

Cloudpath

Enrollment System

End-User Experience for Linux Devices

Software Release 4.3

April 2016

Summary: This document describes the end-user experience for devices running the Fedora or Ubuntu operating system and using the Cloudpath ES to onboard to a secure wireless network.

Document Type: Information

Audience: Network Administrator, End-User



End-User Experience for Linux Devices

Software Release 4.3

April 2016

Copyright © 2016 Ruckus Wireless, Inc. All Rights Reserved.

This document contains Ruckus Wireless confidential and proprietary information. It is not to be copied, disclosed or distributed in any manner, in whole or in part, without express written authorization of a Customer Advocacy representative of Ruckus Wireless, Inc. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing, RUCKUS WIRELESS PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

ZoneFlex™, BeamFlex™, MediaFlex™, ChannelFly™, and the Ruckus Wireless logo are trademarks of Ruckus Wireless, Inc. All other brands and product names are trademarks of their respective holders.

Copyright © 2016 Ruckus Wireless, Inc. All rights reserved.

End-User Experience for Linux Devices

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.

The Cloudpath ES 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 the Cloudpath ES to migrate a device running a Linux operating system to the secure network.

Supported Versions

The Cloudpath ES supports the following Linux versions:

- Ubuntu version 9.04, and later
- Fedora version 18, and later

Cloudpath ES User Experience

The Cloudpath ES 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.

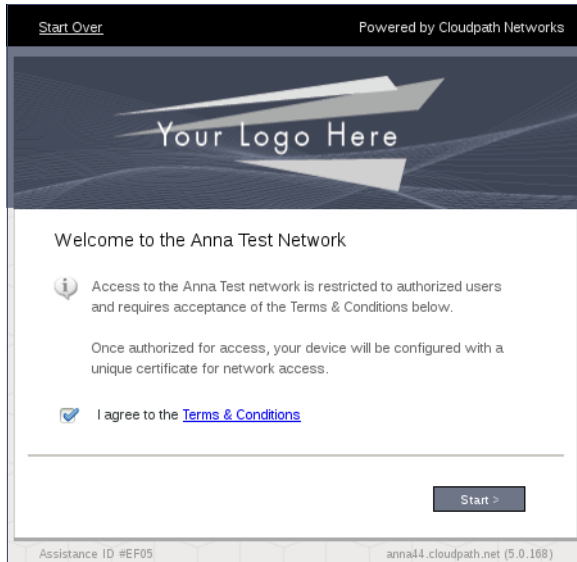
Welcome Screen With AUP

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 ES 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 page text and *Start* button may be customized. Click *Start* to continue.

User Type

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

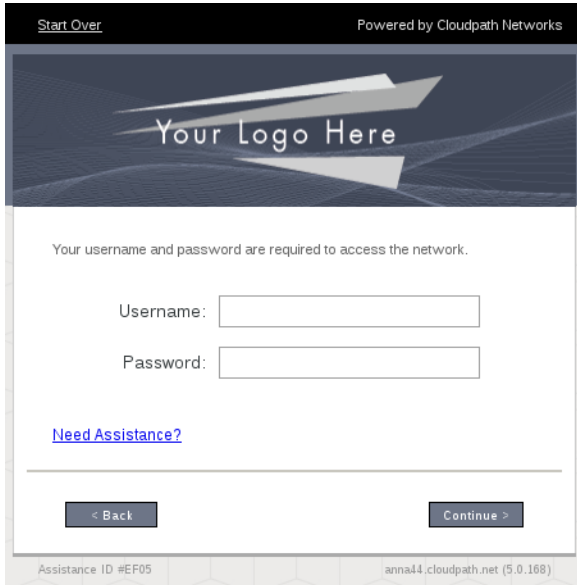


Select the user type to continue. This example follows the *Employee* workflow branch.

