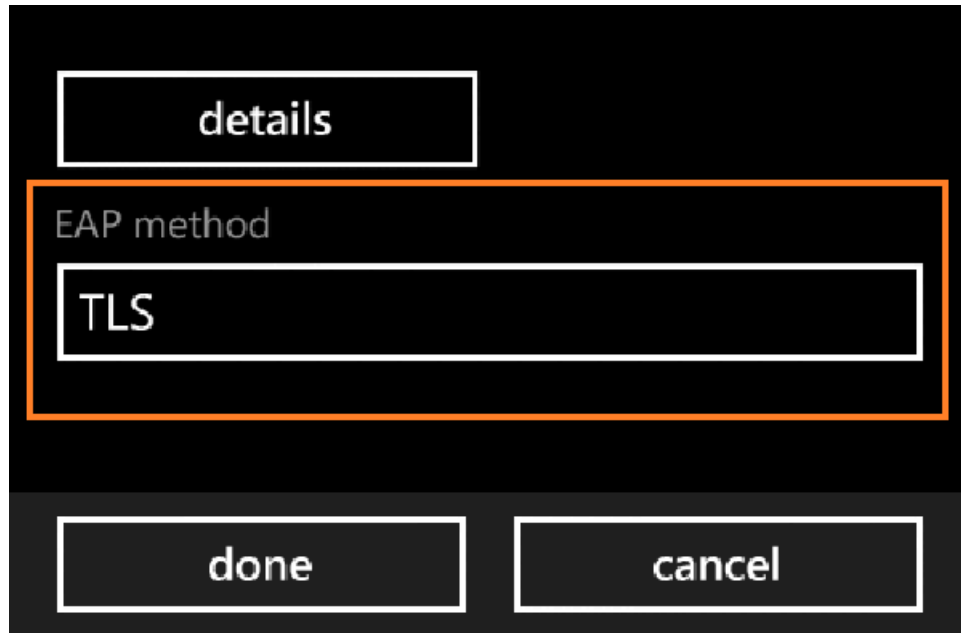
- Server Certificate Validation must be **certificate authority**.
- Choose the **Root CA Certificate** to match the configuration instructions.

FIGURE 23 Choose A Root CA Certificate



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

FIGURE 24 EAP Method



End-User Experience for Windows Devices

- Supported Windows versions..... 39
- User Experience..... 39

Supported Windows versions

Cloudpath supports Windows Vista, Windows 7, 8, 10, and later, with automated 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 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 an enrollment can differ, depending on the selection that is made.

Welcome Screen With AUP

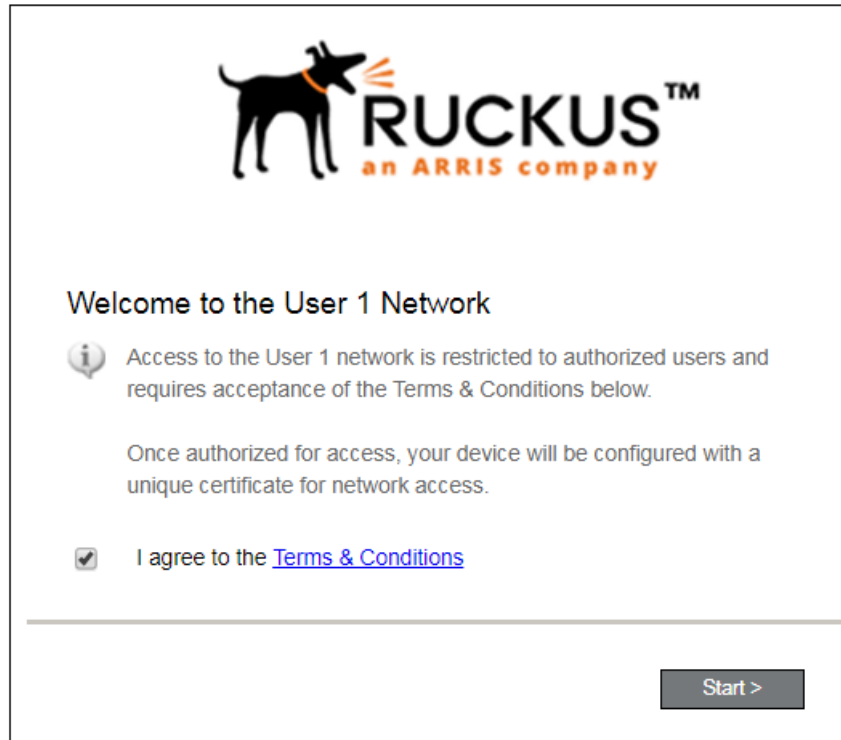
When the user enters the enrollment URL on their device, the Login (or Welcome) screen displays.

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 25 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 26 User Type Prompt

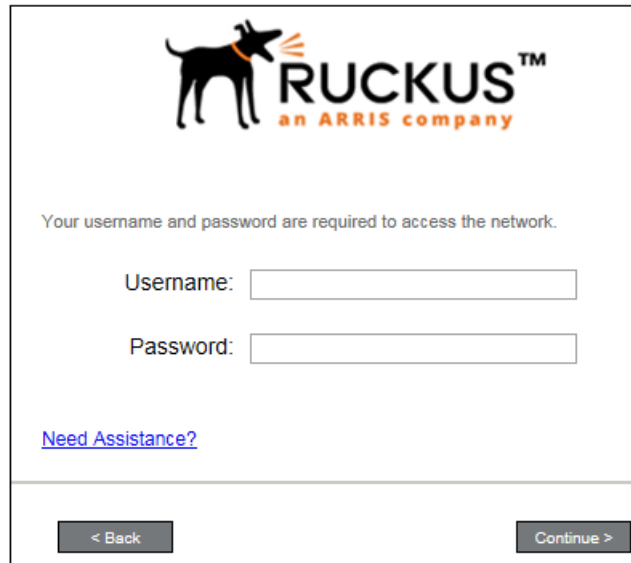



Select the user type to continue. This example follows the *Employee* workflow branch.

User Credentials

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

FIGURE 27 User Credential Prompt





Your username and password are required to access the network.

Username:

Password:

[Need Assistance?](#)

< Back Continue >

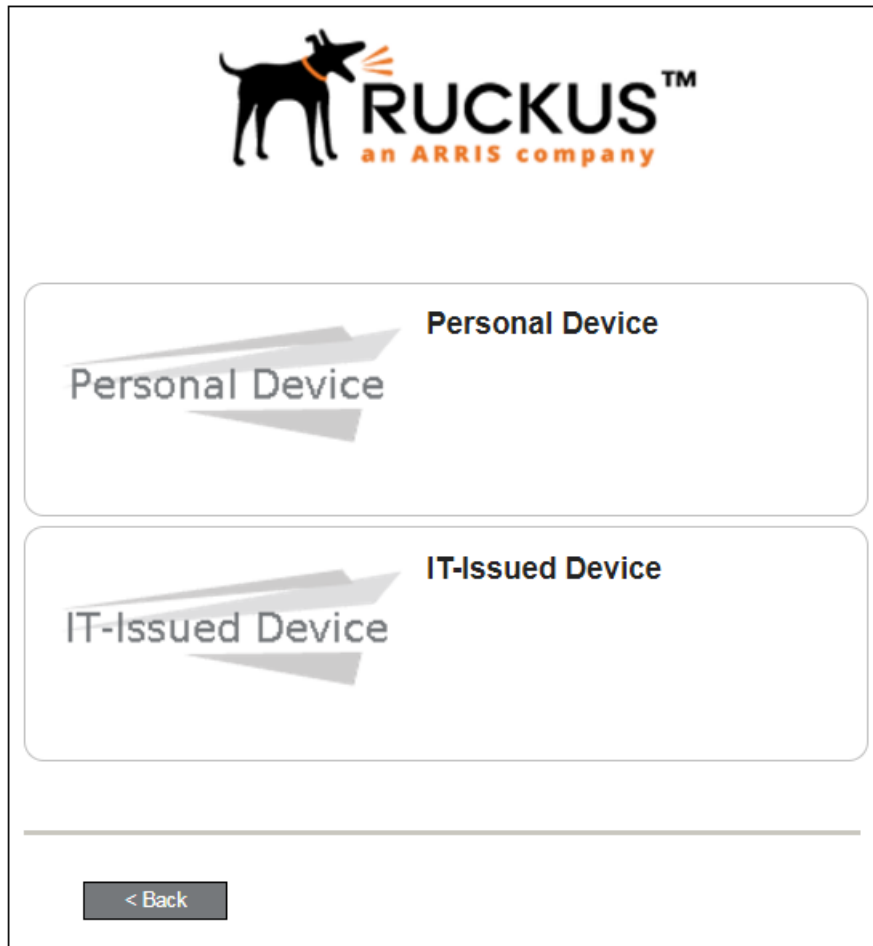
Enter the user credentials and click **Continue**.

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 28 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 29 Voucher Code Prompt



Enter the voucher that you received.

Voucher:

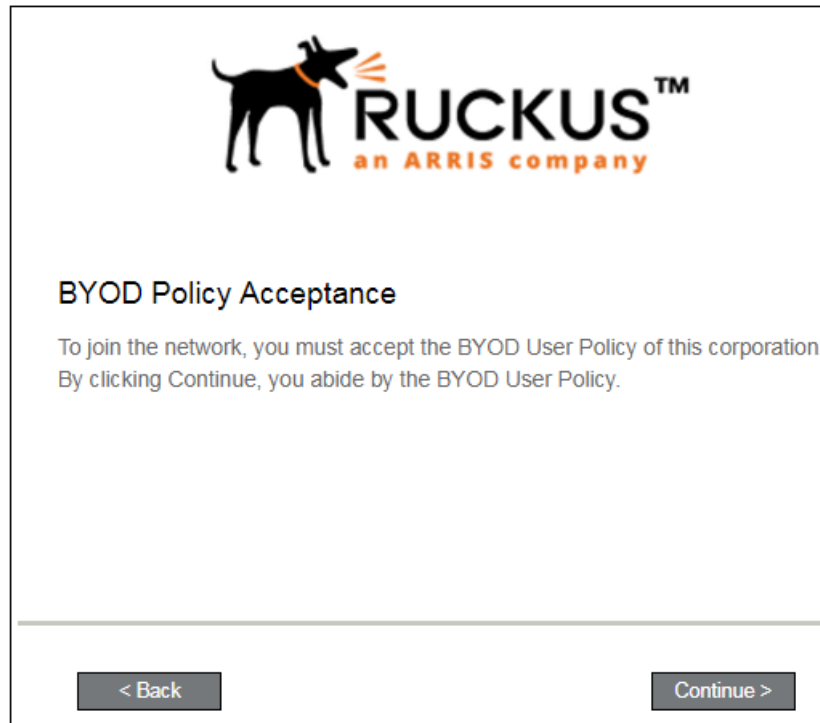
< Back Continue >

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 30 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 Windows 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. These user experience options are set in the Cloudpath 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.

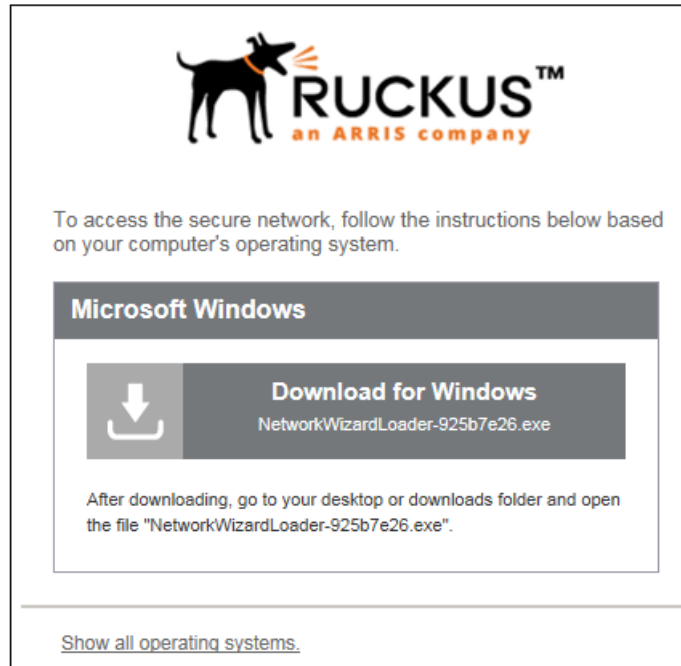
Download and Run Application

The default user experience setting for Windows devices 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 Windows-specific instructions.

FIGURE 31 Windows Download Page

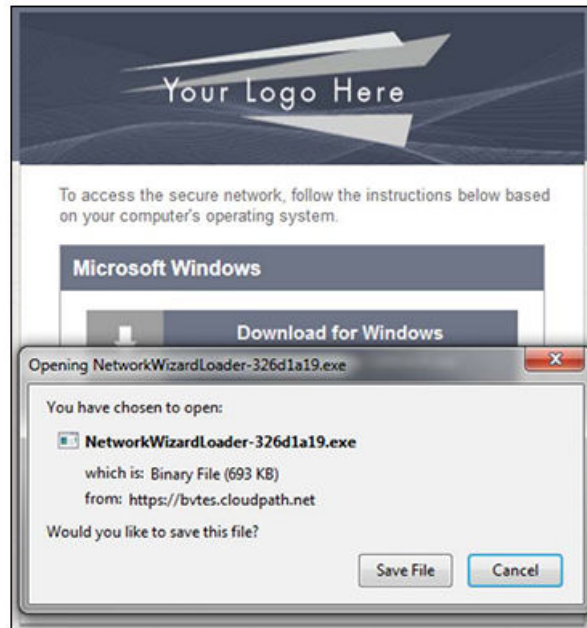


Click the down arrow to download the zip file, which contains the application file.

Save the File

You will be asked to save the application file.

FIGURE 32 Save File



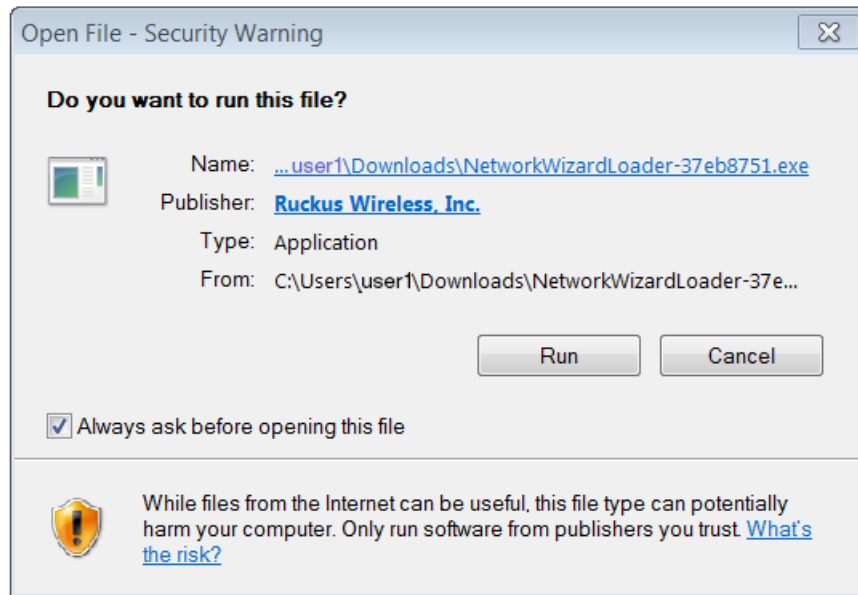
Locate and Open the File

Find the **Cloudpath** application file in your Downloads folder, then double-click this file to start the Wizard, which runs through the configuration and migration process.

Confirm Running the File

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

FIGURE 33 Confirm Running the File



Click **Run** 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.

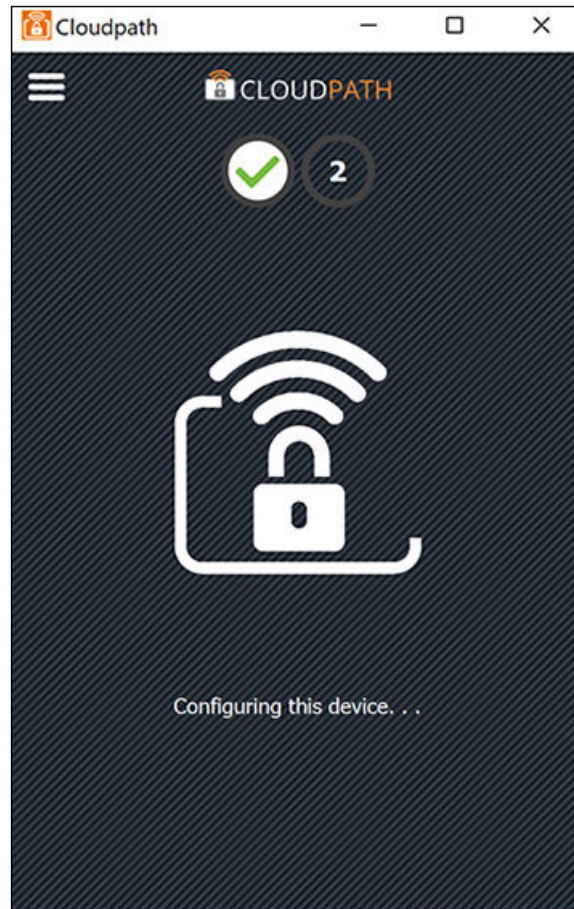
Loading System Configuration

The Wizard opens and begins the configuration process. You may receive a status message on your device such as: "Loading Configuration."

Configuring the Device

The application begins the configuration process.

FIGURE 34 Configuring the Device



Click **Yes** if asked to install the certificate. The entire configuration process should take less than one minute. The application continues with the authentication process.

Connecting to Secure Network

The application attempts to associate to the wireless network. You may receive a status message on your device such as: "Attempting to connect to the network..."

Validating Connectivity

The application continues with the validation process.

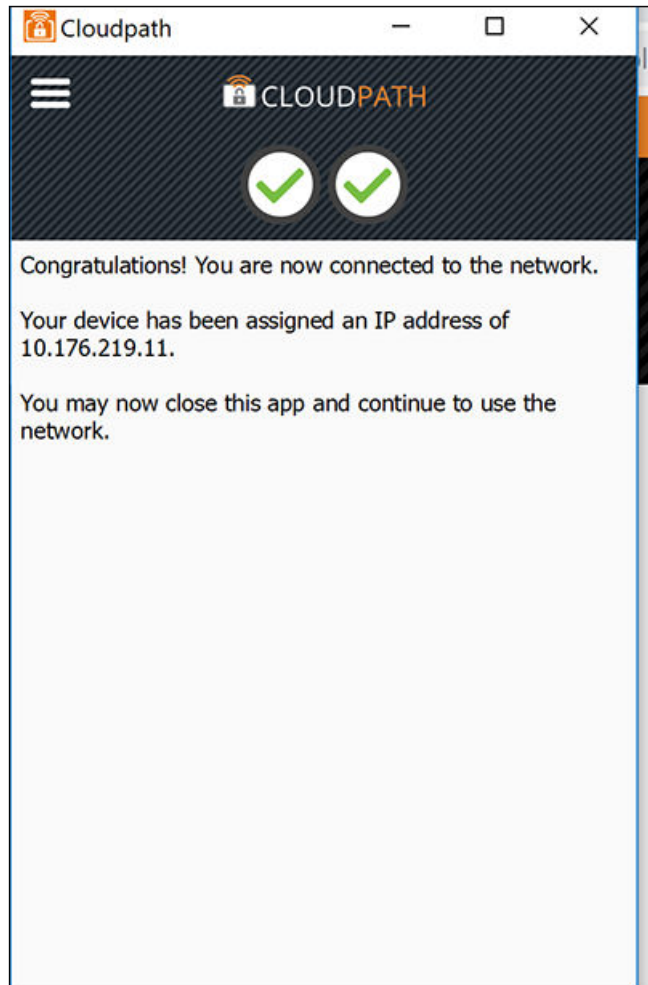
When the association with the secure network is successful, the application attempts to acquire a network address. A screen may appear briefly to indicate that connectivity is being validated.

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.

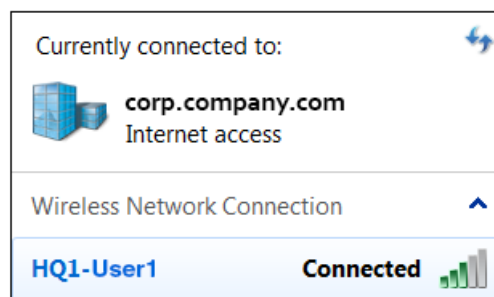
FIGURE 35 Connected to the Network



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 36 Verifying Wireless Connection



The Wireless Network Connection panel displays the network to which you are connected.

Other Methods for Launching Application

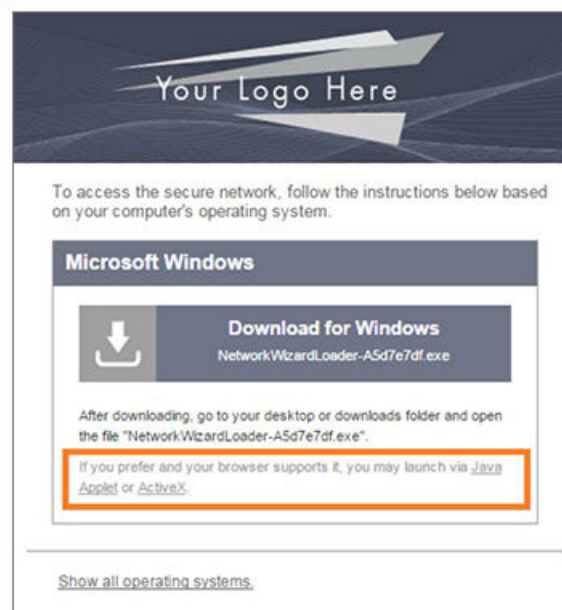
The default user experience setting will display the download page to allow the user to download, install, and run the application. The network administrator can elect to configure other user experience settings, such as automatically launching the application, or, if using the Internet Explorer browser, the user can manually launch the application using ActiveX.

Starting Application from Java Applet

If your configuration is set up to automatically run the Java applet, the Download page does not appear. Instead, a Java console opens and the application automatically starts. If this is your network setting, go to the Wizard Application User Experience section to view the end-user experience.

You can also launch the Java applet manually from the download page. Use the **launch via Java applet** link, instead of downloading and installing the application manually.

FIGURE 37 Manually Launch Applet



The application launches as a Java applet.

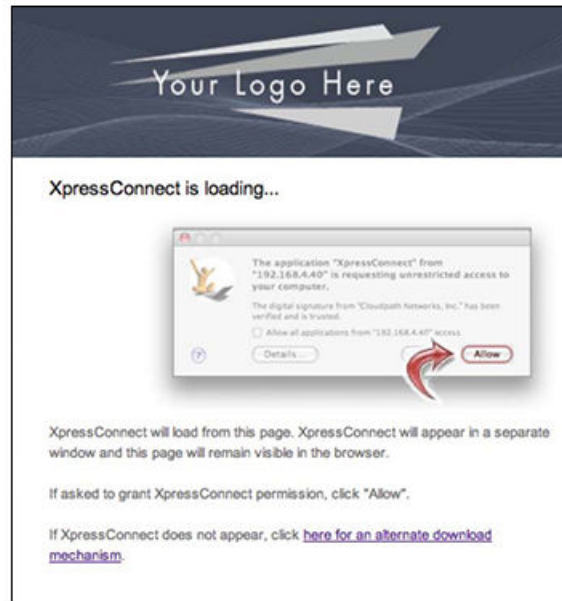
NOTE

This method does not work if Java is not installed on the device. If Java is installed, but requires an update, you may be prompted to update before you can continue.

Load Application

The application loads onto the device.

FIGURE 38 Load Application

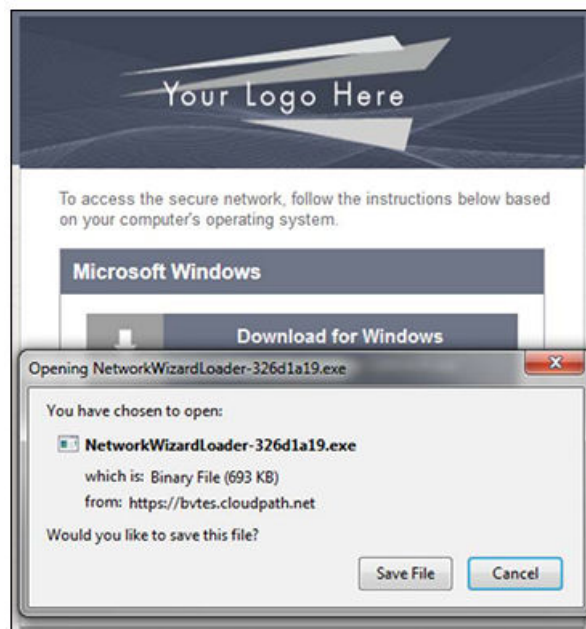


The application continues to check the device settings.

Save File

Confirm that you want to save the Cloudpath application to your downloads folder.

FIGURE 39 Save File



Click **Save File** to continue.

Trust Application

The Windows operating system might prompt you to trust the Cloudpath application.

FIGURE 40 Trust Application



Click **Run** to continue. The configuration wizard starts.

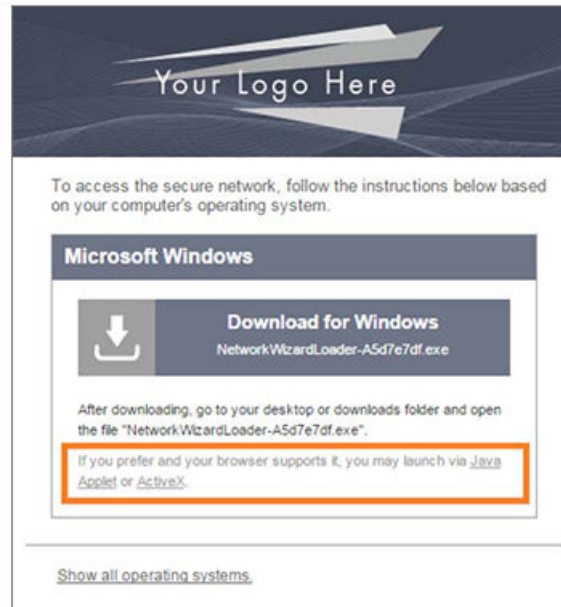
See the Wizard Application User Experience section to view the end-user experience.

Launch Application Using ActiveX

If your configuration is set up to automatically run the Java applet, the Download page does not appear. Instead, a Java console opens and the application automatically starts. If this is your network setting, go to the Wizard Application User Experience section to view the end-user experience.

You can also launch the application manually from the download page using ActiveX, instead of downloading and installing the application manually.

FIGURE 41 Manually Launch Applet



Double-click the ActiveX link to launch the application.

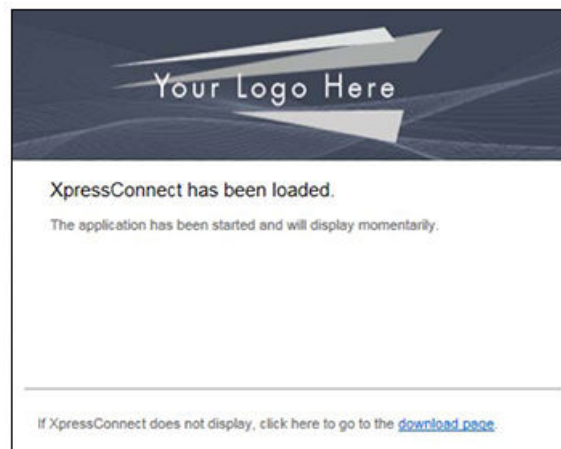
NOTE

This method works on the Internet Explorer browser with ActiveX enabled.

