

Krestfield OCSP Responder

Setup and Configuration Guide

Version 3.5

Overview

The Krestfield OCSP Responder is an RFC6960 compliant OCSP server offering the following features:

- Single stand-alone installation with no need for a separate IIS instance
- Support for Microsoft Security Providers as well as PKCS#11 supporting devices (including nCipher and Thales Luna HSMs)
- Certificate automation - automatic provisioning of signing certificates from your Microsoft CA and auto-renewals
- Multiple CAs can be supported by a single installation

It consists of the following components:

- The Management Console
 - The application that is used to configure the system
- The OCSP Responder Service
 - A windows service that runs independently of the Management Console. It is responsible for processing the requests and returning the responses based on the configuration generated by the Management Console
 - In the Services snap-in this service is named *Krestfield OCSP Responder*

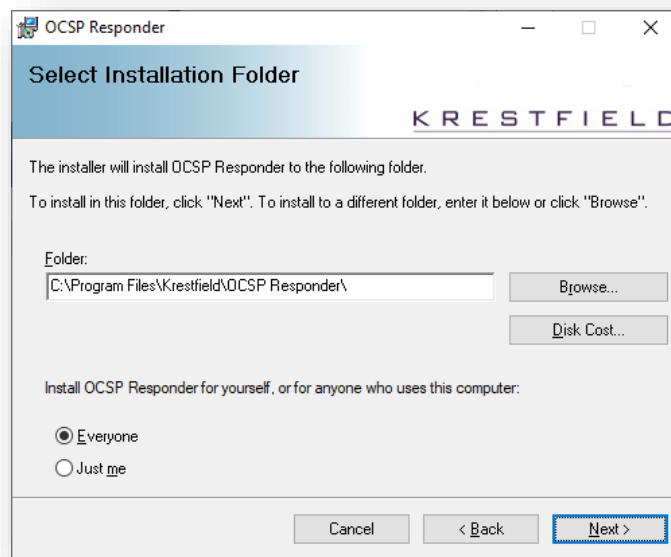
The Krestfield OCSP Responder is supported on the following operating systems:

- Windows Server 2016
- Windows Server 2019

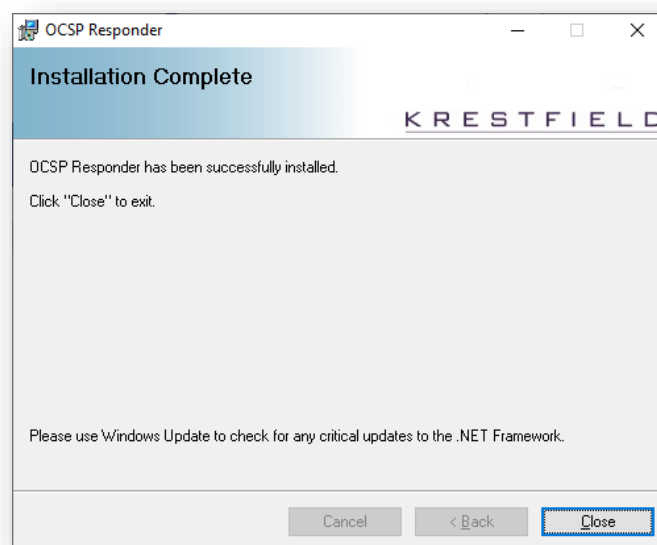
Installation

The server requires .NET version **4.7.2** or above

Double click the **SetupOCSPResponderV3.5.msi** installation file and click **Next** at the start up screen:



Accept the default or choose an alternative installation folder and click **Next** and **Next** again



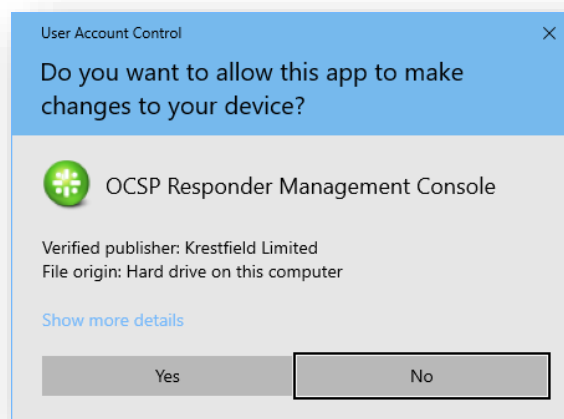
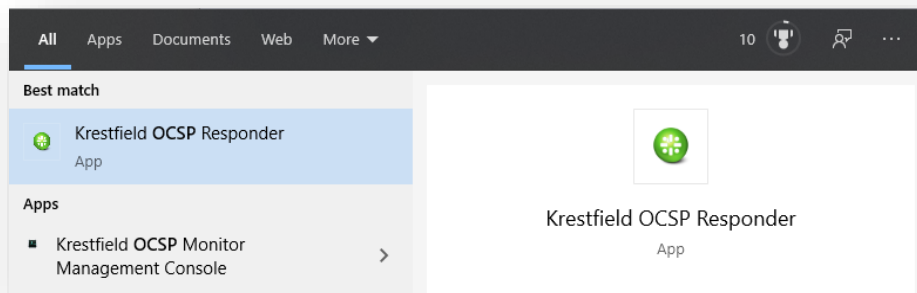
Click **Close**

Starting the Server

Double click the icon from the desktop:

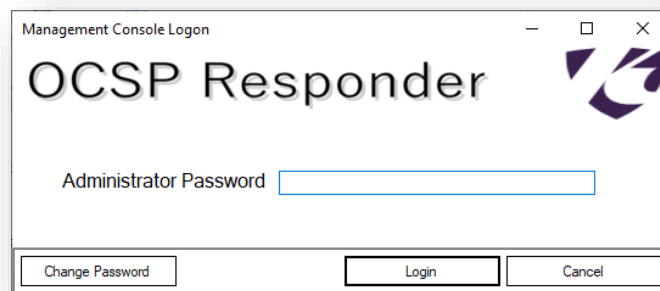


Or click the **Start** button and navigate to **All Programs → Krestfield → OCSF Responder** and click **Krestfield OCSF Responder**



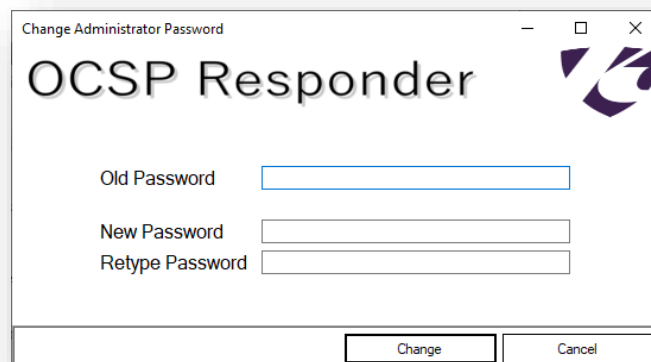
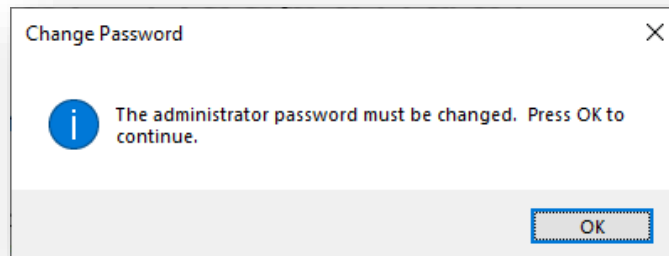
If the User Account Control dialog appears, click **Yes**. The Management Console runs under administrative privileges in order to manage and monitor the underlying OCSF Responder Service

The logon dialog will appear:



Enter the administrative password and press **Login**

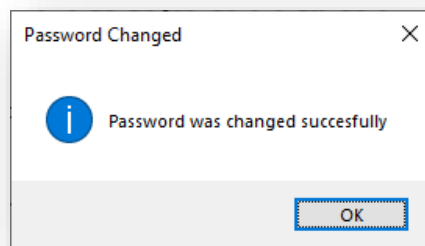
If this is the first time of using the OCSP Responder the following will be displayed:



As you are required to change the default password

The default password (to be enter as Old Password) is **password**. This should be changed to a new stronger password

For New Password type the **new password** and re-enter this in the Retype Password field. Click **Change**

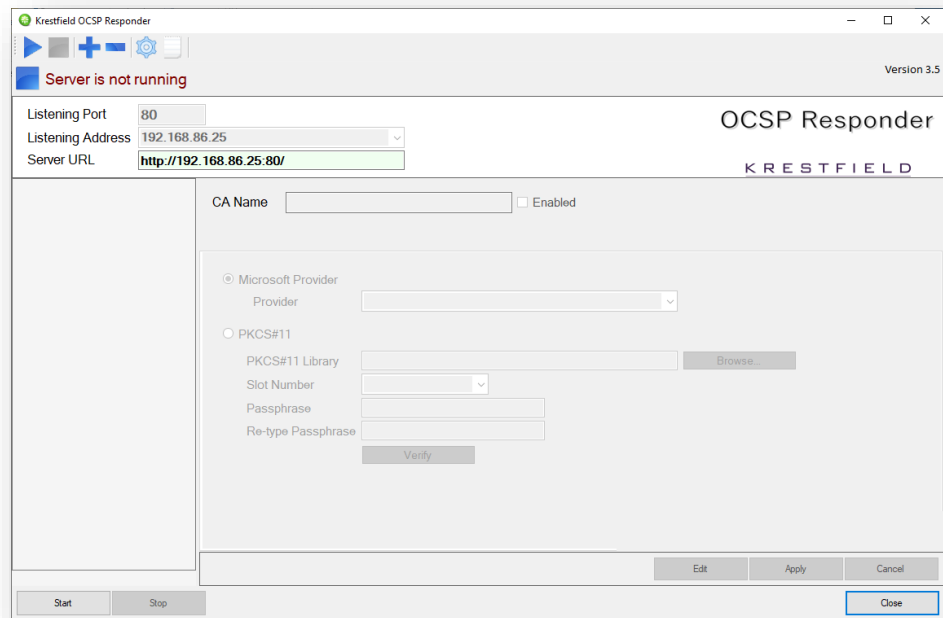


Click **OK** at the Password Changed confirmation dialog. Subsequently you will use this password to login

Note: The change password option can be followed at any point in the future by clicking the **Change Password** option at the logon screen. If the password is lost contact support at support@krestfield.com who will advise on options

Configuration

Once logged in the following screen will be presented:



The main controls are as follows:



Start the OCSP Responder service



Stop the OCSP Responder service



Add a new CA



Delete an existing CA



Display the settings dialog




Display the log file

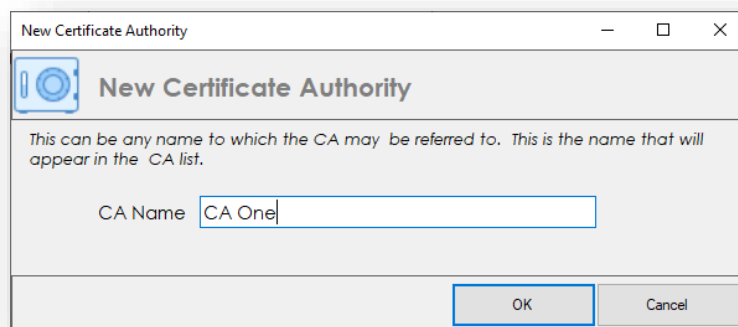
Adding a new CA

The server can cater for any number of CAs. In a regular three tier PKI there are usually one or two OCSP responders – one returning the status of the certificates issued from the Subordinate CA (i.e. the end-entity certificates) and one could be responsible for returning the status of certificates issued from the root CA (i.e. the Subordinate CA certificate and other certificates that may be issued directly from the root – such as OCSP signing certificates)

A single installation of the Krestfield OCSP server can provide the status for certificates issued from both the subordinate and root CAs as well as any number of other CAs. They do not need to be under the same hierarchy - one instance could potentially provide the status from several PKIs

When an OCSP request is received the server will look at the issuer information for that certificate and try to match it against one of the CAs that has been configured. It will then use the settings for this CA to produce a response

To add a new CA, click the **Add new CA** button: 

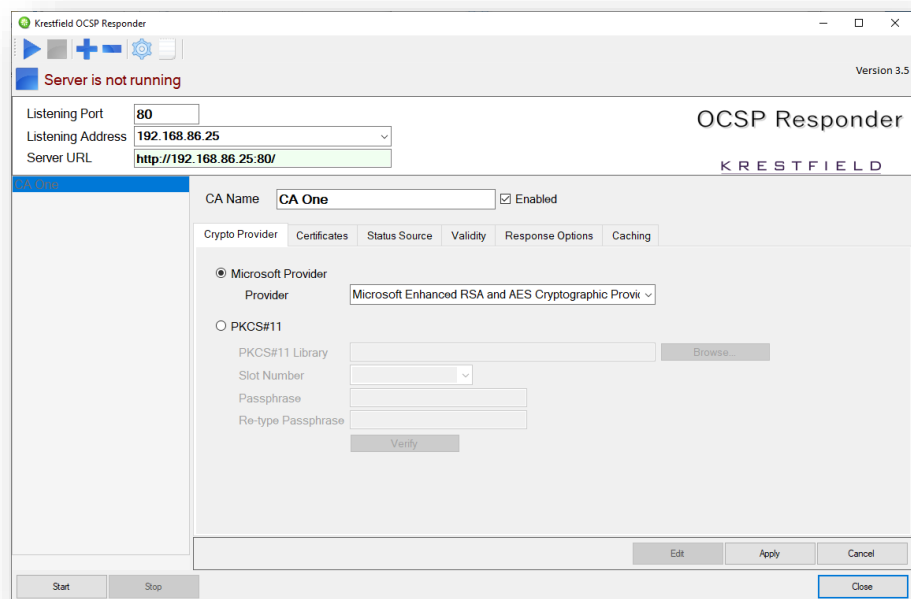


Enter a name for the CA and click **OK**. This can be any name and does not need to be the name of the CA itself, although this is often useful

Configure the Crypto Provider

The Responder supports Microsoft CNG (Crypto Next Generation) security providers and the PKCS#11 interface. Each CA can use either of these interfaces

To configure the Crypto Provider, select the **Crypto Provider** tab



The provider configured here will be used to generate and store the OCSP signing keys

Microsoft Provider

If a Microsoft Crypto Provider is to be used, select **Microsoft Provider** and select from the drop down list the required provider e.g. *Microsoft Enhanced RSA and AES Cryptographic Provider*

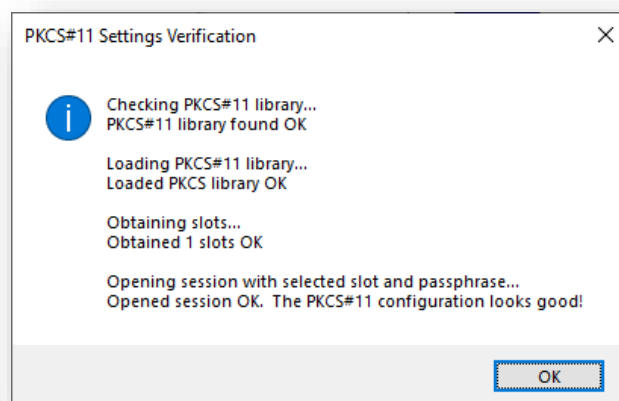
PKCS#11 Provider

If a PKCS#11 Crypto Provider is to be used select **PKCS#11** and browse to the PKCS#11 library (usually a dynamic link library - .dll file) provided by the vendor of the device (e.g. an HSM)

Select from the **Slot Number** combo the slot to use (refer to the vendor documentation for information on which slot to select). For Thales nCipher slot 0 usually refers to the module and slots 1, 2... etc refer to the Operator smartcard slots. If Operator smartcards are being used, select the slot with the label for the cardset in use