User Credentials

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

FIGURE 3. User Credential Prompt



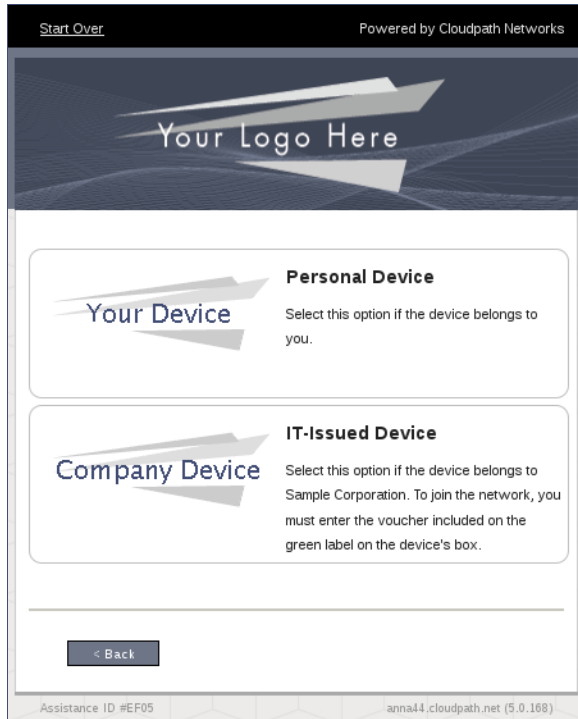
The screenshot shows a web-based user credential prompt. At the top left, there is a link labeled "Start Over". At the top right, it says "Powered by Cloudpath Networks". The main header area features a dark blue background with a white arrow graphic pointing right and the text "Your Logo Here". Below this, a message states: "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 password field is a blue link labeled "Need Assistance?". At the bottom of the form area, there are two buttons: "< Back" on the left and "Continue >" on the right. The footer of the page contains the text "Assistance ID #EF05" on the left and "anna44.cloudpath.net (5.0.168)" on the right.

Enter the user credentials and click *Continue*.

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 a IT-Issued Device would be allowed to bypass the MAC address prompt.

FIGURE 4. Device Type Prompt



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

Voucher Code

Your network might require that you enter a voucher (one-time password) as an additional verification step. Vouchers are typically sent email or SMS from a network sponsor or administrator.

FIGURE 5. Voucher Code Prompt

Start Over Powered by Cloudpath Networks

Your Logo Here

Congratulations on receiving a new device. The box of your device contains a green sticker. The sticker contains a voucher code in a format similar to SC000000. Please enter that voucher code below.

Voucher Code:

[Need Assistance?](#)

< Back Continue >

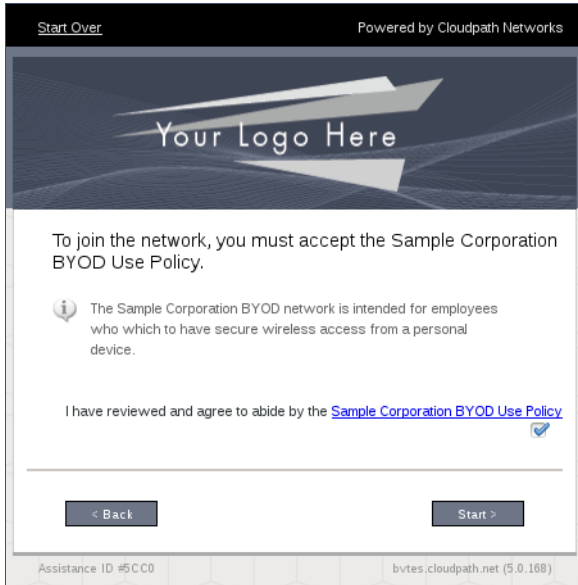
Assistance ID #EF05 anna44.cloudpath.net (5.0.168)

Enter the voucher code and click *Continue*.

BYOD Policy

Typically, you must agree to the terms and policies of the network before you can continue.

FIGURE 6. BYOD Policy



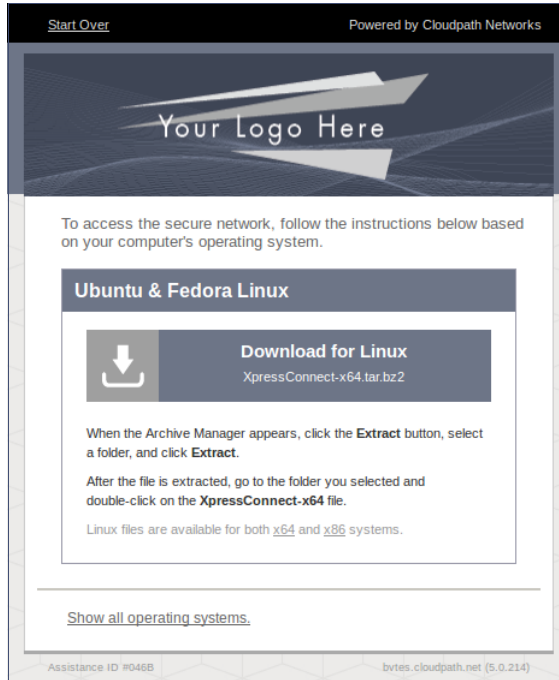
Click *Start* to continue.

