

Cloudpath End-User Experience for Managed and Unmanaged Chromebooks

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 Devices.....4
- Cloudpath User Experience.....4
 - Enrollment Workflow..... 4
 - Managed or Unmanaged Chromebooks..... 8

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 URL:

<https://www.chromium.org/chromium-os/developer-information-for-chrome-os-devices>

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.

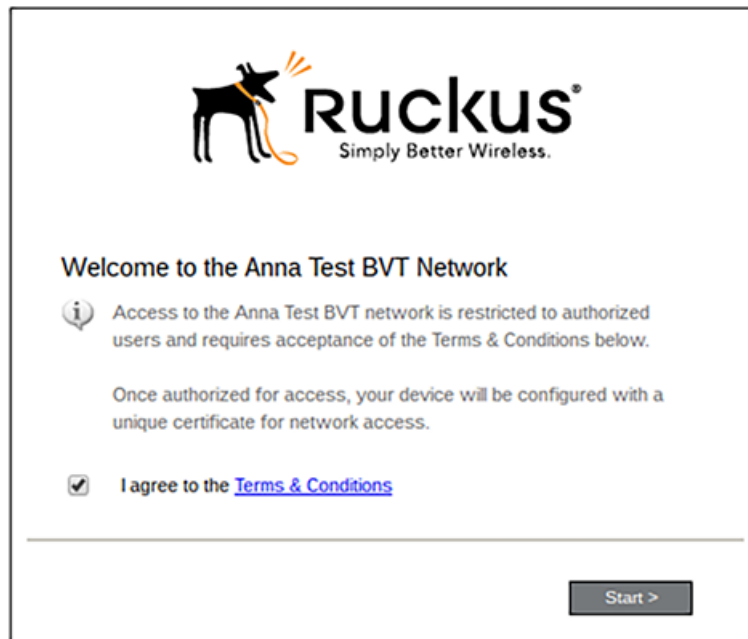
Enrollment Workflow

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 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



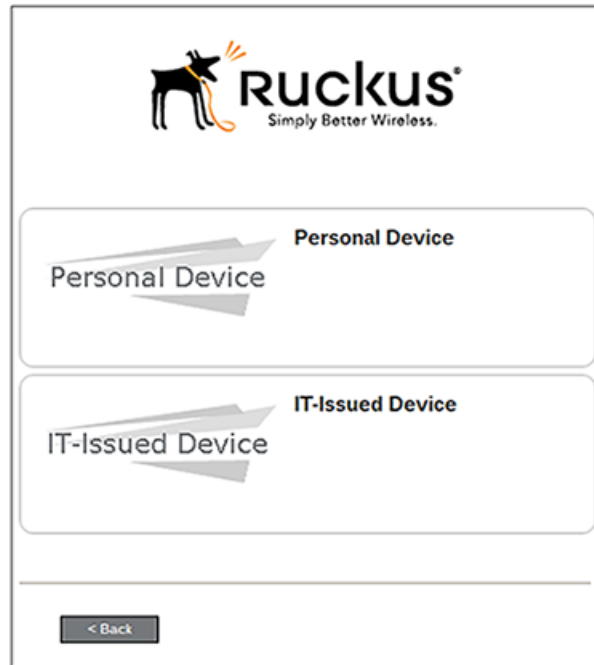
The image shows a login screen for Ruckus. At the top center is the Ruckus logo, which consists of a black silhouette of a dog with an orange leash and three orange curved lines above its head, followed by the word "Ruckus" in a bold, black, sans-serif font. Below the logo is the tagline "Simply Better Wireless." in a smaller, black, sans-serif font. Below the logo and tagline is the text "Your username and password are required to access the network." in a black, sans-serif font. Below this text are two input fields: "Username:" followed by a white rectangular box with a thin black border, and "Password:" followed by a white rectangular box with a thin black border. Below the input fields is a blue, underlined link that says "Need Assistance?". At the bottom of the screen, there are two grey buttons with white text: "< Back" on the left and "Continue >" on the right. The entire form is enclosed in a thin black border.

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 sections 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

Chrome OS

- If you are not logged in as the Chromebook owner, log out and log back in as the owner.

