



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

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

www.ascertia.com

OCSP Monitor User Manual

Document Version: 2.2.0.1

Document Issued: January, 2010

©Copyright Ascertia Ltd, 2010

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

Contents

1	Introduction	3
1.1	Scope	3
1.2	Intended Readership	3
1.3	Conventions	3
1.4	Technical support	3
2	Overview	4
3	Configuring OCSP Monitor	5
3.1	Settings	5
3.2	Email / SMS Contacts	13
3.3	Create Test Scenario	16
3.4	Create Test Case	25
3.5	Edit Scenarios and Test Cases	27
4	Using OCSP Monitor	30
4.1	Importing the Commercial License File	30
4.2	Example Reports	30
4.3	Live Report	34
4.4	Show Last Warning Report	37
4.5	Show End of Day Report	38
4.6	History Viewer	39

1 Introduction

1.1 Scope

This manual describes how to operate the OCSP Monitor application on Windows® operating systems.

1.2 Intended Readership

This guide is intended for administrators/operators who are responsible for monitoring an OCSP service within an organization or on behalf of an organization.

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 Technical support

If Technical Support is required, Ascertia has a dedicated support team providing debugging assistance, integration assistance and general customer support services. 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 describe 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 confirm:

- The operating system and any applied service packs;
- The logs, DB and XML folders from the location;
<Operating System Drive>\Program Files\Ascertia\OCSP Monitor
- Any screenshots displaying error messages;
- Steps on how to reproduce any errors.

2 Overview

OCSP Monitor is a product that runs as a service on a Windows server or desktop system to continually monitor the status of one or more OCSP responders. Various types of tests can be setup ranging from simple availability checks to complex full policy checking with positive and negative test checking. The OCSP responders being monitored must be compliant with the RFC 2560 specification.

The management and configuration of OCSP Monitor is handled via a user friendly GUI. The warning or summary reports produced by OCSP Monitor are sent by email or SMS to identified support staff or business managers.

OCSP Monitor allows administrators to:

- Create a “Test Scenario” which specifies:
 - The OCSP responder being tested
 - The schedule for executing the test scenario
 - The settings for warning and summary reports (i.e. the format of these reports and to whom these should be sent).
- Within a Test Scenario, an administrator can create one or more “Test Cases”. For each Test Case the administrator can define:
 - The target certificate to be checked by the OCSP responder
 - The expected response from the OCSP responder for this test case (i.e. good, revoked, unknown, etc.)
 - The OCSP request configuration, whether to add nonce, service locator extensions, whether requests should be signed and if so with which key/certificate, and how to process the OCSP responses received

Before using OCSP Monitor to assess a particular OCSP service, the administrator needs to perform some basic configurations:

- Set-up the trust anchors which will be used to verify the OCSP response signature and certificate chain
- Configure proxy settings, specify default locations for scenario reports; configure email server settings and daily report scheduler settings.
- Configure email contacts that are to receive reports from OCSP Monitor

This manual describes how to perform these tasks.

OCSP Monitor also records all transactions within its database and provides a sophisticated history viewer for viewing these past transactions. A live status viewer provides live summary information on the tests configured and currently in progress and also provides details of the test case results.

3 Configuring OCSP Monitor

This section describes the initial configuration actions an administrator needs to make before creating and running test scenarios (it is recommended that the list below is followed in order):

1. Set-up the default trust anchor list, so that OCSP responses can be verified and trusted (note the trust anchor selection can be defined on a per test scenario)
2. Set-up any proxy details that are needed to communicate with the OCSP responder(s)
3. Define the location where reports are to be saved
4. Define the email server and optional SMS server details so that OCSP Monitor can send reports to recipients via these
5. Set a schedule for the daily email reports and to whom these should be sent
6. Create email and SMS contacts for those people that need to receive email and/or SMS reports from OCSP Monitor

SMS is only used for warning reports because these are of urgent nature and are limited in size. Email is used for all report types including end of scenario and end of day reports.

3.1 Settings

Launch OCSP Monitor and click the **Settings** option in the right pane:



IMPORTANT:
Changes to OCSP Monitor can only be applied when the service is stopped.

3.1.1 Trust Anchor

The OCSP Monitor Trust Anchor list stores trusted certificates. The list is used to store self-signed Root CA certificates which are the final trust points for the certificates used by OCSP Monitor in its test scenarios.

When OCSP Monitor receives an OCSP response it will attempt to verify it by building a certificate chain from the OCSP responder's certificate to a Root CA certificate in the Trust Anchor list. If a chain can be successfully built then the OCSP responder is authenticated and trusted. If not the OCSP response cannot be trusted.

The intermediate CA certificates can be retrieved by OCSP Monitor from the OCSP response message itself or alternatively they can also be added to the OCSP Monitor Trust Anchor list. It does not matter which way OCSP Monitor obtains the intermediate certificates as long as a successful chain of certificates can be built to Root CA in the Trust Anchor list.

