ONVIF™

Analytics Client Test Specification

Version 17.06

June 2017

REVISION HISTORY

Vers.	Date	Description
17.06	Jun 15, 2017	The following test cases added accoring to #201: Motion Detection Test Cases
17.06	Jun 14, 2017	First issue of Analytics Client Test Specification. The following test cases added accoring to #201: Get Supported Rules Test Cases Get Rules Test Cases

Table of Contents

1 Introduction

The goal of the ONVIF Test Specification set is to make it possible to realize fully interoperable IP physical security implementations from different vendors. This specification also acts as an input document to the development of a test tool which will be used to test the ONVIF Client implementation conformance towards ONVIF standard. This Client Test Tool analyzes network communications between ONVIF Devices and Clients being tested and determines whether a specific Client is ONVIF conformant (see ONVIF Conformance Process Specification).

This particular document defines test cases required for testing Analytics features of a Client application e.g. Get Supported Rules, Get Rules, Create Rules, Motion Region Detector rule configuration and Motion Region Detecto event notification. It also describes the test framework, test setup, prerequisites, test policies needed for the execution of the described test cases.

1.1 Scope

This ONVIF Analytics Client Test Specification defines and regulates the conformance testing procedure for the ONVIF conformant Clients in the scope of Analytics Service features. Conformance testing is meant to be black-box network traces analysis and verification. The objective of this specification is to provide the test cases to test individual requirements of ONVIF Clients in the scope of Analytics Service features according to ONVIF Analytics Service Specification.

The principal intended purposes are:

- Provide self-assessment tool for implementations.
- Provide comprehensive test suite coverage for Analytics Service features.

This specification **does not** address the following:

- Product use cases and non-functional (performance and regression) testing and analysis.
- SOAP Implementation Interoperability test i.e. Web Services Interoperability Basic Profile version 2.0 (WS-I BP2.0).
- Network protocol implementation Conformance test for HTTPS, HTTP, RTP and RTSP protocols.

The following sections cover test cases needed for the verification of relevant features as mentioned in the ONVIF Profile Specifications.

1.2 Get Supported Rules

Get Supported Rules section specifies Client ability to retrieve supported rules.

1.3 Get Rules

Get Rules section specifies Client ability to retrieve available rules.

1.4 Motion Detection

Motion Detection section specifies Client ability to create Motion Region Detector rules and to receive notifications of Motion Region Detector events.

2 Normative references

- ONVIF Conformance Process Specification:

  https://www.onvif.org/profiles/conformance/

- ONVIF Profile Policy:

  https://www.onvif.org/profiles/

- ONVIF Core Specifications:

  https://www.onvif.org/profiles/specifications/

- ONVIF Core Client Test Specification:

  https://www.onvif.org/profiles/conformance/client-test/

- ONVIF Profile T Specification:

  https://www.onvif.org/profiles/profile-t/

- ONVIF Analytics Service Specification:

  https://www.onvif.org/profiles/specifications/

- ISO/IEC Directives, Part 2, Annex H:

  www.iso.org/directives

- ISO 16484-5:2014-09 Annex P:

  https://www.iso.org/obp/ui/#!iso:std:63753:en

- W3C SOAP 1.2, Part 1, Messaging Framework:

  http://www.w3.org/TR/soap12-part1/

- W3C XML Schema Part 1: Structures Second Edition:

  http://www.w3.org/TR/xmlschema-1/

- W3C XML Schema Part 2: Datatypes Second Edition:

  "http://www.w3.org/TR/xmlschema-2/ [http://www.w3.org/TR/xmlschema-2/]

- W3C Web Services Addressing 1.0 – Core:

  http://www.w3.org/TR/ws-addr-core/

3 Terms and Definitions

3.1 Conventions

The key words "shall", "shall not", "should", "should not", "may", "need not", "can", "cannot" in this specification are to be interpreted as described in [ISO/IEC Directives Part 2].

3.2 Definitions

This section describes terms and definitions used in this document.