Enter the **Passphrase** for the slot and retype. Note: For Thales nCipher, if an Operator card set slot were selected this is the Operator card set passphrase. For other implementations this may be a PIN or a combination of username and pin. Again, refer to the vendor documentation for more details

When all fields have been entered click the **Verify** button to test the configuration



If any errors are reported, check the library, slot and passwords are correct that the PKCS#11 device has been configured correctly and is accessible. Then retry

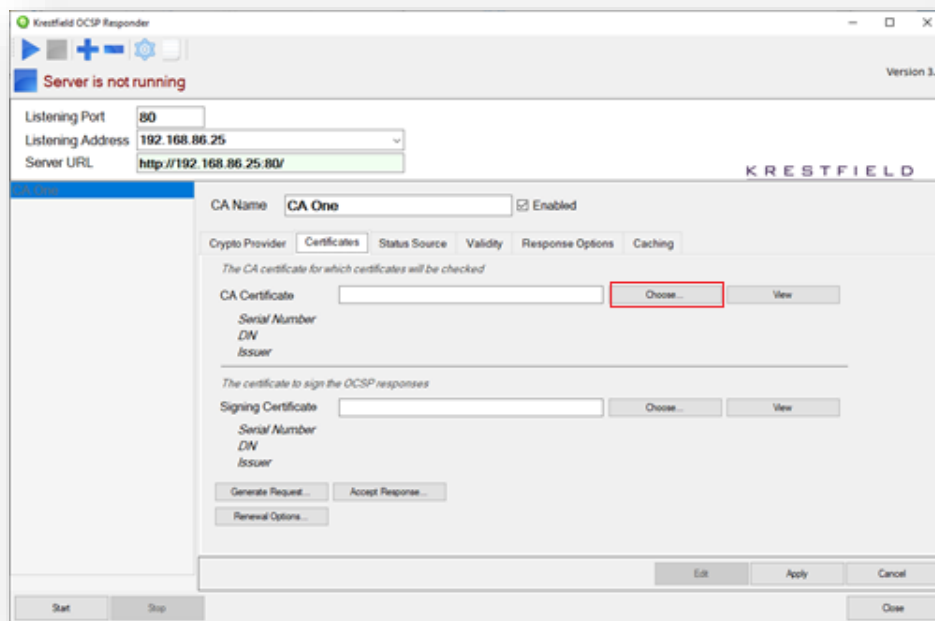
Click **Apply**

Configure Certificates

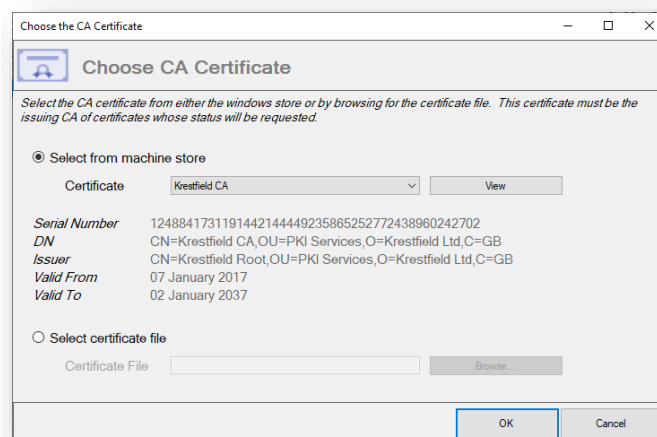
Before configuring the certificates ensure that the Crypto Provider has been specified and the configuration applied

For each CA, the CA certificate itself must be specified. This is the issuer certificate of the certificates whose status will be responded on

Select the **Certificates** Tab and click **Edit**



Click **Choose** from the **CA Certificate** section



If the CA is already in the machine store, choose the correct CA certificate from the drop down. Otherwise, select the **Select certificate file** option and click **Browse** to locate the CA certificate file. Once the CA certificate has been chosen, click **OK**

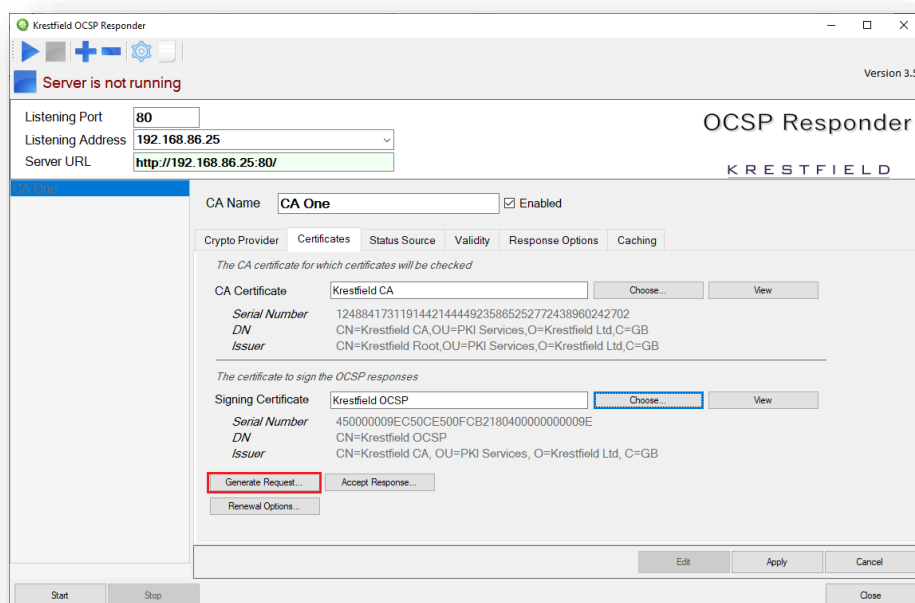
Next, the signing certificate must be specified. This is the certificate that will sign the OCSP responses and is usually issued from the CA the responder is providing responses for, but can also be from a CA further up the hierarchy (e.g. the root CA), or from another delegated CA

If a signing certificate already exists in the Crypto Provider selected i.e. in the local Microsoft store (if a Microsoft Provider was selected), or on the PKCS#11 device (if PKCS#11 selected) then click **Choose** against the Signing Certificate

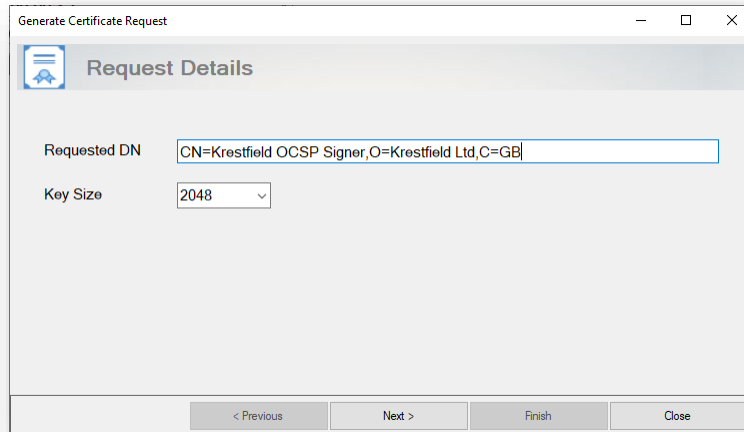


From the **Certificate** drop down select the required signing certificate and then click **OK**

If the certificate has not yet been issued, it is possible to generate a request as follows:



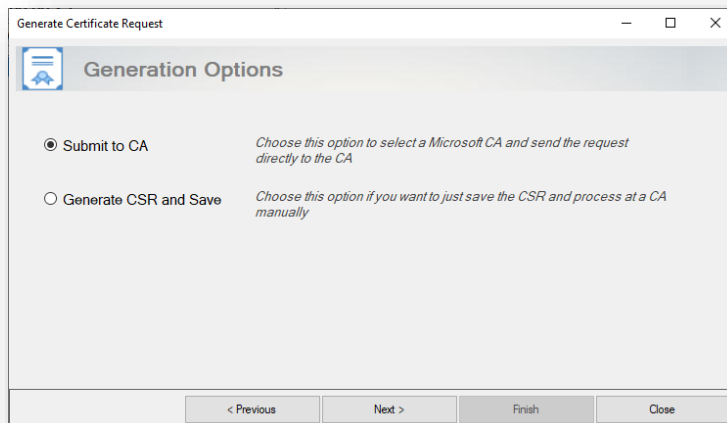
Back on the **Certificates** tab, click the **Generate Request** button



The screenshot shows the 'Generate Certificate Request' dialog box with the 'Request Details' tab selected. The 'Requested DN' field contains the text 'CN=Krestfield OCSP Signer,O=Krestfield Ltd,C=GB'. The 'Key Size' dropdown menu is set to '2048'. At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Close'.