OCSP Monitor uses two cryptographic toolkits for resilience, these are:

CML (Certificate Management Library) which is the primary mechanism for certificate path building and a fallback mechanism which uses Microsoft CAPI (Cryptographic Application Programming Interface). The reason for this is that CML follows PKI standards very closely and may reject some certificates which are not encoded precisely to these standards. Microsoft CAPI is more tolerant of other certificate profiles.



When Microsoft CAPI is used for certificate path building then there is an additional requirement from Microsoft CAPI to install complete certificate chain (including Root CA) also in the Microsoft Windows keystore so that path building process can be initiated. Note the final trust point (a Root CA) must be defined in the OCSP Monitor Trust Anchor list irrespective of whether CML or Microsoft CAPI is used during path building.

If OCSP Monitor fails to trust the OCSP responder then the OCSP responder certificate chain should be added to the Windows keystore, for example by using Internet Explorer. Ensure that the certificates are added to the system account as this is the profile that OCSP Monitor uses when validating OCSP responses.

To add certificates in the OCSP Monitor **Trust Anchor** list you import them from a file or from Internet Explorer:



The six options at the bottom of this screen are explored:

Add certificate from file: A certificate file can be added to the Trust Anchor by clicking this link.

Add certificate from Internet Explorer: A certificate can be copied from Internet Explorer CAPI stores and added to the OCSP Monitor Trust Anchor list by clicking this link.

Add Certificate chain: A complete certificate chain can be added to the Trust Anchor by clicking this link.

Remove certificate from Trust Anchor: A defined certificate can be deleted from the Trust Anchor list.

Import Trust Anchor: A file with a “.pss” extension containing one or many certificates can be imported in the Trust Anchor by clicking this link.

Export Trust Anchor: All the certificates in the Trust Anchor can be exported as a single file with a “.pss” extension by clicking this link.

3.1.2 Proxy Settings

If a proxy server is being used, the proxy settings can be set by selecting the **Proxy** option from the left pane and then providing the proxy Address and Port. Other configuration data such as authentication details can be defined.

Click the **Apply** button once the proxy settings have been configured.



3.1.3 Scenario Reports Location

The Scenario Reports Location can be specified on the physical drive where the scenario reports are to be saved:



Ensure that the **Apply** button is clicked once the default folder for the scenario reports has been specified.

3.1.4 Email / SMS Server

Clicking on the Email / SMS Server option in the left pane enables the email / SMS server settings.

Configure the Email tab by specifying the Email format either as Plain Text or HTML, Sender Name, Sender Email, Outgoing Mail Server (SMTP) and its port. If the SMTP server requires authentication then provide the username/password for the email account.



The screenshot shows the 'Settings' window of the 'Ascertia OCSP Monitor'. The 'Email / SMS Server' section is active. It features two tabs: 'Email' (selected) and 'SMS'. The 'Email' tab contains the following fields and controls:

- Email Format:** A dropdown menu set to 'Plain Text'.
- Sender Name:** A text box containing 'Ascertia OCSP Monitor'.
- Sender Email:** A text box containing 'ocsp.monitor@ascertia.com'.
- Outgoing mail server (SMTP):** A text box containing 'smtp.ascertia.com'.
- Port:** A text box containing '25'.
- Test:** A button to verify the SMTP server settings.
- ☐ **Outgoing email server (SMTP) requires authentication**
- Username:** A text box (empty).
- Password:** A text box (empty).
- Apply:** A button to save the settings.

The left sidebar of the settings window lists other configuration options: Trust Anchors, Proxy, Scenario Reports Location, **Email / SMS Server** (highlighted), and Daily Report Scheduler.



Click the Test button to verify the email server settings are working.

Configure the SMS tab by specifying the SMS Server Address, User Name, Password, API Id and the Phone Number. The phone number is only required for testing purposes. Use the test button to check the configuration and a test SMS will be sent to that phone.



Fields	Descriptions
SMS Server Address	Enter the server address e.g. http://api.clickatell.com . Ascertia has tested the service provided by: www.clickatell.com .
User Name	Enter the username of the account created at the Clickatell website.
Password	Enter the password of the account created.
API Id	This specifies the application being used on the Clickatell website (e.g. XML, HTTP).
Phone Number	Optionally enter the phone number which will receive the test warning messages.



The SMS Service only works with the Clickatell account.

3.1.5 Daily Report Scheduler

Clicking on the Daily Report Scheduler option in the left pane enables scheduling of the Daily Summary report for all test scenarios which have been selected for inclusion in this report. The following details need to be specified:

- Subject (of the email)
- Initial Message (i.e. the email body text before including the results);
- Recipients (to whom the daily report will be sent);
- Generation Time (this should be after the stop time of all test scenarios).



The screenshot shows the 'Ascertia OCSP Monitor' application window. The title bar includes the application name and standard window controls. The main header features the 'OCSP Monitor' logo and 'Help' and 'About' buttons. Below this is a 'Settings' section with a 'Back to Home' button. On the left, a sidebar lists various settings: Trust Anchors, Proxy, Scenario Reports Location, Email / SMS Server, and 'Daily Report Scheduler' (which is currently selected). The 'Daily Report Scheduler' panel contains the following fields:

- Subject:** A text box containing 'OCSP Monitor Daily Report'.
- Generation Time:** A time selection control showing '11:59 PM'.
- Initial Message:** A large text area containing 'Initial Daily Report Message'.
- Recipients:** A table with two columns: 'Display Name' and 'Email Address'. The table is currently empty.

