



Ascertia Limited
40 Occam Road
Surrey Research Park
Guildford
Surrey
GU2 7YG

Tel: +44 1483 685500
Fax: +44 1483 573704

www.ascertia.com

OCSP Client Tool V2.2

User Guide

Document Version: 2.2.0.2

Document Issued: December 2009

©Copyright Ascertia Ltd, 2009

This document contains commercial-in-confidence material. It must not be disclosed to any third party without the written authority of Ascertia Limited.

Commercial-in-Confidence

Contents

1	Introduction	3
1.1	Scope.....	3
1.2	Intended Readership	3
1.3	Conventions.....	3
1.4	Glossary and Abbreviations.....	3
1.5	Technical Support.....	3
1.6	Copyright Information	4
2	Overview	5
2.1	Objective	5
2.2	Menus	5
2.3	OCSP Request Tab	8
2.4	Result Tab	14
2.5	Sample OCSP Response	16
3	Advance Configuration	21
4	Trust Anchors Configuration.....	23
5	Logging Configuration	26
6	Proxy Configuration	27

1 Introduction

1.1 Scope

This manual describes how to use Ascertia OCSP Client Tool v2.2.

1.2 Intended Readership

This guide is intended for administrators and corporate security analysts, who are deploying an OCSP-enabled PKI. The server administrator is defined as a system administrator, or network administrator, who is responsible for installing, configuring, and maintaining OCSP server(s).

It is assumed that the reader has a good understanding of PKI concepts, in particular prior knowledge of trust models, certificate and CRL profiles and OCSP certificate validation is required.

1.3 Conventions

The following typographical conventions are used in this guide to help locate and identify information:

- **Bold text** identifies menu names, menu options, items you can click on the screen, file names, folder names, and keyboard keys;
- `Courier` font identifies code and text that appears on the command line.
- **Bold courier** identifies commands that you are required to type in.

1.4 Glossary and Abbreviations

AIA	Authority Information Access (a certificate extension field which can identify the address of the OCSP server responsible for this certificate)
CA	Certification Authority
DNAME (or DN)	Distinguished Name
OCSP	Online Certificate Status Protocol, version 1.0
OCSP client	An application, which can make OCSP request calls to an OCSP server.
OCSP server	Also referred to as OCSP responder (i.e. a server which can receive OCSP requests and provide OCSP responses). TrustFinderOCSP is an OCSP server.
RP	Relying Party application (i.e. an OCSP client application)
SSL	Secure Sockets Layer
TF	TrustFinderOCSP Server

1.5 Technical Support

If technical support is required, Ascertia has a dedicated support team providing debugging assistance, integration assistance and general customer support. Ascertia Support can be accessed in the following ways:

Support Website:	https://www.ascertia.com/personalized/support.aspx
Support Email:	support@ascertia.com
Support MSN Messenger:	support@ascertia.com
Skype:	ascertia.support

In addition to the free support service described above, Ascertia provides formal support agreements with all product sales. Please contact sales@ascertia.com for more details.

A Product Support Questionnaire should be completed to provide Ascertia Support with further information about your system environment. When requesting help it is always important to provide:

- Network environment
- System Platform
- Specific problems and steps and how to reproduce it.
- Specific problem and steps on how to reproduce it (please send any screen snapshots, logs, OCSP Client Tool version/build information etc (available from the application's About box)).

1.6 Copyright Information

The information in this document is subject to change without notice and does not represent a commitment on the part of Ascertia Ltd. Ascertia does not accept any responsibility for any errors that may appear in this document.

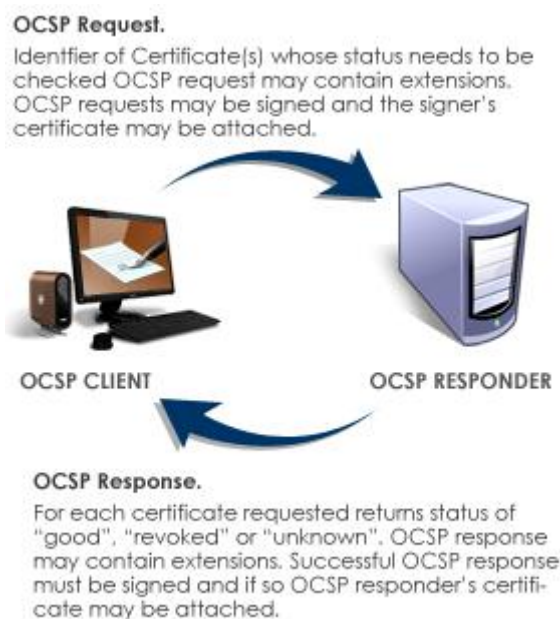
The software described in this document is furnished under a license and may be used only in accordance with the terms of such license. The documentation is issued in confidence for the purposes only for which it is supplied. It must not be reproduced in whole or in part or used for tendering or manufacturing purposes except under an agreement or with the consent in writing of Ascertia Ltd, and then only on the condition that this notice is included in any such reproduction. No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly there from shall be given orally or in writing or communicated in any manner whatsoever to any third party being an individual firm or company or any employee thereof without the prior consent in writing of Ascertia Ltd. Ascertia, the Ascertia logo, OCSP Client Tool, the OCSP Client Tool Logo, TrustFinderOCSP, the TrustFinderOCSP logo are trademarks of Ascertia Ltd. Other trademarks used throughout this publication are the property of their respective owners.

All URLs given were active at the time of going to press. Ascertia makes no guarantee of their continued validity and takes no responsibility for their content.

Written and published in Guildford, England, by Ascertia Ltd.

2 Overview

The OCSP specification defines - a request/response protocol, where the OCSP client (i.e. a Relying Party application) generates an OCSP request asking for the status of one or more digital certificates and the OCSP responder provides an unsigned or signed OCSP response on the status of the digital certificates requested. A successful OCSP response can be "good", "revoked" or "unknown". The OCSP specification has been defined by IETF as RFC2560 and is available at <http://www.ietf.org/rfc/rfc2560.txt>



The OCSP Client Tool is an OCSP enabled application, which allows you to generate OCSP requests and to send these to an OCSP responder (such as TrustFinderOCSP as illustrated above).

2.1 Objective

The Ascertia OCSP Client Tool V2.2 allows administrators to:

- Choose one or more certificates to be included in an OCSP request.
- Generate an OCSP request containing all of the desired CertIDs and any required extensions.
- Send the generated OCSP request to a chosen OCSP responder or automatically using the AIA extension present in the target certificates, this can be done with or without SSL.
- Receive and validate the OCSP responses from the OCSP responder.
- Establish and maintain a list of trusted CA certificates and OCSP responder certificates.
- Keep a record of all OCSP transactions as configured in OCSP Client Tool.

Each of the above options can be configured within a specific OCSP Client Tool profile. Multiple profiles are supported and the operator can easily switch from one profile to another when testing differing OCSP responders,

OCSP Client Tool V2.2 is compliant with [RFC2560](http://www.ietf.org/rfc/rfc2560.txt) and should be interoperable with all standard OCSP responders (it has been successfully tested with many publicly available OCSP responders).

2.2 Menus

This section describes the menu options within the OCSP Client Tool:

2.2.1 Main Menu

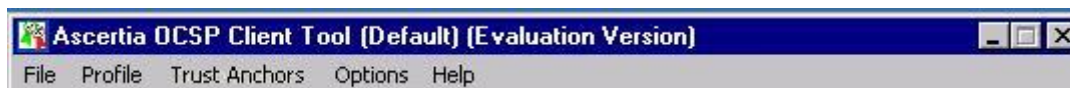


Figure: Main Menu of OCSP Client Tool

2.2.2 File Menu

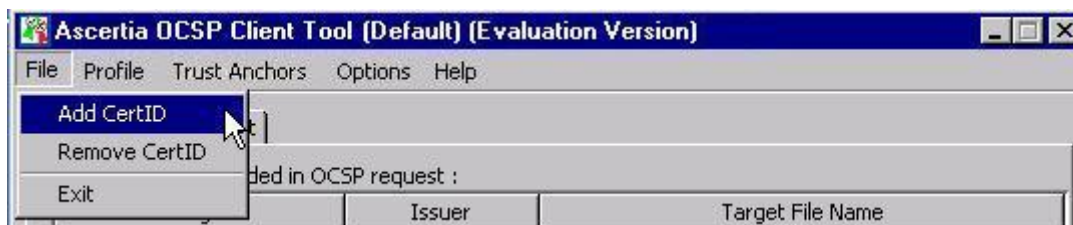


Figure: File Menu of OCSP Client Tool

File Menu Command	Purpose
Add CertID	Used to add new certificate(s) to an OCSP request.
Remove CertID	Used to remove existing certificate(s) from an OCSP request
Exit	Used to Exit the application.

