TECHNICAL DOCUMENTATION

Cloudpath

Enrollment System

End-User Experience for Managed and Unmanaged Chromebooks

Software Release 4.3

April 2016

Summary: This document describes the end-user experience for managed and unmanaged Chromebooks that are using the Enrollment System to onboard to a secure wireless network.

Document Type: Information

Audience: Network Administrator, End-User

Cloudpath

End-User Experience for Managed and Unmanaged Chromebooks

Software Release 4.3

April 2016

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.

End-User Experience for Managed and Unmanaged Chromebooks

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.

The Cloudpath ES can automatically distribute user and device certificates to both IT-managed and unmanaged (BYOD) Chromebooks.

- For IT-managed Chromebooks, the ES 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, the ES 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), the Cloudpath ES provides a secure method for Automatic Device Enablement.

Supported Devices

The ES supports all Chrome OS devices supported by Google. To see a list of devices currently supported by Google, consult the following URLs:

https://www.google.com/chrome/devices/eol.html

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

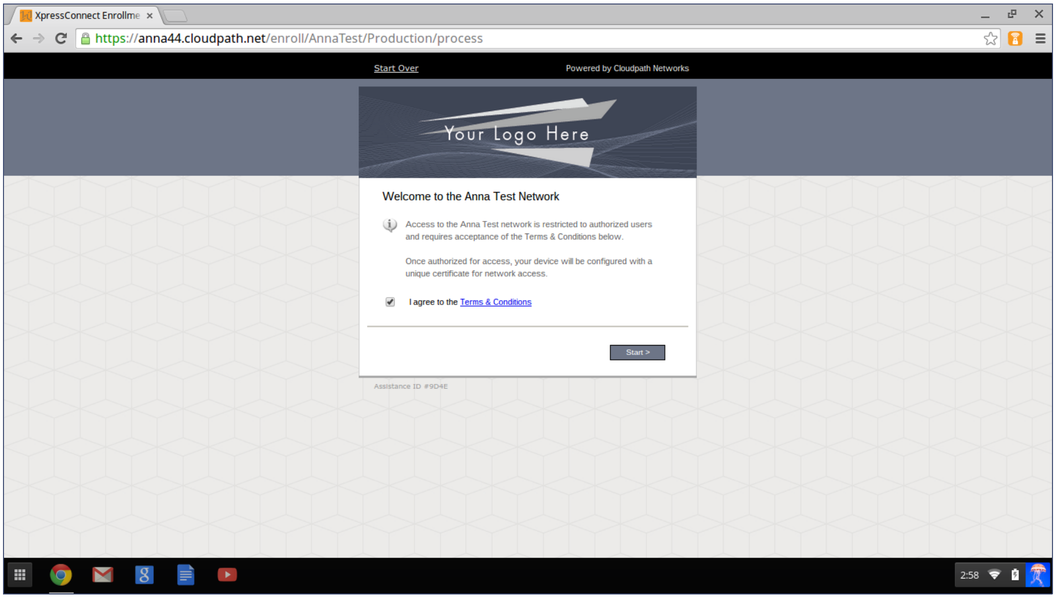
Enrollment Workflow

During enrollment, the Chrome OS is detected and the ES 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 ES Welcome screen displays.

FIGURE 1. Wizard Welcome Page



XpressConnect Enrollme
https://anna44.cloudpath.net/enroll/AnnaTest/Production/process
Start Over
Powered by Cloudpath Networks
Your Logo Here

Welcome to the Anna Test Network

Access to the Anna Test network is restricted to authorized users and requires acceptance of the Terms & Conditions below.

Once authorized for access, your device will be configured with a unique certificate for network access.

