

Cloudpath End-User Experience for Android Operating Systems

Supporting Software Release 5.2

Copyright Notice and Proprietary Information

Copyright 2017 Brocade Communications Systems, Inc. All rights reserved.

No part of this documentation may be used, reproduced, transmitted, or translated, in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without prior written permission of or as expressly provided by under license from Brocade.

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. BROCADE and RUCKUS WIRELESS, INC. AND THEIR LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. BROCADE and RUCKUS RESERVE THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL BROCADE or RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and in other countries. Brocade, the B-wing symbol, MyBrocade, and ICX are trademarks of Brocade Communications Systems, Inc. in the United States and in other countries. Other trademarks may belong to third parties.

Contents

Introduction.....	5
Overview.....	5
Supported Android Versions.....	5
Cloudpath User Experience.....	7
Introduction.....	7
Welcome Screen With AUP.....	7
User Type Prompt.....	8
User Credentials.....	9
Device Type.....	10
BYOD Use Policy.....	11
Android-Specific Configuration Instructions.....	12
Download and Install Application.....	14
Install from Google Play.....	15
Install from Amazon Market.....	19
Local Download.....	21
Configure Application.....	25
Cloudpath Wizard User Experience.....	27
Introduction.....	27
User Experience Example for Android Version 4.3, and Later.....	27
Network Monitored Message.....	27
Attempting to Connect to the Network.....	27
Connected.....	28
User Experience Example for Android Version 4.2, and Earlier.....	29
Passcode PIN or Pattern Lock.....	30
How to Respond to Certificate Installation Prompts.....	31
Extract Certificate.....	31
Name the Certificate.....	32
Alternate Credential Store.....	33
Attempting to Connect to the Network.....	34
Validating Connectivity.....	35
Connected.....	35
Troubleshooting.....	37
Common Android Issues.....	37
Retrieve Log Files.....	37
Passwords and Lock Screen PINs.....	38
Blank Certificate Field.....	39
Certificate Passwords.....	39
Android .netconfig File.....	39
Memory Card.....	39
Uninstalling the Application.....	39
Remove Device Administrator.....	39
Remove Certificates.....	40
Remove SSID.....	40
Remove Log Files.....	40

Introduction

- Overview..... 5
- Supported Android Versions..... 5

Overview

Cloudpath Enrollment System (ES) is a lightweight, connection wizard, customized by the network administrator, which automates the configuration process, resolves software conflicts, and migrates your Wi-Fi connection to the secure network.

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.

Supported Android Versions

Cloudpath supports the following operating systems for Android devices: 4.0.3 (Ice Cream Sandwich), 4.1, 4.2, and 4.3 (Jelly Bean), 4.4 (KitKat), 5.x (Lollipop), 6.x (Marshmallow), and 7.x (Nougat), as well as a 'support next version' flag.

NOTE

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

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

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

Cloudpath User Experience

- Introduction..... 7
- Welcome Screen With AUP..... 7
- User Type Prompt..... 8
- User Credentials..... 9
- Device Type..... 10
- BYOD Use Policy..... 11
- Android-Specific Configuration Instructions..... 12
- Download and Install Application..... 14
- Configure Application..... 25

Introduction

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.

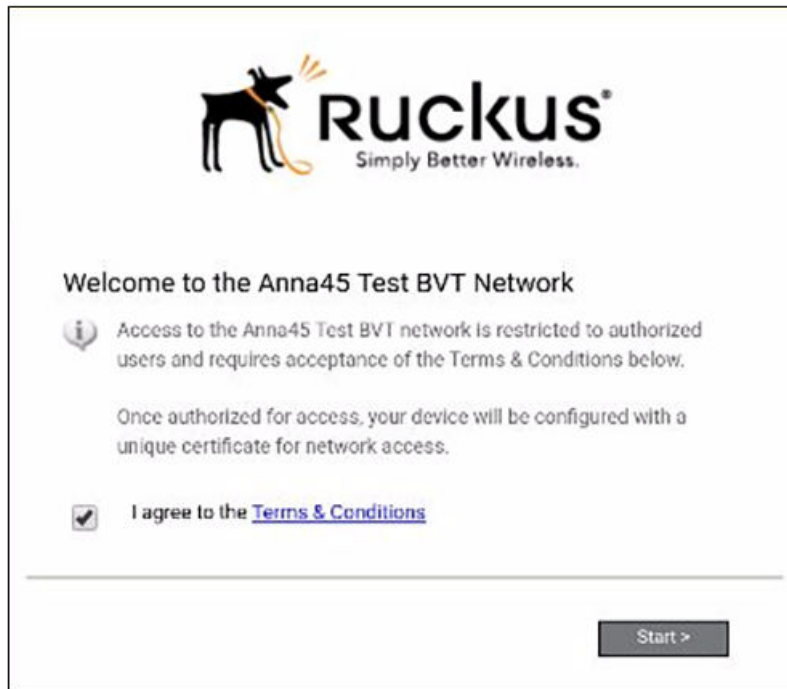
Welcome Screen With AUP

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 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** screen or **Start** button can be customized.

User Type Prompt

If required by the network, the user might see a User Type prompt. For example, an Employee might be required to enter domain credentials, and a Guest or Partner might be required to enroll using their social media credentials.

FIGURE 2 User Type Prompt

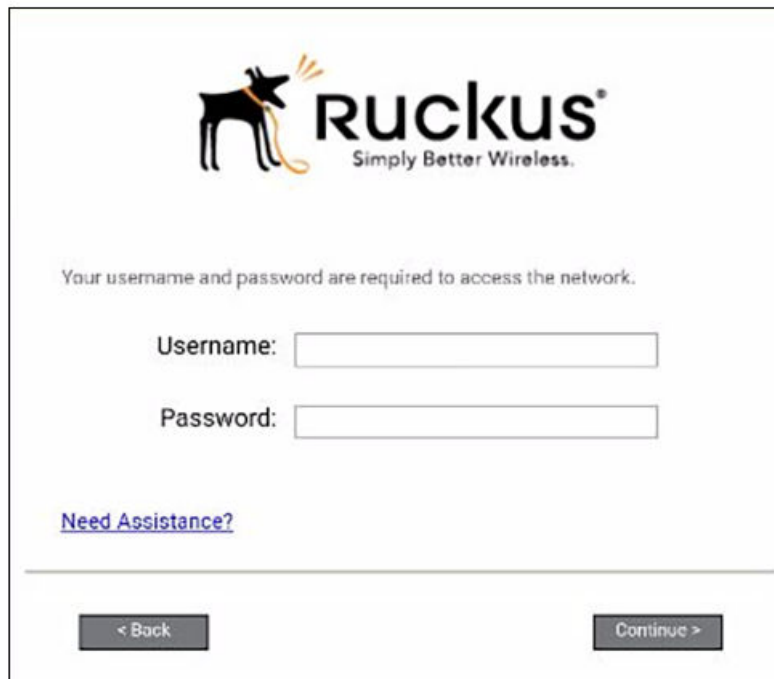


Select the **user type** to continue. This example follows the **Employee** workflow.

User Credentials

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

FIGURE 3 User Credential Prompt



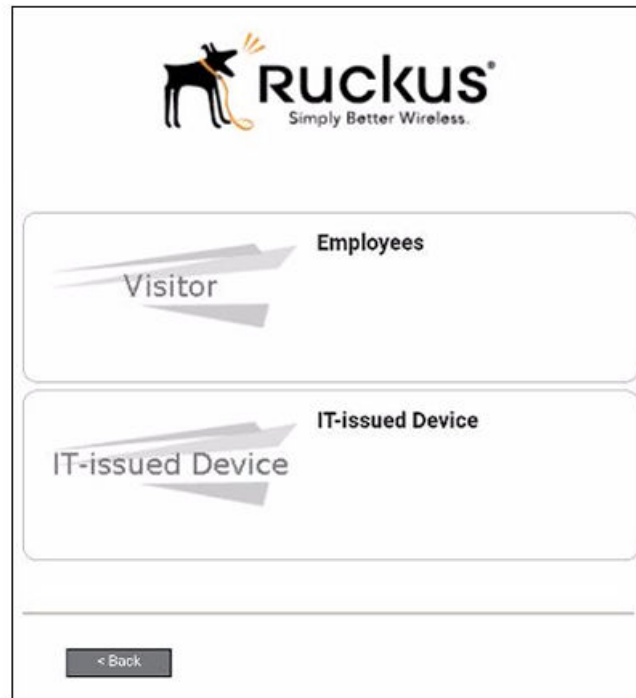
The image shows a user credential prompt screen for Ruckus. At the top, there is the Ruckus logo, which features a black silhouette of a dog with a yellow leash and a yellow speech bubble above its head. To the right of the logo, the word "Ruckus" is written in a bold, black, sans-serif font, with the tagline "Simply Better Wireless." underneath it. Below the logo and tagline, the text "Your username and password are required to access the network." is displayed. Underneath this text, there are two input fields: "Username:" followed by a white rectangular box, and "Password:" followed by a white rectangular box. Below the input fields, there is a blue, underlined link that says "Need Assistance?". At the bottom of the screen, there are two buttons: a grey button with a left-pointing arrow and the text "< Back", and a grey button with the text "Continue >" and a right-pointing arrow.