At the bottom right of the 'Recipients' table, there is a small icon of a person with a plus sign, and an 'Apply' button.

3.2 Email / SMS Contacts

To manage email / SMS contacts and specify who will receive OCSP Monitor reports go to the OCSP Monitor Home screen and click the **Email / SMS Contacts** option in the right pane.



The following screen will be displayed:



Click the **Add an email contact** option.

Enter the Name, Phone Number and Email Address of the recipient who are to receive OCSP Monitor reports and click the **Add** button.



Name	Phone no.	Email Address
Ascertia Support	0441483685500	support@ascertia.com

Name: Phone no: Email Address:



The **Phone** number is an optional field, required only in when using SMS messages; **Name & Email Address** are compulsory fields.

3.3 Create Test Scenario

To create a test scenario and set its reporting schedule go to the OCSP Monitor Home screen and click the **Create Test Scenario** option:



The Create Test Scenario wizard will start up.

3.3.1 General

Enter a **Scenario Name** (e.g. OCSP Test Scenario 1) in the General section of the wizard and click right arrow button:



3.3.2 OCSP Responder

Configure the OCSP responder settings by entering the **Host** which is the OCSP responder address (e.g. <http://ocsp.globaltrustfinder.com>), **Port** (e.g. 80), connection **Timeout** (e.g. 30 secs) and **OCSP Freshness Threshold** limit (e.g. 0 mins). Click on the right arrow button to proceed.



Connection **Timeout** is the time that OCSP Monitor tries to connect with the OCSP responder. If this **Timeout** is reached and OCSP responder cannot be contacted then OCSP Monitor will close the connection.

OCSP Freshness Threshold

OCSP Monitor checks the freshness of an OCSP response by comparing the difference between the "thisUpdate" time and "ProducedAt" time, with the value configured in OCSP Freshness Threshold field for this scenario. If the OCSP response was produced using revocation info (e.g. a CRL) at a time which is in excess of this threshold setting, then it implies that it is using "stale" information (i.e. it is using a CRL which is now stale).

To illustrate how this works, imagine the following scenario: a CA issues CRL with a lifetime of 1 hour, but a new CRL is actually issued every 15 mins (these are often referred to as over-issued CRLs). So a CRL is issued every 15 mins with each having a lifetime of 1 hour. Also assume that the threshold is configured as 15 mins in OCSP Monitor. Now the following situation can arise:

Time 12:00PM, CA issues CRL1, OCSP responder retrieves this and uses it for its responses.

Time 12:15PM, CA issues CRL2, but for some reason OCSP responder fails to receive this and continue to use CRL1.

Time 12:16PM, OCSP responder receives a request to validate a certificate. Now the OCSP response will have a thisUpdate showing 12:00PM (since it is still using CRL1) but a producedAt time showing 12:16 (i.e. this is the time at which the responder produced this response). The difference between these two times is 16 mins. So this allows OCSP Monitor to detect that the OCSP responder

is using a stale CRL as its back-end revocation information provider, since the producedAt time is beyond the defined threshold.



The difference between the thisUpdate and the ProducedAt time values should be less than or equal to the configured Threshold value for the scenario, in order for OCSP Monitor to accept the response as fresh.

The 0 threshold configured for a scenario means that the OCSP freshness will not be checked for this scenario.

If the OCSP responder requires digest **Authentication** then give a **Username** and **Password** for the relevant network proxy.



Click the **Test Connection** button to verify that the OCSP responder settings are valid.

3.3.3 Scheduler

Now set the scenario **Start Time** and **Stop Time**, also specify the time interval at which to run the test scenario (e.g. run scenario every 5 minutes). If the scenario is not to be run at weekends click on the **Do not run at week-ends** checkbox. If the results of this scenario are to be included in the end of day summary report click the **Include in Daily Summary Report** checkbox:



The screenshot shows the 'Ascertia OCSP Monitor' application window. The title bar reads 'Ascertia OCSP Monitor'. The main header area contains the 'OCSP Monitor' logo and 'Help' and 'About' buttons. Below this is a blue bar with a 'Create Test Scenario' button and a 'Back to Home' button. The left sidebar contains icons for 'General', 'OCSP Responder', 'Scheduler' (which is selected), 'Report', and 'Trust Anchors'. The main content area is titled 'Scheduler' and contains the following settings:

- Start Time: 12:05
- Stop Time: 22:55
- Run Scenario after every: 5 Min.
- ☒ Do not run at week-ends
- ☒ Include in End of Day Summary Report

At the bottom right of the Scheduler panel, there are two blue arrows pointing left and right.

3.3.4 Warning & Summary Reports

Warning reports are only generated when the actual results of a test case do not match the expected results that we configured. Summary reports on the other hand are optional which can be configured to be sent at the test scenario stop time. These summary reports are sent regardless of what results were actually achieved.

