



## **Purchase & Apply a WWW Certificate in Cloudpath**

**How To**

## 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.

## Overview

This document provides a step-by-step guide for purchasing and installing a WWW server certificate in Cloudpath.

Cloudpath has an onboard Certificate Authority (CA) that can issue a server certificate to the onboard Radius Server and also issue client certificates for enrolling clients. After a client certificate has been issued, all client onboarding authentications take place using this client certificate. However, these certificates, which are used in the client enrollment/onboarding process and are separate and distinct from the WWW Certificate required for secure HTTPS access.

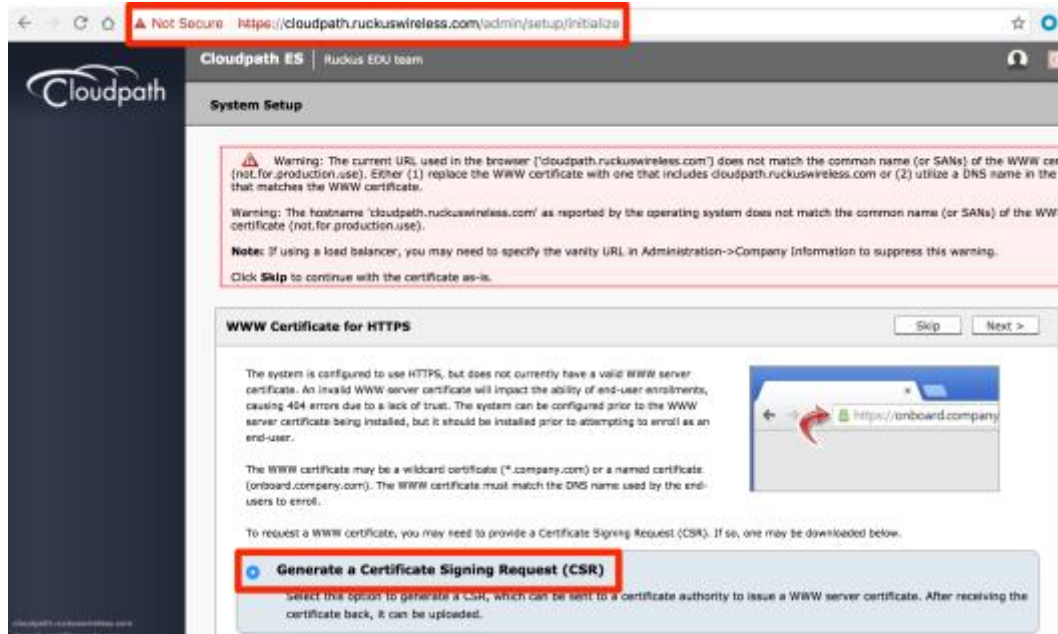
For secure HTTPS access to Cloudpath, it also requires a WWW Server Certificate (aka SSL Certificate). This certificate prevents any client 404 errors caused due to lack of trust when clients access Cloudpath as a part of the enrollment process.

This document addresses this latter WWW or SSL Certificate mentioned above. The Cloudpath system can be configured prior to the WWW server certificate being installed, but the WWW Certificate should be installed before attempting to enroll end-users. A few items about this WWW Server Certificate:

1. The WWW certificate may be a wildcard certificate (\*.company.com) or a named certificate (test.company.com).
2. The WWW certificate must match the DNS name used by the end-users to enroll.
3. To request a WWW certificate, you may need to provide a Certificate Signing Request (CSR). As explained later, the CSR can be generated and downloaded from Cloudpath after the system is set up.

## Cloudpath Without a WWW Server Certificate

Cloudpath can be setup without the SSL certificate. However, as shown below, accessing it produces the following security warnings and an opportunity to generate a Certificate Signing Request (CSR)



## Purchasing a WWW Certificate

As mentioned above, the WWW Server Certificate for Cloudpath can be a wildcard certificate (\*.company.com) or a named certificate (test.company.com). Certificates for varying durations (for example 1/2/3 years) can be purchased from any number of Certificate Authorities. Examples include GoDaddy, DigiCert, StartSSL, etc. The website for each CA clearly details the procedure for applying and obtaining such a certificate. In general, the following is required:

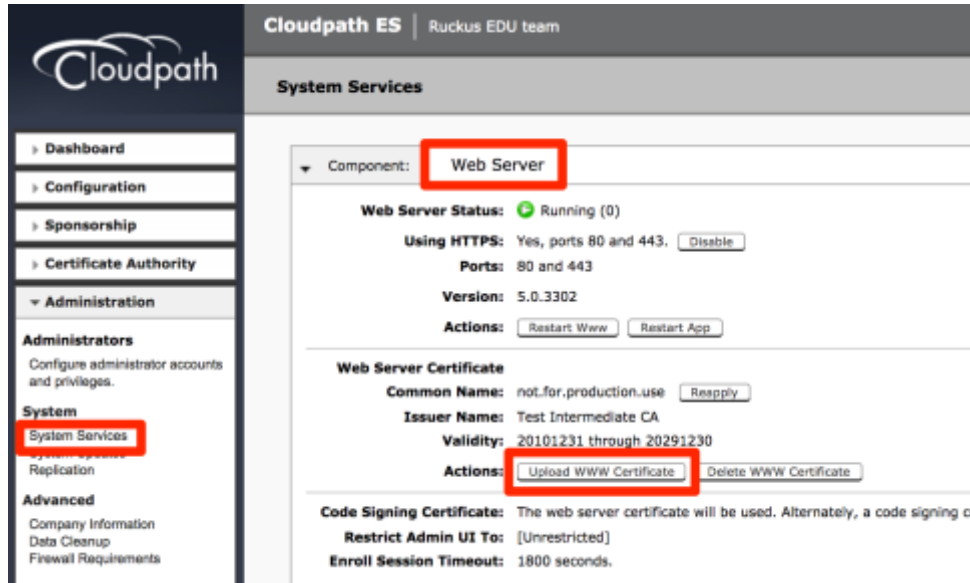
1. Hostname or Domain Name (test.company.com or \*.company.com)
2. Updated WHOIS record with the correct company name, address, contact information, etc. Usually, the order fulfillment email containing the certificate is emailed to the contact on record.
3. Certificate Signing Request (generated by Cloudpath, see below)

Usually such a certificate is obtained in a few hours after submission of the request and the appropriate payment.

January 2017

## Generating Certificate Signing Request (CSR)

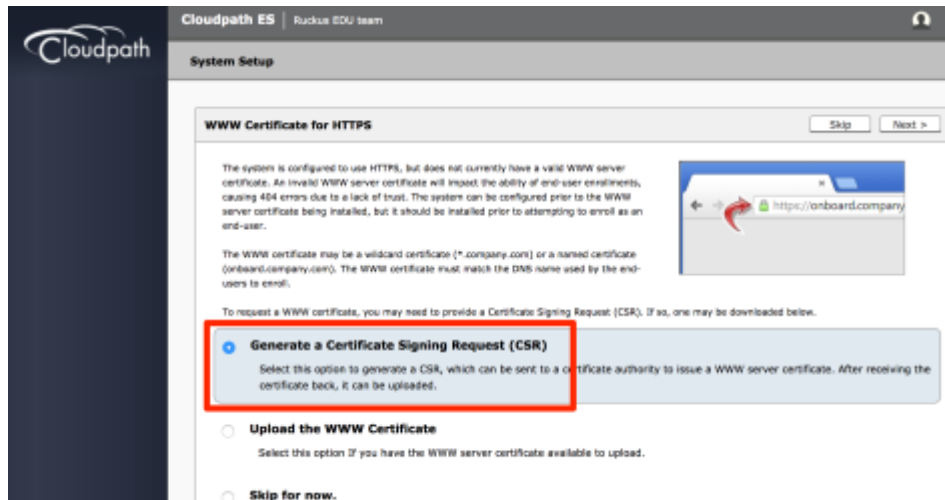
Cloudpath can generate a hostname CSR as shown below. This CSR can be generated from the initial browsing to an insecure installation or from Administration->System->System Services->Web Server->Upload WWW Certificate.



The screenshot shows the Cloudpath ES interface for the 'Web Server' component. The 'Web Server Certificate' section is highlighted with a red box, showing the following details:

- Common Name:** not.for.production.use
- Issuer Name:** Test Intermediate CA
- Validity:** 20101231 through 20291230
- Actions:** Upload WWW Certificate (highlighted with a red box), Delete WWW Certificate

Other visible details include: Web Server Status: Running (0); Using HTTPS: Yes, ports 80 and 443; Ports: 80 and 443; Version: 5.0.3302.



The screenshot shows the 'WWW Certificate for HTTPS' setup screen. The 'Generate a Certificate Signing Request (CSR)' option is selected and highlighted with a red box. The text below it reads: 'Select this option to generate a CSR, which can be sent to a certificate authority to issue a WWW server certificate. After receiving the certificate back, it can be uploaded.'

Other options include 'Upload the WWW Certificate' and 'Skip for now.'

January 2017

### Create CSR for HTTPS

< Back

The fields below will be included in the certificate signing request (CSR). Some organizations have strict requirements for the values required in Leaving fields blank is ok.

**Descriptive Fields**  
The following fields are included in the certificate to identify the owner. These fields are not modifiable, so be careful with spelling.

