FortiADC - OCSP Stapling

Version 5.4.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

February 07, 2020
FortiADC 5.4.0 OCSP Stapling
01-540-000000-20200207

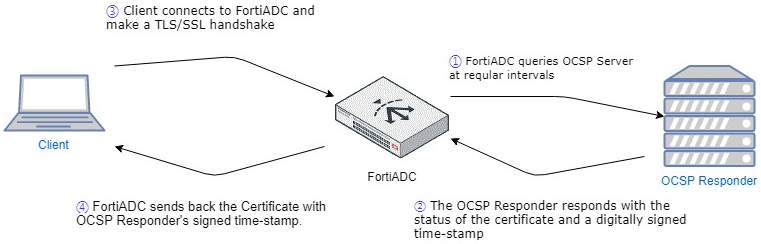
TABLE OF CONTENTS

Change Log

Date	Change Description
2019-09-03	Initial release.

Introduction

OCSP stapling is an improved approach to OCSP, for verifying the revocation status of certificates. Rather than having the client contact the OCSP server to validate the certificate status each time it makes a request, FortiADC can be configured to periodically query the OCSP server and cache a time-stamped OCSP response for a set period. The cached response is then included, or "stapled," with the TLS/SSL handshake so that the client can validate the certificate status when it makes a request.



This method of verifying the revocation status of certificates shifts the resource cost in providing OCSP responses from the client to the presenter of a certificate. In addition, because fewer overall queries to the OCSP responder will be made when OCSP stapling is configured, the total resource cost in verifying the revocation status of certificates is also reduced. FortiADC allows you to upload an OCSP response file, or configure an OCSP to let FortiADC download the OCSP response from the OCSP server, or both.

This document will show you how to setup the OCSP stapling configures.

Before you begin, you must:

- Have Read-Write permission for System settings.
- Have the server certificate added to Local Certificate
- Have the CA that issues the server certificate added to Intermediate CA
- Have the OCSP signing certificate or CA Chain to verify the signature of the OCSP Responder

Deployment

The FortiADC must verify the authenticity of the OCSP responder's SSL certificate. We need to import the Certificate Authority (CA) certificate used to verify the OCSP responder's SSL certificate, or use one of the CA chain certificates.

You should consider using two scenarios under the following condition:

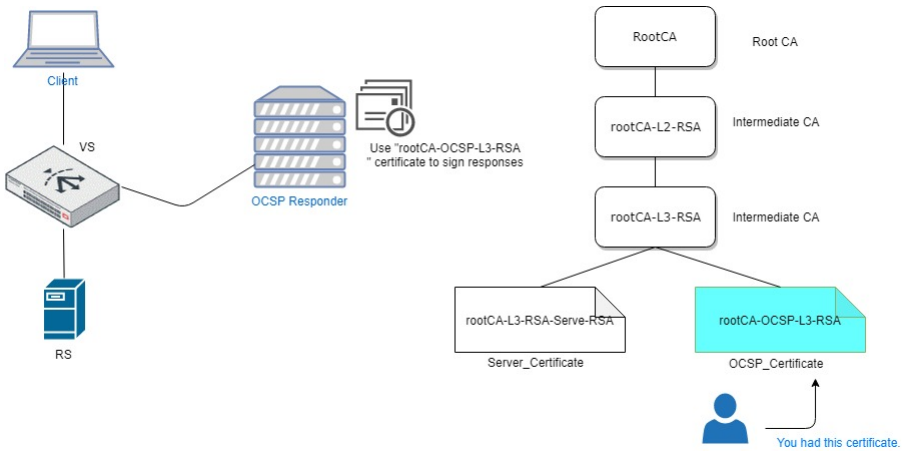
- The OCSP responder's SSL certificate is signed directly by certificate and you have it.
- The OCSP responder's SSL certificate is signed by one of the certificate in the full CA chain and you don't have it.