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

Device Type

If required by the network, the user might see a **Device Type** prompt. For example, a **Visitor** selection might add a prompt for a MAC address, and an **IT-Issued device** would be allowed to bypass the MAC address prompt.

FIGURE 4 Device Type Prompt

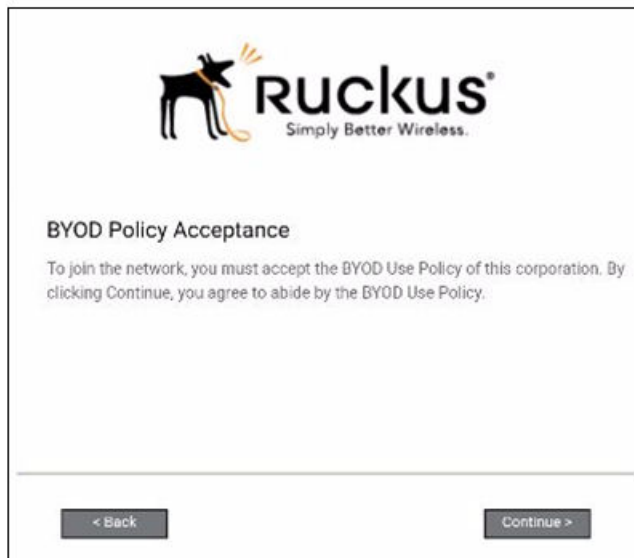


Select a **device type** to continue. This example follows the **Visitor** workflow.

BYOD Use Policy

A BYOD use policy prompts the user to accept the conditions for using a personal device on a secure network.

FIGURE 5 BYOD Use Policy



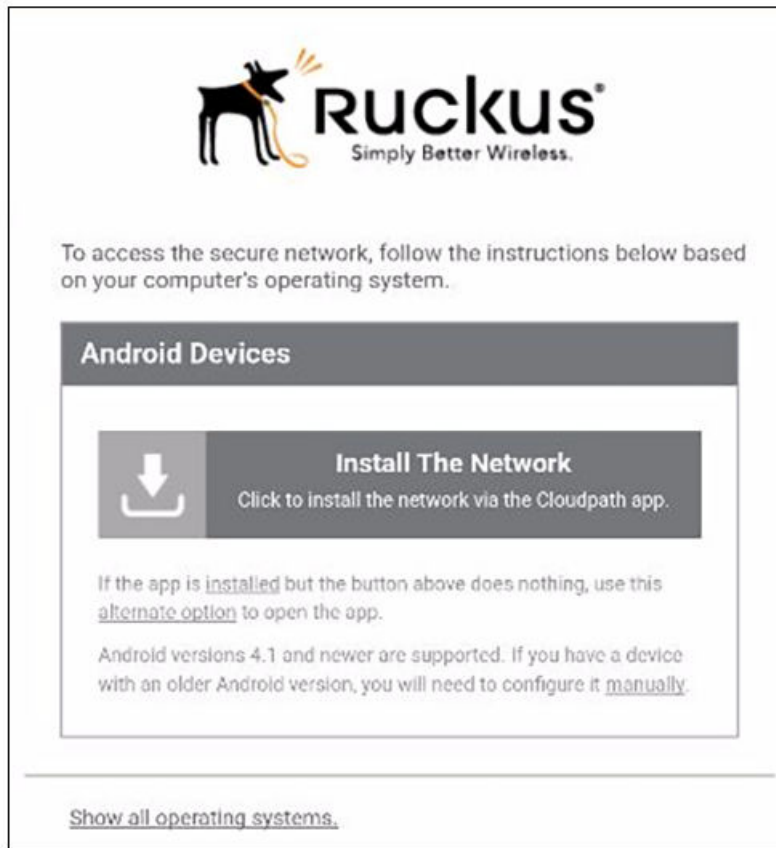
Review the use policy and tap the **Continue** button.

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.

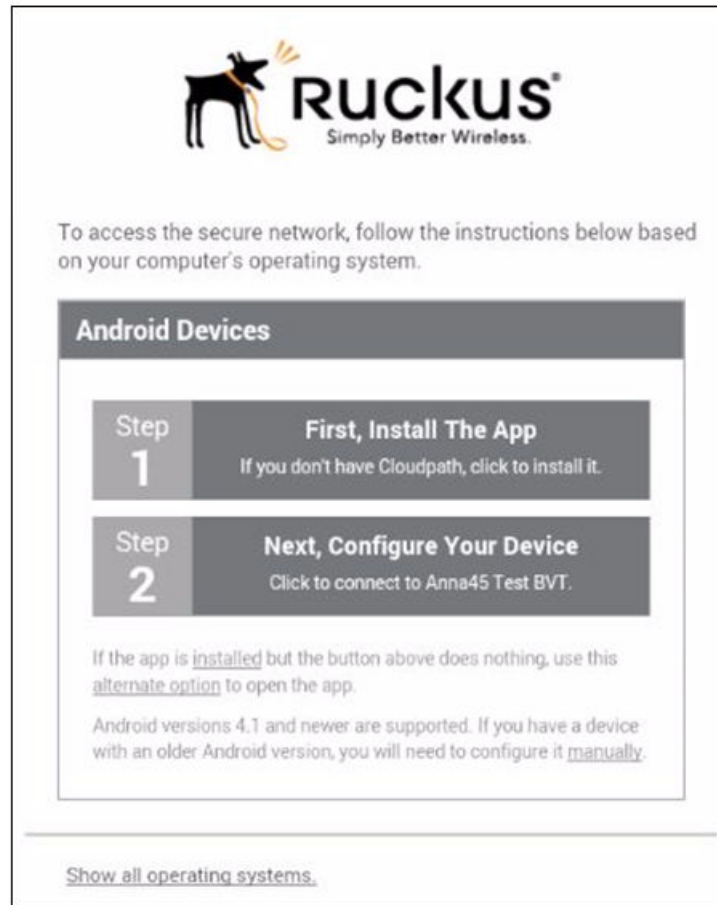
FIGURE 6 Instructions for Devices Running Android OS 6.0 or Newer



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

The following screen is displayed for devices running the Android operating system 5.x or earlier.