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

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 7. Linux Download Page

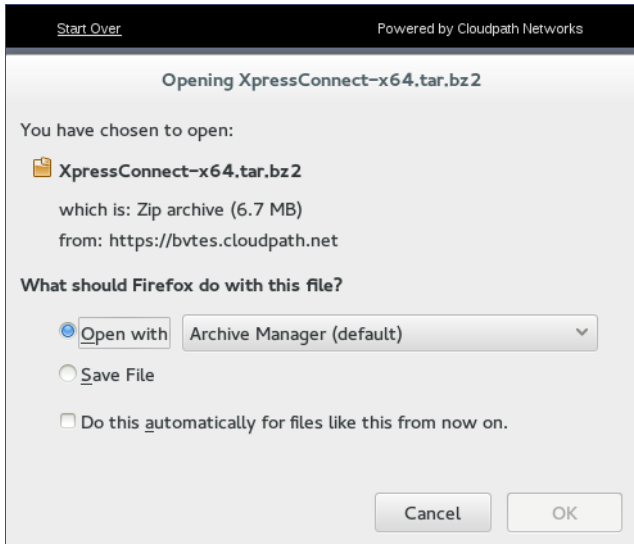


Click the down arrow to download the tar file, which contains the application files.

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 8. Open Download File

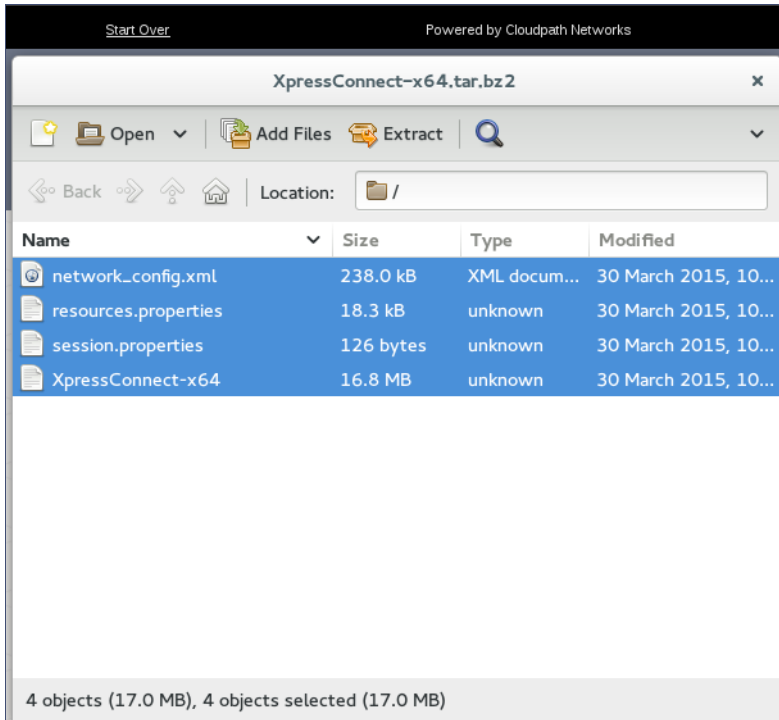


Click *OK* to continue.

Extract Downloaded Files

Extract the application files that were downloaded.