Load Application

ActiveX loads the application on the device and it automatically starts the configuration and migration process.

FIGURE 42 Load Application



See the Wizard Application User Experience section to view the rest of the end-user experience.

End-User Experience for iOS Devices

- Supported iOS Versions..... 55
- User Prompts..... 55

Supported iOS Versions

The Cloudpath application supports iOS versions 9.0, and later, with automated configuration. All earlier versions are supported with a manual configuration.

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

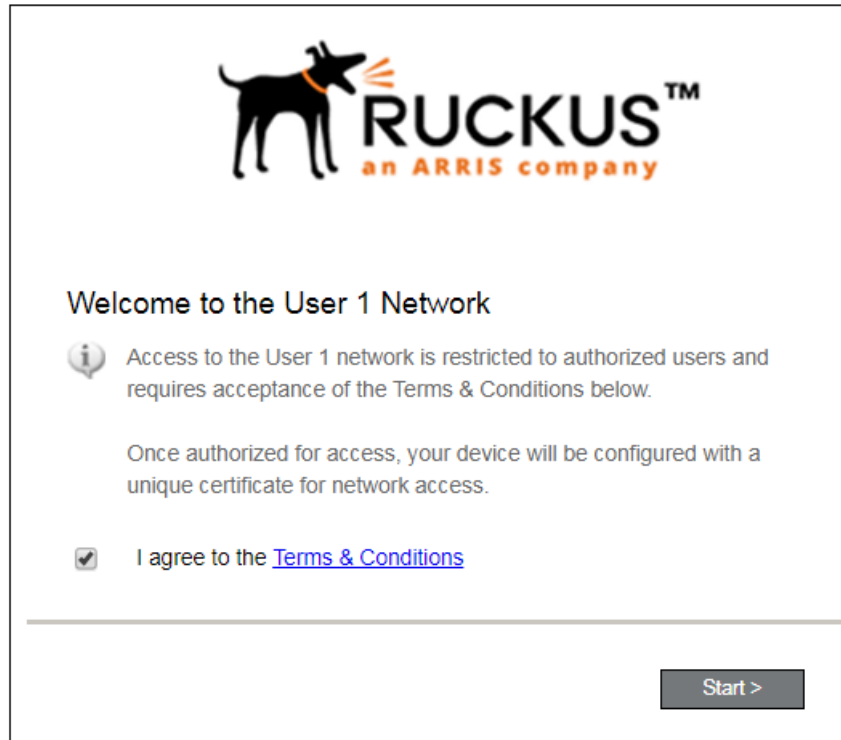
When the user enters the enrollment URL on their device, the Login (or Welcome) screen displays.

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 43 Welcome Screen



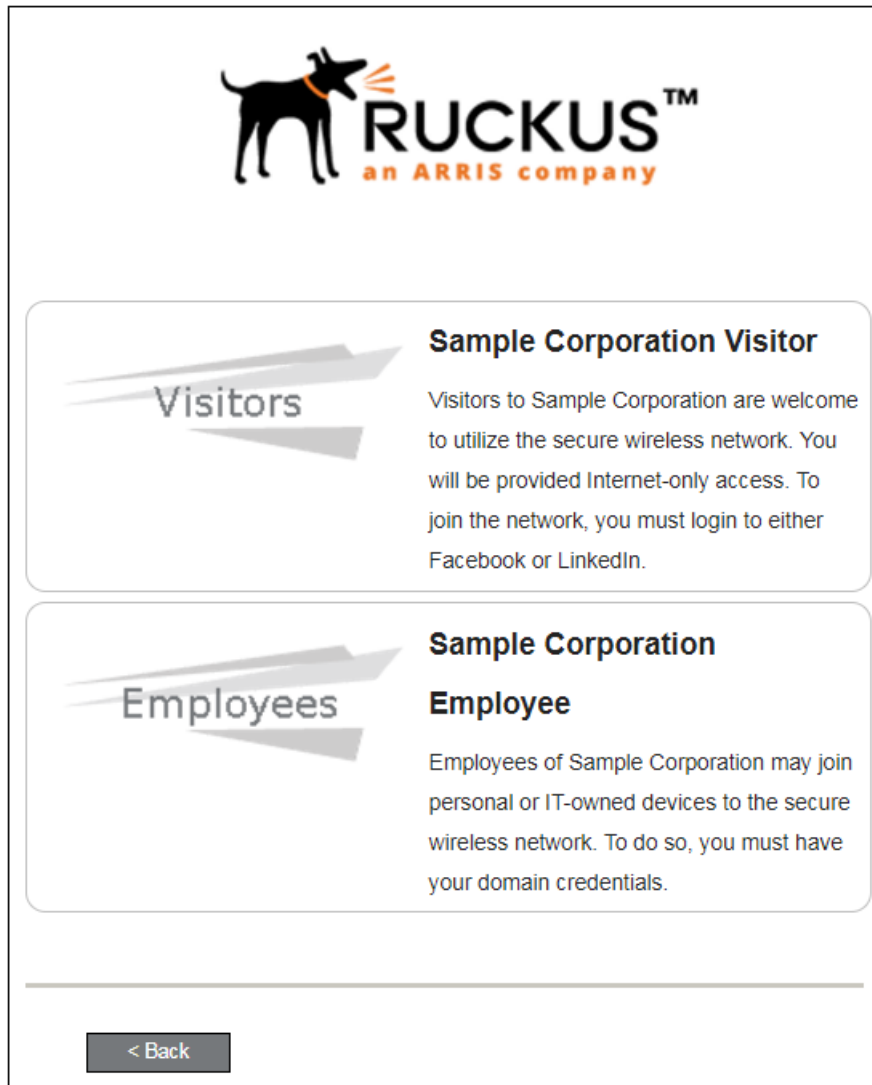
An acceptable use policy (AUP) prompt displays a message and requires that the user signal acceptance to continue. The welcome text and Start button can be customized.

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 44 User Type Prompt

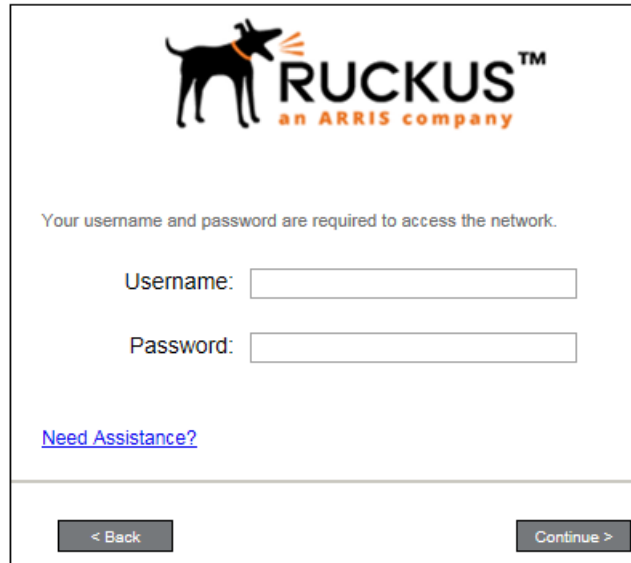


Select the user type to continue. This example follows the *Employee* workflow branch.

User Credentials

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

FIGURE 45 User Credential Prompt



The screenshot shows a login prompt for Ruckus, an ARRIS company. At the top is the Ruckus logo, which features a black silhouette of a dog with three orange lines above its head, followed by the text "RUCKUS™" and "an ARRIS company" in orange. Below the logo, the text reads "Your username and password are required to access the network." There are two input fields: "Username:" followed by a white rectangular box, and "Password:" followed by a white rectangular box. Below the input fields is a blue hyperlink that says "Need Assistance?". At the bottom of the screen, there are two grey buttons: "< Back" on the left and "Continue >" on the right.

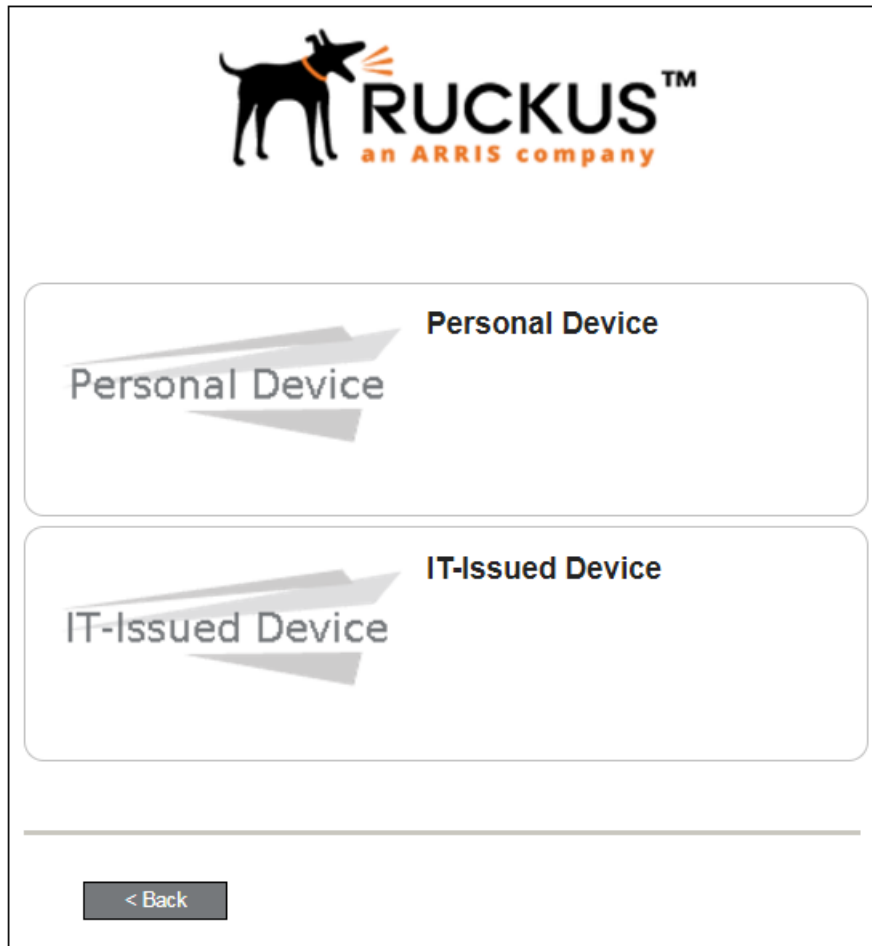
Enter the user credentials and click **Continue**.

Device Type

If required by the network, the user might 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 46 Device Type Prompt



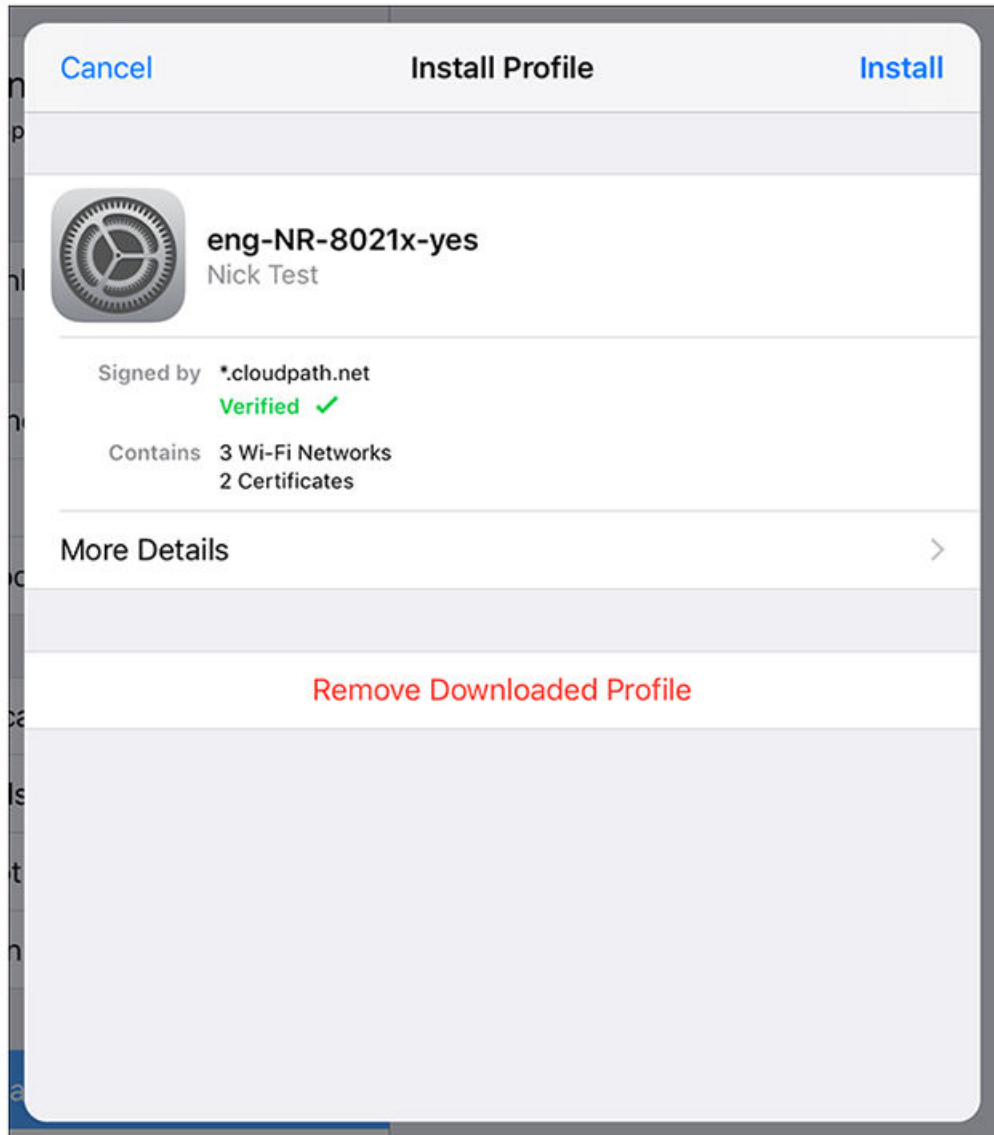
Select a device type to continue. This example follows the IT-Issued Device enrollment workflow.

Install Profile

Follow these steps:

1. Go to the main screen of your iOS device.
2. Tap the Settings icon.
3. Tap **Profile Downloaded**.
4. On the Install Profile window, tap **Install**:

FIGURE 47 Install Profile



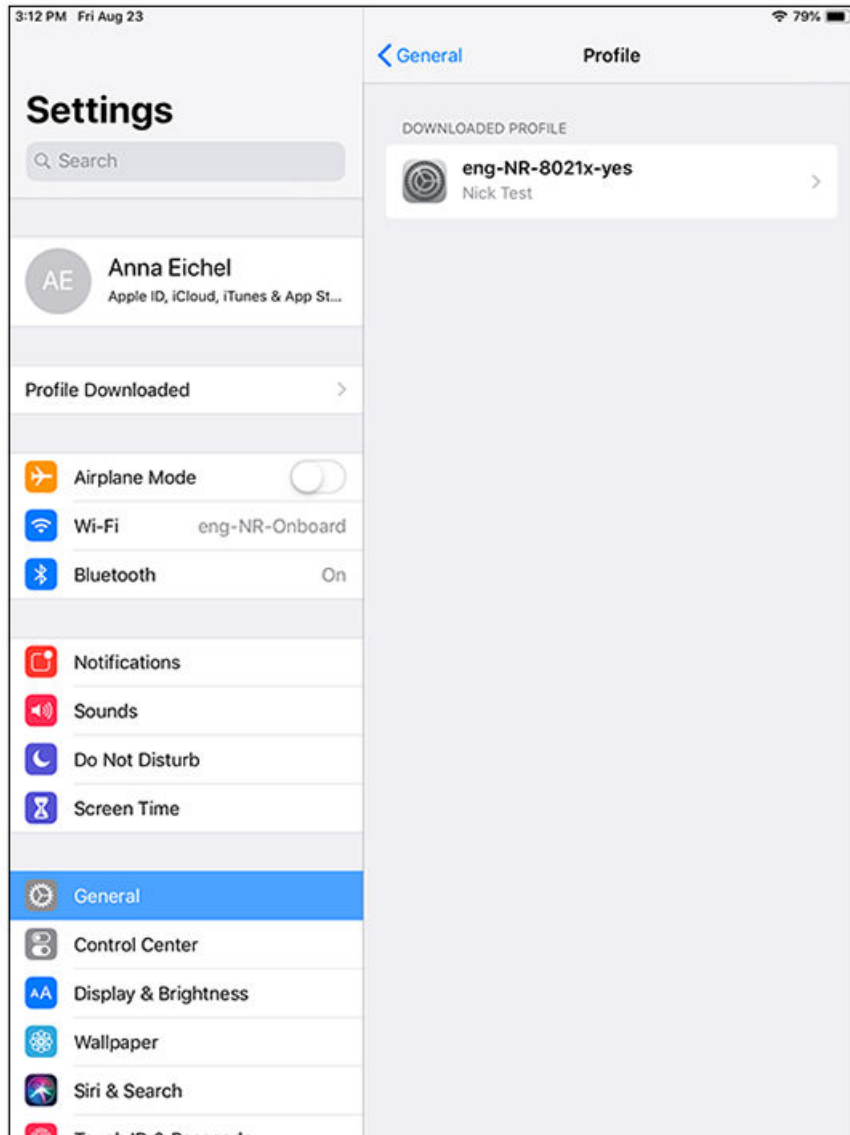
5. If prompted, enter the device passcode and continue.
6. If prompted, install the root CA.
7. If prompted, confirm the installation of the profile.
8. You should receive a "Profile Installed" message. Tap **Done**.

Connect to Secure Network

Follow these steps:

1. If you wish to view the profile, go to **Settings > General > Profiles**:

FIGURE 48 View Profile



2. In **Settings** > **Wi-Fi**, tap and set the Wi-Fi switch to on.
3. In **Settings** > **Wi-Fi**, select the secure SSID network.
The user should be connected to the secure network.

End-User Experience for MAC Devices

- Supported MAC OS Versions.....63
- User Experience.....63

Supported MAC OS Versions

Cloudpath supports Mac OS X version 10.11 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

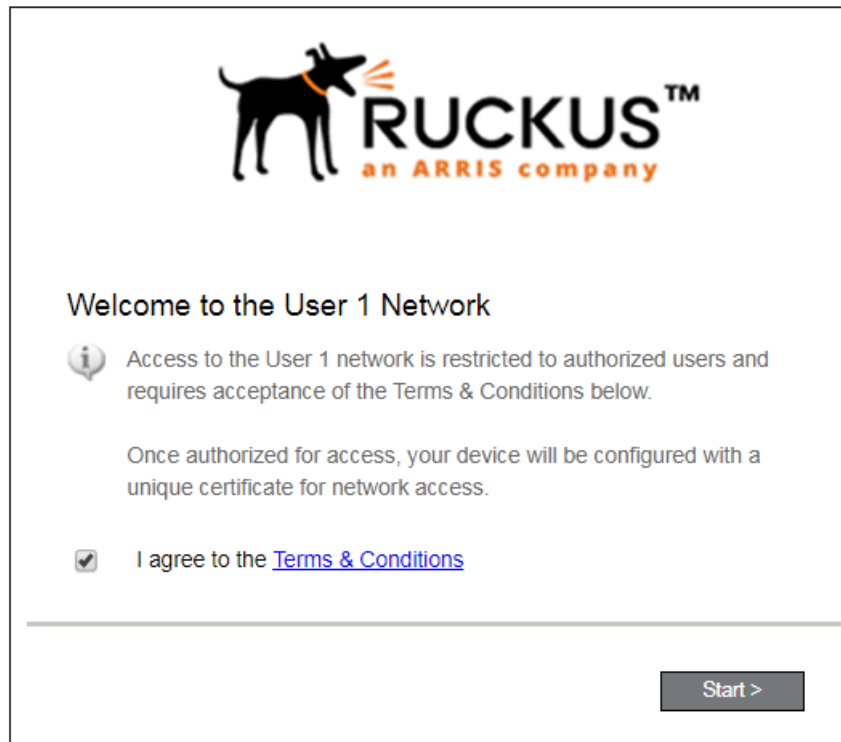
When the user enters the enrollment URL on their device, the Login (or Welcome) screen displays.

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 49 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 50 User Type Prompt

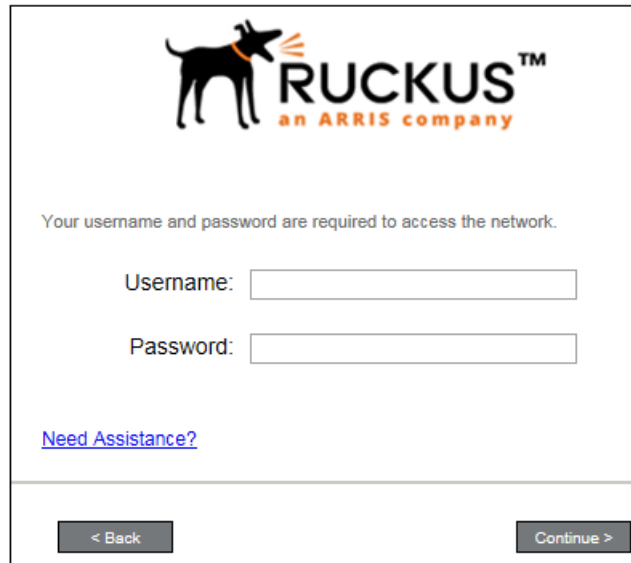



Select the user type to continue. This example follows the *Employee* workflow branch.

User Credentials

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

FIGURE 51 User Credential Prompt





Your username and password are required to access the network.

Username:

Password:

[Need Assistance?](#)

< Back Continue >

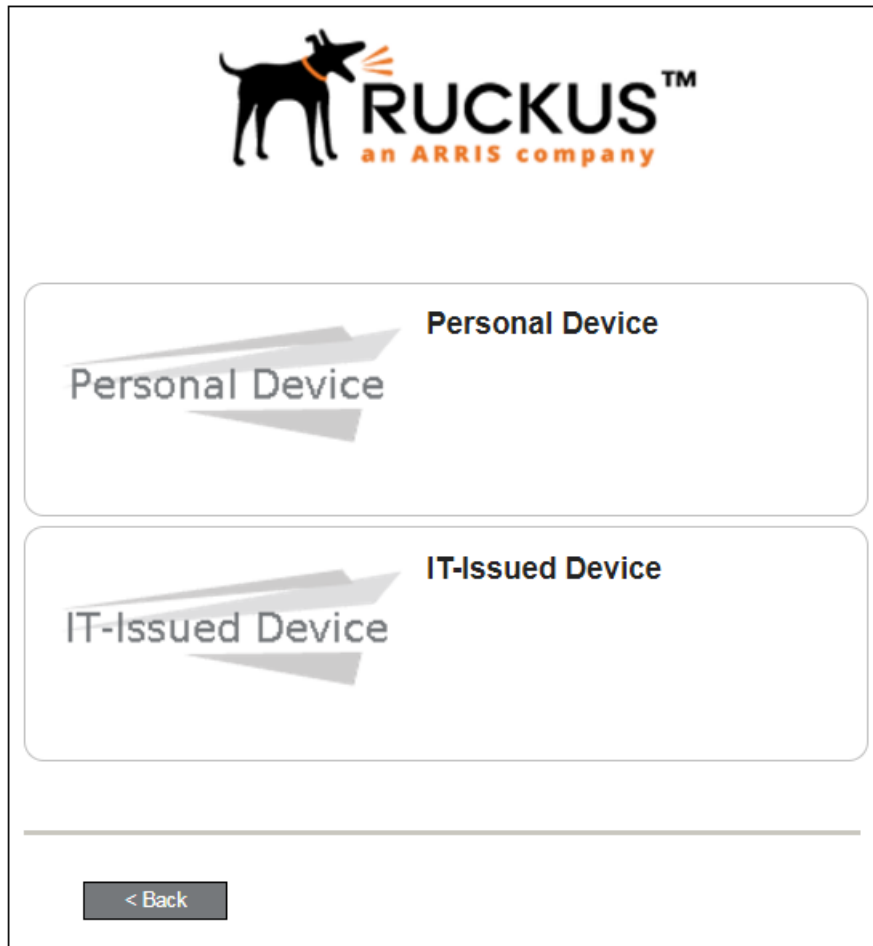
Enter the user credentials and click **Continue**.

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 52 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 53 Voucher Code Prompt



Enter the voucher that you received.

Voucher:

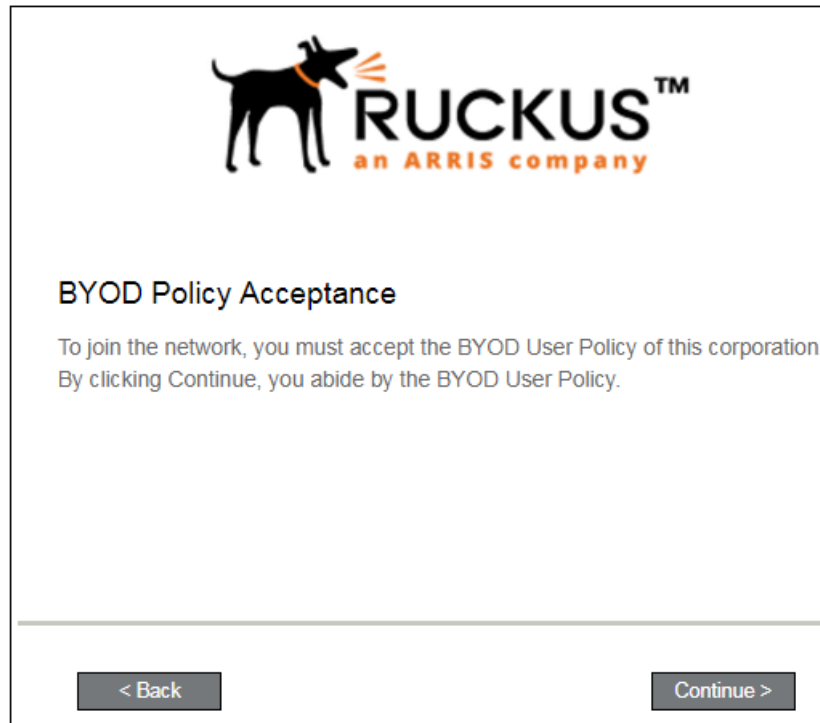
< Back Continue >

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 54 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.