Enter the required distinguished name in the **Requested DN** field and select the key size. The key algorithm will be RSA

Click **Next**

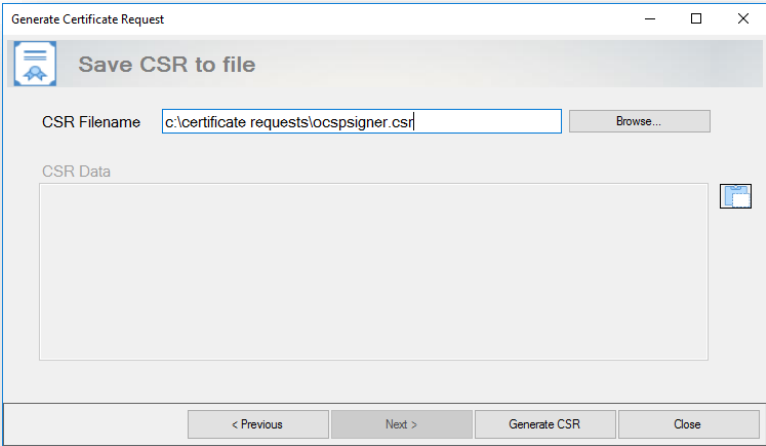



The screenshot shows the 'Generate Certificate Request' dialog box with the 'Generation Options' tab selected. There are two radio button options: 'Submit to CA' (selected) and 'Generate CSR and Save'. The 'Submit to CA' option has a description: 'Choose this option to select a Microsoft CA and send the request directly to the CA'. The 'Generate CSR and Save' option has a description: 'Choose this option if you want to just save the CSR and process at a CA manually'. At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Close'.

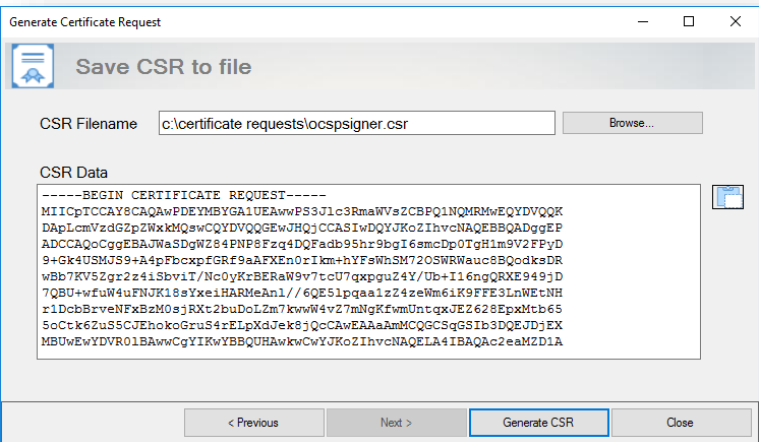
If you wish the OCSP Responder to obtain the certificate automatically, select the **Submit to CA** option. Otherwise, select the **Generate CSR and Save** option. This latter option will require manual processing of the CSR (Certificate Signing Request)

Generate CSR and Save

If the *Generate CSR and Save* option is chosen, clicking **Next** will display the following:

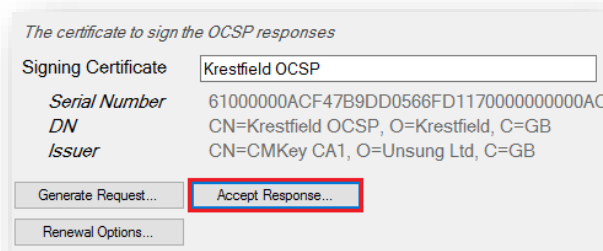



Choose a location to save the CSR and click **Generate CSR**. The CSR will be saved to the location specified and also displayed in the *CSR Data* text box. This CSR data can be copied by clicking the  button

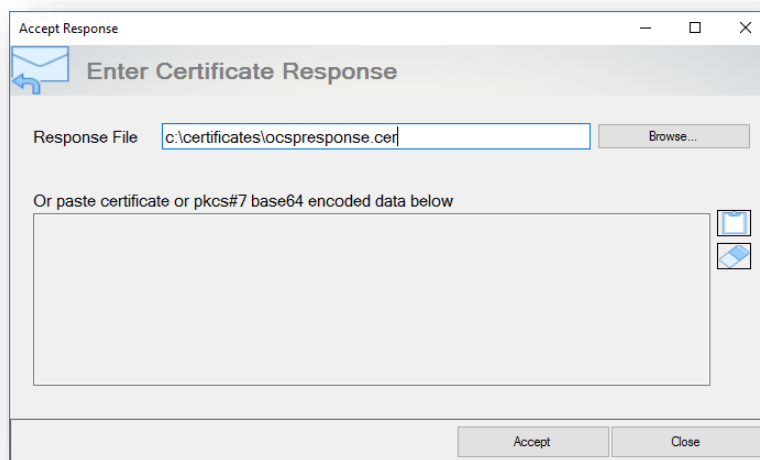


Click **Close** when finished to close the dialog

This CSR must be processed at the issuing CA and the certificate response (as a .cer or .p7b file) obtained. When this has been carried out, back on the **Certificates** tab, click the **Accept Response...** button:



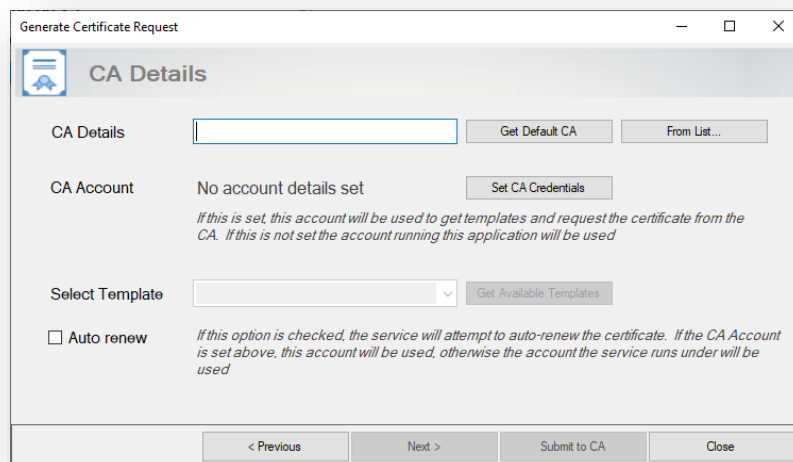
Either select the location of the Response File or if the data is PEM encoded it can be pasted in by clicking the  button



Click **Accept**

Submit to CA

If *Submit to CA* is chosen the following screen will be shown:



The screenshot shows a 'Generate Certificate Request' dialog box with a 'CA Details' tab. The 'CA Details' field is empty, with buttons for 'Get Default CA' and 'From List...'. The 'CA Account' section shows 'No account details set' with a 'Set CA Credentials' button and a note: 'If this is set, this account will be used to get templates and request the certificate from the CA. If this is not set the account running this application will be used'. The 'Select Template' dropdown is empty, with a 'Get Available Templates' button. The 'Auto renew' checkbox is unchecked, with a note: 'If this option is checked, the service will attempt to auto-renew the certificate. If the CA Account is set above, this account will be used, otherwise the account the service runs under will be used'. At the bottom are buttons for '< Previous', 'Next >', 'Submit to CA', and 'Close'.

