

Cloudpath End-User Experience for BlackBerry Devices

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

- Overview..... 4
 - Supported BlackBerry Versions.....4
- Cloudpath User Experience.....4
 - Enrollment Steps.....4
 - BlackBerry Configuration Instructions.....9
 - Download Certificates..... 11
 - Import Certificates..... 16
 - Configure Wi-Fi Settings.....28

Overview

The Cloudpath Enrollment System (ES) automates WPA2-Enterprise configuration on any device that connects to the network and automatically connects the device to a secure SSID. This Automated Device Enablement (ADE) means authorized devices onboard simply and securely, with the appropriate level of access.

Cloudpath supports all operating systems including Windows, Mac OS X, iOS, Android, Linux, Chromebooks, and more.

This document provides an example of the end-user process for using Cloudpath to migrate a BlackBerry device to the secure network.

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.

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

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

Cloudpath User Experience

Cloudpath provides the prompts that guide the user through the sequence of steps that make up the enrollment workflow. During this process, the user enters information as requested, and makes selections about user type, device type, among others. 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.

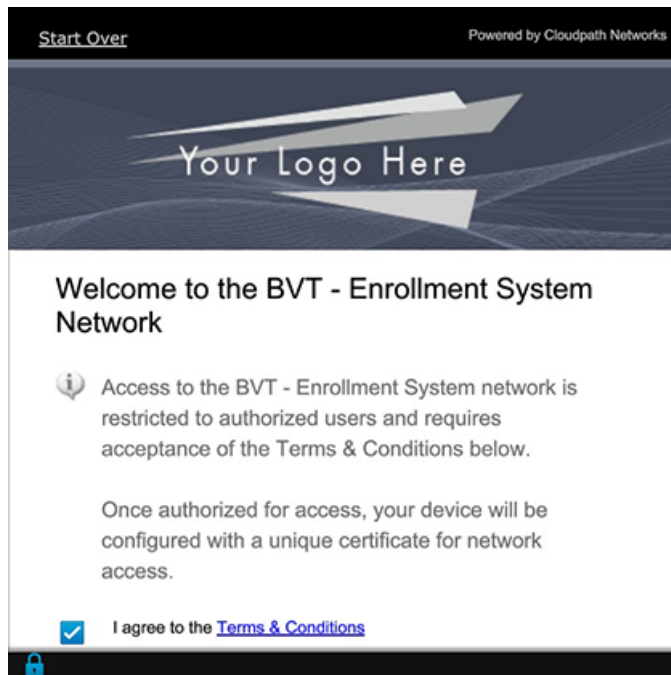
Welcome Screen With AUP

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 1 Enrollment Welcome Screen

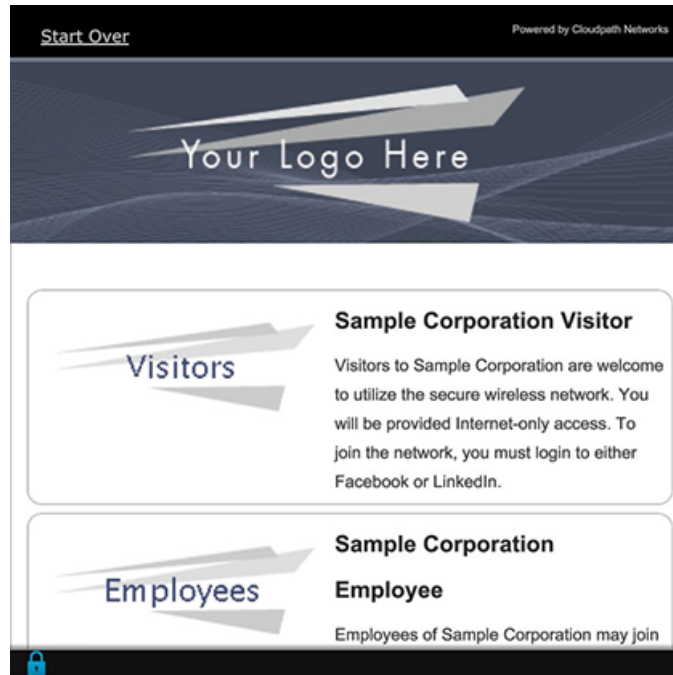


An acceptable use policy (AUP) prompt displays a message and requires that the user signal acceptance to continue. The text on the **Welcome** page and **Start** button can be customized.

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 Visitor might be required to enroll using their social media credentials.

FIGURE 2 User Type Prompt



Select the user type to continue. This example enrollment 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

Start Over Powered by Cloudpath Networks

Your Logo Here

Your username and password are required to access the network.

Username:

Password:

[Need Assistance?](#)