☑ I agree to the Terms & Conditions

Assistance ID #9D4E

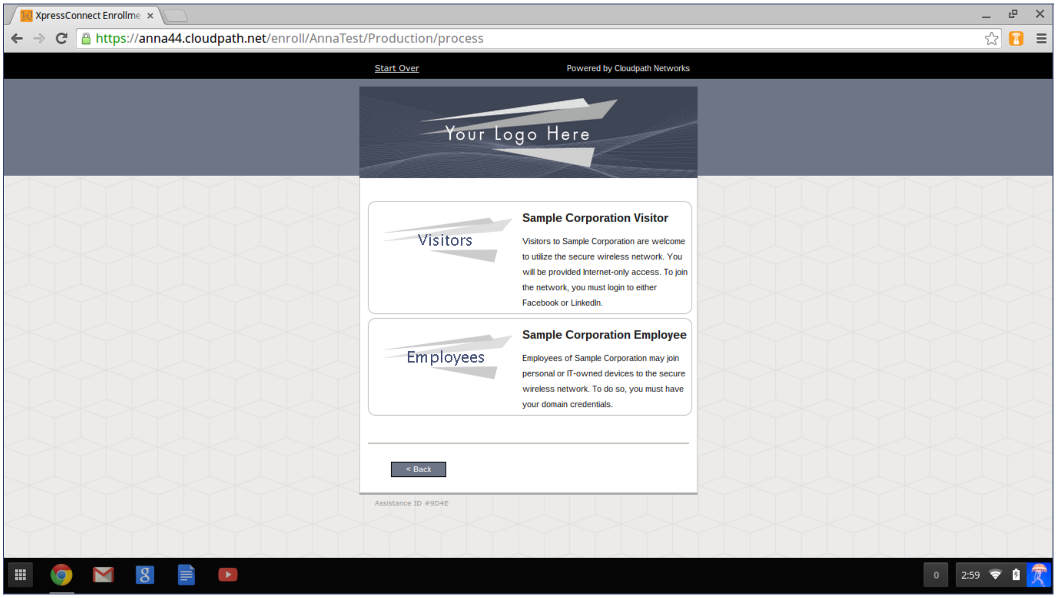
The login screen is typically customized with the logo, colors, and text for the organization or institution. The screens in this example use the default look and feel of the application.

Click *Start* to continue.

User Type Prompt

If required by the network, the user might see a User Type prompt. A user type prompt can provided a branch in the workflow for the different types of users on your network. For example, in an education network, the user types might be Student/Staff/Faculty, or in Enterprise network, they might be Employees/Visitors/Contractors.

FIGURE 2. User Type Prompt


XpressConnect Enrollme ×
https://anna44.cloudpath.net/enroll/AnnaTest/Production/process
Start Over
Powered by Cloudpath Networks
Your Logo Here
Visitors
Employees
< Back
2:59

Sample Corporation Visitor

Visitors to Sample Corporation are welcome to utilize the secure wireless network. You will be provided Internet-only access. To join the network, you must login to either Facebook or LinkedIn.

Sample Corporation Employee

Employees of Sample Corporation may join personal or IT-owned devices to the secure wireless network. To do so, you must have your domain credentials.