Once you know the server cert and CA are correct and you can connect to the correct OCSP responde. Now it time to setup the FortiADC.

Scenario 1 –The OCSP responder's SSL certificate is signed directly by the certificate which is in your possession

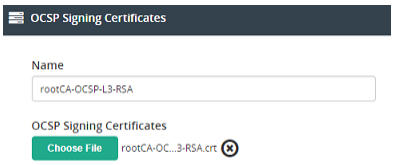
This scenario assumes you have the certificate that is the OCSP responder certificate to sign responses with.

1. Topology



2. Importing the OCSP signing certificates

1. Go to **System > Certificate->Verify** then click the tab **OCSP Signing Certificates**
2. Click **+Import** to display the configuration editor
3. Type a name for the certificate in the text box.
4. Click **Choose File** and browse to the file on your computer for OCSP Signing Certificates.
5. **Save** the configuration.

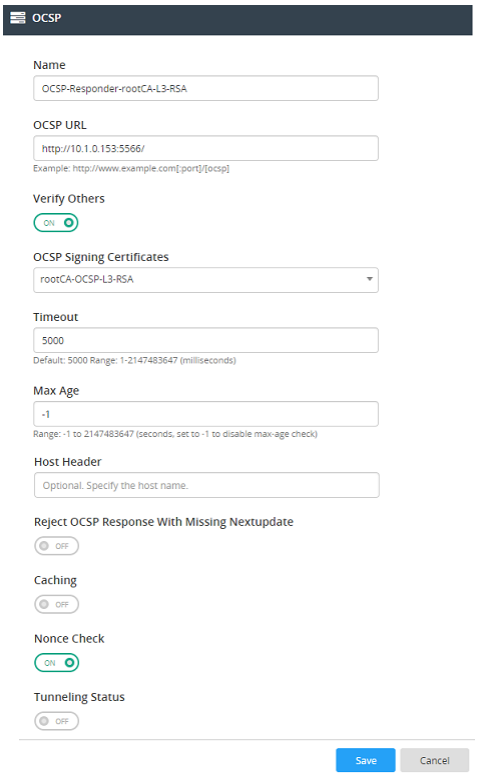


3. Adding OCSPs

1. Go to **System > Certificate->Verify** then click the tab **OCSP**
2. Click **Create New** to display the configuration editor.
3. Complete the key configuration as shown below.

Name	Enter a unique name for the OCSP profile
OCSP URL	Specify the URL of the OCSP Responder.
Verify Others	The default is enabled, you must select an OCSP Signing Certificate.
OCSP Signing Certificates	Selected OCSP signing certificate matches the OCSP response signature.

4. **Save** the configuration.



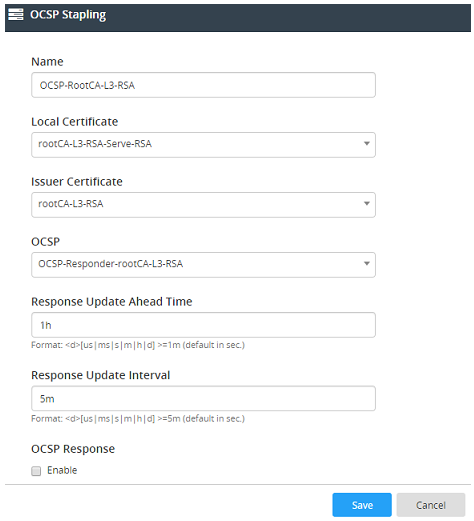
4. To configure OCSP stapling

1. Go to **System > Certificate > Manage Certificates** then Click the tab "**OCSP Stapling**"
2. Click **+Import** to display the configuration editor.