In this section of the wizard, you can define the format of the Warning reports and Summary reports and to whom they should be sent.

In the Warning Reports tab, enter the **Warning Report** email **Subject**, **Initial email body text**, **SMS body text** and number of previous warning reports to be sent with this alert and the email/SMS **Recipients** who should receive the warning reports.




The **Warning Report** can be configured receive as either an email or SMS or both from the Channel option in the Recipient List.

In the Summary Reports tab, configure the summary report details. This is an optional report only sent at the test scenario stop time. This report provides details of all the test cases that ran between the scenario's start and stop time together with the performance statistics and details of any failures.

Enter the **Summary Report** settings by selecting the option to **Send Summary Report at Scenario Stop Time** and then specifying the email **Subject**, **Initial email body text**, and the email **Recipients** who should receive summary reports.

Click the right arrow button to proceed with the wizard:



The **Summary Report** will be sent once the scenario has stopped and the time interval mentioned in Scheduler > 'Run scenario after every' field has elapsed e.g. With a time interval of 5 mins and a scenario stops time of 11:53 PM, the scenario summary report will be sent at 11:53 PM + 5 mins, i.e. 11:58 PM.

3.3.5 Trust Anchor

All test scenarios by default use the OCSP Monitor's default Trust Anchor list, which is configured centrally in the main OCSP Monitor Settings section as described earlier. However in addition to this each Test Scenario can refine the default Trust Anchor to specify exactly which Trust Anchor(s) are to be selected for this scenario.

Simply select a certificate from the Default Trust Anchor List and then move it to the Scenario's Trust Anchor list by using the >> button. It will then be shown in the right-hand box.



Click the save button to complete the wizard.

3.3.6 Configuring OCSP Responder Clock Tolerance

The OCSP response tolerance can be configured in the "OCSPMonitorScenarioManagement.xml" file. This file is present in the following location:

<Operating System Drive>\Program Files\Ascertia\OCSP Monitor\XML

The tolerance is checked by comparing the **ProducedAt**, **ThisUpdate** and **NextUpdate** of OCSP response with a threshold value configured for each Scenario. In case the threshold exceeds, the response is not trusted and a warning report is generated.

The relevant tags are shown as below:

```
<FriendlyName>OCSP Test Scenario 1</FriendlyName>
  <UseCentralTrustAnchor>1</UseCentralTrustAnchor>
  <OCSPConfiguration>
    <Address>http://ocsp.globaltrustfinder.com</Address>
    <Port>80</Port>
    <Path></Path>
    <Timeout>30</Timeout>
    <DigestAuthentication Enabled="0">
      <UserName></UserName>
      <Password></Password>
    </DigestAuthentication>
    <OcsResponseTolerance>
      <ThisUpdate>120</ThisUpdate>
      <NextUpdate>120</NextUpdate>
      <ProducedAt>120</ProducedAt>
    </OcsResponseTolerance>
    <OCSPFreshnessThreshold>0</OCSPFreshnessThreshold>
  </OCSPConfiguration>
```



By default the tolerance is configured to 120 seconds for each scenario.

3.4 Create Test Case

To configure test cases and assign them to a test scenario go to the OCSP Monitor Home screen and click the **Create Test Case** option in the right pane.



In the screen below, first enable the test case by setting the **Test Case Status** to **Active** (only the active test cases within a test scenario are executed, **Inactive** test cases are ignored at the time of running the test scenario), set the **Expected Result** as **Good**, **Revoked**, or **Unknown** etc. based on what the responder is expected to return for this test case. A test case must be associated with any existing test scenario so that whenever this test scenario is run the test case will be executed.

Enter a **Test Case Name** and select "check revocation" for individual certificates or a PKCS#7 certificate chain. The browser can be used to identify the certificates or the certificate chain. When importing individual certificates ensure the correct issuer certificate is selected for the target certificate. I.e. the target certificate is the actual certificates whose status is being checked, the issuer certificate is the CA certificate which issued the target certificate. Both of these certificates are needed to generate the CertID which is placed in the OCSP request message.

To configure the format of the OCSP request to be sent to the OCSP responder the following checkboxes can be checked:

- **Add Nonce** (this extension helps prevent replay attacks, the OCSP responder must return the same nonce value in the OCSP response message in order for the OCSP response to be trusted)
- **Add Service Locator** (this extension allows OCSP relaying from one OCSP responder to some other authoritative OCSP responder. The Service Locator extension takes the value from the AIA extension of the certificate)

- **Verify OCSP Signature** (if this is not selected OCSP Monitor will automatically trust the OCSP response without any verification. If it is selected OCSP Monitor will need to verify the signature on the OCSP response message and also build and validate the certificate chain for the OCSP responder certificate).
- **Sign OCSP request** (this allows signing of OCSP request messages, if this is enabled then select the signer key using the Browse button). Keys in PFX and PKCS#12 format (.pfx extension) can be used for signing purposes.

Click the save button to save the test case settings:



3.5 Edit Scenarios and Test Cases

To review and edit existing Test Scenarios and Test Case settings click on the **Edit Scenarios and Test Cases** option.