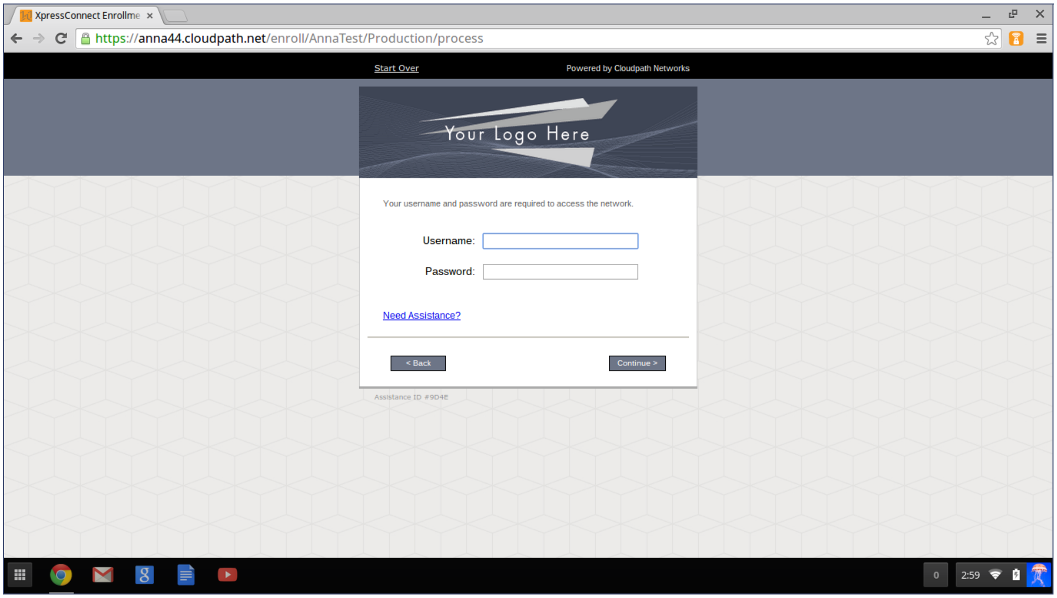
Assistance ID #9D4E

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

User Credentials

If required by the network, the user can be prompted enter their credentials. A user credential prompt might request credentials from an AD or LDAP server, or from RADIUS via PAP.

FIGURE 3. User Credentials



https://anna44.cloudpath.net/enroll/AnnaTest/Production/process

Your username and password are required to access the network.

Username:

Password:

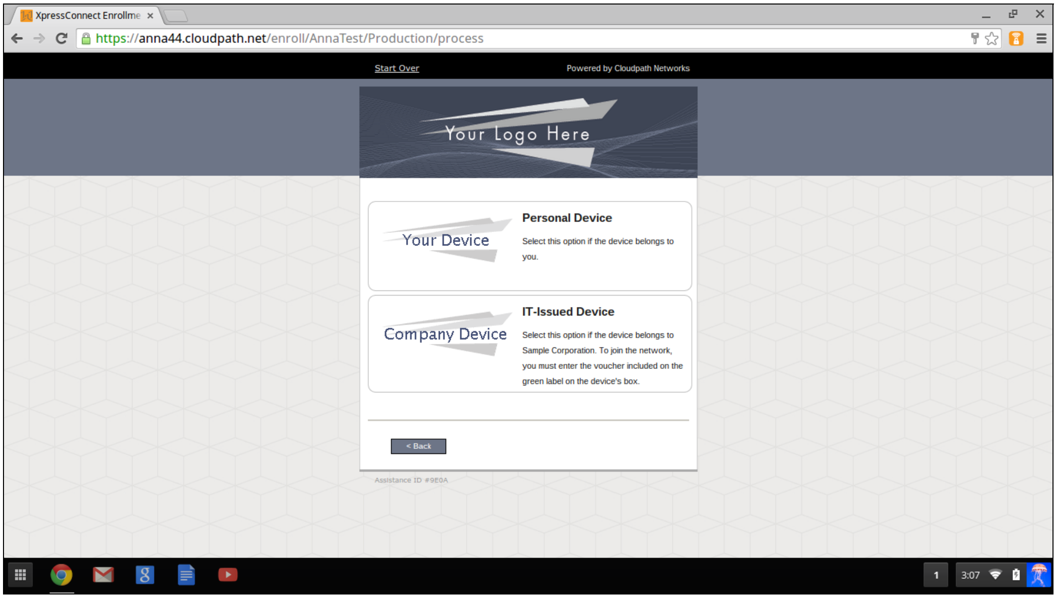
Assistance ID #9D4E

Enter the user credentials and click *Continue*.

Device Type

If required by the network, the user might see a Device Type prompt. A device type prompt can provided a branch in the workflow for the different types of devices on your network.

FIGURE 4. Device Type Prompt



Personal Device

Select this option if the device belongs to you.