FIGURE 7 Instructions for Devices Running Android OS 5.x or Earlier

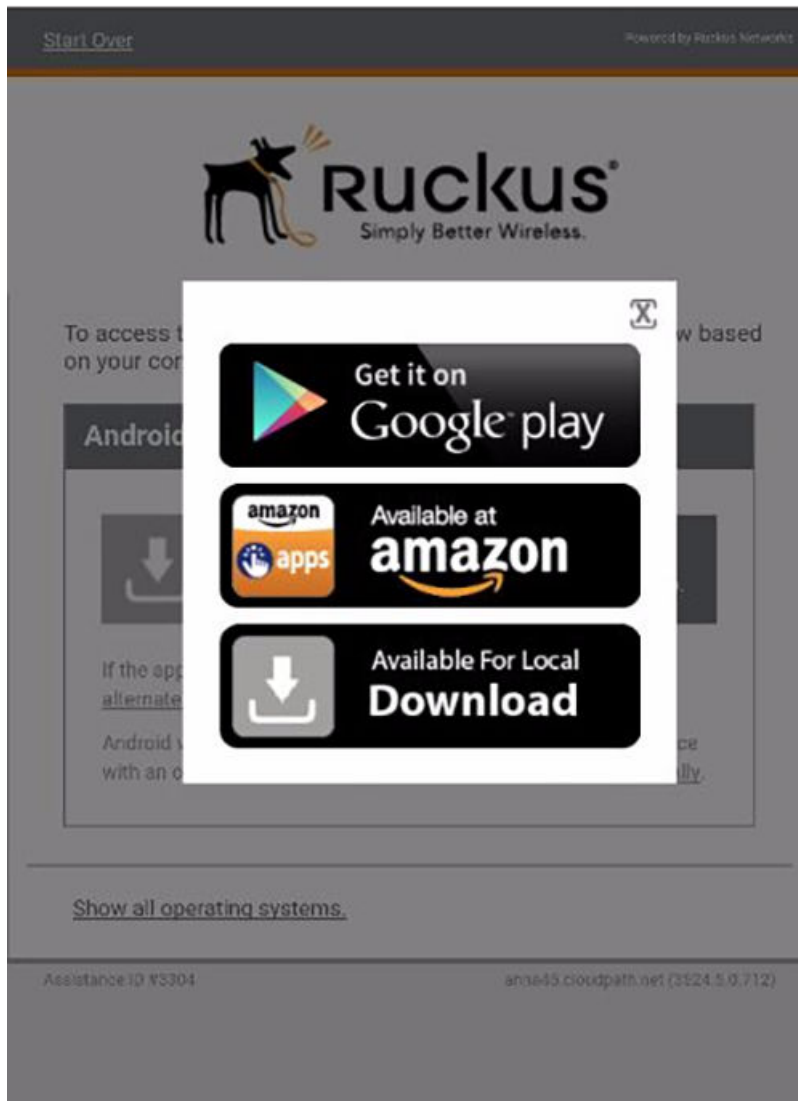


Tap **Step 1: First, Install the App** to start the installation process.

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 8 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 9 Install from Google Play Store

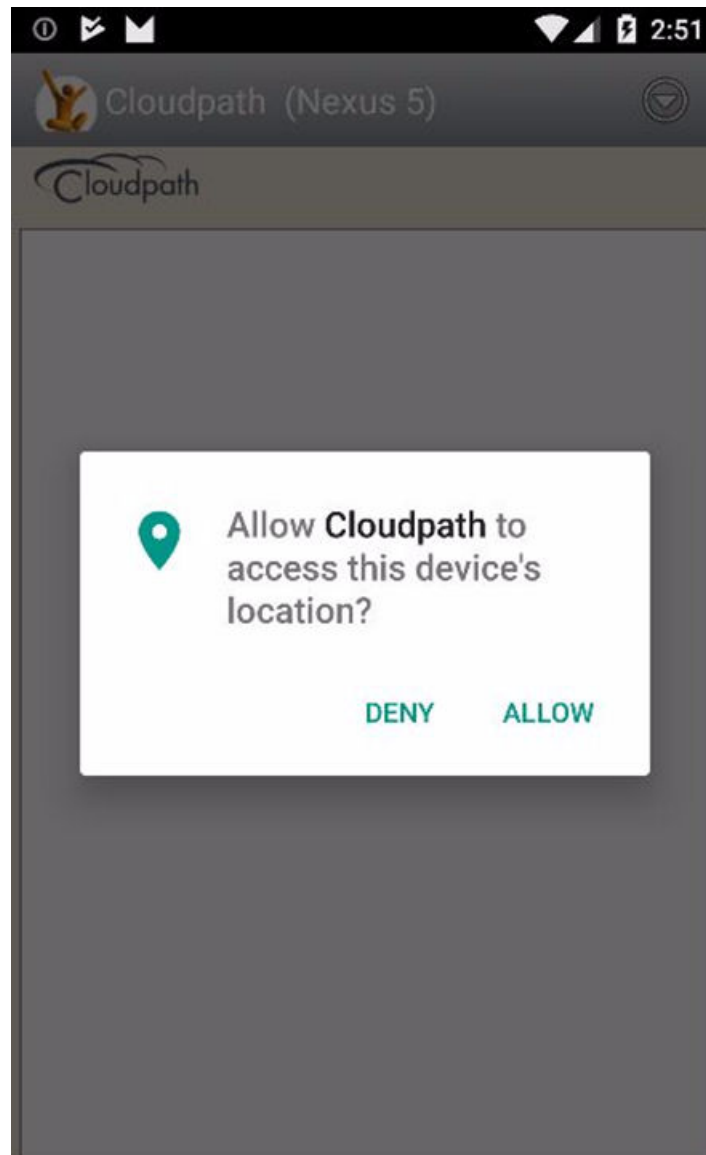


Tap **Install** to continue.

Accept Access Request

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

FIGURE 10 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, your next step depends on your Android version.

FIGURE 11 Installation Finished - Next Step Depends on Android Version



Do one of the following, depending on your Android version:

- If you are running Android version 6.0 or later, click the **Open** button, then follow the instructions in the [User Experience Example for Android Version 4.3, and Later](#) on page 27 section.
- If you are running a version earlier than Android 6.0, do *not* tap the **Open** button. Instead, use the **Back** arrow to return to the **Installation and Configuration** screen. Next, to run the configuration wizard, refer to the [Configure Application](#) on page 25 section.

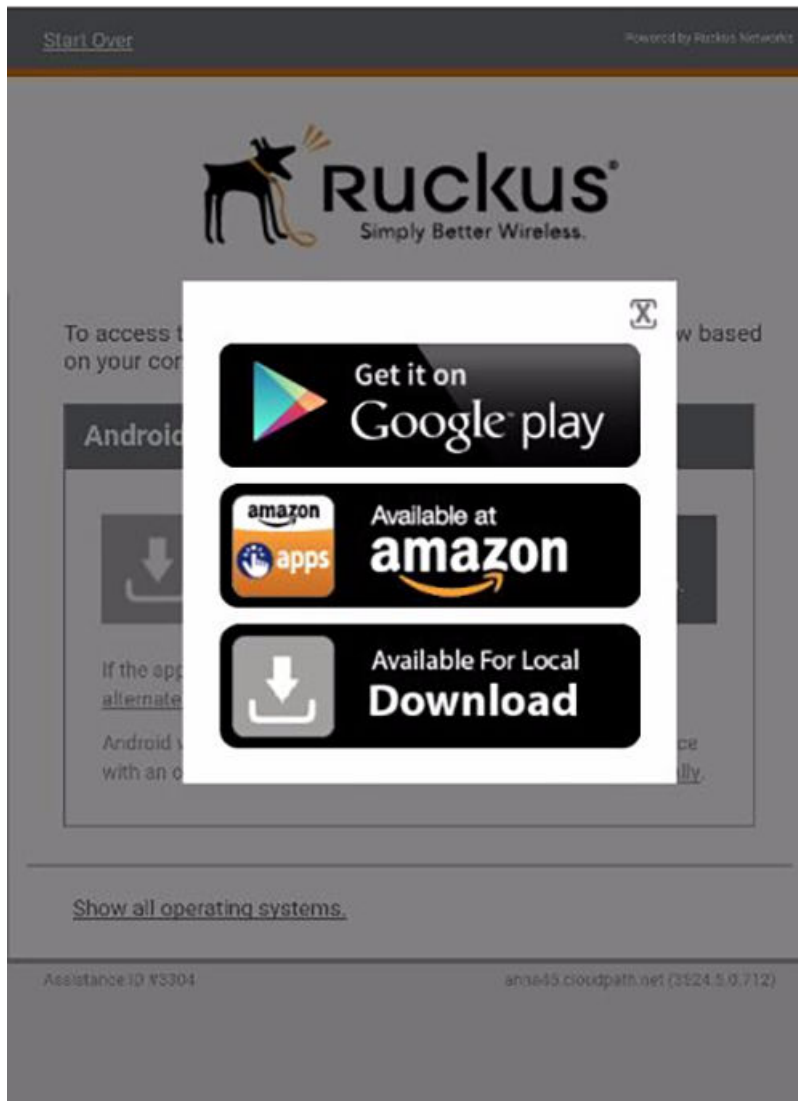
NOTE

If you are first returned to the Installation and Configuration screen, you might need to close the installation options pop-up. Refer to the [Close Download Options \(Android versions 5.0 and earlier\)](#) on page 19 section.

Close Download Options (Android versions 5.0 and earlier)

If you are returned to the **Installation and Configuration** screen, you might need to close the installation options pop-up.

