



Managing SSL Certificates for SmartZone Controllers

Installing and managing X.509 certificates for the SmartZone platform

Geeta Kulkarni

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
What's Covered Here	5
Requirements for this Document.....	5
SSL Certificate Overview	6
SmartZone Certificate Overview	7
SmartZone Certificate Store.....	7
Getting an SSL Certificate.....	7
Wildcard Certificates	7
Procedure Overview.....	7
Generate a CSR for the SmartZone	7
Common Issues	15
URL Bar Doesn't Turn Green	15
Appendix A: Purchasing an SSL Certificate.....	16

Intended Audience

This document provides an overview of how to configure a SmartZone to use SSL certificates. Some knowledge of X.509 certificates, public key cryptography and certificate authorities is recommended.

Overview

X.509 SSL certificates are used by SmartZone controllers to secure and encrypt key communications. This document describes how to request, install and manage SSL certificates for use by the Ruckus SmartZone controller platform. This document is broken into the following main categories:

- SSL Certificate Overview
- How the SmartZone Uses SSL Certificates
- Installing an SSL Certificate for SmartZone

What's Covered Here

This document is not an exhaustive description of all possible solutions. It focuses on the basics of how to generate and install an SSL certificate to encrypt and secure communications on the SmartZone controller platform.

Requirements for this Document

In order to successfully follow the steps in this document, the following equipment (at a minimum) is required and assumed:

- A Ruckus SmartZone controller
- An SSL certificate suitable for installation on the SmartZone controller to be deployed

SSL Certificate Overview

SSL (Secure Sockets Layer) is an industry standard which is used by millions of websites for protection of their online transactions with their customers. SSL is the standard security technology that is used for establishing an encrypted link between a web server and a browser. This encrypted link ensures that all the data exchanged between the web server and browsers remain private, integral and secure.

SSL helps prevent attackers, hackers or intrusive companies such as ISPs from tampering with the data sent between the websites and user browsers. It is critical for protecting sensitive information such as a credit card numbers, bank details, personal information, etc. It also helps in preventing the website from eavesdropping, data tampering, message forgery and injecting advertisements into the websites' resources.

In order to create an SSL connection, the web server requires an SSL Certificate. All SSL Certificates are issued to either companies or legally accountable individuals. It will typically contain the domain name of a website, name, address, city, state and country of the company or an individual who is legally accountable for the web domain. It also contains the expiration date of the Certificate and details of the Certification Authority responsible for its issuance. When a browser connects to a secure site it will retrieve the site's SSL Certificate and check that it has not expired, it has been issued by a Certification Authority the browser trusts, and that it is being used by the website for which it has been issued. If it fails on any one of these checks the browser will display a warning to the end user letting them know that the site is not secured by SSL.

Before purchasing an SSL certificate, the user must be aware of his requirements as there is a wide range of certificates the types of SSL certificates available in the market.

Types of SSL Certificates:

1. *Domain Validated SSL Certificates or DV SSL:* SSL certification encrypts and protects information transmitted online from being intercepted and stolen by third parties. On the other hand, plain SSL does not help users cross-check the website's identity. These are easy to obtain online, with no identity check by a human being. The ease of acquiring SSL Certificate has even encouraged phishers and other malicious entities to use them in establishing their online "credibility."
2. *Extended Validation, or [EV SSL](#):* It raises the bar on standard SSL validation processes, incorporating some of the highest standards in identity assurance to establish the legitimacy of online entities. Certificate Authorities put applicant websites through rigorous evaluation procedures and meticulous documentation checks to confirm their authenticity and ownership. This systematic authentication process, also known as the Extended Validation Standard, is based on a set of guidelines prescribed for CAs to adhere to when they receive a request for a digital certificate from an organization or business entity.
3. *Organization validated or OV SSL certificates* require more validation than DV certificates, but provide more trust. For this type, the CA will verify the actual business that is attempting to get the certificate. The organization's name is also listed in the certificate, giving added trust that both the website and the company are reputable. OVs are usually used by corporations, governments and other entities that want to provide an extra layer of confidence to their visitors.
4. *Subject Alternative Name or SAN Certificates:* These certificates offer the same encryption as DV SSL but protect multiple sites. So a single SAN certificate can be used to secure multiple websites like ruckus.com, ruckuswireless.com, tmeruckus.com, etc. These are also called Multi-domain or Unified Communication Certificate (UCC) SSLs.
5. *Wildcard SSL:* A Wildcard SSL encrypts all information submitted to a single website or any of its related pages (subdomains). One single certificate protects all the subdomains of a single domain e.g. one wild card certificate will protect all the websites like ruckus.com, mail.ruckus.com, tme.ruckus.com, etc.