Double click on an existing Test Scenario and edit the details as required.

To remove a Test Scenario, right-click on a selected scenario and click on the **Remove** option.



Ensure that the OCSP Monitor service is restarted after editing these details so that the changed data is picked up by the running service.

Double click on an existing Test Case and edit the details as required.

To remove a Test Case, right-click on a selected Test Case and click on **Remove** option.



4 Using OCSP Monitor

4.1 Importing the Commercial License File

After purchasing OCSP Monitor a commercial license file (with an EKF file extension) will be provided. This allows OCSP Monitor to be used beyond the trial period.

This file needs to be saved at the following location:

<Operating System Drive>\Program Files\Ascertia\OCSP Monitor\License

Note: This assumes that OCSP Monitor has been installed on the **C:** drive within the **Program Files** folder.

4.2 Example Reports

4.2.1 Example Warning Report

The following is an example Warning Report. Such warning reports are only sent when the response from the OCSP responder does not match the specified expected result. As shown below the failed Test Cases are highlighted in yellow.

The sample warning report in the HTML format:



Please check your test cases, one of these has failed for some reason:

Scenario Failure Report

Scenario Name: GTF - every 5 mins - must always pass
Scenario Start Time: 00:05:35
Scenario Stop Time: 23:55:35
Time Interval: 5 mins
OCSP Responder: <http://ocsp.globaltrustfinder.com:80>

Warning Report Created At:			2006-07-08 16:36:52		
Serial No.	Test Case Name	Transaction ID	Received Response	Expected Response	Result
1	Testing of Good Cert - every 5 mins - should not fail	41	Good	Good	Pass
2	Error condition test case - should always fail	42	Good	Unknown	***Fail***

The example warning report in the text format:

one of your configured test cases has failed, details are as follows:

Scenario Warning Report

```
-----
Scenario Name:      OCSP Test Scenraio1
Scenario Start Time: 00:55:35
Scenario Stop Time:  23:55:35
Time Interval:      5 mins
OCSP Responder:     http://www.ocsp.globaltrustfinder.com:80
```

Current Warning Report

Warning Report Created At: 2008-10-07 16:36:52

```
-----
Serial No:          1
Test Case Name:     Error condition test case - should always fail
Transaction ID:     42
Received Response:  Good
Expected Response:  Unknown
Result:             ***Fail***
```

The example warning report in the SMS format:

Scenario; OCSP Test Scenario1
Test Case; Check Revocation
Status has reported a failure at
08-10-2008 14:10:35

4.2.2 Example Summary Report

The following is an example Summary Report. Such reports are only sent at the Test Scenario stop time if this option has been enabled.

The performance statistics are expected to be of significant value in monitoring service level agreements and also during capacity planning exercises.

A sample summary report in HTML format is shown here:



Following is the summary of test cases executed for this test scenario:

Scenario Summary Report

Scenario Name: GTF - every 5 mins - must always pass
 Scenario Start Time: 00:05:35
 Scenario Stop Time: 23:55:35
 Number of times scenario was run: 95
 Time Interval: 5 mins
 OCSP Responder: <http://ocsp.globaltrustfinder.com:80>

Summary Report Created At:	Sunday, July 09, 2006 00:05:35
Minimum Response Time:	1.18 (sec)
Average Response Time:	1.73 (sec)
Maximum Response Time:	2.28 (sec)
Total Test Cases Failed:	73
Total Test Cases Passed:	91

The sample summary report in text format:

The test scenario summary report follows

Scenario Summary Report

```

Scenario Name:                OCSP Test Scenario1
Scenario Start Time:          00:05:55
Scenario Stop Time:           23:50:55
Number of times scenario was run: 95
Time Interval:                5 mins
OCSP Responder:               http://ocsp.globaltrustfinder.com:80
  
```

```

Summary Report Created At:    Saturday, October 07, 2008 23:55:55
Minimum Response Time:        0.01 (sec)
Average Response Time:        1.75 (sec)
Maximum Response Time:        13.61 (sec)
Total Test Cases Failed:      73
Total Test Cases Passed:      117
  
```

Test Case Name Number of Failures

```

Check Revocation Status1      35
Check Revocation Status1      38
  
```


4.2.3 Daily Summary Report

The following is an example Daily Summary Report. This report is only sent at the scheduled “end of day” and only for those Test Scenarios that have been selected for inclusion in this report - set when creating the Test Scenario.

Performance statistics are shown as in the Test Scenario summary report. The number of failures is shown and highlighted in yellow for easy viewing.