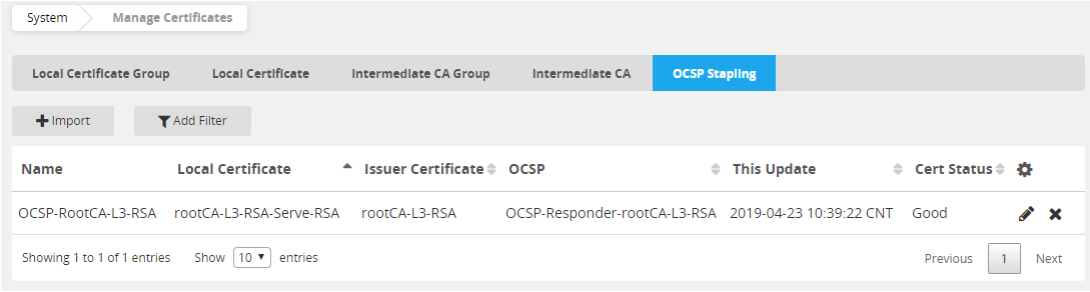
3. Complete the key configuration as shown below.

Name	Enter a unique name for the OCSP stapling.
Local Certificate	Select the Virtual Server's SSL certificate to verify revocation status.
Issuer Certificate	Select the CA certificate that issued the above local certificate.
OCSP	Select the OCSP profile to add to the OCSP stapling configuration

4. Click **Save** to save the configuration.



5. Check if the OCSP responder's Cert Status is good.

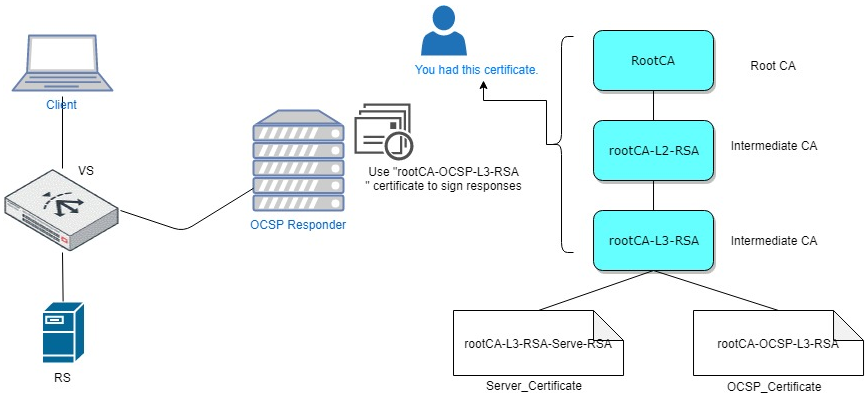


If the query fails, verify that your CA is the same that signed the OCSP responder's certificate. Also verify that the connection between FortiADC and OCSP responder server is reachable. (See Troubleshooting on page 16.)

Scenario 2 – The OCSP responder's SSL certificate is signed by one of th certificates in the full CA chain which is *not* in your possession

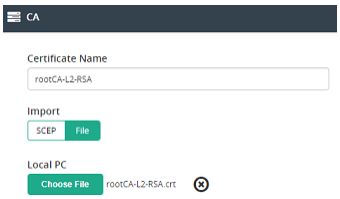
This scenario assumes you do not have the certificate that is the OCSP responder certificate to sign responses with. But you need to have the CA chain from your provider.

1. Topology

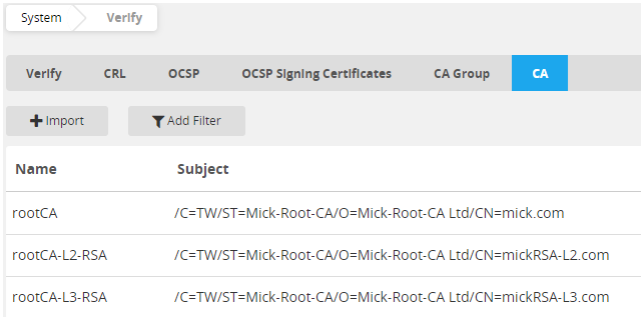


2. To import CAs

1. Go to **System > Certificate > Verify** then Click the tab "**CA**"
2. Click **+Import** to display the configuration editor.
3. Type a name for the certificate in the text box.
4. Click the "File" for Import
5. Click **Choose File** and browse to the file on your computer for CA.
6. **Save** the configuration.