SmartZone Certificate Overview

A SmartZone controller makes use of SSL certificates to perform a number of functions:

- Secure and encrypt management traffic between a client device and the web UI interface
- Secure and encrypt the AP portal page used for web-based authentication
- Secure and encrypt a WISPr hotspot login portal
- Secure and encrypt control traffic between the SmartZone controller and the AP
- Implement Hospot 2.0 OSU Server-Only Authenticated L2 Encryption Network (OSEN)

SmartZone Certificate Store

The certificate store is the central storage for all the security certificates that the controller uses for its web interface, AP portal, and hotspots. By default, each SmartZone controller ships with a certificate issued by the Ruckus Wireless Certificate Authority (CA). However, because this default certificate is signed by Ruckus Wireless and is not recognized by most web browsers, a security warning appears whenever you connect to the web interface or users connect to the AP portal or a hotspot. To prevent these security warnings from appearing, you can import an SSL certificate that is issued by a recognized certificate authority.

Getting an SSL Certificate

Wildcard Certificates

A wildcard certificate is not issued to a specific hostname and can be used for any device using an FQDN within the domain for which it was provisioned. If using a wildcard certificate, steps 1-2 below are not required.

Procedure Overview

Before the default SmartZone certificate can be replaced with a new one, you must get a new certificate provisioned. The following steps are typically used:

1. Generate a Certificate Signing Request (CSR)
2. Submit the CSR to a CA
3. Install the certificate on the SmartZone
4. Assign certificate from the certificate store for a particular functionality

The basic process to acquire an SSL certificate is the same regardless of the CA used, although each CA may have slightly different requirements. For a step-by-step example of how to purchase an SSL certificate, please see [Appendix A: Purchasing an SSL Certificate](#).

Generate a CSR for the SmartZone

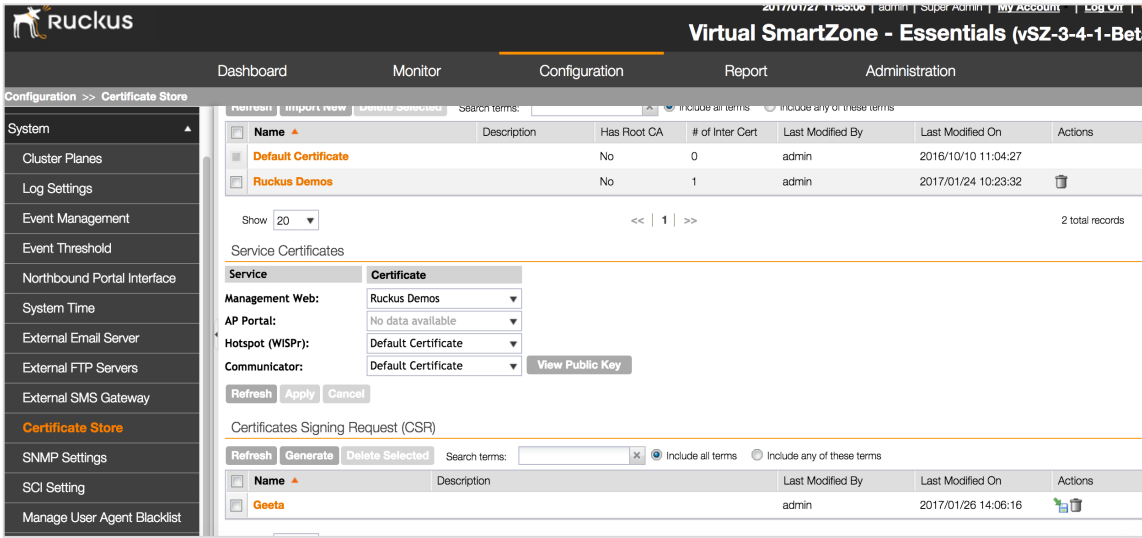
The first order of business is to generate a Certificate Signing Request on the Smart Zone WebUI, followed by creating a request with one of the commercial certificate authorities (CA), SSL certificate providers or domain registrars to complete the purchase. If you do not have an account with that CA you may be required to create one. Public CAs also require a requestor provide proof they have ownership or administrative control over the domain in which the certificate is issued. If this has not already been performed with the CA additional time may be required for verification before a certificate is issued.

Step 1: Generate a Certificate Signing Request (CSR) on the SmartZone

Follow the steps below to generate a certificate request and to import a signed certificate into the controller.

The controller web interface provides a form that you can use to create the CSR file.

1. Go to Configuration > System > Certificate Store. The Certificate Store page appears.
2. In the Certificate Signing Request (CSR) section, click Generate. The Generate New Certificate Signing Request (CSR) form appears.