FIGURE 12 Close Download Options Window

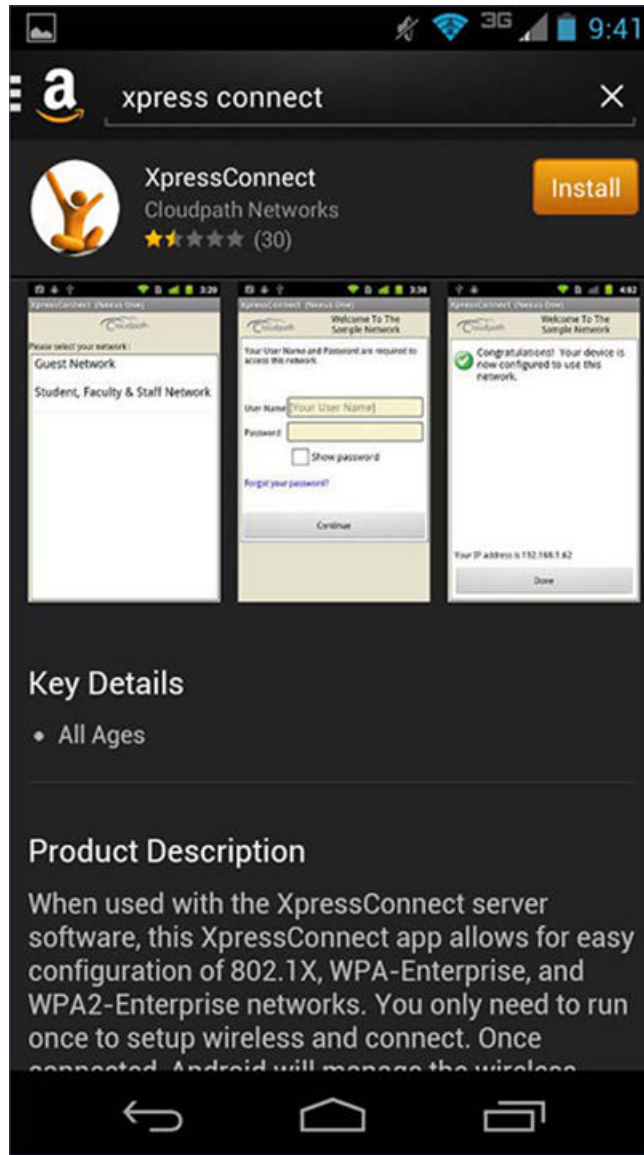


Tap the **X** in the top-right corner of the pop-up window to continue.

Install from Amazon Market

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

FIGURE 13 Install From Amazon Market

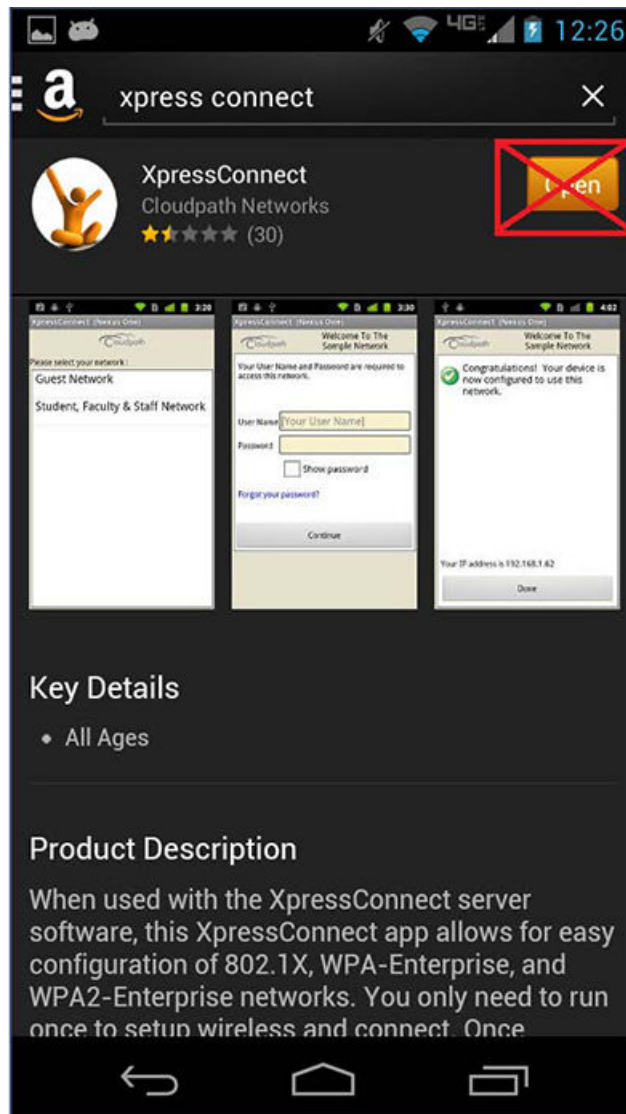


Click **Install** to start the installation process.

Return to Configuration Screen

After the application has been installed on the device, you might be prompted to open the application from the Amazon Market installation screen. Do *not* open the application from this screen.

FIGURE 14 Installation Finished

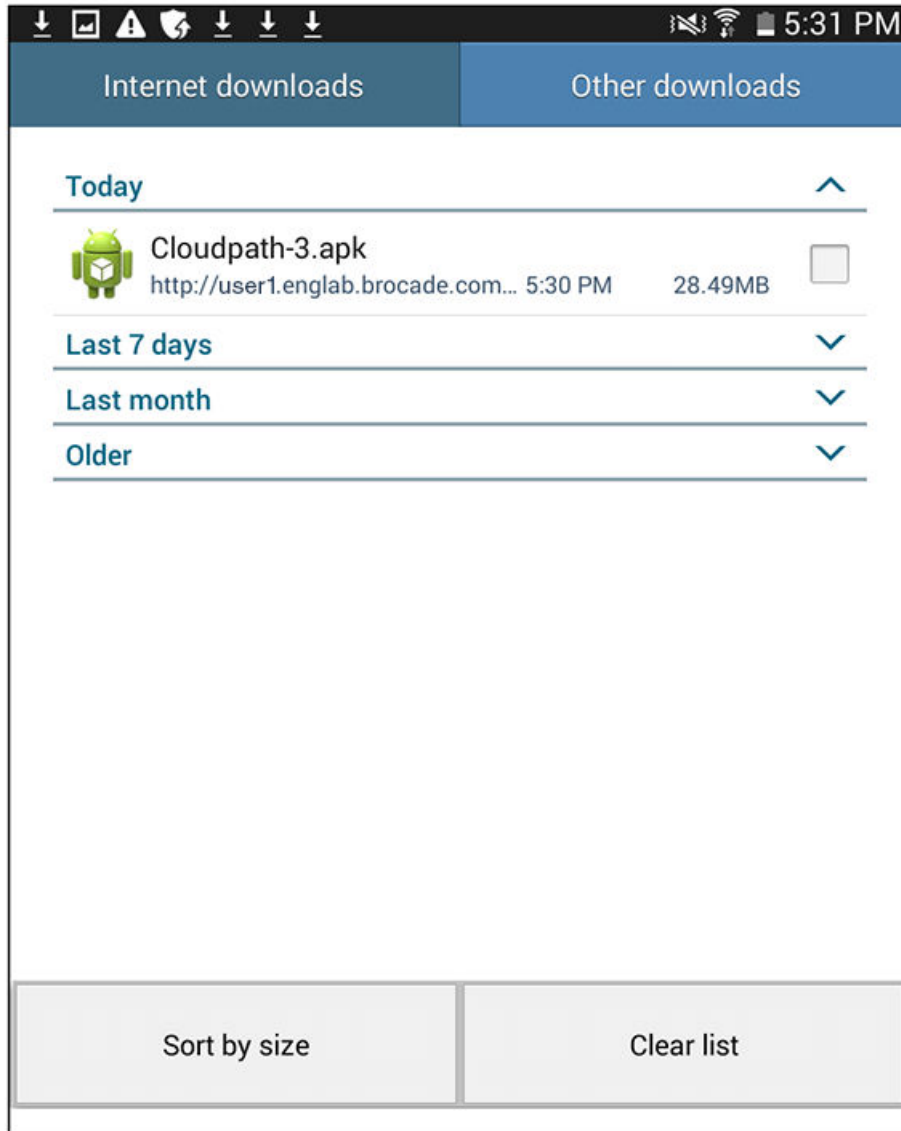


Do *not* tap the **Open** button. Instead, use the **Back** arrow to return to the **Installation and Configuration** screen. Next, to run the configuration wizard, refer to the [Configure Application](#) on page 25 section.

