



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.

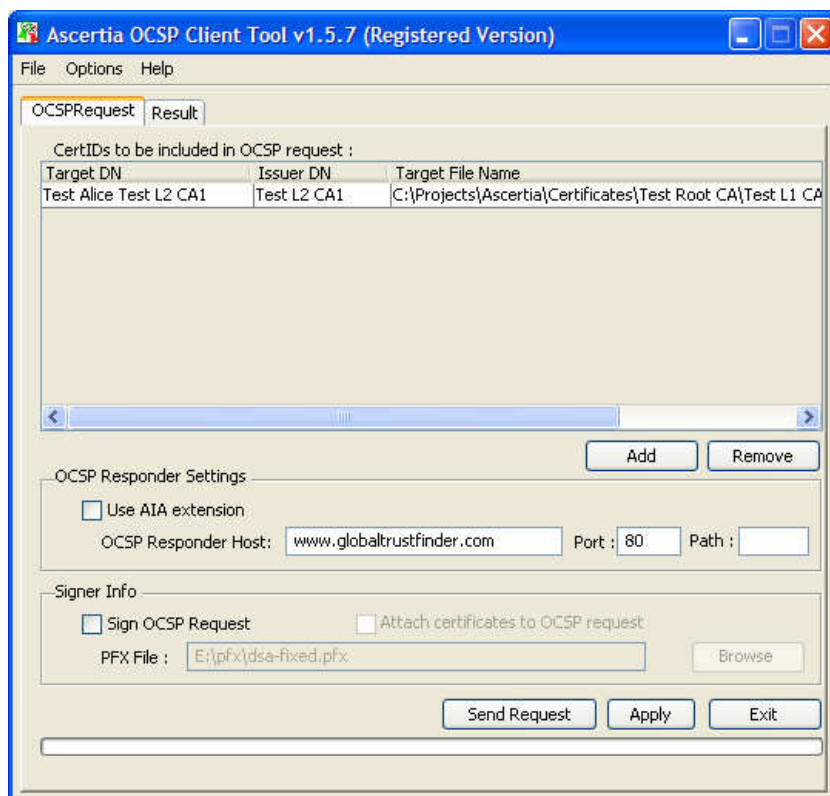
The OCSP Client Tool allows you to:

- 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 RFC2560, 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 32 bit platforms.

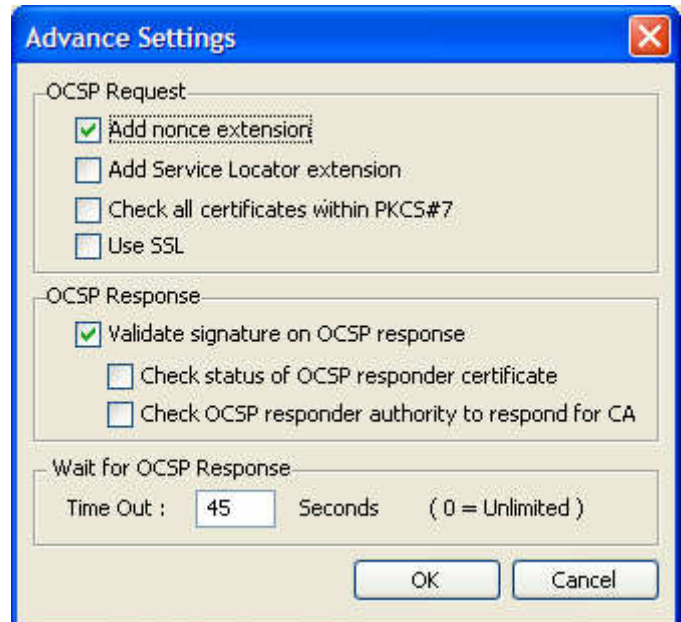
The main GUI is shown opposite and shows the ease with which OCSP Client Tool can be used to create OCSP requests. All main parameters are presented so that they can easily be changed.



Other settings can be configured using the Advanced Settings option.

