

Cloudpath

Enrollment System

End-User Experience for Managed and Unmanaged Chromebooks

Software Release 5.0

December 2016

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

Document Type: Information

Audience: Network Administrator, End-User



End-User Experience for Managed and Unmanaged Chromebooks

Software Release 5.0

December 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 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.

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 Devices

Cloudpath 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 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.

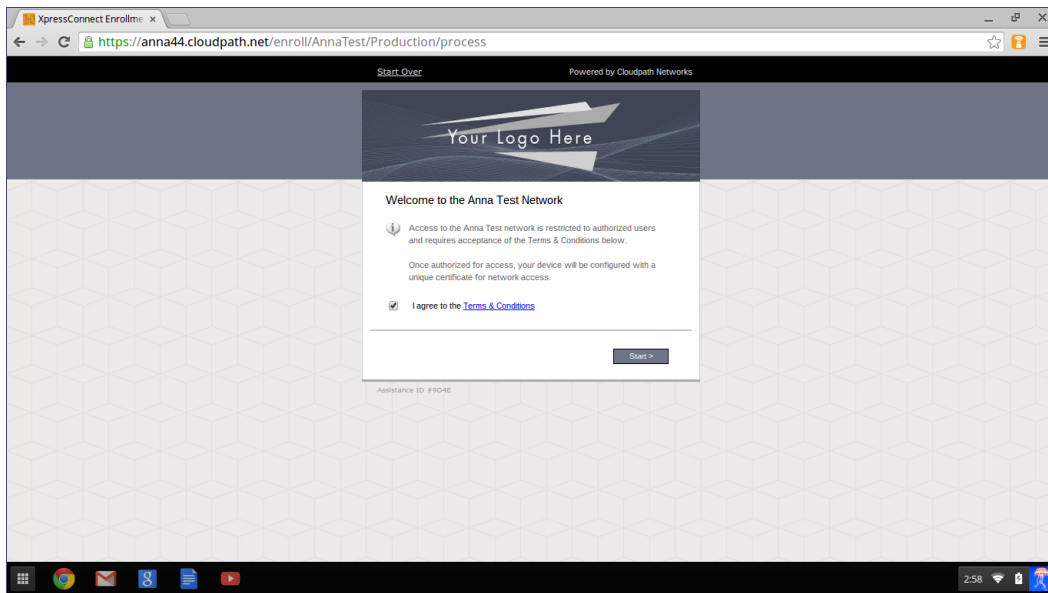
Enrollment Workflow

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 1. Wizard Welcome Page



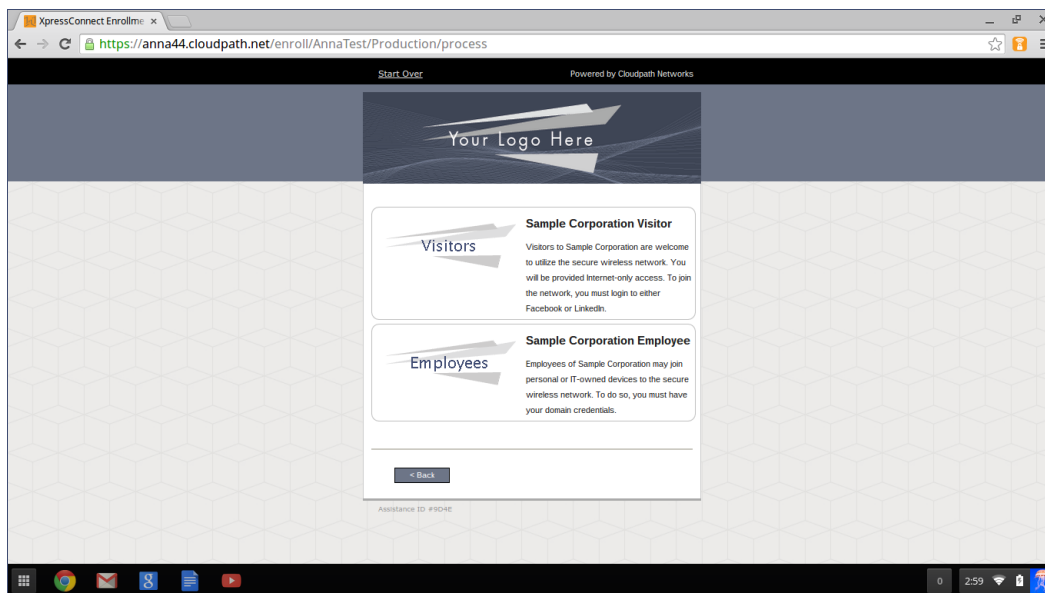
The login screen is typically customized with the logo, colors, and text for the organization or institution. The screens in this example use the default look and feel of the application.

