



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:

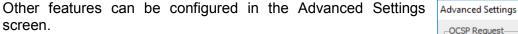
- Create one or more test profiles for testing one or more OCSPs with different certificates and test settings such as nonce and service locator extensions
- Define one or more certificates to be included in an OCSP request to a specified responder
- Send the OCSP request using a defined URL or use the 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 (Default)		_				
File Profile Trust Anchors Op	File Profile Trust Anchors Options Help					
Create OCSP Request Impor	t OCSP Request Result					
CertIDs to be included in OCS	Prequest :					
Target	Issuer	Target F	ile Name			
John Smith	Ascertia Public CA 1	Target.cer				
OCSP Responder Settings		Add	Remove			
Use AIA extension						
OCSP Responder URL:	http://ocsp.globaltrustfinder.com					
Signer Info Sign OCSP Request PFX File :	Attach certificates to OCS	P request	Browse			
	Send Request	Save	Exit			



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
- 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 Request/R	esponse	×	(	🙀 OCSP Client Tool (D	efault)			—		×
OCSP Request	OCSP Response	ASN.1 Format		File Profile Trust Anch	ors Options	Help				
		1		Create OCSP Request	Import OC	SP Request Result				
_	Field	Value			-1 1					
OCSP Resp		0: successful		Certificate Revocatio	n Check :					
Response 1	Гуре	Basic OCSP Response		CertID John Smith		CertID Status	Trusted	Trust 9	status	_
Version		1		John Smith		good	Irusted			
Responder	ID	CN=GlobalTrustFinder-OCSP-NoCh								
Produced A		Wed Nov 15 18:26:11 PKT 2017								
Single Resp	onses	1								
Response B	Extensions	1								
Signature		sha1WithRSAEncryption								
				Results detail with re	sponder revoc Action	ation check : Perform	ied		Results	
				Nonce		Yes		Ж		
				Certificate Status		Yes		jood		
				Response signature ve		Yes		ОК		
				Responder status cheo		No				
				Responder authorisatio	on check	No	-			
		Export OK						Save	Ð	xit
		Export OK								

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			
	ertia.com			

OCSP Request			
Add nonce extension			
✓ Add Service Locator extension			
Check all certificates within PKCS#7			
Hash Algorithm: SHA256 💌			
OCSP Response			
✓ Verify signature on OCSP response			
Check status of OCSP responder certificate			
Check OCSP responder authority to respond for CA			
HTTP Method			
POST			
⊖ get			
Wait for OCSP Response			
Timeout : 30 Seconds (0 = Unlimited)			
OK Cancel			

 $\times$