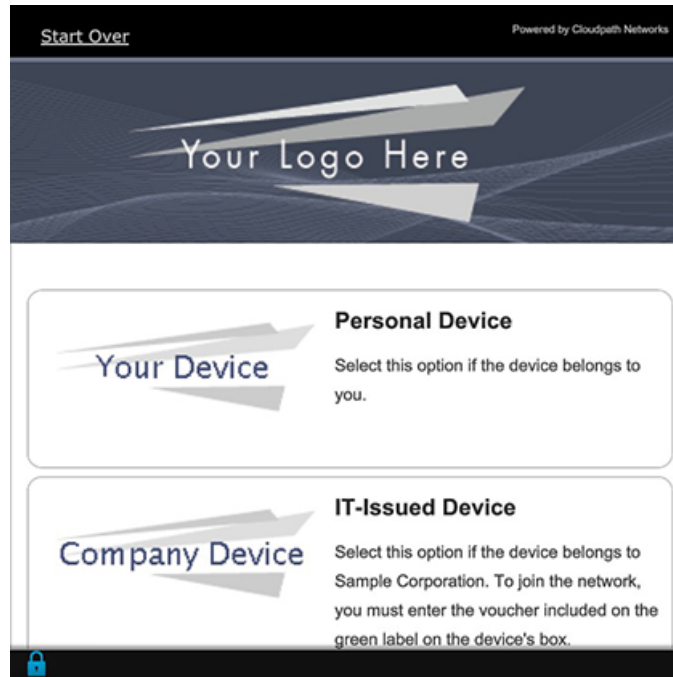
Previous Next

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

Device Type

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

FIGURE 4 Device Type Prompt

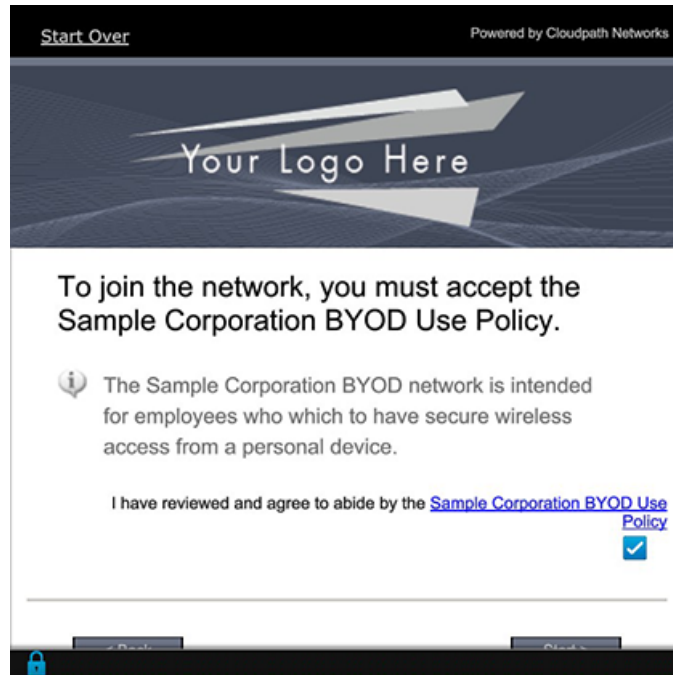


Select a device type to continue. This example follows the **Personal Device** workflow.

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 **Start** button.

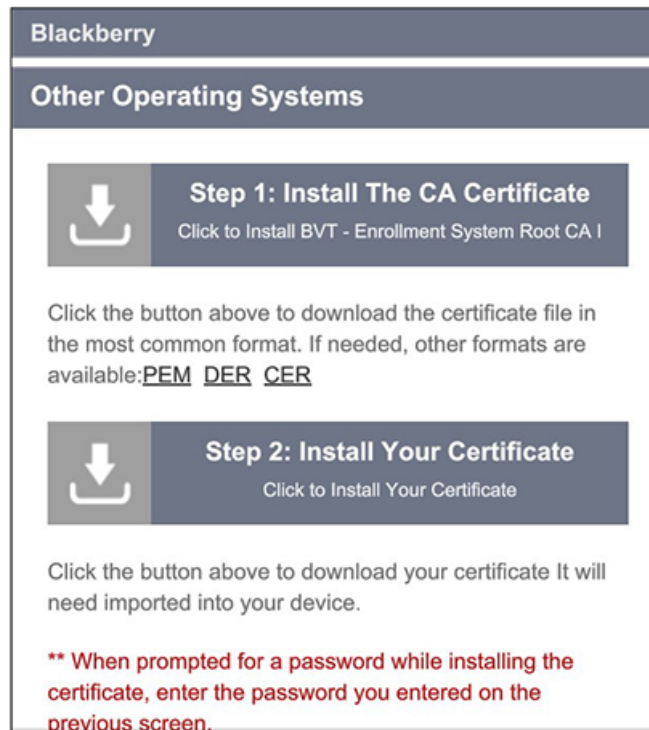
BlackBerry Configuration Instructions

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 6 BlackBerry Instructions - Steps 1-2



The screenshot shows a BlackBerry configuration screen titled "Blackberry" with a sub-header "Other Operating Systems". It contains two main steps:

- Step 1: Install The CA Certificate**
Click to Install BVT - Enrollment System Root CA I
- Step 2: Install Your Certificate**
Click to Install Your Certificate

Below Step 1, there is a paragraph: "Click the button above to download the certificate file in the most common format. If needed, other formats are available: [PEM](#) [DER](#) [CER](#)".

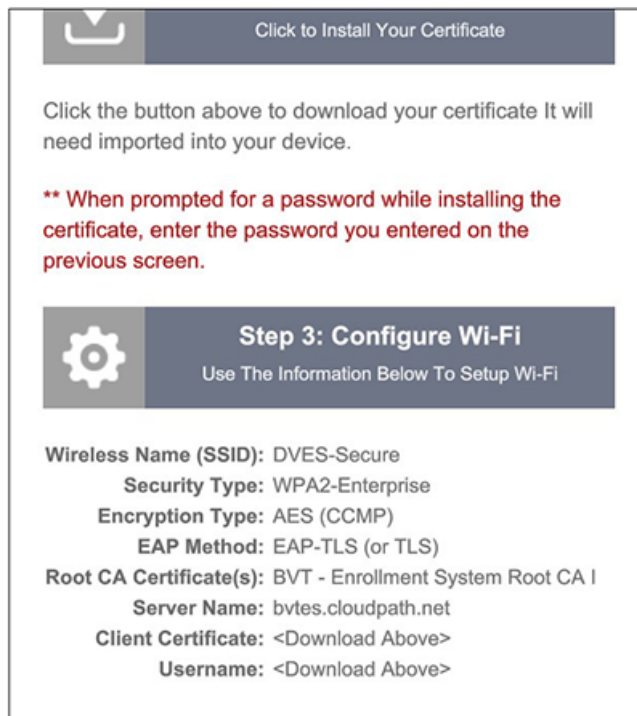
Below Step 2, there is a paragraph: "Click the button above to download your certificate It will need imported into your device."

At the bottom, there is a red note: "** When prompted for a password while installing the certificate, enter the password you entered on the previous screen."

Configure Wi-Fi Instructions

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

FIGURE 7 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.