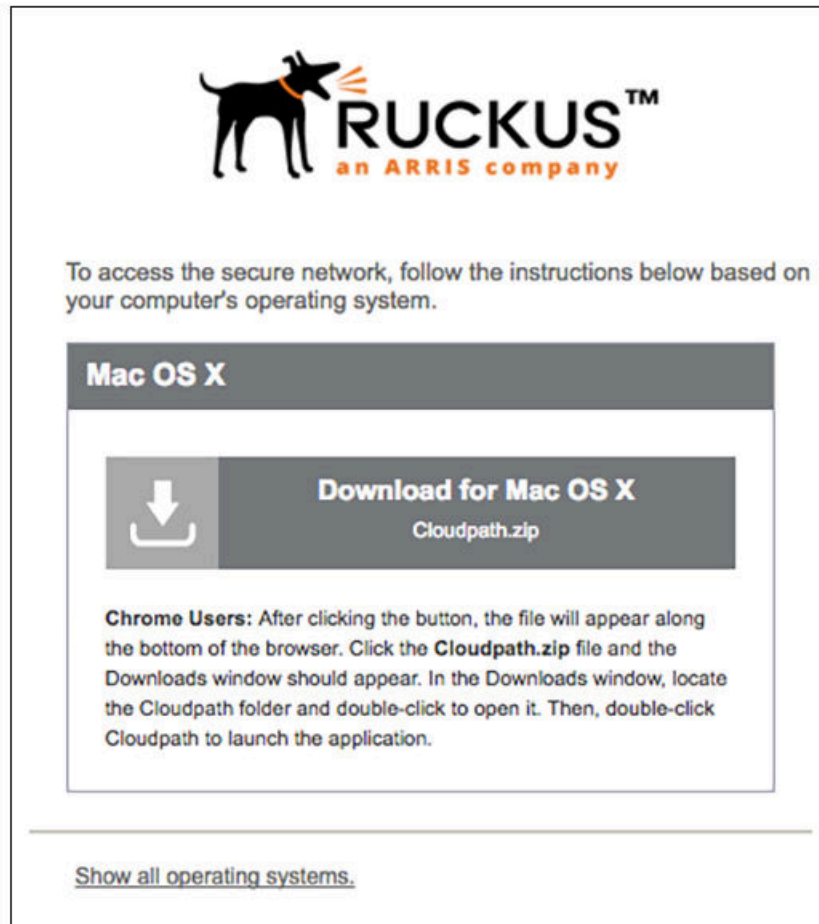
Download and Run Application

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 55 Mac OS X Download Page

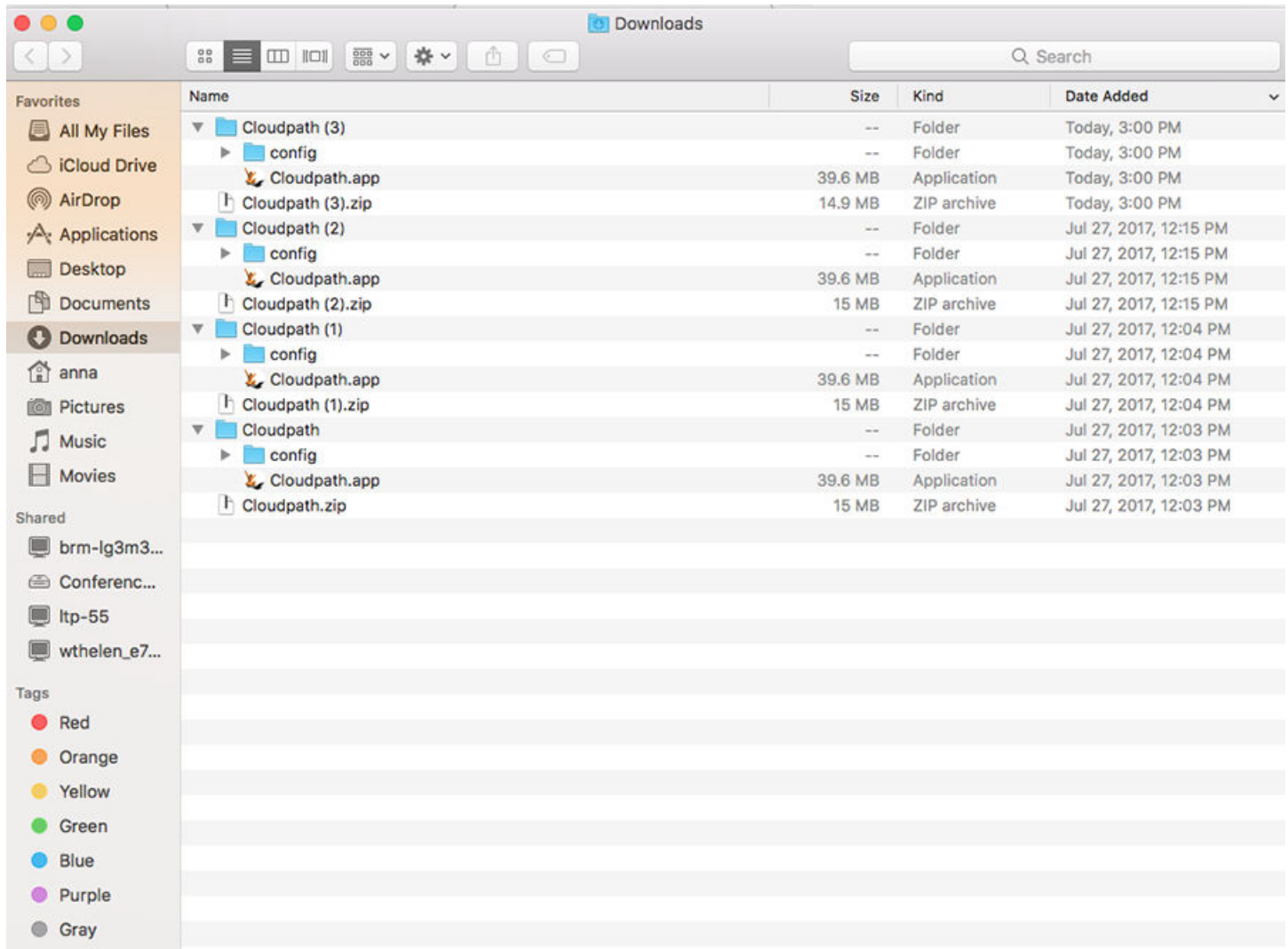


Click the **down arrow** to download the zip file, which contains the application files.

Open Downloaded Files

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

FIGURE 56 Open Download File

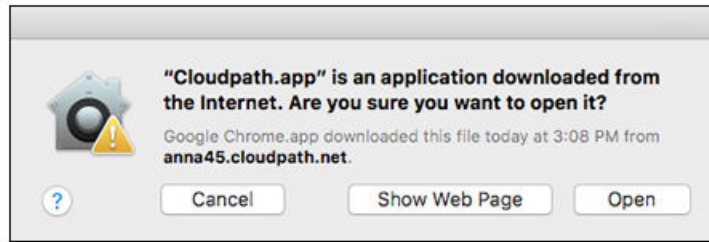


Double-click the Cloudpath application to start the Wizard, which runs through the configuration and migration process.

Confirm Open File

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

FIGURE 57 Confirm Open File



Click **Open** to continue.

Wizard Application User Experience

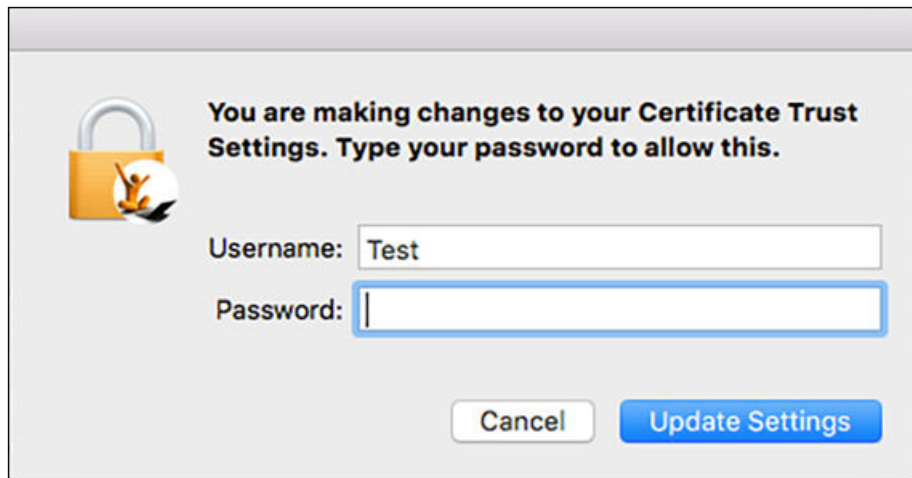
After the user has gone through the enrollment prompts, the Wizard runs to configure the wireless network settings on the device.

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

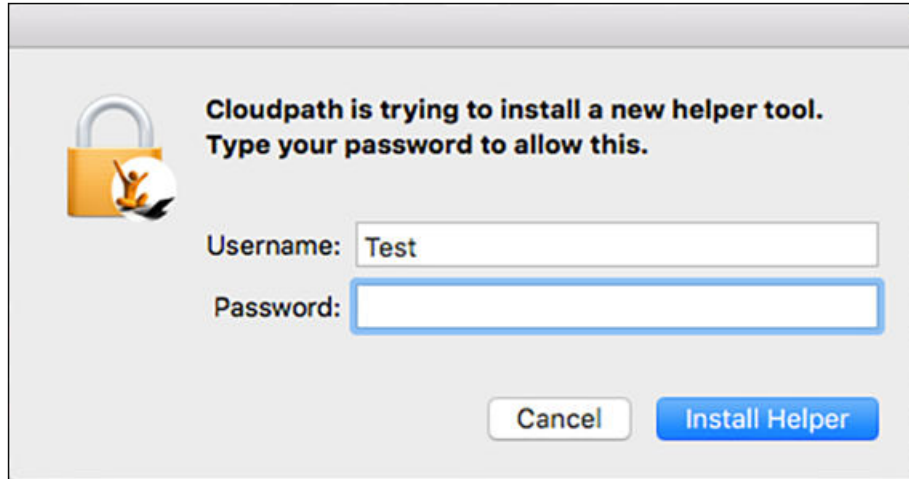
FIGURE 58 Enter Credentials for Certificate Trust Settings



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

Helper tool

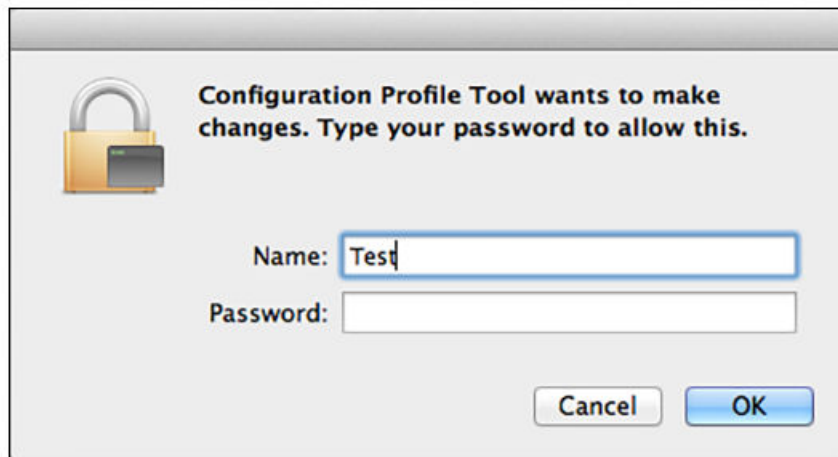
FIGURE 59 Enter Credentials for Helper Tool



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

Configuration Profile Tool

FIGURE 60 Enter Credentials for Configuration Profile Tool

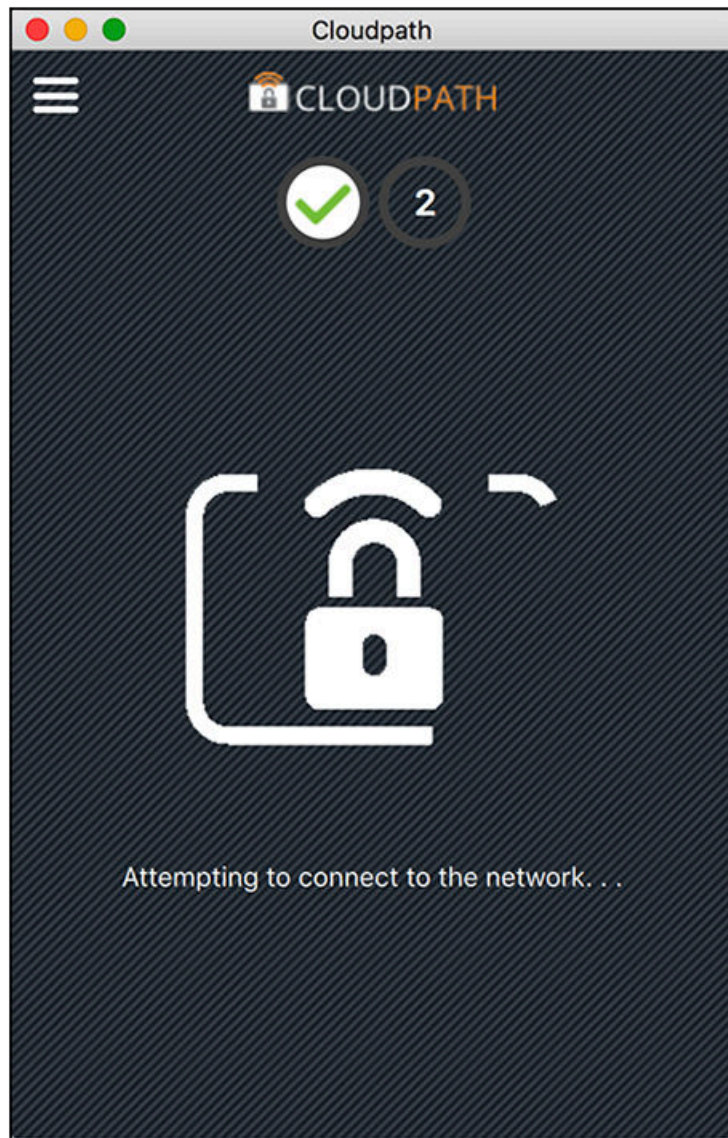


Enter the password and click **OK**. The application continues.

Attempting to Connect to Secure Network

The application attempts to associate to the wireless network.

FIGURE 61 Attempting to Connect to Secure Network

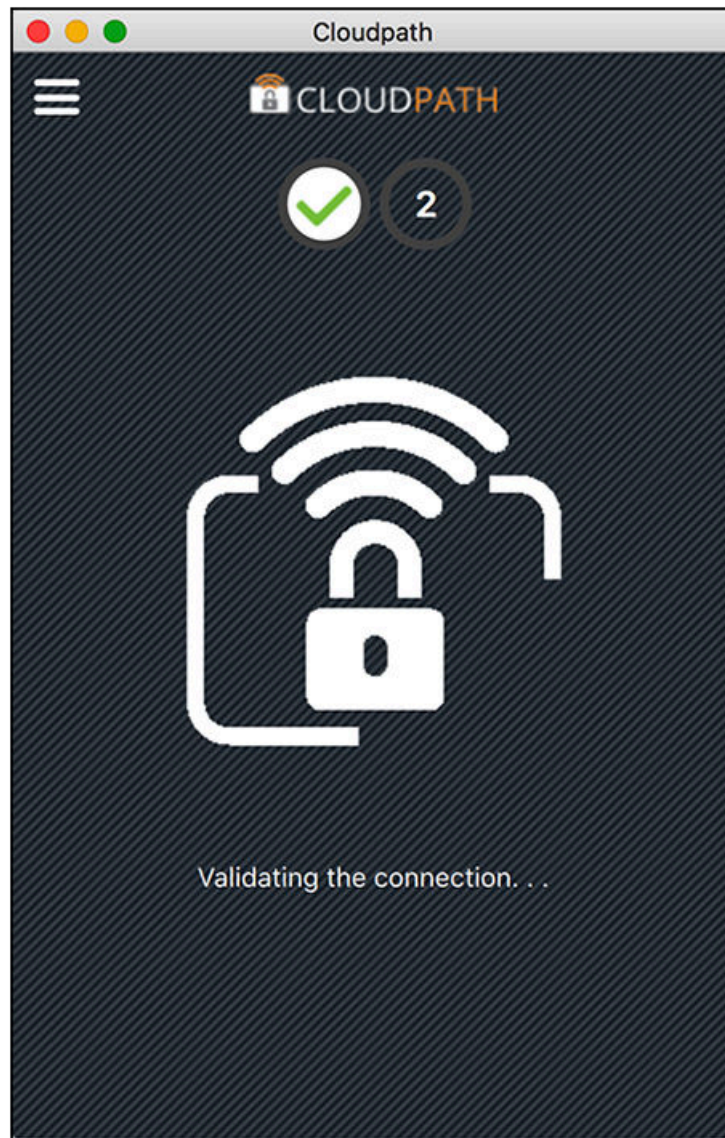


The application continues with the validation process.

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 62 Validating Connectivity

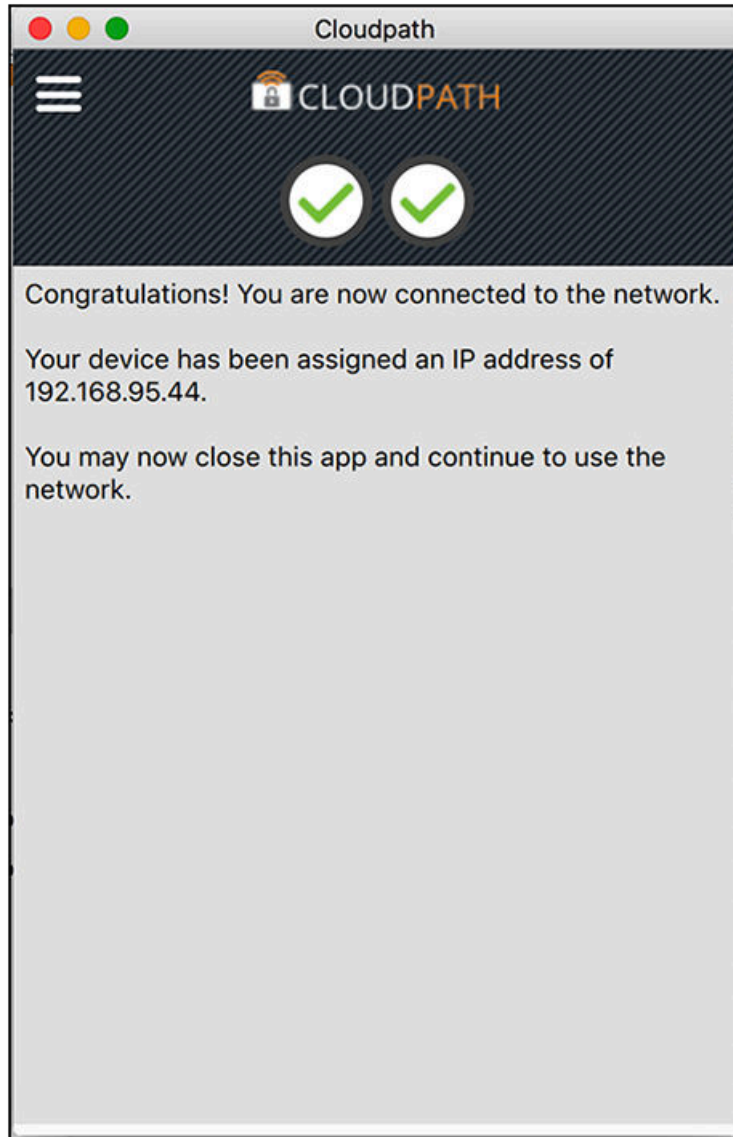


The application continues with the connection process.

Connected to Secure Network

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

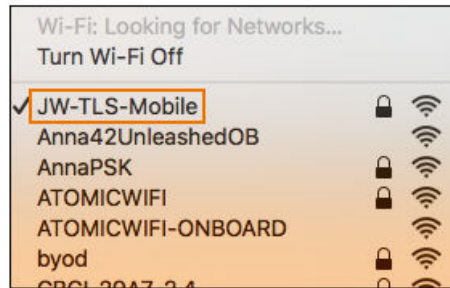
FIGURE 63 Connected to Secure Network



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 64 Secure Network



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

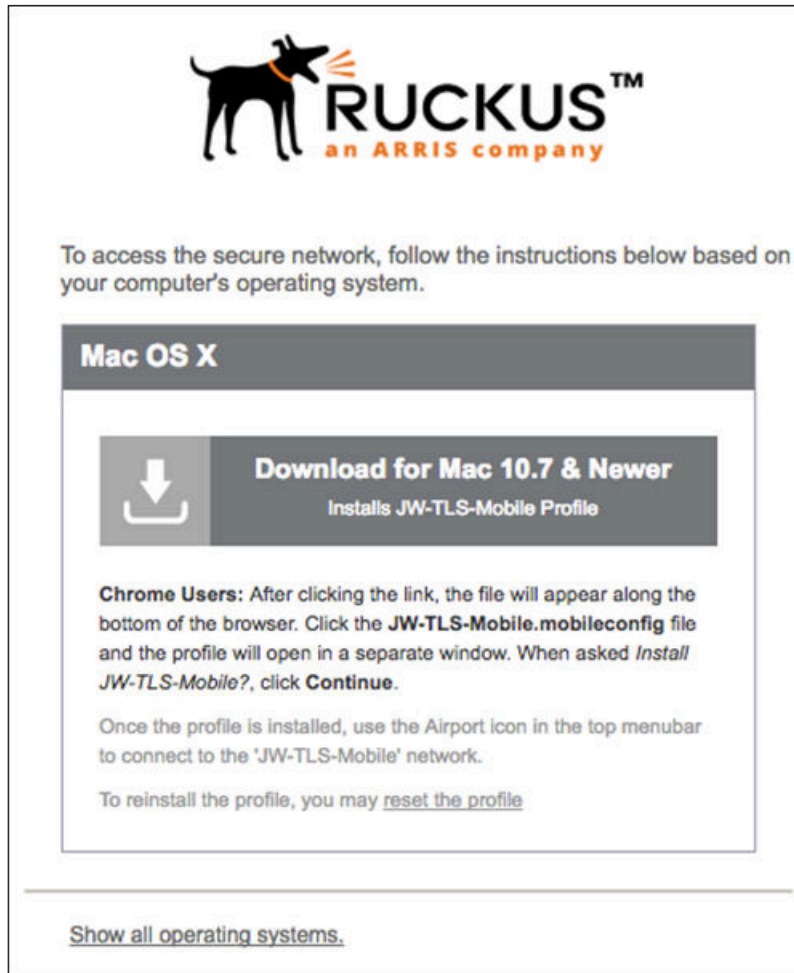
Install Network Profile to Configure Wi-Fi

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 65 Download Profile Page

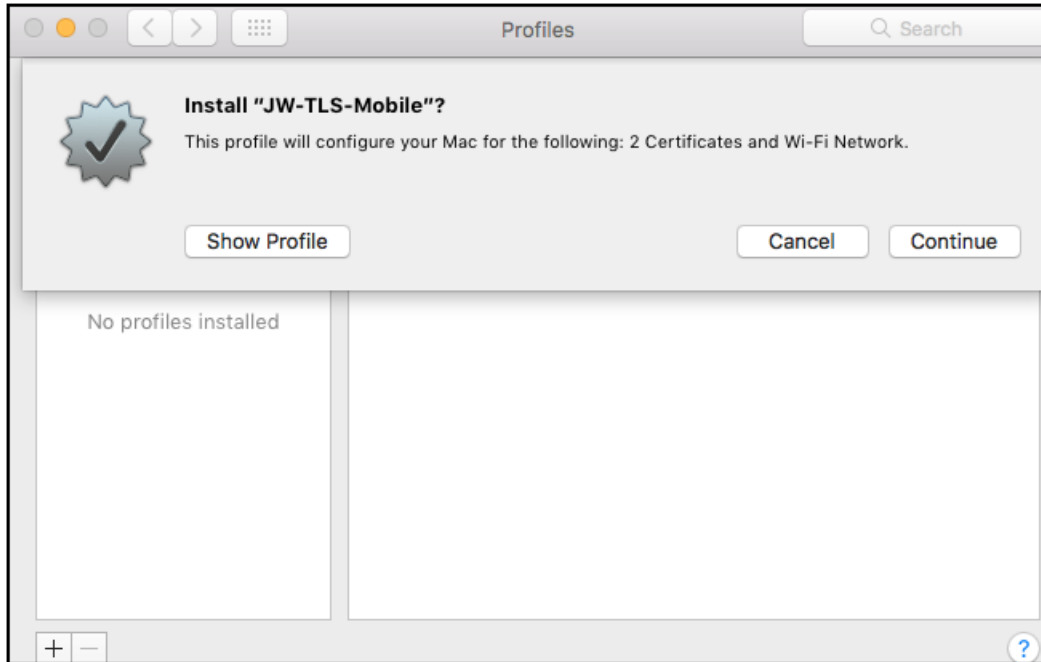


Click the **down arrow** to download the profile. If a profile has been previously installed, use the **Reset the Profile** link.

Install Profile

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

FIGURE 66 Install Profile

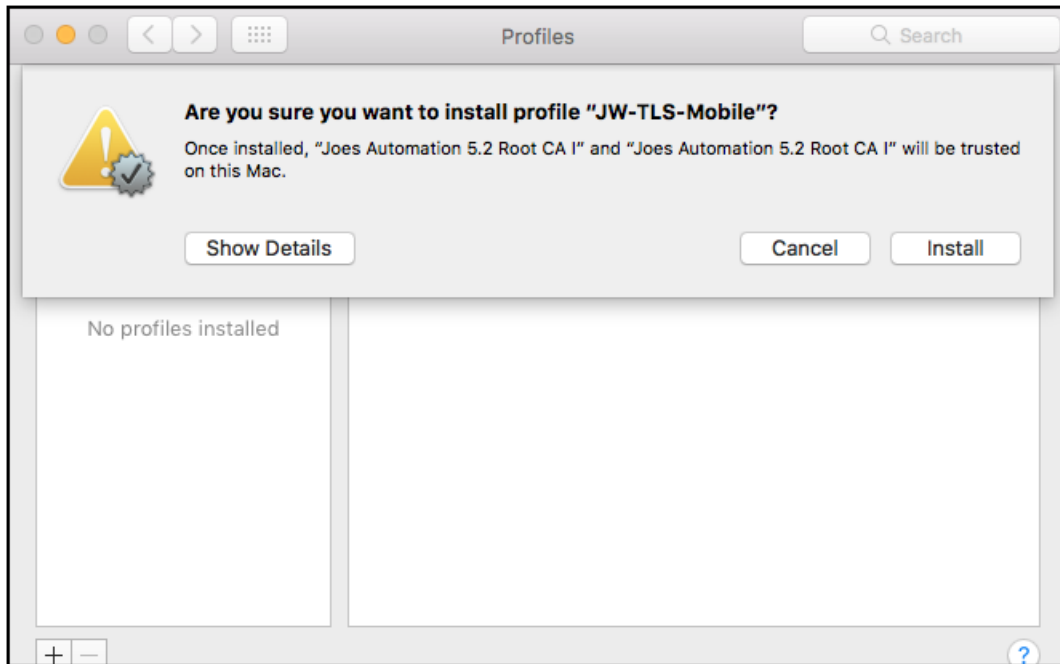


Click **Show Profile** to view profile details. Click **Continue** (or Install) to install the network profile.
Continue with profile installation.

Install Profile Confirmation

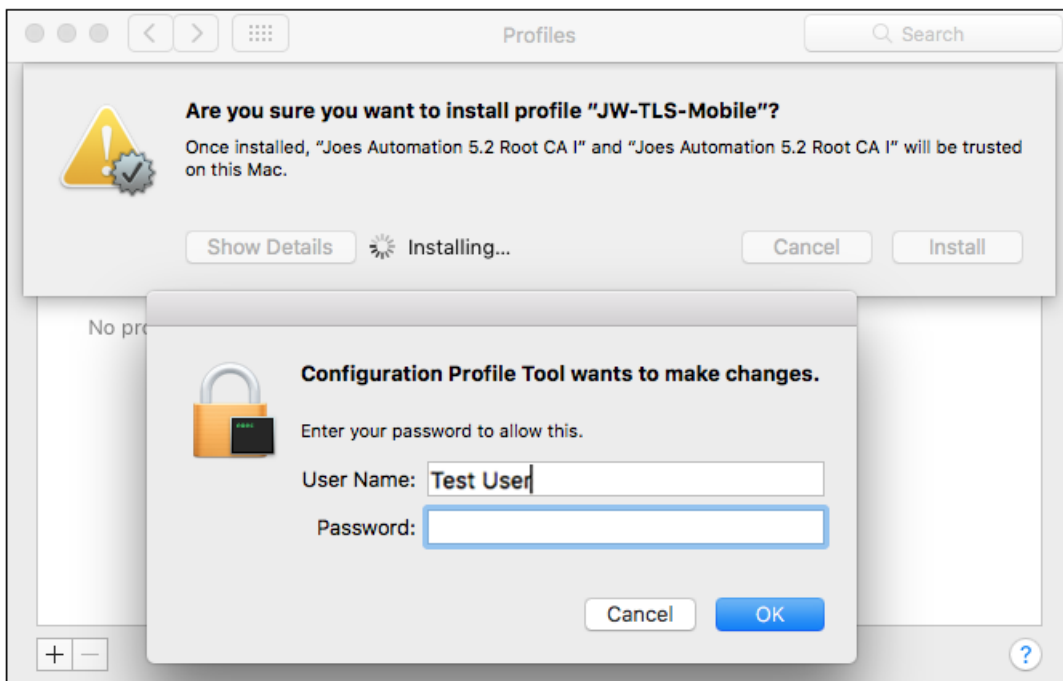
You are prompted to confirm that you want to install the network profile on the device.