IT-Issued Device

Select this option if the device belongs to Sample Corporation. To join the network, you must enter the voucher included on the green label on the device's box.

Select the device type to continue. This example follows the *Personal Device* 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 links to continue with the user experience example for your configuration.

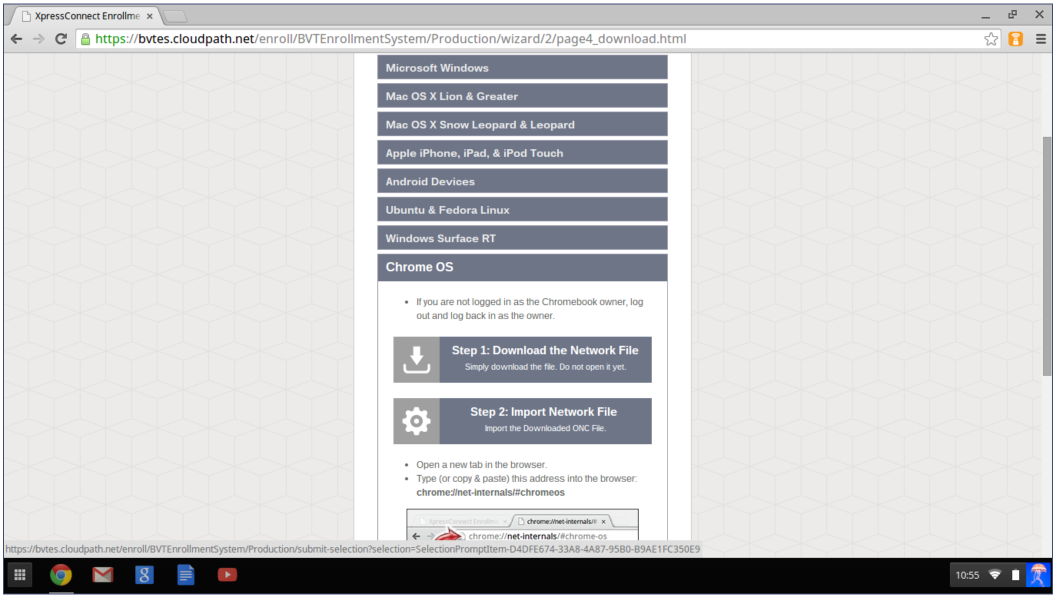
- Unmanaged Chromebook User Experience
- Managed Chromebooks With Extension User Experience

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 5. Configuration Installation Instructions



XpressConnect Enrollme
https://bvtes.cloudpath.net/enroll/BVTEnrollmentSystem/Production/wizard/2/page4_download.html
Microsoft Windows
Mac OS X Lion & Greater
Mac OS X Snow Leopard & Leopard
Apple iPhone, iPad, & iPod Touch
Android Devices
Ubuntu & Fedora Linux
Windows Surface RT
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**

XpressConnect Enrollme
chrome://net-internals/#
chrome://net-internals/#chrome-os
https://bvtes.cloudpath.net/enroll/BVTEnrollmentSystem/Production/submit-selection?selection=SelectionPromptItem-D4DFE674-33A8-4A87-95B0-B9AE1FC350E9
10:55

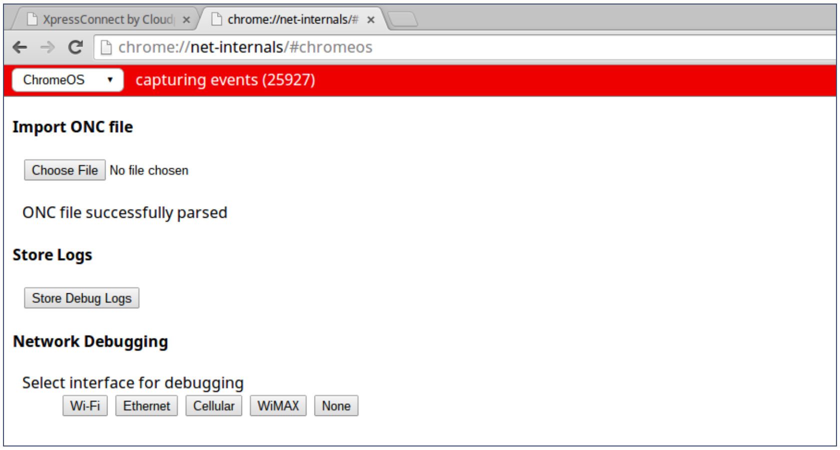
The manual download page shows the Chromebook instructions.