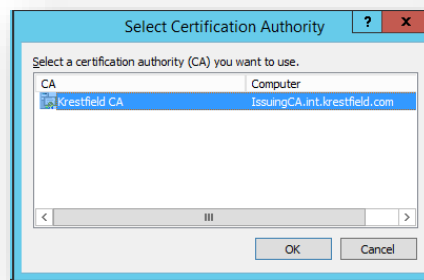
CA Details

For CA Details, enter the CA details in the form `hostname\ca_name`, as returned in the config section when `certutil` is run e.g.:

```
C:\>certutil
Entry 0: (Local)
Name: 'Krestfield CA'
Organizational Unit: 'PKI Services'
Organization: 'Krestfield Ltd'
Locality: ''
State: ''
Country/region: 'GB'
Config: 'IssuingCA.int.krestfield.com\Krestfield CA'
Exchange Certificate: 'IssuingCA.int.krestfield.com_Krestfield CA.crt'
Signature Certificate: 'IssuingCA.int.krestfield.com_Krestfield CA.crt'
Description: ''
Server: 'IssuingCA.int.krestfield.com'
Authority: 'Krestfield CA'
Sanitized Name: 'Krestfield CA'
Short Name: 'Krestfield CA'
```

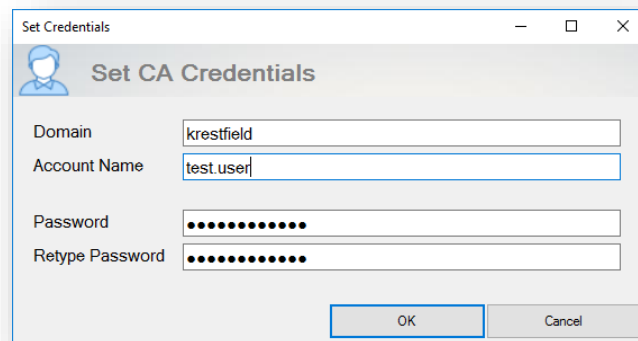
In the above example the CA details would be: `IssuingCA.int.krestfield.com\Krestfield CA`

Alternatively, to populate this field with the default CA details (e.g. if you only have one CA in your environment), click **Get Default CA**. Or, if you have multiple CAs available you may click **From List...** which will present a dialog from where the chosen CA can be selected

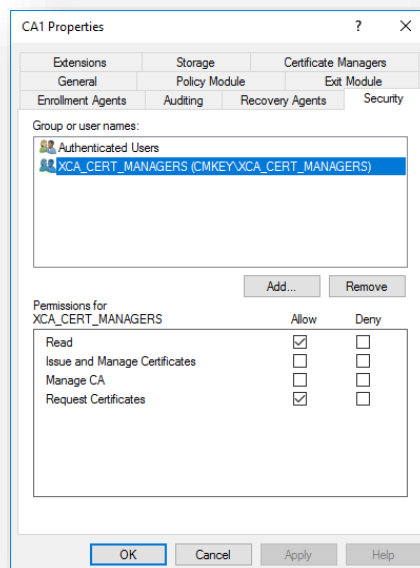


Set CA Credentials

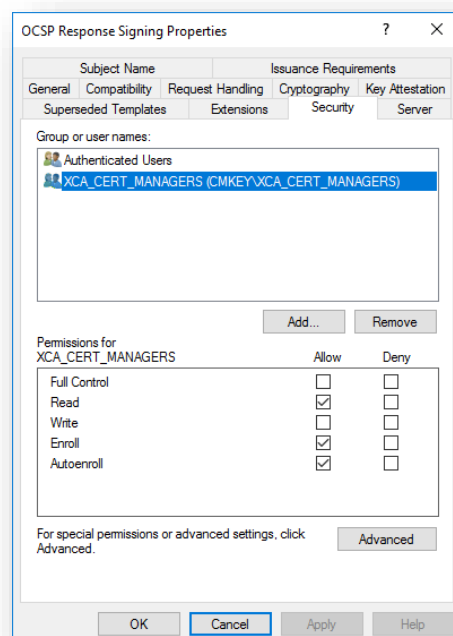
The account that will be used to communicate with the CA may be set by clicking the **Set CA Credentials** button and completing the form:



These account details (or a group the user is a member of) must have permissions to request certificates from the CA. The following example shows the CA properties with the *Security* tab selected. A group called XCA_CERT_MANAGERS has *Read* and the *Request Certificates* privileges. If the account to be specified is a member of this group they will be able to request certificates



The user (or group they are a member of) will also require *Read*, *Enroll* and *Autoenroll* permissions on the certificate template. The following example shows the properties of the *OCSP Response Signing* template with the *Security* tab selected. The XCA_CERT MANAGERS group has the required permissions set, so any account in this group will be able to auto-enrol for certificates from this template



If no CA Credentials are set then the accounts that run the management console and underlying service (Krestfield OCSP Responder) will be used when certificates are issued. If you wish to use this option, you should set the service to run under a specific service account that has the correct permissions

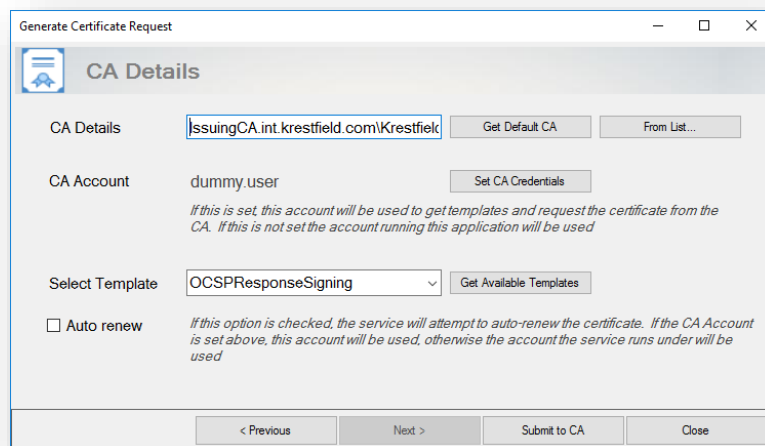
Credentials are encrypted by the application and also tied to the hosting server. They are not stored in the clear in the configuration

Get Available Templates

Click this option to obtain the list of available OCSP signing templates on the targeted CA. If an account has been set in the CA Credentials dialog, this will be used to request the available templates from the CA, otherwise the account the Management Console is running under will be used

Select the required template from the drop down

Note only templates that have the OCSP Signing enhanced key usage set will be listed here



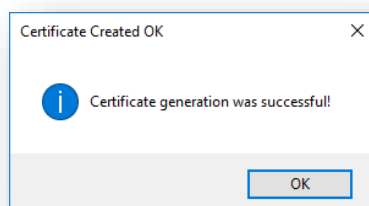
Auto Renew

The certificate can be renewed before it expires automatically. Click the **Auto renew** check box to enable this. Note that this operation will be performed by the service and so the service account or CA Account set previously will be used to request the certificate from the CA

Further renewal options such as frequency of checking etc. can be set on the options dialog (see Cert Expiry Checks below)

Generate Request

Click the Generate Request option to generate the CSR using the selected Crypto Provider, submit the request to the CA, import the certificate and configure it as the signing certificate



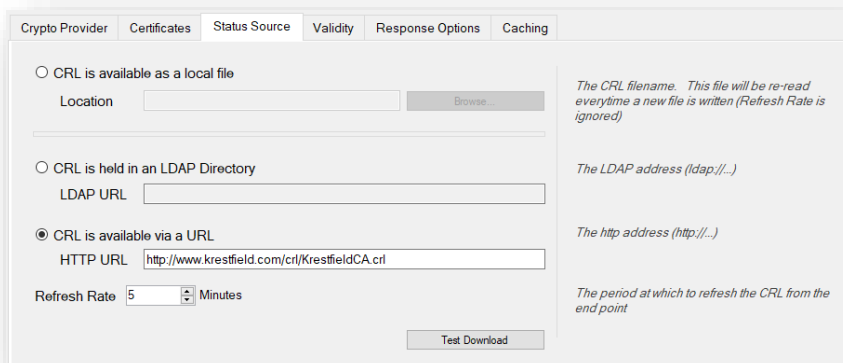
Click **OK** and then **Close** to close the *Generate Certificate Request* dialog