FIGURE 67 Install Profile Confirmation Prompt



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

FIGURE 68 Enter Credentials for Configuration Profile Tool

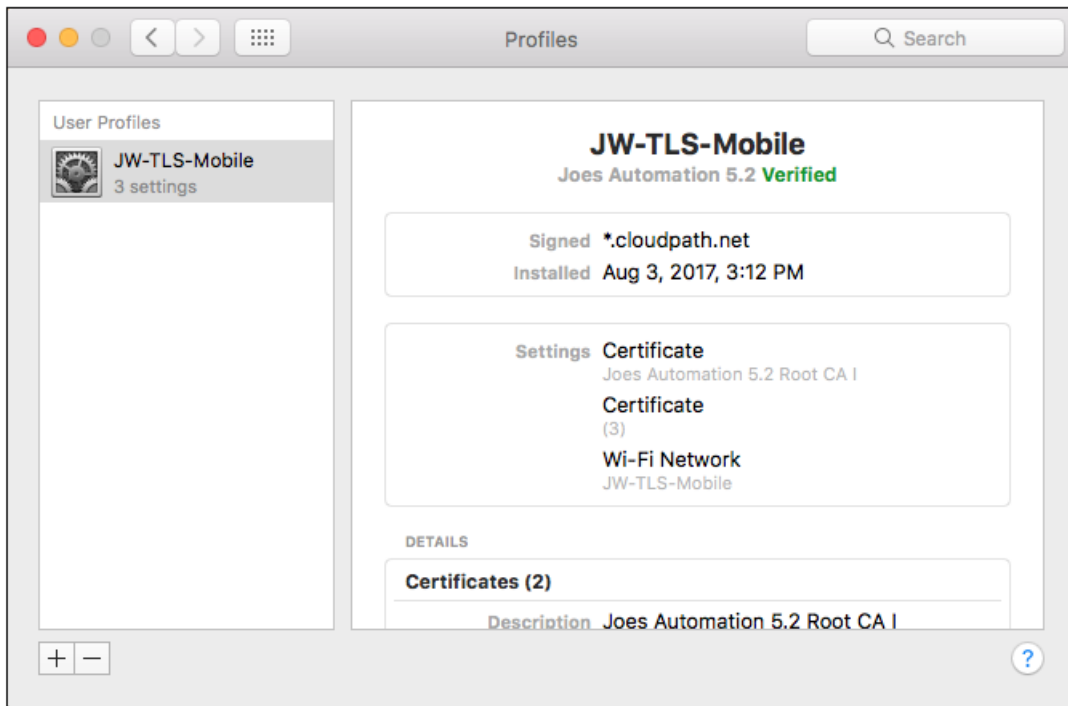


Enter the password and click **OK**.

Profile installed

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

FIGURE 69 Profile Installed

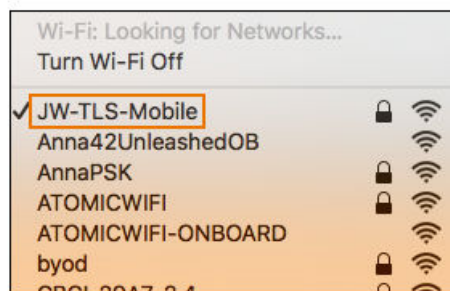


Close this page and proceed with connecting to the wireless network.

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 70 Secure Network



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

End-User Experience for Linux Devices

- Supported Linux Versions..... 83
- Cloudpath User Experience..... 83
- Wizard Application User Experience..... 92

Supported Linux Versions

Cloudpath supports the following Linux versions with automated configuration:

- Ubuntu version 15.04 and later
- Fedora version 22 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

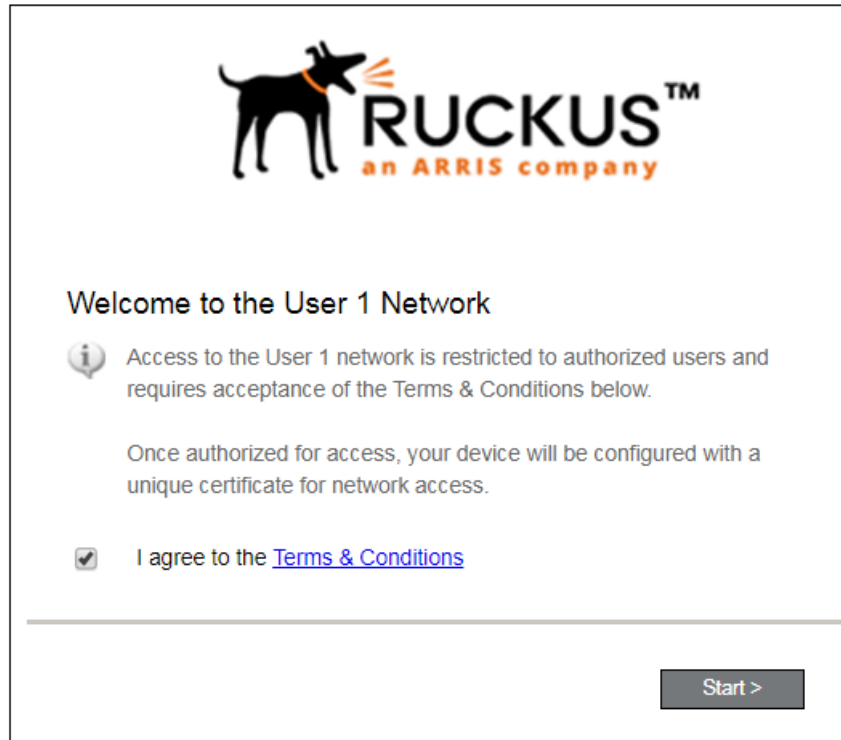
When the user enters the enrollment URL on their device, the Login (or Welcome) screen displays.

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 the Cloudpath Welcome page to start the enrollment process.

FIGURE 71 Welcome Screen



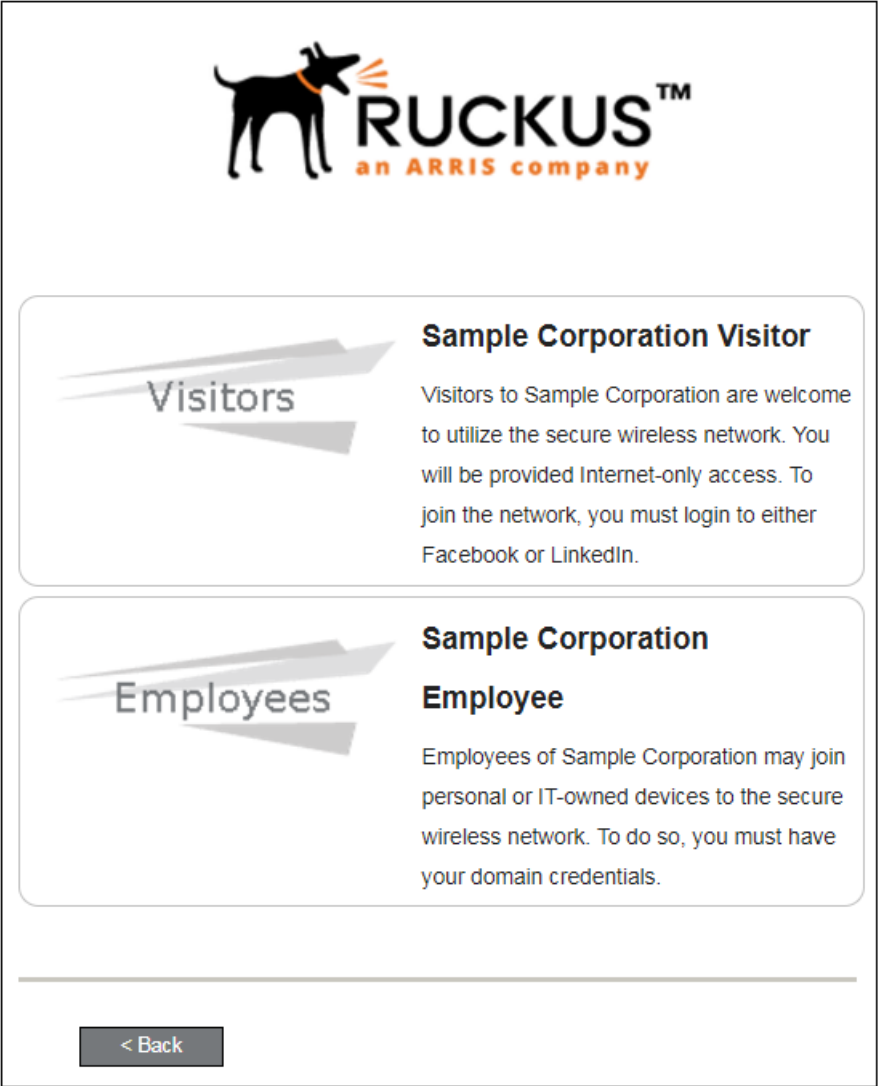
An acceptable use policy (AUP) prompt displays a message and requires that the user signal acceptance to continue. The welcome text and Start button can be customized.

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 72 User Type Prompt

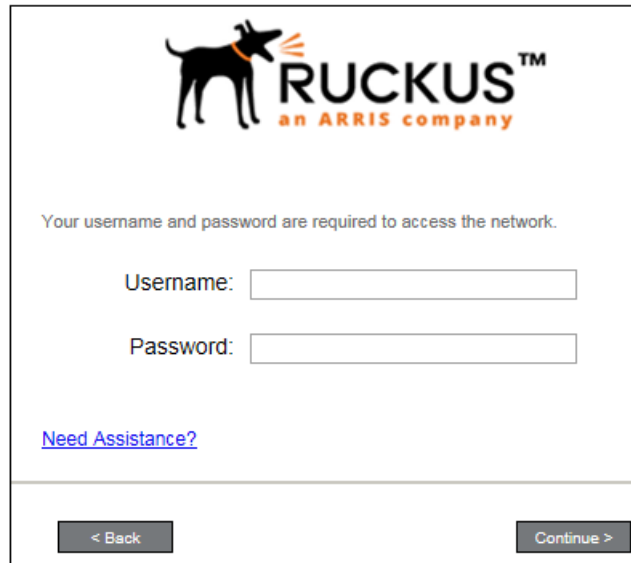



Select the user type to continue. This example follows the *Employee* workflow branch.

User Credentials

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

FIGURE 73 User Credential Prompt





Your username and password are required to access the network.

Username:

Password:

[Need Assistance?](#)

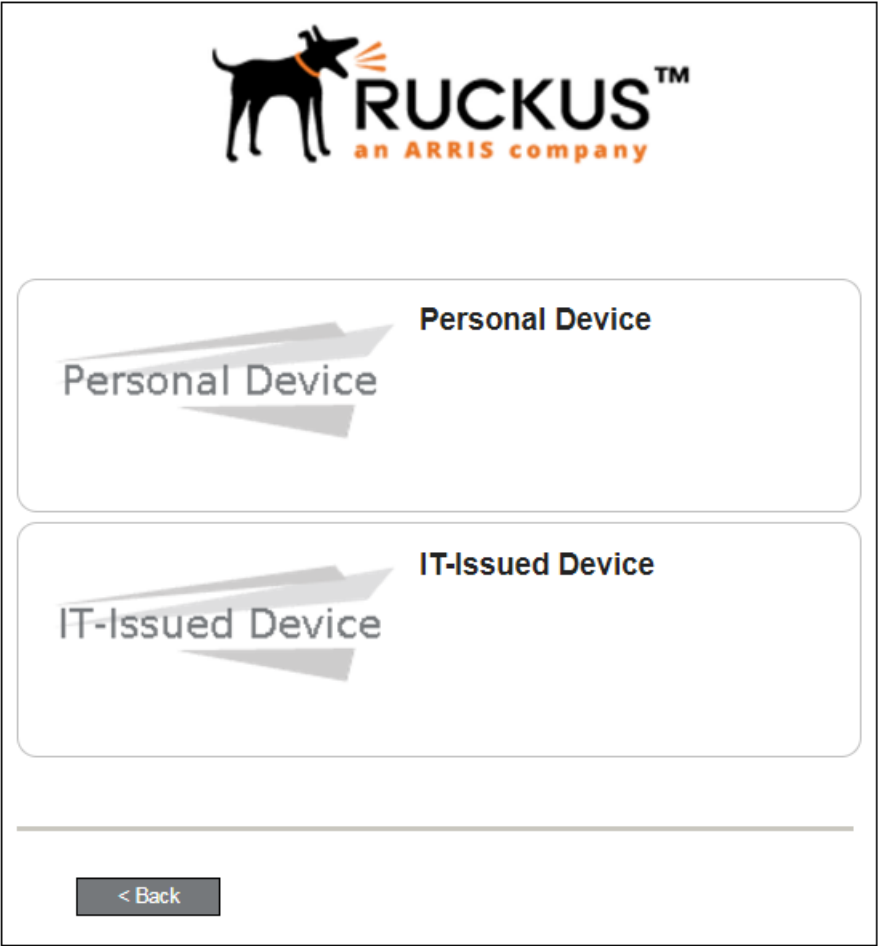
Enter the user credentials and click **Continue**.

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 74 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 75 Voucher Code Prompt



Enter the voucher that you received.

Voucher:

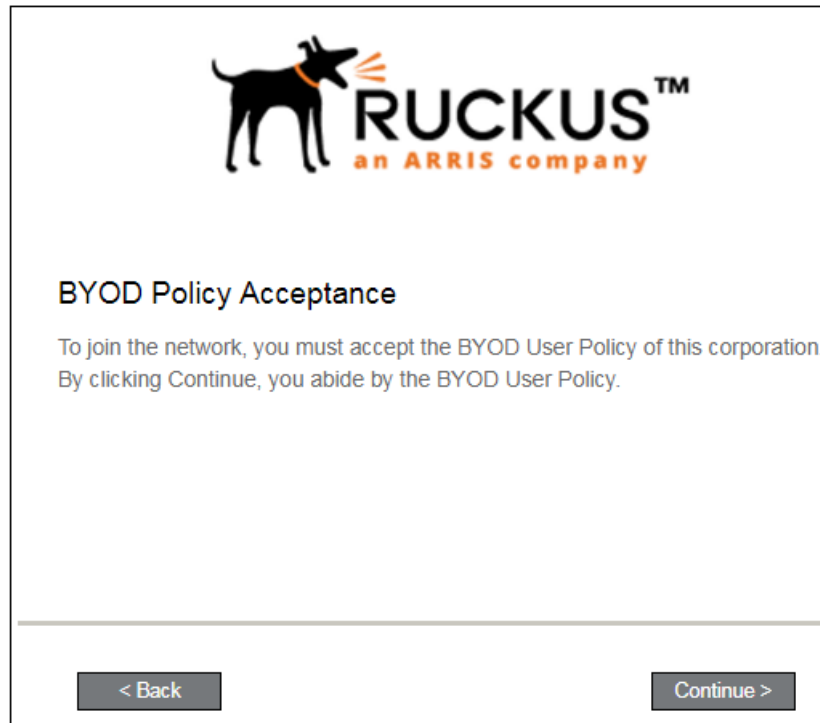
< Back Continue >

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 76 BYOD Policy



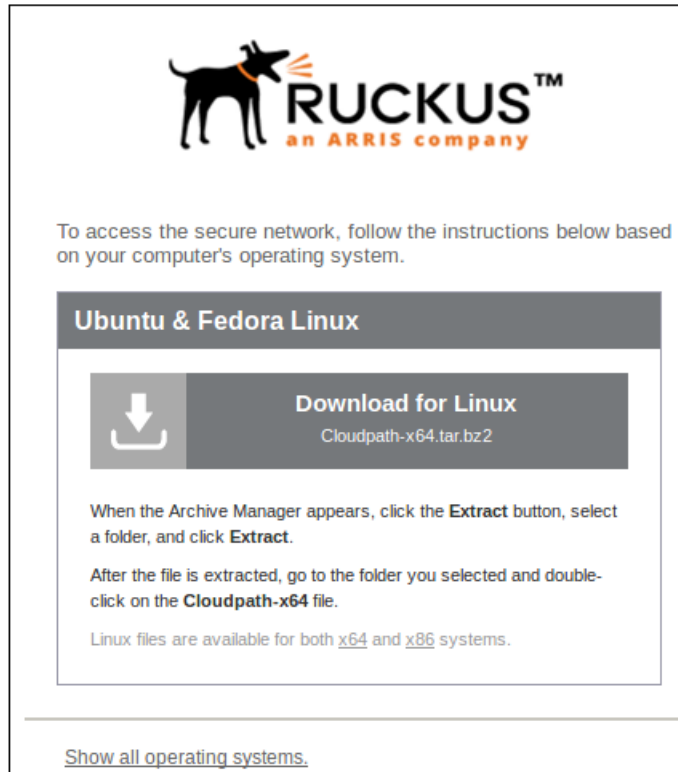
Click **Start** to continue.

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

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 77 Linux Download Page

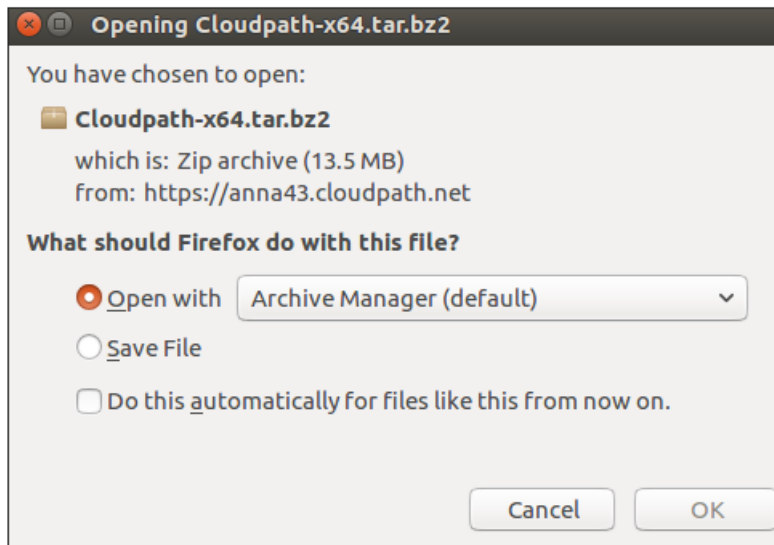


Click the **down arrow** to download the tar file, which contains the application files.

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 78 Open Download File

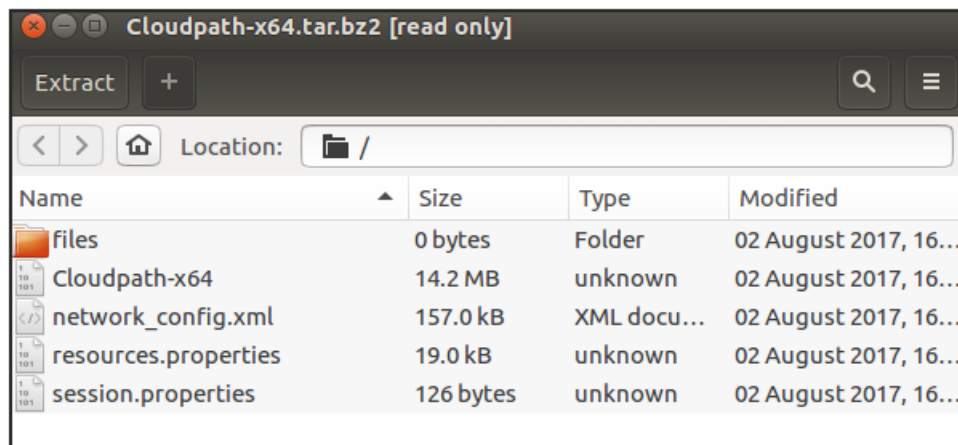


Click **OK** to continue.

Extract Downloaded Files

Extract the application files that were downloaded.

FIGURE 79 Select Files to be Extracted



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

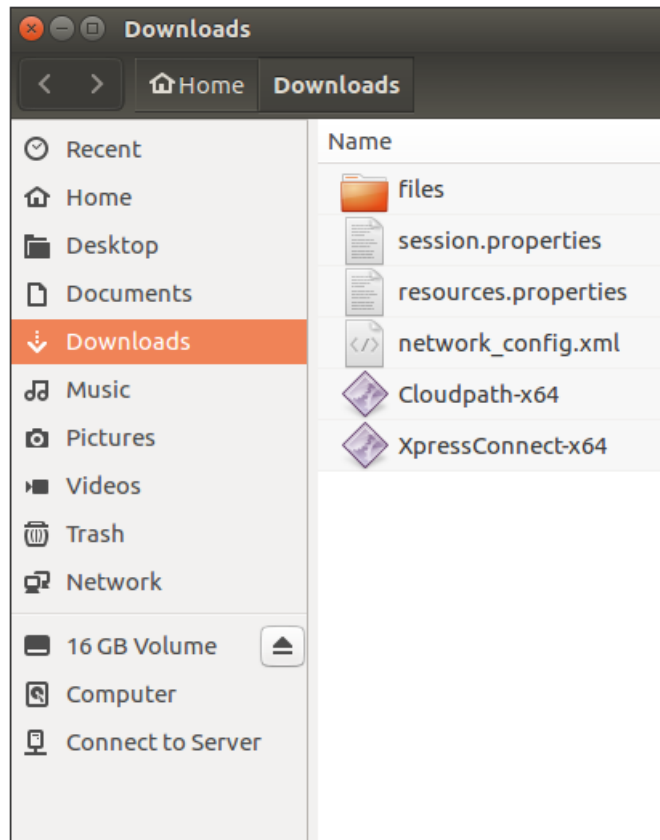
Open Application File

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 80 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. A screen may appear to indicate that the device is being configured.

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

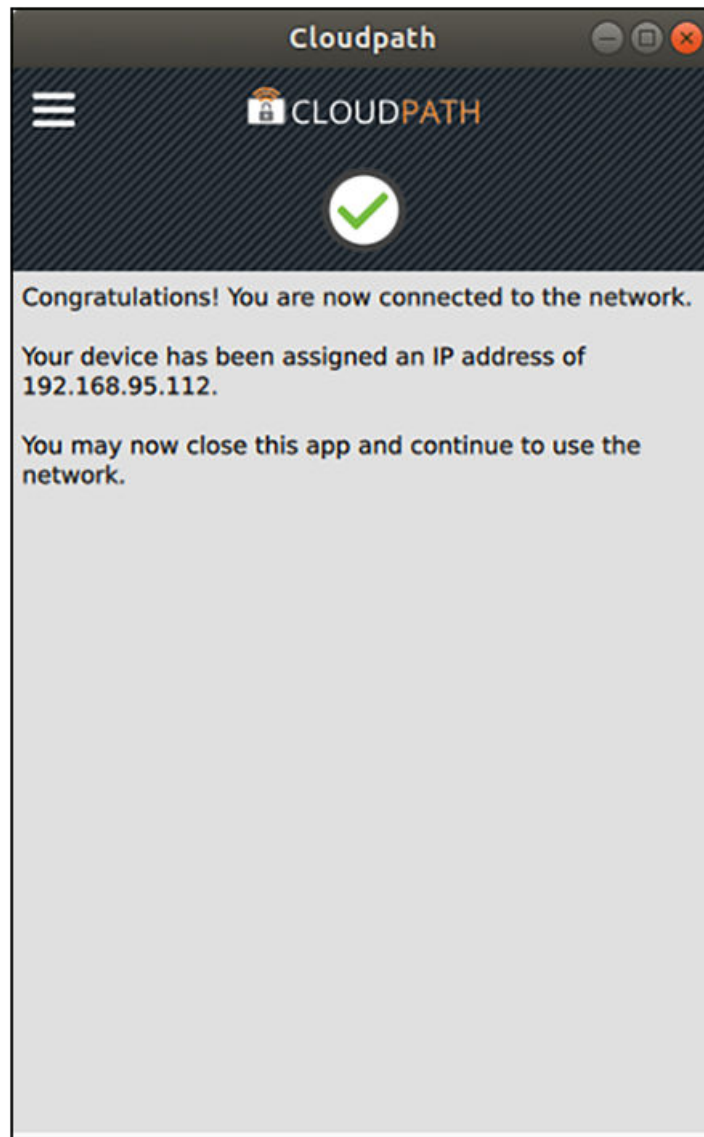
When the association with the secure network is successful, the application attempts to acquire a network address. A screen may briefly appear to indicate that connectivity is being validated.

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.

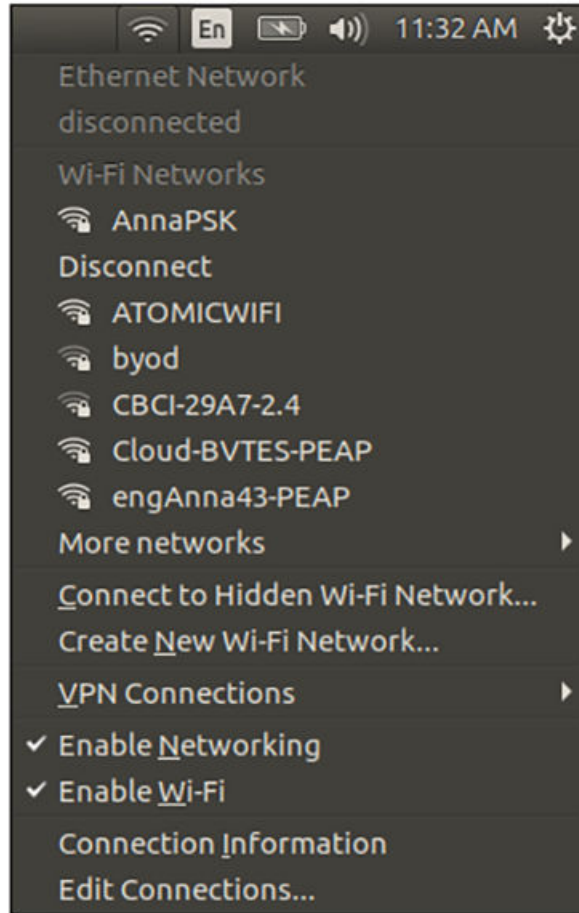
FIGURE 81 Connected to Secure Network



View Network Connection

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

FIGURE 82 View Wireless Network



The Wi-Fi setting displays the secure network.

End-User Experience for Blackberry Devices

- Supported BlackBerry Versions..... 95
- Cloudpath User Experience..... 95

Supported BlackBerry Versions

Cloudpath supports BlackBerry Smartphones equipped with Wi-Fi radios that support 802.1X.

NOTE

Your network may not support all versions of BlackBerry. Contact your network help desk to verify the supported BlackBerry versions.