Step 1 provides the link to download the ONC file.

Step 2 provides instructions for importing the ONC file.

- Copy the URL from the instructions.
- Paste the URL into a new browser window. The Chrome OS *Import ONC File* page displays.

FIGURE 6. Import ONC File



XpressConnect by Cloud × | chrome://net-internals/# ×

chrome://net-internals/#chromeos

ChromeOS ▾ capturing events (25927)

Import ONC file

Choose File No file chosen

ONC file successfully parsed

Store Logs

Store Debug Logs

Network Debugging

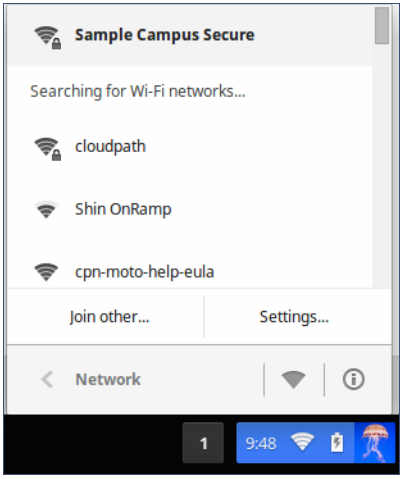
Select interface for debugging

Wi-Fi | Ethernet | Cellular | WiMAX | None

- 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 7. Select Wi-Fi Network



Sample Campus Secure

Searching for Wi-Fi networks...

cloudpath

Shin OnRamp

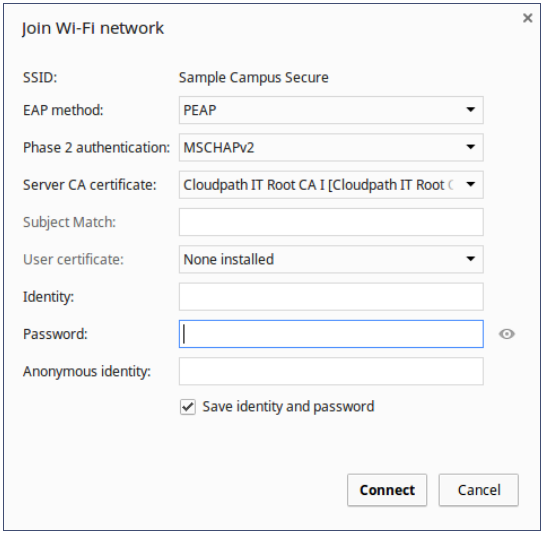
cpn-moto-help-eula

Join other... | Settings...

Network

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

FIGURE 8. Enter User Credentials



Join Wi-Fi network

SSID: Sample Campus Secure

EAP method: PEAP

Phase 2 authentication: MSCHAPv2

Server CA certificate: Cloudpath IT Root CA I [Cloudpath IT Root C

Subject Match:

User certificate: None installed

Identity:

Password:

Anonymous identity:

☑ Save identity and password

The user should now be connected to the secure network.