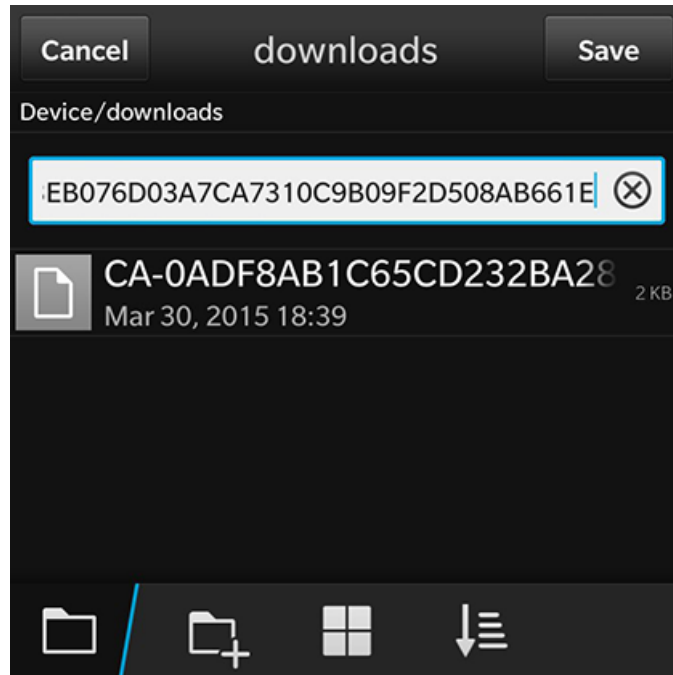
Download CA Certificates

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 8 Save CA Certificate

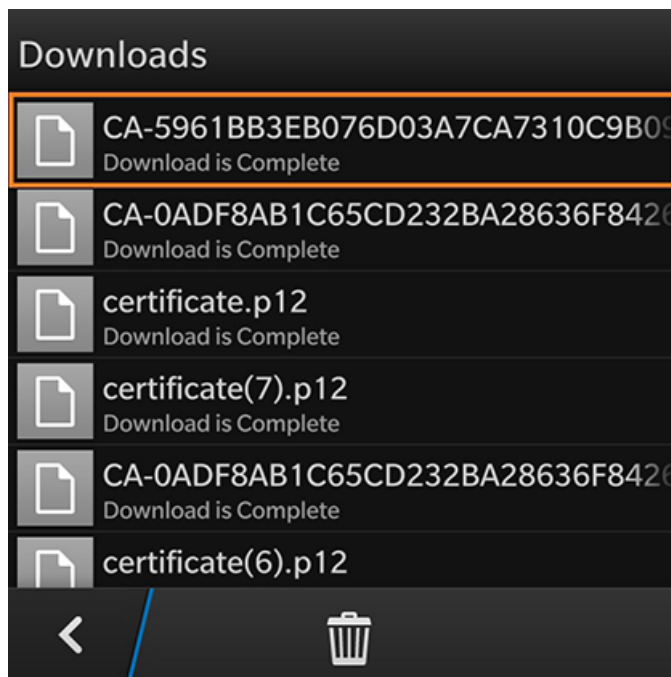


Tap **Save** to download the certificate. The screen displays a brief message to confirm that the download was complete.

CA Certificate in Downloads Folder

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

FIGURE 9 CA Certificate



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

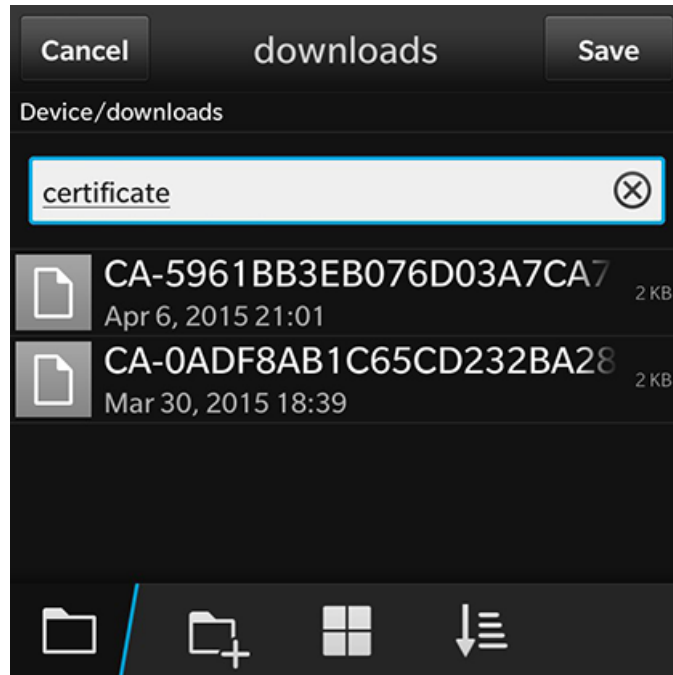
Download User Certificate

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 10 Save User Certificate

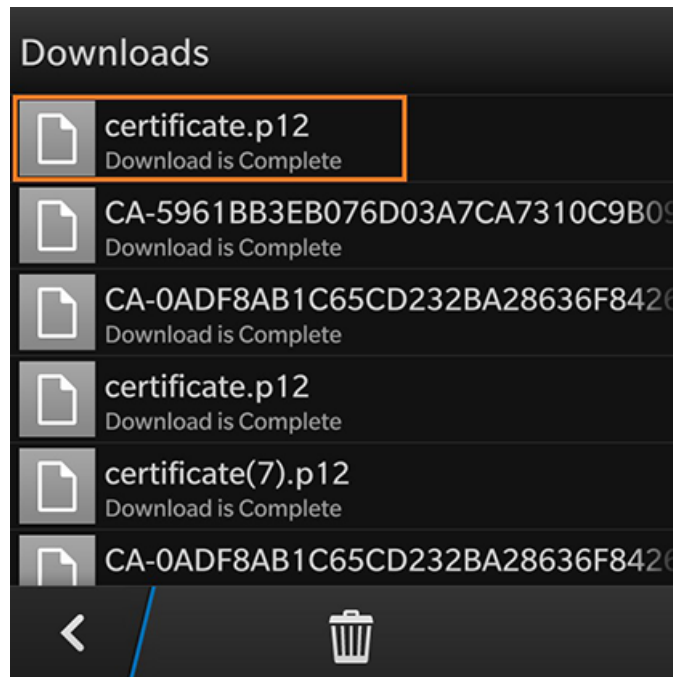


Tap **Save** to download the certificate. The screen displays a brief message to confirm that the download was complete.