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 Steps

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

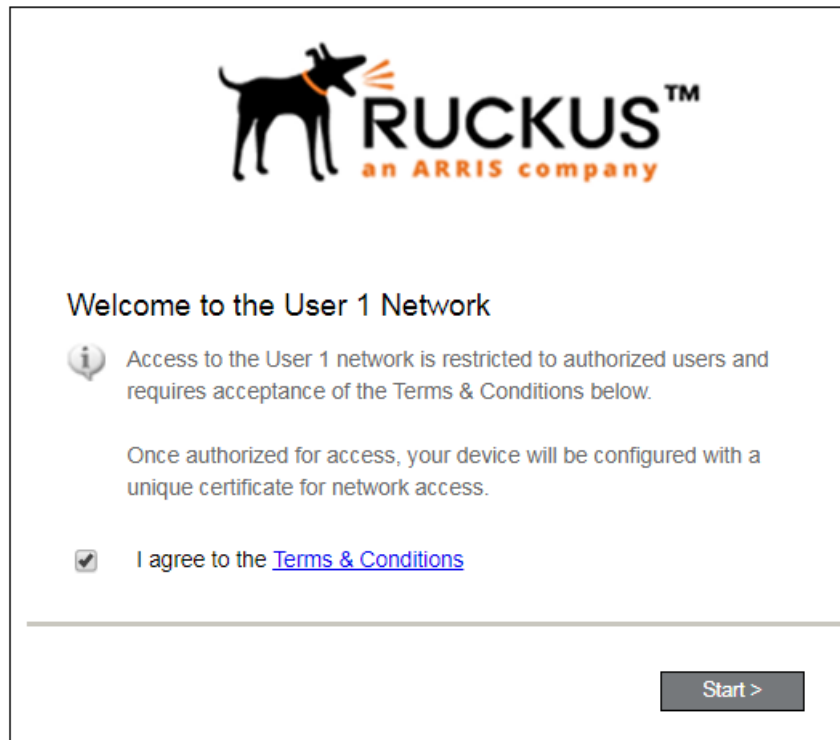
Welcome Screen With AUP

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 83 Enrollment Welcome Screen



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

Welcome Screen With AUP

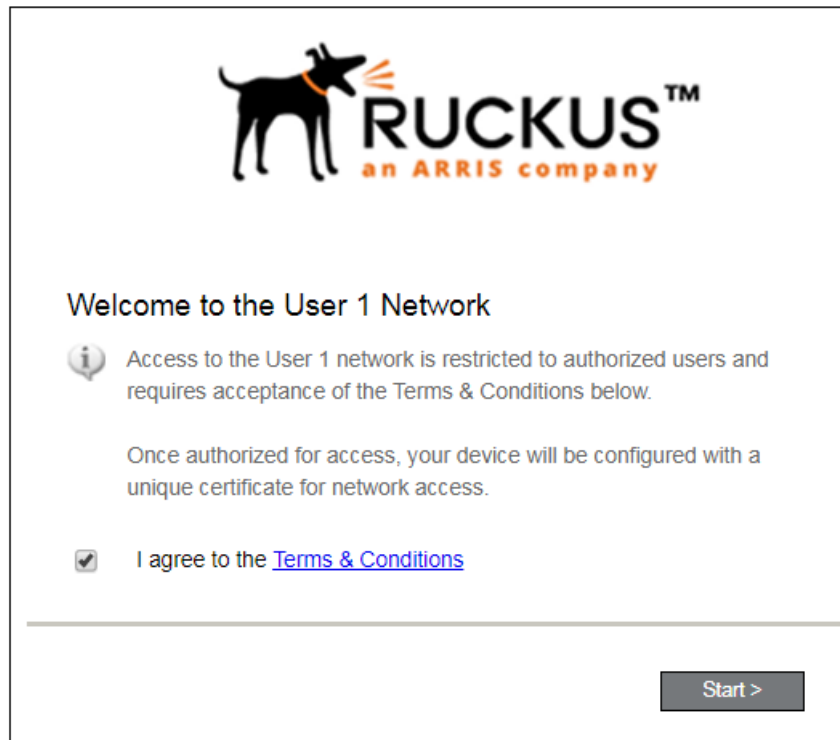
When the user enters the enrollment URL on their device, the Login (or Welcome) screen displays.

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 84 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 85 User Type Prompt

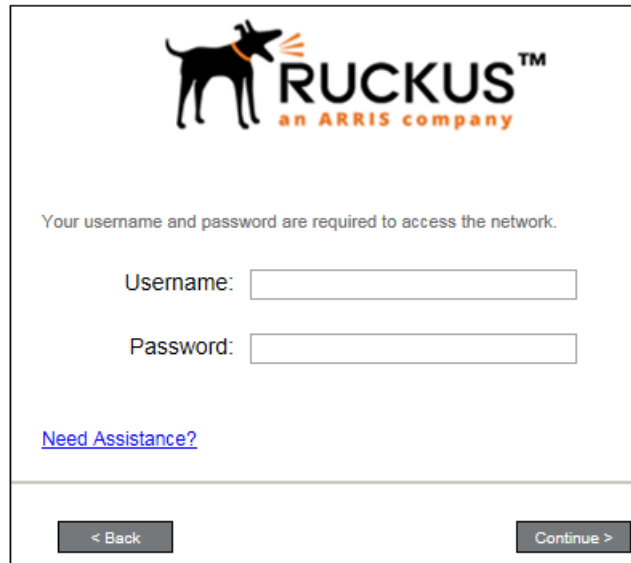


Select the user type to continue. This example follows the *Employee* workflow branch.

User Credentials

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

FIGURE 86 User Credential Prompt



RUCKUS™
an ARRIS company

Your username and password are required to access the network.

Username:

Password:

[Need Assistance?](#)

< Back Continue >

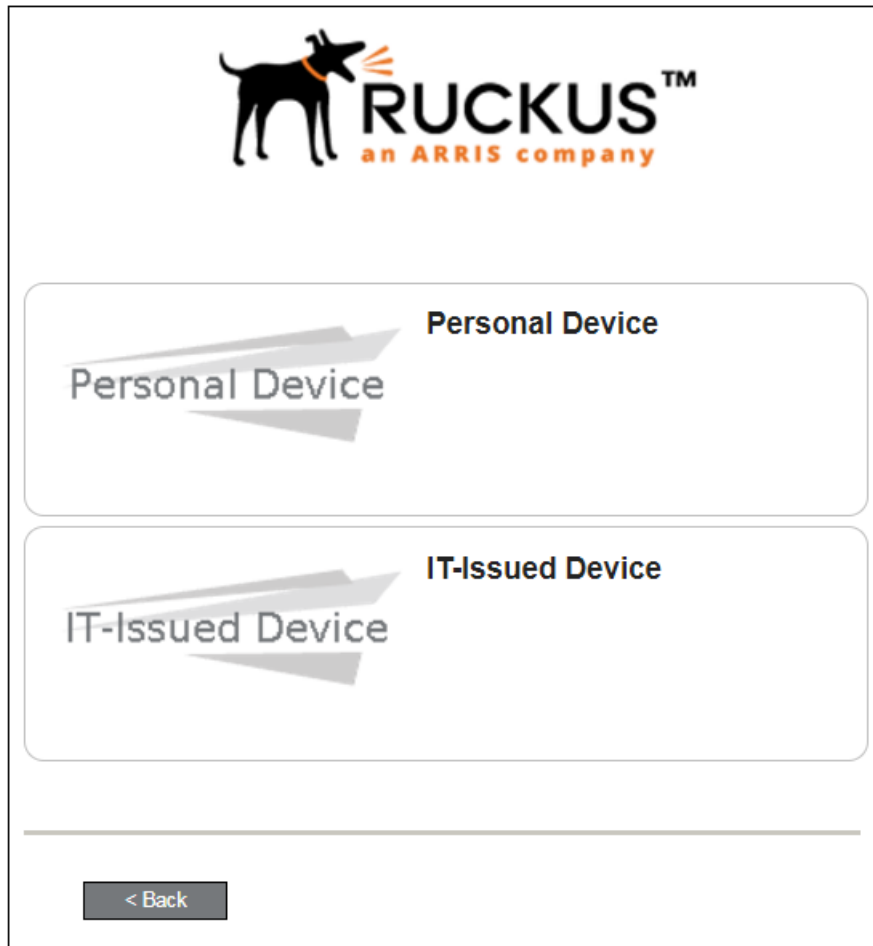
Enter the user credentials and click **Continue**.

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 87 Device Type Prompt

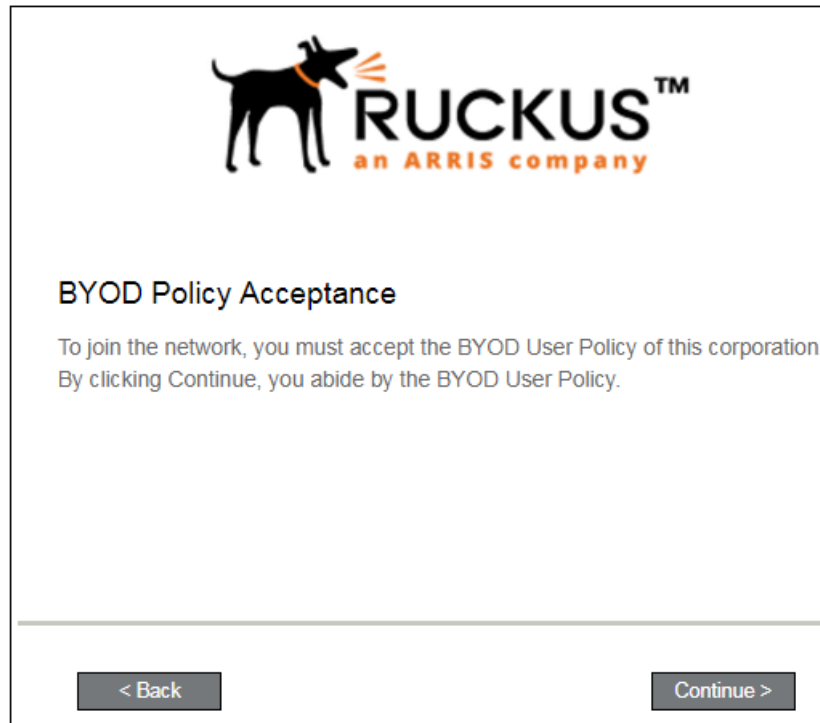


Select a device type to continue. This example follows the IT-Issued Device enrollment workflow.

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 88 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.

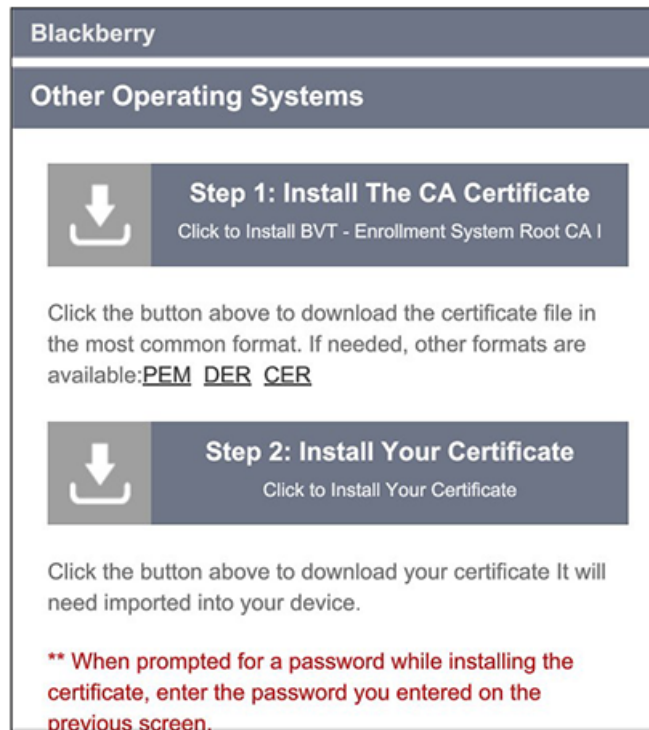
BlackBerry Configuration Instructions

The application detects the user agent for a BlackBerry device and provides the correct configuration instructions. BlackBerry instructions are displayed on the **Other Operating Systems** tab. This screen includes the steps required to install the certificates and to configure the device for the secure wireless network.

Install Certificates

For this sample configuration, Steps 1 and 2 provide instructions for downloading the CA certificate and user certificate.

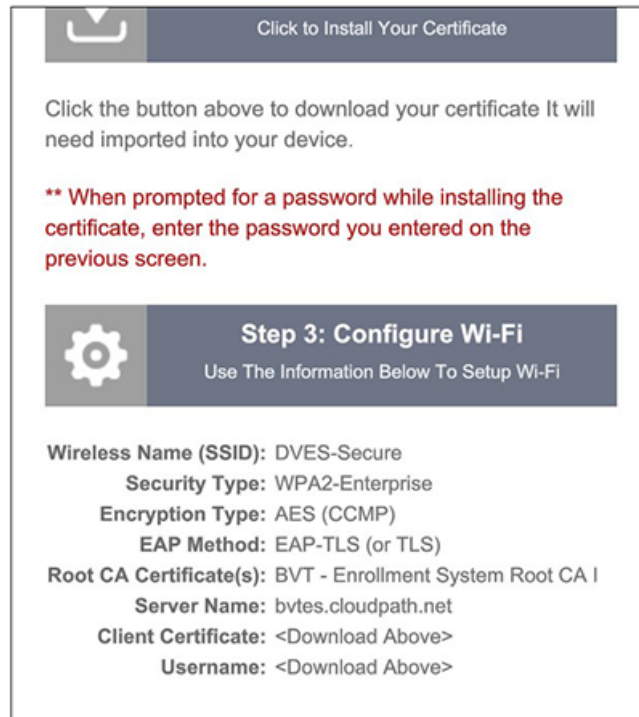
FIGURE 89 BlackBerry Instructions - Steps 1-2



Configure Wi-Fi Instructions

For this sample configuration, Step 3 provides the wireless network settings.

FIGURE 90 BlackBerry Instructions - Step 3



NOTE

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

Continue with the next sections to download and import the certificates.

Download Certificates

From the **Other Operating Systems** tab on the configuration instructions screen, tap the down arrow to download the certificates.

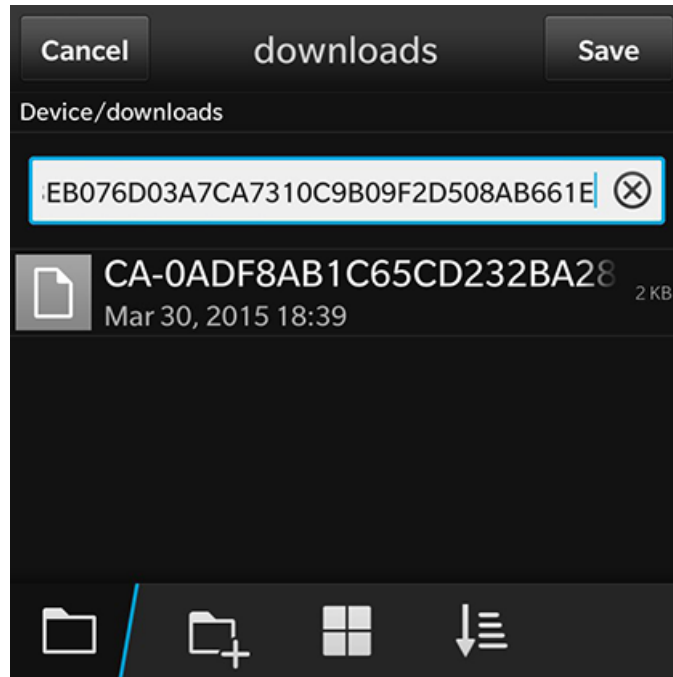
Download CA Certificates

Tap the down arrow next to **Step 1: Install The CA Certificate**. You are prompted to **Save** the certificate with the default name or enter a different name.

NOTE

If you rename the certificate, it is only renamed in the **Downloads** folder. The BlackBerry OS saves to the certificate store using the default certificate name.

FIGURE 91 Save CA Certificate

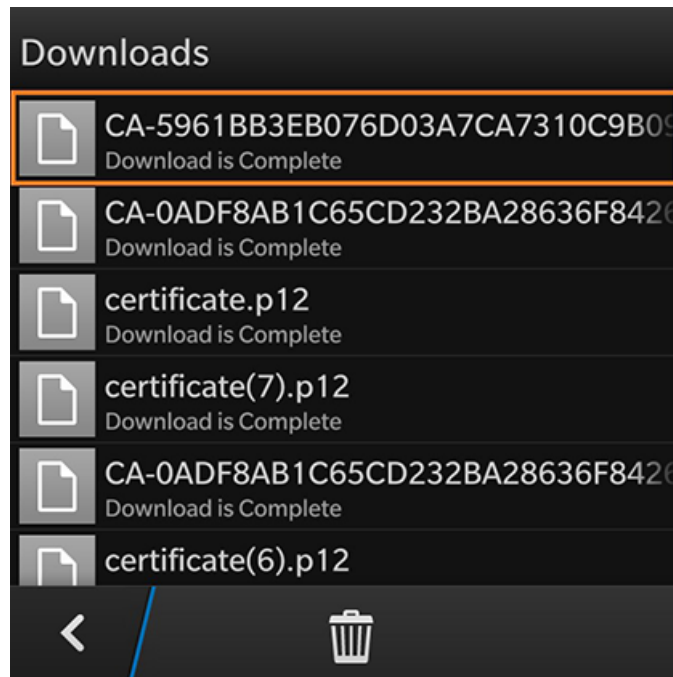


Tap **Save** to download the certificate. The screen displays a brief message to confirm that the download was complete.

CA Certificate in Downloads Folder

The certificate is listed in the **Downloads** folder.

FIGURE 92 CA Certificate



Tap the back arrow at the bottom left to return to the configuration instructions screen.

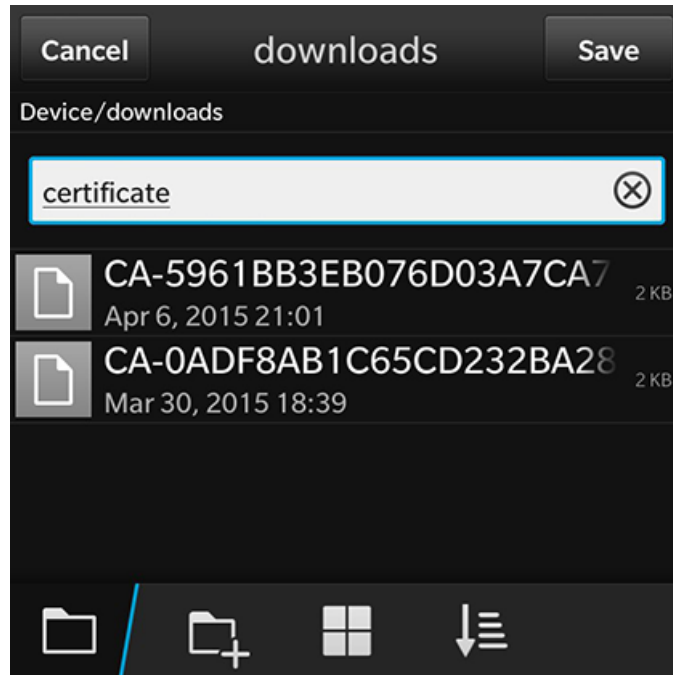
Download User Certificate

Tap the down arrow next to **Step 2: Install Your Certificate**. You are prompted to **Save** the certificate with the default name or enter a different name.

NOTE

If you rename the certificate, it is only renamed in the **Downloads** folder. The BlackBerry OS saves to the certificate store using the default certificate name.

FIGURE 93 Save User Certificate

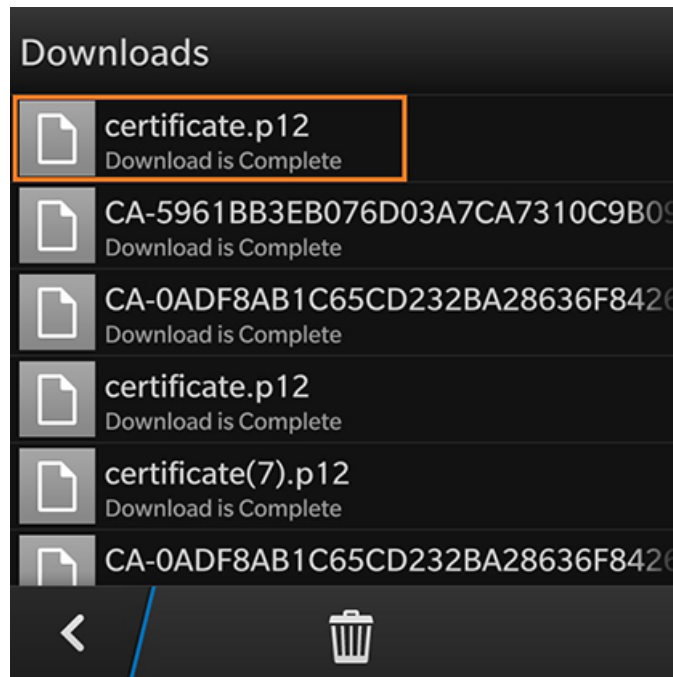


Tap **Save** to download the certificate. The screen displays a brief message to confirm that the download was complete.

User Certificate in Downloads Folder

The certificate is listed in the **Downloads** folder.

FIGURE 94 User Certificate

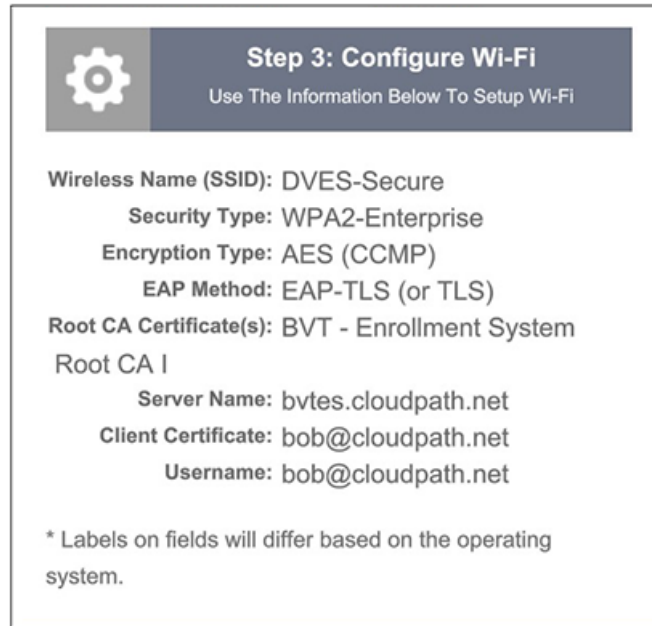


Tap the back arrow at the bottom left to return to the configuration instructions screen.

Configuration Instructions

After the certificates have been downloaded, you are returned to the configuration instructions screen.

FIGURE 95 Configuration Instructions



This final step contains all the information you need to configure the wireless settings on your device. Make note of the CA Certificate, Client Certificate, and Wireless Network Name before you continue.

The next step is to import the CA and user certificates to the certificate store.

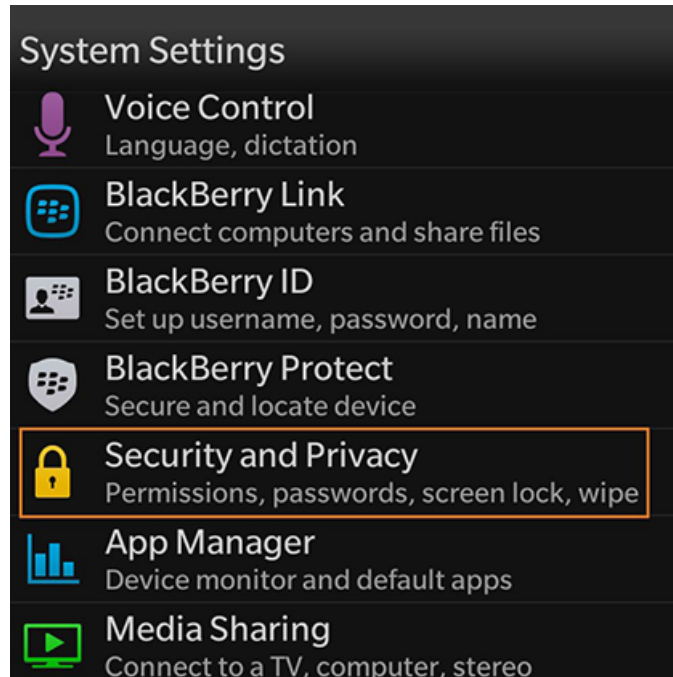
Import Certificates

After the certificates have been downloaded to the device, they must be imported to the certificate store

System Settings

Go to the **System Settings** for the device.

FIGURE 96 System Settings for Importing Certificates

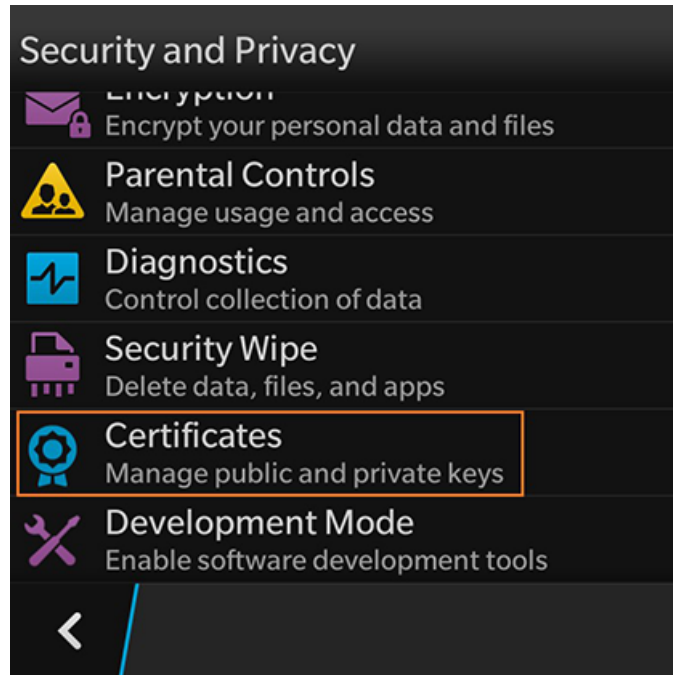


Tap **Security and Privacy** to continue.

Security and Privacy Settings

Certificate settings are listed under **Security and Privacy**.

FIGURE 97 Security and Privacy Settings

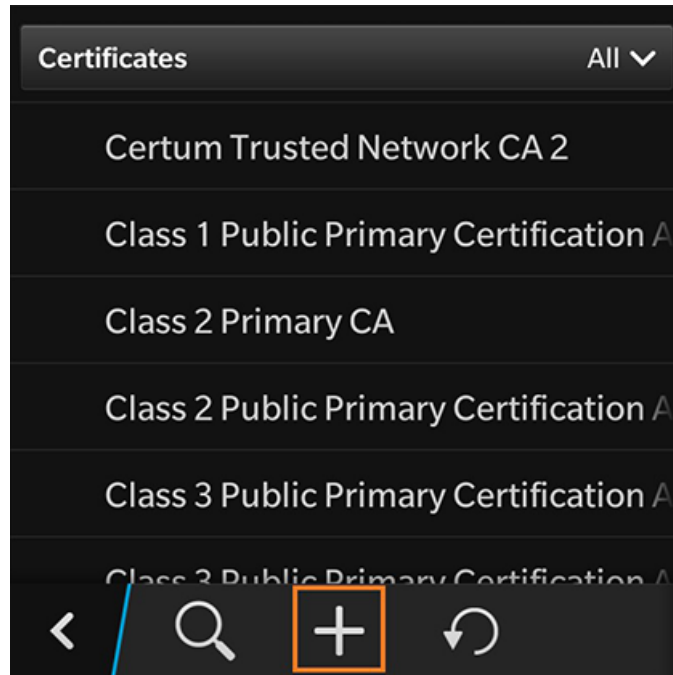


Tap **Certificates** to continue.