Local Download

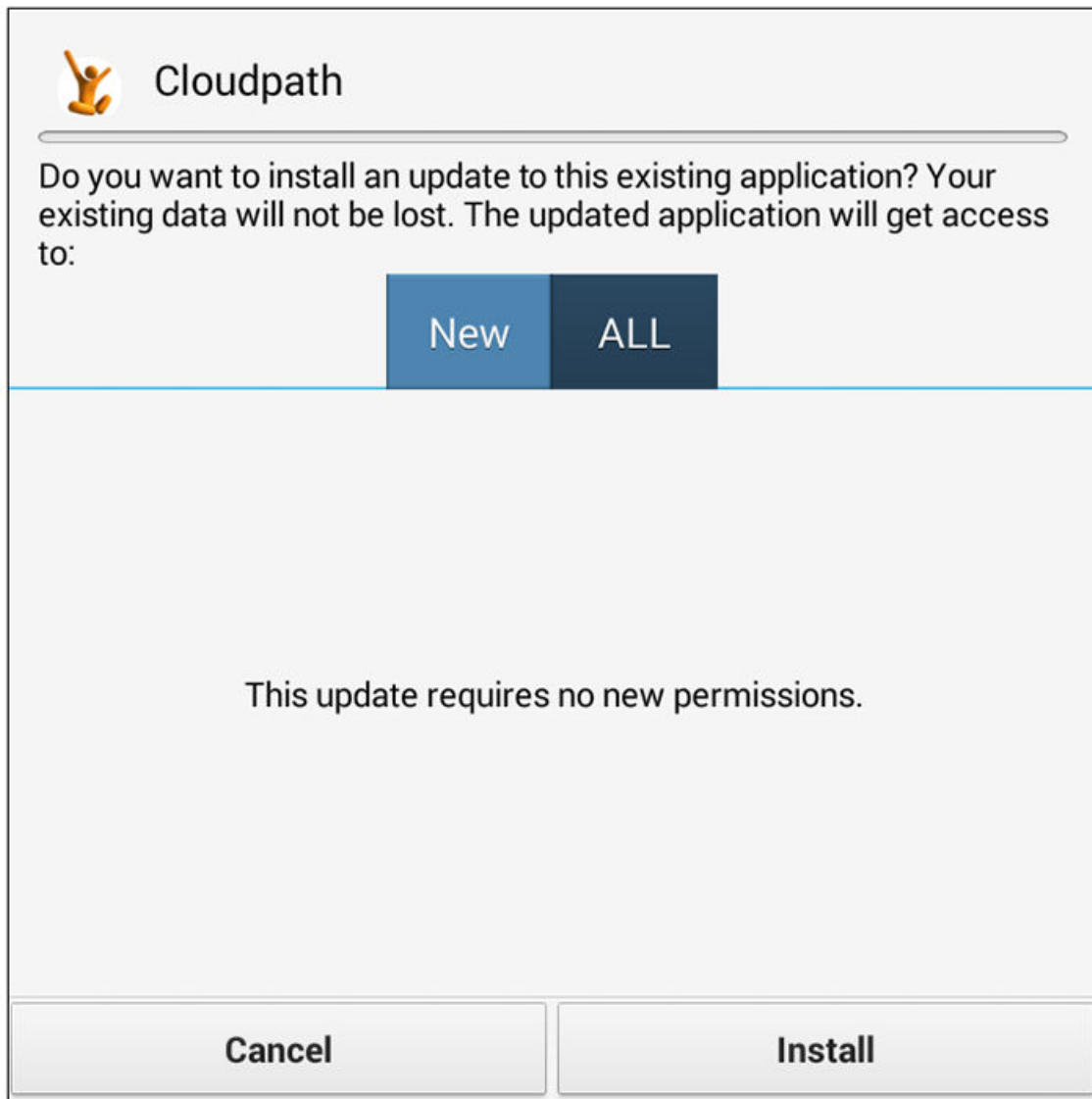
If permitted by the network configuration, the application is available for download from a local web server. Go to the device **Downloads** to locate the Cloudpath.apk file.

FIGURE 15 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 16 Install an Update?

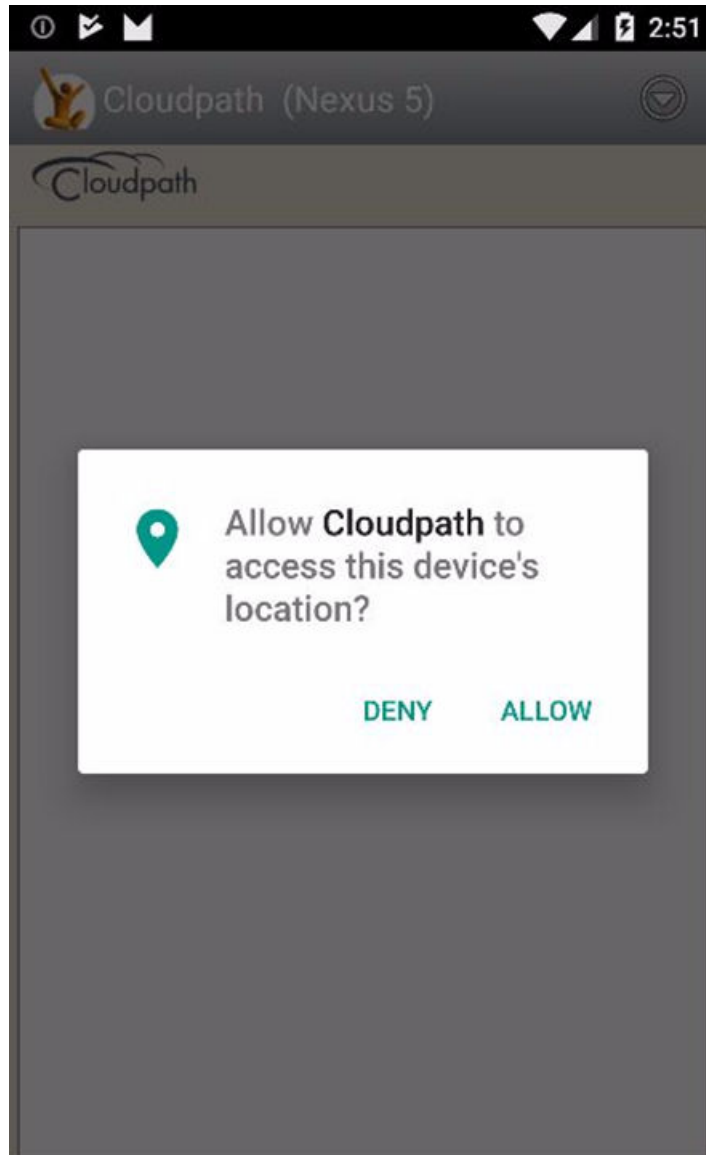


Select either New or ALL, and tap **Install**.

Accept Access Request

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

FIGURE 17 Access To Device Location

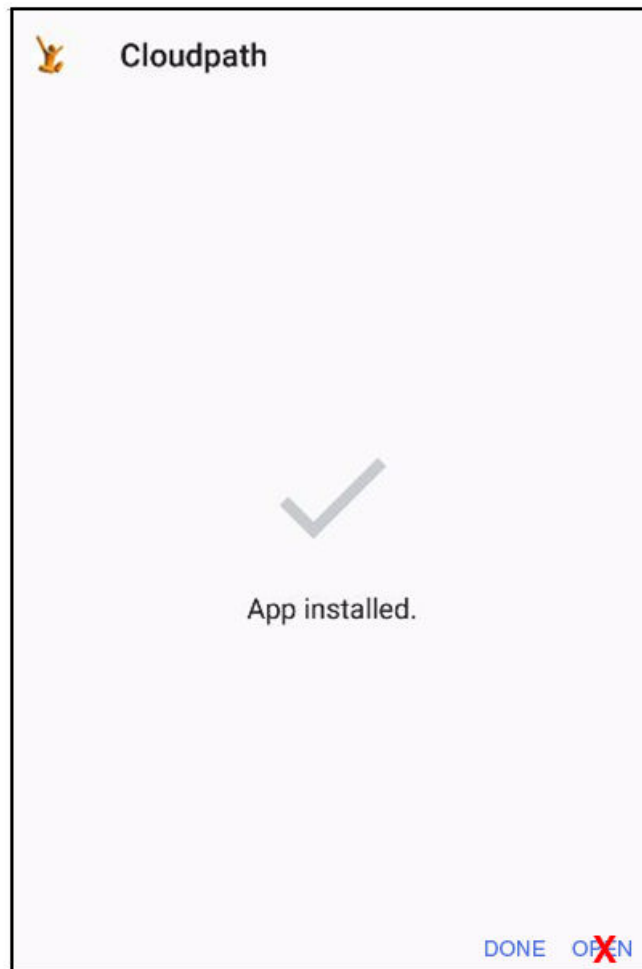


Click **Allow** to continue.

Return to Configuration Screen

After the application has been installed on the device, you might be prompted to open the application, as in the screen shown below. Do *not* open the application from this screen.

