Trust Monitor - Advanced OCSP Monitor and CRL Monitor Services

OCSP Monitor

Continuous Monitoring and Reporting

Online Certificate Status Protocol (OCSP) servers are the cornerstone of a trusted PKI infrastructure, providing essential e-ID validation services and are the basis for checking the trust and managing the liability associated with this. It is crucial that their validation policy is checked, that they remain highly available to relying parties and that reliable performance statistics can be provided to check service provider SLAs.

OCSP Monitor allows a variety of positive and negative test cases to be defined. One or more test cases can be defined to run each day within a number of Test Scenarios. Various reports are available to provide summary and detailed results.

Automated OCSP Monitoring

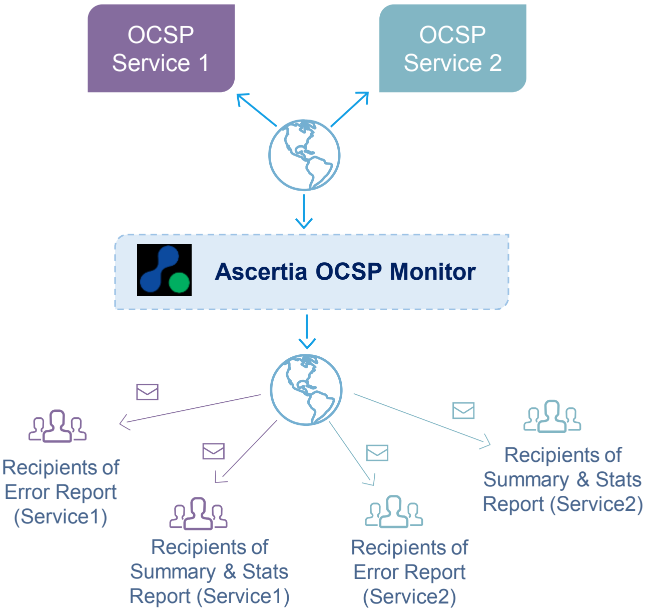
Ascertia OCSP Monitor is a sophisticated test product that enables security administrators to easily detect OCSP service failures or irregularities. It is designed for 24 x 7 automated monitoring although it can also be used interactively when required. OCSP Monitor enables administrators to identify availability or security policy issues and fix unexpected conditions before users report them.

OCSP Monitor is also very useful for organisations that consume OCSP services. They can monitor the service and easily compare this with the Service Level Agreement (SLA). An end-of-day report provides all the key statistics required.

Maximize your OCSP Server uptime

OCSP Monitor provides immediate real-time feedback on OCSP validation issues as they arise. Where OCSP services are used it is often assumed that they are functioning correctly and will continue to do so - this is often not the case.

OCSP Monitor allows multiple test scenarios to be run. These can check for expected and unexpected behaviours and monitor OCSP server performance.

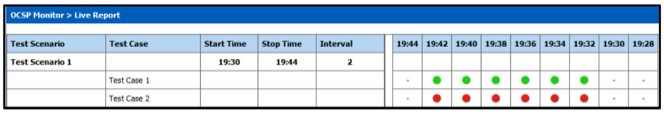

OCSP Service 1
OCSP Service 2
Ascertia OCSP Monitor
Recipients of Error Report (Service1)
Recipients of Summary & Stats Report (Service1)
Recipients of Error Report (Service2)
Recipients of Summary & Stats Report (Service2)

- Automatically and continuously monitors one or more OCSP services for correct functioning and correct results, plus availability and performance
- Runs as a server based monitor service using a secure web-browser interface that enables role based access control for security operators to view results and configure unique tests and package these into a test scenario.
- OCSP responder compliance can be checked using multiple test cases to check compliance with expected validation policy settings
- OCSP Responder availability can be checked using frequent simple test cases to that responses are received in a time way that matches the desired SLA
- For all test cases OCSP Monitor will record any failures and report on these as well as gather statistics to be detailed in an end of day report. Live reporting is also available – see below
- Select which admin staff receive error reports and summary reports by email and/ or SMS
- Test all accessible responders (primary, back-up, test) from a single location with a single tool
- OCSP Monitor is an RFC 6960 compliant OCSP client and can communicate with RFC 6960 compliant responders
- Easy to deploy and use - no server-side component or agent is required for monitoring