User Certificate in Downloads Folder

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

FIGURE 11 User Certificate

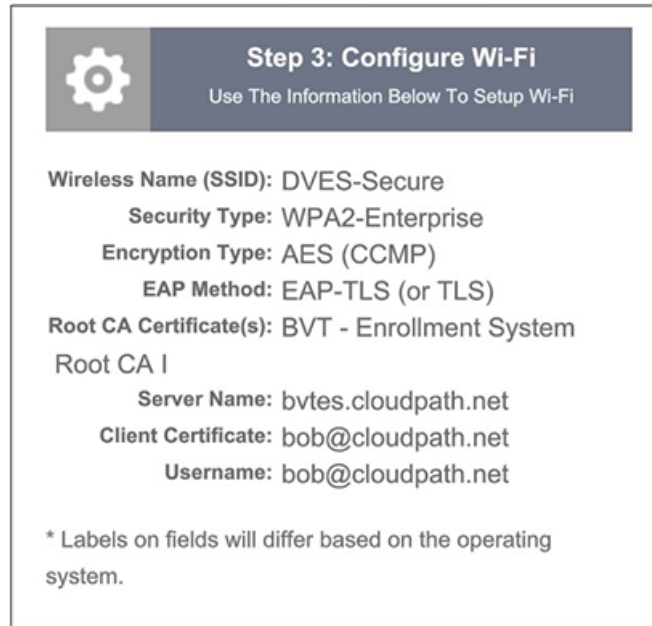


Tap the back arrow at the bottom left to return to the configuration instructions screen.

Configuration Instructions

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

FIGURE 12 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.

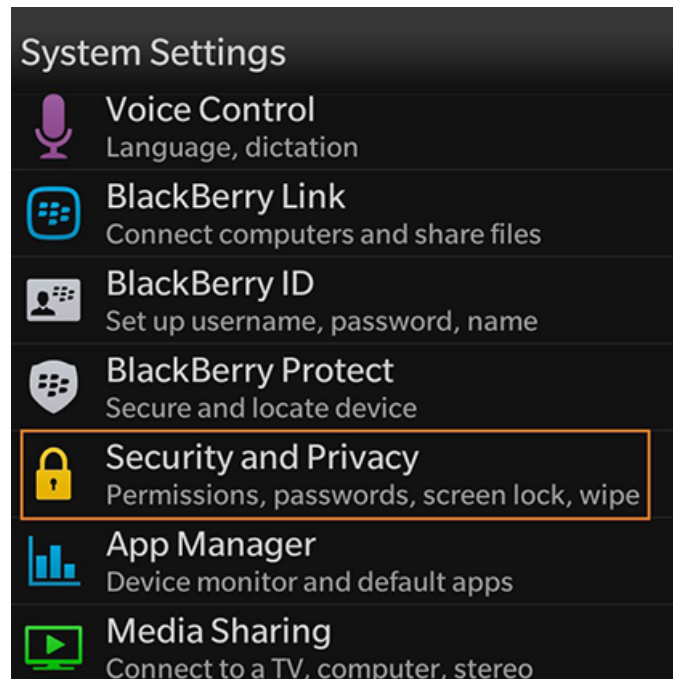
Import Certificates

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 13 System Settings for Importing Certificates

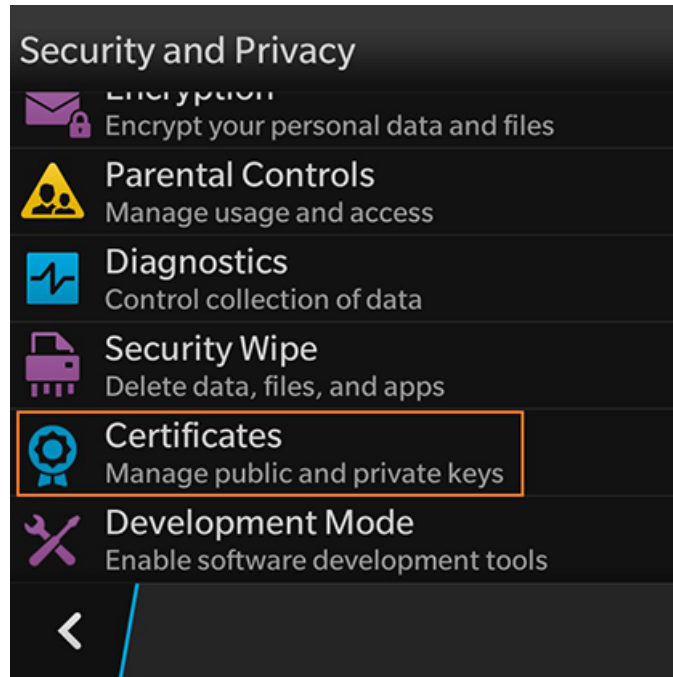


Tap **Security and Privacy** to continue.

Security and Privacy Settings

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

FIGURE 14 Security and Privacy Settings

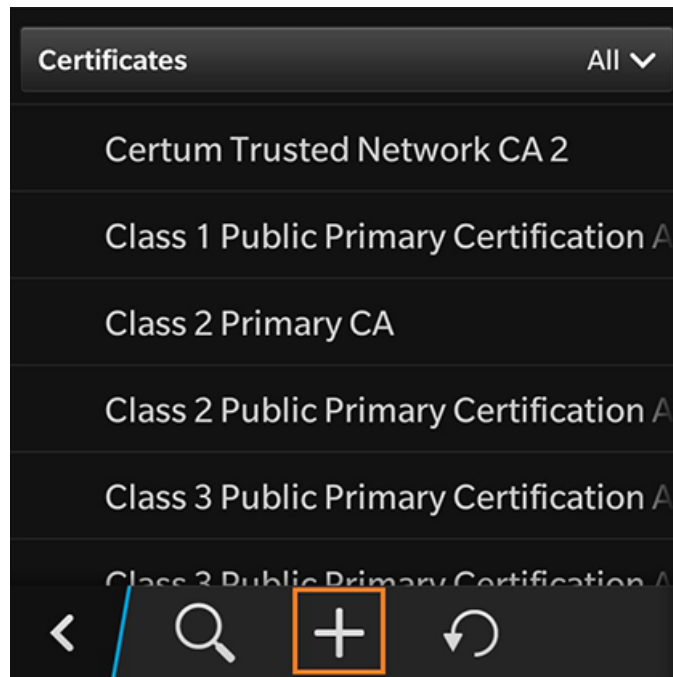


Tap **Certificates** to continue.