Address	An address refers to a URI.
Profile	See ONVIF Profile Policy.
ONVIF Device	Computer appliance or software program that exposes one or multiple ONVIF Web Services.
ONVIF Client	Computer appliance or software program that uses ONVIF Web Services.
Conversation	A Conversation is all exchanges between two MAC addresses that contains SOAP request and response.
Network	A network is an interconnected group of devices communicating using the Internet protocol.
Network Trace Capture file	Data file created by a network protocol analyzer software (such as Wireshark). Contains network packets data recorded during a live network communications.
Media Profile	A media profile maps a video and/or audio source to a video and/or an audio encoder, PTZ and analytics configurations.
SOAP	SOAP is a lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. It uses XML technologies to define an extensible messaging framework providing a message construct that can be exchanged over a variety of underlying protocols.
Client Test Tool	ONVIF Client Test Tool that tests ONVIF Client implementation towards the ONVIF Test Specification set.
Valid Device Response	Device has responded to specific request with code HTTP or RTSP 200 OK and SOAP fault message has not appeared.

3.3 Abbreviations

This section describes abbreviations used in this document.

HTTP Hyper Text Transport Protocol.

HTTPS Hyper Text Transport Protocol over Secure Socket Layer.

URI Uniform Resource Identifier.

WSDL Web Services Description Language.

XML eXtensible Markup Language.

3.4 Namespaces

Prefix and namespaces used in this test specification are listed in Table 1. These prefixes are not part of the standard and an implementation can use any prefix.

Table 3.1. Defined namespaces in this specification

Prefix	Namespace URI	Description
soapenv	http://www.w3.org/2003/05/soap-envelope	Envelope namespace as defined by SOAP 1.2 [SOAP 1.2, Part 1]
tt	http://www.onvif.org/ver10/schema	ONVIF XML schema descriptions
axt	http://www.onvif.org/ver20/analytics/wsdl	The namespace for the WSDL Analytics service
tns1	http://www.onvif.org/ver10/topics	The namespace for the ONVIF topic namespace

4 Test Overview

This section provides information for the test setup procedure and required prerequisites that should be followed during test case execution.

An ONVIF Client with Analytics features supports and with Motion Region Detector rule support can retrieve available Rules, create tt:MotionRegionDetector rule, and receive notifications of Motion Region Detector events.

An ONVIF Profile is described by a fixed set of functionalities through a number of services that are provided by the ONVIF standard. A number of services and functionalities are mandatory for each type of ONVIF Profile. An ONVIF Device and ONVIF Client may support any combination of Profiles and other optional services and functionalities.

4.1 General

Test Cases are grouped depending on features. Each Test Cases group provides description of feature requirement level for Profiles, expected scenario under test and related test cases:

- Feature Level Requirement
- Expected Scenarios Under Test
- List of Test Cases

4.1.1 Feature Level Requirement

Feature Level Requirement item contains a feature ID and feature requirement level for the Profiles, which will be used for Profiles conformance.

If Feature Level Requirement is defined as Mandatory for some Profile, Client shall pass Expected Scenario Under Test for each Device with this Profile support to claim this Profile Conformance.

If Feature Level Requirement is defined as Conditional, Optional for some Profile, Client shall pass Expected Scenario Under Test for at least one Device with this Profile support to claim feature as supported.

4.1.2 Expected Scenarios Under Test

Expected Scenarios Under Test item contains expected scenario under test, conditions when the feature will be defined as supported and as not supported.

4.1.3 Test Cases

Test Case items contain list of test cases which are related to feature. Test cases provide exact procedure of testing feature support conditions.

Each Test Case contains the following parts:

- Test Label - Unique label for each test
- Test Case ID - Unique ID for each test
- Profile Normative References - Requirement level for the feature under test is defined in Profile Specification. This reference is informative and will not be used in conformance procedure.
- Feature Under Test - Feature which is under current test. Typically a particular command or an event.
- Test Purpose - The purpose of current test case.
- Pre-Requisite - The pre-requisite defines when the test should be performed. In case if pre-reqiusite does not match, the test result will be NOT DETECTED.
- Test Procedure - scenario expected to be reflected in network trace file.
- Test Result - Passed and failed criteria of the test case. Depending on these criteria test result will be defined as PASSED or FAILED.
- Validated Feature List - list of features ID related to this test case.