Click *Start* to continue.

User Type Prompt

If required by the network, the user might see a User Type prompt. A user type prompt can provide 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 an Enterprise network, they might be Employees/Visitors/Contractors.

FIGURE 2. User Type Prompt

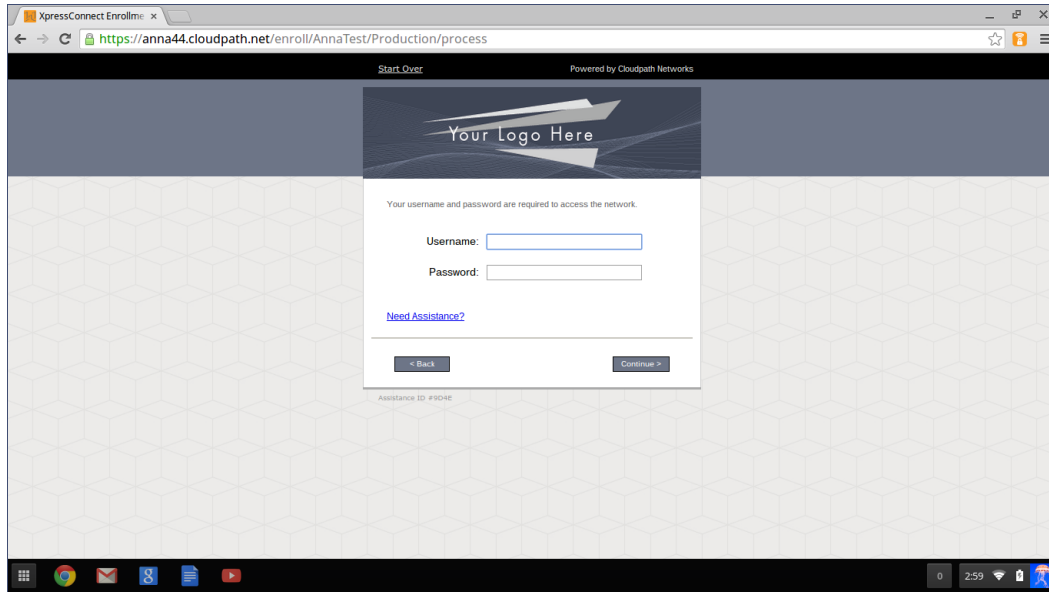


Select the user type to continue. This example follows the *Employee* workflow.