FIGURE 9. Select Files to be Extracted



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

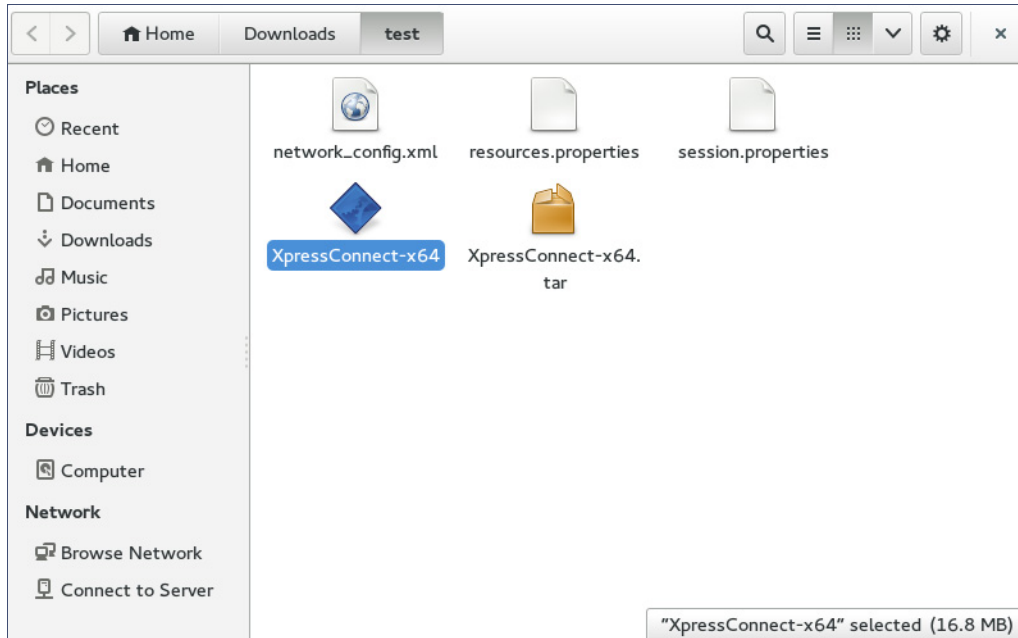
Open Application File

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 10. Open Application File



The Wizard runs through the configuration and migration process.

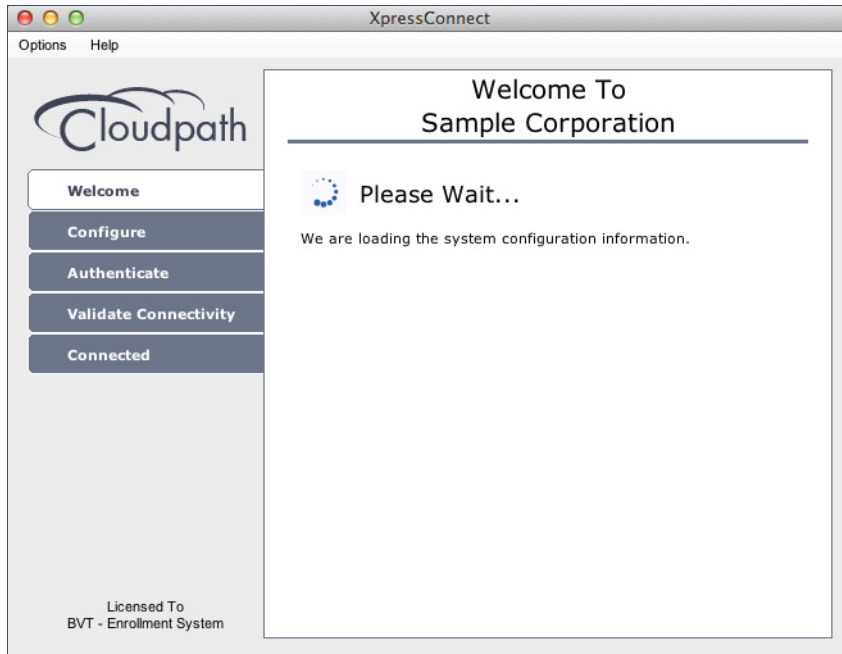
Wizard Application User Experience

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

Loading System Configuration

The Wizard opens and begins the configuration process.