The product allows multiple profiles in which different settings can be made to accommodate different tests. The settings include:

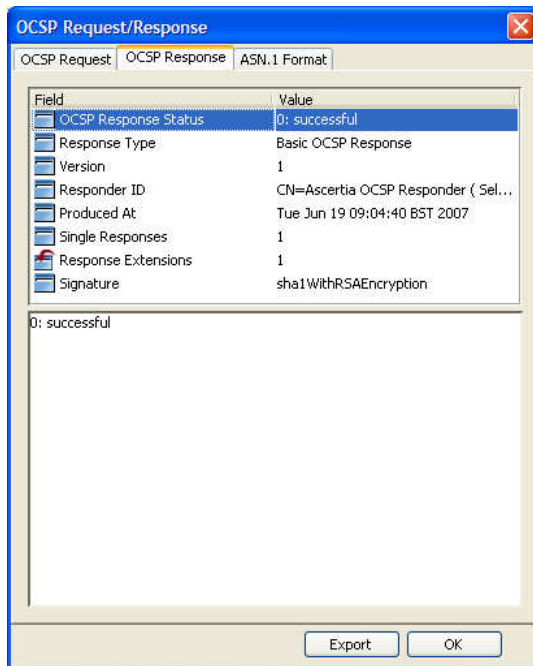
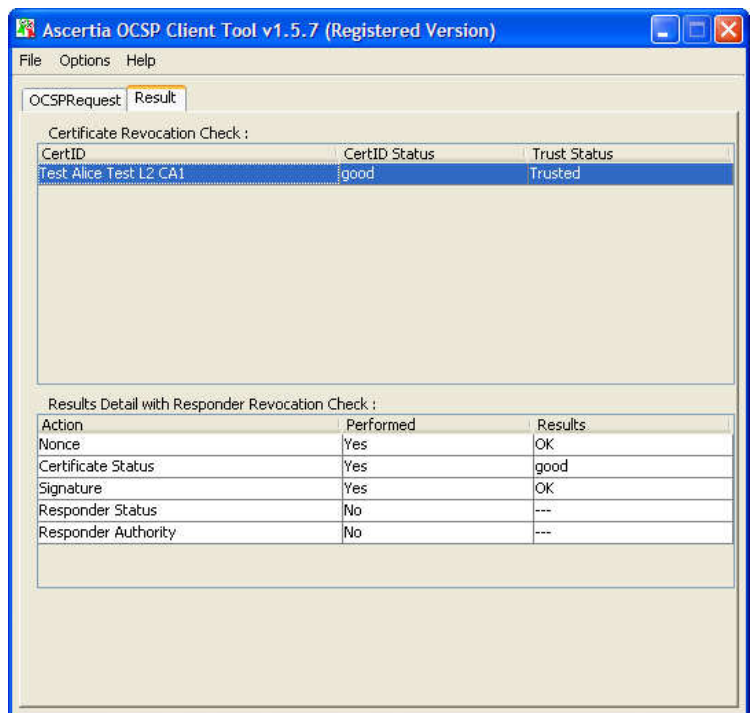
- a nonce to prevent reply attacks
- a service locator extension (to check that the OCSP server can proxy the requests to other OCSP servers in 4-corner models)
- Checking all certificates within the chain
- Use SSL to protect the request/response data
- How to check the OCSP response validity
- The time-out setting



The response data is examined in detail and the results are displayed as shown.

A separate analysis screen is made available to look at the detail of the request / response transaction.

In summary OCSP Client Tool offer a comprehensive facility to help manage one or more OCSP services.



System Requirements:	Windows XP, Windows 2000, Windows 2003 Windows 2008
Interfaces and Protocols:	RFC 2560 (OCSP), TLS/SSL, Communication through proxy (including digest authentication) PFX/PKCS#12 for OCSP request signing, X.509v1 and v3 certificates.

Ascertia Limited
 Web: www.ascertia.com
 Email: info@ascertia.com
 Tel: +44 1256 895416 US: +1 508 283 1890
 40 Occam Road, Guildford, Surrey, GU2 7YG, UK
 © Copyright Ascertia Limited 2009. All Rights Reserved, E&OE