Configure the Status Source

The status source is the CRL (Certificate Revocation List) file, produced by the CA. It contains the revocation status of certificates issued from this CA

When using OCSP it is usual for a new CRL to be generated by the CA frequently and/or every time a certificate is revoked. This ensures that the OCSP has the most up to date information

To configure this, select the **Status Source** tab



The CRL can be accessed from the following locations:

- A file
 - The CRL may be copied to a location the OCSP server can access or the file location may be a share on another machine. To choose this option select the **CRL is available as a local file** option and type or browse to the CRL location
- An LDAP address
 - The Microsoft CA can publish the CRL to Active Directory. This location can then be accessed by the responder. To use this option, select the **CRL is held in an LDAP Directory** option and enter the LDAP address
- An http location
 - If the CRL in question is published to an http end point, this can also be configured. To use this option select the **CRL is available via a URL** option and enter the http address

The easiest way to find the LDAP or http address is often just to open a certificate issued from the CA and view the *CRL Distribution Points* extension. A typical entry may look like this:

```
[1]CRL Distribution Point
  Distribution Point Name:
    Full Name:
      URL=ldap:///CN=Krestfield CA,CN=IssuingCA,CN=CDP,CN=Public Key
      Services,CN=Services,CN=Configuration,DC=int,DC=krestfield,DC=com?certificateRevocationList?base?objectClass=cRLDi
      stributionPoint
      (ldap:///CN=Krestfield%20CA,CN=IssuingCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC
      =int,DC=krestfield,DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint)
      URL=http://www.krestfield.com/crl/KrestfieldCA.cr
```

The ldap address highlighted in **blue** could be copied and pasted into the **LDAP URL** location

☒ CRL is held in an LDAP Directory

LDAP URL

Or the http address highlighted in **green** could be copied to the **HTTP URL** location

☒ CRL is available via a URL

HTTP URL

The choice of which location to use depends on the design of the CA. Note that these locations can also be monitored using the *Krestfield CRL OCSP Monitor*

To test the accuracy of the LDAP or HTTP locations, click the **Test Download** button. This will attempt to retrieve and display the CRL from the location specified. This will confirm that the CRL is accessible at that point

If an LDAP or HTTP URL location is used, the responder can check for a fresh CRL at the interval specified by the *Refresh Rate*:

Refresh Rate

I.e. in this example the server will check (download from the URL or LDAP address) for a new CRL every five minutes

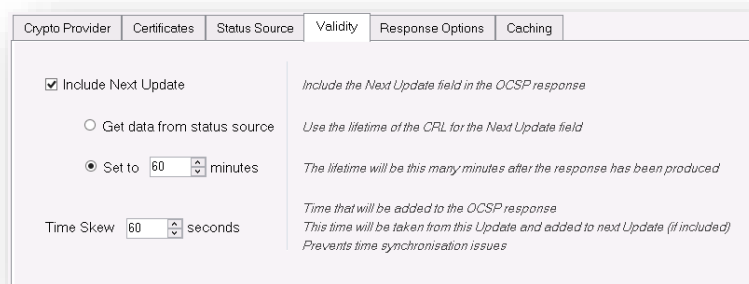
If a file location is used, a new CRL will be read every time it is produced. For example, if the CRL is produced via a scheduled task every five minutes, the responder will recognise when the CRL has been updated and automatically reload

Configure Response Validity

OCSP Responses have a lifetime, contained within the **Next Update** field within the response data. This indicates how long the recipient can rely on this information for

For rapid revocation status updates, it is generally a short period (5 – 10 minutes) but could be longer depending on the use and security requirements

To configure the lifetime of an OCSP response, click on the **Validity** tab



The screenshot shows the 'Validity' tab of the OCSP Responder configuration. It contains the following settings:

- ☒ **Include Next Update**
Include the Next Update field in the OCSP response
- ☐ **Get data from status source**
Use the lifetime of the CRL for the Next Update field
- ☒ **Set to 60 minutes**
The lifetime will be this many minutes after the response has been produced
- Time Skew 60 seconds**
*Time that will be added to the OCSP response
This time will be taken from this Update and added to next Update (if included)
Prevents time synchronisation issues*


If the *Next Update* field should be included in the responses, check the **Include Next Update** check box (if this is not checked the OCSP response will not include the Next Update field entry)

Choose either **Get data from status source** (the OCSP Response will use the Next update field from the CRL) or **Set to a specified number of minutes** (the OCSP response will always be generated with a Next Update this number of minutes from the creation time)

If there are any potential timing issues (e.g. if some clients may not have their clocks synchronised), set **Time Skew** to the number of seconds to extend the validity of a response to take into account time drift. The number of seconds specified will be taken from the **produced at** and **this update** fields and added to the **next update** field

Configure Response Options

Select the **Response Options** tab:



The screenshot shows the 'Response Options' tab of the Krestfield OCSP Responder configuration window. The window has tabs for 'Crypto Provider', 'Certificates', 'Status Source', 'Validity', 'Response Options', and 'Caching'. The 'Response Options' tab is active. It contains several configuration options:

- ☒ **Respect NONCE**: If a Nonce (Number Once) is included in the request it will be returned in the response.
- ☐ **Requests must be signed**: If a request is not signed an error (Signature Required) will be returned.
- Signing Hash Algorithm**: A dropdown menu currently set to 'SHA-256'. The hash algorithm used when signing the response.
- Test Options**:
 - ☐ **Return GOOD for all requests**: WARNING: For test purposes only. No matter what the CFL contains of what CA the certificate has been issued from - return GOOD.
 - ☐ **Delay response by** 0 milliseconds: WARNING: For test purposes only. Delays the sending of the response by the number of milliseconds specified.

The following options are available:

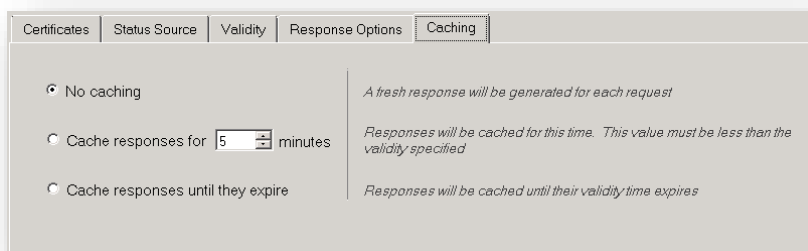
- **Respect NONCE**
 - If checked and a Nonce (Number Once) value is included in the request, a fresh response will be generated with the same Nonce as received in the request (added to the response Nonce extension). If this is not checked then a Nonce will never be included in the response
- **Requests must be signed**
 - If this option is checked, OCSP requests will be rejected (UNAUTHORIZED will be returned) unless signed by a certificate issued from the same CA as configured
- **Signing Hash Algorithm**
 - What algorithm to sign the OCSP Response with. The options are:
 - SHA-1
 - SHA-256
 - SHA-284
 - SHA-512
- **Return GOOD for all requests**
 - This option instructs the server to ignore the status source and return GOOD for all OCSP Requests. **WARNING: This option should be used for test purposes only. Although another use could be as an emergency measure to allow clients to operate in the case where the status source has failed to be produced. But this should be a temporary change and only enabled subject to a risk assessment.**
When this option is enabled revoked certificates will be accepted by clients as being valid - as a GOOD response will always be returned regardless of the revocation status of the certificate.
- **Delay response**
 - This option can be used to assist testing and trouble-shooting. Essentially the response is delayed for the number of milliseconds specified
Enabling this option in a production environment can severely impact performance

Configure Caching

OCSP Responses can be cached to improve performance. If caching is enabled and a request is received for a certificate which has previously been responded on. Then, if still valid, the previously generated OCSP response will be returned unchanged

This removes the need to perform all the calculations required to produce a fresh response and generate the digital signature for every request

To configure caching select the **Caching** tab:




The screenshot shows the 'Caching' tab of the OCSP Responder configuration window. It contains three radio button options for caching, each with a descriptive text box to its right. The first option, 'No caching', is selected. The second option, 'Cache responses for 5 minutes', has a text box with '5' and a 'minutes' label. The third option is 'Cache responses until they expire'.