2.2.3 Profile Menu

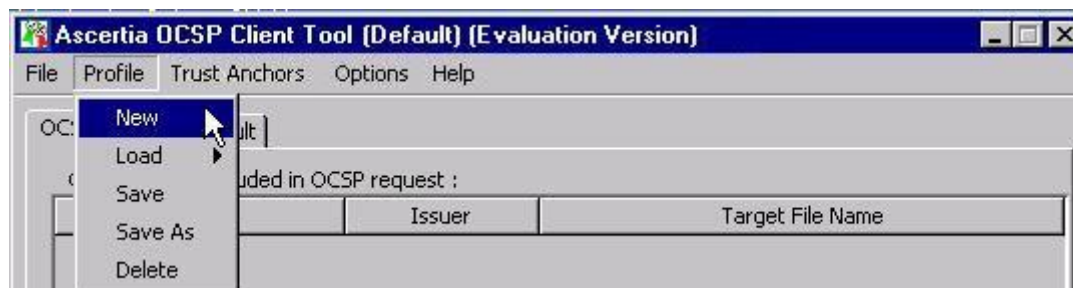


Figure: Profile Menu of OCSP Client Tool

Profile Menu Command	Purpose
New	Used to create new profile (i.e. set of OCSP Client Tool configurations).
Load	Load an existing profile (the sub-menu will show a list of all existing profiles, simply select one to load its settings).
Save	The configuration data within a specific profile can be amended and then saved using the Save menu option.
Save As	Use the Save As menu option to save the currently open OCSP Client Profile under a different profile name.
Delete	The Delete menu option allows you to delete a profile.



A profile contains all of the data associated with a particular OCSP request/response configuration of the OCSP Client Tool and this data can be saved under a profile name. The configuration data includes Trust Anchor information as well as settings such as the target certificate, OCSP responder details, request signing certificate and advanced settings. The default profile has the default settings provided by Ascertia, the default profile can be modified to suit local requirements but cannot be deleted.

Note the currently loaded profile name is shown within the application's top title bar.

2.2.4 Trust Anchors Menu

This menu is used to configure Trusted CAs and Trusted OCSP Responders.

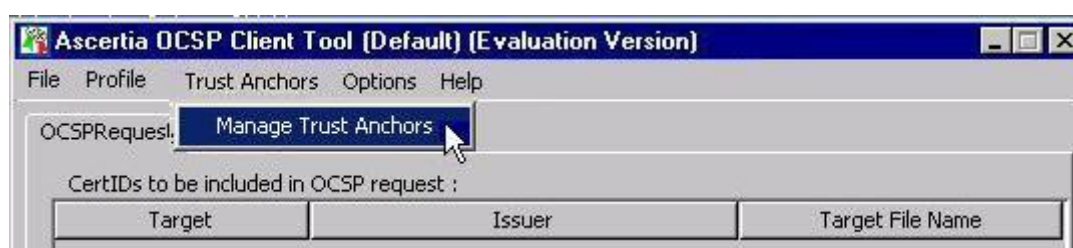


Figure: Trust Anchors Menu of OCSP Client Tool

2.2.5 Options Menu

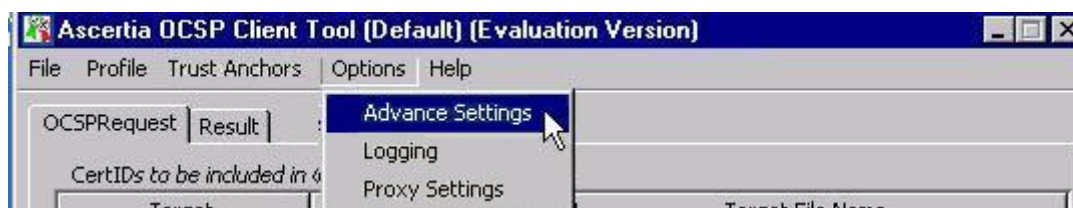


Figure: Options Menu of OCSP Client Tool

Options Menu Command	Purpose
Advance Settings	Used to configure advanced OCSP request/response handling settings.
Logging	Used to configure OCSP request/response logging.
Proxy Settings	Used to configure Proxy settings (if operating behind a proxy or firewall).

2.2.6 Help Menu

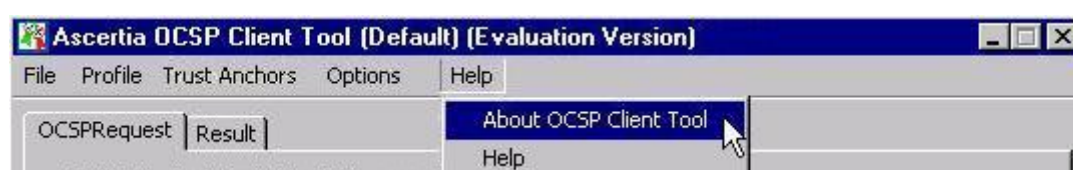


Figure: Help Menu of OCSP Client Tool

Help Menu Command	Purpose
About OCSP Client Tool	For checking the product version and license info.
Help	For accessing the help file.



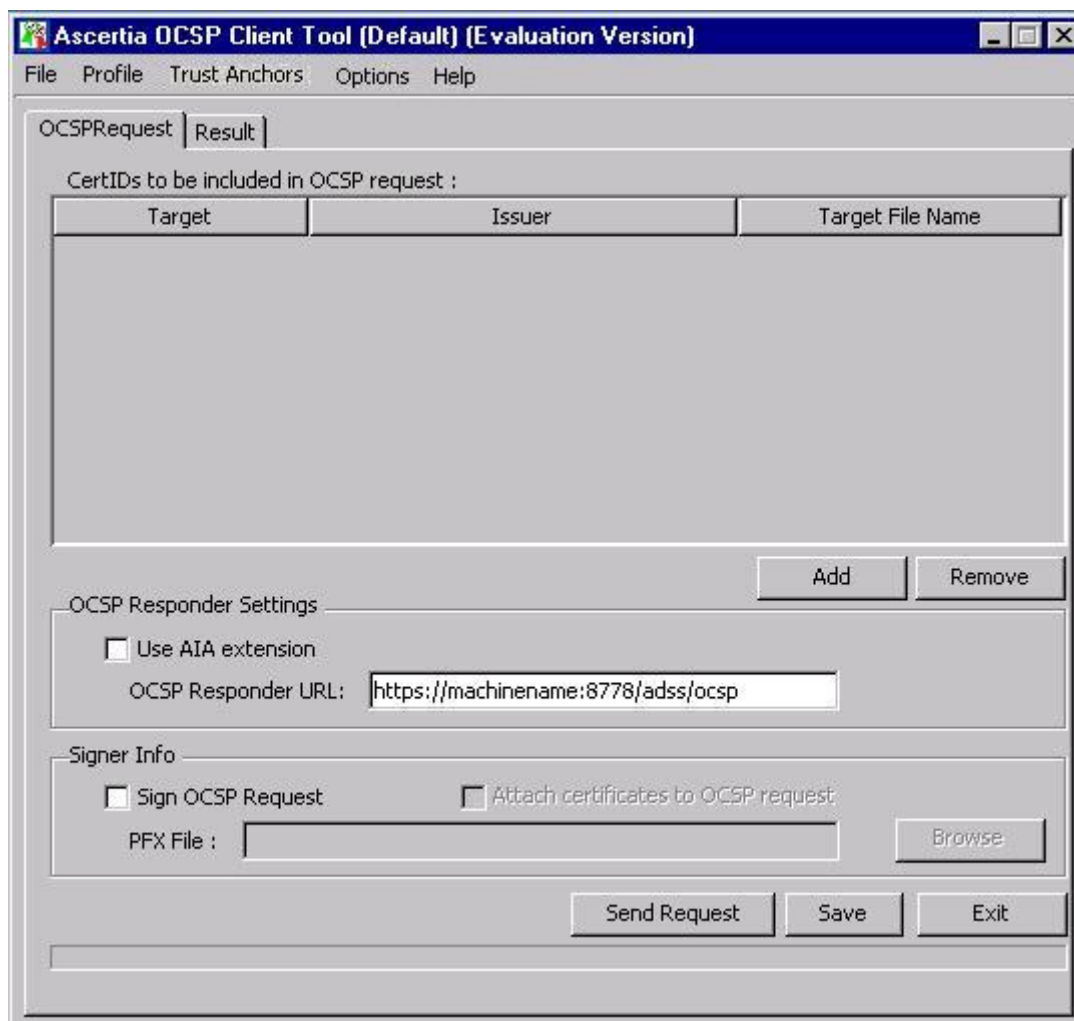
Figure: About product version/Build along with licensing information