FIGURE 11. Please Wait

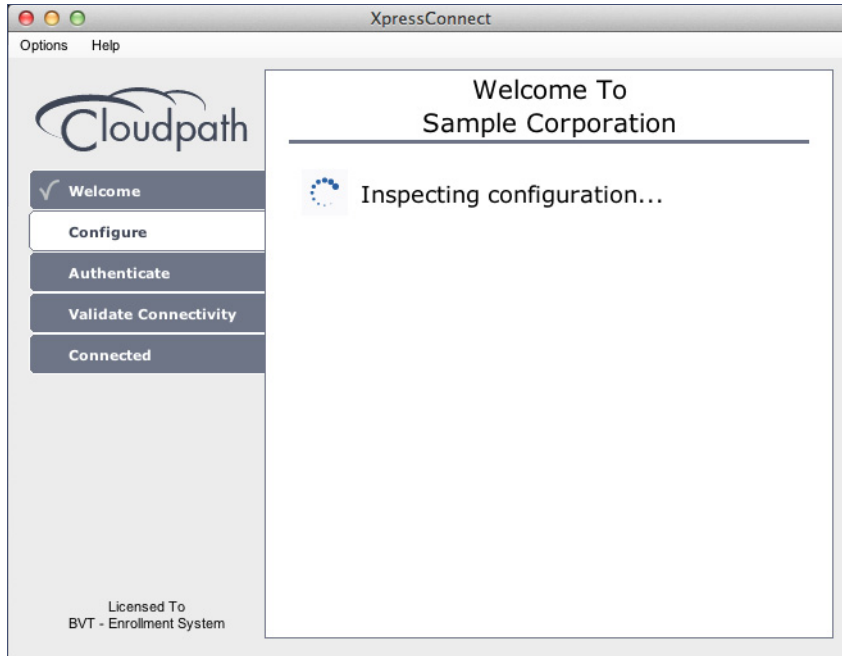


The configuration process takes less than a minute.

Inspecting Configuration

The application verifies that your computer's configuration is correct for the secure network.

FIGURE 12. Inspecting Configuration

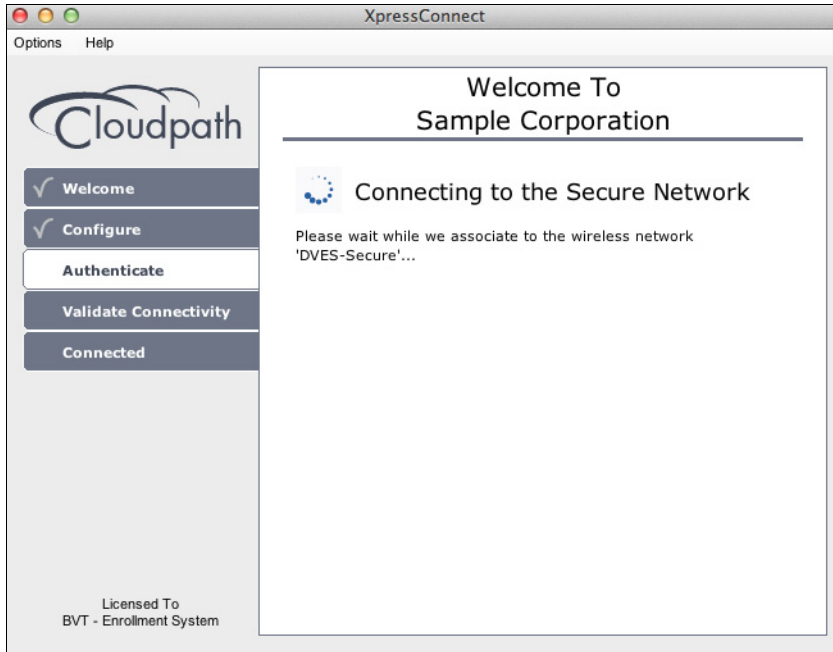


The application continues with the authentication process.

Connecting to Secure Network

The application attempts to associate to the wireless network.

FIGURE 13. Connection to Secure Network

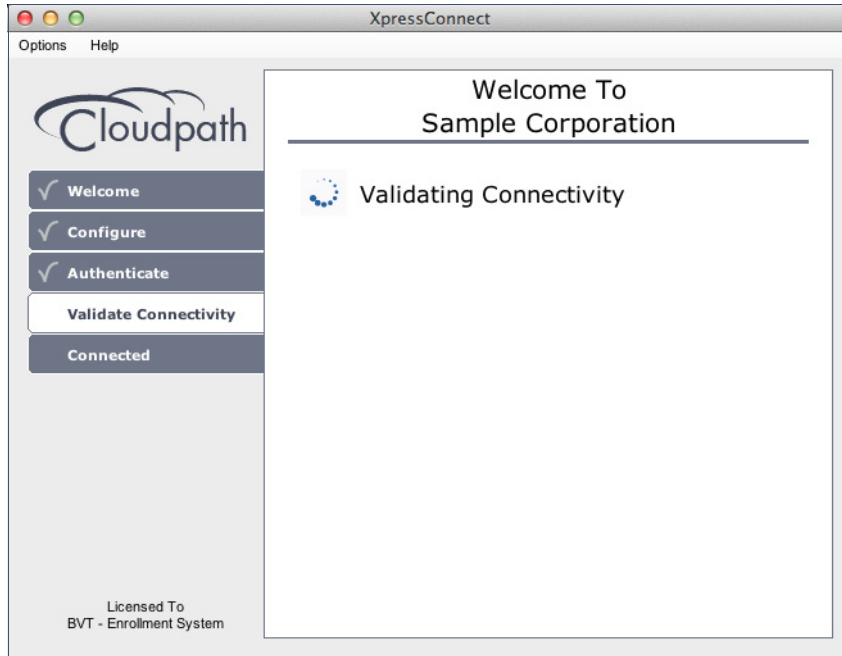


The application continues with the validation process.