Add Certificate

The certificate store is displayed.

FIGURE 98 Add Certificate

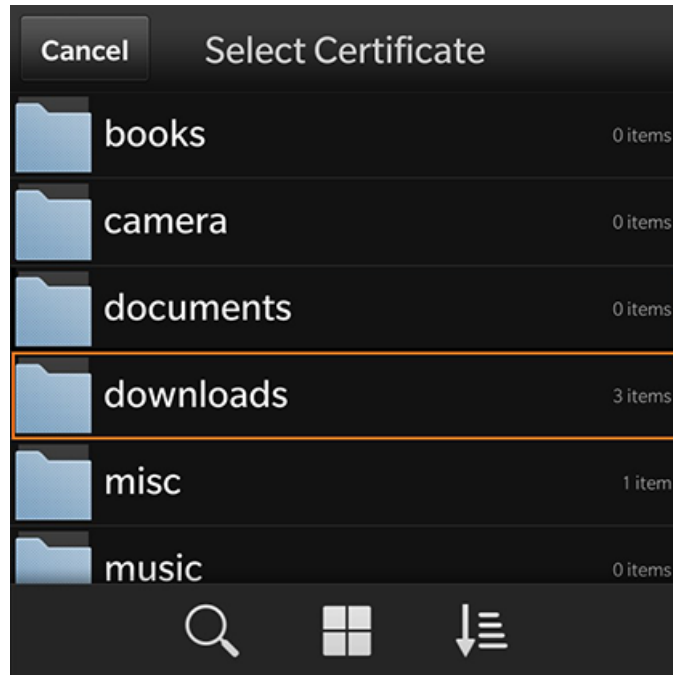


Click the plus sign to add a CA certificate.

Select Downloads Folder

On the **Select Certificates** screen, locate the **Downloads** folder.

FIGURE 99 Select Downloads Folder

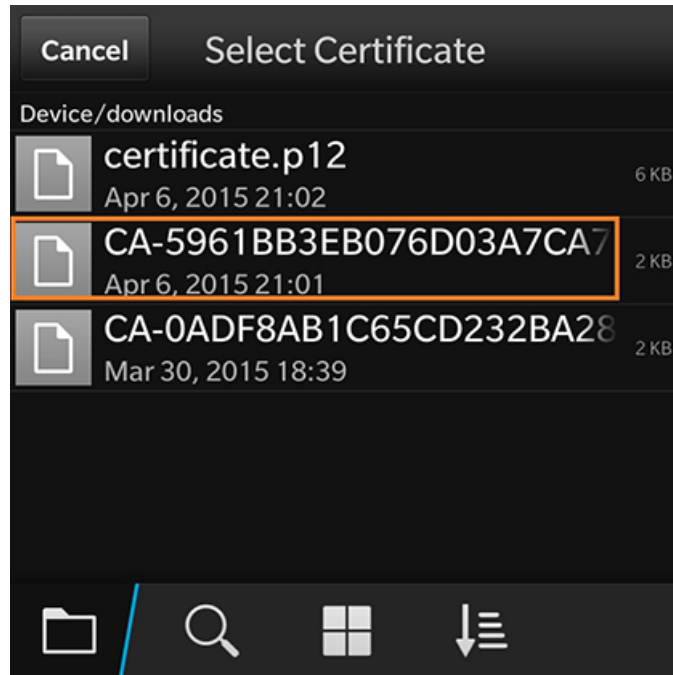


Tap the **Downloads** folder to view the certificates available for import.

Select CA Certificate

Select the CA certificate that was previously downloaded.

FIGURE 100 Select CA Certificate

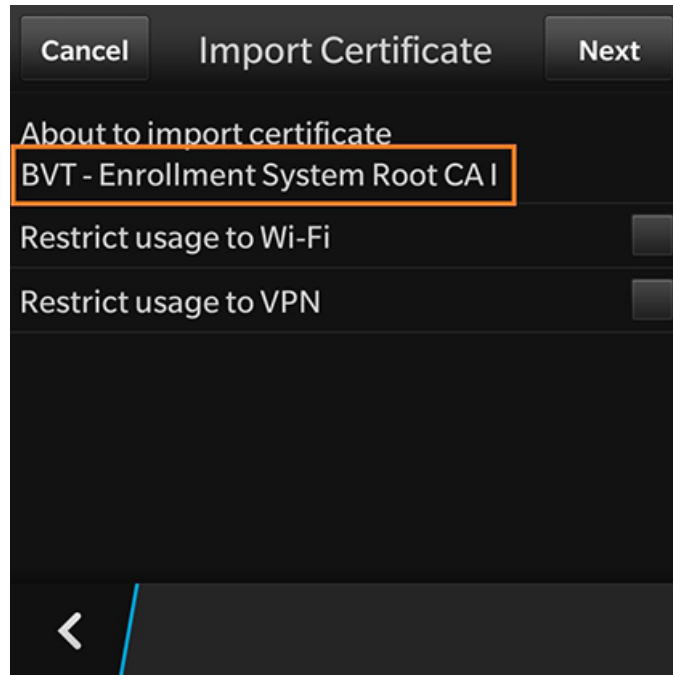


Tap the CA certificate to import.

CA Certificate Settings

On the **Import Certificate** screen, verify that you are importing the CA certificate that was listed on the configuration instructions. Leave the certificate usage restriction settings unchecked.

FIGURE 101 CA Certificate Settings



Tap the back arrow at the bottom left to return to the certificate store.

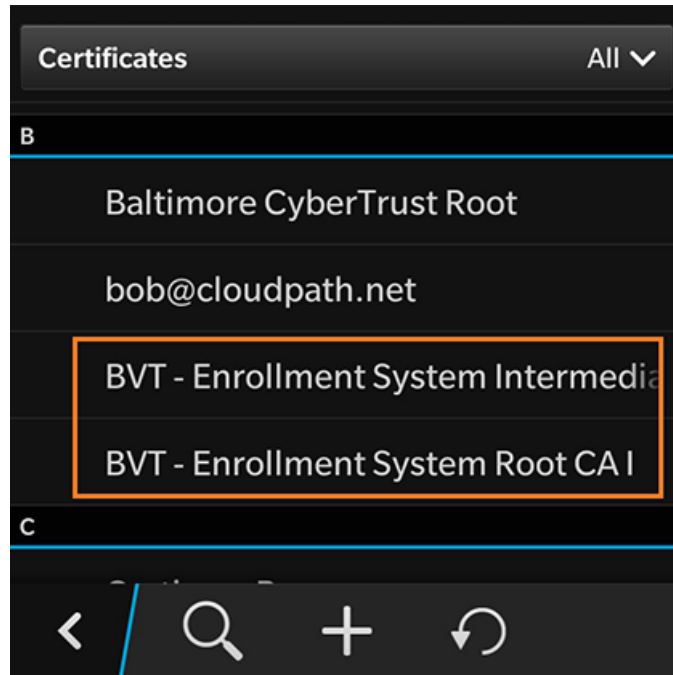
Certificate Imported

There is a brief message that indicates that the certificate was imported. The **Certificates** screen displays. Swipe the list to view your CA certificate.

NOTE

If your CA certificate contains both a Root and an Intermediate certificate, both are imported in to the certificate store.

FIGURE 102 Certificate Imported

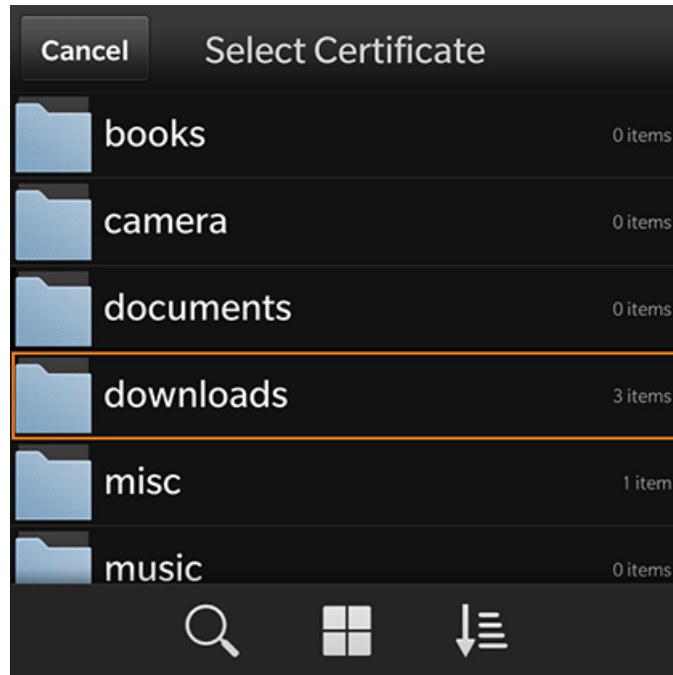


Click the plus sign to add the User certificate.

Select Downloads Folder

On the **Select Certificates** screen, locate the **Downloads** folder.

FIGURE 103 Select Downloads Folder

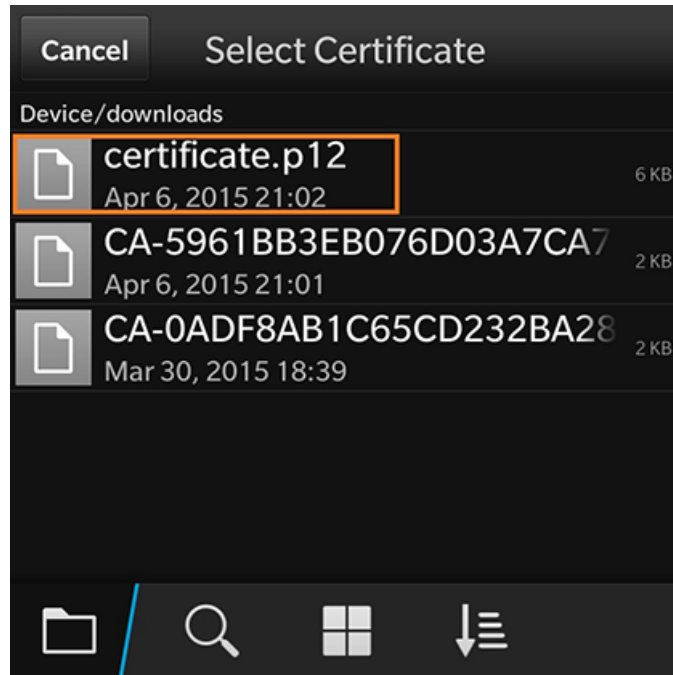


Tap the **Downloads** folder to view the certificates available for import.

Select User Certificate to Import

Select the user certificate that was previously downloaded.

FIGURE 104 Select User Certificate

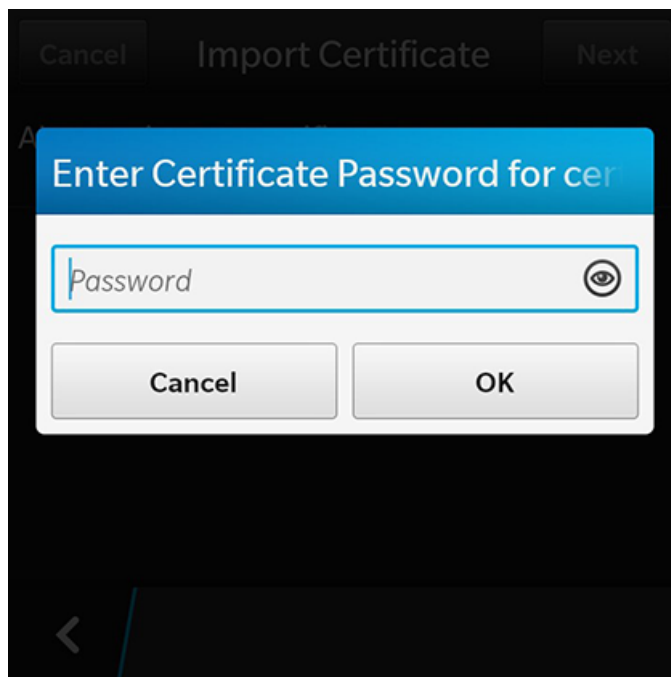


Tap the user certificate to import.

Enter User Certificate Password

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

FIGURE 105 Enter Password for User Certificate



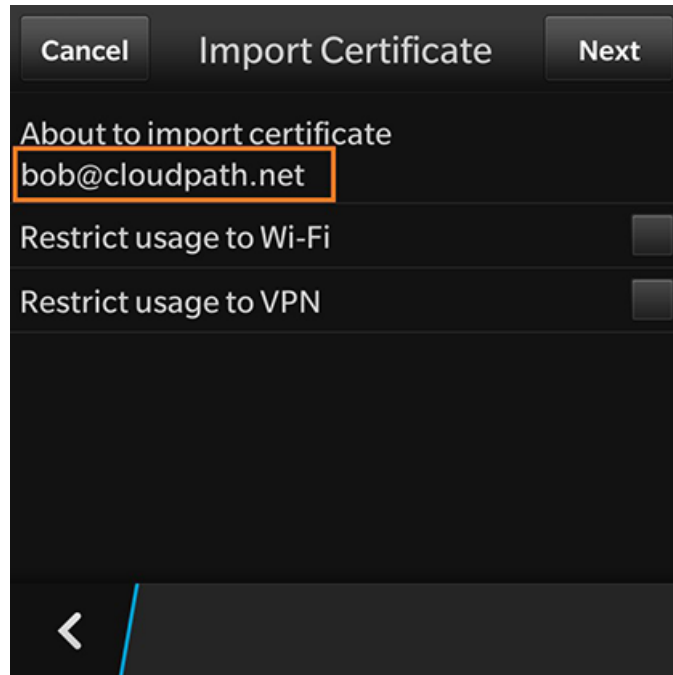
Enter the password from your user credentials. For example, if your user credentials are username=bob and password=bob1, then enter **bob1** for the user certificate password.

Tap **Ok** to continue with importing the user certificate.

User Certificate Settings

On the **Import Certificate** screen, verify that you are importing the user certificate that was listed on the configuration instructions. Leave the certificate usage restriction settings unchecked.

FIGURE 106 User Certificate Settings for Importing a Certificate

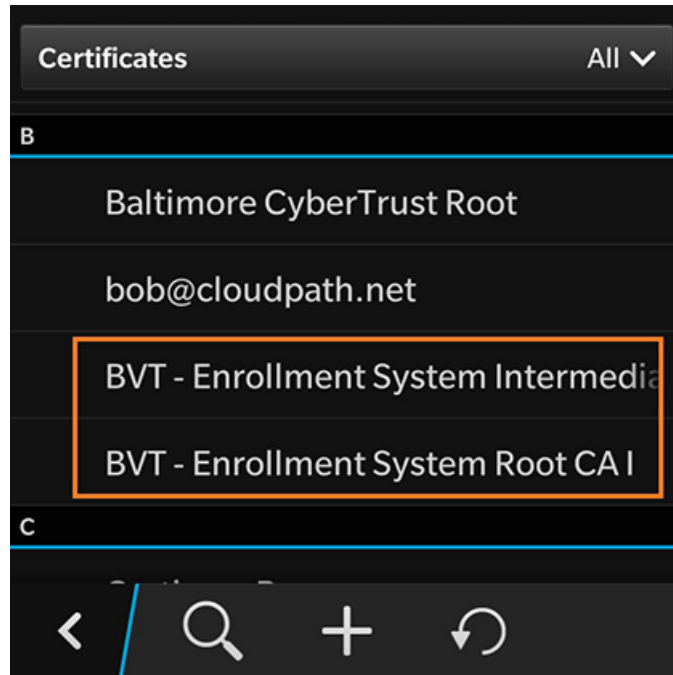


Tap the back arrow at the bottom left to return to the certificate store.

Certificate Imported

There is a brief message that indicates that the certificate was imported. The **Certificates** screen displays. Swipe the list to view your user certificate.

FIGURE 107 Certificate Imported



Tap the back arrow in the bottom left to return to the **Security and Privacy** screen, and then again to return to the **System Settings** screen.

Configure Wi-Fi Settings

Return to the device **System Settings** screen to configure the wireless network settings.

System Settings

The Wi-Fi settings are configured in **Network and Connections**.

FIGURE 108 System Settings for Wi-Fi

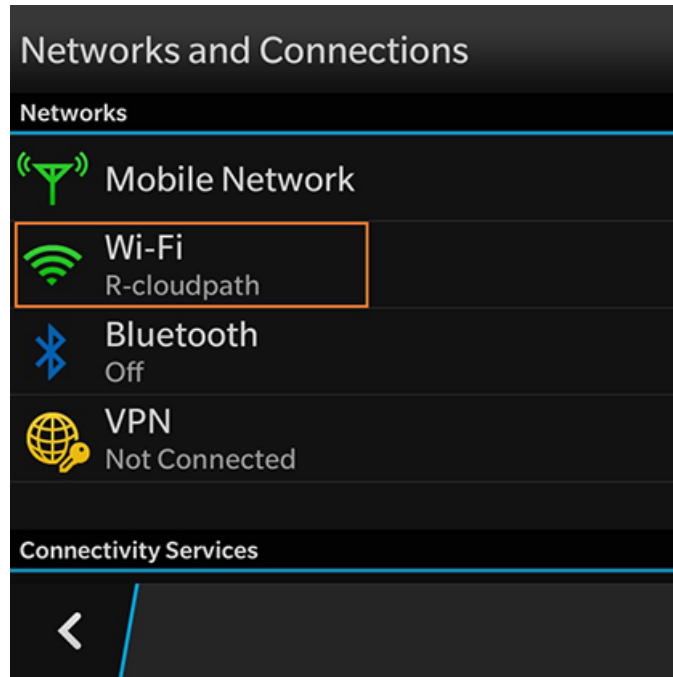


Tap **Network and Connections** to continue.

Network and Connections

The **Wi-Fi** setting displays your current wireless network connection.

FIGURE 109 Networks and Connections



Select **Wi-Fi** to continue.

Wi-Fi Networks

The **Wi-Fi Networks** tab lists the available wireless networks.

FIGURE 110 Wi-Fi Settings

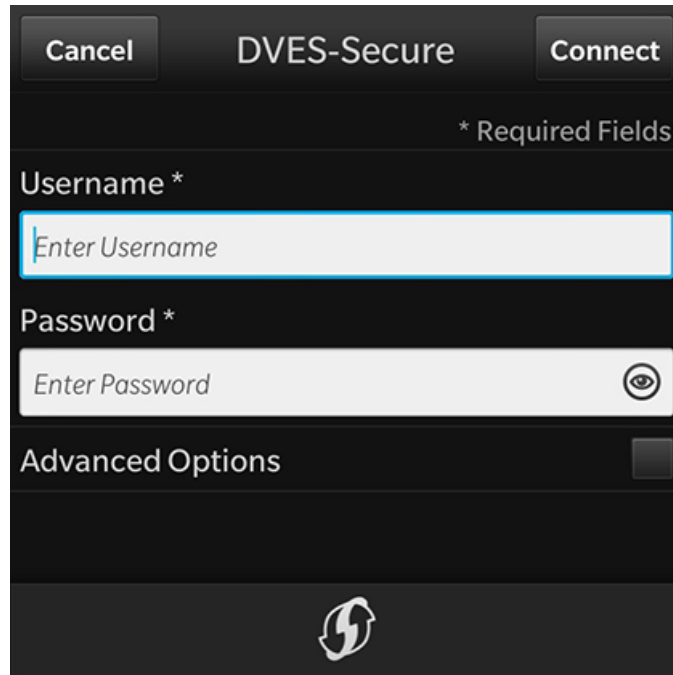


Swipe through the list of **Available Networks** to locate the **Wireless Network Name** from the configuration instructions. See the **Configuration Instructions** section to review the correct settings.

Wi-Fi Settings - User Credentials

The secure wireless settings require your user credentials.

FIGURE 111 User Credentials for Wireless Network

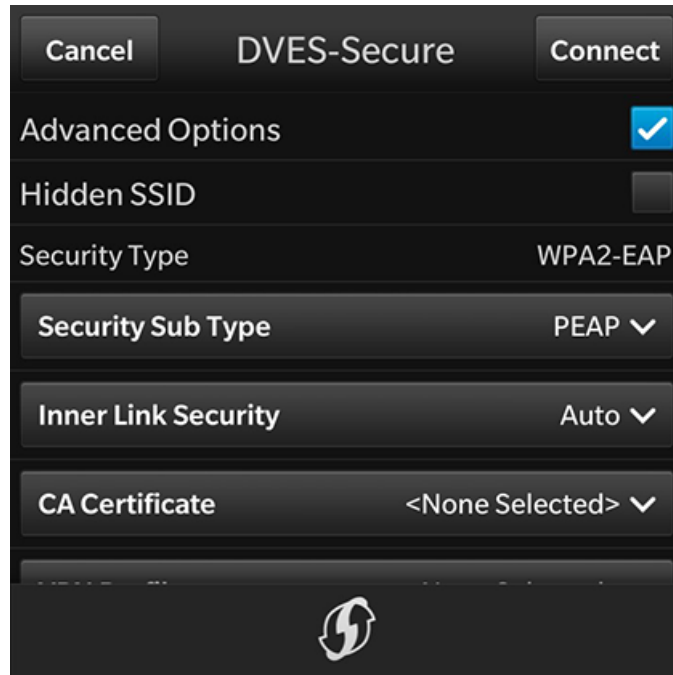


Enter the same user credentials from the enrollment workflow steps. See the User Credentials section to review these settings.

Advanced Options

The secure wireless network requires additional settings.

FIGURE 112 Advanced Options

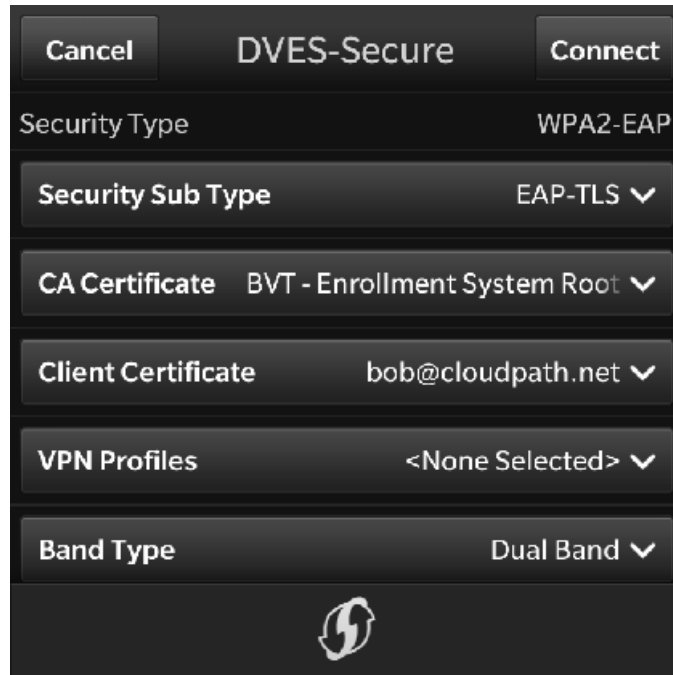


Check the **Advanced Options** box to expose additional wireless configuration settings.

Wi-Fi Settings - Security Type Settings

The secure wireless network requires that you select the correct **Security Type**, **Security Sub Type**, **CA Certificate**, and **Client Certificate** settings.

FIGURE 113 Security Type Settings



Use the following selections for the secure wireless network:

- Security Type = WPA2-EAP
- Security Sub Type = EAP-TLS
- CA Certificate = The CA certificate that was downloaded and imported.
- Client Certificate = The client certificate that was downloaded and imported.
- VPN Profiles = None
- Band Type = Leave the default, Dual Band

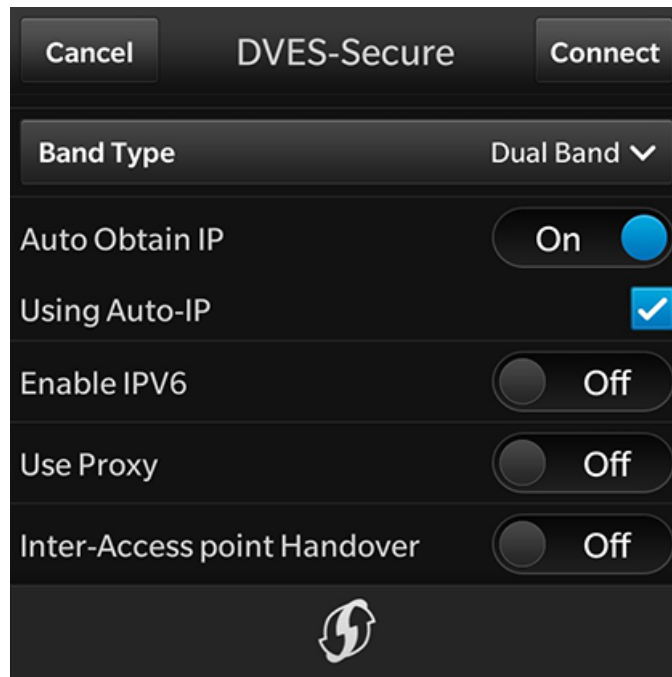
Wi-Fi Settings - Optional Settings

Typically, the secure wireless network does not require the optional settings.

NOTE

The network administrator might require a different setting for these options. If you have difficulty connecting, contact the network help desk for assistance.

FIGURE 114 Optional Settings



In most cases, the following settings can be left in their default positions:

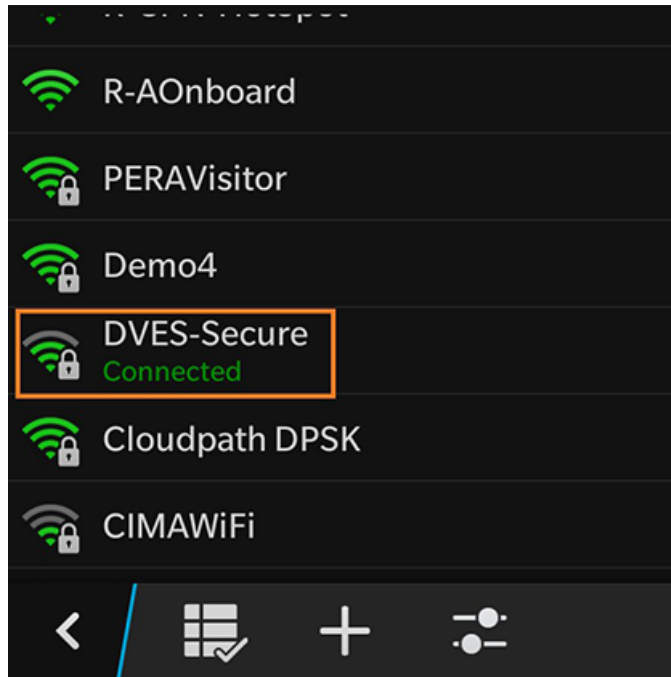
- Auto Obtain IP = On
- Using Auto-IP = Selected
- Enable IPV6 = Off
- Use Proxy = Off
- Inter-Access point Handover = Off

Tap **Connect** to connect to the secure wireless network.

Device Connected

You should now be connected to the secure wireless network.

FIGURE 115 Device Connected



The Wi-Fi screen displays the secure wireless network to which you are connected.

End-User Experience for Chromebook Devices

- Overview..... 129
- Supported Chrome OS Devices..... 129
- Cloudpath User Experience..... 129

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 Chrome OS Devices

Cloudpath supports Chrome OS version 51 and later.