FIGURE 18 Application Installed

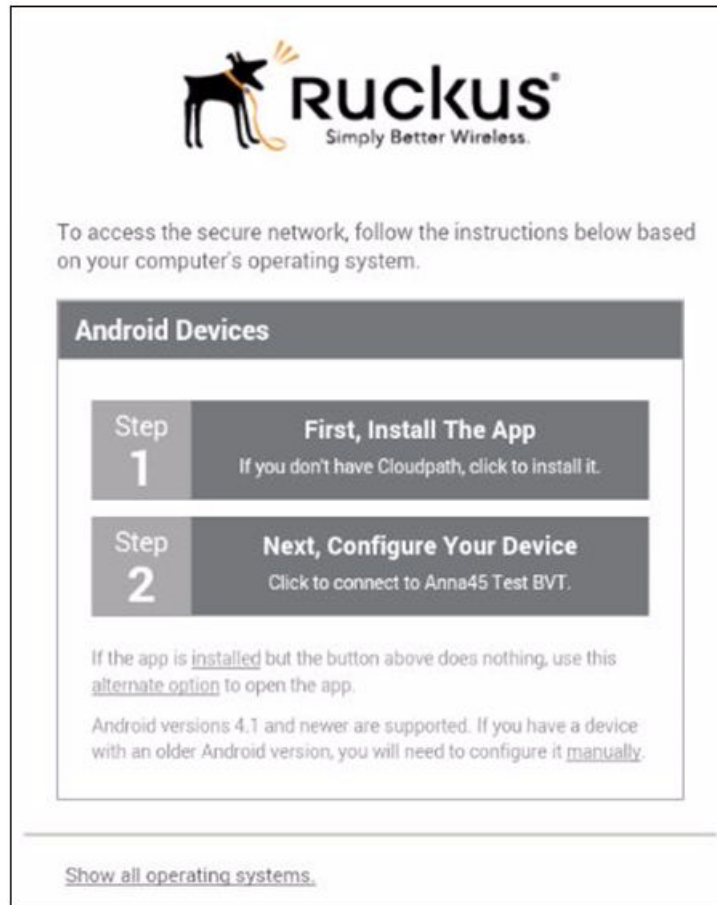


Click **Done**, then return to the **Installation and Configuration** screen. To run the configuration wizard, refer to the [Configure Application](#) on page 25 section.

Configure Application

Only if you are running Android versions 5.0 or earlier, you must return to the **Installation and Configuration** screen shown below, and tap **Next, Configure Your Device**.

FIGURE 19 Configure Your Device



NOTE

If your device does not respond to the Configure link (like certain Samsung devices), there is an alternative option link for launching the application.

After the application is installed, the Wizard opens to start configuring the device.

See the following sections for an example of the Wizard user experience on Android devices.

Cloudpath Wizard User Experience

- Introduction..... 27
- User Experience Example for Android Version 4.3, and Later.....27
- User Experience Example for Android Version 4.2, and Earlier..... 29

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.

NOTE

The user experience is slightly different for devices running Android OS version 4.3, and earlier than it is for devices running newer Android versions. Namely, in the older versions, you are prompted to install the credentials into the keystore.

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

User Experience Example for Android Version 4.3, and Later

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

For the user experience for devices running older Android versions, see User Experience Example for Android Version 4.2, and Earlier.

Network Monitored Message

On certain Android devices, the OS is programmed to bring up this 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 20 Attempting to Connect



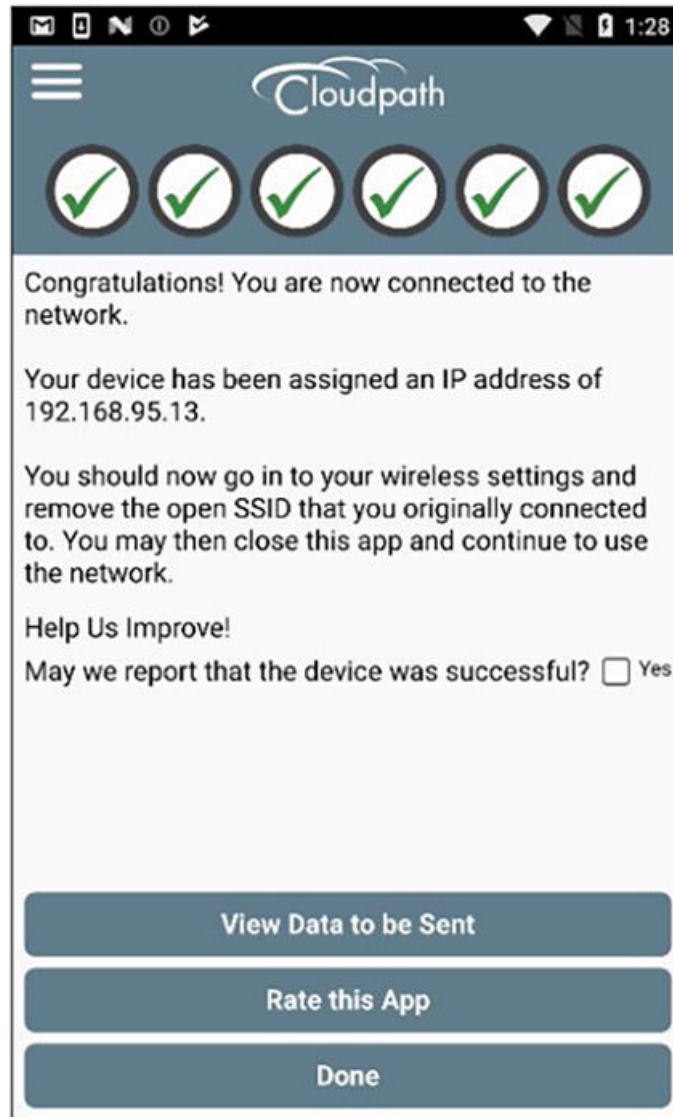
NOTE

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 21 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.

User Experience Example for Android Version 4.2, and Earlier

The user experience is slightly different for devices running Android OS version 4.2, and earlier. Namely, the user is prompted to install the credentials into the keystore.

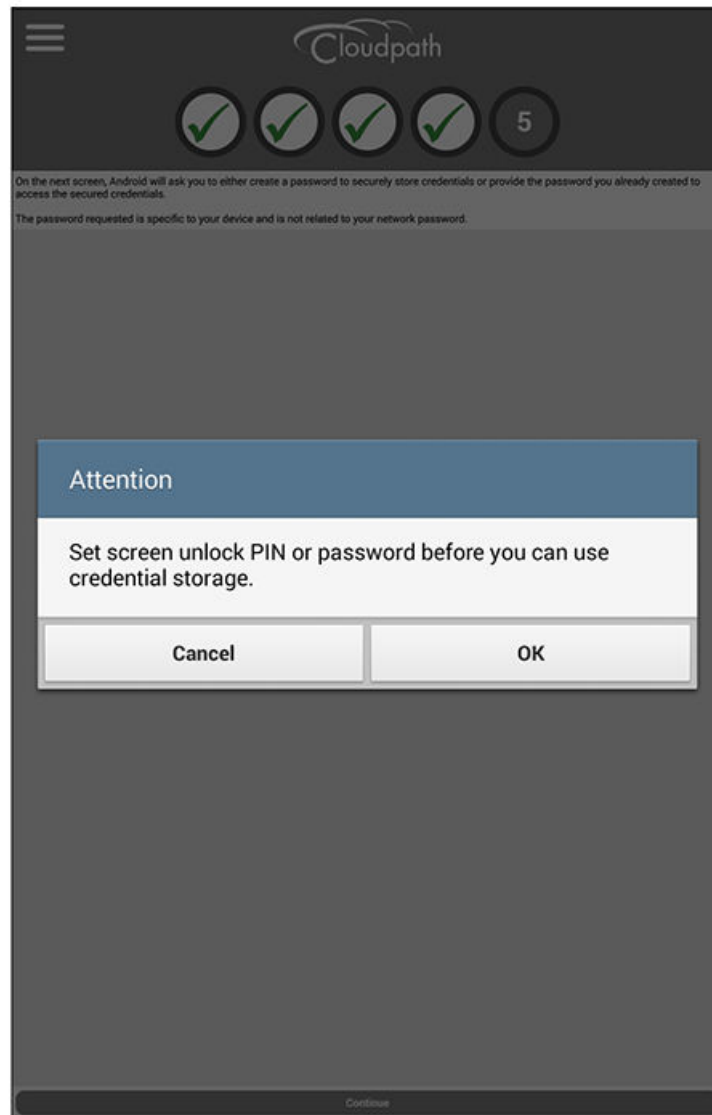
Before each certificate prompt, the application displays a message that tells you how to respond on the credential extraction and installation screens.