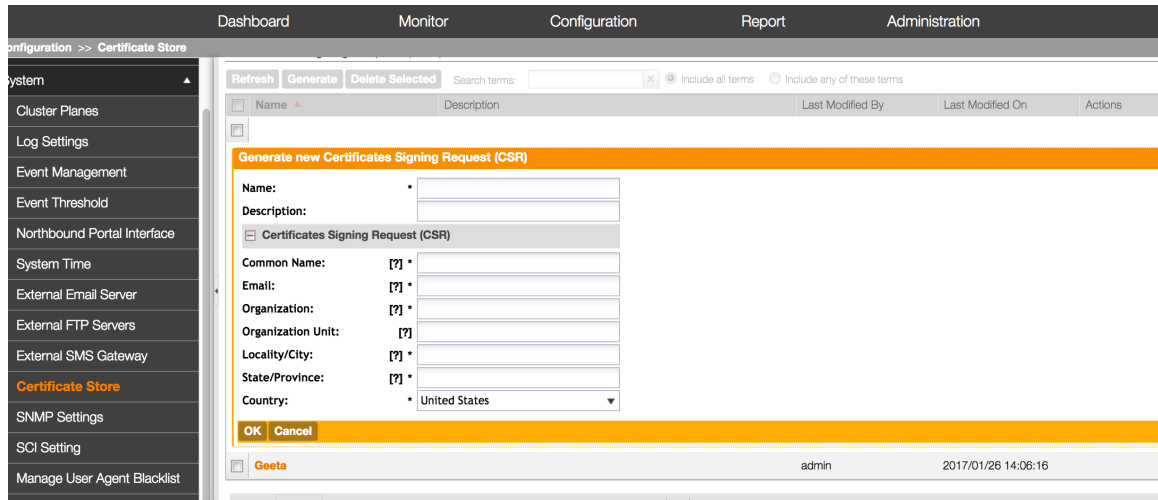


- In Name, type a name for this CSR.
- In Description, type a description for this CSR.
- In the Certificates Signing Request (CSR) section, fill out the following boxes:
- Example of Table 1. Insert> Caption> Table

Option Name	Description
Common Name	Type the fully qualified domain name of your Web server. This must be an exact match (for example, www.ruckuswireless.com)
Email	Type your email address (for example, joe@ruckuswireless.com).
Organization	Type the complete legal name of your organization (for example, Ruckus Wireless, Inc.). Do not abbreviate your organization name
Organization Unit	Type the name of the division, department, or section in your organization that manages network security (for example, Network Management).
Locality/City	Type the city where your organization is legally located (for example, Sunnyvale).
State/Province	Type the state or province where your organization is legally located (for example,

June 2017

	California) Do not abbreviate the state or province name.
Country	Select the country where your organization is location from the drop-down list.



7. Click OK. The controller generates the certificate request. When the certificate request file is ready, your web browser automatically downloads it.
8. Go to the default download folder of your Web browser and locate the certificate request file. The file name is myreq.zip.
9. Use a text editor (for example, Notepad) to open the certificate request file.

Step 2: Submit CSR to a Certificate Authority

The next step of purchasing an SSL certificate is to submit the CSR to one of the commercial certificate authorities or domain registrars, such as godaddy.com, startSSL.com and digicert.com, among many others. In the following steps we shall look at purchasing certificates from godaddy.com. However, other authorities employ similar steps which are easy to follow as well.

In this example, we are purchasing a standard SSL DV (domain verification) certificate. Note that the time period purchased is 2 years. This means the certificate will expire in two years. You may renew the certificate however you will need to upload the new certificate (with the new expiration date) at that time.

SSL Certificates
SSL Certificates
Extended Validation SSL Certificates
Organizational Validation SSL Certificates
SAN SSL Certificate
Wildcard SSL Certificates
Code Signing Certificate

Protect one website

As low as
\$55.99/year
On sale - **Save 20%**
\$69.99 /year when you renew⁴

Add to Cart

- Secures one website
- Strongest encryption on the market
- Available in DV, OV and EV SSL Certificates [?](#)
- Boosts your site's Google ranking
- EV SSL turns browser bar green [?](#)

Protect multiple websites

UCC/SAN SSL [?](#)

As low as
\$134.99/year
On sale - **Save 10%**
\$149.99 /year when you renew⁴

Add to Cart

- Secures up to five websites [?](#)
- Strongest encryption on the market
- Available in DV, OV and EV SSL Certificates [?](#)
- Boosts your site's Google ranking
- EV SSL turns browser bar green [?](#)

Protect all subdomains

Wildcard SSL [?](#)

As low as
\$269.99/year
On sale - **Save 10%**
\$299.99 /year when you renew⁴

Add to Cart

- Secures one website and all its sub-domains
- Strongest encryption on the market
- Available in DV and OV SSL Certificates [?](#)
- Boosts your site's Google ranking