Add Certificate

The certificate store is displayed.

FIGURE 15 Add Certificate

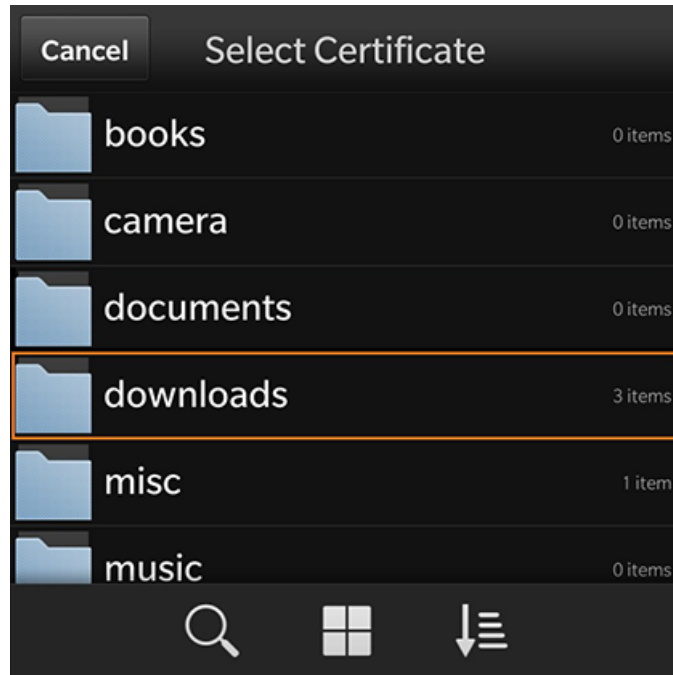


Click the plus sign to add a CA certificate.

Select Downloads Folder

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

FIGURE 16 Select Downloads Folder

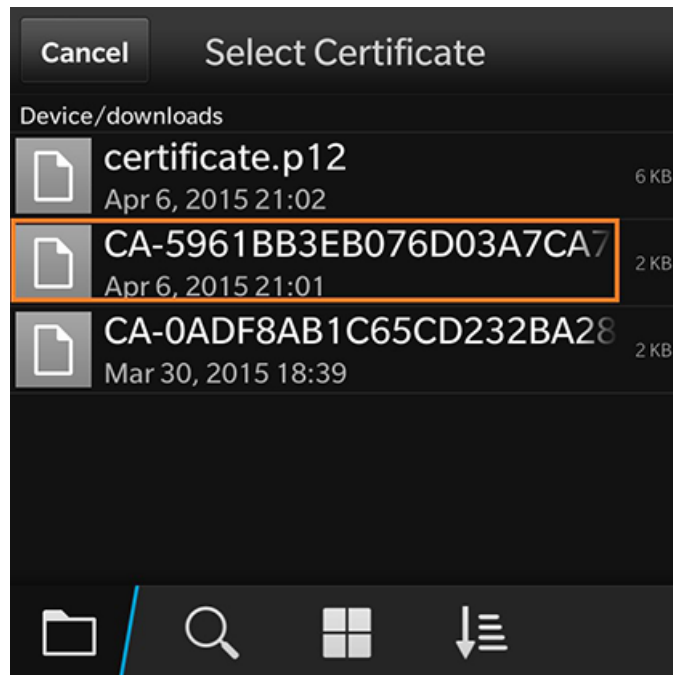


Tap the **Downloads** folder to view the certificates available for import.

Select CA Certificate

Select the CA certificate that was previously downloaded.

FIGURE 17 Select CA Certificate

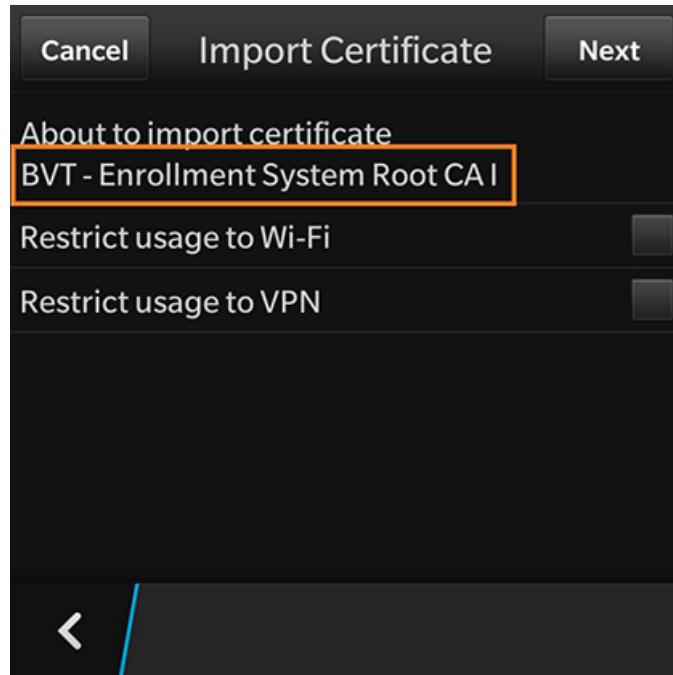


Tap the CA certificate to import.