Passcode PIN or Pattern Lock

The Android OS requires the user to enter your passcode PIN or pattern to unlock the keystore and install the certificates on the device.

The application provides instructions for responding to these prompts. Read each screen carefully and respond as directed to the screens that follow.

FIGURE 22 Prompt to Respond to Passcode Lock



Tap **OK** to continue.

If requested, confirm the screen lock passcode to allow the application to install the certificate into the keystore.

NOTE

Certain Android devices do not allow a pattern to secure the keystore. This is a function of the Android OS and not the Cloudpath application. In these cases, the user is prompted to enter a PIN passcode for the screen lock before they can continue.

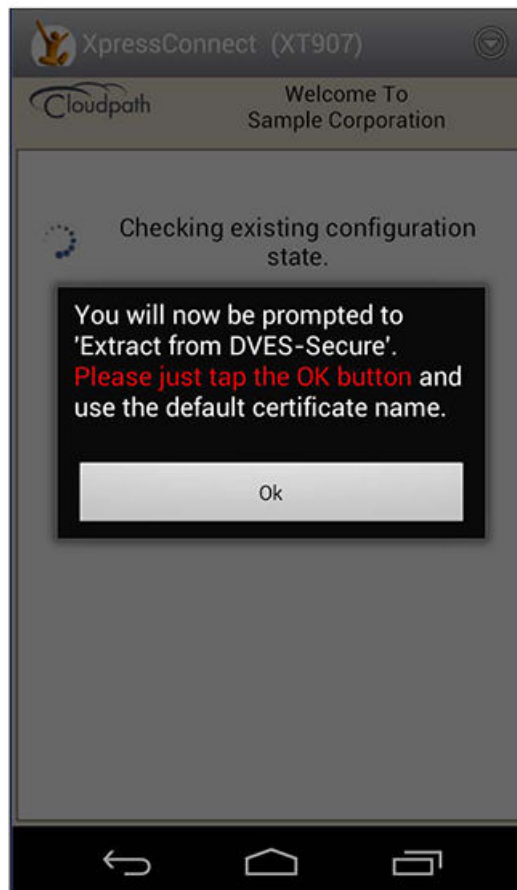
Enter the passcode PIN or pattern lock to continue.

How to Respond to Certificate Installation Prompts

Before each certificate prompt, the application displays a message that tells the user how to respond on the following credential extraction and installation screens.

Read each screen carefully and respond as directed to the screens that follow.

FIGURE 23 How to Respond to Certificate Prompts



Tap **OK** to continue.

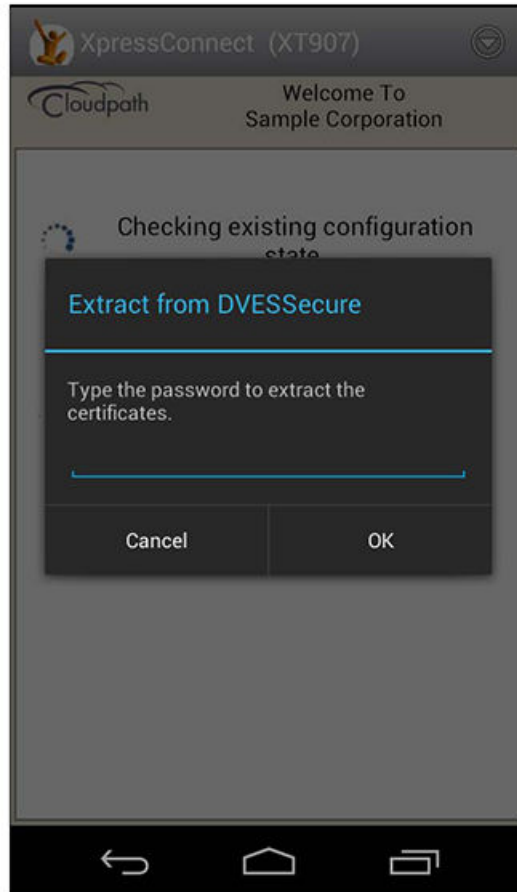
Extract Certificate

The device requires access to the keystore to extract the certificate.

Cloudpath Wizard User Experience

User Experience Example for Android Version 4.2, and Earlier

FIGURE 24 Password to Extract the Certificate

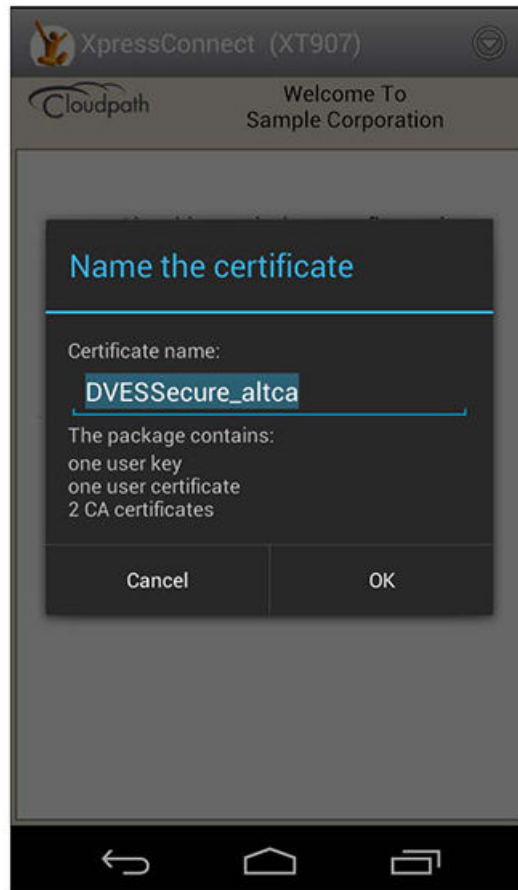


Tap **OK** to extract the certificate, as instructed on the previous screen.

Name the Certificate

The application pre-populates the certificate name based on the network configuration.

FIGURE 25 Name the Certificate



If the previous screen indicated that you must enter a certificate name, enter it on this screen. Otherwise, tap **OK** to keep the default name.

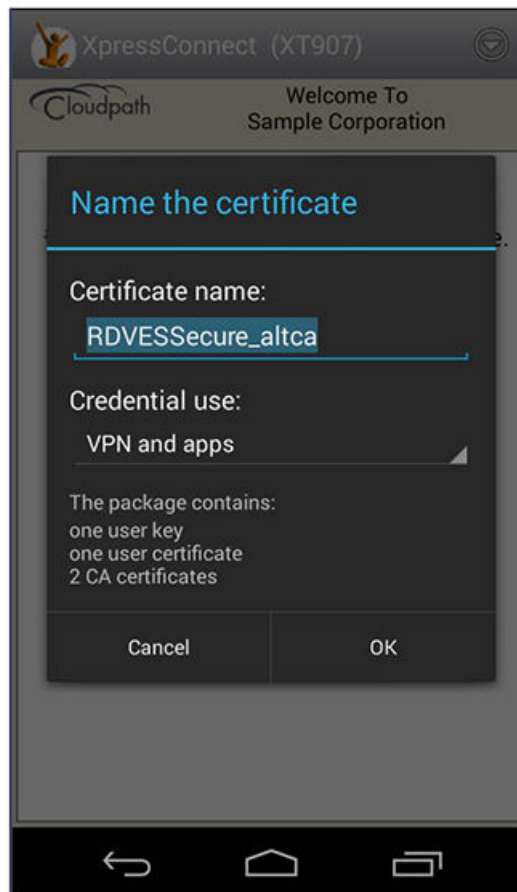
NOTE

If the network has been configured for additional credentials, you might be required to repeat the previous 3 steps (Message, Extract, Name Certificate).

Alternate Credential Store

If the OS settings require that the user certificate be installed in the web browser store, you might see this prompt for the alternate credential store.