2.3 OCSP Request Tab

The purpose of the OCSP Request tab is to:

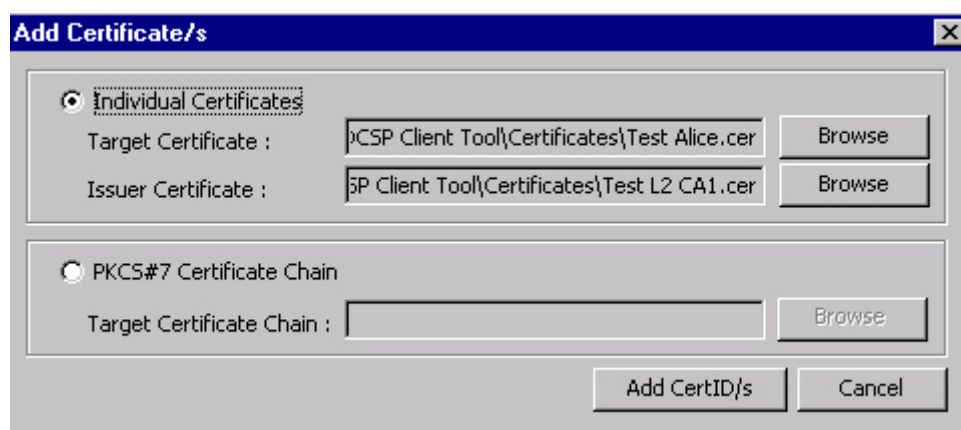
- Identify the certificate(s) that are required to be included in the OCSP request
- Identify the address of the OCSP responder or select use of the certificates AIA extension to locate the responder
- Configure whether the OCSP request is to be signed, and if so allowing the OCSP request signing PFX/PKCS#12 file to be selected
- Sending the OCSP request and monitoring its progress
- Saving changes to profiles
- Exiting the application

A screenshot of the OCSP Request tab is shown below and then each aspect of the configuration is discussed in more detail in the sections below.



2.3.1 Adding CertIDs to an OCSP Request

To add certificates identifiers (certIDs) in an OCSP request, click the **Add** button, this opens a dialog, from which you can identify the certificates to be included within the OCSP request message. Alternatively it is possible to select the **File** menu and click on the **Add CertID** menu item.



Certificates can be added which are either part of a PKCS#7 certificate chain or as an individual certificate. If the PKCS#7 chain is selected then a valid PKCS#7 file in either DER or PEM formats must be selected, this file must include both the target certificate and its issuer certificate (CA certificate).

The term “target certificate” refers to the certificate for which the revocation status is to be checked.

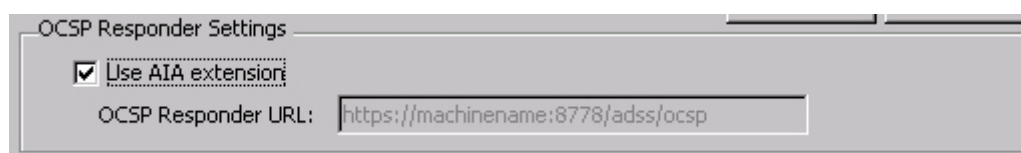
If individual certificate files are selected then again it must be ensured that the correct issuer certificate is selected for the target certificate (note this is required to fully identify the certificate and build the CertID which will be placed inside the OCSP request). Individual certificate files can be in either .CRT or .CER or .PEM formats. Pressing the **Add CertID(s)** button will add the selected certificate information in the list.

The user can add any number of PKCS#7 and individual certificates since a single OCSP request can contain multiple certIDs for validation. However note not all OCSP responders can handle multiple CertIDs within a single OCSP request message, for further details check your OCSP responder.

You can also **remove** a CertID by clicking the **Remove** button or by selecting **File** menu and clicking on **Remove CertID** menu item.

2.3.2 Locating the OCSP Responder

If the **Use AIA extension** check box is selected then OCSP Client Tool will send the OCSP request according to the AIA extension taken from the target certificate. Note that if there are more than one CertID in the OCSP request message and if **Use AIA extension** option is selected then each CertID will be sent to the respective URL present in its AIA extensions. If there is no AIA extension then an error message will be shown.



The other option is to configure a default host address for the OCSP responder (in either domain name or IP address format) in **OCSP Responder URL**. In this case all of the OCSP Requests will be sent to the same OCSP Responder.

The OCSP responder address should identify any port numbers (unless default ports are used) and path information. In case SSL/TLS is used then this must be identified by the use of HTTPS within the address.



Figure: Valid OCSP Responder address

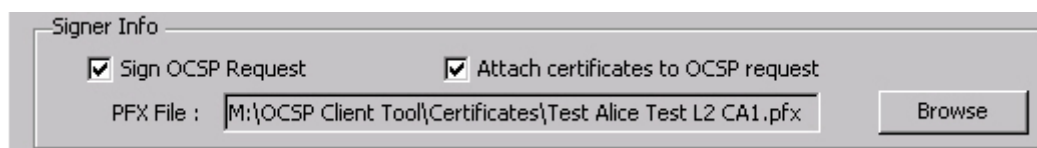


Figure: Invalid OCSP Responder address

The address will work for LAN as well as for an IP network. Note only Server-based SSL authentication is provided in this version of the OCSP Client Tool. Typically if client authentication is required then the OCSP requests should be signed. However if SSL client authentication is required then this can be provided as part of a specific project delivery.

2.3.3 Signing the OCSP request message

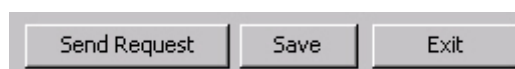
Some OCSP responders only accept signed OCSP requests. If the **Sign OCSP Request** checkbox is selected then all the other items become available otherwise they are grayed-out. Use the Browse button to select a PKCS#12/PFX file, the password must also be entered:



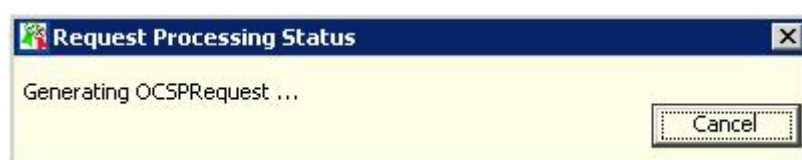
The **Attach certificates to OCSP** request checkbox will attach the certificates associated with the signing PKCS#12/PFX file to the OCSP request before sending. This will help the OCSP responder to build a certificate path for the requester and to validate the signature on the OCSP request message.

2.3.4 Sending an OCSP request, Saving Profiles & Exiting the application

Upon pressing the **Send Request** the OCSP Client Tool takes into account the configurations in the **Advance Settings** (described later), and then forms an OCSP request and sends it to the identified OCSP responder.



Once sending the request, OCSP Client Tool then waits for the OCSP response from OCSP Responder. A pop-up window describes the communication with OCSP Responder.