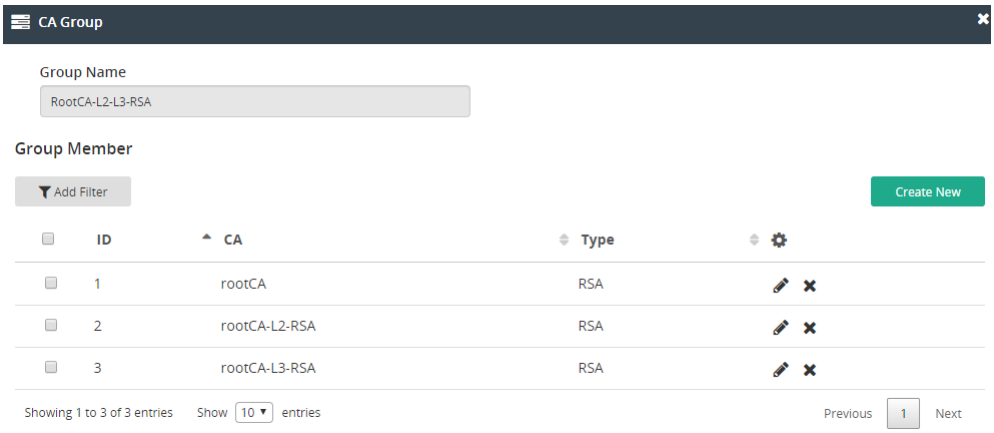


7. Complete all certificates uploaded in the CA chain.



3. Create a CA group

1. Go to **System > Certificate > Verify** then Click the tab "**CA Group**"
2. Click **Create New** to display the configuration editor.
3. Name the CA group and click **Save** when done. The new CA group appears on the CA Group page
4. Click the Edit icon in the far-right column to bring up the configuration editor.
5. Click **Create New.**
6. Click the down arrow and select the desired CA from the list menu to add to the group.
7. Click **Save** when done.