FIGURE 26 VPN and Apps Certificate Store

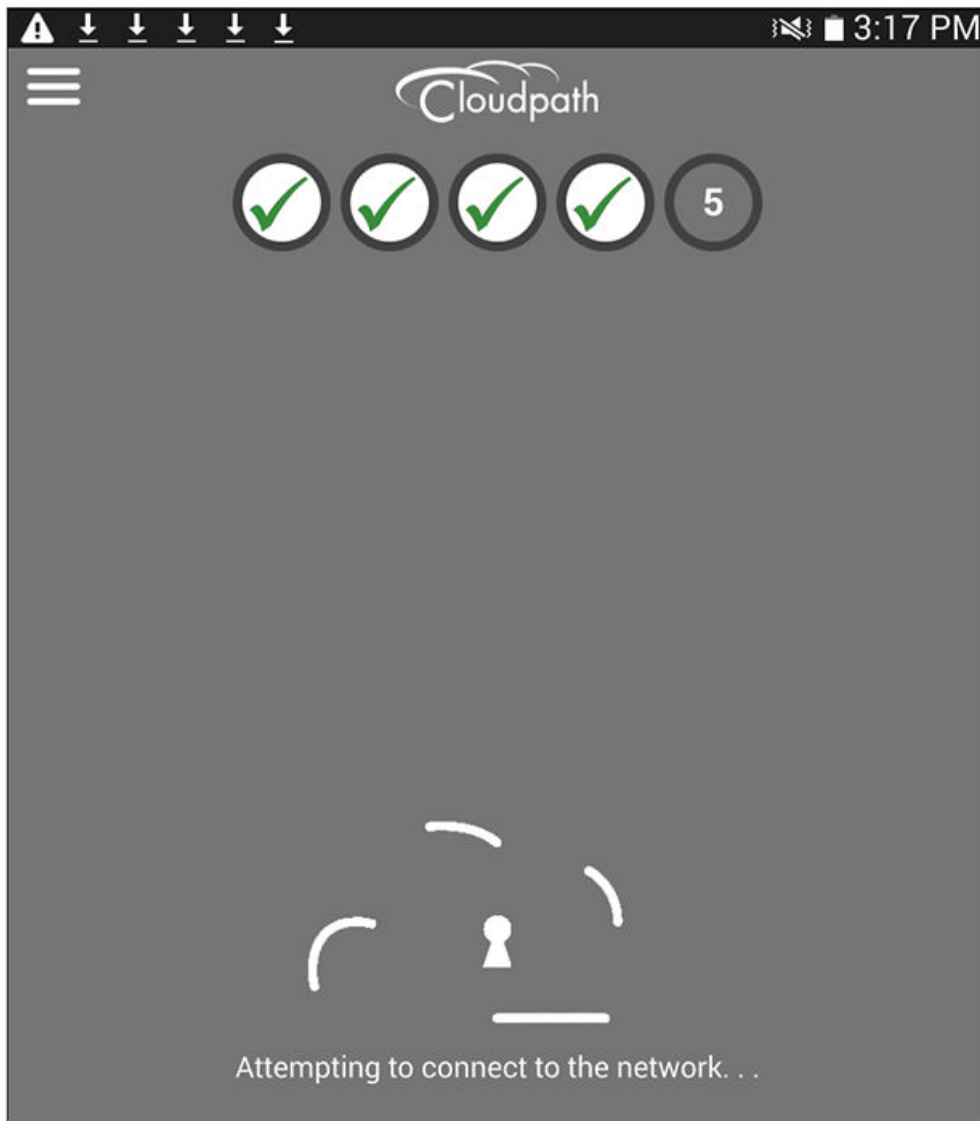


Tap **OK** to continue.

Attempting to Connect to the Network

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

FIGURE 27 Attempting to Connect



The application continues the connection process without user intervention.

Validating Connectivity

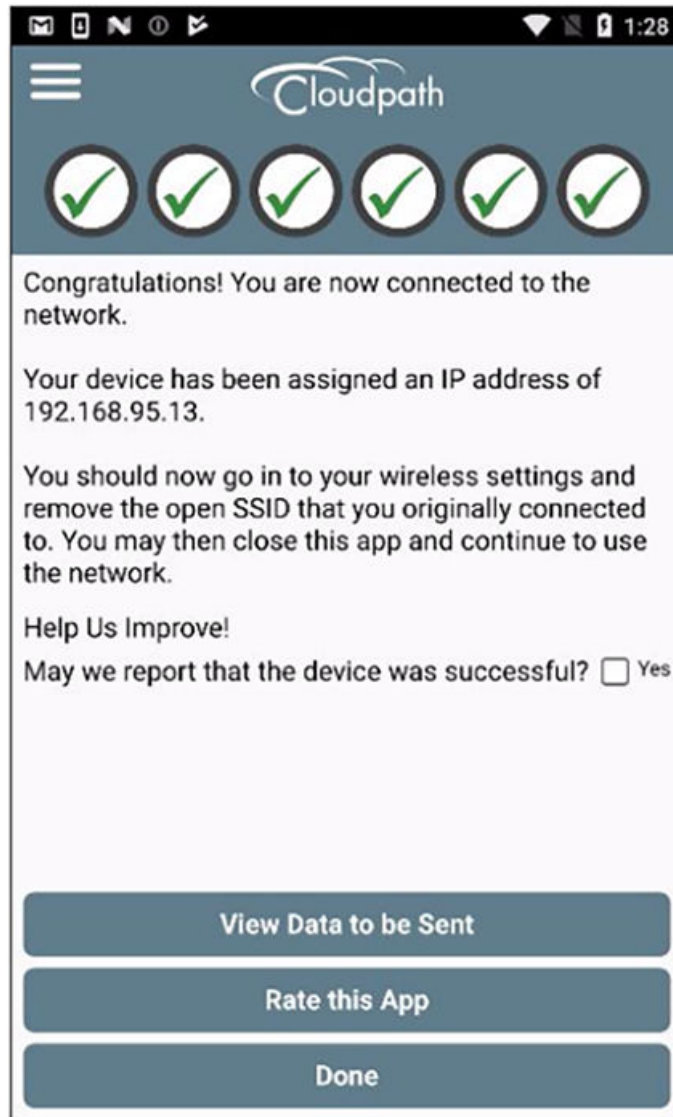
The Wizard ensures that association and authentication are successful, and verifies that an IP address is received. A screen appears briefly to indicate that connectivity is being validated.

The application continues the connection process without user intervention.

Connected

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

FIGURE 28 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..... 37
- Retrieve Log Files..... 37
- Passwords and Lock Screen PINs.....38
- Blank Certificate Field..... 39
- Certificate Passwords.....39
- Android .netconfig File..... 39
- Memory Card..... 39
- Uninstalling the Application.....39

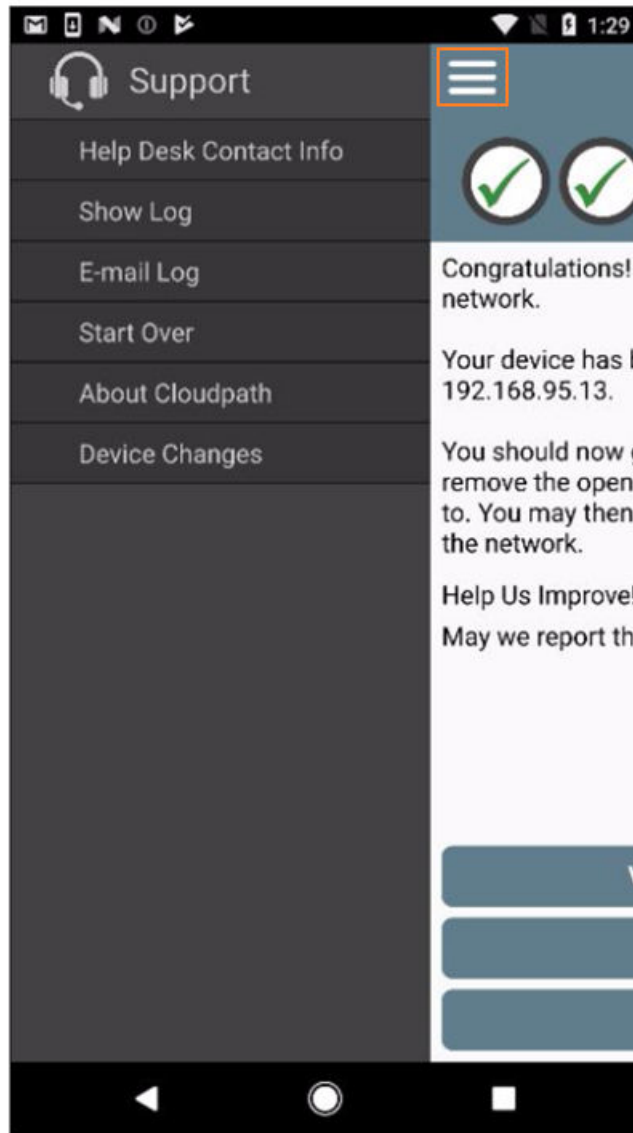
Common Android Issues

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 29 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. On Android versions prior to version 4.0, a password is needed to access the key store. From versions 4.0 through 6.0, 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.



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