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

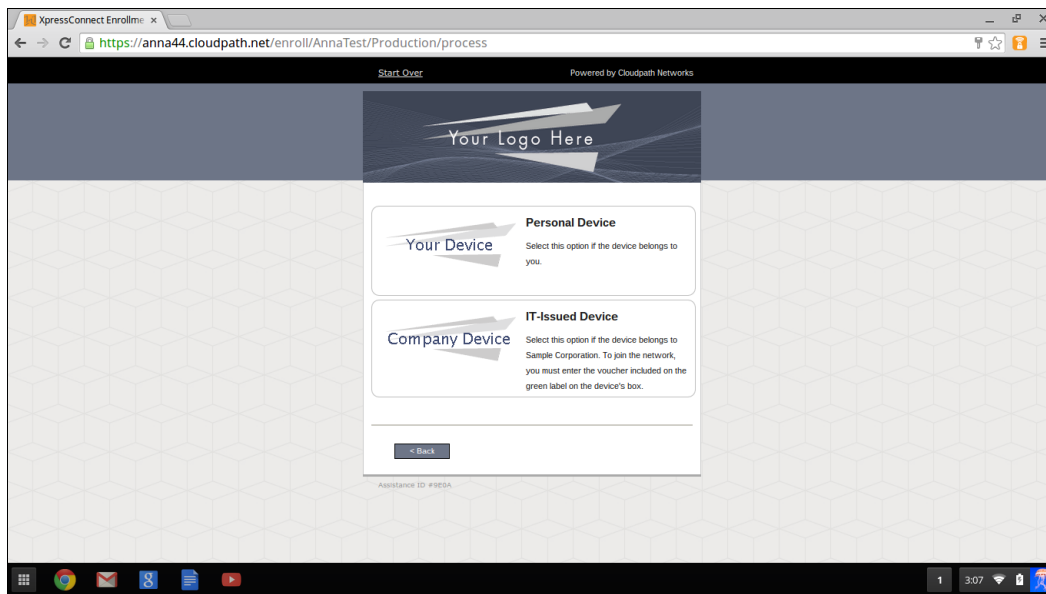


Enter the user credentials and click *Continue*.

Device Type

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

FIGURE 4. Device Type Prompt



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



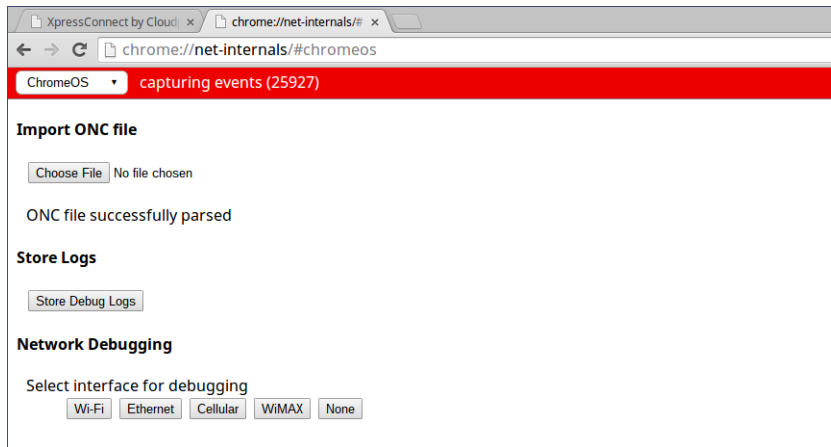
The manual download page shows the Chromebook instructions.

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.

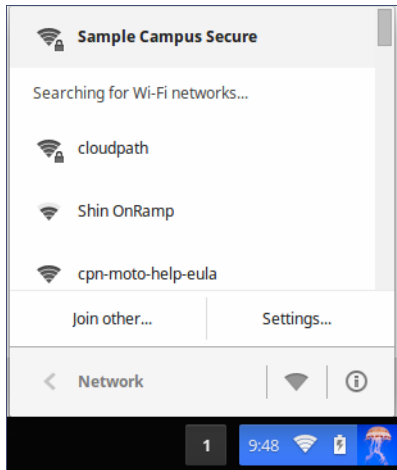
FIGURE 6. Import ONC File



- Click *Choose File* and browse to select the <NetworkName>.onc file.

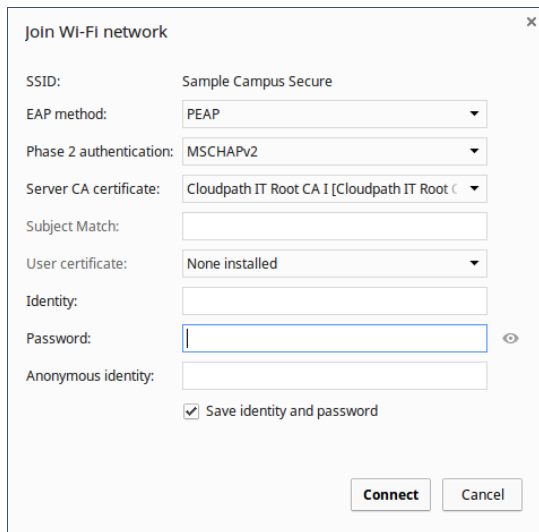
After the ONC file installed, click the *Wi-Fi* icon in the bottom right corner of your screen and select the secure network.