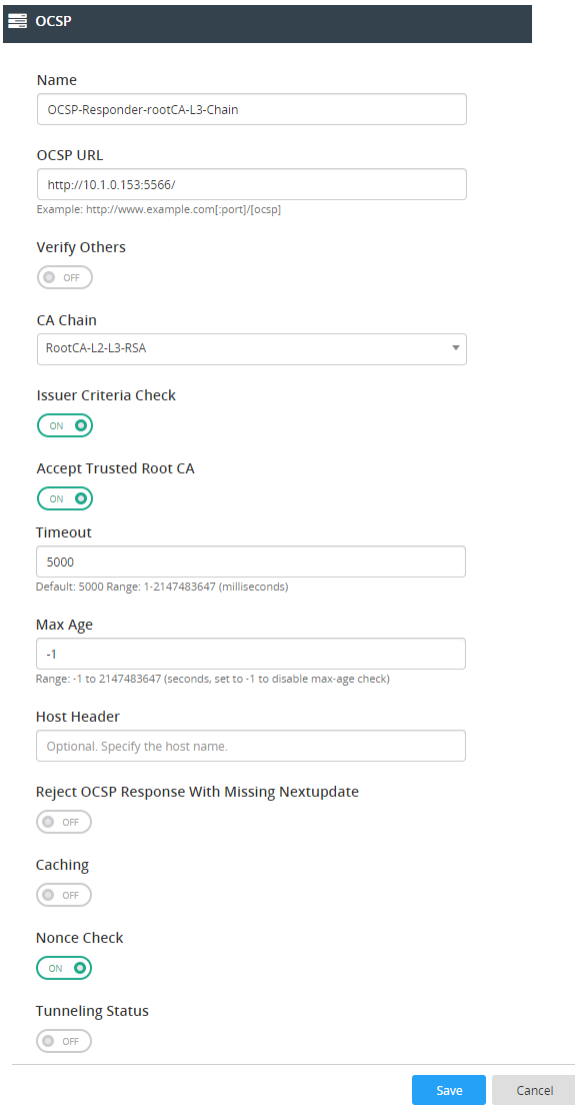


4. Adding OCSPs

1. Go to **System > Certificate->Verify** then click the tab **OCSP.**
2. Click **Create New** to display the configuration editor.
3. 3. Complete the key configuration as below snapshot.

Name	Enter a unique name for the OCSP profile.
OCSP URL	Specify the URL of the OCSP Responder.
Verify Others	Off, you must use CA chain.
CA Chain	Selected a CA chain that matches the OCSP response signature.

4. **Save** the configuration.

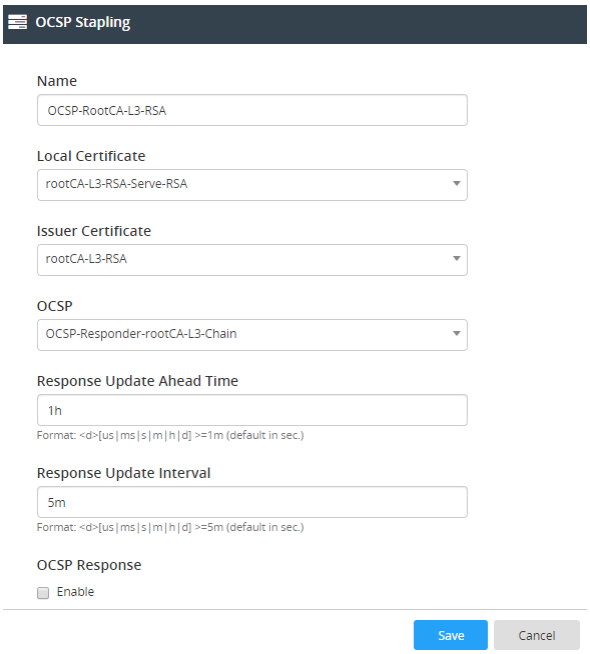


5. To configure OCSP stapling

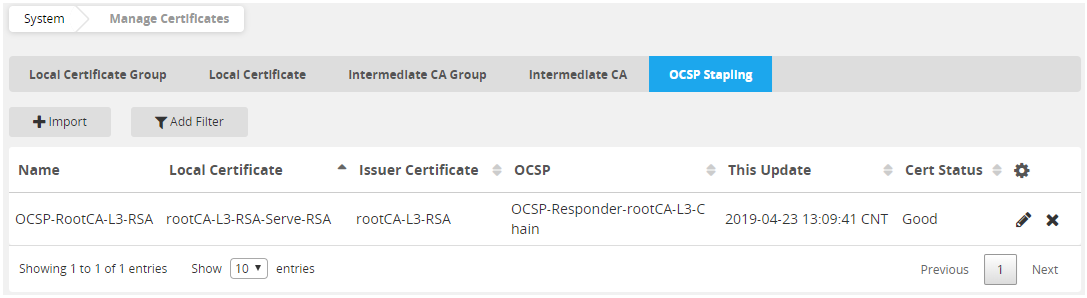
1. Go to **System > Certificate > Manage Certificates** then Click the tab "**OCSP Stapling**"
2. Click **+Import** to display the configuration editor.
3. Complete the key configuration as shown below.

Name	Enter a unique name for the OCSP stapling
Local Certificate	Select the Virtual Server's SSL certificate to verify revocation status.
Issuer Certificate	Select the CA certificate that issued the above local certificate.
OCSP	Select the OCSP profile to add to the OCSP stapling configuration.