Select your certificate

Standard SSL DV

- Best for blogs and social websites
- Validates domain ownership
- USD \$100,000 warranty

\$55.99/yr
~~\$69.99/yr~~
On Sale (Save 20%)

Deluxe SSL OV

- Best for businesses and organizations
- Validates domain ownership and organization
- USD \$250,000 warranty

\$89.99/yr
~~\$99.99/yr~~
On Sale (Save 10%)

Premium SSL EV

- Best for eCommerce websites
- Validates domain ownership and highest level of organization authentication
- High-assurance green address bar:

\$99.99/yr
~~\$199.99/yr~~
On Sale (Save 50%)

Select Term Length

Lock in your savings with a multi-year term.

1 year

\$69.99/yr

2 years

\$55.99/yr
~~\$69.99/yr~~
On Sale (Save 20%)

3 years

\$49.99/yr
~~\$69.99/yr~~
On Sale (Save 28%)

When you are prompted for the certificate signing request, copy and paste the entire content of myreq.csr. After selecting an appropriate SSL certificate and submitting the CSR, complete the purchase.

After the SSL certificate provider approves your CSR, you will receive the signed certificate via email or would be available to download.

The following is an example of a signed certificate that you will receive from your SSL certificate provider:

June 2017

```
-----BEGIN CERTIFICATE-----
MIIFVjCCBD6gAwIBAgIQLfAGuqKukMumWhbVf5v4vDANBgkqhkiG9w0B
AQUFADCBfnsDELMAkGA1UEBhMCVVMxZjZAVBgNVBAoTDlZlcm1TaWduLC
BJbmMuMR8wHQYDVQQLfnBgEgEFBQcBAQRtMGswJAYIKwYBBQUHMAGGGGh0
dHA6Ly9vY3NwLnZlcm1zaWduLmNvfnbTBDBGgrBgEgEFBQcwAoY3aHR0cD
ovL1NWU1NlY3VyZS1haWEudmVyaXNpZ24uY29tfnL1NWU1NlY3VyZTIw
MDUtYWlhLmNlcjBuBgggrBgEgEFBQcBDARiMGChXqBcMFowWDBWfnFglpbW
FnZS9naWYwITAFMacGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEFGD
AmfnFiRodHRwOi8vbG9nbY52ZXJpc2lnbi5jb20vbnNsb2dvMS5naWYw
DQYJKoZIhvcNfnAQEFBQADggEBAI/S2dmm/kgPeVAlS IHmx-
751o4oq8+fwehRDBmQDaKiBvVXGZ5ZMfnnoc3DMYDjx0SrI9lkPsn223
CV3UVBZo385g1T4iKwXgcQ7/WF6QcUYOE6HK+4ZGcfnHermFf3fv3C1-
FoCjq+zEu8ZboUf3fWbGprGRA+MR/dDI1dTPtSUG7/zWjXO5jC//
fn0pykSlDw/q8hgO8kq30S8JzCwkqrXJfQ050N4TJtgb/
```

Copy the content of the signed certificate, and then paste it into a text file and save the file.

You can now import the SSL certificate into the controller.

Step 3: Import the New Certificate to the SmartZone Certificate Store

When you have an SSL certificate issued by an SSL certificate provider, you can import it into the controller and use it for HTTPS communication.