Option	Description
<input checked="" type="radio"/> No caching	A fresh response will be generated for each request
<input type="radio"/> Cache responses for 5 minutes	Responses will be cached for this time. This value must be less than the validity specified
<input type="radio"/> Cache responses until they expire	Responses will be cached until their validity time expires

Select from the following options:

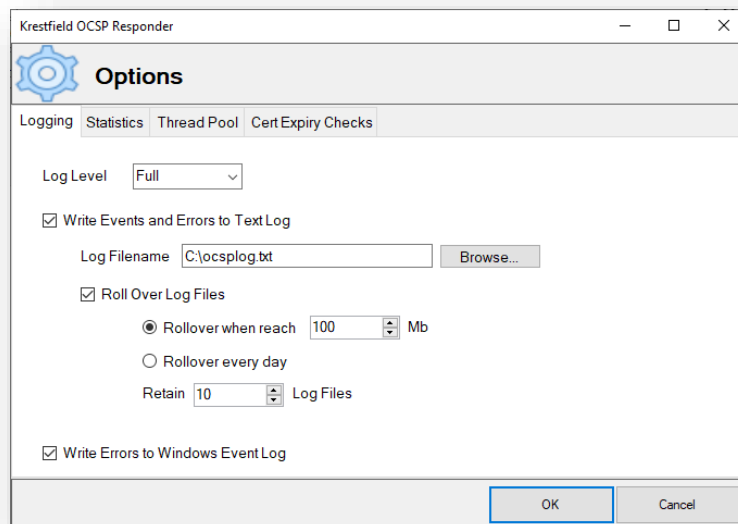
- No caching
 - No caching will be performed. A newly generated response will be produced for each request
- Cache responses for N minutes
 - A response will be cached for a number of minutes before a fresh response will again be generated Note: Ideally the validity of the OCSP response should be larger than the number of minutes specified here, although the responder will automatically generate a fresh response if a cached version has expired
- Cache responses until they expire
 - Use the Next Update field in the OCSP Response to decide how long to cache the response for

Configure Other Options

Click on the  button to bring up the **Options** dialog

Logging

To configure the Logging options, click on the **Logging** tab



The Log Level can be set to

- Full
 - Maximum logging including all OCSP requests, responses and processing steps
- Minimum
 - Only OCSP requests and responses will be logged
- None
 - Nothing will be logged

Events and errors can be written to a text file. Check the **Write Events and Errors to Text Log** option then choose the **Log Filename**

If Full logging is enabled, log files can become large. Therefore, it is best practise to archive off old logs and roll over local logs. Check the **Roll Over Log Files** option and choose whether to roll over based on size, or roll over based on time (every day). The number of rolled over log files to retain can also be set

The rolling over of log files works as follows:

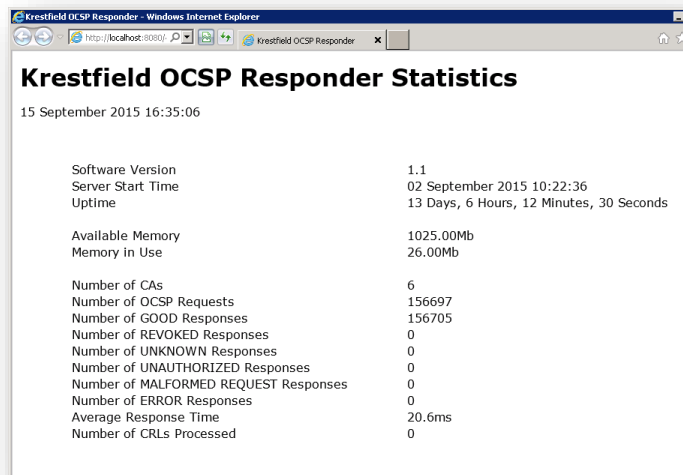
The current log will always be named as chosen in the Log Filename text box e.g. logfile.txt

If this log file reaches its rollover limit (size or date) it is copied to a file called <filename>1.<ext> e.g. logfile1.txt. If there already exists a previous logfile1.txt, this will be renamed logfile2.txt and so on until the number of log files reaches the limit to retain. At which point the last (oldest) file is deleted

Errors can be written to the Windows Event Log. To configure this check the **Write Errors to Windows Event Log** option. Entries will have a Source = *Krestfield OCSP Responder* and Event ID = 2560

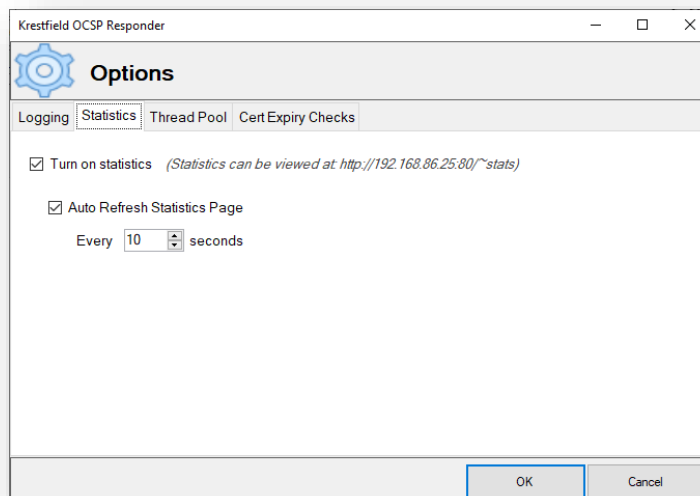
Statistics

The Server can produce statistics which can be viewed via a web browser. The location of the statistics page can be accessed from **http://<server name>:<server port>/~stats** e.g. **http://ocsp.company.com/~stats**




Krestfield OCSP Responder Statistics	
15 September 2015 16:35:06	
Software Version	1.1
Server Start Time	02 September 2015 10:22:36
Uptime	13 Days, 6 Hours, 12 Minutes, 30 Seconds
Available Memory	1025.00Mb
Memory in Use	26.00Mb
Number of CAs	6
Number of OCSP Requests	156697
Number of GOOD Responses	156705
Number of REVOKED Responses	0
Number of UNKNOWN Responses	0
Number of UNAUTHORIZED Responses	0
Number of MALFORMED REQUEST Responses	0
Number of ERROR Responses	0
Average Response Time	20.6ms
Number of CRLs Processed	0

To configure the statistics, click the **Statistics** tab:



Krestfield OCSP Responder

 **Options**

Logging | **Statistics** | Thread Pool | Cert Expiry Checks

☒ Turn on statistics (Statistics can be viewed at: <http://192.168.86.25.80/~stats>)

☒ Auto Refresh Statistics Page

Every seconds

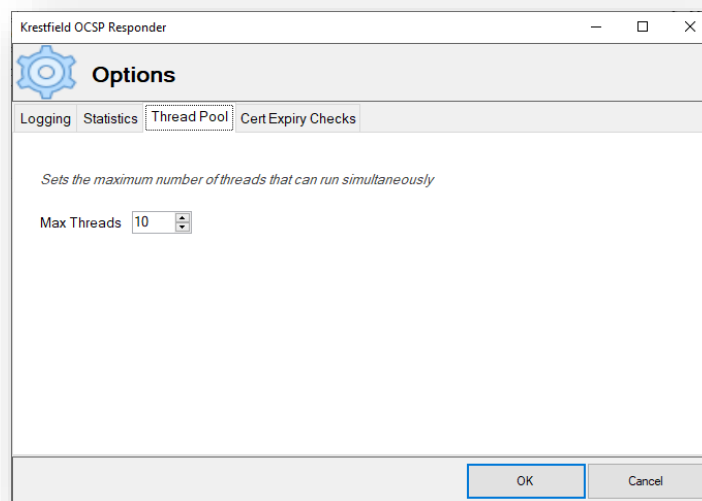
OK Cancel

Check the **Turn on statistics** option to start producing the statistics page

Check the **Auto Refresh Statistics Page** option if you want the web page to auto-refresh and select the number of seconds at which the page will refresh