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 18 CA Certificate Settings



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

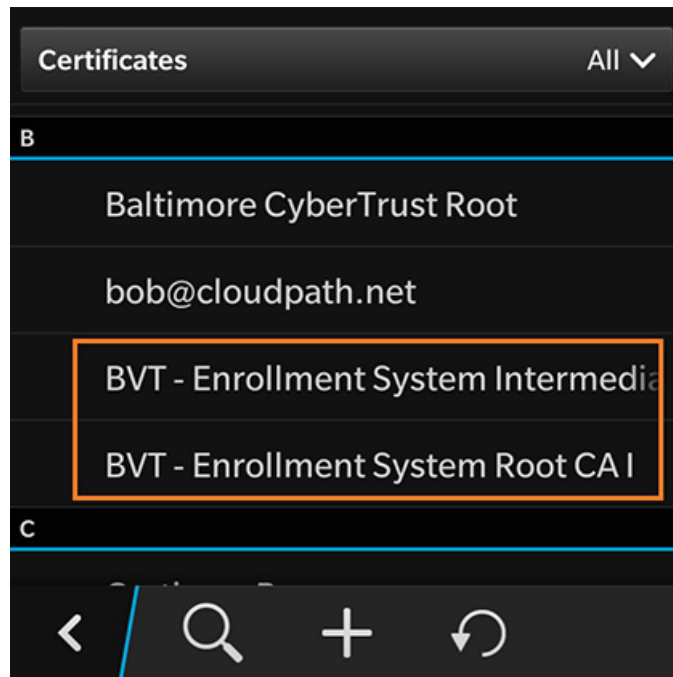
Certificate Imported

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 19 Certificate Imported

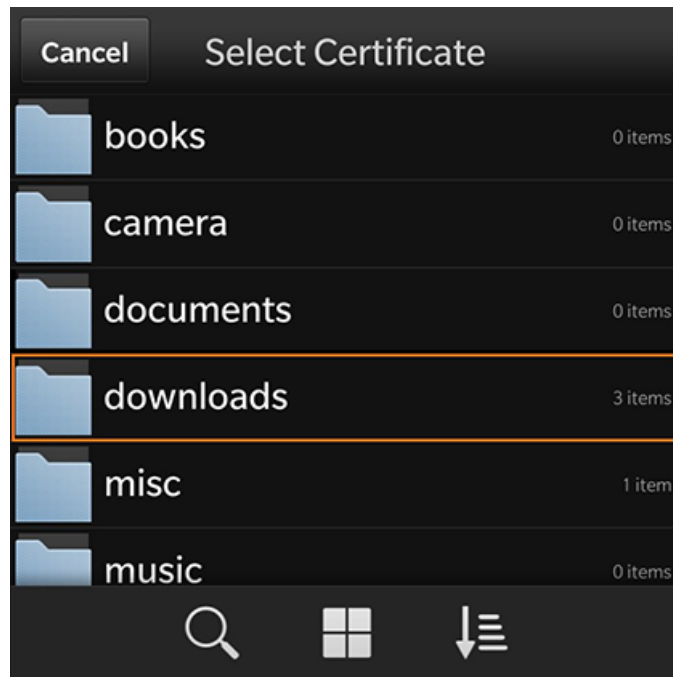


Click the plus sign to add the User certificate.

Select Downloads Folder

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

FIGURE 20 Select Downloads Folder

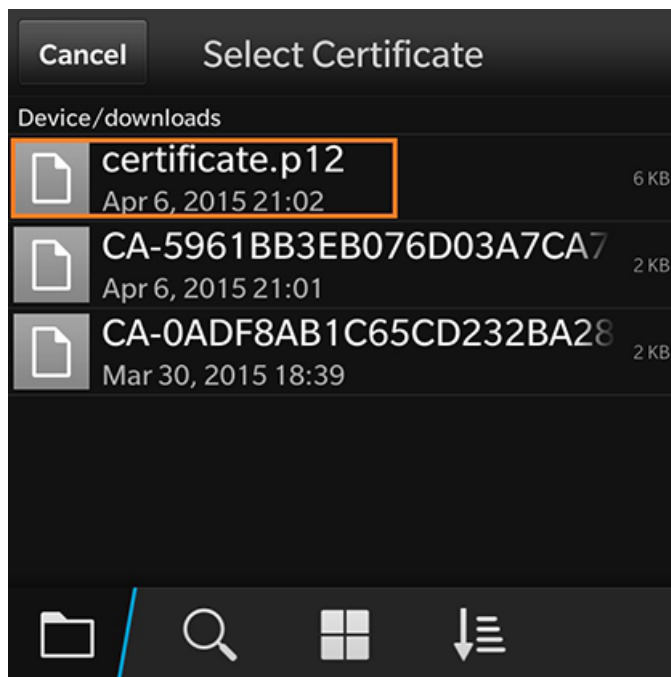


Tap the **Downloads** folder to view the certificates available for import.

Select User Certificate to Import

Select the user certificate that was previously downloaded.

FIGURE 21 Select User Certificate

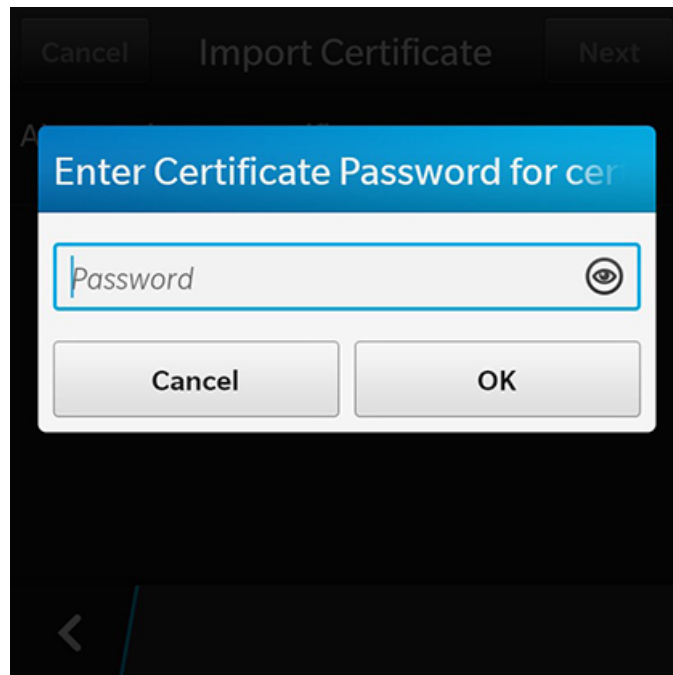


Tap the user certificate to import.