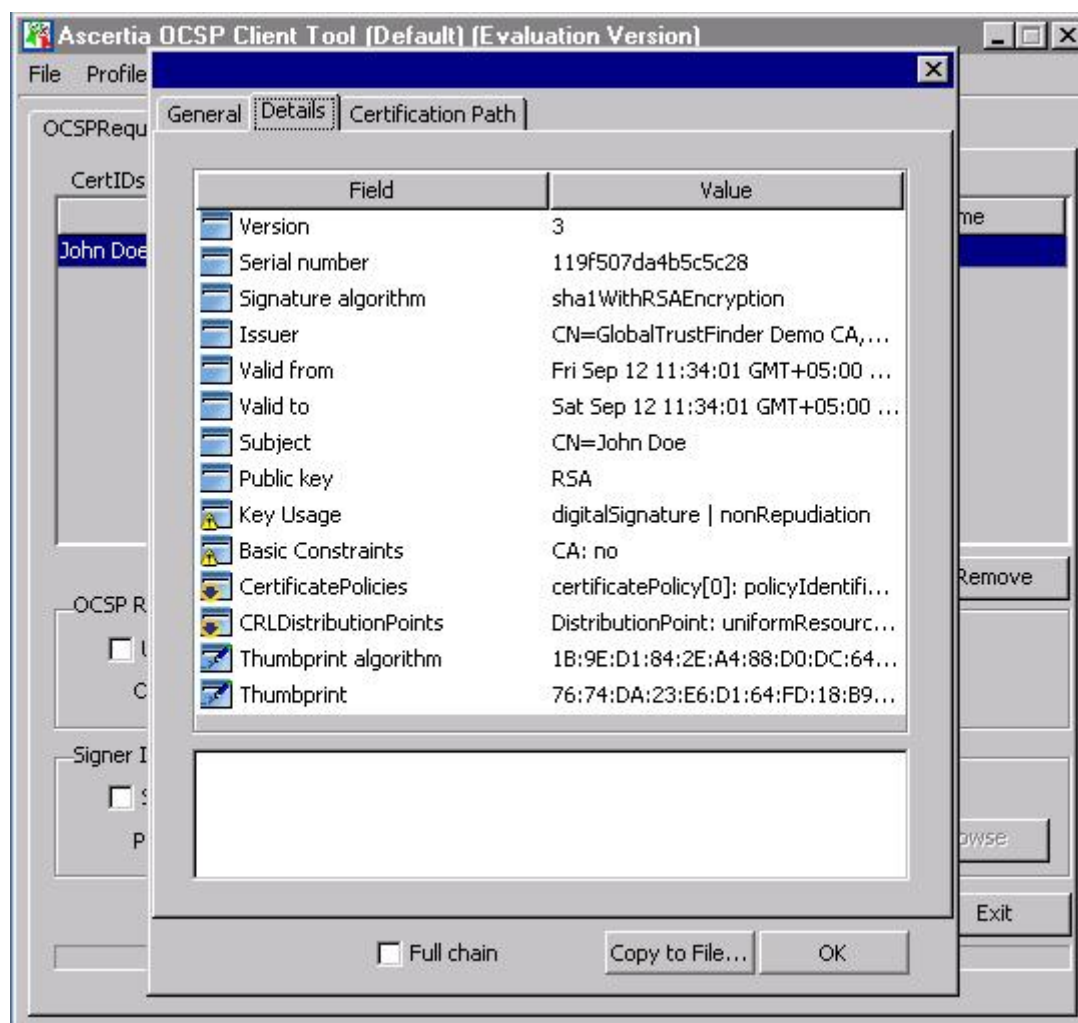
A Progress Bar at the bottom of Main User Interface describes that processing is currently being done.

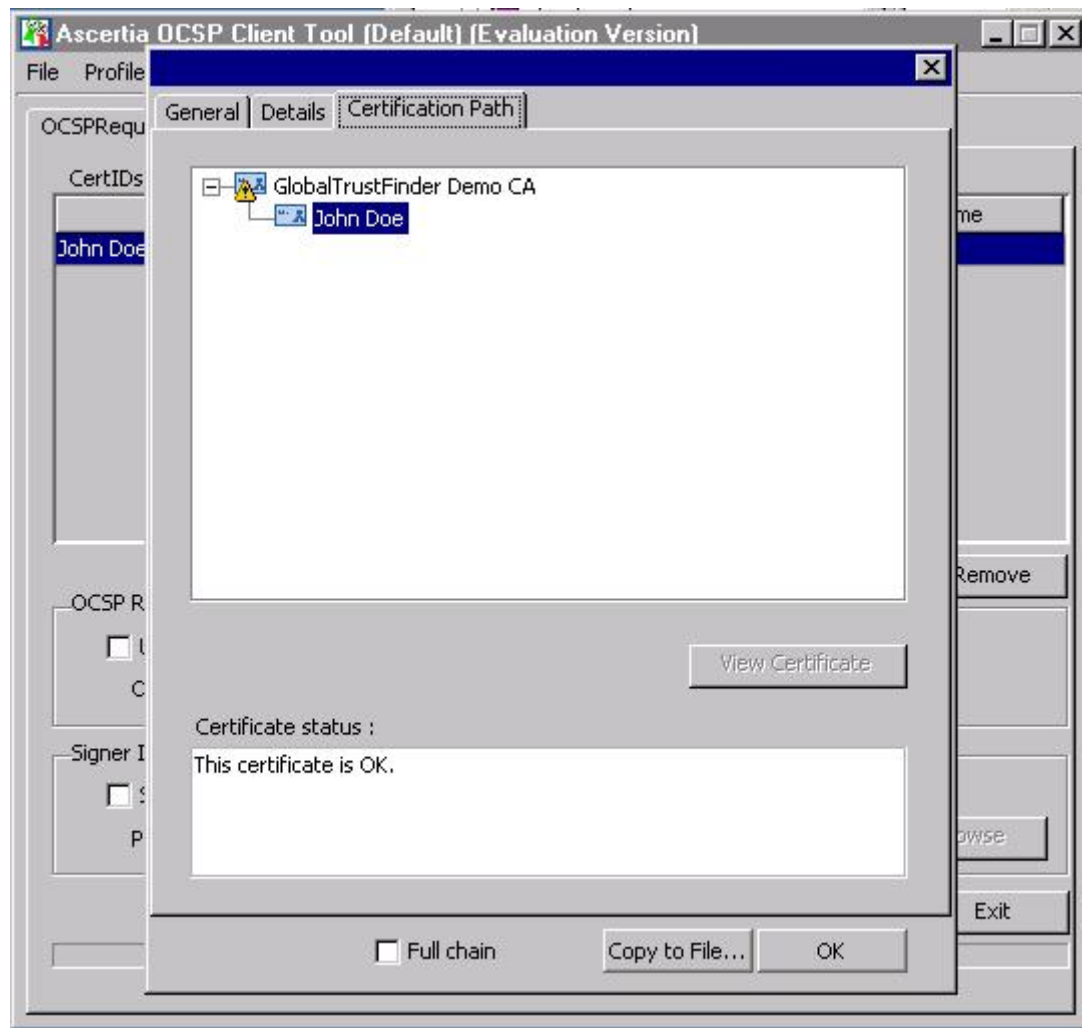


Once OCSP Responses are received the pop-up window is hidden and responses are shown in the **Results** Tab (explained below).

The **Save** button allows you to save any changes made to the configuration in the current OCSP Client Tool profile.

Certificates can be examined in detail by double-clicking the relevant certificate in the request table:

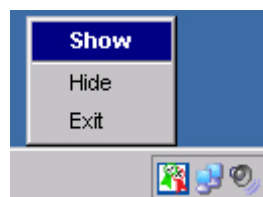




Note when the OCSP Client Tool is launched, it is also added to the System Tray.