FIGURE 7. Select Wi-Fi Network



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

FIGURE 8. Enter User Credentials



The screenshot shows a dialog box titled "Join Wi-Fi network" with a close button (X) in the top right corner. The dialog contains the following fields and options:

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

The user should now be connected to the secure network.

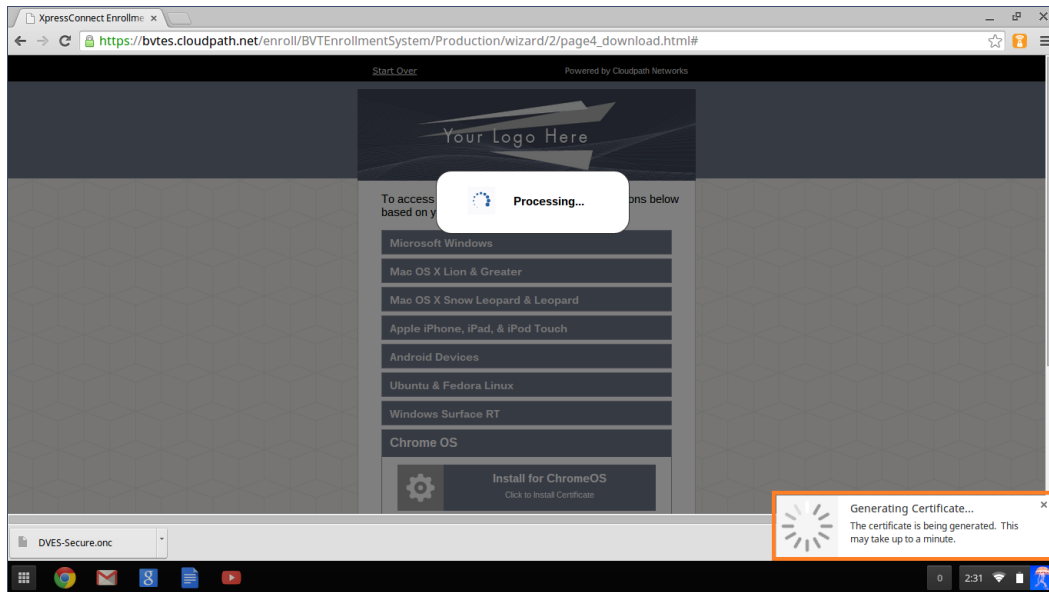
Managed Chromebooks With Extension User Experience

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.

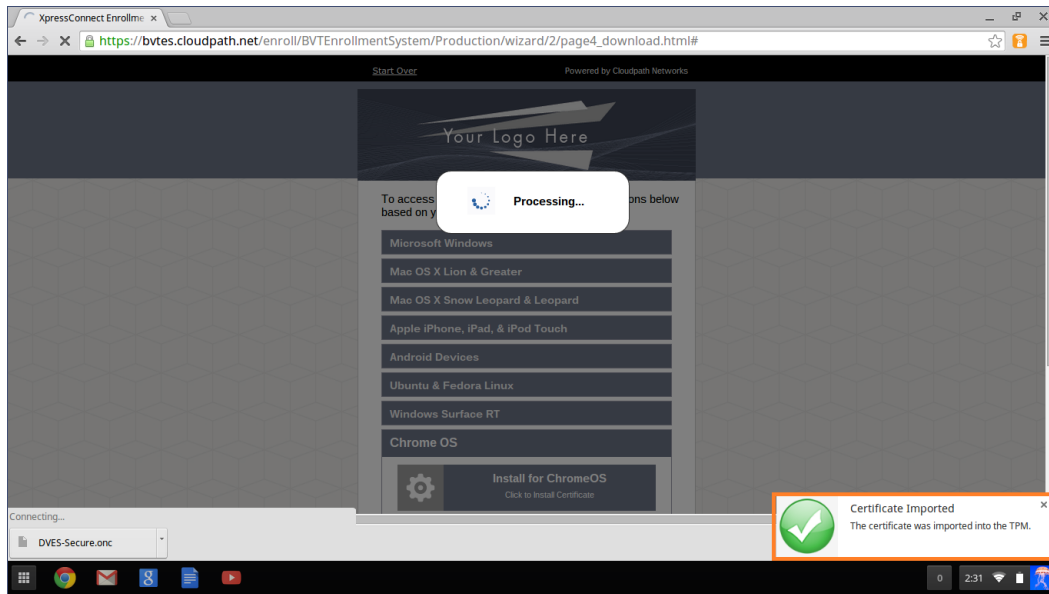
The extension generates the certificate.