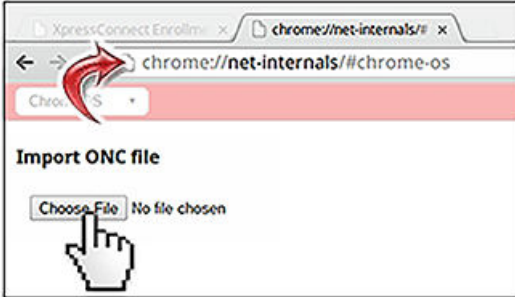
**Step 1: Download the Network File**

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



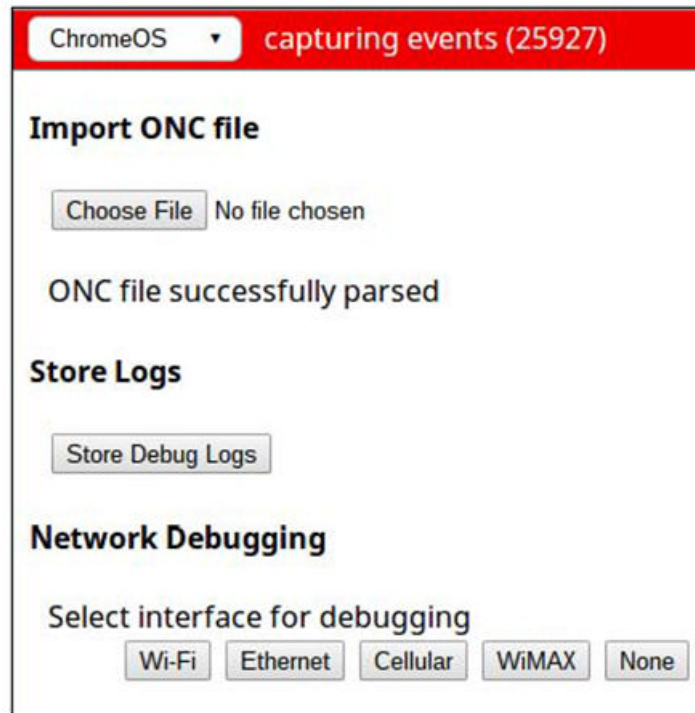
- Under **Import ONC File**, click **Choose File**
- Select the downloaded **eng-Anna43.onc** file and click **Open**.
- If an error is not reported, your device is now configured for the network.
- To connect, select 'eng-Anna43' from the list of **wireless networks**.

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.

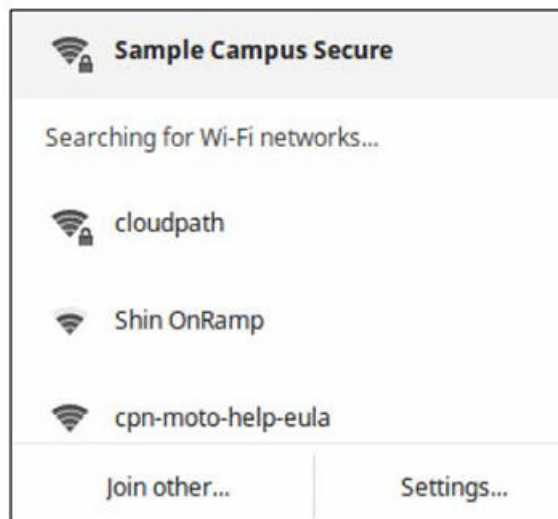
FIGURE 6 Import ONC File



- Copy the URL from the instructions.
- Paste the URL into a new browser window. The Chrome OS Import ONC File page displays.
- 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 'Join Wi-Fi network' dialog box with the following fields and values:

- SSID: Sample Campus Secure
- EAP method: PEAP
- Phase 2 authentication: MSCHAPv2
- Server CA certificate: Cloudpath IT Root CA 1 [Cloudpath IT Root C
- Subject Match: (empty)
- User certificate: None installed
- Identity: (empty)
- Password: (empty)
- Anonymous identity: (empty)

At the bottom, there is a checked checkbox for 'Save identity and password' and two buttons: 'Connect' and 'Cancel'.

The user should now be connected to the secure network.

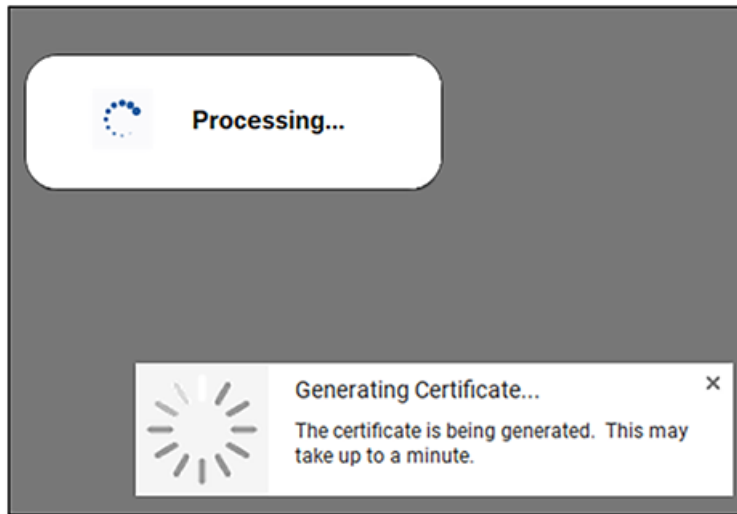
Managed Chromebooks With Extension User Experience

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.