The sample daily summary report in the HTML format:



Following is end of day summary report:

Scenario Summary Report

Scenario Name: OCSP Test Scenario 1
 Scenario Start Time: 09:00:00
 Scenario Stop Time: 16:00:00
 Number of times scenario was run: 438
 Time Interval: 1 mins
 OCSP Responder: http://gtf

Summary Report Created At:	Wednesday, July 12, 2006 17:00:00
Minimum Response Time:	4.58 (sec)
Average Response Time:	4.58 (sec)
Maximum Response Time:	26.22 (sec)
Total Test Cases Failed:	46
Total Test Cases Passed:	0

Test Case Name	Number of Failures
Check Alice Cert. Revocation	46

Scenario Summary Report

Scenario Name: OCSP Test Scenario 2
 Scenario Start Time: 09:00:00
 Scenario Stop Time: 16:00:00
 Number of times scenario was run: 21
 Time Interval: 1 mins
 OCSP Responder: http://gtf

Summary Report Created At:	Wednesday, July 12, 2006 17:00:00
Minimum Response Time:	4.57 (sec)
Average Response Time:	4.57 (sec)
Maximum Response Time:	21.62 (sec)
Total Test Cases Failed:	18
Total Test Cases Passed:	0

Test Case Name	Number of Failures
Check Charlie Cert. Revocation	18

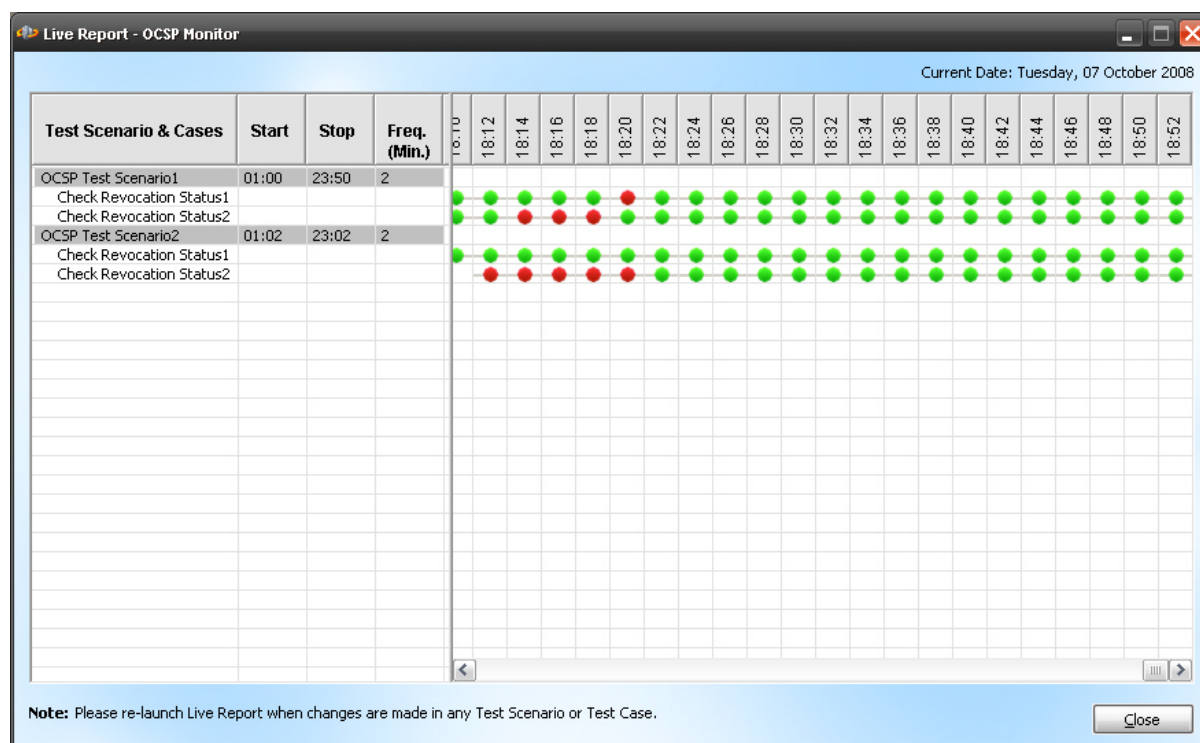


If no scenario is selected to be included in the **Daily Summary Report**, then an empty daily report will be generated.

4.3 Live Report

The status of the test cases currently running and their respective results can be viewed by clicking on the Live Report button.





This will show the active test scenarios and their respective test cases currently running.

The statuses of the test scenarios are presented using green and red dots. Green dots represent successful transactions and red dots represent failed transactions. Clicking on the dots will provide summary details of that transaction (e.g. Transaction ID, Target Certificate, Result).



The OCSP Request and Response window can be opened by clicking the **View OCSP Request/Response** button.

