



Configure Cloudpath with an Intermediate Certificate for Content Filtering

Technical Note

October 2017

Copyright Notice and Proprietary Information

Copyright 2017 Ruckus Wireless, Inc. All rights reserved.

No part of this documentation may be reproduced, transmitted, or translated, in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without prior written permission of Ruckus Wireless, Inc. ("Ruckus"), or as expressly provided by under license from Ruckus.

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. RUCKUS AND ITS 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. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT, SHALL 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 is a trademark of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.

Table of Contents

Overview	5
The Role and Challenges of Content Filtering	5
Increased Use of Encryption for All Web Traffic	5
Trusted Man-in-the-Middle to Intercept and Decrypt HTTPS Traffic.....	5
Cloudpath Support for HTTPS T-MIM Inspection	5
How We Do It	6
Procedure Overview	6
Step 1: Obtain Web Filter Root Certificate.....	6
Step 2: Configure the Web Filter to Use an SSL Certificate	9
Step 3: Configuring Cloudpath with Web Filter Root Certificate	9
Step 4: Verification.....	9
Summary	10
About Ruckus	11
Copyright 2017 Ruckus Wireless, Inc. All Rights Reserved	11

October 2017

Intended Audience

This document provides an overview of how to configure Ruckus Cloudpath with an intermediate certificate for content filtering. Some knowledge of Ruckus Cloudpath and content filtering is recommended.

October 2017

Overview

The Role and Challenges of Content Filtering

Web content filters work by examining and then allowing or blocking the traffic that flows through them per the configured rules and policies. This is easily understood in the context of unencrypted HTTP traffic. However, such examination of traffic is not possible in the encrypted HTTPS case.

Increased Use of Encryption for All Web Traffic

Historically, HTTPS has been used by servers that stored critical information (for example banks and financial institutions). However, over time, due to privacy concerns, more and more sites (for example Google, Facebook, Twitter, etc.) are switching over to HTTPS. Google switching all of its services (Google Apps for Education, Google Play, Google Docs, YouTube, etc.) to HTTPS becomes problematic in the education environment. With all of the content flowing between the client (student) devices and the Google servers now being encrypted, content filtering becomes a challenge.

One way for content filters to determine the web site being visited is to examine the SSL certificate returned by the site. This can be used even if the rest of the traffic is encrypted. But even this mechanism has become of limited use. This is because many sites like Google now use a wildcard certificate for all its subdomains, which leads to the general URL detail problem with these connections. There is no way to know what the client is browsing within the site by merely examining the sever certificate. A web site called `good.google.com` uses the same SSL certificate as `adult-content.google.com`. Without the ability to decrypt the data, determining exactly which site and content is being accessed has become extremely difficult if not impossible.

Trusted Man-in-the-Middle to Intercept and Decrypt HTTPS Traffic

There is however, one possible way to decrypt secure HTTPS traffic. In this scenario, encrypted HTTPS traffic is decrypted and read as plain text HTTP traffic. This method, called the "Trusted Man in the Middle", offers the least privacy but the greatest security because all traffic is intercepted and decrypted. Once the content is readable, it is now subject to the web content filtering rules. In this scenario, the web filter is set up as a proxy. It acts as an intermediary and intercepts and decrypts all client-server traffic before it is sent to the destination server. This works because the client is presented with the web filter's SSL certificate and uses this to encrypt and decrypt traffic rather than the destination server. For this to work however, the client needs to trust the web filter. Web browsers come pre-installed with the root certificates of many major certificate authorities. However, most web content filters create their own certificates, also called a self-signed certificate, and thus one needs to add their root certificate to the client's repository of trusted certificate authority certificates. This allows the clients to validate and trust the web filter. This can be a real challenge since it requires touching every client that might send traffic through the web filter.

Cloudpath Support for HTTPS T-MIM Inspection

This is where Cloudpath comes in. Client onboarding via Cloudpath is via a certificate. This certificate is used for authentication when granting wireless access to the client. However, one can include the web filter root certificate as a part of the client enrollment process, so that the client now has two certificates: one for wireless access and one for "Trusted Man in the Middle" HTTPS browsing. This effectively removes the manual process of configuring a device which is a large part of the headache involved in setting up this kind of scenario.