Validating Connectivity

When the association with the secure network is successful, the application attempts to acquire a network address.

FIGURE 14. Validating Connectivity

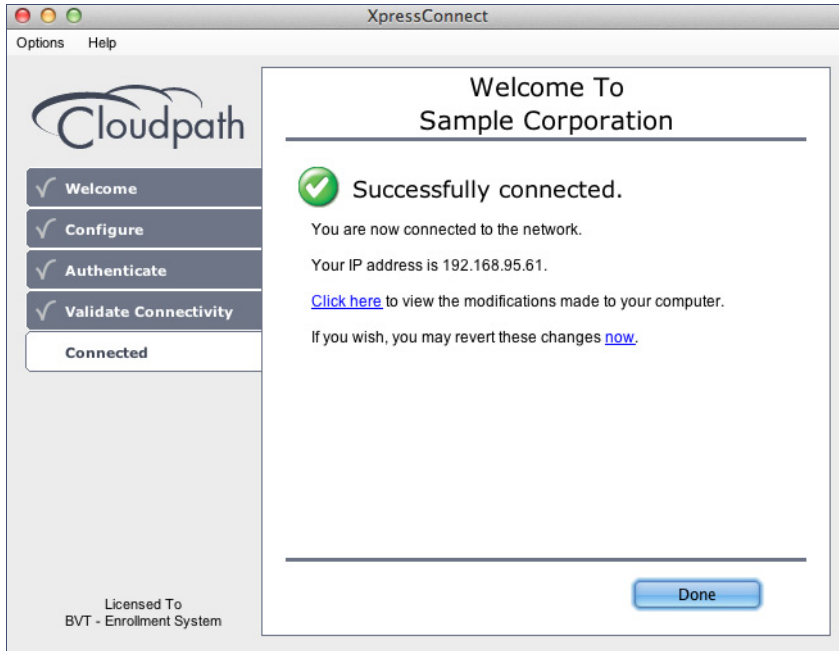


The application continues with the connection process.

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 15. Connected to Secure Network

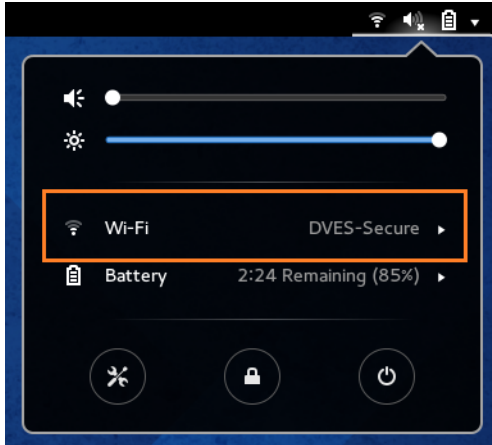


Click *Done*.

View Network Connection

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

FIGURE 16. View Wireless Network



The Wi-Fi setting displays the secure network.

Additional Documentation

You can find detailed information in the Cloudpath ES configuration guides, located on the left-menu *Support* tab of the ES Admin UI.

About Cloudpath

Cloudpath Networks, Inc. provides automated device enablement (ADE) solutions that simplify the adoption of standards-based Wi-Fi security, including WPA2-Enterprise, 802.1X, and X.509, in diverse BYOD environments. Founded in 2006, Cloudpath Networks invented the modern onboarding model for personal devices and continues to drive the industry's adoption of standards-based security en masse. The Cloudpath solutions are proven worldwide to bring simplicity to secure networks through automated and easy-to-use form and function. To learn more, visit www.cloudpath.net.

If you need technical assistance, discover a bug, or have other technical questions, email support at support@cloudpath.net.

Contact Information

General Inquiries: info@cloudpath.net

Support: support@cloudpath.net

Sales: sales@cloudpath.net

Media: media@cloudpath.net

Marketing: marketing@cloudpath.net

Phone: +1 303.647.1495 (US)

+1 866.472.6053 (US)

+44 (01) 161.261.1400 (UK)

Fax: +1 760.462.4569

Address: 1120 W 122nd Ave, Suite 302

Westminster, CO 80234 USA