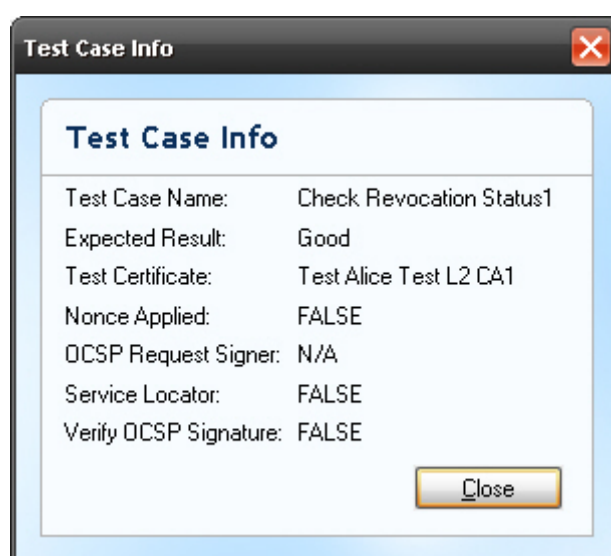
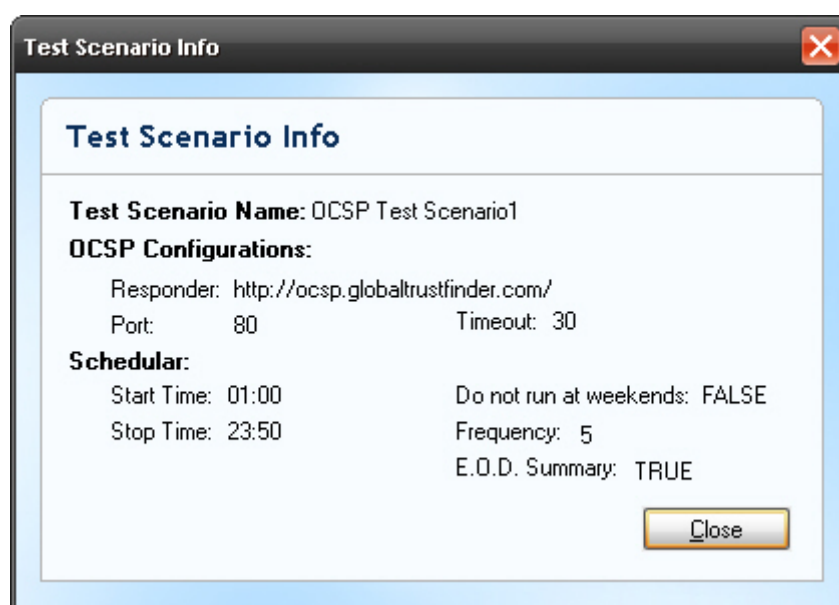
Live Report will show the transactions for the current day only (i.e. 24-hour), when the next day starts the previous days details are cleared.

The Column frequency (i.e. the time scale setting) in the Live Report is automatically set to the minimum frequency of any active test scenario configured in the OCSP Monitor i.e. 2 minutes is the minimum frequency shown in the image above.



The OCSP Monitor Live Report retrieves and displays the information of the transactions from the database after every 10 seconds.

Information about the Test Scenario and the Test Case can be retrieved in the form of a pop-up by clicking on the respective option within the Live Report window. When clicked on the test scenario, a pop-up appears providing the details of the scenario configured (e.g. Responder address, Port no., Start/Stop time, Frequency). Similarly when clicked on the test case, a pop-up appears providing the test case configured (e.g. Test Certificate, Expected Result).



4.4 Show Last Warning Report

The last warning report can be viewed by clicking on the option **Show Last Warning Report** on the OCSP Monitor Home page.



4.5 Show End of Day Report

The last end of day summary report can be viewed by clicking the option **Show End of Day Report** on the OCSP Monitor Home page.




4.6 History Viewer

The History Viewer enables old OCSP request and response transaction details to be viewed and can be accessed by clicking on the **History Viewer** button on the OCSP Monitor Home page.







The following is a screenshot of the OCSP Monitor History viewer:



Transaction ID	Test Scenario	Test Case	Target Cert Alias	Request Date/Time	Response Time ...	Result
406	s1	bob revoked	Test Bob Test L2...	2008-09-24 10:30:25.4320	0.89	PASS
405	s1	alice good	Test Alice Test L...	2008-09-24 10:30:25.4320	1.00	PASS
404	s6	rod good	Rod Crook	2008-09-24 10:06:28.7390	0.01	FAIL
403	s6	alice good	Test Alice Test L...	2008-09-24 10:06:28.7230	0.03	PASS
402	s5	alice sig required	Test Alice Test L...	2008-09-24 10:04:23.7340	0.42	PASS
401	s5	bob unknown	Test Bob Test L2...	2008-09-24 10:04:23.7340	0.42	FAIL
400	s4	bob malformed	Test Bob Test L2...	2008-09-24 10:03:55.7330	20.13	PASS
399	s4	alice unknown	Test Alice Test L...	2008-09-24 10:03:55.7330	20.13	FAIL
398	s3	alice good	Test Alice Test L...	2008-09-24 10:02:13.8380	0.95	FAIL:...
397	s3	bob revoked	Test Bob Test L2...	2008-09-24 10:02:13.8380	1.06	FAIL:...
396	s2	bob revoked	Test Bob Test L2...	2008-09-24 10:01:02.7260	0.86	PASS
395	s2	alice good	Test Alice Test L...	2008-09-24 10:01:02.7110	0.78	PASS
394	s1	bob revoked	Test Bob Test L2...	2008-09-24 10:00:25.3660	0.92	PASS

The failed transactions are shown highlighted in yellow.

The transactions are shown in pages and these pages can be navigated using the forward and back buttons:  . The current screen can be refreshed by clicking on the refresh  button.

