OCSP Client Tool

The OCSP Client Tool can be used to ensure that important Validation Authority systems are operating effectively, in line with their specification and the validation policies that are being enforced. OCSP Client Tool can be used both during the installation and configuration of an OCSP Responder environment as well as during upgrade processes. It is also a useful tool for confirming correct operation of an OCSP Responder when client issues are reported.

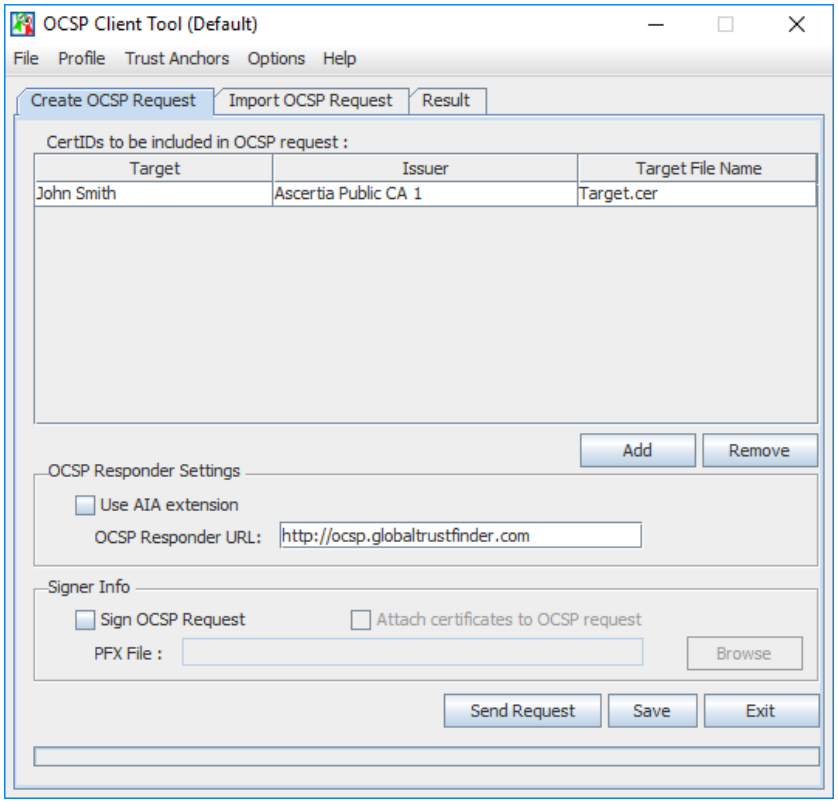
The OCSP Client Tool allows you to:

- Create one or more test profiles for testing one or more OCSPs with different certificates and test settings such as nonce and service locator extensions
- Define one or more certificates to be included in an OCSP request to a specified responder
- Send the OCSP request using a defined URL or use the AIA extension contained within the certificate(s)
- Send OCSP requests over SSL/TLS
- Send OCSP requests via proxies with optional digest authentication
- Send signed and unsigned OCSP requests
- Receive and validate the OCSP responses coming back from the OCSP Server
- Establish and maintain a list of trusted CAs and OCSP Servers
- Keep an audit log of all OCSP transactions

The Ascertia OCSP Client Tool is fully compliant with the OCSP specifications as defined in IETF RFC6960 and interoperates with any OCSP server meeting this standard. The tool is fully GUI based to allow easy installation and configuration.

The OCSP Client Tool is written in Java and is supported on Windows 64 and 32 bit platforms.

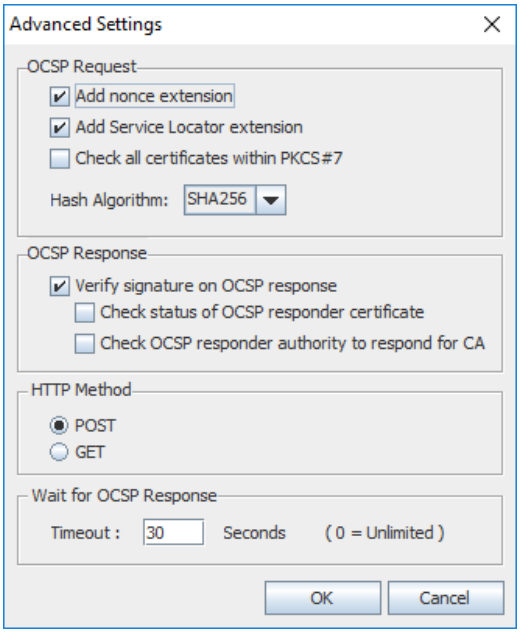
The main GUI is shown opposite and shows the ease with which OCSP Client Tool can be used to create OCSP requests. All main parameters are presented so that they can easily be changed.