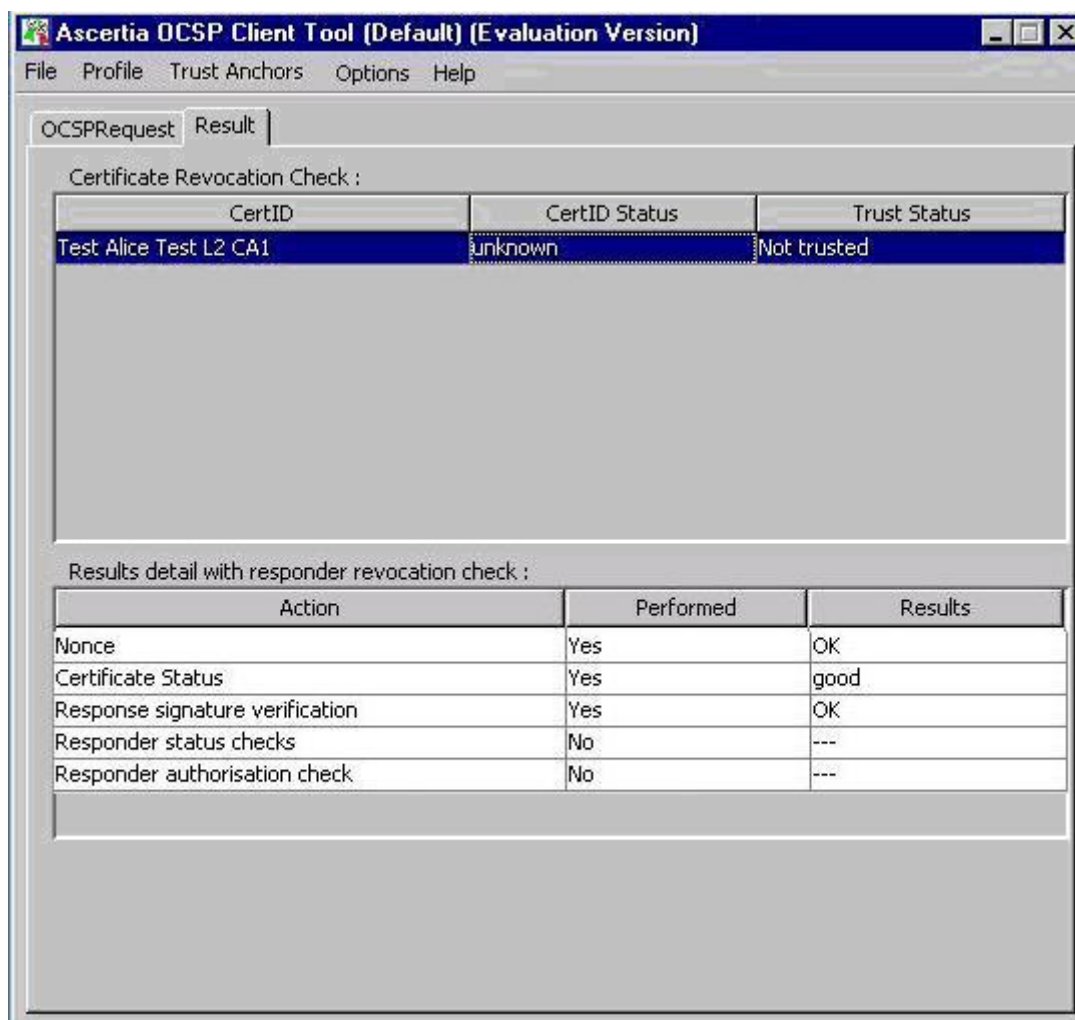


The application can be closed by pressing the **Exit** button from the OCSP request tab, or by pressing the **Exit** option from **File** Menu or by right-clicking the OCSP Client Tool System Tray Icon and selecting **Exit** option.



2.4 Result Tab

The **Result Tab** will be shown once an OCSP Response has been received. OCSP Client Tool not only checks the revocation of the target certificates specified in **OCSP Request** Tab but can also check the revocation status of (each) responder's certificate status too (i.e. to determine if the OCSP responder can be trusted).



The **Certificate Revocation Check** section of this window shows the details regarding the revocation information of the selected certificates (referred to as target certificates) where as **Responder Revocation Check** section shows the revocation information of each Responder certificate from where the OCSP response was received. Details of each section are described in more detail below:

2.4.1 Certificate Revocation Check

Grid Column	Values	Description
CertID	-	Alias of each target certificate (this identifies the subject of the certificate).
CertID Status	- good - revoked	This identifies the revocation status of the target certificate obtained directly from the OCSP response (without any processing).

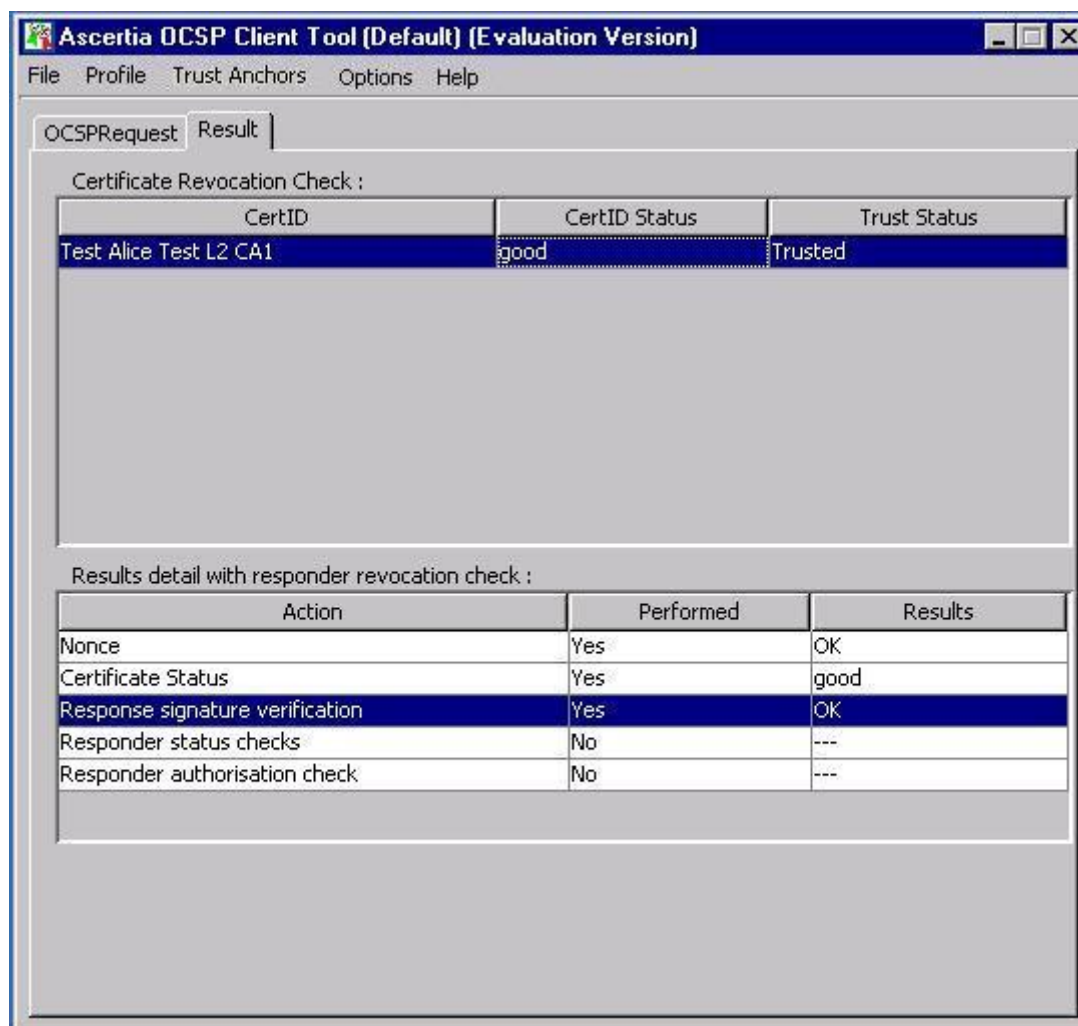
	- unknown	
Trust Status	<ul style="list-style-type: none"> - Trusted - Not Trusted 	Shows whether the target certificate can be trusted or not. This decision is based not only on whether or not the target certificate is good, revoked or unknown but also other checks performed as configured in the OCSP Client Tool. For example, nonce check, signature validation check, responder's certificate OCSP status check and OCSP responder authority check. If any of these checks are not performed successfully, then the overall rating of the certificate is considered "Not Trusted".