4.2 Test Setup

Collect Network traces files required by the test cases.

Collect Feature List XML files for Devices detected in the Network Trace files.

Client shall support all mandatory and conditional features listed in the Device Feature List XML file supplied for the Profiles supported by the Client.

For ONVIF compatibility, the ONVIF Client shall follow the requirements of the conformance process. For details please see the latest ONVIF Conformance Process Specification.

4.3 Prerequisites

The pre-requisites for executing the test cases described in this Test Specification include:

The Device shall be configured with an IPv4 address.

The Device shall be able to be discovered by the Client.

5 Get Supported Rules Test Cases

5.1 Feature Level Requirement:

Validated Feature: Get Supported Rules

Profile T Requirement: Conditional

5.2 Expected Scenarios Under Test:

1. Client connects to Device to retrieve supported Rules using the **GetSupportedRules** operation.
2. Client is considered as supporting Get Supported Rules if the following conditions are met:
   - Client is able to retrieve supported Rules using the **GetSupportedRules** operation.
3. Client is considered as NOT supporting Get Supported Rules if ANY of the following is TRUE:
   - No valid device response to **GetSupportedRules** request.

5.3 GET SUPPORTED RULES

Test Label: Get Supported Rules

Test Case ID: GETSUPPORTEDRULES-1

Profile T Normative Reference: Conditional

Feature Under Test: Get Supported Rules

Test Purpose: To verify that Client is able to retrieve supported rules using the **GetSupportedRules** operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one conversation between Client and Device with GetSupportedRules operation present.
- Device supports Rule Engine (RuleEngine).

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **GetSupportedRules** request message to retrieve supported Rules from the Device.
2. Device responds with code HTTP 200 OK and **GetSupportedRulesResponse** message.

Test Result:

PASS -

- Client **GetSupportedRules** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **GetSupportedRules** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **axt:GetSupportedRules** AND
- Device response on the **GetSupportedRules** request fulfills the following requirements:
  - [S2] It has HTTP 200 response code AND
  - [S3] **soapenv:Body** element has child element **axt:GetSupportedRulesResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: get_supported_rules.get_supported_rules

6 Get Rules Test Cases

6.1 Feature Level Requirement:

Validated Feature: Get Rules

Profile T Requirement: Conditional

6.2 Expected Scenarios Under Test:

1. Client connects to Device to retrieve available Rules using the **GetRules** operation.
2. Client is considered as supporting Get Rules if the following conditions are met:
   - Client is able to retrieve available Rules using the **GetRules** operation.
3. Client is considered as NOT supporting Get Rules if ANY of the following is TRUE:
   - No valid device response to **GetRules** request.

6.3 GET RULES

Test Label: Get Rules

Test Case ID: GETRULES-1

Profile T Normative Reference: Conditional

Feature Under Test: Get Rules

Test Purpose: To verify that Client is able to retrieve available rules using the **GetRules** operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one conversation between Client and Device with GetRules operation present.
- Device supports Rule Engine (RuleEngine).

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **GetRules** request message to retrieve available Rules from the Device.
2. Device responds with code HTTP 200 OK and **GetRulesResponse** message.

Test Result:

PASS -

- Client **GetRules** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **GetRules** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **axt:GetRules** AND
- Device response on the **GetRules** request fulfills the following requirements:
  - [S2] It has HTTP 200 response code AND
  - [S3] **soapenv:Body** element has child element **axt:GetRulesResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: get_rules.get_rules