4. Click **Save** to save the configuration.



5. Check if the OCSP responder Cert Status is good.



If the query fails, verify that your CA is the same that signed the OCSP responder's certificate. Also verify that the connection between FortiADC and OCSP responder server is reachable. (See Troubleshooting on page 16.)

Apply the settings to VS

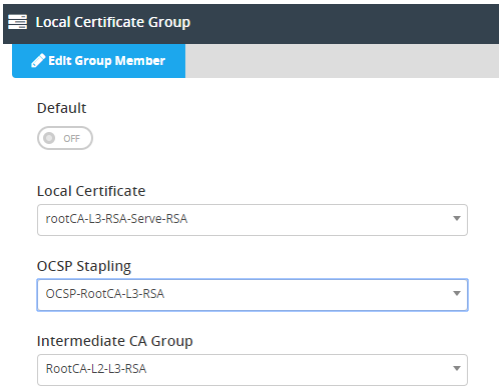
1. Create a local certificate group

1. Go to **System > Certificate > Manage Certificates** then click the tab **Local Certificate Group**.
2. Click **Create New** to display the configuration editor.
3. Complete the key configuration as below snapshot.
4. Enter the **Group Name** then click **Save**.
5. To add Group Members to a Local Certificate Group, click the (edit) icon in the row of the group.
6. Click **Create New** to display the configuration editor.

7. Complete the key configuration as shown below.

Local Certificate	Select the certificate that the virtual server will use.
OCSP Stapling	Select an OCSP Stapling configuration.
Intermediated CA Group	Select the full CA chain of server certificates to the group.

8. Click **Save** to save the configuration

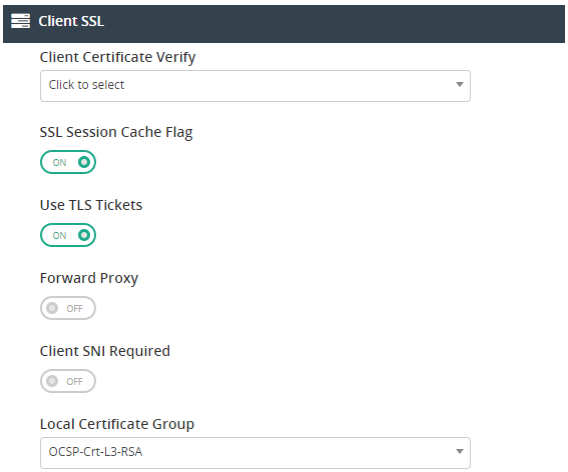


2. Create a Client SSL profile

1. Go to **Server Load Balance > Application Resources** then click the tab **Client SSL.**
2. Click **Create New** to display the configuration editor.
3. 3. Complete the key configuration as shown below.

Name	Enter a unique name for the profile.
Local Certificate Group	Select the one that we just added.

4. Click **Save** to save the configuration.



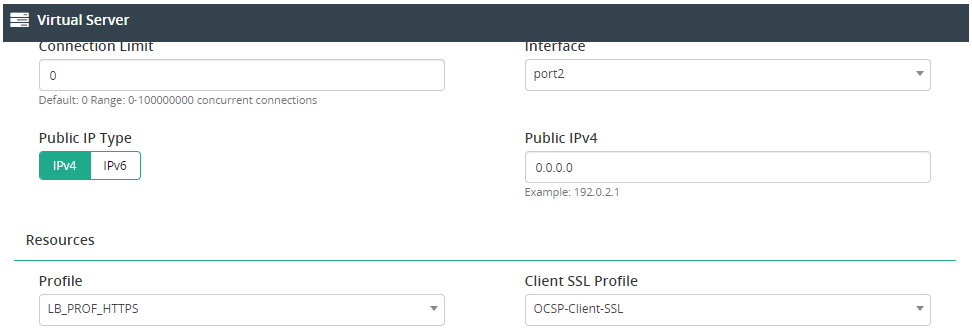
3. Link the Client SSL profile to VS

1. Go to **Server Load Balance > Virtual Server** then click the tab **Virtual Server**.
2. To apply the Client SSL profile to the VS, click the (edit) icon in the row of the virtual servers.