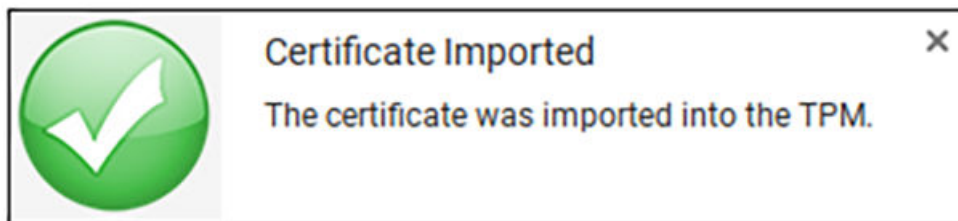
The extension generates the certificate.

FIGURE 9 Generating Certificate



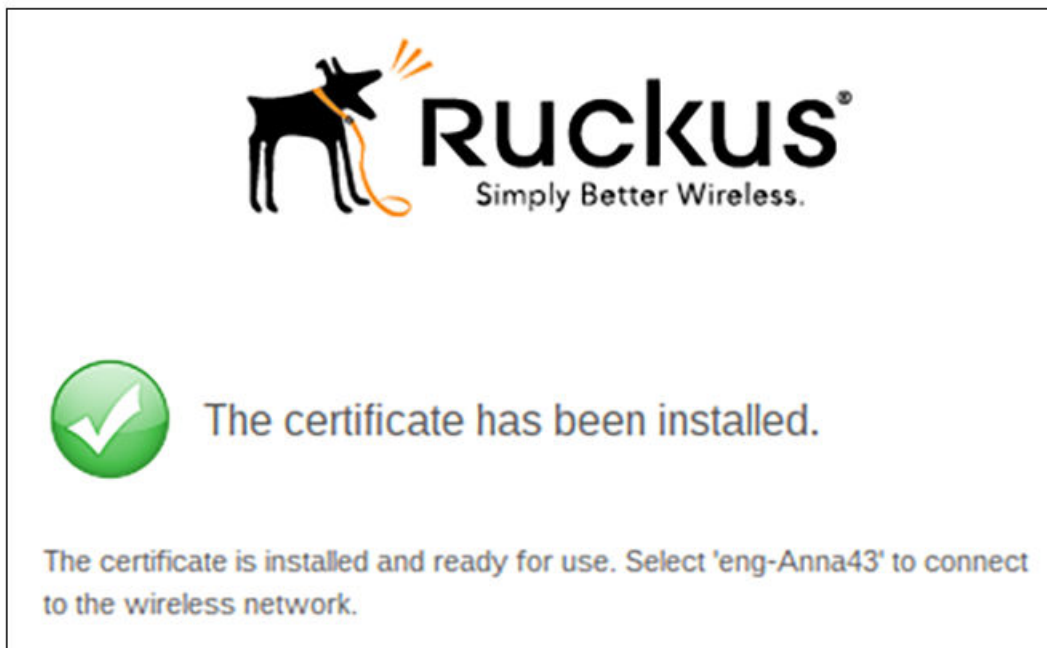
The extension imports the certificate into the TPM.

FIGURE 10 Certificate Imported



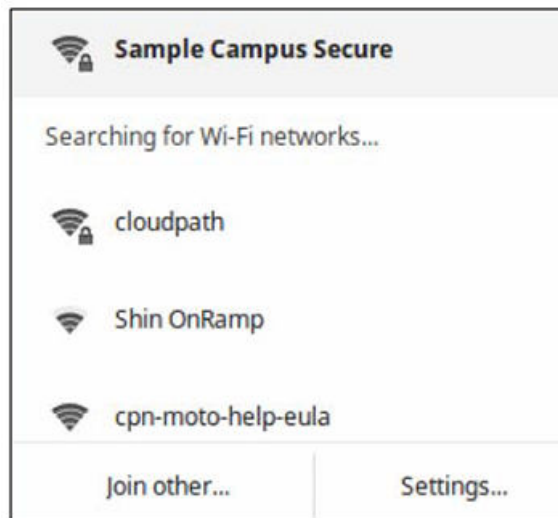
When the certificate installation is complete, a message displays indicating that the certificate is installed and ready for use.

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.



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