7 Motion Detection Test Cases

7.1 Feature Level Requirement:

Validated Feature: Motion Detection

Profile T Requirement: Conditional

7.2 Expected Scenarios Under Test:

1. Client connects to Device to retrieve available Rules using the **GetRules** and **GetSupportedRules** operations.
2. Client creates Rules of type **tt:MotionRegionDetector** using the **GetRuleOptions** and **CreateRules** operations.
3. Client subscribes to device messages using **CreatePullPointSubscription** operation to get **Motion Region Detector** notifications.
4. Client is considered as supporting Motion Detection if the following conditions are met:
   - Client supports **Get Supported Rules** feature AND
   - Client supports **Get Rules** feature AND
   - Client supports **EventHandling_Pullpoint** feature AND
   - Client is able to retrieve options of Rules of type **tt:MotionRegionDetector** using **GetRuleOptions** operation AND
   - Client is able to create Rules of type **tt:MotionRegionDetector** using **CreateRules** operation AND
   - Client is able to retrieve **tns1:RuleEngine/MotionRegionDetector/Motion** notifications about Motion Region Detector if device supports MotionRegionDetector Rule.
5. Client is considered as NOT supporting Motion Detection if ANY of the following is TRUE:
   - Client does not support **Get Supported Rules** feature OR
   - Client does not support **Get Rules** feature OR
   - Client does not support **EventHandling_Pullpoint** feature OR
   - No valid device response to **GetRuleOptions** request with RuleType value is equal to **tt:MotionRegionDetector** OR

- No valid device response to **CreateRules** request with Rule Type value is equal to **tt:MotionRegionDetector** OR
- Client is not able to retrieve **tns1:RuleEngine/MotionRegionDetector/Motion** notifications about Motion Region Detector if device supports MotionRegionDetector Rule.

7.3 GET MOTION REGION DETECTOR RULE OPTIONS

Test Label: Get Rule Options

Test Case ID: MOTIONDETECTION-1

Profile T Normative Reference: Conditional

Feature Under Test: Get Rule Options

Test Purpose: To verify that Client is able to retrieve MotionRegionDetector rule options using the **GetRuleOptions** operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one conversation between Client and Device with GetRuleOptions operation with RuleType value is equal to **tt:MotionRegionDetector** present.
- Device supports Rule Options (RuleOptions).

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **GetRuleOptions** request message with RuleType value is equal to **tt:MotionRegionDetector** to retrieve motion region detector rule options from the Device.
2. Device responds with code HTTP 200 OK and **GetRuleOptions** message.

Test Result:

PASS -

- Client **GetRuleOptions** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **GetRuleOptions** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **axt:GetRuleOptions** AND

- [S2] **axt:GetRuleOptions** element has child element **axt:RuleType** AND
- [S3] **axt:GetRuleOptions/axt:RuleType** element value is equal to **tt:MotionRegionDetector** AND

- Device response on the **GetRuleOptions** request fulfills the following requirements:
  - [S2] It has HTTP 200 response code AND
  - [S3] **soapenv:Body** element has child element **axt:GetRuleOptionsResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: motion_detection.get_motion_region_detector_rule_options

7.4 CREATE MOTION REGION DETECTOR RULE

Test Label: Create Rules

Test Case ID: MOTIONDETECTION-2

Profile T Normative Reference: Conditional

Feature Under Test: Create Rules

Test Purpose: To verify that Client is able to create MotionRegionDetector rule using the **CreateRules** operation.

Pre-Requisite:

- The Network Trace Capture files contains at least one conversation between Client and Device with **CreateRules** operation with Rule Type value is equal to **tt:MotionRegionDetector** present.
- Device supports Rule Engine (RuleEngine).

Test Procedure (expected to be reflected in network trace file):

1. Client invokes **CreateRules** request message with Rule element that has Type value is equal to **tt:MotionRegionDetector** to create motion region detector rule on the Device.
2. Device responds with code HTTP 200 OK and **CreateRules** message.

Test Result:

PASS -

- Client **CreateRules** request messages are valid according to XML Schemas listed in Namespaces AND
- Client **CreateRules** request in Test Procedure fulfills the following requirements:
  - [S1] **soapenv:Body** element has child element **axt:CreateRules** AND
  - [S2] **axt:CreateRules** element has child element **axt:Rule** with **@Type = tt:MotionRegionDetector** AND
- Device response on the **CreateRules** request fulfills the following requirements:
  - [S3] It has HTTP 200 response code AND
  - [S4] **soapenv:Body** element has child element **axt:CreateRulesResponse**.

FAIL -

- The Client failed PASS criteria.

Validated Feature List: motion_detection.create_motion_region_detector_rule