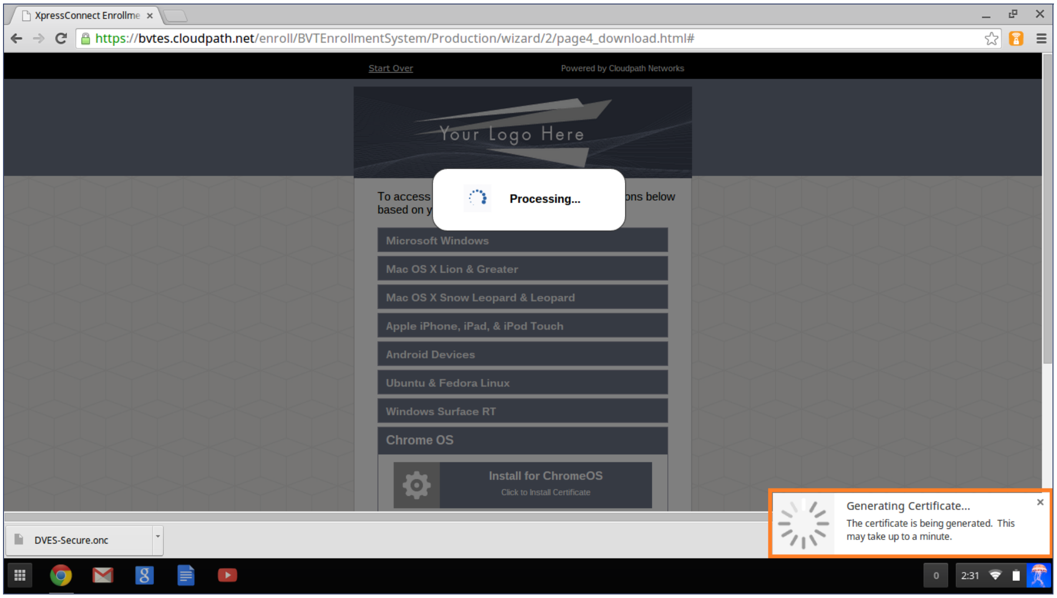
Managed Chromebooks With Extension User Experience

If managed Chromebooks are configured, the download page does not display.

When the ES detects the Chrome OS during enrollment, the extension automatically generates and installs the CA certificate into the TPM.

The extension generates the certificate.

FIGURE 9. Generating Certificate

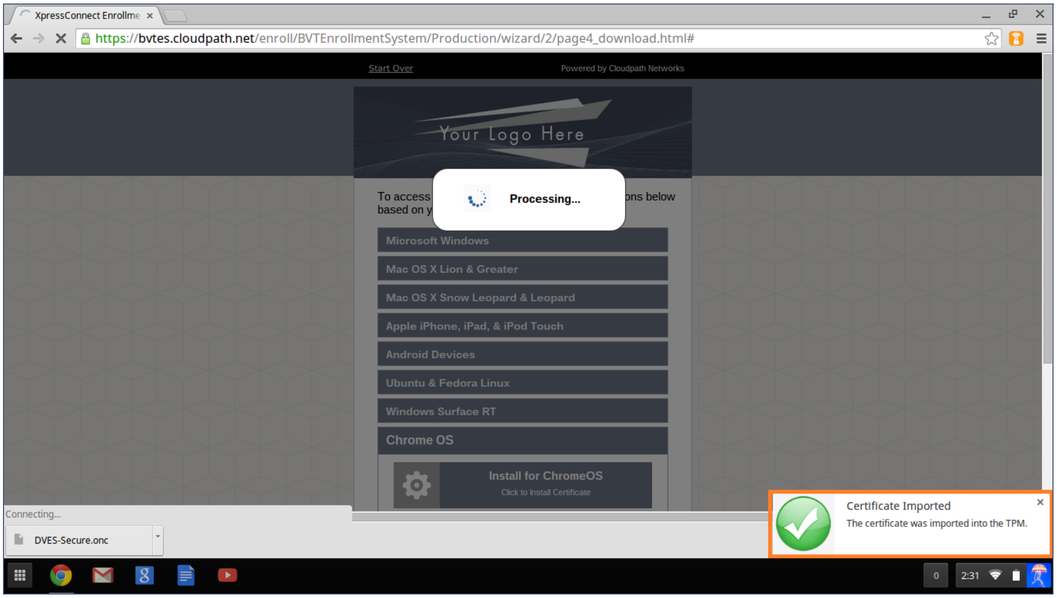


Generating Certificate...