Enter User Certificate Password

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

FIGURE 22 Enter Password for User Certificate



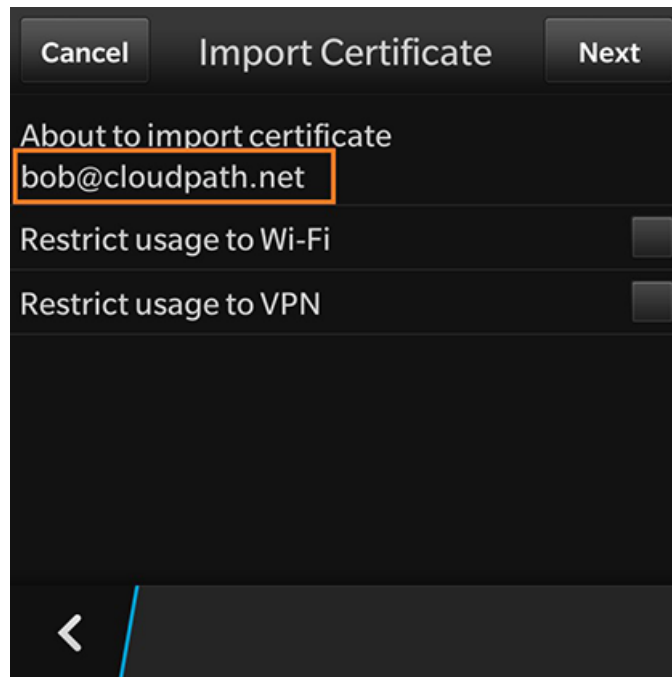
Enter the password from your user credentials. For example, if your user credentials are username=bob and password=bob1, then enter **bob1** for the user certificate password.

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 23 User Certificate Settings for Importing a Certificate

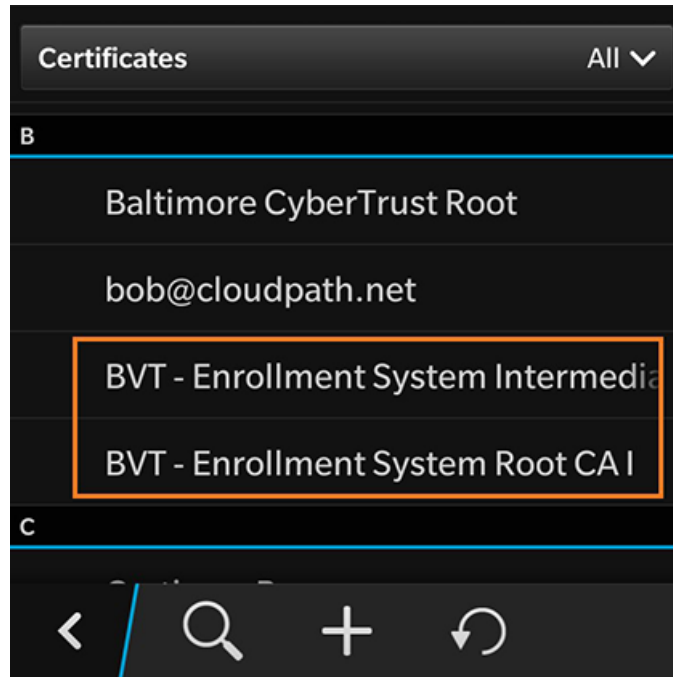


Tap the back arrow at the bottom left to return to the certificate store.

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 24 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 25 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 26 Networks and Connections



Select **Wi-Fi** to continue.

Wi-Fi Networks

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

FIGURE 27 Wi-Fi Settings

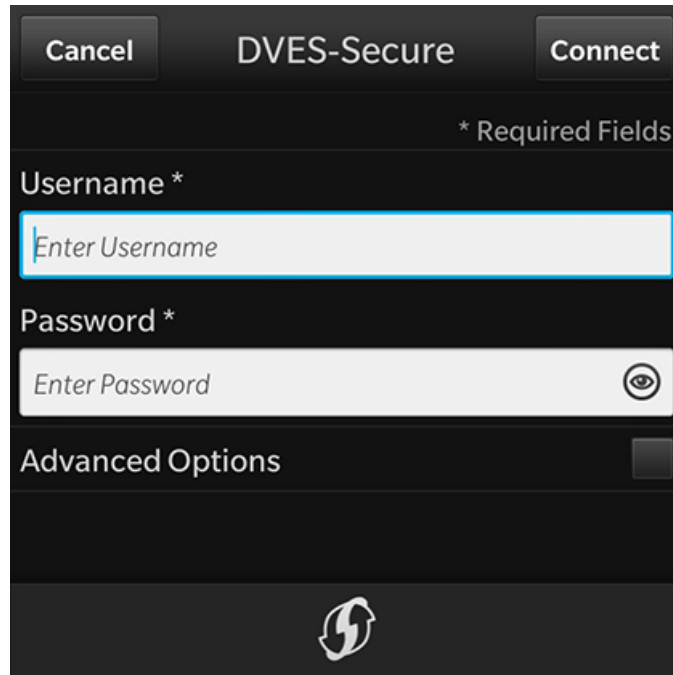


Swipe through the list of **Available Networks** to locate the **Wireless Network Name** from the configuration instructions. See the **Configuration Instructions** section to review the correct settings.

Wi-Fi Settings - User Credentials

The secure wireless settings require your user credentials.