Thread Pool

The number of threads the server will create for parallel processing of requests can be set by selecting the **Thread Pool** tab

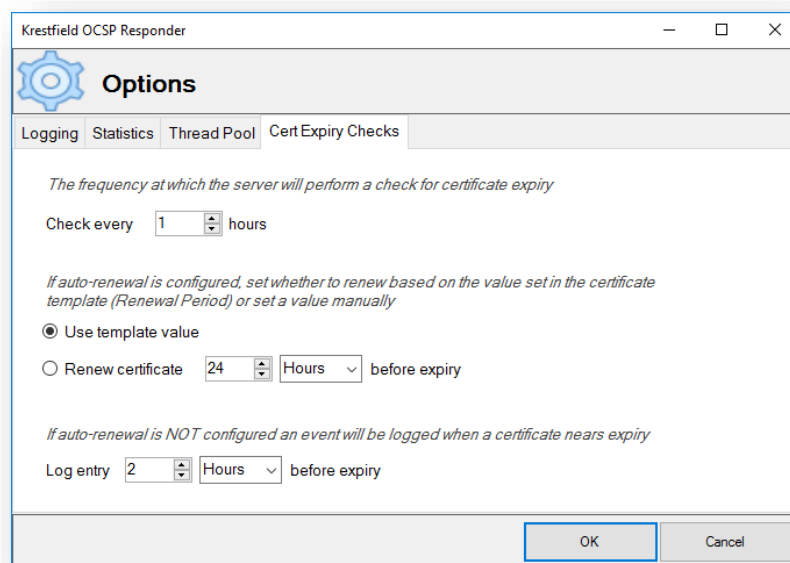


Set the value for **Max Threads**

The server will create a thread pool at start-up which will grow to this size and be utilised for parallel processing. More threads may increase performance but greater values can also increase start-up time or consume HSM connections. The optimum value is dependent on the system resources and generally a value of 10 should be configured initially and larger values then trialled, if further performance is required

Cert Expiry Checks

If any signing certificates are configured to auto-renew, this tab allows the setting of how often to check and when to renew those certificates



The *Check every* option dictates how often the server will check for certificate expiry. For certificates that have a short life (e.g. a number of days or less), this can be set to a number of hours. For longer life certificates you may only want to check every day (24 hours) or week (168 hours)

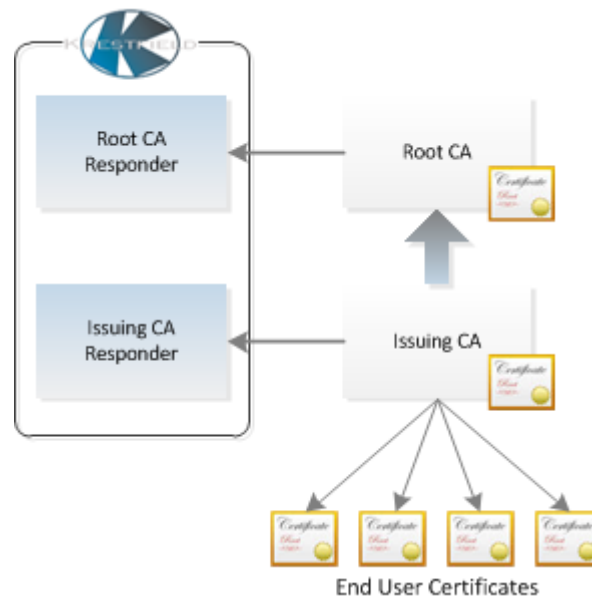
Note that whether the certificate is going to be auto-renewed or not, its expiry time will still be checked and log entries will be created

If a certificate is configured to auto-renew the time to renew can be dictated by the CA Certificate Template (which has a Renewal Period time configured) or this time can be set manually. To set the renewal time select the **Renew certificate** option and set the number of hours/days to renew before expiry

If auto-renewal is not configured, the server will start to log that a certificate is expiring at the period defined by *Log entry*. For example, if a certificate has a lifetime of six months, you may wish to start logging entries 30 days before expiry to ensure the log entry is picked up and acted on in good time

Example Configuration

Consider the following typical PKI hierarchy:



Root CA is the self-signed, root CA and issued the **Issuing CA** certificate. **Issuing CA** then issues the end-user certificates.

Root CA Responder will provide responses for the Issuing CA certificate and the **Issuing CA Responder** certificate. It has been configured with the **Root CA** as the CA certificate, and has been issued a signing certificate from **Root CA**

Issuing CA Responder will provide responses for the end user certificates. It has been configured with the **Issuing CA** certificate as the CA certificate, and has been issued with a signing certificate from **Issuing CA**

All revocation checking in this environment must be performed via OCSF

When a signature produced by an end-user certificate is verified the following revocation checks will be performed:

1. A request for the revocation status of the end-user certificate is sent to the **Issuing CA Responder**
2. The **Issuing CA Responder** returns a signed response containing the revocation status of this end-user certificate
3. The revocation status of the OCSF signing certificate used to sign this response will then be checked (Note: if the no-check extension is set within the OCSF signing certificate, this will not occur). This request is sent to the **Root CA Responder**
4. The **Root CA Responder** returns a signed response containing the revocation status of the **Issuing CA Responder** certificate
5. A request is then sent to the **Root CA Responder** for the status of the **Issuing CA** certificate. This is sent to the **Root CA Responder**
6. The **Root CA Responder** returns a signed response containing the revocation status of the **Issuing CA** Certificate

Both of these responders can be setup within a single instance of the Krestfield OCSP Responder

To configure this setup the following steps should be taken:

1. Create a new CA called **Root CA Responder** and configure the preferred Crypto Provider for this CA
2. For the CA Certificate, select the **Root CA certificate**
3. Generate a certificate request and send this to the Root CA for signing. This certificate should be issued with enhanced key usage to include OCSP Signing (1.3.6.1.5.5.7.3.9) and the OCSP No Revocation Checking extension set. Import the response
4. Set the Status source to point to the CRL issued from the Root CA
5. Configure the Validity, Response Options and Caching as required
6. Create a new CA called **Issuing CA Responder** and configure the preferred Crypto Provider for this CA
7. For the CA Certificate, select the **Issuing CA certificate**
8. Create a Certificate request and send this to the Issuing CA for signing. This certificate should be issued with enhanced key usage to include OCSP Signing (1.3.6.1.5.5.7.3.9). Optionally, it can be also issued with the OCSP No Revocation Checking extensions set. Import the response
9. Set the Status source to point to the CRL issued from the Issuing CA
10. Configure the Validity, Response Options and Caching as required
11. Configure Logging and Statistics from the Options menu as required
12. Start the OCSP Responder

Other Information

Configuration File

The configuration is stored in an xml file and is located here:

C:\ProgramData\Krestfield\OCSPResponder\config.xml

This file should be included in regular backups

Location of Management Console Log

Operations performed by the Management Console (such as the generation of certificate requests) are logged to the Management Console Log here:

C:\ProgramData\Krestfield\OCSPResponder\OCSPRespMCLog.txt

Event IDs in system log

If the option to write errors to the windows event log is set, any errors will also be reported in the Windows Event Log. These events have the following properties:

Log Name: Application
Source: Krestfield OCSP Responder
Event ID: 2560

Support

If you experience any issues with the Krestfield OCSP Responder or require help or advice on any aspects of the systems setup, contact support via email at **support@krestfield.com** or visit our web site at <https://www.krestfield.com>