The certificate is being generated. This may take up to a minute.

The extension imports the certificate into the TPM.

FIGURE 10. Certificate Imported

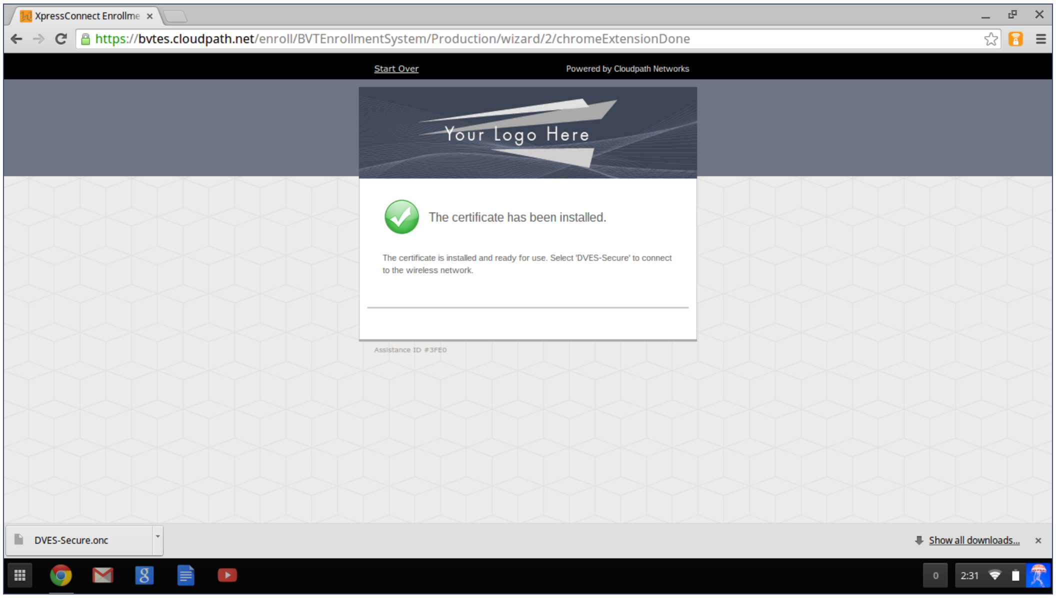


Certificate Imported

The certificate was imported into the TPM.

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

FIGURE 11. Certificate Installed


XpressConnect Enrollme
https://bvtes.cloudpath.net/enroll/BVTEnrollmentSystem/Production/wizard/2/chromeExtensionDone
Start Over
Powered by Cloudpath Networks
Your Logo Here
DVES-Secure.onc
Show all downloads...
0
2:31

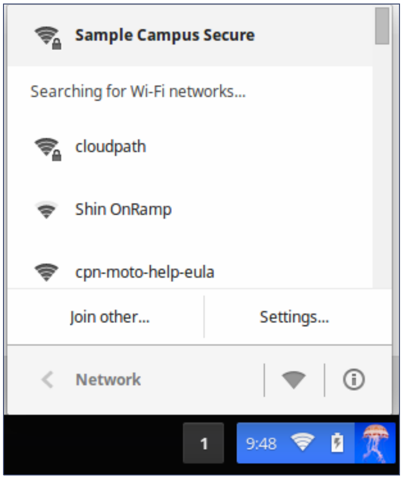
The certificate has been installed.

The certificate is installed and ready for use. Select 'DVES-Secure' to connect to the wireless network.

Assistance ID #3FE0

If not automatically migrated, click the *Wi-Fi* icon in the bottom right corner of your screen and select the secure network.

FIGURE 12. Select Wi-Fi Network



The user should now be connected to 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