October 2017

How We Do It

Procedure Overview

The following steps are required to configure Cloudpath to install the root certificate for a web filter on newly onboarded clients:

1. Obtain a web filter root certificate
2. Configure the web filter to use an SSL certificate
3. Load/Add the SSL certificate installation to the Cloudpath onboarding process
4. Verify traffic is correctly decrypted by the web filter

Step 1: Obtain Web Filter Root Certificate

Where to obtain this web filter root certificate (sometimes called an intermediate proxy certificate) depends very much on the filter under consideration. You will have to refer to the documentation for the filter that is being used. As an example, the cloud implementation of the LightSpeed web filter provides this at <https://ruckus.lightspeedsystems.com/laccess/proxycerthelp>

This is illustrated below in Figure 1: Lightspeed Proxy Certificate

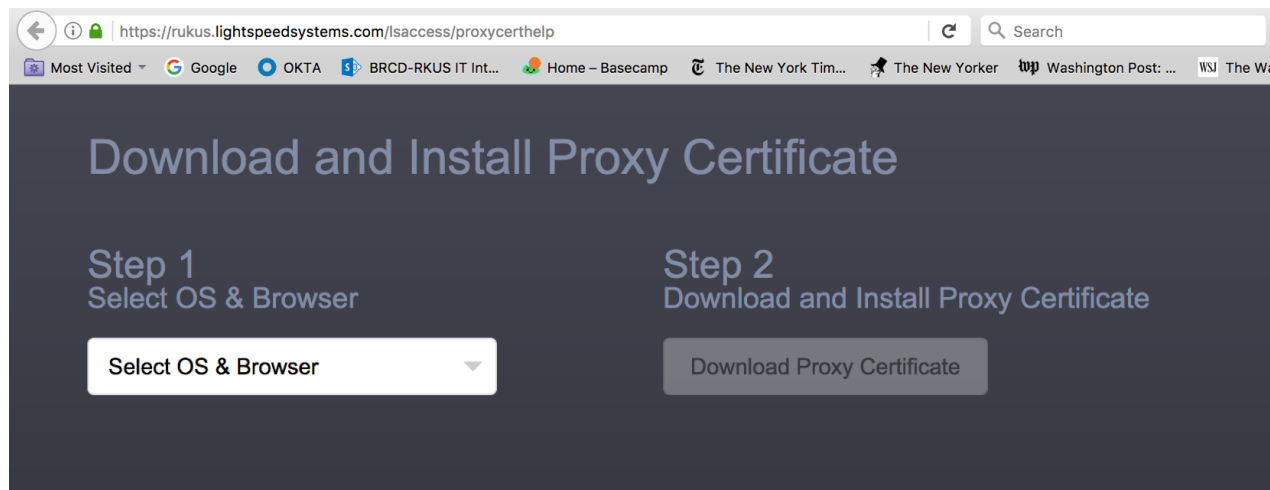


FIGURE 1: LIGHTSPEED PROXY CERTIFICATE

October 2017

Make the appropriate selection based on your OS and browser preference. This is illustrated below in Figure 2: Select OS

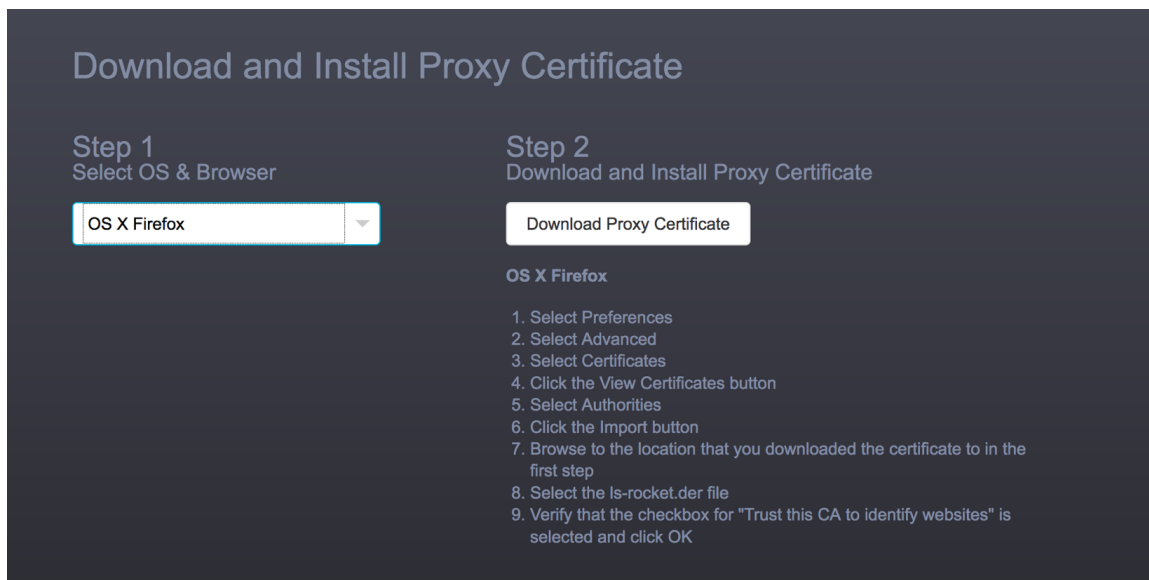


FIGURE 3: SELECT OS

October 2017

Then save the certificate file as shown in Figures 3 and 4.