Real-time tests

OCSP Monitor tests the status of your OCSP Servers by making real OCSP client requests. It is easy to set up and manage. Multiple test cases can be defined, and then brought together into one or more test scenarios which run for defined periods each day. These can be quickly amended or added to as required.

The following screen shows the live report dashboard screen that allows administrators to review the results obtained from one or more test scenarios. Green means the test ran as expected and red means the test found a problem. Click on the dots to see the details.



OCSP Monitor > Live Report

Test Scenario	Test Case	Start Time	Stop Time	Interval	19:44	19:42	19:40	19:38	19:36	19:34	19:32	19:30	19:28
Test Scenario 1		19:30	19:44	2									
	Test Case 1				-	🟢	🟢	🟢	🟢	🟢	🟢	-	-
	Test Case 2				-	🔴	🔴	🔴	🔴	🔴	🔴	-	-

Ascertia: Identity proven, Trust delivered

ADSS Server – High Trust OCSP Monitor Services

Continuous Monitoring

OCSP Monitor is designed to run 24x7 and allow various Test Scenarios to be run at their configured daily time intervals to monitor performance and validation policy. These approaches are recommended:

- Checking availability and response times by running a check on a valid certificate every few minutes and obtaining the overall service minimum, maximum and average response times
- Checking that a fresh CRL is being used by the OCSP responder, for example using a CRL freshness policy test as required
- Running a comprehensive policy check twice a day to ensure that the defined validation policy is being enforced
- Running checks on disaster recovery systems to ensure they are operational

Detailed Monitoring Checks and Alerts

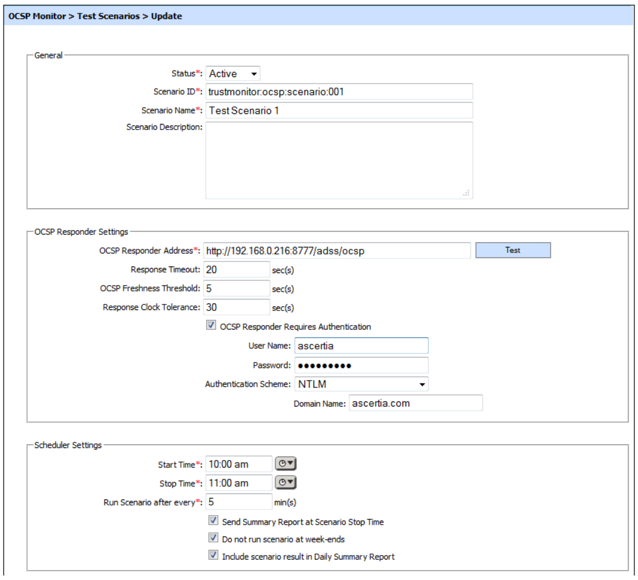
OCSP Monitor has been designed by security experts to provide high quality management information, for example:

- Each test scenario can have several test cases to perform multiple positive and negative checks
- Each test scenario can have its own trust anchors defined for accurate trust checking
- When a test scenario fails a customisable failure report is sent to a defined list of operations staff - each scenario can have different staff identified
- Customisable reports can be sent using SMS or email or both as required - both internal and external staff can be notified - useful when using managed services
- When a scenario completes a summary report can be sent to selected service management staff showing the minimum, average and maximum response delay statistics observed as well as a summary of the successful and failed tests observed during the period
- At the end of day a summary report for all scenarios can be sent to service management staff detailing the main statistics for all scenarios

Easy Configuration

OCSP Monitor has an intuitive wizard to help set-up test scenarios and the required test cases within these. Each test scenario can be set to run between specific start and stop times. Reports can be customised per test scenario.