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

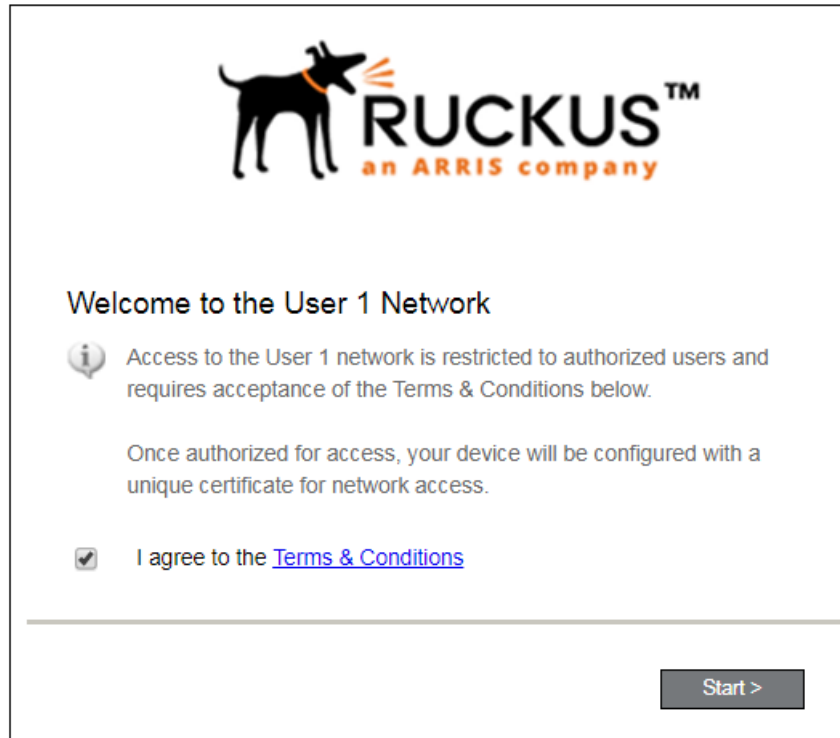
During enrollment, the Chrome OS is detected and Cloudpath provides Chrome OS-specific instructions for downloading the configuration file and installing it on the device manually, or automatically if extensions are configured. After the configuration file is installed, the user simply connects the secure 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 116 Wizard Welcome Page



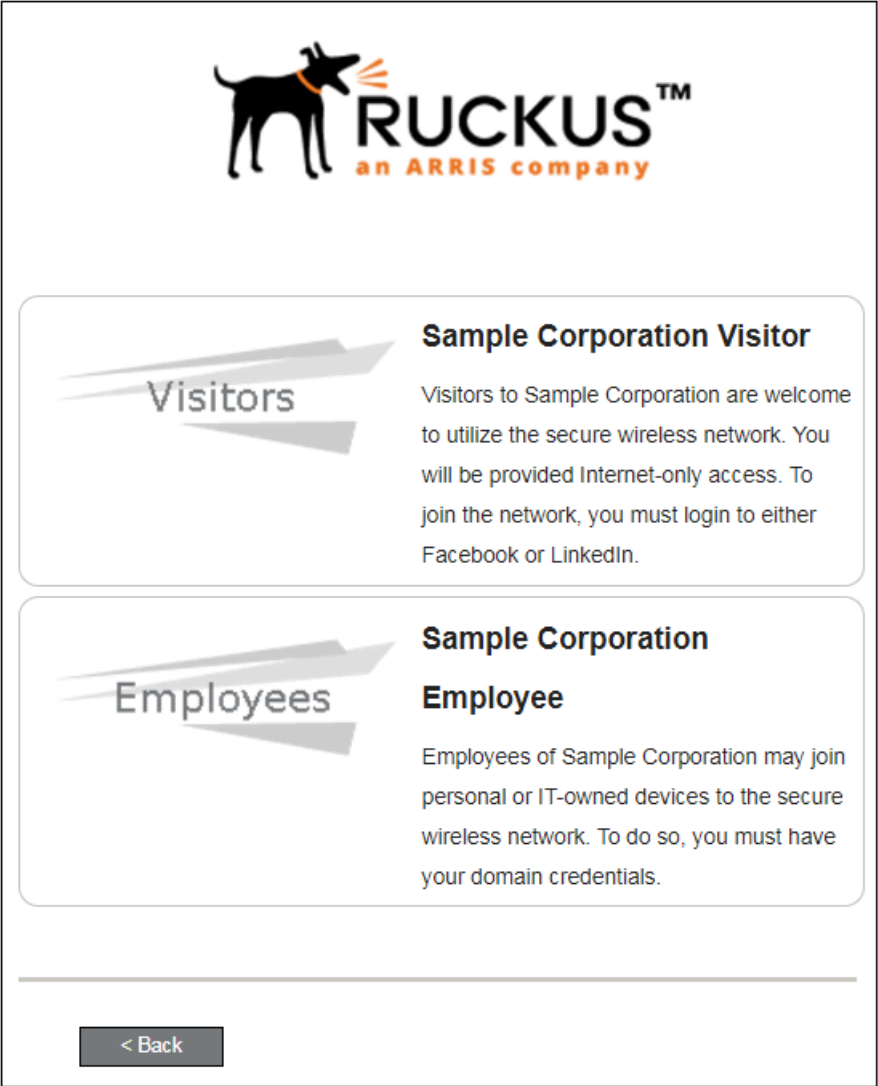
The login screen is typically customized with the logo, colors, and text for the organization or institution. The screens in this example use the default look and feel of the application.

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 117 User Type Prompt

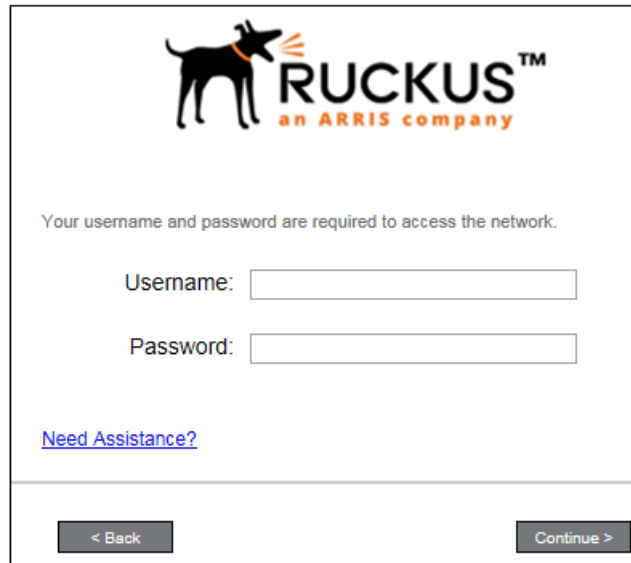



Select the user type to continue. This example follows the *Employee* workflow branch.

User Credentials

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

FIGURE 118 User Credential Prompt





Your username and password are required to access the network.

Username:

Password:

[Need Assistance?](#)

< Back Continue >

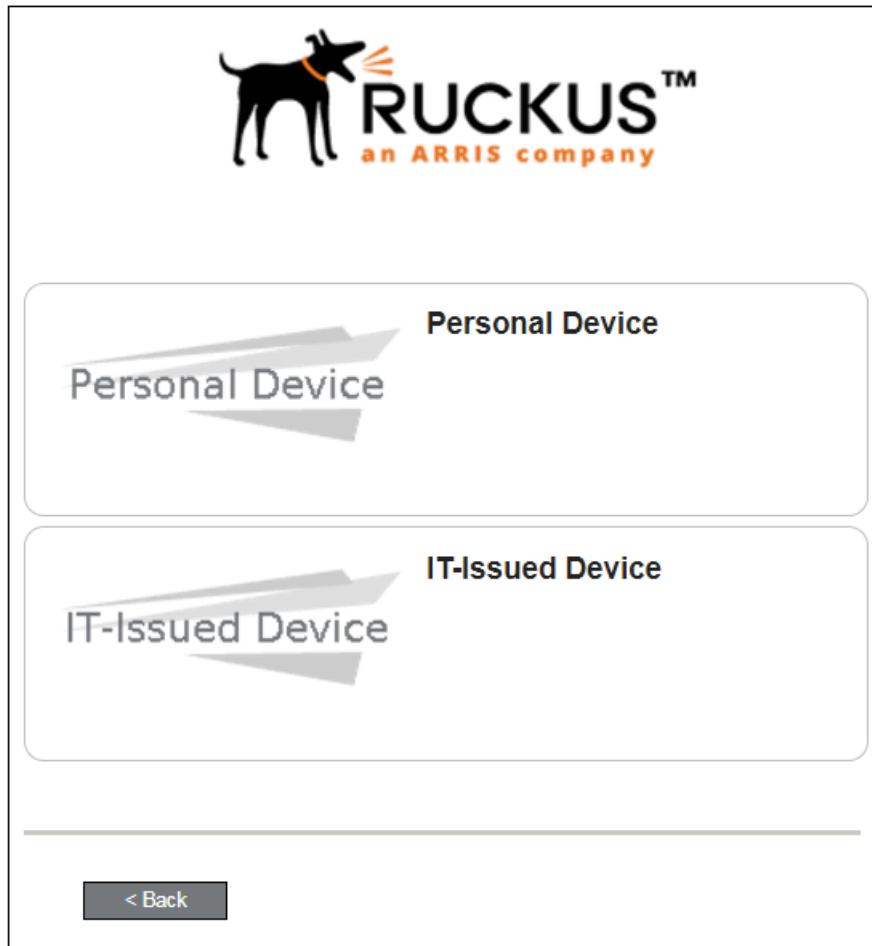
Enter the user credentials and click **Continue**.

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 119 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 120 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" (with a download icon) and "Step 2: Import Network File" (with a gear icon). Step 2 includes instructions to open a new browser tab and enter the address "chrome://net-internals/#chromeos". A screenshot of a browser window shows the address bar with "chrome://net-internals/#chrome-os" and a red arrow pointing to the address. Below the address bar, the page title is "Import ONC file" and there is a "Choose File" button with "No file chosen" next to it. A hand cursor is shown clicking the button. Below this browser screenshot, a final list of instructions is provided: "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.

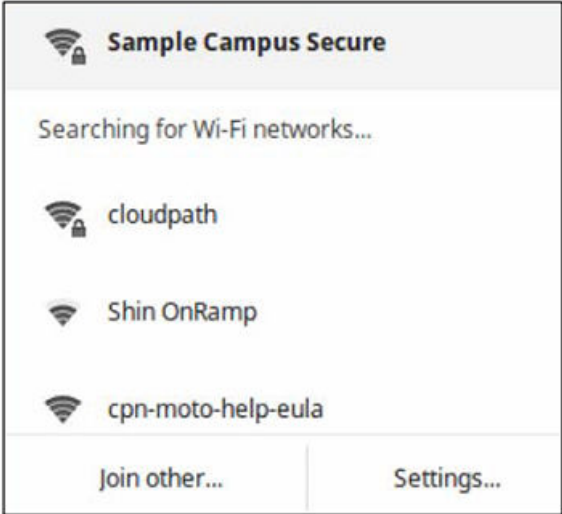
FIGURE 121 Import ONC File



- 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 122 Select Wi-Fi Network



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

FIGURE 123 Enter User Credentials

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

- SSID: Sample Campus Secure
- EAP method: PEAP (dropdown)
- Phase 2 authentication: MSCHAPv2 (dropdown)
- Server CA certificate: Cloudpath IT Root CA 1 [Cloudpath IT Root C (dropdown)
- Subject Match: (empty text field)
- User certificate: None installed (dropdown)
- Identity: (empty text field)
- Password: (empty password field with a toggle icon on the right)
- Anonymous identity: (empty text field)
- Save identity and password
- Buttons: Connect, Cancel

The user should now be connected to the secure network.

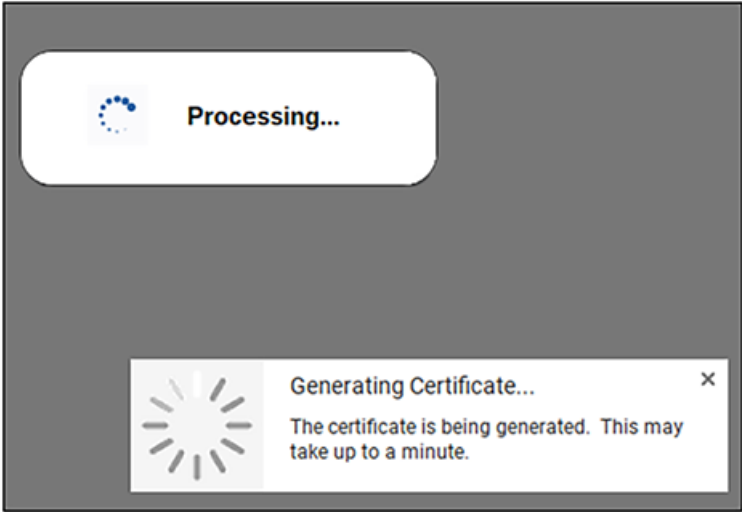
Managed Chromebooks With Extension User Experience

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.

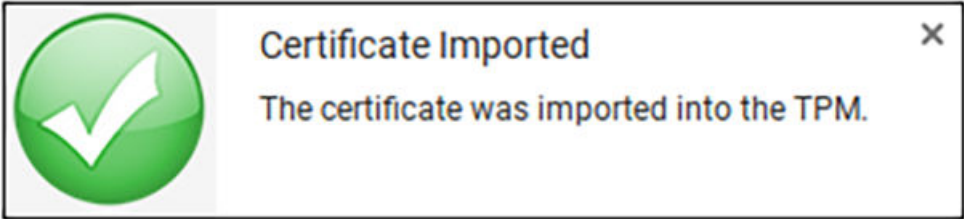
The extension generates the certificate.

FIGURE 124 Generating Certificate



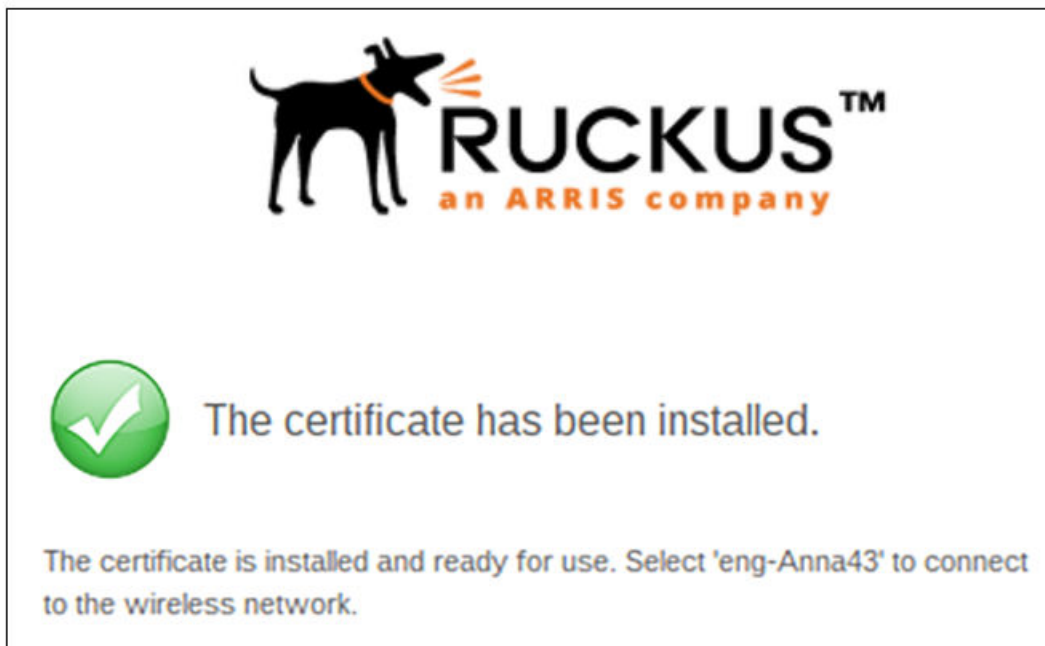
The extension imports the certificate into the TPM.

FIGURE 125 Certificate Imported



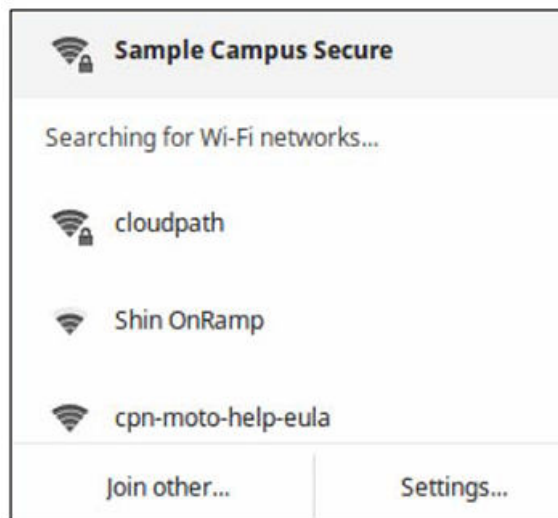
When the certificate installation is complete, a message displays indicating that the certificate is installed and ready for use.

FIGURE 126 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 127 Select Wi-Fi Network



The user should now be connected to the secure network.

End-User Experience for Android Devices

- Supported Android Versions..... 139
- Cloudpath User Experience..... 139
- Troubleshooting..... 156

Supported Android Versions

Cloudpath supports the following operating systems for Android devices: 6.0 and later

NOTE

Networks may not support all versions of the Android OS. Contact the network help desk to verify the supported Android versions.

NOTE

The Android operating system presents a challenge when it comes to offering a consistent user experience because the different vendor and operating system combinations behave in slightly different ways. During the device configuration process, the Cloudpath Wizard makes every attempt to provide a seamless experience by detecting the OS version on the device and providing the appropriate user prompts during the onboarding process.

Cloudpath User Experience

Welcome Screen With AUP

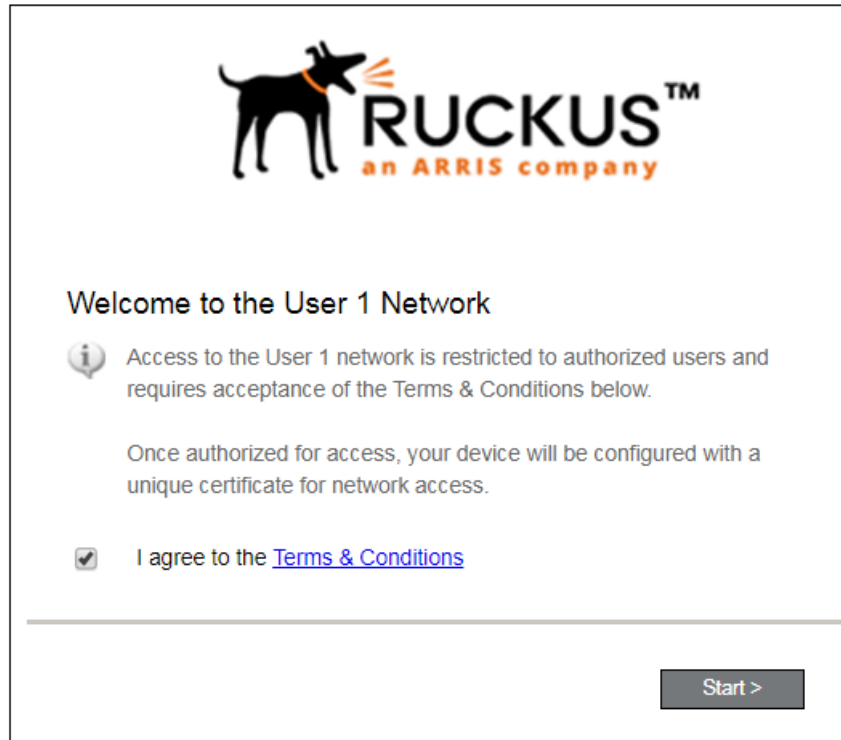
When the user enters the enrollment URL on their device, the Login (or Welcome) screen displays.

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 128 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 129 User Type Prompt

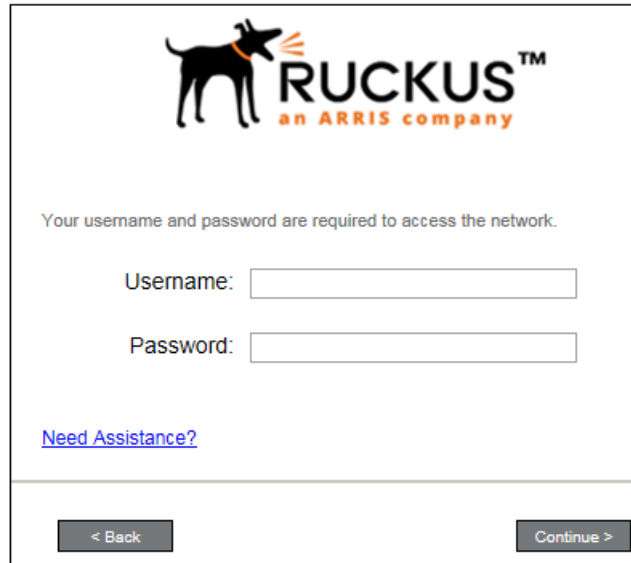


Select the user type to continue. This example follows the *Employee* workflow branch.

User Credentials

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

FIGURE 130 User Credential Prompt



The screenshot shows a user credential prompt screen for Ruckus, an ARRIS company. At the top, there is a logo featuring a black dog silhouette with orange sound waves next to the text "RUCKUS™" and "an ARRIS company" below it. Below the logo, the text reads "Your username and password are required to access the network." There are two input fields: "Username:" followed by a text box, and "Password:" followed by a text box. Below the input fields is a blue hyperlink that says "Need Assistance?". At the bottom of the screen, there are two buttons: "< Back" on the left and "Continue >" on the right.

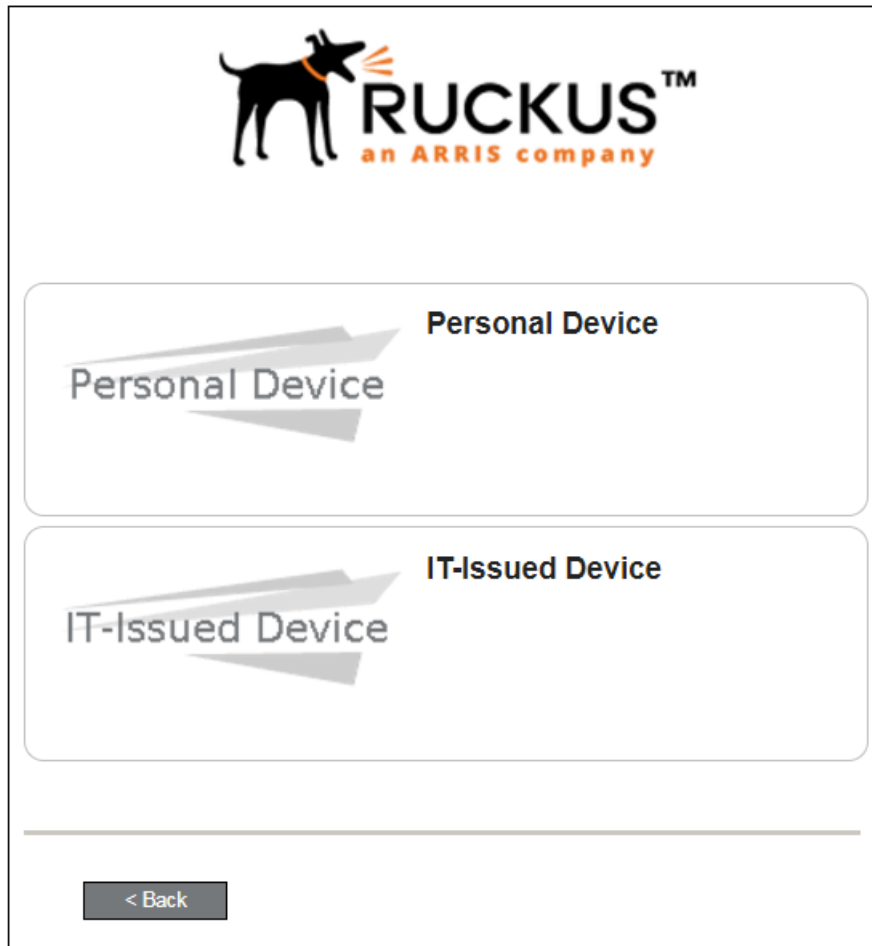
Enter the user credentials and click **Continue**.

Device Type

If required by the network, the user might 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 131 Device Type Prompt

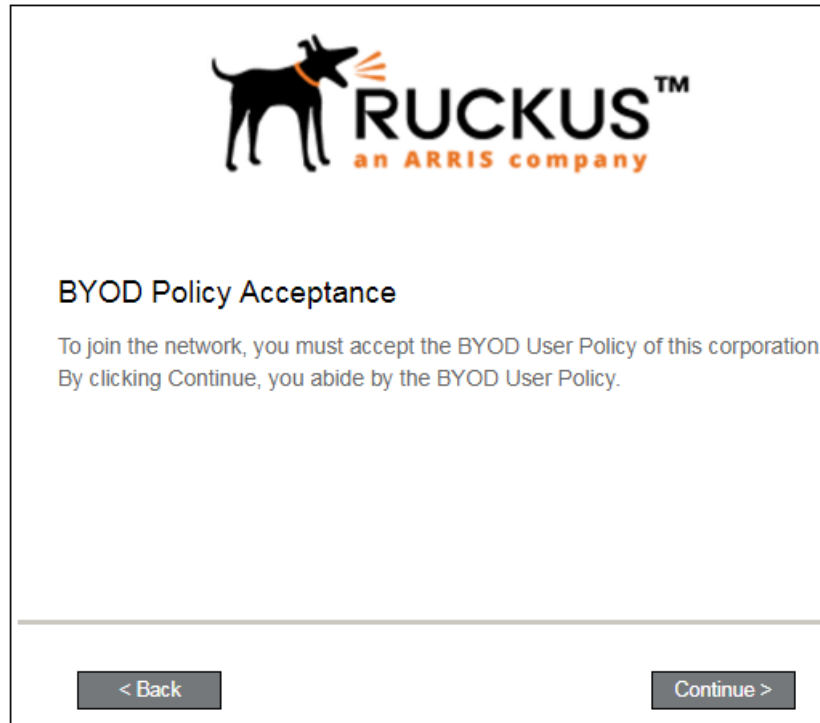


Select a device type to continue. This example follows the IT-Issued Device enrollment workflow.

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 132 BYOD Policy



Click **Start** to continue.