**Common Name:**  \*

**Organization:**

**Organizational Unit:**

**Email Address:**

**Locality:**

**State:**

**Country:**

**Advanced Fields**  
The following fields are normally not changed.

**Subject Alternative Names:**

**Title:**

**Algorithm:**

**Key Length:**

### Cloudpath ES

Ruckus EDU team

#### System Setup

### Download CSR for HTTPS

Upload

**Step 1:** The certificate signing request (CSR) has been generated. Click the Download CSR button below to download the CSR file.

**Step 2:** Visit the certificate authority website and, when asked to do so, upload this CSR file. After submitting the CSR to the certifi authority, they will normally provide you with 2 files: (1) the certificate and (2) the CA chain.

**Step 3:** If you have the certificate files now, you may upload the certificate now. If not, click 'Upload Later' and you will be prompted upload them the next time you log into the Cloudpath ES.

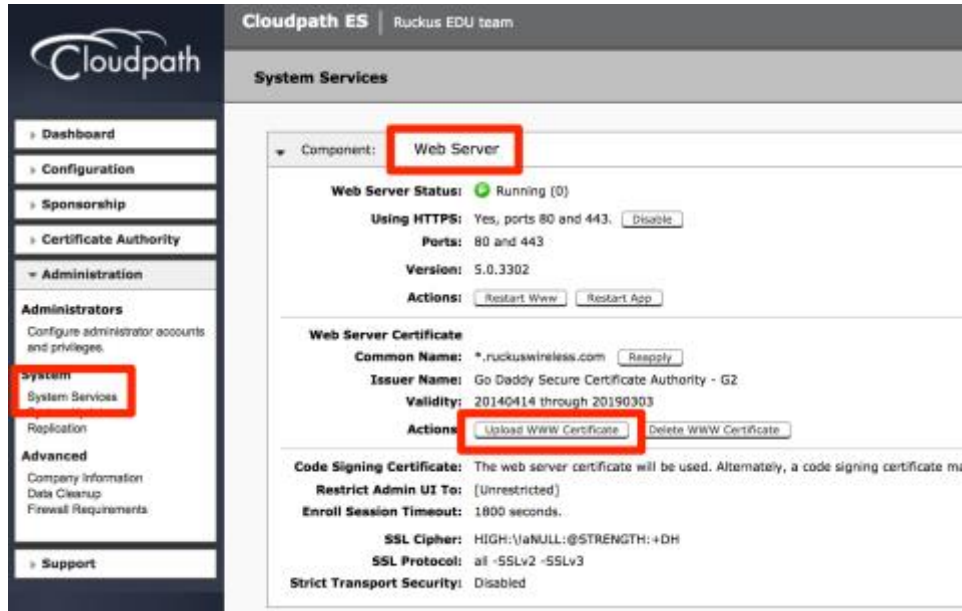
Name	Date Modified
<input type="checkbox"/> cloudpathruckuswirelesscom.csr	Today, 10:42 AM
<input type="checkbox"/> WebEX_Meeting.ics	Today, 9:19 AM
<input type="checkbox"/> Enjoy_Visit_2017-02-03.ics	Jan 24, 2017, 2:36 PM
<input type="checkbox"/> VAR Sales Enablement Workshop Agendas.docx	Jan 19, 2017, 9:15 AM

The CSR is a \*.csr file (found in the browser downloads folder) which is then submitted to the CA.