2.4.2 Result Details with Responder Revocation Check

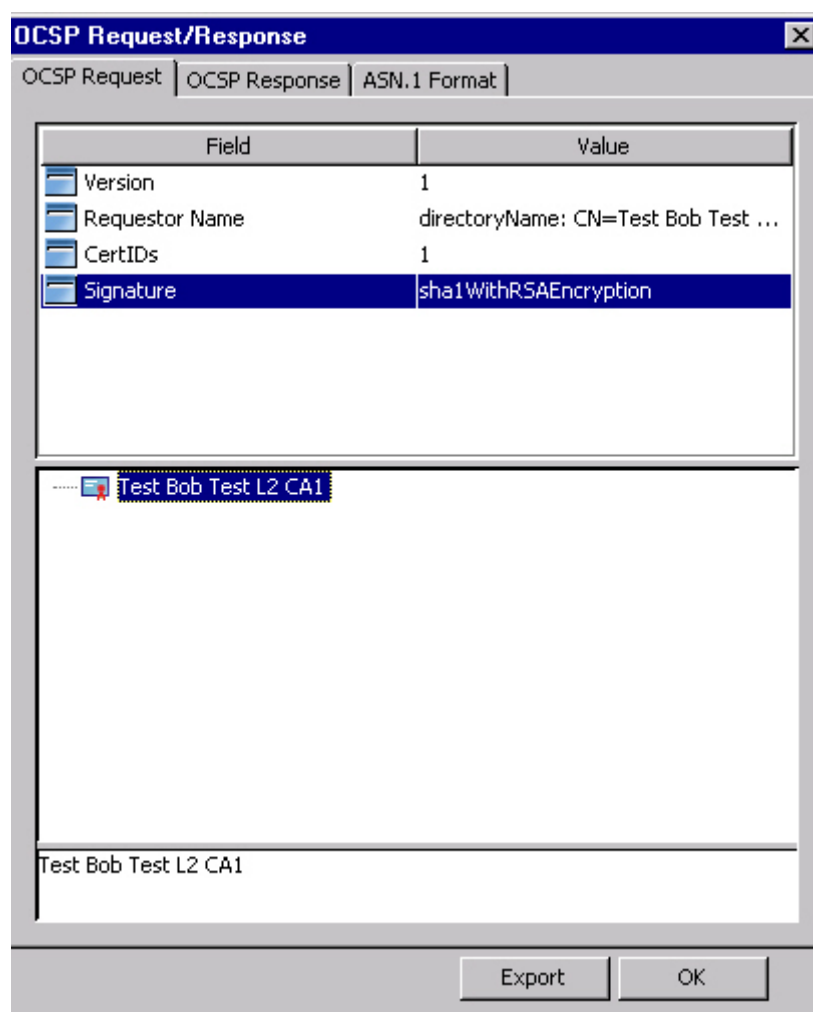
Grid Column	Values	Description
Action	<ul style="list-style-type: none"> - Nonce - Certificate Status - Signature - Responder Status - Responder Authority 	<p>This column identifies all actions that could be carried out by the OCSP Client Tool.</p> <ul style="list-style-type: none"> - helps to detect replayed OCSP responses (achieves this by matching an OCSP response against the corresponding OCSP request using unique numbers added the OCSP request and response). - Status of the target certificate as sent by OCSP responder in OCSP response. This should be the same as the CertID Status in the "certificate revocation check" section. - This checks the signature on the OCSP response to ensure it is cryptographically correct and that the signer (i.e. OCSP responder) is trusted by building a certificate chain to a configured Trust Anchor. - This generates another OCSP request to check the status of the OCSP Responder's certificate. The response received back in this case is checked with regards to nonce, signature, certificate status and responder authority as configured in OCSP Client Tool. - Checks that the OCSP responder is authorized to respond for the target certificate (i.e. the OCSP responder's certificate was issued by the same CA which issued the target certificate and the OCSP responder's certificate contains an Extended Key Usage extension which is marked "OCSP signing").
Performed	<ul style="list-style-type: none"> - Yes - No 	This simply describes whether the corresponding action was performed or not.
Results	<ul style="list-style-type: none"> - good - revoked - unknown - OK - Failed 	This provides the results for the relevant operation.

2.5 Sample OCSP Response

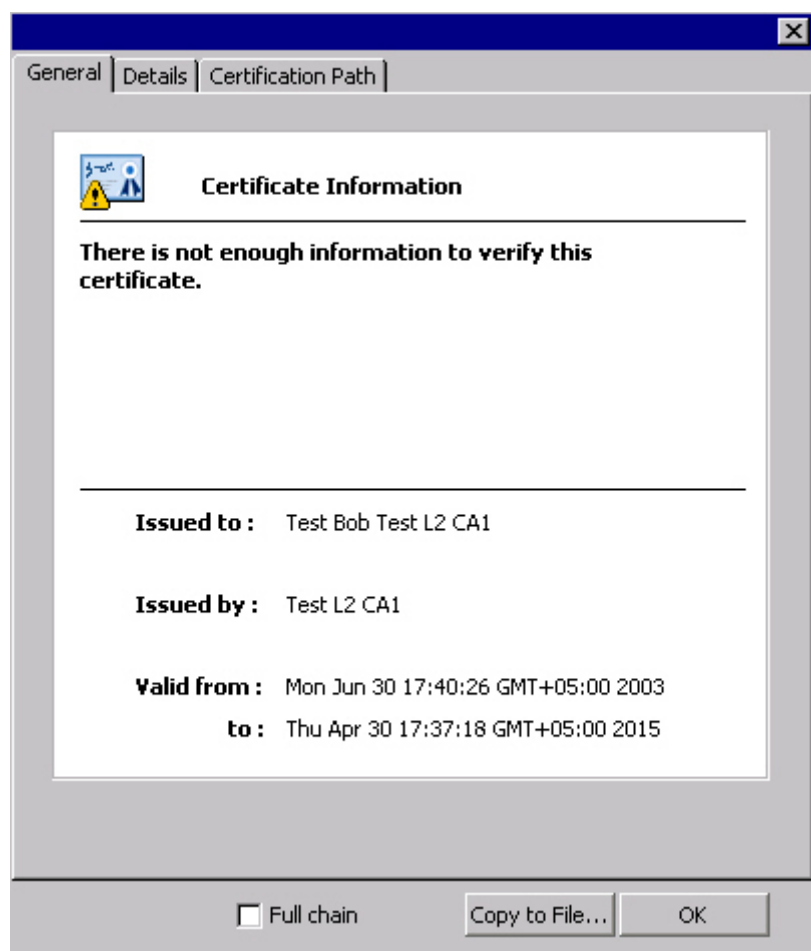
On sending an OCSP Request following is the Response shown in the **Results** Tab



Double clicking on a particular entry in **Certificate Revocation Check** section and this will show the OCSP Request and Response in human readable format as shown below:



You can also double-click the certificate to view the certificate details:



Double-click the OCSP Response to view the response details:

OCSP Request/Response

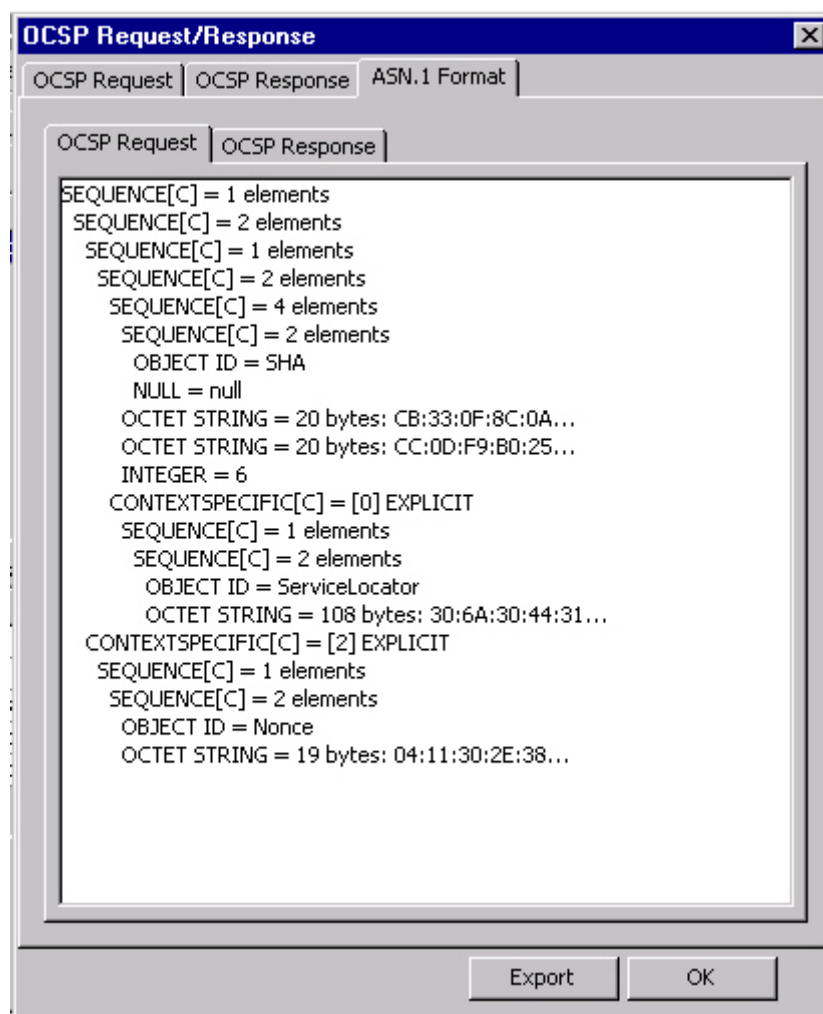
OCSP Request | **OCSP Response** | ASN.1 Format