FIGURE 9. Generating Certificate



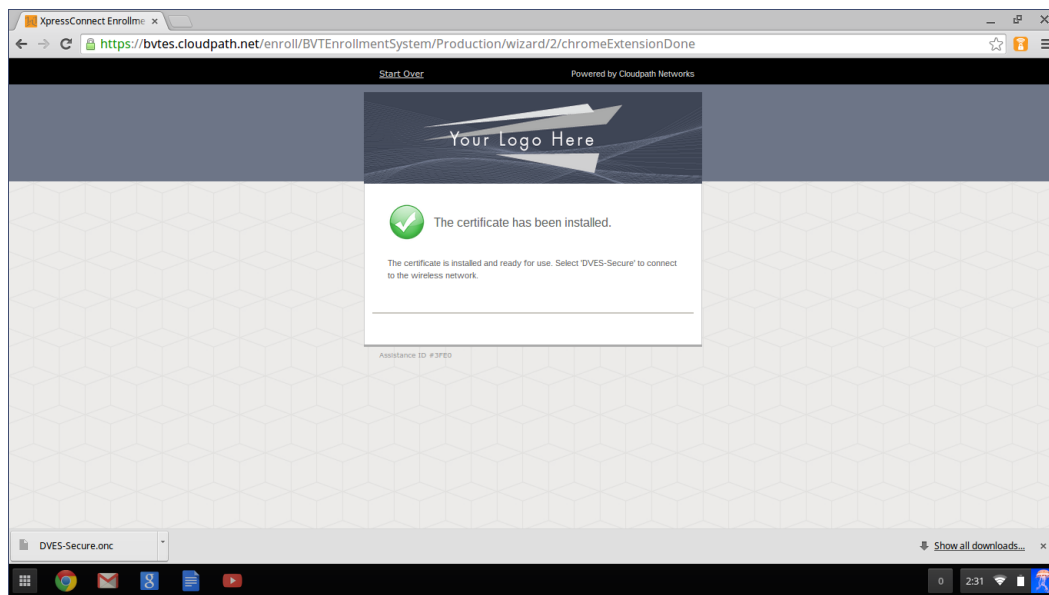
The extension imports the certificate into the TPM.

FIGURE 10. Certificate Imported



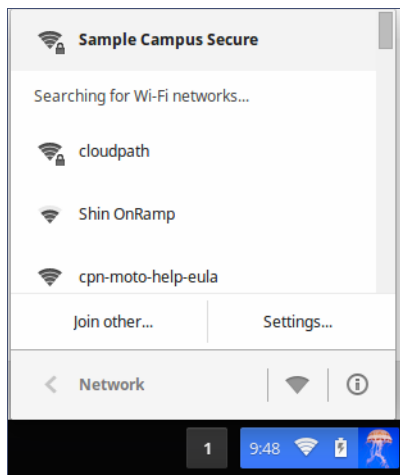
When the certificate installation is complete, a message displays indicating that the certificate is installed and ready for use.

FIGURE 11. 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 12. Select Wi-Fi Network



The user should now be connected to the secure network.