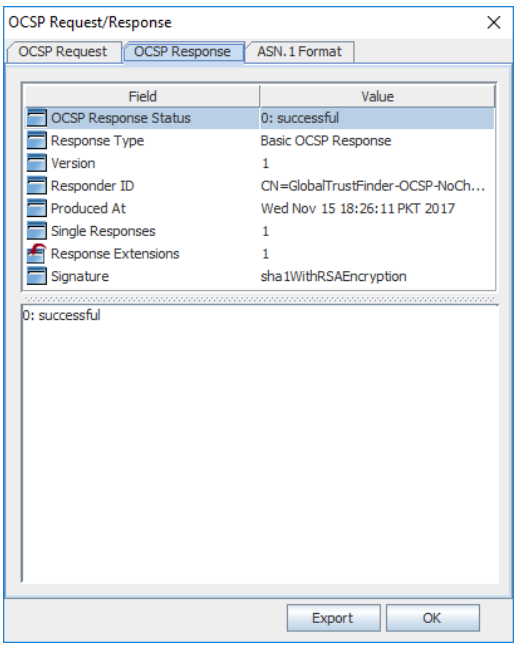
OCSP Client Tool - for advanced OCSP checking

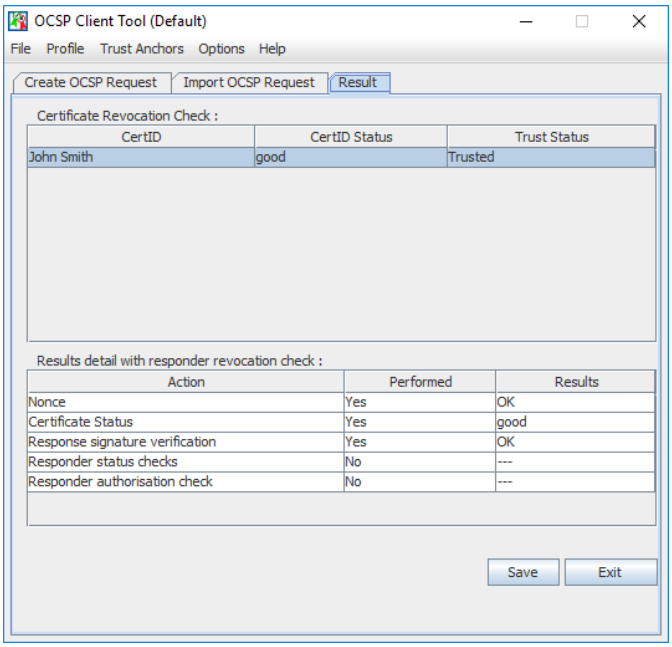
Other features can be configured in the Advanced Settings screen.
OCSP Client Tool allows multiple profiles in which different settings can be made to accommodate different tests. The settings include:

a) A nonce to prevent reply attacks
b) A service locator extension to check that the target OCSP server can proxy a request to other authoritative OCSP servers.
c) Checking all certificates within the chain
d) Use SSL to protect the request/ response data
e) Checking the OCSP response validity and checking the OCSP Responder is authoritative for the issuer CA
f) Defining which HTTP protocol (Post or Get) will be used
g) The time-out setting



The response data is examined in detail and the results are displayed as shown below. A separate analysis screen is made available to look at the detail of the request / response transaction.
In summary OCSP Client Tool offers a comprehensive facility to help manage and check the validation policy settings for one or more OCSP Validation Authority services.





OCSP Crusher Requirements and Standards Compliance:

Operating systems:	Windows 10, 8, 7, Windows Server 2016, 2012 R2, 2012, 2008 R2
Standards:	RFC 6960 OCSP
Interfaces:	HTTP and HTTPS communications for OCSP requests/ responses
Certificate types:	X.509v1 and X.509v3

Ascertia Limited
Web: www.ascertia.com
Email: info@ascertia.com
Tel: +44 203 633 1177
40 Occam Road, Guildford, Surrey, GU2 7YG, UK

Signed by: Rod Crook
Signed at: 2017-11-28 09:00:18 +00:00
Reason: I approve this document