Field	Value
OCSP Response Status	0: successful
Response Type	Basic OCSP Response
Version	1
Responder ID	EMAIL=insecure@test.insecure,CN...
Produced At	Thu Sep 25 13:04:13 GMT+05:00 2...
Single Responses	1
Response Extensions	1
Signature	sha1WithRSAEncryption

Single Response: 1

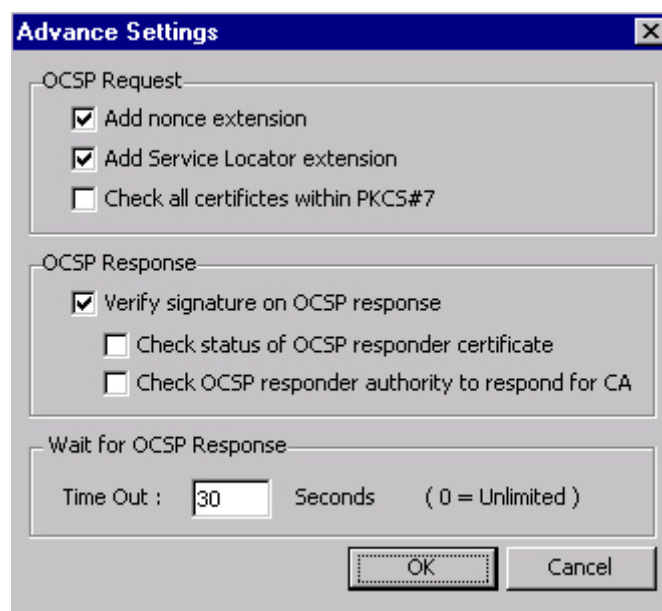
- Serial Number: 0x5
 - Hash Algorithm: SHA (1.3.14.3.2.26)
 - Issuer Name Hash: CB:33:0F:8C:0A:46:3D:FA:3A:0F:90:08:9
 - Issuer Key Hash: CC:0D:F9:B0:25:20:09:39:AA:4B:7D:CD:6A
- Cert Status: unknown**
- This Update: Sun Oct 24 11:00:11 GMT+05:00 2004
- Next Update: Mon Oct 25 11:00:11 GMT+05:00 2004

Cert Status: unknown



3 Advance Configuration

The **Options > Advance Settings** menu item is used to configure aspects of the OCSP request, processing options for the OCSP response and timeout settings:



The **OCSP Request** section allows the following settings:

- **Add nonce extension** – in this case a unique number is added to the OCSP request and the response is checked to ensure that it contains the same value.
- **Add service locator extension** – this is obtained from the target certificate's AIA extension and is included in Service Locator extension of the OCSP request message. If the AIA field is not present then the application will ask whether to proceed or not if this option is selected.
- **Check all certificates within PKCS#7 chain** – this means that if a PKCS#7 was used to identify the target certificate, then all of the certificates within the PKCS#7chain will be converted into CertIDs and included in the OCSP request.

Note that if the final certificate in the chain is not a Root certificate and its CertID can therefore not be formed then this certificate will be ignored in the OCSP request. If unchecked then only the first pair of certificates (i.e. target certificate and its issuer certificate) present in PKCS#7 file will be used to create the CertID.

The **OCSP Response** section of the tab allows you to perform the following:

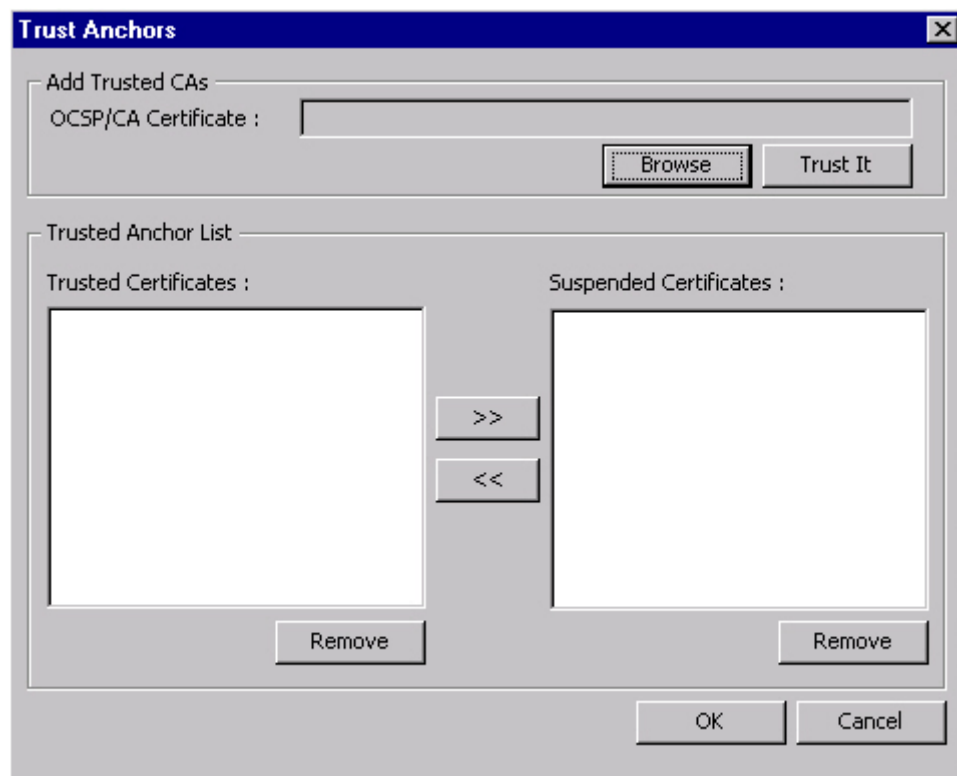
- **Validate signature on OCSP response** – If not selected, OCSP Client Tool simply assumes that the OCSP response was signed correctly and that a valid certificate path for the OCSP responder can be built. So it simply displays the OCSP responses as shown previously without any further processing. If this option is not selected then the other options in this section are also turned off. If this option is selected then the signature will be validated to a final trust point (or anchor). The configuring of trust anchors is explained later.
- **Check status of OCSP responder certificate** – When an OCSP response is received and it is not from a trusted OCSP responder (explained below) and its certificate does NOT contain a "noCheck" extension then the status of this OCSP Responder's certificate is checked. It can be checked again against the configuration made on the **OCSP Request** tab (using AIA or OCSP Responder URL). Therefore another OCSP request is formed to check



the status of the OCSP responder's certificate. This process is repeated until an OCSP responder certificate is encountered which either contains a "noCheck" extension or the OCSP responder certificate is a trusted responder. Currently to avoid loops, the OCSP Client performs this loop only once. Please consult Ascertia if you require this precaution to be removed.