3. Click tab "**General**" to display the configuration
4. Complete the key configuration as shown below.

Client SSL Profile	Select the one that you just added.

5. Click **Save** to save the configuration



Testing OCSP Stapling

We have configured OCSP stapling and we want to test whether or not it works. It is easy to check using the openssl s_client command:

Use OPENSSL

```
openssl s_client -connect yourdomain.com:443 -tlsextdebug -status
```

In the response, look for the OCSP response:

```
OCSP response:
======================================
OCSP Response Data:
OCSP Response Status: successful (0x0)
Response Type: Basic OCSP Response
```

That means the OCSP stapling is working. If you get a response as below, the OCSP stapling is not enabled.

```
OCSP response: no response sent
```

Troubleshooting

If there is any problem with OCSP stapling, we can use the console to print out the diagnose debug message.

1. Setup the diagnose debug print out level in the console

1. Connect your management computer to the FortiADC.
2. Enable the diagnose debug output for crlupdated.

```
FortiADC-VM # diagnose debug module crlupdated all
FortiADC-VM # diagnose debug enable
```

3. You will see the related OCSP information printed.

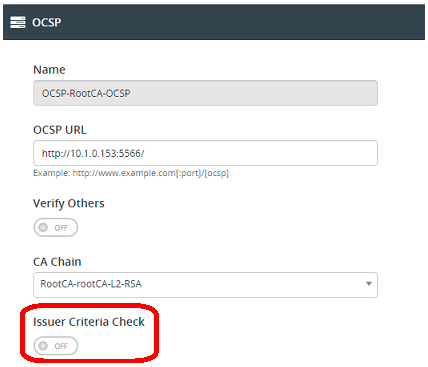
2. The following are common error cases

The delegated check failure:

```
ocsp_download(593): OCSP: Response received
ocsp_download(614): OCSP: OCSP_basic_verify using ca chain
ocsp_download(626): error string is error:2706A067:OCSP routines:ocsp_check_
     delegated:missing ocspsigning usage
ocsp_download(626): error string is error:00000000:lib(0):func(0):reason(0)
ocsp_download(628): OCSP error: OCSP_basic_verify using ca chain
```

Solution:

We can turn off the "Issue Criteria Check" to ignore the the delegated certificate check in the OCSP profile.

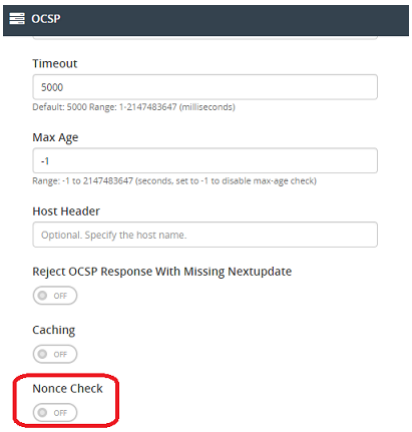


The OCSP nonce check error:

```
ocsp_download(593): OCSP: Response received
ocsp_download(602): OCSP error: OCSP_check_nonce
__poll_callback(702): OCSP download failed
```

Solution:

We can turn off the "Nonce Check" to ignore the the OCSP nonce check failure in the OCSP response.



The Issuers of the OCSP response check failure:

```
ocsp_download(593): OCSP: Response received
ocsp_download(608): OCSP: OCSP_basic_verify using issuers
ocsp_download(610): OCSP error: OCSP_basic_verify using issuers
```

Solution:

The certificate you provided is different from the OCSP responder certificate that signed the response, please correct it using the same with the responder certificate or try to use the CA chain to check it.

If you want to try to use CA chain, please refer to Scenario 2 in Deployment on page 6 in this document.