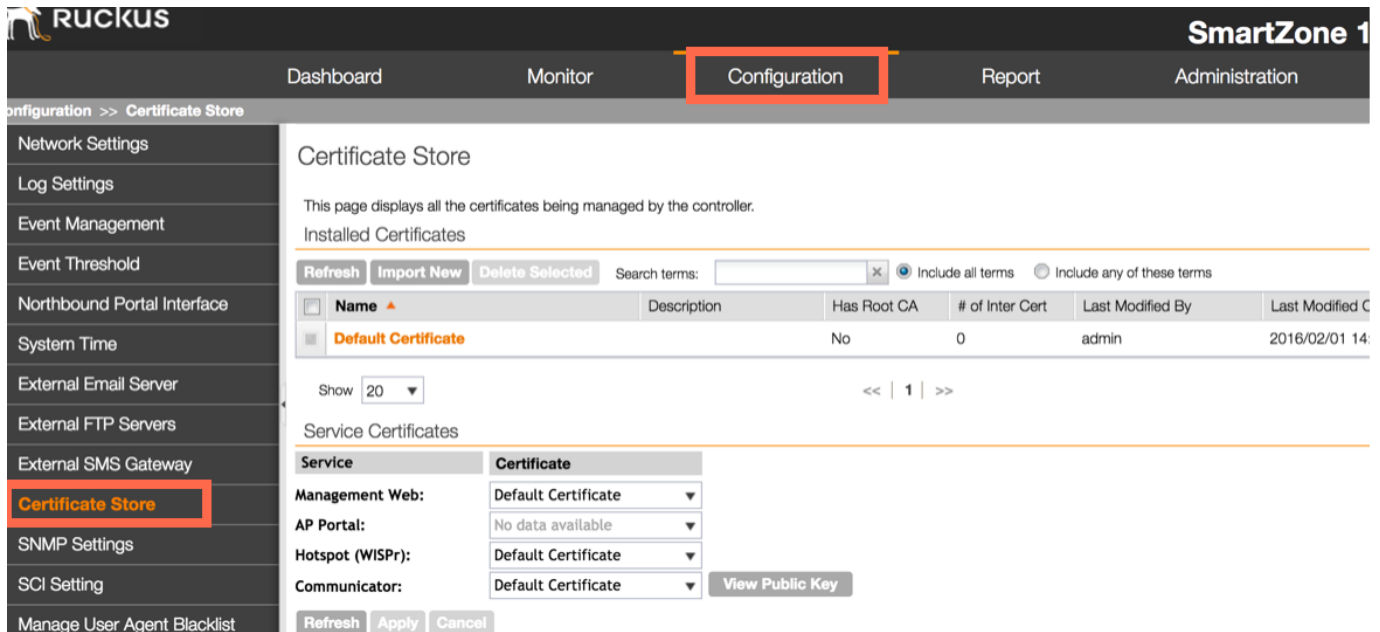
To complete this procedure, you will need the following items:

- The signed server certificate
- The complete CA chain (intermediate and root certificates if applicable)
- The private key file
- The passphrase used for the private key (if used)

NOTE: The file size of each signed certificate and intermediate certificate must not exceed 8192 bytes. If a certificate exceeds 8192 bytes, you will be unable to import it into the controller.

Follow these steps to import a signed server certificate.

1. Copy the signed certificate file, intermediate CA certificate file, and private key file to a location (either on the local drive or a network share) that you can access from the controller web interface.
2. Go to Configuration > SCG System.
3. On the sidebar, click Certificate Store. The Certificate Store page appears. The Import New Certificate form appears.



Configuration >> Certificate Store

Certificate Store

This page displays all the certificates being managed by the controller.

Installed Certificates

Refresh Import New Delete Selected Search terms: Include all terms Include any of these terms

Name	Description	Has Root CA	# of Inter Cert	Last Modified By	Last Modified C
Default Certificate		No	0	admin	2016/02/01 14:

Show 20 << | 1 | >>

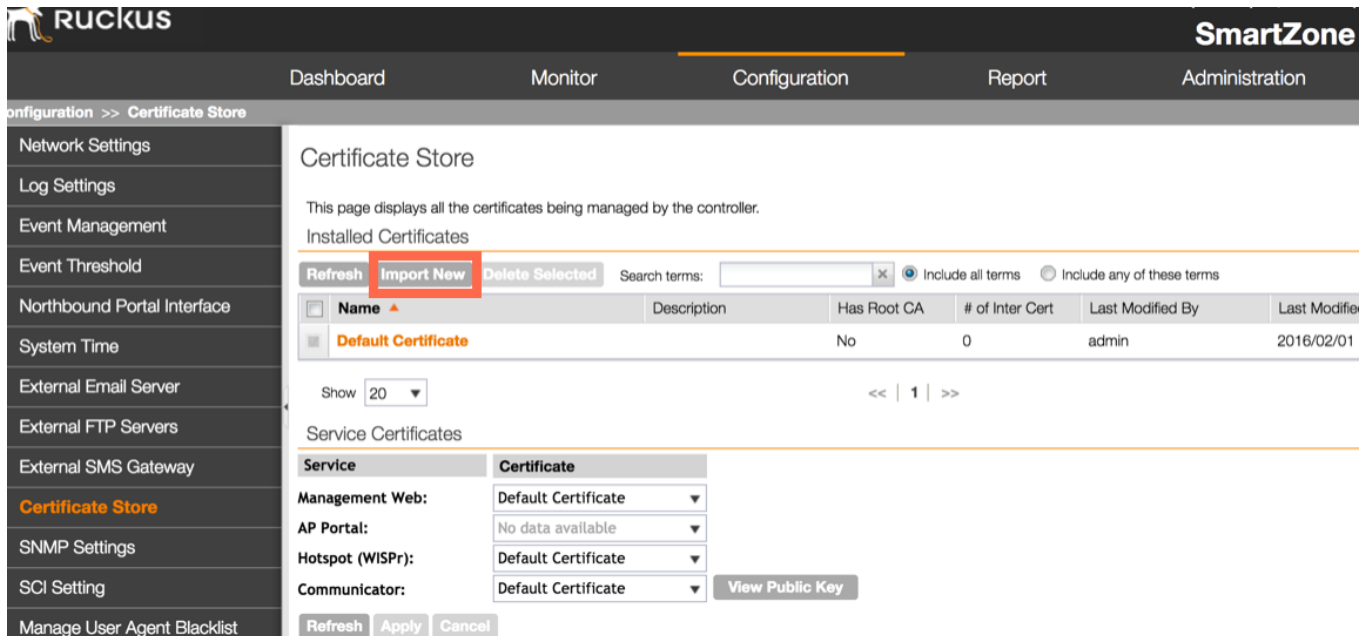
Service Certificates

Service	Certificate
Management Web:	Default Certificate
AP Portal:	No data available
Hotspot (WISPr):	Default Certificate
Communicator:	Default Certificate

View Public Key

Refresh Apply Cancel

- In the Installed Certificates section, click Import New. The Import New Certificate form appears.



Configuration >> Certificate Store

Certificate Store

This page displays all the certificates being managed by the controller.

Installed Certificates

Refresh Import New Delete Selected Search terms: Include all terms Include any of these terms

Name	Description	Has Root CA	# of Inter Cert	Last Modified By	Last Modified
Default Certificate		No	0	admin	2016/02/01

Show 20 << | 1 | >>

Service Certificates

Service	Certificate
Management Web:	Default Certificate
AP Portal:	No data available
Hotspot (WISPr):	Default Certificate
Communicator:	Default Certificate

View Public Key

Refresh Apply Cancel

June 2017

Certificate Store

This page displays all the certificates being managed by the controller.

Installed Certificates

Refresh Import New Delete Selected Search terms: Include all terms Include any of these terms

<input type="checkbox"/>	Name ▲	Description	Has Root CA	# of Inter Cert	Last Modified By	Last Modified On	Act
Import new Certificate							
Name: *		<input type="text"/>					
Description:		<input type="text"/>					
<input checked="" type="checkbox"/> Server Certificate							
OK Cancel							
<input type="checkbox"/>	Default Certificate		No	0	admin	2016/02/01 14:22:11	

- Import the server certificate by completing the following steps:
 - In Server Certificate, click Browse. The Open dialog box appears.
 - Locate and select the certificate file, and then click Open.
- Import the intermediate CA certificate by completing the following steps: a) In Intermediate CA certificate, click Browse. The Open dialog box appears. b) Locate and select the intermediate CA certificate file, and then click Open.
- If you need to upload additional intermediate CA certificates to establish a chain of trust to the signed certificate, repeat the above step.
- When you finish uploading all the required intermediate certificates, import the private key file either by uploading file itself or selecting the CSR you generated earlier.
 - Optional: To upload the private key file, click Upload. Click Browse, locate and select the private key file. Click Open.
 - Optional: To select the CSR, click Using CSR, then select the CSR that you generated earlier.

Dashboard Monitor Configuration Report Administration

Configuration >> Certificate Store

Network Settings
Log Settings
Event Management
Event Threshold
Northbound Portal Interface
System Time
External Email Server
External FTP Servers
External SMS Gateway
Certificate Store
SNMP Settings
SCI Setting
Manage User Agent Blacklist

Server Certificate: * a6f07ca0ebc8c1f.crt Browse Clear

Intermediate CA certificate: [?] gd_bundle-g2-g1.crt Browse Clear

Browse Clear

Browse Clear

Root CA certificate: [?] Browse Clear

Private Key: * Upload ruckusdemos.net.key Browse Clear

Using CSR No data available

Key Passphrase:

OK Cancel

<input type="checkbox"/>	Default Certificate		No	0	admin	2016/02/01 14:22:11	
--------------------------	---------------------	--	----	---	-------	---------------------	--

- In Key Passphrase, enter the passphrase that has been assigned to private key file.
- Click OK. The page refreshes and the certificate you imported appears in the Installed Certificate section.

June 2017

Step 4: Assign the Certificate

Once the certificate has been uploaded to the certificate store, the final step is to assign the certificate to the desired functionality. A SmartZone controller makes use of SSL certificates to perform a number of functions:

- Secure and encrypt management traffic between a client device and the web UI interface
- Secure and encrypt the AP portal page used for web-based authentication
- Secure and encrypt a WISPr hotspot login portal
- Secure and encrypt control traffic between the SmartZone controller and the AP
- Implement Hospot 2.0 OSU Server-Only Authenticated L2 Encryption Network (OSEN)

Certificate Store

This page displays all the certificates being managed by the controller.