FIGURE 28 User Credentials for Wireless Network

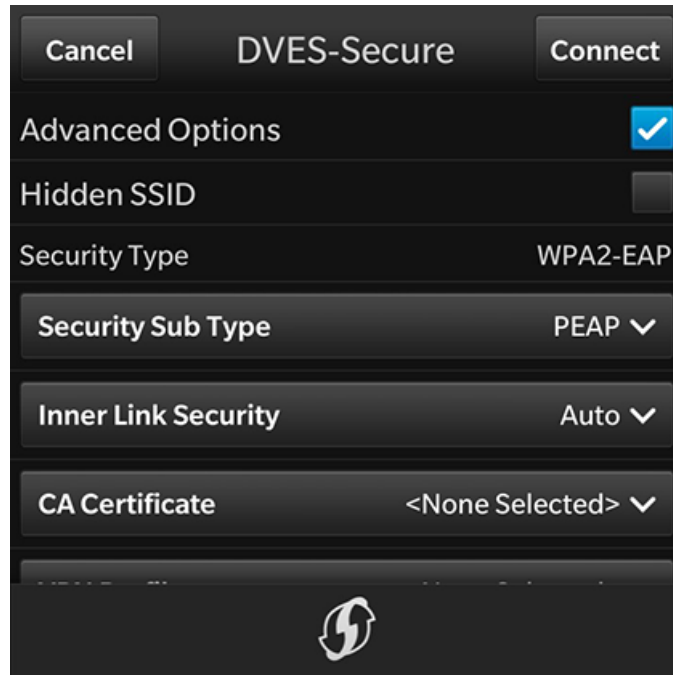


Enter the same user credentials from the enrollment workflow steps. See the User Credentials section to review these settings.

Advanced Options

The secure wireless network requires additional settings.

FIGURE 29 Advanced Options

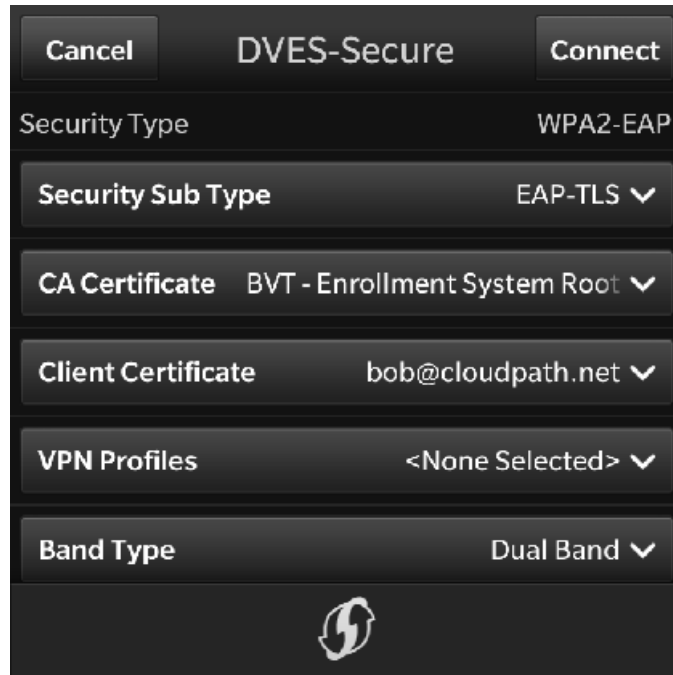


Check the **Advanced Options** box to expose additional wireless configuration settings.

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 30 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

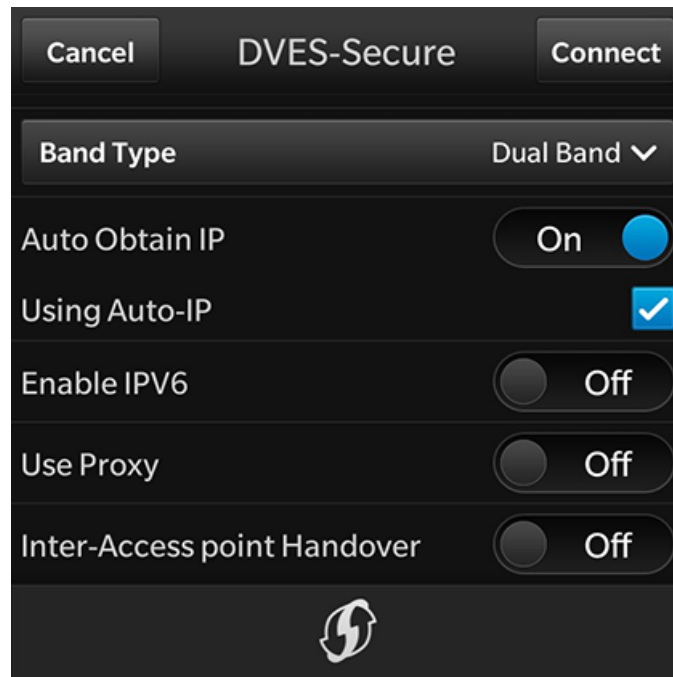
Wi-Fi Settings - Optional Settings

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 31 Optional Settings



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

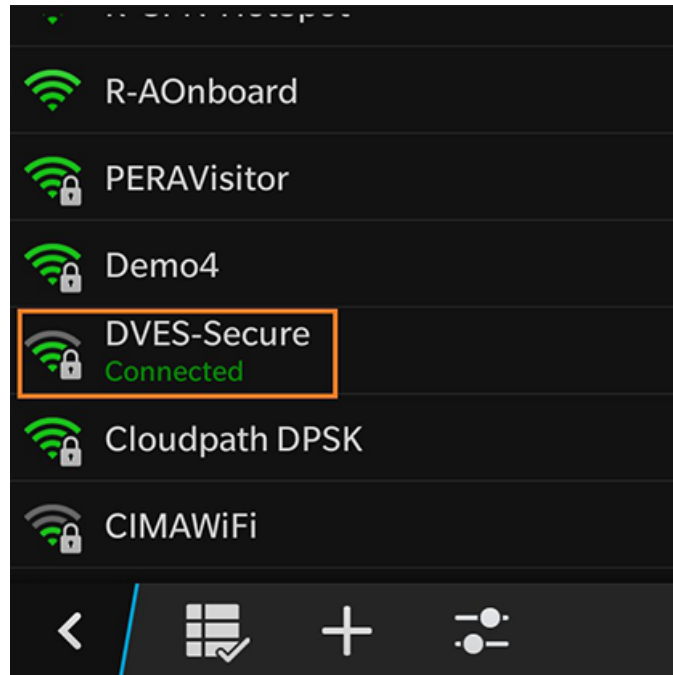
- Auto Obtain IP = On
- Using Auto-IP = Selected
- Enable IPV6 = Off
- Use Proxy = Off
- Inter-Access point Handover = Off

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

Device Connected

You should now be connected to the secure wireless network.

FIGURE 32 Device Connected



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



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