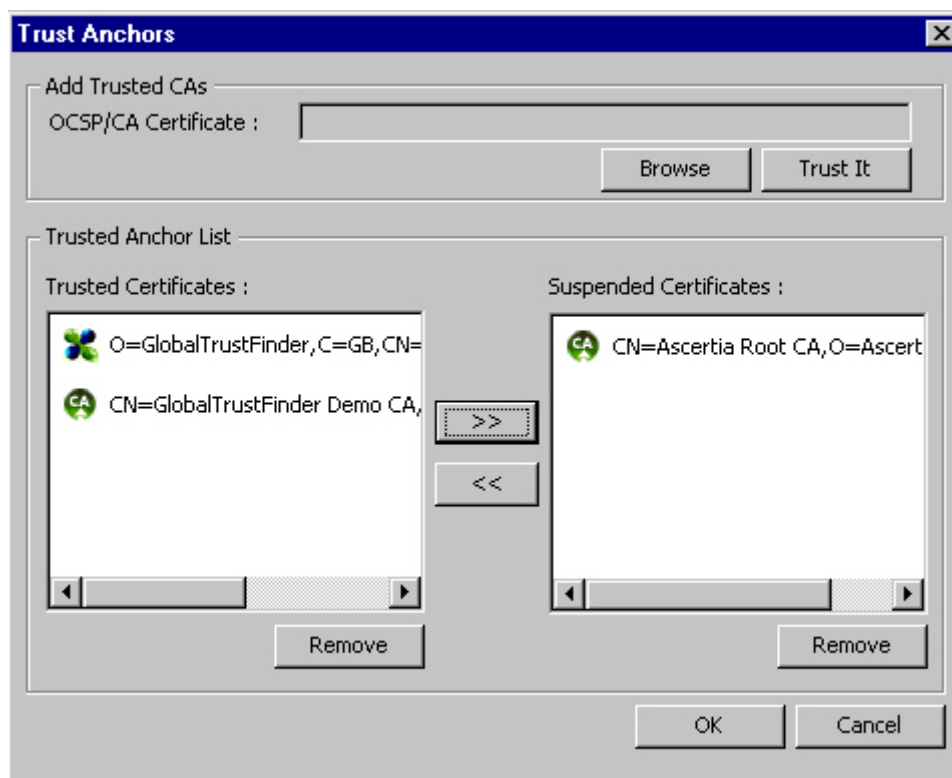
- **Check Responder has authority to respond for issuer** – If enabled the software will check the OCSP responder's certificate to see if it was issued by the same CA which issued the CertID which is being checked; and that the OCSP responder's certificate contains the Extended Key Usage extension showing "OCSP signing". This proves that the issuing CA has authorized this responder to provide revocation information on its behalf. If this check is configured but fails then the responder cannot be trusted.

4 Trust Anchors Configuration

The **Trust Anchors > Manage Trust Anchors** menu item is used to configure Trusted CAs and Trusted OCSP Responders. The meaning and purpose of these is explained below.



Only two kinds of certificates can be added to the Trusted Anchor List; CA certificates and Responder certificates represented by  and  images respectively.



The Trusted Root CA certificates act as a final point for certificate path building. All certificate paths (i.e. for validating received OCSP responses) must end with a certificate of a Trusted Root CA if OCSP responses are being validated.

The Trusted OCSP responders can be added as a final point for validating OCSP responses, i.e. the status of these OCSP responders is considered “good” without any further OCSP checking.

- It only trust an OCSP responder cert if it can build a chain to either a self-signed Root CA existing within the TA list or the OCSP responder is directly trusted in the TA list
- It builds certificate chains using either intermediate CAs held within the OCSP Client Tool TA list or available from the OCSP response.

Note therefore the intermediate CA certs in the Trust Anchor list are only to aid path building and do not form final trust points for certificate validation.

The **Suspend** and **Reactivate** buttons help to transfer the Trusted certificates between the two Lists. If a Certificate is suspended than it will not be used for trust purposes for any response. You can also remove a Trusted Anchor by clicking **Remove** button.

A User can view the certificate contents of certificates present in Trusted Anchor List by double clicking the respected certificate.

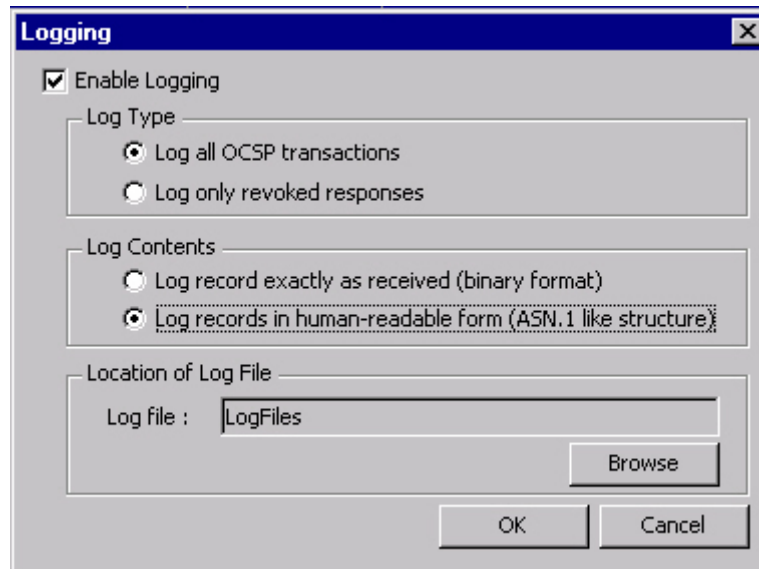
Also note that in order for OCSP Client Tool to communicate with an OCSP responder running over SSL channel, the issuer of responder’s SSL certificate or the SSL certificate itself needs to be trusted in the java keystore for OCSP Client Tool. This java keystore is separate from the OCSP Client Tool trusted anchor list. To serve this purpose, any certificates registered in the trusted anchor list are automatically added to the OCSP Client Tool Java keystore. Certificates are removed from the java keystore upon suspending or removing them from the trusted anchor list. Certificates are added back to the java keystore when reactivated in the trusted anchor list.



The Ascertia Root CA certificate which comes pre-registered in the OCSP Client Tool trusted anchor list is not added to the java keystore. If this is required to trust SSL certificates issued by the Ascertia Root CA then suspend this certificate and reactivate it to add it to the java keystore.

5 Logging Configuration

The **Option > Logging** menu item is used to configure the OCSP transactions:

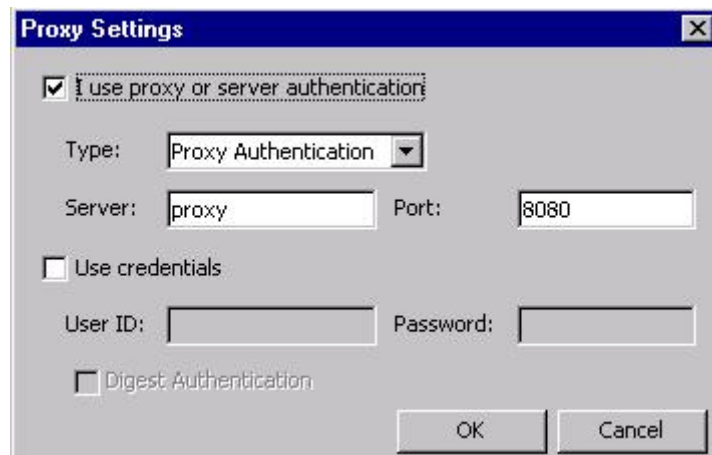


The OCSP Client Tool logging can record either all OCSP request/responses or just those OCSP requests/responses which contain at least one “revoked” CertID. The logs are recorded in DER format. By default all of the log information is being stored in **ocspTransaction.dat** file created during Installation, but the location can be changed.

The log records can be created either in the binary format or in the form of ASN.1 like structure. The ASN.1 base log records are human readable and are easier to understand.

6 Proxy Configuration

The **Option > Proxy** menu item is used to configure the proxy settings:



If the OCSP Client Tool is running behind a proxy server or a web server which requires authentication, then use the Proxy Settings dialog to select relevant type for authentication and also configure the server name and port settings. If a username and password is required to authenticate in your environment then select the checkbox "Use credentials" and provide a valid username and password. Optionally select the "Digest Authentication" checkbox if this is applicable in your environment.

*** End of document ***