Installed Certificates

Name	Description	Has Root CA	# of Inter Cert
Default Certificate		No	0

Refresh Import New Delete Selected Search terms: Include all terms Include any of these terms

Show 20 << | 1 | >>

Service Certificates

Service	Certificate
Management Web:	Default Certificate
AP Portal:	No data available
Hotspot (WISPr):	Default Certificate
Communicator:	Default Certificate

Refresh Apply Cancel View Public Key

Dashboard Monitor Configuration Report Administration

Configuration >> Certificate Store

This page displays all the certificates being managed by the controller.

Installed Certificates

Name	Description	Has Root CA	# of Inter Cert	Last Modified By	Last Modified On
Default Certificate		No	0	admin	2016/02/01 14:22:11
Geeta		No	1	admin	2017/02/13 16:55:59

Show 20 << | 1 | >>

Service Certificates

Service	Certificate
Management Web:	Default Certificate
AP Portal:	Reload...
Hotspot (WISPr):	Default Certificate
Communicator:	Geeta

Refresh Apply Cancel View Public Key

You have completed importing a signed SSL certificate to the controller!

June 2017

Troubleshooting

Common Issues

URL Bar Doesn't Turn Green

This is commonly because the browser needs to be refreshed or the URL does not contain the correct FQDN. A URL containing the IP address of the controller will not match a certificate issued to an FQDN.

Appendix A: Purchasing an SSL Certificate

Purchasing an SSL Certificate is a two-step process. The first order of business is to generate a Certificate Signing Request on the Smart Zone WebUI, followed by creating an account with one of the commercial certificate authorities (CA), SSL certificate providers or domain registrars to complete the purchase.

I. Generate a Certificate Signing Request:

Follow the steps below to generate a certificate request and to import a signed certificate into the controller.

The controller web interface provides a form that you can use to create the CSR file.

10. Go to Configuration > System > Certificate Store. The Certificate Store page appears.

11. In the Certificate Signing Request (CSR) section, click Generate. The Generate New Certificate Signing Request (CSR) form appears.

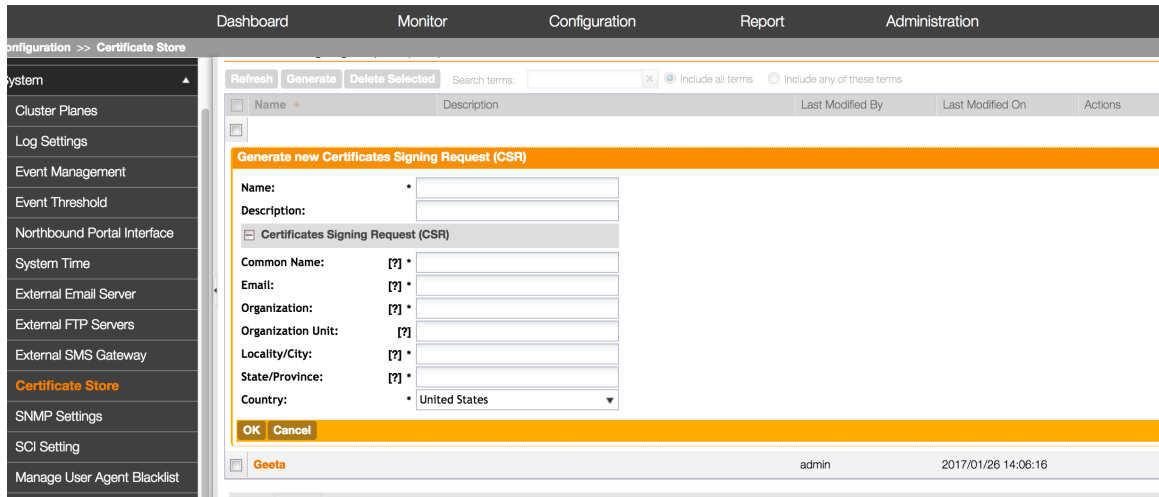
12. In Name, type a name for this CSR.

13. In Description, type a description for this CSR.

14. In the Certificates Signing Request (CSR) section, fill out the following boxes:

Option	Description
Common Name	Type the fully qualified domain name of your Web server. This must be an exact match (for example, www.ruckuswireless.com)
Email	Type your email address (for example, joe@ruckuswireless.com).
Organization	Type the complete legal name of your organization (for example, Ruckus Wireless, Inc.). Do not

	abbreviate your organization name
Organization Unit	Type the name of the division, department, or section in your organization that manages network security (for example, Network Management).
Locality/City	Type the city where your organization is legally located (for example, Sunnyvale).
State/Province	Type the state or province where your organization is legally located (for example, California) Do not abbreviate the state or province name.
Country	Select the country where your organization is location from the drop-down list.



15. Click OK. The controller generates the certificate request. When the certificate request file is ready, your web browser automatically downloads it.
16. Go to the default download folder of your Web browser and locate the certificate request file. The file name is myreq.zip.
17. Use a text editor (for example, Notepad) to open the certificate request file.