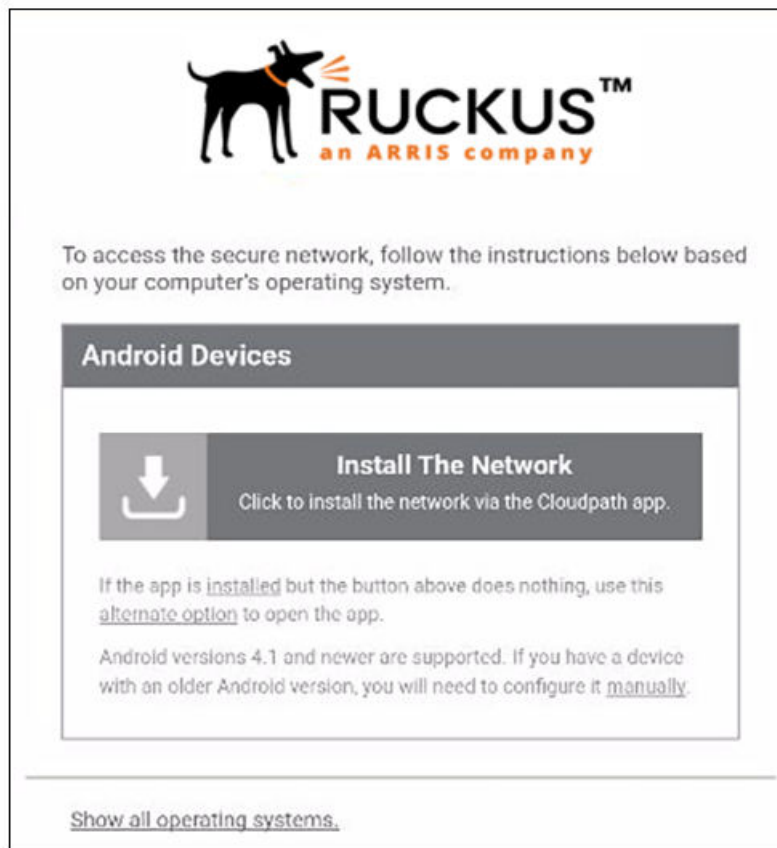
After the enrollment prompts, the user will download and run the configuration Wizard to migrate the device to the secure network.

Android-Specific Configuration Instructions

The application detects the user agent for the Android operating system and provides the correct installation and configuration instructions.

The following screen is displayed for devices running the Android operating system 6.0 or newer.

FIGURE 133 Instructions for Devices Running Android OS 6.0 or Newer

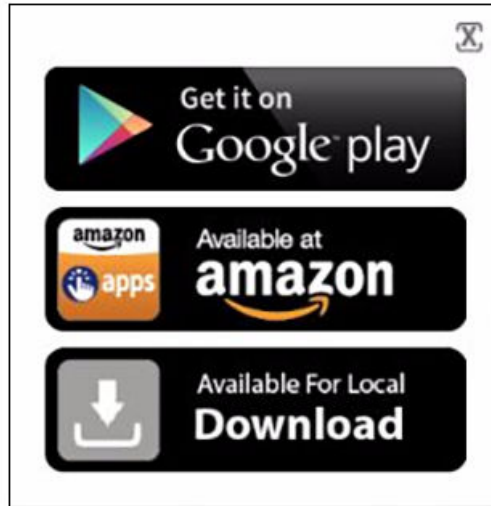


Tap **Install the Network** to start the installation process.

Download and Install Application

The application is available from Google Play Store, Amazon Market, and as a Direct Download from a local web server. The network administrator can limit the download options. In this case, the download prompt may not display all three options.

FIGURE 134 Select Installation Method



Select the installation method to continue.

Install from Google Play

If permitted by the network configuration, the application can be installed from the Google Play Store.

FIGURE 135 Install from Google Play Store

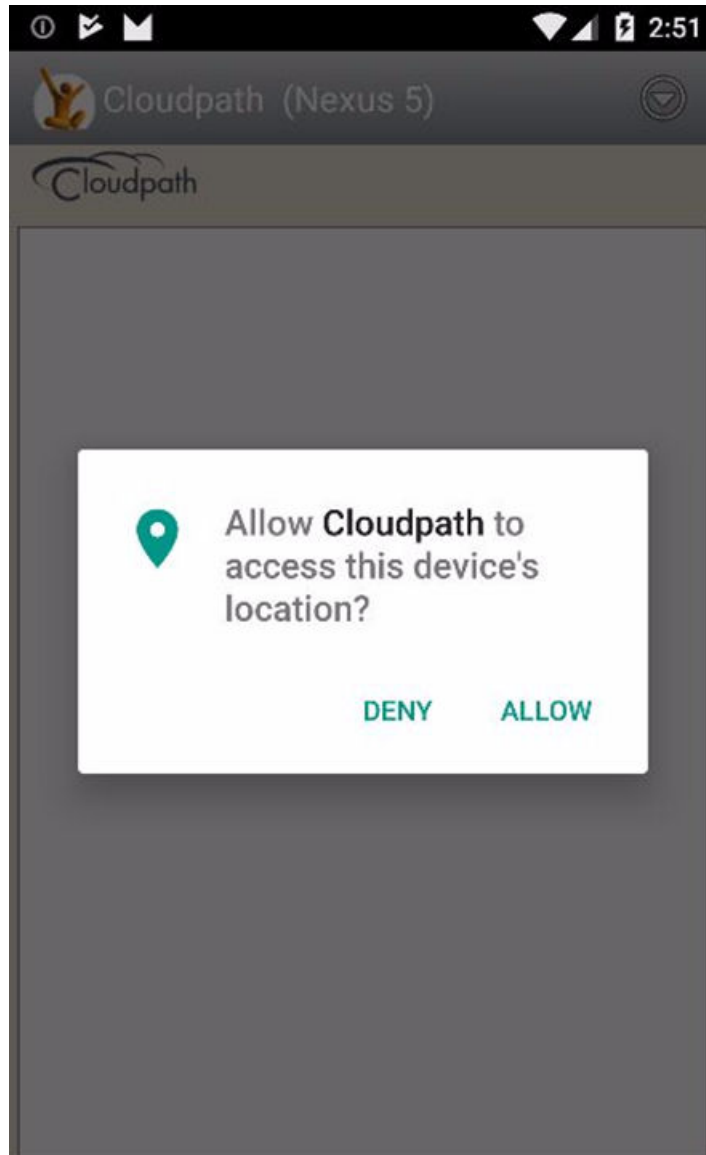


Tap **Install** to continue.

Accept Access Request

To run the enrollment wizard and configure the device, the application requires access to location of the device.

FIGURE 136 Access To Device Location

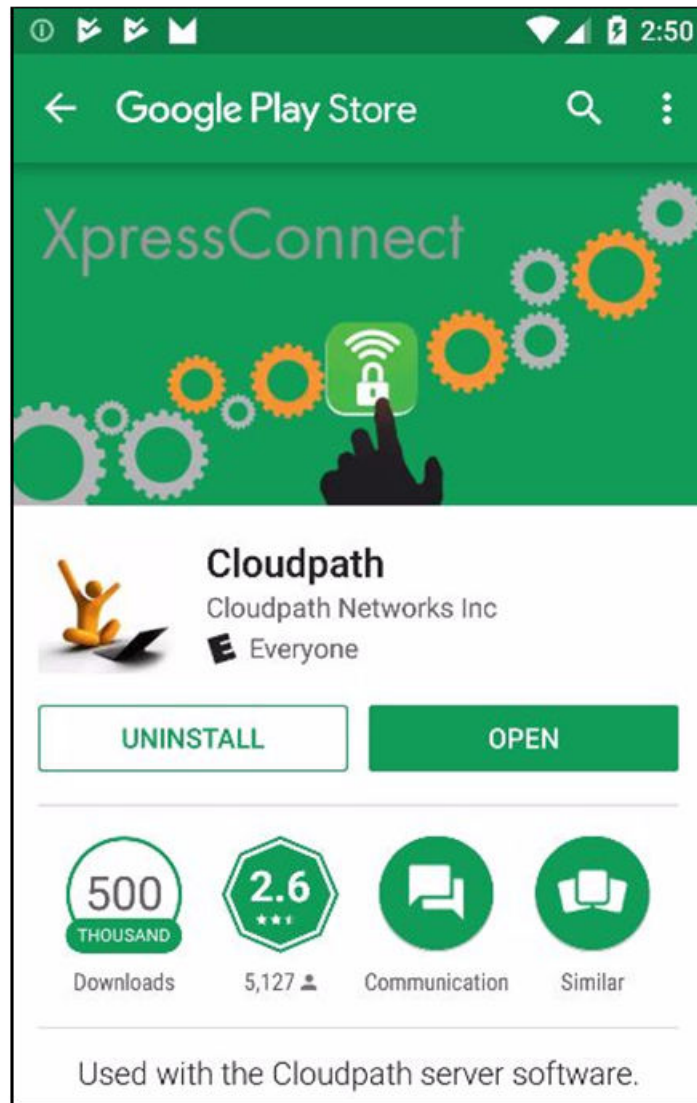


Tap **Allow** to continue.

Next Step After Application is Installed on Device

If you are using the Google Play Store installation, click the **Open** button, then follow the instructions in the [User Experience Example for Android Version 6.0 and Later](#) on page 154 section.

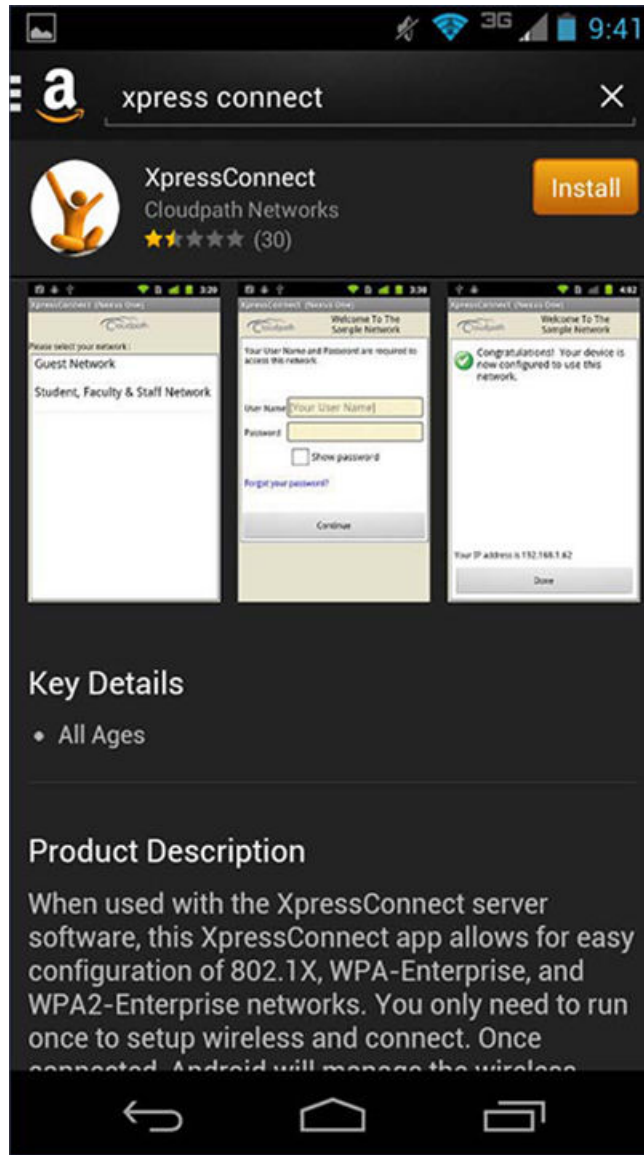
FIGURE 137 Installation Finished - Click Open



Install from Amazon Market

If permitted by the network configuration, the application can be installed from the Amazon Market.

FIGURE 138 Install From Amazon Market



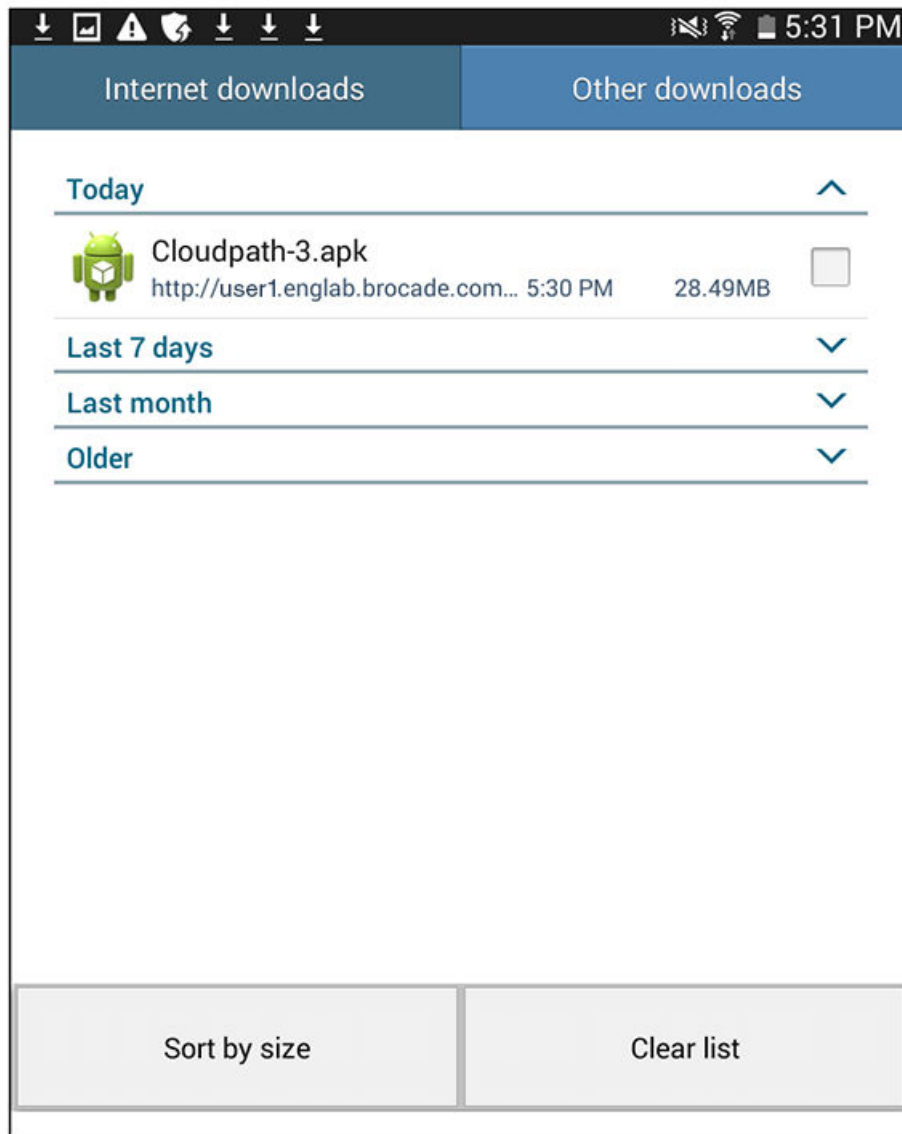
Click **Install** to start the installation process.

When installation is complete, refer to [Wizard Application User Experience](#) on page 48.

Local Download

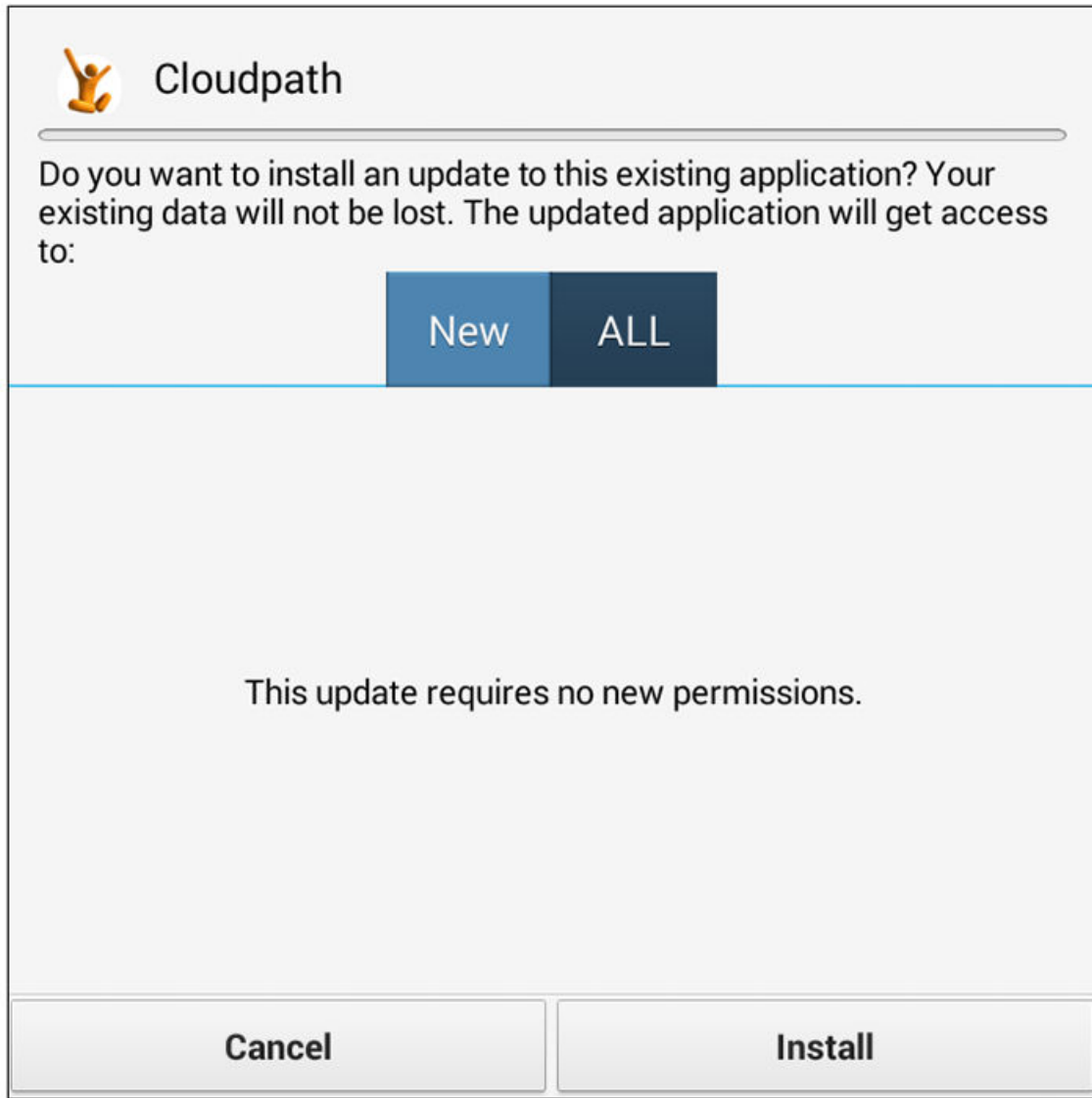
If permitted by the network configuration, the application is available for download from a local web server. Go to the device **Downloads** to locate the Cloudpath.apk file.

FIGURE 139 Local Download



Double-tap the Cloudpath application to start the installation process.
You may be asked if you want to install an update to the existing application.

FIGURE 140 Install an Update?

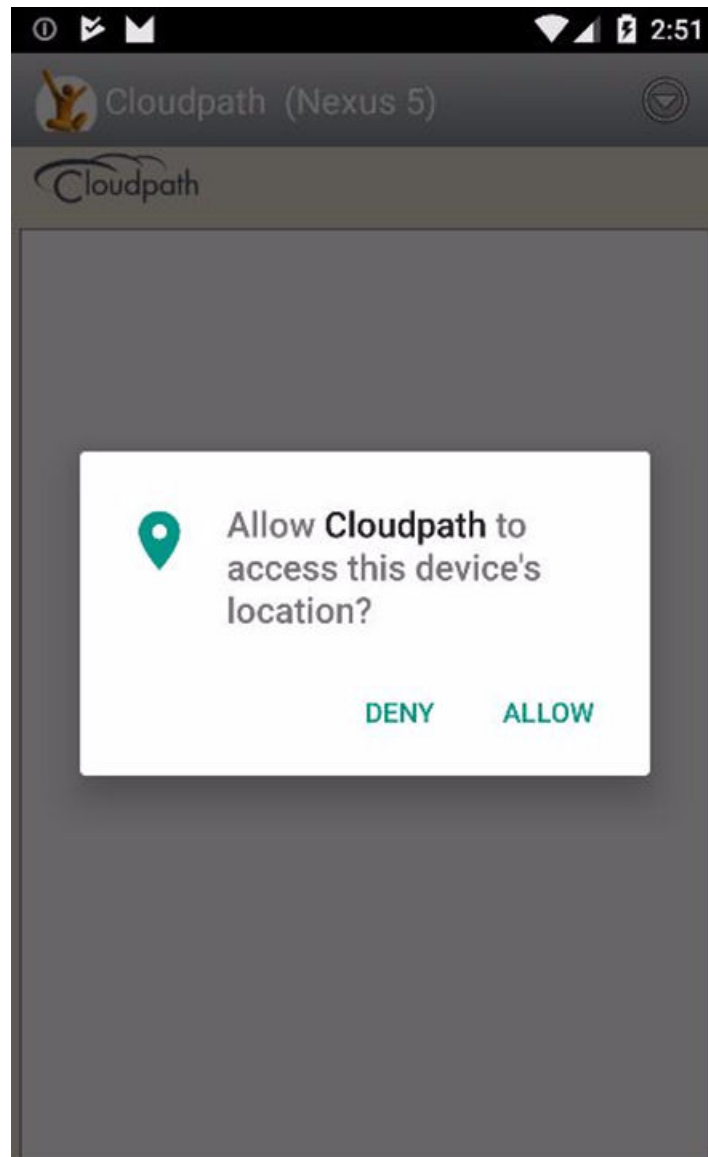


Select either New or ALL, and tap **Install**.

Accept Access Request

To run the enrollment wizard and configure the device, the application requires access to the location of the device.

FIGURE 141 Access To Device Location



Click **Allow** to continue.

When installation is complete, refer to [Wizard Application User Experience](#) on page 48.

Cloudpath Wizard User Experience

Introduction

The Wizard is the dissolvable application that runs during enrollment. The Wizard examines the device operating system and configuration to determine how to proceed with configuring the device for the secure network.

The following sections provide example screens that a user might see during the Wizard configuration process.

User Experience Example for Android Version 6.0 and Later

The device configuration process is more streamlined, with fewer user prompts, for Android devices running a newer version of the operating system.

Network Monitored Message

On certain Android devices, the OS is programmed to bring up a "Network Monitored" message, if the application might be changing settings on your device. Aside from the Wi-Fi settings and adding a certificate to the certificate store, the application does not monitor or share information on your device. If this message comes up during your network enrollment process, it can be ignored.

Tap **Continue** to continue with enrollment.

Attempting to Connect to the Network

After configuring the device, the application attempts to move the device to the secure network.

FIGURE 142 Attempting to Connect



NOTE

In some configurations, the device is configured, but not migrated to secure network. In these cases, the network administrator allows the device to be pre-configured, for use when the device is in range of the secure network.

Connected

When the enrollment process is finished, the application indicates that the device has been moved to the secure network.

FIGURE 143 Connected



When the application has successfully configured the device and migrated it to the secure network, a message displays indicating that the process has completed.

Troubleshooting

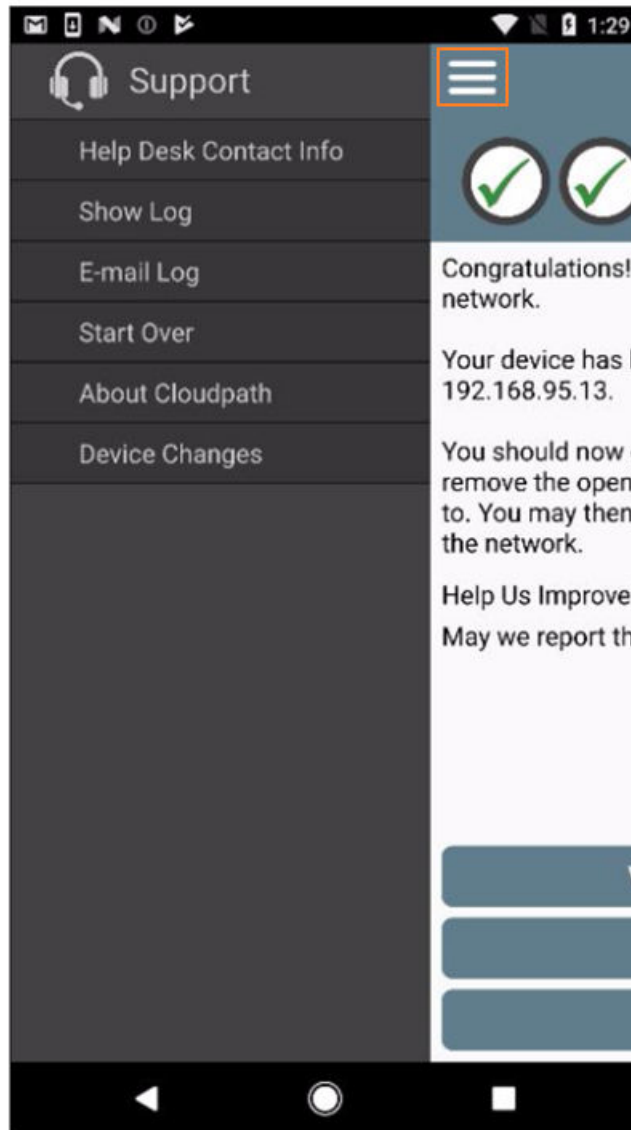
Common Android Issues

This chapter describes issues with using Cloudpath on the Android operating system that might prompt you to contact the network help desk.

Retrieve Log Files

Administrators can direct users with connection issues to email a log file from the Android device to Cloudpath Support.

FIGURE 144 Menu to E-mail Log File



Tap the **menu** button on the top right of the screen (the three horizontal bars highlighted in the figure) and select **E-mail log file**.

Passwords and Lock Screen PINs

The Android operating system stores portions of the data needed to authenticate in an encrypted key store. The lock screen pin is the password that is used to access the key store, which is why the operating system requires that the lock screen to be enabled.

To clear the key store, Go to the **Settings** screen, select **Security**, and scroll to the bottom of the screen and select **Clear Credentials**.

Blank Certificate Field

Android does not have a supported method for getting certificate chains in to the key store for use in authentication. Because of this, Cloudpath uses workarounds to make the authentication system use certificate chains. However, some workarounds do not show up in the settings screen.

In addition, if Android claims the certificate was installed in the key store and then the authentication fails, the application falls back to our workaround methods. This is done because some devices claim to have installed the certificate, but actually don't.

Certificate Passwords

Android APIs do not allow Cloudpath to specify the password when the application inserts the certificate into the key store. The workaround is to use a password prompt to install the certificate. You simply enter the password that is displayed in the password prompt and Cloudpath installs the certificate.

Android .netconfig File

If you tap the link to **Continue** with configuration of the network and receive a message that says it downloaded a file called android.netconfig, you need to check the device for the following issues:

1. You do not have the Cloudpath Wizard installed, so the server cannot instruct the device to start the application and use the file.
2. You were prompted to Play Online or Download when tapping the link, and selected **Download**. The user must select Play Online for the wizard to start up.
3. There is a misconfiguration in the server. Contact the local help desk for more information.

Memory Card

In some cases, the Cloudpath Wizard stores data on the memory card in the device. If you remove or change the memory card, authentication fails, and you must redeploy the wizard with the new memory card in the device to get it working properly.

Uninstalling the Application

It is sometimes necessary to remove the 802.1X configuration and certificates provided by the wizard before you can uninstall the application. This is enforced by the device OS, and not by the Cloudpath Wizard.

If you encounter issues while attempting to uninstall the Cloudpath application from your Android device, check the following settings.

Remove Device Administrator

If the device has any settings configured that use Android's device administration capabilities (such as mobile device management), the Cloudpath Wizard creates an administrative user during installation and this user must be removed before Cloudpath can be uninstalled.

Go to **Settings > Security**, select **Device Administrator** and uncheck the Cloudpath administrative user.

Remove Certificates

If there are certificates on the device that were installed by the Wizard, they should be removed. Go to **Settings > Security** and select **Clear Credentials** (or **Clear Storage**).

Remove SSID

The user might be required to remove the SSID from the device. Go to **Settings > Wi-Fi**, locate the SSID for the network, and tap **Forget**.

Remove Log Files

If the Cloudpath log files remain on the device, they can be removed. Mount the device as a drive, and locate the `Cloudpath.log` and `Cloudpath_old.log` files on the device internal storage.



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