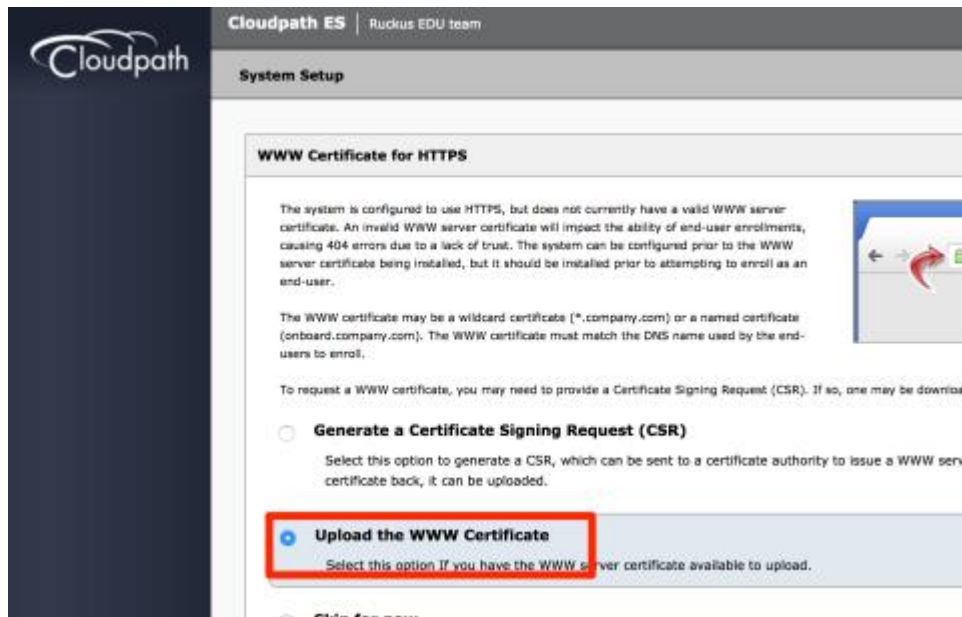
January 2017

## Uploading the WWW Certificate

Cloudpath supports Web Server certificates in the P12 format, password protected P12 or one can upload the individual certificate components: the public key, chain and private key or password protected private key. As shown below, the WWW certificate can be uploaded in Administration->System->System Services->Web Server->Upload WWW Certificate.



The screenshot shows the Cloudpath ES interface. On the left is a navigation menu with 'System Services' highlighted. The main content area is titled 'System Services' and shows the 'Web Server' component selected. The 'Web Server Certificate' section is expanded, showing details like 'Common Name: \*.ruckuswireless.com' and 'Validity: 20140414 through 20190303'. The 'Upload WWW Certificate' button is highlighted with a red box.

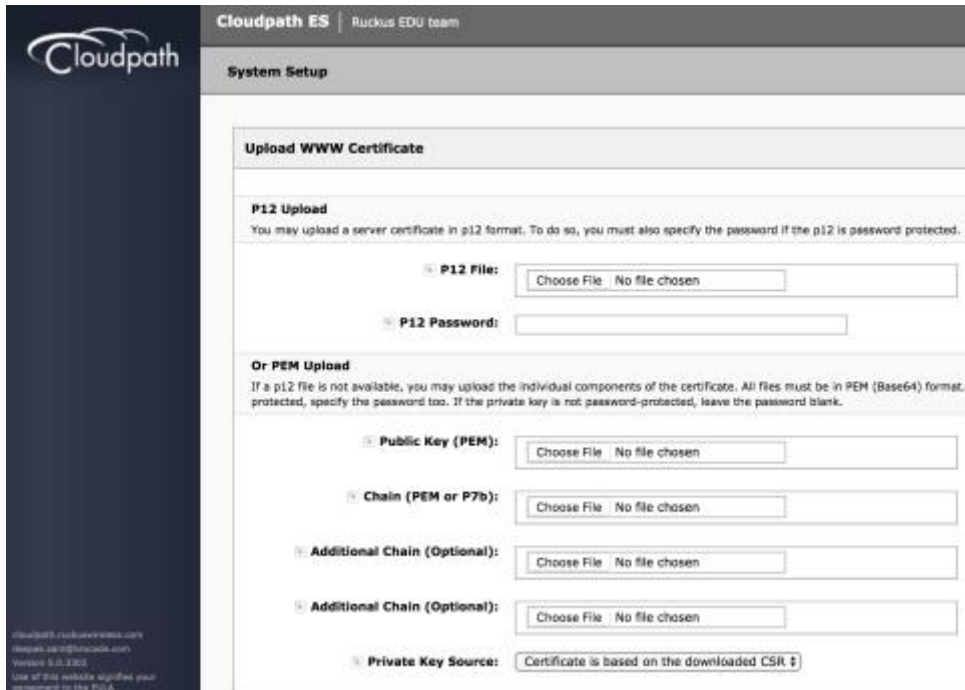


The screenshot shows the 'WWW Certificate for HTTPS' configuration page. It contains explanatory text about certificates and a list of options. The 'Upload the WWW Certificate' option is selected and highlighted with a red box. The other options are 'Generate a Certificate Signing Request (CSR)' and 'Skip for now'.

# How To

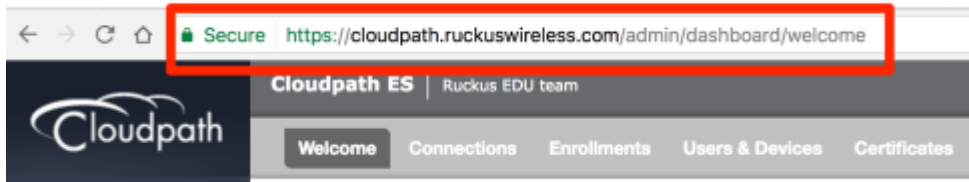
## Purchase & Apply a WWW Server Certificate in Cloudpath

January 2017



## Verification

Once the certificate has been applied, secure HTTPS access is possible as shown below.



### 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, 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