Part of the Test Scenario update screen is shown below:



OCSP Monitor > Test Scenarios > Update

General

Status*: Active

Scenario ID*: trustmonitor:ocsp:scenario:001

Scenario Name*: Test Scenario 1

Scenario Description:

OCSP Responder Settings

OCSP Responder Address*: http://192.168.0.216:8777/adss/ocsp

Response Timeout: 20 sec(s)

OCSP Freshness Threshold: 5 sec(s)

Response Clock Tolerance: 30 sec(s)

☑ OCSP Responder Requires Authentication

User Name: ascertia

Password: ●●●●●●●●●

Authentication Scheme: NTLM

Domain Name: ascertia.com

Scheduler Settings

Start Time*: 10:00 am

Stop Time*: 11:00 am

Run Scenario after every*: 5 min(s)

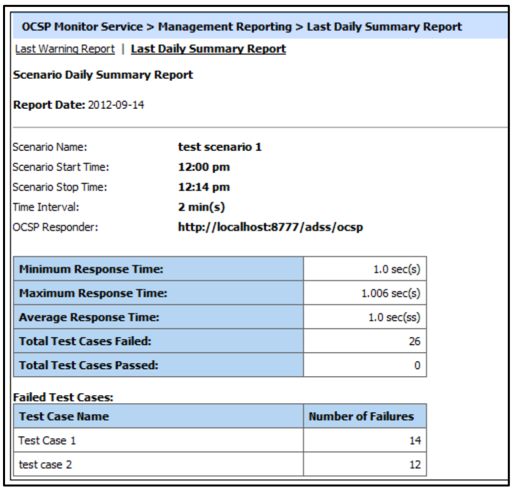
☑ Send Summary Report at Scenario Stop Time

☑ Do not run scenario at week-ends

☑ Include scenario result in Daily Summary Report

Detailed Reporting

OCSP Service Level Agreements can now be accurately checked and reported on. The ability to identify and report on OCSP service issues has been difficult until now. OCSP Monitor provides for easy change of test policies so that a selected level of detailed testing can be carried as required to suit the business demands. History data is maintained and detailed analysis of OCSP request and response data is available as a standard feature. Immediate warning reports and also daily summary reports are produced that provide valuable information:



OCSP Monitor Service > Management Reporting > Last Daily Summary Report

Last Warning Report | Last Daily Summary Report

Scenario Daily Summary Report

Report Date: 2012-09-14

Scenario Name:	test scenario 1
Scenario Start Time:	12:00 pm
Scenario Stop Time:	12:14 pm
Time Interval:	2 min(s)
OCSP Responder:	http://localhost:8777/adss/ocsp

Minimum Response Time:	1.0 sec(s)
Maximum Response Time:	1.006 sec(s)
Average Response Time:	1.0 sec(ss)
Total Test Cases Failed:	26
Total Test Cases Passed:	0

Failed Test Cases:

Test Case Name	Number of Failures
Test Case 1	14
test case 2	12

OCSP Monitor Standards Compliance:

Standards:	RFC 6960 OCSP
Certificate types:	X.509v3 certificates for test cases
Operating systems:	Windows Server 2016, 2012 R2, 2012, 2008 R2, Linux (RedHat, Centos, SuSe, others)
Databases:	SQL Server 2016, 2014, 2012, Oracle 12c, 11g, PostgreSQL 9, 8, MySQL (Percona & Oracle), Azure SQL
Interfaces:	HTTP and HTTPS communications for OCSP requests/ responses
Operator interface:	Mutually-authenticated HTTPS secure web-interface for administrators, plus email, SMS, SNMP & syslog alerting

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: 2017-11-14 15:38:32 +00:00
Reason: I approve this document

Rod Crook

Ascertia Limited
ascertia
Identity proven, Trust delivered

Ascertia: Identity proven, Trust delivered