II. Completing the purchase:

The next step of purchasing an SSL certificate is to create an account with one of the commercial certificate authorities or domain registrars, such as godaddy.com, startSSL.com and digicert.com, among many others. In the following steps we shall look at purchasing certificates from godaddy.com. However, other authorities employ similar steps which are easy to follow as well.



Protect one website

As low as **\$55.99/year**
On sale - **Save 20%**
\$69.99 /year when you renew⁴

Add to Cart

- Secures one website
- Strongest encryption on the market
- Available in DV, OV and EV SSL Certificates [?](#)
- Boosts your site's Google ranking
- EV SSL turns browser bar green [?](#)

Protect multiple websites

UCC/SAN SSL [?](#)

As low as **\$134.99/year**
On sale - **Save 10%**
\$149.99 /year when you renew⁴

Add to Cart

- Secures up to five websites [?](#)
- Strongest encryption on the market
- Available in DV, OV and EV SSL Certificates [?](#)
- Boosts your site's Google ranking
- EV SSL turns browser bar green [?](#)

Protect all subdomains

Wildcard SSL [?](#)

As low as **\$269.99/year**
On sale - **Save 10%**
\$299.99 /year when you renew⁴

Add to Cart

- Secures one website and all its sub-domains
- Strongest encryption on the market
- Available in DV and OV SSL Certificates [?](#)
- Boosts your site's Google ranking

Select your certificate

<input checked="" type="radio"/> Standard SSL DV <ul style="list-style-type: none"> Best for blogs and social websites Validates domain ownership USD \$100,000 warranty 	\$55.99/yr \$69.99/yr On Sale (Save 20%)
<input type="radio"/> Deluxe SSL OV <ul style="list-style-type: none"> Best for businesses and organizations Validates domain ownership and organization USD \$250,000 warranty 	\$89.99/yr \$99.99/yr On Sale (Save 10%)
<input type="radio"/> Premium SSL EV <ul style="list-style-type: none"> Best for eCommerce websites Validates domain ownership and highest level of organization authentication High-assurance green address bar 	\$99.99/yr \$199.99/yr On Sale (Save 50%)

Select Term Length

Lock in your savings with a multi-year term.

<input type="radio"/> 1 year	\$69.99/yr
<input checked="" type="radio"/> 2 years	\$55.99/yr \$69.99/yr On Sale (Save 20%)
<input type="radio"/> 3 years	\$49.99/yr \$69.99/yr On Sale (Save 28%)

When you are prompted for the certificate signing request, copy and paste the entire content of myreq.csr. After selecting an appropriate SSL certificate and submitting the CSR, complete the purchase.

After the SSL certificate provider approves your CSR, you will receive the signed certificate via email or would be available to download.

The following is an example of a signed certificate that you will receive from your SSL certificate provider:

```
-----BEGIN CERTIFICATE-----
MIIFVjCCBD6gAwIBAgIQLfaGuqKukMumWhbVf5v4vDANBgkqhkiG9w0B
AQUFADCBfnDELMAkGA1UEBhMCVVMxZzAVBgNVBAoTDlZlcm1TaWduLC
BjbmMuMR8wHQYDVQQLfnBgEgFBQcBAQRtMGswJAYIKwYBBQUHMAGGGGh0
dHA6Ly9vY3NwLnZlcm1zaWduLmNvfnbTBDBGgrBgEgFBQcAoY3aHR0cD
ovL1NWU1NlY3VyZS1haWEudmVyaXNpZ24uY29tfnL1NWU1NlY3VyZTIw
MDUtYWlhLmNlcjBuBgggrBgEgFBQcBDARiMGChXqBcMFowWDBWfnFglpbW
FnZS9naWYwITAFMacGBSS0AwIaBBRLa7kolgYMu9BSOJsprEsHiyEFGD
AmfnFiRodHRwOi8vbG9nb352ZXJpc2lnbi5jb20vdmNsb2dvMS5naWYw
DQYJKoZIhvcNfnAQEgFBQADggEBAI/S2dmm/kgPeVALsIHmx-
751o4oq8+fwehRDBmQDaKiBvVXGZ5ZMfnnoc3DMYDjx0SrI9lkPsn223
CV3UVBZo385g1T4iKwXgcQ7/WF6QcUYOE6HK+4ZGcfnHermFf3fv3C1-
FoCjq+zEu8ZboUf3fWbGprGRA+MR/dDi1dTptSUG7/zWjX05jC//
fn0pykSlDw/q8hgO8kq30S8JzCwkqrXJfQ050N4TJtgb/
```

June 2017

Copy the content of the signed certificate, and then paste it into a text file and save the file.

You can now import the SSL certificate into the controller.

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