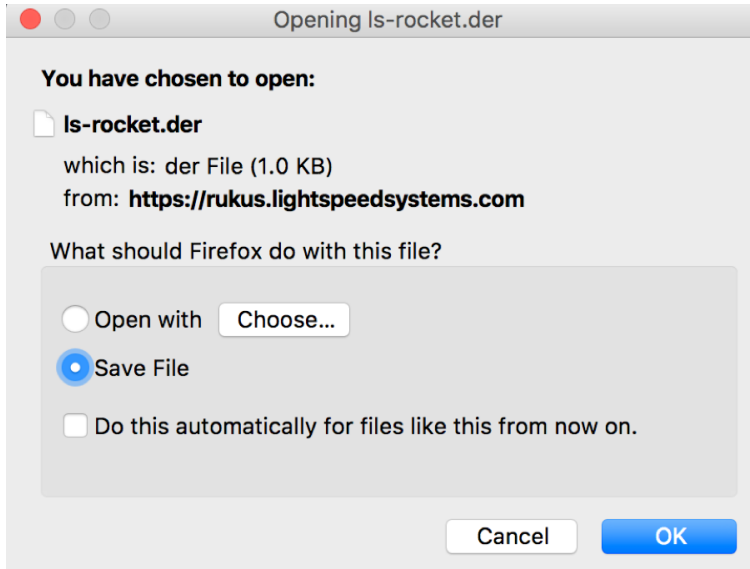


FIGURE 3: CERTIFICATE FILE

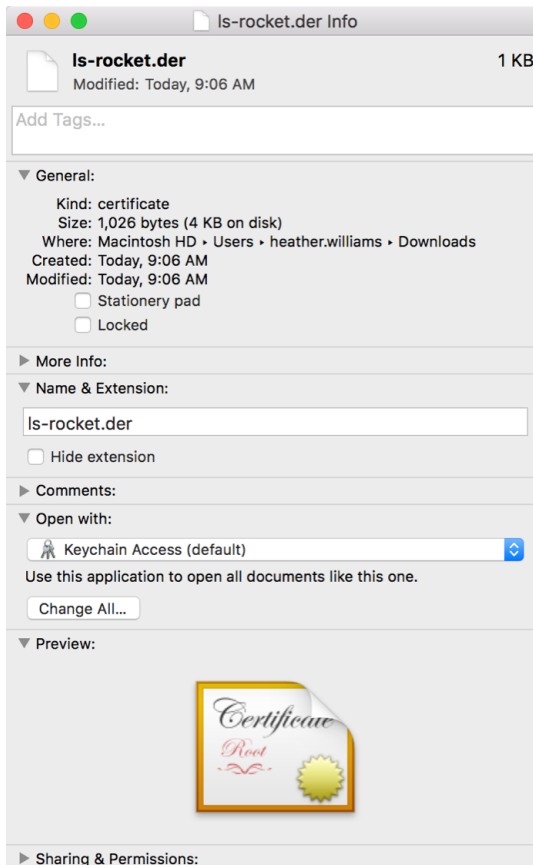


FIGURE 4: CERTIFICATE FILE DETAILS

October 2017

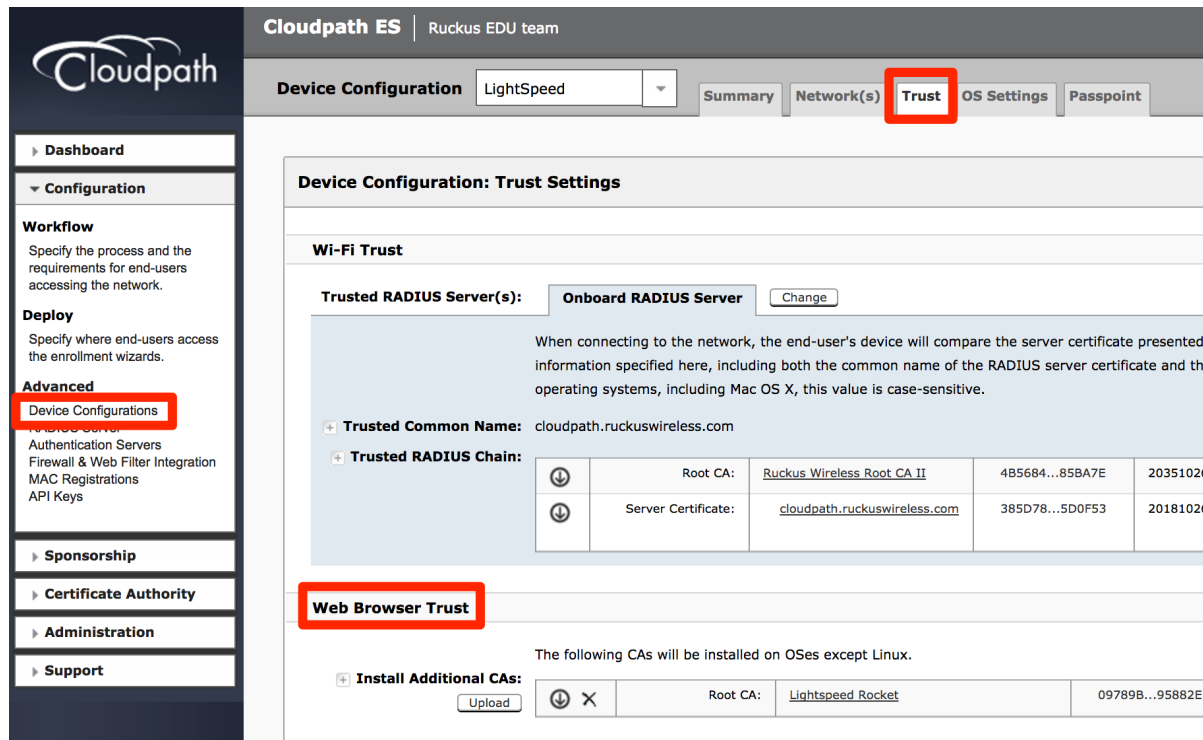
Step 2: Configure the Web Filter to Use an SSL Certificate