A particular transaction can be searched for by entering the **Transaction ID** and pressing the **Go** button. A filter can also be applied to all records by clicking on the configure filter  button.

<input type="checkbox"/> Test Scenario Name:	<input type="text"/>	<input type="checkbox"/> Target Cert Alias:	<input type="text"/>	AND <input type="button" value="v"/>
<input type="checkbox"/> Transaction Status:	PASS <input type="button" value="v"/>	<input type="checkbox"/> Request Date:	18-05-09 <input type="button" value="v"/>	day(s)
<input type="checkbox"/> Test Case Name:	<input type="text"/>	AND <input type="button" value="v"/>		
				<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

Searching can be performed by applying a filter using different combinations of **Transaction Status**, **Test Scenario Name**, **Test Case Name**, **Target Cert Alias** and **Request Date**.

If the **Test Scenario Name** is selected then make sure that the correct scenario name is given in order to match it against the records in the database. It will result in a blank report in the History Viewer if an incorrect scenario name is given. Once a correct scenario name is given then it will further filter the records based upon other selected search criteria.



When applying a filter OCSP Monitor will retrieve the records from the database matching any character given in the text fields of the filter criteria.

Test Scenario Name: Enter the scenario name.


Transaction Status: Can be set to either “PASS” or “FAIL”.

Test Case Name: Enter the test case name.

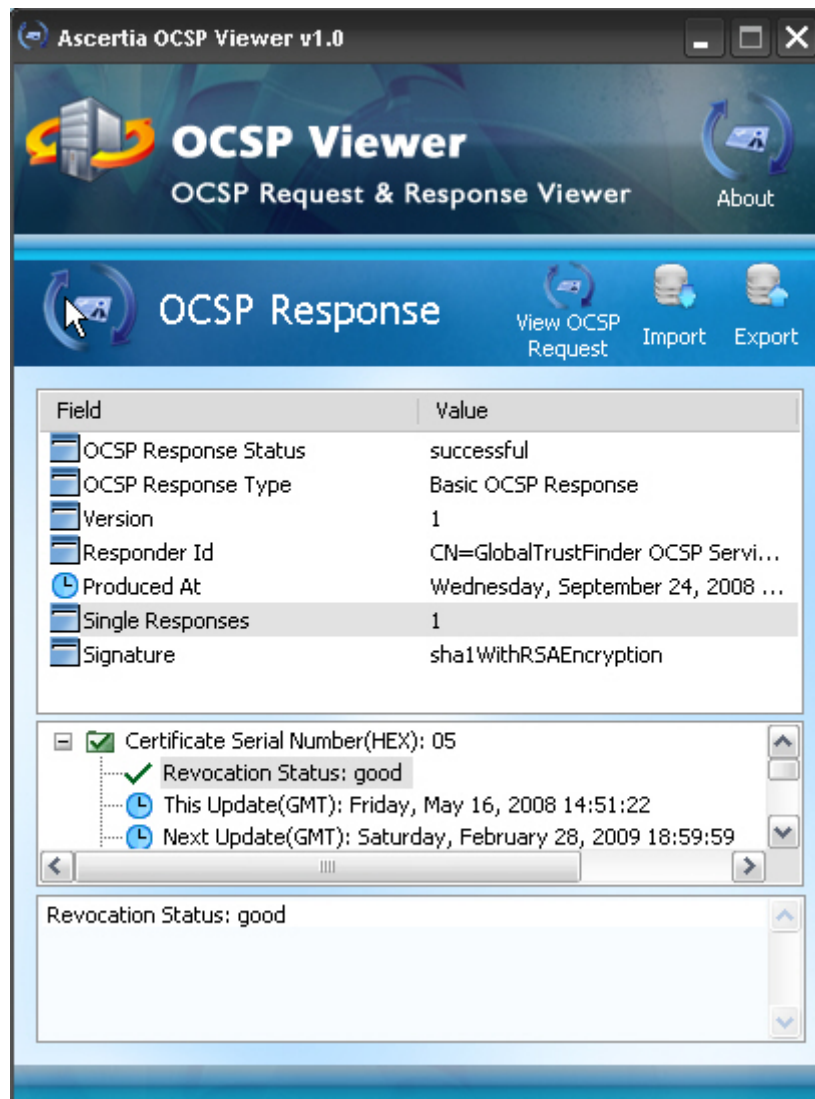
Target Cert Alias: Enter the target certificate alias.

Request Time: Enter the date from which all records starting from the selected date till the present are to be displayed.

A filter can be applied by clicking the **Apply** button and it can be cancelled by clicking on the **Cancel** button.

A filter can be removed from the records by clicking on the show all  button.

To view an actual OCSP request/response transaction, select a transaction and then click on the OCSP viewer button, this will show the following:



This viewer allows both the OCSP request and response message to be shown, by pressing the relevant button from the viewer's toolbar. The transaction can also be exported and saved as a file (and later imported for viewing). The details of each field within the request or response message can be viewed in detail by selecting the field from the top part of the viewer; the bottom part of the viewer then expands on that field.