Since each web filter uses a different set of commands and process, explaining how to configure the web filter to use an SSL certificate and download it is beyond the scope of this document. For more information, please refer to the administrator's guide for your web filter.

Step 3: Configuring Cloudpath with Web Filter Root Certificate

In Cloudpath you can configure the Enrollment System to trust the certificate you just downloaded. As shown below, for your specific Workflow, the certificate should be added under Device Configuration->Trust->Web Browser Trust.

When the client device is onboarded, this certificate then is installed on the client as a part of the enrollment process allowing the client to now trust the web filter.



The screenshot shows the Cloudpath ES configuration interface for the 'Ruckus EDU team'. The 'Device Configuration' section is selected, and the 'Trust' tab is highlighted with a red box. The 'Device Configuration: Trust Settings' page is displayed, showing 'Wi-Fi Trust' and 'Web Browser Trust' sections. The 'Web Browser Trust' section is highlighted with a red box. The 'Trusted RADIUS Chain' table is also visible.

Root CA:	Root CA:	4B5684...85BA7E	20351026
+	Trusted Common Name:	cloudpath.ruckuswireless.com	
+	Trusted RADIUS Chain:		
⬇	Root CA:	Ruckus Wireless Root CA II	4B5684...85BA7E
⬇	Server Certificate:	cloudpath.ruckuswireless.com	385D78...5D0F53

Root CA:	09789B...95882E		
+	Install Additional CAs:		
⬇	Root CA:	LightSpeed Rocket	09789B...95882E

FIGURE 5: DEVICE CONFIGURATION

Step 4: Verification

Once everything is setup correctly, onboard a client and then try to browse with https to a forbidden site. The filter should correctly intercept and block access.

October 2017

Summary

Using the “Trusted Man in the Middle” method allows you to filter encrypted HTTPS traffic by setting up a web filter as a proxy. Adding a web content filter’s own certificate to the client browser ensures that the client devices will trust the web filter and provide the security gained by web filtering.

October 2017

About Ruckus

Headquartered in Sunnyvale, CA, Ruckus Wireless, Inc. is a global supplier of advanced wireless systems for the rapidly expanding mobile Internet infrastructure market. The company offers a wide range of indoor and outdoor “Smart Wi-Fi” products to mobile carriers, broadband service providers, and corporate enterprises, and has over 36,000 end-customers worldwide. Ruckus technology addresses Wi-Fi capacity and coverage challenges caused by the ever-increasing amount of traffic on wireless networks due to accelerated adoption of mobile devices such as smartphones and tablets. Ruckus invented and has patented state-of-the-art wireless voice, video, and data technology innovations, such as adaptive antenna arrays that extend signal range, increase client data rates, and avoid interference, providing consistent and reliable distribution of delay-sensitive multimedia content and services over standard 802.11 Wi-Fi. For more information, visit <http://www.ruckuswireless.com>.

Ruckus and Ruckus Wireless are trademarks of Ruckus Wireless, Inc. in the United States and other countries.

Copyright 2017 Ruckus Wireless, Inc. All Rights Reserved.

Copyright Notice and Proprietary Information No part of this documentation may be reproduced, transmitted, or translated, in any form or by any means without prior written permission of Ruckus Wireless, Inc. (“Ruckus”), or as expressly provided by under license from Ruckus

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of 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. RUCKUS AND ITS 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. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE,